Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N)
[Bai10, YC11], (n, t, n) [LHYZ12], (t, n)
[QD16, ZPYW12], 0 [XHX+17], 1
[XHX+17], 1, 2, 3 [SMDS11]. $100$ [Sch16a],
11 [LJ17], 13 [Blo15]. 2
[AM19, DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGL10, WK18, WY12]. 22
[MNP12], 2k [Sun16]. 3
[AP10, Bro19, CG12b, DWWZ12, FWS13,
GZH12, GH11a, KWS+12, LJ17, LJ15,
MKH+12, RS16, SS16a, SS12a, SGS14,
WSSO12, tWmC12, YT11a, YI14, YPRI17],
32 × 32 [SA14], 3 × 3 [AMVZ12]. 4
[COP+14, DWWZ12, HLYS14]. $49.00$
[Sch15a]. 5 [YN19]. 8 [LPO+17, ZSH+19].

$S9$ [APPVP15]. = [JJUW10], + [PYH+18], 2
[YNX+16]. 3 [LHM14]. M$^T$ [HRB13]. α
[TTL10]. c [KRDH13]. d [QD16], d × d
[KA17]. ℓ [ZTL15]. $F_p + \nu F_p$ [WGF16]. γ
[DWZ12]. GF(2)[x] [SF12]. GF(2m)
[HJ19, SKH15]. GF(2m) [LBOX12]. K
[FXP12, FR16, CHX13, SG19a, XMY+17,
XLP+18, ZZC17, ZHT16]. L(1/4 + o(1))
[JJ13]. M [MMSD13, OS11]. Fq,p
g30
[AMORH13]. Fq [SS13]. N/P [HN10].
GF(2^4)2 [GM16b]. GF(2^8) [GM16b]. GF(q)
[LPO10]. LWE [BV14]. μ [Jia14a]. N
[FR16]. n × k(k ≥ n/2) [MC11]. O(d13d)
[KA17]. O(n^2) [KS11]. P [DG17, GT19]. π
EHKSS19]. ±1 [HZW+14]. q
[CZCD18, GMS11]. S [LJ15]. t
[HJM+11, Oba11]. w [Kre13].
-Encoded [DG17]. -Encoding [XHX+17].
-Spotty [OS11]. -trimmed [TTL10]. .onion [Boy16].
0.13um [KLM+12].
1 [AAE+14, Ano15b, BH15, Bar16a, CGCS12, Con17, Ful10, MSas12, SKP15].
1-58848-551-3 [Ful10]. '10 [Ano10a]. 1024 [Bro17, Win17]. 10Gbps [PRGBSAC19].
[HIDFGPC15].
3 [ABM+12, BD15, jCPB+12, Ful10, LC17, Mor19a, NIS15]. 30th [Rab10]. 31st [PJ12].
[BBTC20]. 5th [BYL10, vDKS11]. 6 [Ano17b, Bai12, Mur10]. 64/128 [LJ18].
8.8/11.2 [GLIC10]. 800 [MMKP16]. 800-160 [MMKP16]. 802.11 [FLH13, ZBR11]. 802.11s [BOB13]. 802.15.4 [NBZP17]. 802.16e [CL11]. 802.16m [FZZ+12]. 85 [WZM12a]. 85th
[RNQ16]. 959 [ÁCZ16]. 978 [Ano15b, Ano17b, Bai12, Mur10]. 978-0-691-14175-6 [Ano17b].
978-3-540-49243-6 [Mur10]. 9798 [BCM12, BCM13]. 9th [Cra12, GLIC10, HWG10].
AAA [BT18, MLM16]. AAA-based [MLM16]. AAO-T [FQZF18]. Abandon [Loo15]. ABE
[FIJJH12, HQZH14, HLC+19, OSNZ19, QZZ18, TY16a, YMC+17, ZSW+18b].
abelian [CDLSY14, HWS+19, LR15, Shch19b]. ability [WS12]. abnormal [AKM+15]. ABO
[ZYY19]. ABO-LTFs [ZYY19]. Abort
Advert [MT17]. Advertisement [Ano16j, AMHJ10]. Advertises [AHS13].
AEP [LZD+19]. AEP-PPA [LZD+19].
AES [ARG19, ABO+17, BW16, BBP13, BKR11, BB10, DGP10, FAA+18, FLYL16a, FLYL16b, GLMS18, GM16b, HMKG19, HF14b, LB13, Mar10c, MM14b, PBCC14, RTMA18, SY15a, VGA19, WJ19, YWF18].
AES-Like [BW16, WJ19].
AET [HTC+15].
Aliation [XLM+12, XGLM14, XZLW15].
Aliation-Hiding [XLM+12, XGLM14, XZLW15].
Ane [BCEM15, LYL+18, GZHD12].
Ane-transformation-invariant [GZHD12].
Africacrypt [BL10].
After [Sch18].
Against [Ano17e, BVS+13, BCHC19, BL15, BL16, CW12b, CMA14, DZS+18, DL17, FDY+19, GDDL18, GDC16, HET19, HLC+19, KMZS19, MSS+18, MWES19, Sch13, SGR15, SLY+16, WSA15, AATM18, ASBdS16, AYSZ14, BBP13, BD18, BVIB12, BPR14a, DB14b, BFK16, BSR+14, BK12b, BH19, Bu16, BCCK15, CKHP19, Che15, CG14a, CGCS12, CBJY16, CGH17, DHL10, DK17, Dya19, EWS14, FTV+10, zGXW12, GSC17, HLL18, HYL19, JSM18a, JHJ12, LDC13, LHM+10, LGY+12, LLY+12a, LWC14, MCI+19, Ma16, MBP19, MD12b, MN12, NDR13, OF11, OSNZ19, QWR+18, SBM15, SEY14, SY15b, SD12, TLL13, WHN+12, Yn12, ZLQ15, ZHS+19, vV16].
Age [Bla12, SR14, Lan17, Sto12].
Aged [Re15].
agency [Ald11, Kum10, ABJ13].
agent [GPVCdBRO12].
Aggregate [CCT+14, PSM17, WCD19, GLB+18, LLY15, LLL+18, ZQWZ10, ZDHZ18, CLW16].
Aggregated [NLY15]. Aggregated-Proof [NLY15].
Aggregating [DP12].
Aggregation [ARWK19, BJL16, EKOS19, LHKR10, SP15b, YM18, ZHW+16, DXWD16, DZC16, GLM+19, RR17, WMY16].
Aging [SKV12].
Agnostic [HFW+19].
Agriculture [APK+18].
Aided [BGK12, BCGK12, BGB12, Gop19, GMS14, LNWZ19, MV19, Vua10, ABBD13, LLY15, SGJ+18, SAA11, WLF17].
AIPSteg [AGL16].
Air [AUMT16, KTM+18, VOG18, ZW+18].
Aircraft [XWZW16].
Airflow [RSCX18].
Airway [RSCX18].
AK [XHC+12].
AK-PPM [XHC+12].
AKA [LLS+13].
AKF [KD15].
al [LL18, LLS16, MWZ12, PLW13, SB+12, Mac14, Neb15].
al-Qaeda [Mac14, Neb15].
al [ABJ13, SBLH14].
Alan [CS12, Don14, Hel17b, LCKBJ12].
Algebra [PWB17, Xie12a, Xic12b, BS15, Bul10b, CFR11, DWZ12, GFPG14, Nam19].
Algebraic [ACA+16, HHJ+19, LHC+19, LKY19, SK11, Tam15, Wat10, WCXZ17, Bul10a, CFR11, FMB+18, SA14, YTM+14].
Algorithm [AA19, ABC17, Ano11b, AK14b, BGTJ14, BKL18, CNR14, CS10, jCPB+12, DCM18, ESS12, GKB17, HZS105, JLH12, JS12, JHJ12, JL16, KB10, LL11, LT14a, LLL17a, LLL18, LYYL+18, MSL+17, MRL+18, NdMM16, NV10, RR11, RVR12, WHZ12, WZCC18, YPRI17, YH16, ZSW+12, ZWW17, AIA+18b, Ang16].
Aging [SKV12].
Agnes [Bur11, Joh15].
Agnostic [HFW+19].
Agreement [ADSH18, BSBB19, CH16, HCL+14, HEC+12, KMZS19, MNS11, TM12, WSS12, XLM+12, XGLM14, XZLW15, YLSZ19, AAL19, AQRH+18, APK+18, AN15, BGD12, CSD18, CTL13, DLK+16, EBAQ17, GH16, HPC12, HWB10, HWB12, ISC+16, IB11, IOV+18, SSI11, KIH19, KP18, KIW+16, KD+17, LLSL13, LYY06, LIK+17, MHL18, NCL13, Nos11, Nos14, OK+17, OSAN19, PY19, hSZ15, TLL12, WXY+17, XCL13, XXYC19, XMHD13, XHM14, YZ+14, YY13, ZWQ+11, ZT16, ZGL+18a, ZZC15, OHJ10].
Agriculture [APK+18].
Aided [BGK12, BCGK12, BGB12, Gop19, GMS14, LNWZ19, MV19, Vua10, ABBD13, LLY15, SGJ+18, SAA11, WLF17].
Algebra [PWB17, Xie12a, Xic12b, BS15, Bul10b, CFR11, DWZ12, GFPG14, Nam19].
Algebraic [ACA+16, HHJ+19, LHC+19, LKY19, SK11, Tam15, Wat10, WCXZ17, Bul10a, CFR11, FMB+18, SA14, YTM+14].
Algorithm [AA19, ABC17, Ano11b, AK14b, BGTJ14, BKL18, CNR14, CS10, jCPB+12, DCM18, ESS12, GKB17, HZS105, JLH12, JS12, JHJ12, JL16, KB10, LL11, LT14a, LLL17a, LLL18, LYY+18, MSL+17, MRL+18, NdMM16, NV10, RR11, RVR12, WHZ12, WZCC18, YPRI17, YH16, ZSW+12, ZWW17, AIA+18b, Ang16].
[BDK11, TG12]. anonymizing [TMK11].

**Anonymous** [APMCR13, CG12a, CZLC12a, CCF17, Chi12, DK12, FH10b, FHZW18, HLT+15, KP18, LIK+17, LQX19, LZCK14, Muf16, Per13, RSN14, SYWX19, TAKS10, Ver17, Wan14, WX+17, WYML16, ZJ14, ZMW16, AKIC18, A KS19, ATK11, BT18, CCSV11, Chi13a, CG11, FS GW12, Gop19, GTSS19, HL14, ISC+16, KCS+18, LNK+18b, LZD+19, LWK+19, LM14, LSQ15, LY15, LY14, MYYR13, MML16, QMC17, VS11, WLS14, XXXY19, YZL+18, YYK+19].

ANSI [Ano11b].

answer [Pec12].

answers [Wu16].

Anti [Alz19, KKK+18b, QZ14].

Anti-Counterfeiting [Alz19].

anti-forensics [QZ14].

Anti-reversible [KKK+18b].

Antinoise [WXL+17].

Antispoo ﬀ ng [MR14b].

Antoine [AY12a, AY12b].

Any [BHT18, Goo12, LP11].

Anything [Nor17].

AODV [SS15].

Apache [Lit14].

APBT [ZWWW17].

API [FLW12, PTR18, QF19].

Append [YNR12b].

Append-Only [YNR12b].

Applicability [Scr18].

Application [AKP12, AK14b, BD15, BRT12, BS12, CCL+19, CKL13, CCKM16, CCW+10, CWZ19, CST16, CCLZ10, CHS15, JS18b, Kiü15, LW11a, LWPK12, MNS11, O012, SEHK12, SS13, XJW+16, YWK10b, YTS12, ZHI15, ZM16, Abe10, BGE+18, BBPP13, BT18, CZ15b, CBJY16, GLIC10, GSGM16, HURU11, HH15, JZU+19, Jia14b, LGKY10, LWPK14, MSM+18b, NAL17, OTO18, SE18, SGFCRM+18, WYZ+17, WD19, XHH12, YY11, ZWQ+11, ZÁC17].

Application-Level [CCW+10].

Application-Speciﬁc [BD15].

Applications [AMVZ12, AEP18, Ana14, ABL+18, BBD19, BPKW12, Ber18, BKST18, BCG+12b, BJCHA17, BS12, CZL12a, CZLC12b, CPS16, CK18, D02, D07, DK15, FSK10, GKM16, GRL12, HSC19, HvS12, HJ19, HN10, HGOZ19, HVP+18, JWJ+17, LAT17, Nac12, NV10, Nie02, ODSS17, PJ12, RBS+17, RQD+15, Sas18, SCPSN10a, SCPSN10b, SG19b, Sha10, Shp03, SYV+19, Ter11, TYK+12, WH17, YR11, ZZQ+19, ZYY19, APMCR13, Ano11a, A KS19, BD16, CFR11, CSZ+11, CQX18, CDA14, Durt5, EBFLK13, FES10, Fri10a, GJ18, GHD19, G110, KKK+18b, KO16, LWZG10, LSQ15, LR15, LBOX12, LTT10, MS13c, MZL+19, MM14b, OSP+19, OK18, PHWM10, PKA15, SWW+17, WMC17, ZZ15, ZS18].

Applied [BSS11, KP10, MR10, BTW15, OPHC16, Xie12a, Xie12b].

Applying [Bar12, Elb09, NML19, sCR19a].

Approach [CTC+15, Chi16, DZS+18, DBT19, HMKG19, HLAZ15, HLW12, KRH18, KKA15, MN13, MZ17b, MHMSGH16, PS14, RP12, SLGZ12, Sia12, SH15, SC12, TCN+17, TLIW12, Vec12, VKC15, WYC14, yWXyZ+18, ZW15, AHG18, AL15, AT10, BSS11, CWZL13, CLZ+17, CO11, CML16, DEL19, DZS+12, FMB+18, GGH+16b, Ham19, JKA+18, KL13, LFGCGCR14, MCP15, MSGCDPSS18, NC13, PJ18, SAM+19b, SE16, SPK17, SA19, Tan18, WMYR16].

Approaches [GW16, LC15, NR15, SBV14, TCM19, MK+12, OK18].

Appropriate [SP15b].

Approximate [CN12, JSCM17, SGS14].

AppSec [RQD+15].

April [GLIC10, IEE13, PJ12, vDKS11].

Arab [Bro11].

Arabic [AIF+19].

Arbitrator [CCKM16].

arbitrarily [BCDN17].

Arbitrary [FHR14, DWZ12, Gen10].

Arbitrary-State [FHR14].

Arbitration [Kü15].

Arbitrator [WSA15].

architect [GW14].

Architectural [MD12, VCK+12, ZWT13].

Architecture [ADSH18, BCE+10, BEM16, HEP+11, HKL+14, Int19, KS18b, KCR11, KCC17, KAK18, LGR14, LWM16, MCDB12, MJGS12, MC11, NDMMW16, NVM+17, RC18, RMP10, SG12, SWM+10, SLI11.
SM18, VDB+16, YHSW19, AL15, Ano13f, ABO+17, BVIB12, LXMW12, MJS13, SSA18, SSS11, SSPL+13, XHM14, SAAB10, architecture-independent [BVIB12].

BCDN17, BZD+16b, BSR+14, BH19,
BCFK15, CBJY16, CGH17, dCCSM+12,
DCAT12, DJL+12, DK7, Dra16, Eng15,
EA12, FTV+10, FIO15, GPP+16, GLMS18,
GBNM11, HAK19, HAGTAR13, KMI0a,
KPS10, LDC13, LHM+10, LWK11, MBP19,
NDNR13, OF11, PX13, SGP+17, TK19,
TS16a, TY16b, TLL13, VS11, WWBC14.
attacks [WWDN12]. attempt [Fel13].
Attestation [BWS19, FQZF18]. ATtiny
[EEG12]. Attribute [AAC16, AHL+12,
BFK+10, Boy13, CD16b, CDL18, CDLW19,
CHI+19, FHR14, GZZ+13, GSW+16, Gli12,
GVW15, HSMY12, HBC+19, Her14, KGP12,
LW11b, LW11c, LW12, LJLC12, LYZ+13,
LHL+14, LAL+15, LHL+15, LW16, OT12,
PAA18, PB12, RVH+16, Rao17, SSW12,
TYM+17, WDC18, WHL15, WHLH16,
WHLH17, XMLC13, XWLI16, XHX+17,
ZPM+15, ZQQ15, ZMM17, ZHH15, BTK15,
CPPT18, FNWL18, HZL18, HZW18,
HYS18, HKHK13, JSMG18a, JSMG18b,
LCL+15, LFZ+17, LFWS15, LYL15,
LJW+17, LJWY18, LDZW19, Nam19,
QRW+18, RD17, SLL+19, WLWG11,
WZC16, WXSI17, XZP+19, XTZ+19,
YSQM19, YCT15, ZWM14, ZML17,
ZGL+18a, ZYW+19, Ver17].
Attribute-Based
[AAC16, BFK+10, Boy13, CD16b, CDLW19,
CHI+19, FHR14, GZZ+13, GSW+16,
GVW15, HSMY12, HBC+19, LW11b, LW11c,
LW12, LJLC12, LYZ+13, LHL+14, LAL+15,
LHL15, LW16, PB12, RVH+16, Rao17,
SSW12, TYM+17, WDC18, WHL15,
WHLH17, XMLC13, XWLI16, XHX+17,
ZPM+15, ZQQ15, ZMM17, ABL+12, CDL18,
Her14, WHLH16, CPPT18, HZL18, HYS18,
HKHK13, JSMG18a, JSMG18b, LCL+15,
LFZ+17, LFWS15, LYL15, LJW+17,
LJWY18, LDZW19, Nam19, QRW+18,
RD17, WLWG11, WZC16, XWLS17, XZP+19,
XTZ+19, YSQM19, YCT15, ZML17,
ZYW+19, Ver17]. Attribute-Hiding
[OT12, ZWM14]. Attributes
[CG12a, VKK+19, Yon11, LCL+17a].
Attribution [AIF+19, XIC+12, FNP+15].
Au-Id [HWZZ19]. Auction
[Con10, JWNS19, DDL15, HM+11].
auctions [MR14c, QS18]. Audience
[DE17]. Audio
[Ber18, DA12, FM15, GCK12, HGT15,
KD12a, KD12b, Lai14, LSL12b, NXH+17,
QF19, TC10, gWPnyY+14, XNG+14,
XNRG15, XNP+18, ZS12, LSQ11a, SKEG14,
yWPnyL11, XWYZ12, YQH12].
Audio-Visual [La14]. Audit [YNR12b].
Auditing [LMD16, LCPD15, TCN+17,
XWK+17, YTS+16, YXA+16].
Augmenting [AV18]. August
[AB10a, JY14, MV12, RAB10]. Aura
[HFCR13]. Austin [IEE13]. Australia
[Col17]. AuthCropper [KL+19].
Authentic [AVS+18, HLT+15, SZMK13].
Authenticate [HM12]. Authenticated
[Alo12, ADSH18, BSBB19, BCO13,
BDMLN16, CLL16, CLY14, CSES14, CRE+12,
DS11, EAA12, ESS12, FVSI7, FFL12,
GTT11, GL12, GZ12, HCl12, HL10a, HCL+14,
HEC+12, KMY18, KLK+19, LHKR10, LY16,
LH11c, LCCJ13, LT10, MR14a, MY12,
MMS17b, MVKS14, MSU13, PTT16, Sar10b,
Smi11b, Tan11, TW14, WDV18, XLM+12,
XHC+12, XGLM14, XZLW15, YS12,
YLSZ19, YLW13, YRT+16, Yon12, ZPZ+16,
ZXH16, ABC+18, AIB+16, ABR15, CTL13,
FA14b, FIO15, GPP+12, GLM+11, HPC12,
HWB10, HBW12, HL11, HPY10, ISC+16,
JKA+18, KMTG12, LWS10, LHH11,
LML+13, NCL13, Nos11, Nos14, ODK+17,
OSSAN19, PPTT15, P18, PPG19,
SMBA10, TCS14, Tso13, TKHK14, WZM12a,
WZM12b, WTT12, WXW14, XCL13,
XZW+18, YC12, YZZ+14, YZL+18, YLL+18,
ZT16, ZGL+18a, ZWV18, ZG10, ZSC15].
Authenticating
[BS12, CHX13, GRL12, OKG+12, RPG12,
WY12, ZCWS15, Bel18b, Cer18,
LFGCGCRP14, PGLL10, RR16, ZLDD14].

**Authentication**

[AV18, AA19, ADM19, AAA19, AMSPL19, ASO14, AAZ16, ACAT15, ACKB19, AUMT16, ABB19a, ATC17, BL12, BCE12, BCM12, BNNH19, BSSV12, Bel18a, BKST18, BCD12, Bis17, BF11, Boy16, BKPJ16, BS12, CGCGPDMG12, CTC15, CCI14, CSH18, CRS18, CCW10, CCF17, CCI19, CJ13, CD12, CJP12, CHL13, DL15, DCM18, DBPS12, DPKW12, DP12, FLH13, FR16, FMTR12, FD11, GWP19, GHS14, Gli12, GI12, GMDR19, GM14, GU13, GMVV17, GCK12, HZC12, Hvs12, HQY18, HKK19, HLLC11, Har13, Hay13, HBCC13, HM10, HPCL12, HCETPL12, HKL12, HFS18, HFCR13, HXC11, HLCL11, HCYZ18, HWZZ19, HK18, IGR16, JN12, JCM12, Jia17, JLX19, JAE10, KP12, KS18b, KLN15, KTM18, KRM10, KSD17, KPC11, KTA12, KGP12, Kim15, KPKS12, KLM12, KO16, KH10, LLC11, LKBK19, LH12, LFF18, LLG15].

**Authentication**

[LCLL15, LNZ13, LZCK14, LNXL15, LCR12, LLZ12, MWZ12, MEFO12, MKH12, MBC15, MRR17, MRS17, May15, MLBL12, Mor12, MSKR17, MPM17, NR11, NR12, NSBM17, NLLJ12, NLY15, OdH12, O012, O12, PSSK19, PCDG14, PPRT12, PDT12, PWVT12, RS11, RWLL14, RSX18, RNS14, SG18, Sa1a2a, SBS12, SBS18, Sar12, SCG16, Sch15b, SKV12, ST14, SM12, SD12, Shi11, SGC14, SSA13, SPK17, SRRM18, SC12, SCMS18, SZDL14, SHS12, SAA12b, SRK17, SRK18, TGC16, TWNC18, TYK12, TM12, Vet10, WgMdZJ12, WHZ12, WZX12, WgMW12, WZCC18, WSS12, WAK19, WT10b, Xia12, YTP11, YFT17, ZBR11, ZHW16, ZWZ17a, ZHS10, ZLDD12, ZLDC15, AMN18, AaBT16, AB13, AATM18, AMKC19, ARL13, Aia15, AL15, AMPG13, AHM18, APK18, AIM19, Alp18, AIKC18, ACF16, AZF12, AYS19, AT110, ACC13, AN15, ACM12, BK19].

**authentication**

[BOP14, BS13a, BGE18, BDM18, BDL19, BD18, BCM13, BGAD12, BBTC20, BDM19, BB19, BLAN16, BAI10, BMM12, BhvOS15, BT18, BTW15, BM11, CLM12, CML18, CLP13b, CAM19, CTL12, CJXX19, CSD18, CNF18, CH10, CCSW11, CHS11, CHJ13, CZ15a, Chi13a, CCMB19, CJP15, Cho14, CL11, CHL19, CRS13, CDWM19, DCA12, DC12, DRN16, DEL19, DLK16, DMV15, DLN13, DZS12, DMT12, uHAN18, EA12, ED19, EA11, FPBG14, FHH10a, FLL14, FP12, Far14, FA14a, FHZW18, FQZF18, FMA18, FHM10, FZZ12, GJ13, GMSW14, GHD19, GEAR11, GPLZ13, GH15, GH16, GAI18, Gop19, GCS19, GMP11, GLB18, GBC19, GTTS19, HU15, HSH11, Ham12, Ham19, HZW19, HW19, HHS18, HDPC13, HZC14, HK17, HZWW17, HL12, HLI4, HCM11, HLC16, HPL19, HCC10, HS11, IMB17, IAA19, IC17, IG11, IB11, IOV18].

**authentication**

[JAc16, JNUH17, JKAU19, Jia16, JKL16, JM16, JAS11, JXLZ15, KPP16, Ken11, KKG14, KSB17, KCS18, KVe18, Kim11, Kim16, KIH19, KS19, KP18, KPB17, KLW16, KLM17, KDW17, KKD18, LLL15, LLZ16, LC17, LLY06, LH11b, LT13, LH10c, LNM11, LMJC11, LXMW12, LNN13, LMK13, LJK14, LIK17, LCM17, LNK18a, LWK18, LNK18b, LLD19, LWK19, LW19, LHM14, LH13, LSQ15, LHH18, Lit14, LWLW11, LTC15a, LYL15, LZZ19b, LDR12, LTT10, MM12, MMLN15, MCN18, MDMH18, MV011, MMP19, MA17b, MMS17c, MWV18, MZL19, MCRB19, MHL18, MK12a, MGB19, NSDA17, NR17, NACLR12, NCCG13, NM18, NLYZ12, NML19, NB13, NXS10, NMX15, OSP19, OF11, OCG11, OYHS14, PYH18, PYP10, Par12b, PLGMCdF18, PCK19, PZBF18, PA10,
PKA15, PRN+19, QMC17, QMW17, QLZ19, RR17, SSSA18, SCFB15, SPLHCB14, SB17, SGGCR+16, Sar10a, SK18, SSNS15].

authentication
[SVY19, SGJ+18, hSZZ15, SCHK10, SYWX19, SNG+17, SCR19b, SA15, SYW17, SSS11, SKEG14, SA19, SMS+16, SHBC19, Tan12b, Tan15b, Tan18, TODQ18, TZTC16, TG17, TLL12, VSB+19, Wan13, WW14, WLZ+16, Wan18b, WCFW18, WXSH19, Wat14a, Wat15, WDKV19, WT10a, WKHI11, WXK+17, XHH12, XWDN12, XHCH14, XCCY19, XMHD13, XHM14, YI17, YH16, YHHS16, YYY+19, YWYK+10a, YSL+10, YMM13, YN19, YY13, YD17, ZYL+10, ZQWZ10, ZCLL14, ZQD16, ZGL+18b, ZDH18, ZZZY+19, ZHH+17, ZX11, ZLY+19, ZZL+18, OHJ10]. authentication-chaining [EA11].

authenticators [SYY+17].

authenticity [ADF12, VBC+15].

Authority [LNXY15, XZLW15, ZQQ15, JB11, SLL+19, ZWY+19, ZZ12].

Authorization [CS14, LMGC17, MPM+17, AL15, DFJ+17, FHM+10, JAE10, JAS+11].

Authorized [GHY18, HTC+15, LLSW16, Ma17a, WZH19]. authorizing [Bel18b].

Authorship [AIF+19, BT15, BAG12, LCM+17].

Autoblocking [LLLH18, YH16].

Automata [CCD15, Gas13, dRSdlVC12, Ang16, DGL19, HBBRNM+16, KFE19, SS11, WOLS12].

automata-based [SS11].

Automated [BHC19, CCK12, CCK16, DRS16, GLLSN12, JGP+18, LGM+16, Ste15a, Tom16, YSS14, BJR+14, GMMJ11, KKK+16].

Automatic [HWWZ19, MMP19, WW12, HL19].

Automation [BGK12, DZS+18, IEI11a, KPP16].

Automotive [HK18, LMS16, MPM+17].

Autonomic [SEK+19].

Autonomous [MPA+18, BT18, SMS+16].

Auxiliary [DMS+16, DL12, GGHW17, XXZ12, YCY12, Kom18]. Auxiliary-Input [XXZ12, Kom18].

Availability [CK11, ADF12, CFVP16]. Available [Ano16e, HGOZ19]. avatars [NSX+18].

AVC [JSZS12, JHHN12, LW13c]. average [Lim11, YL11].

Avoidance [RH+16]. Avoiding [AMMV18, BHCdFR12]. AVR [LPO+17].

award [Ano16i, Orm16]. Awarded [Ten18].

Aware [ARWK19, BCF16, HFS+19, JSA17, LJ17, LMHH14, LMS16, QL17, YTH17, ARL13, AKS19, DDY+19, GHD19, LWYM16, MGP10, TODQ18, Wan13, ZDHZ18, ZFH+18]. Awareness [HSC19, MSas12, SAM+18, HPJ+19, L10, MSas13].

axiomatic [AT10]. axis [WMU14]. Azure [Sti19].
BCEO19, BCEO20, BBB+16a, BSSV12, BHG12, BKPW12, BRT12, BHH+15, BBKL19, BS13b, BFK+10, Bon12, BSJ15, BF19, Boy13, BKJP12, BDH11, BCF+14, But17, CMLS15, CLL16, CGMO14, CKHP19, CMRH17, CCM17, CSH+18, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST+17, CZCD18, CLND19, CGL+12, CDD13, CGY+13, CD12, Chl12, CK18, CD16b, CDLW19, CHH+19, DSM14, DHT+19, DL17, DS19, DA12, DLZ+16b, EM12, EK+16, EFGT18, FM15, FHH10b, FHR14, FZT14, FGRQ18, FGM10, FYD+19, FR15, FVS17, FP19, FSX12b, FSX12c, FSX12a, GT19, GW12, GDL18, GZZ+13, GSW+16, GV14b, GI12, GY13, GDCC16, GVW15, GJJ15, GJZ17, GRRZ14, HZC+12, HSMY12, HSM14, HBC+19, HEP+11, HIJ+19, HLI10a, HXZ15, HWZ18, HCP12, HKL+12. Based [HG12, HMR12, HSA14, HWS+19, HPO+15, HKR+18, HGT15, HLC+14, HLN+10, Hul13, HRS16, HBG+17, HEC+12, HM19, HP12, HP17, JTZ+16, JP19, JHHN12, JEA+15, JKHe12, KMZS19, KS18b, KZG10, KK12, KKA15, Kha10, KLY+12, KSSY12, KP112, KHRG19, KRB12, KAK18, KS15, LMG17, LMG+18, LY+18a, LKY+19, LTK16, LSL12a, LKBK19, LSL12b, LW11b, LW11c, LW12, LHF12, LJLC12, LYZ+13, LHL+14, LTH+15, LLC+15, LDZ16, LTYZ16, LLZ+17, LLLH18, LPL15, LSLW15, LAL+15, LH11c, Lin15, LYL+18, LP12, LNWW19, LNZ+13, LCCJ13, LWCJ14, LNX15, LHL15, LW16, LPO+17, LWH18, LDL19, LZZ+19a, LGPRH14, LDB+15, LD13, LSC12, LBR12, LLLH18, MWZ12, Ma17a, MLO17, MEF012, MCD12, MVV12, MD12, MBC15, MK13, MZ17b, MCS+15, MMS17b, MKF+16, MCF17, Men13a, MST18, Mor12, MSKRJ17, MKAA17, Muf16, NS15, NC12, NXH+17, NDR+19, NXB13, NLL12, NLY15, pNyWyY+14]. Based [OTD10, PB12, PSSK19, PTT16, PYM+15, PDNH15, PPS12b, PYS18, PG12, PAS13b, PNRC17, QJC+18, QF19, RVH+16, RSR+19, RZZ+15, RS16, Rao17, RRI17, RDZ+16, RVRC12, RW12, RJV+18, SBS18, SSW12, Sar18a, SS13, Sen17, SLK18, SXH+19, SJ12, SGP+12, SPG+19, SP15b, SSA13, SRA17, SNCK18, SH15, SGH15, TB18, TKR14, TWZ11, TW12, TWW+12, TYM+17, TSH17, TT12, TTH15, TFS19, TC10, VDB+16, VGL15, VGA15, Vle12, WY10, Wan10, WSO12, WgMW12, WYW+13, Wan14, WZ18, yWxY+18, WDC18, WLH15, WHL17, WCL+18, WT10b, WMS+12, WZC19, XNG+14, XN15, XXZ12, XML13, XLQ09, XQL11, Xio12, XGL14, XWL16, XJW+16, XJR+17, XHHX+17, XHZ+19, YE12, YZCL12, YXZ+12, YGFL15, YHSW19, YTS12, Ye10, Ye14, YH16, YTH17, YY15, Y+17, YKNS12, YH+10, YM15, Y+11, YK++12, YCZ12, ZSP+19, ZPM+15, ZJ11, ZXZ+11, ZDL12, ZLH+12]. Based [QZQ15, ZMW16, ZXY16, ZWW21, ZZM17, ZWZ17b, YZZ+19, ZPW16, ZHW15, ZVG16, ZPXX17, ZGJC18, ZYM18, ZYH+19, ZHL15, AM18, AGL16, AAB16, ARL13, AY14a, AHS14, AAL19, AAT16, AA14, ASO14, AI+18a, AIM+19, AKG13, ASVE13, ACA+16, ARG19, AM19, Ara13, ATI+10, ACC+13, AHL+12, BK19, AVA18, BS15, BDM18, BDL+19, BBBBB13, BD18, BGD12, BAAS13, BBTC20, BFF+19, BOB13, BWR12a, BW13, BWA13, BM12, BZ16a, BC18, BTK15, BB16b, BK12b, CPPT18, CML+18, CXX+19, CFL13, CFY+10, CL11, CL12, CL15, CNF+18, CRS+18, CG12b, CSZ+11, CHX13, CSS+13, CW14a, CLC+19, CWZ19, CXW19, CC19, CT19, CJP12, CIP15, CCG10, CTL13, Cho14, Con12, CHL19, dCCSM+12, Cry11, CD18, DSC12, DMG19, DZ14, DNL13, Dra16, uHAN+18, EZ15, FHY13, FG19, Far14, FA14a, FA14b, FO15]. Based [Fay16, FLYL16b, FHZ18, FMC19,
FNWL18, Gal13, GJ13, GCH+19,
GMGCCC15, GMRT+15, GKCK11,
GJMP15, GCS+dp11, GAB19, GMS11,
GLL+18, GBC19, HSH11, HT11, HKA+18,
Ham19, HZW19, HW19, HHBS18, HGWY11,
HSM13, HZC+14, HZL18, HF14a, HWDL16,
HZZW17, HZWW18, HBBrNM+16, HLR11,
Her14, HWB10, HWB12, HB13, HL14,
HL11, HLC12, HLC16, HYWS11, HY18,
HYF18, HPY10, HKHK13, HCC10, Hwa11,
IMB17, IM14, ISC+16, IB11, IA15, IOV+18,
Jac16, JNUH17, JKAU19, JK13, JLT+12,
JCL+18, JZS+10, JMW+16, JSMG18a,
JSMG18b, JLX+19, JDV16, KFE19, KPP16,
KK13, KM10a, KHM13, KTM+18, KKG14,
KLS+18, Khl18, KD18, Kim11, KG010,
KD19, KLI+17, KKD+18, KL11, KSH18a,
KSH18b, LXLY12, LLZ+16, Lau12, LLC10,
LK14, LHM13, LHY+10, LHN+10, LH10c,
LZJX10, LNM+11, LMJ11, LK12,
LXMW12, LKAT12, LLHS12, LNLK13,
LXJ14, LDZ+14, LCL+15, LZY+16], based
[LYYM16, LFZ+17, LNK+18a, LWK+18,
LWW+19, LCT+14, LFWS15, LLM+19,
LPdS10, Lin14a, LHI+18, LLY+12a, LW10,
LQQ11a, LSQ11b, LWK11, LW13b, LZC14,
LPZJ15, LCT+15a, LYL15, LLY+17,
LJWY18, LDZW19, LWW+10, LL16a,
LW13c, LWY12, LYL14, MCN+18, MCP15,
MJGS12, MJ13, MLM16, MWW+18,
MZL+19, MMF15, MMZ12, MM13, Mes15,
MCRB19, MBB11, MO14, MSGCDPSS18,
MHT+13, MG15, MS17, Num19, NR11,
NM18, NCL13, NZL+15, NMX15,
OMPPL+19, PPA18, PYH+18, PLPW13,
PPTK14, Par18, PWW10, PGLL10, PSL+19,
PBB16, PLGMCdF18, PCK19, PS14, PL16,
PKA15, PC14, PPR+12, QZDJ16, QRW+18,
QYWX16, QMWW17, QLZ19, RD17, RG10,
RS15, SPLHCB14, SERF12, SGGCR+16,
SSL+19, SAM+19b, SI12, SD17, SYL13,
SE14, SE16, SK18, SH11, SM11, SNN14,
SZHY19, SR10, hSZ15, SCKH10, SA16b,
SPK17, SSAF11, SHC+16, SWW+16, SSS11].

based [SKEG14, SC19b, Sun16, SG16,
SHBK19, SS11, TPL16, TQL+14, Tia15,
TH16, THA+13, TTL10, TPKT12,
TOKH14, UKR+19, VN11, WVY11,
WWY11, WLLG11, WLD11, WZC16,
WLFX17, WMX+17, Wan18a, WMX19,
WXSH19, WZG+12, WHL16,
WS14, WS12, WTT12, WOLS12, WCCH18,
XHH12, XZWW16, XW12, XCL13, XWS17,
XZP+19, XCH14, XWZ+18, XTZ+19,
XMHD13, XHM14, YWL+17, YWJ+19,
yYqWqZC13, Yan14, YTM+14, YCC16,
XIA+18, YSOM19, YWY+19, YCT15,
YTF+18, YY13, YLS12, YMS10, YKC+12,
YLZ+16, YXA+16, YL11, ZZKA17, ZAAB17,
ZYGT17, ZLW+12, ZCL14, ZT14, ZT16,
ZQD16, ZML17, ZGL+18a, ZGL+18b,
ZXY+19, ZZ12, ZHH+17, ZL12, ZHV14,
ZDW+16, ZYM19, ZLY+19, LZX10, Ver17,
HZC+14, MM12, PP11, ZBR11, Kat13].

Based-Encryption [ZHW15],
based-wireless [HKA+18], Bases
[EVP10, TSH14, FES10], Basing
[Mat14, MN10], Basis
[BNA15, ERRMRG15, RMRM19, CG12b,
Har15, LLP+18, Tam15], Batch
[WSQ+16, ZPXX17, AGHP14, CCG10, MGB19],
batch-based [CCG10], Batters [Chi13b],
Battery [CKHP19], battles
[ANO15a, Ano16b, Sch15c], Bay
[ANO10a, DDS12], Bayes [McG11, Sim10],
Bayesian [Alz19, WYW+13, ZLW+17], BC
[LSG+19], Be
[ASV+18, DSM14, Mos18, Par12a, YM16,
AZH11, Ana14, Dya19, Eve16, Ree15, RK11],
BeagleBone [CRI16], Beat [LTKP16],
BECAN [LLZ+12], Becomes [Bra13],
been [Ana14], before [GST12, Goo12],
Beginner [Gre19a, She17], Beginning
[Chu16, Zor12], Behavior [ASV+18, GSC17,
RSX18, KNL15, SPK17, VB19],
behavioral
[BOP14, CAM19, HT11, MWW+18],
Behaviors [GAF+15, HL19, ZMYB17].
[ACAT+15]. Bletchley [Bai12, Ano11c, Bri11, Col17, Cop06, Cop10a, Cop10b, GMT+12, GW14, McKi10, McKi11, McKi12, Pca11, Smi10, Smi11a, Smi15b, Smi15a].

**Blind** [AP10, Ano15a, BCPV11, LCLW17, LGRtRH14, MR16, MMN12, RS16, YMWS11, HKB14, MO14, RM15, RM18, WLD11, yWpWyYpN13]. **Blindfold** [Nac16]. **Blindfolded** [Vai11]. **Blinding** [CLHC12, KHHH14]. **Block** [AMVZ12, BRS17, BSS+13, BFMT16, BDGH15, BCG+12b, CWP12, DWWZ12, EGG+12, FXP+17, GLSN12, GT12, GST12, GNL12, IS12, KR11, KWS+12, LYK19, LWZ12, LJ17, LCLW17, LGLL12, LWKP12, LWPFF12, MCDB12, MRTV12, OGK+15, PH12a, PDI+19, PRC12, Pud12, SJKL18, SG+12, SSA13, WW12, YCL17, ZSW+12, BNY14, Jeo13, KM11, LGP19, LPZJ15, LC13, LYHH14, LWKP14, MCL+19, MN12, MHI15, MHY+18, PL16, Sar11, SKK10, TQL+14, Tn17a, WB12, WWBC14, ZSW+18a, JKP12].

**Block-Parallel** [MCDB12]. **Block-Wise** [SS13]. **BlockA** [CHL19]. **Blockchain** [Alz19, Ano19c, ATD17, AHWB20, CLC+19, Eya17, Hur16, HM19, JWNS19, KV18, NML19, Pec17, Scr18, SG19b, SJZG19, TBY17, VFS+19, ZXL19, HHBS18, JLX+19, LHI+18, Nor17, CHL19].

**Blockchain-Based** [HM19, HHBS18, JLX+19, LHI+18]. **Blockchain-Enabled** [KV18, NML19]. **Blockchains** [BNMH17, RM19, WSL+19]. **blockcipher** [CMS17]. **Blockciphers** [LST12]. **Blocks** [JSK+17, Bra15]. **Bloom** [ATKH+17]. **Blowfish** [KB10]. **BLS** [BP18]. **BlueKrypt** [Gir15]. **Boardroom** [LHF12].

**Bodacious** [KM10c]. **Body** [LZCK14, LCR+18, ASO14, KP18, LIK+17, LZZ19b, SG+18, WDV18]. **body-sensor** [ASO14]. **bogus** [XWDN12]. **Bombe** [Bur11, Car10]. **Bonebrake** [SS10c]. **Boneh** [TK19]. **Bonneau** [Ano16a]. **Book** [Ano15b, Ano16a, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kob10, Low12, Mei10, Mur10, Sha15a, Sha10, SR14, Ter11, Sto12].

**Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LV11, WT13, YCC16, ZZQ+19]. **Boolean-based** [CW14a, YCC16]. **Boomerang** [BCG10]. **Bootstrapping** [BGV14, GM14, KKK+16]. **Border** [LGM+16, ZTSR12]. **Born** [LJY16]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Bottom** [Ano15a, Ano16a, Ano17b, Ayu12, Bar12, Dew11, Fra10, Joh10, Keb15, Kob10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12].

**Boundary** [ACZ16, AS17, CW14a, DQFL12, FY11, LV11, WT13, YCC16, ZZQ+19]. **Boundary-based** [CW14a, YCC16]. **Booster** [HC16]. **Bootstrap** [BCG10]. **Bootstrapping** [BGV14, GM14, KKK+16]. **Border** [LGM+16, ZTSR12]. **Born** [LJY16]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LV11, WT13, YCC16, ZZQ+19]. **Boundaries** [BCG10]. **Border** [LGM+16, ZTSR12]. **Born** [LJY16]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Bottom** [Ano15a, Ano16a, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kob10, Low12, Mei10, Mur10, Sha15a, Sha10, SR14, Ter11, Sto12].

**Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LV11, WT13, YCC16, ZZQ+19]. **Boundaries** [BCG10]. **Border** [LGM+16, ZTSR12]. **Born** [LJY16]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Bottom** [Ano15a, Ano16a, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kob10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12].

**Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LV11, WT13, YCC16, ZZQ+19]. **Boundaries** [BCG10]. **Border** [LGM+16, ZTSR12]. **Born** [LJY16]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Bottom** [Ano15a, Ano16a, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kob10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12].
SXH+19, WQZ+16, XJW+16, Yan14, ZHW15, CPPT18, DLN13, SM19b, WWYY11, WDZ19, XWDN12, XZP+19, YMM13, ZWQ+11, ZZ12, Zha13.

