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/
05 August 2019
Version 1.474

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N) [Bai10, YC11], (n, t, n) [LHYZ12], (t, n) [QD16, ZPY12]. 0 [XHX+17]. 1 [XHX+17]. 1, 2, 3 [SMD11]. 11 [LJ17]. 13 [B15]. 2 [DBPS12, EAA+16, ESS12, JR13, MCDB12, PGL10, WY12]. 22 [MN12]. 2^k [Sun16]. 3 [AP10, CG12b, DWZ12, FWS13, GZHD12, GH11a, KWS+12, LJ17, LJ15, MKH+12, RS16, SS10b, SS12a, SGS14, WSS12, tWmC12, YT11a, YH14, YPRI17]. 32 \times 32 [SA14]. 3 \times 3 [ÄMVZ12]. 4 [COP+14, DWZ12, HLYS14]. $49.00 [Sch15a]. 8 [LPO+17]. $9 [APPV15] = [JJUW10]. $[PYH+18]. 2 [YNX+16]. 3 [LHM14]. MT [HRB13]. \alpha [TTL10]. c [KRDH13]. d [QD16]. d \times d [KA17]. \ell [ZTL15]. F_p + \nu F_p [WGF16]. \gamma [DWZ12]. GF(2)[x] [SF12]. GF(2^m) [SKH15]. GF(2^n) [LBOX12]. K [FXP12, FR16, CHX13, XLP+18, ZHT16]. L(1/4 + o(1)) [Jou13]. M [MMS13, ÔS11]. F_{q,500} [AMORH13]. F_q [SS13]. N/P [HN10]. GF(q) [LPd10]. LWE [BV14]. \mu [Jia14a]. N [FR16]. n \times k(k \geq n/2) [MC11]. O(d_1^d) [KA17]. O(n^2) [KS11]. P [DG17]. \pm 1 [HW+14]. q [GMS11]. S [LJ15]. t [HJM+11, Oba11]. w [Kre13].


.onion [Boy16].

0.13um [KLM+12].


3 [ABM+12, BD15, jCPB+12, Full0, LC17]. 30th [Rab10]. 31st [PJ12]. 384-bit [MMN12]. 3GPP [FPBG14].


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

72 [HYS18]. 768-bit [KFL+10].

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


Advanced [Bö10, CSYY18, DR10, TC10, YWF18, ALL+18, DDFR13, GLC10, Kra12, MKRM10, NdMMW16, SKK10]. Advances [LLK18, PHWM10, WP15, Abe10, Gil10, LW11a, PJJ12, Rab10]. Advantage [WSSO12]. Adversarial [BAG12, BJR+14]. Adversaries [BC14, XTK10]. Adversary [Yon12, KS11, LXY12, ZPWY12]. Advertisement [Ano16a, AMHJ10].


Affiliation-Hiding [XLM+12, XGLM14, XZLW15]. Affine [BCEM15, GZHD12, ZWM14]. affine-transformation-invariant [GZHD12]. Afraid [Par12a]. Africa [BL10]. Africacrypt [BL10]. after [Sch18]. Against [Ano17e, BVS+13, BL15, CW12b, CMA14, DZS+18, GDCC16, HCTET1+12, Sch13, SGH15, SLY+16, WSA15, AATM18, ASBdS16, BDBBP13, BVIB12, BPR14a, BPR14b, BFK16, BSR+14, BK12b, Bud16, Che15, CG14a, CGCS12, CGH17, DHLA10, DK17, EWS14, FT+10, zGXW12, GSC17, HLLG18, JSMG18, JHHN12, LGL+12, LLY+12a, LWC14, Maf16, MDP12, NDNDR13, OF11, QRW+18, SE14, SY15b, SD12, TLL13, WHN+12, Yon12, ZLQ15, ZHS+19].


