

# 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](mailto:beebe@math.utah.edu), [beebe@acm.org](mailto:beebe@acm.org),  
[beebe@computer.org](mailto:beebe@computer.org) (Internet)  
WWW URL: <http://www.math.utah.edu/~beebe/>

23 May 2019  
Version 1.07

## Title word cross-reference

[BM05, Sne05]. **2004** [DSY06]. **2012**  
[SKK<sup>+</sup>17]. **2013** [BJ15].

$(t, n)$  [QDW09].  $2^w$  [Bae10].  $k$   
[BDD01, MU18, RMSCR19].  $n$  [CC12].  $O(n)$   
[DYDW10].  $t$  [BDD01].

**3** [ABM<sup>+</sup>12]. **3GPP** [EWR<sup>+</sup>09].

**88** [vOLW05].

**AAnA** [SK14]. **absence** [AvO13]. **absolute**  
[AvO13]. **abstract** [BLM11, DM07, MS14].  
**abstract-based** [BLM11]. **abstraction**  
[MLCS16]. **abused** [CYA<sup>+</sup>18]. **Acceptable**  
[BB04b]. **Access**  
[Lop18, SAL17, ACF17, ACBC<sup>+</sup>15, BLM11,  
CF03, CK08, CZ06, HSMY12, JSMG18a,  
KAC16, KAC17, Kud02, LD17, LRB<sup>+</sup>10,  
MS15, Pen12, PMPGMLL12, RD16].  
**account** [BRS06]. **accounts** [ASN<sup>+</sup>16].  
**accreditation** [DFBJR18]. **Accumulable**

**-anonymization** [MU18, RMSCR19]. **-ary**  
[Bae10]. **-database** [BDD01]. **-Diffie**  
[CC12]. **-private** [BDD01].

**.NET** [KKKV07].

**/SSL** [BJ16].

**1** [KJS17]. **11770** [CH16].

**2.0** [AMLH18]. **2002** [ACM05]. **2003**

[SEXY18]. **accumulator** [KYH18]. **accumulators** [CHKO12, JCL<sup>+</sup>18]. **accuracy** [QLOW09]. **accurate** [CYA<sup>+</sup>18, SSD14]. **achievable** [Pla09]. **achieve** [Pen13]. **Achieving** [AICC18, IZS08]. **ACM** [BJ15]. **acoustic** [HS15]. **acquisition** [YP12]. **action** [JG15]. **Active** [LCPD14, CBC08, DGZFGH13]. **actual** [MTSH18]. **actually** [BM11]. **ad** [Gol12, MS11, SF17]. **ad-hoc** [MS11]. **Adapting** [GLP03, Sen14]. **Adaptive** [PPSS13, MdSC<sup>+</sup>15]. **Adding** [CON09]. **ADroid** [RHGTSC17]. **advanced** [PGMLK<sup>+</sup>13, TMP13]. **adversary** [QDW09]. **advertising** [KOSU16]. **affects** [CFBvO09]. **against** [DdP13, EMRN17, GYL<sup>+</sup>07, GI19, KK17, MS11, MYLZ14, Nui12, SK06, VSR15, ZRJ14]. **agent** [LV10]. **Aggregate** [CL13]. **aggregation** [GKS19]. **agreement** [CCS07, CL09, FGS12, GNS14, ZWQ<sup>+</sup>17]. **Alambic** [ABFO08]. **alert** [SGJ19]. **algebraic** [DS07, KM10, SSVC16]. **Algorithm** [JMV01, Bae10, GS15, MU18, SKK<sup>+</sup>17, TLX09]. **algorithms** [BEPL<sup>+</sup>17, KU16, ML14]. **alignment** [KSM10]. **all-encompassing** [EHM15]. **All-or-Nothing** [MTW<sup>+</sup>14]. **allocation** [SGJ19]. **along** [VH19]. **AMACs** [CL13]. **ambients** [TZH04]. **Analysing** [HL04]. **Analysis** [AMRR17, CG14, DBMS10, GLP03, SSFB15, ZZW<sup>+</sup>10, ABCC08, ASN<sup>+</sup>16, AC08, BGKZ12, BEPL<sup>+</sup>17, Bel10, BDMM19, BBR18, BFT08, BNN04, CPPK15, CF07, DFF<sup>+</sup>16, DRPW12, dSFK19, GLMS<sup>+</sup>04, GKBS12, HLKI15, IMI18, IDHRPCMP15, KW15, KAC17, KA18, LRB<sup>+</sup>10, MWZ06, MTW<sup>+</sup>14, NRC15, OT06, PDB11, QLOW09, SK16, SS05a, SB09, SSE<sup>+</sup>15, SPDR17, Vaj16, VdWZ14, WYL<sup>+</sup>12, XSA13]. **Analyzing** [BJ16, vOLW05]. **anchor** [BB04b]. **AND-gate** [JSMG18b]. **Android** [GPS17, IDHRPCMP15, KA18, LMMS17, MS15, RHGTSC17]. **anomaly** [DGF<sup>+</sup>17, KCM<sup>+</sup>15, RHGTSC17]. **anomaly-based** [RHGTSC17]. **Anonymity** [LSWW14, DFBJR18, HLS18, SS05a]. **anonymization** [HN14, MU18, RMSCR19]. **anonymizing** [ZO13]. **Anonymous** [BFG<sup>+</sup>13, LcSCL<sup>+</sup>18, SK14, ACHO13, ABFL12, BCL09, CPPK15, KWCK19, KCB17, SF17]. **answer** [WZ07]. **anti** [GKBS12]. **anti-SPIT** [GKBS12]. **antiviruses** [ASAAS15]. **any** [DdP13]. **API** [You06]. **apples** [BBR18]. **applicable** [QDW<sup>+</sup>15]. **application** [DGF<sup>+</sup>17, Pen12, Roe11a, Roe11b, SPM13, VdWZ14, ZZW<sup>+</sup>10]. **application-layer** [DGF<sup>+</sup>17]. **Applications** [Gri06, BCA<sup>+</sup>10, BNTW12, DJN10, DTK<sup>+</sup>18, GSS10, HSMY12, HZL<sup>+</sup>17, KGG09, SNX19, WYL<sup>+</sup>12, vORM06]. **Applied** [BJ15]. **approach** [AV17, CFG17, CMS10, CACB16, DS07, Fra18, HBH12, KAC16, KAC17, KKK17, LVK18, MG17, MMS16, MSGCDPSS18, MYLZ14, NA14, TWP08, VSR15]. **approaches** [ZO13]. **apps** [GPS17]. **architecture** [AKG16, EHM15, EWR<sup>+</sup>09, LV10, MSP<sup>+</sup>13]. **architectures** [WW07]. **area** [LCL16]. **arguments** [ABM<sup>+</sup>12]. **arithmetic** [ABB17, KW15]. **ARITO** [SSD14]. **ary** [Bae10]. **ASICS** [BCF<sup>+</sup>17]. **aspects** [AICC18]. **assessment** [WHS18]. **assigned** [JTV19]. **assisted** [DYDW10, VPI15]. **association** [VH19]. **assumption** [HIST09]. **assurance** [ABN14, LVK18]. **asymmetric** [ZWQ<sup>+</sup>17]. **Ate** [ZZH08]. **ATNA** [ACBC<sup>+</sup>15]. **attack** [AYHK18, DSB19, DRPW12, dSFK19, GMS03, Lu09, ML14, SS05a, SSD14, ZXZ<sup>+</sup>11]. **attacker** [RMPADF13]. **Attacking** [SGE02]. **attacks** [ASAAS15, BRS06, CACB16, DGF<sup>+</sup>17, EMRN17, HS15, Hub12, KM10, LLWY09, MS11, Pen11, PPL15, SSVC16, TTS<sup>+</sup>06, VSR15, XCW<sup>+</sup>12]. **attestation**

[BFG<sup>+</sup>13, BCL09, CGL<sup>+</sup>11]. **attribute** [JSMG18a, JSMG18b, QLZH15, QDW<sup>+</sup>15, RD16]. **attribute-based** [JSMG18a, JSMG18b, QLZH15, QDW<sup>+</sup>15, RD16]. **attributes** [JSMG18a]. **auctions** [Bra06]. **audio** [dSFK19]. **Audit** [CCD<sup>+</sup>07, BS05]. **Audit-based** [CCD<sup>+</sup>07]. **auditing** [WMS<sup>+</sup>19]. **AUTH** [RG13]. **authenticated** [BBR18, BCF<sup>+</sup>17, IMI18, Lin15, MPS10, Ust11, YLL<sup>+</sup>18, YRW14, ZWQ<sup>+</sup>17]. **Authenticating** [CF07]. **Authentication** [DNF<sup>+</sup>19, GCSABdSS12, BPW05b, BJ16, CL13, DSB19, DFF<sup>+</sup>16, EWR<sup>+</sup>09, Gol12, GTM11, HC10, HCN15, HL04, IT05, KWCK19, KML03, KB13, LSWW14, LCPD14, MB16, ML17, MSKD16, MS09, PS17, RG13, SK14, Smi04, TWP08, VHT09, WLLW14]. **authentications** [HZL<sup>+</sup>17]. **authorities** [LMMO04]. **authority** [CON09, QLZH15]. **authorization** [BZV05, KLMM09, RV03, SSFB15, SK14, WZ07]. **authorized** [ZZG19]. **automata** [BCL13, DLR15, LBW05]. **Automated** [GLMS<sup>+</sup>04, JG15, GH05, dAKdG10]. **automatic** [ACMV15]. **automatically** [KM07, XCW<sup>+</sup>12]. **automating** [SNX19]. **availability** [Bel10]. **AVL** [RBD02]. **aware** [DGF<sup>+</sup>17, KJG<sup>+</sup>11, MBRPS18, RSPMB16, Vaj16]. **awareness** [MPS14].

**back** [KNL16]. **balance** [MYLZ14]. **BAR** [KCB17]. **Based** [LLW<sup>+</sup>16, AYHK18, ACB14, AC08, BFP03, BFPP07, BBR18, BLM11, CCD<sup>+</sup>07, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FGS12, GCH<sup>+</sup>19, GPS17, GBDJ14, GTM11, HJDC15, HS09, HC10, HRL09, IMI18, IT05, JCL<sup>+</sup>18, JSMG18a, JSMG18b, KG11, KKK17, KML03, KLMM09, Kud02, KNL16, LMG17, LKH09, sLC05, LH15, LMD17, LD17, LP11, LBZ<sup>+</sup>10, LMMO04, MPS10, MGV17, MPS14, MP15, MS09, MMS16, MS11, MS14, MRW02, MSGCDPSS18, MFES04, NAM06, NSNK06, NMBB12, OT06, Pen11, PPL15, QLZH15, QDW09, QDW<sup>+</sup>15, RD16, RBEH15, RG13, RMSCR19, RV03, RHGTSC17, SJ09, SBB19, SV11, SPM13, SSP14, SS05a, SK14, SS05b, SdHZ16, SAT09, SGE02, SPDR17, TLX09, TND<sup>+</sup>15, Ust11, VH19, WR08, XCW<sup>+</sup>12, XSA13, YSM10, ZGC07, ZWQ<sup>+</sup>17, ZVH15]. **basic** [BCJ<sup>+</sup>11]. **batch** [Pen13]. **Bayes** [Sen14]. **Bayesian** [ETAHCR08, GBG18]. **be** [ASN<sup>+</sup>16]. **bee** [SS17]. **beehives** [SS17]. **behaves** [ASN<sup>+</sup>16]. **Behavior** [CACB16, MLCS16, XCW<sup>+</sup>12]. **Behavior-based** [CACB16, XCW<sup>+</sup>12]. **behavioral** [KLMM09]. **Behaviour** [PPL15, LCPD14]. **benefit** [DRPW12]. **benefits** [Rus04]. **better** [RAC16]. **between** [FGS12, LKH09]. **bidimensional** [KCM<sup>+</sup>15]. **bilayer** [MLCS16]. **bindings** [MSKD16]. **Bio** [ZZW<sup>+</sup>10]. **Bio-Inspired** [ZZW<sup>+</sup>10]. **Biometric** [Pla09, BCA<sup>+</sup>10, HCN15, IT05]. **biometrics** [BCA<sup>+</sup>10]. **Bipartite** [YOV09]. **birthmark** [XCW<sup>+</sup>12]. **bit** [GSS10, SBB19, YOV09]. **bit-length** [YOV09]. **Bitcoin** [AMLH18, ML17]. **bits** [BR18]. **Black** [DTK<sup>+</sup>18]. **Black-box** [DTK<sup>+</sup>18]. **blank** [WPD18]. **BlindIdM** [NA14]. **block** [CYK09, KM10, Lu09]. **blocks** [CMR06]. **Bloom** [MB16]. **bootstrapping** [EWR<sup>+</sup>09]. **botnet** [AKG16]. **botnets** [AMLH18, KA18, LL14]. **bounded** [LVK18]. **box** [DTK<sup>+</sup>18]. **Breaking** [Dan07]. **Bring** [ACMV15]. **Broadcast** [GSP<sup>+</sup>16, KCB17, LLW<sup>+</sup>16, CL09, PPSS13]. **BRSIM** [BP08]. **BRSIM/UC** [BP08]. **Building** [LD07]. **business** [KAC16, KBH07].

**cache** [TTS<sup>+</sup>06]. **caching** [ACB14]. **calculus** [BNN04]. **Canada** [Lev07]. **candidates** [ABM<sup>+</sup>12]. **can't** [JTV19]. **capabilities** [ASAAS15, Lop18]. **capability** [CL08, Fon08]. **capacity** [SJ09]. **capture** [MR03]. **card** [ABFL12, DMDD16,

