

A Complete Bibliography of Publications in *International Journal of Information Security*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254

FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)

WWW URL: <https://www.math.utah.edu/~beebe/>

26 September 2023

Version 1.32

Title word cross-reference

128-bit [CDP22]. **19** [PGMPPC22].
2.0 [AMLH18, MP22]. **2002** [ACM05]. **2003** [BM05, Sne05]. **2004** [DSY06]. **2012** [SKK+17]. **2013** [BJ15]. **25022** [MD23b].
 (t, n) [QDW09]. 2^w [Bae10]. K [BHZ+21, BDD01, MU18, RMSCR19, Rov23, TNA23]. LU [MARK20]. n [CC12]. $O(n)$ [DYDW10]. t [BDD01].
3 [ABM+12]. **3GPP** [EWR+09]. **3T's** [RB23].
-anonymity [TNA23]. **-anonymization** [MU18, RMSCR19]. **-ary** [Bae10]. **-based** [Yan21]. **-database** [BDD01]. **-Diffie** [CC12]. **-means** [Rov23]. **-private** [BDD01].
4.0 [SDG22].
5 [DWU+23]. **5G** [Alg22, KIP22].
.NET [KKKV07].
802.15.6 [KDM22]. **88** [vOLW05].
/SSL [BJ16].
= [TGNA22].
1 [KJS17]. **100G** [GDA22]. **11770** [CH16].
AAIA [YYH+23]. **AAAnA** [SK14].

abnormal [JJJ21]. **absence** [AvO13].
absolute [AvO13]. **abstract**
 [BLM11, DM07, MS14]. **abstract-based**
 [BLM11]. **abstraction** [MLCS16]. **abused**
 [CYA+18]. **AC** [Mdmf22]. **Acceptable**
 [BB04b]. **Access**
 [Lop18, SAL17, AMZ22, ACF17, AFA+23,
 ACBC+15, BAB23, BLM11, CF03, CK08,
 CZ06, GGJ22, HSMY12, IOU+21, JSMG18a,
 KAC16, KAC17, Kud02, LD17, LRB+10,
 MG23, MS15, PMDS23, Pen12,
 PMPGMLLM12, RD16, RT23, SRD+21].
accessibility [SHA20]. **Accessible** [KB23].
account [BRS06]. **Accountable** [GGJ22].
accounts [ASN+16]. **accreditation**
 [DFBJR18]. **Accumulable** [SEXY18].
accumulator [KYH18]. **accumulators**
 [CHKO12, HRMM20, JCL+18]. **accuracy**
 [QLOW09]. **accurate** [CYA+18, SSD14].
achievable [Pla09]. **achieve** [Pen13].
Achieving [AICC18, IZS08, RSD19]. **ACM**
 [BJ15]. **acoustic** [CBRY20, HS15].
acquisition [YP12]. **across** [IKS22]. **action**
 [JG15, PKHS23]. **action-mask** [PKHS23].
actionable [SBG22]. **Active** [LCPD14,
 CBRY20, CBC08, DGZFGH13, LTC23].
activities [JJJ21, OBH+20, YKP22].
activity [AAZAA23]. **actual** [MTSH18].
actually [BM11]. **Ad**
 [LH23, Gol12, MS11, SF17]. **ad-hoc** [MS11].
Adapting [GLP03, Sen14]. **Adaptive**
 [GZH+23, PPSS13, MdSC+15]. **Adding**
 [CON09]. **Additional** [YAY+21].
addressing [ASA23]. **administration**
 [KK22]. **adoption** [ZJS22]. **ADroid**
 [RHGTSC17]. **advanced**
 [PGMLK+13, TS20, TMP13]. **Adversarial**
 [KCC+23, LSR+23, AVM23, GZH+23,
 TCE23, ZTV23]. **adversary**
 [ORK23, QDW09]. **adverse** [SGC22].
advertising [KOSU16, UBK23]. **affects**
 [CFBvO09]. **After** [PSTS20]. **against**
 [ANN23, AP22, BHL+21, DdP13, EMRN17,
 FTS+20, GYL+07, GI19, KK17, LSR+23,
 MLYL20, MS11, MYLZ14, Nui12, SK06,
 SB22, SAH22, TSMH19, VSR15, WWZ+23,
 YYH+23, BZ20, ZRJ14]. **agent**
 [LV10, PKHS23, PDM20, TGNA22, EZ22].
agent-based [PDM20]. **Aggregate** [CL13].
aggregation
 [GLMS19, GKS19, LL21, YYH+23].
aggregation-based [GLMS19]. **agile**
 [SHOL23]. **agreement** [AAV22, CCS07,
 CL09, FGS12, GNS14, KDM22, WQW+17].
AI [ZP23]. **AI-assisted** [ZP23]. **AiCEF**
 [ZP23]. **aided** [NT20]. **AIHGAT** [WGH23].
Alambic [ABFO08]. **alert**
 [Mdmf22, SGJ19]. **alerts** [STD21].
algebraic [DS07, KM10, SSVC16].
Algorithm [AP22, JMV01, AT22, Bae10,
 BHZ+21, GS15, MB23, MU18, PV22,
 SKK+17, TLX09, Zen22]. **algorithms**
 [ASA23, BEPL+17, KU16, ML14, WT21].
alignment [KSM10]. **all-encompassing**
 [EHM15]. **All-or-Nothing** [MTW+14].
allocation [SGJ19]. **allotROPism**
 [LNX22]. **along** [VH19]. **AMACs** [CL13].
ambients [TZH04]. **among** [AHX+23].
analyses [TS22]. **Analysing** [HL04].
Analysis [AMRR17, BR20, CG14, DBMS10,
 GLP03, SSFB15, Zha23, ZZW+10, AGZA22,
 ABCC08, ASN+16, AAB20, AC08, BGKZ12,
 BEPL+17, Bel10, BDMM19, BR23, BBR18,
 BFT08, BNN04, CPPK15, CF07, DFF+16,
 DRPW12, FN19, dSFK19, GAdFGM23,
 GLMS+04, GKBS12, HLKI15, IMI18,
 IOU+21, IDHRPCMP15, KW15, KAC17,
 KKK22a, KA18, LRB+10, MWZ06,
 MTW+14, MD23b, NRC15, OO20, OT06,
 PCT22, PDB11, QLOW09, RSV23, SK16,
 SS05a, SB09, SSM+20, SSL22a, SSE+15,
 SDG22, SPDR17, SRSM23, Vaj16, VdWZ14,
 WYL+12, WGH23, XSA13, YWW22, YA22,
 YL19, ZHZ22]. **analysis-based** [BR23].
analytics [SCO21]. **analyzer** [PAI+23].
Analyzing [BJ16, GMLM23, RRI+19,
 vOLW05, ABK22, SGLC19]. **anchor**
 [BB04b]. **AND-gate** [JSMG18b]. **Android**

[LSV⁺23, ACS21, AAB20, BSK⁺23, CAS22, EZLC21, GPS17, IS23, IOU⁺21, IKS22, IDHRPCMP15, KBY22, KA18, LMMS17, LWL⁺21, LSG22, LLG22, MGR19, MS15, RHGTSC17, STW⁺23]. **Anomalous** [AZ22]. **anomaly** [DGF⁺17, KCM⁺15, MD23a, ME23, RHGTSC17, SKH⁺23]. **anomaly-based** [RHGTSC17]. **Anonymity** [GP23, LSWW14, Man21, BSK⁺20, DFBJR18, HLS18, SS05a, TNA23]. **anonymization** [AT22, CR20, HN14, MU18, RMSCR19]. **anonymizing** [ZO13]. **Anonymous** [BFG⁺13, LeSCL⁺18, SK14, ACHO13, ABFL12, BSV22, BCL09, CPPK15, KLPL21, KWCK19, KCB17, SF17, SDR20]. **ANS** [CDP22]. **ANS-based** [CDP22]. **answer** [RRI⁺19, WZ07]. **anti** [GKBS12, KKK22b, AHC⁺21]. **Anti-BIUFF** [AHC⁺21]. **anti-malware** [KKK22b]. **anti-SPIT** [GKBS12]. **antiviruses** [ASAAS15]. **any** [DdP13]. **AOMDV** [MG19]. **API** [IKS22, You06]. **app** [CAS22, IKS22]. **apples** [BBR18]. **applicable** [QDW⁺15]. **application** [ACS21, ANN23, BB22, BEd23, DGF⁺17, KSB23, Pen12, RSV23, Roe11a, Roe11b, SPM13, VdWZ14, ZZW⁺10]. **application-layer** [DGF⁺17]. **Applications** [Gri06, AAB20, BCA⁺10, BR23, BNTW12, DJN10, DTK⁺18, GSS10, HSMY12, HZL⁺17, KGG09, LS23, SCO21, SNX19, TSZ22, WYL⁺12, WCS20, vORM06]. **Applied** [BJ15]. **Applying** [MI22]. **approach** [AuHD⁺23, AZ22, AV17, BHL⁺21, CFG17, CMS10, BABB16, DS07, EZLC21, Fra18, GA23, HBH12, JBK21, KAC16, KAC17, KCB20, KKK17, KDYS19, LVK18, LTC23, LH23, MGV17, MARK20, MMS16, MLCQ21, MG23, ME23, MSGCDPSS18, MYLZ14, MP22, NNL20, NA14, PM23, PNG⁺20, SRK⁺20, SGSS23, TWP08, VSR15, ZKP⁺23]. **approaches** [JJJ21, SBS23, SAH22, ZO13, ZSN23]. **approximate** [Rov23]. **apps** [CSL⁺23, EZLC21, GPS17]. **APT** [SGSS23]. **APTs** [GMdFLR23]. **architecture** [AKG16, BS22, EHM15, EWR⁺09, FZ21, LV10, MSP⁺13, MdAN23, MSKS20, SRSM23, TCE23, Zha23]. **architectures** [AFA⁺23, SSL22a, WW07]. **area** [LCL16, MPG21]. **areas** [BS21]. **arguments** [ABM⁺12]. **arithmetic** [ABB17, KW15]. **ARITO** [SSD14]. **ARM** [BZ20]. **art** [TDGL23]. **ary** [Bae10]. **ASICS** [BCF⁺17]. **aspects** [AICC18]. **assembly** [WGH23, Zha23]. **assessment** [AK23, EAM⁺23, HXTP23, JBK21, KB23, NBA⁺21, Sep23, WHS18, ZTG22]. **Asset** [SSR22]. **assigned** [JTV19]. **assisted** [DYDW10, LWL23, PDM20, VPI15, ZP23]. **association** [OBH⁺20, VH19]. **assumption** [HIST09]. **assurance** [ABN14, LVK18, SKY23]. **asymmetric** [ZWQ⁺17]. **Ate** [ZZH08]. **ATNA** [ACBC⁺15]. **attack** [AZ19, AYHK18, ASZ⁺23, BB22, BHZ⁺21, CSL⁺23, DSB19, DRPW12, FAMMZ23, dSFK19, GMS03, GZH⁺23, KAK23, Lu09, ML14, PHS22, RSV23, SLGP23, SS05a, SBD23, SSD14, SSL22b, SSV22, SDG22, TCT22, WWZ⁺23, YAY⁺21, YYH⁺23, ZXZ⁺11]. **attacker** [RMPADF13]. **Attacking** [SGE02]. **Attacks** [AKZM20, MLC23, ASAAS15, AP22, BHL⁺21, BRS06, BDG23, CK23a, CK23b, CKKK23, CBRY20, BABB16, DGF⁺17, EMRN17, FTS⁺20, HS15, HXTP23, Hub12, JK22, KSB23, KM10, KDYS19, LLWY09, LSR⁺23, LH23, MLCQ21, MLYL20, MS11, NBA⁺21, ORK23, Pen11, PSTS20, PNG⁺20, PPL15, SGLC19, SB22, SSVC16, TTS⁺06, VSR15, XCW⁺12, YNC22, ZTV23]. **Attention** [ACS21]. **attestation** [BFG⁺13, BCL09, CGL⁺11, KLPL21]. **attitude** [AHX⁺23]. **Attribute**

[SRD⁺21, TNA23, BAB23, GGJ22, JSMG18a, JSMG18b, KLZ⁺21, NCBG23, ORK23, PMDS23, QLZH15, QDW⁺15, RD16, ZLZL20]. **Attribute-based** [SRD⁺21, BAB23, GGJ22, JSMG18a, JSMG18b, KLZ⁺21, PMDS23, QLZH15, QDW⁺15, RD16, ZLZL20]. **attributes** [JSMG18a, KLZ⁺21]. **auctions** [Bra06]. **audio** [dSFK19]. **Audit** [CCD⁺07, BS05]. **Audit-based** [CCD⁺07]. **auditing** [SXZC20, WMS⁺19]. **AUTH** [RG13]. **Authenticated** [HM22, AAV22, BBR18, BCF⁺17, CHMS21, IMI18, KDM21, Lin15, MPS10, Ust11, YLL⁺18, YRW14, ZWQ⁺17]. **Authenticating** [CF07, AZ22]. **Authentication** [BAB23, DNF⁺19, GCSÁBdSS12, AGZA22, BPW05b, BEY23, Bra22, BJ16, CL13, DSB19, DFF⁺16, EWR⁺09, Gol12, GTM11, Hal20, HC10, HCN15, HL04, HKO22, IS23, IT05, KKY⁺23, KWCK19, KML03, KB13, LSWW14, LCPD14, LSR⁺23, MB16, ML17, MSKD16, MS09, MNC20, MD23b, MP22, PS17, RG13, SK14, Smi04, SCO21, SDR20, TWP08, VHT09, WLLW14, YWW22]. **Authentication-enabled** [BAB23]. **authentications** [HZL⁺17]. **authenticators** [SXZC20]. **authorities** [LMMO04]. **authority** [CON09, QLZH15]. **authorization** [BZV05, KLMM09, MP22, RV03, SSFB15, SK14, WZ07]. **authorized** [ZZG19]. **automata** [BCL13, DLR15, LBW05]. **Automated** [BB22, GLMS⁺04, JG15, GH05, SSM⁺20, dAKdG10]. **Automatic** [SDG22, ACMV15, CAS22, KKK22a, PLA⁺21, ZLGZ19]. **automatically** [KM07, XCW⁺12]. **automating** [SNX19]. **automation** [CSL⁺23]. **autoML** [PAI⁺23]. **autonomous** [AG23]. **availability** [Bel10]. **AVL** [RBD02]. **aware** [Alg22, DGF⁺17, KJG⁺11, MBRPS18, RSPMB16, SRK⁺20, TGNA22, Vaj16, YKP22]. **awareness** [MPS14]. **AWS** [AMZ22].

back [KNL16]. **balance** [MYLZ14]. **BAPRP** [LH23]. **BAR** [KCB17]. **Based** [LLW⁺16, AK23, AYHK18, ACB14, ASZ⁺23, AuHD⁺23, AZ22, AC08, BHKM23, BFP03, BFPP07, BR23, BS22, BAB23, BBR18, BLM11, CDP22, CCD⁺07, CSC⁺23, CMS10, CCS07, CHZ16, CFBvO09, BABB16, CSL⁺23, CG23, CK08, Dan07, Des09, EZLC21, EMRN17, FZ21, FAMMZ23, FGS12, GCH⁺19, GPS17, GLMS19, GGJ22, GDA22, GBDJ14, GMSS23, GTM11, HJDC15, Ham23, HS09, HC10, HRL09, HKO22, INS21, IMI18, IT05, JCL⁺18, JSMG18a, JSMG18b, JBK21, KG11, KLZ⁺21, KAK22, KBY22, KKY⁺23, KKK17, KM22, KML03, KLMM09, Kud02, KB22, KNL16, LMG17, LKH09, LLH21, sLC05, LH15, LMD17, LD17, LWA21, LP11, LBZ⁺10, LMMO04, LSR⁺23, LSG22, LSV⁺23, LLG22, MPS10, MGV17, MPS14, MP15, MS09, MMS16, MKS⁺23, MdMF22, MLYL20, MK21, MS11, MD23b, MUIH⁺21, MS14, ME23, Moh23, MLC23, MB23]. **based** [MRW02, MSGCDPSS18, MFES04, NAM06, NSNK06, NNL20, NMBB12, OT06, PMDS23, PDM20, Pen11, PGMPPC22, PPL15, QLZH15, QDW09, QDW⁺15, RD16, RBEH15, RG13, RMSCR19, Rov23, RV03, RHGTSC17, SJ09, SBB19, SV11, SPM13, SKLP20, SSP14, SS05a, SBD23, SRK⁺20, SSL22a, STW⁺23, SK14, SRD⁺21, SS05b, SdHZ16, SCO21, SSJ22, SHW23, SAT09, SDR20, SGE02, SPDR17, TLX09, TDRR20, TND⁺15, Ust11, VH19, WR08, WCS20, XCW⁺12, XSA13, Yan21, YA22, YL20, YSM10, ZBC23, ZGC07, ZWQ⁺17, ZLGZ19, ZLZL20, ZTG22, ZGRS23, ZVH15, ZKP⁺23]. **basic** [BCJ⁺11]. **batch** [Pen13]. **Bayes** [Sen14]. **Bayesian** [ETAHCR08, GBG18, SGSS23]. **be** [ASN⁺16, EZLC21]. **beamforming** [KCC⁺23]. **bee** [SS17]. **beehives** [SS17]. **behaves** [ASN⁺16]. **Behavior** [BABB16, AZ22, MLCS16, XCW⁺12]. **Behavior-based** [BABB16, XCW⁺12].

behavioral[BEY23, CSC⁺23, KLMM09, SCO21].**behavioral-based** [CSC⁺23]. **Behaviour** [PPL15, AHX⁺23, IS23, LCPD14, ZTV23].**belief** [SGSS23]. **benchmark** [BB22].**benefit** [DRPW12, Zen22]. **benefits**[Rus04]. **better** [RAC16]. **between**[ACS21, Auf20, FGS12, LKH09]. **beyond** [SB22]. **bibliometric** [AAM23].**bidimensional** [KCM⁺15]. **big** [CLG23].**bilayer** [MLCS16]. **binary** [ZSN23].**bindings** [MSKD16]. **Bio** [ZZW⁺10].**Bio-Inspired** [ZZW⁺10]. **Biometric**[Pla09, BCA⁺10, HCN15, IT05, LSR⁺23].**biometrics** [BEY23, BCA⁺10, SCO21].**Bipartite** [YOV09]. **birth** [VMCR23].**birthmark** [XCW⁺12]. **bisection**[UMN⁺20]. **bit**

[CDP22, GSS10, SBB19, SKLP20, YOV09].

bit-length [YOV09]. **Bitcoin**[AMLH18, BSK⁺20, FTS⁺20, ML17,PSDSNAHJ19, Sat20]. **BitCracker** [AB22].**BitLocker** [AB22]. **BitM** [TCT22]. **bits**[BR18]. **Black**[DTK⁺18, GZH⁺23, LSR⁺23]. **Black-box**[DTK⁺18, GZH⁺23, LSR⁺23]. **blackhole**[LH23]. **blank** [WPD18]. **BlindIdM** [NA14].**block** [CYK09, KM10, Lu09, MARK20].**Blockchain** [MdAN23, Moh23, AAM23,AHC⁺21, FYF22, GGJ22, LLH21, LWA21,

LWL23, MLYL20, MG23, PGMPPC22,

SSV22, YSD⁺20, YL20, ZWX20, ZLJW20].**blockchain-based**

[LLH21, LWA21, PGMPPC22, YL20].

blockchain-enabled [LWL23, ZWX20].**Blockchain-oriented** [Moh23].**blockchains** [GAdFGM23]. **blocks**[CMR06]. **BLoCNet** [BCGL23]. **Bloom**[MB16]. **BIUFF** [AHC⁺21]. **bootstrapping**[EWR⁺09]. **botnet**[AKG16, FN19, HGH23, NNL20]. **botnets**[AMLH18, FN19, KA18, LL14]. **bounded**[LVK18]. **box**[CKW19, DTK⁺18, GZH⁺23, LSR⁺23].**Brazilian** [MdAN23]. **Breaking**[Dan07, RSMA19]. **Bring** [ACMV15].**Broadcast** [GSP⁺16, KCB17, LLW⁺16,CL09, Man21, PPSS13]. **browser**

[PSTS20, TSMH19, TCT22].

Browser-in-the-Middle [TCT22]. **BRSIM**[BP08]. **BRSIM/UC** [BP08]. **Bu** [AKT23].**Bu-Dash** [AKT23]. **Building** [LD07].**Business** [ANN23, INS21, KAC16, KBH07].**Business-layer** [ANN23].**cache** [TTS⁺06]. **caching** [ACB14]. **CADS**[FAMMZ23]. **CADS-ML** [FAMMZ23].**CADS-ML/DL** [FAMMZ23]. **calculus**[BNN04]. **call** [LWL⁺21, STW⁺23, YAY⁺21].**calls** [IKS22]. **Canada** [Lev07]. **candidates**[ABM⁺12]. **can't** [JTV19]. **capabilities**[ASAAS15, Lop18]. **capability**[CL08, Fon08]. **capacity** [SJ09]. **capture**[MR03]. **card** [ABFL12, DMDD16,GdKGV14, MUiH⁺21, MS14, MLM19].**card-based** [MUiH⁺21, MS14]. **cardiac**[NBA⁺21]. **cards** [MPP14]. **carried**[QLOW09]. **cascade** [WPD18].**cascade-instantiable** [WPD18]. **case**[BSCZ11, BDG21, GLMS⁺04, IS23, SKY23,SKK⁺17, TS20, TNA23, ZD22, ZHZ22].**cases** [Pla09]. **cash** [LCL14].**CASSANDRA** [MCD11]. **cast** [YYK⁺18].**Causal** [BR23]. **CCA** [PPSS13]. **CDH**[HIST09]. **centered** [GMGM21].**centralized** [AM23]. **centric**[AFA⁺23, CAS22]. **ceremonies** [MdSC⁺15].**Certificate**

[MFES04, CLPP11, Rus04, SVKV21, Ust11].

certificate-based [Ust11]. **certificate-free**[CLPP11]. **Certificateless** [RSD19,ZWQ⁺17, CFG17, Den08, FGS12, SSP14].**certificates** [PGMPPC22, ZJS22].**certification** [BCF⁺17, LMMO04].**certified** [IZS08]. **cFEM** [MKS⁺23].**chained** [DZW⁺18]. **chains** [AHC⁺21].**Chaintegrity** [ZWX20]. **challenge**[LWA21, MLYL20]. **challenge-based**

[LWA21, MLYL20]. **challenged** [KB23]. **Challenges** [TSZ22, HC10]. **changes** [YAY⁺21]. **channel** [CBRY20, dSFK19, HS15, KDYS19, MSKD16, MS09, MTW⁺14, SB22]. **channels** [DHW11, KK17, KML03, MPG21]. **chaos** [KAK22]. **chaos-based** [KAK22]. **chaotic** [PV22, ZMS22]. **characteristics** [BSK⁺23]. **characterization** [GMdFLR23, MSN02]. **charging** [ACT23]. **cheating** [CG21]. **check** [KO02]. **checker** [BMV05]. **checking** [AC08, GKBS12, HL04, MS15, NST09, YAM⁺15]. **checksums** [GKKT10]. **CHES** [DSY06]. **chip** [KKY⁺23]. **choice** [Tor20]. **ChoKIFA** [BHL⁺21]. **chosen** [LLW⁺16]. **chosen-ciphertext** [LLW⁺16]. **chrome** [PSOMS22]. **CIED** [NBA⁺21]. **CIP** [Yan21]. **cipher** [Lu09, TTS⁺06]. **ciphers** [CYK09, IMI18, KM10]. **Ciphertext** [JSMG18a, JSMG18b, LMG17, LLW⁺16, XZ21]. **Ciphertext-policy** [JSMG18a, JSMG18b]. **ciphertexts** [JSMG18b, PPSS13]. **circuits** [ZXZ22]. **civil** [MdAN23]. **class** [DS07, GDA22, MLCS16]. **classes** [ASA23]. **Classification** [SAL17, CBC08, GDA22, JBK21, LTC23, LWL⁺21, PLA⁺21, ZSN23]. **classifiers** [PKHS23]. **classify** [BEPL⁺17]. **Classifying** [SAH22]. **click** [ALPW13, CFBvO09, MBHT17, SGLC19]. **click-based** [CFBvO09]. **client** [ANN23, Bra22]. **client-side** [ANN23]. **clients** [SPDR17]. **close** [DHW11]. **Cloud** [Abb13, ABN14, Ano14, BMP⁺14, BS22, CMMPS15, CSL⁺23, DDX19, FZ21, FAMMZ23, FSG⁺14, GGJ22, GMH14, HK19, KNL16, LZQ⁺18, LS23, Man21, MSGCDPSS18, NT20, PDM20, PPL15, SKY23, VH19, WMS⁺19, YAM⁺15, ZLZL20, Alg22]. **cloud-based** [BS22, CSL⁺23, FAMMZ23, KNL16]. **cloud-outsourcing** [ZLZL20]. **cluster** [MKS⁺23]. **clustering** [BT07, PLA⁺21, RMSCR19, SKK⁺17, STD21, TBGB20]. **clustering-based** [RMSCR19]. **CNN** [SSL22b]. **co** [BMP⁺14, PPL15]. **co-residence** [PPL15]. **co-resident** [BMP⁺14]. **code** [BSK⁺23, DMDD16, HZL⁺17, KKKV07, LS23]. **codes** [BHKM23, CL13, Nui12]. **coding** [EMRN17, TWP08]. **coding-enabled** [EMRN17]. **Coin** [KM22]. **Coin-based** [KM22]. **collaborative** [BEd23, LWA21, LWL23, MLYL20]. **collect** [PD21]. **collection** [BSV22, SV11]. **Collision** [MS09, CHKO12, Hal20, KW15]. **collision-resistant** [CHKO12]. **collusion** [DdP13, LL21, Nui12]. **collusion-resistant** [LL21]. **collusion-secure** [Nui12]. **Colored** [SSFB15]. **coloring** [RS18]. **colors** [PM23]. **Coloured** [BKBB20, BBB20]. **column** [CMS10]. **combinations** [KAC17]. **combinatorial** [CMR06]. **combined** [CLG23]. **Combining** [SCO21, GMSS23, SSE⁺15]. **command** [SNX19]. **commerce** [ABFO08, GLP03, ZGC07]. **commercial** [NVB⁺02]. **commitment** [GSS10, HCN15]. **commitments** [WCS20]. **Commix** [SNX19]. **commodity** [TND⁺15]. **commodity-based** [TND⁺15]. **common** [DMP13]. **communication** [CPPK15, DWU⁺23, GBG18, KCB17, LMD17, LLG22, PBI⁺23, VdWZ14]. **communication-efficient** [LMD17]. **communications** [FZ21, KAK22, KIP22, MG19, MB16]. **Comparing** [BBR18, GMLM23]. **comparison** [AHX⁺23, SDW23, SRD⁺21]. **comparisons** [AL05]. **compatible** [LI07]. **Complete** [ABCC08, BB04a, LCL14, MSN02]. **completeness** [WHS18]. **complex** [SDG22]. **compliance** [CCD⁺07]. **Compliant** [DVB02, PSOMS22]. **components** [AV17]. **composability** [Vaj16]. **composable** [BFS⁺13]. **comprehensive**

[BF13, CKKK23, HGH23, KSB23, LRB⁺10, Moh23, SB09]. **compressing** [MP16]. **compression** [CDP22, RSMA19]. **compromised** [SPDR17]. **computation** [ABB17, BNTW12, DDX19, PCK22a, Pen13]. **Computational** [BP04, LCL16]. **Computations** [KM22, BGP07b, KU16]. **compute** [MCD11]. **Computer** [Lan01, BCEM04, LL14, vORM06]. **Computing** [BJ15, Ano14, LI07, PDM20, Pri04]. **concept** [Sen14]. **conceptual** [JGK14]. **Concise** [WCS20]. **Concrete** [BLM11, BCL09, RSD19]. **Concrete-** [BLM11]. **concurrent** [ASAAS15]. **condition** [ANN23]. **Conditional** [BDHK08]. **conditions** [BDPV14, sLC05, SGC22]. **Conference** [CL09]. **confidential** [HN14]. **confidentiality** [BB04a, KNL16, XZ21]. **configuration** [ABR16, ABCC08]. **confinement** [Fon08, SPM13, SS05b]. **confirmation** [PSDSNAHJ19]. **conflict** [RV03]. **conjunctive** [FRG19, LZQ⁺18]. **connected** [MLCQ21, Yan21]. **connection** [BS22, LSWW14, SS05a]. **connection-based** [SS05a]. **considering** [HXTF23, TTS⁺06]. **constant** [BGP07b, PPSS13]. **constant-round** [BGP07b]. **constant-size** [PPSS13]. **constants** [BR17]. **constrained** [SS17]. **construct** [YSM10]. **construction** [Ala17, ASZ⁺23, BGKZ12, NSNK06, YYK⁺18]. **constructions** [HSMY12, KME⁺16, ZVH15]. **consumer** [LKH09]. **consumption** [RBEH15]. **consumption-based** [RBEH15]. **contacts** [DMP13]. **containing** [IT05]. **Content** [BFP03, HC10, LKH09, Pla09, SSJ22, ZP23]. **Content-based** [BFP03, HC10, SSJ22]. **context** [DGF⁺17, GMGM21, HS09, JGK14, SRK⁺20, SCO21]. **context-aware** [DGF⁺17, SRK⁺20]. **context-centered** [GMGM21]. **context-sensitive** [HS09]. **contextual** [CCB08]. **Continuous** [Yan21, BEY23, EG18, GGP21]. **continuous-time** [GGP21]. **contourlet** [SJ10]. **contract** [IZS08, MdAN23]. **contracts** [GYL⁺07]. **Control** [LMMS17, SAL17, AMZ22, AM23, ACF17, AFA⁺23, AJC⁺09, Ano11b, ACBC⁺15, BAB23, BLM11, BNN04, CF03, CCD⁺07, CK08, CZ06, GGJ22, HS09, HSMY12, KAC16, KAC17, KLMM09, Kud02, KB22, KNL16, LRB⁺10, MSKS20, MG23, MS15, Pen12, RT23, RM12, SRD⁺21, TZH04, ZM07]. **Controlled** [BB04a, BFG⁺13, SM10]. **controller** [MPG21]. **conversations** [DBMS10]. **convertible** [LL21, Lin15]. **convex** [ALPW13]. **Convey** [SSR22]. **cookie** [ACB14]. **cookie-based** [ACB14]. **cooperation** [AGIK07]. **coprocessors** [Smi04]. **core** [KKK22b]. **correcting** [KM07]. **Correction** [BKBB20, CK23a, LSV⁺23]. **correlation** [MdMF22]. **corruption** [BHKM23]. **corruptions** [KLPL21]. **cost** [DRPW12, DYDW10, Zen22]. **cost-benefit** [DRPW12, Zen22]. **counter** [BF13]. **counter-measure** [BF13]. **counterfeit** [AHC⁺21]. **Countermeasure** [MLC23, GBDJ14, MTW⁺14, Pen11]. **countermeasures** [ACT23, Bae10, JK22, PSTS20, SB22, YNC22]. **Counting** [KM10]. **country** [SKK⁺17]. **cover** [SJ10]. **COVERAGE** [AGIK07]. **covert** [DHW11, MPG21]. **COVID** [PGMPPC22]. **COVID-19** [PGMPPC22]. **Cracker** [SGE02]. **create** [SKB23]. **credential** [AYHK18, ABFL12]. **credentials** [AFA⁺23, SF17]. **Critical** [EEB⁺15]. **cross** [IS23, PMPGMLLM12]. **cross-layer** [PMPGMLLM12]. **cross-setting** [IS23]. **CRT** [OT06]. **CRT-based** [OT06]. **CRUST** [GW09]. **Cryptanalysis** [ALPW13, DSY06, JT21, MS11]. **Cryptanalytic** [CJMS19]. **Crypto** [You06]. **cryptocurrency** [FYF22]. **cryptographic**

[ARMLS06, BPW05b, BGK08, BDH⁺10, DFF⁺16, DSRHC16, GW09, JCL⁺18, KU16, K us05, MR03, MS14, MSGCDPSS18, ZJS22]. **Cryptographically** [BCJ⁺11]. **cryptography** [ALOW15, Bra22, KIP22, LP11, SDR20]. **cryptologic** [DVB02]. **cryptosystem** [HCN15, IT05, KAK22, MS11, SGE02]. **cryptosystems** [KG11, NMBB12, OT06]. **Cryptoviral** [You06]. **CSOC** [SGJC18, SGJ19, SGC22]. **CT** [FYF22]. **CT-GCN** [FYF22]. **cuckoo** [VH19]. **current** [HC10]. **Curve** [JMV01, KIP22, SDR20]. **curves** [HMCD04, KSZ07]. **cut** [UMN⁺20]. **Cyber** [AG23, HXTP23, KMMG23, MBH⁺21, SSD14, TDGL23, AK23, CK23a, CK23b, CG23, LWL23, NBA⁺21, PAI⁺23, PCK22b, RV19, SDW23, SBGP21, SBG22, SB22, SAH22, YNC22, ZP23]. **Cyber-attack** [SSD14]. **cyber-attacks** [NBA⁺21]. **Cyber-physical** [HXTP23, AK23, CK23a, CK23b, LWL23, PCK22b]. **cyber-security** [CG23]. **Cyberattack** [TBGB20]. **cyberbullying** [KB22]. **cybersecurity** [EAM⁺23, SB22, VSN22]. **cycle** [AYHK18].

D2D [KIP22]. **damage** [WGMB13]. **DAMe** [PMPGMLLM12]. **DAPP** [KKK22a]. **dark** [ZD22]. **darknet** [OBH⁺20]. **Dash** [AKT23]. **Data** [LMMS17, PCK22b, SV11, SAL17, VdWZ14, AT22, AaBZS23, AAZAA23, ACF17, ABN14, AAB20, BS05, BNTW12, BDH⁺10, CR20, CTM⁺16, CKS21, CLG23, EMRN17, EAH⁺07, GSAMCA18, GKS19, HJDC15, HK19, HXTP23, HH16, JK22, JJJ21, K us05, LLH21, LL21, LD17, LS23, Man21, MSKS20, MSGCDPSS18, NT20, OO20, OSSK16, OBH⁺20, RT23, SBS23, SAC22, SSL22a, SRD⁺21, SBG22, SMMN12, SXZC20, TS22, TNA23, VH19, XZ21, YAM⁺15, ZO13, ZLZL20, ZTG22, Zha23]. **data-leakage** [RT23]. **Database** [KSM10, BDD01, DA21]. **databases** [BW08, CMS10, EAH⁺07, HN14]. **dataset** [ASA23, BCGL23, NRC15]. **dataset-independent** [BCGL23]. **datasets** [MU18, SKB23]. **day** [DGF⁺17, SLGP23]. **DDoS** [AZ19, KSB23, KCB20, SRSM23]. **DEALER** [MPP21]. **dealership** [GSP⁺16]. **decentralised** [PC19]. **decentralized** [LLWY09, LSG22, LSV⁺23, MPP21, SVKV21]. **deception** [CK23a, CK23b]. **decidability** [K us05]. **decision** [PHS22, WPD18, ZGRS23]. **decomposition** [MARK20]. **dedicated** [ZZG19]. **deduplication** [NT20]. **Deep** [ME23, AAZAA23, BCGL23, HNHY23, KBY22, KCB20, MK21, SJS22]. **deepfake** [AVM23]. **Defeating** [DSB19, ZHZ22]. **defences** [HXTP23, PNG⁺20]. **defending** [SK06]. **Defense** [WWZ⁺23, AG23, BB22, KK22, MYLZ14, TCE23, VSR15, WR08, ZRJ14]. **defense-in-depth** [AG23]. **defenses** [BDG23, LLWY09]. **defensive** [AVM23, KCC⁺23]. **defined** [KSB23, MdMF22, SKH⁺23]. **Definition** [TMP13]. **degree** [SSVC16]. **Delay** [ZO13]. **Delay-sensitive** [ZO13]. **delays** [SDW23]. **delegatability** [HYWS11]. **Delegation** [CK08, BGTCCBB10, CON09, GOBdIC11, PMDS23, WZ07, ZZG19]. **delegations** [RV03]. **deniable** [GCH⁺19, JT21]. **Denial** [LLWY09, WR08, TGS17]. **denial-of-service** [WR08]. **dependence** [HS09]. **dependencies** [ACF17]. **Dependency** [AK23, CMS10]. **Dependency-based** [AK23, CMS10]. **deploying** [GDA22]. **Deployment** [ACBC⁺15, HIDFGHR19, AAV22, Das12]. **deployments** [PCT22]. **depth** [AG23, PCT22, SAT09]. **description** [SM10]. **descriptions** [CAS22]. **Design** [DNF⁺19, KAK22, MBRPS18, SRSM23, BSCZ11, CMR06, CFBvO09, FN19, KMMG23, LMMO04, NCBG23, SBD23]. **designated** [HSMW08, HYWS11, RSD19].

designed [KCM⁺15]. **Designing** [AV17, PDM20]. **desynchronization** [Tip22]. **detect** [BABB16, EZLC21, JJJ21, MLCQ21]. **Detecting** [DGF⁺17, AGIK07, BHKM23, BMP⁺14, KDYS19, PPL15, SGLC19, vORM06]. **Detection** [ABR16, CPPK15, sLC05, SAL17, AZ19, ATS23, ASAAS15, ASA23, Alg22, AuHD⁺23, ASN⁺16, AZ22, AVM23, BSK⁺23, BEPL⁺17, BHL⁺21, BDMM19, BR23, BT07, BCGL23, CK23a, CK23b, CSC⁺23, CL08, CLG23, CG21, DTK⁺18, DGF⁺17, FAMMZ23, GPS17, GDA22, Ham23, HGH23, HNHY23, IKS22, KAK23, KKK22a, KBY22, KA18, KKK17, KJG⁺11, KB22, KSM10, LWA21, LWL23, MD23a, MKS⁺23, McH01, MLYL20, MLCS16, MK21, MI22, ME23, MB23, MP22, NNL20, PM23, PAI⁺23, PDM20, PV22, RSV23, RB23, RBEH15, RHGTSC17, SBS23, SLGP23, Sen14, SBD23, SRK⁺20, SGSS23, STW⁺23, SF17, SKB23, SKH⁺23, SSJ22, STD21, TBGB20, TKKO20, TLX09, VL13, WGH23, WAB⁺09, ZKP⁺23, ZXZ⁺11, ZTV23, ZGK07]. **detection-based** [AZ22]. **detector** [SBD23]. **detectors** [AvO13]. **deterministic** [GS15, RMSCR19]. **DeTRACT** [SVKV21]. **Developing** [KBJ22, SK16]. **Development** [KK17, INS21, LNX22]. **device** [GA23, KWCK19, ACMV15]. **Devices** [LMMS17, ABK22, BS22, FBFGE21, GCSÁBdSS12, IDHRPCMP15, LKH09, LCPD14, LSG22, MR03, MNC20, NBA⁺21, TKKO20, UBK23, ZLZL20, LSV⁺23]. **DFTMicroagg** [AT22]. **dictatorship** [Tor20]. **Differential** [dSFK19, MTW⁺14, SAC22, ZHZ22]. **differentially** [DA21, PHS22]. **Diffie** [CC12, DS07]. **diffusion** [GGP21]. **Digital** [JMV01, SSM⁺20, SSR22, ASF04, GA23, JG15, PGMPPC22, TSZ22, ZTG22]. **dimensional** [SGSS23]. **direct** [BCL09, KME⁺16, KLPL21]. **directions** [TDGL23]. **disassembling** [BSK⁺23]. **disclosure** [KPM12, ORK23, RAC16, TNA23]. **discounts** [DFBJR18]. **discovery** [CYA⁺18, DMP13, JM17]. **discrete** [HMCD04, SBD23]. **Discretionary** [Fon08]. **discrimination** [ZZG19]. **Disposable** [HRMM20]. **Disposal** [SSM⁺20]. **dissociation** [VH19]. **distillation** [KCC⁺23]. **distinguish** [HTM11]. **Distributed** [AFA⁺23, RS18, ASF04, BEd23, Das12, DHS04, HN14, KKK17, Pen12, TLX09, WZ07]. **Distributing** [VSM06, AYHK18]. **distribution** [ASF04, BFPP07, CMR06, GP17, MARK20, PSA23, YYK⁺18]. **diversification** [BB22]. **DL** [FAMMZ23]. **DNA** [IHNT02]. **DNS** [BDG21, SPDR17, ZTV23]. **Do** [BM11, EZLC21]. **document** [CF03]. **documents** [BFP03, BFPP07]. **does** [GSM⁺11]. **Dolev** [BPW05b, BP08]. **domain** [CON09, CYA⁺18, KCB20, LSR⁺23, PGMLK⁺13, SCL⁺18, SBG22, YA22]. **domain-specific** [LSR⁺23]. **DomainProfiler** [CYA⁺18]. **domains** [GMH14, ZMS22]. **dominant** [PM23]. **DOMtegrity** [TSMH19]. **don't** [JTV19]. **Double** [ACHO13, PSDSNAHJ19, PS17]. **Double-authentication-preventing** [PS17]. **Double-spending** [PSDSNAHJ19]. **Double-trapdoor** [ACHO13]. **down** [Auf20, JTV19]. **download** [NRC15]. **DPA** [Bae10]. **DREAD** [ZTG22]. **drift** [Sen14]. **drive** [NRC15]. **drive-by** [NRC15]. **driven** [AMZ22]. **DRM** [LKH09]. **DroidRista** [AAB20]. **DSA** [MR04]. **DTE** [LH15]. **DTLS** [TGS17]. **dual** [AT22]. **dual-level** [AT22]. **DUEF** [CR20]. **DUEF-GA** [CR20]. **during** [CBC08]. **Dynamic** [BDMM19, DFBJR18, HK19, KYH18, Roe11a, ZM07, ANN23, AKT23, CON09, CMS10, CZ06, HRMM20, KK17, KCB20,

RV19, SSE⁺¹⁵, YYK⁺¹⁸, Roe11b]. **dynamicity** [AICC18]. **dynamics** [MRW02].

E-business [KBH07]. **E-cash** [LCL14]. **e-commerce** [GLP03, ZGC07]. **e-government** [GOBdIC11]. **e-healthcare** [QDW⁺¹⁵]. **e-services** [DDPS02]. **e-voting** [MS11, Pen11, ZWX20]. **Early** [RSV23, BHL⁺²¹, CYA⁺¹⁸]. **eavesdropping** [CPPK15]. **ECDSA** [JMV01]. **eCK** [Ala17]. **eCK-secure** [Ala17]. **edge** [SSL22a]. **edge-based** [SSL22a]. **Edit** [LBW05, BCL13]. **Editorial** [GMO01, Gol08]. **editors** [ANS⁺¹², CM16, TCS⁺²⁰, CHM18, DMRS07, JZ11, YSM16, ZLL12]. **education** [AHX⁺²³, KMMG23]. **eduroam** [PMPGMLLM12]. **eduroam/DAMe** [PMPGMLLM12]. **effect** [BR23, Zha23].

