
Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/
12 October 2018
Version 1.440

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N) [Bai10, YC11], (a, t, n) [LHYZ12], (t, n) [QD16, ZPYW12]. 0 [XHX+17]. 1 [XHX+17]. 1, 2, 3 [SMDS11]. 11 [LJ17]. 13 [Blo15]. 2 [DBPS12, EAA+16, ESS12, JR13, MCDB12, PGLL10, WY12]. 22 [MNP12]. 2k [Sun16]. 3 [AP10, CG12b, DWWZ12, FWS13, GZHD12, GH11a, KWS+12, LJ17, LJ15, MKH+12, RS16, SS10b, SS12a, SGS14, WSSO12, tWmC12, YT11a, YI14, YPRI17]. 32 × 32 [SA14]. 3 × 3 [ÁMVZ12]. 4 [COP14, DWZ12, HLYS14]. $49.00$ [Sch15a]. 8 [LPO+17]. $89$ [APPVP15]. = [JJUW10]. + [PYH+18]. 2 [YNX+16]. 3 [LHM14]. MT [HRB13]. α [TTL10]. c [KRDH13]. d [QD16]. d × d [KA17]. t [ZTL15]. $F_p + \nu F_p$ [WGF16], $\gamma$ [DWZ12]. $GF(2)[x]$ [SF12]. $GF(2^n)$ [SKH15]. $GF(2^n)$ [LBOX12]. $K$ [FXP12, FR16, CHX13, ZHT16]. $L(1/4 + o(1))$ [Jou13]. $M$ [MMSD13, ÖS11]. $F_{q^{1000}}$ [AMORH13]. $F_q$ [SS13]. $NP$ [HN10]. $GF(q)$ [LPdS10]. LWE [BV14]. $\mu$ [Jia14a]. $N$ [FR16]. $n \times k (k \geq n/2)$ [MC11]. $O(d^{13})$ [KA17]. $O(n^2)$ [KS11]. $P$ [DG17]. $\pm 1$ [HZW+14]. $q$ [GMS11]. S [LJ15]. t [HJM+11, Ob11]. w [Kre13].

**Algebra** [Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14]. **Algebraic** [SK11, Tam15, Wat10, Bul10a, CFR11, jCPB+12, ESS12, GKS87, JHL12, JSZS12, JIHN12, JL16, KB10, LL11, LT14a, LLL17, MRL+18, NdMMW16, NV10, RR11, RVRSCM12, WHZ12, WZCC18, YPR17, YH16, ZSW+12, Ant14, BGJT13, BMB16, CG12b, Chm10, EEAZ13, JK13, Jou13, KY10, KHM13, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WZ12, XTK10, YWL+17, ZLW+12, ZL12, AC16, ZOC10]. **Algorithm** [ABCL17, Ano11b, AK14, BGJT14, CNR14, jCPB+12, ESS12, GKS87, JHL12, JSZS12, JIHN12, JL16, KB10, LL11, LT14a, LLL17, MRL+18, NdMMW16, NV10, RR11, RVRSCM12, WHZ12, WZCC18, YPR17, YH16, ZSW+12, Ant14, BGJT13, BMB16, CG12b, Chm10, EEAZ13, JK13, Jou13, KY10, KHM13, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WZ12, XTK10, YWL+17, ZLW+12, ZL12, AC16, ZOC10]. **Algorithmic** [GO17, AY12]. **Algorithmics** [Gas13]. **Algorithms** [AMKA17, AB10b, BCG12a, BJ10, CN12, GP17, KRDH13, MR14a, MM17, TKM12, WH18, YS15, ZW15, AGHP14, Fri10a, Mac12, NACL12, NC13, OO10, OO18, Xie12]. **Ali** [ABJ13]. **Alignment** [Don14, IA15]. **all-seeing** [Tox14]. **Allowing** [PRC12]. **Allows** [Bro17]. **Almost** [BKST18, FLL12, GDCC16, Oba11]. **Almost-Tight** [GDCC16]. **Almost-Universal** [BKST18]. **Altera** [SMOP15]. **Alternating** [BKLS12, KDH15]. **AMBTC** [KSSY12]. **America** [AB10a, Bha16, Fag17]. **American** [Sch15a, Mun17]. **Americans** [ABJ13]. **amount** [EEAZ13]. **Amplification** [ABF12, HMR14]. **Analog** [KOP12, SOS15]. **Analyses** [ZPXX17]. **Analysing** [GRL12]. **Analysis** [ABS+12, ARP12, BRS17, BBB+16a, BC14, BS14, CFE16, CCG+16, CGL+12, DKMR15, FSWF11, GZZ+13, GWM16, GLG12, HC12, HHH+13, HZW17, HB17, IBM13a, IS12, JT12a, KOP12, Kre13, LPS12, LTKP16, LCK11, LLW16, LGLL12, MD12b, MAS16, MRTV12, MR10, NDC+13, NSA15, NAL17, PHI12a, PFS12, PS14, RZZ+15, Rao10, RBS+17, SK11, SY15a, SR12a, Shi11, SZDL14, SCGW+14, VKC15, WDDW12, YZLC12, ZH15, Aia15, AC16, AN15, BNY14, CFH+13, CFL13, DMV15, DK17, DHW+13, DMT12, FTV+10, FAA+18, FHM+12, HM10, Lan11, MFH13, LLYZ12, PPA18, PL16, QGGL13, RIF+11, SKEG14, TQL+14, TLM13, Tso13, VS11, Ven14, ZZKA17]. **Analysis-Based** [RZZ+15]. **Analytic** [Kuz11, Sha10, ZW15]. **analytical** [CDPL16]. **Analytics** [BLV17]. **Analyzing** [HREJ14, YGD+17]. **Ancient** [Fox13, Rao10]. **and/or** [YLA+13]. **Android** [Chi13b, EBFR13, SFE10]. **Android-Powered** [SFE10]. **Angle** [ZPW16]. **Angle-Based** [ZPW16]. **Angular** [pNyWyY+14]. **Anisotropic** [ZZCJ14]. **Annotated** [ATS15]. **Announcing** [SBK+17]. **Annual** [Ano10, IEE10, IEE11b, PJ12, Gil10, Rab10]. **Anonymity** [CDFS10, HEC+12, MV16b, MR10, SCGW+14, VFV17, WLY17, AIB+16, BAG12, GH16, HLR11, Par12b, PSJ+13, SGJ+18, WW14, YHL16, ZX11]. **Anonymity-Based** [HEC+12]. **anonymity-preserving** [AIB+16]. **anonymization** [XTK10]. **anonymized** [BDK11, TG12]. **anonymizing** [TMK11]. **Anonymous** [CG12a, CZLC12a, CCF17, Chi12, DK12, FHH10b, FH11W8, HLT+15, KP18, LK+17, LZCK14, Muf16, Per13, RSN14, TAKS10, Wan14, WXL+17, WYML16, ZJ14, ZMW16, AIK18, ATK11, BT18, CC118, Chi1a, CG111, FSGW12, HL14, ISC+16, LNK+18b, LHM14, LYL15, LY14, MYY13, QC17, VS11, YZL+18]. **ANSI** [Ano11b]. **answers** [Wu16]. **anti** [QZ14]. **anti-forensics** [QZ14]. **Antinoise** [WXL+17]. **Antispoofing** [MR14b]. **Antoine** [AY12]. **any** [Goo12, LP11]. **Apache** [Lit14]. **API** [FIL12]. **Append** [YR12b].
Application [AKP12, AK14, BRT12, BS12, CKB13, CCKM16, CCW+10, CSTR16, CLCZ10, CHS15, Küp15, LW11a, LWK12, MNS11, OO12, SEHK12, SS13, XJW+16, YWK10b, YTS12, ZH15, ZM16, Abe10, BBBBB13, BT18, CZ15b, GLIC10, HH15, Jia14b, LGKY10, LWK14, MSM+18b, NAL17, OTO18, SE18, SGFCRM+18, XHH12, YY11, ZWQ+11, ZÁC17].

Application-Level [CCW+10].

Applications [AMVZ12, Ana14, BKPW12, Ber18, BKS18, BCG+12b, BJCHA17, BS12, CZL12a, CZL12b, CPS16, DK15, FSK10, GKM16, GRL12, Hvs12, HN10, JWJ+17, Nac12, NV10, PJ12, RBS+17, RQD+15, SCPSN10a, SCPSN10b, Sha10, Ter11, TYK+12, WH17, YR11, Ano11a, CFR11, CSZ+11, CQX18, CDA14, Dur15, EBFK13, FES10, Fri10a, Gil10, KO16, LWZG10, LR15, LBOX12, LTT10, MS13c, MM14b, OK18, PHVM10, PK15, SWW+17, ZZ15, ZMS18].

Applied [BSS11, KP10, MR10, Xie12].

Applying [Bar12].

Approach [CTC+15, Ch16, HL15, HLW12, KKA15, MKN13, MZ17b, PS14, RP12, SLGZ12, Sha12, SH15, SC12, TNC+17, TLW12, Vle12, VCK15, WYCF14, yWXyZ+18, ZW15, AL15, AT10, BSS11, CLZ+17, CO11, CML16, DZS+12, FMB+18, GGH+16b, KL13, LGFCGCP14, MCP15, NC13, PJ18, SE16, WMYR16].

Approaches [GWM16, LC15, SB14, MKH+12, OK18].

Appropriate [SP15b].

Approximate [CN12, JSC17, SG14].

AppSécur [RQD+15].

April [GLIC10, IEE13, PJ12, vDKS11].

Arab [Bro11].

Arbitrable [CCKM16].

Arbitrary [FHR14, DWZ12, Gen10].

Arbitrary-State [FHR14].

Arbitration [Küp15].

Arbitrator [WSA15].

architect [GW14].

Architectural [MD12b, VCK+12, ZWT13].

Architecture [BCE+10, HKL+14, KS18, KCR11, KCC17, KAK18, LGR14, MCB12, MJGS12, MC11, NdMMW16, NVM+17, RMP10, SWM+10, SL11, VDB+16, AL15, Ano13d, VB1B12, LXMW12, MJS13, SS11, SSPL+13, SAAB10].

architecture-independent [BVIB12].

Architectures [AMK17, BGG+13, BJCHA17, CMO+16, CHS15, DFKC17, MKAA17, FPBC14, HL14, MK11, Nov10].

Area [GMVV17, HC17, LZCK14, WH17, KP18, LMJ11, LK+17, Nov10, SGJ+18].

Area-Time [HC17].

Areas [MV12, JY14].

Arguments [BCI+13, AMB+12].

ARIA [PH12a].

Arithmetic [AIK14, AAB17, Fre10, GH11a, HSA14, IEE13, KHF10, PG12, DTZ12, MO14].

Array [BL12, MCD12, NKW14].

Arrays [LB13, TRD11, KM10a].

Art [ABJ13, BLM17, LLK18, Sen17, BDK11].

ARX [KN10].

Asa [Bai12].

ASIACRYPT [WL11a, Abe10].

ASIC [CFZ+10, KMY18, MKAA17].

Asking [DL15].

ASM [Vle12].

ASM-Based [Vle12].

ASP.NET [DR11].

Assessing [CBL13].

assets [WHJ17].

Assignment [LMS16].

Assisted [KCC17, HZW18].

Associated [Sar10b].

associative [BS15].

Associativity [ABR12].

Assumption [LZC12a, LZX14, ZG10].

Assumptions [BDH11, CZF12, DN12, GKS17, KM10c, PDH15, ABW10].

Assurance [BMBS10, Bar15, KMP+11, RBNB15, WL11, Ser12].

Assured [Tan15a, WMYR16].

Asymmetric [HG12, XLM+12, XGLM14, XZLW15, ZWQ+11, CSS+13].

asymmetric-histogram [CSS+13].

asymptotic [DTZ12, TD14].

Asymptotically [LPS12].

Attack [Ano15d, BRS17, BMS12, Bro17, CJP12, DSB15, FXP+17, zGXW12, GV14b, GDCC16, HCETPL+12, HL1Z15, JHL12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LWK12, LWP12, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNS17, CJP15, DD1R13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYHH14, ...]
Atttacker [BL15]. Attacks

ARP12, Aso17e, BGK12, BFK16, BKBK14, Che15, CMA14, DGIS12, DHLAW10, DHB16, EWS14, GPT14, Hay13, HRS16, JSK+16, JWJ+17, KNR10, LLC11, LWZ12, LWCJ14, LCL17b, MD12b, PYN+13, PS12, Sas12, SEY14, SY15a, SH15, SVG16, SGH15, WW14, WHN+12, XNG+14, YL17, YCM+13, ZLQ15, AATM18, BBBP13, BVIB12, BSR+14, CGH17, dCCSM+12, DCAT12, DJL+12, DK17, Dra16, EA12, FTV+10, FIO15, GPP+16, GBNM11, KM10a, KPS10, LWK11, NDNR13, OF11, PX13, TS16a, TY16b, TLL13, VS11, WWBC14, XWDN12.

attack [Fel13]. attestation [FQZF18]. ATtiny [EGG+12]. 

Attributes [CG12a, Yon11, LCL+17a]. Attribution [XHC+12, FNP+15]. Auction [Con10, HJM+11]. auctions [MR14c, QS18]. Audience [DTE17]. Audio [Ber18, DA12, FM15, GCK12, HGT15, KD12a, KD12b, LSL12b, NXH+17, TC10, gWpNyY+14, XNG+14, XNRG15, ZS12, LSQ11a, SKEG14, yWpNyL11, YQH12].

Audit [YNR12b]. Auditing [LMD16, TCM+17, YYS+16, YXA+16]. August [AB10a, JY14, MV12, Rab10].

Authentication [ALo12, BCO13, BDML16, CCL16, CLY14, CCS14, CRE+12, DS11, EAA12, ESS12, FVS17, FFL12, GTP11, GL12, GZ12, HC12, HL10a, HCL+14, HEC+12, KMY18, LHK10, LY16, LH11b, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHKS14, MSU13, PTT16, Sar10b, Smi11b, Tan11, TW14, XLM+12, XHL14, XZLW15, YS12, YL13, YRT+16, You12, ZPZ+16, ZMH16, AIB+16, CTL13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HL11, HPY10, ISC+16, LWS10, LH11, LML+13, NCL13, Nos11, Nos14, PPTT15, PJ18, SMBA10, TCS14, Tso13, TKHK14, WZM12a, WZM12b, WZM12c, XWXC14, XCL13, XZM18, YC12, YZZ+14, YZL+18, ZT16, ZXWA18, ZG10, ZZC15]. Authenticating [BS12, CHX13, GRL12, OKG+12, RPG12, WY12, ZCS15, LFCCGCP14, PGLL10].
HCPLSB12, HCETPL+12, HKL+12, HXC+11, HLC11, IGR+16, JN12, JCM12, Jia17, JAE10, KPI12, KS18, KRM+10, KSD+17, KPC+11, KLY+12, KTA12, KGP12, Kim15, KPKS12, KLM+12, KO16, KH10, LLC11, LH12, LLG15, LCLL15, LNZ+13, LZCK14, LNX15, LLZ+12, MWZ12, MEF012, MKH+12, MBC15, MRT17, MRS+17, May15, MLBL12, Mor12, MSKRJ17, MPM+17, NR11, NR12, NLLJ12, NLY15, OdH12, OLS12, PCGD14, PPRT12, PDT12, PWVT12.

Authentication [RS11, RWLL14, RSN14, Saa12a, SBS+12, Sar12, SGC14, SSA13, SC12, SD12, Shi11, SGC16, Sch15b, SKV12, ST14, SM12, SD12, Shi11, SGC14, SSA13, SC12, SZDL14, SHS12, SAA12b, SRK+17, TGC16, TYK+12, TM12, Vet10, WgMdZlZ12, WHZ12, WZXL12, WgMW12, WC12, WSS12, WT10b, Xio12, YTP11, YFT17, ZBR11, ZHW+16, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, Aia15, AL15, AHM+18, APK+18, Alp18, AIKC18, ACIF16, AZF+12, ATI+10, AN15, ACM12, BS13a, BDM18, BCM13, BGAD12, BLAN+16, BAL10, BMM12, BVrOS15, BT18, BM11, CLM+12, CML+18, CLP+13b, CTL12, CSD18, CH10, CCW11, CHS11, CLHJ13, CZ15a, Chi13a, CJP15, Cho14, CL11, DCAT12, DSCS12, DLK+16, DMV15, DLN13, DZS+12, DMT12, uHAN+18, EA12, ED19, EA11, FBP14, FH110a, FLL+14, FXP12, Far14, FA14a, FHZW18, FQZ18, FMA+18, GJ13, GMSW14, GH16, GAI+18, GCSAddP11].

authentication [GLB+18, HU15, HSH11, Ham12, HDPC13, HZC+14, HZWW17, HLL14, HCM11, HLC16, HCC10, HS11, IMB17, IC17, IG11, IB11, IOV+18, Jac16, JNU17, Jia16, JKL+16, JW+16, JAS+11, JXLZ15, KPP16, Kem11, KKG14, KSB+17, KV+18, Kim11, Kim16, KPI18, KBP17, KLW+16, KDX+17, LLLS13, LLZ+16, LC17, LH11a, LT13, LH10c, LNM+11, LMJC11, LMX12, LNK13, LXJ14, LIK+17, LCM+17, LNK+18a, LWK+18, LNk+18b, LHM14, LH13, Lit14, LWLW11, LTC+15a, LY15, LBR12, LTT10, MM12, MCN+18, MoV11, MA17, MMS17c, MK12a, NR17, NACL12, NCCG13, NLY12, NB13, OF11, OCG11, OYHSB14, PYH+18, PYP10, Par12b, PLGMCD18, PZBF18, PA10, PKA15, QMC17, QMW17, SPLLHB14, SB17, SGCG+16, Sar10a, SGJ+18, hSZZ15, SCKH10, SA15, SYW17, SSS11, SKEG14, Tan12b, Tan15b, TODQ18, TG17, TLL12, Wan13, WW14, WL+16, WCFW18, Wat14a, Wat15, WT10a, WKK11].

authentication [GLB+18, HU15, HSH11, Ham12, HDPC13, HZC+14, HZWW17, HLL14, HCM11, HLC16, HCC10, HS11, IMB17, IC17, IG11, IB11, IOV+18, Jac16, JNU17, Jia16, JKL+16, JW+16, JAS+11, JXLZ15, KPP16, Kem11, KKG14, KSB+17, KV+18, Kim11, Kim16, KPI18, KBP17, KLW+16, KDX+17, LLLS13, LLZ+16, LC17, LH11a, LT13, LH10c, LNM+11, LMJC11, LMX12, LNK13, LXJ14, LIK+17, LCM+17, LNK+18a, LWK+18, LNk+18b, LHM14, LH13, Lit14, LWLW11, LTC+15a, LY15, LBR12, LTT10, MM12, MCN+18, MoV11, MA17, MMS17c, MK12a, NR17, NACL12, NCCG13, NLY12, NB13, OF11, OCG11, OYHSB14, PYH+18, PYP10, Par12b, PLGMCD18, PZBF18, PA10, PKA15, QMC17, QMW17, SPLLHB14, SB17, SGCG+16, Sar10a, SGJ+18, hSZZ15, SCKH10, SA15, SYW17, SSS11, SKEG14, Tan12b, Tan15b, TODQ18, TG17, TLL12, Wan13, WW14, WL+16, WCFW18, Wat14a, Wat15, WT10a, WKK11].
Awareness [MSas12, Li10, MSas13].

axiomatic [AT10].

B [Tan12a]. B-Spline [Tan12a]. Back [KRM+10, SKS+18, YZLC12, Ran10].

Backdoor [Sch13, Fel13]. Backside [DDR+16]. backup [Cor14a]. backward [BM11].

Bacterial [Kar12]. bad [Hai17, RY10]. BAF [YNR12a]. Bake [Boy16].


balls [Svo14]. band [MMSD13]. Bandwidth [GST13, NR11, LLZ+12].

Bandwidth-Efficient [LLZ+12]. Banking [KSD+17, RBS+17, KVvE18]. banned [Eve16].

Baptiste [Dew11]. Barbara [Rab10]. Barcodes [DY12]. Barrier [JR14, KS11]. barriers [LKKL13]. base [MS12a, XSWC10]. Based [ADM12, AGW15, ASM12, AAC+16, ABCL17, Ano11b, ASS15, BWL16, BL12, BSS16, BJP12, BKP12, BRT12, BHH+15, BS13b, BFK+10, Bon12, BSJ15, Boy13, BKL11, BCF+14, CML15, CSM+14, CCM17, CSH+18, CZLC12a, CZLC12b, CLHC12, CZZC13, CLY14, CZLC14, CST+17, CGL+12, CDD12, CGY+13, CD12, Chi12, CD16, DSMN14, DA12, DLZ+16b, EM12, EKB+16, FM15, FHH10b, FHR14, FZT14, FGM10, FVS17, FSX12b, FSX12c, FSX12a, GWW15, GZZ+13, GSW+16, GV14b, GI12, GY13, GDCC16, GVW15, GJJ15, GJ17, HZC+12, HSM12, HSM14, HL10a, HX12, HCPLSB12, HKL+12, HG12, HMR12, HSA14, HPO+15, HKR+18, HGT15, HLC+14, HLN+10, Hui13, HRS16, HBG+17, HEC+12, HP12, JTHZ+16, JHNN12, JEA+15, JKeYeY12, KS18, KZG10, KK12, KKA15, Kha10, KLY+12, KSSY12, KPKS12, KRB12, KAK18, KS15, LMGC17, LMG+18]. Based [LTKP16, LSL12a, LSL12b, LW11b, LW11c].
[ADI11, AK14, MBR15, MBF18, SA14].

Binary-Ternary [ADI11]. Binding
[HEC+12, ZLQ15]. Bio
[OK18, GPVCdBRO12]. Bio-inspired
[OK18, GPVCdBRO12]. BioAura
[MSKRJ17]. biographical [Maf16].

Biometric
[Alp18, ATI+10, BCTPL16, DWB12, JN12, KHMb13, LGM+16, May15, NGAuHQ16, Sar12, SKV12, Vet10, AHM+18, DIMT12, GCSдждп11, HT11, LK12, LТС+15аa, MLBL12, Sar10a, Sar18a, SR10].

biometric-based [SR10]. Biometrics
[BW13, ERLM16, SP13, ZPW16, FHZW18, GM16, LXLY12, LH10c, LNM+11, LNK+18a, MRRT17, SS17].

biosensor [Kim16]. biotic
[Sha10]. Birthday
[LST12, SXL16, Nac12]. Birthday-Bound
[LST12]. Bit
[CG14a, GV14b, HG12, LJK17, LPO+17, NIS12, Ros11, YLL+12, APPVP15, KS11, KFL+10, MNN12, PLsvdLE10, RH10, TWZ+12, VN17].

Bit-Wise [CG14a]. Bitcoin
[ADMM16, BRS17, BH15, Bra15, Chi13b, HB14, Hur16, JSK+17, Mic16, Sir16, Tay17, TS16b, VFV17, WLY17, WHJ17].

Biometrics [MPJ+16]. BitErrant [Ano17a].

Bits
[BF12, LLL17, YCL17]. Bitstream
[SMOP15]. Bivariate
[TWZ11]. Bivium
[EVP10]. BIX [Maf16]. BLAC [TAKS10].

Black
[BR14, CPS16, HHP17, KOS16, KMO14, MSas13, JB11, Rja12, SS10b, DD13, SK14, YSC16, ZZ12, Cri16].

Black-Box
[BR14, HHP17, KMO14, Rja12, SS10b, KOS16, MSas13, ZZ12]. Blackbox
[MSas12, SS12a]. BLAKE
[AMPH14, GV14b]. BLAKE-512-Based
[GV14b]. Blanchette
[SR14]. Blended
[ACAT+15]. Bletchley
[Bai12, Ano11c, Bri11, Cop10a, Cop10b, GW14, McKI10, MCK11, MCK12, Pea11, Sm11a, Sm15b, Sm15a]. Blind
[AP10, Ano15a, BCPv11, LCLW17, LGPH14, MR16, MNN12, RS16, YMWs11, HKB14, MO14, RSM15, WLB11, yWpWypN13].

Blindfold [Nac16]. Blindfolded [Vai11].

Blindness [CLHC12, KHH14]. Block
[AMVZ12, BRS17, BSS+13, BFMT16, BDGH15, BCG+12b, CWP12, DWWZ12, EGG+12, FXP+17, GLLSN12, GT12, GST12, GNL12, IS12, KR11, KWS+12, LWZ12, LJJ17, LCLW17, LGLL12, LWKP12, LWPF12, MCD12, MRTV12, OGK+15, PH12a, PRC12, Pud12, SGP+12, SSA13, WW12, YCL17, ZSW+12, BNY14, Jeo13, KM11, LPZJ15, LC13, LYHH14, LWKP14, MN12, MIV15, MHY+18, PL16, Sar11, SKK10, TQL+14, Tan17a, WB12, WWBC14, ZSW+18a, JKP12]. Block-Parallel
[MCDB12]. Block-Wise [SSA13].

Blockchain [Hur16]. blockcipher
[CMMS17]. Blockciphers [LST12]. Blocks
[JSK+17, Bra15]. Bloom [ATKH+17].

Blowfish
[KB10]. BlueKrypt
[Gir15]. Boardroom
[LHF12]. Bodacious
[KM10c].

Body
[LZCK14, ASO14, KP18, LIK+17, SGJ+18]. body-sensor [ASO14].

bogus [XWDN12]. Bombe
[Bur11, Car10]. Bonebreak
[SS10c]. Book
[Ano15b, Ano17b, Ayu12, Bar12, Dew11, Full0, Joh10, Keh15, Kob10, Low12, Me10, Murr10, Sch15a, Sha10, SR14, Ter11, Sto12].

Boolean
[ACZ16, AS17, CW14a, DQFL12, FY11, LV11, WT13, YCC16].

Boolean-based
[CW14a, YCC16]. Bootstrapping
[BGV14, GM14]. Border
[LG+16, ZTSR12]. BotMosaic
[HB13].

Botnet [NSA15]. botnets [HB13]. Bottom
[Smi11b]. Bound [LST12]. Bounded
[GWV12, GJO+13, PDNH15, QZZ18, SS12a, ZYT13, IM14]. bounding [PYH+18].

Bound
[Jia17, LJ15, SNJ11, SS10b, Sha10].

Bouzefrane [Ano15b]. Box
[BW16, BCGN16, BR14, CPS16, HHP17, KMO14, Mic10b, Rja12, SS10b, KOS16,
CGCS12, DM18, DG12, DWWZ12, Fis15, FXP+17, GLLSN12, GCS+13, HZ11, Hey17, IOM12, JKPK12, KR11, KWS+12, LPS12, LWZ12, LJ17, LWPF12, LWP12, MRTV12, MHC12, MS12h, OGK+15, PH12a, PRC12, WSSO12, WHN+12, YCL17, AMS+10, BNY14, CR12, HKT11, Hol12, Jie13, KHD15, Lew10, LC13, LYHH14, LWK14, MNP12, PL16, Ree15, RS14, Sar11, WYL14, WWBC14, ZSW+18a, LGL+12. Ciphers [ABS+12, BMS12, BSS+13, BKLS12, Bru12, CW12, DG12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNL12, Hey17, IS12, KPC+16, Kla10, LCLW17, LGLL12, LJ16, MD12b, NN12, Pud12, Sas12, SEHK12, Vua10, WH18, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KM10a, LWK11, MRT10, MHV15, MHY+18, QGGL13, SK10, TQL+14, WB12]. Ciphertext [BD12, CW12, zGXW12, HLV12, JMG+16, JSMG18, KA17, LZC12a, LML12, MH14, PDNI15, PPS+12b, Rao17, RW12, RS10, SSW12, VS12, WWHL12, XMCL13, XW1L16, ZWH15, CPT18, FS1G1W12, GLM+16, GH12, HPY10, HKK13, KTT12, LCT+14, LFWS15, LZZ14, QRR+18, RD17, SGM16, WLFX17, XWS17, LAL+15, HLH15]. Ciphertext-only [KA17]. Ciphertext-Policy [Rao17, XMCL13, XW1L16, ZWH15, JSMG18, LFWS15, QRRW+18, XWS17, SGM16, LAL+15, HLH15]. Ciphertexts [Sta12, WQZ+16, AHI+12, LCT+14, NMP+13, WXLY16]. Circle [SC10]. Circuit [Kar12, MTY11, XWS17, XW1L16, Lai12, MS13a]. Circuit-Size [MTY11]. Circuits [AIK14, AS17, BR14, GGH+16a, GHH1a, GV15, MB18, SS10b, SS12a]. Circumventing [BAG12]. Ciphertext [BAG12]. CIISSP [STC11]. Citizen [Ano16d]. City [Ano17d, GAI+18, LNX+18a]. Claims [SKG14]. Class [BCG12a, SY15a, XYXYX11, BJ16, Go12, KK10]. Classes [ÁCZ16]. Classical [DSL18, JEA+15, MSU13, SSU12, CR12, RK11]. Classification [HPC10, KAHKB17, SGP+12, ZLW+17, LHL+18]. Classifiers [KGV16, LCM+17]. classroom [Pow14]. Claudius [Hol12]. CLEFIA [LWZ12, TSL11, TS16a, WB12]. CLEFIA-128 [TSL11]. CLEFIA-type [WB12]. Client [AS12, CTC+15, FD11, RAZS15, Vle12, FA14a, FA14b, hSZ15, WT10a]. Client-Based [AS12]. Client-Centric [Vle12], client-server [FA14b, hSZ15]. Clients [Chi16, LH13]. cloaking [NZL+15]. Close [Wal18]. Cloud [AJA16, BCQ+13, BCK17, CWL+14, CW16, CDF16, CCT+14, CLW16, DXA14, FC14M, FPY15, JLS12, KMSM15, KS18, KKA15, Kip15, LA15, LYZ+13, LGR14, LLC+15, LXY15, MLO17, PSM17, Pet12, RSG15, SGJ+18, SKH17, SRA17, TV15, Vle12, WLFX17, WWW17, XNK15, XWS16, XMCL13, XW1L16, XW1Y+16, YDY+16, YHL16, YXA+16, YMC+17, ZDL12, ZLDC15, ZVG16, ZLW+17, AABT16, AZPC14, AS14, AAZ+16, AKK+17, ADH17, ALL+18, BGI4, BK12b, CFVP16, CSD18, CLH+16, CZ15b, CDL18, FH13, FNW18, GLB+18, GZS+18, HSM13, HZ1W18, HYS18, IMB17, Jeol13, KA14, KK1+13, KKM+14, KSB+17, LXP+14, LZY+16, LAL+15, LW13a, LYL15, LHL15, LCY+16, LC17, ML16, NR17, NB13, PPA18, P11a, Re107, SYY+17, SAR18b, SL10, SKB+17, SWW+16, WW+17, TLLM13, WL12, WMX+17, WCCH18, XX15, XY+18, YYS+16, YZCT17, YHH18, YWT+12, ZYC+17, ZDW+16, ZWS+18, ZF1+18, ZH16]. Cloud-aided [SGJ+18, WFLX17]. Cloud-Based [KS18, SRA17, AS14, BK12b, WC18]. Cloud-Manager-Based [KA15]. Cloud-of-Clouds [BCQ+13]. Cloudier [CFE16]. Clouds

code-breaking [Ant14, Bri11].

code-cracking [War11]. codebreaker [Car11].

codebreakers [Ano11c, Bud16, Maf16, McK12, Smi11a].