GdKGV14, MS14, MLM19]. **card-based** [MS14]. **cards** [MPP14]. **carried** [QLOW09]. **cascade** [WPD18]. **cascade-instantiable** [WPD18]. **case** [BSCZ11, GLMS<sup>+</sup>04, SKK<sup>+</sup>17]. **cases** [Pla09]. **cash** [LCL14]. **CASSANDRA** [MCD11]. **cast** [YYK<sup>+</sup>18]. **CCA** [PPSS13]. **CDH** [HIST09]. **ceremonies** [MdSC<sup>+</sup>15]. **Certificate** [MFES04, CLPP11, Rus04, Ust11]. **certificate-based** [Ust11]. **certificate-free** [CLPP11]. **Certificateless** [ZWQ<sup>+</sup>17, CFG17, Den08, FGS12, SSP14]. **certification** [BCF<sup>+</sup>17, LMMO04]. **certified** [IZS08]. **chained** [DZW<sup>+</sup>18]. **challenges** [HC10]. **channel** [dSFK19, HS15, MSKD16, MS09, MTW<sup>+</sup>14]. **channels** [DHW11, KK17, KML03]. **characterization** [MSN02]. **check** [KO02]. **checker** [BMV05]. **checking** [AC08, GKBS1, HL04, MS15, NST09, YAM<sup>+</sup>15]. **checksums** [GKKT10]. **CHES** [DSY06]. **chosen** [LLW<sup>+</sup>16]. **chosen-ciphertext** [LLW<sup>+</sup>16]. **cipher** [Lu09, TTS<sup>+</sup>06]. **ciphers** [CYK09, IMI18, KM10]. **Ciphertext** [JSMG18a, JSMG18b, LMG17, LLW<sup>+</sup>16]. **Ciphertext-policy** [JSMG18a, JSMG18b]. **ciphertexts** [JSMG18b, PPSS13]. **class** [DS07, MLCS16]. **Classification** [SAL17, CBC08]. **classify** [BEPL<sup>+</sup>17]. **click** [ALPW13, CFBvO09, MBHT17]. **click-based** [CFBvO09]. **clients** [SPDR17]. **close** [DHW11]. **Cloud** [Abb13, ABN14, Ano14, BMP<sup>+</sup>14, CMMPS15, FSG<sup>+</sup>14, GMH14, HK19, KNL16, LZQ<sup>+</sup>18, MSGCDPSS18, PPL15, VH19, WMS<sup>+</sup>19, YAM<sup>+</sup>15]. **cloud-based** [KNL16]. **clustering** [BT07, RMSCR19, SKK<sup>+</sup>17]. **clustering-based** [RMSCR19]. **co** [BMP<sup>+</sup>14, PPL15]. **co-residence** [PPL15]. **co-resident** [BMP<sup>+</sup>14]. **code** [DMDD16, HZL<sup>+</sup>17, KKKV07]. **codes** [CL13, Nui12]. **coding** [EMRN17, TWP08]. **coding-enabled** [EMRN17]. **collection** [SV11]. **Collision** [MS09, CHKO12, KW15]. **collision-resistant** [CHKO12]. **collusion** [DdP13, Nui12]. **collusion-secure** [Nui12]. **Colored** [SSFB15]. **coloring** [RS18]. **column** [CMS10]. **combinations** [KAC17]. **combinatorial** [CMR06]. **combining** [SSE<sup>+</sup>15]. **command** [SNX19]. **commerce** [ABFO08, GLP03, ZGC07]. **commercial** [NVB<sup>+</sup>02]. **commitment** [GSS10, HCN15]. **Commix** [SNX19]. **commodity** [TND<sup>+</sup>15]. **commodity-based** [TND<sup>+</sup>15]. **common** [DMP13]. **communication** [CPPK15, GBG18, KCB17, LMD17, VdWZ14]. **communication-efficient** [LMD17]. **communications** [MB16]. **Comparing** [BBR18]. **comparisons** [AL05]. **compatible** [LI07]. **Complete** [ABCC08, BB04a, LCL14, MSN02]. **completeness** [WHS18]. **compliance** [CCD<sup>+</sup>07]. **Compliant** [DVB02]. **components** [AV17]. **composability** [Vaj16]. **composable** [BFS<sup>+</sup>13]. **comprehensive** [BF13, LRB<sup>+</sup>10, SB09]. **compressing** [MP16]. **compromised** [SPDR17]. **computation** [ABB17, BNTW12, Pen13]. **Computational** [BP04, LCL16]. **computations** [BGP07b, KU16]. **compute** [MCD11]. **Computer** [Lan01, BCEM04, LL14, vORM06]. **Computing** [BJ15, Ano14, LI07, Pri04]. **concept** [Sen14]. **conceptual** [JGK14]. **Concrete** [BLM11, BCL09]. **Concrete-** [BLM11]. **concurrent** [ASAAS15]. **Conditional** [BDHK08]. **conditions** [BDPV14, sLC05]. **Conference** [CL09]. **confidential** [HN14]. **confidentiality** [BB04a, KNL16]. **configuration** [ABR16, ABCC08]. **confinement** [Fon08, SPM13, SS05b]. **conflict** [RV03]. **conjunctive** [LZQ<sup>+</sup>18]. **connection** [LSWW14, SS05a]. **connection-based** [SS05a]. **considering** [TTS<sup>+</sup>06]. **constant**

[BGP07b, PPSS13]. **constant-round** [BGP07b]. **constant-size** [PPSS13]. **constants** [BR17]. **constrained** [SS17]. **construct** [YSM10]. **construction** [Ala17, BGKZ12, NSNK06, YYK<sup>+</sup>18]. **constructions** [HSMY12, KME<sup>+</sup>16, ZVH15]. **consumer** [LKH09]. **consumption** [RBEH15]. **consumption-based** [RBEH15]. **contacts** [DMP13]. **containing** [IT05]. **Content** [BFP03, HC10, LKH09, Pla09]. **Content-based** [BFP03, HC10]. **context** [DGF<sup>+</sup>17, HS09, JGK14]. **context-aware** [DGF<sup>+</sup>17]. **context-sensitive** [HS09]. **contextual** [CCB08]. **continuous** [EG18]. **contourlet** [SJ10]. **contract** [IZS08]. **contracts** [GYL<sup>+</sup>07]. **Control** [LMMS17, SAL17, ACF17, AJC<sup>+</sup>09, Ano11b, ACBC<sup>+</sup>15, BLM11, BNN04, CF03, CCD<sup>+</sup>07, CK08, CZ06, HS09, HSMY12, KAC16, KAC17, KLMM09, Kud02, KNL16, LRB<sup>+</sup>10, MS15, Pen12, RM12, TZH04, ZM07]. **Controlled** [BB04a, BFG<sup>+</sup>13, SM10]. **conversations** [DBMS10]. **convertible** [Lin15]. **convex** [ALPW13]. **cookie** [ACB14]. **cookie-based** [ACB14]. **cooperation** [AGIK07]. **coprocessors** [Smi04]. **correcting** [KM07]. **cost** [DRPW12, DYDW10]. **cost-benefit** [DRPW12]. **counter** [BF13]. **counter-measure** [BF13]. **countermeasure** [GBDJ14, MTW<sup>+</sup>14, Pen11]. **countermeasures** [Bae10]. **Counting** [KM10]. **country** [SKK<sup>+</sup>17]. **cover** [SJ10]. **COVERAGE** [AGIK07]. **covert** [DHW11]. **Cracker** [SGE02]. **credential** [AYHK18, ABFL12]. **credentials** [SF17]. **Critical** [EEB<sup>+</sup>15]. **cross** [PMPGMLLM12]. **cross-layer** [PMPGMLLM12]. **CRT** [OT06]. **CRT-based** [OT06]. **CRUST** [GW09]. **Cryptanalysis** [ALPW13, DSY06, MS11]. **Cryptanalytic** [CJMS19]. **Crypto** [You06]. **cryptographic** [ARMLS06, BPW05b, BGK08, BDH<sup>+</sup>10, DFF<sup>+</sup>16, DSRHC16, GW09, JCL<sup>+</sup>18, KU16, Küs05, MR03, MS14, MSGCDPSS18]. **Cryptographically** [BCJ<sup>+</sup>11]. **cryptography** [ALOW15, LP11]. **cryptologic** [DVB02]. **cryptosystem** [HCN15, IT05, MS11, SGE02]. **cryptosystems** [KG11, NMBB12, OT06]. **Cryptoviral** [You06]. **CSOC** [SGJC18, SGJ19]. **cuckoo** [VH19]. **current** [HC10]. **Curve** [JMV01]. **curves** [HMCD04, KSZ07]. **Cyber** [SSD14]. **Cyber-attack** [SSD14]. **cycle** [AYHK18].

**damage** [WGMB13]. **DAME** [PMPGMLLM12]. **Data** [LMMS17, SV11, SAL17, VdWZ14, ACF17, ABN14, BS05, BNTW12, BDH<sup>+</sup>10, CTM<sup>+</sup>16, EMRN17, EAH<sup>+</sup>07, GSAMCA18, GKS19, HJDC15, HK19, HH16, Küs05, LD17, MSGCDPSS18, OSSK16, SMMN12, VH19, YAM<sup>+</sup>15, ZO13]. **Database** [KSM10, BDD01]. **databases** [BW08, CMS10, EAH<sup>+</sup>07, HN14]. **dataset** [NRC15]. **datasets** [MU18]. **day** [DGF<sup>+</sup>17]. **dealership** [GSP<sup>+</sup>16]. **decentralized** [LLWY09]. **decidability** [Küs05]. **decision** [WPD18]. **dedicated** [ZZG19]. **Defeating** [DSB19]. **defending** [SK06]. **defense** [MYLZ14, VSR15, WR08, ZRJ14]. **defenses** [LLWY09]. **Definition** [TMP13]. **degree** [SSVC16]. **Delay** [ZO13]. **Delay-sensitive** [ZO13]. **delegatability** [HYWS11]. **Delegation** [CK08, BGTCCBB10, CON09, GOBdlC11, WZ07, ZZG19]. **delegations** [RV03]. **deniable** [GCH<sup>+</sup>19]. **Denial** [LLWY09, WR08, TGS17]. **denial-of-service** [WR08]. **dependence** [HS09]. **dependencies** [ACF17]. **dependency** [CMS10]. **dependency-based** [CMS10]. **Deployment** [ACBC<sup>+</sup>15, HIDFGHR19, Das12]. **depth** [SAT09]. **description** [SM10]. **Design** [DNF<sup>+</sup>19, MBRPS18, BSCZ11, CMR06, CFBvO09, LMMO04]. **designated**

[HSMW08, HYWS11]. **designed** [KCM<sup>+</sup>15]. **Designing** [AV17]. **detect** [CACB16]. **Detecting** [DGF<sup>+</sup>17, AGIK07, BMP<sup>+</sup>14, PPL15, vORM06]. **Detection** [ABR16, CPPK15, sLC05, SAL17, ASAAS15, ASN<sup>+</sup>16, BEPL<sup>+</sup>17, BDMM19, BT07, CL08, DTK<sup>+</sup>18, DGF<sup>+</sup>17, GPS17, KA18, KKK17, KJG<sup>+</sup>11, KSM10, McH01, MLCS16, RBEH15, RHGTSC17, Sen14, SF17, TLX09, VL13, WAB<sup>+</sup>09, ZXZ<sup>+</sup>11, ZGK07]. **detectors** [AvO13]. **deterministic** [GS15, RMSCR19]. **developing** [SK16]. **Development** [KK17]. **device** [KWCK19, ACMV15]. **Devices** [LMMS17, GCSÁBdSS12, IDHRPCMP15, LKH09, LCPD14, MR03]. **Differential** [dSFK19, MTW<sup>+</sup>14]. **Diffie** [CC12, DS07]. **Digital** [JMV01, ASF04, JG15]. **direct** [BCL09, KME<sup>+</sup>16]. **disclosure** [KPM12, RAC16]. **discounts** [DFBJR18]. **discovery** [CYA<sup>+</sup>18, DMP13, JM17]. **discrete** [HMCD04]. **Discretionary** [Fon08]. **discrimination** [ZZG19]. **dissociation** [VH19]. **distinguish** [HTM11]. **Distributed** [RS18, ASF04, Das12, DHS04, HN14, KKK17, Pen12, TLX09, WZ07]. **Distributing** [VSM06, AYHK18]. **distribution** [ASF04, BFPP07, CMR06, GP17, YYK<sup>+</sup>18]. **DNA** [IHNT02]. **DNS** [SPDR17]. **Do** [BM11]. **document** [CF03]. **documents** [BFP03, BFPP07]. **does** [GSM<sup>+</sup>11]. **Dolev** [BPW05b, BP08]. **domain** [CON09, CYA<sup>+</sup>18, PGMLK<sup>+</sup>13, SCL<sup>+</sup>18]. **DomainProfiler** [CYA<sup>+</sup>18]. **domains** [GMH14]. **don't** [JTV19]. **Double** [ACHO13, PS17]. **Double-authentication-preventing** [PS17]. **Double-trapdoor** [ACHO13]. **down** [JTV19]. **download** [NRC15]. **DPA** [Bae10]. **drift** [Sen14]. **drive** [NRC15]. **drive-by** [NRC15]. **DRM** [LKH09]. **DSA** [MR04]. **DTE** [LH15]. **DTLS** [TGS17]. **during** [CBC08]. **Dynamic** [BDMM19, DFBJR18, HK19, KYH18, Roe11a, ZM07, CON09, CMS10, CZ06, KK17, SSE<sup>+</sup>15, YYK<sup>+</sup>18, Roe11b]. **dynamicity** [AICC18]. **dynamics** [MRW02].

**E-business** [KBH07]. **E-cash** [LCL14]. **e-commerce** [GLP03, ZGC07]. **e-government** [GOBdlC11]. **e-healthcare** [QDW<sup>+</sup>15]. **e-services** [DDPS02]. **e-voting** [MS11, Pen11]. **early** [CYA<sup>+</sup>18]. **eavesdropping** [CPPK15]. **ECDSA** [JMV01]. **eCK** [Ala17]. **eCK-secure** [Ala17]. **Edit** [LBW05, BCL13]. **Editorial** [GMO01, Gol08]. **editors** [ANS<sup>+</sup>12, CM16, CHM18, DMRS07, JZ11, YSM16, ZLL12]. **eduroam** [PMPGMLLM12]. **eduroam/DAMe** [PMPGMLLM12]. **effective** [ZGC07]. **Effectiveness** [SK16, SGJC18]. **effects** [SV11]. **efficiency** [HMCD04, MG17, PDB11, Pen13]. **Efficient** [HRL09, HH16, HYWS11, JCL<sup>+</sup>18, KJ14, KU16, KSZ07, LMG17, LBZ<sup>+</sup>10, MP16, NP10, RD16, SMMN12, Bae10, BR18, BCD<sup>+</sup>13, EMRN17, HN14, HYWS12, LMD17, LCL14, MCD11, Pen11]. **effort** [SGJ19]. **eID** [RLEM18]. **Elastic** [CYK09]. **Electronic** [GSM<sup>+</sup>11, ABFO08, BDHZ15, DJN10, KO02]. **Elias** [BR18]. **elicit** [SK16]. **elliptic** [HMCD04, KSZ07, JMV01]. **email** [IZS08, WR15]. **Embedding** [BDH<sup>+</sup>10, SJ09]. **enabled** [EMRN17]. **Enabling** [BS05]. **encapsulation** [MPS14]. **encompassing** [EHM15]. **encrypted** [CTM<sup>+</sup>16, DBMS10, GSAMCA18, HH16, KJ14, OSSK16, SEXY18, WPD18, WR15]. **encryption** [ARMLS06, BZ03, CC12, Den08, EHSS14, FGS12, GMMV05, GSP<sup>+</sup>16, HK19, IMI18, JCL<sup>+</sup>18, JSMG18a, JSMG18b, KME<sup>+</sup>16, LMG17, LZQ<sup>+</sup>18, Lin15, PPSS13, QLZH15, QDW<sup>+</sup>15, SSP14, YP06, ZZG19, ZVH15, LLW<sup>+</sup>16, Dan07]. **end** [BB04b]. **ended** [Küs05]. **energy** [RBEH15]. **enforced** [BM11]. **enforcement** [ACMV15,

