A Bibliography of Publications on Cryptography:
2010–2019

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu,beebe@acm.org,beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/
03 December 2019
Version 1.493

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N) [Bai10, YC11], (n, t, n) [LHYZ12], (t, n) [QD16, ZPWY12]. 0 [XHX+17]. 1

[XHX+17]. 1, 2, 3 [SMDS11]. 11 [LJ17]. 13 [Blo15]. 2 [DBPS12, EAA+16, ESS12, JR13, MCDB12, PGLL10, WY12]. 22 [MNP12]. 2k [Sun16]. 3 [AP10, Bro19, CG12b, DWZ12, FWS13, GZH12, GH11a, KWS+12, LJ17, LJ15, MKH+12, RS16, SS10b, SS12a, SGS14, WSS12, tWmC12, YT11a, YI14, YPRI17]. 32 × 32 [SA14]. 3 × 3 [ÁMVZ12]. 4

[COP+14, DWZ12, HLYS14]. $49.00 [Sch15a]. 5 [YN19]. 8 [LPO+17, ZSH+19].


[DWZ12]. GF(2)[x] [SF12]. GF(2n) [HJ19, SH15]. GF(2n) [LBOX12]. K

[FXP12, FR16, CHX13, XMY+17, XLP+18, ZC17, ZHT16]. L(1/4 + o(1)) [Jou13]. M

[MMSD13, ÖS11]. Fq [AMORH13]. Fq [SS13]. N[P [HN10]. GF(q) [LPO10]. LWE

[BV14]. μ [Jia14a]. N [FR16].

n × k(k ≥ n/2) [MC11]. O(d13) [KA17]. O(n2) [KS11]. P [DG17, GT19]. π


-band [MMSD13]. -Bit [LPO+17, ZSH+19].


[DWZ12, QD16]. -Diversity [ZTL15].
-Encoded [DG17]. -Encoding [XHX+17].
-Men [KRDH13]. -Multiple [LTC+15b].
-nearest [XMY+17]. -NN [ZZC17, ZHT16].

.onion [Boy16].

0.13um [KLM+12].

1 [AAE+14, Ano15b, BH15, Bar16, CGCS12, Ful10, MSas12, SKP15]. 1-58488-551-3 [Ful10]. *10 [Ano10]. 1024 [Bro17, Win17].


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

72 [HYS18]. 768-bit [KFL+10]. 795-bit [BGG+19].

8.8/11.2 [GLIC10]. 802.11 [FLH13, ZBR11]. 802.11s [BOB13]. 802.15.4 [NBZP17]. 802.16e [CL11]. 802.16m [FZZ+12]. 85 [WZM12a].


AAA [BT18, MLM16]. AAA-based [MLM16]. AAoT [FQZF18]. Abandon [Loc15]. ABE
[FIHJ12, HQZH14, HLC+19, OCNZ19, QZZ18, TY16a, YMC+17, ZSW+18b]. abelian [CDLSY14, LR15]. ability [WS12]. absence [AGH+17]. Abstract
[CMO+16, DOS15, SKH15, XZL+19]. Accelerator
[MSR+17, MRL+18, PC16, WOLP15]. Accelerators
[AW15, AW17, GP17, HKL+14, OSH16, BAB+13, KKJ+16]. accelerometers [ZZL+18]. ACCENT
[PP11]. Acceptance [SPM+13]. Access
[AMSP19, AWSS17, BFK+10, CO11, CGH11, DLZ+16b, FCM14, GRRZ18, HLC+18, HP12, LGLK17, LPL15, MSL18, MK12b, NA10b, PV17, PB12, QZL+16a, RSN14, SGC14, SC12, WS13, XMLC13,
OSNZ19, QRW+18, SEY14, SY15b, SD12, TLL13, WHN+12, Yon12, ZLQ15, ZHS+19.

Age [Bla12, SR14, Lan17, Sto12]. Aged [Ree15]. agency [Ald11, ABJ13]. agent [GPVCdBR012]. Aggregate [CCT+14, PSM17, GLB+18, LLY15, LLL+18, ZQWZ10, ZDHZ18, CLW16].

Aggregated [LY15]. Aggregated-Proof [LY15]. Aggregating [DP12].

Agriculture [APK+18]. Aided [BGK12, BCGK12, BGB12, Gop19, GMSV14, MV19, Vua10, ABBD13, LYL15, SGJ+18, SSAF11, WLFX17]. AIPISteg [AGLW16].


Algebra [PWBJ17, Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14, Nag19].

Algebraic [HIJ+19, HLC+19, LYK19, SK11, Tam15, Wat10, Bul10a, CFR11, SA14, YTM+14]. Algorithm [AA19, ABCL17, Ano11b, AK14, BGJT14, BKLS18, CRN14, jCPB+12, DCM18, ESS12, GKB17, JH12, JSZ12, JJHN12, JL16, KB10, LL11, LT14a, LLL17a, LLLH18, MSR+17, MRL+18, NdMMW16, NV10, RR11, RVRSCM12, WHZ12, WZCC18, YP117, YH16, ZSW+12, ZWWW17, Ant14, BGJT13, BMB16, CG12b, Chm10, EEA13, JK13, Jou13, KY10, KHMB13, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WGTZ+12, XTK10, YWL+17, ZLW+12, ZL12, ÁCZ16, ZOC10].

Algorithm [GO17, KRH18, RZ19, AY12].

Algorithmics [Gas13]. Algorithms [AMKA17, AB10b, BCG12a, BJ10b, CN12, GP17, KRDH13, KRHR19, MR14a, MM17, RPHJ11, TKM12, WH18, YS15, ZW15, AGHP14, Fria10, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WGTZ+12, XTK10, YWL+17, ZLW+12, ZL12, ÁCZ16, ZOC10].


Almost-Tight [GDCC16]. Almost-Universal [BKST18]. Alpha [MV18]. Altera [SMOP15]. alternate [ZLW+12]. Alternating [BKLS12, KDH15].

AMBTC [KSSY12]. AMD [Arm19, BWS19, MZLS18]. America [AB10a, Bha16, Fag17]. American [Sch15a, Mun17]. Americans [ABJ13].

Amoeba [MPA+18]. among [BP11, MPJ+16, SS17a]. amount [EEAZ13]. Amplification [ABF12, HMR14]. Analog [KOP12, SOS15]. Analyses [ZPXX17].

Analysing [GRL12]. Analysis [ABS+12, ARP12, BR17, BBB+16a, BC14, BS14, BKLS18, Bu18, CFE16, CCG+16, CGL+12, DKMR15, FWSF11, GZZ+13, GWM16, GLG12, GA19, HC12, HHH+13, HZWW17, HB17, IBM13a, IS12, JT12a].
MD12b, PDJ+19, PYM+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, VWC19, WW14, WHN+12, XNG+14, YL17, YCM+13, ZLQ15, ZHS+19, AATM18, BBBP13, BVIB12, BSR+14, CGH17, dCCSM+12, DCAT12, DJL+12, DK17, Dra16, EA12, FTV+10, FIO15, GPP+16, GBNM11, HAK19, HAGTdFR13, KM10a, KPS10, LDC13, LWK11, NDNR13, OF11, PX13, SGP+17, TK19, TS16a, TY16b, TLL13, VS11, WWBC14, XWDN12.

Attestation [BWS19, FQZF18].

Attribute [AAC+16, AHL+12, BFK+10, Boy13, CD16, CDL18, CDLW19, CHH+19, FHR14, GZ+13, GSW+16, Gil12, 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, TMY+17, WDC18, WHL15, WHL16, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQ15, ZWM17, ZHW15, BTK15, CPPT18, FNWL18, HZL18, HZWW18, HYS18, HKHK13, JSMS18, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, LJWW18, LDZW19, Nam19, QRW+18, RD17, SLL+19, WLWG11, XWS17, XZP+19, XTZ+19, YCT15, ZW1M4, ZML17, ZGL+18a].

Attribute-Based [AAC+16, BFK+10, Boy13, CD16, CDL18, CHH+19, FHR14, GZ+13, GSW+16, GVW15, HSMY12, HBC+19, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TMY+17, WDC18, WHL15, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQ15, ZWM17, AHL+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMS18, LCL+15, LFZ+17, LFWS15, LYL15, LJWW18, LDZW19, Nam19, QRW+18, RD17, WLWG11, XWS17, XZP+19, XTZ+19, YCT15, ZM1L7].

Attribute-Hiding [OT12, ZWM14].

Attributes [CG12a, VKK+19, Yon11, LCL+17a].

Attribution [AIF+19, XHC+12, FNP+15].

Auction [Con10, JWS19, HJM+11].

auctions [MR14c, QS18].

Audience [DTE17].

Audio [Ber18, DA12, FM15, GCK12, HGT15, KD12a, KD12b, LAL14, LS11b, NXH+17, Q19, TC10, gWpNyY+14, XNG+14, XNRG15, XNP+18, ZS12, LSQ11a, SKEG14, yWpNyL11, YWYZ12, YQH12].

Audio-Visual [LAL14].

Audit [YNR12b].

Auditing [LMD16, TCR+17, YSY+16, XYA+16].

Augmenting [AV18].

August [AB10a, JY14, MV12, Rab10].

Aura [HFCR13].

AuthCropper [KLK+19].

Authentic [**********]

Authenticate [HM12].

Authenticated [**********]
AAZ+16, ACAT+15, ACKB19, AUMT16, ABB19a, BL12, BCE+12, BCM12, BSSV12, Bel18a, BKT18, BCD+12, Bis17, BF11, Boy16, BKJP12, BSV12, CGCGPDMG12, CTC+15, CC14, CSH+18, CCW+10, CCF17, CCC19, CJ13, CD12, CJP12, CLH13, DL15, DCM18, DBP512, DPKW12, DP12, FLH13, FR16, FMTR12, FD11, GHS14, Gil12, GI12, GMDR19, GI12, GM14, GI13, GMVV17, GCK12, HZC+12, HvSi2, HLLC11, Hay13, HBCC13, HM10, HCPLSB12, HCETPL+12, HKL+12, HFCR13, HXC+11, HLCL11, HRK18, IGR+16, JN12, JCM12, Jia17, JLX+19, JAE10, KP12, KS18b, KLN15, KRM+10, KSD+17, KPC+11, KLY+12, KTA12, KG12, Kim15, KPKS12, KLM+12, KO16, KH10, LLC11, LH12, LG15, LCLL15, LNZ+13, LZC14, LNX15, LLZ+12, MWZ12, MEFO12, MKH+12, MBC15, MRTT17, MRS+17, May15, MLBL12, Mor12]. **Authentication** [MSKRJ17, MPM+17, NR11, NR12, NSBM17, NLLJ12, NLY15, OdH12, OO12, OŠ12, PSSK19, PCDG14, PPRT12, PDT12, PWVT12, RS11, RWLL14, RSX18, RSN14, SG18, Saa12a, SBS+12, SBS18, Sar12, SG16, Sch15b, SKV12, ST14, SM12, SD12, Shi11, SG14, SSA13, SPK17, SRRM18, SC12, SCMS18, SZDL14, SBS12, SAA12b, SRK+17, SRK+18, TGGC16, TNWC18, TYK+12, TM12, Vet10, WgMdzZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WAK+19, WT10b, Xio12, YTP11, YFT17, ZBR11, ZHW+16, ZWZ17a, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, ARL13, Aia15, AL15, APMC13, AHM+18, APK+18, AIM+19, Alp18, AIK18, AC16, AZF+12, AKS19, ATI+10, ACC+13, AN15, ACM12, BOP14, BS13a, BGE+18, BDM18, BD18, BCM13, BGAD12, BDM+19, BLAN+16, BAL10, BM12, BHvOS15, BT18, BTW15, BM11, CLM+12, CML+18]. **Authentication** [CLP+13b, CAM19, CTL12, CJXX19, CSD18, CH10, CSSW11, CHS11, CLHJ13, CZ15a, Chi13a, CJP15, Cho14, CL11, CRS13, CDWM19, DCT12, DSCS12, DRN16, DEL19, DLK+16, DMV15, DLN13, DZS+12, DMT12, hHAN+18, EA12, ED19, EA11, FPBG14, FHH10a, FLL+14, FXP12, Far14, FA14a, FHZW18, FQZF18, FMA+18, FHM+10, FZZ+12, GJ13, GMSW14, GH19, GEH11, GPLZ13, GH15, GH16, GAI+18, Gop19, GCSAddP11, GM11J1, GLB+18, GBC19, GTSS19, HU15, HSH11, Ham12, Ham19, HW19, HBH18, HDP13, HZC+14, HK17, HZWW17, HL12, HL14, HCM11, HCL16, HPL+19, HCC10, HS11, IMB17, IAA+19, IC17, IG11, IB11, IOV+18, Jac16, JN1H17, JKAU19, Jia16, JK+16, JM1W+16, JAS+11, JXLZ15, KPP16, Kem11, KKG14, KSB+17, KV18, Kim11, Kin16, KIH19, KS19, KP18, KB17, KLW+16, KDW+17, LLLS13, LZ+16, LC17, LH11b, LT13, LH10c, LNM+11]. **Authentication** [LMJC11, LMXW12, LNNH13, LK13L13, LXJ14, LIK+17, LCM+17, LNK+18a, LWK+18, LNK+18b, LZD+19, LWK+19, LHW+14, LH13, LSQ15, LHH+18, LIt14, LWL11, LTC+15, LYL15, LZ19b, LBR12, LTT10, MM12, MMLN15, MCN+18, MDHM18, MvO11, MMLP19, MA17, MMS17c, MWW+18, MCR19, MK12a, NDA17, NR17, NACL12, NCCG13, NM18, NLYZ12, NML19, NB13, NXS10, NMX15, OSP+19, OF11, OCG11, OYHSB14, PYH+18, PYP10, Par12b, PLGMCdF18, PCK19, PZBF18, PA10, PKA15, PRN+19, QMC17, QMW17, QLZ19, RR17, SSA18, SCFB15, SPLHCB14, SB17, SGGR+16, Sar10a, SK18, SSS15, SY19, SGJ+18, hSZZ15, SCKH10, SYWX19, SNG+17, SCR19, SA15, SYW17, SSS11, SKEG14, SA19, SMS+16, SHBC19, Tan12b, Tan15b, Tan18, TODQ18, TZTC16, TG17, TLL12, Wan13, WW14, WLZ+16, WCFW18, WZZW20, Wat14a, Wat15, WDKV19, WTi1a, WKLH11, WXK+17, XHH12].
authentication
[XWDN12, XHCH14, XXCY19, XMHD13, XHM14, YI17, YHL16, YHHS16, YWK+10a, YSL+10, YMM13, YN19, YID17, ZYL+10, ZQWZ10, ZCLL14, ZGL+18b, ZDHZ18, ZHH+17, ZX11, ZLY+19, ZZL+18, OHJ10].

authentication-chaining [EA11].

authenticators [SY+17].

Backdoor [Sch13, Fed13].

Backside [DDR+16].

Backup [MPA+18, Cor14a].

backward [BM11].

Bacterial [Kar12].

Bad [KMZS19, Hai17, RY10].

BAF [YNR12a].

Bake [Boy16].

Balanced [YTP11].

balancing [FXP12, PRN+19, Zha15a].

Ballots [CW12b, LHF12].

balls [Svo14].

band [MMSD13].

Bandwidth [GST13, NR11, LLZ+12].

Bandwidth-Efficient [LLZ+12].

Banking [KSD+17, RBS+17, GMJJ11, KVvE18].

banned [Eve16].

BANs [BLL+19].

Baptiste [Dew11].

Barbara [Rab10].

Barcodes [WK12].

Barrier [JR14, KS11].

barriers [LKKL13].

base [MS12a, XSSWC10].

Based [ADM12, ADM19, AGW15, ASM12, AAC+16, ABCL17, Ano11b, ASS15, AYS15, BWLA16, BL12, BCE019, BBB+16a, BSSV12, BHG12, BKPW12, BRT12, BHH+15, BS13b, BFK+10, Bon12, BSJ15, BF19, Boy13, BKJP12, BDH11, BCF+14, CMLS15, CLL16, CGMO14, CKHP19, CMM17, CSH+18, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST+17, CLN19, CGL+12, CDD13, CGY+13, CD12, CHi12, CK18, CD16, CDLW19, CHH+19, DSMM14, DS19, DA12, DLZ+16b, EM12, EKB+16, FM15, FHH10b, FHR14, FZT14, FGM10, FYD+19, FR15, FVS17, FP19, FSX12b, FSX12c, FSX12a, GT19, GWWC15, GZZ+13, GSW+16, GV14b, GI12, GYW13, GDCC16, GVW15, GJJ15, GJJ17, GRRZ18, HZC+12, HSMY12, HSM14, HBC+19, HEP+11, HL1+19, HL10a, HZX15, HWZP18, HCP1SL12, HKL+12, HG12, HMR12, HSA14, HPO+15, HKR+18, HGT15, HCL+14, HLN+10, Hül13, HRS16, HBG+17, HEC+12, HM19].

Based [HP12, JTZ+16, JHHN12, JEA+15, JKHgY12, KMSZ19, KSI18b, KZG10, KK12}
Based [RW12, SBS18, SSW12, Sar18a, SS13, Sen17, SJLK18, SXH19, SJ12, SGP12, SPG19, SP15b, SSA13, SRAA17, Snck18, Sh15, SGH15, TB18, TKR14, TWZ11, TW12, TZ12, TYM17, TSH17, TT12, TTH15, TFS19, TC10, VDB16, VCA15, Vle12, WY10, Wan10, WSS012, WGMW12, WYW18, Wan14, WZC18, yWXyZ18, WDC18, WLH15, WCL18, WT10b, WMS12, WZC18, XNG14, XNR15, XZ12, XMLC13, XQL11, Xio12, XGLM14, XWLJ16, XJW16, XJR17, XHZ17, XHZ19, XYE12, YZLC12, YZX12, YGFL15, YHSW19, YTS12, Ye10, Ye14, YH16, YTH17, YY15, Y17, YKNS12, YHK10, YMWS11, YKC11, YFK12, YCYZ12, ZSP19, ZPM15, ZJ11, XZ11, ZDL12, ZLH12, ZQQ15, ZMW16, ZXY16, ZWW17, ZMZ17, ZWZ17b, ZZ19, ZP16, ZW15, ZV16, ZPX17, ZYM18, ZYH19, ZHL15, AMN18, AGLW16, AaBT16, ARL13, AY14a, AHS14, AAT16, AA14, ASO14, AIA18, AIM19, AKG13, ASVE13]. Based [Ara13, AT110, ACC13, AHL12, BS15, BDM18, BBBBB13, BD18, BGAD12, BAAS13, BDM19, BB13, BW12, BWA13, BM12, BC18, BTK15, BB16b, BK12b, CPPT18, CML18, CX19, CFL13, CFY10, CLLL11, CTL12, CLS12, CG12b, CSZ11, CHX13, CSS13, CW14a, CLC19, CTH13, CJP12, CJ15, CC10, CT13, Cho14, Con12, dCCSM12, Cra11, CDL18, DSC12, DGMT19, DZ14, DLN13, Dra16, uHAN18, EZ15, FH13, FG19, Far14, FA14b, FIO15, Fay16, FHZW18, FMC19, FNWL18, Gal13, GJ13, GMGCCC15, GMRT15, GKCK11, GJMP15, GCS1addP11, GAB19, GMS11, GLL18, GBC19, HSH11, HT11, Ham19, HW19, HΗB18, HGWY11, HSM13, HZ14, HL12, HFD14a, HWD16, HZW17, HZZ18, HBBRNM16, HLR11, Her14, HW10, HW12, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HYF18, HPY10, HHHK13, HCC10]. Based [Hwa11, IMB17, IM14, ISC16, IB11, IA15, IOV18, Jac16, JNUH17, JKAU19, JK13, JLT12, JZS10, JM16, JSGM18, JLF19, KOP16, KK13, KM10a, KHMB13, KG14, KD18, Kim11, KGO10, KL11, KSH18, LXY12, ZL16, Lai12, LLC10, LK14, LHM13, LH10c, LZX10, LNN11, LMJC11, LK12, LXMW12, LKAT12, LLHS12, LNLK13, LXXJ14, LCL15, LZ16, LFZL17, LNK18a, LWK18, LCT14, LFWS15, LSM19, LPdS10, Lin14a, LHH18, LL12a, LW10, LSL11a, LSQ11b, LWK11, LW13b, LZC14, LPZJ15, LTH15a, LY15, LY15, LW17, LWYW18, LDZW19, LWW10, LL16a, LW13c, LWY12, LY14, MCN18, MCP15, MJS12, MJS13, MLM16, MWW18, MM12, MM13, Mes15, MCRB19, MBB11, MO14, MHT13, MG15, MS17, Nam19, NR11, NM18, NCL13, NZL15, NMX15, OMT19, OPA18, PYH18, PLPW13, PTK14, Par18, PWW10, PGL10, PZL19, PPB16, PLGMC18,
PCK19, PS14]. based
[PL16, PKA15, PC14, PPR+12, QZDJ16, QRW+18, QYW16, QMW17, QLZ19, RD17, RG10, RS15, SPLHC14, SERF12, SGKCR+16, SLL+19, SI12, SYL13, SE14, SE16, SK18, SH11, SM11, SNM14, SZHY19, SR10, hZZ15, SCKH10, SA16b, SPK17, SSAF11, SWW+16, SSS11, SKEG14, Sun16, SGM16, SHBC19, SS11, TPL16, TQL+14, Tia15, TH16, THA+13, TTL10, TPKT12, TKHK14, VS11, VN17, WWYZ11, WWYY11, WLWG11, WLDB11, WLFX17, WMX+17, Wan18, WDZ19, WGZ+12, WHLH16, WS14, WS24, WTT12, WOLS12, WCCH18, XHH12, XWZW16, XW12, XCL13, XWS17, XZP+19, XHICH14, XZW+18, XTZ+19, XMH13D, XHM14, YWL+17, YWJ+19, yYqWqZC13, Yn14, YTM+14, YCC16, YXA+18, YYW+19, YCT15, YTF+18, YLS12, YMSH10, YKC+12, YLZ+16, YXA+16, YLI11, ZKKA17, ZLW+12, ZCLL14, ZT14, ZTZ16, ZML17, ZGL+18a, ZGL+18b, ZZ12, ZHH+17, ZL12, ZVH14, ZDW+16, ZLY+19, LZJX10, HZC+14, MM12, PP11, ZBR11]. based [Kat13]. Based-Encryption
[ZHW15]. Bases [EVP10, TSH14, FES10].
Basing [Mat14, MN10]. Basis
[BNA15, ERRMG15, RERM19, CG12b, Har15, LLP+18, Tum15]. Batch
[ZIPXX17, AGHP14, CCG10]. batch-based
[CCG10]. Batters [Chi13b]. Battery
[CKHP19]. battles
[Ano15e, Ano16f, Sch15c]. Bay
[Ano10, DDS12]. Bayes [McC11]. Bayesian
[YYW+13, ZLW+17]. Be
[DSMM14, Mos18, Par12a, YM16, AZH11, Ana14, Eve16, Ree15, RK11]. BeagleBone
[Cri16]. Beat [LTKP16]. BECAN
[LLZ+12]. Becomes [Bra13]. been [Ana14]. before [GST12, Goo12]. Beginner
[Gre19a, She17]. Beginning [Chu16]. Behavior
[GSC17, RSX18, KLN15, SPK17]. behavioral
[BOP14, CAM19, HT11, MWW+18]. Behaviors
[GAF+15, HL19, ZMYB17]. Behavioural
[MT17]. Behind
[Fre10, Sti19]. Beijing [BYL10, Yau10]. Being
[NSP+18]. Beissinger [Ayu12]. Belief
[BT12]. Bell [JEA’15, QD16].
Benchmarked [MKAA17]. Benchmarking
[MTM18, ZXKK17]. Benefit [HB14]. benefits
[Wat14a]. Benford [AOT13]. Bessel
[GI13]. best [Cha13c, Tay19]. Beta
[MV18]. Beth [CTHP13]. better
[LCL+17a]. Between [HSV11, KAI18, LRW14, SAKM16, CLM+12, HLR11, KPP11, Kim16, PBCC14, WDD12].
Beyond
[JL18, LST12, MJS13, RS18, TS16b, FNP+15, JR14]. BGP [SV16].
BGV [GHPS12, GHPS13]. BGV-Style
[GHPS12, GHPS13]. Biased
[UH19, LLP+18]. Biclique
[BKR11, KD13]. Bidirectional
[GMNS15, GH12]. bifurcation [SE18]. Big
[FYD+19, GRRZ18, HLC+18, LLS19, MLO17, Mal13, MMS17b, PH16, PNRC17, PWS+19b, YDY+16, ZLW+17, FS18, HL19, LSBN14, QCX18, Tan17b, WS14, WS19].
Biggs [Low12]. bilateral [IT12b]. bile
[RBS+17]. Bilinear
[Ab12, ASS15, IL15, LZY+16, YS12, ZZ15, ZY17b].
Bilinear-map
[LZY+16]. billions
[Hof16, SMBA10]. Binary
[AD11, ADSH18, AK14, MBR15, MBF18, SA14].
Binary-Ternary
[AD11]. Binding
[HEC+12, LBC18, ZLQ15]. Bio
[OK18, GPVdBR12, ZHL+11].
bi-cryptographic
[ZHL+11]. Bio-inspired
[OK18, GPVdBR12].
BioAura [MSKR17]. biographical
[Maf16]. Biometric
[Alp18, ATI+10, BDM+19, BCTPL16, DWR12, JNL2, KHM13, LGM+16, May15, NGAUHQ16, PMG+19b, Sar12, SKV12, SRRM18, SSP19, Vet10, AHM+18, DEL19, DMT12, GCSAdP11, GBC19, HT11, Ham19, LK12, LTC+15a, MLBL12, Sar10a, Sar18a, SR10].
Biometric-based
[BDM+19, GBC19, SR10]. Biometrics
[AHN+18, BW13, ERLM16, SP13, ZPW16, BOP14, FHZW18, GM16, LXYLY12, LH10c, LNM+11, LNK+18a, MRRT17, SS17a, SCFB15]. biometrics-based
[FHZW18, LXLY12, LH10c, LNM+11].
biosensor [Kim16]. Birkhäuser [Sha10].
Birthday [LST12, SXL16, Nac12]. Birthday-Bound [LST12]. Bit
[CG14a, GV14b, HG12, HS18, LJK17, LPO+17, NIS12, Ros11, YLL+12, APPVP15, BGG+19, KS11, KFL+10, MNN12, PLSvdLE10, RH10, TWZ+12, VN17, ZSH+19]. Bit-Wise [CG14a]. BitCoding [HS18]. Bitcoin
[ADMM16, BRS17, BH15, Bra15, Chi13b, HB14, Hur16, JSK+17, Mic16, NIS12, Ros11, YLL+12, APPVP15, BGG+19, KS11, KFL+10, MNN12, PLSvdLE10, RH10, TWZ+12, VN17, ZSH+19]. Bit-Wise [CG14a]. BitCoding [HS18].
[BCG19, Jia17, LJ15, SNJ11, SS10b, Sha10].

**Bouzefrane** [Ano15b]. **Box** [BW16, BCGN16, BR14, CPS16, HHP17, KMO14, Mic10b, Rja12, SS10b, SWF+19, KOS16, LRV13, MSas13, RMP10, SGFCRM+18, ZZ12, ZSW+18a]. **Boxes** [NN12, WJ19, L15, SS11]. **Boyle** [Mat19].

**BRAMs** [DGP10]. **Branch** [EPAG16].

**Branchless** [RBS+17]. **Brave** [KMI10c].

**Brazil** [BA18]. **Brazilian** [Ut13]. **Breach** [SD12]. **Break** [Av12].

**Breakers** [St15, Mun17]. **Breaking** [AP13, CN12, Che18, Cop10a, KS11, RSMA19, TPL16, WgM11, Ant14, Bri11].

**Breaks** [Ano17c]. **breakthrough** [Goo12]. **breath** [LSR13].

**Breathing-Based** [CSH+18]. **Bregman** [CCZC13].

**Bribery** [CW12b].

**BRW** [JR14, CJP12, CJP15].

**Broken** [Bat10, Hea15].

**Brokendown** [MDAB10].

**Broker** [TKR14]. **Brocker-Less** [TKR14].

**Browser** [QF19, ACC+13, GIJ12].

**browser-based** [ACC+13].

**Browsers** [FVJ19, Ree15].

**browsing** [MWW+18].

**Bruce** [Sev16].

**Brute** [CJP12, JR14, CJP15].

**Brute-Force** [JR14, CJP12, CJP15].

**BRW** [CMLRHS13].

**BSeIn** [LHH+18].

**BTC** [CLF11, QCJ+18].

**BTC-compressed** [CLF11].

**Bubbles** [HHBS18], **Buchwald** [ABJ13], **Bucket** [BKKV10].

**Bug** [Ch13b].

**Building** [BPS16, GB19, KMP+11, MJS13, Sev16, WL11, LCKBJ12].

**built** [GS18].

**built-in** [GS18].

**Burden** [Bla12, SR14].

**Bus** [AN17].

**Business** [LB+15].

**Buyer** [Fra16, KJN+16].

**Buyer-Friendly** [Fra16].

**BYOE** [Tan17a].

**byte** [Hof15, Hof16].

**Bytecode** [SEC+19].

**bytes** [PBC14].

**Byzantine** [KS11, LKA19, YKG13].

**Byzantine-resistant** [YKG13].

**C** [AD12, ACZ16, Cra14, DJJ14].

**C1G2** [MK12a].

**CA** [ACM11, D12b, Kia11, Lin14b, Pie10, Rab10].

**CABA** [MSKRJ17].

**CABE** [HHX+17].

**Cache** [AB15, ADR18, CBZ19, DKM15, HLA15, SY15a, DJ12, DK17, MCL+19].

**CacheAudit** [DKM15].

**Caches** [LLG16, CDPLCA16, DJJ+12].

**Caching** [AD18, HLA15].

**cackled** [Bai12].

**CAD** [PGL10].

**Caernarvon** [KM10c].

**Calculus** [MR10, J13].

**Calibrated** [LC15].

**California** [Ano10, IEE11b].

**Call** [Ano16a, Ano16b, Ano16c, CS14, Hor19, KRM+10].

**Call-Back** [KRM+10].

**Calls** [Mur16].

**can** [PKS18].

**Cambridge** [ACM10, PJ12].

**Camellia** [BJS15, LWP12, LWP14, SEH12].

**Camellia-192** [BJS15].

**cameras** [MK+12].

**Can**

**Can’t** [RAS15].

**CAOVerif** [ABF+14].

**Capabilities** [GFBF12, Lop15a, KMG17].

**Capability** [IA15, LLZ+17, LT13].

**Capability-Based** [LLZ+17].

**Capacity** [LLY+18, TQ18, WYL18, XNR15, YWW10, BCD19, CLZ+17, GHJ12, PW11, WLH13].

**Capacity-aware** [TQ18].

**Capacity-Raising** [YWW10].

**Capitalism** [Fid18].

**CAPTCHA** [OTO18, SKE14].

**CAPTCHA-based** [SKE14].

**Capture** [MBC+18, NY+14].

**Capture-the-Flag** [MBC+18].

**captured** [SPK17].

**capturing**
[PKS18]. Card [BDFK12, HMR12, HCL+14, PDT12, Ano17c, CLHHJ13, GLIC10, LNKL13, Mar10b, Chol10, SD12]. CARDIS [GLIC10].


CBA [KRM+10].CCA [AHS14, BW16, CB1916, CZL14, LLPY16, LTZY16, LSLW15, LLG19, MSas12, PDN15, SYL13, SLZ12, yYQWz13, ZY17a, ZSW+18b].

CCA-Secure [BW16, CZL14, LTZY16, SYL13, yYQWz13, ZSW+18b]. CCA1 [M13]. CCA2 [Gal13, GV14b, LLW16, LLSW16, MVVR12, RG10, Z1Z12, ZY17b].


CTA [YFT17]. cell [LLY+12a].

cell-counting-based [LLY+12a]. Cells [SB16].

Cellular [dRsd1C12, FMA+18, HB16, HCM11, KRM+10, SS11, WOL12].

Censorship [DR16]. centralized [NAACL12].

centre [McK10, McK11, Pa16, IS+C+16]. Centric [DLZ+16b, FP19, Vle12, XZH+19, ZVG16, AHM+18, BLY17, BPP10, PN10, YWY+19].


Certificate-Based [GWWC15, HP12, LTH+15, WMS+12, YLZ+16, GLL+18, LL16a]. Certificateless [CT18, GWWC15, IL15, LZCK14, RSD19, SZS14, TCL15, WMS+12, YT11a, YT11b, YJS18, ZSY19, HPC12, JXLZ15, LL16b, SGJ+18, ZQWZ10, ZY17b]. Certificates [MW16, SC12, GIJ+12, HERE14].


chaff [KHM13]. Chain [EAA+16, FVK17, KP13, QZL+16a, QZL+16b, YFT17, YSF+18, YFT18, CR12, Par18, CL16, SJWH+17]. Chaining [GGK18, YM18, EA11]. Chains [GGK19, JSK+17, HLYS14, JCHS16].

Challenge [AD12, GHS14, SPK17, YDH+15, ZCC15].

Challenges [CN12, FS15, FRA15, LA14, LLG16, MRS+17, PCK20, PCY+17, SBV14, TCMLN19, ALL+18, HOD19, KJN+16, WS14]. Chances [ALL+18].

Change [KMI18, ZWT13]. Changeable [FGM10, ZCL+12]. changed [Mac12].

changes [PTRV18]. Channel [AN17, ASN11, Bu18, CDK+10, CBL13, CATB19, DZS+18, EWS14, GWM16, GPT14, HLH19, KOP12, LGR14, NDC+13, PR12, SG15, TT12, YLI7, ZBPF18, ADG16, BVB12, CPT18, CAM19, DMWS12, DJL+12, GZSW19, GSAV18, JLT+12, LFK19, MFH13]. Channels [ASN12, BGN17, DKMR15, EPAG16, KW14, SS19, Vua10, AGH+17, BCND19, BEB+18, CL16, DMV15, DLC+16, LWZG10, MCL+19, NR11, SRB+12, ZPZ+16].

Chaos [AIA+18, LW13c, RR11, RVRSCM12, C11, LW13b, jT12b, ZLW+12, SGFCRM+18]. chaos-and-Hamming [C11].

Chaos-Based [RR11, RVRSCM12, AIA+18, LW13c, ZLW+12].

Chaotic [BCGH11, IAD10, LF+18, Ye10, Bro19, GCH15, IS+C+16, KLW+16, LWK+18].
LW10, LZKX19, NES+14, WGZ+12, ZT14]. Chapman [Ful10]. Character [SS12b].
Characteristic [BGJT14, SR10, ZWZ17a, BGJT13, Jou13]. Characteristics [SSP19, TCMLN19, BEB+18].


Ciphers [ABS+12, BMS12, BSS+13, BM18, BKLS12, Bru12, CWP12, DGFH18, DGIS12, DJG+15, EGG+12, EKP+13, GT12, GST12, GLN12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCLW17, LGLL12, LJ16, MD12h, NN12, PDJ+19, Pud12, Sas12, SEHK12, SJKL18, Vua10, WH18, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KM10a, LGBP19, LKMK11, MLC+19, MRT10, MH15, MHY+18, QGGL13, SKK10, TQL+14, WB12]. Ciphertext [BDPS12, CWWL12, CHH+19, zGXW12, HLW12, JMG+16, JSMG18, KA17, LZC12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XMCL13, XWLJ16, YLM19, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, KTT12, LCT+14, LFWS15, LZC14, LDZW19, QRW+18, RD17, SGM16, WLFX17, XWS17, LAL+15, LHL15]. Ciphertext-only [KA17]. Ciphertext-Policy [CHH+19, Rao17, XMCL13, XWLJ16, ZHW15, JSMG18, LFWS15, LDZW19, QRW+18, XWS17, LAL+15, LHL15].

