
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/

09 March 2019
Version 1.458

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N) [Bai10, YC11], (n, t, n) [LHYZ12], (t, n) [QD16, ZPWY12]. 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]. 2 [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]. γ [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, OS11]. $F_{q^{k^200}}$ [AMORH13]. $F_q$ [SS13]. $\mathcal{NP}$ [HN10]. $GF(q)$ [LPdS10]. LWE [BV14]. μ [Jia14a]. N [FR16]. n × k(k ≥ n/2) [MC11]. O(d13) [KA17]. O(n2) [KS11]. P [DG17]. ±1 [HJM+14]. q [GMS11]. S [LJ15]. t [HJM+11, Ob11]. w [Kre13].

-trimmed [TTL10].

.onion [Boy16].

0.13um [KLM+12].

1 [AAE+14, Ano15b, BH15, Bar16, CGCS12, Ful10, MSas12, SKP15]. 1-58488-551-3 [Ful10]. '10 [Ano10]. 1024 [Bro17, Win17]. 128 [LW11a, Wes16, Ano10].
2D [HIDFGPC15].

3 [ABM+12, jCPB+12, Ful10, LC17]. 30th [Rab10]. 31st [PJ12]. 348-bit [MMN12].
3GPP [FPBG14].


5G [CML+18, FMA+18]. 5th [BYL10, vDKS11].

6 [Ano17b, Bai12, Mur10]. 65th [Nac12].

72 [HYS18]. 768-bit [KFL+10].
al-Qaeda [Mac14, Keb15].

Alan [CS12, Don14, Hel17, LCKBJ12].

Algebra [Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14].

Algorithm [ABCL17, Ano11b, AK14, BGTJ14, BKLS18, CNR14, jCPB+12, ESS12, GKSBI7, JHL12, JSZS12, JHHN12, JL16, KB10, LL11, LT14a, LLL17a, MRL+18, NdMMW16, NV10, RR11, RVRSCM12, WHZ12, WZCC18, YPR11, YH16, ZSW+12, Ant14, BGJT13, BMB16, CG12b, Chm10, EEAZ13, JK13, Jou13, KY10, KHMB13, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, W0GZ+12, XTK10, YWL+17, ZLW+12, ZL12, ACZ16, ZOC10].

Algorithmic [GO17, AY12].

Algorithmics [Gas13].

Algorithms [AMKA17, AB10b, BCG12a, BJ10, CN12, GP17, KRDH13, MR14a, MM17, TKM12, WH18, YS15, ZW15, AGHP14, Fri10a, Mac12, NACLR12, NC13, O010, O018, Xie12].

Alignment [Don14, IA15].

Almost-Tight [GDCC16].

Almost-Universal [BKST18].

Alterna [SMOP15].

Alternating [BKL12, CN12].

American [Sch12a, Mun17].

Analyses [ZPXX17].

Analysis [ABS+12, ARP12, BR17, BBB+16a, BC14, BS14, BKLS18, CFE16, CCG+16, CGL+12, DMR15, FSFW11, GZZ+13, GMC16, GLG12, HC12, HHH+13, HZWW17, HB17, IBM13a, IS12, JT12a, KE19, KOP12, Kre13, LPS12, LTKP16, LCK11, LLW16, LGLL12, MD12b, MAS16, MRTV12, MR10, NDC+13, NSA15, NAL17, PH12a, PFS12, PS14, RZZ+15, Rao10, RBS+17, SK11, SY15a, SR12a, Sh11, SZDL14, SCGW+14, VKC15, WDDW12, YZLC12, Zh15, ZAG19, Aia15, AFC16, AN15, BNY14, CFH+13, CFL13, DMV15, DK17, DW+13, DMT12, FTV+10, FAA+18, FHM+12, HM10, Lan11, MFH13, NLYZ12, PPA18, PL16, QGGL13, RITF+11, SKEG14, TQL+14, TLMM13, Ts013, VS11, Ven14, ZK17].

Analysis-Based [RZZ+15].

Android [Chi13a, EBFK13, FHM+12, SFE10].

Android-Powered [SFE10].

Angle-Based [ZPWW16].

Angular [pNyWyY+14].

Anisotropic [ZZJC14].

Anonymity-Based [HEC+12].

Anonymity-preserving [AIB+16].

 anonymization [XTK10].

 anonymous [TMK11].

Anonymous [CG12a, CZLC12a, CC17, Ch12, DX12, FHH10b, FH18, HLT+15, KP18, LIK+17, LZ14, Muf16, Per13, RSN14, TKS10, Wan14, WX+17, WYML16, ZJ14, ZMW16, AICK18, AT11, BT18, CCSW11, Chi13a, CG11, FSGW12, GTSS19, HL14, ISC+16, LNK+18b, LHM14, LLY15, LY14, MYRR13, QMC17, VS11, WLS14, YZL+18].

ANSI
[Ano15d, BRS17, BMS12, Bro17, CJP12, DSM15, FXP+17, zGXW12, GV14b, GDCC16, HCTTPL+12, HLAZ15, JHL12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LWKP12, LWPF12, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNST17, CJP15, DDFR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYHH14, LWKP14, MBB11, MNP12, NZL+15, SB17, SXL16, WYL13]. attacker [PLGMCdF18]. Attackers [BL15]. Attacks [ARP12, Ano17e, BGK12, BFK16, BKBK14, Che15, CMA14, DGI15, DHLAW10, DHB16, EWS14, GPT14, HLL18, Hay13, HRS16, JSK+16, JWJ+17, KNR10, LLC11, LWZ12, LCJC14, LCL17b, MD12b, PYM+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, WW14, WHN+12, XNG+14, YL17, YCM+13, ZLQ15, ZHS+19, AATM18, BBP13, BVB12, BSR+14, CGH17, dCCSM+12, DCAT12, DJL+12, DK17, Dra16, EA12, FTV+10, FIO15, GPP+16, GBNM11, KM10a, KPS10, LWK11, NDNR13, OF11, PX13, SG+17, TK19, TS16a, TY16b, TLL13, VS11, WWBC14, XWDN12]. attempt [Fel13]. attestation [FQZF18]. ATtiny [EGG+12]. Attribute [AAC+16, AHW+12, BFK+10, Boy13, CD16, CGL18, FHR14, GZZ+13, GSW+16, Gl12, GVW15, HSMY12, Her14, KGP12, LW11b, LW11c, LW12, LJJL12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, OT12, PPA18, PB12, RVH+16, Rao17, SSW12, TMY+17, WDC18, WHL15, XMLC13, XWJ16, XHX+17, ZPM+15, ZQQ15, ZSM17, AHW+12, CDL18, Her14, WHL16, WPS15, YC12, YZZ+16, ZHZ18, YSM12, LW11b, LW11c, LW12, LJLC12, LYY+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, WPS15, YC12, YZZ+16, ZHZ18, YSM12, LW11b, LW11c, LW12, LJLC12, LYY+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TMY+17, WDC18, WHL15, XMLC13, XWJ16, XHX+17, ZPM+15, ZQQ15, ZSM17, AHW+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LY15, LJW+17, LJWY18, LDZW19, QRW+18, RD17, XWS17, YCT15, ZML17]. Attribute-Hiding [OT12, ZWM14]. 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, TCN+17, YYS+16, YXA+16]. August [AB10a, JY14, MV12, Rab10]. Austin [IEE13]. Authentic [HLT+15, SZMK13]. Authenticate [HM12]. Authenticated [Al12, BCO13, BDMLN16, CL16, CNY14, CCS14, CRE+12, DS11, EAA12, ESP12, FVS17, FLL12, GPP+12, GL12, GZ12, HC12, HL10a, HCL+14, HEC+12, KMY18, LHKR10, LY16, LHL1b, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHKS14, MSU13, PT16, Sar10b, Smi11b, Tan11, TW14, XLM+12, XCH+12, XGLM14, XZLW15, YS12, YLJ13, YRT+16, Yon12, ZPZ+16, ZXH16, AIB+16, CT13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HWB12, HL11, HPY10, ISC+16, KMTG12, LWS10, LHH11, LML+13, NCL13, Nos11, Nos14, PPT15, PJ18, SMB10, TCS14, Tso13, TKHK14, WZM12a, WZM12b, WTT12, XWXC14, XCL13, XWZ+18, YCY12, YZZ+14, YZL+18, ZT16, ZXWA18, ZG10, ZZZC15]. Authenticating [BS12, CHX13, GRL12, OKG+12, RPG12, WY12, ZCWS15, Cer18, LFGGCCRP14, PGLL10, ZLDD14]. Authentication [ASO14, AAZ+16, ACAT+15, AUMT16,
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_ /:.,;!?@#%^&*()[]{}<>~`|\+=\[]
BJR⁺14, KKK⁺16]. Automatic
[MMP19, WW12]. Automation
[BGK12, IEE11a, KPP16]. Automotive
[LMS16, MPM⁺17]. autonomous [BT18].
Auxiliary [DMS⁺16, DL12, GHWH17, XXZ12, YCZY12]. Auxiliary-Input
[XZ12]. Availability
[CK11, ADF12, CFVP16]. Available
[Ano16d]. AVC [JSZS12, JH1N12, LW13c]. average [Lim11, YL11]. avoid [CFZ⁺10]. Avoidance
[RVH⁺16]. avoiding [BHCdFR12]. AVR [LPO⁺17]. award [Ano16g, Orm16]. Aware
[BCF16, LMMH14, LSL16, QLL17, Wan13, ZFH⁺18]. 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]. Balanced [YTP11]. balancing
[FXP12, PRN⁺19, Zha15a]. Ballots
[CW12b, LH12]. balls [Svo14]. band
[MMSD13]. Bandwidth
[GST13, NR11, LLZ⁺12]. Bandwidth-Efficient [LLZ⁺12]. Banking
[KSD⁺17, RBS⁺17, KV⁺E18]. banned
[Ev16]. BANs [BLL⁺19]. Baptiste
[Dew11]. Barbara [Rab10]. Barcodes
[Wy12]. Barrier [JR14, KS11]. barriers
[LKKL13]. base [MS12a, XSWC10]. Based
[ADM12, AGW15, ASM12, AAC⁺16, ABC17, Ano11b, AOS15, AYS15, BWL16, BL12, BBB⁺16a, BSSV12, BHG12, BKPW12, BRT12, BHH⁺15, BS13b, BFK⁺10, Bon12, BSJ15, Boy13, BKJP12, BDH11, BCF⁺14, CMSL15, CLL16, CGM14, CCM17, CSH⁺18, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST⁺17, CGL⁺12, CDD13, CGY⁺13, CD12, Chi12, CK18, CD16, DSSM14, DA12, DLZ⁺16b, EM12, EKB⁺16, FM15, FHH10b, FHR14, FZ14, GM10, FVS17, FSX12b, FSX12c, FSX12a, GWWC15, GZZ⁺13, GSW⁺16, GV14b, GI12, GY13, GDC16, GVW15, GJJ15, GJZ17, HZC⁺12, HSMY12, HSM14, HL10a, HZX15, HCPSLB12, HKL⁺12, HG12, HM12, HSA14, HPO⁺15, HKR⁺18, HGT15, HLC⁺14, HLN⁺10, Hui13, HRS16, HBG⁺17, HE⁺10, HP12, JTH⁺16, JH1N12, JEA⁺15, JKH12, KS18, KZG10, KK12, KKA15, Kha10, KLY⁺12, KSSY12, KPKS12, KRB12, KAK18, KS15]. Based
[LMGC17, LMG⁺18, LTKP16, LSL12a, LSL12b, LW11b, LW11c, LW12, LH12, LJLC12, LYZ⁺13, LHL⁺14, LTH⁺15, LLC⁺15, LTZ16, LLL⁺17, LPL15, LSL15, LAL⁺15, Lnl15, LP12, LNZ⁺13, LCCJ13, LWCJ14, LNX15, LHL15, LW16, LPO⁺17, LGPRH14, LDB⁺15, LD13, LSC12, LBR12, LLH18, MWZ12, MLO17, MEFO12, MCD12, MV12, MD12b, MBC15, MK1N13, MZ17b, MCS⁺15, MMS17b, MKF⁺16, MCF17, Men13a, MST18, Mor12, MSKRJ17, MK1A17, Mu16, NC12, NX17⁺1, NXB13, NLLJ12, NLY15, pNWyY⁺14, OT10, PB12, PTT16, PYM⁺15, PD1H15, PPS12b, PYS18, PG12, PAS13b, PRNC17, RVH⁺16, RZZ⁺15, RS16, Rao17, RR11, RDZ⁺16, RVRSCM12, RW12, SS12, Sar18a, SS13, S17, SJ12, SGP⁺12, SP15b, SSA13, SRA17, SH15, SGH15, TB18, TKR14, TWZ11, TW12, TZW⁺12, TYM⁺17, TSH17, TT12, TTH15, TC10, VDB⁺16, VAG15, Vle12, WY10, Wan10]. Based
[WSSO12, WgMW12, WYW⁺13, Wan14, WZCC18, yWYXZ⁺18, WDC18, WLH15, WCL⁺18, WT10b, WMS⁺12, XNG⁺14, XNRG15, XXZ12, XML13, XQL11, Xio12, XGLM14, XWLJ16, XJW⁺16, XJR⁺17, XHŽ⁺17, YE12, YZLC12, YZX⁺12, YFG15, YTS12, Ye10, Ye14, YH16, YTH17, YYO15, Y⁺17, YKNS12, YHK⁺10, YMWS11,
based [DLN13, Dra16, uHAN18, EZ15, FH13, Far14, FAI14a, FAI14b, FIO15, Fay16, FHZW18, FNWL18, Gal13, GJ13, GMRT15, GKCK11, GJMP15, GCS AddP11, GMS11, GLL18, HSH11, HT11, Ham19, HGWY11, HSM13, HZC14, HZL18, HF14a, HWDL16, HZW17, HZW18, HBBRN16, HLR11, Her14, HBW12, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HYF18, HPY10, HKHK13, HCC10, Hwa11, IMB17, IM14, ISC16, IB11, IA15, IOV18, Jac16, JNUH17, JKAU19, JK13, JLT12, JZS10, JMW16, JSMG18, KPP16, KK13, KM10a, KNMB13, KKG14, Kim11, KGO10, KLI1, KSH18, LXL12, LLZ16, Lalu2, LLC10, LK14, LH10c, LZJX10, LNM11, LMJC11, LLK12, LXMW12, LKAT12, LLHS12, LNLK13, LXJ14, LCL15, LZY16, LFZ17, LNK18a, LWK18, LCT14, LFWS15, LLM19, LPdS10, Lin14a, LLY12a, LW10, LSQ11a, LSQ11b, LWK11, LW13b, LZC14, LPZJ15, LTL15, LTY15, LW17, [based [LJYW18, LDZW19, LW18+10, LL16a, LW13c, LWY12, LY14, MCN18, MCP15, MJGS12, MJJS13, MLM16, MMZ12, MNI13, Mes15, MBB11, MO14, MHT13, MG15, MS17, NR11, NCL13, NZL15, PPPA18, PYH18, PLPW13, PTK14, PW10, PGLL10, PPB16, PLGMCdf18, PS14, PL16, PKA15, PC14, PR12, QZDJ16, QRW18, QYW16, QMW17, RD17, RG10, RS15, SPLHC14, SGGCR16, SI12, SYL13, SE14, SE16, SH11, SN11, SMN14, SR10, hSSZ15, SCKH10, SA16b, SAAF11, SWW16, SSS11, SKEG14, Sun16, SM16, SHBC19, SS11, TPL16, TQL14, Tan15, TH16, TTL10, TPKT12, TKHK14, VS11, VN17, WWYZ11, WWYY11, WLD11, WLFX17, WMX17, Wan18, WGZ12, WHHL16, WS14, WS12, WTT12, WOLS12, WCH18, XHH12, XZW16, WX12, XCL13, XWS17, XHCH14, XZW18, XMHD13, XHM14, YWL17, YqWqZC13, Yan14, YTM14, YCC16, XYA18, YCT15, YLS12, YMSH10, YKC12, [based [YLZ16, YXA16, YL11, ZZKA17, ZLW12, ZCL14, ZT14, ZTZ16, ZML17, ZZ12, ZHI17, ZL12, ZVH14, ZDW16, ZLY19, LZJX10, HZC14, MM12, PP11, ZBR11, Kat13, [Based-Encryption [ZHW15], Bases [EVP10, TSH14, FES10], Basing [Mat14, MN10], Basis [BNA15, ERRMG15, CG12b, Har15, LLP18, Tam15], Batch [ZPXX17, AGHP14, CCG10], batch-based [CCG10], Batters [Chi13b], battles [Ano15e, Ano16f, Sch15c], Bay [Ano10, DDS12], Bayes [McC11], Bayesian [WYW13, ZLW17], Be [DSMM14, Par12a, YM16, AZH11, Ana14, Eve16, Ree15, RK11], BeagleBone [Cri16], Beat [LTKP16], BECAN [LLZ12], Becomes [Bra13], been [Ana14], before [GST12, Goo12], Beginning [Chu16], Behavior [GSC17], behavioral [HT11], Behaviors [GAF15], Behind [Fre10], Beijing [BYL10, Yan10], Beissinger [Ayu12], Belief [BT12], Bell [JEA15, QD16], Benchmarking [MKAA17], benchmarking [ZZKA17], Benefit [HB14], benefits [Wat14a], Benford [AOT13], Bessel [GJ13], best [Cha13c], Beth [CTHP13], better
Between [KA18, LRVW14, SAKM16, CLM+12, HLR11, KPP16, Kim16, PBC14, WDD15]. Beyond [LST12, MJS13, TS16b, FNP+15, JR14].


Bidirectional [GMNS15, GH12]. bifurcation [SE18]. Big [MLO17, Mal13, MMS17b, PNRC17, YDY+16, ZLW+17, FS18, LSB14, QCX18, Tan17b, WS14].


Bio [OK18, GPVCdBRO12]. Bio-inspired [OK18, GPVCdBRO12]. BioAura [MSKRJ17]. biographical [Maf16]. Biometric [Alp18, ATI+10, BCTPL16, DWB12, JN12, KHB13, LGM+16, May15, NGAuHQ16, Sar12, Skv12, Vet10, AHM+18, DIMIT12, GCSÁdP11, HT11, Ham19, LK12, LTC+15a, MLBL12, Sar10a, Sar18a, SR10].

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

biometrics-based [FHZW18, LXLY12, LH10c, LNM+11]. biosensor [Kim16]. Birhäuser [Sha10]. Birthday [LST12, SXL16, Nac12].

Birthday-Bound [LST12]. Bit [CG14a, GV14b, HG12, HS18, LJK17, LPO+17, NIS12, Ros11, YLL+12, APPVP15, KS11, KFL+10, MN12, PLsVL10, RH10, TWZ+12, VN17]. Bit-Wise [CG14a].


Black [BR14, CPS16, HHP17, KOS16, KMO14, MSas13, JB11, Rja12, SS10b, DD13, SK14, YSC16, ZZ12, Crit16]. Black-Box [BR14, HHP17, KMO14, Rja12, SS10b, KOS16, MSas13, ZZ12]. Blackbox [MSas12, SS12a].


Block [AMVZ12, BRS17, BSS+13, BFMT16, BDGH15, BCG+12b, CPW12, DWWZZ12, EGG+12, FXP+17, GL/S12, GT12, GST12, GN12, IS12, KR11, KWS+12, LWZ12, LJ17, LGL17, LG/LL12, LWKP12, LW/FP12, MCD12, MRT/2, OGK+15, PHI/2a, PRC12, Pud12, SGP+12, SSA13, WW12, YCL17, ZSW+12, BNY14, Jeo13, KM11, LPZJ15, LC13, LYHH14, LWKP14, MP12, MV15, MHY+18, PL16, Sar11, S/11, SKK10, TQL+14, Tan17a, WB12, WWBC14, ZSW+12, JP12]. Block-Parallel [MCD12]. Block-Wise [SSA13].


Body [LZCK14, ASO14, KP18, LK+17, SGJ+18]. body-sensor [ASO14]. bogus [XWDN12].
Bombe [Bur11, Car10]. Bonebrake
[SS10c]. Boneh [TK19]. Book
[Ano15b, Ano17b, Ayu12, Bar12, Dew11,
Full10, Joh10, Keb15, Kob10, Low12, Mei10,
Mur10, Sch15a, Sha10, SR14, Ter11, Sto12].
Boolean [ACZ16, AS17, CW14a, DQFL12,
FY11, LVV11, WT13, YCC16].
Boolean-based [CW14a, YCC16].
Bootstrapping [BGV14, GM14].
Border [LGM16, ZTSR12].
BotMosaic [HB13].
Botnet [NSA15].
Botnets [HB13].
Bottom [Smi11b].
Bound [LST12, TK19].
Bounded [GVW12, GJO13, PDNH15, QZZ18,
SS12a, ZYT13, IM14].
bounding [PYH18].
Bounds [Jia17, LJ15, SNJ11, SS10b, Sha10].
Bouzefrane [Ano15b].
Box [BW16, BCGN16, BR14, CPS16, HHP17,
KMO14, Mic10b, Rja12, SS10b, Kos16,
LRW13, MSas13, RMP10, SGFCRM18, 
ZZ12, ZSW18a].
Boxes [NN12, LJ15, SS11].
BRAMs [DG10].
Branch [EPAG16]. Branchless [RBS17].
Brave [KM10c].
Breath [SD12, JB11].
Break [Ayu12, Win17].
Breakers [Sti15, Mun17].
Breking [AP13, CN12, Cop10a, KS11, TPL16,
WgMdZZ12, Ant14, Bri11].
Breaks [Ano17e].
breakthrough [Goo12].
breath [LSR13].
Breathing [CH18].
Breathing-Based [CH18].
Bregman [CCZ13].
Bribery [CW12b].
Bringing [LRVW14, TMGP13].
Briggs [Bai12].
Bring [Zha15a].
Bringing [Ano15c, OYHSB14].
Britain [Ald11].
British [And13].
Broadcast [BS14, GMVV17, HMR14, KH10, LMG17,
LMG18, PSM17, PPS12a, WQZ16,
XJW16, Yan14, ZHW15, CPPT18, DLN13,
WWYY11, XWDN12, YMM13, ZWQ11,
ZZ12, Zhu13].
Broadcasting [O012, MK11, OCGD11, YY11].
broke [Bat10, Hea15].
Broken [MDAB10].
Broker [TKR14].
Broker-Less [TKR14].
browser [GIJ12].
browsers [Ree15].
Bruce [Sev16].
Brute [CJP12, JR14, CJP15].
Brute-Force
[JR14, CJP12, CJP15].
BRW [CMLRHS13].
BTC [CLF11].
BTC-compressed [CLF11].
Buchwald [ABJ13].
Bucket [BKKV10].
Bug [Chi13b].
Building [BPS16, KMP11, MJS13, Sev16,
WL11, LCKBJ12].
Burdens [Bla12, SR14].
Bus [AN17].
Business
[LDB15].
Buyer [Fra16, KJN16].
Buyer-Friendly [Fra16].
BYOE [Tan17a].
byte [Hof15, Hof16].
bytes [PBC14].
Byzantine [KS11, LLKA19, YGKG13].
Byzantine-resistant [YGKG13].
C [AD12, ACZ16, C1G212a].
CA [ACM11, D12b, Kai11, Lin14b, Pie10, Rab10].
CABA [MSKR17].
CABE [XH17].
Cache [AB15, ADR18, DKMR15, HLAZ15, SY15a, DJL12, DK17].
CacheAudit [DKMR15].
Caches
[LLG16, CDPLCA16, DJL12].
Caching [ADR18, HLAZ15].
cackled [Bai12].
CAD [PGL10].
Caernarvon [KMP11].
Calculus [MR10, Jou13].
Calibrated [LC15].
California [Ano10, IEE11b].
Call [Ano16a, Ano16b, Ano16h, CS14, CRM10].
Call-Back [KRM10].
Calls [Mur16].
cam [PKS18].
Cambridge [ACM10, PJ12].
Camel [O15, LWP12, LWP12, LWP14, SEHK12].
Camellia-192 [BLO15].
cameras [MKH12].
Can [Alo12, AZH11, Bar15, D1M14, YM16,
RK11, Rus15, Sto12, GMVV17, LMS16].
Canada [JY14, MV12].
Cancellation
[DLMM18].
Candidate [GHH16a].
candidates [ABM12].
canonical [Bull10a].
CANS [HW10, LT11].
Can’t [RAZ15].
CAOVerif [ABF14].
Capabilities
[RGBF12, Lop15a].
Capability
[IA15, LZZ17].
Capability-Based
[LZ17].
Capacity
[TODQ18, XNRG15, YWW10, CLZ17,
GZH12, PW12, WH13].
Capacity-aware [TODQ18].
Capacity-Raising [YWW10].
Capitalism
[Fid18]. **CAPTCHA** [OTO18, SKEG14]. **CAPTCHA-based** [SKEG14]. **Capture** [NYR14]. capturing [PKS18]. **Card** [BDFK12, HMR12, HCL+14, PDT12, Ano17c, CLHJ13, GLIC10, LNKL13, Mar10b, Cho10, SD12]. **CARDIS** [GLIC10].

**Cards** [BSJ15, LA10, PWVT12, WgMdZIZ12, WgMW12, CHS11, HCC10, KY10, LH10c, LNM+11, LXMW12, MM12, SGGCR+16, YZZ+14, YSL+10]. care [FHV16]. Carlo [CR12, FVK17]. Carol [Xie12]. Carry [GWM16]. Carved [LC15].

**Cascade** [WDG18]. Cascading [GT12].

Case [Ano17c, DR11, SBS+12, SY15a, YL17, LKKL13, MD12a, SS17]. **Cash** [YMWS11]. Casting [CW12b]. cat [Pow14].

**Catalog** [AHS13]. CBA [KRM+10]. **CCA** [AHS14, BWLA16, CCL14, LTZY16, LSW15, MSas12, PDNH15, SYL13, SLZ12, yYqWqZC13, ZY17a, ZSW+18b].

**CCA-Secure** [BWLA16, CCL14, LTZY16, SYL13, yYqWqZC13, ZSW+18b]. **CCA1** [MSas13]. **CCA2** [Gal13, GV14b, LLW16, LLSW16, MVVR12, RG10, ZZ12, ZY17b].

**CCA2-secure** [LLW16, ZY17b]. **CCM** [SKK10]. **CDF** [Ara13]. **CDH** [PDNH15, ZG10]. **CDPS** [LLL+17b].

**CDTA** [YFT17]. cell [LLY+12a]. cell-counting-based [LLY+12a]. **Cells** [DSB16]. **Cellular** [dRSdlVC12, FMA+18, HBBRM+16, HCM11, KRM+10, SS11, WOLS12].

**Censorship** [DRS16]. centralized [NACLR12]. centre [McK10, McKi11, Pal16, ISC+16]. **Centric** [DLZ+16b, Vie12, ZVG16, AHM+18, BLV17, BPP10, PN10]. **centroid** [LWY12].

**Centuries** [Gri15, M-G11]. **Century** [Wes16]. Cerf [Cer15, Cer18]. **Certificate** [GWWC15, HP12, LTH+15, WMS+12, YLZ+16, BJR+14, GLL+18, Lan13, LL16a, MBF+13, NPH+14, JB11].

**Certificate-Based** [GWWC15, HP12, LTH+15, WMS+12, YLZ+16, GLL+18, LL16a]. **Certificateless** [CT18, GWWC15, IL15, LZCK14, SJS14, TCL15, WMS+12, YT11a, YT11b, HPC12, JXLZ15, LL16b, SGJ+18, ZQWZ10, ZY17b].