AICC18, BCL13, DLR15, LBW05].  
**enforcing** [BB04a]. **engineering**  
 [GMMZ06, MLM19, SK16]. **Enhanced**  
 [ABN14, YAM<sup>+</sup>15, LV10, MSP<sup>+</sup>13, JTV19].  
**Enhancing** [ACB14, CLW<sup>+</sup>11, KLMM09].  
**Ensuring** [SAT09, SGJ19]. **enterprise**  
 [WYL<sup>+</sup>12]. **Entropy**  
 [BEPL<sup>+</sup>17, HLKI15, SV11]. **environment**  
 [CLW<sup>+</sup>11, GOBdlC11, LRB<sup>+</sup>10, NVB<sup>+</sup>02].  
**environments**  
 [FSG<sup>+</sup>14, GYL<sup>+</sup>07, LI07, PPL15, WAB<sup>+</sup>09].  
**epidemics** [AGIK07]. **equations**  
 [KM10, SSV16]. **Erratum** [Roe11b]. **error**  
 [RMPADF13]. **errors** [ABR16]. **Escrow**  
 [ARMLS06, YSM10]. **Escrow-free**  
 [ARMLS06]. **ESORICS** [Sne05].  
**establishing** [Abb13]. **establishment**  
 [BVS07, Das12, YRW14]. **Estimating**  
 [AD08, WHS18]. **estimation** [RMPADF13].  
**EUFORBIA** [BFP03]. **evading** [XCW<sup>+</sup>12].  
**Evaluation**  
 [AvO13, AKG16, BB04a, HIDFGHR19,  
 RHL17, SK06, SNX19, TND<sup>+</sup>15].  
**evenhandedness** [ZS08]. **events**  
 [RHGTSC17]. **evidence** [SdHZ16].  
**evidence-based** [SdHZ16]. **EXAM**  
 [LRB<sup>+</sup>10]. **exchange**  
 [Ala17, BBR18, BCF<sup>+</sup>17, BFS<sup>+</sup>13, CHZ16,  
 DGZFGH13, ETAHCR08, HYWS12, MPS10,  
 MPP14, MSN02, SEXY18, Ust11, YLL<sup>+</sup>18].  
**excursus** [Fra18]. **Execution**  
 [SK06, MLO<sup>+</sup>04]. **exhaustive** [KJS17].  
**experimental** [BCD<sup>+</sup>13, DSB19].  
**experiments** [QLOW09]. **explicit** [KAC16].  
**exploitation** [JM17, MLM19, SNX19].  
**exploiting** [ACF17]. **exploits** [ZRJ14].  
**exploring** [HS15]. **exponentiation** [Bae10].  
**expression** [WR15]. **expressive** [RD16].  
**extended**  
 [ACF17, BGTCCBB10, Lop18, MS15].  
**Extending** [KKKV07]. **extension**  
 [JSMG18a]. **external** [CLW<sup>+</sup>11]. **extortion**  
 [You06]. **extractable** [WT16].  
**FA** [Bae10]. **faceted** [BFT08, QLOW09].  
**facets** [AKG16]. **factor** [CG14, ML17].  
**failures** [SK06]. **Fair** [KM03, DGZFGH13,  
 GRV05, HYWS12, SEXY18, SGJ19].  
**familiarity** [ZGC07]. **familiarity-based**  
 [ZGC07]. **family** [AMP12, MSN02]. **fault**  
 [CL09, GKS19, RBD02]. **fault-tolerance**  
 [CL09]. **fault-tolerant** [GKS19, RBD02].  
**FCS** [ACM05]. **FCS/VERIFY** [ACM05].  
**feature** [YP06]. **federated** [WW07].  
**federating** [PMPGMLLM12]. **file** [sLC05].  
**file-based** [sLC05]. **filter** [MB16, VH19].  
**filtering** [BFP03]. **find** [SSVC16]. **fine**  
 [KLMM09]. **fine-grained** [KLMM09].  
**fingerprint** [CC10, Nui12]. **finite** [BCL13].  
**firewall** [ABR16, KNL16, MWZ06]. **first**  
 [LM06]. **first-order** [LM06]. **fixed**  
 [HMCD04]. **Flexible** [JSMG18b, QDW<sup>+</sup>15].  
**floating** [ABB17, KW15]. **floating-point**  
 [ABB17]. **Flow**  
 [HS09, SdHZ16, BMP<sup>+</sup>14, BNN04, ZM07].  
**Flow-based** [SdHZ16]. **Flow-sensitive**  
 [HS09]. **Flowchart** [SM10]. **fly** [CL13].  
**form** [DdP13]. **Formal** [ACMV15, GKBS12,  
 Yon18, dAKdG10, CMN<sup>+</sup>18, KAC17,  
 NSNK06, PDB11, RV03, VdWZ14].  
**formalism** [GBDJ14]. **formalization**  
 [MS14]. **forward** [CDF<sup>+</sup>13, KME<sup>+</sup>16].  
**forward-secure** [KME<sup>+</sup>16]. **four** [Dan07].  
**Fractional** [BCA<sup>+</sup>10]. **framework**  
 [Abb13, ABFL12, BFT08, KNL16, MB16,  
 MLO<sup>+</sup>04, RV03, Vaj16, VdWZ14, WR08,  
 WHS18, XSA13, ZRJ14]. **free**  
 [ARMLS06, BGKZ12, CLPP11, YRW14].  
**freeness** [HIST09]. **friendly** [CLPP11].  
**Fujisaki** [GMMV05]. **full** [Bra06]. **Fully**  
 [CDF<sup>+</sup>13]. **function** [BGKZ12, SB14].  
**functionality** [SPM13].  
**functionality-based** [SPM13]. **functions**  
 [AMP12, EG18, GKKT10, MS09, SM10].  
**future** [CYA<sup>+</sup>18, LMMP06]. **fuzzy**  
 [HCN15].  
**Gait** [HCN15]. **Game**

[wLW05, LVK18, WYL+12]. **game-theoretic** [LVK18]. **gate** [JSMG18b]. **general** [BCD+13, Pen11]. **generalised** [BKMR08]. **generalization** [DJN10]. **Generalized** [BR18, KMR09]. **Generalizing** [KG11, AMP12]. **generated** [IHNT02]. **Generating** [LC04]. **generation** [AMLH18, KJG+11, KSZ07, MR04]. **Generic** [Ala17, ZVH15, EWR+09, KME+16]. **geographic** [ABN14]. **GeoProof** [ABN14]. **geospatial** [HK19]. **gesture** [GCSÁBdSS12]. **Global** [Pri04]. **goals** [RGL16]. **gossip** [ML14]. **government** [GOBdIC11]. **GPU** [VPI15]. **GPU-assisted** [VPI15]. **GQ** [HRL09]. **grained** [KLMM09]. **graph** [BCEM04, RV03]. **graph-theoretical** [BCEM04]. **graphical** [CG14, CFBvO09, GTM11, WLLW14]. **graphs** [HS09, HLKI15, KB13]. **grid** [CLPP11, KLMM09, LP11]. **ground** [AvO13]. **Group** [EHSS14, BVS07, DFBJR18, GNS14, IDHRPCMP15, RBD02, YLL+18, ZWQ+17]. **groups** [PJ10]. **guarantee** [ABCC08, Bel10]. **guarantees** [LSWW14]. **guest** [ANS+12, CM16, CHM18, DMRS07, JZ11, YSM16, ZLL12].

**Haar** [KCM+15]. **hand** [GCSÁBdSS12]. **Handling** [WZ07]. **handshake** [TGS17]. **hard** [EAH+07]. **hard-to-reverse** [EAH+07]. **hardening** [DMDD16, DRPW12, MRW02]. **hardware** [BSCZ11, DYDW10]. **hardware-assisted** [DYDW10]. **harvesting** [BR18]. **hash** [AMP12, BGKZ12, GKKT10, MS09, MFES04, SB14]. **hashing** [BDPV14, CHKO12, CJMS19, MP16]. **health** [BDHZ15, QLZH15]. **healthcare** [QDW+15]. **Hellman** [CC12, DS07]. **heterogeneous** [RLEM18, SAT09]. **HIBE** [ZZG19]. **hidden** [ABB17, GSS10, SSVC16]. **Hiding** [GI19]. **Hierarchical** [NAM06, JCL+18, LLW+16]. **High** [BNTW12, BB04b, Pen13]. **high-end** [BB04b]. **High-performance** [BNTW12]. **higher** [PDB11]. **HiveSec** [SS17]. **hoc** [Gol12, MS11, SF17]. **homomorphic** [EMRN17, MMS16, SEXY18]. **HoneyCirculator** [AYHK18]. **honeypot** [AYHK18]. **hop** [BT07]. **host** [CLW+11]. **hotels** [DZW+18]. **hull** [ALPW13]. **human** [ALPW13, MBHT17]. **Hybrid** [KML03, CC10, GMMV05, MMS16].

**ID** [FGS12, ZZG19]. **ID-based** [FGS12]. **identification** [ALPW13, CL08, GBG18, GI19, LcSCL+18, MGV17, NRC15]. **Identifier** [ZZG19]. **identifiers** [IHNT02]. **identifying** [KGG09, SPDR17]. **Identity** [CCS07, LP11, LLW+16, CHZ16, GOBdIC11, HRL09, JCL+18, LMG17, LBZ+10, MPS14, NA14, TMP13, Ust11, VdWZ14, YSM10, ZWQ+17]. **Identity-Based** [LLW+16, CCS07, LP11, CHZ16, HRL09, JCL+18, LMG17, LBZ+10, MPS14, Ust11, YSM10, ZWQ+17]. **IDSIC** [CL08]. **IEC** [CH16]. **If** [ASN+16, MBHT17]. **IHE** [ACBC+15]. **II** [BB04b]. **IIJ** [SKK+17]. **image** [HC10]. **images** [HLKI15, MBHT17]. **immune** [Hub12]. **impact** [SSD14]. **implement** [ABFL12]. **implementation** [BSCZ11, DNF+19, IDHRPCMP15, MBRPS18, MFES04]. **implemented** [MS15]. **Implementing** [ALOW15, BGK08]. **implications** [HMCD04]. **implies** [EHSS14]. **Improved** [HLS18, ABN14, MLCS16]. **Improving** [CH16, TTS+06, BJ16, TGS17, TG05]. **IMS** [VL13]. **incentive** [LI07]. **incomplete** [BW08]. **Incompleteness** [SAL17]. **Inconsistency** [SAL17]. **incorporating** [BCF+17]. **indifferentiability** [BGKZ12]. **inductive** [MP15]. **industrial** [RM12]. **inference** [AJC+09, JG15]. **Information** [KBH07, TND+15, ASF04, AD08, ABFL12, BDHZ15, BB04a, BDD01, CMMPS15,



DdP13, DBMS10, EFH09, GI19, HS09, IHNT02, KPM12, LMD17, LcSCL<sup>+18</sup>, MU18, NAM06, Pla09, WHS18, ZM07]. **information-distribution** [ASF04]. **Information-theoretically** [TND<sup>+15</sup>]. **infrastructure** [CLPP11, TMP13, Gri06]. **Infrastructures** [EEB<sup>+15</sup>]. **injection** [DSB19, DTK<sup>+18</sup>, SNX19]. **insecure** [KM07]. **Insider** [YP12]. **inspection** [BDF04]. **inspired** [SS17, ZZW<sup>+10</sup>]. **instance** [Sen14]. **instance-weighted** [Sen14]. **instances** [BMP<sup>+14</sup>, JG15]. **instantiable** [WPD18]. **instantiations** [CYK09]. **Instruction** [DM07]. **Instruction-level** [DM07]. **insurance** [GYL<sup>+07</sup>]. **Integrating** [Ust11, ZGK07]. **Integrity** [IMI18, LZQ<sup>+18</sup>, EEB<sup>+15</sup>, LVK18, YAM<sup>+15</sup>, EEB<sup>+15</sup>]. **integrity-checking** [YAM<sup>+15</sup>]. **Integrity-OrBAC** [EEB<sup>+15</sup>]. **Integrity-verifiable** [LZQ<sup>+18</sup>]. **intelligence** [KKK17]. **intelligence-based** [KKK17]. **Interacting** [vOLW05]. **Interactive** [MS09, CDF<sup>+13</sup>, CHZ16, CL09, EHSS14, MS09]. **interface** [CFBvO09]. **intermediaries** [DGZFGH13]. **International** [KBH07]. **Internet** [DHS04]. **interpretation** [DM07]. **intersection** [MCD11]. **introspection** [AYHK18]. **Intrusion** [BT07, McH01, WAB<sup>+09</sup>, CL08, KKK17, KSM10, RBEH15, TLX09, VL13, ZGK07]. **intrusions** [MYLZ14]. **Investigating** [ASAAS15]. **investigation** [SGJ19]. **investigations** [JG15]. **involvement** [ZBD06]. **IP** [CACB16, RS18, WAB<sup>+09</sup>]. **IPsec** [TG05]. **IPTV** [KOSU16]. **ISC** [BM05]. **ISO** [CH16, DFF<sup>+16</sup>]. **ISO-standards-track** [DFF<sup>+16</sup>]. **ISO/IEC** [CH16]. **isomorphisms** [GMS03]. **Issue** [KBH07, Ano11b, ACM05, BJ15, BM05, Daw04, Pri04, Sne05]. **issues** [FSG<sup>+14</sup>, HC10].

**Java** [MLM19]. **Journal** [KBH07].

**KAMU** [PGMLK<sup>+13</sup>]. **Kasahara** [CHZ16]. **Keeping** [BW08]. **kerberized** [PMPGMLLM12]. **Kerberos** [BCJ<sup>+11</sup>, MPP14, PGMLK<sup>+13</sup>]. **Key** [BRS06, Gri06, NVB<sup>+02</sup>, Ala17, ALOW15, BCJ<sup>+11</sup>, BZ03, BBR18, BVS07, BCF<sup>+17</sup>, BFS<sup>+13</sup>, CMR06, CCS07, CC12, CHZ16, CL09, CH16, DJN10, Das12, EHSS14, FGS12, GNS14, GP17, Lu09, MPS10, MPS14, MPP14, MSN02, RHL17, RBD02, SSP14, TGS17, Ust11, YLL<sup>+18</sup>, YRW14, YYK<sup>+18</sup>, YSM10, ZWQ<sup>+17</sup>]. **Keyboard** [HS15]. **keys** [BDH<sup>+10</sup>, GW09, IT05, LC04, PPSS13, Pla09]. **keystroke** [CF07, MRW02]. **Keyword** [VH19, LZQ<sup>+18</sup>, OSSK16]. **Keyword-based** [VH19]. **knowledge** [YP12].

**labels** [ZM07]. **Large** [TLX09, Das12, RLEM18, SMMN12]. **Large-scale** [TLX09, Das12, RLEM18]. **Lattice** [GCH<sup>+19</sup>, SSP14, BBR18]. **Lattice-based** [GCH<sup>+19</sup>, SSP14, BBR18]. **lattices** [KJ14]. **layer** [DGF<sup>+17</sup>, PMPGMLLM12, WR08]. **leakage** [AD08, DdP13, DBMS10, WT16]. **leakage-resilient** [WT16]. **learning** [GSAMCA18, GBG18, KA18, SSE<sup>+15</sup>, TLX09]. **left** [Bae10]. **legal** [Lev07]. **length** [YOV09]. **Less** [BFS<sup>+13</sup>]. **level** [DM07, SCL<sup>+18</sup>, SGJC18]. **library** [BPW05b]. **Lightweight** [RBEH15]. **like** [ASN<sup>+16</sup>]. **Limits** [BP08]. **line** [BCD<sup>+13</sup>, LMMO04]. **line/on** [BCD<sup>+13</sup>]. **Link** [DMDD16]. **Link-time** [DMDD16]. **linkability** [BFG<sup>+13</sup>]. **Linkable** [GP17]. **list** [Des09]. **list-based** [Des09]. **Listega** [Des09]. **localization** [ZXZ<sup>+11</sup>]. **location** [EG18]. **lockpicking** [GdKGV14]. **log** [HBH12]. **logarithm** [HMCD04]. **logic** [LM06, SdHZ16]. **login** [KPM12]. **looks** [ASN<sup>+16</sup>]. **loss** [MU18]. **lottery** [GSS10].

**Low** [BGP07b, GS15, MU18, SSV16].  
**low-deterministic** [GS15].  
**Low-randomness** [BGP07b]. **LPN** [RG13].  
**LTE** [LSWW14].

**MAC** [EMRN17]. **MAC-based** [EMRN17].  
**machine** [GSAMCA18, KA18, MS14, SSE<sup>+</sup>15].  
**machine-learning** [SSE<sup>+</sup>15]. **machines** [MLCS16, vOLW05]. **Making** [BR17].  
**MALICIA** [NRC15]. **malicious** [ABB17, BRS06, CMS10, GPS17, RHGTSC17, WGMB13]. **Malware** [HLKI15, MLCS16, BEPL<sup>+</sup>17, BDMM19, SKK<sup>+</sup>17, VPI15, ZRJ14]. **manageability** [TG05]. **Management** [CF03, ASF04, BF13, CH16, GMMZ06, GH05, LLWY09, Lop18, LcSCL<sup>+</sup>18, NA14, RHL17, RLEM18, RBD02, SSN15, TMP13, VdWZ14, WPD18, WW07, dAKdG10, vOLW05].  
**managing** [AMLH18]. **mandatory** [DLR15]. **Markov** [ABB17, RHL17].  
**masquerade** [Sen14]. **matching** [FHV18, SBB19]. **MaX** [BFP03].  
**maximum** [AD08]. **McEliece** [NMBB12].  
**McEliece-based** [NMBB12]. **mean** [BM11].  
**measure** [BF13, SGJC18]. **measurement** [RMPADF13]. **Measuring** [RGL16].  
**mechanism** [ACF17, LI07]. **mechanisms** [LBW05]. **media** [RAC16]. **mediated** [VSM06]. **meets** [LLBL18]. **memory** [CJMS19, SV11, vOLW05]. **memory-based** [SV11]. **merging** [CMR06]. **Merkle** [MFES04]. **mesh** [EHM15, SSN15].  
**Message** [ANS<sup>+</sup>12, CM16, CHM18, JZ11, YSM16, ZLL12, CL13, GP17, MS09].  
**metering** [MSP<sup>+</sup>13, RDK18]. **Method** [SAL17, CYK09, IT05, KGG09, MP15, PJ10, SPDR17, WHS18]. **methodology** [AvO13, Des09, GMMZ06, SGJC18, SGJ19].  
**methods** [CMN<sup>+</sup>18]. **microaggregation** [SMMN12]. **microblogging** [ASN<sup>+</sup>16].  
**Microsoft** [You06]. **minimisation** [VdWZ14]. **Minimizing** [KPM12, ZBD06].

