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/

09 June 2021
Version 1.518

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K,N)
[Bai10, YC11], (n,t,n) [LHYZ12], (t,n)
[QD16, ZPYW12]. 0 [XHX+17]. 1
[XHX+17]. 1, 2, 3 [SMDS11]. $100$ [Sch16a],
11 [LJ17]. 13 [Blo15]. 2
[AM19, DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGLL10, WK18, WY12]. 22
[MNP12]. 2 $k$ [Sun16]. 3
[AP10, Bro19, CG12b, DWWZ12, FWS13,
GZHD12, GH11a, KWS+12, LJ17, LJ15,
MKH+12, RS16, SS10b, SS12a, SGS14,
WSSO12, tWmC12, YT11a, YI14, YPRI17].
32 × 32 [SA14]. 3 × 3 [ÃMVZ12]. 4
[COP+14, DWZ12, HLYS14]. $49.00$
[Sch15a]. 5 [YN19]. 8 [LPO+17, ZSH+19].

$9$ [APPVP15], = [JJUW10], + [PYH+18]. $2$
[YNX+16]. $3$ [LHM14], $MT$ [HRB13]. $\alpha$
[TTL10]. $c$ [KRDH13]. $d$ [QD16]. $d$ x $d$
[KA17]. $\ell$ [ZTL15]. $F^\nu_p$ [WGF16]. $\gamma$
[DWZ12]. $GF(2)[x]$ [SF12]. $GF(2^n)$
[HJ19, SKH15]. $GF(2^n)$ [LBOX12]. $K$
[FXP12, FR16, CHX13, SG19a, XMY+17,
XLP+18, ZGC17, ZHT16]. $L(1/4 + o(1))$
[Jou13]. $M$ [MMSD13, OS11]. $F_{p_{250}}$
[AMORH13]. $F_q$ [SS13]. $NP$ [HN10],
$GF(2^n)^2$ [GM16b]. $GF(2^n)$ [GM16b]. $GF(q)$
[LPDs10]. $LWE$ [BV14]. $\mu$ [Jia14a]. $N$
[FR16]. $n \times k(k \ge n/2)$ [MC11]. $O(d13^d)$
[KA17]. $O(n^2)$ [KS11]. $P$ [DG17, GT19]. $\pi$
[EHKSS19]. $\pm 1$ [HZW+14]. $q$
[CZCD18, GMS11]. $S$ [LJ15]. $t$
[HJM+11, Oba11]. $w$ [Kre13].
Abstraction [HZS+19]. Absurd [Fai19]. Abuse [JSMG18a, QRW+18]. Abusing [VWC19].

Academic [NSP+18, SDC+17]. Accelerate [Roh19]. Accelerating [AVAH18, CMO+16, DOS+15, SKH15, XZL+19]. Accelerator [BYDC19].


Access-Control [LGLK17]. AccessAuth [TODQ18]. accessing [TODQ18].

Acoustic [DLMM+11a, ACM10, ACM11, Orm16].

Additive [TM18, ZDL12, YJC18].

Additively [Mor19b, PKTK12]. Address [Bel15, WLY17, PSJ+13]. addresses [AZH11, CBL16].

Addressing [SVG16, SRB+12, VKK+19]. Adelson [BBB16b, Adelson-Velski].

Adjacency [SA15]. adjacent [Kre13, Khl18].

Adjustable [BWR12b].

Adversarial [BAG12, GA19, BCND19]. Adversary [Yon12, KS11, LXLY12, OSNZ19, ZPYW12].

Advert [MT17]. Advertisement [Ano16j, AMHJ10]. Advertises [AHS13].

AEP [LZD+19]. AEP-PPA [LZD+19].
AES [ARG19, ABO+17, BW16, BBBP13, BKR11, BB10, DGP10, FAA+18, FLYL16a, FLYL16b, GLMS18, GM16b, HMKG19, HF14b, LB13, Mar10c, MM14b, PBCC14, RMTA18, SY15a, VAI19, WJ19, YWF18].

AES-Like [BW16, WJ19]. AET [HTC+15].

Aliation [XLM+12, XGLM14, XZLW15].

Aliation-Hiding [XLM+12, XGLM14, XZLW15]. Aliations [VKK+19].

Ane [BCEM15, LYL+18, GZHD12, ZWM14].

ane-transformation-invariant [GZHD12]. Afraid [Par12a].

Africa [BL10]. Africacrypt [BL10]. after [Sch18]. Against [Ano17e, BVS+13, BCHC19, BL15, BL16, CW12b, CMA14, DZS+18, DL17, FDY+19, GDL18, GDC16, HCT+12, HLC+19, KMZ19, MSS+18, MWES19, Sch13, SGH15, SLY+16, WSA15, AATM18, ASB16, AYSZ14, BBP13, BD18, BVI12, BPR14a, BPR14b, BFK16, BSR+14, BK12b, Bud16, BCFK15, CKHP19, Che15, CG14a, CGCS12, CB16, CG17, DHLAW10, DK17, Dya19, EWS14, FTV+10, zGXW12, GSC17, HLLG18, HYL+19, JSMG18a, JH11N, LDC13, LHM+10, LGL+12, LLY+12a, LWCJ14, MCL+19, Maf16, MD12b, MNP12, NDR13, OF11, OSNZ19, QRW+18, SBM15, SEY15b, SD12, TLL13, WHN+12, Yon12, ZLQ15, ZWQ+11, ZZC15, OHJ10].

age [Bla12, SR14, Lan17, Sto12]. Aged [Ree15].

agency [Ald11, Kum10, ABJ13].

agent [GPVcBR12]. Aggregate [CCT+14, PSM17, WCD19, GLB+18, LLY15, LLL+18, ZQWZ10, ZDH18, CLW16].

Aggregated [NLY15]. Aggregated-Proof [NLY15]. Aggregating [DP12].

Aggregation [ARWK19, BKL16, EKOS19, LHKR10, SP15b, YM18, ZHW+16, DXWD16, DZC16, GLM+19, RR17, WMY16].

Aging [SKV12].

Agnes [Bur11, Joh15].

Agnostic [HFW+19]. Agreement [ADSH18, BSBB19, Chi16, HCL+14, HEC+12, KMZ19, MNS11, TM12, WSS12, XLM+12, XGLM14, XZLW15, YLSZ19, AAL19, AQRH+18, APK+18, AN15, BGAD12, CSD18, CTL13, DLK+16, ERA+17, GH16, HPC12, HKB10, HWB12, ISC+16, IB11, IOV+18, KS11, KIH19, KP18, KLW+16, KDW+17, LLLS13, LLY06, LK+17, MHL18, NCL13, Nos11, Nos14, OKD+17, OSANAM19, PY19, sZSS15, TLL12, WXK+17, XCL13, XXY19, XMHD13, XHM14, YZZ+14, YY13, ZWQ+11, ZZC15, OHJ10].

agriculture [APK+18]. Aided [BGK12, BCGK12, BGB12, Gop19, GMSV14, LNWZ19, MV19, Vua10, ABB13, LD15, SGR+18, SSA11, WLF17].

AIPISTeg [AGL16]. Air [AUMT16, KTM+18, VOGB18, ZWX+18].

aircraft [XWZW16]. Airflow [RSCX18].

Airway [RSCX18]. AK [XHC+12].

AK-PPM [XHC+12]. AKA [LLL13].

AKF [KDH15]. al [LLW16, LLSW16, MWZ12, PLPW13, SBS+12, Mac14, Keb15].

al-Qaeda [Mac14, Keb15].

[ABJ13, SPLHCB14]. Alan [CS12, Don14, Hel17, LCKBJ12].

Algebra [PWB17, Xie12a, Xie12b, BS15, Bul10b, CFR11, DWZ12, FGP14, Nag19].

Algebraic [ACA+16, HJJ+19, HLC+19, LK19, SK11, Tam15, Wat10, WCXZ17, Bul10a, CFR11, FMB+18, SA14, YTM+14].

Algorithm [AA19, ABC17, Ano11b, AK14b, BGJT14, BKLS18, CNR14, CS10, LPC+12, DCM18, ESS12, GKS17, HZSL05, JH12, JSW12, JHH12, JH16, KB10, LL11, LT14a, LLL17a, LLLH18, LLY+18, MSR+17, MRL+18, NdMMW16, NV10, RR11, RVRSCM12, WHZ12, WZCC18, YPR17, YH16, ZSW+12, ZWW17, AIA+18b, Ang16, Ant14, ARG19, BYDC19, BGJT13, BMB16, CG12b, C1L16, Chun10, EEA13, GJ19, HZW19, JK13, Jou13, KY10, KHMB13, LC17, LR15, MS12a, MM14b, MNM+16,
GBNM11, HAK19, HAGTdFR13, KM10a, KPS10, LDC13, LHM+10, LWK11, NDNR13, OF11, PX13, SGP+17, TK19, TS16a, TY16b, TLL13, VSI11, WWBC14, XWDN12, attempt [Fel13]. Attestation [BWS19, FQZF18]. ATtiny [EGG+12]. Attribute [AAC+16, AHL+12, BFK+10, Boy13, CD16b, CDL18, CDLW19, CHH+19, FHR14, GZZ+13, GSW+16, Gli12, GVW15, HSMY12, HBC+19, Her14, KGP12, LW11b, LW11c, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, OT12, PPA18, PB12, RVH+16, Rao17, SSW12, TMY+17, WDC18, WLH15, WHLH16, WHLH17, XMLC13, XWL16, XHY+17, ZPM+15, ZQQ15, ZMZ17, ZHZ15, BTK15, CPPT18, FWNL18, HZL18, HZWL18, HY18S, HKHK13, JSMG18a, JSMG18b, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, LHY18, LDZW19, Nam19, QRW+18, RD17, SLL+19, WLWG11, WZC16, XWS17, XZP+19, XTZ+19, YSQM19, YCT15, ZWM14, ZML17, ZGL+18a, ZWY+19, Ver17]. Attribute-Based [AAC+16, BFK+10, Boy13, CD16b, CDLW19, CHH+19, FHR14, GZZ+13, GSW+16, GVW15, HSMY12, HBC+19, LDZW19, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TMY+17, WDC18, WLH15, WHLH17, XMLC13, XWL16, XHY+17, ZPM+15, ZQQ15, ZMZ17, AHL+12, CDL18, Her14, WHLH16, CPPT18, HZL18, HY18S, HKHK13, JSMG18a, JSMG18b, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, LHY18, LDZW19, Nam19, QRW+18, RD17, WLWG11, WZC16, XWS17, XZP+19, XTZ+19, YSQM19, YCT15, ZWM14, ZML17, ZWY+19, Ver17]. Attribute-Hiding [OT12, ZWM14]. Attributes [CG12a, VKK+19, YON11, LCL+17a]. Attribution [AIF+19, XHC+12, FNP+15]. Au-Id [HWZZ19]. Auction [Con10, JWNS19, DDL15, HM+11]. auctions [MR14c, QS18]. Audience [DTE17]. Audio [Ber18, DA12, FM15, GCT+12, HK15, KDI2a, KDI2b, Lad14, LSL12b, NXH+17, QF19, TC10, gWpNyY+14, XNG+14, XMLC13, XWL16, XHY+17, YSQM19, ZWM14, ZQQ15, ZZM17, AHL+12, CDL18, Her14, WHLH16, CPPT18, HZL18, HY18S, HKHK13, JSMG18a, JSMG18b, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, LHY18, LDZW19, Nam19, QRW+18, RD17, WLWG11, WZC16, XWS17, XZP+19, XTZ+19, YSQM19, YCT15, ZWM14, ZML17, ZWY+19, Ver17]. Audio-Visual [Lal14]. Audit [YNR12b]. Auditing [LMD16, LCDP15, TCN+17, XWK+17, YSY+16, XA+16]. Augmenting [AV18]. Augment [AB10a, JY14, MV12, Rab10]. Aura [HFCR13]. Austin [IEE13]. AuthCropper [KLK+19]. Authentic [AV18, HLT+15, SZMK13]. Authenticate [HM12]. Authenticated [Alo12, ADSH18, BSB19, BCO13, BDMLN16, CLL16, CLY14, CCS14, CRE+12, DS11, EAA12, FNP15, FSA12, FLL12, GTR11, GL12, HCA+12, HLC+14, HEC+12, KMY18, KLK+19, LHK10, LY16, LH11c, LCCJ13, LTT10, MR14a, MM12, MMS17b, MHKS14, MSU13, PTT16, Sar10b, Smi11b, Tan11, TW14, WDV18, XLM+12, XHC+12, XGLM14, XZLW15, YS12, YLSZ19, YLW13, YRT+16, YON12, ZPZ+16, ZKH16, ABC+18, AIB+16, ABR15, CTL13, FAI4b, FIO15, GPN+12, GLM+11, HPC12, HWB10, HWB12, HL11, HSY10, ISC+16, JKA+18, KMTG12, LWS10, LIH11, LML+13, NCL13, Nos11, Nos14, ODK+17, OSAN19, PTT15, PJ18, PPG19, SMBA10, TCS14, Ts013, TKH14, WZM12a, WZM12b, WVT12, WWC14, XCL13, XWZ+18, YC12, YZ+14, YZL+18, YLL+18, ZTT16, ZGL+18a, ZW18a, ZG10, ZZC15]. Authenticating [BS12, CHX13, GRL12, OKG+12, RPG12, WY12, ZCS15, Bel18b, Cer18, LFGCGCRP14, PGL10, RR16, ZLDD14]. Authentication [AV18, AA19, ADM19, AAA+19, AMSPL19, ASO14, AAZ+16, ACAT+15, ACKB19, AUMT16, ABB19a, ATC17, BL12, BCE+12,
BCM12, BNNH19, BSSV12, Bel18a, BKST18, BCD +12, Bis17, BF11, Boy16, BJKP12, BSV2, CGCGPDMG12, CTC +15, CCR14, CSH +18, CRS +18, CCW +10, CCF17, CCI19, CJ13, CD12, CJIP12, CLH13, DL15, DCM18, DBPS12, DPKW12, DP12, FLH13, FR16, FMT12, FD11, GWP +19, GHS14, Gli12, GI12, GMDR19, GM14, GU13, GMV17, GCK12, HZC +12, HvSi2, HQY +18, HKK19, HLLC11, Har13, Hay13, HBCC13, HM10, HCPLSB12, HCETPL +12, HKL +12, HFS +19, HFCR13, HXC +11, HLCL11, HCYZ18, HWZZ19, HRK18, IGR +16, JN12, JCM12, Jia17, JLY +19, JAE10, KP12, KS18b, KLN15, KTM +18, KRM +10, KSD +17, KPC +11, KLY +12, KTA12, KGP12, Kim15, KPKS12, KLM +12, KO16, KH10, LCL11, LKBK19, LHI2, LFIH18, LLG15. [Authentication [LCLL15, LNZ +13, LZCK14, LNXY15, LCR +18, LLZ +12, MWZ12, MEFO12, MKH +12, MBC15, MRRT17, MRS +17, May15, MLB12, Mort2, MSKRJ17, MPM +17, NR11, NR12, NSBM17, NLLJ12, NLY15, OdH12, O012, OSH12, PSSK19, PCDG14, PPR12, PDT12, PWVT12, RS11, RWLL14, RX18, RSN14, SGG18, Saal2a, SBS +12, SBS18, Sar12, SGC16, Sch15b, SKV12, ST14, SM12, SD12, Shl11, SGC14, SSA13, SPK17, SRRM18, SC12, SCMS18, SZDL14, SHS12, SA012b, SRK +17, SRK +18, TGC16, TWNC18, TYK +12, TM12, Vet10, WgmIdZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WAK +19, WT10b, Xio12, YTP11, YFT17, ZBR11, ZHW +16, ZWZ17a, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, AMK19, ARL13, Aia15, AL15, APMCR13, AHH +18, APK +18, AIM +19, Alp18, AIK18, ACF16, AZF +12, AKS19, ATI +10, ACC +13, AN15, ACM12, BK19, BOF14]. [Authentication [BS13a, BGE +18, BDM18, BDL +19, BD18, BCM13, BGAD12, BBTC20, BDMM +19, BB19, BAL +16, BAL10, BBMM12, BHoMS15, BT18, BTW15, BM11, CLM +12, CML +18, CLP +13b, CAM19, CTL12, CJXX19, CSD18, CNF +18, CH10, CWS11, CHS11, CLHJ13, CZ15a, Chi13a, CCMB19, CJ15, Cho14, CL11, CHL19, CR13, CDWM19, DCA12, DCS12, DRN16, DEL19, DLK +16, DMV15, DSN13, DZS +12, DMT12, uHAN +18, EA12, ED19, EA11, FBBG14, FHH10a, FLL +14, FPX12, Far14, FA14a, FHZW18, FQZ18, FMA +18, FH +10, FZZ +12, GJ13, GMSW14, GHD19, GEAHR11, GPLZ13, GH15, GH16, GAL +18, Gop19, GCAd11, GMJ11, GL +18, GBC19, GTSS19, HU15, HSH11, Ham12, Ham19, HZW19, HW19, HBBS18, HDPC13, HZC +14, HK17, HZWW17, HL12, HL14, HCM11, HLC16, HPL +19, HCC10, HS11, IMB17, IAA +19, IC17, IG11, IB11, IOV +18, Jac16]. [Authentication [JNUH17, JKAU19, Jia16, JKL +16, JMW +16, JAS +11, JXLS15, KPP16, Kem11, KKG14, KSB +17, KSC +18, KV18, Kim11, Kim16, KIH19, KS19, KP18, KPB17, KLW +16, KLW +17, KKD +18, LLL13, LLZ +16, LC17, LLY06, LH11b, LT13, LH0c, LNM +11, LMJC11, LMW12, LNNH13, LNK13, LJX14, LK +17, LCM +17, LNK +18a, LWK +18, LNK +18b, LZD +19, LWK +19, LW19, LHM14, LH13, LSQ15, LHH +18, Lit14, LWL11, LTC +15a, LYL15, LZZ19b, LBR12, LTT10, M12, MMLN15, MCM +18, MDHM18, MV011, MMP19, MA17b, MMS17c, MW +18, MZL +19, MCRB19, MHL18, MK12a, MGB19, NDA18, NR17, NACLR12, NCC13, NM18, NLY12, NML9, NB13, NXS10, NMX15, OSP +19, OF11, OCDG11, OYHS14, PYH +18, PYP10, Par12b, PLGMCf18, PCK19, PZBF18, PA10, PKA15, PNR +19, QMC17, QMW17, QLZ19, RR17, SSA18, SCBF15, SPLLCH14, SB17, SGGR +16, Sar10a, SK18, SSNS15]. [Authentication [SVY19, SGJ +18, hSZZ15, SCKH10, SYWX19, SNG +17, SCR19b,
SA15, SYW17, SSS11, SKEG14, SA19, SMS+16, SHBC19, Tan12b, Tan15b, Tan18, TODQ18, TZTC16, TG17, TLL12, Wan13, WW14, WLZ+16, Wan18b, WCFW18, WXSH19, Wat14a, Wat15, WDKV19, WT10a, WKH11, WXK+17, XHH12, XWDN12, XHCH14, XXCY19, XMHD13, XHM14, YI17, YHL16, YHHS16, YK+19, YWK+10a, YSL+10, YMM13, YN19, YY13, YD17, ZYL+10, ZQWZ10, ZCLL14, ZQD16, ZGL+18b, ZDHZ18, ZHY+19, ZX11, ZLY+19, ZZL+18, OHJ10.

authentication-chaining [EA11].

authenticators [SYY+17]. authenticity [ADF12, VBC+15].

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

Authorization [CS14, LMGC17, MPM+17, YKK18, AL15, DFJ+17, FHM+10, JAE10, JAS+11].

Authorized [GHY18, HTC+15, LLSW16, Ma17a, WZCH19]. authorizing [Bel18b].

Authorship [AIF+19, BTW15, BAG12, LCM+17].

Autoblocking [LLLH18, YH16].

Automata [CCD15, Gas13, dRSdVC12, Ang16, DGL19, HBBRM+16, KFE19, SS11, WOLS12].

automata-based [SS11].

Automated [BHC19, CCK12, CCCK16, DRS16, GLLSN12, JGP+18, LGM+16, Ste15a, Tom16, YSS14, BJR+14, GMMJ11, KKK+16].

Automatic [HWZZ19, MMP19, WW12, HL19].

Automation [BGK12, DZS+18, IEE11a, KPP16].

Automotive [HK18, LMS16, MPM+17].

Autonomous [SEK+19].

Autonomous [MPA+18, BT18, SMS+16]. Auxiliary [DMS+16, DL12, GGHW17, XXZ12, YCZY12, Kom18]. Auxiliary-Input [XXZ12, Kom18].

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

AVC [JSZS12, JHHN12, LW13c]. average [Lim11, YL11]. avoid [CFZ+10].

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

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

Aware [ARWK19, BCF16, HFS+19, JSA17, LJP17, LMHH14, LMS16, QLL17, YTH17, ARL13, AKS19, DQY+19, GHD19, LWYM16, MGP10, TODQ18, Wan13, ZDHZ18, ZFH+18]. Awareness [HSC19, MSas12, SAM+18, HPJ+19, Li10, MSas13].

axiomatic [AT10]. axis [WMU14]. Azure [Sti19].
HBBRNM+16, HLR11, Her14, HWB10, HWB12, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HYF18, HPY10, HKHZ13, HCC10, Hwa11, IMB17, IM14, ISC+16, IB11, IA15, IOV+18, Jac16, JNUH17, JKAU19, JK13, JLT+12, JCL+18, JZS+10, MJW+16, JSMG18a, JSMG18b, JLX+19, JDV16, KFE19, KPP16, KK13, KM10a, KHMB13, KTM+18, KKG14, KCS+18, Khl18, KD18, Kim11, KGO10, KD19, KLW+17, KKD+18, KL11, KS18a, KS18b, LXLY12, LLZ+16, Lns12, LLC10, LK14, LHM13, LYY+10, LH10c, LZJ10, LNM+11, LMJC11, LK12, LXM12, LKAT12, LLHS12, LNK13, LXR14, LDZ+14, LCL+15. based [LZY+16, LWYM16, LFZ+17, LNK+18a, LWK+18, LW+19, LCT+14, LFWS15, LLM+19, LPdS10, Lin14a, LHH+18, LYY+12a, LW10, LSQ11a, LSQ11b, LW11, LW13b, LZC14, LPZJ15, LTC+15a, LYL15, LY15, LJW+17, LJW18, LDZW19, LWW+10, LL16a, LW13c, LWY12, LY14, MCN+18, MCP15, MJGS12, MJS13, MLM16, MWW+18, MZL+19, MMF15, MMZ12, MM13, Mes15, MCRB19, MBB11, MO14, MSGCDPSS18, MHT+13, MG15, NM19, NM19b, NM19c, NZL+15, NMX15, OMPSP+19, PAP18, PYY+18, PLPW13, PTK14, Par18, PWW10, PGLL10, PZL+19, PPB16, PLGMCdF18, PCK19, PS14, PL16, PAK15, PC14, PPR+12, QZDJ16, QRW+18, QYWX16, QMW17, QLZ19, RD17, RG10, RS15, SPLHCB14, SERF12, SGGCR+16, SLL+19, SAM+19b, SL12, SD17, SYL13, SE14, SE16, SK18, SH11, SM11, SMN14, SZHY19, SR10, hSZ15, SCKH10, SA16b, SKP17, SSAF11, SHC+16, SWW+16].

based [SS11, SKEG14, SC19b, Sun16, SG16, SHBC19, SS11, TPL16, TQL+14, Tia15, TH16, THA+13, TTL10, TPKT12, TKHK14, VS11, VN17, WWYZ11, WWYY11, WLWG11, WLDB11, WZC16, WLFX17, WMX+17, Wan18a, WMXZ19, WXH19, WGD19, WZG+12, WHLH16, WS14, WS12, WTT12, WOLS12, WCC18, XHH12, XWZW16, XW12, XCL13, WXS17, XZP+19, XHCH14, XWZ+18, XTZ+19, XMHD13, XHM14, YWS+17, YJW+19, yYqWqZC13, Yan14, YTM+14, YCC16, YX+18, YSQM19, YYY+19, YJY+18, YY13, YLS12, YM10, YKC+12, YLZ+16, YXX+16, YLL11, ZK17, ZAA17, ZG17, ZL16, ZCL14, ZT14, ZT16, ZQD+16, ZML17, ZGL+18a, ZGL+18b, ZYW+19, ZY12, ZHJ+17, ZLC12, ZHY14, ZDW+16, ZYM19, ZLY+19, LZJX10, Ver17, HZC+14, MM12, PP11, ZBR11, M14].

Based-Encryption [ZHW15]. based-wireless [HKA+18]. Bases [EVP10, TSH14, FES10]. Basing [Mat14, MN10]. Basis [BNA15, ERRM15, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12, CM12].

Batch [WSY+16, ZPXX17, AGHP14, CCG10, MGB19].


BeagleBone [Cri16]. Beat [LTKP16].

BECAN [LLZ+12]. Becomes [Bra13].

been [Ana14], before [GST12, Goo12].

Beginner [Gre19a, She17]. Beginning [Chu16, Zor12]. Behavior [ASV+18, GSC17, RSX18, KLN15, SPK17].

behavioral [BOP14, CAM19, HT11, MWW+18].

Behaviors [GAF+15, HL19, ZMYB17].

Behavioural [MT17]. Behind [Fre10, Sti19]. Beijing [BYL10, Yan10].

Being [NLP+18]. Beissinger [Ay12].

Belief [BT12]. Bell [JE+15, QD16].

Benchmarked [MKAA17]. Benchmarking
[MTM18, ZZKA17]. Benefit [HB14].
benefits [Wat14a]. Benford [AOT13].
Bessel [GG13]. best [Cha13c, Tay19]. bet [Rom12]. Beta [MV18]. Beth [CTHP13].
better [LCL+17a]. Between
[HSUS11, KA18, LRVW14, SAKM16, CLM+12, HLR11, KPP16, Kim16, PBCC14, WDDW12]. Beyond
[JJ18, LST12, MJS13, RS18, TS16b, FNP+15, JR14]. BGP [SVG16]. BGV [GHPS12, GHPS13].
BGV-Style [GHPS12, GHPS13]. Bias [BHT18]. Biased [USH19, LLP+18].
Biclique [BKR11, KDH13]. Bidirectional
[GMNS15, GH12]. bifurcation [SE18]. Big
[FYD+19, GRRZ18, HLC+18, KBP18, LLSL19, MLO17, Mal13, MMS17b, PH16, PNRC17, PWS+19b, YDY+16, ZLW+17, FS18, HL19, JLC18, LSBN14, QCX18, Rom12, Tan17b, WS14, WS19]. biggest
[Rom11]. Biggs [Low12]. bilateral
[jT12b]. bile [RS+17]. Bilinear [Abe12, ASS15, IL15, LZY+16, YS12, ZZ15, ZY17b].
Bilinear-map [LZY+16]. Bill [Bel15].
billions [Hof16, SMBA10]. Binary
[ADI11, ABSSS19, ADSH18, AK14b, MBR15, MFB18, DGK18, SA14].
Binary-Ternary [ADI11]. Binding
[HEC+12, LBC18, ZLQ15, LZ11]. Bio
[OK18, VGA19, AJYG18, GPVdcBRO12, ZHL+11]. bio-cryptographic [ZHL+11]. biocryptosystems [AJYG18].
Bio-inspired [OK18, GPVdcBRO12]. Bio-Key [VGA19]. BioAura [MSKRF17].
biographical [Maf16]. biomedical
[AIA+18b]. Biometric
[Alp18, ATI+10, BDM+19, BCTPL16, DWB12, HFS+19, JN12, KHM13, LGM+16, May15, NGAuH16, PMG+19b, Sar12, SKV12, SRRM18, SSP19, Vet10, YYK+17, AAL19, AHM+18, BK19, DEL19, DMT12, GCSAddP11, GBC19, HT11, Ham19, KCS+18, LK12, LTC+15a, MLBL12, Sar10a, Sar18a, SR10, SC19b, YWZ+18, ZQD16]. Biometric-based
[BDM+19, GBC19, KCS+18, SR10].
Biometrics [AHN+18, BW13, ERLM16, SP13, ZPW16, AGBR19, BOP14, CNF+18, FHZW18, GM16a, KLW+17, LXYL12, LH10c, LNM+11, LH14, LNK+18a, MRRT17, Rom11, SS17a, SCFB15, YY13].
biometrics-based [CNF+18, FHZW18, KLW+17, LXYL12, LH10c, LNM+11, YY13]. biosensor [Kim16]. Birkhäuser [Sha10].
birth [YY17a]. Birthday
[ACD18, LST12, GJ19, SXL16, Nac12]. Birthday-Bound [LST12]. birthday-type
[GG19]. Birthmarking [TLZ+17]. Bit
[CK17, CG14a, GV14b, HG12, HS18, KTM19, LJK17, LPO+17, NIS12, Ros11, YLL+12, APPVP15, BGG+19, KS11, KFL+10, MMN12, PLsvdLE10, RH10, SLXX16, TWZ+12, VN17, ZSH+19]. bit-pair [SLXX16]. Bit-Wise [CG14a].
BitCoding [HS18]. Bitcoin
[ADMM16, BR18, BH15, Bra15, Ch13b, HB14, Hur16, IM16, JSK+17, Mic16, Sir16, Tay17, TS16b, VFV17a, VFV17b, WLY17, WHJ17, Ano16a]. Bitcoins [MPJ+16].
BitErrant [Ano17a]. Bits
[BF12, LLL17a, YCL17]. Bitsliced
[HMKG19]. Bitstream [SMOP15].
Bivariate [TWZ11]. Bivium [EVP10]. BIX
[Muf16]. BLAC [TAKS10]. Black
[BR14, CPS16, HHP17, KOS16, KMO14, MSas13, JB11, Rja12, SSS10b, YKA16, DD13, SK14, YSC16, ZZ12, Cri16]. Black-Box
[BR14, HHP17, KMO14, Rja12, SSS10b, KOS16, MSas13, ZZ12]. Blackbox
[MSas12, SS12a]. Blackhole [SS15]. BlackWatch [HSC19]. BLAKE
[AMP14, GV14b]. BLAKE-512-Based
[GV14b]. Blanche [SR14]. Blended
[ACAT+15]. Bletchley [Bai12, Ano11c, Bri11, Cop06, Cop10a, Cop10b, GMT+12, GW14, McK10, McK11, McK12, Pen11, Sim10, Smi11a, Smi15b, Smi15a]. Blind
[AP10, Ano15a, BCPV11, LCLW17, LGPRH14, MR16, MMN12, RS16,
broke [Bat10, Heal15]. Broken [MDAB10].
Brocker [TKR14]. Broker-Less [TKR14].
Browse [NA14]. Browser
[QF19, ABR13, ACC+13, BCFK15, GJ+12].
browser-based [ACC+13]. Browsers
[FVJ19, Reel15]. browsing
[MWW+18, YYY+19]. Bruce [Sev16].
Brute [CJP12, JR14, CJP15]. Brute-Force
[JR14, CJP12, CJP15]. BRW [CMLRHS13].
BSn [LHH+18]. BTC [CLF11, GJC+18].
BTC-compressed [CLF11]. Bubbles
[HHBS18]. Buchwald [ABJ13]. Bucket
[BKKV10]. Bug [Ch13b]. Build [IM16].
Building [BPS16, GB19, KMP+11, MJS13,
Sev16, WL11, LCKBJ12]. built [GSAV18].
built-in [GSAV18]. Bullet [McG16].
Burden [Bai12, SR14]. Bus [AN17].
Business [LDB+15]. Butterfly [HQY+18].
Buyer [Fra16, KJN+16]. Buyer-Friendly
[Fra16]. BYOE [Tan1a]. byte
[Hof15, Hof16]. Bytecode [SEK+19]. bytes
[PBCC14]. Byzantine
[KS11, LLKA19, YKGK13]. Byzantine-resistant
[YKGK13].
C [AD12, ACZ16, Cra14, DGJ14]. C&C
[GN16]. C1G2 [MK12a]. CA [ACM11,
Dun12b, Kii11, Lin14b, Pie10, Rab10].
CABA [MSK17]. CAFE [XH+17].
Cache [AB15, ADR18, CBR19, DKMR15,
FDY+19, HL AZ15, LWL16, SY15a,
YDV19, DJL+12, DK17, MCL+19].
CacheAudit [DKMR15]. Caches
[LLGJ16, CDPLCA16, DJL+12]. Caching
[ADR18, HL AZ15]. cackled [Bai12]. CAD
[PGLL10]. Caernarvon [KMP+11].
Calculus [MR10, Jou13]. Calibrated
[LC15]. California
[ANO10a, IEE11b, IEE15, MSH+16]. Call
[ANO16b, ANO16c, ANO16j, CS14, Hor19,
KRM+10]. Call-Back [KRM+10]. Calls
[Mur16, KGP+19]. cam [PKS18].
Cambridge [ACM10, PJ12]. Camellia
[Blo15, LWK12, LWPF12, LWK14,
SEHK12]. Camellia-192 [Blo15]. Camera
[ATC17]. Cameras [ASV+18, MKH+12].
Can [Alo12, AZH11, Bar15, DSM14,
KNTU13, YM16, PeC17, RK11, Rus15, Sto12,
GMVV17, LMS16]. Canada [YJ14, MV12].
Canal [GWP+19]. Cancelable
[QLZ19, AJYG18, LZ11, LH14, YWZ+18].
Cancellation [DLMM+18]. cancelled
[Ano14c]. Candidate [GG+16a].
candidates [ABM+12]. canonical [Bui10a].
CANS [HWG10, LTW11]. Can’t
[ASV+18, Kn17, RAZ15, PZ15].
CAOVerif [ABF+14]. Capabilities
[CHN+18, GB12, Lop15a, KMG17].
Capability [IA15, LLZ+17, LT13].
Capability-Based [LLZ+17]. Capacity
[LY+18, TQD18, WLY+18, XNR15,
YW10, BCN19, CLZ+17, GZH12,
PWLL13, WL13]. Capacity-aware
[TQD18]. Capacity-Raising [YW10].
Capitalism [Fid18]. CAPTCHA
[OTO18, SKE14]. CAPTCHA-based
[SKE14]. Capture
[ASV+18, MBC+18, NYR+14].
Capture-the-Flag [MBC+18]. Captured
[HHZ19, SPK17]. capturing [PKS18].
Card [BDF12, HMR12, HCL+14, PDT12,
Alo17c, CLHJ13, GLC10, LNK13,
Mar10b, Cho10, SD12]. CARDIS [GLC10].
Cards [BSJ15, LA10, PWVT12,
WgM12, CHS11, HCC10, KY10, LH10c,
LMM+11, LMM12, MM12,
SG12]. care [FHV16]. caricature [CLY18].
CariGANs [CLY18]. Carlo [CR12, FY17, QGH17].
Carol [Xie12a, Xie12b]. Carry [GWM16].
Carrying [PV17]. Carved [LC15].
CASCA [DZ+18]. Cascade [WGD18].
cascaded [DGL19]. Cascading [GT12].
Case [Alo17c, DR11, Kii17, SBS+12,
SY15a, SRT12, Uto13, YL17, Dya19, KID18,
LKK13, M12a, SS17a]. Cases [SG19b].
Cash [YMWS11, Bro12, Pec12, Zor12].
Casting [CW12b]. cat [Pow14]. Catalan
Characterizing

[Alr13, BS13b, CRS+18, DPCM16, RZ19, YZLC12, YDVF19, DDD14, PLGMCdF18].

Charging

[Ash14, JR13, RVS+18, MPJ+16]. Changing

[CKHP19, LSY+16]. Chart [Pec17].

Chattarjee [K13]. Cheat [WS12].

cheat-preventing [WS12]. Cheater

[KI11, Ob11]. Chebyshev

[HD19, LW+19, LPsS10]. Check [GST12].

Check-before-Output [GST12].

Checkability [LHL+14]. Checkable

[IW14]. Checking [FYMY15, YL17, SYY+17, YXA+16, PZL+19]. Chen

[LLL10]. Chennai [BC11]. China

[BYL10, IEE1a, LTW11, Yan10]. Chinese

[HF14a]. Chip [Bis17, HZS+19, KS18a, LGLK17, MDAB10, BAB+13, BGG+13]. Chips

[Man13, SS15]. Chirp [OWHS12].

Cho [SPLHCB14]. Chocolate [Svo14].

Choice [LPP+18]. Choosing [BL17].

Choquet [SH11, SM11, SNM14]. Chosen

[FSGW12, zGXW12, HLW12, HPY10, LCT+14, LZC12a, LMLL12, MH14, RS10, WWHL12, GLM+16, GH12, LZC14].

Chosen-Ciphertext

[RS10, FSGW12, LCT+14, GH12, LZC14].

Church [ABJ13]. CHURNs [RBNB15].

Cipher [BW16, BFMT16, BCG+12b, CMLS15, CGCS12, DM18, DG12, DWZW12, EHKSS19, Fis15, FXP+17, GLSN12, GCS+13, HZ11, Hey17, IOM12, JKDP12, KR11, KWS+12, LPS12, LYK19, LWZ12, LJ17, LJPK12, LPFW12, MRTC12, MH12, MS12b, OGK+15, PH12a, PRC12, WSN10, WHN+12, YCL17, ZAG19, AMS+10, BNY14, CR12, FVK17, HKT11, Hol12, Jez13, KDH15, Lew10, LCI13, LYHH14, LWKP14, MNP12, PL16, Rec15, RS14, Sar11, WY14, WWC14, ZSW+18a, GLG+12].

Ciphers [ABS+12, BMS12, BSS+13, BM18, BKL12, Bru12, CWP12, DGFH18, DGLS12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNL12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCIW17, LGLL12, LJ16, MD12b, NN12, PDJ+19, Pud12, Sas12, SEK12, SJLK18, StA1a, Vua10, WH18, WW12, Xie12a, Xie12b, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, GMR+12, KMI10a, LGP19, LWK11, MCL+19, MRT10, MHV15, MMY+18, QGGL13, SKE10, TQL+14, W12].

Ciphertext

[BDPS12, CWWL12, CHH+19, zGXW12, HLW12, JMG+16, JSMG18a, KA17, LZC12a, LMLL12, MH14, PDNH15, PPS1b2, Rao17, RVZ12, RS10, SSW12, VSR12, WWHL12, XMCL13, XWLJ16, YM19, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT+14, LFWS15, LZC14, LDZW19, QRW+18, RD17, SG16, WZC16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertext-only [KA17].

Ciphertext-Policy [CHH+19, Rao17, XMCL13, XLWJ16, ZHW15, JSMG18a, JSMG18b, LFWS15, LDZW19, QRW+18, WZC16, XWS17, LAL+15, LHL15].

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

Circle [SC10].

Circuit [AH19, EAAA19, Kar12, MTY11, XWS17, XLWJ16, Lau12, MS13a].

Circuit-Size [MTY11].

Circumventing

[BAG12]. CISSP [STC11].

cities

[LDZ+19, SSSA18]. Citizen [Ano16c].

City [Ano17d, GAI+18, JZU+19, LNK+18a].

Claimant [Y17]. Claims [SKGY14]. Clara

[MSH+16].

Class [BCG12a, SY15a, XXYYX11, BJ16, Geo12, KK10].

Classes [ACZ16].

Classical [BCD17, DSB18, JEA+15, MSU13, SSU12, CR12, RK11].

Classical-quantum [BCD17].

Classification [CHH+19, HPC10, HS18, KAHKB17, SGP+12, ZLW+17, ACM19, HZW19, LHL+18].

Classifiers [KGV16, LCM+17].

classroom [Pow14].
YTP11, Yek10, ATI⁺¹₀, Bull10a, CZ15a, Chi3a, Fag17, Hea15, LTT10, MG15, OŠ11, Tan15b, YSLL14, Ayu12, Low12, Nag19.

**Codevelopment** [DF16]. **Coding** [ACA⁺¹⁶, Che11, CWL16, CJ13, CG14a, DG17, Hes12, LCLL15, Per13, SSKL16, WCXZ17, AZF⁺¹₂, Bull10b, CJXX19, DTZZ12, JZS⁺¹₀, KM11, LLP⁺¹₈, NDNR13, OF11, Tan15b, YTM⁺¹₄, Kim15].

**CoDiP2P** [NCCG13]. **Codon** [HEK18]. **Coecients** [BDB14]. **Coercion** [CW12b].

**Cognitive** [PP11, BSBG19, Kim11, OK18, RPG12]. **Cohen** [Ara13]. **Coherence** [VDV19]. **Coin** [ALR13, BHT18, CLP13a, CK17, DSMM14, Mat14, BB14, Wag16]. **Coins** [Fok12].

**CoinTerra** [BH15]. **COIP** [BCF16]. **COIP-Continuous** [BCF16].

**Colbert** [Dew11]. **Collaborating** [SDC⁺¹₇]. **Collaboration** [CRE⁺¹₂, PCPK14, CWZL13, DYZ⁺¹₅, HY18]. **Collaboration-Preserving** [CRE⁺¹₂].

**Collaborative** [MJW⁺¹₈, LLY₀₆, LT₁₄b, HB13]. **Collaboratec** [Ano16g]. **collect** [Sch15c].

**Collective** [M16]. **Collision** [BK12a, ZL12, AKY13, Con17, SKP15, SBK⁺¹₇]. **Collision-based** [ZL12].

**Collision-Resistant** [BK12a]. **Collusion** [MMSD13, RH⁺¹₆, FLZ⁺¹₂, GMRT⁺¹₅, SCBL16, ZZL⁺¹₉].

**collusion-attack-resilient** [SCBL16]. **collusion-resistant** [GMRT⁺¹₅].

**collusion-resisting** [ZZL⁺¹₉]. **Collusions** [GVW12].

**Color** [BCPV11, DD13, FR16, HD19, LW10, MR16, RMG18, ST15, yWXYZ⁺¹₈, YQWX15, Bro19, MSM⁺¹₈b, SMN14, yWpWypM13, WGZ⁺¹₂, YSC16].

**colors** [MMLN15]. **Colossal** [Hai17].

**Colossus** [Cop06, Cop10a, Cop10b, HP18, Wil18]. **Coloured** [PS14]. **Column** [FS15].

**combating** [FTV⁺¹₀]. **combination** [Wat14a]. **combinational** [MS13a].

**Combinatorial** [ZAC17]. **Combined** [PP10b, PDJ⁺¹₉, RMTA18]. **Combining** [AGBR19, Chi3a, CDF⁺¹₀]. **Coming** [SOG15]. **Comment** [LCLL15, Ver17].

**Comments** [IC17, Kim15, hSZZ15, Tan11, TGL15, XWS17]. **Commerce** [Bla16, Hv16, Orm16, Ano11a].

**Commitment** [CK17]. **Commitments** [Pas13a, CSZ⁺¹₁, LP11]. **Committee** [Bla16]. **commodity** [KKJ⁺¹₆].

**Common** [CN12, DHB16, ESRI14]. **Communication** [ADM19, Alz19, BPSD17, Big08, BCG19, CCM17, CCW⁺¹₀, FMS12b, Gas13, GPVCdRO12, kW₁₄, Low12, OKG⁺¹₂, Wan13, ZC13, ZHW⁺¹₆, AASSA18, ADG16, BEB⁺¹₈, DKL⁺¹₆, GM13b, HCCC11, HLYS14, HPY10, KRM⁺¹₀, KTUI16, LT₁₃, LyWSZ10, MCN⁺¹₈, QMC17, RK11, SAAF11, SSPL⁺¹₃, Tso13, WLZ⁺¹₆, YKMG13, Zhu13, vDKS11].

**communication-efficient** [Tso13, Zhu13]. **Communication-resource-aware** [Wan13]. **communicationless** [DGL19].

**Communications** [FMC19, JTZ⁺¹₆, KSD⁺¹₇, KYEV⁺¹₈, O012, PSM⁺¹₈, RSD19, SSKL16, SMS14, AMN18, Ang16, BC16, DMM10, DZC16, Edw17, FHH10a, Han12, LFGCGCRP14, LLZ⁺¹₂, MLY⁺¹₈, RS15, TKG⁺¹₇, WDZL13, ZYY⁺¹₉].

**Community** [BPS16]. **Commutative** [CLHC12, SLGZ12]. **Commutativity** [ABR12].

**Commuting** [Fuc11, AKG13]. **Compact** [CFOR12, CKLM13, EGG⁺¹₅].

**Compacting** [CPPT18]. **Companion** [KR11]. **Comparable** [XHI⁺¹₇].

**Comparative** [DDR⁺¹₆, MVH15, BKR19, NR11]. **Comparing** [KTM⁺¹₈]. **Comparison** [CGCS12, DWB12, HPC₁₀, KU₁₂, KA18, MZLS18, ST₁₄, HM10, LCM⁺¹₇].