Compress [LC13]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16].
Compressed-Domain [WLZL12].
Compressibility [HN10]. Compression [CNT12, DLGT19, DA12, LD13, MAL10, PMZ13, PPP10b, TCN+17, WHZ12, ZSP+19, Ara13, CMMS17, DTZZ12, LK14, Li10, LPZJ15, PP11, QZ14, RSMA19, SI12].
Computer-Aided [BGK12, BCGK12, BGB12, ABBD13]. Computers [Mos18, Cop10b, LCKBJ12, Mac12, MvO11, PHWM10]. Computing [ACM10, ACM11, AJA16, Aoi17c, BCG+12b, BTK15, CLB19, Cer14, CGB+10, DXA14, EAA12, FES10, Gen10, GB19, JWNS19, KMSM15, KP17, LCK11, LT14a, LYZ+13, LLC+15, LLGJ16, LNX15, LXY15, MLO17, OS16, PAF18, Pet12, RS18, SJWH+17, SL10, Vai11, V1e12, XMLC13, XWLJ16, YE12, YZDZ19, YHL16, ZLDC15, AaBT16, AAZ+16, And13, CZ15b, CSTR16, DKL+16, DWZ12, Gop19, HSM13, HYS18, Jeo13, JSMG18, KKA14, KKM+13, KKM+14, KSB+17, KH18, LKX+14, LYL15, LHL15, MS12a, NR17, Nam19, NCCG13, PPA18, PP11, PKA15, QZDJ16, QRW+18, Rao17, Tan12b, WSC14, Wan18, WDKV19, WLS14, WL19, XXX15, XZP+19, XXY+18, XTZ+19, YHHM18, YWJK+10a, YQOL17, YY11, ZWS+18, ZLY+19, ZSW+18b, YXA+18].
XTZ+19, XLC+19, ZZ11].
conjective-subset [ZZ11]. Connection [CW12b, HLYS14, WGD18, MZ17a].
Connectivity [GTT11], conscious [Ree15].
Consecutive [Tan12a]. Consensus
[ABCL17, JSK+17, LLKA19].
Consequences [Ess17, SS19, WVC19].
Consideration [CJP12, CJP15, KM10b].
Considerations [BF19, KD12b].
considering [MLMSMG12]. Consistency
[BCK17, SES+16]. Consolidated [KKA14].
Constant [App14, AEHS15, BBCL19,
CWWL12, KOTY17, HKPP16, KMO14,
LP11, LSQX19, Pan14, ZMW16, AHL+12,
DWZ12, LCT+14, SG16].
Constant-Round
[KOTY17, KMO14, LP11]. Constant-Size
[AEHS15, AHL+12, LCT+14, SG16].
Constant-Time [BBCL19]. constants
[DWZ12].
Constraint [WZ19]. Constraints
[CCKM16]. Construct [SGY11, WT13].
Constructing [CDSLY14, ZSW+12, HRV10].
Construction
[BWLA16, DF11, EM12, FZT14, GWWC15,
HHPL17, KMO14, MSas12, Rog16, Sar10b,
ST14, WZ15, WCL+18, WMS+12, XHX+17,
ZL19, LFZ+17, MSas13, SA14, YWL+17,
YT11b, YKC+12, ZCLL14].
Constructions [BCF+14, DQPL12, HL10b, KOTY17, SNJ11,
SES+16, CZ15a, CGKO11, NAL17, Zim10].
Construct [Mau12, WB12], constructs
[BP10]. consumption [JS18a]. Containers
[HVP+18]. Containing [XWDN12].
contemporaries [LCKBJ12].
Contemporary [Opp11].
Content [ADR18, BCP14a, MHT+13, PMZ13,
PSFS15, WHZ12, WZXL12, YT12, ZXZ+11,
GPN+12, HPL+19, JS18a, YWW+19].
Content-based [MHT+13, YWW+19],
content-centric [YWW+19]. Contents
[BCG10, MSM+18b, SKS+18]. contest
[Cra14]. Contests [WXY+17]. Context
[AKS19, Fra16, SYV+19, ZCWS15, BGE+18,
SSSA18]. Context-aware [AKS19].
Context-Driven [SYV+19]. contextual
[Svo14]. Continual
[BKPV10, XZY+12, YZ12, YCY12].
Continual-Leakage [YZ12]. Continually
[DLNW11]. Continuous
[ACAT+15, BCF16, DHLAW10, uHAN+18,
FMNV14, GMDR19, MSK17J7, PYP10,
SCFB15, Sch15b, SRT12, Yam12, ZY17a,
ZYM18, ZYH+19, ARL13, BTW15,
CXX+19, CRS13, PLGMCdF18, SCR19].
Continuous-Tone [Yan12]. contract
[MMP19, Men13b]. contrast
[DAM+14, GLW13, LYL10b, MM14a].
Contributory [WQZ+16]. Control
[AMSPL19, ATS15, BFK+10, DLZ+16b,
GGK18, GRZ18, HBC+19, HHS+15,
HLC+18, LGM+16, LGLK17, LJP17, MM17,
MK12b, NA10b, PV17, QZL+16a, RSN14,
SC14, SYV+19, TBCB15, XMLC13,
XHZ+19, YTH17, ARL13, ACK+10,
AMHJ10, CLH+16, CO11, Cra11, FG19,
FNWL18, FS18, GHD19, HPJ+19, JAS+11,
LCL+17a, LCL+15, LHH+18, MDHM18,
NM10, QCLX18, RR17, Sch15c, SA15,
Tan12b, Wan18, XHH12, XYML19,
YWJ+19, ZML17, ZDHZ18, ZVH14,
ZWS+18, ZFZ+18, ZZL+18]. Controllable
[FH13, ZLDC15, ZHT16]. Controlled
[FMTR12, WP17, Har16, SM10c, XLC+19].
Controller [GMV17]. Controllers
[AMH+16]. controls [CGH11], controversy
[McG11]. conundrum [Eve12].
Conversations [WBC+10]. Converse
[KPKS12]. Conversion [BJ10b].
Convertible
[CLL16, LH11c, HL11, LHH11, XWXC14].
Convex [LLSL19]. Convolution
[DWZ18, HW19]. Convolutional
[WL18, KMG17, MG15]. Cookie [FV19].
cookies [DCAT12]. Cooperative

D [AP10, Bro19, CG12b, DBPS12, DWW12, EAA+16, GZHD12, KWS+12, LJ17, LJ15, MCD12, MKH+12, PGLL10, RS16, SGS14, SRK+17, SRK+18, WSSO12, WY12, tWmC12, Y114, YPRI17]. D-Based [WSSO12]. D-like [LJ15]. D-PUF [SRK+17, SRK+18]. D2D [Gop19, PSM+18]. D2D-Aided [Gop19]. Dana [Ano10]. Dandelion [VFV17]. Dangerous [HLW12, GIJ+12]. Dao [FMS12a, Dao-Fa [FMS12a], Daoism [FMS12a], Darel [Xie12], Darmstadt [FBM12, Sen10], DASH [KCC17]. Datas [ARWK19, Ano13c, ADF12, Bar12, BJL16, BCD+12, BJL12, BW12, BKLS18, CML+14, CMS15, CCW+10, CSV15, CCT+14, CLW16, CDLW19, CHH+19, DDS12, Dan12, Dr12, DK16a, DMS+16, DA12, DCA18, DLZ+16b, EKB+16, FMY15, FYD+19, FPY15, FRS+16, GTT11, GRRZ18, HSM14, HWZ18, HLT+18, HLT+15, HVP+18, HZX+18, HK14, IBM13a, KRDH13, KG16, LLP19, LLZ+17, LLS19, LWC14, LLZ+12, LZZ+12b, MLO17, Mal13, MMS17b, MJW+18, MG19, MJ14b, NNAM10, NR12, PV17, PD14, PSM17, PZL+19, PBC+17, PHI2b, PH16, PNC17, FWS+19b, QZL+16a, QZZ18, RCP+18, Rea16, RSN14, SG18, SAKM16, Sar10b, SNSK18, SP15b, SKH17, Sia12, SLM10, SR16, TCN+17, Tan15a, Vai12, VSV15, WZCC18, XNK15, XWS16, YDY+16, YDZ19, YJSL18, YMC+17, ZXY16, ZPXX17, ZTL15, ZLW+17, AP10, ASO14, AIM+19, Ana14, Ano11a, Ara13, ADH17, ALL+18, BBL+19, BHI19, BTPL15, BC18]. data [BKV13, BT15, CDGC12, CLH+16, CDF+10, CDL10, DFJ+10, DTZ12, DRD11, ED17, FS18, GHD19, Gen10, GLB+18, GZS+18, HSM13, HKA19, HKE+15, HLS19, HML16, HSV18, HYF18, JKA+18, JHCC14, Kim16, KH18, KWH16, LSN14, LT14b, LXX+14, LZY+16, LLL+17b, LHL+18, LFWS15, LAL+15, LCW+16, LZC17, LLL+18, LL16a, LHA+16, MHK14, MRR+18, Nam19, O018, OSS16, PM19a, PWS19a, QCX18, QYqWqZC13, YY11].
QLZ19, RR16, RR17, SLL+19, Sch15c, SYY+17, SAR18b, SPK17, SWW+17, Tan17b, TMK11, TKM13z, WLWG11, WLH13, WDZ19, WLS14, WZLW13, WS14, WS19, WL19, XXX15, XWZ+18, XYW+18, YYS+16, YQOL17, YXA+16, YNX+16, ZZKA17, ZMM+10, ZWY+13, ZSC17, ZHT16, ZZL+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, PBP19, PRZB12, SVGE14, Suc12, XMY+17, YX18], Databases [FCM14, HPC10, JKHeY12, Kaw15, RP12, WP17, GA11, JK13, LCY+16, SS17a, TG12], datacenters [PRN+19], Dataset [SP13], datasets [LVRY10], Datasets [DPP10b], Daubechies [Ara13, SM12], Daunting [IBM13a], Days [Bai12, Bri11], DB [PYH+18], DBDH [CW14b], DBMS [SERF12], DC [LHF12], DC-Net [LHF12], DCT [BDB14, LP12, SS17b], DDH [LZC12a], DDoS [PSI+13, SP15a], De-synchronization [XNG+14, AATM18], Death [Moo14], Debate [Bla16], Debiasing [USH19], Debs [SM15b], debugging [MFH13], Decade [SOG15], December [Abel0, BYL10, BC11, Che11, GG10, HWG10, LH10a, LW11a, LTW11, Yan10, Yan11], Decentralized [ABCL17, CD16, GZZ+13, HSMY12, HK14, MT17, PPS12a, PAS13b, RH+16, RSN14, TS16b, XTZ+19, YM19, HHS18, SLL+19], Decentralizing [LW11b], Deception [GA19, vdWEG18], Deciding [CLCZ10, sch12c], Decipher [Cor14b], Deciphering [Bla16, GMNS15, GSAV18], decision [PKA15, RPG12], Decisional [CCL+19, LZC14], Decisions [Bel18a, YWK10b], declarations [HWY14], Declassified [ABJ13], Decodable [Yek10], decoder [PMG19a], Decoding [DBPS12, GMNS15, Bax14, Bul10a], Decomposition [AGH+17, LSL12b, gWpNyY+14, BWA13], Decompression [PP10b], Deconstructing [Tar10], Decrypted [Kob10], Decrypting [CR12, Tay19], Decryption [AN12, KB10, PTK12, FNWL18, LJW+17, LJWY18, SES+16, SM10a, SM10b, Wu16, XTZ+19, XYL19, ZSW+18b], Dedicated [Lin17, Nac12, NSP+18, AKS19], deductive [ABF+14], Deduplication [CDLW19, MGJ19, QLL17, SKH17, YDY+16, YZDZ19, ZHZ+19, KH18, SAR18b, ZFH+18], Deep [DLGT19, FGR+17, WYL18], defeated [Kap13], defects [FES10], defences [NDNR13], Defend [Ano17e, Sch13], Defending [LWCJ14, YFT18], Defense [MPA+18, PSJ+13], Defenses [AN17], Defensive [Pfl10], Defined [KYEY+18, SAM+18], definition [LWL10a, WSC14, YKC+12], Definitions [BBD19, GLW12, MAu12, CGKO11, KM14, KGO10, XXWC14], Degeneracy [WH18], degradation [MMS+17a], Degree [KA18, LH18], degrees [MZ17a], Delay [CCKM16, GMNS15, LFX+18, LBR12, M KK17, JLT+12, XW13, MCL+19], Delegatable [WZ11, XLC+19], Delegated [MZHY15, TMC15], Delegation [FMTR12, SSW12, XWL16, YZ12, YAM+15, JSMG18, NAL17, XWS17, XPZ+19, ZWM14], Deletion [DMS+16, MGJ19, Rea16], Delfs [Mur10], Delivery [PSS+13, SSPC12], demand [KKJ+16], Demodulation [KOP12], demonstrating [LHA+16], Demonstration [GKG19], demosaicking [HLC16], Deniability [TCS14], Deniable [DF11, zGXW12, HLLC11, HS11, Jia14b, JXLZ15, LXL14], Denial [BKBK14], Dense
[BFM12]. **Density** [Gre19b, LC15, LSQ11b]. **Density-based** [LSQ11b]. **Dependable** [BCQ+13]. **Dependency** [SGP+12].
**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, Lau12]. **Derivative** [LSQ11a]. **Derivative-based** [LSQ11a].
**derived** [JS18a, ZMM+10]. DES-like [CGCS12].
**Design** [AMN18, Abe12, ARH+18b, AIB+16, ADD10, AUMT16, Bel18a, BKL+13, DZS+18, DHB16, DR11, FSK10, HSA14, JLZ18, JWJ+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QLL17, RYF+13, Sch13, SAAB10, SZDL14, THA+13, VKPI17, WKB16, WDKV19, ZHX16, BBDP16, CZ14, DRN16, Gor10, KHF10, KDW+17, MNNW15, MAH+12, MHY+18, SVGE14, ZYC+17].
**Designated** [WHJ17, HYWS11, RPSL10, SY15b]. **Designated-verifier** [WHJ17].
**Designation** [Che15, LSQ11a] designed [Goo12]. **Designer** [KMY18].
**Designing** [CDK+10, DZS+18, FLW12, MRT10, PSD15, SR10]. **Designs** [BGK12, PCY+17, KDH15].
**desynchronisation** [LDC13]. **Detected** [Ess17]. **Detecting** [BKK14, Ess17, GAS+16, HLIW12, KW14, SH15, YSC+15, LLIW11]. **Detection** [AMKA17, ATS15, ARWK19, CBO+18, DSB15, DF11, GZH17, HDWH12, KU14, LGL+12, LC15, MKRM10, MKAA17, MKASJ18, NDC+13, NSMS14, SAJL16, SBV14, SXH+19, SP15a, SRAA17, SGS14, TM18, YFT17, AKKY17, AOT13, BM13, HB13, JC13, KLC+10, LDC13, Maz13, MHT+13, WYL13, vWEG18].
**Detective** [Cho10]. **Detector** [LTKP16]. **Detector-Based** [LTKP16]. **Determine** [FSWF11, Sto12]. **Determining** [Bar19, NN12, Scr18].
**Deterministic** [MPRS12, NIS12, XXZ12, DTZZ12].
**Deterring** [WGJT10]. **DEUCE** [YNQ15].
**devoted** [Hamilton].
**Developed** [Ham19]. **Developed** [Har16].
**Developed** [Ham19]. **Development** [CH11].
**Development** [Pau10]. **Developments** [GCK12, Vai11].
**Device** [ADIM19, ABCL17, CFXY17, DFKC17, HSUS11, KLM+12, SRK+17, SRK+18, TYK+12, ZSH+19, CRS13, GM16, KKG14, Kim16, OSP+19, Par12b, SHBC19, VV19, XHH12]. **Device-to-Device** [ADIM19]. **Devices** [AAC+16, BDM+19, CSY+18, DLW11, EGG+12, FMC19, GPT12, GD16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, RC18, RSM18, RPH11, Sch15b, SFE10, SWF+19, VWC19, WKB16, WT10b, XJR+17, Aia15, CLP+13b, CFL13, CTL12, Chi13a, FRT13, GTSS19, IB11, KPP16, LKAT12, MV10, MHT15, NSBM17, OYHS14, PCK19, SSNS15, SCR19, SHBC19, TZTC16, TG17, ZPZ+16].
**DFA** [PDJ+19, WH17]. **DFA-Resistant** [WH17]. **DFT** [DDFR13]. **DHA** [AKY13].
**DHA-256** [AKY13].
**Diagram** [WGD18].
**dictionary** [NN15].
**dictionaries** [ABR15].
**Diff** [Maf16, MBB11]. did [CMG+18].
**Diego** [Ano10, Lin14b].
**Dies** [Mar10a, MMB17].
**Difference** [BS14, YTP11, JK13].
**differences** [LHM13].
**Differencing** [LyW12, YWW10].
**Different** [GZ12, HHH+13, KU12, AKK+17, ABW10].
**Differential** [BMS12, BNY14, CPW12, CGCS12, ESS15, FXP+17, KWS+12, LYK19, LGL+12, LJF16, LJ15, LYHH14, MRT12, PH12a, QGGL13, RCP+18, Sun11, WHN+12, Blo15, DDFR13, LLL10, MNP12, PBCC14, SDM10, SDM14, TSLL11, TS16a, WYL14].
**Differentially**
[RCBK19]. Differentials [WW12].
Differentiation [Söd13]. Differing
[GGHW17]. Differing-Inputs [GGHW17].
Diffie [LZC14, ABD+15, Chi16, Hof16, HLCL11, HLYS14, LNL+19, Orm16, RH10].
Diffusion [ZHL15, WB12, jT12b]. DIG
[NKW14]. DigiNotar [JB11]. digit
[KWH16]. Digital
[AYS15, BBC+13, BM13, BCP14a, FMS12a, FR15, GP17, HPO+15, Jin10, Joh10, JL16, LNC+12, MBF+13, MSI10, MMN12, NC12, nPyWY+14, Orm16, PH12b, PAS13b, SAA15, SM13, Söd13, SC12, SOS15, TC11, TAP19, TS16b, Yon11, Y+17, YLS12, dRSdVC12, AGHP14, BPP10, Bro19, CCG10, Cls18, FLZ+12, Fri10a, GMS11, Har14, HAGTDFR13, KM11, Lan13, LWZ10, MS13b, MM14a, MO14, QCX18, Sim15b, SL10, yWpYNL11, ZKKA17, Zet14, ZSMS18, Ano13a, Ano15b, Mou15].
Dilly [Bat10]. Dimensional
[Ano17d, LLY+18, LZC+12b, XYXYX11, XL+18, DWZ12, QD16]. dimensions
[Fal15]. direct [GH12]. Directed
[NLLJ12, KPS10]. Direction [NS12].
Directional [JS18a]. Directions
[BKBK14, CDFZ16, Hof16, PPA18].
Directly [LZC12a]. directory [SMABA10].
Disability [Söd13]. disabled [HFT16].
dissociation [TMLS12]. Disaster
[NRZQ15, BBG+17]. Disclosure [SY+19, DZS+12, PKA15, SB17, WGTJ10, ZCC17].
Discovery
[MJW+18, MJS+19, Ano11a, MMP19].
Discrete
[BGJT14, CLL16, HKR+18, KLM+12, SRT12, Xie12, AMORH13, BGJT13, BGG+19, MM13, Mes15, TPL16, VM14].
Discrete-Continuous [SRT12].
discrimination [GPVcBRO12].
Discriminative [DHLT19, YT14].
Discussion
[Gil12, Wil18, Bull10a].
Discussions [KD12b]. Disk [GM14, Ran16].
Disks [Mar10c]. disparate [SSY12].
Dispatching [YTH17]. dispersed [ED19].
Disreputable [ABJ13]. Disruption
[HK14]. Disruption-Tolerant [HK14].
Dissection [Dun12a]. Dissent [SCGW+14].
Distance [ABB+19b, HK18, PYH+18].
Distance-Bounding [ABB+19b].
Distillation [BJ16]. Distinguisher
[DWWZ12, AMS+10]. Distinguishers
[SEHK12, ZSW+12, AY14b, AP11].
Distinguishing [KMK0a]. Distortion
[FHS13, Jia17, LGW12, MM17].
Distortions [WLZ12]. Distributed
[ADH19, Ano10, BKBK14, BEM15, CGB+10, DCA19, FCM14, KY+19, HSM+14, HEP+11, HXC+11, HCL+14, HZX+18, LM16, LL15, LNZ+13, LWC14, PBC+17, SWF+19, SB18, YXZ+12, YK11, ZLDC15, BVL17, CSTR16, dCCSB+16, FG19, GAI+18, NDS+17, NCCG13, PR+19, TG12, XW13].

Distributed-Healthcare [ZLDC15].
Distributing [Kip13, MS16]. Distribution
[BCG19, EAA+16, JEA+15, Lop15b, MT17, MSU13, NNA10, SK11, SN11, Saa18, TC10, AASSAA18, ABB+14, BB14, BGP+17, CML16, FHZW18, JKS+16, JLT+12, LLP+18, NACL12, VV19, YWL+17, Yan14, YHS16, YL11, ZWS+18]. dithered
[UUN13]. Diversity [ZLTL15]. Division
[HJ+19, SS12b, YWM19, MN14]. Divisors
[CN12]. Divulge [ABJ13]. DLSF
[PNRC17]. Dmail [CCS14]. DNA
[AEH17, HEK18, WGT+12]. DNP3
[ACF16, CDWM19]. DNS
[HLAZ15, PCK20]. Do [Bow11]. doc
[NN15]. Document
[BTHJ12, BPP10, DBPS12, DS19].
Document-centric [BPP10]. Documents
[Bla12, HCM12, Sta13, ZZX18, ZDL12, CH11, GA11, SR14]. Does [GA19, LRW17].
Doesn’t [RS11, SS12a]. dog [Ran14].
Doing [JCM12]. Domain
[AGW15, BDFK12, BBM15, CLY14, DG17, LA15, MR16, PDM12, SZH19, SGY11,
SAM^18, WLZL12, gWpNyY^+14, ZWZ17b, AMKI2, BGAD12, GJ13, IG11, LXCMM11, LPZJ15, LBR12, PWW10, QMC17, SCKH10, yWpWyYpN13, YZL^+18, YWK^+10a, YCM^+13. **Domain-Specific** [BDFK12]. **Domains** [LQD^+16, LRWV14, KGO10, NES^+14].


**Double-Boomerang** [BCG10]. **Double-SP** [Sas12]. Doubling [Zha12]. Doubly [CFZ12, CW14b]. Doubly-Spatial [CFZ12].

Douglas [Ber16a]. Down [Aoi17e, McG11].

**Download** [ZGC16]. **DPA** [JZ11]. **Draft** [MCEF17]. **DRAM** [SRK^+17]. **SRK** [SRK^+18].

**DRAMs** [LSC^+15]. **DRAW** [NSBM17].

**DRAW-A-PIN** [NSBM17], drawn [NSBM17]. **DRBG** [YGS^+17]. Drift [GKS17, JSZ12]. Drift-Compensated [GKS17]. Driscoll [Bur11, Joh15]. Drive [DGFH18, SYC^+17, Mac12, SYW17].

**Drive-Thru** [SYC^+17, SYW17]. Driven [BMP12, DLM^+18, SYv^+19, APMCR13, LSQ15]. driver [GBC19]. **DriverAuth** [GBC19]. **DriverGuard** [CDD13]. **DRM** [Pet12]. **Drones** [SNCK18]. **DSA** [Dra16].

**DSC** [LJ19]. **DSP** [MS13c]. **DSPs** [DGP10]. **DPs** [DSS12]. DSSH [YLS12].

**DTKI** [YCR16]. **DTLS** [AP13]. **DTRAB** [FTV^+10]. Dual [BWR12a, CCG^+16, CMG^+18, HF14b, HPL^+19, NLYZ12, PAF18, BW13, CFN^+14].

**Dual-Mode** [PAF18]. **Dual-Rail** [HF14b]. **Dummy** [GST12]. duplication [LWJ11].

Duqu [BPBF12]. Durable [LY15]. Durfee [TK19].

**During** [FGR^+17, ABJ13, BDM^+19, RS17]. **DWT** [LD13, SJ12]. dyadic [MO14]. Dynamic [ABB19a, BCG10, EKB^+16, FHR14, HH15, KYH18, LHM^+15, MWZ12, MM12, NKWF14, OMNER19, PPS12a, PNRC17, RC18, SSW12, SY14, SVK12, SG14, VM15, XNKG15, XWSW16, XYZ^+12, XWZ^+18, YLSZ19, XYZL16, BSBG19, CTL12, CSTR16, DSCS12, EA11, GLM^+11, GLB^+18, JZS^+10, KKM^+13, KH18, KPB17, LDC13, LXMW12, LMH14, LZC17, LZZ19b, NSX^+18, NPH^+14, PZL^+19, PSJ^+13, SES^+16, SSS11, SM10c, SGM16, WDC19, XHM14, YZL^+18, YD17, ZSMS18, ZZZ^+18].

dynamic-identity [JZS^+10]. dynamical [JT12b].

**Dynamics** [RSCX18, AaBT16, GEAH11, LTC^+15a, LüId12, MCRB19, TzTC16].

dynamics-based [AaBT16]. dyslexic [Bha16].

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

**E-Health** [AMSPL19, WMX^+17, AKS19, IC17, OSP^+19, YZL^+18, JKL^+16].

**E-Learning** [You11]. e-mail [BTW15].

**E-passport** [NSBM17]. **E-rental** [LY14].

**E-Voting** [KV18, LGPRH14]. **E2** [WYL14].

**EAC** [LZJX10]. **Each** [YLL^+12]. **EAP** [FLH13, HZC^+14, ZCL14]. **EAP-based** [HZC^+14, ZCL14]. **Early** [Bel18a, Bro11, And13]. **Earth** [Har14].

easier [MBF^+13]. Easy [Bel16, SMDS11, Tay14, Wu16, ZDW^+16].

**Eat** [DSSW14]. **Eavesdropping** [CW16, Han12, PX13, YSJL14]. **EC** [Dra16, CFN^+14, CCG^+16, CMG^+18]. **ECC** [BSSV12, CBL10, HJ19, JMW^+16, KRH18, ZSH^+19]. **ECC-Based** [BSSV12]. **ECDSA** [BBB^+16a, DHB16].

**ECG** [HW19, PLGMC18]. **ECG-based** [PLGMC18]. Echo [DLM^+18, HGT15]. **Echo-Based** [HGT15]. **economic** [WDZ19].

economy [Sir16]. **Ecosystem** [Fri13, RVS^+18]. **Ecosystems** [LDB^+15, MPP19]. eCryptfs [XZL^+19].

**Ed25519** [TV19]. **EDAK** [ABB19a]. **EdDSA** [JL16]. **Edge** [AHM^+18, DF16, KA18, XHZ^+19, JZU^+19].
MD15, PRN+19, Sun16, XZP+19.

Edge-Based [XHZ+19]. Edge-centric [AHM+18]. edge-enabled [JZU+19].

Edition [Cor14a, Kob10, Gre19b]. Editorial [OK18, Ano19a]. Editors [BdD19, LLK18].

Education [LRVW14]. Edwards [ADSH18, JL16, LT14a, YTS12].

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

Eect [PLGMCdF18, WB12]. Eective [HLT+15, KRDH13, WMX+17]. Eectively [YMC+17]. Eects [MAL10, SKV12, SHBC19].

Eciency [ABF12, Chi16, DG17, FRS+16, HRV10, LLML12, LCL+17a, MS13b, WXL16].

Efficient [ABBD13, ASBdS16, ABB19a, BWLA16, BCGH11, BHG12, BV11, BV14, CG12a, CML+18, CMLRHS13, CWWL12, CJ13, DA18, DWB12, Duni12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GHT11, GPN+12, GPT12, GH15, GZ17, GCH15, HZC+12, HZC+14, HZL18, HL10b, HBCC13, HZX15, HKL+12, HI12, HDPG1C15, HCDM12, HH16, HC17, IAD10, KPC+11, Kim15, KHPF16, KKK+18, KH10, LLP+18, LDDAM12, LST12, LNNH13, LXK+14, LCLL15, LSLW15, LLSL19, LH10b, LWHS17, LZC17, LBOX12, MX13, MTY11, MVR12, MU12, MKASJ18, MC11, MN14, NES+14, NdMWW16, NZM10, OSP+19, PB12, PAF18, PZL+19, PRC12, PG12, PCPK14, PRNC17, RSD19, RBHP15, SLL+19, SGY11, SZS14, SOR16, SGM16, TSB18, TCLF16, TWZ11, TT12, TM18, USH19, WDCL18, WSL14, WQZ+16, WCCH18, XLWZ16, XMCL13, XMY+17, XHZ19, YHL16, YNR12a, YNR12b, YLW13, YNQ15]. Efficient [YLA+13, YS15, ZQWZ10, ZLH+12, ZSW+12, ZZJX+14, ZXYL16, ZCL+19, ZHS+19, ZPW16, ZHW15, ZZC17, AZPC14, AZF+12, ABBI13, CH11, CCWW11, CLHJ13, CZ14, Cho14, Crla11, CGKO11, EA12, FLL+14, Far14, FA14a, FA14b, FIO15, FZZ+12, FNWL18, GH16, GLM+11, HPC12, HYS18, ISC+16, IB11, IOV+18, JCHS16, JZS+10, KKG14, KIH19, KLI11, KSH18, LLLS13, LH11b, LH10c, LXMW12, LZD+19, LAL+15, MDHM18, MLM16, Mes15, Nov10, NXS10, OCGD11, PZBF18, PC14, Rao17, SZMK13, THA+13, TLL12, Tso13, TKKH14, VN17, WYL13, WL+16, WT10a, WXK+17, XWZW16, yYqWqZC13, ZLY10, ZZ11, ZCLL14, ZTZ16, ZZC15, Zlu13, LLZ+12, TCL15]. Efficiently [FWS13, LGH+17, SLY+16].

Effort [RSBGN12]. Effort-Release [RSBGN12].

EGHR [CML+18]. eHealth [TMGP13].

eID [SGGCR+16]. eight [Sun11].

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

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

Election [ADH19, Ess17, TKM12].

Elections [CEL+19, QS18]. Electoral [CEL+19]. Electrical [VYT18].

Electrocardiogram [BLL+19, OMPSP+19, ZGL+18b].

Electrocardiogram-based [ZGL+18b].

Electrocardiography [LLH18, YH16].

Electromagnetic [HHH+13]. Electronic [Bla12, PWVT12, SR14, YMWS11, CLC+19].

Elementary [Led16, Sch15a, CM13].

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

ElGamal [HLH19, ADM19]. ElGamal-like [HLH19].

Eliminating [Sod13]. Elliptic [ADM19, ADI11, AK14, ARM15, DW12, FHLD19, Gre19a, GPT12, LGH+17, LWHS17, MST18, PPH12, SG15, Sh17, AMN18, BAAS13, BL14, BL17, BBB16b, Ch14, Far14, IB11, KK10, MC18, MS13b, NZM10, SH15, WHJ17].

elliptic-curve [BL17].

Elliptic-Elgamal-Based [ADM19]. ELmD [BDMLN16]. Elsevier [Ano15b]. Email [Bel16, CCS14, XJW+16, WR15].

embed [KPS10].

Embedded [AB15, BS12, BJCWA17, CXFY17, HJ19, HC17, JWJ+17, JLP17, LWHS17, MGG+19, SOG15, SK12b, SWF+19, SS17b, SDM+12, WXY+17, YGD+17, YS15, ZSH+19, Ano11a, CVG+13,
Embedding [ER10, MFH13, WHZ19, XWZW16].
Embedding [FR15, KD12a, MCD12, XNRG15, XNP18, XZZ18, YE12, ZS12, EA11, LHM13, MKH12, PWL13].
Embeddings [FH13, Emergible [YT12].
Emerged [McG11].
Emergence [LMB12].
Emergency [HLKL15, YTH17, BDM19, KLC10].
Emerging [BSV12, KSA16, OS16, FPBG14, ZHH17].
Empirical [GWpNyY14, EBFK13, Sar14].
Employees [Mor12].
Employing [LGLK17].
EMV [Cho10].
Enable [SMS14].
Enabled [GPT12, HFT16, KV18, QZL16a, QZL16b, SG12, SGC16, SSPC12, YSF18, BMM12, JZU19, NML19, TODQ18, YFT18].
Enabled/disabled [HFT16].
Enables [IBM13a].
Enabling [FRS16, GWY19, JSM18, PSM18, SSY12, WPZM16, YSF18, MMP19, Sch12b].
eNB [CLM12].
Enciphering [CMLRHS13, HMR12, MLCH10, MKAS18, Sar11].
Enclaves [WBA17].
Encoded [DG17, HS18].
encoder [PMG19a].
Encoding [BR14, CK18, SK12a, TJZF12, XHX17, PC14, Sun16].
Encounter [NA10a].
Encrypt [RAZS15, Ran14].
Crypt [ADR18, BTHJ12, CWL14, CWL16, Cor14a, CDLW19, CHH19, DWB12, DCA18, FCM14, FRS16, Fyo19, Gen13, GLG12, GKG19, GZH17, GWY19, HWZP18, HITZ12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kaw15, KG16, LA15, LGLK17, LQD16, Lop12, Mur16, NBZP17, NNAM10, PCK20, PBC17, QLL17, SAKM16, SZHY19, Sia12, SOR16, TM18, Uto13, Vai12, WBC10, XWSW16, YDY16, ZDL12, ZXYL16, ZVG16, ZLW17].
AHM18, AZH11, BBPD16, BTPLST15, BGP17, BKV13, BT15, BL11, CH11, Ctri6, CDL18, DLK16, DRD11, DJ19, ED17, FTV10, Gen10, GZS18, HKA19, HH16, KHI, LXX14, LZY16, LH1L18, LW13a, MRR18, OSSK16, PWS19a, PB19, PRZB12, SEXY18, SWW17, Suc12, TKM13, WR15, WS19, WL19, XMY17, XYW18, Yaa19, YXD18, YQOL17, ZLY10, ZC17, ZFH18, ZHT16].
Encrypting [CC10, Mar10c, dRsdlV12, Cia18, LFGCGR14, Pow14].
Encryption [ADM12, AV12, AUA1C, AEW17, ALO12, AAC16, Anol13c, Anol14, Anol15c, Anol17d, ARM19, AKP12, AFB12, AS16, BVS13, BWLA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12a, BS14, BV18, Bla16, BKLS12, BDPS12, BJIP14, BDML16, Boy13, BV11, BV14, BGV14, CVM14, CM1O16, CL16, CWWL12, CN12, CZF12, CLHC12, Che15, Che18, CGL12, Chi12, Chu16, CRE12, Con18, CNT12, CLW16, CD16, DR10, DN12, DFJ10, DSB18, Des10b, DGFI18, DOS15, Dun12a, DF11, EAA12, ESS12, FH16b, FHR14, FJHJ12, Fei19, FFL12, Fuc11, GWWC15, GGH16a, GGH17, GM13, GZ13, GSW16, GH11a, GH11b, GHS12, GHPS12, GDC16, GVW12, GVW15, GM14, GL12, GKS17, Gue16, HSMY12, HLLG18, HZ11, HG12, Hor19, HC17, HTC15, HLL19, HP12, Int19, IAD10, JLS12, JHL12, Jia14a, JR14, Kam13, KB10].
Encyclopedia [KME12, KMY18, KTT12, KOS16, KKA15, KFOS12, KHP16, KKK18, KMJ18, KS12, KHRG19, LMG17, LMG18, Lmm17, Led16, LLSW16, LLPY19, LW11b, LW11c, LW12, LBLC12, LY13, LHL14, LCC15, LTZ16, LLL17a, LFX18, LLLH18, LSW15, LH11c, LSQ18, LB13, LY15, LW16, LYY18, LLML12, LH18, MZH15, MLO17, MMP14, MR14a, MTY11, MSM18a, MVVR12, MS17b, MSR17, MRL18, MB18, MPRS12, MZLS18, MT12, MKRM10, MSas12, Nac16, NdMM16, NT12, NMS14, NAL17, OT12, OGK15, PM13, PR12, PB12, PDN15, PRGB15a, Per13, PKTK12, PPS12a, SYS18, PMZ12, PCL17, PRSV17, PWS19b, RVH16, RCP18, RZZ15,
RM18, RSBGN12, RDZ+16, RVRSCM12, SG18, Saa12a, SSW12, SERF12, Sar10b, Sch15a, SLGZ12, SXH+19, SZS14, She14, SWF+19, Smi11b, Sta12, SGH15, SMOP15, Tan11, TCN+17, TCL15, TMC15, Tan17b, TDTD13, TKR14, TT12]. Encryption [TFS19, Unr15, Val11, VSR12, VOG15, Wal18, WHC+15, WP17, WDCL18, WSS12, Wat12, WLC12, WDDW12, W15, WWHL12, WMS+12, WQZ+16, WZC19, XNg15, XY18, XXZ12, XJWX13, XWLJ16, XJW+16, XHX+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YQ15, YKC+11, YFK+12, YCZY12, YKLL12, ZOC10, ZPM+15, ZZQ+19, ZDL12, ZYT13, ZW1515, ZQ15, ZMW16, ZSM17, ZZY+19, ZHW15, ZY17a, ZYM18, ZWS+18, ZYH+19, ZHZ+19, AHS14, AASAA18, ATKH+17, AKKY17, Ana14, Ana13b, Ana15e, Ana16f, AB12, AM10, ACD+15, AHI+12, BBL+19, BAAS13, BC18, BKR19, B14, BSW12, BGP+17, BTK15, Bro19, CPPT18, CVFP16, CFZ+10, CW14b, CLH+16, CMM1715, CLC+19, CZ155, CS11, Chn10, CW12a, CDF+10, CM13, CGKO11, DLZ16a, DMD17, DTZZ12, DMD18, Eve12, Eve16, FAA+18, FH13, FSWG11, FSWG12, Fy16, GMOC1C15, GH13, GHPS13, GLM+16, GH12, GLL+18]; encryption [GZX19, HGW11, HQZH14, HZL18, HKA19, HWD16, HZW18, HL19, HT13, HLR11, H11, HFT16, HTC17, HY18, HYF18, HHA919, HHK13, JZU+19, JCHS16, Jia14b, JSMG18, JHCC14, JSM+18, Kam16, KHM13, KKM+14, LL16, LCL+17a, LGP19, LCL+15, LFO+17, LCT+14, LFWS15, LLM+19, LPdS10, LL111, LW10, LK10, LW13b, LZC14, LPZ15, LCY+16, LZZ17, LJW+17, LJYW18, LLL+18, LZKX19, LDZ19, LL16a, LW13c, LSG12, LLG19, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSas13, NES+14, Nam19, OPHC16, ONSZ19, PPA18, Pet12, PB19, QVR+18, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, SLL+19, Sar11, SYL13, SE14, SE16, SH11, SM11, SMN14, SLZ12, SY15b, Sha13, SVGE14, SGFCRM+18, SLM10, SKB+17, Spa16, SGP+17, SGM16, Tam15, TPL16, jT12b, WGJT10, WY10, WY11, WYY11, WLC11, WHY+12, WDD13, WFX17, Wan18, WDZ19, WZG+12, WLS14, WCCH18, WWZ16, WWXC14, XS1C10]; encryption [XXX15, XWS17, XZP+19, XZ14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZY17+1C, ZGL+18a, ZCL+19, ZZZ12, ZL12, ZDW+16, ZY17b, ZCZ+19, Zhu13, Wan14, LAL+15, Sar18a, Kat13]. Encryption-based [SERF12, BC18, XWW+18]. Encryption/Decryption [KB10]. Encryptions [zGX12, LG12, SL1+16, RD17]. Encyclopedia [vTJ11]. End [Ano15c, BRR+15, BGP+17, CFE16, Ch16, RST15a, RST15b, Bel18b, Chi13a, JZU+19]. End-to-End [CFE16, RST15a, RST15b, Ano15c, BRR+15, BGP+17, JZU+19]. endomorphism [FWS13]. Endomorphisms [AK14, LGH+17]. enemies [Fag17]. Enemy [BC14, CAC14]. Energetic [PDMR12]. Energy [Ano15d, AZF+12, ABC+17, B1a16, CKHP19, GPR+19, JEA+15, LSC+15, MP12, PAF18, RPHJ11, TCF16, TCN+17, VN17, CZ14, ZTT16]. Energy-Efficient [MP12, TCF16]. Energy-Harvesting [ABC+17]. Energy-time [Ano15d]. Enforced [Set16]. Enforcement [LLZ+17, Tan15a, Cra11, CFG+17]. engagement [LSBN14]. engaging [ISC+16]. engine [BS13a]. Engineering [BCHL19, Bel18a, FSK10, GHD19, LLK18, MS18a, MP12, PGL10, SN1+17,
TQL+14. Engines [LB13, BGG+13].

enhance [CZ14, SLM10]. Enhanced [DTE17, KY10, KKM+13, MS17, SGG18, SS15, TV15, YI17, YGC16, AMN18, ACK+10, DLK+16, GM16, LNKL13, YQOL17].

Enhancement [FSX12b, LA15, NNA10, CHS11, SVY19].

Enhancements [Che18, FSX12c], Enhancing [CSW12, IA15, Lan13, YS15].

Enigma

[KM15, KM16, LHA+16, Ore14, Ano16c, Bur11, Kap11, Kap13, McG11, McK12].

Enigmas [Bat10]. Enough [JCM12, Ano14].

Enrollment [YVZ+12, DEL19]. ensuing [SS17a]. Ensure [PWS+19b].

Entanglement [Ano15d, JEA].

Entanglement-Based [JEA+15].

Enterprise

[TGC16, XZL+19, Din10, KLN15, NB13].

Enterprise-Level [XZL+19].

Entropies

[BCM12, BCM13].

Entropy [DSSDW14, DK16b, KPW13, VS16, YGFL15, BNY14].

Entropy-Based [YGF15].

enumerators [OŠ11]. Environment

[AARJ12, BCGN16, FYD+19, KKA15, MLO17, MRS+17, RQD+15, SGG18, SAM+19, TV15, VFFHF19, YMA17, FHZW18, GAI+18, HL19, HLY14, KKM+14, Kim16, KS19, NR17, Par12b, RR16, SYWX19, SKB+17, WL12, WCFW18, WT10a, XXX15, YWK+10a].

Environments

[HXHP17, HLLK15, LQY10, PAS13b, TMGP13, VFS+19, XLP+18, CLHJ13, CTL13, KPP16, KAS15, LNK+18b, LW13a, LCY+16, NAACL12, SCY15, SA19, Tan12b, VDO14, VGL14, WZZW20].

Eof [Gup15]. ePassport [ABHC+16].

Ephemeralizer [Tan15a].

Episodic

[WAK+19].