Effective [AuHD⁺²³, ASZ⁺²³, MGRR19, ZGC07]. **Effectiveness** [SK16, SGJC18, SGC22]. **effects** [SV11]. **efficiency** [HMCD04, MGV17, PDB11, Pen13]. **Efficient** [CLG23, HRL09, HH16, HYWS11, JCL⁺¹⁸, KLZ⁺²¹, KJ14, KU16, KSZ07, LMG17, LBZ⁺¹⁰, MP16, MRG23, NP10, PCK22a, RD16, SMMN12, AKMW20, Bae10, BR18, BS21, BCD⁺¹³, CKS21, EMRN17, FAMMZ23, HN14, HYWS12, KKK22b, LMD17, LCL14, LWL⁺²¹, MG19, MCD11, NT20, Pen11, PV22, YYH⁺²³]. **effort** [SGJ19]. **eID** [RLEM18]. **eIDs** [HRMM20]. **Elastic** [CYK09]. **electric** [ACT23]. **Electronic** [GSM⁺¹¹, ABFO08, BDHZ15, BSV22, DJN10, GP23, KO02, NBA⁺²¹]. **Elias** [BR18]. **elicit** [SK16]. **elicitation** [FFG20]. **elliptic** [HMCD04, KIP22, KSZ07, SDR20, JMV01]. **email** [IZS08, WR15]. **emails** [SSM⁺²⁰]. **Embedding** [BDH⁺¹⁰, SJ09]. **EMBLEM** [SKLP20]. **employee** [Sep23]. **enabled** [AAV22, BAB23, EMRN17, LWL23, NBA⁺²¹, ZWX20, SHA20]. **Enabling** [BS05, JAYZ21]. **encapsulation** [MPS14, SKLP20]. **encoding** [SKLP20, ZSN23]. **encompassing** [EHM15]. **Encouraging** [YM19]. **encrypted** [ABK22, CTM⁺¹⁶, CKS21, DBMS10, GSAMCA18, HH16, KJ14, OO20, OSSK16, SEXY18, WPD18, WR15]. **encryption** [ARMLS06, AKMW20, BZ03, CDP22, CC12, CHMS21, Den08, DDX19, EHSS14, FRG19, FGS12, GMMV05, GSP⁺¹⁶, HK19, IMI18, JCL⁺¹⁸, JSMG18a, JSMG18b, KME⁺¹⁶, KLZ⁺²¹, LMG17, LZQ⁺¹⁸, Lin15, MRG23, PMDS23, PPSS13, QLZH15, QDW⁺¹⁵, SSP14, SRD⁺²¹, STD21, XZ21, YP06, ZZG19, ZVH15, ZMS22, LLW⁺¹⁶, Dan07]. **end** [BB04b]. **ended** [Küs05]. **energy** [RBEH15]. **enforced** [BM11, GGJ22]. **enforcement** [ACMV15, AICC18, BCL13, DLR15, LBW05]. **enforcing** [BB04a]. **engine** [LNX22]. **engineering** [AZ19, GMMZ06, MLM19, SK16, BZ20]. **enhance** [SCO21]. **Enhanced** [ABN14, GGP21, YAM⁺¹⁵, KBJ22, LV10, MSP⁺¹³, PV22, SDR20, JTV19]. **Enhancing** [ACB14, CLW⁺¹¹, DA21, KLMM09, MLYL20, XZ21]. **ensemble** [AuHD⁺²³, YA22, ZBC23]. **Ensuring** [SAT09, SGJ19, TSMH19]. **enterprise** [WYL⁺¹²]. **entity** [ZP23]. **Entropy** [BEPL⁺¹⁷, HLKI15, SV11]. **environment** [BEd23, CLW⁺¹¹, CLG23, GOBdIC11, INS21, KAK23, LRB⁺¹⁰, MI22, NVB⁺⁰², YL20, ZBC23]. **environmental** [SHA20]. **environments** [AKMW20, FSG⁺¹⁴, GYL⁺⁰⁷, LI07, PPL15, WAB⁺⁰⁹]. **epidemics** [AGIK07]. **equations** [KM10, SSVC16]. **Erratum** [Roe11b]. **Error** [KKY⁺²³, RMPADF13]. **errors** [ABR16]. **escalation** [FTS⁺²⁰, YAY⁺²¹]. **Escrow** [ARMLS06, YSM10]. **Escrow-free** [ARMLS06]. **ESORICS** [Sne05]. **Establishing** [BS22, Abb13].

establishment [BVS07, Das12, YRW14]. **Estimating** [AD08, WHS18]. **estimation** [RMPADF13]. **EUFORBIA** [BFP03]. **Evading** [PKHS23, XCW⁺12]. **Evaluating** [JJJ21, MUiH⁺21, PHS22]. **Evaluation** [AvO13, BDG23, AZ19, AMZ22, AKG16, BB04a, CR20, HIDFGHR19, RHL17, SKY23, SK06, SNX19, TKKO20, TND⁺15]. **evenhandedness** [ZS08]. **event** [AMZ22, SBD23]. **event-driven** [AMZ22]. **events** [RHGTSC17]. **everlasting** [GP23]. **evidence** [GA23, SdHZ16]. **evidence-based** [SdHZ16]. **evident** [GMSS23]. **EXAM** [LRB⁺10]. **exchange** [Ala17, BBR18, BCF⁺17, BFS⁺13, CHZ16, DGZFGH13, ETAHCR08, HM22, HYWS12, MPS10, MPP14, MPP21, MSN02, SEXY18, Ust11, YLL⁺18]. **excursus** [Fra18]. **executable** [BHKM23]. **Execution** [SK06, BHKM23, MLO⁺04, MUiH⁺21]. **exercise** [CG23, ZP23]. **exfiltration** [ZTV23]. **exfiltrator** [ZTV23]. **exhaustive** [KJS17]. **experience** [MdAN23]. **experimental** [AMZ22, BCD⁺13, DSB19]. **experiments** [QLOW09]. **explicit** [KAC16]. **exploitation** [JM17, MLM19, SNX19]. **exploiting** [ACF17]. **exploits** [ZRJ14]. **exploring** [HS15]. **exponentiation** [Bae10]. **expression** [WR15]. **expressive** [RD16]. **extended** [ACF17, AKT23, BGTCBB10, Lop18, MS15]. **Extending** [AMZ22, KKKV07]. **extension** [JSMG18a]. **extensions** [PSTS20, PSOMS22, TSMH19]. **external** [CLW⁺11]. **extortion** [You06]. **extractable** [KKK22b, WT16]. **extraction** [GA23, MKS⁺23].

FA [Bae10]. **faceted** [BFT08, QLOW09]. **facets** [AKG16]. **factor** [AGZA22, CG14, ML17, MNC20]. **failures** [SK06]. **Fair** [KM03, DGZFGH13, GRV05, HYWS12, SEXY18, SGJ19]. **fake** [RB23]. **false** [HXTP23]. **familiarity** [ZGC07]. **familiarity-based** [ZGC07]. **family** [AMP12, MSN02, PLA⁺21]. **Fast** [Rov23, ZLZL20]. **fault** [CL09, GKS19, RBD02]. **fault-tolerance** [CL09]. **fault-tolerant** [GKS19, RBD02]. **FCS** [ACM05]. **FCS/VERIFY** [ACM05]. **FDCO** [ZLZL20]. **Feature** [KCB20, AZ19, MKS⁺23, SBS23, YP06]. **features** [AVM23, GDA22, ZJS22]. **Federated** [Ham23, TGNA22, WW07, YYH⁺23]. **federating** [PMPGMLLM12]. **file** [BLS⁺23, sLC05, ZLGZ19, ZLGZ19]. **file-based** [sLC05]. **filter** [MB16, VH19]. **filtering** [BFP03, HBK22]. **find** [SSVC16]. **fine** [KLMM09, RT23]. **fine-grained** [KLMM09, RT23]. **fingerprint** [CC10, Nui12]. **finite** [BCL13]. **firewall** [ABR16, KNL16, MWZ06]. **firewalls** [HBK22]. **firmware** [YL20]. **first** [LM06, ZD22]. **first-order** [LM06]. **fixed** [HMCD04]. **FL** [TGNA22]. **Flexible** [JSMG18b, ORK23, QDW⁺15, SBG22]. **floating** [ABB17, KW15]. **floating-point** [ABB17]. **Flood** [MLC23]. **flooding** [BHL⁺21, JK22]. **Flow** [HS09, SdHZ16, AAB20, BMP⁺14, BNN04, MP22, ZM07]. **Flow-based** [SdHZ16]. **Flow-sensitive** [HS09]. **Flowchart** [SM10]. **flows** [IKS22]. **fly** [CL13]. **focusing** [KKK22b, YAY⁺21]. **fog** [AAV22, KAK23]. **Fog-based** [Moh23]. **fog-enabled** [AAV22]. **fog-IoT** [KAK23]. **FOO** [ZLJW20]. **forensic** [GA23, GMGM21]. **form** [DdP13]. **Formal** [ACMV15, GKBS12, Yon18, dAKdG10, BKBB20, BBB20, CMN⁺18, KAC17, NSNK06, PDB11, RV03, VdWZ14]. **formalism** [GBDJ14]. **formalization** [MS14]. **format** [ZLGZ19]. **format-based** [ZLGZ19]. **forward** [CDF⁺13, KME⁺16]. **forward-secure** [KME⁺16]. **FOTB** [YL20]. **four** [Dan07]. **Fractional** [BCA⁺10]. **fragmentation** [LS23]. **frame** [SHW23]. **framework** [AZ19, Abb13, AAB20, AVM23, ABFL12, BFT08, CR20, EAM⁺23, JAYZ21,

KMMG23, KAK23, KNL16, LWA21, LWL23, MB16, MLO⁺04, Moh23, PDM20, RV19, RV03, SVKV21, SSM⁺20, SKY23, Vaj16, VdWZ14, WR08, WHS18, XSA13, Yan21, YL20, ZP23, ZRJ14, ZGRS23]. **free** [ARMLS06, BGKZ12, CLPP11, YRW14]. **freeness** [HIST09]. **frequency** [YA22]. **friendly** [CLPP11]. **Fujisaki** [GMMV05]. **full** [Bra06]. **Fully** [CDF⁺13, MLCQ21]. **function** [AGZA22, BGKZ12, KKY⁺23, LWL⁺21, SB14, STW⁺23]. **functional** [WCS20]. **functionality** [SPM13]. **functionality-based** [SPM13]. **functions** [AMZ22, AMP12, EG18, GKKT10, MS09, SM10]. **future** [CYA⁺18, LMMP06, PSA23, TDGL23]. **fuzzy** [HCN15, TMM⁺19].

G [DWU⁺23, DWU⁺23]. **G/6** [DWU⁺23]. **GA** [CR20]. **Gait** [HCN15]. **Game** [wLW05, LVK18, PNG⁺20, WYL⁺12]. **game-theoretic** [LVK18, PNG⁺20]. **games** [MB23]. **gap** [Auf20]. **garbled** [ZXZ22]. **gate** [JSMG18b]. **GCN** [FYF22]. **general** [BCD⁺13, Pen11]. **generalised** [BKMR08]. **generalization** [DJN10]. **Generalized** [BR18, KMR09]. **Generalizing** [KG11, AMP12]. **generated** [IHNT02]. **Generating** [LC04]. **generation** [AKZM20, AMLH18, BHZ⁺21, CAS22, KJG⁺11, KSZ07, MR04, YKP22, ZP23]. **Generic** [Ala17, ZVH15, EWR⁺09, KME⁺16]. **geographic** [ABN14]. **GeoProof** [ABN14]. **geospatial** [HK19]. **gesture** [GCSÁBdSS12]. **Global** [Pri04]. **goals** [RGL16]. **Gossamer** [DDZ22]. **gossip** [ML14]. **government** [GOBdC11]. **GPU** [VPI15]. **GPU-assisted** [VPI15]. **GPUs** [AB22]. **GQ** [HRL09]. **graduates** [AHX⁺23]. **grained** [KLMM09, RT23]. **graph** [BCEM04, CR20, NNL20, RV03, STW⁺23, WGH23, WWZ⁺23, YL19]. **graph-based** [NNL20]. **graph-theoretical** [BCEM04]. **graphical** [AKT23, CG14, CFBvO09, GTM11, IS23, WLLW14]. **graphs** [HS09, HLKI15, KB13, LWL⁺21, SDG22]. **grey** [CKW19]. **grey-box** [CKW19]. **grid** [AKZM20, AT22, CLPP11, KLMM09, LP11, PSA23, PNG⁺20]. **Gridchain** [PSA23]. **grids** [MD23a, SAH22]. **ground** [AvO13]. **Group** [EHSS14, TDRR20, BVS07, DFBJR18, GNS14, HM22, IDHRPCMP15, PBI⁺23, RBD02, YLL⁺18, ZWQ⁺17]. **groups** [PJ10]. **guarantee** [ABCC08, Bel10]. **guarantees** [LSWW14]. **Guard** [ZLGZ19]. **guessers** [PCT22]. **guest** [ANS⁺12, CM16, TCS⁺20, CHM18, DMRS07, JZ11, YSM16, ZLL12].

Haar [KCM⁺15]. **hacking** [EZ22]. **hand** [GCSÁBdSS12]. **Handling** [WZ07]. **hands** [CKKK23]. **hands-on** [CKKK23]. **handshake** [TGS17]. **hard** [EAH⁺07]. **hard-to-reverse** [EAH⁺07]. **hardening** [DMDD16, DRPW12, MRW02, Zen22]. **hardware** [BSCZ11, DYDW10, KBJ22, KKK22b]. **hardware-assisted** [DYDW10]. **harvesting** [BR18]. **hash** [AMP12, BGKZ12, GKKT10, MS09, MFES04, SB14]. **HashEdDSA** [BST21]. **hashing** [BDPV14, CHKO12, CJMS19, MP16]. **health** [BDHZ15, QLZH15, SAC22, SHA20, SDR20]. **health/accessibility** [SHA20]. **healthcare** [BEd23, MG23, QDW⁺15]. **Hellman** [CC12, DS07]. **heterogeneous** [RLEM18, SAT09, WGH23]. **HIBE** [ZZG19]. **hidden** [ABB17, GSS10, SSVC16]. **Hiding** [GI19, XZ21, ZXZ22]. **Hierarchical** [BKBB20, BBB20, NAM06, FTS⁺20, JCL⁺18, LLW⁺16]. **High** [BNTW12, AM23, BB04b, KKK22b, Pen13]. **high-efficient** [KKK22b]. **high-end** [BB04b]. **High-performance** [BNTW12]. **high-rate** [AM23]. **higher** [PDB11]. **Highly** [PGMPPC22, AAB20]. **hijacking**

[SGLC19]. **history** [TDRR20]. **HiveSec** [SS17]. **Hoc** [LH23, Gol12, MS11, SF17]. **home** [AZ22, FBFGEM21, SRD⁺21]. **homes** [BAB23, HKO22]. **homology** [WGH23]. **homomorphic** [DDX19, EMRN17, MMS16, Rov23, SEXY18, STD21, SXZC20]. **HoneyCirculator** [AYHK18]. **honeypot** [LSG22, LSV⁺23]. **honeypot** [AYHK18]. **hop** [BT07]. **host** [CLW⁺11, KLPL21]. **hotels** [DZW⁺18]. **HTTP** [MLC23]. **HTTPScout** [MLC23]. **hull** [ALPW13]. **human** [AAZAA23, ALPW13, MBHT17]. **hunger** [MB23]. **Hybrid** [KML03, BCGL23, CC10, GMMV05, MMS16, MB23, SGSS23, TCE23]. **Hydras** [PC19]. **hyperparameter** [GZH⁺23].

IC [AHC⁺21]. **ID** [FGS12, WCS20, ZZG19]. **ID-based** [FGS12, WCS20]. **identification** [AAZAA23, ASZ⁺23, ALPW13, CL08, FYF22, GBG18, GI19, LcSCL⁺18, MG17, NCBG23, NRC15, PLA⁺21]. **Identifier** [ZZG19]. **identifiers** [IHNT02]. **identifying** [KGG09, SPDR17]. **Identity** [CCS07, LP11, LLW⁺16, CHZ16, GOBdlC11, GMLM23, HRL09, JCL⁺18, LMG17, LBZ⁺10, MPS14, NA14, ORK23, TMP13, Ust11, VdWZ14, YSM10, ZWQ⁺17]. **Identity-Based** [LLW⁺16, CCS07, LP11, CHZ16, HRL09, JCL⁺18, LMG17, LBZ⁺10, MPS14, Ust11, YSM10, ZWQ⁺17]. **IDS** [ATS23, ZBC23]. **IDSIC** [CL08]. **IEC** [CH16, MD23b]. **IEEE** [KDM22]. **If** [ASN⁺16, MBHT17]. **IHE** [ACBC⁺15]. **II** [BB04b]. **IIJ** [SKK⁺17]. **image** [HC10, ZMS22]. **images** [HLKI15, MBHT17]. **imbalanced** [ASA23]. **immune** [Hub12, MdMF22]. **immutable** [SVKV21]. **impact** [SSD14]. **implantable** [NBA⁺21]. **implement** [ABFL12]. **implementation** [Auf20, BSCZ11, DNF⁺19, IDHRPCMP15, KAK22, MBRPS18, MFES04, TKKO20].

implementations [RSMA19, UMN⁺20]. **implemented** [MS15]. **Implementing** [ALOW15, BGK08]. **implications** [HMCD04]. **implies** [EHSS14]. **improve** [YM19]. **Improved** [HLS18, ABN14, LS23, MLCS16, WT21, ZLJW20]. **improvement** [AaBZS23, YWW22, Yan21]. **Improving** [CH16, KLPL21, TTS⁺06, BJ16, TGS17, TG05]. **IMS** [VL13]. **in-depth** [PCT22]. **in-VM-assisted** [PDM20]. **inappropriate** [LTC23]. **incentive** [LI07]. **incentives** [MPP21]. **incidents** [SDW23]. **incomplete** [BW08]. **Incompleteness** [SAL17]. **Inconsistency** [SAL17, ACS21]. **incorporating** [BCF⁺17]. **incremental** [TBGB20, ZKP⁺23]. **independent** [BCGL23]. **indifferentiability** [BGKZ12]. **indistinguishability** [SXZC20]. **individual** [Man21]. **inductive** [MP15]. **industrial** [RM12]. **industry** [SDW23, SDG22]. **industry-level** [SDW23]. **inference** [AJC⁺09, JG15, WWZ⁺23]. **influences** [AHX⁺23]. **inform** [PCT22]. **Information** [KBH07, TND⁺15, ASF04, AD08, AFA⁺23, ABFL12, BDHZ15, BB04a, BDD01, CMMPS15, DdP13, DBMS10, EFH09, GI19, HS09, INS21, IKS22, IHNT02, KPM12, LLH21, LTC23, LMD17, LcSCL⁺18, MU18, NAM06, PD21, Pla09, TKKO20, WHS18, ZM07]. **information-centric** [AFA⁺23]. **information-distribution** [ASF04]. **Information-theoretically** [TND⁺15]. **informed** [AG23]. **infrastructure** [CLPP11, SSV22, TS20, TMP13, Gri06]. **infrastructures** [ACT23, EEB⁺15]. **Inheritance** [SSR22]. **injection** [DSB19, DTK⁺18, HXTP23, SNX19]. **insecure** [KM07]. **insecurity** [Sat20]. **Insider** [SSV22, YP12, ASA23, MLYL20, Sep23, YA22]. **inspection** [BDF04]. **inspired** [SS17, ZZW⁺10]. **instance** [Sen14]. **instance-weighted** [Sen14]. **instances** [BMP⁺14, JG15]. **instantiable** [WPD18]. **instantiations** [CYK09].

Instruction [DM07, WGH23].
Instruction-level [DM07]. **insurance** [GYL⁺07, TDGL23]. **integers** [DDX19].
Integrating [Ust11, ZGK07]. **integration** [VCD21]. **Integrity** [IMI18, LZQ⁺18, EEB⁺15, LVK18, SXZC20, TSMH19, YAM⁺15, EEB⁺15].
integrity-checking [YAM⁺15].
Integrity-OrBAC [EEB⁺15].
Integrity-verifiable [LZQ⁺18].
intelligence [KKK17, MPP21, RV19, SBGP21, VSN22].
intelligence-based [KKK17]. **Intelligent** [CSC⁺23, ZGRS23]. **intent** [LLG22, EZLC21]. **intent-based** [LLG22].
IntentAuth [LLG22]. **inter** [LLG22].
inter-process [LLG22]. **Interacting** [vOLW05]. **interactions** [Sep23].
Interactive [MS09, CDF⁺13, CHZ16, CL09, EHSS14, JT21, KBJ22, MS09]. **interest** [BHL⁺21, JK22]. **interface** [CFBvO09].
intermediaries [DGZFGH13]. **internal** [Sep23]. **International** [KBH07]. **Internet** [AHX⁺23, DHS04, Ham23]. **InterPlanetary** [BLS⁺23]. **interpretability** [ZGRS23].
interpretable [CLG23]. **interpretation** [DM07]. **interruption** [AKZM20].
intersection [MCD11]. **introspection** [AYHK18]. **Intrusion** [BT07, McH01, SBS23, WAB⁺09, ATS23, Alg22, AuHD⁺23, BR23, BCGL23, CL08, CLG23, GDA22, Ham23, KKK17, KSM10, LWA21, LWL23, MKS⁺23, MLYL20, MK21, ME23, MB23, PV22, RBEH15, SRK⁺20, SSJ22, STD21, TBGB20, TLX09, VL13, ZKP⁺23, ZGK07].
intrusions [MYLZ14]. **inversion** [PHS22].
inverting [YYH⁺23]. **Investigating** [ASAAS15]. **Investigation** [KSB23, PSA23, SGJ19]. **investigations** [GMGM21, JG15]. **involvement** [ZBD06].
IoT [LSV⁺23, AAV22, AMZ22, AKMW20, Auf20, BR23, BS22, CSC⁺23, FFG20, GA23, GMGM21, KAK23, KAK22, KKK22b, LSG22, MNC20, NNL20, OBH⁺20, PV22, SHA20, SHOL23, TKKO20, YL20, ZBC23].
IoT-enabled [SHA20]. **IoT-oriented** [KKK22b]. **IoUT** [Moh23]. **IoV** [AGZA22].
IP [BABB16, RS18, WAB⁺09]. **IPFS** [BLS⁺23, PC19]. **IPsec** [TG05]. **IPTV** [KOSU16]. **ISC** [BM05]. **ISM** [MdMF22].
ISM-AC [MdMF22]. **ISO** [CH16, DFF⁺16, MD23b].
ISO-standards-track [DFF⁺16]. **ISO/IEC** [CH16, MD23b]. **isogeny** [HM22]. **isolation** [JAYZ21]. **isomorphisms** [GMS03]. **ISP** [KCB20]. **Issue** [KBH07, Ano11b, ACM05, BJ15, BM05, Daw04, Pri04, Sne05, YSD⁺20].
issues [FSG⁺14, HC10].
Java [MLM19]. **join** [TDRR20]. **Journal** [KBH07].
KAMU [PGMLK⁺13]. **Kasahara** [CHZ16].
Keeping [BW08]. **kerberized** [PMPGMLLM12]. **Kerberos** [BCJ⁺11, MPP14, PGMLK⁺13]. **kernel** [YAY⁺21]. **Key** [AKMW20, BRS06, Gri06, MARK20, NVB⁺02, AAV22, Ala17, ALOW15, BCJ⁺11, BZ03, BBR18, BVS07, BCF⁺17, Bra22, BFS⁺13, CMR06, CCS07, CC12, CHZ16, CL09, CH16, DJN10, Das12, EHSS14, FRG19, FGS12, GNS14, GP17, Hal20, HM22, KDM22, Lu09, MPS10, MPS14, MPP14, MSN02, RHL17, RBD02, SKLP20, SSP14, TMM⁺19, TGS17, Ust11, YLL⁺18, YRW14, YYK⁺18, YSM10, ZWQ⁺17].
Key-updatable [AKMW20]. **Keyboard** [HS15, LSR⁺23]. **keyboard-based** [LSR⁺23]. **keys** [BR20, BS22, BDH⁺10, GW09, IT05, LC04, PPSS13, Pla09].
keystroke [CF07, MRW02]. **Keyword** [VH19, AKMW20, FRG19, LZQ⁺18, OO20, OSSK16]. **Keyword-based** [VH19]. **kNN** [OO20]. **knowledge** [AHX⁺23, SBG22, WCS20, YP12].
labels [ZM07]. **language** [HNHY23, TS20].

Large [TLX09, Das12, RLEM18, SMMN12, SDG22, ZWX20]. **Large-scale** [TLX09, Das12, RLEM18, SDG22, ZWX20]. **LASSI** [AAV22]. **lateral** [SKB23]. **Lattice** [GCH⁺19, SSP14, BBR18, WT21]. **Lattice-based** [GCH⁺19, SSP14, BBR18]. **lattices** [KJ14]. **law** [MdAN23]. **layer** [ANN23, DGF⁺17, KSB23, PMPGMLLM12, WR08]. **LDES** [SBD23]. **leakage** [AD08, DdP13, DBMS10, RT23, WT16, XZ21]. **leakage-resilient** [WT16, XZ21]. **learner** [HNHY23]. **Learning** [MLC23, AZ19, AAZAA23, BCGL23, CG23, EZ22, GSAMCA18, GBG18, Ham23, KBY22, KA18, KCB20, KB22, LL22, LTC23, LH23, MK21, ME23, MP22, NCBG23, OBH⁺20, PM23, SBS23, SLGP23, SRK⁺20, SKB23, SKH⁺23, SSE⁺15, TLX09, TGNA22, YYH⁺23, YA22, ZBC23]. **learning-based** [Ham23, KBY22, KB22, SRK⁺20]. **least** [PSOMS22]. **left** [Bae10]. **legacy** [KSB23]. **legal** [Lev07]. **length** [YOV09]. **Less** [BFS⁺13]. **let** [EZLC21]. **level** [AT22, AHX⁺23, DM07, MG23, SDW23, SCL⁺18, SGJC18, SGC22, ZTG22]. **Leveraging** [RV19, GDA22, GMdFLR23]. **Lib2Desc** [CAS22]. **libraries** [CAS22]. **library** [BPW05b]. **LightGBM** [PV22]. **Lightweight** [MNC20, RBEH15, AAV22, KAK22, PDM20]. **like** [ASN⁺16]. **Limits** [BP08]. **line** [BCD⁺13, LMMO04]. **line/on** [BCD⁺13]. **linear** [SBD23]. **Link** [DMDD16]. **Link-time** [DMDD16]. **linkability** [BFG⁺13]. **Linkable** [GP17]. **list** [Des09]. **list-based** [Des09]. **Listega** [Des09]. **literature** [ATS23, SAC22]. **local** [LWL⁺21, PSA23]. **localization** [ZXZ⁺11]. **location** [EG18]. **lock** [AMZ22]. **Lockmix** [BSK⁺20]. **lockpicking** [GdKGV14]. **log** [HBH12, YKP22]. **logarithm** [HMCD04]. **logarithmic** [HM22]. **logarithmic-order** [HM22]. **logging** [GMSS23]. **logic** [LM06, SBD23, SdHZ16]. **login** [KPM12]. **logs** [LL22, SKB23]. **long** [ZKP⁺23]. **look** [Auf20, ZD22]. **looks** [ASN⁺16]. **loss** [MU18]. **lottery** [GSS10]. **Low** [BGP07b, GS15, MU18, SSVC16]. **low-deterministic** [GS15]. **Low-randomness** [BGP07b]. **LPN** [RG13]. **LTE** [LSWW14]. **LWE** [SKLP20]. **LWE-based** [SKLP20]. **m** [LNX22]. **MAC** [EMRN17, SHW23]. **MAC-based** [EMRN17]. **Machine** [MLC23, MP22, AZ19, GSAMCA18, KA18, KB22, LL22, LH23, MS14, PM23, SBS23, SLGP23, SKB23, SKH⁺23, SSE⁺15]. **machine-learning** [SSE⁺15]. **machines** [MLCS16, PDM20, vOLW05]. **Maintaining** [SGC22]. **Making** [BR17]. **MalFamAware** [PLA⁺21]. **MALICIA** [NRC15]. **Malicious** [BSK⁺23, GAdFGM23, NCBG23, AKZM20, ABB17, BRS06, CMS10, GPS17, KK22, LNX22, RHGTSC17, TSMH19, WGMB13]. **Malware** [HLKI15, MLCS16, ZSN23, BEPL⁺17, BDMM19, CSC⁺23, GAdFGM23, KBY22, KKK22b, LWL⁺21, MI22, OBH⁺20, PKHS23, PDM20, PC19, PLA⁺21, SGSS23, STW⁺23, SKK⁺17, TKKO20, VPI15, WGH23, ZRJ14]. **manageability** [TG05]. **Management** [CF03, ASF04, AG23, BF13, CH16, GMMZ06, GMLM23, GH05, LLWY09, Lop18, LcSCL⁺18, NA14, PGMPPC22, RHL17, RLEM18, RBD02, SHA20, SSN15, TMP13, VdWZ14, WPD18, WW07, dAKdG10, vOLW05]. **managing** [AMLH18]. **mandatory** [DLR15]. **MANET** [Alg22]. **MANET-Cloud** [Alg22]. **manipulation** [PD21]. **map** [ZGRS23, MD23b]. **MAPAS** [KBY22]. **maps** [ZMS22]. **marketplaces** [ZTG22]. **Markov** [ABB17, RHL17]. **mask** [PKHS23]. **masking** [Rov23]. **masquerade** [Sen14]. **matching** [FHV18, SBB19]. **MaX** [BFP03]. **maximum** [AD08, BHZ⁺21]. **McEliece** [NMBB12]. **McEliece-based** [NMBB12]. **mean** [BM11]. **means** [Rov23].

measure [BF13, ORK23, SGJC18]. **measurement** [RMPADF13]. **Measuring** [RGL16, SBCP21]. **mechanism** [ACF17, IOU⁺21, LI07, PD21, TKKO20, YAY⁺21]. **mechanisms** [CSL⁺23, LBW05]. **media** [KB22, RAC16, ZLGZ19]. **mediated** [Hal20, VSM06]. **medical** [LLH21]. **meet** [FN19]. **meets** [AB22, LLBL18]. **member** [TDRR20]. **membership** [WWZ⁺23]. **memorability** [YM19]. **memory** [BHKM23, CJMS19, SV11, ZKP⁺23, vOLW05]. **memory-based** [SV11]. **mercurial** [WCS20]. **merging** [CMR06]. **Merkle** [MFES04]. **mesh** [EHM15, SSN15]. **Message** [ANS⁺12, CM16, CHM18, JZ11, TCS⁺20, YSM16, ZLL12, CL13, GP17, MS09]. **messages** [AM23]. **messaging** [Man21]. **metadata** [ACS21, KKK22b]. **metamorphic** [LNX22]. **metering** [GLMS19, MSP⁺13, RDK18, SSV22, TS20]. **Method** [SAL17, BHKM23, CYK09, FFG20, IT05, KGG09, KB23, MP15, MKS⁺23, PJ10, SKLP20, Sep23, SPDR17, WGH23, WHS18, YKP22]. **methodology** [AvO13, Des09, GMMZ06, GMGM21, SGJC18, SGJ19]. **methods** [BSK⁺23, CMN⁺18, MD23a, SBS23, TS22]. **metrics** [BDG23]. **metro** [JAYZ21]. **microaggregation** [SMMN12]. **microblogging** [ASN⁺16]. **microscope** [PCT22]. **Microsoft** [You06]. **Middle** [TCT22]. **middleware** [SRD⁺21]. **military** [SBG22]. **minimisation** [VdWZ14]. **Minimizing** [KPM12, ZBD06]. **mining** [BDMM19, BNTW12, HBH12, Sat20]. **misbehavior** [SF17]. **MITF** [SKK⁺17]. **Mitigating** [YA22, SRSM23]. **mitigation** [AHC⁺21, BHL⁺21, KCB20, KB22, SSV22, SDG22, YP12]. **mitigations** [KCC⁺23]. **mix** [BSK⁺20, Dan07, MS11, Pen11]. **mix-based** [MS11, Pen11]. **mix-related** [Dan07]. **ML/DL** [FAMMZ23]. **mmWave** [KCC⁺23]. **Mobile** [EWR⁺09, FN19, HGH23, LMMS17, ABK22, ACB14, AAZAA23, AKG16, AMRR17, CSL⁺23, CF07, GSM⁺11, GCSÁBdSS12, HIDFGHR19, HCN15, HRMM20, HZL⁺17, IDHRPCMP15, LCPD14, LH15, LL14, LV10, MTSH18, UBK23, WGMB13, ZLZL20, BT07, SSE⁺15]. **mobile-phone** [WGMB13]. **Mobile-Sandbox** [SSE⁺15]. **MobileTrust** [LV10]. **Model** [SSR22, ASF04, Ala17, ASZ⁺23, ABB17, AC08, BMV05, BGTCCBB10, BS22, BCEM04, EEB⁺15, FBFGEM21, FYF22, GMMZ06, Gol12, GYL⁺07, GKBS12, HNHY23, HL04, INS21, JGK14, Kud02, LL22, LTC23, LH15, MdSC⁺15, MdMF22, NSNK06, PHS22, QLOW09, RSD19, SK16, SPM13, SSP14, SKH⁺23, SHW23, Tip22, TND⁺15, YLL⁺18, ZGC07, ZTG22, EZ22, ZZW⁺10]. **model-checking** [AC08]. **model-oriented** [SK16]. **Modeling** [CCB08, DLR15, SDW23, ACMV15, BEd23, EZ22, GMLM23, KAC17, MB23, Sep23, Yon18]. **models** [ABB17, Auf20, Den08, DRPW12, FGS12, GGP21, KAC16, KB22, KCC⁺23]. **modes** [BDPV14]. **Modification** [PDB11]. **modified** [KJS17, ZTV23]. **modular** [MSKD16, YOV09]. **modules** [KKK22a]. **monitor** [SGJC18]. **monitoring** [HBH12, IOU⁺21, SHA20, SDR20, vORM06]. **motivate** [Fra18]. **mouse** [LSR⁺23, YA22]. **mouse-** [LSR⁺23]. **movement** [SKB23]. **moving** [BB22, DA21, HXTP23]. **MPC** [BST21, KBJ22, RSMA19]. **MQTT** [PV22, ZBC23]. **MQTT-IoT** [PV22]. **Multi** [BT07, EHM15, KWCK19, LS23, OSSK16, YYK⁺18, ZZW⁺10, BNTW12, BFT08, CON09, Das12, FAMMZ23, GMH14, HNHY23, KM03, LWL⁺21, MNC20, PGMLK⁺13, PBI⁺23, QLZH15, QLOW09, SKLP20, SGSS23, WR08, Zen22]. **multi-attack** [FAMMZ23]. **multi-authority** [QLZH15]. **multi-bit** [SKLP20]. **Multi-cast** [YYK⁺18]. **multi-classification** [LWL⁺21].

Multi-cloud [LS23]. **Multi-device** [KWCK19]. **multi-dimensional** [SGSS23]. **multi-domain** [CON09, PGMLK⁺13]. **multi-domains** [GMH14]. **multi-faceted** [BFT08, QLOW09]. **multi-factor** [MNC20]. **Multi-hop** [BT07]. **Multi-keyword** [OSSK16]. **multi-language** [HNHY23]. **multi-layer** [WR08]. **Multi-Net** [ZZW⁺10]. **multi-objective** [PBI⁺23, Zen22]. **Multi-operator** [EHM15]. **multi-party** [BNTW12, KM03]. **multi-phase** [Das12]. **multiagent** [ZGC07]. **multicast** [DWU⁺23, MP15, PJ10, TWP08]. **multicast-based** [MP15]. **multicoupon** [HIDFGHR19]. **multifaceted** [JBK21]. **multifactor** [IT05]. **multiple** [CC12, HMCD04, WMS⁺19]. **multiple-key** [CC12]. **multiplication** [YOV09]. **multiplications** [HTM11]. **multipliers** [YOV09]. **multiresolution** [VSR15]. **multiset** [BA16]. **multisignatures** [HRL09]. **must** [ASN⁺16]. **Mutual** [HZL⁺17, MNC20].

naive [Sen14]. **named** [JK22, ZP23]. **names** [CYA⁺18]. **Narrow** [Tip22]. **NDCG** [BDG23]. **NDN** [BHL⁺21]. **need** [JTV19]. **Negative** [EFH09, EAH⁺07, DNF⁺19]. **negotiation** [KLMM09]. **negotiation-based** [KLMM09]. **neighborhood** [LWL⁺21]. **Net** [ZZW⁺10, WYL⁺12]. **Nets** [BKBB20, BBB20, SSFB15]. **Network** [GPS17, ATSS23, ABK22, ABCC08, AuHD⁺23, BB22, BMP⁺14, CLG23, CL09, EMRN17, GDA22, GBG18, GH05, JJJ21, LBZ⁺10, wLW05, MARK20, MKS⁺23, ME23, MYLZ14, MPG21, PAI⁺23, PMPGMLLM12, RSV23, RS18, SGSS23, SAT09, SRSM23, TLX09, TCE23, WYL⁺12, YKP22, Zen22, Zha23, dAKdG10]. **Network-based** [GPS17]. **Networked** [MR03, BHZ⁺21, SRD⁺21]. **networking** [AFA⁺23, JK22, MdMF22]. **networks** [ACB14, BDG23, CMR06, CPPK15, Das12, DRPW12, DWU⁺23, EHM15, EMRN17, FN19, Gol12, GDA22, GGP21, GBG18, KSB23, KIP22, LTC23, LH23, MLYL20, RBEH15, RMSCR19, SS17, SSN15, SF17, SKH⁺23, SDG22, WWZ⁺23, YRW14, ZXZ⁺11, BT07]. **neural** [BDG23, WWZ⁺23]. **news** [RB23]. **next** [AMLH18, EZLC21, EZLC21]. **next-generation** [AMLH18]. **Next-Intent** [EZLC21]. **NICs** [CBC08]. **nightmare** [EZLC21]. **NIZK** [WT16]. **NLP** [MI22]. **no** [BB04b, CMN⁺18]. **Node.js** [KKK22a]. **nodes** [BHZ⁺21]. **noise** [EG18]. **noisy** [BDH⁺10, KML03]. **non** [CDF⁺13, CHZ16, CL09, EHSS14, GRV05, HYWS11, JT21, KBJ22, KM03, MP16, RMSCR19, SB22]. **non-compressing** [MP16]. **non-cyber** [SB22]. **non-delegatability** [HYWS11]. **non-deterministic** [RMSCR19]. **non-interactive** [CDF⁺13, CHZ16, CL09, EHSS14, JT21, KBJ22]. **non-repudiation** [GRV05, KM03]. **noninterference** [BP04]. **nonlinear** [MB23]. **notaries** [MdAN23]. **note** [ZZH08]. **Nothing** [MTW⁺14]. **notions** [BCL09, BFS⁺13]. **Novel** [Alg22, KK22, KNL16, Lin15, MK21, MG23, MB23, NNL20, SGSS23, SHW23, WGH23]. **NSDroid** [LWL⁺21]. **number** [SBD23]. **numerical** [SMMN12, TNA23, ZO13].

OAuth [MP22]. **Obfuscated** [VCD21, BR20]. **obfuscation** [OSSK16, SXZC20]. **object** [HS09, SRD⁺21, SS05b]. **object-sensitive** [HS09]. **objective** [PBI⁺23, Zen22]. **objects** [DA21, RT23]. **oblivious** [BA16, HSMY12, LD17, TND⁺15]. **observatory** [VSN22]. **observer** [YAY⁺21]. **obtain** [Bra06]. **OCCP** [ACT23]. **Octopus** [BLS⁺23]. **Off** [BCD⁺13, CJMS19]. **Off-line** [BCD⁺13]. **Off-line/on-line** [BCD⁺13]. **Offline** [MWZ06, LMG17, LBZ⁺10]. **OFMC** [BMV05]. **Ohgishi** [CHZ16].

Okamoto [GMMV05]. **on-line** [BCD⁺13, LMMO04]. **on-the-fly** [CL13]. **one** [GMS03, GDA22, MLCS16, YRW14]. **one-class** [GDA22, MLCS16]. **one-pass** [YRW14]. **onion** [CDF⁺13, CFG17]. **OnionDNS** [SCL⁺18]. **Online** [SSR22, KB22, LMG17, LD07, LBZ⁺10, PLA⁺21]. **online/offline** [LMG17, LBZ⁺10]. **only** [LD17]. **Opacity** [BKMR08]. **open** [Küs05, RM12, SVKV21, SKB23, VSN22]. **open-ended** [Küs05]. **open-source** [SKB23, VSN22]. **opening** [EHSS14]. **operational** [SGJC18, SGC22]. **operations** [BA16, HTM11, NRC15]. **operator** [EHM15]. **Optimal** [DRPW12, EG18, GYL⁺07, VSR15]. **optimisation** [PDB11]. **optimistic** [DGZFGH13, HYWS12, SEXY18]. **Optimization** [HBK22, MU18, GZH⁺23, KLZ⁺21, LL14, PBI⁺23, TGNA22, Zen22]. **oracle** [HYWS11, Yon18]. **oracles** [HSMW08, HYWS12]. **OrBAC** [EEB⁺15, GBDJ14]. **order** [HM22, LM06, PSTS20]. **organization** [INS21]. **oriented** [KKK22b, Moh23, SK16, WW07]. **OSBE** [HSMY12]. **OSN** [RT23]. **OSPU** [Zha23]. **Outbound** [Smi04]. **Outsourced** [CG21, FHV18, CTM⁺16, LD17]. **outsourcing** [AL05, GYL⁺07, HJDC15, KU16, ZLZL20]. **overlays** [MLCQ21]. **overview** [BMP05, TS22]. **Own** [ACMV15].