**comparisons** [Mid10]. **compartentiated** [EZ15]. **Compensated** [GKS17].
Compensation [JSZS12, WMU14].

Competition [CPB+12]. Competitive [MD15].

Compilation [CHS15]. Compiler [LWS10]. Compiling [CR10].


Completeness [FKS+13]. Completion [MHW+19].

Complexity [BBD19, BIKK14, BCG19, BW12, DP12, FS15, Gas13, HHS+15, Slp03, AAT16, DJL+12, Jou13, KGO10, LWW+10, SDM14].

Complex [pNyWyY+14, VGA15, BW13, LZKX19]. Complex [MHW+19].

Complete [Ash14, BCEO19, BCEO20, BS14, FLH13, GHKL11]. Completely [Con17, Win17].

Completion [MHW+19].

Complex-Field [GM16b]. Composite [Dun12a, GM16b, ZL19, BBDL+17, NDSA17].

Composite [Dun12a, GM16b, ZL19, BBDL+17, NDSA17]. Composite-Field [GM16b]. Composition [LJS+14, NRZQ15, Ana14, AGH+17].

Component [BKLS18, MV16a, Bre18]. Components [RITF+11]. Composable [DN12, KMO14].

Composing [TW14]. Composite [Dun12a, GM16b, ZL19, BBDL+17, NDSA17]. Composite-Field [GM16b]. Composition [LJS+14, NRZQ15, Ana14, AGH+17].

Comprehensive [GSFT16, YFT17, YJSL18, ZBP18, Bul10a, KA15]. compress [LC13]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16].

Compressed-Domain [WLZL12].

Compressibility [HN10]. Compression [CNT12, DLGT19, DA12, JSA17, LIF19, LD13, MAL10, PMZ13, PP10b, TCN+17, WHZ12, ZSP+19, Ara13, CMMS17, DTZZ12, KV19, LK14, Li10, LPZJ15, PP11, QZ14, RSMA19, SI12]. compression-based [SI12].

Compression/Decompression [PP10b].

Compressive [CCZC13]. Compromise [YNR12b, GBNM11, PX13]. Compromised [DSSDW14, DSSDW17, ZYL+10].

Compromising [BC14, BM18].

Compulsory [QRW+18]. Compute [YHS18].

Computability [Gas13]. Computable [LGH+17, FWS13]. Computation [ARM15a, ARH14, ABPP16, ABL+18, Ash14, Bee17, BDOZ11, CATB19, Fri10b, GST12, GVW12, GHKL11, HP14, HC17, HZX+18, IE11a, Jin10, KW14, KMO14, LHM+15, LQD+16, MMP14, Mal13, NSMS14, PST13, RS17a, SZHY19, SVCV15, SZQ+17, TX16, TM18, Wat10, ABDP15, AB10b, BHH19, DEL19, DGL19, LDDAM12, PHGR16, TG12, YSQM19, vDKS11].

Computational [BBD19, BCO13, GKS17, RD17, RPHJ11, TBCB15, HRS13, SJ19, SDM14].

Computationally [BCEO19, BCEO20].

Computations [ARM15b, CK18, KHPP16, Nac16, PH16, ADMM16, BK12b, LW+19, LR15, SSAF11, TLLM13].

Computer [BGK12, BCG12, BGB12, BD19, Bul10b, DF16, Gas13, IEE10, IEE11b, IEE13, LL15, MS16, Nag19, Niel02, Orm16, PWB17, Roh19, TBL19, T17, Ter11, Vua10, ABBD13, DK12, FGPGP14, PHWM10, Sta11c]. Computer-Aided [BGK12, BCG12, BGB12, ABBD13].

Computers [Mos18, Bre18, Cop06, Cop10b, Dya19, LCKB12, Mac12, MvO11, PHWM10].

Computing [ACM10, ACM11, AMMV18, Abb12, AJA16, Ano17e, BCG+12b, BTK15, CB19, Cer14, CGB+10, DXA14, EAA12, EES10, Gen10, GB19, JWS19, KMSM15, KP17, LCK11, LT14a, LY+13, LCC+15, LGJ16, LNYX15, MLO17, OS16, PAF18, Pet12, RS18, Roh19, SJW17, SLM10, Vai11, Vie12, WRP70, XMLC13, XWLJ16, YE12, YU16, YHL16, ZLDC15, Aab16, AAZ+16, And13, And19, ABR13, BZD16, CXWT19, CZ15b, CSR16, DKL+16, DWZ12, DYZ+15, Dya19, GQH17, Gop19, HSM13, HYS18, Jec13, JSMG18a, KKA14, KKM+13, KKK+14, KSB+17, KH18, LXX+14, LLH17, LLY15, LHL15, MS12a, NR17, Nur19, NCCG13, ODK+17, PPA18, PP11, PKA15, QZDJ16, QRW+18, Rao17, Tan12b, WSC14, Wan18a, WDKV19, WLS14, WL19, XXX15, ZXP+19, XYZ+18, }


CRT-exponent [PT19]. Crypt [HHAW19]. Cryptanalysis [Bar16b, BW12, Bor10, CWP12, CGCS12, DG12, DJG+15, Far14, GST13, Gor10, HK14a, Hin10, IOM12, Jel13, JL18, Kha10, KN10, KWS+12, LH10b, LNM+11, LJF16, LFX+18, LSQ18a, LSQX19, LJ16, MWZ12, MV19, MZ15, NBX13, OTD10, PSOMPL13, SPLHCB14, SM10a, SM10b, TY16a, TG17, Vua10, Wag10, WWVY11, WWY11, WSSO12, WYW14, XQL11, YCL17, YMWS11, AP11, BMB16, BKR11, Bul10a, Bul10b, CJL16, Con12, DMSD18, Eis10, FVK17, Her10, KDH13, LLLK10, LFW+16, Nov10, PT19, RITF+11, SDM10, SDM14, Sun11, SvT10, Tam15, TSSL11, WYL14, WWBC14, AY12a, AY12b].


cryptograms [Shy15]. Cryptographer [Dun12b, Kia11, Pie10]. Cryptographers [Ano16e, BPS16, Goo12]. Cryptographic [Abe12, AMKA17, AD12, ARH+18b, ARH+18a, ÂMVZ12, App15, AHWB20, BME12, BOD19, BEM16, BCGK12, BGB12, Bar15, BCM+15, BCHL19, BIKK14, BLS12, BDP11, BFCZ12, BDGH15, Bla12, BKL+13, BSJ15, BNA15, CCK12, CCK16, CK17, CFE16, jCPB+12, CBL13, CHN+18, Cor14b, CATB19, CFG+17, DB16, Des10a, DQFL12, DR11, Ess17, FKS+13, FY11, FLW12, Gir15, GM11, GLR10, GG11, Har16, HN10, HHH+13, HST14, HSA14, IBM13b, JR13, JHW+19, KOP12, LVV11, LLK18, Loc15, MV12, MKK17, MP12, MKAA17, Muf16, MK12b, NIS13, NA10b, PTT16, PFS12, PS14, PJ12, RMP10, RSBN12, RPHJ11, Rja12, RBHP15, SK11, SEY14, SFKR15, Sch12e, Sev16, SGG11, SPF15b, Shp03, SDM+12, SR14, SOF12, TW12, Tom16, WSL+19, WRP70, XZL+19, YCL12, YNR12a, YNR12b, YS15, ZSY19, ABDP15, AY14a]. cryptographic [ABB+14, ABF+14, ABC+12, ABO+17, BYDC19, Bar19, BFG+14, BJ10a, Bon19, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGJN14, EBP+13, ESR14, GGH+16b, GJJ18, Gil10, GLR13, HYL+19,
Cryptographic-Key [SK11]. Cryptographical [KU12]. Cryptographically [ADD10, BCGH11, BJL12, BKLS18, MC11, NDG17, PLSvdLE10, SVCV15, CBL10, GCH15, HJM11, SA14]. Cryptography [ACZ16, Alz19, Ano15c, Ano15d, Ano16b, Ano19a, Ano19b, App14, AAB17, AG18, ACM17, ARM15b, Bar12, BGK12, Bar15, BBCL19, BRT12, BCGN16, Big08, Bon12, BF19, BKKV10, BJ10b, Buc10, BLM17a, BLM17b, BLM18, BCF14, CNR14, CT18, CJFH14, Cas10, CGMO14, Che17, CST17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK02, DK07, DK15, DXA14, DP17, DBT19, DHLAW10, DF16, DKS12, DR11, Eis10, Elb09, FPS12, FHLD19, Feh10, FSK10, Fid18, FB12, Fre10, GT19, GO17, GFBF12, Gol19, G’13, Gre19a, GPT12, GLW12, Ham17, HEP11, Hes12, HGI12, HR19, HPS08, HKR18, JS18b, JT12a, KM10c, KP10, KAK18, LSL12a, Lin17, LWL10b, LGY12, LMHH14, LGH17, LWHS17, LPO17, MO12, MS10, Mau12, Men13a, MR14e, Mic10b, MST18, MV12]. Cryptography [MMB17, NNA10, NDR19, Nie02, NS12, Orm16, PP10a, PÁBC19, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16c, Sch18, Sch19b, Sen10, SS13, Sen17, SK12b, Sca10, Sca12a, Smi15a, SGS14, Sma16, Sta11b, Ste15a, VS16, VCA19, WWL14, WY12, Wes16, Yam12, Yan11, YTS12, YL17, YYW19, ZZC14, ZAC17, vdtDSHP17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBD13, And19, Anol11a, ABW10, ACK10, BOB13, BB14, Ber14, BL14, BL17, BAB13, Blö12, BSR14, BSW12, BBB16b, CFR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSLY14, DDD14, DA18, Dav11, DD13, DGMT19, Dur15, Far14, GCVR17, GAB19, Har15, HH15, HZW17, Hof19, Hof16, IM14, JLT12, JY14, JW14, KL08, KL15, KD18, KKK11, KK10, KO10]. Cryptography [Kre13, KKD18, KSH18, KSH18b, Lam13, Lan11, LLLK10, Lin14b, LWL10a, Lid12, LY14, MCN18, MS13b, MD12a, MCP15, Mic10a, MHL18, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSAF11, Sta11c, St11l, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA18, YDH15, YR11, YN19, ZXW18, vDKS11, Che11, LJJ1X10, Nas12, Con12b, Auc10, Gas13, Low12, Mei10, Mur10, Ter11]. cryptography-based [BOB13]. Cryptography-Related [Cil11]. Cryptol [Lau12]. Cryptolocker [Ano13b, Ano14a]. Cryptology [BC11, Bro11, Dun12b, LW11a, Nag19, PWBJ17, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPG14, Gili0, GG10, K11a, LH10a, M17a, Pal16, P10, Rab10, HWG10, LT11, Kob10]. Cryptomania [Gen13]. Cryptprocessor [EHKSS19, GV14b, SW10]. cryptoscheme [SLXX16]. Cryptosystem [CCT14, KD19, LH10b, SZHY19, SW10, WSO16, Zaj19, ACD18, AK14a, BS15, Chi13a, Gal13, GV14a, GLB18, IB11, LZ11, LYT10, MM13, MG15, N10, SVT10, yYQWZC13, YY11, YY13, sCR19a]. Cryptosystems [AD11, CLN19, OTD10, PSM17, ZSP19, AHG18, AJY18, AVAH18, BNST17, FWS13, SA16b, ZYM19]. Cryptovirology [YY17a]. CryptRandTest [DB16]. CS [LJ19]. Csec [AD12]. CT [Dun12b, Kia11, Pie10]. CT-RSA [Dun12b, Kia11, Pie10]. CTRL [HKK19].CTRL-PACE [HKK19]. Cube [HJ19, MS12b, WMW19]. Cubic [RW12, VM14]. Cuckoo [BHKN13, sCR19a].
CUDA [DLV16], Cue [KTM+18].
Cue-based [KTM+18]. CueAuth [KTM+18]. cultural [Mid10]. Culture [Bla12, SR14]. Currencies [TSl16b].
Currency [AHWB20, DMO+19, Cou12a].
Current [DP17, GCK12, FPBG14]. Curve [GG11, HB14]. curvature [GJ13].
curvature-feature [GJ13]. Curve [ARM15a, ADI11, ADSH18, ARM15b, BJ10b, FHLID19, GT19, GPT12, LGH+17, LWAS17, MSTA17, NR15, PÅBC+19, PPH12, SG15, vRDSPI17, AMN18, BL14, BL17, BBB16b, Cho14, Far14, FWS13, IB11, Khl18, KKM11, KK10, Kre13, KKD+18, MCN+18, MS13b, MHL18, NZM10, SKH15, WHJ17, YY13, JL16]. Curve25519 [SG15].
Curve41417 [BCL14]. Curves [AMMV18, ACA+16, AK14b, BSCTV17, BWR12a, CMRH17, DW12, Gre19a, LL11, LT14a, MST18, Nag19, PWBJ17, Sch19b, She17, TX16, YTS12, BL17, BP18, FK19].
Custom [ÖDSS17], Customization [OdH12]. cut [Fai19]. Cyber [LJS+14, vdWEG18, GQH17, GHD19, HZWZ18, KSA16, QMC17].
Cyber-Espionage [LJS+14].
cyber-physical [GHD19, HZWZ18, QMC17].
Cyber-security [vdWEG18]. Cybernetica [Ano17c].
Cybersecurity [Bel15, DF16, Hel17, Lan17, LRVW14, Mos18, Sch19a, SDC+17, SPG+19, YK16, AP18, GQH17].
CybSI [KY16]. Cycle [HG12, KU12, MKN13]. Cycle-Based [MKN13].
Cycles [BSCTV17, WBA17, CLCZ10]. Cyclic [Chel18, OTD10].

D [AM19, AP10, Bro19, CG12b, DBPS12, DWWZ12, EAA+16, GZHD12, KWS+12, LJ17, LJ15, MCD12, MKH+12, PGLL10, RS16, SGS14, SRK+17, SRK+18, WSSO12, WK18, WY12, tWmC12, YI14, YPR17].
D-Based [WSSO12]. D-like [LJ15].

D-PUF [SRK+17, SRK+18]. D2D [Gop19, PSM+18]. D2D-Aided [Gop19]. DaaS [AAH+19]. DALP [LWYM16]. Dana [Ano10a]. Dandelion [FVB+18, VFV17a, VFV17b]. Dangerous [HLW12, GIJ+12]. Dao [FMS12a]. Dao-Fa [FMS12a]. Daoism [FMS12a]. Darel [Xie12a, Xie12b]. Darmstadt [FBM12, Sen10]. DASH [KCC17]. Data [AAA+19, ARWK19, Ano13e, ADF12, Bar12, BJL16, BCD+12, BJL12, BW12, BKLS18, CWL+14, CMLS15, CCW+10, CSV15, CCT+14, CLW16, CDM19, CHH+19, DSS12, Dan12, DR12, DK16a, DMS+16, DA12, DCA12, DLZ+16b, Elb09, EKOS19, EKB+16, FYMY15, FYY+19, FPY15, FR+16, GTT11, GRRZ18, HSM14, HWZP18, HLC+18, HLT+15, HVP+18, HZX+18, HK14b, IBM13a, KRKH13, KGV16, KBP18, KD19, LLPY19, LLZ+17, LSL19, LWCJ14, LCP15, LLZ+12, LZC+12b, Ma17a, MLO17, Mal13, MMS17b, MJW+18, MGJ19, MM14b, NNAM10, NR12, PV17, PD14, PSM17, PZL+19, PBC+17, PH12b, PH16, PRRC17, PWS+19b, QZL+16a, QZZ18, RCP+18, Rea16, RDK19, RS14, SAKM16, Sar10b, SMSK18, SP15b, SKH17, Sia12, SC19a, SLM10, SOR16, TCN+17, Tan15a, Vai12, VSV15, WZCC18, WHL17, XNKG15, XWSW16, YD+16, YZDZ19, YJSL18, YMC+17, ZYX16, ZPXX17, ZTL15, ZLZ+17, AP10, AAH+19].
data [ASO14, AIM+19, Ano14, Ano11a, Ara13, ADH17, ALL+18, BLL+19, BC16, BHH19, BTPLST15, BC18, BG16, BVI13, BT15, CD16a, CDGC12, CLH+16, CDF+10, CDL18, DDY+19, DFJ+10, DTZ12, DRD11, DYZ+15, DZC16, ED17, FS18, GHD19, Gen10, GSAMCA18, GLB+18, GZS+18, HKA+18, HSM13, HKA19, HKW+15, HL19, HK19, HMKC12, HH16, HYS18, HYF18, JKA+18, JLC18, JHCC14, KCS+18, Kim16, KV19, KH18, KWH16, LSB14, LT14b,
December [MFH13]. debugging
Debiasing [JHCC14, LW13a, PBP19, PRZB12, SVGE14, BDB14, LP12, SS17b].
Death [Moo14]. deadly [ABL].
Databases [NNAM10]. Data-Oriented [LHF12].
Data-Classifiers [KGV16].
Data-Compression [DA12].
data-independent [BCG16].
Data-Minimizing [BCD12].
Data-Centric [DLZ*16b].
Data-Classifiers [KGV16].
Data-Compression [DA12].
data-independent [BCG16].
Data-Minimizing [BCD12].
Database [BTHJ12, SBV14, WCL*18, AAH*19, BL11, JHCC14, LW13a, PBP19, PRZB12, SVGE14, Suc12, XMY*17, YXD18].
database-as-a-service [AAH*19].
Databases [ABL*18, FCM14, HPC10, JKHeY12, Kaw15, RP12, WP17, GA11, JK13, LCY*16, SS17a, TG12].
datacenters [PRN*19]. Dataset [SP13].
datasets [LVRY10]. DATS [HVP*18]. Daubechies
[Ara13, SM12, ST15]. Daunting [IBM13a].
Day [MMB17, Zet14, Hof16]. Days
[Bai12, Bri11]. DB [FYH*18]. DBDH [CW14b]. DBMS [SERF12]. DC [LHF12].
DC-Net [LHF12]. DCT
[DBB14, LP12, SS17b]. DDI [LZC12a].
DDoS [PSJ13, SP15a].
De-synchronization [XNG*14, AATM18].
deadly [HLV10]. Dealing [Sha13, VN16].
Death [Moo14]. Debate [Bla16].
Debiasing [USH19]. Debs [Sm15b].
debugging [MFH13]. Decade [SOG15].
December [Abe10, BYL10, BC11, Che11, GG10, HWG10, LH10a, LW11a, LTW11, Yan10, Yan11]. Decentralization [JP19].
Decentralized [ABCL17, CD16b, GZZ*13, HMSY12, HK14b, MT17, PPS12a, PAS13b, RVH*16, RSN14, TS16b, XTZ*19, YM19, HHBS18, SLL*19, WZC16]. Decentralizing
[LIW11b]. Deception [GA19, vdWEG18].
Deciding [CLCZ10, Sch12c]. Decipher
[Cor14b]. Deciphering
[Bla16, GMNS15, GSAV18].
decision [PKA15, RPG12]. Decisional
[CCL*19, LZC14]. Decisions
[Bel18a, YWK10b]. declarations
[HWYW14]. Declassified [ABJ13].
Decodable [Yek10]. decoder [PMG19a].
Decoding
[DBPS12, GMNS15, Bax14, Bul10a].
Decomposition
[AGH*17, LSL12b, gWpNyY*14, BWA13].
Decompression [PP10b, SCH*16].
Deconstructing [Tar10]. Decoupling
[DMO*19, IM16]. Decrypt [Kob10].
Decryption [CR12, Tay19]. Decryption
[AN12, KB10, PKTK12, FNWL18, LJW*17, LJWY18, SES*16, SM10a, SM10b, Wu16, XTZ*19, XYML19, ZSW*18b]. Dedicated
[Lin17, Nac12, NSP*18, AKS19]. deductive
[ABF*14].
Deduplication
[CDLW19, MGJ19, QLL17, SKH17, YDY*16, YZDZ19, ZH*19, KH18, SAR18b, ZFH*18].
Deep [BNMH17, CRS*18, DLTG19, FGR*17, HCZY18, Mor19b, RDK19, RHLK18, WYL18, ACM19].
default [BMDT19]. defeated [Kap13]. defects
[FES10]. defences [NDNR13]. Defend
[Alo17e, FDY*19, Sch13]. Defending
[LWCJ14, YFT18]. Defense
[MPA*18, RCK17, YDV19, PSJ*13].
Defenses
[AN17]. Defensive [Pfl10].
Defined [KYEY*18, SAM*18].
definition
[LWL10a, WSC14, YKC*18].
Definitions
[BBD19, GLW12, MAU12, CGKO11, KM14, KGO10, XXWC14]. Degeneracy [WH18].
degradation [MMS*17a]. Degree
forces [CMRH17, KA18, LHW18]. degrees
[MZ17a]. Delay
[CCKM16, GMNS15, LFX+18, LBR12,
MKK17, JLT+12, WX13, MCL+19].
Delegatable [WZ11, XLC+19]. Delegated
[MZHY15, TMC15]. Delegation
[FMTR12, GLJ16, SSW12, XWLJ16, YZ12,
YAM+15, JSMG18a, NAL17, XWS17,
XZP+19, ZWM14]. Deletion
[DMS+16, MGJ19, Rea16]. Delfs [Mur10].
Delivery [PSS+13, SSPC12]. demand
[KKJ+16, LWYM16]. Demand-aware
[LWYM16]. Demodulation [KOP12].
demonstrating [LHA+16].
Demonstration [GKG19]. demosaicking
[HLC16]. Deniability [TCS14]. Deniable
[DF11, zGXW12, HLLC11, GCH+19, HS11,
Jia14b, JXLZ15, LXJ14]. Denial
[BKBK14]. Dense [BFM12]. Density
[Gre19b, LC15, LSQ11b]. density-based
[LSQ11b]. Dependable [BCQ+13].
Dependency [MWES19, SGP+12].
dependent [GdM16, PKA15]. deployed
[MFH13, RY10]. Deployment
[BSA+19, WXX+17]. DepSky [BCQ+13].
Depth [GH11a, RS16, SS10b, SS12a].
Depths [GH11a, SS10b, SS12a].
Depth-Based [RS16]. Derivation
[LBR12, Cha13a, Lau12]. Derivative
[LSQ11a]. Derivative-based [LSQ11a].
derived [JS18a, ZMM+10]. DES-like
[AHG18, CGCS12]. Description
[WH18, PLCGS11]. Design
[AMN18, Abe12, ARH+18b, AIB+16,
ADD10, AUMT16, Bel18a, BKL+13,
DZS+18, DHH16, DR11, FSK10, HSA14,
JLZ18, JWJ+17, KPP16, KW14, KLW+17,
Lop12, MS13a, MFG16, MRL+18, Mur16,
NBZP17, NYR+14, PC16, QLL17, RYF+13,
Sch13, SAAB10, SZDL14, THA+13, VDKP17,
WKB16, WDKV19, YJC18, ZHX16,
BBDP16, CZ14, DRN16, Gor10, KHF10,
KDW+17, MNNW15, MAK+12, MHY+18,
OSANAM19, SVGE14, ZYC+17].
Designated
[WHJ17, HYWS11, RPS10, SY15b].
Designated-verifier [WHJ17].
Designation [Che15, LSQ11b], designed
[Goo12]. Designer [KMY18]. Designing
[CDK+10, DZS+18, FLW12, MRT10, PSD15,
SR10]. Designs [BGK12, PCY+17, KDB15].
desynchronisation [LDC13]. Detailed
[DLV16, ZPXX17]. Detect
[JWJ+17, NSA15, WLP15, Lan11].
detectability [LRW17]. Detectable
[Ess17]. Detecting
[BKBK14, CZ19, Ess17, GAS+16, HWL12,
KW14, SH15, VCD16, YSC+15, LWL11].
Detection [AMKA17, ATS15, ARWK19,
BEM16, CBO+18, DSB15, DF11, GN16,
GZH17, HDWH12, HCYZ18, KU14,
LGL+12, LC15, MKRM10, MKAA17,
MKASJ18, NDC+13, NSMS14, SAJL16,
SBV14, SXH+19, SP15a, SRAA17, SGS14,
TLZ+17, TM18, YFT17, AKKY17, AOT13,
BM13, CB16, HB13, JC13, JVD16,
KKK+18b, KLC+10, LDC13, Maz13,
MMF15, MHT+13, WYL13, vdWEG18].
Detective [Cho10]. Detector [LTK16].
Detector-Based [LTK16].
determination [JK19]. Determine
[FPSF11, Sto12]. Determining
[Bar19, NN12, Scr18]. Deterministic
[MPRS12, NIS12, XXZ12, DTZZ12].
Deterring [WGJT10]. DEUCE [YNQ15].
develop [Ham19]. Developed [Har16].
developers [Ano14c]. Developing
[CH11]. Development
[Pau10]. Developments
[GCK12, Vai11]. Device [ADM19, ABC17,
CFXY17, DFKC17, HSUS11, KLM+12,
SRK+17, SRK+18, TYK+12, ZSH+19,
CRS13, GM16a, KKG14, Kim16, OSP+19,
Par12b, SBHC19, VV19, XHH12].
Device-to-Device [ADM19]. Devices
[AAC+16, ATC17, BDM+19, CSH+18,
CRS+18, DLWW11, EGG+12, FMC19,
GPT12, GdM16, GMSV14, HHH+13,
HDWH12, HFS+19, JMG+16, LFH18,
XWSW16, XZY+12, XWZ+18, YLSZ19, ZXYL16, BSBBG19, CTL12, CBJJY16, CSTR16, DSCS11, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KKK+18b, KH18, KBP17, LDC13, LLY06, LXMW12, LHM14, LZZ19b, NSX+18, NPH+14, PZL+19, PSJ+12, SES+16, SSS11, SM10c, SGM16, WDBZ19, XHM14, YZL+18, YD17, ZSMS18, ZZZ+18. dynamics-based [JZS+10].
dynamical [JT12].

Dynamics [RSCX18, AaBT16, GEAHRI11, LTC+15a, Lidd12, MCRB19, TZTC16].
dynamics-based [AaBT16].
dyslexic [Bha16].
e-commerce [Ano11a]. E-exam [Mor12].
E-Health [AMSPL19, WMX+17, AKS19, IC17, OSP+19, YZL+18, JK+16].
E-Learning [Yon11].
e-mail [BTW15, Sch16b].
e-Passport [HKK19, LZXJ10].
e-Passports [LG10].
e-rental [LY14].

E-Voting [KV18, LGPRH14, KZZ17].
E.T. [Sch16a].
E2 [WYL14].
E2E [KZZ17].

EAC [LZXJ10].

Each [YL+12].

EAP [FLH13, HZC+14, ZCLL14].

EAP-based [HZC+14, ZCLL14].

Ear [GWP+19].

EarpEcho [GWP+19].

Early [Bell8a, Bro11, And13].

Earth [Har14].
easier [MFB+13].

easy [Bell16, SMDST1, Tay14, Wu16, ZD+16].

Eat [DSSDW14, DSSDW17].

Eavesdropping [CWL16, Han12, PX13, YSJJ14].

EbH [GmdFPLC17].

EC [Dra16, CFN+14, CCG+16, CMG+18].

ECB4CI [YZW+18].

ECC [BSSV12, CBL10, HI19, JW+16, KRH18, MMBS19, ZSH+19].

ECC-Based [BSSV12].

ECDSA [BBB+16a, DHB16].

ECG [GmdFPLC17, HZW19, HW19, PLGMCdf18, ZABB17].

ECG-based [PLGMCdf18].

Echo [DLMM+18, GWP+19, HGT15].

Echo-Based [HGT15].

economic [WDZ19].
economy [S16].
Ecosystem [Fri13, RVS+18].

Ecosystems [LDB+15, MMP19].

eCryptfs [XZL+19].

Ed25519 [TV19].

EDAK [ABB19a].

EdDSA [JL16].

Edge [AHM+18, DF16, KAZ18, CXW19, JZU+19, MD15, PR+19, Sun16, XZP+19].

Edge-Based [XZL+19].

dge-centric [AHM+18].

dge-enabled [JZU+19].

Edges [BDL+19].

Edition [Cor14a, Koi10, Gre19b]. Editorial

LSQZ17, OK18, Ano19a].

Editors [BdD19, LLL18].

Education [LRVW14].

Edward [Ano16a, Sim10].

Edwards [ADSH18, JL16, LT14a, YTS12].

Edwards-curve [JL16].

EFADS [WLS14].

Effective [PLGMCdF18, WB12].

Effective [HLLT+15, KRD13, WHLH17, WM+17].

Effectively [YMC+17].

effectiveness [Eng15].

Effects [ASV+18, MAL10, SKV12, SHBC19].

efficacy [ABB12, Chi16, DG17, FRS+16, HRV10, LLM12, LCL+17a, MS13b, WXY16].

efficient [ABB13, ASBD16, ABB19a, BWW16, BCGH11, BG12, BBKL19, BV11, BV14, CG12a, CML+18, CS10, CMLRHS13, CWWL12, CZZ18, CJ13, DA18, DZC16, DWB12, Duni12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTT11, GP+12, GPT12, GJJ15, GH12, GZH17, GCH15, HZC+12, HZC+14, HZL18, HL10b, HBCC13, HZX15, HKL+12, HIFPC15, HCDM12, HH16, HC17, HZLS05, IAD10, JCL+18, KZZ17, KPC+11, Kim15, KHP16, KKK+18a, KH10, LKP+18, LDDAM12, LKT12, LNNH13, LKL+14, LCLL15, LZW19, LSW15, LSSL19, LHY12, LCDP15, LSY+16, LWHS17, LZC17, LLD19, LBOX12, MX13, MTY11, MVVR12, MU12, MP12, MKAS18, MC11, MN14, NES+14, NMDMW16, NZM10, OSP+19, PB12, PAF18, PZL+19, PRC12, PG12, PCPK14,
PNRC17, RSD19, RS17a, RM19, RBHP15, SLL+19, SGY11, SZS14, SOR16, SGM16, TS18, TLCF16, TWZ11, TT12, TM18.

Efficient
[USH19, WDCL18, WLS14, WQZ+16, WCC18, XLWZ16, XMLC13, XMY+17, XHZ+19, YHL16, YNR12a, YNR12b, YLW13, YNYQ15, YLA+13, YS15, ZGY18, ZQWZ10, ZLH+12, ZSW+12, ZJX+14, ZXYL16, ZCL+19, ZHS+19, ZPW16, ZHW15, ZZC17, AQRI+18, AZPC14, AZF+12, ABR15, BBB19, CH11, CCSW11, CLHJ13, CZ14, Cho14, Cra11, CGKO11, EA12, FL+14, Far14, FA14a, FA14b, FIO15, FLYL16b, FZZ+12, FNWL18, GH16, GLM+11, HPC12, HYS18, ISC+16, IB11, IOV+18, JCHS16, JZS+10, KKG14, KV19, KIH19, KL11, KSH18a, KSH18b, LLLS13, LH11b, LH10c, LYW+10, LXMW12, LLH17, LZD+19, LAL+15, MDHM18, MLM16, Mes15, MGB19, Nov10, NSS10, OCGD11, PZBF18, PC14, Rao17, SZZM13, SM19b, THA+13, TTL12, Tso13, TKHK14, VN17, WYL13, WLZ+16, WT10a, WXK+17, XZW16, XWX+17, yQWqZC13, ZLY10, ZLL14, ZT16, ZCC15, Zhu13, sCR19a, LLZ+12, TCL15].

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

Eort
[RSBGN12].

Eort-Release
[RSBGN12].

EGHR
[CML+18].

eHealth
[TMG13].
eID
[SGGCR+16].
eight
[Sun11].
eight-round
[Sun11].

Einführung
[Bar12].

Election
[ADH19, Ess17, RS17b, TKM12].

Elements
[Kra12].

Elevation
[LZC+12b].

ElGamal
[HLH19, ADM19].

ElGamal-like
[HLH19].

Eliminating
[Söd13].

Elimination
[FRQ18].

Elliptic
[AMV18, ARM15a, ADM19, ADI11, AK14b, ARM15b, BSCTV17, CMRH17, DW12, FHLD19, Gre19a, GPT12, KKM11, LGH+17, LHWS17, MSTA17, MST18, NR15, PABC+19, PH12, SG15, Sch19b, She17, vRDHSP17, AMN18, BAAAS13, BL14, BL17, BBB16b, Cho14, Far14, FK19, IB11, Kh18, KK10, KKD+18, MCN+18, MS13b, MHL18, NZ10, SKH15, WHJ17, YY13].

elliptic-curve
[BL17].

Elliptic-Elgamal-Based
[ADM19].

ELmD
[BDM16].

Elsevier
[Ano15b].

Email
[Bel16, CCS14, RS19, XJW+16, WR15].

embed
[KPS10].

Embedded
[Kit10].

Embedding
[CMRH17, FR15, KD12a, MCD12, XNRG15, XNP+18, XZZ18, YE12, ZS12, EA11, LHM13, MKH+12, PWL13].

Embeddings
[FHS13].

Emergence
[BSV12, KSA16, OS16, FPBG14, GLL16, ZHH+17].

emphasis
[GMT+12].

Empirical
[gWpNyY+14, EBFK13, Sar14].

Employees
[Mor12].

EMV
[Cho10].

Enabled
[SMS14].

Enable
[GPT12, HFT16, KV18, QZL+16a, QZL+16b, SG12, SGC16, SSPC12, YSF+18, BM12, JZU+19, NML19, TODQ18, YFT18].

Enabled/disabled
[HFT16].

Emergency
[HLKL15, YTH17, BDM+19, KLC+10].

Emerging
[BS12, KSA16, OS16, FBPG14, GLL16, ZHH+17].

emphasis
[GMT+12].

Encapsulation
[KG19].
Enciphering [CMLRHS13, HMR12, MLCH10, MKASJ18, Sar11]. Enclo"aves [WBA17]. Encoded [DG17, HS18].

encoder [PMG19a]. Encoding [BR14, CK12, TAJF12, XHX17, CJL16, PC14, SM19a, Sun16]. Encounter [NA10a]. Encrypt [RAZS15, Ran14].

Encrypted [ADR18, BTHJ12, BSA19, CWL14, CWL16, Cor14a, CDLW19, CHH19, DWB12, DCA18, FGRQ18, FCM14, FRS16, Fyo19, Gen13, GLG12, GKG19, GZH17, GYW19, HWZP18, HTZR12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kaw15, KGV16, LA15, LGLK17, LQD16, Lop12, Mur16, NBZP17, NNAM10, PBC17, QLL17, Roh19, SAKM16, SZHY19, Sia12, SOR16, TM18, Uto13, Vai12, WBC10, XWSW16, YDY16, ZDL12, ZXY16, ZVG16, AZH11, BBDP16, BTPLST15, BGP17, BKV13, BTK15, BL11, CH11, Cri16, CDL18, DDY19, DKL16, DRD11, DJ19, ED17, FTV10, Gen10, GSAMCA18, GZS18, GSGM16, HKA19, HJ16, JLC18, KH18, LXX14, LZY16, LHL18, LNWZ19, LW11b, LW11c, LW12, LJLC12, LYZ13, LHL14, LLC15, LTZY16, LLL17a, LFX18, LLLH18, LSLW15, LHC11, LSQ18b, LW19, LB13, LY15, LW16, LY18b, LV17, LML12, LLM18, ZMY15, MLO17, MPP14, MR14a, MTY11, MSM18a, MUVR12, MMS17b, MRR17, MRR18, MBF18, MPRS12, MZLS18, MOR19b, MT12, MKRM10, MS11a, Nac16, NDMMW16, NTY12, NMS14, NAL17, OT12, OKG15, ÖDSS17, PMZ13, PR12, PB12, PDNH15, PGRBSAC19, Per13, PKTK12, PPS12a, PYS18, PM12, PCY17, PRSV17, PWS19b, RH16, RCP18, RZZ15, RM18, RSBN12, RDZ16, RVRSCM12, Roh19, SGG18, Saa12a, SSW12, SERF12, Sar10b, SJ19, Sch15a, SLGZ12, SXH19, SZS14, She14, SWF19, Smi11b].

Encryption [Sta12, SGH15, SMOP15, Tan11, TCN17, TCL15, TMC15, Tan17b, TTD13, TKR14, TT12, TFS19, Unr15, Vai11, VSR12, VOG15, Wal18, WCH15, WP17, WDCL18, WSS12, Wat12, WLC12, WDDW12, WZ15, WHL17, WWH12, WMS12, WQZ16, WZCH19, XNK15, XY18, XXZ12, XJW13, XWL16, XJW16, XHX17, YZ12, YZX12, Ye10, Ye14, YH16, YKS12, YQ18, YJC18, ZLY10, ZZC17, ZFH18, ZHT16, ZZL19].

Encrypted [YQZ19, YJC18, ZLY10, ZZZ17, ZFH18, ZHT16, ZZL19].

Encrypting [CC10, Mar10c, dRSdVC12, Cl18, LGFCGCRP14, Pow14].

Encryption [ADM12, AV12, AAUC18, AEH17, Alo12, AAC16, AEP18, Ano13e, Ano14b, Ano15c, Ano17d, Arm19, AKP12, ABF12, AS16, AG18, BVS13, BWWL16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12a, BS14, BV18, BIA16, BKLS12, BDPS12, BHPJP14, BDMLN16, Boy13, BV11, BV14, BVG14, CVML14, CMO16, CLL16, CWWL12, CN12, CZF12, CLHC12, Che15, Che18, CGL12, Chil12, Chl16, CRE12, Con18, CNT12, CLW16, CD16b, DR10, DN12, DFJ10, DSLB18, Des10b, DGFH18, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJH12, Fei19, FLL12, Fuc11, GWW15, GGH16a, GGH17, GM13a, GZZ13, GSW16, GH11a, GH11b, GHS12, GHPS12, GDC16, GV12, GVW15, GM14, GL12, GKS17, Guc16, HSMY12, HLLG18, HZ11, HG12, HWS19, Hor19, HC17, HTC15, HLH19, HP12, Int19, IAD10, JLS12, JWA17, JHL12].

Encryption [Jia14a, JR14, Kam13, KB10, KME12, KMY18, KTT12, KOS16, KKA15, KFOS12, KHPP16, KKK18a, KMJ18, KS12, KHR19, LMGC17, LMG18, Laut17, Led16, LLW16, LLPY19, LW11b, LW11c, LW12, LJLC12, LYZ13, LHL14, LLC15, LTZY16, LLL17a, LFX18, LLLH18, LSLW15, LHC11, LSQ18b, LWZ19, LB13, LY15, LW16, LY18b, LATV17, LML12, LLM18, ZMY15, MLO17, MPP14, MR14a, MTY11, MSM18a, MUVR12, MMS17b, MS17, MRL18, MBF18, MRPS12, MZLS18, Mor19b, MT12, MKRM10, MS11a, Nac16, NdMMW16, NTY12, NMS14, NAL17, OT12, OKG15, ÖDSS17, PMZ13, PR12, PB12, PDNH15, PGRBSAC19, Per13, PKTK12, PPS12a, PYS18, PM12, PCY17, PRSV17, PWS19b, RH16, RCP18, RZZ15, RM18, RSBN12, RDZ16, RVRSCM12, Roh19, SGG18, Saa12a, SSW12, SERF12, Sar10b, SJ19, Sch15a, SLGZ12, SXH19, SZS14, She14, SWF19, Smi11b].
[DKS12]. Even-Mansour [LPS12]. 
Even-Odd [Faa19]. event [CWZL13, CXX+19]. EventGuard [SLI11].
every [Hof16]. everyday [HST14]. 
Everyone [Ano15c]. everywhere [Laz15].
Evidence [Bla12, Lai14, SR14]. evident [MN10].

Evolution [LQY10, Tay17, BHvOS15]. Exact [TKM12]. exam [Mor12]. Examination [MMKP16, VCK+12]. Examining [SP13].
Example [KD12b]. Excellence [SDC+17].
Exchange [CLY14, CST16].

Exhaustive [FMA19]. existing [CJFH14].
Existing [MS16, Sch15b].

Existence [LTC15, F2654hD4].

Expected [DMV15, KOTY17]. Experience [AD12, BSA+19, SK18]. Experiences [HGOZ19, JAE10].
Experimental [LCW+16, DHW+13]. Experimentally [LHA+16]. Experts [Sto12]. Explicit [AQD12, FHS13, HP17, FIO15, ZZC15].

Exploitability [CFN+14]. exploitation [MAK+12, NCCG13]. Exploiting [ACK+10, BDGH15, HJ+19, HL12, VDB+16, VTY18, YDV19, XHYZ+19].

Exploits [ZGC16]. Exploration [AUMT16, ABDP15, RYF+13]. Exploring [Cil11, FNP+15, HPJ+19, HSUS11, KMG17, TLCF16, WHC+15].

Explosion [YY17a]. exponent [PT19, SM10a]. exponentially [RK11].

Exponentiation [EZW18, VN17, WSQ+16]. exponents [SM10b]. Exposing [ERLM16, ZG10].

Expression [WR15]. Expressions [TCMLN19]. Extend [TMC15].

Extensible [YZ12]. Extension [ARH14, DBT19, EKP+13, GFBB12, GT12, RW12, SGY11, HTC17, LYW+10, ZJ+14].

Extensions [FVJ19, LWW10b, RS17a].

Extensive [AIF+19, FVJ19]. external [ZZKA17]. Extract [AN12].

Extract-Transform-Load [AN12].

Extractability [BCP14b]. Extractable [CZLC12b, CZLC14, GGHW17].

Fabrication [FMS12a]. Fabrication-Induced [VDB+16]. Face [AQD12, MHW+19, RSX18, XHH12].

Facial [KRB12, TCMLN19, WSS+19]. facilitate [Chi13a]. Facsimile [Ano16c]. Factor [AMSPL19, ATC17, HXC+11, LCC11, PSSK19, AIB+16, BD18, CLP+13b, CNF+18, DRN16, DMWS12, ED19, GMMJ11, HC12, IC17, JKL+16, JMW+16, Kem11, LNK+18a, LNK+18b, LW19, Lit14, MDHM18, NMX15, SNG+17, WW14, Wat14a].

Factoring [APPVP15, LML12, BG+19, MM13, SD17].

