Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N) [Bai10, YC11], (n, t, n) [LHYZ12], (t, n) [QD16, ZPYW12]. 0 [XHX+17]. 1 [XHX+17]. 1, 2, 3 [SMD11]. 11 [LJ17]. 13 [Blo15]. 2 [DBPS12, EAA+16, ESS12, JR13, MCDB12, PGLL10, WY12]. 22 [MN12]. 2k [Sun16]. 3 [AP10, CG12b, DWZ12, FWS13, GZH12, H11a, KWS+12, LJ17, LJ15, MKH+12, RS16, SS10b, SS12a, SGS14, WSSO12, tWmC12, Y11a, Y14, YPRI17].


Vua10, ABBD13, LYL15, SGJ+18, SSAF11, WLFX17. \textbf{AIPISteG} [AGLW16]. Air [AUMT16, VOGB18, ZXW+18]. aircraft [XWZW16]. \textbf{Airflow} [RSCX18]. \textbf{Airway} [RSCX18]. AK [XHC+12]. AK-PPM [XHC+12]. \textbf{AKA} [LLLS13]. AKF [KDH15]. al [LLW16, LLSW16, MWZ12, PLPW13, SBS+12, Mac14, Keb15]. al-Qaeda [Mac14, Keb15]. Alan [CS12, Don14, Hel17, LCKBJ12]. \textbf{Algebra} [Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14]. \textbf{Algebraic} [SK11, Tam15, Wat10, Bul10a, CFR11]. \textbf{Algorithm} [ABCL17, AN10b, AK14, BGGJ14, BKLS18, CR14, JCPB+12, DCM18, ESS12, GKS17, JH12, JSZ12, JHHN12, JL16, KB10, LL11, LTT14a, LLLL18, MRL+18, NdMMW16, NV10, RR11, RVRS12, WHZ12, WZ1C18, YPR11, Y116, ZSW+12, Ant14, BGJT13, BM16, CG12b, Ch10, EEA13, JK13, Jou13, KY10, KHMB13, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGLL10, PA10, PC14, SH11, SL10, SWW+17, JT12b, TTL10, WGG+12, XT10, YWL+17, ZL12, ZL12, ÁCZ16, ZOC10]. \textbf{Algorithmic} [GO17, KR18, AY12]. \textbf{Algorithms} [Gas13]. \textbf{Analysis} [AMKA17, AB10, BCG12a, B10, CN12, GP17, KR13, MR14a, MM17, TKM12, WH18, YS15, ZW15, ACHP14, Fri10a, Mac12, NAEL12, NC13, O10, O18, Xie12]. \textbf{Aliens} [ABJ13]. \textbf{Alignment} [Don14, IA15]. \textbf{Almost-Many} [CCL+19]. \textbf{All-Seeing} [Tox14]. \textbf{Allowing} [PRC12]. \textbf{Alloc} [Bro17]. \textbf{Almost} [BKST18, FFL12, GDCC16, Oba11]. \textbf{Almost-Tight} [GDCC16]. \textbf{Almost-Universal} [BKST18]. \textbf{Amoeba} [MPA+18]. among [BP11, MPJ+16, SS17]. \textbf{amount} [EEAZ13]. \textbf{Amplification} [ABF12, HMR14]. \textbf{Analog} [K102, S15]. \textbf{Analyses} [ZPXX17]. \textbf{Analysis} [GRL12]. \textbf{Analysis} [ABS+12, AR12, BRS17, BB16a, BC14, BS14, BKLS18, CFE16, CCG+16, CGL+12, DKMR15, FSW17, GZZ+13, GM16, GLG12, HC12, HHH+13, HZ1W17, HB17, IBM13a, IS12, JT12a, KE19, KOP12, Kre13, LPS12, LTKP16, L11, LL16, LLL12, MD12b, MAS16, MRTV12, MR10, NDC+13, NSA15, NAL17, PH12a, PS12, PS14, RZZ+15, Rao10, RBS+17, SK11, SY15a, SR12a, Shi11, SZ1L14, SCGW+14, VKC15, WDDW12, YZ1C12, ZH15, ZAG19, ZBF18, Aia15, ACF16, AN15, BNY14, CFH+13, CFL13, DM15V, DK17, DWH+13, DMT12, FTV+10, FAA+18, FH12+12, HM10, Lan11, MFB13, NLYZ12, PPA18, PL16, QGGL13, RITF+11, SK14, TQL+14, TL1M13, Tso13, VS11, Ven14, ZK17A]. \textbf{Analysis-Based} [RZZ+15]. \textbf{Analytic} [Kuz11, Sha10, ZW15]. \textbf{analytical} [CDPLCA16, TKMZ13]. \textbf{Analytics} [BL17]. \textbf{Analyzing} [HREJ14, YGD+17]. \textbf{anchors} [BCC+19]. \textbf{Ancient} [Fox13, Rao10]. and/or [YLA+13]. \textbf{Android} [Chi13b, EB1K13, FH12+12, SF10]. \textbf{Android-Powered} [SF10]. \textbf{Angle} [ZP16, KS18]. \textbf{Angle-Based} [ZP16]. \textbf{Angular} [pNyWy14]. \textbf{Anisotropic} [ZZCJ14]. \textbf{Annotated} [ATS15]. \textbf{Announcing} [SBK+17]. \textbf{Annual} [An10, EE10, EE11b, PJ12, Gil10, Rab10]. \textbf{Anomaly} [AKK17]. \textbf{Anonymity} [CD1S10, HEC+12, MV16b, MR10, SCGW+14, VFF17, WLY17, AIB+16, BAG12, GH16, HLR11, Par12b, PSJ+13, SGJ+18, WW14, YHL16, Z11]. \textbf{Anonymity-Based} [HEC+12]. \textbf{anonymity-preserving} [AIB+16]. \textbf{anonymized} [XTK10].
Asymptotically [LPS12]. Attack [Ano15d, BRS17, BMS12, Bro17, Che18, CJP12, DSB15, FXP17, zGXW12, GV14b, GDC16, HCEP12, HLAZ15, JHLH12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LJ19, LWKP12, LWPF12, MPA+18, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNST17, CJP15, DDFR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYHH14, LWKP14, MBB11, MN12, NZL+15, SB17, SXL16, WYL13]. attacker [PLGMCdF18]. Attackers [BL15]. Attacks [ARP12, Ano17c, BGK12, BFK16, BKK14, Che15, CMA14, DZS+18, DG1S12, DHLAW10, DHB16, EWS14, GPT14, HLLG18, Hay13, HRS16, JKR10, LLC11, LWZ12, LWCJ14, LCL17b, MD12b, PYM+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, WW14, WHN+12, XNG+14, YL17, YCM+13, ZLQ15, ZHS+19, AATT18, BBP13, BVBI12, BSR+14, CGH17, dCCSM+12, DCAT12, Dlj+12, DK17, Dra16, EA12, FTV+10, FIO15, GPP+16, GBNN11, KMI0a, KPS10, LWK11, NDNR13, OF11, PX13, SGP+17, TK19, TS16a, TY16b, TLL13, VS11, WWBC14, XWDN12].
attempt [Fel13]. attestation [FQZF18]. ATtiny [EGG+12]. Attribute [AAC+16, AHL+12, BFK+10, Boy13, CD16, CDL18, CHH+19, FHR14, GZZ+13, GSW+16, Gi12, GVW15, HSMY12, HBC+19, Her14, KGP12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, OT12, PPA18, PB12, RVH+16, Rao17, SSW12, TYM+17, WDC18, WH15, WHL16, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQQ15, ZZZ17, ZW15, CPPT18, FNL18, HZL18, HZWZ18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, LJWY18, LDZW19, Nam19, QRV+18, RD17, XWS17, YCT15, ZWM14, ZML17]. Attribute-Based [AAC+16, BFK+10, Boy13, CD16, CHH+19, FHR14, GZZ+13, GSW+16, GVW15, HSMY12, HBC+19, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TYM+17, WDC18, WH15, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQQ15, ZZZ17, AHT+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, LJWY18, LDZW19, Nam19, QRV+18, RD17, XWS17, YCT15, ZML17]. Attribution [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, QF19, TC10, gWPnY+14, XNG+14, XNRG15, XNP+18, ZS12, LSQ11a, SKEG14, yWPnL11, YQH12]. Audit [YNR12b]. Auditing [LMD16, TCN+17, YYS+16, YX+16]. August [AB10a, JY14, MV12, Rab10]. Austin [IEE13]. Authentic [HTL+15, SZMK13]. Authenticate [HM12]. Authenticated [Alo12, BCO13, BDMLN16, CCL16, CLY14, CCS14, CRE+12, DS11,
EAA12, ESS12, FVS17, FFL12, GTT11, GL12, GZ12, HC12, HL10a, HCL+14, HEC+12, KMY18, LHHRK10, LY16, LH11b, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHK14, MSU13, PTT16, Sar10b, Smi11b, SKV12, ST14, SM12, SD12, Shi11, SGC14, SSA13, SC12, SCMS18, SZDL14, SHS12, SAA12b, SRK+17, TGC16, TYK+12, TM12, Vet10, WgMdZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WT10b, Xio12, YTF17, ZBR11, ZHW+16, ZW17, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, Aia15, AL15, AHM+18, APK+18, Alp18, AIK18, ACF16, AZF+12, ATI+10, AN15, ACM12, BS13a, BDM18, BCM13, BGAD12, BLAN+16, BAL10, BMM12, BVhOS15, BT18, BTW15, BM11, CLM+12, CLM+18, CLP+13b, CTL12, CXX19, CSD18, CH10, CCWS11, CHS11, CLHJ13, C15a, Ch13a, CJP15, Cho14, CL11, DCA12, DCS12, DLK+16, DMV15, DNL13, DZS+12, DMT12, uHAN+18, EA12, ED19, EA11, FPBG14, FHH10a, FLL+14, FXP12, Far14].

Authentication [BS12, CHX13, GRL12, OKG+12, RPG12, WY12, ZCWS15, Cer18, LFGCGCRP14, PGLL10, ZLDD14].

Authentication [ASO14, AAZ+16, ACAT+15, AUMT16, ABB19, BL12, BCE+12, BCM12, BSS12, Bel18, BKST18, BCD+12, Bis17, Boy16, BKP12, BSV12, CGCGPDM12, CTC+15, CC14, CSH+18, CCW+10, CCC17, CJ13, CD12, CJP12, CLH13, DL15, DCM18, DBPS12, DKPW12, DP12, FH13, FR16, FMTR12, FD11, GHS14, Gl12, GI12, GM14, GU13, GMVV17, GCK12, HZC+12, Hv12, HLC11, Har13, Hay13, HBC13, HM10, HCP12SB12, HCTEP+12, HZ18, HX14, HZC10, HS11, Har13, Ham19, HDPC13, HZC+14, HZWW17, HL14, HCM11, HCL16, HCC10, HS11, IMB17, IC17, IG11, IB11, IOV+18, Jac16, JNUH17, KJAU19, Jia16, JKL+16, JMW+16, JAX+11, JXZ15, KPM16, Kem11, KG14, KSB+17, KVeE18, Kim11, Kim16, KIH19, KP18, KBP17, KLW+16, KWD+17, LLSL13, LZC+16, LC17, LH11a, LT13, LH10c, LNM+11, LMJC11, LW12, LNK13, LK14, LIK+17, LMC+17, LNK+18a, LW+18, LNK+18b, LHM14, LH13, Lit14, LWLW11, LTC+15a, LL15, LR12, LTL10, MM12, MCN+18, MvO11, MPM19, MA17, MMS17c, MK12a, NR17, NACL12, NCCG13, NLZH12, NB13, OF11, OCD11, OYHS14, PHY+18, PYT10, Part12b, PLGMC5F18, PZBF18, PA10, PKA15, PRN+19, QMC17, QMM17, SPLH14, SB17, SGGCR+16, Sar10a, SGJ+18, hSZZ15].

Authentication [SCH10, SA15, SYW17, SSS11, SKEG14, SHB19, Tan12b, Tan15b, TOD18, TG17,
authentication-chaining [EA11].
authenticators [SYY+17]. authenticity [ADF12].
Authority [LNXY15, XZLW15, ZQQ15, JB11, ZZ12].
Authorization [CS14, LMGC17, MPM+17, YKK18, AL15, DFJ+17, JAE10, JAS+11].
Authorized [HTC+15, LLSW16].
Authorship [BTW15, BAG12, LCM+17].
Autoblocking [LLLH18, YH16].
Automata [CCD15, Gas13, dRSdVC12, HBBRNM+16, SS11, WOLS12].
automata-based [SS11]. Automated [CCK12, CCCK16, DR516, GLSN12, LGM+16, Ste15a, Tom16, YSS14, BJ+14, KKK+16]. Automatic [MMP19, WW12].
Automation [BGK12, DZS+18, IEE11a, KPP16].
Automotive [HK18, LMS16, MPM+17].
Autonomic [SEK+19]. Autonomous [MPA+18, BT18]. Auxiliary [DMS+16, DL12, GGHW17, XXZ12, YCZ12].
Avoidance [RVH+16]. avoiding [BHCdFR12]. AVR [LPO+17]. award [Ano16g, Orm16]. Aware [BCF16, LMHH14, LMS16, QLL17, YTH17, GHD19, MGP10, TODQ18, Wan13, ZF+18].
Awareness [MSas12, Li10, MSas13]. axiomatic [AT10]. Azure [Sti19].

B [Tan12a]. B-Spline [Tan12a]. Back [KRM+10, SKS+18, YZLC12, Ran10].
Bandwidth-Efficient [LLZ+12]. Banking [KSD+17, RBS+17, KVvE18]. banned [Eve16]. BANs [BL+19]. Baptiste [Dew11]. Barbara [Rab10]. Barcodes [WY12]. Barrier [JR14, KS11]. barriers [LKKL13]. base [MS12a, XSWC10]. Based [ADM12, AGW15, ASM12, AAC+16, ABCL17, Ano11b, AS15, AYS15, BWLA16, BL12, BBB+16a, BSSV12, BHG12, BKPW12, BRT12, BHH+15, BS13b, BFK+10, Bon12, BS15, BF19, Boy13, BKP12, BDH11, BCF+14, CMLS15, CLL16, CGMO14, CCM17, CSH+18, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST+17, CLND19, CGL+12, CDD13, CGY+13, CD12, Ch12, CK18, CD16, CHH+19, DSSM14, DS19, DA12, DLZ+16b, EM12, EKB+16, FM15, FHH10b, FHR14, FZT14, FGM10, FVS17, FSX12b, FSX12c, FSX12a, GWWC15, GZZ+13, GSW+16, GV14b, GI12, GY12, GDCC16, GV15, GJJ15, GJZ17, HZ+12, HSMY12, HSM14, HBC+19, HL10a, HXZ15, HCPLSB12, HKL+12, HG12, HMR12, HSA14, HP0+15, HKR+18, HGT15, HCL+14, HLN+10, Hul13, HRS16, HBG+17, HEC+12, HM19, HP12, JZT+16, JHJN12, JEA+15, JKHcY12, KS18, KZG10, KK12, KKA15, Kha10, KLY+12].
Based [KSSY12, KP KS12, KRB12, KAK18, KS15, LMGC17, LMG+18, LTPK16, LSL12a, LSL12b, LW11b, LW11c, LW12, LHF12, LJLC12, LYZ+13, LHL+14, LTH+15, LLC+15, LTZ16, LLZ+17, LLLH18, LPL15, LSLW15, LAL+15, LH11b, Lin15, LP12, LNZ+13, LCCJ13, LWCJ14, LNY15, LHL15, LW16, LPO+17, LGPRH14, LDB+15, LD13, LSC12, LBR12, LLH18,
MWZ12, MLO17, MEFO12, MCDB12, MVV12, MD12b, MBC15, MKN13, MZ17b, MCS+15, MMS17b, MKF+16, MCF17, Men13a, MST18, Mor12, MKR17, MKAA17, Muf16, NC12, NXH+17, NXB13, NLLJ12, NLY15, pNyWyY+14, OTD10, PB12, PTT16, PYS15+15, PSH15, PSS2b, PYS18, PG12, PAS13b, PRNC17, QC+18, QF19, RVH+16, RSR+19, RZZ+15, RS16, Ra17, RR11, RZ+16, RYRS12, RW12, SSW12, Sar18a, SS13, Sen17, SJ12, SPG+12, SPG+19, SP15b, SSA13, SRA17, SH15, SGH15, TB18, TKR14, TWZ11, TW12].

Based [TWZ+12, TYM+17, TSH17, TT12, TTH15, TC10, VDB+16, VGA15, Vle12, WY10, Wan10, WSSO12, WgMW12, WY+13, Wan14, WZCC18, wWxyZ+18, WDC18, WLH15, WCL+18, WT10b, WMS+12, XNG+14, XNRG15, XXZ12, XM1C13, XQL11, Xio12, XGLM14, XWLJ16, XJW+16, XR+17, XHX+17, YE12, YZL12, YZX+12, YGFL15, YTS12, Ye10, Ye14, YH16, YTH17, YO15, Y+17, YKNS12, YHK+10, YMWS11, YKC+11, YFK+12, YCY12, ZSP+19, ZPM+15, ZJ11, ZZ+11, ZDL12, ZLH+12, ZQF15, ZMW16, ZXYL16, ZZZ17, ZPW16, ZHW15, ZVG16, ZPX17, ZY18, ZY+19, ZHL15, AMN18, AGL16, AaBT16, AY14a, AHS14, AAT16, AA14, ASO14, A+18, AKG13, ASVE13, Ara13, ATT+10, AHL+12, BS15, BDM18, BBBF13, BGAD12, BAAS13, BOB13, BWR12, BW13, BWA13, BM12, BC18, BB16b, BK12b, CPPT18, CML+18, CFL13, CFY+10, CCLL11, CT12, CLSW12, CG12b, CSZ+11, CHX13, CSS+13]. Based [CW14a, CT13, CP12, CJ15, CCG10, CT13, Ch14, Con12, dCCSM+12, Cra11, CDL18, DSCS12, DZ14, DLN13, Dra16, uHAN+18, EZ15, FH13, Far14, FA14a, FA14b, FIO15, Fay16, FHZW18, FNW1L8, Gal13, GJ13, GMG1C15, GMRT+15, GKCK11, GJMP15, GCSADD11, GMS11, GLL+18, HSH11, HT11, Ham19, HG5Y11, HSM13, HC+14, HZL18, HF14a, HWDL16, HZWW17, HZWW18, HBBRM+16, HLR11, Her14, HBW12, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HYF18, HPY10, HKH13, HCC10, Hwa11, IMB17, IM14, ISC+16, IB11, IA15, IOV+18, Jac16, JNHU17, JKA19, JKI3, JLT+12, JZS+10, JMW+16, JSMG18, KKP16, KK13, KM10a, KHM13, KKG14, Kim11, KG010, KL11, KSH18, LXYL12, LZZ+16, Lau12, LLC10, LK14, LH10c, LZJX10, LNM+11, LMJC11, LK12, LXMW12, LKAT12, LLS12, LNK13, LXJ14, LCL+15, LZY+16, LFZ+17, LNK+18a, LWK+18, LCT+14, LFWS15, LLM+19]. Base [LPdS10, Lin14a, LLY+12a, LW10, LSQ11a, LSQ11b, LW11, LW13b, LZZ+14, LPZ15, LCT+15a, LYL15, LY15, LJW+17, LJWY18, LDZW19, LWW+10, LL16a, LW13c, LWY12, LY14, MCN+15, MJS12, MJS13, MLM16, MMZ12, MM13, Mes15, MB11, MO14, MHT+13, MG15, MS17, Nam19, NR11, NCL13, NZL+15, PPA18, PYH+18, PLFW13, PTK14, PW10, PGL10, PPB16, PLGCd18, PS14, PL16, PKA15, PC14, PPR+12, QZDJ16, QRW+18, QYW1X, QMW17, RD17, RG10, RS15, SPLHC14, SGGCR+16, SI12, SYL13, SE14, SE16, SH11, SM11, SNM14, SR10, hSZZ15, SCKH10, SA16b, SSA11, SWW+16, SSS11, SKEG14, Sun16, SGM16, SHBC19, SS11, TPL16, TQL+14, Tia15, TH16, TTL10, TPKT12, TKH14, VS11, NN17, WYYZ11, WYYY11, WLD11, WLFX17, WMX+17, Wan18, WGZ+12, WHLH16, WS14, WS12, WTT12, WOLS12, WC18, XHH12, XWW16, WX12, XCL13]. Based [XWS17, XHCH14, XWW+18, XMHD13, XHM14, YWL+17, yYqWqZC13, Yan14, YTM+14, YCC16, YXA+18, YCT15, YLS12, YMS10, YKC+12, YLZ+16, YX+16, YL11, ZZKA17, ZLW+12, ZCCL14, ZT14, ZT16, ZML17, ZZ12, ZHZ+17, ZL12, ZVH14, ZDW+16, ZLY+19, LZJX10,
Chain [EAA+16, FVK17, KPW13, QZL+16a, QZL+16b, YFT17, YSF+18, YFT18, CR12, CL16, SJWH+17].
Chaining [EA11].
Chains [JSK+17, HLYS14, JCHS16].
Challenge [AD12, GHS14, YDH+15, ZCC15].

Challenges
[CN12, FS15, FrA15, LLGJ16, MRS+17, PCY+17, SBV14, ALL+18, KJN+16, WS14].

Chances [ALL+18].
Change [KMJ18, ZWT13].
Changeable [FGM10, ZCL+12]. changed [Mac12].

Channel
[AN17, ASN11, CDK+10, CBL13, DZS+18, EWS14, GWM6, GPT14, HLH19, KOP12, LGR14, NDC+13, PRC12, SG15, TT12, YL17, ZBPF18, ADG16, BVIB12, CPT18, DMWS12, DJL+12, JLT+12, MFH13].

Channels [ASN12, BGN17, DMKR15, EPAG16, KW14, SS19, Vua10, AGH+17, CL16, DMV15, DKL+16, LWGZ10, NR11, SRB+12, ZPZ+16].

Chaos [AIA+18, LW13c, RR11, RVRSCL12, CCL11, LW13b, JT12b, ZIW+12, SGFCRM+18].

chaos-and-Hamming [CCL11].

Chaos-Based [RR11, RVRSCL12, AIA+18, LW13c, ZIW+12].

Chaotic
[BCGH11, IAD10, LFX+18, Ye10, GCH15, ISC+16, KLW+16, LWK+18, LW10, NES+14, WGW+12, ZT14].

Chapman [Ful10].

Character [SS26].

Characteristic
[BDPS12, BR12, CWWL12, CHH+12, DJG+15, EGG+12, EKP+13, GT12, GSN12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCLW17, LGLL12, LJ16, MD12b, NN12, Pud12, Sas12, SEKH12, Vua10, WH18, WW12, XDC12, ZH15, ZSW+12, Zha12, Zha12, Bay10, Bia12, Bor10, Die12, KM10a, LWK11, MRT10, MRT10, MH15, MH15, QGGL13, SKK10, TQL+14, WB12].

Ciphers
[ABS+12, BMS12, BSS+13, BKLS12, Bru12, CWP12, DGI12, DJG+15, EGG+12, EKP+13, GT12, GSN12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCLW17, LGLL12, LJ16, MD12b, NN12, Pud12, Sas12, SEKH12, Vua10, WH18, WW12, XDC12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KM10a, LWK11, MRT10, MH15, MH15, QGGL13, SKK10, TQL+14, WB12].

Ciphertext
[BDPS12, CWWL12, CHH+19, zGXW12, HLW12, JMG+16, JSMG18, KA17, LNW12, ML12, MH14, PNDH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWH12, XLC13, XWL16, ZHW15, CPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, KTT12, LCT+14, LFWS15, LZC14, LDZW19, QRW+18, RD17, SG16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertext-only [KA17].
Ciphertext-Policy
[CHH+19, Rao17, XMLC13, XWLJ16, ZHW15, JSMG18, LFWS15, LDZW19, QRW+18, XWS17, LAL+15, LHL15].

Ciphertexts [LLPY19, Sta12, WQZ+16, AHL+12, LCT+14, NMP+13, WXLY16].

Circle [SC10].

Circuits [Kai12, MTY11, XWS17, XWLJ16, Lan12, MS13a].

Circuit-Size [MTY11].

Classifiers [AIK14, AS17, BR14, GHG+16a, GH11a, GVV15, MB18, SS10b, SS12a].

Class [BG12].

Citizens [Ano16d].

City [Ano17d, GAI+18, LNK+18a].

Claims [SKGY14].

Class [BCG12a, SY15a, XYXYX11, BJ16, Goo12, KK10].

Classes [ACZ16].

Classical [DSL18, JEA+15, MS13, SU12, CR12, RK11].

Classification [CHH+19, HPC10, HS18, KAHK17, SG+12, ZLW+17, LHL+18].

Classifiers [KV16, LCM+17].

classroom [Pow14].

Claudius [Hol12].

CLEFIA [LWZ12, TSL11, TS16a, WB12].

CLEFIA-128 [TSL11].

CLEFIA-type [WB12].

Client [ASM12, CTC+15, FD11, RAZS15, Vel12, FA14a, FA14b, hSZZ15, WT10a].

Client-Based [ASM12].

Client-Centric [Vel12].

client-server [FA14b, hSZZ15].

Clients [Chi16, LLPY19, LH13].

cloaking [NZL+15].

Close [Wal18].

Cloud [AJ16, BCQ+13, BCK17, CCL+14, CWL16, CDFZ16, CCT+14, CLW16, DK16a, DXA14, FCM14, FPY15, Her19, JLS12, KMSM15, KS18, KKA15, Kup15, LA15, LLP19, LYZ+13, LGR14, LLC+15, LNYX15, MLO17, PSM17, Pet12, PBC+17, RSG15, SG18, SGJ+18, SKH17, SRA17, TV15, Vle12, WLFX17, WW17, XNKG15, XWS16, XMLC13, XWLJ16, XWX+16, YDY+16, YHL16, YXA+16, YMC+17, ZZQ+19, ZDL12, ZL15, ZGV16, ZLW+17, ZZZ+18, Aab16, AKKY17, AZP14, ASO14, AAZ+16, AKK+17, ADH17, ALL+18, BG14, BK12b, CFVP16, CSV18, CLH+16, CZ15b, CD18, FH13, FNWL18, GLB+18, GZS+18, HSM13, HZW18, HYS18, IMB17, Joo13, KKA14, KKM+13, KKM+14, KSB+17, LKX+14, LZY+16, LAL+15, LW13a, LYL15, LHL15, LCY+16, LZZC17, MLM16, NR17, Nam19, NB13, PPA18, PP11, Rao17, SYE+17, SAR18b, SL10, SKB+17, SWW+16, SWW+17, TLM13, WL12, WSC14, WMX+17, WLS14, WC18, WL19, XXY15].

Cloud [XYW+18, YYS+16, YZCT17, YHMH18, YQOL17, YWT+12, ZYC+17, ZVH14, ZDW+16, ZWS+18, ZFH+19, ZLY+19, ZHT16].

Cloud-aided [SGJ+18, WLFX17].

Cloud-Based
[KS18, SRAA17, ASO14, BK12b, WCCH18].

Cloud-Manager-Based [KKA15].

Cloud-of-Clouds [BCQ+13].

Cloudier [CF16].

Clouds [BCQ+13, HLC+18, RSN14, HFT16, IC17, JKL+16, LFWS15, LL16a, W17, YNX+16].

Clustered [DS11, KS18].

Clustering [KRD13, VSV15].

CMAC [SK10].

Co [MBR15, MRL+18].

Co-Design [MRL+18].

Co-Processor [MBR15].

coal [KO16].

cocktail [O10].

code [AD12, Bud16, CCL+13, Cop10a, Fox13, HG12, KSSY12, Mun17, PYM+13, SS13, Sen17, St15, War11, ABBD13, Ant14, Bha16, Bri11, CCL11, GJJ+12, MCP15, McG11, McK12, Moe14, OF11, PA10, Wes15].

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

code-breaking [Ant14, Bri11].

Code-cracking [War11].

codebreaker [Car11].

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

Codebreaking [Bai12, RS18, Cop10b, McK10, McK11].

Coded [She14].

Codes [An19, BBC+13, Bay10, BKST18, DBPS12, DPW18, FMNV14, GMNS15, Gr15, HC17, KW14, MBR15, OTD10].
SEY14, ST14, TLW12, WGF16, WSS12, Xie12, YTP11, Yek10, ATI+10, Bull10a, CZ15a, Chi13a, Fag17, Hea15, LTT10, MG15, ÖS11, Tan15b, YSJL14, Ayu12, Low12.

Codevelopment [DF16]. Coding [Che11, CWL16, CJ13, CG14a, DG17, Hes12, LCLL15, Per13, AZF+12, Bul10b, CJXX19, DTZZ12, JZS+10, KM11, LLP+18, NDNR13, OF11, Tan15b, YTM+14, Kim15].


collaborative [LT14b, HB13]. collect [Sch15c]. Collision [BK12a, ZL12, AKY13, SKP15, SBK+17]. Collision-based [ZL12].

Collision-Resistant [BK12a]. Collusion [MMSD13, RH+16, FLZ+12, GMRT+15]. collusion-resistant [GMRT+15].


Combined [PP10b]. Combining [Chi13a, CDF+10]. Coming [SOC15].

Comment [LCLL15]. Comments [IC17, Kim15, hSSZ15, Tan11, TCL15, XWS17].


communication-efficient [Tso13, Znu13]. Communication-resource-aware [Wan13]. Communications [JTZ+16, KSD+17, KYEV+18, OOS12, RSD19, SMS14, AMN18, Edw17, FHH10a, Han12, LFCCCGRP14, LLZ+16, MHY+18, RS15, WDZL13].


comparisons [Mid10]. compartmented [EZ15]. Compensated [GKS17].


Component [BKLS18, MV16a]. components [RITF+11]. Composable [DN12, KMO14]. Composing [TW14].

Composite [Dun12a, BBDL+17]. Compositional [LJS+14, NRZQ15, Ana14, AGH+17]. compound [BJ16, KPS10, jT12b].

Comprehensive
[GSFT16, YFT17, ZBP18, Bul10a, KAS15].
compress [LC13]. Compressed
[DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16]. Compressed-Domain
[WLZL12]. Compressibility
[HN10]. Compression
[CNT12, DA12, LD13, MAL10, PMZ13, PP10b, TCN17, WHZ12, ZSP19, Ara13, CMMS17, DTZZ12, KL14, Li10, LPZJ15, PP11, QZ14, RSMA19, SI12]. compression-based [SI12].
Compress/Decompress [PP10b].
Compressive [CCZC13]. Compromise [YNR12b, GBNM11, PX13].
[ARH14, Ash14, Bee17, BDOZ11, Fri10b, GST12, GVW12, GHKL11, LPZJ15, Mal13, NSMS14, PST13, SDCV15, SI12, Wat10, ABDP15, AB10b, BHH19, LDAM12, PHGR16, SI12, vDKS11].
Computational
[BCO13, GKS17, RD17, TBCB15, HRS13, SDM14]. Computations
[ARM15, CK18, KHP16, Nac16, ADMM16, BK12b, LR15, SSF11, TLMM13].
Compute [Vai12].
Computers
[Mos18, Cop10b, LCKBJ12, Mac12, MV11, PHWM10]. Computing
[ACM10, ACM11, AIA16, Ano17e, BCG12b, Cer14, CGB10, DXA14, EAA12, FES10, Gen10, KMS15, KP17, LCK11, LT14a, LYZ13, LLGJ16, LNYX15, MLO17, OS16, PAF18, Pet12, RS18, sjw11, SLM10, Vai11, Vle12, XMLC13, XWLJ16, YE12, YHL16, ZLDC15, AaBT16, AAZ16, And13, CZI15, CSTR16, DKL16, DWZ12, HSM13, HYS18, Jee13, JSMG18, KKA14, KKM13, KKM14, KSB17, KH18, LXX14, LYL15, LHL15, MS12a, NR17, Nam19, NCCG13, PPA18, PP11, PKA15, QZDJ16, QRW18, Rao17, Tan12b, WSC14, Wan18, WDKV19, WLS14, WL19, XX15, XXY18, YYH18, YW10a, YQOL17, YY11, ZWS18, ZLY19, ZSW18b, YAX18]. concealing [EEAZ13]. Concept
[TMC15]. Conceptual
[PMZ12, SP13, TSH14]. Concrete
[BS14]. Concurrent
[CLP13a, FCM14, GJO13, MKRM10, OOR14, AKG13, SRB12, XJW13]. condition
[TD14]. Conditional
[HBCC13, KP13, LG15, LSL15, MLO17, XJW16, MSG11, MSG12, HWDL16, HYF18, IOV18, LCT14, PZBF18, SKB17, Tan12b]. Conditionally
[ZJ14]. Conditions
[Ano17d]. Conference
[BC11, CGB10, Ch11, Cra12, Dan12, Dun12b, FB12, GLIC10, IE11a, JY14, LCK11, LSW11, LSW11, P12, SNJ11, Sah13, Yan10, AB10a, Abe10, BYL10, BL10, GII10, GGO10, HW10, Kia11, LH10a, PIE10, Rab10, vDKS11]. Confidential
[HS11, AZPC14]. Confidentiality
[BFK10, HLLC11, OFMR16, SZQ17, WDDW12, B12, CHX13, ZHT16]. Confidentiality-Preserving
[OFMR16, SZQ17]. Configurable
[CVG13]. Configuration
[Bis17, SHBC19]. Configurations
[SS10b]. Congruence
[V11]. conjecture
[GV14a]. conjunction
[Kre13]. Conjunctive
[CWWL12, BL11, WL19, ZZ11]. conjunctive-subset
[ZZ11]. Connection
[CW12b, HLYS14, WGD18, MZ17a]. Connectivity
[GT11]. conscious
[RC15]. Consecutive
[Tan12a]. Consensus
[ABCL17, JSK17, LLKA19]. Consequences
[E17, SS19].
Consideration [CJP12, CJP15, KM10b].