P2ADF [KAK23]. **P2P** [MLCQ21]. **P3** [BS22, YL19]. **PAASO** [TGNA22]. **packet** [JK22, AM23]. **packets** [vORM06]. **packing** [BEPL⁺17]. **pads** [dSFK19]. **page** [PD21, TSMH19]. **PageDumper** [PD21]. **pages** [PM23, SGLC19]. **Paillier** [NSNK06, DJN10]. **Paillier-based** [NSNK06]. **pairing** [MSGCDPSS18, YRW14, ZZH08]. **pairing-based** [MSGCDPSS18]. **pairing-free** [YRW14]. **pairings** [BCL09, CCS07]. **papers** [ACM05]. **paradigm** [BCD⁺13]. **parallel** [HBK22]. **parallelism** [SBB19]. **parallelizable** [MP16]. **parameter** [DTK⁺18]. **parameters** [NMBB12]. **parazoa** [AMP12]. **parking** [BS21]. **partial** [CKW19, XZ21]. **particle** [TGNA22]. **parties** [HZZ⁺17, KPM12]. **party** [BNTW12, CAS22, KM03, LCL16, MR04]. **pass** [YRW14]. **passenger** [AG23]. **Passive** [CBC08, SS05a, ALOW15]. **Passive-attack** [SS05a]. **Password** [CHMS21, MPS10, MRW02, PCT22, AKT23, CG14, CJMS19, GTM11, HKO22, KJS17, KB23, Lop18, MSKD16, SB09, WLLW14, YM19, YL19]. **Password-authenticated** [CHMS21, MPS10]. **password-based** [HKO22]. **passwords** [CFBvO09, JTV19, YL19]. **past** [JG15, LMMP06]. **patching** [JM17]. **paths** [BHZ⁺21]. **PatrioT** [SHOL23]. **Pattern** [IS23, FHV18, OSSK16, SBB19, TS20, YA22]. **patterns** [CFBvO09]. **pay** [BS21, Roe11a, Roe11b, DZW⁺18]. **pay-by-phone** [BS21]. **pay-TV** [Roe11b, Roe11a, DZW⁺18]. **PBAC** [Kud02]. **PDGuard** [MSKS20]. **peer** [BLS⁺23]. **peer-to-peer** [BLS⁺23]. **PEKS** [AKMW20]. **perception** [MTSH18]. **Perceptual** [SB14]. **Perfect** [Hub12]. **performance** [AZ19, BBR18, BNTW12, DDZ22, HIDFGHR19, IDHRPCMP15, SK16, SSN15]. **Periodicity** [JM17]. **permissions** [ACS21, ZSN23]. **permutations** [BR17]. **Persona** [SSR22]. **personal** [IHNT02, MSKS20, QLZH15]. **personality** [PPL15]. **personalized** [CG23]. **perspective** [AAM23]. **perspectives** [INS21]. **perturbation** [WWZ⁺23]. **Petri** [BKBB20, SSFB15, BBB20]. **phase** [Das12]. **Phish** [PM23]. **Phish-Sight** [PM23]. **phishing** [FYF22, PM23]. **phone**

[BS21, CF07, GSM⁺11, HCN15, WGMB13]. **phylogeny** [BDMM19]. **physical** [AGZA22, AK23, CK23a, CK23b, HXTP23, LWL23, PCK22b, SM10]. **physically** [BR17, BR20, KKY⁺23]. **PIN** [dSFK19]. **PINs** [MTSH18]. **PIOAs** [Yon18]. **PIR** [DYDW10]. **pirates** [Nui12]. **PiSHi** [MBHT17]. **PKI** [BB04b, Daw04, LC04, LMMP06, LMMO04, SVKV21, VSM06]. **PLAID** [DFF⁺16]. **Plaintext** [MPS14]. **plane** [AM23]. **platform** [IDHRPCMP15, MBRPS18, MG23]. **platforms** [KPM12, RHGTSC17]. **playground** [PC19]. **PLC** [JAYZ21]. **please** [PSTS20]. **point** [ABB17, KW15]. **poisoning** [BDG21]. **policies** [ABCC08, ACMV15, AICC18, BCL13, BBB20, CF03, CCB08, KAC17, LBW05, LRB⁺10, RRI⁺19, SB09, SRD⁺21, BKBB20]. **Policy** [SAL17, BZV05, GMH14, JSMG18a, JSMG18b, KNL16, MS15, TG05, XSA13, dAKdG10]. **PolicyUpdater** [CZ06]. **pollution** [EMRN17, KKK22a]. **Polly** [SGE02]. **polymorphic** [KJG⁺11]. **polynomial** [PCK22a, SGE02, TND⁺15]. **polynomial-based** [SGE02]. **polynomials** [GMS03]. **popular** [FBFGEM21]. **Portfolio** [LL14]. **post** [TSZ22]. **post-quantum** [TSZ22]. **posteriori** [ACBC⁺15]. **postfix** [YL19]. **postgraduates** [AHX⁺23]. **Posthumously** [SSR22]. **potential** [WGMB13]. **power** [AKZM20, MD23a]. **practicability** [IDHRPCMP15]. **Practical** [DDX19, LLW⁺16, ALOW15, GKS19, HRMM20, KOSU16, KBY22, LCL14, MI22, Pen12, SHOL23, VHT09, WR15]. **practices** [LD07]. **Pragmatic** [KDM22]. **pre** [CMR06, MARK20, Pen13]. **pre-computation** [Pen13]. **pre-distribution** [CMR06, MARK20]. **precise** [AAB20, IKS22]. **prediction** [KCC⁺23]. **predictive** [LL22]. **Preface** [Ano11a, ACM05, BGP07a, BM05, Daw04, DV08, DMRS07, Pri04, Sne05, Wai04, ZL06]. **prefix** [BGKZ12, YL19]. **presence** [ZTV23]. **present** [LMMP06]. **preservation** [LLH21, RAC16]. **preserve** [EEB⁺15]. **preserved** [JSMG18a, LD17]. **preserving** [ABFO08, BEY23, BGK08, BLS⁺23, BSK⁺20, BS21, CTM⁺16, DFBJR18, GGJ22, GKS19, HLS18, HRMM20, KAK23, KOSU16, KB13, KNL16, MB16, MCD11, NST09, NA14, QLZH15, RDK18, SSL22a, STD21, Tor20, WMS⁺19, YWW22, Yan21]. **Preventing** [RAC16, PS17, YP12]. **prevention** [Alg22, LH23, PSDSNAHJ19, VL13, YAY⁺21]. **primitives** [MP16, SM10]. **principle** [Bel10]. **Principles** [CGL⁺11]. **prioritization** [SDG22]. **Privacy** [AaBZS23, BEY23, KB13, MB16, MSP⁺13, NST09, QLZH15, RDK18, SSL22a, UBK23, ABFO08, AJC⁺09, AMRR17, BGK08, BLS⁺23, BSK⁺20, BCA⁺10, BDHZ15, BS21, Bra06, CR20, CTM⁺16, EG18, EAH⁺07, GGJ22, GLMS⁺04, GGP21, GKS19, GYL⁺07, GP23, HRMM20, KAK23, KOSU16, KBH07, KNL16, LD07, LD17, LeSCL⁺18, MCD11, MBRPS18, NA14, OAJ23, PGMLK⁺13, PSA23, RSPMB16, RMPADF13, SAC22, STD21, Tip22, Tor20, TGNA22, WMS⁺19, YWW22, Yan21, YSD⁺20, YAM⁺15, ZHZ22, ZZG19]. **privacy-aware** [MBRPS18, RSPMB16, TGNA22]. **Privacy-enhanced** [MSP⁺13]. **privacy-preserved** [LD17]. **Privacy-preserving** [BEY23, KB13, MB16, NST09, QLZH15, RDK18, ABFO08, BGK08, BSK⁺20, BS21, CTM⁺16, GKS19, HRMM20, KAK23, KOSU16, MCD11, NA14, STD21, Tor20, WMS⁺19, YWW22, Yan21]. **Private** [BA16, DMP13, BDD01, BGP07b, DA21, KW15, LMD17, PHS22, PGMPPC22, TMM⁺19, VH19, WR15]. **privilege** [FTS⁺20, PMDS23, PSOMS22, YAY⁺21]. **Probabilistic** [DHW11, BP04, GYL⁺07, MCD11, PJ10]. **probability** [BHZ⁺21]. **problem**

[CC12, GOBdlC11, GMS03, GP17, KG11, RG13, TWP08, YSM10]. **problems** [HMCD04]. **process** [BDMM19, HBH12, LLG22, Yan21]. **processes** [RHL17]. **processing** [MSKS20]. **processor** [KKK22b, TKKO20]. **profiling** [LCPD14, YA22]. **program** [BDF04, HS09]. **programmability** [Yon18]. **programmable** [Smi04]. **programming** [RRI⁺19, WZ07]. **programs** [KM07, WGMB13]. **progressive** [WPD18]. **project** [BFP03]. **proof** [HLS18, WLLW14]. **proofs** [BCJ⁺11]. **propagation** [IKS22]. **property** [TS20]. **Proposal** [IHNT02, IT05]. **proposals** [BJ16]. **protect** [TS22]. **protected** [BJ16]. **Protecting** [EAH⁺07, SAH22]. **Protection** [AM23, BZ20, AJC⁺09, GKBS12, KK17, MGRR19]. **protections** [VCD21]. **protocol** [AAV22, AGZA22, Ala17, ALPW13, Bel10, BFT08, CL09, DFF⁺16, DGZFGH13, HL04, HYWS12, KIP22, LSWW14, LH23, MG19, ML17, MNC20, RG13, RGL16, SDR20, YRW14, YAM⁺15, ZBC23]. **Protocols** [DHS04, LSG22, LSV⁺23, AC08, ABFL12, BGK08, BMV05, BBR18, Bra22, BNN04, CCS07, DVB02, DS07, Fra18, GLP03, GRV05, Hal20, HLS18, KM03, K us05, LCL16, MPI15, MUIH⁺21, MSN02, MS14, SSFB15, Ust11, Vaj16, VdWZ14]. **prototype** [KKK22a, TKKO20]. **Provable** [YRW14, NSNK06]. **Provably** [FRG19, LCL14, RG13, VHT09, YYK⁺18]. **provenance** [Abb13]. **provided** [TS22]. **providing** [PGMLK⁺13]. **Provision** [Kud02]. **Provision-based** [Kud02]. **provisioning** [TGS17]. **proxy** [LL22, Lin15]. **pseudo** [HIST09]. **pseudo-freeness** [HIST09]. **PSO** [TGNA22]. **Public** [Bra22, SXZC20, AKMW20, ALOW15, BCJ⁺11, BZ03, DJN10, EHSS14, FRG19, GW09, GMdFLR23, LC04, Pen12, SSP14, Gri06]. **public-key** [AKMW20, ALOW15, BCJ⁺11, DJN10, EHSS14, FRG19, SSP14]. **publishing** [AAM23, SAC22]. **PUF** [AHC⁺21]. **push** [BFPP07]. **push-based** [BFPP07]. **pushdown** [BCL13]. **puzzle** [WR08]. **puzzle-based** [WR08]. **PVSS** [Pen12].

QR [HZL⁺17]. **QR-code** [HZL⁺17]. **quality** [SBCP21]. **quantitative** [JBK21, SKY23]. **quantum** [Sat20, TSZ22]. **queries** [MRG23]. **query** [BB04a, KCM⁺15]. **queue** [BF13]. **QUIC** [CKKK23]. **quick** [WT21]. **quotient** [PCK22a].

R [SKLP20]. **race** [ANN23, sLC05]. **racer** [ANN23]. **RADS** [SKH⁺23]. **RAM** [LD17]. **RAM-based** [LD17]. **ramp** [LMD17]. **Random** [ASA23, Tor20, BR17, BR18, Das12, HSMW08, HYWS11, HYWS12, UMN⁺20, VSR15, Yon18]. **randomization** [PCK22b]. **Randomized** [ML14]. **randomness** [BGP07b]. **range** [KMMG23, MRG23]. **rank** [BDG23]. **ranked** [OO20]. **ransomware** [CMN⁺18]. **ratcheting** [GMSS23]. **rate** [AM23]. **rational** [ETAHCR08]. **RBAC** [BGTCCBB10]. **re** [GI19, Dan07]. **Re-encryption** [Dan07]. **re-identification** [GI19]. **reacting** [AGIK07]. **reactive** [BDHK08]. **Reactively** [BPW05a]. **reader** [GdKGV14]. **Real** [CK23b, GDA22, KCB17, RLEM18, SBS23, SKH⁺23, TSZ22, CK23a]. **Real-time** [CK23b, GDA22, KCB17, SBS23, SKH⁺23, CK23a]. **real-world** [TSZ22]. **realistic** [BB22, HS15]. **realization** [KAC16]. **realize** [AKMW20]. **realizing** [RD16, ZZG19]. **really** [BM11]. **reasoning** [GMMZ06]. **receivers** [AP22]. **reciprocal** [BDG23]. **recognition** [GCS AbdSS12, ZP23]. **Recommendation** [PBI⁺23, OAJ23]. **recommendations** [YNC22]. **recommender** [ABFO08]. **record** [QLZH15]. **records** [QDW⁺15]. **recovery** [CMS10, JAYZ21, NVB⁺02]. **rectangle** [Lu09]. **recursive** [Rus04]. **Redistributing**

[LKH09]. **reduction** [KKY⁺23, WT21]. **redundancy** [JAYZ21]. **references** [ZD22]. **refinement** [dAKdG10]. **reflects** [PPL15]. **refunds** [KO02]. **regions** [EG18]. **regression** [MB23]. **Regular** [Bae10, WR15]. **regular-expression** [WR15]. **regulated** [BS21]. **reinforcement** [EZ22, ME23, SRK⁺20]. **rekeying** [PJ10, TDRR20]. **Related** [Lu09, AaBZS23, Dan07]. **Related-key** [Lu09]. **relation** [MS11, Pen11]. **Relations** [FGS12]. **relationships** [CTM⁺16, RAC16]. **release** [BFS⁺13]. **release** [DA21, NAM06]. **reliable** [ABCC08, AvO13]. **remanence** [SV11]. **remote** [CGL⁺11, GW09, KK22, MMS16, YAM⁺15]. **renewable** [BDH⁺10]. **reordering** [WT21]. **Repairing** [GLMS19]. **repeated** [KLZ⁺21, vORM06]. **Replacement** [XCW⁺12]. **reporting** [MPP21, SDW23, SBG22]. **representations** [EFH09]. **repudiation** [GRV05, KM03]. **reputation** [LI07, SSV22, SdHZ16]. **Requirements** [GMMZ06, WW07, CSL⁺23, FFG20, SK16]. **resampling** [ASA23]. **Rescue** [BST21]. **Research** [Gri06, GDA22, RM12, SHOL23]. **residence** [PPL15]. **resident** [BMP⁺14]. **resilience** [SAH22]. **resilient** [MR03, WT16, XZ21]. **resistance** [TGS17]. **resistant** [CHKO12, LL21, SCL⁺18, MS09]. **resolutions** [RV03]. **Resolving** [CTM⁺16]. **resource** [LVK18, SS17]. **resource-bounded** [LVK18]. **resource-constrained** [SS17]. **resources** [GMdFLR23, TZH04]. **response** [SSD14]. **Restricted** [SF17]. **Restricting** [RT23]. **results** [BCD⁺13, DLR15]. **retention** [GSM⁺11]. **retraining** [KCC⁺23]. **retrieval** [BDD01, LMD17]. **reusable** [KO02]. **reveal** [GSM⁺11]. **Reverse** [MLM19, EAH⁺07, BZ20]. **reversed** [KYH18]. **review** [ATS23, CKKK23, KSB23, OAJ23, RB23, SAC22, VMCR23]. **revisited** [BZ03, BRS06, BVS07, BCD⁺13, CHZ16, GMMV05, RSD19, RDK18]. **Revisiting** [CKKK23]. **revocable** [JCL⁺18, Lin15]. **revocation** [HRMM20, MFES04, NST09, QLZH15, ZJS22]. **revoke** [NP10]. **revoking** [DdP13]. **RFID** [ALOW15, SV11, Tip22]. **rich** [RMSCR19]. **right** [Bae10, Lop18]. **right-to-left** [Bae10]. **rights** [ASF04, LKH09]. **Rigorous** [GH05]. **ring** [GCH⁺19, JT21]. **rings** [PCK22a]. **Risk** [INS21, MYLZ14, NBA⁺21, AK23, AG23, EAM⁺23, HXTP23, MTSH18, ORK23, RV19, SSD14, SCO21, SDG22, TNA23, WHS18, ZTG22]. **risk-based** [SCO21]. **risk-level** [ZTG22]. **risks** [GYL⁺07, JBK21]. **RL** [PKHS23]. **Robotics** [YNC22]. **robust** [GKBS12, MS11, SRK⁺20]. **robustness** [ZWX20]. **role** [BSK⁺23, CK08, ZVH15]. **role-based** [CK08, ZVH15]. **ROM** [MLM19]. **RORI** [GBDJ14]. **RORI-based** [GBDJ14]. **round** [ABM⁺12, BGP07b, GNS14, NSNK06]. **rounds** [Lu09]. **Routing** [SSN15, BT07, CDF⁺13, CFG17, KCB17, LH23, MG19]. **RPCAE** [Lin15]. **rPIR** [LMD17]. **RSA** [LC04, MPS10]. **rule** [KAC16, OBH⁺20]. **rules** [ABCC08, HBK22, KAC17]. **run** [LBW05, PD21]. **run-time** [LBW05, PD21]. **runtime** [DLR15, KDYS19]. **safeguarding** [BCA⁺10]. **safer** [CMMPS15]. **safety** [AaBZS23]. **safety-related** [AaBZS23]. **sail** [BB04b]. **SAINT** [VSN22]. **Sakai** [CHZ16]. **saliency** [ZGRS23]. **salp** [PV22]. **SAML** [EWR⁺09]. **samples** [SSVC16]. **Sandbox** [SSE⁺15]. **sanitization** [ZLGZ19]. **SARSA** [ME23]. **SARSA-based** [ME23]. **SAS** [KJG⁺11]. **SAT** [AC08]. **SAT-based** [AC08]. **satellite** [KW15]. **SCADA** [Ano11b, HBH12]. **scalability** [TGS17]. **Scalable** [HKO22, RMSCR19, HRMM20, KCB17, MK21, SB14, YYK⁺18]. **scale**

[Das12, RLEM18, SDG22, TLX09, ZWX20]. **scan** [AvO13]. **scanning** [CBC08]. **scattered** [SBG22]. **scenario** [ASZ+23, SRD+21]. **scenarios** [HS15, PGMLK+13]. **scheduling** [PNG+20]. **scheme** [AaBZS23, AKT23, BZ03, BDD01, BCL09, CG14, CMR06, CC10, Das12, DSY06, EMRN17, FTS+20, HCN15, IS23, JT21, KOSU16, LLH21, Lin15, MD23b, NT20, PDB11, QDW09, RHL17, RSD19, SHA20, WLLW14, YWW22, YYH+23, ZLZL20, ZLJW20]. **schemes** [BPW05a, BR18, CJMS19, DdP13, Dan07, DHS04, Den08, GP17, HSMY12, HYWS11, NP10, PBI+23, TMM+19]. **score** [SSV22]. **scoring** [OSSK16]. **SDN** [AM23, LWL23, MLCQ21, Moh23, MLC23, SHW23]. **SDN-assisted** [LWL23]. **SDN/Fog** [Moh23]. **SDN/Fog-based** [Moh23]. **SDSI** [LM06]. **SE** [MG19]. **SE-AOMDV** [MG19]. **SealFSv2** [GMSS23]. **search** [AKMW20, CKS21, FRG19, HH16, KJS17, OO20, OSSK16]. **searchability** [HJDC15]. **searchable** [CHMS21, HK19, LZQ+18, MRG23]. **searches** [WR15]. **searching** [VH19]. **Seberry** [BZ03]. **second** [ABM+12]. **secrecy** [CDF+13, Hub12]. **secret** [CG21, DdP13, GMS03, HJDC15, LMD17, PPSS13, QDW09]. **secrets** [BW08, JTV19]. **Secure** [ABB17, AL05, BVS07, CKW19, CKS21, CSL+23, DZW+18, FTS+20, HN14, HSMW08, KW15, KM22, LL21, LCL16, MSKD16, PMDS23, SJ09, SBB19, UMN+20, ZXZ+11, ASF04, Ala17, BPW05a, BSK+20, BDF04, BNTW12, BT07, DdP13, DWU+23, DDX19, FZ21, FRG19, GA23, KME+16, KAK22, KU16, KSZ07, LCL14, LLW+16, MG19, MB16, MLO+04, MBRPS18, MPP14, MD23b, MSKS20, MG23, Moh23, NT20, NMBB12, Nui12, OO20, PJ10, PBI+23, QDW+15, RG13, SJ10, SK16, Smi04, TND+15, WPD18, YL20, YYK+18, YAM+15]. **secured** [BS22, EHM15]. **Securing** [DDPS02, LLG22, MPG21, ZBC23, BFPP07, CC10, PDM20, PCK22b]. **Security** [AGZA22, Ano14, BCL13, BDHZ15, FSG+14, GMH14, HJDC15, OO20, OT06, PNG+20, SB22, YWW22, ZZW+10, AK23, ACB14, ABCC08, ANN23, AHX+23, ABM+12, Ano11b, AC08, Auf20, AICC18, BCJ+11, BGKZ12, BMV05, Bel10, BKBB20, BBB20, BCF+17, BFT08, BCL09, BFS+13, BNN04, BCEM04, CDP22, CAS22, CLW+11, CKKK23, CFBvO09, CG23, CYK09, CLPP11, CCB08, DSB19, DM07, Den08, DRPW12, EHM15, FGS12, GS15, GLMS+04, GYL+07, GMLM23, GRV05, GH05, HS15, HMCD04, INS21, JBK21, JGK14, KBJ22, KMMG23, KLPL21, KIP22, KKKV07, KBH07, KLMM09, KMR09, KCC+23, Lan01, LBW05, LP11, LV10, LS23, wLW05, MBH+21, MdSC+15, MP15, MdMF22, MSGCDPSS18, NSNK06, PDB11, RM12, RG13, RGL16, SK16, SS17, SKY23, SSN15, SBG22, SM10, SAT09, TG05, VSM06, WYL+12, WHS18]. **security** [YNC22, YLL+18, YRW14, YSD+20, YP06, YM19, Zha23, ZGRS23, ZM07, dAKdG10, vOLW05, BJ15, Pri04, KBH07]. **security-centric** [CAS22]. **security-mediated** [VSM06]. **security-sensitive** [HS15]. **SEDS** [NT20]. **seizure** [SCL+18]. **seizure-resistant** [SCL+18]. **selected** [ACM05]. **Selecting** [NMBB12]. **selection** [GBDJ14, SBS23, SJ10, SKY23, Ssvc16, ZGC07]. **selective** [ZZG19]. **selective-ID** [ZZG19]. **self** [GMLM23, KK22]. **self-defense** [KK22]. **self-sovereign** [GMLM23]. **SELinux** [XSA13]. **sellers** [ZGC07]. **semantic** [YKP22]. **semantic-aware** [YKP22]. **semantics** [KJG+11]. **semi** [Zha23]. **semi-network** [Zha23]. **sensitive** [HS15, HS09, RAC16, STW+23, TS22, ZO13]. **sensor** [AAZAA23, CMR06, Das12, KCM+15, LBZ+10, MARK20, OBH+20, RBEH15, YRW14, ZXZ+11]. **sensors**

[CSC⁺23, CLW⁺11, MTS18]. **sequence** [AL05, BZV05, BSK⁺23, KSM10]. **sequential** [BDPV14]. **series** [KKK22b]. **server** [Bra22, MYLZ14, NT20]. **server-aided** [NT20]. **service** [BSK⁺20, LLWY09, NA14, WR08, WW07, TGS17]. **service-oriented** [WW07]. **services** [AV17, DDPS02, EWR⁺09, GGJ22, KBH07, MdAN23, MS15, PMPGMLLM12, SHA20, SKY23, VL13]. **session** [LL22, SCO21]. **sessions** [ACB14]. **set** [BA16, MCD11, RRI⁺19, WZ07, BMP05]. **Sets** [SAL17, WCS20]. **setting** [IS23]. **settings** [AVM23]. **SFCGDroid** [STW⁺23]. **SHA** [ABM⁺12, KJS17]. **SHA-1** [KJS17]. **SHA-3** [ABM⁺12]. **shared** [BS05]. **sharing** [CMMPS15, CG21, HJDC15, LKH09, LMD17, QDW09, SSL22a]. **sharing-based** [HJDC15, LMD17]. **ships** [AG23]. **Short** [Nui12, JSMG18b, LMG17, SK14, ZKP⁺23]. **short-term** [ZKP⁺23]. **shortcut** [MLM19]. **shot** [SLGP23]. **Shoulder** [WLLW14]. **Shoulder-surfing-proof** [WLLW14]. **shuffle** [DYDW10, Pen13]. **shuffles** [NSNK06]. **shuffling** [PDB11]. **side** [ANN23, CBRY20, dSFK19, HS15, KDYS19, MTW⁺14, SB22]. **side-channel** [CBRY20, dSFK19, KDYS19, MTW⁺14, SB22]. **SIEM** [VMCR23]. **Sight** [PM23]. **Signature** [JMV01, TMM⁺19, BPW05a, DHS04, EHSS14, GP17, HSMW08, HYWS11, JT21, KJG⁺11, LBZ⁺10, LWL⁺21, RD16, RSD19, Yon18, ZBD06]. **signatures** [ACHO13, BCD⁺13, GCH⁺19, IDHRPCMP15, IT05, KJ14, MR04, PS17, SEXY18, SK14, WPD18, YSM10]. **signcrypton** [LMG17, RD16]. **signers** [BRS06]. **signing** [IZS08, TSZ22]. **SilentKnock** [VHT09]. **simple** [BR20, MD23b]. **Simplified** [BCL09]. **simulatability** [BDHK08]. **simulatable** [BPW05b]. **simulation** [BB22, SB09, WT16]. **simulation-extractable** [WT16]. **simultaneous** [Man21]. **size** [DFBJR18, PPSS13]. **Skype** [DBMS10]. **SLE** [vOLW05]. **slicing** [MS15]. **small** [MP16]. **smart** [AKZM20, AT22, AMZ22, AZ22, BAB23, DMDD16, FBFGEM21, GdKGV14, GLMS19, HKO22, MSP⁺13, MPP14, MdAN23, PNG⁺20, RDK18, SSL22b, SRD⁺21, SSV22, SAH22, Yan21, GAdFGM23]. **smashing** [MGRR19]. **smudge** [SSL22b]. **SOAP** [DDPS02]. **social** [DMP13, FN19, KPM12, KB22, LTC23, RAC16, Tor20]. **software** [JM17, KSB23, LNX22, MLO⁺04, MdMF22, SK16, SK06, SKH⁺23, VCD21, XCW⁺12, ZGK07]. **software-defined** [KSB23, MdMF22, SKH⁺23]. **solution** [MCD11, PMPGMLLM12, SK16]. **solutions** [HIDFGHR19]. **Solving** [GOBdlC11, GP17, HMCDO4]. **some** [BR20]. **SonarSnoop** [CBRY20]. **sound** [BCJ⁺11, BDPV14]. **soundness** [BP08]. **source** [SKB23, VSN22]. **sources** [CF03]. **sovereign** [GMLM23]. **Space** [MBH⁺21, PCK22b]. **spam** [ASN⁺16, BABB16, SSM⁺20]. **spammer** [ASN⁺16]. **sparse** [ACB14]. **spatial** [AVM23, DA21, ZMS22]. **spatio** [SKK⁺17]. **spatio-temporal** [SKK⁺17]. **spatiotemporal** [ZMS22]. **Special** [Ano11b, BJ15, KBH07, YSD⁺20, ACM05, BM05, Daw04, Pri04, Sne05]. **specific** [KME⁺16, LSR⁺23]. **specification** [TS20]. **specifications** [ZGK07]. **Specifying** [BGK08]. **spectrum** [CSC⁺23]. **spending** [PSDSNAHJ19]. **spirit** [PSOMS22]. **SPIT** [GKBS12]. **SPKI** [LM06]. **SPKI/SDSI** [LM06]. **sponge** [AMP12]. **spoofing** [Hub12]. **spotlight** [ACT23]. **spread** [WGMB13]. **SpyDetector** [KDYS19]. **SQL** [DSB19]. **squaring** [HTM11]. **SRAM** [KKY⁺23]. **SRAM-based** [KKY⁺23]. **SRU** [CLG23]. **SSH** [LL22]. **SSL-protected** [BJ16]. **SSO** [PMPGMLLM12]. **SSPFA** [MGRR19]. **stabilizers** [BR20]. **Stack**

[BDF04, MGRR19]. **stacking** [AuHD⁺23]. **stacking-based** [AuHD⁺23]. **stages** [ASZ⁺23]. **standard** [Ala17, CH16, RSD19, SSP14]. **standards** [DFV⁺16]. **star** [RS18]. **State** [vOLW05, TDGL23]. **Stateful** [LMMS17, YLL⁺18]. **Static** [SS05b, AAB20, CMS10, MS15, SCO21, SSE⁺15, ZM07]. **status** [HC10]. **Std** [KDM22]. **steal** [SGLC19]. **Stealing** [MTSH18]. **stealth** [KK22]. **steganography** [Des09, SJ09, SJ10]. **steps** [ASZ⁺23]. **sticky** [SRD⁺21]. **Stochastic** [WYL⁺12]. **storage** [GW09, GMSS23, LZQ⁺18, NT20, YAM⁺15]. **storage-based** [GMSS23]. **storages** [CTM⁺16]. **storing** [HK19]. **STORK** [RLEM18]. **STR** [IHNT02]. **strategies** [wLW05]. **stream** [GDA22, HL04, IMI18, TWP08]. **stream-based** [GDA22]. **streaming** [ZO13, ZHZ22]. **Street** [MD23b]. **strength** [KB23, RGL16]. **STRIDE** [ZTG22]. **STRIDE/DREAD** [ZTG22]. **string** [KCM⁺15]. **Strong** [CHKO12, XZ21, HYWS11, YLL⁺18]. **stronger** [PDB11]. **Strongly** [WT16]. **Structural** [KA18, GI19]. **structure** [QDW09, TTS⁺06]. **structures** [KN07, K us05, RD16, Rus04]. **study** [BSCZ11, BKBB20, BBB20, BDG21, BF13, CKKK23, DSB19, DSRHC16, GLMS⁺04, IS23, KB22, OBH⁺20, SKY23, SKK⁺17, TS20, XSA13, ZD22, ZHZ22]. **Studying** [WT21]. **style** [BPW05b, BP08]. **subject** [LcSCL⁺18]. **subjective** [SdHZ16]. **subset** [FRG19, KG11]. **subspace** [RG13]. **substitution** [AP22, BRS06]. **subsystem** [VSN22]. **subtree** [Roe11a, Roe11b]. **Sufficient** [BDPV14]. **suffix** [BGKZ12]. **suffix-free-prefix-free** [BGKZ12]. **suitable** [Pla09]. **sum** [KG11]. **supersingular** [HM22]. **Supervised** [GSAMCA18, SKB23]. **supply** [AKZM20, AHC⁺21]. **support** [CON09, MLCS16, ZGRS23]. **supporting** [ARMLS06, JSMG18a, JSMG18b, MRG23, RV03]. **supports** [WR15]. **surface** [ZD22]. **surfing** [WLLW14]. **surveillance** [Lev07, LcSCL⁺18, MBRPS18, RSPMB16]. **Survey** [ZMS22, ABK22, Den08, FSG⁺14, HGH23, JK22, MD23a, TSZ22, UBK23]. **surveys** [AAM23, Ano22]. **suspect** [GBG18]. **swarm** [KKK17, PV22, TGNA22]. **swarms** [SS17]. **switching** [SHW23]. **symbolic** [BHKM23, BMV05, BFT08]. **Symmetric** [BPW05b, Bra22, HK19, MRG23]. **Symposium** [BJ15]. **Sysmon** [SKB23]. **System** [JTV19, ATS23, AMZ22, ABFO08, Alg22, AZ22, Ano11b, BLS⁺23, BEd23, BFP03, BFPP07, BR23, BS21, BSV22, BCGL23, CL08, CZ06, DJN10, EZLC21, FAMMZ23, GLMS19, Ham23, IZS08, KO02, KJS17, KBY22, LKH09, LCL14, MGV17, Man21, MK21, ME23, MFES04, MS15, PGMPPC22, PV22, RM12, RLEM18, RBEH15, SBS23, SBD23, SRK⁺20, SSD14, SSJ22, TS20, VL13, YAY⁺21, ZWX20, ZTG22, vORM06, DNF⁺19]. **System-assigned** [JTV19]. **system-based** [EZLC21, MGV17]. **Systematic** [VMCR23, ATS23, OAJ23, SAC22, SK16, TS22]. **systems** [ASF04, AK23, AMRR17, BDHZ15, BHZ⁺21, BB04a, BCF⁺17, BKMR08, CK23b, DSRHC16, GMH14, GMLM23, HZL⁺17, Hub12, JAYZ21, LVK18, LLH21, LWL23, LV10, MB23, OAJ23, PCK22b, RSPMB16, Roe11a, SK16, SV11, SS05a, SDR20, SB22, TBGB20, ZGC07, ZGRS23, dAKdG10, CK23a, Roe11b]. **table** [PD21]. **TabNet** [CLG23]. **Tacit** [JTV19]. **tag** [EMRN17]. **tagging** [GP17]. **tags** [ACH013, ALOW15, LL21]. **taint** [IKS22]. **Taking** [BRS06, KNL16]. **tallying** [MMS16]. **Talos** [CMN⁺18]. **tamper** [GMSS23]. **tamper-evident** [GMSS23]. **tampering** [DTK⁺18]. **target** [BB22, BHZ⁺21, HXTP23]. **targeted**

[GBG18, KOSU16, MLCQ21, UBK23]. **task** [Yon18]. **task-PIOAs** [Yon18]. **taxonomies** [RB23]. **taxonomy** [CSL+23]. **TCP** [FZ21]. **TCP/UDP** [FZ21]. **TCP/UDP-based** [FZ21]. **technical** [GMdFLR23]. **technique** [GLP03, Rov23, SSVC16, WT21]. **Techniques** [TG05, BMP+14, CH16, KK22, KA18, LSR+23, MI22, OAJ23, SMMN12, SSE+15, ZMS22]. **technologies** [KBH07, SAT09, YSD+20]. **technology** [LH15, SSV22, VMCR23]. **telecare** [LLH21]. **telemetry** [NBA+21]. **telemetry-enabled** [NBA+21]. **telephony** [AMRR17, BABB16]. **tell** [MBHT17]. **templates** [CC10, HTM11]. **temporal** [AVM23, DA21, SBD23, SKK+17, TS20]. **Temporarily** [GSS10]. **TENET** [TCE23]. **term** [ZKP+23]. **TermID** [KKK17]. **terms** [MUIH+21]. **test** [LLBL18]. **testbed** [RM12]. **testing** [ANN23, AV17]. **tests** [CSL+23]. **text** [ZSN23]. **their** [Auf20, HSMY12, KAC17, PNG+20, SB22, WGMB13]. **theoretic** [LVK18, PNG+20]. **theoretical** [BCEM04]. **theoretically** [TND+15]. **Theory** [Rus04, CG23]. **theory-based** [CG23]. **there** [ACS21]. **Things** [Ham23]. **third** [CAS22, KPM12]. **third-party** [CAS22]. **threat** [ASA23, AG23, Auf20, GMLM23, IOU+21, MdSC+15, MPP21, PAI+23, RV19, SBCP21, Sep23, SHOL23, YP12, YA22]. **threat-informed** [AG23]. **threats** [ACT23, SAH22, VSN22]. **three** [LCL16, NSNK06, Nui12, AGZA22]. **Three-factor** [AGZA22]. **three-party** [LCL16]. **three-round** [NSNK06]. **Threshold** [Pen12, WMS+19, BCD+13, HKO22, JSMG18b, QDW09]. **Thresholdizing** [BST21]. **ThunderSecure** [GDA22]. **Time** [KME+16, BDG21, CK23b, CJMS19, DMDD16, GDA22, GGP21, KKK22b, KCB17, LLBL18, LKH09, LBW05, MUIH+21, NAM06, PD21, RB23, SBS23, SKH+23, Vaj16, CK23a]. **time-aware** [Vaj16]. **time-based** [LKH09, NAM06]. **time-memory** [CJMS19]. **Time-specific** [KME+16]. **Timed** [BKBB20, BBB20, GLMS+04]. **timing** [DHW11, KK17]. **TLS** [BJ16]. **TLS-** [BJ16]. **TLS-/SSL-protected** [BJ16]. **Token** [GTM11]. **Token-based** [GTM11]. **tokenization** [DSRHC16]. **tolerance** [CL09, SSD14]. **tolerant** [GKS19, RBD02]. **toll** [BSV22]. **tool** [KK22, SB09, SKB23, VSN22]. **tools** [AV17]. **top** [SCL+18]. **top-level** [SCL+18]. **Topology** [ZXZ22]. **Topology-hiding** [ZXZ22]. **Tor** [ZD22]. **toys** [Yan21]. **trace** [NP10]. **traceable** [ACHO13, Man21, SK14]. **traceback** [RS18]. **tracing** [DdP13, LCL14, Roe11a, Roe11b]. **Track** [Ano22, BJ15, DFF+16]. **Tracking** [ZJS22]. **trade** [CJMS19]. **trade-off** [CJMS19]. **tradeoff** [SSN15]. **traditional** [GLP03]. **traffic** [ABK22, JJJ21, PAI+23, RSV23, SBS23, SPDR17, ZHZ22]. **train** [JAYZ21]. **training** [CG23, GSAMCA18, KMMG23]. **transactions** [BLS+23, CMS10, FYF22, PSDSNAHJ19, SK06]. **transform** [KCM+15, SJ10, ZMS22]. **Transformational** [KM07]. **transformations** [BZV05, BDF04]. **Transforms** [MTW+14]. **transition** [BKMR08]. **transparent** [SVKV21]. **trapdoor** [ACHO13]. **TRBAC** [BKBB20, BBB20]. **tree** [ABR16, BDPV14, DRPW12, MFES04, PHS22]. **trees** [KB13, RBD02]. **Trends** [AAM23, TDGL23]. **triage** [TBGB20]. **triangle** [LCL16]. **Trojan** [BSCZ11]. **truly** [BR18]. **Trust** [BE23, KN07, Abb13, Alg22, FFG20, FFBGEM21, GMMZ06, KBH07, LD07, LLWY09, LV10, QLOW09, RSPMB16, SHA20, WW07, ZGC07]. **trust-aware** [Alg22]. **TrUStAPIS** [FFG20]. **Trusted** [LH15, CKW19, KBJ22]. **trustworthy** [MBRPS18]. **truth** [AvO13]. **TTP** [ZBD06]. **TTS** [DSY06]. **Tuning** [GNS14]. **turnkey**

[SKB23]. **TV** [Roe11b, DZW⁺¹⁸, Roe11a]. **twice** [YOV09]. **Two** [LTC23, MR04, ML17, CG14, GNS14, MS09, MG23, SSFB15]. **two-channel** [MS09]. **Two-factor** [ML17, CG14]. **two-level** [MG23]. **Two-model** [LTC23]. **Two-party** [MR04]. **two-round** [GNS14]. **type** [EZLC21, FN19]. **typing** [DM07, KM07]. **typology** [DWU⁺²³, RB23].

ubiquitous [LI07]. **UC** [BP08]. **UDP-based** [FZ21]. **UMTS** [LSWW14]. **UMTS/LTE** [LSWW14]. **unauthorized** [YP12]. **Uncertain** [AJC⁺⁰⁹]. **uncertainty** [SdHZ16]. **unclonable** [AGZA22, BR17, KKY⁺²³, SM10]. **uncovering** [VSN22]. **undergraduates** [AHX⁺²³]. **Understanding** [LM06, MS15, RSPMB16, WGMB13, YL19]. **undetectable** [VHT09]. **unforgeability** [Hal20, Yon18]. **unification** [KM07]. **unified** [GA23]. **uniform** [KAC16]. **unifying** [BCD⁺¹³]. **unit** [BHKM23]. **unit-based** [BHKM23]. **universal** [AKT23, HSMW08, Vaj16, ZWX20, ZXZ22, Dan07]. **unknown** [BEPL⁺¹⁷]. **unlinkable** [BSV22]. **Unlock** [IS23]. **unlocking** [IS23]. **unmanaged** [KKKV07]. **Unpicking** [DFF⁺¹⁶]. **untrusted** [GW09]. **updatable** [ABR16, AKMW20]. **update** [JSMG18a, YL20]. **updates** [AKMW20]. **uploaders** [WMS⁺¹⁹]. **URL** [KCM⁺¹⁵]. **usability** [MD23b]. **Usage** [LMMS17, SF17, YA22]. **use** [LMMO04, Pla09, SK06, SS05b]. **use-based** [SS05b]. **useful** [DHS04]. **User** [AAZAA23, CFBvO09, CLPP11, Hal20, BFG⁺¹³, CON09, IS23, MGV17, MTSH18, MD23b, PGMLK⁺¹³, XSA13, YL19]. **user-controlled** [BFG⁺¹³]. **User-friendly** [CLPP11]. **User-mediated** [Hal20]. **users** [AZ22, CF07, KOSU16, KB23, YM19, YA22]. **uses** [GAdFGM23]. **Using** [BBB20, GBG18, HTM11, RBD02, SJ10, Sen14, STD21, TZH04, AMZ22, AGZA22, ACB14, AAZAA23, AMLH18, AuHD⁺²³, AFA⁺²³, AG23, AGIK07, AHC⁺²¹, AVM23, AICC18, ACBC⁺¹⁵, BEY23, BMP⁺¹⁴, BCL13, BDMM19, BS22, BCGL23, BDG23, CAS22, CLW⁺¹¹, CF07, DGF⁺¹⁷, EWR⁺⁰⁹, GKKT10, GGJ22, GSAMCA18, GBDJ14, GKBS12, HLKI15, HCN15, HL04, IDHRPCMP15, JCL⁺¹⁸, KK22, KJS17, KA18, KIP22, KSM10, KCC⁺²³, LL22, LM06, LWL⁺²¹, MB16, MARK20, MSKD16, MP15, MLYL20, MP16, MLCS16, MD23b, NCBG23, OBH⁺²⁰, PMDS23, PKHS23, PM23, PV22, PBI⁺²³, QLZH15, RHL17, RSV23, RT23, RRI⁺¹⁹, SBS23, SSFB15, SBD23, SSD14, SGSS23, SSL22b, SSV22, SKH⁺²³, TBGB20, TKKO20, VH19, WGH23, Yon18, You06, ZP23, ZBC23, ZLJW20, ZMS22, vOLW05, BKBB20]. **utilising** [LCPD14]. **utilities** [DA21]. **utility** [CR20, GGP21]. **utilized** [IKS22]. **utilizing** [ZSN23].

validating [BS22]. **validation** [AGIK07, ZBD06, dAKdG10]. **valley** [Auf20]. **Value** [IKS22]. **Value-utilized** [IKS22]. **VANET** [AaBZS23, YWW22]. **variants** [BCD⁺¹³]. **variation** [LNX22]. **various** [TS22]. **Vaudenay** [Tip22]. **vector** [MMS16, MLCS16]. **vector-based** [MMS16]. **vehicle** [ACT23]. **vehicular** [LH23, MG19, MB16, SF17]. **verifiability** [ZWX20]. **Verifiable** [NSNK06, AFA⁺²³, KU16, LZQ⁺¹⁸, PCK22a]. **Verifiably** [WPD18, KJ14, SEXY18]. **verification** [BMP05, CKW19, CL13, DS07, GMH14, Pen12, Pen13, Yon18, Zha23]. **verifier** [HSMW08, HYWS11, RSD19]. **VERIFY** [ACM05]. **Verifying** [MP15]. **version** [AKT23, SBD23]. **versus** [Bra22, LSR⁺²³, MTSH18]. **very** [Bae10]. **via** [AaBZS23, IOU⁺²¹, MTSH18, MS14, ZHZ22]. **victims** [CMN⁺¹⁸]. **video**

[LcSCL⁺18, MBRPS18, RSPMB16, SB14].
View [MD23b]. **views** [KMR09]. **violation** [GYL⁺07]. **virtual** [PDM20, RM12, SHW23]. **visible** [LC04].
Visualization [XSA13, JJJ21, YL19].
Visualization-based [XSA13]. **visualized** [HLKI15]. **visualizing** [SBCP21]. **visually** [KB23]. **VM** [PDM20]. **voice** [WAB⁺09].
VoIP [VL13]. **voltage** [MPG21]. **volumes** [SMMN12]. **voting** [DJN10, GP23, MMS16, MS11, Pen11, ZWX20, ZLJW20].
vulnerabilities [BHKM23, DTK⁺18, SNX19, YNC22].
vulnerability [AV17, JM17, KKK22a, MLM19, MP22, ZRJ14, EZLC21].

wallet [FTS⁺20]. **warning** [ABFL12].
Waste [SSM⁺20]. **Watermarking** [Fra18, BMP⁺14]. **wavelet** [KCM⁺15].
weaknesses [DDZ22]. **wearable** [SAC22, SDR20]. **Web** [EZ22, AYHK18, ANN23, AV17, DTK⁺18, GLMS⁺04, LL22, MSKD16, PM23, RSV23, SGLC19, SCO21, TSMH19, ZD22, BFP03, BJ16, EWR⁺09, IOU⁺21, KGG09, SNX19].
web-based [AYHK18]. **webshell** [HNHY23]. **website** [NCBG23]. **WebView** [IOU⁺21]. **weighted** [Sen14]. **wildcard** [CKS21, HH16]. **WinRAR** [YP06].
Wireless [BT07, CMR06, CBC08, EHM15, EMRN17, KKK17, LBZ⁺10, MARK20, RBEH15, SS17, SSN15, YRW14, ZXZ⁺11].
Wirelessly [GdKGV14]. **within** [KCB20].
without [GW09, HSMW08, HYWS11, HYWS12, SXZC20, YSM10, ZXZ22].
workflow [ARMLS06]. **working** [AHX⁺23].
workplace [Lev07]. **world** [TSZ22, ZD22].
worm [AGIK07, KJG⁺11]. **worms** [vORM06]. **wrinkle** [BDG21]. **Write** [LD17, JTV19]. **Write-only** [LD17].