Factorization [COU12b, FS15, HWS+19, KKK+18a].
KFL+10, Kuz11, YAM+15, Mes15, TPL16].
factors [HK17]. failed [And19]. Failing
[Ceri14]. Fails [ABD+15, ABD+19]. Failure
[WCL+18]. Fair [ALR13, CSV15, DSM14,
DG15, WSA15, SEXY18]. Fair-Exchange
[DG15]. Fairness
[ALR13, Ash14, GHKL11, Wag16, MV16b].
Fake [KU14]. Fallen [HCPLSB12]. False
[LLZ+12, MWES19, CDGC12]. Families
[BSS+13, KU12, FK19]. Family
[ARH+18b, BMS12, BKST18, CBXJ19,
DGIS12, DJG+15, FLS+10, FFL12, GNL12,
LYY+18b, MFG16, SMB15, YCL17,
BDPV12]. Fanin [SS12a]. Fast [BLAN+16,
Bru12, CHS15, DSLB18, DGK18, GSN+16,
HMKG19, JGP+18, Kh18, LGLK17, NR12,
PRSV17, Raz19, Rom11, SRRM18, WHZ12,
WBA17, WQZ+13, ZHW+16, FH10a,
KHM13, LNNH13, MBB11, YM18].
FastAD [SMBA10]. Faster
[CNJ12, EZW18, FHILOJR18, HLV17,
TH16, ZSP+19, Ant14]. Fault
[AMKA17, BMS12, BBB+16a, FXP+17,
GST12, JWJ+17, JKP12, JT12a, LYK19,
LGL+12, LCL1W7, LGL12, MSSI17,
MKRM10, MKKA17, PH12a, RZZ+15,
SMB15, SEY14, WCD19, YGD+17, BEM16,
BBBP13, PBC114, WMY16].
Fault-Based [BBB+16a]. fault-resistant
[PBC114]. Fault-Tolerant
[WCD19, WMY16]. Faults
[EFGT18, SMB15]. Faulty [LYY+16].
FBAC [YJW+19]. FBI [Bha16]. FC
[DSS12, Dan12]. FCMDT [BSBG19].
FDM [BD18]. FEAD [ZWM14].
Feasibility
[AAC+16, FKS+13, OMPSP+19, WHC+15].
Feature
[Ber18, SGb+12, YKA16, ZWWW17,
FTV+10, GJ13, HZW19, MHT+13].
Feature-Based [ZWWW17]. Features
[MHW+19, Y114, ZTL15, AAL19, FNP+15,
JS18a, LCM+17, LTC+15a, NMX15].
Feauveau [Ara13]. February
[Ano10a, DDS12, Dan12, Dun12b, K11, Lin14b].
FedCohesion [CCFM12]. Federated
[BS13b, CCFM12, CSM14, MJW+18,
SAM+19a, BMBS10, BSBG19, JAS+11,
TOD18]. federated-IoT-enabled
[TOD18]. Federation [SS10a, NB13].
federations [MMS+17a, ML16].
Feedback [HZ11, Hey17, PYM+15,
SKGY14, ZHI15, LWK11]. Feedback-Based
[PYM+15]. FEIPS [DG15]. Feistel
[BFMT16, KDH15, SAS12, SEHK12]. Felten
[Ano16a]. FESSD [LGL17]. Few [SM15].
FHE [CK18]. FHE-Based [CK18]. FHS
[SP15a]. fi [BMDT19, YNR12a]. FL-BAF
[YNR12a]. Fiat [BD13, B13]. Fibonacci
[FM15, LLP+18]. Fibonacci-number
[LLP+18]. Fidelity [BCP14a]. Field
[Alz19, CLF+17, GPH13, GM16b, HSA14,
SS12a, TGC16, ZAG19, EAB+19]. Fields
[ARH14, BGJT14, HL17, NR15, ZL19,
AA14, BGJT13, C15a, LBOX12, ØS11].
Fight [Ano16f, Wu16]. File
[DMS+16, LY16, T1CF616, XZL+19, ZGC16,
FLYL16b, GSGM16, YHH16], Files
[Uto13, Con17]. Filling [BWR12a]. Filter
[Kaw15, ATKH+17]. filtered [HT17].
filtered-equality-test [HT17]. Filtering
[LLZ+12, CDGC12]. Finance
[Eya17, TBY17]. Financial
[Ano11b, Ber12, GQH17, DDS12, Dan12].
Finding [Hof16, Stc15a]. Fine
[CDD13, PV17, YTH17, ZML17, CLH+16,
FSGW11, LHH+18, XYM19].
Fine-Grained [CDD13, PV17, YTH17,
ZML17, CLH+16, LHH+18, XYM19].
Finely [GT19]. Finely-Pipelined [GT19].
FinFET [ZJ11]. FinFET-Based [ZJ11].
Finder [KLY+12, NSB17]. finger-drawn
[NSB17]. Fingerprint
[DS19, MR14b, AJY18, HW19, KKG14,
LYC+10, ZHL+11, ZHH+17]. Fingerprint-Based
[DS19]. Fingerprinting [QF19, SNCK18, TSH17,
ZS12, FLZ+12, KBP18, RS17c].
Fingerprints [YKY+17]. Finite
[BGJT14, CHS15, GMNS15, HVL17,
HWS+19, WDG19, ZL19, AA14, BGJT13,
CZ15a, GPLZ13, LBOX12, OŚ11].
Finite-State-Machine [CHS15].
Finite-time [WDG19]. FinTech [MZL+19].
Firms [Ano15e]. First [Ano17d, BH15,
DR10, LFX+18, LSQZ17, MS17, PC16,
Wil18, AB10a, BCV12, Bre18, Con17,
Kimi11, 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]. Flaw
[Moo12, SH15, Ste15a, Ano13a, ACC+13].
Flaw-Finding [Ste15a]. Flaws
[DR11, FVJ19, HLV10]. FlexDPDP
[EKB+16]. Flexible
[GT19, JSMG18b, LGWY12, PAF18, TV19,
BGG+13, WDZ19, WLS14, ZL12, ZFH+18].
Flexlist [EKB+16]. Flexlist-Based
[EKB+16]. flip [Bre18, Wal16]. flip-flop
[Bre18]. Flipping [BHT18, CK17].
Floating [EZW18, AKM+15]. Flood
[DHT+19]. flop [Bre18]. Flow
[ATS15, DJ19, HBC+19, WX1+17, CFG+17,
KL13, IWy12, PPR+12, SRB+12]. Flowers
[Hai17]. Flows [CDD13, HKB14, WYL13].
fly [PS14]. Fog [FMC19, JNVS19, Gop19,
JSMG18a, HK18, LWW+19, QRW+18,
Wan18a, WDKV19, ZSW+18b, YXA+18].
Fog-based [FMC19]. Follows [Arm19].
FontCode [XZZ18]. Foolproof [FFL12].
Force [JRF14, CJP12, CJP15]. forensic
[Har14]. Forensics [Ber18, CFXY17,
DLGT19, AKM+11, Har14, QZ14, SM13].
Foreseeable [ATD17, Dya19]. Forex
[DMO+19]. forged [HREJ14]. forgeries
[YQH12]. Forgery [LC15, BM13, LWW11].
forgotten [And13]. Form
[HHS18, DWZ12, Kre13, Khl18]. Formal
[ACF16, EWS14, FVB+18, HK14a, HSA14,
KGO10, PLCGS11, ZW15, Aia15, CDWM19,
THA+13, XWXC14]. Formalization
[LNWZ19]. Formalized [YCR16, NML19].
Formally [KRH18, HKA+18]. formats
[ZT14]. forms [TY16a]. formula [DWZ12].
forthcoming [DGK18, MMP19]. FORTIS
[GSFT16]. Forum [Rau15]. Forward
[ABD+15, BVS+13, BDH11, FLH13,
GSFT16, HLT+15, KME+12, KZG10,
LTH+15, NMS14, WLH15, WHLH17, XM12,
Yon12, YHK+10, YKC+11, ABD+19,
ATKH+17, BML11, NJB19, TCS14, WL19,
YFK+12]. Forward-Secure
[BVS+13, KME+12, LTH+15, NMS14,
WLH15, YKC+11, YFK+12].
ForwardDiffSigs [BAL10]. forwarding
[VN17]. Found [Moo12, Ano13a].
Foundations
[BCHL19, Des10a, Gol19, IEE10, IEE11b,
Lin17, Nie02, SN10, Sta11c, Ter11].
Four [LyWIZZ12, MSL13]. Four-Pixel
[LyWIZZ12]. Fourier
[GJ13, yWpWyYpN13]. Fourth [Kob10].
FOX [LJF16]. FPGA
[AMKA17, Ang16, BCE+10, BYDC19,
BDGH15, CFZ+10, CHS15, EAAAA19,
GBF12, HQ19, HF14b, LDL19, MM14a,
MAK+12, RJV+18, TV19, YT16, ZLQ15].
FPGA-Based [RJV+18]. FPGA/ASIC
[CFZ+10]. FPGAs
[DPG10, GT19, RHLK18, SMOP15, VMV15].
Fractal [JZT+16, KM11]. fraction [IK15].
fractional [BW13, VM14]. Frail
[AAA+19, CHHW12, MCDB12, SSA13,
WK18, ZWZ17a, CCLL11, PGLL10, WHZ12].
fragment [BPP10]. Fragmentation
[BDPS12, CDF+10]. frame
[FMB+18, YQH12]. Frames [DG17, IM14].
Framework [BJL16, CD12, DG17, HXC+11,
KPC+16, KYEV+18, LLG15, LSC+15,
LY15, LQD+16, LNG19, MSU13, SK11,
Scr18, SYC+17, SEK+19, TSH14, VKPI17,
XHZ+19, ZJ14, ATKH+17, BHCdFR12,
CRS13, GQH17, GM13b, HPL+19, JZ+19,
KKGK10, KM14, KS19, MMS+17a, MBF+13, PSO+13, PLCGS11, PAK15, SD10, SA16b, SYW17, SA19, ZYC+17.


Frequency-Based [LWCJ14]. fresh [GJ19]. Freshness [RBNB15]. Fresnelet [FMB+18]. Friendly [Fra16, KCC17, SDZL14, ACM12, BP18, FK19, KLW+16, RD17, WOLS12].

Frontside [DDR+16]. FSR [MD12b]. FSR-Based [MD12b]. Fugue [AP11]. Fujisaki [TFS19]. Full [Arm19, ALR13, DGFH18, HR19, HEC+12, LW12, VS16, WLC12, BKR11, DDM17, LC13, Ran16, SWW+17, SKP15, Tam15, TY16b].

full-hiding [DDM17]. full-text [SWW+17]. Fully [AKP12, BV11, BV14, BGV14, CMO+16, CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, KKK+18a, LMG17, LSLW15, LJY16, LATV17, LSC12, MV12, MSM18a, Nac16, NCCG13, PB12, SGR15, Vai11, VV19, WHC+15, XVZ+18, ZZ12, DDL15, GH13, ZZ1+14, ZML17].

Fully-Homomorphic (GH11b).

Fully-Homomorphic-Encryption [CN12]. Fun [APPVP15]. Function [AMPH14, Bee17, BKST18, BBKL19, CJ13, FL5+10, GKG18, GKG19, GHY18, LJF19, LyWIZZ12, MMS17b, RJV+18, SGY11, WSSO12, YWJ+19, AKY13, ABO+17, AP11, Bar19, BDPV12, CMMS17, Con17, KL14, LP11, RS14, Sar11, SXL16, SCBL16, TQL+14, WYW14].

Function-based [YWJ+19]. Functional [AS16, BV18, BSW12, Boy13, GGH+16a, GVW12, LQD+16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14].

Functionalities [JR13]. Functions [ACZ16, ALR13, BBC+14, BIKK14, BNPW12, BHT18, BK12a, CCL+19, CPS16, DSSM14, DQFL12, FY11, LVV11, NIS15, NR12, Rja12, RW12, SMS14, SLV+16, Tan12a, WCXZ17, YTP11, AY14a, BDP11, BDK16, BC19, C12b, CQX18, CW12a, ESR14, Gen10, HRV10, HL12, Komi18, S10, QZDJ16, WT13]. fundamental [Bre18].

Fundamentals [Joh10]. Further [HCL+14, WHY+12]. Fus [FMS12a]. Fusion [ABCL17, YYK+17, HW19]. Future [AYS15, BCE+12, BKBK14, BNPW12, BHT18, BK12a, CCL+19, CPS16, DSSM14, DQFL12, FY11, LVV11, NIS15, NR12, Rja12, RW12, SMS14, SLV+16, Tan12a, WCXZ17, YTP11, AY14a, BDP11, BDK16, BC19, C12b, CQX18, CW12a, ESR14, Gen10, HRV10, HL12, Komi18, S10, QZDJ16, WT13].

Future-proof [Mon13]. Fuzzy [HWZP18, KRHD13, NC12, SH11, USH19, XJWW13, Alp18, BSBG19, HK17, KMB13, LYC+10, MMS13, SM11, SX14, SC19b].

FV [MRL+18, RJV+18].


Gait [XJR+17]. Gait-Key [XJR+17]. Gaithashing [NMX15]. Gallai [SS10b].

Galois [CFR11, CLF+17, HSA14]. gambling [Aha14]. Game [ADH19, MZA+13, LPPZJ15, P15, SD10, SKEG14].

Game-Theoretic [ADH19, SD10, SKEG14].


Garbling [APP13]. Gard [Kap11]. Gate
[Kar12, EAB+19, JSMG18b]. Gates
[App13, BBKL19]. Gateway
[WZM12a, WZM12b, WL11, WXK+17].
Gateway-oriented [WZM12a, WZM12b].
Gateways [RVS+18]. Gather [Hon17].
Gauss [BPBF12]. Gaussian
[HKR+18, IMERM19, YWL+17]. gave
[Fau19]. Gaze [KTM+18]. GCD
[ABSSS19, KI11]. GCHQ [Ald11]. GCM
[SKK10]. GMC/GMAC [SKK10]. GDLP
[MMZ12]. Gear [AHS13]. Geckos [GSC17].
geese [Bai12]. Gender [Abb12].
GenePrint [HAY+16]. Gener [HYS18].
General [Bar16a, BCKP17, CJX19,
FJHJ12, GFBF12, Gue16, HP12, KOTY17,
LPL15, LNH19, PBL12, SJWH+17, YFF12,
ABDP15, Bai12, DGGN14, GMT+12,
HQZH14, LWS10, WSI2, YC11, ZYC17].

General-Purpose
[Gre16, ABDP15, DGGN14]. generalisation
[LR15]. Generalised [Hes12].

Generalization [GMNS15]. Generalized
[BFMT16, GL19, LPL15, PT19, PC14,
TY16b, Ye14, ZCGZ18, ZAC17, ADG16,
BNS17, KL11, NCI3, YMSH10].

Generated
[ADD10, LCL17b, NN12, XYXYX11, YM18,
AGHP14, CBL10, JS18a, LIW13b].

Generating [No16f, Con17]. Generation
[ABS+12, BCGH11, BH15, GT19, HEP+11,
LKBK19, LTC+15b, MR14a, MJG12,
NIS12, PS14, SOS15, SRK+17, SRK+18,
XJR+17, Aia15, ACD+15, BDK16, CXX19,
GMRT+15, GMDFPL17, GCH15,
KHM13, KKM+13, OMPS1+19,
SGFCRM+18, SPK17, W13, YDH+15,
ZYGT17, ZYGY18, ZHL+11]. Generator
[ADD10, BK12a, CSDK+10, MVV12,
NN10, NKF14, CFY+10, LGK10,
MRT10, PLSTD10, SH11, SM11, XSW10].

Generators [AS17, DSB18, LTKP16,
MFG16, NIS12, PFS12, CP13, GR19b,
HRV10, MG15, S111, Zim10]. Generic
[BWL16, BR14, Chi16, DL17, GWW15,
HXC+11, Sar10b, SY15a, WCL+18, ZCL14,
GM13b, HCY+16, NXS10, YL11b, ZYM19].

generically [MHK14]. Genetic
[JK13, MM17a, ASVE13, EEA13, PTK14].
genius [Hai17]. Genomic
[BKLS18, RCP+18]. Gentry [Ghi11].
Genuine [HR13]. genus [FWS13]. geo
[FG19, Har14]. geo-distributed [FG19].
geo-location [Har14]. geodesices [ZCJ14].
Geographic [LC17]. Geolocation [FPY15].
Geometric
[ACA+16, DSB16, GT11, WLZ12,
YWNW15, CLZ+17, GZHD12, LZW19].
geometrical [TLL13]. Geometrically
[HYW+13]. Geometry
[WM12, CFI11, CZ15a]. geospatial
[HK19]. German
[BDFK12, Bl12, Bu10, Cop10a]. Germany
[FBM12, GLC10, Sen10, Wat10]. Gesture
[LCL17b, RSX18, SCR19b, SHBC19].
gesture-based [SHBC19]. gesture-typing
[SCR19b]. Gestures
[AUM16, KTM+18, GCSAD11]. Get
[GPT14, Sch11]. gets [Con12a, Kum10].

Getting [ESS15]. GF [GT19]. GGH
[CJL16, LH10b]. GH [AK14a]. GH-public
[AK14a]. Ghost [CDA14]. GHZ [CCL+13].

GHZ-State [CCL+13]. giant [Joh15].

GIFT [CWZ19]. girls [Mun17]. Girod
[GMNS15]. given [Bar19]. GLARM
[LL+16]. Glass [Fyo19]. glimpse [Mic10a].

Global [CLP13a, CLH13, MRS+17, GH16,
HL11b, TMK11, ZX11, LNK+18a]. Globally
[CCL14, LG10]. Glyph [XZZ18]. GMAC
[SKK10]. Goal [BMR12]. Goal-Driven
[BMP12]. Goes [BCD+12, RY10].

Goldfeder [An16a]. Goldreich [Lin17].
Goldstrike [BH15]. Goldwasser [Gol19].

Goliath [Sch15c]. Gong [LLW16]. Good
[DQFL12, FY11, Raz19, LSBN14, RY10,
SA14, WT13]. goodbye [HU15]. Google
[Har14, Loc15, VGN14]. Goppa [MBR15].

Gordon [GW14]. gossip [FG19].
gossip-based [FG19]. GOST
Govern [Nor17].

Government [Ano15e].

GPG [Ran14].

GPGPU [CBL10, RVRSCM12].

GPGPUs [TLCF16].

GPU [AHG18, BCGH11, EZW18, GCH15, HBBRMN16, JHCC14, KFE19, LGP19, LFK19, MBB11, ZOC10].

GPUs [AVAH18, VKPI17].

Graded [BR14].

Grain [BMS12, SBM15, FSWG11].

Grained [CDD13, PV17, YTH17, LHH18, XYML19, ZML17].

Granular [SVy19].

Graph [ATS15, GTT11, WH18, GJMP15].

Graph-based [GJMP15].

Graphic [SKH15].

Graphical [BCV12, MC19, CTL12, ENG15, LCCJ13, LWL17, MZL19].

Graphics [HHMK14, ABDP15, KY10, PGLL10].

Graphs [BFM12, KU12, KA18, LBL12, BBGT12, KLN15].

Grassroots [GB19].

Gray [DA10, UUN13].

Gray-Level [DA10].

Great [Acz11].

Green [DCSB16, ZTZ16].

Grey [BCKP17, LRW13].

Grey-box [LRW13].

GREYC [AGBR19].

GREYC-Hashing [AGBR19].

Grid [CGB10, DLZ16, KS15, LPL15, VTY18, AMN18, BC16, CDWM19, DZC16, JAS11, MCN18, WS12, YN19].

Grid-Based [LPL15, WS12].

Grids [SC10, CT11b, GLW13, LWK19, SHY15, JAE10].

Gröbner [EVP10, FES10, Tan15].

Gros [Dan12].

Grostl [ABO17].

Ground [KP17].

Group [AEHS15, BSBB19, BSV12, CZCD18, CGY13, CLW16, DT13, FVS17, HL10a, Har13, LLZ16, LCCJ13, LW17, TW14, XL14, XG14, XZL15, YJS18, ZKH16, AKK17, CML18, GBNM11, HCC11, HPY10, IOV18, LL13, LWS10, LLM19, PY19, RS15, SCBL16, WDZL13, WTT12, YZ18, YLL18, ZZKA17, ZWQ11, ZGL18a].

Group-based [LZ16, CML18].

Group-key [IOV18].

Grouping [LNZ13].

Grouping-Proofs-Based [LNZ13].

Groups [Abe12, GZ12, HWS19, XNK15, YS12, YKNS12, LLY06, MZ17a, WQZ13, ZZ15].

Grover [JL18].

GRS [TD14].

GSR [LC17].

Guangdong [IEE11a].

Guaranteed [TBCB15].

Guarantees [FVB18].

Guerrillas [Has16].

Guess [FSWF11, Fok12].

Guessing [Che15, LCL17b, XJW13, FIO15].

Guest [Ano19a, Gup15, BDD19, LKL18].

Guidance [BD15].

Guide [She17, STC11, Han12, Gre19a].

Guided [CJFH14, ZMS18].

Guiding [DGJN14].

GVW [HL+19].

Psy [SAMP19].

Gyroscopes [SNCK18].

Gurov [JL18].

GRS [TD14].

GSR [LC17].

Guaranteed [TBCB15].

Guarantees [FVB18].

Guerrillas [Has16].

Guess [FSWF11, Fok12].

Guessing [Che15, LCL17b, XJW13, FIO15].

Guest [Ano19a, Gup15, BDD19, LKL18].

Guidance [BD15].

Guide [She17, STC11, Han12, Gre19a].

Guided [CJFH14, ZMS18].

Guiding [DGJN14].

GVW [HL+19].

Psy [SAMP19].

Gyroscopes [SNCK18].

H.264 [JSZ12, JHIN12, LLH12, LW13c].

H.264/AVC [JSZ12, JHIN12, LW13c].

H.264/SVC [MU12, WDDW12, ZLD12, ZLD14].

H.265 [GKB17].

H.265/HEVC [GKB17].

Hastad [Ten18].

Hacker [ZGC16].

Hacking [GHS14, Hea15, JEA15, STA13].

Hacks [Ran10].

Halftone [GL10].

Hall [Ful10, Don14].

Hall-CRC [Ful10].

Hamming [HRK18, CCL11, KSSY12].

Hand [SR12a, Cho10].

Hand-held [Cho10].

Handauth [HBC13].

Handbook [Bec17, AB10b].

Handheld [RPHJ11, CTL12].

Handoff [HZC12, HZC14, XH14, ZBR11, ZCL14].

Handover [HBC13, LBR12, CLM12, CML18].

Hands [Bre18, GPT14, BSS11].

Hand-written [BSS11].

Handshake [KK12, KK13, SM10c, WZ11].

Handwriting [SKV12].

Hands [Mur10].

Haptic [ASVE13].

Hankel [Ye10].

Hans [Mur10].

Hard
Hard-to-Invert [ZWTM15]. Hardcover [Joh10]. Harder [KTA12, Sch16c]. Hardness [AH19, BHNK13, SS13]. Hardware [AW15, AW17, ARH+18a, ADSH18, BNMH17, BRPB13, BDMLN16, BJCHA17, CMLRHS13, DZS+18, DOS15, ERRMG15, GP17, GPR+19, GCVR17, GM16b, GCS+13, HHL+14, HG12, HSA14, HC17, HLN+10, KAK18, LGH+17, LLKA19, LRVW14, MLCH10, MCS+15, MRL+18, MHY+18, NDC+13, NdMMW16, PC16, PG12, RMP10, SN10, Set16, St19, Tay17, VCD16, WOLP15, YSF+18, YDV19, ZL19, ZHS+19, ZAG+19, ZYT13, ZYY19, BDK11, LCL+17a, Sch15c, Smi15a, XZP+19, XZLW15, Ara13, DDM17, HZL18, KWH16, LXLY12, LT14b, SM19a, UUN11, WLH13, WZLW13, ZWM14].

Hierarchies [DMM10]. Hierarchy
[NA10b, VN16]. High
[AW17, ASBdS16, Ano17d, ARM15b, Bar15, BDL+11, CLB19, DM15, DG17, FHLD19, FYD+19, GL12, GCS+13, HKMG19, HZI1, KFE19, KMP+11, KPC+16, KAK18, LTKP16, LCK11, LLY+18, LPO+17, MS13b, MS13c, MM17b, MSR+17, PCPK14, WYCF14, WL11, XNRG15, XLP+18, AHG18, ABBD13, GZHD17, GCVR17, JLC18, KL13, MAK+12, PABC+19, RS17c, WLH13, WXYL16, WZLW13, WKLH11].

High-Assurance [Bar15, KMP+11, WL11].

High-capacity [GZHD12].

High-Dimensional [Ano17d, XLP+18].

High-Efficiency [DG17].

High-Impact [DM15].

High-Level [AW17, KPC+16, ABBD13].

High-Order [FYD+19].

High-Performance [GCS+13, KAK18, LPO+17, CLB19, FHLD19, AHG18, GCVR17, PABC+19].

High-Rate [PCPK14].

High-Security [WYCF14, BDL+11].

High-Throughput [HMKG19, MAK+12].

Higher [LWK12, PRC12, gWpNyY+14, ZSW+12, LWK14].

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

Highly [CD16a, SZDL14, SC19b, ACD+15, DT13].

HIGHT [CWP12, WWBC14].

Hui [HEP+11].

Hijacking [BCFK15, DCAT12].

HILL [KPW13, KA17].

HIMMO [GMRT+15].

himself [Pro15].

Hindering [BTPLST15].

HISS [DT13].

histogram [CSS+13, Lin14a].

Historians [Cer14].

Historical [hai17, Han12].

History [ABJ13, Ano19b, Cer14, Cop10a, LT14b, McK10, McK11, SE16, Sm15a].

history-free [SE16].

Hitler [Hea15, Moo14].

hitting [GR19b].

HIV [GSGM16].

HMAC [GWM16, MAK+12, YGS+17].

HMAC-DRBG [YGS+17].

HMAC-SHA256 [GWM16].

Hoc [LH12, PD14, She14, SS15, XHC+12, BBB19, KM10b, LXJ14, PY19, SGGCR+16, WXSH19].

Hoffstein [Me10].

HOL4 [HK14a].

Holden [Ano17b].

Hole [Ano15d, BKKV10, PC16, YKA16].

Holocaust [Han12].

Home [BD18, HXHP17, KHN+11, KPP16, SYWX19, Cor14a].

Homes [VJH+18].

Homogeneous [HT11].

Homomorphic [AAUC18, AKP12, BV11, BV14, BGV14, CMO+16, CN12, CJ13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHPS12, GHY18, KOS16, KVG16, Kim15, KKK+18a, KHRG19, Lali17, LCLL15, LATV17, MLO17, MSM18a, MSR+17, MRL+18, MBF18, Mor19b, Nac16, ODSS17, PTKK12, RCP+18, RMZW19, Roh19, RJV+18, Tan15b, Vai11, WHC+15, WXX+18, AKKY17, BDOZ11, BC18, CIXX19, CW12a, DMD18, GH13, GHPS13, GLM+16, LLW16, SEXY18, Tan15, WSC14, YJ14, ZJ14, ZY+17].

Homomorphically [SG19a].

Homomorphism [Bra13].

Honey [JR14].

Hop [RWLL14, LCT+14].

Hop-by-Hop [RWLL14].

Hope [BD18, HXHP17, KHN+11, KPP16].

Hoping [RCP18].

Host [BD18, HXHP17, KHN+11, KPP16].

Hosted [SG19a].

hostile [CDA14].

HotCalls [WBA17].

House [Ano16, Bla16].

HP [CGB+10].

HPC [KV19].

Hromkovic [Gas13].

HTTP [BHCdFR12].

Huang [LLSW16].

Huffman [Sun16].

Hui [FMS12a].

Hui-Yuan [FMS12a].

Human [HHS+15, HWZZ19, IA15, DIMT12, HZW19, HW19, LW+10, PYH+18].

Humans [RBNB15, RB17].

Hummingbird- [ESS12].

Hummingbird [ESS12].

hunt [Bha16].

hunted [McG11].

HVS [RMG18].

HWMP [BOB13].

Hybrid [ADI11, ARM15b, JLZ18, JHW+19, KBL11, KKA15, LP12, LLD19, MMBS19, NGAUQ16, OO12, Per13, RCBK19, SGG18, SRT12, XWLJ16, Zaj19, SAM+19a, AM19, BYDC19, EEAZ13, KP18,.
WXLY16, WS14, XWS17, BOB13].
Hybrid-Double [ARM15b].
hybrid-indexed [WXLY16]. hybridization
[MMSD13]. Hyderabad [GG10]. Hyper
[BL14, KÖ14, LZKKX19, WGZ+12].
Hyper-and-elliptic-curve [BL14].
hyper-chaotic [WGZ+12].
Hyper-heuristics [KÖ14]. Hyperchaotic
[GMGCCC15]. hyperelliptic
[FWS13, Kre13]. hypergeometric [YL11].
Hyperledger [BHH19]. HyPoRes
[MMBS19].
i-NVM [CS11], I/O [CDD13]. i2b2
[RCP+18]. IB [CZLC14]. IBBE [SXH+19].
IBC [BOB13]. IBC-HWMP [BOB13].
IBM [ABC+12, AC+15, BAB+13,
HKL+14, JSM+18]. ICA [tWmC12].
ICICTA [IEE11a]. ICISC [LH10a].
ICISSP [Ano19a]. ICN [CHL19]. ICs
[GSFT16]. ID
[Ano17c, CTL13, CDPLCA16, EZ15, HCC10,
IB11, KGO10, LMGC17, LY14, MWZ12,
MM12, MMZ12, Mes15, PLPW13, Rom11,
TPL16, TT12, TTH15, Wan18a, WDZ19,
WT10b, WTT12, HWZZ19]. ID-based
[MM12, LMGC17, MWZ12, TT12, TTH15,
WT10b, CTL13, EZ15, HCC10, IB11,
KGO10, LY14, MMZ12, Mes15, PLPW13,
TPL16, Wan18a, WDZ19, WTT12].
ID-card [Ano17c]. ID2S [YRT+16]. IDEA
[BNY14]. Ideal
[LPO+17, WCL+18, HKT11, yQWQZC13].
idealness [TD14]. Ideas [FREP17, Mac12].
idempotent [Dur15]. Identical [Bow11].
Identifiable [Oka11]. Identification
[CZCD18, FSX12b, FSX12c, FSX12a,
HWZZ19, KG+19, VGA15, YGF15,
YKK18, AGLW16, BOP14, CTHP13, CJP12,
CJP15, DJ19, EA12, HQ+16, HL19, KI11,
KL13, NLY12, WYZ+17, YTM+14,
ZAAB17]. identified [AZH11]. Identifier
[LHW18, GSGM16, MJS13]. identifiers
[Cer18]. Identifying [Bel18b, CZ19, CSV15,
SVG16, ZCSW15, CAM19]. Identities
[KHN+11, LBC18, GLM+11]. Identity
[AHN+18, AQD12, ASM12, ASVE13,
Ano15b, ACAT+15, ASS15, BWLA16,
BCF16, BHG12, BKPW12, BDFK12, Ber12,
Ber17, BS13b, Bow11, Cal13, CCFM12,
CSL+14, CSZ+11, CZLC12a, CZLC12b,
CLHC12, CZLC14, CLND19, CGL+12,
CGY+13, Chi12, dCCSM+12, Fan19,
FFH10b, FZT14, FR15, FSX12b, FSX12c,
FSX12a, GOPB12, GR19a, Gl11a, GY13,
GDCC16, GJJ15, GJZ17, HZC+12, HvS12,
HSM13, HSM14, HXZ15, HYWS11, HYFY18,
JGP+18, KKA14, KRB12, Kuz11, LMG+18,
LYX+19, LMB12, LSL12a, LKAT12, LXJ14,
LLC+15, LTZ16, LSLW15, LH11c, LSC12,
LBR12, MLO17, MHW+19, MFB+13,
MJGS12, MJW+18, MR10, OdH12, Par12a,
PSX+13, PSJ+13, PVWT12, RDZ+16, RS15,
S10a, SG12, SS10b, SS12a, SAAB10, Sch11,
Ser12, SXX+19, SPSC12, SKGY14,
SWW+16, SGH15, TKR14, Tia15, TH16,
THA+13, TMGP13, TAP19, TFS19,
VJH+18, Vie12, VFHF19, WY10, Wan14].
Identity
[WXCH19, XXZ12, XLQ09, XQL11,
XJW+16, YZZ+12, YTM+14, Yon11,
YHK+10, YKC+11, YF+12, YCZ12,
ZLH+12, ZMW16, ZYZ+19, ZDW+16,
ZPXX17, ZYM18, ZYH+19, ZTZR12,
vdWEG18, ATKH+17, Ano13f, BMBRS10,
BOB13, BSBG19, BMM12, BBGT12,
CTHP13, dCCSB+16, DZ14, Din10, DWZ12,
FA14b, GMRT+15, GR19b, GPVCdBR012,
HPJ+19, HZC+14, HWDL16, HZWW17,
HLR11, HFCR13, HB10, HB12, HL11,
HP10, Hwa11, JCL+18, JZ+10, KKGK10,
KKM+13, KL11, LKLL13, LK12, LMXW12,
LCT+14, MMS+17a, MD15, MGP10, MJS13,
MLM16, MM13, NLC13, NML19, ÖSL11,
PZL+19, PLCGS11, QYWX16, RG10,
Rom12, SSY12, SE14, SE16, SR10, bSZ15,
SA16b, Sim15b, SSAF11, SSS11, SGM16,
VGL14, WWYZ11, WWYY11, WSC14,
WLFX17, WMX+17, Wan18b, WWXMZ19, WHZ19, Wat14b, WWW17, XW12, XCL13, XHM14, YWL+17, YWJ+19, yYqWqZC13, YYS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZMYB17, ZZ12, ZYM19.

Identity [LZJX10, PN10, Sar18a, Kat13].

Identity-as-a-Service [VFFHF19].

Identity-authentication [NML19].

Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CLND19, CGL12, CGY13, Chi12, FHH10b, FZT14, FR15, FSX12b, FSX12c, FSX12a, GY13, GJ15, GJZ17, HZC12, HSM14, HZX15, LMG18, LYX19, LSL12a, LSL12, LLC+15, LTZY16, LSLW15, LH11c, LSC12, LBR12, MLO17, RDZ+16, SGI15, TKR14, TFS19, Wan14, WZCH14, XZJ16, XJW16, YZX+12, YHK+10, YKC+11, YFK+12, YCZ+12, ZLH+12, ZMW16, ZYH19, ZPX17, ZYM18, ZYH+19, CSZ+11, HSM13, HYWS11, HYF18, LKAT12, LJJ14, MJG12, RS15, SXH+19, SWW+16, Tai15, TH16, ZDW+16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HWDL16, HZWW17, HLR11, HWB10, HWB12, HL11, HPY10, Hwa11, JCL+18, LK12, LCT+14, MJS13, MM13, NCL13, PZL+19, QYW16, RG10, SE14, SE16, hSZ15, SA16b, SSAF11, SGM16, WLFX17, XW12, XCL13, YWL+17, YWJ+19, yYqWqZC13, YKC+12, YXA+16, ZZ12, ZYM19, LZJX10, Kat13].

Identity-Enabled [SG12].

Identity-Hidden [PSS+13].


IEEE802.16e [HLC11]. if [ABJ13, Pec17, Rus15]. IFIP [GLIC10]. IFP [MMZ12]. IFFT [BD18]. Igor [Sha10]. II [Mun17, SCBSN10b, SMOP15, ZWS+18]. III [SMOP15]. ILA [HZS+19]. Illegal [ABJ13]. Illinois [Nor17]. Illogical [Hel17]. Illumination [KLY+12]. Illusion [GHS14]. Illustrated [Cop10a]. Im [BGI10, BGI+12]. IMA [Che11]. IMACC [Che11]. Image [BS11, Bai10, BAAS13, BDB14, BWR12a, CJFH14, CCC19, DA10, DCM18, DS19, GRRZ18, HD19, IAD10, JKH+12, KPS10, KLC+19, LA15, LLL17, LFX+18, LLLH18, LZKX19, MBC15, MAL10, MS+18b, PWW10, QJC+18, RS16, RVRSCM12, SH11, SM11, SZY19, SJ12, SGP+12, SMS18, SS17b, SSA13, SRAA17, SZST18, TB18, VFG19, WHZ12, WZXL12, WY1W+13, WYCF14, yWVY+18, WYK12, WYL18, YLL+12, YWWN15, Ye10, Ye14, YX16, YX18, ZZZ+11, ZWW17, ZWZ17a, ZWZ17b, ARG19, AM19, BWA13, BM13, Bro19, CT11a, CW14a, EA11, FMB+18, GKCK11, HAK19, HLC16, KMG17, KM11, KKK+18b, LCM11, LW10, LWL11, LW13b, LHZJ15, M114, MS17, NES+14, PTK14, SE18, Sch12a, SM13, SM12, SN14, ST15, SGFCRM+18, Sun16, JT12b, TTL10, TLL13, UUN11, UUN13, yWpWpN13, WDG19, WHZ+19, WZG+12, WSS+19, WKH11, WOL12, XSW10, YWL+17, YCL11, YCC16]. Image [YSC16, ZLW+12, ZT14, ZSMS18, ZL12].

Image-Enabled [CJFH14].

Image-Scrambling [LLL17a].


Imperfection [ABD+15, ABD+19, BHvOS15].
Impersonation [AATM18, GBNM11].
Implantable [BDM+19]. Implants
[Mict16, SSPL+13]. Implausibility
[GGHW17]. Implementation
[AAUC18, BW16, BKLS18, BSJ15,
BDMLN16, EGG+12, FHLOJRH18,
FHLID19, GP17, GL12, GPT12, GM16b,
GCS+13, HMKG19, HJ19, HF14b, JLZ18,
KB10, KG16, LYL+18, MFG16, MAS16,
NdMMW16, QLL17, RMP10, Sec18, TV19,
VKKII17, ZPM+15, AN18, Ang16,
BDP+12, GH13, GAB19, HBBRM+16,
KFE19, KY10, KSH18a, KSH18b, MM14a,
MNNW15, NES+14, PBCC14, SK14,
SAAB10, SVGE14, SF12].
Implementations
[BFCZ12, BFK16, BDGH15, BJ10b, Bru12,
CMLRHS13, CBL13, ERRMG15, EKOS19,
GZSW19, LGH+17, MLCH10, MWES19,
NDR+19, SJKI18, SG19b, Tom16, VV19,
YZLC12, ZSH+19, ABBD13, ABF+14,
BFG+14, BJ+14, CFN+14, CGH17,
LBOX12, RSMA19, Sta11c, ZSW+18a].
Implementing
[Dav11, GH11b, HTZR12, KV19, LTC+15a,
SG15, SVGE14, SLM10, VOG15, SA16b].
Implications
[DK16a, OSH16, SC19a].
Implicit
[BBD19, HP+17, DZW12, SSNS15].
Imply
[ALR13, LRW17].
Importance
[TC10]. Impossibility
[ACM+17, BCF+14, Mat14]. Impossible
[Blo15, CWP12, LJF16, TSSL11, WYL14,
WW12, MNP12, SDM10, SDM14].
improbable [TS16a]. Improve
[AQD12, PM19a]. Improved
[Ber18, BCP14a, Chi12, CGKO11, DL17,
FVK17, GLSN12, GR19a, HLS18, HJI+19,
IK15, JLH12, KZG10, LTA14, LWZ12,
LJF16, LJF19, LHH11, LCCJ13, LC15,
LY+18, LSG+19, LML12, MM17b,
PH12a, QZ14, SK12a, SEHK12, SS10b,
SP15a, TS16a, WCD19, WLC12, WWBC14,
YHHS16, ZJ11, ZLDD12, ZZL+19, CNF+18,
CBL10, GLW13, HWB12, Nam19, PWLL13,
SD10, XHH12, YSQM19, Wan14].
Improvement
[FRS+16, LFX+18, LYL+18,
LJ19, MWZ12, PLP13, AN15, BMB16,
CHS11, Far14, LNM+11]. improvements
[EA12, HRV10, Tso13]. Improving
[AB15, BCM+15, Chi16, FMS12b, GMS11, HLC11,
MHC12, Sar10a, SS11, YWF18, YKS10].
impulse
[LZX+19]. IMS
[GI11, MEF012, VGL14]. in-browser
[ABR13]. In-Memory
[PAF18]. In-Order
[ZBP18]. In-Situ
[GRR18]. Incentive
[SS10b, TS16a, WCD19, WLC12, WWBC14,
YHHS16, ZJ11, ZLDD12, ZZL+19, CNF+18,
CBL10, GLW13, HWB12, Nam19, PWLL13,
SD10, XHH12, YSQM19, Wan14].
Improvement
[FRS+16, LFX+18, LYL+18,
LJ19, MWZ12, PLP13, AN15, BMB16,
CHS11, Far14, LNM+11]. improvements
[EA12, HRV10, Tso13]. Improving
[AB15, BCM+15, Chi16, FMS12b, GMS11, HLC11,
MHC12, Sar10a, SS11, YWF18, YKS10].
impulse
[LZX+19]. IMS
[GI11, MEF012, VGL14]. in-browser
[ABR13]. In-Memory
[PAF18]. In-Order
[ZBP18]. In-Situ
[GRR18]. Incentive
[SS10b, TS16a, WCD19, WLC12, WWBC14,
YHHS16, ZJ11, ZLDD12, ZZL+19, CNF+18,
CBL10, GLW13, HWB12, Nam19, PWLL13,
SD10, XHH12, YSQM19, Wan14].
Improvement
[FRS+16, LFX+18, LYL+18,
LJ19, MWZ12, PLP13, AN15, BMB16,
CHS11, Far14, LNM+11]. improvements
[EA12, HRV10, Tso13]. Improving
[AB15, BCM+15, Chi16, FMS12b, GMS11, HLC11,
MHC12, Sar10a, SS11, YWF18, YKS10].
Influence [RSCX18]. Information
LK18, LJY16, Pas13a, PPR+12, Yan14].

_interceptor_ [Cho10]. _Interceptors_ [Don14].

Intercloud [DCA19]. _Interest_ [Sch19a].

_interface_ [WBA17], _interference_ [BBCL19]. _Intermittent_ [VJH+18, CL16].

Internal [LCR+18]. International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FBM12, GLIC10, JY14, LCK11, LW11a, LTW11, MV12, PJ12, Sen10, TT18, Wat10, Yan10, Yan11, AB10a, Abe10, Ano11a, BYL10, BL10, Gil10, GG10, HGW10, LH10a, IEE11a].

Internet [Ano13f, LFHGCGR14, TW14, AAC+16, Ano13d, AKS19, BCHL19, Bel18b, BLU+15, CLF+17, CCMB19, CW12b, CEL+19, DRS16, DG15, FREP17, FMA+19, Fri13, Gel13, GMDR19, HKA+18, Ham19, HZL18, HEP+11, JKA19, JTT+16, KHRG19, LNK+18b, LW19, LGH+17, LSG16, MJGS12, MJ313, MLS13, MCF17, NLLJ12, NLY15, Orm16, PLGCD18, SB17, SXH+19, SS19, Sö13, SYV+19, SYW17, SYC+17, SKEG14, VWC19, WCCH18, XLC+19, YCT15, ZDZH18, ZSY19].

Internet-Draft [MCF17].


_interplay_ [JW14].

Interpolation [JTZ+16, KU14].

Interpretation [MZ17b].

Interpretation-Based [M17].


Intrinsically [SRK+17, SRK+18]. Introducing [Ano16g, Fay16].

Introduction [AG18, BCHL19, Bdl19, DK02, DK07, DK15, G13, G13, Gre19b, HPS08, JSK+17, KL08, KL15, LKL18, Low12, Mei10, Men13a, Sch15a, SOG15, Sta11c, Big08, CM13, Buc10, Led16, Sch15a, Ful10, Mur10].

_Intrusion_ [NSMS14, SAJ16, SBV14, YKC+12, MMF15]. _Intrusion-resilient_ [YKC+12].

Invention [ORM16]. invents [Ant14].

Inverse [JS18b, RMTA18, RMERM19].

Inversion [NSMS14, SAJ16, SBV14, YKC+12].

InvisiMem [AN17]. INVISIOS [AARJ12].

Invited [SS19]. Involution [BRL].

Involvement [LKB19].

IoT [AATM18, AMSPL19, AMKC19, APMCR13, BD1+19, BBTC20, CC17, CSH+18, FQZ18, FMC19, GA1+18, HHBS18, Hod19, KKK+18b, KKD+18, LSQ15, LZZ+19a, MMP19, NVM+17, OSANAM19, PCK19, RC18, SSSA18, SG16, SJKL18, TODQ18, TG17, Wan18b, WCFW18, WXY+17, XYL19, YWJ+19, YFT17, YFT18, YTH17, ZCWS15, ZLY+19]. _IoT-Based_ [YTH17, ZLY+19]. _IoT-Enabled_ [SGC16].

IoT-FBAC [YWJ+19]. _IoTs_ [SAJ16, ZSW+18a].


iridescent [YW+17]. _ISDN_ [Ano15b, Ano17b, BAI12, JOH10, MUR10, SCH15a].


Lattice [ADM12, Ano11b, AYS15, BSJ15, EM12, EFGT18, FGM10, GCH+19, HPO+15, HKR+18, LNZW19, LPO+17, MLO17, NDR+19, PG12, AAT16, AWAH18, Dra16, LLM+19, MGB19]. Lattice-Based [ADM12, Ano11b, AYS15, BSJ15, EM12, EFGT18, HPO+15, HKR+18, LNZW19, LPO+17, MLO17, NDR+19, PG12, GCH+19, AAT16, LLM+19]. Lattices [Boy13, LYY+18a, LYX+19, Lau17, TH16, XZX12, ZQQ15, KRE13, TIA15, XLWZ16, yYQWqZC13]. launch [Zet14]. LAUP [BNH19]. Laurent [Ano15b, Ver17]. Law [Bla12, SR14, Wu16, AOT13]. Layer [HQY+18, LHM+15, PRGBSAC19, ZNH16, HQY+16, LKKL13, ZHH+17]. Layered [Bel19, BS14, GRL12, WWL+14, JCHS16, Tan18, ZC12]. Layering [YYK+17]. LBlock [KDH13, MNP12]. LDGM [BBC+13]. Lead [Arn19]. Leader [ADH19, TKM12]. leads [Ano14a]. leak [BBG+17]. Leakage [AV12, Bar16b, BKKV10, CBRZ19, CBL13, DCA18, DHB16, FPS12, GDL18, HHH+13, HHP17, HHS18, IL15, Kom18, LTZ16, LSQZ17, NTKG17, NTY12, Pan14, SGH15, TTH15, WNW18, ZXY+12, YZLC12, YZ12, YCYZ12, ZYT13, ZWMT15, ZM16, ZM17, ZY+19, ZY19, ZY17a, ZY17b, ZYM18, ZYH+19, ZBP18, ABC+18, CQX18, DLZ16a, DMWS12, GV14a, GLL+18, HYL+19, LLG19, GSP+17, YLZ+16, ZWM14, ZCC15, ZYM19]. Leakage-Free [IL15, LSQZ17, TTH15].