**Certificates** [Muf16, SC12, GIJ+12, HREJ14]. **Certification** [LDB+15]. **Certified** [ABBD13, CLL16, STC11, HL14, LH13, XWXC14]. **CertShim** [NP+14]. chaff [KHMB13].

**Chain** [EAA+16, FVK17, KPW13, QZL+16a, QZL+16b, YFT17, CR12, CL16, SJWH+17]. chaining [EA11]. **Chains** [JSK+17, HLYS14, JCHS16]. **Challenge** [AD12, GHS14, YDH+15, ZCC15].

**Challenges** [CN12, FS15, Fra15, LLGJ16, MRS+17, PCV+17, SBV14, ALL+18, KJN+16, WS14].

**Changes** [ALL+18]. change [ZWT13]. **Changeable** [FGM10, ZCL+12]. changed [Mac12]. **Channel** [AN17, ASN11, CDK+10, CBL13, EWS14, GWM16, GPT14, KOP12, LG14, NDC+13, PRC12, SG15, TTI12, YL17, ADG16, BVIB12, CPPT18, DMWS12, DJL+12, JLT+12, MFH13].

**Channels** [ASN12, BGN17, DKMR15, EPAG16, LW13b, SR11, RVRSCM12, SR11, SBS+11, SY15].

**Chaotic** [BGGH11, IAD10, Ye10, GCH15, ISG+16, KLW+16, LWK+18, LW10, NES+14, WZG+12, ZT14].

**Chapman** [Fu10]. **Character** [SS12b]. Characteristic [BGJT14, SR10, BGJT13, Jou13].

**Characterization** [ALR13, BS13b, DPCM16, YZLC12, DDD14, PLGMCdF18].

**Characterizing** [Ash14, JR13, MPJ+16].

**Chattarjee** [Kat13]. cheat [WS12]. cheat-preventing [WS12].

**Cheater** [KI11, Ob11]. **Chebyshev** [LPdS10].
SLM10, Vai11, Vle12, XMLC13, XWLJ16, YE12, YHL16, ZLDC15, AaBT16, AAZ+16, And13, CJI5b, CSTR16, DKL+16, DWZ12, HSM13, HYS18, Geo13, JSMG18, KKA14, KKM+13, KKM+14, KB+17, KH18, LKX+14, LYL15, LHL15, MS12a, NR17, NCCG13, PPA18, PF11, PKA15, QZD16, QRW+18, Rao17, Tan12b, WSC14, Wan18, WDKV19, WLS14, WL19, XXX15, XY+18, YHM18, YQL17, YY11, ZWS+18, ZLY+19, ZSW+18b, YXA+18. conceal [EIAZ13].

Concept [TMC15].

Conceptual [PMZ12, SPM+13, TSH14].

Concrete [BS14]. Concurrent [CLP13a, FCM14, GJO+13, MKRM10, OOR+14, AKG13, SRB+12, XLIW16].

condition [TD14]. Conditional [HBCC13, KPW13, LLG15, LSLW15, MLOI17, XJW+16, FSGW11, FSGW12, HWDL16, HYF18, IOV+18, LCT+14, PZBF18, SKB+17, Tan12b]. Conditionally [ZJ14]. Conditions [Ano17d]. Conference [BC11, CGB+10, Che11, Cra12, Dan12, Dun12b, FBM12, GLIC10, IEE11a, JY14, LCK11, LW11a, LTW11, Lin14b, PJ12, SNJ11, Sah13, Yan10, AB10a, Abe10, BYL10, BL10, Gill10, GG10, HWG10, Kia11, LH10a, Pie10, Rab10, vDKS11]. Confidential [HS11, AZPC14].

Confidentiality [BFK+10, HLLC11, OFMR16, SZQ+17, WDDW12, Bia12, CHX13, ZHT16].


Consecutive [Tan12a]. Consensus [ABCL17, JSK+17, LLKA19].

Consequences [Ess17]. Consideration [CJP12, CJP15, KM10b]. Considerations [KD12b]. considering [MLMSMG12].

Consistency [BCK17, SES+16]. Consolidated [KKA14]. Constant [App14, AEHS15, CWWL12, KOTY17, KHP16, KMO14, LP11, Pan14, ZMW16, AHL+12, DWZ12, LCT+14, SGM16].

Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHL+12, LCT+14, SGM16].

constants [DWZ12]. Constraining [BSJ15, CSH+18, EAA12, JMG+16, YNR12a, Yon12, DMV15, KAS15, LLZ+16, LCL+17a].


Construction [BWLA16, DF11, EM12, FZT14, GWWC15, HHP17, KMO14, MSas12, Rog16, Sar10b, ST14, WZ15, WCL+18, WMS+12, XH+17, LFZ+17, MSas13, SA14, YWL+17, YT11b, YKC+12, ZCLL14].

Constructions [BCF+14, DQFL12, HL10b, KOTY17, SNJ11, SES+16, CIZ15a, CGKO11, NAL17, Zin10].

Constructive [Mau12, WB12]. constructs [BP10]. Containing [XWDN12]. contemporaries [LCBKJ12].

Contemporary [Opp11]. Content [ADR18, BCP14a, MHT+13, PMZ13, PZPS15, WHZ12, WZXL12, YT12, ZZ+11, GPX+12]. Content-based [MHT+13].


Continual [BKKV10, XZY+12, YZ12, YCZ12].

Continual-Leakage [YZ12]. Continually [DLW11]. Continuous [ACAT+15, BCF16, DHLAW10, uHAN+18, FMN14, MSKRJ17, PYP10, Sch15b, Yan12, ZY17a, ZYM16, BTW15, PLGMCdF18].

Continuous-Tone [Yam12]. contract
[MMP19, Men13b]. contrast
[DDD14, GLW13, LWL10a, MM14a].
Contributory [WQZ+16]. Control
[ATS15, BFK+10, DLZ+16b, HHS+15,
LGZ+16, MM17, MK12b, NA10b, QZL+16a,
RSN14, SGC14, TBCB15, XMLC13, YTH17,
ACK+10, AMHJ10, CLH+16, CO11, Cra11,
FNWL18, FS18, GHD19, JAS+11, LCL+17a,
LCL+15, NZM10, QCX18, Sch15c, SA15,
Tan12b, Wan18, XHH12, ZML17, ZVH14,
ZWS+18, ZFH+18]. Controllable
[FIH13, ZLDC15, ZHT16]. Controlled
[FMTR12, WP17, Har16]. Controller
[GMV17]. Controllers [AMH+16].
corresponding [YT12, MHT+13]. Copyright
[CG12a, SSW12]. Credible
[ZW15]. creditors [Pea11]. criticism
[OdH12]. Criteria [PYS18, ZZKA17].
Criteria-Based [PYS18]. crittografia
[Sac14]. CRM [LHM+15]. Cropping
[SR12b]. Cross [AKK+17, CLY14, DSB15,
LHM+15, MV16a, YGFL15, YZL+18,
ZXH16, ZTSR12, SS17, der10].
Cross-Border [ZTSR12]. Cross-Domain
[CLY14, YZL+18]. Cross-group [AKK+17].
Cross-Layer [LHM+15, ZXH16].
cross-matching [SS17]. Cross-Site
[DSB15]. Crossword [Mar10a]. Cryptis
[GSC17]. Cryptanalysis [BW12, Bor10,
CWP12, GCGS12, DG12, DJG+15, Far14,
GST13, Gor10, Hin10, IOM12, Jia13, Kha10,
KN10, KWS+12, LH10b, LNM+11, LJF16,
LJ16, MWZ12, NXB13, OTD10,
PSOMPL13, SPLHCB14, SM10a, SM10b,
TY16a, TG17, Vua10, Wag10, WWYZ11,
WYYY11, WSSO12, WYW14, XQL11,
YCL17, YMWS11, AP11, BMB16, BKR11,
Cryptography-Related [Cil11]. Cryptol
[BC11, Bro11, Dun12b, LW11a, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPGP14, 
Gil10, GG10, Kia11, LH10a, MZ17a, Pal16, Pie10, Rab10, HWG10, LTW11, Kob10].
Cryptomania [Gen13]. Cryptoprocessor
[GV14b, SWM†10]. Cryptosystem
[CCT†14, LH10b, SWM†10, BS15, Chi13a, 
Gal13, GV14a, GLB†18, IB11, MM13, 
MG15, NZM10, SvT10, yYqWqZC13, YY11].
Cryptosystems [ADI11, OTD10, PSM17, 
BNST17, FWS13, SA16b]. Csec
[AD12]. CT
[Dun12b, Kia11, Pie10]. CT-RSA
[Dun12b, Kia11, Pie10]. Cube
[MS12b]. Cubic
[RV12, VM14]. Cuckoo
[BHK13]. CUDA
[DLV16]. cultural
[Mid10]. Culture
[Bla12, SR14]. Currencies
[TS16b]. Current
[DP17, GCK12, FPBG14]. Curse
[GG11, HB14]. curvature
[GJ13]. curvature-feature
[GJ13]. Curve
[ADI11, ARM15, BJ10, GPT12, LGH†17, 
LWHS17, PPH12, SG15, AMN18, BL14, 
BL17, BBB16b, Cho14, Far14, FWS13, IB11, 
KK10, Krc13, MCN†18, MS13b, NZM10, 
SKH15, WHJ17, JL16]. Curve25519
[SG15]. Curve41417 [BCL14]. Curves
[AK14, BWR12, DW12, LL11, LT14a, 
MST18, YTS12, BL17, BP18]. Customization
[ODH12]. Cyber
[LJ†14, GHD19, HZW18, KSA16, QMC17].
Cyber-Espionage [LJ†14].
cyber-physical
[GH19, HZW18, QMC17]. Cybernetica
[Ano17c]. Cybersecurity
[DF16, Hel17, Lan17, LRVW14]. Cycle
[HG12, KU12, MNK13]. Cycle-Based
[MKN13]. Cycles
[WBA17, CLCZ10]. Cyclic
[ODT10].

D [AP10, CG12b, DBPS12, DWWZ12, 
EAA†16, GZH12, KWS†12, LJ17, LJ15, 
MCDB12, MKH†12, PGLL10, RS16, SGS14, 
SRK†17, WSSO12, WY12, tWmC12, YI14, 
YPRI17]. D-Based
[WSSO12]. D-like
[LJ15]. D-PUF
[SRK†17]. Dana
[Ano10]. Dandelion
[VFV17]. Dangerous
[HLW12, GLJ†12]. Dao
[FMS12a]. Dao-Fa
[FMS12a]. Daoism
[FMS12a]. Darel
[Xie12]. Darmstadt
[FBM12, Sen10]. DASH
[KCC17]. Data
[Ano13c, ADT12, Bar12, BJL16, BCD†12, 
BJL12, BW12, BKLS18, CWL†14, CMLS15, 
CCW†10, CSV15, CCT†14, CLW16, DDS12, 
Dan12, DR12, DMS†16, DA12, DCA18, 
DLZ†16b, EKB†16, FMY15, FPY15, 
FRS†16, GT11, HSM14, HLT†15, HK14, 
IBM13a, KRDH13, KG16, LLZ†17, 
LWCJ14, LLZ†12, LZC†12b, MLO17, 
Mal13, MMS17b, MM14b, NNA10, NR12, 
PD14, PSM17, PH12b, PNRC17, QZL†16a, 
QZZ18, RCP†18, Rea16, RSN14, SGG18, 
SAKM16, Sar10b, SMSK18, SP15b, SKH17, 
Sia12, SL10, TCN†17, Tan15a, Vai12, 
VSV15, WZCC18, XNK15, XWSW16, 
YDY†16, YMC†17, ZXL16, ZPKX17, 
ZRT15, ZLW†17, AP10, ASO14, Ana14, 
Ano11a, ARA13, ADH17, ALL†18, BLL†19, 
BTPL15, BC18, BKV13, CDGC12, 
CLH†16, CDF†10, CDL18, DFJ†10, 
DTZZ12, DRD11, ED17, FS18, GHD19, 
Gen10, GLB†18, GZS†18, HSM13, 
HWK†15, HMCK12, HH16, HYS18, HYF18, 
JHCC14, Kim16, KH18, KWH16]. data
[LSBN14, LT14b, LXK†14, LZY†16, 
LLL†17b, LHL†18, LFWS15, LAL†15, 
LCW†16, LZC17, LLL†18, LL16a, LHA†16, 
MHKS14, OOI18, OSSK16, QCX18, Sch15c, 
SYY†17, SAR18b, SWV†17, Tan17b, 
TMK11, TKMZ13, LTH13, LWS14, 
WZLW13, WS14, WL19, XXX15, XWZ†18, 
XY†18, YVS†16, YQL17, YXAX†16, 
YNX†16, ZZKA17, ZMM†10, ZWY†13, 
ZHT16, AEH17, HLYS14, Sch15c].
Data-Centric [DLZ†16b].
Data-Classifiers [KG16].
Data-Compression [DA12].
Data-Minimizing [BCD†12].
Data-Oriented [NNAM10]. Database [BTHJ12, SBV14, WCL+18, BL11, JC14, LW13a, PRZB12, Suc12, YXD18].

Databases [FCM14, HPC10, JKZeY12, Kaw15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12], datacenters [PRN+19]. Dataset [SP13].


Description [WH18, PLS11]. Design [AMN18, Abe12, ARH+18, AIB+16, ADD10, AUM16, Bel18, BKL+13, DHB16, DR11, FSK10, HSA14, JWJ+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYY+14, PC16, QLL17, RYF+13, Sch13, SAAB10, SZDL14, VPK17, WKB16, WDKV19, XZH16, CZ14, Gor10, KHF10, KDW+17, MNN15, MAK+12, MYY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].

Designated-verifier [WHJ17]. Designation [Che15, LSQ11a]. designed
[Goo12]. Designer [KMY18]. Designing
[CDK10, FLW12, MRT10, PSD15, SR10].
Designs [BGK12, PCY+17, KDH15].
Detailed [DL16, ZPXX17]. Detect
[JW1+17, NSA15, WOLP15, Lan11],
detectability [LRW17]. Detectable
[Ess17]. Detecting
[BKBK14, Ess17, GAS+16, HLW12, KW14, SH15, YSC+15, LWLW11]. Detection
[AMKA17, ATS15, DSB15, DF11, GZH17, HDWH12, KU14, LGL+12, LC15, MKRM10, MKAA17, NDC+13, NSMS14, SAIJ16, SBV14, SPI5a, SRAA17, SGS14, TM18, YFT17, AKKY17, AOT13, BM13, HB13, JC13, KLC+10, Maz13, MHT+13, WYL13].
Detective [Cho10]. Detector [LTKP16].
Detector-Based [LTKP16]. Determine
[FSWF11, Sto12]. Determining [NN12].
Deterministic
[MPRS12, NS12, XXZ12, DTZZ12].
Detering [WGJT10]. DEUCE [YNQ15],
develop [Ham19]. Developed [Har16].
Developing [CH11]. Development
[Pal10]. Developments [GCK12, Vai11].
Device [ABCL17, CFXY17, DFKC17, KLM+12, SRK+17, TYK+12, GM16, KKG14, Kim16, Par12b, SHBC19, XHH12].
Devices
[AAC+16, CSF+18, DLW11, EGG+12, GPT12, GD16, GMSV14, HH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, WKB16, WT10b, XJR+17, Aia15, CLP+13b, CFL13, CTL12, Chi13a, FRT13, GTSS19, IB11, KPP16, LKAT12, MvO11, MHV15, OYHSB14, SHBC19, TG17, ZPZ+16]. DFA
[WH17]. DFA-Resistant [WH17]. DFT
[DDFR13]. DHA [AKY13]. DHA-256
[AKY13]. DHTs [YGGK13]. Diagram
[WGD18]. dickory [NN15]. dictionary
[Maf16, MBB1]. did [CMG+18]. Diego
[Ano10, Lin14b]. Dies [Mar10a, MMB17].
Difference [BS14, YTP11, JK13].
Differencing [LyWZ212, YWW10].

Different
[GZ12, HH+13, KU12, AKK+17, ABW10].
Differential
[BMS12, BNY14, CWP12, CGCS12, ESS15, FXP+17, KWS+12, LGL+12, LJF16, LJ15, LYHH14, MRTV12, PH12a, QGGL13, RCP+18, Sun11, WHN+12, Bla15, DDFR13, LLLK10, MNP12, PBCC14, SDM10, SDM14, TSSL11, TS16a, WYL14]. Differentials
[WW12]. Differing [GWH17].
Differing-Inputs [GGHW17]. Diffie
[LCZ14, ABD+15, Ch16, Hof16, HLC11, HLYS14, Orn16, 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, MSI10, MMN12, NC12, pNyWyY+14, Orn16, PH12b, PAS13b, SAA15, SM13, SC12, SOS15, TC11, TS16b, Yon11, Y+17, YLS12, dRsVdVC12, AGHP14, BPP10, CCG10, FLZ+12, Fri10a, GMS11, Har14, KM11, Lan13, LWZG10, MS13b, MM14a, MO14, QCX18, Sim15b, SLM10, yWpNyL11, ZZKA17, Zet14, ZSMS18, Ano13a, Ano15b, Mou15]. Dilly [Bat10].
Dimensional
[Ano17d, LZC+12b, XYYX11, DWZ12, QD16]. dimensions
[Pal15]. direct [GH12]. Directed
[NNLJ12, KPS10]. Direction [NS12].
Directions
[BKBK14, CDFZ16, Hof16, PPA18].
Directly [LZC12a]. directory [SMBA10].
disabled [HFT16]. disassociation
[TMLS12]. Disaster [NRZQ15, BBG+17].
disclosure
[DZS+12, PKA15, SB17, WGJ10].
discovery [Ano11a, MMP19]. Discrete
[BGJT14, CCL16, HKR+18, KLM+12, Xie12, AMORH13, BGJT13, MM13, Mes15, TPL16, VM14]. discrimination
[GPVCdBRO12]. Discriminative [YI14].
Discussion [Gli12, W118, Bul10a].
Discussions [KD12b]. Disk [GMI14, Ran16].
e-commerce [Ano11a]. E-exam [Mor12].

E-health
[WMX+17, IC17, YZL+18, JKL+16].

E-Learning [Yon11]. e-mail [BTW15].

E-passport [LZiX10]. e-rental [LY14].


EAP-based [HZC+14, ZCLL14]. Early [Bel18, Bro11, And13]. Earth [Har14].

easier [MBF+13]. Easy [Bel16, SMS11, Tay14, Wu16, ZDW+16].

Eat [DSSDW14]. Eavesdropping [CWL16, Han12, PX13, YS1L14]. EC [Dra16, CFN+14, CCG+16, CMG+18]. ECC [BSSV12, JMW+16]. ECC-Based [BSSV12]. ECDSA [BBB+16a, DHB16].

ECG [PLGMCdF18]. ECG-based [PLGMCdF18]. Echo [DLM+18, HGT15].

Echo-Based [HGT15]. economy [Sir16].

Ecosystems [LDB+15, MMR19]. EDAK [ABB19]. EdDSA [JL16]. Edge [AHM+18, DF16, KAI18, MD15, PRN+19, Sun16].

Edge-centric [AHM+18]. Edition [Cor14a, Kob10]. Editorial [OK18].

Editors [LLK18]. Education [LRWV14].

Edwards [JL16, LT14a, YTS12].

Edwards-curve [JL16]. EFADS [WLS14].

Effect [PLGMCdF18, WB12]. Effective [HLS+15, KRDH13, WMX+17]. Effectively [YM+17].

Effects [MAL10, SKV12, SHBC19]. Efficiency [ABF12, Chi16, DG17, FRS+16, HRV10, LMLL12, LCL+17a, MS13b, WXLY16].

Efficient [ABB13, ASB+16, ABB19, BWL16, BCGH11, BHG12, BV11, BV14, CG12a, CML+18, CMLRH13, CWWL12, CJ13, DWR12, Dn11a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTC11, GPN+12, GPT12, GJJ15, GH12, GZH17, GCH15, HZC+14, HZC+14, HL18, HL10b, HBC13, HZX15, HKL+12, HIDFGPC15, HCDM12, HH16, HC17, IAD10, KPC+11, Kim15, KHPP16, KH10, LLP+18, LDDA12, LZT12, LXX+14, LCLL15, LSLW15, LHYZ12, LWHS17, LZC17, LBOX12, MXY13, MTY11, MVVR12, MU12, MP12, MC11, MN14, NES+14, NdMMW16, NZM10, PB12, PAF18, PRC12, PG12, PCPK14, PRNC17, RBHP15, SGG11, SZZ14, SGM16, TLF16, TWZ11, TT12, TM18, WDC18, WLS14, WQZ+16, WCCH18, XLWZ16, XLMC13, YHL16, YNMR12a, YNMR12b, YLW13, YNQ15, YLA+13, YS15, ZQW10, ZLY+12, ZSW+12, ZXX+14, ZXYL16, ZCL+19, ZHS+19, ZPK16, ZHW15, AZPC14, AIZ+12, CH11, CSGW11].

efficient [CLJH13, CZZ14, Cho14, Cra11, CGKO11, EA12, FLL+14, Far14, FA14a, FA14b, FIO15, FNWL18, GH16, GLM+11, HPC12, HYS18, ISC+16, IB11, IOV+18, JCH16, JZS+10, KKG14, KHH19, KL11, KHS18, LLLS13, LH11a, LH10c, LXMW12, LCL+15, MLM16, Mes15, Nov10, OCDD11, PZBF18, PC14, RAO17, SZMK13, TTL12, TSS13, TTHK14, VN17, WLY13, WLZ+16, WT1a, WXK+17, XWZW16, yWqWzC13, ZLY10, ZZ11, ZCLL14, ZTT16, ZC15, ZH13, LLZ+12, TCC15].

Efficiently [FWS13, LGH+17, SLY+16].

Effort [RSGN12]. Effort-Release [RSGN12].

EGHR [CML+18]. eHealth [TMGP13].
eID [SGGCR+16]. eight [Sun11].

eight-round [Sun11]. Einführung [Buc10].

Einstein [HR13, Wes15]. Elbirt [Bar12].

Election [Ess17, TKM12]. elections [QS18].

electrocardiogram [BLL+19].

Electrocardiography [YH16].

Electromagnetic [HHH+13]. Electronic
[Bla12, PWVT12, SR14, YWMS11].

Elementary [Led16, Sch15a, CM13].

Elements [Kra12]. Elevation [LZC+12b].

Elliptic [AD11, AK14, ARM15, DW12, GPT12, LGH+17, LWHS17, MST18, PPH12, SG15, AMN18, BAA13, BL14, BL17, BBB16b, Cho14, Far14, IB11, KK10, MCN+18, MS13b, NZM10, SKH15, WHJ17].
elliptic-curve [BL17]. ELmD [BDMLN16].
Elsevier [Ano15b]. Email
[Bel16, CCS14, XJW+16, WR15]. embed
[KPS10]. Embedded
[AB15, BS12, BJCHA17, CFXY17, HC17,
JWJ+17, LWHS17, SOG15, SK12b, SDM+12,
WXY+17, YGD+17, YS15, Ano11a,
CVG+13, Eis10, MFI13, XWZW16].
Embedding
[KD12a, MCD12, XNRG15, XZZ18, YE12,
ZS12, EA11, MKH+12, PWWL13].
Embeddings [FHS13]. Emergable
[YT12]. emerged [McG11]. Emergence [LM12],
Emergency [HLKL15, YTH17, KLC+10].
Emerging [BSV12, KSA16, OS16, FPBG14,
YSJ+16, LW15, Ano11a, CVG+13, Eis10,
MFI13, EMV [Cho10]. Enable [SMS14]. Enabled
[GPT12, HFT16, QZL+16a, QZL+16b,
SGC16, SSPC12, BMM12, TODQ18].
Enabled/disabled [HFT16]. Enables
[IBM13a]. Enabling
[FRS+16, JSM+18, SSY12, WPZM16,
YSJ+16, MMP19, Sch12b]. eNB [CLM+12].
Enciphering
[CMLRHS13, HMR12, MLCH10, Sar11].
Enclaves [WBA17]. Encoded
[DG17, HS18]. Encoding [Br14, CK18,
SK12a, TJJF12, XHX+17, PC14, Sun16].
Encounter [NA10a]. Encrypt
[RAZS15, Ran14]. Encrypted
[ADR18, BTHJ12, CWL+14, CWL16,
Cor14a, DWB12, DCA18, FCM14, FRS+16,
Gen13, GLG12, GZH17, HTZ12, HB17,
HCDM12, IMB17, IBM13a, JSCM17, Kaw15,
KGV16, LA15, LQD+16, Lop12, Mur16,
NBZP17, NNAM10, QLL17, SAKM16, Sia12,
TM18, Vai12, WBC+10, XWSW16,
YDY+16, ZDL12, ZXYL16, ZVG16,
ZLW+17, AHH+18, AZH11, BTPLST15,
BGP+17, BKV13, BL11, CH11, Cri16,
CDL18, DKL+16, DRD11, ED17, FTV+10,
Gen10, GZS+18, HH16, KH18, LKX+14,
LZY+16, LHL+18, LW13a, OSSK16,
PRZB12, SEXY18, SWW+17, Snc12,
TKMZ13, WR15, WL19, XWY+18, XYD18,
YQOL17, ZLY10, ZFH+18, ZHT16].
Encrypting [CC10, Mar10c, dRSdVC12,
LFGC4CP14, Pow14]. Encryption
[ADM12, AV12, AHE17, Alo12, AAC+16,
Ano13c, Ano14, Ano15c, Ano17d, AKP12,
ABF12, AS16, BVS+13, BWLA16, BPR14a,
BPR14b, Bel16, BDOZ11, BWR12, BS14,
BV18, Bla16, BKLS12, BDP12, BHJP14,
BDMLN16, Boy13, BV11, BV14, BGV14,
CVM14, CMO+16, CCL16, CWWL12, CN12,
CZF12, CLHC12, Che15, CGL+12, Chi12,
Chu16, CRE+12, Con18, CNT12, CLW16,
CD16, DR10, DN12, DFJ+10, DSB18,
Des10b, DOS15, Dun12a, DF11, EAA12,
ESS12, FHH10b, FHR14, FJH12, FLL12,
Fuc11, GWWC15, GGH+16a, GGH17,
GM13, GZZ+13, GSW+16, GHI1a, GHI1b,
GHS12, GHPS12, GDCC16, GVW12,
GVW15, GM14, GL12, GKS17, Gue16,
HSMY12, HLLG18, HZ11, HG12, HC17,
HTC+15, HP12, IAD10, JLS12, JHL12,
Jia14a, JR14, Kami13, KB10, KME+12,
KMY18, KTT12, KOS16, KKA15, KFOS12,
KHPP16]. Encryption
[KS12, LMGC17, LMG+18, Lai17, Led16,
LSLW16, LW11b, LW11c, LW12, LLLC12,
LYZ+13, LHL+14, LLK+15, LTZY16,
LLL17a, LSJW15, LH11b, LSJQ18, LB13,
LY15, LW16, LYY+18, LLML12, LHL18,
MZHY15, MLO17, MMP14, MR14a, MTK11,
MSM18a, MVVR12, MSSI17b, MRL+18,
MBF18, MPRS12, MT12, MRM10, MSAs12,
Nac16, NdMMW16, NTY12, NMS14, NAL17,
OT12, OKG+15, PMZ13, PR12, PB12,
PNNH15, Per13, PKTK12, PPS12a, PYS18,
PM12, PCY+17, PRSV17, RVH+16,
RCP+18, RZZ+15, RSG12, RDZ+16,
RVRS12, SG18, Saa12a, SSW12, Sar10b,
Sch15a, SLGZ12, SSZ14, She14, Sm11b,
Sta12, SH15, SMOP15, Tan11, TCN+17,
TCL15, TMC15, Tan17b, TTD13, TRK14,
Encryption
[XHX\textsuperscript{+}17, YZ12, YZX\textsuperscript{+}12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC\textsuperscript{+}11, YFK\textsuperscript{+}12, YCY12, YKKL12, ZOC10, ZPM\textsuperscript{+}15, ZDL12, ZYT13, ZWTM15, ZQ15, ZMW16, ZMI7, ZHW15, ZY17a, ZYM18, ZWS\textsuperscript{+}18, AHS14, ATK17, AKKY17, Ana14, Ano13b, Ano15c, Ano16f, ABR12, AMHJ10, ACD\textsuperscript{+}15, AHL12, BLL\textsuperscript{+}19, BAAS13, BC18, BG14, BSW12, BGP\textsuperscript{+}17, CPPT18, CFVP16, CFZ\textsuperscript{+}10, CW14b, CLH\textsuperscript{+}16, CMMS17, CZ15b, CS11, Chm10, CW12a, CDF\textsuperscript{+}10, CM13, CGKO11, DLZ16a, DMD17, DTZZ12, Eve12, Eve16, FAA\textsuperscript{+}18, FSGW11, FSGW12, FMB\textsuperscript{+}18, Fay16, GMOGCC15, GH13, GHPS13, GLM\textsuperscript{+}16, GI12, GLL\textsuperscript{+}18, HG14, HQZH14, HZ18, HWDL16, HZW18, HT13, HL11, HFT16, HTC17, HYS18, HY18, HKHK13, JCH16, Jia14b, JSMG18, JHC\textsuperscript{+}14, JSM\textsuperscript{+}18, Kam16, KMB13, KKM\textsuperscript{+}14, LLW16, LCL\textsuperscript{+}17a, LCL\textsuperscript{+}15, LFZ\textsuperscript{+}17, LCT\textsuperscript{+}14, LFWS15, LLM\textsuperscript{+}19, LP\textsuperscript{+}19, LH11, LW10, LW13b, LCO14, LPZ15, LCY\textsuperscript{+}16]. encryption
[LCI17, L17, LW17, LLW18, LLL\textsuperscript{+}18, LDZ19, LL16a, LW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSs13, NES\textsuperscript{+}14, PPA18, Pet12, QRW\textsuperscript{+}18, Ran16, RG10, RWZ13, RPSL10, SES\textsuperscript{+}16, SE18, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SGFCRM\textsuperscript{+}18, SLM10, SKB\textsuperscript{+}17, Spa16, SGP\textsuperscript{+}17, SG16, Tam15, TPI16, jT12b, WG1T10, WY10, WW17, WWY11, WHY12, WDZ13, WFX17, Wan18, WGZ\textsuperscript{+}12, WLS14, WC18, XWZ16, XW1C14, XSW10, XDX15, XWS17, XWZ\textsuperscript{+}18, YT11b, yYqWzC13, Yan14, YZ17, YHH18, YCT15, YLZ\textsuperscript{+}16, YL11, ZWQ\textsuperscript{+}11, ZZ11, ZLW\textsuperscript{+}12, ZW14, ZWT14, Zha15a, ZCC15, ZML17, ZYC\textsuperscript{+}17, ZCL\textsuperscript{+}19, ZZ12, Z12, ZDW\textsuperscript{+}16, ZY17b, Zhu13, Wan14, LAL\textsuperscript{+}15, Sar18a, Kat13].

encryption-based
[B18, XZ\textsuperscript{+}18]. Encryption/Decryption
[KB10].