X.509 [ZJS22]. **XACML** [CON09, RRI⁺19].
Xen [PPL15]. **Xen-based** [PPL15]. **XML** [BFPP07, CF03, KMR09]. **XOR**

[BP08, BGP07b]. **XQuery** [DTK⁺18].
XTEA [Lu09].

Yao [BPW05b, BP08]. **Yao-style** [BPW05b, BP08]. **yoking** [HLS18].

Zephyrus [GAdFGM23]. **zero** [DGF⁺17, PSDSNAHJ19, SLGP23, WCS20].
zero-confirmation [PSDSNAHJ19]. **zero-day** [DGF⁺17, SLGP23]. **zero-knowledge** [WCS20]. **zero-shot** [SLGP23]. **Zheng** [BZ03]. **ZombieCoin** [AMLH18].

References

Alzaidi:2020:DHP

[AAB20]

Areej Alzaidi, Suhair Alshehri, and Seyed M. Buhari. DroidRista: a highly precise static data flow analysis framework for Android applications. *International Journal of Information Security*, 19(5): 523–536, October 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00471-w>.

Al-ani:2023:PSI

[AaBZS23]

Ruqayah Al-ani, Thar Baker, Bo Zhou, and Qi Shi. Privacy and safety improvement of VANET data via a safety-related privacy scheme. *International Journal of Information Security*, 22(4): 763–783, August 2023. CODEN ????? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00662-6>.
- [AAM23] **Ahmad:2023:TPB**
Hira Ahmad, Muhammad Ahtazaz Ahsan, and Adnan Noor Mian. Trends in publishing blockchain surveys: a bibliometric perspective. *International Journal of Information Security*, 22(2):511–523, April 2023. [AB22] CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00653-z>.
- [AAV22] **Abdussami:2022:LLA**
Mohammad Abdussami, Ruhul Amin, and Satyanarayana Vollala. LASSI: a lightweight authenticated key agreement protocol for fog-enabled IoT deployment. *International Journal of Information Security*, 21(6):1373–1387, December 2022. [Abb13] CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00619-1>.
- [AAZAA23] **Alawneh:2023:UIU**
Luay Alawneh, Mohammad Al-Zinati, and Mahmoud Al-Ayyoub. User identification using deep learning and human activity mobile sensor data. *International Journal of Information Security*, 22(1):289–301, February 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00640-4>.
- Agostini:2022:BBM**
E. Agostini and M. Bernaschi. BitCracker: BitLocker meets GPUs. *International Journal of Information Security*, 21(5):1005–1018, October 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00589-4>.
- Abbadi:2013:FET**
Imad M. Abbadi. A framework for establishing trust in cloud provenance. *International Journal of Information Security*, 12(2):111–128, April 2013. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0179-0>.
- Aliasgari:2017:SCH**
Mehrdad Aliasgari, Ma-

- rina Blanton, and Fattaneh Bayatbabolghani. Secure computation of hidden Markov models and secure floating-point arithmetic in the malicious model. *International Journal of Information Security*, 16(6): 577–601, November 2017. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0350-0>. [ABFO08]
- Alfaro:2008:CAC**
- [ABCC08] J. G. Alfaro, N. Boulahia-Cuppens, and F. Cuppens. Complete analysis of configuration rules to guarantee reliable network security policies. *International Journal of Information Security*, 7(2):103–122, April 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0045-7>. [ABK22]
- Ates:2012:WHI**
- [ABFL12] Mikaël Ates, Francesco Buccafurri, Jacques Fayolle, and Gianluca Lax. A warning on how to implement anonymous credential protocols into the information card framework. *International Journal of Information Security*, 11(1):33–40, February 2012. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0150-5>. [Aimeur:2008:LPP]
- Esmā Aïmeur, Gilles Brassard, José M. Fernandez, and Flavien Serge Mani Onana. ALAMBIC: a privacy-preserving recommender system for electronic commerce. *International Journal of Information Security*, 7(5): 307–334, October 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0049-3>. [Agrawal:2022:SAE]
- Ankit Agrawal, Ashutosh Bhatia, and Rekha Kaushik. A survey on analyzing encrypted network traffic of mobile devices. *International Journal of Information Security*, 21(4): 873–915, August 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00581-y>. [Andreeva:2012:SAS]
- Elena Andreeva, Andrey Bogdanov, Bart Mennink,

- Bart Preneel, and Christian Rechberger. On security arguments of the second round SHA-3 candidates. *International Journal of Information Security*, 11(2):103–120, April 2012. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0156-7>. [AC08]
- [ABN14] Aiiad Albeshri, Colin Boyd, and Juan González Nieto. Enhanced Geo-Proof: improved geographic assurance for data in the cloud. *International Journal of Information Security*, 13(2):191–198, April 2014. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0217-6>. [ACB14]
- [ABR16] Tarek Abbes, Adel Bouhoula, and Michaël Rusinowitch. Detection of firewall configuration errors with updatable tree. *International Journal of Information Security*, 15(3):301–317, June 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0290-0>. [Armando:2008:SBM]
- Alessandro Armando and Luca Compagna. SAT-based model-checking for security protocols analysis. *International Journal of Information Security*, 7(1):3–32, January 2008. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0041-y>. [Alabrah:2014:ESC]
- Amerah Alabrah, Jeffrey Cashion, and Mostafa Bassiouni. Enhancing security of cookie-based sessions in mobile networks using sparse caching. *International Journal of Information Security*, 13(4):355–366, August 2014. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0223-8>. [Azkia:2015:DPA]
- Hanieh Azkia, Nora Cuppens, Boulahia, Frédéric Cuppens, Gouenou Coatrieux, and Said Oulmakhzoune. Deployment of a posteriori access control using IHE ATNA. *International Journal of In-*

- formation Security*, 14(5): 471–483, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0265-6>.
- [ACF17] **Albertini:2017:EAC**
Davide Alberto Albertini, Barbara Carminati, and Elena Ferrari. An extended access control mechanism exploiting data dependencies. *International Journal of Information Security*, 16(1):75–89, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0322-4>.
- [ACHO13] **Abe:2013:DTA**
Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo. Double-trapdoor anonymous tags for traceable signatures. *International Journal of Information Security*, 12(1):19–31, February 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0184-3>.
- [ACM05] **Autexier:2005:PSI**
Serge Autexier, Iliano Cervesato, and Heiko Mantel. Preface to the special issue of selected papers from FCS/VERIFY 2002. *International Journal of Information Security*, 4(1–2):1, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0053-9>; <http://link.springer.com/content/pdf/10.1007/s10207-004-0053-9.pdf>.
- [ACMV15] **Armando:2015:FMA**
Alessandro Armando, Gabriele Costa, Alessio Merlo, and Luca Verderame. Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security*, 14(2):123–140, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0252-y>.
- [ACS21] **Alecakir:2021:ATI**
Huseyin Alecakir, Burcu Can, and Sevil Sen. Attention: there is an inconsistency between Android permissions and application metadata! *International Journal of Information Security*, 20(6):

- 797–815, December 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00536-1>.
- [ACT23] **Alcaraz:2023:OST**
Cristina Alcaraz, Jesus Cumplido, and Alicia Triviño. OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security*, 22(5):1395–1421, October 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00698-8>.
- [AD08] **Aldini:2008:EMI**
Alessandro Aldini and Alessandra Di Pierro. Estimating the maximum information leakage. *International Journal of Information Security*, 7(3): 219–242, June 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0050-x>.
- [AFA⁺23] **Alzahrani:2023:DAC**
Bander Alzahrani, Nikos Fotiou, Aiiad Albeshri, Abdullah Almuhaimeed, and Khalid Alsubhi. Distributed access control for information-centric networking architectures using verifiable credentials. *International Journal of Information Security*, 22(2):467–478, April 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00649-9>.
- [AG23] **Amro:2023:CRM**
Ahmed Amro and Vasileios Gkioulos. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security*, 22(1):249–288, February 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00638-y>.
- [AGIK07] **Anagnostakis:2007:CDR**
Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. COVERAGE: detecting and reacting to worm epidemics using cooperation and validation. *International Journal of Information Security*, 6(6):361–378, October 2007. CODEN ????. ISSN 1615-5262 (print), 1615-

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0032-z>. [AHX+23]
- [AGZA22] Ilyes Ahmim, Nacira Ghoulmi-Zine, and Marwa Ahmim. Security analysis on “Three-factor authentication protocol using physical unclonable function for IoV”. *International Journal of Information Security*, 21(5): 1019–1026, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00595-6>. [Ahmim:2022:SAT]
- [AHC+21] Leonardo Aniello, Basel Halak, Peter Chai, Riddhi Dhall, Mircea Mihalea, and Adrian Wilczynski. Anti-BIUFF: towards counterfeits mitigation in IC supply chains using blockchain and PUF. *International Journal of Information Security*, 20(3):445–460, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00513-8>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00513-8.pdf>. [AIC+09]
- [Aniello:2021:ABT] [AICC18] Leonardo Aniello, Basel Halak, Peter Chai, Riddhi Dhall, Mircea Mihalea, and Adrian Wilczynski. Anti-BIUFF: towards counterfeits mitigation in IC supply chains using blockchain and PUF. *International Journal of Information Security*, 20(3):445–460, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00513-8>. [Aniello:2021:ABT]
- [An:2023:HEL] Qin An, Wilson Cheong Hin Hong, XiaoShu Xu, Yunfeng Zhang, and Kimberly Kolletar-Zhu. How education level influences Internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, 22(2):305–317, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00637-z>. [An:2023:HEL]
- [Ayed:2018:ADS] Samiha Ayed, Muhammad Sabir Idrees, Nora Cuppens, and Frederic Cuppens. Achieving dynamicity in security policies enforcement using aspects. *International Journal of Information Security*, 17(1): 83–103, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0357-6>. [Ayed:2018:ADS]
- [An:2009:UIC] Xiangdong An, Dawn Jutla, Nick Cercone, Charyote Pluempitiwiriyaewej,

- and Hai Wang. Uncertain inference control in privacy protection. *International Journal of Information Security*, 8(6): 423–431, December 2009. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0088-z>. [AKMW20]
- [AK23] Aida Akbarzadeh and Sokratis K. Katsikas. Dependency-based security risk assessment for cyber-physical systems. *International Journal of Information Security*, 22(3):563–578, June 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00608-4>. [AKT23]
- [AKG16] Marios Anagnostopoulos, Georgios Kambourakis, and Stefanos Gritzalis. New facets of mobile botnet: architecture and evaluation. *International Journal of Information Security*, 15(5): 455–473, October 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0310-0>. [AKZM20]
- Anada:2020:KUP**
Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki, and Yohei Watanabe. Key-updatable public-key encryption with keyword search (or: How to realize PEKS with efficient key updates for IoT environments). *International Journal of Information Security*, 19(1):15–38, February 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00441-2>.
- Andriotis:2023:BDU**
Panagiotis Andriotis, Myles Kirby, and Atsuhiko Takasu. Bu-Dash: a universal and dynamic graphical password scheme (extended version). *International Journal of Information Security*, 22(2):381–401, April 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00642-2>.
- Adepu:2020:ASG**
Sridhar Adepu, Nandha Kumar Kandasamy, Jianying Zhou, and Aditya Mathur. Attacks on smart grid: power supply interruption

- and malicious power generation. *International Journal of Information Security*, 19(2):189–211, April 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00452-z>.
- [AL05] Mikhail J. Atallah and Jiangtao Li. Secure outsourcing of sequence comparisons. *International Journal of Information Security*, 4(4):277–287, October 2005. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0070-3>.
- [Ala17] Janaka Alawatugoda. Generic construction of an eCK-secure key exchange protocol in the standard model. *International Journal of Information Security*, 16(5):541–557, October 2017. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0346-9>.
- [Alg22] Saleh A. Alghamdi. Novel trust-aware intrusion de-
- tection and prevention system for 5G MANET-Cloud. *International Journal of Information Security*, 21(3):469–488, June 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00531-6>.
- [ALOW15] Alex Arbit, Yoel Livne, Yossef Oren, and Avishai Wool. Implementing public-key cryptography on passive RFID tags is practical. *International Journal of Information Security*, 14(1):85–99, February 2015. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0236-y>.
- [ALPW13] Hassan Jameel Asghar, Shujun Li, Josef Pieprzyk, and Huaxiong Wang. Cryptanalysis of the convex hull click human identification protocol. *International Journal of Information Security*, 12(2):83–96, April 2013. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0161-x>.

- [AM23] **Ahmad:2023:PCS**
 Suhail Ahmad and Ajaz Hus-
 sain Mir. Protection
 of centralized SDN con-
 trol plane from high-rate
 Packet-In messages. *In-*
ternational Journal of In-
formation Security, 22(5):
 1197–1206, October 2023.
 CODEN ???? ISSN
 1615-5262 (print), 1615-
 5270 (electronic). URL
[https://link.springer.
 com/article/10.1007/s10207-](https://link.springer.com/article/10.1007/s10207-023-00685-z)
 023-00685-z.
- [AMRR17] **Arapinis:2017:APM**
 Myrto Arapinis, Loretta Ilaria
 Mancini, Eike Ritter, and
 Mark Dermot Ryan. Anal-
 ysis of privacy in mobile
 telephony systems. *In-*
ternational Journal of In-
formation Security, 16(5):
 491–523, October 2017.
 CODEN ???? ISSN
 1615-5262 (print), 1615-
 5270 (electronic). URL
[http://link.springer.
 com/article/10.1007/s10207-](http://link.springer.com/article/10.1007/s10207-016-0338-9)
 016-0338-9; [http://
 link.springer.com/content/
 pdf/10.1007/s10207-016-](http://link.springer.com/content/pdf/10.1007/s10207-016-0338-9.pdf)
 0338-9.pdf.
- [AMRH18] **Ali:2018:ZMN**
 Syed Taha Ali, Patrick
 McCorry, Peter Hyun-
 Jeen Lee, and Feng Hao.
 ZombieCoin 2.0: manag-
 ing next-generation bot-
 nets using Bitcoin. *In-*
ternational Journal of In-
formation Security, 17(4):
 411–422, August 2018.
 CODEN ???? ISSN [AMZ22]
 1615-5262 (print), 1615-
 5270 (electronic). URL
[http://link.springer.
 com/article/10.1007/s10207-](http://link.springer.com/article/10.1007/s10207-017-0379-8)
 017-0379-8.
- [AMP12] **Andreeva:2012:PGF**
 Elena Andreeva, Bart Men-
 nink, and Bart Preneel.
 The parazoa family: gen-
 eralizing the sponge hash
 functions. *International
 Journal of Information Se-*
curity, 11(3):149–165, June
 2012. CODEN ???? ISSN
 1615-5262 (print), 1615-
 5270 (electronic). URL
[https://link.springer.
 com/article/10.1007/s10207-](https://link.springer.com/article/10.1007/s10207-021-00558-3)
 021-00558-3.
- 5270 (electronic). URL
[http://link.springer.
 com/article/10.1007/s10207-](http://link.springer.com/article/10.1007/s10207-012-0157-6)
 012-0157-6.
- Ahmad:2022:EAC**
 Tahir Ahmad, Umberto
 Morelli, and Nicola Zan-
 none. Extending ac-
 cess control in AWS IoT
 through event-driven func-
 tions: an experimental
 evaluation using a smart
 lock system. *Interna-*
tional Journal of Informa-
tion Security, 21(2):379–
 408, April 2022. CO-
 DEN ???? ISSN
 1615-5262 (print), 1615-
 5270 (electronic). URL
[https://link.springer.
 com/article/10.1007/s10207-](https://link.springer.com/article/10.1007/s10207-021-00558-3)
 021-00558-3.

- [ANN23] **Alidoosti:2023:BLC**
 Mitra Alidoosti, Alireza Nowroozi, and Ahmad Nickabadi. Business-layer client-side racer: dynamic security testing of the web application against client-side race condition in the business layer. *International Journal of Information Security*, 22(4): 1029–1054, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00671-5>.
- [Ano14] **Anonymous:2014:SCC**
 Anonymous. Security in cloud computing. *International Journal of Information Security*, 13(2): 95–96, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0232-2>.
- [Ano11a] **Anonymous:2011:P**
 Anonymous. Preface. *International Journal of Information Security*, 10(2): 61, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0134-5>; <http://link.springer.com/content/pdf/10.1007/s10207-011-0134-5.pdf>.
- [Ano11b] **Anonymous:2011:SIS**
 Anonymous. Special issue on “SCADA and control system security”. *International Journal of Information Security*, 10(2):135–136, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0134-5>.
- [Ano22] **Anonymous:2022:TS**
 Anonymous. Track for surveys. *International Journal of Information Security*, 21(1):159, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00546-7>.
- Ahmed:2012:MGE**
 Irfan Ahmed, Martin Naedele, Bradley Schatz, Ryoichi Sasaki, and Andrew West. Message from the guest editors. *International Journal of Information Security*, 11(4): 213, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0054-7>.

- 012-0168-3; <http://link.springer.com/content/pdf/10.1007/s10207-012-0168-3.pdf>.
- [AP22] **Armour:2022:ASA**
 Marcel Armour and Bertram Poettering. Algorithm substitution attacks against receivers. *International Journal of Information Security*, 21(5):1027–1050, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00596-5>. [ASAAS15]
- [ARMLS06] **Al-Riyami:2006:EFE**
 S. S. Al-Riyami, J. Malone-Lee, and N. P. Smart. Escrow-free encryption supporting cryptographic workflow. *International Journal of Information Security*, 5(4):217–229, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0002-x>. [ASF04]
- [ASA23] **Al-Shehari:2023:RRA**
 Taher Al-Shehari and Rakan A. Alsowail. Random resampling algorithms for addressing the imbalanced dataset classes in insider threat detection. *International Journal of Information Security*, 22(3):611–629, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00651-1>. **Al-Saleh:2015:IDC**
 Mohammed I. Al-Saleh, Fatima M. AbuHjeela, and Ziad A. Al-Sharif. Investigating the detection capabilities of antiviruses under concurrent attacks. *International Journal of Information Security*, 14(4):387–396, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0261-x>. **Abie:2004:DDR**
 Habtamu Abie, Pål Spilling, and Bent Foyen. A distributed digital rights management model for secure information-distribution systems. *International Journal of Information Security*, 3(2):113–128, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0058-4>.

- [ASN⁺16] **Almaatouq:2016:IIL** Abdullah Almaatouq, Erez Shmueli, Mariam Nouh, Ahmad Alabdulkareem, Vivek K. Singh, Mansour Alsaleh, Abdulrahman Alarifi, Anas Alfaris, and Alex ‘Sandy’ Pentland. If it looks like a spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts. *International Journal of Information Security*, 15(5): 475–491, October 2016. [AT22] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0321-5>.
- [ASZ⁺23] **Alhaj:2023:EAS** Taqwa Ahmed Alhaj, Maheyzah Md Siraj, Anazida Zainal, Inshirah Idris, Anjum Nazir, Fatin Elhaj, and Tasneem Darwish. An effective attack scenario construction model based on identification of attack steps and stages. *International Journal of Information Security*, 22(5): 1481–1496, October 2023. [Auf20] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00701-2>.
- Adewole:2022:DDL** Kayode S. Adewole and Vicenç Torra. DFTMicroagg: a dual-level anonymization algorithm for smart grid data. *International Journal of Information Security*, 21(6):1299–1321, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00612-8>.
- Abdulganiyu:2023:SLR** Oluwadamilare Harazeem Abdulganiyu, Taha Ait Tchakoucht, and Yakub Kayode Saheed. A systematic literature review for network intrusion detection system (IDS). *International Journal of Information Security*, 22(5): 1125–1162, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00682-2>.
- Aufner:2020:ISG** Peter Aufner. The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, 19(1):3–14, February 2020. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00445-y>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00445-y.pdf>. [AVM23]
- [AuHD⁺23] Muhammad Ali, Mansoor ul Haque, Muhammad Hanif Durad, Anila Usman, Syed Muhammad Mohsin, Hana Mujlid, and Carsten Maple. Effective network intrusion detection using stacking-based ensemble approach. *International Journal of Information Security*, 22(6):1781–1798, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00718-7>. [AvO13]
- [AV17] Nuno Antunes and Marco Vieira. Designing vulnerability testing tools for web services: approach, components, and tools. *International Journal of Information Security*, 16(4):435–457, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0334-0>. [AYHK18]
- Asha:2023:DFD**
S. Asha, P. Vinod, and Varun G. Menon. A defensive framework for deep-fake detection under adversarial settings using temporal and spatial features. *International Journal of Information Security*, 22(5):1371–1382, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00695-x>.
- Alsaleh:2013:EAA**
Mansour Alsaleh and P. C. van Oorschot. Evaluation in the absence of absolute ground truth: toward reliable evaluation methodology for scan detectors. *International Journal of Information Security*, 12(2):97–110, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0178-1>.
- Akiyama:2018:HDC**
Mitsuaki Akiyama, Takeshi Yagi, Takeo Hariu, and Youki Kadobayashi. HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle. *International Journal of*

- Information Security*, 17 (2):135–151, April 2018. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL [BA16] <http://link.springer.com/article/10.1007/s10207-017-0361-5>; <http://link.springer.com/content/pdf/10.1007/s10207-017-0361-5.pdf>.
- [AZ19] **Aamir:2019:DAD**
 Muhammad Aamir and Syed Mustafa Ali Zaidi. DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. *International Journal of Information Security*, 18(6):761–785, December 2019. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL [BAB23] <http://link.springer.com/article/10.1007/s10207-019-00434-1>.
- [AZ22] **Amraoui:2022:ABD**
 Nouredine Amraoui and Belhassen Zouari. Anomalous behavior detection-based approach for authenticating smart home system users. *International Journal of Information Security*, 21(3):611–636, June 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL [BABB16] <https://link.springer.com/article/10.1007/s10207-022-00639-x>.
- Blanton:2016:POS**
 Marina Blanton and Everaldo Aguiar. Private and oblivious set and multiset operations. *International Journal of Information Security*, 15(5):493–518, October 2016. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0301-1>.
- Bilgen:2023:AEA**
 Melike Burakgazi Bilgen, Osman Abul, and Kemal Bicakci. Authentication-enabled attribute-based access control for smart homes. *International Journal of Information Security*, 22(2):479–495, April 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00639-x>.
- Chikha:2016:BBA**
 Randa Jabeur Ben Chikha, Tarek Abbes, Wassim Ben Chikha, and Adel Bouhoula. Behavior-based approach to detect spam over IP telephony attacks. *International Journal of Information Security*, 15(2):131–143, April 2016.

- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0281-1>.
- [Bae10] **Baek:2010:RAR** Yoo-Jin Baek. Regular 2^w -ary right-to-left exponentiation algorithm with very efficient DPA and FA countermeasures. *International Journal of Information Security*, 9(5):363–370, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0118-x>.
- [BB04a] **Biskup:2004:CQE** Joachim Biskup and Piero Bonatti. Controlled query evaluation for enforcing confidentiality in complete information systems. *International Journal of Information Security*, 3(1):14–27, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0032-1>.
- [BB04b] **Blakley:2004:ASN** B. Blakley and G. R. Blakley. All sail, no anchor II: Acceptable high-end PKI. *International Journal of Information Security*, 2(2):66–77, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0029-1>.
- [BB22] **Bajic:2022:ABN** Alexander Bajic and Georg T. Becker. Automated benchmark network diversification for realistic attack simulation with application to moving target defense. *International Journal of Information Security*, 21(2):253–278, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00552-9>.
- [BBB20] **BenAttia:2020:UHT** Hasiba Ben Attia, Laid Kahloul Saber Benharzallah, and Samir Bourekkache. Using hierarchical timed coloured Petri nets in the formal study of TRBAC security policies. *International Journal of Information Security*, 19(2):163–187, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00448-9>. See author name correction [BKBB20].

- [BBR18] **Bindel:2018:CAA**
 Nina Bindel, Johannes Buchmann, and Susanne Rieß. Comparing apples with apples: performance analysis of lattice-based authenticated key exchange protocols. *International Journal of Information Security*, 17(6): 701–718, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0397-6>. [BCEM04]
- [BCA⁺10] **Bayly:2010:FBS**
 Duncan Bayly, Maurice Castro, Arathi Arakala, Jason Jeffers, and Kathy Horadam. Fractional biometrics: safeguarding privacy in biometric applications. *International Journal of Information Security*, 9(1):69–82, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0096-z>. [BCF⁺17]
- [BCD⁺13] **Bresson:2013:LLS**
 Emmanuel Bresson, Dario Catalano, Mario Di Raimondo, Dario Fiore, and Rosario Gennaro. Offline/on-line signatures revisited: a general unifying paradigm, efficient threshold variants and experimental results. *International Journal of Information Security*, 12(6): 439–465, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0200-2>. [Burgess:2004:GTM]
- Mark Burgess, Geoffrey Canright, and Kenth Engø-Monsen. A graph-theoretical model of computer security. *International Journal of Information Security*, 3(2):70–85, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0044-x>. [Boyd:2017:AAK]
- Colin Boyd, Cas Cremers, Michèle Feltz, Kenneth G. Paterson, Bertram Poettering, and Douglas Stebila. ASICS: authenticated key exchange security incorporating certification systems. *International Journal of Information Security*, 16(2):151–171, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0044-x>.

- com/article/10.1007/s10207-015-0312-y.
- [BCGL23] **Bowen:2023:BHD**
 Brandon Bowen, Anitha Chennamaneni, Ana Goulart, and Daisy Lin. BLoC-Net: a hybrid, dataset-independent intrusion detection system using deep learning. *International Journal of Information Security*, 22(4):893–917, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00663-5>. [BCL13]
- [BCJ+11] **Backes:2011:CSS**
 Michael Backes, Iliano Cervesato, Aaron D. Jagard, Andre Scedrov, and Joe-Kai Tsay. Cryptographically sound security proofs for basic and public-key Kerberos. *International Journal of Information Security*, 10(2):107–134, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0125-6>. [BDD01]
- [BCL09] **Brickell:2009:SSN**
 Ernie Brickell, Liqun Chen, and Jiangtao Li. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings. *International Journal of Information Security*, 8(5):315–330, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0076-3>. [Beauquier:2013:SPE]
- Danièle Beauquier, Joëlle Cohen, and Ruggero Lanotte. Security policies enforcement using finite and pushdown edit automata. *International Journal of Information Security*, 12(4):319–336, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0195-8>. [Blundo:2001:PDI]
- Carlo Blundo, Paolo D’Arco, and Alfredo De Santis. A t -private k -database information retrieval scheme. *International Journal of Information Security*, 1(1):64–68, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100005>.

- [BDF04] **Bartoletti:2004:SIS**
 Massimo Bartoletti, Pierpaolo Degano, and Gian Luigi Ferrari. Stack inspection and secure program transformations. *International Journal of Information Security*, 2(3-4):187–217, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0038-8>.
- [BDG21] **Berger:2021:WTC**
 Harel Berger, Amit Z. Dvir, and Moti Geva. A wrinkle in time: a case study in DNS poisoning. *International Journal of Information Security*, 20(3):313–329, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00502-x>.
- [BDG23] **Brama:2023:ENN**
 Haya Brama, Lih Dery, and Tal Grinshpoun. Evaluation of neural networks defenses and attacks using NDCG and reciprocal rank metrics. *International Journal of Information Security*, 22(2):525–540, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00652-0>.
- [BDH⁺10] **Buhan:2010:ERC**
 Ileana Buhan, Jeroen Doumen, Pieter Hartel, Qian Tang, and Raymond Veldhuis. Embedding renewable cryptographic keys into noisy data. *International Journal of Information Security*, 9(3):193–208, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0103-4>.
- [BDHK08] **Backes:2008:CRS**
 Michael Backes, Markus Dürmuth, Dennis Hofheinz, and Ralf Küsters. Conditional reactive simulatability. *International Journal of Information Security*, 7(2):155–169, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0046-6>.
- [BDHZ15] **Bertino:2015:SPE**
 Elisa Bertino, Robert H. Deng, Xinyi Huang, and Jianying Zhou. Security and privacy of electronic health information systems. *Internation*

- tional Journal of Information Security*, 14(6): 485–486, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0303-z>; <http://link.springer.com/content/pdf/10.1007/s10207-015-0303-z.pdf>. [BE_d23]
- [BDMM19] Mario Luca Bernardi, Marta Cimitile Damiano Distante, Fabio Martinelli, and Francesco Mercaldo. Dynamic malware detection and phylogeny analysis using process mining. *International Journal of Information Security*, 18(3):257–284, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0415-3>. [Bel10]
- [BDPV14] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sufficient conditions for sound tree and sequential hashing modes. *International Journal of Information Security*, 13(4):335–353, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0220-y>. [Barhoun:2023:TMD]
- Rabie Barhoun and Maryam Ed-daibouni. Trust modeling in a distributed collaborative environment: application to a collaborative healthcare system. *International Journal of Information Security*, 22(6):1585–1604, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00707-w>. [Bella:2010:PGA]
- Giampaolo Bella. The principle of guarantee availability for security protocol analysis. *International Journal of Information Security*, 9(2):83–97, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0097-y>. [Bat-Erdene:2017:EAC]
- Munkhbayar Bat-Erdene, Hyundo Park, Hongzhe Li, Heejo Lee, and Mahn-Soo Choi. Entropy analysis to classify unknown packing algorithms for malware detection. *International Journal of Information Security*, 16(3):227–248, June

2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0330-4>.
- [BEY23] Ahmed Fraz Baig, Sigurd Eskeland, and Bian Yang. Privacy-preserving continuous authentication using behavioral biometrics. *International Journal of Information Security*, 22(6):1833–1847, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00721-y>.
- [BF13] Daniel Boteanu and José M. Fernandez. A comprehensive study of queue management as a DoS counter-measure. *International Journal of Information Security*, 12(5): 347–382, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0197-6>.
- [BFG⁺13] D. Bernhard, G. Fuchs-bauer, E. Ghadafi, N. P. Smart, and B. Warinschi. Anonymous attes-
- tation with user-controlled linkability. *International Journal of Information Security*, 12(3):219–249, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0191-z>.
- [BFP03] Elisa Bertino, Elena Ferrari, and Andrea Peregó. Content-based filtering of Web documents: the MaX system and the EUFOR-BIA project. *International Journal of Information Security*, 2(1): 45–58, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0024-6>.
- [BFPP07] Elisa Bertino, Elena Ferrari, Federica Paci, and Loredana Parasiliti Provenza. A system for securing push-based distribution of XML documents. *International Journal of Information Security*, 6(4):255–284, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0020-3>.

- [BFS⁺13] **Brzuska:2013:LMR**
 C. Brzuska, M. Fischlin, N. P. Smart, B. Warinschi, and S. C. Williams. Less is more: relaxed yet composable security notions for key exchange. *International Journal of Information Security*, 12(4):267–297, August 2013. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0192-y>. [BGKZ12]
- [BFT08] **Bracciali:2008:SFM**
 Andrea Bracciali, Gianluigi Ferrari, and Emilio Tosto. A symbolic framework for multi-faceted security protocol analysis. *International Journal of Information Security*, 7(1):55–84, January 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0043-9>. [BGP07a]
- [BGK08] **Balopoulos:2008:SIP**
 Theodoros Balopoulos, Stefanos Gritzalis, and Sokratis K. Katsikas. Specifying and implementing privacy-preserving cryptographic protocols. *International Journal of Information Security*, 7(6):395–420, November 2008. [BGP07b]
- CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0057-y>.
- Bagheri:2012:SFP**
 Nasour Bagheri, Praveen Gauravaram, Lars R. Knudsen, and Erik Zenger. The suffix-free-prefix-free hash function construction and its indiffer-entiability security analysis. *International Journal of Information Security*, 11(6):419–434, November 2012. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0175-4>.
- Backes:2007:P**
 Michael Backes, Stefanos Gritzalis, and Bart Preneel. Preface. *International Journal of Information Security*, 6(6):359–360, October 2007. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0034-x>.
- Blundo:2007:LRC**
 Carlo Blundo, Clemente Galdi, and Giuseppe Persiano. Low-randomness constant-round private XOR

computations. *International Journal of Information Security*, 6(1):15–26, January 2007. CODEN ????. ISSN [BHL+21] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0007-5>.

Ben-Ghorbel-Talbi:2010:DME

[BGTCCBB10] Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Bouhahia, and Adel Bouhoula. A delegation model for extended RBAC. *International Journal of Information Security*, 9(3):209–236, June 2010. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0104-3>. [BHZ+21]

Baradaran:2023:UBS

[BHKM23] Sara Baradaran, Mahdi Heidari, Ali Kamali, and Maryam Mouzarani. A unit-based symbolic execution method for detecting memory corruption vulnerabilities in executable codes. *International Journal of Information Security*, 22(5):1277–1290, October 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL [BJ15] <https://link.springer.com/article/10.1007/s10207-023-00691-1>.

[com/article/10.1007/s10207-023-00691-1](http://link.springer.com/article/10.1007/s10207-023-00691-1).

Benarfa:2021:CED

Abdelmadjid Benarfa, Muhammad Hassan, Eleonora Losiouk, Alberto Compagno, Mohamed Bachir Yagoubi, and Mauro Conti. ChoK-IFA+: an early detection and mitigation approach against interest flooding attacks in NDN. *International Journal of Information Security*, 20(3):269–285, June 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00500-z>.

Bi:2021:MPA

Kun Bi, Dezhi Han, Guichen Zhang, Kuan-Ching Li, and Aniello Castiglione. K maximum probability attack paths generation algorithm for target nodes in networked systems. *International Journal of Information Security*, 20(4):535–551, August 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00517-4>.

Bella:2015:SIS

Giampaolo Bella and Helge Janicke. Special issue

- on the Security Track at the ACM Symposium on Applied Computing 2013. *International Journal of Information Security*, 14(2):101–102, April 2015. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0280-2>; <http://link.springer.com/content/pdf/10.1007/s10207-015-0280-2.pdf>. [BIMR08]
- [BJ16] Christopher W. Brown and Michael Jenkins. Analyzing proposals for improving authentication on the TLS/SSL-protected Web. *International Journal of Information Security*, 15(6):621–635, November 2016. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0316-2>. [BLM11]
- [BKBB20] Hasiba Ben Attia, Laid Kahloul, Saber Benharzallah, and Samir Bourekkache. Correction to: Using Hierarchical Timed Coloured Petri Nets in the formal study of TRBAC security policies. *International Journal of Information Security*, 19(2):241, April 2020. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0138-1>. [BLS⁺23]
- [Brown:2016:API] Christopher W. Brown and Michael Jenkins. Analyzing proposals for improving authentication on the TLS/SSL-protected Web. *International Journal of Information Security*, 15(6):621–635, November 2016. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0316-2>. [BLM11]
- [Bryans:2008:OGT] Jeremy W. Bryans, Maciej Koutny, Laurent Mazaré, and Peter Y. A. Ryan. Opacity generalised to transition systems. *International Journal of Information Security*, 7(6):421–435, November 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0058-x>.
- [Bouzida:2011:CAB] Yacine Bouzida, Luigi Logrippo, and Serge Mankovski. Concrete- and abstract-based access control. *International Journal of Information Security*, 10(4):223–238, August 2011. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0138-1>.
- [Bandara:2023:OPP] Eranga Bandara, Xueping Liang, Sachin Shetty, Ravi Mukkamala, Peter Foytik,

- Nalin Ranasinghe, and Kasun De Zoysa. Octopus: privacy preserving peer-to-peer transactions system with InterPlanetary file system (IPFS). *International Journal of Information Security*, 22(3):591–609, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00650-2>. [BMP05]
- Colin Boyd and Wenbo Mao. Preface to the special issue on ISC 2003. *International Journal of Information Security*, 4(4):227, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0066-4>. [BM05]
- Nataliia Bielova and Fabio Massacci. Do you really mean what you actually enforced? *International Journal of Information Security*, 10(4):239–254, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0137-2>. [BMV05]
- Giampaolo Bella, Fabio Massacci, and Lawrence C. Paulson. An overview of the verification of SET. *International Journal of Information Security*, 4(1–2):17–28, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0047-7>. **Bella:2005:OVS**
- Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. On detecting co-resident cloud instances using network flow watermarking techniques. *International Journal of Information Security*, 13(2):171–189, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0210-0>. **Bates:2014:DCR**
- David Basin, Sebastian Mödersheim, and Luca Viganò. OFMC: a symbolic model checker for security protocols. *International Journal of Information Security*, 4(3):181–208, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0047-7>. **Basin:2005:OSM**

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0055-7>.
- [BNN04] **Buchholtz:2004:CCF**
 Mikael Buchholtz, Hanne Riis Nielson, and Flemming Nielson. A calculus for control flow analysis of security protocols. *International Journal of Information Security*, 2(3-4):145–167, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0036-x>. [BP08]
- [BNTW12] **Bogdanov:2012:HPS**
 Dan Bogdanov, Margus Nitsoo, Tomas Toft, and Jan Willemson. High-performance secure multi-party computation for data mining applications. *International Journal of Information Security*, 11(6):403–418, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0177-2>. [BPW05a]
- [BP04] **Backes:2004:CPN**
 Michael Backes and Birgit Pfitzmann. Computational probabilistic noninterference. *International Journal of Information Security*, 3(1):42–60, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0039-7>. [BPW05b]
- Backes:2008:LBU**
 Michael Backes and Birgit Pfitzmann. Limits of the BRSIM/UC soundness of Dolev–Yao-style XOR. *International Journal of Information Security*, 7(1):33–54, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0040-z>. [BPW05a]
- Backes:2005:RSS**
 Michael Backes, Birgit Pfitzmann, and Michael Waidner. Reactively secure signature schemes. *International Journal of Information Security*, 4(4):242–252, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0062-8>. [BPW05b]
- Backes:2005:SAS**
 Michael Backes, Birgit Pfitzmann, and Michael Waidner. Symmetric authentication in a simulatable Dolev–Yao-style cryp-

- tographic library. *International Journal of Information Security*, 4(3): 135–154, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0056-6>.
- [BR17] **Bernardini:2017:MRP**
Riccardo Bernardini and Roberto Rinaldo. Making random permutations from physically unclonable constants. *International Journal of Information Security*, 16(3):249–261, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0324-2>.
- [BR18] **Bernardini:2018:GES**
Riccardo Bernardini and Roberto Rinaldo. Generalized Elias schemes for efficient harvesting of truly random bits. *International Journal of Information Security*, 17(1): 67–81, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0358-5>.
- [BR20] **Bernardini:2020:ASS**
Riccardo Bernardini and
- [BR23] **Bhaskara:2023:CEA**
Srividya Bhaskara and Santosh Singh Rathore. Causal effect analysis-based intrusion detection system for IoT applications. *International Journal of Information Security*, 22(4):931–946, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00674-2>.
- [Bra06] **Brandt:2006:HOF**
Felix Brandt. How to obtain full privacy in auctions. *International Journal of Information Security*, 5(4):201–216, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0001-y>.
- [Bra22] **Braeken:2022:PKV**
An Braeken. Pub-

- lic key versus symmetric key cryptography in client-server authentication protocols. *International Journal of Information Security*, 21(1): 103–114, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00543-w>. [BS21]
- Bohli:2006:KSA**
- [BRS06] Jens-Matthias Bohli, Stefan Röhrich, and Rainer Steinwandt. Key substitution attacks revisited: Taking into account malicious signers. *International Journal of Information Security*, 5(1):30–36, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0071-2>. [BS22]
- Baldwin:2005:ESA**
- [BS05] Adrian Baldwin and Simon Shiu. Enabling shared audit data. *International Journal of Information Security*, 4(4): 263–276, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0061-9>. [BSCZ11]
- Borges:2021:EPP**
- Ricard Borges and Francesc Sebé. An efficient privacy-preserving pay-by-phone system for regulated parking areas. *International Journal of Information Security*, 20(5): 715–727, October 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00527-2>.
- Bhattacharjya:2022:EVS**
- Sairath Bhattacharjya and Hossein Saiedian. Establishing and validating secured keys for IoT devices: using P3 connection model on a cloud-based architecture. *International Journal of Information Security*, 21(3):427–436, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00562-7>.
- Baumgarten:2011:CSH**
- Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno. A case study in hardware Trojan design and implementation. *International Journal of Information Security*, 10(1):1–14, February 2011.