Leave [GA19, CMG+18]. Lecture [He17].
LED [SI12, JKP12, MRTV12]. Ledger [Mu16].
Leeds [vDKS11]. Left [BBG+17].
Left-to-right [BBG+17], Legacy [CS12, Smi11b, CGH17]. Legal [ZTSR12].
LeGall [Ara13]. Legislation [PH12b].
Legitimacy [MI16]. Lemonade [DFKC17].
Lemons [DFKC17]. Length [AS17, GT12, Gir15, PDNH15, PNRC17, Zha12].
Length-Doubling [Zha12]. LIGHT-WEIGHT [SWF].
Lifting [LSL12b]. Lifecycle [Tan15a].
Levels [HLC12, MRT10, WGD18].
Libgcrypt [ADD10]. Libertarian [Sch12b].
Library [Fel13, HHAW19].
Lexicographic [ZAC17]. LFSR
[HLIC12, MRT10, WGD18]. LFSRs [QGGL13]. Liability [Bra13]. Liars
Library [ACZ16, Bec17, BLS12, FLW12, KRH18].
Licensing [EAAA19]. Lie [HWS+19]. Life
[MKN13, SCMS18, McK10, McK11, War11].
Lifecycle [Tan15a]. Lifetime [HSUS11].
Lifting [LSL12b]. Light [JEA+15, SWF+19, PCK19, SJ19, ARH+18a].
Light-Weight [SWF+19]. lightning [Ran10]. Lightweight
[ADM19, AMSPL19, AMKA17, AARJ12, BNNH19, BCHL19, BSS+13, BFM16, BKL+13, BM11, CGCGPDMG12, CWP12, CCF17, DS11, ESS12, EKP+13, FVB+18, FQZF18, GNL12, GAI+18, Gop19, GMVV17, GMSV14, HZW18, HCETPL+12, IS12, IOM12, KE19, MO12, MFG16, MPM+17, PCDG14, SBS18, She14, YN19, ZYW+13, ZSY19, ZLY+19, ZSH+19, AMN18, AATM18, AMK19, AKKY17, BLL+19, BC16, BB19, Bor10, BB16b, CL11, DA18, FLL+14, GH15, GTSS19, KDH15, LLZ+16, MCN+18, MNP12, MV15, MHY+18, OSANAM19, PJ18, PSIo+13, SGJ+18, Tan12b, TG17, WLZ+16, WCFW18, WWBC14, XWZ+18, XXCY19, XHM14, YCT15, ZZY+19, ZSY+18a]. Like [BW16, ERLM16, HP17, WJ19, AHG18, CGCS12, CJZ13, HLH19, KO16, LJ15, LJ16, RS14].
Lilliput [BFMT16]. Limitations [CK17, DR12]. Limited [DFKC17, ZZC17].
Limited-Use [DFKC17]. Limits [AS16, GV14a, KS12]. Lindell [Fu10]. Line
[FFL12, LKBP19, YMWS11]. Linear [BCT+13, BW12, CGCS12, CMA14, EKP+13, FGMP12, HK14a, LGLL12, LJ15, LJ16, LFW+16, WGF16, YCL17, BBEP14, Bul10a, DMS18, FES10, GMGCCC15, Her10, HCCC11, LWK11, OSh11, SA14, XSWC10]. Linear/Linear [EKP+13].
Linearly [ADD10]. Lines [HR19].
Linguistic [OO18, OO10, OT10]. linguists [Maf16]. link [Ham12, VS11].
link-state [Ham12]. Linkable [YLA+13].
Linkage [RCBK19]. linked [JCHS16].
linking [SGSM16, NPH+14]. Links
[PRGBS19]. Linux [Fe13, HHAW19].
Lipreading [OS12]. LISA [PC19].
LISISAP [VS11]. List [AEHS15].
Listening [Lane17, Sch16a]. Listless [SS17b].
literature [IAC+19]. live [ZZC14].
live-wire [ZZC14]. Liveness
[HCY18, OS12]. Lives [Acz11, McK12].
Lizard [MSS+18]. LLL [NV10]. Load
[AN12, FXP12, PRn+19, SG19a]. Loc
[CDPLCA16]. Loc/ID [CDPLCA16]. Local
[pNyWyY14, TM11, V15, WY+13, LMJC11, LW+10, PTK14]. Locality
[Kaw15, NCC13]. Localization
[SRAA17, GAI+18, NC13, SCY15]. Locally
[Yek10]. locating [ZY+10]. Location
[AV18, JP19, Kin11, PSd15, PIA15].
RSX18, SNCK18, VKK+19, WPZM16, WK18, CXX+19, CHX13, Har14, JK19, LWYM16, NZL+15, PC14, YXA+18.

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

Location-dependent [PKA15].

Location-Privacy [PSD15].

Locations [KD12a, Alp18].

Locator [LHW18, MJS13].

loci [FES10].

Lock [YTF+18].

Locking [AB15, FHS13, LCW+16, LHA+16].

locus [HPJ+19].

Loève [BCPV11].

Loop [YKK18, PGLL10].

Log-polar [YKK18, PGLL10].

Logarithm [BGJT14, CLL16, VM14, AMORH13, BGJT13, MM13, Mes15, TPL16].

Logarithms [BGG+19].

LogCA [AW15, AW17].

Logging [YNR12a, YNR12b].

Logic [Che18, Cil11, DGP10, He17, Nie02, RZZ+15, Ter11].

logical [CO11].

Logistic [JHW16, ABSS17, Bai10, BCO13, JK19, LH19, CHX13, Har14, JK19, LWYM16, NZL+15].

Low-area [ABO+17].

Low-Bandwidth [GST13, NR11].

Low-Bit-Rate [LJK17].

Low-complexity [DLJ+12].

Low-Cost

[ABC+17, GI12, LZZ+19a, Man13, NVM+17, LEW19].

Low-Distortion [FHS13].

low-end [Ch13a].

Low-Latency [BCG+12b].

low-level [CJL16].

Low-Overhead [AWSS17].

Low-Power [SAJL16, WT10b, FMC19].

low-resource [FQZF18, MH15, ZPZ+16].

Lower [BCG19, LKI9, Sha10, Shp03].

LP231 [LKI4].

LPM [LD13, PJ18].

LPN [HLK+12].

LPSNR [LP12].

LR [YJ12, ZWM14].

LR-FEAD [ZWM14].

LR-UESDE [YZ12].

LSB [DA10, LH13, Tan12a].

LTE [CLM+12, DLK+15, LLS13, QMW17, SGC16, TM12].

LTFs [ZY19].

Lucas [RW12].

Lucia [DDS12, Dan12].

Lucky [AP13].

Lumpur [HWG10].

Luo [RSD19].

LUT [HF14b].

Luther [ABJ13].

LWE [BV11, XY18].

LWT [TB18].

Lyra2 [ASBdS16].

LZSS [CFY+10].

M [Orm16, Ver17, Hs12].

M-Identity [Hs12].

M2M [TKG+17].

MA [ACM10, TT18].

MAC [Kem15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, OPS14, VN16, WCXZ17].

MacGuffin [LGL+12].

Machine [AGHP14, An16d, CHS15, GN16, KD19, Sch12a, TKG+17, ABBB13, GJ13, GSA18, Gup15, LLZ+16, LHA+16, QMC17, RY10, TTL10, War11, WS14, TKG+17].

Machine-generated [AGHP14].

Machine-learning [KD19].

machine-to-machine [QMC17].

Machines [Ber16b, HB17, BBDL+17, KSKU13, PWW10].

Macrakis [Kem15].

MACs [DL17].

MacWilliams [ÖS11].

Made [Orm16, Sna16, SD18].

Magic [KÖ14, PHN+12].

Magnetic [VDB+16].

Magnifying [DKL+16].

Mail [BTW15, Sch16b].

Main [AMH+16, LY15, ZHZ+19, CS11, HHA19].

Maintaining [WP15].

Make [Aux12, BP06].

makes [Kem11].
Malaysia [HWG10]. Malicious
[AAE+14, ARWK19, BL15, BL16, Mor19a, TM18, VGA15, BK12b, ONSZ19, WTT12], malleable [KTT12]. Malleable
[CKL13, DPW18, MSas12, CG14a, FMNV14, LP11, MSas13, OOR+14, Pas13a]. Mallory [FHM+12]. Malware
[ATS15, GN16, GAF+15, JC13, OMNER19, Uto13, Ano14a, Goo12, KGP+19, Yaa19]. man [And13, Bat10, Kap13, Moo14]. Management
[ASM12, ABB19a, BD15, Bar16a, BS13b, CCFM12, CSL+14, GOPB12, Gla11, KP12, KKA14, Lop15b, MKF+16, MJW+18, MK17, MMHSGH16, PN10, RC18, TMGP13, Vie12, YZDZ19, YZX+12, YSS14, ZJ11, ZTSR12, BMBS10, BSBG19, BBi16b, CFL13, Cha13c, dCCSM+12, dCCSB+16, Din10, KH18, MLMSMG12, MGP10, PLCGS11, Sch11, SK18, SR10, SA15, SWW+16, SCRL16, THA+13, WSC14, WDV18, WKDVK19, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b]. Manager [KKA15, Kim16]. Managing [Lal14, MD15, BC18]. MANET [KTUI16]. MANETs [Yan14, ZYGY18]. Manhattan
[CBL13, LHW18, MS17, JS18a, MM14a]. Mappings [MC11, CDPLCA16]. mapreduce [DMD18, LJL12]. Maps
[Ye14, BAAS13, BSBG19, KCS+18, KLW+16, LWW+19, IW10]. maps-based [LWW+19]. March
[Ano10a, Cra12, DDS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, WZM12a]. Marche
[GZSW19, WH17]. Masking [HF14b, PYM+13, USH19]. Mass
[BPR14a, BPR14b]. Masses [Ano15c, BCHC19]. massive [FLYL16a]. Master
[Dew11, LYX+19, Man10a]. Matching [Lin15, RCBK19, Tan12a, DA18, LHM13, MR14c, MHT+13, PPTT15, SS17a, SM10c, YZL+18]. MathCW [Bee17]. Mathematical
[Bee17, FGPGP14, Ham17, HPS08, IBM13a, Me10, Sch15a, Wes16, KM14, OO10, Stat11c]. Mathematical-Function
[Ano17b, Ayu12, BP06, Led16, Nie02, Sch15a, Ter11, CM13, Kra12, PHWM10, Wes16]. MATLAB
[TRD11]. Matrices
[AMVZ12, BNA15, AKG13, FES10]. Matrix
[BFMT16, IAD10, KKK+18a, LYY+18b, SK12a, TDTD13, Ye10, Cha13b, LLM+19, TK14]. matrix-vector [LLM+19]. Matter
[Rau15, SS12a, DKA+14]. Maturity
[ABPP16]. Max [And13]. Maximizing
[DBPS12]. Maxims [Kob10]. Maxwell
[LGZP19]. May
[BL10, FBM12, Gil10, IEE15, Sen10]. maze
[LLC10]. mbedTLS [YGS+17]. MC
[HIDFGC15]. MC-2D [HIDFGC15]. McEliece
[DN12, GV14b, MBR15, MT12, MG15, OTD10, SWM+10, VOG15, Zaj19]. Mclaughlin
[GL19]. McOE [FFL12]. MDPC
[GAB19, HC17, VOG15]. Me
[Will11, XHH12]. Mean
[SZH19, TTL10]. Meaningful
[LTC+15, SA16a]. Means
[KRDH13, AMHJ10, Kam16, LG10, Pal16,
SG19a. Measure [DDD14].
Measure-independent [DDD14].
measurement [QLZ19, VGN14].
Measurements [DTE17]. Measuring [MMF15, DMWS12]. Mechanical
[MMF15, DTE17].
Mechanism [ABB19a, KG19, KD12b, LL15, LLY+18, Lin15, PPKT12, Saa12a, SMOP15, ZHS+19, BBT120, CL11, FP12, KJJ+16, MCRB19, NXS10, PLPW13, PSJ+13, WB12, YXA+16, ZWM14]. Mechanisms [CBO+18, CCC19, GPR+19, JWSN19, JSK+17, SAG18, FHH10a, KSA16, MMZ12, PLGMDf18].
Media [KBL11, FHL10a, vdWEG18]. Mediated [Fra16, YHK+10]. Medical
[BDM+19, KBL11, UUN11, AIA+18a, AM19, AMK12, KCS+18, KSA16, AMKC19, KLC+10]. Medicine [MA17b, LWK+18]. MEIDSN [KLC+10]. Meet
[LJ17, LJ18, LYD+18, LSG+19, LWKP12, LWPF12, LWKP14, vV16]. Meet-in-the-
[LYD+18]. Meet-in-the-Middle
[LJ17, LJ18, LSG+19, LWKP12, LWF12, LWKP14, vV16], meeting [Hof16, JK19]. Meets
[RBBHP15, BSR+14, MZA+13, PYH+18, SM13]. Mega [WYL18].
Members [YWZ+12]. Membership
[FHR14]. MemGuard [ZC14]. MemJam
[MMWS19]. Memorial [Ano11c]. Memoriam [Gre11]. Memories [AWSS17, BDGH15, JAS17, RM18, SM18, YNQ15]. Memory
[AN17, ABSSS19, ASBdS16, Arm19, AMH+16, BKKV10, DLZ16a, DHLAW10, GKM16, GM13a, GPR+19, Gue16, HT13, HF14b, Int19, KM18, LGLK17, LY15, MZLS18, PAF18, RC18, Raz19, RB18, TLC16, WAK+19, XZL+19, ZHS+19, BDK16, BAB+13, CZ14, CS11, CVG+13, HHAW19, VCK+12, ZWT13, vV16]. memory-hard [BDK16]. Memory-less
[GM13a]. memoryless [BJ16]. Memristor
[MCS+15, WDG19]. Memristor-Based
[MCS+15]. MEMS [SNCK18]. men
[McK10, McK11, McK12, MPJ+16]. mercurial [BDK16]. Memory-less
[GM13a]. Memory-less
[BDK16]. Memristor
[MCS+15, WDG19]. Memristor-Based
[MCS+15]. MEMS [SNCK18]. men
[McK10, McK11, McK12, MPJ+16]. mercurial [CSZ+11]. Merkle
[ABS+12, AEP18, AK14a, DKP12, HLLC11, Jia17, KHH14, PSS+13, PPS12b, PA10, RW114, BCDN17, BCN19, CJXX19, CMMS17, EEAZ13, Jia16, LC17, LWK+19, YMM13, YJC18]. Message-Based
[PS12b]. Messages
[CCD19, CCD20, Gen13, YLL+12, BMM12, BTW15, KPS10, LCM+17, MSL13, SA15]. Messaging
[BFK+10, Wu17]. messy
[BBDL+17]. Meta
[SKE+18]. Meta-Heuristics
[SKE+18]. Metadata
[Gla11]. Metaheuristic
[HCETPL+12]. Metamorphic
[ATS15]. metaphors
[Mat19]. metering
[HRK+19, JLC18, WMYR16]. Meters
[DM15]. Method
[AGW15, Ara13, BBB+16a, CZ19, FLH13, GLLSN12, GMNS15, HXHP17, HHS+15, KTM19, LyWZZ12, LP12, LD13, LBR12, MUI2, OWHS12, PS14, PWS+19b, QF19, SAA15, SY15a, SXH+19, SP15a, SDD14, USH19, WZXL12, WZCC18, WJ19, XNG+14, XRNG15, YOO15, AGW15, AIA+18a, ARG19, BLL+19, CSS+13, DJ19, Dra16, FVK17, JS18a, JDV16, Kh18, KHH14, LLC10, LH11a, LT13, LT14b, LPZJ15, MO14, PWW10, SI12, WT13, YWT+12, ZYGT17]. Methodology
[CBL13, Uto13, ZZKA17]. Methods
[BCEO19, BCEO20, BBK14, KOB10, LW12, GMT+12, GSGM16, IAA+19, KSB+17, KVvE18, OO10, TMK11, TPKT12]. Metric
[YGFL15, DMWS12]. Metrics
[CVM14, PGLCX17, SSP19, BC18]. Mexico
[AB10a]. Meyer
[Bur11, Joh15]. MIBS
[CWZ19]. Micral
[Gol19]. Microarchitecture
[MSI18]. Microarchitecture
[ZBPF18].
Microcontroller [GL12].
Microcontrollers [LP0+17]. Microcosmic [WWC+11]. Micropayment [RM19].
microphones [GSVA18]. Microprocessors [SK12b]. Microsoft [Loe15]. Mid
[AUMT16, KTM+18]. Mid-Air [AUMT16, KTM+18]. Middle
[LJ17, LJ18, LYD+18, LSG+19, LWP12, LWPF12, LWP14, vV16]. Middlebox
[FGQ18, FGR+17]. Middlebox-Based
[FGQ18]. Midway [Car11]. Might
[Hur16]. Migration [SHS12], MIKEY
[TW14]. Military [HK14b]. Miller
[Ano16a, Sch15a, LL11, LT14a, Led16, LR15].
million [Sch16a]. Millionaire [GKS17].
MILP [CWZ19]. MILP-based [CWZ19].
MIMETIC [ACMP19]. Mind
[SNG+17, WP15]. mines [K016]. MinHash
[HWZP18]. MinHash-Based [HWZP18].
Miniature [HWS+19]. Minimal
[ARH+18b, BDH11, MZ17a, SMB15].
Minimalism [DKS12].Minimally
[AARJ12]. Minimization [AH19].
Minimizing [BCD+12]. Minimum
[KHPP16, DZS+12]. Mining
[BH15, BJL12, CZ19, DK16a, HDWH12,
WZCC18, ZW15, Ano11a, ZMYB17]. Minus
[NXB13]. miracles [MR14c]. Mirror
[Ano10b]. Misbehaving [TAKS10, ATK11].
Misson [Ano10a]. Mistakes [DBH16].
misuse [EBFK13]. Mitigate
[BKJP12, SS15]. Mitigating
[EPAG16, HRS16, SNG+17]. Mitigation
[BRS17, DHT+19, LGR14, DJL+12].
miTLS [BFK16]. MitM [TY16b]. mix
[WGJ10]. mix-networks [WGJ10].
Mixed [ST16]. ML [Ksi12]. mMTC
[CML+18]. MNC [IM16]. Mo [RBS+17].
Mobile [ATC17, BCD+12, CBJY16, FD11,
GPT12, GdM16, HsS12, HFS+19, HLLK15,
KP12, KKA15, LH12, LBC18, May15,
NRZQ15, PH16, RSX18, Sch15b, SFE10,
She14, SS15, SAA12b, WPZM16, WT10b,
XHH12, XNKG15, XHC+12, YHL16, Yon11,
ZLDD12, Aia15, AZ1+16, ALL+18,
CLP+13b, CTL12, CCSW11, CWXX16,
CTL13, CRS13, uHAN+18, FHH10a, FA14b,
FHZW18, FHM+10, GM16a, GH16,
HZW17, HZW18, HL14, IAA+19, IB11,
Kem11, KKA14, KKM+13, KKM+14,
KKG14, KSB+17, KS19, LH11a, LZD+19,
LH13, MHL18, OKD+17, OYHSB14, Par12b,
SSA18, SLL+19, SSNC15, hSSZ15, SM19b,
SCR19b, SSAF11, SKB+17, SHBC19,
TZTC16, TKHK14, WSC14, WT10a,
YHNM18, YNX+16, ZLDD14, ZDW+16,
ZC12, ACM19, MBF+13, SLL10].
mobile-cloud [KKM+13]. mobiles
[GCSA+P11]. Mobility
[CML13, LNK+18a, CL11, GH16, LH11b,
MYR+13, THA+13, YLS12, ZX11]. Modal
[HFS+19, BOP14, GB19, SCFB15].
Modality [SSP19]. Mode
[HZ11, Mar10c, PAF18, gWpNyY+14,
WLC12, ZH+19, Fay16]. Model
[AW15, AW17, App13, BBCL19, Bul18,
CT18, CLP13a, CBX19, Fyo19, GLG12,
GJO+13, GJJ15, GJZ17, GGP18, GRRZ18,
HZX15, IA15, JHW+19, Kar12, KP17,
LYX+19, LK18, LDZ16, LHM+15, LZC+12b,
MVVR12, PYM+15, PNRC17, RSD19,
S14, SP+13, TBCB15, WWC+11,
WWHL12, XZY+12, Y12, ZY19, ZHL15,
BSBG19, BL11, CK11, CWXX16,
CDPLA16, DFJ+17, HKT11, HTC17,
KU13, KS19, LZT12, LCY+16, LL16b,
MG10, Mas17, MM13, NSA17, NB13,
RR16, SERF12, SK18, WYL13, WZM12a,
WZM12b, YC12, YLL+18, ZCL+19, TCL15].
Model-based [IA15]. Model-Predictive
[TBCB15]. Modeling
[BL16, CJFH14, GBNM11, LTKP16,
MK13, PAS13b, RSX18, ZMYB17, An14,
CDGC12, MHY+18]. Modelling
[BBBD14, BL15, ACF16, Eng15, KSI12].
Models [BSA+19, CRS+18, KMSM15,
OS16, VN16, ABR15, GZH12D, CZC+19].
Modern
AG18, Fri12, Ful10, OMNER19, RAZS15, She17, KL08, KL15, KAS15, Gre19a.

Modes [GLLSN12, PC16, FAA+18, SKK10].

MODI [MBF+13]. Modification [LSW16]. modified

[CTHP13, EEAZ13, MM14b]. Modular

[Abel2, DDF+19, EZW18, GL19, LNL+19, Bro19, VN17]. modulation [KPB17].

Moduli [APPVP15, GL19].

Moment

[PTK14, TPK12, yWpNyL11]. Moment-based [PTK14, TPKT12].

Monaco [Gil10].

Money [RBS+17]. Monitoring [BCE+10, ASO14, APK+18, KO16].

Monitors [IF16]. monopolizable [DJL+12]. Monte [CR12, FVK17, GQH17].

Montréal [JY14]. Morphing [MBC15].

Morphology [IA15]. MorphoSys [MD12a].


[GZH17, JHNN12, LFH18, AP10, SYW17].

Motions [HWWZ19]. Mouse


Movement [ERLM16, GB19, ZPW16].

Movements [SRRM18]. Mozilla [Loe15].

MP3 [YWWY12, YQH12]. MPC

[GGHR14, RSMa19]. MPEG [YYO15].

MPEG-4 [YYO15]. MPI [GM13b]. MPSS

[SLL10]. MRAM

[DSB16, PAF18, VDB+16]. MRAM-Based [VDB+16]. MrCrypt [TLMM13].

MSP430 [KSH18a, KSH18b]. MSP430X

[GL12, Soe18]. MST, ttn3 [SwT10]. Much

[DL15]. Muhammad [ABJ13]. Multi

[ABL+18, ASS15, BEM16, BBEP14, BRT12, CWL+14, Chi12, DLGT19, GVW12, GJZ17, HYS11, HCL12, HFS+19, HRS16, IG11, JS18a, KTT12, KMO14, LyWSZ10, MZHY15, MEFO12, MLBL12, NAGuHQ16, OKG+12, OSSK16, PSSK19, SK12b, SOR16, SAM+18, TWZ+12, TYM+17, TFS19, Wan14, WOLP15, XWSW16, YWW10, Ye14, YYK+17, ZC13, ZQQ15, ZYW+19, ZLDC15, AVAH18, BOP14, BGG+13, CPPT18, CLP+13b, CFVZ16, CJXX19, CG12b, CLHJ13, CW14a, CZ15b, DDY+19, DRN16, DFJ+17, DGL19, FHZW18, GOGCC15, GPVdBRO12, GZS+18, GBC19, HL14, HL11, HCCCL11, HLCL12, ISC+16, JCHS16, KM11, KL+17, LXXW12, LKX+14, LZWZ19, LCT+14, LH13, LW12, Mas17, MML16, QMC17, SCFB15, SLL+19, SCY15, SWW+16, SSS11, TLL12, WDL13, WSQ+16, WXK+17, XWZ16, XHM14, YCC16, YQZ+19, YN19, YY13, ZZZA17].

multi-agent [GPVdBRO12]. multi-authenticated [HL11]. Multi-Authority

[ZQQ15, ZYW+19, SLL+19]. Multi-Biometric

[NGAguHQ16, YYY+17, MBL12]. Multi-bit [TWZ+12]. multi-channel

[CPPT18]. Multi-cipher text [KT12]. multi-cloud

[CFV16, SWW+16]. multi-cloud-server [KL+17]. multi-core

[AVAH18]. multi-criteria [ZZZA17]. multi-crypto-processor [BGG+13].

multi-dimensional [LZWW19]. Multi-Directional [JS18a].

Multi-Domain [SAM+18, GI11, QMC17]. multi-exponentiation [WSQ+16].

Multi-Factor

[PSSK19, HCL12, CLP+13b, DRN16]. multi-fault


multi-generation [CGJXX19]. multi-hop

[LCT+14]. Multi-instance [BRT12]. Multi-Key word

[CWL+14, XWSW16, OSSK16, DDY+19, GZS+18, LKX+14, YQZ+19]. multi-lateral

[SCY15]. multi-layered [JCHS16]. Multi-Level [ZLLC15, MEO12].

multi-linear [BBEP14]. Multi-Modal

[HFS+19, BOP14, GBC19, SCFB15].

Multi-Party [ABL+18, KMO14, TYM+17, GVW12, LyWSZ10, DGL19, XWZ16].
Multi-Proxy [ASS15, GJJ17]. multi-purpose [KM11]. Multi-Receiver
[TSS19, Wan14, Chi12]. Multi-sawtooth [Ye14]. Multi-scale [DLGT19, CG12b].
multi-scroll [GMOGCC15].
Multi-Secret [HYS11, ZC13, CW14a, HCCC11, HLC12].
Multi-Signature [ASS15]. multi-stage [Mas17], Multi-target
[HRS16]. multi-use [CZ15b]. Multi-User [MZ15, SOR16, OKG12, MML16].
multibit [KPS10]. Multicast
[CC14, PSM18, BAL10, DMM10, HGW11, LTT10, NAACL12]. Multicore
[RJV19, SHC16]. Multicoupon
[HIDFGPC15]. multidesignated [AYS14]. Multidevice [DPCM16]. Multidimensional
[AJA16]. Multifactor [MMY12, KS19].
Multigigabit [PP10]. multihop [ADF12].
Multikey [LATV17]. Multilayer
[NXH17]. Multilevel
[FMS12b, HF14a, NSA15, SERF12].
multilinear [CJL16]. Multimedia
[BCC10, NSA15, PMZ13, PZPS15, PYM15, WLY15, ZW15, Zha15b, ZSA12, GJJ18,
HM10, HWYW14, HPL19, LLLK10, Wan13, XWZW16, TW14]. Multimodal
[GMI16a, Sar18a, ACM19, AHW18, ATI10, MHT13]. MultiObjective
[ZÁC17]. Multiparticulate [HR13].
Multi-part [BDOZ11, CCL13, Fri10b, ADMM16, BHH19, LDDAM12]. Multipath
[LH12, OPHC16]. Multiple
[DSB15, Dun12a, FR16, HWZP18, HZL15, KBL11, LTC15b, LQD16, Ma17a,
NDC13, SY14, SC10, SKS18, Sta12, WWL14, XNP18, GJJ18, GZS18,
LWZ10, LTC15a, LZZ17, MN14, PZ19, RWZ13, TKHK14, YQZ19, YJC18].
Multiple-Layered [WLL14].
Multiple-Parameter [NDC13].
Multiple-Privacy [HZSL15, MN14].
Multiple-Secret [SC10]. Multiplication
[ARM15a, AK14b, CMO16, GL19, HL17, LNL19, N15, SK12b, YTS12, AAT16,
DG18, Kh18, SHK15, SF12].
Multiplicative [RMERM19, KHHH14].
multiplicity [HL14]. Multipliers
[ARM15b, GT19]. Multireceiver [FHH10b]. multi-secret [FGMP12]. multiserver
[CNF18]. Multiset [FA19, MST17].
Multispectral [DC18]. Multistream
[WXX17]. Multithreaded [TLZ17].
Multitone [GL10]. Multivariate [CLND19, DP17, ST16, YT16, YHD15].
multiview [WSS19]. multiwatermarking
[WL12]. multiwavelet [PWW10]. Munich
[Wat10]. Music [NTK17, WS16], musical
[Ana14]. Mutt [Ran14]. Mutual
[CJP12, GH12, GM14, Kim16, RZ19, SBS12, WT10b, AT1M18, BDM18, BDL19, CJP15,
Cho14, CL11, FHH10a, Far14, GPLZ13, GH16, HDPC13, IB11, JUH17, JKU19, KIU19,
KIP18, KLW16, L1K17, LHH18, MPM19, SPLHC14, TG17, XCY19,
XMHD13]. MVP [CD12]. mvSERS
[HLKL15]. My [GTP14, CMG18]. Myself
[ASV18, W11].

N [Ver17]. Naccache [A18]. NAF
[TX16]. Naive [ZLW17]. Name
[FP19, YCM13]. Name-Based [FP19].
Named [LLZ17]. Names
[ABJ13, MPJ16]. Narayanan [An16a].
National [Fid18, ABJ13]. Natural
[MC19, ZCS15], nature [KL13]. Naval
[Don14]. navigation [JS18a]. Navy [Maf16].
Nazis [Hea15]. NDSS [An10a]. Near
[Alz19]. Nearest
[XLP18, LR10, XMY17, ZZL19].
nearby

nearest-neighbor [LR10]. nearly

network-based [YS12]. Network-Coded [She14]. Network-on-Chip [Bis17]. Networking [CKHP19, FVB18, FP19, KYEV18, LCK11, LLZ17, ZHL15, Kin11, LCM17]. Networks [ABCL17, ABC17, BN14, BPSD17, BC010, BFMT16, CS14, CSX18, DLGT19, DS11, DF16, FMS12b, GMYV17, HZC12, HBC13, HK14b, JWNS19, KHN11, KHK10, LLCL11, LL15, LHM15, LZCK14, LWC14, LLZ12, M KK17, MPM17, NSA15, NYR14, OOI12, OKG12, PYM15, PSM18, PCPK14, RWLL14, RSV18, SWYP12, Sh14, SP15b, SS15, Smi11b, SL11, SZZT18, SAM18, TCN17, WXL17, WLY15, WZCH19, XHC12, XHZ19, YM16, YHSW19, ZC13, ZW15, ZH15b, ZLDD12, ZSA12, Aia15, AQRH18, AS014, AKP18, AIB16, AIKC18, ADF12, BDK11, BNN19, BBB19, BLAN16, BBB16b, CDGC12, CLM12, CML18, CLSW12, CL11, DSCS12, DK12, DLN13, EEA13, FA14b, FHA18, GL16, GH16, HKA18, HG1W11, HZC14, HZWW17, HCC11, HCM11, HCT10, HY18, JNU17, JLT12, JMW16, KM17, KM10b, KLC10, KO16, KLW16, KDW17, LLSS13, LC17, LMJC11, LNNH13, LX14, LK17, LNK18b, LZZ19b].

networks [MGM18b, NXS10, OPH16, OSAN19, PY19, QMW17, RR17, RGP12, SPD10, SGGR16, SA12, SJ18, SM1K13, hSS15, SK10, TD1Q, TKH14, WGT10, Wn13, WW14, WMC17, WXY19, WDV18, WXX17, WX13, XWDN12, XCH14, XMHD13, YHS16, YY19, YN19, ZYG17, ZWQ11, ZBR11, ZCLL14, ZTZ16, ZLDD14, ZHI17, ZX11, LNK18a].


GM13b, LC17, PX13, SAAB10.

**Node-Capture** [NYR+14]. **Nodes** [VGA15, ZYL+10]. **Noise**

[ASN11, Fyo19, LKBK19, YMA17, BCND19, QLZ19, ZHH+17]. **Noised** [JLS12]. **Noisy**

[ASN12, HZW+14]. **Non**

[AH19, AS17, AMH+16, BBCL19, BCI+13, CG14a, CPS16, DIL+12, DPW18, EKP+13, FHKP17, FMNV14, GL19, GZX19, HWS+19, HKB14, JSA17, KTT12, LK18, LLG15, MFS12, OOR+14, Pas13a, QJC+18, RM18, RMG18, Svo14, SM18, WgMW12, XZL+19, YNQ15, YKX12, ZLDD12, AY14a, AM19, BS15, CS11, ESR14, GIJ+12, Kre13, Lan11, LJY16, LP11, MFS13, SES+16, SXL16, VBC+15, XSWC10, Yan14, Kh18]. **Non-** [AH19].

**Non-abelian** [HWS+19]. **non-adjacent** [KTT12].

**Non-associative** [BS15].

**Non-Black-Box** [CPS16].

**Non-blind** [HKB14, RMG18].

**Non-Boolean** [AS17].

**Non-browser** [GIJ+12]. **non-compliant** [Lan11]. **Non-contextual** [Svo14].

**Non-Coprime** [GL19].

**non-cryptographic** [AY14a, ESR14].

**non-dynamic** [SES+16]. **Non-interactive** [BCI+13, LK18, Pas13a, LJY16, Yan14].

**Non-interference** [BBCL19].

**Non-intrusive** [MFS13]. **non-iterative** [SXL16].

**Non-Linear** [EKP+13, XSWC10].

**Non-Linear/Linear** [EKP+13].

**Non-malleability** [KTT12].

**Non-Malleable** [DPW18, MFS12, CG14a, FMNV14, OOR+14, Pas13a, LP11, MFS13].

**non-medical** [AM19]. **Non-monopolizable** [DLJ+12].

**Non-perfect** [FHKP17].

**Non-Repudiation** [LLG15, VBC+15].

**Non-stationary** [ZLDD12]. **Non-tamper** [WgMW12].

**Non-transferable** [GZX19].

**Non-uniform** [QJC+18]. **Non-uniformly** [YKX12].

**Non-Volatile** [AMH+16, JSA17, RM18, SM18, XZL+19, YNQ15, CS11].

**Nonce** [KMZS19]. **Nonce-Based** [KMZS19]. **NonInteractive**

[KOS16, GOS12, MBC+18]. **Nonlinear**

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

**Nonlinearity** [MM17b].

**Nonlinear** [Fyo19].

**Nonvolatile** [ZH+19]. **Norm** [FHS13]. **Normal** [RMERM19, TY16a].

**Normalization** [KLY+12, SJ12].

**Normalized** [YGFL15]. **Norm** [Low12]. **Note**

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

**nothing** [Cer15].

**Notifications** [LBC18].

**Notions** [KFOS12, SNJ11, Sar12, BP11].

**Novel**

[CLHC12, DCM18, KRH13, LY+18a, LY+19, LLG15, YNQ15, CS11].

**Nonce** [KMZS19].

**Nonce-Based** [KMZS19].

**NonInteractive**

[KOS16, GOS12, MBC+18].

**Nonlinear**

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

**Nonlinearity** [MM17b].

**Nonlinearly** [CCM+15, KW14, LW13a, Lud12].

**Nonlinearly** [Fyo19].

**Nonvolatile** [ZH+19]. **Norm** [FHS13]. **Normal** [RMERM19, TY16a].

**Normalization** [KLY+12, SJ12].

**Normalized** [YGFL15]. **Norm** [Low12]. **Note**

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

**nothing** [Cer15].

**Notifications** [LBC18].

**Notions** [KFOS12, SNJ11, Sar12, BP11].

**Novel**

[CLHC12, DCM18, KRH13, LY+18a, LY+19, LLG15, YNQ15, CS11].

**Nonce** [KMZS19].

**Nonce-Based** [KMZS19].

**NonInteractive**

[KOS16, GOS12, MBC+18].
O [CDD13]. **Obfuscated** [LMS16, OWHS12, ZM16]. **Obfuscating** [BG1+10, BG1+12]. **Obfuscation** [ABCL17, AS16, AWSS17, BBC+14, BCKP17, BV18, BCP14b, BR14, CZ15b, DRS16, EMW14, FKOV15, GGHR14, GGH+16a, GGHW17, MI14, ZL19, BBGT12, CFVP16, GGH+16b, OSSK16]. **Obfuscation-Based** [ABCL17]. **Obfuscator** [FDY+19]. **Obfuscators** [PSD15]. **ObfusMem** [AWSS17]. **Objects** [BCK17, SSSA18]. **Oblivious** [DN12, WCL+18, CGH11, GLM+19]. **Obscure** [GLM+19]. **Obscuring** [VGL14]. **obscurity** [Edw14]. **observation** [WHY+12]. **Observations** [CJZ13, HCL+14]. **Obtaining** [BB10]. **Occasion** [Nac12]. **Ocean** [FG19]. **October** [CGB+10, IEE10, IEE11b]. **octonions** [BS15]. **Odd** [Faa19, GJMP15]. **Oded** [Lin17]. **ODIN** [ABCL17]. **odyssey** [Car11]. **OFDM** [CLZ+17]. **Off** [GPT14, GHS14, YMWS11]. **Off-Line** [YMWS11]. **Off-Path** [GHS14]. **offering** [Par12b]. **Offers** [Pau10]. **Office** [Mor12]. **officers** [Maf16]. **Official** [Küp15]. **Offline** [Auo15a, GAS+16, JMG+16, LJJW+17, LKAT12, RSM15, XTZ+19, ZC17]. **Offline/online** [LJJW+17]. **Offloading** [JHCC14]. **Offs** [ASBD16, BS14, GPR+19, SR10]. **offsets** [YQH12]. **Okanomo** [TSF19]. **Old** [Che17, FREP17, GY13]. **On-Chip** [LGLK17, BAB+13]. **On-cloud** [EAAA19]. **On-demand** [KKJ+16]. **On-Line** [FFL12]. **On-siteDriverID** [SGGC1+16]. **On-the-fly** [PS14]. **One** [BHT18, CBXJ19, CMRH17, CPS16, DSSM14, DCAT12, FD11, HP14, HG12, Mat14, NA10a, Par18, PC16, TYM+17, WCXZ17, XW12, XYXYX11, XZLW15, Yon12, BM15, FHH10a, GPLZ13, HRV10, JK19, Kom18, LP11, LW10, LW13b, LML+13, Nor17, RK11, Rus15, SM10a, SPKI7, SCBL16, TCS14, ZQWZ10]. **One-Dimensional** [XYXYX11]. **One-Round** [TYM+17, XZLW15, Yon12, XW12, JK19, TCS14]. **One-Sided** [HP14]. **One-Time** [NA10a, DCAT12, Par18, BM15, FHH10a, GPLZ13, LW10, LW13b, LML+13, SPKI7]. **One-Time-Password** [FD11]. **One-Way** [BHT18, CBXJ19, CPS16, DSSM14, Mat14, WCXZ17, HRV10, Kom18, LP11, RK11, SCBL16]. **Onion** [KZG10]. **Online** [BPSD17, HL19, JMG+16, KSD+17, PSM17, SKGY14, SZTT18, WXY+17, WZCH19, ZHL15, AQRH+18, CCG10, DJ19, HYF18, KVwE18, LKAT12, LJJW+17, MSM+18b, SKS+18, SYW17, XTZ+19]. **Online/Oline** [JMG+16, LKAT12, XTZ+19]. **Only** [BB10, YNRI2b, YL13, Bul10a, KMTG12, KA17, Sar11]. **Open** [SS19, ABF+14, MHV15, Pow14, Win17, ZWQ+11]. **open-source** [ABF+14, Pow14]. **OpenCL** [ABDP15]. **Opening** [GDCC16, LZE12a, LLH18, LZE14]. **Openings** [SP13]. **openness** [Bia12]. **OpenPGP** [MBB11]. **OpenStack** [CSL+14]. **Operable** [BCF16]. **Operand** [MS18]. **Operating** [KMP+11, CDA14, MNNW15]. **Operation** [GLLSN12, JB11, SBS18, ALL+18, Fay16, Lin14a, SKK10, WGG+12]. **Operational** [CRE+12, CM11, RZ19]. **Operations** [Cil11, SEY14, SZHY19, YWW10, KKJ+16, LZY+16]. **operative** [HFCR13]. **Opportunistic** [AA19]. **Opportunities** [Lau17, Mic10b]. **opportunity** [Sch11]. **Optical** [PRGBSAC19]. **Optimal** [AS17, CK17, DSSDW14, DSSDW17, GJJ18, GM16b, HRB13, PDH15, PPS12h, QJC+18, TX16, WU14, Chas13a, CXWT19, DDD14, MCL+19, PPTT15, SYV19]. **Optimality** [MM17a, SDM+12]. **Optimally** [DSSM14, GT12]. **Optimally-Fair** [DSSM14]. **Optimised** [CMO+16].
Optimising [EVP10]. Optimistic
[WSA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12,
GCSAddP11, KHF10, PTK14, RYF+13,
ZSMS18, sCR19a]. Optimizations [ZAG19].

Optimized
[ARH+18a, AYS15, EKB+16, GAB19,
HGT15, LNL+19, MBF+13, MBR15, JS18a].
Optimizing [DWZ18, ZSMS18].

Optimum
[Oba11, YFF12]. Optional
[PC16]. OR-Proof
[FSX12c]. Oracle
[CBJX19, GLM+16, HKT11]. Oracles
[FZT14, FSX12a, GSW+16, XLQ09, XQL11,
YS12, YKC+11, YLA+13, ZYM18, LLY15,
RG10, SYL13, WWYY11, YFK+12].

ORAM [RM18]. Order
[DCA18, FYD+19, KS12, LFX+18,
LWKPI2, PRCl2, YKCL12, ZDL12,
ZSW+12, ZBPFI18, AKY13, BKR19, LW13a,
LCY+16, LWKP14, gWpNyY+14, YL11].

Order-Hiding [DCA18].
Order-Preserving [KS12, YKCL12, YL11], order-revealing [BKR19].

ordered [AAL19]. organisational [Smi15a].
Organization [RSGG15]. Orientated
[TJZF12]. Oriented
[NNAM10, Rog16, RSGG15, WW12,
NML19, SK18, WZM12a, WZM12b].

Origins [SZJG19]. Orthogonal
[FYD+19, tWmC12, XNP+18]. Oscillator
[VKBS10]. OSN [BCF16, BBDP16], OSNs
[SZZT18, PZPS15]. other [BDK16, Smit15b].
OTS [Höl13]. outliers [Sch12b]. Outlive
[Hur16]. Output [DK16b, GST12, NIS15,
NR12, Uto13, PBCC14]. Outputs
[SNCK18]. Outright [ABJ13]. outsource
[XTZ+19]. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18,
LQD+16, PD14, RZD+16, XLP+18, YMA17,
YMC+17, DFJ+10, FS18, HKA19, HMC12,
LCL+15, LCM+16, LJC+17, QZDJ16,
YSQM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+14, LLSL19, LJWC18,
OSNZ19, LWW+19, SKB+17, SWW+16,
XMY+17]. outwitted [Car11, Fag17].

Outsourcing [EV10]. Optimistic
[WSA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12,
GCSAddP11, KHF10, PTK14, RYF+13,
ZSMS18, sCR19a]. Optimizations [ZAG19].

Outraged
[Hur16]. Output [DK16b, GST12, NIS15,
NR12, Uto13, PBCC14]. Outputs
[SNCK18]. Outright [ABJ13]. outsource
[XTZ+19]. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18,
LQD+16, PD14, RZD+16, XLP+18, YMA17,
YMC+17, DFJ+10, FS18, HKA19, HMC12,
LCL+15, LCM+16, LJC+17, QZDJ16,
YSQM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+14, LLSL19, LJWC18,
OSNZ19, LWW+19, SKB+17, SWW+16,
XMY+17]. outwitted [Car11, Fag17].

Outsourcing [EV10]. Optimistic
[WSA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12,
GCSAddP11, KHF10, PTK14, RYF+13,
ZSMS18, sCR19a]. Optimizations [ZAG19].

Outraged
[Hur16]. Output [DK16b, GST12, NIS15,
NR12, Uto13, PBCC14]. Outputs
[SNCK18]. Outright [ABJ13]. outsource
[XTZ+19]. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18,
LQD+16, PD14, RZD+16, XLP+18, YMA17,
YMC+17, DFJ+10, FS18, HKA19, HMC12,
LCL+15, LCM+16, LJC+17, QZDJ16,
YSQM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+14, LLSL19, LJWC18,
OSNZ19, LWW+19, SKB+17, SWW+16,
XMY+17]. outwitted [Car11, Fag17].

Outsourcing [EV10]. Optimistic
[WSA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12,
GCSAddP11, KHF10, PTK14, RYF+13,
ZSMS18, sCR19a]. Optimizations [ZAG19].