Encryptions
[zGXW12, LG12, SLY\textsuperscript{+}16, RD17].

Encyclopedia
[vTJ11]. End
[Ano15c, BRR\textsuperscript{+}15, BGP\textsuperscript{+}17, CFE16, Chn16, RST15a, RST15b, Chi13a]. End-to-End
[CFE16, RST15a, RST15b, Ano15c, BRR\textsuperscript{+}15, BGP\textsuperscript{+}17]. endomorphism
[FWS13]. Endomorphisms
[AK14, LH17]. enemies
[Fag17]. Enemy
[BC14, CAC14]. Energetic
[PDMR12].

Energy
[ABC\textsuperscript{+}17].

Energy-Efficient
[MP12, TLC16].

Energy-Harvesting
[ABC\textsuperscript{+}17].

Energy-time
[Ano15d]. Enforced
[Set16]. Enforcement
[LLZ\textsuperscript{+}17, Tan15a, Cra11]. engagement
[LSBN14]. engaging
[ISC\textsuperscript{+}16]. engine
[BS15a]. Engineering
[Bel18, FSK10, GHD19, LLK18, MS18a, MP12, PGLL10, TQL\textsuperscript{+}14]. Engines
[LB13, BGG\textsuperscript{+}13]. enhance
[CZ14, SLM10]. Enhanced
[DTE17, KY10, KKM\textsuperscript{+}13, MS17, SGG18, TV15, YCC16, AN18, ACK\textsuperscript{+}10, DLK\textsuperscript{+}16, G16, LNK13, YQOL17].

Enhancement
[FSX12b, LA15, NNA10, CHS11].

Enhancements
[FSX12b]. Enhancing
[CSW12, IA15, Lan13, YS15]. Enigma
[KM15, KM16, LHA\textsuperscript{+}16, Ore14, Ano16c, Bur11, Kap11, Kap13, McG11, McK12]. Enigmas
[Bat10]. Enough
[JC12, Ano14]. Enrollment
[YWZ\textsuperscript{+}12]. ensuing
[SS17]. Entanglement
[Ano15d, JEA\textsuperscript{+}15].

Entanglement-Based
[JEA\textsuperscript{+}15]. Enterprise
[TGC16, Din10, NB13].

Enterprises
[KCR11]. Entities
[GZ12].

Entity
[BCM12, BCM13]. Entropy
Extending [ZSW+12]. Extensible [YZ12].
Extension [ARH14, EKP+13, GFBF12, GT12, RW12, SGY11, HTC17, ZXJ+14].
Extensions [LWL10b, external [ZZKA17].
Extract [AN12].
Extract-Transform-Load [AN12].
Extractability [BCP14b]. Extractable [CZLC12b, CZLC14, GGHW17].
Extraction [BWLA16, GST13, GPP16, extractors [Zim10].
extraordinary [Hol12], extreme [GJ13].
Extruded [CJFH14]. Eye [ERLM16, SM13, Tox14].

F5 [LLY+12b]. Fa [FMS12a]. fabricating [WW13]. Fabrication [VDB16].
Fabrication-Induced [VDB+16]. Facet [AQD12, XHH12]. Facial [KRBI2].
facilitate [Chi13a]. Facsimile [Ano16d].
Factor [HXC+11, LLC11, AIB+16, CLP+13b, DMWS12, ED19, HC12, IC17, JKL+16, JMW+16, Kem11, LNK+18a, LNK+18b, Lit14, WW14, Wat14a].
Factoring [APPVP15, LML12, MM13].
Factorization [Cou12, FS15, KFL+10, Kuz11, YAM+15, Mesi5, TPL16]. Fails [Cer14]. Fails [ABD+15].
Fairness [ALR13, Ash14, GHKL11, Wag16, MV16b].
Fake [KU14]. Fallen [HCPLS12]. False [LLZ+12, CDGC12].
Families [BSS+13, KU12]. Family [ARH+18, BMS12, BKST18, DGIS12, DJG+15, FLS+10, FFL12, GN12, LYY+18, MFG16, YCL17].
Fanin [SS12a]. Fast [BLAN+16, Bru12, CHS15, DSLB18, GSN+16, NR12, PRSV17, WHZ12, WBA17, WQZ+13, ZHW+16, FHH10a, KHBMB13, MBB11]. FastAD [SMBA10].
Faster [CN12, HVL17, TH16, Ant14]. Fault [AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JT12a, LGL+12, LCLW17, LGLL12, MKRM10, MKAA17, PH12a, RZZ+15, SEY14, YGD+17, BBBP13, PBCC14, WMYR16]. Fault-Based [BBB+16a]. fault-resistant [PBCC14].
fault-tolerant [WMYR16]. FBI [Bha16].
FC [DDS12, Dan12]. FEAD [ZWM14].
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 [Ano10, DDS12, Dan12, Dun12b, Kha11, Lin14b].
FedCohesion [CCFM12]. Federated [BS13b, CCFM12, CSL+14, BMBS10, JAS+11, TOSQ18].
Federated-IoT-enabled [TOSQ18].
Federation [SS10a, NB13]. federations [MMS17a, MLM16]. Feedback [HZ11, Hey17, PYM+15, SKGY14, ZH15, LWK11].
Feedback-Based [PYM+15].
FEIPS [DG15]. Feistel [BFMT16, KDH15, Sas12, SEHK12].
FHE [CK18]. FHE-Based [CK18]. FHSN [SP15a]. FI [YNR12a]. FI-BAF [YNR12a].
Flat [BDSG+13]. Fibonacci [FM15, LLP+18].
Fibonacci-number [LLP+18]. Fidelity [BCP14a]. Field [CLF+17, GHPS13, HSA14, SS12a, TGC16, ZAG19]. Fields [ARH14, BGJT14, HVL17, AA14, BGJT13, CZA15a, LBOX12, ÖÖ11].
filtered [HTC17]. filtered-equality-test [HTC17]. Filtering [LLZ+12, CDGC12].
Financial [Ano11b, Ber12, DDS12, Dan12].
Finding [Hof16, Ste15a]. Fine [CDD13, YTH17, ZML17, CLH+16, FSWG11].
Fine-Grained [CDD13, YTH17, ZML17, CLH+16].
FinFET [ZJ11]. FinFET-Based [ZJ11].
Finger [KLY+12]. Fingerprint [MR14b, KKG14, ZHH+17]. Fingerprinting
[TH17, ZS12, FLZ+12, RS17]. Finite
Fully-Homomorphic [GH11b].
Fully-Homomorphic-Encryption [CN12].

[Har14]. geo-location [Har14]. geodesics
[ZZCJ14]. Geographic [LC17].

Geolocation [FPY15]. Geometric
[DSB16, GTT11, WA12, YWNW15, CLZ\textsuperscript{+17}, GZHD12]. geometrical [TL13].

Geometrically [WYW\textsuperscript{+13}]. Geometry
[tWmC12, CFR11, CZ15a]. German
[BDSF12, Blö12, Buc10, Cop10a].

Germany [FBM12, GLIC10, Sen10, Wat10].

Gesture [LCL17b, SHBC19]. gesture-based
[AUMT16, GCSAddP11]. Get
[ESS15]. GGH
[LH10b].

Ghost [CDA14]. GHZ
[CC\textsuperscript{+13}]. GHZ-State [CCL\textsuperscript{+13}]. giant [Joh15]. girls
[Mun17].

Girod [GMNS15]. GLARM
[LLZ\textsuperscript{+16}]. glimpse [Mic10a]. Global
[CLP13a, CLH13, MRS\textsuperscript{+17}, GH16, LH11a, TMK11, ZXL11, LNK\textsuperscript{+18}].

Globally [CCS14]. Glyph [XXZ18]. GMAC
[SKK10].

Goal [BMP12]. Goal-Driven [BMP12].

Goes [BCD\textsuperscript{+12}, RY10].

Goldreich [Lin17].

Goldstrike [BH15]. Goliath [Sch15c].

Gong [LW16]. 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 [RVRS12].

GPGPUs [LCF16].

GPU [BCGH11, GCH15, HBBRNM\textsuperscript{+16}, JHCC14, MBB11, ZOC10].

GPUs [VKP17].

Graded [BR14].

grail [Wat15, Mic10a]. Grain
[BMS12, FSGW11].

Grained
[CDD13, YTH17, CLH\textsuperscript{+16}, ZML17].

Graph
[ATS15, GTH11, WH18, GJMP15].

graph-based [GJMP15].

Graphical [BCV12, CTL12, LTC\textsuperscript{+15a}].

graphical-based [CTL12].

Graphics
[HHMK14, ABDP15, KY10, PGL10].

Graphs [BFM12, KU12, KA18, Lw17, PMZ12, BBGT12].

Gray [DA10, UUN13].

Gray-Level [DA10]. Great [Acz11]. green
[dCCSB\textsuperscript{+16}, ZT16].

Grey [LRW13].

Grey-box [LRW13].

Grid
[CGB\textsuperscript{+10}, DLZ\textsuperscript{+16}b, KS15, LPL15, AMN18, JAS\textsuperscript{+11}, MCN\textsuperscript{+18}, WS12, YY11].

Grid-Based [LPL15, WS12].

Grinds
[SC10, CT11b, GLW13, SHY15, JAE10].

Gröbner [EVP10, FES10, Tam15].

Gros [Dan12].

Ground [KP17].

Groups
[AEHS15, BS12, CGY\textsuperscript{+13}, CLW16, DT13, FVS17, HL10a, Har13, LLZ\textsuperscript{+16}, LCCJ13, TW14, XLM\textsuperscript{+12}, XGLM14, XZL15, ZXH16, AKK\textsuperscript{+17}, CML\textsuperscript{+18}, GBNM11, HCCC11, HPY10, IOV\textsuperscript{+18}, LLLS13, LWS10, LLM\textsuperscript{+19}, RS15, WDLZ13, WTT12, YZL\textsuperscript{+18}, ZZA17, ZWQ\textsuperscript{+11}].

Group-based
[LLZ\textsuperscript{+16}, CML\textsuperscript{+18}].

group-key [IOV18].

Grouping
[LNZ\textsuperscript{+13}].

Grouping-Proofs-Based
[LNZ\textsuperscript{+13}].

Groups
[ABe12, GZ12, XNKGM15, YS12, YKNS12, MZ17a, WQZ\textsuperscript{+13}, ZZ15].

GRS
[TD14].

GSR
[LC17].

Guangdong
[IEE11a].

Guaranteed
[TBC15].

Guerrillas
[Has16].

Guess
[FSWF11, Fok12].

_guessing
[Che15, LCL17b, XJWW13, FIO15].

Guest
[Gup15, LLK18].

Guide
[STC11, Han12].

Guided
[CJFH14, ZSMS18].

Guiding
[DGNJ14].

H.264
[JSZ12, JH012, LLHS12, LW13c, MU12, WDDW12, ZLDD12, ZLDD14].

H.264/AVC
[JSZ12, JH012, LW13c].

H.264/SVC
[MU12, WDDW12, ZLDD12, ZLDD14].

H.265
[GKSB17].

H.265/HEVC
[GKSB17].

Hack
[DLV16, FOL16, RAN10, RAN14, RAN16].

Hacker
[ZGC16].

Hacking
[GHS14, Hea15, JEA\textsuperscript{+15}, Sta13].

hacks
[Ran10].

Halftone
[GL10].

Hall
[Ful10, Don14].

Hall-CRC
[Ful10].

Hamming
[CCCL11, KSY12].

Hand
[SR12a, Cho10].

hand-held
[Cho10].

Handauth
[HBC13].

Handbook
[Bee17, AB10b].

handheld
[CTL12].
High-Efficiency [DG17]. High-Impact [DM15]. High-Level [AW17, KPC+16, ABBD13].
High-Performance [GCS+13, KAK18, LPO+17, GCVR17].
High-throughput [MAK+12]. Higher-Order [LWKP12, PRC12, gWpNyY+14, ZSW+12, LWKP14].
Highly [SZDL14, ACD+15, DT13]. HIGHT [CWP12, WWBC14]. hijacking [DCAT12].
HILL [KPW13, KA17]. HIMMO [GMRT+15]. Hindering [BTPLST15].
HISS [DT13]. histogram [CSS+13, Lin14a]. Historians [Cer14]. Historical [Hai17, Han12].
History [ABJ13, Ano19, Cer14, Cop10a, LT14b, McK10, McK11, SE16, Sm15a].
history-free [SE16], Hitler [Hea15, Moo14]. HMAC [GWM16, MAK+12, YGS+17].
HMAC-DRBG [YGS+17]. HMAC-SHA256 [GWM16]. Hoc [LH12, PD14, She14, XHC+12, KM10b, LXX14, GSGCR+16]. Hoffstein [Mei10].
Holden [Ano17b]. Hole [Ano15d, BKKV10, PC16]. Holocaust [Han12]. holy [Wat15, Mic10a]. home [KPP16, Cor14a].
Homogeneous [HT11]. Homomorphic [AKP12, BV11, BV14, BGV14, CMO+16, CN12, CJ13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHPS12, KOS16, KGV16, Kim15, Lau17, LCLL15, MLO17, MSM18a, MRL+18, MBF18, Nac16, PTKT12, RCP+18, Tan15b, Vai11, WHC+15, XWZ+18, AKKY17, BDOZ11, BC18, CJXX19, CW12a, GH13, GHPS13, GLM+16, LLIW16, SEXY18, Tam15, WSC14, ZXJ+14, ZYC+17].
host [LKKL13, der10]. hostile [CDA14]. HotCalls [WBA17]. House [Ano16h, Bbl16]. HP [CGB+10].
HVS [RMG18]. HWMP [BOB13]. Hybrid [ADH11, ARM15, KBL11, KKA15, LP12, NGAuQ16, OQ12, Per13, SGG18, XWLL16, EEAZ13, KPI18, WSL16, WS14, XWS17, BOB13]. Hybrid-Double [ARM15]. hybrid-indexed [XWLL16].
IBC-HWMP [BOB13]. IBM [ABC+12, ACD+15, BAB+13, HKL+14, JSM+18].
ICA [tWmC12]. ICICTA [IEEE11a]. ICISC [LHL0a]. ICs [GSFT16]. ID [Ano17c, CTL13, CDPLCA16, EZ15, HCC10, IB11, KG010, LMG17, LLY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, TPL16, TT12, TTH15, Wan18, WT10b, WTT12].
ID-based [MM12, LMG17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KG010, LLY14, 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].
YGFL15, YKK18, AGLW16, CTHP13, CJP12, CJP15, EA12, HQY+16, KI11, KL13, NLYZ12, YTm+14. **identified** [AZH11].

**identifier** [MJS13]. **identifiers** [Cer18].

**Identifying** [CSV15, SVG16, ZCSW15].

**identities** [GLM+11]. **Identity** [AQD12, ASM12, ASVE13, Ano15b, ACAT+15, ASS15, BWLA16, BCF16, BHG12, BKPW12, BDFK12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CZLC12a, CZLC12b, CLHC12, CZLC14, CGL+12, CGY+13, Chii12, dCCSM+12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GOPB12, KY13, GDCC16, GJJ15, GJJ17, HZC+12, HvS12, HSM13, HSM14, HZC15, HYWS11, HYF18, KKA14, KRB12, Kuz11, LMG+18, LMB12, LSL12a, LKAT12, LXJ14, LCC+15, LTZ16, LD11, LSC12, LCR12, MLO17, MBE+13, MJGS12, M10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, Ser12, SSPC12, SK14, SWW+16, SGH15, TCR14, Tia15, TH16, TMGP13, Vle12, WY10, Wan14, XXZ12, XQL11, XJW+16, YXZ+12, YTm+14, Yon11, YHK+10, YKc+11, YFK+12, YC12, ZH12+12, ZMW16, ZDW+16, ZPXX17, ZYM18, ZTSR12, ATKH+17. **identity** [Ano13d, BMBS10, BOB13, BMM12, BBGT12, CTHP13, dCCS+16, DZ14, Din10, DWZ12, FA14b, GM15+15, GPVClBRO12, HZC+14, HWD16, HZWW17, HL11, HLB12, HL11, HPM10, Hwa11, JZS+10, KKGK10, KLM+13, KL11, LK12, LXM12, LC+14, MMS+17a, MD15, MGP10, MJGS13, MML16, MM13, NCL13, OJ11, PLCCS11, QYWX16, RG10, SSY12, SE14, SE16, SR10, hSS2Z15, SA16b, Sim15b, SSS11, SSS11, SM16, WWYZ11, WYWY11, WSC14, WLFX17, WMX+17, Wat14b, WWW17, XW12, XCL13, XH14, YWL+17, YQWqZ13, YPS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZJ12, LZXJ10, PN10, Sar18a, Kat13].

**Identity-Based** [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGY+13, Chii12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GY13, GJJ15, GJ17, HZC+12, HSM14, HZC15, LMG+18, LSL12a, LCC+15, LTZ16, LSLW15, LH11b, LSC12, LBR12, MLO17, RDZ+16, SGH15, TCR14, Wan14, XXY12, XJW+16, YXZ+12, YHK+10, YKc+11, YFK+12, YC12, ZH12+12, ZMW16, PZX17, ZYM18, CSZ+11, HSM13, HYWS11, HYF18, LKAT12, LJ14, MJGS12, RS15, SWW+16, Tia15, TH16, ZDW+16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HWD16, HZWW17, HL11, HLB12, HL11, HPM10, Hwa11, LK12, LCT+14, MJGS13, MM13, NCL13, QYWX16, RG10, SE14, SE16, hSS2Z15, SA16b, SSS11, SM16, WLFX17, XW12, XCL13, YW+17, yQWqZ13, YKC+12, YXA+16, ZJ12, LZXJ10, 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]. **IP** [MMZ12]. **Igor** [Sha10]. **II** [Mun17, SCP101b, SMOP15, ZWS+18].

**III** [SMOP15]. **Illegal** [ABJ13]. **Ilogical** [Hel17]. **Illumination** [KLY+12]. **Illusion** [GHS14]. **Illustrated** [Cop10a]. **Im** [BGI+10, BGI+12] **IMA** [Che11]. **IMACC** [Che11]. **Image** [Bal10, BAA13, BB14, BWR12, CJFH14, DA10, IAD10, JH12, KPS10, LA15, LLL17a, MBC15, MAL10, MSM+18b, PWW10, RS16, RVRSCM12, SH11, SM11, SJ12, SP+12, SMK18, SSA13, SRAA17, SZT18, TB18, WHZ12, WZL12, WW+13, WYCF14, yQWqZ18, WYK12, YL+12, YN15, Ye10, Ye14, YH16, YXD18, ZZX+11, BWA13, BM13, CT11a, CW14a, EA11, FMB+18, GKK11, HLC16, KM11, LXML11, LW10, LULW11,
BF11, CVM14, CDGC12, CGB+10, CST+17, CBL13, Dew11, DP12, FHKP17, FHS13, HHH+13, IF16, JHHN12, LG12, LW11a, Low12, MA17, MAL10, NTKG17, SGC14, STC11, TWZ11, WSS12, XZZ18, Yan10, Ye10, ZZ15, ZHL15, AB10a, Abe10, AL15, ASVE13, BSS11, BGP+17, DMWS12, KL13, LWK+18, MKH+12, Mar10b, SRB+12, WW13, BYL10, LH10a.

Invention
[YKWF14, CDSLY14, KK10, MZ17a, TLL13].

Invariant
[ZXYL16].

Invisibility
[KHHH14].

IoT
[ISO/IEC BCM12, BCM13, TS16a, WWBC14].

Irregular
[JKHeY12].

Isogeny-Based
[KAK18, Lau17].

Isolating
[LG12].

ISSAC
[Wat10].

Issue
[Ano13d, Ano16a, Ano16b, Ano16h, CSYY18, GO17, LW13a, LKL18, XW13, PHWM10, Sim15b].

IP
[ZXYL16].

Invert
[yWpNyL11].

involution
[BCM12, BCM13, TS16a, WWBC14].

IRIW
[KK10, MZ17a, TLL13].

Inert
[ZXYL16].

invertible
[SLY16].

Investigating
[SPM+13].

Investigations
[Bl16a, Har14].

ISN
[ISO/IEC BCM12, BCM13, TS16a, WWBC14].

ISO-IEC
[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, LKL18, XW13, PHWM10, Sim15b].

Italian
[Sac14].

Italy
[Cra12].

Item
[YD17].

Iterate
[HHR11].

Iterated
[ILPS12].

Iteration
[CCZC13].

Iterative
[SXL16].

ITUbee
[FXP+17].

J
[Bar12, Led16, Sch15a, WZM12a].

J2ME
[GPT12].

J2ME-Enabled
[GPT12].

Jacobian
[BAAS13].

Jacobians
[Hes12].

Jacques
[Nac12].

jamming
[YSJ14].

Janet
[Ayu12].

Japan
[Sah13, Maf16].

Japanese
[Don14].

Java
[GPT12, XHH12].

Jaypee
[CGB+10].

Jean
[Dew11, Nac12, SR14].

Jean-Baptiste
[Dew11].

Jean-Francois
[SR14].

Jean-Jacques
[Nac12].

Jeffrey
[Mei10].

Jill
[Mei10].

Joe
[Car11].

John
[Wes16].

Johnny
[HM12, RAZS15].

Join
[PD14].

Joint
[ABF12, LC15, PMZ13, TCN+17, LSQ11b, ZC12].

Jonathan
[Ful10, Mou15].

Jones
[Ber16a].

Jose
[ACM11].

Joseph
[Mei10].

Joshua
[Ano17b].

Journey
[CST17].

Joux
[AY12].

JPEG
[AOT13, LSQ11b, LC15, MAL10, QZ14, SK12a, WHZ12, WLIH13, ZC12].

JPEG-2000
[ZC12].

July
[Wat10].

Junction
[VDB+16].

June
[ACM10, ACM11, Gill0, Kap11, Wes16].

Juniper
[CCG+16, CMG*18].

Juraj
[Gas13].

Just
[Pfi10].

JXTA
[AMHJ10].

K
[BKLS12, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CJ13, Ch16, CCT+14, CNT12, Cou12, CMA14, DWWZ12, DL12, EAA+16, FZT13, FVS17, FBMI2, GFBF12, GT12, GZZ+13, GSW+16, GST13, GPT14,
[YYO15].


Large-Scale [DM15, JKHeY12, LQD+16, dCCSB+16, FXP12, GSN+16, SR10, ZZKA17, ZVH14].


Lattice [ADM12, Ano11b, AYS15, BSJ15, EM12, FGM10, HPO+15, HKR+18, LPO+17, MLO17, PG12, AAT16, Dra16, LLM+19].

Lattice-Based [ADM12, Ano11b, AYS15, BSJ15, EM12, HPO+15, HKR+18, LPO+17, MLO17, PG12, AAT16, LLM+19].

Lattices [Boy13, Lau17, TH16, XZ12, ZQQ15, Kre13, Tia15, XLW16, yQyWqZ13].


Layer [LHM+15, ZHX16, HQY+16, LKK13, ZHIH+17].

Layered [BS14, GRL12, WWL+14, JCHS16, ZC12].


Leakage [AV12, BKKV10, CBL13, DCA18, DHB16, FPS12, HHH+13, HHP17, IL15, LTZ16, NTKG17, NTY12, Pan14, SGH15, TTH15, Wan18, XZY+12, YZLC12, YZ12, YCZY12, ZYT13, ZWTM15, ZM16, ZZZ17, ZY17a, ZY17b, ZYM18, CQX18, DLZ16a, DMWS12, GV14a, GLL+18, SGP+17, YLZ+16, ZWM14, ZCC15]. Leakage-Free [IL15, TTH15]. Leakage-Resilience [NTY12]. Leakage-Resilient [AV12, FPS12, LTZY16, Pan14, XZY+12, ZYT13, ZZZ17, ZY17a, ZYM18, ZY17b, CQX18, DLZ16a, GV14a].


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

LeGall [Ara13]. Legislation [PH12].

Lemonade [DFKC17]. Lemons [DFKC17].


Less [TKR14, GM13, Kam16]. Lessons [KMP+11, TGC16, WL11, CMG+18]. Level [AW17, Ano15a, BRPB13, BKJP12, CCW+10, DA10, Gh12, HS18, JWJ+17, KPC+16, KGP12, MV16a, ZLD15, ABBD13, MEFQ12, RS17, UUN13, VS11, YT11a, BAI12].