Considerations [BF19, KD12b].

considering [MLMSMG12]. Consistency [BCK17, SES⁺16]. Consolidated [KKA14].

Constant [App14, AEHS15, CWWL12, KOTY17, KHPP16, KMO14, LP11, LSQX19, Pan14, ZMW16, AHL⁺12, DWZ12, LCT⁺14, SGM16]. Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHL⁺12, LCT⁺14, SGM16].

constants [DWZ12]. Consistent [BCK17, SES⁺16]. Consolidated [KKA14]. Constant

Consistency [BCK17, SES⁺16]. Consolidated [KKA14].

Constant [App14, AEHS15, CWWL12, KOTY17, KHPP16, KMO14, LP11, LSQX19, Pan14, ZMW16, AHL⁺12, DWZ12, LCT⁺14, SGM16]. Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHL⁺12, LCT⁺14, SGM16].

constants [DWZ12]. Consistent [BCK17, SES⁺16]. Consolidated [KKA14]. Constant

Consistency [BCK17, SES⁺16]. Consolidated [KKA14].

Constant [App14, AEHS15, CWWL12, KOTY17, KHPP16, KMO14, LP11, LSQX19, Pan14, ZMW16, AHL⁺12, DWZ12, LCT⁺14, SGM16]. Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHL⁺12, LCT⁺14, SGM16].

constants [DWZ12]. Consistent [BCK17, SES⁺16]. Consolidated [KKA14]. Constant

Consistency [BCK17, SES⁺16]. Consolidated [KKA14].

Constant [App14, AEHS15, CWWL12, KOTY17, KHPP16, KMO14, LP11, LSQX19, Pan14, ZMW16, AHL⁺12, DWZ12, LCT⁺14, SGM16]. Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHL⁺12, LCT⁺14, SGM16].

constants [DWZ12]. Consistent [BCK17, SES⁺16]. Consolidated [KKA14]. Constant

Consistency [BCK17, SES⁺16]. Consolidated [KKA14].

Constant [App14, AEHS15, CWWL12, KOTY17, KHPP16, KMO14, LP11, LSQX19, Pan14, ZMW16, AHL⁺12, DWZ12, LCT⁺14, SGM16]. Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHL⁺12, LCT⁺14, SGM16].

constants [DWZ12]. Consistent [BCK17, SES⁺16]. Consolidated [KKA14]. Constant

Consistency [BCK17, SES⁺16]. Consolidated [KKA14].
CZ14, CJP15, LEW19, Sar10a, YL11].
Cost-Eective [HLT+15, WMX+17].
Costas [TRD11]. Costs [KHP16].
couldn’t [Bha16]. Countdown [Zet14].
Counter [ARP12, KMJ18, Fay16].

Counterexample [KPW13]. Counterfeit [YFT17].
Counterfeiting [Ano16e].
counterfeits [GSN+16]. Countermeasure [BBB+16a, MD12b].
Countermeasures [BGN17, DZS+18, EWS14, PZPS15, DK17, FAA+18]. counting [Bha16].

Cover [UUN13]. Covert [EPAG16, JTZ+16, NSA15, LTY+10, SRB+12].
CovertBand [NTKG17].
Cozzens [Led16, Sch15a].
CP [TY16a, YMC+17].
CP-ABE [YMC+17].
CPM [PYM+13].
CPS [FQZF18].
CPU [ZBPF18].

Create [DFKC17]. creating [OO10].
Creativity [WP15].

Credential [JMW+16, KKM+13, XMHD13].
Credentials [CG12a, SSW12].

Credit [Mar10b].

Crisis [OdH12]. Criteria [PYS18, ZZKA17].

Criteria-Based [PYS18].

Crittogra a [Sac14].

Cryptanalyzing [LLL17a, LLLH18, ZLW+12]. CryptDB [PRZB12]. Cryptic [Mar10a].

Cryptographer [Dun12b, Kla11, Pie10].

Cryptographers [Ano16d, BPS16, Goo12].

Cryptographic [Abe12, AMA17, AD12, ARH+18, AMVZ12, App15, BCGK12, BGB12, Bar15, BCM+15, BIKK14, BLS12, BDP11, BFCZ12, BDGH15, Bla12, BKL+13, BSJ15, BNA15, CCK12, CCC16, CFE16, jCBP+12, CBL13, Cor14b, Des10a, DQFL12, DR11, Ess17, FKS+13, FY11, FLW12, Gir15, GM11, GLR10, GG11, Har16, HN10, HHH+13, HST14, HSA14, IBM13b, JR13, JHW+19, KOP12, LVV11, LLK18, Loe15, MV12, MP12, MKAA17, Muf16, MK12b, NIS13, NA10b, PTT16, PFS12, PS14, PJ12, RMP10, RSBN12, Rja12, RBHP15, SK11, SEY14, SKFR15, Sch12c, Sev16, SGG11, SP15b, SDM+12, SR14, SOF12, TW12, Tom16, YZLC12, YNR12a, YNR12b, YS15, ABDP15, AIY14a, ABB+14, ABF+14, ABC+12, BFG+14, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGJN14, EBFK13, ESR14, GGH+16b, Gil10].

Cryptographic [GLR13, KSU13, KAS15, KKK+16, LGKY10, LLL+17b, MS13c, Mat19, MM12, MM13, Mes15, MN10, NDN13, O018, Pal15, PLPW13, PsDo+13, QZJD16, SD10, WT13, WMX+17, YSM14, ZVH14, Zim10, Sha10].
Cryptographic-Key [SK11].
Cryptographical [KU12].
Cryptographically
[ADD10, BCGH11, BJL12, BKLS18, MC11, NDG+17, PLStvLE10, SVCV15, GCH15, HJM+11, SA14]. Cryptography
[ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, Ano19a, App14, AAB17, ACM+17, ARM15, Bar12, BGK12, BRT12, BCGN16, Bon12, BF19, BKKV10, BJ10, Buc10, BL17, BLM18, BCF+14, CTR14, CT18, CJSF14, CMO14, Che17, CST+17, CDFZ16, CS12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FIS12, FHD19, Fe10, FSK10, Fil18, FM12, Fre10, GO17, GFBF12, G’13, GPT12, GLW12, Ham17, Hes12, HG12, HKR+18, JS18, JT12a, KM10c, KPP10, KAK18, LSL12a, Lin17, LWL10b, LGWY12, LMHH14, LGH’17, LWHS17, LPO+17, MO12, MSL10, Nan12, Men13a, MR14c, Mic10b, MST18, MV12, MMB17, NNA10, NS12, Orm16, PP10a, PHP12, PG12, RW12, Rog16, SY14, SG15, SOG15, Schl16, Sch18, Sen10, SSI3]. Cryptography
[Sen17, SK12b, SA16a, Sim15a, SGS14, Sm16, St11a, St15a, VS16, WWL+14, WY12, Wst16, Ym12, Yan11, YTS12, YL17, ZZGJ14, ZAC17, vTJ11, AM18, AMORH13, AEH17, AAT16, AA14, ABBD13, Ano11a, ABW10, ACK’10, BOB13, BB14, Ber14, BL14, B17, BAB+13, B12, BSR’14, BS12, BB16b, CCR11, Cha13b, CQX18, Cho14, CST16, Co12, CSSLY14, DDD14, Dav11, DD13, Dur15, Far14, GCVR17, Har15, HH15, HZW17, Hof16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Li12, LY14, MCN+18, MS13b, MD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, Ry10, Sac14, Sah13, SK14, SSAF11, Sta11b, St11, So14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA+18, YDH+15].
cryptography [YR11, ZXW+18, vDKS11, Che11, LZXJ10, Nan12, Con12, Ful10, Gas13, Low12, Mei10, Mur10, Ter11].
cryptography-based [BOB13].
Cryptography-Related [Cil11]. Cryptol [Lau12]. Cryptology
[BC11, Bro11, Dun12b, LW11a, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPG14, Gil10, GG10, K11a, LH10a, MZ17a, Pal16, Pie10, Rab10, HWG10, LT11, Kob10].
Cryptomania [Gen13]. Cryptoprocessor
[GV14b, SWM+10]. Cryptosystem
[CCT+14, LH10b, SWM+10, BS15, Chi13a, Gal13, GyV14a, GLB+18, IB11, MM13, MG15, NZM10, Svt10, yYqkC13, YY11].
Cryptosystems
[ADI11, CLND19, OTD10, PSM17, ZSP+19, BNST17, FWS13, SA16b].
CS [LJ19]. Csec [AD12]. CT
[Jun12b, K11, Pie10]. CT-RSA
[Jun12b, K11, Pie10]. Cube [MS12b].
Cubic [RW12, VM14]. Cuckoo [BHK13].
CUDA [DLV16], cultural [Mid10].
Culture [Bla12, SR14]. Currencies
[TS16b]. Current [BP17, GCK12, FPBG14].
Curse [GG11, HB14]. curvature [GJ13].
curvature-feature [GJ13]. Curve
[ADI11, ARM15, BJ10, FHLD19, GPT12, LGH’17, LWHS17, PPH12, SG15, AM18, BL14, BL17, BB16b, Cho14, Far14, FWS13, IB11, K10, Kre13, MCN+18, MS13b, NZM10, SK15, WH17, JL16].
Curve25519 [SG15]. Curve4117 [BLC14].
Curves
[AK14, BWR12, DW12, LL11, LT14a, MST18, YTS12, BL17, BP18].
Customization [OdH12]. Cyber
[LJS+14, GH19, HZW18, KSA16, QMC17].
Cyber-Espionage
[LJS+14].
cyber-physical
[GHD19, HZW18, QMC17]. Cybernetica
[An17c]. Cybersecurity [DF16, Hel17, Lan17, LRW14, Mos18, Sch19, SPG+19].
Cycle
[He12, KU12, MKN13].
Cycle-Based [MKN13]. Cycles
Cyclic [Che18, OTD10].

D [AP10, CG12b, DBPS12, DWWZ12, EAA+16, GZHD12, KWS+12, LJ17, LJ15, MCDB12, MKH+12, PGLL10, RS16, SGS14, SRK+17, WSSO12, WY12, tWmC12, YI14, YPR17]. D-Based [WSSO12]. D-like [LJ15]. D-PUF [SRK+17]. Dana [Ano10].


DASH [KCC17]. Data [Ano13c, ADF12, Bar12, BJL16, BCD+12, BJL12, BW12, BKLS18, CWL+14, CMLS15, CCW+10, CSV15, CCT+14, CLW16, CHI+19, DDS12, Dan12, DR12, DK16a, DMS+16, DA12, DCA18, DLZ+16b, EKB+16, FYMY15, FPY15, FRS+16, GTT11, HSM14, HLC+18, HLZ+15, HK14, IBM13a, KRDH13, KGV16, LLPY19, LLZ+17, LWCJ14, LLZ+12, LZC+12b, MLO17, Mal13, MMS17b, MM14b, NNAM10, NR12, PD14, PSM17, PBC+17, PH12b, PRN17, QZL+16a, QZZ18, RCP+18, Real6, RSN14, SGG18, SAKM16, Sar10b, SMSK18, SP15b, SKH17, Sia12, SLM10, TCI+17, Tan15a, Vai12, VS15, WZC18, XNK15, XWSW16, YDY+16, YMC+17, ZXY16, ZPXX17, ZTL15, ZLZ+17, AP10, ASO14, Ana14, Ana11a, Ara13, ADH17, ALL+18, BLL+19, BHI19, BTPL15, BC18, BKV13, CDGC12, CLH+16, CDF+10, CDL18, DFJ+10, DTZ12, DRD11, ED17, F818, GHD19, Gen10, GLB+18, GZS+18, HSM13, HWK+15, HMC12]. data [HH16, HYS18, HYF18, JW14, JHCC14, Kim16, KI18, KWH16, LSBN14, LT14b, LXX+14, LZ+16, LLL+17b, LHL+18, LFWS15, LAL+15, LCW+16, LZZ17, LLL+18, LL6a, LHA+16, MHKS14, Nam19, OI18, OSSK16, QCX18, SCH15c, SY+17, SAR18b, SWW+17, Tan17b, TMK11, TKMZ13, WLH13, WLS14, WZLW13, WS14, WL19, XXX15, XWZ+18, XY+18, YSS+16, YQOL17, YXA+16, YNX+16, ZKGA17, ZMM+10, ZY+13, ZHTL16, ZZZ+18, AEH17, HLYS14, SCH15c]. Data-Centric [DLZ+16b]. Data-Classifiers [KGV16].

Data-Compression [DA12]. Data-Minimizing [BCD+12]. Data-Oriented [NNAM10]. Database [BTHJ12, SBV14, WCL+18, BL11, JHCC14, LW13a, PRZB12, Suc12, YXD18].

Databases [FCM14, HPC10, JHEY12, Kaw15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12].


Decentralizing [LW11b]. Deciding [CLC10, Sch12c]. Decipher [Cor14b].


Decodable [Yek10]. Decoding [DBPS12, GMNS15, Bax14, Bul10a].

Dedicated [Lin17, Nac12]. Deductive [ABF+14]. Deduplication [QLL17, SKH17, YDY+16, ZHZ+19, KH18, SAR18b, ZFH+18]. Deep [FGR+17].

defeated [Kap13]. defects [FES10].
defensive [P].
defnition [LWL10a, WSC14, YKC+12].
definitions [GLW12, Mau12, CGKO11, KM14, KGO10, XWXC14]. Degeneracy [WH18]. degradation [MMS+17a]. Degree [KA18]. degrees [MZ17a].
deray [CCKM16, GMNS15, LFX+18, LBR12, JLT+12, WX13]. Delegatable [WZ11].
delegated [MZHY15, TMC15]. Delegation [FMTR12, SSW12, XWLJ16, YZ12, YAM+15, JSMG18, NAL17, XWS17, ZWM14].
deletion [DMS+16, Rea16]. Delfs [Mur10].
delivery [FSS+13, SSFC12].
demonstrating [LHA+16]. demonsaaing [HLC16].
deniability [TCS14]. Deniable [DF11, zGXW12, HLLC11, HS11, Jia14b, JXLZ15, LXJ14]. Denial [BKKB14]. Dense [BFM12].
dependent [GdM16, PKA15]. deployed [MFH13, RY10]. deployment [WXK+17].

DepSky [BCQ+13]. Depth [GH11a, RS16, SS10b, SS12a]. Depth- [GH11a, SS10b, SS12a]. Depth-Based [RS16]. Derivation [LBR12, Cha13a, Lan12]. Derivative [LSQ11a]. Derivative-based [LSQ11a]. derived [ZMM+10]. DES-like [CGCS12]. Description [WH18, PLCGS11]. Design [AMN18, Abe12, ARH+18, AIB+16, ADD10, AUMT16, Bel18, BKL+13, DZS+18, DHB16, DR11, FSK10, HSA14, JWJ+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QLL17, RYF+13, Sch13, SAA10, SZDL14, VPK17, WKB16, WDKV19, ZHX16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].


device [AAC+16, CSH+18, DLWW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, ZXH16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].


device [AAC+16, CSH+18, DLWW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, ZXH16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].


device [AAC+16, CSH+18, DLWW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, ZXH16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].

Device [AAC+16, CSH+18, DLWW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, ZXH16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].

Device [AAC+16, CSH+18, DLWW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, ZXH16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, ZYC+17]. Designated [WHJ17, HYWS11, RPSL10, SY15b].
[AEH17, HEK18, WGZ+12]. **DNP3**

[ACF16]. **DNS** [HLAZ15]. **Do** [Bow11]. **doc** [NN15]. **Document**

[BTHJ12, BPP10, DBPS12, DS19]. **Document-centric** [BPP10]. **Documents**

[Bla12, HCDM12, Sta13, XZZ18, ZDL12, CH11, GA11, SR14]. **does** [LRW17].

**Doesn’t** [RS11, SS12a]. **dog** [Ran14].

**Doing** [JCM12]. **Domain**

[AGW15, BDFK12, BM15, CLY14, DG17, LA15, MR16, PDMR12, SGG13, WLZL12, gWpNyY+14, AMK12, BGAD12, GJ13, IG11, LXCMI12, LPZ15, LBR12, PW110, QMC17, SCKH10, yWpWyYP13, YZL+18, YWK+10a, YCM+13]. **Domain-Specific**

[BDK12]. **Domains**

[LQD+16, LRVW14, KGO10, NES+14]. **domination** [GJMP15]. **Don’t**

[BCK17, FHV16]. **Dopant** [BRPB13].

**Dopant-Level** [BRPB13]. **DoS-resistant** [HCC10]. **dots** [Lid12]. **Double** [AK14, ARM15, Lin15, LEW19, PKTK12, Sas12].

**Double-SP** [Sas12]. **Doubling** [Zha12].

**Doubly** [CZF12, CW14b]. **Doubly-Spatial** [CZF12]. **Douglas** [Ber16a]. **Down**

[Ano17e, McG11]. **Download** [ZGC16].

**DPA** [ZI11]. **Draft** [MCF17]. **DRAM**

[SRK+17]. **DRAMs** [LSC+15]. **DRBG**

[YGS+17]. **Drift** [GKS17, JS12].

**Drift Compensated** [GKS17]. **Driscoll**

[Bur11, Joh15]. **Drive**

[SYC+17, Mac12, SYW17]. **Drive-Thru**

[SYC+17, SYW17]. **Driven**

[BMP12, DLMM+18]. **DriverGuard**

[CDD13]. **DRM** [Pet12]. **DSA** [Dra16].

**DSC** [LJ19]. **DSP** [MS13c]. **DSPs**

[DGP10]. **DSS** [Ano13a]. **DSSH** [YLS12].

**DTKI** [YCR16]. **DTLS** [AP13]. **DTRAB**

[FTV+10]. **Dual**

[BWR12, CCG+16, CMG+18, HF14b, NLY12, PAF18, Bwi13, CFN+14].

**Dual-Mode** [PAF18]. **Dual-Rail** [HF14b].

**Dummy** [GST12]. **duplication** [LWLW11].

**Durable** [LY15]. **Durfee** [TK19]. **During**

[FGR+17, ABJ13, RS17]. **DWT**

[LD13, SJ12]. **dyadic** [MO14]. **Dynamic**

[ABB19, EKB+16, FHR14, HH15, KSY18, LHM+15, MWZ12, MM12, NKWF14, PPS12a, PNR17, SS12, SY14, SKV12, SGC14, VMV15, XNK15, XWSW16, XZY+12, XZW+18, ZXYL16, CTL12, CSTR16, DSC12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KH18, KPB17, LMXW12, LHM14, LZC17, NPH+14, PSJ+13, SES+16, SSS11, SGM16, XHM14, YZL+18, YD17, ZS18, ZZZ+18].

**dynamic-identity** [JZS+10]. **dynamical**

[jT12b]. **Dynamics**

[RSCX18, AaBT16, LTC+15a, Lü12].

**dynamics-based** [AaBT16]. **dyslexic**

[Bha16].

e-commerce [Ano11a]. **E-exam** [Mor12].

**E-health**

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

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

**E-passport** [LZJ10]. **e-rental** [LY14].

**E-Voting** [KV18, LGPH14]. **E2** [WY14].

**EAC** [LZX10]. **Each** [YLL+12]. **EAP**

[FLH13, HZC+14, ZCL14]. **EAP-based**

[HZC+14, ZCL14]. **Early**

[Bel18, Bro11, And13]. **Earth** [Har14].

**easier** [MBF+13]. **Easy**

[Bel16, SMD11, Tay14, Wu16, ZDW+16].

**Eat** [DSSDW14]. **Eavesdropping**

[CWL16, Han12, PX13, YSJ14]. **EC**

[Dra16, CFC+14, CCG+16, CMG+18]. **ECC**

[BSSV12, JMW+16, KRR18]. **ECC-Based**

[BSSV12]. **ECDSA** [BBB+16a, DHB16].

**ECG** [PLGMCdF18]. **ECG-based**

[PLGMCdF18]. **Echo** [DLMM+18, HGT15].

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

**Ecosystems** [LDB+15, MMP19]. **EDAK**

[ABB19]. **EdDSA** [JL16]. **Edge** [AHM+18, DF16, KA18, MD15, PRN+19, Sun16].

**Edge-centric** [AHM+18]. **Edition**

[Cor14a, Kob10]. **Editorial** [OK18].

**Editors** [BD19, LLK18]. **Education**
Effect [PLGMCdF18, WB12]. Effective [HLT†+15, KRDH13, WMX†+17]. Effectively [YMC†+17]. Effects
[MAL10, SKV12, SHBC19]. Efficiency [ABF12, Chi16, DG17, FRS†+16, HRV10, LML12, LCL†+17a, MS13b, WXLY16].
Efficient
[ABBD13, ABaS16, ABB19, BWL16, BCGH11, BGH12, BV11, BV14, CG12a, CML†+18, CMLRHS13, CWWL12, CJ13, DBW12, Dnm12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTT11, GP†+12, GPT12, GJ15, GH12, GZH17, GCH15, HZC†+12, HZC†+14, HZL18, HL10b, HBCC13, HZX15, HKL†+12, HIFDCPC15, HCDM12, HH16, HC17, IAD10, KPC†+11, Kim15, KHP16, KH10, LLP†+18, LDDAM12, LZT12, LXX†+14, LCLL15, LSLW15, LHYZ12, LHWS17, LZC17, LBOX12, MX13, MTY11, MVVR12, MU12, MP12, MC11, MN14, NES†+14, NdMMW16, NNM10, PB12, PAF18, PRC12, PG17, PFCP14, PNRC17, RD19, RBHP15, GSY11, SZS14, SGM16, TLF16, TWZ11, TT12, TM18, USH19, WDC18, WLS14, WQZ†+16, WCC18, XLWZ16, XMCL13, YHL16, YNR12a, YNR12b, YLW13, YNQ15, YLA†+13, YS15, ZQWZ10, ZLI†+12, ZSW†+12, ZXJ†+14, ZXYL16, ZCL†+19, ZHS†+19, ZPW16, ZHW15, AZPC14, AZF†+12]. Efficient
[CH11, CCSW11, CLHJ13, CZ14, Cho14, Cra11, CGKO11, EA12, FLL†+14, Far14, FA14α, FA14b, FIO15, FNWL18, GH16, GLM†+11, HPC12, HYS18, ISC†+16, IB11, IOV†+18, JCHS16, JZS†+10, KK14, KIH19, KL11, KSH18, LLLS13, LH11a, LH10c, LXMW12, LAL†+15, ML16, Mes15, Nov10, OCGD11, PZBF18, PC14, Rao17, SZMK13, TLL12, Tso13, TKHK14, VN17, WYLY13, WLZ†+16, WT10a, WXK†+17, WXZW16, yYqWqZC13, ZLY10, ZSZ11, ZCLL14, ZTZ16, ZC15, ZHu13, LLZ†+12, TCL15]. Efficiently [FWS13, LGH†+17, SLY†+16].
Effort [RSGBN12]. Effort-Release [RSGBN12]. EGH [CLR†+18]. eHealth [TMGP13]. eiD [SGGR†+16]. eight
[Sun11]. eight-round [Sun11]. Einführung [Buc10]. Einstein [HR13, Wes15]. Elbirt
[Bar12]. Election [Ess17, TKM12].
Elections [CEL†+19, QS18]. Electoral [CEL†+19]. electrocardiography [PLLH18, YL16].
Electromagnetic [HH1†+13]. Electronic [Bl12, PWVT12, SR14, YMSW11].
Elementary [Ld16, Sch15a, CM13].
Elements [Kra12]. Elevation [LZC†+12b].
ElGamal [HLH19]. ElGamal-like [HLH19].
Elliptic
[AD11, AK14, AR15, DW12, FHL19, GPT12, LGH†+17, LWHS17, M18, PPH12, SG15, AMN18, BAAS13, BL14, BL17, BBB16b, Chol, Far14, IB11, KK10, MC†+18, MS13b, N10, SKH15, WHH17].
eLLiptic-curve [BL17]. ELMd [BDML16].
Elsevier [An15a]. Email
[Bel16, CCS14, XJW†+16, WR15]. embed
[KPS10]. Embedded
[AB15, BS12, BJCHA17, CFXY17, HJ17, JH†+17, LWHS17, MGG†+19, SOG15, SK12b, SDM†+12, WXY†+17, YGD†+17, YS15, An11a, CVG†+13, E10, MFH13, XWZ16].
Embedding [KD12a, MCD12, XR15, XNP†+18, ZZ18, YE12, ZS12, EA11, MKH†+12, PWL13]. Embeddings [FHS13].
Emergable [YT12]. emerged [Mc11].
Emergence [LMB12]. Emergency
[HLKL15, YTH17, KLC†+10]. Emerging
[BSV12, KSA16, OS16, FPBG14, ZHH†+17].
Empirical [gWpN14]+, EFB13, Sar14].
Employees [Mor12]. Employing
[LGKL17]. EMV [Cho10]. Enable [SMS14].
Enabled
[GPT12, HFT16, KV18, QQZ†+16, QQZ†+16b, SGC16, SSPC12, YSF†+18, BM12, TOD18, YFT18].
Enabled/disabled [HFT16]. Enables
[IBM13a]. Enabling
Enciphering

[CMLR, HMR12, MLCH10, Sar11].

Encodes

[WB17].

Encrypted

[DG17, HS18].

Encoding

[BR14, CK18, SK12a, TJJF12, XHX+17, PC14, Sun16].

Encounter

[NA10a].

Encrypt

[RASZ15, Ran14].

Encryption

[AD18, BTHJ12, CWL+14, CWL16, Cor14a, CHN+19, DWB12, DCA18, FCM14, FRS+16, Gen13, GLG12, GZHT12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kaw15, KG16, LA15, LGLK17, LQD+16, Lop12, Mur16, NBP17, NNM10, PBC+17, QL17, SAKM16, Sis12, TM18, Vai12, WBC+10, XWSW16, YDY+16, ZDL12, ZXY16, ZVG16, ZLW+17, AHM+18, AZH11, BTPST15, BPG+17, BKV13, BL11, CH11, CRI16, DKL18, DRD11, ED17, FTV+10, Gen10, GZS+18, HH16, KH18, LXX+14, LZY+16, LHL+18, LW13a, OSSK16, PRZ12, SEXY18, SWW+17, Snc12, TKM13, WR15, WL19, XHY+18, YX18, YQOL17, ZLY10, ZFH+18, ZHT16].

Encrypting

[CC10, Mar10c, dRSdlVC12, LGFCGCRP14, Pow14].

Encryption

[ADM12, AV12, AHI17, Alo12, AAC+16, Ano13c, Ano14, Ano15c, Ano17d, AKP12, ABF12, AB16, BV5+13, BLWA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12, BSI14, BV18, Bla16, BKLS12, BPDS12, BHP14, BMDLN16, Boy13, BV11, BV14, BGV14, CVMI14, CMO+16, CL16, CWL12, CN12, CZF12, CLHC12, Che15, Che18, CGL+12, Chi12, Chu16, CRE+12, Con18, CNT12, CLW16, CD16, DR10, DN12, DFJ+10, DSB18, Des10b, DOS15, Dnu12a, DF11, EAA12, ESI12, FHI10b, FHR14, FJH12, Fei19, FFL12, Fuc11, GWWC15, GGH+16a, GGHW17, GM13, GZ+13, GSW+16, GH11a, GH11b, GHS12, GHPS12, GDCG16, GVW12, GVW15, GM14, GL12, GKS17, Gue16, HMSY12, HLLG18, HZ11, HG12, Hor19, HC17, HTC+15, HLH19, HP12, IAD10, JLS12, JH12, Jia14a, JR14, KAM13, KB10, KME+12, KMY18, KTT12].

Encryption

[KOS16, KKA15, KFOS12, KHPP16, KMY18, KS12, LGMC17, LMG+18, Lnu17, Led16, LSW16, LFLY19, LW11b, LW11c, LW12, LJLC12, LYY+13, LHL+14, LLC+15, LTZY16, LLL17a, LFX+18, LLLH18, LSLW15, LH11b, LSQ18, LB13, LY15, LW16, LYY+18, LML12, LH18, MZY15, MLO17, MMP14, MR14a, MYT11, MSM18a, MVVR12, MBS17b, MRL+18, MBF18, MP212, MT12, MRM10, MSas12, Nac16, NdMMW16, NTY12, NMS14, NAL17, OT12, OGK+15, PMZ13, PR12, PB12, PDNH15, PRGBSA19, Per13, PTKT12, PPS12a, PYS18, PMZ12, PCY+17, PRSV17, RVH+16, RCP+18, RZZ+15, RM18, RSBGN12, RDZ+16, RVRSCM12, SGG18, Saa12a, SSW12, SRL10b, Sch15a, SLGZ12, SZS14, Sh14, Sm11b, Sta12, SGH15, SMOP15, Tan11, TCN+17, TLC15, TMC15, Tan17b, TD13, TKR14, TT12, Unr15, Vai11, VSR12, VOG15, Wal18, WCH+15, WP17, WDCL18, WSS12, Wat12, WLC12].

Encryption

[WDD12, WZ15, WWHL12, WMS+12, WZQ+16, XNK15, XY18, XXZ12, XJWW13, XWLL16, XJW+16, XHX+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC+11, YFK+12, YCY12, YKK12, ZOC10, ZPM+15, ZZQ+19, ZDL12, ZYT13, ZWTM15, ZQQ15, ZMW16, ZMM17, ZHW15, ZY17a, ZYM18, ZWS+18, ZYH+19, ZHZ+19, AHS14, AKHH+17, AKK17, Ana14, Ano13b, Ano15c, Ano16f, AR12, AMH10, ACD+15, AHL+12, BLL+19, BAAS13, BC18, BG14, BSW12, BGP+17, CPPT18, CFVP16, CFZ+10, CW14b, CLH+16, CMM17, CZ15b, CS11, Chni10, CW12a, CDF+10, CM13, CGKO11, DLZ16a, DDM17, DTZ12, Eve12, Eve16, FAA+18, FH13, FSGW11, FSWG12, FMB+18, Fay16, GMOGCCC15,
GH13, GHPS13, GLM+16, GH12, GLL+18, GZXA19, HGWY11, HQZH14, HZL18, HWDL16, HZWZ18, HT13, HLR11, HL11, HFT16, HTC17, HYS18, HYF18, HKHK13, JCHS16, Jianh14, Ji14h, JHCC14, JSM+18, Kam16, KHMB13, KKM+14].

Encryption [LLW16, LCL+17a, LCL+15, LFZ+17, LCT+14, LFWS15, LLM+19, LPdS10, LHH11, LW10, LW13b, LZC14, LPZJ15, LCY+16, LZC17, LJW+17, LJY18, LLL+18, LDZW19, LL16a, LW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSas13, NES+14, Nam19, PPA18, Pet12, QRW+18, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SGFCRM+18, SLM10, SKB+17, Spa16, SGP+17, SGM16, Tam15, TPL16, tJ12b, WGTJ10, WY10, WWYZ11, WYYY11, WHY+12, WZDZ13, WLFX17, Wan18, WGZ+12, WLS14, WCCH18, XWZW16, XWXC14, XSWC10, XXX15, XWS17, XWZ+18, YTL1b, yYqWqZC13, Yan14, YZCT17, YHHM18, YCT15, YLZ+16, YL11, ZWQ+11, ZZ11, ZLW+12, ZXJ+14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZYC+17, ZCL+19, ZZ12, ZL12, ZWD+16, ZY17b, Zhu13, Wan14, LAL+15, Sar18a, Kat13], encryption-based [BC18, XWZ+18].

Encryption/Decryption [KB10].

Encryptions [zGXW12, LG12, SLY+16, RD17].

Encyclopedia [vTJ11].

End [Ano15c, BRR+15, BGP+17, CFE16, Ch16, RST15a, RST15b, Ch13a].

End-to-End [CFE16, RST15a, RST15b, Ano15c, BRR+15, BGP+17].

Endomorphism [FWS13].

Endomorphisms [AK14, LGH+17], enemies [Fag17].

Energy [Ano15d, AZF+12, ABC+17, Bla16, JEA+15, LSC+15, MP12, PAF18, TLCF16, TCN+17, VN17, CZ14, ZTZ16].
Erratum [YFK+12]. Error [KW14, LSC+15, MCP15, TLCF16, AT+10, Chi13a, LTT10]. Error-correcting [MCP15, LTT10]. Errors [TM18, CSS+13].

Ergodic [GLW12, SS13, WGD18, HKT11]. Era [Mos18, QCX18, ABJ13]. Ergodic [IAD10].


Equivalence [ABR12, CCK12, CCK16, GLW12, SS13, WGD18, HKT11]. Era [Mos18, QCX18, ABJ13]. Ergodic [IAD10].


Evaluators [ZK17]. Evaluators [KSS16]. Evaluators [ZK17]. Evaluate [Bai12]. Essays [Nac12].


Fabrication-Induced [VDB+16]. Face [AQP12, XHH12]. Facial [KRB12]. facilitate [Chi13a]. Facsimile [Ano16d].

Factor [HXC+11, LLC11, AIB+16, CLP+13b, DMWS12, ED19, HC12, IC17, JKL+16, JM+16, Kem11, LN+18a, LN+18b, Lit14, WW14, Wat14a].

Factorization [APPVP15, LLM12, MM13].

Face [HXC+11, LLC11, AIB+16, CLP+13b, DMWS12, ED19, HC12, IC17, JKL+16, JM+16, Kem11, LN+18a, LN+18b, Lit14, WW14, Wat14a].

FastAD [SMBA10].

Faster [CN12, HVL17, TH16, ZSP+19, 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, PBC14, WMYR16].


Features [Y1+14, ZTL15, FNP+15, LCM+17, LTC+15a].

Feauveau [Ara13]. February [Ano10, DDS12, Dan12, Dun12b, Kha11, Lin14b].