CODEN ???? ISSN
1615-5262 (print), 1615-
5270 (electronic). URL [BST21]
<http://link.springer.com/article/10.1007/s10207-010-0115-0>.

Bao:2020:LSP

[BSK⁺20]

Zijian Bao, Wenbo Shi, Saru Kumari, Zhi yin Kong, and Chien-Ming Chen. Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity. *International Journal of Information Security*, 19(3):311–321, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00459-6>. [BSV22]

Balikcioglu:2023:MCD

[BSK⁺23]

Pinar G. Balikcioglu, Melih Sirlanci, Ozge A. Kucuk, Bulut Ulukapi, Ramazan K. Turkmen, and Cengiz Acarturk. Malicious code detection in Android: the role of sequence characteristics and disassembling methods. *International Journal of Information Security*, 22(1):107–118, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00626-2>. [BT07]

Bonte:2021:THM

Charlotte Bonte, Nigel P. Smart, and Titouan Tanguy. Thresholdizing HashEd-DSA: MPC to the rescue. *International Journal of Information Security*, 20(6):879–894, December 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-021-00539-6>.

Borges:2022:AUE

Ricard Borges, Francesc Sebé, and Magda Valls. An anonymous and unlinkable electronic toll collection system. *International Journal of Information Security*, 21(5):1151–1162, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00604-8>.

Bononi:2007:IDS

Luciano Bononi and Carlo Tacconi. Intrusion detection for secure clustering and routing in Mobile Multi-hop Wireless Networks. *International Journal of Information Security*, 6(6):379–392, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

- <http://link.springer.com/article/10.1007/s10207-007-0035-9>.
- [BVS07] Jens-Matthias Bohli, María Isabel González Vasco, and Rainer Steinwandt. Secure group key establishment revisited. *International Journal of Information Security*, 6(4):243–254, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0018-x>.
- [BZ20] Raz Ben Yehuda and Nezer Jacob Zaidenberg. Protection against reverse engineering in ARM. *International Journal of Information Security*, 19(1):39–51, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00450-1>.
- [BW08] Joachim Biskup and Torben Weibert. Keeping secrets in incomplete databases. *International Journal of Information Security*, 7(3):199–217, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0037-7>.
- [BZ03] Joonsang Baek and Yuliang Zheng. Zheng and Sherry’s public key encryption scheme revisited. *International Journal of Information Security*, 2(1):37–44, November 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0069-1>.
- [CAS22] Beyza Cevik, Nur Altıparmak, and Sevil Sen. Lib2Desc: automatic generation of security-centric Android app descriptions using third-party libraries. *International Journal of Information Security*, 21

Bohli:2007:SGK**Yehuda:2020:PAR****Biskup:2008:KSI****Bai:2005:SAP****Baek:2003:ZSP****Cevik:2022:LAG**

- (5):1107–1125, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00601-x>.
- [CBC08] Cherita L. Corbett, Raheem A. Beyah, and John A. Copeland. Passive classification of wireless NICs during active scanning. *International Journal of Information Security*, 7(5):335–348, October 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0053-7>.
- [CBRY20] Peng Cheng, Ibrahim Ethem Bagci, Utz Roedig, and Jeff Yan. SonarSnoop: active acoustic side-channel attacks. *International Journal of Information Security*, 19(2):213–228, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00449-8>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00449-8.pdf>.
- [CC10] Haiyong Chen and Hailiang Chen. A hybrid scheme for securing fingerprint templates. *International Journal of Information Security*, 9(5):353–361, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0114-1>.
- [CC12] Liqun Chen and Yu Chen. The n -Diffie–Hellman problem and multiple-key encryption. *International Journal of Information Security*, 11(5):305–320, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0171-8>.
- [CCB08] Frédéric Cuppens and Nora Cuppens-Boulahia. Modeling contextual security policies. *International Journal of Information Security*, 7(4):285–305, August 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0051-9>.
- [CCD⁺07] J. G. Cederquist, R. Corin,

- M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *International Journal of Information Security*, 6(2-3):133–151, March 2007. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0017-y>. [CDP22]
- [CCS07] **Chen:2007:IBK**
L. Chen, Z. Cheng, and N. P. Smart. Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4):213–241, July 2007. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0011-9>. [CF03]
- [CDF+13] **Catalano:2013:FNI**
Dario Catalano, Mario Di Raimondo, Dario Fiore, Rosario Gennaro, and Orazio Puglisi. Fully non-interactive onion routing with forward secrecy. *International Journal of Information Security*, 12(1):33–47, February 2013. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0020-x>. [CF07]
- Camtepe:2022:ABC**
Seyit Camtepe, Jarek Duda, and Josef Pieprzyk. ANS-based compression and encryption with 128-bit security. *International Journal of Information Security*, 21(5):1051–1067, October 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00597-4>.
- Carminati:2003:MAC**
Barbara Carminati and Elena Ferrari. Management of access control policies for XML document sources. *International Journal of Information Security*, 1(4):236–260, July 2003. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0020-x>.
- Clarke:2007:AMP**
N. L. Clarke and S. M. Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6(1):1–14, January 2007. CODEN ????? ISSN 1615-5262 (print), 1615-

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0006-6>.
- [CFBvO09] **Chiasson:2009:UID**
Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. User interface design affects security: patterns in click-based graphical passwords. *International Journal of Information Security*, 8(6):387–398, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0080-7>.
- [CFG17] **Catalano:2017:CAO**
Dario Catalano, Dario Fiore, and Rosario Genaro. A certificateless approach to onion routing. *International Journal of Information Security*, 16(3):327–343, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0337-x>.
- [CG14] **Catuogno:2014:ATF**
Luigi Catuogno and Clemente Galdi. Analysis of a two-factor graphical password scheme. *International Journal of Information Security*, 13(5):421–437, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0228-y>.
- [CG21] **Cianciullo:2021:OCD**
Louis Cianciullo and Hossein Ghodosi. Outsourced cheating detection for secret sharing. *International Journal of Information Security*, 20(6):871–878, December 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-021-00538-7>.
- [CG23] **Chowdhury:2023:PLT**
Nabin Chowdhury and Vasileios Gkioulos. A personalized learning theory-based cyber-security training exercise. *International Journal of Information Security*, 22(6):1531–1546, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00704-z>.
- [CGL⁺11] **Coker:2011:PRA**
George Coker, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O’Hanlon,

- John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen. Principles of remote attestation. *International Journal of Information Security*, 10(2):63–81, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0124-7>. [CHM18]
- Cremers:2016:III**
- [CH16] Cas Cremers and Marko Horvat. Improving the ISO/IEC 11770 standard for key management techniques. *International Journal of Information Security*, 15(6):659–673, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0306-9>; <http://link.springer.com/content/pdf/10.1007/s10207-015-0306-9.pdf>. [CHMS21]
- Camacho:2012:SAC**
- [CHKO12] Philippe Camacho, Alejandro Hevia, Marcos Kiwi, and Roberto Opazo. Strong accumulators from collision-resistant hashing. *International Journal of Information Security*, 11(5):349–363, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0169-2>. [Chen:2018:MGE]
- Liquan Chen, Jinguang Han, and Chris Mitchell. Message from the Guest Editors. *International Journal of Information Security*, 17(5):491–492, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0416-2>. [Chen:2021:PAS]
- Liquan Chen, Kaibin Huang, Mark Manulis, and Venkatesh Sekar. Password-authenticated searchable encryption. *International Journal of Information Security*, 20(5):675–693, October 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00524-5>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00524-5.pdf>. [Chen:2016:SOK]
- Yu Chen, Qiong Huang, and Zongyang Zhang. Sakai–Ohgishi–Kasahara identity-based non-interactive key exchange revisited and

- more. *International Journal of Information Security*, 15(1):15–33, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0274-0>.
- [CJMS19] Donghoon Chang, Arpan Jati, Sweta Mishra, and Somitra Kumar Sanadhya. Cryptanalytic time-memory trade-off for password hashing schemes. *International Journal of Information Security*, 18(2):163–180, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0405-5>.
- [CK08] Jason Crampton and Hemant Khambhammettu. Delegation in role-based access control. *International Journal of Information Security*, 7(2):123–136, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0044-8>.
- [CK23a] Feiyang Cai and Xenofon Koutsoukos. Correction: Real-time detection of deception attacks in cyber-physical systems. *International Journal of Information Security*, 22(5):1383, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00696-w>. See [CK23b].
- [CK23b] Feiyang Cai and Xenofon Koutsoukos. Real-time detection of deception attacks in cyber-physical systems. *International Journal of Information Security*, 22(5):1099–1114, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00677-z>. See correction [CK23a].
- [CKKK23] Efstratios Chatzoglou, Vasileios Kouliaridis, Georgios Karopoulos, and Georgios Kambourakis. Revisiting QUIC attacks: a comprehensive review on QUIC security and a hands-on study. *International Journal of Information Security*, 22(2):347–365, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-

Chang:2019:CTM

Cai:2023:RTD

Crampton:2008:DRB

Chatzoglou:2023:RQA

Cai:2023:CRT

- 5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00630-6>.
- [CKS21] **Chatterjee:2021:SEW**
Sanjit Chatterjee, Manish Kesarwani, and Akash Shah. Secure and efficient wildcard search over encrypted data. *International Journal of Information Security*, 20(2):199–244, April 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00492-w>.
- [CKW19] **Cai:2019:STP**
Yixian Cai, George Karakostas, and Alan Wassng. Secure and trusted partial grey-box verification. *International Journal of Information Security*, 18(6):677–700, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00431-4>.
- [CL08] **Chen:2008:IID**
Pei-Te Chen and Chi-Sung Laih. IDSIC: an intrusion detection system with identification capability. *International Journal of Information Security*, 7(3):185–197, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0024-z>.
- [CL09] **Cheng:2009:CKA**
Jiin-Chiou Cheng and Chi-Sung Laih. Conference key agreement protocol with non-interactive fault-tolerance over broadcast network. *International Journal of Information Security*, 8(1):37–48, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0062-1>.
- [CL13] **Chen:2013:AMA**
Yu-Shian Chen and Chin-Laung Lei. Aggregate message authentication codes (AMACs) with on-the-fly verification. *International Journal of Information Security*, 12(6):495–504, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0202-0>.
- [CLG23] **Chen:2023:EIS**
Yingchun Chen, Jinguo Li, and Naiwang Guo. Efficient and interpretable

- SRU combined with Tab-Net for network intrusion detection in the big data environment. *International Journal of Information Security*, 22(3):679–689, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00656-w>. [CM16]
- [CLPP11] Jason Crampton, Hoon Wei Lim, Kenneth G. Paterson, and Geraint Price. User-friendly and certificate-free grid security infrastructure. *International Journal of Information Security*, 10(3):137–153, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0123-8>. [CMMPS15]
- [CLW⁺11] Ee-Chien Chang, Liming Lu, Yongzheng Wu, Roland H. C. Yap, and Jie Yu. Enhancing host security using external environment sensors. *International Journal of Information Security*, 10(5):285–299, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0130-9>. [CMN⁺18]
- [Chen:2016:MGE] Liqun Chen and Chris Mitchell. Message from the guest editors. *International Journal of Information Security*, 15(6):573–574, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0353-x>.
- [Casassa-Mont:2015:TSI] Marco Casassa-Mont, Ilaria Matteucci, Marinella Petrocchi, and Marco Luca Sbordio. Towards safer information sharing in the cloud. *International Journal of Information Security*, 14(4):319–334, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0258-5>.
- [Cimitile:2018:TNM] Aniello Cimitile, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, and Corrado Aaron Visaggio. Talos: no more ransomware victims with formal methods. *International Journal of Information Security*, 17(6):719–738, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-

5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0398-5>.

Chakrabarti:2006:KPD

[CMR06]

Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal Roy. A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design. *International Journal of Information Security*, 5(2):105–114, April 2006. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0085-4>. [CPPK15]

Chakraborty:2010:CDB

[CMS10]

Anindya Chakraborty, Arun K. Majumdar, and Shamik Sural. A column dependency-based approach for static and dynamic recovery of databases from malicious transactions. *International Journal of Information Security*, 9(1):51–67, February 2010. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0095-0>. [CR20]

Chadwick:2009:ASX

[CON09]

David W. Chadwick, Sassa Otenko, and Tuan Anh Nguyen. Adding sup-

port to XACML for multi-domain user to user dynamic delegation of authority. *International Journal of Information Security*, 8(2):137–152, April 2009. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0073-y>.

Chakravarty:2015:DAE

Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security*, 14(3):205–220, June 2015. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0256-7>.

Casas-Roma:2020:DGD

Jordi Casas-Roma. DUEFGA: data utility and privacy evaluation framework for graph anonymization. *International Journal of Information Security*, 19(4):465–478, August 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-0095-0>.

- com/article/10.1007/s10207-019-00469-4. [CTM⁺16]
- [CSC⁺23] **Celdran:2023:IBB**
 Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Miguel Azorín Castillo, G r me Bovet, Gregorio Mart nez P rez, and Burkhard Stiller. Intelligent and behavioral-based detection of malware in IoT spectrum sensors. *International Journal of Information Security*, 22(3):541–561, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00602-w>. [CMA⁺18]
- [CSL⁺23] **Chimuco:2023:SCB**
 Francisco T. Chimuco, Jo o B. F. Sequeiros, Carolina Galv o Lopes, Tiago M. C. Sim es, M rio M. Freire, and Pedro R. M. In cio. Secure cloud-based mobile apps: attack taxonomy, requirements, mechanisms, tests and automation. *International Journal of Information Security*, 22(4):833–867, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00669-z>. [CK⁺09]
- Celdran:2016:RPP**
 Alberto Huertas Celdr n, Gin s D lera Tormo, F lix G mez M rmol, Manuel Gil P rez, and Gregorio Mart nez P rez. Resolving privacy-preserving relationships over outsourced encrypted data storages. *International Journal of Information Security*, 15(2):195–209, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0283-z>.
- Chiba:2018:DTA**
 Daiki Chiba, Takeshi Yagi, Mitsuaki Akiyama, Toshiki Shibahara, Tatsuya Mori, and Shigeki Goto. Domain-Profiler: toward accurate and early discovery of domain names abused in future. *International Journal of Information Security*, 17(6):661–680, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0396-7>; <http://link.springer.com/content/pdf/10.1007/s10207-017-0396-7.pdf>.
- Cook:2009:EBC**
 Debra L. Cook, Moti Yung, and Angelos D.

- Keromytis. Elastic block ciphers: method, security and instantiations. [dAKdG10] *International Journal of Information Security*, 8 (3):211–231, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0075-9>.
- [CZ06] **Crescini:2006:PSD**
Vino Fernando Crescini and Yan Zhang. PolicyUpdater: a system for dynamic access control. *International Journal of Information Security*, 5 (3):145–165, July 2006. [Dan07] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0078-8>.
- [DA21] **Deldar:2021:EST**
Fatemeh Deldar and Mahdi Abadi. Enhancing spatial and temporal utilities in differentially private moving objects database release. *International Journal of Information Security*, 20(4):511–533, August 2021. [Das12] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00516-5>.
- deAlbuquerque:2010:FVA**
João Porto de Albuquerque, Heiko Krumm, and Paulo Lício de Geus. Formal validation of automated policy refinement in the management of network security systems. *International Journal of Information Security*, 9 (2):99–125, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0101-6>.
- Danezis:2007:BFM**
George Danezis. Breaking four mix-related schemes based on Universal Re-encryption. *International Journal of Information Security*, 6(6):393–402, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0033-y>.
- Das:2012:RKE**
Ashok Kumar Das. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. *International Journal of Information Security*, 11 (3):189–211, June 2012. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0162-9>.
- [Daw04] **Dawson:2004:PSI**
E. Dawson. Preface to the special issue on PKI. *International Journal of Information Security*, 2(2):65, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0031-7>; <http://link.springer.com/content/pdf/10.1007/s10207-003-0031-7.pdf>. [DDPS02]
- [DBMS10] **Dupasquier:2010:AIL**
Benoît Dupasquier, Stefan Burschka, Kieran McLaughlin, and Sakir Sezer. Analysis of information leakage from encrypted Skype conversations. *International Journal of Information Security*, 9(5):313–325, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0111-4>. [DDX19]
- [DdP13] **DArco:2013:TTR**
Paolo D’Arco and Angel Perez del Pozo. Toward tracing and revoking schemes secure against collusion and any form of secret information leakage. *International Journal of Information Security*, 12(1):1–17, February 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0186-1>. [Damiani:2002:SSS]
- E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. Securing SOAP e-services. *International Journal of Information Security*, 1(2):100–115, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100009>. [Dyer:2019:PHE]
- James Dyer, Martin Dyer, and Jie Xu. Practical homomorphic encryption over the integers for secure computation in the cloud. *International Journal of Information Security*, 18(5):549–579, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00427-0>. [D’Arco:2022:GWP]
- [D’Arco:2022:GWP] P. D’Arco, R. De Prisco,

- and R. Zaccagnino. Gosamer: weaknesses and performance. *International Journal of Information Security*, 21(3):669–687, June 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00575-2>.
- [Den08] Alexander W. Dent. A survey of certificateless encryption schemes and security models. *International Journal of Information Security*, 7(5):349–377, October 2008. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0055-0>.
- [Des09] Abdelrahman Desoky. Listega: list-based steganography methodology. *International Journal of Information Security*, 8(4):247–261, August 2009. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0079-0>.
- [DFBJR18] Josep Domingo-Ferrer, Alberto Blanco-Justicia, and R. Zaccagnino. Dynamic group size accreditation and group discounts preserving anonymity. *International Journal of Information Security*, 17(3):243–260, June 2018. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0368-y>.
- [DFB+16] Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azurra Marson, Arno Mittelbach, and Kenneth G. Paterson. Unpicking PLAID: a cryptographic analysis of an ISO-standards-track authentication protocol. *International Journal of Information Security*, 15(6):637–657, November 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0309-6>.
- [DGF+17] Patrick Duessel, Christian Gehl, Ulrich Flegel, Sven Dietrich, and Michael Meier. Detecting zero-day attacks using context-aware anomaly detection at the application-layer. *International Journal of Information Security*, 16(5):507–520, October 2017. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0368-y>.
- [Dent:2008:SCE] Alexander W. Dent. A survey of certificateless encryption schemes and security models. *International Journal of Information Security*, 7(5):349–377, October 2008. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0055-0>.
- [Degabriele:2016:UPC] Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azurra Marson, Arno Mittelbach, and Kenneth G. Paterson. Unpicking PLAID: a cryptographic analysis of an ISO-standards-track authentication protocol. *International Journal of Information Security*, 15(6):637–657, November 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0309-6>.
- [Desoky:2009:LLB] Abdelrahman Desoky. Listega: list-based steganography methodology. *International Journal of Information Security*, 8(4):247–261, August 2009. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0079-0>.
- [Duessel:2017:DZD] Patrick Duessel, Christian Gehl, Ulrich Flegel, Sven Dietrich, and Michael Meier. Detecting zero-day attacks using context-aware anomaly detection at the application-layer. *International Journal of Information Security*, 16(5):507–520, October 2017. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0368-y>.
- [Domingo-Ferrer:2018:DGS] Josep Domingo-Ferrer, Alberto Blanco-Justicia, and R. Zaccagnino. Dynamic group size accreditation and group discounts preserving anonymity. *International Journal of Information Security*, 17(3):243–260, June 2018. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0368-y>.

formation Security, 16(5): 475–490, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0344-y>.

Draper-Gil:2013:OFE

[DGZFGH13]

G. Draper-Gil, J. Zhou, J. L. Ferrer-Gomila, and M. F. Hinarejos. An optimistic fair exchange protocol with active intermediaries. *International Journal of Information Security*, 12(4):299–318, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0194-9>.

[DJN10]

Daza:2004:PUI

[DHS04]

Vanesa Daza, Javier Heranz, and Germán Sáez. Protocols useful on the Internet from distributed signature schemes. *International Journal of Information Security*, 3(2): 61–69, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0043-y>.

[DLR15]

DiPierro:2011:PTC

[DHW11]

Alessandra Di Pierro, Chris Hankin, and Her-

bert Wiklicky. Probabilistic timing covert channels: to close or not to close? *International Journal of Information Security*, 10(2):83–106, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0107-0>.

Damgaard:2010:GPP

Ivan Damgård, Mads Jurik, and Jesper Buus Nielsen. A generalization of Paillier’s public-key system with applications to electronic voting. *International Journal of Information Security*, 9(6): 371–385, December 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0119-9>.

Dolzhenko:2015:MRE

Egor Dolzhenko, Jay Ligatti, and Srikar Reddy. Modeling runtime enforcement with mandatory results automata. *International Journal of Information Security*, 14(1):47–60, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0043-y>.

- com/article/10.1007/s10207-014-0239-8.
- [DM07] **DeFrancesco:2007:ILS**
 Nicoletta De Francesco and Luca Martini. Instruction-level security typing by abstract interpretation. [DMRS07] *International Journal of Information Security*, 6(2-3):85–106, March 2007. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0015-0>.
- [DMDD16] **DeKeulenaer:2016:LTS**
 Ronald De Keulenaer, Jonas Maebe, Koen De Bosschere, and Bjorn De Sutter. [DNF+19] Link-time smart card code hardening. *International Journal of Information Security*, 15(2):111–130, April 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0282-0>.
- [DMP13] **DeCristofaro:2013:PDC**
 Emiliano De Cristofaro, Mark Manulis, and Bertram Poettering. Private discovery of common social contacts. *International Journal of Information Security*, 12(1):49–65, February 2013. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0183-4>.
- [Dimitrakos:2007:GEP]
 Theo Dimitrakos, Fabio Martinelli, Peter Y. A. Ryan, and Steve Schneider. Guest Editors' preface. *International Journal of Information Security*, 6(2-3):65–66, March 2007. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0012-3>.
- [Dasgupta:2019:DIN]
 Dipankar Dasgupta, Abhijit Kumar Nag, Denise Ferebee, Sanjib Kumar Saha, Kul Prasad Subedi, Arunava Roy, Alvaro Madero, Abel Sanchez, and John R. Williams. Design and implementation of Negative Authentication System. *International Journal of Information Security*, 18(1):23–48, February 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0395-8>.
- [Dewri:2012:OSH]
 Rinku Dewri, Indrajit Ray, Nayot Poolsappasit, and

- Darrell Whitley. Optimal security hardening on attack tree models of networks: a cost-benefit analysis. *International Journal of Information Security*, 11(3):167–188, June 2012. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0160-y>. [dSFK19]
- Delicata:2007:AAV**
- [DS07] Rob Delicata and Steve Schneider. An algebraic approach to the verification of a class of Diffie-Hellman protocols. *International Journal of Information Security*, 6(2-3):183–196, March 2007. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0013-2>. [DSRHC16]
- Das:2019:DSI**
- [DSB19] Debasish Das, Utpal Sharma, and D. K. Bhattacharyya. Defeating SQL injection attack in authentication security: an experimental study. *International Journal of Information Security*, 18(1):1–22, February 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0313-x>. [DSY06]
- Faria:2019:DAA**
- Gerson de Souza Faria and Hae Yong Kim. Differential audio analysis: a new side-channel attack on PIN pads. *International Journal of Information Security*, 18(1):73–84, February 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0403-7>. [Diaz-Santiago:2016:CST]
- Sandra Díaz-Santiago, Lil María Rodríguez-Henríquez, and Debrup Chakraborty. A cryptographic study of tokenization systems. *International Journal of Information Security*, 15(4):413–432, August 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0313-x>. [Ding:2006:CNT]
- Jintai Ding, Dieter Schmidt, and Zhijun Yin. Cryptanalysis of the new TTS scheme in CHES 2004. *International Journal of Information Security*, 5(4):231–240, October 2006. CODEN ????? ISSN 1615-5262 (print), 1615-

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0003-9>.
- Deepa:2018:BBD**
- [DTK⁺18] G. Deepa, P. Santhi Thilagam, Furqan Ahmed Khan, Amit Praseed, Alwyn R. Pais, and Nushafreen Palsetia. Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications. *International Journal of Information Security*, 17(1): 105–120, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0359-4>.
- Degano:2008:P**
- [DV08] Pierpaolo Degano and Luca Viganò. Preface. *International Journal of Information Security*, 7(1): 1, January 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0038-6>.
- Dawson:2002:CCP**
- [DVB02] Ed Dawson, Kapali Viswanathan, and Colin Boyd. Compliant cryptologic protocols. *International Journal of Information Security*, 1(3): 189–202, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-002-0016-y>.
- Din:2023:TSM**
- Nizamud Din, Abdul Waheed, Shamsher Ullah, Noor Ul Amin, Gautam Srivastava, Farhan Ullah, and Jerry Chun-Wei Lin. A typology of secure multicast communication over 5 G/6 G networks. *International Journal of Information Security*, 22(4): 1055–1073, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00678-y>.
- Ding:2010:NHA**
- [DYDW10] Xuhua Ding, Yanjiang Yang, Robert H. Deng, and Shuhong Wang. A new hardware-assisted PIR with $O(n)$ shuffle cost. *International Journal of Information Security*, 9(4):237–252, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0105-2>.

- [DZW⁺18] **Deng:2018:SPT**
 Hua Deng, Yunya Zhou, Qianhong Wu, Bo Qin, and Jianwei Liu. Secure pay-TV for chained hotels. *International Journal of Information Security*, 17(1):33–42, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0354-9>. [EEB⁺15]
- [EAH⁺07] **Esponda:2007:PDP**
 Fernando Esponda, Elena S. Ackley, Paul Helman, Haixia Jia, and Stephanie Forrest. Protecting data privacy through hard-to-reverse negative databases. *International Journal of Information Security*, 6(6):403–415, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0030-1>. [EFH09]
- [EAM⁺23] **Ekstedt:2023:YAC**
 Mathias Ekstedt, Zeeshan Afzal, Preetam Mukherjee, Simon Hacks, and Robert Lagerström. Yet another cybersecurity risk assessment framework. *International Journal of Information Security*, 22(6):1713–1729, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00713-y>. [ElHassani:2015:ION]
- ElHassani:2015:ION**
 Abdeljebar Ameziane El Hassani, Anas Abou El Kalam, Adel Bouhoula, Ryma Abassi, and Abdelah Ait Ouahman. Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity. *International Journal of Information Security*, 14(4):367–385, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0254-9>.
- Esponda:2009:NRI**
 Fernando Esponda, Stephanie Forrest, and Paul Helman. Negative representations of information. *International Journal of Information Security*, 8(5):331–345, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0078-1>.
- ElSalamouny:2018:ONF**
 Ehab ElSalamouny and Sébastien Gambs. Optimal noise functions for

- location privacy on continuous regions. *International Journal of Information Security*, 17(6): 613–630, November 2018. [EMRN17]
 CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0384-y>.
- [EHM15] **Egners:2015:MOW**
 André Egners, Patrick Herrmann, and Ulrike Meyer. Multi-operator wireless mesh networks secured by an all-encompassing security architecture. *International Journal of Information Security*, 14(2):169–186, April 2015. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0244-y>.
- [EHSS14] **Emura:2014:GSI**
 Keita Emura, Goichiro Hanaoka, Yusuke Sakai, and Jacob C. N. Schuldt. Group signature implies public-key encryption with non-interactive opening. *International Journal of Information Security*, 13(1):51–62, February 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0204-y>.
- [ETAHCR08] **Estevez-Tapiador:2008:BRE**
 Juan M. Estevez-Tapiador, Almudena Alcaide, Julio C. Hernandez-Castro, and Arturo Ribagorda. Bayesian rational exchange. *International Journal of Information Security*, 7(1): 85–100, January 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0039-5>.
- [EWR⁺09] **Elmufti:2009:MWS**
 Kalid Elmufti, Dasun Weerasinghe, M. Rajarajan, Veselin Rakocevic, Sanowar Khan, and

- John A. MacDonald. Mobile Web services authentication using SAML and 3GPP generic bootstrapping architecture. *International Journal of Information Security*, 8(2): 77–87, April 2009. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0065-y>. [FAMMZ23]
- Erdodi:2022:AWM**
- [EZ22] László Erdődi and Fabio Massimo Zennaro. The Agent Web Model: modeling web hacking for reinforcement learning. *International Journal of Information Security*, 21(2):293–309, April 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00554-7>. [FBFGEM21]
- El-Zawawy:2021:DLN**
- [EZLC21] Mohamed A. El-Zawawy, Eleonora Losiouk, and Mauro Conti. Do not let Next-Intent Vulnerability be your next nightmare: type system-based approach to detect it in Android apps. *International Journal of Information Security*, 20(1):39–58, February 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00491-x>. [Farhat:2023:CMD]
- Saida Farhat, Manel Abdelkader, Amel Meddeb-Makhlouf, and Faouzi Zarai. CADS-ML/DL: efficient cloud-based multi-attack detection system. *International Journal of Information Security*, 22(6):1989–2013, December 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00729-4>.
- Ferraris:2021:TMP**
- Davide Ferraris, Daniel Bastos, Carmen Fernandez-Gago, and Fadi El-Moussa. A trust model for popular smart home devices. *International Journal of Information Security*, 20(4):571–587, August 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00519-2>.
- Ferraris:2020:TTR**
- Davide Ferraris and Carmen Fernandez-Gago. TrUStAPIS: a trust requirements elicitation method for IoT. *In-*

- International Journal of Information Security*, 19(1): 111–127, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00438-x>.
- [FGS12] **Fiore:2012:RBS**
D. Fiore, R. Gennaro, and N. P. Smart. Relations between the security models for certificateless encryption and ID-based key agreement. *International Journal of Information Security*, 11(1):1–22, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0149-y>.
- [FHV18] **Faust:2018:OPM**
Sebastian Faust, Carmit Hazay, and Daniele Venturi. Outsourced pattern matching. *International Journal of Information Security*, 17(3):327–346, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0374-0>.
- [FN19] **Faghani:2019:MBM**
Mohammad R. Faghani and Uyen T. Nguyen. Mobile botnets meet social networks: design and analysis of a new type of botnet. *International Journal of Information Security*, 18(4):423–449, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0412-6>.
- [Fon08] **Fong:2008:DCC**
Philip W. L. Fong. Discretionary capability confinement. *International Journal of Information Security*, 7(2):137–154, April 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0047-5>.
- [Fra18] **Frattolillo:2018:WPE**
Franco Frattolillo. Watermarking protocols: an excursus to motivate a new approach. *International Journal of Information Security*, 17(5):587–601, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0386-9>.
- [FRG19] **Farras:2019:PSP**
Oriol Farràs and Jordi Ribes-González. Provably

- secure public-key encryption with conjunctive and subset keyword search. *International Journal of Information Security*, 18(5): 533–548, October 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-00426-7>. [FYF22]
- Fernandes:2014:SIC**
- [FSG+14] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio. Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2):113–170, April 2014. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0208-7>. [FZ21]
- Fan:2020:SHB**
- [FTS+20] Chun-I Fan, Yi-Fan Tseng, Hui-Po Su, Ruei-Hau Hsu, and Hiroaki Kikuchi. Secure hierarchical Bitcoin wallet scheme against privilege escalation attacks. *International Journal of Information Security*, 19(3):245–255, June 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00476-5>. [GA23]
- Fu:2022:CGP**
- Bingxue Fu, Xing Yu, and Tao Feng. CT-GCN: a phishing identification model for blockchain cryptocurrency transactions. *International Journal of Information Security*, 21(6):1223–1232, December 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00606-6>.
- Faisal:2021:SAT**
- Abu Faisal and Mohammad Zulkernine. A secure architecture for TCP/UDP-based cloud communications. *International Journal of Information Security*, 20(2):161–179, April 2021. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00511-w>.
- Gandhi:2023:TUS**
- Kapilan Kulayan Arumugam Gandhi and Chamundeswar Arumugam. Toward a unified and secure approach for extraction of forensic digital evidence from an IoT device. *International Journal of In-*

formation Security, 22 (2):417–431, April 2023. CODEN ???? ISSN [GBG18] 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00645-z>.

Gimenez-Aguilar:2023:MUB

[GAdFGM23] Mar Gimenez-Aguilar, Jose Maria de Fuentes, and Lorena Gonzalez-Manzano. Malicious uses of blockchains by malware: from the analysis to Smart-Zephyrus. *International Journal of Information Security*, 22(5): 1445–1480, October 2023. CODEN ???? ISSN [GCH⁺19] 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00700-3>.

Granadillo:2014:RBC

[GBDJ14] Gustavo Gonzalez Granadillo, Malek Belhaouane, Hervé Debar, and Grégoire Jacob. RORI-based countermeasure selection using the OrBAC formalism. *International Journal of Information Security*, 13(1):63–79, February 2014. CODEN ???? ISSN [GCSÁBdSS12] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0207-8>.

Gruber:2018:UTB

A. Gruber and I. Ben-Gal. Using targeted Bayesian network learning for suspect identification in communication networks. *International Journal of Information Security*, 17 (2):169–181, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0362-4>.

Gao:2019:LBD

Wen Gao, Liqun Chen, Yupu Hu, Christopher J. P. Newton, Baocang Wang, and Jiangshan Chen. Lattice-based deniable ring signatures. *International Journal of Information Security*, 18 (3):355–370, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0417-1>; <http://link.springer.com/content/pdf/10.1007/s10207-018-0417-1.pdf>.

Guerra-Casanova:2012:AMD

J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra. Authentication in mobile devices through hand gesture recognition. *International*

- Journal of Information Security*, 11(2):65–83, April 2012. CODEN ????? ISSN [GGJ22]
1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0154-9>.
- [GDA22] **Gong:2022:TDR**
Qian Gong, Phil DeMar, and Mine Altunay. ThunderSecure: deploying real-time intrusion detection for 100G research networks by leveraging stream-based features and one-class classification network. *International Journal of Information Security*, 21(4): 799–812, August 2022. [GGP21]
CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00584-9>.
- [GdKGV14] **Garcia:2014:WLS**
Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Wirelessly lockpicking a smart card reader. *International Journal of Information Security*, 13(5): 403–420, October 2014. [GH05]
CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0234-0>.
- Ghorbel:2022:APP**
Amal Ghorbel, Mahmoud Ghorbel, and Mohamed Jmaiel. Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. *International Journal of Information Security*, 21(3):489–508, June 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00565-4>.
- Granese:2021:EMP**
Federica Granese, Daniele Gorla, and Catuscia Palamidessi. Enhanced models for privacy and utility in continuous-time diffusion networks. *International Journal of Information Security*, 20(5):763–782, October 2021. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00530-7>.
- Guttman:2005:RAN**
Joshua D. Guttman and Amy L. Herzog. Rigorous automated network security management. *International Journal of Information Security*, 4(1–2):29–48, February 2005. CODEN ????? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0052-x>.
- [GI19] **Gulyas:2019:HIA**
Gábor György Gulyás and Sándor Imre. Hiding information against structural re-identification. *International Journal of Information Security*, 18(2):125–139, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0400-x>. [GKS19]
- [GKBS12] **Gritzalis:2012:FAR**
Dimitris Gritzalis, Panagiotis Katsaros, Stylianos Basagiannis, and Yannis Soudris. Formal analysis for robust anti-SPIT protection using model checking. *International Journal of Information Security*, 11(2):121–135, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0159-4>. [GLMS⁺04]
- [GKKT10] **Gauravaram:2010:HFU**
Praveen Gauravaram, John Kelsey, Lars R. Knudsen, and Søren S. Thomsen. On hash functions using checksums. *International Journal of Information Security*, 9(2):137–151, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0100-7>. **Grining:2019:PPP**
Krzysztof Grining, Marek Klonowski, and Piotr Syga. On practical privacy-preserving fault-tolerant data aggregation. *International Journal of Information Security*, 18(3):285–304, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0413-5>. **Gorrieri:2004:AAT**
Roberto Gorrieri, Ruggero Lanotte, Andrea Maggiolo-Schettini, Fabio Martinelli, Simone Tini, and Enrico Tronci. Automated analysis of timed security: a case study on web privacy. *International Journal of Information Security*, 2(3–4):168–186, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0037-9>.

- [GLMS19] **Garra:2019:RAB** Ricard Garra, Dominik Leibenger, Josep M. Miret, and Francesc Sebé. Repairing an aggregation-based smart metering system. *International Journal of Information Security*, 18(5): 637–646, October 2019. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00435-0>. [GMGM21]
- [GLP03] **Gurgens:2003:ACP** Sigrid Gurgens, Javier Lopez, and René Peralta. Analysis of e-commerce protocols: Adapting a traditional technique. *International Journal of Information Security*, 2(1): 21–36, November 2003. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0021-9>. [GMH14]
- [GMdFLR23] **Gonzalez-Manzano:2023:TCA** Lorena González-Manzano, José M. de Fuentes, Flavio Lombardi, and Cristina Ramos. A technical characterization of APTs by leveraging public resources. *International Journal of Information Security*, 22(6):1567–1584, December 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00706-x>. [Gomez:2021:CCM]
- [Gomez:2021:CCM] Juan Manuel Castelo Gómez, Javier Carrillo Mondéjar, José Roldán Gómez, and José Luis Martínez Martínez. A context-centered methodology for IoT forensic investigations. *International Journal of Information Security*, 20(5): 647–673, October 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00523-6>. [Gougliadis:2014:SPV]
- [Gougliadis:2014:SPV] Antonios Gougliadis, Ioannis Mavridis, and Vincent C. Hu. Security policy verification for multi-domains in cloud systems. *International Journal of Information Security*, 13(2):97–111, April 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0205-x>. [Gruner:2023:ACS]
- [Gruner:2023:ACS] Andreas Grüner, Alexander Mühle, Niko Lockenwitz, and Christoph Meinel.

- Analyzing and comparing the security of self-sovereign identity management systems through threat modeling. *International Journal of Information Security*, 22(5): 1231–1248, October 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00688-w>. [GMO01]
- Galindo:2005:FOH**
- [GMMV05] David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar. Fujisaki–Okamoto hybrid encryption revisited. *International Journal of Information Security*, 4(4): 228–241, October 2005. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0042-z>. [GMS03]
- Giorgini:2006:RET**
- [GMMZ06] Paolo Giorgini, Fabio Massacci, John Mylopoulos, and Nicola Zannone. Requirements engineering for trust management: model, methodology, and reasoning. *International Journal of Information Security*, 5(4):257–274, October 2006. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0005-7>. [Gollman:2001:E]
- Geiselmann:2003:AIP**
- Dieter Gollman, Catherine A. Meadows, and Eiji Okamoto. Editorial. *International Journal of Information Security*, 1(1):1–2, August 2001. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100004>. [Geiselmann:2003:AIP]
- Willi Geiselmann, Willi Meier, and Rainer Steinwandt. An attack on the isomorphisms of polynomials problem with one secret. *International Journal of Information Security*, 2(1):59–64, November 2003. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0025-5>. [Guardiola-Muzquiz:2023:SCS]
- Guardiola-Muzquiz:2023:SCS**
- [GMSS23] Gorka Guardiola-Múzquiz and Enrique Soriano-Salvador. SealFSv2: combining storage-based and ratcheting for tamper-evident logging. *International Journal of Information Security*, 22(2):447–466, April 2023. CODEN ????? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00643-1>.
- [GNS14] Weizheng Gao, Kashi Neupane, and Rainer Steinwandt. Tuning a two-round group key agreement. *International Journal of Information Security*, 13(5):467–476, October 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0225-6>.
- [GOBdlC11] Sergio Sánchez García, Ana Gómez Oliva, Emilia Pérez Belleboni, and Iván Pau de la Cruz. Solving identity delegation problem in the e-government environment. *International Journal of Information Security*, 10(6):351–372, November 2011. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0140-7>.
- [Gol08] Dieter Gollmann. Editorial. *International Journal of Information Security*, 7(2):101, April 2008.
- [Gol12] Jovan Dj. Golić. A new authentication model for ad hoc networks. *International Journal of Information Security*, 11(5):333–347, October 2012. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0167-4>.
- [GP17] Felix Günther and Bertram Poettering. Linkable message tagging: solving the key distribution problem of signature schemes. *International Journal of Information Security*, 16(3):281–297, June 2017. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0327-z>.
- [GP23] Panagiotis Grontas and Aris Pagourtzis. Anonymity and everlasting privacy in electronic voting. *International Journal of Information Security*, 22(4):1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00643-1>.
- [Golic:2012:NAM] Jovan Dj. Golić. A new authentication model for ad hoc networks. *International Journal of Information Security*, 11(5):333–347, October 2012. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0167-4>.
- [Gao:2014:TTR] Weizheng Gao, Kashi Neupane, and Rainer Steinwandt. Tuning a two-round group key agreement. *International Journal of Information Security*, 13(5):467–476, October 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00643-1>.
- [Garcia:2011:SID] Sergio Sánchez García, Ana Gómez Oliva, Emilia Pérez Belleboni, and Iván Pau de la Cruz. Solving identity delegation problem in the e-government environment. *International Journal of Information Security*, 10(6):351–372, November 2011. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0140-7>.
- [Gunther:2017:LMT] Felix Günther and Bertram Poettering. Linkable message tagging: solving the key distribution problem of signature schemes. *International Journal of Information Security*, 16(3):281–297, June 2017. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0327-z>.
- [Grontas:2023:AEP] Panagiotis Grontas and Aris Pagourtzis. Anonymity and everlasting privacy in electronic voting. *International Journal of Information Security*, 22(4):1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00643-1>.