Epistemic [Sch12c].

EPR [UUN11].

Equality

[CHH+19, HTC+15, LLSW16, MZHY15, WZCH19, HTC17, ZCZQ19, ZCL+19].

Equational [ABR12].

Equations

[BB10, SR12a].

Equi [PD14].

Equi-Join [PD14].

Equifax [Ber17].

Equijoin [WP17].

Equivalence [ABR12, CCK12, CCK16, GLW12, SS13, WGD18, HKT11].

Era

[Mos18, OMNER19, QCX18, ABJ13].

Ergodic [IAD10].

Erratum [YFK+12].

Error

[KW14, LSC+15, MCP15, MKASJ18, TLCF16, ATI+10, Chi13a, LTT10].

Error-correcting [MCP15, LTT10].

Errors

[TM18, CSS+13].

ErsatzPasswords

[GAS+16].

Escapers [SXH+19].

Escrow

[MR10, WLY17, ZLH+12, HKH13].

Escrow-Free [ZLI+12].

Escrowable

[NCL13].

eSkyline [BKV13].

Espionage

[LJS+14].

Essay [Bai12].

Essays [Nac12].

ESTA

[SS15].

Establishing

[DKL+16, GSFT16].

Establishment

[AS12, Ano11b, BCO13, DL12, NYR+14, BEB+18, GTSS19, SZMK13, ZPZ+16, ZWX+18].

Estimation

[BCF16, GSN+16].

Estonian

[Ano17c].

Ethernet

[ABHC+16].

Everyday

[CLY14, CST+17, DG15, FSWS17, GZ12, HC12, LY16, MSU13, TYM+17, WSA15].
Extract [BWLA16, GST13, GPT14, PCPK14, GPP+16]. Extractor [USH19].
extractors [Zim10], extraordinary [Hol12], extreme [GJ13]. Extruded [CJFH14], Eye [ERLM16, SRRM18, SM13, Tox14].

F5 [LLY+12b]. Fa [FMS12a]. Fabric [BH19], fabricating [WW13].
Fabrication [VDB+16].
Fabrication-Induced [VDB+16]. Face [AQD12, MHW+19, RSX18, XHH12]. Facial [KRB12, TCMLN19, WSS+19]. facilitate [Chi13a]. Facsimile [Ano16d]. Factor [AMSPL19, HXC+11, LLC11, PSSK19, AIB+16, BD18, CLP+13b, DRN16, DMWS12, ED19, GMMJ11, HC12, IC17, JKL+16, JMW+16, Ken11, LNK+18a, LNK+18b, Lit14, MDHM18, NMX15, SNG+17, WW14, WZZW20, Wat14a].

Factoring [APPVP15, LLM12, BGG+19, MM13].
Factorization [Cou12, FS15, KKK+18, KFL+10, Kuz11, YAM+15, Mes15, TPL16], factors [HK17]. Failing [Cer14]. Fails [WCL+18]. failures [WZZW20]. Fair-Exchange [DG15].

FACIL [ALR13, Ash14, GHKL11, WSS+16, MV16b].

Fake [KU14]. Fallen [HCPLSB12]. False [LLZ+12, CDGC12]. Families [BSS+13, KU12].
Family [AH+18b, BMS12, BKST18, CBXJ19, DGS12, DJG+15, FLS+10, FFL12, GNL12, LYY+18, MFG16, YCL17]. Fanin [SS12a].

Fast [BLAN+16, Bru12, CHS15, DSLB18, GSN+16, JGP+18, LGLK17, NR12, PRSV17, Ra19, SRRM18, WHZ12, WBA17, WQZ+13, ZHW+16, FHH10a, KHMB13, LNNH13, MBB11, YMY18]. FastAD [SMB10]. Faster [CN12, HVL17, TH16, ZSP+19, Ant14].

Fault
[AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JP12, JT12a, LK19, LCL+12, LCLW17, LGLL12, MKRM10, MKAA17, PH12a, RZZ+15, SEY14, YGD+17, BBPB13, PBC14, WM16].

Fault-Based [BBB+16a], fault-resistant [PBC14], fault-tolerant [WM16].

FBAC [YWJ+19], FBA [Bha16], FC [DDS12, Dan12], FCMDT [BSBG19].

FDM [BD18], FEAD [ZWM14].

Finding [Hof16, Ste15a]. Fine [CDD13, PV17, YTH17, ZML17, CLH+16, FSGW11, LHH+18, XYML19].

Fine-Grained [CDD13, PV17, YTH17, ZML17, CLH+16, LHH+18, XYML19].

Finely [GT19], Finely-Pipelined [GT19].

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

Finger [KLY+12, NSBM17], finger-drawn [NSBM17]. Fingerprint [DS19, MR14b, HW19, KKG14, ZHL+11, ZHH+17].

Fingerprint-Based [DS19].

Fingerprinting [QF19, SNCK18, TSH17, ZS12, FLZ+12, RS17]. Finite [BGJT14, CHS15, GMNS15, HVL17, ZL19, AA14, BGJT13, CZ15a, GPL13, LBOX12, ÖS11].

Finite-State-Machine [CHS15]. firms [Ano15a]. First [Ano17d, BH15, DR10, LFX+18, MS17, PC16, WS18, AB10a, BCV12, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14].

First-Generation [BH15]. First-Order [LFX+18].

Fischlin [ABGR13], Fishbone [KS19], fistful [MPJ+16], fit [KGO10]. Fix [DLV16, HLV10]. Fixed [Chm10, Lim11].

Flag [MBC+18], Flame [BPBF12, Goo12]. Flat [LHW18].

Floo [Moo12, SH15, Ste15a, ACC+13].

Flaw-Finding [Ste15a]. Flaws [DR11, FVJ19, HLV10].

Flexible [GT19, LGYW12, PAF18, TV19, BGG+13, WDD19, WLS14, ZL12, ZFH+18]. Flexlist [EBK+16]. Flexlist-Based [EBK+16]. flip [Wag16].

Flow [ATS15, DJ19, HBC+19, WXL+17, CFG+17, KL13, IWY12, PRP+12, SRB+12].

Flowers [Hai17]. Flows [CDD13, HKB14, WYL13].

fly [PS14], Fog [FMC19, JWS19, Gop19, JSMG18, KH18, QRW+18, Wan18, WDKV19, ZSW+18b, YXA+18].

Fog-based [FMC19]. Follows [Arm19]. FontCode [XZZ18], Foolproof [FFL12]. Force [JR14, CJP12, CJP15].

Financial
[AS16, BV18, BSW12, Boy13, GGH+16a, GVV12, LQD+16, MVV12, Ruz15, Wat12, ZYT13, ZWTM15, ZWM14].

**Functionalities** [JR13]. **Functions** [ACZ16, ALR13, BCC+14, BIKK14, BKPW12, BK12a, CCL+19, CPS16, DSM14, DQFL12, FY11, LVV11, NR12, Rja12, RW12, SMS14, SLY+16, Tan12a, YTP11, AY14a, BDP11, CG12b, CQX18, CW12a, ESR14, Gen10, HRV10, HL12, Li10, QZDJ16, WT13]. Fundamentals [Joh10]. Further [HCL+14, WHY+12]. *Fus* [FMS12a]. Fusion [ABCL17, HW19].

**Future** [AYS15, BCE+12, BKK14, Bon12, BLU+15, CDFZ16, Fri13, GCK12, HYS18, KHN+11, Mon13, SG19, Ano13d, FPBG14, Mac12, PPA18, PHWM10, MJS13].

**Future-proof** [Mon13]. *Fuzzy* [HWZP18, KRDH13, NC12, SH11, USH19, XJWW13, Alp18, BSBG19, HK17, KHB13, MM13, SM11, SNM14]. *FV* [MRL+18].


gambling [Ana14]. Game [ADH19, MZA+13, LPZJ15, SD10, SKEG14]. Game-Theoretic [ADH19, SD10, SKEG14].

Gap [LRWW14, TMGP13, PPA18]. Gaps [SPM+13, DKL+16]. Garble [AIK14].


Gateway-oriented [WZM12a, WZM12b].

Gateways [RVS+18]. Gauss [BPBF12].

Gaussian [HKR+18, RMM19, YWL+17].


Gear [AHS13]. Geckos [GSC17].

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

Gener [HYS18]. General [Bar16, CJXX19, FJHJ12, GFBF12, Gue16, HP12, KOTY17, LPL15, LNG19, PB12, SJWH+17, YFF12, ABDP15, Bai12, DGJN14, HQZH14, LWS10, WS12, YC11, ZYC+17]. General-Purpose [Gue16, ABDP15, DGJN14].

generalisation [LR15]. Generalised [Hes12].

Generalization [GMNS15]. Generalized [BFMT16, GL19, LPL15, PC14, TY16b, Ye14, ZAC17, ADG16, BNST17, KL11, NC13, YMSH10]. Generated [ADD10, LCLI7b, NN12, XXYYX11, YM18, AGHP14, CBL10, JS11a, LW13b].

Generating [Ano16e]. Generation [ABS+12, BCGH11, BH15, GT19, HEP+11, LTC+15b, MR14a, MJGS12, NIS12, PS14, SOS15, SRK+17, SRK+18, XJR+17, Aia15, ACD+15, CJXX19, GMRT+15, GCH15, KHM13, KKM+13, OMPSP+19, SGFCRM+18, SPK17, WX13, YDH+15, ZHL+11]. Generator [ADD10, BK12a, CDK+10, MVV12, NN10, NKF14, CFY+10, LGK10, MRT10, PLSD10, SH11, SM11, XS10].

Generators [AS17, DLS10, LTP16, MFG16, NIS12, PS12, CR19, HR10, MG15, St11, Zim10]. Generic [BWLA16, BR14, Chi16, GWWC15, HXC+11, Sar10b, SY15a, WCL+18, ZCLL14, HQY+16, XNS10, YT11b].

generically [MHKS14]. Genetic [JK13, MM17, ASY13, EEAZ13, PTK14].

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

Genuine [HR13]. genius [FWS13]. geo [FG19, Har14].

geo-distributed [FG19].

geo-location [Har14].

geodesics [ZZC14].

Geographic [LC17]. Geolocation [FPY15].

Geometric [DSB16, GTT11, WLZ12, YWNW15, CLZ+17, GZH12].

geometrical [TLL13]. Geometrically [WYW+13].

Geometry [WmCl2, CFR11, CZ15a]. German [BDFK12, Blö12, Buc10, Cop10a]. Germany
Gesture [LCL17b, RSX18, SCR19, SHBC19].

gesture-based [SHBC19]. gesture-typing [SCR19].

Get [GPT14, Sch11].

Getting [ESS15]. GF [GT19].

Ghost [CDA14].

GHZ [CCL13]. GHZ-State [CCL13].

giant [Joh15]. girls [Mun17].

Gird [AUM16, GCS AddP11].

Girod [GMNS15].

given [Bar19]. GLARM [LLZ16].

Glass [Fyo19]. glimpse [Mic10a].

Global [CLP13a, CLH13, MRS17, GH16, LH11b, TMK11, ZX11, LNK18].

Globally [CCS14].

Glyph [XZZ18].

GMAC [SKK10].

Goal [BMP12].

Goal-Driven [BMP12].

Goes [BCD12, RY10].

Goldreich [Lin17].

Goldstrike [BH15].

Goliath [Sch15c].

Gong [LLW16].

Good [DQFL12, FY11, Raz19, LSBN14, RY10, SA14, WT13].

goodbye [HU15].

Google [Har14, Loe15, VGN14].

Goppa [MBR15].

Gordon [GW14].

gossip [FG19]. gossip-based [FG19].

gossip-based [FG19].

goal [BMP12].

Goal-Driven [BMP12].

Get [GPT14, Sch11].

Getting [ESS15].

GF [GT19].

Ghost [CDA14].

GHZ [CCL13].

GHZ-State [CCL13].

Giant [Joh15].

Girls [Mun17].

Girod [AUM16, GCS AddP11].

Gird [AUM16, GCS AddP11].

Girod [GMNS15].

given [Bar19].

GLARM [LLZ16].

Glass [Fyo19]. glimpse [Mic10a].

Global [CLP13a, CLH13, MRS17, GH16, LH11b, TMK11, ZX11, LNK18].

Globally [CCS14].

Glyph [XZZ18].

GMAC [SKK10].

Goal [BMP12].

Goal-Driven [BMP12].

Goes [BCD12, RY10].

Goldreich [Lin17].

Goldstrike [BH15].

Goliath [Sch15c].

Gong [LLW16].

Good [DQFL12, FY11, Raz19, LSBN14, RY10, SA14, WT13].

goodbye [HU15].

Google [Har14, Loe15, VGN14].

Goppa [MBR15].

Gordon [GW14].

gossip [FG19]. gossip-based [FG19].

goal [BMP12].

Goal-Driven [BMP12].

Get [GPT14, Sch11].
Hamming [HRK18, CCLL11, KSSY12].

Hand [SR12a, Choi10]. hand-held [Choi10].

Handauth [HBCC13]. Handbook [Bee17, AB10b]. Handheld [RPHJ11, CTL12]. Handoff [HZC+12, HZC+14, XHCH14, ZBR11, ZCLL14].

Handover [HBCC13, LBR12, CLM+12, CML+18, FZZ+12, HZWV17, LNNH13, QMW17, YHL16, YHHS16, YLS12]. Hands [GPT14, BSS11]. hands-on [BSS11].

Handshake [KK12, KK13, SM10c, WZ11].

Handwriting [SKV12]. Handwritten [GdM16, ASVE13].

Hankel [Ye10]. Hans [Mur10]. haptic [ASVE13].

Hard [KPC+11, Mar10c, ZWTM15, RPHJ12].

Hard-to-Invert [ZWTM15].

Hardcover [Joh10].

Harder [KTA12, Sch16]. Hardness [AH19, BHKN13, SS13]. Hardware [AW15, AW17, ARH+18a, ADSP18, BRPB13, BDMLN16, BJA17, CMRL13, DZS+18, DOS15, EAP17, GPR+17, GCV17, GCS+13, HGL12, HSA14, HC17, HLY10, KAK18, LGH+17, LKA19, LRW14, MLCH10, MCS+15, MRL+18, MLY+18, NDL+13, NDMMW16, PC16, PG12, RMP10, SN10, Set16, St19, Tay17, WOLP15, YSF+18, ZL19, ZHS+19, ZAG19, AMN18, BDM18, BGG+13, KHF10, MD12a, NS10, Nov10].

Hardware-Assisted [LLKA19, GPR+19].

Hardware-Based [HLN+10].

Hardware-Enabled [YSF+18].

Hardware-Enforced [Set16].

Hardware-Intrinsic [SN10, NS10].

Hardware/Software [MRL+18].

hardwares [SKH15].

Harmonic [YWNW15]. Harnessing [DFKC17].

HAS-160 [WLC12]. Hash [Ano12, AMPH14, BHH+15, BKST18, BK12a, CLP13a, JCPB+12, CCL12a, CCL12b, CCL14, CJP12, DCM18, EAA+16, FLS+10, GI12, HCP1812, Hui13, HRS16, HBG+17, LYX+19, MKF+16, MCF17, MKAA17, MKASJ18, NTO12, NXP13, PTT16, RA12, SGI11, WOS12, ZMM17, ZHZ+19, AY14a, AKY13, AP11, CJP15, ESR14, HL12, KKG14, Par18, PPB16, RSP14, SPL1814, SXL16, WYW14, ZCQ19].

Hash-Based [BHH+15, GI12, HCP1812, Hui13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, NXP13, CJP12, CJP15, PPB16, SPL1814].

Hash-Counter-Hash [MKASJ18].


Headline [YGF15]. Health [AMSPL19, LYZ+13, LHL15, RAO17, ZVG16, AKS19, BC18, CLC+19, Ham19, ICI17, OSP+19, WMX+17, YZL+18, ZDHZ18, JKL+16].

Healthcare [BN14, HCL15, ZLC15, ASO14, Kim16, ZGL+18b].

Heating [Bla16]. Heartbeat [IA15]. Heartbleed [DKA+14, Ven14]. hedging [RY10].

Heights [Gen13]. held [Choi10]. Helios [CFE16]. Hell [Han12].

Hellman [ABD+15, CH16, Hof16, HLC11, HLS14, LZC14, LNL+19, ORM16, RH10].

Helmut [Mur10]. helped [Smi11a]. helper [RWZ13].

HeNB [CLM+12]. Herodotus [Keb15, Mac14]. heroine [Fug17].

Heterogeneous [KS18a, SP15b, YZDZ19, AIKC18, AB191a, SZMK13, SCKH10].

Heuristic [BGJT14]. Heuristics [SKE+18].

HEVC [DG17, GKS17]. HIBE [LW11c, LQX19].

Hickory [NN15].

Hidden [FMS12b, PSS+13, YLL+12, ZYT13, BD11, LCL+17a, Sch15c, Sni15a, XZP+19].

Hiding [DCA18, GGH+16b, GL10, JHHN12, MK12b, OT12, XLM+12, XG14, XZW15, ARA13, DMD17, HZH18, KWH16, LXLY12, LT14b, UUN11, WLIH13, WZL13, ZWM14]. hiera [Lac15]. Hierarchical [ADM12, BSS12, FSX12a, LSL15].
Higher-Order [LWKP14, KPC [KPW13, KA17].

Hijacking [DCAT12].

Hierarchical [BZ18, KAK18, LTKP16, HHS [RMG18].

Hill [KPP16, KHRG19, KAK18, LPO [LWKP12, PRC12, AW17, ASBdS16, Ano17d, ARM15, Bar15, DDL +11, CLB19, DM15, DG17, FHLD19, FYD +19, GL12, GCS +13, HZ11, KMP +11, KPC +16, KAK18, LTKP16, LCK11, LLY +18, LPO +17, MS13b, MS13c, MSR +17, PCPK14, WYCF14, WL11, XNRG15, XLP +18, ABBD13, GZHD12, GCVR17, KL13, MAK +12, RS17, WLH13, WXLY16, WZLW13, WKH11]. High-Assurance [Bar15, KMP +11, WL11]. high-capacity [GZH12].

High-Dimensional [Ano17d, XLP +18]. High-Efficiency [DG17].

High-impact [LWKP12, PRC12, AW17, ASBdS16, Ano17d, ARM15, Bar15, DDL +11, CLB19, DM15, DG17, FHLD19, FYD +19, GL12, GCS +13, HZ11, KMP +11, KPC +16, KAK18, LTKP16, LCK11, LLY +18, LPO +17, MS13b, MS13c, MSR +17, PCPK14, WYCF14, WL11, XNRG15, XLP +18, ABBD13, GZHD12, GCVR17, KL13, MAK +12, RS17, WLH13, WXLY16, WZLW13, WKH11]. High-Assurance [Bar15, KMP +11, WL11]. high-capacity [GZH12].

High-Speed [ARM15, HZ11, LTKP16, MSR +17, BDL +11, KL13].

High-speed [ARM15, HZ11, LTKP16, MSR +17, BDL +11, KL13].

High-throughput [MAK +12]. Higher [LWK12, PRC12, gWpNyY +14, ZSW +12, LWK14]. Higher-Order [LWK12, PRC12, ZSW +12, gWpNyY +14, LWK14].

Highly [SDL14, AC +15, DT13]. HIGHT [CWP12, WWBC14]. HiMap [HEP +11].


Histogram [CSS +13, Lin14a]. Historians [Cer14]. Historical [Hai17, Han12]. History [ABJ13, Ano19b, Cer14, Cop10a, LT14b, McK10, McK11, SE16, Sm15a].


Homomorphic [AAUC18, AKP12, BV11, BV14, BGV14, CMO +16, CN12, CJ13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHP12, KOS16, KGV16, Kim15, KKK +18, KHRG19, Lau17, LCLL15, MLO17, MSM18a, MSR +17, MRL +18, MBF18, Nac16, PKTK12, RPC +18, RMZW19, Tam15b, Vaii1, WHC +15, WXZ +18, AKKY17, BDOZ11, BC18, CJXX19, CW12a, DMD18, GH13, GHP13, GLM +16, LLW16, SEXY18, Tam15, WSC14, XZJ +14, ZYC +17].


Host [THA +13, LKKL13, der10]. hostile [CDA14]. HotCalls [WBA17]. House [Ano16h, Bha16]. HP [CGB +10].


Hummingbird [ESS12]. Hummingbird [ESS12]. hunt [Bha16], hunted [McG11].

HVS [RMG18]. HWMP [BOB13]. Hybrid [ADI11, ARM15, JLL18, JHY +19, KBL11, KKA15, LP12, NAUHQ16, OO12, Per13, RCB19, SGG18, SRT12, XWLJ16, SAM +19, EEAZ13, KP18, WXLY16, WS14, XWS17, BOB13].

Hybrid-Double [ARM15]. hybrid-indexed [WXLY16].

Hybridization [MMSD13]. Hyderabad [GG10]. Hyper [BL14, LZX19, WGZ +12].

Hyper-and-elliptic-curve [BL14].

Hyperledger [BHH19].


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

IBM [ABC+12, ACD+15, BAB+13, HKL+14, JSM+18]. ICA [tWmC12].

ICICTA [IEE11a]. ICISC [LH10a].

ICISSP [Ano19a]. ICs [GSFT16]. ID [Ano17c, CTL13, CDPLCA16, EZ15, HCC10, IB11, KGO10, LMGC17, LY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, TPL16, TT12, TTH15, Wan18, WDZ19, WT10b, WTT12].

ID-based [MM12, LMGC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WDZ19, WTT12].

ID-card [Ano17c].

ID-based [MM12, LMGC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WDZ19, WTT12].

ID-card [Ano17c].

ID-based [MM12, LMGC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WDZ19, WTT12].

ID-card [Ano17c].

ID-based [MM12, LMGC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WDZ19, WTT12].

ID-card [Ano17c].

ID-based [MM12, LMGC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WDZ19, WTT12].

ID-card [Ano17c].

Identity-as-a-Service [VFFHF19].

Identity [XJW+16, YZX+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCYY12, ZLH+12, ZMN16, ZY+19, ZDW+16, ZPXX17, ZYM18, ZYH+19, ZTSR12, vdWEG18, ATKH+17, Ano13d, BMBS10, BOB13, BBG19, BMM12, BBGT12, CTP13, dCCSB+16, DZ14, Din10, DWZ12, FA14b, GMRT+15, GR19, GPVCD+12, HPJ+19, HZC+14, HWDL16, HZWW17, HLR11, HFCR13, HWB10, HWB12, HL11, HPY10, Hwa11, JZS+10, KKGK10, KKM+13, KL11, LKKL13, LK12, LXMW12, LCT+14, MMS+17a, MD15, MGP10, MJS13, MLM16, MM13, NCL13, NML19, ÖSL11, PZL+19, PLCG16, QYWX16, RG10, SSY12, SE14, SE16, SR10, hSZ15, SA16b, Sim15b, SSAF11, SSS11, SGM16, VGL14, WWZY11, WWY11, WSC14, WLFX17, WMX+17, WHZ+19, Wat14b, WWW17, XV12, XCL13, XHM14, YWL+17, YWJ+19, yYqWq13C, YXS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZMYTH17, ZZ12, LZJX10, PN10, Sar18a, Kat13].

Identity [XJW+16, YZX+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCYY12, ZLH+12, ZMN16, ZY+19, ZDW+16, ZPXX17, ZYM18, ZYH+19, ZTSR12, vdWEG18, ATKH+17, Ano13d, BMBS10, BOB13, BBG19, BMM12, BBGT12, CTP13, dCCSB+16, DZ14, Din10, DWZ12, FA14b, GMRT+15, GR19, GPVCD+12, HPJ+19, HZC+14, HWDL16, HZWW17, HLR11, HFCR13, HWB10, HWB12, HL11, HPY10, Hwa11, JZS+10, KKGK10, KKM+13, KL11, LKKL13, LK12, LXMW12, LCT+14, MMS+17a, MD15, MGP10, MJS13, MLM16, MM13, NCL13, NML19, ÖSL11, PZL+19, PLCG16, QYWX16, RG10, SSY12, SE14, SE16, SR10, hSZ15, SA16b, Sim15b, SSAF11, SSS11, SGM16, VGL14, WWZY11, WWY11, WSC14, WLFX17, WMX+17, WHZ+19, Wat14b, WWW17, XV12, XCL13, XHM14, YWL+17, YWJ+19, yYqWq13C, YXS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZMYTH17, ZZ12, LZJX10, PN10, Sar18a, Kat13].

Identity-as-a-Service [VFFHF19].
Sta11b, ZSW+18a. Implementing
[Dav11, GH11b, HTZR12, LTC++15a, SG15,
SVGE14, SL10, VOG15, SA16b].
Implications [DK16a, OSH16]. Implicit
[BB13, DWX12, SSNS15]. Imply
[AL13, LRW17]. Importance
[YL17, MLMSMG12]. Important [TC10].
Impossibility [ACM+17, BCF++14, Mat14].
Impossible
[Blo15, CWP12, LJJ16, TSL11, WYL14,
WW12, MNP12, SD10, SD14]. improbable [TS16a]. Improve
[AQD12, PMG19]. Improved
[Ber18, BCP14a, Chi12, CGKO11, FVK17,
GLLSN12, HJJ+19, IK15, JHL12, KZG10,
LT14a, LWW12, LJJ16, LHH11, LCC13,
LC15, LLLM12, PH12a, QZ14, SK12a,
SEH12, SS10b, SP15a, TS16a, WLC12,
WWBC14, YHHS16, ZJ11, ZLDD12, CBL10,
GL13, HWW12, Nam19, PW1L13, SD10,
XHH12, Wan14]. Improvement
[FRS++16, LFX++18, LJ19, MWZ12, PLPW13,
AN15, BMB16, CHS11, Far14, LNM++11].
Improvements [EA12, HRV10, Tso13].
Improving [AB15, BCM++15, Chi16,
FMS12b, GMS11, HLC11, MHC12, Sar10a,
SS11, YWF18, YKS10]. impulse
[LZKX19]. IMS [G11, MEO12, VGL14].
In-Memory [PAF18]. In-Order [ZBP18].
In-Situ [GRZ18]. Incentive
[SW17, YTH17]. Incentive-Aware
[YTH17]. Incident [CCG++16, CMG++18].
Inclusive [FD11]. Inconsistencies
[YSC++15]. inconsistent [OF12]. Increase
[NNAN10]. Increasing
[AEG17, CLZ++17, HSC19, PKS18, RSX18].
Incremental [KKM++14, MPR12, CS11].
Incrementing [KS15]. IND-CCA [AHS14].
IND-CCA2 [Gal13, MVVR12]. indefinite
[Svo14]. Independent
[FCM14, MTY11, MKRM10, YE12, ZTL15,
BV112, DDD14, SCR19, VV19]. Index
[LHHR10, PSS++13, ZXYL16, Jou13,
LLHS12, LW13a]. Index-Based
[ZXYL16, LLHS12]. indexed [WXLY16].
Indexing [HCM12]. India
[BC11, CGB++10, GJG10]. Indicator [KU12].
Indicators [YT12, Pal16]. Indirect
[ABS++12]. Indistinguishability
[AS16, BCEO19, BV18, FMM15, GGRH14,
GtH++16a]. Indistinguishable [LG12].
Individually [MB12]. INDORCYPRT
[BC11, GJG10]. Induced [VDB++16].
induction [BBBP13]. industrial
[GHD19, OSP++19]. Industry
[Amo11b, QZL++16a, SXH++19, Cha13c,
LHH++18, Men13b, ZS18]. Infective
[GST12]. Inference
[Bro11, DBPS12, NC12]. Inferencing
[BPS17, PTRV18]. Influence [RSCX18].
Information
[AQD12, ABCL17, Bai10, BF11, CVM14,
CDGC12, CBK19, CGB++10, CST++17,
CBL13, Dew11, DP12, FHK17, FHS13,
FP19, HBC++19, HHH++13, IF16, JHNN12,
LG12, LW11a, Loo12, MA17, MAL10,
NKG17, R19, SGC14, ST11, TWZ11,
Uto13, WSS12, XZZ18, XHZ++19, Yan10,
Yek10, ZZ15, ZHL15, ZBP18, AB10a,
Abel10, AL15, ASVE13, BSS11, BGP++17,
CFG++17, DMW12, GLM++19, HPJ++19,
KL13, LWK++18, MKH++12, M10b, SRB++12,
WHZ++19, WW13, Amo19, BYL10, LHI10a].
Information-Centric [FP19].
Information-Theoretic
[CVM14, WSS12, CDGC12, GLM++19].
Information-theoretical [ZZ15, KL13].
InfraStructs [WW13]. Infrastructure
[GM13, HEP++11, PN10, VFFH19, GAI++18,
JAE10, SA12]. Infrastructures
[MJW++18, FHM++10]. ingenious [Mac12].
Inhibiting [GAS++16]. Initial [PAS13b].
initialization [PCK19]. initiation [AN15].
Injected [LLZ++12]. Injecting
[BBGT12, LZKX19]. Injection
[ABS++12, ARP12, DDR++16, JWJ++17,
PYM++13, YGD++17]. Injections [LH17].
Ink [Keb15, Mac14]. Inner [ADM12,
LMG+18, OT12, YKNS12, DDM17.
Inner-Product [YKNS12]. innovations
[JS18]. Input
[GGHW17, XXZ12, PBC14]. Inputs
[GGHW17]. INSCRYP'T [BYL10].
Insecure [BCGN16, BWS19, Mur16, Lani17].
Insecurity [Bel19, HZX15, LSQ15, LRW17,
SWYP12, WY10, Wan14]. insertion
[XWDN12]. inside-out [AP11]. Insider
[AJA16, ERLM16, LJS+14]. Insights
[AH19]. Inspection
[FGR+17, VCK+12, AZH11]. Inspired
[RMG18, BW13, GPVCdR012, OK18].
Inspires [SPG+19]. Instability [LMB12].
Installment [SYC+17]. instance [BRT12].
Instances [HN10]. instead [AGH+17].
Institute [Wes16]. Instruction
[ARP12, AB15, EKP+13, HZS+19, YM18,
BVIB12, SF12]. Instruction-Cache [AB15].
Instruction-Level [HHE+19]. Instructions
[FHLH19]. Insulated [FHTZ13, HLH1c, HLH1,
RG10, RWZ13, WWYZ11]. Integer
[Cou12, LLY+18, AMK12, MM13, Mes15,
MN14, PC14]. Integrals [CN12, CNT12].
Integral [AY14b, LWZ12, ZSW+12, SM11,
SNM14, SH11]. Integrated
[LY15, MU12, AL15, SY12]. Integrating
[CFZ+10, LH12, OdH12, AEH17, HLS14,
MCL+19]. Integration
[AQD12, Kar12, ZWY+13]. Integrity
[BCP14a, BCK17, DGFH18, FMY15,
MV16a, PZL+19, PH12b, SB18, TSB18,
VBC+15, ED17, SWW+16, YAX+16,
YNX+16]. Intel [Arm19, MZLS18, SF12].
intellectual [Bar19]. Intelligence [Dew11,
SG19, Ald11, Bud16, GW14, Han12, Maf16].
Intelligent
[AMK12, IEE11a, SAJL16, VFS+19, Wat14a,
HLYS14, MKH+12, SMS+16, ZCZ+19].
intensify [HL12]. Inter
[LBR12, OMPSP+19, BGAD12, SCKH10,
SA15, SHBC19, YWK+10a]. Inter-domain
[LBR12, BGAD12, SCKH10, YWK+10a].
Inter-Pulse [OMPSPL+19]. inter-router
[SA15]. inter-session [SHBC19].
Interaction [HSUS11, BBDP16, HK17].
Interactive [CJFH14, DF11, FSGW11,
BCL+13, LH11a, Pas13a, PPR+12, Yan14].
interceptor [Cho10]. Intercepts [Don14].
Intercloud [DCA19]. Interest [Sch19].
Interface [WBA17]. interference
[BBCL19]. intermittent [CL16].
International [ACM10, ACM11, BC11,
CGB+10, Che11, Dan12, FBM12, GLIC10,
JY14, LCK11, LW11a, LTW11, MV12, PJ12,
Sen10, Wat10, Yan10, Yan11, AB10a, Abe10,
Ano11a, BYL10, BL10, GL10, GG10,
HWG10, LHC10, IEE11a]. Internet
[Ano13d, LFGCGRP14, TW14, AAC+16,
Ano13b, AKS19, BCLH19, Bel18b, BLU+15,
CLF+17, CW12b, CEL+19, DRS16, DG15,
Fri13, Gil13, GMDR19, Ham19, HZL18,
HEP+11, JKAU19, JTM+16, KHRG19,
LNK+18b, LGH+17, LSG16, MJS12,
MJS13, MCF17, NLLJ12, NLY15, Orm16,
PLGMD18, SB17, SXH+19, SS19, Söd13,
SY+19, SYW17, SYC+17, SKEG14,
VWC19, WCC18, XLC+19, YCT15,
ZDHZ18, ZSY19]. Internet-Draft [MCF17].
Internetworking [SAAB10].
interoperability [HWK+15]. interplay
[AW14]. Interpolation [JTZ+16, KU14].
Interpretation [MZ17b].
Interpretation-Based [MZ17b].
Interpreter [MS18]. intersection
[LZ+16]. Interval
[PPR+12, Cra11, DTZ12, LWY12, MO14].
Interval-based [PPR+12, Cra11].
Intervals [OMPSPL+19]. Intra [HF14b].
Intra-Masking [HF14b]. Intrinsic
[HRK18, SN10, NS10, RCW15].
Intrinsically [SRK+17, SRK+18].
Introducing [Fay16]. Introduction
[BCHL19, BdD19, DK15, Gas13, G’13,
Gre19b, JSK+17, LLK18, Low12, Mei10,
Men13a, Sch15a, SOG15, Sta11b, CM13,
Buc10, Led16, Sch15a, Fu10, Mur10].
Intrusion
[NSMS14, SAJL16, SBV14, YKC+12].

Intrusion-resilient [YKC+12]. Intrusive [AARJ12, MFH13]. Invariance [yWpNyL11]. Invariant [CSW12, NKWF14, RS16, WYW+13, YWNN15, GZH12, LXCM11]. Invariants [NKWF14, CSLS14, KK10, MZ17a, TLL13].

Invention [Orm16]. Invent [Ant14].


Invisible [Keh15, Mac14, SYL13].

InvisiMem [AN17]. INVISIOS [AARJ12]. Invited [SS19].

Involving [HLCL11]. IoT [AATM18, AMSPL19, APMC13, CCM17, CSH+18, FQZF18, FMC19, GALT+18, HHBS18, Hodd19, LSQ15, LZZ+19a, MPP19, NV17+17, PCK19, RC18, SSSA18, SGC16, SJL18, TODQ18, TG17, WCFW18, WXX+17, XYY19, YWJ+19, YFT17, YFT18, YTH17, ZCSS15, ZLY+19].

IoT-Based [YTH17, YLY+19].

IoT-Enabled [SGC16]. IoT-FCAC [YWJ+19].

IoTs [SAJL16, ZSW+18a]. IP [AGLW16, AZH11, PJ18, PA10, RS17, SP15a, TZZF12, WBC+10]. IP-SEC [PA10].

IPE [ZM16]. iPhone [Wu16].

IPs [EAAA19, GSF16, NGD+17]. IPv6 [KP12].

IRC [HB13]. IRC-based [HB13].

IRIW [JKHeY12]. Irregular [YW1+17].

ISBN [Ano15b, Ano17b, Bai21, Joh10, Murl10, Sch15a].


ISO [BCM12, BCM13, TS16a, WWBC14].

ISO/IEC [BCM12, BCM13].

Isogonies [Y+17]. Isogony [BF19, KD18, KAK18, Lau17, LNL+19, ZSP+19]. Isogony-Based [BF19, KAK18, ZSP+19, KD18]. Isolated [GKG19, YS15, KKJ+16]. Isolating [LG12].

Isolation [GGK18]. Isopleth [HGOZ19].

ISSAC [Wat10].

ISSAC [Wat10]. Issue

[Ano13d, Ano16a, Ano16b, Ano16h, Ano19a, BCHL19, CSYY18, GO17, LW13a, LLK18, XW13, YYW19, PHWM10, Sim15b]. Issues [ABHC+16, PZPS15, VKK+19, JAE10, KJN+16, MV15, SVGE14].

ISTE [Ano15b].

Italian [Sac14]. Italy [Cra12].

items [YD17]. Iterate [HHK11].

Iterated [LPS12]. Iteration [CCZ13]. Iterative [QJ+18, SXL16].

ITU (b) [FXP+17].

iVector {RSR+19}. iVector-Based [RSR+19].

J [Bar12, Led16, Sch15a, WZM12a].

J2ME [GPT12]. J2ME-Enabled [GPT12].

Jacobian [BAAS13].

Jacobians [Hes12].

Jacques [Nac12].

Jamming [YSJL14].

Janet [Ayu12].

Japan [Sah13, Maf16].

Japanese [Don14].

Java [GPT12, XHH12].

Jaypee [CBG+10].

Jean [Dew11, Nac12, SR14].

Jean-Baptiste [Dew11].

Jean-Francois [SR14].

Jean-Jacques [Nac12].

Jeffrey [Mei10].

Jill [Mei10].

Joe [Car11].

Johan [Ten18].

John [Wei16].

Johnny [HM12, RA15].

Join [PD14].

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

Jonathan [Fu10, Mou15].

Jones [Ber16a].

Jose [ACM11].

Joseph [Mei10].

Joshua [Ano17b].

Journey [CFST17].

Joux [AY12].

JPEG [AOT13, DLGT19, LSQ11b, LC15, MAL10, QZ14, SK12a, WHZ12, WLT13, ZC12].

JPEG-2000 [ZC12].

Julia [KD18].

Julia/Nemo [KD18].

July [Wat10].

Junction [VDB+16].

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

Juniper [CCC+16, CMG+18].

Juraj [Gas13].

Just [Pfl10].

JXTA [AMH10].

K2 [PS12].

Kalyna [OGK+15].

Karatsuba [BCL14, MIR+17, MRL+18].

Karhunen [BCPV11].

KASE [CLW16].

Katz [Fu10, Mou15].

KDM [CBJX19, MTK11].

Keccak [BDP+12].

keep [Rus15].