FedCohesion [CCFM12]. Federated [BS13b, CCFM12, CSL+14, SAM+19, BMBS10, JAS+11, TODQ18].

federated-IoT-enabled [TODQ18].

Federation [SS10a, NB13]. federations [MMS+17a, MLM16]. Feedback [HZ11, Hey17, PYM+15, SKGY14, ZH15, LWK11].

Feedback-Based [PYM+15]. FEIPS [DG15]. Feistel [BFMT16, KDH15, Sas12, SEHK12].

FESSD [LGLK17]. FHE [CK18].

FHE-Based [CK18]. FHD [SP15a]. FI [YNR12a]. FI-BAF [YNR12a]. Fiat [BDG+13]. Fibonacci [FM15, LLP+18].

Fibonacci-number [ LLP+18]. Fidelity [BCP14a]. Field [CLF+17, GHP13, HSA14, SS12a, TGC16, ZAG19].

Fields [ARH14, BGJT14, HVL17, AA14, BGJT13, C15a, LBOX12, ÔS11].


filtered [HTC17]. filtered-equality-test [HTC17]. Filtering [LLZ+12, CDD12].

Financial [Ano11b, Ber12, DDS12, Dan12]. Finding [Hof16, Ste15a]. Fine [CDD13, YTH17, ZML17, CLH+16, FSGW11].

Fine-Grained [CDD13, YTH17, ZML17, CLH+16].

FinFET [ZJ11]. FinFET-Based [ZJ11].

Finger [KLY+12]. Fingerprint [DS19, MR14b, KKG14, Kie17].

Fingerprint-Based [DS19].

Fingerprinting [QF19, TSH17, ZS12, FZ+12, RS17]. Finite [BGJT14, C15, GMNS15, HVL17, AA14, BGJT13, C15a, GPLZ13, LBOX12, ÔS11].

Finite-State-Machine [CHS15]. firms [Ano15e]. First [Ano17d, BH15, DR10, FFX+18, MS17, PC16, Wil18, AB10a, BC12, Kim11, LCK12, Mic10a, SBK+17, Zet14].


Flexible [EBK+16]. Flexible [LGWY12, PAF18, BGG+13, WLS14, ZL12, ZFH+18].

Flexible [EBK+16]. Flexlist-Based [EBK+16]. flip [Wag16]. Flow [ATS15, HBC+19, WXL+17, KL13, ILYW12, PPR+12, SRB+12].

Flowers [Hall17]. Flows [CDD13, HKB14, WYL13]. fly [PS14]. fog [JSMG18, KH18, QRW+18, Wan18, WDKV19, ZSW+18b, YXA+18].

FontCode [XZZ18]. Foolproof [FLR12]. Force [JR14, CJP12, CJP15]. Forensics [Ber18, CFXY17, AKM+11, Har14, QZ14, SM13].


Forward-Secure [BVS+13, KME+12, LTH+15, NMS14, WLH15, YKC+11, YFK+12]. ForwardDiffSig [BAL10]. forwarding [VN17].


FOX [LIF16]. FPGA [AMKA17, BCE+10, BDGH15, CFZ+10, CHS15, GFBF12, HF14b, MM14a, MAK+12, ZLQ15].


Framework [BJL16, CD12, DG17, HXC+11, KPC+16, KVE+18, LLG15, LSC+15, LY15, LQD+16, MSU13, SK11, Scr18, SYC+17, SEK+19, TSH14, VKP17, ZJ14, ATKH+17, BCHdFR12, KKGK10, KMI14, MMS+17a, MBF+13, PSdO+13, PLCGS11, PAKA15, SD10, SA16b, SYW17, ZYC+17]. frameworks [LSBN14]. France [Kap11].

Francis [Joh10]. Francisco [Dun12b, Kia11, Pie10]. Francois [SR14].


Freedom [Con18]. Freestart [SKP15].

French [Ant14]. Frequency [BBM15, KAHK17, LTKP16, LWCJ14, TC10, CJP12, CJP15, EA12, NLYZ12].

Frequency-Based [LWCJ14]. Freshness [RBNB15]. Fresnelet [FMB+18]. Friendly [Fra16, KCC17, SZZD14, ACM12, BP18, KLM+16, RD17, WOLS12]. Frontside [DDR+16].

FSR [MD12b]. FSR-Based [MD12b]. Fugue [AP11]. Full

[ALR13, HEC+12, LW12, VS16, WLC12, BKR11, DDM17, LC13, Ran16, SWW+17, SKP15, Tam15, TY16b]. full-hiding [DDM17]. full-text [SWW+17]. Fully

[AKP12, BV11, BV14, BGV14, CMO+16, CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, LMG17, LSLW15, LSC12, MVL12, MS18a, Nac16, NCCG13, PB12, SGH15, VAI11, VV19, WHC+15, XWZ+18, ZZ12, GH13, ZSJ+14, ZML17].

Fully-Homomorphic [GH11b].
Fully-Homomorphic-Encryption [CN12].

Fun [APPVP15]. Function
[AMPH14, Bee17, BKST18, FLS+10, LyWIZZ12, MMS17b, SGY11, WSSO12, AKY13, AP11, CMMS17, LK14, LP11, RS14, Sar11, SXL16, TQL+14, WYW14].

Functional [AS16, BV18, BSW12, Boy13, GGH+16a, GVW12, LQD+16, MV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14].

Functionalities [JR13]. Functions
[ACZ16, ALR13, BBC+14, BIKK14, BKPW12, BK12a, CCL+19, CPS16, DSMM14, DQFL12, FY11, LVD11, NR12, Rja12, RW12, SMS14, SLY+16, Tan12a, YTP11, AY14a, BDPI11, CG12b, CQX18, CW12a, ESR114, Gen10, HRV10, Li10, QZDJ16, WT13].

Fundamentals [Joh10]. Further
[HCL+14, WHY+12]. Fus
[FMS12a]. Fusion
[ABCL17]. Future
[AYS15, BCE+12, BKBK14, Bon12, CDFZ16, GCK12, HYS18, Mon13, Ano13d, FBP14, Mac12, PPA18, PHWM10, MJS13].

Future-proof [Mon13]. Fuzzy
[KRDH13, NC12, SH11, USH19, XJJW13, Alp18, KHM13, MMSD13, SM11, SMN14].

FV [MRL+18].

G [HLYS14]. G2 [BP18]. G2C [BMP12].

GA [MMSD13]. GA-fuzzy [MMSD13].

gadgets [Gel13]. Gait [XRJ+17, XJR+17].

Gait-Based [XJR+17]. Gait-Key
[XJR+17]. Gallai [SS10b]. Galois
[CFR11, CLF+17, HSA14]. gambling
[Ana14]. Game
[MZA+13, LPZJ15, SD10, SKEG14]. game-theoretic
[SD10, SKEG14]. Gap
[LRVW14, TGM13, PPA18]. Gaps
[SM+13, DKL+16]. Garble
[AIK14].

Garbling [App13]. Gard [Kap11]. Gate
[Kar12]. Gates [App13]. Gateway
[WZM12a, WZM12b, WL11, WXX+17].

Gateway-oriented [WZM12a, WZM12b]. Gaussian
[HKR+18, RMERM19, YWL+17].

GCD [KI11]. GCHQ [Ald11]. GMC
[SKK10]. GCM/GMAC [SKK10]. GDLP
[MMZ12]. Gear [AHS13]. Geckos [GSC17].

geese [Bai12]. GenePrint
[HQY+16].

Gener [HY18]. General
[Bar16, CJXX19, FJHH12, GFBB12, Gue16, HP12, KOTY17, LPL15, PBI2, SJWH+17, YFF12, ABDP15, Bai12, DQGI14, HQZ14, LWS10, WS12, YCI11, ZYC+17].

General-Purpose
[Gue16, ABDP15, DJJN14]. generalisation
[LR15]. Generalised [Hes12].

Generalization [GMNS15]. Generalized
[BBMT16, LPL15, PC14, TY16b, Ye14, ZAC17, ADG16, BNST17, KL11, NC13, YMSH10]. Generated
[ADD10, LCL17b, NN12, XYXY11, AGHP14, LW13b].

Generating [Ano16e]. Generation
[ABS+12, BCGH11, BH15, LCT+15b, MR14a, MJG12, NIS12, PS14, SO15, SRK+17, XJR+17, Aia15, ACD+15, CIJX19, GARR+15, GCH15, KHM13, KKM+13, SFCR+18, WX13, YDH+15].

Generator
[ADD10, BK12a, CDK+10, MV12, NNAM10, NKF14, CFY+10, LGKY10, MRT10, PLSD10, SH11, SM11, XSWC10].

Generators
[AS17, DSLB18, LTKP16, MFG16, NIS12, PFS12, CP13, HRV10, MG15, St11, Zim10].

Generic [BWLA16, BR14, Chi16, GWCC15, HXC+11, Sar10b, SY15a, WCL+18, ZCCL14, HQY+16, YT11b].

gerenically
[MHKS14]. Genetic
[JK13, MM17, ASVE13, HAEZ13, PTK14].

genius [Hai17]. Genomic
[BKL18, RCP+18]. Gentry
[GH11b].

Genuine
[HR13]. genus
[FWS13]. geo
[Har14]. geo-location
[Har14]. geodesics
[ZJC14]. Geographic
[LC17].

Geolocation
[PPY15].

Geometric
[DBB16, GTTT11, WLZ12, YWW15, CLZ+17, GZH12]. geometrical
[TL13].

Geometrically
[WYW+13]. Geometry
[tWmC12, CFR11, CZ15a]. German
Handwriting [SKV12]. Handwritten [GdM16, ASVE13]. Hankel [Ye10]. Hans [Mur10]. haptic [ASVE13]. Hard [KPC†11, Mar10c, ZWTM15, RPG12]. Hard-to-Invert [ZWTM15]. Hardcover [Joh10]. Harder [KTA12, Sch16]. Hardness [BHKN13, SS13]. Hardware [AW15, AW17, BRPB13, BDMLN16, BUCHA17, CMLRHS13, DZS†18, DOS15, ERRMG15, GCVR17, GCS†13, HKL†14, HG12, HSA14, HC17, HLN†10, KAK18, LGH†17, LLKA19, LRVW14, MLCH10, MCS†15, MRL†18, MHY†18, NDC†13, NmM16, PC16, PG12, RMP10, SN10, Set16, Sti19, Tay17, WOLP15, YSF†18, ZHS†19, ZAG19, AMN18, BDM18, BGG†13, KHF10, MD12a, NS10, Nov10]. Hardware-Assisted [LLKA19]. Hardware-Based [HLN†10]. Hardware-Enabled [YSF†18]. Hardware-Enforced [Set16]. Hardware-Intrinsic [SN10, NS10]. Hardware/Software [MRL†18]. hardwares [SKH15]. Hardy [Xie12]. Harmonic [YWWN15]. Harnessing [DFKC17]. Harvesting [ABC†17, ZGC16]. HAS-160 [WLC12]. Hash [Ano12, AMPH14, BHH†15, BKST18, BK12a, CLP13a, jCPB†12, CZLC12a, CZLC12b, CZLC14, CJJP12, DCM18, EAA†16, FLS†10, GI12, HCPBS12, Hü13, HRS16, HBG†17, MKF†16, MCF17, MKA17, NTY12, NR12, NXB13, PTT16, Rja12, SGY11, WSSO12, ZM17, ZHZ†19, AY14a, AKY13, AP11, CJJP15, ESR14, KKG14, PPB16, RS14, SPLHC14, SXL16, WYW14]. Hash-Based [BHH†15, GI12, HCPBS12, Hü13, HRS16, HBG†17, MKF†16, MCF17, MKA17, N XB13, CJJP12, CJP15, PPB16, SPLHC14]. Hashing [AAE†14, ASBdS16, BHKN13, BKL†13, BP18, Kaw15, CP13]. Haskell [Rus15]. hatching [WYK12]. HB [HSH11, PYH†18]. HDH [PDNH15]. Headline [YGFL15]. Health [LYZ†13, LHL15, Rao17, ZVG16, BC18, Ham19, IC17, WMX†17, YZL†18, JKL†16]. Healthcare [BN14, HLKL15, ZLDC15, ASO14, Kim16]. Hearing [Bla16]. Heartbeat [IA15]. Heartbleed [DKA†14, Ven14]. hedging [YR10]. Heights [Gen13]. held [Cho10]. Helios [CFF16]. Hell [Han12]. Hellman [ABD†15, Chi16, HoF16, HLCL11, HLYS14, LZZ14, LNL†19, Om16, RH10]. Helmut [Mur10]. helped [Smie11a]. helper [RWZ13]. HeNB [CLM†12]. Herodotus [Keb15, Mac14]. heroine [Fag17]. Heterogeneous [SP15b, AIKC18, ABB19, SZMK13, SCKH10]. Heuristic [BGPJT14]. HEVC [DG17, KGSB17]. HIBE [LW11c, LSQX19]. Hickory [NN15]. Hidden [FMS12b, PSS†13, YLL†12, ZYT13, BDK11, LCL†17a, Sch15c, Smi15a]. Hiding [DCA18, GGH†16b, GI10, JHNN12, MK12b, OT12, XLM†12, XGL14, WZL15, Ara13, DDM17, HZL18, KWH16, LXLY12, LT14b, UUN11, WLH13, WZL13, ZWM14]. hiera [Lac15]. Hierarchical [ADM12, BSSV12, FSX12a, LSLW15, NMS14, NLY15, OT12, WYML16, ZMW16, ZHW†16, DCS12, HYS18, KPB17, LF†17, NZM10, RG10, SE14, SE16, WWYZ11]. Hierarchy [NA10b, VN16]. High [AW17, ASBdS16, Ano17d, ARM15, Bar15, BDL†11, DM15, DG17, FHL19, GI12, GCS†13, HZ11, KMP†11, KPC†16, KAK18, LTKP16, LCK11, LLY†18, LPO†17, MS13b, MS13c, PCPK14, WYCF14, WL11, XNRG15, XLP†18, ABB13, GZHD12, GCVR17, KL13, MAK†12, RS17, WLH13, WXLY16, WZL13, WHH11]. High-Assurance [Bar15, KMP†11, WL11]. high-capacity [GZHD12]. High-Dimensional [Ano17d, XLP†18]. High-Efficiency [DG17]. High-Impact [DM15]. High-Level [AW17, KPC†16, ABB13].
YXD18, ZXZ+11, ZWZ17, BWA13, BM13, CT11a, CW14a, EA11, FMB+18, GKCK11, HLC16, KM11, LXCM11, LW10, LWLW11, LW13b, LPZJ15, MO14, MS17, NES+14, PTK14, SE18, Sch12a, SM13, SM12, SNM14, SGFCRM+18, Sun16, jT12b, TTL10, TLL13, UUN11, UUN13, yWpWyYP13, WGZ+12, WKH11, WOLS12, XSWC10, YWL+17, YC11, YCC16, YSL16, ZLW+12, ZT14, ZSMS18, ZL12]. **Image-Guided** [CJFH14].

**Image-Scrambling** [LLL17a].

**ImageMagick** [Tay14].

**Imagery** [BCP14a, Ara13].

**Images** [BCPV11, BBM15, CLF11, FR16, GL10, LC15, LLY+12b, MR16, NC12, Yam12, dRsdiVC12, AMK12, DD13, HWYV14, LW13b, MM14a, MKH+13, UUN13, WLH13, WZLW13]. **imaging** [WW13].

**IMFlexCom** [PAF18].

**IMI** [PN10].

**imitation** [Hai17].

**Impact** [Alo12, BLS12, DM15, SF12].

**Impartial** [BCF16].

**Imperceptibility** [HTG15].

**Imperceptible** [Lin14a].

**Imperfect** [ABD+15, BHvOS15].

**impersonation** [AATM18, GBNM11].

**Implants** [Mic16, SSPL+13].

**Implausibility** [GGHW17].

**Implementation** [BW16, BKLS18, BSJ15, BDMLN16, EGG+12, FHL19, GP17, GL12, GPT12, GCS+13, HF14b, KB10, KG16, MF16, MAS16, NdMM16, QLL17, RMP10, VKP17, ZP+15, AMN18, BDP+12, GH13, HBBRMN+16, KY10, KSH18, MM14a, MNW12, NES+14, PBCC14, SK14, SAAB10, SF12].

**Implementations** [BFCZ12, BFK16, BDGH15, BJ10, Bru12, CMLRHS13, CBL13, ERRMG15, LGH+17, MLCH10, Tom16, YZLC12, ABBD13, ABF+14, BFG+14, BJ+14, CFN+14, CGH17, LBOX12, RSMA19, Sta11b, ZSW+14a].

**Implementing** [Dav11, GH11b, HTZR12, LTC+15a, SG15, SLM10, Vog15, SA16b].

**Implications** [DK16a, OS16].

**implicit** [DWZ12].

**Imply** [ALR13, LRW17].

**Importance** [YL17, MLMSMG12].

**Important** [TC10].

**Impossibility** [ACM+17, BCF+14, Mat14].

**Impossible** [BLo15, CWP12, LJJ16, TSL11, WL14, WW12, MNP12, SDM10, SDM14].

**improbable** [TS16a].

**Improve** [AQD12].

**Improved** [Ber18, BCP14a, Chi12, CGKO11, FVK17, GLLSN12, IK15, JLL12, KZG10, LT14a, LW12, LJJ16, LHL11, LCCJ13, LC15, LML12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GLW13, HWB12, Nam19, PWLL13, SDM10, XHH12, Wan14].

**Improvement** [FRS+16, LFX+18, LJJ19, MWZ12, PLPW13, AN15, BMB16, CHS11, Fur14, LNM+11].

**improvements** [EA12, HRV10, Tso13].

**Improving** [AB15, BCM+15, Chi16, FMS12b, GMS11, HLC11, MHC12, Sar10a, SS11, YWF18, YKBS10].

**IMS** [IG11, MEFO12].

**In-Memory** [PAF18].

**In-Order** [ZBP18].

**Incentive** [SJWH+17, YTH17].

**Incentive-Aware** [YTH17].

**Incident** [CCG+16, CMG+18].

**Inclusive** [FD11].

**Inconsistencies** [YSC+15].

**inconsistent** [OF12].

**Increase** [NNAM10].

**Increasing** [AEH17, CLZ+17, PKS18].

**Incremental** [KKM+14, MPRS12, CS11].

**Incrementing** [KS15].

**IND-CCA** [AHS14].

**IND-CCA2** [Gil13, MVVR12].

**indefinite** [Svo14].

**Independent** [FCM14, M11, MKRM10, YE12, ZTL15,BVIB12, DDD14, VV19].

**Index** [LHKL10, PSS+13, ZXYL16, JUN13, LLHS12, LW13a].

**Index-Based** [ZXYL16, LLHS12].

**Indexing** [HCDM12].

**India** [BC11, CGB+10, GG10].

**Indicator** [KU12].

**Indicators** [Y12, Pal16].

**Indirect** [ABS+12].

**Indistinguishability** [AS16, BV18, FMY15, GHHR14, GGH+16a].

**Indistinguishable** [LG12].

**Individual** [LMB12].

**INDOCRYP** [BC11, GG10].
Induced [VDB+16]. Induction [BBBP13].
industrial [GHD19]. Industry [Ano11b, QZL+16a, Cha13c, Men13b, ZSMS18].

Infective [GST12]. Inference [Bro11, DBPS12, NC12]. Inferring [BPSD17].
Influence [RSCX18].

Information [AQD12, ABCL17, Bai10, BF11, CVM14, CDGC12, CGB+10, CST+17, CBL13, Dew11, DP12, FHKP17, FHS13, HBC+19, HHI+13, IF16, JHHN12, LG12, LW11a, Low12, MA17, MAL10, NTKG17, SGC14, STC11, TWZ11, WSS12, XZZ18, Yan10, Yek10, ZZ15, ZHL15, ZBPF18, AB10a, Abe10, AL15, ASVE13, BSS11, BGP+17, DMWS12, KL13, LWK+18, MKH+12, Mar10b, SRB+12, WW13, YL10, LH10a].

Information-Theoretic [CVM14, WSS12, CDGC12]. Information-theoretical [ZZ15, KL13].

InfraStructs [WW13]. Infrastructure [GM13, PN10, GAI+18, JAE10, SA12].

ingenious [Mac12]. Inhibiting [GAS+16].
Initial [PAS13b]. initiation [AN15].

Injected [LLZ+12]. Injecting [BBGT12].
Injection [ABS+12, ARP12, DDR+16, JWJ+17, PYM+13, YGD+17]. Injections [LCLW17]. Ink [Keb15, Mac14]. Inner [ADM12, LMG+18, OT12, YKNS12, DDM17]. Inner-Product [YKNS12].

innovations [JSM+18]. Input [GGHW17, XXZ12, PBCC14]. Inputs [GGHW17]. INSCRYP [BYL10].

Insecure [BCGN16, Mur16, Lan17].


Inspires [SPG+19]. Instability [LMB12].

Installment [SYC+17]. instance [BRT12].

Instances [HN10]. instead [AGH+17].

Institute [Wes16]. Instruction [ARP12, AB15, EKP+13, HZS+19, BVIB12, SF12].

Integral [AY14b, LWZ12, ZSW+12, SM11, SNM14, SH11]. Integrated [LY15, MU12, AL15, SYL12]. Integrating [CFZ+10, LH12, OdH12, AEH17, HLYS14]. Integration [AQD12, Kar12, ZY+W13].

Integrity [BCP14a, BCK17, FMYM15, MV16a, PH12b, SB18, ED17, SWW+16, YXA+16, YNX+16].

Intel [SF12]. Intelligence [Dew11, Ald11, Bud16, GW14, Han12, Maf16]. Intelligent [AMK12, IEE11a, SAJL16, Wat14a, HLYS14, MKH+12].
Inter [LBR12, BGAD12, SCKH10, SA15, SHBC19, YWK+10a]. Inter-domain [LBR12, BGAD12, SCKH10, YWK+10a].


Interactive [CJFH14, DF11, FSGW11, BCI+13, Pas13a, PPR+12, Yan14].
interceptor [Cho10]. Intercepts [Don14].

Interest [Sch19]. Interface [WBA17].

intermittent [CL16]. International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FB12, GLIC10, JY14, LCK11, LW11a, LTW11, MV12, Pdj12, Sen10, Wat10, Yan10, Yan11, AB10a, Abe10, Anol1a, BYL10, BL10, Gll10, GG10, HWG10, LH10a, IE11a].

Internet [Anol13d, LFGCGR14, TW14, AAC+16, Anol13b, CLF+17, CW12b, CEL+19, DRS16, DG15, Gel13, Ham19, HZL18, JKAU19, JZT+16, LNK+18b, LGH+17, LSG16, MJGS12, MJLS13, MCF17, NLLJ12, NLY15, Orn16, PLGMCdF18, SB17, SS19, SYW17, SYC+17, SKEG14, WCCH18, YCT15].

Internet-Draft [MCF17].

Internetworking [SAAB10].

Key [ASN12, Ano11b, ABB19, BN14, BVS+13, BL12, BBD+16a, BD15, Bar16, BCO13, BKL12, BF11, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CLND19, CJ13, Chi16, CCT+14, CNT12, Cou12, CMA14, DWWZ12, DL12, EAA+16, FZT13, FVS17, FBM12, GFBB12, GT12, GZZ+13, GSW+16, GST13, GPT14, Gir15, GKS17, GZ12, GLB+18, HSMY12, HLLG12, HC12, HL10a, HCL+14, HTP+15, HEC+12, HL119, Jia14a, JEA+15, KP12, KTT12, KFOS12, Kim15, LLSW16, LCLL15, LQY10, LY16, LH11b, LSQL18, LCCJ13, LYY+18, LBR12, LL18, MZHY15, MV12, MMP14, MTY11, MMY12, MV19, MPS12, MSU13, NNA10, NYR+14, NTY12, Orm16, PSM17, PDMH15, PCPK14, Pub12, PNRC17, RVH+16, RSBGN12, RW12, Saa12a, SK11, SNJ11, SEHK12, Sas18, SK12b, SWM+10, Sia12, SGH15, SLY+16, TMC15, TYM+17, TM12, WP17, WSS12, WLC12, WZ15, WCL+18].

Key [WWHL12, WT10b, XNKG15, XXZ12, Xio12, XLM+12, XJWV13, XGLM14, XZLW15, XJR+17, YM16, YZX+12, YS12, YLW13, YRT+16, YL17, Yon12, YKC+11, YKF+12, ZSP+19, ZXH16, ZY17a, AA14, ATKH+17, APK+18, ABB+14, AKG13, AIB+16, ABV10, AN15, BS15, BGAD12, BB14, BJ16, BSW12, BGG+13, BBB16b, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLZ10, DLK+16, DGIS12, Dur15, FHH10a, FA14b, FIO15, FHZW18, GMRT+15, GPP+16, GH16, GBNN11, GLM+11, GTSS19, HPC12, HZWW17, HBW12, HL11, HLYS14, HTP17, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSMG18, KDH15, KMTG12, KKG14, KIH19, KP18, KLW+16, KDW+17, LLLS13, LLP+18, LW10, LKL+17, LPdS10, LW13b, LZC14, LML+13, MNP12, MRT10, NACL12, NCL13, Nos11, Nos14, RG10, RWZ13, RPSL10, SES+16, Sar14, Sav16, SLZ12, SY15b, ZMK13, hSZZ15, SA15, SG+17, SvT10, TK19].

Key [TCS14, TLL12, Tso13, TGHK14, VV19, VN17, WZYZ11, WDKV19, WZM12a, WZM12b, WT10a, WTT12, WQZ+13, WXX+17, WX12, WX13, XCL13, XMHD13, XHM14, YT11b, YC12, Yan14, YZZ+14, YHHS16, YZL+18, YLZ+16, ZP+16, WZQ+11, ZZ11, ZCC13, ZT16, ZZ+18, ZW11, ZCL+19, ZG10, ZCZ15, ZY17b, ZWS+18, ZHT16, CLW16, OHJ10, XJR+17].

Key-Aggregate [CCT+14, PSM17, GLB+18, CLW16]. Key-Agreement [WSS12, APK+18]. Key-Alternating [BKLS12]. Key-Based [Xio12]. key-correlations [Sar14].


Keyed [KE19, MMS17b, YHHM18].


Keys [ASN11, BF12, Bro17, CC10, HDWH12, LSQX19, MS16, PSM17, TW14, ZMW16, CMG+18, HL14, IK15, LLY15, LH13, LW10, LLL+18, RWZ13]. keystream [SM11]. Keystroke [AAIB16, SP13, CTL12, LTC+15a].

Keyword [CWL+14, Che15, HCDM12, HLH19].
LSQL18, WDCL18, XWSW16, XJWW13, ZXYL16, BL11, CLH+16, FSGW12, GZS+18, LXX+14, OSSK16, SY15b, WHY+12, WXLY16, XYW+18, YZCT17.

Keywords [CWWL12, ZL11], KGC [YT11a]. kid [Tan17a]. Kind [WJ19]. King [ABJ13]. kiss [HU15, KYE+18, Ros11].


L [Low12, Xie12]. Labs [Ven14]. Labyrinth [Fox13]. Lacks [BDSG+13]. LACE

[BCO13]. Land [Sch18]. Landis [BB16b].

Languages [MX13, Wat12]. LANs [FL13].

Lapin [HKL+12]. Laptop [GPT14]. Large

[AN12, DM15, FWNW18, JLS14, JKHeY12, KCR11, KU12, LW16, LQD+16, MC11, SP13, dCCSB+16, EEAZ13, FXP12, GSN+16, LFZ+17, LBOX12, SR10, ZZKA17, ZVH14].

Large-Scale

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

LARK [DS11]. Laser

[DDR+16, FNP+15, Lied12]. Last


Latin [AB10a]. Latinicrypt [AB10a].

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, XXZ12, ZQQ15, Kre13, Tia15, XLWZ16, yYqWyZC13]. launch [Zet14]. Laurens [Ano15b]. Law

[Bla12, SR14, Wu16, AOT13]. Layered [Dreff12, BS14, GRL12, WW1+14, JCHS16, ZC12]. LBlock [KDH13, MNP12].

LDGM [BBC+13].

Leader [TK12]. leak [BBG+17]. Leakage

[AV12, BBK10, BCL13, DCA18, DHB16, FPS12, HH+13, HHP17, IL15, LTZY16, NTKG17, NTY12, Pan14, SGH15, TTH15, Wan18, ZY12, YZLC12, YZ12, YZC12, ZYT13, ZWMT15, ZM16, ZMM17, ZY17a, ZY17b, ZY18, ZYH+19, ZBFP18, CQX18, DLZ16a, DMWS12, GV14a, GL18+18, SGP+17, YLZ+16, ZWM14, ZCC15].

Leakage-Free [IL15, TTH15].

Leakage-Resilience [NYT12].

Leakage-Resilient

[AV12, FPS12, LTZY16, Pan14, ZY12+12, ZYT13, ZMM17, ZY17a, ZY18, ZYH+19, ZY17b, ZY18, ZYH+19, ZBFP18, CQX18, DLZ16a, DMWS12, GV14a, GL18+18, SGP+17, YLZ+16, ZWM14, ZCC15].

leakage-tolerating [ZWM14]. Leaking

[BF11]. Leaks [DL16, Sav13a]. Leaky

[DL16]. Leap [Ano16c]. Learned

[KMP+11, WL11]. Learning

[CTC15, KPC+11, KRB12, SPG+19, Yon11, GJ13, Sch12a, WS14, BCV12]. learning-based [WS14]. leave [CMG+18].

Lecture [Hel17]. LED


Left-to-right [BBG+17]. Legacy

[CS12, Smi11b, CGH17]. Legal [ZTSR12].

LeGall [IS12, JKP12, MRTV12].

Legalize [PH12b].

Lemonade [DFKC17]. Lenmons [DFKC17]. Length [AS17, GT12, GY15, PND15, PNRC17, Zha12]. Length-Doubling
lens [PHN+12]. LEO [RM18].
LESPP [WLZ+16]. Less
[TKR14, GM13, Kam16]. Lessons
[KMP+11, TGC16, WL11, CMG+18]. Level
[AW17, Anu15a, BRPB13, BKP12, CCW+10, DA10, Gli12, HZS+19, HS18, JWJ+17, KPC+16, KGP12, MV16a, ZLDC15, ABBD13, MEFO12, RS17, UUN13, VS1, YTI11a, Bai12]. Leveled [BGV14].
leveling [LY15]. Levels [HLCL11, LRW17].
Leveraging
[DMS+16, HCM11, MvO11, SKGY14].
Lewis [Mar10a]. Lexicographic [ZAC17].
LFSR [HLC12, MRT10, WGD18]. LFSRs
[QGGL13]. Liability [Bra13]. Liars
[Sch12b]. Libgcrypt
[DK16b, Bro17, Win17]. LibrA [GMVV17].
Library
[ACZ16, Bee17, BLS12, FLW12, KRH18].
Life
[MKN13, SCMS18, McK10, McK11, War11].
Lifecyle [Tan15a]. Lifetime [HSUS11].
Lifting [LSL12b]. Light [JEA+15].
lightweight [Ran10]. Lightweight
[AMKA17, AARJ12, BSS+13, BFMT16, BKL+13, BM11, CGCPGMDG12, CWP12, CCF17, DS11, ESS12, EKP+13, FQZF18, GNL12, GAI+18, GMVV17, GMSV14, HZWZ18, HCTEPL+12, IS12, IOM12, KE19, MO12, MFG16, MPM+17, PCDG14, She14, ZYW+13, ZLY+19, AMN18, AATM18, AKKY17, BLL+19, Bor10, BBB16b, CL11, FLL+14, GTSS19, KDH15, LLI+16, MCN+18, MNP12, MHV15, MYY+18, PJ18, PSSO+13, SGJ+18, Tan12b, TG17, WLZ+16, WCFW18, WWBC14, XWZ+18, XHM14, YCT15, ZSW+18a]. Like
[BW16, ERLM16, WJ19, CGCS12, HLH19, KO16, LLI15, LJ16, RS14]. Liliput
[BFMT16]. Limitations [DR12]. Limited
[DFKC17]. Limited-Use [DFKC17]. Limits
[AS16, GV14a, KS12]. Lindell [Full10]. Line
[FFL12, YMWS11]. Linear
[BCL+13, BW12, CGCS12, CMA14, EKP+13, FGMP12, LGLL12, LJ15, LJ16, LFW+16, WGF16, YCL17, BBEPT14, Bul10a, FES10, GMOGCC15, Her10, HCCC11, LWKI11, ÖSI11, SA14, XSWC10]. Linear/Linear [EKP+13]. Linearly
[ADD10]. Linguistic
[OO18, OO10, OTO18]. linguists [Maf16].
link [Ham12, VS11]. link-state [Ham12].
Linkable [YLA+13]. linked [JCHS16].
linking [NPH+14]. Links [PRGBSAC19].
Linux [Fel13]. Lipreading [OS12].
LISISAP [VS11]. List [AEEH15].
Listening [Lan17]. live [ZZCJ14]. live-wire
[ZZCJ14]. Liveness [OS12]. Lives
[Acz11, Mck12]. LLL [NV10]. Load
[AN12, FXP12, PRN+19]. Loc
[CDPLCA16]. Loc/ID [CDPLCA16]. Local
[pNyWyY+14, TMKI11, VGA15, WYW+13, LMJC11, LWW+10, PTK14]. Locality
[Kaw15, NCCG13]. Localization
[SRAA17, GAI+18, NC13, SCY15]. Locally
[Yek10]. locating [ZYL+10]. Location
[Kim11, PSD15, PAK15, WPZM16, CHX13, Har14, NZL+15, PC14, YXA+18].
Location-based [Kim11, CHX13, NZL+15].
Location-dependent [PKA15].
Location-Privacy [PSD15]. Locations
[KD12a, Alp18]. locator [MJS13]. loci
[FES10]. Locking
[AB15, FHS13, LCW+16, LHA+16]. Loève
[BCPV11]. Log [YKK18, PGLL10].
Log-polar [YKK18, PGLL10]. Logarithm
[BGJT14, CLL16, VM14, AMORH13, BGJT13, MM13, Mes15, TPL16]. LogCA
[AW15, AW17]. Logging
[YNR12a, YNR12b]. Logic [Che18, Cil11, DGP10, Hei17, RZZ+15, Ter11]. logical
long [CFVP16, BF12]. long-term
[CFVP16]. look [AY14a]. look-up [AY14a].
Looks [ERLM16, KTA12, Sch16]. lookup
[LDDAM12]. lookup-table [LDDAM12].
Loop [JS16, DWZ12]. losing [SLZ12]. Loss
[DK16b, JTW+16, DMV15]. Lossless
MACHINES [Das12, LZC+12], GJ13, TTT10, WLT13].
Lossy [BKPV12, CCL+19, CW12a, DN12, AS04, CQX18].
Lost [WB1A7, love
[Fag17, FHM+12, Lovers [Keb15, Mac14]].
Low [ABC+17, AWSS17, Bai10, BCO13, BCG+12, CMLS15, DJL+12, FHS13, GST13, GL12, LJK17, LBR12, Man13, NVM+17, RM18, RS17, SAJL16, WT10b, ZJ11, CZ14, Chi13a, FQZF18, LGKY10, LKAT12, LEW19, MHV15, NR11, ZPZ+16].
Low-Bandwidth [GST13, NR11].
Low-Bit-Rate [LJK17].
Low-complexity [DJL+12].
Low-Cost [ABC+17, GI12, Man13, NVM+17, LEW19].
Low-Distortion [FHS13].
Low-end [Chi13a].
Low-Latency [BCG+12b].
Low-Overhead [AWSS17].
Low-Power [SAJL16, WT10b].
Low-resource [FQZF18, MHV15, ZPZ+16].
Lower [LJ15, Sh1a].
LP [2031 [LK14]].
LPM
[LD13, PJ18].
LPSNR [LP12].
LR [YZ12, ZWM14].
LR-UESDE [YZ12].
LSB [DA10, Tan12a].
LTE [CLM+12, DLK+16, LLLS13, QMW17, SG16, TM12].
Lucas [RW12].
Lucia [DDS12, Dan12].
Lucky [AP13].
Lumpur [HWG10].
Luo [RSD19].
LUT [HF14b].
Luther [ABJ13].
LWE [BV11, XY18].
LWT [TB18].
Lyra2 [ASBdS16].
LZSS [CFY+10].