Outraged
[Hur16]. Output [DK16b, GST12, NIS15,
NR12, Uto13, PBCC14]. Outputs
[SNCK18]. Outright [ABJ13]. outsource
[XTZ+19]. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18,
LQD+16, PD14, RZD+16, XLP+18, YMA17,
YMC+17, DFJ+10, FS18, HKA19, HMC12,
LCL+15, LCM+16, LJC+17, QZDJ16,
YSQM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+14, LLSL19, LJWC18,
OSNZ19, LWW+19, SKB+17, SWW+16,
XMY+17]. outwitted [Car11, Fag17].

Outsourcing [EV10]. Optimistic
[WSA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12,
GCSAddP11, KHF10, PTK14, RYF+13,
ZSMS18, sCR19a]. Optimizations [ZAG19].

Outraged
[Hur16]. Output [DK16b, GST12, NIS15,
NR12, Uto13, PBCC14]. Outputs
[SNCK18]. Outright [ABJ13]. outsource
[XTZ+19]. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18,
LQD+16, PD14, RZD+16, XLP+18, YMA17,
YMC+17, DFJ+10, FS18, HKA19, HMC12,
LCL+15, LCM+16, LJC+17, QZDJ16,
YSQM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+14, LLSL19, LJWC18,
OSNZ19, LWW+19, SKB+17, SWW+16,
XMY+17]. outwitted [Car11, Fag17].
Ano16b, Ano16c, Ano16j, CWZL13, LW13a, XW13, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11. Paradigm
[ABGR13, BSV12, Mau12, MP12, TAP19, Gop19, KKM11, WQZ+13]. Parallel
[AAH+19, App14, ARM15b, BBM15, BTK15, CGB+10, GP17, HW19, LY16, LB13, MCDB12, MC11, NdMMW16, NR15, SMD11, YE12, ZGL+16b, CSTR16, FLYL16a, FLYL16b, MRT10, RBW13, WWYZ11]. parallelism [SD17].
Parameter [NDC+13, MZ15]. parameterized [GR19b]. Parameters
[HRB13, MBF18, LZXX19]. parametric [Bul10a]. Paranoia [Cor14a]. Parity
[Raz19]. Park [Ano11c, Bri11, Cop06, Cop10a, Cop10b, GMT+12, GW14, McK10, MK11, MC11, Pea11, Sim10, Smi11a, Smi15b, Smi15a, Bai12]. Parsing
[MHW+19]. Part
[BLM18, VM14, BD15, Bar16a, BBCL19]. Partial
[CBJX19, DLV16, GBDF12, HFW+19, LG12, SGS14, TK19, WDDW12, Bax14, EBAÇ17]. Partial-Shape [HFW+19]. Partially
[KB10, XZP+19]. participants [KSU13, WTT12]. participating [CH10]. Participation [Abb12]. particle [ZSMS18]. Parties
[YCR16, Kip13]. Partitioned
[FVS17]. Partitioning
[ADR18, DMD18, SHC+16, AP11]. partitioning-based [SHC+16]. partitions
[CFG+17]. Party
[ABL+18, Ash14, BBKL19, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, OSH16, QZL+16b, TYM+17, ZM16, DGL19, ED19, FIO15, GVW12, HPC12, HWB10, HWB12, LyWSZ10, LML+13, OSANAM19, Tso13, TKHK14, XLWZ16, XCL13, YC12, YZZ+14, ZSC15, GHKL11]. Pascal
[LG10]. Password
[ASBD16, BRT12, CLY14, DM15, DGMT19, FVS17, FD11, GAS+16, HKK19, HCL+14, LLD19, Lop15a, Lop15b, RS11, SD12, Shi11, WGMW12, YLM13, YRT+16, ZHX16, ABK13, AICK18, BDK16, CTL12, DSCS12, Eng15, FA14a, FIO15, FHV16, GPLZ13, HCC10, IOV+18, KMTG12, LWS10, LNN13, LZ19b, MM12, MVL+19, MCRB19, Par18, SVY19, Tso13, TKHK14, WZM12a, WZM12b, YC12, ZXWA18]. Password-Authenticated
[HCL+14, YRT+16, ZHX16, LWS10, WZM12a, WZM12b]. Password-Based
[BRT12, CLY14, FVS17, WGMW12, DGMT19, DSCS12, FA14a, FIO15, IOV+18, TKHK14]. Password-Only
[YLW13, KMTG12]. Passwords
[BHVOS15, LCL17b, BCV12, Che13, GPLZ13]. Past
[Bon12]. Patching
[BCFK15]. Patchwork
[NHX+17, XNG+14]. Patchwork-Based
[NHX+17, XNG+14]. Path
[AMS+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13]. Patient
[ZLDC15, VZG16]. Patient-Centric
[ZVG16]. Pattern
[DCA18, PSS19, YTF+18, ATKH+17, DA18, uHAN+18, KPS10, OSSK16, PPTT15]. Pattern-Based
[PSSK19]. Patterns
[Ano16f, BPSD17, TSH17, WLP15, BDK11, BCG15, LHM13, NML19, SPK17]. PAWN
[JNUH17]. Pay
[EAAAI9, CCSW11]. Pay-per-use
[EAAA19]. pay-TV
[CCSW11]. Payload
[CHH12, 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]. PDF
[Con17]. PDGC
[CGB+10]. PEA
[ZGL+18b]. Peaks
[TC10]. pearl
[Rus15]. Pecherskii
[Kuz11]. PEDCKS
[XLC+19]. peer
[LLY06, NCCG13, ZYW+13].
YE12, YK16, ABF^+14, NCCG13, nor17.


Player [GJO^+13, Pless [Ayu12, plugged [PP11], plus [WXMZ19], PN [XNP^+18], POB [SRAA17]. Podolsky [HR13]. Point [AKH14b, EZW18, MH14, ZC13, ZM16, AKM^+15, Kh18]. Point-To-Point [ZC13]. Point/Polynomial [ZM16]. Point/Polynomial-Advantage [GR19b, Bul10a].

WSSO12, ZM16, AAT16, BGJT13, Bul10a, ERRMG15, FS15, HVL17, HKHK13, JSMG18a, JSMG18b, LFWS15, LJWY18, LDZW19, QRW^+18, TY16a, WZ16, XWS17, XZP^+19, LAL^+15, LHL15].


Polarities [XNP^+18]. policies [Cra11, CFG^+17, DFJ^+10, LHM14]. Policy [CHH^+19, FVJ19, GZZ^+13, GS^+16, HSMY12, MK12b, PV17, RVH^+16, Rao17, SVG16, XMLC13, XWLJ16, ZHW15, FS18, HZL18, HKHK13, JSMG18a, JSMG18b, LFWS15, LJWY18, LDZW19, QRW^+18, TY16a, WZ16, XWS17, XZP^+19, LAL^+15, LHL15].
[MC19, HYF18]. Precision
[EZW18, HZSL05, MN14, SK12b].
Precomputation [GKM16, Bon19].
Predicate [KHPP16, LNWW19, NMS14, YKSN12, ZYT13, FH13, HFT16].
Predictability [DK16b]. prediction
[CSS+13]. Predictive [TBC15].
Predictors [EPAG16]. Predistribution
[YM16]. Preface [Ano19c, YYW19].
Prefetch [FDY+19]. Prefetch-Obfuscator
[FDY+19]. Preimage [Li10]. Preceeding
[Ran16]. Presence [BDPS12]. Present
[Bon12, LJ16, WH17]. PRESENT-like
[LJ16]. Preservation
[BCP14a, LLG15, YSV15, YJSL18, Yon11, FZZ+12, LVRY10, TMLS12]. preserve
[BAG12]. preserved [SW+17].
Preserving
[ABC117, BJL16, BHNK13, BJL12, CWL+14, CRE+12, EKOS19, GZZ+13, HSMY12, HLLC11, HX+11, HHMK14, HK18, KKK+18a, KLL+19, KS12, LMGC17, LNXY15, LS+16, LQD+16, MHW+19, MJS+19, Mor19b, MTM18, NMS14, OFM16, PR12, PD14, PSS+13, PPR12, Pet12, RVH+16, RSR+19, RHLK18, RBHP15, SZDL14, SZQ+17, SZTT18, VFFH19, WPZM16, WZCC18, YKKL12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, AMPCR13, AIB+16, ALL+18, BC16, BBPD16, BLV17, CCMB19, DZC16, FH13, FMA+18, GH15, GH16, GAI+18, GA11, HSH11, HLS18, HKA19, IC17, IOV+18, JKL+16, JLC18, JXL+19, KKH18, LHL+18, LZD+19, LSIQ15, LW13a, LCDP15, LCY+16, LLG19, MGB19, OSP+19, PZBF18, QLZ19, RR16, SYV+17, SMS+16, Tan12b, TSH14, WLZ+16, WZC16, WMC17, Wan18b, YYK+19, YMM13, YNX+16, YL11, ZYW+13, ZOSZ17]. Press
[Ano15b, Ano17b]. Press/Elsevier
[Ano15b]. Prevent
[HLAZ15, PYM+13, JSK+16]. Preventing
[DCAT12, HAK19, MT17, CAM19, SKEG14, WS12]. Prevention [CWL16, VS11]. price
[Ano13b]. Primality [Cout12b]. PRIME
[ACK+10, GM13a]. Primes [Gre19b].
Primitive [App15, MCS+15]. Primitives
[BSJ15, CK17, EAA12, HL+10, SP15b, ABPD15, BSR+14, Gor10, WSL+19].
PRINCE [BC+12b]. Princeton
[Ano17b]. Principal [BKL+18]. Principle
[KYE+18, WW14]. Principles [DK02, DK07, DK15, FS10, KL08, Fru0a, Sta11b].
print [PKS10, PKS18]. print-cam [PKS18].
print-scans [PKS10]. Printer
[EMW14, FNP+15]. Prior [NA10a].
Priority [LMS16, Bia12]. Prisoners
[Mac14, GSGM16, Keb15]. PriSTE
[CXX+19]. Privacy [AKM+11, AKKY17, ABC117, Ano19a, ABR13, ALL+18, ACM12, ABHC+16, BN14, BCF16, BA18, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DCA9, DTE17, ESS15, EKOS19, FGR+17, Fei19, Fru13, GZZ+13, HSMY12, HCC13, HXHP17, HX+11, HK18, IEE15, JN12, JLX+19, JP19, KM10b, KKK+18a, KLL+19, KCC17, Kni17, KS12, KH18, LMGC17, LSBN14, LLG15, LCP15, LNXY15, LS+16, LQD+16, MYYR13, MJS+19, MV18, Mor19b, MTM18, NMS14, PD14, PSS+13, PPR12, PZPS15, PSD15, Pet12, PH16, RVH+16, RSR+19, RCP+18, RWLL14, Roh19, RHLK18, RBHP15, SS17a, SG12, Set16, SZDL14, SZTT18, SOF12, TMLS12, TMG13, VDK+19, VFFH19, WPZM16, WMC17, WZCC18, WMYR16, YJSL18, YYK+17, YMM13, Yon11, YY17a, ZHW+16, ZMI16, ZOSZ17, ZXL19, ZHW15, ZLDC15, ZHL15, ZTL15, vG17, ARL13, AMPCR13, AIA+18b, ACK+10, BE+18].
privacy [BC16, BBPD16, BP11, BAG12, CD16a, CXX+19, CCMB19, CDF+10, DZC16, DZS+12, FH13, FMA+18, FZZ+12, GAI+18, HSH11, HKA19, HKR+19, HPL+19, IC17, IOV+18, JKL+16, JLC18, Kaml16, KKGK10, KM14, LYW+10, LWYM16, LHL+18, LZD+19, LSIQ15,
MZA +13, MGP10, MGB19, NJB19, OSP +19, PX13, PZBF18, QLZ19, RR16, Sav16, Sch11, SSNS15, SLZ12, SYY +17, SCY15, SWW +17, SMS +16, Tan12b, WLZ +16, WZC16, Wan18b, WWW17, WS13, YYS +16, YXA +18, YYK +19, YQOL17, YNX +16, ZWY +13, ZDHZ18, ZZY +19.

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 [ABCL17, BJL16, BWL +14, EKOS19, GZZ +13, HSMY12, KKK +18a, LGMC17, LNX15, LSY +16, LQD +16, MJS +19, Mor19b, MTM18, NSMS14, PD14, PPRT12, Pet12, RVH +16, RSR +19, RHLK18, RBHP15, SZDL14, SZS18, VFFH19, WPZM16, WZCC18, ZHW +16, ZM16, ZHW15, ZLDC15, ZTL15, AKM +11, AKKY +17, ALL +18, JX +19, KH18, LCPD15, WMC17, ZOSZ17, APCR13, BC16, BBDP16, BLV17, CCMB19, DZC16, FMA +18, GAI +18, HSH11, HKA19, JLC18, LHL +18, LZD +19, LSQ15, MGB19, PZBF18, QLZ19, RR16, SYY +17, SMS +16, Tan12b, WZC16, Wan18b, YYK +19, ZWY +13].

Privacy-Protecting [Roh19, CD16a].

Privacy-supporting [ABR13].

Private [BBKL19, BKLS18, GM13a, Jia14a, LSQX19, MV19, QLZ +16b, RCBK19, RDK19, Sia12, WCL +18, Yek10, ZMW16, ZXYL16, BHH19, DDL15, HJM +11, HYF18, IK15, WR15, vV16].

Private-Key [MV19].

private-keys [IK15].

Privilege [Cha13c, QRW +18].

Privileged [Dn10, WDZL13].

Prize [Ten18].

PRNG [DK16b].

Proactive [SLL10, WMYR16].

Proactively [OPHC16].

Probabilistic [BFG +14, Rao10, WP17, KSU13].

Probabilistically [IW14].

Probability [DF11, HLC16].

Probability-based [HLC16], probable [Sav13b].

Probably [MMS17b].

probe [Edw14].

Problem [CLL16, GR19a, GKS17, HWS +19, Hor19, LGGJ16, NA10b, TKM12, Bar19, Mes15, MR14c, Pec17, RH10, VM14].

Problems [AH19, Dun12a, Fra15, GTT11, KRDH13, KPC +11, Lal14, RBS +17, CJL16, SK14, TPL16, WS14].

Procedure [CS14, OS12].

Proceedings [LCK11, TT18, Wat10, ACM10, ACM11, Abe10, BC11, CGB +10, Che11, Cra12, DJune12, FBM12, Gil10, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLIC10, IEE11a, Kia11, Lin14b, Sah13].

process [CWZL13].

Processing [JGP +18, SAKM16, SZHY19, TKMZ13, VKPI17, BKV13, HWK +15, MS13b, PRZB12, WS14].

Processor [BH15, CLF +17, HHL +14, LB13, MBR15, RVJ +18, YT16, YS15, ABDP15, BAB +13, BGG +13, KSH18b, SSPL +13, Tar10, KSH18a].

Processors [GFBF12, Gue16, SJLK18, RYF +13].

PrODACT [FDY +19].

producer [CHL19].

Product [ADM12, CCM +15, OT12, YKNS12, And19, Cha13b, DMD18, ABP15, BAB +13, BGG +13, KSH18b, SSPL +13].

Products [LMG +18, RS10].

Professional [HGOZ19, STC11].

Profiled [Bar16b].

Profiles [BCF16].

Profiling [DP12].

Profit [APPVP15].

Program [MZ17b, TLZ +17, Wal18, CLZ +17, DMD18, GGH +16b, MSH13].

Programmability [HP18].

Programmable [ABP16, CLF +17, Ang16, EAB +19].

Programming [Bee17, BC115, LSL19, SY14, ASVE13, GLMS18, HLV10].

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

Progress [AB10a, BL10, BC11, GG10].

Progressive [SA16a].

Prohibition [Hor19].

Project [SPG +19, Ano14c, Rom11].
ACK+10, SS10c, Wii18]. **Project-Based** [SPG+19]. **projective** [CZ15a]. **Prominent** [ABJ13]. **Promise** [Pau10, PWVT12].

**promised** [HS11]. **Proof** [BDSG+13, Bla12, CZLC12a, CZLC14, FSX12c, GKG19, Kuz11, LYY+18a, LYY+19, LW12, LYY+16, NLY15, SR14, Ste15a, ZMZ17, HSL18, Mon13, PPTT15, VBC+15, WHJ13, ZCZQ19].

**Proof-of-Concept** [GKG19].

**Proof-of-Knowledge** [LYY+16]. **Proofs** [BBD19, BGK12, BCGK12, BGB12, BCI+13, BDSG+13, CZLC12b, DKL+19, IW14, LNZ+13, Mau12, NLY12, NLY+16, NLY19, OHJ+10, Par12b, SSA18, SPLHC14, SB17, SGJ+18, SWW+16, SSS11, SSSL+13, TG17, THA+13, Tso13].

**protocol** [TKHK14, VS11, WMC17, WYZ+17, Wan18b, WCFW18, WDZ19, WDV18, WZM12a, WZM12b, WLS14, WMY16, WT10a, WTT12, WCC18, XLC13, XHM14, YC12, YZZ+14, YYK+19, YMM13, YN19, ZWO+11, ZT+16, ZY+17, ZWX+18, ZW18, ZG10, ZZC15, ZZ11, BOB13, CJP12, LFGCGCR14, Ste15b].

**Protocols** [ADH19, AP13, ABHC+16, BMP12, BSBB19, CCK12, CCCK16, CMRH17, CCF17, CZCD18, CDD19, CDD20, Con10, CM11, EFGT18, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KL08, KOS16, LY16, LML+17, MV19, MS16, MT12, Mur16, NYY+14, NSMS14, PS14, RB17, SBS+12, SBS18, Sch12e, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13d, AKS19, ACC+13, ACM12, BJ10a, BKR19, CML+18, CR10, CLCZ10, DGN14, FTV+10, GBMN11, GLR13, HSH11, HLS18, Ham12, HDPC13, HZW17, HST14, HWB10, KJN+16, KSL13, KSL12, KKK+16, LDC13, LLY06, LKSK13, MN10, NR11, Nos11, Nos14, SD10, WMU14, YSL+10].

**Prototype** [Bar16b].

**Proto** [KPC+16]. **Provable** [BKLS12, CC14, EKB+16, Rog16, YJSL18, YMS10, YYY19, ZXX11, ZPX+17, FA14a, HRS13, LHH11, SYX19, WB12, XCL13].


PSMPA [ZLDC15]. PSO [TLL13]. PSpace [JLX+19].

Public
[Alz19, Ane11b, ABW10, BVS+13, BB14, BM18, BKL18, BKKV10, CT18, CLP13a, Che15, CLND19, CNT12, Coulb2, EKOS19, FBM12, GKS17, HEP+11, HWS+19, HTC+15, HLM19, IM14, JLT+12, JNWS19, KFOS12, LYY+19, LLSW16, LG10, LPsS10, LSQL18b, LZC14, LCP15, LLH18, MZHY15, MPM14, MTY11, Mat14, MPRS12, Mufi6, NTY12, Ormi6, PDHN15, RSBGN12, RVS+18, RW12, RBHP15, SG18, Saa12a, Sch19a, SK12b, Seo18, SWM+10, Sia12, SC12, SLY+16, SGP+17, ST15, TTT12, WP17, WZ15, WWH12, Wil18, WSQ+16, XNK15, XXZ12, Xio12, XJWW13, YL17, YKC+11, YFK+12, YMC+17, ZCZQ19, ZY17a, AA14, ATKH+17, AK14a, AVAH18, BS15, BZD16, BSW12, CFG+17, Durr15, HZZW17, Hod19, HL14, HYL+19, HT17, LSN14, LLY15, LL13, LL16a, LLG19, RPSL10, SES+16, SY15b, SLXX16, VN17, XWK+17, XLC+19, YT11b, YYS+16, YN19, ZZ11, ZC15].

Public-Coin [CLP13a, Mat14]. Public-Key
[BS15, BKKV10, GKS17, KFOS12, LLH18, MPM14, MPRS12, Mufi6, NTY12, Ormi6, PDHN15, RSBGN12, RVS+18, RW12, RBHP15, SG18, Saa12a, Sch19a, SK12b, Seo18, SWM+10, Sia12, SC12, SWS10, Sia12, XNK15, XJWW13, YL17, YKC+11, YFK+12, YMC+17, ZCZQ19, ZY17a, AA14, ATKH+17, AK14a, AVAH18, BS15, BZD16, BSW12, CFG+17, Durr15, HZZW17, Hod19, HL14, HYL+19, HT17, LSN14, LLY15, LL13, LL16a, LLG19, RPSL10, SES+16, SY15b, SLXX16, VN17, XWK+17, XLC+19, YT11b, YYS+16, YN19, ZZ11, ZC15].

Publication
[MMKP16, ZTL15]. Publicly
[NMP+13, SZQ+17, YNR12a]. Publish
[BS15, BKKV10, GKS17, KFOS12, LLH18, MPM14, MPRS12, NTY12, Ormi6, PDHN15, RSBGN12, RW12, SK12b, Seo18, SWM+10, Sia12, XNK15, XJWW13, YKC+11, YFK+12, ZY17a, ABW10, IM14, LPsS10, LZC14, AVAH18, BZD16, BSW12, HYL+19, LLG19, RPSL10, SES+16, VN17, ZC15, ZY17b].

Publicly
[CLP13a, Mat14].

Publicly
[CLP13a, Mat14].
Quantization-Based [HRK18, IGR+16, LZZ+19a, USH19]. Pulse
[OMPSPL+19, MRRT17]. pulse-response
[MRRT17]. punctured [MG15]. puppet
[Lac15]. Purpose
[GFBF12, Guc16, ABDP15, DGJN14, KM11].

purposes [ABB+14, KNTU13]. Push
[LBC18, Wu17]. Pushdown
[CCD15]. Pushing [FHN16]. Putting
[MMKP16]. Puzzle [IBM13a]. Puzzles
[RSBG12, dCCSM+12, dCCSB+16]. Py
[DG12]. Py-Family [DG12]. pyramid
[MT+13].

Q&A [AHN+18, Hof15, Hof16]. Q3 [Ven14].
Qaeda [Mac14, Keb15]. QARMA [LJ18].
QARMA-64 [LJ18]. QARMA-64/128
[LJ18]. QC [JY14, GAB19, HIC17, VOG15].
QC-MDPC [HC17]. QIM [LJK17]. QIP
[JUU10]. Q&O [Ksi12]. QoP-ML [Ksi12].
QoS [BCG10]. QS [AZPC14, HDW12].

Quadratic [KRDH13, SEY14, YDH+15].
Quadraticity [MS12a]. Quality
[BSA+19, CSW12, Ksi12, NN12, YCM+13, SS11, WZLW13, WKH11]. Quantifying
[CBRZ19, GZW19]. Quantitative
[BL15, BL16, MLBL12, MV16b, HM10].
Quantization [SA13].

Quantization-Based [SA13]. quantizer
[Pau19]. Quantum
[And19, Ano15d, Ano16d, Ano17d, Ano17e, BB14, Ber14, Bro12, BCF+14, CK17, Che17, CCL+13, Feh10, FKS+13, Fol16, JEA+15, JL18, Kar12, KPI10, KG19, LK18, LM14, LHA+16, MS16, MSU13, Mos18, MKAA17, NNA10, NA10b, NDR+19, QCX18, RK11, RSM15, RS18, Sas18, Sti11, SD18, TKM12, Urr15, WCL+18, Y+17, ZWS+18, AP18, ABB+14, BJ16, BCDN17, BCND19, CML16, Dya19, Edw17, FRT13, GJMP15, IM14, JSK+16, KKK+16, LLP+18, Lam13, LyWSZ10, LCW+16, Lüd12, QD16, SPD+10, SK14, Svo14, VV19, WMU14, YDH+15, vDKS11, Sen10, Yan11]. Quantum-

Oblivious-Key-Transfer-Based
[WCL+18]. Quasi
[BGJT14, OWHS12, OTD10, BGJT13].

Quasi-Chirp [OWHS12]. Quasi-Cyclic
[OTD10]. Quasi-Polynomial
[BGJT14, BGJT13]. Quaternion
[HD19, YWNY15, yWPWypN13].

Queries
[GYW19, HLW12, LHK10, PBC+17, ZZQ+19, BKV13, CHX13, DFJ+17, GLM+19, HMCK12, PRZB12, TKMZ13, WL19].

Query [DCA18, GA11, PCDG14, WCL+18, XLP+18, AAI+19, AZPC14, BS13a, BKR19, CH11, ED17, HNK+15, JCHS16, JLC18, LZX+14, LZW19, LW13a, XMY+17, YQOL17, ZZC17, ZHT16, ZXL+19].

Query-preserving [GA11]. Quest [Fox13].

Question [TWNC18, Cha13b]. Quisquater
[Nac12]. Quorum [Kar12].

R [Gre19a, BS12, DB16, LVV11, LJF19, PP10b, WYW14]. R3579X [BDK11].

Rabbit [FSFW11]. Rabin [Chi13a]. Radar
[Laz15]. Radial
[HD19, pNyWyY+14, CG12b]. Radio
[KAHKB17, CJP12, CJP15, EA12, Kim11, NLYZ12, RGP12]. radio-frequency
[CJP12, CJP15]. Radix
[ARM15a, GKC11]. Radix-8 [ARM15a].

RAGuard [ZHS+19]. Rail [HF14b]. raised
[LJY16]. Raising [YWW10].

RAKAPOSHI [IOM12]. RAM [RYF+13].

Ramanujan [KK10]. Ramifications
[ALR13]. rampant [Ano13b]. Random
[Ana14, CBJX19, CDK+10, DSHL18, EAA+16, FZT14, FSX12a, GSW+16, Gre17, KS15, LTPK16, LPL15, MIH16, NIS12, NNAM10, NN12, SC10, SRK+17, SRK+18, TM18, WS12, XYZXY11, XLQ09, XQL11, YM16, YS12, YFK+12, YLA+13, ZYM18, Ara13, CFY+10, CT11b, GPLZ13, GLM+16, GLW13, HKT11, KM10a, LGKY10, LLY15, LHM13, MRT10, MG15, PL浑身E10, QLZ19, RG10, SMDS11, SYL13, SH11, SM11, Syl15, Sti11, WWYY11,
Reputation-Based [PAS13b]. Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13]. Requirements [OS16]. Requires [Raz19], requiring [KHH14].

Respect [CATB19]. Respiratory [RSCX18]. Response [DGS12, LjF16, Hof16, KGO10].

Reséting [TTH13]. Resess [TYH17]. Resettably [CPS16]. Resettably-Sound [COP14].

Resilience [AMHJ10, FQZF18, KAS15, LLZ18, ZSH18, AMHJ10, FQZF18, KAS15, LLZ18].

Resilient [AY12, BKKV10, FPS12, HD19, HHS18, JP19, LTZY16, LD13, NYR14, Pan14, PDS15, XZY12, YZ12, YNR12b, YCZY12, ZYT13, ZWTM15, ZMM17, ZYY19, ZY17a, ZYM18, ZYH18, ABC12, CAM19, CXQ18, DLZ16a, GV14a, KPS10, Kom18, LLG19, MMSD13, SCBL16, SGP17, Wan18a, YSJL14, YKC12, YLZ16, ZY17b, ZYM19].

Resistant [CGCS12, GZSW19, PRC12, WLZL12, ZJ11, DLN13, FIO15, XYML19].

Resisting [BK12a, CDK10, GV14b, HF14b, SRRM18, WHZ12, WgMW12, WH17, YPR17, FK19, GMRT15, HCC10, PBCC14, VCK12, WTT12, YKGK13].

Resisting [Mak11, Tam15, ZYL19]. Resistive [DSB16, TLCF16]. Resistivity [MM17b].

Resolution [LW18]. Resonance [LCR18].

Resource [CSH18, CRH18, HM19, JMG16, JWNS19, SSMK13, YNR12a, ZSH19, AMH10, FQZF18, KAS15, LLZ16, MHV15, Wan13, XWZW16, ZPZ16].

Resource-Constrained [CSH18, CRH18, YNR12a, LLZ16].

Resource-constraint [ZSH19].

Resource-efficient [SSMK13, XWZW16].

Resources [Brem18, IM16, Pau19, HRK19].
CCLL11, CLSW12, CNF+18, CH10, CT11a, CLHJ13, CW14a, CTHP13, CB11y16, Cho14, DDD+19, DSCS12, EAA+16, EZ15, FLL+14, Fat16, FA14a, FHZW18, FZZ+12, GHZD12, GJ13, GMRT+15, GJJ18, GPLZ13, GLM+16, GH16, GAI+18, GBC19, GTSS19, HKA+18, HZW18, HBBNM+16, HL12, HL11, HCCC11, HLC16, HCC10, Hwa11, IB11, JNUI17, JKAU19, JLT+12, JZS+10, JMW+16, KFE19, KII11, KPP16, KDH15, KK13, KHM13, KKM+13, KKM+14, KKK14, KCS+18, Kim16, KKK+18b, KIH19, KP18, KL+16, KLW+17, KDW+17, KKD+18, KWH16, KL11, LXLY12, LLZ+16, LSR13, LYT+10, LH10c, LWY+10, LZJX10, LN+11, LMJC11, LK12, LLHS12, LNKL13, LDZ+14, LWYM16, LK+17, LNK+18a.

**Scheme**

[LWK+18, LNK+18b, LWK+19, LFSW15, LH13, LHH11, LWL0a, LWLW11, LW13b, LZX14, ZZZ19b, LDZW19, LL16a, LL16b, LWY12, MCN+18, MSS17c, MK12a, MGB19, M13a, NRI17, Nos14, NMX15, ODK+17, OSNZ19, OPS14, OSAN19, PY19, PZBF18, QMC17, QMW17, RPSL10, SGGR+16, SM11, SYWX19, SCR19b, SMS+16, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWYZ11, WY111, yWPlyl11, WLH13, WZL13, WLZ+16, WLX16, WFX17, Wan18a, WXMZ19, WXSR19, WZ+19, WDVK19, WZ11, WKK11, WOLS12, WX+17, XHH12, XWXW16, XWXC14, XXX15, XWK+17, XTZ+19, XXY19, XMHD13, YWJ+19, YC11, YC16, YYH18, YSM19, YWK+10a, YCT15, YX18, YQOL17, YY13, YMSH10, ZYL+10, ZYL10, ZXY14, ZYC+17, ZZY+19, ZWY+19, ZPWX12, ZHH+17, ZY17b, ZF+18, ZLY+19, ZC12, ZSR11, DT13, LLZ+12].

**Schemes**

[AAUC18, ACA+16, ABF12, BVS+13, BF12, BBEP14, BSJ15, CMLRHS13, Czc18, CLND19, CGL+12, Chu16, Des10b, EFGT18, FHKP17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZCK14, MLCH10, MR14b, MMS17b, MBF18, MKRM10, MKAS18, Oba11, PB12, PNDH15, PH12b, Sch10, Shi11, SKH17, SSU12, SFR12, WGF16, YNR12a, YNR12b, Yek10, YWZ+12, AGHP14, AN15, AXL+12, BKR19, CDGC12, CJXX19, CHS11, CCG10, CTL13, DDD14, DD13, DZ14, FPB14, FGMP12, FMA+18, HAK19, HDWL16, HM10, KU116, LWV+19, LHY12, MM12, MA17b, NZL+15, QYWX16, SES+16, Sar10a, Sar11, hSSZ15, SAR18b, BW14, YT11b, ZCL+12, ZCL14, ZT14].

**Schneider**

[Se16]. **Scholarship** [SPG+19].

**Scholarship-for-Service** [SPG+19].

**School** [Hom17]. **Science**

[Bow11, Gas13, IEE10, IEE11b, Nie02, Ter11, Bia12, PHWM10, Pet11]. **scientists**

[Goo12]. **Scientometric** [Pal15, Pal16].

**Scope** [Bai12]. **Scope** [GCS+11, Pip19].

**Scoring** [GSM16]. **scrambler** [Pou19].

**Scrambling** [LLL17]. **scream** [MDS18].

**Screen** [SPW+16, CT12, IAA+19]. **Script**

[Rao10, Bax14]. **Scripting** [DSB15]. **scroll** [GMOGCC15]. **SDB** [HWK+15].

**SDDO** [PL16]. **SDDO-based** [PL16]. **SDH** [GSM11].

**SDIVIP** [YNX+16]. **SDN** [DHT+19, KCC17, YHSW19]. **SDN-Based**

[DHT+19, YHSW19]. **SDVS** [Wan10]. **SE** [LLL13]. **SE-AKA** [LLL13]. **seals**

[MN10]. **Seam** [LC15]. **Scam** [LC15]. **Seam-Carved**

[LC15]. **Search** [AHA+18, CWW+14, CHe15, DCA18, FR+16, GTT11, HWWZ18, HCD12, HL19, LSQL18b, SOR16, TMC15, WDCL18, WW12, XWSW16, XJWW13, ZXYL16, AHI18, BRZ16, BTK15, BL11, CHL+16, DDD+19, FH13, FSGW12, GZS+18, HAK19, HH16, MRR+18, NJB19, OSS16, PWS18a, SY15b, WHY+12, WLY16, WMC17, WS19, WXY+18, XTW+19, XLC+19, YXD18, YQOL17, YQZ+19, Z11, scR19a].

**Searchable** [BHJP14, CWWL12, CLW16, CGK01, FJHJ12, HKA19, PBC+17, PCY+17, XNK15, ZZQ+19, CLC+19].
Searches [Sia12, WR15], searching [GPN+12], Seattle [LCK11, KCR11].

Seberry [AHS10]. SEC [PA10]. SecLAP [AMKC19]. SECO [DYZ+15]. Second [AKY13, ABM+12, Gre19b, LGP19, SNG+17]. Secondary [RS11]. Secrecy [AKY13, ABM+12, Gre19b, LGP19, SNG+17]. Secondary [RS11]. Secrecy-preserving [TSH14]. Secrecy [ABD+15, BKST18, BCND19, KZG10, TSH14, Yon12, ABD+19, ATKH+17, Bia12, RCV15, TCS14]. Secrecy-preserving [TSH14]. Secret [ASN11, ASN12, ADH17, Ayu12, Bai10, BBP+16a, BFM12, BBEPT14, BP06, BCDN17, BCND19, Bri11, BLU+15, CCM+15, CFOR12, CCL+13, DR12, Dew11, EM12, EA11, FHKP17, FR16, Fok12, HYS11, HL10a, Has16, HZX+18, JLS12, KU14, KS18b, KOTY17, KK12, KKI3, KSSY12, KS15, LKBK19, LHF12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Oba11, PCPK14, QS18, SLL10, SC10, SS10c, SSU12, Sti15, TLL12, TWZ11, WKB16, WGF16, Wil18, XZY+12, XRJ+17, YFF12, YWZ+12, ZC13, Aal11, AIM+19, ADG16, AKK+17, Ara13, AGBR19, BJ16, BEB+18, Bud16, Cha13e, CT11b, CW14a, CLZ+17, DD13, EAAZ13, EZ15, FHH10a, GEAHR11, GJMP15, GLW13, HF14a, HH15, Hea15, HBBRN+16, HCC11, HLC12, KFE19, KI11, KTU16, LXY12, LH11a, LT13, LyWSZ10, LHYZ12, LEW19, Mas17, McK10, McK11, McK12]. secret [MMB11, OO10, Par18, Pea11, Pet11, QD16, Rus15, SB17, SA12, SAR18b, SM10c, TQL+14, TD14, UUN11, UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, WX13, YC11, YC16, YSC16, ZCL+12, ZZ15, ZPWW12, LSC+15, Bai12]. secret-key [BJ16]. Secret-Sharing [BBEPT14].

Secretion [RSCX18]. Secretocracy [Ber16c]. Secrets [BT12, CG14b, DLWW11, FMS12a, Kob10, Man13, Bha16, Cop06, Cop10b, GGH+16b, Gup15, HRS13, LDC13, Sni11a, Ano17b].

SECRYPT [Ano19a]. Section [BdD19]. Secure [ADM19, AMKC19, AAL19, Alz+19, ACA+16, ADMM16, ABP+16, ABL+18, AARJ12, Ash14, AMH+16, BV+13, BIAL16, BG1H16, BCG12a, BCQ+13, BWA13, BJL12, BJJP14, BF11, Bru12, BD11, BCEM15, CFOR12, CCM+17, CZF12, CZLC14, Che15, CDWM19, CMA14, CDLW19, DM18, DL15, DMS+16, DG15, DYZ+15, DLZ+16b, Edw17, EAB+19, FLH13, FYD+19, FMC19, Fri10b, FD11, FSX12a, GQQ17, zGXW12, GKM16, GGHR14, GFBF12, GT12, GV14b, GHKL11, GM14, GZS+18, HvS12, HSM14, HLLG18, Har16, HL10b, HP14, HTZ+12, HMCK12, HLC+18, HKL+15, HYS18, HK14b, HL19, IL15, Jac16, JKA+18, JHW+19, KW14, KME+12, KHN+11, KYE+18, KD19, Kip15, KH10, LI+S+14, LL15, LH12, LYY+13, LTH+15, LTZ16, LSD15, LL19, LLGJ16, LSQ18b, LV15, LHL15, LWML16, LML12, LSC12, MLO17, MMP14, MDHM18, Mal13, MV1R12, MMS17b, MGJ19, MK12a, MKAA17].

Secure [NBZP17, NDG+17, NR12, NMS14, NSMS14, PB12, PSM17, Per13, PBC+17, PRN+19, QZL+16b, QZDJ16, QZZ18, RC18, RPM10, RR17, Rea16, RMZ19, RSGG15, RS19, SAM+19a, SNJ11, SSK16, ST19, SWS14, SVCV15, SP15b, SKH17, SS15, SRAA17, SAR18b, SSAF11, SVG16, SYW17, SYC+17, SMLS14, SZDL14, SGH15, SLY+16, SR12b, SM18, TB18, TCL15, TWZ11, TG12, TGC16, VTY18, VMV15, WGM12, WKB16, WXY16, WLY17, WC11L18, WDZ19, WHL15, WBA17, WWHL12, WS19, WMS+12, tWmC12, XWSW16, XL09, XJW13, XLP+18, XHZ+19, YNR12a, YNR12b, YTH17, YQZ+19, YHK+10, YKC+11, YAM+15, YY17b, YGD+17, ZZX+11, ZDL12, ZDH18, ZHV14, ZVG16, ZHT16, ZLW+17, ZHZ+19, ZBR11, AHS14, APK+18, ABBD13, ACF16, AKK+17,
ACD+15, AYSZ14, BMDT19, BOB13, BHH19, BZD16, BKR19, BSR+14, CCLL11, CSD18, CLHJ13, CW14a, CS11, CDL18, DA18, DEL19, DMM10, 
secure [DGL19, DMD18, FHH10a, FLYL16b, FS18, Gal13, GAI+18, GLL+18, GCH15, HGWY11, HWW+15, HLYS14, HTC17, HPY10, IB11, JZZ+10, KPP16, KKA14, KRM+10, KCS+18, Kου16, KLW+17, KDW+17, KKD+18, LLLS13, LDDAM12, LH11b, LLW16, LSR13, LHM+10, LDZ+14, LWK+18, LZWZ19, LWK+19, LCT+14, LAL+15, LJY16, LHH+18, LL16a, LL16b, LBOX12, MR14c, MHY+18, NR17, NAACL12, NAL17, ODK+17, OSNZ19, OSANAM19, PABC+19, Psdo+13, PSLvdLe10, PWS19a, PY19, PBP19, Rao17, RG10, RYF+13, RITF+11, RS15, SGGR+16, SYL13, SWW+16, SSI1, SM10c, SSLP+13, SXL16, SLXX16, SC19b, Tar10, TLLM13, THA+13, TLL12, VS11, WLZ+16, WMX+17, WXMZ19, WHZ+19, WDKV19, WCH18, WL19, XXWC14, XXX15, XZF+19, XMY+17, XWK+17, XYML19, YC12, yYqWqZC13, YZZ+14, YZC17, YQOL17, YY11, YLS12, YJC18, YMSH10, ZLY10, ZCLL14, ZZ15, ZQD16, ZYC+17, ZG10]. 
secure [ZZ12, ZX11, ZY17b, ZC12, Zhn13, ZZL+19, ZSW+18b, Ano12, DZLB18, HK18, OKG+12, YSS14, YFK+12]. Secure-TWS [OKG+12]. 
Secure [LC17, SGG18]. 
SecureLR [JHW+19]. Securely [CC10, KP17, LHL+14, MS16, WXY+17, BC18, der10]. SecureMR [DMD18]. 
Securing [AASSA18, BK12b, CMLS15, CST+17, Cla18, NPH+14, PMZ13, SFE10, SSMK18, SWF+19, SL111, Ste15b, TKR14, YMA17, YT12, YWW+19, CR10, Din10, GH15, SKS+18, SA15, Tox14, YZW+18]. 
Securities [WWL+14]. Security [ABJ13, AHN+18, ASBdS16, Ano13f, Ano15a, Ano15d, Ano19a, ABF12, AN15, ABHC+16, ABB+19b, AYS15, BCE+10, BSBB19, BA18, BCM+15, BCHL19, BRT12, BPR14a, BPR14b, BLS12, BCGN16, BDPS12, Bra15, BDH11, BP10, CFST17, CFE16, CBX19, CHS11, CFXY17, CCD15, CCD19, CCD20, CPS16, CM11, DDS12, Dan12, DR12, DK16a, DFKC17, Elb09, FREQ17, FMA+18, Fid18, FMA+19, FP19, FSX12b, FSX12c, GN16, GZZ+13, GR19a, GPR+19, GSC17, HC12, Hei17, Her19, HB17, HUS11, HWW12, HXC+11, HCL11, HLT+15, HLN+10, IEE15, IS12, IGR+16, JN12, JSA17, Jia14a, KBL11, KS18b, KFOS12, KSD+17, KDI12b, LPS12, LST12, LW11a, LK14, LLPY19, LJ17, LW12, LLZ+17, LTW11, LSQZ17, LYL+18, LSQ18b, LP12, LRW17, LZC12a, LWL+17, LZZ+19a, LNG19, LDB+15, LMS16, LLH18, MMKP16, MTK11, MKN13]. 
Security [MCS+15, MH14, Mau12, MV16a, MGG+19, MLBL12, PMP+17, MMHS16, Nac12, NNAM10, NGD+17, NVM+17, Nos11, Nos14, OSH16, Orm16, OS16, Pas13a, PZPS15, PGLCX17, PDNH15, PS16, PL16, PDT12, PNRC17, RB17, RCP+18, RVS+18, RQD+15, RWZ12, Rog16, RS10, SGG18, SN10, SNJ11, SBS+12, SBS8, SPD+10, Sar12, Sch13, SD12, Shi11, SC19a, SLM10, STC11, Sti19, SSP19, SAM+18, SMOP15, SCGW+14, Ts013, TV15, VFFHF19, Wal18, WYCF14, WSA15, WZC16, WRP70, WSS12, WTHL17, WCL+18, WS14, Yan10, YZLC12, YSF+18, YHSW19, YGS+17, YYK+17, YSS14, Yon11, YYW19, Zha15b, ZM18, ZX19, ZYY19, ZY17a, ZYH+19, ZCZ+19, VTJ11, AMN18, AB10a, Abe10, ABGR13, And19, ABM+12, Ano11a, AM19, AGBR19, ADH17, BYL10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTHP13, CLCZ10, CVG+13]. security [DLK+16, DGMT19, DXWD16, DHW+13, Edw14, FHM+12, FA14a, Fei19, Fis15, GHD19, GM16a, GLM+16, GMMJ11, GMS11, GH12, HPJ+19, HWDL16, HWG10, HLR11, HRS13, Hod19, HLV10, IAA+19, JK19, KNTU13, KSA16, KKK+16, Lan10,
Lan13, LDC13, LH10a, LZ11, LXM12, LHH11, LZC14, LSG16, LLG19, MZA+13, MZL+19, Men13b, MM14b, MSGCDPSS18, MSM+18b, NS10, Nam19, NCL13, NLYZ12, NML19, OK18, OYHSB14, PHWM10, PMG19a, QYW16, QLZ19, Ree15, RPSL10, RH10, SA12, Ser12, SY19, SLZ12, SY15b, SYWX19, Sir16, Sta11b, Tan17b, TODQ18, Tay19, THA+13, TKG+17, UUN11, VCK+12, WCFW18, XCL13, YLL+18, YY17a, ZAABB17, Zha15a, vdWEG18, XW12, YKC+12, Bar12].

Security-Aware [LJP17, LMS16, GHD19].

security-enhanced [AMN18].

security-modified [MM14b]. SEDURA [LY15].

see [PZ15]. Seed [AS17, LYHH14, Sun11].

seeing [Tox14]. seen [Goo12, PWS+19b].