Leveled [BGV14]. leveling [LY15]. Levels [HLC11, LRL17].

Leveraging [DMS+16, HCM11, MvO11, SKGY14].

Lewis [Mar10a]. Lexicographic [ZAC17].


Light [JEA+15]. lightning [Ran10]. Lightweight [AMKA17, AARJ12, BSS+13, BFTM16, BKL+13, BM11, CGC16, DMWS12, CWP12, CCF17, DS11, ESS12, EKP+13, FQZF18].
GNL12, GAI\textsuperscript{+}18, GMVV17, GMSV14, HZWZ18, HCETPL\textsuperscript{+}12, IS12, IOM12, KE19, MO12, MFG16, MPM\textsuperscript{+}17, PCDG14, Shel14, ZWY\textsuperscript{+}13, ZLY\textsuperscript{+}19, AMN18, AATM18, AKKY17, BLL\textsuperscript{+}19, Bor10, BBB16b, CL11, FLL\textsuperscript{+}14, GTSS19, KDH15, LLZ\textsuperscript{+}16, MCN\textsuperscript{+}18, MNP12, MV15, MHY\textsuperscript{+}18, PJ18, PSdO\textsuperscript{+}13, SGJ\textsuperscript{+}18, Tan12b, TG17, WLZ\textsuperscript{+}16, WCFW18, WWCBC14, XWZ\textsuperscript{+}18, XHM14, YCT15, ZSW\textsuperscript{+}18a. Like [BW16, ERLM16, CGCS12, KO16, LJ15, LJ16, RS14]. Lilliput [BFMT16]. Limitations [DR12]. Limited [DFKC17]. Limited-Use [DFKC17]. Limits [AS16, GV14a, KS12]. Lindell [Ful10]. Line [FEL12, YMWS11]. Linear [BC1\textsuperscript{+}13, BW12, CGCS12, CMA14, EKP\textsuperscript{+}13, FGMP12, LGLL12, LJ15, LJ16, LFW\textsuperscript{+}16, WGF16, YCL17, BBEP14, Bul10a, FES10, MOGOGCC15, Her10, HCCC11, LJ15, O811, SA14, XSWC10]. Linear/Linear [EKP\textsuperscript{+}13]. Linearly [ADD10]. Linguistic [OO18, OO10, OTO18]. linguists [Maf16]. link [Ham12, VS11]. link-state [Ham12]. Linkable [YLA\textsuperscript{+}13]. linked [JCHS16]. linking [NPH\textsuperscript{+}14]. Linux [Fel13]. Lipreading [OS12]. LISISAP [VS11]. List [AEHS15]. Listening [Lan17]. live [ZZCJ14]. live-wire [ZZCJ14]. Liveness [OS12]. Lives [Acz11, McK12]. LLL [NV10]. Load [AN12, FXP12, PRN\textsuperscript{+}19]. Loc [CDPLCA16]. Loc/ID [CDPLCA16]. Local [pNyWyY\textsuperscript{+}14, TMK11, VGA15, WYW\textsuperscript{+}13, LMJC11, LWW\textsuperscript{+}10, PTK14]. Locality [Kaw15, NCCG13]. Localization [SRAA17, GAI\textsuperscript{+}18, NC13, SCY15]. Locally [Yek10]. locating [ZYL\textsuperscript{+}10]. Location [Kim11, PSD15, PAK15, WPZM16, CHX13, Har14, NZL\textsuperscript{+}15, PC14, YXX\textsuperscript{+}18]. Location-based [Kim11, CHX13, NZL\textsuperscript{+}15]. Location-dependent [PKA15]. Location-Privacy [PSD15]. Locations [KD12a, Alp18]. locator [MJS13]. loci [FES10]. Locking [AB15, FHS13, LCW\textsuperscript{+}16, LHA\textsuperscript{+}16]. Loève [BCP11]. Log [YKK18, PGLL10]. Log-polar [YKK18, PGLL10]. Logarithm [BGJT14, CLL16, VM14, AMORH13, BGJT13, MM13, Mes15, TPL16]. LogCA [AW17]. Logging [YNR12a, YNRT12b]. Logic [Cll11, DGP10, Hel17, RZZ\textsuperscript{+}15, Ter11]. logical [CO11]. Loiss [DG12]. long [CFVP16, BF12]. long-term [CFVP16]. look [AY14a]. look-up [AY14a]. Looks [ERLM16, KTA12, Sch16]. lookup [LDDAM12]. lookup-table [LDDAM12]. loop [DWA12]. losing [SLZ12]. Loss [DK16, JTZ\textsuperscript{+}16, DMV15]. Lossless [DA12, LZA\textsuperscript{+}12b, GJ13, TTL10, WH13]. Lossy [BKPW12, CW12a, DN12, ASO14, CQX18]. Lost [WBA17]. love [Fag17, FHM\textsuperscript{+}12]. Lovers [Keb15, Mac14]. Low [ABC\textsuperscript{+}17, AWSS17, Ba10, BCO13, BCG\textsuperscript{+}12b, CMLS15, DJL\textsuperscript{+}12, FHS13, GST13, G12, LJK17, LBR12, Man13, NVM\textsuperscript{+}17, RS17, SAJL16, WT10b, ZJ11, CZ14, Chi13a, FQZF18, LKGY10, LKAT12, LEW19, MV15, NR11, ZPZ\textsuperscript{+}16]. Low-Bandwidth [GST13, NR11]. Low-Bit-Rate [LJK17]. Low-complexity [DJL\textsuperscript{+}12]. Low-Cost [ABC\textsuperscript{+}17, GI12, Man13, NVM\textsuperscript{+}17, LEW19]. Low-Distortion [FHS13]. low-end [Chl13a]. Low-Latency [BCG\textsuperscript{+}12b]. Low-Overhead [AWSS17]. Low-Power [SAJL16, WT10b]. low-resource [FQZF18, MV15, ZPZ\textsuperscript{+}16]. Lower [LJ15, Sha10]. lp231 [LK14]. LPM [LD13, PJ18]. LPN [HKL14]. LPSNR [LP12]. LR [Y12, ZWM14]. LR-FEAD [ZWM14]. LR-UESDE [Y12]. LSB [DAA10, Tan12a]. LTE [CLM\textsuperscript{+}12, DLK\textsuperscript{+}16, LL13, QMW17, SGC16, TM12]. Lucas [RW12]. Lucia [DDS12, Dan12]. Lucky [AP13]. Lumpur [HWG10]. LUT [HF14b]. Luther [ABJ13]. LWE [BV11, XY18].
MitM [TY16b]. mix [WGJT10].
mix-networks [WGJT10]. Mixed [ST16].
mMTC [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, AAZ+16, ALL+18, CLP+13b, CTL12, CWSN11, CT12, uHAN+18, FHH10a, FA14b, FHZW18, GM16, GH16, HZW17, HZW18, HL14, IB11, Kem11, KKA14, KKM+13, KKM+14, KKG14, KSB+17, LH13, OYHSB14, Par12b, hSZZ15, SSAF11, SKB+17, SHBC19, TKHK14, WSC14, WT10a, YHH18, YNX+16, ZLDD14, ZDW+16, ZC12, MFB+13, SLL10].
mobile-cloud [KKM+13]. mobiles [GCSAddP11]. Mobility [CLH13, LNK+18a, CL11, GH16, LH11a, MYYR13, YLS12, ZX11]. Mode [HZ11, Mar10c, PAF18, gWPNyY+14, WLC12, Fay16]. Model [AW17, App13, CT18, CLP13a, GLG12, GJO+13, GJJ15, GJZ17, HZ15, IA15, Kar12, KP17, LHM+15, LZC+12b, MVR12, PYM+15, PNRC17, SZZ14, SPM+13, TBCB15, WWC+11, WWH12, XZY+12, Yon12, ZH15, BL11, CK11, CDPLC16, DFJ+17, HKT11, HTC17, KSU13, LZT12, LCY+16, LL16b, MGP10, Mas17, MM13, NB13, WYL13, WZM12a, WZM12b, YC12, ZCL+19, TCH15]. Model-Predictive [TBCB15]. Model-based [IA15].

Model-Predictive [TBCB15].
Modeling [CJFH14, GBNM11, LTPK16, MKN13, PAS13b, Ana14, CDGC12, MY+18].
Modular [Abe12, VN17]. modulation [CPB17]. Moduli [APPV15]. Modulus [CNT12, LyWIZ12, SEY14, KFL+10].


MPSS [SLL10]. MRAM [DSB16, PAF18, VDB+16]. MRAM-Based [VDB+16]. MrCrypt [TLM13]. MSP430 [KSH18].

MSP430X [GL12]. MST_1tn3 [SvT10]. Much [DL15]. Muhammad [ABJ13]. Multi [ASS15, BBEPT14, BRT12, CWL+14, Chi12, GVV12, GZJ12, HYS11, HC12, HRS16, IG11, KTT12, KMO14, LyWSZ10, MZHY15, MEFO12, MLBL12, NGAuHQ16, OKG+12, OSSK16, SK12b, TWZ+12, TTM+17, Wan14, WOLP15, XWSW16, YWW10, Ye14, ZC13, ZQQ15, ZLDC15, BGG+13, CPPT18, CLP+13b, CFVP16, CJXX19, CG12b, CLHJ13, CW14a, CZ15b, DFJ+17, FHZW18, GMOGCCC15, GPVCD12, GZS+18, HL14, HL14, HCC11, HLC12, ISC+16, JCHS16, KM11, LXMW12, LXX+14, LCT+14, LH13, LWY12, Mas17, QMC17, SCY15, SWW+16, SSS11, TLL12, WDZL13, WXX+17, XLYZ16, XHM14, YCC16,ZZKA17]. multi-agent [GPVCD12]. multi-authenticated [HL11].

Multi-Biometric [NGA16, MLBL12]. Multi-bit [TWZ+12]. multi-channel
Multi-ciphertext [CFVP16, SWW+16].
Multi-criteria [ZZK17].
Multi-crypto-processor [BGG+13].
Multi-domain [IG11, QMC17].
Multi-factor [HC12, CLP+13b].
Multi-flow [LWY12].
Multi-gateway [WXK+17].
Multi-generation [CJXX19].
Multi-hop [LCT+14].
Multi-instance [BRT12].
Multi-KeyWord [CWL+14, XWSW16, OSSK16, GZS+18, LXX+14].
Multi-lateral [SCY15].
Multi-layered [JCH16].
Multi-Level [ZLDC15, MEFO12].
Multi-linear [BBEPT14].
Multi-Party [KMO14, TYM+17, GVW12, LyWSZ10, XLWZ16].
Multi-Pixel [YWY10].
Multi-precision [SK12b].
multi-privileged [WDZL13].
Multi-Proxy [ASS15, GJZ17].
multi-purpose [KMI1].
Multi-Receiver [WK14, Chi12].
Multi-sawtooth [Ye14].
multi-scale [CG12b].
multi-scroll [GMOGCCC15].
Multi-Secret [HYS11, ZC13, CW14a, HCC11, HLC12].
Multi-Segment [WOLP15].
multi-server [CLHJ13, FHZW18, HL14, ISC+16, LXMW12, LH13, SSS11, TLL12, XHM14].
Multi-Signature [ASS15].
multi-stage [M17].
Multi-target [HRS16].
multi-use [CZ15b].
Multi-User [MZY15, OKG+12].
multibit [KPS10].
Multicast [CC14, BAL10, HGKY11, LIT10, NACLR12].
Multicoupon [HHDFGC15].
Multidevice [DPCM16].
Multidimension [AJA16].
Multidimensional
[Her10, WWBC14, HMCK12].
Multifactor [MMY12].
Multigigabit [PP10b].
multi-hop [ADF12].
Multilayer [NXH+17].
Multilevel [FMS12b, HF14a, NSA15].
Multimedia [NSA15, PMZ13, PZPS15, PM+15, WLY+15, ZW15, Zha15b, ZSA12, HM10, HWYW14, LLLK10, Wan13, XWSW16, TW14].
Multimodal [GM16, Sar18a, AHM+18, ATT+10, MHT+13].
MultiObjective [ZÁC17].
Multipartite [HR13].
Multiparty [BDOZ11, CCL+13, Fri10b, ADMM16, LDDAM12].
Multipath [LH12].
Multiple
[DSB15, DUN12a, FR16, KBL11, LTC+15, 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, HVL17, SK12b, YTS12, AAT16, SKH15, SF12].
multiplicative
[KHHH14].
multipliers [ARM15].
Multireceiver [FHH10b].
multisecret [FGMP12].
Multistream [WXL+17].
Multitone [GL10].
Multivariate
[DP17, ST16, YL17, YDH+15].
multiwatermarking [WL12].
multiwavelet [PPW10].
Munich [Wat10].
Music [NTKG17, Wes16].
musical [Ana14].
Mutt [Tan14].
Mutual
[CJP12, GI12, GM14, Kim16, SBS+12, WT10b, AATM18, BDM18, CJP15, Cho14, CL11, FHH10a, Far14, GPLZ13, GH16, HDPC13, IB11, JNUH17, JKAU19, KIH19, KP18, KLW+16, LK+17, MMP19, SPLHC14, TG17, XMHD13].
MVP
[CD12].
mvSERS [HLKL15].
My
[GPT14, CMG+18].
Naïve [ZW+17].
Name [YCM+13].
Named [LLZ+17].
Names
[ABJ13, MPJ+16].
National
[Fid18, ABJ13].
Natural [ZWS15].
nature [KL13].
Naval [Don14].
Navy
[Maf16].
Nazis [Hea15].
NDSS [Ano10].
nearest [LVR10].
nearby [PHGR16].
necessary
[TD14].
NECPPA [PZBF18].
needs
[Sch12b].
neglected [Joh15].
Negligible
[DF11].
negotiation [MMP19].
Neighbor
[KA18, LVR10].
Neighborhood [DA10].

Network-Assisted [KCC17]. network-based [YLS12]. Network-Coded [She14]. Network-on-Chip [Bis17]. Networking [LCK11, LLZ+17, ZHL15, Kim11, LCM+17]. Networks [ABCL17, ABC+17, BN14, BPSD17, BFMT16, CS14, CSH+18, DS11, DF16, FMS12b, GMV17, HZC+12, HBC13, HK14, KHI10, LLCI1, LL15, LHM+15, LZCK14, LWCJ14, LLZ+12, MPN+17, NSA15, NRY+14, OO12, OKG+12, PYM+15, PCPK14, RWLL14, SWYP12, She14, SP15b, Smil11b, SL111, SZT18, TCN+17, WXL+17, WLY+15, XHC+12, YMI6, ZC13, ZW15, Zha15b, ZLDD12, ZSA12, Aia15, ASO14, APK+18, AIB+16, AIKCI18, ADF12, BDK11, BLAN+16, BBB16b, CDGC12, CLM+12, CML+18, CLSW12, CL11, DSCS12, DK12, DLN13, EEA13, FA14b, FMA+18, GH16, HGYY11, HZC+14, HZWW17, HCC11, HCM11, HTC+10, HYF18, JNLI17, JLT+12, JM1W+16, KM10b, KLC+10, KO16, KLV+16, KDW+17, LLLS13, LC17, LMJC11, LXY14, LK17, LN+18b, M5M+18b, QMW17, RPG12, SGCR+16, SA12, SGJ+18, SZMK13, lSZZ15, SKK10, TODQ18, TKHK14, WGJT10, Wan13, WW14, WXK+17, WX13, XWDN12, XCHCI4, XMHD13, YHH16, ZWQ+11].

networks [ZR11, ZCLL14, ZTW16, ZLDD14, ZHH+17, ZX11, LNK+18a].

Neural [CSH+18, SKS+18, YZLC12, EEAZ13].

Neuroscience [BSR+14, JW14].

Neutrality [Kha10]. Neutrality-Based [Kha10]. Nevada [IEE10]. never [Bai12].


Next-Generation [MR14a]. NFC [LY14, Mic16]. NFSR [WGD18].

Niederreiter [HIC17, MVVR12].


nobody [Sto12]. Node [NYR+14, OKG+12, LC17, PX13, SAAB10]. Node-Capture [NYR+14]. Nodes [VGA15, ZYL+10].

Noise [ASN11, YM17, ZHH+17]. Noised [JLS12].

Noisy [ASN12, HZ+14]. Non [AS17, AMH+16, BCI+13, CG14a, CPS16, DJL+12, DPW18, EKP+13, FHKP17, FMVN14, HKB14, KTT12, LLG15, MH13, MSas12, OOR+14, Pas13a, RMG18, Svo14, WgMW12, YNQ15, YKCI12, ZLDD12, AY14a, BS15, CS11, ESI14, GI12, GI1+12, Kre13, Lan11, LP11, MSas13, SES+16, SXL6, XSWC10, Yan14]. non-adjacent [Kre13].

non-associative [BS15]. Non-Black-Box [CPS16]. Non-blind [HKB14, RMG18].


Non-contextual [Svo14].

non-cryptographic [AY14a, ESI14].

non-dynamic [SES+16]. Non-interactive [BCI+13, Pas13a, Yan14]. Non-intrusive [MH13].

non-iterative [SXL6].

Non-Linear [EKP+13, XSWC10]. Non-Linear/Linear [EKP+13].
Non-malleability [KTT12].
Non-Malleable [DPW18, MSas12, CG14a, FMNV14, OOR’14, Pas13a, LP11, MSas13].
Non-monopolizable [DJL’12].
Non-perfect [FHKP17].
Non-Repudiation [LLG15].
Non-stationary [ZLDD12]. Non-tamper [WgMW12]. Non-uniformly [YKDL12].
Non-Volatile [AMH’16,YNQ15,CS11].
NonInteractive [KOS16,GOS12].
Nonlinear
Norm [Low12]. Note [HYS11,Gal13,Hwa11,Lin11]. nothing [Cer15]. Notions
[KFOS12,SNJ1,Sal12,BP11]. Novel [CLHC12,KRHD13,LLG15,LyWZZ12, LH1b, MJGS12, MCS’15, SWM’10, SC’12, VN16, WHZ12, WZXL12, YZX’12, Ye14, ZMZ17, BOB13, CH10, DDFR13, GPLZ13, HCCC11,J XLZ15, LXC11, LMJC11, LH13, LWW’10, LML’13, MRT10, NZL’15, PZBF18, SYW17, Sun16, TG17, jT12b, WYL13, WZG’12, YWT’12, ZBR11].
November [Kap11,LCK11,Yan11]. NSA [ABJ13,Ano13b,AHS13,Bud16, Men13b, Sta13, Tox14]. NSDG [SSP12]. NTOW [BS15]. NTRUEncrypt [DWZ18,KY10].
NTRUSign [Wan10]. NTT [MCDB12].
NTRU-Based [MCDB12]. Nuclear [Hel17].
Number
[AD11,BKLS12,CDK’10,DSL18,Fok12, Ham17, KAI18, LTPK16,LCLW17,MFG16, NIS12, NNAM10, Shal0, SARA17, SRK’17, CFY’10, CP13, LLP’18, LGKY10,Lin11, MS12a, MRT10, SH11, Sti11, XSWC10].
Numbering [MNS11]. Numbers
Numerology [GG11]. NVMM [CS11].
O [CDD13]. Obfuscated
[LSM16,OWHS12,ZM16]. Obfuscating [BGI’10,BGI’12]. Obfuscation [ABCL17, AS16, AWSS17, BBC’14, BV18, BCP14b, BR14, CZ15b, DRS16, EMW14, FKO15, GGHR14, GGH’16a, GGHW17, MH14, BBGT12, CFVP16, GGH’16b, OSSK16].
Obfuscation-Based [ABCL17].
Obfuscators [PSD15]. Obfuscated
[AWSS17]. Object [BCK17]. Objects
[ZCWS15,HST14,SMBA10,WW13].
Oblivious
[DN12,WCL’18,CGH11,RYF’13].
Obscurity [Edw14]. observation
[WHY’12]. Observations [HCL’14].
Obtaining [BB10]. Occasion [Nac12].
October [CGB’10,IEE10,IEE11b].
OFDM [CLZ’17].
[Par12b]. Offers [Pau10]. Office [Mor12].
officers [Maf16]. Official [Küp15]. Offline
[Ano15a,GAS’16, JMG’16, JW’17, LKAT12, RSM15].
Offline/online
[LW’17]. Offloading [JHCC14]. Offs
[ASBD16,BS14,SR10]. offsets [YQH12].
Old [Che17,GY13]. on-chip [BAB’13].
On-Line [FFL12]. On-siteDriverID
[SGGCR16]. On-the-fly [PS14]. One
[CP16,DSMM14,DCAT12,FD11,HP14, HG12,Mat14,NA10a,PC16,TYM’17, XW12,XXYYX11,XZLW15,Yon12,BM15, FHH10a,GPLZ13,HRV10,LP11, LW10,LW13b,LML’13, RK11,Rus15,SM10a, TCS14,QZWZ10]. One-Dimensional
[XXYYX11]. One-Round
[TYM’17,XZLW15,Yon12,XW12,TCS14].
One-Sided [HP14]. One-Time
[NA10a,DCAT12,BM15,FHH10a,GPLZ13, LW10,LW13b,LML’13]. One-Time-Password [FD11]. One-Way
[CP16,DSMM14,Mat14,HRV10,LP11,
RK11. Onion [KZG10]. Online [BPSD17, JMGG+16, KSD+17, PSM17, SKGY14, SZTZ18, WXY+17, ZHL15, CCG10, HYF18, KveE18, LKAT12, LJW+17, MSM+18b, SKS+18, SYW17].


TLL13, YWT\textsuperscript{12}. protection-key
[HLYS14]. Protocol
[BL12, BC14, BCM\textsuperscript{15}, BSSV12, BFK16, CC14, CCM17, FLH13, FMTR12, Fra16, GI12, HsV12, HC12, HLo10a, HCP11S12, HCE\textsuperscript{TPL}\textsuperscript{12}, HKL\textsuperscript{12}, JTZ\textsuperscript{16}, KMO14, LNZ\textsuperscript{13}, LCCJ13, LNXY15, MBC15, MR10, PSS\textsuperscript{13}, SBS\textsuperscript{12}, SGC16, TYYK\textsuperscript{12}, WT10b, XJR\textsuperscript{17}, YS12, YWF18, YZW\textsuperscript{12}, ZXZ\textsuperscript{11}, AAT18, AGK13, AIB\textsuperscript{16}, AIKC18, AN15, BDM18, BGAD12, CSD18, CCSW11, CJP15, DLK\textsuperscript{16}, EA12, FA14b, FIO15, GMSW14, GLM\textsuperscript{11}, HPC12, HWB12, HLo14, IC17, IOV\textsuperscript{18}, JKL\textsuperscript{16}, JXLZ15, Kim11, KO16, LLLS13, LDDAM12, LKKL13, LWS10, LXMW12, LEW19, LY14, ML1\textsuperscript{33}, NCL13, NLYZ12, OS16, PR12b, SPL11C14, SB17, SGG\textsuperscript{18}, SWS\textsuperscript{16}, SSS\textsuperscript{11}, SSLP\textsuperscript{T13}, TG17, Tso13, TPKH14, VS11, WCFW18, WZM12a, WZM12b, WLS14, WMYR16, WT10a, WTT12, WCCH18, XCL13, XHM14, YC12, YZZ\textsuperscript{14}, YMM13, ZWQ\textsuperscript{11}, ZTZ16, ZYC\textsuperscript{17}, ZXW\textsuperscript{18}, ZWX18, ZG10, ZZC15, ZX11, BOB13, CJP12, LFGCCG14).

Protocol [Ste15b]. Protocols [AP13, ABHC\textsuperscript{16}, BMP12, CCK12, CCK16, CCF17, CCD15, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLC11, HLo10b, KOS16, LY16, MS16, MT12, Mur16, NYY\textsuperscript{14}, NSMS14, PS14, SBS\textsuperscript{12}, Sch12c, SOF12, TM12, Xio12, YRT\textsuperscript{16}, Aia15, Ano13b, ACM12, CML\textsuperscript{18}, CR10, CLCZ10, DGJ14, FTV\textsuperscript{10}, GBNM1, GLR13, HSH11, Ham12, HDPC13, HZW17, HST14, KJN\textsuperscript{16}, Ksu13, KKK\textsuperscript{16}, LKKL13, MN10, NR11, Nos11, Nos14, SD10, YSL\textsuperscript{10}].

Prototyping [KPC\textsuperscript{16}]. Provably
[BKLS12, CC14, EKB\textsuperscript{16}, Rog16, YMSH10, ZX11, ZPXX17, FA14a, HRS13, LHN11, WB12, XCL13]. Provably [BCGAP12M1, BCM12, BCM13, BHJ14, FH10a, GLL\textsuperscript{18}, IL15, LH11a, LL16b, PSM17, WMS\textsuperscript{12}, XJW13, YC12, YZZ\textsuperscript{14}, ZG10, ABBD13, FIO15, SXL16, XWXC14]. prove

DGJ14]. provenance [CDL18, ZOSZ17]. Provide [Ano15a]. Provided [KS12].

Providence [Sch15a]. provider [DFJ\textsuperscript{17}]. providers [AKK\textsuperscript{17}, BK12b, YWK10b].

Providing
[DLN13, HTZR12, KS18, MLM16]. Proving
[Sar14, AGH\textsuperscript{17}]. Proximity [IW14, Alp18].

Proxy [AS15, GSW\textsuperscript{16}, GJ15, GJ17, HG1Y11, HX15, KP12, LSL15, LAL\textsuperscript{15}, LSC12, MLO17, MBC15, NAL17, Pet12, PR17, SY13, WY10, WMS14, XJW\textsuperscript{16}, YM11, YCM\textsuperscript{13}, BGP\textsuperscript{17}, CLH\textsuperscript{16}, FSGW11, FSGW12, GHI2, HWDL16, HYF18, KKM\textsuperscript{14}, LCT\textsuperscript{14}, LF15, LL16a, LL16b, QMW17, SL12, SK\textsuperscript{17}, Tia15, Why\textsuperscript{12}, Wan18, WLS14, XWXC14, YZCT17, ZLY10, ZDW\textsuperscript{16}].

Proxy-invisible [SYL13]. Ps [HDWH12].

Pseudo
[NN12, XXYY11, CFY\textsuperscript{10}, KM10a, MG15, PLsv1E10, SH11, SM11, XSW10, Zim10].

Pseudo-Random
[XXYY11, CFY\textsuperscript{10}, KM10a, MG15, PLsv1E10, SH11, SM11, XSW10, Zim10]. pseudonym [XHM14]. Pseudonymous
[BDFK12]. Pseudoprime [DW12].

Pseudorandom
[AS17, BCGH11, BK12a, Kla10, MFG16, CP13, GCH15, HRV10].
Pseudorandomness [Sha10]. PSMPA
[ZLDC15]. PSO [TLL13]. PSPACE
[JJUW10]. Public
[Ano11b, ABW10, BVS\textsuperscript{13}, BB14, BKLS12, BBK10, CT18, CLP13a, Che15, CNT12, Cou12, FAM12, KSI17, HCT\textsuperscript{15}, IM14, JLT\textsuperscript{12}, KFOS12, LLS16, LPd10, LSQ18, LZC14, LH18, MZHY15, MMP14, MT11, Mat14, MPRS12, Muf16, NTY12, ORm16, PD15, RSBGN12, RW12, RBHP15, SG18, Saa12a, SK12b, SWM\textsuperscript{10}, Sia12, SC12, SL\textsuperscript{16}, SGP\textsuperscript{17}, SvT10, TMC15, TT12, WP17, WZ15, WWHL12, Wil18, XNK15, XZ12, Xio12, XJW13, YL17, YK\textsuperscript{11}, YFK\textsuperscript{12}, YMC\textsuperscript{17}, ZY17a, AA14, ATKH\textsuperscript{17}, BS15, BSW12, Dur15,
HZWW17, HL14, HTC17, LSBN14, LLY15, LFWS15, LH13, LL16a, RPSL10, SES+16, SY15b, VN17, YT11b, YYS+16, ZZ11, ZCC15, ZCL+19, ZY17b, FB12.