Broadcasting
[OO12, MK11, OCGD11, SM19b, YY11].
broke [Bat10, Hea15].
Broken [MDAB10, Tur18].
Broker [TKR14].
Broker-Less [TKR14].
Browse [NA14].

Browser
[QF19, ABR13, ACC+13, BCFK15, GJH+12].
browser-based [ACC+13].
Browsers [FVJ19, Rec15],
browsing [MWW+18, YYY+19].
Bruce [Sev16].

Brute [CJP12, JR14, CJP15]. Brute-Force [JR14, CJP12, CJP15].
BRW [CMLRHS13].
BSeIn [LHH+18].
BTC [CLF11, QJ+18].
BTC-compressed [CLF11].
Bubbles [HHBS18].
Buchwald [ABJ13],
Bucket BKKV10. Bug [Chii13b].
Build [IM16].

Building [BPS16, GB19, KMP+11, MJS13, Sev16, WL11, CHH+13, LCKBJ12].
 built [GSBV18], built-in [GSBV18],
Bullet [MC16].
Burdens [Bla12, SR14]. Bus
[AN17].
Business [LDB+15].
Butterfly [HQY+18].
Buyer [Fra16, KJN+16].
Buyer-Friendly [Fra16].
BYOE [Tan17a].
byte [Hof15, Hof16].
Bytecode [SEK+19].
bytes [PBC14].
Byzantine
[KS11, LLKA19, YGK13].

Byzantine-resistant [YKGK13].

C [AD12, ACZ16, Cra14, DGJN14].
C&C [GN16].
C1G2 [MKD12a].
CA [ACM11, Dm12b, Kid11, Lin14b, Ple10, Rab10].
CABA [MSKRJ17].
CABE [XHH+17].
Cache [AB15, ADR18, CBRZ19, DMRK15, FHY+19, HLZ15, LWML16, SY15a, YD19, DJL+12, DK17, MCL+19].
CacheAudit [DMRK15].
Caches
[LLGJ16, CDPLCA16, DJL+12].
Caching
[ADR18, HLZ15].
cackled [Bus12].
CAD [PGLL10].
Caernarvon [KMP+11].
Calculus
[MR10, Jou13].
Calibrated
[LC15].
California
[Ano10a, IEE11b, IEE15, MSH+16].
Call
[Ano16b, Ano16c, Ano16j, CS14, Hor19, KRM+10].
Call-Back [KRM+10].
Calls
[Mur16, KGP+19],
can [PKS18].
Cambridge
[ACM10, PJ12],
Camellia
[Bl10, LW12, LWF12, LW14, SEHK12].
Camellia-192 [Bl15].
Camera
[ATC17].
Cameras
[ASV+18, MKH+12].
Can
[Alo12, AZH11, Bar15, DMM14, KNT13, YM16, Pec17, RK11, Rus15, Sto12, GMVV17, LMS16].
Canada
[YY14, MV12].
Canal
[GW+19].
Canceled
[QLZ19, AJYG18, LZ11, LH14, YWZ+18].
Cancellation
[DLMM+18].
cancelled
[Ano14c].
Candidate
[GH+16a].
candidates
[ABM+12],
canonical [Bus10a].
CANS
[HWG10, LTW11].
Can’t
[ASV+18, Kni17, RAZS15, PZ15].
CAOVerif
[ABF+14].
Capabilities
[CHN+18, GF12, Lop15a, KMG17].
Capability
[IA15, LLZ+17, LT13].

Capability-Based
[LLZ+17].
Capacity
[LLY+18, TDLQ18, WY18, XNRG15, YWW10, BCN19, CLZ+17, GZH12, PWL13, WHL13].
Capacity-aware
[TODQ18].
Capacity-Raising
[YWW10].
Capitalism
[Fid18].
CAPTCHA
[OTO18, SKEG14].
CAPTCHA-based
[SKEG14].
Capture
[ASV+18, MBC+18, NYR+14].
Capture-the-Flag
[MBC+18].
Captured
[HWZZ19, SPK17],
capturing [PKS18].
Card
[BDFT12, HMR12, HCL+14, PTD12, Ano17c, CLH13, GLC10, LK11, Mom10b, Cho10, SD12].
CARDIS
[GLC10].
Cards
[BS15, LA10, PWVT12, WGMdZ12, WGMW12, CHS11, CHH+13, HCC10, KY10, LH10c, LNM+11, LXMW12, MM12, SGGR+16, YZS+14, YSL+10, YY13].
care
[FHV16].
caricature
[CJY18].
CariGANs
[CJY18].
Carlo
[CL12, FVK17, GQH17].
Carol
[Xie12a, Xie12b].
Carry
[GWM16].
Carrying [PV17]. Carved [LC15].
CASCAC [DZS+18]. Cascade [WGD18].
cascaded [DGL19]. Cascading [GT12].
Case [Ano17c, DR11, Kni17, SBS+12,
SY15a, SRT12, Uto13, YL17, Dya19, KD18,
LKKL13, MD12a, SS17a]. Cases [SG19b].
Cash [YMWS11, Bro12, Pec12, Zor12].
Casting [CW12b]. cat [Pow14].
Catalan [SAM+19b]. Catalog [AHS13].
Catching [SXH+19]. CBA [KRM+10]. CCA
[AHS14, BWLA16, CBX19, CZLC14,
HWS+19, LLPY19, LTZY16, LSLW15,
LLG19, MSas12, PDNH15, SYL13, SLZ12,
yYqWqZC13, ZLY19, ZY17a, ZSW+18b].
CCA-Secure [BWLA16, CZLC14, LTZY16,
SYL13, yYqWqZC13, ZSW+18b]. CCA1
[MSas13]. CCA2 [Gal13, GV14b, LLW16,
LLSW16, MVVR12, RG10, ZZ12, ZY17b].
CCA2-secure [LLW16, ZY17b]. CCM
[SKK10]. CDF [Ara13]. CDH
[PDNH15, ZG10]. CDPS [LLL+17b].
CDTA [YFT17]. cell [LLY+12a].
Cell-counting-based [LLY+12a]. Cells
[DSB16]. Cellulare [dRsdIC12, Ang16,
FMA+18, HBBRNM+16, HCM11, KFE19,
KRM+10, SS11, WOLS12]. Censorship
[DR16]. Centers [SDC+17]. centralized
[NACLR12]. centre
[McK10, McK11, Pal16, ISC+16]. Centric
[DLZ+16b, FP19, Vle12, XHZ+19, ZVG16,
AHM+18, BLV17, BPP10, PN10, YYW+19].
centroid [LWF12]. Centuries
[Cer15, Cer18]. Certificate
[GWWC15, HP12, LTH+15, LDZ16,
WMS+12, YLZ+16, ZGCZ18, BJR+14,
GGL+18, Lan13, LH+10, LDZ+14, LL16a,
MBF+13, NPH+14, JB11]. Certificate-based
[CT18, GWWC15, IL15, LSQL17, LSQL18a,
LZCK14, RSD19, SZS14, TCL15, WMS+12,
YT11a, YT11b, YJSL18, YY17b, ZM18,
ZSY19, DXWD16, HPC12, JXLZ15, LL16b,
SGJ+18, ZQWZ10, ZY17b]. Certificates
[HP17, Muf16, SC12, GIJ+12, HREJ14].
Certification [LDB+15, Ver17]. Certified
[ABB13, CLL16, STC11, HL14, LH13,
XWX14, YN19]. CertShim [NP+14].
chaff [KHM13]. Chain
[EA+16, FV17, KV13, QZL+16a,
QZL+16b, YFT17, YSF+18, YFT18, CR12,
Par18, CL16, SJWH+17]. Chaining
[GGK18, YM18, EA11]. Chains
[GKG19, JSAK+17, HLYS14, JCHS16].
Challenge
[AD12, GHS14, SPK17, YDH+15, ZCC15].
Challenges
[CNI2, FREP17, FS15, Fra15, Lal14, LLGJ16,
MRS+17, PCY+17, SBV14, TCMLN19,
ALL+18, Hod19, KIN+16, WS14]. Chances
[ALL+18]. Change [KMK18, ZWT13].
Changeable [FGM10, ZCL+12]. changed
[Mac12]. changes [PTR18]. Changing
[Abb12]. Channel
[AMMV18, AN17, AN11, ACA+16, Bar16b,
BCHC19, Bul18, CDK+10, CBL13, CATB19,
DZS+18, EWS14, GWM16, GPT14, HLH19,
KOP12, LGR14, LWML16, NDC+13, PRC12,
SG15, T12, YL17, ZBF18, ADG16,
BVIB12, BCDN16, CPPT18, CAM19,
DMWS12, DIL+12, GZSW19, GSAV18,
JLT+12, LM14, LFK19, MFH13, ZGY18].
Channels
[ASN12, BGN17, DMR15, EPAG16,
FDY+19, KW14, SS19, VCD16, Vua10,
YDV19, AGH+17, BCND19, BEB+18, CL16,
DMV15, DKL+16, LWZG10, MCL+19,
NR11, SM19b, SRB+12, WMU14, ZPZ+16].
Chaos [AIA+18a, LW13c, RRR11,
RVRSC12, ARG19, CCL11, LW13b,
J12b, ZLW+12, SFCRM+18].
chaos-and-Hamming [CCL11].
Chaos-Based [RR11, RVRSC12,
AIA+18a, LW13c, ZLW+12]. Chaotic
[BCGH11, IAD10, LFX+18, Yel10, Bro19,
GCH15, ISC+16, KCS+18, KLW+16, LWK+18, LWL+19, LW10, LZZX19, NES+14, WDG19, WZG+12, ZT14.

Chapman [Fa110]. Character [SS12b].

Characteristic [BGJT14, NR15, SR10, ZWZ17a, BGJT13, Jou13]. Characteristics [SSF19, TCMLN19, BEB+18].

Characterization [ALR13, BS13b, DPCM16, RZ19, YZLC12, YDY19, DDD14, PLGMCdF18].

Characterizing [Ash14, JR13, RVS+18, MPJ16]. Charging [CKHP19, LSY+16]. chart [Pec17].


Checkability [LHL+14]. Checkable [IW14]. Checking [FYMY15, YL17, SYY+17, YXA+16, PZL+19]. Chen [LLLK10].


choice [LLP+18]. choosing [BL17].

Choquet [SH11, SM11, SNM14]. Chosen [FSGW12, zGXW12, HLW12, HPY10, LCT+14, LCZ12a, LLML12, MH14, RS10, WWHL12, GLM+16, GH12, LZF14].

Chosen-Ciphertext [RS10, FSGW12, LCT+14, GH12, LZF14].

Church [ABJ13]. CHURNs [RBNB15].

Cipher [BW16, BFMT16, BCG+12b, CMLS15, CGCS12, DM18, DG12, DWWZ12, EHKS19, Fis15, FXP+17, GLLSN12, GCS+13, HZ11, Hey17, IOM12, JKP12, KR11, KWS+12, LPS12, LYK19, LWZ12, LJ17, LJ19, LWK12, LPFW12, MRTV12, MHC12, MS12b, OGK+15, PH12a, PRC12, WSSO12, WHN+12, YCL17, ZAG19, AMS+10, BNY14, CR12, FVK17, HKT11, Hol12, JEO13, KDH15, Lew10, LC13, LYHH14, LWKP14, MNP12, PL16, Ree15, RS14, Sar11, WYL14, WWBC14, ZSW+18a, LGL+12].

Ciphers [ABS+12, BMS12, BSS+13, BM18, BKL12, BRu12, CPW12, DGFH18, DGIS12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNL12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCLW17, LLJ12, LJ16, MD12b, NN12, PDJ+19, Pud12, Sas12, SEHK12, SLIK18, Sta11a, Vua10, WH18, WW12, Xie12a, Xie12b, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, GMT+12, KMI0a, LGP19, LWK11, MCL+19, MRT10, MH15, MHY+18, QGGL13, SKK10, TQL+14, WB12].

Ciphertext [BDPS12, CWWL12, CHH+19, zGXW12, HLW12, JMG+16, JSMG18a, KA17, LCZ12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XLMC13, XLWJ16, YM19, ZHW15, CPPT18, SFGW12, GLM+16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT+14, LFWS15, LCZ14, LDZW19, QRW+18, RD17, SGM16, WZC16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertext-only [KA17].

Ciphertext-Policy [CHH+19, Rao17, XMLC13, XLWJ16, YL17, JSMG18a, KA17, LCZ12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XLMC13, XLWJ16, YM19, ZHW15, CPPT18, SFGW12, GLM+16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT+14, LFWS15, LCZ14, LDZW19, QRW+18, RD17, SGM16, WZC16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertexts [LLPY19, Sta12, WQZ+16, AHL+12, JSMG18b, LCT+14, NMP+13, WXLY16, ZYW+19]. Circle [SC10].

Circuit [AH19, EAAAA19, Kar12, MY11, XWS17, XLWJ16, Lau12, MS13a].

Circuit-Size [MY11]. Circuits [AIK14, AS17, BCP17, BR14, GGH+16a, GH11a, GVW15, MFB18, SS10b, SS12a].


cities [LZD+19, SS18]. Citizen [Ano16e]. City [Ano17d, GAI+18, JZU+19, LNK+18a].

claimant [YI17]. Claims [SKGY14]. Clara [MSH+16]. Class [BCG12a, SY15a].

Classical-quantum [BCDN17].

Classification [CHH+19, HPC10, HS18, KAHKB17, SGP+12, ZLW+17, ACM19, HZW19, LHL+18]. Classifiers [KGV16, LCM+17]. classroom [Pow14].

Claudius [Hol12]. Clean [Fri13]. CLEFIA [LWZ12, TSL11, TS16a, WB12].

CLEFIA-128 [TSL11]. CLEFIA-type [WB12]. Client [ASM12, CTC+15, FD11, RAZS15, Vle12, BK19, FA14a, FA14b, GSGM16, JLY+19, MHL18, SG19a, hSZS15, WT10a].


cloaking [CHH+13]. Close [Wal18]. Cloud [AJA16, BDL+19, BCQ+13, BT15, BCK17, CWL+14, CWL16, DFZ16, CCT+14, CLW16, CDLW19, DK16a, DXA14, FYD+19, FC14, FPY15, HW18, Her19, JLS12, JWNS19, KMSM15, KS18b, KKA15, Kup15, LA15, LLP19, LYZ+13, LGR14, LL+15, LCP15, LNX15, MLO17, MJW+18, MGJ19, PSM17, Pet12, BCB+17, SGG15, SG18, SGJ+18, SKH17, SRA17, SOR16, TV15, Vle12, VV19, WLFX17, WR17, WHL17, WWW17, XNK15, XSW16, XMCL13, XWL16, XJW+16, YDY+16, YZD19, YHL16, YJSL18, YXA+16, YM+17, ZZQ+19, ZDL12, ZLDC15, ZVG16, ZLW+17, ZZL+18, AaBT16, AKKY17, AZPC14, AS14, AAV+16, ACK+17, ABR13, ADH17, ALL+18, Bel18b, BSGB19, BZD16a, BG14, BK12b, CFVP16, CSD18, CLH+16, CXW17, CZ15b, CDL18, DDD+19, DYZ+15, EAAAA19, FH13, FLYL16a, FNW18, GQH17, GLB+18, GZS+18, HSM13, HZW18, HK19, HYL+19, HYS18, IMB17, JEO13, KKA14, KKM+14, KSB+17. cloud [KLW+17, KKD+18, LZX+14, LZY+16, LLH17, LZW19, LWW+19, LAL+15, LWA13a, LYL15, LHL15, LCY+16, LZC17, MLM16, MSG18, NR17, Nam19, NB13, ODK+17, PPA18, PP11, PPG19, PWS19a, Rao17, RR16, SG19a, SSL+19, SYY+17, SAR18b, SM10, SKB+17, SWW+16, SWW+17, SA19, TLMM13, WLWG11, WL12, WSC14, WM+17, WXMZ19, WD18, WLS14, WS19, WCH18, WL19, XXX15, XWK+17, XYX+18, XTZ+19, XYL19, YYS+16, YZCT17, YHMM1, YQOL17, YQZ+19, YWT+12, ZYC+17, ZVH14, ZDW+16, ZZC17, ZWS+18, ZFH+18, ZLY+19, ZHT16, ZZL+19].

Cloud-aided [SGJ+18, WLFX17].

Cloud-assisted [VD18]. Cloud-Based [KSR18b, SRA17, ASO14, BK12b, WCCH18].

cloud-edge [CW18]. Cloud-Edges [BD19]. cloud-hosted [SG19a].

Cloud-Manager-Based [KKA15].

Cloud-of-Clouds [BCQ+13]. Cloud/Fog [JWNS19, LWW+19].

Cloudier [CFE16]. Clouds [BCQ+13, HLC+18, RHL18, RSN14, HFT16, IC17, JKL+16, LFW15, LL16a, Wu17, YNX+16].

Cloudier [CFE16]. Clouds [BCQ+13, HLC+18, RHL18, RSN14, HFT16, IC17, JKL+16, LFW15, LL16a, Wu17, YNX+16]. cloudier [BYD19].

Clustered [DS11, KS18b]. Clustering [KRD13, SVS15].

CMAC [SKK10]. Co [LF18, MB15, RML+18, HFC13] Co-analysis [LF18].

Co-Design [MRL+18].

Co-operative [HFC13].

Co-Processor [MBR15].

colg [KO16].

collection [OHJ10].

Coda [Beri16a].

Code [AD12, Bud16, CCL+13, Col17, Cop10a, Fox13, HG12, KSY12, Mun17, PY+13, SS13, Sen17, Sti15, War11, ABB13, Ant14, Bha16, Bri11, CCL11, CM19, CB16, EM19, GJ+12, GAB19, MCP15, Mc11, McK12, Moo14, OF11, PTR18, PA10, Wes15].

Code-Based [HG12, SS13, Sen17, CM19, GAB19, MCP15].

codex [Ant14, Bri11].

Code-breaking [War11].

codebreaker [Car11].

Codebreakers
[DDR+16, MHV15, BKR19, NR11]. Comparing [KTM+18]. Comparison
[CGCS12, DWB12, HPC10, KU12, KA18, MZLS18, ST14, HM10, LCM+17].
comparisons [Mid10]. compartmented [EZ15]. Compensated
[GKSB17]. Compensation [JSZS12, WMU14]. Compensated
[GSFT16, YFT17, YJSL18, ZBPF18, Bul10a, Kas15]. compress
[LC13]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16].
Compressed-Field [GM16b]. Composition
[LJS+14, NRZQ15, Ana14, AGH+17]. compound
[BJ16, KPS10, JT12b]. Comprehensive [GSFT16, YFT17, YJSL18, ZBPF18, Bul10a, Kas15]. compress
[LC13]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16].
Compressed-Field [GM16b]. Composition
[LJS+14, NRZQ15, Ana14, AGH+17]. Compressive [CCZC13]. Compromise
[YNR12b, GBNM11, PX13]. Compromised
[DSSDW14, DSSDW17, ZYL+10]. Compromising [BC14, BM18].
[LGH+17, FWS13]. Computation
[ARM15a, ARH14, ABPP16, ABL+18, Ash14, Bee17, BDOZ11, CATB19, Fria10b, GTS12, GVW12, GHKL11, HP14, HC17, HZX+18, IEE11a, Jin10, KW14, KMO14, LHM+15, LQD+16, MP14, Mali3, NSMS14, PST13, Risi1a, SZHY19, SVCV15, SZQ+17, TX16, TM18, Wat10, ABDP15, AB10b, BHH19, DEL19, DGL19, LDDAM12, PHGR16, TG12, YSQM19, vDKS11].
Computational
[BBD19, BCO13, GKS17, RD17, RPHJ11, TBCB15, HRS13, SJ19, SDM14].
Computationally [BCEO19, BCEO20]. Computation
[ARM15b, CK18, KHPP16, Nac16, PH16, ADMM16, BK12b, LWW+19, LR15, SSAF11, TLMM13]. Compute
[MJW+18, Vai12, PZ15]. Computer
[BGK12, BCGK12, BGB12, ABBD13, DK12, FGPGP14, PHWM10, Sta11c]. Computer-Aided
[BGK12, BCGK12, BGB12, ABBD13]. Computers
[Mos18, Bre18, Cop06, Cop10b, Dya19, LCKBJ12, Mac12, MvO11, PHWM10].
Computing
[ACM10, ACM11, AMMV18, Abb12, AHA16, Ano17e, BCG+12b, BTK15, CLB19, Cer14, CGB+10, DXA14, EAA12, FES10, Gen10, GB19, JWNS19, KMSM15, KP17, LCK11, LT14a, LYZ+13, LLC+15, LLJG16, LNYX15, MLO17, OS16, PAF18, Pet12, RS18, Roh19, SJW+17, SLM10, Vai11, Vle12, WRP70, XMLC13, XWLJ16, YE12, YZDZ19, YHL16, ZLDC15, AaBT16, AZ+16, And13, And19,
ABR13, BZD16a, CXWT19, CZ15b, CSTR16, DKL+16, DWZ12, DYZ+15, Dya19, GQH17, Gop19, HSM13, HYS18, Jeo13, JSMG18a, KKA14, KKM+13, KKM+14, KSB+17, KH18, LXX+14, LLH17, LYL15, LHL15, MS12a, NR17, Nam19, NCCG13, ODK+17, PP11, PKA15, QZDJ16, QRW+18, Rao17, Tan12b, WSC14, Wan18a, WDKV19, WLS14, WL19, XXX15, XZF+19, XYH+18, YHG15, YHL15, ZHW15, ZLY+19, ZSW+18b, YXX+18]. conceal

Content [AAA’19, ADR18, BCP14a, KD19, MHT+13, PMZ13, PZPS15, WHZ12, WZX12, YT12, ZZX+11, GPN+12, HPL+19, JS18a, YWY+19]. Content-based [KD19, MHT+13, YWY+19].
Continuous-Tone [Yam12]. contract [MMP19, Men13b]. Contracts [BNMH17].
contrast [DDD14, GLW13, LWL10a, MM14a]. Contributors [Ma17a]. Contributory [QWZ+16]. Control [AMSPL19, ATS15, BFK+10, DLZ+16b, GKK18, GRRZ18, HBC+19, HHS+15, HLC+18, LGM+16, LGLK17, LJ17P, MM17a, MK12b, NAI0b, PV17, QZL+16a, RSN14, SGC14, SYv+19, TBCB15, XMCL13, XHZ+19, YTH17, ARL13, ACK+10, AMHJ10, BBTC20, CLH+16, CO11, Cra11, FG19, FNW18, FS18, GHD19, HPJ+19, JAS+11, LCL+17a, LCL+15, LH17, LHH+18, MDHM18, NZM10, QCX18, RR17, Sch15c, SA15, Tan12b, Wan18a, XHH12, XYML19, YWJ+19, ZML17, ZDHZ18, ZVH14, ZWS+18, ZFH+18, ZZL+18].
CorrectDB [BS13a]. correcting [ATI+10, LTT10, MCP15]. Correction [KSH18a, LSC+15, yWXZ+18, Chl13a, Sun16]. Correctness [YGS+17, WS13].
Correlated [RS10, Jia16, ZPZ+16].
Correlation [BW12, FAA+18, LD13, SDM+12, WWBC14, XHH12, YCL17]. correlations [Sar14]. Correspondence [SY14]. corresponding [DWZ12].
Corrigendum [HYS18, WZM12a].
Corrupted [Fyo19]. cosmography [Pet11].
Countermeasure
[BBB16a, MD12b, GJ19, HYL19].
Countermeasures [BGN17, DZS18, EWS14, PZPS15, DK17, FAA18].
Counters [BM18]. Counting
[Bul18, LLY12a]. Coupling [SMS14].
Countermeasures [BGN17, DZS18, EWS14, PZPS15, DK17, FAA18].
Counters [BM18]. Counting
[Bul18, LLY12a]. Coupling [SMS14].
RPHJ11, Rja12, RBHP15, SK11, SEY14, SFKR15, Sch12e, Sev16, SGY11, SP15b, Shp03, SDM+12, SR14, SOF12, TW12, Tom16, WSL+19, WRP70, XZL+19, YZLC12, YNR12a, YNR12b, YS15, ZSY19, ABDP15].

Cryptographic [AY14a, ABB+14, ABF+14, ABC+12, ABO+17, BYDC19, Bar19, BFG+14, BJ10a, Bon19, CFL13, Cha13a, CZF+10, CR10, CP13, CLCZ10, Cra11, DGJ14, EFHK13, ESR14, GGH+16b, GJJ18, Gil10, GLR13, HYL+19, JCL+18, KKJ+16, KSU13, KAS15, KSH12, KKK+16, LGKY10, LLL+17b, MS13e, Mat19, MMZ12, MM13, Mes15, MSGCDPSS18, MN10, NDNR13, OO18, OMPSP+19, Pal15, PLPW13, PSH+13, QZDJ16, SD10, WT13, WMX+17, YSM14, ZHL+11, ZHY14, Zim10, Sha10].

Cryptographic-Key [SK11].

Cryptographical [KU12].

Cryptographically [ADD10, BCGL11, BJ12, BLS18, MC11, NG+17, PLs+10, SVC15, CBL10, GCH15, HJM+11, SA14]. Cryptography [ACZ16, Alz19, ABO+17, AA+14, ABC+12, AB10a, AG18, AMJ+17, ARM15b, Bar12, BGK12, Bar15, BBCL19, BRT12, BCGN16, Big08, Bon12, BF19, BKKV10, BJ10b, Buc10, BLM17a, BLM17b, BLM18, BCF+14, CNR14, CT18, CFH14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK02, DK07, DK15, DXA14, DP17, DBT19, DHLAW10, DF16, DKS12, DR11, Eis10, Elb09, FPS12, FHL19, Feh10, FSK10, Fid18, FMB12, Fre10, GT19, GO17, GFBF12, Gol19, G+13, Gre19a, GPT12, GLW12, Ham17, HEP+11, Hes12, HGI12, HR19, HPS08, HKR+18, JS18b, JT12a, KM10e, KP10, KAK18, LSL12a, Lin17, LWL10b, LGWY12, LMHH14, LGH+17, LWHS17, LPO+17, MI12, MS10, Maur12, Men13a, MR14c, Mi10b, MST18, MV12]. Cryptography [MMB17, NNA10, NDR+19, Nie02, NS12, Orn16, PP10a, PÁBC+19, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16c, Sch18, Sch19b, Sen10, SS13, Sen17, SK12b, Seo18, She17, SA16a, Sim15a, SGS14, Sma16, Sta11b, Ste15a, VS16, VGF19, WFL+14, WY12, Wns16, Yan12, YTS12, YL17, YW+19, ZZCJ14, ZZ17, vRDHP17, vTJ11, AMN18, AMOR13, AEH17, AAT16, AA+14, ABD13, And19, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Bö12, BSR+14, BS12, BBB16b, CFR11, Cha13b, CQX18, Cho14, CSR16, Con12, CDS14, DDD14, DA18, DAV11, DD13, DGT19, Dur15, Far14, GCVR17, GAB19, Har15, HZWW17, Hod19, Hof16, IM14, JLT+12, JY14, JW14, Kam19, KL08, KL15, KD18, KMK11, KKI0].

cryptography [KGO10, Kre13, KKD+18, KSH18a, KSH18b, Lam13, Lan11, LLLK10, Lin14b, LWL10a, Li1d12, LY14, MCN+18, MSH13, MD12a, MCO15, Mic10a, MHL18, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SAFA11, Sta11c, Sti11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YTL1a, YSC16, YX+18, YDH+15, YR11, YN19, ZKW+18, vDKS11, Che11, LZX10, Nac12, Con12b, Ful10, Gas13, Lwa12, Mei10, Mur10, Ter11].
cryptography-based [BOB13].


Cryptography [Gen13]. Cryptoprocessor [EHKSS19, GV14b, SWM+10].
cryptoscheme [SLX16]. Cryptosystem [CCT+14, KD19, LH10b, SZHY19, SWM+10, WSP+16, Zaj19, ACD18, AK14a, BS15, Chi13a, Gal13, GV14a, GLB+18, IB11,
LZ11, LYC^10, MM13, MG15, NZM10, SvT10, yYqWqZC13, YY11, YY13, sCR19a.

Cryptosystems [ADI11, CLND19, OTD10, PSM17, ZSP^+19, AHG18, AJYG18, AVAH18, BNST17, FWS13, SA16b, ZYM19].

Cryptovirology [YY17a]. CryptRndTest [DB16].

CryptRND [ADI11, CLND19, OTD10, PSM17, ZSP^+19, AHG18, AJYG18, AVAH18, BNST17, FWS13, SA16b, ZYM19].

CryptRndTest [DB16]. CS [LJ19]. Csec [ADI12]. CT [Dun12b, Kia11, Pie10]. CT-RSA [Dun12b, Kia11, Pie10]. CTRL [HKK19].

CTRL-FA [HKK19]. Cube [HIJ^+19, MS12b, YWM19]. Cubic [RW12, VM14]. Cuckoo [BHKN13, sCR19a].

CUDA [DLV16]. Cue [KT^+18].

Cue-based [KT^+18]. CUEAuth [KT^+18]. cultural [Mid10]. Culture [Bl12, SR14]. Currencies [TS16b].

Currency [AHWB20, DMO^+19, Cou12a]. Current [DP17, GCK12, FPBG14]. Curves [CG12b, DBPS12, DWWZ12, EAA^+16, GZHD12, KWS^+12, LJ17, LJ19, MCDB12, MKH^+12, PGLL10, RS16, SGS14, SRK^+17, SRK^+18, WSSO12, WK18, WY12, tWnCl12, YI14, YPR17].

CybSI [YK16]. Cycle [BG12, KU12, MKN13]. Cycle-Based [MKN13]. Cycles [BCTV17, WBA17, CLCZ10]. Cyclic [Che18, OTD10].

D [AM19, AP10, Bro19, CG12b, DBPS12, DWWZ12, EAA^+16, GZHD12, KWS^+12, LJ17, LJ19, MCDB12, MKH^+12, PGLL10, RS16, SGS14, SRK^+17, SRK^+18, WSSO12, WK18, WY12, tWnCl12, YI14, YPR17]. D-Based [WSSO12]. D-like [LJ15].

D-PUF [SRK^+17, SRK^+18]. D2D [Gop19, PSM^+18]. D2D-Aided [Gop19].


Darmstadt [FBM12, Sen10]. DASH [KCC17]. Data [AAA^+19, ARWK19, Ana13e, ADF12, Bar12, BJL16, BCD^+12, BJL12, BW12, BKLS18, CWL^+14, CMLS15, CCW^+10, CSV15, CCT^+14, CLW16, CDLW19, CHI^+19, DDS12, Dan12, DR12, DK16a, DMS^+16, DA12, DCA18, DLZ^+16b, Ebb09, EKOS19, EKB^+16, FMY15, FYD^+19, FPY15, FRS^+16, GKK11, GRRZ18, HSM14, HWZP18, HLC^+18, HLT^+15, HVP^+18, HXZ^+18, HK14b, IBM13a, KRHD13, KGV16, KP18, KD19, LPPY19, LLZ^+17, LLS19, LWJC14, LCP15, LLZ^+12, LZC^+12b, Ma17a, MLO17, Mal13, MMS17b, MJW^+18, MGJ19, MM14b, NNAM10, NR12, PV17, PDD14, PSM17, PZL^+19, PBC^+17, PH12b, PH16, PNRC17, PWS^+19b, QZL^+16a, QZZ18, RCP^+18, Rea16, RDK19, RSN14, SG18, SAKM16, Sar10b, SMIK18, SP15b, SKH17, Sia12, SC19a, SL10, SOL6, TCN^+17, TAN15a, VAI12, VSV15, WZCC18, WLDHL17, XNKG15, XSWS16, YDY^+16, YZDZ19, YJSL18, YMC^+17, ZXYL16, ZPXX17, ZTL15, ZLW^+17, AP10, AAH^+19].
data
[ASO14, AIM+19, Ana14, Ano11a, Ara13, ADH17, ALL+18, BLL+19, BC16, BHH19, BTPLST15, BC18, BCGS16, BKV13, BTK15, CD16a, CDGC12, CLH+16, CDF10, CDL18, DDY+19, DFJ+10, DTZZ12, DRD11, DYZ+15, DZC16, ED17, FS18, GHD19, Gen10, GSAMCA18, GLB+18, GZS+18, HKA+18, HSM13, HKA19, HWK+15, HL19, HK19, HMKC12, HH16, HYS18, HYF18, JKA+18, JLC18, JHCC14, KCS+18, Kim16, KV19b, KH18, KWH16, LSBN14, LT14b, LXK+14, LZY+16, LLL+17b, LLI17, LHL+18, LZWZ19, LFWS15, LAL+15, LCW+16, LZZ17, LLL+18, LLI16a, LHA+16, MHKS14, MRR+18, MSGCDPS18, NJB19, Nam19, OO18, OSSK16, OSANAM19, PPG19, PMG19a, PWS19a, PZ15, QCX18, QLZ19, RR16, RR17, SLL+19, Sch15c, SD17, SYY+16, SM19a, SM19b, SAR18b, SPK17, SWW+17, Tan17b, TMK11, TMT13, WLG11, WLI13, WMC17, WXMZ19, WDDZ19, WLS14, WZLW13, WS14, WS19, WL19, XXX15].

Data-Centric [DLZ+16b].
Data-Classifiers [LG16].
Data-Compression [DA12].
data-independent [BCGS16].
Data-Minimizing [BCCD+12].
Data-Oriented [NNAM10].
Database [BTHJ12, SBV14, WCL+18, AAH+19, BL11, JHCC14, LW13a, PBP19, PRZB12, SVGE14, Suc12, XMY+17, YXD18].
database-as-a-service [AAH+19].
Databases [ABL+18, FCM14, HPC10, JKHvY12, Kav15, RP12, WP17, GA11, JK13, LCY+16, SS17a, TG12].
datacenters [PRN+19].
Dataset [SP13].
datasets [LVRY10].
DATS [HVP+18].
Daubechies [Ara13, SM12, ST15].
Daunting [IBM13a].

David [RNQ16].
Day [MMB17, Zet14, Hof16].
Days [Bai12, Bri11].
DB [PYH+18].
DBDH [CW14b].
DBMS [SERF12].
DC [LHY12].
D-Net [LHY12].
DCT [BDB14, LP12, SS17b].
DDH [LZC12a].
DDoS [PSJ+13, SP15a].

De-synchronization [XNG+14, AATM18].
deadly [HLV10].
Dealing [Sha13, VN16].
Death [Moo14].
Debate [Bla16].
Debiasing [USH19].
Debs [Smii5b].

debugging [MFH13].
Decade [SOG15].

December [Abe10, BYL10, BC11, Che11, GG10, HWG10, LH10a, LW11a, LTW11, Yan10, Yan11].
Decentralization [JP19].
Decentralized [ABCL17, CD16b, GZZ+13, HSMY12, HK14b, MT17, PPS12a, PAS13b, RVH+16, RSN14, TS16b, XZT+19, YM19, HHBS18, SLL+19, WZC16].

Decentralizing [LW11b].
Deception [GA19, vdWEG18].
Deciding [CLCZ10, Sch12c].
Decipher [Cor14b].
Deciphering [Bla16, GMNS15, GSAV18].
decision [PKA15, RPG12].
Decisional [CCL+19, LZZ14].
Decisions [Bel18a, YWK10b].
declarations [HWYW14].
Declassified [ABJ13].

Decodable [Yek10].
decoder [PMG19a].
Decoding [DP12, GMNS15, Bax14, Bull0a].

Decomposition [AGH+17, LSL12b, gWpNyY+14, BWA13].
Decompression [PP10b, SHC+16].

Deconstructing [Tar10].
Decoupling [DMO+19, IM16].
decouplings [VSB+19].
decryptable [MBP19].
Decrypted [Kob10].
Decryption [CR12, Tay19].

Decryption [AN12, KB10, PKTK12, FNWL18, LHY17, LHY18, SES+16, SM10a, SM10b, Wu16, XZT+19, XYM19, ZSW+18b].

Dedicated [Lin17, Nac12, NSP+18, AKS19, RNQ16].
deductive [ABF+14].
Deduplication [CDTW19, MGJ19, QL17, SSK17, YDY+16, YZD19, ZHZ+19, KH18, SAR18b, ZFH+18].
Deep [BNMH17, CRS+18, DLGT19].
FGR+17, HCYZ18, Mor19b, RDK19, RHLK18, WYL18, ACMP19). default
[BMDT19]. defeated [Kap13]. defects
[FES10]. defences [NDNR13]. Defend
[Ano17e, FY19, Sch13]. Defending
[LWCJ14, YFT18]. Defense
[MPA+18, RCK17, YDV19, PSJ+13]. Defenses
[AN17]. Defensive
[Hel17a]. Defined
[KYEV+18, SAM+18]. definition
[LWL10a, WSD14, YXC+12]. Definitions
[BBDD19, GLW12, MAU12, CGKO11, KM14, KGO10, XWC14]. Degeneracy
[WH18]. degradation
[MMS+17a]. Degree
[CMRH17, KA18, LHW18]. degrees
[MZ17a]. Delay
[CCCK16, GMNS15, LFX+18, LBR12, MKK17, JLT+12, XW13, MCL+19].
Delegatable [WZ11, XLC+19]. Delegated
[MZH15, TMC15]. Delegation
[FMTR12, GLW12, SSW12, XWLJ16, YZ12, YM+15, JSMS17a, NAL17, XWS17, XZP+19, ZWM14]. Deletion
[DM+16, MGJ19, Real16]. Delfs
[Mur10]. Delivery
[PS+13, SSPC12]. demand
[KKJ+16, LWYM16]. demand-aware
[LWYM16]. Demodulation
[KOP12]. demonstrating
[LHA+16]. Demonstration
[KG19]. demosaicking
[HLC16]. Deniability
[TCS14]. Deniable
[DF11, zGXW12, HLLC11, GCH+19, HS11, Jia14b, JXLJ15, LXJ14]. Denial
[BKBK14]. Dense
[BFM12]. Density
[Ge19b, LC15, LQ11b]. density-based
[LQ11b]. Dependency
[MWES19, SG+12]. dependent
[GDM16, PKA15]. deployed
[MFH13, RY10]. Deployment
[BAA+19, WXK+17]. DepSky
[BCQ+13]. Depth
[GH11a, RS16, SS10b, SS12a].
Depth-
[GH11a, SS10b, SS12a].
Depth-Based
[RS16]. Derivation
[LBR12, Cha13a, Lau12]. Derivative
[LSQ11a]. Derivative-based
[LSQ11a]. derived
[JS18a, ZMM+10]. DES-like
[AGH18, CGCS12]. Description
[WH18, PCLG+11]. Design
[AMN18, Abc12, ARH+18b, AIB+16, ADD10, AUMT16, Bel18a, BKL+13, DZS+18, DHB16, DR11, FSK10, HSA14, JLZ18, JWJ+17, KPP16, KW14, KLT+17, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NRY+14, PC16, QLL17, RYY+13, Sch13, SAAB10, SZDL14, TH+13, VPI17, WKB16, WDKV19, YJC18, ZXH16, BBDP16, CZ14, DRN16, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MYH+18, OSANAM19, SVGE14, ZYC+17].
Designated
[WH17, HYWS11, RPSL10, SY15b].
Designated-verifier
[WHJ17]. Designation
[Che15, LSQL18b]. designed
[Goo12]. Designer
[KMY18]. Designing
[CDK+10, DZS+18, FLW12, MRT10, PSD15, SR10]. Designs
[BGK12, PCY+17, KDH15]. desynchronisation
[LDC13]. Detected
[LI16, ZPXX17]. Detect
[JWJ+17, NSA15, WOLP15, Lan11]. detectability
[LRW17]. Detectable
[Ess17]. Detecting
[BKBB14, CZ19, Ess17, GAS+16, HLW12, KW14, SH15, VCD16, YSC+15, LWWL11]. Detection
[AMKA17, ATS15, ARWK19, BEM16, CBO+18, DSB15, DF11, GN16, GZH17, HDHW12, HCYZ18, KU14, LGL+12, LC15, MKRM10, MKAA17, MKASJ18, NDC+13, NSMS14, SAJL16, SBV14, SXH+19, SP15a, SRAA17, SGS14, TLZ+17, TM18, YFT17, ZHS10, AKKY17, AOT13, BM13, CBYJ16, HBI13, JC13, JGD16, KKK+18b, KLC+10, LCD13, Maz13, MMF15, MHT+13, WYL13, vdWEG18].
Detective
[Cho10]. Detector
[LTP16]. Detector-Based
[LTP16]. determination
[JK19]. Determine
[FSWF11, Sto12]. Determining
[Bar19, NN12, Scr18]. Deterministic
[MPS12, NS12, XXZ12, DTZZ12].
Deterring [WGJT10]. DEUCE [YNQ15].
develop [Ham19]. Developed [Har16].
developers [Ano14c]. Developing [CH11].
Development [Pau10]. Developments [GCK12, Vai11].
Device [ADM19, ABCL17, CFXY17, DFKC17, HSUS11, KLM+12, SRK+17, SRK+18, TYK+12, ZSH+19, CRS13, GM16a, KKG14, Kim16, OSP+19, Par12b, SHBC9, YV19, XHI12].
Device-to-Device [ADM19]. Devices [AAC+16, ATCI17, BDM+19, CSH+18, CR+13, DLWW11, EGG+12, FMC19, GPT12, GdM16, GMSV14, HH+13, HDWH12, HFS+19, JMG+16, LFH18, LWHS17, LLD19, MFG16, May15, MS16, NVM+17, RC18, RSX18, RPHJ11, Sch15b, SFE10, SWF+19, VWC19, WKB16, WIT10b, XJR+17, Aia15, BMD19, CLP+13b, CFI13, CTL12, Chi13a, FRT13, GTSS19, HFF16, IB11, KPP16, LKAT12, Mo11, MHV15, NSBM17, OYHSB14, PCK19, SNS15, SCR19b, SHBC9, TZTC16, TG17, Wan18b, ZP+16]. DFA [PD+19, WH17].
DFA-Resistant [WH17]. DFT [DFDR13].
DHA [AKY13]. DHA-256 [AKY13].
DHTs [YKG13]. Diagram [WGD18].
dickory [NN15]. dictionaries [ABR15].
Difference [BS14, YTP11, JK13]. differences [LHM13].
Differencing [LyWZ12, YWW10].
Different [GZ12, HHH+13, KU12, AKK+17, AB1O].
Differential [BMS12, Bar16, BNY14, CWP12, CGCS12, DMSD18, ESS15, FXP+17, KWS+12, LYK19, LGL+12, LJJ16, LJJ15, LYH14, MSS17, MRTV12, PH12a, QGGL13, RCP+18, SBM15, Sun11, URK+19, WHN+12, Bk15, DDFR13, GLMS18, LLLK10, MNP12, PBCC14, SDM10, SDM14, TSL11, TS16a, WYL14].
Differential-linear [DMSD18].
Differentially [RCBK19]. Differentials [WW12]. Differentiation [Sod13].
Differing [GGHW17]. Differing-Inputs [GGHW17]. Diffie [LZCI4, ABD+15, ABD+19, Chi16, FHLOJR18, Hof16, HLCL11, HLYS14, LNL+19, Orn16, RH10].
Digit [MH16, KWH16]. Digital [AAA+19, AYS15, BBC+13, BM13, BCP14a, FMS12a, FR15, GP17, HPO+15, Jin10, Joh10, JL16, LWC+12b, MBF+13, MS10, MM12, MHMSGH16, NC12, pNyWy1+14, Orn16, PH12b, PAS13b, RCK17, SA15, SM13, Sod13, SC12, SOS15, TC11, TAP19, TS16b, Yon11, Y+17, YLS12, dRSdVC12, AGHP14, BP10, Bao19, CCG10, Cia18, FLZ+12, Fri10a, GMS11, Har14, HAGTDF13, KM11, Lan13, LWG10, MS13b, MM14a, MO14, Pau19, QCX18, Sim15b, SLIM10, yWpNyL11, ZZZA17, Zet14, ZSMS18, Ano13c, Ano15b, Mon15].
Dilly [Bat10]. Dimensional [Ano17d, LLY+18, LWC+12b, XYYX11, XLP+18, DWZ12, HZW19, LZW19, QD16].
dimensions [Pal15]. direct [GH12].
Directed [NLLI12, KPS10]. Direction [NS12]. Directional [JS18a]. Directions [BKBK14, CDFZ16, Hof16, PPA18].
Directly [LZCI2a]. directory [SMB10].
Disability [Sod13]. disabled [HFT16].
disassociation [TMLS12]. Disaster [NRRQ15, BBG+17]. Disclosure [GR19a, SYv+19, DZS+12, FKA15, SB17, WGJ10, ZZC7]. discourse [Hel17a].
Discovery [MJW+18, MJS+19, Ano11a, MPM19].
Discrete [BGGT14, CLL16, HKR+18, KLM+12, SRT12, Xic12a, Xic12b, AMORH13, BGJT13, BGG+19, MM13, Mes15, ST15, TPL16, VM14].
Discrete-Continuous [SRT12].
derimization [GPVCbRO12].
Discriminative [DLGT19, Y14].
Discussion [Gli12, Will8, Bul10a].

emerged [McG11]. Emergence [LMB12].
Emergency
[HLKL15, YTH17, BDM+19, KLC+10].
Emerging [BSV12, KSA16, OS16, FPBG14,
GLL16, ZHH+17]. emphasis [GMT+12].
Empirical [wPnY+14, EBFK13, Sar14].
Employees [Mor12]. Employing [LGLK17].
EMV [Cho10]. Enable [SMS14].
Enabled [GPT12, HFT16, KV18, QZL+16a, QZL+16b,
SG12, SGC16, SSC12, YSF+18, BMM12,
JZU+19, NML19, TODQ18, YFT18].
Enabled/disabled [HFT16]. Enables [IBM13a].
Enabling [FRS+16, GYW+19, JSM+18, PSM+18,
SSY12, WPZM16, YYS+16, MMP19, Sch12b].
eNB [CLM+12]. Encapsulation [KG19].
Enciphering [CMLRHS13, HMR12, MLCH10, MKASJ18, Sar11].
Enclaves [WBA17]. Encoded [DG17, HS18].
encoder [PMG19a]. Encoding
[BR14, CK18, SK12a, TJZF12, XHX+17,
CJL16, PC14, SM19a, Sun16].
Encounter [NA10a]. Encrypt [RAZS15, Ran14].