- 819–832, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00666-2>.
- [GPS17] **Garg:2017:NBD**
Shree Garg, Sateesh K. Peddoju, and Anil K. Sarje. Network-based detection of Android malicious apps. *International Journal of Information Security*, 16(4):385–400, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0343-z>.
- [Gri06] **Gritzalis:2006:PKI**
Stefanos Gritzalis. Public Key Infrastructure: Research and applications. *International Journal of Information Security*, 5(1):1–2, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0075-y>.
- [GRV05] **Gurgens:2005:SFN**
Sigrid Gurgens, Carsten Rudolph, and Holger Vogt. On the security of fair non-repudiation protocols. *International Journal of In-*
- formation Security*, 4(4):253–262, October 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0063-7>.
- [GS15] **Giffhorn:2015:NAL**
Dennis Giffhorn and Gregor Snelting. A new algorithm for low-deterministic security. *International Journal of Information Security*, 14(3):263–287, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0257-6>.
- [GSAMCA18] **Gonzalez-Serrano:2018:SML**
Francisco-Javier González-Serrano, Adrián Amor-Martín, and Jorge Casamayón-Antón. Supervised machine learning using encrypted training data. *International Journal of Information Security*, 17(4):365–377, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0381-1>.
- [GSM⁺11] **Glisson:2011:ERW**
William Bradley Glisson, Tim Storer, Gavin Mayall, Iain Moug, and George

- Grispos. Electronic retention: what does your mobile phone reveal about you? *International Journal of Information Security*, 10(6):337–349, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0144-3>. [GTM11]
- [GSP⁺16] Clémentine Gritti, Willy Susilo, Thomas Plantard, Kaitai Liang, and Duncan S. Wong. Broadcast encryption with dealership. *International Journal of Information Security*, 15(3):271–283, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0285-x>. [GW09]
- [GSS10] David M. Goldschlag, Stuart G. Stubblebine, and Paul F. Syverson. Temporarily hidden bit commitment and lottery applications. *International Journal of Information Security*, 9(1):33–50, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0094-1>. [Gyorffy:2011:TBG]
- John Charles Gyorffy, Andrew F. Tappenden, and James Miller. Token-based graphical password authentication. *International Journal of Information Security*, 10(6):321–336, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0147-0>. [Geron:2009:CCR]
- Erel Geron and Avishai Wool. CRUST: cryptographic remote untrusted storage without public keys. *International Journal of Information Security*, 8(5):357–377, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0081-6>. [Gritzalis:2007:PMO]
- S. Gritzalis, A. N. Yannacopoulos, C. Lambri-noudakis, P. Hatzopoulos, and S. K. Katsikas. A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments.

- International Journal of Information Security*, 6 (4):197–211, July 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0010-x>.
- Guan:2023:AHO**
- [GZH+23] Zhenyu Guan, Lixin Zhang, Bohan Huang, Bihe Zhao, and Song Bian. Adaptive hyperparameter optimization for black-box adversarial attack. *International Journal of Information Security*, 22 (6):1765–1779, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00716-9>. [HBH12]
- Hale:2020:UMA**
- [Hal20] Britta Hale. User-mediated authentication protocols and unforgeability in key collision. *International Journal of Information Security*, 19(6):609–621, December 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00479-2>. [HBK22]
- Hamdi:2023:FLB**
- [Ham23] Najet Hamdi. Federated learning-based intrusion detection system for Internet of Things. *International Journal of Information Security*, 22 (6):1937–1948, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00727-6>.
- Hadziosmanovic:2012:LMA**
- Dina Hadziosmanović, Damiano Bolzoni, and Pieter H. Hartel. A log mining approach for process monitoring in SCADA. *International Journal of Information Security*, 11(4):231–251, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0163-8>; <http://link.springer.com/content/pdf/10.1007/s10207-012-0163-8.pdf>.
- Hadjadj:2022:OPF**
- Taha Elamine Hadjadj, Adel Bouhoula, and Riadh Ksantini. Optimization of parallel firewalls filtering rules. *International Journal of Information Security*, 21(2):323–340, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00479-2>.

- com/article/10.1007/s10207-021-00557-4.
- [HCN15] **Han:2010:CBI**
 Shui-Hua Han and Chao-Hsien Chu. Content-based image authentication: current status, issues, and challenges. *International Journal of Information Security*, 9(1): 19–32, February 2010. [HH16]
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0093-2>.
- [HCN15] **Hoang:2015:GAM**
 Thang Hoang, Deokjai Choi, and Thuc Nguyen. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security*, 14(6): 549–560, November 2015. [HIDFGHR19]
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0273-1>.
- [HGH23] **Hamzenejadi:2023:MBD**
 Sajad Hamzenejadi, Mahdieh Ghazvini, and Seyedamiryousef Hosseini. Mobile botnet detection: a comprehensive survey. *International Journal of Information Security*, 22(1): 137–175, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00624-4>.
- [HGH23] **Hu:2016:EWS**
 Changhui Hu and Lidong Han. Efficient wildcard search over encrypted data. *International Journal of Information Security*, 15(5):539–547, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0302-0>.
- [HGH23] **Hinarejos:2019:DPE**
 M. Francisca Hinarejos, Andreu-Pere Isern-Deyà, Josep-Lluís Ferrer-Gomila, and Llorenç Huguet-Rotger. Deployment and performance evaluation of mobile multicoupon solutions. *International Journal of Information Security*, 18(1): 101–124, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0404-6>; <http://link.springer.com/content/pdf/10.1007/s10207-018-0404-6.pdf>.

- [HIST09] **Hasegawa:2009:PFC**
 Shingo Hasegawa, Shuji Isobe, Hiroki Shizuya, and Katsuhiko Tashiro. On the pseudo-freeness and the CDH assumption. *International Journal of Information Security*, 8(5): 347–355, October 2009. [HKO22]
 CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0087-0>.
- [HJDC15] **Hadavi:2015:SSS**
 Mohammad Ali Hadavi, Rasool Jalili, Ernesto Damiani, and Stelvio Cimato. Security and searchability in secret sharing-based data outsourcing. *International Journal of Information Security*, 14(6):513–529, November 2015. [HL04]
 CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0277-x>.
- [HK19] **Hiemenz:2019:DSS**
 Benedikt Hiemenz and Michel Krämer. Dynamic searchable symmetric encryption for storing geospatial data in the cloud. *International Journal of Information Security*, 18(3):333–354, June 2019. [HLKI15]
- Huszt:2022:SPB**
 Andrea Huszti, Szabolcs Kovács, and Norbert Oláh. Scalable, password-based and threshold authentication for smart homes. *International Journal of Information Security*, 21(4):707–723, August 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00578-7>.
- Hopcroft:2004:ASA**
 Philippa Hopcroft and Gavin Lowe. Analysing a stream authentication protocol using model checking. *International Journal of Information Security*, 3(1):2–13, October 2004. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0040-1>.
- Han:2015:MAU**
 Kyoung Soo Han, Jae Hyun Lim, Boojoong Kang, and Eul Gyu Im. Malware analysis using visualized images and entropy graphs.
- CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0414-4>.

- International Journal of Information Security*, 14 (1):1–14, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0242-0>.
- [HLS18] **Ham:2018:IYP**
 HyoungMin Ham, JongHyup Lee, and JooSeok Song. Improved yoking proof protocols for preserving anonymity. *International Journal of Information Security*, 17(4):379–393, August 2018. [HN14] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0383-z>.
- [HM22] **Hougaard:2022:ALO**
 Hector B. Hougaard and Atsuko Miyaji. Authenticated logarithmic-order supersingular isogeny group key exchange. *International Journal of Information Security*, 21(2):207–221, April 2022. [HNHY23] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00549-4>.
- [HMCD04] **Hitchcock:2004:ESM**
 Yvonne Hitchcock, Paul Montague, Gary Carter, and Ed Dawson. The efficiency of solving multiple discrete logarithm problems and the implications for the security of fixed elliptic curves. *International Journal of Information Security*, 3(2):86–98, November 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0045-9>.
- Herranz:2014:SEA**
 Javier Herranz and Jordi Nin. Secure and efficient anonymization of distributed confidential databases. *International Journal of Information Security*, 13(6):497–512, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0237-x>.
- Hannousse:2023:DLM**
 Abdelhakim Hannousse, Mohamed Cherif Nait-Hamoud, and Salima Yahiouche. A deep learner model for multi-language webshell detection. *International Journal of Information Security*, 22(1):47–61, February 2023. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00615-5>.
- [Harn:2009:EIB]
[HRL09] Lein Harn, Jian Ren, and Changlu Lin. Efficient identity-based GQ multisignatures. *International Journal of Information Security*, 8(3):205–210, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0072-z>. [HS15]
- [Holzl:2020:DDA]
[HRMM20] Michael Hölzl, Michael Roland, Omid Mir, and René Mayrhofer. Disposable dynamic accumulators: toward practical privacy-preserving mobile eIDs with scalable revocation. *International Journal of Information Security*, 19(4):401–417, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00458-7>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00458-7.pdf>. [HSMW08]
- [Hammer:2009:FSC]
[HS09] Christian Hammer and Gregor Snelting. Flow-sensitive, context-sensitive, and object-sensitive information flow control based on program dependence graphs. *International Journal of Information Security*, 8(6):399–422, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0086-1>.
- [Halevi:2015:KAS]
Tzipora Halevi and Nitesh Saxena. Keyboard acoustic side channel attacks: exploring realistic and security-sensitive scenarios. *International Journal of Information Security*, 14(5):443–456, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0264-7>.
- [Huang:2008:SUD]
Xinyi Huang, Willy Susilo, Yi Mu, and Wei Wu. Secure universal designated verifier signature without random oracles. *International Journal of Information Security*, 7(3):171–183, June 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com>.

- com/article/10.1007/s10207-007-0021-2.
- [HSMY12] **Han:2012:NCO**
Jinguang Han, Willy Susilo, Yi Mu, and Jun Yan. New constructions of OSBE schemes and their applications in oblivious access control. *International Journal of Information Security*, 11(6): 389–401, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0176-3>.
- [HTM11] **Hanley:2011:UTD**
Neil Hanley, Michael Tunstall, and William P. Marne. Using templates to distinguish multiplications from squaring operations. *International Journal of Information Security*, 10(4):255–266, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0135-4>.
- [Hub12] **Huber:2012:PSS**
Michael Huber. Perfect secrecy systems immune to spoofing attacks. *International Journal of Information Security*, 11(4): 281–289, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0166-5>.
- [HXT23] **Higgins:2023:CPR**
Martin Higgins, Wangkun Xu, Fei Teng, and Thomas Parisini. Cyber-physical risk assessment for false data injection attacks considering moving target defences. *International Journal of Information Security*, 22(3):579–589, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00621-7>.
- [HYWS11] **Huang:2011:ESD**
Qiong Huang, Guomin Yang, Duncan S. Wong, and Willy Susilo. Efficient strong designated verifier signature schemes without random oracle or with non-delegatability. *International Journal of Information Security*, 10(6): 373–385, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0146-1>.
- [HYWS12] **Huang:2012:NEO**
Qiong Huang, Guomin Yang, Duncan S. Wong,

and Willy Susilo. A new efficient optimistic fair exchange protocol without random oracles. *International Journal of Information Security*, 11(1):53–63, February 2012. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0152-3>. [UHT02]

Huang:2017:MAP

[HZL⁺17]

Cheng-Ta Huang, Yu-Hong Zhang, Li-Chiun Lin, Wei-Jen Wang, and Shiuh-Jeng Wang. Mutual authentications to parties with QR-code applications in mobile systems. *International Journal of Information Security*, 16(5):525–540, October 2017. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0349-6>. [IKS22]

Isern-Deya:2015:PUG

[IDHRPCMP15]

Andreu Pere Isern-Deyà, Llorenç Huguet-Rotger, M. Magdalena Payeras-Capellà, and Macià Mut-Puigserver. On the practicability of using group signatures on mobile devices: implementation and performance analysis on the Android platform. *International Journal of In-*

formation Security, 14(4):335–345, August 2015. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0259-4>.

Itakura:2002:PPI

Yukio Itakura, Masaki Hashiyada, Toshio Nagashima, and Shigeo Tsujii. Proposal on personal identifiers generated from the STR information of DNA. *International Journal of Information Security*, 1(3):149–160, November 2002. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-002-0013-1>.

Inayoshi:2022:VUT

Hiroki Inayoshi, Shohei Kakei, and Shoichi Saito. Value-utilized taint propagation: toward precise detection of apps' information flows across Android API calls. *International Journal of Information Security*, 21(5):1127–1149, October 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00603-9>.

- [IMI18] **Imamura:2018:IAA**
 Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata. Integrity analysis of authenticated encryption based on stream ciphers. *International Journal of Information Security*, 17(5):493–511, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0378-9>.
- [INS21] **Ibnugraha:2021:RMD** [IS23]
 Prajna Deshanta Ibnugraha, Lukito Edi Nugroho, and Paulus Insap Santosa. Risk model development for information security in organization environment based on business perspectives. *International Journal of Information Security*, 20(1):113–126, February 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00495-7>.
- [IOU+21] **Imamura:2021:WAM** [IT05]
 Yuta Imamura, Rintaro Orito, Hiroyuki Uekawa, Kritsana Chaikaew, Patara Leelaprute, Masaya Sato, and Toshihiro Yamauchi. Web access monitoring mechanism via Android WebView for threat analysis. *International Journal of Information Security*, 20(6):833–847, December 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00534-3>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00534-3.pdf>.
- Ibrahim:2023:CSS**
 Nasir Ibrahim and Harin Sellahewa. A cross-setting study of user unlocking behaviour in a graphical authentication scheme: a case study on Android Pattern Unlock. *International Journal of Information Security*, 22(6):1849–1863, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00722-x>.
- Itakura:2005:PMB**
 Yukio Itakura and Shigeo Tsujii. Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures. *International Journal of Information Security*, 4(4):288–296, October 2005. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0065-5>.
- [IZS08] **Imamoto:2008:AEC**
Kenji Imamoto, Jianying Zhou, and Kouichi Sakurai. Achieving evenhandedness in certified email system for contract signing. *International Journal of Information Security*, 7(6): 383–394, November 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0056-z>.
- [JAYZ21] **Josephlal:2021:EIR**
Edwin Franco Myloth Josephlal, Sridhar Adepu, Zheng Yang, and Jianying Zhou. Enabling isolation and recovery in PLC redundancy framework of metro train systems. *International Journal of Information Security*, 20(6): 783–795, December 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00529-0>.
- [JBK21] **Jouini:2021:QAS**
Mouna Jouini, Latifa Ben Arfa Rabai, and Ridha Khedri. A quantitative as-
- essment of security risks based on a multifaceted classification approach. *International Journal of Information Security*, 20(4): 493–510, August 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00515-6>.
- [JCL⁺18] **Jia:2018:ERH**
Hongyong Jia, Yue Chen, Julong Lan, Kaixiang Huang, and Jun Wang. Efficient revocable hierarchical identity-based encryption using cryptographic accumulators. *International Journal of Information Security*, 17(4): 477–490, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0387-8>.
- [JG15] **James:2015:AIP**
Joshua I. James and Pavel Gladyshev. Automated inference of past action instances in digital investigations. *International Journal of Information Security*, 14(3):249–261, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0051-0>.

- com/article/10.1007/s10207-014-0249-6.
- [JGK14] **Jovanovikj:2014:CMS**
 Vladimir Jovanovikj, Dusan Gabrijelcic, and Tomaz Klobucar. A conceptual model of security context. *International Journal of Information Security*, 13(6):571–581, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0229-x>. [JM17]
- [JJJ21] **Ji:2021:EVA**
 Soo-Yeon Ji, Bong-Keun Jeong, and Dong Hyun Jeong. Evaluating visualization approaches to detect abnormal activities in network traffic data. *International Journal of Information Security*, 20(3):331–345, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00504-9>. [JMV01]
- [JK22] **Jeet:2022:SIP**
 Rabari Jeet and P. Arun Raj Kumar. A survey on interest packet flooding attacks and its countermeasures in named data networking. *International Journal of Information Security*, 21(5):1163–1187, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00591-w>. **Joh:2017:PSV**
- [Joh:2017:PSV] HyunChul Joh and Yashwant K. Malaiya. Periodicity in software vulnerability discovery, patching and exploitation. *International Journal of Information Security*, 16(6):673–690, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0345-x>. **Johnson:2001:ECD**
- [Johnson:2001:ECD] Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100002>. **Jiang:2018:CPA**
- [Jiang:2018:CPA] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption supporting access policy update and its extension

- with preserved attributes. *International Journal of Information Security*, 17 (5):533–548, October 2018. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0388-7>. [JTV19]
- [JSMG18b] Yin hao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. *International Journal of Information Security*, 17(4): 463–475, August 2018. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0376-y>. [JZ11]
- [JT21] Huiwen Jia and Chunming Tang. Cryptanalysis of a non-interactive deniable ring signature scheme. *International Journal of Information Security*, 20(1): 103–112, February 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00497-5>. [KA18]
- Joudaki:2019:ETS**
Zeinab Joudaki, Julie Thorpe, and Miguel Vargas Martin. Enhanced Tacit Secrets: System-assigned passwords you can’t write down, but don’t need to. *International Journal of Information Security*, 18 (2):239–255, April 2019. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0408-2>.
- Jajodia:2011:MGE**
Sushil Jajodia and Jianying Zhou. Message from the Guest Editors. *International Journal of Information Security*, 10(5): 267–268, October 2011. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0131-8>; <http://link.springer.com/content/pdf/10.1007/s10207-011-0131-8.pdf>.
- Kirubavathi:2018:SAD**
G. Kirubavathi and R. Anitha. Structural analysis and detection of Android botnets using machine learning techniques. *International Journal of Information Security*, 17 (2):153–167, April 2018.

- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0363-3>.
- [KAC16] **Karimi:2016:UAA**
 Vahid R. Karimi, Paulo S. C. Alencar, and Donald D. Cowan. A uniform approach for access control and business models with explicit rule realization. *International Journal of Information Security*, 15(2):145–171, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0275-z>.
- [KAC17] **Karimi:2017:FMA**
 Vahid R. Karimi, Paulo S. C. Alencar, and Donald D. Cowan. A formal modeling and analysis approach for access control rules, policies, and their combinations. *International Journal of Information Security*, 16(1):43–74, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0314-4>.
- [KAK22] **Kifouche:2022:DIN**
 Abdenour Kifouche, Mohamed Salah Azzaz, and Remy Kocik. Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications. *International Journal of Information Security*, 21(6):1247–1262, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00609-3>.
- [KAK23] **Kaur:2023:PPP**
 Jasleen Kaur, Alka Agrawal, and Raees Ahmad Khan. P2ADF: a privacy-preserving attack detection framework in fog-IoT environment. *International Journal of Information Security*, 22(4):749–762, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00661-7>.
- [KB13] **Kundu:2013:PPA**
 Ashish Kundu and Elisa Bertino. Privacy-preserving authentication of trees and graphs. *International Journal of Information Security*, 12(6):467–494, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0066-1>.

- com/article/10.1007/s10207-013-0198-5.
- [KB22] **Kumar:2022:SML**
 Raju Kumar and Aruna Bhat. A study of machine learning-based models for detection, control, and mitigation of cyberbullying in online social media. *International Journal of Information Security*, 21(6):1409–1431, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00600-y>. [KBJ22]
- [KB23] **Kuppusamy:2023:APS**
 K. S. Kuppusamy and G. Balayogi. Accessible password strength assessment method for visually challenged users. *International Journal of Information Security*, 22(6):1731–1741, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00714-x>. [KBY22]
- [KBH07] **Knight:2007:IJI**
 Scott Knight, Scott Buffett, and Patrick C. K. Hung. The *International Journal of Information Security* special issue on privacy, security and trust technologies and e-business services. *International Journal of Information Security*, 6(5):285–286, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0036-8>.
- Karl:2022:DNI**
 Ryan Karl, Hannah Burchfield, and Taeho Jung. Developing non-interactive MPC with trusted hardware for enhanced security. *International Journal of Information Security*, 21(4):777–797, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00583-w>.
- Kim:2022:MPD**
 Jinsung Kim, Younghoon Ban, and Jeong Hyun Yi. MAPAS: a practical deep learning-based Android malware detection system. *International Journal of Information Security*, 21(4):725–738, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00579-6>.

- [KCB17] **Kotzanikolaou:2017:BAR**
Panayiotis Kotzanikolaou, George Chatzisoironiou, and Mike Burmester. Broadcast anonymous routing (BAR): scalable real-time anonymous communication. *International Journal of Information Security*, 16(3):313–326, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0318-0>. [KCM⁺15]
- [KCB20] **Ko:2020:FDD**
Ili Ko, Desmond Chambers, and Enda Barrett. Feature dynamic deep learning approach for DDoS mitigation within the ISP domain. *International Journal of Information Security*, 19(1):53–70, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00453-y>. [KDM22]
- [KCC⁺23] **Kuzlu:2023:ASM**
Murat Kuzlu, Ferhat Ozgur Catak, Umit Cali, Evren Catak, and Ozgur Guler. Adversarial security mitigations of mmWave beamforming prediction models using defensive distillation and adversarial retrain-
ing. *International Journal of Information Security*, 22(2):319–332, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00644-0>. [Kozakevicius:2015:UQS]
- Alice Kozakevicius, Cristian Cappo, Bruno A. Mozzaquatro, Raul Ceretta Nunes, and Christian E. Schaerer. URL query string anomaly sensor designed with the bidimensional Haar wavelet transform. *International Journal of Information Security*, 14(6):561–581, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0276-y>. [Khan:2022:PAK]
- Haibat Khan, Benjamin Dowling, and Keith M. Martin. Pragmatic authenticated key agreement for IEEE Std 802.15.6. *International Journal of Information Security*, 21(3):577–595, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00570-7>.

- [KDYS19] **Kulah:2019:SAD**
 Yusuf Kulah, Berkay Dincer, Cemal Yilmaz, and Erkay Savas. SpyDetector: an approach for detecting side-channel attacks at runtime. *International Journal of Information Security*, 18(4): 393–422, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0411-7>.
- [KIP22] **Kate:2011:GCB**
 Aniket Kate and Ian Goldberg. Generalizing cryptosystems based on the subset sum problem. *International Journal of Information Security*, 10(3):189–199, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0129-2>.
- [KGG09] **Kozina:2009:MIW**
 Mario Kozina, Marin Golub, and Stjepan Gros. A method for identifying Web applications. *International Journal of Information Security*, 8(6): 455–467, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0092-3>.
- [KJ14] **Kishore:2022:SPD**
 R. Kishore, I. Ioannou, and A. Pitsillides. A security protocol for D2D communications in 5G networks using elliptic curve cryptography. *International Journal of Information Security*, 21(6):1389–1408, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00620-8>.
- [KJG+11] **Kim:2014:EVE**
 Kee Sung Kim and Ik Rae Jeong. Efficient verifiably encrypted signatures from lattices. *International Journal of Information Security*, 13(4): 305–314, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0226-0>.
- [Kong:2011:SSA] **Kong:2011:SSA**
 Deguang Kong, Yoon-Chan Jhi, Tao Gong, Sen-cun Zhu, Peng Liu, and Hongsheng Xi. SAS: semantics aware signature generation for polymorphic worm detection. *In-*

- International Journal of Information Security*, 10(5): 269–283, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0132-7>.
- [KJS17] Minchul Kim, Younghwan Jung, and Junghwan Song. A modified exhaustive search on a password system using SHA-1. *International Journal of Information Security*, 16(3):263–269, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0332-2>.
- [KK17] Shahrzad Kananizadeh and Kirill Kononenko. Development of dynamic protection against timing channels. *International Journal of Information Security*, 16(6):641–651, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0356-7>.
- [KK22] Ioannis Kazoleas and Panagiotis Karampelas. A novel malicious remote administration tool using stealth and self-defense techniques. *International Journal of Information Security*, 21(2):357–378, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00559-2>.
- [KKK17] Constantinos Koliass, Vasilis Koliass, and Georgios Kambourakis. TermID: a distributed swarm intelligence-based approach for wireless intrusion detection. *International Journal of Information Security*, 16(4):401–416, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0335-z>.
- [KKK22a] Hee Yeon Kim, Ji Hoon Kim, and Kyounggon Kim. DAPP: automatic detection and analysis of prototype pollution vulnerability in Node.js modules. *International Journal of Information Security*, 21(1):1–23, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00559-2>.

- com/article/10.1007/s10207-020-00537-0.
- [KKK22b] **Koike:2022:IOH**
 Kazuki Koike, Ryotaro Kobayashi, and Masahiko Katoh. IoT-oriented high-efficient anti-malware hardware focusing on time series metadata extractable from inside a processor core. *International Journal of Information Security*, 21(4):1–19, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00577-0>. [KLMM09]
- [KKKV07] **Klinkoff:2007:ENS**
 Patrick Klinkoff, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. Extending .NET security to unmanaged code. *International Journal of Information Security*, 6(6):417–428, October 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0031-0>. [KLPL21]
- [KKY+23] **Kim:2023:ERS**
 Moon-Seok Kim, Sungho Kim, Sang-Kyung Yoo, Bong-Soo Lee, Ji-Man Yu, Il-Woong Tcho, and Yang-Kyu Choi. Error reduction of SRAM-based physically unclonable function for chip authentication. *International Journal of Information Security*, 22(5):1087–1098, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00668-0>. **Koshutanski:2009:EGS**
 Hristo Koshutanski, Aliaksandr Lazouski, Fabio Martinelli, and Paolo Mori. Enhancing grid security by fine-grained behavioral control and negotiation-based authorization. *International Journal of Information Security*, 8(4):291–314, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0083-4>. **Kim:2021:ISD**
 Hyoseung Kim, Kwangsu Lee, Jong Hwan Park, and Dong Hoon Lee. Improving the security of direct anonymous attestation under host corruptions. *International Journal of Information Security*, 20(4):475–492, August 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-021-0083-4>.

- com/article/10.1007/s10207-020-00507-6.
- [KLZ⁺21] **Khan:2021:EAB**
 Fawad Khan, Hui Li, Yinghui Zhang, Haider Abbas, and Tahreem Yaqoob. Efficient attribute-based encryption with repeated attributes optimization. *International Journal of Information Security*, 20(3):431–444, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00505-8>. [KM10]
- [KM03] **Kremer:2003:FMP**
 Steve Kremer and Olivier Markowitch. Fair multi-party non-repudiation protocols. *International Journal of Information Security*, 1(4):223–235, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0019-3>. [KM22]
- [KM07] **Kopf:2007:TTU**
 Boris Köpf and Heiko Mantel. Transformational typing and unification for automatically correcting insecure programs. *International Journal of Information Security*, 6(2–3):107–131, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0016-z>. [KME⁺16]
- Knudsen:2010:CEA**
 Lars R. Knudsen and Charlotte V. Miolane. Counting equations in algebraic attacks on block ciphers. *International Journal of Information Security*, 9(2):127–135, April 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0099-9>. [Koman:2022:CBS]
- Komano:2022:CBS**
 Yuichi Komano and Takaaki Mizuki. Coin-based secure computations. *International Journal of Information Security*, 21(4):833–846, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00585-8>. [Kasamatsu:2016:TSE]
- Kasamatsu:2016:TSE**
 Kohei Kasamatsu, Takahiro Matsuda, Keita Emura, Nuttapong Attrapadung, Goichiro Hanaoka, and Hideki Imai. Time-specific encryption from forward-secure encryption: generic and direct constructions.

- International Journal of Information Security*, 15 (5):549–571, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0304-y>.
- Korzhik:2003:HAB**
- [KML03] Valery Korzhik and Guillermo Morales-Luna. Hybrid authentication based on noisy channels. *International Journal of Information Security*, 1(4):203–210, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-002-0017-x>. [KN07]
- Katsantonis:2023:CRD**
- [KMMG23] M. N. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis. Cyber range design framework for cyber security education and training. *International Journal of Information Security*, 22(4):1005–1027, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00680-4>. [KNL16]
- Kuper:2009:GXS**
- [KMR09] Gabriel Kuper, Fabio Masciaci, and Nataliya Ras-sadko. Generalized XML security views. *International Journal of Information Security*, 8(3):173–203, June 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0074-x>.
- Krukow:2007:TS**
- Karl Krukow and Mogens Nielsen. Trust structures. *International Journal of Information Security*, 6(2–3):153–181, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0014-1>.
- Kurek:2016:TBC**
- Tytus Kurek, Marcin Niemiec, and Artur Lason. Taking back control of privacy: a novel framework for preserving cloud-based firewall policy confidentiality. *International Journal of Information Security*, 15(3):235–250, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0292-y>; <http://link.springer.com/content/pdf/10.1007/s10207-015-0292-y.pdf>.

- [KO02] **Kim:2002:NEC**
S. Kim and H. Oh. A new electronic check system with reusable refunds. *International Journal of Information Security*, 1(3): 175–188, November 2002. [KSB23]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-002-0015-z>.
- [KOSU16] **Khayati:2016:PPP**
Leyli Javid Khayati, Cengiz Orencik, Erkay Savas, and Berkant Ustaoğlu. A practical privacy-preserving targeted advertising scheme for IPTV users. *International Journal of Information Security*, 15(4): 335–360, August 2016. [KSM10]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0296-7>.
- [KPM12] **Kontaxis:2012:MID**
Georgios Kontaxis, Michalis Polychronakis, and Evangelos P. Markatos. Minimizing information disclosure to third parties in social login platforms. *International Journal of Information Security*, 11(5): 321–332, October 2012. [KSZ07]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0102-5>.
- Kaur:2023:IAL**
Sarabjeet Kaur, Amanpreet Kaur Sandhu, and Abhinav Bhandari. Investigation of application layer DDoS attacks in legacy and software-defined networks: a comprehensive review. *International Journal of Information Security*, 22(6):1949–1988, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00728-5>.
- Kundu:2010:DID**
Amlan Kundu, Shamik Sural, and A. K. Majumdar. Database intrusion detection using sequence alignment. *International Journal of Information Security*, 9(3):179–191, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0102-5>.
- Konstantinou:2007:EGS**
Elisavet Konstantinou, Yannis C. Stamatiou, and Christos Zaroliagis. Efficient generation of secure elliptic curves. *Internationa*

- tional Journal of Information Security*, 6(1):47–63, January 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0009-3>.
- [KU16] **Kiraz:2016:EVA**
Mehmet Sabir Kiraz and Osmanbey Uzunkol. Efficient and verifiable algorithms for secure outsourcing of cryptographic computations. *International Journal of Information Security*, 15(5):519–537, October 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0308-7>.
- [Kud02] **Kudo:2002:PPB**
Michiharu Kudo. PBAC: Provision-based access control model. *International Journal of Information Security*, 1(2):116–130, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100010>.
- [Küs05] **Kusters:2005:DCP**
Ralf Küsters. On the decidability of cryptographic protocols with open-ended
- [KW15] **Kamm:2015:SFP**
Liina Kamm and Jan Willemsen. Secure floating point arithmetic and private satellite collision analysis. *International Journal of Information Security*, 14(6):531–548, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0271-8>; <http://link.springer.com/content/pdf/10.1007/s10207-014-0271-8.pdf>.
- [KWCK19] **Kluczniak:2019:MDA**
Kamil Kluczniak, Jianfeng Wang, Xiaofeng Chen, and Mirosław Kutylowski. Multi-device anonymous authentication. *International Journal of Information Security*, 18(2):181–197, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0406-4>; <http://>
- data structures. *International Journal of Information Security*, 4(1–2):49–70, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0050-z>.

- link.springer.com/content/pdf/10.1007/s10207-018-0406-4.pdf.
- [KYH18] **Kuo:2018:DRA** [LBZ⁺10] Tsung-Min Kuo, Sung-Ming Yen, and Meng-Che Han. Dynamic reversed accumulator. *International Journal of Information Security*, 17(2):183–191, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0360-6>.
- [Lan01] **Landwehr:2001:CS** [LC04] Carl E. Landwehr. Computer security. *International Journal of Information Security*, 1(1):3–13, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100003>.
- [LBW05] **Ligatti:2005:EAE** [LCL14] Jay Ligatti, Lujio Bauer, and David Walker. Edit automata: enforcement mechanisms for run-time security policies. *International Journal of Information Security*, 4(1–2):2–16, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0046-8>.
- Liu:2010:EOO** Joseph K. Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, and Jun Wen Wong. Efficient online/offline identity-based signature for wireless sensor network. *International Journal of Information Security*, 9(4):287–296, August 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0109-y>.
- Laih:2004:GVR** C. S. Laih and K. Y. Chen. Generating visible RSA public keys for PKI. *International Journal of Information Security*, 2(2):103–109, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0030-8>.
- Lian:2014:PSC** Bin Lian, Gongliang Chen, and Jianhua Li. Provably secure e-cash system with practical and efficient complete tracing. *International Journal of Information Security*, 13(3):271–289, June 2014. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0240-2>.
- Liu:2016:STP**
- [LCL16] Liang Liu, Xiaofeng Chen, and Wenjing Lou. Secure three-party computational protocols for triangle area. *International Journal of Information Security*, 15(1):1–13, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0284-y>. [LD07]
- Li:2014:AAM**
- [LCPD14] Fudong Li, Nathan Clarke, Maria Papadaki, and Paul Dowland. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 13(3):229–244, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0209-6>. [LD17]
- Luo:2018:ASI**
- [LcSCL⁺18] Ying Luo, Sen ching S. Cheung, Riccardo Lazzeretti, Tommaso Pignata, and Mauro Barni. Anonymous subject identification and privacy information management in video surveillance. *International Journal of Information Security*, 17(3):261–278, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0380-2>.
- Lauer:2007:BOT**
- Thomas W. Lauer and Xiaodong Deng. Building online trust through privacy practices. *International Journal of Information Security*, 6(5):323–331, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0028-8>.
- Li:2017:WOO**
- Lichun Li and Anwitaman Datta. Write-only oblivious RAM-based privacy-preserved access of outsourced data. *International Journal of Information Security*, 16(1):23–42, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0329-x>; <http://link.springer.com/content/>

- pdf/10.1007/s10207-016-0329-x.pdf.
- [Lev07] Avner Levin. Is workplace surveillance legal in Canada? *International Journal of Information Security*, 6(5): 313–321, September 2007. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0026-x>.
- [LH15] Tao Li and Aiqun Hu. Trusted mobile model based on DTE technology. *International Journal of Information Security*, 14(5):457–469, October 2015. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0266-5>.
- [LH23] Ngoc T. Luong and Doan Hoang. BAPRP: a machine learning approach to blackhole attacks prevention routing protocol in vehicular ad hoc networks. *International Journal of Information Security*, 22(6):1547–1566, December 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00705-y>.
- [LI07] Jinshan Liu and Valérie Isarny. An incentive compatible reputation mechanism for ubiquitous computing environments. *International Journal of Information Security*, 6(5): 297–311, September 2007. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0029-7>.
- [Lin15] Han-Yu Lin. RPCAE: a novel revocable proxy convertible authenticated encryption scheme. *International Journal of Information Security*, 14(5): 431–441, October 2015. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0269-2>.
- [LKH09] Sangho Lee, Jong Kim, and Sung Je Hong. Redistributing time-based rights between consumer devices for content sharing in DRM system. *International Journal of Information Security*, 8(4):

- 263–273, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0082-5>.
Liao:2014:POC
- [LL14] Qi Liao and Zhen Li. Portfolio optimization of computer and mobile botnets. *International Journal of Information Security*, 13(1):1–14, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0206-9>.
Leontiadis:2021:SCR
- [LL21] Iraklis Leontiadis and Ming Li. Secure and collusion-resistant data aggregation from convertible tags. *International Journal of Information Security*, 20(1):1–20, February 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00485-4>.
Lee:2022:SPM
- [LL22] Junwon Lee and Heejo Lee. An SSH predictive model using machine learning with web proxy session logs. *International Journal of Information Security*, 21(2):311–322, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00555-6>.
Lanet:2018:WTM
- [LLBL18] Jean-Louis Lanet, Hélène Le Boudier, Mohammed Benattou, and Axel Legay. When time meets test. *International Journal of Information Security*, 17(4):395–409, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0371-3>.
Lyvas:2022:EIS
- [LLG22] Christos Lyvas, Costas Lambrinouidakis, and Dimitris Geneiatakis. IntentAuth: Securing Android’s intent-based inter-process communication. *International Journal of Information Security*, 21(5):973–982, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00592-9>.
Lee:2021:BBM
- [LLH21] Tian-Fu Lee, Hong-Ze Li, and Yi-Pei Hsieh. A blockchain-based medical

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0320-6>.
- [LMMO04] **Lopez:2004:PDB**
 Javier Lopez, Antonio Maña, Jose A. Montenegro, and Juan J. Ortega. PKI design based on the use of on-line certification authorities. *International Journal of Information Security*, 2(2):91–102, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0027-3>. [LNX22]
- [LMMP06] **Lioy:2006:PPP**
 Antonio Lioy, Marius Marian, Natalia Moltchanova, and Massimiliano Pala. PKI past, present and future. *International Journal of Information Security*, 5(1):18–29, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0077-9>. [Lop18]
- [LMMS17] **Lazouski:2017:SDU**
 Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori, and Andrea Saracino. Stateful data usage control for Android mobile devices. *International Journal of Information Security*, 16(4):345–369, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0336-y>. **Lyvas:2022:MME**
 Christos Lyvas, Christoforos Ntantogian, and Christos Xenakis. [m]allotROPism: a metamorphic engine for malicious software variation development. *International Journal of Information Security*, 21(1):61–78, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00541-y>. **Lopriore:2018:ARM**
 Lanfranco Lopriore. Access right management by extended password capabilities. *International Journal of Information Security*, 17(5):603–612, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0390-0>. **Lim:2011:IBC**
 Hoon Wei Lim and Kenneth G. Paterson. Identity-based cryptography for

- grid security. *International Journal of Information Security*, 10(1): 15–32, February 2011. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0116-z>. [LSG22]
- [LRB⁺10] Dan Lin, Prathima Rao, Elisa Bertino, Ninghui Li, and Jorge Lobo. EXAM: a comprehensive environment for the analysis of access control policies. *International Journal of Information Security*, 9(4): 253–273, August 2010. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0106-1>. [LSR⁺23]
- [LS23] Rudolf Lovrencić and Dejan Skvorc. Multi-cloud applications: data and code fragmentation for improved security. *International Journal of Information Security*, 22(3):713–721, June 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00658-8>. [LSV⁺23]
- Lygerou:2022:DHI**
- Irini Lygerou, Shreyas Srinivasa, and Dimitris Gritzalis. A decentralized honeypot for IoT protocols based on Android devices. *International Journal of Information Security*, 21(6):1211–1222, December 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00605-7>. See correction [LSV⁺23].
- Lopez:2023:AAA**
- Christian López, Jesús Solano, Esteban Rivera, Lizzy Tengana, Johana Florez-Lozano, Alejandra Castelblanco, and Martín Ochoa. Adversarial attacks against mouse- and keyboard-based biometric authentication: black-box versus domain-specific techniques. *International Journal of Information Security*, 22(6):1665–1685, December 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00711-0>.
- Lygerou:2023:CDH**
- Irini Lygerou, Shreyas Srinivasa, Emmanouil Vasilo-manolakis, George Ster-

- giopoulos, and Dimitris Gritzalis. Correction to: A decentralized honeypot for IoT Protocols based on Android devices. *International Journal of Information Security*, 22(1):303, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00628-0>. See [LSG22].
- [LSWW14] **Lee:2014:AGU** Ming-Feng Lee, Nigel P. Smart, Bogdan Warinschi, and Gaven J. Watson. Anonymity guarantees of the UMTS/LTE authentication and connection protocol. *International Journal of Information Security*, 13(6):513–527, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0231-3>.
- [LTC23] **Levshun:2023:TMA** Dmitry Levshun, Olga Tushkanova, and Andrey Chechulin. Two-model active learning approach for inappropriate information classification in social networks. *International Journal of Information Security*, 22(6):1921–1936, December 2023.
- [Lu09] **Lu:2009:RKR** Jiqiang Lu. Related-key rectangle attack on 36 rounds of the XTEA block cipher. *International Journal of Information Security*, 8(1):1–11, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0059-9>.
- [LV10] **Lin:2010:MTE** Ching Lin and Vijay Varadharajan. MobileTrust: a trust enhanced security architecture for mobile agent systems. *International Journal of Information Security*, 9(3):153–178, June 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0098-x>.
- [LVK18] **Laszka:2018:GTA** Aron Laszka, Yevgeniy Vorobeychik, and Xenofon Koutsoukos. A game-theoretic approach for integrity assurance in resource-bounded systems.

- International Journal of Information Security*, 17(2):221–242, April 2018. [LWL23]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0364-2>.
- [LWA21] Wenjuan Li, Yu Wang, and Man Ho Au. Toward a blockchain-based framework for challenge-based collaborative intrusion detection. *International Journal of Information Security*, 20(2):127–139, April 2021. [LZQ+18]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00488-6>.
- [LWL+21] Pengfei Liu, Weiping Wang, Xi Luo, Haodong Wang, and Chushu Liu. NSDroid: efficient multi-classification of Android malware using neighborhood signature in local function call graphs. *International Journal of Information Security*, 20(1):59–71, February 2021. [Man21]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00489-5>.
- Li:2023:BEC**
Wenjuan Li, Yu Wang, and Jin Li. A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems. *International Journal of Information Security*, 22(5):1219–1230, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00687-x>.
- Li:2018:IVC**
Yuxi Li, Fucai Zhou, Yuhai Qin, Muqing Lin, and Zifeng Xu. Integrity-verifiable conjunctive keyword searchable encryption in cloud storage. *International Journal of Information Security*, 17(5):549–568, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0394-9>.
- Mandal:2021:ATC**
Mriganka Mandal. Anonymity in traceable cloud data broadcast system with simultaneous individual messaging. *International Journal of Information Security*, 20(3):405–430, June 2021. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00512-9>.
- [MARK20] **Manasrah:2020:KPD**
 Ahmed M. Manasrah, Areej R. AL-Rabadi, and Najib A. Kofahi. Key pre-distribution approach using block LU decomposition in wireless sensor network. *International Journal of Information Security*, 19(5):579–596, October 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00477-4>.
- [MB16] **Malhi:2016:PPA**
 Avleen Malhi and Shalini Batra. Privacy-preserving authentication framework using Bloom filter for secure vehicular communications. *International Journal of Information Security*, 15(4):433–453, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0299-4>.
- [MB23] **Mohammadi:2023:NHH**
 Shahriar Mohammadi and Mehdi Babagoli. A novel hybrid hunger games algorithm for intrusion detection systems based on nonlinear regression modeling. *International Journal of Information Security*, 22(5):1177–1195, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00684-0>.
- [MBH⁺21] **Manulis:2021:CSN**
 M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis. Cyber security in new space. *International Journal of Information Security*, 20(3):287–311, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00503-w>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00503-w.pdf>.
- [MBHT17] **Mehrnezhad:2017:PCI**
 Maryam Mehrnezhad, Abbas Ghaemi Bafghi, Ahad Harati, and Ehsan Toreini. PiSHi: click the images and I tell if you are a human. *International Journal of Information Security*, 16(2):133–149, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207->

015-0311-z; <http://link.springer.com/content/pdf/10.1007/s10207-015-0311-z.pdf>.