Selected [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12].

Selection [KO14, KD12a, KD19, RP12, SEY14, YKA16, DRN16, FXP12]. Selective [BTHJ12, GDCC16, JSA17, LW12, LSC+15, LZC12a, LLH18, PWS+19b, LZC14, LW13c].

Selective-Opening [LLH18]. Self [Cer18, CLL16, CHHW12, CSV15, DM18, HZ11, LCL+17a, LPPY19, LH12, LHM14, PRGBSA19, RCK17, SAA15, SM12, TAP19, WHZ12, WXWC14, ZLDC15, AGH+17, FXP12, HIL14, LT13, LH13, SH11, YN19].

Self-adaptive [LHM14, FXP12, SH11].

Self-authenticating [Cer18].

Self-Authentication [LH12, LT13].

Self-Certified [CLL16, WXWC14, HL14, LH13, YN19].

self-composition [AGH+17].

Self-Controllable [ZLDC15]. Self-Defense [RCK17]. Self-Identifying [CSV15].

Self-Recovery [SAA15, CHHW12].


seller [KJN+16]. Semantic [DDY+19, MHW+19, YZCT17, HLR11, HT17, JS18a, WS19].

Semantic-aware [DDY+19]. semantically [PBP19, SLXX16].

Semantics [CM11, Gli12, KGP12]. Semi [AAA+19, BDOZ11, KKK+16, SEK+19, WHZ12, XZLW15, PLL10].

Semi-automated [KKK+16].

Semi-Autonomic [SEK+19]. Semi-Fragile [AAA+19, WHZ12, PLL10].

Semi-homomorphic [BDOZ11].

Semi-trusted [XZLW15]. Seminary [SS10c].


Sensemaking [HGOZ19]. Sensing [CCZC13, Kar12, MJS+19, PWS+19b, uHAN+18, RPG12, WXZW16, Fay16].

Sensitive [Kaw15, RQD+15, Tan15a, QCX18]. Sensitivity [YGD+17, LWW+10].

Sensor [ABC+17, BNI4, CS14, DS11, KH10, LLC11, LLZ+12, NNAM10, NVR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YM16, ASO14, APK+18, AIB+16, AIKC18, ADF12, BNNH19, BLAN+16, BB16b, CDGC12, CLSW12, DSCS12, DLN13, HKA+18, HTC+10, JNUH17, JMW+16, KLC+10, KO16, KLW+16, KDW+17, LC17, LNK+18b, PL16, RR17, SZMK13, SKK10, Wan13, WW14, WDVL18, WXX+17, XWDN12, XMHD13, ZYGT17, ZYL+10].


Sequence [PFS12, WGD+12]. Sequences [ADD10, Kla10, NN12, XP+18, XYXYX11, HLC12, VM14].

Sequential [GLR10, GLR13, HWZZ19, LLY15, TLZ+17, SM19a, WYL13].

serial [MCRB19]. Series [BJL16, EKOS19, Die12]. Serious [AG18].
Serpent [PC16], serpentine [KKM11].

Server
[AV18, BCO13, Che15, GMSV14, LSQ18b, LNWZ19, LY15, MV19, YLW13, ATK1+17, BK19, BBP16, CSD18, CLHJ13, FA14b, FHZW18, HDPC13, HL14, IS1+16, KMTG12, KLW1+17, LH13, MHL18, SY15b, hSZ15, SSAF11, SSS11, TLL12, WT10a, XHM14, YN19, YY13].

Server-Aided
[GMSV14, LNWZ19, MV19, SSAF11].

Server-Designation
[Che15, LSQL18b].

Server-Side
[BCO13].

Servers
[DRDI11, KKD1+18, PAB1+19, SG19a, WLWG11].

Service
[BKBK14, CCSI14, GKK18, GKG19, Hay13, LDB1+15, LBR12, MJW1+18, NRZ15, RSG15, SPG1+19, SPCC12, Sti15, VS16, VFFH19, AaBT16, AA1+19, HK17, KPP16, LHL1+18, LW13a, MMP19, MLM16, Par12b, SVY19, WU17, YWK10b, ZX11, CWZL13, YCM1+13].

Service-Based
[LDB1+15].

Service-Oriented
[RSG15].

Services
[An11b, DLZ1+16, JP19, MEPO12, OO12, PSM1+18, ZHL15, AZPC14, Bel18b, CXX1+19, CAM19, CSD18, CHX13, DYZ1+15, GAI1+18, IMB17, IG11, LWYM16, LZD1+19, MSL13, NDSA17, NZL1+15, OD1+17, PP11, WDKV19, XXX15, YJC18].

Session
[BS12, BKJP12, CFST17, SH12, AN15, BCFK15, DCAT12, DGMT19, SHBC19].

Session-Based
[BKBK12].

Set
[Cor1+14, EKP1+13, RS17a, YZ12, Con12, GR19b, TMK11]. set-valued [TMK11].

SETI [Sch16a].

Sets
[GL19, SPK17, SF12].

Settings
[GA19, GZ12].

Setup
[KZZ17, SOR16, Jia16].

Seventh
[CS10].

Several
[HLC1+19, Sas12, ZT14].

SGX
[MZLS18, TSB18, WBA17].

SHA
[AAE1+14, ABM1+12, App15, JCPB1+12, Con17, LC17, MAK1+12, Mor19a, NIS15, SKP15].

SHA-1
[AAE1+14, Con17, SKP15].

SHA-256
[App15, MAK1+12].

SHA-3
[ABM1+12, JCPB1+12, LC17, Mor19a, NIS15].

SHA1
[Con17, SBK1+17].

SHA256
[GWM16].

SHA3
[FLYL16b].

Sha
[Gol19].

SHAIP
[HRK18].

Shakes
[CNR14].

Shamir
[BDSG1+13, UUN11, WKB16].

Shannon
[AMS1+10].

Shape
[AAE1+14, Con17, SKP15].

SHA1
[Con17, SBK1+17].

SHA256
[App15, MAK1+12].

SHA3
[FLYL16b].

Shadow
[Kap11].

Shadows
[YSC1+15, SLXX16].

Sha
[Gol19].

SHAIP
[HRK18].

Shakes
[CNR14].

Shamir
[BDSG1+13, UUN11, WKB16].

Shannon
[AMS1+10].

Shape
[AAE1+14, Con17, SKP15].

SHA1
[Con17, SBK1+17].

SHA256
[GWM16].

SHA3
[FLYL16b].

Shadow
[Kap11].

Shadows
[YSC1+15, SLXX16].

Sha
[Gol19].

SHAIP
[HRK18].

Shakes
[ABK13, ACC+13, LL15, MEFO12, Sas12, SPM+13, CJXX19, GMMJ11, MCRB19].
single-factor [GMMJ11].
single-generation [CJXX19]. Single-SP [Sas12]. Singular [LSL12b, BWA13].
sins [HLV10]. SIP [KKGK10, ZT16]. SIP-based [ZT16]. SIPF [SYC+17]. Site
[DSB15, SS10c]. siteDriverID
[DSB15, SS10c].
SLV
[SM11b].
Size-Constrained [EAA12]. Skein
[FLS+10, KN10]. Skill [SCMS18]. Skin
Slantlet [TK14]. Slicing [MZ17b]. Slide
[IOM12, LC13]. Sliding
[BBB+17, Bro17, Win17]. SLISCP
[ARH+18a, ARH+18b]. SLISCP-light
[ARH+18a]. SLMAP [HCETPL+12]. Slow
[Smi11b]. SLV
[AV18]. SM2 [ZSH+19].
Small
[BGJT14, BKLS12, BB10, CJ13, HJ19, Kim15, LCLL15, NR15, WCTX17, YM16, 
YT16, AAT16, BGJT13, Jou13, MZ15, PT19].
Smart
[AN17, ABC17, BMNH17, BD18, BSJ15, DLZ+16b, HXHP17, HCL+14, HK18, 
LFH18, LA10, MGF16, PDT12, VHJ+18, WgMdZiZ12, WgMW12, AMN18, BC16, 
Bel18b, CHS11, CLHJ13, DZC16, GHD19, GA1+18, Ham19, HRK+19, HCC10, JZU+19, 
LH10c, LNM+11, LXMW12, LNKL13, LNK+18a, LZD+19, LWK+19, LTC+15a, 
MM12, MCN+18, SSSA18, SYWX19, WMYR16, YZZ+14, YSL+10, YY13, 
ZGL+18b, ZDHZ18, ZZY+19, Cho10, GLIC10, SD12].
Smart-Card-Based
[HCL+14]. SmartEdge [JZU+19].
Smartphone [MDMJ17, uHAN+18, DL15].
Smartphones
[Cor14b, GSAV18, MWW+18]. Smartwatch
[LFH18]. smartwatches [NM18]. smashed
[Fag17]. Smith [Ano16]. Smooth
[LYY+18a, XYXXY11, YC11, ZBR11]. SMS
[KRM+10, LH11a, Psdo+13, PCK19, RVS+18]. SMS4 [LYL+18]. SMSCrypto
[Psdo+13]. SMSes [SNX+17]. smuggle
[MSL13]. Snake [BBD16]. Snakes [PC16].
SNOW [PC16]. Snowden [Tox14]. SNUSE
[DEL19]. SoC [HZS+19, GSC17, ZAAB17].
Social
[BPDS17, GB19, KTA12, NSA15, 
NRZQ15, PYM+15, Rog16, SKGY14, 
SZZT18, VKH+19, WLY+15, WZCH19, 
ZW15, Zha15b, ZHL15, AQRH+18, BDK11, 
HYF18, LCM+17, LZC17, MSM+18b, 
SN+17, SKS+18, Smi15a, WMC17, 
WXMZ19, YZL+18, vdWEG18]. Society
[ATD17, Sch15a, Sch12b]. Socio [NS12].
Socio-Rational [NS12]. SoD [VN16]. Soft
[Her19, Jin10, TLCF16, SS17a]. Soft-Error
[TLCF16]. Softw [WZM12a]. Software
[Bar15, Bee17, BHC19, EWS14, 
FHLORH18, GZSW19, KYEV+18, 
LRVV14, MRL+18, MV16a, Sco18, 
SAM+18, TLZ+17, YGD+17, ZPM+15, 
AGHP14, ABF+14, CFh+13, DK17, Eve16, 
GGH+16b, GJ+12, HL10, KHF10, 
LBOX12, SF12, YWT+12].
Software-Defined [KYEV+18, SAM+18].
Solan
[CGB+10]. solid [Crt16]. Solution
[DHT+19, Frat15, GSFT16, HLKL15, Kam13, 
NA10b, YFT17, YFT18, Cor14a, MDHM18, 
SVGE14, ZAAB17, SAM+19a]. Solutions
[Ano19c, BCL19, LLGJ16, BLV17, KAS15, 
MMP19, OMPSP+19, TKG+17, WW14].
solve [Pec17]. Solved [IBM13a]. Solving
[Ano17c, BB10, Hod19, Bul10a]. Some
[AD12, Ber12, Dur15, LFW10b, Mid10].
someday [And19]. Somewhat
[HTC17, KOS16, MFB18, RJV+18]. Song
[Con12b]. Sood [MWZ12]. SOSEMANUK
[PC16]. SOT [PAF18]. SOT-MRAM
[PAF18]. Sound
[COP+14, Gol19, HCY18, LSL13, Sav15].
Source [Bis17, FKO15, MBC15, RWL14,
Source-Based [MBC15]. Source [Lal14].
[Boy16, ZYY19, MvO11, RK11]. Strongly
[DDM17, HHP17, KW14, YS12]. Structural
[LYY+18b, BKD11]. Structure
[CJZ13, HP12, LDMM14, LJ15,
LLG19, MKRM10, WYCF14, WJ19, CD16a,
JKA+18, LXLY12, SM19b, ZLW+12,
ZPWY12]. Structure-Independent
[MKR10]. Structure-preserving
[LLG19]. Structures
[GTT11, HHH+13, LHKR10, LPL15, PB12,
TSB18, DDFR13, MHKS14, PPG19, Shy15,
WS12, XWZ+18, ZZ15]. STT [VDB+16].
Students
[PP10a, SDC+17, SPG+19]. Studies
[Uto13]. Study
[AIF+19, Ano17c, DDR+16, MZLS18,
SY15a, SPG+19, STC11, CC10, EBKF13,
KD18, MHV15, SS17a, VG14]. Stuxnet
[BPM12, Kus13, Zet14]. Style
[GHPS12, GHPS13]. Stylistic
[BAG12]. Sub [GPLZ13].
sub-passwords [GPLZ13]. Subcommittee
[Bla16]. Subgroup [CCL+19]. Subject
[SC19a]. subliminal [LWZG10].
submarines [McG11]. subnormal
[AKM15]. Subrecursive [BBD19].
Subscribe [BGP+17, DLZ+16b, OFMR16,
PRSV17, SLI11, TRK14, YSM14]. Subset
[BS14, RP12, AVAH18, ZZ11]. subspaces
[ZWM14]. Substituted [HD19].
Substitution
[DA10, KTM19, SGFR1+18, FVK17].
substitution-transposition [FVK17].
Substring [MRR+18, SOR16].
substraction [MRT10]. success [Ano14a].
 Succinct [BTC+13, CKLM13]. Such
[Roh19]. sufficient [TD14]. suitable
[Jeol13, SKB+17]. Suit
[MTM18, NAACL12]. sum [AVAH18].
Sumo
[BS12]. Sums [SS12b]. sum [Cer15].
Super
[Sch19b, BCND19, MZ17a].
super-activation [BCND19].
Super-Isolated
[Sch19b]. Supercycle
[BHJO18]. Superpoly
[HIJ+19]. Supersingular
[FHIOJRH18, Lai17, LNL+19, Y+17].
Supervised
[CTC+15, GSAMCA18, HXHP17]. Supply
[QZL+16a, QZL+16b, YFT17, YSF+18,
YFT18]. Support
[MU18, ZZQ+19, CZ14, HHAW19, JAS+11,
MMF15, PWW10, PA15, TNL10, VCK+12,
ZMM+10, ZBR11]. Supporting [BHH19,
CDLW19, FMTR12, HGOZ19, HCDM12,
PH16, SG12, SOR16, Ver17, ABR13, HZL18,
JSMG18b, YYS+16, CWZL13]. supports
[WR15]. Surfaces
[Sch19b, CDSLY14]. Surprises
[Bow11]. Surrpexion
[SFRR15]. Surveillance
[BPR14a, BPR14b, GZH17, KKL+19, Lan10, Ano16h, Fei19].
Survey
[AAUC18, ACKB19, ABH+16,
ABB+19b, BGN17, BCTPL+16, BHJP14,
BJCHA17, CLB19, DM19, GMD19,
HP10, KMY18, KSD+17, LGM+16,
MR14b, MSH18a, MS10, MRR+19,
NV10, OFMR16, OMNER19, PGLCX17,
PWS19a, SHH17, SPP19, TR11, TS16b,
VV18, AA+16, ABB+14, ADH17, BM13,
BBG+13, BEB+18, FMA+18, HKA19,
HT13, HATDR13, KJN+16, KAS15,
LK10, MMP19, Ma17b, Maz13, MHV15,
MR11, PA18, TZZT16, TGK+17, VBC+15,
WW17]. Survival
[YCM+13, MMS+17a].
Surviving
[CFST17]. suspect
[der10]. sustainability
[KPB18]. SVC
[MU12, WDDW12, ZLDL12, ZLDL14].
SVD
[AM19, FYD+19, LP12, TB18,
ZWW17, ZWZ17a, ZWZ17b]. SVM
[TL13]. swarm
[ZSM18]. Swarms
[VOGB18]. SWIFT
[PLCGS11]. Switching
[CNT12, GHS12, GHPS13, WB12,
WWW12]. Sybil
[AQRH+18, dCCSM+12].
Sybil-precaution
[AQRH+18]. Sylvester
[SS10b]. Symbol
[CS10]. Symbolic
[BCEO19, BCEO20, Bul18, CBRS19, Wat10].
Symmetric
[BPR14a, BPR14b, BDPS12, CVM14, FSP12,
GFBF12, JCHS16, KTT12, Kha10, MM17b,
PR12, PCY+17, TWZ11, WRP70, YKNS12,
BGG+13, CGKO11, DLZ16a, FH13,
GMRT, GMdFPLC17, Gor10, GCVR17, HK19, KAS15, LZF17, SKK10, ZCZ+19.


Synergy [KRB12]. Synergy-Based [KRB12]. Synopses [RCBK19]. Synthesis [SKE+18, TCMLN19, RS17c]. Syst [HYS18, WZM12a].

System [AD11, Alz19, Ano10a, BBC19, BD18, CZLC12a, CZLC14, Cor14b, CRST15, DDE+19, DG15, GOPB12, Har16, HHS+19, HZS+19, IAD10, JN12, JLZ18, JWJ+17, Jin10, KMP+11, KZZ17, LYS+19, LFX+18, LSY+16, LHW18, Lop12, MMBS19, MLBL12, NSMS14, PSSK19, QLL17, RSCX18, SNM18, SRAA17, SLI11, XZL+19, YE12, YXZ+12, YKK18, ZM17, ZPW16, ZLDC15, ZVG16, AHM+18, ARG19, BIC18, BGG+13, Bul10a, CH11, CTL12, CZ14, CS11, FYL16b, FNWL18, GKCK11, GH15, HHBS18, HSK+15, HJM+11, HLYS14, JC13, KGP+19, LLLK10, LLL+17b, LHH+18, Lit14, LTC+15a, LLL+18, LZK19X, MS12a, MNNW15, PSOMPL13, SSPL+13, WMX+17, WDZ19, WGWZ+12, XWZW16, XYML19, YZL+18, YWW+12, ZCZQ19, ZYGT17, ZMM+10, ZML17, ZZL+18, KKA14, Dew11].

System-Level [BBC19, JWJ+17].

System-on-Chip [HZS+19]. Systematic [CCG+16, CBL13, PC16, IAA+19]. Systems [AMSPL19, AN12, AEPC16, AB15, Ano19a, BL15, BL16, BS13b, BCTPL16, BB10, C19, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HLN+10, HK18, KS18a, KKK+19, LLY+18a, LMD16, LQY10, LY16, LNZ+13, MT17, MR14b, MJS+19, OS12, PGLCX17, PMG+19b, PRSV17, PH16, QZL+16b, RST15a, RST15b, SBS+12, SBS18, SSLK16, SFK15, Sev16, SKH17, SG14, SMD+12, STC11, SSP19, TKR14, YNR12a, AT10, AT1+10, BK19, BGE+18, BD1+19, CFV16, CFZ+10, CLZ+17, Cla18, dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DEL19, DZS+12, Eis10, FXP12, GMGCCC15, GH19, GSN+16, GPVcBRO12, HZW18, JSK+16, JHCC14, KSA16, LCL+15, LWK+18, MDHM18, MLSMSMG12, MGP10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRB+12, SMS+16, WDG19, WS14, YSM14, ZAAB17, ZGL+18b, ZVH14, Zhi13, MA17b, MMKP16, Ano11a].

Systems-on-Chip [KSI18]. Symtolic [MCDB12]. Systolic-Array [MCDB12].

SZK [MX13].


Tampered [SAA13]. Tampering [ABSS19, CG14a, QIC+18, SRAA17, HYL+19, SGP+17]. Tangible [LHF18].

TAO [Sta13]. Taormina [Cra12]. Tap [NM18, ADG16]. Tap-based [NM18]. taps [GSV18]. Target [CZ19, APMCR13, HRS16, LSQ15].

Target-driven [APMCR13, LSQ15].

Targeted [ABJ13]. Tasks [TS18].


Tampered [SAA13]. Tampering [ABSS19, CG14a, QIC+18, SRAA17, HYL+19, SGP+17]. Tangible [LHF18].

TAO [Sta13]. Taormina [Cra12]. Tap [NM18, ADG16]. Tap-based [NM18]. taps [GSV18]. Target [CZ19, APMCR13, HRS16, LSQ15].

Target-driven [APMCR13, LSQ15].

Targeted [ABJ13]. Tasks [TS18].
ED19, Köp13. Third-Party
[OSH16, QZL+16b. Third-Round
[Gre19a, thou [BDK11. Threat
[CSVY18, ALL+18, Ven14, ZMYB17. Threats
[AJA16, ERLM16, GSC17, LJS+14, vdG17, TKG+17. Three
[AMSP19, CZ15a, HXC+11, LLY+18, LZC+12b, OSANAM19, PC16, Shi11,
YKNS12, AIB+16, CNF+18, HWB10, IC17, JKL+16, LNK+18a, LNK+18b, LML+13,
Tso13, TKHK14, XCL13, YC12, YZZ+14. Three-Dimensional
[LLY+18, LZC+12b. Three-Factor
[AMSP19, HXC+11, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b. three-party
[HWB10, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14. Threshold
[CT11b, Cil11, FGM10, GLW13, HEP+11, HYS11, LML10b, LYY+16, SSU12,
Stat12, Tan11, WYCF14, WLH15, XLQ09, YFF12, YHK+10, YLA+13, ZCL+12, DZ14,
FGMP12, HF14a, HH15, JSMG18b, JLY16, OO10, QD16, SES+16, Shy15, SGM16,
TD14, ZKJ+14, ZPWY12. thresholding
[PC14. thrive [Sch12b. Throughput
[HMKG19, MAK+12. Thru
[SYC+17, SYW17. Thwart [LJS+14. Thwarting
[LWML16, XT10k. Ticket
[LMJC11, tied [Men13b. Tiered
[GGK18. Ties [PYM+15. Tight
[GDCC16, LPS12, LLH18, ZYH+19. Tightly
[HELLG18. Time
[AEPI8, ASBD16, Aon17d, Append1, AYS15, BBCL19, BJL16, Che17, EKOS19, FD11,
GSC17, HC17, HGT15, IF16, JWJ+17, JEA+15, KME+12, LCL+17a, LFX+18,
MWES19, NA10a, Nov10, PNRC17, Raz19, RHLK18, Ste15b, WLZL12, YE12, AY14a,
Aon15d, BM15, CC14, DCAT12, FHH10a, GPLZ13, GMdFPLC17, HU15, LW10,
LW13b, LML+13, MK11, NSX+18, Par18, SPK17, WDG19, XLC+19, Aon16i. Time-area
[Nov10. Time-Delay
[LFX+18. time-invariant [GMDFPLC17. Time-Memory
[ASBD16. Time-Series
[BJL16, EKOS19. Time-Space
[Raz19. Time-Specific [KME+12. Time-Spread
[HGT15. Timed
[Jia14b, KFOS12, Tan15a, Unr15, WSS12. Timed-Ephemizer
[BGN17, FDY+19, GV14b, HAY13, LGR14, LFK19, VCD16, YDV19, AKM+15,
AGH+17, MCL+19, SRB+12. Tiny
[AV18, AP13, BBDL+17, BFCZ12, BJR+14, CFN+14, DAI11. TLS-based
[Ber16b, Cla18, Mac12. Token
[Ye10. Token-Leakage
[ZM16. tokenisation
[Mar10b. tokenless [Wat14a. Tokens
[Muf16, DCAT12, HU15. Tokyo
[Sah13. Tolerant
[HK14b, M KK17, WCD19, ZM16, BZD16, JLT+12, WMYR16, XW13. tolerating
[ZW14. Tone
[Yam12. Too
[DL15, DSSDW14, DSSDW17, Ros11. Tool
[ASM12, DKMR15. Toolbox
[AHS13, TRD11. Toolkit
[BJL12. Tools
[Abe12, BKBK14, GO17, Ste15a, Lan11. Top
[SS12a, SS10c, Sta13, CHX13. top-
[CHX13. Top-Fanin
[SS12a, Top-Secret
[SS10c. Topics
[SCPSN10a, SCPSN10b, AB10b, DUN12a, KI11, Pie10. Topology
[HMK14. Topology-Preserving
[HMK14. Tor [LLY+12a. Toronto
[MV12. torsion [HR19. Tossing
[ALR13, DSSM14, Fok12, BB14. Touch
[KTM+18, MWW+18, SPW+16, SHBC19,
Alp18, CTL12, IAA+19, NSBM17, TZT16C. touchstroke [Alp18. TouchWB
[MWW+18. Tower [ZAG19. TPM
[GY13, KHN+11. TQC [vDKS11. Trace
[ABR12, GA19, PS14, AA14, WGGT10. Traceability
[HECTPL+12, WYML16,
WHLH16, YFT17, Chi13a, YYS+16.

Traceable [LDZW19, QRW+18].
Traceable-then-revocable [LDZW19].
traceback [LWY12, PJ18, WYL13]. traces [MYYR13].

Track [Dun12b, Kla11, Pie10].
Tracking [GZH17, MDMJ17, SNCK18].

Track-Offs [ASBDs16, BS14, GPR+19, SR10].
Trade-Os [ASBDs16, BS14, GPR+19, SR10].
Trading [TW12].

Traditional [SPK17].

Traffic [BSA+19, DRS16, FGRQ18, HS18, KAHKB17, VV18, ACM19, AZH11, FTV+10, PPR+12, Tay19, VS11].
traffic-feature [FTV+10].
Traffic [HM12, GSAMCA18].

Traitor [LVRY10].
Transaction [BGAD12, MMLN15, KVvE18, OYHSB14].
Transaction-based [BGAD12].

transactional [SPK17].
Transactions [DG15, Mic16, Mu16, PAS13b, TV15, DK12, FG19, MLMSMG12].

Transceiver [NBZP17].
Transcript [Gli12].
Transfer [AMSPL19, DN12, FMTR12, HL10a, LCCJ13, WCL+18].
transferable [GZX19].
Transform [AN12, BCPV11, KTM19, LSL12b, pNyWyY+14, OWHS12, SM12, YWNW15, BW13, MO14, NES+14, PC14, ST15, TK14, yWpWyYpN13].

Transformation [CRE+12, FJHJ12, NBX13, TFS19, tWmC12, GZHD12, HQZH14, PGLL10].
limitations [CJXX19, SA14].

Transforming [Eya17].
transmission [AK14a, BCDN17, BCND19, OSANAM19, PSdO+13, WQZ+13].

Transmissions [CBO+18].
Transmitter [KPB17].
Transparency [TJZF12].

Trust [Bar15, BL16, BCK17, DCA19, Gli12, GM14, GSFT16, HHBS18, IGR+16, KMSM15, KGP12, PYM+15, PH12b, PAS13b, Rau15, SG12, TMGP13, TV15, WLY+15, Zha15b, BSBG19, CO11, KGO10, MLMSMG12, MGP10, Sch12b, YTL11a].

Trusted [AWSS17, EAA12, FPY15, SS15, YCR16, ED19, HT+10, Kup13, SP+10, ZXLW15, YI17].

Trustworthiness [RSX18, WXSH19].

Tunnels

Tunnel [VDB+16, ZBR11].

Turing

Turtle

Tutorials
Tweakable [CMLRHS13, LST12, MLCH10, MKASJ18, Sar1, Zha12].
Tweeter [BTW15].
Twee [BCV12].
Twelve [BCV12].
Tweakable [CMLRHS13, LST12, MLCH10, MKASJ18, Sar1, Zha12].
Two [Ash14, ATC17, Bra12, CTL13, DZ14, ED19, GGH14, GL16b, HP14, HWB10, KMTG12, KO16, KU12, LLC11, LW19, Lit14, NSMS14, OTD10, YSL10, YLW13, ZM16, AN15, BD18, CSD18, CHS11, Con17, DHW13, FIO15, GMMJ11, HZW19, HPC12, HWDL16, HWB12, JLT12, JMW16, Kem11, Li10, LM14, MDHM18, McG11, MX15, OMPS19, QYWX16, Rus15, SM10b, hSZZ15, WW14, Wat14a, YT11b, ZZC15, GHKL11].
two-channel [JLT12].
two-dimensional [HZW19].
Two-Party [Ash14, HL10b, HP14, KOS16, NSMS14, ZM16, FIO15, HPC12, HWB12, ZZC15, GHKL11].
Two-Round [GGHR14].
Two-Server [LYW13, KMTG12, CSD18].
two-way [LM14].
Two-Device [MD12a].
TWS [OKG12].
Type [AKP12, CFL13, HWS19, PFS12, SH15, ACD18, BN17, GJ19, SYL13, WB12].
Type-based [CFL13, SYL13].
Two-Flaw [SH15].
Two-Phase [BCEM15].
Typing [CCDD19, CCDD20, SCR19b].
U.S. [Maf16].
Ubiquitous [HFS19, OS16, Par12b].
U&SDE [YZ12].
UHF [HQY16].
UK [Che11, PJ12, vD11, Ano15c, Kum10].
Ukraine [OGK15].
Ultra [SBS18, AATM18, GW14, TG17, WCFW18].
Ultra-Lightweight [SBS18, AATM18, TG17, WCFW18].
ultralightweight [ACM12, GMSW14, SB17].
UMTS [OHJ10, TM12].
un-traceability [Chi13a].
unaided [CAM19].
Unattended [BN14].
unauthentic [MLMSM12].
Unauthorized [CBO18].
Unbounded [LYW13, YZ12].
unbreakable [Bha16, Pan19].
Uncalibrated [SGP12].
Uncensored [Ald11].
Uncertainty [FHS13, BBGT12].
Unclonable [Ano16f].
Unconditional [Jia14a].
Unconditionally [CFOR12, LHF12, NJ11].
Unconditionally-Secure [CFOR12].
Unconstrained [GEAH11].
uncorrelated [MSS18b].
Uncovering [FMS12a, WBC10].
Undeciphered [RRo10].
Undeniable [BHG12].
Underbelly [Her19].
underfeeding [BBBP13].
derunhanded [Cra14].
Understanding [Elb09, EPAG16, P10a, Bar12].
Undetectable [CEL19].
Undisturbed [YCL17].
Unexpanded [SA16a].
Unforgeable [HHP17].
Unidirectional [LSC12, DKL16].
Unified [HK17, ZSW12, ABO17].
Uniform [HZS19, QJC18].
uniformly [YKL12].
Unilaterally [GRL12].
Unintended [ESS17, SS19].
union [BBDDL17, Bud16].
Unique [SSPC12, SOS15, GSGM16].
unit [PP10b, Sta13, MS13a, MS13b, MS13c].
unital [WMU14].
units [ABDP15].
Universal [ASM12, BKST12, BJJ12, NR12, KS19].
Universally [DN12].
University [LW17, FNW18, LFZ17].
University [Ano17b, CGB10, Wes16].
unlike [Goo12].
unlikely [Fag17].
Unlimited [IBM13].
Unlocking [VS16].
unmanned [XWZW16].
unpaired [CL18].
Unprovable [Pas13a].
unsafe [Con17].
Unsigncryption [EZ15].
unspoofable [NR11].
unstructured [CML16].
Unsupervised [CZ19, HFW19].
Until [BWS19].
untold [Mun17, Pea11].
untraceability [KIH19, YHL16].
untraceable [AIKC18, JMW16].
Untrusted [HZX+18, LQY10, MS16, ATKH+17, DRD11, MvO11, WS13].

Updatable [LLPY19, LCL+17a]. Update [BCE+10, KE19, LQY10, FS18, WLFX17].

Updated [BSW19]. [VOGB18].

Updatability [GCSADDP11, LJWY18]. Upper [AVMZ12].

URLs [AY14a]. USA [Dun12b, IEE13, IEE15, Kia11, Lin14b, MSH+16, Pie10, Rab10, ACM10, ACM11, IEE10, IEE11b, TT18].

USability [RAZS15, GMMJ11, KNTU13]. Usability [BCE+10, KE19, LQY10, FS18, WLFX17].

Usage [HR19, NSP+18, AKK+17, BHCdFR12].

Use [CSV15, DFKC17, IM16, KOS16, NR12, SD17, Söd13, YT12, der10, CZ15b, Die12, dCCSB+16, Dya19].

Usenet [Bel18a]. User [BOP14, BLV17, BKJP12, FLH13, GMDR19, GmM16, GMMJ11, Har16, HWZZ19, JN12, Kni17, LCL11, LCL17b, MZHY15, MBC15, MDMJ17, OdH12, PdT12, PWV12, RVH+16, SOR16, SZDL14, SP+13, VJH+18, VFFHF19, WgMdZIZ12, WgMW12, WAK+19, ZHS+19, ZPW16, AaBT16, ATKH+17, APK+18, BT18, CH10, CHS11, CLHJ13, DSCS12, DEL19, GH16, GTSS19, HFCR13, HL12, HL14, JS18a, KLN15, KKM+13, KLW+16, KDW+17, L10c, LNM+11, LNLK13, LH16, MM12, MWW+18, MML16, MHL18, NM18, OKG+12, SCFB15, SK18, SSNS15, liSSZ15, SPK17, SHBC19, VGL14, WLWG1, WDKV19, WT10a, WOLS12, YHL16, YSL+10, YN19, ZWY+19].

User-centric [BLV17]. User-controlled [Har16]. User-Friendly [SZDL14, WOLS12].

User-Generated [LCL17b]. User-Level [BKJP12]. user-participating [CH10].

User-related [GMDR19]. User-Tailored [Kni17]. User-Transparent [ZHS+19].

Users [DPCM16, KKA15, TAKS10, WPZM16, ATK11, Bel18b, uHAN+18, FLYL16a, FHM+10]. uses [Rus15]. Using [AA19, ABS+12, ABB+14, Alz19, Ano15a, Ayu12, ARM15b, BBC+13, BCPV11, Bee17, BP06, BFMT16, BKL12, BJ+14, CST+17, CCC19, CCL+13, DSB16, DR12, DA10, DBPS12, DL12, ERLM16, ERRM15, EZW18, FHL19, FMS12a, GWP+19, GH11a, GMDFPLC17, GM16b, GSC17, GAS+16, HEK18, HXHP17, HHS+15, HD19, HWZZ19, IL15, JSA17, Jin10, JEA15, KTM19, KBL11, KÖ14, KH+11, KG19, Lac15, Lan11, LYZ+13, LY+18, LLGJ16, LCR+18, LBC18, MM17a, MBC15, MRL+18, MS16, NIS12, NGAUH16, NNAM10, NN12, NSM14, PMZ13, PSS+13, PA18, PDMR12, PdT12, PCPK14, RX18, RRM19, RVRCM12, RHLK18, SR12a, SFE10, SS17b, SS19, SSA13, SCC12, SR12b, Tani12, TKR14, VJH+18, WWL+14, WgMdZIZ12, WHLH17, WY12, WAK+19, XNP+18, XZZ18, YM18, YWW10, YNNW15, YYM19, YCL17, YSS14, ZH15, ZWW17, ZWZ17a, ZP16].

Using [ZS12, dRSdlVC12, ACMP19, AASSAA18, ATKH+17, AHM+18, APK+18, ASVE13, BK19, BLL+19, BOP14, BM13, CS+18, CHS11, CR12, CLHJ13, CB16, CP13, Cri16, DA18, Dav11, DTZ12, DGFH18, DMD18, uHAN+18, EEA13, FES10, GQH17, GR19b, GSAAMA18, GSA18, GSGM16, HAK19, Ham19, Har14, HK14a, HK17, HZWW17, HFCR13, HWB12, HLI4, HPY10, HCC10, HS11, JKA+18, JCHS16, JCL+18, JM+16, KG+19, KI11, KY10, KKK14, KCS+18, KM11, KKK+18b, KSU13, KTUI16, KP17, KD19, KLW+16, LXX12, LLP+18, LC17, LH11a, LH10c, LNM+11, LXMW12, LH13, LZKX19, LM14, LML+13, MM12, MML15, MS13a, MMSD13, MM14a, MKH+12, MRRT17, MSR+17, MSM+18b, MGB19, NSX+18, NTKG17, NSBM17, PBC14, PB19, PC14, QD16, RR17, RS15, RS17c, SCFB15, SKE+18, Sar11, SM19a, ST15, SGFCRM+18, SKS+18,
SAR18b, SPK17, SLXX16, SA19. using [SC19b, SCBL16, TLCF16, TG17, TK14, TL13, UUN11, yWpNyL11, gWpNyY+14, WMX+17, WHJ17, WXK+17, YWJ+19, YQH12, YZZ+14, YSL+10, YN19, ZZKA17, ZLW+12, ZYC+17, ZXW+18, ZZL+18]. uth [CHL19]. utilization [NZM10]. Utilizing [BM18].


W [Mar10a, Xie12a, Xie12b, Hü13]. W-OTS [Hü13]. WA [LCK11]. Waknaghat [CGB+10]. Walker [Xie12a, Xie12b]. Wallets [Chi13b]. Wallis [Wes16]. Wan [RSD19]. wants [Nor17]. War [Has16, Mun17, Bud16, Car11, Smii11a]. Warbler [MFG16]. Warm [MCL+19]. warriors [Bud16]. wartime [McK10, McK11]. was [Goo12, LHA+12]. Watching [NSP+18]. Watermark [CHHW12, DLM+18, EMW14, FRR15, GRRZ18, Jiao10, KBL11, LZZ+12b, MCDB12, QJC+18, SJ12, YE12, ZS12, HB13, TLL13, WYL13]. Watermark-Based [GRRZ18]. Watermark-Driven [DLM+18]. Watermarking [AAA+19, BCGAPM12, BF12, BCFV11, BBD14, BCG10, BBM15, CG12b, CHHW12, CCZC13, CHN+18, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HEK18, HD19, HGT15, HM14K14, JZSS12, Joh10, JKH+Y12, KD12a, LSL12b, LLY+18, LP12, LD13, MM17a, MR16, MU12, NGAuH16, NC12, NEX+17, pNYWY+14, OWHS12, RS16, RP12, RR11, RMG18, SA15, SLGZ12, SS17b, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZW12, WYW+13, gWPWY+14, WX1+17, yWXY+18, WK18, tWmC12, XNG+14, XNR15, XNP+18, YWNW15, YPR17, YKK18, YOO15, ZXY+11, ZWGW17, ZWZ17a, ZWZW17b, AP10, AIA+18a, AIA+18b, AIM+19, AM19, AMK12, BWR12b, BW13, BWA13, CCL11, CT11a, CSS+13, GZH12, GA11, HAIK9, HKA+18, HU11, HK14, HWYW14, HPL+19, JK13, KMG17, KPS10, KZN+16, KM11, LSR13, LXC11, LLHS12, Lin14a, LHY12, MMSD13, MM14a, MO14, MK11, NC13].

watermarking [PTK14, PWLL13, PWL10, PGLL10, PKS18, PC14, PPR+12, RS17c, SKS+18, Tay14, TK14, TTL10, TPK12, WLDB11, yWPWL11, Wan13, yWPWY+1, WZW13, YWT+12, ZZKA17, ZS18]. Watermarking-Encryption [SLGZ12].
References

Akyildiz:2014:OTB

Abouaroek:2019:NAU
Musaeed Abouaroek and Khaleel Ahmad. Node au-

**Aditya:2019:ISF**


**Applebaum:2017:AC**


**Abo-alian:2016:KDB**


**Ambrosin:2016:FAB**


**Albertini:2014:MHE**

Ahmad:2019:PQE


Al-Azzam:2018:SRC


Akleyklek:2016:SPM


Aghili:2018:ISA

Seyed Farhad Aghili, Maedeh Ashouri-Talouki, and Hamid

**Acar:2018:SHE**  

**Alizadeh:2016:AMC**  

**Abdalla:2010:PCL**  

**Atallah:2010:ATC**  

**Anand:2015:ICL**  
REFERENCES

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


Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan Capkun, Gerhard
REFERENCES


Almeida:2013:CCA


Arnold:2012:ICC


Ateniese:2017:LCS


Agrawal:2018:RLR


Ambrosin:2017:OBB

Moreno Ambrosin, Paolo Braca, Mauro Conti,

**Adrian:2015:IFS**


**Agosta:2015:OPP**


**Adrian:2019:IFS**


**Abe:2010:ACA**

Masayuki Abe, editor. *Advances in cryptology — Asiacrypt 2010: 16th international conference on the theory and application of cryptography and information security*, Singapore,

Ab:2012:TBG


Ariaga:2012:JSS


Almeida:2014:COS


Ananth:2013:SFP


Avoine:2016:SSP


REFERENCES


Aldaya:2019:MTA

Applebaum:2010:PKC

Alzubi:2016:SCC

Arias-Cabarcos:2015:BIP

Armando:2013:AFB

Arnold:2015:NGH
REFERENCES


Avoine:2012:PFS


Aceto:2019:MME


Ausz:2011:SWL


Alvarez-Cubero:2016:AVL

Aizatulin:2012:VCC


Anyanwu:2010:DCS


Ayday:2012:DAA


Aliberti:2016:RPS


Attasena:2017:SSC


Abraham:2019:DPL

dl.acm.org/ft_gateway.cfm?id=3303712.

**Adikari:2011:HBT**

**Abdalla:2012:LBH**

**Abro:2019:LEE**

**Andrychowicz:2016:SMC**

**Araldo:2018:CEC**

**Anandakumar:2018:RHA**
Ahmed:2017:IRD


Attrapadung:2015:RGS


Aminifar:2018:OME


Aumasson:2017:SCP


Atighehchi:2019:GHC


Antonopoulos:2017:DIS

Timos Antonopoulos, Paul Gazzillo, Michael Hicks, Eric Koskinen, Tachio Teraiuchi, and Shiyi Wei. De-

**REFERENCES**

<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Issue</th>
<th>Pages</th>
<th>CODEN</th>
<th>ISSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Attrapadung</td>
<td>Nuttapon Attrapadung,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ali:2018:ECM


Akhtar:2018:BSI


Appelbaum:2013:SSG


Au:2020:SIC


REFERENCES


**Azarderakhsh:2014:NDP**


**Almulla:2013:CKE**


**Anada:2017:CGS**


**Alabdulatif:2017:PPA**


**Afanasyev:2011:PPN**

Andrysco:2015:SFP


Armknecht:2012:STH


Arfaoui:2019:CAA


AlTawy:2013:SOC


Aiash:2015:IAA


Aldrich:2011:GUS

Richard J. (Richard James)
REFERENCES


Au:2018:PPP


Alomair:2012:AEH


Asharov:2013:FCF


Alzahrani:2019:SAC

Araghi:2019:EHI


Awad:2016:SSZ


Aghili:2019:SSL

Abarzua:2018:ASC


Abbasinezhad-Mood:2018:DHI


Adj:2013:WDC


Aumasson:2014:HFB


Ahmadian:2010:PDS

cess control and ownership transfer scheme for e-health systems in IoT. [AN15]
FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://
www.sciencedirect.com/
sience/article/pii/S0167739X18331297.

Alvarez:2012:CAB
Rafael Álvarez, Francisco Martínez, José-Francisco Vicent, and Antonio Zamora.
Cryptographic applications of 3 × 3 block upper triangular matrices. Lecture
Notes in Computer Science, 7209:97–104, 2012. CODEN LNCSD9. ISSN
com/chapter/10.1007/978-3-642-28931-6_10/.

Albrecht:2012:SDL
Alexander Albrecht and Felix Naumann. Schema decryption for large extract-
transform-load systems. Lecture Notes in Computer Science, 7532:116–
link.springer.com/chapter/10.1007/978-3-642-34002-4_9/.

Arshad:2015:SAI
Hamed Arshad and Morteza Nikooghadam. Security analysis and improvement of
two authentication and key agreement schemes for session initiation proto-
col. The Journal of Supercomputing, 71(8):3163–3180, August 2015. CO-

Aga:2017:ISM
Shaizeen Aga and Satish Narayanasamy. InvisiMem: Smart memory defenses for
memory bus side channel. ACM SIGARCH Computer Architecture News, 45(2):

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
SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL http://
Anderson:2013:MNF


Anderson:2019:QCN


Anghelescu:2016:FIP


Anonymous:2010:NDS


Anonymous:2010:MML


Anonymous:2011:AIS

Anon
Anonymous:2011:AXL

Anon
Anonymous:2011:MCB

Anon
Anonymous:2012:SHS

Anon
Anonymous:2013:CFF

Anon
Anonymous:2013:CRR

Anon
Anonymous:2013:DSS

Anon
Anonymous:2013:NCI
Anonymous. NSA has cracked Internet encryption protocols. Network Security, 2013(9):1–2, September 2013. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (elec-


[Ano16c] Anonymous. Call for papers special issue on

**Anonymous:2016:EMT**


**Anonymous:2016:FVM**


**Anonymous:2016:GUP**


**Anonymous:2016:ICd**


**Anonymous:2016:MBE**


**Anonymous:2016:SWT**


**Anonymous:2016:SIR**

Anonymous:2017:BA

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

Anonymous:2017:BRM


Anonymous:2017:CCS


Anonymous:2017:HDQ


Anonymous:2017:MBH

against quantum computing attacks.