Encrypted [ADR18, BTHJ12, BSA+19, CWL+14,
CWL16, Cor14a, CdLW19, CHH+19, DWB12, DCA18, FGRQ18, FCM14,
FRS+16, Fyo19, Gen13, GLG12, GKG19,
GZH17, GYW+19, HWZP18, HTZ12,
HB17, HCDM12, IMB17, IBM13a, JSCM17,
Kaw15, KGV16, LA15, LGKL17, LQD+16,
Lof12, Mur16, NBZP17, NNAM10, PBC+17,
QLL10, Roh19, SAKM16, SzyH19, Sia12,
SOR16, TM18, Uto13, Vai12, WBC+10,
XWSW16, YDY+16, ZDL12, ZXY16,
ZVG16, ZLW+17, ACMP19, AAH+19,
AHM+18, AZH11, BBDP16, BTPLST15,
BGP+17, BKV13, BTK15, BL11, CH11,
Crl16, CDL18, DDD+19, DKL+16, DRD11,
DJ19, EM19, ED17, FTV+10, Gen10,
GSAMCA18, GZS+18, GSGM16, HKA19,
HH16, JLC18, KH18, LKX+14, LZY+16,
LHL+18, LZW19, LW13a, MRR+18,
NJB19, OSSK16, PWS19a, PBP19, PRZB12,
SG19a, Sch16b, SEXY18, SM19b, SWW+17,
Suc12, TKMZ13, WR15, WS19, WL19,
XMY+17, XYW+18, Yaa19, YXD18].
encrypted [YQQL17, YQZ+19, YJC18,
ZLY10, ZZZC17, ZFH+18, ZHT16, ZZL+19].
Encryption [CC10, Mar10c, dRSdVC12,
Cla18, LGFCGCRP14, Pow14]. Encryption
[ADM12, AV12, AUC18, AHE17, Al012,
AAC+16, APE18, Anol3e, Anol4b, Anol5c,
Anol7d, Arm19, AKP12, ABF12, AS16,
AG18, BVS+13, BWLA16, BPR14a,
BPR14b, Bel16, BDOZ11, BWR12a, BS14,
BV18, Bla16, BKLS12, BDPS12, BLJP14,
BDMLN16, Boy13, BV11, BV14, BGV14,
CVM14, CMO+16, CMLL16, CWWL12, CN12,
CFZ12, CLHC12, Che15, Che18, CGL+12,
Chl12, Chl16, CRE+12, Con18, CNT12,
CLW16, CD16b, DR10, DN12, DFJ+10,
DSL18, Des10b, DGFH18, DOS15, Dun12a,
DF11, EAA12, ESS12, FHII10b, FHR14,
FJHJ12, Fei19, FFL12, Fuc11, GWWC15,
GGH+16a, GGHW17, GM13a, GZZ+13,
GWS+16, GH11a, GH11b, GHS12, GHPS12,
GDCC16, GWVL2, GVW15, GM14, GL12,
GKS17, Gnc16, HSMY12, HLLG18, HZ11,
HG12, HWS+19, Hor19, HC17, HTC+15,
HLH19, HP12, Int19, IAD10, JLS12, JSA17,
JLH12]. Encryption
[Jia14a, JR14, Kam13, KB10, KME+12,
KMY18, KTT12, KOS16, KKA15, KFOS12,
KHP16, KKK+18a, KMJ18, KS12,
KHGR19, LMGC17, LMG+18, Lau17,
Led16, LLSW16, LLPY19, LW11b, LW11c,
LW12, LJLC12, LYZ+13, LHL+14, LLC+15,
LTY16, LLL17a, LFX+18, LLLH18,
LSL15, LH11c, LSQ18b, LWZ19, LB13,
LY15, LW16, LYY+16b, LATV17, LML12,
LHL18, MZHY15, MLO17, MNP14, MR14a,
MTY11, MSM18a, MVVR12, MMS17b,
MSR+17, MRL+18, MBF18, MPRS12,
MZLS18, Mor19b, MT12, MKRM10, MSas12,
Nac16, NdMMW16, NTY12, NMS14,
NAL17, OT12, OGK+15, ODSS17, PMZ13,
PR12, PB12, PDNH15, PRGSAC19, Per13,
PKTK12, PPS12a, PYS18, PMZ12, PCY+17, PRSV17, PWS+19b, RVH+16, RCP+18, RZZ+15, RM18, RSSBGN12, RDZ+16, RVRSCM12, Roh19, SGG18, Saa2a, SSW12, SERF12, Sar10b, SJ19, Sch15a, SLGZ12, SXH+19, SZZ14, She14, SWF+19, Smi11b].

**Encryption**

[Sta12, SGH15, SMOP15, Tan11, TCN+17, TCI15, TMC15, Tan17b, TDT13, TKR14, TT12, TFS19, Unr15, Vai11, VSR12, VOG15, Wal18, WHC+15, WP17, WDC18, WSS12, Wat12, WLC12, WDD12, WZ15, WHLH17, WWHL12, WMS+12, WQZ+16, WZCH19, XNK15, XY18, XXZ12, XJWW13, XWLJ16, XJW+16, XHX+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC+11, YPK+12, YCZY12, YKKL12, ZOC10, Zaj19, ZPM+15, ZZQ+19, ZDL12, ZYT13, ZWTM15, ZQQ15, ZM16, ZZM17, ZY19, ZHX15, ZY11a, ZYM18, ZWS+18, ZYH+19, ZIH+19, ABC+18, AHS14, AASSA18, ATKH+17, AKKY17, Ana14, Ang16, Ano13d, Aro15e, Aro16h, ARG19, ABR12, AMHJ10, ACD+15, AHI+12, BLL+19, BAAS13, BZD16a, BC18, BKR19, BG14, BSW12, BGP+17, BTK15, Bro19, CPT18, CFVP16, CFZ+10, CW14b, CLH+16, CMM17, CLC+19, CXWT19, C2z15b, CS11, Chm10, CW12a, CJW+19, CDF+10].

**encryption** [CM13, CGKO11, DLZ16a, DDM17, DTZZ12, DMD18, Eve12, Eve16, FAA+18, FH13, FSWG11, FSWG12, FMB+18, Fay16, GMOGCCC15, GH13, GPSPS13, GLM+16, GH12, GLL+18, GZX19, HGWW11, HQZH14, HZL18, HKA19, HWDL16, HZWS18, HL19, Hel17a, HT13, HLR11, HK19, HL11, HYL+19, HFT16, HTC17, HYS18, HYF18, HHA19, HKHK13, JZU+19, JCHS16, JCL+18, Jia14b, JSMG18a, JSMG18b, JC1CC14, JSM+18, KAM16, KHM13, KKM+14, KV19b, LLW16, LCL+17a, LGP19, LCL+15, LFZ+17, LWW+19, LCT+14, LFWS15, LLM+19, LPdS10, LHH11, LW10, LK10, LW13b, LZZ14, LPZJ15, LCY+16, LCC17, LJJ+17, LJSW18, LL16a, LW13c, LSC12, LG19, MBP19, Mar12, Mar10b, MMS17c, Mes15, MML16, Mid10, Mon13, MSa13, NES+14, Nam19, OPHC16, OSNZ19, PPA18, Pet12, PBP19, QRW+18, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, SSL+19, Sar11, SYL13, SE14, SE16, SH11, SM11].

**encryption** [SNM14, SLZ12, SY15b, Sha13, SGFRCM+18, SLM10, SKB+17, Spa16, SGP+17, SGM16, Tan15, TPL16, jT12b, WGG10, WY10, WYYZ11, WYYW11, WLG11, WHY+12, WDLZ13, WZC16, WLFX17, Wan18a, WM19, WDG19, WDZ19, WGZ+12, WLS14, WCCH18, WXXW16, WXW14, XSWC10, XXX15, XS17, XZP+19, XWZ+18, XTZ+19, XLC+19, YWJ+19, YT11b, yYqWqZC13, Yan14, YTZ17, YHM18, YSQM19, YWW+19, YCT15, YJC18, YLZ+16, YLL10, ZCQ19, ZAA17, ZWQ+11, ZZ11, ZLW+12, ZJX+14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZYC+17, ZGL+18a, ZCL+19, ZWY+19, ZZ12, ZL12, ZDW+16, ZY17b, ZCZ+19, Zhi13, Wan14, GMdFPLC17, LAL+15, Sar18a, Kat13].

**Encryption-based**

[SERF12, BC18, XWZ+18].

**Encryption/Decryption** [KB10].

**Encryptions**

[ZXGW12, LG12, SL16+16, RD17].

**Encyclopedia** [vTJ11].

**End**

[Ano15c, BRR+15, BGP+17, CFE16, Chn16, MMHMSG16, RST15a, RST15b, Bel18b, Bro12, Chi13a, EM19, JZU+19, Wan18b, Zor12].

**end-devices** [Wan18b].

**End-to-End**

[CFE16, MMHMSG16, RST15a, RST15b, Ano15c, BRR+15, BGP+17, EM19, JZU+19].

**endomorphism** [FWS13].

**Endomorphisms** [AK14b, LGH+17].

**Endurance** [JSA17].

**Endurance-Aware** [JSA17].

**enemies** [Fag17].

**Enemy**
Extruded [CJFH14].

**Feature**
- [ERLM16, SRRM18, SM13, Tox14].
- [F2654hD4 Ber16a, F5 [LLY+12b].
- [Fa FMS12a]. Fabric [BHH19], fabricating [WW13]. Fabrication [VDB+16].
- Fabrication-Induced [VDB+16]. Face [AQR12, MHV+19, RSX18, XHH12]. Facial [KRB12, TCM19, WSS+19]. facilitate [Chi13a]. Facsimile [Ano16e]. facto
- [EM19]. Factor
- [AMSPL19, ATC17, HXC+11, LLC11, PSSK19, AIB+16, BD18, CLP+13b, CNF+18, DRN16, DMWS12, ED19, GMMJ11, HC12, IC17, JKL+16, JMW+16, Kem11, LNK+18a, LNK+18b, LW19, Lit14, MDHM18, NMX15, SNG+17, WW14, Wat14a]. Factoring
- [APPV15, KV19a, LLML12, BGG+19, MM13, SD17].
- Factorization
- [Coul12b, FS15, HWS+19, KKK+18a, KFL+10, Kuz11, YAM+15, Mes15, TPL16]. factors
- [HK17]. failed [And19]. Failing
- [Cer14]. Fails
- [ABD+15, ABD+19]. Failure
- [WCL+18]. Fair [ALR13, CSV15, DSM14, DG15, WSA15, SEXY18]. Fair-Exchange [DG15].
- Fairness
- [ALR13, Ash14, GHKL11, Wag16, MV16b].
- Fake
- [KU14]. Fallen [HCLPS12]. False
- [LLZ+12, MWES19, CDG12]. Families
- [BSS+13, KU12, FK19]. Family
- [ARH+18b, BMS12, BKST18, CBX19, DGIS12, DJG+15, FLS+10, FFL12, GN12L, LYY+18b, MFG16, SBM15, YCL17, BDPV12]. Famin [SS12a]. Fast
- [BLAN16, Bru12, CHS15, DLSB18, DGK18, GS+16, HMKG19, JGP+18, Khl18, LGLK17, NR12, PRSV17, Roz19, Rom11, SRRM18, WHZ12, WBA17, WQZ+13, ZHW+16, FHTH10a, KHM13, LNNH13, MB11, YML18].
- FastAD [SMB10]. Faster
- [CN12, EZW18, FHLOR18, HVL17, TH16, ZSP+19, Ant14]. Fault
- [AMKA17, BMS12, BB+16a, FXP+17, GST12, JWJ+17, JKP12, JTK12a, LYK19, LGL+12, LCLW17, LGL+12, MSS17, MKRM10, MKAA17, PH12a, RZZ+15, SBM15, SEY14, WCD19, YGD+17, BEM16, BBBP13, PCBC14, WMYR16]. Fault-Based [BBB+16a]. fault-resistant [PCBC14]. Fault-Tolerant [WCD19, WMYR16]. Faults
- [EFDT18, SBM15]. Faulty
- [LYY+16]. FBAC
- [YWJ+19]. FBI [Bha16]. FC
- [DDS12, Dan12]. FCMDT [BSBG19]. FDM [BD18]. FEAD [ZWM14].
- Feasibility
- [AAC+16, FKS+13, OMPS1+19, WHC+15]. Feature
- [Ber18, SGP+12, YKA16, ZWWW17, FTV+10, GJ13, HZW19, MHT+13].
- Feature-Based [ZWWW17]. Features
- [MHW+19, Y14, ZTL15, AAL19, FNP+15, JS18a, LCM+17, LTC+15a, NMX15]. Feauveau
- [Ara13]. February
- [Ano10a, DSD12, Dan12, Doultry12, Kua11, Lin14b]. FedCohesion [CCFM12]. Federated
- [BS13b, CCFM12, CSS+14, MJW+18, SAM+19a, BMB10, BSBG19, J11, TODQ18]. federated-IoT-enabled
- [TODQ18]. Federation
- [SS10a, NB13]. federations
- [MMS+17a, MLM16]. Feedback
- [HZ11, Hey17, PYM+15, SKGY14, ZH15, LWK11]. Feedback-Based
- [PYM+15]. FEIPS
- [DG15]. Feistel
- [BFMT16, KD15, Sasa12, SEHK12]. Felten
- [Ano16a]. FESSD [LGL17]. Few
- [SBM15]. FHE
- [CK18]. FHE-Based [CK18]. FHS
- [SP15a]. fi [BMDT19, YNR12a]. FIB [YNR12a]. Fiat
- [BSD+13]. Fibonacci
- [FM15, LLP+18]. Fibonacci-number
- [LLP+18]. Fidelity
- [BCP14a]. Field
- [Alz19, CLF+17, GHPS13, GM16b, HSA14, SS12a, TGC16, ZAG19, EAB+19]. Fields
- [ARH14, BGJT14, HVL17, NR15, ZL19, AA14, BGJT13, C15a, LBOX12, Oz11].
- Fight
- [Ano16f, Wu16]. File
- [DMS+16, LY16, TLF16, XZL+19, ZGC16, FLYL16b, GSGM16, VSB+19, YHHM18].
**FOX** [LJF16]. **FPGA**
[AMKA17, Ang16, BCE+10, BYDC19, BDGH15, CFZ+10, CHS15, EAAAI19, GFBF12, HJ19, HF14b, LLD19, MM14a, MAK+12, RJV+18, TV19, YTL+16, ZLQ15].
**FPGA-Based** [RJV+18]. **FPGA/ASIC** [CFZ+10]. **FPGAs**
[DGP10, GT19, RHLK18, SMOP15, VMV15].
**Fractal** [JTZ+16, KM11].
**fraction** [IK15].
**fractional** [BW13, VM14].
**Fragile**
[AAA+19, CHHW12, MCDB12, SSA13, WK18, ZHS10, CCLL11, PGLL10, WHZ12].
**fragment** [BPP10].
**Fragmentation** [BDPS12, CDF10].
**frame** [FMB+18, YQH12].
**Franchise** [BBM15, KAHKB17, LTKP16, LWCJ14, TC10, CJP12, CJP15, EA12, NLYY12].
**Friendly** [RBNB15].
**Fresnelet** [FMB+18].
**Friendly** [FRA16, KCC17, SZDL14, ACM12, BP18, FK19, KLW+16, RD17, WOL12].
**Frontside** [DDR+16]. **FSR** [MD12b].
**FSR-Based** [MD12b]. **Fugue** [AP11].
**Fujisaki** [TFS19].
**full-hiding** [DDM17].
**full-text** [SWW+17].
**Fully** [AKP12, BV11, BV14, BGV14, CMO+16, CN12, CFZ12, CNT12, DOS15, GH11a, GH11b, GHS12, LLC11, KKK+18a, LMGC17, LSLW15, LJY16, LATV17, LSC12, MV12, MS18a, Nc16, NCCG13, PB12, SGH15, VAI11, VV19, WHC+15, XWZ+18, ZZ12, DDL15, GH13, MBP19, ZX+14, ZML17].
**Fully-Homomorphic** [GH11b].
**Fully-Homomorphic-Encryption** [CN12].
**Fun** [APPVP15].
**Function**
[AMPH14, Bee17, BKST18, BBL19, CJZ13, FLS+10, GKI18, GKY18, LJT19, LyWZZ12, MMS17b, RJV+18, SGGY11, WSO12, YW+19, AKY13, ABO+17, AP11, Bar19, BDPV12, CMSM17, Con17, CL14, LP11, RS14, Sar11, SXL16, SCBL16, TQL+14, WYW14].
**Function-based** [YW+19].
**Functionalities** [JR13].
**Fundamentals** [Joh10].
**Fusion** [ABCL17, YYK+17, HW19].
**Future** [AYS15, BCE+12, BKBK14, Bon12, BLU+15, BKP12, BHT18, BK12a, CCL+19, CPS16, D5MM14, DQFL12, FY11, LVV11, NBS15, NR12, RJA12, RW12, SMS14, SL+16, Tan12a, WFXZ17, YTP11, AY14a, BD11, BDK16, BCG16, CGL12b, CQX18, CW12a, ESR14, Gen10, HRV10, HL12, Kom18, Li10, QZD16, WT13].
**Fundamentals** [Joh10].
**Further**
[HCL+14, WHY+12].
**Fusion** [FMS12a].
**Fusion** [ACZ16, ALR13, BBC+14, BKIK14, BKPW12, BHT18, BK12a, CCL+19, CPS16, D5SM14, DQFL12, FY11, LVV11, NBS15, NR12, RJA12, RW12, SMS14, SL+16, Tan12a, WFXZ17, YTP11, AY14a, BD11, BDK16, BCG16, CGL12b, CQX18, CW12a, ESR14, Gen10, HRV10, HL12, Kom18, Li10, QZD16, WT13].
**fundamental** [Bre18].
**Fus** [FMS12a].
**Future** [AYS15, BCE+12, BKBK14, Bon12, BLU+15, CDFZ16, Fri13, GCK12, HY18, KH+11, Mon13, SG19b, AP18, Ano13f, Dya19, ...

H.264 [JSZS12, JHNN12, LLHS12, LW13c, MU12, WDDW12, ZLDD12, ZLDD14].

H.264/AVC [JSZS12, JHNN12, LW13c].

H.264/SVC [MU12, WDDW12, ZLDD12, ZLDD14].
[Keb15, Mac14]. **heroine** [Fag17]. **Hess** [HP17]. **Hess-Like** [HP17]. **Heterogeneous** [KS18a, SP15b, YZDZ19, AIC18, ABB19a, SZMK13, SCKH10, SHC+16]. **Heuristic** [BGJT14]. **Heuristics** [SKE+18, KO14]. **HEVC** [DG17, GKSB17]. **HIBE** [LW11c, LSQX19]. **Hickory** [NN15]. **Hidden** [FMS12b, PSS+13, YLL+12, ZYT13, ZYY19, BDK11, LCL+17a, Sch15c, Smi15a, XZP+19]. **Hiding** [AAA+19, DCA18, GGH+16b, GL10, JHHN12, KD19, MK12b, OT12, XLM+12, XGLM14, XZLW15, Ara13, DDM17, HZL18, KWH16, LXLY12, LT14b, SM19a, UUN11, WLH13, WZLW13, ZWM14]. **Hierarchical** [ADM12, BSSV12, DBT19, FSX12a, LSLW15, LHW18, NMS14, NLY15, OT12, SSA18, WLG11, WYML16, WHLH17, ZMW16, ZHY+16, ZYH19, DSCS12, HYS18, JCL+18, KPB17, LFZ+17, NLM10, RG10, SE14, SE16, WZY11]. **Hierarchies** [DMM10]. **Hierarchy** [NA10b, VN16]. **High** [AW17, ASBD16, Ano17d, ARM15b, Bar15, BDL+11, CLB19, DM15, DG17, FHL19, FYD+19, GL12, GCS+13, HMKG19, HZ11, KFE19, KMP+11, KPC+16, KAK18, LTKP16, LCK11, LLY+18, LPO+17, MS13b, MS13c, MM17b, MSR+17, PCKP14, WYC14, WL11, XNRG15, XL+18, AHG18, ABBD13, GZHD12, GCVR17, JLC18, KL13, MAK+12, PABC+19, RS17c, WLH13, WXL16, WZLW13, WKL11]. **High-Assurance** [Bar15, KMP+11, WL11]. **high-capacity** [GZHD12]. **High-Dimensional** [Ano17d, XL+18]. **High-Efficiency** [DG17]. **High-Impact** [DM15]. **High-Level** [AW17, KPC+16, ABBD13]. **High-Order** [FYD+19]. **High-Performance** [GCS+13, KAK18, LPO+17, CLB19, FHL19, AHG18, GCVR17, PABC+19]. **High-Rate** [PCPK14]. **High-Security** [WYCF14, BDL+11]. **High-Speed** [ARM15b, HZ11, LTKP16, MSR+17, BDL+11, KFE19, KL13]. **High-Throughput** [HMKG19, MAK+12]. **Higher** [LWK12, PRC12, gWpNyY+14, ZSW+12, LWKP14]. **Higher-Order** [LWK12, PRC12, ZSW+12, gWpNyY+14, LWKP14]. **Highly** [CD16a, SZDL14, SC19b, ACD+15, DT13]. **HIGHT** [CWP12, WWBC14]. **HiiMap** [HEP+11]. **hijacking** [BCFK15, DCAT12]. **HILL** [KPW13, KA17]. **HIMMO** [GMRT+15]. **himself** [Pro15]. **Hindering** [BTPST15]. **HISS** [DT13]. **histogram** [CSS+13, Lin14a]. **Historians** [Cer14]. **Historical** [Hai17, Han12]. **History** [ABJ13, Ano19b, Cer14, Cop10a, Hel17a, LT14b, Mc10, Mc11, SE16, Smi15a]. **history-free** [SE16]. **Hitler** [Hea15, Moo14]. **hitting** [GR19b]. **HIV** [GSGM16]. **HAMAC** [GW16, MAK+12, YGS+17]. **HAMAC-DRBG** [YGS+17]. **HAMAC-SHA256** [GW16]. **Hoc** [LH12, PD14, She14, SS15, XHC+12, BBB19, KM10b, LXJ14, PY19, SGGR+16, WXSH19]. **Hoffstein** [Mei10]. **HOL4** [HK14a]. **Holden** [Ano17b]. **Hole** [Ano15d, BKKV10, PC16, YKA16]. **Holocaust** [Han12]. **holy** [Wat15, Mic10a]. **Home** [BD18, HXHP17, KH11, KPP16, SXW19, Cor14a]. **Homes** [VJH+18]. **Homogeneous** [HT11]. **Homomorphic** [AAUC18, AKP12, BV11, BV14, BGV14, CMO+16, CN12, CJ13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHPS12, GHY18, KOS16, KGV16, Kim15, KKK+18a, KRHRG19, Laur17, LCLL15, LATV17, MLO17, MSM18a, MSR+17, MRL+18, MBF18, Mor19b, Nas16, ÔDDS17, PTK12, RCP+18, RMZW19, Roh19, RJ+18, Tan15b, Vai11, WHC+15, WCXZ17, XWZ+18, AKKY17, BDOZ11, BC18, CJXX19, CW12a, DMD18, GH13, GHPS13, GLM+16, LLW16, MBP19, SEXY18, Tam15,
WSC14, YJC18, ZXJ+14, ZYC+17.

Homomorphically [SG19a].


hostile [CDA14]. HotCalls [WBA17].

House [Ano16j, Bla16]. HP [CGB+10].

HPC [KV19b]. Hromkovic [Gas13].

HTTP [BHCdFR12]. Huang [LLSW16].

Human [Sun16]. Hui [FMS12a]. Hui-Yuan [FMS12a].

Humans [RBNB15, LKKL13, der10].

human [THA+13, LKKL13, der10]. hosted [SG19a].

hostile [CDA14]. HotCalls [WBA17].

House [Ano16j, Bla16]. HP [CGB+10].

HPC [KV19b]. Hromkovic [Gas13].

HTTP [BHCdFR12]. Huang [LLSW16].

Huffman [Sun16]. Hui [FMS12a]. Hui-Yuan [FMS12a].

Human [HHS+15, HWZZ19, IA15, DMT12, HZW19, HW19, LWW+10, PYH+18]. Humans [RBNB15, RB17].

Hummingbird [ESS12].

Hummingbird- [ESS12]. hunt [Bha16].


Hybrid [ADI11, ARM15b, JLZ18, JHW+19, KBL11, KKA15, LP12, LLD19, MMBS19, NGAuHQ16, OOI2, Per13, RCBBK9, SGG18, SRT12, XWLJ16, Zaj19, SAM+19a, AM19, BYDC19, EEAZ13, KP18, WXLY16, WS14, XWS17, BOB13].

Hybrid-Double [ARM15b].

hybrid-indexed [WXLY16]. hybridization [MMSD13].

Hyderabad [GG10]. Hyper [BL14, KO14, LZXK19, WGZ+12].

Hyper-and-elliptic-curve [BL14].

hyper-chaotic [WGZ+12].

Hyper-heuristics [KÖ14]. Hyperchaotic [GMOGCC15]. hyperelliptic [FWS3, Kre13].

hypergeometric [YL11].

Hyperledger [BHH19]. HyPoRes [MBBS19].


IBC [BOB13]. IBC-HWMP [BOB13].

IBM [ABC+12, ACD+15, BAB+13, HKL+14, JSM+18]. ICA [tWMcC12].

ICICTA [IEE11a]. ICISC [LH0a].

ICISSP [Ano19a]. ICN [CHL19]. ICs [GSFT16]. ID

[Ano17c, CTL13, CDPLCA16, EZ15, HCC10, IB11, KGO10, LGMC17, LY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, Rom11, TPL16, TT12, TTH15, Wan18a, WZD19, WT10b, WT12, HWZZ19].

ID-based [MM12, LGMC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18a, WZD19, WT12].

ID-card [Ano17c]. ID2S [YRT+16]. IDEA [BNY14]. Ideal [LPO+17, MCL18, HKT11, yYqWqZC13].

idealness [TD14]. Ideas [FREP17, Mac12].

ideompotent [Dur15]. Identical [Bow11].

Identifiable [Oba11]. Identification [CZCD18, FSX12b, FSX12c, FSX12a, HWZZ19, KGP+19, VGA15, YGFL15, YKK18, AGLW16, BOP14, CTHP13, CJP12, CJP15, DJ19, EA12, HQY+16, HL19, KI11, KL13, NLYZ12, WYZ+17, YTM+14, ZAAAB7].

identified [AZH11]. Identifier [LHW18, GSGM16, MJS13]. identifiers [Cer18].

Identifying [Bel18b, CZ19, CSV15, SVG16, ZCWS15, CAM19]. Identities [KHN+11, LBC18, GML+11].

Identity [AHN+18, AQR+12, ASM12, ASVE13, Ano15b, ACAP+15, ASS15, BWLA16, BCF16, BHG12, BKF12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CZLC12a, CZLC12b, CLHC12, CLHC14, CLND19, CGL+12, CGY+13, Chi12, dCASS+12, Fan19, FHH10b, FZT14, FR15, FSX12b, FSX12a, FSX12b, GOPB12, GR19a, GLa11, GY13, GDC16, GJJ15, GJZ17, HZC+12, HvS12, HSM13, HSM14, HXZ15, HYWS11, HYF18, JGP+18, KKA14, KRB12, Kuz11, LMG+18, LYS+19, LMB12, LSL12a, LKAT12, LXJ14, LLC+15, LTZY16, LSLW15, LH11c, LSC12, LBR12, MLO17, MHW+19, MBF+13, MJGS12, MJW+18, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SG12, SS10b, SS12a, SAAB10, Sch11, Ser12, SXH+19, SPPC12, SKGY14,
Identity

[WER19, XZ12, XQ11, XJW16, YZX12, YTM14, Yon11, YHK10, YKC11, YFF12, YCY12, ZLH12, ZM16, YZZ19, ZDW16, ZPXX17, ZMY18, ZYY19, ZT12, vWEG18, ATKH17, An13f, BMBS10, BOB13, BS19, BMM12, BBG12, CTHP12, dCCS16, DZ14, Dn10, DW12, FA14b, GMRT15, GR19, GPCdBR12, HP19, HZC14, HDDL16, HZWW17, HLR11, HFCR13, HWB10, HW12, HL11, HP10, Hwa11, JCL18, JZS10, KKGK10, KKM13, KL11, LKK13, LK12, LXWM12, LCT14, MMS17a, MD15, MGP10, MJS13, ML16, MM13, NCL13, NML19, O11, P19, PLGS11, QYWX16, RG10, Rom12, SSY12, SE14, SE16, SR10, hS15, SA16b, Sim15b, SDA11, SSS11, SG16, VGL14, WWZ11, WWY11, WSC14, WLFX17, WM17, Wan18b, WX19, WHZ19, Wat14b, WWW17, XW12, XCL13, XHM14, YW17, YW19, yWqZC13, YX16, YMSH10, YKC12, YX16, YNX16, ZMY17, ZZ12, ZYM19.

Identity [LZX10, P10, Sar18a, Kat13].

Identity-as-a-Service [VFF19].

Identity-authentication [NML19].

Identity-Based [ASS15, BWLA16, BHG12, BKP12, CZL12a, CZL12b, CZL14, CL19, CGL12, CGY13, Ch12, FHH10b, FZ14, FR15, FSX12b, FSX12c, FSX12a, GY13, GJ15, GJ17, HZC12, HSM14, HZX15, LGM18, LY19, LSL12a, LCC15, LT16, LSL15, LH11c, LSC25, LBR12, MLO17, RD12, SH15, TK14, TFS19, Wan14, WZC19, XZ12, XJW16, YZX12, YHK10, YKC11, YFF12, YCY12, ZL12, ZM16, YZZ19, ZPXX17, ZY18, CSZ11, HSM13, HYW51, HYF18, KAT12, LXJ14, MJGS12, RS15, SXH19, SWW16, Tia15, TH16, ZDW16, BOB13, BMM12, CTHP13, DZ14, F14b, GMRT15, HZC14, HDDL16, HZWW17, HLR11, HW10, HW12, HL11, HPY10, Hwa11, JCL18, LK12, LCT14, MJS13, MM13, NCL13, PZ19, QYWX16, RG10, SE14, SE16, hS15, SA16b, SS11, SG16, WLFX17, XW12, XCL13, YW17, yYqZC13, YK12, YX16, ZZ12, ZYM19, LZX10, Kat13].

Identity-Enabled [S12].

Identity-Hidden [PSS13].

Identity-Preserving [MHW19].


IEEE802.16e [HLC11].

if [ABJ13, Pec17, Rus15]. IFIP [GLC10]. IFP [MM12]. IFTTT [BD18]. Igor [S10]. II [Mun17, SCPS110b, SOP15, ZVS18].


Illustrated [Cop10a]. Im [BG10, BGI12]. IMA [Che11]. IMACC [Che11]. Image [BS11, Bai10, BAA13, BDB14, BWR12a, CJFH14, CCC19, DA10, DCM18, DS19, GRRZ18, HD19, IAD10, JKeY12, KPS10, KLC19, LA15, LLL17a, LFX18, LLLL18, LZX19, MBC15, MAL10, MSM18b, PW10, QJC18, RS16, RVRCM12, SH11, SM11, SHY19, SJ12, SG12, SMK18, SS17b, SSA13, SRAA17, SZTZ18, TB18, VEA19, WHZ12, WZX12, WYW13, WYFC14, yWX18, WYK12, WYL18, YLL12, YWNN15, Ye10, Ye14, YH16, YX18, ZZX11, ZWW17, ZWH17a, ZWZ17b, ZHS10, ARG19, AM19, BWA13, BM13, Bro19, CT11a, CW14a, EA11, FMB18, GKK11, HAK19, HLC16, KMG17, KM11, KKK18b, LXX11, LW10, LWL11, LW13b, LPZ15, MO14, MS17,
NES\textsuperscript{+14}, PTK14, SE18, Sch12a, SM13, SM12, SNM14, ST15, SGFCRM\textsuperscript{+18}, Sun16, jT12b, TTL10, TLI13, UUN11, UUN13, yWpWyYpN13, WDG19, WHZ\textsuperscript{+19}, WGGZ\textsuperscript{+12}, WSS\textsuperscript{+19}, WKHI1, WOLS12, XSWC10, YWL\textsuperscript{+17}, YC11]. image [YCC16, YSC16, ZLW\textsuperscript{+12}, ZT14, ZSM18, ZL12].

Image-Guided [CJFH14].

Image-Scrambling [LLL17a].

ImageMagick [Tay14].

Imagery [BCP14a, Ara13].

Images [BCPV11, BBM15, CLF11, FR16, GL10, LC15, LLY\textsuperscript{+12b}, MR16, NC12, Yam12, dRsdVc12, AM19, AMK12, DD13, HWYW14, LW13b, MM14a, MKH\textsuperscript{+12}, UUN13, WLH13, WZL13].

Imaging [WW13].

IMFlexCom [PAF18].

IMI [PN10].

imitation [Hai17, Pro15].

Impact [Alo12, ACC\textsuperscript{+13}, ATD17, BLS12, DM15, SF12, vRDhsp17, BGE\textsuperscript{+18}, HURU11].

Impartial [BCF16].

Imperceptibility [HTG15].

Imperceptible [Lin14a].

Impersonation [AATM18, GBNM11].

Implantable [BDM\textsuperscript{+19}].

Implants [Mic16, SSPL\textsuperscript{+13}].

Implausibility [GGHW17].

Implementation [AAUC18, BW16, BKL18, BSJ15, BDMLN16, EGG\textsuperscript{+12}, FLH0JRH18, FHLd19, GP17, GL12, GPT12, GM16b, GC\textsuperscript{+13}, HMKG19, HIJ19, HF14b, JZ18, KB10, KGV16, LLY\textsuperscript{+18}, MFG16, MAS16, NdMMW16, QLL17, RMP10, Soe18, TV19, VV19, VKPI17, ZPM\textsuperscript{+15}, AN18, Ang16, BDP\textsuperscript{+12}, GH13, GAB19, HBBRN16, KFE19, KY10, KSH18a, KSH18b, MM14a, MNNW15, NES\textsuperscript{+14}, PBCC14, SK14, SAAB10, SVGE14, SF12].

Implementations [BFCZ12, BFK16, BDGH15, BJ10b, Bru12, CMLRHS13, CBL13, ERRMG15, EKOS19, GZSW19, LGH\textsuperscript{+17}, MLCH10, MWES19, NDR\textsuperscript{+19}, SJLK18, SG19b, Tom16, VV18, YZLC12, ZSH\textsuperscript{+19}, ABBD13, ABF\textsuperscript{+14}, BFG\textsuperscript{+14}, BJR\textsuperscript{+14}, CFB14, CFN\textsuperscript{+14}, CGH17, LBOX12, RSMA19, Sta11c, ZSW\textsuperscript{+18a}].

Implementing [Dav11, GH11b, HTZR12, KV19b, LTC\textsuperscript{+15a}, SG15, SVGE14, SLM10, VOG15, SA16b].

Implications [DK16a, OSH16, SC19a].

Implicit [BDD19, HP17, DWZ12, SSM15].

Implies [BHT18].

Improve [AQD12, PMG19a].

Improved [Ber18, BCP14a, Chi12, CGK011, DL17, FVK17, GLLSN12, GR19a, HLS18, HIJ\textsuperscript{+19}, IK15, JH12, KZG10, LT14a, LWZ12, LJF16, LJF19, LHH11, LCCJ13, LC15, LYD\textsuperscript{+18}, LSG\textsuperscript{+19}, LLML12, MM17b, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WCD19, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, ZL12\textsuperscript{+19}, CNF\textsuperscript{+18}, CBL10, GLW13, HWB12, Nam19, PWL13, SD10, XHH12, YSQM19, Wan14].

Improvement [FRS\textsuperscript{+16}, LFX\textsuperscript{+18}, LYL\textsuperscript{+18}, LJ19, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNM\textsuperscript{+11}].

improvements [EA12, HRV10, Tso13].

Improving [AB15, BCM\textsuperscript{+15}, Chi16, FMS12b, GMS11, HLC11, MHC12, Sar10a, SS11, YFW18, YKS10, ZHS10].

impulse [LZKK19].

IMS [IG11, MEFO12, VGL14].

in-browser [ABR13].

In-Memory [PAF18].

In-Order [ZBPF18].

In-Situ [GRRZ18].

Incentive [SJWH\textsuperscript{+17}, YTH17].

Incentive-Aware [YTH17].

Incident [CCG\textsuperscript{+16}, CMG\textsuperscript{+18}, GQH17].

Inclusive [FD11].

Incomplete [VJH\textsuperscript{+18}].

Inconsistencies [YSC\textsuperscript{+15}].

inconsistent [OF12].

Increase [NNAM10].

Increasing [AEH17, CLZ\textsuperscript{+17}, HSC19, PKS18, RSX18].

Incremental [KKM\textsuperscript{+14}, MPRS12, CS11].

Incrementing [KS15].

IND-CCA [AHS14].
Integration
Integrity
Intercloud
Intellectual
Intensify
Inter
Inter-domain
Inter-Pulse
Introduction
Interactive
Interception
Intra
Intrinsically
Intersection
Invariants
Invertible
Inversion
Invisibility
InvisiMem
Invited
Isolated
Internet-Draft
Internet-of-Things
Internetworking
Interoperability
Interoperable
Interpolation
Interpretation
Interpretation-Based
Interpreters
Interval
Interval-based
Intermediaries
Inter-domain
Intra-domain
Intra-Masking
Intra-interaction
Intra-node
Intrusion-resilient
Investigating
Investigations
Investigation
Invention
Inverses
Inversion
Invisibility
InvisiMem
INVISIOS
Invited
Involution
Involvement [LKBK19]. Involving
[HCLL11, RB17]. IoT
[AATM18, AMSPL19, AMKC19, APMCRI13, BDL+19, BBTC20, CCM17, CSH+18, FQZF18, FM19, GA1+18, HHBS18, Hod19, KV19a, KKK+18b, KKD+18, LSQ15, LZZ+19a, MFP19, NVM+17, OSANAM19, PCK19, RC18, SSA18, SGC16, SJLK18, TODQ18, TG17, Wan18b, WCFW18, WXK+17, XYML19, YWJ+19, YFT17, YFT18, YTH17, ZCWS15, ZLY+19].

IoT-Based [YTH17, ZLY+19].