Public-Coin [CLP13a, Mat14].

Public-Key [BVS+13, BKKV10, GKS17, KFOS12, LLH18, MMP14, MPRS12, NTY12, Orm16, PDNH15, RSBGN12, RW12, SK12b, SWM+10, Sia12, XNKG15, XJWW13, YKC+11, YFK+12, ZY17a, ABW10, IM14, LPdS10, LZC14, BSW12, RPSL10, SES+16, VN17, ZCC15, ZY17b].

Publication [ZTL15].

Publicly [NMP+13, SZQ+17, YNR12a].

Publish [BGP+17, DLZ+16b, OFMR16, PRSV17, SLI11, TKR14, YSM14].

Publish/Subscribe [DLZ+16b, OFMR16, PRSV17, TKR14, YSM14].

published [MYYR13].

Publisher [Ful10, Mur10].

Publishing [VSV15, LLL+17b].

Puebla [AB10a].

PUF [BDM18, CCKM16, CCM17, DS16, KPKS12, LKM+12, MVV12, SRK+17, VDB+16].

PUF-Based [CCM17, KPKS12, MVV12, BDM18].

Pufferfish [KM14].

PUFKY [MVV12].

PUFs [IGR+16].

pulse [MRRT17].

pulse-response [MRRT17].

punctured [MG15].

Purpose [GBFB12, Gue16, ABDP15, DGNJ14, KM11].

purposes [ABB+14].

push [Wu17].

Pushdown [CCD15].

Pushing [FHV16].

Puzzle [IBM13a].

Puzzles [RSBGN12, dCCSM+12, dCCSB+16].

Py [DGIS12].

Py-Family [DGIS12].

pyramid [MHT+13].

Q&A [Hof15, Hof16].

Q3 [Ven14].

Quaeda [Mac14, Keb15].

QC [CY14, HC17, VOG15].

QC-MDPC [HC17].

QIM [LJK17].

QIP [JJUW10].

QS [AZPC14, HDWH12].

Quadratic [KRDH13, SEY14, YDH+15].

Quadraticity [MS12b].

Quality [CS12, NN12, YCM+13, SS11, WZLW13, WKH11].

Quantitative [BL15, MLBL12, MV16b, HM10].

Quantization [SSA13].

Quantization-Based [SSA13].

Quantum [Ano15d, Ano16c, Ano17d, Aou17e, BB14, Ber14, BCF+14, Che17, CCL+13, Feh10, FKS+13, Fol16, JEA+15, Kar12, KP10, LLK18, LHA+16, MS16, MSU13, MKAA17, NNA10, NA10b, QCX18, RK11, RSM15, Sti11, TMI12, Unr15, WCL+18, Y+17, ZWS+18, ABB+14, BJ16, CML16, Edw17, FRT13, GJMP15, IM14, JSK+16, KKK+16, LLP+18, LyWSZ10, LCW+16, Lüd12, QD16, SK14, Svo14, 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, TKMZ13, WL19].

Query [DCA18, GA11, PCDG14, WCL+18, AZPC14, BS13a, CH11, ED17, HWK+15, JCHS16, LKX+14, LW13a, YQOL17, ZHT16].

Query-preserving [GA11].

Quest [Fox13].

question [Cha13b].

Quisquater [Nac12].

Quorum [Kar12].

R [BS12, LVV11, PP10b, WYW14].

R3579X [BDK11].

Rabbit [FSWF11].

Rabin [Chi13a].

Radial [pNyWyY+14, CG12b].

Radio [KAHK17, CJP12, CJP15, EA12, Kim11, NLZY12, RGP12].

radio-frequency [CJP12, CJP15].

radix [GKCK11].

RAGuard [ZHS+19].

Rail [HF14b].

Raising [YWW10].

RAKAPOSHI [IOM12].

RAM [BYF+13].

Ramanujan [KK10].

Ramiﬁcations [ALR13].

Random [Ana14, CDK+10, DSLB18, EAA+16, FZT14, FSX12a, GSW+16, Gre17, KS15, LTKP16, LPL15, NIS12, NAM10, NN12, SC10, SRK+17, TM18, WS12, XYXYX11,
Refinements [LL11]. reflections [Hai17, OF12]. refractive [PHN+12].
Refresh [LSC+15]. Regaining [WBA17].
Register [TLCF16, LWK11]. Registers [LLGJ16, ZH15]. Registration [ISC+16].
Regular [CQX18, Wat12, WR15]. regular-expression [WR15]. regulating [DFJ+10]. regulatory [BP10]. regulatory-compliant [BP10].
Reinforcing [WXY+17]. Rejewski [Kap13].
Rekeying-Aware [QLL17]. Related [Cil11, CMA14, DGS12, HLLG18, Pud12, WLC12, MNP12]. Related-Key [CMA14, HLLG18, Pud12, WLC12, DGS12].
Relational [HPC10, RP12, WP17, BFG+14, BL11, GA11, JK13, PYP10]. Relations [BP11, FHS13, HLR11, WGD18, KGO10, LLM+19]. Release [KFOS12, RSBGN12, Umr15, WSS12].
remapping [PSJ+13]. Remarks [SSU12].
Remote [BCE+10, CS14, FYMY15, LZCK14, Sar12, SYY+17, VM15, WgMdZ12, WgMW12, CHS11, HU15, IB11, KKG14, LH10c, LNM+11, LNKL13, LWK18, LH13, MM12, Sar10a, WQZ+13, YSL+10]. remotely [Wat14b, YHHM18]. Removing [HKHK13].
Renewal [MMY12]. renewed [GPLZ13].
rental [LY14]. Reordering [Alo12].
Repositories [Ano15a]. repository [RSM15]. Representation [AGW15, BFM16, MHT+13]. Representation-Based [AGW15].
Representatives [Bla16]. reproducible [CW12a]. Repudiation [LLG15].
requiring [KHHH14]. Rescue [TSH17].
Resettably-Sound [COP14]. Resilience [NTY12, GLL+18]. Resiliency [YM16].
Resilient [AV12, BKKV10, FPI12, LTZY16, LD13, NYR+14, Pan14, PSD15, XZY+12, YZ12, YN12b, YCY12, ZYT13, ZWTM15, ZMM17, ZY17a, ZYM18, CQX18, DLZ16a, GV14a, KPS10, MM1313, SGP+17, Wan18, YSFL14, YKC+12, YLZ+16, ZY17b].
Resistance [CGCS12, PRC12, WLZ12, ZJ11, DLN13, FIO15]. Resistant [BK12a, CDK+10, GV14b, HF14b, WH12, WgMW12, WH17, YP117, GMZ15, HCC10, PBCC14, VCK+12, WTT12, YKGG13].
Resource-Constrained [CSH+18, YN12a, LLZ+16]. Resource-efficient [SZMK13, XWZ16].
Respiratory [RSCX18]. Response [GHS14, HLLL15, ZWH+16, MRRT17].
Rethinking [Che13, HU15, LSG16, MV16a].
Retrieval [BBB+16a, BTHJ12, CJP12, HK14, JMG+16, JHK12, Yek10, ZXZ+11, CJP15, SWW+17]. returned [War11].
reusable [RS17]. Reuse [ABF12]. Reveal


Scalar [YTS12, SHK15]. Scale [DM15, GU13, JKHeY12, LQD+16, CG12b, dCCSB+16, FXP12, GSN+16, SR10, ZZKA17, ZVH14].


Schedules [Pud12]. scheduling [MV16b]. Schema [AN12]. Scheme [ASS15, Bai10, BHG12, BS14, BKJP12, BDH11, CMS15, CLL16, CCW+10, CLH12, CHH12, CCZC13, CGY+13, CLH13, CWW12, DA10, DS11, DKS12, FR16, FG10, GZ+13, GHL11b, GJZ17, GLW12, GZH17, HYS11, HIDFGPC15, HMR12, HHP17, HL13, HP12, IL15, JSZS12, KU14, KP12, KTT12, KI12, KKA15, KSSY12, KLM+12, LSL12b, LHF12, LTH+15, LTYZ16, LHI11b, LGYY12, LTC+15b, LYY+18, LGPR14, MWZ12, MVR12, MRL+18, MN12, MSas12, NXB13, NLLJ12, NLY15, Pet12, PDA12, RVH+16, RMG18, SK12a, SJ12, SG+12, SD12, She14, ST16, SP15b, SJW+17, SSA13, Tan11, TTD13, TWZ11, WY10, WgMDZI12, WgMW12, gWpNyY+14, WH15, XWS16, XHC+16, XJWW13, YM16, Yami12, YZX+12, Ye10, Ye14, YTH17, YL17, Y+17, YHK+10, YMS11, ZPM+15, ZC13, ZQQ15, ZLDD12, ZY17a, AMN18, AHS14, APK+18, AKK+17, BOB13, BAL10, BM12, BBB16b, CCL11, CLSW12].

scheme [CH10, CT11a, CLHI13, CW14a, CTHP13, Cho14, DCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, FHZW18, GZH12, GJ13, GMR+15, GPLZ13, GLM+16, GH16, GAI+18, GTSS19, HZW18, HBBRM+16, HL11, HCC11, HL16, HCC10, Hwa11, IB11, JNU17, JKAI19, JLT+12, JSZ+10, JM+16, KI11, KPP16, KDHI15, KK13, KMB13, KKM+13, KKM+14, KKG14, Kim16, KHI19, KP18, KLW+16, KDW+17, KWH16, KL11, LXYL12, LLZ+16, LSR13, LH10c, LZX10, LNM+11, LMJC11, LK12, LHS12, LNLK13, LK+17, LNK+18a, LWK+18, LK+18b, LFWS15, LHI3, LHH11, LWW10a, LWW11, LW13b, LZC14, LDZW19, LL16a, LL16b, LWY12, MCN+18, MMS17c, MK12a, MSas13, NR17, Nos14, PZBF18, QMC17, QMW17, RPS10, SGGC+16, SM11, Tan12b, TY16a, TK14, TD14, TL13, TTL12, UUN11, WWYZ11, WYYY11, yWpNyL11, WLH13, WDZL13,
WLZ+16, WLFX17, Wan18, WDKV19, WZ11, WKH11, WOLS12, WXK+17, XHH12, XWZW16, WXWC14, XXX15].

scheme [XMHD13, YC11, YCC16, YHHM18, YWK+10a, YCT15, YXD18, YQOL17, YMSH10, ZYL+19, ZLY10, ZXJ+14, ZYC+17, ZPYW12, ZHI+17, ZY17b, ZFH+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12]. Schemes [ABF12, BVS+13, BFM12, BBEPT14, BSJ15, CMLRHS13, CGL+12, Chu16, Des10b, FHKP17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZCK14, MLCH10, MR14b, MMS17b, MBB18, MKRM10, Oba11, PB12, PDNH15, PH12b, Sch10, Shi11, SKH17, SSU12, VSR12, WGF16, YNR12a, YNR12b, Yik10, YWZ+12, AGHP14, AN15, AHL+12, CDGC12, CJXX19, CHS11, CCG10, CTL13, DDD14, DD13, DZ14, FPG14, FGMP12, FMA+18, HWDL16, HM10, KTUI16, LHYZ12, MM12, MA17, NZL+15, QYWX16, SES+16, Sar10a, Sar11, hSZS15, SAR18b, WW14, YT11b, ZCL+12, ZCLL14, ZT14].


Seattle [LCK11, KCR11]. Seberry [AHS14]. SEC [PA10]. Secondary [RS11]. Secrecy [ABD+15, BKST18, KZG10, TSH14, Yon12, AKY13, ABM+12]. secrecy-preserving [TSH14]. Secret [ASN11, ASN12, ADH17, Ayu12, Bai10, BBB+16a, BFM12, BBEPT14, Bri11, CCM+15, CFOR12, CCL+13, DR12, Dew11, EM12, EA11, FHKP17, FR16, Fok12, HYS11, HL10a, Has16, JLS12, Ku14, SK18, KOTY17, KK12, KK13, KSSY12, KS15, LH12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Oba11, PCPK14, QSI18, SLL10, SC10, SS10c, SUS12, Sti15, TLW12, TWZ11, WKB16, WGF16, Wik18, XZY+12, XJR+17, YFF12, YWZ+12, ZC13, Ald11, ADG16, AKK+17, Ara13, BJ16, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEA13, EZ15, FHH10a, GJMP15, GLW13, HF14a, HH15, Hea15, HBBRM16, HCC11, HLC12, KI11, KTUI16, LXY12, LT13, LyW510, LHY12, LEW19, Mas17, Mc10, McK11, McK12, MB11, OO10, Pea11, Pet11, QD16, Rus15, SB17, SA12, SAR18b, TQL+14, TD14, UUN11]. secret [UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, WX13, YC11, YCC16, YSC16, ZCL+12, ZZZ15, ZPWY12, LSC+15, BAI12]. secret-key [BJ16]. Secret-Sharing [BBEPT14]. Secretion [RSCX18]. Secretocracy [Ber16b]. Secrets [BT12, CG14b, DLWW11, FMS12a, KOB10, Man13, Bha16, Cop10b, GGH+16b, Gup15, HRS13, Sm11a, Aol17b]. Secure [ADMM16, AARRJ12, Ash14, AMH+16, BVS+13, BBLA16, BCW11, BCG12a, BCQ+13, BWA13, BJL12, BHJP14, BF11,
Security-Aware [LMS16, GHD19].
security-enhanced [AMN18].
security-modified [MM14b].
SEDURA [LY15].
Seed [AS17, LYHH14, Sun11].
seeing [Tox14].
seen [Goo12].
Segment [WOLP15].
Segmentation [WYW+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 [Cer18, CLL16, CHHW12, CSV15, DM18, HZ11, LCL+17a, LH12, LH11, SAA15, SM12, WHZ12, XWXC14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11].
Self-adaptive [LHM14, FXP12, SH11].
Self-authenticating [Cer18].
Self-Authentication [LH12, LT13].
Self-Certified [CCLL16, XWXC14, 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, HTC17].
Semi [BDOZ11, KKK+16, WHZ12, ZLW15, PGLL10].
Semi-automated [KKK+16]. Semi-fragile [WHZ12, PGLL10].
Semi-homomorphic [BDOZ11]. Semi-trusted [XZLW15].
Seminary [SS10c].
Sender [WZ15]. Sensational [YGFJ15].
Sensi [Kem11]. Sensing [CCZC13, Kar12, uHAN+18, RPG12, XWZW16, Fay16].
Sensitive [Kaw15, RQD+15, Tan15a, QCX18].
Sensivity [YGD+17, LW+10].
Sensor [ABC+17, BN14, CS14, DS11, KH10, LLY+12, NNAM10, NYR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YM16, ASO14, APK+18, AIB+16, AIFC18, ADF12, BLAN+16, BIB16b, CDGC12, CLSW12, DSCS12, DLN13, HTC+10, JHU+17, JMW+16, KLC+10, KO16, KLW+16, KDW+17, LC17, LNK+18b, PL16, SZMK13, SKK10, Wan13, WW14, WXL+17, XWDN12, XMHD13, ZYL+10].
Sensors [DL12, LIK+17].
Sensory [SGC14]. Seoul [LH10a, LW11a]. separation [MJS13].
Sequence [PFIS12, WZG+12]. Sequences [ADD10, Kla10, NN12, XXYYX11, HLC12, VM14].
Sequential [GLR10, GLR13, LLY15, WYL13].
Series [BJL16, Die12].
Serpent [PC16].
Server [BCO13, Che15, GMSV14, LSQL18, LY15, YLW13, ATKH+17, CSD18, CLHJ13, FA14b, FZH18, HDPC13, HL14, ISC+16, KMTG12, LXM12, LH13, SY15b, hSZZ15, SSAF11, SS11, TLL12, WT10a, XHM14].
Server-Aided [GMSV14, LLY15, SSAF11].
Server-Designation [Che15, LSQL18].
Server-Side [BCO13]. servers [DRD11].
Service [BKJK14, CCS14, Hay13, LDB+15, LBR12, NRZQ15, RGSG15, SPPC12, St15, VS16, AaBT16, KPP16, LHL+18, LW13a, MMP19, MLM16, Par12b, Wu17, YWK10b, ZX11, YCM+13]. Service-Based [LDB+15].
Service-Oriented [RSG15]. Services [ANO11b, DLZ+16b, MEFO12, OO12, ZHL15, AZPC14, CSD18, CHX13, GAI+18, IMB17, IG11, NZL+15, PP11, WDK19, XXX15].
Session [BS12, BKJP12, CFST17, SHS12, AN15, DCAT12, SHBC19]. Session-Based
[BKJP12]. Set
[Cor14b, EKP+13, YZ12, Con12, TMK11].
set-valued [TMK11]. sets [SF12]. Setting
[BKLS12, HHP17, MZHY15, TYM+17, XXZ12, ZHL15]. Settings [GZ12]. setup
[Jia16]. Several [Sas12, ZT14]. SGX
[WBA17]. SHA [AAE+14, ABM+12, App15, jCPB+12, LC17, MAK+12, SKP15]. SHA-1
[AAE+14, SKP15]. SHA-256
[App15, MAK+12]. SHA-3
[ABM+12, jCPB+12, LC17]. SHA1
[SBK+17]. SHA256
[GWM16]. Shadow
[Kap11]. Shadows [YSC+15]. Shakes
[CNR14]. Shamir
[BDSG+13, UUN11, WKB16]. Shannon
[AMS+10]. Shape [RITF+11, SY14, Pet11].
Shapes
[CJFH14, LMHH14, SY14, SGS14, ZZCJ14].
Share [LTC+15b, ZPYW12]. shareable
[XWY+18]. Shared [DRD11, LNX15, OKG+12, TYK+12, XJR+17, PZPS15, SA12, TG12, YYS+16, YNX+16].
shared-secret [SA12]. Shares
[CFOR12, KU14, SA16a, WY12]. Sharing
[Bai10, BFM12, BBEPT14, CCM+15, CFOR12, CCL+13, CCT+14, CLW16, DR12, EM12, FHKP17, FR16, HYS11, HL10a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KS15, LYZ+13, LPL15, Lin15, LCCJ13, LTC+15b, LLKA19, NS12, Oba11, PSM17, QZZ18, SC10, SU12, SZTT18, TLW12, TZW11, WYCF14, WKB16, WGF16, XNKG15, XZY+12, YFF12, YWZ+12, ZC13, AKE+17, ADH17, CT11b, CW14a, EZ15, EA11, FGMP12, GPLZ13, GJ15, GLW13, GLB+18, HFF14a, HBBNN+16, HCCC11, HLC12, HYF18, KI11, KTU16, KPB17, LXY12, LT13, LFWS15, LAL+15, LyWSZ10, LHYZ12, LHL15, LLL+18, LEW19, LL16a, Mas17, OQ10, OQ18, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WLS14, WKK11, WS12, WOLS12, YC11, YCC16, ZCL+12, ZZ15, ZPYW12, SLL10].
Shell [WZCC18, YSS14, Tay14]. Shenzhen
[IEE11a]. Shield [NDG+17, KGV16]. Shift
[AKP12, ZHI15, LWK11]. Shift-Type
[AKP12]. Shifting [YWW10, CSS+13]. Shih
[Joh10]. Shopping [AHS13]. Shor
[MNM+16]. Short
[BHG12, CWWL12, NR12, SKV12, WQZ+16, XGLM14, LLY15, RD17, ZPYW12].
Short-Output [NR12]. Shorter
[Hü13, PPB16, TH16]. Should [Eve16]. shown
[Ana14]. shows [Goo12]. Shparlinski
[Sha10]. Shredder [AMH+16]. Shredding
[AMH+16]. SHS
[Ano12]. Shuffler [BVIB12]. Shuffles
[CKLM13]. shunned [Ree15]. Sicily
[Cra12]. Side [AN17, BCO13, CFE16, CDK+10, CBL13, DMWS12, DKMR15, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, SR12a, Vua10, YL17, BVIB12, DJ+12, MFH13]. Side-Channel
[CBL13, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, YL17, DMWS12, BVIB12, MFH13]. Sided
[HP14]. Sieve
[VM14]. SIFT [KLY+12]. Sign
[LL15, MEFO12, SPM+13]. Sign-On
[LL15, MEFO12, SPM+13]. Signal
[Kar12, BLL+19, MS13b, RITF+11]. Signals
[LJK17, XNRG15, AIA+18]. Signature
[Ano13a, ABF12, ASS15, AEHS15, BHG12, BDH11, CGB+13, FGM10, GJ15, GJZ17, GMSV14, HZ15, HPP+15, HHP17, Hü13, JL16, LTH+15, LGPH14, MM12, NBX13, PH12a, ST16, TTH15, WZXL12, WLB15, WYML16, WHLH16, XGLM14, Y+17, YHK+10, YMSW11, YLA+13, ZJ14, ZLH+12, AGPH14, CLSW12, CCG10, DZ14, DLN13, HYWS11, Hwa11, JZS+10, LWZ10, LL16b, NOS14, QYWX16, QMW17, QCX18, RSM15, SLM10, VSS1, WSC14, XIW16, YWL+17, YLS12, YKC+12, ZLY+10]. signature-based
[DLN13, QWM17]. Signatures
[Ano15a, ABC+17, AYS15, BBC+13, BDFK12, BHH+15, Fuc11, GY13, GdM16, HS18, Hü13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, ORM16,
PST13, TH16, ASVE13, BDL+11, BPP10, GMS11, Her14, LLY15, PPB16, SEXY18, Tia15, ZQWZ10, Mou15. Signtryption
[CMA14, DZY10, FZT13, FZT14, IL15, LSL12a, Rao17, QXL11, ZYD10, EZ15, HPY10, HS11, KL11, LK12, LZT12, LKAT12, YMSH10, LHL15]. Signed
[KWH16]. signer [Hwa11]. Signing
[YAM+15, JC13]. Silent
[AMH+16]. Silverman [Mei10]. similarity [ZFH+18]. similarity-aware
[AMKA17, BSS+13]. Simple [Ano13c, CFZ12, LYY+18, Ros11, Sar10b, Sma16, TDTD13, ZH15, Zim10, CLM+12, MMS17c]. Simpler
[TH16]. Simplified [PS12]. Simulation
[CPS16, LLH18, MS13a]. Simulation-Based
[LLH18]. simulations [Ana14]. Simultaneous
[YWZ+12]. Singapore
[Abe10]. Single [ABK13, LL15, MEF012, Sas12, SPM+13, CJXX19]. single-generation
[CJXX19]. Single-SP
[Sas12]. Singular [LSL12b, BWA13]. sins
[HILV10]. SIP
[KKGK10, ZTZ16]. SIP-based
[ZTZ16]. SIP
[SYC+17]. Site
[DSB15, SS10c]. siteDriverID
[IBM13a]. Size
[AS17, AEHS15, CJ13, CSW12, EAA12, Kim15, LCLL15, MTY11, ZMW16, AHW+12, LCT+14, PPTT15, SGM16, SHBC19]. Size-Constrained
[EA12]. Skein
[FLS+10, KNR10]. Skin [AQD12]. skyline
[BKV13]. Slantlet
[TK14]. Slicing
[MZ17b]. Slide
[IOM12, LC13]. Sliding
[BBG+17, Bro17, Win17]. sLiSCP
[ARH+18]. SLMAP
[HCETPL+12]. Slow
[Sm11b]. Small
[BGJT14, BKLS12, BB10, CJ13, Kin15, LCLL15, YM16, AAT16, BGJT13, Jou13]. Smart
[AN17, ABC17, BSJ15, DLZ+16b, HCL+14, LA10, MFG16, PTD12, WgMdZ12, WgMW12, AMN18, CHS11, CLHJ13, GHD19, GAI+18, Ham19, HCC10, LH10c, LNM+11, LXMW12, LNKL13, LNK+18a, LTC+15a, MM12, MCN+18, WMYR16, YZZ+14, YSL+10, Cho10, GLIC10, SD12]. Smart-Card-Based
[HCL+14]. Smartphone
[MDMJ17, uHAN+18, DL15]. Smartphones
[Cor14b]. smashed [Fag17]. Smith
[Ano16g]. Smooth
[XYYXY11, YC11, ZBR11]. SMS
[KRM+10, PSdO+13]. SMSCrypto
[PSdO+13]. Snakes
[PC16]. SNOW
[PC16]. Snowden
[Tox14]. SoC
[GSC17]. Social
[BPSD17, KTA12, NSA15, NRZQ15, PYM+15, Rog16, SKGY14, SZTZ18, WLY+15, ZW15, Zha15b, ZHL15, BDK11, HYF18, LCM+17, LZC17, GSM+18b, SKS+18, Smi15a, YZL+18]. Society
[Sch20a, Sch20b]. Socio
[NS12]. Socio-Rational
[NS12]. SoD
[VN16]. Soft
[Jin10, TLCF16, SS17]. Soft-Error
[TLCF16]. Softw
[WZM12a]. Software
[Bar15, Bee17, EWS14, LRVW14, MRL15, WZM12a]. Software
[ABF+14, CFH+13, DK17, Eve16, GGH+16b, GIJ+12, HLV10, KHF10, LBOX12, SF12, YWT+12]. Solan
[CGB+10]. solid
[Cri16]. Solution
[Fra15, GSFT16, HLKL15, Kam13, NA10b, YFT17, Cor14a]. Solutions
[LLGJ16, BLV17, KAS15, MMP19, WW14]. Solved
[IBM13a]. Solving
[Ano17c, BB10, Bul10a]. Some
[AD12, Ber12, Dur15, LWL10b, Mid10]. Somewhat
[HTC17, KOS16, MBF18]. Song
[Con12]. Sood
[MWZ12]. SOEMONUK
[PC16]. SOT
[PAF18]. SOT-MRAM
[PAF18]. Sound
[COP14, LSR13, Sav15]. Source
[Bis17, FKOV15, MBC15, RWLL14, ZPM+18]. Sources
[LLG16, BLV17, KAS15, MMP19, WW14]. Solved
[IBM13a]. Solving
[Ano17c, BB10, Bul10a]. Some
[AD12, Ber12, Dur15, LWL10b, Mid10]. Somewhat
[HTC17, KOS16, MBF18]. Song
[Con12]. Sood
[MWZ12]. SOEMONUK
[PC16]. SOT
[PAF18]. SOT-MRAM
[PAF18]. Sound
[COP14, LSR13, Sav15]. Source
[Bis17, FKOV15, MBC15, RWLL14, ABF+14, LZC17, PX13, Pow14]. Source-Based
[MB15]. Sources
[DHB16, BJ16, SSY12]. South
[BL10, LW11a]. Soviet
[Bud16]. SP
[Sas12, SEHK12]. SPAPBox
[FG+17]. Space
[BWR12, BKL+13, NYR+14, RMG18, MMM+18b, RFY+13, ZZ15]. Space-Filling
[BWR12]. Spaces
[SH15]. spam
[SKEG14]. Spanish
Survival [YCM+13, MMS+17a]. Surviving [CFST17], suspect [der10]. SVC
[MU12, WDDW12, ZLDD12, ZLDD14]. SVD [LP12, TB18]. SVM [TLL13, swarm
[ZSMS18]. SWIFT [PLCGS11]. Switching
[CNT12, GHPS12, GHPS13, WB12]. Sybil
dCCSM+12]. Sylvie [SS10b]. Symbolic
[Wat10]. Symmetric
[BPR11a, BPR11b, BDPS12, CVM14,
FPS12, GFBF12, JCHS16, KTT12,
Khalo, PR12, PCY+17, TW11, YKNS12,
BGG+13, CGK011, DLZ16a, FH13,
GMRT+15, Gor10, GCVR17, KAS15,
LZC17, SKK10]. Symmetric-Key
[Gor10, GCVR17, KAS15, LZC17, SKK10].
Symmetry-Key [CVM14, 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, yWXyZ+18, AATM18, XNG+
14]. Synchronized [DM18, ACM12].
Synchronizing [HZ11]. SYND [MHC12].
Syndromes [BBC+13]. Synergy [KRB12].
Synergy-Based [KRB12]. synthesis
[RS17]. Syst [HYS18, WZM12a]. System
[AD11, Ano10, CZLC12a, CZLC14,
Cor14b, CRST15, DG15, GOPB12,
Har16, HHS+15, IAD10, JN12,
JWV+17, Jin10, KMP+11,
Lop12, MLBL12, NMS14, QLL17,
RSCX18, SMSK18, SRAA17, SLI11,
YE12, YZX+12, YKK18, ZZM17,
ZPW16, ZLDC15, ZVGM16,
AHM+18, BC18, BGG+13, Bul10a,
CH11, CTL12, CZ14, CS11,
FNWL18, GCK11, HWK+15,
HJM+11, HLYS14, JC13,
LLK10, LLL+17b, Lit14, LTC+15a,
LLL+18, MS12a, MNNW15,
PSOMPL13, SSPL+13, WMX+17,
VGZ+12, WXW16, YZL+18,
ZMM+10, ZML17, KKA14,
Dew11]. System-Level [JWV+17].
Systematic
[CCG+16, CBL13, PC16]. Systems
[AN12, AB15, BL15, BS13b, BCPT16,
BB10, CWL16, CCF17, CRE+12,
DLZ+16b, GI12, HXC+11, HCL+14,
HLN+10, LMD16, LQY10, LY16,
LNZ+13, MR14b, OS12,
PRSV17, QZL+16b, RST15a,
RST15b, SBS+12, SFKR15, Sev16,
SKH17, SGC14, SDM+12, STC11,
TKR14, YNR12a, AT10,
ATI+10, CFVP16, CFZ+10, CLZ+17,
dCCSM+12, dCCSB+16, CGH11,
CVG+13, CDA14, DZS+12, Eis10,
FXP12, GMOGCCC15, GHD19,
GSN+16, GPVcBRO12, HZGW18,
JSK+16, JHCC14, KSA16,
LCL+15, LWK+18, MLMSMG12,
MGP10, MFH13, NLYZ12, QMC17,
SS10a, SR10, SRB+12, WS14,
YSM14, ZHV14, Zhu13, MA17,
Ano11a]. Symmetric [MCDB12].
Systolic-Array [MCDB12]. SZK
[MX13]. T [SJWH+17]. T-Chain
[SJWH+17]. Table
[CCL+13, AY14a, LDDAM12]. Tables
[PTT16, XHM14]. Tag
[NNAM10, PPH12, CJP15,
SPLHC14, CJP12]. Tags
[M012, HSH11, HDPC13,
HQQ+16, LEW19, MK12a,
PLSvdLE10, TG17, WCFW18].
Taipei [Yan11]. Taiwan [Yan11]. Takes
[Ano16c]. Talking [FD11]. Tamed
[NXB13]. taming [BBDL+17]. tamper
[MN10, NC13, WgMW12]. tamper-evident
[MN10]. Tamperable [ACM+17].
Tampered [SSA13]. Tampering
[CG14a, SRAA17, SGp+17]. TAO
[Sta13]. Taormina [Cra12]. tap [ADG16]. target
[HRS16]. Targeted [ABJ13]. Tasks
[Abe12, FKS+13, CL16]. Taxonomy
[AJ16, GAF+15, KMS15, MA17]. Taylor
[Joh10]. TCC [Cra12, Lin14b, Sah13]. TEA
[CWP12]. Teaching [GY13]. Team
[LJS+14, Pfi10, Ant14]. Tear
[Boy16]. Tear-Free [Boy16]. TEASE
[ZBR11]. tech [Aono15e]. Technical
[Sir16, TS16b, Wag16, JW14, Suc12].
Technique [HEK18, KBL11, ZLDD14,
BBBP13, CPPT18, GCSAddP11, SM12,
SKS+18, TS16a, ZWS+18]. Techniques
[Bis17, DA12, GOS12, HPC10, HL10b,
LW12, Mor12, PJ12, AB10b, BM13,
FGPGP14, Gil10, HT13, KHF10,
LH11a, OO18, VN17, WMX+17, Joh10].
technologies
[JAE10, JAS+11, Lan10, MMP19].