Aggregating [DP12]. Aggregation [BJ16, LHKR10, SP15b, ZHW+16, WMYR16]. Aging [SK12]. Agnes [Bur11, Joh15]. Agreement [Chi16, HCL+14, EHC+12, MNS11, TM12, WSS12, XLM+12, XGLM14, XZLW15, APK+18, AN15, BGAD12, CSD18, CTL13, DLK+16, GH16, HPC12, HWB12, ISC+16, IB11, IOV+18, KS11, KIH19, KP18, KLM+16, KDW+17, LLL13, LIK+17, NCL13, Nos11, Nos14, hSZZ15, TLL12, WXK+17, XCL13, XMHD13, XHM14, YZZ+14, ZQW+11, ZTZ16, ZZC15, OHH10]. agriculture [APK+18]. Aided [BGK12, BCGK12, BGB12, GMSV14].
Vua\textsuperscript{10}, ABBD\textsubscript{13}, LYL\textsubscript{15}, SGJ\textsuperscript{+18}, SSAF\textsubscript{11}, WLFX\textsubscript{17}. \textbf{AIP1Ste}g \textsuperscript{[AGLW16]} Air \textsuperscript{[AUMT16, VOGB18, XZW\textsuperscript{+18}]. aircraft \textsuperscript{[XWZW16]} Airflow \textsuperscript{[RSCX18]} Airway \textsuperscript{[RSCX18]} AX \textsuperscript{[XHC\textsuperscript{+12}]. AK-PPM \textsuperscript{[XHC\textsuperscript{+12}]. AKA \textsuperscript{[LLLS13]} AKF \textsuperscript{[KDH15]} al \textsuperscript{[LLW16, LLSW16, MWZ12, PLPW13, SBS\textsuperscript{+12}, Ma14, Ke15]. al-Qa}eda \textsuperscript{[Ma14, Ke15]. al \textsuperscript{[ABJ13, SPLHCB14]} Alan \textsuperscript{[CS12, Don14, Hel17, LCKBJ12]} Algebra \textsuperscript{[Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14]. Algebra} \textsuperscript{ic \textsuperscript{[SK11, Tam15, Wat10, Bul10a, CFR11, FMB\textsuperscript{+18}, SA14, YTM\textsuperscript{+14}. Algorithm} \textsuperscript{[ABCL17, Ano11b, AK14, BGJT14, BKLS18, CNR14, JCPB\textsuperscript{+12}, DCM18, ESS12, GKS\textsuperscript{B17}, JH12, JSZS12, JHHN12, JI16, KB10, LL11, LT14a, LLL17a, LLLH18, MRL\textsuperscript{+18}, NdM\textsuperscript{MW16}, NV10, RR11, RVRC1\textsuperscript{M12}, WH12, WZC18, YPR17, YH16, ZSW\textsuperscript{+12}, Ant14, BGJT13, BMB\textsuperscript{16}, CG\textsubscript{12b}, Chm10, EEAZ\textsuperscript{13}, JK\textsuperscript{13}, KY10, KMB\textsuperscript{13}, LC17, LR15, MS12a, MM14b, MN\textsuperscript{+16}, MN14, PGL\textsuperscript{L10}, PA10, PC14, SH11, SL1\textsuperscript{M10, SWW\textsuperscript{+17}, JT12b, TTI10, WGG\textsuperscript{+12}, XTK10, YWL\textsuperscript{+17}, Z\textsuperscript{LW12}, ZL12, \textsuperscript{Á}C\textsuperscript{Z16, ZOC10}. Algorithmic} \textsuperscript{[GO17, KKH18, AY12]. Algorithms} \textsuperscript{[Gas13]. Algorithms} \textsuperscript{[AMKA17, AB10b, BCG12a, BJ10, CN12, GP17, KRD13, MR14a, MM17, TKM12, WH18, YS15, ZW15, AGHP14, Fri10a, Mac12, NACL\textsuperscript{R12}, NC13, OO10, OO10, Xie12, \textsuperscript{[Al13]. Aliens} \textsuperscript{[Sch18]}] Alignment \textsuperscript{[Don14, IA15]. all-seeing} \textsuperscript{[Tox14]. Allowing} \textsuperscript{[PRC12]. Allows} \textsuperscript{[Bro17]. Almost} \textsuperscript{[BKST18, FFL12, GDCC16, Oba11]. Almost-Tight} \textsuperscript{[GDCC16]. Almost-Universal} \textsuperscript{[BKST18]. Altera} \textsuperscript{[SMOP15]. alternate} \textsuperscript{[ZLW\textsuperscript{+12}. Alternating} \textsuperscript{[BKLS12, KD15]. AMBTC} \textsuperscript{[KSSY12]. America} \textsuperscript{[AB10a, Bha16, Fag17]. American} \textsuperscript{[Sch15a, Mun17]. Americans} \textsuperscript{[ABJ13]. Amoeba} \textsuperscript{[MPA\textsuperscript{+18}. among [BP11, MPJ\textsuperscript{+16}, SS17]. amount} \textsuperscript{[EEAZ13]. Amplification} \textsuperscript{[ABF12, HMR14]. Analog} \textsuperscript{[KOP12, SOS15]. Analyses} \textsuperscript{[ZPX17]. Analysing} \textsuperscript{[GRL12]. Analysis} \textsuperscript{[ABS\textsuperscript{+12}, ARP12, BRS17, BBB\textsuperscript{+16a}, BC14, BS14, BKLS18, CFE16, CCG\textsuperscript{+16}, CGL\textsuperscript{+12}, DKMR15, FSW11, GZZ\textsuperscript{+13}, GWM16, GLG12, HC12, HH\textsuperscript{H\textsuperscript{+13}, HZW17, HB17, IBC13a, IS12, JT12a, KE19, KOP12, Kre13, LPS12, LTKP16, LKC11, LLW16, LGL11, MD12b, MAS16, MRT12, MR10, NDC\textsuperscript{+13}, NSA15, NAL17, PH12a, PFS12, PS14, RZZ\textsuperscript{+15}, Rao10, RBS\textsuperscript{+17}, SK11, SY15a, SR12a, Sh11, SZDL14, SCGW\textsuperscript{+14}, VKC15, WDDW12, YZLC12, ZH15, ZAG19, ZBPF18, Aia15, ACF16, AN15, BNY14, CFH\textsuperscript{+13}, CFL13, DMV15, DK7, DHW\textsuperscript{+13}, DMIT12, FTV\textsuperscript{+10}, FAA\textsuperscript{+18}, FHM\textsuperscript{+12}, HM10, Lan11, MFH13, NLYZ12, PPA18, PL16, QGGL13, RITF\textsuperscript{+11}, SKE14, TQL\textsuperscript{+14}, TLMM13, Tso13, VS11, Ven14, ZZK17. Analysis-]"
Assessing [CBL13]. assets [WHJ17].
Assignment [LMS16]. Assisted
[KCC17, LLKA19, HZWZ18]. Associated
[Sar10b]. associative [BS15]. Associativity
[ABR12]. Assumption
[LZC12a, LZC14, ZG10]. Assumptions
[BDH11, CZF12, DN12, GK17, KM10c,
PDNH15, ABW10]. Assurance [BMBS10,
Bar15, KMP+11, RBNB15, WL11, Ser12].
Assured [Tan15a, WMYR16]. Asymmetric
[ HG12, XLM+12, XGLM14, XZLW15,
ZZQ+19, ZWQ+11, CSS+13]. asymmetric-histogram [CSS+13]. asymptotic [DTZZ12, TD14].
Asymptotically [LPS12]. Attack
[Ano15d, BRS17, BMS12, Bro17, Che18,
CJP12, DSB15, MBB11, MN12,
NZL+15, SB17, SXL16, WYL13]. attacker
[PLGMCdF18]. Attackers [BL15]. Attacks
[ARP12, Ano17e, BGK12, BFK16, BKBK14,
Che15, CMA14, DZ+18, DGIS12,
DHLAW10, DHB16, EWS14, GPT14,
HLLG18, Hay13, HRS16, JSK+16, JW+17,
KNR10, LLC11, LWZ12, LWJC14, LCL17b,
MD12b, PYM+13, PS12, Sas12, SE14,
SY15a, SP15a, SH15, SVG16, HJ15, WH+14,
WH+12, XNG+14, YL17, YCM+13,
ZLQ15, ZHS+19, AATM18, BBP13,
BV12B, BSR+14, CGH17, dCCSM+12,
DCAT12, DJL+12, DK17, Dra16, EA12,
FVT+10, FIO15, GPP+16, GBNM11,
KM10a, KPS10, LW11, NDN13, OF11,
PX13, SG+17, TK19, TS16a, TY16b,
TLL13, VS11, WWBC14, XWDN12].
attempt [Fel13]. attestation [FQZF18].
ATtiny [EGG+12]. Attribute
[AAC+16, AHL+12, BFK+10, Boy13, CD16,
CDL18, FHR14, GZZ+13, GSW+16, Gli12,
GVW15, HSMY12, Her14, KGP12, LW11b,
LW11c, LW12, L JL12, LY+13, LHL+14,
LAL+15, LHL15, LW16, OT12, PPA18,
P12, RV+16, Rao17, SSW12, TYM+17,
WDC18, WLH15, WHL16, XML13,
XWL16, XHY+17, ZP+15, ZQQ+15,
ZM17, ZWH15, CPPT18, FNWL18,
HZL18, HZW18, HYS18, HKH13,
JSMG18, LCL+15, LFZ+17, LFWS15,
LYL15, LJ+17, LJYW18, LDZW19,
Nam19, QRW+18, RD17, XWS17, YCT15,
ZWM14, ZML17]. Attribute-Based
[AAC+16, BFK+10, Boy13, CD16, FHR14,
GZZ+13, GSW+16, GVW15, HSMY12,
LW11b, LW11c, LW12, LJL12, LY+13,
LHL+14, LAL+15, LHL15, LW16, PB12,
RV+16, Rao17, SSW12, TYM+17,
WDC18, WLH15, XML13, XWL16,
XHY+17, ZP+15, ZQQ+15, ZM17,
AHL+12, CD18, Her14, WHL16, CPPT18,
HZ18, HYS18, HKH13, JSMG18,
LCL+15, LFZ+17, LFWS15, LYL15,
LJ+17, LJYW18, LDZW19, Nam19,
QRW+18, RD17, XWS17, YCT15, ZWM14,
ZML17]. Attribute-Hiding
[OT12, ZWM14]. Attributes
[CGI2a, Yon11, LCL+17a]. Attribution
[XHC+12, FNP+15]. Auction
[Con10, HJM+11]. auctions [MR14c, QS18].
Audience [DTE17]. Audio [Ber18, DA12,
FM15, GCK12, HGT15, KD12a, KD12b,
LSL12b, NXH+17, TC10, gWpNy+14,
XNG+14, XNRG15, XNP+18, ZS12,
LSQ11a, SKEG14, yWpNy11, YQH12].
Audit [YNR12b]. Auditing
[LMD16, TCN+17, YYS+16, YXA+16].
August [ABI10a, JY14, MV12, Rab10].
Austin [IEE13]. Authentic
[HTL+15, SZM13]. Authenticate [HM12].
Authenticated [Alo12, BCO13, BDMLN16,
CLL16, CLY14, CCS14, CRE+12, DS11,
EAA12, ES12, FVS17, FFL12, GTT11,
GL12, GZ12, HC12, HL10a, HCL+14,
HEC+12, KMY18, LHKR10, LY16, LH11b,
LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHKS14, MSU13, PTT16, Sar10b, Smi11b, Tan11, TW14, XLM+12, XHC+12, XGLM14, XZLW15, YS12, YLW13, YRT+16, Von12, ZPZ+16, ZXH16, AIB+16, CTL13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HWB12, HL11, HPY10, ISC+16, KMTG12, LWS10, LHH11, LML+13, NCL13, Nos11, Nos14, PPTT15, PJ18, SMBA10, TCS14, Tso13, TKHK14, WZM12a, WZM12b, WTT12, XWXC14, XCL13, XWZ+18, YC12, YZZ+14, YZL+18, ZTZ16, ZXWA18, ZG10, ZZC15].