IoT-Enabled [SGC16]. IoT-FBAC
[YWJ+19]. IoTs [SAJL16, ZSW+18a]. IP
[AGLW16, AZH11, LMS10, FJ18, PA10, RS17c, SP15a, TJJZ12, WBC+10]. IP-SEC
[PA10]. IPE [ZM16]. iPhone
[Wu16]. IPs
[EAAA19, GSFT16, NDG+17]. IPv6
[KP12]. IRC [HB13]. IRC-based [HB13]. iris
[HURU11]. IRIW [JKHeY12]. irrregular
[YWL+17]. Isabelle
[Kam19]. ISBN
[Ano15b, Ano17b, Bai12, Joh10, Mur10, Sch15a]. ISBN-13
[Joh10]. Islet
[Dan12]. ISO
[BCM12, BCM13, TS16a, WWBC14]. ISO/IEC
[BCM12, BCM13]. Isogenous
[Y+17]. Isogenous [AMMV18]. Isogenous
[BF19, FHLOJR18, KD18, KAK18, Lan17, LNL+19, ZSP+19]. Isogenous-Based
[BF19, KAK18, ZSP+19, KD18]. Isolated
[GK19, Sch19b, YSI15, KKK+16]. Isolating
[LG12]. Isolation
[GGK18]. Isomorphic
[AMMV18]. Isopleth
[HGOZ19]. ISSAC
[Wat10]. Issue
[Ano13f, Ano16b, Ano16c, Ano16]. Issue
[Ano19a, AHWB20, BCHL19, CWZL13, CSYY18, GO17, LW13a, LLK18, XW13, YYW19, PHW10, Sim15b]. Issues
[ABHC+16, PZPS15, VKK+19, JAE10, KJN+16, MVH15, SVGE14]. ISTE
[Ano15b]. Italian
[Sac14]. Italy
[Cra12]. Item
[CZ19]. Items
[CZ19, YD17]. Iterate
[HRR11]. Iterated
[LPS12]. Iteration
[CCZC13]. Iterative
[QJC+18, SXL16]. ITUbee
[FXP+17]. iVector
[RSR+19]. iVector-Based
[RSR+19].
[ASN12, Alz19, ADSH18, Ano11b, ABB19a, BN14, BVS+13, BL12, BSBB19, BBB+16a, BD15, Bar16a, BR19, Ber16a, BM18, BCO13, BKLS12, BF11, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CLND19, CWZ19, CJ13, Chi16, CCT+14, CNT12, Cou12b, CMA14, DWWZ12, DL12, EAA+16, EFG18, FZT13, FHLOJRH18, FVS17, FBMI2, GDLL18, GFBF12, GT12, GZZ+13, GSW+16, GST13, GPT14, Gir15, GKS17, GZ12, GLB+18, GYW+19, HSMY12, HLLG18, HEP+11, HC12, HWS+19, HCL+14, HTC+15, HEC+12, HLH19, Jia14a, JEA+15, KP12, KMKZ19, KTT12, KFOS12, Kim15, KG19, LLSW16, LGBK19, LG10, LLLL15, LD16, LQY10, LLY16, LH11c, LSQL18b, LCCJ13, LWL+17, LYY+18b, LBR12, LLH18, MZHY15, MVT12, MMP14, MTY11, MMY12, MV19, MK17, MPRS12, MSN11, MSU13, NNA10, NYY+14, NTY12, Om16, PSM17, PD15, PCK14, Pud12, PRC17]. Key [RVH+16, RSBGN12, RW12, Saa12a, SK11, SNJ11, SEKH12, Saa18, SK12b, Sec18, SWM+10, Sia12, SD11, SGG15, SLV+16, TMC15, TMY+17, TM12, VCA19, WP17, WSS12, WLC12, WZ15, WCL+18, WWHL12, WT10b, WSQ+16, WCX17, XNG15, XX12, Xio12, XLM+12, XJWW13, XGLM14, XCLW15, XR+17, YM16, YZX+12, YSU12, YLSZ19, YLY13, YRT+16, YL17, Yon12, YKC+11, YFK+12, ZSP+19, ZHX16, ZY17a, AHG18, AAL19, AA14, AQRR+18, AKTH+17, APK+18, ABB+14, AKGI3, ABB+16, ABW10, ABR13, AN15, AK44, AYSZ14, AVA18, BS15, BGAD12, BB14, BZD16a, BJ16, BS12, Bon19, BGG+13, BEB+18, BB16b, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLCZ10, DLK+16, DGL15, Dur15, DMSD18, EBAÇ17, FHH10a, FA14b, FIO15, FHZW18, GMRT+15, GPP+16, GLMS18, GmDFPCL17, GH16, GBNN11, GLM+11, GSAV18, GTSS19, HPC12, HZWW17, Hod19, HWB10]. key [HBW12, HL11, HLY+19, HLYS14, HTC17, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSMG18a, KDH15, KMTG12, KKG14, KV19b, KIH19, KP18, KLW+16, KD+17, LLLS13, LLP+18, LLY06, LZ11, LHM+10, LW+19, LWS10, LDZ+14, LK+17, LP10, LW13b, LZC14, LM14, LML+13, LG19, MNP12, MHL18, MRT10, NAAC12, NCL13, Nso11, Nso14, ODK+17, OSANAM19, PY19, RR16, RG10, RWZ13, RPSL10, SES+16, SPD+10, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZZ15, SA15, SLXX16, SCBL16, SGP+17, Sv17, TK19, TCS14, TLL12, Tso13, TKHK14, VV19, VN17, WWZY11, WR10, WMU14, WDV18, WDKV19, WZM12a, WZ11, WT10a, WTT12, WQ+13, WX+17, WX12, WX13, XC13, XX19, XYL19, XCL+19, XMHD13, XM14, YT11b, YCI12, Yan14, YZZ+14, YHS16, YZL+18, YLL+18, YN19, YYY13, YLZ+16, ZCZQ19, ZP+16, ZG+17, ZGY18, ZW+11, Z ZZ11, ZHL+11, ZCC15, ZTT16, ZGL+18a, ZWX+18]. key [ZW18, ZLC+19, ZG10, ZCC15, ZCC17, ZY17b, ZWS+18, ZCZ+19, ZHT16, vV16, CLW16, OHJ10, XR+17]. Key-Aggregate [CCT+14, PSM17, GLB+18, CLW16]. Key-Agreement [WSS12, APK+18]. Key-Alternating [BKLS12]. Key-Based [Xio12]. key-correlations [Sar14]. key-delegation [JSMG18a]. key-disclosure [ZZC17]. Key-Insulated [BCO13]. Key-Extraction [GPT14]. key-hash [KKG14]. Key-Policy [GZZ+13, GSW+16, HSMY12, RVH+16]. Keyed [KE19, MMS17b, YHHM18]. Keyed-Function [MMS17b]. KEYing [TW14, BCPV11, ABC+18, GJ19]. Keyless
keyrings [MBB11].

[BCO13], [Lanczos [FYD+19].

Lanczos-Based [FYD+19]. [Land [Sch18].

Landis [BBB16b]. language [Ksi12].

Languages [MX13, Wat12]. LANs [FLH13].

Lapin [HKL+12]. Lapport [GPT14].

Large [AN12, DM15, FNWL18, JLS12, JKHeY12,

KCR11, KU12, LLS19, LW16, LQD+16,

MC11, SP13, And19, dCCSB+16, DEL19,

EEAZ13, FXP12, GSN+16, LFZ+17,

LBOX12, SR10, VSB+19, ZZKA17, ZVH14].

Large-Scale [DM15, JKHeY12, LLS19,

LQD+16, And19, dCCSB+16, DEL19,

FXP12, GSN+16, SR10, ZZKA17, ZVH14].

LARK [DS11]. Laser

[DDR+16, FNP+15, Lüd12]. Last

[Hof15, Hof16]. Latency

[AYS15, BCG+12b]. Latency-Optimized

[AYS15]. lateral [SCY15]. Latest [Ber17].

Latin [AB10a]. Latincrypt [AB10a].

Lattice [ADM12, Akl11, AYS15, BSJ15,

EM12, EFGT18, FG10, GCH+19,

HPO+15, HKR+18, LNWZ19, LPO+17,

MLO17, NDR+19, PG12, AAT16, AVAH18,

BH19, Dra16, LLM+19, MGB19].

Lattice-Based [ADM12, Akl11, AYS15,

BSJ15, EM12, EFGT18, HPO+15, HKR+18,

LNWZ19, LPO+17, MLO17, NDR+19,

PG12, GCH+19, AAT16, LLM+19].

Lattices [Boy13, LYY+18a, LYX+19, Lau17,

TH16, XXZ12, ZQQ15, Kre13, Tia15,

XLWZ16, yYqWqZC13]. launch [Zet14].

LAUP [BNH19]. Laurent

[Ano15b, Ver17]. Law

[Bl12, SR14, Wu16, AOT13, ZHS10]. Layer

[HYX+18, LHM+15, PRGBSAC19, ZH16,

HYQ+16, LKK13, ZNH+17]. Layered

[Bel19, BS14, GRL12, WWL+14, JCHS16,

Tan18, ZC12]. Layering [YXK+17]. LBlock

[MRD13, MN12]. LDGm [BBC+13]. Lead

[Arm19]. Leader [ADH19, TKM12]. leads

[Ano14a]. leak [BBG+17]. Leakage

[AV12, Bar16b, BKK10, CBRZ19, CBL13,

DCA18, DHB16, FPS12, GDDL18, HHH+13,

HHP17, HHS18, IL15, Kom18, LTZY16,
Leakage-Free \([IL15, LSQZ17, TTH15]\).
Leakage-Resilient \([AV12, FPS12, HHS18, LTZY16, Pan14, XZY+12, ZYT13, ZMM17, ZYT17a, ZYT17b, ZYT18, ZYY+19, ZYH+19, ZBF18, ABC+18, CQX18, DLZ16a, DMWS12, GV14a, GLL+18, HYL+19, LLG19, SGP+17, YLZ+16, ZWM14, ZCC15, ZYM19]\). Leakage-tolerating \([ZWM14]\).
Leaking \([BF11]\). Leaks \([CATB19, DLV16, JGP+18, Sav13a]\). Leaky \([DLWW11]\).
Leap \([Ano16d]\). Learned \([KMP+11, WL11]\). Learning \([BNMH17, Bar16b, CTC+15, CRS+18, GN16, HFW+19, HXHP17, HGOZ19, KPC+11, KRB12, Mor19b, Raz19, RDK19, RHLK18, SPG+19, Yon11, ACM19, GJ13, GSAMCA18, KMG17, KD19, Sch12a, WS14, BCV12]\). Learning-based \([WS14]\). Least \([KTM19]\). Leave \([GA19, CMG+18]\). Lecture \([Hel17b]\). LED \([IS12, JKP12, MRTV12]\). Ledger \([Mufl6]\). Leeds \([vDKS11]\). Left \([BBG+17]\). Left-to-right \([BBG+17]\). Legacy \([CS12, Smi11b, CGH17]\). Legal \([ZTSR12]\). LeGall \([Ara13]\). Legislation \([PH12b]\). Legitimacy \([IM16]\). Lemonade \([DFKC17]\). Lemons \([DFKC17]\). Length \([AS17, GT12, Gir15, PDNH15, PNRC17, Zha12]\).
Length-Doubling \([Zha12]\). Lengths \([BR19]\). lens \([PHN+12]\). LEO \([RM18]\). LEESPP \([WLZ+16]\). Less \([TKR14, GM13a, Kam16]\). Lessons \([KMP+11, TGCl6, WL11, CMG+18]\). Level \([AW17, Ano15a, BBCL19, BRPB13, BKJP12, CCW+10, DA10, FGRQ18, Gli12, HZS+19, HS18, JW+17, KPC+16, KGP12, MV16a, XZL+19, ZLDC15, ABBD13, CIL16, MEFO12, RS17c, UUN13, VS11, YT11a, Bai12]\). Leveled \([BV14]\). Leveling \([LY15]\). Levels \([HLCL11, LRW17]\). Leveraging \([DMS+16, GMDR19, HCM11, MV11, SKGY14, ZYGY18]\). Lewis \([Mar10a]\). Lexicographic \([ZAC17]\). LFSR \([HLC12, MRT10, WGD18]\). LFSRs \([QGGL13]\). Liability \([Bra13]\). Liars \([Sch12b]\). Libertarian \([Eya17]\). Libgcrypt \([DK16b, Bro17, Win17]\). LiBrA \([GMVV17]\). Library \([ACZ16, Bee17, BLS12, FLM12, KRH18]\). Licensing \([EAAAA19]\). Lie \([HWS+19]\). Life \([MKN13, SCS18, McK10, McK11, War11]\). Lifecycle \([Tan15a]\). Lifetime \([HSUS11]\). Lifting \([LSL12]\). Light \([JEA+15, SWF+19, PCK19, SJ19, ARH+18a]\). Light-Weight \([SWF+19]\). lightning \([Ran10]\). Lightweight \([ADM19, AMSPL19, AMKA17, AARJ12, BNNH19, BCHL19, BSS+13, BFMT16, BKL+13, BM11, CGCGPD12, CWP12, CCF17, DS11, ESK12, EKP+13, FVB+18, FQZF18, GNL12, GAI+18, Gop19, GMVV17, GMSV14, HZW18, HCETPL+12, IS12, IO12, KE19, MO12, MFG16, MPM+17, PCDG14, SBS18, Sh14, YN19, ZYW+13, ZY19, ZLY+19, ZSH+19, AMN18, AATM18, AKKY17, BLL+19, BC16, BBB19, Bor10, BBB16b, CL11, DA18, FLL+14, GH15, GTSS19, KDH15, LLZ+16, MCN+18, MN12, MV15, MYY+18, OSANAM19, PJ18, PSO+13, SGJ+18, Tan12b, TG17, WLZ+16, WCFW18, WWBC14, WXZ+18, XCY19, XM14, YCT15, ZZ+19, ZSW+18a]\). Like \([BW16, ERLM16, HP17, WJ19, AHG18, CGCS12, CZZ13, DLH19, K15, LJ15, LJ16, RS14]\). Lilliput \([BFMT16]\). Limitations \([CK17, DR12]\). Limited \([DFKC17, ZZC17]\). Limited-Use \([DFKC17]\). Limits \([AS16, GV14a, KS12]\). Lindell \([Fu10]\). Line \([FFL12, LKBK19, YMW11]\). Linear \([BCT+13, BW12, CGCS12, CMA14\)
EKP+13, FGMP12, HK14a, LGLL12, LJ15, LJ16, LFW+16, WGP16, YCL17, BBP14, Bul10a, DMSD18, FES10, GMGCCC15, Her10, HCC11, LWK11, ÖS11, SA14, XSWC10. **Linear/Linear** [EKP+13].

Linearly [ADD10, MBP19]. **Lines** [HR19].

Linguistic [OO18, OOT18]. linguists [Ma16]. **link** [Ham12, VS11].

link-state [Ham12]. **Linkable** [YLA+13].

Linkage [RCBK19]. linked [JCHS16].

linking [GSGM16, NPH].


Location-Based [RSX18, SNCK18, VKK]. Location-Privacy [AV18, JP19, Kim11, PSD15, PKA15].

Locality [CDPLCA16], **Loc/ID** [CDPLCA16]. Local [pNyWyY+14, TKM11, VGA15, WYW+13, LMJC11, LWW+10, PTK14].

Locality-Based [JP19, Kim11, CXX+19, CHX13, LWYM16, NZL+15]. Location-dependent [PKA15].


Log [YKK18, PGLL10]. **Log-polar** [YKK18, PGLL10]. Logarithm [BGJT14, CLL16, VM14, AMORH13, BGJT13, MM13, Mes15, TPL16].

logarithms [BGG+19]. **LogCA** [AW15, AW17]. **Logging** [YNR12a, YNR12b]. **Logic** [Che18, Cil11, DGP10, He17b, Nie02, RZZ+15, Ter11].

logical [CO11]. **Logistic** [JHW+19]. **logo** [BWR12b]. Loiss [DG12]. Long [Lam13, vdG17, CFVP16, VBC+15, BF12].

Long-distance [Lam13]. Long-Term [vdG17, CFVP16, VBC+19]. **look** [AY14a].

look-up [AY14a]. **Looks** [ERLM16, KTA12, Sch16c]. lookup [LDDAM12]. lookup-table [LDDAM12].

Loop [EFGT18, JS18b, DWZ12]. Loop-Abort [EFGT18]. losing [SLZ+12].

Loss [DK16b, JTZ+16, DMV15]. Lossless [DA12, LZC+12b, GJ13, TTL10, WLH13].

Lossy [BKP12, CCL+19, CW12a, DN12, ASO14, CQX18]. Lost [WBA17]. love [Fag17, FH+12]. Lovers [Keb15, Mac14].

Low [ABC+17, AWS17, Bai10, BCO13, BCG+12b, CMLS15, DJL+12, FHS13, FMC19, GST13, GI12, LJK17, LZZ+19a, LBR12, Man13, NVM+17, RM18, RS17c, SJAL16, WT10b, ZJ11, ABO+17, CZ14, CJL16, Chi13a, FQZF18, LGKY10, LKAT12, LEW19, MHV15, NR11, SG19a, ZPZ+16].

low-area [ABO+17]. **Low-Bandwidth** [GST13, NR11]. Low-Bit-Rate [LJK17].

Low-complexity [DLJ+12]. Low-Cost [ABC+17, GI12, LZZ+19a, Man13, NVM+17, LEW19]. Low-Distortion [FHS13].

Low-End [AC13]. **Low-Latency** [BCG+12b]. low-level [CJL16].


LR-UDES [YHZ12]. **LSB** [DA10, LHM13, Tan12a]. LTE [CLM+12, DLK+16, LLS13, QMW17, SG16, TM12].

Luther [ABJ13]. LWE [BV11, XY18]. LWT [TB18]. Lyra2 [ASBdS16]. LZSS [CFY+10].

M [Orm16, Ver17, HvS12]. M-Identity [HvS12]. M2M [TKG+17]. MA [ACM10, TT18]. MAC [Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, OPS14, VN16, WCXZ17].

MacGuffin [LGL+12]. Machine [AGHP14, Ano16d, CHS15, GN16, KD19, Sch12a, TKG+17, ABBD13, GJ13, GSAMCA18, Gup15, LLZ+16, LHA+16, QMC17, Ry10, TTL10, War11, WS14, TKG+17].


Magnifying [DKL+16]. mail [BTW15, Sch16b]. Main [AMH+16, LY15, ZHZ+19, CS11, HHAW19]. Maintaining [WK18]. Make [Ano10a, Cra12, DDS12, Dan12b, IEE11a, Pie10, Sah13, WZM12a].

Management [Dew11, LYX+19, Mar10a]. Mapping [MCLM13, DPW18, MSas12, CG14a, FNMV14, LP11, MSas13, OOR+14, Pas13a].


Mass [BP14a, BPR14b]. Masses [Ano15c, BCHC19]. massive [FLYL16a]. Master [Dew11, LYX+19, Mar10a].

Matching [Lin15, RCBK19, Tan12a, DA18, LHM13, MR14c, MHT+13, PPTT15, SS17a, SM10c, YZL+18]. MathCW [Bee17].
Mathematical
Metaheuristic [HCETPL+12].
Metamorphic [ATS15].
Meters [DM15].
Method [AGW15, Ara13, BBB+16a, CZ19, FLH13, GLLSN12, GMNS15, HXHP17, HHS+15, KTM19, LyWZZ12, LP12, LD13, LBR12, MU12, OWHS12, PS14, PWS+19b, QF19, SAA15, SY15a, SXH+19, SP15a, SZDL14, USH19, WZXL12, WZCC18, WJ19, XNG+14, XNRG15, YYO15, AGLW16, AIA+18a, ARG19, BLL+19, CSS+13, DJ19, Dra16, FVK17, JS18a, JDV16, Khl18, KHHH14, LLC10, LH11a, LT13, LT14b, LPZJ15, Mar12, MO14, PWW10, SI12, WT13, YWT+12, ZYGT17].
Methodology [CBL13, Uto13, ZZKA17].
Methods [BCEO19, BCEO20, BKBK14, Kob10, LW12, GMT+12, GSGM16, IAA+19, KSB+17, KVvE18, OO10, TMK11, TPKT12].
Metrics [YGFL15, DMWS12].
Metrics [CVM14, PGLCX17, SSP19, BC18].
Mexico [AB10a].
Microarchitectural [MSI18].
Microarchitecture [ZBPF18].
Microcontroller [GL12].
Microcontrollers [LPO+17].
Microcosmic [WWC+11].
Micropayment [RM19].
microphones [GSAV18].
microprocessors [SK12b].
Microsoft [Loc15].
Mid [AUMT16, KTM+18].
Mid-Air [AUMT16, KTM+18].
Middle [LJ17, LJ18, LYD+18, LSG+19, LWKP12, LWPF12, LWPK14, vV16].
Middlebox [FGRQ18, FGR+17].
Middlebox-Based [FGRQ18].
Midway [Car11].
Might [Hur16].
Migration [SHS12].
MIKEY [TW14].
Military [HK14b].
Million [Sch16a].
MILP [CWZ19].
MIMETIC [ACMP19].
Mind [SNG+17, WP15].
mines [KO16].
MinHash [HWZP18].
MinHash-Based [HWZP18].
Miniature [HWS+19].
Minimal [ARH+18b, BDH11, MZi17a, SBM15].
Minimalism [DKS12].
Minimally [AARJ12].
Minimization [AH19].
Minimizing [BCD+12].
Minimum [KHPP16, DZS+12].
Mining [BH15, BJL12, CZ19, DK16a, HDWH12, WZCC18, ZW15, Ano11a, ZMYB17].
Minus [NXB13].
miracles [ML14c].
Mirror [Ano10b].
Misbehaving [TAKS10, ATK11].
Misson [Ano10a].
Mistakes [DHB16].
misuse [EBFK13].
Mitigate [BKJP12, SS15].
Mitigating [EPAG16, HRS16, SNG+17].
Mitigation [BRS17, DHT+19, LGR14, DJL+12].
miTLS [BFK16].
MitM [TY16b].
mix [WGJT10].
mix-networks [WGJT10].
Mixed [ST16].
ML [Ksi12].
mMTC [CML+18].
MNC [IM16].
Mo [RBS+17].
Mobile [ATC17, BCD+12, CBKY16, FD11, GPT12, GdM16, HS12, HFS+19, HLKL15, KP12, KKA15, LH12, LBC18, May15, NRZQ15, PH16, RSX18, Sch15b, SFE10, She14, SS15, SAA12b, WPZM16, WT10b, XHX12, XNKG15, XHC+12, YHL16, Yon11, ZLDD12, Aia15, AZ+16, ALL+18, CLP+13b, CTL12, CCSW11, CWXW16, CTL13, CRSL13, uHAN+18, FHH10a, FA14b, FHZW18, FH+10, GM16a, GH16, HZWW17, HZWL18, HL14, IAA+19, IB11, Kem11, KKA14, KKM+13, KKM+14, KKG14, KSB+17, KS19, LH11a, LZD+19, LH13, MHL18, ODK+17, OYHSB4, Par12b, SSA18, SLL+19, SNS15, hZSZ15, SM19b, SCR19b, SSAF11, SKB+17, SHBC19, TZTC16, TKHK14, WSC14, WT10a, YHHM18, YNX+16, ZLDD14, ZDW+16, ZC12, ACMP19, MBF+13, SLL10].
mobile-cloud [KKM+13].
mobiles [GCSAdP11].
Mobility [CLH13, LNK+18a, CL11, GH16, LH11b, MYYR13, THA+13, YLS12, ZX11].
Modal
Multi-Biometric
[NGAuHQ16, YYK+17, MLBL12].
Multi-bit
[TWZ+12]. multi-channel
[CPPT18]. Multi-ciphertext [KTT12].
multi-cloud [CFVP16, SWW+16].
multi-cloud-server [KLW+17]. multi-core
[AVAH18]. multi-criteria [ZZKA17].
multi-crypto-processor [BGG+13].
multi-dimensional [LZWZ19].
Multi-Directional [JS18a].
multi-Domain [SAM+18, IG11, QMC17].
multi-exponentiation [WSQ+16].
multi-Factor [PSSK19, HC12, CLP+13b, DRN16].
multi-generation [CGJX19]. multi-hop [LCT+14]. Multi-instance [BRT12].
Multi-KeyWord
[CWL+14, XWSW16, OSSK16, DDY+19, GZS+18, LKX+14, YQZ+19]. multi-lateral
[SCY15]. multi-layered [JCHS16].
multi-level [ZLDC15, MEFO12].
multi-linear [BBEPT14]. Multi-Modal
[HFS+19, BOP14, GBC19, SCFB15].
multi-Party [ABL+18, KMO14, TYM+17, GVW12, LyWSZ10, DGL19, XLWZ16].
Multi-Pixel [YWW10]. multi-privileged [WDLZ13].
Multi-Proxy [ASS15, GJZ17]. multi-purpose [KM11].
Multi-Receiver [TFS19, Wan14, Chi16]. Multi-sawtooth
[Ye14]. Multi-scale [DLGT19, CG12b]. multi-scroll [GMGCCC15].
Multi-Secret
[HYS11, ZC13, CW14a, HCCC11, HLC12].
Multi-Segment [WOLP15]. multi-server
[CLHJ13, FHZW18, HL14, ISC+16, LXMW12, LH13, SSS11, TLL12, XHM14, YN19, YY13].
Multi-Signature [ASS15].
multi-stage [Mas17]. Multi-target
[HR16]. multi-use [CZ15b]. Multi-User
[MZHY15, SOR16, OKG+12, MML16]. multibit [KPS10]. Multicast
[CC14, PSM+18, BAL10, DMM10, HGWW11, LIT10, NAeCR12].
Multicore
[RJ+18, SHC+16]. Multicoupon
[HDGFPC15]. multidesignated [AYSZ14].
Multidevice [DPCM16]. Multidimensional
[AJA16].
Multifactor
[He10, WWBC14, HMCK12, JLC18].
Multifactor
[MHY12, KS19]. Multigigabit
[PP10b]. multi-hop [ADF12].
Multikey
[LATV17]. Multilayer
[NXH+17]. Multilevel
[FMS12h, HF14a, NSA15, SERF12].
multilinear
[CIL16]. Multimedia
[BCG10, NSA15, PMZ13, PZPS15, PYM+15, WLY+15, ZW15, Zha15b, ZSA12, GJJ18, HM10, HWYW14, HPL+19, LLLK10, Wan13, XWZW16, TT14].
Multimodal
[GM16a, Sar18a, ACM19, AHM+18, ATI+10, MHT+13]. MultiObjective
[ZAC17]. Multipartite
[HR13].
Multiparty
[BDOZ11, CCL+13, Fri10b, ADMM16, BHH19, LDDAM12]. Multipath
[LH12, OPHC16].
Multiple
[DSB15, Dzu12a, FR16, HWZP18, HZSL05, KBL11, LTC+15b, LQD+16, Ma17a, NDC+13, SY14, SC10, SKS+18, St12, WWL+14, XNP+18, GJJ18, GZS+18, LWZG10, LTC+15a, LZC17, MN14, PZL+19, RWZ13, TKHK14, YQZ+19, YJC18].
Multiple-Layered
[LWZG10, LTC+15a, LZC17, MN14, PZL+19, RWZ13, TKHK14, YQZ+19, YJC18].
Multiple-Precision
[ZAC17]. Multiphase
[LH12, OPHC16].
Multiplex
[DSB15, Dzu12a, FR16, HWZP18, HZSL05, KBL11, LTC+15b, LQD+16, Ma17a, NDC+13, SY14, SC10, SKS+18, St12, WWL+14, XNP+18, GJJ18, GZS+18, LWZG10, LTC+15a, LZC17, MN14, PZL+19, RWZ13, TKHK14, YQZ+19, YJC18].
Multiplication
[ARM15a, AK14b, CMQ+16, GL19, HVL17, LN+19, NRT15, SK12b, YTS12, AAT16, DGK18, Khl18, SKH15, SF12].
Multiplicative
[RMERM19, KHHH14].
multiplicity
[LA14]. Multipliers
[ARM15b, GT19]. Multi-receiver
[FHH10b].
multisecret
[FGMP12]. multiserver
[CNF+18]. Multiset
[FA19]. MST17. Multispectral
[DCM18]. Multithread
[WXL+17]. Multithreaded
[TLZ+17].
Multitone
[GL10]. Multivariate
[CLND19,
negotiation
neglected

Network-Assisted
[KKC17], network-based [YLS12].

Network-Coded [She14].

Network-on-Chip [Bis17]. Networking [CKHP19, FVB+18, FP19, KYEV+18, LCK11, LLZ+17, ZHL15, Kim11, LCM+17]. Networks [ABCL17, ABC+17, BN14, BPSD17, BCG10, BFMT16, CS14, CSH+18, DLGT19, DS11, DF16, FMS12b, GMVV17, HZC+12, HBC13, HK14b, JZS+10, KL15, KP18, LH11b, LKKL13, MZA+13, MJS18, OF11, PL16, RCW15, Ser12, SCKH10, SKS+18, Sta11b, Tan15b, THA+13, WYL13, WS14, YLS12, ZOSZ17, Ste15b].

Network-Assisted [KKC17], network-based [YLS12].

Network-Coded [She14].

Network-on-Chip [Bis17]. Networking [CKHP19, FVB+18, FP19, KYEV+18, LCK11, LLZ+17, ZHL15, Kim11, LCM+17]. Networks [ABCL17, ABC+17, BN14, BPSD17, BCG10, BFMT16, CS14, CSH+18, DLGT19, DS11, DF16, FMS12b, GMVV17, HZC+12, HBC13, HK14b, JZS+10, KL15, KP18, LH11b, LKKL13, MZA+13, MJS18, OF11, PL16, RCW15, Ser12, SCKH10, SKS+18, Sta11b, Tan15b, THA+13, WYL13, WS14, YLS12, ZOSZ17, Ste15b].
TKHK14, WGJT10, Wan13, WW14, WMC17, WXSH19, WDV18, WXK+17, XW13, XWDN12, XHCH14, XMHD13, YHHS16, YWY+19, YN19, ZYG17, ZWQ+11, ZB11, ZCLL14, ZT16, ZLDD14, ZHH+17, ZX11, LNK+18a.

Neural [CSH+18, RSX18, SKS+18, YZLC12, EEAZ13, HZW19, HW19, KMG17].

Neuroscience [BSR+14, JW14].

Neutrality [Kha10].

Neutrality-Based [Kha10].

Neutrosophic [JS18b].

Nevada [IEE10].

never [Bai12].

Newcache [LWML16].

Newly [ABJ13].

Newman [And13].

News [And19, Edw14, Edw17, Lam13, Sav13a, Sav15, Sav16].

Next [HEP+11, MR14a, MJGS12, Aia15, ACD+15].

Next-Generation [MR14a].

NFC [LY14, Mic16].

Niederreiter [HC17, MVVR12].

Nievergelt [Ter11].

Nine [Mac12, LYHH14].

NIST [MMKP16, ZSH+19].

NIZK [Pas13a].

NIZKCTF [MBC+18].

NIZKs [CKLM13].

NLM [OPS14].

NN [ZZC17, ZHT16].

No [WDDW12, Wu16, KHHH14, MPJ+16].

'nobody' [Sto12].

Node [AA19, ARWK19, NYR+14, OKG+12, GM13b, LC17, PX13, SAAB10].

Node-Capture [NYR+14].

Nodes [VGA15, ZYL+10].

Noise [ASN11, Fyo19, LKBK19, YMA17, BCND19, QL19, ZHH+17].

Noised [JLS12].

Noisy [ASN12, HZW+14].

Non [AH19, AS17, AMH+16, BBCL19, BCI+13, CG14a, CPS16, DJL+12, DPW18, EKP+13, FHKP17, FMNV14, GL19, GZXA19, HWS+19, HK14, JSA17, KTT12, K18, LLG15, MFH13, MS12, OOR+14, Pas13a, QIC+18, RM18, RMG18, Svo14, SM18, WgMW12, XZL+19, YNQ15, YKCL12, ZLDD12, AY14a, AM19, BS15, CS11, ESII14, GIJ+12, Kre13, Lan11, LJY16, LP11, MS13, SES+16, SXL16, VBC+15, XSWC10, Yan14, Kh18].

Non- [AH19].

Non-abelian [HWS+19].

non-adjacent [Kre13, Kh18].

non-associative [BS15].

Non-Black-Box [CPS16].

Non-blind [HK14, RM18].

Non-Boolean [AS17].

non-browser [GIJ+12].

non-compliant [Lan11].

Non-contextual [Svo14].

Non-Coprime [GL19].

non-cryptographic [AY14a, ESRI14].

non-dynamic [SES+16].

Non-interactive [BCI+13, LK18, Pas13a, LJ16, Yan14].

Non-interference [BBC19].

Non-intrusive [MFH13].

non-iterative [SXL16].

Non-Interactive [KOS16, GOS12, MBC+18].

Nonlinear [CCM+15, KW14, LW13a, Lud12].

Nonlinearity [MM17b].

Nonlinearly [Fyo19].

Nonvolatile [ZHZ+19].

Norm [FHS13].

Normal [RMERM19, TY16a].

Normalization [KLY+12, SJ12].

Normalized [YGLF15].

Norman [Low12].

Note [HYS11, Gal13, GR19b, Hwa11, Lim11].

nothing [Cer15].

Notifications [LBC18].

Notions [KFSO12, SNJ11, Sar12, BP11].

Novel [CLHC12, DCM18, KRKH13, LYY+18a, LYX+19, LLG15, LyWZZ12, LH11e, MJGS12, MCS+15, SKL16, SWM+10, SC12, VN16, WHZ12, WZXL12, YZX+12].
MSM\textsuperscript{+18b}, SKS\textsuperscript{+18}, SYW17, XTZ\textsuperscript{+19}].

**Online/Offline**

[JMG\textsuperscript{+16}, LKA12, XTZ\textsuperscript{+19}]. Only

[BB10, YNR12b, YLW13, Bul10a, KMTG12, KA17, Sar11]. **Open** [SS19, ABF\textsuperscript{+14}, MHV15, Pow14, Win17, ZWQ\textsuperscript{+11}].

**open-source** [ABF\textsuperscript{+14}, Pow14]. **OpenCL** [ABDF15].

**opening** [GDCC16, LZC12a, LLH18, LZC14].

**Openings** [SP13]. openness [Bia12].

**OpenPGP** [MBB11]. **OpenStack** [CSL\textsuperscript{+14}]. Operable [BCF16].

**Operand** [MSI18]. **Operating** [KMP\textsuperscript{+11}, CDA14, MNNW15].

**Operation** [GLLSN12, JB11, SBS18, ALL\textsuperscript{+18}, Fay16, Lin14a, SKK10, WGZ\textsuperscript{+12}].

Operational [CRE\textsuperscript{+12}, CM11, MNNW15].

Operations [Cil11, SEY14, SZHY19, YWW10, KKKJ\textsuperscript{+16}, LZY\textsuperscript{+16}]. operative [HFCR13].

Opportunistic [AA19]. Opportunities [Lau17, Mic10b], opportunity [Sch11].

**Optical** [PRGBSAC19]. Optimal [AS17, CK17, DSSDW14, GJJ18, GM16b, HRB13, PD16, QIC\textsuperscript{+18}, TX16, WMU14, Cha13a, CXWT19, DDD14, MCL\textsuperscript{+19}, PPTT15, SYV19].

Optimality [MM17a, SDM\textsuperscript{+12}]. Optimally [DSMM14, GT12]. Optimally-Fair [DSMM14]. Optimised [CMO\textsuperscript{+16}].

**Optimising** [EV10]. Optimistic [WA15, SEXY18].

Optimization [AEP18, KD19, WH17, Z\texttextsuperscript{+17}, FLZ\textsuperscript{+12}, GCG\texttextsuperscript{+18}, KHH10, PTK14, RF\textsuperscript{+13}, ZSM18, sCR19a]. Optimizations [ZAG19].

**Optimized** [ARH\textsuperscript{+18a}, AYS15, EKB\textsuperscript{+16}, GAB19, HGT15, LNL\textsuperscript{+19}, MBF\textsuperscript{+13}, MBR15, JS18a].

**Optimizing** [DWZ18, ZSM18]. Optimum [Oba11, YFF12]. Optional [PC16].

**OR-Proof** [FXS12a]. Oracle

[CBJX19, GLM\textsuperscript{+16}, HKT11]. Oracles [FZT14, FXS12a, GSW\textsuperscript{+16}, XLQ09, XQL11, YS12, YKC\textsuperscript{+11}, YLA\textsuperscript{+13}, ZYM18, LLY15, RG10, SYL13, WWYY11, YFK\textsuperscript{+12}].

**ORAM** [RM18]. Order

[DC17, FYD\textsuperscript{+19}, KS12, LFX\textsuperscript{+18}, LWK12, PRC12, YK12, ZDL12, ZSW\textsuperscript{+12}, ZBP18, AKY13, BKR19, LW13a, LCTY\textsuperscript{+16}, LWK14, gWP\textsuperscript{+14}, YL11].

**Order-Hiding** [DCA18].

**Order-Preserving** [KS12, YK12, YL11]. order-revealing [BKR19].

**OpenStack** [CSL\textsuperscript{+14}]. Operable [BCF16].

**Operand** [MSI18]. **Operating** [KMP\textsuperscript{+11}, CDA14, MNNW15].

**Operation** [GLLSN12, JB11, SBS18, ALL\textsuperscript{+18}, Fay16, Lin14a, SKK10, WGZ\textsuperscript{+12}].

Operational [CRE\textsuperscript{+12}, CM11, MNNW15].

Operations [Cil11, SEY14, SZHY19, YWW10, KKKJ\textsuperscript{+16}, LZY\textsuperscript{+16}]. operative [HFCR13].

Opportunistic [AA19]. Opportunities [Lau17, Mic10b], opportunity [Sch11].

**Optical** [PRGBSAC19]. Optimal [AS17, CK17, DSSDW14, GJJ18, GM16b, HRB13, PD16, QIC\textsuperscript{+18}, TX16, WMU14, Cha13a, CXWT19, DDD14, MCL\textsuperscript{+19}, PPTT15, SYV19].

Optimality [MM17a, SDM\textsuperscript{+12}]. Optimally [DSMM14, GT12]. Optimally-Fair [DSMM14]. Optimised [CMO\textsuperscript{+16}].

**Optimising** [EV10]. Optimistic [WA15, SEXY18].

Optimization [AEP18, KD19, WH17, Z\texttextsuperscript{+17}, FLZ\textsuperscript{+12}, GCG\texttextsuperscript{+18}, KHH10, PTK14, RF\textsuperscript{+13}, ZSM18, sCR19a]. Optimizations [ZAG19].

**Optimized** [ARH\textsuperscript{+18a}, AYS15, EKB\textsuperscript{+16}, GAB19, HGT15, LNL\textsuperscript{+19}, MBF\textsuperscript{+13}, MBR15, JS18a].

**Optimizing** [DWZ18, ZSM18]. Optimum [Oba11, YFF12]. Optional [PC16].

**OR-Proof** [FSX12a]. Oracle

[CBJX19, GLM\textsuperscript{+16}, HKT11]. Oracles [FZT14, FXS12a, GSW\textsuperscript{+16}, XLQ09, XQL11, YS12, YKC\textsuperscript{+11}, YLA\textsuperscript{+13}, ZYM18, LLY15, RG10, SYL13, WWYY11, YFK\textsuperscript{+12}].
Password-Only
[HQY+18, HQY+16, ZHH+17]. +physicist
| [Dya19]. +physio | [HT11].
| physio-behavioral | [HT11]. Pi
| [MR10, EHKK19]. Pi-Calculus | [MR10].
| PICADOR | [BGP+17]. PICARO | [PRC12]. Piccolo
| [IS12, Jel13]. picture | [SM13]. piecewise
| GMOGCC15]. PIN | [MDAB10, NSBM17]. Pinch
| [DG10]. PinMe | [AV18]. Pinocchio
| [PHGR16]. PIN | [AV18]. Pioneers
| [MDMJ17]. Pinning | [Men13b]. Pioneers
| [Oro16]. Pipeline | [PPG19]. Pioneers
| [MDAB10, NSBM17]. Pinning | [PPG19]. Pipeline-integrity
| [SM13]. Pioneers | [PPG19]. Pipelineable
| [CFL13]. PKDS | [BDM16]. Pipelined
| [HTC15]. PKE | [BDM16]. Pipelined
| [HTC15]. PKE-AET | [BDM16]. Pipelined
| [HTC15]. PKI | [BDM16]. Pipelined
| [KGO10]. PKZIP | [BDM16]. Pipelined
| [TLZ+17]. plain | [BDM16]. Pipelined
| [LW13b]. Plaintext | [BDM16]. Pipelined
| [BM15, LLY12a]. Plan | [BDM16]. Pipelined
| [LH11, LHC15]. Plan | [BDM16]. Pipelined
| [DK12b]. Play | [BDM16]. Pipelined
| [But17, Shp10, VGN14]. Player
| [GJO+13]. Pless | [Ayu12]. Ploos
| [PP11]. plus | [WXZ19]. PN
| [XNP18]. POB | [XNP18]. POB
| [SAA17]. Podo | [GH13]. Point
| [AK14b, EZW18, MH14, ZC13, ZM16, AKM+15, Kh18]. Point-To-Point
| [ZC13]. Point/Polynomial
| [ZM16]. Pointers
| [Lop12, FYM+13]. Points
| [SC12, Chm10, Lin11]. Poisoning
| [YWW10]. Polaris
| [YWW10]. Polars
| [BGP+17, HQY+16, ZHH+17].
[Mac14, GSGM16, Keb15]. PriSTE
[CXX+19]. Privacy [AKM+11, AKKY17, ABCL17, Ano19a, ABR13, ALL+18, ACM12, ABHC+16, BN14, BC16, BAI18, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DCA19, DTE17, ESS15, EKOS19, FGR+17, Fci19, Fri13, GZZ+13, HSMY12, HBC13, HXHP17, HXC+11, HK18, IEE15, JN12, JX+19, JP19, KM10b, KKK+18a, KL+19, KCC17, Kni17, KS12, KH18, LMGC17, LSBN14, LLG15, LCPD15, LNX15, LSY+16, LQD+16, MYYR13, MJS+19, MV18, Mor19b, MTM18, NSMS14, PD14, PSS+13, PPT12, PZPS15, PSD15, Pet12, PH16, RVH+16, RSR+19, RCP+18, RWLL14, Rohl19, RHLK18, RBH15, SS17a, SG12, Set16, SZDL14, SZTT18, SOF12, TMLS12, TMG13, VKK+19, VFFH19, WPZ16, WMC17, WZC18, WMY16, YJSL18, YY+17, YMI13, Yon11, YY17a, ZHW+16, ZM16, ZOSZ17, ZXL19, ZHW15, ZLDC15, ZHL15, ZTL15, vdG17, AR13, APMCR13, AIA+18b, ACK+10, BGE+18].

privacy [BC16, BBPD16, BP11, BAG12, CD16a, CXX+19, CMB19, CDF+10, DZC16, DZS+12, FH13, FMA+18, FZZ+12, GAI+18, HSH11, HKA19, HPL+19, IC17, IOV+18, JKL+16, JLC18, Kam16, KKKG10, KM14, LWY+10, LWYM16, LHL+18, LZD+19, LQ15, MZA+13, MGP10, MGB19, NJB19, OSP+19, PX13, PZBF18, QLZ19, RRL16, Sav16, Sch11, SSMS15, SLZ12, SYY+17, SCY15, SWW+17, SMS+16, Tan12b, UK+19, WLZ+16, WC16, Wan18b, WWW17, WS13, YSS+16, YXA+18, YY+19, YQL17, YNX+16, ZWY+13, ZDH18, ZZY+19].

Privacy-averse [WMYR16].

Privacy-Aware [BCF16, ARL13, MGP10, ZDH18].

Privacy-Based [BS13b].

Privacy-Enhanced [DTE17, ACK+10, YQOL17].

Privacy-Friendly [KCC17, ACM12].

Privacy-Preservation [LLG15].

privacy-preserved [SWW+17].

Privacy-Preserving
[ABCL17, BKL16, BKL12, CWW+14, EKOS19, GAI+19, HSH11, HKA19, HSMS14, PD14, PPT12, Pet12, RH16, RSR+19, RHLK18, RBH15, SS17a, TMLS12, TMG13, VKK+19, VFFH19, WPZ16, WMC17, WZC18, WMY16, YJSL18, YY+17, YMI13, Yon11, YY17a, ZHW+16, ZM16, ZOSZ17, ZXL19, ZHW15, ZLDC15, ZHL15, ZTL15, vdG17, AR13, APMCR13, AIA+18b, ACK+10, BGE+18].

privacy [BC16, BBPD16, BP11, BAG12, CD16a, CXX+19, CMB19, CDF+10, DZC16, DZS+12, FH13, FMA+18, FZZ+12, GAI+18, HSH11, HKA19, HPL+19, IC17, IOV+18, JKL+16, JLC18, Kam16, KKKG10, KM14, LWY+10, LWYM16, LHL+18, LZD+19, LQ15, MZA+13, MGP10, MGB19, NJB19, OSP+19, PX13, PZBF18, QLZ19, RRL16, Sav16, Sch11, SSMS15, SLZ12, SYY+17, SCY15, SWW+17, SMS+16, Tan12b, UK+19, WLZ+16, WC16, Wan18b, WWW17, WS13, YSS+16, YXA+18, YY+19, YQL17, YNX+16, ZWY+13, ZDH18, ZZY+19].

Privacy-averse [WMYR16].

Privacy-Aware [BCF16, ARL13, MGP10, ZDH18].

Privacy-Based [BS13b].

Privacy-Enhanced [DTE17, ACK+10, YQOL17].