Technology [CGB+10, FoJ16, EEI11a, Wu16, Ham19, IMB17].
telecare [LWK+18, MA17].

Telephony [SKEG14].

Television [DTE17]. Tell [Cer14].

Template [NGAuHQ16, SKV12].

Templates [DWB12, AHM+18].

temporal-credential-based [JMW+16, XMHD13].

temporary [JMW+16, MHT+13, XMHD13].

Tenant [TV15].

terahertz [WW13].

Term [SKV12, CFVP16].

termination [SRB+12].

Ternary [ADI11].

Test [HTC+15, JEA+15, LLSW16, MZHY15, SS10b, WH18, HTC17, ZCL+19, Ano16g].

Testable [RMP10].

tester [RPSL10, SY15b].

Testing [Cou12, SS12a, AY14a].

tests [GLG12, MS12b, Sim15a].

Texas [IEE13].

Text [GdM16, SMSK18, XZZ18, CR12, SI12, SWW+17]. Text-dependent [GdM16].

Textbook [PP10a].

Texture [TSH17].

Theft [Ber12, Ber17, BTPLST15].

Their [CZLC12b, CK18, 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 [AC10, ACM11, CCKM16, CDFZ16, CDFS10, Cra12, FGM10, FB12, FS15, He12, LW11a, Lin14b, Nac12, Per13, PJ12, RBHP15, RST15a, RST15b, Sah13, SAKM16, Sha10, Wsl16, Yan10, Abe10, AR10b, Bul10b, CFR11, Gil10, LPZJ15, MZA+13, McG11, YTM+14, Cra12, Lin14b, Sah13, vDKS11].

theory-based [LPZJ15].

There [Cer15, McK10, McK11, SM13].

Thin [Chi16].

things [FQZF18, AAC+16, CLF+17, Ham19, HZL18, JKAU19, LNK+18b, LGH+17, NLLJ12, NLY15, PLGMDF18, SB17, WCH18, YCT15].

Third [JCPR12, QZL+16b, Sen10, BL10, ED19, Kip13].

Third-Party [QZL+16b].

Third-Round [JCPR12].

Thirteen [AP13].

Thou [BDK11].

Threat [CSYY18, ALL+18, Ven14].

Threats [AJA16, ERLM16, GSC17, LJS+14].

Three [CZ15a, HXC+11, LZC+12b, PC16, Sh11, YKNS12, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKKH14, XCL13, YC12, YZZ+14].

Three-Dimensional [LZC+12b].

Three-Factor [HXC+11, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b].

three-party [LML+13, Tso13, TKKH14, XCL13, YC12, YZZ+14].

Threshold [CT11b, Cil11, FGM10, GLW13, HYS11, LWL10b, SSU12, Sta12, Tan11, WYCF14, WLH15, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, HH15, OO10, QD16, SES+16, Shy15, SGM16, TD14, ZXJ+14, ZPYW12].

thresholding [PC14].

thrive [Sch12b].

throughput [MAK+12].

Thru [SYC+17, SYW17].

Thwart [LJS+14].

Thwarting [XTK10].

Ticket [XHCH14].

Ticket-based [XHCH14].

tickets [LMJC11].

tied [Men13b].

Ties [PYM+15].

Tight [GDC16, LPS12, LLH18].

Tightly [HLLG18].

Time [ASBDs16, Ane17d, App14, AYS15, BJL16, Che17, F11, GSC17, HC17, HGT15, IF16, JWJ+17, JEA+15, KME+12, LCL+17a, NA10a, Nov10, PNRC17, Ste15b, WLZL12, YE12, AY14a, Ano15d, BM15, CC14, DCT12, FHH10a, GPLZ13, 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, Unr15, WSS12].

Timed-Ephemerizer [Tan15a].
Trusted [AWSS17, EAA12, FPY15, YCR16, ED19, HTC+10, Küp13, XZLW15].

Trusted [AWSS17, EAA12, FPY15, YCR16, ED19, HTC+10, Küp13, XZLW15].

Trusted [AWSS17, EAA12, FPY15, YCR16, ED19, HTC+10, Küp13, XZLW15].

Twice [BM15].

Two [Ash14, Bru12, CTL13, DZ14, ED19, GGH14, GLW12, HL10b, HP14, KMTG12, KOS16, KU12, LLC11, Lit14, NMS14, OTD10, YSL+10, YLW13, ZM16, AN15, CSD18, CHS11, DHW+13, FIO15, HPC12, HWDL16, HWB12, JLT+12, JMW+16, Kem11, Li10, Mcg11, QYW16, Rus15, SM10b, hSZZ15, WW14, Wat14a, YT11b, ZZC15, GHKL11].

Two-Channel [JLT+12].

Two-Party [Ash14, HL10b, HP14, KOS16, NMS14, ZM16, FIO15, HPC12, HWB12, ZZC15, GHKL11].

Two-Round [GGHR14].

Two-Server [YLTW13, KMTG12, CSD18].

Two-Thread [MD12a].

Type [AKP12, CFL13, PFS12, SH15, BNST17, SYL13, WB12].

Type-Based [CFL13, SYL13].

Type-Flaw [SH15].

Types [BCEM15].

U.S. [Maf16].

Ubiquitous [OS16, Par12b].

UDES [YZ12].

UHF [HQY+16, PPH12].

UK [Che11, FJ12, vDKS11, Ano15e].

Ukraine [OGK+15].

Ultra [AATM18, TG17, WCF18].

Ultra-Lightweight

Ultra-Lightweight
[ÁMVZ12]. URLs [AY14a]. USA [Dun12b, IEE13, Koa11, Lin14b, Pie10, Rab10, ACM10, ACM11, IEE10, IEE11b]. Usability [RAZS15]. Usable [DL15, TGC16]. usage [AKK17, BHCdFR12]. Use [CSV15, DFKC17, KOS16, NR12, YT12, der10, CZH15b, Die12, Hof16, KK10, MBF13, O010, Sti11, UK18]. Used [CGCGPDMG12, BM15, MS13b]. useful [dCCSB16, Usernet [Be18]]. User [BLV17, BKJP12, FLH13, Gdm16, Har16, JN12, LLC11, LCL17b, MZHY15, MBC15, MDB17, OdHi12, PDT12, PWVT12, RVH16, SDZ14, SP+13, WgMdZ12, WgMW12, ZHS19, ZPW16, AabT16, ATKH17, APK18, BT18, CH10, CSH11, CLHJ13, DSCS12, GH16, GTSS19, HL14, KKM13, KLW16, KDW17, LH10c, LNM11, LNKL13, LH13, MM12, OKG12, hSZZ15, SHBC19, WDKV19, WT10a, WOLS12, YHL16, YSL10]. User-centric [BLV17]. User-controlled [Har16].

User-Friendly [SDZ14, WOLS12]. User-Generated [LCL17b]. User-Level [BKJP12]. user-participating [CH10]. User-Transparent [ZHS19]. Users [DPCM16, KKA15, TAKS10, WPZ16, ATK11, uHAN18]. uses [Rus15]. Using [ABS12, ABB14, Anot15a, Ayu12, ARM15, BBC13, BCPV11, Bee17, BFMT16, BKLS12, BJR14, CST17, CCL13, DSB16, DR12, DA10, DBPS12, DL12, ERLM16, ERRMG15, FMS12a, GH11a, GSC17, GAS16, HEK18, HHS15, IL15, JIN10, JEA15, KL11, Lac15, Lan11, LYK13, LLG16, MM17, MBC15, MRL18, MS16, NIS12, NGuH16, NNAM10, NN12, NMS14, PMZ13, PSS13, PAF18, PDM12, PDT12, PCPK14, RVRC12, SR12a, SFE10, SSA13, SRA17, SC12, SR12b, Tan12a, TKR14, WWL14, WgMdZ12, WY12, XZI18, YWW10, YNNW15, YCL17, YSS14, ZH15, ZPW16, ZS12, dRsdVC12, ATKH17, AHiM18, APK18, ASVE13, BLL19, BM13, CSH18, CHS11, CR12, CLHJ13, CP13, CR16, DAV11, DTZZ12, uHAN18, EEAZ13, FES10, Ham19, Har14, HZW17, HWW12, H14, HYY10, HCC10, HS11, JCS16, JMW16, K11, KY10, KKG14, KM11].

using [KUS13, KUTU16, KBP17, KLL16, LXX12, LLP18, LCI17, LH10c, LNM11, LXMW12, LH13, LML13, MM12, MS13a, MMSD13, MM14a, MKH12, MRRT17, GSM18b, NTK17, PBC14, PC14, QD16, RS15, RS17, Sar11, SGFC18, SRS18, SAR18b, TLC16, TG17, TK14, TLL13, UUN11, WY12, WHJ17, YQH12, YZZ14, YSL10, ZK1A17, ZLW12, ZY1C17, ZXW18].

utilization [NZM10].


Verifiability [RST15a, RST15b, VSR12, WWHL12, YMC+17, BRR+15, Hwa11]. Verifiable [CFE16, CRST15, Fuc11, HYS11, HLC12, LLL+18, QD16, RDZ+16, SZQ+17, WWHL16, YNR12a, YCR16, LZY+16, LJW+17, NMP+13, FHGR16, QS18, XWS17, ZZ15]. verifiably [SEXY18, ZLY10].

Verification [App15, ABR12, BL15, CCK12, CCCK16, CM11, EWS14, Ess17, GLLSN12, GdM16, GMSV14, Lin15, MV16a, OS12, PNRC17, SOF12, Tom16, Vet10, ZPW16, AGHP14, ABF+14, ASVE13, BFG+14, BTW15, GNP+12, KKK+16, LEW19, MR14c, NPH+14, SD10, XHM14, YNX+16].


Video [BWR12, D1G1, KS1B17, JSZS12, O1+S, TWZ+12, WLZL12, YE12, YT12, Cri16, LLHS12, MK11, OCGD11, XWZW16].


Vulnerability [M1N13, TM12, VKC15, Wal18, Ano17f, DMWS12, MYY13]. Vulnerable [Ano15d]. vVote [CRST15].

W [Mar10a, X1e12, H1l13]. W-OTS [H1l13]. WA [LCK11]. Waknaghat [CGB+10].

Walker [Xie12]. Wallets [Chi13b]. Wallis [Wes16]. War [Has16, M1n17, Bud16, Car11, Sml11a].

Warbler [MFG16]. warriors [Bud16]. wartime [McK10, McK11]. was [Goo12, LHA+12]. Watermark [CHHW12, DLM+18, EM14, J1n10, KBL11, LZC+12b, MCD12, SJ12, YE12, ZS12, HB13, TLL13, WYL13].

Watermark-Driven [DLM+18].

Watermarking [BCGAPM12, BF12, BCPV11, BDB14, BBM15, CG12b, CHHW12, CCZC13, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HEK18, HGT15, HMMK14, JSZS12, Joh10, JKHeY12, KD12a, LSL12b, LP12, LD13, MM17, MR16, MU12, NGAnuo1Q16, NC12, NXH+17, pNyWyY+14, OWHS12, RS16, RP12, RR11, RMG18, SAA15, SLGZ12, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, gWpNyY+14, W1W12].
REFERENCES


References

Akyildiz:2014:OTB

Applebaum:2017:AC

Abo-alian:2016:KDB
Ambrosin:2016:FAB


Albertini:2014:MHE


Arora:2012:ILM


Akleylek:2016:SPM


Aghili:2018:ISA

REFERENCES


Athmani:2019:EED

Almeida:2013:CCA

Ambrosin:2017:OBB

Ateniese:2017:LCS

Arnold:2012:ICC
Adrian:2015:IFS

Agosta:2015:OPP

Abe:2010:ACA

Abe:2012:TBG

Arriaga:2012:JSS
REFERENCES

Almeida:2014:COS

Ananth:2013:SFP

Avoine:2016:SSP

Aid:2013:DIO

Acar:2013:SPA
Andreeva:2012:SAS


Arapinis:2012:RET


Arias-Cabarcos:2015:BIP


Arnold:2015:NGH

T. W. Arnold, M. Check, E. A. Dames, J. Dayka,

[ACM10]


[ACM11]


[ACK10]

REFERENCES


REFERENCES


Ahmed:2017:IRD


Attrapadung:2015:RGS


Antonopoulos:2017:DIS


Ahani:2015:AAI


Akin:2014:MGA


Abdullaziz:2016:AAI

REFERENCES

Attrapadung:2012:ABE


Ali:2018:ECM


Appelbaum:2013:SSG


Ak:2014:ICS


Aia:2015:FAA


Ali:2018:CBR

Zulfiqar Ali, Muhammad Imran, Mansour Alsulaiman, Muhammad
REFERENCES


Amin:2016:DAP

Amin:2018:UAP

Alhanahnah:2016:MTI

Applebaum:2014:HGA

Alander:2016:MAB
REFERENCES

October 2014. CODEN IT-COB4. ISSN 0018-9340 (print), 1557-9956 (electronic).


[AlTawy:2013:SOC] Riham AlTawy, Aleksandar Kircanski, and Amr Youssef. Second order col-
REFERENCES

Alash:2015:IAA


Aldrich:2011:GUS


Au:2018:PPP


Alomair:2012:AEH


Alpar:2018:BTA

REFERENCES


Adj:2013:WDC


Aumasson:2014:HFB


Albrecht:2012:SDL


Arshad:2015:SAI


[AMS+10] Zahra Ahmadian, Javad Mohajeri, Mahmoud Salmasizadeh, Risto M. Hakala, and Kaisa Nyberg. A prac-
REFERENCES


**Aga:2017:ISM**


**Anawis:2014:ARR**


**Anderson:2013:MNF**


**Anonymous:2010:NDS**


**Anonymous:2011:AIS**

Anonymous, editor. *ACIS international symposium on cryptography, and network security, data mining and knowledge discovery, e-commerce and its applications, and embedded systems*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA,
Anonymous:2011:AXL


Anonymous:2011:MCB


Anonymous:2012:SHS


Anonymous:2013:DSS


Anonymous:2013:NCI


Anonymous:2013:SSD


Anonymous:2013:SIS

Anonymous. Special issue on “Security and identity architecture for the future Internet”. Communicati...
REFERENCES


Anonymous:2014:ERE


Anonymous:2015:BSU


Anonymous:2015:BRDa


Anonymous:2015:QCS


Anonymous:2015:UGB

[Ano15e] Anonymous. UK Government battles tech firms over encryption. Net-
Anonymous:2016:CPSd


Anonymous:2016:CPSe


Anonymous:2016:EMT

REFERENCES


[Ano17a] Anonymous. BitErrant attack. Web site, March 6, 2017. URL http://biterrant.io/. The story describes how SHA-1 collision attacks could lead to bogus, and malware, file downloads via BitTorrent: the obvious solution, which should have been adopted long ago, is to use multiple checksum algorithms, and require all to match before concluding that two files are in fact identical.


[Ano17c] 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.

city-conditions-first-time.

Anonymous:2017:MBH


Anonymous:2017:RV


The ROCA vulnerability affects millions of smartcards, and devices using 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.

Anonymous:2019:HCC


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW

REFERENCES

Aumasson:2011:CHF


AlFardan:2013:LTB


Ali:2018:SUA


Applebaum:2013:GXG


Applebaum:2014:CCP


Appel:2015:VCP

REFERENCES

ISSN 0164-0925 (print), 1558-4593 (electronic).


[ARM15] Reza Azarderakhsh and Arash Reyhani-Masoleh. Parallel and high-speed computations of elliptic curve cryptography us-


Ahmadi:2011:SKC

Ahmadi:2012:SKE


Asaar:2015:IBM

Alsulaiman:2013:IVB

Altman:2010:AAP
Alon Altman and Moshe Tennenholtz. An axiomatic

**Argyropoulos:2010:BTP**


**Au:2011:PPT**


**Alam:2015:ACF**


**Aslan:2016:DEM**

Ahmada:2014:RTN

Ahltawy:2014:IDR

Aysu:2015:FRT
Aydin Aysu, Bilgiday Yuce, and Patrick Schau-


REFERENCES


Barthe:2015:HAC


Barker:2016:RKM


Baylis:2010:CC


Bulygin:2010:OSS


Bax:2014:PPD


Bennett:2014:QCP


Beurdouche:2017:MSU


Beimel:2014:MLS


Bernstein:2017:SRD


Boldi:2012:IUG


Bollman:2015:PWI


Bernstein:2011:PCI

Daniel J. Bernstein and Sanjit Chatterjee, editors. *Progress in Cryptology — INDOCRYPT 2011: 12th International Conference on Cryptology in India, Chennai, India*,
Bichsel:2012:DMA

Badrignans:2010:SSA

Balfanz:2012:FA

Basin:2014:KYE

Bocu:2018:HEB
REFERENCES


REFERENCES


REFERENCES


[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


Belkacem:2014:DCM


REFERENCES

www.sciencedirect.com/
science/article/pii/S0743731518302582.

Bosseut:2016:EP


Bendlin:2011:SHE


Bertoni:2011:CSF


Bendlin:2011:SHE


Bertoni:2012:KIO


Boldyreva:2012:SSE


Bitansky:2013:WFS

Beebe:2017:MFC


Bellovin:2016:EEE


Bellovin:2018:UAE


Berghel:2012:ITF


Bera:2014:QC


Berghel:2016:DJT


Berghel:2016:S

REFERENCES


Bobba:2010:ABM


Bhargavan:2016:MVP


Beimel:2012:SSS


Bhargavan:2016:MVP


Boldyrev:2014:MEW


Battistello:2012:TBA

REFERENCES

Barthe:2012:CACb


Bossuet:2013:AFS


Barak:2010:IPO


Barak:2012:IPO


Barbulescu:2013:QPA

Barbulescu:2014:HQP


Barthe:2012:ACA


Biswas:2017:STC


Borcea:2017:PEE


Brakerski:2014:LFH


Barkatullah:2015:GCF

REFERENCES


Bonneau:2015:PEI


Biswas:2017:SA


Brumley:2010:CAI


Boche:2016:DSK

REFERENCES

CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.


Benhamouda:2016:NFP


Bouti:2012:SCB


Boldyrev:2012:NPG


Benhamouda:2016:NFP

[BK12b] Adil Bouti and Jörg Keller. Securing cloud-based computations against malicious


REFERENCES


REFERENCES


Byun:2011:SMC


Bai:2012:SSR


Bernstein:2014:HEC


Bidgoly:2015:MQV


Bernstein:2017:SCS


Blanchette:2012:BPC

REFERENCES

Blaze:2016:UHR


Benzaid:2016:FAW


Bai:2019:LMD


Buchmann:2017:PCU


Blomer:2012:TKG


Blondeau:2015:IDA

REFERENCES


Baldwin:2010:AFI


Biswas:2012:IBA


Backes:2012:GCP


Banik:2012:DFA


Babamir:2014:AKP


Buckley:2015:RVV

REFERENCES


REFERENCES


REFERENCES

128

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

**Bellare:2014:SSEa**


**Bellare:2014:SSEb**


**Boneh:2016:BCR**


**Balsa:2017:TIC**


**Brakerski:2014:VBB**


**Brakerski:2013:WHB**

REFERENCES


REFERENCES

Bellare:2012:MIS


Brumley:2012:SFI


Bajaj:2013:CSE


Birrell:2013:FIM


Bhattacherjee:2014:CAT


Bagheri:2015:NNA

REFERENCES


Boorghany:2015:CIL


Bojinov:2014:NMC


Basin:2011:AIS


Beaulieu:2013:SSF


Batina:2012:HEB

REFERENCES


Brocardo:2015:AVM


Buchmann:2010:EKG


Bulygin:2010:AOP


Bulygin:2010:CAC


Burke:2011:AMD

Brakerski:2011:EFH


Brakerski:2014:EFH


Bitansky:2018:IOF


Bayrak:2012:AII


Baek:2013:SPK


Bogdanov:2012:ZCL


Bhatnagar:2013:BIW

REFERENCES

[135]


[BAC14] CACM Sta. Know your steganographic enemy. Communications of
the Association for Computing Machinery, 57(5): 8, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


0169-2968 (print), 1875-8681 (electronic).

Chadha:2016:AVE


Chretien:2015:SPP


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO


Checkoway:2016:SAJ

Stephen Checkoway, Shaanan Colhney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Ho-vav Shacham, and Ralf-Philipp Weinmann. A systematic analysis of the Juniper Dual EC incident.
REFERENCES


Chadha:2012:AVE

Chatterjee:2016:TAD

Chou:2013:UGS

Chatterjee:2017:PBS

Chappell:2013:MCS

Cascudo:2015:SSN

Chatterjee:2017:PBS
REFERENCES


**Cho:2014:DGA**


**Chen:2011:EAA**


**Chu:2014:KAC**


**Chen:2010:ALD**


**Chen:2013:WSB**

REFERENCES


REFERENCES


[CFXY17] Kim-Kwang Raymond Choo, Yunsu Fei, Yang Xiang, and Yu Yu. Embedded device forensics and security. ACM Transactions
on Embedded Computing Systems, 16(2):50:1–50:??, April 2017. CODEN ???.
ISSN 1539-9087 (print), 1558-3465 (electronic).

**Chang:2010:PRN**


**Chen:2010:IFA**


**Cheraghchi:2014:NMC**


**Che:2012:WAM**


**Corrigan-Gibbs:2014:KS**

REFERENCES

145

magazine/article/?article_id=74801.

**Chaudhuri:2010:PIC**


**Caballero-Gil:2012:LAR**


**Chmiel:2012:EPC**


**Coull:2011:ACO**


**Cohney:2017:PSR**


**Curtmola:2011:SSE**

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

Cheng:2012:PAI


Cheng:2013:NIB


Chen:2010:NUP


Chang:2011:DEQ


Chan:2013:OCK

REFERENCES

Chang:2013:MPQ


Chappell:2013:PMI


Chen:2011:CCI


Cheswick:2013:RP


Chen:2015:SSS


Chen:2017:CSQ


[Cho10] Omar S. Choudary. The Smart Card detective: a hand-held EMV intersector. M. Phil. dissertation in Advance...
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


Chang:2019:GTS

REFERENCES

Chandra:2011:AST

Chung:2018:ERN

Chase:2013:SMN

Chuang:2011:LMA

Colin:2016:CTC

Comon-Lundh:2010:DSP
Chang:2011:RSB


Chen:2017:PGF


Chen:2016:RPR


Chen:2012:NCB


Chen:2013:TSE

REFERENCES


Baojiang Cui, Zheli Liu, and Lingyu Wang. Key-Aggregate Searchable Encryption (KASE) for group data sharing via cloud storage. *IEEE Transactions*


[CMG+18] Stephen Checkoway, Jacob Maskiewicz, Christina

CHECKOWAY:2018:WDL
REFERENCES


Jiageng Chen, Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. Vari-


DEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

**Corthesy:2014:SSD**


**Coutinho:2012:RPT**


**Claessen:2013:SPN**


**Canard:2018:NTC**


**Chung:2016:NBB**


**Chen:2018:RLF**

Yu Chen, Baodong Qin, and Haiyang Xue. Regular lossy functions and their applications in leakage-


[Chen:2012:DCC]

[Crampton:2011:PEC]

[Cramer:2012:TCT]

[Crav:2014:UCC]

[Clear:2012:CPA]
Michael Clear, Karl Reid, Desmond Ennis, Arthur Hughes, and Hitesh Tewari. Collaboration-preserving authenticated encryption for operational transformation systems. Lecture
160


REFERENCES


Chen:2017:SIE


Chong:2015:SID

Stephen Chong, Christian...