Collision-based [ZL12]. Collision-Resistant [BK12a]. Collusion [MMSD13, RVH +16, FLZ +12, GMRT +15].
collision-resistant [GMRT +15]. Collusions [GVW12]. Color [BCPV11, DD13, FR16, LW10, MR16, yWXyZ +18, YWNW15, MSM +18b, SNM14, yWpWypN13, WGZ +12, YSC16].

Colossal [Hai17]. Colossus [Cop10a, Cop10b, Will8]. Coloured [OHJ10].

Collaboration [CRE +12, PCPK14, HYS18]. Collaboration-Preserving [CRE +12].
collaborative [LT14b, HB13]. collect [Sch15c].

Compact [CFOR12, CKLM13, EGG +12, MAS16, VSR12, ZMW16]. compacting [CPPT18].

Commentary [LCLL15]. Comments [IC17, Kim15, hSZZ15, Tan11, TCL15, XWS17].


Comparative [DDR +16, MHV15, NR11]. Comparison [CGCS12, DWB12, HPC10, KU12, ST14, HM10, LCM +17]. comparisons [Mid10].
Confidential [HS11, AZPC14].
Confidentiality [BFK+10, HLLC11, OFMR16, SZQ+17, WDDW12, Bia12, CHX13, ZHT16].
Confidentiality-Preserving [OFMR16, SZQ+17]. Configurable [CVG+13]. Configuration [Bis17].
conscious [Ree15]. Consecutive [Tan12a]. Consensus [ABCL17, JSK+17].
Consequences [Ess17]. Consideration [CJP12, CJP15, KM10b]. Considerations [KD12b]. considering [MLMSMG12].
Consistency [BCK17, SES+16]. Consolidated [KKA14]. Constant-Round [KOTY17, KMO14, LP11].
Constant-Size [AEHS15, AHL+12, LCT+14, SG16]. constants [DWZ12]. Constrained [BS15, CSH+18, EAA12, JMG+16, YNR12a, Yon12, DMV15, KAS15, LZX+16, LCL+17a].
Construction [BWLA16, DF11, EM12, FZ14, GWWC15, HH17, KMO14, MSA12, Rog16, Sar10b, St14, WZ15, WCL+18, WMS+12, XHX+17, LFZ+17, MSA13, SA14, YWL+17, YT11b, YKC+12, ZCL14]. Constructions [BCF+14, DQFL12, HL10b, KOTY17, SNJ11, SES+16, CZ15a, CGKO11, NAL17, Zim10].
Constructive [Mau12, WB12]. constructs [BP10]. Containing [XWDN12]. contemporaries [LCKBJ12].
Continual [BKKV10, ZXY+12, YZ12, YCZY12].
Continual-Leakage [YZ12]. Continually [DLWW11]. Continuous [ACAT+15, BCF16, DHLAW10, uHAN+18, FMNV14, MSKR17, PYP10, Sch15b, Yam12, ZY17a, ZYM18, PLGMCD18].
Continuous-Tone [Yam12]. contract [Men13]. contrast [DDD14, GLW13, LXL10a, MM14a].
Contributory [WQZ+16]. Control [ATS15, BFK+10, DLZ+16b, HHS+15, LGM+16, MM17, MK12b, NA10b, QZL+16a, RSN14, SGC14, TBCB15, XMLC13, YTH17, ACK+10, AMH10, CLH+16, CO11, Cra11, FNWL18, FS18, JAS+11, LCL+17a, LCL+15, NZM10, QCX18, Sch15c, SA15, Tan12b, Wan18, XHH12, ZML17, ZWS+18, ZFH+18].
Controllable [FH13, ZLDC15, ZHT16].
Controlled [FMTR12, WP17, Har16].
Conversations [WBC+10]. Converse [KPKS12]. Conversion [BJ10].
Convertible [C1L16, LSH11, HL11, LHH11, XWXC14].
Convolution [DWZ18]. convolutional [MG15]. cookies [DCAT12]. Cooperative [LLZ+12, SJWH+17, ZLDC15, WQZ+13].
Coppersmith [Dra16]. coprocessor [ABC+12, BGG+13, IBM13b]. coprocessors [GCVR17]. Copy [YT12, MHT+13].
CorrectDB [BS13a]. correcting
[ATI+10, LTT10, MCP15]. Correction
[LSC+15, yWXyZ+18, Chi13a, Sun16].
Correctness [YGS+17, WS13]. Correlated
[RS10, Jia16, ZPZ+16]. Correlation
[BW12, FAy+18, LD13, SDM+12.
WWBC14, XHH12, YCL17]. correlations
[Sar14]. Correspondence [SY14].
corresponding [DWZ12]. Corrigendum
[HYS18, WZM12a]. cosmography [Pet11].
Cost [ABC+17, AMH+16, CMLS15, CJP12,
GI12, HLT+15, Man13, NVM+17, WMX+17,
CZ14, CJIP15, LEW19, Sar10a, YL11].
Cost-Effective [HLT+15, WMX+17].
Cost-Eective [HLT+15, WMX+17].
Costas [TRD11]. Costs [KHPP16].
couldn’t [Bha16]. Countdown [Zet14].
Counter [ARP12, Fay16].
Counterexample [KPW13]. Counterfeit
[YFT17]. Counterfeiting [Ano16c].
counterfeits [GSN+16]. Countermeasure
[BGN17, EWS14, PZPS15, DK17, FAA+18].
counting [LLY+12a]. Counting [LLY+12a].
cover [UUN13]. Covert [EPAG16, JTW+16,
NAA15, LT13, LyWZ10, SRB+12].
CoverBand [NTK17]. Cozzens
[Led16, Sch15a]. CP [TY16a, YMC+17].
CP-ABE [YMC+17]. CPM [PYM+13].
CPs [FQZ18]. Crack [Fox13]. cracked
[Ano13b, McG11, McK12, Moo14].
Cracking [Gri15, GAS+16, War11].
crawlers [GNP+12]. CRC
[Ful10, Joh10, GMSW14]. CRC/Taylor
[Joh10]. Create [DFKC17]. creating
[OO10]. Creativity [WP15]. credential
[JMW+16, KKM+13, XMHD13].
Credentials [CG12a, SSW12]. Credible
Crisis [Odh12]. Criteria [PS18, ZK17].
Criteria-Based [PS18]. crittografia
[Sac14]. CRM [LHM+15]. Cropping
[SR12a]. Cross [AKK+17, CLY14, DS15,
LHM+15, MV16a, YGL15, YZL+18,
ZHX16, ZTSR12, SS17, der10].
Cross-Border [ZTSR12]. Cross-Domain
[CLY14, YZL+18]. Cross-group [AKK+17].
Cross-Layer [LHM+15, ZHX16].
cross-matching [SS17]. Cross-Site
[DSB15]. Crossword [Mar10a]. Cryptis
[GSC17]. Cryptanalysis
[BW12, Bor10, CWP12, GC12, DG12,
DJG+15, Far14, GST13, Gor10, Hin10,
IOM12, Jie13, Kha10, KN10, KWS+12,
LH16b, LNM+11, LJF16, LJ16, MWZ12,
NXB13, OTD10, PSOMPL13, SPLHC14,
SM10, SM10b, TY16a, TG17, Vua10, Wag10,
WWYZ11, WWY11, WSS12, WWY14,
XQL11, YCL17, YMWS11, AP11, BMB16,
BKR11, Bul10a, Bul10b, Con12, Eisi10,
Her10, KDH13, LLLK10, LFW+16, Nov10,
RITF+11, SDM10, SDM14, Sun11, SvT10,
Tani15, TSL11, WY11, WWBC14, AY12].
Crypalyzing [LLL17, ZLW+12].
CryptDB [PRZB12]. Cryptic [Mar10a].
Crypto [Goo12, Pf10, Rab10, SCPSN10a,
SCPSN10b, WL11, BSR+14, BCG+13].
Cryptoclub [Ay12]. Cryptocurrencies
[JSK+17]. Cryptocurrency [BH15].
cryptograms [Shy15]. Cryptographer
[Dun12b, Kya11, Pie10]. Cryptographers
[Ano16d, BPS16, Goo12]. Cryptographic
[Abe12, AMKA17, AD12, ARH+18,
AMVZ12, App15, BMP12, BCGK12,
BGB12, Bar15, BCM+15, BKK14, BLS12,
BPD11, FBCZ12, BDGH15, Bia12, BKL+13,
BSJ15, BNA15, CCK12, CCCC16, CFE16,
jCPB+12, CBL13, Cor14b, Des10a, DQFL12,
DR11, Ess17, FKS+13, FY11, FLW12, Gir15,
GM11, GLR10, GIG1, Hfa16, HN10,
HHH+13, HST14, HSA14, IBM13b, JR13,
KOP12, LVV11, LK18, Lo05, M1V12,
MP12, MKAA17, Mfu16, MJ12b, NIS13,
NA10b, PTT16, PFS12, P14, PJ12, RPM10,
RSBGN12, Rja12, RBHP15, SK11, SEY14,
SFK15, Sch12c, Sev16, SGY11, SP15b,
SDM+12, SR14, SOF12, TW12, Tom16,
YZ1C12, YNR12a, YNR12b, YS15, ABP15,
AY14a, ABB+14, ABF+14, ABC+12,
BFG+14, CFL13, Cha13a, CFZ+10, CR10,
CP13, CLCZ10, Cra11, DGJN14, EBFK13, ESRN14, GGH+16b, Gil10, GLR13].

cryptographic [KSU13, KAS15, KKK+16, LGKY10, MS13c, MMZ12, MM13, Mes15, MN10, NDNR13, O018, Pal15, PLPW13, Psdo+13, QZDJ16, SD10, WT13, WMX+17, YSM14, Zim10, Sha10].

cryptographic-Key [SK11].

cryptographical [KU12].

cryptographically [ADD10, BCGH11, BJL12, MC11, NDG+17, PLSvdLE10, SVCV15, GCH15, HJM+11, SA14].

cryptography [ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, App14, AAB17, ACM+17, ARM15, Bar12, BGK12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BLM17, BCF+14, CNR14, CT18, CJFH14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DP17, DLAW10, DF16, DKS12, DR11, Eis10, FPS12, Fe10, FSK10, FBM12, Fre10, GO17, GFBF12, G+13, GPT12, GLW12, Han17, Hes12, HG12, HKR+18, JT12a, KM10c, KPI10, KAK18, LSL12a, Lin17, LWL10b, LGWY12, LMHH14, LGH+17, LWHS17, LPO+17, MO12, MSI10, Mau12, MR14c, Mic10b, MV12, MMB17, NNA10, N812, Orm16, PP10a, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16, Sen10, SS13, Sen17, SK12b, SA16a, Sim15a, SGS14, Smal6, Sta11a, Ste15a, VS16].

cryptography [WWL+14, YY12, Wes16, Yam12, Yan11, YTS12, Y17, ZZZC14, ZAC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AAA14, ABBD13, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BAB+13, Bi512, BR+14, BS12, BB16b, CBR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSL14, DDD14, Dav11, DD13, Dur15, Far14, GCVR17, Har15, HH15, HZWW17, Hof16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Lüüd12, LY14, MCN+18, MS13b, MD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSAF11, Sta11b, Sti11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA+18, YDH+15, YR11, ZWX+18, vDKS11, Che11, LZJX10, Nac12, Cou12, Ful10, Gas13, Low12].

cryptography [Mei10, Mur10, Ter11].

cryptography-based [BOB13].

cryptography-Related [Cil11].

Cryptol [Lau12].

cryptological [BC11, Bro11, Dun12b, LG11a, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FP14, Gil10, GG10, K11a, LH10a, MZ17a, Pal16, Pie10, Rab10, HWG10, LT11, Kob10].

Cryptomania [Gen13].

cryptoprocessor [GV14b, Sw+10].

cryptosystem [CCT+14, LHIb, Sw+10, BS15, Ch13a, Gal13, GV14a, GL8+18, IB11, MM13, MG15, NZ10, Svt10, yQyW13, YY11].

cryptosystems [AD11, O11, PSM17, BNST17, FWS13, SA16b].

csec [AD12].

CT [Dun12b, K11a, Pie10].

CT-RSA [Dun12b, K11a, Pie10].

cube [MS12b].

cubic [RW12, VM14].

cuckoo [BHKN13].

CUDA [DL16].

cultural [Mid10].

culture [Bla12, SR14].

currencies [TS16s].

current [DP17, GCK12, FPBG14].

curse [GG11, HB14].

curvature [GJ13].

curvature-feature [GJ13].

curve [AD11, ARM15, BJ10, GPT12, LGH+17, LWHS17, PPH12, SG15, AN18, BL14, BBB16b, Cho14, Far14, FWS13, IB11, K10, Kre13, MCN+18, MS13b, NZM10, SKH15, WHJ17, JL16].

curve25519 [SG15].

curve41417 [BCL14].

curves [AK14, BWR12, DW12, LL11, LT14a, YTS12].

Customization [OdH12].

cyber [LJS+14, HZW18, KSA16, QMC17].

cyber-Espionage [LJS+14].

cyber-physical [LJS+18, QMC17].

cybernetica [Ano17c].

cybersecurity [DF16, Hel17, Lan17, LRV14].

cycle
Cycle-Based [MKN13]. Cycles [WBA17, CLCZ10].

D [AP10, CG12b, DBPS12, DWWZ12, EAA+16, GZH12, KWS+12, LJ17, LJ15, MCD12, MKH+12, PGL10, RS16, SGS14, SRK+17, WSSO12, WY12, tWmC12, YI14, YPR17]. D-Based [WSSO12]. D-like [LJ15]. D-PUF [SRK+17]. Dana [Ano10].


DASH [KCC17]. Data [Ano13c, AD12, Bar12, BJL16, BCD+12, BJL12, BW12, CWL+14, CMLS15, CCW+10, CSV15, CCT+14, CLW16, DDS12, Dan12, DR12, DMS+16, DA12, DLZ+16, EKB+16, FMY15, FPY15, FRS+16, GTT11, HSM14, HLT+15, HK14, IBM13a, KRDH13, KGV16, LLZ+17, LWCJ14, LLZ+12, LZC+12b, MLO17, Mal13, MMS17b, MM14b, NNAM10, NR12, PD14, PEM17, PH12b, PRNC17, QZL+16a, QQZ18, Real16, RSN14, SAKM16, Sar10b, SP15b, SKH17, Sia12, SLM10, TCN+17, Tan15a, Vai12, VSV15, WZCC18, XNKG15, XWSW16, YDY+16, YMC+17, ZXYL16, ZPX17, ZTL15, ZLW+17, AP10, ASO14, Ana14, Ano11a, Ara13, ADH17, ALL+18, BTP17T15, BC18, BKV13, CDGC12, CLH+16, CDF+10, CDL18, DFJ+10, DTZZ12, DRD11, ED17, FS18, Gen10, GLB+18, GZS+18, HSM13, HKW+15, HMCK12, HH16, HYS18, HYF18, JHCC14, Kim16, KIH18, KWH16, LSBN14, LT14b, LKX+14, LZY+16, LHL+18, LFWS15, LAL+15].

Data [LCW+16, LZC17, LLL+18, LL16a, LHA+16, MHKS14, OQ18, OSSK16, QCX18, Sch15c, SYY+17, SAR18b, SWW+17, Tan17b, TMK11, TPKM13, WLI13, WZLW13, WS14, XXX15, XWZ+18, XY+18, YYS+16, YXA+16, YNX+16, ZZKA17, ZMM+10, ZWY+13, ZHT17, AEH17, HLYS14, Sch15c]. Data-Centric [DLZ+16b]. Data-Classifiers [KGV16]. Data-Compression [DA12]. Data-Minimizing [BCD+12]. Data-Oriented [NNAM10]. Database [BTHJ12, SBV14, WCL+18, BL11, JHCC14, LW13a, PRZB12, Suc12, YXD18].

Databases [FCM14, HPC10, JKHeY12, Kaw15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12]. Dataset [SP13]. datasets [LVRY10].


De-synchronization [XNG+14, AATM18]. deadly [HLV10]. Dealing [Shai13, VN16].


Decentralized [ABCL17, CD16, GZZ+13, HSMY12, HK14, PPS12a, PAS13b, RH19+16, RSN14, TS16b]. Decentralizing [LW11b]. Deciding [CLCZ10, Sch12c]. Decipher [Cor14b].

Deciphering [Bla16, GMS15]. decision [PKA15, RGP12]. Decisional [LZC14].

Decisions [Bel18, YWK10b]. declarations [HWYW14]. Declassified [ABJ13].

Decodable [Yek10]. Decoding [BBPS12, GMS15, Bax14, Bul10a].

Decomposition [AGH+17, LSL12b, gWpNyY+14, BWA13]. Decompression [PP10b]. Deconstructing [Tar10]. Decrypted [Kob10]. Decrypting [CR12]. Decryption [AN12, KB10, PKKT12, FNWL18, L JW+17, LJWY18, SES+16, SM10a, SM10b, Wu16, ZSW+18b].

Dedicated [Lin17, Nac12]. deductive [ABF+14]. Deduplication [QLL17, SKH17,

Defensive [Pfi10]. definition [LWL10a, YKC+12]. Definitions [GLW12, Mau12, CGKO11, KM14, KGO10, XWXC14]. Degeneracy [WH18].


Delegated [MZYH15, TMC15]. Delegation [FMTR12, SSW12, XWLJ16, YZ12, YAM+15, JSMG18, NAL17, XWS17, ZWM14].


Demodulation [KOP12]. demonstrating [LHA+16]. demosnaick [HLC16].


Densily-based [LSQ11b]. Dependable [BCQ+13]. Dependency [SGP+12].

dependent [GdM16, PAK15]. deployed [MFH13, RY10]. deployment [WXK+17].

DepSky [BCQ+13]. Depth [GH11a, RS16, SS10b, SS12a].

Depth-Based [RS16]. Derivation [LBR12, Cha13a, Lau12]. Derivative [LSQ11a]. Derivative-based [LSQ11a].

derived [ZMM+10]. DES-like [CGS12].

Description [WH18, PLCGS11]. Design [AMN18, Abe12, ARH+18, AIB+16, ADD10, AUMT16, Bel18, BKL+13, DHB16, DRI11, FSK10, HSA14, JWJ+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QLL17, RYF+13, Sch13, SAA10, SZDL14, VPK17, WKB16, ZHX16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17].

Designated [WHJ17, HYWS11, RPSL10, SY15b].

Designated-verifier [WHJ17].

Designation [Che15]. designed [Goo12].

Designer [KMY18]. Designing [CDK+10, FLW12, MRT10, PSD15, SR10].

Designs [BGK12, PCY+17, KDH15].

Detailed [DLV16, ZPXX17]. Detect [JWJ+17, NSA15, WOLP15, Lan11].

detectability [LRW17]. Detectable [Ess17].

Detect [BKBK14, Ess17, GAS+16, HLW12, KW14, SH15, YSC+15, LWIW11].

Detection [AMKA17, ATS15, DSB15, DF11, GZH17, HDWH12, KU14, LGL+12, LC15, MKRM10, MKAA17, NDC+13, NSMS14, SAJL16, SBV14, SP15a, SRAA17, SG14, TM18, YFT17, AOT13, BM13, HB13, JC13, KLC+10, Maz13, MHT+13, WYL13].

Detective [Cho10]. Detector [LTKP16].

Detector-Based [LTKP16].

Determine [FSWF11, Sto12]. Determining [NN12].

Deterministic [MPRS12, NIS12, XXZ12, DTZZ12].

Deterring [WGJT10]. DEUCE [YNQ15].

Developed [Har16]. Developing [CH11].

Development [Pau10].

Devices [AAC+16, CSH+18, DIW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, WKB16, WT10b, XJR+17, Aia15, CLP+13b, CFL13, CTL12, Chi13a, FRT13, IB11, KPP16, LKAT12, MvO11, MV15, OYHSB14, TG17, ZPZ+16].

DFA [WH17].

DFA-Resistant [WH17]. DFT [DDFR13].

DHA [AKY13].

DHA-256 [AKY13].

DHTS [YKKG13].

dictionary [Maf16, MBB11].

Diego [Ano10, Lin14b].

Dies [Mar10a, MMB17].

Difference [BS14, YTP11, JK13].
Differencing [LyWIZZ12, YWW10].
Different
[GZ12, HHH+13, KU12, AKK+17, ABW10].
Differential [BMS12, BNY14, CWP12, CGCS12, ESS15, FXP+17, KWS+12, LGL+12, LJJ16, LJJ15, LYHH14, MRTV12, PH12a, QGGL13, Sun11, WHN+12, Blo15, DDDR13, LLLK10, MNP12, PBCC14, SDM10, SDM14, TSSL11, TS16a, WYL14].
Differentials [WW12].
Differing [GGHW17].
Differing-Inputs [GGHW17].
Die
[LZC14, ABD+15, Chi16, Hof16, HLCL11, HLYS14, Orm16, RH10].
Diffusion [ZHL15, WB12, jT12b].
DIG [NKWF14].
DigiNotar [JB11].
digit [KWH16].
Digital
[AYS15, BBC+13, BM13, BCP14a, FMS12a, GP17, HPO+15, Jin10, Joh10, JL16, LZC+12b, MBF+13, MS10, MN12, NC12, pNyWyY+14, Orm16, PH12b, PAS13b, SAA15, SM13, SC12, SOS15, TC11, TS16b, Yon11, Y+17, YLS12, dRsdlVC12, AGHP14, BPP10, CCG10, FLZ+12, Fri10a, GMS11, Har14, KM11, Lan13, LWZG10, MS13b, MM14a, MO14, QCX18, Sim15b, SL10, yWpNyL11, ZZKA17, Zet14, ZS1S18, Ano13a, Ano15b, Mon15].
Dilly
[Bat10].
Dimensional
[Ano17d, LZC+12b, XYXYX11, DWZ12, QD16].
dimensions
[Pal15].
direct [GH12].
Directed
[LLJ12, KPS10].
Direction
[NS12].
Directions
[BKKB14, CDFZ16, Hof16, PPA18].
Directly
[LZC12a].
directory [SMBA10].
disabled [HFT16].
dissociation
[TMLS12].
Disaster
[NRZQ15, BBG+17].
disclosure
[DSZ+12, PK15, SB17, WGGT10].
discovery
[Ano11a].
Discrete
[BGJT14, CLL16, HKR+18, KLM+12, Xie12, AMORH13, BGJT13, MM13, Mes15, TPL16, VM14].
discrimination
[GPVCdBRO12].
Discriminative
[YY14].
Discussion
[Gli12, Wil18, Bul10a].
Discussions
[KD12b].
Disk
[GM14, Ran16].
Disks
[Mar10c].
disparate
[SSY12].
Dispatching
[YTH17].
dispersed
[ED19].
Disreputable
[ABJ13].
Disruption
[HK14].
Disruption-Tolerant
[HK14].
Dissection
[Dun12a].
Dissent
[SCGW+14].
Distance
[PHY+18].
Distillation
[BJ16].
Distinguisher
[WW12, AMS+10].
Distinguishers
[SEHK12, ZSW+12, AP11].
Distinguishing
[KM10a].
Distortion
[FHS13, Jia17, LGY12, MM17].
Distortions
[WLZ12].
Distributed
[Ano10, BKBK14, BCEM15, CGB+10, FCM14, HSM14, HXC+11, HCL+14, LMD16, LL15, LNZ+13, IWCJ14, YZX+12, YKCL12, ZLDC15, BLV17, CSTR16, dCCSB+16, GAI+18, NCC13, TGI2, XW13].
Distributed-Healthcare
[ZLDC15].
Distributing
[Küp13, MS16].
Distribution
[EA+16, JEA+15, Lop15b, MS13, NNA10, SK11, SN11, TC10, ABB+14, BB14, BGP+17, CML16, FHZ18, JSK+16, JLT+12, LLP+18, NAC12, YWL+17, YHHS16, YL11, ZWS+18].
dithered
[UUN13].
Diversity
[ZTL15].
Division
[SS12b, MN14].
Divisors
[CN12].
Divulges
[ABJ13].
DLSeF
[PNRC17].
Dmail
[CCS14].
DNA
[AEH17, WCG+12].
DNP3
[ACF16].
DNS
[HSLA15].
Do
[Bow11].
doc
[NN15].
Document
[BTHJ12, BPP10, DBPS12].
Document-centric
[BPP10].
Documents
[Bl12, HCDM12, Sta13, ZDL12, CH11, GA11, SR14].
does
[LRW17].
Doesn’t
[RS11, SS12a].
dog
[Ran14].
Doing
[JCM12].
Domain
[AGW15, DBK12, CLY14, DG17, LA15, MR16, PDM12, SGGY11, WLZ12, gWpNyY+14, AMK12, BGAD12, GJ13, IG11, LXC11, LPZ15, LBR12, PW10, QMC17, SCKH10, yWpWyYN13, YZL+18, YWK+10a, YCM+13].
Domain-Specific
[DBK12].
Domains
E-health
[WMX++17, IC17, YZL++18, JKL++16].
E-Learning [Yon11]. E-passport [LZJX10].
e-rental [LY14]. E-Voting [LGPRH14]. E2
[WL14]. EAC [LZJX10]. Each [YLL++12].
EAP [FLH13, HZC++14, ZCLL14].
EAP-based [HZC++14, ZCLL14]. Early
[Bel18, Bro11, And13]. Earth [Har14].
easier [MBF++13]. Easy
[Bel16, SMDS11, Tay14, Wu16, ZDW++16].
Eat [DSSDW14]. Eavesdropping
[CWL16, Han12, PX13, YSJT14]. EC
[Dra16, CFN++14, CCG++16]. ECC
[BSSV12, JMW++16]. ECC-Based
[BSSV12]. ECDSA [BBB++16a, DHB16].
ECG [PLGMCdf18]. ECG-based
[PLGMCdf18]. Echo [DLMM++18, HG1T15].
Echo-Based [HG1T15]. economy [Sir16].
Ecosystems [LDB++15]. EdDSA [JL16].
Edge [AHM++18, DF16, MD15, Sun16].
Edge-centric [AHM++18]. Edition
[Cor14a, Kob10]. Editorial [OK18]. Editors
[LLK18]. Education [LRVW14]. Edwards
[YL16, LT14a, YTS12]. Edwards-curve
[YL16]. Effect [PLGMCdf18, WB12].
Effective [HLT++15, KRHH13, WMX++17].
Effectively [YMC++17]. Effects
[MAL10, SKV12]. Efficiency
[ABF12, CH16, DG17, FRS++16, HRV10,
LLML12, LCL++17a, MS13b, WXLY16].
Efficient
[ABBD13, ASBdS16, BWLA16, BCGL11,
BG12, BV11, BV14, CG12a, CML++18,
CMLRHS13, CWWL12, CJ13, DWB12,
Duna12a, DG17, EM12, FLH13, FHS13,
GT12, GH13, GTP11, GPN++12, GPT12,
GJJ15, GH12, GH17, GCH15, HZC++12, HZC++14,
HZL18, HL10b, HBCC13, HX15, HKL++12,
HDG1C15, HCDM12, HH16, HC17, IAD10,
KPC++11, Kim15, KHP16, KH10, LLP++18,
LDDAM12, LDT12, LKK++14, LCL15,
LSW15, LHY12, LHWS17, LZC17,
LBOX12, MX13, MTK13, MVR12, MU12,
MP12, MC11, MN14, NES++14, NdMMW16,
NZM10, PB12, PRC12, PG12, PCPK14, PRNC17, RBHP15, SGY11, SZH14, SGM16, TLF16, TWZ11, TT12, TM18, WDCL18, WQZ16, WCCH18, XLWZ16, XMCL13, YHL16, YNR12a, YNR12b, YLW13, YNQ15, YLA13, YS15, ZQWZ10, ZLH12, ZSW12, ZXJ14, ZXYL16, ZPW16, ZHW15, AZPC14, AZF12, CH11, CCSW11, CLHJJ13, CZ14, Cho14, Cra11, CGK011. 

Efficient [EA12, FLL14, Far14, FA14a, FA14b, FIO15, FNWL18, GH16, GLM11, HPC12, HYS18, ISC16, IB11, IOV18, JCHS16, JZS10, KKG14, KLI1, KSH18, LLL13, LH11a, LHO10c, LXMW12, LAL15, MLM16, Mes15, Nov10, OCGD11, PZBF18, PC14, Rao17, SZMK13, TLL12, Tso13, TKHK14, VN17, WYL13, WLZ16, WT10a, WXK17, XZW10, yYWqWZC13, ZLY10, ZNI1, ZCCL14, ZT16, ZZC15, ZH13, LZ12, TCL15]. Efficiently [FWS13, LGH17, SLY16]. Effort [RSGN12]. Effort—Release [RSGN12]. EGHR [CML18]. EHealth [TMGP13]. eID [SGCR16]. eight [Sun11]. 

eight-round [Sun11]. Einführung [Buc10]. Einstein [HR13, Wesi15]. Elbirt [Bar12]. Election [Ess17, TKM12]; elections [QIS18]. 


Elements [Kra12]. Elevation [LZC12]. Elliptic [ADI11, AK14, AR15, DW12, GPT12, LGH17, LWH17, PPH12, SG15, AMN18, BAAS13, BL14, BBN16b, Cho14, Far14, IB11, KX10, MC18, MS13b, NZZ10, SKH15, WH17]. ELmD [BDMLN16]. Elsevier [Ano15]. Email [Bel16, CCS14, XJW16, WR15]. embed [KPS10].

Embedded [AB15, BS12, BJCHA17, CFXY17, HC17, JWJ17, LWH17, SOG15, SK12b, SDM12, WXY17, YGD17, YS15, Ano11a, CVG13, Eis10, MFH13, XWZW16].


Emerging [BSV12, KSA16, OS16, FPBG14, ZHH17]. Empirical [gWPnY14, EBKF13, Sar14]. Employees [Mor12]. EMV [Cho10].

Enable [MS14]. Enabled [GPT12, HFT16, QZL16a, QZL16b, SGC16, SSPC12, BMM12, TODQ18]. Enabled/disabled [HFT16]. Enables [IBM13a]. Enabling [FRS16, JSM18, SSY12, WPZM16, YYS16, Sch12b]. eNB [CLM12]. Enciphering [CMLRHS13, HRM12, MLCH10, Sar11].

Encloses [WBA17]. Encoded [DG17]. Encoding [BR14, SK12a, TJZ12, XHX17, PC14, Sun16]. Encounter [NA10a].

Encrypt [RAZ15, Ran14]. Encrypted [ADR18, BTHJ12, CWL14, CWL16, Cor14a, DWB12, FCM14, FRS16, Gen13, GLG12, GZH17, HTZ12, HB17, HCDM12, IMB17, IBM13a, JSCH17, Kau15, KGV16, LA16, LQD16, Lop12, Mur16, NBZP17, NNAM10, QLL17, SAKM16, Sia12, TM18, Vai12, WBC10, XWSW16, YDY16, ZD12, ZXYL16, ZVG16, ZLW17, ZHM17, AZTH11, BTPLST15, BGP17, BKV13, BL11, CH11, Cri16, CDL18, DKL16, DRD11, ED17, FTV10, Gen10, GZS18, HH16, KHI18, LXX14, LZY16, LHL18, LW13a, OSSK16, PRZB12, SEXY18, SWW17, Suc12, TKM13, WR15, XWY18, XDY18, ZLY10, ZFH18, ZHT16].