Privacy-Friendly [KCC17, ACM12].

Privacy-Preservation [LLG15].

privacy-preserved [SWW+17].

Privacy-Preserving
[ABCL17, BKL16, BKL12, CWW+14, EKOS19, GAI+19, HSH11, HKA19, HSMS14, PD14, PPT12, Pet12, RH16, RSR+19, RHLK18, RBH15, SS17a, TMLS12, TMG13, VKK+19, VFFH19, WPZ16, WMC17, WZC18, WMY16, YJSL18, YY+17, YMI13, Yon11, YY17a, ZHW+16, ZM16, ZOSZ17, ZXL19, ZHW15, ZLDC15, ZHL15, ZTL15, vdG17, AR13, APMCR13, AIA+18b, ACK+10, BGE+18].

privacy [BC16, BBPD16, BP11, BAG12, CD16a, CXX+19, CMB19, CDF+10, DZC16, DZS+12, FH13, FMA+18, FZZ+12, GAI+18, HSH11, HKA19, HPL+19, IC17, IOV+18, JKL+16, JLC18, Kam16, KKKG10, KM14, LWY+10, LWYM16, LHL+18, LZD+19, LQ15, MZA+13, MGP10, MGB19, NJB19, OSP+19, PX13, PZBF18, QLZ19, RRL16, Sav16, Sch11, SSMS15, SLZ12, SYY+17, SCY15, SWW+17, SMS+16, Tan12b, UK+19, WLZ+16, WC16, Wan18b, WWW17, WS13, YSS+16, YXA+18, YY+19, YQL17, YNX+16, ZWY+13, ZDH18, ZZY+19].

Privacy-averse [WMYR16].

Privacy-Aware [BCF16, ARL13, MGP10, ZDH18].

Privacy-Based [BS13b].

Privacy-Enhanced [DTE17, ACK+10, YQOL17].

Privacy-Friendly [KCC17, ACM12].
Gil10, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLC10, IEE11a, Kia11, Lin14b, Sah13].

process [CWZL13]. Processing [JGP+18, SAKM16, SZHY19, TKMZ13, VKPI17, BKPV13, HWK+15, MS13b, PRZB12, WS14].

Processor [BH15, CLF+17, HKL+14, LB13, MBR15, RJV+18, YT16, YS15, ABDP15, BAB+13, BGC+13, KSH18b, SSPL+13, Tar10, KSH18a]. Processors [GFBF12, Gue16, SJLK18, RYF16].

Products [FDY19, VBC15, SR14, Ste15a, ZZM17, HLS18, Mon13]. Product [PRodACT].

Project-Based [FDY+19]. producer [CHL19].

Project [SPG+19, ANo14c, Rom11, ACK+10, SS10c, Wil18]. Project-Based [SPG+19].

Prominent [ABJ13]. Promised [HS11].

Proof [BDG+12, Bla12, CZLC12a, CZLC14, FSX12c, GKG19, Kuz11, LYY+18a, LYY+19, LW12, LYY+16, NLY15, SR14, Ste15a, ZMZ17, HLS18, Mon13, PPT15, VBC+15, WH17, ZCQ19].

Proof-of-Concept [GKG19].

Proof-of-Knowledge [Lyy+15].

Proofs [BBD18, BKG12, BC11b, BGB12, BCI+13, BDSG+13, CZLC12b, DKL+19, IW14, LNZ+13, Mau12, NTY12, RB17, Sav13b, WPZM16, AGHP14, KPP16, KKK+16, Li10].

Propagate [GWM16]. Propagation [SKS+18, WWC+11, YZLC12, CWXW16].

Properties [CCK12, CCKK16, DQFL12, FY11, HJJ+19, JS18b, JR13, KU12, Sch12c, CLCZ10, SAM+19b, WT13]. Property [HJJ+19, HEC+12, PR12, Rja12, YWM19, Bar19]. Properties [Ber12].

Protection [CTC+15, CKHP19, YMC+17, BVIB12, CDF+10, dCCSM+12]. Protected [BDGH15, SG15, AGBR19]. Protecting [BC15a, GSFT16, LLPY19, Mats10].

Program [AIM+19, BCHC19, CDD13, DCA19, EAAAb19, GST12, GPR+19, HXHP17, JP19, Lop12, NGahu1Q6, NDT+17, RR11, SEY14, SJ12, ZWWW17, AIA+18b, AT1+10, HLys14, HPL+19, KKM+13, KSI12, LZ11, WLYM16, LR1Y10, RS17c, TLL13, YWT+12, ZZY19].

proof-key [HLys14]. Protocol [ADSH18, BL12, BC14, BCM+15, BNH19, BSSV12, BFK16, BBKL19, CC14, CCM17, DCA19, FLH13, FHL0JR18, FMTR12, Fra16, G112, Hsv12, HC12, HL10a, HCP12, HCETPL+12, HKL+12, JTT+16, JHW+19, KMS19, KMO14, LNZ+13, LCCJ13, LNXY15, LYY+16, MBC15, MR10, PSS+13, SBS+12, SGCC16, SS15, TWC18, TYK+12, WT10b, XJR+17, YS12, YWF18, YLSZ19, YWZ+12, ZZX+11, ZSY19, AATM18, AMKC19, AQRR+18, AKG13, AIB+16, AIKC18, AN15, BDM18, BGAD12, CSD18, CWS11, CCMB19, CJP15, DLK+16, DDL15, EA12, EBAC17, EM10, FA14b, FIO15, GMSW14, GH15, Gop19, GLM+11, HPC12, HWB12, HL14, IC17, IOV+18, JK19, JKL+16, JXLZ15, Kim11, KO16, LLLS13, LDDAM12, LKKL13, LWS10, LXM12, LZ+19, LEW19, LY14, LML+13, NCL13, NLYZ12, NML19, OHJ10, Par12b, SSAa18, SPLHC14, SB17, SGJ+18, SWW+16, SSS11, SSPL+13, TG17, THA+13].
protocol [Tso13, TKHK14, VS11, WMC17, WYZ+17, Wan18b, WCFW18, WDZ19, WDV18, WZM12a, WZM12b, WLS14, WMYR16, WT10a, WTT12, WCCH18, XCL13, XHM14, YC12, YZZ+14, YVK+19, YMM13, YN19, ZWQ+11, ZTZ16, ZYC+17, ZXW+18, ZXWA18, ZG10, ZZZ15, ZX11, BOB13, CJP12, LFGGCRP14, Ste15b].

Protocols
[ADH19, AP13, ABHC+16, BMP12, BSBB19, CCK12, CCCK16, CMRH17, CCF17, CZCD18, CCD15, CCD19, CCD20, Con10, CM11, EFGT18, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KL08, KOS16, LY16, LHW+17, MV19, MS16, MT12, Mur16, NYR+14, NSM14, PS14, RB17, SBS+12, SBS18, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Anol13d, AKS19, ACC+13, ACM12, BJI10a, BK19, CML+18, CR10, CLCZ10, DGJN14, FTV+10, GBN11, GLR13, HSH11, HLS18, Ham12, HDPC13, HZW17, HST14, HWB10, KJN+16, KSU13, Ksl12, KKK+16, LDC13, LLY06, LKK13, MN10, NR11, Nos11, Nos14, SD10, WMU14, YSL+10].

Prototype [Bar16b]. Prototyping [KPC+16]. Provable
[BKLS12, CC14, EKB+16, Rog16, YLS18, YMS10, YY19, Z11, ZPXX17, FA14a, HRS13, LHH11, SYXW19, WB12, XCL13].

Provably [BCGAPM12, BCM12, BCM13, BCGS16, BHJP14, FHH10a, GLL+18, IIL15, LH11b, LDZ+14, LL16b, ODK+17, PS17, RMZW19, WMS+12, XLO99, XJWW13, YC12, YZZ+14, ZG10, ABBD13, FIO15, KC18, KKLW+17, LHDZ+19, LWK+19, SM10c, SXL16, XWXC14].

[DLN13, Gol19, HTZR12, KS18a, KS18b, MLL16].

Proving [Sar14, AGH+17].

Proximity [IW14, ARL13, Alp18].

proximity-based [ARL13]. Proxy
[ASS15, DHT+19, GSW+16, GJI15, GJ17, GZK19, HGWY11, HX15, KP12, LK18, LSW15, LAL+15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW+16, YMWS11, YCM+13, BGP+17, CLH+16, FSGW11, FSGW12, GH12, HWD16, HRY+18, KKM+14, LCT+14, LFS15, LL16a, LL16b, QMW17, SLZ12, SKB+17, Tia15, WHY+12, Wan18a, WXM19, WLS14, XWXC14, YZCT17, ZLY10, ZDW+16].

Proxy-invisible
[SYL13]. Ps [HDW12]. Pseudo [NN12, XYXY11, Zaj19, CFY+10, KM10a, MG15, PLs10e10, SH11, SM11, XSWC10, Zim10]. Pseudo-Random
[XYZY11, Zaj19, CFY+10, KM10a, MG15, PLs10e10, SH11, SM11, XSWC10, Zim10]. pseudonym [XHM14]. Pseudonymous [DFK12]. Pseudoprime [DW12].

Pseudorandom [AS17, BCG11, BK12a, Kla10, MFG16, CP13, GCH15, HR10].

Pseudorandomness [Shp03, Sha10].

PSMPA [ZLDC15]. PSO [TLL13].

PSPACE [JJUW10]. PTAS [JLX+19].

Public [Aiz19, Anol11b, ABW10, BVS+13, BB14, BM18, BKL12, BKKV10, CT18, CLP13a, Che15, CLN19, CNT12, Cou12b, EK10, FM12, GKS17, HEN+11, HWS+19, HCT+15, HLH19, IM14, JLT+12, JW19, KFOS12, LXY+19, LSW16, LG10, LHA+12a, LP10, LSQ18b, LZC14, LCP15, LH11, MZY15, M14, M14, MAT11, MPR12, Muf16, N12, O16, PDN15, RSBG12, RV+18, RW12, RBHP15, SGG18, Saa12a, Sch19a, SK12b, Seo18, SWM+10, Sia12, SC12, SLY+16, SGP+17, Svi10, TMC15, T12, WP17, WZ15, WWH12, Will18, WSQ+16, XNK15, XZ12, Xio12, XWW13, YL17, YKC+11, YFK+12, YMC+17, ZCZQ19, ZY17a, AA14, ATK+17, AK14a, AVA18,
Real-Time [AEP18, AYS15, GSC17, JWJ+17, PNRCL17, RHLK18, WLZL12, YE12, AC14, MK11, YE14a, NSX+18].

Real-valued [BNA15].


Reasoning [TSH14]. reboot [And19].

Rebound [KNR10, Sas12]. recall [LTC+15a]. recall-based [LTC+15a].


Recovery [Bro17, DSSDW14, DSSDW17, LYY+18b, LL19, MPA+18, NRQZ15, QJC+18, SAA15, SSSA13, WZ15, BM15, CHHW12, CGH17, MBP19, PX13].

Rectangle [CWZ19, WL15]. Recurrent [CSH+18, Pud12]. Recursive [LXYL12, WH18]. ReDCrypt [RHLK18]. Redesigning [VFV17a, VFV17b].

Redistributed [LXCM11]. Reduced [BW12, DWZZ12, KN10, LWZ12, LJ18, LYD+18, LS+19, LWPF12, vV16, AKY13, AY14b, DMSD18, LF+16].


Refractal [Hai17, OF12]. Reflexive [SRRM18]. refractive [PHN+12]. Refresh [LS15].


Rejewski [Kap13]. Rekeying [DT13, QLL17, CLSW12, DS11]. Rekeying-Aware [QLL17]. Related [AH19, CWZ19, Cil11, CMA14, DGI12, HLLG18, Pud12, WLC12, DGI12, GLMS18]. Related-Key [CWZ19, CMA14, HLLG18, Pud12, WLC12, DGI12, GLMS18].

Relational [HPC10, RPH12, WP17, BFG+14, BL11, GA11, JK13, PYP10]. Relations [BP11, FHS13, HLR11, WGD18, KGO10, LLM+19].

Relationship [CZ19]. Release [KFO12, KSBG12, Unr15, WSS12]. released [GSGM16]. Relevance [Sim15a].

Reliability [HSUS11, C14]. Reliable [AMKA17, ADG16, Bai10, CCI4, KMI18, MG19, MKAS18, WKB16, ACD+15, CL16, SM19a, ZC12]. Relying [TAKS10].
remapping [PSJ+13]. Remarks [SSU12].
remediations [ACC+13]. Remote
[BCE+10, BWS19, CS14, FMYM15, LZCK14, MHL18, Sar12, SYY+17, VMV15, WgMdZIZ12, WgMW12, CHS11, HU15, HL12, IB11, KKG14, LH10c, LNM+11, LNK13, LWK+18, LH13, MCL+19, MM12, Sar10a, WQZ+13, YSL+10, YN19, PZL+19].
motely [Wat14b, YHMM18]. Removing
[HKHK13]. renewable [URK+19].
Renewal [MMY12]. renewed [GPLZ13].
rental [LY14]. Reordering [Alo12].
repackaging [CBJY16]. Repair [SEK+19].
Repairing [BCM12, BCM13]. Repeatedly
[TAKS10, ATK11]. repeater [SPD+10].
replacement [LHM+10]. Replay
[SRRM18, ZLQ15]. Replay-Resistant
[SRRM18]. replicas [PZL+19]. Report
[jCPB+12, MT17, Zor12, GMT+12]. reports
[RPG12]. Repositories [Ano15a].
repository [RSN15]. Representation
[AGW15, BFMT16, GM16b, MMBS19, MC19, MH16, MHT+13].
Representation-Based [AGW15].
Representatives [Bla16]. reproducible
[CW12a]. Reproducing [Sod13].
Repudiation [LLG15, VBC+15].
Repurposing [GY13]. Reputation
[BL15, LHM+15, PAS13b, MGP10].
Reputation-Based [PAS13b]. Request
[KK12, KK13]. Request-Based-Revealing
[KK12, KK13]. Requirements [OS16].
Requires [Raz19]. requiring [KHHH14].
ResC [YFT18]. Rescue [TSH17].
Research [BNNM17, BA18, CDFZ16, FREP17, Roh19, SDC+17, SPG+19, WP15, BEB+18, GLIC10, Hof16, Pal15, Ven14].
Researchers
[Con12, Con17, Edw14, Wal18, Win17].
Reservation [LSY+16]. reset [RY10].
Resettable [CPS16]. Resettably
[COP+14]. Resettable-Sound [COP+14].
Residue [CS10]. Resilience [CATB19, NTY12, C JW+19, GLL+18, HYL+19].
Resiliency [YM16]. Resilient
[AV12, BKKV10, FPS12, HD19, HHS18, JP19, LTZY16, LD13, N YR+14, Pan14, PSD15, XZY+12, Y12, YNR12h, YCZY12, ZYT13, ZWT M15, ZM17, ZYY+19, ZYY19, ZY17a, ZYM18, ZYH+19, ABC+18, CAM19, CQX18, DLZ16a, GVI4a, KPS10, K om18, LLG19, MMSD13, SCBL16, SG P+17, Wan18a, YSJL14, YKC+12, Y LZ+16, ZY17b, ZYM19]. Resistance
[CGCS12, GZSW19, PRC12, WLZL12, ZJ11, DLN13, FIO15, X YML19]. Resistant
[BK12a, CDK+10, GV14b, HFI14b, SRRM18, WHZ12, WgMW12, WH17, YPRI17, FK19, GMRT+15, HCC10, PBCC14, VCK+12, WTT12, YKGK13]. resisting
[SXL16, Tam15, ZZL+19]. Resistive
[DSB16, TLF16]. Resistivity [MM17b].
Resolution [LHM+18]. Resonance
[LCR+18]. Resource
[CSH+18, CRS+18, HM19, JMG+16, JWNS19, SZMK13, YNR12a, ZSH+19, AMHJ10, FQZF18, KAS15, LLZ+16, MH15, Wan13, WZWX16, ZPZ+16].
Resource-Constrained
[CSH+18, CRS+18, YNR12a, LLZ+16].
Resource-Constraints [ZSH+19]. Resource-efficiency [SZMK13, W ZWX16]. Resources
[Bre18, IM16, Pau19, URK+19].
Respect [CATB19]. Respiratory
[RSCX18]. Response
[GH S14, HLLKL15, ZHW+16, MRT17].
Resprting [TBCB15]. REST [LNG19].
REST-Security [LNG19]. restoration
[WHZ12]. restricted [CLH+16]. result
[ACK+10, ED17]. Results
[DGIS12, LJF16, Hof16, KGO10, VSB+19].
Rethinking
[Che13, HU15, LSG16, MV16a, WYZ+17]. Retrieval
[BBB+16a, BTHJ12, CJP12, DS19, HK14b, JMG+16, JKHY12, Yek10, ZXZ+11, CJP15, SWW+17]. Retrieving
[Uto13]. returned [War11]. reusable
[RS17c]. Reuse [ABF12]. Reveal [Sta13].
Revealed [Ano15d]. Revealing [BT12, KK12, BKR19, KK13]. reverse [TQL+14]. reversed [KYH18].
Reversibility [FSX12b, HWYW14].
Reversible [CLF11, CSS+13, HHS+15, MM17a, MR16, NC12, AMK12, CT11a, HLC16, JK13, KKK+16b, MM14a, NC13, PWLL13, PC14, SM19a, TK14, WOLS12].
Reversibly [MKH+12]. Review [Ano15b, Ano16a, Ano17b, AY12a, AY12b, Ayu12, Bai12, Bar12, Cou12b, Dew11, Ful10, Gas13, Gre19a, Gre19b, Hom17, Joh10, Kat13, Keh15, Koh10, Led16, Lop15b, Low12, Mei10, Mou15, Mur10, Nag19, PMG+19b, Sch15a, Sha10, Ter11, Xie12a, Xie12b, IAA+19, JAS+11, MM12, TPTK12].
Reviewed [Sch15a]. Reviews [SR14].
Revised [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. Revising [BT12].
revision [LT14b]. Revisiting [GLMS18, RSD19, TLW12, WSA15].
Reviving [TLZ+17]. Revocability [WHIL16]. Revocable [AEHS15, CD16b, LNZW19, MML16, QZZ18, SE14, SE16, SZS14, SZDL14, TCL15, TT12, Unr15, FLL+14, JCL+18, LDZW19, WLFX17, WTT12].
Revocation [AEHS15, LLC+15, LW16, Lop15b, RDZ+16, XMLC13, YWZ+12, ATK11, LJWY18, WLWG11, ZYW+19]. Revoking [TAKS10].
Revolutionized [Orn16]. RF [VJH+18].
RF-Data [VJH+18]. RFID
[CJIP15, AATM18, AMKC19, BL12, BSSV12, BM11, CGCGPDM12, CCF17, CJIP12, Cho14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, GH15, GAI+18, HSH11, HDPC13, HQY+16, HQY+18, HCPLSB12, HECTPL+12, HWZZ19, JLTZ18, KNTU13, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLsvLE10, QZL+16a, QZL+16b, SBS+12, SPLHCB14, SBS18, SSKL16, TG17, WH17, WCFW18, YFT18].
RFID-Enabled [YFT18, QZL+16a, QZL+16b]. RFID-WSN [JLZ18]. RFID/NFC [Mic16]. RFID
[DMS11, MT15, ST16]. RI
[Sch15a]. Rich [CS12, GYW+19]. Richman [Xie12a, Xie12b]. Riddle [Fox13, KM15, KM16].
ride [GBC19]. ride-sharing [GBC19]. Right [Bro17, RCK17, SR12a, BBG+17, LHA+12b, Sch11].
Rightful [RR11]. Rights [LVRY10, SC19a, GLL16]. Rigorous [DK17].
Ring [CZCD18, GHPS12, HKL+12, LYY+16, XY18, YKBS10, YLA+13, ZZ14, ZGCZ18, DZ14, GCH+19, Hwa11, LYW+10].
RLWE-Based [GDLL18]. RNG [CGH17]. RNGs [DSSDW14, DSSDW17]. RNS [BEM16, CATB19, DBT19, GL19]. RNTS [PSOMPL13]. roaming [SCKH10, ZXL].
[SPW+16, VOGB18]. Robust [BCGAPM12, BCG12a, CFOR12, DKL+19, GKSBI7, HURU11, HZC+12, JSZS12, LSL12b, LSR13, MR16, MU12, MS16, MC11, nNyWyY+14, OCGD11, RR11, RMG18, SJ12, SS17b, SC12, SZZT18, TLCF16, TK14, TTL10, WLDB11, WgmDZ1Z12, wGwNyY+14, XNG+14, YWNW15, YH3W19, YYO15, YY13, ZWZ17b, AP10, AIA+18a, BWR12b, CLM+12, CNF+18, EAA+16, GZH12, HZC+14, HZL18, IOV+18, KMG17, KIH19,
LNK+18a, LW10, LZZ19b, PKS18, RS17c, yWpNyL11, yWpWyYpN13, WYZ+17, WHZ+19, YSL+10, ZHH+17. Robustness [HGT15, YKB10, AEH17], ROCA [Ano17], Rochefort [Car11], Rock [Cri16].
Rock-solid [Cri16], Rodney [DDS12], Rogozin [Kuz11], rogue [AYS14], Rule [GB19, PH12, ZVG16, HPJ+19, ZHV14].
Role-Based [ZVG16, ZHV14]. Ron [LHA+12b], Room [Sm11b, Pea11], Root [ARH14], ROP [ZHS+19], Rosen [HR13].
Rosenhain [CSLY14], Rotation [MM17b, SBS18, LWLW11]. Rotational [KN10, KN10].
Routing [Ber17, Round [Ber17], jCPB+12, COP+14, CJS13, DWWZ12, GGHR14, KOTY17, KMO14, LWZ12, LJ17, LJ18, LYD+18, LSG+19, Pan14, TYM+17, XZLW15, Yon12, AY14b, ABB+12, BlO5, DMD18, JK19, LP11, LF+16, Sun11, TSL11, TQL+14, TCS14, XW12].
Round-Reduced [DWWZ12, DMSD18]. Rounds [GST12, Ssa12, MYHH14, MNP12]. Router [M17, JLZ18, SA15].
Routing [ARWK19, Ham12, KZG10, WLY+15, LSG16, LC17].
Routing-Aware [ARWK19]. RSA [Dun12b, Kia11, Pie10, APPVP15, BBBP13, Bro17, BNS17, CCL+19, CLSW12, Chm10, GM13a, GST13, Her14, Hin10, HLY14, IK15, KV19a, KHHH14, KFL+10, Lim11, LFK19, MV19, MZ15, Moo12, PT19, PY19, SM10a, SM10b, SLM10, TK19, Win17, XWK+17, YHK+10, YXA+16, sCR19a].
RunStream [KPC+16]. Runtime [BJ10a, CLP+13b]. Rupture [KA18].
Russian [McG11]. Ryoan [HZX+18]. s [Sch15a, MM17b, NN12, RMP10, RMTA18, SS11, WJ19]. S-Box [RMTA18, RMP10].
S-Box/Inverse [RMTA18]. S-Boxes [MM17b, NN12, WJ19, SS11], S3BD [WS19]. SA [LHM14], SAC [JY14, MV12].
SDAT [SM12]. SAE [DLK+16]. SAE/LTE [DLK+16]. SAFE [DSL18, RQD+15, BL17, Gel13].
SafeCurves [BL17], Safeguarding [FGR+17, NML19]. Safely [HM12]. SAFER [YCL17]. Safety [OS16, BMM12, KO16, SAM19a]. said [Pro15]. Salsa20 [MAS16]. same [Con17].
Sanitize [PH12b], Sanitizers [YM19]. Sanjit [Kas13], Santa [MSH+16, Rab10].
Sanya [LTW11], SARFUM [BCE+10].
Sarkar [Kat13], SAT [Che18], satphone [DHW+13], SA15 [CDWM19]. SAW [CFH+13], sawtooth [Ye14], SC11 [LCK11], SCA [HF14b, PD19].
Scalar [ARM15a, NR15, YTS12, SKH15]. Scale [DM15, GU13, JKH12, LL19, LQD+16, And19, CG12b, dCCSB+16, DEL19, DLT19, FX12, GSN+16, SR10, VSB+19, ZZK17, ZV14]. Scaling [PPG19, YM18].
Scan [LWK11, DDFR13, KPS10]. Scan-based [LWK11]. scanning [Ara13]. Scattering [KA18], Scenarios [DSB15, HURU11, LWW+19]. Schedules [Pud12]. Scheduling
[DK16a, LJP17, MV16b]. Schema [AN12].

Scheme [ARM15a, ADM19, AMSPL19, ASS15, Bai10, BHG12, BS14, BKJP12, BDH11, CMLS15, CLL16, CCW+10, CLHC12, CHWH12, CCZC13, CCC19, CGY+13, CLH13, CSW12, DA10, DS11, DKS12, EAAAA19, FR16, FGM10, GZZ+13, GH11b, GJZ17, GLW12, GZH17, HYS11, HIDFGPC15, HM12, HWS+19, HLC+18, HHP17, Hul13, HLH19, HP12, IL15, JSZS12, JLY+19, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KLM+12, LSL12b, LHF12, LTH+15, LTZY16, LH11c, LSQZ17, LSQI18a, LGWY12, LCDP15, LTY+15b, LYY+18b, LGPLR14, MWZ12, MVVR12, MR+18, MMN12, MSA13, NNX12, NLY15, Pet12, PDT12, RVH+16, RSD19, RM18, SK12a, SSKL16, SJ12, SGP+12, SD12, She14, ST16, SWF+19, SP15b, SJWH+17, SSA13, Ten11, TTD13, TWZ11, WLY10, WGMdZ12, WGMW12, yWpNyY+14, WLH15, XWSW16, XHC+12, XJWW13, YMY16, Yam12, YXZ+12, Ye10, Ye14, YTH17, YLY+17, YHK+10, YMWS11].

Scheme [YY17b, ZPM+15, ZQZ+19, ZC13, ZQQ15, ZWZ17, ZM18, ZLDD12, ZY17a, ZGCZ18, AMN18, ARL13, AHS14, AKP+18, AKK+17, AM19, BC16, BDL+19, BD18, BDM+19, BOB13, BBB19, BAL10, BWR12, BMM12, BZD16a, BBB16b, CCLLI11, CLSW12, CNF+18, CH10, CT11a, CLHJ13, CW14a, CTH13, CBJY16, Cho14, DMY+19, DCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, FHZ18, FZZ+12, GZH12, GJ13, GMRT+15, GJ18, GPLZ13, GLM+16, GH16, GAI+18, GBC19, GTSS19, HKA+18, HZW28, HBBBM+16, HL12, HL11, HCCCI11, HLC16, HCC10, Hwa11, IB11, JNUH17, JKAU19, JLT+12, JZS+10, JMW+16, KFE19, KI11, KPP16, KDH15, KK13, KMB13, KKM+13, KKM+14, KKG14, KCS+18, Kim16, KKK+18b, KHi19, KPI8, KLY+16, KLY+17, KWD+17, KKD+18, KWH16, KLI11, LXLY12, LLZ+16, LSR13, LYE+10, LH10c, LYW+10, LZX10, LNM+11, LMQC11, LK12, LLH12, LNKL13, LDZ+14, LWYM16, LYY17+17, LNNK+18a].

Scheme [LVW+18, LNNK+18b, LWK+19, LFW15, LH13, LHH11, LWL10a, LWL11, LW13b, LZC14, LZZ19b, LDW19, LL16a, LLY12, MCN+18, MMS17c, MK12a, MGB19, MSA13, NR17, Nos14, NMX15, ODK+17, OSNZ19, OPS14, OSANAM19, PY19, PZBF18, QMC17, QMW17, RPSL10, SGGR+16, SM11, SYWX19, SCR19b, SMS+16, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWYZ11, WWYY11, yWpNyL11, WLH13, WDZL13, WLZ+16, WC16, WLFX17, Wan18a, WMX19, WXSH19, WHZ+19, WDKV19, WZ11, WKHI10, WLS12, WXK+17, XHH12, XWWZ16, XWXC14, XXX15, XWK+17, XTZ+19, XXCY19, XMHD13, YWJ+19, YCY11, YC16, YHMM18, YSQM19, WPK+10a, YCT15, YX18, YQOL17, YY13, YMSH10, ZYL+10, ZLY10, ZJX+14, ZYC+17, ZZZY+19, ZWY+19, ZPWW12, ZHH+17, ZY17b, ZHP+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12].

Schemes [AAUC18, ACA+16, ABF12, BVS+13, BF12, BBEPT14, BS15, CMLRHS13, CZCD18, CLND19, CGL+12, Chu16, Des10b, EFGT18, FHKP17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZK14, MLCH10, MR14b, MMS17b, MFB18, MKRM10, MKASJ18, OBA11, PB12, PDNH15, PH12b, Sch10, Shi11, SKH17, SU12, VSR12, WGF16, YNR12a, YNR12b, Yek10, YWZ+12, AGHP14, AN15, AHL+12, BK19, CDGC12, CXX19, CHS11, CCG10, CTL13, DDD14, DDI3, DZ14, FPBG14, FGMP12, FMA+18, HKA19, HWDL16, HM10, KTUI16, LW+19, LHY12, MM12, MBP19, MA17b, NZL+15, QYWX16, SES+16, Sar10a, Sar11, hSZZ15, SAR18b, WW14, YT11b, ZCL+12, ZCML14, ZT14].

Schneier [Sev16]. Scholarship [SPG+19].
Scholarship-for-Service [SPG+19].
School [Hom17]. Science
[Bow11, Gas13, IEE10, IEE11b, Nie02, Ter11, Bia12, PHWM10, Pet11]. scientists
[Goo12]. Scientometric [Pal15, Pal16].
Scope [Bai12]. Score [GCSAddP11, HW19].
screening (OSSK16). scrambling [Pau19].
Scrambling [LLL17a]. screening [DMSD18].
Screen [SPW+16, CTL12, IA+A+19]. Script
[Rao10, Bax14]. Scripting [DSB15]. scroll
[GMOGCCC15]. SDB [HWK+15]. SDDO
[PL16]. SDDO-based [PL16]. SDH
[GMS11]. SDIVIP [YNX+16]. SDN
[DHT+19, KCC17, YHSW19]. SDN-Based
[DHT+19, YHSW19]. SDVS [Wan10]. SE
[LLLS13]. SE-AKA [LLLS13]. seals
[MIN10]. Seam [LC15]. Seam-Carved
[LC15]. Search [AHN+18, CWL+14, Che15, DCA18, FRS+16, GTT11, HWZP18, HCDM12, HLH19, LSQ18b, SOR16, TMC15, WDC18, WW12, XWSW16, XJWW13, ZXY16, AH18, BZ16a, BTK15, BL11, CHL+19, DDD+19, FH13, FSGW12, GZS+18, HKA19, HH16, MRR+18, NJB19, OSSK16, PWS19a, SY15b, WHY+12, WXLY16, WMC17, WS19, XWY+18, XZT+19, XLC+19, YDX18, YQO17, YQZ+19, ZZ11, sCR19a].
Searchable [BHJP14, CWW12, CLW16, CGK011, FJH12, HKA19, PBC+17, PCY+17, XNK15, ZQZ+19, CLC+19, CXWT19, DLZ16a, DRD11, HQZH14, HK19, HTC17, JCHS16, LZZ17, LLL+18, MML16, RPSL10, WXLY16, WC18, YZT17].
Searches [Sia12, WR15]. searching
[GPN+12]. Seattle [LCK11, KCR11].
Seberry [AHS14]. SEC [PA10]. SecLAP
[AMK19]. SECO [DYZ+15]. Second
[AKY13, ABM+12, Gre19b, LGP19, SNG+17]. Secondary [RS11]. Secrecy
[ABD+15, BKST18, BCN19, KZG10, TSH14, Yon12, ABD+19, ATKH+17, Bia12, RCW15, TCS14]. Secrecy-preserving
[TSH14]. Secret [ASN11, ASN12, ADH17, Ayu12, Bai10, BBB+16a, BM12, BBEPT14, BP06, BCDN17, BCND19, Bri11, BLU+15, CCM+15, CFR012, CCL+13, DR12, Dew11, EMI12, EA11, FHKP17, FR16, Fok12, HYS11, HL10a, Has16, HZ+18, JLS12, KU14, KS18b, KOTY17, KK12, KK13, KSSY12, KS15, LKBK19, LHF12, LPI15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Oba1a, PCPK14, QS18, SLL10, SC10, SS10c, SSI12, Sst15, TLW12, TWZ11, WKB16, WGF16, Wil18, XYZ+12, XJR+17, YFF12, YWZ+12, ZCI13, Ald11, AIM+19, ADG16, AKK+17, Ara13, AGBR19, BJ16, BGB+18, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEAZ13, EZ15, FH10a, GEAHR11, GJMP15, GLW13, HF14a, HH15, Hea15, HBB16+16, HCC11, HLC12, KFE19, KI11, KU16, LXY12, LHL11, LT13, LyWS10, LHYZ12, LEW19, Mas17, McK10, McK11, Mc12].
secure [MBB11, OOI10, Par18, Pea11, Pet11, QD16, Rus15, SB17, SA12, SAR18b, SM10c, TQL+14, TD14, UUN11, UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, WX13, YC11, YCC16, YSC12, ZZ15, ZP0Y12, LSC+15, Bai12]. secret-key
[BJ16]. Secret-Sharing [BBEPT14].
Secretion [RSC18]. Secretocracy
[Ber16c]. Secrets
[BT12, CG14b, DLWW11, FMS12a, Kob10, Man13, Bha16, Cop06, Cop10b, GGH+16b, Gup15, HRS13, LDC13, Sm11a, Aon17b]. SECURE [Aon19a]. Section [Bd19].
Secure [ADM19, AMKC19, AAL19, Alz19, ACA+16, ADMM16, ABPP16, ABL+18, AAR12, Ash14, AMH+16, BS+13, BWLA16, BCGH11, BCG12a, BCQ+13, BWA13, BJL12, BHJ14, BF11, Bru12, BDH11, BEM15, CFR12, CCM17, CZF12, CZLC14, Che15, CDWM19, CMA14, CDLW19, DM18, DL15, DMS+16, DG15, DYZ+15, DLZ+16b, Edw17, EAB+19, FLH13, FYD+19, FMC19, Fri10b, FD11, FSX12a, GQH17, ZGXW12, KGM16,
GGHR14, GFBF12, GT12, GV14b, GHKL11, GM14, GZS+18, HsV12, HSM14, HLLG18, Har16, HL10b, HP14, HTZR12, HMCK12, HLC+18, HLKL15, HYS18, HK14b, HLH19, IL15, Jac16, JKA+18, JHW, KL14, KME+12, KH+11, KVEY+18, KD19, Kip15, KH10, LJS+14, LL15, LH12, LYZ+13, LTH+15, LTZY16, LSL15, LSL19, LLG16, LSQ18b, LY15, LHR15, LWML16, LLL12, LSC12, LMO17, MMP14, MDHM18, Mal13, MVVR12, MMS17b, MGJ19, MK12a, MKAA17].

Secure [NBZP17, NGD+17, NR12, NMS14, NSMS14, PB12, PSM17, Per13, PBC+17, PRN+19, QZL+16b, QZDJ16, QZZ18, RC18, RPM10, RR17, Rea16, RMZW19, RSGG15, RS19, SAM+19a, SNJ11, SSKL16, ST19, SZ14, SVVC15, SP15b, SKH17, SS15, SRAA17, SAR18b, SSAF11, SVG16, SYW17, SYC+17, SMS14, SZDL14, SGH15, SLY+16, SR12b, SM18, TB18, TGL15, TWZ11, TG12, TGC16, VT18, VM15, WgM12, WKB16, WXLY16, WLY17, WDC18, WDZ19, WHL15, WBA17, WWHL12, WS19, WMS+12, tWmC12, XWSW16, XLQ09, XJWW13, XLP+18, XHZ+19, YNRI2a, YNR12b, YTH17, YQZ+19, YHK+10, YKC+11, YAM+15, YY17b, YGD+17, ZZ+11, ZDL12, ZDH18, ZVH14, ZVG16, ZHT16, ZLW+17, ZHZ+19, ZBR11, AHS14, APK+18, ABBD13, AC16, AKK+17, ACD+15, AYSZ14, BMDT19, BOB13, BHIH19, BDZ16a, BKR19, BSR+14, CCLL11, CSD18, CLHJ13, CW14a, CS11, CD18, DA18, DEL19, DMM10].

Secure [DGCL19, DMD18, FHHL0a, FLL+14, FSGW12, FAI4b, FI015, FLYL16b, FS18, Gal13, GAI+18, GLL+18, GCH15, HGWW11, HKW+15, HLYS14, HTC17, HPY10, IB11, JZS+10, KPP16, KKA14, KRM+10, KCS+18, KTUI16, KLW+17, KDW+17, KKD+18, LLLS13, LDDAM12, LH11b, LLW16, LSR13, LHM+10, LDZ+14, LWK+18, LZD+19, LZW19, LWK+19, LCT+14, LAL+15, LIY16, LHH+18, LL16a, LL16b, LBOX12, MR14c, MHY+18, NR17, NACLR12, NAL17, ODK+17, OSNZ19, OSANAM19, PABC+19, PSiO+13, PLSvdLE10, PWS19a, PY19, PPB19, Rao17, RG10, RYF+13, RITF+11, RS15, SGGCR+16, SYL13, SWW+16, SSS11, SM16c, SSPL+13, SXL16, SLX16, SC19b, Tar10, TLLM13, THA+13, TLL12, VS11, WLZ+16, WMX+17, WXMZ19, WHZ+19, WDKV19, WCH18, WL19, XWWC14, XXX15, XZP+19, XMY+17, XKW+17, YXMY19, YC12, yYqWqZC13, YZZ+14, YZCT17, YQQL17, YY11, YLS12, YJC18, YMSH10, ZLY10, ZCLL14, ZZ15, ZQD16, ZYC+17, ZG10].

Secured [ZZ12, ZX11, ZY17b, ZC12, Zhu13, ZZL+19, ZSW+18b, Ano12, DSDL18, HRK18, OKG+12, YSS14, YFK+12]. Secure-TWS [OKG+12].

Secured [LC17, SGG18].

Secure [CC10, KP17, LHL+14, MS16, WXY+17, BC18, der10]. SecureMR [DMD18].

Securing [AASSAA18, BK12b, CMLS15, CST+17, Cla18, NPH+14, PMZ13, SFE10, SMSK18, SWF+19, SL11, Ste15b, TKR14, YMA17, YT12, WYY+19, CR10, Din10, GH15, SKS+18, SA15, Tox14, WYZ+18].

Securities [WWL+14]. Security [ABJ13, AHN+18, ASBdS16, Ano13f, Ano15a, Ano15d, Ano19a, AFB12, AN15, ABHC+16, ABB+19b, AYS15, BCE+10, BSBB19, BA18, BCM+15, BCL19, BRT12, BPR14a, BPR14b, BLS12, BCGN16, BDPS12, Bra15, BDH11, BP10, CFST17, CF16, CBX19, CHS11, CFXY17, CCD15, CDD19, CDD20, CPS16, CM11, DDS12, Dan12, DR12, DK16a, DFKC17, Elb09, FREP17, FMA+18, Fid18, FMA+19, FP19, FSX12b, FSX12c, GN16, GZZ+13, GR19a, GPR+19, GSC17, HC12, Hel17b, Her19, HB17, HUS11, HLW12, HXC+11, HLCL11, HLT+15, HLN+10, IEE15, IS12, IGR+16, JN12, JSA17, Jia14a, KBL11, KS18b, KFOS12, KSD+17, KD12b, LPS12, LST12,
Security [MCS+15, MH14, Mau12, MV16a, MGG+19, MLBL12, MPM+17, MHMCS16, Nac12, NNAM10, NDG+17, NVM+17, Nos11, Nos14, OSH16, Orm16, Osi16, Pas13a, PZPS15, PGLCX17, PDNH15, PS14, PL16, PDT12, PNRC17, RB17, RCP+18, RVS+18, RQD+15, RZW12, Rog16, RS10, SGG18, SN10, SNJ11, SBS+12, SBS18, SPD+10, Sar12, Sch13, SD12, Shi11, SCI19a, SLM10, STC11, Sti19, SSP19, SAM+18, SMOP15, SCGW+14, Tso13, TV15, VFFHP19, Wal18, WYCF14, WSA15, WZC16, WRP70, WSS12, WHL17, WCL+18, WS14, Yn10, YZC12, YSF+18, YHS19, YGS+17, YYK+17, YSS14, Yon11, YYW19, Zha15b, ZM18, ZXL19, ZYY19, ZY17a, ZYH+19, ZCZ+19, vTJ11, AMN18, AB10a, Abe10, ABGR13, And19, ABM+12, Ano11a, AM19, AGBR19, ADH17, BYL10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTHP13, CLCZ10, CVG+13].

security-boosted [LJP17, LMS16, GHD19].

security-enhanced [AMN18].

security-modified [MM14b].

SEDURA [LY15]. see [PZ15]. Seed [AS17, LHYH14, S11]. seeing [Tox14].

seen [Goo12, PWS+19b]. Segment [WOLP15].

Segmentation [WYW+13, ZZCJ14]. selectable [GLM+11].

Selected [DDS12, Dan12, MV12, BY10, JY14, LH10a, vDKS11, JY14, MV12].

Selection [K014, KD12a, KD19, RP12, SEY14, YKA16, DRN16, FXP12]. Selective [BTHJ12, GDCC16, JSA17, LW12, LSC+15, LZZ12a, LLH18, PWS+19b, LZZ14, LW13c].

Selective-Opening [LLH18]. Self [Cer18, CLL16, CHHW12, CSV15, BM18, HZ11, LCL+17a, LLPY19, LH12, LH14, PRGBSAC19, RCK17, SAA15, SM12, TAP19, WHZ12, WXW14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11, YN19].

Self-adaptive [LHM14, FXP12, SH11].

Self-authenticating [Cer18].

Self-Authentication [HL12, LT13].

Self-Certified [CLL16, WXW14, HL14, LH13, YN19].

self-composition [AGH+17].


Self-Recovery [SAA15, CHHW12].

Self-restoration [WHZ12]. Self-Sovereign [TAP19].

Self-Synchronized [BM18, PRGBSAC19], Self-Synchronizing [HZ11].

Self-Updateable [LLPY19, LCL+17a]. SELinux [SFE10].

seller [KJN+16]. Semantic [DDY+19, MHW+19, YZC17, HL11, HTHC17, JS18a, W8319].

Semantic-aware [DDY+19].

semanically [PPB19, SL16].

Semantics [CM11, Gl12, KGR12].

Semi [AAA+19, BDOZ11, KKK+16, SEK+19, WHZ12, XZLW15, ZHS10, PGLL10].

Semi-automated [KKK+16].

Semi-Autonomic [SEK+19]. Semi-Fragile [AAA+19, ZHS10, WHZ12, PGLL10].