MA [Orm16, HvS12].
M-Identity [HvS12].
MAC
[Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN13].
MacGuffin [LGL+12].
Machine
[AGHP14, Ano16c, CHS15, Sch12a, ABBD13, GJ13, Gup15, LLZ+16, LHA+16, QMC17, RT10, TTL10, War11, WS14].
Machine-generated [AGHP14].
machine-to-machine [QMC17].
Machines [Ber16a, HB17, BBDL+17, KSU13, PW10].
Macrakis [Keb15].
MacWilliams [ÖS11].
Made [Orm16, Sma16].
magic [PHN+12].
Magnetic [VDB+16].
Magnifying [DKL+16].
mail [BTW15].
Main
[AMH+16, LY15, ZHZ+19, CS11].
Maintaining [WP15].
Make [Ayu12].
makes [Ken11].
Making
[BG14, dCCSB+16, Gel13, LA10, ZDW+16].
Malaysia [HWG10].
Malicious [AAE+14, BL15, TM18, VGA15, BK12b, WTT12].
malleability [KT12].
Malleable
[CKLM13, DPW18, MSas12, CG14a, FMNV14, LP11, MSas13, OOR+14, Pas13a].
Mallory [FHM+12].
Malware
[ATS15, GAF+15, JC13, Goo12].
man
[And13, Bat10, Kap13, Mool14].
Management
[ASM12, ABB19, BD15, Bar16, BS13b, CCMF12, CSL+14, GOPB12, KP12, KKA14, Lop15b, MKF+16, PN10, TMGP13, Vle12, YZX+12, YSS14, ZJ11, ZTSR12, BMBS10, BBB16b, CFL13, Cha13c, dCCSM+12, dCCSB+16, Din10, KH18, MLMSMG12, MGP10, PLCGS11, Sch11, SR10, SA15, SWW+16, WSC14, WDKV19, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b].
Manager
[KKA15, Kim16].
Managing [MD15, BC18].
MANET [KTU116].
MANETs [Yan14].
Manhattan [SS10c].
manipulation [OF12].
Mansour
[DKS12, LPS12].
Manual
[Sac14].
Manuscript [Ano16d].
Many
[CCL+19, LB13, HRS13, ZQWZ10].
Many-Core
[LB13].
many-to-one [ZQWZ10].
Map [XYXYX11, ISC+16, LZY+16, LWK+16, FC14, SE18, ZT14].
map-based [LWK+18].
Maple [G+13].
Mapping [CBL13, MS17, MM14a].
Mappings [MC11, CDPLCA16].
MapReduce [LLJ12].
Maps
[Ye14, BAAS13, KLW+16, LW10].
March
[Ano10, Cra12, DDS12, Dan12, Din12b, IEE11a, Pie10, Sah13, WZM12a].
Marche
[CCMF12].
Margaret [Led16, Sch15a].
Marian [Kap13].
market [YWK10b].
marking [PJ18].
Markov [CR12, FVK17].
Marotto [SE18].
Marshall [Don14].
XNG+14, XNRG15, YYO15, AGLW16, AIA+18, BLL+19, CSS+13, Dra16, FVK17, KHHH14, LLC10, LT13, LT14b, LPZJ15, MO14, PWW10, SI12, WT13, YWT+12.

**Methodology** [CBL13, ZZKA17]. Methods [BKBK14, Kob10, LW12, KSB+17, KVvE18, OO10, TMK11, TPKT12]. Metric [YGFL15, DMWS12]. Metrics [CVM14, BC18].


Mitigating [EPAG16, HRS16]. Mitigation [BRs17, LGR14, DJL+12]. mixTLS [BFK16]. MitM [TY16b]. mix [WJT10]. mix-networks [WGT10]. Mixed [ST16]. mMTC [CML+18]. Mo [RBS+17]. Mobile [BCD+12, FD11, GPT12, GdM16, Hs12, HLL15, 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, CCSV11, CT13, uHAN+18, FHH10a, FA14b, FHZW18, GM16, GH16, HZWW17, HZW18, HL14, IB11, KMK11, KKA14, KKM+13, KKM+14, KKG14, KSB+17, LH13, OYHSB14, Par12b, hSZZ15, SSAFE11, SKB+17, SHBC19, TKHK14, WSC14, WT10a, YHHM18, YNX+16, ZLDD14, ZDW+16, ZC12, MFB+13, SSL10].

**mobile-cloud** [KKM+13]. mobiles [GCSAddP11]. Mobility [CLH13, LNK+18, CL11, GH16, LH11a, MYYR13, YLS12, ZK11]. Mode [HZ11, Mar10c, PAF18, gWpNyY+14, WLC12, ZHZ+19, Fay16]. Model [AW15, AW17, App13, CT18, CLP13a, CBJX19, GLG12, GJO+13, GJJ15, GJJ17, HZX15, IA15, JH+19, Kar12, KP17, LHM+15, LZC+12b, MVVR12, PYM+15, PNRC17, RSD19, SLS14, SPM+13, TBCB15, WWC+11, WWH12, XYZ+12, Yon12, ZHL15, BL11, CK11, CDPLCA16, DF+17, HKT11, HT17, KSV13, LZT12, LCY+16, L16b, MGP10, Mat17, MM13, NB13, WYL13, WZM12a, WZM12b, YC12, ZCL+19, TLC15]. Model-based [IA15].

**Model-Predictive** [TBCB15]. Modeling [CJFH14, GBNM11, LTKP16, MN13, PAS13b, Ana14, CDGC12, MHY+18]. Model-Predictive [TBCB15]. Modeling [CJFH14, GBNM11, LTKP16, MN13, PAS13b, Ana14, CDGC12, MHY+18].


multi-hop [LCT+14]. Multi-instance [BRT12]. Multi-Key (CRW14, XWSW16, OSSK16, GZS+18, LXK+14].


multi-stage [ZC13b]. Multi-User [MZY15, OKG+12].

multibit [KPS10]. Multicast [CC14, BAL10, HGWW11, LTT10, NAACL12].

Multicoupon [HIDFGPC15]. Multidevice [DPCM16]. Multidimensional [AJA16].

Multidimensional [Her10, WWBC14, HMMC12]. Multifactor [MYY12]. Multigigabit [PP10b].

multihop [ADF12]. Multilayer [NXH+17].


MultiObjective [ZAC17]. Multipartite [HR13]. Multiparty [BDOZ11, CCL+13, Fri10b, ADMM16, BHH19, LDAM12].

Multipath [LH12]. Multiple [DSB15, Duni12a, FR16, KBL11, LTC+15b, LQD+16, NDC+13, SY14, SC10, SKS+18, Sta12, WWL+14, XNP+18, 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, LNL+19, SK12b, YTS12, AAT16, SKH15, SF12].
Multicative [RMERM19, KHHH14].
Multipliers [ARM15].
multireceiver [FHH10b].
multisecret [FGMP12].
multispectral [DCM18].
multistream [WXL+17].
multitone [GL10].
Multivariate [CLND19, DP17, ST16, YL17, YDH+15].
multiwatermarking [WL12].
multiwavelet [PWW10]. Munich [Wat10].
Music [NTKG17, Wes16]. musical [Ana14].
Mutt [Ran14].
Mutual [CJP12, GI12, GM14, Kim16, SBS+12, WT10b, AATM18, BDM18, CJ13, CLH13, CL11, FHH10a, Far14, GPLZ13, GH16, HDPC13, IB11, JKAU19, KLW+16, LIK+17, MMP19, SPP12, TG17, XMHD13].
MVP [CD12]. mvSERS [HKL15]. My [GPT14, CMG+18].
Naive [ZLW+17]. Name [YCM+13].
Named [LLZ+17]. Names [ABJ13, MPJ+16].
National [Fid18, ABJ13].
Natural [ZCWS15]. nature [KL13].
Naval [Don14]. Navy [Maf16].
Neighboring [LSQ11b, LC15]. Neighbors [XLP+18].
Network [Ano10, Bis17, CWL16, CJ13, CLH13, DRS16, Hay13, HDWH12, HS18, Kim15, KCC17, LH12, LLLL15, LY16, LTW11, MJGS12, NNAM10, NRZQ15, SGC16, She14, TLW12, VFP17, VFV17, VGA15, VKC15, WP15, YZLC12, YSLJ14, AKM+11, AL15, Ano11a, AZF+12, CIXX19, CL11, DLK+16, FPG14, HGWI10, HB13, HKB14, JZS+10, KP18, LHL11a, LKKL13, MZA+13, MJS13, NDRN13, OF11, PL16, RCW15, Ser12, SCKH10, SKS+18, Sta11a, Tan15b, WLY13, WS14, YLS12, ZOZ17, Ste15b].
Network-Assisted [KCC17]. network-based [YLS12]. Network-Coded [She14].
Network-on-Chip [Bis17]. Networking [KYEV+18, LCK11, LLZ+17, ZHL15, Kim11, LCM+17]. Networks [ABCL17, ABC+17, BN14, BPSD17, BFMT16, CS14, CSH+18, DS11, DF16, FMS12b, GMV17, HZC+12, HBCC13, HK14, KH10, LLCL11, L15, LHM+15, LZCK14, LWCJ14, LZ+12, MPM+17, NSA15, NYY+14, O0O12, OKS+12, PYM+15, PC14, RWLL14, SWYP12, She14, SP15b, Smi11b, SLI11, SZZT18, TCN+17, WLY+15, WLY+15, XHC+12, YM16, ZC13, ZW15, Zha15b, ZLDD12, ZSA12, Aia15, ASO14, APK+18, AIB+16, AKC18, AD12, BD11, BLAN+16, BB16b, CDGC12, CLM+12, CML+18, CLSW12, CL11, DCS12, DK12, DNN13, EEAZ13, FA14b, FMA+18, GH16, HGWW11, HZC+14, HZWW17, HCCC11, HCM11, HTC+10, HY18, JNUH17, JLT+12, JW16, KM10b, K1C10, KO16, KLW+16, KDW+17, LLLS13, LC17, LMC11, LJX14, LIK+17, LKN+18b, MSM+18b, QMW17, RHP12, SGCC+16, SA12, SG+18, SZMK13, SZZT15, SKK10, TODQ18, TKHK14, WGJT10, Wan13, WW14, WX+17, XW13, XWDN12, XHCH14, XMHD13, YHS16, ZWQ+11].
networks [ZBR11, ZC16, ZT16, ZLDD14, ZHH+17, Z11, LNK+18a].
Neural [CSH+18, SKS+18, YZLC12, EEAZ13].
Neuroscience [BSR+14, JW14].
Newman [And13]. News [Edw14, Edw17, Sav13a, Sav15, Sav16].
Next [MR14a, MJGS12, Aia15, ACD+15]. Next-Generation [MR14a]. NFC [LY14, Mic16]. NFSR [WGD18].
Niederreiter [HC17, MV12]. Nievergelt [Ter11]. Nine [Mac12, LYHH14].
NIZK [Pas13a]. NIZKCTF [MBC+18].
NIZKs [CKLM13]. NN [ZHT16]. No [WDDW12, Wu16, KHHH14, MPJ+16].
nobody [Sto12]. Node [NYR+14, OKG+12, LC17, PX13, SAAB10].
Node-Capture [NYR+14]. Nodes [VGA15, ZYL+10]. Noise [ASN11, YMA17, ZHH+17]. Noised [JLS12].
Noisy [ASN12, HZW+14]. Non [AS17, AMH+16, BCF+13, CG14a, CPS16, DJL+12, DPW18, EKP+13, FHKP17, FMNV14, GZX19, HKB14, KTT12, LLG15, MFH13, MSas12, OOR+14, Pas13a, QJC+18, RM18, RMG18, Svo14, SM18, WgMW12, YNQ15, YKKL12, ZLDD12, Ay14a, BS15, CS11, ESR14, GIJ+12, Kre13, Lan11, LP11, MSas13, SES+16, SXL16, XSWC10, Yan14]. non-adjacent [Kre13]. non-associative [BS15]. Non-Black-Box [CPS16].
Non-blind [HKB14, RMG18].
Non-contextual [Svo14].
non-cryptographic [AY14a, ESR14].
non-dynamic [SES+16]. Non-interactive [BCI+13, Pas13a, Yan14]. Non-intrusive [MFH13]. non-iterative [SXL16].
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-transferable [GZX19].
Non-uniform [QJC+18]. Non-uniformly [YKKL12]. Non-Volatile [AMH+16, RM18, SM18, YNQ15, CS11].
NonInteractive [KOS16, GOS12, MBC+18]. Nonlinear [CCM+15, KW14, LW13a, Lüd12].
Nonvolatile [ZHF+19]. Norm [FHS13].
Normal [RMERM19, TY16a].
Normalization [KLX+12, SJ12].
Normalized [YGFL15]. Norman [Low12].
Note [HYS11, Gal13, Hwa11, Lim11]. nothing [Cer15].
Notions [KFSO12, SNJ11, Sar12, BP11].
Novel [CLHC12, DCM18, KRH13, LLG15, LyWZZ12, LH11b, MJGS12, MCS+15, SWM+10, SC12, VN16, WHZ12, WZXL12, YZX+12, Yb16, ZMM17, BCR13, CH10, DDF13, GPLZ13, HCC11, JXZL15, LXCM11, LMJC11, LH13, LW+10, ML+13, MRT10, NZL+15, PZBF18, SYW17, Sun16, TG17, J12b, WYL13, WZG+12, YWT+12, ZBR11].
November [Kap11, LCK11, Yan11].
NSA [ABJ13, Ano13b, AHS13, Bu16, Men13b, Sta13, Toy14].
NSDG [SPC12].
NTOW [BS15]. NTRUEncrypt [DW18, KY10].
NTURSign [Wan10]. NTT [MCD12].
NTT-Based [MCD12]. Nuclear [Hel17].
Number [AD11, BKLS12, CDK+10, DLS18, Fok12, Ham17, KA18, LTKP16, LCLW17, MFG16, NIS12, NNAM10, Sha10, SRAA17, SRK+17, WJ19, CFY+10, CP13, LLP+18, LGKY10, Lim11, MS12a, MRT10, SH11, Sli11, XSWC10].
Numbering [MNS11]. Numbers [BCGH11, CK18, FM15, Sh10, AZH11, Ana14, GCH15, SMD11, ZOC10].
numerical [GKCK11]. Numerical [CML16].
Numerology [GG11]. NVMM [CS11].
O [CDD13]. Obfuscated
Order [DCA18, KS12, LFX+18, LWKP12, PRC12, YKKL12, ZDL12, ZSW+12, ZBF18, AKY13, LW13a, LCY+16, LWKP14, gWpNyY+14, YL11].

Order-Hiding [DCA18].

Order-Preserving [KS12, YL11].

organisational [Smi15a].

Organization [RSGG15].

Orientated [TJZF12].

Oriented [NNAM10, Rog16, RSGG15, WW12, WZM12a, WZM12b].

Origins [SJZG19].

Orthogonal [tWmC12, XNP+18].

Oscillator [YKBS10].

OSN [BCF16].

OSNs [SZZT18, PZPS15].

other [Smi15b].

OTS [Hül13].

Outliers [Sch12b].

Outlive [Hur16].

Output [DK16b, GST12, NR12, PBCC14].

Outright [ABJ13].

Outsourceable [QZZ18].

Outsourced [FRS+16, LLC+15, LHL+18, LQD+16, PD14, RDZ+16, XLP+18, YMA17, YMC+17, DFJ+10, FS18, HMCK12, LCL+15, LCY+16, LJW+17, QZDJ16, ZML17, ZSW+18b].

Outsourcing [DR12, LJLC12, LHL+14, LJWY18, SKB+17, SWW+16].

Outwitted [Car11, Fag17].

Over-the-Air [VOGB18, ZXW+18].

Overcoming [BKKV10, DY13].

Overhead [AWS17, Bai10, CCW+10, GHS12, RM18, ZJ11, RS17].

Overlay [CHS15, MJS13].

Overview [Bla16].

owners [Zha15a].

Outsiders [GZS+18].

Ownership [FMTR12, RR11, HWYW14, KH18].

Oxford [Che11, Wes16].

Ozarow [ADG16].

Pairing-Based

[Bon12, CST+17, KZG10, LGPRH14, Men13a, MST18, YTS12, BP18, Con12, KSH18].

pairing-free [LL16a, YT11b].

pairing-friendly [BP18].

Pairings [ASS15, Hof15, IL15, LT14a, HWB12, QYWX16, RS15, UK18].

Part [MCP15].

Pairwise [DL12, YM16].

Pan [Kat13].

Palm [IEE11b].

Pan-European [GKB12].

Panaea [Hor19].

Paper [TSH17, Ano16a, SK14, YFK+12].

Papers [Ano16a, Ano16b, Ano16h, LW13a, XW13, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11].

Paradigm [ABGR13, BS12, Mau12, MP12, TAP19, WQZ+13].

Parallel [App14, ARM15, CBM15, CGB10, GP17, LY16, LB13, MCDB12, MC11, NDMMW16, SMDS11, YE12, CSTR16, MRT10, RG10, RWZ13, WWYZ11].

Parameters [HRB13, MBF18], parametric [Bull10a].

Paranoia [Cor14a].

Part [Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, MCk12, Pnn11, Smi11a, Smi15b, Smi15a, Bai12].

Part [BLM18, VM14, BD15, Bar16].

Pass [CBJX19, DLV16, GFBF12, LG12, SGS14, TK19, WDDW12, Bax14].

Partitioned [KSU13, WTT12].

participating [CH10].

participle [ZSM18].

Parties [YCR16, Küp13].

Partitioned [FVS17].

Partitioning [ADR18, AP11].

Party [Ash14, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, OSH16, QZL+16b, TMY+17, ZMI6, ED19, FIO15, GVW12, HPC12, HWB12, LyWSZ10, LML+13, Tso13, TKHK14, XLWZ16, XCL13, YC12, YZZ+14, ZZ15, GHKL11].

Passau [GLIC10].

PASSERINE [Saa12a].

Passion [Hof15].

Passport [LZJX10].

Password [ASBdS16, BRT12, CYL14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b].
Password-Authenticated
[HS, YRT+16, ZXH16, IWS10, WZM12a, WZM12b]. Password-Based
Precomputation [GKM16]. Predicate [KHPP16, NMS14, YKNS12, ZYT13, FH13, HFT16].
Predictability [DK16b]. prediction [CSS+13]. Predictive [TBCB15].
[ABCL17, BJL16, BHKN13, BJL12, CWL+14, CRE+12, GZZ+13, HSMY12, HLLC11, HXC+11, HHMK14, HK18, KS12, LMGC17, LNXY15, LQD+16, MTM18, NMS14, OFMR16, PR12, PD14, PSS+13, PRPT12, Pet12, RHV+16, RSR+19, RBHP15, SZDL14, SZQ+17, SZTZ18, WPZM16, WZCC18, YKKL12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, AIB+16, ALL+18, BLV17, FH13, FMA+18, GH16, GAI+18, GA11, HSH11, IC17, IOV+18, JKL+16, KH18, LHL+18, LW13a, LCY+16, PZBF18, SYY+17, Tan12b, TSH14, WLZ+16, YMM13, YNX+16, YL11, ZWY+13, ZOSZ17]. Press
[Ano15b, Ano17b]. Press/Elsevier
[Ano15b]. Prevent
[HLAZ15, PYM+13, JSK+16]. Preventing
[DCAT12, SKEG14, WS12]. Prevention
[CWL16, VS11]. Primality [Coup12].
PRIME [ACK+10, GM13]. Primitive
[App15, MCS+15]. Primitives
[BS15, EAA12, HLN+10, SP15b, ABDP15, BSR+14, Gor10]. PRINCE [BCG+12b].
Princeton [Ano17b]. Principal [BKL18].
Principle [KYE14, WW14]. Principles
[DK15, FSK10, Fri10a, Sta11a]. print
[KPS10, PKS18]. print-cam [PKS18].
print-scan [PKS10]. Printer
[EMW14, FNP+15]. Prior [NA10a].
Priority [LMS16, Bia12]. Prisoners
[Mac14, Keb15]. Privacy
[AKM+11, AKKY17, ABCL17, ALL+18, ACM12, ABHC+16, BN14, BCF16, BA18, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DTE17, ESS15, FGR+17, Fei19, GZZ+13, HSMY12, HBC13, HXC+11, HK18, JM12, KM10b, KCC17, KS12, KH18, LMGC17, LSBN14, LLG15, LNXY15, LQD+16, MYR13, MTM18, NMS14, PD14, PSS+13, PRPT12, PZPS15, PS15, Pet12, RHV+16, RSR+19, RCP+18, RWLL14, RBHP15, SS17, Set16, SZDL14, SZZT18, SOF12, TMLS12, TMGP13, WPZM16, WZCC18, WMY16, YMM13, Yon11, ZHW+16, ZM16, ZOSZ17, ZHW15, ZLDC15, ZTL15, ACK+10, BAG12, CDF+10, DZ+12, FH13, FMA+18, GAI+18, HSH11, IC17, IOV+18, JKL+16, Kan16, KKGK10, KM14, LHL+18, MZA+13, MGP10, PX13, PZBF18, Sav16, Sch11, SLZ12, SY+17, SCY15, SWW+17, Tan12b, WLZ+16, WWW17, WS13, YYS+16, YX+18, YQOL17, YNX+16].
privacy [ZY+13]. Privacy-assured
[WMY16]. Privacy-Aware
[BCF16, MGP10]. Privacy-Based [BS13b].
Privacy-Enhanced
[DTE17, ACK+10, YQOL17].
Privacy-Friendly [KCC17, ACM12].
Privacy-Preservation [LW15].
privacy-preserved [SWW+17].
Privacy-Preserving
[ABCL17, BJL16, BJL12, CWL+14, GZZ+13, HSMY12, LMGC17, LNXY15, LQD+16, MTM18, NMS14, PD14, PRPT12, Pet12, RHV+16, RSR+19, RBHP15, SZDL14, SZZT18, WPZM16, WZCC18, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, ACK+11, AKKY17, ALL+18, KH18, ZOSZ17, BLV17, FMA+18, GAI+18, HSH11, LHL+18, PZBF18, SY+17, Tan12b, ZWY+13]. Privates
[BKL18, GM13, Jia14a, LQSX19, MV19, QZL+16b, Sia12, WCL+18, Yek10, ZMW16, ZXYL16, BHH19, HJM+11.
HYF18, IK15, WR15. **Private-Key [MV19].** private-keys [IK15]. Privilege [Cha13c, QRW+18]. Privileged [Din10, WDZL13]. **PRNG [DK16b].**

Probabilistic [BFG+14, Rao10, WP17, Ksu13].


**Problems** [Dun12a, Fra15, Gtt11, Krdh13, KPC+11, RBS+17, SK14, TPL16, WS14]. **Procedure [CS14, OS12].** Proceedings [Lck11, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Dun12b, FBM12, G110, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, Ltw11, Pie10, PJ12, Rab10, Sen10, Yan10, Van11, AB10a, BL10, GLIC10, IEE11a, Kia11, Lin14b, Sah13].

**Processing** [Sak16, TkMz13, VKP17, BKV13, Hwk+15, Ms13b, PRZB12, WS14].

**Processor** [BH15, CLF+17, Hkl+14, LB13, Mbr15, Ys15, ABDP15, BAb+13, BGG+13, Ksh18, SSPl+13, Tar10].

Processors [GfBf12, Guc16, RYF+13]. **Product [Adm12, Ccm15, Ot12, Ykns12, Cha13b, Ddm17].**

**Products** [LMG*18, Rs10]. Professional [Stc11].

**Profiles** [Bcf16]. **Profiling** [DP12]. Profit [AppVp15]. Program [MZ17b, Wa18, CLZ+17, GGH+16b, Mfh13].

**Programmable** [CLF+17]. Programming [Bee17, BcM15, SY14, Asve13, Hlv10].

**Programs** [Bgi+10, Bgi12, Cl16].

Progress [Ab10a, Bl10, Bc11, Gg10].

Progressive [Sa16a]. **Prohibition** [Hor19].

Project [SpG+19, Ack+10, Ss10c, Wi18].


**Proof** [BdSg+13, Bla12, CzLc12a, CzLc14, Fsx12c, Kuz11, Lw12, Nly15, Sr14, Ste15a, Zzm17, Mon13, PptT15, Whj17].

Proofs [BGk12, Bcgk12, BgB12, Bci+13, BdSg+13, Czlc12b, IW14, Lnz+13, Mau12, Nty12, Sav13b, Wpzm16, Aghp14, Kpp16, Kkn+16, Ll10].

**Propagate** [Gwm16]. Propagation [SkS+18, Wwc+11, Yzc12].

Properties [CcK12, CcK16, DqF12, Fy11, Js18, Jr13, Ku12, Sch12c, ClcZ10, Wt13].

Property [Hec+12, Pr12, Rja12].

**Proportions** [Ber12]. Propose [BftM16]. proposed [Bax14]. Protect [Ctc+15, Ymc+17, Bvib12, Cdf+10, Dccsm+12].

Protected [BdGh15, Sg15]. Protecting [Bcp14a, Gsf16, LpY19, Mar10b, Rcp+18, Scy15, Wat14b, Atkh+17, Cda14].

**Protection** [Cdd13, Gst12, Lop12, NaAuH16, Ndg+17, Rr11, Sey14, Sj12, Ati+10, Hlys14, Kkm+13, Lvy10, Rs17, Tll13, Ywt+12].

**protection-key** [Hlys14]. Protocol [Bl12, Bc14, Cbm+15, Bsv12, Bfk16, Cc14, Ccm17, Flh13, Fmtr12, Fra16, G112, HvS12, Hc12, Hl10a, HcPlsB12, Hcetp1+12, Hkl+12, Jtz+16, Jhw+19, Kmo14, Lnz13, Lccj13, Lnxy15, Mbc15, Mr10, Sss13, Sbs12, Sgc16, Tyk+12, Wt10b, Xjr+17, Ys12, YfW18, Ywz+12, Xzz+11, Aatm18, Akg13, Aib+16, Akc18, An15, Bdm18, BgAd12, Csd18, Ccss11, Cjp15, Dlk+16, Ea12, Fa14b, Fio15, Gmsw14, Glm+11, Hpc12, Hwb12, Hl14, Ic17, Iov+18, Jkl+16, Jxlz15, KIm11, Ko16, Llls13, LdDm12, Lkkl13, Lws10, LxMw12, Lw19, Ly14, Lml13, Ncl13, Nlyz12, Ohj10, Par12b, SphLcb14, Sb17, Sgj18, Sww+16, Sss11, Sssl+13, Tg17, Ts013, Tkkh14, Vs11, Wcfw18, Wzm12a, Wzm12b, Wls14, Wmyr16, Wt10a, Wtt12, WcCh18, Xcl13, Xhm14, Yc12, Yzz+14, Ymm13, Zqw+11, Ztz16, Zyc+17.
[Stel15b]. Protocols
[AP13, ABHC+16, BMP12, CCK12, CCK16, CCF17, CCD15, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KO516, LY16, MV19, MS16, MT12, Myr16, NYR+14, NSMS14, PS14, SBS+12, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13b, ACM12, CML+18, CR10, CLCZ10, DJG14, FTV+10, GBNN11, GLR13, HSH11, Ham12, HDP13, HZWW17, HST14, KJN+16, KSU13, KKK+16, LKIL13, MN10, NR11, Nos11, Nos14, SD10, YSL+10].

Prototyping [KPC+16]. Provable
[BKLS12, CC14, EKB+16, Rog16, YMSH10, ZX11, ZPXX17, FA14a, HRS13, LHH11, WB12, XCL13]. Provably [BCGAM12, BCL12, BCM13, BJHP14, FHH10a, GL+18, IL15, LH11a, LL16b, PSM17, WMS+12, XJWW13, YC12, YZZ+14, ZG10, ABBD13, FIO15, SXL16, WXX14]. prove [DGJ14]. provenance [CDL18, ZOSZ17].

Produce [Ano15a]. Provided [KS12].

Provider [Sch15a]. provider [DFJ+17]. providers [AKK+17, BK12b, YWK10b].

Providing [DLN13, HTZ12, KS18, MLM16]. Proving [Sar14, AGH+17]. Proximity [IW14, Alp18].

Proxy
[ASS15, GSW+16, GJG15, GJJ17, GZGA19, HGWY11, HZX15, KP12, LSLW15, LAL+15, LSC12, MLO17, MBC13, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW+16, YMWS11, YMC+13, BGP+17, CLH+16, FSWG11, FSWG12, GH12, HWD16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, LL16b, QMW17, SL12, SKB+17, Tia15, WHY+12, Wan18, WLS14, XWXC14, YZCT17, ZLY10, ZDW+16].

Proxy-invisible [SYL13]. Ps [HDH12].

Pseudo
[NN12, XYXYX11, CFY+10, KM10a, MG15, PLSvdLE10, SH11, SM11, XSWC10, Zim10].

Pseudo-Random
[XYXYX11, CFY+10, KM10a, MG15, PLSvdLE10, SH11, SM11, XSWC10].

Pseudonym [XHM14]. Pseudonymous [DBF+12]. Pseudoprime [DW12].

Pseudorandom [AS17, BCGH11, BK12a, Kla10, MFG16, CP13, GCH15, HRV10].

Pseudorandomness [Sha10]. PSMPA [ZDC15]. PSO [TLL13]. PSPACE [JJU10]. Public
[An11b, ABW10, BVS+13, BB14, BKLS12, BKVK10, CT18, CLP13a, CHe5, CLND19, CNT12, Con12, FBM12, GKS17, HTC+15, HLLH19, IM14, JLT+12, KFOS12, LLSW16, LP+10, LS18, LZ14, LKH18, MZY15, MPP14, MTY11, Mat14, MPRS12, Mu16, NTY12, Orm16, PDN15, RSBG12, RW12, RBHP15, SGG18, Saa12a, Sch19, SK12b, SWM+10, Sia12, SC12, SLY+16, SGP+17, SVT10, TMC15, TTT12, WP17, WJ15, WWH12, Wi18, XNKG15, XXZ12, Xio12, XJWW13, YL17, YKC+11, YFK+12, YMC+17, ZY17a, AA14, ATK+17, BS15, BSW12, Dur15, HZWW17, HL14, HTCC17, LSNB14, LLY15, LFWS15, LH13, LL16a, RPSL10, SES+16, SY15b, VN17, YTT11b, YYS+16, ZN11, ZCC15, ZCL+19, ZY17b].

Publication [ZL15]. Publicly
[NMP+13, SQZ+17, YNR12a]. Publish
[BGP+17, DLZ+16b, OFMR16, PRSV17, SLH11, TKR14, YSM14].

Publish/Subscribe [DLZ+16b, OFMR16, PRSV17, TKR14, YSM14]. published [MY13]. Publisher [Ful10, Mur10].