Encrypting [CC10, Mar10c, dSrlVC12, LGFCG1R14, Pow14]. Encryption [ADM12, AV12, AEH17, Ato12, AAC16, Ano13c, Ano14, Ano15c, Ano17d, APK12, ABF12, AS16, BV15, BWL16, BPR14a, BPR14b, Bel16, BDOZ11, BW12, BS14, Bla16, BKLS12, BPDS12, BHP14, BDML16, Boy13, BV11, BV14, BVG14,
CVM14, CMO+16, CLL16, CWWL12, CN12, CZF12, CLHC12, Che15, CGL+12, Chi12, Chu16, CRE+12, Con18,CNT12, CLW16, CD16, DR10, DN12, DFJ+10, DLSLB18, Des10b, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJHJ12, FFL12, Fuc11, GWWC15, GH+16a, GGHW17, GM13, GZZ+13, GSW+16, GH11a, GH11b, GHS12, GHP512, GDCC16, GVW12, GVV15, GM14, GL12, GKS17, Gue16, HSMY12, HZ11, HG12, HC17, HRC+15, HP12, IAD10, JLS12, JLH12, Jia14a, JR14, Kam13, KB10, KME+12, KMY18, KTT12, KOS16, KKA15, KFOS12, KHPP16, KS12, LMGC17]. Encryption
[LMG+18, Lau17, Led16, LLSW16, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LLC+15, LTZY16, PLL17, LSLW15, LH11b, LB15, LY15, LW16, LMLL12, LLI18, MZHY15, MLO17, MMP14, MR14a, MTY11, MS18a, MVVR12, MMS17b, MRL+18, MBF18, MPRS12, MTK12, KMRM10, M Sas12, Nac16, NdMMW16, NTY12, NMS14, NAL17, O T12, OGG+15, PMZ13, PR12, PB12, PDDN15, Per13, PKTK12, PPS12a, PY115, PM12, PCY+17, PRSV17, RVH+16, RZZ+15, RSGBN12, RDZ+16, RVRS12, Saa12a, SSW12, Sar10b, Sch15a, SLGZ12, SZZ14, She14, Smi11b, Sta12, SGH15, SMOP15, Tan11, TCN+17, TCL15, TCM15, Tan17b, TDD13, TKR14, TT12, U11r15, Vai11, VSR12, VOG15, Wal18, WHC+15, WP17, WDC18, WSS12, Wat12, WLC12, WDDW12, WZ15, WWHl12, WMS+12, WQZ+16, XNK15, XY18, XXZ12, XJW13, XWLJ16, XJX+16, XHX+17, YZ12, YZYX+12, Ye10, Ye14, YH16, YKNS12]. Encryption
[YNQ15, YKC+11, YFK+12, YCZY12, YKKL12, ZOC10, ZPM+15, ZDL12, ZYT13, ZWTM15, ZQQ15, ZMW16, ZZM17, ZHW15, ZY17a, ZYM18, ZWS+18, AHS14, ATKH+17, Ana14, Ano13b, Ano15e, Ano16f, ABR12, AMHJ10, ACD+15, AHL+12, BAAS13, BC18, BG14, BSW12, BGP+17, CPT18, CFVP16, CFZ+10, CW14b, CLH+16, CMSM17, CZ15b, CS11, Chen10, CW12a, CDF+10, CM13, CGKO11, DLZ16a, DDM17, DTZZ12, Eve12, Eve16, FAA+18, FH13, FGW11, FSGW12, FMB+18, Fay16, GMDQG15, GH13, GHP513, GLM+16, GH12, GLL+18, HGWY11, HQHZ14, HZZ18, HWDL16, HWZ18, HT13, HL11, HLT13, HYS18, HYF18, HKHK13, JCHS16, Jia14b, JSMG18, JHCC14, JSM+18, Kam16, KHMB13, KKM+14, LW16, LCL+17a, LCL+15, LFZ+17, LCT+14, LFS15, LPdS10, LH11, LW10, LW11b, LZ12, LCZ14, LPZ15, LCV+16, LZC17, LJW+17, LJYW18, LLL+18, LL16a, LW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10]. Encryption
[Mon13, M Sas13, NES+14, PPA18, Pet12, QRW+18, Ran16, RG10, RWZ13, RPS10, SES+16, SE18, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SGFCR+18, SLM10, SKB+17, Spa16, SG16, Tam15, TPL16, jT12b, WQJT10, WY10, WWZ11, WWY11, WHY+12, WDZL13, WLFX17, Wan18, W GZ+12, WCH18, XWZW16, XWC14, XSWC10, XXX15, XWS17, XWZ+18, YT11b, yYqWzC13, YZCT17, YHM18, YCT15, YLZ+16, YL11, ZWQ+11, ZZ11, ZLW+12, ZXJ+14, ZWM14, ZT14, Zha15a, ZCC15, ZM17, ZYC+17, ZZ12, ZL12, ZDW+16, ZY17b, Zhu13, Wan14, LAL+15, Sar18a, Kat13]. Encryption-based [BC18, XWZ+18]. Encryption/Decryption [KB10].
Encryptions
[zGXW12, LG12, SYL+16, RD17].
Encyclopedia [vTJ11]. End
[Ano15c, BRR+15, BGP+17, CFE16, Chn16, RST15a, RST15b, Chn13a].
End-to-End [CFE16, RST15a, RST15b, Ano15c, BRR+15, BGP+17].
Endomorphism [FWS13]. Endomorphisms
[AK14, LGH+17]. enemies [Fag17]. Enemy
[BC14, CAC14]. **Energetic** [PDMR12].
**Energy** [Ano15d, AZF+12, ABC+17, Bla16, JEA+15, LSC+15, MP12, TLCF16, TCN+17, VN17, CZ14, ZTZ16]. **Energy-Efficient** [MP12, TLCF16]. **Energy-Harvesting** [ABC+17]. **Energy-time** [Ano15d].


**EUROCRYPT** [PJ12, Gil10]. **Europe** [GKP12, Mid10]. **European** [GKP12]. **Evaluating** [RAZ15, WP15]. **Evaluation** [CGCS12, DM15, EGG+12, KVvE18, KLM+12, MKN13, MLBL12, SMOP15, ZLDD14, FPBG14, TPKT12, ZZKA17]. **Evaluations** [ZM16]. **evaluators** [ZZKA17]. **Evasive** [BBC+14]. **Eve** [AAE+14, ERLM16, FHM+12]. **Even** [ARH14, LPS12, Ano14, DKS12].

**Even-Mansour** [LPS12]. **EventGuard** [SLI11]. **every** [Hof16]. **everyday** [HST14]. **Everyone** [Ano15c]. **Evidence** [Blu12, SL11]. **evident** [MN10]. **Evolution** [LQY10, Tay17, BHvOS15]. **Exact** [TMK12]. **exam** [Mor12]. **examination** [VCK+12]. **Examining** [SP10]. **Example** [KD12b]. **Exchange** [CLY14, CST+17, DG15, FVS17, GZ12, HC12, LY16, MSU13, TYM+17, WSA15, WT10b, YS12, YLW13, YRT+16, Yon12, ZHI16, AKG13, AIB+16, FHH10a, FA14b, FIO15, GBNM11, GLM+11, Jia14b, LWS10, LML+13, SEXY18, TCS14, Tso13, TKHK14,
WHJ17, WZM12a, WZM12b, WT10a, WTT12, XW12, YC12, ZXWA18, ZG10].
Excitation [SOS15]. Exclusive [Men13].
Execution [AARJ12, RQD+15, YS15],
existing [FMA+18, HT13]. Expanding [MS16, Sch15b]. Expansion [LTC+15b, TS16a, BAB+13, Die12, JK13, Pet11].
Expectations [DY13]. Expected [DMV15, KOT17]. Experience [AD12].
experiences [JAE10]. Experimental [LCW+16, DHW+13]. Experimentally [LHA+16]. Experts [Sto12]. Explicit [AQD12, FHS13, FIO15, ZZC15],
explainability [CFN+14]. exploitation [MAK+12, NCCG13]. Exploiting [ACK+10, BDGH15, VDB+16, ZPF+16].
Exploits [ZGC16]. Exploration [AUMT16, ABDP15, RYF+13]. Exploring [Cil11, FNP+15, TLC16, WHC+15].

**Facet**

facilitate [Chi13a]. Facsimile [Ano16d].
Factor [HXC+11, LLC11, AIB+16, CLP+13b, DMWS12, ED19, HC12, IC17, JKL+16, JMW+16, Ken11, LNK+18a, LNK+18b, Lit14, WW14, Wat14a].
Factoring [APPVP15, LLML12, MM13].
Factorization [Con12, FS15, KFL+10, Kuz11, YAM+15, Mes15, TPL16]. Failing [Cer14].
Fairness [ALR13, Ash14, GHKL11, Wg16, MV16b].
Fake [KU14]. Fallen [HCPLSB12]. False [LLZ+12, CDDG12]. Families [BSS+13, Ku12]. Family [ARH+18, BMS12, BKST18, DGIS12, DJG+15, FLS+10, FFL12, GNL12, MGF16, YCL17]. Fanin [S12a].
Fast [BLAN+16, Bru12, CHS15, DSLB18, GSN+16, NR12, PRSV17, WHZ12, WBA17, WQZ+13, ZHW+16, FHH10a, HKMB13, MBB11].
Fast-AD [SMB10]. Faster [CN12, HL17, TH16, Ant14]. Fault [AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JTL2a, LGL+12, LCLW17, LGLL12, MKR10, MKA17, PH12a, RZZ+15, SEY14, YGD+17, BBBP13, PBCC14, WMYR16].
Fault-Based [BBB+16a]. fault-resistant [PBC14]. fault-tolerant [WMYR16]. FFI [Bha16].
FC [DDS12, Dan12]. FEAD [ZW14].
Feasibility [AAC+16, FKS+13, WHC+15].
Feature [Ber18, SGP+12, FTV+10, GJ13, MHT+13].
Features [YI14, ZTL15, FNP+15, LCM+17, LTC+15a].
Feauveau [Ara13]. February [An10]. DDS12, Dan12, Dun12b, Kiva11, Lin14b].
FedCohesion [CCFM12]. Federated [BS13b, CCFM12, CSL+14, BMBS10, JAS+11, TODQ18].
federated-IoT-enabled [TODQ18].
Federation [SS10a, NB13]. federations [MMS+17a, MLM16]. Feedback [HZ11,
Fundamentals [Joh10]. Further
[HCL+14, WHY+12]. Fus [FMS12a].
Fusion [ABCL17]. Future
[AYS15, BCE+12, BKBK14, Bon12, CDFZ16, GCK12, HYS18, Mon13, Ano13d, FPBG14, Mac12, PPA18, PHWM10, MJS13].
Future-proof [Mon13]. Fuzzy
[KRDH13, NC12, SH11, XJWW13, Alp18, KHMB13, MMSD13, SM11, SNM14].

G [HLYS14]. G2C [BMP12]. GA
[MMSD13]. GA-fuzzy [MMSD13]. gadgets
[Get13]. Gait [XJR+17, XJR+17].
Gait-Based [XJR+17]. Gait-Key
[XJR+17]. Gallai [SS10b]. Galois
[CFR11, CLF+17, HSA14]. gambling
[Ana14]. Game
[MZA+13, LPJZ15, SD10, SKEG14].
game-theoretic [SD10, SKEG14]. Gap
[LRVW14, TMGP13, PPA18]. Gaps
[SPM+13, DKL+16]. Garble [AIK14].
Garbling [App13]. Gard [Kap11]. Gate
[Kar12]. Gases [App13]. Gateway
[WZM12a, WZM12b, WL11, WXK+17].
Gateway-oriented [WZM12a, WZM12b].
Gaussian [HKR+18, YWL+17]. GCD
GCM/GMAC [SKK10]. GDLP [MMZ12].
Gear [AHS13]. Geckos [GSC17]. geese
[Bai12]. GenePrint [HQQ+16]. Gener
[HYS18]. General
[FHJH12, GFBF12, Gue16, HP12, KOTY17, LPL15, PB12, SJWH+17, YFF12, ABPD15, Bai12, DGNJ14, HQZH14, LWS10, WS12, YC11, ZYC+17]. General-Purpose
[Gue16, ABPD15, DGNJ14]. generalisation
[LR15]. Generalised [Hes12].
Generalization [GMNS15]. Generalized
[BFMT16, LPL15, PC14, TY16b, Ye14, ZAC17, ADG16, BNS17, KLI1, NC13, YMSH10]. Generated [ADD10, LCL17b, NN12, XYXYX11, AGHP14, LW13b].
Generating [Ano16e]. Generation
Generator [ADD10, BK12a, CDK10, MVV12, NNAM10, NKWF14, CFY10, LGKY10, MRT10, PLvdLE10, SH11, SM11, XSWC10].

Generators [AS17, DSLB18, LTKP16, MFG16, NIS12, PFS12, CP13, HRV10, MG15, Sti11, Zim10].

Generic [BWLA16, BR14, Chi16, GWWC15, HXC11, Sar10b, SY15a, WCL18, ZCLL14, HQY16, YT11b].

Generically [MHKS14]. Genetic [JK13, MM17, ASVE13, EEAZ13, PTK14].

genius [Hai17].

Gentry [GH11b].

Genuine [HR13].

Genus [FWS13].

go [Har14].

geo-location [Har14].

geodesics [ZZCJ14].

Geographic [LC17].

Geolocation [FPY15].

Geometric [DSB16, GTT11, WLZ12, YWNV15, WCL18, ZCLL14, HQY16, YT11b].

geometrical [TLL13].

Geometrically [WYW13].

Geometry [tWmC12, CFR11, CZ15a].

German [BDFK12, Bt12, Buc10, Cop10a].

Germany [FBM12, GLIC10, Sen10, Wat10].

Gesture [LCL17b].


Getting [ES15].

GGH [LH10b].

Ghost [CDA14].

GHZ [CCL13].

GH-Z-State [CCL13].

giant [Joh15].

girls [Mun17].

Girod [GMNS15].

GLARM [LLZ16]. glimpse [Mic10a].

Global [CLP13a, CLH13, MRS17, GH16, LH11a, TMK11, ZX11, LNK18a].

Globally [CCS14].

GMAC [SKK10].

Goal [BMP12].

Goal-Driven [BMP12].

Goes [BCD12, RY10].

Goldebrech [Lin17].

Goldstrike [BH15].

Goliath [Sch15c].

Gong [LLW16].

Good [DQFL12, FY11, LSBN14, RY10, SA14, WT13].

goodbye [HU15].

Google [Har14, Loe15, VGN14].

Goppa [MBR15].

Gordon [GW14].

GOST [LC13, WYW14].

Government [Ano15e].

GPG [Ran14].

GPGPU [RVRSCM12].

GPGPUs [TLCF16].

GPU [BCGH11, GCH15, HBMRNM16, JHCC14, MB11, ZOC10].

GPUs [VKP17].

Graded [BR14].

grail [Wat15, Mic10a].

Grain [BMS12, FSGW11].

Grain-based [GJMP15].

graph-based [GJMP15].

dish [SKH15].

Graphical [BCV12, CTL12, LTC15a].

graphical-based [CTL12].

Graphics [HHMK14, ABDP15, KY10, PGLL10].

Graphs [BFM12, KY12, Lai17, PMZ12, BGBT12].

Gray [DA10, UUN13].

Gray-Level [DA10].

great [Acz11].

green [dCCSB16, ZTZ16].

Grey [LRW13].

Grey-box [LRW13].

Grid [CGB10, DLZ16b, KS15, LPL15, AMN18, JAS11, MCN18, WS12, YY11].

Grid-Based [LPL15, WS12].

Grids [SC10, CT11b, GL13, Shy15, JAE10].

Gröbner [EVP10, FES10, Tam15].

Gros [Dan12].

Ground [KP17].

Group [AEHS15, BSV12, CGY13, CLW16, DT13, FVS17, HL10a, Har13, LLZ16, LCCJ13, TW14, XLM12, XGLM14, XZLW15, ZNH16, AKK17, CML18, GBMN11, HCCC11, HPY10, IOV18, LLS13, LWS10, RS15, WDZL13, WTT12, YZL18, ZZKA17, ZWQ11].

Group-based [LLZ16, CML18].

Group-key [IOV18].

Grouping [LNZ13].

Grouping-Proofs-Based [LNZ13].

Groups [Abe12, GZ12, XNK15, YS12, YKNS12, MZ17a, WQZ13, ZZ15].

GRS [TD14].

GSR [LC17].

Guaranteed [TBCB15].

Guess [FSWF11, Fok12].

Guessing [Che15, LCL17b, XJJW13, FIO15].

Guest [Gup15, LLK18].

Guidance [STC11, Han12].

Guided [CJFH14, ZSMS18].

Guiding [DGJN14].
HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WTT12.

**ID-card** [Ano17c]. **ID2S** [YRT+16]. **IDEA** [BNY14]. **Ideal** [LPO+17, WCL+18, HKT11, yYqWqZC13]. **idealness** [TD14]. **ideas** [Mac12]. **idempotent** [Dur15]. **Identical** [Bow11]. **Identifiable** [Oba11]. **Identification** [FSX12b, FSX12c, FSX12a, VGA15, YGFL15, AGLW16, CTHP13, CJP12, CJP15, EA12, HQY+16, KI11, KL13, NLYZ12, YTM+14]. **identified** [AZH11]. **identifier** [MJS13]. **Identifying** [CSV15, SVG16, ZCWS15]. **identities** [GLM+11]. **Identity** [AQD12, ASM12, ASVE13, Ano15b, ACAT+15, ASS15, BWLA16, BCF16, BHG12, BPKW12, BDFK12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CZLC12a, CZLC12b, CLHC12, CZLC14, CGL+12, CGY+13, Chi12, dCCSM+12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GOPB12, GY13, GDCC16, GJJ15, GJJ17, HZC+12, HvS12, HSM13, HSM14, HZC15, HYWS11, HYF18, KKA14, KRB12, Kuz11, LMG+18, LMB12, LSL12a, LKAT12, LXL14, LLC+15, LTZY16, LSLW15, LH11b, LSC12, LBR12, MLO17, MBF+13, MGJS12, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SS10b, IdM12, SAAB10, Sch11, Ser12, SSPC12, SKGY14, SWW+16, SGH15, TKB14, Tia15, TH16, TMGP13, Vei12, WY10, Wan14, XXZ12, XQL11, XJW+16, YZX+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCY12, ZLH+12, ZMW16, ZWD+16, ZPXX17, ZYM18, ZTSR12, ATKH+17].

**identity** [Ano13k, BMBS10, BOB13, BMM12, BBGT12, CTHP13, dCCSB+16, DZ14, Din10, DWZ12, FA14b, GMRT+15, GPVCdBRO12, HZC+14, HWDL16, HZWW17, HLR11, HLI11, HWPY10, Hwa11, JGS+10, KKGK10, KKM+13, KL11, LKLK13, LK12, LXMW12, LCT+14, MMS+17a, MD15, MGP10, MJS13, MLM16, MM13, NCL13, OŠ11, PLCGS11, QYW16, RG10, SYY12, SE14, SE16, SR10, hSSZ15, SA16b, Sim15b, SSA11, SSS11, SMG16, WWY11, WWWW17, WMX+17, Wat14b, WWW17, XW12, XCL13, YWL+17, yYqWqZC13, YYS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZZ12, LZJX10, PN10, Sar18a, Kat13]. **Identity-Based** [ASS15, BWLA16, BHG12, BPKW12, CZLC12a, CZLC12b, CZLC14, CGL+12, CGY+13, Chi12, FHH10b, FZT14, FSX12b, FSX12c, FY13, GJJ15, GJJ17, HZC+12, HSM14, HZC15, LMG+18, LSL12a, LL+15, LTZY16, LSLW15, LH11b, LSC12, LBR12, MLO17, RDZ+16, SGH15, TCR14, Wan14, XZ12, XJW+16, YZX+12, YHK+10, YKC+11, YFK+12, YCY12, ZLH+12, ZMW16, ZPXX17, ZYM18, CSZ+11, HSM13, HYWS11, HYF18, LKAT12, LXJ14, MJGS12, RS15, SWW+16, Tia15, TH16, ZWD+16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HWDL16, HZWW17, HLR11, HLI11, HPY10, Hwa11, LK12, LCT+14, MJS13, MM13, NCL13, QYW16, RG10, SE14, SE16, hSSZ15, SA16b, SSA11, SMG16, WLFX17, XW12, XCL13, YWW+17, yYqWqZC13, YKC+12, YXA+16, ZZ12, LZJX10, Kat13].

**Identity-Hidden** [PSS+13]. **IdM** [ACAT+15]. **IDs** [SOS15]. **IEC** [BCM12, BCM13]. **IEEE** [IEE10, IEE11b, IEE13, Yan10, BOB13, CL11, FLH13, NBZP17, ZBR11]. **IEEE802.16e** [HLCL11]. if [ABJ13, Rus15]. **IFIP** [GLIC10]. **IFP** [MMZ12]. **Igor** [Sha10]. **II** [Mun17, SCPSN10b, SMOP15, ZWS+18]. **III** [SMOP15]. **Illegal** [ABJ13]. **Illogical** [Hel17]. **Illustration** [KLY+12]. **Illustration** [GHS14]. **Illustrated** [Cop10a]. **Im** [BG1+10, BG1+12]. **IMA** [Che11]. **IMACC** [Che11]. **Image** [Bai10, BAAS13, BDB14, BWR12, CFH14, LCT+14].
DA10, IAD10, JKHeY12, KPS10, LA15, LLI17, MBC15, MAL10, MSM+18b, PWW10, RS16, RVRS12, SH11, SM11, SJ12, SGP+12, SSA13, SRAA17, SZZT18, WHZ12, WXX12, WYY+13, WYCF14, yWXYZ+18, WYK12, YLL+12, YWWN15, Ye10, Ye14, YH16, YX18, ZXZ+11, BWA13, BM13, CT11a, CW14a, EA11, FMB+18, GCK11, HLC16, KM11, LXCM11, LW10, LWLW11, LW13b, LPZJ15, MO14, MS17, NES+14, PTK14, SE18, Sch12a, SM12, SNM14, SGFCRM+18, Sun16, jT12b, TTL10, TLL13, UUN11, UUN13, yWpWyYpN13, WG+12, WKH11, WOLS12, XSSWC10, YWL+17, YC11, YCC16, YSC16, ZLW+12, ZT14, ZSMS18, ZL12. Image-Guided [CJFH14]. Image-Scrambling [LLL17]. ImageMagick [Tay14]. Imagery [BCP14a, Ara13]. Images [BCPV11, CLF11, FR16, GL10, LC15, LLY+12b, MR16, NC12, Yam12, dR5dVC12, AMK12, DD13, HWVW14, LW13b, MM14a, MKH+12, UUN13, WHL13, WZLW13].


Implementations [BFCZ12, BFK16, BDGH15, BJ10, Bru12, CMLRHS13, CBL13, ERRMG15, LGH+17, MLCH10, Tom16, YZLC12, ABBD13, ABF+14, BFG+14, BJR+14, CFN+14, CGH17, LBOX12, Stat11b, ZSW+18a].

Implementing [Dav11, GH11b, HTZR12, LTC+15a, SG15, SLM10, VOG15, SA16b]. implicit [DWZ12]. Imly [ALR13, LRW17]. Importance [YL17, LMMSG12]. Important [TC10]. Impossibility [ACM+17, BCF+14, Mat14]. Impossible [BLo15, CWP12, LJF16, TSSL11, WYL14, WWC12, MNP12, SDM10, SDM14]. improbable [TS16a]. Improve [AQP12].

Improved [Ber18, BCP14a, Chi12, CGK011, GLLSN12, IK15, JLH12, KZG10, LT14a, LWZ12, LJF16, LH11, LCC13, LC15, LML12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GL13, PWLL13, SDM10, XHH12, Wan14].

Improvement [FRS+16, MWZ12, PLPW13, AN15, BMB16, CHS11, Fur14, LNM+11]. improvements [EA12, HRV10, Tso13]. Improving [Ber18, BCP14a, Chi12, CGK011, GLLSN12, IK15, JLH12, KZG10, LT14a, LWZ12, LJF16, LH11, LCC13, LC15, LML12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GL13, PWLL13, SDM10, XHH12, Wan14].

Induced [VDB+16]. induction [BBBP13].
Industry [Ano11b, QZL+16a, Cha13c, Men13, ZS18]. Infective [GST12].
Inference [Bro11, DBPS12, NC12]. Inferring [BPSD17].
Information [AQD12, ABCL17, Bai10, BF11, CVM14, CDGC12, CGB+10, CST+17, CBL13, Dew11, DP12, FH17, FHS13, HHH+13, IF16, JHNN12, LG12, LW11a, Low12, MA17, MAL10, NTKG17, SGC14, STC11, TWZ11, WSS12, Yan10, Yek10, ZZ15, ZHL15, AB10a, Abe10, AL15, ASVE13, BSS11, BGP+17, DMWS12, KL13, LWK+18, MKH+12, Mar10b, SRB+12, WW13, BYL10, LH10a].
Information-Theoretic [CVM14, WSS12, CDGC12]. Information-theoretical [ZZ15, KL13].
InfraStructs [WW13]. Infrastructure [GM13, PN10, GAI+18, JAE10, SA12]. ingenious [Mac12]. Inhibiting [GAS+16].
Initial [PAS13b]. initiation [AN15].
Injected [LLZ+12]. Injecting [BBGT12].
Injection [ABS+12, ARP12, DDR+16, JWJ+17, PYM+13, YGD+17]. Injections [LCLW17]. Ink [Keb15, Mac14]. Inner [ADM12, LMG+18, OT12, YKNS12, DDM17]. Inner-Product [YKNS12].
innovations [JSM+18]. Input [GGHW17, XXZ12, PBC14]. Inputs [GGHW17].
INSCRYPT [BYL10].
Insecure [BCGN16, Mur16, Lan17].
Insider [AJA16, ERLM16, LJS+14]. Inspection [FGR+17, VCK+12, AZH11]. inspired [BW13, GPVCdBRO12, OK18].
interceptor [Cho10]. Intercepts [Don14].
Interface [WBA17]. intermittent [CL16]. International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FB12, GLC10, JY14, LCK11, LW11a, LTW11, MV12, PJ12, Sen10, Wat10, Yan10, Yan11, AB10a, Abe10, Ano11a, BYL10, BL10, Gil10, GG10, HWG10, LH10a, IEE11a]. Internet [Ano13d, LFGCGCP14, TW14, AAC+16, Ano13b, CLF+17, CW12b, DRS16, DG15, Gel13, HZL18, JZT+16, LNK+18b, LGH+17, LSG16, MJGS12, MJS13, MCF17, NLL12, NLY15, Orm16, PLGMCdF18, SB17, SYW17, SYC+17, SKEG14, WCCH18, YCT15].
Internet-Draft [MCF17]. Internetworking [SAAB10].
interoperability [HKW+15]. interplay [JW14].
Interpolation [JZT+16, KU14]. Interpretation [MZ17b]. Interpretation-Based [MZ17b].
intersection [LZ+16]. Interval [PPR+12, Cra11, DTZ12, LWY12, MO14].
Interval-based [PPR+12, Cra11]. Intra [HF14b]. Intra-Masking [HF14b].
Intrinsic [SN10, NS10, RCW15]. Intrinsically [SRK+17]. Introducing
Invention
[NSMS14, SAJL16, SBV14, YKC12].

Intrusion-resilient [YKC12]. Intrusive
[AARJ12, MFH13]. Invariance
[yWpnL11]. Invariant
[CSW12, NKWF14, RS16, WYW13,
YWNW15, GZHD12, LXCM11]. Invariants
[NKWF14, CDsLY14, KK10, MZ17a, TLL13].

Invention [Orm16]. Invents [Ant14].
inversion [KH14]. Invert [ZWT15].

Inverted [ZXY16]. Invertible
[SLY16, UUN13]. Investigating
[SMP13]. Investigations [Blah16, Har14].

Invisibility [BN14]. Invisible
[Keb15, Mac14, SYL13]. InvisiMem [AN17].

INVISIOS [AARJ12]. Involution [Bru12].

Involving [HLCL11]. IoT
[AATM18, CCM17, CSH18, FQZF18,
GAI18, NVM17, SG16, TODQ18, TG17,
WCFW18, WXK17, YFT17, YTH17,
ZCWS15]. IoT-Based [YTH17].

IoT-Enabled [SGC16]. IoTs
[SAJL16, ZSW18a]. IP
[AGLW16, AZH11, PJ18, PA10, RS17,
SP15a, T2ZF12, WBC10]. IP-SEC [PA10].

IPE [ZM16]. iPhone [Wu16]. IPs
[GSFT16, NDG17]. IPv6 [KP12]. IRC
[HB13]. IRC-based [HB13]. IRIW
[JKe12]. irregular [YWL17]. ISBN
[Ano15b, Ano17b, BAI12, Joh10, Mur10,

ISO [BCM12, BCM13, TS16a, WWBC14].
ISO/IEC [BCM12, BCM13]. Isogenies
[Y+17]. Isogeny [KAK18, Lau17].

Isogeny-Based [KAK18]. Isolated [YS15].
Isolating [LG12]. ISSAC [Wat10]. Issue
[Ano13d, Ano16a, Ano16b, Ano16h,
CSYY18, GO17, LW13a, LLK18, XW13,
PHWM10, Sim15b]. Issues [ABHC16,
PZPS15, JAE10, KJN16, MHV15]. ISTE
[Ano15b]. Italian [Sac14]. Italy [Cra12].

J [Bar12, Led16, Sch15a, ZWM12a]. J2ME
[GPT12]. J2ME-Enabled [GPT12].
Jacobian [BAAS13]. Jacobians [Hes12].
Jacques [Nac12]. Jamming [YSL14].
Janet [Ayu12]. Japan [Sah13, Maf16].
Japanese [Don14]. Java [GPT12, XHH12].
Jaypee [CGB10]. Jean
[Dew11, Nac12, SR14]. Jean-Baptiste
[Dew11]. Jean-Francois [SR14].
Jean-Jacques [Nac12]. Jeffrey [Mei10].
Johnny [HM12, RA15]. Join [PD14].
Joint [ABF12, LC15, PM13, TC17,
LSQ11b, ZC12]. Jonathan [Ful10, Mou15].
Jones [Ber16a]. Jose [ACM11]. Joseph
[Mei10]. Joshua [Ano17b]. Journey
[CFST17]. Jouxs [AY12]. JPEG
[AOT13, LSQ11b, LC15, MAL10, QZ14,
SK12a, WHZ12, WHL13, ZC12].


Junction [VDB16]. June
[ACM10, ACM11, Gil10, Kap11, Wes16].

Juniper [CCG16]. Juraj [Gas13]. Just
[Ph10]. JXTA [AMHJ10].

K2 [PS12]. Kalyna [OGK15]. Karatsuba
[BCL14, MRL18]. Karhunen [BCP11].

KASE [CLW16]. Katz [Ful10, Mou15].