Martinez-Balleste:2018:DIS

- [MBRPS18] Antoni Martínez-Ballesté, Hatem Rashwan, Domenc Puig, and Agusti Solanas. Design and implementation of a secure and trustworthy platform for privacy-aware video surveillance. *International Journal of Information Security*, 17(3):279–290, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0370-4>.

Marconi:2011:CPE

- [MCD11] Luciana Marconi, Mauro Conti, and Roberto Di Pietro. CASSANDRA: a probabilistic, efficient, and privacy-preserving solution to compute set intersection. *International Journal of Information Security*, 10(5):301–319, October 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0133-6>.

McHugh:2001:IID

- [McH01] John McHugh. Intrusion and intrusion detection. *International Jour-*

nal of Information Security, 1(1):14–35, August 2001. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100001>.

Madabhusi:2023:SAD

Srinidhi Madabhusi and Rinku Dewri. A survey of anomaly detection methods for power grids. *International Journal of Information Security*, 22(6):1799–1832, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00720-z>.

Mishra:2023:SSU

Kailash Chandra Mishra and Subrata Dutta. A simple and secure user authentication scheme using Map Street View with usability analysis based on ISO/IEC 25022. *International Journal of Information Security*, 22(2):403–415, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00636-0>.

Menezes:2023:BSC

Leonardo Dias Menezes, Luciano Vieira de Araújo, and Marislei Nishijima.

- Blockchain and smart contract architecture for notaries services under civil law: a Brazilian experience. *International Journal of Information Security*, 22(4):869–880, August 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00673-3>. [ME23]
- [MdMF22] Roberto Vasconcelos Melo, Douglas D. J. de Macedo, and Mauricio Martinuzzi Fiorenza. ISM-AC: an immune security model based on alert correlation and software-defined networking. *International Journal of Information Security*, 21(2):191–205, April 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00550-x>. [MFES04]
- [MdSC⁺15] Jean Everson Martina, Eduardo dos Santos, Marcelo Carlomagno Carlos, Geraint Price, and Ricardo Felipe Custódio. An adaptive threat model for security ceremonies. *International Journal of Information Security*, 14(2):103–121, April 2015. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0026-4>. [MG19]
- [Melo:2022:IAI] Roberto Vasconcelos Melo, Douglas D. J. de Macedo, and Mauricio Martinuzzi Fiorenza. ISM-AC: an immune security model based on alert correlation and software-defined networking. *International Journal of Information Security*, 21(2):191–205, April 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00550-x>. [MFES04]
- [Mohamed:2023:DSB] Safa Mohamed and Ridha Ejbali. Deep SARSA-based reinforcement learning approach for anomaly network intrusion detection system. *International Journal of Information Security*, 22(1):235–247, February 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00634-2>.
- [Munoz:2004:CRS] Jose L. Muñoz, Jordi Forne, Oscar Esparza, and Miguel Soriano. Certificate revocation system implementation based on the Merkle hash tree. *International Journal of Information Security*, 2(2):110–124, January 2004. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0026-4>.
- [Makhlouf:2019:SAS] Amel Meddeb Makhlouf and Mohsen Guizani. SE-AOMDV: secure and effi-

- cient AOMDV routing protocol for vehicular communications. *International Journal of Information Security*, 18(5): 665–676, October 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00436-z>. [MGV17]
- [MG23] Shweta Mittal and Mohona Ghosh. A novel two-level secure access control approach for blockchain platform in healthcare. *International Journal of Information Security*, 22(4): 799–817, August 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00664-4>. [MI22]
- [MGRR19] Héctor Marco-Gisbert and Ismael Ripoll-Ripoll. SSPFA: effective stack smashing protection for Android OS. *International Journal of Information Security*, 18(4):519–532, August 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-00425-8>; <http://link.springer.com/content/pdf/10.1007/s10207-018-00425-8.pdf>. [Malatras:2017:EUI]
- Apostolos Malatras, Dimitris Geneiatakis, and Ioannis Vakalis. On the efficiency of user identification: a system-based approach. *International Journal of Information Security*, 16(6):653–671, November 2017. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0340-2>; <http://link.springer.com/content/pdf/10.1007/s10207-016-0340-2.pdf>. [Mimura:2022:ANT]
- Mamoru Mimura and Ryo Ito. Applying NLP techniques to malware detection in a practical environment. *International Journal of Information Security*, 21(2):279–291, April 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00553-8>. [Mighan:2021:NSI]
- Soosan Naderi Mighan and Mohsen Kahani. A novel scalable intrusion detection system based on deep

- learning. *International Journal of Information Security*, 20(3):387–403, June 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00508-5>. [ML17]
- [MKS⁺23] Md. Mumtahn Habib Ullah Mazumder, Md. Eusha Kadir, Sadia Sharmin, Md. Shariful Islam, and Muhammad Mahbub Alam. cFEM: a cluster based feature extraction method for network intrusion detection. *International Journal of Information Security*, 22(5):1355–1369, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00694-y>. [MLC23]
- [ML14] Mousa Mousazadeh and Behrouz Tork Ladani. Randomized gossip algorithms under attack. *International Journal of Information Security*, 13(4):391–402, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0221-x>. [MLCQ21]
- Mann:2017:TFA**
Christopher Mann and Daniel Loebenberger. Two-factor authentication for the Bitcoin protocol. *International Journal of Information Security*, 16(2):213–226, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0325-1>.
- Mohammadi:2023:HML**
Reza Mohammadi, Chhagan Lal, and Mauro Conti. HTTPScout: a machine learning based countermeasure for HTTP flood attacks in SDN. *International Journal of Information Security*, 22(2):367–379, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00641-3>.
- Mousazadeh:2014:RGA**
- Medina-Lopez:2021:SAD**
Cristóbal Medina-López, L. G. Casado, and Yuan-song Qiao. An SDN approach to detect targeted attacks in P2P fully connected overlays. *International Journal of Information Security*, 20(2):245–255, April 2021. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00499-3>.
- Miao:2016:MDU**
- [MLCS16] Qiguang Miao, Jiachen Liu, Ying Cao, and Jianfeng Song. Malware detection using bilayer behavior abstraction and improved one-class support vector machines. *International Journal of Information Security*, 15(4): 361–379, August 2016. [MLYL20] CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0297-6>.
- Mesbah:2019:REJ**
- [MLM19] Abdelhak Mesbah, Jean-Louis Lanet, and Mohamed Mezghiche. Reverse engineering Java Card and vulnerability exploitation: a shortcut to ROM. *International Journal of Information Security*, 18(1): 85–100, February 2019. [MMS16] CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0401-9>.
- Mana:2004:FSE**
- [MLO⁺04] Antonio Maña, Javier Lopez, Juan J. Ortega, Ernesto Pimentel, and Jose M. Troya. A framework for secure execution of software. *International Journal of Information Security*, 3(2): 99–112, November 2004. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0048-6>.
- Meng:2020:ECB**
- Weizhi Meng, Wenjuan Li, Laurence T. Yang, and Peng Li. Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. *International Journal of Information Security*, 19(3):279–290, June 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00462-x>.
- Mateu:2016:HAV**
- Víctor Mateu, Josep M. Miret, and Francesc Sebé. A hybrid approach to vector-based homomorphic tallying remote voting. *International Journal of Information Security*, 15(2):211–221, April 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

- <http://link.springer.com/article/10.1007/s10207-015-0279-8>.
- Melki:2020:LMF**
- [MNC20] Reem Melki, Hassan N. Noura, and Ali Chehab. Lightweight multi-factor mutual authentication protocol for IoT devices. [MP16] *International Journal of Information Security*, 19(6): 679–694, December 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00484-5>.
- Mohammadi:2023:CBO**
- [Moh23] Reza Mohammadi. A comprehensive blockchain-oriented secure framework for SDN/Fog-based IoUT. [MP22] *International Journal of Information Security*, 22(5):1163–1175, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00683-1>.
- Martina:2015:VMB**
- [MP15] Jean Everson Martina and Lawrence Charles Paulson. Verifying multicast-based security protocols using the inductive method. [MPG21] *International Journal of Information Security*, 14(2):187–204, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0251-z>.
- Mennink:2016:EPH**
- Bart Mennink and Bart Preneel. Efficient parallelizable hashing using small non-compressing primitives. *International Journal of Information Security*, 15(3):285–300, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0288-7>.
- Munonye:2022:MLA**
- Kindson Munonye and Martinek Péter. Machine learning approach to vulnerability detection in OAuth 2.0 authentication and authorization flow. *International Journal of Information Security*, 21(2):223–237, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00551-w>.
- Murvay:2021:SCA**
- Pal-Stefan Murvay, Lucian Popa, and Bogdan Groza. Securing the controller area network with

- covert voltage channels. *International Journal of Information Security*, 20(6): 817–831, December 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00532-5>. [MPS10]
- Mavrogiannopoulos:2014:TSK**
- [MPP14] Nikos Mavrogiannopoulos, Andreas Pashalidis, and Bart Preneel. Toward a secure Kerberos key exchange with smart cards. *International Journal of Information Security*, 13(3):217–228, June 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0213-x>. [MPS14]
- Menges:2021:DDI**
- [MPP21] Florian Menges, Benedikt Putz, and Günther Pernul. DEALER: decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security*, 20(5): 741–761, October 2021. [MR03] CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00528-1>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00528-1.pdf>. [MPS10]
- MacKenzie:2010:PAK**
- Philip MacKenzie, Sarvar Patel, and Ram Swaminathan. Password-authenticated key exchange based on RSA. *International Journal of Information Security*, 9(6): 387–410, December 2010. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0120-3>. [MPS10]
- Manulis:2014:PAI**
- Mark Manulis, Bertram Poettering, and Douglas Stebila. Plaintext awareness in identity-based key encapsulation. *International Journal of Information Security*, 13(1): 25–49, February 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0218-5>. [MPS14]
- MacKenzie:2003:NCD**
- Philip MacKenzie and Michael K. Reiter. Networked cryptographic devices resilient to capture. *International Journal of Information Security*, 2(1):1–20, November 2003. CODEN ????. ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0022-8>.
- [MR04] **MacKenzie:2004:TPG**
Philip MacKenzie and Michael K. Reiter. Two-party generation of DSA signatures. *International Journal of Information Security*, 2(3-4): 218–239, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0041-0>.
- [MRG23] **Molla:2023:ESS**
Eirini Molla, Panagiotis Rizomiliotis, and Stefanos Gritzalis. Efficient searchable symmetric encryption supporting range queries. *International Journal of Information Security*, 22(4):785–798, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00667-1>.
- [MRW02] **Monrose:2002:PHB**
Fabian Monrose, Michael K. Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 1(2):69–83, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100006>.
- [MS09] **Mashatan:2009:ITC**
Atefeh Mashatan and Douglas R. Stinson. Interactive two-channel message authentication based on Interactive-Collision Resistant hash functions. *International Journal of Information Security*, 8(1): 49–60, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0063-0>.
- [MS11] **Miret:2011:CAH**
Josep M. Miret and Francesc Sebé. Cryptanalysis of an ad-hoc cryptosystem for mix-based e-voting robust against relation attacks. *International Journal of Information Security*, 10(6):387–389, November 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0145-2>.
- [MS14] **Mizuki:2014:FCB**
Takaaki Mizuki and Hiroki Shizuya. A formalization of card-based cryptographic

- protocols via abstract machine. *International Journal of Information Security*, 13(1):15–23, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0219-4>. [MSKD16]
- [MS15] Tanveer Mustafa and Karsten Sohr. Understanding the implemented access control policy of Android system services with slicing and extended static checking. *International Journal of Information Security*, 14(4):347–366, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0260-y>. [MSKS20]
- [MSGCDPSS18] Miguel Morales-Sandoval, Jose Luis Gonzalez-Compean, Arturo Diaz-Perez, and Victor J. Sosa-Sosa. A pairing-based cryptographic approach for data security in the cloud. *International Journal of Information Security*, 17(4):441–461, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0375-z>. [Manulis:2016:SMP]
- Mark Manulis, Douglas Stebila, Franziskus Kiefer, and Nick Denham. Secure modular password authentication for the web using channel bindings. *International Journal of Information Security*, 15(6):597–620, November 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0348-7>; <http://link.springer.com/content/pdf/10.1007/s10207-016-0348-7.pdf>. [Mitropoulos:2020:PAC]
- Dimitris Mitropoulos, Thodoris Sotiropoulos, Nikos Koutsovasilis, and Diomidis Spinelis. PDGuard: an architecture for the control and secure processing of personal data. *International Journal of Information Security*, 19(4):479–498, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00468-5>. [Mizuki:2002:CCF]
- Takaaki Mizuki, Hiroki Shizuya, and Takao Nishizeki.

- A complete characterization of a family of key exchange protocols. *International Journal of Information Security*, 1(2): 131–142, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100011>. [MTW+14]
- [MSP+13] Félix Gómez Mármol, Christoph Sorge, Ronald Petric, Osman Ugus, Dirk Westhoff, and Gregorio Martínez Pérez. Privacy-enhanced architecture for smart metering. *International Journal of Information Security*, 12(2):67–82, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0181-6>. [MU18]
- [MTSH18] Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. Stealing PINs via mobile sensors: actual risk versus user perception. *International Journal of Information Security*, 17(3):291–313, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0369-x>; <http://link.springer.com/content/pdf/10.1007/s10207-017-0369-x.pdf>. [McEvoy:2014:ANT]
- Robert P. McEvoy, Michael Tunstall, Claire Whelan, Colin C. Murphy, and William P. Marnane. All-or-Nothing Transforms as a countermeasure to differential side-channel analysis. *International Journal of Information Security*, 13(3):291–304, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0212-y>. [Murakami:2018:OAA]
- Keisuke Murakami and Takeaki Uno. Optimization algorithm for k -anonymization of datasets with low information loss. *International Journal of Information Security*, 17(6):631–644, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0392-y>. [Miyahara:2021:ECB]
- Daiki Miyahara, Itaru Ueda, Yu ichi Hayashi,

- Takaaki Mizuki, and Hideaki Sone. Evaluating card-based protocols in terms of execution time. *International Journal of Information Security*, 20(5): 729–740, October 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00525-4>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00525-4.pdf>. **Mayer:2006:OFA**
- [MWZ06] Alain Mayer, Avishai Wool, and Elisha Ziskind. Offline firewall analysis. *International Journal of Information Security*, 5(3):125–144, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0074-z>. **Mu:2014:RBD**
- [MYLZ14] Chengpo Mu, Meng Yu, Yingjiu Li, and Wanyu Zang. Risk balance defense approach against intrusions for network server. *International Journal of Information Security*, 13(3):255–269, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0214-9>. **Nunez:2014:BPP**
- [NA14] David Nuñez and Isaac Agudo. BlindIdM: a privacy-preserving approach for identity management as a service. *International Journal of Information Security*, 13(2):199–215, April 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0230-4>. **Nali:2006:HTB**
- [NAM06] Deholo Nali, Carlisle Adams, and Ali Miri. Hierarchical time-based information release. *International Journal of Information Security*, 5(2):92–104, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0084-5>. **Ngamboe:2021:RAC**
- [NBA⁺21] Mikaëla Ngamboé, Paul Berthier, Nader Ammari, Katia Dyrda, and José M. Fernandez. Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED). *International Journal of Information Security*, 20(4):

- 621–645, August 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00522-7>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00522-7.pdf>. [NNL20]
- [NCBG23] Or Naim, Doron Cohen, and Irad Ben-Gal. Malicious website identification using design attribute learning. *International Journal of Information Security*, 22(5): 1207–1217, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00686-y>. [NP10]
- [NMBB12] Robert Niebuhr, Mohammed Meziani, Stanislav Bulygin, and Johannes Buchmann. Selecting parameters for secure McEliece-based cryptosystems. *International Journal of Information Security*, 11(3):137–147, June 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0153-2>. [NRC15]
- Nguyen:2020:NGB**
Huy-Trung Nguyen, Quoc-Dung Ngo, and Van-Hoang Le. A novel graph-based approach for IoT botnet detection. *International Journal of Information Security*, 19(5): 567–577, October 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00475-6>.
- Naor:2010:ETR**
Moni Naor and Benny Pinkas. Efficient trace and revoke schemes. *International Journal of Information Security*, 9(6): 411–424, December 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0121-2>.
- Nappa:2015:MDI**
Antonio Nappa, M. Zubair Rafique, and Juan Caballero. The MALICIA dataset: identification and analysis of drive-by download operations. *International Journal of Information Security*, 14(1):15–33, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

- <http://link.springer.com/article/10.1007/s10207-014-0248-7>.
- [NSNK06] Lan Nguyen, Rei Safavi-Naini, and Kaoru Kurosawa. Verifiable shuffles: a formal model and a paillier-based three-round construction with provable security. *International Journal of Information Security*, 5(4):241–255, October 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0004-8>.
- [Nui12] Koji Nuida. Short collusion-secure fingerprint codes against three pirates. *International Journal of Information Security*, 11(2):85–102, April 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0155-8>.
- [NST09] M. Narasimha, J. Solis, and G. Tsudik. Privacy-preserving revocation checking. *International Journal of Information Security*, 8(1):61–75, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0064-z>.
- [NT20] Sanjeet Kumar Nayak and Somanath Tripathy. SEDS: secure and efficient server-aided data deduplication scheme for cloud storage. *International Journal of Information Security*, 19(2):229–240, April 2020.
- [NVB+02] J. M. González Nieto, K. Viswanathan, C. Boyd, A. Clark, and E. Dawson. Key recovery for the commercial environment. *International Journal of Information Security*, 1(3):161–174, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-002-0014-0>.
- [OAJ23] Taiwo Blessing Ogunseyi, Cossi Blaise Avoussoukpo, and Yiqiang Jiang. A systematic review of privacy techniques in recommendation systems. *In-*

- ternational Journal of Information Security*, 22 (6):1651–1664, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00710-1>. [ORK23]
- [OBH⁺20] **Ozawa:2020:SIM**
Seiichi Ozawa, Tao Ban, Naoki Hashimoto, Junji Nakazato, and Jumpei Shimamura. A study of IoT malware activities using association rule learning for darknet sensor data. *International Journal of Information Security*, 19 (1):83–92, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00439-w>. [OSSK16]
- [OO20] **Ogata:2020:SAS**
Wakaha Ogata and Takaaki Otemori. Security analysis of secure kNN and ranked keyword search over encrypted data. *International Journal of Information Security*, 19(4): 419–425, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00461-y>. [OT06]
- Orooji:2023:FAD**
Marmar Orooji, Seyedeh Shaghayegh Rabbanian, and Gerald M. Knapp. Flexible adversary disclosure risk measure for identity and attribute disclosure attacks. *International Journal of Information Security*, 22 (3):631–645, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00654-y>.
- Orencik:2016:MKS**
Cengiz Orencik, Ayse Selcuk, ErKay Savas, and Murat Kantarcioğlu. Multi-keyword search over encrypted data with scoring and search pattern obfuscation. *International Journal of Information Security*, 15(3):251–269, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0294-9>.
- Okeya:2006:SAC**
Katsuyuki Okeya and Tsuyoshi Takagi. Security analysis of CRT-based cryptosystems. *International Journal of Information Security*, 5(3):177–185, July 2006. CODEN ???? ISSN

1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0080-1>. [PC19]

Papanikolaou:2023:ANT

[PAI⁺23]

Alexandros Papanikolaou, Aggelos Alevizopoulos, Christos Ilioudis, Konstantinos Demertzis, and Konstantinos Rantos. An autoML network traffic analyzer for cyber threat detection. *International Journal of Information Security*, 22(5): 1511–1530, October 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00703-0>. [PCK22a]

Prantl:2023:RSG

[PBI⁺23]

Thomas Prantl, André Bauer, Lukas Iffländer, Christian Krupitzer, and Samuel Kounev. Recommendation of secure group communication schemes using multi-objective optimization. *International Journal of Information Security*, 22(5): 1291–1332, October 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00692-0>. [PCK22b]

Patsakis:2019:HID

Constantinos Patsakis and Fran Casino. Hydras and IPFS: a decentralised playground for malware. *International Journal of Information Security*, 18(6): 787–799, December 2019. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00443-0>.

Park:2022:EVC

Jai Hyun Park, Jung Hee Cheon, and Dongwoo Kim. Efficient verifiable computation over quotient polynomial rings. *International Journal of Information Security*, 21(5): 953–971, October 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00590-x>.

Potteiger:2022:DSR

Bradley Potteiger, Feiyang Cai, and Xenofon Koutsoukos. Data space randomization for securing cyber-physical systems. *International Journal of Information Security*, 21(3):597–610, June 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL

- <https://link.springer.com/article/10.1007/s10207-021-00568-1>.
- [PCT22] **Parish:2022:PGU**
Zach Parish, Connor Cushing, and Julie Thorpe. Password guessers under a microscope: an in-depth analysis to inform deployments. *International Journal of Information Security*, 21(2):409–425, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00560-9>. [PDM20]
- [PD21] **Parida:2021:PMC**
Trushna Parida and Suvrojit Das. PageDumper: a mechanism to collect page table manipulation information at run-time. *International Journal of Information Security*, 20(4):603–619, August 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00520-9>. [Pen11]
- [PDB11] **Peng:2011:MOS**
Kun Peng, Ed Dawson, and Feng Bao. Modification and optimisation of a shuffling scheme: stronger security, formal analysis and higher efficiency. *International Journal of Information Security*, 10(1):33–47, February 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0117-y>. [Patil:2020:DVA]
- [Patil:2020:DVA] Rajendra Patil, Harsha Dudeja, and Chirag Modi. Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. *International Journal of Information Security*, 19(2):147–162, April 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00447-w>. [Peng:2011:GEC]
- [Peng:2011:GEC] Kun Peng. A general and efficient countermeasure to relation attacks in mix-based e-voting. *International Journal of Information Security*, 10(1):49–60, February 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0122-1>. [Peng:2012:TDA]
- [Peng:2012:TDA] Kun Peng. Threshold

- distributed access control with public verification: a practical application of PVSS. *International Journal of Information Security*, 11(1):23–31, February 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0151-4>.
- [Pen13] Kun Peng. A shuffle to achieve high efficiency through pre-computation and batch verification. *International Journal of Information Security*, 12(4): 337–345, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0193-x>.
- [PGMLK⁺13] F. Pereñíguez-García, R. Marín-López, G. Kambourakis, A. Ruiz-Martínez, S. Gritzalis, and A. F. Skarmeta-Gómez. KAMU: providing advanced user privacy in Kerberos multi-domain scenarios. *International Journal of Information Security*, 12(6): 505–525, November 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0201-1>.
- [PGMPPC22] Rosa Pericàs-Gornals, Macià Mut-Puigserver, and M. Magdalena Payeras-Capellà. Highly private blockchain-based management system for digital COVID-19 certificates. *International Journal of Information Security*, 21(5): 1069–1090, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00598-3>.
- [PHS22] Cheolhee Park, Dowon Hong, and Changho Seo. Evaluating differentially private decision tree model over model inversion attack. *International Journal of Information Security*, 21(3):1–14, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00564-5>.
- [PJ10] Alwyn R. Pais and Shankar Joshi. A new probabilistic rekeying method for secure multicast groups. *International Journal of Information Security*, 9

- (4):275–286, August 2010. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0108-z>.
- [PKHS23] Saurabh Pandey, Nitesh Kumar, Anand Handa, and Sandeep Kumar Shukla. Evading malware classifiers using RL agent with action-mask. *International Journal of Information Security*, 22(6):1743–1763, December 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00715-w>.
- [Plao9] Rainer Plaga. Biometric keys: suitable use cases and achievable information content. *International Journal of Information Security*, 8(6):447–454, December 2009. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0090-5>.
- [PLA+21] Gregorio Pitolli, Giuseppe Laurenza, Leonardo Aniello, Leonardo Querzoni, and Roberto Baldoni. MalFamAware: automatic family identification and malware classification through online clustering. *International Journal of Information Security*, 20(3):371–386, June 2021. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00509-4>.
- [PM23] Pankaj Pandey and Nishchol Mishra. Phish-Sight: a new approach for phishing detection using dominant colors on web pages and machine learning. *International Journal of Information Security*, 22(4):881–891, August 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00672-4>.
- [PMDS23] Suryakanta Panda, Samrat Mondal, Ashok Kumar Das, and Willy Susilo. Secure access privilege delegation using attribute-based encryption. *International Journal of Information Security*, 22(5):1261–1276, October 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

- <https://link.springer.com/article/10.1007/s10207-023-00690-2>
- Perez-Mendez:2012:CLS** [PPL15]
- [PMPGMLLM12] Alejandro Pérez-Méndez, Fernando Pereñíguez-García, Rafael Marín-López, and Gabriel López-Millán. A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network. *International Journal of Information Security*, 11(6):365–388, November 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0174-5>.
- Pilz:2020:SAS** [PPSS13]
- [PNG+20] M. Pilz, F. Baghaei Naeni, K. Grammont, C. Smaghe, M. Davis, J.-C. Nebel, L. Al-Fagih, and E. Pfluegel. Security attacks on smart grid scheduling and their defences: a game-theoretic approach. *International Journal of Information Security*, 19(4):427–443, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00460-z>; <http://link.springer.com/content/>
- <http://link.springer.com/article/10.1007/s10207-014-0255-8>
- Pitropakis:2015:BRP**
- Nikolaos Pitropakis, Aggelos Pikrakis, and Costas Lambrinouidakis. Behaviour reflects personality: detecting co-residence attacks on Xen-based cloud environments. *International Journal of Information Security*, 14(4):299–305, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0255-8>.
- Phan:2013:ACB**
- Duong-Hieu Phan, David Pointcheval, Siamak F. Shahandashti, and Mario Strefer. Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. *International Journal of Information Security*, 12(4):251–265, August 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0190-0>.
- Priami:2004:PSI**
- Corrado Priami. Preface to the special issue on Security in Global Computing. *International Jour-*

- nal of Information Security*, 2(3-4):125, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0034-z>; <http://link.springer.com/content/pdf/10.1007/s10207-004-0034-z.pdf>. [PSDSNAHJ19]
- Poettering:2017:DAP**
- [PS17] Bertram Poettering and Douglas Stebila. Double-authentication-preventing signatures. *International Journal of Information Security*, 16(1):1-22, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0307-8>. [PSOMS22]
- Picazo-Sanchez:2023:GIP**
- [PSA23] Pablo Picazo-Sanchez and Magnus Almgren. Grid-chain: an investigation of privacy for the future local distribution grid. *International Journal of Information Security*, 22(1):29-46, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00622-6>. [PSTS20]
- Perez-Sola:2019:DSP**
- Cristina Pérez-Solà, Sergi Delgado-Segura, Guillermo Navarro-Arribas, and Jordi Herrera-Joancomartí. Double-spending prevention for Bitcoin zero-confirmation transactions. *International Journal of Information Security*, 18(4):451-463, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0422-4>.
- Picazo-Sanchez:2022:CEC**
- Pablo Picazo-Sanchez, Lara Ortiz-Martin, and Andrei Sabelfeld. Are chrome extensions compliant with the spirit of least privilege? *International Journal of Information Security*, 21(6):1283-1297, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00610-w>.
- Picazo-Sanchez:2020:AYP**
- Pablo Picazo-Sanchez, Juan Tapiador, and Gerardo Schneider. After you, please: browser extensions order attacks and countermeasures. *International Journal of Information Security*, 19(6):

- 623–638, December 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00481-8>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00481-8.pdf>.
- [PV22] C. Prajisha and A. R. Vasudevan. An efficient intrusion detection system for MQTT-IoT using enhanced chaotic salp swarm algorithm and LightGBM. *International Journal of Information Security*, 21(6):1263–1282, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00611-9>.
- [QDW09] Huawang Qin, Yuewei Dai, and Zhiquan Wang. A secret sharing scheme based on (t, n) threshold and adversary structure. *International Journal of Information Security*, 8(5):379–385, October 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0085-2>.
- [QDW+15] Bo Qin, Hua Deng, Qianhong Wu, Josep Domingo-Ferrer, David Naccache, and Yunya Zhou. Flexible attribute-based encryption applicable to secure e-healthcare records. *International Journal of Information Security*, 14(6):499–511, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0272-7>.
- [QLOW09] Karl Quinn, David Lewis, Declan O’Sullivan, and Vincent P. Wade. An analysis of accuracy experiments carried out over of a multi-faceted model of trust. *International Journal of Information Security*, 8(2):103–119, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0069-7>.
- [QLZH15] Huiling Qian, Jiguo Li, Yichen Zhang, and Jinguang Han. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. *Inter-*

Qin:2015:FAB

Bo Qin, Hua Deng, Qianhong Wu, Josep Domingo-Ferrer, David Naccache, and Yunya Zhou. Flexible attribute-based encryption applicable to secure e-healthcare records. *International Journal of Information Security*, 14(6):499–511, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0272-7>.

Quinn:2009:AAE

Karl Quinn, David Lewis, Declan O’Sullivan, and Vincent P. Wade. An analysis of accuracy experiments carried out over of a multi-faceted model of trust. *International Journal of Information Security*, 8(2):103–119, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0069-7>.

Qian:2015:PPP

Huiling Qian, Jiguo Li, Yichen Zhang, and Jinguang Han. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. *Inter-*

- national Journal of Information Security*, 14(6): 487–497, November 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0270-9>.
- [RAC16] Elie Raad, Bechara Al Bouna, and Richard Chbeir. Preventing sensitive relationships disclosure for better social media preservation. *International Journal of Information Security*, 15(2):173–194, April 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0278-9>.
- [RB23] Shubhangi Rastogi and Divya Bansal. A review on fake news detection 3T’s: typology, time of detection, taxonomies. *International Journal of Information Security*, 22(1): 177–212, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00625-3>.
- [RBD02] Ohad Rodeh, Kenneth P. Birman, and Danny Dolev. Using AVL trees for fault-tolerant group key management. *International Journal of Information Security*, 1(2):84–99, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100008>.
- [RBEH15] Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani, and Matthias Hollick. Lightweight energy consumption-based intrusion detection system for wireless sensor networks. *International Journal of Information Security*, 14(2):155–167, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0241-1>.
- [RD16] Y. Sreenivasa Rao and Ratna Dutta. Efficient attribute-based signature and signcryption realizing expressive access structures. *International Journal of Information Security*, 15(1): 81–109, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0000-0>.

- com/article/10.1007/s10207-015-0289-6.
- [RDK18] **Rial:2018:PPS**
 Alfredo Rial, George Danezis, and Markulf Kohlweiss. Privacy-preserving smart metering revisited. *International Journal of Information Security*, 17(1):1–31, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0355-8>. [RHGTSC17]
- [RG13] **Rizomiliotis:2013:SAP**
 Panagiotis Rizomiliotis and Stefanos Gritzalis. On the security of AUTH, a provably secure authentication protocol based on the subspace LPN problem. *International Journal of Information Security*, 12(2):151–154, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0188-z>. [RHL17]
- [RGL16] **Rowe:2016:MPS**
 Paul D. Rowe, Joshua D. Guttman, and Moses D. Liskov. Measuring protocol strength with security goals. *International Journal of Information Security*, 15(6):575–596, November 2016. [RLEM18]
- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0319-z>.
- Ruiz-Heras:2017:AAB**
 A. Ruiz-Heras, P. García-Teodoro, and L. Sánchez-Casado. ADroid: anomaly-based detection of malicious events in Android platforms. *International Journal of Information Security*, 16(4):371–384, August 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0333-1>.
- Ragab-Hassen:2017:KMS**
 Hani Ragab-Hassen and Esmá Lounes. A key management scheme evaluation using Markov processes. *International Journal of Information Security*, 16(3):271–280, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0323-3>; <http://link.springer.com/content/pdf/10.1007/s10207-016-0323-3.pdf>.
- Ribeiro:2018:SRH**
 Carlos Ribeiro, Herbert

- Leitold, Simon Esposito, and David Mitzam. STORK: a real, heterogeneous, large-scale eID management system. *International Journal of Information Security*, 17(5):569–585, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0385-x>. [RMSCR19]
- Reaves:2012:OVT**
- [RM12] Bradley Reaves and Thomas Morris. An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11(4):215–229, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0164-7>. [Roe11a]
- Rebollo-Monedero:2013:MPA**
- [RMPADF13] David Rebollo-Monedero, Javier Parra-Arnau, Claudia Diaz, and Jordi Forné. On the measurement of privacy as an attacker’s estimation error. *International Journal of Information Security*, 12(2):129–149, April 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0126-5>. See erratum [Roe11b]. [Roe11b]
- Ros-Martin:2019:SND**
- Miguel Ros-Martín, Julián Salas, and Jordi Casas-Roma. Scalable non-deterministic clustering-based k -anonymization for rich networks. *International Journal of Information Security*, 18(2):219–238, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0409-1>.
- Roelse:2011:DST**
- Peter Roelse. Dynamic subtree tracing and its application in pay-TV systems. *International Journal of Information Security*, 10(3):173–187, June 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0126-5>. See erratum [Roe11b].
- Roelse:2011:EDS**
- Peter Roelse. Erratum to: Dynamic subtree tracing and its application in pay-TV systems. *International Journal of Information Security*, 10(6):391, November 2011. CODEN ???? ISSN

- 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0141-6>; <http://link.springer.com/content/pdf/10.1007/s10207-011-0141-6.pdf>. See [Roe11a].
- [Rov23] **Rovida:2023:FAH**
Lorenzo Rovida. Fast but approximate homomorphic k -means based on masking technique. [RSD19] *International Journal of Information Security*, 22(6):1605–1619, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00708-9>.
- [RRI⁺19] **Rezvani:2019:AXP**
Mohsen Rezvani, David Rajaratnam, Aleksandar Ignjatovic, Maurice Pagnucco, and Sanjay Jha. Analyzing XACML policies using answer set programming. [RSMA19] *International Journal of Information Security*, 18(4):465–479, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0421-5>.
- [RS18] **Roy:2018:DSC**
Sangita Roy and Ashok Singh Sairam. Distributed star coloring of network for IP traceback. *International Journal of Information Security*, 17(3):315–326, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0366-0>.
- Rastegari:2019:CDV**
Parvin Rastegari, Willy Susilo, and Mohammad Dakhilalian. Certificateless designated verifier signature revisited: achieving a concrete scheme in the standard model. *International Journal of Information Security*, 18(5):619–635, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00430-5>.
- Resende:2019:BMI**
João S. Resende, Patrícia R. Sousa, Rolando Martins, and Luís Antunes. Breaking MPC implementations through compression. *International Journal of Information Security*, 18(4):505–518, August 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0424-2>.

- [RSPMB16] **Rashwan:2016:UTP**
 Hatem A. Rashwan, Agusti Solanas, Domènec Puig, and Antoni Martínez-Ballesté. Understanding trust in privacy-aware video surveillance systems. [Rus04] *International Journal of Information Security*, 15(3):225–234, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0286-9>.
- [RSV23] **Rajic:2023:EWA**
 Branislav Rajić, Zarko Stanisavljević, and Pavle Vuletić. Early web application attack detection using network traffic analysis. [RV03] *International Journal of Information Security*, 22(1):77–91, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00627-1>.
- [RT23] **Rathore:2023:RDL**
 Nemi Chandra Rathore and Somanath Tripathy. Restricting data-leakage using fine-grained access control on OSN objects. [RV19] *International Journal of Information Security*, 22(1):93–106, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00629-z>.
- Russell:2004:TBR**
 Selwyn Russell. Theory and benefits of recursive certificate structures. *International Journal of Information Security*, 2(2):78–90, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0028-2>.
- Ruan:2003:FGB**
 Chun Ruan and Vijay Varadharajan. A formal graph based framework for supporting authorization delegations and conflict resolutions. *International Journal of Information Security*, 1(4):211–222, July 2003. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0018-4>.
- Riesco:2019:LCT**
 R. Riesco and V. A. Villagrà. Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal of Information Security*, 18(6):715–739, December 2019.

- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00433-2>.
- Saifuzzaman:2022:SLR**
- [SAC22] Munshi Saifuzzaman, Tajkia Nuri Ananna, and Farida Chowdhury. A systematic literature review on wearable health data publishing under differential privacy. *International Journal of Information Security*, 21(4):847–872, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00576-1>.
- SAT09**
- [SAH22] Andrew D. Syrmakesis, Cristina Alcaraz, and Nikos D. Hatziaargyriou. Classifying resilience approaches for protecting smart grids against cyber threats. *International Journal of Information Security*, 21(5):1189–1210, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00594-7>.
- Sat20**
- [SAL17] **Shaikh:2017:DCM**
Riaz Ahmed Shaikh, Kameel
- Adi, and Luigi Logrippo. A data classification method for inconsistency and incompleteness detection in access control policy sets. *International Journal of Information Security*, 16(1):91–113, February 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0317-1>.
- Sourour:2009:ESD**
- Meharouech Sourour, Bouhoula Adel, and Abbes Tarek. Ensuring security in depth based on heterogeneous network security technologies. *International Journal of Information Security*, 8(4):233–246, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0077-2>.
- Sattath:2020:IQB**
- Or Sattath. On the insecurity of quantum Bitcoin mining. *International Journal of Information Security*, 19(3):291–302, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00493-9>.

- [SB09] **Shay:2009:CST**
Richard Shay and Elisa Bertino. A comprehensive simulation tool for the analysis of password policies. *International Journal of Information Security*, 8(4):275–289, August 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0084-3>.
- [SB14] **Saikia:2014:PHF**
Navajit Saikia and Prabin K. Bora. Perceptual hash function for scalable video. *International Journal of Information Security*, 13(1):81–93, February 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0211-z>.
- [SB22] **Spence:2022:SBC**
Aaron Spence and Shaun Bangay. Security beyond cybersecurity: side-channel attacks against non-cyber systems and their countermeasures. *International Journal of Information Security*, 21(3):437–453, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00563-6>.
- [SBB19] **Samadani:2019:SPM**
Mohammad Hasan Samadani, Mehdi Berenjkoob, and Marina Blanton. Secure pattern matching based on bit parallelism. *International Journal of Information Security*, 18(3):371–391, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0410-8>.
- [SBCP21] **Schlette:2021:MVC**
Daniel Schlette, Fabian Böhm, Marco Caselli, and Günther Pernul. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, 20(1):21–38, February 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00490-y>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00490-y.pdf>.
- [SBD23] **Seth:2023:LDD**
Abhay Deep Seth, Santosh Biswas, and Amit Kumar Dhar. LDES: detector design for version number attack detection us-

- ing linear temporal logic based on discrete event system. *International Journal of Information Security*, 22(4):961–985, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00665-3>. [SCL⁺18]
- [SBG22] Florian Skopik, Arndt Bonitz, and Günter Göhler. From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. *International Journal of Information Security*, 21(6):1323–1347, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00613-7>. [SCO21]
- [SBS23] Gulab Sah, Subhasish Banerjee, and Sweet Singh. Intrusion detection system over real-time data traffic using machine learning methods with feature selection approaches. *International Journal of Information Security*, 22(1):1–27, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00616-4>. [Scaife:2018:OSR]
- Nolen Scaife, Henry Carter, Lyrissa Lidsky, Rachael L. Jones, and Patrick Traynor. OnionDNS: a seizure-resistant top-level domain. *International Journal of Information Security*, 17(6):645–660, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0391-z>. [Solano:2021:CBB]
- Jesus Solano, Luis Camacho, and Martín Ochoa. Combining behavioral biometrics and session context analytics to enhance risk-based static authentication in web applications. *International Journal of Information Security*, 20(2):181–197, April 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00510-x>. [Stergiopoulos:2022:AAA]
- George Stergiopoulos, Panagiotis Dedousis, and Dimitris Gritzalis. Automatic analysis of attack graphs for risk mitigation and prioritization on

- large-scale and complex networks in Industry 4.0. *International Journal of Information Security*, 21(1):37–59, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00533-4>. [SDW23]
- [SdHZ16] **Skoric:2016:FBR**
Boris Skorić, Sebastiaan J. A. de Hoogh, and Nicola Zannone. Flow-based reputation with uncertainty: evidence-based subjective logic. *International Journal of Information Security*, 15(4):381–402, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0298-5>; <http://link.springer.com/content/pdf/10.1007/s10207-015-0298-5.pdf>. [Sen14]
- [SDR20] **Sowjanya:2020:ECC**
K. Sowjanya, Mou Dasgupta, and Sangram Ray. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *International Journal of Information Security*, 19(1):129–146, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0238-9>. [Sep23]
- Sangari:2023:MRD**
Seema Sangari, Eric Dallah, and Michael Whitman. Modeling reporting delays in cyber incidents: an industry-level comparison. *International Journal of Information Security*, 22(1):63–76, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00623-5>. [Sen:2014:UIW]
- Sevil Sen. Using instance-weighted naive Bayes for adapting concept drift in masquerade detection. *International Journal of Information Security*, 13(6):583–590, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0238-9>. [Sepehrzadeh:2023:MIT]
- Hamed Sepehrzadeh. A method for insider threat assessment by modeling the internal employee interactions. *International Journal of Information Security*, 22(5):

- 1385–1393, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00697-9>. [SGC22]
- [SEXY18] Jae Hong Seo, Keita Emura, Keita Xagawa, and Kazuki Yoneyama. Accumulable optimistic fair exchange from verifiably encrypted homomorphic signatures. *International Journal of Information Security*, 17(2):193–220, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0367-z>. [SGE02]
- [SF17] Ankit Singh and Hervais C. Simo Fhom. Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. *International Journal of Information Security*, 16(2):195–211, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0328-y>. [SGJ19]
- Shah:2022:MLO**
Ankit Shah, Rajesh Ganesan, and Hasan Cam. Maintaining the level of operational effectiveness of a CSOC under adverse conditions. *International Journal of Information Security*, 21(3):637–651, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00573-4>.
- Steinwandt:2002:APB**
Rainer Steinwandt, Willi Geiselmann, and Regine Endsuleit. Attacking a polynomial-based cryptosystem: Polly cracker. *International Journal of Information Security*, 1(3):143–148, November 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-002-0012-2>.
- Shah:2019:MEF**
Ankit Shah, Rajesh Ganesan, and Sushil Jajodia. A methodology for ensuring fair allocation of CSOC effort for alert investigation. *International Journal of Information Security*, 18(2):199–218, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0407-3>.
- Shah:2018:MMM**
- [SGJC18] Ankit Shah, Rajesh Ganesan, Sushil Jajodia, and Hasan Cam. A methodology to measure and monitor level of operational effectiveness of a CSOC. *International Journal of Information Security*, 17(2):121–134, April 2018. CODEN ???? ISSN [SHA20] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0365-1>.
- Saini:2019:YCS**
- [SGLC19] Anil Saini, Manoj Singh Gaur, Vijay Laxmi, and Mauro Conti. You click, I steal: analyzing and detecting click hijacking attacks in web pages. *International Journal of Information Security*, 18(4):481–504, August 2019. CODEN ???? ISSN [SHOL23] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0423-3>.
- Sharma:2023:NAD**
- [SGSS23] Amit Sharma, Brij B. Gupta, Awadhesh Kumar Singh, and V. K. Saraswat. A novel approach for de-
- tection of APT malware using multi-dimensional hybrid Bayesian belief network. *International Journal of Information Security*, 22(1):119–135, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00631-5>.
- Shayesteh:2020:TMS**
- Behshid Shayesteh, Vesal Hakami, and Ahmad Akbari. A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. *International Journal of Information Security*, 19(1):93–110, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00446-x>.
- Suren:2023:PPA**
- Emre Süren, Fredrik Heiding, Johannes Olegård, and Robert Lagerström. PatrioT: practical and agile threat research for IoT. *International Journal of Information Security*, 22(1):213–233, February 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00446-x>.