Keeping
KEM [CZLC14]. Kepler [LGP19]. kept [Cha13c]. Kerberos [SCKH10, TW14]. Kernel [HHAW19]. Key [ASN12, ADSH18, Ano11b, ABB19a, BN14, BVS+13, BL12, BSBB19, BBB+16a, BA15, Bar16, BM18, BCO13, BKLS12, BF11, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CLND19, CJ13, Ch16, CCT’14, CNT12, Cou12, CMA14, DWWZ12, DL12, EAA+16, FZT13, FSV17, FM12, GFBF12, GT12, GZZ+13, GSW+16, GST13, GPT14, Gir15, GKS17, GZ12, GLB+18, GYW+19, HSMY12, HLLG18, HEP+11, HC12, HL10a, HCL+14, HTE+15, HEC+12, HLLH19, Jia14a, JEA+15, KP12, KMZS19, KTT12, KFSO12, Kim15, LXY+19, LSLW16, LCLL15, LQY10, LY16, LH11c, LSQ18, LCCJ13, LYY+18, LBR12, LLH18, MZHY15, MVV12, MPP14, MTT11, MM12, MV19, MKK17, MPRS12, MNS11, MSU13, NNA10, NYR+14, NTY12, Orm16, PSM17, PDHN15, PUCK14, Pud12, PNRC17, RVH+16, RSBGN12, RW12, Saa12a, SK11, SNJ11, SEHK12, Sias18, SK12b, Soe18, SWM+10, Sia12]. Key [SGH15, SLY+16, TMC15, TYY+17, TM12, WP17, WSS12, WLC12, WZ15, WCL+18, WWHL12, WT10b, XNKG15, XX12, Xio12, XLM+12, XJWW13, XGLM14, XZLW15, XJR+17, YM16, YXZ+12, YS12, YLSZ19, YLW13, YRT+16, YL17, You12, YKC+11, YFK+12, ZSP+19, ZHX16, ZY17a, AA14, ATKH+17, APK+18, ABB+14, AKG13, AIB+16, ABW10, AN15, BS15, BGD12, BB14, BJ16, BSW12, BGG+13, BEB+18, BBB16b, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLCZ10, DLK+16, DGS12, Dur15, FHH10a, FA14b, FI015, FHZW18, GMR+15, GPP+16, GH16, GBN11, GLM+11, GSAV18, GTSS19, HPC12, HZWW17, Hod19, HWB10, HWB12, HL11, HLYS14, HTC17, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSMG18, KDH15, KMTG12, KKG14, KIH19, KP18, KLV+16, KDW+17, LLIS13, LLP+18, LWS10, LIK+17, LPDs10, LW13b, LZO14, LML+13, LLG19, MPN12, MRT10, NAACL12, NCL13, Nos11]. key [Nos14, RR16, RG10, RWZ13, RFSL10, SES+16, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZ15, SA15, SGP+17, SV10, TK19, TCS14, TLL12, Tso13, TKKH14, VV19, VN17, WWYZ11, WDVB18, WDVK19, WZM12a, WZM12b, WT10a, WTT12, WQZ+13, WXX+17, WX12, UX3, XCL13, XXY+19, XLYM19, XLC+19, XMHD13, XM14, YT11b, YC12, Yan14, YZZ+14, YHHS16, YZL+18, YN19, YLZ+16, ZCZQ19, ZPZ+16, ZWQ+11, ZZ11, ZHL+11, ZCC15, ZT16, ZGL+13a, ZXX+18, ZWX18, ZC19+19, ZICO15, ZC17, ZY17b, ZWS+18, ZCZ+19, ZHT16, CLW16, OHJ10, XJR+17]. Key-Aggregate [CCT+14, PSM17, GLB+18, CLW16]. Key-Agreement [WSS12, APK+18]. Key-Based [Xio12]. Key-correlations [Sar14]. Key-delegation [JSMG18]. Key-disclosure [ZCZ17]. Key-Establishment [BCO13]. Key-Extraction [GPT14]. Key-hash [KKG14]. Key-Insulated [FZT13, LH11c, HL11, RG10, RWZ13, WWYZ11]. Key-Length [GT12]. Key-Length-Based [PNRC17]. Key-Policy [GZZ+13, GSW+16, HSMY12, RVH+16]. Keyed [KE19, MMS17b, YHHM18]. Keyed-Function [MMS17b]. Keying [TW14, BCW11]. Keyless [PDMR12, ZWX+18]. Keyrings [MBB11]. Keys [ASN11, BF12, Bro17, CC10, HDWH12, LSQ19, MS16, PSM17, TW14, ZMWE16, CMG+18, HL14, IK15, LLY15, LH13, LW10, LLL+18, RWZ13]. keystream [SM11]. Keystroke [AaBT16, SP13, BGE+18, CT12, GEAH11, LCT+15a, MCRB19]. Keyword [CWL+14, Che15, HWZP18, HCDM12, HL19, LSQ18, WC18, WDSW16, XJWW13, ZXYL16, BL11, CLH+16].
FSGW12, GZS+18, LXX+14, OSSK16, SY15b, WHY+12, WXLY16, XXY+18, XZX+19, XLC+19, YZCT17. Keywords [CWWL12, ZZ11], KGC [YT11a], kid [Tan17a], Kind [WJ19], King [ABJ13], kiss [HU15, KYEY+18, Ros11], KLEIN [GNY12], Klepto [XY18], Knapsacks [Dun12a], Know [CEL+19], Knebl [Mur10], Knights [CEL+19], knocking [KSB+19]. Know [BC14, CAC14, XTK10]. Knowledge [CLP13a, COP+14, GJO+13, GOS12, IW14, MX13, MBC+18, MT12, ORR+14, Pan14, TSH14, Ano11a, KPP16, LLM+19, MDHM18]. Known [DWWZ12, JLLH12, SEHK12]. Known-Key [DWWZ12, SEHK12]. Knuth [Ten18]. Kobitz [BJ10b]. Kode [NN15]. Korea [LH10a, LW11a]. KP [FJHJ12, HQZH14]. KP-ABE [FJHJ12, HQZH14]. Kristie [Keb15]. Kryptographie [Blö12]. Kryptographie [Buc10]. Kuala [HWG10]. Kurtosis [YYO15].


Left-to-right [BBG+17]. Legacy [CS12, Smi11b, CGH17]. Legal [ZTSR12].
Length [AS17, GT12, Gir15, PDNH15, PNRC17, Zha12]. Length-Doubling [Zha12].
LFSRs [HS18, JWJ12, BKJP12, CCW17, AW17, Ano15a, BBCL19, BRPB13, Li18, QGGL13, DK16b, Bro17, Win17].
LiBrA [Sch12b]. Libgcrypt [GMVV17]. Library [ACZ16, Bec17, BLS12, FLW12, KRH18].
Licensing [EAAA19]. Life [MK13, SCMS18, McK10, McK11, War11].
Lifecycle [Tan15a]. Lifetime [HSUS11].
Lifting [LSL12b]. Light [JEa15, SWF19, PCK19, ARH18a].
Light-Weight [SWF19]. lightning [Ran10].
Lightweight [ADM19, AMSPL19, AMKA17, AARJ12, BCHL19, BSS13, BFMT16, BKL13, BM11, CGGPDMG12, CWP12, CCF17, DS11, ESS12, EKP13, FQZF18, GNL12, GAI18, Gop19, GMVV17, GMSV14, HZW18, HCTEPL12, IS12, IOM12, KE19, MO12, MFG16, MPM17, PCDG14, SBS18, She14, YN19, ZWY13, ZSY19, ZLY19, ZSH19, AMN18, AATM18, AKKY17, BLL19, Bor10, BBB16b, CL11, DA18, FLL14, GH15, GTSS19, KDH15, LLZ16, MCN18, MNP12, MHV15, MHY18, PJ18, PSDo13, SGJ18, Tan12b, TG17, WLZ16, WCFW18, WWBC14, XWZ18, XXCY19, XHM14, YCT15, ZSW18a]. Like [BW16, ERLM16, WJ19, CGCS12, HLH19, KO16, LJ15, LJ16, RS14]. Lilliput [BFMT16]. Limitations [DR12]. Limited [DFKC17, ZZC17]. Limited-Use [DFKC17]. Limits [AS16, GV14a, KS12]. Lindell [Ful10]. Line [FFL12, YMWS11]. Linear [BCI13, BW12, CGCS12, CMA14, EKP13, FGMP12, LGGL12, LJ15, LJ16, LFW16, WGF16, YCL17, BBEP14, Bul10a, FES10, GMOGCC15, Her10, HCCC11, LWK11, ÖS11, SA14, XSWC10]. Linear/Linear [EKP13]. Linearly [ADD10]. Linguistic [OO18, OO10, OTO18]. linguists [Maf16]. link [Ham12, VS11]. link-state [Ham12].
SWW+16, THA+13, WSC14, WDV18, WDKV19, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b]. Manager
[KK15, Kim16]. Managing
[La14, MD15, BC18]. MANET [KTUI16].
MANETs [Yan14]. Manhattan [SS10c].
manipulation [OF12]. Mansour
[DKS12, LPS12]. Manual
[Sac14]. Manuale
[Sac14]. Manuscript
[Ano16d]. Many
[CCL+19, LB13, HRS13, ZQWZ10].
Many-Core [LB13]. many-to-one
[ZQWZ10]. Map
[XYYY11, Br19, ISC+16, LZY+16, LWK+18, PC14, SE18, ZT14]. map-based
[LWK+18]. Maple [G’13]. Mapping
[CBL13, LHW18, MS17, JS18a, MM14a].
mappings [MC11, CDPLCA16].
mapreduce [DMD18, LJJ12]. Maps
[Ye14, BAAS13, BSBG14, KLW+16, LW10].
March [Ano10, Cra12, DDS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, ZWM14].
Marche [CCFM12]. Margaret
[Led16, Sch15a]. Marian
[Kap13]. market
[YWK10b]. marking [PJ18]. Markov
[CR12, FV17]. Marotto
[SE18]. Marshall
[Don14]. Martin
[ABJ13, Hof16]. Maryline
[Ano15b]. Mashup
[HTZR12]. Mashup-Providing
[HTZR12]. Masked
[GZW19, WH17]. Masking
[HF14b, PY+13, USH19]. Mass
[BPR14a, BPR14b]. Masses
[Ano15c].
Master
[Dew11, LYX+19, Mar10a].
Matching
[Lin15, RCBK19, Tan12a, DA18, LHM13, MR14c, MHT+13, PPTT15, SS17a, SM10c, YZL+18].
MathCW
[Bee17].
Mathematical
[Bee17, FGPGP14, Ham17, IBM13a, Mei10, Sch15a, Wes16, KM14, O010, Sta11b].
Mathematical-Function
[Bee17].
Mathematician
[Ano17e].
Mathematicians
[Acz11].
Mathematics
[Ano17b, Ayu12, Led16, Sch15a, Ter11, CM13, Kra12, PHWM10, Wes16].
MATLAB
[TRD11]. Matrices
[ÁMVZ12, BNA15, AKG13, FES10]. Matrix
[BFMT16, IAD10, KKK+18, LYY+18, SK12a, TD11T, Ye10, Cha13b, LLM+19, TK14].
matrix-vector
[LLM+19]. Matter
[Ran15, SS12a, DKA+14]. Max
[And13].
Maximizing
[DBPS12]. Maxims
[Kob10].
Maxwell
[LGP19]. May
[BL10, FBM12, Gil10, Sen10]. maze
[LLC10]. mbedTLS
[YGS+17]. MC
[HIDFGP15]. MC-2D
[HIDFGP15].
McEliece
[DN12, GV14b, MBR15, MT12, MG15, OTD10, SWM+10, VOG15].
Mclaughlin
[GL19]. McOE
[FFL12].
MDPC
[GAB19, HC17, VOG15]. ME
[XHH12]. Mean
[SZHY19, TTL10]. Meaningful
[LTC+15b, SA16a]. Means
[KRDH13, AMHJ10, Kam16, Pal16].
Measure
[DDD14]. Measure-independent
[DDD14]. measurement
[QLZ19, VGN14].
Measurements
[DTE17]. measuring
[DMWS12]. Mechanical
[RSCX18, Mat19].
Mechanism
[ABB19a, KD12b, LL15, LLY+18, Lin15, PTKK12, Saa12a, SMOP15, ZHS+19, CL11, FXP12, KKK+16, MCRB19, NXS10, PLPW13, PSJ+13, WB12, XYA+16, ZWM14].
Mechanisms
[CBO+18, CCC19, GPR+19, JNWS19, JSK+17, SGG18, FHH10a, KSA16, MMZ12, PLGMcDF18].
Media
[KBL11, Fri10a, vdWEG18].
Mediated
[Fra16, YHK+10]. Medical
[BDM+19, KBL11, UUN11, AIA+18, AMK12, KSA16, KLC+10]. Medicine
[MA17, LWK+18]. MEDiSN
[KLC+10].
Meet
[LJ17, LWKP12, LWFP12, LWKP14].
Meet-in-the-Middle
[LJ17, LWKP12, LWFP12, LWKP14].
meeting
[Hof16]. Meets
[RBHP15, BSR+14, MZA+13, PYH+18, SM13]. Mega
[WYL18]. Members
[YZW+12].
Membership
[FHR14]. MemGuard
[CZ14]. Memorial
[Ano11e]. Memoriam
[Gre11]. Memories
[AWSS17, BDGH15, RM18, SM18, YNQ15]. Memory
Kem11, KKA14, KKM+13, KKM+14, KKK14, KS15, KSB+17, KS19, LL11a, LZD+19, LH13, OYHSL4, Par12b, SSSA18, SLL+19, SSNS+15, hSZS15, SCR19, SSAF11, SKB+17, SBHC19, TZTC14, TKHK14, WSC14, WT10a, YHHM18, YNX+16, ZLDD14, ZDW+16, ZC12, MFB+13, SSL10.

mobile-cloud [KKM+13], mobiles [GCSAddP11].

Model [CLH13, LNK+18a, CL11, GH16, LH11b, MYYR13, THA+13, YLS12, ZX11].

Modality [BOP14, GBC19, SCFB15].

Model-based [IA15].

Model-Predictive [TBCB15].

Modeling [CJFH14, GBNM11, LTKP16, MKN15, OS16, VN19, ABR15, GZHD12, ZCZ+19].

Modern [Fri12, Fu10, OMNER19, RAZS15, She17, KAS15, Gre19a].

Modes [KMSM15, OS16, VN19, ABR15, GZHD12, ZCZ+19].

Modelling [BDB14, BL15, ACF16, KSI12].

Models [KMSM15, OS16, VN19, ABR15, GZHD12, ZCZ+19].

Modular [Abe12, GL19, LNL+19, Bro19, VN17].

modal [GCSAddP11].

Modality [CLH13, LNK+18a, CL11, GH16, LH11b, MYYR13, THA+13, YLS12, ZX11].

Modelling [BDB14, BL15, ACF16, KSI12].

Models [KMSM15, OS16, VN19, ABR15, GZHD12, ZCZ+19].

modified [CTHP13, EEAZ13, MM14b].

Modular [APPPV15, GL19].

Modulus [CNT12, LyWIZZ12, SEY14, KFL+10].

Moment [PTK14, GJ13, TPKT12, yWpNyLY11].

Moment-based [PTK14, TPKT12].

Moments [HD19, WLBDB11].

Monte [CR12, FKV17].

Montreal [JY14].

Morphing [MBC15].

Morphology [IA15].

MorphoSys [MD12a].

Morris [Gre11].

MORUS [YWM19].

most [Ald11, ESR14, GIJ+12].

Motion [GZH17, JHHN12, AP10, SYW17].

Mouse [ZPW16, HT11].

mouse-based [HT11].

Movement [ERLM16, GB19, ZPW16].

Movements [SRRM18].

Mozilla [LOE15].

MP3 [YWYZ12, YQH12].

MPC [GGHR14, RSMA19].

MPEG [YYO15].

MPEG-4 [YYO15].

MRAM [DSB16, PAF18, VDB+16].

MRAM-Based [VDB+16].

MrCrypt [TLMM13].

MSP430 [KSH18].

MSP430X [GL12, Seo18].

MST 1tn3 [SwT10].

Much [DL15].

Muhammad [ABJ13].

Multi [ASS15, BBEPT14, BRT12, CWL+14, CH12, DLGT19, GVW12, GJZ17, HYS11, HC12, HRS16, IG11, JS18a, KTT12, KMO14, LyWS10, MZYH15, MEF012, MLBL12, NGAuHQ16, OKG+12, OSSK16, PSSK19, SK12h, SOR16, SAM+18, TWZ+12, TYM+17, TFS19, Wan14, WOP15, XWSW16, YWY10, Ye14, ZC13, ZQY15, ZLDC15, BOP14, BGG+13, CPPT18, CLP+13b, CFVP16, CJXX19, CG12b, CLHJ13, CW14a, CZ15b, DRN16, DFJ+17, FHZW18, GOMGC15, GPVCBRO12, GZS+18, GBC19, HL14, HL11, HCC11, HLC12, ISC+16, JCHS16, KM11, LXMW12, LXK+15, LCT+14, LH13, LWY12, Mas17, QMC17, CFGB15, SLL+19, SCY15, SWW+16, SSS11, TLL12, WDD13, WZZW20, WIX+17, XLWZ16, XHM14, YCC16, YNH19, ZZKA17].

multi-agent
Naïve [ZLW+17]. Name [FP19, YCM+13].
Name-Based [FP19]. Named [LLZ+17].
Names [ABJ13, MPJ+16]. National
[Fid18, ABJ13]. Natural [ZCWS15].
nature [KL13]. Naval [Don14]. navigation
[JS18a]. Navy [Maf16]. Nazis [Hea15].
NDSS [Ano10]. Nearest [XLP+18, LVRY10, XMY+17].
nearest-neighbor [LVRY10]. nearly
[PHGR16]. necessary [TD14]. NECPPA
[PZBF18]. Need [LNG19]. needs [Sch12b].
neglected [Joh15]. Negligible [DF11].
negotiation [MMP19]. Neighbor
[KA18, LVRY10]. Neighborhood [DA10].
Neighboring [LSQ11b, LC15]. Neighbors
[XLP+18]. neighbour [XMY+17]. Neil
[Pea11]. NeMHIP [THA+13]. Nemo
[KD18]. Neon [ZMM+10]. nested
[FHH10a]. Net [LHF12]. Nets [PS14].
Nets-based [PS14]. Network
[AA19, Ano10, Bis17, CWL16, CJ13, CLH13,
DRS16, Hay13, HDWH12, HS18, Kim15,
KCC17, LH12, LCLL15, LY16, LTW11,
MJG012, NNAM10, NRZQ15, SGC16, She14,
TLW12, VV18, VKPI17, VFV17, VQA15,
VKC15, WP15, WYL18, YZLC12, YSJL14,
AKM+11, AL15, Ano11a, AZF+12, CJXX19,
CL11, DLK+16, FPBG14, FZZ+12, HW19,
HL19, HWG10, HBI3, HKB14, JZS+10,
KLH15, KP18, LH11b, LKCL13, MZA+13,
MJS13, NDNR13, OF11, PL16, RCV15,
Ser12, SCKH10, SKS+18, St11a, Tan15b,
THA+13, WYL13, WS14, YLS12, ZOSZ17,
Ste15b]. Network-Assisted [KCC17].
network-based [YLS12]. Network-Coded
[She14]. Network-on-Chip [Bis17].
Networking [CKHP19, FP19, KYEV+18,
LCK11, LLZ+17, ZHL15, Kim11, LCM+17].
Networks
[ABC17, ABC+17, BN14, BPSD17, BCG10,
BFMT16, CS14, CSH+18, DLGT19, DS11,
DF16, FMS12b, GMVV17, HZC+12,
HBC13, HK14, JWNS19, KHN+11, KH10,
LL11, LL15, LHM+15, LZCK14, LWCJ14,
LLZ+12, MKK17, MPM+17, NSA15,
NYR+14, OO12, OKG+12, PYM+15,
PSM+18, PCPK14, RWLL14, RSX18,
SWYP12, She14, SP15b, SS15, SMI11b,
SLH11, SZZT18, SAM+18, TCN+17,
WXL+17, WLY+15, WZCH19, XHC+12,
XHZ+19, YMI6, YHSW19, ZC13, ZW15,
Zha15b, ZLDD12, ZSA12, Aia15, ASO14,
APK+18, AIB+16, AIKC18, ADF12, BDK11,
BLAN+16, BBBBB16, CDGC12, CLM+12,
CML+18, CLSW12, CL11, DSCS12, DK12,
DLN13, EEA13, FA14b, FMA+18, GH16,
HGWW11, HZC+14, HZWW17, HCCC11,
HCM11, HTC+10, HY18, JNU17, JLT+12,
JMW+16, KMG17, KM10b, KLC+10, KO16, KLW+16, KDW+17,
LLLS13, LC17, LMMC11, LNNH13, LJJ14,
LIK+17, LNK+18b, LZZ19b, MSM+18b,
NXS10, OPHC16, QMW17, RR17].
networks
[RPG12, SGGCR+16, SA12, SGJ+18,
SZMK13, hSZZ15, SKK10, TODQ18,
TKHK14, WGJT10, Wan13, WW14,
WVD18, WXK+17, WX13, XWDN12,
XHCH14, XMHD13, YHS16, YWW+19,
YN19, ZWW+11, ZBR11, ZSSL14, ZTT16,
ZLDD14, ZH+17, ZXX11, LNK+18a].
Neural [CSH+18, RSX18, SKS+18, YZLC12,
EEAZ13, HW19, KMG17]. Neuroscience
[BSR+14, JW14]. Neutrality [Kha10].
Neutrality-Based [Kha10]. Neutrosophic
[JS18b]. Nevada [IEE10]. never [Bai12].
Newly [ABJ13]. Newman [And13]. News
[Edw14, Edw17, Sav13a, Sav15, Sav16].
Next
[HEP+11, MR14a, MJG12, Aia15, ACD+15].
Next-Generation [MR14a]. NFC
[LY14, Mic16]. NFSR [WGD18].
Niederreiter [HCC17, MVVR12].
Nievergelt [Ter11]. Nine
[Mac12, LYHH14]. NIST [ZSH+19]. NIZK
[Pas13a]. NIZKCTF [MBC+18]. NIZKs

Noised [JLS12]. Noisy [ASN12, HZW+14]. Non [AH19, AS17, AMH+16, BBCL19, BCI+13, CG14a, CPS16, DJL+12, DPW18, EKP+13, FHKP17, FMNV14, GL19, GZX19, HKB14, KTT12, LLG15, MFH13, MSas12, OOR+14, Pas13a, QJC+18, RM18, RMG18, Svo14, SM18, WgmW12, XZL+19, YNQ15, YKKL12, ZLDD12, AY14a, BS15, CS11, ESR14, GIJ+12, Kre13, Lan11, LP11, MSas13, SES+16, SXL16, VBC+15, XSWC10, Yan14]. Non- [AH19]. non-adjacent [Kre13]. non-associative [BS15]. Non-Black-Box [CPS16]. Non-blind [HKB14, RMG18]. Non-Boolean [AS17]. non-browser [GIJ+12]. non-compliant [Lan11].


Non-malleability [KTT12]. Non-Malleable [DPW18, MSas12, CG14a, FMNV14, OOR+14, Pas13a, LP11, MSas13]. Non-monopolizable [DJL+12]. Non-perfect [FHKP17].


Norm [Low12]. Note [HYS11, Gal13, GR19, Hwa11, Lim11]. nothing [Cer15]. Notifications [LBC18]. Novels [CLHC12, DCM18, KRxH+13, LLG15, LyWZ12, LH11c, MJGS12, MSC+15, SWM+10, SC12, VN16, WHZ12, WZXL12, YZX+14, YLSZ19, Ye14, ZZM17, BOB13, BSBG19, CH10, DDFR13, GPLZ13, HCC11, IZXL15, LCM11, LMJC11, LH13, LWW+10, LML+13, MRT10, NZL+15, PZBF18, SCR19, SYW17, Sun16, TG17, jT12b, WLYL13, WZG+12, YWT+12, ZBR11].


NTT [MCDB12]. NTT-Based [MCDB12]. Nuclear [Hel17]. Number [AD11, BKLS12, CDK+10, DSB18, Fok12, Ham17, KA18, LTKP16, LCLW17, MFG16, NIS12, NNAM10, Sha10, SRAA17, SRK+17, SRK+18, WJ19, CFY+10, CP13, LLP+18, LGKY10, Lim11, MS12a, MRT10, SH11, Sti11, XSWC10, Gre19b]. Numbering [MNS11].


O [CDD13]. Obfuscated [LMS16, OWHS12, ZM16]. Obfuscating [BG1+10, BG1+12]. Obfuscation [ABCL17, AS16, AWSS17, BBC+14, BV18,
BCP14b, BR14, CZ15b, DRS16, EMW14, FKOV15, GGHR14, GHG+16a, GGHW17, MH14, ZL19, BBGT12, CFVP16, GHG+16b, OSSK16]. Obfuscation-Based [ABCL17], Obfuscators [PSD15], ObfusMem [AWSS17], Object [BCK17, SSSA18].

Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17, SSSA18].

Obfuscation-Based [ABCL17].

Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17, SSSA18].

Obfuscation-Based [ABCL17]. Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17, SSSA18].

Obfuscation-Based [ABCL17]. Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17, SSSA18].

Obfuscation-Based [ABCL17]. Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17, SSSA18].
SGS14, TK19, WDDW12, Bax14].
Partial-Shape [HFW+19]. Partially [KB10, XZP+19]. participants [KSU13, WTT12]. participating [CH10].
Particle [ZSM18]. Parties [YCR16, Kip13]. Partitioned [FVS17].
Pascal [LGP19]. Passau [GLIC10]. PASSERINE [Saa12a]. Passion [Hof15].
Passive [DHB16, GSC17, SB17, BM13, uHAN+18, LWL11, MK12a]. passport [LZJX10].
Password [ASBD16, BRT12, CLY14, DM15, DGMT19, FS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZHX16, ABK13, AIKC18, CTL12, DSCS12, FA14a, FIO15, FHV16, GPLZ13, HCC10, IOV+18, KMTG12, LWS10, LNK13, LZZ19b, MM12, MoO11, MCRB19, Par18, SVY19, Tso13, TKHK14, WZM12a, WZM12b, YC12, ZXWA18].
Patchwork-Based [NXH+17, XNG+14].
Path [DMS+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13]. Patient [ZLDC15, ZVG16]. Patient-Centric [ZVG16].
Pattern [DCA18, PSSK19, YTF+18, ATKH+17, DA18, uHAN+18, KPS10, OSSK16, PPTT15].
Pattern-Based [PSSK19]. Patterns [Ano16e, BPSD17, TSH17, WOLP15, BDK11, LHM13, NML19, SPK17]. PAWN [JNUH17]. Pay [EAAAA19, CCSW11].
Pay-per-use [EAAAA19], pay-TV [CCSW11].
PayLoad [CHHW12, AZH11, JNUH17, JKAU19].
payload-based [JNUH17, JKAU19].
Payment [DG15, SYC+17, SYW17]. Payments [RBHP15, MPJ+16]. PC [YE12].
PC-Based [YE12]. PCIE [IBM13b]. PCM [LY15].
PCM-based [LY15]. PCPs [MX13].
PCs [GPT14, GPP+16]. PDGC [CGB+10].
PEA [ZGL+18b]. Peaks [TC10]. pearl [Rus15].
Pecherskii [Kuz11]. PEDCKS [XLC+19]. peer [NCCG13, ZYW+13].
Perfect [Pas13a, Sch13, CZ15a, FHKP17, LLC10, Lew10, XW12]. perfectly [ADG16].
Performance [Alo12, AW15, AW17, AB15, BM18, CGL+12, CC10, DLK+16, DGFH18, DBPS12, EGG+12, ESRI14, FPBG14, GLG12, GPR+19, GCS+13, HKL+14, KRHC19, KAK8, LCK11, LPG19, LPO+17, MHC12, SKV12, SSP19, TPKT12, WDDW12, Xio12, YWFL18, ZLDD12, ABPD15, BGE+18, CLB19, FHL19, GCVR17, MCL+19, MMS+17a, MS13c, ZLDD14].
Permission [VN16]. Permutation [LJ16, Bar19, GMSW14, LK14].
permutation-based [LK14]. Permutations [ARH+18b, ARH+18a, BKLS12, Faa19, Mat14]. Persistent [CSYY18, SXH+19, TYK+12, ALL+18, PKA15]. person [PN10]. person-centric [PN10].
Personal
posed [Lan10]. Position [BCF+14, CGMO14, MS17, SOR16, YXA+18].

Position-Based [BCF+14, CGMO14].

Positioning [HK18]. Positive [CKHP19].

Possession

[EkB+16, YJSL18, ZPXX17, SYY+17].

possibility [BGI+10, BGI+12]. Possible

[BF12, Fra15, Orm16]. Post

[LLK18, MKAA17, NDR+19, Y+17, ZCC15, YDH+15, Sen10, Yan11].

Post-challenge

[ZCC15]. Post-Quantum

[LLK18, MKAA17, NDR+19, Y+17, YDH+15, Sen10, Yan11]. postcamera

[Lin14a]. Postfix [HEK18]. Postquantum

[Ano16a, Ano16b, BLM17, BLM18, Lau17, MGG+19, YZC+17]. Posts [AIF+19].

posture [SHBC19].

[Cil11, VS16, ZW15]. Power [ARP12, AS16, CKHP19, HHR11, MMP14, MD12b, MAS16, MS17, SAJL16, SDM+12, TQL+14, WT10b, YAM+15, ZH15, ZJ11, FAA+18, FMC19, LGKY10, LKAT12, QGGL13, RITF+11].

Power-Positive [CKHP19]. POWER7

[BAB+13]. Powered [SFE10]. PowerEN

[HKL+14]. Powerful [IP16]. pp

[Joh10, Sch15a, CGCS12]. PP-1 [CGCS12].

PPA [LZD+19]. PPFM [MS17]. PPM

[XHC+12]. PQCrypto [Sen10, Yan11].

Practical

[ATK11, BHH+15, BDH11, CLSW12, CGH17, Cra11, DZY10, EA12, FPS12, FS1K0, HSA14, HPO+15, HK+18, LW16, LJYW18, MBF18, PPTT15, PDJ+19, RWZ13, TSH17, WHLH16, XW13, YZLC12, ZYD10, ZLW+17, AMS+10, BS13a, C1N+14, JSK+16, LFZ+17, PHGR16, WR15, YKGGK13, ZSW+18a]. practicality

[NDNR13, Zha15a]. Practice

[ABD+15, CDFZ16, FBM12, PWVT12, Rog16, RBHP15, RST15a, RST15b, SN10, SAKM16, NS10, Sta11a].

Practice-Oriented [Rog16]. practices

[Tay19]. Practitioners [PP10a].

Pre

[YWL+17, YHHS16]. pre-distribution

[YHHS16]. Pre-image [YWL+17].

Preaveraging [GWM16]. PRECISE

[HYF18]. precision [MN14, SK12b].

Precomputation [GKM16].

Predicate

[HKPP16, NMS14, YKNS12, ZYT13, FH13, HFT16].

Predictability [DK16b].

prediction [CSS+13]. Predictive

[TBCB15]. Predictors [EPAG16].

Predistribution [YM16].

Preface

[Ano19c, YYW19]. Preimage [Li10].

Preseding [Ran16]. Presence [BDPS12].

Present

[Bon12, LJ16, WH17].

PRESENT-like [LJ16].

Preservation

[BCP14a, LLG15, VSV15, YJSL18, Yon11, FZZ+12, LVRY10, TMLS12]. preserve

[BAG12]. preserved [SWW+17].

Preserving

[ABCL17, BJL16, BHKN13, BJL12, CWL+14, CRE+12, GZZ+13, HSHMY12, HLLC11, HXC+11, HMK14, HK18, KKK+18, KLK+19, KS12, LMG17, LNXY15, LQD+16, MHW+19, MJS+19, MTM18, NMS14, OFMR16, PR12, PD14, PSS+13, PPRT12, Pet12, RVH+16, RSR+19, RBHP15, SZDL14, SZQ+17, SZTT18, VFFHF19, WPZM16, WZCC18, YK12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, APMCR13, AIB+16, ALL+18, BBDP16, BLV17, FH13, FMA+18, GH15, GH16, GAI+18, GA11, HSH11, HAK19, IC17, IOV18, JKL+16, JLX+19, KH18, LHL+18, LZD+19, LSQ15, LW13a, LCY+16, LLG19, OSP+19, PZB18, QLZ19, RR16, SYY+17, SMS+16, Tan12b, TSH14, WLZ+16, YMM13, YNX+16, YL11, ZYW+13, ZOS17]. Press

[Ano15b, Ano17b]. Press/Elsevier

[Ano15b]. Prevent

[HLAZ15, PYM+13, JSDK+16]. Preventing

[DCAT12, HAK19, MT17, CAM19, SKEG14, WS12]. Prevention

[CW16, VS11].

Primality [Cou12]. PRIME

[ACK+10, GM13]. Primes [Gre19b].