Semi-homomorphic [BDOZ11].
shareable [XWY+18]. Shared
[DRD11, LNXY15, NSP+18, OKG+12, TYK+12, XJR+17, YJSL18, GEAH11, LDC13, Par18, PZPS15, SA12, TG12, YYS+16, YNX+16]. shared-secret [SA12]. Shares
[BLU+15, CFOR12, KU14, SA16a, WY12, AIM+19, LJY16]. Sharing
[Bai10, BFM12, BBP14, CCM+15, CFOR12, CCL+13, CVP14, CLW16, DR12, EM12, FHKP17, FR16, HYS11, HLI0a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KS15, LYZ+13, LPL15, Lin15, LCCJ13, LTY+15, LLKA19, NS12, Oba11, PSM17, QZZ18, QJC+18, SC10, SSU12, SZZT18, TIL12, TWZ11, WYCF14, WK16, WGF16, WHLH17, XNKG15, XZY+12, YFF12, YWZ+12, ZC13, AKK+17, ADH17, CD16a, CT11b, CW14a, CLC+19, EZ15, EA11, FGMP12, GPLZ13, GJMP15, GLW13, GLB+18, GBC19, HF14a, HBRMN+16, HCCC11, HLC12, HYF18, KFE19, KU11, KTV16, KPB17, LXY12, LH11a, LT13, LFWS15, LAL+15, LyWSZ10, LHYZ12, LHIL15, LLY+18, LEW19, LLI16a, Mas17, O010, O018, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WLWG11, WMC17, WMXZ19, WHZ+19, WZ19, WLS14, WKH11, WS12, WOLS12, YC11, YCC16, ZCL+12, ZZ15, ZPYW12, SLL10]. Shell
[WZCC18, YSS14, Tay14]. Shemanske
[Gre19a]. Shenzhen
[IEE11a]. Shield
[NDG+17, KGV16]. Shift
[AKP12, TAP19, ZHI15, KKM11, LKW11]. Shift-Type
[AKP12]. Shifting
[YWW10, CSS+13]. Shih
[Joh10]. Shilling
[CZ19]. Shopping
[ASH13]. Shor
[HL18, NMN+16]. Short
[GH12, CWWL12, FR15, NR12, SKV12, WQZ+16, XLM14, JSMG18b, LLY15, LJJY16, RD17, ZPWW12]. Short-Output
[NR12]. Shorter
[HL13, PPB16, TH16]. Should
[Bel15, Eve16]. shown
[Ana14]. shows
[Goo12]. Shparlinski
[Sha10]. Shredder
[AMH+16]. Shredding
[AMH+16]. SHS
[Ano12]. Shuffle
[HMR12]. shuffler
[BVIB12]. Shuffles
[CKLM13]. shunned
[Ree15]. Sicily
[Cra12]. Side
[AMMV18, AN17, Bar16b, BHC19, BCQ13, Bul18, CFE16, CDK+10, CBL13, CATB19, DZS+18, DMWS12, DKMR15, EWS14, GZSW19, GWM16, GPT14, KOP12, LWML16, LFK19, NDC+13, PRC12, SG15, SR12a, Vua10, YL17, ZBP18, BVIB12, CAM19, DJL+12, GSAV18, MCL+19, MFH13, SG19a]. Side-Channel
[AMMV18, Bar16b, BHC19, Bul18, CBL13, CATB19, DZS+18, EWS14, GWM16, GPT14, KOP12, LWML16, NDC+13, PRC12, SG15, YL17, ZBP18, DMWS12, GZSW19, LFK19, BVIB12, GSAV18, MFH13]. Sided
[HP14]. Sieve
[VM14]. sieving
[SD17]. SIFT
[KLY+12]. Sign
[ACC+13, LL15, MEF012, SPM+13]. Sign-On
[ACC+13, LL15, MEF012, SPM+13]. Signal
[GDLL18, Kar12, BLM+19, MS13b, RITF+11, EM19]. Signals
[Col17, Fyo19, LJK17, XNRG15, AIA+18a, AIA+18b]. Signature
[Ano13c, ABCF12, ASS15, AEHS15, BHG12, BDH11, CZZD18, CLND19, CGY+13, EFGT18, FGM10, FR15, GJJ15, GJZ17, GMSV14, GHTY18, HXZ15, HOF+15, HHP17, H113, HP17, JL16, LKL18, LT+15, LDZ16, LYY+16, LGPRH14, MMN12, NNX13, PH12b, ST16, TTH15, WZXL12, WLI15, WYLM16, WHLH16, XLQ09, XLM14, Y+17, YHK+10, YWSS11, YLA+13, ZJ14, ZLH+12, ZSY19, AGHP14, CLSW12, CGG10, Con17, DZ14, DXWD16, DLN13, HYS11, Hwa11, JZS+10, LHM+10, LDZ+14, LWZG10, LL16b, Nos14, QYWX16, QMW17, QCX18, RSM15, SLM10, VS11, WSC14, XLWZ16, YWL+17, YLS12, YKC+12, ZLY10]. signature-based
[DLN13, QMW17]. Signatures
[Ano15a, ABC+17, AYS15, BBC+13, BFSK12, BHH+15, But17, DMO+19, Fuc11, Gy13, GdM16, HHS18,
HS18, Hül13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, Orm16, PST13, TH16, Ver17, WCD19, YT16, ASVE13, AYSZ14, BDL+11, BH19, BPP10, GCH+19, GMS11, HAGTdFR13, Her14, LLY15, LJY16, PPB16, SEXY18, Tia15, ZQWZ10, Mou15.


Small [BGJT14, BKLS12, BB10, CJ13, HJ19, Kim15, LCLL15, NR15, WCXZ17, YM16, YT16, AAT16, BGJT13, Jou13, MZ15, PT19].

Smart [AN17, ABCL17, BMH17, BD18, BSJ15, DLZ+16b, HXHP17, HCL+14, HK18, LHF18, LA10, MFG16, PDT12, VJH+18, WgMdz12, WgMW12, AMN18, BC16, Bel18b, CHS11, CLHJ13, CHH+13, DZC16, GHD19, GAI+18, Ham19, HCC10, JZU+19, LH10c, LNM+11, LXMW12, LNLK13, LNK+18a, LZD+19, LWK+19, LTC+15a, MM12, MCN+18, SSSA18, SYWX19, URR+19, WMYR16, YZZ+14, YSL+10, YY13, ZGL+18b, ZhDUH18, ZZYZ+19, Cho10, GLIC10, SD12]. Smart-Card-Based [HCL+14]. SmartEdge [JZU+19].

Smartphone [MDMJ17, uHAN+18, DL15].

[CJZ13]. Spy
[AHS13, FKO15, Bha16, Goo12]. Spying
[VWC19]. SQL [BS13a, Suc12]. Square
[ARH14]. Squares [KÖ14]. Squashing
[GH11a]. SRAM [KLM+12]. SSD
[LGLK17, MP+18]. SSH
[YSS14, Cri16, Lit14, Ran10, der10]. SSL
[BJR+14, Dav11, FHM+12, GI+12, HREJ14, NPH+14, PP+11, Tay19]. SSL/TLS
[BJR+14, Dav11, PP11]. SSL/TLS-based
[PP11]. SSO [MLM16]. St
[DDS12, Dan12, MNS11]. ST-Numbering
[MNS11]. stack [JSM+18], stage [Masi17], stakeholders [RR16]. STAMP [WPZM16].

Standard [Ano12, Ano13c, App13, ABC+17, BCM12, BV11, BV14, CT18, GJJ15, GJZ17, HZX15, LYX+19, LK18, LDZ16, Loe15, MVVR12, NIS15, OKC+15, RSD19, SZS14, TCL15, WWH12, You12, ZC13, BCM13, HTC17, Kim11, LST12, LL16b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, ZCL+19, AEH17, MKRM10, NdMMW16, SJ19].

standardisation [EM19]. Standardising [EM19]. Standardization [TRD11].

Standardized [BLN16]. Standards [BCM+15, Che17, DHW+13, NIS13]. start [Rom11]. starts [Sch16a]. State
[BVS+13, BL17a, BL17b, But17, CG14a, CCL+13, CHS15, Dew11, DP17, FHR14, LK18, MK+16, OMN+19, Sen17, WGD18, XZY+12, YM18, BBDL+17, CK11, CG17, Ham12, Mid10, QD16, Sir16].

Stateful [BVS+13, NTY12, VKP17, VSR12, YLL+18]. Stateless
[BHH+15, GM11, MKAA17, NTY12, VDO14, BBPD+16, DCAT12].

Stateless/Stateful [NTY12]. statement [NIS13]. Static
[DKMR15, IF16, Lan11, TLLM13]. Station
[LY+16, Smi11a]. stationary [ZLDD12]. Statistical
[Böh10, Bro11, DBPS12, HZ11, Hey17, LTKP16, OOR+14, SP13, Sim15a, GMT+12, SA19]. Statistical-Attack

[SP13]. Statistics [gWpNyY+14]. Statutory [PH12b]. Stealing
[WRZ12, VWC19]. Stealthy [BRBP13]. Steering [HR13]. Steganalysis
[Böh10, DA12, Fri12, JHNN12, KDI12, LJK17, LC15, SG+12, Tan12a, YLL+12, Y114, YPRI17, BS11, LH13, LSQ11a, LSQ11b, Sch12a]. Steganalysis-Resistant
[YPRI17]. Steganalytic [Ber18, YPRI17]. Steganographic
[DA10, HHS+15, LyWZ12, WP15, AGL16, LLC10, CAIC14]. Steganography
[AAA+19, AGW15, BCG12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZW+14, JG10, KTM19, LJK17, LLY+12b, MAL10, PDM12, Paul10, SK12a, SR12b, TIZF12, WWL+14, WYL18, WYZZ12, YWW10, ZSA12, AOT13, BS11, BDK11, BCDL11, EEA13, GCK11, KKK+18b, LyWSZ10, LRW13, LRW17, LWW+10, Maz13, MS1+18b, MS17, PHN+12, PMG19a, SAM+19b, SI12, ST15, Sun16, WKH11, WOLS12, ZMS14].

Stego [YLL+12, SMSK18]. Stego-Image [YLL+12]. Stellenbosch [BL10]. step
[AKY13, YXA+18]. Steps [Ano13c].

Stereotypes [Söd13]. Stern [ACD18].

STES [CMLS15]. Steven
[Ano16a, Led16, Sch15a]. Still
[RAZS15, UK18]. Stochastic [ADR18].

stolen [Bha16]. Stopping [Sav13a].

StopWatch [LGR14]. Storage
[BCQ+13, CW16, CCT+14, CLW16, CDL19, DKL+19, GLG12, HSM14, HLC+18, JSCM17, Kip15, LCK11, LMD16, LW14, LDP15, PBC+17, QL17, SKH17, WLL17, XNK15, YZZ19, YJS18, ZDL12, ZG16, AY14a, AKK+17, BP10, CFV16, CFZ+10, CLH+16, CDF+10, CD18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, SSL+19, Sar10a, SY+17, SWW+16, SWW+17, W13, XWK+17, XYM19, YYS+16, YZCT17, YJC18, ZYC+17, ZVH14].

store [KV19b].
Stored [CMLS15, RSN14]. Stores [BCK17, GYW+19]. stories [Smi15b, ZMYB17]. Storing [DLWW11, HK19, LZC17]. storm [ACM12].

dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DEL19, DZS+12, Eis10, FXP12, GOMO GCCC15, GHD19, GSN+16, GPVCdRO12, HZWZ18, JSK+16, HHCC14, KSA16, LCL+15, LWK+18, MDHM18, MLMSMG12, MGP10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRR+12, SMS+16, WDG19, WS14, YSM14, ZAAB17, ZGL+18b, ZHI14, MA17b, MMKP16, ANo11a].

Systems-on-Chip [KS18a].

Systolic [MCDB12].

Systolic-Array [MCDB12].

SZK [MX13].

T [SJWH+17].

T-Chain [SJWH+17].

Table [CCL+13, AY14a, LDDAM12].

Tables [PTT16, XHM14].

Tackling [USH19].

Tag [NNAM10, PPH12, CJP15, SPLHCBI4, CJP12].

Targets [MO12, HSH11, HDPC13, HQY+16, KNTU13, LEW19, MK12a, PLsvLE10, TG17, WCFW18].

Tailored [Kni17].

Taipei [Yan11].

Taiwan [Yan11].

Takes [Ano16d].

Talking [FD11].

Talks [McG16].

Tamed [NXB13].

taming [BBDL+17].

tamper [CBJY16, KKK+18b, MN10, NC13, WGMW12].

tamper-evident [MN10].

Tamperable [ACM+17].

Tampering [ABA119, CG14a, QJC+18, SRAA17, HYL+19, SGP+17].

Tangible [LFH18].

TAO [Sta13].

Taormina [Cra12].

Tap [NM18, ADG16].

Tap-based [NM18].

taps [GSAV18].

Target [CZ19, APMCR13, HRS16, LSQ15].

target-driven [APMCR13, LSQ15].

Targeted [ABJ13].

Tasks [Abe12, FKS+13, LJP17, CL16].

Taxonomy [AJA16, GAF+15, KMSM15, HAGTdFR13, MA17b].

Taylor [Joh10].

Tc [XLC+19].

TC-PEDCKS [XLC+19].

TCC [Cra12, Lin14b, Sah13].

TCP [DHT+19].

TEA [CWP12].

Teaching [GY13, SCMS18].

Team [LJS+14, Ph10, Ant14].

Tear [Boy16].

Tear-Free [Boy16].

TEASE [ZBR11].

tech [Ano15c].

Technical [Sir16, TS16b, Wag16, Bon19, JW14, Suc12].

Technique [HEK18, KBL11, ZLDD14, BBBP13, CPPT18, GCSAdP11, LH11a, Nam19, SM12, ST15, SKS+18, TS16a, ZWS+18].

Techniques [Bis17, DA12, GOS12, HPC10, HL10b, KD19, LW12, Mor12, PJ12, VV18, AB10b, BM13, FGPGP14, Gil10, HT13, KHF10, LH11b, OO18, SM19a, VN17, WMX+17, Joh10].

Technologies [ATD17, GB19, Int19, RC18, SJZG19, JAE10, JAS+11, Lan10, MMP19, Ano16a].

Technology [Ano19c, AHWB20, CGB+10, Eya17, Fol16, IEE11a, MZLS18, TBY17, VFS+19, Wu16, Ham19, IMB17, Pec17].

telecare [LWK+18, MA17b].

telephone [GMMJ11].

Telepresence [NSP+18].

Television [DTE17].

Tell [Cer14, Pec17].

Template [NGAuHQ16, SKV12, XYY+17, AJYG18, ATI10, GCSAdP11, SCI19b].

Templates [DWB12, AYH+18, AGBR19, LH14, QLZ19].

temporal [DZC+16, JM12+16, MHT+13, XMDH13].

temporal-credential-based [JM12+16, XMDH13].

Tenant [TV15].

Tensor [FYD+19].

Terabit [LGP19].

terahertz [WW13].

Term [SKV12, vG17, CFVP16, VBC+15].

termination [SRB+12].

TERMinator [MTM18].

Ternary [ADI11].

Test [CHH+19, HTC+15, JEA+15, LLSW16, MZH15, SS10b, WH18, WZCH19, HTC17, ZCQ19, ZCL+19, Ano16i].

Testable [RMP10].

Testbed [BNN19].

tester [RPSL10, SY15b].

Testing [BCG19, Cou12b, DB16, SS12a, Ay14a, BR+14, GR19b].

Tests [GLG12, MS12b, Sim15a, YM18].

Texas [IEE13].

Text [GA19, GDM16, SMSK18, XZZ18, CR12, HAK19, SH12, SWW+17, ZMY17].

Text-dependent [GDM16].

Textbook
[PP10a]. Texture [TSH17]. textures
[NSX+18]. thanks [CBL10]. Theft
[Ber12, Ber17, BTPLST15, ZMYB17]. Their
[CZLC12b, CK18, FVJ19, HR19, JS18b, JSK+17, NR12, ZYY19, CQX18, FLYL16a, Hof16, IK15, KK10, Mat19, Stil11]. them
[HLV10, JSDK+16, Nor17, Rus15].

Theological [SS10c]. Theorem
[Lau12, HF14a]. Theorem-based
[Lau12]. Theoretic
[ADH19, CVM14, MAL10, WSS12, CDGC12, GLM+19, SD10, SKEG14].
theoretical
[KL13, ZZ15, Gas13]. Theoretically
[TWZ11, DGL19]. Theories
[ABR12]. Theory
[ACM10, ACM11, AAUC18, CCKM16, CDFZ16, CDFS10, Cra12, FGM10, FBM12, FS15, Gre19b, Hes12, LW11a, Lin14b, Nac12, Per13, PJ12, RZ19, RBHP15, RST15a, RST15b, Sah13, SAKM16, Sha10, Sp03, Wes16, Yan10, Abe10, AB10b, Bul10b, CFR11, Gil10, LPZJ15, MZA+13, McG11, YTM+14, Cra12, Lin14b, Sah13, vDKS11].

Thinning [Taj16, JGX+19]. Thin-client
[JLX+19]. things
[FOZF18, AAC+16, AKS19, BCHL9, Bel18b, CLF+17, CCMB19, FREP17, FMA+19, GMDR19, HKA+18, Hum19, HZL18, JKAU19, KHGG19, LNK+18b, LW19, LGH+17, NLLJ12, NLY15, PLGMCdF18, SB17, SXH+19, SS19, SY+19, VWC19, WCCH18, XLC+19, YCT15, ZDZH18, ZSY19]. Third
[jCPB+12, OSH16, QZL+16b, Sen10, BL10, ED19, Kip13]. Third-Party
[OSH16, QZL+16b]. Third-Round
[jCPB+12]. Thirteen
[AP13]. Thomas
[Gre19a]. thou
[BDK11]. Threat
[CSYY18, ALL+18, Ven14, ZMYB17]. Threats
[AJA16, ERLM16, GSC17, JLS+14, vdG17, TKG+17]. Three
[AMSL19, CZ15a, HXC+11, LLY+18, LZC+12b, OSANAM19, PC16, Shi11, YKNS12, AIB+16, CNF+18, HWB10, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14]. Three-Dimensional
[LLY+18, LZC+12b]. Three-Factor
[AMSL19, HXC+11, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b].

three-party
[HWB10, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].
Threshold
[CT11b, Cil11, FGM10, GLW13, HEP+11, HYS11, LW10b, LYY+16, SSU12, Sta12, Tan11, WYCF14, WLH15, XLQ09, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, HH15, JSMG18b, LJY16, OO10, QD16, SES+16, Shy15, SGM16, TD14, ZXJ+14, ZPWY12].

threatening
[PC14]. thrive
[Sch12b]. Throughput
[HMKG19, MAK+12]. Thru
[SYC+17, SYW17]. Thwart
[JLS+14]. Thwarting
[LWML16, XTK10]. Ticket
[XCHH14]. Ticket-based
[XCHH14]. tickets
[LMJC11]. tied
[Men13b]. Tiered
[GGK18]. Ties
[PYM+15]. Tight
[GDC16, LPS12, LLH18, ZYH+19].

Tightly
[HLLG18]. Time
[AE18, ASBdS16, Ano17d, App14, AYS15, BBC19, BJL16, Che17, EKOS19, FD11, GSC17, HC17, HGT15, IF16, JW1+17, JEA+15, KME+12, LCL+17a, LFX+18, MWES19, NA10a, Nov10, PNRC17, Raz19, RHLK18, Ste15b, WLZL12, YE12, AY14a, Ano15d, BM15, CC14, DCAT12, FHH10a, GPLZ13, GMDFLP17, Hu15, LW10, LW13b, LML+13, MK11, NSX+18, Par18, SPK17, WDG19, XLC+19, Ano16].

Time-area
[Nov10]. Time-Delay
[LFX+18]. time-invariant
[GMDFLP17]. Time-Memory
[ASBdS16]. Time-Series
[BJL16, EKOS19]. Time-Space
[Raz19]. Time-Specific
[KME+12]. Time-Spread
[HGT15]. Timed
[Jia14b, KFOS12, Tan15a, Unr15, WSS12]. Timed-Ephemizer
[Tan15a]. Timed-Release
[KFOS12, Unr15, WSS12].
Timing [BGN17, FDY+19, GV14b, Hay13, LGR14, LFK19, VCD16, YDV19, AKM+15, AGH+17, MCL+19, SRB+12]. Tiny [ZOC10], Titan [PP10b], Titan-R [PP10b].

TLS [AV18, AP13, BB13, BFC12, BZD+16b, BJ+14, CFN+14, Dev11]. Tiny [ZOC10], Titan [PP10b], Tiny-R [PP10b]. TLS-based [PP11], TMDTO [MSS+18].


Trace [ABR12, GA19, PS14, AA14, WGJT10]. Traceability [HCETPL+12, WYML16, WHL16, YFT17, Chi13a, YYS+16]. Traceable [LDZW19, QRV+18]. Traceable-then-revocable [LDZW19]. Traceback [LWY12, PJ18, WYL13]. traces [MY13]. Tracing [LW16, PPS12b, WXL+17, MFH13, PPR+12]. Track [Dun12b, Kia11, Pie10]. Tracking [GZH17, MDMJ17, SNCK18]. Trade [ASBD16, BS14, GPR+19, SR10].

Trade-Offs [ASBD16, BS14, GPR+19, SR10]. Tradeoff [WDDW12, MV16b]. Trading [TW12].


transactions [DG15, Mic16, Mu16, PAS13b, TV15, DK12, FG19, MLMSMG12]. Transceiver [NBZ17]. Transcript [Gli12]. Transfer [AMSPL19, DN12, FMTR12, HL10a, LCCJ13, WCL+18]. transferable [GZAX19]. Transform [AN12, BCPV11, KTM19, LSL12b, pNyWyY+14, OWHS12, SM12, YWN15, BW13, MO14, NES+14, PC14, ST15, TK14, yWpWyYpN13].

Transformation [CRE+12, FJH12, NXB13, TFS19]. transmission [AK14a, BCDN17, BCND19, OSAN19, PsIo+13, WQZ+13]. Transmissions [CBO+18]. Transmitter [KP17].

Transparency [TJZF12], Transparency-Orientated [TJZF12]. Transparent [CCW+10, XTK10, ZHS+19, CRS13, JDV16]. Transport [RBHP15, TW14]. transportation [MS+16]. transposition [FVK17]. Trapdoor [BKPD12, CCL+19, CBX19, CWW12, Mat14, RPSL10, CSZ+11, CW12a].

treatment [YSM14]. Tree
[BS14, CCC19, HSH11, XWZ+18, BW13, BBB16b, CD16a, CFG+17, SCB16].
**Tree-based** [HSH11]. **Trees** [SB18, BTPLST15, Kam19]. **Trends** [Fri12, GCK12, ZMS14, JAE10]. **Triangular** [AMVZ12, RR16]. **Tricks** [GY13]. **Trigger** [SS19]. **trimmed** [TTL10]. **TRIMS** [MGP10]. **Triple** [BW13, BBB16b, CD16a, CFG+17, SCBL16].
**Trees** [HSH11]. **Trees** [SB18, BTPLST15, Kam19]. **Trends** [Fri12, GCK12, ZMS14, JAE10]. **Triangular** [AMVZ12, RR16]. **Tricks** [GY13]. **Trigger** [SS19]. **trimmed** [TTL10]. **TRIMS** [MGP10]. **Triple** [BW13, BBB16b, CD16a, CFG+17, SCBL16].

**TrueCrypt** [Ano14c]. **TrueErase** [DMS+16]. **Truly** [LA10]. **Truncated** [KWS+12, WW12]. **Trust** [Bar15, BL16, BCK17, DCA19, Gli12, GM14, GSFT16, HHBS18, IGR+16, KMSM15, KGP12, PYM+15, PH12b, PAS13b, Rau15, SG12, TMGP13, TV15, WLY+15, Zha15b, BSBG19, CO11, KGO10, MLMSMG12, MGP10, Sch12b, SR12a]. **Trust** [Bar15, BL16, BCK17, DCA19, Gli12, GM14, GSFT16, HHBS18, IGR+16, KMSM15, KGP12, PYM+15, PH12b, PAS13b, Rau15, SG12, TMGP13, TV15, WLY+15, Zha15b, BSBG19, CO11, KGO10, MLMSMG12, MGP10, Sch12b, SR12a].

**Trustworthiness** [RSX18, WXSH19]. **trustworthiness-based** [WXSH19]. **Trustworthiness** [RSX18, WXSH19]. **Trustworthiness** [RSX18, WXSH19]. **Trust** [MJS+19]. **try** [Nor17, YK16]. **Try-CybSI** [YK16]. **Trying** [YK16]. **TTP** [ATK11]. **TTP-free** [ATK11]. **TTPs** [KGO10, TAKS10]. **Tulip** [JB11].

**Tunnel** [VDB+16, ZBR11]. **Tunnel-based** [ZBR11]. **tunnels** [Cri16]. **Tunny** [Cip10a, GMT+12]. **Turing** [Orr16, Blő12, Car10, CS12, Don14, Hai17, Hel17b, KUS13, LCKBJ12, Pro15]. **turns** [Bre18]. **Turtle** [WZCC18]. **Tutorials** [Lin17]. **Tutte** [Hai17]. **TV** [CCSW11].

**Tweakable** [CMLRHS13, LST12, MLCH10, MKASJ18, Sar11, Zha12]. **tweet** [BTW15]. **twelve** [BCV12]. **twice** [BM15]. **TWINE** [KDH13, LYD+18, TY16b]. **TWINE-128** [LYD+18]. **Twins** [Bow11]. **TwistIn** [LFH18]. **Twitter** [AIF+19].
Using [ZPW16, ZS12, dRSdlVC12, ACMP19, AASSAA18, ATKH17, AHM18, APK18, ASVE13, BK19, BOP14, BM13, CSH18, CHS11, CR12, CLHJ13, CBJY16, CP13, Cri16, DA18, Dav11, DTZZ12, DGFH18, DMD18, uHAN18, EEAZ13, FES10, GQH17, GR19b, GSA18, GS18, HAK19, Ham19, Har14, HK14a, HK17, HZWW17, HFC13, HWB12, HL14, HPY10, HCC10, HS11, JKA18, JCHS16, JCL18, JM16, KG19, KI11, KY10, KG14, KCS18, KM11, KKK18b, KS13, KU16, KB17, KD19, KLW16, LXLY12, LLP18, LC17, LH11a, LH10c, LNM11, LMX12, LH13, LZ19, LM14, LML13, MM12, ML15, MM14, MM15, MM16, MKH12, MRRT17, MSR17, MS18b, MGB19, NSX18, NTKG17, NSBM17, PBCC14, PB19, PC14, QD16, RR17, RS15, RS17c, SCBF15, SKE18, Sar11, SM19a, ST15, SGFCRM18, SKS18, SAR18b, SPK17, SLXX16], using [SA19, SC19b, SCBL16, TLC16, TG17, TK14, TLL13, UUN11, VSB19, yWpNyL11, gWpNyY14, WMX17, WHJ17, XWK17, YWJ19, YQH12, YZZ14, YSL10, YN19, ZZKA17, ZLW12, ZYC17, ZXW18, ZZL18], using [CHL19]. utilization [NZM10]. Utilizing [BM18].


Valued [BNA15, TMK11]. VANETs [BMM12, CGCGPDMG12, CST17, IOV18, LLG15, MGB19, YMM13]. Variability [VDB16, SHBC19]. Variable [CHHW12, CMMS17, XNP18, DTZZ12].


Vector [ACZ16, FHLD19, HHHK14, JH112, Kaw15, RS17a, WK18, Zaj19, ZYT13, ZM16, DWZ12, LLM19, PW11, TTL10, ZZ15].


Vehicles [LSY16]. Vehicular [HLKL15, ZH16, BB19, KM10b, SGGR16, WXSH19]. Vein [KLY12].

Velskii [BBB16b]. Ventilated [RSCX18]. Vera [Ayu12]. Verifiability [EKOS19, RST5a, RST5b, VSR12, WWHL12, YMC17, BRR15, Hwa11].

Verifiable [CFE16, CRST15, Fuc11, HYS11, HLC12, HLC18, KZZ17, LW18, ZL18, NJB19, QD16, RDZ16, RS17b,
SZQ+17, XWLJ16, YNR12a, YCR16, GLM+19, LZY+16, LJW+17, MGB19, NMP+13, PHGR16, QS18, XWS17, ZZ15. 

verifiably [SEXY18, ZLY10]. Verification [AV18, App15, ABR12, BCEO19, BCEO20, BL15, BL16, CCK12, CCCK16, CM11, EWS14, Ess17, GLLSN12, GdM16, GMSV14, HZS+19, Lin15, MT17, MV16a, OS12, PNRC17, RSR+19, SOF12, TSB18, Tom16, Vet10, ZPW16, AGHP14, ABF+14, ASVE13, BK19, BFG+14, BJ10a, BTW15, GPN+12, HFCR13, KKK+16, LEW19, MR14c, NPH+14, SD10, XHM14, YNX+16].

Veriﬁed [BFCZ12, YGS+17, HKA+18].

Veriﬁer [DGJN14, HYWS11, WHJ17].

Veriﬁers [AYSZ14].

Verify [BCK17, KRH18, SKGY14, KNTU13, SWW+16].

Verifying [AD12, BFK16, GZSW19].

Verlag [Mei10].

Version [BCP14a, Faa19, KO14, DXWD16, ZDW+16].

Versions [LWPF12, PS12].

Versus [DDR+16, NNA10, ABJ13, Svo14].

Very [BFM12, SBM15, YT16, Jou13, Kum10].

Via [ADR18, BSCTV17, ABC+18, AGH18, BHKN13, BCI+13, BCG19, BR14, Bul18, CBRRZ19, CDSLY14, CFG+17, CLW16, DM19, GT12, GST13, GVW12, Gre19b, HFW+19, JHW+19, KKK+18a, LT13, LT14b, LFH18, LH14, LEW19, LLKA19, MH14, Mor19b, PV17, PTK14, QZDJ16, RS10, SE11, SFF11, SKEG14, TBCB15, WSS+19, tWmC12, YFW18, Yon11, ZOC10, ZCZQ19, Zim10].

Vice [LMS10].

Vichy [Kap11].

Vicious [NN15].

victory [Pea11].

Video [BWR12a, BSA+19, DG17, GKB17, JSZS12, OS12, TWZ+12, WLZL12, YE12, YT12, YTF+18, Crl16, LLHS12, LT10, MK11, OCDF11, PMG19a, XZWZ16].

Video-based [YTF+18].

Videos [AAA+19, GZH17, JSCM17].

Vietnam [ABJ13].

View [RS16, TWZ+12, YCM+13, ZGC16, CWZL13].

View-Invariant [RS16].

Viewpoint [BMDT19].

Views [VGA15, TG12].

Virtual [BCKP17, BR14, Cou12a, HB17, LBC18, RI10, VDO14, CDA14].

Virtualization [CDD13, RC18, QZDJ16].

Virtualization-Based [CDD13, QZDJ16].

Virus [WOLP15], visibility [FG19].

Visible [Cas10, HWYW14, LZC+12b, PCK19, WZJW13, Lin14a].

Virtually [SEXY18, ZLY10].

Vienna [ZLY10].

Villas [BVA15, CSW12, GLW12, HHS+15, KU14, KS15, Lai14, LPL15, LHL10b, LGWY12, LMHH14, LTC+15, OTO18, SA16a, SC10, Shy15, TWNC18, WY12, Ym12, ZZX+11, CT11b, CSTR16, DDD14, DD13, GJJ18, GLW13, HT11, LHL10a, MSM+18b, WYK12, WS12, YSC16, YR11].

Visualizing [Sav15].

VLSI [KB10].

VMOR [MSI18].

Vocal [LCR+18].

Voice [BFC16, BFG+14, BKG17, BSCTV17, ABC+18, AGH18, BHKN13, BCI+13, BCG19, BR14, Bul18, CBRRZ19, CDSLY14, CFG+17, CLW16, DM19, GT12, GST13, GVW12, Gre19b, HFW+19, JHW+19, KKK+18a, LT13, LT14b, LFH18, LH14, LEW19, LLKA19, MH14, Mr19b, PV17, PTK14, QZDJ16, RS10, SE11, SFF11, SKEG14, TBCB15, WSS+19, tWmC12, YFW18, Yon11, ZOC10, ZCZQ19, Zim10].

View-Invariant [RS16].

Viewpoint [BMDT19].

Views [VGA15, TG12].
watermark [Bud16]. wartime [McK10, McK11]. Was [Tur18, Goo12, LHA+12b]. Watching [NSP+18]. Watermark [CHHW12, DLXM+18, EMW14, FR15, GRRZ18, Jin10, KBL11, LZC+12b, MCDB12, QJC+18, SJ12, YE12, ZS12, HB13, TLL13, WYL13]. Watermark-Based [RRZ18]. Watermark-Driven [DLXM+18]. Watermarking [AAA+19, BCGAPM12, BF12, BCPV11, BDB14, BCG10, BMM15, CG12b, CHHW12, CCZC13, CHN+18, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HEK18, HD19, HHT15, HHHK14, JSZS12, Joh10, JKH12, KID12a, LSL12b, LLY+18, LP12, LD13, MM17a, MR16, MU12, NGAAH16, NC12, NH17, pNyWyY+14, OWHS12, RS16, RP12, RR11, RGM18, SA15, SLGZ12, SS17b, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZ12, WYW+13, gWpNyY+14, WLX+17, yWxY+18, WK18, tWum12, XNG+14, XNRG15, XNP+18, YWNV15, YP117, YKK18, YYo15, ZZ+11, ZZWW17, ZWZ17a, ZWZ17b, ZHS10, AP10, AIA+18a, AIA+18b, AIM+19, AM19, AMK12, BWR12b, BW13, BWA13, CCLL11, CT11a, CSS+13, GZH12, GA11, HAK19, HKA+18, HURU11, HKB14, HWYW14, HPL+19, JK11, KMG17, KPS10, KJN+16, KM11, LSR13, LXC11, LLHS12, Lin14a, LWY12, MMS13, MM14a, MO14, MK11].

References

Akyildiz:2014:OTB


Abo-alian:2016:KDB


Applebaum:2017:AC


Aditya:2019:ISF


Zheng:2017:ZIDS


Zodiac:2017:Zodiac


Zynq:2017:Zynq


---

REFERENCES

perience, 28(9):2567–2585, June 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).  

Ambrosin:2016:FAB


Albertini:2014:MHE


Ahmad:2019:PQE


Akdogan:2019:SKA


Arora:2012:ILM

Divya Arora, Najwa Aaraj, Anand Raghunathan, and Niraj K. Jha. INVI-SIOS: a lightweight, minimally intrusive secure execution environment. ACM
REFERENCES


Al-Azzam:2018:SRC


Akleylek:2016:SPM


Aghili:2018:ISA


Acar:2018:SHE


Alizadeh:2016:AMC


Abdalla:2010:PCL

Michel Abdalla and Paulo S. L. M. Barreto, edi-


David W. Archer, Dan


105

REFERENCES


Atighehchi:2015:NME


AlMashrafi:2012:AIM


Aldaya:2019:MTA


Applebaum:2010:PKC


Alzubi:2016:SCC

REFERENCES

Arias-Cabarcos:2015:BIP

Armando:2013:AFB

Arnold:2015:NGH

Anastasiadis:2018:BTA

Amoah:2016:FMA
Ardagna:2010:ECP


Arias-Cabarcos:2019:SAA


Avoine:2012:PFS


Austrin:2017:ICT

Aceto:2019:MME


Aczel:2011:SWL


Alvarez-Cubero:2016:AVL


Aizatulin:2012:VCC


Anyanwu:2010:DCS


Ayday:2012:DAA

REFERENCES


REFERENCES


REFERENCES


Aumasson:2017:SCP

Atighehchi:2019:GHC

Antonopoulos:2017:DIS

Akinyele:2014:MGA

Abdullahaziz:2016:AAI

**Allender:2019:NIN**


**Ahmadzadeh:2018:HPE**


**Attrapadung:2012:ABE**


**Ali:2018:ECM**


**Akhtar:2018:BSI**

REFERENCES

[113]

(1941-0166 (electronic)).

[Appelbaum:2013:SSG]


[Ak:2014:ICS]


[Aiash:2015:FAA]


REFERENCES


REFERENCES


Alhanahnah:2016:MTI


Almulla:2013:CKE


Anada:2017:CGS

Hiroaki Anada, Junpei Kawamoto, Chenyutao Ke, Kirill Morozov, and Kouichi Sakurai. Cross-

**Alabdulatif:2017:PPA**


**Afanasyev:2011:PPN**


**Andrysco:2015:SFP**


**Armknecht:2012:STH**


**Arfaoui:2019:CAA**

REFERENCES


REFERENCES

Alpar:2018:BT

Asharov:2013:FCF

Araghi:2019:EHI

Awad:2016:SSZ

Alzahrani:2019:SAC

Arnedo-Moreno:2010:JRA
[AMK12] Muhammad Arsalan, Sana Am-breen Malik, and Asiful-lah Khan. Intelligent re-
versible watermarking in integer wavelet domain
for medical images. The Journal of Systems and
Software, 85(4):883–894, April 2012. CODEN JS-
SODM. ISSN 0164-1212 (print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0164121211002858.

[AMV18] Rodrigo Abarzúa, Santi Martínez, Valeria Men-
doza, and Javier Valera. Avoiding side-channel at-
tacks by computing isoge-
nous and isomorphic el-
liptic curves. Mathematics in Computer Science,
ISSN 1661-8270 (print), 1661-
8289 (electronic).

[AMKA17] Prashant Ahir, Mehran Moza-
ifi-Kermani, and Reza Azarderakhsh. Lightwe-
ight architectures for reliable
and fault detection Simon
and Speck cryptographic
algorithms on FPGA.
ACM Transactions on Em-
bdeded Computing Systems,
16(4):109:1–109:??, August
2017. CODEN ???
ISSN 1539-9087 (print), 1558-
3465 (electronic).

[AMN18] Dariush Abbasinezhad-
Mood and Morteza Nik-
oghadam. Design and hardware im-
plementation of a security-
enhanced elliptic curve
authentication scheme for
smart grid communications.
Future Generation
Computer Systems, 84(??):
47–57, July 2018. CODEN
FGSEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167739X17315376.

[AMORH13] Gora Adj, Alfred Menezes,
Thomaz Oliveira, and Fran-
isco Rodríguez-Henriquez.
Weakness of $F_{3,500}$ for dis-
crete logarithm cryptogra-

REFERENCES


Arshad:2015:SAI


Aga:2017:ISM


Anawis:2014:ARR


Anderson:2013:MNF


Anderson:2019:QCN


Anghelescu:2016:FIP

Petre Anghelescu. FPGA implementation of programmable cellular automata encryption algorithm for network communications. *International Journal of Com-
REFERENCES

Anonymous:2010:NDS


Anonymous:2010:MML


Anonymous:2011:AIS


Anonymous:2011:AXL


Anonymous:2011:MCB


Anonymous:2011:SHS


Anonymous:2013:CFF

Anonymous. Crypto flaw
REFERENCES


REFERENCES


[Ano15e] Anonymous. UK Gov-
ernment battles tech firms

**Anonymous:2016:BRBa**


**Anonymous:2016:CPSd**


**Anonymous:2016:CPSe**


**Anonymous:2016:EMT**


**Anonymous:2016:FVM**


**Anonymous:2016:GUP**

REFERENCES

126


**Anonymous:2016:ICd**


**Anonymous:2016:MBE**


**Anonymous:2016:SWT**


**Anonymous:2016:SIR**


**Anonymous:2017:BA**

Anonymous. BitErrant attack. Web site, March 6, 2017. URL http://biterrant.io/. The story describes how SHA-1 collision attacks could lead to bogus, and malware, file downloads via BitTorrent: the obvious solution, which should have been adopted long ago, is to use multiple checksum algorithms, and require all to match before concluding that two files are in fact identical.

**Anonymous:2017:BRM**


**Anonymous:2017:CCS**

The story describes a poor choice of generating large (about 1024 bits) primes \( p \) and \( q \) that led to crackable RSA cryptography. The solution for Estonia was to switch to elliptic-curve cryptography that was also supported by the cards.

Anonymous:2017:HDQ


Anonymous:2017:MBH


Anonymous:2017:RV


Anonymous:2019:GES


Anonymous:2019:HCC

REFERENCES


Anonymous:2019:PBT


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF


AlFardan:2013:LTB


Abellan:2018:FCQ

C. Abellan and V. Pruneri. The future of cybersecurity is quantum. IEEE Spec-
REFERENCES

Ali:2018:SUA

Alcaide:2013:AAP

Applebaum:2013:GXG

Applebaum:2014:CCP

Appel:2015:VCP

Albrecht:2015:FBR
Martin R. Albrecht, Davide Papini, Kenneth G. Paterson, and Ricardo Villanueva-Polanco. Fac-

Al-Qarni:2012:EII


Al-Qurishi:2018:EKA


Arai:2013:MDH


Arab:2019:IEM


Adj:2014:SRC

G. Adj and F. Rodriguez-Henriquez. Square root computation over even extension fields. IEEE Trans-

Altawy:2018:SLT


Altawy:2018:TCM


Agudo:2013:PAC


Abdulrahman:2015:NRR


Azarderakhsh:2015:PHS

REFERENCES

Armasu:2019:IFA


Ambrose:2012:RII


Alghamdi:2019:RAM


Asharov:2014:TCC


Artemenko:2017:PGO


Andrade:2016:LEP


Asharov:2014:LPI

[Ash14] Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. Lecture Notes in Computer Sci-
REFERENCES

Al-Sinani:2012:UCB

Ahmadi:2011:SK

Ahmadi:2012:SKE


Asaar:2015:IBM

Alharbi:2018:CME
Rawan Alharbi, Tammy Stump, Nilofar Vafaie, Angela Pfammatter, Bonnie Spring, and Nabil Alshu-


REFERENCES


Abdelrahman Abdou and P. C. Van Oorschot. Server location verification (SLV) and server location pinning: Aug-

**Badawi:2018:ASS**


**Altaf:2015:LPM**


**Awad:2017:OLO**


**Anzala-Yamajako:2012:RAC**


**Anzala-Yamajako:2012:RBC**

Ahmad:2014:RTN


AlTawy:2014:IDR


Aysu:2015:FRT


Au:2014:SMV


Ayub:2012:BRB


Apavatjrut:2012:EEA

July 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Alshammari:2011:CET


Alavi:2014:RQE


Barcellos:2018:RSP


Behnia:2013:IEB


Blaner:2013:IPP


Brennan:2012:ASC

2012. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).


[Bar16b] Timo Bartkewitz. Leakage prototype learning

**Bard:2019:DWG**  
[Bar19]  

**Batey:2010:DMW**  
[Bat10]  

**Bax:2014:PPD**  
[Bax14]  

**Baylis:2010:CC**  
[Bay10]  

**Bulygin:2010:OSS**  
[BB10]  

**Bennett:2014:QCP**  
[BB14]  


Barak:2014:OEF

Barthe:2019:SLN

Beurdouche:2017:MSU

Barenghi:2016:PPE
Beimel:2014:MLS


Bernstein:2017:SRD


Boldi:2012:IUG


Bingol:2019:EPP


Bollman:2015:PWI


Behrad:2020:NSA

REFERENCES

Bernstein:2011:PCI


Basin:2014:KYE


Bao:2016:LPP


Bocu:2018:HEB


Balagurusamy:2019:CA

Bichsel:2012:DMA


Boche:2017:CQA


Badrignans:2010:SSA


Balfanz:2012:FA


Bugliesi:2015:ART


Bana:2019:VMC

REFERENCES

146

(print), 1557-945X (electronic).