- com/article/10.1007/s10207-022-00633-3.
- [SHW23] **Song:2023:NFS**
Guangjia Song, Jianhua Hu, and Hui Wang. A novel frame switching model based on virtual MAC in SDN. *International Journal of Information Security*, 22(3):723–736, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00659-7>.
- [SJ09] **Sajedi:2009:SSB**
Hedieh Sajedi and Mansour Jamzad. Secure steganography based on embedding capacity. *International Journal of Information Security*, 8(6):433–445, December 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0089-y>.
- [SJ10] **Sajedi:2010:UCT**
Hedieh Sajedi and Mansour Jamzad. Using contourlet transform and cover selection for secure steganography. *International Journal of Information Security*, 9(5):337–352, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0227-z>.
- [SK06] **Sidiroglou:2006:ETD**
Stelios Sidiroglou and Angelos D. Keromytis. Execution transactions for defending against software failures: use and evaluation. *International Journal of Information Security*, 5(2):77–91, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0083-6>.
- [SK14] **Shin:2014:AAA**
Sooyeon Shin and Taekyong Kwon. AAnA: Anonymous authentication and authorization based on short traceable signatures. *International Journal of Information Security*, 13(5):477–495, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0227-z>.
- [SK16] **Salini:2016:EPA**
P. Salini and S. Kanmani. Effectiveness and performance analysis of model-oriented security requirements engineering to elicit

security requirements: a systematic solution for developing secure software systems. *International Journal of Information Security*, 15(3):319–334, June 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0305-x>. [SKK+17]

Smiliotopoulos:2023:DLM

[SKB23]

Christos Smiliotopoulos, Georgios Kambourakis, and Konstantia Barbatsalou. On the detection of lateral movement through supervised machine learning and an open-source tool to create turnkey datasets from Sysmon logs. *International Journal of Information Security*, 22(6):1893–1919, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00725-8>. [SKLP20]

Sneha:2023:RRT

[SKH+23]

M. Sneha, A. Keerthan Kumar, Nikhil V. Hegde, A. S. Anish, and G. Shobha. RADS: a real-time anomaly detection model for software-defined networks using machine learning. *International Journal of Information Security*, 22(6):1881–1891, December

2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00724-9>.

Sisaat:2017:STM

Khamphao Sisaat, Surin Kittitornkun, Hiroaki Kikuchi, Chaxiong Yukonhiatou, Masato Terada, and Hiroshi Ishii. A spatio-temporal malware and country clustering algorithm: 2012 IIJ MITF case study. *International Journal of Information Security*, 16(5):459–473, October 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0342-0>.

Seo:2020:ERL

Minhye Seo, Suhri Kim, Dong Hoon Lee, and Jong Hwan Park. EMBLEM: (R)LWE-based key encapsulation with a new multi-bit encoding method. *International Journal of Information Security*, 19(4):383–399, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00456-9>.

- [SKY23] **Shukla:2023:QFS**
Ankur Shukla, Basel Katt, and Muhammad Mudassar Yamin. A quantitative framework for security assurance evaluation and selection of cloud services: a case study. [SM10] *International Journal of Information Security*, 22(6):1621–1650, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00709-8>.
- [sLC05] **Lhee:2005:DFB**
Kyung suk Lhee and Steve J. Chapin. Detection of file-based race conditions. *International Journal of Information Security*, 4(1-2): 105–119, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0068-2>. [Smi04]
- [SLGP23] **Sarhan:2023:ZSM**
Mohanad Sarhan, Siamak Layeghy, Marcus Gallagher, and Marius Portmann. From zero-shot machine learning to zero-day attack detection. *International Journal of Information Security*, 22(4): 947–959, August 2023. [SMMN12]
- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00676-0>.
- Skoric:2010:FDS**
Boris Skorić and Marc X. Makkes. Flowchart description of security primitives for controlled physical unclonable functions. *International Journal of Information Security*, 9(5): 327–335, October 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0113-2>.
- Smith:2004:OAP**
Sean W. Smith. Outbound authentication for programmable secure coprocessors. *International Journal of Information Security*, 3(1):28–41, October 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0033-0>.
- Sole:2012:EMT**
Marc Solé, Victor Muntés-Mulero, and Jordi Nin. Efficient microaggregation techniques for large numerical data volumes. *International Journal of In-*

- formation Security*, 11(4): 253–267, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0158-5>.
- [Sne05] Einar Snekkenes. Preface to the special issue on ESORICS 2003. *International Journal of Information Security*, 4(3):133–134, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0054-8>.
- [SNX19] Anastasios Stasinopoulos, Christoforos Ntantogian, and Christos Xenakis. Commix: automating evaluation and exploitation of command injection vulnerabilities in Web applications. *International Journal of Information Security*, 18(1):49–72, February 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0399-z>.
- [SPDR17] Matija Stevanovic, Jens Myrup Pedersen, Alessandro D’Alconzo, and Stefan Ruehrup. A method for identifying compromised clients based on DNS traffic analysis. *International Journal of Information Security*, 16(2):115–132, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0331-3>.
- [SPM13] Z. Cliffe Schreuders, Christian Payne, and Tanya McGill. The functionality-based application confinement model. *International Journal of Information Security*, 12(5):393–422, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0199-4>.
- [SRD⁺21] Sabrina Sicari, Alessandra Rizzardi, Gianluca Dini, Pericle Perazzo, Michele La Manna, and Alberto Coen-Porisini. Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware. *International Journal of Information Security*, 20(5):695–713, October 2021. CODEN ???? ISSN

Snekkenes:2005:PSI

Schreuders:2013:FBA

Stasinopoulos:2019:CAE

Sicari:2021:ABE

Stevanovic:2017:MIC

1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00526-3>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00526-3.pdf>. [SS05a]

Sethi:2020:CAR

[SRK⁺20]

Kamalakanta Sethi, E. Sai Rupesh, Rahul Kumar, Padmalochan Bera, and Y. Venu Madhav. A context-aware robust intrusion detection system: a reinforcement learning-based approach. [SS05b] *International Journal of Information Security*, 19(6):657–678, December 2020. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00482-7>.

Swati:2023:DAD

[SRSM23]

Swati, Sangita Roy, Jawar Singh, and Jimson Mathew. [SS17] Design and analysis of DDoS mitigating network architecture. *International Journal of Information Security*, 22(2):333–345, April 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00635-1>.

Serjantov:2005:PAA

Andrei Serjantov and Peter Sewell. Passive-attack analysis for connection-based anonymity systems. *International Journal of Information Security*, 4(3):172–180, June 2005. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0059-3>.

Skalka:2005:SUB

Christian Skalka and Scott Smith. Static use-based object confinement. *International Journal of Information Security*, 4(1–2):87–104, February 2005. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0049-5>.

Sampangi:2017:HSR

Raghav V. Sampangi and Srinivas Sampalli. HiveSec: security in resource-constrained wireless networks inspired by beehives and bee swarms. *International Journal of Information Security*, 16(4):417–433, August 2017. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0049-5>.

- com/article/10.1007/s10207-016-0341-1.
- Shameli-Sendi:2014:ACA**
- [SSD14] Alireza Shameli-Sendi and Michel Dagenais. ARITO: Cyber-attack response system using accurate risk impact tolerance. *International Journal of Information Security*, 13(4): 367–390, August 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0222-9>. [SSJ22]
- Spreitzenbarth:2015:MSC**
- [SSE⁺15] Michael Spreitzenbarth, Thomas Schreck, Florian Echtler, Daniel Arp, and Johannes Hoffmann. Mobile-Sandbox: combining static and dynamic analysis with machine-learning techniques. *International Journal of Information Security*, 14(2):141–153, April 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0250-0>. [SSL22a]
- Seifi:2015:ATA**
- [SSFB15] Younes Seifi, Suriadi Suriadi, Ernest Foo, and Colin Boyd. Analysis of two authorization protocols using Colored Petri Nets. [SSL22b]
- International Journal of Information Security*, 14(3):221–247, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0243-z>.
- Soltani:2022:CBD**
- Mahdi Soltani, Mahdi Jafari Siavoshani, and Amir Hosein Jahangir. A content-based deep intrusion detection system. *International Journal of Information Security*, 21(3):547–562, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00567-2>.
- Sheikhalishahi:2022:PPD**
- Mina Sheikhalishahi, Andrea Saracino, and Antonio La Marra. Privacy preserving data sharing and analysis for edge-based architectures. *International Journal of Information Security*, 21(1): 79–101, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00542-x>.
- Shin:2022:NSS**
- Hansub Shin, Sungyong

- Sim, and Younho Lee. A new smart smudge attack using CNN. *International Journal of Information Security*, 21(1):25–36, February 2022. CODEN ????? ISSN [SSP14] 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00540-z>.
- [SSM⁺20] Mina Sheikhalishahi, Andrea Saracino, Fabio Martinelli, Antonio La Marra, Mohammed Mejri, and Nadia Tawbi. Digital waste disposal: an automated framework for analysis of spam emails. *International Journal of Information Security*, 19(5):499–522, October 2020. CODEN ????? ISSN [SSR22] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00470-x>.
- [SSN15] Helber Silva, Aldri Santos, and Michele Nogueira. Routing management for performance and security tradeoff in wireless mesh networks. *International Journal of Information Security*, 14(1):35–46, February 2015. CODEN ????? ISSN [SSV22] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0246-9>.
- Sepahi:2014:LBC**
- Reza Sepahi, Ron Steinfeld, and Josef Pieprzyk. Lattice-based certificate-less public-key encryption in the standard model. *International Journal of Information Security*, 13(4):315–333, August 2014. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0215-8>.
- Singh:2022:DAI**
- Ram Govind Singh, Ananya Shrivastava, and Sushmita Ruj. A digital asset inheritance model to convey online persona posthumously. *International Journal of Information Security*, 21(5):983–1003, October 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00593-8>.
- Singh:2022:IAM**
- Jaya Singh, Ayush Sinha, and Om Prakash Vyas. Insider attack mitigation in a smart metering infrastructure using reputation

- score and blockchain technology. *International Journal of Information Security*, 21(3):527–546, June 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00561-8>. [STW⁺23]
- [SSVC16] Petr Susil, Pouyan Sepehrdad, Serge Vaudenay, and Nicolas Courtois. On selection of samples in algebraic attacks and a new technique to find hidden low degree equations. *International Journal of Information Security*, 15(1):51–65, February 2016. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0295-8>. [SV11]
- [STD21] Georgios Spathoulas, Georgios Theodoridis, and Georgios-Paraskevas Damiris. Using homomorphic encryption for privacy-preserving clustering of intrusion detection alerts. *International Journal of Information Security*, 20(3):347–370, June 2021. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00506-7>. [Shi:2023:SAM]
- Sibo Shi, Shengwei Tian, Bo Wang, Tiejun Zhou, and Guanxin Chen. SFCG-Droid: Android malware detection based on sensitive function call graph. *International Journal of Information Security*, 22(5):1115–1124, October 2023. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00679-x>. [Saxena:2011:DRE]
- Nitesh Saxena and Jonathan Voris. Data remanence effects on memory-based entropy collection for RFID systems. *International Journal of Information Security*, 10(4):213–222, August 2011. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0139-0>. [Sermpinis:2021:DDT]
- Thomas Sermpinis, George Vlahavas, Konstantinos Karasavvas, and Athena Vakali. DeTRACT: a decentralized, transparent, immutable and open PKI certificate framework. *In-*

- ternational Journal of Information Security*, 20(4): 553–570, August 2021. [TCE23]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00518-3>.
- [SXZC20] Lixue Sun, Chunxiang Xu, Yuan Zhang, and Kefei Chen. Public data integrity auditing without homomorphic authenticators from indistinguishability obfuscation. *International Journal of Information Security*, 19(6): 711–720, December 2020. [TCS+20]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00486-8>.
- [TBGB20] Sona Taheri, Adil M. Bagirov, Iqbal Gondal, and Simon Brown. Cyberattack triage using incremental clustering for intrusion detection systems. *International Journal of Information Security*, 19(5):597–607, October 2020. [TCT22]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00478-3>.
- Tuna:2023:TNH**
Omer Faruk Tuna, Ferhat Ozgur Catak, and M. Taner Eskil. TENET: a new hybrid network architecture for adversarial defense. *International Journal of Information Security*, 22(4): 987–1004, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00675-1>.
- Takahashi:2020:MGE**
Takeshi Takahashi, Rodrigo Roman Castro, Bilhanan Silverajan, Ryan K. L. Ko, and Said Tabet. Message from the guest editors. *International Journal of Information Security*, 19(1):1–2, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00472-9>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00472-9.pdf>.
- Tommasi:2022:BMB**
Franco Tommasi, Christian Catalano, and Ivan Taurino. Browser-in-the-Middle (BitM) attack. *International Journal of Information Security*, 21

- (2):179–189, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00548-5>.
- [TDGL23] **Tsohou:2023:CIS**
 Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinouidakis. Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, 22(3):737–748, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00660-8>.
- [TDRR20] **Tiloca:2020:GRB**
 Marco Tiloca, Gianluca Dini, Kiki Rizki, and Shahid Raza. Group rekeying based on member join history. *International Journal of Information Security*, 19(4):343–381, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00451-0>.
- [TG05] **Trostle:2005:TIS**
 Jonathan Trostle and Bill Gossman. Techniques for improving the security and manageability of IPsec policy. *International Journal of Information Security*, 4(3):209–226, June 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0064-6>.
- [TGNA22] **Torra:2022:PPF**
 Vicenç Torra, Edgar Galván, and Guillermo Navarro-Arribas. PSO + FL = PAASO: particle swarm optimization + federated learning = privacy-aware agent swarm optimization. *International Journal of Information Security*, 21(6):1349–1359, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00614-6>.
- [TGS17] **Tiloca:2017:IRD**
 Marco Tiloca, Christian Gehrman, and Ludwig Seitz. On improving resistance to Denial of Service and key provisioning scalability of the DTLS handshake. *International Journal of Information Security*, 16(2):173–193, April 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-00451-0>.

- com/article/10.1007/s10207-016-0326-0.
- [Tip22] **Tiplea:2022:NPD**
 Ferucio Laurentiu Tiplea. Narrow privacy and desynchronization in Vaudenay's RFID model. *International Journal of Information Security*, 21(3):563–575, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00569-0>. [TMM+19]
- [TKKO20] **Takase:2020:PIE**
 Hayate Takase, Ryotaro Kobayashi, Masahiko Kato, and Ren Ohmura. A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information. *International Journal of Information Security*, 19(1):71–81, February 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00437-y>. [TMP13]
- [TLX09] **Tian:2009:LSN**
 Daxin Tian, Yanheng Liu, and Yang Xiang. Large-scale network intrusion detection based on distributed learning algorithm. *International Journal of Information Security*, 8(1):25–35, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0061-2>. [Takahashi:2019:SSF]
- Kenta Takahashi, Takahiro Matsuda, Takao Murakami, Goichiro Hanaoka, and Masakatsu Nishigaki. Signature schemes with a fuzzy private key. *International Journal of Information Security*, 18(5):581–617, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00428-z>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00428-z.pdf>. [Tormo:2013:DAI]
- Ginés Dólera Tormo, Gabriel López Millán, and Gregorio Martínez Pérez. Definition of an advanced identity management infrastructure. *International Journal of Information Security*, 12(3):173–200, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0189-y>.

- [TNA23] **Torra:2023:ADR**
 Vicenç Torra and Guillermo Navarro-Arribas. Attribute disclosure risk for k -anonymity: the case of numerical data. *International Journal of Information Security*, 22(6):2015–2024, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00730-x>. [TS20]
- [TND⁺15] **Tonicelli:2015:ITS**
 Rafael Tonicelli, Anderson C. A. Nascimento, Rafael Dowsley, Jörn Müller-Quade, Hideki Imai, Goichiro Hanaoka, and Akira Otsuka. Information-theoretically secure oblivious polynomial evaluation in the commodity-based model. *International Journal of Information Security*, 14(1):73–84, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0247-8>. [TS22]
- [Tor20] **Torra:2020:RDP**
 Vicenç Torra. Random dictatorship for privacy-preserving social choice. *International Journal of Information Security*, 19(5):537–545, October 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00474-7>. [TS20]
- Tavizi:2020:LPS**
 Tina Tavizi and Mehdi Shajari. A language and a pattern system for temporal property specification: advanced metering infrastructure case study. *International Journal of Information Security*, 19(6):695–710, December 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00483-6>.
- Templ:2022:SOM**
 Matthias Templ and Murat Sariyar. A systematic overview on methods to protect sensitive data provided for various analyses. *International Journal of Information Security*, 21(6):1233–1246, December 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00607-5>.

- [TSMH19] **Toreini:2019:DEW**
 Ehsan Toreini, Siamak F. Shahandashti, Maryam Mehrnezhad, and Feng Hao. DOMtegrity: ensuring web page integrity against malicious browser extensions. *International Journal of Information Security*, 18(6):801–814, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00442-1>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00442-1.pdf>.
- [TWP08] **Tartary:2008:CAM**
 Christophe Tartary, Huaxiong Wang, and Josef Pieprzyk. A coding approach to the multicast stream authentication problem. *International Journal of Information Security*, 7(4):265–283, August 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0048-4>.
- [TSZ22] **Tan:2022:CPQ**
 Teik Guan Tan, Pawel Szalachowski, and Jianying Zhou. Challenges of post-quantum digital signing in real-world applications: a survey. *International Journal of Information Security*, 21(4):937–952, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00587-6>.
- [TTS+06] **Tsunoo:2006:ICA**
 Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Hiroyasu Kubo, and Kazuhiko Minematsu. Improving cache attacks by considering cipher structure. *International Journal of Information Security*, 5(3):166–176, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0079-7>.
- [TZH04] **Teller:2004:UAC**
 David Teller, Pascal Zimmer, and Daniel Hirschhoff. Using ambients to control resources. *International Journal of Information Security*, 2(3–4):126–144, August 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0035-y>.

- [UBK23] **Ullah:2023:PTA**
 Imdad Ullah, Roksana Boreli, and Salil S. Kanhere. Privacy in targeted advertising on mobile devices: a survey. [Vaj16] *International Journal of Information Security*, 22(3):647–678, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00655-x>.
- [UMN+20] **Ueda:2020:SIR**
 Itaru Ueda, Daiki Miyahara, Akihiro Nishimura, Yu ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. [VCD21] Secure implementations of a random bisection cut. *International Journal of Information Security*, 19(4):445–452, August 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00463-w>.
- [Ust11] **Ustaoglu:2011:IIB**
 Berkant Ustaoglu. Integrating identity-based and certificate-based authenticated key exchange protocols. [VdWZ14] *International Journal of Information Security*, 10(4):201–212, August 2011. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-00494-8>.
- Vajda:2016:ATA**
 István Vajda. On the analysis of time-aware protocols in universal composability framework. *International Journal of Information Security*, 15(4):403–412, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0300-2>.
- VandenBroeck:2021:OIS**
 Jens Van den Broeck, Bart Coppens, and Bjorn De Sutter. Obfuscated integration of software protections. *International Journal of Information Security*, 20(1):73–101, February 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00494-8>.
- Veeningen:2014:DMC**
 Meilof Veeningen, Benne de Weger, and Nicola Zanone. Data minimisation in communication protocols: a formal analysis framework and application to identity management. *In-*

- ternational Journal of Information Security*, 13(6): 529–569, November 2014. [VL13]
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0235-z>.
- [VH19] **Vora:2019:KBP**
Aishwarya Vipul Vora and Saumya Hegde. Keyword-based private searching on cloud data along with keyword association and dissociation using cuckoo filter. *International Journal of Information Security*, 18(3):305–319, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0418-0>. [VMCR23]
- [VHT09] **Vasserman:2009:IKN**
Eugene Y. Vasserman, Nicholas Hopper, and James Tyra. SILENT-KNOCK: practical, provably undetectable authentication. *International Journal of Information Security*, 8(2):121–135, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0070-1>. [vOLW05]
- Vrakas:2013:IDP**
Nikos Vrakas and Costas Lambrinouidakis. An intrusion detection and prevention system for IMS and VoIP services. *International Journal of Information Security*, 12(3):201–217, June 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0187-0>.
- Velasquez:2023:SRS**
Juan Miguel López Velásquez, Sergio Mauricio Martínez Monterrubio, Luis Enrique Sánchez Crespo, and David Garcia Rosado. Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*, 22(3):691–711, June 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00657-9>.
- vonOheimb:2005:ASM**
David von Oheimb, Volkmar Lotz, and Georg Walter. Analyzing SLE 88 memory management security using Interacting State Machines. *International Journal of Information Security*, 4(3):155–171, June

2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0057-5>.

vanOorschot:2006:MSD

[vORM06]

Paul C. van Oorschot, Jean-Marc Robert, and Miguel Vargas Martin. A monitoring system for detecting repeated packets with applications to computer worms. *International Journal of Information Security*, 5(3):186–199, July 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0081-8>.

[VSN22]

Vasiliadis:2015:GAM

[VPI15]

Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. GPU-assisted malware. *International Journal of Information Security*, 14(3):289–297, June 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0262-9>.

[VSR15]

Vanrenen:2006:DSM

[VSM06]

Gabriel Vanrenen, Sean Smith, and John Marchesini. Distributing security-mediated PKI. *International Journal of Infor-*

mation Security, 5(1):3–17, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0076-x>.

Vlachos:2022:SOS

Vasileios Vlachos, Yannis C. Stamatiou, and Sotiris Nikolettseas. The SAINT observatory subsystem: an open-source intelligence tool for uncovering cybersecurity threats. *International Journal of Information Security*, 21(5):1091–1106, October 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00599-2>.

Valenzuela:2015:MAO

Michael Valenzuela, Ferenc Szidarovszky, and Jerzy Rozenblit. A multiresolution approach for optimal defense against random attacks. *International Journal of Information Security*, 14(1):61–72, February 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0245-x>.

- [WAB⁺09] **Wu:2009:IDV** Yu-Sung Wu, Vinita Apte, Saurabh Bagchi, Sachin Garg, and Navjot Singh. Intrusion detection in voice over IP environments. *International Journal of Information Security*, 8(3): 153–172, June 2009. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0071-0>. [WGH23]
- [Wai04] **Waidner:2004:P** Michael Waidner. Preface. *International Journal of Information Security*, 3(1):1, October 2004. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0051-y>; <http://link.springer.com/content/pdf/10.1007/s10207-004-0051-y.pdf>. [WGMB13]
- [WCS20] **Wu:2020:CIB** Chunhui Wu, Xiaofeng Chen, and Willy Susilo. Concise ID-based mercurial functional commitments and applications to zero-knowledge sets. *International Journal of Information Security*, 19(4): 453–464, August 2020. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0203-z>. [WHS18]
- Wang:2023:ANM** Runzheng Wang, Jian Gao, and Shuhua Huang. AIHGAT: a novel method of malware detection and homology analysis using assembly instruction heterogeneous graph. *International Journal of Information Security*, 22(5): 1423–1443, October 2023. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00699-7>.
- Wang:2013:USM** Pu Wang, Marta C. González, Ronaldo Menezes, and Albert-László Barabási. Understanding the spread of malicious mobile-phone programs and their damage potential. *International Journal of Information Security*, 12(5): 383–392, October 2013. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0203-z>.
- Wangen:2018:FEI** Gaute Wangen, Christoffer Hallstensen, and Einar

- Snekkenes. A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17(6): 681–699, November 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0382-0>; <http://link.springer.com/content/pdf/10.1007/s10207-017-0382-0.pdf>. [WMS⁺19]
- [WLLW14] Tzong-Sun Wu, Ming-Lun Lee, Han-Yu Lin, and Chao-Yuan Wang. Shoulder-surfing-proof graphical password authentication scheme. *International Journal of Information Security*, 13(3):245–254, June 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0216-7>. [WPD18]
- [wLW05] Kong wei Lye and Jeanette M. Wing. Game strategies in network security. *International Journal of Information Security*, 4(1-2):71–86, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0060-x>. [Wu:2019:TPP]
- Ge Wu, Yi Mu, Willy Susilo, Fuchun Guo, and Futai Zhang. Threshold privacy-preserving cloud auditing with multiple uploaders. *International Journal of Information Security*, 18(3):321–331, June 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0420-6>. [Wu:2014:SSP]
- Yujue Wang, HweeHwa Pang, and Robert H. Deng. Verifiably encrypted cascade-instantiable blank signatures to secure progressive decision management. *International Journal of Information Security*, 17(3):347–363, June 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0372-2>. [Wang:2018:VEC]
- [WR08] XiaoFeng Wang and Michael K. Reiter. A multi-layer framework for puzzle-based denial-of-service defense. *International Journal of Information Security*, 7(4):243–263, August 2008. [Wang:2005:GSN]
- [Wang:2008:MLF]

- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0042-x>.
- Wei:2015:TPE**
- [WR15] Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-expression searches. *International Journal of Information Security*, 14(5): 397–416, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0268-3>; <http://link.springer.com/content/pdf/10.1007/s10207-014-0268-3.pdf>. [WW07]
- Wang:2016:SSE**
- [WT16] Yuyu Wang and Keisuke Tanaka. Strongly simulation-extractable leakage-resilient NIZK. *International Journal of Information Security*, 15(1):67–79, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0291-z>.
- Wang:2021:SLR**
- [WT21] Yuntao Wang and Tsuyoshi Takagi. Studying lattice reduction algorithms improved by quick reordering technique. *International Journal of Information Security*, 20(2):257–268, April 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00501-y>.
- Wu:2007:RFT**
- Zhengping Wu and Alfred C. Weaver. Requirements of federated trust management for service-oriented architectures. *International Journal of Information Security*, 6(5): 287–296, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0027-9>.
- Wang:2023:DAM**
- Kai Wang, Jinxia Wu, Tianqing Zhu, Wei Ren, and Ying Hong. Defense against membership inference attack in graph neural networks through graph perturbation. *International Journal of Information Security*, 22(2):497–509, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-0027-9>.

- com/article/10.1007/s10207-022-00646-y.
- [WYL⁺12] **Wang:2012:SGN**
 Yuanzhuo Wang, Min Yu, Jingyuan Li, Kun Meng, Chuang Lin, and Xueqi Cheng. Stochastic game net and applications in security analysis for enterprise network. *International Journal of Information Security*, 11 (1):41–52, February 2012. [XSA13] CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0148-z>.
- [WZ07] **Wang:2007:HDA**
 Shujing Wang and Yan Zhang. Handling distributed authorization with delegation through answer set programming. *International Journal of Information Security*, 6 (1):27–46, January 2007. [XZ21] CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0008-4>.
- [XCW⁺12] **Xin:2012:RAA**
 Zhi Xin, Huiyu Chen, Xince Wang, Peng Liu, Sencun Zhu, Bing Mao, and Li Xie. Replacement attacks: automatically evading behavior-based software birthmark. *International Journal of Information Security*, 11 (5):293–304, October 2012. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0170-9>.
- Xu:2013:VBP**
 Wenjuan Xu, Mohamed Shehab, and Gail-Joon Ahn. Visualization-based policy analysis for SELinux: framework and user study. *International Journal of Information Security*, 12 (3):155–171, June 2013. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0180-7>.
- Xu:2021:SLR**
 Jia Xu and Jianying Zhou. Strong leakage-resilient encryption: enhancing data confidentiality by hiding partial ciphertext. *International Journal of Information Security*, 20 (2):141–159, April 2021. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-020-00487-7>.

- [YA22] **Yildirim:2022:MIT**
 Metehan Yildirim and Emin Anarim. Mitigating insider threat by profiling users based on mouse usage pattern: ensemble learning and frequency domain analysis. *International Journal of Information Security*, 21 (2):239–251, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00544-9>. [YAY+21]
- [YAM+15] **Yu:2015:EPR**
 Yong Yu, Man Ho Au, Yi Mu, Shaohua Tang, Jian Ren, Willy Susilo, and Liju Dong. Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. *International Journal of Information Security*, 14(4):307–318, August 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0263-8>. [YKP22]
- [Yan21] **Yankson:2021:CIP**
 Benjamin Yankson. Continuous improvement process (CIP)-based privacy-preserving framework for smart connected toys. *International Journal of Information Security*, 20(6):849–869, December 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00535-2>. [Yamauchi:2021:AKO]
- Toshihiro Yamauchi, Yohei Akao, Ryota Yoshitani, Yuichi Nakamura, and Masaki Hashimoto. Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes. *International Journal of Information Security*, 20(4):461–473, August 2021. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00514-7>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00514-7.pdf>. [Yichiet:2022:SAL]
- Aun Yichiet, Yen-Min Jasmine Khaw, and Vasaki Ponnusamy. A semantic-aware log generation method for network activities. *International Journal of Information Security*, 21 (2):161–177, April 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

- <https://link.springer.com/article/10.1007/s10207-021-00547-6>.
- Yu:2019:UUP**
- [YL19] Xiaoying Yu and Qi Liao. Understanding user passwords through password prefix and postfix (P3) graph analysis and visualization. *International Journal of Information Security*, 18(5): 647–663, October 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00432-3>.
- Yohan:2020:FSB**
- [YL20] Alexander Yohan and Nai-Wei Lo. FOTB: a secure blockchain-based firmware update framework for IoT environment. *International Journal of Information Security*, 19(3):257–278, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00467-6>.
- Yang:2018:NSS**
- [YLL+18] Zheng Yang, Chao Liu, Wanping Liu, Daigu Zhang, and Song Luo. A new strong security model for stateful authenticated group key exchange. *International Journal of Information Security*, 17(4): 423–440, August 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0373-1>.
- Yildirim:2019:EUI**
- [YM19] M. Yildirim and I. Mackie. Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18(6): 741–759, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00429-y>; <http://link.springer.com/content/pdf/10.1007/s10207-019-00429-y.pdf>.
- Yaacoub:2022:RCS**
- [YNC22] Jean-Paul A. Yaacoub, Hassan N. Noura, and Ali Chehab. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1): 115–158, February 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00545-8>.

- [Yon18] **Yoneyama:2018:FMR**
 Kazuki Yoneyama. Formal modeling of random oracle programmability and verification of signature unforgeability using task-PIOAs. *International Journal of Information Security*, 17(1):43–66, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0352-y>.
- [You06] **Young:2006:CEU**
 Adam L. Young. Cryptoviral extortion using Microsoft’s crypto API. *International Journal of Information Security*, 5(2):67–76, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0082-7>.
- [YOV09] **Yoshino:2009:BMM**
 Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume. Bipartite modular multiplication with twice the bit-length of multipliers. *International Journal of Information Security*, 8(1):13–23, February 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0165-6>.
- [YP06] **Yeo:2006:SWE**
 Gary S.-W. Yeo and Raphael C.-W. Phan. On the security of the WinRAR encryption feature. *International Journal of Information Security*, 5(2):115–123, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0086-3>.
- [YR12] **Yaseen:2012:ITM**
 Qussai Yaseen and Brajendra Panda. Insider threat mitigation: preventing unauthorized knowledge acquisition. *International Journal of Information Security*, 11(4):269–280, August 2012. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0165-6>.
- [YRW14] **Yasmin:2014:PSP**
 Rehana Yasmin, Eike Ritter, and Guilin Wang. Provable security of a pairing-free one-pass authenticated key establishment protocol for wireless sensor networks. *International Journal of In-*

- formation Security*, 13(5): 453–465, October 2014. CODEN ????. ISSN [YSM16] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0224-7>.
- [YSD+20] **Yeh:2020:SIS**
Kuo-Hui Yeh, Chunhua Su, Robert H. Deng, Moti Yung, and Mirosław Kutylowski. Special issue on security and privacy of blockchain technologies. *International Journal of Information Security*, 19(3):243–244, June 2020. CODEN ????. ISSN [YWW22] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-020-00496-6>; <http://link.springer.com/content/pdf/10.1007/s10207-020-00496-6.pdf>.
- [YSM10] **Yuen:2010:HCI**
Tsz Hon Yuen, Willy Susilo, and Yi Mu. How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, 9(4): 297–311, August 2010. CODEN ????. ISSN [YYH+23] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0110-5>.
- Yang:2016:MGE**
Guomin Yang, Willy Susilo, and Yi Mu. Message from the Guest Editors. *International Journal of Information Security*, 15(2):223–224, April 2016. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0315-3>; <http://link.springer.com/content/pdf/10.1007/s10207-016-0315-3.pdf>.
- Yang:2022:SAI**
Xiaodong Yang, Wenjia Wang, and Caifen Wang. Security analysis and improvement of a privacy-preserving authentication scheme in VANET. *International Journal of Information Security*, 21(6):1361–1371, December 2022. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00617-3>.
- Yang:2023:AEA**
Zhen Yang, Shisong Yang, Yunbo Huang, José-Fernán Martínez, Lourdes López, and Yuwen Chen. AAIA: an efficient aggregation scheme against inverting attack for federated learning. *International Jour-*

- nal of Information Security*, 22(4):919–930, August 2023. CODEN ???? ISSN [ZBD06] 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00670-6>.
- [YYK⁺18] **Yoneyama:2018:MCK**
Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, and Tomohide Yamamoto. Multi-cast key distribution: scalable, dynamic and provably secure construction. *International Journal of Information Security*, 17(5): 513–532, October 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0389-6>. [ZD22]
- [ZBC23] **Zeghida:2023:SMP**
Hayette Zeghida, Mehdi Boulaiche, and Ramdane Chikh. Securing MQTT protocol for IoT environment using IDS based on ensemble learning. *International Journal of Information Security*, 22(4): 1075–1086, August 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00681-3>. [Zen22]
- Zhou:2006:MTI**
Jianying Zhou, Feng Bao, and Robert Deng. Minimizing TTP’s involvement in signature validation. *International Journal of Information Security*, 5(1):37–47, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0072-1>.
- Zabihimayvan:2022:FLR**
Mahdieh Zabihimayvan and Derek Doran. A first look at references from the dark to the surface web world: a case study in Tor. *International Journal of Information Security*, 21(4):739–755, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00580-z>.
- Zenitani:2022:MOC**
Kengo Zenitani. A multi-objective cost-benefit optimization algorithm for network hardening. *International Journal of Information Security*, 21(4): 813–832, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00580-z>.

- com/article/10.1007/s10207-022-00586-7.
- Zhang:2007:FBT**
- [ZGC07] Jie Zhang, Ali A. Ghorbani, and Robin Cohen. A familiarity-based trust model for effective selection of sellers in multiagent e-commerce systems. *International Journal of Information Security*, 6(5): 333–344, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0025-y>. [Zha23]
- Zulkernine:2007:ISS**
- [ZGK07] Mohammad Zulkernine, Mathews Graves, and Muhammad Umair Ahmed Khan. Integrating software specifications into intrusion detection. *International Journal of Information Security*, 6(5): 345–357, September 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0023-0>. [ZH22]
- Zhang:2023:ISF**
- [ZGRS23] Denghui Zhang, Zhaoquan Gu, Lijing Ren, and Muhammad Shafiq. An interpretability security framework for intelligent decision support systems based on saliency map. *International Journal of Information Security*, 22(5): 1249–1260, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00689-9>.
- Zhang:2023:AOS**
- Yin Sheng Zhang. Analysis of OGPU security effect and data assembly verification under semi-network OS architecture. *International Journal of Information Security*, 22(5): 1497–1509, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00702-1>.
- Zhang:2022:DTA**
- Xiaokuan Zhang, Jihun Hamm, and Yinqian Zhang. Defeating traffic analysis via differential privacy: a case study on streaming traffic. *International Journal of Information Security*, 21(3):689–706, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00574-3>.

- [ZJS22] **Zulfiqar:2022:TAR**
Maryam Zulfiqar, Muhammad Umar Janjua, and Jack W. Stokes. Tracking adoption of revocation and cryptographic features in X.509 certificates. *International Journal of Information Security*, 21(3):653–668, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00572-5>.
- [ZLGZ19] **Zhang:2019:FGA**
Tao Zhang, Wang Hao Lee, Mingyuan Gao, and Jianying Zhou. File Guard: automatic format-based media file sanitization. *International Journal of Information Security*, 18(6):701–713, December 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00440-3>.
- [ZKP+23] **Zhou:2023:IDA**
Hanxun Zhou, Longyu Kang, Hong Pan, Guo Wei, and Yong Feng. An intrusion detection approach based on incremental long short-term memory. *International Journal of Information Security*, 22(2):433–446, April 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00632-4>.
- [ZLJW20] **Zhou:2020:IFV**
Yuanjian Zhou, Yining Liu, Chengshun Jiang, and Shulan Wang. An improved FOO voting scheme using blockchain. *International Journal of Information Security*, 19(3):303–310, June 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00457-8>.
- [ZL06] **Zhou:2006:P**
Jianying Zhou and Javier Lopez. Preface. *International Journal of Information Security*, 5(2):65–66, April 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL
- [ZLL12] **Zhou:2012:MGE**
Jianying Zhou, Xuejia Lai, and Hui Li. Message from the Guest Editors. *International Journal of Information Security*, 11(5):291–292, October 2012. CODEN ???? ISSN 1615-5262 (print), 1615-

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0172-7>; <http://link.springer.com/content/pdf/10.1007/s10207-012-0172-7.pdf>.
- [ZLZL20] **Zhang:2020:FAB** Yanting Zhang, Jianwei Liu, Zongyang Zhang, and Weiran Liu. FDCO: attribute-based fast data cloud-outsourcing scheme for mobile devices. *International Journal of Information Security*, 19(6): 639–656, December 2020. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00480-9>. [ZO13]
- [ZM07] **Zheng:2007:DSL** Lantian Zheng and Andrew C. Myers. Dynamic security labels and static information flow control. *International Journal of Information Security*, 6(2–3):67–84, March 2007. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0019-9>. [ZP23]
- [ZMS22] **Zia:2022:SIE** Unsub Zia, Mark McCartney, and Ali Sajjad. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, 21(4):917–935, August 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-022-00588-5>. **Zakerzadeh:2013:DSA** Hessam Zakerzadeh and Sylvia L. Osborn. Delay-sensitive approaches for anonymizing numerical streaming data. *International Journal of Information Security*, 12(5): 423–437, October 2013. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0196-7>. **Zacharis:2023:AAA** Alexandros Zacharis and Constantinos Patsakis. AiCEF: an AI-assisted cyber exercise content generation framework using named entity recognition. *International Journal of Information Security*, 22(5): 1333–1354, October 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00000-0>.

- com/article/10.1007/s10207-023-00693-z.
- Zhang:2014:DFA**
- [ZRJ14] Meng Zhang, Anand Raghunathan, and Niraj K. Jha. A defense framework against malware and vulnerability exploits. *International Journal of Information Security*, 13(5):439–452, October 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0233-1>.
- Zyout:2023:MCA**
- [ZSN23] Mo'ath Zyout, Raed Shatnawi, and Hassan Najadat. Malware classification approaches utilizing binary and text encoding of permissions. *International Journal of Information Security*, 22(6):1687–1712, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00712-z>.
- Zhang:2022:RLA**
- [ZTG22] Lu Zhang, Arie Taal, and Paola Grosso. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*, 21(3):509–525, June 2022. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00566-3>.
- Ziza:2023:DED**
- [ZTV23] Kristijan Ziza, Predrag Tadić, and Pavle Vuletić. DNS exfiltration detection in the presence of adversarial attacks and modified exfiltrator behaviour. *International Journal of Information Security*, 22(6):1865–1880, December 2023. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-023-00723-w>.
- Zhou:2015:GCR**
- [ZVH15] Lan Zhou, Vijay Varadharajan, and Michael Hitchens. Generic constructions for role-based encryption. *International Journal of Information Security*, 14(5):417–430, October 2015. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0267-4>.
- Zhang:2017:CIB**
- [ZWQ⁺17] Lei Zhang, Qianhong Wu, Bo Qin, Hua Deng, Jiang-

- tao Li, Jianwei Liu, and Wenchang Shi. Certificateless and identity-based authenticated asymmetric group key agreement. *International Journal of Information Security*, 16(5): 559–576, October 2017. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0339-8>.
Zhang:2020:CBE
- [ZWX20] Shufan Zhang, Lili Wang, and Hu Xiong. Chain-integrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, 19(3):323–341, June 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-00465-8>.
Zhang:2022:THG
- [ZZG19] Zheng Zhang, Shaohao Xie, and Fangguo Zhang. Topology-hiding garbled circuits without universal circuits. *International Journal of Information Security*, 21(2):341–356, April 2022. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00556-5>.
Zheng:2019:IDR
- [ZZZ+11] Wen Tao Zhu, Yang Xiang, Jianying Zhou, Robert H. Deng, and Feng Bao. Secure localization with attack detection in wireless sensor networks. *International Journal of Information Security*, 10(3):155–171, June 2011. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0402-8>.
Zhu:2011:SLA
- [ZZH08] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang. A note on the Ate pairing. *International Journal of Information Security*, 10(3):323–341, June 2020. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <https://link.springer.com/article/10.1007/s10207-021-00556-5>.
Zhao:2008:NAP

formation Security, 7(6): 379–382, November 2008. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0054-1>.

Zheng:2010:AAB

[ZZW⁺10]

Ruijuan Zheng, Mingchuan Zhang, Qingtao Wu, Shibao Sun, and Jiexin Pu. Analysis and application of Bio-Inspired Multi-Net Security Model. *International Journal of Information Security*, 9(1):1–17, February 2010. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0091-4>.