**mining** [BDMM19, BNTW12, HBH12].  
**misbehavior** [SF17]. **MITF** [SKK<sup>+</sup>17].  
**mitigation** [YP12]. **mix** [Dan07, MS11, Pen11]. **mix-based** [MS11, Pen11]. **mix-related** [Dan07].  
**Mobile** [EWR<sup>+</sup>09, LMMS17, ACB14, AKG16, AMRR17, CF07, GSM<sup>+</sup>11, GCSAbdSS12, HIDFGHR19, HCN15, HZL<sup>+</sup>17, IDHRPCMP15, LCPD14, LH15, LL14, LV10, MTSH18, WGMB13, BT07, SSE<sup>+</sup>15].  
**mobile-phone** [WGMB13].  
**Mobile-Sandbox** [SSE<sup>+</sup>15]. **MobileTrust** [LV10]. **model** [ASF04, Ala17, ABB17, AC08, BMV05, BGTCCBB10, BCEM04, EEB<sup>+</sup>15, GMMZ06, Gol12, GYL<sup>+</sup>07, GKBS12, HL04, JGK14, Kud02, LH15, MdSC<sup>+</sup>15, NSNK06, QLOW09, SK16, SPM13, SSP14, TND<sup>+</sup>15, YLL<sup>+</sup>18, ZGC07, ZZW<sup>+</sup>10].  
**model-checking** [AC08]. **model-oriented** [SK16]. **Modeling** [CCB08, DLR15, ACMV15, KAC17, Yon18].  
**models** [ABB17, Den08, DRPW12, FGS12, KAC16].  
**modes** [BDPV14]. **Modification** [PDB11].  
**modified** [KJS17]. **modular** [MSKD16, YOV09]. **monitor** [SGJC18].  
**monitoring** [HBH12, vORM06]. **motivate** [Fra18]. **Multi** [BT07, EHM15, KWCK19, OSSK16, YYK<sup>+</sup>18, ZZW<sup>+</sup>10, BNTW12, BFT08, CON09, Das12, GMH14, KM03, PGMLK<sup>+</sup>13, QLZH15, QLOW09, WR08].  
**multi-authority** [QLZH15]. **Multi-cast** [YYK<sup>+</sup>18]. **Multi-device** [KWCK19].  
**multi-domain** [CON09, PGMLK<sup>+</sup>13].  
**multi-domains** [GMH14]. **multi-faceted** [BFT08, QLOW09]. **Multi-hop** [BT07].  
**Multi-keyword** [OSSK16]. **multi-layer** [WR08]. **Multi-Net** [ZZW<sup>+</sup>10].  
**Multi-operator** [EHM15]. **multi-party** [BNTW12, KM03]. **multi-phase** [Das12].  
**multiagent** [ZGC07]. **multicast** [MP15, PJ10, TWP08]. **multicast-based**

[MP15]. **multicoupon** [HIDFGHR19]. **multifactor** [IT05]. **multiple** [CC12, HMCD04, WMS<sup>+</sup>19]. **multiple-key** [CC12]. **multiplication** [YOV09]. **multiplications** [HTM11]. **multipliers** [YOV09]. **multiresolution** [VSR15]. **multiset** [BA16]. **multisignatures** [HRL09]. **must** [ASN<sup>+</sup>16]. **Mutual** [HZL<sup>+</sup>17].

**naive** [Sen14]. **names** [CYA<sup>+</sup>18]. **need** [JTV19]. **Negative** [EFH09, EAH<sup>+</sup>07, DNF<sup>+</sup>19]. **negotiation** [KLMM09]. **negotiation-based** [KLMM09]. **Net** [ZZW<sup>+</sup>10, WYL<sup>+</sup>12]. **Nets** [SSF15]. **Network** [GPS17, ABCC08, BMP<sup>+</sup>14, CL09, EMRN17, GBG18, GH05, LBZ<sup>+</sup>10, wLW05, MYLZ14, PMPGMLLM12, RS18, SAT09, TLX09, WYL<sup>+</sup>12, dAKdG10]. **Network-based** [GPS17]. **Networked** [MR03]. **networks** [ACB14, CMR06, CPPK15, Das12, DRPW12, EHM15, EMRN17, Gol12, GBG18, RBEH15, RMSCR19, SS17, SSN15, SF17, YRW14, ZXZ<sup>+</sup>11, BT07]. **next** [AMLH18]. **next-generation** [AMLH18]. **NICs** [CBC08]. **NIZK** [WT16]. **no** [BB04b, CMN<sup>+</sup>18]. **noise** [EG18]. **noisy** [BDH<sup>+</sup>10, KML03]. **non** [CDF<sup>+</sup>13, CHZ16, CL09, EHSS14, GRV05, HYWS11, KM03, MP16, RMSCR19]. **non-compressing** [MP16]. **non-delegatability** [HYWS11]. **non-deterministic** [RMSCR19]. **non-interactive** [CDF<sup>+</sup>13, CHZ16, CL09, EHSS14]. **non-repudiation** [GRV05, KM03]. **noninterference** [BP04]. **note** [ZZH08]. **Nothing** [MTW<sup>+</sup>14]. **notions** [BCL09, BFS<sup>+</sup>13]. **novel** [KNL16, Lin15]. **numerical** [SMMN12, ZO13].

**obfuscation** [OSSK16]. **object** [HS09, SS05b]. **object-sensitive** [HS09].

**oblivious** [BA16, HSMY12, LD17, TND<sup>+</sup>15]. **obtain** [Bra06]. **Off** [BCD<sup>+</sup>13, CJMS19]. **Off-line** [BCD<sup>+</sup>13]. **Off-line/on-line** [BCD<sup>+</sup>13]. **Offline** [MWZ06, LMG17, LBZ<sup>+</sup>10]. **OFMC** [BMV05]. **Ohgishi** [CHZ16]. **Okamoto** [GMMV05]. **on-line** [BCD<sup>+</sup>13, LMMO04]. **on-the-fly** [CL13]. **one** [GMS03, MLCS16, YRW14]. **one-class** [MLCS16]. **one-pass** [YRW14]. **onion** [CDF<sup>+</sup>13, CFG17]. **OnionDNS** [SCL<sup>+</sup>18]. **online** [LMG17, LD07, LBZ<sup>+</sup>10]. **online/offline** [LMG17, LBZ<sup>+</sup>10]. **only** [LD17]. **Opacity** [BKMR08]. **open** [Küs05, RM12]. **open-ended** [Küs05]. **opening** [EHSS14]. **operational** [SGJC18]. **operations** [BA16, HTM11, NRC15]. **operator** [EHM15]. **Optimal** [DRPW12, EG18, GYL<sup>+</sup>07, VSR15]. **optimisation** [PDB11]. **optimistic** [DGZFGH13, HYWS12, SEXY18]. **Optimization** [MU18, LL14]. **oracle** [HYWS11, Yon18]. **oracles** [HSMW08, HYWS12]. **OrBAC** [EEB<sup>+</sup>15, GBDJ14]. **order** [LM06]. **oriented** [SK16, WW07]. **OSBE** [HSMY12]. **Outbound** [Smi04]. **Outsourced** [FHV18, CTM<sup>+</sup>16, LD17]. **outsourcing** [AL05, GYL<sup>+</sup>07, HJDC15, KU16]. **overview** [BMP05]. **Own** [ACMV15].

**packets** [vORM06]. **packing** [BEPL<sup>+</sup>17]. **pads** [dSFK19]. **Paillier** [NSNK06, DJN10]. **Paillier-based** [NSNK06]. **pairing** [MSGCDPSS18, YRW14, ZZH08]. **pairing-based** [MSGCDPSS18]. **pairing-free** [YRW14]. **pairings** [BCL09, CCS07]. **papers** [ACM05]. **paradigm** [BCD<sup>+</sup>13]. **parallelism** [SBB19]. **parallelizable** [MP16]. **parameter** [DTK<sup>+</sup>18]. **parameters** [NMBB12]. **parazoa** [AMP12]. **parties** [HZL<sup>+</sup>17, KPM12]. **party** [BNTW12, KM03, LCL16, MR04]. **pass**

[YRW14]. **Passive** [CBC08, SS05a, ALOW15]. **Passive-attack** [SS05a]. **Password** [MPS10, MRW02, CG14, CJMS19, GTM11, KJS17, Lop18, MSKD16, SB09, WLLW14]. **Password-authenticated** [MPS10]. **passwords** [CFBvO09, JTV19]. **past** [JG15, LMMP06]. **patching** [JM17]. **pattern** [FHV18, OSSK16, SBB19]. **patterns** [CFBvO09]. **pay** [Roe11a, Roe11b, DZW<sup>+</sup>18]. **pay-TV** [Roe11b, Roe11a, DZW<sup>+</sup>18]. **PBAC** [Kud02]. **perception** [MTSH18]. **Perceptual** [SB14]. **Perfect** [Hub12]. **performance** [BBR18, BNTW12, HIDFGHR19, IDHRPCMP15, SK16, SSN15]. **Periodicity** [JM17]. **permutations** [BR17]. **personal** [IHNT02, QLZH15]. **personality** [PPL15]. **Petri** [SSFB15]. **phase** [Das12]. **phone** [CF07, GSM<sup>+</sup>11, HCN15, WGMB13]. **phylogeny** [BDM19]. **physical** [SM10]. **physically** [BR17]. **PIN** [dSFK19]. **PINs** [MTSH18]. **PIOAs** [Yon18]. **PIR** [DYDW10]. **pirates** [Nui12]. **PiSHi** [MBHT17]. **PKI** [BB04b, Daw04, LC04, LMMP06, LMMO04, VSM06]. **PLAID** [DFF<sup>+</sup>16]. **Plaintext** [MPS14]. **platform** [IDHRPCMP15, MBRPS18]. **platforms** [KPM12, RHGTSC17]. **point** [ABB17, KW15]. **policies** [ABCC08, ACMV15, AICC18, BCL13, CF03, CCB08, KAC17, LBW05, LRB<sup>+</sup>10, SB09]. **Policy** [SAL17, BZV05, GMH14, JSMG18a, JSMG18b, KNL16, MS15, TG05, XSA13, dAKdG10]. **PolicyUpdater** [CZ06]. **pollution** [EMRN17]. **Polly** [SGE02]. **polymorphic** [KJG<sup>+</sup>11]. **polynomial** [SGE02, TND<sup>+</sup>15]. **polynomial-based** [SGE02]. **polynomials** [GMS03]. **Portfolio** [LL14]. **posteriori** [ACBC<sup>+</sup>15]. **potential** [WGMB13]. **practicability** [IDHRPCMP15]. **Practical** [LLW<sup>+</sup>16, ALOW15, GKS19, KOSU16, LCL14, Pen12, VHT09, WR15]. **practices** [LD07]. **pre** [CMR06, Pen13]. **pre-computation** [Pen13]. **pre-distribution** [CMR06]. **Preface** [Ano11a, ACM05, BGP07a, BM05, Daw04, DV08, DMRS07, Pri04, Sne05, Wai04, ZL06]. **prefix** [BGKZ12]. **present** [LMMP06]. **preservation** [RAC16]. **preserve** [EEB<sup>+</sup>15]. **preserved** [JSMG18a, LD17]. **preserving** [ABFO08, BGK08, CTM<sup>+</sup>16, DFBJR18, GKS19, HLS18, KOSU16, KB13, KNL16, MB16, MCD11, NST09, NA14, QLZH15, RDK18, WMS<sup>+</sup>19]. **Preventing** [RAC16, PS17, YP12]. **prevention** [VL13]. **primitives** [MP16, SM10]. **principle** [Bel10]. **Principles** [CGL<sup>+</sup>11]. **Privacy** [KB13, MB16, MSP<sup>+</sup>13, NST09, QLZH15, RDK18, ABFO08, AJC<sup>+</sup>09, AMRR17, BGK08, BCA<sup>+</sup>10, BDHZ15, Bra06, CTM<sup>+</sup>16, EG18, EAH<sup>+</sup>07, GLMS<sup>+</sup>04, GKS19, GYL<sup>+</sup>07, KOSU16, KBH07, KNL16, LD07, LD17, LeSCL<sup>+</sup>18, MCD11, MBRPS18, NA14, PGMLK<sup>+</sup>13, RSPMB16, RMPADF13, WMS<sup>+</sup>19, YAM<sup>+</sup>15, ZZG19]. **privacy-aware** [MBRPS18, RSPMB16]. **Privacy-enhanced** [MSP<sup>+</sup>13]. **privacy-preserved** [LD17]. **Privacy-preserving** [KB13, MB16, NST09, QLZH15, RDK18, ABFO08, BGK08, CTM<sup>+</sup>16, GKS19, KOSU16, MCD11, NA14, WMS<sup>+</sup>19]. **Private** [BA16, DMP13, BDD01, BGP07b, KW15, LMD17, VH19, WR15]. **Probabilistic** [DHW11, BP04, GYL<sup>+</sup>07, MCD11, PJ10]. **problem** [CC12, GOBdLC11, GMS03, GP17, KG11, RG13, TWP08, YSM10]. **problems** [HMCD04]. **process** [BDM19, HBH12]. **processes** [RHL17]. **profiling** [LCPD14]. **program** [BDF04, HS09]. **programmability** [Yon18]. **programmable** [Smi04]. **programming** [WZ07]. **programs** [KM07, WGMB13]. **progressive** [WPD18]. **project** [BFP03]. **proof** [HLS18, WLLW14]. **proofs** [BCJ<sup>+</sup>11]. **Proposal**

[IHNT02, IT05]. **proposals** [BJ16]. **protected** [BJ16]. **Protecting** [EAH<sup>+</sup>07]. **protection** [AJC<sup>+</sup>09, GKBS12, KK17]. **protocol** [Ala17, ALPW13, Bel10, BFT08, CL09, DFF<sup>+</sup>16, DGZFGH13, HL04, HYWS12, LSWW14, ML17, RG13, RGL16, YRW14, YAM<sup>+</sup>15]. **Protocols** [DHS04, AC08, ABFL12, BGK08, BMV05, BBR18, BNN04, CCS07, DVB02, DS07, Fra18, GLP03, GRV05, HLS18, KM03, K us05, LCL16, MP15, MSN02, MS14, SSFB15, Ust11, Vaj16, VdWZ14]. **Provable** [YRW14, NSNK06]. **Provably** [LCL14, RG13, VHT09, YYK<sup>+</sup>18]. **provenance** [Abb13]. **providing** [PGMLK<sup>+</sup>13]. **Provision** [Kud02]. **Provision-based** [Kud02]. **provisioning** [TGS17]. **proxy** [Lin15]. **pseudo** [HIST09]. **pseudo-freeness** [HIST09]. **public** [ALOW15, BCJ<sup>+</sup>11, BZ03, DJN10, EHSS14, GW09, LC04, Pen12, SSP14, Gri06]. **public-key** [ALOW15, BCJ<sup>+</sup>11, DJN10, EHSS14, SSP14]. **push** [BFPP07]. **push-based** [BFPP07]. **pushdown** [BCL13]. **puzzle** [WR08]. **puzzle-based** [WR08]. **PVSS** [Pen12].