Anonymous:2017:RV


Anonymous:2019:GES


Anonymous:2019:HCC


Anonymous:2019:PBT


Anonymous:2019:HCC


Anonymous:2019:PBT


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW

Parag Agarwal and Balakrishnan Prabhakaran. Blind
REFERENCES


Aumasson:2011:CHF


AlFardan:2013:LTB


Abellan:2018:FCQ


Ali:2018:SUA


Alcaide:2013:AAP


Applebaum:2013:GXG

Benny Applebaum. Garbling XOR gates “for
References


Applebaum:2014:CCP


Appel:2015:VCP


Albrecht:2015:FBR


Al-Qarni:2012:EI


Al-Qurishi:2018:EKA

REFERENCES

Arai:2013:MDH

Arab:2019:IEM

Adj:2014:SRC

Altawy:2018:SLT

Altawy:2018:TCM

Agudo:2013:PAC
Isaac Agudo, Ruben Rios, and Javier Lopez. A privacy-aware continuous

**Abdulrahman:2015:NRR**


**Azarderakhsh:2015:PHS**


**Armasu:2019:IFA**


**Ambrose:2012:RII**


**Alghamdi:2019:RAM**


**Asharov:2016:LPI**

Gilad Asharov and Gil Segev. Limits on the
CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

**Artemenko:2017:PGO**

CODEN ????. ISSN 1942-3454 (print), 1942-3462 (electronic).

**Andrade:2016:LEP**

CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

**Asharov:2014:TCC**


**Al-Sinani:2012:UCB**


**Ahmadi:2011:SK**


**Ahmadi:2012:SKE**

CODEN LNCSD9. ISSN


Asaar:2015:IBM


Alharbi:2018:CME


Alsulaiman:2013:IVB


Altman:2010:AAP


Azimpourkivi:2017:CBT

[ATC17] Mozghan Azimpourkivi, Umut Topkara, and Bog-


REFERENCES


Aslan:2016:DEM


Abdalla:2012:LRS


Abdou:2018:SLV

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


Badawi:2018:ASS


Altafa:2015:LPM


Altafa:2017:LHL

Muhammad Shoail Bin Altaf and David A. Wood.
REFERENCES


Awad:2017:OLO


Anzala-Yamajako:2012:RAC


Anzala-Yamajako:2012:RBC


Ahmad:2014:RTN


AlTawy:2014:IDR


Aysu:2015:FRT

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

**Au:2014:SMV**

**Ayub:2012:BRB**

**Apavatjrut:2012:EEA**

**Alshammari:2011:CET**

**Alavi:2014:RQE**

**Barcellos:2018:RSP**
REFERENCES


Barbay:2012:BRB


Barthe:2015:HAC


Barker:2016:RKM


Bartkewitz:2016:LPL


Bard:2019:DWG


Batey:2010:DMW


Bax:2014:PPD

Stephen Bax. A proposed partial decoding of the Voynich script. Web report, Centre for Research in English Language Learning and Assessment (CRELLA), University of Bedfordshire, Luton, Bed-
REFERENCES


Baylis:2010:CC

Bulygin:2010:OSS

Bennett:2014:QCP

Barenghi:2016:FBS

Boumerzoug:2016:LKM

Benyamina:2019:ANE
Zakarya Benyamina, Khefifa Benahmed, and Fateh Bounaama. ANEL: a novel efficient and lightweight


REFERENCES


Beurdouche:2017:MSU


Barenghi:2016:PPE


Beimel:2014:MLS


Bernstein:2017:SRD


Boldi:2012:IUG


Bingol:2019:EPP

Muhammed Ali Bingöl, Osman Bicher, Mehmet Sabir.

Bollman:2015:PWI


Behrad:2020:NSA


Bernstein:2011:PCI


Basin:2014:KYE


Bao:2016:LPP

Haiyong Bao and Le Chen. A lightweight privacy-preserving scheme with data integrity for smart grid communications. Concurrency and Computa-
REFERENCES


[BCC+19]

[BC18]


[BCE+10]

Badrignans:2010:SSA


[Bocu:2018:HEB]


[BiChel:2012:DMA]


[Boche:2017:CQA]


[Badrig]
REFERENCES

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

Balfanz:2012:FA


Bugliesi:2015:ART


Bana:2019:VMC


Buhrman:2014:PBQ


Bahri:2016:CCO

REFERENCES

DEN ????. ISSN 1559-1131 (print), 1559-114X (electronic).


[Baelde:2012:TPR]
REFERENCES


[BCGN16] Lejla Batina, Sherman S. M. Chow, Gerhard Hanke, and Zhe Liu. Introduction to the special

**Bitansky:2013:SNI**


**Brandenburger:2017:DTC**


**Bitansky:2017:VGB**


**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 Universiteit Eindhoven, Chicago, IL 60607-7045, USA and P.O. Box 513, 5600 MB Eindhoven, The Netherlands, July 6, 2014. 19 pp. URL http://cr.yp.to/ecdh/cu...
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-28641-4_8/


REFERENCES


[Basso:2011:BW]


[Biddle:2012:GPL]


[Barker:2015:RKM]


[Bessani:2013:DDS]


[Blasco:2016:SWB]


[Blasco:2016:SWB]
REFERENCES


[BK11] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou R3579X?: anonymized social networks, hidden...


**Bosseut:2016:EPA**


**Bendlin:2011:SHE**


**Bertoni:2011:CSF**


**Bertoni:2012:KIO**


**Boldyreva:2012:SSE**

Bertoni:2012:KSF

Bitansky:2013:WFS

Bottarelli:2018:PCW

Beebe:2017:MFC

Bellovin:2015:WRC

Bellovin:2016:EEE
REFERENCES


Bellovin:2018:UAE


Beltran:2018:IAA


Bajard:2016:MFA


Bera:2014:QC


Berghel:2016:CKF


Berghel:2016:DJT

Hal Berghel. Douglas Jones on today’s voting machines. Computer, 49
156 REFERENCES


Berghel:2016:S

Berghel:2017:ELR

Berretti:2018:IAS

Bouman:2011:SAW

Bas:2012:BLK

Bos:2019:ACI

Bhargavan:2012:VCI
Karthikeyan Bhargavan,

**Barthe:2014:PRV**


**Bobba:2010:ABM**


**Bhargavan:2016:MVP**


**Beimel:2012:SSS**


**Berger:2016:EGF**

REFERENCES


[BGG+19] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Em-


REFERENCES

Biswas:2017:STC


Borcea:2017:PEE


Bhattacharjee:2016:SWC


Blasco:2012:FAS

REFERENCES

www.sciencedirect.com/
science/article/pii/S1084804511001901.

behnia:2012:sei


Bernstein:2015:SPS


Benhamouda:2019:SPD


Bosch:2014:SPS


Berman:2013:HPR


Berman:2018:CFC

REFERENCES

ISSN 0004-5411 (print),
1557-735X (electronic).

Bonneau:2015:PEI

Biagioli:2012:CCS

Biggs:2008:CII

Beimel:2014:CCW

Biswa:2017:SA

Bauer:2010:RV
REFERENCES

Brumley:2010:CAI


Bogdanov:2012:UTC


Boche:2016:DSK


Bouraoui:2017:HAE


Benhamouda:2016:NFP


Brubaker:2014:UFA

<table>
<thead>
<tr>
<th>REFERENCES</th>
<th>Page 164</th>
</tr>
</thead>
</table>

**Boldyrev:2012:NPG**

**Bouti:2012:SCB**

**Babamir:2019:DDB**

**Bhuyan:2014:DDD**

**Braun:2012:ULA**
REFERENCES


[BKR11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full...


[BL12] Yu Bai and Yanlong Liu. A synchronization strengthen RFID authentication protocol based on key array. Lecture Notes in Computer Science, 7530:
REFERENCES


Benzaid:2016:FAW


Bai:2019:LMD


Buchmann:2017:PCU


Buchmann:2018:PCP


Buchmann:2017:PCS


Blomer:2012:TKG

REFERENCES

. Special Issue: Alan Turing.


REFERENCES


REFERENCES


Annie Gilda Roselin Arockia Baskaran, Priyadarsi Nanda Surya Nepal, and Sean He. Testbed evaluation of lightweight authentication protocol (LAUP) for 6LoWPAN wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 31...
REFERENCES


REFERENCES


Burns:2010:SCR


Bohli:2011:RAP


Budroni:2018:HGB


Bencsath:2012:CSD


Brooke:2010:DCX


Bellare:2014:SSEa


Bellare:2014:SSEb

Mihir Bellare, Kenneth Paterson, and Phillip Rogaway. Security of symmetric encryption against
mass surveillance. In ???? ,
editor, Advances in Cryptology – CRYPTO 2014,
pages 1–19. Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, UK / etc., 2014. ISBN ???
LCCN ???. URL ???

**Boneh:2016:BCR**

Dan Boneh, Kenny Paterson, and Nigel P. Smart.
Building a community of real-world cryptographers.
*IEEE Security & Privacy*, 14(6):7–9, November/December 2016. CO-
DEN ???. ISSN 1540-7993 (print), 1558-4046 (electronic). URL
https://www.computer.
org/csdl/mags/sp/2016/
06/msp2016060007.html.

**Balsa:2017:TIC**

Ero Balsa, Cristina P{é}rez-
Solà, and Claudia Diaz.
Towards inferring communication patterns in on-
line social networks. *ACM
Transactions on Internet
Technology (TOIT)*, 17(3):
32:1–32:??, July 2017. CO-
DEN ???. ISSN 1533-5399
(print), 1557-6051 (elec-
tronic).

**Brakerski:2014:VBB**

Zvika Brakerski and Guy N.
Rothblum. Virtual black-
box obfuscation for all cir-
cuits via generic graded en-
coding. *Lecture Notes in
Computer Science*, 8349:
1–25, 2014. CODEN
LNCS06. ISSN 0302-9743
(print), 1611-3349 (elec-
springer.com/chapter/10.1007/978-
3-642-54242-8_1/
http://link.springer.com/put
content/pdf/bfm:978-3-642-
54242-8_1.pdf.

**Brakerski:2013:WHB**

Zvika Brakerski. When ho-
omorphism becomes a li-
ability. *Lecture Notes in
Computer Science*, 7785:
143–161, 2013. CODEN
LNCS06. ISSN 0302-9743
(print), 1611-3349 (elec-
springer.com/chapter/10.1007/978-
3-642-36594-2_9/.

**Bradbury:2015:BSB**

D. Bradbury. In blocks [security Bitcoin].
*Engineering Technology*, 10(2):
68–71, March 2015. ISSN
1750-9637 (print), 1750-
9645 (electronic).

**Brewster:2018:RCF**

R. Brewster. Re-creating
the first flip-flop — a fun-
damental component of
computers turns 100 [re-
sources hands on]. *IEEE
Spectrum*, 55(6):13–14,
June 2018. CODEN
IEESAM. ISSN 0018-9235
(print), 1939-9340 (elec-
tronic).


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


S. Bag, S. Ruj, and K. Sakurai. Bitcoin block
REFERENCES


**Bellare:2012:MIS**


**Baja:2013:CSE**


**Birrell:2013:FIM**


**Bhattacherjee:2014:CAT**

Sanjay Bhattacherjee and Palash Sarkar. Concrete

**Bergsma:2012:PAW**


**Brumley:2012:SFI**


**Bachrach:2011:ISS**


**Bellare:2012:MIS**


**Baja:2013:CSE**


**Birrell:2013:FIM**


**Bhattacherjee:2014:CAT**

Sanjay Bhattacherjee and Palash Sarkar. Concrete

**Bagheri:2015:NNA**


**Bronzino:2019:ISV**


**Bendiab:2019:FNF**


**Ben-Sasson:2017:SZK**

REFERENCES


[BV13] Ioannis Broustis, Ganapathy S. Sundaram, and Harish Viswanathan. Group

**Boneh:2012:FEN**


**Biskup:2012:RBR**


**Braeken:2018:AAA**


**Bosch:2012:SDR**


**Bouabana-Tebib:2015:PSE**


**Blasco:2015:HDT**

[BTPLST15] Jorge Blasco, Juan E. Tapiador, Pedro Peris-
Lopez, and Guillermo Suarez-Tangil. Hinder-
ing data theft with en-
crypted data trees. The Journal of Systems and Software, 101(??):147–158, March 2015. CODEN JS-
SODM. ISSN 0164-1212 [Bud16] (print), 1873-1228 (elec-
science/article/pii/S0164121214002775.

Brocardo:2015:AVM [BTW15] Marcelo Luiz Brocardo, Issa Traore, and Isaac Woungang. Authorship verification of e-mail and tweet messages applied for continuous authentica-
SSBM. ISSN 0022-0000 (print), 1090-2724 (elec-
science/article/pii/S0022000014001834.

Buchmann:2010:EKG [Buc10] Johannes Buchmann. Einführung in die Kryptographie. (Ger-
man) [Introduction to Cryptography]. Springer-
Lehrbuch. Springer-Verlag, [Bull10b] Berlin, Germany / Hei-
delberg, Germany / Lon-
springer.com/mathematics/

Bulygin:2010:AOP [Bul10a] Stanislav Bulygin. Abstract only: Polynomial system solving for decoding linear codes and algebraic cryptanalysis param-
metric polynomial system discussion: canonical com-
prehensive. ACM Communications in Computer Algebra, 44(2):72, June 2010. CODEN ???? ISSN 1932-2232 (print), 1932-
2240 (electronic).

Bulygin:2010:CAC [Bul10b] Stanislav Bulygin. Computer algebra in coding theory and cryptanal-
ysis. Südwestdeutscher Ver-
lag für Hochschulschriften, Saarbrücken, Germany, 2010. ISBN 3-8381-0948-1. ???? pp. LCCN ????

breakers and the secret in-
telligence war against the Soviet Union. Alfred A. Knopf, New York, NY, USA, 2016. ISBN 0-385-
35266-2; 0-385-35267-0. xxi + 389 + 16 pp. LCCN UB256.U6 B83 2016.
**REFERENCES**


REFERENCES


REFERENCES


[Car10] Staff:2014:KYS

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

[CAC14] Caldwell:2013:INP


[Carr10] Carlson:2011:JRW


J. Courtois, L. Abbas-Turki, and J. Bajard.

Chang:2019:KCS


Cho:2016:MAT


Cheneau:2010:SIP


Cobb:2013:LMS


Chang:2018:DMU

Doohwang Chang, Ganapati Bhat, Umit Ogras, Bertan Bakkaloglu, and Sule Ozev. Detection mechanisms for unauthorized wireless transmissions. *ACM Transactions on Design Automation of Electronic Sys-

Chattopadhyay:2019:QIL


Chacin:2010:EKS


Chang:2014:RRT


Chen:2019:IAS


Chadha:2016:AVE


Chretien:2015:SPP


Chretien:2019:TMF

Rémy Chrétien, Véronique Cortier, Antoine Dallon,
REFERENCES


Chretien:2020:TMF


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO


Checkoway:2016:SAJ

REFERENCES


[Cascudo:2015:SSN] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, Carles Padró, and Chaoping Xing. On secret sharing with nonlinear prod-

Chatterjee:2017:PBS


Chikouche:2019:PPC


Cho:2014:DGA


Chen:2011:EAA


Chu:2014:KA


Chen:2010:ALD

Songqing Chen, Shiping Chen, Xinyuan Wang, Zhao Zhang, and Sushil Jajodia. An application-level data transparent authentication scheme without communication over-

**Chen:2013:WSB**


**Chiasson:2012:MWB**


**Canard:2016:HPP**


**Cui:2016:RDA**


**Criswell:2014:VGP**


**Cheng:2013:DVB**

Yueqiang Cheng, Xuhua Ding, and Robert H. Deng. DriverGuard: Virtualization-based fine-grained protection on I/O flows. *ACM Transactions*
REFERENCES


Ciriani:2010:TPA


[CDGC12] Zhen Cao, Hui Deng, Zhi Guan, and Zhong Chen.

Cao:2016:CCT


Chari:2010:DSC


[GLIC10]
REFERENCES

193


Cui:2018:ABC

Cui:2019:ABS

Coras:2016:AML

Costello:2014:CAS

Cremers:2019:SAG

Culhane:2019:KKR

Ceruzzi:2014:HFT
P. E. Ceruzzi. Are historians failing to tell the real story about the history of computing? *IEEE Annals of the History of Com-*


REFERENCES

Checkoway:2014:PED


Cevallos:2012:USR


Carstensen:2011:AAA


Calzavara:2017:SWJ


Celesti:2016:ALT


Choo:2017:EDF

Kim-Kwang Raymond Choo, Yunsu Fei, Yang Xiang,

**Chang:2010:PRN**


**Chen:2010:IFA**


**Camenisch:2012:EAA**


**Che:2012:WAM**


**Cheraghchi:2014:NMC**


**Corrigan-Gibbs:2014:KS**

REFERENCES

November/December 2014.

**Chaudhuri:2010:PIC**


**Caballero-Gil:2012:LAR**


**Chmiel:2012:EPC**


**Coul1:2011:ACO**


**Cohney:2017:PSR**

REFERENCES


Cheng:2012:PAI


Chandran:2014:PBC


Cheng:2013:NIB


Chen:2010:NUP


Chang:2011:DEQ


Chan:2013:OCK

REFERENCES

Chang:2013:MPQ


Chappell:2013:PMI


Chen:2011:CCI


Cheswick:2013:RP


Chen:2015:SSS


Chen:2017:CSQ

REFERENCES

Chen:2018:ESA


Cui:2019:CPA


Chen:2012:SRF


Chien:2012:IAM


Chien:2013:CR


Chirgwin:2013:ABB

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


REFERENCES


Cheon:2016:ANP


Cho:2012:CBF


Chang:2019:GTS


Cui:2013:OSL

T. Cui, C. Jin, and G. Zhang. Observations of

Chandra:2011:AST


Chailloux:2017:PLQ


Chung:2018:ERN


Chang:2019:PPN


Chase:2013:SMN

REFERENCES

Chuang:2011:LMA


Colin:2016:CTC


Claxson:2018:SVE


Calegari:2019:WPH


Chen:2019:BBS


Comon-Lundh:2010:DSP

Chang:2011:RSB

Chen:2017:PGF

Chong:2013:ASG

Chen:2016:RPR

Chen:2012:NCB

Chen:2013:TSE
Chande:2016:NSC

Cao:2012:SRH

Chen:2019:IBS

Canetti:2013:PCC

Castro:2013:RAM

Chang:2012:PRS
Cui:2016:KAS


Chen:2014:CDP


Cao:2018:CUP


Cheng:2017:ISK


Cremers:2011:OSV


Cozzens:2013:MEE

Margaret B. Cozzens and Steven J. Miller. The mathematics of encryption: an elementary introduction, volume 29 of Math-
REFERENCES


Debrup Chakraborty, Cuauhtemoc Mancillas-Lopez, Francisco Rodriguez-Henriquez, and Palash Sarkar. Efficient hardware implementations of BRW polynomials and tweakable enci-

**Chakraborty:2015:SSC**


**Chen:2017:VME**


**Cao:2016:OMA**


**Chatterjee:2017:IPB**


**Chen:2012:FAA**


**Chaudhry:2018:IRB**

Shehzad Ashraf Chaudhry, Husnain Naqvi, Moham-

CNRS:2014:NAS


Coron:2012:PKC


Chin:2011:ACS


Conitzer:2010:AP


Constantin:2012:RSN


Constantin:2017:SHF

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


Cordova:2014:EBS


Corthesy:2014:SSD


Courtland:2012:VCG


Coutinho:2012:RPT


Claessen:2013:SPN


Canard:2018:NTC

REFERENCES

Chung:2016:NBB


Chen:2018:RLF


Chevalier:2010:CSC


Chen:2012:DCC


Crampton:2011:PEC


Cramer:2012:TCT

REFERENCES


REFERENCES


Chadwick:2014:AFI


Chen:2013:RWM


Chen:2017:SIE


Ciegis:2016:ADP


Chong:2015:SID


Chow:2012:EPV

Yang-Wai Chow, Willy Susilo, and Duncan S. Wong. Enhancing the perceived visual quality of a size invariant visual cryptography scheme. Lec-
Chen:2018:SIA


Chen:2011:IBT


Chen:2011:ARI


Chen:2011:TVS


Canard:2018:CPK


Calzavara:2015:SLA


Chin:2013:SMB

Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng, and

**Chang:2012:GBP**


**Chou:2013:TIB**


**Crenne:2013:CMS**


**Calmon:2014:ITM**


**Choi:2012:LTFT**


Jiazhe Chen, Meiqin Wang, and Bart Preneel. Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT. *Lecture*


Chen:2012:CKS


Cao:2013:SIPa


Chen:2016:WPM


Chen:2019:WBS


Chen:2012:FSD


Chen:2012:AIB


Chen:2012:IBE


Chen:2014:CSI


Dharwadkar:2010:SSG


Djebbar:2012:ASB

Fatiha Djebbar and Begoñad Ayad. Audio steganalysis based on lossless data-compression techniques. Lecture Notes in Computer Science, 7618:1–9, 2012. CODEN LNCS69. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
Darivandpour:2018:ESP


Danezis:2012:FCDb


Demirhan:2016:CRP


Davies:2011:IST


Diong:2012:DAU


Djath:2019:HAR

Libey Djath, Karim Bigou, and Arnaud Tisserand. Hierarchical approach in RNS base extension for asymmetric cryptography. In Takagi et al. [TBL19],


Ding:2018:NPH


DePrisco:2013:CVC


DaRolt:2013:NDS


Dreier:2015:BFP


Datta:2017:SFH

Pratish Datta, Ratna

Castro:2016:FVB


Danezis:2012:FCDa


DeOliveiraNunes:2019:SSC


der.hans. Use SSH to cross a suspect host securely.
Desmedt:2010:CF


Desmedt:2010:ES


DuPont:2016:ECC


DeCapitaniDiVimercati:2010:EPR

DeCapitanidiVimercati:2017:AMM


Deng:2017:LLH


Ding:2012:CLS


Djuric:2015:FSF


Dutta:2017:EFC


Dickens:2018:SCI

REFERENCES

1523-2867 (print), 1558-1160 (electronic).

**Dupressoir:2014:GGP**


**Ding:2012:NRR**


**Drucker:2018:FMB**


**Dolev:2019:AAC**


**Demay:2019:PSS**


**Drimer:2010:DBP**

REFERENCES


REFERENCES


REFERENCES


Dolev:2012:ATC


Delfs:2015:ICP


Delimitrou:2016:SID


Dorre:2016:ELO


Doychev:2017:RAS


Durumeric:2014:MH

[DKA+14] Zakir Durumeric, James

Dolev:2016:MCG

Dobrev:2015:CTS

Dobyrev:2015:CTS

Doder:2012:MAR
[DKPW12]

Dodon:2012:MCE
REFERENCES


**Dong:2012:UAS**


**DeLuca:2015:SUS**


**Dinur:2017:IGA**


**Deng:2019:DMS**


**Degefa:2016:PSE**


**Djaziri-Larbi:2018:WDA**

REFERENCES

Dong:2013:PRS

DiPietro:2016:CLD

Dodis:2011:SSC

Dai:2016:MLR

Duan:2016:SDC

DeCarneDeCarnavalet:2015:LSE
REFERENCES


[DMSD18] Ashutosh Dhar Dwivedi, Pawel Morawiecki, Rajani Singh, and Shalini Dhar. Differential-linear...


Christian A. Duncan and Vir V. Phoha. On the complexity of aggregating information for authentica-


REFERENCES


[Dra16]

[Dong:2011:SSE]

[Dasgupta:2016:TDA]

[Dixon:2016:NTO]

[delRey:2012:EDI]

[Dini:2011:LLA]
Gianluca Dini and Ida M. Savino. LARK: a lightweight authenticated ReKeying scheme for clustered wireless sensor networks. ACM
REFERENCES


Dixit:2019:FBD


Das:2015:DCS


Das:2016:MPU


Das:2012:DPB


Deng:2018:SFE


Dachman-Soled:2014:COF

Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin. Can optimally-fair coin tossing be based on one-way functions?
REFERENCES


Dinis:2013:HHS

Drosatos:2017:PET

Deng:2012:VIA


Dinis:2013:HHS

Drosatos:2017:PET

Deng:2012:VIA
REFERENCES


REFERENCES


Dong:2012:NDI

Dai:2018:OPC

Deng:2014:CCC

Deng:2016:NCS

Dodis:2013:OYE

Dyakonov:2019:WWU
M. Dyakonov. When will useful quantum com-

---

**Dong:2015:SSS**


---

**Deng:2014:TNI**


---

**Dong:2016:EPP**


---

**Doss:2012:MDA**


---

**Delledonne:2018:CDA**

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


REFERENCES


Erbagci:2019:SHE


Ermis:2017:KAP


Egele:2013:ESC


Esiner:2017:QRI


Esiner:2019:TFA


Mohamed El-Hadedy, Amit Kulkarni, Dirk Stroobandt,
and Kevin Skadron. Reco-
Pi: a reconfigurable cryp-
toprocessor for $\pi$-cipher.
Journal of Parallel and
Distributed Computing,
133(??):420–431, November
2019. CODEN JPD-
CER. ISSN 0743-7315
(print), 1096-0848 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0743731517301636

**Eisenbarth:2010:CCE**

Thomas Eisenbarth. Crypt-
tography and cryptanal-
ysis for embedded sys-
tems, volume 11 of IT-
Security. Europäischer
Universitätsverlag, Berlin,
Germany, 2010. ISBN 3-
LCCN ???

**Esiner:2016:FFB**

Ertem Esiner, Adilet Kach-
keev, Samuel Braunfeld,
Alptekin Küpçü, and
Özmun Özkasap. FlexD-
PDP: Flexlist-based optim-
dized dynamic provable
data possession. ACM
Transactions on Storage,
12(4):23:1–23:??, August
2016. CODEN ??? ISSN
1553-3077 (print), 1553-
3093 (electronic).

**Emura:2019:PPA**

Keita Emura, Hayato
Kimura, Toshihiro Ohi-
gashi, and Tatsuya Suzuki.
Privacy-preserving aggre-
gation of time-series data
with public verifiabil-
ity from simple assump-
tions and its implementa-
tions. The Computer
Journal, 62(4):614–630,
April 2019. CODEN CM-
PAJ6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
academic.oup.com/comjnl/
article/62/4/614/5263983

**Engels:2013:NULL**

Susanne Engels, Elif Bilge
Kavun, Christof Paar,
Tolga Yalcin, and Hristina
Mihajloska. A non-linear/
linear instruction set exten-
sion for lightweight ciphers.
In IEEE [IEE13], pages 67–
ISSN 1063-6889. LCCN

**Elbirt:2009:UAC**

Adam J. Elbirt. Under-
standing and Applying
Cryptography and Data Se-
curity. CRC Press, 2000
N.W. Corporate Blvd.,
Boca Raton, FL 33431-
9868, USA, 2009. ISBN 1-
4200-6160-7. xxvii + 637
pp. LCCN QA76.9.A25
E43 2009. URL http:
//www.loc.gov/catdir/
toc/ecip0821/2008028154.
hml.

**El Bansarkhani:2012:ELB**

Rachid El Bansarkhani
and Mohammed Meziani.
An efficient lattice-based


Engels:2012:HLA


Ebadi:2015:DPN


Essex:2017:DDU


Everett:2012:EC


Everett:2016:SES


Eibach:2010:OGB

Eldib:2014:FVS


Eyal:2017:BTT


Enos:2015:IBS


Emmart:2018:FME


Farash:2014:ECC


Farash:2014:SEI

REFERENCES


Fahd:2018:CPA


Fahl:2019:MVE


Fagone:2017:WWS


Fairley:2019:EWC


Farash:2014:CIE


Fay:2016:ICM


REFERENCES


REFERENCES


**Farris:2017:IRN**


**Faz-Hernandez:2019:HPI**


**Faz-Hernandez:2018:FSI**


**Forne:2010:PAA**


**Fahl:2012:WEM**

Fan:2014:ASA


Fawzi:2013:LDN


Florencio:2016:PSD


Feng:2018:ABB


Fidler:2018:CCN


Farash:2015:PSE

REFERENCES


Fan:2014:RRS

Ferguson:2010:SHF

Forler:2012:DAC

Fei:2016:PPA

Fei:2016:SEF

Feng:2012:CAO
Hui Feng, Hefei Ling, Fuhao Zou, Weiqi Yan, and Zhengding Lu. A collusion attack optimization strategy for digital fingerprinting. *ACM Transactions on Multimedia Computing, Communications, and

Fallahpour:2015:AWB


Ferrag:2018:SCN


See retraction notice [?].

Ferretti:2019:FBS

REFERENCES

Faust:2014:CNM


Feng:2012:USD


Fraczek:2012:MSI


Fernandez-Mir:2012:SRA


Ferreira:2015:LPA


Fu:2018:LUA

Xingbing Fu, Xuyun Nie, Ting Wu, and Fagen Li. Large universe attribute based access control with efficient decryption in cloud storage system. *The Journal of Systems and
REFERENCES


Fokkink:2012:TCG


Folger:2016:TQH


Fox:2013:RLQ


Fotiou:2019:NBS


Faigl:2014:PEC


Faust:2012:PLR

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

Fu:2015:TVG


Feng:2018:ALA


Fiore:2015:EIB


Fathimal:2016:SSS


Frattolillo:2015:WPP


Frattolillo:2016:BFM

REFERENCES

ISSN 1559-1131 (print), 1559-114X (electronic).

Frey:2010:ABC

Fernandes:2017:ITS

Fridrich:2010:SDM

Frikken:2010:SMC

Fridrich:2012:MTS

Fritsch:2013:CPE

Fu:2016:EPS
Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, and Fengxiao Huang. Enabling personalized search over encrypted outsourced
REFERENCES


REFERENCES

Feng:2011:GDA


Feng:2011:GDA


Fujio:2011:SHI


Fujio:2011:SHI


Fujio:2012:SEP


Fujio:2012:SEP


Fujio:2012:SEP


Fadl:2010:DCA


Fadl:2010:DCA


Fadl:2010:DCA

Georg Fuchsbauer. Com-
REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_14.

Fulton:2010:BRB


Fanti:2018:DLC


Franken:2019:ECP


Fathi-Vajargah:2017:IMC


Fiore:2017:PGP

Feng:2013:ECE


Fanyang:2012:SAK


Fan:2015:IRD


Feng:2011:VBF


Feng:2019:SHO


Fan:2015:IRD

REFERENCES

[Fyodorov:2019:SGM]

[Fan:2013:KIS]

[Fan:2014:NCI]

[Fu:2012:EHA]

[GomezPardo:2013:ICM]


[Grondahl:2019:TAA]
Tommi Gröndahl and N. Asokan. Text analysis in

Guimaraes:2019:OIQ


Gop:2018:LPP


Galindo:2013:NIC


Gasarch:2013:RBC


Wen Gao, Liqun Chen, Yupu Hu, Christopher J. P. Newton, Baocang


REFERENCES

comjnl.oxfordjournals.org/content/59/11/1669.

Gao:2018:PRR

Guerin:2016:TDU

Giot:2011:UKD

Geller:2013:MIS

Gentry:2010:CAF

Gentry:2013:EMH
Gaspar:2012:SEF


Gong:2010:PCI


Grigg:2011:CCN


Garg:2016:CIO


Garg:2016:HSS


Garg:2014:TRS

Sanjam Garg, Craig Gentry, Shai Halevi, and Mariana Raykova. Two-round

[Garg:2017:IDI]


REFERENCES

Gope:2015:RLA


Gope:2016:EMA


Genge:2019:ESA


Gordon:2011:CFS


Gentry:2012:RSB


Gentry:2013:FSB

References


Henri Gilbert, editor. *Advances in cryptology — Eurocrypt 2010: 29th annual international conference on the theory and ap-


Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. On weak odd domination and graph-
REFERENCES


**Goyal:2013:CZK**


**Gu:2017:IBM**


**Geetha:2011:VRN**


**Gunleifsen:2019:PCD**


**Garay:2016:MPA**


**Grigoriev:2017:YMP**

Dima Grigoriev, Laszlo B. Kish, and Vladimir Shpil- rain. Yao’s millionaires’ problem and public-key en-

**Gaj:2017:DCR**


**Guo:2010:HMW**


**Gu:2019:GRM**


**Glassey:2011:MIM**


**Guo:2018:KAA**


Guo:2011:EDA


Gong:2016:HES


Gupta:2019:OIT


Gerault:2018:RAR


Gradwohl:2010:SRC

REFERENCES

Gradwohl:2013:SRC

Guo:2012:ETD

Guo:2013:TVS


Goglin:2013:KGS

Gotzfried:2014:MAT
Johannes Götzfried and Tilo Müller. Mutual

Gofman:2016:MBE


Gueron:2016:HIA


Gonzalez-Manzano:2019:LUR


Gunson:2011:UPS

REFERENCES

www.sciencedirect.com/
science/article/pii/S0167404810001148

Giambruno:2015:GGB


Garcia-Martinez:2015:HEB


Garcia-Morchon:2015:HCR


Guo:2011:ISS


Guo:2014:SAS


Gao:2014:URA

[Ljou14] Lijun Gao, Maode Ma, Yantai Shu, and Yuhua Wei. An ultralightweight RFID authentication protocol with CRC and permutation. Journal of Net-


REFERENCES


Goodin:2012:CBS


Gope:2019:LLA


Garcia:2012:ERP


Gorski:2010:CDS


Groth:2012:NTN


Glowacz:2017:IDW


Gong:2013:NOT

[GPLZ13] Longyan Gong, Jingxin Pan, Beibei Liu, and

Goodrich:2012:EVW


Gottel:2019:SPE


Grossschadl:2012:EJI


Genkin:2016:PKE


Genkin:2014:GYH

Daniel Genkin, Itamar Pipman, and Eran Tromer. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs. Report, Technion and Tel Aviv University, Tel Aviv, Israel, July 31, 2014.
REFERENCES


Gonzalez-Pardo:2012:CID


Gai:2017:SCI


Ghatak:2019:IBS


Ghosal:2019:NPP


Greengard:2011:MRM


Green:2017:SSE

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

**Green:2019:RMC**


**Green:2019:RNT**


**Gibson-Robinson:2012:AAL**


**Guo:2018:WBS**


**Gonzalez-Serrano:2018:SML**

References


[Gorbunov:2015:ABE]


[Gebotys:2016:PCP]

[Gao:2019:EUE]


[Gao:2015:GCC]
Wei Gao, Guilin Wang, Xueli Wang, and Kefei

**Goh:2013:TOT**


**Guo:2019:EER**


**Gao:2012:RHC**

REFERENCES


[Haigh:2017:HR] Thomas Haigh. Historical reflections: Colossal genius: Tutte, Flowers, and a bad imitation of Turing. Communications of the As-


Lein Harn. Group authentication. *IEEE Trans-
Harrington:2014:GEF

Harrington:2014:GEF

Hardesty:2015:BAC

Hardesty:2016:SUC

Hastings:2016:SWS

Hayes:2013:NSA

Houmansadr:2013:BCN

Hurlburt:2014:BBC

Hetzelt:2017:SAE
Felicitas Hetzelt and Robert Buhren. Security analysis of encrypted virtual machines. *ACM SIG-
REFERENCES


**Hernandez-Becerril:2016:GIS**


**Han:2019:ABI**


**He:2013:HEH**


**Hulsing:2017:XEH**


**Hao:2012:SAM**


**Hu:2017:ATE**

Jingwei Hu and Ray C. C. Cheung. Area-time efficient computation of Niederreiter en-


Hsu:2011:WLC

Hernandez-Castro:2012:AFH

Huang:2018:BLD

Hosny:2019:RCI

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

Heninger:2012:MYP
Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection

Heath:2015:HNS


Hwang:2012:ABA


Hamad:2018:DWU


Hellman:2017:TLC


Hanka:2011:DPK

Oliver Hanka, Michael Eichhorn, Martin Pfannenstein, Jörg Eberspächer, and Eckehard Steinbach. A distributed public key infrastructure based on threshold cryptography for the HiiMap next genera-
REFERENCES

Hermelin:2010:MLC

Herranz:2014:ABS

Herardian:2019:SUC

Hess:2012:GJC

Hess:2012:GJC

Heys:2017:SCF

Harn:2014:MTS

Hoang:2014:IMD
Anh-Tuan Hoang and Takeshi Fujino. Intramasking dual-rail memory on LUT implementation for SCA-resistant AES on FPGA. ACM Transactions on Reconfigurable Technology and Systems, 7(2):
REFERENCES

Hocking:2013:COU


Hin:2019:CUR


Huang:2016:EDP


Hanocka:2019:APS


Heyse:2012:TOC

Hibschman:2019:ISS

Hua:2015:TSE

Han:2011:PEB

Harn:2015:DTS

Hu:2016:EWS

Huber:2019:FCL
Manuel Huber, Julian Horsch, Junaid Ali, and Sascha Wessel. Freeze and crypt: Linux kernel support for main memory encryption. *Computers &
Hammi:2018:BTD
Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrrouchni.


Hayashi:2013:AEI

Huber:2014:TPW

Haitner:2011:PRI

Hong:2015:RSM
Wien Hong, Gwoboa Horng, Chih-Wei Shiu, Tung-Shou Chen, and Yu-Chi Chen. Reversible steganographic method using complexity
REFERENCES


[HJM+11] Markus Hinkelmann, Andreas Jakoby, Nina Möbius, Tiark Rompf, and

**Hasan:2014:TFL**


**Hur:2014:SDR**


**Hasan:2017:UAF**


**Hussain:2018:PPP**


**Hiemenz:2019:DSS**


**Hameed:2018:TFV**


**Handa:2019:SES**


**Houmansadr:2014:NBW**


**Hur:2013:REC**


**Hanzlik:2019:CPC**


**Heyse:2012:LEA**

Heil:2014:APH


Howe:2018:PDG


Holenstein:2011:ERO


Harn:2010:AGK


Hazay:2010:EST


Hu:2018:SVA


Hu:2019:AAA


Huang:2011:ISL


Hwang:2019:ELS


Huang:2015:MSE


Harn:2011:FDM

[HLCL11] Lein Harn, Chia-Yin Lee, Changlu Lin, and Chin-

Han:2018:TSE


Herranz:2011:RBS


Ham:2018:IYP


Huang:2015:CEA

REFERENCES

ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

**Howard:2010:DSS**


**Hohenberger:2012:DDQ**


**Huang:2014:SWC**


**Hefeeda:2010:ASM**


**Herzberg:2012:TJA**


**Hwang:2019:BBR**

Hore:2012:SMR

Hajihassani:2019:FAI

Hoang:2012:ESB

Hirt:2014:BA

Hajihassani:2019:FAI

Hodgson:2019:SSC

Hoffmann:2015:LBQb
Leah Hoffmann. Last byte: Q&A: A passion for pairings. Communications of the A-
REFERENCES


Hyla:2017:HLS


Haigh:2018:CP


Halder:2010:WTR


He:2012:ECT


Hadlington:2019:ERW


Hurrah:2019:DWF

REFERENCES

Howe:2015:PLB

Hoffstein:2008:IMC

Hur:2010:CCS

Han:2016:GGA

Han:2018:BEI
Han:2014:GTK


He:2013:GME


Hisil:2019:KLF


Hulsing:2013:OPX


Huang:2014:AFS


Hussain:2018:SSH

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

**Hassan:2019:DPR**


**Herranz:2013:SMS**


**Hulsing:2016:MMT**


**Haitner:2010:EIC**


**Hwang:2011:CDA**

REFERENCES


Huang:2015:PAP


Huang:2017:SSS


Hald:2015:RRA


Hulsing:2013:WOS


Herbert:2012:SMP


Hurlburt:2016:MBO

REFERENCES

Hammerle-Uhl:2011:RWI


Harvey:2017:FPM


Hunger:2018:DDC


Han:2012:MIA


Hammad:2019:PSF


Hwang:2011:NIB

REFERENCES


[He:2016:STI] Haibo Hong, Licheng Wang, Jun Shao, Jianhua Yan, Haseeb Ahmad, Guiyi Wei, Mande Xie, and Yixian Yang. A miniature


REFERENCES

Huang:2018:PIB

Huang:2018:CT

Hu:2019:CA

Hao:2011:NTV

Huang:2011:IBS

Han:2012:ERI


Han:2014:ERI


Han:2018:ERA


Huang:2019:ILA


Huang:2005:EMP

Liusheng Huang, Hong Zhong, Hong Shen, and Yonglong Luo. An efficient multiple-precision division algorithm. In Hong Shen and Koji Nakano,
editors, Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005. PD-CAT 2005: 5–8 December 2005, Dalian, China, pages 971–974. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7695-2405-2. LCCN QA76.58 J1752 2005. The authors present an integer-division algorithm that runs three to five times faster than Knuth’s 1981 original. However, there is an error in the renormalization algorithm that is corrected in [MN14], while retaining the speedup.

Han:2014:ATS


Hammad:2019:NTD


He:2017:AHA


He:2018:LAB

Qian He, Ning Zhang, Yongzhuang Wei, and Yan Zhang. Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems. Computer Networks (Amsterdam, Netherlands:
He:2015:IEI


Hunt:2018:RDS


Islam:2015:MBA


Ibrahim:2019:RAM


Ismail:2010:EAE

Iszam:2011:MES

IBM:2013:DMP

IEEE:2011:ICI
IEEE:2011:PIA


IEEE:2013:PIS


IEEE:2015:ISS


Imanimehr:2016:HPR


Islam:2011:MD


Iyengar:2016:SPS

Anirudh Iyengar, Swaroop Ghosh, Kenneth Ramclam,

[IMai:2015:IRR]

[IL15]

[Ioannou:2014:PKC]

[IMB17]
In tel:2019:IAM


Isobe:2012:SAL


Isobe:2012:SCL


Irshad:2016:EAM

Ishai:2014:PCP


Jacobs:2016:STB


Jie:2010:AAI


Jie:2011:RGA


Prins:2011:DCA


Jain:2013:MSD


Jho:2016:SSE

REFERENCES

November 2016. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Jia:2018:ERH


Jakobsson:2012:AWD


Chang:2012:TRR


Joldzic:2016:TSA


Jogenfors:2015:HBT


Jeong:2013:CBC


Jaeger:2018:FAP


Jo:2014:ODE


Jing:2012:MVB

Huiyun Jing, Xin He, Qi Han, and Xiamu Niu. Motion vector based information hiding algorithm for H.264/AVC against motion vector steganalysis. [Jia14a]

Jiang:2012:SSL

Jiang:2019:SSL


**Jiang:2016:MAC**


**Jiang:2017:BMA**


**Jin:2010:ADW**


**Jin:2010:QP**


**Jawad:2013:GAD**


**Jannati:2019:SOR**

Hoda Jannati and Ramtin Khosravi. On the security of one-round meeting location determination protocol. *Information Processing Letters*, 146(??):35–38,


Simon Josefsson and Ilari Liusvaara. Edwards-curve


Ji:2018:DIR


Jiang:2016:OOC


Jiang:2016:UTC


Jain:2012:BAS


Jan:2017:PPB

REFERENCES

[Johnson:2010:BRF]

[Johnson:2015:NGA]

[Joux:2013:NIC]

[Jin:2019:RPP]

[Jeans:2013:CCP]

[Juels:2014:HEE]
Jain:2018:MDN


Jaiyela:2018:IPN


Jalili:2017:EAS


Jevdjic:2017:ASC


Jailili:2016:APQ


Jalili:2017:EAS


Jaiyela:2018:IPN


Jain:2016:APQ


Tong:2012:NBD


Jiang:2016:SLD


Juels:2014:INC


Jiang:2017:SLD


Jiao:2019:AMC

REFERENCES

September 2019. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).