Bana:2020:VMC


Buhrman:2014:PBQ


Benedetto:2010:DQE


Bahri:2016:CCO


Bafi:2012:SCS

REFERENCES


Boneh:2016:BHP


Belleville:2019:ASP


Batina:2019:ISI


Brandenburger:2017:DTC

REFERENCES


REFERENCES

Bicakci:2013:LSS


Botta:2014:PCI


Boyle:2014:EO


Basso:2011:BW


Bessani:2013:DDS


Blasco:2016:SWB


REFERENCES


Barbareschi:2019:PBM


Barbareschi:2018:PBH


Belkhouja:2019:BBA


Bossuet:2016:EPA


Bendlin:2011:SHE

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Bhargavan:2016:MVP


Beimel:2012:SSS


Berger:2016:EGF


Boldyreva:2014:MEW


Battistello:2012:TBA


Barthe:2012:CACb

Balagani:2018:IAC


Bossuet:2013:AFS


Boudot:2019:BFD


Barak:2010:IPO


Barak:2012:IPO


Barbulescu:2013:QPA

Razvan Barbulescu, Pierrick Gaudry, Antoine Joux,

Barbulescu:2014:HQP


Barthe:2012:ACA


Bisce:2017:STC


Borcea:2017:PEE


Brak:2014:LFH

Barkatullah:2015:GCF


Bhattacharjee:2016:SWC


Breitner:2019:BNS


Bhattacharjee:2016:SWC


Behnia:2012:SEI

REFERENCES

10.1007/978-3-642-32287-7_12/


Benhamouda:2019:SPD


[BHH19]

[BHKN13]

[BHT18]

[BHvOS15]

[BHJP14]

Berman:2013:HPR


Berman:2018:CFC


Bonneau:2015:PEI

REFERENCES

cacm.acm.org/magazines/2015/7/188731/fulltext.

Biagioli:2012:CCS

Biggs:2008:CII

Beimel:2014:CCW

Biswas:2017:SAI

Bauer:2010:RVC

Brumley:2010:CAI
Boche:2016:DSK


Bouraoui:2017:HAE


Bogdanov:2012:UTC


Benhamouda:2016:NFP


Brubaker:2014:UFA


Bolyrevra:2012:NPG

REFERENCES

eprint.iacr.org/2012/056.


[BKL+13] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. SPONGENT: The design...

**Bogdanov:2012:KAC**


**Bogdanov:2018:IEA**


**Bellare:2012:IBL**


**Bogdanov:2011:BCF**


**Bogatov:2019:CEO**

REFERENCES


REFERENCES

Bidgoly:2015:MQV


Bidgoly:2016:MQV


Blanc:2012:BPC


Blaze:2016:UHR


Benzaid:2016:FAW


REFERENCES


REFERENCES


Bhattacharya:2018:UPC


Benamara:2016:ICA


Baldwin:2010:AFI


Bartoli:2019:VEW


Biswas:2012:IBA


Backes:2012:GCP

Michael Backes, Matteo Maffei, and Kim Pecina. G2C: Cryptographic protocols from goal-driven specifications. Lecture
REFERENCES


[Bon19] Dan Boneh. Attacking cryptographic key ex-

**Bailey:2014:UIA**


**Borghoff:2010:CLC**


**Boyen:2013:ABF**


**Boyce:2016:BOT**


**Beissinger:2006:CUM**


**Burns:2010:SCR**

Randal Burns and Zachary Peterson. Security con-


REFERENCES

Boneh:2016:BCR


Balsa:2017:TIC


Brakerski:2013:WHB


Bradbury:2015:BSB


Brewster:2018:RCF

R. Brewster. Re-creating the first flip-flop — a fun-


REFERENCES


[Birrell:2013:FIM] Eleanor Birrell and Fred B. Schneider. Federated identity management systems:
REFERENCES


[Bhattacherjee:2014:CAT]

[Bagheri:2015:NNA]

[Bronzino:2019:ISV]

[Bala:2019:SAG]

[Bendiab:2019:FNF]

[Ben-Sasson:2017:SZK]
Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and

**Boorghany:2015:CIL**


**Bojinov:2014:NMC**


**Batina:2012:HEB**

REFERENCES

Broustis:2012:GAN


Boneh:2012:FEN


Biskup:2012:RBR


Braeken:2018:AAA


Bosch:2012:SDR


Bouabana-Tebib:2015:PSE

REFERENCES


[Bul10b] Stanislav Bulygin. *Com-
REFERENCES

puter algebra in coding theory and cryptanalysis. Südwestdeutscher Verlag für Hochschulschriften, Saarbrücken, Germany, 2010. ISBN 3-8381-0948-1. ?? pp. LCCN ???.


[BV14] Burke:2011:AMD


Ali Galip Bayrak, Nikola Velickovic, Paolo Ienne, and Wayne Burleson. An architecture-independent instruction shuffler to protect against side-channel

**Baek:2013:SPK**


**Bogdanov:2012:ZCL**


**Bhatnagar:2013:SRI**


**Bai:2016:ALC**


**Baek:2016:EGC**

Joonsang Baek, Duncan S. Wong, Jin Li, and Man Ho Au. Efficient generic construction of CCA-secure identity-based encryption from randomness extrac-
REFERENCES

Bhatnagar:2012:IVE

185


Bhatnagar:2012:NRA


Buhren:2019:IUP


Bai:2019:HAF


Bao:2010:ISC


Bo:2016:ETK


Bock:2016:NDA


Caldwell:2013:INP


Chakraborty:2019:TIP


Carter:2010:TB


Carlson:2011:JRW

Elliot Carlson. *Joe Rochefort’s war: the odyssey of the codebreaker who outwitted Yamamoto at Midway*. Naval Institute
REFERENCES


www.sciencedirect.com/
science/article/pii/S0167404809001461.


REFERENCES

Chadha:2016:AVE


Chretien:2015:SPP


Chretien:2019:TMF


Chretien:2020:TMF


Chen:2017:LAA


Carota:2012:FFI

Chou:2010:PSO


Checkoway:2016:SAJ


Chadha:2012:AVE


Chatterjee:2016:TAD


Chou:2013:UGS


Cao:2019:AML

[Nanyuan:19] Nanyuan Cao, Zhenfu Cao, Zhen Liu, Xiaolei Dong, and Xiaopeng Zhao. All-but-many lossy trapdoor functions under decisional RSA subgroup

Chang:2011:SFW


Cascudo:2015:SSN


Chatterjee:2017:PBS


Chikouche:2019:PPC


Cho:2014:DGA


Chen:2011:EAA

Tien-Ho Chen, Yeu-Chiu Chen, Wei-Kuan Shih, and Hsin-Wen Wei. An efficient anonymous authentication protocol for mobile pay-TV. *Journal of Net-


REFERENCES


[Crampton:2017:CEI] Jason Crampton, Naomi Farley, Gregory Gutin, Mark Jones, and Bertram Poettering. Cryptographic enforcement of information...

**Carter:2013:SSA**


**Centenaro:2013:TBA**


**Checkoway:2014:PED**


**Cevallos:2012:USR**


**Carstensen:2011:AAA**


**Calzavara:2017:SWJ**

Stefano Calzavara, Riccardo Focardi, Marco

Celesti:2016:ALT


Cho:2017:EDF


Chang:2010:PRN


Chen:2010:IFA


Camenisch:2012:EAA


Che:2012:WAM

Xiangju Che and Zhanheng Gao.

**Cheraghchi:2014:NMC**


**Corrigan-Gibbs:2014:KS**


**Chaudhuri:2010:PIC**


**Caballero-Gil:2012:LAR**


**Chmiel:2012:EPC**


CHENG:2010:NUP


CHANG:2011:DEQ


CHAN:2013:OCK


CHANG:2013:MPQ


CHAPPELL:2013:PMI


CHEN:2011:CCH


CHESWICK:2013:RP

REFERENCES

February 2013. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES

Cohen:2018:WCC

Choudary:2010:SCD

Chou:2014:EMA

Chen:2011:SEI

Cooke:2015:FSM

Chu:2016:BEE

[CHX13] Qian Chen, Haibo Hu, and Jianliang Xu. Authenticating top-k queries in
location-based services with confidentiality. Proceedings of the VLDB Endowment,
7(1):49–60, September 2013. CODEN ????. ISSN 2150-8097.

[Cilardo:2011:EPT] Alessandro Cilardo. Exploring the potential of
threshold logic for cryptography-related operations. IEEE Transactions on
Computers, 60(4):452–462, April 2011. CODEN ITCOB4. ISSN 0018-9340 (print),
1557-9956 (electronic).

size for authentication in network coding. IEEE Transactions on Computers,
62(10):2096–2100, October 2013. CODEN ITCOB4. ISSN 0018-9340 (print),
1557-9956 (electronic). See comments [LCLL15, Kim15].

[Cao:2014:SCI] Yan-Pei Cao, Tao Ju, Zhao Fu, and Shi-Min Hu. Shapes and cryptography:
Interactive image-guided modeling of extruded shapes. Computer Graphics Forum,
33(7):101–110, October 2014. CODEN CGFODY. ISSN 0167-7055 (print),
1467-8659 (electronic).

problems and cryptanalysis of the GGH multilinear map without a low-
level encoding of zero. LMS Journal of Computation and Mathematics, 19(A):
org/core/product/230ECFEE6AF4D8027FF3E139

[Cho:2012:CBF] Jung-Sik Cho, Young-Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and
retrieval cost: a hash-based radio-frequency identification (RFID) Tag Mutual
Authentication Protocol. Computers and Mathematics with Applications,
69(1):58–65, January 2012. CODEN CMAPDK. ISSN 0898-1221 (print),
1873-7668.
See cryptanalysis [SPLHCB14].


[Cho:2015:CBF]


[Cui:2013:OSL]


[Chandra:2011:AST]


[Chang:2019:GTS]

[CK17] André Chailloux and Iordanis Kerenidis. Physi-

**Chung:2018:ERN**

**Chuang:2011:LMA**

**Colin:2016:CTC**
Alexei Colin and Brandon Lucia. Chain: tasks and channels for reliable intermittent programs. *ACM SIGPLAN Notices*, 51(10):514–530, October 2016. CODEN SINODQ. ISSN 0362-1340 (print), 1523-
Claxson:2018:SVE

Calegari:2019:WPH

Chen:2019:BBS

Comon-Lundh:2010:DSP

Chang:2011:RSB

Chen:2017:PGF
REFERENCES

Chong:2013:ASG


Chen:2016:RPR


Chen:2012:NCB


Chen:2013:TSE


Chande:2016:NSC


Cao:2012:SRH


Cao:2018:CUP

Cheng:2017:ISK

Cremers:2011:OSV

Cozzens:2013:MEE

Cui:2014:SSA


Jiageng Chen, Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. Variable message encryption through blockcipher compression function. *Concur-
REFERENCES

Cao:2016:OMA

Chatterjee:2017:IPB

Chen:2012:FAA

Chaudhry:2018:IRB

CNRS:2014:NAS

See [BGJT14].

Coron:2012:PKC
Jean-Sébastien Coron, David


[Con17] Lucian Constantin. The SHA1 hash function is now completely unsafe: Researchers have achieved the first practical SHA-1 collision, generating two PDF files with the same signature. *ComputerWorld*, ?? (??):??, February 23, 2017. CODEN CMPWAB. ISSN 0010-4841. URL https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html.
REFERENCES

Connolly:2018:FE


Copeland:2006:CSB


Copeland:2010:CBG


Copeland:2010:CSB


Chung:2014:RRS


Cordova:2014:EBS


Corthesy:2014:SSD

[Cor14b] Sébastien Corthésy. Smartphones set out to decipher

[Courtland:2012:VCG]

[Coutinho:2012:RPT]

[Claessen:2013:SPN]

[Canard:2018:NTC]

[Chung:2016:NBB]

[Chen:2018:RLF]
Yu Chen, Baodong Qin, and Haiyang Xue. Regular

---

Chevalier:2010:CSC


---

Chen:2012:DCC


---

Crav

er:2014:UCC


---

Clear:2012:CPA

Michael Clear, Karl Reid, Desmond Ennis, Arthur Hughes, and Hitesh Tewari. Collaboration-preserving authenticated encryption


---

Cramer:2012:TCT


2.

---

Crampton:2011:PEC


---

CRE+12

Michael Clear, Karl Reid, Desmond Ennis, Arthur Hughes, and Hitesh Tewari. Collaboration-preserving authenticated encryption


[CS11] Siddhartha Chhabra and


REFERENCES

Chen:2013:RWM


Chen:2017:SIE


Chow:2012:EPV


Chen:2018:SIA

REFERENCES


Chou:2013:TIB


Crenne:2013:CMS


Calmon:2014:ITM


Choi:2012:LTTF


Chung:2012:CBI


Zhenhua Chen, Chunying Wu, Daoshun Wang, and Shundong Li. Conjunctive keywords searchable encryption with efficient pairing, constant ciphertext and short trapdoor. *Lecture Notes in Computer Science*, 7299:
176–189, 2012. CO-


[CZ14] Long Chen and Zhao Zhang. MemGuard: a low cost and energy efficient design to support and enhance memory system reliability. ACM


[CWZL13] Jian Cao, Jie Wang, Haiyan Zhao, and Minglu Li. Special issue papers: An event view specification approach for Supporting Service process collaboration. Concurrency and
Chen:2015:TCP

Cheng:2015:OMU

Cai:2019:UMD

Chen:2018:ERS

Chen:2012:FSD

Chen:2012:AIB
Yu Chen, Zongyang Zhang, Dongdai Lin, and Zhenfu

Chen:2012:IBE


Chen:2014:CSI


Dharwadkar:2010:SSG


Djebbar:2012:ASB


Darivandpour:2018:ESP

REFERENCES


[DePrisco:2013:CVC] Roberto De Prisco and Alfredo De Santis. Color vi-

**DArco:2014:MIC**


**Dreier:2015:BFP**


**Datta:2017:SFH**


**Castro:2016:FVB**


[DaRolt:2013:NDS]


[DDS12] Danezis:2012:FCDa


[Del19] DeOliveiraNunes:2019:SSC


[Des10a] Desmedt:2010:CF

Desmedt:2010:ES


Dew:2011:BRB


DuPont:2016:ECC


Durmuth:2011:DEN


DeCapitaniDiVimercati:2010:EPR


DeCapitaniDiVimercati:2017:AMM

REFERENCES


REFERENCES


Dong:2019:FOI


Ding:2015:CWF


Domnitser:2012:NMC


Delfs:2002:ICP


Delfs:2007:ICP


Dolev:2012:ATC

Shlomi Dolev and Marina


Dorre:2016:ELO

Delfs:2015:ICP

Delimitrou:2016:SID

Doychev:2017:RAS

Durumeric:2014:MH
Dolev:2016:MCG


Dobre:2019:PWR


Doychev:2015:CTS


Dodd:2012:MAR


Dunkelman:2012:MCE


Dong:2012:UAS


DeLuca:2015:SUS


Dinur:2017:IGA


Djaziri-Larbi:2018:WDA


Dong:2013:PRS

[DLN13] Qi Dong, Dongganga Liu, and Peng Ning. Providing DoS resistance for...

**DiPietro:2016:CLD**


**Dodis:2011:SSC**


**Dai:2016:MLR**


**Duan:2016:SDC**


**DeCarneDeCarnavalet:2015:LSE**


**Daneshgar:2018:SSS**

REFERENCES


REFERENCES


REFERENCES


Draziotis:2016:EDL


Dong:2011:SSE


Dasgupta:2016:TDA


Dixon:2016:NTO


delRey:2012:EDI


Dini:2011:LLA


Dixit:2019:FBD

Umesh D. Dixit and M. S.

**Das:2015:DCS**


**Das:2016:MPU**


**Das:2012:DPB**


**Deng:2018:SFE**


**Dachman-Soled:2014:COF**

Do
[102x681]is:2014:HEY


Do
[102x681]is:2017:HEY


Dini:2013:HHS


Drosatos:2017:PET


Deng:2012:VIA


Dunkelman:2012:MEK

[Dun12a] Orr Dunkelman. From multiple encryption to knapsacks — efficient dissection of composite problems. Lecture Notes in
REFERENCES

Computer Science, 7668:

Dunkelman:2012:TCC


Durcheva:2015:SAI


David:2012:PRE


Dorn:2012:ECE


Dong:2012:KKD

Dong:2012:NDI


Dai:2018:OPC


Deng:2014:CCC


Deng:2016:NCS


Dodis:2013:OWE


Dyakonov:2019:WWU

REFERENCES

CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Dong:2015:SSS


Deng:2014:TNI


Dong:2016:EPP


Doss:2012:MDA


Delledonne:2018:CDA


Dent:2010:PS


Erbagci:2019:SHE


Ermis:2017:KAP


Esiner:2017:QRI


Esiner:2019:TF


Edwards:2014:NRP

Chris Edwards. News: Researchers probe security...
through obscurity. *Communications of the Association for Computing Machinery*, 57(8):11–13, August 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

**Edwards:2017:NSQ**


**El-Emam:2013:NSA**


**Espitau:2018:LAF**


**Eisenbarth:2012:CIP**


**El-Hadedy:2019:RPR**

REFERENCES


REFERENCES

Ermoshina:2019:SRC

Embar:2014:PWO

English:2015:SME

Evtushkin:2016:UMC

Eberz:2016:LLE

El-Razouk:2015:NHI


Tobias Eibach, Gunnar Völkel, and Enrico Pilz. Optimising Gröbner bases


[Jennifer Eling:2014:FVS]


REFERENCES

Feigenbaum:2019:PSE


Felten:2013:LBA


Faugere:2010:CLR


Fleischmann:2012:MFA


Fan:2019:OVG


Feng:2010:CTS


Farras:2012:LTM

[FGMP12] Oriol Farràs, Ignacio Gra-

**Faugere:2014:MCA**


**Fan:2017:SSP**


**Fan:2018:MBP**


**Fan:2013:CPP**


**Fan:2010:PSN**

(print), 1558-2566 (electronic).


[Fahl:2012:WEM] Sascha Fahl, Marian Harbach, Thomas Muders,

Fan:2014:ASA


Fawzi:2013:LDN


Florencio:2016:PSD


Feng:2018:ABB


Fidler:2018:CCN

Farash:2015:PSE


Fisher:2015:CS


Fei:2012:GTK


Fotiadiis:2019:TRF


Fanti:2015:SVS


Fehr:2013:FCC

REFERENCES

Fan:2013:CEM


Fan:2014:RRS


Ferguson:2010:SHF


Forler:2012:DAC


Fei:2016:PPA


Fei:2016:SEF

Xiongwei Fei, Kenli Li, Wangdong Yang, and Keqin Li. A secure and efficient file protecting system based on SHA3 and parallel AES. *Parallel Computing*, 52(??):106–132, February 2016. CODEN PACEJ. ISSN 0167-8191 (print), 1872-7336 (elect-
REFERENCES


[Feng:2012:CAO]


[FLZ+12]

[Fallahpour:2015:AWB]


[FM15]

[Ferrag:2018:SCN]


[FMA+19]


[FMA+18]


[FMB+18]


REFERENCES

(0):105–125, 2015. ISSN 0379-0738. URL http://www.sciencedirect.com/science/article/pii/S0379073814005064. See also [?].


Zoltán Faigl, Jani Pelilikka, László Bokor, and Andrei Gurkov. Performance evaluation of current and emerging authentication schemes for future 3GPP network architectures. Com-
REFERENCES


Faust:2012:PLR


F:2015:TVG


Fu:2015:TVG


Fiore:2015:EIB


F:2018:ALA


Fathimal:2016:SSS

REFERENCES


REFERENCES


[Fang:2012:CCS] Liming Fang, Willy Susilo, Chunpeng Ge, and Jian-


Fadlullah:2010:DCA


Fuchsbauer:2011:CSV


Fulton:2010:BRB


Fanti:2018:DLC


Franken:2019:ECP


Fathi-Vajargah:2017:IMC

REFERENCES


REFERENCES

355–367, September 2019. ISSN 2332-7790.

[Fan:2015:IRD]


[FYMY15]

[Fan:2013:KIS]


[Fan:2014:NCI]

[Fyodorov:2019:SGM]


[Fyo19]

[Fu:2012:EHA]


[FZT14]

[FZT13]

REFERENCES


[Grondahl:2019:TAA]

[Guimaraes:2019:OIQ]

[Galgio:2013:NIC]


[Gope:2018:LPP]
Gasarch:2013:RBC


Gutierrez:2016:IDO


Ghoshal:2019:RSC


Gupta:2019:DRB


Gorantla:2011:MKC


Guyeux:2015:ECS

Christophe Guyeux, Raphaël Couturier, and Pierre-Cyrille Héam. Efficient and cryptographically se-

Gao:2019:LBD


Gupta:2012:CDF


Gupta:2013:HPH


Gupta:2013:PDC


Gupta:2013:HPH


Guerra-Casanova:2011:SOT


Granado-Criado:2017:HCH


[GGH+16b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Hiding secrets in software: a cryptographic approach

**Garg:2014:TRS**


**Garg:2017:IDI**


**Gunleifsen:2018:TCP**


**Gentry:2011:FHE**


**Gentry:2011:IGF**


**Guo:2012:EBP**

REFERENCES


REFERENCES

editor, *ACM Conference on Computer and Communications Security*, page ??


P. Geetha, V. S. Jayanthi, and A. N. Jayanthi. Optimal visual cryptographic scheme with multiple share creation for multimedia ap-


Juan A. Garay, Vladimir Kolesnikov, and Rae McEl- lan. MAC precomputation with applications to secure


**Gagne:2012:AVB**


**Guo:2011:EDA**


**Gong:2016:HES**


**Gupta:2019:OIT**


**Gerault:2018:RAR**

REFERENCES


[GM13b] Brice Goglin and Stéphanie Moreaud. KNEM: a

Gotzfried:2014:MAT


Gofman:2016:MBE


Gueron:2016:HIA


Gonzalez-Manzano:2017:EHE


Gonzalez-Manzano:2019:LUR


REFERENCES


Gao:2014:URA


Good:2012:BTC


Groza:2017:LCL


Gardiner:2016:SML


Gong:2012:KNF

REFERENCES


Glowacz:2017:IDW

Gong:2013:NOT

Goodrich:2012:EVW

Genkin:2016:PKE

Gottel:2019:SPE

Grossschadl:2012:EJI
REFERENCES


Genkin:2014:GYH
Daniel Genkin, Itamar Pippman, and Eran Tromer. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs. Report, Technion and Tel Aviv University, Tel Aviv, Israel, July 31, 2014. 25 pp. URL http://www.cs.tau.ac.il/~tromer/handsoff/.

Gonzalez-Pardo:2012:CID

Gai:2017:SCI

Ghatak:2019:IBS

Ghosal:2019:NPP

Greengard:2011:MRM
Samuel Greengard. In

**Green:2017:SSE**

**Green:2019:RMC**

**Green:2019:RNT**

**Grimes:2015:CCT**

**Gibson-Robinson:2012:AAL**

**Guo:2018:WBS**
References


**Gierlichs:2012:ICD**


**Genkin:2013:RKE**


**Ge:2016:KPA**


**Gazi:2012:EOS**


**Gallin:2019:GFP**

Gupta:2019:LAU

Goodrich:2011:EAD

Grosse:2013:AS

Gueron:2016:MEG

Gupta:2015:GEM

Galindo:2014:LCL


REFERENCES

Gao:2012:RHC


Guo:2018:SMK


Ge:2013:SAP


Gao:2019:VQS


Guo:2019:NTP


Hernandez-Ardieta:2013:TSA

Jorge L. Hernandez-Ardieta.


Hanyok:2012:EHH


Harn:2013:GA


Harrington:2014:GEF


Hardesty:2015:BAC


Hardesty:2016:SUC


Hastings:2016:SWS


Hayes:2013:NSA


Houmansadr:2013:BCN

REFERENCES


REFERENCES


REFERENCES

Han:2013:RMA

Song Han, Tharam Dillon, Vidy Potdar, and Elizabeth Chang. RFID mutual authentication protocols for tags and readers with and without a server. *International Journal of Computer Systems Science and Engineering*, 28(2):??, ????. 2013. CODEN CSSEEI. ISSN 0267-6192.

Heninger:2012:MYP


Heath:2015:HNS


Hwang:2012:ABA


Hamad:2018:DWU


Hellegren:2017:HCD

References

**Hellman:2017:TLC**

**Hanka:2011:DPK**

**Hermelin:2010:MLC**

**Herranz:2014:ABS**

**Herardian:2019:SUC**

**Hess:2012:GJC**

**Heys:2017:SCF**
Howard M. Heys. Statistical cipher feedback of stream ciphers. *The
REFERENCES

Harn:2014:MTS

Hoang:2014:IMD

Hocking:2013:COU

Hastings:2016:WKR

Hintze:2019:CUR
Huang:2016:EDP

Hanocka:2019:APS

Hibschman:2019:ISS

Hua:2015:TSE

Han:2011:PEB
REFERENCES


Harn:2015:DTS


Hu:2016:EWS


Huber:2014:TPW


Hammi:2018:BTD


Hayashi:2013:AEI


Huber:2019:FCL

[HHMK14] Stefan Huber, Martin Held, Peter Meerwald, and Roland Kwitt. Topology-


**Hinek:2010:CRV**


**Harb:2019:FIE**


**Hinkelmann:2011:CPA**


**Hasan:2014:TFL**


**Hur:2014:SDR**


**Hasan:2017:UAF**

Ragib Hasan and Rasib Khan. Unified authentication factors and fuzzy service access using interaction provenance. *Comput-

Hameed:2018:TFV


Hameed:2018:TFV


Hameed:2018:TFV

Hanzlik:2019:CPC


Heyse:2012:LEA


Holenstein:2011:ERO

Harn:2010:AGK


Hazay:2010:EST


Hsieh:2012:EHF


Hsieh:2014:AMU


Hejun:2019:OAI

Zhu Hejun and Zhu Liehuang.

**Hmood:2015:ACA**


**Hu:2012:VMS**


**Hu:2016:PBR**


**Hu:2018:AAA**


**Hu:2019:AAA**


**Huang:2011:ISL**

Y.-L. Huang, F.-Y. Leu, C.-H. Chiu, and I.-L. Lin. Improving security levels of IEEE802.16e authenti-

**Hwang:2019:ELS**


**Huang:2015:MSE**


**Huffmire:2010:SPR**

1936-7406 (print), 1936-7414 (electronic).


Hefeeda:2010:ASM

Herzberg:2012:TJA

Hwang:2019:BBR

Hore:2012:SMR

Hajihassani:2019:FAI

Hoang:2012:ESB


Horsman:2019:CPE


Hyla:2012:CBE


Hazay:2014:OSA


Hyla:2017:HLS


Haigh:2018:CP


Halder:2010:WTR


Junbeom Hur, Chanil Park, and Hyunsoo Yoon. Chosen ciphertext secure authenticated group communication using identity-

**Han:2016:GGA**


**Han:2018:BEI**


**Han:2014:GTK**


**He:2013:GME**


**Hisil:2019:KLF**

Huseyin Hisil and Joost Renes. On Kummer lines with full rational 2-torsion...

[Hulsing:2013:OPX]


[HREJ14]


[HRS16]


[Haitner:2010:EIC]

Iftach Haitner, Omer Reingold, and Salil Vadhan.


[Haitner:2018:SSH]

Siam Umar Hussain, M. Sadegh Riazi, and Farinaz Koushanfar. SHAIP: Secure Ham-

[Hwang:2011:CDA]


[HS11]


[HS18]


[Halevi:2011:TBH]


[Han:2013:IBD]


Henson:2013:MES


Hu:2010:TTW


Huang:2015:PAP


Huang:2017:SSS


Herbert:2012:SMP


Hald:2015:RRA

Hulsing:2013:WOS


Hurlburt:2016:MBO


Hammerle-Uhl:2011:RWI


Harvey:2017:FPM


Hunger:2018:DDC


Han:2012:MIA


Hammad:2019:PSF

[HW19] Mohamed Hammad and Kuanquan Wang. Parallel score fusion of ECG and fingerprint for hu-

[Hwang:2011:NIB]


[HWDL16]


[HWG10]

REFERENCES

UK / etc., 2010. ISBN 3-642-17618-6 (softcover). LCCN ????


**He:2017:APP**


**Huang:2018:PIB**


**Hu:2019:CAC**


**Hao:2011:NTV**


**Huang:2018:CT**

REFERENCES


Huang:2011:IBS


Heys:2011:PSC


Han:2012:ERI


Han:2018:ERA


Huang:2019:ILA

[HZS+19] Bo-Yuan Huang, Hongce Zhang, Pramod Subra-

**Huang:2005:EMP**


**Han:2014:ATS**


**Hammad:2019:NTD**


**He:2017:AHA**

Debiao He, Sherali Zeadally, Libing Wu, and Huaqun Wang. Analysis of handover authentication protocols for mobile wireless

**He:2018:LAB**


**He:2015:IEI**


**Hunt:2018:RDS**


**Islam:2015:MBA**


**Ibrahim:2019:RAM**

Tahir Musa Ibrahim, Shaﬁ’i Muhammad Abdalhamid, Ala Abdusalam Alaroood, Haruna Chiroma, Mohammed Ali Al-garadi, Nadim Rana, Amina Nuhu Muhammad, Adamu Abubakar, Khalid Haruna, and Lubna A. Gabralla. Recent advances in mobile touch screen security authentica-
REFERENCES

Ismail:2010:EAE


Islam:2011:MES


IBM:2013:DMP


IBM:2013:IPC


Irshad:2017:CPP


IEEE:2010:PIA

REFERENCES


REFERENCES


Irshad:2016:EAM


Ishai:2014:PCP


Jacobs:2016:STB


Jie:2010:AAI


Jie:2011:RGA


Prins:2011:DCA

JR Prins and Business Unit Cybercrime. Diginotar certificate authority breach
REFERENCES


Jain:2013:MSD


Jho:2016:SSE


Jia:2018:ERH


Jakobsson:2012:AWD


Chang:2012:TRR


Joldzic:2016:TSA

REFERENCES


REFERENCES

ISSN 0001-0782 (print), 1557-7317 (electronic).

**Jawad:2013:GAD**

**Jannati:2019:SOR**

**Jamil:2018:SPU**

**Jan:2019:PBM**

**Jun:2012:IIR**

**Jiang:2016:PPT**
Qi Jiang, Muhammad Khurram Khan, Xiang Lu, Jianfeng Ma, and Debiao He. A privacy preserving three-

**Jovanovic:2012:FAL**


**Josefsson:2016:ECD**


**Jordan:2018:QCS**


**Jiang:2018:AHP**


**Jeong:2012:IKP**


**Jajodia:2012:RET**

Sushil Jajodia, Witold Litwin, and Thomas Schwarz. Recoverable encryption through noised secret over a large cloud. *Lecture Notes in Computer Sci-
Jia:2012:PKD

Jiang:2019:PPP

Ji:2018:DIR

Jiang:2016:OOC

Jiang:2016:UTC
Jain:2012:BAS


Jan:2017:PPB


Johnson:2010:BRF


Johnson:2015:NGA


Joux:2013:NIC


Jin:2019:RPP

Jes:2013:CCP  

Juels:2014:HEE  

Jaiyeola:2018:IPN  

Jalili:2017:EAS  

Jevdjic:2017:ASC  
Jain:2016:APQ

Judi:2017:BCI

Jord:2018:EPE

Jiang:2018:CPA

Jiang:2018:FCP
[JSMG18b] Yinhao 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 In-

Jiang:2012:DCA


Joye:2012:FAC


Juels:2014:INC


Khazaei:2017:COA


Kurkc:2018:CBE


Kornycy:2017:RFT


Koziel:2018:HPS


Kamp:2013:MES


Kamp:2016:MEM

Kammuller:2019:ATI


Kapera:2011:SPD


Kapera:2013:MRM


Katz:2013:RIB


Kong:2015:CSM


Karafyllidis:2012:QGC

Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP


Kim:2011:SSE


Khan:2018:APS


Koz:2012:ASE


Kara:2019:ALS


Kemshall:2011:WMT


Kabirirad:2019:HSG


Kleinjung:2010:FBR

Thorsten Kleinjung, Kazu maro Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA modulus. Report 1.4, EPFL IC LACAL [and others], Station 14, CH-1015 Lausanne, Switzerland [and others], February.

Kikuchi:2012:SSN

KFOS12


Kostic:2019:UNV

KG19


Kramer:2010:FDC

KGO10


Kim:2012:SLT

KGP12


K:2019:IAM

KGP+19


Khedr:2016:SSH

KGV16

Kwon:2010:SEB


Koo:2018:PPD


Khazaei:2010:NBS


Kastner:2010:AOT


Kim:2014:MBM


Khleborodov:2018:FEC

Khalil-Hani:2013:BEB


Kinkelin:2011:UTS


Kim:2016:EPE


Kolsch:2019:SBP


Kai:2011:CIS


Kiayias:2011:TCC


[KK10] Elisavet Konstantinou and Aristides Kontogeorgis. Ramanujan’s class invariants and their use in elliptic curve cryptography. *Computers and
Kawai:2012:SHS

Kawai:2013:SHS

Khalil:2014:CIM

Khan:2015:CMB

Kumari:2018:SAS

Khan:2014:MEK
Muhammad Khurram Khan.

Koblitz:2011:ECC


Khan:2013:EDC


Khan:2014:IPR


Katz:2008:IMC


Kushwah:2011:EIB

Prashant Kushwah and Sunder Lal. An efficient identity based generalized


Patrick Koeberl, Jiangtao

Kumari:2016:UFM

Kumari:2017:DPS

Kim:2012:INS

Kent:2015:AGA

Kumari:2016:UFM
REFERENCES

Keller:2010:D


Khomejani:2010:PCT


Koblitz:2010:BNW


Kiani:2011:MPD


Kifer:2014:PFM


Koblitz:2015:RWE


Koblitz:2016:RWE

[KM16] Neal Koblitz and Alfred Menezes. A riddle wrapped


Kanwal:2015:TTM


Katz:2012:TSP


Kavun:2018:SAE


Kang:2019:NBK


Khovratovich:2010:RCA


Knijnenburg:2017:PCE


Khovratovich:2010:RRA

Dmitry Khovratovich, Ivica Nikolić, and Christian


REFERENCES


[KP18] Aneesh M. Koya and Deepthi P. P. Anonymous hybrid mutual authentication and key agreement scheme for wireless

**Kumar:2017:TAU**


**Kobusinska:2018:BDF**


**Kiltz:2011:EAH**


**Khalid:2016:RHL**


**Kocabas:2012:CPB**


REFERENCES


Kumar:2015:RGB


Kalayappan:2018:PAH


Karthiga:2018:PSA


Korac:2019:FMU


Kocabas:2016:ESM


Khan:2017:TPK

REFERENCES


Kiljan:2017:SAC


Kwon:2018:CEI


Kwon:2018:EIP


Ksiezopolski:2012:QMQ


Kim:2012:SSS


Klingler:2013:UPT

[KSU13] Lee Klingler, Rainer Stein-

Kim:2012:SAH


Khamis:2018:CCT


Kalita:2019:NSM


Kawachi:2012:SKE


Kobayashi:2016:ASC

Kei Kobayashi, Yosuke Totani, Keisuke Utsu, and Hiroshi Ishii. Achieving secure communication over...
REFERENCES


[Klisowski:2012:CCP]


[Kai:2014:FSD]


[Kupcu:2013:DTT]


[Kupcu:2015:OAS]


[Kushner:2013:RSS]


[Kuznetsov:2011:APP]


[KWH16] Wen-Chung Kuo, Chun-Cheng Wang, and Hong-


Lu:2010:MSC

Lathey:2015:IEE

Lackey:2015:UHP

Lallie:2014:PCM

Liang:2015:SEC

Lamonica:2013:LDQ

Landau:2010:SSR
Susan Eva Landau. Surveillance or security?: The


REFERENCES


Laxmi:2017:GGS


Liu:2013:IAG


Liu:2015:IEP


Lathrop:2011:SPI


Lavington:2012:ATH


Li:2015:NAC

[Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia,

Lee:2017:SUE


Liu:2017:GAU


Li:2015:CEH


Li:2017:RNF


Li:2017:CCF

REFERENCES

Liu:2018:VRU


Liang:2014:CCS


Liu:2016:ECD


Liu:2016NOP


Louchene:2013:WMR

Ahmed Louchene and Ammar Dahmani. Watermarking method resilient to RST and compression based on DWT, LPM and phase correlation. *International Journal of Com-
REFERENCES


[Liu:2019:TTR] Zhenhua Liu, Shuhong Duan, Peilin Zhou, and Baocang Wang. Traceable-

**Ledin:2016:RME**


**Lewand:2010:PC**


**Liu:2019:DVP**


**Lago-Fernandez:2014:NAA**


**Leung:2018:TTA**


**Luo:2019:SCT**

Chao Luo, Yunsi Fei, and David Kaeli. Side-channel timing attack of RSA on a GPU. *ACM Transactions


REFERENCES


Ruggero Donida Labati, Angelo Genovese, Enrique

Lee:2019:TES


Lopez-Garcia:2014:PBB


Li:2014:SCA


Liu:2012:FVC


Lee:2010:ISC


Supachote Lertvoratham and Pipat Hiranvanichakorn. Integrating secure multi-path mobile ad hoc network with self-authentication strategy. *International Journal of Computer Ap-


[102x681]REFERENCES


Li:2012:BVS

Lin:2011:ICA

Li:2010:AIS

Liu:2015:SSP

Liu:2018:BBB

LHH11+14


Li:2018:OPP


Li:2010:CCB


Lerch-Hostalot:2013:LMS


Lian:2014:SSA


REFERENCES

Lindell:2014:TCT


Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP

[LJ16] Guo-Qiang Liu and Chenhui Jin. Linear cryptanalysis of PRESENT-like ciphers with secret permutation. The Co-
REFERENCES

Li:2016:IRI

Li:2017:MMA

Li:2018:MMA

Liu:2019:ICA

Li:2019:IID

Li:2017:SQS
Li:2012:OEA


Lesi:2017:SAS


Laszka:2014:STC


Liu:2017:OOA


Liu:2018:PAB


Libert:2016:BRD

REFERENCES


Leva:2013:ABN


Le:2011:RMA


Lee:2015:TSS


Lu:2016:PFC


Lu:2016:PSC


Lee:2010:PMB

[LLC10] Hui-Lung Lee, Chia-Feng

Lee:2011:TA


Li:2015:IBE


Liu:2019:EEA


Li:2015:ANA


Lyu:2019:SPP


Lin:2016:SCU

[LLGJ16] Jingqiang Lin, Bo Luo, Le Guan, and Jiwu Jing. Secure computing using registers and caches: The

**Li:2017:ESD**


**Lyu:2018:PKE**


**Li:2017:CIS**


**Liu:2019:SBC**


**Li:2017:CIS**

Chengqing Li, Dongdong Lin, and Jinhu Lu. Cryptanalyzing an image-scrambling
encryption algorithm of pixel bits. *IEEE Multi-
Media*, 24(3):64–71, July/September 2017. CO-
DEN IEMUE4. ISSN 1070-986X (print), 1941-
org/csdl/mags/mu/2017/
03/mmu2017030064-abs.
.html.

**Li:2017:CCD**

[LHLH18] Tong Li, Zheli Liu, Jin
Li, Chunfu Jia, and Kuan-
Ching Li. CDPS: A cryp-
tographic data pub-
lishing system. *Jour-
nal of Computer and Sys-
tem Sciences*, 89(??):80–
91, November 2017. CO-
DEN JCSSBM. ISSN 0022-
0000 (print), 1090-2724
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0022000016301313.

**Li:2018:CIE**

C. Li, D. Lin, J. Lü,
and F. Hao. Cryptana-
lyzing an image encryption
algorithm based on auto-
blocking and electrocardio-
graphy. *IEEE MultiMe-
dia*, 25(4):46–56, October/
December 2018. CODEN
IEMUE4. ISSN 1070-986x
(print), 1941-0166 (elec-
tronic).

**Li:2010:DCY**

Chengqing Li, Shujun Li,
Kwok-Tung Lo, and Kyan-
doghere Kyamakya. A dif-
f erential cryptanalysis of
Yen–Chen–Wu multimedia
cryptography system. *The
Journal of Systems and
Software*, 83(8):1443–1452,
August 2010. CODEN JS-
SODM. ISSN 0164-1212.

**Lai:2013:SAS**

Chengzhe Lai, Hui Li,
Rongxing Lu, and Xue
man (Sher-
man) Shen. SE-AKA: a se-
cure and efficient group au-
thentication protocol for LTE net-
works. *Computer Networks
(Amsterdam, Netherlands:
1999)*, 57(17):3492–3510,
December 9, 2013. CO-
DEN ????? ISSN 1389-1286
(print), 1872-7069 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S1389128613002570.


Lu:2012:BBE


Lai:2016:GGB


Li:2017:CBS


Lucamarini:2014:QKD


Lambert-Mogiliansky:2012:EI

Le:2016:ADS


Lai:2018:IBB


Lai:2017:FPP


Liu:2014:SCS


Li:2011:NRA


Lv:2013:NTP

REFERENCES


Liu:2019:OMM


Li:2011:CIB


Liu:2013:GPB


Liu:2013:EAF


Ling:2019:SAR


Loeb:2015:MGM


Lopriore:2012:EPP


Lopriore:2015:PMD


Low:2012:BRB


Lin:2011:CRN


in encryption domain. 

Liu:2016:PPO


Libert:2010:KES


Lubicz:2015:GMA


Liskiewicz:2013:GBS


Liskiewicz:2017:SLS


Lin:2018:CPF


Lin:2018:SSS


Lin:2019:CCA


Lin:2017:ESF


Lei:2013:RSW


Landecker:2012:TBB

REFERENCES


www.sciencedirect.com/science/article/pii/S1084804515000612


Dong Hoon Lee and Xiaoyun Wang, editors. Advances in Cryptology — ASIACRYPT 2011: 17th
REFERENCES


[LW13c] Allison Lewko and Brent Waters. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. The Journal of Systems and Software, 86
REFERENCES


Lui:2013:CBS

[LW13c] Lui:2013:CBS

Lui:2016:PAB

[LW16] Li:2019:TFA

Liu:2014:DAF


Li:2019:TFA

Liu:2017:EEC

[LWHS17] Li:2019:TFA

Liu:2011:SBA
REFERENCES

CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Li:2018:SCM


Li:2019:PSA


Lu:2014:HOM


Lu:2012:HOM


Liu:2010:NDC

Liu:2010:SET


Liu:2017:SRG


Liu:2011:PIA


Liu:2016:NSC


Lu:2012:MMA


Li:2010:GCP


Lin:2010:DSM


Li:2011:NIW


Lai:2012:RHB


Li:2014:EMK


Li:2014:IBD


Li:2012:ESD

[Xiong Li, Yongping Xiong, Jian Ma, and Wendong Wang. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Ap-

Luo:2014:ARP


Liu:2015:SDS


Lim:2016:AKE


Li:2010:AFF


Liu:2018:IMM


Lu:2014:DAN

[LYHH14] Jiqiang Lu, Wun-She Yap, Matt Henricksen, and


Xin Liao, Qiao yan Wen, Ying Sun, and Jie Zhang.

Lai:2019:NIB


Liu:2016:FIT


Lai:2018:NSH


Liu:2018:SKR


Li:2013:SSS

Leng:2011:DKB


Liu:2012:SOCa


Luo:2012:LVT


Liu:2014:PKE


Liu:2017:ESS


Liu:2014:CRA


**Li:2019:APA**


**Li:2010:PES**


**Liu:2019:IEU**


**Li:2012:ESS**


**Li:2019:ESM**


REFERENCES


With a foreword by Christopher M. Bishop.