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

**Authentication** [ASO14, AAZ+16, ACAT+15, AUMT16, ABB19, BL12, BCE+12, BCM12, BSSV12, Bel18, BKST18, BFD+12, Bis17, BF11, Boy16, BKJP12, BSV12, CGCGPDG12, CTC+15, CC14, CSH+18, CCW+10, CCF17, CJ13, CD12, CJ12, CLH13, DL15, DCM18, DBPS12, DP12, FLH13, FR16, FMTR12, FD11, GH14, Gl12, GI12, GM14, GU13, GMV17, GCK12, HZC+12, Hs12, HLC11, Har13, Hay13, HBC13, HM10, HCP12, HCTPL+12, HKL+12, HXC+11, HLC11, HRK18, IGX+16, J12, JCM12, Jia17, JAE10, KP12, KS18, KR1+10, KSD+17, KPC+11, KLY+12, KTA12, KPG12, Kim15, KPKS12, KLM+12, KO16, KH10, LLC11, LH12, LLG15, LCLL15, LN12+13, LZCK14, LNX15, LLZ+12, MWZ12, MEOF12, MKH+12, MBC15, MRR17, MRS+17, May15, MLBL12, Mor12, MSKR17, MPK+17, NR11, NR12, NLLJ12, NLY15, OdH12, OQ12, OS12, PCD14].

**Authentication** [PPRT12, PTT12, PWVT12, RS11, RWL14, RSN14, SG18, Saa12a, SBS+12, Sar12, SG16, Sch15b, SKV12, ST14, SM12, SD12, Sh11, SG14, SSA13, SC12, SCMS18, SZDL14, SHS12, SAA12b, SRK+17, TGC16, TYK+12, TM12, Vet10, WgMdZIZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WT10b, Xio12, YPT11, YFT17, ZBR11, ZHW+16, ZWZ17, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, Aia15, AL15, AHM+18, APK+18, Alp18, AIK1C18, ACF16, AFD+12, ATI+10, AN15, ACM12, BS13a, BDM18, BCM13, BGAD12, BLAX+16, BAL10, BMM12, BvOS15, BT18, BTW15, BM11, CLM+12, CML+18, CLP+13b, CTL12, CJXX19, CSD18, CH10, CCW11, CHS11, CLH13, CZ15a, Chi13a, CP15, Cho14, CL11, DCA12, DCS12, DLK+16, DMV15, DLN13, DZS+12, DIMT12, uHAN+18, EA12, ED19, EA11, FPBG14, FHH10a, FLL+14, FXP12, Far14].

**authentication** [PPRT12, PDT12, PWVT12, RS11, RWL14, RSN14, SG18, Saa12a, SBS+12, Sar12, SG16, Sch15b, SKV12, ST14, SM12, SD12, Sh11, SG14, SSA13, SC12, SCMS18, SZDL14, SHS12, SAA12b, SRK+17, TGC16, TYK+12, TM12, Vet10, WgMdZIZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WT10b, Xio12, YPT11, YFT17, ZBR11, ZHW+16, ZWZ17, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, Aia15, AL15, AHM+18, APK+18, Alp18, AIK1C18, ACF16, AFD+12, ATI+10, AN15, ACM12, BS13a, BDM18, BCM13, BGAD12, BLAX+16, BAL10, BMM12, BvOS15, BT18, BTW15, BM11, CLM+12, CML+18, CLP+13b, CTL12, CJXX19, CSD18, CH10, CCW11, CHS11, CLH13, CZ15a, Chi13a, CP15, Cho14, CL11, DCA12, DCS12, DLK+16, DMV15, DLN13, DZS+12, DIMT12, uHAN+18, EA12, ED19, EA11, FPBG14, FHH10a, FLL+14, FXP12, Far14].
XMHD13, XHM14, YHL16, YHHS16, YWK+10a, YSL+10, YMM13, YD17, ZYL+10, ZQZW10, ZCLL14, ZHH+17, ZX11, ZLY+19, ZSL+18, OHJ10.