Primitive [App15, MCS+15]. Primitives

[BSJ15, EAA12, HLN+10, SP15b, ABDP15, BSR+14, Gor10, WSL+19]. PRINCE
Princeton [Ano17b].
Principles [BKLS18].
[BCG+12b].
Principal [KYEY+18, WW14].
[BCG+12b].
Privacy [KPS10, PKS18].
[BCG+12b].
Print [KPS10, PKS18].
Print-cam [PKS18].
Print-scan [KPS10].
Printer [EMW14, FNP+15].
Priority [LMS16, Bia12].
[BCG+12b].
Privacy [AKM+11, AKKY17, ALL+18, ACM12, ABHC+16, BN14, BCF16, BA18, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DCA19, DTE17, ESS15, FGR+17, Fei19, Fri13, GZZ+13, HSMY12, HBCC13, HXH+17, HXC+11, HK18, JN12, JLX+19, KM10b, KKK+18, KLR+19, KCC17, KSI2, KHH18, LMGC17, LSBN14, LLG15, LXY15, LQD+16, MYY13, MJS+19, MV18, MTM18, NSS14, PD14, PSS+13, PPP12, PZPS15, PSD15, Pet12, PH16, RHV+16, RSR+19, RCP+18, RWL14, RBHP15, SS17a, SG12, Set16, SZDL14, SZT18, SOF12, TMLS12, TMGP13, VKK+19, VFFH19, WPM16, WZCC18, WMYR16, YJS18, YMM13, Yon11, ZHW+16, ZM16, ZOSZ17, ZXL19, ZHW15, ZLDC15, ZHL15, ZTL15, ARL13, APMC13, ACK+10, BGE+18, BBPD16, BPL1, BAG12, CXX+19, CDF+10, DZS+12, FH13, FMA+18, FZZ+12, GAI18, HSH11, HKA19, HPL+19, IC17, IOV+18].
Privacy-assured [WMYR16].
Privacy-Aware [BCF16, ARL13, MGP10, ZDHZ18].
Privacy-Based [BS13b].
Privacy-Enhanced [DTE17, ACK+10, YQOL17].
Privacy-Friendly [KCC17, ACM12].
Privacy-Preservation [LLG15].
privacy-preserved [SWW+17].
Privacy-Preserving [ACCL17, BJL16, BJL12, CWL+14, GZZ+13, HSMY12, KKK+18, LMGC17, LNY+15, LQD+16, MJS+19, MTM18, NSMS14, PD14, PPP12, Pet12, RHV+16, RSR+19, RBHP15, SDL14, ZTT18, VFFF19, WPM16, WZCC18, ZHW+16, ZM16, ZHW15, ZTL15, ZTI11, AKKY17, AL+18, JLX+19, KH18, ZOSZ17, APMCR13, BBPD16, BLV17, FMA+18, GAI+18, HSH11, HKA19, HHL+18, LZZ+19, LQ15, PZBF18, QLZ19, RR16, SYY+17, SMS+16, TAN12b, ZYW+13].
Private [BKLS18, GM13, JIA14a, LSQ15, MV19, QZL+16b, RCBK19, 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].
Prize [Ten18].
PRNG [DK16b].
Proactive [SLL10, WMYR16].
Proactively [OPHC16].
Probabilistic [BFG+14, Rao10, WP17, KSU13].
Probability [DF11, HLC16].
Probability-based [HLC16].
probable [Sav13b].
Probably [MMS17b].
probe [Edw14].
Problem [CLL16, GKS17, Hor19, LLGJ16, NA10b, TKM12, Bar19, Mes15, MR14c, RH10, VM14].
Problems [AH19, Duni12a, Fra15, GT11, KRHD13, KPC+11, LAL14, RBS+17, SK14, TPL16, WSL14].
Procedure [CS14, OS12].
Proceedings [LCK11, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Duni12b, FBM12, Gil10, GG10, HWG10, IEE10, IEE11b, IEE13, IWL11a, LTT11, Ple10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLC10, IEE11a, Kin11, Lin14b, Sah13].
Processing [JGP+18, SAKM16, SZHY19,
TKMZ13, VKPI17, 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** [GBFB12, Gue16, SJLK18, RYF+13]. **Product** [ADM12, CCM+15, OT12, YKNS12, Cha13b, DMB17, YI17]. **productivity** [Tay19]. **Products** [LMG+18, RS10]. **Professional** [HGOZ19, STCI1]. **Profiles** [BCF16]. **Profiling** [DP12]. **Profit** [APPVP15]. **Program** [MZI17b, Wal18, CLZ+17, DMD18, GGH+16b, MFF13]. **Programmable** [CLF+17]. **Programming** [Bee17, BEM15, LSSL19, SY14, ASVE13, HL10]. **Programs** [BGI+10, BGI+12, CL16]. **Progress** [AB10a, BL10, BC11, GG10]. **Progressive** [SA16a]. **Prohibition** [Hor19]. **Project** [SPG+19, ACK+10, SS10c, Wll18]. **Project-Based** [SPG+19]. **projective** [CZ15a]. **Prominent** [ABJ13]. **Promise** [Pau10, PWVT12]. **promised** [HS11]. **Proof** [BDSG+13, Bla12, CZL12a, CZL14, FSX12c, GKG19, Kuz11, LYX+19, LW12, NLY15, SR14, Ste15a, Z zm17, Mon13, PPT15, VBC+15, WHJ17, ZCZ19]. **Proof-of-Concept** [GKG19]. **Proofs** [BBD19, BGK12, BCG12, BGB12, BCI+13, BSDG+13, CZL12b, IJW14, LNZ+13, Mau12, NTY12, Sav13b, WPZ16, AGHP14, KPP16, KKK+16, Lii10]. **Propagate** [GWMI16]. **Propagation** [SKS+18, WWC+11, YZLC12]. **Properties** [CCK12, CCCK16, DQFL12, FY11, HJJ+19, JS18b, JR13, KU12, Sch12c, CLCZ10, WT13]. **Property** [HJJ+19, HEC+12, PR12, Rja12, YWM19, Bar19]. **Proportions** [Ber12]. **Propose** [BFMT16]. **proposed** [Bax14, HWB10]. **Protect** [CTC+15, CKHP19, YMC+17, BVBI12, CDF+10, dCCSM+12]. **Protected** [BDGH15, SG15]. **Protecting** [BCP14a, GSFT16, LLPY19, Mar10b, RCP+18, SCY15, Wat14b, ATKH+17, CXX+19, CDA14]. **Protection** [AIM+19, CDD13, DCA19, EAAAA19, GST12, GPR+19, HXHP17, Lop12, NGAnH16, NDG+17, RR11, SEY14, SJ12, ZWW17, ATI+10, HLYS14, HPL+19, KKM+13, Ksz12, LVY10, RS17, TLL13, YWT+12]. **protection-key** [HLYS14]. **Protocol** [ADSH18, BL12, BC14, BCM+15, BSSV12, BF16, CC14, CCM17, DCA19, FLH13, FMTR12, Fra16, GI12, Hs11, HC12, HL10a, HCP18, HCET+12, HKL+12, JHZ+16, JHW+19, Kms19, KMO14, LNZ+13, LCCJ13, LNXY15, MBC15, MR10, PSS+13, SBS+12, SGC16, SS15, TWNC18, TYK+12, WT10b, XJR+17, YS12, YWF18, YLS19, YWZ+12, ZXZ+11, ZSY19, AAM18, AKG13, AIB+16, AICK18, AN15, BDM18, BGAD12, CSD18, CSG11, CJP15, DLK+16, EA12, FA14b, FIO15, GMSW14, GH15, Gop19, GLM+11, HPC12, HWB12, HL14, IC17, IOV+18, JKL+16, JXLZ15, Kim11, KO16, LLS13, LDDAM12, LKkl13, LWS10, LXMW12, LZD+19, LEW19, LY14, LML+13, NCL13, NLYZ12, NML19, OHJ10, Par12b, SSA18, SPL18b, SB17, SGJ+18, SWW+16, SSS11, SSL+13, TGI17, THA+13, Tso13, TKHK14, VS11, WCWF18, WZD19, WD18, WZM12a, WZM12b, WLS14, WMYR16, WT10a, WTT12, WCCH18, XCL13]. **protocol** [XHM14, YC12, YZQ+14, YMM13,YN19, ZwQ+11, ZT16, ZYC+17, ZWX+18, ZXWA18, ZG10, ZZC15, XN11, BOB13, CJP12, LGFCCGRP14, Ste15b]. **Protocols** [ADH19, AP13, ABHC+16, BMP12, BSBB19, CCK12, CCCK16, CCF17, CCD15, CCDD19, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KOS16, LY16, MV19, MS16, MT12, MUR16, NRY+14, NSMS14, PS14, SBS+12, SBS18, Sch12c, SOF12, TM12, Xio12, YRT+16, Ala15, Ano13b, AKS19, ACC+13, ACM12, BJ10a, BKR19, CML+18, CR10, CLCZ10, DGNJ14, FTV+10.]
Prototyping [KPC+16]. **Provable** [BKLS12, CC14, EKB+16, Rog16, YJS18, YMSH10, YYW19, ZX11, ZPX17, FA14a, HRS13, LHH11, SYWX19, WB12, XCL13]. **Proving** [Sar14, AGH+17]. **Proximity** [IW14, ARL13, Alp18]. **proximity-based** [ARL13]. **Proxy** [ASS15, GSW+16, GJJ15, GJZ17, GZXA19, HGWY11, HXZ15, KP12, LSLW15, LAL+15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW+16, YMWS11, YCM+13, BGP+17, CLH+16, FSGW11, FSGW12, GH12, HWDL16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, LL16b, QMW17, SLZ12, SKB+17, Tia15, WHY+12, Wan18, WLS14, XWC14, YZCT14, ZLY10, ZDW+16]. **Proxy-invisible** [SYL13]. **Ps** [HDWH12]. **Pseudo** [NN12, XYZXY11, CFY+10, KM10a, MG15, PLsvdLE10, SH11, SM11, XSWC10, Zim10]. **Pseudo-Random** [XYZXY11, CFY+10, KM10a, MG15, PLsvdLE10, SH11, SM11, XSWC10, Zim10]. **Pseudonym** [XHM14]. **Pseudonymous** [BDFK12]. **Pseudoprime** [DW12]. **Pseudorandom** [AS17, BCGH11, BK12a, Kla10, MFG16, CP13, GCH15, HRV10]. **Pseudorandomness** [Sha10]. **PSMPA** [ZLDC15]. **PSO** [TLL13]. **PTSPACE** [JJUW10]. **PTAS** [JLX+19]. **Public** [Ano11b, ABW10, BVS+13, BB14, BM18, BKLS12, BKKV10, CT18, CLP13a, Che15, CLN19, CNT12, Con12, FBM12, GKS17, HEP+11, HTC+15, HLI19, IM14, JLT+12, JWNS19, KFOS12, LYX+19, LLSW16, LPs10, LSQL18, LZC14, LLH18, MZH15, MMP14, MT11, Mat14, MPRS12, Muf16, NTY12, Orm16, PDNH15, RSGBN12, RVS+18, RW12, RBHP15, SGG18, Saa12a, Sch19, SK12b, Seo18, SWM+10, Sia12, SC12, SLY+16, SGP+17, SvT10, TMC15, TT12, WP17, WZ15, WWHL12, Wil18, XNKG15, XXJ12, Xio12, XJW13, YL17, YKC+11, YFK+12, YMC+17, ZCQ19, ZY17a, AA14, ATKH+17, BS15, BSW12, CFG+17, Dnr15, HZW17, Hld19, HL14, HT17, LSNB14, LL15, LFWS15, LH13, LL16a, LG19, RPSL10, SES+16, SY15b, VN17, XLC+19, YT11b, YYS+16, YN19, ZZ11, ZCC15, ZCL+19, ZY17b, FB12]. **Public-Coin** [CLP13a, Mat14]. **Public-Key** [BVS+13, BKKV10, GKS17, KFOS12, LL18, MMP14, MPRS12, NTY12, Orm16, PDNH15, RSGBN12, RW12, SK12b, Seo18, SWM+10, Sia12, XNKG15, XJW13, YKC+11, YFK+12, ZY17a, ABW10, IM14, LPs10, LZC14, BWS12, LLG19, RPSL10, SES+16, VN17, XCC15, ZY17b]. **Publication** [ZTL15]. **Publicly** [NMP+13, SZQ+17, YNR12a]. **Publish** [BGP+17, DLZ+16b, OFMR16, PRSV17, SLI11, TKR14, YSM14]. **Publish/Subcribe** [DLZ+16b, OFMR16, PRSV17, TKR14, YSM14]. **published** [MYR13]. **Publisher** [Fal10, Mur10]. **Publishing** [VSV15, LLL+17b]. **Puebla** [AB10a]. **PUF** [BDM18, CCKM16, CCM17, DS16, KPKS12, KL+12, MV12, SRK+17, SRK+18, VDB+16]. **PUF-Based** [CC17, KPKS12, MV12, BDM18].
Pufferfish [KM14]. PUFKY [MVV12].
PUFs [IRK18, IGR+16, LZZ+19a, USH19].
Pulse [OMPSPL+19, MRRT17].
pulse-response [MRRT17], punctured [MG15]. puppet [Lac15]. Purpose
Pushdown [CCD15]. Pushing [FHV16].
Puzzle [IBM13a]. Puzzles [RSBG12, dCCSM+12, dCCSB+16]. Py
[DGIS12]. Py-Family [DGIS12]. pyramid [MHT+13].
Q&A [AHN+18, Hof15, Hof16]. Q3 [Ven14].
Qaeda [Mac14, Keb15]. QC
[YY14, GAB19, HC17, VOG15]. QC-MDPC
[HC17]. QIM [LJK17]. QIP [JJUW10].
QoP [Ksi12]. QoP-ML [Ksi12]. QoS
[BGC10]. QS [AZPC14, HDW12].
Quadratic [KRDH13, SEY14, YDH+15].
Quadraticity [MS12b]. Quality
[CSCW12, KSI12, NNI12, YCM+13, SS11, WZLW13, WKH11]. Quantifying
[CBRZ19, GZSW19]. Quantitative
[BL15, MLBL12, MV16b, HM16].
Quantization [SSA13].
Quantization-Based [SSA13]. Quantum
[ANO15d, ANO16c, ANO17d, ANO17e, BB14, Ber14, BCF+14, Che17, CCL+13, Feh10,
FKS+13, Fol16, JEA+15, JL18, Kar12, KP10, LLK18, LHA+16, MS16, MSU13,
Mos18, MKAA17, NNA10, NA10b, NDR+19, QCX18, RK11, RMS15, RS18, Sasi18, Sti11,
TKM12, Unr15, WCL+18, Y+17, ZWS+18, ABB+14, BJ16, BCND19, CML16, Edw17,
FRT13, GMJ15, MI14, JSK+16, KK+16, LLP+18, LyWSZ10, LCW+16, Liid12, QD16,
SK14, Svo14, VV19, YHD+15, vDKS11, Sen10, Yan11]. Quantum-Oblivious-Key-
Transfer-Based [WCL+18]. Quasi
[BGJT14, OWHS12, OTD10, BGJT13].
Quasi-Chirp [OWHS12]. Quasi-Cyclic
[OTD10]. Quasi-Polynomial
[BGJT14, BGJT13]. Quaternion
[HD19, YNWN15, yWPyN13].
Queries [GYW+19, HLS12, LHKR10,
PBC+17, ZZQ+19, BKV13, CHX13,
DFJ+17, GLM+19, HMCK12, PCK20,
PRZB12, TKMZ13, WL19]. Query
[DA18, GA11, PCDG14, WCL+18,
XLP+18, AZPC14, BS13a, BKR19, CH11,
ED17, HWK+15, JCHS16, LK+14, LW13a,
XMY+17, YQOL17, ZCC17, ZHT16].
Query-preserving [GA11]. Quest [Fox13].
Question [TWNC18, Cha13b]. Quisquater
[Nac12]. Quorum [Kar12].
R [Gre19a, BS12, LV11, PP10b, WYW14].
R3579X [BDK11]. Rabbit [FSW11].
Rabin [Chi13a]. Radial
[HD19, pNyWY+14, CG12b]. Radio
[KAHK17, CJP12, CJP15, EA12, Kim11,
NLYZ12, RPG12]. radio-frequency
[CJP12, CJP15]. radix [GKCK11].
RAGuard [ZHS+19]. Rail [HF14b].
Raising [YW10]. RAKAPOSTI
[IOM12]. RAM [RYF+13]. Ramamujan
[KK10]. Ramifications [ALR13]. Random
[Ana14, CBXJ19, CDK+10, DSLB18,
EAA+16, FZT14, FSX12a, GSW+16, Grec17,
KS15, LTKP16, LPL15, NIS12, NAM10,
NN12, SC10, SRK+17, SRK+18, TM18,
WS12, XYXY11, XQL11, YM16, YS12,
YKC+11, YFK+12, YLA+13, ZYM18,
Ara13, CFY+10, CT11b, GPLZ13, GLM+16,
GLW13, HKT11, KM10a, LGK10, LLY15,
LHM13, MRT10, MG15, PLSvdLE10,
QLZ19, RG10, SMD51, SYL13, SH11,
SM11, Shy15, Sti11, WWWY11, XSWC10,
ZOC10, ZPZ+16, Zim10]. Random-Grid
[KS15]. Randomization [Gas13].
Randomized [ARP12, CATB19, GT12,
HHR11, SR12b, BWA13]. Randomness
[AY14a, Ana14, ABF12, ACM+17, BWLA16,
KMS19, MSH10, MS16, DTZZ12, FR13,
RY10, TC11]. Range
[DA18, BKR19, HMCK12, JCHS16].
range-query [BRK19]. Rank
Ranked [SS10b, FES10].
Ranking [ZDL12, AT10].
Ransomware [MPA+18].
Rapid [KPC+16], rare [Sch11].
RASP [AZPC14], RASP-QS [AZPC14].
Rate [LJK17, PPS12b, PCPK14].
Rationality [GLR10, GLR13].
RBAC [VN16].
RC4 [GCS+13, Loc15, Ree15, RS14, Sar14].
RC4-like [RS14].
Re-authentication [LBR12, FXP12, LMJC11].
Re-Encryption [GB12, GSW+16, GZXA19, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PRSV17, WY10, XJW+16, BGP+17, CFZ+10, CLH+16, CZ15b, DEL19, FSGW11, FSGW12, FXP12, GH12, HWDL16, HYF18, KKM+14, LMJC11, LCT+14, LFWS15, LL16a, Par18, SYL13, SLZ12, SKB+17, Tia15, WGJT10, WHY+12, Wan18, WLS14, XXX15, YZCT17, ZDW+16, LAL+15].
Re-configurable [ADSH18, HG12, HLN+10, LZZ+19a, MLCH10, NDMMW16, PP10b, PG12, SRK+17, SRK+18, ZLQ15, EHKSS19, MD12a].
Reconstruction [AUD12, BCTPL16, BJCHA17, DM19, IA15, LGM+16, MR14b, BAG12, uHAN+18].
Recommendation [BD15, Bar16, Gir15, KKH+18, NIS12].
Reduction [SSNS15].
Recursive [TP17].
Redesigning [VFV17].
re-enrollment [DEL19].
oregistration [Par18]. re-signatures [Tia15]. Reachability [SVG16]. Reactive [JR13]. Read [LPPY19, Sto12].
Read/Write [LPPY19]. Reader [JLZ18].
Reader/Router [JLZ18]. readers [HDPC13].
Reasoning [TSH14]. Rebound [KNN10, Sas12].
Reco [EHKSS19]. Reco-Pi [EHKSS19]. recoding [TMK11]. Recognition [AQQ12, BCTPL16, BJCHA17, DM19, IA15, LGM+16, MR14b, BAG12, uHAN+18].
Recommendation [BD15, Bar16, Gir15, KKH+18, NIS12].
Reconciling [SSNS15]. Reconconfigurable [ADSH18, HG12, HLN+10, LZZ+19a, MLCH10, NDMMW16, PP10b, PG12, SRK+17, SRK+18, ZLQ15, EHKSS19, MD12a].
Reconstruction [AUD12, BCTPL16, BJCHA17, DM19, IA15, LGM+16, MR14b, BAG12, uHAN+18].
Recursive [TP17].
Redesigning [VFV17].
Redistributed [LXCM11]. Reduced [BW12, DWZ12, KNN10, LWZ12, LJF16, LWPF12, AKY13, Ay14b, LFW+16].
Reduced-Round [LWZ12, Ay14b, LFW+16]. Reducing [TSH18]. Reduction [ABR12, FYD+19, LCLW17, LSC+15, YMA17]. Reductions [BHKN13, BCG19, DW12]. Reference
Reﬁnement [BCEM15].
Reﬁnements [LL11]. reflections [Hai17, OF12]. Reﬂexive [SRM18].
Refractive [PHN+12]. Refresh [LSC+15].
Regaining [WBA17]. Region [CCFM12, HZW+14, KS15, FHV16, LWLW11, WW13].
Refresh [LSC+15]. Regular [CQX18, Wat12, WR15]. regular-expression [WR15].
Regulating [DFJ+10]. regulatory [BP10]. regulatory-compliant [BP10].
Rekeying-Aware [QLL17]. Related [AH19, Cil11, CMA14, DGIS12, HLG18, Pud12, WLC12, GMDR19, MN12].
Related-Key [CMA14, HLG18, Pud12, WLC12, DGIS12]. Relational [HPC10, RP12, WP17, BFG+14, BL11, Ga11, JK13, PFY10]. Relations [BP11, FHS13, HLR11, WGD18, KGO10, LLM+19]. Release [KFSI12, RSBGN12, Unr15, WSS12].
Relevance [Sim15a]. Reliability [HSUS11, Cz14]. Reliable [AMKA17, ADG16, BAI10, CC14, KMJ18, MGJ19, MKASJ18, WBK16, ACD+15, CL16, ZC12].
Repositories [Ano15a]. repository [RSM15]. Representation [AGW15, BFMT16, MHT+13]. Representation-Based [AGW15].
Representatives [Bla16]. reproducible [CW12a]. Reproducing [Söd13].
Repudiation [LLG15, VBC+15]. Repurposing [GY13]. Reputation [BL15, LHM+15, PAS13b, MP10].
Reputation-Based [PAS13b]. Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13]. Requirements [OS16]. Requires [Raz19]. requiring [KHHH14].
ReSC [YFT18]. Rescue [TSH17]. Research [BA18, CDFZ16, SPG+19, WP15, BEB+18, GLIC10, Hof16, Pal15, Ven14].
Researchers [Con12, Edw14, Wal18, Win17]. reset [RY10]. Resettable [CPS16]. Resettably [COP+14]. Resettably-Sound [COP+14].
Resilience [CATB19, NTY12, GLL+18]. Resiliency [YM16]. Resilient [AV12, BKKV10, FPS12, HD19, LTZY16, LD13, Nyr+14, Pan14, PSL15, XZY+12, YZ12, YNR12b, YCYZ12, ZYT13, ZWTM15, ZVM17, ZY+19, Zy17a, ZYM18, ZY19+19, CAM19, CQX18, DLZ16a, GV14a, KPS10, LLG19, MMSD13, SPG+17, Wan18, YSLJ14, YKC+12, YLZ+16, ZY17b]. Resistance [CGCS12, GZSW19, RCR12, WLZL12, ZJ11, DLN13, FIO15, XXHL19]. Resistant [BK12a, CDK+10, GV14a, HF14b, SSRM18, WHZ12, WgMW12, WH17, YPRL17, GMRT+15, HCC10, PBC14, VCK+12, WTT12, YKGK13]. resisting [SXL16, Tan15]. Resistive [DSB16, TLCF16]. Resolution [LHW18]. Resource [CSH+18, HM19, JMG+16, JWNS19, SZMK13, YNR12a, ZSH+19].
AMHJ10, FQZF18, KAS15, LLZ+16, MHV15, Wan13, XZW16, ZPZ+16.

Resource-Constrained
[CSH+18, YNR12a, LLZ+16].

Resource-efficiency [SZMK13, XZW16].

Respect [CATB19]. Respiratory
[RSCX18]. Response
[GSH14, HLKL15, ZHW+16, MRRT17].

Resprinting [TCBC15]. REST [LNG19].

REST-Security [LNG19]. restoration
[WHZ12]. restricted [CLH+16]. result
[ACK+10, ED17]. Results
[DGIS12, LJF16, Hof16, KGO10].

Rethinking [Che13, HU15, LSG16, MV16a].

Retrieve [BBB+16a, BTTHJ12, CJP12, DS19, HK14, JMG+16, JKeY12, Yek10, ZZX+11, CJP15, SWW+17]. Retrieving
[Uto13]. returned [War11]. reusable
[RS17]. Reuse [ABF12]. Reveal [Sta13].

Revealed [Ano15d]. Revealing
[BT12, KK12, BK19, KK13]. reverse
[TQL+14]. reversed [KYH18].

Reversibility [FSX12b, 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, YJ12, Ayu12, Bail12, Bar12, Cou12, Dew11, Ful10, Gas13, Gre19a, Gre19b, Jol10, Kat13, Ke15, Kob10, Led16, Lop15b, Low12, Mei10, Moz15, Mur10, Nag19, PMG+19b, Sch15a, Sha10, Ter11, Xie12, IAA+19, JAS+11, MM12, TPDK12]. Reviewed
[Sch15a]. Reviews [SR14].

Revised [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. Revising [BT12].

Revision [LT14b]. Revisited
[Cly14, DKPW12, DKS12, GWCC15, KFS12, LL11, Lop15a, PKTK12, Sar12, Tan12a, BCL14, DGMT19, HKT11, HYWS11, TS16a, ZCL+12]. Revisiting
[RSD19, TLW12, WSA15]. Revocability
[WHLH16]. Revocable
[AEHS15, CD16, QQZ18, SE14, SE16, SZS14, SZDL14, TCL15, TT12, Unr15, FLL+14, LDZ19, WLFX17, WTT12]. Revocation
[AEHS15, LLC+15, LW16, Lop15b, RDZ+16, XMLC13, YWZ+12, ATK11, LKW18, WLWG11]. Revoking [TAKS10].

Revolutionized [Orm16]. RFID
[CJP15, AATM18, BL12, BSSV12, BM11, CGGPDG12, CCF17, CJP12, Cho14, DZS+12, FLL+14, Far14, FMTR12, GSMW14, GH12, GSN+16, GH15, GAI+18, HSH11, HDPC13, HQY+16, HCPLSB12, HCTET+12, JZ18, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLSvdLE10, QZL+16a, QZL+16b, SBS+12, SPLHCB14, SBS18, TG17, WH17, WCFW18, YFT18].

RFID-Enabled
[YFT18, QZL+16a, QZL+16b]. RFID-WSN
[SLY18]. RFID/NFC [Mic16]. RFID
[KOP12]. RGB [SNM14, ST16]. RI
[Sch15a]. Rich [CS12, GYW+19]. Richman
[Xie12]. Riddle [Fox13, KM15, KM16]. ride
[GBC19]. ride-sharing [GBC19]. Right
[Bro17, SR12a, BBG+17, LHA+12, Sch11].

Rightful [RR11]. Rights [LVRY10].

Rigorous [DK17]. Ring
[GHPS12, HKL+12, XY18, YKBS10, YLA+13, JZ14, DZ14, Hwa11]. Ring-LPN
[HKL+12]. Ring-LWE [XY18]. Rings
[YMW16]. RISC [ZBPBF18]. rise
[Ano14, Mat19, Yaa19]. Risk
[Zhao15b, GBC19, NML19, PAK15, SK18]. risk-based
[GBC19, SK18]. risk-oriented
[NML19]. risks [Lan10, SS17a]. RKA
[Sly+16]. RKA-Secure [Sly+16].

RLCPs [DDS12]. RLCWE [XJ+14]. RNG
[CGH17]. RNGs [DSSD14]. RNS
[CATB19, GL19]. RNTS [PSOMPL13].

roaming [SCK10, ZX11]. Robbery
[N.SP+18, AASSA18]. Robotic
[SPW+16, VOB18]. Robust
[BCGAP12, BCG12a, CFOR12, GKS17, GKS17].
HZC⁺12, JSZS12, LSL12b, LSR13, MR16, 
MU12, MS16, MC11, pNyWY⁺14, 
OCGD11, RR11, RMG18, SJ12, SS17b, 
SC12, SZZT18, TLCF16, TK14, TTL10, 
WLSB11, WgMdz112, gWpNy⁺14, 
XNG⁺14, YWNW15, YHSW19, YYO15, 
ZWZ17b, AP10, AIA⁺18, BWRz12b, 
CLM⁺12, EAA⁺16, GZH12, HZC⁺14, 
HZL18, IOV⁺18, KMG17, KI19H, LN⁺18a, 
LW10, LZZ19b, PKS18, RS17, yWpNyL11, 
yWpWyN13, WHZ⁺19, YSL⁺10, 
ZH11H⁺19. Robustness

[HGT15, YKBS10, AE17]. ROCA
[Ano17t]. Rochefort [Car11]. Rock [Cri16].

Rock-solid [Cri16]. Rodney [DDS12].

Rogozin [Kuz11]. Role

[GB19, PH12b, ZVG16, HPJ⁺19, ZVH14].

Role-Based [ZVG16, ZVH14]. Ron

[LHA⁺12]. Room [Sni11b, Pea11]. Root

[ARH14]. ROP [ZHS⁺19]. Rosen [HR13].

Rosenhain [CDSL14]. Rotation

[SB18, LWL11]. Rotational

[KN10, KNR10]. Roulette [Ber17]. Round

[Ber17, jCPB⁺12, COP⁺14, DWWZ12, 
GGLH14, KOTY17, KMO14, LWZ12, LJ17, 
Pan14, TYM⁺17, XZLW15, Yon12, AY14b, 
ABM⁺12, Blo15, LP11, LFW⁺16, Sun11, 
TSL11, TQL⁺14, TCS14, XW12].

Round-Reduced [DWWZ12]. Rounds

[GST12, Sas12, LYHH14, MNP12]. Router

[Bis17, JLZ18, SA15]. Routing [ARWK19, 
Ham12, KZG10, WLY⁺15, LSG16, LC17].

Routing-Aware [ARWK19]. RSA

[Dun12b, KIA11, Pie10, APPV15, BBBP13, 
Bro17, BNS17, CCL⁺19, CLSW12, Chn10, 
GM13, GST13, Her11b, Hin10, HLYS14, IK15, 
KHH11H, KFL⁺10, Lim11, LFK19, MV19, 
Moo12, SM10a, SM10b, SL10, TM10, TK19, 
Win17, YHK⁺10, XYA⁺16]. RSA-1024

[Bro17, Win17]. RSEL [FLL⁺14]. RST

[LD13]. rubber [BSR⁺14]. Rule

[KPW13, NC12, TW12, McG11, YWYZ12].

Rule-Based [TW12]. rules [PTRV18].

Rumor [FKOV15]. Run [CEL⁺19, IF16].

Run-Time [IF16]. RunStream [KPC⁺16].

Runtime [BJ10a, CLP⁺13b]. Rupture

[KA18]. Russian [McG11]. Ryoan

[HZX⁺18].
[DK16a, LJP17, MV16b]. Schema [AN12].

**Scheme** [ADM19, AMSP19, ASS15, Bai10, BHG12, BS14, BKPJ12, BDH11, CMLS15, CLL16, CCW10, CLHC12, CHW12, CCZ13, CCC19, CGY13, CLH13, CSW12, DA10, DS11, DKS12, EAAA19, FR16, FGM10, GZZ13, GH11b, GJZ17, GLW12, GZH17, HYS11, HIFG15, HMR12, HLC18, HHP17, Höl13, HLH19, HP12, IL15, JSZ12, JLX19, KU14, KPI2, KTT12, KKA15, KSS12, KLM12, LSL12b, LHF12, LTH15, LTZY16, LHC11c, LGWY12, LTC15b, LYY18, LGPR14, MWZ12, MVVR12, MRL18, MMN12, MSas12, NNX13, NLLJ12, NLY15, Pei12, PDT12, RVH16, RSD19, RMG18, SK12a, SJ12, SG12, SD12, She14, ST16, SWF19, SP15b, SJW17, SSA13, Tan11, TTD13, TWZ11, WY10, WgMdZ12, WgMW12, gWpN14, WH15, XWS16, XHC12, XJW13, YM16, Yam12, YZ13, Ye10, Ye14, YTH17, YL17, Y17, YHK10, YWMS11, ZPM15, ZZQ19, ZC13, ZQQ15, ZWX17b, ZLDD12, ZY17a].

**scheme** [AMN18, ARL13, AHS14, APK18, AKK17, BD18, BDM19, BOB13, BAL10, BWR12b, BMM12, BBB16b, CLLL11, CLSW12, CH10, CT11a, CLHJ13, CW14a, CTHP13, Cho14, DCS12, EAA16, EZ15, FLL14, Far14, FA14a, FHZ18, FZZ12, GH12, GJ13, GMRT15, GJ18, GPLZ13, GLM16, GH16, GAI18, GBC19, GTSS19, HZWZ18, HBBRM16, HL12, HL11, HCC11, HLC16, HCC10, Hwa11, IB11, JNH17, JKAU19, JLT12, JZS10, JMW16, K11, KPP16, KDH15, KKH13, KHM13, KKM14, KKG14, Kim16, KHI19, KP18, KL16, KDW17, KHW16, KL11, LLY12, LZ16, LS13, LH10c, LZJX10, LNM11, LMCJ11, LK12, LLHS12, LNLK13, LDK17, LNK18a, LWK18, LNK18b, LWK19, LFWS15, LH13, LHH11, LWL10a, LWLW11, LW13b, LZC14, LZZ19b, LDZW19, LL16a, LL16b, LWY12, MCN18, MMS17c, MK12a, MSas13, NR17, Nos14, NMX15, OSN19, PZBF18, QMC17, QMW17, RPS10, SGSC16].

**scheme** [SM11, SYWX19, SCR19, SMS16, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWYZ11, WWY11, wWpNYL11, WHL13, WDZL13, WLZ16, WLFX17, Wan18, WHZ19, WDKV19, WZ11, WKH11, WOLS12, WXK17, XHI12, XZW16, XWC14, XXX15, XTZ19, XXX19, XMHD13, YWJ19, YC11, YCC16, YHMM18, YWK10a, YCT15, YXD18, YQQL17, YMSH10, ZYL10, ZLY10, ZXJ14, ZYC17, ZPYV12, ZHH17, ZY17b, ZFZ18, ZLY19, ZC12, ZBR11, DT13, LL12].

**Schemes** [AAUC18, ABF12, BVS13, BFM12, BBEP14, BS15, CMLRHS13, CLND19, CGL12, Chu16, Des10b, FHKP17, FLL12, HSM14, HLLG18, HPO15, LVL10b, LZCK14, MLCHI0, MR14b, MMS17b, MBF18, MKRM10, MAJAS18, Oba11, PB12, PDN15, PH12b, Sch10, Shi11, SK17, SSU12, VSR12, WGF16, YNR12a, YNR12b, Yek10, YWZ12, AGHP14, AN15, AHI12, BKR19, CDGC12, CXX19, CHS11, CGG10, CTL13, DDD14, D13, DZ14, FPBG14, FGMP12, FMA18, HKA19, HWD16, HM10, KTUU16, LYH12, MM12, MA17, NTL15, QXYW16, SES16, Sar10a, Sar11, hHZ15, SAR18b, WW14, WZZW20, Y11b, ZCL12, ZC14, ZT14].

**Schneider** [Sev16].

**Scholarship** [SPG19].

**Scholarship-for-Service** [SPG19].

**Science** [Bow11, Gas13, IEE10, IEE11b, Ter11, Bia12, PHWM10, Pet11].

**scientists** [Goo12].

**Scientometric** [Pal15, Pal16].

**Scope** [Bai12].

**Score** [GCSADD11, HW19].

**scoring** [OSSK16].

**Scrambling** [LL17a].

**Screen** [SPW16, CTL12, IAA19].

**Script** [Rao10, Bax4].

**Scripting** [DSSB15].

**scroll** [GMOGCC15].

**SDB** [HWK+15].

**SDDO** [PL16].

**SDDO-based** [PL16].

**SDH** [GMS11].

**SDVIP** [YNX16].

**SDN**
[KCC17, YHSW19]. **SDN-Based** [YHSW19]. **SDVSN** [Wan10]. **SE** [LLLS13]. **SE-AKA** [LLLS13]. **seals** [MN10]. **Seam** [LC15]. **Seam-Carved** [LC15]. **Search** [AHN+18, CWL+14, Che15, DCA18, FRS+16, GTT+11, HWZP+18, HCDM12, HLH19, LSQJ+18, SOR16, TMC15, WDCL18, WW12, XWSW16, XJWW13, ZXYL16, BTW15, BL11, CLH+16, FH13, FSGW12, GZS+18, HKA19, HH16, MRR+18, OSK16, PWS19a, SY15b, WHY+12, WXYL16, WS19, XWY+18, XZ+19, XLC+19, YXD18, YQOL17, ZZ11]. **Searchable** [BHJP14, CWWL12, CLW16, CGKO11, FJHHJ12, HKA19, PBC+17, FCY+17, XNKG15, ZZQ+19, CLC+19, DLZ16a, DRD11, HQZH14, HTC17, JCHS16, LZZ17, LLL+18, RPSL10, WXYL16, WCC18, YZCT17]. **Searches** [Sia12, WR15]. **searching** [GPN+12]. **Seattle** [LCK11, KCR11]. **Seberry** [AHS14]. **SEC** [PA10]. **Second** [AKY13, ABM+12, Gre19b, LGP19, SNG+17]. **Secondary** [RS11]. **Secrecy** [ABD+15, BKST18, BCN19, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCW15, TCS14]. **Secrecy-preserving** [TSH14]. **Secret** [ASN11, ASN12, ADH17, Ayu12, Bai10, BB+16a, BFM12, BBP14, BCN19, Bri11, BLU+15, CCM+15, CFOR12, CCL+13, DR12, Dew11, EM12, EA11, FHKP17, FR16, Fok12, HYS11, HL10a, Has16, HZ+18, JLS12, KU14, KS18b, KOTY17, KK12, KK13, KSSY12, KS15, LHF12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Oba11, PCPK14, QS18, SLL10, SC10, SS10c, SSU12, Sti15, TLW12, TWZ11, WKB16, WGF16, Wli18, XZY+12, XJR+17, YFF12, YWZ+12, ZCL+13, Ak11, AIM+19, ADG16, AKK+17, Ara13, BJ16, BEB+18, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DDI13, EEA13z, EZ15, FHH10a, GEAHR11, GJMP15, GLW13, HF14a, HH15, Hea15, HBBRNM+16, HCCC11, HLC12, KI11, KTUI16, LXLY12, LH11a, LT13, LyWSZ10, LHYZ12, LEW19, Mas17, McK10, McK11, McK12, MBB11, OO10, Par18, Pea11, Pet11]. **secret** [QD16, Rus15, SB17, SA12, SAR18b, SM10c, TQL+14, TD14, UUN11, UUN13, WYL13, WZ12, WOLS12, Wu17, XW13, YC11, YSC16, ZCL+12, ZZ15, ZPYW12, LSC+15, Bia12]. **secret-key** [QD16, Rus15, SB17, SA12, SAR18b, SM10c, TQL+14, TD14, UUN11, UUN13, WYL13, WZ12, WOLS12, Wu17, XW13, YC11, YSC16, ZCL+12, ZZ15, ZPYW12, LSC+15, Bia12]. **Secret-Sharing** [BBEPT14]. **Secretion** [RSCX18]. **Secretocracy** [Ber16b]. **Secrets** [BT12, CG14b, DLWW11, FMS12a, Kob10, Man13, Bha16, Cop10b, GGH+16b, HSM14, HLLG18, Har16, HL10b, HP14, HTZR12, HMCK12, HLC+18, HYS18, HK14, HLH19, IL15, Jac16, JKA+18, JHW+19, KW14, KME+12, KHN+11, KHEV+18, Kup15, KH10, LJS+14, LL15, LH12, LYZ+13, LTH+15, LTZ16, LSL15, LSL19, LLGJ16, LSQ18, LY15, LHL15, LML12, LSC12, MLO17, MMP14, MDHM18, Mal13, MVVR12, MMS17b, MGJ19, MK12a, MKAA17, NBZP17, NDG+17, NR12, NMS14, NMS14, PB12, PSM17, Per13, PBC+17, PRN+19, QZL+16b]. **Secure** [QZDJ16, QZZ18, RC18, RM10, RR17, Rea16, RMZW19, RSGG15, SAM+19, SNJ11, ST19, SZS14, SVCV15, SP15b, SKH17, SS15, SRAA17, SAR18b, SSAF11, SVG16, SY17, SYC+17, SM14, SZDL14, SGH15, SLY+16, SR12b, SM18, TB18,
Server-Aided
[GMSV14, MV19, LYL15, SSAF11].
Server-Designation
[Che15, LSQL18].
Server-Side
[BCO13]. Servers
[HWZP18, DRD11, WLWG11]. Service
[BKKB14, CCS14, GGK18, GKG19, Hay13, LDB+15, LBR12, MJW+18, NRZQ15, RSGG15, SPG+19, SPPC12, Sti15, VS16, VFFHF19, AaBT16, HK17, KPP16, LHL+18, LW13a, MMP19, MLM16, Par12b, SVY19, Wu17, YWK10b, ZX11, YCM+13].
Services
[BKBK14, CCS14, GKG19, Hay13, LDB+15, LBR12, MJW+18, NRZQ15, RSGG15, SPG+19, SPPC12, Sti15, VS16, VFFHF19, AaBT16, HK17, KPP16, LHL+18, LW13a, MMP19, MLM16, Par12b, SVY19, Wu17, YWK10b, ZX11, YCM+13].
Session-Based
[LDB+15].
Session-Based
[LDB+15].
Set
[Cor14b, EKP+13, YZ12, Con12, GR19, TMK11].
set-valued
[TMK11].
Sets
[GL19, SPK17, SF12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
Settings
[GA19, GZ12].
Setup
[SOR16, Jia16].
Sessions
[GA19, GZ12].
}.
DZS\(^{+18}\), DMWS\(^{12}\), DKMR\(^{15}\), EWS\(^{14}\), GZSWI\(^{19}\), GWM\(^{16}\), GPT\(^{14}\), KOP\(^{12}\), LFK\(^{19}\), NDC\(^{+13}\), PRC\(^{12}\), SG\(^{15}\), SR\(^{12a}\), Vua\(^{10}\), YL\(^{17}\), ZBPFI\(^{18}\), VBIB\(^{12}\), CAM\(^{19}\), DJL\(^{+12}\), GSAV\(^{18}\), MCL\(^{+19}\), MFH\(^{13}\]. **Side-Channel** [Bul\(^{18}\), CBL\(^{13}\), CATB\(^{19}\), DZS\(^{+18}\), EWS\(^{14}\), GWM\(^{16}\), GPT\(^{14}\), KOP\(^{12}\), NDC\(^{+13}\), PRC\(^{12}\), SG\(^{15}\), YL\(^{17}\), ZBPFI\(^{18}\), DMWS\(^{12}\), GZSWI\(^{19}\), LFK\(^{19}\), VBIB\(^{12}\), GSAV\(^{18}\), MFH\(^{13}\)]. **Side** [HP\(^{14}\)]. **Sign** [ACC\(^{+13}\), LL\(^{15}\), MEFO\(^{12}\), SPM\(^{+13}\)]. **Sign-On** [ACC\(^{+13}\), LL\(^{15}\), MEFO\(^{12}\), SPM\(^{+13}\)]. **Signal** [Kar\(^{12}\), BLL\(^{+19}\), MS\(^{13b}\), RITF\(^{+11}\)]. **Signals** [Fyo\(^{19}\), LJK\(^{17}\), XNRG\(^{15}\), AIA\(^{+18}\)]. **Signature** [Ano\(^{13a}\), ABF\(^{12}\), ASS\(^{15}\), AEHS\(^{15}\), BHG\(^{12}\), BDH\(^{11}\), CLND\(^{19}\), CGY\(^{+13}\), FGM\(^{10}\), FR\(^{15}\), GJJ\(^{15}\), GJZ\(^{17}\), GMSV\(^{14}\), HZX\(^{+15}\), HPT\(^{+15}\), HHP\(^{17}\), Hü\(^{13}\), JLI\(^{6}\), LTH\(^{+15}\), LGPRH\(^{14}\), MM\(^{12}\), NXB\(^{13}\), PH\(^{12b}\), ST\(^{16}\), TTH\(^{15}\), WZXL\(^{12}\), WLH\(^{15}\), WYL\(^{16}\), XG\(^{14}\), Y\(^{+17}\), YHK\(^{+10}\), YL\(^{+13}\), ZJ\(^{14}\), ZLY\(^{10}\)]. **signature-based** [DLN\(^{13}\), QMW\(^{17}\)]. **Signcryption** [CMA\(^{14}\), DZY\(^{10}\), FZT\(^{13}\), FZT\(^{14}\), ILI\(^{5}\), LSL\(^{12a}\), Rao\(^{17}\), RSD\(^{19}\), RMZ\(^{19}\), XQL\(^{11}\), ZYD\(^{10}\), EZ\(^{15}\), HPY\(^{10}\), HS\(^{11}\), KL\(^{11}\), LK\(^{12}\), LZT\(^{12}\), LKAT\(^{12}\), YMSH\(^{10}\), LHM\(^{15}\)]. **Signed** [KWH\(^{16}\)]. **Signer** [Hwa\(^{11}\)]. **Significantly** [CBL\(^{10}\)]. **Signing** [YAM\(^{+15}\), JC\(^{13}\)].
smartwatches [NM18], smashed [Fag17].

Smart [Ano16g], Smooth [XYXYX11, YC11, ZBR11]. SMS [KRM*10, LH11a, PsDo*13, PCK19, RVS*18]. SMS-Crypto [PsDo*13]. SMSes [SNG*17]. Snake [BBDP16], Snakes [PC16]. SNOW [PC16]. Snowden [Tox14]. SNUSE [DEL19]. SoC [HZS*19, GSC17]. Social [BPSD17, GB19, KTA12, NSA15, NRZQ15, PYM*15, Rog16, SKGY14, SZZT18, VKK*19, WLY*15, WZCH19, ZW15, Zha15b, ZHL15, BDK11, HYF18, LCM*17, LZC17, MSM*18b, SNG*17, SSK*18, Sml15a, YZL*18, vdWEG18]. Society [Sch15a, Sch12b] [NS12]. Socio-Rational [NS12]. SoD [VN16]. Soft [Her19, Jin10, TLCF16, SS17a]. Soft-Error [TLCF16]. Softw [WZM12a]. Software [Bar15, Bee17, EWS14, GZSW19, KYEVE*18, LRVW14, MRL*18, MV16a, Seo18, SAM*18, YGD*17, ZPM*15, AGHP14, ABF*14, CHF*13, DK17, Eve16, GGH*16b, GJJ*12, HLV10, KHF10, LBOX12, SF12, YWT*12]. Software-Defined [KYEVE*18, SAM*18].