*Calzavara:2015:SLA* Stefano Calzavara, Gabriele Tolomei, Andrea Casini,

Chin:2013:SMB


Chang:2012:GBP


Chou:2013:TIB


Crenne:2013:CMS


Calmon:2014:ITM

REFERENCES


Choi:2012:LT
[164]

Chung:2012:CBI
[184]

Chen:2014:DSE
[224]

Cao:2014:PPM
[252]

Chen:2016:EPN
[283]
Chen:2012:IDC

Chen:2012:CKS

Chen:2014:MLC

Chen:2015:TCP

Cheng:2015:OMU


REFERENCES

Danezis:2012:FCDb


Davies:2011:IST


Diong:2012:DAU


Dou:2018:OHR


Dacosta:2012:OTC


Cordeiro:2016:MPG

Weverton Luis da Costa Cordeiro, Flávio Roberto Santos, Marinho Pilla Barcelos, Luciano Paschoal Gaspary, Hanna Kavalionak, Alessio Guerrieri, and Alberto Montresor. Making

**Cordeiro:2012:IMB**


**DePrisco:2013:CVC**


**DaRolt:2013:NDS**


**Datta:2017:SFH**

Castro:2016:FVB


Danezis:2012:FCDa


Dew:2011:BRB

REFERENCES


REFERENCES


REFERENCES


[Dom12] Leonid Domnitser, Aamer

**Dolev:2012:ATC**


**Dello:2015:ICP**


**Dorre:2016:ELO**


**Doychev:2017:RAS**


**Durumeric:2014:MH**

Dolev:2016:MCG


Doychev:2015:CTS


Dodis:2012:MAR


Dunkelman:2012:MCE


Dong:2012:UAS


DeLuca:2015:SUS

Alexander De Luca and Janne Lindqvist. Is secure and usable Smartphone authentication asking too much? *Computer,
REFERENCES

Degefa:2016:PSE


Djaziri-Larbi:2018:WDA


Dong:2013:PRS


DiPietro:2016:CLD


Dodis:2011:SSC


Dai:2016:MLR

Shuguang Dai, Huige Li, and Fangguo Zhang. Memory leakage-resilient searchable symmetric encryption. Future Generation Computer Systems,
Duan:2016:SDC

DeCarneDeCarnavalet:2015:LSE

Demme:2012:SCV
REFERENCES


David:2012:UCO


Donovan:2014:ATM


Doroz:2015:AFH

Y. Doroz, E. Ozturk, and B. Sunar. Accelerating fully homomorphic encryption in hardware. IEEE Transactions on Comput-


Duncan:2012:CAI


Ding:2017:CSM


Das:2016:CWM

Dziembowski:2018:NMC


Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE

REFERENCES


Deng:2018:SFE


Dachman-Soled:2014:COF


Dini:2013:HHS


Drosatos:2017:PET


REFERENCES

Dong:2012:KKD


Dong:2012:NDI


Dai:2018:OPC


Deng:2014:CCC


Dodis:2013:O


Deng:2014:TNI

Lunzhi Deng and Jiwen Zeng. Two new identity-based threshold ring sig-
REFERENCES


Ehdaie:2016:HCR

Egele:2013:ESC

Esiner:2017:QRI

Esiner:2019:TFA

Edwards:2014:NRP

Edwards:2017:NSQ


Embar:2014:PWO

Evtushkin:2016:UMC

Eberz:2016:LLE

El-Razouk:2015:NHI

Estebanez:2014:PMC

Engels:2012:HLA
REFERENCES


Enos:2015:IBS


Farash:2014:ECC


Farash:2014:SEI


Fahd:2018:CPA


Fagone:2017:WWS


Farash:2014:CIE

Mohammad Sabzinejad Farash. Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. The Journal of Supercomputing, 70(2):987–
REFERENCES


[Fel13] Edward Felten. The Linux backdoor attempt


[Fel13] Edward Felten. The Linux backdoor attempt
freedom-to-tinker.com/
blog/felten/the-linux-
backdoor-attempt-of-2003/.

[FES10] Jean-Charles Faugère, Mo-
hab Safey El Din, and
Pierre-Jean Spaenlehauer.
Computing loci of rank de-
fects of linear matrices us-
ing Gröbner bases and ap-
plications to cryptology. In
Watt [Wat10], pages 257–
LCCN QA76.95 .I59 2010.

[FLE12] Ewan Fleischmann, Chris-
tian Forler, and Stefan
Lucks. McOE: a fam-
ily of almost foolproof on-
line authenticated encryp-
tion schemes. Lecture
Notes in Computer Sci-
CODEN LNCSDO. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-34047-5_12/.

[FGR17] Jingyuan Fan, Chaowen
Fan:2017:SSP

[FGR+17] E-Government (ICCEE),
Guangzhou, China, 7–9
May 2010. IEEE Computer
Society Press, 1109 Spring
Street, Suite 300, Silver
Spring, MD 20910, USA,
LCCN ???. URL http://
ieeeexplore.ieee.org/
servlet/opac?punumber=
5589107.

[FAR12] Oriol Farràs, Ignacio Gra-
cia, Sebastià Martín, and
Carles Padró. Linear
threshold multisecret shar-
ing schemes. Information
Processing Letters, 112
(17–18):667–673, Septem-
ber 30, 2012. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0020019012001378.
REFERENCES


Fan:2013:CPP


Fan:2010:AMI


Farras:2017:IRN


Fahl:2012:WEM


Fan:2010:PSN


REFERENCES

4913, December 10, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


REFERENCES

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

Ferguson:2010:SHF

Forler:2012:DAC

Feng:2012:CAO

Fallahpour:2015:AWB

Ferrag:2018:SCN

Farwa:2018:FAI
Shabieh Farwa, Nazeer Muhammad, Nargis Bibi, Sajjad A. Haider, Syed R. Naqvi, and Sheraz Anjum. Fresnelet approach for image encryption in the algebraic frame. Applied


REFERENCES


REFERENCES


**Fu:2015:TVG**


**Feng:2018:ALA**


**Fathimal:2016:SSS**


**Frattolillo:2015:WPP**


**Frattolillo:2016:BFM**


**Frey:2010:ABC**


[FS18] Somchart Fugkeaw and Hiroyuki Sato. Scalable and secure access control policy update for outsourced big data. *Future Generation Computer Systems*, 79 (part 1)(??):364–
REFERENCES


[Fang:2011:ICP]


[Fang:2012:CCS]


[Feng:2011:GDA]


[Feng:2011:GD]


[Feng:2011:GD]


[Fujioka:2012:SHI]

[FSX12b] Atsushi Fujioka, Taiichi Saito, and Keita Xagawa. Security enhance-

[Fujioka:2012:SEP]


[Fadlullah:2010:DCA]


[FVT+10]


REFERENCES

Groß-Amblard:2011:QPW

Gregio:2015:TTM

Gop:2018:LPP
Prosanta Gope, Ruhul Amin, S. K. Hafizul Islam, Neeraj Kumar, and Vinod Kumar Bhalla. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Future Generation Computer Systems, 83(??):629–637,

Fan:2013:KIS

Fan:2014:NCI

GomezPardo:2013:ICM

[GA11]
[FZT13]
[FZT14]
[GAF+15]
[GAI+18]
REFERENCES


Current developments and future trends in audio authentication. *IEEE Multi-

[Sourav Sen Gupta, A. Chatt-
topadhyay, K. Sinha, S. Maitra, and B. P. Sinha. High-performance hard-
ware implementation for RC4 stream cipher. *IEEE Transactions on Com-

[J. Guerra-Casanova, C. Sán-
chez-Avila, A. de Santos Sierra, and G. Bailador del Pozo. Score optimization and template updat-
ing in a biometric tech-
SODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://www.sciencedirect.com/
science/article/pii/S0164121211001427.

[Nilson Donizete Guerin, Jr., Flavio de Barros Vi-
dal, and Bruno Macchi-
avello. Text-dependent user verification of handwritten words and signa-
org/content/59/9/1415.
REFERENCES

Geller:2013:MIS


Gentry:2010:CAF


Gentry:2013:EMH


Gong:2010:PCI


Grigg:2011:CCN


Garg:2016:CIO


Gaspar:2012:SEF

Lubos Gaspar, Viktor Fischer, Lilian Bossuet, and Sanjam Garg, Craig Gentry, Shai Halevi, Mari-
Sanjam Garg, Craig Gentry, Shai Halevi, Mari-
a Raykova, Amit Sahai, and Brent Waters.
Candidate indistinguishability obfuscation and func-
929, 2016. CODEN SMJCAT. ISSN 0097-5397
(print), 1095-7111 (electronic).

Sanjam Garg, Craig Gentry, Shai Halevi, Mari-
a Raykova, Amit Sahai, and Brent Waters. Hiding
secrets in software: a cryptographic approach
to program obfuscation. *Communications of the
Association for Computing Machinery*, 59(5):
113–120, May 2016. CODEN CACMA2. ISSN
0001-0782 (print), 1557-7317 (electronic). URL

Sanjam Garg, Craig Gentry, Shai Halevi, and
Mari Raykova. Two-round secure MPC from indis-
tinguishability obfuscation. *Lecture Notes in
LNCSD9. ISSN 0302-9743 (print), 1611-
com/content/pdf/10.1007/978-3-642-20465-4_9.

Lifeng Guo and Lei Hu. Efficient bidirectional proxy


[GHPS13] Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart. Field switching


REFERENCES

3-642-13189-1 (softcover).
LCCN ????

cryptographic key length
recommendation. Web site,
February 26, 2015. URL
http://www.keylength.
com/.

Gao:2013:LCA

[GGJ13] Guangyong Gao and Guoping
Jiang. A lossless
copyright authentication
scheme based on Bessel-
Fourier moment and ex-
treme learning machine
in curvature-feature do-
main. The Journal
of Systems and Soft-
ware, 86(1):222–232, January 2013. CODEN JS-
SODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0164121212002270.

Gu:2015:EIB

identity-based proxy signa-
ture in the standard model. The Computer
Journal, 58(4):792–807,
April 2015. CODEN CM-
PJA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
conqnl.oxfordjournals.
org/content/58/4/792.

Gravier:2015:WOD

Sylvain Gravier, Jérôme
Javelle, Mehdi Mhalla, and
Simon Perdrix. On weak
odd domination and graph-
based quantum secret shar-
ing. Theoretical Computer
Science, 598(??):129–137,
September 20, 2015. CO-
DEN TCSCDI. ISSN 0304-
3975 (print), 1879-2294
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397515004806.

Goyal:2013:CZK

Vipul Goyal, Abhishek
Jain, Rafail Ostrovsky,
Silas Richelson, and Ivan
Visconti. Concurrent zero
knowledge in the bounded
player model. Lecture
Notes in Computer Sci-
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-36594-2_4/.

Gu:2017:IBM

Ke Gu, Weijia Jia, and
Jianming Zhang. Identity-
based multi-proxy signa-
ture scheme in the standard model. Fundamenta
Informaticae, 150(2):179–
210, ????. 2017. CODEN
FUMAAJ. ISSN 0169-2968
(print), 1875-8681 (elec-
tronic).
Geetha:2011:VRN  

Gaj:2017:DCR  

Garay:2016:MPA  

Guo:2010:HMW  

Grigoriev:2017:YMP  


Guo:2011:EDA


Guo:2012:ETD


Gradwohl:2010:SRC


Gradwohl:2013:SRC


Guo:2012:ETD


**Garcia-Morchon:2015:HCR**


**Guo:2011:ISS**


**Guo:2014:SAS**


**Gao:2014:URA**


**Groza:2017:LCL**

REFERENCES


Gong:2013:NOT


Goodrich:2012:EVW


Genkin:2016:PKE


Grossschadl:2012:EJI


Genkin:2014:GYH

Daniel Genkin, Itamar Pihman, 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

Antonio González-Pardo, Pablo Varona, David Camacho, and Francisco de Borja Rodríguez Ortiz. Communication by identity discrimination in bio-inspired multi-agent sys-

**Greengard:2011:MRM**


**Green:2017:SSE**


**Grimes:2015:CCT**


**Gibson-Robinson:2012:AAL**


**Guha:2017:RTS**


**Guin:2016:FCS**

Ujjwal Guin, Qihang Shi, Domenic Forte, and Mark M. Tehranipoor. FORTIS: a comprehensive solution for establishing forward trust for protecting IPs and ICs.
REFERENCES


220


[GWpNyY] Xiangyang Wang, Panpan Niu, Hongying Yang, Yan Zhang, and Tianxiao Ma. A robust audio watermarking scheme using higher-order statistics in empirical mode decomposition domain. *Fundamenta*

Gao:2015:GCC


Goh:2013:TOT


Guo:2012:AKE


Guo:2017:EMD


Gao:2012:RHC


Guo:2018:SMK

Ziqing Guo, Hua Zhang, Caijun Sun, Qiaoyan Wen, and Wenmin Li. Secure multi-keyword ranked


REFERENCES


[Harn:2013:GA]


[Har16] Hardesty:2016:SUC

[Has16] Hastings:2016:SWS


REFERENCES


Hurlburt:2014:BBC


Hetzelt:2017:SAE


Hernandez-Becerril:2016:GIS


He:2013:HEH


Hulsing:2017:XEH


Hao:2012:SAM


[HCL+14] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, and Li Xu. Further observations on smart-card-based password-authenticated


[Huang:2014:FOS] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, and Li Xu. Further observations on smart-card-based password-authenticated
REFERENCES


[Hwang:2012:ABA] Jung Yeon Hwang, Sungwook Eom, Ku-Young Chang, Pil Joong Lee, and

Hamad:2018:DWU


Hellman:2017:TLC


Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Heys:2017:SCF

**Harn:2014:MTS**


**Hoang:2014:IMD**


**Hua:2015:TSE**


**Heyse:2012:TOC**


**Huang:2016:EDP**


**Han:2011:PEB**

REFERENCES


(HH+13) Y.-I. Hayashi, Y. Hayashi, N. Homma, T. Mizuki, and T. Aoki. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. IEEE Transactions on Electromagnetic Compatibility, ??


HONG:2015:RSM


HINAREJOS:2015:MES


HINEK:2010:CRV


HIKELMANN:2011:CPA


HUR:2014:SDR


HOUMANSADR:2014:NBW

REFERENCES


REFERENCES

tronic). URL http://
/ieeexplore.ieee.org/
stamp/stamp.jsp?tp=&arnumber=
5416683.

[HL10b] Carmit Hazay and Yehuda
Lindell. Efficient Secure
Two-Party Protocols:
Techniques and Construc-
tions. Information Security
and Cryptography. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc., 2010. ISBN 3-642-
14302-4 (hardcover), 3-642-
14303-2 (e-book). ISSN
1619-7100 (print), 2197-
845X (electronic). xiii +
263 + 1 pp. LCCN Z103
H39 2010. URL http://
www.springerlink.com/
content/978-3-642-14303-
8.

[HLC12] Chunqiang Hu, Xiaofeng
Liao, and Xiuzehn Cheng.
Verifiable multi-secret shar-
ing based on LFSR se-
quencies. Theoretical Com-
puter Science, 445(1):52–
62, August 3, 2012. CODEN
TCSCDI. ISSN 0304-
3975 (print), 1879-2294
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397512004276.

[Hs:2011:NIB] Chien-Lung Hsu and Han-
Yu Lin. New identity-based
key-insulated convertible
multi-authenticated en-
cryption scheme. Journal
of Network and Computer
Applications, 34(5):1724–
1731, September 2011. CO-
DEN JNCAF3. ISSN 1084-
8045 (print), 1095-8592
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1084804511001172.

[HL14] Wen-Bin Hsieh and Jenq-
Shiou Leu. An anony-

mous mobile user authenti-
cation protocol using self-
certified public keys based
on multi-server architec-
tures. The Journal of Su-
percomputing, 70(1):133–
148, October 2014. CO-
DEN JOSUED. ISSN
0920-8542 (print), 1573-
0484 (electronic). URL
http://link.springer.
com/article/10.1007/s11227-
014-1135-8.

[Hmood:2015:A] Haider Salim Hmood, Zhi-
tang Li, Hasan Khalaf Ab-
dulwahid, and Yang Zhang.
Adaptive caching approach
to prevent DNS cache poi-
soning attack. The Com-
puter Journal, 58(4):973–
985, April 2015. CODEN
CMPJA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
comjnl.oxfordjournals.
org/content/58/4/973.

[Hu:2012:VMS] Chunqiang Hu, Xiaofeng
Liao, and Xiuzhen Cheng.
Verifiable multi-secret shar-
ing based on LFSR se-
quencies. Theoretical Com-
puter Science, 445(1):52–
62, August 3, 2012. CODEN
TCSCDI. ISSN 0304-
3975 (print), 1879-2294
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397512004276.
Hu:2016:PBR


Huang:2011:ISL


Huang:2015:MSE


Harn:2011:FDM


Han:2018:TSE


Huffmire:2010:SPR

Ted Huffmire, Timothy Levin, Thuy Nguyen, Cynthia Irvine, Brett Brotherston, Gang Wang, Timothy Sherwood, and Ryan Kast-


References


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Shi:2015:CTS

Hu:2010:TTW

Hamdy:2011:HPB

Henson:2013:MES

Huang:2015:SSS

Huang:2017:SSS
Kaibin Huang, Raylin Tso, and Yu-Chi Chen. Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption. Journal of Com-
Herbert:2012:SMP


Hald:2015:RRA


Hurlburt:2016:MBO


Harvey:2017:FPM


Han:2012:MIA


REFERENCES


See [?].


[Hao:2011:NTV]

[Huang:2011:GFT]

[Huang:2018:PIB]

[Huang:2018:CT]


See [?].

Heys:2011:PSC


Han:2012:ERI


Han:2014:ATS


He:2017:AHA


He:2018:LAB


He:2015:IEI


Islam:2015:MBA


Ismail:2010:EAE


Islam:2011:MES

IEEE:2010:PIA

IEEE:2011:ICI

IBM:2013:DMP

IBM:2013:IPC

Irshad:2017:CPP

IEEE:2011:PIA
REFERENCES

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. The Computer Journal,


REFERENCES

Irshad:2016:EAM

Ishai:2014:PCP

Jie:2010:AAI

Jie:2011:RGA

Prins:2011:DCA
JR Prins and Business Unit
REFERENCES


Jain:2013:MSD


Jho:2016:SSE


Jakobsson:2012:AWD


Chang:2012:TRR


Jogenfors:2015:HBT


Jeong:2013:CBC

REFERENCES


**Jin:2010:ADW**


**Jain:2010:QP**


**Jawad:2013:GAD**


**Jiang:2016:PPT**


**Jun:2012:IIR**


**Jan:2019:PBM**


**Jin:2010:ADW**


**Jain:2010:QP**


**Jawad:2013:GAD**


**Jiang:2016:PPT**

REFERENCES


Jovanovic:2012:FAL


Joseffson:2016:ECD


Jeong:2012:IKP

REFERENCES


**Jefs:2013:CCP**


**Juels:2014:HEE**


**Jevdjic:2017:ASC**


**Jain:2016:APQ**


**Jadmayer:2017:BCI**

REFERENCES


Jiang:2016:CVI


Juels:2014:INC


Jiang:2017:SLD


Joux:2014:SAC


Jiang:2010:EDI

Yixin Jiang, Haojin Zhu,
REFERENCES


Khazaei:2017:COA


Kurkcu:2018:CBE


Kornycky:2017:RFT


Koziel:2018:HPS


Kamp:2013:MES


Kamp:2016:MEM

REFERENCES

Kapera:2011:SPD

Kapera:2013:MRM

Karafyllidis:2012:QGC

Kong:2015:CSM

Katz:2013:RIB

Kawamoto:2015:LSH

Karthigaikumar:2010:PPV
P. Karthigaikumar and K. Baskaran. Partially pipelined VLSI implementation of Blowfish encryption/decryption algo-
REFERENCES


REFERENCES

Karakoc:2015:AKA


Kumari:2017:DSU


Kara:2019:ALS


Keblusek:2015:BRK


Kemshall:2011:WMT


Kleinjung:2010:FBR

[Thorsten Kleinjung, Kazumaro Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne]
REFERENCES


Kikuchi:2012:SSN


Kramer:2010:FDC


Kim:2012:SLT


Khedr:2016:SSH


Kwon:2010:SEB


REFERENCES

[102x68] KAI:2011:CIS


[102x68] KIAYIAS:2011:TCC


[102x68] KOMPARA:2019:REM


[102x68] KIM:2011:LBA


[102x68] KIM:2015:CEH


[102x68] KIM:2016:MAS


[KKA15] Abdul Nasir Khan, M. L. Mat Kiah, and Mazhar Ali. A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid ap-
REFERENCES


Khan:2014:MEK


Karopoulos:2010:FIP


Kubota:2016:SAV


Khan:2013:EDC


Khan:2014:IPR


Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Hamed Arshad,


REFERENCES

Kifer:2014:PFM


Koblitz:2015:RWE


Koblitz:2016:RWE


Kasamatsu:2012:TSE


Kiyoshima:2014:CRB


Karger:2011:LLB

Kanwal:2015:TTM


Katz:2012:TSP


Kavun:2018:SAE


Khovratovich:2010:RCA


Khovratovich:2010:RRA


Kumari:2016:APW


Koblitz:2010:BRB

Neal Koblitz. Book review: Decrypted Secrets: Methods and Maxims of
REFERENCES

CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Kasper:2012:SCA

CODEN LNCSDD. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-25286-0_5/.

Khamsemanan:2016:BBU

CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Kawachi:2017:GCR

Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasumaga. General constructions of rational secret sharing with expected constant-round re-


Kollmitzer:2010:AQC


Kang:2012:AKM


Kolman:2017:SCG

Eyal Kolman and Benny Pinkas. Securely computing a ground speed model.
REFERENCES


Koya:2018:AHM


Kumar:2017:TAU


Kiltz:2011:EAH


Khalid:2016:RHL


Kocabas:2012:CPB

Kang:2016:DSA

Keskinarkaus:2010:IWD

Krenn:2013:CCR

Knudsen:2011:BCC

Krantz:2012:EAM

Kostinger:2012:SBL
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-32717-9_20/.


REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-28490-8_14/.

**Klingler:2013:UPT**


**Kim:2012:SAH**


**Kawachi:2012:SKE**


**Kobayashi:2016:ASC**


**Klisowski:2012:CCP**


**Kai:2014:FSD**

Hiroshi Kai and Keita Ueda. Fake shares detection on a visual secret shar-
Kupcu:2013:DTT


Kupcu:2015:OAS


Kuznetsov:2011:APP


Kiljan:2018:ETA


Karpovsky:2014:DSS


Kuo:2016:SDD

Koyama:2012:NTD


Kamal:2010:EIN


Kuo:2018:DRA


Kate:2010:PBO


Lu:2010:MSC


Lathey:2015:IEE


Lackey:2015:UHP


[102x681]Liang:2015:SEC


[184x610]Landau:2010:SSR


[184x610]Landau:2017:LCI


[184x610]Launchbury:2012:TBC


[184x622]Lauter:2017:POL


B. Prathusha Laxmi and A. Chilambuchelvan. GSR: Geographic Secured Routing using SHA-3 algorithm.

Liu:2013:IA


Lathrop:2011:SPI


Lavington:2012:ATH


Li:2015:NAC


Lee:2017:SUE

Kwangsu Lee, Seung Geol Choi, Dong Hoon Lee, Jong Hwan Park, and Moti Yung. Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency. Theoretical Computer Sci-

[Li:2017:GAU]

[Li:2015:CEH]

[Li:2017:CCF]

[Liang:2014:CCS]


[Ledin:2016:RME]


[Lewand:2010:PC]


[Liu:2019:DVP]


[Liu:2016:LCR]


[Liang:2015:CPA]

Kaitai Liang, Liming Fang, Duncan S. Wong, and Willy Susilo. A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public

**Li:2017:PCL**


**Lancrenon:2012:IP1**


**Liu:2017:ECC**


**Lan:2010:RNG**


**Li:2012:FDM**


REFERENCES

Lee:2010:CGC

Li:2010:EBB

Lee:2011:PSE

Lin:2011:NIB

Lertvorratatham:2012:ISM

Liao:2013:NMS


REFERENCES


Li:2010:PAP


Li:2017:AMA


Lim:2011:NAN


Lin:2014:IVW


Lindell:2014:TCT

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
</table>
| Li:2016:IRI | Xinran Li, Chen-Hui Jin, and Fang-Wei Fu. Improved results of impossible differential cryptanaly-

**[Li:2017:SQS]**


**[LJW+17]**


**[Liu:2017:OO]**


Lin:2016:SCU


Lyu:2018:PKE


Li:2012:RIB


Li:2017:CIS


Liu:2018:GEI


Liu:2019:SBC

REFERENCES


Li:2017:CCD


Liu:2018:VSE


Libert:2019:ZKA


Lu:2012:IEC


[LLML12] Xianhui Lu, Bao Li, Qixiang Mei, and Yamin Liu.


REFERENCES


[LMD16] Anh Le, Athina Markopoulou, and Alexandros G. Dimakis. Auditing for dis-


[Liu:2015:SAB] Hong Liu, Huansheng


Robert J. Low. Book re-


[LPL12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An asymptoti-


Liskiewicz:2013:GBS

Liskiewicz:2017:SLS

Lane:2014:PBD

Luo:2012:FSU

Lin:2015:SSE

Lychev:2016:RSI
Lee:2012:IBS


Lei:2012:RAW


Liang:2015:EFC


Liu:2011:DBA


Liu:2011:NJD


Lin:2018:SSS

REFERENCES


[LT15a] Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang, Wang-Jui Tsai, and Po-Kai Zhong. Implementing multiple biometric features for a recall-based graph-

**Liu:2015:MSG**


**Lao:2016:BFD**


**Lysyanskaya:2010:AEC**


**Lin:2011:CNS**

Li:2016:LRC


Ludge:2012:NLD


Lucchese:2010:RPT


Lafitte:2011:CBF


Liu:2010:CIE


REFERENCES

Liu:2013:TIE

Lui:2013:CBS

Liu:2014:DAF

Liu:2017:EEC

Liu:2011:SBA

Li:2018:SCM
Xiong Li, Fan Wu, Muhammad Khurram Khan, Lili

Lu:2012:HOM


Lu:2014:HOM


Liu:2010:NDC


Liu:2010:SET


Liu:2011:PIA


Lu:2012:MMA


Lu:2012:ICB


Li:2010:GCP


Li:2012:IIA


Lou:2010:NAS


Lou:2010:NAS

Dai-Rui Lin, Chih-I Wang, Zhi-Kai Zhang, and D. J. Guan. A digital signature with multiple subliminal channels and its

[Li:2011:N1W]

[Li:2014:IBD]

[Li:2014:EMK]

[Lai:2012:RHB]

[Li:2012:ESD]
Luo:2014:ARP


Liu:2015:SDS


Lim:2016:AKE


Lu:2014:DAN


Liu:2015:SAA


Liao:2012:NSM


REFERENCES

1519, June 10, 2014. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Liu:2017:ESS

Liu:2014:CRA

Liu:2012:ESS

Li:2010:PES

Li:2016:BMA

Masdari:2017:STA
REFERENCES


MacCormick:2012:NAC


With a foreword by Christopher M. Bishop.