[184x646] Jiang:2010:EDI


[JY14]


[KA17]

REFERENCES

www.sciencedirect.com/science/article/pii/S0020019016301338

Kurkcu:2018:CBE


Kornycy:2017:RFT


Koziel:2018:HPS


Kamp:2013:MES


Kamp:2016:MEM


Kapera:2011:SPD


Kapera:2013:MRM

REFERENCES

Karafyllidis:2012:QGC


Kong:2015:CSM


Katz:2013:RIB


Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP

Jan Willem Kleinrouweler, Sergio Cabrero, and Pablo Cesar. An SDN ar-

**Kim:2011:SSE**


**Khan:2018:APS**


**Koz:2012:ASE**


**Kraetzer:2012:PCS**


**Kiefer:2018:IBC**


**Kumar:2019:SSH**

[KD19] Chanchal Kumar and Mo-

Karakoc:2013:BCL


Karakoc:2015:AKA


Kumari:2017:DSU


Kara:2019:ALS


Keblusek:2015:BRK

Kemshall:2011:WMT


Kabirirad:2019:HSG


Kleinjung:2010:FBR


Kikuchi:2012:SSN


Kostic:2019:UNV


Kramer:2010:FDC

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


Kim:2012:SLT

K:2019:IAM

Khedr:2016:SSH

Kwon:2010:SEB

Koo:2018:PPD

Khazaei:2010:NBS
Shahram Khazaei. Neutrality-Based Symmetric Cryptanalysis. Thèse, École


Intae Kim, Seong Oun Hwang, Jong Hwan Park, and Chanil Park. An efficient predicate encryption with constant pairing computations and min-


*Kim:2015:CEH* Y. Kim. Comments on “An Efficient Homomorphic MAC with Small Key

Kim:2016:MAS


Khan:2016:BSW


Konstantinou:2010:RCI


Kawai:2012:SHS


Kawai:2013:SHS


Khalil:2014:CIM

Issa Khalil, Abdallah


Yonggon Kim, Ohmin Kwon, Jinsoo Jang, Seongwook Jin, Hyeongboo Baek, Brent Byunghoon Kang, and Hyunsoo Yoon. On-demand bootstrapping mechanism for isolated

Kubota:2016:SAV


Kim:2018:ARD


Koblitz:2011:ECC


Khan:2013:EDC


**Khan:2014:IPR**


**Kushwah:2011:EIB**


**Khakpour:2013:ITA**


**Katz:2008:IMC**


**Katz:2015:IMC**

Klapper:2010:PSS


Ko:2010:MME


Koebeler:2012:EPD


Kent:2015:AGA


Kumari:2016:UFD

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


[KM10c] Neal Koblitz and Alfred Menezes. The brave new world of bodacious assumptions in cryptography. *Notices of the American Mathematical Soci-


Kline:2018:CAR


Kiyoshima:2014:CRB


Kanter:2011:LLB


Kavun:2018:SAE

REFERENCES

January 2018. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).


Kumari:2016:APW


Koblitz:2010:BRB


Komargodski:2018:LRO


Kawachi:2017:GCR


Kasper:2012:SCA


Khamsemanan:2016:BBU

REFERENCES


REFERENCES


Kiltz:2011:EAH

Khalid:2016:RHL

Kocabaş:2012:CPB

Kang:2016:DSA

Keskinarkaus:2010:IWD

Krenn:2013:CCR
[KPW13] Stephan Krenn, Krzysztof Pietrzak, and Akshay Wa-
REFERENCES


**Knudsen:2011:BCC**


**Krantz:2012:EAM**


**Kostinger:2012:SBL**


**Kannan:2013:NQF**


**Krenn:2013:AWI**

REFERENCES


[KS18b] I Karthiga and Sharmila Sankar. Providing secret authentication in clus-

Korac:2019:FMU


Kocabas:2016:ESM


Khan:2017:TPK


Kiljan:2017:SAC


Kwon:2018:CEI

See [KSH18b].

Kwon:2018:EIP


Ksiezopolski:2012:QMQ


Kim:2012:SAH


Khamis:2018:CCT

Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zeeschwitz, Jens Le, Andreas Bulling, and Florian Alt. CueAuth: Comparing touch, mid-air gestures, and gaze for cue-based authentication on

Kalita:2019:NSM


Kawachi:2012:SKE


Kobayashi:2016:ASC


Klisowski:2012:CCP


Kai:2014:FSD

Kumagai:2010:UGS

Kupcu:2013:DTT

Kupcu:2015:OAS

Kushner:2013:RSS

Kuznetsov:2011:APP

Kshetri:2018:BEV

Kim:2019:IED


REFERENCES


REFERENCES


REFERENCES


**Lavington:2012:A**


**Li:2015:NAC**


**Lee:2017:SUE**


**Li:2015:CEH**


**Li:2015:GAU**


REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Li:2014:PSC</td>
<td>Jiguo Li, Haiting Du, Yichen Zhang, Tao Li, and...</td>
<td></td>
</tr>
</tbody>
</table>

URLs:

- http://comjnl.oxfordjournals.org/content/58/4/709

ISSN numbers:

- 1084-8045 (print)
- 1925-7074 (electronic)
- 1206-212X (print)
- 1872-6208 (electronic)
- 0362-1340 (print)
- 1558-1160 (electronic)


REFERENCES


and Computation: Practice and Experience, 29 (17), September 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


Junghee Lee, Kalidas Ganesh, Hyuk-Jun Lee,

Liu:2012:LFA


Labati:2016:BRA


Lee:2019:TES


Lopez-Garcia:2014:PBB


Li:2014:SCA


Liu:2012:FVC

Feng Liu, Teng Guo,


Lin:2011:NIB

Lertvorratham:2012:ISM

Liao:2013:NMS

Li:2014:ARM

Lenstra:2012:RWW

Lum:2016:QEM
REFERENCES


Li:2012:BVS

Lih:2011:ICA

Lin:2018:BBB

Li:2010:AIS

Lin:2014:SOA

Liu:2015:SSP
Jianghua Liu, Xinyi Huang,


REFERENCES


[Li:2010:PAP]

[Li2017:AMA]

[Li:2014:IVW]

REFERENCES


REFERENCES


Li:2017:MMA


Li:2018:MMA


Liu:2019:ICA


Li:2016:IRI


Li:2019:IID


Li:2017:SQS


REFERENCES


Liu:2010:SVE [LK10]

Li:2012:BIB [LK12]

Lee:2014:SPB [LK14]

Lee:2018:NIC [LK18]

Li:2012:IBO [LKAT12]

Lee:2019:VCS [LKBK19]
Kyuin Lee, Neil Klingsmith, Suman Banerjee, and Younghyun Kim. VoltKey: Continuous secret key generation based on power line noise for zero-involvement pairing and authentication. Pro-


Jingqiang Lin, Bo Luo, Le Guan, and Jiwu Jing. Secure computing using registers and caches.

**Li:2017:ESD**


**Lyu:2018:PKE**


**Li:2017:CIS**

Chengqing Li, Dongdong Lin, and Jinhui Lu. Cryptanalyzing an image-scrambling.

**Liu:2018:GEI**


**Liu:2019:SBC**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Liu:2018:GEI**


**Li:2017:CCD**


**Li:2018:CIE**


**Liu:2018:VSE**


**Liu:2018:VSE**

REFERENCES


REFERENCES


REFERENCES


Le:2016:ADS


Lai:2018:IBB


Lai:2017:FPP


Liu:2014:SCS


Li:2011:NRA


Lv:2013:NTP

REFERENCES

[Lubacz:2010:VI]

[Lukasiewycz:2016:SAO]

[LoIacono:2019:NGR]

[Li:2018:RBB]

[Li:2018:TF]


Loeb:2015:MGM

Lopriore:2012:EPP

Lopriore:2015:PCR

Lopriore:2015:PMD

Low:2012:BRB

Lin:2011:CRN

[LP12] Ling:2012:SHS


Liu:2016:PPO


Libert:2010:KES


Lubicz:2015:GMA


Lukowiak:2014:CEB


Liskiewicz:2013:GBS


Liskiewicz:2017:SLS

not imply detectability. 


**Lane:2014:PBD**


**Luo:2012:FSU**


**Liu:2019:IMM**


REFERENCES

Lin:2018:CPF


Lin:2018:SSS


Lin:2019:CCA


Lin:2017:ESF


Lei:2013:RSW


Landecker:2012:TBB

REFERENCES

Liu:2016:EPP

Le:2014:IMX

Lee:2013:CCM

Lee:2014:NDH

Liu:2015:IMB


REFERENCES

Li:2016:LRC


Ludge:2012:NLD


Lucchese:2010:RPT


Lafitte:2011:CBF


Liu:2010:CIE


Lee:2011:ACA

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


Lui:2013:CBS

Liu:2016:PAB

Liu:2017:EEC

Liu:2011:SBA
Li:2018:SCM


Li:2019:PSA


Lu:2014:HOM


Lu:2010:NDC

Liu:2010:SET


Liu:2017:SRG


Liu:2011:PIA


Liu:2016:NSC


Lu:2012:MMA


Li:2010:GCP

Hui Li, Chuan-Kun Wu,


REFERENCES


REFERENCES


Le:2019:ADF


Liu:2015:SAA


Lin:2018:SEI


Li:2010:ESS


Liao:2012:NSM


Liao:2010:MPC


**Li:2019:APA**


**Liu:2019:IEU**


**Li:2019:EPM**

REFERENCES

Li:2016:BMA


Liu:2019:XBL


Liu:2019:RAS


Ma:2017:AEJ


Masdari:2017:STA


MacCormick:2012:NAC

John MacCormick. *Nine algorithms that changed the future: the ingenious ideas that drive today’s computers*. Princeton University Press, Princeton, NJ, USA,


REFERENCES


-Martin:2010:FWL-


-Martin:2010:PCC-


-Martin:2010:XMA-


-Mazumdar:2016:CIS-


-Mashhadi:2017:NMS-


-Matsuda:2014:IBP-


-Matthiessen:2019:RCM-


Maurer:2012:CCN


Ma:2015:BAM


Matias:2018:NNZ

Malone:2013:MOD


Migliore:2018:PPF


Massolino:2015:OSC


Mukhopadhyay:2011:PEA


Matula:2019:PCG

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

Madanayake:2012:BPS


McGrew:2017:IDH

REFERENCES


McGrayne:2011:TWH

McGraw:2016:SBTd

McKay:2011:SLB

McK10
Sinclair McKay. The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there. Gardners Books, 2011. ISBN 1-84513-633-0. ???? pp. LCCN ????.

Ma:2019:TOP
Mahmood:2018:ECC


Marquez-Corbella:2015:ECP


Mhenni:2019:DSA


Mathew:2015:NMB


Majzoub:2012:MRH


Mansouri:2012:ACA

REFERENCES


Mansfield-Devine:2015:MIC


Murdoch:2010:CPB


Mosenia:2017:PTS


Malina:2018:SET


Meiklejohn:2010:BRB

[Mei10] Sarah Meiklejohn. Book review: An Introduction to Mathematical Cryptography, by Jeffrey Hoffstein,
REFERENCES


Menezes:2013:IPB


Menn:2013:ESC


Meshram:2015:EIB


Mandal:2016:DIW


Moreno:2013:NIP


Moufek:2015:MCB

REFERENCES

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


[Meziani:2012:IPS] Mohammed Meziani, Ger-

**Miller:2014:ADS**


**Mo:2018:RUA**


**Munoz-Hernandez:2016:EES**


**Mou:2013:CBC**


**Mohd:2015:SLB**

Ma:2019:PFC


[MHW+19]

Mohd:2018:HDM


[MHY+18]

Micciancio:2010:FGC


[Mic10a]

Michiels:2010:OWB


[Michiels:2010:OWB]

Michael:2016:RNI


[Mic16]

Midgley:2010:SEE

Martinez-Julia:2012:NIB


Martinez-Julia:2013:BSI


Miao:2019:PPT


Memon:2018:TFS


Mohanty:2011:RTP


Moessner:2012:SAS

Muller:2012:HPC

Mozaari-Kermani:2017:FDA

Mozaari-Kermani:2018:ERE

McGrew:2016:SMH

Malik:2012:AIC
REFERENCES

Menesidou:2017:CKM

Marconato:2013:VLC

Mozaffari-Kermani:2010:CSI

Montecchi:2012:QSE

Mancillas-Lopez:2010:RHI

Mendez:2016:PES
Alejandro Pérez Méndez, Rafael Marín López, and Gabriel López Millán. Providing efficient SSO to


Mondal:2014:DSM


Maity:2017:ODC


Mazumdar:2017:CRS


Mulholland:2017:DCD


Martins:2019:HHR


Merlo:2015:MEP


Mailloux:2016:PSS

Logan O. Mailloux, Michael A. McEvilley, Stephen Khou, and John M. Pecarina.

Miao:2016:RAS

Maeng:2015:TAU

Moldovyan:2012:BBD

Mahmoody:2014:PPK

Marino:2019:ACN
Macedo:2017:SSP


Mazumder:2017:PSK


Mazumder:2017:SAE


Maity:2013:CRS


Matsuo:2012:MAK


Meshram:2012:IBC

Chandrashekhar Meshram, Suchitra A. Meshram, and Mingwu Zhang. An ID-based cryptographic mechanisms based on GDLP and IFP. *Information Processing Letters,*
REFERENCES

Morgan:2010:BCP

Mukhopadhyay:2014:EMP

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

Monz:2016:RSS

McKusick:2015:DIF

Minier:2012:RKI
REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-34478-7_8./ [MP12]

Morawiecki:2019:MS


Moriai:2019:PPD


Mosca:2018:CEQ


Moulick:2015:RDS


Minier:2012:EEC


Min:2018:AAB


Meiklejohn:2016:FBC

REFERENCES


Mundhenk:2017:SAN


Mironov:2012:IDP


Mukhamedov:2010:IEP


Maimut:2014:AET


Marasco:2014:SAS


Micali:2014:CMS

Manimehalai:2016:NRR


Migliore:2018:HSC


Moataz:2018:SSE


Martinovic:2017:AUP


Matsumoto:2017:ACG


Moghadam:2010:DRN

[I. Zarei Moghadam, A. S. Rostami, and M. R. Tanhatalab. Designing a random number generator with novel parallel LFSR substructure for key stream ciphers. In 2010 Interna-
REFERENCES


REFERENCES


[Meyers:2013:BCM] Steven Myers, Mona Sergi, and abhi shelat. Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness.


[Myers:2013:BBC] Steven Myers, Mona Sergi, and abhi shelat. Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness.


[Montuschi:2016:ISC] Paolo Montuschi, Michael Schulte, Javier Hormigo, Stuart Oberman, and

Marton:2010:RDC


Mashimo:2018:VMS


Mosenia:2017:CCA


Mazurczyk:2013:FWS


Martins:2018:SFH


Muhammad:2018:ISU

Khan Muhammad, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik. Image steganography using uncorrelated color space and its appli-


Mosca:2013:QKD

Morozov:2012:ZKP

Mamais:2017:BVP

Mouris:2018:TSB

Malkin:2011:ECS

Meerwald:2012:ER
Muftic:2016:BCC


Mundy:2017:CGU


Murphy:2010:BRB


Murdoch:2016:IDP


Miri:2012:SAC


Min:2016:RSC

REFERENCES


Xianmeng Meng and Xuexin Zheng. Cryptanalysis of

Marko:2017:MDI

Mastroeni:2017:APS

Manshaei:2013:GTM

Ma:2015:PKE

Meng:2019:ESF

Mofrad:2018:CSI
Saeid Mofrad, Fengwei Zhang, Shiyong Lu, and Weidong (Larry) Shi. A comparison study of In-


Nagy:2010:OTP


Nagy:2010:QCS


Naccache:2012:SAK


Naccache:2016:FHE


Nikiforakis:2014:BYO


Naccache:2012:CST


Naccache:2016:FHE
Nagaraj:2019:RCC

Nunez:2017:PRE

Namasudra:2019:IAB

Naskar:2013:GTL


Niev:2002:FLM

NIST:2012:RRN

NIST:2013:CSS

NIST:2015:SSP

Najafi:2019:VRS

Nguyen:2014:DDI
Ning:2012:DPB


Ning:2015:APB


Ning:2012:DCA


Norta:2019:SFB


Nieto:2013:PV


Nguyen:2018:TBU

REFERENCES

2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).


REFERENCES

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


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-34266-0_2.


Nguyen:2012:LRS


Nguyen:2010:LAS


Noorman:2017:SLC


Nie:2013:CHB

REFERENCES

Natgunanathan:2017:PBM


Ntantogian:2010:GME


Newell:2014:NCR


Niu:2015:NAS


Nikooghadam:2010:EUE


Obana:2011:AOC

REFERENCES

Oligeri:2011:REA


Obrenovic:2012:IUC


Odelu:2017:PSA


Otturk:2017:CAH


Oggier:2011:AAC


Obrien:2012:EPM


Onica:2016:CPP


**Oliynykov:2015:NES** [OGK+15]


**Ou:2010:CPA** [OHJ10]


**Ogiela:2018:EBI** [OK18]


**Oliveira:2012:STA**


**Or-Meir:2019:DMA** [OMNER19]


**Ortiz-Martin:2019:FAI**

Lara Ortiz-Martin, Pablo Picazo-Sanchez, Pedro

Ogiela:2010:UML


Ogiela:2018:LTC


Orlandi:2014:SCN


Obert:2016:PAC

James Obert, Inna Pivkina, Hong Huang, and Huiping Cao. Proactively applied encryption in multipath networks. *Comput-
Oppliger:2011:CC


Orumiehchilah:2014:PAN


Orejel:2014:E


Ormond:2016:CPR


Ozen:2011:MIS


Owczarek:2012:LPL

REFERENCES


Praba:2010:MAC


Parrilla:2019:ECC


Parveen:2018:IEE


Pal:2015:SDC


Pal:2016:ACC


Pandey:2014:ACR

Parent:2012:WAI


Park:2012:APO


Pass:2013:USP


Pranata:2013:MDR


Paulson:2010:SDO


Paul:2019:RCS


**Pandit:2012:EFS**


**Poh:2017:SDV**


**Park:2014:FRI**


**Poddar:2019:AED**


**Pun:2014:GIT**

Paul:2016:TSO


Papadopoulos:2014:LQA


Perkovic:2019:LVL


Premnath:2014:EHR


Poh:2017:SSE


Pang:2014:PPA


Patranabis:2019:SCS


Paul:2012:KSS


Pereira:2015:PKE


Pippal:2012:SVU


Pearson:2011:NWC


Peck:2012:CAC


Peck:2017:BWD

Morgan E. Peck. Blockchain world — do you need a blockchain? This chart will


Pendleton:2017:SSS


Peng:2010:SFW


Park:2012:IDF


Pohls:2012:RDI


Premnath:2016:SPC


Parno:2016:PNP

REFERENCES


Papas:2012:MLR


Park:2010:SIC


Pieprzyk:2010:TCC


Pointcheval:2012:ACE


Patel:2018:LLA

Hasmukh Patel and Devesh C. Jinwala. LPM: A lightweight authenticated packet marking approach for IP traceback. Computer
Premarathne:2015:LDD


Pramila:2018:ICA


Peter:2012:AHE


Phuc:2016:SAS


Perez:2011:FDS

Alejandro Pérez, Gabriel López, Óscar Cánovas, and Antonio F. Gómez-Skarmeta. Formal description of the SWIFT identity management framework. *Future Generation...
REFERENCES


Peris-Lopez:2018:EAC


Pang:2013:IMA


Peris-Lopez:2010:CSP


Perumal:2019:SDE


Pisani:2019:ABS

Paulo Henrique Pisani, Abir Mhenni, Romain Giot, Estelle Cherrier, Norman Poh, André Carlos Ponce de Leon Ferreira de Carvalho, Christophe Rosenberger, and Najoua Essoukri Ben Amara. Adaptive biometric systems: Review and per-
REFERENCES


REFERENCES


[PPSTT15] Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia,

Pandey:2012:PPS


Piret:2012:PBC


Proufoot:2015:WTH


Polyakov:2017:FPR

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


REFERENCES

Phatak:2013:SIN


Patranabis:2017:PSK


Pizzi:2018:ETM


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Pankhuri:2019:PBM

REFERENCES


Papamanthou:2013:SCC
[102x681]


Peng:2019:GCS
[184x646]


Papakostas:2014:MBL
[102x681]


Paletov:2018:ICA
[184x646]


Papamanthou:2016:AHT
[102x681]


Pudo:2012:RKA
[102x681]

Padget:2017:FGA


Pellikaan:2017:CCC


Pei:2013:ARW


Pham:2019:SSS


Puthal:2019:SSE


Poller:2012:EIC


Peng:2010:IWM

Hong Peng, Jun Wang, and

Pongaliur:2013:SNS


Pja:2019:SSG


Pagnin:2018:HDB


Philippaerts:2013:CMC


Pei:2015:SWT


Papadopoulos:2010:CAR

Stavros Papadopoulos, Yin Yang, and Dimitris Pa-

**Phuong:2018:CBE**


**Pops18**


**Pournaghi:2018:NNE**


**Peng:2019:EDI**


**Patsakis:2015:PSM**


**Qiu:2018:QDS**

Lirong Qiu, Feng Cai, and


REFERENCES

QLZ19

QMC17

QMW17

QRW+18

QS18

QYWX16
Zhen Qin, Chen Yuan, Yilei Wang, and Hu Xiong. On the security of two identity-based signature schemes based on pair-
Qian:2014:IAF


Qi:2016:SCF


Qi:2016:SID


Qin:2018:BR


Rabin:2010:A

Tal Rabin, editor. *Advances in cryptology — Crypto 2010: 30th annual cryptography conference, Santa Barbara, CA, USA*,
REFERENCES


[Raz19] Ran Raz. Fast learning requires good memory: a time-space lower bound for


[RC18] Jithin R and Priya Chandran. Secure and dynamic memory management architecture for virtualization technologies in

**Rao:2019:HPR**


**Rabinovich:2017:WNI**


**Raisaro:2018:PPS**


**Rabbachin:2015:WNI**


**Rao:2017:CFA**


REFERENCES

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

**Robert-Inacio:2011:SAP**


**Rjasko:2012:BBP**


**Roy:2018:HFB**


**Regev:2011:QOW**


**Rakshit:2018:LLO**


**Rezaeibagha:2019:EMC**

REFERENCES

Reyhani-Masoleh:2019:NMI


Reyhani-Masoleh:2018:NAR


Roy:2018:HIR


Rezaeibagha:2019:PSB


Rahaman:2010:STB


Rogaway:2016:POP

Rohloff:2019:CAR

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

Romero:2011:FSW


Romero:2012:IBB


Rose:2011:KBT


Rao:2012:SSA


Rifa-Pous:2012:AHD


Rifa-Pous:2011:CEC


Rhee:2010:TSS

Hyun Sook Rhee, Jong Hwan Park, Willy Susilo, and Dong Hoon Lee. Trapdoor security in a searchable public-key encryption

**Ren:2015:ASE**


**Rawat:2011:CBR**


**Razaque:2016:TDP**


**Razzaque:2017:SDA**


**Rosen:2010:CCS**


**Reeder:2011:WPD**


**Rivest:2014:SSR**

Ronald L. Rivest and Jacob C. N. Schuldt. Spritz —


Resende:2019:BMI


Ruj:2014:DAC


Rahulamathavan:2019:PPI


Ryan:2015:EEVa


Ryan:2015:EEVb


Rexha:2018:ITF


Jian Ren, Jie Wu, Yun Li, and Jian Li. Hop-by-hop message authentication and source privacy in wireless sensor networks. *IEEE Transactions...*


**Sang:2012:SSF**


**Sakalli:2014:ACC**


**Somanatha:2015:RAK**


**Shivani:2016:PVC**


**Siad:2016:NFI**

REFERENCES

Subramanian:2019:SAF


Saarinen:2012:PPK


Suoran:2012:SAM


Sarreshtedari:2015:WMD


Schutz:2010:DIN


Sacco:2014:MC


Sahai:2013:TCT


Sarier:2010:IAS
Sarier:2012:SNB


[Sar10a]

S Sarkar:2010:SGC


[Sar10b]

S Sarkar:2011:TES


[Sar11]

S Sarkar:2014:PEK


[Sar14]

S Sarkar:2018:MBI

REFERENCES


Safkhani:2017:PSD


Shwartz:2018:DMI


Stevens:2017:AFS


Sarkar:2015:DFA


Safkhani:2012:SMA


Safkhani:2018:SRO


Santos:2014:ACD

Ricardo Jorge Santos, Jorge Bernardino, and

Shyu:2010:VMS

Srinivasan:2012:RAP

Singh:2019:SID

Sujitha:2019:HSP

Sun:2016:TCA

Saevanee:2015:CUA
REFERENCES


REFERENCES

com/chapter/10.1007/978-3-642-33167-1_6/.

Schneier:2013:HDD

Schneier:2015:DGH

Schneider:2016:MSI

Schneider:2016:DEE

Schaefer:2015:BRB

Schaffer:2015:ECA
Schneier:2016:CHT


Schneier:2018:CAA


Schneier:2019:CPI


Scholl:2019:SIE


Shrestha:2010:KBA


Stobert:2018:TAL


Seberry:2010:CTAa

Seberry:2010:CTAb


Scriber:2018:FDB


Shu:2015:PML


Saleh:2010:GTF


Shen:2012:PAS

Jing Shen and Yusong Du. A password authentication...


Shakiba:2014:CCI


Seo:2014:RHI


Seo:2016:RHI


Salman:2018:BMM


Sasaki:2012:IKK


Staples:2019:SAB

J. Staples, C. Endicott, L. Krause, P. Pal, P. Samouelian, R. Schantz, and A. Wellman. A semi-autonomic bytecode re-

Sendrier:2010:PQC

Sendrier:2017:CBC

Seo:2018:CSI

Serrato:2012:IAN

Sallam:2012:EBM

Sakai:2016:CDN
Sethumadhavan:2016:HEP


Severance:2016:BSB


Seo:2018:AOF


Savas:2014:SMQ


Su:2012:IIN


Shabtai:2010:SAP

REFERENCES

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

Schneier:2015:SWC


Sarma:2012:STP


Sasdrich:2015:ICS


Sakellariou:2019:HEK


Sgantzos:2019:AII


Shu:2014:DAS


Saxena:2016:API

Neetesh Saxena, Santiago Grijalva, and Narendra S.

**Silva-Garcia:2018:SBG**


**S:2018:EDS**


**Sun:2015:FSW**


**Shen:2018:CAL**


Seyedzadeh:2011:IEA


Song:2015:ADT


Shallit:2010:BRB


Shaw:2013:DE


Syed:2019:TGB


Sodsong:2016:DPB

[SHC+16] Wasuwee Sodsong, Jingu Hong, Seongwook Chung, Yeongkyu Lim, Shin-Dug Kim, and Bernd Burgstaller. Dynamic partitioning-based JPEG


REFERENCES

Suoranta:2012:ASM


Shyu:2015:VCR


Satir:2012:CBT


Siad:2012:NAP


Simpson:2010:ESB


Simion:2015:RST


Simmonds:2015:DI


REFERENCES


Stevens:2015:FCF


Singh:2018:MWT


Scheidat:2012:STT


Schmitz:2012:NA


Srivatsa:2011:ESA


[Sarkar:2010:CRM] Santanu Sarkar and Sub-


[Swami:2018:AAS] Shivam Swami and Kartik Mohanram. ARSENAL: Architecture for se-

**Shibu:2019:ARR**


**Shokri:2019:ESS**


**Smart:2016:CMS**


**Stanton:2010:FAD**


**Salmon:2011:PRN**


**Smith:2011:SSX**

REFERENCES

Smith:2011:RBA

Smith:2015:HHB

Smith:2015:DBP

Swierczynski:2015:PSE

Stankovski:2014:CFE

Sucasas:2016:APP
Sharma:2018:CSS


Sadeghi:2010:THI


Son:2018:GFD


Siadati:2017:MYS


Safavi-Naini:2011:USC


Seyedzadeh:2014:RCI

Seyed Mohammad Seyedzadeh, Benyamin Norouzi, and Sattar Mirzakuchaki. RGB


Serwadda:2013:ELK [SP13] Abdul Serwadda and Vir V. Phoha. Examining a large keystroke biometrics dataset for statistical-

**Shiaeles:2015:FII**


**Shim:2015:SDA**


**Spafford:2016:SE**


**Salvail:2010:STR**


**Sherman:2019:PBL**


[SR12a] Thorsten Ernst Schilling


Soubhagya Sutar, Arnab Raha, Devadatta Kulkarni, Rajeev Shorey, Jeffrey Tew, and Vijay Raghunathan. D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication and random number generation. ACM


[Szaban:2011:IQB]


[Saxena:2012:BIT]


[Shparlinski:2012:CSD]


[Sadhyaa:2017:PRE]

Shivani:2017:RIE


Siegel:2019:UOC


Singh:2013:QBF


Smith:2011:SMC


Sakai:2016:NCS


Shahandashti:2015:RUP


REFERENCES


REFERENCES


**Stallings:2011:C**


**Stallings:2011:CNS**


**Stanoyevitch:2011:ICM**


**Staneck:2012:TEM**


**Staff:2013:ITD**


**Stewart:2011:CCI**


**Steel:2015:APF**


ShanmugaPriya:2019:PAS


Shi:2019:LWW


Shoufan:2010:NCA


Song:2016:IBS


Song:2017:PPF


Sheldon:2012:IWN

Sha:2019:CED


Su:2016:PSN


Sahillioglu:2014:SCM


Savas:2015:GMA


Shao:2015:SAS


Song:2017:SSI

Jun Song, Fan Yang, Kim-Kwang Raymond Choo, Zhijian Zhuang, and Lizhe Wang. SIPF: a secure installment payment framework for drive-thru Inter-
REFERENCES

Seo:2013:PIC

SoltaniPanah:2019:CDG

Shuai:2019:AAS

Song:2017:SAM

Sui:2014:DAH
Yan Sui, Xukai Zou,


Tsang:2010:BRR


Tan:2012:SLM


Tamayo:2015:AFH


Tan:2012:LCP


Tan:2011:CTA


Tan:2015:ETE

REFERENCES

Tang:2015:HAC

Tankard:2017:BNK

Tankard:2017:ECB

Tankard:2018:LAA


Tarnovsky:2010:DSP

Taylor:2014:WSE

Taylor:2017:EBH
Taylor:2019:DST


Talbi:2018:SIW


Tilli:2015:GCR


Takagi:2019:ISC


Treleaven:2017:BTF


Tuan:2010:AWB

Taylor:2011:DR


Tang:2015:CER


Testa:2019:SFE


Tiplea:2014:NSC

Ferucio Laurentiu Tiplea and Constantin Catalin Dragan. A necessary and sufficient condition for the asymptotic idealness of the...

References

[Tao:2013:SMS]

[Teng:2018:KP]

[Terai:2011:BRB]

[Tseng:2019:AMR]

[Tassa:2012:SDC]

[Tewari:2017:CNU]
The references include works by Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong, who discuss secure and usable enterprise authentication: Lessons from the field. Their work is published in IEEE Security & Privacy, 14(5):14–21, September/October 2016.


Nerea Toledo, Marivi Higuero, Jasone Astorga, Marina Aguado, and Jean Marie Bonnin evaluate the security of NeMHIP, a new secure and efficient network mobility management protocol based on the host identity protocol. Their findings are published in Computers & Security, 32(??):1–18, February 2013.


Rasha Thabit and Bee Ee Khoo introduce a robust reversible watermarking scheme using Slantlet transform matrix. This work is found in The Journal of Systems and Soft-


REFERENCES


Tian:2017:RSP


Tsay:2012:VUL


Tsoutsos:2018:EDM


Tormo:2013:IMP


Terrovitis:2011:LGR

Manolis Terrovitis, Nikos Mamoulis, and Panos Kal-

**Terrovitis:2012:PPD**


**Tao:2018:AAC**


**Tomb:2016:AVR**


**Taox:2014:NSS**


**Tsougenis:2012:PEM**


**Tan:2016:BIB**

Chik How Tan, Theo Fanuela Prabowo, and Duc-Phong Le. Breaking an ID-based encryption based on discrete logarithm and factor-
Tang:2014:PAB


Tschorsch:2016:BBT


Taassori:2018:VRP


Tao:2014:CFS

Jia Tao, Giora Slutzki, and Vasant Honavar. A conceptual framework for secrecy-preserving reasoning in knowledge bases. *ACM
REFERENCES


[Toreini:2017:TRP]


[Tang:2011:IDC]


[Tso:2013:SAI]


[Tseng:2012:ERI]


[Tenca:2018:PIS]


[Tseng:2015:LFI]

Tsai:2010:RLI  

Tupakula:2015:TES  

Turan:2019:CFF  

Thorpe:2012:CRB  

Tripunitara:2014:CKM  

Wu:2012:SWG  
http://link.springer.com/chapter/10.1007/978-3-642-28693-3_4.

Toor:2018:VQA


Tartary:2011:EIT


Tian:2012:SSB


Trost:2016:OPC


Tan:2016:CCA


Tolba:2016:GMA

REFERENCES


Dominique Unruh. Re-


[VIGIL2015:IAN] Martín Vigil, Johannes Buchmann, Daniel Cabar-

Venkataramani:2016:DHC


Valamehr:2012:IRM


Vatajelu:2016:SMB


VandeGraaf:2017:LTT


vanDam:2011:TQC

REFERENCES


Visegrady:2014:SCV


Vandewalt:2018:CSI


VenafiLabs:2014:VLQ


Vergnaud:2017:CAB


Vetter:2010:ABV


Vo:2019:ISA

REFERENCES


REFERENCES

**Viennot:2014:MSG**


**Vasishht:2018:DEU**


**Vu:2015:NAN**


**Vgena:2019:TAL**


**Vasiliadis:2017:DIS**


**Vleju:2012:CCA**

Mircea Boris Vleju. A

**Vivek:2014:CSC**


**Vliegen:2015:SRD**


**Vollala:2017:EEM**


**VonMaurich:2015:IQM**


**Varadharajan:2018:AUR**

[V. S. Varadharajan, D. S. Onge, C. Guß, and G. Bel-
REFERENCES


**vanRijswijk-Deij:2017:PIE**


**Vembuselvi:2011:LLL**


**Vassilev:2016:ESU**


**Vivist:2012:CSE**


**Vlachos:2015:DPC**


**vanTilborg:2011:ECS**

Viswanathan:2018:EEG


Vuagnoux:2010:CAC


vanVredendaal:2016:RMM


VanDijkhuizen:2018:SNT


Vazirani:2019:FDI


Valente:2019:SSA

REFERENCES

Wagner:2016:TPF

Woo:2019:UEM

Walter:2018:RCS

Wang:2010:NSB

Wang:2013:CRA

Wang:2014:IIA
Huaqun Wang. Insecurity of ‘Improved Anonymous


REFERENCES

Watts:2014:PYI


Watts:2015:HGA


Wang:2012:PCE


Weisse:2017:RLC


Wright:2010:USP


Wu:2018:ESS

Wang:2019:IFT

Wang:2018:SNU

Wei:2018:GCQ

Wu:2017:HMA

Wang:2018:SEA

Wei:2012:NTB
Zhuo Wei, Xuhua Ding, Robert Huijie Deng, and Yongdong Wu. No trade-off between confidentiality...

Wang:2019:FTSa


Wazid:2019:DSK


Wazid:2018:AKM


Wang:2019:SFE


Wang:2013:SES

Guojun Wang, Qiushuang Du, Wei Zhou, and Qin Liu. A scalable encryption scheme for multi-privileged group communi-

West:2015:EC


0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-35606-3_13/


REFERENCES

Wei:2016:PAB

Wei:2017:CES

Wang:2012:NFS


Wang:2012:FOP
REFERENCES


**Wu:2011:HQI**


**Weissman:2011:LLB**


**Wang:2012:MCE**


**Wu:2019:VFS**


**Wei:2012:IRK**

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

**Wang:2011:RBM**

Wang:2017:CAS


Wang:2013:HCL


Wei:2015:FST


Wei:2014:EEF


Wang:2011:HAB


Wu:2015:TRM


Wang:2017:CES

Wang:2015:PPK

Won:2016:PAA

Wu:2012:UFS

Wendzel:2015:CME

Wendzel:2015:CME

Wang:2017:PPK

**Wang:2016:SEP**


**Wu:2013:FTR**


**Wu:2016:CBE**


**Wei:2015:TPE**


**Wani:1970:PEA**


**Wang:2019:CPB**


**Wu:2016:BPK**


**Watanabe:2012:ITT**


**Wei:2019:VF**


**Wang:2012:PAC**


Wei-Chen Wu. A secret push messaging service in

**Wu:2012:AST**


**WWBC14**


**Wen:2014:MZC**

REFERENCES


Wu:2018:SMI


Wei:2016:APS


Wang:2013:BSB


Wang:2014:CGR


Wang:2017:RRA


Wen:2011:DSH

[Wei:2015:CPK]

[Wang:2016:SAP]

[Wang:2018:AMB]

[WZLW13]

[WZC16]

[WZCH19]

[WZM12a]
REFERENCES

Wei:2012:GOP


[WZM12b]

Wang:2012:NIS


[XGLM14]

Xiong:2013:NIB


[XHC+12]

Xu:2014:AHA


[XGLM14]

Xu:2012:APA


[Xu:2019:TPT] Lingling Xu, Jin Li, Xiaofeng Chen, Wanhua Li, Shaohua Tang, and Hao-

Xue:2012:AHA


Xue:2018:SNN


Xiong:2009:PSI


Xiang:2016:EMP


Xue:2013:TCB


REFERENCES


Xiong:2011:CIB


Xin:2010:IEB


Xiao:2010:TAT

Xiaokui Xiao, Yufei Tao, and Nick Koudas. Transparent anonymization: Thwarting adversaries who know


Xu:2019:DAB


Xie:2012:ORI


Xie:2013:SIP

Yongming Xie and Guojun Wang. Special issue papers:

**Xiong:2012:CBP**


**Xu:2017:SEP**


**Xia:2016:SDM**


**Xie:2014:SCP**

**Xu:2018:SKS**

**Xiao:2016:REM**

**Xu:2019:LAM**


REFERENCES

Xu:2015:ORA

Xiong:2019:PPH

Xiong:2012:CLR

Xiao:2018:FEI

Yoo:2017:PQD

Yaacoubi:2019:REM
Yamaguchi:2012:EVC


Yu:2015:SDS


Yang:2010:PII


Yang:2011:PQC


Yang:2014:BEB


Yang:2011:GSS

Ching-Nung Yang and

[YC12]


[YC12]


[YC12]


[YC12]


[YC12]

REFERENCES


Zheng Yan, Wenxiu Ding, Xixun Yu, Haiqi Zhu, and


Jia Yu, Fanyu, Kong, Xiangguo Cheng, Rong Hao, and Jianxi Fan. Erratum to the paper: Forward-Secure Identity-Based Public-Key

**Yang:2017:CCS**


**Yang:2018:RRE**


**Yuce:2017:AFI**


**Yang:2015:SHI**


**Ye:2017:VCS**


Ye:2016:IEA


[YH+10]


Yu:2010:IBF

[YHL16]


Yang:2016:EHA


Ya:2019:RSA

Yang:2014:MDF


Yamada:2017:EPA


Youn:2018:DAH


Yang:2018:CPG


Yang:2016:TCP


Yassein:2016:FSB

REFERENCES


Dae Hyun Yum, Duk Soo Kim, Jin Seok Kim, and Pil Joong Lee. Order-preserving encryption for non-uniformly distributed plaintexts. *Lecture Notes
REFERENCES


Yoshino:2012:SIP


Yum:2011:ACO


Yuen:2013:ELT


Yang:2012:WSI

REFERENCES


Osman Yagan and Armand M. Makowski. Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key...


 REFERENCES


Yong Yu, Jianbing Ni, Qi Xia, Xiaofen Wang,

Yong:2011:SPP

**[Yon11]**


Yoneyama:2012:ORA

**[Yon12]**


Yang:2017:SAS

**[YPRI17]**


Yang:2012:EMA

**[YQH12]**


Yin:2017:QPE

**[YQOL17]**

Hui Yin, Zheng Qin, Lu Ou, and Keqin Li. A query privacy-enhanced and secure search scheme over encrypted data in cloud computing. *Journal of Computer and System Sciences*, 90(??):14–27, December 2017. CODEN JCSSBM. ISSN 0022-0000
REFERENCES


[Yin:2019:SCM]


[Yang:2012:SAK]


[Yengisetty:2011:AVC]


[Yumbul:2015:EEP]


[Yi:2016:IPA]

[YSC+15] Bin Yang, Xingming Sun, Xianyi Chen, Jianjun Zhang, and Xu Li. Exposing photographic splicing by detecting the inconsistencies in shad-

**Yang:2016:ECV**


**Yang:2018:HEP**


**Yang:2019:ISO**


**Yuen:2014:TCT**


Yao:2010:IDA


Yao:2010:ASP


Yan:2017:PIS


Ye:2019:NCA


Yang:2015:RCI


Wang:2011:RDA


Yu:2012:SME


Yang:2018:EEC


Yu:2016:CDI


Yang:2018:PBC


Ye:2018:ISS

REFERENCES

**Yoon:2011:SBC**


**Yoon:2013:RBB**


**Young:2017:PSC**


**Yu:2017:PFS**


**Yildiz:2017:BLF**


**Yang:2019:NPP**

[YYK+19] Xu Yang, Xun Yi, Ibrahim Khalil, Hui Cui, Xuechao Yang, Surya Nepal, Xinyi Huang, and Yali Zeng. A new privacy-preserving authentication protocol for

**Yesilyurt:2015:RWM**


**Yang:2013:ECS**


**Yang:2016:EPA**


**Yu:2019:PSI**


**Yang:2012:LUC**

Yang:2017:SKS


Yang:2019:HDS


Yang:2018:CDD


Yang:2012:BPN


Yang:2012:NIB


Yang:2014:PST

Haomin Yang, Yaoxue Zhang, Yuezhi Zhou, Xiaoming Fu, Hao Liu,

Zhai:2017:EEI


Zajac:2019:HEM


Zon-2018:CSC


Zidaric:2019:HOA


REFERENCES


Zhang:2012:AOP


Zhou:2016:IBP


Zetter:2014:CZD


Zhou:2018:SAE


Zhao:2010:PSA


Zhou:2016:HFD

Zhou:2018:CBG


Zhang:2018:AAG


Zadeh:2015:ASP


Zhang:2012:LDC

Haibin Zhang. Length-


[ZHU19] P. Zuo, Y. Hua, M. Zhao, W. Zhou, and Y. Guo. Write deduplication and hash mode encryption for secure nonvolatile main memory. *IEEE Mi-

**Zimand:2010:SEC**


**Zhang:2011:FBP**


**Zeng:2014:NFC**


**Zhou:2012:CBF**


**Zhang:2019:CCF**


**Zhou:2015:PPS**

REFERENCES

645

Zhao:2012:IAS

Zhao:2014:TAH

Zhang:2012:EEF

Zhang:2015:RBA

Zhang:2012:CCB
REFERENCES

Zhu:2017:PSN


Zhang:2010:ESP


Zhou:2019:LIB


Zhang:2016:TLT


Zhang:2018:SPF


Zhang:2017:FGA

REFERENCES

Zhang:2010:NSS


Zielinska:2014:TS


Zhang:2016:CAH


Zaeem:2017:MAI


Zafar:2010:GRN


Zorpette:2012:BEC

Glenn Zorpette. The beginning of the end of cash?
Zhang:2017:PPN


Zavattoni:2015:SIA


Zheng:2016:EUV


Zhao:2012:SSS


Zhou:2017:IBB


Zenger:2016:AKE

Christian T. Zenger, Mario Pietersz, Jan Zimmer, Jan-Felix Posielek, Thorben Lenze, and Christof Paar. Authenticated key establishment for low-resource devices exploiting correlated random channels. Computer Networks (Amsterdam, Netherlands: 1999), 109 (part 1)(??):105–123,
Zhang:2016:SBA


Zhang:2015:MAA


Zhang:2010:EMO


Zmudzinski:2012:WEU


Zhao:2012:SSM


Zhou:2019:LIN


Zheng:2018:GDP


Zanon:2019:FKC


Zhang:2012:EHO


Zhou:2018:TPW


Zuo:2018:CSA

Zhou:2019:LCP

Zhang:2014:NCM

Zhu:2015:PPD

Zwattendorfer:2012:CBL

Zhang:2016:EEA

Zhou:2016:SRB
REFERENCES


Zilberberg:2013:PCM


Zilberberg:2013:PCM

Zhang:2015:FER


Zhang:2015:FER

Zhang:2017:FBI


Zhang:2017:FBI

Zhang:2013:LPP


Zhang:2013:LPP

Zhang:2019:MAA


Zhang:2019:MAA

Zhang:2017:FWI

REFERENCES


[ZXWA18] Yuexin Zhang, Yang Xiang, Wei Wu, and Abdulhameed Alelaiwi. A

**Zhang:2016:DEP**


**Zhang:2011:SIR**


**Zhou:2017:CLR**


**Zhou:2017:LRC**


**Zhang:2017:GFD**

REFERENCES


Zheng:2010:PS


Zhan:2017:NKG


Zhan:2018:EKG


Zhan:2018:EKG

[ZYM18] Zhan:2018:CLR


Zhou:2019:CLR


Zhou:2018:CLR


Zhao:2012:FCS


Zhang:2015:ITS


Zheng:2015:EPT


Zhou:2017:ENQ


Zaidan:2017:NDW