KDM [MITY11]. Keccak [BDP12]. keep
[Rus15]. Keeping [CG14b, Man13, Gup15].

KEM [CZLC14]. kept [Chai3c]. Kerberos
[SCKH10, TW14]. Key
[ASN12, Ano11b, BN14, BVS13, BL12,
BBB16a, BCO13, BKL12, BF11, BKKV10,
BB10, CVM14, CT18, CL14, Che15, CJ13,
Chi16, CCT14, CNT12, Cou12, CMA14,
DWWZ12, DL12, EAA16, FZT13, FVS17,
FMB12, GFBF12, GT12, GZZ13, GSW16,
GST13, GPT14, Gir15, GKS17, GZ12.]
GLB\textsuperscript{+18}, HSMY12, HC12, HL10\textsuperscript{a}, HCL\textsuperscript{+14}, HTC\textsuperscript{+15}, HEC\textsuperscript{+12}, Jia14a, JEA\textsuperscript{+15}, KP12, KTT12, KFOS12, Kin15, LLSW16, LCLL15, LQY10, LY16, LH11b, LCCJ13, LBR12, LLH18, MZHY15, MVV12, MMP14, MTS11, MMY12, MPRS12, MNS11, MSU13, NNA10, NYR\textsuperscript{+14}, NTY12, Om16, PSM17, PDNH15, PCPK14, Pud12, PNRC17, RVH\textsuperscript{+16}, RSBN12, RW12, Saa12a, SK11, SNJ11, SEHK12, SK12b, SWM\textsuperscript{+10}, Sia12, SGH15, SLY\textsuperscript{+16}, TMC15, TYM\textsuperscript{+17}, TM12, WP17, WSS12, WLC12, WZ15, WCL\textsuperscript{+18}, WWHL12, WT10b, XNKG15, XXZ12, Xia12, XLM\textsuperscript{+12}, XJWW13, XGLM14, XZLW15, XJR\textsuperscript{+17}, YM16. \textbf{Key} [VYZ\textsuperscript{+12}, YS12, YLW13, YRT\textsuperscript{+16}, YL17, Yon12, YKC\textsuperscript{+11}, YFK\textsuperscript{+12}, ZHX16, ZY17a, AA14, ATKH\textsuperscript{+17}, APK\textsuperscript{+18}, ABB\textsuperscript{+14}, AKG13, AIB\textsuperscript{+16}, ABW10, AN15, BS15, BGAD12, BB14, BJ16, BSW12, BGG\textsuperscript{+13}, BBB16b, CFL13, Cha13a, CSD18, CLZ\textsuperscript{+17}, CTL13, CML16, CLCZ10, DLK\textsuperscript{+16}, DGIS12, Dur15, FHH10a, FA14b, FIO15, FHZW18, GMRT\textsuperscript{+15}, GPP\textsuperscript{+16}, GH16, GBNM11, GLM\textsuperscript{+11}, HPC12, HZWW17, HL11, HLYS14, IM14, ISC\textsuperscript{+16}, IB11, IOV\textsuperscript{+18}, JSK\textsuperscript{+16}, JLT\textsuperscript{+12}, Jia14b, JSMG18, KDH15, KK14, KP18, KLW\textsuperscript{+16}, KDW\textsuperscript{+17}, LLLS13, LLP\textsuperscript{+18}, LWS10, LIK\textsuperscript{+17}, LPdS10, LW13b, LZC14, LML\textsuperscript{+13}, MN12, MRT10, NACLR12, NCL13, Nos11, Nos14, RG10, RWZ13, RPS10, SES\textsuperscript{+16}, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZZ15, SA15, Sy10, TCS14, TLL12, Tso13, TKHK14, VN17, WWY121, WMZ12a, WMZ12b, WT10a, WT12, WQZ\textsuperscript{+13}, WX17, WX12, WX13, XCL13, XMHD13, YT11b, YC12, YZZ\textsuperscript{+14}, YHHS16]. \textbf{key} [YZL\textsuperscript{+18}, YLZ\textsuperscript{+16}, ZPZ\textsuperscript{+16}, ZWQ\textsuperscript{+11}, ZZ11, ZCC15, ZTZ16, ZXW\textsuperscript{+18}, ZXWA18, ZG10, ZCC15, Zy17b, ZWS\textsuperscript{+18}, ZHT16, CLW16, OHJ10, XJR\textsuperscript{+17}. \textbf{Key-Aggregate} [CCT\textsuperscript{+14}, PSM17, GLB\textsuperscript{+18}, CLW16]. \textbf{Key-Agreement} [WSS12, APK\textsuperscript{+18}].

\textbf{Key-Alternating} [BKLS12]. \textbf{Key-Based} [Xio12]. \textbf{key-correlations} [Sar14]. \textbf{key-delegation} [JSMG18]. \textbf{Key-Establishment} [BCO13]. \textbf{Key-Extraction} [GPT14]. \textbf{key-hash} [KKG14]. \textbf{Key-Insulated} [FZT13, LH11b, HL11, RG10, RWZ13, WWYZ11]. \textbf{Key-Length} [GT12]. \textbf{Key-Length-Based} [PNRC17]. \textbf{Key-Policy} [GZZ\textsuperscript{+13}, GSW\textsuperscript{+16}, HSY12, RVH\textsuperscript{+16}]. \textbf{Keyed} [MMS17b, YHHM18]. \textbf{Keyed-Function} [MMS17b]. \textbf{KEYing} [TW14, BCP11]. \textbf{Keyless} [PDMR12, ZXW\textsuperscript{+18}]. \textbf{keyrings} [MBB11].

\textbf{Keys} [ASN11, BF12, Bro17, CC10, HDWH12, MS16, PSM17, TW14, ZMW16, HL14, IK15, LLY15, LH13, LW10, LLL\textsuperscript{+18}, RWZ13]. \textbf{keystream} [SM11]. \textbf{Keystroke} [AaBT16, SP13, CTL12, LTC\textsuperscript{+15a}]. \textbf{Keyword} [CW\textsuperscript{+14}, Che15, HCDM12, WDCL18, XWS16, XJWW13, XZYL16, BL11, CLH\textsuperscript{+16}, FSGW12, GZS\textsuperscript{+18}, LUK\textsuperscript{+14}, OSSK16, SY15b, WHY\textsuperscript{+12}, WXLY16, XLY\textsuperscript{+18}, YZCT17]. \textbf{Keywords} [CWWL12, ZZ11]. \textbf{KGC} [YT11a]. \textbf{kid} [Tan17a]. \textbf{King} [ABJ13]. \textbf{kiss} [HU15, Ros11]. \textbf{KLEIN} [GNL12]. \textbf{Klepto} [XY18]. \textbf{Knacksnap} [Dun12a]. \textbf{Knebl} [Mur10]. \textbf{knocking} [KSB\textsuperscript{+17}]. \textbf{Know} [BC14, CAC14, XTK10]. \textbf{Knowledge} [CLP13a, COP14, GJO\textsuperscript{+13}, GOS12, IW14, MX13, MT12, OOR\textsuperscript{+14}, Pan14, TSH14, Ano11a, KPP16]. \textbf{Known} [DWWZ12, JHL12, SEHK12]. \textbf{Known-Key} [DWWZ12, SEHK12]. \textbf{Koblitz} [BJ10]. \textbf{Kode} [NN15]. \textbf{Korea} [LH10a, LW11a]. \textbf{KP} [FJHHJ12, HQZH14]. \textbf{KP-ABE} [FJHHJ12, HQZH14]. \textbf{Kristie} [Keb15]. \textbf{Kryptografie} [Blö12]. \textbf{Kryptographie} [Buc10]. \textbf{Kuala} [HWG10]. \textbf{Kurtosis} [YYO15].

L [Low12, Xie12]. \textbf{Labs} [Ven14]. \textbf{Labyrinth}

Large-Scale [DM15, JKH12, LQD+16, dCCSB+16, FXP12, GSN+16, SR10, ZZK17]. LARK [DS11]. Laser [DDR+16, FNP+15, Li12d].


Lattice [ADM12, Ano11b, AYS15, BSJ15, EM12, FGM10, HPO+15, HKR+18, LPO+17, MLO17, PG12, AAT16, Dra16].

Lattice-Based [ADM12, Ano11b, AYS15, BSJ15, EM12, HPO+15, HKR+18, LPO+17, MLO17, PG12, AAT16]. Lattices [Boy13, Lau17, TH16, XXZ12, ZQQ15, Krel13, Tia15, XUWZ16, yYqWzc13].


LBlock [KDH13, MNP12]. LDGM [BBC+13]. Leader [TKM12]. leak [BBG+17]. Leakage [AV12, BKKV10, CBL13, DHB16, FPS12, HHH+13, HHP17, IL15, LTZ16, NTKG17, NTY12, Pan14, SGH15, TTH15, Wan18, XZY+12, YZLC12, YZ12, YCZ12, ZYT13, ZWMT15, ZM16, ZZM17, ZY17a, ZY17b, ZYM18, CQX18, DLZ16a, DMW12, GV14a, GL1+18, YLZ+16, ZWM14, ZC15].

Leakage-Free [IL15, TTH15].

Leakage-Resilience [NTY12].


Leeds [vDKS11]. Left [BBG+17].

Left-to-right [BBG+17]. Legacy [CS12, Smi11b, CGH17]. Legal [ZTSR12].


Lessons [KMP+11, TGC16, WL11]. Level [AW17, Ano15a, BRPB13, BKJP12, COW+10, DAO10, Gli12, JW1+17, KPC+16, KG12, MV16a, ZLDC15, ABB13, MEFO12, RS17, UUN13, VS11, YT11a, BAI12].

Leveled [BVG14]. leveling [LY15].

Levels [HLCL11, LRW17]. Leveraging [DMS+16, HCM11, Mo11, SKG14].

Lewis [Mar10a]. Lexicographic [ZAC17]. LFSR [HLC12, MRT10]. LFSRs [GQL13].

Liability [Bra13]. Liars [Sch12b].

Libgcrypt [DK16, Bro17, Win17]. LibBrA [GMV17]. Library [ACZ16, Bec17, BLS12, FLW12]. Life [MK13, MeK10, MeK11, War11]. Lifecycle [Tan15a]. Lifting [LSL12b]. Light [JEA+15]. lightning [Ran10]. Lightweight [AMKA17, AAR12, BSS+13, BFMT16, BKL+13, BM11, CGCGPMG12, CPW12, CCF17, DS11, ESS12, EK+13, FQZF18, GNL12, GAI+18, GMV17, GMSV14, HZW18, HCETPL+12, IS12, IOM12, M1012, MFG16, MPM+17, PCDG14, She14, ZWY+13, AMN18, AAT18, Bor10, BBB16b, CL11, FLL+14, KDH15, LLZ+16, MCN+18, MNP12, MHV15, MHY+18, PJ18, PSoD+13, SGJ+18, Tan12b, TG17,
None provided.
ABBD13, GJ13, Gup15, LLZ+16, LHA+16, QMC17, RY10, TTL10, War11, WS14.
Machine-generated [AGHP14].
machine-to-machine [QMC17], Machines
[Ber16a, HB17, BBDL+17, KSU13, PWW10].
Macrakis [Keb15]. MacWilliams [ÖS11].
Made [Orn16, Sma16]. magic [FHN+12].
Magnetic [VDB+16], Magnifying
[DKL+16]. Main [AMH+16, LY15, CS11].
Maintaining [WP15]. Make [Ayu12].
makes [Kem11]. Making [BG14, dCCSB+16, Gel13, LA10, ZDW+16].
Malaysia [HWG10]. Malicious [AAE+14, BL15, TM18, VCAI15, BKI2b, WTT12].
malleability [KTT12]. Malleable
[CKLM13, MSas12, CG14a, FMNV14, LP11, MSas13, OOR+14, Pas13a]. Mallory
[FHM+12]. Malware
[ATS15, GAF+15, JC13, Goo12]. man
[And13, Bat10, Kap13, Moo14].
Management [ASM12, BS1b, CCFM12, CSL+14, GOP12, PK12, KKA14, Lop15b, MKF+16, PN10, TMGP13, Vle12, YZ+12, YSS14, ZJ11, ZTSR12, BMBS10, BB16b, CFL13, Cha13c, dCCS+12, dCCS+16, Din10, KH18, MLMSMG12, MGP10, PLCGS11, Sch11, SR10, SA15, SWW+16, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b]. Manager
[KKA15, Kim16]. Managing [MD15, BC18].
MANET [KTU16]. Manhattan [SS10c].
manipulation [OF12]. Mansour
[DKS12, LPS12]. Manual [Sac14]. Manuale
[Sac14]. Manuscript [Ana16d]. Many
[LB13, HR13, ZQWZ10]. Many-Core
[LB13]. many-to-one [ZQWZ10]. Map
[XYXYX11, ISC+16, LZY+16, LWK+18, PC14, SE18, ZT14]. map-based [LWK+18].
Maple [G+13]. Mapping
[CBL13, MS17, MM14a]. Mappings
[MC11, CDPLCA16]. MapReduce
[LJLC12]. Maps
[Ye14, BAAS13, KLW+16, LW10]. March
[Ano10, Cra12, DDS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, WZM12a]. Marche
[CCFM12]. Margaret [Led16, Sch15a]. Marian
[Kap13]. market [YWK10b].
marking [PJ18]. Markov [CR12]. Marotto
[SE18]. Marshall [Don14]. Martin
[ABJ13, Hof16]. Maryline [Ano15b].
Mashup [HTZR12]. Mashup-Providing
[HTZR12]. Masked [WH17]. Masking
[HF14b, PYM+13]. Mass
[BPR14a, BPR14b]. Masses [Ano15c].
Master [Dew11, Mar10a]. Matching
[Lin15, Tan12a, MR14c, MHT+13, PPTT15, SS17, YZL+18]. MathCW [Be17].
Mathematical
[Be17, FGPGP14, Ham17, IBM13a, Mei10, Sch15a, Wes16, KM14, O010, Sta11b].
Mathematical-Function [Be17]. Mathematician
[Ano17e]. mathematicians [Acz11]. Mathematics
[Ano17b, Ayu12, Led16, Sch15a, Ter11, CM13, Kra12, PHWM10, Wes16].
MATLAB [TRD11]. Matrices
[AMVZ12, BNA15, AGR13, FES10]. Matrix
[BFMT16, IAD10, SK12a, TDDTD13, Ye10, Chai3b, TK14]. Matter
[Rau15, SS12a, DKA+14]. Max
[And13]. Maximizing [DBPS12]. Maxims [Kob10].
May [BL10, FB12, Gil10, Sen10]. maze
[LLC10]. mbedTLS [YGS+17]. MC
[HIDFGP15]. MC-2D [HIDFGP15].
McClellane [DN12, GV14b, MBR15, MT12, MG15, ODT10, SWM+10, VOG15]. McOE
[FFL12]. MDPC [HC17, VOG15]. ME
[XHH12]. mean [TTL10]. Meaningful
[LTC+15b, SA16a]. Means
[KRDH13, AMH10, Kam16, Pal16].
Measure [DDD14]. Measure-independent [DDD14].
measurement [VGN14]. Measurements [DTE17]. measuring
[DMWS12]. Mechanism
[KD12b, LL15, Lin15, PKTK12, Saa12a, SMOP15, CL11, FXP12, PLPW13, PSJ+13, WB12, YXA+16, ZWM14]. Mechanisms
[JSK+17, FHH10a, KSA16, MMZ12,
PLGMCdF18. Media [KBL11, Fri10a].
Mediated [Fra16, YHK+10]. Medical [KBL11, UUN11, AIA+18, AMK12, KSA16, KLC+10]. Medicine [MA17, LWK+18].
MEDiSN [KLC+10]. Meet [LJ17, LWKP12, LWPF12, LWKP14].
Meet-in-the-Middle [LJ17, LWKP12, LWPF12, LWKP14].
meeting [Hof16]. Meets [RBHP15, BSR+14, MZA+13, PYH+18, SM13].
Members [YWZ+12]. Membership [FHR14].
Memory [AN17, ASBdS16, AMH+16, BKKV10, DLZ16a, DHLAW10, GKM16, GM13, Gue16, HT13, HF14b, LY15, TLCF16, BAB+13, CZ14, CS11, CVG+13, VCK+12, ZWT13].
Meshes [SGS14]. Meshram [PLPW13].
Message [ABS+12, DKPW12, HLLC11, Jia17, KHHH14, PSS+13, PPS12b, PA10, RWLL14, CMMM17, EEAZ13, Jia16, LC17, YMM13].
Message-Based [PPS12b]. Messages [Gen13, YLL+12, BMM12, KPS10, LCM+17, SA15].
Metamorphic [ATS15]. metering [WMYR16]. Meters [DM15]. Method [AGW15, Ara13, BBB+16a, FLH13, GLL5N12, GMNS15, HHS+15, LyWiZZ12, LP12, LD13, LBR12, MU12, OWHS12, PS14, SAA15, SY15a, SP15a, SZDL14, WZXL12, WZCC18, XNG+14, XNRG15, YYO15, AGLW16, AIA+18, CSS+13, Dra16, KHHH14, LLC10, LT13, LT14b, LPZJ15, MO14, PWW10, SI12, WT13, YWT+12].
Microsoft [Loe15]. Mid [AUMT16].
Mid-Air [AUMT16]. Middle [LJ17, LWKP12, LWPF12, LWKP14].
MiddleBox [FGR+17]. Midway [Car11]. Might [Hur16]. Migration [SHS12].
MIKEY [TW14]. Military [HK14]. Miller [Sch15a, LL11, LT14a, Led16, LR15].
Millionaire [GKS17]. Mind [WP15].
mines [KO16]. Minimal [ARH+18, BDH11, MZ17a]. Minimalism [DKS12]. Minimally [AAR12].
Minimizing [BCD+12]. Minimum [KHPP16, DZS+12]. Mining [BH15, BJL12, HDWH12, WZCC18, ZW15, Ano11a].
Minus [NXB13]. miracles [MR14c].
Misbehaving [TAKS10, ATK11]. Misson [Ano10].
Mitigation [BRS17, LGR14, DLJ+12]. miTLS [BFK16].
MitM [TY16b]. mix [WGT10]. mix-networks [WGJT10]. Mixed [ST16]. mmTMC [CML+18]. Mo [RBS+17]. Mobile [BCD+12, FD11, GPT12, GdM16, HvS12, HLKL15, KP12, KKA15, LH12, May15, NRZQ15, Sch15b, SFE10, She14, SAA12b, WPZM16, WT10b, XHH12, XNKG15, XHC+12, YHL16, Yon11, ZLDD12, Aia15, AZ+16, ALL+18, CLP+13b, CTL12, CCSW11, CTL13, uHAN+18, FHH10a, FA14b, FHZW18, GM16, GH16, HZWW17, HZW18, HL14, IB11, Kem11, KKA14, KKM+13, KKM+14, KKG14, KSB+17, LH13, OYHSB14, Par12b, hSZZ15, SSAF11, SKB+17, TKHK14, WT10a, YHM18,
mobile-cloud [KKM+13]. mobiles [GCSAddPi11]. Mobility
[CLH13, LNK+18a, CL11, GH16, LH11a, MYYR13, YLS12, ZX11]. Mode [HZ11, Mar10c, gWpNyY+14, WLC12, Fay16].
Model [AW17, App13, CT18, CLP13a, GLG12, GJO+13, GJJ15, GJZ17, HZX15, IA15, Kar12, KP17, LHM+15, LZC+12b, MVVR12, PYM+15, PNRC17, SFS14, SPM+13, TBCB15, WWC+11, WWHL12, XZY+12, Yon12, ZHL15, BL11, CK11, CDPLCA16, DFJ+17, HKT11, KSM13, LZC+12b, MVVR12, PYM+15, PNRC17, SFS14, SPM+13, TBCB15, WLC12, YLS12, ZX11].
Modified [IA15]. Model-Predictive [TBCB15]. Modelling [CJFH14, GBNM11, LTKP16, MKN13, PAS13b, Ana14, CDGC12, MHY+18].
Modern [Fri12, Ful10, RAWS15, KAS15]. Modes [GLLSN12, PC16, FAM+18, SKK10]. MODI [MBF+13]. Modification [LLSW16].
 modified [CTHP13, EEAZ13, MM14b]. Modular [Abe12, VN17]. modulation [KPB17]. Moduli [APPVP15]. Modulus [CNT12, LyWizz12, SEY14, KFL+10].
[ASS15, BBEPT14, BRT12, CWL+14, CHI12, GKV12, GJJ17, HYS11, HCL12, HRS16, IG11, KTT12, KMO14, LyWS10, MZHY15, MEFO12, MLBL12, NGAuHQ16, OKG+12, OSS16, SK12b, TWZ+12, TYY+17, Wan14, WOLP15, XWSW16, YWW10, Ye14, ZC13, ZQQ15, ZLDC15, BGG+13, CPPT18, CLP+13b, CFVP16, CG12b, CLH13, CW14a, C15b, DFJ+17, FHZW18, GMMGG15, GPVCdBO12, GZS+18, HL14, HL14, HCC11, HCL12, ISC+16, JCHS16, KM11, LWM12, LXY+14, LCT+14, LH13, LWY12, Mas17, QMC17, SCY15, SWW+16, SSS11, TLL12, WDL13, WXK+17, XZW16, YCC16, ZZKA17].
multi-agent [GPVCdBO12].
multi-criteria [ZZ17].
multi-crypto-processor [BGG+13]. Multi-domain [IG11, QMC17].
Multi-Proxy [ASS15, GJZ17].
multi-scale [CG12b], multi-scroll [GMOGCC15]. Multi-Secret [HYS11, ZC13, CW14a, HCCC11, HLC12].
Multi-Directional [WOLP15]. multi-server [CLHJ13, FHZW18, HL14, ISC+16, LXMW12, LH13, SSS11, TLL12].
Multi-Signature [ASS15]. multi-stage [Mas17]. Multi-target [HRS16]. multi-use [CZ15b].
Multi-User [MZHY15, OKG+12]. multibit [KPS10]. Multicast [CC14, BAL10, HWYW11, LTT10, NACLR12].
Multicoupon [HIDFGPC15]. Multidevice [DPCM16]. Multidimension [AJA16].
Multidimensional [Her10, WWBC14, HMCK12]. Multifactor [MMY12]. Multigigabit [PP10b].
Multihop [ADF12]. Multilayer [NXH+17]. Multilevel [FMS12b, HF14a, NSA15].
Multimedia [NSA15, PMZ13, PZPS15, PYM+15, WLY+15, ZW15, Zha15b, ZSA12, HM10, HWYW14, LLLK10, Wan13, XZW16, TW14].
Multimodal [GM16, Sar18a, AHM+18, ATI+10, MHT+13]. MultiObjective [ZÁC17]. Multi-partite [HR13].
Multiparty [BDOZ11, CCL+13, Fri10b, ADMM16, LDDAM12]. Multipath [LH12].
Multiple [DSB15, Dum12a, FR16, KBL11, LTB+15b, LQD+16, NDC+13, SY14, SC10, SKS+18, Sta12, WWL+14, GZS+18, LWZG10, LTC+15a, LZC17, MN14, RWZ13, TKHK14].
Multiple-Layered [WWL+14]. Multiple-Parameter [NDC+13]. multiple-precision [MN14].
Multiple-Secret [SC10]. Multiplication [AK14, CMO+16, HVI17, SK12b, YTS12, AAT16, SKH15, SF12]. multiplicative [KHIIH14]. Multipliers [ARM15].
[DP17, ST16, YL17, YDH+15]. multiwatermarking [WL12].
multiwavelet [PWW10]. Munich [Wat10]. Music [NTKG17, Wes16], musical [Ana14].
Mutt [Ran14]. Mutual [CJP12, GH12, GM14, Kim16, SBS+12, WT10b, AATM18, BDM18, CJP15, Cho14, CL11, FHH10a, Far14, GH16, HDPC13, IB11, JNUH17, KP18, KLW+16, LK+17, SPLHC14, TG17, XMHD13]. MVP [CD12]. mvSERS [HLKL15]. My [GPT14].
Naïve [ZLW+17]. Name [YCM+13]. Named [LLZ+17]. Names [ABJ13, MPJ+16].
NDSS [Ano10]. nearly [LVRY10]. nearly-neighbor [LVRY10]. nearly-neighbor [LVRY10].
Net [LFF12]. Nets [PS14]. Nets-based [PS14]. Network [Ano10, Bis17, CWL16, CJ13, CLH13, DRS16, Hay13, HDWH12, Kim15, KCC17, LH12, LCLL15, LY16, LTT11, MJGS12, NNAM10, NRZQ15, SGC16, She14, TL12, VKPI17, VFV17, VQA15, VKC15, WP15, YZLC12, YS1J14, AKM+11, AL15, Ano11a, AZF+12, QL11, DLK+16, FPBG14, HWG10, HB13, HKB14, JZS+10, KP18, LH11a, LKKL13, MZA+13, MJS13, NDNR13, OFF11, PL16, RCW15, Ser12, SCKH10, SKS+18, Sta11a, Tan15b, WYL13, WS14, YLS12, ZOSZ17, Ste15b].
Network-Assisted [KCC17]. network-based [YLS12].
Network-Coded [She14].
Network-on-Chip [Bis17]. Networking [LCK11, LLZ+17, ZHL15, Kim11, LC+17].
Networks

Number [ADI11, BKLS12, CDK+10, DSLB18, Fok12, Ham17, LTKP16, LCLW17, MFG16, NIS12, NNAM10, Sha10, SRAA17, SRK+17, CFY+10, CP13, LLP+18, LGKY10, Lim11, MS12a, MRT10, SH11, Sti11, XSWC10].


O [CDD13]. Obfuscated [LMS16, OWHS12, ZM16]. Obfuscating [BGI+10, BGI+12]. Obfuscation [ABCL17, AS16, AWSS17, BBC+14, BCP14b, BR14, CZ15b, DRS16, EMW14, FKOV15, GGHR14, GG+16a, GGH+17, MH14, BBGT12, CFVP16, GG+16b, OOSK16].

Obfuscation-Based [ABC17]. Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17]. Objects [ZCWS15, HST14, SMBA10, WW13].


October [CGB+10, IE10, IEE11b].


Old [Che17, GY13]. on-chip [BAB+13].

On-Line [FFL12]. On-siteDriverID [SGGCR+16]. On-the-fly [PS14]. One [CPS16, DSMM14, DCAT12, FD11, HP14, HG12, Mat14, NA10a, PC16, TYM+17, XW12, XYXYX11, XZLW15, Yon12, BM15, FHH10a, HRV10, LP11, LW10, LW13b, LML+13, RK11, Rus15, SM10a, TCS14, ZQWZ10]. One-Dimensional [XYXYX11].

One-Round [TYM+17, XZLW15, Yon12, XW12, TCS14].

One-Sided [HP14]. One-Time [NA10a, DCAT12, BM15, FHH10a, LW10, LW13b, LML+13]. One-Time-Password [FD11]. One-Way [CPS16, DSMM14, Mat14, HRV10, LP11, RK11]. Onion [KZG10]. Online [BPSD17, JMG+16, KSD+17, PSM17, SKGY14, SZT18, WXY+17, ZHL15, CCG10, HYF18, KV+E18, LKAT12, LJW+17, MSM+18b, SSK+18, SYW17].


Openings [SP13]. openness [Bia12].


Opportunities [Lau17, Mic10b]. opportunity [Sch11]. Optimal [AS17, DSSDW14, HRB13, PDNH15, PPS12b, Cha13a, DDD14, PPT15]. Optimality [MM17, SDM+12]. Optimally-Fair [DSMM14, GT12].
[DSMM14]. Optimised [CMO+16]. Optimising [EVP10]. Optimistic
[WSA15, SEXY18]. Optimization
[WH17, ZÁC17, FLZ+12, GCSAdP11, KHF10, PTK14, RYF+13, ZSM18].
Optimized [AYS15, EKB+16, HGT15, MBF+13, MBR15]. Optimizing
[DWZ18, ZSM18]. Optimum
[Oba11, YFF12]. Optional [PC16]. OR-Proof [FSX12c]. Oracle
[GLM+16, HKT11]. Oracles
[FZT14, FSX12a, GSW+16, QXL11, YS12, YKC+11, YLA+13, ZYM18, LLY15, RG10,
SYL13, WWYY11, YFK+12]. Order
[KS12, LWKP12, PRC12, YKKL12, ZDL12, ZSW+12, AKY13, LW13a, LCY+16,
LWK14, gWpNyY+14, YL11]. Order-Preserving [KS12, YKKL12, YL11]. organisation [Smi15a]. Organization
[RSGG15]. Orientated [TJZF12]. Oriented [NNAM10, Rog16, RSGG15,
WW12, WZM12a, WZM12b]. Orthogonal [tWmC12]. Oscillator [YKBS10]. OSN
[BCF16]. OSNs [SZZT18, PZPS15]. other [Smi15b]. OTS [Hül13]. outliers [Sch12b].
Outlive [Hur16]. Output
[DK16, GST12, NR12, PBCC14]. Outright
[ABJ13]. Outsourceable [QZZ18]. Outsourced
[FRS+16, LLC+15, LHL+18, QLD+16, PD14, RDZ+16, YMA17, YMC+17, DFJ+10,
FS18, HMCK12, LCL+15, LCY+16, LJW+17, QZDJ16, ZML17, ZSW+18b].
Outsourcing [DR12, JLJC12, LHL+14, LJYW18, SKB+17, SWW+16]. outwitted
[Car11, Fag17]. over-the-air [ZWX+18].
Overcoming [BKKV10, DY13]. Overhead
[AWSS17, Bai10, CCW+10, GHS12, ZJ11, RS17]. Overlay
[CHS15, MJS13]. Oversight
[Bla16]. overview
[AA14, BDP+12]. own [Zha15a]. owners [GZS+18]. Ownership
[FMTR12, RR11, HWYW14, KH18]. Oxford
[Che11, Wes16]. Ozarow [ADG16]. P2P [dCCSM+12]. Packet
[FRG+17, JTZ+16, VKP17, XHC+12, MV16b, PJ18, PX13, XWDN12]. Packets
[Bis17]. Pads [NA10a, BM15]. Paillier
[Lin15]. Pairing
[Bon12, CWWL12, CST+17, KZG10, HKPP16, LGPRH14, YTS12, Con12,
KSH18, LL16a, LR15, YT11b, ZY17b]. Pairing-Based
[Bon12, CST+17, KZG10, LGPRH14, YTS12, Con12, KSH18].
pairing-free [LL16a, YT11b]. Pairings
[ASS15, Hof15, IL15, LT14a, QYW16, RS15, UK18]. pairs [MCP15]. Pairwise
[DL12, YM16]. Palash [Kat13]. Palm
[IEE11b]. Pan [GOPB12]. Pan-European
[GOPB12]. Paper
[TSH17, Ano16g, SK14, YFK+12]. Papers
[Ano16a, Ano16b, Ano16h, LW13a, LW13, DSS12, Dan12, MV12, BYL10, YJ14,
LH10a, vDKS11]. Paradigm
[ABGR13, BSV12, Man12, MP12, WQZ+13]. Parallel
[App14, ARM15, CGB+10, GP17, LY16, LB13, MCDB12, MC11, NdMMW16,
SMDS11, YE12, CSTR16, MRT10, RG10, RWZ13, WWYZ11]. Parameter
[NDC+13]. Parameters
[HRB13, MBF18]. parametric
[Bul10a]. Paranoia
[Cor14a]. Park
[Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, McK11, McK12, Pea11, Smi11a,
Smi15b, Smi15a, Bai12]. part [VM14].
Partial
[DLV16, GFBF12, LG12, SGS14, WDDW12, Bax14]. Partially
[KB10]. participants
[KSU13, WTT12]. participating
[CH10]. particle [ZSM18]. Parties
[YCR16, Kup13]. Partitioned
[FVS17]. Partitioning [ADR18, AP11].
Party
[Ash14, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, QZL+16b, TYM+17, ZM16, ED19,
FIO15, GVV12, HFC12, LyWSZ10, LML+13, Tso13, TKHK14, XLWZ16,
XCL13, YC12, YZZ+14, ZC15, GHKL11].
Passau [GLIC10]. PASSERINE [Saa12a].
Passion [Hof15]. Passive [DHB16, GSC17, SB17, BM13, uHAN+18, LRLW11, MK12a].