Solar [CGB*10]. solid [Cri16]. Solution [Fra15, GSFPT16, HLKLI5, Kam13, NA10b, YFT17, YFT18, Cor14a, MDHM18, SVG14, SAM*19]. Solutions [Ano19c, BCHLI19, LLGJ16, BLV17, KAS15, MPP19, OMPSPL*19, WW14]. Solved [IBM13a]. Solving [Ano17c, BB10, Hod19, Bul10a]. Some [AD12, Ber12, Dur15, LVL10b, Mid10].

spongy [RS14]. Spoof [SP15a]. spotty [OS11]. Spread [HGT15, KD12a, PSJ13, TZM13, XNRG15, XNP18, LWY12, MMSD13].


Mac14, Mun17, Pea11, Pet11]. **Strand** [SH15]. **Strange** [Acz11, Gre17].

**Strangeness** [Ber12]. **Strategic** [Sch12c].

**Strategies** [DSSDW14, TJZF12, YCM+13, AZF+12, DRN16, WWW17]. **Strategy** [LH12, NRZQ15, FLZ+12].

**Stratix** [SMOP15, SMOP15].

**Stream** [ABS+12, BMS12, CMLS15, DM18, DGFH18, DG12, DGIS12, DJG+15, GKS17, GCS+13, HZ11, Hey17, IOM12, KE19, KPC+16, Kla10, MD12b, MHC12, MS12b, NN12, PNRC17, WH18, WHN+12, ZH15, Die12, KM10a, LW13b, MRT10, OCDG11, QGGL13, RS14].

**StreamCiphers** [ERRMG15].

**Streaming** [ZSA12, Cri16, XWZ+18, ZC12].

**Streams** [PCDG14, PWS+19b, HM10, PYP10].

**Street** [Gli12, KGP12].

**Street-Level** [Gli12, KGP12].

**Strength** [DM15, FHV16, Spa16].

**Strengthen** [BL12].

**Strengths** [XNP+18].

**Stribog** [AY14b].

**strikes** [Ran10].

**string** [FHV16].

**Strings** [SKE+18].

**Strong** [ADD10, KFOS12, PYM+15, SA19, SAA12b, Yon12, GH15, GH16, HYWS11, NCL13, OYHSB14, SVY19, WLZ+16].

**StrongBox** [DGFLH18].

**Stronger** [Boy16, MvO11, RK11].

**Strongly** [DDM17, HHP17, KW14, YS12].

**Structural** [LY+18, BDK11].

**Structure** [IP12, LMMH14, LJ15, LLG19, MKRM10, WYCF14, WJ19, JKA+18, LXLY12, ZLW+12, ZPYW12].

**Structure-Independent** [MKRM10].

**Structure-preserving** [LLG19].

**Structured** [PMZ12].

**Structures** [GTT11, HHH+13, LHKR10, PL15, PB12, TSB18, DDFR18, MKHS14, Slv15, WS12, XWZ+18, ZZ15].

**STT** [VDB+16].

**Students** [PP10a, SPG+19].

**Studies** [Uto13].

**Study** [AIF+19, Ano17c, DDR+16, MZLS18, SY15a, SPG+19, STC11, CCG10, EBFK13, KD18, MVH15, SS17a, VGN14].

**Stuxnet** [BPBF12, Zet14].

**Style** [GHPS12, GHPS13].

**Stylistic** [GA19].

**stylometry** [BAG12].

**sub** [GPLZ13].

**sub-passwords** [GPLZ13].

**Subcommittee** [Bla16].

**Subgroup** [CCL+19].

**subliminal** [LWZG10].

**submarines** [McG11].

**Subrecursive** [BBD19].

**Subscribe** [BG17, DLZ+16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

**Subset** [BS14, RP12, ZZ11].

**subspaces** [ZWM14].

**Substitution** [DA10, SGFCRM+18, FVK17].

**substitution-transposition** [FVK17].

**Substring** [MRR+18, SOR16].

**substructure** [MRT10].

**Succinct** [BCI+13, CKLM13].

**sufficient** [TD14].

**suitable** [Jeo13, SKB+17].

**Suit** [MTM18, NAACL12].

**Sumo** [BS12].

**Sums** [SS12b].

**sun** [Cer15].

**super** [BCND19, MZ17a].

**super-activation** [BCND19].

**Superpoly** [HIJ+19].

**Supersingular** [Lau17, LNL+19, Y+17].

**Supervised** [CTC+15, HXHP17].

**Supply** [QZL+16a, QZL+16b, YFT17, YSF+18, YFT18].

**Support** [MSI18, ZZQ+19, CZ14, HHAW19, JAS+11, PWW10, PAK15, TTL10, VCK+12, ZMM+10, ZBR11].

**Supporting** [HHWP19, SKH17, JAS+11, PWW10, PAK15, TTL10, VCK+12, ZMM+10, ZBR11].

**Supports** [WR15].

**surfaces** [CDSLY14].

**Surprises** [Bow11].

**Surreptitiously** [SFKR15].

**Surveillance** [BPR14a, BPR14b, GZH17, KLK+19, Lan10, Ano16f, Fei19].

**Survey** [AAUC18, AKB19, ABHC+16, ABB+19b, BGN17, BCTPL16, BHJ14, BJCHA17, CLB19, DM19, GMD19, HPC10, KMY18, KSD+17, LGM+16, MR14b, MSM18a, MSH10, MKK17, NDR+19, NV10, OFMR16, OMNER19, PWS19a, SKH17, SSP19, TRD11, TS16b, VV18, AAZ+16, ABB+14, ADH17, BM13, BGG+13, BEB+18, FMA+18, HKA19, HT13, HAGTdFR13, KJN+16, KAS15, LK10, MMP19, MA17, MA13, MVH15, NR11, PPA18, TZTC16,
Synchronized Synergy [KRB12]. Sybil [dCCSM+12]. Sylvester [SS10b]. Symbolic [BCEO19, Bul18, CRZ19, Wat10].

Symmetric

[BPR11a, BPR11b, BDPS12, CVM14, FPS12, GFBF12, JCHS16, KTT12, Kha10, PR12, PCY+17, TWZ11, YKNS12, BGG+13, CGKO11, DLZ16a, FH13, GMRT+15, Gor10, GCVR17, KA15, LZC17, SKK10, ZCZ+19].

Symmetric-Key [CVM14, KTT12]. symmetrical [RS17]. Symmetry [SG14]. Symposium [ACMI0, ACM11, Aou10, IEE10, IEE11b, IEE13, Wat10, Aou11a]. symptom [YZL+18]. symptom-matching [YZL+18]. Synchronization [BL12, VTY18, WXY+17, yWXY+18, AATM18, XNG+14].

Synchronized


Synergy [KRB12]. Synergy-Based [KRB12]. Synopses [RCBK19]. Synthesis [SKE+18, TCMLN19, RS17]. Syst

[HI518, WZM12a]. System [ADI11, Aou10, BBCL19, BD18, CZLC12a, CZLC14, Cor14b, CRST15, DG15, GOPB12, Har16, HHS+15, HZS+19, IAD10, JN12, JLZ18, JWJ+17, Jiu10, KMP+11, LYY+19, LFX+18, LWH18, Lop12, MLBL12, NSMS14, PSSK19, QL17, RSCX18, SMSK18, SRAA17, SLI11, XZL+19, YX12, YZX+12, YKK18, ZM11, ZP16, ZLDC15, ZV16, AHM+18, BC18, BGG+13, Bul10a, CH11, CTL12, CZ14, CS11, FNWL18, GKK11, GH15, HHBS18, HWW+15, HJM+11, HLYS14, JC13, LLLK10, LLL+17b, LHH+18, Lit14, LTC+15a, LLL+18, LZZX19, MS12a, MNW15, PSOMPL13, SSPL+13, WMX+17, WDJ19, WGG+12, XWX16, XYLM19, YZZ+18, ZCZQ19, ZMM+10, ZML17, ZZZ+18, KKA14, Dew11]. System-Level [BBCL19, JWJ+17]. System-on-Chip [HZS+19]. Systematic [CCG+16, CBL13, PC16, IAA+19].

Systems [AMSPL19, AN12, AB15, Ano19a, BL15, BS13b, BCTPL16, BB10, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HL+10, HK18, KS18a, KLL+19, LMD16, LQY10, LY16, NZ+13, MT17, MR14b, MJS+19, OŚ12, PMG+19b, PRSV17, PH16, QZL+16b, RST15a, RST15b, SBS+12, SBS18, SFKR15, Sev16, SH17, SGC4, SDM+12, STC11, SPP19, TKR14, YN12a, AT10, ATT+10, BGE+18, CFVP16, CFZ+10, CLZ+17, Cla18, dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DEL19, DZS+12, Eis10, EXP12, GMOGCC15, GHD19, GSN+16, GPVCdB12, HZW18, JSDK+16, JHCC14, KSA16, LCL+15, LWK+18, MDHM18, MLMSM12, MG10, MFH13, NLYZ12, QM17, SS10a, SR10, SRB+12, SMS+16, WS14, YSM14, ZGL+18b, ZV1414, Zhu13, MA17, Ano11a]. Systems-on-Chip [KS18a]. Systolic [MDBC12].

Systolic-Array [MDBC12]. SZK [MX13].

T [SJW+17]. T-Chain [SJW+17]. Table [CCL+13, AY14a, LDDAM12]. Tables [PTT16, XHM14]. Tackling [US19]. Tag [NNM10, PPH12, CJP15, SPLHBC14, CJP12]. Tags [MO12, HSH11, HDPC13, HGY+16, LEW19, MK12a, PLVdE10, TG17, WCFW18].


[MN10, NC13, WGM12]. tamper-evident [MN10]. Tamperable [ACM+17].

Tampered [SSA13]. Tampering [CFL14a, QJC+18, SSA17, SGP+17]. TAO
[Sta13]. **Taormina** [Cra12]. **Tap**
[NM18, ADG16]. **Tap-based** [NM18]. **taps**
[GSAV18]. **target**
[APMCR13, HRS16, LSQ15]. **target-driven**
[APMCR13, LSQ15]. **Targeted** [ABJ13].

**Tasks** [Abe12, FKS+13, LJP17, CL16].
**Taxonomy** [AJA16, GAF+15, KMSM15,
HAGT+13, MA17]. **Taylor** [Joh10]. **Te
c[XLC+19]. **Tc-PEDCKS** [XLC+19]. **TCC**
[Cra12, Lin14b, Sah13]. **TEA** [CWP12].

**Teaching** [GSAV18]. **Team**
[LJS+14, P10, Ant14]. **Tear** [Boy16].
**Tear-Free** [Boy16]. **TEASE** [ZBR11].

**Tech** [Ano15e]. **Technical**
[Sir16, TS16b, Wag16, JW14, Suc12].

**Technique** [HEK18, KBL11, ZLDD14,
BBBP13, CPPT18, GCSAddP11, LH11a,
Nam19, SM12, SKS+18, TS16a, ZWS+18].

**Techniques** [Bis17, DA12, GOS12, HPC10,
HL10b, LW12, Mor12, PJ12, VV18, AB10b,
BM13, FGPgp14, Gill0, HT13, KHF10,
LH11b, OO18, VN17, WMX+17, Joh10].

**Technologies** [GB19, Int19, RC18, SJZG19,
JAE10, JAS+11, Lan10, MPP19].

**Technology**
[Ano19c, CGB+10, Fol16, IEE11a, MZLS18,
VFS+19, Wu16, Ham19, IMB17]. **telecare**
[LKW+18, MA17]. **telephone** [GMMJ11].
**telephony** [Clai18, SEKEG14]. **Telepresence**
[NSP+18]. **Television** [DTE17]. **Tell**
[Cer14]. **Template**
[NGAHLQ16, SKV12, ATI+10, GCSAddP11].

**Templates** [DWB12, AHM+18, QLZ19].
**temporal** [JMW+16, MHT+13, XMH13].

**temporal-credential-based**
[JMW+16, XMH13]. **Tenant** [TV15].

**Tensor** [FYD+19]. **Terabit** [LGP19].
**terahertz** [WW13]. **Term**
[SKV12, CFVP16, VBC+15]. **termination**
[SRB+12]. **TERMINator** [MTM18].

**Ternary** [AD11]. **Test**
[CHH+19, HTCC+15, JEA+15, LSSLW16,
MZHY15, SS10b, WH18, WZCH19, HTCC17,
ZCZQ19, ZCL+19, Ano16g]. **Testable**
[RMP10]. **tester** [RPSL10, SY15b]. **Testing**
[BCG19, Cou12, SS12a, AYT+14, GR19].

**Tests** [GLG12, MS12b, SMM18, ZZZ18, CR12,
HAK19, SI2, SWW+17, ZMY17].

**Text-dependent** [GDM16]. **Textbook**
[PP10a]. **Texture** [TSH17]. **textures**
[NSX+18]. **thanks** [CBL10]. **Theft**
[Ber12, Ber17, BTPL+15, ZMY17]. **Their**
[CZL12b, CK18, FVJ19, JS18b, JSK+17,
NR12, CQX18, Ho16, IK15, KI10, Mat19,
Sti11]. **them** [HLV10, JSK+16, Rus15].

**Theological** [SS10c]. **Theorem**
[Lau12, HF14a]. **Theorem-based** [Lau12].

**Theoretic** [AD19, CVM14, MAL10, WSS12, CDGC12,
GLM+19, SD10, SEKE14]. **Theoretical**
[KL13, ZZ15, Gas13]. **Theoretically**
[TWZ11]. **Theories** [ABR12]. **Theory**
[ACM10, ACM11, AUC18, CCM16,
CDFZ16, CDFS10, Cra12, FGM10, FBM12,
FS15, Gre19b, Hes12, LW11a, Lin14b, Nac12,
Per13, PJ12, RZ19, RB15, RST15a,
RST15b, Sah13, SAKM16, Sha10, Wes16,
Yan10, Abe10, AB10b, Bu10b, CF11,
Geo10, LPZJ15, MZ1+13, MG11, YTM+14,
Crai12, Lin14b, Sah13, vDKS11].

**theory-based** [LPZJ15]. **There**
[Cer15, NSP+18, McK10, McK11, SM13].

**Thin** [Ch16, JX+19]. **Thin-client**
[JX+19]. **things** [FQZ18, AAC+16, A19, BCHL19,
Bel18a, CLF+17, GMDR19, Ham19, HZL18,
JKA19, KHRG19, LNK+18b, LGH+17,
NLIJ12, NLY15, PLGMCF18, SB17,
SXH+19, SS19, SYV+19, VWC19, WCCH18,
XLC+19, YCT15, ZDHZ18, ZSY19]. **Third**
[jCPB+12, OSH16, QZL+16b, Sen10, BL10,
ED19, Kup13]. **Third-Party**
[OSH16, QZL+16b]. **Third-Round**
[jCPB+12]. **Thirteen** [AP13]. **Thomas**
[Ge19a]. **thou** [BDK11]. **Threat**
Three-Factor [AMSPL19, CI15a, HX+11, LLY+18, LZ+12b, PC16, SH11, YKNS12, AIB+16, HWB10, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].

Three-Dimensional [LLY+18, LZ+12b].

Three-Factor [AMSPL19, LFX, YLA].

Three-party [HWB10, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].

Three-Dimensional [LLY+18, LZ+12b].

Timed-Ephemerizer [Tan15a].

Timed-Release [KFOS12, Unr15, WSS12].

Timing [BGN17, GV14b, Hay13, LGR14, LFK19, AGH+17, MCL+19, SRB+12].

Tiny [ZOC10].

Titan [PP10b].

Titan-R [PP10b].

TLS [AV18, AP13, BBDL+17, BFCZ12, BJ+14, CFN+14, Dav11].

TLS-based [PP11].

Today [Ber16a, Cia18, Mac12].

Toeplitz [Ye10].

Token [TYK+12, ZM16, IMB17, Jac16, OMPSPL+19].

ten-based [Jac16].

Token-Leakage [ZM16].

tokenisation [Mar10b], tokenless [Wat14a].

Tokens [Muf16, DCAT12, Hu15].

Tokyo [Sah13].

Tolerant [HK14, MKK17, ZM16, JLT+12, WMYR16, XW13].

Tolerating [ZWM14].

Tone [Yam12].

Too [DL15, DSSDW14, Ros11].

Tool [ASM12, DKL15].

Toolbox [AH13, TRD11].

Toolkit [BJL12].

Tools [Abe12, BKBK14, G017, Ste15a, Lan11].

Top [SS12a, SS10c, Sta13, CHX13].

Top-then-revocable [SS10c].

Topics [SCPSN10a, SCPSN10b].

Today [PP11].

Today [PP10b].

Today [PP10b].

Today [PP10b].

Today [PP10b].

Today [PP10b].

Top-Secret [SS10c].

Touch [Alp18].

TouchWB [MWW+18].

Tower [ZAG19].

TPM [GV13, KHN+11].

TQC [vDKS11].

Trace [ABR12, GA19, PS14, AA14, WJJT10].

Traceability [HCETPL+12, WYML16, WHLH16, YFT17, Chi13a, YYS+16].

Traceable [LDZW19, QRW+18].

Traceable-then-revocable [LDZW19].

traceback [LWY12, PJ18, WY13].

traces [MYR13].

Tracing [LYW12, PPS12b, WXL+17, MFI13, PPR+12].

Track [Dun12b, Kia11, Pie10].

Tracking [GZL17, MDMJ17, SNKC18].

Trade [ASBD16, BS14, GPR+19, SR10].

Trade-Offs [ASBD16, BS14, GPR+19, SR10].
[ASBdS16, BS14, GPR+19, SR10]. Tradeoff [WDDW12, MV16b]. Trading [TW12].
Traditional [SSP19]. Traffic
[DRS16, HS18, KAHKB17, VV18, AZH11, FTV+10, PPR+12, Tay19, VS11].
traffic-feature [FTV+10]. Training [HM12]. Trait [LVY10].
transaction [BGAD12]. Transactional [SPK17].
Transactions [DG15, Mic16, Muf16, PAS13b, TV15, DK12, FG19, MLMSMG12].
Transceiver [NBZP17]. Transcript [Gli12]. Transfer
[AMSPL19, DN12, FMTR12, HL10a, LCCJ13, WCL+18]. transferable
[GSX19]. Transform
[AN12, BCPV11, LSL12b, pNyWY+14, OWHS12, SM12, YWNW15, BW13, MO14, NES+14, PC14, TK14, yWpWY+13].
Transcription [CRE12, FJIJ12, NXB13, TFS19, tWmC12, GZHHD12, HQZH14, PGLL10].
transformation [CJXX19, SA14].
transition [CK11]. translation
[CLY18, WSS+19]. transmission
[BCND19, PsD0+13, WQZ+13].
Transmissions [CBO+18]. Transmitter
[KPB17]. Transparency [TJZF12].
Transparency-Orientated [TJZF12].
Transparent
[CCW+10, XTK10, ZHS+19, CRS13].
Transport [RBHP15, TW14].
transportation [SMS+16]. transposition
[FKV17]. Trapped
[BKPW12, CCL+19, CBX19, CWWL12, Mat14, RPSL10, CSZ+11, CW12a].
treatment [YSM14]. Tree
[BS14, CCC19, HSH11, XWZ+18, BW13, BBB16b, CFG+17]. Tree-based [HSH11].
Trees [SB18, BTPLST15]. Trends
[FR12, GCK12, ZMS14, JAE10]. Triangular
[AMVZ12, RR16]. Tricks [GY13]. Trigger
[SS19]. trimmed [TTL10]. TRIMS
[MGP10]. Triple [LW13b, MS12a]. triple-base [MS12a]. Triple-image
[LW13b]. Triplet [JS18b]. triumphant
[McG11]. Trivium [MS12b, SR12a]. TRNGs [YKBS10]. Trojan
[NDC+13].
Trojans [BRPB13]. True
[FRT13, LTKP16, Fag17]. TrueErase
[DMS+16]. Truly [LA10]. Truncated
[KWS+12, WW12]. Trust
[Bar15, BCK17, DCA19, Gli12, GM14, GSFT16, HHBS18, IGR+16, KMSM15, KGP12, PYM+15, PH12b, PAS13b, Rau15, SG12, TMGP13, TV15, WLY+15, Zha15b, BSBG19, CO11, KG010, MLMSMG12, MGP10, Sch12b, YT11a]. Trusted
[AWSS17, EAA12, FPY15, SS15, YCR16, ED19, HTC+10, Kup13, XZLW15, YI17].
Trustworthiness [RXS18]. Trustworthy
[PSM+18, KM10b]. Truth [MJS+19]. TTP
[ATK11]. TTP-free [ATK11]. TTPs
[KGO10, TAKS11]. Tulip [JB11]. Tunnel
tunnels [Cri16]. Tunny [Cop10a]. Turing
[Orn16, Blö12, Car10, CS12, Don14, Hail17, He117, KSU13, LCKBJ12]. Turtle
[WZCC18]. Tutorials [Lin17]. Tutte
[Hai17]. TV [CCSW11]. Tweakable
[CMLRHS13, LST12, MLCH10, MKASJ18, Sar11, Zha12]. tweet [BTW15].
double [BCV12]. twice [BM15]. TWIN
[KDH13, TY16b]. Twins [Bow11].
Twitter [AIP+19]. Two
[Ash14, Brui2, CTL13, DZ14, ED19, GGH14, GLW12, HL10b, HP14, HWB10, KMTG12, KOS16, KU12, LLC11, Lit14, NSMS14, OTD10, YSL+10, YLW13, ZM16, AN15, BD18, CSD18, CHS11, DHW+13, FIO15, GMJ11, HPC12, HUD16, HWB12, JLT+12, JMW+16, Ken11, Li10, MDHM18, MG11, NMX15, OPSPL+19, QYWX16, Rus15, SMI10b, hSZZ15, WW14, Wat14a, YT11b, ZCC15, GHKL11].
two-channel [JLT+12]. Two-Factor
[LLC11, ED19, Lit14, BD18, GMJ11,
Two-Party [Ash14, HL10b, HP14, KOS16, NSMS14, ZM16, FIO15, HPC12, HWB12, ZZC15, GHKL11].

Two-Round [GGHR14].

Two-Server [YLW13, KMTG12, CSD18].

Two-Phase [MD12a].

TWS [OKG12].

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

Type-based [CFL13, SYL13].

Type-Flaw [SH15].

Types [BCEM15].

Typing [CCDD19, SCR19].

U.S. [Maf16].

Ubiquitous [OS16, Par12b].

UESDE [YZ12].

UHF [HQY16, PPH12].

UK [Che11, PFI12, vDKS11, Ano15e].

Ukraine [OGK15 +15].

Ultra [SBS18, AATM18, GW14, TG17, WCFW18].

Ultra-Lightweight [SBS18, AATM18, TG17, WCFW18].

unaided [CAM19].

Unattended [BN14].

unauthorized [MLSMG12].

Unauthorized [CBO18].

Unbounded [LW11c, YZ12].

unbreakable [Bha16].

Uncalibrated [SGT18].

Uncensored [Ald11].

Uncertainty [FHS13, BBGT12].

Unclonable [ANO16e].

Unconditional [Jia14a].

Unconditionally [CFOR12, LHF12, SNJ11].

Unconditionally-Secure [CFOR12].

Unconstrained [GAEHR11].

unrelated [MSM18b].

Uncovering [FMS12a, WBC10].

Undeciphered [Rao10].

Undeniable [BHG12].

Underbelly [Her19].

underfeeding [BBBB13].

underhanded [Cra14].

Understanding [EPAG16, PP10a, WZZW20, Bar12].

Undetectable [CEL19].

Undisturbed [YCL17].

Unexpanded [SA16a].

Unforgeable [HHP17].

Unidirectional [LSC12, DKL16].

Unified [HK17, ZSW12].

Uniform [HZS19, QJC18].

uniformly [YKKL12].

Unilaterally [GRL12].

Unintended [Ess17, SS19].

union [BBDL17, Bud16].

Unique [SSPC12, SOS15].

Unit [PP10b, Sta13, MS13a, MS13b, MS13c].

units [ABDP15].

Universal [ASM12, BKST18, BJL12, NR12, KS19].

Universally [DN12].

Universality [LW16, FNWL18, LFZ17].

University [Ano17b, CGB10, Wes16].

unlike [Goo12].

unlikely [Fag17].

Unlimited [IBM13a].

Unlocking [VS16].

unmanned [XZW16].

unpaired [CLY18].

Unprovably [Pas13a].

unsigncryption [EZ15].

unspoofable [NR11].

unstructured [CML16].

Unsupervised [HWF19].

Until [BWS19].

untold [Mun17, Pea11].

untraceability [KHIH19, YHL16].

untraceable [AIKC18, JMW16].

Untrusted [HZX18, LQY10, MS16, ATKH17, DRD11, MsO11, WS13].

Updatable [LLPY19, LCL17a].

Update [BCE10, KE19, LQY10, FS18, WFLX17].

Updated [BWS19].

updates [VOGB18].

updates [GCSAddP11, LJW18].

Use [CSV15, DFKC17, KOS16, NR12, Sod13, YT12, der10, CZ15b, Die12, EAAAA19, Hof16, KK10, LDC13, MFET13, Mat19, O010, Si11, UK18, SG19].

Used [CGCGPDM12, BM15, MS13b].

useful [dCCSB16].

Usenet [Bel18a].

User [BOP14, BLV17, BKJP12, FLH13, GMDR19, GdM16, GMJ11, Har16, JN12, LLC11, LCL17b, MZH15, MBC15, MDMJ17, OdH12, PHT12, PWVT12, RVH16, SOR16, SZDL14, SPM13, VFFH19, WgMdZ12].
Vein [KLY+12]. Velskii [BBB16].

Ventilated [RSCX18]. Vera [Ayu12].

Verifiability [RST15a, RST15b, VSR12, WWHL12, YMC+17, BRJ+15, Hwa11]. Verifiable [CFE16, CRST15, Fuc11, YCR16, GLM+19, LZY+16, LJW+17, NMP+13, PHGR16, QS18, XWS17, ZZ15].

Verified [BFCZ12, YGS+17]. verifier [DGJN14, HYWS11, WHJ17]. Verify [BCK17, KRH18, SKGY14, SWW+16].

Verifying [AD12, BFK16, GZSW19].


Versus [DDR+16, NNA10, ABB13, Svo14]. Very [BFM12, Jon13]. Via [ADR18, BHKN13, BCI+13, BCG19, BR14, Bu18, CBZR19, CDSL14, CFG+17, CLW16, DM19, GT12, GST13, GVW12, Gre19b, HFW+19, JHWF+19, KKK+18, LT13, LT14b, LEW19, LLKA19, MH14, PV17, PTK14, QZDJ16, RS10, SE16, SSAF11, SKEG14, TBCB15, WSS+19, tWmc12, YWF18, Yon11, ZOC10, ZCQ19, Zin10].

Vichy [Kap11]. Vicious [NN15].

Video [BGAD12, Cla18, Maz13, SS10a, VGL14, ZTW16]. Video-based [BWR12a, DG17, GSB17, JSZS12, OS12, TWZ+12, WLZL12, YE12, YT12, YTF+18, Crl16, LHS12, LK10, MK11, OCDG11, PMG19a, XWZW16]. Videos [GZH17, JSCM17].


Virtualization [CDD13, RC18, QZDJ16]. Virtualization-Based [CDD13, QZDJ16].

Virus [WOLP15]. visibility [FG19].

Visible [Cas10, HWYW14, LZY+12b, PCK19, WZLW13, Lin14a]. vision [BSW12, LWW+10]. Vista [FG19].

Voice [JTZ+16, WBC+10, LFGCCGRP14, TJZF12]. Voice-over-IP [TJZF12]. VoIP [BGAD12, Cla18, Maz13, SS10a, VGL14, ZTW16]. VoIP/IMS [VGL14].


Vulnerability [MKN13, TM12, VKC15, Wal18, Ano17f, DMWS12, MYYR13]. Vulnerable [Ano15d].

vVote [CRST15].

W [Mar10a, Xie12, Hül13]. W-OTS [Hül13].

WA [LCK11]. Wakanaghat [CGB+10].

Walker [Xie12]. Wallets [Ch13b]. Wallis [Wes16].

War [RSD19].

Warbler [MFG16]. Warm [MCL+19].

warriors [Bud16].

Warming [MCL+19]. was [Goo12, HLA+12].

Watching [NSP+18]. Watermark
Watermark-Based [GRRZ18].  
Watermark-Driven [DLMM+18].

Watermarking [BCGAPM12, BF12, BCPV11, BDB14, BCG10, BM15, CG12b, CHHW12, CCZC13, DG17, FK10, FK11, FK12, FK13, FK14, FK15, FK16, FK17, GPL17, HPC10, HEK18, HD19, HGT15, HHMK14, JSZS12, Joh10, JKHeY12, KD12a, LSL12b, LRY18, LP12, LD13, MM17, MR16, NGAuHQ16, NC12, NX17, pNyWyY14, OWHS12, RS16, RP12, RR11, RM18, SAA15, SLGZ12, SS17b, SSA13, TB18, TW12, TC10, WHZ12, WLZ12, WYW13, gWyNyY14, WX17, yWXZ18, tWyC12, XNG14, XNRG15, XNP18, YWN15, YPR17, YKK18, YY10, ZXX11, ZWW17, ZWZ17a, ZWZ17b, AP10, AIA18, AIM19, AMK12, BWR12b, BW13, BWA13, CCLL11, CT11a, CSS13, GZHD12, GA11, HAK19, HK14, HWYW14, HPL19, JK13, KMG17, KPS10, KJN16, KM11, LSR13, LXCM11, LLHS12, LNY14, LWS12, MM13, MM14a, MO14, MK11, NC13, PTK14, PWLL13, PW10, PGL10, PSL18, PC14, PPR12].

watermarking [RS17, SK18, T14, TK14, TTT10, TPWL11, yWyNyL11, Wan13, yWyWyypN13, WZLW13, YWT12, ZZKA17, ZSMS18].

Watermarking-Encryption [SLGZ12].

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

Wavelet [AGW15, LS12b, MR16, Araj13, AMK12, BW13, LXCM11, MO14, yWyNyL11].

Wavelet-Domain [MR16]. wavelets [MMSD13]. Way [CBJX19, CPS16, DSM14, Mat14, HR10, LP11, RK11].

WBAN [KS18b, XXY19]. WBANs [KIH19, OS19]. Weak
世界-class [Goo12]. Worm [WWC+11].
Worst [BIKK14]. would [McG11].
Wrapped [KM15, KM16]. Write
[LLPY19, YNQ15, ZHZ+19].
Write-Efficient [YNQ15]. writing [LT14b].
wrong [LHA+12, UK18]. WSN
[DL12, JLZ18]. WSNs
[ARWK19, ABB19a, YLSZ19, ZYL+10]. Wu
[LLK10]. WW2 [Don14]. Wyner
[ADG16].

X [Sm11a]. X25519 [TV19]. X.998
[An11b]. X.998-2010 [An11b]. XML
[BPP10, CH11, GA11]. XMSS
[BDH11, HRB13, HBG+17]. XOR
[App13, LZZ+19a]. XOR-Based [LZZ+19a].
XTEA [CWP12, IS12]. XTS [Mar10c].
XVIII [Sch15a].

Yamamoto [Car11]. Yan [Cou12]. Yao
[GKS17]. YCbCr [RMG18]. Years
[DR10, BCV12]. Yehuda [Ful10]. Yen
[LLK10]. Young [Söd13]. Yuan [FMS12a].
YubiKey [Jac16]. Yves [Ter11].

Z [JSM+18]. z13 [ACD+15]. Zero
[AMH+16, BW12, CLP13a, COP+14, GJO+13, GOS12, IW14, LLM+19, MX13, MBC+18, MT12, OOR+14, Pan14, SJ12, WCL+18, YCL17, Zet14, AIA+18, KPP16, MDHM18, TLL13, WWBC14].
Zero-Correlation [BW12, YCL17, WWBC14].
Zero-Cost [AMH+16]. Zero-Knowledge
[CLP13a, GOS12, IW14, MX13, MBC+18, MT12, Pan14, LLM+19, KPP16, MDHM18].
Zero-Watermark [SJ12, TLL13]. zero-
watermarking [AIA+18]. Zheng [AHS14].
ZIDS [NSM14]. Zodiac [SDM10]. ZUC
[WH+12].
References


REFERENCES


Acar:2018:SHE

Al-Azzam:2018:SRC

Aghili:2018:ISA

Akhleyelek:2016:SPM

Al-Azzam:2018:SRC

Aghili:2018:ISA

Akhleyelek:2016:SPM
Alizadeh:2016:AMC


Abdalla:2010:PCL


Atallah:2010:ATC


Anand:2015:ICL


Alleaume:2014:UQK

Athmani:2019:EED


Avoine:2019:SDB


Almeida:2013:CCA


Arnold:2012:ICC


Ateniese:2017:LCS

Giuseppe Ateniese, Giuseppe Bianchi, Angelo T. Capossele, Chiara Petrioli, and Dora Spenza. Low-cost standard signatures for energy-harvesting wireless sensor networks. *ACM Transactions on Embedded
Am}brosin:2017:OBB


Adrian:2015:IFS


Agosta:2015:OPP


Abe:2010:ACA


Abe:2012:TBG

Masayuki Abe. Tools over bilinear groups for modular design of cryptographic tasks. Lecture
Arriaga:2012:JSS


Almeida:2014:COS


Ananth:2013:SFP


Avoine:2016:SSP


Aid:2013:DIO

Matthew M. Aid, William Burr, and Thomas R. Johnson, editors. “Disreputable if Not Outright Illegal”: the National Security Agency versus Martin Luther King, Muhammad Ali, Art Buchwald, Frank Church, et al.: Newly Declassified History Di-


Applebaum:2010:PKC


Arias-Cabarcos:2015:BIP


Armando:2013:AFB


Arnold:2015:NGH


Amoah:2016:FMA

Ardagna:2010:ECP


Arias-Cabarcos:2019:SAA


Avoine:2012:PFS


Austrin:2017:ICT


REFERENCES

**Aczel:2011:SWL**


**Alvarez-Cubero:2016:AVL**


**Aizatulin:2012:VCC**


**Anyanwu:2010:DCS**


**Ayday:2012:DAA**


**Aliberti:2016:RPS**

REFERENCES

**Attasena:2017:SSC**

**Abraham:2019:DPL**

**Adikari:2011:HBT**

**Abdalla:2012:LBH**

**Abro:2019:LEE**

**Andrychowicz:2016:SMC**
References

Araldo:2018:CEC


Anandakumar:2018:RHA


Ahmed:2017:IRD


Attrapadung:2015:RGS


Antonopoulos:2017:DIS


Akinyele:2014:MGA

Abdullaziz:2016:AAI


Ahani:2015:SRB


Allender:2019:NIN


Ali:2018:ECM


Akhatar:2018:BSI

Z. Akhtar, A. Hadid, M. S. Nixon, M. Tistarelli,
REFERENCES


Appelbaum:2013:SSG [AHS13]

Ak:2014:ICS [AHS14]

Aiash:2015:FAA [Aia15]

Ali:2018:CBR

Amin:2016:DAP
REFERENCES

Altakrori:2019:AAA


Applebaum:2014:HGA


Amin:2018:UAP


Ali:2019:PRD


Alhanahnah:2016:MTI

Azarderakhsh:2014:NDP


Almulla:2013:CKE


Anada:2017:CGS


Alabdulatif:2017:PPA


Afanasyev:2011:PPN


Armknecht:2012:STH

References

Arfaoui:2019:CAA

Aiash:2015:IAA

AlTawy:2013:SOC

Aldrich:2011:GUS

Au:2018:PPP
REFERENCES

Alomair:2012:AEH


Alpar:2018:BTA


Arnedo-Moreno:2010:JRA


Asharov:2013:FCF


Awad:2016:SSZ


Arsalan:2012:IRW

REFERENCES

Ahir:2017:LAR

Abbasinezhad-Mood:2018:DHI

Adj:2013:WDC

Aumasson:2014:HFB

Ahmadian:2010:PDS

Aghili:2019:LLT
Seyed Farhad Aghili, Hamid Mala, Mohammad Shojaifar, and Pedro Peris-Lopez.

Álvarez:2012:CAB


Albrecht:2012:SDL


Arshad:2015:SAI


Aga:2017:ISM


Anawis:2014:ARR

Mark Anawis. Applications for randomness: Random numbers have been shown to be valuable in sampling, simulations, modeling, data encryption, gambling and even musical composition. Scientific Computing, 31(11):28–30, November 2014. CODEN SCHRCU. ISSN 1930-5753.
REFERENCES

Anderson:2013:MNF
[And13]

Anonymous:2010:NDS
[Ano10]

Anonymous:2011:AXL
[Ano11b]

Anonymous:2011:MCB
[Ano11c]

Anonymous:2012:SHS
[Ano12]

REFERENCES


Anonymous:2013:DSS


Anonymous:2013:NCI


Anonymous:2013:SSD


Anonymous:2013:SIS


Anonymous:2014:ERE


Anonymous:2015:BSU

Anonymous:2015:BRDa


Anonymous:2015:CEB


Anonymous:2015:QCS


Anonymous:2015:UGB


Anonymous:2016:CPSd


Anonymous:2016:CPSe

Anonymous:2016:EMT


Anonymous:2016:FVM


Anonymous:2016:GUP


Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

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

Anonymous:2017:BRM  


Anonymous:2017:CCS  

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

Anonymous:2017:HDQ  


Anonymous:2017:MBH  


Anonymous:2017:RV  

Anonymous:2019:GES


Anonymous:2019:HCC


Anonymous:2019:PBT


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF

AlFardan:2013:LTB

Ali:2018:SUA

Alcaide:2013:AAP

Applebaum:2013:GXG

Applebaum:2014:CCP

Appel:2015:VCP
Andrew W. Appel. Veri-

**Albrecht:2015:FBR**


**Al-Qarni:2012:EII**


**Arai:2013:MDH**


**Adj:2014:SRC**


**Altawy:2018:SLT**

REFERENCES

AlTawy:2018:TCM


Agudo:2013:PAC


Ambrose:2012:RII


Alghamdi:2019:RAM


REFERENCES

http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_16

Ahmadi:2012:SKE


Asaar:2015:IBM


Alsulaiman:2013:IVB


Altman:2010:AAP


Argyropoulos:2010:BTP

Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, Yannis Damousis, Michael G. Strintzis, Martin Braun, and Serge Boverie. Biometric template protection in multimodal authentication systems based on er-

**Au:2011:PPT**


**Al-Tariq:2017:SFP**


Abdou:2018:SLV

Altaf:2015:LPM

Altaf:2017:LHL

Awad:2017:OLO

Anzala-Yamajako:2012:RAC

Ahmad:2014:RTN

AlTawy:2014:IDR
Riham AlTawy and Amr M. Youssef. Integral distinguishers for reduced-round Stribog. *Information Pro-

Aysu:2015:FRT


Ayub:2012:BRB


Apavatjrut:2012:EEA


Alshammari:2011:CET


Alavi:2014:RQE


Barcellos:2018:RSP

M. Barcellos and D. F. Araújo. Research in security and privacy in Brazil. IEEE Security & Privacy,
REFERENCES

16(6):14–21, November/December 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).