Publishing [VS15, LLL+17b]. Pueba
[AB10a]. PUF [BDM18, CCK16, CCM17,
DSB16, KPKS12, KLM+12, MVV12, SRK+17, VDB+16. PUF-Based
[CCM17, KPKS12, MVV12, BDM18]. Pufferfish [KM14]. PUFKY [MVV12].
PUFs [HRK18, IGR+16, USH19]. pulse [MRRT17]. pulse-response [MRRT17].
punctured [MG15]. puppet [Lac15].
Purpose
[GSB12, Gue16, ABDP15, DGJN14, KM11]. purposes [ABB+14]. push [Wu17].
Pushdown [CCD15]. Pushing [FHV16].
Puzzle
[IBM13a]. Puzzles [RSBN12, dCCSM+12, dCCSB+16].
Py [DGlS12]. Py-Family [DGlS12]. pyramid [MHT+13].
Q&A [AHN+18, Hof15, Hof16]. Q3 [Ven14].
Qaeda [Mac14, Keb15]. QC [JY14, HC17, VOG15]. QC-MDPC [HC17].
QIM [LJ17]. QIP [JW10]. QS [AZPC14, HDW12]. Quadratic
[MRRT17]. Quadraticity [MS12b]. Quality [CSW12, NN12, YCM+13, SS11, WZLW13, WKH11]. Quantitative
[BL15, MLBL12, MV16b, HM10].
Quantization [SSA13].
Quantization-Based [SSA13]. Quantum
[Ano15d, Ano16c, Ano17d, Ano17e, BB14, Ber14, BCF+14, Che17, CCL+13, Feh10, FKS+13, Fol16, JAE+15, JL18, Kar12, KP10, LLIK17, MLA+17, MS16, MSU13, MS16, MKAA17, NNA10, NA10b, QCX18, RK11, RSM15, RS18, Sas18, Sl11, TM12, Unr15, WL18+17, WZS+19, ABB+14, BJ16, CML16, Edw17, FRT13, GJMP15, IM14, JSK+16, KKK+16, LLP+18, LyWSZ10, LCW+16, Lüdl12, QD16, SK14, Svo14, VV19, YDH+15, vDKS11, Sen10, Yan11].
Quantum-Oblivious-Key-Transfer-Based [WCL+18]. Quasi
[BDK11]. Quasichirp [OWHS12]. Quasi-Cyclic
[OTD10]. Quasi-Polynomial
[BDK11]. Quaternion
[YWNW15, yWpWyYpN13]. Queries
[HL12, LHKR10, PBC+17, ZZQ+19, BKV13, CHX13, DFJ+17, HMK12, PRZB12, TKMZ13, WL19]. Query
[DA18, GA11, PCDB14, WCL+18, XLP+18, AZPC14, BS13a, CH11, ED17, HKW+15, JCHS16, LXX+14, LW13a, YQOL17, ZHT16]. Query-preserving
[GA11]. Quest [Fox13]. question [Ch13b].
Quisquater [Nac12]. Quorum [Kar12].
R [BS12, LV11, PP10b, WY14].
R3579X [BDK11]. Rabbit [FSW11].
Rabin [Chi13a]. Radial
[pNyWY+14, CG12b]. Radio
[KAHKB17, CJP12, CJP15, EA12, Kin11, NLYN12, RGN12]. radio-frequency
[CJP12, CJP15]. radix [GCK11].
RAGuard [ZHS+19]. Rail [HF14b].
Raising [YW10]. RAKAPOSI
[IO12]. RAM [RYF+13]. Ramamujan
[KK10]. Ramifications [ALR13]. Random
[Ana14, CBJX19, CDK+10, DSLB18, EAA+16, FZH14, FSX12a, GSW+16, Gre17, KS15, LTKP16, LPL15, NIS12, NN10, NN12, SRK+17, TM18, WS12, XYXYX11, XQL11, YM16, YS12, YKC+11, YFK+12, YLA+13, ZMY18, Ara13, CFY+10, CT11b, GPLZ13, GLM+16, GLW13, HKT11, KM10a, LGKY10, LL15, MRT10, MG15, PLsVL10, RG10, SMD11, SYL13, SH11, SM11, Shy15, St11, WWYY11, XSW10, ZOC10, ZPS+16, Zim10]. Random-Grid
[KS15]. Randomization [Gas13].
Randomized
[ARP12, GT12, HHR11, SR12b, BWA13]. Randomness
[AY14a, Ana14, ABF12, ACM+17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11].
Range
[DA18, HMK12, JCHS16]. Rank
[SS10b, FES10]. Ranked
[WL18+14, XWSW16, GZS+18, LXX+14]. Ranking
[ZDL12, AT10]. Ransomware
[MPA+18]. Rapid [KPC+16]. rare [Sch11].

Re-authentication [LBR12, FXP12, LMJC11]. Re-Encryption [GSW+16, KKA15, LSLW15, MLO17, NAL17, PRSV17, WY10, XJW+16, ABR12, GZXA19, LSC12, Pet12, SY13, SY16, Tia15, WGJT10, WHY+12, Wan18, WLS14, XXX15, YZCT17, ZDW+16, L15].


Reduced-Round [LWZ12, AY14b, LFW+16]. Reduction [ABR12, LCLW17, LSC+15, YMA17]. Reductions [BHKN13, DW12]. Reference [LHLS12, IM14]. Refinement [BCEM15]. Refinements [LL11], reflections [Hai17, OF12]. refractive [PHN+12].


regular-expression [WR15], regulating [DF+10]. regulatory [BP10]. regulatory-compliant [BP10].
Reinforcing [WXY+17]. Rejewski [Kap13].
Rekeying [DT13, QLL17, CLSW12, DS11].
Rekeying-Aware [QLL17]. Related
[CII11, CMA14, DGIS12, HLLG18, Pud12, WLC12, MNP12]. Related-Key
[CMA14, HLLG18, Pud12, WLC12, DGIS12].
Relational [HPC10, RP12, WP17, BFG+14, BL11, GA11, JK13, PYP10]. Relations
[BP11, FHS13, HLR11, WGD18, KGO10, LLM+19]. Release
[KFOS12, RSBN12, Unr15, WSS12].
Relevance [Sim15a]. Reliability [HSUS11, CZ14].
Reliable [AMKA17, ADG16, Bai10, CC14, KMJ18, WKB16, ACD+15, CL16, ZC12].
Relying [TAKS10]. Remanagement [PSJ+13]. Remarks [SSU12].
Remote [BCE+10, CS14, FYMY15, LZCK14, Sar12, SYY+17, VMV15, WgMdZ12, WgMW12, CHS11, HU15, IB11, KKG14, LH10c, LNM+11, LNKL13, LWK+18, LH13, MM12, Sar10a, WQZ+13, YSL+10]. remotely
[Wat14b, YHHM18]. Removing [HKK13].
Renewal [MMY12]. renewed [GPLZ13].
rental [LY14]. Reordering [Alo12]. Repair
[SEK19]. Repairing [BCM12, BCM13].
Repeatedly [TAKS10, ATK11]. Replay
[QL15]. Report [CBP+12]. reports
[RPG12]. Repositories [Ano15a].
repository [RSM15]. Representation
[AGW15, BMJT16, MHT+13].
Representation-Based [AGW15].
Representatives [Bla16]. reproducible
[CW12a]. Repudiation [LLG15].
Repurposing [GY13]. Reputation
[BL15, LHM+15, PAS13b, MGP10].
Reputation-Based [PAS13b]. Request
[KK12, KK13]. Request-Based-Revealing
[KK12, KK13]. Requirements [OS16].
requiring [KHHH14]. ReSC [YFT18].
Rescue [TSH17]. Research
[BA18, CDFZ16, SPG+19, WP15, GLIC10, Hof16, Pal15, Ven14]. Researchers
[Con12, Edw14, Wal18, Win17]. reset
[RY10]. Resettable [CP16]. Resettably
[COP+14]. Resettably-Sound [COP+14].
Resilience [NTY12, GLL+18]. Resiliency
[YM16]. Resilient
[AV12, BKKV10, FPS12, LTZY16, LD13, NYR+14, Pan14, PSL15, XZY+12, YZ12, YNR12b, YCZY12, ZYT13, ZWTM15, ZZM17, ZY17a, ZYM18, ZYH+19, CQX18, DLZ16a, GV14a, KPS10, MMMD13, SGP+17, Wan18, YSJL14, YKC+12, YLZ+16, ZY17b].
Resistance [CGCS12, PRC12, WLZ12, ZJ11, DLMN13, FIO15]. Resistant
[BK12a, CDK+10, GV14b, HF14b, WHZ12, WgMW12, WH17, YPRI17, GMRT+15, HCC10, PBCC14, VCK+12, WTT12, YKGK13]. resisting [SLX16, Tam15].
Resistive [DSB16, TLCF16]. Resource
[CSH+18, HM19, JMG+16, SZMK13, YNR12a, AMHJ10, FQZ18, KAS15, LLZ+16, MHV15, Wan13, XWZW16, ZPZ+16]. Resource-Constrained
[CSH+18, YNR12a, LLZ+16].
Resource-efficient [SZMK13, XWZW16].
Respiratory [RSCX18]. Response
[GHSL14, HLKL15, ZHW+16, MRRT17].
Resprinting [TBCB15]. restoration
[WHZ12]. restricted [CLH+16]. result
[ACK+10, ED17]. Results
[DGIS12, LFJ16, Hof16, KGO10].
Rethinking [Che13, HU15, LSG16, MV16a].
Retrieval [BBB+16a, BTHJ12, CJ12, DS19, HK14, JMG+16, JKHeY12, Yek10, XZX+11, CJ15, SWW+17]. returned
[War11]. reusable [RS17]. Reuse [ABF12].
Reveal [Sta13]. Revealed [Ano15a].
Revealing [BT12, KK12, KK13]. reverse
[TQL+14]. reversed [KYH18].
Reversibility [FSX12a, HWYW14].
Reversible [CLF11, CSS+13, HHS+15, MM17, MR16, NC12, AMK12, CT11a, HLC16, JK13, MM14a, NC13, PWLL13, PC14, TK14, WOLS12]. Reversibly
[MKH+12]. Review
[Ano15b, Ano17b, Ay12, Ay1u, Bao12, Bar12, Cau12, Dew11, Ful10, Gas13, Joh10, Kat13, Kei15, Koi10, Led16, Lop15b, Low12, Me10, Mou15, Mur10, Sha15a, Sha10, Ter11, Xie12, Jas+11, MM12, TPK12].

Reviewed [Sch15a]. Reviews [SR14]. Revised [DDS12, Dan12, MV12, BYL10, JY14, LIh10a, vDKS11]. Revising [BT12].

Revision [LT14b]. Revisited [CLY12, DKS12, FKS12, LL11, Lop15a, PKT12, Sar12, Tan12a, BCL14, HKT11, HYWS11, TS16a, ZCL+12].

Revisiting [RSD19, TLW12, WSA15].

Revocability [WHLH16]. Revocable [AEHS15, CD16, QZZ18, SE14, SE16, SZS14, SZDL14, TCL15, TT12, Unr15, FLL+14, LDZW19, WLF17, WTT12]. Revocation [AEHS15, LLC+15, LW16, Lop15b, RDZ+16, XMCL13, YWZ+12, ATK11, LJWY18].

Revoking [TAKS10]. Revolutionized [Ou16]. RFID [CJP15, AATM18, BL12, BSSV12, BM11, CCGPDMG12, CCIF17, CJP12, Chou14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, GAI+18, HSH11, HDPC13, HQY+16, HCPLS12, HCETPL+12, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLs1d10, QZL+16a, QZL+16b, SBS+12, SPLHCB14, TG17, WH17, WCFW18, YFT18].


Richman [Xie12]. Riddle [Fox13, KM15, KM16]. Right [Bro17, SR12a, BBG+17, LHA+12, Sch11].

Rightful [RR11]. Rights [LRVY10].


Robust [BCGAPM12, BCG12a, CFOR12, GKS17, HZC+12, JSS12, LSL12b, LSR13, MR16, MU12, MS16, MC11, pNYW+14, OCGD11, RR11, RMG18, SJ12, SC12, SZTT18, TLCF16, TK14, TTL10, WLDB11, WgMdZ12, gwpw+14, XNG+14, YWWW15, YYO15, AP10, AIA+18, CLM+12, EAA+16, GZHD12, HZC+14, HZL18, IOV+18, KIH19, LNK+18a, LW10, PKS18, RS17, yWPw+11, yWPw+13, YSL+10, ZHH+17].


Rotational [KN10, KN101]. Roulette [Ber17]. Round [Ber17, jCPB+12, COP+14, DWWZ12, GHHR14, KOTY17, KMO14, LWZ12, LJ17, Pan14, TYM+17, XZLW15, Yon12, YAY14, ABM+12, BLO+15, LFP+16, Sun11, TSL11, TQL+14, TCS14, XW12].

Round-Reduced [DWWZ12]. Rounds [GCT12, SAS12, LYH14, MNP12]. Router [BIS17, SA15]. Running [HAN12, KZG10, WLY+15, LSG16, LC17].

RSA [DUN12b, KIA11, PIE10, APPVP15, BBP13, BRO17, BNST17, CCL+19, CSL12, Chm10, GM13, GST13, Her14, HIN10, HLYS14, IK15, KHHH14, KFL+10, Lim11, MV19, MOO12, SM10a, SM10b, SLM10, TK19, WIN17, YHK+10, YXA+16].

Rule [KPW13, NC12, TW12, McG11].
Rule-Based [TW12]. Rumor [FKOV15].
Run [CEL+19, IF16]. Run-Time [IF16].
s [Sch15a, NN12, RMP10, SS11, WJ19].
SafeCurves [BL17]. Safeguarding [FGR+17]. Safely [HM12]. SAFER [YCL17].
Santa [Rab10]. Sanya [LTW11]. SARFUM [BCE+10]. Sarkar [Kat13].
[WXK]+17, XHH12, XZW16, XWC14, XXX15, XMD13, YC11, YCC16, YHHM18, YWK+10a, YCT15, YXD18, YQOL17, YMSH10, ZYL+10, ZLY10, ZX14+14, ZYC+17, ZPY12, ZHH+17, ZY17b, ZFH+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12. **Schemes**

[ABF12, BVS+13, BFM12, BBP14, BSJ15, CMLRH13, CLND19, CGL+12, Ch16, Des10b, FHKP17, FFL12, HSM14, HLLG18, HPO+15, IWL10b, LZCK14, MLCH10, MR14b, MMS17b, MBF18, MKRM10, Ob11, PB12, PDNH15, PH12b, Sch10, Shi11, SKH17, SSU12, VSR12, WGF16, YNR12a, YNR12b, Yek10, YWZ+12, AGHP14, An15, AHL+12, CDGC12, CJXX19, CHS11, CCG10, CTL13, DDD14, DD13, DZ14, FBPB14, FGPM12, FMA+18, HWDL16, HM10, KUT116, LHY12, MD12, MA17, NZL+15, QYW16, SES+16, Sar10a, Sar11, hZZ15, SAR18b, WW14, YT11b, ZCL+12, ZCLL14, ZT14. **Schneider** [Sev16]. **Scholarship** [SPG+19]. **Scholarship-for-Service** [SPG+19].

**Science** [Bow11, Gas13, IEE10, IEE11b, Tr11, Bia12, PHWM10, Pet11]. **scientists** [Goo12]. **Scientometric** [Pal15, Pal16].

**Scope** [Bai12]. **Score** [GCDP11].

**scoring** [OSK16]. **Scrambling** [LLL17a].

**Screen** [SPW+16, CTL12]. **Script** [Rao10, Bax14]. **Scripting** [DSB15]. **scroll** [GMOG15]. **SDB** [HWW+15]. **SDDO** [PL16]. **SDDO-based** [PL16]. **SDH** [GMS11]. **SDVIP** [YNX+16]. **SDN** [KCC17]. **SDVS** [Wan10]. **SE** [LLL13].

**SE-AKA** [LLL13]. **seals** [MN10]. **Seam** [LC15]. **Seam-Carved** [LC15]. **Search** [AHN+18, CWL+14, Che15, DCA18, FRS+16, Gt11, HCDM12, HLI9, LSQL18, TMC15, WDCL18, WW12, XSW16, XJW13, ZXY16, BL11, CLH+16, FHI3, FSGW12, GZS+18, HH16, OSSK16, SY15b, WHY+12, WXLY16, XXY+18, YXD18, YQOL17, ZZ11].

**Searchable** [BHJP14, CWW12, CLW16, CGKO11, FJSH12, PBC+17, PCY+17, XNKG15, ZZQ+19, DLZ16a, DRD11, HQZH14, HTC17, JCHS16, LZC17, LLL+18, RPS10, WXL16, WCCH18, YZCT17].

**Searches** [Sia12, WR15]. **searching** [GP+12]. **Seattle** [LCK11, KCR11].

**Seberry** [AHS14]. **SEC** [PA10]. **Second** [AKY13, ABM+12]. **Secondary** [RS11].

**Secrecy** [ABD+15, BKST18, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCU15, TCS14].

**Secrecy-preserving** [TSH14]. **Secret** [ASN11, ASN12, ADH17, Ayu12, Bai10, BBB+16a, BFM12, BBP14, Bri11, CCM+15, CFORE12, CCL+13, DRI12, Dew11, EM12, EA11, FHKP17, FR16, Fok12, HYS11, HL10a, Has16, JLS12, KU14, KS18, KOTY17, KK12, KK13, KSSY12, KS15, LHF12, LPL15, Lin15, LCCJ13, LTC+15, LJ16, LLKA19, Men13b, MNS11, NS12, Ob11, PCK14, QS18, SLL10, SC10, SS10c, SSS12, St15, TLW12, TWZ11, WKB16, WGF16, Wil18, XZY+12, XRJ+17, YFF12, YWZ+12, ZC13, Ald11, ADG16, AKK+17, Ara13, BJ16, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEAZ13, EZI5, FHI10a, GJMP15, GLW13, HF14a, HH15, Hea15, HBBRNM+16, HCCC11, HLC12, KI11, KTU16, LXLY12, LT13, LyWS10, LHYZ12, LEW19, Mas17, McK10, McK11, McK12, MB11, OO10, Pea11, Pet11, QD16, Rus15, SB17, SA12, SAR18b, TQL+14, TD14, UUN11]. **secret** [UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, XW13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPY12, LSC+15, Bai12].

**secret-key** [BJ16]. **Secret-Sharing** [BBP14]. **Secretion** [RSCX18].

**Secretocracy** [Ber16b]. **Secrets** [BT12, CG14b, DLWW11, FMS12a, Kobi10, Man13, Bha16, Cop10b, GGH+16b, Gup15, HRS13, Smi11a, Anol17b]. **Section** [BD19].

**Secure** [ADMM16, AARJ12, Ash14, AMH+16,


Sequence [PFS12, WGZ+12]. Sequences [ADD10, Kla10, NN12, XNP+18, XYXYX11, HLC12, VM14]. Sequential [GLR10, GLR13, LLY13, WYL13]. Series [BJL16, Dice12]. Serpent [PC16]. Server [BCO13, Che15, GMSV14, LSQL18, LY15, MV19, YL13, AKTH+17, CSD18, CLH13, FA14b, FHZW18, HDPC13, HL14, ISC+16, KMGT12, LXMW12, LH13, SY15b, hSZ15, SSAF11, SSS11, TLL12, WT10a, XHM14].

Server-Aided
Server-Designation [Che15, LSQL18].
Server-Side [BCO13]. servers [DRD11].
Service [BBBK14, CCS14, Hay13, LDB+15, LBRA12, NRZQ15, RSGG15, SPG+19, SSSC12, Sti15, VS16, AaBT16, KPP16, LHl+18, LW13a, MMP19, MLM16, Par12b, Wu17, YWK10b, ZX11, YCM+13].
Service-Based [LDB+15].
Service-Oriented [RSGG15]. Services [Ano11b, DLZ+16b, MEFO12, OO12, ZHL15, AZPC14, CSID18, CHX13, GAI+18, IMB17, IG11, NZL+15, PP11, WDKV19, 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].
Share [LTC+15b, ZPXY12]. shareable [XWY+18]. Shared [DRD11, LNX15, OKG+12, TYK+12, XJR+17, FPZP15, SA12, TG12, YXS+16, YNX+16].
shared-secret [SA12]. Shares [CFOR12, KU14, SA16a, WV12]. Sharing [Bai10, BFM12, BBPE14, CCM+15, CFR12, CCT+13, CCL+14, CLW16, DR12, EM12, FHKP17, FR16, HYS11, HL10a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KS15, LYZ+13, LPL15, Lil15, LCCJ13, LTC+15b, LLKA19, NS12, Ob11, PSM17, QZZ18, QCJ+18, SC10, SSU12, SZZT18, TL12, TWZ11, WYCF14, WKB16, WGF16, XNKG15, XZY+12, YFF12, YWZ+12, ZC13, AKK+17, ADH17, CT11b, CW14a, EZ15, EA11, FGMP12, GPLZ13, GJMP15, GLW13, GLB+18, HF14a, HBRRM+16, HCCC11, HLC12, HYF18, K111, KUT116, KP171, LXYL12, LT13, LFWS15, LAL+15, LyWSZ10, LHY12, LHL15, LLL+18, LEW19, LL16a, Mas17, OO10, OO18, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WLS14, WKB11, WS12, WOLS12, YC11, YCC16, ZCL+12, ZZ15, ZPXY12, SLL10]. Shell [WZCC18, YSS14, Tay14]. Shenzhen [IEE11a]. Shield [NDG+17, KG16]. Shift [AKP12, TAP19, ZHI5, LWK11]. Shift-Type [AKP12]. Shifting [YWW10, CSS+13]. Shih [Joh10].
Shopping [AHS13]. Shor [JL18, MNM+16]. Short [BHG12, CWWL12, NR12, SKV12, WQZ+16, XGLM14, LLY15, RD17, ZPXY12].
Shuffle [HM12]. shuffler [BVI12]. Shuffles [CKLM13]. shunned [Rec15]. Sicily [Cra12]. Side [AN17, BCO13, CFE16, CDK+10, CBL13, DZS+18, DMWS12, DKMR15, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, SR12a, Vua10, YL17, ZBPF18, BVIB12, DJL+12, MFH13].
Side-Channel [CBL13, DZS+18, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, Y17, ZBPF18, DMWS12, BVIB12, MFH13].
[LJK17, XNRG15, AIA+18]. **Signature**
[Ano13a, ABF12, ASS15, AEHS15, BHG12, BDH11, CLND19, CGY+13, FGM10, GJJ15, GJZ17, GMSV14, HZK15, HPO+15, HHP17, Hui13, JL16, LTH+15, LGPRH14, MMN12, NXB13, PH12b, ST16, TTH15, WZXL12, WLH15, WYML16, WHL16, XGLM14, Y+17, YH+10, YMWS11, YLA+13, ZJ14, ZLH+12, AGHP14, CLSW12, CCG10, DZ14, DLN13, HYWS11, Hwa11, JZS+10, IWZG10, LL16b, Nos14, QYWX16, QMW17, QCX18, RSM15, SLM10, VS11,WSC14, XLWZ16, YWL+17, YLS12, YKC+12, ZLY10].

**signature-based** [DLN13, QMW17].

**Signatures** [Ano15a, ABC+17, AYS15, BBC+13, BDFK12, BH+15, Fuc11, GY13, GD16, HS18, Hui13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, Orn16, PST13, TH16, ASVE13, BDL+11, BPP10, GMS11, Her14, LLY15, PPB16, SEXY18, Tia15, QWZ10, Mou15]. **Signcryption** [CMA14, DZY10, FZT13, FZT14, IL15, LSL12a, Rao17, RSD19, XQL11, ZYD10, EZ15, HPY10, HS11, KL11, LK12, LZT12, LKT12, YMSH10, LHL15]. **Signed** [KWH16]. signer [Hwa11]. **Signing** [YAM+15, JC13]. Silent [AMH+16].

**Silverman** [Mei10]. **similarity** [ZFH+18]. **similarity-aware** [ZFH+18]. Simon [AMKA17, BSS+13]. **Simple** [Ano13c, CZF12, 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** [Abb13, LL15, MEF012, Sas12, SPM+13, CIXX19].

**single-generation** [CIXX19]. **Single-SP** [Sas12]. **Singular** [LSL12b, BWA13].**sins** [HLV10]. **SIP** [KKG10, ZTZ16].

**SIP-based** [ZTZ16]. **SIPF** [SYC+17]. Site [DSB15, SS10c]. siteDriverID [SGGCR+16]. **Size** [AS17, AEHS15, CJ13, CSW12, EAA12, Kim15, LCLL15, LSQX19, MTY11, JWZ16, AHL+12, LCT+14, PPTT15, SGM16, SHBC19].

**Size-Constrained** [EAA12]. **Skein** [FLS+10, KN10]. **Skill** [CSM18]. **Skin** [AQD12]. **skyline** [BKV13]. **Slantlet** [TK14]. **Slicing** [Miz17]. Slide [IOM12, LC13].

**Sliding** [BBG+17, Bro17, W17]. sLiSCP [ARH+18]. **SLMAP** [HCETPL+12]. Slow [Smi11b]. Small [BGJ14, BKLS12, BB10, CJ13, Kim15, LCLL15, YM16, AAT16, BGJT13, Jou13].

**Smart** [An17, ABC17, BSJ15, DLZ+16b, HCL+14, HK18, LA10, MF16, PDI12, WgmdZ12, WgMW12, AMN18, CH13, LHJ13, GHD19, GAI+18, Ham19, HCC10, LH10c, LNM+11, LXMW12, LNLK13, LNK+18a, LTC+15a, MM12, MCN+18, WMYR16, YZZ+14, YSL+10, Choi0, GL10, SD12].

**Smart-Card-Based** [HCL+14].

**Smartphone** [MDMJ17, uHAN+18, DL15].

**Smartphones** [Cor14b]. smashed [Fag17].

**Smith** [Ano16g]. Smooth [XXXY11, YC11, ZBR11]. **SMS** [KRM+10, PSdO+13]. **SMSCrypto** [PSdO+13]. Snakes [PC16]. **SNOW** [PC16].

**Snowden** [Tox14]. SoC [HZ+19, GSC17].

**Social** [BPS17, KTA12, NAI15, NQR+15, PYM+15, Rog16, SKGY14, SZT18, WLY+15, ZW15, Zha15b, ZHL15, BDK11, HYF18, LCM+17, LZC17, MSM+18b, SSK+18, Sm15a, YZ18].

**Society** [Sch15a, Sch12b]. Socio [NS12].

**Socio-Rational** [NS12]. SoD [V16]. Soft [Her19, Jin10, TLCF16, SS17]. Soft-Error [TLCF16]. Softw [WZM12a].

Software [Bar15, Bee17, EWS14, KYE18, LRVW14, MRL+18, MV16a, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GJ+12, HLV10, KHF10, LBOX12, SF12, WYT+12].

**Software-Defined** [KYE+18]. Solan
Spatiotemporal Spectrum-Based Solutions [Ano19b, LLGJ16, BLV17, KAS15, MMP19, WW14]. Solved [IBM13a].

Solved [Ano17c, BB10, Bul10a]. Some [AD12, Ber12, Dur15, LWL10b, Mid10].

Somewhat [H_TC17, KOS16, MBF18]. Song [Cout12]. Sood [MWZ12]. SOSEMANUK [PC16]. SOT [PAF18]. SOT-MRAM [PAF18]. Sound [COP+14, LSR13, Sav15].

Source [Bis17, FKOV15, MCB15, RWLL14, ABE+14, LZC17, PX13, Pow14].

Source-Based [MBC15]. Sources [DBH16, BJ16, SSY12]. South [BL10, LW11a]. Sovereign [TAP19]. Soviet [Bud16]. SP [Sas12, SEHK12]. SPADBox [FGR+17].

Space [BWR12, BKL12, NYR+14, RMG18, MSN+18b, RYF+13, Z15]. Space-Filling [BWR12]. Spaces [SH15], spam [SKG+14].

Spanish [Pett11, SGCR+16]. Sparse [AGW15, AAT16, BBC+13]. SPARTA [MSS+17a]. SpartanRPC [CS14]. Spatial [AV12, CZF12, PDM12, CW14b, NZL+15].

Spatiotemporal [DIMT12]. Speaker [BJCHA17, PPRT12, RSR+19]. Special [Ano13d, Ano16a, Ano16b, Ano16h, AB10b, Bdl19, CSYY18, GO17, LW13a, LK18, PHWM10, WX13]. Specific [BD15, BDF12, KME+12]. Specification [HZS+19, SK11, SD10]. Specifications [BMP12].

SPECK [LFW+16, AMKA17, BSS+13]. Spectrum [KD12a, TWZ+12, XNRG15, XNP+18, KBP17, LWY12, MMSD13].

Spectrum-Based [TWZ+12, XNRG15]. Speech [AGW15, LJK17, SAA15, YMA17]. Speed [ARM15, GLJ2, HZ11, KP17, LTKP16, BDL+11, KL13]. Speeding [RVRSCM12]. Speedup [Che18]. SPEKS [Che15]. spell [Bha16]. Sphere [Sti19].


STAMP [WPZM16]. Standard [Ano12, Ano13a, App13, ABC+17, BCM12, BV11, BV14, CT18, GJ15, GJZ15, HXZ15, Loe15, MVVR12, OGG+15, RSD19, SJS14, TCL15, WWHL12, Yon12, ZC13, BCM13, HTC17, Kim11, LzT12, LL16b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, ZCL+19, AEH17, MKRM10, NMMW16].

Standardization [TRD11]. Standards [BCM+15, Che17, DHW+13, NIS13]. State [BV1+13, BLM17, CG14a, CCL+13, CS15, Dew11, DP17, FHR14, LLK18, MKF+16, Sen17, WGD18, XZY+12, BBDL+17, CK11, CGH17, Ham12, Mid10, QD16, Sir16].

Stateful [BV1+13, NTY12, VPK17, VSR12]. Stateless [BHH+15, GM11, MKA17, NTY12, VDO14, DCAT12]. Stateless/Stateful [NTY12]. statement [NIS13]. Static [DKMR15, IF16, Lan11, TLMM13]. Station
[Sm11a]. stationary [ZLDD12]. Statistical
[Böh10, Bro11, DBPS12, HZ11, Hey17,
LTRP16, OOR+14, SP13, Sim15a].
Statistical-Attack [SP13]. Statistics
[gWpN+Y+14]. Statutory [PH12b].
Stealing [RWZ12]. Stealthy [BRPB13].
Steering [HR13]. Steganalysis
[Böh10, DA12, Fr12, JHUN12, KD12b,
LJK17, LC15, SGP+12, Tan12a, YLL+12,
Y14, YP117, LSQ11a, LSQ11b, Sch12a].
Steganalysis-Resistant [YP117].
Steganalytic [Ber18, YPRI17].
Steganographic
[DA10, HHS+15, LyWZ12, WP15,
AGLW16, LLC10, CAC14]. Steganography
[AGW15, BCG12a, CLF11, FR16, FMS12b,
Fri10a, Fri12, HZW+14, Joh10, LJK17,
LLY+12b, MAL10, PDMR12, Pau10, SK12a,
SR12b, TZJF12, WWL+14, YWW10, ZSA12,
AOT13, BDK11, BHCdFR12, EEAZ13,
GKC11, LyWSZ10, LRW13, LRW17,
LWW+10, Maz13, MSM+18b, MS17,
PHN+12, SI12, Sun16, WKH11, WOLS12,
ZMS14]. Stego [YLL+12, SM18].
Stego-Image [YLL+12]. Stellenbosch
[BL10]. step [AKY13, XYA+18]. Steps
[Ano13c]. STES [CMLS15]. Steven
[Led16, Sch15a]. Still [RAS15, UK18].
Stochastic [ADR18], stolen [Bha16].
Stopping [Sav13a]. StopWatch [LGR14].
Storage [BCO+13, CWL16, CCT+14,
CLW16, GLG12, HSM14, HLC+18, JSCM17,
Kiup15, LCK11, LMD16, LWJC14, PBC+17,
QLL17, SKH17, XNKG15, ZDL12, ZVG16,
AY14a, AKK+17, BP10, CFVP16, CFZ+10,
CHL+16, CDF+10, CDI18, ED19, FH13,
FNWL18, GLB+18, HSM13, LBOX12,
Sar10a, SYY+17, SWW+16, SWW+17,
WS13, YYS+16, YZC17, ZYC+17, ZVH14].
Stories [CMLS15, RSN14]. Stores [BCK17].
Stories [Sm15b]. Storing
[DLWW11, LZZ17]. storm [ACM12]. Story
[Cer14, Keb15, Ald11, Fag17, Gre17, Hea15,
Mac14, Mun17, Pea11, Pet11]. Strand
[SH15]. Strange [Acz11, Gre17].
Strangeness [Ber12]. Strategic [Sch12c].
Strategies [DSSD14, TJZ12, YCM+13,
AZF+12, WWW17]. Strategy
[LH12, NRZQ15, FL+12]. Stratix
[SMOP15, SMCP15]. Stream [ABS+12,
BMS12, CMLS15, DM18, DGI12, DGS12,
DJG+15, KGB17, GCS+13, HZ11, Hey17,
IOM12, KE19, KPC+16, Kla10, MD12b,
MHC12, MS12b, NN12, PRNC17, WH18,
WHN+12, ZH15, Die12, KM10a, LWK11,
LWW13, MRT10, OCG11, QGL13, RS14].
StreamCiphers [ERRMG15]. Streaming
[ZSA12, Cri16, XWZ+18, ZC12]. Streams
[PCDG14, HM10, PYP10]. Street
[Gli12, KPG12]. Street-Level
[Gli12, KPG12]. Strength
[DM15, FHV16, Spa16]. Strengthen [BL12].
Strengths [XNP+18]. Stribog [AY14b].
strikes [Ran10]. string [FHV16]. Strong
[ADD10, KFOS12, PYM+15, SAA12b,
Yon12, GH16, HYS11, NCL13, OYHSB14,
WLZ+16]. Stronger [Boy16, MvO11, RK11].
Strongly [DMD17, HHP17, KW14, YS12].
Structural [LYY+18, BDK11]. Structure
[HP12, LMH14, LJ15, MKRM10, WYCF14,
WJ19, LXY12, ZLW+12, ZPWY12].
Structure-Independent [MKRM10].
Structured [PMZ12]. Structures [GT11,
HHH+13, LHKR10, LPL15, PB12, DDR13,
MHKS14, SLY15, WS12, XWZ+18, ZW15].
STT [VDB+16]. Students
[PP10a, SPG+19]. Study
[Ano17c, DHR+16, SY15a, SPG+19, STC11,
CCG10, EBFK13, MVH15, SS17, VGN14].
Stuxnet [Zet14]. Style [GHS12, GHS13].
stylometry [BAG12]. sub [GPLZ13].
sub-passwords [GPLZ13]. Subcommittee
[Bla16]. Subgroup [CCL+19]. subliminal
Subscribe [BGP+17, DLZ+16b, OFMR16,
PRSV17, SL11, TKR14, YSM14]. Subset
[BS14, RP12, ZZ11]. subspaces [ZWM14].
Substitution
[DA10, SGFCRM+18, FVK17]. substitution-transposition [FVK17].
structure [MRT10]. Succinct [BCT+13, CKLM13], sufficient [TD14].
suitable [Jeo13, SKB+17]. Suite [MTM18, NACLR12]. Sumo [BS12]. Sums [SSB2b]. sun [Cer15]. super [MZ17a].
Supersingular [Lau17, LNL+19, Y+17]. Supervised [CTC+15]. Supply [QZL+16a, QZL+16b, YFT17, YSF+18, YFT18].
Support [MSI18, ZZQ+19, CZ14, JAS+11, PWW10, PKA15, TLI10, VCK+12, ZMM+10, ZBR11].
Supporting [BHH19, FMTR12, HCDM12, HZL18, YYS+16]. supports [WR15].
Survey [ABHC+16, BGN17, BCTPL16, BHJP14, BJCHA17, HPC10, KMY18, KSD+17, LGM+16, MR14b, MS18a, MS10, NV10, OFMR16, SKH17, TRD11, TS16b, AAZ+16, ABB+14, ADH17, BM13, BGG+13, FMA+18, HT13, KJN+16, KAS15, MMP19, MA17, Maz13, MHV15, NR11, PPA18, WWW17].
Survival [YCM+13, MMS+17a]. Surviving [CFST17]. suspect [der10]. SVC [MU12, WDDW12, ZLDD12, ZLDD14].
SVD [LP12, TB18, WZ17]. SVM [TLL13].
swarm [ZSMS18]. Swarms [VOGB18].
Symmetric [BPR14a, BPR14b, BDP12, CVM14, FPS12, GBBF12, JCHS16, KTT12, Kha10, PR12, PCY+17, TWZ11, YKS12, BGG+13, CGKO11, DLZ16a, FH13, GMRT+15, Gor10, GCV17, KAS15, Lzc17, SKK10].
Symmetric-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, yWXY+18, AATM18, XNG+14].
Synergy [KRB12]. Synergy-Based [KRB12], synthesis [RS17]. Syst [HYS18, WZM12a]. System [AD11, Ano10, CZLC12a, CZLC14, Cor14b, CRST15, DG15, GOPB12, Har16, HHS+15, HZS+19, IAD10, JN12, JWJ+17, Jin10, KMP+11, LFX+18, Lop12, MLBL12, NSMS14, QLL17, RSCX18, SMK18, SRAA17, SL11, YE12, YXZ+12, YKK18, ZMM17, ZPW16, ZLDC15, ZVG16, AHM+18, BC18, BGG+13, Bu10a, CH11, CTL12, CZ14, CS11, FNLW18, GCK11, HWK+15, HJM+11, HLYS14, JC13, LLLK10, LLL+17b, Lit14, LTX+15a, LLL+18, MS12a, MNN15, PSOMPL13, SS1+13, WMX+17, WGZ+12, XWZW16, YZL+18, ZMM+10, ZML17, ZZL+18, KKA14, Dew11].
System-Level [JWJ+17].
System-on-Chip [HZS+19]. Systematic [CCG+16, CBL13, PC16]. Systems [AN12, AB15, BL15, BS13b, BCTPL16, BB10, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HLN+10, HK18, LMD16, LQY10, LY16, LNZ+13, MR14b, OŠ12, PRS17, QZL+16b, RST15a, RST15b, SBS+12, SFKR15, Sev10, SKH17, SGC14, SDM+12, STCI11, TKR14, YNR12a, AT10, ATI+10, CFVM16, CFZ+10, CLZ+17, dCCSM+12, dCCSB+16, CGHI11, CVG+13, CDA14, DZS+12, Eis10, FXP12, GMGCCCC15, GHD19, GSN+16, GPVCD102, HZW18, JSK+16, JHCC14, KSA16, LCL+15, LWK+18, MLMSG12, MGP10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRB+12, WS14, YSM14, ZHV14, Zhu13, MA17, Ano11a]. Systolic [MCDB12]. Systolic-Array [MCDB12]. SZK [MX13].
LNK\(^{18a}\), LNK\(^{18b}\), LML\(^{13}\), Tso13, TKHK14, XCL13, YC12, YZZ\(^{14}\).