Macrakis:2014:PLS


Maffleo:2016:UNC


Michail:2012:EHT


Moskowitz:2010:ITE


Malkin:2013:SCB

Mangard:2013:KSL

Martin:2010:FWL

Martin:2010:PCC

Matsuda:2014:IBP
REFERENCES


Maurer:2012:CCN


Mayron:2015:BAM


Mazurczyk:2013:VSD


Milo:2011:FGB


Mao:2015:PUA


Malone:2013:MOD

Migliore:2018:PPF

Massolino:2015:OSC

Mukhopadhyay:2011:PEA

Madanayake:2012:BPS

McGrew:2017:IDH

McGrayne:2011:TWH

McKay:2010:SLB


McKay:2011:SLB


McKay:2012:SLC


Mahmood:2018:ECC


Marquez-Corbella:2015:ECP


Mathew:2015:NMB


Majzoub:2012:MRH

[MD12a] Sohaib Majzoub and Hassan Diab. MorphoSys reconfigurable hardware for cryptography: the Twofish
REFERENCES

Mansouri:2012:ACA

Mansfield-Devine:2015:MIC

Murdoch:2010:CPB

Mosenia:2017:PTS

Maachaoui:2012:MLA

Meiklejohn:2010:BRB

*Menezes:2013:IPB*


*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 Science*

Marmol:2010:TPA


Matsuda:2014:CCS


Meziani:2012:IPS


Mou:2013:CBC


Mohd:2015:SLB

Bassam J. Mohd, Thaier Hayajneh, and Athanasios V. Vasilakos. A survey on lightweight block ciphers for low-resource de-
REFERENCES

Mohd:2018:HDM


Micciancio:2010:FGC


Micciancio:2010:OWB


Midgley:2010:SEE


Martinez-Julia:2012:NIB

Martinez-Julia:2013:BSI


Muller:2012:HPC


Moazaffari-Kermani:2017:FDA


McGrew:2016:SMH


Mohanty:2011:RTP


Moessner:2012:SAS


MK11

MK12a

MK12b

MK13

MK14

MK15

MK16

MK17

MK18

MK19

MK20

MK21


Maity:2014:FIR [MM14a] Hirak Kumar Maity and Santi P. Maity. FPGA implementation of reversible watermarking in digital im-


**[MMP19]** Francesco Marino, Corrado Moiso, and Matteo Petracca. Automatic contract negotiation, service discovery and mutual authentication solu-

**Macedo:2017:SSP**


**Maity:2013:CRS**


**Matsuo:2012:MAK**

REFERENCES

Meshram:2012:IBC


Moran:2010:BCP


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

Marine Minier and María Naya-Plasencia. A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock. *Information Processing Letters*, 112(16):624–629, Au-


REFERENCES


Subhayan Roy Moulick.

Marine Minier and Raphael C.-W. Phan.

Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage.

Philipp Mundhenk, Andrew Paverd, Artur Mrowca, Sebastian Steinhorst, Martin Lukasiwycz, Suhaib A. Fahmy, and Samarjit Chakraborty.

Ilya Mironov, Omkant Pandey, Omer Reingold, and Gil Segev.
Mukhamedov:2010:IEP


Maimut:2014:AET


Marasco:2014:SAS


Micali:2014:CMS


Manimekalai:2016:NRR


Migliore:2018:HSC


Martinovic:2017:AUP

[MRRT17] Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin, and Gene Tsudik. Authentication using pulse-response biometrics. *Com-
Matsumoto:2017:ACG


Moghadam:2010:DRN


[MRTV12]

Mendel:2012:DAL


Maitra:2012:NAC


[MRT10]

Mroczkowski:2012:CAS


References

[MSas13] Myers:2013:BBC


Michele Mosca, Douglas Stebila, and BerkantUstaoglu. Quantum key...

**Morozov:2012:ZKP**


**Malkin:2011:ECS**


**Meerwald:2012:ERW**


**Muftic:2016:BCC**


**Mundy:2017:CGU**


**Murphy:2010:BRB**

Cillian Murphy. Book review: *Introduction to Cryptography*, by Hans...


[Mur16]

Murdoch:2016:IDP


[MV16a]

Miri:2012:SAC


[MvO11]

Mannan:2011:LPD


[MV12]

Mishra:2016:AFP


[MV16b]


[MV16a]

Mishra:2016:AFP


[MV12]

Mannan:2011:LPD


[MV12]

Roel Maes, Anthony Van Herreweghe, and Ingrid Ver-


Mastroeni:2017:APS


Manshaei:2013:GTM


Ma:2015:PKE


Nagy:2010:OTP


Nagy:2010:QCS


Naccache:2012:CST


Naccache:2016:FHE

David Naccache. Fully

**Naranjo:2012:SAK**


**Nunez:2017:PRE**


**Noureeddine:2013:AMT**


**Nain:2017:SPE**


**Naskar:2012:FIR**


Nedjah:2016:PYP


Newell:2013:PCD


Naeem:2014:EIC


Nafea:2016:HMB


NIST:2012:RRN


NIST:2013:CSS

NIST. Cryptographic standards statement. National Institute of Stan-
Nguyen:2014:DDI


Ning:2012:DPB


Ning:2015:APB


Ning:2012:DCA


Nieto:2013:PVC


Nieto:2014:FSH

REFERENCES


[Nos14] Peter Nose. Security weaknesses of a signature scheme and authenticated key agreement protocols. Information Process-
Novotny:2010:TAE


Nichols:2014:CSS


Nguyen:2011:APB


Nguyen:2012:SOU


Namasudra:2017:NSA


Niu:2015:CRS

Dannmei Niu, Lanlan Rui, Cheng Zhong, and Xuesong Qiu. A composition and recovery strategy for mobile social network service in disaster. *The Com-


Nguyen:2012:LRS


Nguyen:2010:LAS


Noorman:2017:SLC


Nie:2013:CHB


Natgunanathan:2017:PBM


Ogiela:2012:UML


Ohtake:2012:AAH


Ogiela:2018:LTC


Orlandi:2014:SCN


Oppliger:2011:CC

REFERENCES

Orejel:2014:E


Ormond:2016:CPR


Ozen:2011:MIS


Owczarek:2012:LPL


Osborn:2016:SSR


Orencik:2016:MKS

REFERENCES


[PA10] V. Lakshmi Praba and G. Arumugam. Message authentication code algo-

**Parveen:2018:IEE**


**Pal:2015:SDC**


**Parent:2012:WAI**


**Park:2012:AP0**


**Pan14**


**Par12a**


Paul:2016:TSO


Papadopoulos:2014:LQA


Premnath:2014:EHR


Poh:2017:SSE


Pang:2014:PPA


Paul:2012:KSS

Pereira:2015:PKE


Pippal:2012:SVU


Pearson:2011:NWC


Persichetti:2013:SAH


Peterson:2011:SWS


Petric:2012:PRE

REFERENCES


Parno:2016:PNP


Papas:2012:MLR


Park:2010:SIC


Pieprzyk:2010:TCC


Pointcheval:2012:ACE

REFERENCES


Premarathne:2015:LDD


Pramila:2018:ICA


Peter:2012:AHE


Phuc:2016:SAS

Tran Song Dat Phuc and Changhoon Lee. Security analysis of SDDO-based block cipher for wireless sensor network. The Journal of Supercomput-


REFERENCES


Pande:2013:SMC


Poursakidis:2010:TPC


Puthal:2017:DDK


Niu:2014:RDW


Powers:2014:OSCa


Paar:2010:UCT


Papadopoulos:2010:TRM

Konstantinos Papadopoulos and Ioannis Papaefstathiou. Titan-R: a multigigabit reconfigurable

**Park:2011:ACC**


**Pereira:2016:SHB**


**Pendl:2012:ECC**


**Pyun:2012:IBF**


Pereira:2013:SLC


[PSdO+13]

Phatak:2013:SIN


[PSJ+13]

Patranabis:2017:PSK


Picazo-Sanchez:2013:CRS


[PSOMPL13]

Park:2013:PPM


REFERENCES

46–54, January/February 2012. ISSN 1540-7993 (print), 1558-4046 (electronic).


REFERENCES

Pughters:2018:CBE

Pouraghani:2018:NNE

Patsakis:2015:PSM

Qiu:2018:QDS

Qin:2016:VTQ

Qu:2013:DPA
Bo Qu, Dawu Gu, Zheng Guo, and Junrong Liu. Differential power analysis of stream ciphers

**Qin:2017:DIR**


**Qiu:2017:AAS**


**Qiao:2018:CTC**


**Quaglia:2018:SVA**

REFERENCES


REFERENCES


REFERENCES

Ruoti:2015:WJS

Rupp:2015:CTM

Radke:2015:CFA

Reaves:2017:MBM

Raisaro:2018:PPS


REFERENCES


REFERENCES


REFERENCES

[Rosen:2010:CCS]

[Reeder:2011:WPD]

[Rivest:2014:SSR]

[Rossi:2015:IBS]

[Rana:2016:DBV]

[Roy:2017:LOS]

[Rangasamy:2012:ERP]
Jothi Rangasamy, Douglas Stebila, Colin Boyd, and Juan Manuel González-Nieto. Effort-release

Ren:2018:IAS


Raju:2014:DA


Ryan:2015:EEVa


Russo:2015:FPT

Alejandro Russo. Functional pearl: two can keep a secret, if one of them uses Haskell. ACM SIGPLAN Notices, 50(9):280–288, September 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Rahulamathavan:2016:UCA


Rodriguez-Vazquez:2012:SCB


Roettger:2012:PKC


Ren:2014:HHM


Rogaway:2012:SCS

REFERENCES


Ren:2013:PPK


Ristenpart:2010:WGR


Rajendran:2015:FAB


Sang:2012:SSF


Sakalli:2014:ACC

Muharrem Tolga Sakalli and Bora Aslan. On the algebraic construction of cryptographically good $32 \times 32$ binary linear transformations. Journal of


[RWZ13]

RY10

[SA12]

[SA14]

[RYF+13]


Sarreshtedari:2015:WMD


Schutz:2010:DIN


Sacco:2014:MC


Sahai:2013:TCT


Saeed:2016:IID


Saleh:2016:PED

Sarier:2010:IAS

Sarkar:2010:SGC

Sarier:2012:SNB

Sarkar:2011:TES

Sarkar:2014:PEK

Sarier:2018:MBI

Singh:2018:SDD
Priyanka Singh, Nishant Agarwal, and Balasubramanian Raman. Secure


REFERENCES

4:??, August 2014. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).


Edward F. Schaefer. Book review: The Mathematics of Encryption: An Elementary Introduction, Re-

[Sch16]


[Sch15b]


[Sch15c]


[Schneier:2016:CHT]


[SCKH10]


Sendrier:2017:CBC


Serrato:2012:IAN


Sakai:2016:CDN


Sethumadhavan:2016:HEP


Severance:2016:BSB


Seo:2018:AOF

Jae Hong Seo, Keita Emura, Keita Xagawa, and Kazuki Yoneyama. Accumulable optimistic fair exchange from verifiably encrypted homomorphic signatures. *International Journal of In-
REFERENCES

[Savas:2014:SMQ]

[Su:2012:IIN]

[Shabtai:2010:SAP]

[Schneier:2015:SWC]

[Sasdrich:2015:ICS]

[Shu:2014:DAS]
Saxena:2016:API


Silva-Garcia:2018:SBG


Sun:2015:FSW


Sanchez-Garcia:2016:SSA


Sun:2015:FSW


[SGY11] Zhang Shaolan, Xing Guobo, and Yang Yixian. An efficient domain extension to construct a cryptographic hash function. In


Amar Siad. A new approach for private searches on public-key encrypted
Simion:2015:RST


Simmonds:2015:DII


Sirer:2016:TPS


Shakeri:2012:RZW


Shin:2017:CGI


Sabri:2011:AFS

Khair Eddin Sabri and Ridha Khedri. Algebraic framework for the specification and analysis of cryptographic-key distribution. Fundamenta Informaticae, 112(4):305–335,
REFERENCES

December 2011. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).


[SK12a] Sachnev:2012:IME

[SK12b] Seo:2012:MPM


[SKB+17] Son:2017:NOC


[Soupionis:2014:GTA]


[SKB+17] Son:2017:NOC


[SKH17] Shin:2017:SSD


Tobias Scheidat, Karl Kümmel, and Claus Vielhauer. Short term template aging effects on biometric dynamic handwrit-
REFERENCES


Roland Schmitz:2012:NAC


Mudhakar Srivatsa:2011:ESA


David Schultz:2010:MMP

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 ???.

U. Somani:2010:IDS


Shi-Feng Sun:2016:RSP

Jun Shao, Peng Liu, and Yuan Zhou. Achieving key privacy without losing CCA security in


Sengupta:2012:SAI


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 ????.


Pawel Swierczynski, Amir Moradi, David Oswald, and Christof Paar. Physical security evaluation

**Stankovski:2014:CFE**


**Sharma:2018:CSS**


**Sadeghi:2010:THI**


3. Foreword by Pim Tuyls.

**Safavi-Naini:2011:USC**


**Seyedzadeh:2014:RCI**

REFERENCES


Suriadi:2012:PCV

Schaumont:2015:IEP

Suresh:2015:AGU

Serwadda:2013:ELK

Shiaeles:2015:FII

Shim:2015:SDA
Kyung-Ah Shim and Cheol-Min Park. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. IEEE Transactions on Parallel and Distributed Sys-

Spafford:2016:SE  

Safkhani:2014:CCA  

Sun:2013:IUP  
San-Tsai Sun, Eric Pospisil.


Serwadda:2016:TRR  

Shaikh:2010:CTO  


REFERENCES

Saklikar:2010:IFV

Saxena:2010:SGC

Sopka:2010:BTS

Szaban:2011:IQB

Saxena:2012:BIT

Shparlinski:2012:CSD
REFERENCES

Sendrier:2013:HCE

Sadhy:2017:PRE

Singh:2013:QBF

Smith:2011:SMC

Shrivastava:2012:UIE

Strydis:2013:SAP
Christos Strydis, Robert M. Seepers, Pedro Peris-Lopez, Dimitrios Siskos,

**Sood:2011:SDI**


**Spiez:2012:RCT**


**Sahai:2012:DCC**


**Schiller:2014:CCA**


**Shen:2016:RMM**

[Wuqiang Shen and Shaohua Tang. RGB, a mixed multivariate signature scheme. *The Com-
REFERENCES


Stallings:2011:CNS


Stanojevitch:2011:ICM


Stanek:2012:TEM


Staff:2013:ITD


Stewart:2011:CCI


Steel:2015:APF

REFERENCES

Stenn:2015:SNT

Stipcevic:2011:QRN

Sticke:2015:CBS

Stolte:2012:EDA

Suciu:2012:SED

Sung:2011:DCE

Sun:2016:NEB
REFERENCES


REFERENCES

www.sciencedirect.com/science/article/pii/S0020019015001283


Song:2017:SSI


Seo:2013:PIC


Sui:2014:DAH


Shi:2013:REA


Song:2017:SAM


Sun:2017:CPP

Sun:2018:RPP

Sun:2017:CPP

Shen:2014:ERC

Shen:2014:ERC

Sun:2018:RPP

Sun:2018:RPP

Tsang:2010:BRR

Tsang:2010:BRR

Tamayo:2015:AFH

Tamayo:2015:AFH

Tan:2011:CTA

Tan:2011:CTA

Tan:2011:CTA


REFERENCES


[Tang:2015:CER]

[Tan:2017:JDC]

[Tian:2014:DFS]

[Tiplea:2014:NSC]

[Tao:2013:SMS]

[Terai:2011:BRB]
REFERENCES

DEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [?].

Tassa:2012:SDC

Tewari:2017:CNU

Tian:2016:IBS

Tian:2015:IBP

Tian:2012:TOE
Thabit:2014:RRW


Takayasu:2019:PKE


Tu:2014:EPB


Tani:2012:EQA


Tu:2013:PAQ


Tariq:2014:SBL

(print), 1558-2183 (electronic).


[Tsay:2012:VUL] Joe-Kai Tsay and Stig F. Mjølsnes. A vulnerability in the UMTS and LTE authentication and key agree-
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL 

Tsoutsos:2018:EDM

[TM18] Nektarios Georgios Tsoutsos and Michail Mani-
atakos. Efficient detection for malicious and random errors in addi-
document/7967774/.

Tang:2015:ECP

[TMC15] Qiang Tang, Hua Ma, and Xiaofeng Chen. Extend the concept of public key encryption with dele-

Tormo:2013:IMP

Girao, and Gregorio Martinez Perez. Identity management — in privacy we trust: Bridging the trust 
gap in eHealth environments. *IEEE Security 
CODEN ????. ISSN 1540-7993 (print), 1558-4046 (electronic).

Terrovitis:2011:LGR

[TMK11] Manolis Terrovitis, Nikos Mamoulis, and Panos Kal-
nis. Local and global recoding methods for anonymizing set-valued data. *VLDB Journal: Very Large 
VLDBFR. ISSN 1066-8888 (print), 0949-877X (elec-
tronic).

Terrovitis:2012:PPD

[TMLS12] Manolis Terrovitis, Nikos Mamoulis, John Liagouris, 
andSpiros Skiadopoulos. Privacy preservation by 
CODEN ????. ISSN 2150-8097.

Tao:2018:AAC

[TODQ18] Ming Tao, Kaoru Ota, Mianxiong Dong, and Zhuzhong Qian. Access-
ssAuth: Capacity-aware security access authenti-
cation in federated-IoT-enabled v2g networks.


[Trd11] Ken Taylor, Scott Rickard,
Tschorsch:2016:BBT


Tao:2014:CFS


Toreini:2017:TRP


Tang:2011:IDC


Tso:2013:SAI


REFERENCES

Wu:2012:SWG

Tartary:2011:EIT

Tian:2012:SSB

Tan:2016:CCA

Tolba:2016:GMA

Trammel:2012:DTP
John Trammel, Ümit Yağcınalp, Andrei Kalfas, James Boag, and Dan Brotsky. Device token protocol for persistent authentication shared across applications. Lecture Notes in Computer Science, 7592:
REFERENCES


[UK18] Uzunkol:2018:SWU


Vuagnoux:2010:CA


Wagstaff:2010:C


Wagner:2016:TPF


Walter:2018:RCS


Wang:2010:NSB


Wang:2013:CRA


Wang:2014:IIA


REFERENCES


REFERENCES

4472-1034-4 (paperback),
1-4472-4660-8 (ePub e-book). 400 pp. LCCN ????


Wei:2012:NCI


Wang:2017:DRM


Wang:2017:DVP


Wei:2016:PAB


[WH17] [WHC+15] [WHLH16]
REFERENCES


### REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume/Issue/Pages</th>
<th>URL</th>
</tr>
</thead>
</table>
REFERENCES


[Wang:2017:ABS] Qi Wang, Xiangxue Li, and Yu Yu. Anonymity for Bitcoin from secure escrow ad-


REFERENCES


[Wu:2016:CBE] Q. Wu, B. Qin, L. Zhang,

Wei:2015:TPE


Wu:2012:RGB


Williams:2013:APC


Whitworth:2014:SPC


Wang:2015:RSA

REFERENCES


[Watanabe:2012:ITT]

[Wang:2012:PAC]

[Wang:2013:NMC]
REFERENCES


[WW14] Ding Wang and Ping Wang. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solu-
Wen:2014:MZC


Wang:2011:MMW


Weng:2012:NCC


Wahaballa:2014:MLS


Werner:2017:CIM

Wang:2011:CIB


Wang:2011:CHI


Wang:2017:FWA


Wang:2016:SHI


Yuechuan Wei, Xiaoyuan Yang, and Chao Li. Impos-


REFERENCES


www.sciencedirect.com/science/article/pii/S1084804512002184


REFERENCES

ISSN 0018-9340 (print), 1557-9956 (electronic).

Xu:2012:AHA

Xiang:2016:EMP

Xue:2013:TCB
Kaiping Xue, Changsha Ma, Peilin Hong, and Rong Ding. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer App-


Xie:2013:ECP

Xiang:2014:PBA

Xia:2015:SPK


REFERENCES


[XWZW16]

**Xu:2018:SKS**


[XWY18]

**Xu:2018:DFH**


[XWZ18]


[XXZ12]


[XXX15]

**Xie:2012:DPK**

Xiao:2018:KRL


[XY18]

Xing-Yuan:2011:PRS


[XYYXY11]

Xiao:2018:FEI


[XZZ18]

Yo+o:2017:PQD


[Y+17]


[Yang:2011:GSS] Ching-Nung Yang and Yu-Ying Chu. A general \((k,n)\) scalable se-

**Yang:2012:PST**


**Yang:2016:EBB**


**Yi:2017:ZCL**


**Yuan:2013:PV**


**Yu:2016:DNF**

Yao:2015:LAB


Yuen:2012:IBE


Yu:2017:PDA


Yasuda:2015:MQC


Yan:2016:DEB


Ye:2010:ACC

Yamada:2012:PBR


Ye:2014:NIE


Yekhanin:2010:LDC


Yoshida:2012:OGT


Yu:2012:EPF


Yang:2017:CCS

REFERENCES


Yuce:2017:AFI


Yang:2015:SHI


Ye:2018:RKF

REFERENCES


Yang:2016:IHA


[184x646]Yu:2010:IBF


Yu:2011:FSI

Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, and Jianxi Fan. Forward-secure identity-based public-key encryption without random oracles. Fundamenta Informaticae, 111(2):241–256,

Yo:2010:IRR


[184x646]Yu:2010:FSI


[184x646]Yang:2016:EHA


[184x646]Yu:2011:FSI

Jia Yu, Fanyu Kong, Xiangguo Cheng, Rong Hao, and Jianxi Fan. Forward-secure identity-based public-key encryption without random oracles. Fundamenta Informaticae, 111(2):241–256,
Yu:2012:IRI

Young:2013:TPC

Yang:2018:AIW

Yum:2012:OPE

Yoshino:2012:SIP

Yum:2011:ACO
Dae Hyun Yum and Pil Joong Lee. On the average cost of order-preserving

Yi:2017:ICM


Yuen:2013:ELT


Yang:2012:WSI


You:2012:DDS


Yi:2013:ETS

Yu:2016:CBE


Yu:2017:A


Yagan:2016:WSN

Yakubu:2017:SSN


Yu:2017:A


Ying:2013:PPB


Yu:2010:PSI


References

Yu:2011:CLE

CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yu:2011:SPP

J. Yong. Security and privacy preservation for mobile E-learning via digital identity attributes. *J.UCS: Journal of Universal Com-
REFERENCES


Yoneyama:2012:ORA


Yang:2012:EMA


Yin:2017:QPE


Yengisetty:2011:AVC


REFERENCES


REFERENCES

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


Lo-Yao Yeh, Woei-Jiunn Tsaur, and Hsin-Han

---

**Yang:2011:CCK**

**Yang:2011:CPK**

**Yamada:2012:UEW**

**Yeh:2017:SIB**
Lo-Yao Yeh, Woei-Jiunn Tsaur, and Hsin-Han

[Yang:2014:IBI]


[YTM+14]


[YTP11]

Yurong Yao, Edward Wat-

Yan:2017:PIS


Yang:2015:RCI


Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


REFERENCES


Yang:2017:SKS


Yang:2018:CDD


Yang:2012:BPN


Yang:2012:NIB


Yang:2014:PST

Zufiria:2017:GLM


Zidaric:2019:HOA


Zhang:2011:TNT


Zhu:2012:JLS


Zhang:2013:RMS


Zhang:2015:PCL

Zongyang Zhang, Sherman S. M. Chow, and Zhenfu Cao. Post-challenge leakage in public-key encryption. *Theoretical Com-
puter Science, 572(??):25–49, March 23, 2015. CO-
DEN TCSCDI. ISSN 0304-
3975 (print), 1879-2294
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397515000377.

[ZCWS15]
Zhi-Kai Zhang, Michael
Cheng Yi Cho, Zong-Yu
Wu, and Shiu-Hyung Win-
ston Sheih. Identifying
and authenticating IoT ob-
jects in a natural con-
text. Computer, 48(8):
81–83, August 2015. CO-
DEN CPTRB4. ISSN
0018-9162 (print), 1558-
0814 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0018916215001598.

[ZDL12]
Jiuling Zhang, Beixing
Deng, and Xing Li. Ad-
ditive order preserving en-
cryption based encrypted
documents ranking in se-
cure cloud storage. Lecture
Notes in Computer
CODEN LNCSDR. ISSN
0302-9743 (print), 1611-

[YWZ11]
Yu, Wen; Wang, Zhi; Zhou,
Yanlin. Novel and Ef
cient Adaptive Intruder
Identification in Wireless
Networks. Journal of Con-
current Engineering & Tech-
CODEN JCETEH. ISSN
0929-5032 (print), 1548-
l.org/journals/toc/jconengtech/19-2/.

[ZCL+12]
Zhifang Zhang, Yeow Meng
Chee, San Ling, Mulan
Liu, and Huaxiong Wang.
Threshold changeable se-
cret sharing schemes revis-
ited. Theoretical Computer
Science, 418(1):106–115,
February 10, 2012. CO-
DEN TCSCDI. ISSN 0304-
3975 (print), 1879-2294
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397511008206.

[ZCL+19]
Kai Zhang, Jie Chen,
Hyung Tae Lee, Haifeng
Qian, and Huaxiong Wang.
Efficient public key en-
cryption with equality test
in the standard model.
Theoretical Computer
Science, 755(??):65–80,
January 10, 2019. CO-
DEN TCSCDI. ISSN 0304-3975
(print), 1879-2294 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S030439751830464X.

[ZCCL14]
Yinghui Zhang, Xiaofeng
Chen, Jin Li, and Hui Li.
Generic construction for se-
cure and efficient handoff
authentication schemes in
EAP-based wireless net-
works. Computer Networks
(’Amsterdam, Netherlands:
1999), 75 (part A)(??):192–
211, December 24, 2014.
CODEN ???. ISSN 1389-
1286 (print), 1872-7069
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1389128614003648.
Zhou:2016:IBP


Zetter:2014:CZD


Zhao:2010:PSA


Zhou:2018:SAE


Zhou:2016:HFD


Gao:2012:DES

REFERENCES


Zimand:2010:SEC


Zhang:2011:FBP


Zeng:2014:NFC


Zhou:2015:PPS


Zhao:2012:IAS

REFERENCES

Zhang:2014:TAH

Zhang:2012:EEF

Zhang:2015:RBA

Zhang:2012:CCB

Zhu:2017:PSN

Zhang:2010:ESP
Jianhong Zhang, Chenglian Liu, and Yixian Yang. An efﬁcient secure proxy veriﬁably encrypted signature


Zhou:2017:IBB

ZU OC
48.5

www.sciencedirect.com/
science/article/pii/S0898122111011382


Zenger:2016:AKE


Zhang:2015:MAA


Zmudzinski:2012:WEU


Zhao:2012:SSM

Zheng:2018:GDP

Zhang:2012:EHO

Zuo:2018:CSA

Zhang:2014:NCM
REFERENCES

Zhu:2015:PPD


Zwattendorfer:2012:CBL


Zhang:2016:EEA


Zhou:2016:SRB


Zhou:2014:SAC


Zhang:2015:FAA

Zhiyong Zhang and Kanhliang Wang. A formal analytic approach to credible potential path and mining


Zhang:2013:LPP


Zhang:2016:PA


Zhang:2014:EFH


Zhang:2018:AKE


Zhang:2018:VPA


Zheng:2015:EPT


Zaidan:2017:NDW


Zhang:2017:NLR