Password [LZJX10].

[ASBdS16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZXH16, ABK13, AKC18, CTL12, DSCS12, FA14a, FIO15, FHV16, HCC10, IOV+18, LWS10, LNKL13, MM12, MoV11, Ts013, TKHK14, WZM12a, WZM12b, YC12, ZXWA18].

Passport-Authenticated [HCL+14, YRT+16, ZXH16, LWS10, WZM12a, WZM12b].

Password-Only [YLW13].

[BBvOS15, LCL17b, BCV12, Che13].

Past [Bon12].

Patchwork [NXH+17, XNG+14].

Patchwork-Based [NXH+17, XNG+14].

Path [DM+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13].

Patient [ZLDC15, ZVG16].

Patient-Centric [ZVG16].

pattern [ATKH+17, uHAN+18, KPS10, OSSK16, PPTT15].

Patterns [An16e, BPSD17, TSH17, WOLP15, BDK11].

PAWN [JNUH17].

Payload [CHW12, AZH11, JNUH17].

Payload-based [JNUH17].

Payment [DG15, SYC+17, SYW17].

Payments [RBHP15, MPJ+16, PC [YE12]].

PC-Based [YE12], PCIe [IBM13b], PCM [LY15].

PC-based [LY15], PCP [MX13].

PCs [GPT14, GPP+16], PDGC [CGB+10].

Peaks [TC10], pearl [Rus15].

Pecherskii [Kuz11], peer [NCCG13, ZWY+13], peer-to-peer [NCCG13, ZWY+13].

Per-File [DMS+16].

Perceived [CSW12], perceptual [MK11].

PEREA [ATK11].

Perfect [Pas13a, Sch13, C15a, FHKP17, LLC10, Lew10, XW12].

perfectly [ADG16].

Performance [Alo12, AW12, AB15, CGL+12, CCG10, DLK+16, DBPS12, EGG+12, ERI14, FPBG14, GLG12, GCS+13, HKL+14, KAK18, LCK11, LPO+17, MHC12, SKV12, TPKT12, WDDW12, Xio12, ZLDD12, ABDP15, GCVR17, MMS+17a, MS13c].

Perform [Ano17d], perimeter [Cal13].

periodic [KPS10], periodical [CLSW15].

Permission [VN16].

Permutation [LJ16, GMSW14, LGK14].

permutation-based [LK14].

Permutations [AR+18, BKL12, Mat14].

Persistent [CSY18, TYK+12, ALL+18, PAK15].

person [PN10], person-centric [PN10].

Personal [ESS15, LYZ+13, Rao17, ALL+18, BC18, MoV11, LHL15].

Personalized [FRS+16, AT10].

Personnel [YTH17].

Perspective [KMY18, MSM18a, RSGG15, Sir16, Wag16, JW14, Suc12, ZWT13].

Perspectives [Sen17, SPM+13].

Pervasive [ACAT+15, BCG+12b, YD17, JSM+18, PAK15, SCY15, TAN12b, YWK+10a].

Petri [PS14].

PGP [RAZ15].

Phase [LD13, NBZP17, ZWT13, ZHH+17].

Phase-change [ZWT13].

Phase-Encrypted [NBZP17].

Phone [MUR16, SAA12b, KRM+10, LTO+15a].

photo [OF12].

Photographic [YSC+15].

photos [Pow14], Phrases [WBC+10].

Physical [GPT14, GPP+16, HH+13], SMOP15, HQY+16, HZW18, KSA16, QMC17, VCK+12, WW13, YD17, ZHH+17].

physical-layer [HQY+16, ZHH+17], physio [HT11], physio-behavioral [HT11].

Pi-Calculus [MR10].

Pi-Calculus- [MR10].

Pi-Calculus- [MR10].

PICADOR [PRC12].

Piccolo [IS12, JEO13], picture [SM13], piecewise [GMOGCC15], PIN [MDAB10], Pinch [DP10], PinMe [MDMJ17], Pinocchio [PHGR16], pioneer [Men13], Pioneers [ORM16], Pipelineable [BDML16].

Pipelined [HZ11, KB10, NDMMM16].

Pipher [ME10].

Pixel [DA10, LLL17, LWIIZZ12, Lin15, LTO+15b, SSA13, YWW10].

Pixel-Value [YWW10].
Pixel-Wise [SSA13]. Pixels [PDMR12, Tan12a]. PKC [FBM12].
PKCS#11 [CFL13]. PKDS [HLCL11, HLYS14]. PKE [HTC15].
PKE-AET [HTC15]. PKI [Dav11, YC16]. PKIs [KGO10]. PKZIP [JLH12].
plain [LW13b]. Plaintext [BM15, JLH12, MSas12, MSas13].
Plaintexts [YKKL12]. Plane [YLL12]. Platform [YE12, ABF14, NCCG13].
Platforms [HTZR12, LMS16, SOG15, LT14b]. Plausibility [KD12b].
Plays [Shp10, VGN14]. Player [GJO13]. Pless [Ayu12].
plugged [PP11]. POB [SRAA17]. Podolsky [HR13].
Poisoning [HLAZ15, YC13]. Polar [YWNW15, PGLL10].
policies [Cra11, DFJ10, LHM14]. Policy [GZZ13, GSW16, ISMY12, MK12b].
RVH16, Rao17, SVG16, XMLC13, XWL16, ZHW15, FSGW11, FS18, HZL18, HKHK13, JSMG18, LFW15, LJW18, QRW18, TY16a, XWS17, LAL15, LHL15].
Polylog [GHS12]. Polynomial [Ano11b, BGJT14, DWZ18, ERRMG15, FS15, HV17, NKWF14, WSS12, ZM16, AAT16, BGJT13, Bul10a, Bul10a].
Polynomial-Advantage [WSS12]. Polynomials [CMLRH13, SS12b, TWZ11, LP10].
Position [BCF14, CGMO14, MS17, YXA18]. Position-Based [BCF14, CGMO14]. Possession [EKB16, ZPXX17, SYY17].
possibility [BGI10, BGI12]. Possible [BF12, Fra15, Orm16]. Post [LLK18, MKAA17, Y17, ZCC15, YDH15, Sen10, Yan11].
Potential [Cil11, VS16, ZW15]. Power [ARP12, AS16, HHR11, MMP14, MD12b, MAS16, MS17, SAJL16, SDM12, TQL14, WT10b, YAM15, ZH15, ZJ11, FAA18, LGKY10, LKT12, QG13, RITF11].
POWER7 [BAB13]. Powered [SFE10].
PQCrypto [Sen10, Yan11]. Practical [ATK11, BHH15, BDH11, CLSW12, CG17, Cra11, DZY10, EA12, FPS12, FSK10, HSA14, HOP15, HKR18, LW16, LJWY18, MBF18, PPTT15, RWZ13, TSH17, WHL16, XW13, YZL12, ZYD10, ZLW17, AMS10, BS13a, CFN14, JSK16, LFZ17, PHGR16, WR15, YK13, ZSW18a].
PRECISE [HYF18]. precision [MN14, SK12b]. Precomputation [GKM16]. Predicate [KHPP16, NMS14, YKNS12, ZYT13, FH13, HFT16].
preserve [BAG12]. preserved [SWW+17].
Preserving [ABCL17, BJL16, BHKN13, BJL12, CWL+14, CRE+12, GZZ+13, HSMY12, HLLC11, HXC+11, HHMK14, KS12, LMGC17, LNXY15, LQD+16, NSMS14, OFMR16, PR12, PD14, PSS+13, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, SZQ+17, SZZT18, WPZM16, WZCC18, YKKL12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AIB+16, ALL+18, BLV17, FH13, FMA+18, GH16, GAI+18, GA11, HSH11, IC17, IOV+18, JKL+16, KH18, LHL+18, LW13a, LCY+16, FZBF18, SYY+17, Tan12b, TSH14, WLZ+16, YMM13, YNX+16, YL11, ZYW+13, ZOS17].
PRIME [ACK+10, GM13]. Primitive [App15, MCS+15]. Primitives [BSJ15, EAA12, HLN+10, SP15b, ABDP15, BSR+14, Gor10]. PRINCE [BCG+12b].
Princeton [Ano17b]. principle [WW14].
Principles [DK15, FSK10, Fri10a, Sta11a]. print [KPS10, PKS18]. print-cam [PKS18].
print-scan [KPS10]. Printer [EMW14, FNP+15]. Prior [NA10a].
Priority [LMS16, Bia12]. Prisoners [Mac14, Keb15]. Privacy [AKM+11, ABCL17, ALL+18, ACM12, AIBC+16, BN14, BCF16, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DTE17, ESS15, FGR+17, GZZ+13, HSMY12, HBCC13, HXC+11, JN12, KM10b, KCC17, KS12, KH18, LMGC17, LSNB14, LLG15, LNXY15, LQD+16, MYYR13, NSMS14, PD14, PSS+13, PPRT12, PZPS15, PSD15, Pet12, RVH+16, RWLL14, RBHP15, SS17, Set16, SZDL14, SZZT18, SOF12, TMLS12, TMGP13, WPZM16, WZCC18, WMYR16, YMM13, Yon11, ZHW+16, ZM16, ZOS17, ZHW15, ZLDC15, ZHL15, ZTL15, ACK+10, BP11, BAG12, CDF+10, DZS+12, FH13, FMA+18, GAI+18, HSH11, IC17, IOV+18, JSK+16, Kam16, KKGK10, KM14, LHL+18, MZA+13, MGP10, PX13, PZBF18, Sav16, Sch11, SLZ12, SYY+17, SCY15, SWW+17, Tan12b, WLZ+16, WWW17, WS13, YYS+16, YXA+18, YNX+16, ZWY+13].
Privacy-assured [WMYR16]. Privacy-Aware [BCF16, MGP10]. Privacy-Based [BS13b].
privacy-preserved [SWW+17]. Privacy-Preserving [ABCL17, BJL16, BJL12, CWL+14, GZZ+13, HSMY12, LMGC17, LNXY15, LQD+16, NSMS14, PD14, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, SZZT18, WPZM16, WZCC18, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, ALL+18, BLV17, FMA+18, GAI+18, HSH11, LHL+18, PZBF18, SYY+17, Tan12b, ZWY+13].
Private [GM13, Jia14a, QZL+16b, Sia12, WCL+18, Yek10, ZMW16, ZXYL16, HJM+11, HYF18, IK15, WR15].
private-keys [IK15]. Privilege [Cha13c, QRW+18]. Privileged [Din10, WDZL13]. PRNG [DK16].
Proactive [SLL10, WMYR16].
Probabilistic [BFG+14, Rao10, WP17, KSU13].
Problems [CJS17, Fra15, GTT11, KRDH13, KPC+11, RBS+17, SK14, TPL16, WS14].
Procedure
Proceedings [LCK11, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che1, Cra12, Dun12b, FBM12, GII10, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLC10, IEE11a, Kia11, Lin14b, Sah13].

Processing [SAKM16, TPK17, BHK13, HWK+15, MS13b, PRZ12, WS14].

Processor [BH15, CLF+17, HKL+14, LB13, MBR15, YS15, ABP15, BAB+13, BGG+13, KSH18, SSPL+13, Tar10].

Processors [GFBF12, Gue16, RYF+13].

Product [ADM12, CCM+15, OT12, YKNS12, Cha13b, DDM17].

Products [LMG+18, RS10].

Professional [STC11].

Profiles [BCF16].

Profiling [DP12].

Program [MZ17b, Wall18, CLZ+17, GGH+16b, MFH13].

Programmable [CLF+17].

Programming [Bee17, BCC15, SY14, ASVE13, HLV10].

Programs [BGI+10, BGI+12, CL16].

Progress [AB10a, BL10, BC11, GG10].

Progressive [SA16a].

Project [ACK+10, SS10c, Wil8].

Projective [CZ15a].

Prominent [AB13].

Promise [Pau10, PWVT12].

Promised [HS11].

Proof [BDSG+13, Bia12, CLZC12a, CLZC14, FSX12c, Kuz11, LW12, NLY15, SR14, Ste15a, ZZM17, Mon13, PPTT15, WH17].

Proofs [BGK12, BCG12, BGB12, BCI+13, BSDG+13, CLZC12b, IW14, LN13+13, Mau12, NTY12, SAV13b, WPZM16, AGHP14, KPP16, KKK+16, Lii10].

Propagate [GWM16].

Propagation [SKS+18, WWC+11, YZL12].

Properties [CCK12, CCCK16, DQFL12, FY11, JR13, KU12, Sch12c, CLCZ10, WT13].

Property [HEC+12, PR12, Rja12].

Proportions [Ber12].

Propose [BFMT16].

Proposed [Bax14].

Protect [CTC+15, YM+17, BV1B12, CDF+10, dCCSM+12].

Protected [BDGH15, SG15].

Protecting [BCP14a, GSFT16, Mar10b, SCY15, Wat14b, ATK+17, CDA14].

Protection [CDD13, GST12, Lop12, NGAuHQ16, NDG+17, RR11, SEY14, SJ12, AT1+10, HLYS14, KKM+13, LVR10, RS17, TLL13, YWT+12].

proof-key [HLYS14].

Protocol [BL12, BC14, BCM+15, BSSV12, BFK16, CC14, CC17, FLH13, FMT12, Fra16, GL12, HvS12, HC12, HL10a, HCP12, HLT+12, JZ+16, KMO14, LNZ+13, CC1J13, LNY15, MBC15, MR10, PSS+13, SBS+12, SCG16, TYK+12, WT10b, XJ+17, YS12, YWZ+12, ZX+11, AATM18, AKG13, AIB+16, AIC18, AN15, BDM18, BGAD12, CSD18, CCSV11, CJP15, DLI+16, EA12, FA14b, FIO15, GMSW14, GLM+11, HLP12, IC14, IOV18, JKL+16, JXLZ15, Kim11, KO16, LLL13, LDDAM12, LKK13, IWS10, LXMW12, LEW19, LY+14, LML+13, NLC13, NLYZ12, OHJ10, Par12b, SPLL1B14, SB17, SGJ+18, SWW+16, SSS11, SSPL+13, TG17, Tso13, TKHK14, VS11, WCFW18, WZM12a, WZM12b, WMY16, WT10a, WTT12, WCCH18, XCL13, YC12, YZZ+14, YMM13, ZWQ+11, ZT16, ZYC+17, ZXC+18, ZXW18, ZG10, ZZC15, ZX11, BOB13, CJP12, LFGCGCRP14, Ste15b].

Protocols [AP13, ABHC+16, BPP12, CCK12, CCCK16, CCF17, CCI15, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLL11, HL10b, KOS16, LY16, MS16, MT12, Mur16, NVR+14, NSMS14, PS14, SBS+12, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Anol13b, ACM12, CML+18, CR10, CLCZ10, DGJN14, FTV+10, GBNM11, GLR13, HSH11, Ham12, HDPC13, HZWW17, HST14, KIN+16, KSU13, KKK+16, LKK113, MN10, NR11, Nos11, Nos14, SD10, YSL+10].

Prototyping [KPC+16].

Provable [BKLS12, CC14, EK+16, Rog16, YMSH10, ZKX11, ZPXX17, FA14a, HRS13, LHH11, WB12, XCL13].

Provably [BCGAPM12, BCM12, BCM13, BHP14, FHH10a].
Quantitative
[BL15, MLBL12, MV16b, HM10].
Quantization [SSA13].
Quantization-Based [SSA13]. Quantum
[Ano15d, Ano16c, Ano17d, Ano17e, BB14, Ber14, BCF+14, Che17, CCL+13, Feh10, FKS+13, Fol16, JEA+15, Kar12, KP10, LK18, LHA+16, MS16, MSU13, MKAA17, NNA10, NA10b, QGX18, RK11, RSM15, Sti11, TKM12, Unr15, WCL+18, Y+17, ZWS+18, ABB+14, BJ16, CML16, Edw17, FRT13, GJMP15, IM14, JSEK+16, KKK+16, LLP+18, LyWSZ10, LCW+16, Lid12, QD16, SK14, Swy14, YDH+15, vDKS11, Sen10, Yan11].
Quantum-Oblivious-Key-Transfer-Based [WCL+18].
Quasi [BGJT14, OWHS12, OTD10, BGJT13].
Quasi-Chirp [OWHS12].
Quasi-Cyclic [OTD10].
Quasi-Polynomial [BGJT14, BGJT13].
Quaternion [YWNW15, yWpWyYpN13].
Queries [HLW12, LHKR10, BKV13, CHX13, DFJ+17, HMCK12, PRZB12, TKM13].
Query [GA11, PCDG14, WCL+18, AZPC14, BS13a, CH11, ED17, HWK+15, JCHS16, LK+14, LW13a, ZHT+16].
Query-preserving [GA11].
Quest [Fox13].
question [Cha13b].
Quisquater [Nac12].
Quorum [Kar12].
R [BS12, LCV11, PP10b, WYW14].
R3579X [BDK11].
Rabbit [FSWF11].
Rabin [Cha13a].
Radial [pNyWY+14, CG12b].
Radio [KAHK17, CJP12, CJP15, EA12, Kim11, NLYZ12, RPF12].
radio-frequency [CJP12, CJP15].
radix [GKCK11].
Rail [HF14b].
Raising [YWW10].
RAKAPOSHI [IOM12].
RAM [RYF+13].
Ramanujan [KK10].
Ramifications [ALR13].
Random [Ana14, CDK+10, DSLB18, EAA+16, FZT14, FSX12a, GSW+16, Gre17, KS15, LTKP16, LPL15, NIS12, NNAM10, NN12, SC10, SRK+17, TM18, WS12, XXYYX+11, XQL11, Y16, YS12, YKC+11, YFK+12, YLA+13, ZYM18, Ara13, CFY+10, CT11b, GLM+16, GLV13, HKT11, KM10a, LGKY10, LLY15, MRT10, MG15, PLSevDE10, RG10, SMDS11, SYL13, SH11, SM11, SHy15, Sti11, WYXY11, XSWC10, ZOC10, ZPZ+16, Zim10].
Random-Grid [KS15].
Randomization [Gas13].
Randomized [ARP12, GT12, HHR11, SR12b, BWA13].
Randomness [AY14a, Ana14, ABF12, ACM+17, BWLA16, MS10, MS16, DTFZ12, FRT13, RY10, TC11].
range [HMCK12, JCHS16].
Rank [SS10b, FES10].
Ranked [CW+14, WSXY+16, GZS+18, LK+14].
Ranking [ZDL12, AT10].
Rapid [KPC+16].
rare [Sch11].
RASP [AZPC14].
RASP-QS [AZPC14].
Rate [LJIK17, PPS12b, PCPK14].
Ratio [FHKP17].
Rational [KN14, KOTY17, NS12, TW11, ZC13].
Rationality [GLR10, GLR13].
RBAC [AN16].
RC4 [GCS+13, Loe15, Reel15, RS14, Sar14].
RC4-like [RS14].
Re [ABR12, GSW+16, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PRSV17, WY10, BGG+17, CFZ+10, CLH+16, CZ5b, FSGW11, FSGW12, FXP12, GH12, HDWL16, HY18, KKM+14, LMC11, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGJT10, WHY+12, Wan18, XXX15, YZCT17, ZDW+16, LAL+15, XJW+16].
Re-authentication [BS12, FXP12, LMC11].
Re-Encryption [GWS+16, KKA15, LSLW15, MLO17, NAL17, PRSV17, ABR12, LSC12, Pet12, WY10, BGG+17, CFZ+10, CLH+16, CZ5b, FSGW11, FSGW12, GH12, HDWL16, HY18, KKM+14, LMC11, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGJT10, WHY+12, Wan18, XXX15, YZCT17, ZDW+16, LAL+15, XJW+16].
Secrecy
[ABD+15, BKST18, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCW15, TCS14].

Secrecy-preserving [TSH14]. Secure
[ASN11, ASN12, ADH17, AYU12, BAI10, BBD+16a, BFMI12, BBEP14, BRI11, CCM+15, CFOR12, CCL+13, DR12, DEW11, EM12, EA11, FHK17, FR16, FK12, HYS11, HL10a, JLS12, KU14, KS18, KOTY17, KK12, KK13, KSSY12, KS15, LH12, LPL15, LIN15, LCC13, LTC+15b, LJ16, Men13, MNS11, NS12, Ob11, PCPK14, QS18, SLL10, SC10, SS10c, SSU12, S16, TL12, TWZ11, WKB16, WGF16, Wikimedia, XZY12, XJR+17, YFF12, YWZ+12, ZC13, AK11, ADG16, AKK+17, ARA13, BJ16, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEA13, EZ15, FHH10a, GMP15, GLW13, HF14a, HH15, Hea15, HBB16, HCC11, HLC12, KI11, KT11, LX12, LT13, LyWS10, LHY12, LE19, M17, MC10, MK11, MC12, MBB11, OOI10, PEA11, PET11, QD16, Rus15, SB17, SA12, SAR18b, TQL+14, TD14, UUN11, UUN13, WYL13, WZ11].

Secret [WS12, WOLS12, Wu17, XW13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPY12, LSC+15, Bai12]. secret-key [BJ16]. Secret-Sharing [BBEP14].

Secretocracy [Ber16b]. Secrets
[BT12, CG14b, DLW11, FMS12a, KOB10, Man13, Bha16, Cop10b, GGH+16b, Gup15, HRS13, SN11a, Arou17]. Secure
[ADMM16, AARJ12, Ash14, AMH+16, BVS+13, BWL16, BCH11, BG12a, BCQ+13, BWA13, BJ12, BHJ14, BF11, BR12, BDH11, BIB15, CFOR12, CCM17, CZC12, CLC14, CH15, CMA14, DM18, DL15, DMS+16, DG15, DLZ+16b, Edw17, FLH13, Fri10b, FD11, FSX12a, zGX12, GKM16, GGH14, GBF12, GT12, GY14b, GHKL11, GM14, GZ+18, HvS12, HS14, Har16, HL10b, HP14, HTZR12, HMK12, HLKL15, HYS18, HK14, IL15, Jac16, KW14, KME+12, Kip15, KHD10, LJS+14, LL15, LH12, LZ+13, LTH+15, LTZ16, LSL15, LLG16, LY15, LHL15, LLML12, LSC12, MLO17, MPM14, Mll13, MVVR12, MNS17b, MK12a, MKAA17, NBZ17, NDG+17, NR12, NMS14, NSMS14, PB12, PSM17, PT13, QZL+16b, QZDJ16, QZ18, RM10, Rea16, RSGG15, SN11, SZ14, SSV15, SP15b, SSKH17, SRA17, SRA17b, SSAF11, SYG16, SYW17, SYC+14, SMS14]. Secure
[SZDL14, SGH15, SLY+16, SR12b, TCL15, TWZ11, TG12, TGC16, VM15, WgMW12, WKB16, WLY16, WLY17, WDC18, WH15, WBA17, WWH12, WMS+12, tWN12, XWS16, XJW13, YN13b, YN13b, YTH17, YHK+10, YKC11, YAM+15, YGD+17, ZZ15, ZDL12, ZVG16, ZHT16, ZLW+17, ZBR11, AHS14, APK+18, ABB13, ACF16, AKK+17, ACD+15, BOB13, BSR+14, CCLL11, CSD18, CLH13J, CW14a, CS11, CDL18, FHH10a, PLL+14, FSG12, FA14b, FIO15, FS18, Gal13, GAI18, GLL18, GCH15, HG14, HWK15, HLS14, HPY10, IB11, JZS+10, KPP16, KAA14, KRM+10, KTU16, KD+17, LLS13, LDM12, LH11a, LLIW16, LSR13, LWX+18, LCT+14, LAL+15, LL16a, LL16b, LBOX12, MR14c, MHY+18, NR17, NAACL12, NAL17, PSO13, PLSE10, Rao17, RG10, RYF+13, RITF+11, RS15, SGGCR+16, SYL13, SWW+16, SSS11, SSPL+13, SX16, Tar10, TLMM13, TLL12, VS11, WLZ+16, WMX+17, WCC18, WXW14, XXX15].
secure [YCI12, yYqWZC13, YZZ+14, YZCT17, YY11, YSL12, YMHS10, ZLY10, ZC11L4, ZZ15, ZYC+17, ZG10, ZZ12, ZXL11, ZY17b, ZC12, ZHI13, ZSW+18b, Aro12, DSLB18, OKG12, YSS14, YZK+12]. Secure-TWS [OKG12]. Secured [LC17]. Securely [CC10, KP17, LHL+14, MS16, WXY+17, BC18, der10]. Securing [BK12b, CML15, CST+17, NPH+14, PMZ13].
SFE10, SLI11, Ste15b, TKR14, YMA17, YT12, CR10, Din10, SKS+18, SA15, Tox14].

**Securities** [WWL+14].  **Security**

[ABJ13, ASBdS16, Ano13d, Ano15a, Ano15d, ABF12, AN15, ABHC+16, AYS15, BCE+10, BCM+15, BRT12, BPR14a, BPR14b, BLS12, BCGN16, BDPS12, Bra15, BDI11, BP10, CFST17, CFE16, CHS11, CFXY17, CCD15, CPS16, CM11, DDS12, Dan12, DR12, DFKC17, FMA+18, FSX12b, FSX12c, GZZ+13, GSC17, HC12, Hel17, HB17, HLW12, HXC+11, HLCL11, HLT+15, HLN+10, IS12, IGR+16, JN12, Jia14a, KBL11, KS18, KFOS12, KSD+17, KD12b, LPS12, LST12, LW11a, LC14, LW12, LLZ+17, LTW11, LP12, LRLW17, LZC12a, LDB+15, LMS16, LLH18, MTY11, MKN13, MCS+15, MA12, MV16a, MLBL12, MPM+17, Nac12, NNAM10, NDG+17, NVM+17, Nos11, Nos14, Orm16, OS16, Pas13a, PZPS15, PDNH15, PS14, PL16, PDT12, PNRC17, QLD+15, RWZ12, Rog16, RS10, SN10, SNJ11, SBS+12, Sar12, Sch13].

**Security-Aware** [LMS16].  **security-enhanced** [AMN18].  **security-modified** [MM14b].  **SEDURA** [LY15].  **Seed** [AS17, LYHH14, Sun11].  **seeing** [Tox14].  **seen** [Goo12].  **Segment** [WOLP15].  **Segmentation** [LYW+13, ZZCJ14].  **selectable** [GLM+11].  **Selected** [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12].  **Selection** [KD12a, RP12, SEY14, FXP12].  **Selective** [BTHJ12, GDCC16, LW12, LSC+15, LZC12a, LLH18, LZC14, LW13c].  **Selective-Opening** [LLH18].  **Self** [CCL16, CHHW12, CSV15, DM18, HZ11, LCL+17a, LH12, LHM14, SAA15, SM12, WHZ12, XWX14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11].  **Self-adaptive** [LHM14, FXP12, SH11].  **Self-Certified** [CCL16, XWX14, HL14, LH13].  **self-composition** [AGH+17].  **Self-Controllable** [ZLDC15].  **Self-Identifying** [CSV15].  **Self-Recovery** [SAA15, CHHW12].  **Self-restoration** [WHZ12].  **Self-Synchronized** [DM18].  **Self-Synchronizing** [HZ11].  **Self-updatable** [LCL+17a].  **SELinux** [SFE10].  **seller** [KJN+16].  **Semantic** [YZCT17, HLR11].  **Semantics** [CM11, Gli12, KGP12].  **Semi** [BDOZ11, KKK+16, WHZ12, XZLW15, PGLL10].  **Semi-automated** [KKK+16].  **Semi-fragile** [WHZ12, PGLL10].  **Semi-homomorphic** [BDOZ11].  **Semi-trusted** [XZLW15].  **Seminarity** [SS10c].  **semirings** [Dur15].  **Sender** [WZ15].  **Sensational** [YGF15].  **sense** [Kem11].  **Sensing** [CCZC13, Kar12, uHAN+18, RPG12, XWZW16, Fay16].  **Sensitive** [Kaw15, RQD+15, Tan15a, QCX18].  **Sensitivity** [YGD+17, LJW+10].  **Sensor** [ABC+17, BN14, CS14, DS11, KH10, LHC11, LLL+12, NNAM10, NYR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YM16].