**QR** [HZL<sup>+</sup>17]. **QR-code** [HZL<sup>+</sup>17]. **query** [BB04a, KCM<sup>+</sup>15]. **queue** [BF13].

**race** [sLC05]. **RAM** [LD17]. **RAM-based** [LD17]. **ramp** [LMD17]. **random** [BR17, BR18, Das12, HSMW08, HYWS11, HYWS12, VSR15, Yon18]. **Randomized** [ML14]. **randomness** [BGP07b]. **ransomware** [CMN<sup>+</sup>18]. **rational** [ETAHCR08]. **RBAC** [BGTCCBB10]. **re** [GI19, Dan07]. **Re-encryption** [Dan07]. **re-identification** [GI19]. **reacting** [AGIK07]. **reactive** [BDHK08]. **Reactively** [BPW05a]. **reader** [GdKGV14]. **real** [KCB17, RLEM18]. **real-time** [KCB17]. **realistic** [HS15]. **realization** [KAC16]. **realizing** [RD16, ZZG19]. **really** [BM11].

**reasoning** [GMMZ06]. **recognition** [GCS ABdSS12]. **recommender** [ABFO08]. **record** [QLZH15]. **records** [QDW<sup>+</sup>15]. **recovery** [CMS10, NVB<sup>+</sup>02]. **rectangle** [Lu09]. **recursive** [Rus04]. **Redistributing** [LKH09]. **refinement** [dAKdG10]. **reflects** [PPL15]. **refunds** [KO02]. **regions** [EG18]. **Regular** [Bae10, WR15]. **regular-expression** [WR15]. **rekeying** [PJ10]. **Related** [Lu09, Dan07]. **Related-key** [Lu09]. **relation** [MS11, Pen11]. **Relations** [FGS12]. **relationships** [CTM<sup>+</sup>16, RAC16]. **relaxed** [BFS<sup>+</sup>13]. **release** [NAM06]. **reliable** [ABCC08, AvO13]. **remanence** [SV11]. **remote** [CGL<sup>+</sup>11, GW09, MMS16, YAM<sup>+</sup>15]. **renewable** [BDH<sup>+</sup>10]. **repeated** [vORM06]. **Replacement** [XCW<sup>+</sup>12]. **representations** [EFH09]. **repudiation** [GRV05, KM03]. **reputation** [LI07, SdHZ16]. **Requirements** [GMMZ06, WW07, SK16]. **Research** [Gri06, RM12]. **residence** [PPL15]. **resident** [BMP<sup>+</sup>14]. **resilient** [MR03, WT16]. **resistance** [TGS17]. **resistant** [CHKO12, SCL<sup>+</sup>18, MS09]. **resolutions** [RV03]. **Resolving** [CTM<sup>+</sup>16]. **resource** [LVK18, SS17]. **resource-bounded** [LVK18]. **resource-constrained** [SS17]. **resources** [TZH04]. **response** [SSD14]. **Restricted** [SF17]. **results** [BCD<sup>+</sup>13, DLR15]. **retention** [GSM<sup>+</sup>11]. **retrieval** [BDD01, LMD17]. **reusable** [KO02]. **reveal** [GSM<sup>+</sup>11]. **Reverse** [MLM19, EAH<sup>+</sup>07]. **reversed** [KYH18]. **revisited** [BZ03, BRS06, BVS07, BCD<sup>+</sup>13, CHZ16, GMMV05, RDK18]. **revocable** [JCL<sup>+</sup>18, Lin15]. **revocation** [MFES04, NST09, QLZH15]. **revoke** [NP10]. **revoking** [DdP13]. **RFID** [ALOW15, SV11]. **rich** [RMSCR19]. **right** [Bae10, Lop18]. **right-to-left** [Bae10]. **rights** [ASF04, LKH09]. **Rigorous** [GH05]. **ring**

[GCH<sup>+</sup>19]. **Risk** [MYLZ14, MTSH18, SSD14, WHS18]. **risks** [GYL<sup>+</sup>07]. **robust** [GKBS12, MS11]. **role** [CK08, ZVH15]. **role-based** [CK08, ZVH15]. **ROM** [MLM19]. **RORI** [GBDJ14]. **RORI-based** [GBDJ14]. **round** [ABM<sup>+</sup>12, BGP07b, GNS14, NSNK06]. **rounds** [Lu09]. **Routing** [SSN15, BT07, CDF<sup>+</sup>13, CFG17, KCB17]. **RPCAE** [Lin15]. **rPIR** [LMD17]. **RSA** [LC04, MPS10]. **rule** [KAC16]. **rules** [ABCC08, KAC17]. **run** [LBW05]. **run-time** [LBW05]. **runtime** [DLR15].

**safeguarding** [BCA<sup>+</sup>10]. **safer** [CMMPS15]. **sail** [BB04b]. **Sakai** [CHZ16]. **SAML** [EWR<sup>+</sup>09]. **samples** [SSVC16]. **Sandbox** [SSE<sup>+</sup>15]. **SAS** [KJG<sup>+</sup>11]. **SAT** [AC08]. **SAT-based** [AC08]. **satellite** [KW15]. **SCADA** [Ano11b, HBH12]. **scalability** [TGS17]. **Scalable** [RMSCR19, KCB17, SB14, YYK<sup>+</sup>18]. **scale** [Das12, RLEM18, TLX09]. **scan** [AvO13]. **scanning** [CBC08]. **scenarios** [HS15, PGMLK<sup>+</sup>13]. **scheme** [BZ03, BDD01, BCL09, CG14, CMR06, CC10, Das12, DSY06, EMRN17, HCN15, KOSU16, Lin15, PDB11, QDW09, RHL17, WLLW14]. **schemes** [BPW05a, BR18, CJMS19, DdP13, Dan07, DHS04, Den08, GP17, HSMY12, HYWS11, NP10]. **scoring** [OSSK16]. **SDSI** [LM06]. **search** [HH16, KJS17, OSSK16]. **searchability** [HJDC15]. **searchable** [HK19, LZQ<sup>+</sup>18]. **searches** [WR15]. **searching** [VH19]. **Seberry** [BZ03]. **second** [ABM<sup>+</sup>12]. **secrecy** [CDF<sup>+</sup>13, Hub12]. **secret** [DdP13, GMS03, HJDC15, LMD17, PPSS13, QDW09]. **secrets** [BW08, JTV19]. **Secure** [ABB17, AL05, BVS07, DZW<sup>+</sup>18, HN14, HSMW08, KW15, LCL16, MSKD16, SJ09, SBB19, ZXZ<sup>+</sup>11, ASF04, Ala17, BPW05a, BDF04, BNTW12, BT07, DdP13, KME<sup>+</sup>16, KU16, KSZ07, LCL14, LLW<sup>+</sup>16, MB16, MLO<sup>+</sup>04, MBRPS18, MPP14, NMBB12, Nui12, PJ10, QDW<sup>+</sup>15, RG13, SJ10, SK16, Smi04, TND<sup>+</sup>15, WPD18, YYK<sup>+</sup>18, YAM<sup>+</sup>15]. **secured** [EHM15]. **Securing** [DDPS02, BFPP07, CC10].

**Security** [Ano14, BCL13, BDHZ15, FSG<sup>+</sup>14, GMH14, HJDC15, OT06, ZZW<sup>+</sup>10, ACB14, ABCC08, ABM<sup>+</sup>12, Ano11b, AC08, AICC18, BCJ<sup>+</sup>11, BGKZ12, BMV05, Bel10, BCF<sup>+</sup>17, BFT08, BCL09, BFS<sup>+</sup>13, BNN04, BCEM04, CLW<sup>+</sup>11, CFBvO09, CYK09, CLPP11, CCB08, DSB19, DM07, Den08, DRPW12, EHM15, FGS12, GS15, GLMS<sup>+</sup>04, GYL<sup>+</sup>07, GRV05, GH05, HS15, HMCD04, JGK14, KKKV07, KBH07, KLMM09, KMR09, Lan01, LBW05, LP11, LV10, wLW05, MdSC<sup>+</sup>15, MP15, MSGCDPSS18, NSNK06, PDB11, RM12, RG13, RGL16, SK16, SS17, SSN15, SM10, SAT09, TG05, VSM06, WYL<sup>+</sup>12, WHS18, YLL<sup>+</sup>18, YRW14, YP06, ZM07, dAKdG10, vOLW05, BJ15, Pri04, KBH07]. **security-mediated** [VSM06]. **security-sensitive** [HS15]. **seizure** [SCL<sup>+</sup>18]. **seizure-resistant** [SCL<sup>+</sup>18]. **selected** [ACM05]. **Selecting** [NMBB12]. **selection** [GBDJ14, SJ10, SSVC16, ZGC07]. **selective** [ZZG19]. **selective-ID** [ZZG19]. **SELinux** [XSA13]. **sellers** [ZGC07]. **semantics** [KJG<sup>+</sup>11]. **sensitive** [HS15, HS09, RAC16, ZO13]. **sensor** [CMR06, Das12, KCM<sup>+</sup>15, LBZ<sup>+</sup>10, RBEH15, YRW14, ZXZ<sup>+</sup>11]. **sensors** [CLW<sup>+</sup>11, MTSH18]. **sequence** [AL05, BZV05, KSM10]. **sequential** [BDPV14]. **server** [MYLZ14]. **service** [LLWY09, NA14, WR08, WW07, TGS17]. **service-oriented** [WW07]. **services** [AV17, DDPS02, EWR<sup>+</sup>09, KBH07, MS15, PMPGMLLM12, VL13]. **sessions** [ACB14]. **set** [BA16, MCD11, WZ07, BMP05]. **Sets** [SAL17]. **SHA** [ABM<sup>+</sup>12, KJS17]. **SHA-1** [KJS17]. **SHA-3** [ABM<sup>+</sup>12]. **shared** [BS05]. **sharing** [CMMPS15, HJDC15, LKH09, LMD17, QDW09]. **sharing-based**

[HJDC15, LMD17]. **Short** [Nui12, JSMG18b, LMG17, SK14]. **shortcut** [MLM19]. **Shoulder** [WLLW14]. **Shoulder-surfing-proof** [WLLW14]. **shuffle** [DYDW10, Pen13]. **shuffles** [NSNK06]. **shuffling** [PDB11]. **side** [dSFK19, HS15, MTW<sup>+</sup>14]. **side-channel** [dSFK19, MTW<sup>+</sup>14]. **Signature** [JMV01, BPW05a, DHS04, EHSS14, GP17, HSMW08, HYWS11, KJG<sup>+</sup>11, LBZ<sup>+</sup>10, RD16, Yon18, ZBD06]. **signatures** [ACHO13, BCD<sup>+</sup>13, GCH<sup>+</sup>19, IDHRPCMP15, IT05, KJ14, MR04, PS17, SEXY18, SK14, WPD18, YSM10]. **signcrypt** [LMG17, RD16]. **signers** [BRS06]. **signing** [IZS08]. **SilentKnock** [VHT09]. **Simplified** [BCL09]. **simulatability** [BDHK08]. **simulatable** [BPW05b]. **simulation** [SB09, WT16]. **simulation-extractable** [WT16]. **size** [DFBJR18, PPSS13]. **Skype** [DBMS10]. **SLE** [vOLW05]. **slicing** [MS15]. **small** [MP16]. **smart** [DMDD16, GdKGV14, MSP<sup>+</sup>13, MPP14, RDK18]. **SOAP** [DDPS02]. **social** [DMP13, KPM12, RAC16]. **software** [JM17, MLO<sup>+</sup>04, SK16, SK06, XCW<sup>+</sup>12, ZGK07]. **solution** [MCD11, PMPGMLLM12, SK16]. **solutions** [HIDFGHR19]. **Solving** [GOBdIC11, GP17, HMCDD04]. **sound** [BCJ<sup>+</sup>11, BDPV14]. **soundness** [BP08]. **sources** [CF03]. **spam** [ASN<sup>+</sup>16, CACB16]. **spammer** [ASN<sup>+</sup>16]. **sparse** [ACB14]. **spatio** [SKK<sup>+</sup>17]. **spatio-temporal** [SKK<sup>+</sup>17]. **Special** [Ano11b, BJ15, KBH07, ACM05, BM05, Daw04, Pri04, Sne05]. **specific** [KME<sup>+</sup>16]. **specifications** [ZGK07]. **Specifying** [BGK08]. **SPIT** [GKBS12]. **SPKI** [LM06]. **SPKI/SDSI** [LM06]. **sponge** [AMP12]. **spoofing** [Hub12]. **spread** [WGMB13]. **SQL** [DSB19]. **squaring** [HTM11]. **SSL-protected** [BJ16]. **SSO** [PMPGMLLM12]. **Stack** [BDF04]. **standard** [Ala17, CH16, SSP14]. **standards** [DFF<sup>+</sup>16]. **star** [RS18]. **State** [vOLW05]. **Stateful** [LMMS17, YLL<sup>+</sup>18]. **Static** [SS05b, CMS10, MS15, SSE<sup>+</sup>15, ZM07]. **status** [HC10]. **Stealing** [MTSH18]. **steganography** [Des09, SJ09, SJ10]. **Stochastic** [WYL<sup>+</sup>12]. **storage** [GW09, LZQ<sup>+</sup>18, YAM<sup>+</sup>15]. **storages** [CTM<sup>+</sup>16]. **storing** [HK19]. **STORK** [RLEM18]. **STR** [IHNT02]. **strategies** [wLW05]. **stream** [HL04, IMI18, TWP08]. **streaming** [ZO13]. **strength** [RGL16]. **string** [KCM<sup>+</sup>15]. **Strong** [CHKO12, HYWS11, YLL<sup>+</sup>18]. **stronger** [PDB11]. **Strongly** [WT16]. **Structural** [KA18, GI19]. **structure** [QDW09, TTS<sup>+</sup>06]. **structures** [KN07, Küs05, RD16, Rus04]. **study** [BSCZ11, BF13, DSB19, DSRHC16, GLMS<sup>+</sup>04, SKK<sup>+</sup>17, XSA13]. **style** [BPW05b, BP08]. **subject** [LcSCL<sup>+</sup>18]. **subjective** [SdHZ16]. **subset** [KG11]. **subspace** [RG13]. **substitution** [BRS06]. **subtree** [Roe11a, Roe11b]. **Sufficient** [BDPV14]. **suffix** [BGKZ12]. **suffix-free-prefix-free** [BGKZ12]. **suitable** [Pla09]. **sum** [KG11]. **Supervised** [GSAMCA18]. **support** [CON09, MLCS16]. **supporting** [ARMLS06, JSMG18a, JSMG18b, RV03]. **supports** [WR15]. **surfing** [WLLW14]. **surveillance** [Lev07, LcSCL<sup>+</sup>18, MBRPS18, RSPMB16]. **survey** [Den08, FSG<sup>+</sup>14]. **suspect** [GBG18]. **swarm** [KKK17]. **swarms** [SS17]. **symbolic** [BMV05, BFT08]. **Symmetric** [BPW05b, HK19]. **Symposium** [BJ15]. **System** [JTV19, ABFO08, Ano11b, BFP03, BFPP07, CL08, CZ06, DJN10, IZS08, KO02, KJS17, LKH09, LCL14, MGV17, MFES04, MS15, RM12, RLEM18, RBEH15, SSD14, VL13, vORM06, DNF<sup>+</sup>19]. **System-assigned** [JTV19]. **system-based** [MGV17]. **systematic** [SK16]. **systems** [ASF04, AMRR17, BDHZ15, BB04a,

BCF<sup>+</sup>17, BKMR08, DSRHC16, GMH14, HZL<sup>+</sup>17, Hub12, LVK18, LV10, RSPMB16, Roe11a, SK16, SV11, SS05a, ZGC07, dAKdG10, Roe11b).