**Three-Dimensional** [LLY\(^{18}\), LZC\(^{12b}\)].

**Three-Factor** [HXC\(^{11}\), AIB\(^{+16}\), IC17, JKL\(^{+16}\), LNK\(^{18a}\), LNK\(^{18b}\)].

**three-party** [LML\(^{13}\), Tso13, TKHK14, XCL13, YC12, YZZ\(^{14}\)].

**Threshold** [CT11b, Cil11, FGM10, GLW13, HYS11, LWL10b, SSU12, Sta12, Tan11, WYC14, WLH15, YFF12, YHK\(^{+10}\), YLA\(^{+13}\), ZCL\(^{+12}\), DZ14, FGMP12, HF14a, HH15, OO10, QD16, SES\(^{*16}\), Shy15, SGM16, TD14, ZJX\(^{+14}\), ZPWY12].

**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** [GDCC16, LPS12, LLH18, ZYH\(^{+19}\)].

**Tightly** [HLLG18].

**Time** [ASBdS16, Ano12d, App14, AYS15, BJL16, Che17, FD11, GSC17, HC17, HGT15, IF16, JWJ\(^{+17}\), JEA\(^{+15}\), KME\(^{+12}\), LCL\(^{+17a}\), LFJ\(^{+18}\), NA10a, Nov10, PNRC17, Ste15b, WLZL12, YE12, AY14a, Ano15d, BM15, CC14, DCAT12, FHH10a, GPLZ13, HU15, LW10, LW13b, LML\(^{+13}\), MK11, Ano16g].

**Time-area** [Nov10].

**Time-Delay** [LFX\(^{+18}\)].

**Time-Memory** [ASBdS16].

**Time-Series** [BJL16].

**Time-Specific** [KME\(^{+12}\)].

**Time-Spread** [HTG15].

**Timed** [Jia14b, KFOS12, Tan15a, Uur15, WSS12].

**Timed-Ephemeral** [Tan15a].

**Timed-Release** [KFOS12, Unr15, WSS12].

**Timing** [BGN17, GV14b, Hay13, LGR14, AGH\(^{+17}\), SRB\(^{+12}\)].

**Tiny** [ZOC10].

**Titan** [PP10b].

**Titan-R** [PP10b].

**TLS** [AP13, BDRL\(^{+17}\), BFCZ12, BJR\(^{+14}\), CFN\(^{+14}\), Dav11].

**TLS-based** [PP11].

**Today** [Ber16a, Mac12].

**Toepplitz** [Ye10].

**Token** [TYK\(^{+12}\), ZM16, IMB17, Jac16].

**token-based** [Jac16].

**Token-Leakage** [ZM16].

**tokenisation** [Mar10b].

**tokenless** [Wat14a].

**Tokens** [Muf16, DCAT12, HU15].

**Tokyo** [Sah13].

**Tolerant** [HK14, ZM16, JLT\(^{+12}\), WMYR16, TX13].

**tolerating** [ZWM14].

**Tone** [Yam12].

**Too** [DL15, DSSDW14, Ros11].

**Tool** [ASM12, DKMR15].

**Toolbox** [BJL12].

**Toolkit** [BJL12].

**Tools** [Abe12, BKBK14, GO17, Ste15a, Lan11].

**Top** [SS12a, SS10c, Sta13, CHX13].

**Top-Fanin** [SS12a].

**Top-Secret** [SS10c].

**Topics** [SCPSN10a, SCPSN10b, AB10b, Dun12b, Kia11, Pie10].

**Topology** [HIMK14].

**Topology-Preserving** [HIMK14].

**Toronto** [LLY\(^{+12a}\)].

**Touch** [SPW\(^{+16}\), SHBC19, Alp18, CTL12].

**touchstroke** [Alp18].

**Tower** [ZAG19].

**TPM** [GY13].

**TQC** [vDKS11].

**Trace** [ABR12, PS14, AA14, WGTJ10].

**Traceability** [HCETPL\(^{+12}\), WYML16, WHLH16, YFT17, Chi13a, YYS\(^{+16}\)].

**Traceable** [LDZW19, QRW\(^{+18}\)].

**Traceable-then-revocable** [LDZW19].

**traceback** [LYW12, PJ18, WYL13].

**traces** [MYR13].

**Tracing** [BW16, PPS12b, WXY\(^{+17}\), MH13, PPR\(^{+12}\)].

**Track** [Dun12b, Kia11, Pie10].

**Tracking** [GZH17, MDMJ17].

**Trade** [ASBdS16, BS14, SR10].

**Trade-Offs** [ASBdS16, BS14, SR10].

**Tradeoff** [WDDW12, MV16b].

**Trading** [TW12].

**Traffic** [DRS16, HS18, KAHKB17, AZH11, FT16, PPR\(^{+12}\), VS11].

**traffic-feature** [FTV\(^{+10}\)].

**Training** [HM12].

**Traitor** [LYW16, PPS12b, Bha16].

**trajectory** [LVRY10].

**Transaction** [BGAD12, KVvE18, OYHSB14].

**Transaction-based** [BGAD12].

**Transactions** [DG15, Mic16, Muf16, PAS13b, TV15, DK12, MLMSMG12].

**Transceiver** [NBZP17].

**Transcript** [Gli12].

**Transfer** [DN12, FMTR12, HL10a, LCC13, WCL\(^{+18}\)].
EEAZ13, FES10, Ham19, Har14, HZWW17, HWB12, HL14, HPY10, HCC10. using [HS11, JCHS16, JMW +16, KI11, KY10, KKG14, KM11, KIU16, KPB17, KLW+16, LXY12, LLP+18, LC17, LH10c, LNM+11, LXMW12, LH13, LML+13, MM12, MS13a, MMSD13, MM14a, MKH+12, MRR+17, MSM+18b, NTK17, PBCC14, PC14, QD16, R15, RS17, Sar11, SGFCRM+18, SKS+18, SAR18b, TCF16, TG17, TK14, TLL13, UUN11, yWpNyL11, gWpNyY+14, WMX+17, WHJ17, YQH16, YZZ+14, YSL+10, ZK17, ZLW+12, ZY+17, ZXW+18, ZSL+18]. utilization [NZM10].


KS15, LPL15, LW10b, LGWY12, LMHH14, LTC+15b,OTO18,SA16a,SC10,Sky15, 
WY12,Yam12,ZZX+11,CT11b,CFSTR16, 
DDD14,DD13,GLW13,HT11,LLW10a, 
MSM+18b,WYK12,WS12,YSC16,YR11.

Visualizing [Sav15]. VLSI [KB10]. 
VMOR [MSI18]. Voice [JTZ+16,WBC+10, 
LFGCGCRP14,TJZF12]. Voice-over-IP 
[JTZ16,WBC10].LFGCGCRP14,TJZF12].

Volatile [AMH+16,RM18,SM18,YNQ15,CK11].

voltage [BBBP13]. volume [WLDB11].

voluntary [WGJT10]. Voting [Ber16a,CFE16,CRST15,CET+19,KV18, 
LHF12, LGPRH14, RST15a, RST15b,Sch10].

Voynich [Ano16d,Bax14]. vs [Bur11,FKOV15,Mar10b]. Vulnerabilities 
[BKJP12,HSUS11,MA16,PDT12,RY10].

Vulnerability [MKN13,TM12,VK15, 
Wal18,Ano17f,DMWS12,MYR13].

Vulnerable [Ano15d]. vVote [CRST15].

W [Mar10a,Xie12,Hüll13]. W-OTS [Hüll13]. 
WA [LCK11]. Waknaghat [CGB+10].

Walker [Xie12]. Wallets [Chi13b]. Wallis 
[Wes16]. Wan [RSD19]. War 
[Has16,Mun17,Bud16,Car11,Sm11a].

Warbler [MFG16]. warriors [Bud16].

wartime [McK10,Mck11]. was 
[Goo12,LHA+12]. Watermark 
[CHHW12,DLMM+18,EMW14,Jin10, 
KBL11,LCZ+12b,MCB12,QJC+18,SJ12, 
YE12,ZS12,BH13,TLL13,WYL13].

Watermark-Driven [DLMM+18].

Watermarking 
[BCGAPM12,BF12,BCPV11,BDB14, 
BBM15,CG12b,CHHW12,CCZC13, 
DG17,FM15,Fra15,Fra16,GKS17,GLP17, 
HPC10,HEK18,HGT15,HMK14,JSZS12,Joh10, 
JKHeY12,KD12a,LS12b,LLY+18,LP12, 
LD13,MM17,MR16,MU12,NGAuHQ16, 
NC12,NHX+17,pNyWY+14,OWHS12, 
RS16,RP12,RR11,RMG18,SAA15, 
SLGZ12,SSA13,TB18,TWZ+12,TC10, 
WHZ12,WLZL12,WYW+13,gWpNYY+14, 
WXL+17, pWxyZ+18,tWmC12, XNG+14, 
XNRG15,XNP+18,YWNW15,YPRI17, 
YKK18,YYO15,ZZZ+11,ZWZ17,AP10, 
AIA+18,AKM12,BW13,BWA13,CCLL11, 
CT11a,CS+13,GZGD12,GA11, HKB14, 
HWYW14,KJ13,KPS10,KPN+16,KM11, 
LSR13,LCXM11,LLHS12,Linf14a, 
LWY12,MMS13,MM14a,MO14,MK11,NC13, 
PTK14,PWLL13,PWW10,PGLL10,PKS18, 
PC14,PPR+12,RS17,SKS+18,Tay14,TK14, 
TTL10,TPKT12,WLDB11,yWpNyl11, 
Wan13,yWpWypN13,WZL13].

watermarking 
[YWT+12,ZZKA17,ZSMS18].

Watermarking-Encryption [SLGZ12].

Watermarks [GL10,YT12]. WAVE 
[BMM12]. WAVE-enabled [BMM12].

Wavelan 
[AGW15,LSL12b,MR16,Ara13,AMK12, 
BW13,LCXM11,MO14,yWpNyl11].

Wavelet-Domain [MR16]. wavelets 
[MMS13]. Way [CBJ19,CPS16, 
DSMM14,Mat14,HRL10,LP11,RK11].

WBAN [KS18]. WBAANs [KH19]. Weak 
[BF11,DY13,HDWH12,PYM+15,Pud12, 
GJMP15,RH10]. Weakening [SFKR15].

Weaker [Sas12]. Weakness [AMORH13].

weaknesses [Nos11,Nos14]. weapon 
[Zet14]. Wear [LY15]. Wear-leveling 
[LY15]. Wearable 
[BCTPL16,XJR+17,GTSS19,LIK+17].

Wearout [DFKC17]. web 
[GP+12,IMB17,CRM+10,KGO10, 
ATKH+17,BS12,BKJP12,CTC+15, 
CFST17,CD12,DR11,Fra16,HCM11, 
QF19,SP15a,SPM+13,ZGC16].

Web-Based [CD12]. web-content 
[GP+12]. WebCallerID [HCM11].

Website [Boy16]. Websites [RS11].

Webster [Pia11]. WECSR [DDS12]. Wei 
[SBS+12]. Weierstrass [LL11]. weight 
[ÖS11]. Weighted [YLL+12,YTH17].

Welchman [GW14]. Well [JCM12]. were
[McK10, McK11]. Western [Han12]. WG [GLIC10, DJG15, ERRMG15, ZAG19].

WG- [ERRMG15]. WG-16 [ZAG19].

Where [CMG18]. Wherefore [BDK11].

Whit [LHA12]. White [BW16, BCGN16, Mic10b, DD13, YSC16, ZSW18a].

White-Box [BW16, BCGN16, Mic10b, ZSW18a].

Whitfield [Hof16]. who

[Bat10, Bha16, Car11, Fag17, Hea15, Kap13, McK10, McK11, McK12, Moo14, XTK10].

Wicked [SGH15]. Widespread [HDWH12].


wildcard [III16]. Wilderness [Acz11].

Will [Mos18]. win [Smi11a]. window [Win17]. windows [BBG17]. Wine [Che17]. Wineskin [Che17]. wins [Ano16g].

wire [ADG16, ZCJ14]. wire-tap [ADG16].

Wireless

[ABC17, BN14, BOB13, CBO18, CS14, DPCM16, DS11, FLM13, HZC12, HBC13, KH10, LLC11, LHM15, LZCK14, LWC14, LLZ12, NNAM10, PCPK14, RCW15, RSD19, RWLL14, SWYP12, SP15b, TCN17, YM16, ZLDD12, APK18, AIB16, AIK18, ADF12, BLAN16, BBB16b, CDGC12, CML18, CLSW12, CL11, DSC12, HGWY11, HZC14, HZW17, HCC11, HT10, 10, HLYS14, JNUI17, JM16+, KP18, KO16, KLW16, KD17+, LC17, LMJC11, LK17, LNK18b, NDN13, PL16, QMW17, SA12, SGJ18, SZMI13, SCKH10, SKK10, TKHK14, Wan13, WW14, WXK17, XHCH14, XMHD13, YHHS16, ZBR11, ZCL14, ZLDD14, ZHI17].

wiretapping [Lan10]. Wiring [HTZR12].

Wise [CG14a, SSA13]. WISP [PPH12].

Withholding [BR17]. Without

[ASS15, CCL13, FZT14, GSW16, GKS17, LTC15b, NA10a, YLA13, AZH11, B12, BF11, BGV14, CCW10, DCA18, FSX12a, GH11a, GST12, GLM16, HDPC13, ISC16, LLY15, LGWY12, RG10, SYL13, SLZ12, TAK10, WYYY11, XQL11, XHM14, YS12, YKC11, YFK12, ZY17b, ZYM18].

Witness [GGH17]. WLAN [KAHK17].

woman [Fag17]. women

[Hea15, McK10, McK11, McK12, Mun17].

Word [WW12]. Word-Oriented [WW12].

Words [GDM16, KM10a]. Work

[RS11, Shp10, Tay14, BG14, Sch15a].

workbench [CFH13]. workflows [BPP10].

working [Wat14b]. Workshop [MV12, Sen10, Yan11].

Workshops [DTS12]. World

[Ano16b, Ano17d, BFK16, BPS16, FKS13, KM10c, LLL18, MDM17, Tom16, Con12, GLJ12, Goo12, LCKB12, Pet11, Sch15c, Zet14, Mun17]. world-class [Goo12].

Worm [WC11]. Worst [BIKK14].

would [McG11]. Wrapped [KM15, KM16].

Write [LLPY19, YQ15, ZH19].

Write-Efficient [NYQ15]. writing [LT14b].

wrong [LHA12, UK18]. WSN [DL12].

WSNs [ABB19, ZYL10]. Wu [LLL10].

WW2 [Don14]. Wyner [ADG16].


XMSS [BDH11, HRB13, HB19]. XOR

[App13]. XTEA [CP12, IS12]. XTS

[Mar10c]. xviii [Mar10c].

Yamamoto [Car11]. Yan [Cou12]. Yao

[GKS17]. YCbCr [RMG18]. Years

[DR10, BCV12]. Yehuda [Ful10]. Yen

[LLL10]. Yuan [FMS12a]. YubiKey

[Jac16]. Yves [Ter11].

Z [JSM18]. z13 [ACD15]. Zero [AMH16].

Zero-Correlation [BW12, YCL17, WWBC14]. Zero-Cost [AMH16]. Zero-Knowledge [CLP13a, GOS12, IW14, MX13].
REFERENCES

MBC$^+$18, MT12, Pan14, LLM$^+$19, KPP16].
ZIDS [NSMS14]. Zodiac [SDM10]. ZUC [WHN$^+$12].

References

Akyildiz:2014:OTB


Applebaum:2017:AC


Abo-alian:2016:KDB


Ambrosin:2016:FAB


Albertini:2014:MHE

Akleylek:2016:SPM


Aghili:2018:ISA


Abdalla:2010:PCL


Arnold:2012:ICC


Adrian:2015:IFS


Agosta:2015:OPP

REFERENCES

Abe:2010:ACA


Abe:2012:TBG


Abriaga:2012:JSS


Almeida:2014:COS


Ananth:2013:SFP


AlMashrafi:2012:AIM


Applebaum:2010:PKC


Arias-Cabarcos:2015:BIP


Arnold:2015:NGH


Amoah:2016:FMA


Ardagna:2010:ECP

Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela


Aizatulin:2012:VCC


Anyanwu:2010:DCS


Ayday:2012:DAA


Aliberti:2016:RPS


Attasena:2017:SSC


Adikari:2011:HBT

References

Abdalla:2012:LBH

Andrychowicz:2016:SMC

Araldo:2018:CEC

Ahmed:2017:IRD

Attrapadung:2015:RGS

Antonopoulos:2017:DIS
Timos Antonopoulos, Paul Gazzillo, Michael Hicks, Eric Koskinen, Tachio Terachi, and Shiyei Wei. De-

**Akinyele:2014:MGA**


**Abdullaziz:2016:AAI**


**Ali:2018:ECM**

REFERENCES


Applebaum:2014:HGA


Amin:2018:UAP


Alhanahmah:2016:MTI


Azarderakhsh:2014:NDP


Almulla:2013:CKE


Anada:2017:CGS

Hiroaki Anada, Junpei Kawamoto, Chenyutao Ke, Kirill Morozov, and Kouichi Sakurai. Cross-group secret sharing scheme for secure usage of cloud

**Alabdulatif:2017:PPA**


**Afanasyev:2011:PPN**


**Armknecht:2012:STH**


**AlTawy:2013:SOC**


**Aiash:2015:IAA**

REFERENCES

[102x681]REFERENCES

www.sciencedirect.com/
science/article/pii/S1084804514001349

Aldrich:2011:GUS

Richard J. (Richard James)
Aldrich. GCHQ: the un-
censored story of Britain’s
most secret intelligence
agency. HarperPress, Lon-
don, UK, 2011. ISBN 0-
00-727847-0 (hardcover), 0-
00-731265-2 (paperback),
0-00-731266-0 (paperback).
666 + 16 pp. LCCN
JN329.I6 A43 2011; UB251.G7
A54 2010.

Au:2018:PPP

Man Ho Au, Kaitai Liang,
Joseph K. Liu, Rongx-
ing Lu, and Jianting
Ning. Privacy-preserving
personal data operation on
mobile cloud: Chances and
challenges over advanced
persistent threat. Future
Generation Computer Sys-
tems, 79 (part 1)(??):337–
349, 2018. CODEN FG-
SEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167739X17326055.

Alpar:2018:BTA

Orcan Alpar. Biometric
touchstroke authentication
by fuzzy proximity of touch
locations. Future Gen-
eration Computer Systems,
86(??):71–80, September
2018. CODEN FG-
SEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167739X17326055.

Asharov:2013:FCF

Gilad Asharov, Yehuda
Lindell, and Tal Rabin.
A full characterization of
functions that imply fair
coin tossing and ramifica-
tions to fairness. 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_14/.

Awad:2016:SSZ

Amro Awad, Pratyusa
Manadhata, Stuart Haber,
Yan Solihin, and William
Horne. Silent shredder:
Zero-cost shredding for
secure non-volatile main

**Arnedo-Moreno:2010:JRA**


**Arsalan:2012:IRW**


**Ahir:2017:LAR**


**Abbasinezhad-Mood:2018:DHI**


**Adj:2013:WDC**


**Aumasson:2014:HFB**

[AMPH14] Jean-Philippe Aumasson, Willi Meier, Raphael C.-
REFERENCES


Ahmadian:2010:PDS


Alvarez:2012:CAB


Albrecht:2012:SDL


Arshad:2015:SAI


Aga:2017:ISM


Anonymous:2015:BSU


Anonymous:2015:QCS


Anonymous:2015:BRDa


Anonymous:2015:CEB


Anonymous:2015:UGB


Anonymous:2016:CPSd


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

Anon:2017:BRM

Anon:2017:CCS
Anonymous. Cybernetica case study: Solving the Estonian ID-card case. Web news story, December 13, 2017. URL https://cyber.ee/en/news/cybernetica-case-study-solving-the-estonian-id-card-case/. The story describes a poor choice of generating large (about 1024 bits) primes $p$ and $q$ that led to crackable RSA cryptography. The solution for Estonia was to switch to elliptic-curve cryptography that was also supported by the cards.

Anon:2017:HDQ

Anon:2017:MBH

Anon:2017:RV
Anonymous. ROCA vul-
The ROCA vulnerability affects millions of smart-cards, 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 filesytems.

Anonymous:2019:HCC

Anonymous:2019:PBT

Anthes:2014:FTI


REFERENCES

ISSN 0020-0190 (print), 1872-6119 (electronic).

AlFardan:2013:LTB


Ali:2018:SUA


Applebaum:2013:GXG


Applebaum:2014:CCP


Appel:2015:VCP


Al-Qarni:2012:EI1


Arai:2013:MDH


Adj:2014:SRC


AlTawy:2018:TCM


Azarderakhsh:2015:PHS

Ambrose:2012:RI


Asharov:2016:LPI


Artemenko:2017:PGO

|---|---|
Argyropoulos:2010:BTP


Au:2011:PPT


Al-Tariq:2017:SFP


Alam:2015:ACF


Aslan:2016:DEM


Abdalla:2012:LRS

Michel Abdalla and Jill-Jenn Vie. Leakage-resilient spatial encryption. *Lecture Notes in Computer*
REFERENCES


Altaf:2015:LPM


Altaf:2017:LHL


Awad:2017:OLO


AlTawy:2014:IDR


Anzala-Yamajako:2012:RAC


Ahmad:2014:RTN


Awad:2017:OLO

REFERENCES

Aysu:2015:FRT

Ayub:2012:BRB

Apavatjrut:2012:EEA

Alshammari:2011:CET

Alavi:2014:RQE

Barcellos:2018:RSP

Behnia:2013:IEB
[BAAS13] S. Behnia, A. Akhavan, A. Akhshani, and A. Sam-
REFERENCES


Bai:2010:RKI

Bailin:2012:ERG

Berbecaru:2010:FSM

Barbay:2012:BRB
Jérémy Barbay. Book re-


Bennett:2014:QCP

Barenghi:2016:FBS

Boumerzoug:2016:LKM
Hayette Boumerzoug, Boucif Amar Bensaber, and Ismail Biskri. A lightweight key management scheme based on an Adelson-Velskii and Landis tree and elliptic curve cryptography for wireless sensor networks.


Barenghi:2013:FIT

Baldi:2013:ULC
Barak:2014:OEF


Beurdouche:2017:MSU


Beimel:2014:MLS


Bernstein:2017:SRD


Boldi:2012:IUG


Bollman:2015:PWI

REFERENCES

Bernstein:2011:PCI

Basin:2014:KYE

Bocu:2018:HEB

Balagusamy:2019:CA

Bichsel:2012:DMA
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-32805-3_5.

Badrignans:2010:SSA


Balfanz:2012:FA


Bugliesi:2015:ART


Buhrman:2014:PBQ


Bahri:2016:CCO


Bahri:2012:SCS


**Brandenburger:2017:DTC**


**Bernstein:2014:CKR**


**Basin:2012:PRI**


**Basin:2013:PRI**


**Basin:2015:ISC**

REFERENCES

mags/sp/2015/03/msp2015030024-abs.html.

[Bicakci:2013:LSS]

[Botta:2014:PCI]

[Boyle:2014:EO]

[Basso:2011:BWC]

[Bessani:2013:DDS]

[Blasco:2016:SWB]
REFERENCES


REFERENCES

2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Buchmann:2011:XPF


Backstrom:2011:WAT


Bernstein:2011:HSH


Barbareschi:2018:PBH


Bossuet:2011:EPA


Bendlin:2011:SHE

REFERENCES


REFERENCES


[Ber18] Stefano Berretti. Improved audio steganalytic


REFERENCES


**Bhargavan:2016:MVP**


**Beimel:2012:SSS**


**Berger:2016:EGF**


**Boldyreva:2014:MEW**


**Battistello:2012:TBA**

REFERENCES

www.sciencedirect.com/science/article/pii/S1084804512000653

Barthe:2012:CA


Bossuet:2013:AFS


Barak:2012:IPO


Barbulescu:2013:QP


Barbulescu:2014:HQP

Razvan Barbulescu, Pierre Gaudry, Antoine Joux, and Emmanuel Thomé. A

[Barthe:2012:ACA]


[Biswas:2017:STC]


[Borcena:2017:PEE]


[Bhattacharjee:2016:SWC]

Yudhijit Bhattacharjee. The spy who couldn’t spell: a dyslexic traitor, an unbreakable code, and the


[Berman:2013:HPR] Itay Berman, Iftach Hait-
REFERENCES


Bouti:2012:SCB

[102x681] REFERENCES


Bhuyan:2014:DDD


Braun:2012:ULA


Brakerski:2010:OHB


Bogdanov:2013:SDS


Bogdanov:2012:KAC

REFERENCES

Bogdanov:2018:IEA


Bellare:2012:IBL


Bogdanov:2011:BCF


Bibak:2018:AUH

Bernstein:2010:PCA

Byun:2011:SMC

Bai:2012:SSR

Bernstein:2014:HEC

Bidgoly:2015:MQV

Bernstein:2017:SCS

Blanchette:2012:BPC
Jean-François Blanchette. *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age*
REFERENCES

Blaze:2016:UHR

Benzaid:2016:FAW

Bai:2019:LMD

Buchmann:2017:PCU

Buchmann:2018:PCP

Blomer:2012:TKG
Johannes Blömer. Turing und Kryptografie. (German) Informatik Spek-
REFERENCES


Blondeau:2015:IDA


Bernstein:2012:SIN


Birajdar:2013:DIF


Bard:2015:PRO

Gregory V. Bard and Theodore McDonough. Plaintext recovery for one-time pads used twice. ACM Communications in Com-
REFERENCES


Benamara:2016:ICA [BMB16]


Baldwin:2010:AFI [BMBS10]


Biswas:2012:IBA [BMM12]


Babamir:2014:AKP [BN14]


Backes:2012:GCP [BMP12]


Banik:2012:DFA [BMS12]

REFERENCES


REFERENCES


REFERENCES


[BR14] Zvika Brakerski and Guy N. Rothblum. Virtual black-

Brakerski:2013:WHB


Bradbury:2015:BSB


Briggs:2011:SDC


Broemeling:2011:AES


Brook:2017:LSR


Becker:2013:SDL

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

Benaloh:2015:EEV

Josh Benaloh, Ronald L. Rivest, Peter Y. A. Ryan,

Bag:2017:BBW


Bellare:2012:MIS


Brumley:2012:SFI


Bergsma:2012:PAW


Baja:2013:CSE


Birrell:2013:FIM


Bhattacherjee:2014:CAT

Sanjay Bhattacherjee and Palash Sarkar. Concrete

Bagheri:2015:NNA


Boorghany:2015:CIL


Bojinov:2014:NMC


Basin:2011:AIS


Beaulieu:2013:SSF

REFERENCES

plan-for-internet-of-things-rejected-by-international-body/67004/.