Service-Oriented [RSGG15]. Services [Aa11b, DLZ+16b, MEF12, OO12, ZHL15, AZPC14, CSD18, CHX13, GAI+18, IMB17, IG11, NZL+15, PP11, XXX15]. Session [BS12, BKJ12, CFST17, SHS12, AN15, DCA12]. Session-Based [BKJ12]. Set [Cor14b, EKP+13, YZ12, Con12, TMK11].


shared-secret [SA12]. Shares [CFOR12, KU14, SA16a, WY12]. Sharing [Bai10, BFM12, BBE14, CCM+15, CFOR12, CCL+13, CCT+14, CIW16, DR12, EM12, FHK17, FR16, HYS11, HL10a, HRS13, HLT+15, KU14, KOTY17, KSS12, KS15, LYT+13, LPL15, Lin15, LCC13, LTC+15b, NS12, Oba11, PSM17, QZ18, SC10, SSU12, SZTT15, TLL12, TWZ11, WYCF14, WKB16, WGF16, XNK15, XZY+12, YFF12, YWZ+12, ZC13, AKK17, ADH17, CT11h, CW14a, EZ15, EAI1, FGMP12, GJMP15, GLW13, GLB18, HF14a, HBBRMN+16, HCCC11, HLC12, HYF18, KH11, KTU16, KPB17, LXY12, LT13, LFWS15, LAL+15, LyWSZ10, LHYZ12, LHL15, LIL+18, LEW19, LL16a, Ma17, O010, O018, QD16, Ral17, SAR18b, TD14, UUN11, UUN13, WKH11, WS12, WOLS12, YC11, YCC16, ZCL+12, ZZ15, ZFWY12, SLL10]. Shell [WZC18, YSS14, TAY14]. Shenzhen [IEE11a]. Shield [NGD+17, KVG16]. Shift [AKP12, ZH15, IWK11]. Shift-Type [AKP12]. Shifting [YY10, CSS+13]. Shih [Joh10]. Shopping [AHS13]. Shor [MN+16]. Short [BHG12, CWW12, NR12, SKV12, WQZ+16, XGL14, LL15, RD17, ZFWY12]. Short-Output [NR12]. Shorter [Hü13, PPB16, TH16]. Should [Eve16]. shown [Ana14]. shows [Goo12]. Shparlinski [Sha10]. Should [Eve16]. Shredder [AMH+16]. Shredding [AMH+16]. SHS [Ana12].
Socio-Rational [NS12], Socio [NS12], SoD [VN16], Soft [Jin10, TLCF16, SS17], Soft-Error [TLCF16], Soft [WZM12a], Software [Bar15, Bee17, EWS14, LRVW14, MRL+18, MV16a, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GIJ+12, HLV10, KHF10, LBOX12, SF12, YWT+12], Solidar [CGB+10], solid [Cri16], Solution [Fra15, GSFT16, HLKL15, Kam13, NA10b, YFT17, Cor14a]. Solutions [LLGJ16, BLV17, KAS15, WW14]. Solved [NA10b, YFT17, Cor14a]. Solution [Mei10, Mur10]. Springer-Verlag [Mei10]. Springs [IEE11b], Spritz [RS14], Spy [AHS13, FKOV15, Bha16, Goo12], SQL [BS13a, Suc12], Square [ARH14], Squashing [GH11a], SRAM [KLM+12], SSH [YSS14, Cri16, Lit14, Rani0, der10], SSL [BJR+14, Dav11, FHM+12, GIJ+12, HREJ14, NPH+14, PP11], SSL/TLS [BJR+14, Dav11, PP11]. SSL/TLS-based [PP11]. SSO [MLM16]. St [DDS12, Dan12, MNS11]. ST-Numbering [MNS11], stack [JSM+18], stage [Mas17]. STAMP [WPZM16]. Standard [Ano12, Ano13a, App13, ABC+17, BCM12, BV11, BV14, CT18, GJJ15, GJZ17, HXZ15, Loe15, MVVR12, OMK+15, SZS14, TCL15, WWHL12, Yon12, ZCL13, BCM13, Kim11, LZW12, L116b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, AEH17, MKRM10, NdMMW16]. Standardization [TRD11], Standards [BCM+15, Che17, DHW+13, NIS13], State [BVS+13, BLM17, CG14a, CCL+13, CHS15, Dew11, DP17, FHR14, LKL18, MKF+16, Sen17, XZY+12, BBDL+17, CK11, CGH17, Ham12, Mid10, QD16, Siri16], Stateful [BVS+13, NTY12, VKPI17, VSR12], Stateless [BHH+15, GM11, MKAA17, NTY12, VDO14, DCA12], Stateless/Stateful [NTY12]. Statement [NS13], Static.
Stationary [ZLDD12]. Statistical [Boh10, Bro11, DBPS12, HZ11, Hey17, LTKP16, OOR+14, SP13, Sim15a].

Stealing [RWW12]. Stealthy [BRPB13].

Steering [HR13]. Steganalysis [Boh10, DA12, Fri12, JHHN12, KD12b, LJK17, LC15, SGF+12, Tan12a, YLL+12, Yi14, YPRI17, LSQ11a, LSQ11b, Sch12a].

Steganalysis-Resistant [YPRI17]. Steganalytic [Ber18, YPRI17].

Steganographic [DA10, HHS+15, LyWlZZ12, WP15, AGLW16, LLC10, CAC14]. Steganography [AGW15, BCG12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZW+14, Joh10, LJK17, LLY+12b, MAL10, PDMR12, Pau10, SK12a, SR12b, TJZF12, WVL+14, YWW10, ZSA12, AOT13, BDK11, BHCdFR12, EEAZ13, GCKK11, LyWSSZ10, LRW13, LRW17, LWW+10, Maz13, MSM+18b, MS17, PHN+12, SI12, Sm16, WKH11, WOLS12, ZMS14].


Stolen [Bha16]. Stopping [Sav13a].

StopWatch [LGR14]. Storage [BCQ+13, CWL16, CCT+14, CLW16, GLG12, HSM14, JSCM17, Kiu515, LCK11, LMD16, LWJ14, QLL17, SKH17, XNKX15, ZDL12, ZVG16, AY14a, AKK+17, BP10, CFVP16, CFZ+10, CLH+16, CDF+10, CDL18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, Sar10a, SY+17, SWW+16, SWW+17, WS13, YSS+16, YZCT17, ZYC+17]. Stored [CMLS15, RSN14]. Stores [BCK17]. stories [Sm15b]. Storing [DLWW11, LZC17].


Strangeness [Ber12]. Strategic [Sch12c].

Strategies [DSSDW14, TJZF12, YCM+13, AZF+12, WW17]. Strategy [LH12, NRZQ15, FLZ+12]. Stratix [SMOP15, SMOP15].

Stream [ABS+12, BMS12, CMLS15, DM18, DG12, DgIS12, DJG+15, GKS17, GCS+13, HZ11, Hey17, IOM12, KPC+16, Kla10, MD12b, MHC12, MS12b, NN12, PRC17, WH18, WHN+12, ZH15, Die12, KM10a, LWK11, LW13b, MRT10, OCG11, QGGL13, RS14].


Strength [DM15, HFW16, Spa16]. Strengthen [BL12].


Strongly [DMM17, HHP17, KW14, YS12]. structural [BDK11].

Structure [HP12, LMHH14, LJ15, MKRM10, WYCF14, LXYL12, ZLW+12, ZPWY12].

Structure-Independent [MKRM10]. Structured [PMZ12]. Structures [GTT11, HHH+13, LHKR10, LPL15, PB12, DDFR13, MHKS14, Sh15, WS12, XWZ+18, ZC15].

STT [VDB+16]. Students [PP10a]. Study [Ano17c, DDR+16, SY15a, STC11, CCG10, EBFK13, MHV15, SS17, VGN14]. Stuxnet [Zet14]. Style [GHP12, GHP13].

stylometry [BAG12]. Subcommittee [Bla16]. subliminal [LWZG10].


Substitution [DA10, SGFCRM+18].

substructure [MRT10]. Succinct [BCT+13, CLKM13]. sufficient [TD14].
suitable [Jeol13, SKB+17], suite [NACLR12]. Sumo [BS12]. Sums [SS12b].
sun [Cer15] super [MZ17a].
Supersingular [Lau17, Y+17]. Supervised [CTC+15]. Supply
[QZL+16a, QZL+16b, YFT17]. support [CZ14, JAS+11, PW10, PKA15, TTL10, VCK+12, ZMM+10, ZBR11]. Supporting
[FMTR12, HCDM12, HZL18, YYS+16]. supports [WR15]. surfaces [CDSLY14].
Surprises [Bow11]. Surrupetiously [SFKR15]. Surveillance
[BPR14a, BPR14b, GZH17, Lan10, Ano16f].
Survey
[ABHC+16, BGN17, BCTPL16, BHJP14, BJCHA17, HPC10, KMY18, KSD+17, LGM+16, MR14b, MSM18a, MS10, NV10, OFM16, SKH17, TRD11, TS16b, AAZ+16, ABB+14, ADH17, BM13, BGG+13, FMA+18, HT13, KIN+16, KAS15, MA17, Maz13, MHV15, NR11, PPA18, WWW17].
Survival [YCM+13, MMS+17a]. Surviving [CFST17]. suspect [der10]. SVC
[MU12, WDDW12, ZLDD12]. SVD [LP12].
SVM [TLL13]. swarm [ZMS18]. SWIFT
[PLCPS11]. Switching
[CNT12, GHPS12, GHPS13, WB12]. Sybil
dCCSM+12. Sylvester
[SS10b]. Symbolic
[Wat10]. Symmetric
[BPR14a, BPR14b, BPD12, CMV14, FPS12, GFBF12, JCHS16, KTT12, Kha10, PR12, PCY+17, TWZ11, YKNS12, BGG+13, CGK011, DLZ6a, FH13, GMRT+15, Gor10, GCVR17, KAS15, LZC17, SKK10]. Symmetric-Key
[CMV14, KTT12].
symmetrical [RS17]. Symmetry [SGS14].
Symposium
[ACM10, ACM11, Ano10, IEE10, IEE11b, IEE13, Wat10, Ano11a].
symptom [YZL+18]. symptom-matching
[YZL+18]. Synchronization
[BL12, WXY+17, yWXY+18, AATM18, XNG+14].
Synchronized [DM18, ACM12].
Synchronizing [H211]. SYND [MHC12].
Syndromes [BBC+13]. Synergy
[KRB12].
Tamperable [ACM+17].
Tampered [SS13].
Taxonomy [CG14a, SRA17].
Targeted [AJA16, GAF+15, KMSM15, MA17].
Tap [ADG16].
Tap [ADG16].
Target [HRS16].
Targeted [ABJ13].
Tasks [Abe12, FKS+13, CL16].
Teaser [ZBR11].
Tech [Ano15e].
Technical [Sir16, TS16b, Wag16, JW14, Suc12].
Tech [Ano15e].
Technical [LJS+14, P10, Ant14].
Tear-Free [Boy16].
Tear-Free [Boy16].
TEASE [ZBR11].
Technology [CGB+10, Fol16, IEE11a, Wu16, IMB17].
telecare [LWK+18, MA17].
Television [SKEG14].
Television [SKEG14].
Tell [Cer14].
Template [NGAuHQ16, SKV12, ATI+10, GCSAddP11].
Templates [DWB12, AHM+18].
temporal-credential-based [JM15+16, MHT+13, XMHD13].
temporal-credential-based [JM15+16, XMHD13].
Tenant [TV15].
terahertz [WW13].
Term [SKV12, CFVP16].
termination [SRB+12].
Ternary [AD11].
Test [HTC+15, JEA+15, LLSW16, MZH15, SS10b, WH18, Ano16g].
Testable [RMP10].
tester [RPSL10, SY15b].
Testing [Cou12, SS12a, AY14a, BJ+14].
Tests [GLG12, MS12b, Sim15a].
Texas [IEE13].
Text [GdM16, CR12, SI12, SWW+17].
Text-dependent [GdM16].
Textbook [PP10a].
Thief [Ber12, Ber17, BTPLST15].
Their [CZLC12b, JSK+17, NR12, CQX18, Hof16, IK15, KK10, Sti11].
them [HLV10, JSK+16, Rus15].
Theological [SS10c].
Theorem [Lau12, HF14a].
Theorem-based [Lau12].
Theoretic [CVM14, MAL10, WSS12, CDGC12, SD10, SKEG14].
theoretical [KL13, ZZ15, Gas13].
Theoretically [TWZ11].
Theories [ABR12].
theory-based [LPZJ15].
There [Cer15, McK10, McK11, SM13].
Thin [Chi16].
things [FQZF18, AAC+16, CLF+17, HZL18, LNK+18b, LGH+17, NLLJ12, NLY15, PLGMCfF18, SB17, WCC18, YCT15].
Third [jCPB+12, QZL+16b, Sen10, BL10, ED19, Kup13].
Third-Party [QZL+16b].
Third-Round [jCPB+12].
Thirteen [AP13].
thou [BDK11].
Threat [CSYY18, ALL+18, Ven14].
Threats [AJA16, ERLM16, GSC17, LJS+14].
Three [CZ15a, HXC+11, LZZ+12b, PC16, Shi11, YKNS12, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].
Three-Dimensional [LZZ+12b].
Three-Factor [HXC+11, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b].
three-party [LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].
Threshold [CT11b, Gil11, FGM10, GLW13, HYS11, L12b, SSU12, Sta12, Tan11, WYCF14, WH15, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGM12, HF14a, HH15, O010, QD16, SES+16, Shy15, SGM16, TD14, ZXJ+14, ZPWY12].
thriving [PC14].
thrive [Sch12b].
throughput [M1012].
Thru [SYC+17, SYW17].
Thwart \[LJS^{+}14\]. Thwarting \[XTK10\]. Ticket \[XHCH14\]. Ticket-based \[XHCH14\]. tickets \[LMJC11\]. tied \[Men13\]. Ties \[PYM^{+}15\]. Tight \[GDCC16, LPS12, LLH18\]. Time \[ASBdS16, Ano17d, App14, AYS15, BJL16, Che17, FD11, GSC17, HC17, HGT15, IF16, JWJ^{+}17, JEA^{+}15, KME^{+}12, LCL^{+}17a, NA10a, Nov10, PNRC17, Ste15b, WLZL12, YE12, AY14a, Ano15d, BM15, CC14, DCAT12, FHH10a, HU15, LW10, LW13b, LML^{+}13, MK11, Ano16g\]. Time-area \[Nov10\]. Time-Memory \[ASBdS16\]. Time-Series \[BJL16\]. Time-Specific \[KME^{+}12\]. Time-Spread \[HGT15\]. Timed \[Jia14b, KFOS12, Tan15a, Urr15, WSS12\]. Timed-Ephemerizer \[Tan15a\]. Timed-Release \[KFO12, Urr15, WSS12\]. Timing \[BGN17, GV14b, Hay13, LGR14, AGH^{+}17, SRB^{+}12\]. Tiny \[ZOC10\]. Titan \[PP10b\]. Titan-R \[PP10b\]. TLS \[AP13, BBDL^{+}17, BJR^{+}14, CFN^{+}14, Dav11\]. TLS-based \[PP11\]. Today \[Ber16a, Mac12\]. Toeplitz \[Ye10\]. Token \[TYK^{+}12, ZM16, IMB17, Jac16\]. token-based \[Jac16\]. Token-Leakage \[ZM16\]. tokenisation \[Mar10b\]. tokenless \[Wat14a\]. Tokens \[Muf16, DCAT12, HU15\]. Tokyo \[Sah13\]. Tolerant \[HK14, ZM16, JLT^{+}12, WMYR16, XW13\]. tolerating \[ZW14\]. Tone \[Yam12\]. Too \[DL15, DSSD14, Ros11\]. Tool \[ASM12, DKMR15\]. Toolbox \[AHS13, TRD11\]. Toolkit \[BJL12\]. Tools \[Abe12, BKBK14, GO17, Ste15a, Lan11\]. Top \[SS12a, SS10c, Sta13, CHX13\]. top- \[CHX13\]. Top-Fanin \[SS12a\]. Top-Secret \[SS10c\]. Topics \[SCPSN10a, SCPSN10b, AB10b, Dun12b, Kia11, Pie10\]. Topology \[HHMK14\]. Topology-Preserving \[HHMK14\]. Topological \[LLOY^{+}12\]. Toronto \[MV12\]. Tossing \[ALR13, DSM14, Fok12, BB14\]. Touch \[SPW^{+}16, Alp18, CTL12\]. touchstroke \[Alp18\]. TPM \[GY13\]. TQC \[vDKS11\]. Trace \[ABR12, PS14, AA14, WXJ10\]. Traceability \[HCETPL^{+}12, WYML16, WHLH16, YFT17, Chi13a, YYS^{+}16\]. traceable \[QRW^{+}18\]. traceback \[LWY12, P18, WYL13\]. traces \[MYR13\]. Tracing \[FW16, PPS12b, WL^{+}17, MFH13, PPR^{+}12\]. Track \[Dun12b, Kia11, Pie10\]. Tracking \[GZH17, MDMJ17\]. Trade \[ASBdS16, BS14, SR10\]. Trade-Offs \[ASBdS16, BS14, SR10\]. Tradeoff \[WDDW12, MV16b\]. Trading \[TW12\]. Traffic \[DRS16, KAHH17, AZHI11, FTV^{+}10, PPR^{+}12, VS11\]. traffic-feature \[FTV^{+}10\]. Training \[HM12\]. Traitor \[LW16, PPS12b, Bha16\]. trajectory \[LVR10\]. Transaction \[BGAD12, KVvE18, OHYB14\]. Transaction-based \[BGAD12\]. Transactions \[DG15, Mic16, Muf16, PAS13b, TV15, DK12, MLMSM12\]. Transceiver \[NBZP17\]. Transcript \[Gli12\]. Transfer \[DN12, FMTR12, HL10a, LCCJ13, WCL^{+}18\]. Transform \[AN12, BCPV11, LSL12b, pNYWyY^{+}14, OWHS12, SM12, YWNW15, BW13, MO14, NEN^{+}14, PC14, TK14, yWpWyY13\]. transition \[CK11\]. transmission \[PSdO^{+}13, WQZ^{+}13\]. Transmitter \[KPB17\]. Transparency \[TJZF12\]. Transparency-Orientated \[TJZF12\]. Transparent \[CCW^{+}10, XTK10\]. Transport \[BBHP15, TW14\]. Trapdoor \[BKPW12, CW12, Mat14, RPSL10, CSZ^{+}11, CW12a\]. treatment \[YS14\]. Tree \[BS14, HSH11, XWZ^{+}18, BW13, BBB16b\]. Tree-based \[HSH11\]. trees \[BTPLS15\].
Trends [Fri12, GCK12, ZMS14, JAE10].
Triangular [AMVZ12]. Tricks [GY13].
trimmed [TTL10]. TRIMS [MGP10].
Triple [LW13b, MS12a]. triple-base
[MS12a]. Triple-image [LW13b].
triumphant [McG11]. Trivium
[MS12b, SR12a]. TRNGs [YKBS10].
Trojan [NDC+13]. Trojans [BRPB13].
True [FR13, LTKP16, Fag17]. TrueErase
[DMS+16]. Truly [LA10].
Truncated [KWS+12, WW12]. Trust
[Bar15, BCK17, Gli12, GM14, GSFT16,
IGR+16, KMSM15, KGP12, PYM+15,
PH12b, PAS13b, Rau15, TMGP13, TV15,
WLY+15, Zha15b, CO11, KGO10,
MLMSMG12, MGP10, Sch12b, YT11a].
Trusted [AWSS17, EAA12, FPY15, YCR16,
ED19, HTC+10, Kip13, XZLW15].
Trustedfree [ATK11]. TTPs
[KGO10, TAKS10]. Tulip
[JB11]. Tunnel
[VDB+16, ZBR11]. Tunnel-based
[ZBR11]. tunnels [Cri16]. Tunny
[Cop10a]. Turing
[Orn16, Bloi2, Car10, CS12, Don14, Hai17,
Hei17, KSU+13, LCJKB12]. Turtle
[WZCC18]. Tutorials [Lim17]. Tutte
[Hai17]. TV
[CCSW11]. Tweakable
[CMLRHS13, LST12, MLCH10, Sar11,
Zha12]. twelve [BCV12]. twice [BM15].
TWINE
[KDH13, TY16b]. Twins
[Bow11]. Two
[Ash14, Bru12, CTL13, DZ14, ED19,
GGHR14, GLW12, HL10b, HP14, KOS16,
KU12, LLC11, Lit14, NSMS14, OTD10,
YSL+10, YLW13, ZM16, AN15, CSD18,
CHS11, DHW+13, FIO15, HPC12, HWDL16,
JLT+12, JMW+16, Kem11, Li10, McG11,
QYWX16, Rus15, SM10b, hszZ15, WW14,
Wat14a, YTL11b, ZCC15, GHKL11].
two-channel [JLT+12]. Two-Factor
[LLC11, ED19, Lit14, JMW+16, Kem11,
WW14, Wat14a]. Two-Party
[Ash14, HL10b, HP14, KOS16, NSMS14,
ZM16, FIO15, HPC12, ZZC15, GHKL11].
Two-Round [GGHR14]. Two-Server
[YLW13, CSD18]. Twofish
[MD12a]. TWS
[OKG+12]. Type
[AKP12, CFL13, PFS12,
SH15, BNST17, SYL13, WB12].
Type-based [CFL13, SYL13]. Type-Flaw
[SH15]. Types [BCEM15].
U.S. [Maf16]. Ubiquitous
[OS16, Par12b]. UESDE
[YZ12]. UHF
[HQY+16, PPH12].
UK [Che11, PJ12, vDKS11, Ano15e].
Ukraine [OGK+15]. ultra
[AATM18, GW14, TG17, WCFW18].
ultra-lightweight
[AATM18, TG17, WCFW18].
U.S.
[Maf16]. Ubiquitous
[OS16, Par12b]. UESDE
[YZ12]. UHF
[HQY+16, PPH12].
UK [Che11, PJ12, vDKS11, Ano15e].
Ukraine [OGK+15]. ultra
[AATM18, GW14, TG17, WCFW18].
ultra-lightweight
[AATM18, TG17, WCFW18].
unlikely [Fag17]. Unlimited [IBM13a]. Unlocking [VS16]. unmanned [XWZW16]. Unprovable [Pas13a]. unsigncryption [EZ15]. unspoofable [NR11]. unstructured [CML16]. untold [Mun17, Pea11]. untraceability [YHL16]. untraceable [AIKC18, JMW16]. Untrusted [LQY10, MS16, ATKH17, DRD11, Mo11, WS13]. updatable [LCL17a]. Update [BCE10, LQY10, FS18, WLFX17]. updating [GCSADDp11, LJWY18]. Upper [AMVZ12]. URLs [AY14a]. USA [Dun12b, IEE13, Kia11, Lin14b, Pie10, Rab10, ACM10, ACM11, IEE10, IEE11b]. Usability [RAZS15]. Use [CSV15, DFKC17, KOS16, NR12, YT12, CZ15b, Die12, Hof16, KK10, MB1+13, OO10, Sli11, UK18]. Used [CGCGPDMG12, BM15, MS13b]. useful [dCCSB1+6]. UseNet [Bel18]. User [BLV17, BKJP12, FLH13, GdM16, Har16, JN12, LLC11, LCL17b, MZHY15, MBC15, MDM17, OdH12, PTD12, PWVT12, RH1+16, SZDL14, SPM+13, WgMdZIZ12, WgMW12, ZPW16, AaBT16, ATKH17, APK+18, BT18, CH10, CHS11, CLHJ13, DSCS12, GH16, HL14, KKM+13, KLW1+6, KDW1+7, LH10c, LNM+11, LNKL13, LH13, MM12, OKG+12, hSSZ15, WT10a, WOLS12, YHL16, YSL+10]. User-centric [BLV17]. User-controlled [Har16]. User-Friendly [SZDL14, WOLS12]. User-Generated [LCL17b]. User-Level [BKJP12]. user-participating [CH10]. Users [DPCM16, KKA15, TAKS10, WPZM16, ATK11, uHAN+18]. uses [Rus15]. Using [ABS12, ABB+14, Ano15a, Ayu12, ARM15, BBC+13, BCPV11, Bee17, BFMT16, BKL12, BJ+14, CST+17, CCL+13, DBS16, DR12, DA10, DBPS12, DL12, ERLM16, ERRMG15, FMS12a, GH11a, GSC17, GAS1+16, HHS1+15, IL15, Jin10, JEA+15, KBL11, Lac15, Lan11, LYZ+13, LLGJ16, MM17, MBC15, MRL+18, MS16, NIS12, NGAuH16, NNAM10, NN12, NSMS14, PMZ13, PSS+13, PDMR12, PTD12, PCPK14, RVRSCM12, SR12a, SFE10, SSA13, SRAA17, SC12, SR12b, Tan12a, TKR14, WWL+14, WgMdZIZ12, WY12, YWW10, YWNW15, YCL17, YSS14, ZH15, ZPW16, ZS12, dRSDlVC12, ATKH17, AHM+18, APK+18, ASVE13, BM13, CSH1+8, CHS11, CR12, CLHJ13, CP13, Cri16, Dav11, DTZZ12, uHAN+18, EEAZ13, FES10, Har14, HZWW17, HL14, HPY10, HCC10, HS11, JCHS16, JMW1+6, KI11, KY10, KKG14, KM11, KSU13, KU16, KP1B17, KLW1+6, LXLY12, LLP+18]. using [LC17, LH10c, LNM+11, LXMW12, LH13, LML+13, MM12, MS13a, MMSD13, MM14a, MKH1+12, MRRT17, MSM+18, NTKG17, PBCC14, PC14, QD16, RS15, RS17, Sar11, SGFCRM18, SKS+18, SAR18b, TLCF16, TG17, TK14, TLL13, UUN11, yWpNyL11, gWpNyY+14, WMX+17, WIIJ17, YQH12, YZZ1+14, YSL+10, ZZKa17, ZLW1+12, ZYC1+17, ZXW+18]. utilization [NZM10].

Vector [ACZ16, HHHN12, Kaw15, ZYT13, ZM16, DWZ12, PWW10, TTL10, ZZ15].
[ADR18, BHKN13, BCI13, BR14, CSLY14, CLW16, GT12, GST13, GVW12, LT13, LT14b, LEW19, MH14, PTK14, QZDJ16, RS10, SE16, SAA11, SKEG14, TBCB15, tWmC12, Yon11, ZOC10, Zin10].
Watermarking [BCGAPM12, BF12, BCPV11, BDB14, CG12b, CHHW12, CCZC13, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HGT15, HHHK14, JSKS12, Joh10].
Welchman [GW14]. Well [JCM12]. were [McK10, McK11]. Western [Han12]. WG [GLIC10, DJG+15, ERRMG15]. WG- [ERRMG15]. Wherefore [BDK11]. Whit [LHA+12]. White [BW16, BCGN16, Mic10b, DD13, YSC16, ZSW+18a].

White-Box [BW16, BCGN16, Mic10b, ZSW+18a].

Whitfield [Hof16]. who [Bat10, Bha16, Car11, Fag17, Hea15, Kap13, McK10, McK11, McK12, Moom14, XT10].


Wireless [ABC+17, BN14, BOB13, CS14, DPCM16, DS11, FLH13, HZC+12, HBCC13, KH10, LLC11, LHM+15, LCK14, LWCJ14, LLZ+12, NNAM10, PCPK14, RCW15, RWLL14, SWYP12, SP15b, TCN+17, YM16, ZLDD12, APK+18, AIB+16, AIK18, ADF12, BLAN+16, BBB16b, CDGC12, CML+18, CLSW12, CL11, DSCS12, HGWW11, HZC+14, HZWW17, HCCC11, HCT+10, HLYS14, JNU17, JMW+16, KP18, KO16, KLW+16, KDW+17, LC17, LMJC11, LKK+17, LNK+18b, NDN13, PL16, QMW17, SA12, SGJ+18, SZMK13, SCKH10, SKK10, TKKH14, Wan13, WW14, WXK+17, XHCH14, XMD13, YHHS16, ZBR11, ZCLL14, ZHH+17].

wiretapping [Lan10]. Wiring [HTZR12]. Wise [CG14a, SSA13]. WISP [PPH12].

Withholding [BRS17]. Without [ASS15, CCL+13, FZT14, GSW+16, GKS17, LTL+15b, NA10a, YLA+13, AZH11, BT12, BF11, BGV14, CCW+10, FSK12a, GH11a, GST12, GLM+16, HDPC13, ISC+16, LLY15, LGWY12, RG10, SYL13, SLZ12, TAKS10, WWYY11, XQL11, YS12, YKC+11.
 References


Ambrosin:2016:FAB


Albertini:2014:MHE


Arora:2012:ILM


Akleylek:2016:SPM


Aghili:2018:ISA

Alizadeh:2016:AMC


Abdalla:2010:PCL


Anand:2015:ICL


Alleaume:2014:UQK

REFERENCES


REFERENCES


Agosta:2015:OPP


Abe:2012:TBG


Arriaga:2012:JSS


Almeida:2014:COS

José Bacelar Almeida, Manuel Barbosa, Jean-Christophe Filliâtre, Jorge Sousa Pinto, and Bárbara Vieira. CAOVerif: an open-source deductive verification platform for cryptographic software implementations. Science of Computer Programming,


Avoine:2016:SSP


Aid:2013:DIO


Acar:2013:SPA


Andreeva:2012:SAS

Arapinis:2012:RET


ALMashrafi:2012:AIM


Applebaum:2010:PKC


Arias-Cabarcos:2015:BIP


Arnold:2015:NGH

REFERENCES

8646 (print), 2151-8556 (electronic).

**Amoah:2016:FMA**


**Ardagna:2010:ECP**


**Avoine:2012:PFS**


**Austrin:2017:ICT**

Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth. On the impossibility of cryptography with tamperable randomness. *Algorithmica, 79*
REFERENCES


Aczel:2011:SWL


Alvarez-Cubero:2016:AVL


Aizatulin:2012:VCC


Ayday:2012:DA


Aliberti:2016:RPS

Attasena:2017:SSC

Adikari:2011:HBT

Abdalla:2012:LBH

Andrychowicz:2016:SMC

Araldo:2018:CEC

Ahmed:2017:IRD
REFERENCES


REFERENCES


Amin:2016:DAP


Applebaum:2014:HGA


Amin:2018:UAP


Alhanahnah:2016:MTI


Azarderakhsh:2014:NDP


Almulla:2013:CKE

M. Almulla, A. Kanso, and M. Ghebleh. A concurrent key exchange protocol based on commuting matrices. Concurrency and Computation: Practice and
REFERENCES


Afanasyev:2011:PPN


Armkn欺诈:2012:STH


AlTawy:2013:SOC


Aiash:2015:IAA

REFERENCES

Aldrich:2011:GUS


Au:2018:PPP


Alpar:2018:BTA


Asharov:2013:FCF


Awad:2016:SSZ

84

REFERENCES

DEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Arnedo-Moreno:2010:JRA


Abbasinezhad-Mood:2018:DHI


Arsalan:2012:IRW


Ahir:2017:LAR


Adj:2013:WDC


Aumasson:2014:HFB


Ahmadian:2010:PDS


Aga:2017:ISM


Anawis:2014:ARR


**Anonymous:2011:AXL**


**Anonymous:2011:MCB**

Anonymous:2012:SHS


Anonymous:2013:DSS


Anonymous:2013:NCI


Anonymous:2013:SSD


Anonymous:2013:SIS


Anonymous:2014:ERE


Anonymous:2015:BSU

Anonymous. Blind signatures using offline repositories provide new level of security. Scientific Computing, ??(??):??, May
REFERENCES

Anonymous:2015:BRDa


Anonymous:2015:CEB


Anonymous:2015:QCS


Anonymous:2015:UGB


Anonymous:2016:CPSd


Anonymous:2016:CPSe

Anonymous. Call for papers special issue on postquantum cryptography. IEEE Security &
REFERENCES

Anon Anonymous:2016:EMT

Anon Anonymous:2016:FVM

Anon Anonymous:2016:GUP

Anonymous:2016:MBE

Anonymous:2016:SWT

Anonymous:2016:SIR

Anonymous:2017:BA
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

Anonymous. Cybernetica case study: Solving the Estonian ID-card case. Web news story., December 13, 2017. URL https://cyber.ee/en/news/cybernetica-case-study-solving-the-estonian-id-card-case/. 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

TPM (Trusted Platform Modules). It allows recovery of the private key from knowledge of the RSA public key, and thus, facilitates malicious cloning of the cards, and decrypting of some encrypted filesystems.

Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF


AlFardan:2013:LTB


Ali:2018:SUA

REFERENCES

Applebaum:2013:GXG

Applebaum:2014:CCP

Appel:2015:VCP

Albrecht:2015:FBR

Al-Qarni:2012:EI

Arai:2013:MDH
Kohei Arai. Method for data hiding based on LeGall 5/3 (Cohen–...