**Tacit** [JTV19]. **tag** [EMRN17]. **tagging** [GP17]. **tags** [ACHO13, ALOW15]. **Taking** [BRS06, KNL16]. **tallying** [MMS16]. **Talos** [CMN<sup>+</sup>18]. **tampering** [DTK<sup>+</sup>18]. **targeted** [GBG18, KOSU16]. **task** [Yon18]. **task-PIOAs** [Yon18]. **technique** [GLP03, SSV16]. **Techniques** [TG05, BMP<sup>+</sup>14, CH16, KA18, SMMN12, SSE<sup>+</sup>15]. **technologies** [KBH07, SAT09]. **technology** [LH15]. **telephony** [AMRR17, CACB16]. **tell** [MBHT17]. **templates** [CC10, HTM11]. **temporal** [SKK<sup>+</sup>17]. **Temporarily** [GSS10]. **TermID** [KKK17]. **test** [LLBL18]. **testbed** [RM12]. **testing** [AV17]. **their** [HSMY12, KAC17, WGMB13]. **theoretic** [LVK18]. **theoretical** [BCEM04]. **theoretically** [TND<sup>+</sup>15]. **Theory** [Rus04]. **third** [KPM12]. **threat** [MdSC<sup>+</sup>15, YP12]. **three** [LCL16, NSNK06, Nui12]. **three-party** [LCL16]. **three-round** [NSNK06]. **Threshold** [Pen12, WMS<sup>+</sup>19, BCD<sup>+</sup>13, JSMG18b, QDW09]. **Time** [KME<sup>+</sup>16, CJMS19, DMDD16, KCB17, LLBL18, LKH09, LBW05, NAM06, Vaj16]. **time-aware** [Vaj16]. **time-based** [LKH09, NAM06]. **time-memory** [CJMS19]. **Time-specific** [KME<sup>+</sup>16]. **timed** [GLMS<sup>+</sup>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]. **tool** [SB09]. **tools** [AV17]. **top** [SCL<sup>+</sup>18]. **top-level** [SCL<sup>+</sup>18]. **trace** [NP10]. **traceable** [ACHO13, SK14]. **traceback** [RS18]. **tracing** [DdP13, LCL14, Roe11a, Roe11b]. **Track** [BJ15, DFF<sup>+</sup>16]. **trade** [CJMS19].

**trade-off** [CJMS19]. **tradeoff** [SSN15]. **traditional** [GLP03]. **traffic** [SPDR17]. **training** [GSAMCA18]. **transactions** [CMS10, SK06]. **transform** [KCM<sup>+</sup>15, SJ10]. **Transformational** [KM07]. **transformations** [BZV05, BDF04]. **Transforms** [MTW<sup>+</sup>14]. **transition** [BKMR08]. **trapdoor** [ACHO13]. **tree** [ABR16, BDPV14, DRPW12, MFES04]. **trees** [KB13, RBD02]. **triangle** [LCL16]. **Trojan** [BSCZ11]. **truly** [BR18]. **Trust** [KN07, Abb13, GMMZ06, KBH07, LD07, LLWY09, LV10, QLOW09, RSPMB16, WW07, ZGC07]. **Trusted** [LH15]. **trustworthy** [MBRPS18]. **truth** [AvO13]. **TTP** [ZBD06]. **TTS** [DSY06]. **Tuning** [GNS14]. **TV** [Roe11b, DZW<sup>+</sup>18, Roe11a]. **twice** [YOV09]. **Two** [MR04, ML17, CG14, GNS14, MS09, SSFB15]. **two-channel** [MS09]. **Two-factor** [ML17, CG14]. **Two-party** [MR04]. **two-round** [GNS14]. **typing** [DM07, KM07].

**ubiquitous** [LI07]. **UC** [BP08]. **UMTS** [LSWW14]. **UMTS/LTE** [LSWW14]. **unauthorized** [YP12]. **Uncertain** [AJC<sup>+</sup>09]. **uncertainty** [SdHZ16]. **unclonable** [BR17, SM10]. **Understanding** [LM06, MS15, RSPMB16, WGMB13]. **undetectable** [VHT09]. **unforgeability** [Yon18]. **unification** [KM07]. **uniform** [KAC16]. **unifying** [BCD<sup>+</sup>13]. **universal** [HSMW08, Vaj16, Dan07]. **unknown** [BEPL<sup>+</sup>17]. **unmanaged** [KKKV07]. **Unpicking** [DFF<sup>+</sup>16]. **untrusted** [GW09]. **updatable** [ABR16]. **update** [JSMG18a]. **uploaders** [WMS<sup>+</sup>19]. **URL** [KCM<sup>+</sup>15]. **Usage** [LMMS17, SF17]. **use** [LMMO04, Pla09, SK06, SS05b]. **use-based** [SS05b]. **useful** [DHS04]. **User** [CFBvO09, CLPP11, BFG<sup>+</sup>13, CON09, MGV17, MTSH18, PGMLK<sup>+</sup>13, XSA13]. **user-controlled** [BFG<sup>+</sup>13]. **User-friendly** [CLPP11]. **users** [CF07, KOSU16]. **Using**



[GBG18, HTM11, RBD02, SJ10, Sen14, TZH04, ACB14, AMLH18, AGIK07, AICC18, ACBC<sup>+</sup>15, BMP<sup>+</sup>14, BCL13, BDMM19, CLW<sup>+</sup>11, CF07, DGF<sup>+</sup>17, EWR<sup>+</sup>09, GKKT10, GSAMCA18, GBDJ14, GKBS12, HLKI15, HCN15, HL04, IDHRPCMP15, JCL<sup>+</sup>18, KJS17, KA18, KSM10, LM06, MB16, MSKD16, MP15, MP16, MLCS16, QLZH15, RHL17, SSFB15, SSD14, VH19, Yon18, You06, vOLW05].  
**utilising** [LCPD14].

**validation** [AGIK07, ZBD06, dAKdG10].

**variants** [BCD<sup>+</sup>13]. **vector**

[MMS16, MLCS16]. **vector-based** [MMS16].

**vehicular** [MB16, SF17]. **Verifiable**

[NSNK06, KU16, LZQ<sup>+</sup>18]. **Verifiably**

[WPD18, KJ14, SEXY18]. **verification**

[BMP05, CL13, DS07, GMH14, Pen12,

Pen13, Yon18]. **verifier**

[HSMW08, HYWS11]. **VERIFY** [ACM05].

**Verifying** [MP15]. **versus** [MTSH18]. **very**

[Bae10]. **via** [MTSH18, MS14]. **victims**

[CMN<sup>+</sup>18]. **video**

[LcSCL<sup>+</sup>18, MBRPS18, RSPMB16, SB14].

**views** [KMR09]. **violation** [GYL<sup>+</sup>07].

**virtual** [RM12]. **visible** [LC04].

**Visualization** [XSA13].

**Visualization-based** [XSA13]. **visualized**

[HLKI15]. **voice** [WAB<sup>+</sup>09]. **VoIP** [VL13].

**volumes** [SMMN12]. **voting**

[DJN10, MMS16, MS11, Pen11].

**vulnerabilities** [DTK<sup>+</sup>18, SNX19].

**vulnerability**

[AV17, JM17, MLM19, ZRJ14].

**warning** [ABFL12]. **Watermarking**

[Fra18, BMP<sup>+</sup>14]. **wavelet** [KCM<sup>+</sup>15]. **web**

[AYHK18, AV17, DTK<sup>+</sup>18, GLMS<sup>+</sup>04,

MSKD16, BFP03, BJ16, EWR<sup>+</sup>09, KGG09,

SNX19]. **web-based** [AYHK18]. **weighted**

[Sen14]. **wildcard** [HH16]. **WinRAR**

[YP06]. **Wireless** [BT07, CMR06, CBC08,

EHM15, EMRN17, KKK17, LBZ<sup>+</sup>10,

RBEH15, SS17, SSN15, YRW14, ZXZ<sup>+</sup>11].

**Wirelessly** [GdKGV14]. **without** [GW09,

HSMW08, HYWS11, HYWS12, YSM10].

**workflow** [ARMLS06]. **workplace** [Lev07].

**worm** [AGIK07, KJG<sup>+</sup>11]. **worms**

[vORM06]. **Write** [LD17, JTV19].

**Write-only** [LD17].

**XACML** [CON09]. **Xen** [PPL15].

**Xen-based** [PPL15]. **XML**

[BFPP07, CF03, KMR09]. **XOR**

[BP08, BGP07b]. **XQuery** [DTK<sup>+</sup>18].

**XTEA** [Lu09].

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

[BPW05b, BP08]. **yoking** [HLS18].

**zero** [DGF<sup>+</sup>17]. **zero-day** [DGF<sup>+</sup>17].

**Zheng** [BZ03]. **ZombieCoin** [AMLH18].

## References

**Abbadi:2013:FET**

[Abb13]

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**

[ABB17]

Mehrdad Aliasgari, Marina 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]
- [ABCC08] **Alfaro:2008:CAC**  
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>. [ABM<sup>+</sup>12]
- [ABFL12] **Ates:2012:WHI**  
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>. [ABN14]
- Aimeur:2008:LPP**  
Esma Aimeur, 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>.
- 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>.
- Albeshri:2014:EGI**  
Aiiad Albeshri, Colin Boyd, and Juan González Nieto. Enhanced GeoProof: improved geographic assurance for data in the cloud. *International Journal of In-*

- formation 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>.
- [ABR16] **Abbes:2016:DFC**  
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>.
- [AC08] **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>.
- [ACB14] **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>.
- [ACBC<sup>+</sup>15] **Azkie: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 Information 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/s10207-017-0041-y>.

- com/article/10.1007/s10207-016-0322-4.
- [ACHO13] 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] 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] 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>.
- [AD08] 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>.
- [AGIK07] 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>.

- [AICC18] **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. [AL05]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0357-6>.
- [AJC<sup>+</sup>09] **An:2009:UIC**  
 Xiangdong An, Dawn Jutla, Nick Cercone, Charnyote Pluempitiwiriyaewej, and Hai Wang. Uncertain inference control in privacy protection. *International Journal of Information Security*, 8(6): 423–431, December 2009. [Ala17]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0088-z>.
- [AKG16] **Anagnostopoulos:2016:NFM**  
 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. [ALOW15]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0310-0>.
- Atallah:2005:SOS**  
 Mikhail J. Atallah and Jiangtao Li. Secure outsourcing of sequence comparisons. *International Journal of Information Security*, 4(4): 277–287, October 2005. [AL05]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0070-3>.
- Alawatugoda:2017:GCM**  
 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. [Ala17]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0346-9>.
- Arbit:2015:IPK**  
 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>. [AMP12]
- [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>. [AMRR17]
- [Ali:2018:ZMN] Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao. ZombieCoin 2.0: managing next-generation botnets using Bitcoin. *International Journal of Information Security*, 17(4): 411–422, August 2018. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0379-8>. [Ano11a]
- [Andreeva:2012:PFG] Elena Andreeva, Bart Menink, and Bart Preneel. The parazoa family: generalizing the sponge hash functions. *International Journal of Information Security*, 11(3):149–165, June 2012. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0157-6>.
- [Arapinis:2017:APM] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Dermot Ryan. Analysis of privacy in mobile telephony systems. *International Journal of Information Security*, 16(5): 491–523, October 2017. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0338-9>; <http://link.springer.com/content/pdf/10.1007/s10207-016-0338-9.pdf>.
- [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/s10207-011-0061-1>.

- 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/s10207-011-0128-3>. [ARMLS06]
- [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>. [ASAAS15]
- [ANS+12] **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/s10207-012-0168-3>. [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>.
- [Al-Saleh:2015:IDC] **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] **Abie:2004:DDR**  
Habtamu Abie, Pål Spilling,

and Bent Foyn. 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>. [AvO13]

**Almaatouq:2016:IIL**

[ASN<sup>+</sup>16]

Abdullah Almaatouq, Erez Shmueli, Mariam Nouh, Ahmad Alabdulkareem, Vivek K. Singh, Mansour Alsaleh, Abdulrahman Alarifi, Anas Alfariis, 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. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0321-5>. [AYHK18]

**Antunes:2017:DVT**

[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>.

**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 <http://link.springer.com/article/10.1007/s10207->



- 017-0361-5; <http://link.springer.com/content/pdf/10.1007/s10207-017-0361-5.pdf>.
- [BA16] **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>.
- [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>.
- [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>.
- [BB04a] **Bayly:2010:FBS**  
Duncan Bayly, Maurice Castro, Arathi Arakala, Jason Jeffers, and Kathy Ho-

- radam. 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<sup>+</sup>17]
- [BCD<sup>+</sup>13] Emmanuel Bresson, Dario Catalano, Mario Di Raimondo, Dario Fiore, and Rosario Gennaro. Off-line/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>. [BCJ<sup>+</sup>11]
- [BCEM04] 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/s10207-015-0312-y>. [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>. [Brickell:2009:SSN]
- Ernie Brickell, Liqun Chen, and Jiangtao Li. Sim-

- plified security notions of direct anonymous attestation and a concrete scheme from pairings. [BDF04] *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>.
- [BCL13] Danièle Beauquier, Joëlle Cohen, and Ruggero Lanotte. Security policies enforcement using finite and pushdown edit automata. [BDH+10] *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>.
- [BDD01] Carlo Blundo, Paolo D’Arco, and Alfredo De Santis. A  $t$ -private  $k$ -database information retrieval scheme. [BDHK08] *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>.
- [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>.
- [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>.
- [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>. [BDPV14]
- [BDHZ15] Elisa Bertino, Robert H. Deng, Xinyi Huang, and Jianying Zhou. Security and privacy of electronic health information systems. *International 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>. [Bel10]
- [BDM19] Mario Luca Bernardi, Marta Cimitile Damiano Distanti, 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>. [BEPL<sup>+</sup>17]
- [Bertoni:2014:SCS] 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>.
- [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>.
- [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<sup>+</sup>13] D. Bernhard, G. Fuchs-bauer, E. Ghadafi, N. P. Smart, and B. Warin-schi. Anonymous attestation 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 Perego. 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>.
- [BFT08] 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<sup>+</sup>13] C. Brzuska, M. Fischlin, N. P. Smart, B. Warin-schi, 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>.
- [BFT08] Andrea Bracciali, Gianluigi

- Ferrari, and Emilio Tuosto. A symbolic framework for multi-faceted security protocol analysis. *International Journal of Information Security*, 7(1):55–84, January 2008. [BGP07a] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0043-9>.
- [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>.
- [BGKZ12] **Bagheri:2012:SFP**  
Nasour Bagheri, Praveen Gauravaram, Lars R. Knudsen, and Erik Zenner. The suffix-free-prefix-free hash function construction and its indistinguishability 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/s10207-006-0007-5>.
- [BGTCCBB10] **Ben-Ghorbel-Talbi:2010:DME**  
Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia, and Adel Bouhoula. A delegation model for extended RBAC. *International Journal of Information Security*, 9(3):209–236, June 2010.
- 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 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0007-5>.

2010. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0104-3>.
- Bella:2015:SIS**
- [BJ15] 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>.
- Brown:2016:API**
- [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>.
- Bryans:2008:OGT**
- [BKMR08] 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>.
- Boyd:2005:PSI**
- 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>.