[BAL10] Diana Berbecaru, Luca Albertalli, and Antonio Lioy. The ForwardDiff sig scheme for multicast authentica-
REFERENCES

Barbay:2012:BRB


Barthe:2015:HAC


Batey:2010:DMW


Bax:2014:PPD


Bard:2019:DWG

partial-decoding-BAX.pdf. [BBB+16a]


REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal/Conference Details</th>
</tr>
</thead>
</table>
Balfanz:2012:FA


Bugliesi:2015:ART

Bugliesi, Michele; Calzavara, Stefano; Eigner, Fabienne; Maffei, Matteo. Affine refinement types for secure distributed programming. *ACM Transactions on Programming Languages and Systems*, 37(4):11:1-11:??, August 2015. CODEN ATPSDET. ISSN 0164-0925 (print), 1558-4593 (electronic).

Bana:2019:VMC


Buhrman:2014:PBQ


Bahri:2016:CCO


Benedetto:2010:DQE

REFERENCES


REFERENCES


Beunardeau:2016:WBC


Batina:2019:ISI


Bernstein:2014:CKR

Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange. Curve41417: Karatsuba revisited. Report, Department of Computer Science, University of Illinois at Chicago, and Department of Mathematics and Computer Science, Technische Universität Eindhoven, Chicago,


[BCP14a] Marco Botta, Davide Cavagnino, and Victor Pomponiu. Protecting the content integrity of digital imagery with fidelity preser-
REFERENCES

Boyle:2014:EO


Basso:2011:BWC


Bessani:2013:DDS


Blasco:2016:SWB


Biddle:2012:GPL


Barker:2015:RKM

REFERENCES


[JBD11] Johannes Buchmann, Eeik Dahmen, and Andreas Hülsing. XMSS — a practical forward secure sig-


REFERENCES


REFERENCES


REFERENCES


Battistello:2012:TBA


Balagani:2018:IAC


Bossuet:2013:AFS

REFERENCES

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

Boudot:2019:BFD


Barak:2010:IPO


Barbulescu:2013:QPA


Barbulescu:2014:HQP


Barthe:2012:ACA

[Gilles Barthe, Benjamin Grégoire, and César Kunz. Automation in computer-aided cryptography: Proofs, attacks and designs. Lecture Notes in Computer Science, 7679:7–8, 2012. CODEN LNCS919. ISSN
REFERENCES


Biswas:2017:STC


Borcea:2017:PEE


Bhattacharjee:2016:SWC


Blasco:2012:FAS

Jorge Blasco, Julio Cesar Hernandez-Castro, Jos&M#243; Marina de Fuentes, and Benjamín Ramos. A framework for avoiding steganography usage over HTTP. *Journal of Network and Computer...*
References


Joseph Bonneau, Cormac Herley, Paul C. van

**Biagioli:2012:CCS**


**Beimel:2014:CCW**


**Biswas:2017:SAT**


**Bauer:2010:RVC**


**Brumley:2010:CAI**


**Boche:2016:DSK**

H. Boche and G. Janßen. Distillation of secret-key from a class of compound memoryless quan-
REFERENCES


[BK12b] Adil Bouti and Jörg Keller.


**Bhuyan:2014:DDD**


**Braun:2012:ULA**


**Brakerski:2010:OHB**


**Bogdanov:2013:SDS**


**Bogdanov:2012:KAC**

REFERENCES


REFERENCES

??, April 2018. CODEN IFCSEN. ISSN 0129-0541.


[B Bernstein:2017:SCS]
REFERENCES


**Blanchette:2012:BPC**


**Bla12**


**Blaze:2016:UHR**


**BLAN+16**


**Buchmann:2017:PCU**


**Bai:2019:LMD**


**Buchmann:2018:PCP**

REFERENCES


REFERENCES

11:??, May 2011. CODEN ATISBQ. ISSN 1094-9224
(print), 1557-7406 (electronic).

Birajdar:2013:DIF
Gajanan K. Birajdar and Vijay H. Mankar. Digital
image forgery detection using passive tech-
niques: A survey. Digital Investigation, 10(3):

Bard:2015:PRO
Gregory V. Bard and Theodore McDonough.
Plaintext recovery for one-
time pads used twice. ACM
Communications in Com-
puter Algebra, 49(1):17–18,
March 2015. CODEN ????
ISSN 1932-2232 (print),
1932-2240 (electronic).

Bhattacharya:2018:UPC
Subir Bhattacharya and Debdeep Mukhopadhyay.
Utilizing performance coun-
ters for compromising pub-
lic key ciphers. ACM
Transactions on Privacy and Security (TOPS),
21(1):5:1–5:??, January 2018. ISSN 2471-2566
(print), 2471-2574 (elec-
acm.org/citation.cfm?id=3156015.

Benamara:2016:ICA
Oualid Benamara, Fatima
Merazka, and Kamel Betina.
An improvement of a
cryptanalysis algorithm. Information Processing
Letters, 116(2):192–196,
February 2016. CODEN IFPLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0020019015001398.

Baldwin:2010:AFI
Adrian Baldwin, Marco Casassa,
Mont, Yolanta Beres, and Simon Shiu. Assurance for
federated identity manage-
ment. Journal of Com-
puter Security, 18(4):541–
572, 2010. CODEN JCSIET. ISSN 0926-227X
(print), 1875-8924 (elec-
tronic).

Biswas:2012:IBA
Subir Biswas, Jelena Misic,
and Vojislav Misic. An
identity-based authentica-
tion scheme for safety mes-
sages in WAVE-enabled
VANETs. International
Journal of Parallel, Emer-
gent and Distributed Sys-
tems: IJPEDS, 27(6):541–
562, 2012. CODEN ????
ISSN 1744-5760 (print),
1744-5779 (electronic).
REFERENCES


Ben-Othman:2013:IHN


Bohme:2010:ASS


Boneh:2012:PBC


Bailey:2014:UIA


Borghoff:2010:CLC


Bowyer:2011:WSD

Kevin W. Bowyer. What surprises do identical twins have for identity science? Computer, 44(7):100–102, July 2011. CODEN CP-TRB4. ISSN 0018-9162


REFERENCES

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

Bellare:2014:SSEa

Bellare:2014:SSEb

Boneh:2016:BCR

Balsa:2017:TIC

Brakerski:2014:VBB

Brakerski:2013:WHB
Zvika Brakerski. When homomorphism becomes a liability. Lecture Notes in Computer Science, 7785:143–161, 2013. CODEN LNCSD9. ISSN 

[BR14]
REFERENCES


Bag:2017:BBW

[152]


REFERENCES

Bellare:2012:MIS

[152]


Birrell:2013:FIM

[152]


Brumley:2012:SFI

[152]


Bhattacherjee:2014:CAT

[152]

Sanjay Bhattacherjee and Palash Sarkar. Concrete analysis and trade-offs for the (complete tree) layered subset difference broadcast encryption scheme. IEEE
References


Bagheri:2015:NNA


Bala:2019:SAG


Bendiab:2019:FNF


Boojinov:2014:NMC


Basin:2011:AIS

David Basin, Patrick Schaller, and Michael Schläfper. Applied information security: a hands-on approach. Springer-Verlag,
REFERENCES


Beaulieu:2013:SSF


Batina:2012:HEB


Broustis:2012:GAN


Boneh:2012:FEN


Biskup:2012:RBR


[Buc10] Johannes Buchmann. *Einführung in die Kryptographie*. (German) [Introduction to Cryptography]. Springer-Lehrbuch. Springer-Verlag,
REFERENCES


Bhatnagar:2013:SRI


Bhatnagar:2012:NRA


Buhren:2019:IUP


Bao:2010:ISC

Feng Bao, Moti Yung, and Dongdai Lin, ed-


[CBRZ19] Sudipta Chattopadhyay, Moritz Beck, Ahmed Rezine, and Andreas Zeller. Quantifying the information leakage in cache attacks via symbolic execution. *ACM
REFERENCES


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO


Checkoway:2016:SAJ


Chadha:2012:AVE


Chatterjee:2016:TAD

REFERENCES


Chou:2013:UGS


Cao:2019:AML


Chang:2011:SFW


Cascudo:2015:SSN


Chatterjee:2017:PBS


Cho:2014:DGA


Chen:2011:EAA


Chen:2013:WSB


Chen:2010:ALD


Chen:2010:ALD

Chu:2014:KAC


Chen:2012:MWB

REFERENCES


Cremers:2019:SA


Culnane:2019:KKR


Ceruzzi:2014:HFT


Cerf:2015:CTN


Cerf:2018:CSA


Chang-Fong:2016:CSC


Crampton:2017:CEI

[CFG+17] Jason Crampton, Naomi Farley, Gregory Gutin, Mark Jones, and Bertram Poettering. Cryptographic enforcement of information

**Carter:2013:SSA**


**Centenaro:2013:TBA**


**Checkoway:2014:PED**


**Cevallos:2012:USR**


**Carstensen:2011:AAA**


**Calzavara:2017:SWJ**

Stefano Calzavara, Riccardo Focardi, Marco

**Celesti:2016:ALT**


**Cho:2017:EDF**


**Chang:2010:PRN**


**Chen:2010:IFA**


**Camenisch:2012:EAA**


**Che:2012:WAM**

[CG12b] Xiangjiu Che and Zhanheng Gao. Watermark-

**Cheraghchi:2014:NMC**


**Corrigan-Gibbs:2014:KS**


**Chaudhuri:2010:PIC**


**Caballero-Gil:2012:LAR**


**Chmiel:2012:EPC**

REFERENCES

[Coul]:2011:ACO

[Cohn]:2017:PSR

[Curt]:2011:SSE

[Chen]:2012:PAI

[Chand]:2014:PBC

[Xia]:2013:NIB
Chen:2010:NUP


Chang:2011:DEQ


Chan:2013:OCK


Chang:2013:MPQ


Chappell:2013:PMI


Chen:2011:CCI


Cheswick:2013:RP

REFERENCES

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


REFERENCES

Chien:2013:CRC

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

Chien:2016:GAI

Chmielowiec:2010:FPR

Choudary:2010:SCD

Chou:2014:EMA
REFERENCES


Cao:2014:SCI [CJFH14] Yan-Pei Cao, Tao Ju, Zhao Fu, and Shi-Min

**Cho:2012:CBF**


**Cho:2015:CBF**


**Chang:2019:GTS**


**Chandra:2011:AST**


**Chung:2018:ERN**

Heewon Chung and Myung-sun Kim. Encoding of rational numbers and their homomorphic computations for FHE-based applications. *International Journal of Found-
REFERENCES


Calegari:2019:WPH


Chen:2019:BBS


Chen:2011:RSB


Chen:2017:PGF


Comon-Lundh:2010:DSP


Chong:2013:ASG

Chen:2016:RPR


Chen:2012:NCB


Chen:2013:TSE


Chande:2016:NSC


Cao:2012:SRH


Chen:2019:IBS

[Jiahui Chen, Jie Ling, Jiutong Ning, and Jintai Ding. Identity-based signature schemes for multivariate public key cryptosys-

**Canetti:2013:PCC** [CLP13a]

**Castro:2013:RAM** [CLP+13b]

**Chang:2012:PRS** [CLSW12]

**Cui:2016:KAS**

**Chen:2014:CDP**

**Cao:2018:CUP**
GRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

**Cheng:2017:ISK**


**Cremers:2011:OSV**


**Cui:2014:SSA**


**Checkoway:2018:WDL**

Coles:2016:NAU


Cao:2018:EEG


Chakraborty:2013:EHI


Chen:2017:VME


Cao:2016:OMA


Constantin:2012:RSN


Connolly:2018:FE


Copeland:2010:CBG


Copeland:2010:CSB


Chung:2014:RRS


Cordova:2014:EBS


Corthesy:2014:SSD

set-out-decipher-cryptographic-system. The article describes use of thousands of mobile phones to attempt a parallel brute-force attack on elliptic-curve and RSA algorithms, in a research project by Ramasany Gowthami and Arjen Lenstra at the LACAL laboratory at EPFL, Lausanne, Switzerland.

Coutinho:2012:RPT


Claessen:2013:SPN


Canard:2018:NTC


Chung:2016:NBB


Chen:2018:RLF


Chevalier:2010:CSC

[Yannick Chevalier and]

Chen:2012:DCC


Crampton:2011:PEC


Cramer:2012:TCT


Crav:2014:UCC


Clear:2012:CPA


Crichlow:2016:RSE

Ramon Crichlow. Rock-solid encrypted video streaming using SSH tunnels
and the BeagleBone Black. 
dl.acm.org/ft_gateway.cfm?id=2933362&ftid=1715428&
dwn=1&CFID=796895669&CFTOKEN=92668082.


[CSD18] Durbadal Chattaraj, Monalisa Sarma, and Ashok Kumar Das. A new two-server authentication and key agreement protocol for accessing secure cloud services. *Computer Networks (Amsterdam, Netherlands: 1999)*, 131(??):144–164, February 11, 2018. CODEN ????. ISSN 1389-1286 (print), 1872-7069 (elec-
REFERENCES


Chauhan:2018:BBA

Chadwick:2014:AFI

Chen:2013:RWM

Chen:2017:SIE

Ciegis:2016:ADP
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Authors</th>
<th>Journal/CODEN/ISSN</th>
<th>Year</th>
</tr>
</thead>
</table>
REFERENCES


[CVM14] Flavio P. Calmon, Mayank Varia, and Muriel Médard. On information-theoretic metrics for symmetric-


REFERENCES


Chen:2012:IDC


Cao:2019:PPS


Chen:2012:CKS


Chen:2015:TCP

Chen:2014:MLC


Cao:2019:PPS


Chen:2012:CKS


Chen:2015:TCP


Chen:2014:MLC


Chen:2015:TCP


Djebbar:2012:ASB

Darivandpour:2018:ESP

Danezis:2012:FCDb

Davies:2011:IST

Diong:2012:DA

Dou:2018:OHR
Yi Dou, Henry C B Chan, and Man Ho Au. Order-hiding range query over encrypted data without


DeOliveiraNunes:2019:SSC


Desmedt:2010:CF


Desmedt:2010:ES


Dew:2011:BRB


Durmath:2011:DEN

Markus Dürmuth and David Mandell Freeman. Deniable encryption with


[Djuric:2015:FSF] Zoran Djuric and Dragan Gasevic. FEIPS: a secure fair-exchange payment sys-
REFERENCES


[DGP10] Saar Drimer, Tim Gîneysu, and Christof Paar. DSPs, BRAMs, and a pinch of logic: Extended recipes for AES on FPGAs. ACM


REFERENCES

www.sciencedirect.com/science/article/pii/S1353485810701446


REFERENCES


Djaziri-Larbi:2018:WDA


Dong:2013:PRS


Dai:2016:MLR


Duan:2016:SDC


John Demme, Robert Martin, Adam Waksman, and Simha Sethumadhavan. Side-channel vulnerability

David:2012:UCO


Donovan:2014:ATM


Doroz:2015:AFH


Duncan:2012:CAI


Ding:2017:CSM


Das:2016:CWM

REFERENCES


Dziembowski:2018:NMC


Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE

REFERENCES

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


REFERENCES

Das:2016:MPU

Das:2012:DPB

Deng:2018:SFE

Dachman-Soled:2014:COF

Dodis:2014:HEY
Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too — optimal recovery strategies for compromised RNGs. Report, Dept. of Computer Science, New York University; Dept. of Computer Science and Applied Mathematics, Weizmann Institute; Dept. of Computer Science, Northeastern University, New York, NY, USA; Tel Aviv, Israel; Boston, MA, USA, March 3, 2014. 27 pp. URL http://eprint.iacr.org/2014/
REFERENCES


**David:2012:PRE**


**Dorn:2012:ECE**


**Dong:2012:KKD**


**Dong:2012:NDI**


**Dai:2018:OPC**


**Deng:2014:CCC**

Robert H. Deng, Yang Xiang, and Man Ho Au.


Eslami:2011:SIS


Erguler:2012:PAI


Ekberg:2012:AEP


Ehdaie:2016:HCR


Elrabaa:2019:PPP


Egele:2013:ESC

Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel.

[Esiner:2017:QRI]


[Esiner:2019:TFA]


[Edw14]


[Edwards:2017:NSQ]


[El-Emam:2013:NSA]


[Eisenbarth:2012:CIP]

Thomas Eisenbarth, Zheng


REFERENCES


**Farash:2014:ECC**


**Farash:2014:SEI**


**Fahd:2018:CPA**


**Faal:2019:MVE**


**Fagone:2017:WWS**

Mohammad Sabzinejad Farash. Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based
REFERENCES


REFERENCES


[FGMP12] Oriol Farràs, Ignacio Gra-

[FH13]

Faugère:2014:MCA


[FGPGP14]

Fan:2010:AMI


[FHH10a]

Fan:2010:PSN


[FH10b]

Fan:2017:SSP


[FGR+17]


REFERENCES


[Fid18] Bradley Fidler. Cryptography, capitalism, and national security. IEEE An-


[Fei:2012:GTK] Han Fei, Qin Jing, Zhao Huawei, and Hu Jiankun. A general transformation...


References


Feng:2012:CAO


Fallaflahpour:2015:AWB


Ferrag:2018:SCN


Ferretti:2019:FBS


Faust:2014:CNM

REFERENCES


REFERENCES


Feng:2018:ALA


Fiore:2015:EIB


Fathimal:2016:SSS


Frattolillo:2015:WPP


Frattolillo:2016:BFM


Frey:2010:ABC


REFERENCES

SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Fugkeaw:2018:SSA


Fang:2011:ICP


Feng:2011:GD


Fang:2012:CCS


Ferguson:2010:CED


Feng:2011:GDA


Fujioka:2012:SHI

Atsushi Fujioka, Taichi Saito, and Keita Xagawa. Secure hierarchical identity-based identification without random oracles. Lecture Notes in Computer Science, 7483:
REFERENCES


**Fathi-Vajargah:2017:IMC**
Behrouz Fathi-Vajargah and Mohadeshe Kanafchian.

**Fiore:2017:PGP**

**Feng:2013:ECE**

**Fiore:2017:PGP**

**Feng:2013:ECE**

**Fanyang:2012:SAK**

**Fu:2017:DFA**
Feng:2011:VBF


Feng:2019:SHO


Fan:2015:IRD


Fan:2014:NCI


Fu:2012:EHA


Fyodorov:2019:SGM


GomezPardo:2013:ICM

Gross-Amblard:2011:QPW

Grondahl:2019:TAA

Guimaraes:2019:OIQ

Gregio:2015:TTM

Gope:2018:LPP
Prosanta Gope, Ruhul Amin, S. K. Hafizul Islam, Neeraj Kumar, and Vinod Kumar Bhalla.

Galindo:2013:NIC

Gasarch:2013:RBC

Ghosal:2019:RSC

Gupta:2019:DRB
Gorantla:2011:MKC


Guyeux:2015:ECS


Gupta:2012:CDF


Gupta:2013:HPH


Guerra-Casanova:2011:SOT


Granado-Criado:2017:HCH

José M. Granado-Criado and Miguel A. Vega-Rodriguez. Hardware

**Gong:2016:ATI**


**Guerin:2016:TDU**


**Giot:2011:UKD**


**Geller:2013:MIS**


**Gentry:2010:CAF**


**Gentry:2013:EMH**

REFERENCES

10.1007/978-3-642-36594-1_2_7?coverImageUrl=/static/0.8699/sites/link/images/abstract_cover_placeholder.png.

Gaspar:2012:SEF

Gong:2010:PCI

Grigg:2011:CCN

Garg:2016:CIO

Garg:2016:HSS


Craig Gentry and Shai Halevi. Efficient implementation of fully homomorphic encryption. US
REFERENCES


**Gope:2015:RLA**


**Gope:2016:EMA**


**Genge:2019:ESA**


**Gordon:2011:CFS**


**Gentry:2012:RSB**


**Gentry:2013:FSB**

Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart. Field switching in BGV-style homomor-

**Gentry:2012:FHE**


**Gilad:2014:PHI**


**Godor:2012:HBM**


**Gilbert:2010:ACE**

REFERENCES

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

Giry:2015:BCK

Gao:2013:LCA

Gu:2015:EIB

Geetha:2018:OVC

Gravier:2015:WOD

Goyal:2013:CZK
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-36594-2_4/


REFERENCES


Gollmann:2010:SCR


Guo:2011:ED


Gong:2016:HES

Linming Gong, Shundong Li, Qing Mao, Daoshun Wang, and Jiawei Dou. A homomorphic encryption scheme with adaptive
chosen ciphertext security but without random oracle. 


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Authors</th>
<th>Details</th>
</tr>
</thead>
</table>
García-Martínez:2015:HEB


García-Morchón:2015:HCR


Guo:2011:ISS


Guo:2014:SAS


Gao:2014:URA


Groza:2017:LCL

[Bogdan Groza, Stefan Murvay, Anthony Van Herewege, and Ingrid Verbauwhede. LiBrA-CAN: Lightweight broadcast au-
REFERENCES


Groth:2012:NTN


Glowacz:2017:IDW


Gong:2013:NOT


Goodrich:2012:EVW


Genkin:2016:PKE


Gottel:2019:SPE


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.

Green:2019:RMC

Green:2019:RNT

Grimes:2015:CCT

Gibson-Robinson:2012:AAL

Guo:2018:WBS

Gupta:2018:SCA

Guha:2017:RTS
Krishnendu Guha, De-

**[GST12]**

**Guin:2016:FCS**


**[GSFT16]**

**Gong:2016:FSC**

Wei Gong, Ivan Stojmenovic, Amiya Nayak, Kebin Liu, and Haoxiang Liu. Fast and scalable counterfeit esti-

**[GSW+16]**

**Gierlichs:2012:ICD**


**[GST13]**

**Genkin:2013:RKE**


**[GST12]**

**Ge:2016:KPA**

Chunpeng Ge, Willy Susilo, Jiandong Wang, Zhiqiu Huang, Liming Fang, and Yongjun Ren. A key-policy attribute-based proxy re-encryption without random oracles. *The Com-


Gueron:2016:MEG


Gupta:2015:GEM


Galindo:2014:LCL


Ghosh:2014:BBB


Gorbunov:2012:FEB


Gorbunov:2015:ABE


Greenberg:2014:GWB

Joel Greenberg and Rosamond Welchman. *Gordon Welchman: Bletchley Park’s architect of ul-
REFERENCES


REFERENCES


[Guo:2017:EMD]

[Gao:2012:RHC]
CODEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

[Guo:2018:SMK]

[Gao:2019:VQS]

[Guo:2019:NTP]
Hui Guo, Zhenfeng Zhang, Jing Xu, and Ningyu An. Non-transferable proxy re-encryption. *The Com-


Hayes:2013: NSA


Houmansadr:2013:BCN


Hurlburt:2014:BBC


Hetzelt:2017:SAE


Hernandez-Becerril:2016:GIS


Han:2019:ABI

REFERENCES

He:2013:HEH

Hulsing:2017:XEH

Hao:2012:SAM

Hu:2017:ATE

Hwang:2010:RIB

Hsu:2011:NLMe

Hore:2012:IED

**Hernandez-Castro:2012:MTA**


**Huang:2014:FOS**


**Hsu:2011:WLC**


**Hernandez-Castro:2012:AFH**


**Hosny:2019:RCI**


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. CO-DEN CSSEEI. ISSN 0267-6192.


REFERENCES


REFERENCES

Harn:2014:MTS

Hoang:2014:IMD

Hocking:2013:COU

Huang:2016:EDP

Hanocka:2019:APS

Heyse:2012:TOC
Stefan Heyse and Tim Güneysu. Towards one cycle per bit asymmetric encryption: Code-based


Huber:2019:FCL


Hammi:2018:BTD


Hayashi:2013:AEI


Huber:2014:TPW


Huang:2017:BBC

Hong:2015:RSM


Hinarejos:2015:MES


Hao:2019:IDP


Hinarejos:2015:MES


Harb:2019:FIE


Hinkelmann:2011:CPA

REFERENCES

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


REFERENCES

Heyse:2012:LEA


Heil:2014:APH


Howe:2018:PDG


Holenstein:2011:ERO


Harn:2010:AGK


Hazay:2010:EST


**Hu:2016:PBR**


**Hu:2018:SVX**


**Hu:2019:AAA**


**Huang:2011:ISL**


**Hwang:2019:ELS**


**Huang:2015:MSE**

Chanying Huang, Hwaseong Lee, Hyoseung Kim, and Dong Hoon Lee. mvSERS: a secure emergency response solution for mobile


REFERENCES

Howard:2010:DSS


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


Leah Hoffmann. Last byte: Q&A: Finding new directions in cryptography: Whitfield Diffie and Martin Hellman on their meeting, their research, and the results that billions use every day. *Communications of the Association for Com-
REFERENCES


Hollings:2012:CCE


Horsman:2019:CPE


Hyla:2012:CBE


He:2012:ECT


[HPZ14] Fei Han, Jing Qin, Huawei Zhao, and Jiankun Hu. A general transformation

**He:2013:GME**


**Hulsing:2013:OPX**


**Huang:2014:AFS**


**Hussain:2018:SSH**


**Herranz:2013:SMS**

REFERENCES


Halevi:2011:TBH


Han:2013:IBD


Han:2014:IBS


Han:2012:PPD


Heather:2014:CPE


Ho:2011:EIB


Shi:2015:CTS

[hSZZ15] Runhua Shi, Hong Zhong, and Shun Zhang. Comments on two schemes of identity-based user authentication and key agreement for mobile client-

**Hamdy:2011:HPB**


**Henson:2013:MES**


**Hu:2010:TTW**


**Huang:2015:PAP**


**Huang:2017:SSS**


**Herbert:2012:SMP**

Matthias Herbert, Tobias Thieme, Jan Zibuschka, and Heiko Roßnagel. Secure mashup-providing platforms — implementing encrypted wiring. *Lecture
Hald:2015:RRA


Hulsing:2013:WOS


Hurlburt:2016:MBO


Harvey:2017:FPM


Hunger:2018:DDC


Han:2012:MIA


REFERENCES

Lecture notes in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-17618-6 (softcover). LCCN ???

[HWK+15] 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.


[Huang:2018:PIB] Qinlong Huang, Yixian Yang, and Jingyi Fu. PRECISE: Identity-based private data sharing with conditional proxy re-encryption.
in online social networks. 


**Hao:2011:NTV**


**Huang:2011:IBS**


**Heys:2011:PSC**


**Han:2012:ERI**

REFERENCES

Han:2014:ERI

Han:2014:ATS

Han:2018:ERA

Huang:2019:ILA

He:2017:AHA
He:2018:LAB


He:2015:IEI


Hunt:2018:RDS


Islam:2015:MBA


Ibrahim:2019:RAM

Ismail:2010:EAE


Islam:2011:MES


IBM:2013:DMP

IBM. Daunting mathematical puzzle solved, enables unlimited analysis of encrypted data. See patent [GH13].

IBM:2013:IPC


Irshad:2017:CPP


IEEE:2010:PIA

IEEE:2011:ICI

IEEE:2011:PIA

IEEE:2013:PIS

Imanimehr:2016:HPR

Islam:2011:MDA

Iyengar:2016:SPS
DEN 1550-4832.

**Imai:2015:IRR**


**Islam:2015:LFP**


**Ioannou:2014:PKC**


**Intel:2019:IAM**


**Isobe:2012:SCL**

Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii. Slide cryptanalysis of lightweight stream cipher RAKAPOSHI. *Lecture Notes in...*
REFERENCES

Islam:2018:REP


Isobe:2012:SAL


Irshad:2016:EAM


Ishai:2014:PCP


Jacobs:2016:STB


JR Prins and Business Unit Cybercrime. Diginotar certificate authority breach "Operation Black Tulip". Unknown, November 2011. Fox-IT.


Jiang:2019:SSL


Jiang:2014:UIS


Jiang:2014:TEA


www.sciencedirect.com/science/article/pii/S030439751400098X.

Jiang:2016:MAC


Jiang:2017:BMA


Jin:2010:ADW

Jain:2010:QP


Jawad:2013:GAD


Jamil:2018:SPU


Jan:2019:PBM


Jun:2012:II


Jiang:2016:PPT

Jovanovic:2012:FAL

Josefsson:2016:ECD

Jordan:2018:QCS

Jeong:2012:IKP

Jajodia:2012:RET

Jia:2012:PKD
Jiang:2019:PPP


Ji:2018:DIR


Jiang:2016:OOC


Jiang:2016:UTC


Jain:2012:BAS


Jan:2017:PPB

REFERENCES

[102x681] 1532-0626 (print), 1532-0634 (electronic).

Johnson:2010:BRF


Johnson:2015:NGA


Joux:2013:NIC


Juels:2014:HEE


Jain:2018:MDN

Ajay Jain and Sachin Soni. Multi-directional navigation method for optimized consumption of user generated content through semantic mapping of features derived from the user generated content. ACM
REFERENCES


Jaiyela:2018:IPN


Jevdjic:2017:ASC


Jain:2016:APQ

Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt, and Gerd Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics, 57(3):366-??, 2016. CODEN CPHEAF. ISSN 0010-7514 (print), 1366-5812 (electronic).

Jordmayer:2017:BCI


Jordan:2018:EPE


[JY+10] Yixin Jiang, Haojin Zhu, Minghui Shi, Xuemin (Sherman) Shen, and Chuang Lin. An efficient dynamic-

Jan:2019:SEE


[JZU19]

Khazaei:2017:COA


[KA17]

Kurkcu:2018:CBE


Kurkcu:2018:CBE

Kornycky:2017:RFT


Kornycky:2017:RFT

Koziel:2018:HPS


Koziel:2018:HPS

Kamp:2013:MES

[Kam13] Poul-Henning Kamp. More encryption is not the solu-
Kamp:2016:MEM


Kapera:2011:SPD


Kapera:2013:MRM


Karafyllidis:2012:QGC


Kong:2015:CSM


Katz:2013:RIB

Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP


Kim:2011:SSE


Koz:2012:ASE


Kraetzer:2012:PCS

[KD12b] Christian Kraetzer and Jana Dittmann. Plausibility considerations on steganalysis as a security mechanism — discussions on the example of audio steganalysis. *Lecture
REFERENCES


Kieffer:2018:IBC [KD18]

Karakoc:2013:BCL [KDH13]

Karakoc:2015:AKA [KDH15]


Kara:2019:ALS [KE19]

Keblusek:2015:BRK [Keb15]
Marika Keblusek. Book review: Kristie Macrakis,

Kemshall:2011:WMT


Kleinjung:2010:FBR


Kikuchi:2012:SSN


Kramer:2010:FDC


Kim:2012:SLT

REFERENCES

Khedr:2016:SSH

Kwon:2010:SEB

Koo:2018:PPD

Khazaei:2010:NBS

Kastner:2010:AOT

Kim:2014:MBM
REFERENCES


KIH19

Kim16

Kim11

Kim15

Kim16

KJN+16

Konstantinou:2010:RCI
REFERENCES


[KKGK10] Giorgos Karopoulos, Georgios Kambourakis, Ste-


Kim:2016:DBM


Kim:2018:EPP


Khan:2013:EDC


Koeberl:2012:EPD


Kent:2015:AGA


Keller:2010:DAS

REFERENCES

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


Khomejani:2010:PCT

Koblitz:2010:BNW

Kiani:2011:MPD

Kifer:2014:PFM

Koblitz:2015:RWE

Koblitz:2016:RWE
Kasamatsu:2012:TSE

Kandi:2017:ELC

Kline:2018:CAR

Kiyoshima:2014:CRB

Karger:2011:LLB

Kanwal:2015:TTM
REFERENCES


REFERENCES

Koblitz:2010:BRB


Kasper:2012:SCA


Khamsemanan:2016:BBU


Kawachi:2017:GCR


Kollmitzer:2010:AQC


Kang:2012:AKM


com/chapter/10.1007/978-3-642-32717-9_20/.

Kannan:2013:NQF

quadratic fuzzy c-means algorithms for effective data clustering problems. The
Computer Journal, 56(3):393–406, March 2013. CODEN CMPJAN. ISSN
0010-4620 (print), 1460-2067 (electronic). URL
http://comjnl.oxfordjournals.org/content/56/3/393.
full.pdf+html.

Krenn:2013:AWI

[Kre13] Daniel Krenn. Analysis of the width-w non-adjacent
form in conjunction with hyperelliptic curve crypto-
tography and with lattices. Theoretical Computer
Science, 491(??):47–70, June 17, 2013. CODEN TC-
SCDI. ISSN 0304-3975 (print), 1879-2294 (elec-
science/article/pii/S0304397513002685.

K:2018:AAF

[SRK+10] Zeeshan Shafa Khan, Khalid Rashid, Fahad Bin Muhayman,
Qutbuddin, and Aneel Rahim. Realization of call-
back authentication (CBA) for secure web to cel-
lular phone SMS communication. Computers and
Mathematics with Applications, 60(2):198–208, July 2010. CODEN
CMAPDK. ISSN 0898-1221 (print), 1873-7668
science/article/pii/S0898122110000118.

Kolesnikov:2012:LPP

[KS12] Vladimir Kolesnikov and Abdullatif Shikfa. On

[KS11] Valerie King and Jared Saia. Breaking the $O(n^2)$ bit barrier: Scalable
Byzantine agreement with an adaptive adversary. Journal of the ACM, 58
(4):18:1–18:24, July 2011. CODEN JACOAH. ISSN
0004-5411.

Kolesnikov:2012:LPP

[VK11] Vladmir Kolesnikov and Abdullatif Shikfa. On
REFERENCES


**Kumar:2015:RGB**


**Kalayappan:2018:PAH**


**Karthiga:2018:PSA**


**Korac:2019:FMU**


**Kocabas:2016:ESM**


**Khan:2017:TPK**

Suleman Khan, Muhammad Shiraz, Laleh Boroumand, Abdullah Gani, and Muhammad Khurram Khan. To-

Kiljan:2017:SAC


Kwon:2018:EIP


Ksiezopolski:2012:QMQ


Kim:2012:SSS


Klingler:2013:UPT

Kim:2012:SAH


Kawachi:2012:SKE


Kobayashi:2016:ASC


Klisowski:2012:CCP


Kai:2014:FSD


Küpcü:2013:DTT

REFERENCES

Kupcu:2015:OAS


Kuznetsov:2011:APP


Kshetri:2018:BEV


Kiljan:2018:ETA


Karpovsky:2014:DSS


Kuo:2016:SDD


Koyama:2012:NTD

Takuma Koyama, Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta. New truncated differential cryptanalysis on
REFERENCES


REFERENCES


Launchbury:2012:TBC


Lauter:2017:POL


Liu:2013:PAE


Loreti:2018:PAB


Luo:2012:ESI


Lupu:2012:IBK


Lu:2013:CSA

[LC13] Linzhen Lu and Shaozhong Chen. A compress slide attack on the full GOST block cipher. Information Processing Letters,


Jenny S. Li, Li-Chiou Chen, John V. Monaco, Pranjal Singh, and Charles C. Tappert. A comparison of classifiers and features for authorship authentication of social networking messages. *Concurrency...

**Liang:2014:CCS**


**Liu:2016:EQD**


**Liu:2016:NOP**


**Louchene:2013:WMR**


**Lotz:2015:SCS**

Volkmar Lotz, Francesco Di Cerbo, Michele Bezzi, Samuel Paul Kalhuvuri, Antonino Sabetta, and Slim


Lago-Fernandez:2014:NAA

Luo:2019:SCT

Liu:2016:LCR

Liang:2015:CPA

Li:2018:CIC

Li:2017:PCL
[LCJ+17] Cong Li, Yuejian Fang, Xing Zhang, Cancan Jin, Qingni Shen, and Zhonghai Wu. A practical construction for large universe hierarchical attribute-based encryption. Concurrency
and Computation: Practice and Experience, 29 (17), September 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


REFERENCES


REFERENCES


[Li:2010:EBB]


**Lertvorratham:2012:ISM**


**Liao:2013:NMS**


**Lenstra:2012:RWW**


**Lum:2016:QEM**


**Li:2012:BVS**

REFERENCES


[Li:2018:OPP] Tong Li, Zhengan Huang, Ping Li, Zheli Liu, and Chunfu Jia. Outsourced


[Lin15] Pei-Yu Lin. Double verification secret sharing mechanism based on adaptive pixel pair matching. ACM Transactions on Multime-
Lindell:2017:TFC


Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP


Li:2017:MMA


Liu:2019:ICA


**REFERENCES**

[Li:2016:IRI]

[Li:2017:SQS]

[Li:2012:OEA]

[Lesi:2017:SAS]

[Laszka:2014:STC]

[Liu:2017:OOA]
Liu:2018:PAB


Liu:2010:SVE


Li:2012:BIB


Lee:2014:SPB


Levi:2013:ABN


[LLC+15] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia,


C. Li, D. Lin, J. Lü, and F. Hao. Cryptanalyzing an image encryption algorithm based on auto-

**Li:2010:DCY**


**Lu:2012:IEC**


**Lai:2013:SAS**


**Lai:2018:EQK**


**Libert:2019:ZKA**

REFERENCES


Lee:2015:SAS


Li:2018:WMH


Lu:2012:BBE


Lai:2016:GGB


Li:2017:CBS


Lambert-Mogiliansky:2012:EII

[LMB12] Ariane Lambert-Mogiliansky and Jerome R. Busemeyer. Emergence and instability of individual iden-
REFERENCES


Lv:2013:NTP[LML+13] Chao Lv, Maode Ma, Hui Li, Jianfeng Ma, and Yaoyu Zhang. An novel three-party authenticated key exchange protocol us-

**Lukasiewycz:2016:SAO**


**LoIacono:2019:NGR**


**Li:2018:RBB**


**Li:2013:ESC**

REFERENCES


REFERENCES

Lima:2010:PKE

J. B. Lima, D. Panario, and R. M. Campello
de Souza. Public-key encryption based on Cheby-
shev polynomials over GF(q). Information Pro-
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-
6119 (electronic).

Lian:2015:GRG

Chunfeng Lian, Liaojun Pang, and Jimin Liang.
Generalized random grid-based visual secret shar-
ing for general access structures. The Computer Jour-
nal, 58(10):2426–2442, October 2015. CODEN CM-
PJA6. ISSN 0010-4620 (print), 1460-2067 (elec-

Liu:2017:HPI

Zhe Liu, Thomas Pöppelmann, Tobias Oder, Hwajeong
Seo, Sujoy Sinha Roy, Tim Güneysu, Johann
Großschädl, Howon Kim, and Ingrid Verbauwhede.
High-performance ideal lattice-based cryptography
on 8-bit AVR microcon-
trollers. ACM Transac-
tions on Embedded Com-
puting Systems, 16(4):
CODEN ???. ISSN 1539-
9087 (print), 1558-3465
(electronic).

Lampe:2012:ATS

Rodolphe Lampe, Jacques Patarin, and Yannick
Seurin. An asymptotically tight security analy-
sis of the iterated even-
Mansour cipher. Lecture Notes in Computer Science,
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-34961-4_18/.

Liu:2015:GTB

Shaohui Liu, Anand Paul,
Guochao Zhang, and Gwang-
gil Jeon. A game theory-based block im-
age compression method in encryption domain.
The Journal of Supercom-
puting, 71(9):3353–3372,
September 2015. CO-
DEN JOSUED. ISSN
0920-8542 (print), 1573-
0484 (electronic). URL
http://link.springer.
com/article/10.1007/s11227-
015-1413-0.