**Adj:2014:SRC**


**Altawy:2018:TCM**


**Asharov:2016:LPI**


**Artemenko:2017:PGO**

Sergei Artemenko and Renan Shaltiel. Pseudo-

**Andrade:2016:LEP**


**Asharov:2014:TCC**


**Ahmadi:2011:SKC**


**Ahmadi:2012:SKE**


**Ali:2014:ALD**

Syed Taha Ali, Vijay Sivaraman, and Diethelm Ostry. Authentication of lossy data in body-sensor networks for cloud-
REFERENCES


Abdullah Al-Tariq, Abu


**Alam:2015:ACF**


**ATS15**


**AV12**


**Abdalla:2012:LRS**


**Altaf:2017:LHL**


**AWSS17**
Anzala-Yamajako:2012:RAC


Ahmad:2014:RTN


AlTawy:2014:IDR


Aysu:2015:FRT


Ayub:2012:BRB


Apavatjrut:2012:EEA

REFERENCES

Alshammari:2011:CET


Alavi:2014:RQE


Behnia:2013:IEB


Blaner:2013:IPP


Brennan:2012:ASC


Bai:2010:RKI

REFERENCES


REFERENCES

Baldi:2013:ULC

Barak:2014:OEF

Beurdouche:2017:MSU

Beimel:2014:MLS

Bernstein:2017:SRD

Boldi:2012:IUG
Paolo Boldi, Francesco Bonchi, Aristides Gionis, and Tamir Tassa. Injecting uncertainty in graphs for


103

REFERENCES


REFERENCES


REFERENCES

Transactions on Privacy and Security (TOPS), 20 (3):8:1–8:??, August 2017. [BCL14]
CODEN ???. ISSN 2471-2566 (print), 2471-2574 (electronic).

Bernstein:2014:CKR


Basin:2012:PRI


Basin:2013:PRI


Basin:2015:ISC


Bicakci:2013:LSS

Botta:2014:PCI


Boyle:2014:EO


Basso:2011:BWC


Bessani:2013:DDS


Blasco:2016:SWB


Biddle:2012:GPL

REFERENCES


REFERENCES


Barbareschi:2018:PBH


Bossuet:2016:EPA


Bendlin:2011:SHE


Berto:2011:CSF


Berto:2012:KIO


Boldyrev:2012:SSE

REFERENCES


REFERENCES


Berghel:2016:S

Berghel:2017:ELR

Berretti:2018:IAS

Bouman:2011:SAW

Bas:2012:BLK

Bhargavan:2012:VC1


REFERENCES

112


[Barbulescu:2013:QP] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux,

Biswas:2017:STC


Borcea:2017:PEE


Brakerski:2014:LFH

REFERENCES


[BHJP14] Christoph Bösch, Pieter Hartel, Willem Jonker, and Andreas Peter. A survey of provably secure searchable


Boche:2016:DSK


Bouraoui:2017:HAE


Bogdanov:2012:UTC


Benhamouda:2016:NFP


Brubaker:2014:UFA


Boldyreva:2012:NPG

Alexandra Boldyreva and Virendra Kumar. A
REFERENCES


**Bouti:2012:SCB**


**Bhuyan:2014:DDD**


**Braun:2012:ULA**


**Brakerski:2010:OHB**


**Bogdanov:2013:SDS**

REFERENCES


[BL10] Daniel J. Bernstein and Tanja Lange, editors. Progress in cryptology — Africacrypt 2010: third in-


Matt Blaze. US House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, Hearing on “Deciphering the Debate over Encryption”. Web document, April 19,


REFERENCES

Burmester:2011:LRA

Birajdar:2013:DIF

Bard:2015:PRO

Baldwin:2010:AFI

Biswas:2012:IBA

Benamara:2016:ICA
REFERENCES


REFERENCES


REFERENCES

Boyce:2016:BOT


Burns:2010:SCR


Bohli:2011:RAP


Brooke:2010:DCX


Bellare:2014:SSEa


Bellare:2014:SSEb


Boneh:2016:BCR

REFERENCES


sliding-right-attack-allows-recovery-of-rsa-1024-keys/126675/. See [BBG+17].

Becker:2013:SDL

Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL http://people.umass.edu/gbecker/BeckerChes13.pdf.

Benaloh:2015:EEV


Bag:2017:BBW


Bellare:2012:MIS


Brumley:2012:SFI


Bergsma:2012:PAW

REFERENCES

r-project.org/archive/2012-1/RJournal_2012-1_Bergsma+Smith.pdf.

Bajaj:2013:CSE


Birrell:2013:FIM


Bhattacherjee:2014:CAT


Bagheri:2015:NNA


Boorghany:2015:CIL


Bojinov:2014:NMC


Basin:2011:AIS

[BS11] David Basin, Patrick Schaller, and Michael Schläffer. Applied information security: a hands-on ap-
REFERENCES


**Bulygin:2010:CAC**


**Burke:2011:AMD**


**Brakerski:2011:EFH**


**Brakerski:2014:EFH**

Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE.

**Bayrak:2012:AI**


**Baeck:2013:SPK**


**Bogdanov:2012:ZCL**

Andrey Bogdanov and Meiqin Wang. Zero-correlation linear crypt-

**Bhatnagar:2013:BIW**


**Bai:2016:ALC**


**Bhatnagar:2013:SRI**


**Baek:2016:EGC**


**Bhatnagar:2012:IVE**


**Bao:2010:ISC**

Feng Bao, Moti Yung, and Dongdai Lin, editors. *Information security and cryptography: 5th international conference, IN-


[CC10] Christian Cachin and Jan Camenisch. Encrypting

[CCF17]  
**Chang:2014:RRT**  

[CC14]  
**Chadha:2016:AVE**  

[CCCK16]  
**Chretien:2015:SPP**  

[CCD15]  

[CGC10]  

[CCG10]  


[Cascudo:2015:SSN] Ignacio Cascudo, Ronald Cramer, Diego Mirandola,

Chatterjee:2017:PBS


Cho:2014:DGA


Chen:2011:EAA


Chu:2014:KAC


Chen:2010:ALD


Costello:2014:CAS

Ceruzzi:2014:HFT

Cerf:2015:CTN

Chang-Fong:2016:CSC

Carter:2013:SSA

Centenaro:2013:TBA
REFERENCES


[CFXY17] Kim-Kwang Raymond Choo, Yunsi Fei, Yang Xiang, and Yu Yu. Embedded device forensics and security. ACM Transactions
REFERENCES

Chang:2010:PRN


Chen:2010:IFA


Camenisch:2012:EAA


Che:2012:WAM


Cheraghchi:2014:NMC


Corrigan-Gibbs:2014:KS

REFERENCES


[Curtmola:2011:SSE] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions

Cheng:2012:PAI


Chandran:2014:PBC


Cheng:2013:NIB


Chen:2010:NUP


Chang:2011:DEQ


Chan:2013:OCK

REFERENCES


REFERENCES


[Chi13b] R. Chirgwin. Android bug batters Bitcoin wallets. The Register, ??(??):??, ???. 2013. URL ????.


REFERENCES


Chou:2014:EMA

Chu:2016:BEE

Chen:2013:ATK

Cilardo:2011:EPT
Alessandro Cilardo. Exploring the potential of threshold logic for cryptography-related operations. IEEE
REFERENCES


Cheng:2013:EHM


Cao:2014:SCI


Cho:2012:CBF


Cho:2015:CBF


Chandra:2011:AST


Chase:2013:SMN

Melissa Chase, Markulf Kohlweiss, Anna Lysyana-
REFERENCES


[Chen:2016:RPR]


[Chen:2012:NCB]

REFERENCES


REFERENCES

150

(print), 1532-0634 (electronic).

Cremers:2011:OSV


Cozzens:2013:MEE


Coles:2016:NAU


Cao:2018:EEG

Efficient hardware implementations of BRW polynomials and tweakable enciphering schemes. 


REFERENCES


REFERENCES


REFERENCES


[Culhane:2015:VVV]

[Chhabra:2011:NSN]
REFERENCES

Clark:2012:RLA


Chapin:2014:SRP


Chattaraj:2018:NTS


Chauhan:2018:BBA


Chadwick:2014:AFI


Chen:2013:RWM

Xianyi Chen, Xingming Sun, Huiyu Sun, Zhili Zhou, and Jianjun Zhang. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. The Journal of Systems and Software,
REFERENCES


Chen:2017:SIE

Ciegis:2016:ADP

Chong:2015:SID

Chow:2012:EPV

Chen:2018:SIA

Chen:2011:IBT
Xiaofeng Chen, Willy Susilo, Fangguo Zhang, Haibo Tian, and Jin Li. Identity-based trapdoor mercurial commitments


REFERENCES

Chou:2013:TIB


Crenne:2013:CMS


Calmon:2014:ITM


Choi:2012:LTF


Chung:2012:CBI


Chen:2014:SBB

REFERENCES


Long Chen and Zhao Zhang. MemGuard: a

**Chen:2015:TCP**


**Cheng:2015:OMU**


**Chen:2015:TCP**


**Chen:2015:OMU**


**Chen:2015:TCP**

Chen:2014:CSI


Dharwadkar:2010:SSG


Djebbar:2012:ASB


Danezis:2012:FCDb


Davies:2011:IST


Diong:2012:DAU

REFERENCES

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32805-3_4/.

Dacosta:2012:OTC


Cordeiro:2012:IMB


DePrisco:2013:CVC


DArco:2014:MIC

REFERENCES


REFERENCES


Markus Dürmuth and David Mandell Freeman. Deniable encryption with negligible detection probability: An interactive construction. *Lecture Notes in Computer Science*, 6632:


Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Giovanni Livraga, Stefano Paraboschi, and Pierangela Samarati. An authorization model for multi
REFERENCES


[DENG:2017:LLH]


[DING:2012:CLS]


[DUJUR:2015:FSF]


[Dutta:2017:EFC]


[Dupressoir:2014:GGP]


[Ding:2012:NRR]

REFERENCES


Dinoor:2010:PIM


Ding:2015:CWF


Domnitser:2012:NMC


Dolev:2012:ATC


Delfs:2015:ICP


Dorre:2016:ELO

[Felix Dörre and Vladimir Klebanov. Entropy loss and output predictability in the Libgcrypt PRNG. Report CVE-2016-6313, Karlsruhe Institute of Technology, Karlsruhe, Germany, August 18, 2016. 2 pp. URL http://:
REFERENCES

//formal.iti.kit.edu/~klebanov/pubs/libgcrypt-cve-2016-6313.pdf.


REFERENCES


*Dimitrakakis:2015:ELA*  

*Demme:2012:SCV*  

*David:2012:UCO*  

*Donovan:2014:ATM*  

*Doroz:2015:AFH*  

*Duncan:2012:CAI*  
James:2017:IFS


Das:2016:CWM


Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL

Konstantinos A. Draziotis. (EC)DSA lattice attacks based on Coppersmith's
REFERENCES


Das:2012:DPB


Deng:2018:SFE


Dachman-Soled:2014:COF


Dodic:2014:HEY


Dini:2013:HHS

REFERENCES


[DW12] C. David and J. Wu. Pseu-


Dodis:2013:OWE


Deng:2014:TNI


Doss:2012:MDA


Dent:2010:PS


Eslami:2011:SIS


Erguler:2012:PAI

[EA12] Imran Erguler and Emin Anarim. Practical attacks and improvements to an efficient radio frequency identification authentication protocol. Concur-
REFERENCES

Ekberg:2012:AEP

Ehdaie:2016:HCR

Egele:2013:ESC

Esiner:2017:QRI

Esiner:2019:TFA

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


REFERENCES


ElBansarkhani:2012:ELB


Embar:2014:PWO


Evtyushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC

REFERENCES

SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Engels:2012:HLA


Ebadi:2015:DPN


Essex:2017:DDU


Everett:2012:EC


Everett:2016:SES


Eibach:2010:OGB

REFERENCES


Farash:2014:CIE

Fay:2016:ICM

Fischlin:2012:PKC

Ferretti:2014:DCI

Fuglerud:2011:SIA
REFERENCES

[Fehr:2010:QC]

Felten:2013:LBA

Faugere:2010:CLR

Fleischmann:2012:MFA

Feng:2010:CTS

Farras:2012:LTM
REFERENCES


REFERENCES


Farash:2015:PSE Mohammad Sabzinejad Farash, Sk Hafizul Islam, and Mohammad S. Obaidat. A provably secure and efficient two-party password-based explicit authenticated key exchange protocol resistance to password guessing at-
REFERENCES

188

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


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


[FLS+10]

Forler:2012:DAC


[FLW12]

Feng:2012:CAO


[FLZ+12]

Ferrag:2018:SCN


Fallahpour:2015:AWB


Farwa:2018:FAI

Shabieh Farwa, Nazeer Muhammad, Nargis Bibi, Sajjad A. Haider, Syed R.


REFERENCES

See also [?].


Sebastian Faust, Krzysztof Pietrzak, and Joachim Schipper. Practical leakage-


[Fu:2015:TVG]


[Feng:2018:ALA]


[Fathimal:2016:SSS]


[Fra15]


[Fra16]

Fridrich:2010:SDM


Fridrich:2012:MTS


Fugkeaw:2018:SSA

Somchart Fugkeaw and

Fu:2016:EPS


Frauchiger:2013:TRR


Forbes:2015:CTC


Fugkeaw:2018:SSA
REFERENCES


---

Fang:2011:ICP


---

Feng:2011:GD


---

Ferguson:2010:CED


---

Fujioka:2012:SHI


[Frecio:2012:SEI]


[Frecio:2012:SEP]


[Frecio:2012:DCA]


[Fuc10]


[Ful10]

REFERENCES

[196]


Feng:2013:ECE


[FWS13]

Fanyang:2012:SAK


[FXP12]

Fan:2015:IRD


[FYM15]

Fan:2013:KIS


[FY11]

Feng:2011:VBF


[FXP+17]
REFERENCES

Fan:2014:NCI


GomezPardo:2013:ICM


Gross-Amblard:2011:QPW


Gope:2018:LPP


Galindo:2013:NIC

David Galindo. A note on an IND-CCA2 secure Paillier-based cryptosystem. *Information Processing Letters*, 113(22–
REFERENCES


Gasarch:2013:RBC


Gutierrez:2016:IDO


Gorantra:2011:MKC


Guyeux:2015:ECS


Gupta:2012:CDF


Gupta:2013:HPH

REFERENCES

Guerra-Casanova:2011:SOT


Granado-Criado:2017:HCH


Gong:2016:ATI


Guerin:2016:TDU


Geller:2013:MIS


Gentry:2010:CAF

Craig Gentry. Computing

**[Gentry:2013:EMH]**


**[Gong:2010:PCI]**


**[Grigg:2011:CCN]**


**[Garg:2016:CIO]**

REFERENCES


REFERENCES


[GHPS14] Yossi Gilad, Amir Herzberg, and Haya Shulman. Off-

**Godor:2012:HBM**


**Georgiev:2012:MDC**


**Gilbert:2010:ACE**


**Giry:2015:BCK**


**Gao:2013:LCA**

REFERENCES

Gu:2015:EIB


Gravier:2015:WOD


Goyal:2013:CZK


Gu:2017:IBM


Geetha:2011:VRN


Garay:2016:MPA

Grigoriev:2017:YMP


Gaj:2017:DCR


Guo:2010:HMW


Gouvêa:2012:HSI


Guo:2018:KAA


Gorawski:2012:EAS

REFERENCES


**Guo:2014:SAS**


**Gao:2014:URA**


**Groza:2017:LCL**


**Gong:2012:KNF**


**Garay:2017:SIA**

Goodin:2012:CBS

Dan Goodin. Crypto breakthrough shows Flame was designed by world-class scientists: The spy malware achieved an attack unlike any cryptographers have seen before. Web document., June 7, 2012. URL http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/.

Garcia:2012:ERP


Gorski:2010:CDS


Groth:2012:NTN


Glowacz:2017:IDW


Goodrich:2012:EVW


Genkin:2016:PKE

Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, and Eran Tromer. Physical key extraction attacks on PCs. Communications of the Association for Computing Machinery, 59(6):70–79, June 2016. CODEN CACMA2. ISSN 0001-0782
Grossschädli:2012:EJI


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


Greengard:2011:MRM


Green:2017:SSE


Grimes:2015:CCT

William Grimes. Cracking codes through the cen-

**Gibson-Robinson:2012:AAL**


**Guha:2017:RTS**


**Guin:2016:FCS**


**Gong:2016:FSC**


**Gierlichs:2012:ICD**


**Genkin:2013:RKE**

Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. Technical and web report, Technion

Ge:2016:KPA


Gazi:2012:EOS


Goodrich:2011:EAD


Grosse:2013:AS


Gueron:2016:MEG


Gebotys:2016:PCP


Wang:2014:RAW


Gao:2015:GCC


Goh:2013:TOT


Guo:2012:AKE


Guo:2017:EMD

Gao:2012:RHC


Guo:2018:SMK


Ge:2013:SAP


Haigh:2017:HRC


Hamamreh:2012:RPA


Hamlin:2017:NMC

Hanyok:2012:EHH


[Han12]

Harn:2013:GA


[Har13]

Harrington:2014:GEF


[Har14]

Hardesty:2015:BAC


[Har15]

Hardesty:2016:SUC


[Har16]

Hayes:2013:NSA


[Hay13]

Houmansadr:2013:BCN

REFERENCES

Hurlburt:2014:BBC


Hetzelt:2017:SAE


Hernandez-Becerril:2016:GIS


He:2013:HEH


Hulsing:2017:XEH


Hao:2012:SAM


Hu:2017:ATE

Jingwei Hu and Ray C. C. Cheung. Area-

**Hwang:2010:RIB**


**Hsu:2011:NLM**


**Hore:2012:IED**


**Hernandez-Castro:2012:MTA**


**Huang:2014:FOS**

REFERENCES

Hsu:2011:WLC

Hernandez-Castro:2012:AFH

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
REFERENCES

CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35416-8_13./

Hellman:2017:TLC


Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Heys:2017:SCF


Harn:2014:MTS

REFERENCES

Hoang:2014:IMD

Hua:2015:TSE

Huang:2016:EDP

Hua:2015:TSE
Hu:2016:EWS


Hayashi:2013:AEI


Huber:2014:TPW


Huang:2017:BBC


Haitner:2011:PRI


Hong:2015:RSM

Hinarejos:2015:MES


Hinek:2010:CRV


Hinkelmann:2011:CPA


Hur:2014:SDR


Houmansadr:2014:NBW


Hur:2013:REC

Heyse:2012:LEA


Heil:2014:APH


Howe:2018:PDG


Holenstein:2011:ERO


Harn:2010:A


Haza


Huang:2015:MSE


Harn:2011:FDM


Huffmire:2010:RBS


Herranz:2011:RBS


Huang:2015:CEA

Xinyi Huang, J. K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou. Cost-effective authentic and anonymous data sharing with forward security. *IEEE Transactions on Computers*, 64(4):971–
REFERENCES

Howard:2010:DSS


Hohenberger:2012:DDQ


Huang:2014:SWC


Hefeeda:2010:ASM


Herzberg:2012:TJA


Hore:2012:SMR

Bijit Hore, Sharad Mehrotra, Mustafa Canim, and Murat Kantarcioğlu. Secure multidimensional range queries over outsourced
REFERENCES

[229]


[Hoang:2012:ESB]


[HMR12]

[Hirt:2014:BA]


[HMR14]


[Hof15]


[Hof16]


[Hollings:2012:CCE]

REFERENCES

Hyla:2012:CBE

Hazay:2014:OSA

Halder:2010:WTR

He:2012:ECT

Howe:2015:PLB

Hur:2010:CCS
Han:2016:GGA


Han:2014:GTK


Hulsing:2013:OPX


Huang:2014:AFS


[HSM13] Jinguang Han, Willy Susilo, and Yi Mu. Identity-based...
REFERENCES

Han:2014:IBS

Han:2012:PPD

Heather:2014:CPE

Shi:2015:CTS

Hamdy:2011:HPB

Henson:2013:MES
 REFERENCES

0360-0300 (print), 1557-7341 (electronic).

Hu:2010:TTW


Huang:2015:PAP


Herbert:2012:SMP


Hald:2015:RRA

Huang:2015:PAP


Hursing:2013:WOS


Hurlburt:2016:MBO


Harvey:2017:FPM

[HVL17] David Harvey, Joris Van Der Hoeven, and Grégoire

Han:2012:MIA


Hwang:2011:NIB


He:2016:STI


Heng:2010:CNS


He:2015:SSQ

Zhian He, Wai Kit Wong, Ben Kao, David Wai Lok Cheung, Rongbin Li, Siu Ming Yiu, and Eric Lo. SDB: a secure query processing system with data interoperability. *Proceedings of the VLDB Endowment*, 8(12): 1876–1879, August 2015. CODEN VLDBFR. ISSN 2150-8097.

Hsu:2014:VWR

Fu-Hau Hsu, Min-Hao Wu, Cheng-Hsing Yang, and


Heys:2011:PSC


Han:2012:ERI


Han:2014:ATS


[He:2017:AHA]


[He:2018:LAB]


[IB11] Sk. Hafizul Islam and G. P. Biswas. A more efficient and secure ID-based remote mutual authentication with key agreement...

IBM:2013:DMP


IBM:2013:IPC


Irshad:2017:CPP


IEEE:2010:PIA


IEEE:2011:ICI


IEEE:2011:PIA


**IEEE:2013:PIS**


**Imanimehr:2016:HPR**


**Islam:2011:MDA**


**Iyengar:2016:SPS**


**Imai:2015:IRR**


**Islam:2015:LFP**

Sk Hafizul Islam and Fagen Li. Leakage-free and
provably secure certificateless signcryption scheme using bilinear pairings. [IOM12]


REFERENCES


Irshad:2016:EAM


Ishai:2014:PCP


Jacobs:2016:STB


Jie:2011:RGA

Prins:2011:DCA


Jain:2013:MSD


Jho:2016:SSE


Jakobsson:2012:AWD


Chang:2012:TRR


Jogenfors:2015:HBT


Jeong:2013:CBC

References

Jo:2014:ODE

Jing:2012:MVB

Jiang:2014:UIS

Jiang:2014:TEA

Jiang:2016:MA

Jiang:2017:BMA
Jin:2010:ADW


Jain:2010:QP


Jawad:2013:GAD


Jun:2012:IIR


Jiang:2016:PPT


Jovanovic:2012:FAL

REFERENCES

Salt Reference

Jajo
dia:2012:RET


Jia:2012:PKD


Jiang:2016:OOC


Jiang:2016:UTC

Qi Jiang, Jianfeng Ma, Fushan Wei, Youliang Tian, Jian Shen, and Yuanyuan Yang. An untraceable temporal-credential-based two-factor authenti-

**Jain:2012:BAS**


**Joh:2013:NGA**


**Jou:2013:NIC**


**JRF:2010:BRF**


**JR13**

R. Amzi Jeffs and Mike Rosulek. Characterizing


Jiang:2018:CPA


Joye:2012:FAC


Tong:2012:NBD


Jiang:2016:CVI

REFERENCES

2016. CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

[Juels:2014:INC]

[Jiang:2017:SLD]

[Jin:2015:NCD]

[Joux:2014:SAC]

[Jiang:2010:EDI]

[Khazaei:2017:COA]
Shahram Khazaei and Siavash Ahmadi. Ciphertext-


Karafyllidis:2012:QGC


Kong:2015:CSM


Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP

[102x366] Jan Willem Kleinrouweler, Sergio Cabrero, and Pablo Cesar. An SDN architecture for privacy-friendly network-assisted DASH. ACM Transactions...

Kim:2011:SSE


Koz:2012:ASE


Karakoc:2013:BCL


Karakoc:2015:AKA


Kumari:2017:DSU

Saru Kumari, Ashok Kumar Das, Mohammad Wazid, Xiong Li, Fan Wu, Kim-Kwang Ray-

**Keblusek:2015:BRK**


**Kemshall:2011:WMT**


**Kleinjung:2010:FBR**


**Kikuchi:2012:SSN**


**Kramer:2010:FDC**

Simon Kramer, Rajeev Goré, and Eiji Okamoto. Formal definitions and complexity results for trust relations and trust domains fit for TTPs, the web of trust, PKIs, and ID-based cryptography. *ACM*
REFERENCES


**Kim:2012:SLT**


**Khedr:2016:SSH**


**Kwon:2010:SEB**


**Koo:2018:PPD**


**Khadaei:2010:NBS**


**Kastner:2010:AOT**


Khalil:2014:CIM


Khan:2015:CMB


Khan:2014:MEK


Karopoulos:2010:FIP


Kubota:2016:SAV

Khan:2013:EDC


Khan:2014:IPR


Kushwah:2011:EIB


Khakpour:2013:ITA


Klapper:2010:PSS


Ko:2010:MME

Jeonggil Ko, Jong Hyun Lim, Yin Chen, Rvazvan Musvalou-E, Andreas Terzis, Gerald M. Masson, Tia


REFERENCES

437–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-7679-8. LCCN ????.


Kiyoshima:2014:CRB


Karger:2011:LLB


Kavun:2018:SAE


Khovratovich:2010:RCA


Khovratovich:2010:RRA


Kumari:2016:APW

Shipra Kumari and Hari Om. Authentication protocol for wireless sensor...

**Koblitz:2010:BRB**


**Kasper:2012:SCA**


**Khamsemanan:2016:BBU**


**Kawachi:2017:GCR**


**Kollmitzer:2010:AQC**


**Kang:2012:AKM**

Hyun-Sun Kang and Chang-Seop Park. An authen-
REFERENCES


**[Kolman:2017:SCG]**


**[KP17]**


**[Koya:2018:AHM]**


**[Kiltz:2011:EAH]**


**[KPB17]**

REFERENCES

Kocabaş:2012:CPB


Kang:2016:DSA


Keskinarkaus:2010:IWD


Krenn:2013:CCR


Knudsen:2011:BCC


Krantz:2012:EAM

Steven G. (Steven George) Krantz. *Elements of advanced mathematics*. Chapman and Hall/CRC, Boca


[KSM+12] Vladimir Kolesnikov and Abdullatif Shikfa. On the limits of privacy provided by order-preserving...
REFERENCES


[Kumar:2015:RGB]


[Karthiga:2018:PSA]


[Kocabas:2016:ESM]


[Khan:2017:TPK]

[Jihoon Kwon, Seog Chung Seo, and Seokhie Hong. An efficient implementation of pairing-based cryptography on MSP430 pro-
REFERENCES


REFERENCES

Ustimenko. On the comparison of cryptographi-
cal properties of two differ-
ent families of graphs
with large cycle indica-
tor. *Mathematics in Com-
puter Science*, 6(2):181–
198, June 2012. CODEN
???? ISSN 1661-
8270 (print), 1661-8289
(electronic). URL http://
www.springerlink.com/openurl.asp?genre=article&
issn=1661-8270&volume=
6&issue=2&spage=181.

Kai:2014:FSD

[KU14] Hiroshi Kai and Keita
Ueda. Fake shares detec-
tion on a visual secret shar-
ing scheme by rational in-
terpolation. *ACM Com-
munications in Computer
Algebra*, 48(3/4):124–126,
September 2014. CODEN
???? ISSN 1932-2232
(print), 1932-2240 (elec-
tronic).

Kupcu:2013:DTT

[Küp13] Alptekin Küçü. Distribut-
ing trusted third parties.
*ACM SIGACT News*, 44
(2):92–112, June 2013. CO-
DEN SIGNDM. ISSN
0163-5700 (print), 1943-
5827 (electronic).

Kupcu:2015:OAS

[Küp15] Alptekin Küçü. Offi-
cial arbitration with se-
cure cloud storage appli-
cation. *The Computer
Journal*, 58(4):831–852,
April 2015. CODEN CM-
PJAl6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
comjnl.oxfordjournals.
org/content/58/4/831.

Kuznetsov:2011:APP

[A. Kuznetsov. Analy-
tic proof of Pecherskii-
Rogozin identity and Wiener-
Hopf factorization. *The-
ory of Probability and its
Applications*, 55(3):432–
443, ???? 2011. CODEN
TPRBAU. ISSN
0040-585X (print), 1095-
7219 (electronic). URL
http://epubs.siam.org/
tvp/resource/1/tprbau/
v55/i3/p432_s1.

Kiljan:2018:ETA

[Sven Kiljan, Harald Vranken,
and Marko van Eekelen. Evalua-
tion of transaction authen-
tication methods for online
banking. *Future Generation
Computer Systems*, 80(??):430–447,
March 2018. CODEN FG-
SEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0167739X16301352.

Karpovsky:2014:DSS

[M. Karpovsky and Zhen
Wang. Design of strongly
secure communication and
computation channels by


REFERENCES

Lathey:2015:IEE

Lackey:2015:UHP

Liang:2015:SEC

Landau:2010:SSR

Langsworth:2011:USA

Langley:2013:EDC

Landau:2017:LCI
REFERENCES

221 pp. LCCN K3264.C65 L38 2017?

Launchbury:2012:TBC

[La12]

Lauter:2017:POL

[Lau17]

Liu:2013:PAE

[LB13]

Luo:2012:ESI

[LBOX12]
Jianqiang Luo, Kevin D. Bowers, Alina Oprea, and Lihao Xu. Efficient software implementations of large finite fields GF(2^n) for secure storage applications. ACM Transactions on Storage, 8(1):2:1–2:??, February 2012. CODEN ???. ISSN 1553-3077 (print), 1553-3093 (electronic).

Lupu:2012:IBK

[LBR12]

Lu:2013:CSA

[LC13]
REFERENCES


[Li:2015:NAC] Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, and Wenjing

[LCL15]

Lee:2017:SUE


[LCL17]

Li:2015:CEH


Li:2017:RNF


Li:2017:CCF

Liang:2014:CCS


Liu:2016:EQD


Liu:2016:NOP


Louchene:2013:WMR


Lotz:2015:SCS


**Li:2017:PCL**


**Lancrenon:2012:IPI**


**Liu:2017:ECC**


**Lan:2010:RNG**


**Li:2012:FDM**

REFERENCES

Liu:2012:LFA

Labati:2016:BRA

Lopez-Garcia:2014:PBB

Lee:2010:ISC
Donghoon Lee and Seokhie Hong, editors. Information, security and cryptography – ICISC 2009: 12th international conference, Seoul, Korea, December 2–4, 2009, revised selected papers, volume 5984 of Lecture notes in computer science. Springer-Verlag,


[LH13] Yi-Pin Liao and Chih-Ming Hsiao. A novel multi-server remote user authentication...