REFERENCES


[Bul10b] Stanislav Bulygin. Computer algebra in coding
REFERENCES


REFERENCES


REFERENCES


**Carota:2012:FFI**


**Chou:2010:PSO**


**Checkoway:2016:SAJ**


**Chadha:2012:AVE**


**Chatterjee:2016:TAD**

REFERENCES

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

Chou:2013:UGS


Cao:2019:AML


Chang:2011:SFW


Cascudo:2015:SSN


Chatterjee:2017:PBS


Cho:2014:DGA

Michael Cheng Yi Cho, Pokai Chen, and Shihpyng Winston Shieh. Dmail: A globally authenticated email service. Com-

Chen:2011:EAA


Chu:2014:KAC


Chen:2010:ALD


Chen:2013:WSB


Chiasson:2012:MWB


Cui:2016:RDA

Hui Cui and Robert H. Deng. Revocable and de-


Cao:2012:ITM


Chari:2010:DSC


Cui:2018:ABC


Coras:2016:AML


Costello:2014:CAS


Culnane:2019:KKR

REFERENCES

Ceruzzi:2014:HFT


Cert:2015:CTN


Cert:2018:CSA


Chang-Fong:2016:CSC


Carter:2013:SSA


Centenaro:2013:TBA


Checkoway:2014:PED

[CFN+14] Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Matthew Green,

Cevallos:2012:USR

Carstensen:2011:AAA

Calzavara:2017:SWJ

Celesti:2016:ALT

Choo:2017:EDF
REFERENCES

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

Chang:2010:PRN


Chen:2010:IFA


Camenisch:2012:EAA


Che:2012:WAM


Cheraghchi:2014:NMC


Corrigan-Gibbs:2014:KS

REFERENCES


REFERENCES


**Chappell:2013:PMI**


**Chen:2011:CCI**


**Cheswick:2013:RP**


**Chen:2015:SSS**


**Chen:2017:CSQ**


**Chen:2018:ESA**

Yung-Chih Chen. Enhancements to SAT attack: Speedup and breaking cyclic logic encryption.
REFERENCES


Cui:2019:CPA


Chen:2012:SRF


Chien:2016:GAI

REFERENCES

Chmielowiec:2010:FPR

Choudary:2010:SCD

Chou:2014:EMA

Chur:2016:BEE

Chen:2013:ATK


Cilardo:2011:EPT


Cheng:2013:EHM


Cao:2014:SCI


Cho:2012:CBF


Cho:2015:CBF

Jung-Sik Cho, Young-Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol. Computers and

Chang:2019:GTS


Chandra:2011:AST


Chung:2018:ERN


Chase:2013:SMN


Chuang:2011:LMA

Colin:2016:CTC


Comon-Lundh:2010:DSP


Chang:2011:RSB


Chen:2016:PGF


Chong:2013:ASG


Chen:2016:RPR

REFERENCES

Chen:2013:TSE

Chande:2016:NSC

Cao:2012:SRH

Chen:2019:IBS

Canetti:2013:PCC
Castro:2013:RAM


Chang:2012:PRS


Cui:2016:KAS


Chen:2014:CDP


Cheng:2017:ISK


Cremers:2011:OSV

REFERENCES


[Coles:2016:NAU]

Chakraborty:2015:SSC


Chakraborty:2013:EHI

Chen:2012:FAA

Chen:2017:VME


CNRS:2014:NAS

CNRS. New algorithm shakes up cryptography. *Scientific Computing*, May
REFERENCES

162


Coron:2012:PKC


CNT12

[CO11]


Chin:2011:ACS

Conn:2010:AP


Connitzer:2010:AP


Connolly:2018:FE


Connolly:2018:FE

Copeland:2010:CBG

REFERENCES


REFERENCES

Canard:2018:NTC

Chung:2016:NBB

Chen:2012:DCC

Chevalier:2010:CSC

Chen:2018:RLF

Chevalier:2010:CSC

Chen:2012:DCC

Crampton:2011:PEC
Cramer:2012:TCT

Crav:2014:UCC

Clear:2012:CPA

Crichlow:2016:RSE

Culhane:2015:VVV

Chhabra:2011:NSN
Clark:2012:RLA

Chapin:2014:SRP

Chattaraj:2018:NTS

Chauhan:2018:BBA

Chadwick:2014:AFI

Chen:2013:RWM
Xianyi Chen, Xingming Sun, Huiyu Sun, Zhili Zhou, and Jianjun Zhang. Reversible watermarking method based on asymmetric histogram shifting of prediction errors. The Journal of Systems and Software,

Chen:2017:SIE


Ciegis:2016:ADP


Chong:2015:SID


Chow:2012:EPV


Chen:2018:SIA


Chen:2011:IBT

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

**Chen:2011:ARI**


**Chen:2011:TVS**


**Canard:2018:CPK**


**Calzavara:2015:SLA**


**Chin:2013:SMB**


**Chang:2012:GBP**

Chou:2013:TIB

Crenne:2013:CMS

Calmon:2014:ITM

Choi:2012:LTF

Chung:2012:CBI

Chen:2014:SBB
REFERENCES

170


Chen:2014:DSE


Cao:2014:PPM


Chen:2016:EPN


Chen:2012:IDC


Chen:2012:CKS


Chen:2014:MLC

Long Chen and Zhao Zhang. MemGuard: a

Chen:2015:TCP


Cheng:2015:OMU


Chen:2012:FSD


Chen:2012:AIB


Chen:2012:IBE

REFERENCES

[Refs]

Chen:2014:CSI

Dharwadkar:2010:SSG

Djebbar:2012:ASB

Danezis:2012:FCDb

Davies:2011:IST

Diong:2012:DAU


References

DePrisco:2013:CVC


Datta:2017:SFH


DArco:2014:MIC


Castro:2016:FVB


DaRolt:2013:NDS

REFERENCES


[der10]


DeCapitaniDiVimercati:2010:EPR


DeCapitanidiVimercati:2017:AMM


Deng:2017:LLH


Ding:2012:CLS


Djuric:2015:FSF


Dutta:2017:EFC

Tanima Dutta and Hari Prabhat Gupta. An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC)-encoded video. *ACM Transactions on Multimedia Computing, Communi-
REFERENCES


Dupressoir:2014:GGP


Ding:2012:NRR


Drimer:2010:DBP


Dubeuf:2016:EPA


Dodis:2010:CA


Driessen:2013:ESA

REFERENCES


Delfs:2015:ICP


Delimitrou:2016:SID


Dorre:2016:ELO


Doychev:2017:RAS


Durumeric:2014:MH


Dolev:2016:MCG

Shlomi Dolev, Ephraim Korach, Xinming Li, Yin Li, and Galit Uzan. Magnifying computing gaps: Establishing encrypted communication over unidirectional channels. Theoretical Computer Science, 636(??):17–26, July 11, 2016. CODEN TCSDFX. ISSN 0304-3975
Doychev:2015:CTS

Dodos:2012:MAR

Dunkelman:2012: MCE

Dong:2012:UAS

DeLuca:2015:SUS

Degefa:2016:PSE
Fikadu B. Degefa, Donghooon Lee, Jiye Kim, Younsung Choi, and Dongho Won.


[Duan:2016:SDC] Li Duan, Dongxi Liu, Yang Zhang, Shiping Chen, Ren Ping Liu, Bo Cheng, and Junliang Chen. Secure


REFERENCES


[Donovan:2014:ATM]


[Doroz:2015:AFH]


[Duncan:2012:CAI]


CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-28879-1_5/.

[Ding:2017:CSM]


[Das:2016:CWM]


[Dziembowski:2018:NMC]

References


REFERENCES

https://www.computer.org/csdl/mags/sp/2016/06/msp2016060043-abs. [DSB15]


REFERENCES

www.sciencedirect.com/science/article/pii/S1084804512000926


REFERENCES

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Reference</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Volume</th>
<th>Number</th>
<th>Pages</th>
<th>Publisher</th>
<th>ISBN</th>
<th>ISSN</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dunkelman</td>
<td>2012</td>
<td>MEK</td>
<td>Lecture Notes in Computer Science</td>
<td>2012</td>
<td>7668</td>
<td>16</td>
<td></td>
<td>CODEN LNCS9D9</td>
<td>0302-9743</td>
<td>1611-3349</td>
<td></td>
</tr>
<tr>
<td>Durcheva</td>
<td>2015</td>
<td>SAI</td>
<td>ACM Communications in Computer Algebra</td>
<td>2015</td>
<td>49</td>
<td>1</td>
<td>19</td>
<td>CODEN ?????</td>
<td>1932-2232</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dorn, Wackersreuther, Böhm</td>
<td>2012</td>
<td>ECE</td>
<td>Lecture Notes in Computer Science</td>
<td>2012</td>
<td>7494</td>
<td>129-142</td>
<td></td>
<td>CODEN LNCS9D9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


REFERENCES


[DZ14] Lunzhi Deng and Jiwen Zeng. Two new identity-based threshold ring sig-


Ekberg:2012:AEP


Ehdaie:2016:HCR


Esiner:2017:QRI


Esiner:2019:TFA


Egele:2013:ESC


Edwards:2014:NRP

REFERENCES

Edwards:2017:NSQ

El-Emam:2013:NSA

Eisenbarth:2012:CIP

Esiner:2016:FFB

Engels:2013:NLL


ElBansarkhani:2012:ELB


Embar:2014:PWO


Evtyushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC

REFERENCES

Engels:2012:HLA

Ebadi:2015:DPN

Essex:2017:DDU

Everett:2012:EC

Everett:2016:SES

Eibach:2010:OGB


Farash:2014:CIE

Fay:2016:ICM

Fischlin:2012:PKC

Ferretti:2014:DCI

Fuglerud:2011:SIA
Fehr:2010:QC


Feigenbaum:2019:PSE


Feltten:2013:LBA


Faugere:2010:CLR


Fleischmann:2012:MFA


Feng:2010:CTS

REFERENCES

Farras:2012:LTM

Faugere:2014:MCA

Fan:2013:CPP

Fan:2010:PSN

Fan:2010:AMI

Fan:2017:SSP


REFERENCES


Giulia Fanti, Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Spy vs. spy: Rumor source obfuscation. *ACM SIGMETRICS Performance Evaluation Re-

Fehr:2013:FCC


Fan:2013:CEM


Fan:2014:RRS

Kai Fan, Jie Li, Hui Li, Xiaohui Liang, Xuemin (Sherman) Shen, and Yintang Yang. RSEL: revocable secure efficient lightweight RFID authen-


Ferguson:2010:SHF


Forler:2012:DAC


Feng:2012:CAO

Hui Feng, Hefei Ling, Fuhao Zou, Weiqi Yan, and Zhengding Lu. A collusion attack optimization strat-


Fraczek:2012:MSI


Fernandez-Mir:2012:SRA


Ferreira:2015:LPA


Fu:2018:LUA


Fokkink:2012:TCG


Folger:2016:TQH

REFERENCES


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


P. Mohamed Fathimal and

[Fri10a]


[Fra15]


[Fra16]


[Fre10]


[Fri10b]


[Fri12]


FEserguson:2010:CED

[FSK10]

Feng:2011:GDA

[FSWF11]

F:2012:SHI

[FSX12a]

F:2012:SEI

[FSX12b]

F:2012:SEP

[FSX12c]

Fadlullah:2010:DCA
Zubair M. Fadlullah, Tarik Taleb, Athanasios V. Vasilakos, Mohsen Guizani, and Nei Kato. DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis. IEEE/ACM
REFERENCES


[Feng:2013:ECE] Jun Feng, Xueming Wang, and Hong Sun. Efficiently computable endomorphism for genus 3 hyperelliptic curve cryptosystems. Information Process-
REFERENCES


REFERENCES

(GomezPardo:2013:ICM)

José Luis Gómez Pardo. 
Introduction to Cryptography with Maple. 
Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2013.

(Gross-Amblard:2011:QPW)


(Gregio:2015:TTM)


(Gope:2018:LPP)


(Galindo:2013:NIC)


(Gasarch:2013:RBC)

William Gasarch. Review of Theoretical Computer Science: Introduction to Automata, Computability,


J. Guerra-Casanova, C. Sánchez Ávila, A. de Santos Sierra, and G. Bailador

Granado-Criado:2017:HCH


[GCVR17]

Gong:2016:ATI


[GDCC16]

[Gen10]

Gentry:2010:CAF


[Gen13]

Gentry:2013:EMH

Craig Gentry. Encrypted messages from the heights.

[GdM16]


[Gel13]

Geller:2013:MIS

Gaspar:2012:SEF


Garg:2016:CIO


Garg:2016:HSS

Sanjam Garg, Craig Gentry, Shai Halevi, Marianna 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
REFERENCES


REFERENCES

Gilad:2014:PHI

Gilbert:2010:ACE

Gir15

Gao:2013:LCA

Giry:2015:BCK

Gj13

Gu:2015:EIB


GJJ15

Gravier:2015:WOD


GJMP15

Goyal:2013:CZK


Gu:2017:IBM


Geetha:2011:VRN

Garay:2016:MPA

Grigoriev:2017:YMP


Gaj:2017:DCR


Guo:2010:HMW


Gouveia:2012:HSI


Guo:2018:KAA


Gorawski:2012:EAS

Gligor:2012:SLT


Gollmann:2010:SCR


Guo:2011:EDA


Guo:2018:PSC


Guo:2014:SAS


Gao:2014:URA


Groza:2017:LCL


Gong:2012:KNF


Garay:2017:SIA

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


Michael T. Goodrich, Charalampos Papamanthou, Duy Nguyen, Roberto Tamassia, Cristina Videira Lopes, Olga Ohrimenko, and Nikos Triandopoulos. Efficient verification of web-content searching through authenticated web


Daniel Genkin, Itamar Pipman, 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/.


story-of-extended-random/. Discussion of suspected NSA-supported back door in the 2007 NIST standard for the Dual Elliptic-Curve default random number generator, and the associated RSA cryptographic library BSAFE. There is evidence that the back door exists in some older Canon laser printers.

**Grimes:2015:CCT**

**Gibson-Robinson:2012:AAL**

**Guha:2017:RTS**

**Guin:2016:FCS**

**Gong:2016:FSC**

**Gierlichs:2012:ICD**
Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall. Infective computation and dummy rounds:

**Genkin:2013:RKE**


**Ge:2016:KPA**


**Gazi:2012:EOS**


**Gupta:2019:LAU**


**Goodrich:2011:EAD**

Michael T. Goodrich, Roberto Tamassia, and Nikos Triandopoulos. Efficient authenticated data structures for graph connectivity and geometric

**Grosse:2013:AS**


**Gueron:2016:MEG**


**Gupta:2015:GEM**


**Gorbunov:2012:FEB**

Gorbunov:2015:ABE

Greenberg:2014:GWB

Gebotys:2016:PCP

Wang:2014:RA

Gao:2015:GCC
Guo:2012:AKE


Guo:2017:EMD


Guo:2019:NTP


Ge:2013:SAP

Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang. Secu-


[Ham17] Nathan Hamlin. Number in mathematical cryp
tography. *Open Jour-


Harn:2013:GA

Harrington:2014:GEF

Hardesty:2015:BA

Hardesty:2016:SUC

Hastings:2016:SWS

Hayes:2013:NSA

Houmansadr:2013:BCN

Hurlburt:2014:BBC

Hetzelt:2017:SAE
[HB17] Felicitas Hetzelt and Robert Buhren. Security anal-
Hernandez-Becerril:2016:GIS


Han:2019:ABI


He:2013:HEH


Hulsing:2017:XEH


Hao:2012:SAM


Hu:2017:ATE

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


Hernandez-Castro:2012:MTA


Hsu:2011:WLC


Hernandez-Castro:2012:AFH


Han:2013:RMA

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

Heninger:2012:MYP


Heath:2015:HNS


Hwang:2012:ABA

REFERENCES


Hamad:2018:DWU


Hellman:2017:TLC


Hermelin:2010:MLC


Herranz:2014:ABS


Herardian:2019:SUC


Hess:2012:GJC


Heys:2017:SCF

Howard M. Heys. Statistical cipher feedback of stream ciphers. The Computer Journal, 60
REFERENCES


Harn:2014:MTS [HF14a]

Hoang:2014:IMD [HF14b]

Huang:2016:EDP [HGT15]

Heyse:2012:TOC [HG12]

Hua:2015:TSE [HGWY11]

Han:2011:PEB [HGWY11]
Yiliang Han, Xiaolin Gui, Xuguang Wu, and Xiaoyuan Yang. Proxy encryption based secure multicast in wireless mesh networks. Journal of Net-
Harn:2015:DTS


Hu:2016:EWS


Hayashi:2013:AEI


Huber:2014:TPW


Huang:2017:BBC


Haitner:2011:PRI

Hinarejos:2015:MES


Hinkleman:2011:CPA


Hur:2014:SDR


Hussain:2018:PPP

Siam Umar Hussain and Farinaz Koushanfar. P3: Privacy preserving positioner for smart automotive systems. ACM Trans-

Houmansadr:2014:NWB

Hur:2013:REC

Heyse:2012:LEA

Heil:2014:APH

Howe:2018:PDG

Holenstein:2011:ERO
Thomas Holenstein, Robin Künzler, and Stefano Tes-
REFERENCES


Hu:2012:VMS


Hu:2016:PBR


Hu:2018:SV5


Huang:2011:ISL


Huang:2015:MSE

(print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2461.


[Howard:2010:DSS] Michael Howard, David LeBlanc, and John Viega. 24 deadly sins of software security: program-
REFERENCES

Hohenberger:2012:DDQ

Huang:2014:SWC

Hefeeda:2010:ASM

Herzberg:2012:TJA

Hwang:2019:BBR

Hore:2012:SMR
Bijit Hore, Sharad Mehrotra, Mustafa Canim, and Murat Kantarcioglu. Secure multidimensional range queries over outsourced data. *VLDB Journal: Very Large Data Bases*, 21(3):
REFERENCES


Hoa:2012:ESB


Hir:2014:BA


Har:2010:CIC

Danny Harnik and Moni Naor. On the compressibility of\begin{math}N\end{math}/\begin{math}P\end{math} instances and cryptographic applications. SIAM Journal on Computing, 39(5):1667–1713, 2010. CODEN: SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hof:2015:LBQb


Hof:2016:LBQb


Hol:2012:CCE


Hor:2019:CPE

G. Horsman. A call for

Hyla:2012:CBE

Hazay:2014:OSA

Halder:2010:WTR

He:2012:ECT

Howe:2015:PLB

Hur:2010:CCS
Junbeom Hur, Chanil Park, and Hyunsoo Yoon. Chosen ciphertext secure authenticated group com-


[Han:2016:GGA] Han:2016:GGA


[He:2013:GME] He:2013:GME


IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2014.
ISBN ?? LCCN ??
URL ??.

Hussain:2018:SSH

Herranz:2013:SMS

Hulsing:2016:MMT

Haitner:2010:EIC

Hwang:2011:CDA

Hubballi:2018:NTC
[NHM18] Neminath Hubballi and Mayank Swarnkar. Bit-Coding: Network traffic classification through encoded bit level signa-
REFERENCES


REFERENCES

Ho:2011:EIB


Shi:2015:CTS


Hamdy:2011:HPB


Henson:2013:MES


Hu:2010:TTW


Huang:2015:PAP


Huang:2017:SSS

Kaibin Huang, Raylin Tso, and Yu-Chi Chen. Some-

Herbert:2012:SMP

Hald:2015:RRA

Hulsing:2013:WOS

Hurlburt:2016:MBO

Harvey:2017:FPM

Han:2012:MIA
Fengling Han and Ron van Schyndel. M-identity and its authentication protocol for secure mobile commerce applications. *Lecture Notes in Computer Science*.
REFERENCES


[HWDL16] Kai He, Jian Weng, Robert H. Deng, and Joseph K. Liu. On the security of two identity-based conditional proxy re-


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

[HYS11]


[HYS18]


[HYS18]

Qinlong Huang, Yixian Yang, and Mansuo Shen. Identity-based designated


[HYS11]


[HYS11]

Qinlong Huang, Guomin Yang, Duncan S. Wong, and Willy Susilo. Identity-based strong designated


[HYS11]


[IAD10] I. A. Ismail, M. Amin,

**Islam:2011:MES**


**IBM:2013:DMP**


**IBM:2013:IPC**


**Irshad:2017:CPP**


**IEEE:2010:PIA**


**IEEE:2011:ICI**

IEEE, editor. *International Conference on Intel-
REFERENCES


[IEEE:2011:PIA]


[IEEE:2013:PIS]


[IEEE11b]


[Imanimehr:2016:HPR]


[Islam:2011:MDA]


[Iyengar:2016:SPS]
Imai:2015:IRR


Islam:2015:LFP


Ioannou:2014:PKC


I:2017:ETB


Isobe:2012:SCL


Islam:2018:REP

[IOV+18] SK Hafizul Islam, Mohammad S. Obaidat, Pandi Vijayakumar, Enas Abdulhay, Fagen Li, and M. Krishna Chaitanya Reddy. A robust and effi-

**Isobe:2012:SAL**


**Irshad:2016:EAM**


**Ishai:2014:PCP**


**Jacobs:2016:STB**


**Jie:2010:AAI**

REFERENCES


Jho:2016:SSE


Prins:2011:DCA


Jho:2016:SSE

REFERENCES


**Jeong:2013:CBC**


**Jo:2014:ODE**


**Jia14a**


**Jing:2012:MVB**


**Jiang:2019:SSL**


**Jiang:2014:UIS**


Jun:2012:IIR


Jiang:2016:PPT


Jovanovic:2012:FAL


Josefsson:2016:ECD


Jordan:2018:QCS


Jeong:2012:IKP

Kyung Chul Jeong, Dong Hoon Lee, and Daewan Han. An

Jajo:2012:RET


Jia:2012:PKD


Jiang:2016:OOC


Jiang:2016:UTC


Jain:2012:BAS


Jaiyeola:2018:IPN


Jevdjic:2017:ASC


Jain:2016:APQ


Judson:2017:BCI


Jordan:2018:EPE

REFERENCES


[JTW14] Ari Juels and Bonnie Wong. The interplay of

**Jiang:2017:SLD**

**Jin:2015:NCD**

**Jouxs:2014:SAC**

**Jiang:2010:EDI**

**Khazaei:2017:COA**


**Karafyllidis:2012:QGC**  

**Kong:2015:CSM**  

**Katz:2013:RIB**  

**Kawamoto:2015:LSH**  

**Karthigaikumar:2010:PPV**  

**Kallel:2011:SMM**  

**Kleinrouweler:2017:SAP**  
Jan Willem Kleinrouweler, Sergio Cabrero, and Pablo Cesar. An SDN ar-

Kim:2011:SSE


Koz:2012:ASE


Kraetzer:2012:PCS


Karakoc:2013:BCL


Karakoc:2015:AKA


Kumari:2017:DSU

Saru Kumari, Ashok Kumar Das, Mohammad

Kara:2019:ALS


Keblusek:2015:BRK


**Kastner:2010:AOT**

**Kim:2014:MBM**

**Khalil-Hani:2013:BEB**

**Kim:2016:EPE**

**Kai:2011:CIS**

**Kiayias:2011:TCC**
REFERENCES

Kompara:2019:REM


Kim:2011:LBA


Kim:2015:CEH


Konstantinou:2010:RCI

Elisavet Konstantinou and Aristides Kontogeorgis.

Kim:2016:MAS


Khan:2016:BSW

REFERENCES


**Kawai:2012:SHS**


**Kawai:2013:SHS**


**Khalil:2014:CIM**


**Khan:2015:CMB**


**Khan:2014:MEK**

Karopoulos:2010:FIP


Kubota:2016:SAV


Khan:2013:EDC


Khan:2014:IPR


Kushwah:2011:EIB

Khakpour:2013:ITA


Klapper:2010:PSS


Ko:2010:MME


Koeberl:2012:EPD


Kumari:2016:UFM


Kim:2012:INS


Keller:2010:DAS


Khomejani:2010:PCT


Koblitz:2010:BNW


Kiani:2011:MPD


Kifer:2014:PFM


Koblitz:2015:RWE

Neal Koblitz and Alfred J. Menezes. A riddle wrapped in an enigma. Report, ????.
Koblitz:2016:RWE

Kasamatsu:2012:TSE

Karger:2011:LLB

Kiyoshima:2014:CRB

Kline:2018:CAR


REFERENCES

Kasper:2012:SCA

Khamsemanan:2016:BBU

Kawachi:2017:GCR

Kollmitzer:2010:AQC

Kang:2012:AKM

Kolman:2017:SCG
REFERENCES

sign of secure authentication scheme between devices based on zero-
knowledge proofs in home automation service envi-
nvironments. The Journal of Supercomputing, 72
(11):4319–4336, November 2016. CODEN JOSUED.
ISSN 0920-8542 (print), 1573-0484 (electronic).

Keskinarkaus:2010:IWD

[KPS10] A. Keskinarkaus, A. Pramila,
and T. Seppänä. Image watermarking with a
[ Kra12] directed periodic pattern
to embed multibit mes-
sages resilient to print-
scan and compound at-
tacks. The Journal of Sys-
tems and Software, 83(10):
1715–1725, October 2010.
CODEN JSSODM. ISSN
0164-1212.

Krenn:2013:CCR

[KPW13] Stephan Krenn, Krzysztof
Pietrzak, and Akshay Wa-
dia. A counterexample to
the chain rule for condi-
tional HILL entropy. Lecture
Notes in Computer Sci-
CODEN LNCSDI. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-3-
642-36594-2_2/.

Knudsen:2011:BCC

[KR11] Lars R. Knudsen and
Matthew J. B. Robshaw.

Kranetz:2012:EAM

[KRDH13] S. R. Kannan, S. Ramthi-
lagam, R. Devi, and

The Block Cipher Compan-
ion. Information Security
and Cryptography. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc., 2011.
ISBN 3-642-
17342-X (e-
book). ISSN 1619-7100
(print), 2197-845X (elec-
LCCN QA76.9.A25 K58
2011; QA76.9.D35.


Sachin Kumar and Rajendra Kumar Sharma. Random-grid based region

References:

**Karthiga:2018:PSA**

**Kocabas:2016:ESM**

**Khan:2017:TPK**

**Kiljan:2017:SAC**

**Kwon:2018:EIP**

**Kim:2012:SSS**
Cheonshik Kim, Dongkyoo Shin, Dongil Shin, and Ching-Nung Yang. A

**Klingler:2013:UPT**


**Kim:2012:SAH**


**Kawachi:2012:SKE**


**Kobayashi:2016:ASC**


**Klisowski:2012:CCP**

Kai:2014:FSD


Kupcu:2013:DTT


Kupcu:2015:OAS


Kuznetsov:2011:APP


Kshetri:2018:BEV


Kiljan:2018:ETA


Karpovsky:2014:DSS

M. Karpovsky and Zhen Wang. Design of strongly secure communication and computation channels by nonlinear error detecting codes. *IEEE Transactions on Computers*, 63


REFERENCES

blogspot.com/2013/01/enhancing-digital-certificate-security.html.

Landau:2017:LCI
[102x681]

Launchbury:2012:TBC
[102x681]

Lauter:2017:POL
[102x681]

Liu:2013:PAE
[102x681]

Luo:2012:ESI
[102x681]
Jianqiang Luo, Kevin D. Bowers, Alina Oprea, and Lihao Xu. Efficient software implementations of large finite fields GF(2^m) for secure storage applications. ACM Transactions on Storage, 8(1):2:1–2:??, February 2012. CODEN ????. ISSN 1553-3077 (print), 1553-3093 (electronic).

Lupu:2012:IBK
[102x681]

Lu:2013:CSA
[102x681]
Linzhen Lu and Shaozhen Chen. A compress slide attack on the full GOST block cipher. Informa-
REFERENCES


REFERENCES


Li:2015:NAC


Lee:2017:SUE


Liu:2017:GAU


Li:2015:CEH


Li:2017:RNF


Li:2017:CCF

Jenny S. Li, Li-Chiou Chen, John V. Monaco, Pranjal Singh, and Charles C.

[Liang:2014:CCS]

[Liu:2016:NOP]

[Louc:2013:WMR]
[Lotz:2015:SCS]

[Launchbury:2012:ELT]

[Liu:2019:DVP]

J. Lago-Fernández, F. Gil-Castiñeira, F. J. González-Castaño, and A. Román-

**Liu:2016:LCR**


**Liang:2015:CPA**


**Li:2018:CIC**


**Liu:2017:ECC**

[LGJ+17] Z. Liu, J. Groschäd, Z. Hu, K. Järvinen, H. Wang, and I. Ver-


REFERENCES

296


[LH16] Daniel J. Lum, John C. Howell, M. S. Allman, Thomas Gerrits, Varun B. Verma, Sae Woo Nam,


REFERENCES

Li:2018:OPP

Lian:2014:SSA

Lin:2015:CND

Liu:2012:ESS

Li:2010:PAP

Li:2017:AMA
Xiong Li, Maged Hamada Ibrahim, Saru Kumari, Arun Kumar Sangaiiah, Vidushi Gupta, and Kim-Kwang Raymond Choo. Anonymous mutual authentication and key agreement scheme for wear-

Lim:2011:NAN


Lin:2014:IVW


Lin:2015:DVS


Lindell:2017:TFC

REFERENCES

Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP


Li:2017:MMR


Liu:2019:ICA


Li:2016:IRI


Li:2017:SQS

Songbin Li, Yizhen Jia, and C.-C. Jay Kuo. Steganalysis of QIM steganography in low-bit-rate speech signals. *IEEE/ACM*
REFERENCES


Li:2012:OEA


Laszka:2014:STC


Liu:2017:OOA


Liu:2018:PAB


Li:2012:BIB


[LL16a] Yang Lu and Jiguao Li. A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds. Future Generation Computer Systems, 62(??):140–147, September 2016. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115


Lyu:2018:PKE


Li:2012:RIB


Liu:2018:GEI


Liu:2019:SBC


Li:2017:CIS


Liu:2017:CCD

[LLL+17b] Tong Li, Zheli Liu, Jin Li, Chunfu Jia, and Kuan-Ching Li. CDPS: A cryptographic data publishing system. *Journal of Computer and System Sciences*, 89(??):80–91, November 2017. CODEN JCSSBM. ISSN 0022-


**REFERENCES**


[Luo:2012:FSI] Xiangyang Luo, Fenlin Liu, Chunfang Yang, Shiguo

Lee2015:SAS


Li2018:WMH


Lu2012:BBE


Lai2016:GGB


Li2017:CBS

[LLZ+17] Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su, Liang He, Kui Ren, Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su, Liang He, and Kui Ren. Capability-based security enforcement in named data network-
Lambert-Mogiliansky:2012:EI [LMB12]

Le:2016:ADS [LMD16]

Lai:2018:IBB [LMG+18]
REFERENCES

Lv:2013:NTP

Lukasiewycz:2016:SAO

Li:2018:RBB

Liu:2013:ESC
Xiong Li, Jianwei Niu, Muhammad Khurram Khan, and Junguo Liao. An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications, 36*(5):1365–1371, September 2013. CODEN JN-
REFERENCES


[Lopriore:2012:EPP] Lanfranco Lopriore. En-


REFERENCES

Lian:2015:GRG


Liu:2017:HPI


Lampe:2012:ATS


Liu:2015:GTB


Liu:2016:PPO


Libert:2010:KES

Lubicz:2015:GMA [LR15]

Lukowiak:2014:CEB [LRV14]

Liskiewicz:2013:GBS [LRW13]

Liskiewicz:2017:SLS

Lane:2014:PBD [LSBN14]

Luo:2012:FSU [LSC12]
REFERENCES

Lin:2015:SSE

Lychev:2016:RSI

Lee:2012:IBS

Liang:2015:EFC
REFERENCES


REFERENCES

com/chapter/10.1007/978-3-642-32009-5_2/.

Lee:2013:CCM


Le:2014:IMX


Lee:2014:NDH


Liu:2015:IMB


Liu:2015:MSG


Li:2015:FSC

Jiguo Li, Huiyun Teng, Xinyi Huang, Yichen
REFERENCES


REFERENCES

Luccese:2010:RPT

Lafitte:2011:CBF

Liu:2010:CIE

Lee:2011:A

Lewko:2011:D
DEN LNCS 9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/content/pdf/10.1007/
978-3-642-20465-4_31.

**Lewko:2011:UHA**

978-3-642-20465-4_30.

**Lewko:2012:NPM**


**Liu:2013:TIE**


**Lui:2013:CBS**


**Liu:2016:PAB**

Zhen Liu and Duncan S. Wong. Practical attribute-based encryption: Traitor

[Li:2018:SCM]


[Liu:2011:SBA]


[Lu:2012:HOM]


[Lu:2014:HOM]


Lou:2010:NAS


Luo:2012:ICB


Lin:2010:DSM


Li:2011:NIA


Li:2014:IBD

Li:2014:EMK


Luo:2014:ARP


Liu:2015:SDS


**Lu:2014:DAN**


**Liao:2010:MPC**


**Liu:2015:SAA**


**Liao:2012:NSM**


**Liu:2018:SKR**


**Li:2013:SSS**

Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and secure sharing of personal


REFERENCES

Li:2010:PES


Li:2012:ESS


Li:2016:BMA


Masdari:2017:STA


MacCormick:2012:NAC


Macrakis:2014:PLS


REFERENCES


Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP


Matthiessen:2019:RCM


Maurer:2012:CCN


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume/Issue</th>
<th>Page Range</th>
<th>Year</th>
<th>DOI/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migliore:2018:PPF</td>
<td>Vincent Migliore, Guillaume Bonnoron, and Car-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Sinclair McKay. The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there. Gardners Books, 2011. ISBN 1-84513-633-0. ?? pp. LCCN ????


Mansouri:2012:ACA

Mansfield-Devine:2015:MIC

Murdoch:2010:CPB

Mosenia:2017:PTS

Maachaoui:2012:MLA

Meiklejohn:2010:BRB
SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [?].

**Menezes:2013:IPB**


**Menn:2013:ESC**


**Meshram:2015:EIB**


**Mandal:2016:DIW**


**Moreno:2013:NIP**


**Moufek:2015:MCB**


**Misoczki:2019:TPS**

R. Misoczki, S. Gulley, V. Gopal, M. G. Dixon,

**REFERENCES**

**Marmol:2010:TPA**


**Matsuda:2014:CCS**


**Mou:2013:CBC**


**Mohd:2015:SLB**

Bassam J. Mohd, Thaier Hayajneh, and Athana-
REFERENCES


Mohd:2018:HDM


Michiels:2010:OWB


Michael:2016:RNI


Midgley:2010:SEE


Martinez-Julia:2012:NIB

Martinez-Julia:2013:BSI


Muller:2012:HPC


Mohanty:2011:RTP


Moessner:2012:SAS


Mozaffari-Kermani:2017:FDA


McGrew:2016:SMH

REFERENCES

Malik:2012:AIC


Marconato:2013:VLC


Montecchi:2012:QSE


Mancillas-Lopez:2010:RHI

Mendez:2016:PES


Manzanares-Lopez:2012:ICU


Ma:2017:LBI


Madhusudhan:2012:DIB


Meshram:2013:IBC


**Mondal:2014:DSM**


**Maity:2017:ODC**


**Mulholland:2017:DCD**


**Moldovyan:2012:BBD**


**Mahmoody:2014:PPK**


**Marino:2019:ACN**

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


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


REFERENCES

Mizuki:2011:ASN

Maimut:2012:LCR

Minamoto:2014:BDI

Mone:2013:FPE

Moore:2012:RFF

Moody:2014:DMW

Morad:2012:OEA
Mosca:2018:CEQ


Moulick:2015:RDS


Minier:2012:EEC


Min:2018:AAB


Meiklejohn:2016:FBC


Mundhenk:2017:SAN

Philipp Mundhenk, Andrew Paverd, Artur Mrowca, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, and Samarjit Chakraborty. Security in automotive networks:


Migliore:2018:HSC


Martinovic:2017:AUP


Matsumoto:2017:ACG


Moghadam:2010:DRN


Mendel:2012:DAL

Maitra:2012:NAC


Mroczkowski:2012:CAS


Maitra:2013:DSM


Maitra:2013:HEM


Maitra:2013:HPM


Miller:2016:RPS


Mukherjee:2017:EPP

Srilekha Mukherjee and Goutam Sanyal. Enhanced position power first mapping (PPFM) based image steganography. *Inter-
REFERENCES


Muhammad:2018:ISU


Miret:2018:PBC


Mosca:2013:QKD


Mouris:2018:TSB


Malkin:2011:ECS

Tal Malkin, Isamu Teranishi, and Moti Yung. Efficient circuit-size independent public key encryption with KDM security. *Lecture Notes in
Meerwald:2012:ERW

Muftic:2016:BCC

Mundy:2017:CGU

Murphy:2010:BRB

Murdoch:2016:IDP

Miri:2012:SAC


K. Preetha Mathew, Sachin Vasant, Sridhar Venkatesan, and C. Pandu Ran-


[MZA+13] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu


REFERENCES


[NB13] Ruchira Naskar and Rajat Subhra Chakraborty. A generalized tamper lo-

Naranjo:2013:FDA


Ni:2013:EIB


Narasimhan:2013:HTD


Ngo:2017:CSS


Nedjah:2016:PYP


[NKWF14] Thanhvu Nguyen, Deepak Kapur, Westley Weimer, and Stephanie Forrest. DIG: a dynamic invariant generator for polynomial and array invari-

**Ning:2012:DPB**


**Ning:2012:DCA**


**Ning:2012:DQB**


**Nieto:2013:PV**


**Nieto:2014:FSH**


**Nguyen:2012:DQB**

[NN12] Anh P. Nguyen and Thuc D. Nguyen. Determining quality of S-

Neville-Neil:2015:KVH

Nagy:2010:KDV

Navin:2010:ETU

Nose:2011:SW

Nose:2014:SWS

Novotny:2010:TAE
Martin Novotny. Time-
area efficient hardware architectures for cryp-
tography and cryptanal-
ysis, volume 12 of IT-
Security. Europäischer
Universitätsverlag, Bochum,
Germany, 2010. ISBN 3-
89966-351-9. xxvi + 194
pp. LCCN ???.