- [BM11] **Bielova:2011:DYR**  
 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>.
- [BMP05] **Bella:2005:OVS**  
 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>.
- [BMP<sup>+</sup>14] **Bates:2014:DCR**  
 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/s10207-014-0036-x>.
- [BMV05] **Basin:2005:OSM**  
 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/s10207-004-0055-7>.
- [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>.
- [BNTW12] **Bogdanov:2012:HPS**  
 Dan Bogdanov, Margus Niitsoo, Tomas Toft, and Jan Willemsen. High-performance secure multiparty computation for data mining applications. *International Journal of In-*



- formation 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>.
- Backes:2004:CPN**
- [BP04] 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>.
- Backes:2008:LBU**
- [BP08] 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>.
- Backes:2005:RSS**
- [BPW05a] Michael Backes, Birgit Pfitzmann, and Michael Waidner. Reactively secure signature schemes. *International Journal of In-*
- formation 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>.
- Backes:2005:SAS**
- [BPW05b] Michael Backes, Birgit Pfitzmann, and Michael Waidner. Symmetric authentication in a simulatable Dolev–Yao-style cryptographic 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>.
- Bernardini:2017:MRP**
- [BR17] 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>.
- Bernardini:2018:GES**
- [BR18] Riccardo Bernardini and Roberto Rinaldo. Gener-

- alized 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>.
- [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>.
- [BRS06] **Bohli:2006:KSA** 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>.
- [BS05] **Baldwin:2005:ESA** 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] **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 <http://link.springer.com/article/10.1007/s10207-010-0115-0>.
- [BT07] **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] **Bohli:2007:SGK** 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>.
- [BZV05] **Bai:2005:SAP** Yun Bai, Yan Zhang, and Vijay Varadharajan. On the sequence of authorization policy transformations. *International Journal of Information Security*, 4(1–2):120–131, February 2005. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-004-0069-1>.
- [BW08] **Biskup:2008:KSI** 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] **Baek:2003:ZSP** Joonsang Baek and Yuliang Zheng. Zheng and Seberry’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/s10207-003-0023-7>.
- [CACB16] **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>.
- [CBC08] **Corbett:2008:PCW** 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>.
- [CC10] **Chen:2010:HSS** 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] **Chen:2012:DHP** 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] **Cuppens:2008:MCS** 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/s10207-006-0011-9>.
- [CCD<sup>+</sup>07] **Cederquist:2007:ABC** 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>.
- [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>.
- [CDF<sup>+</sup>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/s10207-012-0185-2>.
- [CF03] **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>.
- [CF07] **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>.

- [CGL<sup>+</sup>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]
- [CH16] **Cremers:2016:III**  
 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>. [CHZ16]
- [CHKO12] **Camacho:2012:SAC**  
 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]
- [Chen:2018:MGE] Liqun 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:2016:SOK]
- [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>. [Chang:2019:CTM]
- [Chang:2019:CTM] 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>. [CL09]
- Crampton:2008:DRB**
- [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>. [CL13]
- Chen:2008:IID**
- [CL08] Pei-Te Chen and Chi-Sung Lai. 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>. [CLPP11]
- Cheng:2009:CKA**
- Jiin-Chiou Cheng and Chi-Sung Lai. 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>.
- 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>.
- Crampton:2011:UFC**
- 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>.
- Chang:2011:EHS**
- [CLW<sup>+</sup>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>.
- Chen:2016:MGE**
- [CM16] Liquan 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**
- [CMMPS15] Marco Casassa-Mont, Iliana 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**
- [CMN<sup>+</sup>18] 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**
- 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>.



- [CMS10] **Chakraborty:2010:CDB**  
 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>. [CTM+16]
- [CON09] **Chadwick:2009:ASX**  
 David W. Chadwick, Sassa Otenko, and Tuan Anh Nguyen. Adding support 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>. [CYA+18]
- [CPPK15] **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>. **Celdran:2016:RPP**  
 Alberto Huertas Celdrán, Ginés Dólera Tormo, Félix Gómez Mármol, Manuel Gil Pérez, and Gregorio Martínez Pérez. 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/s10207-018-0073-y>.

- com/article/10.1007/s10207-017-0396-7; <http://link.springer.com/content/pdf/10.1007/s10207-017-0396-7.pdf>.
- [CYK09] **Cook:2009:EBC**  
Debra L. Cook, Moti Yung, and Angelos D. Keromytis. Elastic block ciphers: method, security and instantiations. *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>. [Dan07]
- [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. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0078-8>. [Das12]
- [dAKdG10] **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>.
- Dawson:2004:PSI**  
E. Dawson. Preface [Daw04]

- 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]
- Dupasquier:2010:AIL**
- [DBMS10] 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>. [Den08]
- DArco:2013:TTR**
- [DdP13] 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/s10207-008-0055-0>. [Des09]
- 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/s10207-012-0186-1>. [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>. [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>.

<http://link.springer.com/article/10.1007/s10207-009-0079-0>.

**Domingo-Ferrer:2018:DGS**

[DFBJR18]

Josep Domingo-Ferrer, Alberto Blanco-Justicia, and Carla Ràfols. 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>. [DGZFGH13]

**Degabriele:2016:UPC**

[DFF<sup>+</sup>16]

Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra 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>. [DHS04]

**Duessel:2017:DZD**

[DGF<sup>+</sup>17]

Patrick Duessel, Chris-

tian 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): 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**

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>.

**Daza:2004:PUI**

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>.
- [DHW11] **DiPierro:2011:PTC**  
 Alessandra Di Pierro, Chris Hankin, and Herbert 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>. [DM07]
- [DJN10] **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>. [DMDD16]
- [DLR15] **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/s10207-014-0239-8>. [DeFrancesco:2007:ILS]
- [DMP13] **DeFrancesco:2007:ILS**  
 Nicoletta De Francesco and Luca Martini. Instruction-level security typing by abstract interpretation. *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>. [DeKeulenaer:2016:LTS]
- [DMP13] **DeKeulenaer:2016:LTS**  
 Ronald De Keulenaer, Jonas Maebe, Koen De Bosschere, and Bjorn De Sutter. 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>. [DeCristofaro:2013:PDC]
- [DMP13] **DeCristofaro:2013:PDC**  
 Emiliano De Cristofaro, Mark Manulis, and Bertram Poettering. Private discov-

- ery of common social contacts. *International Journal of Information Security*, 12(1):49–65, February 2013. CODEN ????? ISSN [DRPW12] 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0183-4>.
- [DMRS07] **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 [DS07] <http://link.springer.com/article/10.1007/s10207-007-0012-3>.
- [DNF+19] **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 [DSB19] 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>.
- Delicata:2007:AAV**  
 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>.
- Das:2019:DSI**  
 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):23–48, February 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-019-0013-2>.

- urity*, 18(1):1–22, February 2019. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0393-x>.
- [dSFK19] **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>. [DTK<sup>+</sup>18]
- [DSRHC16] **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>. [DV08]
- [DSY06] **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**  
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**  
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>.

- [DVB02] **Dawson:2002:CCP**  
 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>. [EAH<sup>+</sup>07]
- [DYDW10] **Ding:2010:NHA**  
 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>. [EEB<sup>+</sup>15]
- [DZW<sup>+</sup>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>. [EFH09]
- 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>.
- ElHassani:2015:ION**  
 Abdeljebar Ameziane El Hassani, Anas Abou El Kalam, Adel Bouhoula, Ryma Abassi, and Abdellah 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. *In-*



- ternational Journal of Information Security*, 8(5): 331–345, October 2009. [EHSS14]  
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0078-1>.
- [EG18] **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. [ETAHCR08]  
CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0244-y>.
- 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>.
- Esfahani:2017:EHM**  
Alireza Esfahani, Georgios Mantas, Jonathan Rodriguez, and José Carlos Neves. An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks. *International Journal of Information Security*, 16(6): 627–639, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0351-z>.
- Estevez-Tapiador:2008:BRE**  
Juan M. Estevez-Tapiador, Almudena Alcaide, Julio C. Hernandez-Castro, and Arturo Ribagorda. Bayesian rational exchange. *In-*

- 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>. [FHV18]
- [EWR<sup>+</sup>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>. [Fon08]
- [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>. [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>. [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>. [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>.

- [FSG<sup>+</sup>14] **Fernandes:2014:SIC**  
 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>. [GCH<sup>+</sup>19]
- [GBDJ14] **Granadillo:2014:RBC**  
 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 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0207-8>. [GCSÁBdSS12]
- [GBG18] **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 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0154-9>.

- [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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0234-0>.
- [GKBS12] **Gritzalis:2012:FAR**  
 Dimitris Gritzalis, Panagiotis Katsaros, Stylianos Basagiannis, and Yannis Soupionis. 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>.
- [GH05] **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>.
- [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>.
- [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/s10207-019-0052-x>.
- [GKS19] **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>.
- [GLMS+04] **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>.
- [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] **Gouglidis:2014:SPV**  
Antonios Gouglidis, 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>.
- [GMMV05] **Galindo:2005:FOH**  
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>.
- [GMMZ06] **Giorgini:2006:RET**  
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/s10207-006-0021-9>.

- com/article/10.1007/s10207-006-0005-7.
- [GMO01] 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/s10207-013-0225-6](http://link.springer.com/article/10.1007/s102070100004).
- [GOBdlC11] 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/s10207-011-0140-7](http://link.springer.com/article/10.1007/s102070100004).
- [GMS03] 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>.
- [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/s10207-007-0052-8>.
- [Gol08] Dieter Gollmann. Editorial. *International Journal of Information Security*, 7(2):101, April 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0052-8>.
- [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/s10207-011-0140-7>.
- [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>.
- [Gollmann:2008:E] Dieter Gollmann. Editorial. *International Journal of Information Security*, 7(2):101, April 2008. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0052-8>.
- [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/s10207-011-0140-7>.

- <http://link.springer.com/article/10.1007/s10207-012-0167-4>.
- [GP17] **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>.
- [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 Gürgens, Carsten Rudolph, and Holger Vogt. On the security of fair non-repudiation protocols. *International Journal of Information 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<sup>+</sup>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>.
- [GSP<sup>+</sup>16] **Gritti:2016:BED**  
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>.
- [GSS10] **Goldschlag:2010:THB**  
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>.
- [GTM11] **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>.
- [GW09] **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>.



- [GYL<sup>+</sup>07] **Gritzalis:2007:PMO**  
 S. Gritzalis, A. N. Yannacopoulos, C. Lambri-  
 nouidakis, 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 [HCN15]  
 1615-5262 (print), 1615-  
 5270 (electronic). URL  
[http://link.springer.  
 com/article/10.1007/s10207-006-0010-x](http://link.springer.com/article/10.1007/s10207-006-0010-x).
- [HBH12] **Hadziosmanovic:2012:LMA**  
 Dina Hadziosmanović, Damiano Bolzoni, and Pieter H.  
 Hartel. A log mining approach for process moni-  
 toring in SCADA. *International Journal of In-  
 formation Security*, 11(4):  
 231–251, August 2012.  
 CODEN ???? ISSN [HH16]  
 1615-5262 (print), 1615-  
 5270 (electronic). URL  
[http://link.springer.  
 com/article/10.1007/s10207-012-0163-8](http://link.springer.com/article/10.1007/s10207-012-0163-8); [http://  
 link.springer.com/content/  
 pdf/10.1007/s10207-012-0163-8.pdf](http://link.springer.com/content/pdf/10.1007/s10207-012-0163-8.pdf).
- [HC10] **Han:2010:CBI**  
 Shui-Hua Han and Chao-  
 Hsien Chu. Content-  
 based image authentica-  
 tion: current status, is-  
 sues, and challenges. *International Journal of In-  
 formation Security*, 9(1):  
 19–32, February 2010.  
 CODEN ???? ISSN  
 1615-5262 (print), 1615-  
 5270 (electronic). URL  
[http://link.springer.  
 com/article/10.1007/s10207-009-0093-2](http://link.springer.com/article/10.1007/s10207-009-0093-2).
- Hoang:2015:GAM**  
 Thang Hoang, Deokjai  
 Choi, and Thuc Nguyen. Gait authentication on mo-  
 bile phone using biometric cryptosystem and fuzzy  
 commitment scheme. *International Journal of In-  
 formation Security*, 14(6):  
 549–560, November 2015.  
 CODEN ???? ISSN  
 1615-5262 (print), 1615-  
 5270 (electronic). URL  
[http://link.springer.  
 com/article/10.1007/s10207-015-0273-1](http://link.springer.com/article/10.1007/s10207-015-0273-1).
- 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](http://link.springer.com/article/10.1007/s10207-015-0302-0).

- [HIDFGHR19] **Hinarejos:2019:DPE**  
 M. Francisca Hinarejos, Andreu-Pere Isern-Deyà, Josep-Lluís Ferrer-Gomila, and Llorenç Huguët-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>. [HK19]
- [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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0087-0>. [HL04]
- [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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0277-x>.
- 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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0414-4>.
- 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>.

- [HLKI15] **Han:2015:MAU**  
 Kyoung Soo Han, Jae Hyun Lim, Boojoong Kang, and Eul Gyu Im. Malware analysis using visualized images and entropy graphs. *International Journal of Information Security*, 14(1):1–14, February 2015. [HN14]  
 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. [HRL09]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0383-z>.
- [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. [HS09]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0072-z>.
- 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. [HS09]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0237-x>.
- Harn:2009:EIB**  
 Lein Harn, Jian Ren, and Changlu Lin. Efficient identity-based GQ multisignatures. *International Journal of Information Security*, 8(3):205–210, June 2009. [HS09]  
 CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-009-0072-z>.
- Hammer:2009:FSC**  
 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>. [HSMY12]
- [HS15] 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>. [HTM11]
- [HSMW08] 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/article/10.1007/s10207-007-0021-2>. [Hub12]
- 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>.
- Hanley:2011:UTD**  
Neil Hanley, Michael Tunstall, and William P. Marwane. 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>.
- 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>.
- [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>.
- [HZZL+17] **Huang:2017:MAP**  
 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>.
- [IDHRPCMP15] **Isern-Deya:2015:PUG**  
 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 Information 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>.
- [IHNT02] **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>.
- [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>. [JCL<sup>+</sup>18]
- [IT05] **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>. [JG15]
- [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>. **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>. **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/s10207-014-0249-6>.

- [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>. [JSMG18a]
- [JM17] **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>. [JSMG18b]
- [JMV01] **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/s10207-017-0376-y>. [JTV19]
- Jiang:2018:CPA**  
 Yin hao 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>.
- Jiang:2018:FCP**  
 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>.
- 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>. [KAC16]
- [JZ11] 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>. [KAC17]
- [KA18] 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>. [KB13]
- 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>.
- 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>.
- 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 [KCM<sup>+</sup>15]  
<http://link.springer.com/article/10.1007/s10207-013-0198-5>.

**Knight:2007:IJI**

[KBH07]

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 [KG11]  
<http://link.springer.com/article/10.1007/s10207-007-0036-8>.

**Kotzanikolaou:2017:BAR**

[KCB17]

Panayiotis Kotzanikolaou, George Chatzisofofroniou, 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 [KGG09]  
<http://link.springer.com/article/10.1007/s10207-016-0318-0>.

**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>.

**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>.

**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] **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. [KK17] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0226-0>.
- [KJG<sup>+</sup>11] **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. *International Journal of Information Security*, 10(5): 269–283, October 2011. [KKK17] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0132-7>.
- [KJS17] **Kim:2017:MES**  
Minchul Kim, Younghoon 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>.
- Kananizadeh:2017:DDP**  
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>.
- Kolias:2017:TDS**  
Constantinos Kolias, Vasilis Kolias, 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>.