Stefan Mangard. Keeping secrets on low-cost chips. IEEE Security & Privacy,
REFERENCES


Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP

Matthiessen:2019:RCM

Maurer:2012:CCN

Mayron:2015:BAM

Mazurczyk:2013:VSD

Milo:2011:FGB

Mao:2015:PUA

Matias:2018:NNZ
P. Matias, P. Barbosa,


Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. A parallel efficient architecture for large cryptographically robust $n \times k(k \geq n/2)$ mappings. *IEEE Transactions on Computers*, 60(3):375–385, March 2011. CODEN ITCOB4. ISSN 0018-9340
Matula:2019:PCG

David W. Matula and Zizhen Chen. Precise and concise graphical representation of the natural numbers. In Takagi et al. [TBL19], pages 100–103. ISBN 1-72813-366-1. ISSN 1063-6889.

Madanayake:2012:BPS


McGrew:2017:IDH


McGraw:2016:SBTd


McKay:2010:SLB


McKay:2011:SLB

Sinclair McKay. The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were
REFERENCES


McKay:2012:SLC


Ma:2019:TOP


Mahmood:2018:ECC


Marquez-Corbella:2015:ECP


Mhenni:2019:DSA


Mathew:2015:NMB


[MCS+15]

[MCP15]

[MCRB19]

[MCN+18]

[MCK12]
Majzoub:2012:MRH


Mansouri:2012:ACA


Mansfield-Devine:2015:MIC


Moffat:2010:CPB


Malina:2018:SET


Mosenia:2017:PTS

Arsalan Mosenia, Xiao-

Maachaoui:2012:MLA


Meiklejohn:2010:BRB


Menezes:2013:IPB


Menn:2013:ESC


Meshram:2015:EIB


Mandal:2016:DIW

REFERENCES

9087 (print), 1558-3465 (electronic).


[MH14] Takahiro Matsuda and Goichiro Hanaoka. Cho-


[Mou:2013:CBC] Luntian Mou, Tiejun

Mohd:2015:SLB


Ma:2019:PFC


Mohd:2018:HDM


Micciancio:2010:FGC


Michiels:2010:OWB

REFERENCES

1540-7993 (print), 1558-4046 (electronic).

Michael:2016:RNI

K. Michael. RFID/NFC implants for Bitcoin transactions. *IEEE Consumer
Electronics Magazine*, 5(3): 103–106, July 2016. ISSN 2162-2248 (print), 2162-
2256 (electronic).

Midgley:2010:SEE

Stephen Midgley. The state of encryption in Europe: some cultural comparisons.
*Network Security*, 2010(8): 18–19, August 2010. CO-DEN NTSCF5. ISSN 1353-
www.sciencedirect.com/
science/article/pii/S1353485810701070.

Martinez-Julia:2012:NIB

P. Martinez-Julia and A. F. Gómez-Skarmeta. A novel identity-based network ar-
chitecture for next generation Internet. *J.UCS: Journal of Universal Com-
puter Science*, 18(12): 1643–??, ???? 2012. CO-DEN ???? ISSN 0948-
6968. URL http://www.
jucs.org/jucs_18_12/a_novel_identity_based.

Martinez-Julia:2013:BSI

Pedro Martinez-Julia and Antonio F. Skarmeta. Beyond the separation of identi-
fier and locator:

Building an identity-based overlay network architecture for the Future Inter-
et. *Computer Networks (Amsterdam, Netherlands: 1999)*, 57(10):2280–2300,
July 5, 2013. CO-DEN ???? ISSN 1389-1286
(print), 1872-7069 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1389128613000066.

Miao:2019:PPT

Chenglin Miao, Wenjun Jiang, Lu Su, Yahang Li, Suxin Guo, Zhan Qin, Houping Xiao, Jing Gao, and Kui Ren. Privacy-
preserving truth discovery in crowd sensing systems.
DEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic). URL https://
dl.acm.org/ft_gateway. cfm?id=3277505.

Memon:2018:TFS

Towards federated service discovery and identity management in collabora-
tive data and compute cloud infrastruc-
DEN ???? ISSN
Mohanty:2011:RTP


Moessner:2012:SAS


Muller:2012:HPC


Mozaari-Kermani:2017:FD


Mozaari-Kermani:2018:ERE

Daniel McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann. State management for hash-based signatures. *Lecture Notes in Computer Science*, 10074:
REFERENCES


Chandrashekhar Meshram and Suchitra A. Meshram.


Paulo Martins, Jeremy

Merlo:2015:MEP

Mailloux:2016:PSS

Miao:2016:RAS

Maeng:2015:TAU

Moldovyan:2012:BBD

Mahmoody:2014:PPK
Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key en-


This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.


REFERENCES

448


Minier:2012:RKI


Mizuki:2011:ASN


Maimut:2012:LCR


Minamoto:2014:BDI


Mone:2013:FPE


Moore:2012:RFF


**Moody:2014:DMW**


**Morad:2012:OEA**


**Morawiecki:2019:MS**


**Moriai:2019:PPD**


**Mosca:2018:CEQ**


**Moullick:2015:RDS**


**Minier:2012:EEC**


**Min:2018:AAB**


**Meiklejohn:2016:FBC**


**Mundhenk:2017:SAN**


**Mironov:2012:IDP**


**Mukhamedov:2010:IEP**


**Maimut:2014:AET**

Marasco:2014:SAS

Micali:2014:CMS

Manimehalai:2016:NRR

Migliore:2018:HSC

Moataz:2018:SSE

Martinovic:2017:AUP


Morales-Sandoval:2018:PBC


Montuschi:2016:ISC


Marton:2010:RDC


Mashimo:2018:VMS


Mosenia:2017:CCA


Mazurczyk:2013:FWS

W. Mazurczyk, K. Szczypiorski, and J. Lubacz. Four ways to smuggle messages through Internet services. *IEEE Spectrum*, 50(11):42–45, November 2013. CO-
DEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

**Martins:2018:SFH**

**Muhammad:2018:ISU**

**Migliore:2017:HSA**

**Maitra:2017:DFA**

**Maitra:2018:TA**

**Miret:2018:PBC**
Josep M. Miret, Daniel Sadornil, and Juan G. Tena. Pairing-based cryptography on elliptic curves.
REFERENCES


REFERENCES


Ali Miri and Serge Vaudenay, editors. Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11–12, Revised Selected Papers, volume 7118 of Lecture Notes in Computer Science. Springer-Verlag,
REFERENCES


REFERENCES


Mathew:2012:EIC


Moghimi:2019:MFD


Meng:2018:TTB


Ma:2012:CIS


Mahmoody:2013:LEZ

REFERENCES

Ma:2013:PVP

Meng:2015:CRS

Marko:2017:MDI

Mastroeni:2017:APS

Manshaei:2013:GTM

Ma:2015:PKE

Meng:2019:ESF
[MZL19] Weizhi Meng, Liqiu Zhu, Wenjuan Li, Jinguang Han, and Yan Li. Enhancing the security of FinTech


[NACLER12] J. A. M. Naranjo, N. A-

**Nagaraj:2019:RCC**


**Nunez:2017:PRE**


**Namasudra:2019:IAB**


**Noureddine:2013:AMT**


**Nain:2017:SPE**


Xuan Thuy Ngo, Jean-Luc Danger, Sylvain Guilley, Tarik Graba, Yves Mathieu, Zakaria Najm, and...


REFERENCES

Nafea:2016:HMB

Nievergelt:2002:FLM

NIST:2012:RRN

NIST:2013:CSS

NIST:2015:SSP

Najafi:2019:VRS


Nieto:2013:PVC


Nieto:2014:FSH


Ntantogian:2015:GTF


Nguyen:2012:DQB


Neville-Neil:2015:KVH


Nagy:2010:KDV

REFERENCES


Tyler Nichols, Joe Fletcher, Braden Hollenbaek, Adam Bates, Dave Tian, Abdulrahman Alkhelaifi, and Kevin Butler. CertShim: Securing SSL certificate verification through dynamic linking. In ?????, editor, ACM Conference on
REFERENCES

469


Nguyen:2011:APB


Nguyen:2012:SOU


Negre:2015:NPA


Namasudra:2017:NSA


Niu:2015:CRS


Naccache:2010:THI

REFERENCES


[NBX+18] Koki Nagano, Jaewoo Seo, Jun Xing, Lingyu Wei,

Nandakumar:2017:CAI


Nguyen:2012:LRS


Nguyen:2010:LAS


Noorman:2017:SLC

Nie:2013:CHB


Natgunanathan:2017:PBM


Ntantogian:2010:GME


Newell:2014:NCR


Niu:2015:NAS


Nikooghadam:2010:EUE

REFERENCES

Obana:2011:AOC

Oligeri:2011:REA

Obrenovic:2012:IUC

Odelu:2017:PSA

Ozturk:2017:CAH

Oggier:2011:ACA
REFERENCES


Or-Meir:2019:DMA

Ortiz-Martin:2019:FAI

Ogiela:2018:LTC
REFERENCES

Orlandi:2014:SCN

Obert:2016:PAE

Oppliger:2011:CC

Orumiehchiha:2014:PAN

Orejel:2014:E

Ormond:2016:CPR

Ozen:2011:MIS
Mehmet Özen and Vedat Şiap. The MacWilliams

Owczarek:2012:LPL


Osborn:2016:SSR


Ohtake:2019:OSA

REFERENCES

Odelu:2019:EPP


Orencik:2016:MKS


Okamoto:2012:AAH


Otmani:2010:CTM


Ogiela:2018:VCA


Ohzeki:2012:NWM

Kazuhiro Ohzeki, YuanYu Wei, Yutaka Hirakawa,

**Ortiz-Yepes:2014:BSA**


**[OYHSB14]**


**[PA10]**


**[OYHSB14]**


**[PA15]**


**[Pal16]**

Jiban K. Pal. Administering a cryptology centre by means of scientometric

**Pandey:2014:ACR**


**Parent:2012:WAI**


**Park:2012:APO**


**Park:2018:OTP**


**Pass:2013:USP**


**Pranata:2013:MDR**

Ilung Pranata, Rukshan Athauda, and Geoff Skinner. Modeling decentralized reputation-based trust for initial transactions in digital environments. *ACM Transactions on Internet
REFERENCES

Paulson:2010:SDO

Paul:2019:RCS

Pandit:2012:EFS

Poh:2017:SDV

Park:2014:FRI

Poddar:2019:AED
REFERENCES

Pun:2014:GIT


Paul:2016:TSO


Papadopoulos:2014:LQA


Perkovic:2019:LVL


Premnath:2014:EHR


Poh:2017:SSE


Joss Pearson, editor. Neil Webster’s cribs for victory: the untold story
REFERENCES


Morgan E. Peck. Blockchain world — do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectrum, 54(10):38–60, October 2017. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).


Alberto Peinado and Amparo Fuster-Sabater. Cryptographic analysis of a

**Poppelmann:2012:TEA**


**Pendleton:2017:SSS**


**Peng:2010:SFW**


**Park:2012:IDF**


**Pohls:2012:RDI**


REFERENCES


Patel:2018:LLA


Premarathne:2015:LDD


Peter:2012:AHE


Phuc:2016:SAS

Tran Song Dat Phuc and Changhoon Lee. Security analysis of SDDO-
based block cipher for
wireless sensor network.
The Journal of Supercom-
puting, 72(9):3619–3628,
September 2016. CODEN
JOSUED. ISSN
0920-8542 (print), 1573-
0484 (electronic). URL
http://link.springer.
com/article/10.1007/s11227-
015-1589-3.

Perez:2011:FDS
[PLCGS11] Alejandro Pérez, Gabriel
López, Óscar Cánovas,
and Antonio F. Gómez-
Skarmeta. Formal descrip-
tion of the SWIFT iden-
tity management frame-
work. Future Generation
Computer Systems,
27(8):1113–1123,
October 2011. CODEN
FGSEVI. ISSN
0167-739X (print), 1872-
7115 (electronic).

Peris-Lopez:2010:CSP
[PLSvdLE10] Pedro Peris-Lopez,
Enrique San Millán, Jan
C. A. van der Lubbe,
and Luis A. Entrena.
Cryptographically secure
pseudo-random bit gener-
ator for RFID tags. In
2010 International Confer-
ence for Internet Technol-
ogy and Secured Transac-
tions (ICITST), pages 1–
6. IEEE Computer Society
Press, 1109 Spring Street,
Suite 300, Silver Spring,
MD 20910, USA, 2010.
URL http://ieeexplore.
ieee.org/stamp/stamp.
jsp?tp=&arnumber=5678035.

Pang:2013:IMA
Liaojun Pang, Huixian
Li, Qingqi Pei, and Yu-
min Wang. Improvement
on Meshram et al.’s ID-
based cryptographic mech-
anism. Information Pro-
cessing Letters,
113(19–21):789–792,
September/
October 2013. CODEN
IFPLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0020019013002081.

Peris-Lopez:2018:EAC
[PLGMCdF18] Pedro Peris-Lopez,
Lorena González-Manzano,
Carmen Camara, and José María
de Fuentes. Effect of at-
tacker characterization in
ECG-based continuous au-
thentication mechanisms
for Internet of Things.
Future Generation Com-
puter Systems,
81(??):67–77,
April 2018. CODEN
FGSEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0167739X17300407.

Perumal:2019:SDE
Kaliram Perumal, Sug-
anthi Muthusamy, and
Gowrison Gengavel. Sparse
data encoder and decoder
to improve security in

Pisani:2019:ABS


Poh:2012:SEC


Pande:2013:SMC


Poursakidis:2010:TPC


Puthal:2017:DDK


Niu:2014:RDW

Pan pan Niu, Xiang yang Wang, Hong ying Yang, Pei Wang, and Ai long

**Powers:2014:OSCa**


**Paar:2010:UCT**


**Papadopoulos:2010:TRM**


**Park:2011:ACC**


**P:2018:ABE**


**Pereira:2016:SHB**


**Pennino:2019:PIS**


**PPG19**

Pennino:2019:PIS

**PPRT12**


**Pathak:2012:PPS**

Pendl:2012:ECC


**PPH12**

Pendl:2012:ECC

**PPRT12**


**Phan:2012:DDB**


**Phan:2012:MBT**

Duong Hieu Phan, David Pointcheval, and Mario


**PPR12**


**Phan:2012:MBT**

Young June Pyun, Younghee Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing

**PPR+12**

Young June Pyun, Younghee Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing

**PPS12a**


**Phan:2012:MBT**

Young June Pyun, Younghee Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing

**PPS12b**


**Phan:2012:MBT**

Papadopoulos:2015:PAP


Pandey:2012:PPS


Perez-Resa:2019:SSE


Puthal:2019:SAL


REFERENCES

Pankhuri:2019:PBM

Papamasthounou:2013:SCC

Peng:2019:GCS

Papamasthounou:2016:AHT

Papamasthounou:2018:ICA

Papamasthounou:2016:AHT
Charalampos Papamasthounou, Roberto Tamassia, and Nikos Triandopoulos. Authenticated hash tables based on cryptographic accumulators. Al-
Pudo:2012:RKA

Padget:2017:FGA

Pellikaan:2017:CCC

Pei:2013:ARW

Pham:2019:SSS

Puthal:2019:SSE


REFERENCES

Pei:2015:SWT


Papadopoulos:2010:CAR


Phuong:2018:CBE


Popa:2015:HCD


Pouroughi:2018:NNE


Peng:2019:EDI

REFERENCES


Qin:2017:DIR


Qiu:2019:CPT


Qiao:2018:CTC


Quaglia:2018:SVA

Elizabeth A. Quaglia and Ben Smyth. Secret, ver-

**Qin:2016:STI**


**Qian:2014:IAF**


**Qiang:2016:SCF**


**Qi:2016:SID**


**Qi:2016:SPR**


**Qin:2018:BRO**

Baodong Qin, Qinglan Zhao, and Dong Zheng. Bounded revocable and outsourcable ABE for se-


[Royal Academy of Engineering] Rabin:2016:HSP


[Royal Academy of Engineering] Rauscher:2015:FMT

REFERENCES


[R:2018:SDM]

Rao:2019:HPR


[R:2018:PPS]

Rabbachin:2015:WNI


[R:2015:WNI]


REFERENCES

September 15, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).


[RNQ16] Peter Y. A. Ryan, David

[Rom11]


[Ros11]

Kurt Rohloff. Computer arithmetic research to accelerate privacy-protecting encrypted computing such as homomorphic encryption. In Takagi et al. [TBL19], page 197. ISBN 1-72813-366-1. ISSN 1063-6889.

[Roh19]


[Rom12]


[Rom11]


[Ros11]

<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Title</th>
<th>Conference/Journal Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Abdul Razaque and Syed S. Rizvi</td>
<td>Secure data aggregation using access control and authentication</td>
<td></td>
</tr>
</tbody>
</table>


[RS17b] Rivest:2017:WEV


[RSCX18] Roetteler:2018:QCC


[RSD19] Rangasamy:2012:ERP


[RSD19] Rastegari:2019:ECS
Parvin Rastegari, Willy Susilo, and Mohammad
REFERENCES


Roy:2015:SCP


Ribeiro:2015:QBS


Resende:2019:BMI


Rui:2014:DAC


Rahulamathavan:2019:PPI


Ryan:2015:EEV

[RST15a] Peter Y. A. Ryan, Steve Schneider, and Vanessa

Ryan:2015:EEVb


Rexha:2018:ITF


Russo:2015:FPT


Rodriguez-Vazquez:2012:SCB

REFERENCES

Reaves:2018:CSS

Roettger:2012:PKC

Ren:2014:HHM

Rogaway:2012:SCS

Ren:2013:PPK

Ristenpart:2010:WGR
REFERENCES

ndss/10/pdf/15.pdf;
http://www.isoc.org/isoc/
conferences/ndss/10/proceedings.shtml.


[SA12] Ren:2013:DSE


dl.acm.org/ft_gateway. cfm?id=3356867.

Rajendran:2015:FAB


[SA16] Sang:2012:SSF

www.sciencedirect.com/
science/article/pii/S0377042713002719.

Somanatha:2015:RAK

Revathi Bangalore Somanatha and J. William Atwood. Router authentication, key management, and adjacency management for securing inter-router control messages. Computer Networks (Amsterdam, Netherlands:
REFERENCES


Shivani:2016:PVC


Siad:2016:NFI


Subramanian:2019:SAF


Saarinen:2012:PPK


Suoranta:2012:SAM


Sarreshtedari:2015:WMD

Schutz:2010:DIN


Sacco:2014:MC


Sahai:2013:TCT


Saeed:2016:IID


Saleh:2016:PED


Suomalainen:2018:SAS

Sadat:2019:SSG


Saracevic:2019:NAS


Sarier:2010:IAS


Sarier:2012:SNB

Neyire Deniz Sarier. Security notions of bio-

Sarkar:2010:SGC


Sarkar:2011:TES


Savage:2013:PP


Savage:2015:NVS


Savage:2016:NKP


Safkhani:2017:PSD


Shwartz:2018:DMI


Stevens:2017:AFS


Sarkar:2015:DFA


REFERENCES

Sujitha:2019:HSP


Sun:2016:TCA


Saevanee:2015:CUA


Schoenmakers:2010:VS


Schwartz:2011:IMP

Schaathun:2012:MLI


Schneier:2013:HDD


Schaefer:2015:BRB


Schneier:2012:LOE


Schoon:2012:DES

REFERENCES

Schneier:2015:DGH

Schneider:2016:MSI

Schneider:2016:DEE

Schneider:2016:CHT

Schneier:2018:CAA

Schneider:2019:CP1

Scholl:2019:SIE

Shrestha:2010:KBA
Anish Prasad Shrestha, Dong-You Choi, Goo Rak Kwon, and Seung-Jo Han.
REFERENCES


Stobert:2018:tal


Seberry:2010:ctaa


Seberry:2010:ctab


Scriber:2018:fdb


Shree:2019:erc


Smith-Creasey:2019:nwi

Max Smith-Creasey and Muttukrishnan Rajarajan. A novel word-independent gesture-typing continuous authentication scheme for

Shu:2015:PML


Saleh:2010:GTF


Shen:2012:PAS


Sengupta:2017:USB


Streit:2018:PQK


Sherman:2017:ICC

[Alan Sherman, Melissa Dark, Agnes Chan, Ry-


Hwajeong Seo. Compact software implementation of public-key cryptography on MSP430X. *ACM Transactions on Embedded Computing Systems*, 17(3):
Serrato:2012:IAN


Sallam:2012:EBM


Sakai:2016:CDN


Sethumadhavan:2016:HEP


Severance:2016:BSB


Seo:2018:AOF


Sakellariou:2019:HEK


Sgantzos:2019:AII


Shu:2014:DAS


Saxena:2016:API


Silva-Garcia:2018:SBG


S:2018:EDS

REFERENCES

Sanchez-Garcia:2016:SSA


Susilo:2016:EDT


Shankar:2012:BDF


Shim:2011:SA


Shparlinski:2003:CAA


Shparlinski:2010:NWP


Suoranta:2012:ASM


Shyu:2015:VCR


Satir:2012:CBT

Siad:2012:NAP


Simpson:2010:ESB


Simion:2015:RST


Simmonds:2015:DII


Sirt:2016:TPS


Shakeri:2012:RZW


Sartakhti:2019:CPL

Javad Salimi Sartakhti and Saeed Jalili. On the computational power of the light: a plan for breaking Data Encryption Standard. Theoretical Com-
REFERENCES


Scarani:2014:BPQ


Sepczuk:2018:NRB


Son:2017:NOC


Saha:2018:ASS


Soupionis:2014:GTA


Sirivianos:2014:LSF

Michael Sirivianos, Kyungbaek Kim, Jian Wei Gan, and Xiaowei Yang. Leveraging social feedback to verify online identity

Seo:2015:AEC


Shin:2017:SSD


Szalachowski:2010:CCG


Stevens:2015:FCF


Singh:2018:MWT


Scheidat:2012:STT

Tobias Scheidat, Karl Kimmels, and Claus Vielhauer. Short term template aging effects on biometric dynamic handwriting authentication performance. Lecture Notes in
Schmitz:2012:NAC

[SLL+19]

Srivatsa:2011:ESA

[SLM10]

Schultz:2010:MMP

[SLL10]

Su:2016:SSP
Shenghui Su, Shuwang Lü, Maozhi Xu, and Tao Xie. A semantically secure public key cryptoscheme using

**Sun:2016:RSP**


**Slovak:2016:DCD**


**Sarkar:2010:CRM**


**Sorniotti:2010:PSS**


**Seyedzadeh:2011:IES**


**Stanton:2010:FAD**


**Salmon:2011:PRN**

John K. Salmon, Mark A. Moraes, Ron O. Dror, and David E. Shaw. Parallel random numbers: as easy as 1, 2, 3. In Lathrop et al. [LCK11], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ???.

**Smith:2011:SSX**


**Smith:2011:RBA**


**Smith:2015:HBB**


**Smith:2015:DBP**


**Swierczynski:2015:PSE**

Paweł Swierczynski, Amir Moradi, David Oswald, and Christof Paar. Physical security evaluation of the bitstream encryption mechanism of Altera

**Stankovski:2014:CFE**


**Sucasas:2016:APP**


**Sharma:2018:CSS**


**Sadeghi:2010:THI**


**Son:2018:GFD**

Yumnok Son, Juhwan Noh, Jaeyeong Choi, and Yongdae Kim. GyrosFinger: Fingerprinting drones for location tracking based on the outputs of MEMS gyroscopes. *ACM Transactions on Privacy and Security*


**Strizhov:2016:SPS**


**Suresh:2015:AGU**


**Serwadda:2013:ELK**


**Shiaeles:2015:FI**


**Shim:2015:SDA**


**Spafford:2016:SE**

Eugene H. Spafford. The strength of encryption.
Salvail:2010:STR


SHERMAN:2019:PBL


SKRACIC:2017:AAU


SAKHKANI:2014:CCT


SUN:2013:IUP

San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov.

[Serwadda:2016:TRR]

[Shaikh:2010:CTO]

[Schilling:2012:ATU]

[Sur:2012:SSU]

[Stanton:2014:BRB]


**Saklikar:2010:IFV**


**Saxena:2010:SGC**


**Sopka:2010:BTS**


**Szaban:2011:IQB**


**Saxena:2012:BIT**


**Shparlinski:2012:CSD**

REFERENCES


Schillewaert:2014:CCA


Shrestha:2015:CIS


Shen:2016:RMM


Sethumadhavan:2019:SA


Stanoyevitch:2011:ICM


Sta11b


Stanek:2012:TEM

Martin Stanek. Threshold encryption into mul-
REFERENCES


Stiles:2019:HSB


Stolte:2012:EDA


Suciu:2012:SED


Sun:2016:NEB


Shen:2015:CSC


Song:2016:IAR

Shmueli:2014:IDE


Svozil:2014:NCC


Svaba:2010:PKC


ShanmugaPriya:2019:PAS


Shi:2019:LWW


Shoufan:2010:NCA

REFERENCES

Song:2016:IBS


Song:2017:PPF


Sha:2019:CED


Su:2016:PSN


Sahillioglu:2014:SCM

Y. Sahillioğlu and Y. Yemez. Shapes and cryptography: Multiple shape correspondence by dynamic


Sun:2017:CPP


Shen:2014:ERC


Sun:2018:RPP


Tsang:2010:BRR


Tamayo:2015:AFH


Tan:2011:CTA


Sheng-Hua Teng. 2018


Gurkan Tuna, Dimitrios G. Kogias, V. Cagri Gungor, Cengiz Gezer, Erhan

Tu:2014:EPB


Tu:2013:PAQ


Tariq:2014:SBL


Tan:2016:ESE

REFERENCES


Tsoutsos:2018:EDM

Tang:2015:ECP

Tormo:2013:IMP

Terrovitis:2011:LGR

Terrovitis:2012:PPD

Tao:2018:AAC
Ming Tao, Kaoru Ota, Mianxiong Dong, and Zhuzhong Qian. AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks.


**Tezcan:2016:IID**


**Tschorsch:2016:BBT**


**Taassori:2018:VRP**


**Tao:2014:CFS**


**Toreini:2017:TRP**


**Tang:2011:IDC**

Xuehai Tang, Bing Sun, Ruilin Li, and Chao Li. Impossible differential cryptanalysis of 13-round CLEFIA-128. *The Journal of Systems and
REFERENCES


REFERENCES

Tupakula:2015:TES


Tripunitara:2014:CKM


Turan:2019:CFF


Wu:2012:SWG


Thorpe:2012:CRB


Toor:2018:VQA

Tartary:2011:EIT


Tian:2012:SSB


Trost:2016:OPC


Tan:2016:CCA


Tolba:2016:GMA


Trammel:2012:DTP

REFERENCES


Y. Tian: 2017: ORA


P. Teh: 2016: STD


E. ul Haq: 2018: CAS


O. Uzunkol: 2018: SWU


D. Unruh: 2015: RQT


M. Ul Hassan: 2019: DPR

[URK19] Muneeb Ul Hassan, Mubashir Hussain Rehmani, Ramamoohanarao Kotagiri, Jiekui Zhang, and Jinjun Chen. Differential privacy for renewable energy resources


[VenafiLabs:2014:VLQ] Venafi Labs. Venafi Labs Q3 Heartbleed threat re-


[Vo:2019:ISA] Tri Hoang Vo, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell. Identity-as-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. Future Internet,
REFERENCES


**Voulgaris:2019:BTI**


**Vernize:2015:MNI**


**Vijayarajan:2019:BKB**


**Vrakas:2014:OUI**

[NV14] Nikos Vrakas, Dimitris Geniatakis, and Costas...

**Viennot:2014:MSG**


**Vasish:2018:DEU**


**Vu:2015:NAN**


**Vgena:2019:TAL**


**Vasiliadis:2017:DIS**

REFERENCES

1063-6692 (print), 1558-2566 (electronic).

Vleju:2012:CCA

Vivek:2014:CSC

Vliegen:2015:SRD

Veloudis:2016:NPH

Vollala:2017:EEM

VonMaurich:2015:IQM
Varadharajan:2018:AUR


vanRijswijk-Deij:2017:PIE


Vembuselvi:2011:LLL


Vassilev:2016:ESU


Voris:2019:AAU


Vivek:2012:CSE

Vlac\-\-hos:2015:DPC


vanTilborg:2011:ECS


Viswanathan:2018:EEG


Vuagnoux:2010:CAC


vanVredendaal:2016:RMM


VanDijkhuizen:2018:SNT


Vazirani:2019:FDI

Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *Communications of the Association for*
REFERENCES


Valente:2019:SSA


Wagstaff:2010:C


Wagner:2016:TPF


Woo:2019:UEM


Walter:2018:RCS


Wang:2010:NSB

REFERENCES

Wang:2013:CRA

Wang:2014:IIA

Wang:2018:LRI

Wang:2018:PPA

Ward:2011:CCM

Watt:2010:IPI
REFERENCES


Waters:2012:FER


Watts:2014:ICB


Watts:2014:PYI


Watts:2015:HGA


Wang:2012:PCE


Weisse:2017:RLC


Wright:2010:USP

[WBC10] Charles V. Wright, Lucas Ballard, Scott E. Coull, Fabian Monrose, and Gerald M. Masson. Uncover-

Wu:2018:ESS


Wang:2019:IFT


Wang:2018:SNU


Wei:2018:GCQ


Wu:2017:HMA

REFERENCES


Wang:2018:SEA

Wei:2012:NTB

Wazid:2019:DSK

Wazid:2018:AKM

Wang:2019:FTSa


REFERENCES

Wang:2010:DVT

[WGJT10] Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deter-
ring voluntary trace disclosure in re-encryption mix-
18:1–18:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-
7406 (electronic).

Wang:2012:BRR

[WgMdZlZ12] Ding Wang, Chun guang Ma, Sen dong Zhao, and Chang li Zhou. Break-
ing a robust remote user authentication scheme using smart cards. *Lecture
com/chapter/10.1007/978-3-642-35606-3_13/.

Wang:2012:SPB

[WgMW12] Ding Wang, Chun guang Ma, and Peng Wu. Secure password-based remote
user authentication scheme with non-tamper resistant smart cards. *Lecture
Notes in Computer Science*, 7371:114–121, 2012. CODEN LNCSD9. ISSN
com/chapter/10.1007/978-3-642-31540-4_9/.

Wei:2012:NCI

[WGZ+12] Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, and Shiguo Lian.
A novel color image encryption algorithm based on DNA sequence opera-
tion and hyper-chaotic system. *The Journal of Systems and Software*,
85(2):290–299, February 2012. CODEN JS-SODM. ISSN 0164-1212
science/article/pii/S0164121211002147.

Wang:2017:DRM

[WH17] Yi Wang and Yajun Ha. A DFA-resistant and masked PRESENT with area opti-
mization for RFID applications. *ACM Transactions on Embedded Com-
puting Systems*, 16(4):102:1–102:??, August 2017. CODEN ???. ISSN 1539-
9087 (print), 1558-3465 (electronic).

Wang:2018:GAD

[WH18] Lin Wang and Zhi Hu. On graph algorithms for degeneracy test and recursive
description of stream ciphers. *Fundamenta Informaticae*, 160(3):343–359,
???? 2018. CODEN FU-MAAJ. ISSN 0169-2968
REFERENCES


REFERENCES

CMJ6. ISSN 0010-4620

Wang:2018:VMF
Nana Wang and Mohan Kankanhalli. 2D vector map fragile watermarking with region location.
ACM Transactions on Spatial Algorithms and Systems (TSAS), 4(4):12:1–12:??, October 2018. CO-
DEN ???. ISSN 2374-0353. URL https://doi.acm.org/citation.cfm?id=3239163.

Wang:2016:DRS
Zhen Wang, Mark Kar-
povsky, and Lake Bu. De-
sign of reliable and secure devices realizing Shamir's secret sharing.
IEEE Transactions on Comput-
ers, 65(8):2443–2455, ????, 2016. CO-
DEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Wu:2011:HQI
Chia-Chun Wu, Shang-
Juh Kao, and Min-Shiang Hwang. A high quality image sharing with steganography and adaptive authentication scheme.
The Journal of Systems and Software, 84(12):2196–2207, December 2011. CO-
DEN JSSODM. ISSN 0164-1212 (print), 1873-

Weissman:2011:LLB
Clark Weissman and Timo-
thy Levin. Lessons learned from building a high-
assurance crypto gateway.
7993 (print), 1558-4046 (electronic).

Wang:2012:MCE
Jinwei Wang and Shiguo Lian. On multiwatermark-
ing in cloud environment.
Concurrency and Compu-
tation: Practice and Expe-
rience, 24(17):2151–2164, December 10, 2012. CO-
DEN CCPEBO. ISSN 1532-0626 (print), 1532-
0634 (electronic).

Wu:2019:VFS
Zhiqiang Wu and Kenli Li. VBTREE: forward secure conjunctive queries over encrypted data for cloud computing.
VLDB Journal: Very Large Data Bases, 28(1):25–46, February 2019. CO-
DEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic).


[Wu:2012:PSC] Wei Wu, Yi Mu, Willy Susilo, Xinyi Huang, and Li Xu. A provably secure construction of certificate-

Watanabe:2014:OAC


Wang:2017:CES


Wo:2015:UFS


Wendzel:2015:CME

Wang:2017:PPK

Wang:2016:SEP

Wu:2016:CBE

Wei:2015:TPE
Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-expression searches. International Journal of In-


Wang:2015:RSA


Wang:2014:NDH


Wang:2019:CPB


Wu:2016:BPK


Watanabe:2012:ITT

Wei:2019:VFA


Wang:2012:PAC


Wu:2010:IBM


Wang:2013:NMC


Wang:2012:EUA

[TWT12] Tsu-Yang Wu, Yuh-Min Tseng, and Tung-Tso Tsai. A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. Computer Networks


Long Wen, Meiqin Wang, Andrey Bogdanov, and HuaiFeng Chen. Multidimensional zero-correlation attacks on lightweight


Wang:2011:CHI


Wu:2017:EAK


Wang:2017:FWA

Ran Wang, Guangquan Xu, Bin Liu, Yan Cao, and Xiaohong Li. Flow watermarking for anti-noise and multistream trac-
Wang:2019:NTB


Wang:2017:SRS


Wang:2010:IIB


Weir:2012:IHV


Wang:2013:NSW

[WYL13] Xiaogang Wang, Ming Yang, and Junzhou Luo. A novel sequential watermark detection model for efficient traceback of se-

Wang:2014:NAI


Weir:2012:AVC


Wang:2017:SRS


Wang:2010:IIB


Weir:2012:IHV


Wang:2013:NSW


Wei:2014:IDC


Wu:2018:SMI


Wei:2016:APS


Wang:2013:BSB


Wang:2014:CGR


Wang:2017:RRA


REFERENCES


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS


Wang:2012:NIS

REFERENCES


Kaiping Xue, Jianan Hong, Yingjie Xue, David S. L. Wei, Nenghai Yu, and Peilin Hong. CABE: A new comparable attribute-based encryption construction with 0-encoding and 1-encoding. IEEE Transactions on Computers, 66 (9):1491–1503, September 2017. CODEN IT-


Xu:2013:PKE


Xu:2019:TPT


Xue:2018:SNN


Xiong:2009:PSI


Xiang:2016:EMP

REFERENCES


[Xue:2013:TCB] Xue:2013:TCB


REFERENCES


Qian Xu, Chengxiang Tan, Wenye Zhu, Ya Xiao, Zhijie Fan, and Fujia Cheng. Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing. *Future Generation
REFERENCES


[Xiong:2012:CBP] Hu Xiong, Qiaoyan Wang,

abs.html.


CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


**Xu:2019:LAM**


**Xiong:2015:SRE**


**Xie:2012:DPK**


**Xiao:2018:KRL**


**Xu:2019:SIC**


**Xing-Yuan:2011:PRS**

[WXYXY11] Wang Xing-Yuan, Qin
REFERENCES


Xiao:2019:NEA


Xu:2015:ORA


Xiong:2019:PPH


Xiong:2012:CLR


Xiao:2018:FEI

Yoo:2017:PQD


Yaacoubi:2019:REM


Yamaguchi:2012:EVC


Yu:2015:SDS


Yang:2010:PII


Yang:2011:PQC

Yang:2014:BEB


Yang:2011:GSS


Yang:2012:PST


Yang:2016:EBB


Yi:2017:ZCL


Yuan:2013:PVQ

Lihua Yuan, Chao-Chih Chen, Prasant Mohapatra, Chen-Nee Chuah, and Krishna Kant. A proxy
REFERENCES


**Yu:2016:DNF**


**Yao:2015:LAB**


**Yuen:2012:IBE**


**Yu:2017:PDA**


**Yasuda:2015:MQC**

Yao:2019:CTC


Yan:2016:DEB


Ye:2010:ACC


Yamada:2012:PBR


Ye:2014:NIE


Yekhanin:2010:LDC


Yoshida:2012:OGT

Maki Yoshida, Toru Fujiwara, and Marc Fossorier.


Ye:2017:VCS


Ye:2016:IEA


Ye:2016:EHA


Yu:2010:IBF


**Yao:2019:RSA**


**Yang:2014:MDF**


**Yamada:2017:EPA**


**Youn:2018:D**


**Yang:2018:CPG**


**Yang:2016:TCP**

Yassein:2016:FSB

Yoo:2010:IRR

Yu:2011:FSI

Yu:2012:IRI

Young:2013:TPC

Yang:2018:AIW
Zhi-Fang Yang, Chih-Ting Kuo, and Te-Hsi Kuo. Authorization identification by watermarking in log-


Yang:2012:WSI


Yang:2018:NSS


You:2012:DDS


Yang:2019:NAK


Yi:2013:ETS


Yu:2016:CBE

Qihong Yu, Jiguo Li, Yichen Zhang, Wei Wu, Xinyi Huang, and Yang Xiang. Certificate-based encryption resilient to key leakage. The Journal of Systems and Soft-


Bidi Ying, Dimitrios Makrakis, and Hussein T. Mouftah. Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Appli-
REFERENCES

Yu:2010:PSI


Yu:2011:CLE


Ying:2019:LRU


Young:2015:DWE


Yavuz:2012:BFB


Yavuz:2012:ECR

Attila A. Yavuz, Peng Ning, and Michael K. Reiter. Efficient, compromise

Yu:2016:SSD


Yong:2011:SPP


Yoneyama:2012:ORA


Yang:2017:SAS


Yang:2012:EMA

Rui Yang, Zhenhua Qu, and Jiwu Huang. Exposing MP3 audio forgeries using frame offsets. ACM Transactions on Multimedia Computing, Communications, and Applications,
REFERENCES

Yin:2017:QPE

Hui Yin, Zheng Qin, Lu Ou, and Keqin Li.

Yin:2019:SCM


Yengisetty:2011:AVC


Yi:2016:IP


Yang:2012:SAK


Yumbul:2015:EEP

Kazim Yumbul and Erkay Savaş. Enhancing an embedded processor core for efficient and isolated execution of cryptographic al-

Yang:2015:EPS


Yao:2014:NCR


Yang:2018:HEP


Yang:2016:ECV


Yeh:2010:TRR

REFERENCES

Yang:2019:ISO

[YSQM19]

Ylonen:2014:SAA

[YSS14]

Yang:2011:CCK

[YT11b]

Yang:2011:CPK

[YT12]

Yamada:2012:UEW

[YT16]

Yi:2016:VSF
Ye:2018:VBA


Yeh:2017:SIB


Yang:2014:IBI


Yang:2011:ACD


Yasuda:2012:ASM


Yang:2018:IAC

Xiaokun Yang, Wujie Wen, and Ming Fan. Improving AES core performance via an advanced ASBUS protocol. *ACM Journal on Emerging Technolo-
REFERENCES


Hong-Ying Yang, Xiang-Yang Wang, Pan-Pan Niu, and Ai-Long Wang. Robust color image watermarking using geometric

Communications of the Association for Computing Machinery, 53(7):113–117, July 2010. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


Yang:2010:CRS


Wang:2018:CIW


Yang:2019:SCC

Haomiao Yang, Xiaofen Wang, Chun Yang, Xin Cong, and You Zhang. Se-
Yan:2012:SMA


Yu:2012:SME


Yang:2018:EEC


Yu:2016:CDI


Yang:2018:PBC

Ye:2018:ISS


[YY17a]

Young:2017:PSC


[YY17b]

Yu:2017:PFS


[YYK+17]

Yildiz:2017:BLF

Muhammet Yildiz, Berrin Yanikoglu, Alisher Kholmatov, Alper Kanak, Umut Uludag, and Hakan


Yong Yu, Guomin Yang, and Huaxiong Wang. Preface: Special issue cryptography and provable secu-

Yang:2012:LUC


Yang:2017:SKS


Yang:2019:HDS


Yang:2018:CDD


Yang:2012:BPN
YANG:2012:NIB


YANG:2014:PST


Zhai:2017:EEI


Zufiria:2017:GLM


Zidaric:2019:HOA


Zajac:2019:HEM

[Zaj+19] Pavol Zajac. Hybrid encryption from McEliece

**[ZC12]**

Zoni:2018:CSC


**[ZC13]**

Zhang:2011:TNT


**[ZC15]**

Zhang:2015:PCL


**[ZC12]**

Zhu:2012:JLS


**[ZC13]**

Zhang:2013:RMS


**[ZC15]**

Zhang:2012:TCS

Zhifang Zhang, Yeow Meng
REFERENCES


Zhang:2019:EPK


Zhang:2014:GCS


Zeng:2019:PKE


Zhou:2019:SAN

REFERENCES

Zhang:2018:SSH


ZDHZ18

Zhang:2012:AOP


ZDL12

Zett:2014:CZD


Zetter:2014:CZD

Zhou:2016:IBP


ZDW+16

Zhou:2018:SAE

REFERENCES


REFERENCES


Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, and Vijayakumar Bhagavatula. A pitfall in fingerprint bio-

Zhao:2010:IFU


Zhao:2016:SCI


Zhao:2015:IDM


Zhao:2010:IFU


Zhao:2016:SCI

Zhou:2015:EPP

Zhang:2016:PPV

Zuo:2019:WDH

Zimand:2010:SEC

Zhang:2011:FBP

Zeng:2014:NFC
REFERENCES

Zhou:2012:CBF

Zhang:2019:CCF

Zhou:2015:PPS

Zhao:2012:IAS

Zhao:2014:TAH

Zhao:2012:EEF
Yunmei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho
References


Zhang:2015:RBA


Zhang:2012:CCB


Zhu:2017:PSN


Zhang:2010:ESP


Zhou:2019:LIB


REFERENCES

Zaeem:2017:MAI

Zafar:2010:GRN

Zorpette:2012:BEC

Zhang:2017:PPN

Zavattoni:2015:SIA

Zheng:2016:EUV
REFERENCES


REFERENCES

October 6, 2010. CODEN ????? ISSN 1389-1286.

**Zmudzinski:2012:WEU**

**Zhao:2012:SSM**

**Zhou:2019:LIN**

**Zheng:2018:GDP**

**Zanon:2019:FKC**

**Zhang:2012:EHO**
Wentao Zhang, Bozhan Su, Wenling Wu, Dengguo Feng, and Chuankun Wu. Extending higher-order integral: An efficient uni-


[ZWM15] Mingwu Zhang, Chunzhi Wang, and Kirill Morozov. LR-FEAD: leakage-


Zhou:2017:CLR


Zhou:2017:LRC


Zhang:2017:GFD


Zheng:2010:PS


Zhan:2017:NK


Zhan:2018:EK

[ZGY18] Furui Zhan, Nianmin Yao, Zhenguo Gao, and Haitao Yu. Efficient key generation leveraging wireless channel reciprocity for MANETs. Journal of Network and Computer App-


REFERENCES


[Leyou Zhang, Jingxia Zhang, and Yi Mu. Novel leakage-resilient attribute-based encryption from

**Zeng:2019:SAE**


**Zhang:2019:LAS**