authentication-chaining [EA11].
authenticators [SYY+17]. authenticity [ADF12]. Authority [LNXY15, XZLW15, ZQQ15, JB11, ZZ12].
Authorization [CS14, LGMC17, MPM+17, YKK18, AL15, DFJ+17, JAE10, JAS11]. Authorized [HTC+15, LLSW16]. Authorship [BTW15, BAG12, LCM+17].
Autoblocking [LLLH18, YH16]. Automata [CCD15, Gas13, dRSdlVC12, HBBRM+16, SS11, WOLS12].
automata-based [SS11]. Automated [CCK12, CCCK16, DRS16, GLLSN12, LGM+16, Ste15a, Tom16, YSS14, BJR+14, KKK+16]. Automatic [MMP19, WW12].
Automation [BGK12, DZS+18, IEE11a, KPP16]. Automotive [HK18, LMS16, MPM+17].
Autonomic [SEK+19]. Autonomous [MPA+18, BT18]. Auxiliary [DMS+16, DL12, GGH17, XXZ12, YCZY12].
Auxiliary-Input [XXZ12]. Availability [CK11, ADY12, CFVP16]. Available [Ano16d]. AVC [JSZS12, JHHN12, LW13c].
average [Lim11, YL11]. avoid [CFZ+10].
Avoidance [RH+16]. avoiding [BHCdFR12]. AVR [LPO+17]. award [Ano16g, Orm16]. Aware [BCF16, LMMH14, LMS16, QLD17, YTH17, GHD19, MGP10, TODQ18, Wan13, ZFH+18].
Awareness [MSas12, Li10, MSas13].
axiomatic [AT10]. Azure [Sti19].
B [Tan12a]. B-Spline [Tan12a]. Back [KRM+10, SKS+18, YZLC12, Ran10].
Backdoor [Sch13, Fel13]. Backside [DDR+16]. Backup [MPA+18, Cor14a].
Ballots [CW12b, LHF12]. balls [Svo14]. band [Ano16c]. Bandwidth [GTT13, NR11, LLY+12].
Based [ADM12, AGW15, ASM12, AAC+16, ABC17, ANo11a, AYS15, BWLA16, BL12, BDB+16a, BSSV12, BHG12, BKPU12, BRT12, BHH+15, BS13b, BFK+10, Bon12, BS15, BVF19, Boy13, BKJP12, BDH11, BCF+14, CMLS15, CLL16, CGMO14, CMM17, CSH+18, CZLC12a, CZLC12b, CHLC12, CCZC13, CLY14, CCZC14, CST+17, CGL+12, CDD13, CGY+13, CD12, Ch12, CK18, CD16, DSSM14, DS19, DA12, DLZ+16b, EM12, EKB+16, FM15, FHH10b, FHR14, FVT14, FG10, FSM17, FSX12b, FSX12a, GWCC15, GZZ+13, GSW+16, GV14b, GI12, GY13, GDC16, GVW15, GJJ15, GJZ17, HZC+12, HSMY12, HSM14, HL10a, HX15, HPCLS12, HIK+12, HG12, HMR12, HSA14, HPO+15, HKR+18, HTG15, HCL+14, HLN+10, Hul13, HRS16, HBG+17, HEC+12, HM19, HP12, JTH+16, JHHN12, JE15, JKH+Y12, KS18, KZG10, KK12, KKA15, Kha10, KLY+12, KSSY12, KPP12, KR12].
Based [KAK18, KS15, LGMC17, LMMG+18, LTGP16, LSL12a, LSL12b, LW11b, LW11c, LW12, LH12, LJLC12, LYZ+13, LHL+14, LTH+15, LLC+15, LTH16, LLZ+17, LHH18, LPL15, LSW15, LAL+15, LH11b, Lin15, LP12, LNZ+13, LCC13, LWCJ14, LNX15, LH15, LW16, LPO+17, LGPRH14, LDB+15, LD13, LSC12, LBR12, LHH18, MWZ12, MLO17, MEFO12, MCDB12, MVV12, MD12b, MBC15, M013, MZ17b, MCS+15, MMS17b, MKF+16, MCF17, Men13a, MST18, Mor12, MSKR17,
MKAA17, Muf16, NC12, NXH+17, NXB13, NLLJ12, NLY15, pNyWyY+14, OTD10, PB12, PTT16, PYM+15, PDNH15, PPS12b, PYS18, PG12, PAS13b, PNRC17, QC+18, RVI+16, RSR+19, RZZ+15, RS16, Rao17, RR11, RDZ+16, RVRSCM12, RW12, SSW12, Sar18a, SS13, Sen17, SJ12, SGF+12, SPG+19, SP15b, SSA13, SRAA17, SH15, SGH15, TB18, TKR14, TW12, TZW12, TYM+17, TSH17, TT12, TTH15].

Based [TC10, VDB+16, VGA15, Vle12, WY10, Wan10, WSSO12, WgMW12, WYW+13, Wan14, WZCC18, yWXY+18, WDC18, WHL15, WCL+18, WT10b, WMS+12, XNG+14, XNRG15, XXZ12, XMLC13, XQL11, Xio12, XGLM14, XWLJ16, XJW+16, XJR+17, XHZ+17, YEI12, YZLC12, YZX+12, YGFL15, YTS12, Ye10, Ye14, YH16, YTH17, YYO15, Y+17, YKNS12, YHK+10, YMWS11, YKC+11, YFK+12, YCZY12, ZSP+19, ZPM+15, ZJ11, ZXZ+11, ZDL12, ZLH+12, ZQQ15, ZMW16, ZXYL16, ZM17, ZPW16, ZHW15, ZVG16, ZPZX17, ZY18, ZHL15, AMN18, AGL16, AaBT16, AY14a, AHS14, AAT16, AA14, ASO14, AIA+18, AKG13, ASVE13, Ara13, ATI+10, AHL+12, BS15, BDM18, BBBP13, BGAD12, BAAS13, BOB13, BWR12, BW13, BWA13, BMM12, BC18, BBBI16b, BK12b, CPPT18, CML+18, CFL13, CFY+10, CCLL11, CTL12, CSLW12, CG12b, CSZ+11, CHX13, CSS+13, CW14a, CTPH13, CJP12, CJP15, CG10, CTL13].