- [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>. [KM07]
- [KLMM09] **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>. [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>. [KME<sup>+</sup>16]
- 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>. [Knudsen:2010:CEA]
- 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>.
- 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>.
- [KML03] **Korzhik:2003:HAB** [KNL16] 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>.
- [KMR09] **Kuper:2009:GXS** Gabriel Kuper, Fabio Masci, and Nataliya Rasadko. 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>.
- [KN07] **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>.
- Kim:2002:NEC**
- [KO02] S. Kim and H. Oh. A new electronic check system with reusable refunds. *International Journal of Information Security*, 1(3):175–188, November 2002. 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 Ustaoglu. A practical privacy-preserving targeted advertising scheme for IPTV users. *International Journal of Information Security*, 15(4): 335–360, August 2016. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0296-7>. [KSZ07]
- [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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-012-0173-6>. [KU16]
- [KSM10] **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/s10207-015-0308-7>. [Kud02]
- Konstantinou:2007:EGS**  
Elisavet Konstantinou, Yannis C. Stamatiou, and Christos Zaroliagis. Efficient generation of secure elliptic curves. *International 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>.
- 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>.
- Kudo:2002:PPB**  
Michiharu Kudo. PBAC: Provision-based access control model. *International Journal of Infor-*

- mation Security*, 1(2): 116–130, February 2002. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s102070100010>.  
**Kusters:2005:DCP**
- [Küs05] Ralf Küsters. On the decidability of cryptographic protocols with open-ended 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>.  
**Kamm:2015:SFP**
- [KW15] Liina Kamm and Jan Willemson. 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>.  
**Kluczniak:2019:MDA**
- [KWCK19] 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://link.springer.com/content/pdf/10.1007/s10207-018-0406-4.pdf>.  
**Kuo:2018:DRA**
- 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>.  
**Landwehr:2001:CS**
- 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**  
 Jay Ligatti, Lujo 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>. [LCL14]
- [LBZ+10] **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>. [LCL16]
- [LC04] **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]
- 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]
- Liu:2016:STP**  
 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>. [Li:2014:AAM]
- Li:2014:AAM**  
 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>.
- 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**
- [LD07] 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**
- [LD17] Lichun Li and Anwitaman Datta. Write-only oblivious RAM-based privacy-preserved access of out-
- sourced 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>.
- Levin:2007:WSL**
- 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>.
- Li:2015:TMM**
- 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>.
- Liu:2007:ICR**
- Jinshan Liu and Valérie Is-
- [Lev07]
- [LH15]
- [LI07]



- sarny. 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>. [LL14]
- [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>. [LLBL18]
- [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>. [Lee:2009:RTB]
- [LLW<sup>+</sup>16] 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]
- 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>. [Lanet:2018:WTM]
- 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>. [Liu:2016:PCC]
- Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, and Yan Li. Practical chosen-ciphertext secure Hierarchical Identity-Based Broadcast Encryption. *International Journal of Information Security*, 15(1):35–50, February 2016. CODEN ???? ISSN 1615-5262 (print), 1615-

- 5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0287-8>.  
Li:2009:DSA
- [LLWY09] Jiangtao Li, Ninghui Li, Xiaofeng Wang, and Ting Yu. Denial of service attacks and defenses in decentralized trust management. *International Journal of Information Security*, 8(2):89–101, April 2009. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-008-0068-8>.  
Li:2006:USS
- [LM06] Ninghui Li and John C. Mitchell. Understanding SPKI/SDSI using first-order logic. *International Journal of Information Security*, 5(1):48–64, January 2006. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-005-0073-0>.  
Li:2017:RRS
- [LMD17] Lichun Li, Michael Mitzner, and Anwitaman Datta. rPIR: ramp secret sharing-based communication-efficient private information retrieval. *International Journal of Information Security*, 16(6):603–625, November 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0347-8>.  
Lai:2017:EIB
- [LMG17] Jianchang Lai, Yi Mu, and Fuchun Guo. Efficient identity-based online/offline encryption and sign-cryption with short ciphertext. *International Journal of Information Security*, 16(3):299–311, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-016-0320-6>.  
Lopez:2004:PDB
- [LMMO04] 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>.  
Lioy:2006:PPP
- [LMMP06] 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>.
- [LMMS17] 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>.
- [Lop18] 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>.
- [LP11] 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>.
- [LRB<sup>+</sup>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>.
- [LSWW14] 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/s10207-014-0010-0>.

- com/article/10.1007/s10207-014-0231-3.
- [Lu09] 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] 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] Aron Laszka, Yevgeniy Vorobeychik, and Xenophon Koutsoukos. A game-theoretic approach for integrity assurance in resource-bounded systems. *International Journal of Information Security*, 17(2):221–242, April 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0299-4>.
- [LZQ<sup>+</sup>18] 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/s10207-017-0364-2>.
- [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>.
- [MBHT17] 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 [McH01] <http://link.springer.com/article/10.1007/s10207-015-0311-z>; <http://link.springer.com/content/pdf/10.1007/s10207-015-0311-z.pdf>.
- [MBRPS18] Antoni Martínez-Ballesté, Hatem Rashwan, Domenec 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>.
- [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>.
- [McH01] John McHugh. Intrusion and intrusion detection. *International Journal 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>.
- [MdSC<sup>+</sup>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/s10207-014-0253-x>.
- [MFES04] 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):

**McHugh:2001:IID**

**Martina:2015:ATM**

**Marconi:2011:CPE**

**Munoz:2004:CRS**

**Martinez-Balleste:2018:DIS**

- 110–124, January 2004. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-003-0026-4>. [ML17]
- [MGV17] **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>. [MLCS16]
- [ML14] **Mousazadeh:2014:RGA**  
 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>. [MLM19]
- 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>.
- Miao:2016:MDU**  
 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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-015-0297-6>.
- Mesbah:2019:REJ**  
 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.

- CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0401-9>.
- [MLO<sup>+</sup>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>.
- [MMS16] 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>.
- [MP15] Jean Everson Martina and Lawrence Charles Paulson. Verifying multicast-based security protocols using the inductive method. *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>.
- [MP16] 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>.
- [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>.

**Mana:2004:FSE**

**Mennink:2016:EPH**

**Mateu:2016:HAV**

**Mavrogiannopoulos:2014:TSK**

**Martina:2015:VMB**

- [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>.
- [MPS14] **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>.
- [MR03] **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>.
- [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>.
- [MS15] **Mustafa:2015:UIA**  
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>.
- [MSGCDPSS18] **Morales-Sandoval:2018:PBC**  
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>.
- [MSKD16] **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.
- [MSN02] **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] **Marmol:2013:PEA**  
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] **Mehrnezhad:2018:SPM**  
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>.
- [MWZ06] **Mayer:2006:OFA**  
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>.
- [MYLZ14] **Mu:2014:RBD**  
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>.
- [NA14] **Nunez:2014:BPP**  
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>.
- [NAM06] **Nali:2006:HTB**  
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>.
- [NMBB12] **Niebuhr:2012:SPS**  
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>.
- [NP10] **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>.
- [NRC15] 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>.
- [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>.
- [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>.
- [NVB<sup>+</sup>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>.
- [OssK16] Cengiz Orencik, Ayse Selcuk, Erkey Savas, and Mu-
- Nappa:2015:MDI**
- Nuida:2012:SCS**
- Nieto:2002:KRC**
- Orencik:2016:MKS**
- Narasimha:2009:PPR**

- rat 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>. [Pen11]
- [OT06] 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>. [Pen12]
- [PDB11] 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/s10207-011-0151-4>. [Pen13]
- [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/s10207-010-0117-y>. [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>. [Peng:2013:SAH] 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>.

**Pereniguez-Garcia:2013:KPA**

- [PGMLK<sup>+</sup>13] F. Pereñiguez-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>.

**Pais:2010:NPR**

- [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. [PPL15] CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0108-z>.

**Plaga:2009:BKS**

- [Pla09] Rainer Plaga. Biometric keys: suitable use cases and achievable information content. *International Journal of In-*

*formation 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>.

**Perez-Mendez:2012:CLS**

- [PMPGMLLM12] Alejandro Pérez-Méndez, Fernando Pereñiguez-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>.

**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/s10207-015-0090-5>.

- com/article/10.1007/s10207-014-0255-8.
- [PPSS13] **Phan:2013:ACB**  
 Duong-Hieu Phan, David Pointcheval, Siamak F. Shahandashti, and Mario Strefler. 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>. [QDW09]
- [Pri04] **Priami:2004:PSI**  
 Corrado Priami. Preface to the special issue on Security in Global Computing. *International Journal 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>. [QDW+15]
- [PS17] **Poettering:2017:DAP**  
 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>. [Qin:2009:SSS]
- [Qin:2009:SSS]  
 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>.
- [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>.

- [QLOW09] **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>. [RBD02]
- [QLZH15] **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. *International 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>. [RBEH15]
- [RAC16] **Raad:2016:PSR**  
 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>. [Rodeh:2002:UAT]
- [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>. [Riecker:2015:LEC]
- [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>. [Rao:2016:EAB]
- [RD16] Y. Sreenivasa Rao and Ratna Dutta. Efficient attribute-based sig-



- nature 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/s10207-015-0289-6>. [RGL16]
- [RDK18] 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] 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]
- [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. 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>.
- [RLEM18] **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>.
- [RM12] **Reaves:2012:OVT**  
 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>.
- [RMPADF13] **Rebollo-Monedero:2013:MPA**  
 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/s10207-012-0182-5>.
- [RMSCR19] **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>.
- [Roe11a] **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].

- [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].
- [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>.
- [RSPMB16] **Rashwan:2016:UTP**  
 Hatem A. Rashwan, Agusti Solanas, Domènec Puig, and Antoni Martínez-Ballesté. Understanding trust in privacy-aware video surveillance systems. *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/s10207-003-0028-2>.
- [Rus04] **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>.
- [SAL17] **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>.
- [SAL17] **Shaikh:2017:DCM**  
 Riaz Ahmed Shaikh, Kamel 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>.
- [SAT09] **Sourour:2009:ESD** Mehharouech Sourour, Bouhoula Adel, and Abbes Tarek. [SBB19] 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>.
- [SB09] **Shay:2009:CST** Richard Shay and Elisa Bertino. [SCL<sup>+</sup>18] 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>.
- [SCL<sup>+</sup>18] **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>.
- [SdHZ16] **Scaife:2018:OSR** Nolen Scaife, Henry Carter, Lyriisa 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>.
- [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 [SF17] 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] 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. [SGE02] CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0238-9>.
- [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. [SGJ19] CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0367-z>.
- [Singh:2017:RUA] 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>.
- [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>. [SJ10]
- [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 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-017-0365-1>. [SK06]
- [SJ09] 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>. [SK14]
- [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/s10207-010-0112-3>.
- [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>.
- [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>. [L05]

**Salini:2016:EPA**

[SK16]

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>. [SM10]

**Sisaat:2017:STM**

[SKK+17]

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>. [Smi04]

**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>.

**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/s10207-004-0068-2>.

- com/article/10.1007/s10207-004-0033-0.
- [SMMN12] **Sole:2012:EMT**  
 Marc Solé, Victor Muntés-Mulero, and Jordi Nin. Efficient microaggregation techniques for large numerical data volumes. *International Journal of Information 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] **Snekkenes:2005:PSI**  
 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] **Stasinopoulos:2019:CAE**  
 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/s10207-013-0199-4>.
- [SPDR17] **Stevanovic:2017:MIC**  
 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] **Schreuders:2013:FBA**  
 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>.
- [SS05a] **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>.
- [SS05b] 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>.
- [SS17] 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/s10207-016-0341-1>.
- [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/s10207-013-0222-9>.
- [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>.
- [SSF15] Younes Seifi, Suriadi Suriadi, Ernest Foo, and Colin Boyd. Analysis of two authorization protocols using Colored Petri Nets. *International Journal of Information Security*, 14(3):221–247, June 2015. CODEN ????? ISSN 1615-5262 (print), 1615-5270 (electronic). URL

**Skalka:2005:SUB**

**Spreitzenbarth:2015:MSC**

**Sampangi:2017:HSR**

**Seifi:2015:ATA**

**Shameli-Sendi:2014:ACA**

- <http://link.springer.com/article/10.1007/s10207-014-0243-z>.
- [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 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0246-9>.
- [SSP14] Reza Sepahi, Ron Steinfeld, and Josef Pieprzyk. Lattice-based certificateless 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>.
- [SSVC16] Petr Susil, Pouyan Sepehrdad, Serge Vaudenay, and Nicolas Courtois. On selection of samples in algebraic attacks and a new technique to find hid-
- den 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] 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>.
- [TG05] 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>.
- [TGS17] Marco Tiloca, Christian

- Gehrmann, 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/s10207-016-0326-0>. [TND+15]
- [TLX09] 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>. [TTS+06]
- [TMP13] 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>. [Tonicelli:2015:ITS]
- Rafael Tonicelli, Anderson C. A. Nascimento, Rafael Dowsley, Jörn Müller-Quade, Hideki Imai, Goichiro Hanaoka, and Akira Otsubuka. 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>. [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>. [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>. [Vaj16]
- Teller:2004:UAC**
- [TZH04] 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>. [VdWZ14]
- Ustaoglu:2011:IIB**
- [Ust11] Berkant Ustaoglu. Integrating identity-based and certificate-based authenticated key exchange protocols. *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/s10207-011-0136-3>. [VH19]
- 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>.
- 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. *International Journal of Information Security*, 13(6):529–569, November 2014. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-014-0235-z>.
- 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>.
- [VHT09] 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>.
- [VL13] 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>.
- [VOLW05] 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>.
- [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>.
- [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>.
- [VSM06] Gabriel Vanrenen, Sean

**Vasserman:2009:IKN**

**Vrakas:2013:IDP**

**vonOheimb:2005:ASM**

**vanOorschot:2006:MSD**

**Vasiliadis:2015:GAM**

**Vanrenen:2006:DSM**

- Smith, and John Marchesini. Distributing security-mediated PKI. *International Journal of Information 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>. [Wai04]
- [VSR15] 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>. [WGMB13]
- [WAB<sup>+</sup>09] 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>. [WHS18]
- 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>.
- 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>.
- [WLLW14] Tzong-Sun Wu, Ming-Lun Lee, Han-Yu Lin, and Chao-Yuan Wang. [WPD18] 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>.
- [wLW05] Kong wei Lye and Jeanette M. Wing. Game strategies in network security. *International Journal of Information Security*, [WR08] 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>.
- [WMS<sup>+</sup>19] 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>.
- [Wang:2018:VEC] 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:2008:MLF] 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. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-007-0042-x>.
- [Wu:2014:SSP] [Wu:2019:TPP]

- [WR15] **Wei:2015:TPE**  
 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>. [WYL<sup>+</sup>12]
- [WT16] **Wang:2016:SSE**  
 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>. [WZ07]
- [WW07] **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/s10207-006-0008-4>. [XCW<sup>+</sup>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. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-011-0148-z>.
- 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. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0008-4>.
- Xin:2012:RAA**  
 Zhi Xin, Huiyu Chen, Xinche 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>. [YLL+18]
- [XSA13] 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>. [Yon18]
- [YAM+15] 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/s10207-016-0352-y>. [You06]
- [Yang:2018:NSS] 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>. [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>. [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] 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/s10207-008-0060-3>.
- [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. [YSM10] CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-006-0086-3>.
- [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>.
- [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 Information Security*, 13(5):453–465, October 2014. CODEN ????. ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-013-0224-7>.
- [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 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-010-0086-3>.

- com/article/10.1007/s10207-010-0110-5.
- [YSM16] **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>. [ZGC07]
- [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>. [ZGK07]
- [ZBD06] **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>. [Zhang:2007:FBT]
- 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>. [Zulkernine:2007:ISS]
- 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>.

- [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 <http://link.springer.com/article/10.1007/s10207-006-0087-2>.
- [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>.
- [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>.
- [ZO13] **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>.
- [ZRJ14] **Zhang:2014:DFA**  
 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>.
- [ZVH15] **Zhou:2015:GCR**  
 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>.
- [ZWQ<sup>+</sup>17] **Zhang:2017:CIB**  
 Lei Zhang, Qianhong Wu, Bo Qin, Hua Deng, Jiangtao 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>. [ZZH08]
- [ZXZ<sup>+</sup>11] **Zhu:2011:SLA**  
 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/s10207-011-0127-4>. [ZZW<sup>+</sup>10]
- [ZZG19] **Zheng:2019:IDR**  
 Jian-Wu Zheng, Jing Zhao, and Xin-Ping Guan. Identifier discrimination: realizing selective-ID HIBE with authorized delegation and dedicated encryption privacy. *International Journal of Information Security*, 18(2):141–162, April 2019. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL <http://link.springer.com/article/10.1007/s10207-018-0402-8>. **Zhao:2008:NAP**  
 Chang-An Zhao, Fangguo Zhang, and Jiwu Huang. A note on the Ate pairing. *International Journal of Information 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**  
 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/s10207-010-0054-1>.

com/article/10.1007/s10207-  
009-0091-4.