REFERENCES

Lin:2015:DVS


Lindell:2017:TFC


Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP


Li:2017:MMA


Li:2016:IRI

Xinran Li, Chen-Hui Jin, and Fang-Wei Fu. Im-

Li:2017:SQS


Li:2012:OEA


Laszka:2014:STC


Liu:2017:OOA


Liu:2018:PAB

REFERENCES

Li:2012:BIB


Lee:2014:SPB


Leva:2013:ABN


Le:2011:RMA


Lee:2015:TSS


Lee:2015:TSS

Lu:2016:PSC


LL16b


Lee:2010:PMB


Lee:2011:TAT


Li:2015:IBE


Li:2015:ANA

Lin:2016:SCU


Lyu:2018:PKE


Li:2012:RIB


Liu:2018:GEI


Li:2017:CIS


Liu:2018:VSE

[LLL+18] Zheli Liu, Tong Li, Ping Li, Chunfu Jia, and Jin Li. Verifiable searchable encryption with aggregate keys for data sharing system. *Future Generation Computer Systems*, 78
REFERENCES

Li:2010:DCY

Lai:2013:SAS

Lu:2012:IEC
Xianhui Lu, Bao Li, Qixiang Mei, and Yamin Liu. Improved efficiency of chosen ciphertext secure encryption from factoring. [LLW16]

Lai:2018:EQK

Lee:2016:CAM
REFERENCES


**Ling:2012:NCC**


**Luo:2012:FSI**


**Lee:2015:SAS**


**Lu:2012:BBE**


**Lai:2016:GGB**

Chengzhe Lai, Rongxing Lu, Dong Zheng, Hui Li, and Xuemin (Sherman) Shen. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. *Computer Networks (Amsterdam, Netherlands: 1999)*, 99(??):66–81, April 22, 2016. CODEN ???? ISSN 1389-
REFERENCES


REFERENCES

Li:2011:NRA

Lv:2013:NTP

Lukasiewycz:2016:SAO

Li:2018:RBB

Li:2018:TFA


REFERENCES


REFERENCES


Song Luo, Qingni Shen, and Zhong Chen. Fully secure unidirectional identity-based proxy re-encryption.
REFERENCES

Lin:2015:SSE

Lychev:2016:RSI

Lee:2012:IBS

Lin:2015:SSE

Liang:2015:EFC

[LSL12b]

[LSL12a]

[LSG16]

[LSLW15]
Liu:2011:DBA


Liu:2011:NJD


Lei:2013:RSW


Landecker:2012:TBB


Lee:2013:CCM


Le:2014:IMX

REFERENCES

Lee:2014:NDH


Liu:2015:IMB


Liu:2015:MSG


Li:2015:FSC


Lao:2016:BFD


Lysyanskaya:2010:AEC

Anna Lysyanskaya, Roberto Tamassia, and Nikos Triandopoulos. Authenticated


Lin:2011:CNS


Li:2016:LRC


Ludge:2012:NLD


Lucchese:2010:RPT


Lafitte:2011:CBF

Frédéric Lafitte, Dirk Van
REFERENCES


[LWHS17] Zhe Liu, Jian Weng, Zhi Hu, and Hwajeong Seo. Efficient elliptic curve cryptography for embedded de-


[LWL10b] Feng Liu, ChuanKun Wu, and XiJun Lin. Some ex-
REFERENCES

303

Liu:2011:PIA


Liu:2011:PIA

Lu:2012:MMA


Luo:2012:ICB

REFERENCES


REFERENCES


Li:2012:ESD


Luo:2014:ARP


Liu:2015:SDS


Lim:2016:AKE


Lu:2014:DAN

[LY14]


Liu:2015:SAA

[LYL15]

[Zhusong Liu, Hongyang Yan, and Zhike Li. Server-

**Liao:2012:NSM**


**Liao:2010:MPC**


**Li:2013:SSS**


**Luo:2012:LVT**


**Luo:2012:SOCa**


**Liu:2014:PKE**

[Shg+14] Shengli Liu, Fangguo Zhang, and Kefei Chen. Public-key encryption scheme
with selective opening
chosen-ciphertext security
based on the Decisional
Diffie–Hellman assump-
tion. *Concurrency and
Computation: Practice and
Experience*, 26(8):1506–
1519, June 10, 2014. CO-
DEN CCPEBO. ISSN
1532-0626 (print), 1532-
0634 (electronic).

**Liu:2017:ESS**

Chang Liu, Liehuang Zhu,
and Jinjun Chen. Efﬁcient
searchable symmetric en-
cryption for storing multi-
ple source dynamic social
data on cloud. *Journal of
Network and Computer
Applications*, 86(??):3–14,
May 15, 2017. CODEN
JNCAF3. ISSN 1084-8045
(print), 1095-8592 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S108480451630217X.

**Liu:2014:CRA**

Jingwei Liu, Zonghua
Zhang, Xiaofeng Chen,
and Kyung Sup Kwak. Certiﬁ-
cationless remote anonymous
authentication schemes for
wireless body area net-
works. *IEEE Transac-
tions on Parallel and Dis-
tributed Systems*, 25(2):
332–342, February 2014.
CODEN ITDSEO. ISSN
1045-9219 (print), 1558-
2183 (electronic).

**Li:2010:PES**

C. H. Li, X. F. Zhang,
H. Jin, and W. Xiang.
E-passport EAC scheme
based on Identity-Based
Cryptography. *Information
Processing Letters*, 111(1):
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

**Li:2012:ESS**

Fagen Li, Mingwu Zhang,
and Tsuyoshi Takagi. Efﬁ-
cient signcryption in the
standard model. *Concurrency
and Computation: Practice and
Experience*, 24(17):1977–1989,
December 10, 2012. CODEN
CCPEBO. ISSN 1532-0626
(print), 1532-0634 (electronic).

**Li:2016:BMA**

Fuxiang Li, Fucai Zhou,
Heqing Yuan, Zifeng Xu,
and Qiang Wang. Bilinearmap
accumulator-based verifi-
cable intersection opera-
tions on encrypted data
in cloud. *Concurrency and
Computation: Practice and
Experience*, 28(11):3238–
3253, August 10, 2016.
CODEN CCPEBO. ISSN
1532-0626 (print), 1532-
0634 (electronic).

**Masdari:2017:STA**

Mohammad Masdari and
Safiyeh Ahmadzadeh. A

### MacCormick:2012:NAC


### Macrakis:2014:PLS


### Maffeo:2016:UNC


### Michail:2012:EHT


### Moskowitz:2010:ITE

Malkin:2013:SCB


Mangard:2013:KSL


Martin:2010:FWL


Martin:2010:PCC


Mangard:2013:KSL


Mazumdar:2016:CIS


Mashhadi:2017:NMS

Matsuda:2014:IBP


Maurer:2012:CCN


Mayron:2015:BAM


Mazurczyk:2013:VSD


Milo:2011:FGB


Mao:2015:PUA


Malone:2013:MOD

C. V. Malone, E. J. Barkie,

Migliore:2018:PPF


Massolino:2015:OSC


Mukhopadhyay:2011:PEA


Madanayake:2012:BPS


McGrew:2017:IDH


McGrayne:2011:TWH

Sharon Bertsch McGrayne. *The theory that would...*

McKay:2010:SLB


McKay:2011:SLB


McKay:2012:SLC


Mahmood:2018:ECC


Marquez-Corbella:2015:ECP


Mathew:2015:NMB

Jimson Mathew, Rajat Subhra Chakraborty, Durga Prasad Sahoo, Yuanfan Yang, and Dhiraj K. Pradhan. A novel memristor-based hardware security primitive. ACM Transactions...
REFERENCES


[Majzoub:2012:MRH]


[Mansouri:2012:ACA]


[Mansfield-Devine:2015:MIC]


[MD12a]

[MDAB10]


[Mosenia:2017:PTS]


[MD12b]

[MDMJ17]

[MEFO12]

M. Maachaoui, A. Abou El Kalam, C. Fraboul, and A. Ait Ouahman. Multi-level authentication based single sign-on for IMS services. Lecture
Meiklejohn:2010:BRB

Menn:2013:ESC

Meshram:2015:EIB

Mandal:2016:DIW

Moreno:2013:NIP

Moufek:2015:MCB
Hamza Moufek and Kenza Guenda. McEliece cryptosystem based on punctured convolutional codes and the pseudo-random generators. ACM Communications in Computer Algebra, 49(1):21, March 2015. CODEN ????? ISSN
REFERENCES

1932-2232 (print), 1932-2240 (electronic).


Matsuda:2014:CCS


Mou:2013:CBC


Mohd:2015:SLB

Mohd:2018:HDM


Micciancio:2010:FGC


Michiels:2010:OWB


Michael:2016:RNI


Midgley:2010:SEE


Martinez-Julia:2012:NIB


Martinez-Julia:2013:BSI

Pedro Martinez-Julia and Antonio F. Skarmeta. Beyond the separation of


REFERENCES

Malik:2012:AIC


Marconato:2013:VLC


Montecchi:2012:QSE


Mancillas-Lopez:2010:RHI


Mozaffari-Kermani:2010:CSI


Manzanares-Lopez:2012:ICU


Ma:2017:LBI


Madhusudhan:2012:DIB


Meshram:2013:IBC


Ricardo Macedo, Leonardo Melniski, Aldri Santos, Yacine Ghamri-Doudane, and Michele Nogueira. SPARTA: a survival performance degradation frame-


[Moran:2010:BCP] Tal Moran and Moni Naor. Basing cryptographic pro-
REFERENCES


**Mukhopadhyay:2014:EMP**


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

**Monz:2016:RSS**


**McKusick:2015:DIF**


**Minier:2012:RKI**


**Mizuki:2011:ASN**

REFERENCES


Minier:2012:EEC


Meiklejohn:2016:FBC


Mundhenk:2017:SAN


Mironov:2012:IDP


Mukhamedov:2010:IEP


Maimut:2014:AET

[MR14a] Diana Maimut and Reza Reyhanitabar. Author-


[MRS17] Stephanos Matsumoto, Raphael M. Reischuk, Pawel Szalachowski, Tiffany Hyun-Jin Kim, and Adrian Perrig. Authentication challenges in a global environment. *ACM Transac-
Moghadam:2010:DRN


Mendel:2012:DAL


Maitra:2012:NAC


Mroczkowski:2012:CAS


Maitra:2013:DSM


Maitra:2013:HEM

Subhashis Maitra and Amitabha Sinha. High efficiency MAC unit used in digital signal processing and elliptic curve

**Maitra:2013:HPM**


**Miller:2016:RPS**


**Mukherjee:2017:EPP**


**Myers:2012:BCM**


**Myers:2013:BBC**


**Marton:2010:RDC**

REFERENCES


Mosenia:2017:CCA

Martins:2018:SFH

Muhammad:2018:ISU

Mosca:2013:QKD

Morozov:2012:ZKP

Malkin:2011:ECS
Meerwald:2012:ERW

Muftic:2016:BCC

Mundy:2017:CGU

Miri:2012:SAC
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
REFERENCES


Min:2016:RSC

Mishra:2016:AFP

Mannan:2011:LPD

Maes:2012:PFF

Mathew:2012:EIC


Ma:2015:PKE

Sha Ma, Mingwu Zhang, Qiong Huang, and Bo Yang.

Nagy:2010:OTP


Nagy:2010:QCS


Naccache:2012:CST


Naccache:2016:FHE


Naranjo:2012:SAK


Nunez:2017:PRE

David Nuñez, Isaac Agudo,
REFERENCES


**Noureeddine:2013:AMT**


**Nain:2017:SPE**


**Naskar:2012:FIR**


**Naskar:2013:GTL**


**Naranjo:2013:FDA**


[NES+14] Ensherah A. Naeem, Mustafa

**NIST:2013:CSS**


**Nguyen:2014:DDI**


**Ning:2012:DPB**


**Ning:2015:APB**

Huansheng Ning, Hong Liu, and Laurence T. Yang.


REFERENCES

Nagy:2010:KDV


Navin:2010:ETU


Nose:2011:SWA


Nose:2014:SWS


Novotny:2010:TAE


Nichols:2014:CSS

Nguyen:2011:APB


Nguyen:2012:SOU


Namasudra:2017:NSA


Naccache:2010:THI


Nojoumian:2012:SRS

REFERENCES


Noorman:2017:SLC


Nie:2013:CHB


Natgunanathan:2017:PBM


Newell:2014:NCR


Niu:2015:NAS


Nikooghadam:2010:EUE


[OGK+] Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev,
REFERENCES


Ou:2010:CPA


Ogiela:2010:UML


Ogiela:2018:EBI


Oliveira:2012:STA


Ohtake:2012:AAH


Orlandi:2014:SCN


Oppliger:2011:CC


Orejel:2014:E


Ormond:2016:CPR


Ozen:2011:MIS

REFERENCES


[OTO18] Urszula Ogiela, Makoto Takizawa, and Lidia Ogiela. Visual CAPTCHA application in linguistic cryptog-
Ohzeki:2012:NWM

Ortiz-Yep:2014:BSA

Praba:2010:MAC

Pal:2015:SDC

Pal:2016:ACC

Pandey:2014:ACR
Parent:2012:WAI


Park:2012:APO


Pass:2013:USP


Pranata:2013:MDR


Paulson:2010:SDO


Pandit:2012:EFS


REFERENCES

DEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

**Pang:2014:PPA**

**Paul:2012:KSS**

**Pereira:2015:PKE**

**Pippal:2012:SVU**

**Pearson:2011:NWC**

**Persichetti:2013:SAH**


REFERENCES

(Park:2012:IDF)


(Parno:2016:PNP)


(Papas:2012:MLR)


(Park:2010:SIC)


(Pieprzyk:2010:TCC)

Josef Pieprzyk, editor. Topics in cryptology —
REFERENCES


Pointcheval:2012:ACE


Patel:2018:LLA


Premarathne:2015:LDD


Pramila:2018:ICA

REFERENCES

352

www.sciencedirect.com/
science/article/pii/S0164121217302522


REFERENCES


Pande:2013:SMC


Poursakidis:2010:TPC


Puthal:2017:DDK


Niu:2014:RDW


Powers:2014:OSCa

Shawn Powers. The open-source classroom: encrypt-

Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC


P:2018:ABE


Pereira:2016:SHB


Pendl:2012:ECC

Christian Pendl, Markus Pelnar, and Michael Hutter. Elliptic curve cryptography on the WISP UHF RFID tag. Lecture Notes in Computer
REFERENCES

Pyun:2012:IBF

Pathak:2012:PPS

Phan:2012:DDB

Phan:2012:MBT

Papadopoulos:2015:PAP

Pandey:2012:PPS
Omkant Pandey and Yannis Rouselakis. Property preserving symmet-
CODEN LNCS90. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.
com/accesspage/chapter/10.1007/978-3-642-29011-4_22; http://link.springer.
com/chapter/10.1007/978-3-642-29011-4_23/.

Gilles Piret, Thomas Roche, and Claude Carlet. PCARO — a block cipher allowing efficient higher-
order side-channel resistance. Lecture Notes in Computer Science, 7341:311–328, 2012. CO-
com/chapter/10.1007/978-3-642-31284-7_19/.

Raluca Ada Popa, Catherine M. S. Redfeld, Nickolaï Zeldovich, and Hari Bal-

com/chapter/10.1007/978-3-642-25261-7_9/.

REFERENCES

**Perazzo:2015:DRL**


**Pereira:2013:SLC**


**Phatak:2013:SIN**


**Patranabis:2017:PSK**


**Picazo-Sanchez:2013:CRS**


**Park:2013:PPM**


**Papamanthou:2013:SCC**


**Pudovkina:2012:RKA**


**Papakostas:2014:MBL**


**Pei:2013:ARW**


**Papamanthou:2016:AHT**


Papadopoulos:2010:CAR


Phuong:2018:CBE


Pournaghi:2018:NNE


Patsakis:2015:PSM


Qiu:2018:QDS


Qin:2016:VTQ


Qin:2016:STI


Qian:2014:IAF


Qi:2016:SPR


Qi:2016:SID


Qi:2018:BRO

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

Rabin:2010:ACC

Rankin:2010:HLH

Rankin:2014:HEY

Rankin:2010:HLH

Rao:2010:PAA

Rao:2017:SEC

Rauscher:2015:FMT
Ruoti:2015:WJS


Rupp:2015:CTM


Radke:2015:CFA


Reaves:2017:MBM


Rabbachin:2015:WNI


Rao:2017:CFA

Y. Sreenivasa Rao and Ratna Dutta. Computa-

Ren:2016:IBE


Reardon:2016:SDD


Reeve:2015:ARC


Ren:2010:CSH


Roh:2010:BSW


Robert-Inacio:2011:SAP

Frédérique Robert-Inacio, Alain Trémeau, Mike Fournigault, Yannick Teglia, and Pierre-Yvan Liardet.


REFERENCES


Rossi:2015:IBS


Rana:2016:DBV


Roy:2017:LOS


Rangasamy:2012:ERP


Roy:2015:SCP


Ribeiro:2015:QBS

REFERENCES

pdf/10.1142/S0219749915500161.
See also news story [Ano15a].

Ruj:2014:DAC


Ryan:2015:EEVa


Ryan:2015:EEVb


Russo:2015:FPT


Rahulamathavan:2016:UCA


Rodriguez-Vazquez:2012:SCB


Ling Ren, Xiangyao Yu, Christopher W. Fletcher, Marten van Dijk, and Srinivas Devadas. Design space exploration and optimization of path oblivious


Sarkar:2014:PEK


Sarier:2018:MBI


Singh:2018:SDD


Sasaki:2012:DSW


Savage:2013:NSL


Savage:2013:PP

Savage:2015:NVS


Savage:2016:NKP


Safkhani:2017:PSD


Santos:2014:ACD

Shyu:2010:VMS

Srinivasan:2012:RAP

Syta:2014:SAA

Schoenmakers:2010:VS

Schwartz:2011:IMP

Schaathun:2012:MLI

Schneier:2012:LOE
[Sch12b] Bruce Schneier. Liars and outliers: enabling the trust

Schnoor:2012:DES


Schneier:2013:HDD


Schaefer:2015:ECA


Schneier:2015:DGH


Shen:2012:PAS


Shakiba:2010:IID


Souissi:2012:OCP


Shakiba:2014:CCI


Seo:2014:RHI


[Sakai:2016:CDN] Yusuke Sakai, Keita Emura, Jacob C. N. Schuld, Goichiro Hanaoka, and Kazuo Ohta. Constructions of dynamic and non-dynamic threshold public-key encryption schemes with decryption consis-
Sethumadhavan:2016:HEP

Severance:2016:BSB

Seo:2018:AOF

Savas:2014:SMQ

Su:2012:IN

Shabtai:2010:SAP
June 2010. CODEN ????. ISSN 1540-7993 (print), 1558-4046 (electronic).

Schneier:2015:SWC


Sasdrich:2015:ICS


Shu:2014:DAS


Saxena:2016:API


Silva-Garcia:2018:SBG


Sanchez-Garcia:2016:SSA

J. Sánchez-García, J. M. García-Campos, D. G. Reina, S. L. Toral, and F. Barrero. On-siteDriverID: a secure authentication scheme based on Spanish eID cards for vehic-

**Susilo:2016:EDT**


**Shankar:2012:BDF**


**Sipiran:2014:SCA**

Shaolan:2011:EDE


Seyedzadeh:2011:IEA


Song:2015:ADT


Shallit:2010:BRB


Shaw:2013:DE


Shen:2014:LES

Xuemin Shen. A lightweight encryption scheme for network-coded mobile ad hoc networks. IEEE Transactions on Parallel and Distributed Systems, 25(9):2211–2221, September 2014. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (elec-


Simion:2015:RST


Simmonds:2015:DII


Shakeri:2012:RZW


Shin:2017:CGI


Sabri:2011:AFS

Sachnev:2012:IME


Seo:2012:MPM


Scarani:2014:BPQ


Son:2017:NOC


Soupionis:2014:GTA


Sirivianos:2014:LSF

[SKGY14] Michael Sirivianos, Kyungbaek Kim, Jian Wei Gan, and Xiaowei Yang. Leveraging social feedback to verify online identity claims. ACM Transactions on the Web (TWEB), 8(2):
REFERENCES


Seo:2015:AEC [SKH15]

Shin:2017:SSD [SKH17]

Szalachowski:2010:CCG [SKK10]

Stevens:2015:FCF [SKP15]

Singh:2018:MWT [SKS+18]

Scheidat:2012:STT [SKV12]
Schmitz:2012:NAC


Srivatsa:2011:ESA


Schultz:2010:MMP


Somani:2010:IDS

U. Somani, K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. In Chaudhuri et al. [CGB+10], pages 211–216. ISBN 1-4244-7675-5. LCCN ???.

Sun:2016:RSP


Shao:2012:AKP

REFERENCES


REFERENCES


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 ????


Sean W. Smith. Room at the bottom: Authenti-


Pawel Swierczynski, Amir Moradi, David Oswald, and Christof Paar. Physical security evaluation of the bitstream encryption mechanism of Altera Stratix II and Stratix III FPGAs. ACM Transactions on Reconfigurable
Stankovski:2014:CFE


Sadeghi:2010:THI


Safavi-Naini:2011:USC


Seyedzadeh:2014:RCI


Suriadi:2012:PCV

REFERENCES


**Schaumont:2015:IEP**


**Suresh:2015:AGU**


**Serwadda:2013:ELK**

Abdul Serwadda and Vir V. Phoha. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Transactions on Information and System Security*, 16(2):8:1–8:??, September 2013. CODEN ATISBQ.

**Shiaeles:2015:FII**


**Shim:2015:SDA**


**Spafford:2016:SE**

REFERENCES


Sun:2013:IUP


REFERENCES

CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

[Saxena:2010:SGC]

[Saxena:2012:BIT]

[Sopka:2010:BTS]

[Shparlinski:2012:CSD]

[Sendrier:2013:HCE]
Nicolas Sendrier and Dimitris E. Simos. The hardness of code equivalence over $F_q$ and its application to code-based cryptography. Lecture Notes in Computer Science, 7932: 203–216, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-


Sandeep K. Sood, Anil K.

**Spiez:2012:RCT**


**Sahai:2012:DCC**


**Schaffer:2012:EII**


**Schillewaert:2014:CCA**


**Shen:2016:RMM**


**Stallings:2011:CNS**

William Stallings. *Cryptography and network security: principles and prac-
REFERENCES


REFERENCES


Wei Song, Bing Wang, Qian Wang, Zhiyong Peng, Wenjing Lou, and Yihui Cui. A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications. *Journal of Parallel and Distributed Com-

**REFERENCES**


REFERENCES

ISSN 1539-9087 (print), 1558-3465 (electronic).

Seo:2013:PIC


Song:2017:SAM


Shen:2017:RDP


Sui:2014:DAH


Shi:2013:REA


Sun:2017:CPP

Jiameng Sun, Binrui Zhu, Jing Qin, Jiankun Hu, and Qianhong Wu. Confidentiality-

**Shen:2014:ERC**


**Sun:2018:RPP**


**Tsang:2010:BRR**


**Tamayo:2015:AFH**


**Tan:2011:CTA**


**Tan:2012:SLM**

REFERENCES


REFERENCES

Taylor:2017:EBH


Tilli:2015:GCR


Tuan:2010:AWB


Taylor:2011:DR


Tang:2015:CER


Tan:2017:JDC

REFERENCES

Tian:2014:DFS


Tiplea:2014:NSC


Tao:2013:SMS


Terai:2011:BRB


Tassa:2012:SDC


Tewari:2017:CN

REFERENCES


REFERENCES


Tetali:2013:MSA

Tang:2012:RSS

Tsay:2012:VUL

Tsoutsos:2018:EDM

Tang:2015:ECP

Tormo:2013:IMP
Gines Dolera Tormo, Felix Gomez Marmol, Joao

**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.


**Tomb:2016:AVR**  

**Toxen:2014:NSS**  

**Tsougenis:2012:PEM**  
REFERENCES


June 2010. CODEN JSSODM. ISSN 0164-1212.

Tupakula:2015:TES


Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG


Tartary:2011:EIT


Tian:2012:SSB


[UK18] Osmanbey Uzunkol and

Unruh:2015:RQT


Ulutas:2011:MIS


Valamehr:2012:IRM


Unruh:2015:RQT


Vaikuntanathan:2011:CBN

REFERENCES


REFERENCES

Vernize:2015:MNI


Viennot:2014:MSG


Vu:2015:NAN


Vasiliadis:2017:DIS


Vleju:2012:CCA


Vivek:2014:CSC


REFERENCES


REFERENCES

Wang:2010:NSB

Wang:2013:CRA

Wang:2014:IIA

Wang:2018:LRI

Ward:2011:CCM

Watt:2010:IPI
Waters:2012:FER


Watts:2014:ICB


Watts:2014:PYI


Watts:2015:HGA


Wang:2012:PCE


Weisse:2017:RLC


Wright:2010:USP

Charles V. Wright, Lucas Ballard, Scott E. Coull,
REFERENCES


[Wang:2013:SES] 

[Wang:2010:DVT] 

[Wang:2016:SSS] 
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-35606-3_13/

Wang:2012:SPB

Wei:2012:NCI

Wang:2017:DRM

Wang:2018:GAD

Wang:2015:EFF

Wang:2017:DVP
Huaqun Wang, Debiao He, and Yimu Ji. Designated-verifier proof of assets for Bitcoin exchange using elliptic curve cryptography. Future Generation Computer Systems, ??(??):??, ????. 2017. CODEN FGSEVI. ISSN 0167-739X


[Win17] Davey Winder. Re-

[Wang:2016:DRS]

[W-L16]

[Wang:2011:RBM]

[W-L11]

[Wang:2012:MCE]

[Wu:2011:HBI]

[Wang:2012:IRK]
Wei, Yuechuan; Li, Chao; and Cao, Dan. Improved related-key rectangle attack on the full HAS-160 encryption mode. *International Journal of Foundations of Computer Science (IJFCS)*, 23(3):733–744, April 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).


Wang:2012:RTC


Wu:2012:PSC


Wang:2017:CES


Won:2016:PAA


Wang:2015:HAD


Wu:2012:UFS


Wendzel:2015:CME


Wang:2017:PPK


Wang:2016:SEP


Wu:2013:FTR


Wu:2016:CBE


Wei:2015:TPE

Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-


[Wu:2010:IBM] Felix Wu. Law and technology: No easy answers in the fight over iPhone decryption. *Communications of the Association for Computing
REFERENCES

BADMAN 


Wu:2017:SPM


Wu:2012:AST


Willis:2013:IFI


CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Wang:2014:ATF


Wen:2014:MZC


Wang:2011:MMW

Yini Wang, Sheng Wen, Silvio Cesare, Wanlei Zhou, and Yang Xiang. The microcosmic model of


REFERENCES


Wang:2014:NAI


Weir:2012:IHV


Wang:2013:NSW


Wei:2014:IDC


Wei:2016:APS


Wang:2013:BSB

REFERENCES

DEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

[WZCC18]

Wang:2014:CGR


[WYW14]

Wen:2011:DSH


[WZ11]

Wei:2015:CPK


[WZ15]

Wang:2018:AMB


[WZLW13]

Weng:2013:VWI


[WZLW13]
REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-33338-5_8/.

**[XHCH14]**

**[Xi:2012:MDA]**

**[Xie:2012:RAA]**

**[Xiong:2012:PPK]**

**[Xue:2017:CNC]**

**[XJR+17]**
Weitao Xu, Chitra Javali, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. Gait-Key: a gait-based shared se-


[XMLC13] X. Xie, H. Ma, J. Li,


Xiao:2010:TA


Xie:2012:ORI


Xie:2013:SIP

[XWS17] Hu Xiong, Qiang Wang, and Jianfei Sun. Comments on “Circuit ciphertext-policy attribute-based hybrid encryption with veri-

See [XWLJ16].

**Xia:2016:SDM**


**Xie:2014:SCP**


**Xue:2018:SKS**


**Xue:2018:DFH**


**Xiao:2016:REM**

REFERENCES


[XXY+12] Hao Xiong, Cong Zhang, Tsz Hon Yuen, Echo P. Zhang, Siu Ming Yin, and Sihan Qing. Continual leakage-resilient dynamic secret sharing in the


REFERENCES


Yao:2015:LAB


Yuen:2012:IBE


Yu:2017:PDA


Yasuda:2015:MQC


Yan:2016:DEB


Ye:2010:ACC

Guodong Ye. Another constructed chaotic image encryption scheme based on

**Yamada:2012:PBR**


**Ye:2014:NIE**


**Yekhanin:2010:LDC**


**Yoshida:2012:OGT**


**Yu:2012:EPF**


**Ye:2017:VCS**

**Ye:2016:IEA**

**Yang:2018:RKF**
Li Yang, Ziyi Han, Zhenggan Huang, and Jianfeng Ma. A remotely keyed file encryption scheme under mobile cloud computing. *Journal of Net-


REFERENCES


**Yu:2012:IRI**


**YKC+12**


**YKGNK13**


**YKNS12**


**Yoshino:2012:SIP**

Yi:2017:ICM


Yuen:2013:ELT


Yang:2012:WSI


You:2012:DDS


Yi:2013:ETS


Yu:2016:CBE

REFERENCES


Yagan:2016:WSN


Yakubu:2017:SSN


Yu:2017:ACA


Ying:2013:PPB


Yu:2010:PSI


Yu:2011:CLE

Yong Yu, Yi Mu, Guilin Wang, and Ying Sun. Cryptanalysis of an offline electronic cash scheme based on proxy blind signature. The Computer Jour-

[YNQ15] Young:2015:DWE

[YNR12a] Yavuz:2012:BFB

[YNR12b] Yavuz:2012:ECR

[YNR12b] Yong:2011:SPP

[Yoneyama:2012:ORA] Kazuki Yoneyama. One-

**Yang:2017:SAS**


**Yang:2012:EMA**


**Yengisetty:2011:AVC**


**Yang:2012:SAK**

REFERENCES


REFERENCES

Ylonen:2014:SAA


Yang:2011:CCK


Yang:2011:CPK


Yamada:2012:UEW


Yeh:2017:SIB


Yang:2014:IBI

Yang:2011:ACD


Yasuda:2012:ASM


Yao:2010:ASP


Yan:2017:PIS


Yang:2015:RCI

[YWNW15] Hong-Ying Yang, Xiang-Yang Wang, Pan-Pan Ni, and Ai-Long Wang. Robust color image watermarking using geometric invariant quaternion polar harmonic transform. *ACM Transactions on Multime-
REFERENCES

Wang:2011:RDW

Wang:2013:RBC

Yu:2012:NWM

Yang:2010:CRS

Wang:2018:CIW

Yu:2012:SME
Jia Yu, Shuguang Wang, Huawei Zhao, Minglei Shu, Jialiang Lv, and Qiang Guo. A simultaneous members enrollment and revocation protocol for secret sharing schemes. Lecture


REFERENCES


Zhu:2012:JLS


Zhang:2013:RMS


Zhang:2015:PCL


Zhang:2012:TCS


Zhang:2014:GCS

Zhang:2012:AOP

Zhou:2018:SAE

Zhao:2010:PSA

Zhou:2016:HFD
Gao:2012:DES

Zadeh:2015:ASP

Zhang:2012:LDC

Zhang:2015:BYO

Zhang:2015:STR

Zhao:2017:RAS
REFERENCES


Marius Zimand. Simple extractors via constructions of cryptographic pseudorandom generators. *The-
REFERENCES


REFERENCES


**Zhang:2017:FGA**


**Zhang:2016:CAH**


**Zhang:2010:NSS**


**Zafar:2010:GRN**


**Zielinska:2014:TS**


**Zafar:2010:GRN**


**Zhang:2017:PPN**

REFERENCES


Zavattoni:2015:SIA


Zheng:2016:EUV


Zhao:2012:SSS


Zenger:2016:AKE


Zhou:2017:IBB


Zhang:2015:MAA

G. Zhang, J. Qin, and S. Qazi. Multi-authority
attribute-based encryption scheme from lattices. 


**Zhao:2012:SSM**


**Zheng:2018:GDP**

Zhou:2018:TPW


Zuo:2018:CSA


Zhang:2014:NCM


Zhu:2015:PPD


Zwattendorfer:2012:CBL


Zhang:2016:EEA

Liping Zhang, Shanyu Tang, and Shaohui Zhu. An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. *Journal...


REFERENCES

Zilberberg:2013:PCM

Zhang:2015:FER

Zhang:2013:LPP

Zhou:2011:PSA

Zhang:2014:EFH