Based [Cho14, Con12, dCCSM+12, Cra11, CDL18, DSSC12, DZ14, DNL13, Dra16, uHAN+18, EZ15, FHI3, Far14, FA14a, FA14b, FIO15, Fay16, FHZW18, FNNW18, Gal13, GJ13, GMG015, GMRT+15, GKC11, GJMP15, GCSAdP11, GSM11, GLL+18, HSH11, HT11, Ham19, HGWW11, HSM13, HZC+14, HHZ18, HF14a, HWDL16, HZZ+17, HZZW18, HBBRNM+16, HLR11, Her14, HWB12, HB13, HLI14, HL11, HLC12, HLC16, HYWS11, HYS18, HYF18, HYR+10, HHK13, HCC10, Hwa11, IMB17, IM14, ISC+16, IB11, IA15, IOV+18, Jac16, JNUH17, JKAU19, JK13, JLT+12, JZS+10, JMW+16, JSMG18, KP16, KK13, KM10a, KMB13, KKG14, Kim11, GKO10, KL11, KSH18, LXYL12, LLZ+16, Lau12, LLC10, LK14, LH10c, LZJX10, LNM+11, LMJC11, LK12, LXMW12, LKAT12, LLS12, LNK13, LJX14, LCL+15, LZY+16, LFZ+17, LNK+18a, LW18+17, LCT+14, LFWS15, LLM+19, LPdS10, Lin14a, LLY+12a, LW10, LSQ11a, LSQ11b].

Based [LWK11, LW13b, LZC14, LPZ15, LTC+15a, LYL15, LY15, LJW+17, LJYW18, LDZW19, LWW+10, LL16a, LW13c, LWY12, LY14, MCN+18, MCP15, MJGS12, MS13, MLM16, MMZ12, MM13, Mes15, MBB11, MO14, MHT+13, MG15, MS17, Nam19, NR11, NCL13, NZL+15, PPA18, PYH+18, PLPW13, PTK14, PW10, PGLL10, PPB16, PLGMcFD18, PS14, PL16, PKA15, PC14, PR+12, QZDJ16, QRW+18, QYWX16, QMW17, RD17, RG10, RS15, SPLHCB14, SGGCR+16, SH12, SYL13, SE14, SE16, SH11, SM11, SNM14, SR10, hSZ15, SCKH10, SA16b, SAAF11, SWW+16, SSS11, SKEG14, Sun16, SGM16, SHBC19, SS11, SPL16, TQL+14, Tia15, TH16, TTT10, TPKT12, TKHK14, VS11, VN17, WWYZ11, WWWY11, WLD11, WLFX17, WMX+17, Wan18, WGW+12, WHLH16, WS14, WS12, WTT12, WOLS12, WCCH18, XHH12, XZW16, WX12, XCL13, XWS17, XHCH14, XWZ+18, XMHD13, XHM14, YWL+17].

Based [yYqWqZC13, Yan14, YTM+14, YCC16, YXA+18, YCT15, YLS12, YMSH10, YKC+12, YLZ+16, YXA+16, YLI11, ZZKA17, ZZW+12, ZCLL14, ZT14, ZT16, ZML17, ZZ12, ZHH+17, ZL12, ZHV14, ZDW+16, ZLY+19, LZJX10, HZC+14, MM12, PP11, ZBR11, Kat13].

Based-Encryption [ZHW15].

Bases [EVP10, TSH14, FES10].

Basing [Mat14, MN10].