Liu:2016:PPO

Ximeng Liu, Baodong Qin,
Robert H. Deng, Rongxing
Lu, and Jianfeng Ma.

**Libert:2010:KES**


**Lubicz:2015:GMA**


**Lukowiak:2014:CEB**


**Liskiewicz:2013:GBS**


**Liskiewicz:2017:SLS**


**Lane:2014:PBD**

Julia I. Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, editors. *Privacy, big
REFERENCES


Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang, Wang-Jui Tsai, and Po-Kai Zhong. Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on

Liu:2015:MSG


Li:2015:FSC


Lao:2016:BFD


Lysyanskaya:2010:AEC


Lin:2011:CNS

REFERENCES

9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-25512-0.

Li:2016:LRC


Ludge:2012:NLD


Lucchese:2010:RPT


Lafitte:2011:CBF


Liu:2010:CIE

Lee:2011:ACA


Lewko:2011:DAB


Lewko:2011:UHA


Lewko:2012:NPM


Liu:2013:SIP


Liu:2013:TIE

[LW13b] Hongjun Liu and Xingyuan Wang. Triple-image en-


**Li:2019:PSA**


**Lu:2014:HOM**


**Liu:2010:NDC**


**Lu:2012:HOM**


**Liu:2010:SET**

REFERENCES

363


Liu:2011:PIA


Lu:2012:MMA


Li:2010:GCP


Luo:2010:NAS


Luo:2012:ICB


Li:2012:IIA

[LWZ12] Yanjun Li, Wenling Wu, and Lei Zhang. Improved integral attacks on reduced-round CLE-


[Xiong Li, Yongping Xiong, Jian Ma, and Wendong Li:2012:ESD]


REFERENCES


Liu:2012:SOCa


Luo:2012:LVT


Liu:2014:PKE


Liu:2017:ESS


Liu:2014:CRA


Li:2019:APA

[LZD+19] JiLiang Li, WeiGuo Zhang, Vivek Dabra, Kim-Kwang Raymond Choo, Saru Kumari, and Dieter Hogrefe. AEP-PPA: an anonymous, efficient and provably-secure


REFERENCES

dl.acm.org/ft_gateway.cfm?id=3274666.


With a foreword by Christopher M. Bishop.


[Michail:2012:EHT] Harris E. Michail, George S. Athanasiou, Vasili Kelefouras, George Theodoridis, and Costas E. Goutis. On the exploitation of a high-throughput SHA-256 FPGA design for...

Moskowitz:2010:ITE


Malkin:2013:SCB


Mangard:2013:KSL


Martin:2010:FWL


Martin:2010:PCC


Martin:2010:XMA


Mazumdar:2016:CIS

Bodhisatwa Mazumdar, Sk. Subidh Ali, and Ozgur Sinanoglu. A compact implementation of Salsa20 and its power analysis vulnerabilities. *ACM Trans-


REFERENCES


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

Mukhopadhyay:2011:PEA


Madanayake:2012:BPS


McGrew:2017:IDH


McGrayne:2011:TWH


McKay:2010:SLB


Sohaib Majzoub and Has-

**Mansouri:2012:ACA**


**Mansfield-Devine:2015:MIC**


**Murdoch:2010:CPB**


**Malina:2018:SET**


**Mosenia:2017:PTS**

Maachaoui:2012:MLA


Meiklejohn:2010:BRB


Menezes:2013:IPB


Menn:2013:ESC


Meshram:2015:EIB


Mandal:2016:DIW


Moreno:2013:NIP

Carlos Moreno, Sebastian Fischmeister, and M. Anwar Hasan. Non-


Mohammed Meziani, Gerhard Hoffmann, and Pierre-Louis Cayrel. Improving the performance of the SYND stream cipher. *Lecture Notes in Computer Science*, 7374:
REFERENCES

378


Miller:2014:ADS

Mou:2013:CBC

Mohd:2018:HDM
REFERENCES


Micciancio:2010:FGC


Michiels:2010:OWB


Michael:2016:RNI


Midgley:2010:SEE


Miao:2019:PPT

Chenglin Miao, Wenjun Jiang, Lu Su, Yaliang Li, Suxin Guo, Zhan Qin,

Martinez-Julia:2012:NIB


Martinez-Julia:2013:BSI


Memon:2018:TFS


Moessner:2012:SAS


Mozaari-Kermani:2017:FD


Mohanty:2011:RTP

REFERENCES

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

Mozaffari-Kermani:2018:ERE


McGrew:2016:SMH


Menesidou:2017:CKM


Marconato:2013:VLC


Mozaffari-Kermani:2010:CSI


Malik:2012:AIC


Montecchi:2012:QSE


Mancillas-Lopez:2010:RHI


Mendez:2016:PES


Manzanares-Lopez:2012:ICU


Ma:2017:LBI

Chuangguo Ma, Juyan Li, and Weiping Ouyang. Lattice-based identity-based homomorphic conditional proxy re-encryption for secure big data computing in

**Madhusudhan:2012:DIB**


**Meshram:2013:IBC**


**Maity:2014:FIR**


**Mondal:2014:DSM**


**Maity:2017:ODC**


**Mulholland:2017:DCD**

REFERENCES


Mazumder:2017:PSK


Mazumder:2017:SAE


Maity:2013:CRS


Matsuo:2012:MAK


Meshram:2012:IBC


Moran:2010:BCP

REFERENCES

0304-3975 (print), 1879-2294 (electronic).

Mukhopadhay:2014:EMP


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

Monz:2016:RSS


Minier:2012:RKI


Mizuki:2011:ASN


Maimut:2012:LCR

Diana Maimut and Khaled Ouafi. Lightweight cryp-
REFERENCES


Minier:2012:EEC


Min:2018:AAB


Mironov:2012:IDP

com/chapter/10.1007/978-3-642-29011-4_37/.

**Mukhamedov:2010:IEP**


**Maimut:2014:AET**


**Marasco:2014:SAS**


**Micali:2014:CMS**


**Manimehalai:2016:NRR**


**Migliore:2018:HSC**


**Moataz:2018:SSE**

[MRR+18] Tarik Moataz, Indrajit Ray, Indrakshi Ray, Abdul-


<table>
<thead>
<tr>
<th>REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mroczkowski:2012:CAS</strong></td>
</tr>
<tr>
<td>Piotr Mroczkowski and Janusz Szmidt. The cube attack on stream cipher Trivium and quadraticity tests. <em>Fundamenta Informaticae</em>, 114(3-4):309-318, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).</td>
</tr>
<tr>
<td><strong>Maitra:2013:DSM</strong></td>
</tr>
<tr>
<td><strong>Maitra:2013:HEM</strong></td>
</tr>
<tr>
<td><strong>Maitra:2013:HPM</strong></td>
</tr>
<tr>
<td><strong>Miller:2016:RPS</strong></td>
</tr>
<tr>
<td><strong>Mukherjee:2017:EPP</strong></td>
</tr>
<tr>
<td><strong>Myers:2012:BCM</strong></td>
</tr>
<tr>
<td>Steven Myers, Mona Sergi, and abhi shelat. Black-box construction of a</td>
</tr>
</tbody>
</table>


Khan Muhammad, MuhammadSajjad, IrfanMehmood, SeungminRho, and SungWookBaik. Image steganography using uncorrelated color space and its application for security of visual contents in online so-


[Mouris:2018:TSB] Dimitris Mouris, Nektarios Georgios Tsoutsos, and

Malkin:2011:ECS


Meerwald:2012:ERW


Muftic:2016:BCC


Mundy:2017:CGU


Murphy:2010:BRB


Murdoch:2016:IDP

[Mur16] Steven J. Murdoch. Insecure by design: Protocols for encrypted phone
REFERENCES


Mannan:2011:LPD


Maes:2012:PFF


Mathew:2012:EIC


Meng:2018:TTB


Ma:2012:CIS


Mahmoody:2013:LEZ

Mohammad Mahmoody and David Xiao. Languages with efficient zero-knowledge PCPs are in SZK. *Lecture Notes in
REFERENCES

Ma:2013:PVP


Nagy:2010:OTP


Nagy:2010:QCS


Naccache:2012:FHE


Naranjo:2012:SAK


Nagaraj:2019:RCC


Nunez:2017:PRE

[NAL17] David Nuñez, Isaac Agudo, and Javier Lopez. Proxy...


REFERENCES


[NIST12] NIST. Recommendation for random number generation using determinis-
tic random bit generators. Special Publication 800-90, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

NIST:2013:CSS


Nguyen:2014:DDI


Ning:2012:DCA


Ning:2012:DPB


Nguyen:2018:TBU

REFERENCES


George V. Neville-Neil. Kode vicious: Hickory dickory doc. *Communications of the Associa-
REFERENCES

Nagy:2010:KD

Navin:2010:ET

Novotny:2010:T

Nichols:2014:CSS


Mehrdad Nojoumian and Douglas R. Stinson. Socio-rational secret sharing as a new direction in ratio-


Nandakumar:2017:CAI


Nguyen:2012:LRS


Nguyen:2010:LAS


Noorman:2017:SLC


Nie:2013:CHB

REFERENCES

CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-38616-9_10/.

Natgunanathan:2017:PBM


Ntantogian:2010:GME


Newell:2014:NCR


Niu:2015:NAS


Nikooghadam:2010:EUE


Obana:2011:AOC

REFERENCES


[OCDG11]


[OdH12]


[OF11]


[OGK15]

[OF12]


[OFMR16]

[OF12]
Ou:2010:CPA


Ogiela:2018:EBI


Oliveira:2012:STA


Or-Or-Meir:2019:DMA


Ortiz-Martin:2019:FAI


Ogiela:2010:UML

Marek R. Ogiela and Urszula Ogiela. The use of mathematical linguistic methods in creating secret sharing thresh-

**Ohtake:2012:AAH**


**Ogiela:2018:LTC**


**Orlandi:2014:SCN**


**Obert:2016:PAE**


**Oppliger:2011:CC**

REFERENCES


[Ormond:2016:CPR]


[Owczarek:2012:LPL]


[Olsen:2016:SIT]


Ohtake:2019:OSA


Odelu:2019:EPP


Orencik:2016:MKS


Okamoto:2012:AAH


Otmani:2010:CTM


Ogiela:2018:VCA

[Urszula Ogiela, Makoto

Ohzeki:2012:NWM


Ortiz-Yepes:2014:BSA


Praba:2010:MAC


Parveen:2018:IEE


Pal:2015:SDC


Pal:2016:ACC

Jiban K. Pal. Administering a cryptology centre by means of scientometric indicators. *Collnet Jour-
Pandey:2014:ACR


Parent:2012:WAI


Park:2012:APO


Park:2018:OTP


Pass:2013:USP


Pranata:2013:MDR

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

Paulson:2010:SDO


Pandit:2012:EFS


Poh:2017:SDV


Park:2014:FRI


Poddar:2019:AED


Pun:2014:GIT

Paul:2016:TSO

Papadopoulos:2014:LQA

Perkovic:2019:LVL

Patsakis:2020:ECD

Premnath:2014:EHR

Poh:2017:SSE
Geong Sen Poh, Ji-Jian Chin, Wei-Chuen Yau, Kim-Kwang Raymond Choo, and Moesfa Soeheila Mohamad. Searchable sym-


Joss Pearson, editor. *Neil

Persichetti:2013:SAH


Peterson:2011:SWS


Petrlíč:2012:PRE


Pfleeger:2010:CJD


Peinado:2012:CAT


Poppelmann:2012:TEA

REFERENCES


Peng:2010:SFW

Park:2012:IDF

Pohls:2012:RDI

Premnath:2016:SPC

Parno:2016:PNP

Papas:2012:MLR
Marios Papas, Thomas Houit, Derek Nowrouzezahrai, Markus Gross, and Wojciech Jarosz. The magic

Park:2010:SIC


Pieprzyk:2010:TCC


Pointcheval:2012:ACE


Patel:2018:LLA


Premaratne:2015:LDD

Uthpala Subodhani Premaratne, Ibrahim Khalil,

Pramila:2018:ICA


Peter:2012:AHE


Perez:2011:FDS


Peris-Lopez:2018:EAC

Pedro Peris-Lopez, Lorena González-Manzano, Carmen Camara, and José María de Fuentes. Effect of attacker characterization in

Pang:2013:IMA


Peris-Lopez:2010:CSP


Perumal:2019:SDE


Pisani:2019:ABS


Poh:2012:SEC

Geong Sen Poh, Moesfa Soeheila Mohamad, and Muhammad Sen Poh. 2012:SEC

**Pande:2013:SMC**


**Poursakidis:2010:TPC**


**Puthal:2017:DDK**


**Niu:2014:RDW**


**Powers:2014:OSCa**


**Paar:2010:UCT**

Papadopoulos:2010:TRM


Park:2011:ACC


P:2018:ABE


Pereira:2016:SHB


Pendl:2012:ECC


Pyun:2012:IBF

REFERENCES


**Perez-Resa:2019:SSE**


**Puthal:2019:SAL**


**Priemuth-Schmid:2012:ASV**


**Polyakov:2017:FPR**

Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntathan.


**Popa:2012:CPQ**


**Priemuth-Schmid:2012:ASV**


**Permpoonanalarp:2014:FTG**

Yongyuth Permpoonanalarp and Panupong Sornkhom. On-the-fly trace generation approach to the security

**Perazzo:2015:DRL**


**Pereira:2013:SLC**


**Phatak:2013:SIN**


**Patranabis:2017:PSK**


**Pizzi:2018:ETM**

REFERENCES

Picazo-Sanchez:2013:CRS


Park:2013:PPM


Pankhuri:2019:PBM


Papamanthou:2013:SCC


Papakostas:2014:MBL


Paletov:2018:ICA

Rumen Paletov, Petar Tsankov, Veselin Raychev, and Martin Vechev. Inferring crypto API rules from code changes. ACM SIGPLAN Notices, 53(4):450–464, April 2018. CODEN [PSOMPL13] [PST13] [PSS+13] [PTK14] [PSSK19] [PTRV18] [PST13]
Papamanthou:2016:AHT


Pudovkina:2012:RKA


Padget:2017:FGA


Pellikaan:2017:CCC


Pei:2013:AR


Pham:2019:SSS

Puthal:2019:SSE


Poller:2012:EIC


Peng:2010:IWM


Pongaliur:2013:SNS


Pagnin:2018:HDB


Philippaerts:2013:CMC


Pei:2015:SWT

[PYM+15] Qingqi Pei, Dingyu Yan, Lichuan Ma, Zi Li, and


Qiu:2018:QDS

Qin:2016:VTQ

Queiroz:2019:WBF

Qin:2013:DP

Qin:2018:NUW
Qiu:2019:CPT


Qiu:2017:AAS


Qiu:2017:PSB


Qiao:2018:CTC


Quaglia:2018:SVA


Qin:2016:STI

Zhen Qin, Chen Yuan, Yilei Wang, and Hu Xiong.

Qian:2014:IAF


Qi:2016:SPR


Qin:2016:BR


Rabin:2010:ACC

Tal Rabin, editor. *Advances in cryptology —
REFERENCES


dwn=1&CFID=796295669&CFTOKEN=92668082.


Raz:2019:FLR


Ruoti:2015:WJS


Rupp:2015:CTM


Radke:2015:CFA


Reaves:2017:MBM


R:2018:SDM


Rao:2019:HPR

Fang-Yu Rao, Jianneng

Raisaro:2018:PPS


Rabbachin:2015:WNI


Rao:2017:CFA


Ren:2016:IBE


Reardon:2016:SDD

R4223 2016. URL http://www.springerlink.com/content/978-3-319-28778-2.


REFERENCES

1556-6056 (print), 1556-6064 (electronic).


[184x646]Rifa-Pous:2012:AHD

[RPG12]


[102x487]Rifa-Pous:2011:CEC

[RPHJ11]


[102x508]Rhee:2010:TSS

[102x526]Rhee:2010:TSS


[102x563]Razaque:2016:TDP
Razaque:2017:SDA


Rosen:2010:CCS


Reeder:2011:WPD


Rival:2014:SSR


Rossi:2015:IBS


Rana:2016:DBV

REFERENCES


Rib[15]:2015:QBS

Resende:2019:BMI

Ruj:2014:DAC

Rahulamathavan:2019:PP1

Ryan:2015:EEV

Ryan:2015:EEVb
Rexha:2018:ITF


Russo:2015:FPT


Rahulamathavan:2016:UCA


Rodriguez-Vazquez:2012:SCB


Reaves:2018:CSS


Roettger:2012:PK

Eric Roettger and Hugh C. Williams. Public-key cryptography based on a cubic extension of the Lucas functions. *Fundamenta Informaticae*, 114(3–4):325–344, August 2012. CODEN FUMAAJ. ISSN 0169-2968


Rajendran:2015:FAB


Sang:2012:SSF


Sakalli:2014:ACC


Somanatha:2015:RAK


Shivani:2016:PVC


Siad:2016:NFI

A. Siad and M. Amara. A new framework for implementing identity-based cryptosystems. *The Jour-
Subramanian:2019:SAF

Saarinen:2012:PPK

Suoran:2012:SAAM
Sanna Suoranta, André Andrade, and Tuomas Aura. Strong authentication with mobile phone.


Sacco:2014:MC


[Sar10a] Neyire Deniz Sarier. Im-


[SAR18b] Priyanka Singh, Nishant Agarwal, and Balasubramanian Raman. Secure data deduplication using secret sharing schemes over cloud. *Future Genera-
REFERENCES

Sasaki:2012:DSW


Sasaki:2018:QKD


Savage:2013:PP


Savage:2015:NVS


Savage:2016:NKP


Safkhani:2017:PSD

Masoumeh Safkhani and Nasour Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. The Journal
REFERENCES


**Srinivasan:2012:RAP**

**Saevane:2015:CUA**

**Syta:2014:SAA**

**Schoenmakers:2010:VS**

**Schwartz:2011:IMP**

**Schaathun:2012:MLI**
Schneier:2012:LOE


Schneier:2012:DES


Schneier:2013:HDD


Schaefer:2015:BRB


Schaefer:2015:ECA


Schneier:2015:DGH

Bruce Schneier. *Data and Goliath: the hidden battles to collect your data and control your world*. W. W. Norton
REFERENCES

455


Schneier:2016:CHT


Schneier:2018:CAA


Schneier:2019:CPI


Shrestha:2010:KBA


Stobert:2018:TAL


Seberry:2010:CTAa


Seberry:2010:CTAb

Jennifer Seberry, Chris Charnes, Josef Pieprzyk,

**Scriber:2018:FDB**


**Smith-Creasey:2019:NWI**


**Shu:2015:PML**


**Saleh:2010:GTF**


**Shen:2012:PAS**


**Shakiba:2010:IID**

Mohsen Shakiba, Mohammad Dakhilalian, and Hamid Mala. An improved impossible differential cryptanalysis of Zo-
REFERENCES


Yu Sasaki, Sareh Emami, Deukjo Hong, and Ashish Kumar. Improved known-key distinguishers on Feistel-SP ciphers and applica-
REFERENCES

Staples:2019:SAB

Sendrier:2010:PQC

Sendrier:2017:CBC


Seo:2018:CSI

Serrato:2012:IAN

Sallam:2012:EBM


Chen Su and Haining Fan. Impact of Intel’s new instruction sets on software implementation of GF(2)[x] multiplication. *Information Processing*...


Saxena:2016:API


Silva-Garcia:2018:SBG


Sun:2015:FSW


Shen:2018:CAL


**Susilo:2016:EDT**


**Shankar:2012:BDF**


**Sun:2017:PKE**


**Sipiran:2014:SCA**


**Shaolan:2011:EDE**

REFERENCES

**Seyedzadeh:2011:IEA**

**Song:2015:ADT**

**Shallit:2010:BRB**

**Shaw:2013:DE**

**Syed:2019:TGB**

**Shen:2014:LES**

**Shemanske:2017:MCE**


**Shim:2011:SAT**


**Shparlinski:2010:NWP**

Igor E. Shparlinski. Numbers at work and play.

**Shu:2015:VCR**


**Satir:2012:CBT**

REFERENCES

465


Siad:2012:NAP


Simion:2015:RST


Simmonds:2015:DII


Sirer:2016:TPS


Shakeri:2012:RZW


Seo:2018:CIA

REFERENCES

60:1–60:??, June 2018. CODEN ????? ISSN 1539-9087 (print), 1558-3465 (electronic).


Seog Chung Seo, Taehong Kim, and Seokhie Hong. Accelerating elliptic curve scalar multiplication over GF(2^m) on graphic hardwares. *Journal of Parallel and Distributed Computing*, 75(??):152–167, January 2015. CODEN JPD-
REFERENCES


[SKGZ12] Roland Schmitz, Shujun Li, Christos Grecos, and Xinpeng Zhang. A new approach to commutative watermarking-encryption. Lecture Notes


Roland Schmitz, Shujun Li, Christos Grecos, and Xinpeng Zhang. A new approach to commutative watermarking-encryption. Lecture Notes
REFERENCES


Srivatsa:2011:ESA


Schultz:2010:MMP


Sandor:2019:EDM


Sun:2016:RSP


Shao:2012:AKP

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

[Sarkar:2010:CRM]


[Sarkar:2010:CRT]


[Sorniotti:2010:PSS]


[Seyedzadeh:2011:IES]


[Sengupta:2012:SAI]


[Sencar:2013:DIF]

Husrev T. Sencar and Nasir D. Memon, editors. *Digital image forensics: there is more to a picture than meets the eye*. Springer-Verlag, Berlin, Germany.


[Smith:2015:HHB] Christopher Smith. *The hidden history of Bletchley Park: a social and or-
REFERENCES


Foreword by Pim Tuyls.

Son:2018:GFD


Siadati:2017:MYS


Safavi-Naini:2011:USC


Seyedzadeh:2014:RCI


Soderstrom:2013:DDY

Sylvia Söderström. Digital differentiation in young people’s Internet use — eliminating or reproduc-
Suriadi:2012:PCV


Schaumont:2015:IEP


Strizhov:2016:SPS


Suresh:2015:AGU


Serwadda:2013:ELK


Shiaeles:2015:FI


REFERENCES

See [CJP12].

Sun:2013:IUP


Serwadda:2016:TRR


Shaikh:2010:CTO


Schilling:2012:ATU


Sur:2012:SSU


Stanton:2014:BRB

Jeffrey M. Stanton and Ben Rothke. Book reviews: Burdens of Proof: Cryptographic Culture and Evidence Law in the

**Singh:2017:SCB**


**Stefan:2012:ACT**


**Sutar:2017:DPI**


**Sutar:2018:DPI**


**Sluganovic:2018:ARE**

Ivo Sluganovic, Marc Roeschlor, Kasper B. Rasmussen, and Ivan Martinovic. Analysis of reflexive eye movements for fast replay-resistant biometric authentication. *ACM Transactions on Privacy and Security (TOPS)*,


Durgesh Singh, Shivendra Shivani, and Suneeta Agarwal. Quantization-based

**Smith:2011:SMC**


**Shahandashti:2015:RUP**


**Sundararajan:2019:SMC**


**Shrivastava:2012:UIE**


**Strydis:2013:SAP**

References


Sood:2011:SDI


Saadeh:2018:HAP


Spiez:2012:RCT

Stanisław Spieć, Marian Srebrny, and Jerzy Urbanowicz. Remarks on the classical threshold secret sharing schemes. Fundamenta Informaticae, 114(3-4):345–357, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Sahai:2012:DCC


Schaffner:2012:EI


Schillewaert:2014:CCA

Jeroen Schillewaert and Koen Thas. Construction


REFERENCES


[Suc12] Dan Suciu. SQL on an encrypted database: technical perspective. *Communications of the Association for Computing Machinery,*...
REFERENCES

55(9):102, September 2012. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Sung:2011:DCE


Sun:2016:NEB


Shen:2015:CSC


Song:2016:IAR


Shmueli:2014:IDE


Svozil:2014:NCC

REFERENCES


REFERENCES


REFERENCES


dw=1&CFID=75191185&CFTOKEN=91ee750c94b7844b-845283B4-1
9A79-646B-E1E33D080226A5B1.


Shi:2013:REA


Sun:2017:CPP


Shen:2014:ERC

Sun:2018:RPP


Tsang:2010:BRR


Tamayo:2015:AFH


Tan:2011:CTA


Tan:2012:SLM


Tan:2012:LCP

REFERENCES


www.sciencedirect.com/science/article/pii/S1353485818300259 [Tan17a]


Dave Taylor. Work the shell: easy watermark-
ing with ImageMagick. 

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

**Taylor:2017:EBH**

Tay17


**Taylor:2019:DST**

Tay19


**Talbi:2018:SIW**

TB18


**Tilli:2015:GCR**

TBCB15


**Tuan:2010:AWB**

TC10


**Taylor:2011:DR**

TC11

Tang:2015:CER


Testa:2019:SFE


Tian:2014:DFS


Tiplea:2014:NSC


Tao:2013:SMS

[TDTD13] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding. Simple matrix scheme for encryption. Lecture Notes in
REFERENCES


Teng:2018:KPA

Terai:2011:BRB

Tseng:2019:AMR

Tassa:2012:SDC

Tewari:2017:CNU

Theofanos:2016:SUE
Tian:2016:IBS

Toledo:2013:DFS

Thabit:2014:RRW

Takayasu:2019:PKE
REFERENCES


[TL12] Woei-Jiunn Tsaur, Ji-Hong Li, and Wei-Bin Lee. An efficient and secure multi-server authentication scheme with key agreement. The


REFERENCES


REFERENCES


Mohamed Tolba and Amr M. Youssef. Generalized MitM attacks on full TWINE. Information Processing
Trammel:2012:DTP


Tian:2017:ORA


Teh:2016:STD


Ehatisham-ul-Haq:2018:CAS


Uzunkol:2018:SWU

REFERENCES


[vdWEG18] Estee van der Walt,


REFERENCES

**Vive:2014:CSC**

**Vliegen:2015:SRD**

**Vollala:2017:EEM**

**VonMaurich:2015:IQM**

**Varadharajan:2018:AUR**


Vuagnoux:2010:CAC


VanDijkhuizen:2018:SNT


Wagner:2016:TPF


Woo:2019:UEM

Walter:2018:RCS


Wang:2010:NSB


Wang:2013:CRA


Wang:2014:IIA


Wang:2018:LRI


Ward:2011:CCM

Mark Ward. Code-cracking machine returned to life.
REFERENCES


[WBA17] Ofir Weisse, Valeria Bertacco, and Todd Austin. Regain-
ing lost cycles with Hot
Calls: a fast interface for
SGX secure enclaves. ACM
SIGARCH Computer Ar
chitecture News, 45(2):81–
93, May 2017. CODEN
CANED2. ISSN 0163-5964
(print), 1943-5851 (elec-
tronic).

[BCW10] Charles V. Wright, Lucas
Ballard, Scott E. Coull,
Fabian Monrose, and Ger-
ald M. Masson. Uncover-
ing spoken phrases in en-
crypted voice over IP con-
versations. ACM Trans-
actions on Information
and System Security, 13
(4):35:1–35:??, December
2010. CODEN ATISBQ.
ISSN 1094-9224 (print),
1557-7406 (electronic).

[Wang18:SNU] King-Hang Wang, Chien-
Ming Chen, Weicheng
Fang, and Tsu-Yang Wu.
On the security of a new
ultra-lightweight authenti-
cation protocol in IoT en-
vironment for RFID tags.
The Journal of Supercom-
puting, 74(1):65–70, Jan-
uary 2018. CODEN JO-
SUED. ISSN 0920-8542
(print), 1573-0484 (elec-
tronic).

[WCL+18] Chun-Yan Wei, Xiao-
Qiu Cai, Bin Liu, Tian-
Yin Wang, and Fei Gao.
A generic construction of
quantum-oblivious-key-
transfer-based private query
with ideal database se-
curity and zero failure.
IEEE Transactions on
Computers, 67(1):2–8, Jan-
uary 2018. CODEN IT-
COB4. ISSN 0018-9340
(print), 1557-9956 (elec-
tronic). URL http://
ieeexplore.ieee.org/
document/7962191/.

[Wang18:SEA] Haijiang Wang, Xiaolei
Dong, Zhenfu Cao, and
Dongmei Li. Secure and ef-
cient attribute-based en-
cryption with keyword
search. The Computer
Journal, 61(8):1133–1142,
August 1, 2018. CODEN
CMPJA6. ISSN 0010-4620


REFERENCES

[WGJT10] Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deter-
ing voluntary trace disclosure in re-encryption mix-
networks. ACM Transactions on Information and System Security, 13(2):
18:1–18:??, February 2010. CODEN ATISBQ. ISSN
1094-9224 (print), 1557-7406 (electronic).

[WGD18] Hong Wang, Jie Guan, and Lin Ding. On equivalence
relations of state diagram
of cascade connection of
an LFSR into an NFSR.
International Journal of
Foundations of Computer Science (IJFCS), 29(7):??,
November 2018. ISSN
0129-0541. URL https:
//www.worldscientific.
com/doi/10.1142/S0129054118500235.

[WGF16] Xianfang Wang, Jian Gao, and Fang-Wei Fu. Se-
cret sharing schemes from
linear codes over $F_p + νF_p$. International Journal of Foundations of
Computer Science (IJFCS), 27
(5):595–??, August 2016. CODEN IFCSEN. ISSN
0129-0541.

[WGD18] Hong Wang, Jie Guan, and Lin Ding. On equivalence
relations of state diagram
of cascade connection of
an LFSR into an NFSR.
International Journal of
Foundations of Computer Science (IJFCS), 29(7):??,
November 2018. ISSN
0129-0541. URL https:
//www.worldscientific.
com/doi/10.1142/S0129054118500235.

[WGMD12] Ding Wang, Chun guang Ma, Sen dong Zhao, and Chang li Zhou. Break-
ing a robust remote user
authentication scheme using
CODEN LNCS09. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.com/
chapter/10.1007/978-3-
642-35606-3_13/.
Wang:2012:SPB

Wei:2012:NCI

Wang:2017:DRM

Wang:2018:GAD

Wang:2015:EFF

Wang:2017:DVP
Wei:2016:PAB


Wu:2012:DAA


Wang:2012:FOP


Wang:2012:NFS


Wang:2019:RSI


Williams:2018:FPD

Michael Williams. The first public discussion of the secret Colossus Project. *IEEE Annals*


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).


[Wei:2014:EEF]  


Wang:2017:PPK


Wang:2016:SEP


Wu:2013:FTR


Wu:2016:CBE


Wei:2015:TPE


Wu:2012:RGB

Xiaotian Wu and Wei

**Williams:2013:APC**


**Whitworth:2014:SPC**


**Woodworth:2019:SSS**


**Wang:2015:RSA**


**Wang:2014:NDH**


**Wang:2019:CPB**

Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao,

**[WSS12]**

**[WT10a]**

**[WT10b]**
REFERENCES

comjnl.oxfordjournals.org/cgi/content/abstract/53/7/1062; http://comjnl.oxfordjournals.org/cgi/reprint/53/7/1062.


REFERENCES


Werner:2017:CIM


Wang:2011:CIB


Wang:2011:CHI


Wang:2017:EAK


Wang:2016:SHI

[XWLY16] Wei Wang, Peng Xu, Hui Li, and Laurence Tian-

**Wang:2017:SRS**


**Wang:2010:IIB**


**Weir:2012:AVC**


**Wang:2014:NAI**


**Weir:2012:IHV**


**Wang:2013:NSW**

Xiaogang Wang, Ming Yang, and Junzhou Luo. A novel sequential watermark detection model for efficient traceback of secret network attack flows. *Journal of Network and...*
REFERENCES

Wei:2014:IDC


Wu:2018:SMI


Wei:2016:APS


Wang:2013:BSB


Wang:2014:CGR


Wen:2011:DSH

References


REFERENCES


REFERENCES


REFERENCES

Xie:2012:RAA


Xiong:2012:PPK


Xu:2016:CIB


Xu:2013:PKE


Xu:2019:TPT


[XMY+17] Rui Xu, Kirill Morozov, Yanjiang Yang, Jianying Zhou, and Tsuyoshi Tak-

**Xiang:2014:PBA**


**Xia:2015:SPK**


**Xiong:2011:CIB**


**Xin:2010:IEB**

Hong Xin, Zhu Shu-

Xiao:2010:TAT


Xie:2012:ORI


Xie:2013:SIP


REFERENCES


Xiong:2012:CLR


Xiao:2018:FEI


Yoo:2017:PQD


Yaacoubi:2019:REM


Yamaguchi:2012:EVC


Yu:2015:SDS


Yang:2010:PII

Yang:2011:PQC


Yang:2014:BEB


Yang:2011:GSS


Yang:2012:PST


Yang:2016:EBB

REFERENCES


Yi:2017:ZCL


Yuan:2013:PVQ


Yu:2016:DNF


Yao:2015:LAB


Yuen:2012:IBE

Yu:2017:PDA


Yasuda:2015:MQC


Yan:2016:DEB


Ye:2010:A


Yamada:2012:PBR


Ye:2014:NIE


Yekhanin:2010:LDC

Sergey Yekhanin. Locally Decodable Codes and Private Information Retrieval

Yoshida:2012:OGT


Yu:2012:EPF


Yang:2017:CCS


Yang:2018:RRE


Yuce:2017:AFI


Yang:2016:EHA


Yang:2017:RSA


Yang:2018:CPG

REFERENCES


Yoshino:2012:SIP


Yum:2011:ACO


Yang:2012:WSI


You:2012:DDS


Yuen:2013:ELT


You:2012:DDS

Ilsun You, Jong-Hyouk Lee, and Kouichi Saku-rai. DSSH: Digital signature based secure handover


[YMZ*19] Zhongyuan Yao and Yi Mu. ACE with compact cipher-

**Yakubu:2017:SSN**


**Yu:2010:PSI**


**Yu:2011:CLE**


**Ying:2013:PPB**


**Ying:2019:LRU**

Bidi Ying and Amiya


REFERENCES

Yoneyama:2012:ORA

Yang:2017:SAS

Yang:2012:EMA

Yin:2017:QPE

Yengisetty:2011:AVC

Yi:2016:IPA
Xun Yi, Fang-Yu Rao, Zahir Tari, Feng Hao, Elisa Bertino, Ibrahim Khalil, and Albert Y. Zomaya. ID2S password-authenticated key ex-

**Yang:2012:SAK**


**Yang:2016:ECV**


**Yumbul:2015:EEP**


**Yang:2018:HEP**


**Yao:2014:NCR**

Hongyi Yao, Danilo Silva, Sidharth Jaggi, and Michael

Yeh:2010:TRR


Yuen:2014:TCT


Ylonen:2014:SAA


Ye:2018:VBA


Yeh:2017:SIB


Yang:2014:IBI


Yang:2011:ACD


Yasuda:2012:ASM


Yang:2018:IAC

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

[555] 555


Hongyang Yan, Yu Wang, Chunfu Jia, Jin Li, Yang Xiang, and Witold Pedrycz.


Yurong Yao, Edward Watson, and Beverly K. Kahn. Application service providers: market and adoption decisions.

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

Jianhua Yan, Licheng Wang, Jing Li, Muzi Li, Yixian Yang, and Wenbin Yao. Pre-image sample algorithm with irregular Gaussian distribution and construction of identity-based signature. Concurrency and Computation: Practice and Experience, 29(20):??, October 25, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


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

**Wang:2011:RDA**


**Wang:2013:RBC**


**Yu:2012:NWM**


**Yang:2010:CRS**


**Wang:2018:CIW**


**Yang:2019:SCC**

[YWY+19] Haomiao Yang, Xiaofen Wang, Chun Yang, Xin Cong, and You Zhang. Se-


[YZ12] Bo Yang and Mingwu Zhang. LR-UESDE: a continual-leakage re-


REFERENCES

[YZZ+14]

[Yang:2014:PST]

[ZBR11]

[ZBR11]

[ZAG19]

[Zoni:2018:CSC]

[ZBPF18]

[ZBR11]
Zhu:2012:JLS


Zhang:2013:RMS


Zhang:2015:PCL


Zhang:2012:TCS


Zhang:2019:EPK


Zhang:2014:GCS

Zhang:2015:IAI


Zhou:2019:SAN


Zeng:2019:PKE


Zhang:2018:SSH


Zhang:2012:AOP

REFERENCES


REFERENCES

Zhao:2017:RAS


Zhang:2011:PFB


Zhu:2016:SCI

Youwen Zhu, Zhiqiu Huang, and Tsuyoshi Takagi. Secure and controllable k-NN query over encrypted cloud data with key confidentiality. *Journal of Parallel and Distributed Computing*, 89(??):1–12, March 2016. CODEN JPD-

**Zhu:2013:TSC**


**Zuo:2019:WDH**


**Zimand:2010:SEC**


**Zhang:2011:FBP**

Zeng:2014:NFC


Zhou:2012:CBF


Zhang:2019:CCF


Zhou:2015:PPS


Zhao:2012:IAS


Zhao:2014:TAH

[ZLDD14] Yifan Zhao, Swee-Won Lo, Robert H. Deng, and Xuhua Ding. Technique for authenticating H.264/

**Zhang:2012:EEF**


**Zhang:2012:CCB**


**Zhu:2017:PSN**


**Zhang:2010:ESP**


Zaeem:2017:MAI

Zafar:2010:GRN

Zhang:2017:PPN

Zavattoni:2015:SIA

Zheng:2016:EUV

Zhao:2012:SSS
Dawei Zhao, Haipeng Peng, Cong Wang, and Yixian Yang. A secret sharing scheme with a short share realizing the \((t, n)\) threshold and the adversary structure. *Computers
REFERENCES

Zhou:2017:IBB


Zenger:2016:AKE


Zmudzinski:2012:WEU


Zhao:2012:SSM

[Hong Zhao, Yun Q. Shi, and Nirwan Ansari. Steganography in streaming multimedia over net-

Zhou:2019:LIN


Zheng:2018:GDP


Zanon:2019:FKC


Zhang:2012:EHO


Zhou:2018:TPW

REFERENCES


[ZT16] Liping Zhang, Shanyu Tang, and Shaohui Zhu. An energy efficient authenticated key agreement pro-
Zhang:2015:FAA

Zhang:2014:LFL

Zhang:2011:AGK
Lei Zhang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, and Ursula González-Nicolás. Asymmetric group key agreement protocol for open networks and its application to broadcast encryption. *Computer Networks (Amster-
Zhou:2018:QTA


Zilberberg:2013:PCM


Zhang:2015:FEB


Zhang:2017:FBI


Zhang:2013:LPP


Zhang:2017:FWI

Heng Zhang, Chengyou Wang, and Xiao Zhou. Fragile watermarking for image authentication using the characteristic of SVD. *Algorithms (Basel)*, 10(1), March 2017. CODEN ????
REFERENCES


Zhang:2017:RIW

Zhou:2011:PSA

Zhang:2016:PAG

Zhang:2014:EFH

Zhang:2019:SPB

Zhang:2018:AKE
REFERENCES


REFERENCES


Zhou:2018:CLR


Zhang:2010:ASL


Zheng:2010:PS


Zhou:2019:CLR


Zhang:2010:ASL


Zhang:2013:BLR


Zhang:2010:ASL


Zhang:2010:ASL


Zhang:2010:ASL


Zhang:2010:ASL

REFERENCES


References

Zhuan:2014:SCA

Zaidan:2017:NDW

Zhu:2018:CAC

Zhang:2017:NLR

Zeng:2019:SAE