[NR12] Long Hoang Nguyen and A. W. Roscoe. Short-
output universal hash func-
tions and their use in fast and secure data authenti-
cation. Lecture Notes in Computer Science, 7549:
3-642-34047-5_19/.


REFERENCES


[184x551]Nguyen:2010:LAS


[NV10]

[184x586]Nie:2013:CHB


[NXB13]

[184x594]Nie:2013:CHB


[NXB13]

[184x610]Natgunanathan:2017:PBM


[NXH+17]


Andrew Newell, Hongyi Yao, Alex Ryker, Tracey Ho, and Cristina Nita-Rotaru. Node-capture resilient key establishment in sensor networks: Design space and new pro-
REFERENCES


Niu:2015:NAS


Nikooghadam:2010:EUE


Obana:2011:AOC


Olgieri:2011:REA


Obrenovic:2012:IUC


Oggier:2011:ACA

REFERENCES

Obrien:2012:EPM


Onica:2016:CPP


Oliynykov:2015:NES


Ou:2010:CPA


Ogiela:2018:EBI


Oliveira:2012:STA

Ogiela:2010:UML

Ohtake:2012:AAH

Ogiela:2018:LTC

Orlandi:2014:SCN

Oppliger:2011:CC

Orejel:2014:E
REFERENCES


Okamoto:2012:AAH


Otmani:2010:CTM


Ogiela:2018:VCA


Ohzeki:2012:NWM


Ortiz-Yepes:2014:BSA


Praba:2010:MAC

V. Lakshmi Praba and
REFERENCES


REFERENCES

openurl.asp?genre=article&
issn=0920-8542&volume=62&issue=1&page=105. [PB12]

Pass:2013:USP

[Pas13a] Rafael Pass. Unprovable security of perfect
NIZK and non-interactive
non-malleable commit-
ments. Lecture Notes in
Computer Science, 7785:
334–354, 2013. CO-
DEN LNCS9D. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-36594-2_19/. [PB1]

Pranata:2013:MDR

[PAS13b] Ilung Pranata, Rukshan
Athauda, and Geoff Skin-
ner. Modeling decentralized reputation-based trust
for initial transactions in
digital environments. ACM
Transactions on Internet
Technology (TOIT), 12(3):
8:1–8:??, May 2013. CO-
DEN ????? ISSN 1533-5399
(print), 1557-6051 (elec-
tronic).

Paulson:2010:SDO

Steganography development offers promise. Computer,
ISSN 0018-9162 (print),
1558-0814 (electronic).

Pandit:2012:EFS

Tapas Pandit and Rana
Barua. Efficient fully se-
cure attribute-based en-
cryption schemes for gen-
eral access structures.
Lecture Notes in Com-
puter Science, 7496:193–
214, 2012. CODEN
LNCS9D. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer.com/chapter/1
10.1007/978-3-642-33272-
2_13/.

Poh:2017:SDV

Geong Sen Poh, Vishnu Monn
Baskaran, Ji-Jian Chin,
Moesfa Soheila Mohamad,
Kay Win Lee, Dhar-
madharshni Maniam, and
Muhammad Reza Z’aba.
Searchable data vault: En-
crypted queries in secure
distributed cloud storage.
Algorithms (Basel), 10
(2), June 2017. CODEN
ALGOCH. ISSN 1999-
4893 (electronic). URL
https://www.mdpi.com/
1999-4893/10/2/52.

Park:2014:FRI

Jeong Soo Park, Ki Seok
Bae, Yong Je Choi, and
Doo Ho Choi. A fault-
resistant implementation
of AES using differential
bytes between input and
output. The Journal of Su-
percomputing, 67(3):615–
634, March 2014. CO-

Pun:2014:GIT


Paul:2016:TSO


Poh:2017:SSE


Papadopoulos:2014:LQA


Premnath:2014:EHR


Pang:2014:PPA

REFERENCES

September 2014. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Paul:2012:KSS


Pereira:2015:PKE


Pippal:2012:SVU


Persichetti:2013:SAH


Peterson:2011:SWS

Heather R. Peterson. The shape of the world: the story of Spanish expansion and the secret science of cosmography. *Studies in
Petrlic:2012:PRE


Peinado:2012:CAT


Peng:2010:SFW


Park:2012:IDF

References

Notes in Computer Science, 7690:82-95, 2012.
CODEN LNCSB9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL

[PH12b] Henrich C. Pöhls and Focke Höhne. The role of data integrity in EU
digital signature legislation — achieving statutory trust for sanitizable sig-
CODEN LNCSB9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL

[PHWM10] Bryan Parno, Jon Howell, Craig Gentry, and Mar-
iana Raykova. Pinocchio: nearly practical verifi-
cable computation. Communications of the As-
CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-

[PHN+12] Marios Papas, Thomas Houit, Derek Nowrouzezahrai, Markus Gross, and Woj-
ciech Jarosz. The magic lens: refractive steganography. ACM Transactions
CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

[Pie10] Josef Pieprzyk, editor. Topics in cryptography —
CT-RSA 2010: the 10th cryptographers’ track at the RSA conference 2010,
San Francisco, CA, USA, March 1–5, 2010. Proceedings, volume 5985 of
Lecture notes in computer science. Springer-Verlag,
Berlin, Germany / Heidelberg, Germany / London,
Pointcheval:2012:ACE


Pramila:2018:ICA


REFERENCES


**Pathak:2012:PPS**


**Papadopoulos:2015:PAP**


**Pandey:2012:PPS**


**Phan:2012:MBT**


**Phan:2012:DDB**


**Pyun:2012:IBF**

Piret:2012:PBC

Perez-Resa:2019:SSE

Puthal:2019:SAL

Polyakov:2017:FPR

Popa:2012:CPQ
REFERENCES

Priemuth-Schmid:2012:ASV


Permpoonanalarp:2014:FTG


Perazzo:2015:DRL


Pereira:2013:SLC


Phatak:2013:SIN


Patranabis:2017:PSK

[PSM17] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay. Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud. IEEE Transactions on Comput-
Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC


Papakostas:2014:MBL


Papamanthou:2016:AHT


Pudovkina:2012:RKA

Marina Pudovkina. A related-key attack on block

Pei:2013:ARW


PWLL13


POLL12


POLL13


PAGN18


PAGN13

Pieter Philippaerts, Yves Younan, Stijn Muyld, Frank Piessens, Sven Lachmund, and Thomas Walter. CPM: Masking code point-

**Pey:2015:SWT**


**Papadopoulos:2010:CAR**


**Phuong:2018:CBE**


**Pournaghi:2018:NNE**


**Patsakis:2015:PSM**


**Qiu:2018:QDS**

Lirong Qiu, Feng Cai, and


REFERENCES


REFERENCES

Rankin:2014:HEY


Rankin:2016:HSP


Rao:2010:PAA


Rao:2017:SEC


Rauscher:2015:FMT


Ruoti:2015:WJS


Rupp:2015:CTM

Andy Rupp, Fotini Baldimtsi, Gesine Hinterwälder, and Christof Paar. Cryptographic theory meets practice: Efficient and privacy-preserving payments for

**Radke:2015:CFA**


**Reaves:2017:MBM**


**Rao:2017:CFA**


**Rabbachin:2015:WNI**

REFERENCES

Ren:2016:IBE


Reardon:2016:SDD


Reeve:2015:ARC


Ren:2010:CSH


Roh:2010:BSW


Robert-Inacio:2011:SAP


Rjasok:2012:BBP


Regev:2011:QOW


[RK11]

Rakshit:2018:LLO


[RM18]

Reyhani-Masoleh:2019:NMI


[RMERM19]

Roy:2018:HIR


[Rog16]

Rogaway:2016:POP

Rose:2011:KBT

Rao:2012:SSA

Rifa-Pous:2012:AHD

Rhee:2010:TSS

Ren:2015:ASE

Rawat:2011:CBR

Rosen:2010:CCS
Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products.
Reeder:2011:WPD

Rivest:2014:SSR

Rossi:2015:IBS

Rana:2016:DBV

Roy:2017:LOS

Roetteler:2018:QCC
Rangasamy:2012:ERP


Ren:2018:IAS


Rastegari:2019:ECS


Roy:2015:SCP


Ribeiro:2015:QBS


Resende:2019:BMI

REFERENCES


Rodriguez-Vazquez:2012:SCB


Rogaway:2012:SCS


Roettger:2012:PKC


Ren:2013:PPK


Ristenpart:2010:WGR

REFERENCES


Siad:2016:NFI


Saarinen:2012:PPK


Suoranta:2012:SAM


Sarreshtedari:2015:WMD


Schutz:2010:DIN


Sacco:2014:MC


Sahai:2013:TCT

REFERENCES


[Sak16] Palash Sarkar. A simple and generic construction of authenticated encryption with associated data. ACM Transactions
Sarkar:2011:TES

Sarier:2012:SNB

Sarier:2018:MBI

Singh:2018:SDD

Sasaki:2012:DSW
Yu Sasaki. Double-SP is weaker than single-SP: Rebound attacks on Feistel ciphers with several rounds. *Lecture Notes in Computer Science*, 7668:265–282, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-
Sasaki:2018:QKD


Savage:2013:NSL


Savage:2013:PP


Savage:2015:NVS


Safkhani:2017:PSD


Shwartz:2018:DMI

REFERENCES

Stevens:2017:AFS


Safkhani:2012:SMA


Santos:2014:ACD


Srinivasan:2012:RAP


Syta:2014:SAA

REFERENCES

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

[Sch10] Schoenmakers:2010:VS


[Sch12a] Schaathun:2012:ML1

[Sch12b] Schneier:2012:LOE

[Sch12c] Schnoor:2012:DES

[Sch13] Schneier:2013:HDD

[Sch15a] Schaefer:2015:BRB
Edward F. Schaefer. Book review: The Mathematics of Encryption: An Elementary Introduction, Re-


Schafer:2015:ECA


Schafer:2015:DGH


Schafer:2016:CHT


Schneier:2018:CAA


Schneier:2019:CPI


Schrestha:2010:KBA

Anish Prasad Shrestha, Dong-You Choi, Goo Rak Kwon, and Seung-Jo Han. Kerberos based authentication for inter-domain roaming in wireless heterogeneous network. Computers and Mathematics with

Stobert:2018:TAL


Seberry:2010:CTAa


Seberry:2010:CTAb


Scriber:2018:FDB


Shu:2015:PML


Saleh:2010:GTF

REFERENCES


Shen:2012:PAS


Souissi:2012:OCP


Shakiba:2014:CCI


Seo:2014:RHI


Seo:2016:RHI

Jae Hong Seo and Keita Emura. Revocable hierarchical identity-based encryption via history-free approach. Theoretical Computer Science, 615(??):45–60, February 15, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (elec-
REFERENCES


Sakai:2016:CDN

Sethumadhavan:2016:HEP

Severance:2016:BSB

Seo:2018:AOF

Savas:2014:SMQ

Su:2012:IIN
Chen Su and Haining Fan. Impact of Intel’s new instruction sets on software implementation of GF(2)[x] multiplication. *Information Processing Letters*, 112(12):497–


[Shabtai:2010:SAP]

[SF10]

[Schneier:2015:SWC]

[SFKR15]

[Sasdrich:2015:ICS]

[SG15]

[Shu:2014:DAS]

[Saxena:2016:API]

[Silva-Garcia:2018:SBG]
REFERENCES


Sanchez-Garcia:2016:SSA


Shen:2018:CAL


Susilo:2016:EDT

**REFERENCES**

www.sciencedirect.com/science/article/pii/S0304397515008087

**Shankar:2012:BDF**


**Sun:2017:PKE**


**Sipiran:2014:SCA**


**Shaolan:2011:EDE**


**Seyedzadeh:2011:IEA**


**Song:2015:ADT**


**Shallit:2010:BRB**


**Sha10**

**Shaw:2013:DE**


**Shi11**


**Shp10**

Igor E. Shparlinski. Numbers at work and play.
REFERENCES


Suoranta:2012:ASM


Shyu:2015:VCR


Satir:2012:CBT


Siad:2012:NAP


Simion:2015:RST


Simmonds:2015:DI

Sirer:2016:TPS


Shakervari:2012:RZW


Shin:2017:CGI


Sherman:2019:OVB


Sabri:2011:AFS


Sachnev:2012:IME

REFERENCES

Seo:2012:MPM


Scarani:2014:BPQ


Son:2017:NOC


Soupionis:2014:GT


Sirivianos:2014:LSF


Seo:2015:AEC

Seog Chung Seo, Taehong Kim, and Seokkie Hong. Accelerating elliptic curve scalar multiplication over GF($2^m$) on graphic hardwares. *Journal of Parallel and Distributed Comput-


[SKH15] Seog Chung Seo, Taehong Kim, and Seokkie Hong. Accelerating elliptic curve scalar multiplication over GF($2^m$) on graphic hardwares. *Journal of Parallel and Distributed Comput-
REFERENCES

Sinha:2017:SSD


Szalachowski:2010:CCG

P. Szalachowski, B. Ksiezeopol-

Stevens:2015:FCF

Marc Stevens, Pierre Karp-

Singh:2018:MWT

Amit Kumar Singh, Bas-
ant Kumar, Sanjay Ku-
mar Singh, S. P. Ghrera,
and Anand Mohan. Mul-
tiple watermarking tech-
technique for securing online social network contents using back propagation neural network. *Future Generation Computer Systems*, 86(??):926–939, September 2018. CODEN FG-
SEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/

Scheidat:2012:STT

Tobias Scheidat, Karl Kümmel,
and Claus Viel-
hauer. Short term tem-
plate aging effects on bio-
metric dynamic handwriting authentication performance. *Lecture Notes in Computer Science*, 7394:
107–116, 2012. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-

Schmitz:2012:NAC

Roland Schmitz, Shuj-
jun Li, Christos Grecos,
and Xinpeng Zhang. A new approach to com-
mutable watermarking-
encyption. *Lecture Notes*
REFERENCES


Srivatsa:2011:ESA


Schultz:2010:MMP


Somani:2010:IDS

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

Sun:2016:RSP


Shao:2012:AKP


Sarkar:2010:CRM

REFERENCES


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


Stankovski:2014:CFE


Sharma:2018:CSS


Sadeghi:2010:THI


Safavi-Naini:2011:USC


Seyedzadeh:2014:RCI

Suriadi:2012:PCV


Schaumont:2015:IEP


Suresh:2015:AGU


Serwadda:2013:ELK


Shiaeles:2015:FI


Shim:2015:SD

Spaord:2016:SE

Sherman:2019:PBL

Safkhani:2014:CCA

Sun:2013:IUP

Serwadda:2016:TRR

Shaikh:2010:CTO
Siraj A. Shaikh and
REFERENCES


**Schilling:2012:ATU**


**Sur:2012:SSU**


**Stanton:2014:BRB**


**Singh:2017:SCB**


**Stefan:2012:ACT**

REFERENCES

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

Sutar:2017:DPI


Sethumadhavan:2012:CHD


Saklikar:2010:IFV


Sopka:2010:BTS


Szaban:2011:IQB

Saxena:2012:BIT


Shparlinski:2012:CSD


Sendrier:2013:HCE


Sadhy:2017:PRE


Siegel:2019:UOC


Singh:2013:QBF

REFERENCES


REFERENCES


Schaffer:2012:EI1


Schillewaert:2014:CCA


Shen:2016:RMM


Sethumadhaven:2019:SA


Stanoyevitch:2011:ICM


Stanek:2012:TEM

Martin Stanek. Threshold encryption into multiple ciphertexts. Lecture Notes in Computer

**Staff:2013:ITD**

**[Sta13]**

**[STC11]**


**Stewart:2011:CCI**

**[Sti11]**

**Steel:2015:APF**


**[Ste15b]**

**Stem:2015:SNT**


**Stipcevic:2011:QRN**


**[Sti15]**

**Stuckney:2015:CBS**

Stiles:2019:HSB


Stolte:2012:EDA


Suciu:2012:SED


Sung:2011:DCE


Sun:2016:NEB


Shen:2015:CSC


Song:2016:IAR

REFERENCES


REFERENCES

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

Su:2016:PSN


Sahillioglu:2014:SCM


Savas:2015:GMA


Shao:2015:SAS


Song:2017:SSI


Seo:2013:PIC

REFERENCES

www.sciencedirect.com/
science/article/pii/S0304397512010560.

Song:2017:SAM
Jul Song, Fan Yang, and
Lizhe Wang. Secure
authentication in motion:
a novel online payment
framework for drive-thru
Internet. Future Generation
CODEN FGSEVI. ISSN 0167-739X
(print), 1872-7115 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0167739X16301960.

Shen:2017:RDP
Wenting Shen, Guangyang
Yang, Jia Yu, Hanlin
Zhang, Fanyu Kong, and
Rong Hao. Remote data
possession checking with
privacy-preserving authen-
ticators for cloud storage.
Future Generation Computer Systems, 76(??):136–145,
November 2017. CODEN FGSEVI. ISSN 0167-739X
(print), 1872-7115 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0167739X16304939.

Sui:2014:DAH
Yan Sui, Xukai Zou,
Eliza Y. Du, and Feng
Li. Design and analysis
of a highly user-friendly,
secure, privacy-preserving,
and revocable authentica-

tion method. IEEE Trans-
actions on Computers, 63
CODEN ITCOB4. ISSN
0018-9340.

Shi:2013:REA
Qi Shi, Ning Zhang, Mad-
jid Merabti, and Kashif Ki-
fayat. Resource-efficient
authentic key establish-
ment in heterogeneous
wireless sensor networks.
Journal of Parallel and
Distributed Computing,
73(2):235–249, February
2013. CODEN JPD-
CER. ISSN 0743-7315
(print), 1096-0848 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0743731512002547.

Sun:2017:CPP
Jiameng Sun, Binrui Zhu,
Jing Qin, Jiankun Hu, and
Qianhong Wu. Confidentiality-
preserving publicly verifi-
able computation. Interna-
tional Journal of Founda-
tions of Computer Science
(IJFCS), 28(6):799–
??, September 2017. CO-
DEN IFCSEN. ISSN 0129-
0541.

Shen:2014:ERC
Limin Shen, Futai Zhang,
and Yinxia Sun. Efficient
revocable certificateless en-
cryption secure in the stan-
dard model. The Com-
puter Journal, 57(4):592–
601, April 2014. CODEN

Sun:2018:RPP


Tsang:2010:BRR


Tamayo:2015:AFH


Tan:2011:CTA


Tan:2012:SLM


Tan:2012:LCP

Tang:2015:ETE


Tang:2015:HAC


Tankard:2017:BNK


Tankard:2017:ECB


Toth:2019:SSD


Tarnovsky:2010:DSP


Taylor:2014:WSE


Taylor:2017:EBH

Michael Bedford Taylor. The evolution of Bitcoin hardware. Computer, 50
Talbi:2018:SIW

Tilli:2015:GCR

Tuan:2010:AWB

Taylor:2011:DR

Tang:2015:CER

Tan:2017:JDC
Rui Tan, Sheng-Yuan Chiu, Hoang Hai Nguyen, David K. Y. Yau, and Deokwoo Jung. A joint data compression and encryp-

### Tian:2014:DFS


### Tiplea:2014:NSC


### Tao:2013:SMS


### Terai:2011:BRB


### Tassa:2012:SDC


### Tewari:2017:CNU

Aakanksha Tewari and B. B. Gupta. Cryptanalysis of a novel ultra-lightweight mutual authentication pro-
REFERENCES


Theofanos:2016:SUE


Tian:2016:IBS


Tian:2015:IBP


Tian:2012:TOE


Thabit:2014:RRW


Takayasu:2019:PKE

REFERENCES


Tu:2014:EPB

Tani:2012:EQA

Tu:2013:PAQ

Tariq:2014:SBL

Tan:2016:ESE

Tsaur:2012:ESM
Woei-Jiunn Tsaur, Jia-Hong Li, and Wei-Bin Lee. An efficient and secure multi-server authentication scheme with key agreement. The
Tsai:2013:ZWS

Tetali:2013:MSA

Tang:2012:RSS

Tsoutsos:2018:EDM
Tang:2015:ECP


[TMGP13]


[TMK11]


Terrovitis:2012:PPD


Tormo:2013:IMP

RefWorks

[TMDQ18]


Tao:2018:AA

[Tom16]

REFERENCES


**REFERENCES**

[Tschorsch:2016:BBT]

[Tao:2014:CFS]

[Toreini:2017:TRP]

[Tang:2011:IDC]

[Tso:2013:SAI]

[Tseng:2012:ERI]

[Tseng:2015:LFI]
Yuh-Min Tseng, Tung-Tso Tsai, and Sen-Shan Huang. Leakage-free ID-based signature. *The Com-
REFERENCES


Tsai:2010:RLI


Tupakula:2015:TES


Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG


Tartary:2011:EIT

Christophe Tartary, Huaxiong Wang, and Yun Zhang. An efficient and information theoretically secure rational secret sharing scheme based on symmetric bivariate polynomials. International Jour-
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Authors</th>
<th>Journal</th>
<th>Volume</th>
<th>Pages</th>
<th>Year</th>
<th>Digital Object Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tian:2017:ORA</td>
<td>One-round attribute-based key exchange in the multi-party setting</td>
<td>Yangguang Tian, Guomin Yang, Yi Mu, Shiwei Zhang, Kaitai Liang, and Yong Yu</td>
<td>International Journal of Foundations of Computer Science</td>
<td>28(6)</td>
<td>725–??</td>
<td>2017</td>
<td></td>
</tr>
</tbody>
</table>


Varadharajan:2018:AUR


Vembuselvi:2011:LLL


Vassilev:2016:ESU


Vivek:2012:CSE


Vlachos:2015:DPC


vanTilborg:2011:ECS


Vuagnoux:2010:CAC

[Vua10] Martin Vuagnoux. *Computer Aided Cryptanalysis from Ciphers to Side Chan-


REFERENCES


Wei:2018:GCQ


Wang:2018:SEA


Wei:2012:NTB


Wazid:2019:DSK


Wang:2013:SES

REFERENCES

DEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL

West:2015:EC


Wess:2016:JWM


Wang:2018:ERS


Wang:2016:SSS


Wang:2010:DVT


Wang:2012:BRR


REFERENCES

Wei:2016:PAB

Wu:2012:DAA

Wang:2012:NFS

Williams:2018:FPD

Winder:2017:ROS
Davey Winder. Researchers open sliding
REFERENCES


Wang:2019:MBN


Wang:2016:DRS


Wang:2012:MCE


Weissman:2011:LLB


Wang:2012:MCE


Wang:2019:VFS

[Zhiqiang Wu and Kenli Li. VBTREE: forward secure conjunctive queries over encrypted data for cloud computing. VLDB Journal: Very Large Data Bases, 28(1):25–46, February 2019. CODEN
Wei:2012:IRK

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

Wang:2011:RBM


Wang:2017:CAS


Wei:2015:FST

Guiyi Wei, Rongxing Lu, and Jun Shao. EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption. *Journal of Computer and System Sciences*, 80(8):1549–

Wu:2015:TRM


Wang:2017:ABS

Qi Wang, Xiangxue Li, and Yu Yu. Anonymity for Bitcoin from secure escrow address. IEEE Access, ??(??):1, ???. 2017. ISSN 2169-3536.

Wang:2016:LLE


Wang:2012:RTC


Wu:2012:PSC


Wang:2017:CES

Won:2016:PAA


Wang:2015:HAD


Wu:2012:UFS


Wendzel:2015:CME


Wang:2017:PPK


Wang:2016:SEP

Xinlei Wang, Amit Pande, Jindan Zhu, and Prasant Mohapatra. STAMP: En-


[WS14] Jeff Whitworth and Shan...


Tsu-Yang Wu and Yuh-Min Tseng. An efficient user authentication and key exchange protocol for mobile client–server environment. Computer Networks (Amsterdam, Netherlands: 1999), 54(9):1520–1530, June 17,
REFERENCES

2010. CODEN ???? ISSN 1389-1286.

[Wu:2010:IBM]


[Wang:2013:NMC]


[Wu:2016:LTN]


[Wu:2017:SPM]


[Wu:2012:AST]

REFERENCES


**Willis:2013:IFI**

**Wang:2014:ATF**

**Wang:2011:MMW**

**Weng:2012:NCC**
 REFERENCES


cations, and Applications, 8(2S):32:1–32:??, September 2012. CODEN ????
ISSN 1551-6857 (print), 1551-6865 (electronic).

**Wang:2013:NSW**


**Wang:2013:BSB**


**Wei:2014:IDC**


**Wei:2016:APS**

REFERENCES

466

Wei:2015:CPK


Wang:2018:AMB


Weng:2013:VWI


Wei:2012:CSO


Wei:2012:GOP


Wang:2012:NIS

Xiaofeng Wang, Nanning Zheng, Jianru Xue, and

[XHC+12]


[XHCH14]


[XHCH14]


[XHCH14]


[XHCH14]


Xie:2013:ECP


Xiang:2014:PBA


Xia:2015:SPK


Xiang:2018:SSA


Xiang:2015:SSB


Xiong:2011:CIB

REFERENCES


Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing.

IEEE Trans-
REFERENCES


REFERENCES

Xiao:2016:REM

Xiong:2015:SRE

Xie:2012:DPK

Xiao:2018:KRL


Chang Xu, Liehuang Zhu, Zhoujun Li, and Feng Wang. One-round affiliation-hiding authenticated asymmetric group key agree-


Yang:2014:BEB


Yang:2011:GSS


Yang:2012:PST


Yang:2016:EBB

REFERENCES

Yi:2017:ZCL


Yuan:2013:PVQ


Yu:2016:DNF


Yuen:2012:IBE


Yu:2017:PDA

Meng-Day (Mandel) Yu


Yoshida:2012:OGT


Yu:2012:EPF


Yu:2012:EPF

Yuce:2017:AFI


Yang:2017:CCS


Yang:2018:RRE


Yuce:2017:AFI

[YG+17]
Yang:2015:SHI


Ye:2017:VCS


Ye:2016:IEA


Yu:2010:IBF

[YHK+10] Jia Yu, Rong Hao, Fanju Kong, Xiangguo Cheng,


You:2013:TPC


Yang:2018:AIW


Yum:2012:OPE


Yum:2011:ACO


Yoshino:2012:SIP


Yi:2017:ICM


Yuen:2013:ELT


Yang:2012:WSI


You:2012:DDS


Yi:2013:ETS


Yu:2016:CBE


Yagan:2016:WSN

Osman Yagan and Armand M. Makowski. Wireless sensor networks under the random pairwise key predistribution

**Yakubu:2017:SSN**


**Yu:2010:PSI**


**Yu:2011:CLE**


**Young:2015:DWE**

Vinson Young, Prashant J.


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-34117-5_5/.


REFERENCES

DEN LNCS.9. ISSN 0302-9743 (print), 161-3349 (electronic). URL

**Yumbul:2015:EEP**


**Yang:2015:EPS**


**Yang:2016:ECV**


**Yang:2018:HEP**


**Yao:2014:NCR**


**Yeh:2010:TRR**

Kuo-Hui Yeh, Chunhua Su, N. W. Lo, Yingjiu Li, and Yi-Xiang Hung. Two robust remote user authentication protocols using...

**Yuen:2014:TCT**


**Yuen:2014:TCT**


**Ylonen:2014:SAA**


**Yang:2011:CPK**


**YT11a**


**Yang:2011:CCK**

Yang:2014:IBI

Yang:2018:IA

Yang:2011:ACD

Yasuda:2012:ASM

Yao:2010:IDA

Yao:2010:ASP
Yan:2017:PIS


Yang:2015:RCI


Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


Yang:2010:CRS

REFERENCES


**Wang:2018:CIW**


**Yu:2012:SME**


**Ye:2018:ISS**


Yang:2018:CDD


Yang:2012:BPN


Yang:2014:PST


Zufiria:2017:GLM


Zhenxia Zhang, Azzedine Boukerche, and Hussam Ramadan. TEASE: a novel Tunnel-based sEcure Au-


Zongyang Zhang, Sherman S. M. Chow, and Zhenfu


REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31020-1_8./


REFERENCES

Zadeh:2015:ASP

Zhang:2012:LDC

Zhang:2015:BYO

Zhang:2015:STR

Zhao:2017:RAS

Zhu:2015:IDM
Hui Zhu, Cheng Huang, and Hui Li. Information diffusion model based on privacy setting in online social networking ser-

**Zhang:2019:REU**


**Zhu:2016:SCI**


**Zhu:2013:TSC**


**Zhou:2015:EPP**


**Zhang:2016:PPV**


(print), 1558-2183 (electronic). URL http://
csdl.computer.org/csdl/
trans/td/2015/06/06779640-
abs.html.

Zhao:2012:IAS

[ZLDD12] Yifan Zhao, Swee-Won Lo, Robert H. Deng, and
Xuhua Ding. An improved authentication scheme for
H.264/SVC and its performance evaluation over non-
stationary wireless mobile networks. Lecture
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-34601-9_15/.

Zhao:2014:TAH

[ZLDD14] Yifan Zhao, Swee-Won Lo, Robert H. Deng, and
Xuhua Ding. Technique for authenticating H.264/
SVC and its performance evaluation over wireless
mobile networks. Journal of Computer and System
Sciences, 80(3):520–532, May 2014. CODEN
JCSSBM. ISSN 0022-0000
(print), 1090-2724 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0022000013001177.

Zhao:2012:EEF

[ZLH+12] Yunmei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho
Au, and Willy Susilo. Efficient escrow-free identity-
based signature. Lecture
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-33272-2_11/.

Zhang:2015:RBA

binding against FPGA replay attacks. ACM
Transactions on Design Automation of Electronic Systems,
20(2):33:1–33:??, February 2015. CODEN
ATASFO. ISSN 1084-4309
(print), 1557-7309
(electronic).

Zhang:2012:CCB

[ZLW+12] Leo Yu Zhang, Chengqing Li, Kwok-Wo Wong, Shi
Shu, and Guanrong Chen. Cryptanalyzing a chaos-
based image encryption algorithm using alternate
structure. The Journal of Systems and Software,
85(9):2077–2085, September 2012. CODEN
JS-SODM. ISSN 0164-1212
(print), 1873-1228 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S016412121200101X.
Zhu:2017:PSN

Zhang:2010:ESP

Zhou:2019:LIB

Zhang:2016:TLT

Zhang:2017:FGA

Zhang:2010:NSS
REFERENCES

63–74, July 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).


REFERENCES

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

Zhao:2012:SSS


Zhang:2015:MAA


Zhang:2010:EMO


Zmudzinski:2012:WEU

Sascha Zmudzinski and Martin Steinebach. Watermark embedding using audio fingerprinting. *Lecture Notes in Computer
REFERENCES

Zhao:2012:SSM

Zheng:2018:GDP

Zanon:2019:FKC

Zhang:2012:EHO

Zhou:2018:TPW
Zuo:2018:CSA


Zwattendorfer:2012:CBL


Zhang:2014:NCM


Zhang:2016:EEA


Zhu:2015:PPD

REFERENCES


Zhou:2014:SAC


Zhang:2015:FAA


Zhang:2014:LFL


Zhang:2011:AGK


Zhou:2018:QTA

Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki, and Arcangelo Castiglione. Quantum technique for access control in cloud computing II: Encryption and key distribution. *Journal of Network and Computer Applications*, 103(??):178–
REFERENCES

Zilberberg:2013:PCM

Zhang:2015:FER

Zhou:2011:PSA

Zhang:2013:LPP

Zhang:2014:EFH
Xiaojun Zhang, Chunxiang Xu, Chunhua Jin, Run Xie,


(Zhu:2017:CLR)
Zhou:2017:LRC


Zhang:2017:GFD


Zheng:2010:PS


Zhou:2019:CLR


Zhang:2010:ASL


**Zhang:2013:BLR**


**Zhang:2011:EPK**


**Zhao:2012:FCS**


**Zheng:2015:EPT**


Zaidan:2017:NDW


Zhu:2018:CAC


Zhang:2017:NLR


Zeng:2019:SAE