Basis
[CLHC12, KHHH14]. **Block** [AMVZ12, BRS17, BSS13, BFMT16, BDGH15, BCG+12b, CWP12, DWWZ12, EGG12, FXP17, GLLSN12, GT12, GST12, GNLI2, IS12, KR11, KWS12, LWZ12, LJ17, LCLW17, LGLL12, LWKP12, LWP12, MCD12, MRTV12, OGK15, PH12a, PRC12, Pud12, SGP12, SSA13, WW12, YCL17, ZSW12, BNY14, Jeo13, KM11, LPZJ15, LC13, LYHH14, LWKP14, MNP12, MHV15, MXY18, PL16, Sar11, SKK10, TQL14, Tan17a, WB12, WWBC14, ZSW18a, BNY14, Jeo13, KM11, LPZJ15, LC13, LYHH14, LWKP14, MNP12, MHV15, MXY18, PL16, Sar11, SKK10, TQL14, Tan17a, WB12, WWBC14, ZSW18a, JKP12]. **Block-Parallel** [MCDB12]. **Block-Wise** [SSA13]. **Blockchain** [Ano19b, Hur16, KV19, KV19, Scr18, SJZG19]. **Blockchain-Based** [KV19]. **Blockchain-Enabled** [KV19]. **blockcipher** [CMMS17]. **Blockciphers** [LST12]. **Blocks** [JSK17, Bra15]. **Bloom** [ATKH17]. **Blowfish** [KB10]. **BLS** [BP18]. **BlueKrypt** [Gir15]. **Boardroom** [LHF12]. **Bodacious** [KM10c]. **Body** [LZCK14, ASO14, KP18, LK17, SGJ18, body-sensor [ASO14]. **bogus** [XWDN12]. **Bombe** [Bur11, Car10]. **Bonebrake** [SS10c]. **Boneh** [TK19]. **Book** [Ano15b, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kobi10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12]. **Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LVV11, WT13, YCC16, ZZQ19]. **Boolean-based** [CW14a, YCC16]. **Bootstrapping** [BVG14, GM14]. **Border** [LGM16, ZTSR12]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Bottom** [Sm11b]. **Bound** [LST12, TK19]. **Bounded** [GVW12, GJO+13, PDN15, QZZ18, SS12a, ZYT13, IM14, bounded in [PYH+18]. **Bounds** [Lia17, LJ15, SN11, SS10b, Sha10]. **Bouzefrane** [Ano15b]. **Box** [BW16, BCGN16, BR14, CPS16, HHP17, KMO14, Mic10b, Rja12, SS10b, KOS16, LRW13, MSas13, RMP10, SGFCRM+18, ZZ12, ZSW+18a]. **Boxes** [NN12, LJ15, SS11]. **Boyle** [Mat19]. **BRAMs** [DP10]. **Branch** [EPAG16]. **Branchless** [RBS+17]. **Brave** [KM10c]. **Brazil** [BA18]. **Breach** [SD12, JB11]. **Break** [Ayu12, Win17]. **Breakers** [Sti15, Mun17]. **Breaking** [AP13, CN12, Che18, Cop10a, RSMA19, TPL16, WgMdzlZ12, Ant14, Bri11]. **Breakthrough** [Goo12]. **Breath** [LSR13]. **Breathing** [CSH18]. **Breathing-Based** [CSH18]. **Bregman** [CCZC13]. **Bribery** [CW12b]. **Bridge** [BRW14, TMGP13]. **Briggs** [Bai12]. **Bring** [Zha15a]. **Bringing** [Ano15c, OYHSB14]. **Britain** [Ald11]. **British** [And13]. **Broadcast** [BS14, GMD14, HMR14, KHL10, LGMC17, LGQ+18, PSM17, PPS12a, WQZ16, XJW16, Yan14, ZHW15, CPPT18, DLN13, WWYY11, XWDN12, YMM13, ZWQ+11, ZZ12, Zha13]. **Broadcasting** [OO12, MK11, OCG11, YY11]. **broke** [Bat10, Hea15]. **Broken** [MDAB10]. **Broker** [TKR14]. **Breaker-Less** [TKR14]. **browser** [GF12]. **Browsers** [FVJ19, Rec15]. **Bruce** [Sev16]. **Brute** [CJP12, JR14, CJP15]. **Brute-Force** [JR14, CJP12, CJP15]. **BRW** [CMR13]. **BTC** [CLF11, QJC18]. **BTC-compressed** [CLF11]. **Buchwald** [ABJ13]. **Bucket** [KKV10]. **Bug** [Ch13b]. **Building** [BPS16, KMP11, MJS13, Sev16, WL11, LCKBJ12]. **Burdens** [Lia12, SR14]. **Bus** [AN17]. **Business** [LDB15]. **Buyer** [Fra16, KJN16]. **Buyer-Friendly** [Fra16]. **BYOE** [Tan17a]. **byte** [Hof15, Hof16]. **Bytecode** [SEK19]. **bytes** [PBC14]. **Byzantine** [KS11, LKA19, YKGK13]. **Byzantine-resistant** [YKGK13]. **C** [AD12, ACZ16, Cra14, DGJN14]. **C1G2** [MK12a]. **CA** [ACM11, Dn12b, KIA11, Lin14b, Pie10, Rab10]. **CABA** [MSKJ17]. **CABE** [XHZ17]. **Cache** [AB15, ADR18, DKMR15, HLAZ15, SY15a, DLJ+12, DK17].
Challenges [CN12, FS15, Fra15, LLGJ16, MRS+17, PCY+17, SBV14, ALL+18, KJN+16, WS14].

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

Channel
[AN17, ASN11, CDK+10, CBL13, DZS+18, EWS14, GWM16, GPT14, HLH19, KOP12, LG14, NDC+13, PRC12, SG15, TT12, YL17, ZBF18, ADG16, BV12, CPPT18, DMWS12, DJL+12, JLT+12, MFH13].

Channels [ASN12, BGN17, DKMR15, EPAG16, KW14, SS19, Vua10, AGH+17, CL16, DMV15, DKL+16, IWMG10, NR11, SRB+12, ZPZ+16].

Chaos [AIA+18, LW13c, RR11, RVRSC12, CPLL11, LW13b, jT12b, ZLW+12, SGFCRM+18].

chaos-and-Hamming [CCL11].

Chaos-Based [RR11, RVRSC12, AIA+18, LW13c]. Chaotic [BCGH11, IAD10, LFX+18, Ye10, GCH15, ISC+16, KLW+16, LWK+18, LW10, NES+14, WGZ+12, ZT14].

Chapman [Ful10]. Character [SS12b]. Characteristic [BGJT14, SR10, ZW17, BGJT13, Jou13].

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

Characterizing [Ash14, JR13, MPJ+16].

Chattarjee [Kat13], cheat [WS12].

cheat-preventing [WS12]. Cheater
[KI11, Oba11]. Chebyshev [LPdS10].

Check [GST12]. Check-before-Output [GST12]. Checkability [LHL+14].


Chosen-Ciphertext
[RS10, FSGW12, LCT+14, GH12, LSC14].

Church [ABJ13]. CHURNs [RBNB15].

Cipher
[BW16, BFMT16, BCG+12b, CMLMS15, CGCS12, DM18, DG12, DWW12, Fis15, FXP+17, GLLS12, GCS+13, HZ11, Hey17, IOM12, JKP12, KL11, KWS+12, LPS12, LW12, LJ17, LWKP12, LWPF12, MRT12, MHC12, MS12b, OKG+15, PH12a, PRC12, WSS12, WHN+12, YCL17, ZAG19, AMS+10, BNY14, CR12, FVK17, HKT11, Hol12, Jeo13, KDH15, Lew10, LC13, LHYH14, LWKP14, MNP12, PL16, Rec15, RS14, Sar11, WYL14, WWBC14, ZSW+18, LGL+12].

Ciphers [ABS+12, BMS12, BSS+13, BKLS12, Bru12, CWP12, DGIS12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNL12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCLW17, LGLL12, LJ16, MD12b, NN12, Pud12, Sas12, SEHK12, Vua10, WH18, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KM10a, LW11, MRT10, MH15, MHY+18, QGG13, SKK10, TQL+14, WB12].

Ciphertext [BDPS12, CWW12, zGXW12, HL12, JMG+16, JSM18, KA17, LSC12a, LLML12, MH14, PDN15, PPS12b, Rao17, RW12, RS10, SSW12, SR12, WH12, XML13, XMLJ16, ZHW12, CPPT18, FSGW12, GLM+16, GH12, HP10, HHK13, KTT12, LCT+14, LFS15, LSC14, LDZW12, QRM+18, RD17, SGM16, WFLX17, XWS17, LAL+15, LHL15].

Ciphertext-only [KA17].

Ciphertext-Policy
[Rao17, XMLC13, XWLJ16, ZHW15, JSM18, LFWS15, LDZW12, QRM+18, XWS17, LAL+15, LHL15]. Ciphertexts
[LLPY19, Sta12, WQZ+16, AHI+12, LCT+14, NMP+13, WXLY16]. Circle
Circuit [Kar12, MTY11, XWS17, XWLI16, Lui12, MS13a].  
Circuit-Size [MTY11].  
Circuits [AIK14, AS17, GGH+16a, GH11a, GVW15, MFB18, SS10b, SS12a].  
circumstance [ZLY+19].  
Circumventing [BAG12].  
CISSP [STC11].  
Citizen [Ano16d].  
City [Ano17d, GA18, LNK+18a].  
Claims [SKGY14].  
Class [BCG12a, SY15a, XYXYX11, BJ16, Goo12, KK10].  
Classes [ACZ16].  
Classical [DSLB18, JE15, MSU13, SSU12, CR12, RK11].  
Classification [HPC10, HS18, KAHKB17, SGP+12, ZLW+17, LHL+18].  
Classifiers [KGV16, LCM+17].  
Classroom [Pow14].  
Claudius [Hol12].  
CLEFIA [LWZ12, TSLL11, TS16a, WB12].  
CLEFIA-128 [TSLL11].  
CLEFIA-type [WB12].  
Client [ASM12, CTC+15, FD11, RAZS15, Vlc12, FA14a, FA14b, hSZ15, WT10a].  
Client-Based [ASM12].  
Client-Centric [Vlc12].  
cloud [XWY+18, YYS+16, YZCT17, YHHM18, YQL17, YWT+12, ZYC+17, ZVH14, ZDW+16, ZWS+18, ZHY+18, ZLY+19, ZHT16].  
Cloud-aided [SGJ+18, WLFX17].  
Cloud-Based [KS18, SRAA17, ASO14, BK12b, WCH18].  
Cloud-Manager-Based [KKA15].  
Cloud-of-Clouds [BCQ+13].  
Cloudier [CFE16].  
Clouds [BCQ+13, HLC+18, RSN14, HFT16, IC17, JKL+16, LFWS15, LL16a, Wu17, YNX+16].  
Clustered [DS11, KS18].  
Clustering [KRDH13, VS15].  
CMAC [SKK10].  
Co [MBR15, MRL+18].  
Co-Design [MRL+18].  
Co-Processor [MBR15].  
coal [KO16].  
cocktail [OHJ10].  
Code [AD12, Bud16, CCL+13, Cop10a, Fox13, HG12, KSS12, Mun17, PYM+13, SS13, Sen17, Sti15, War11, ABBD13, Ant14, Bha16, Bri11, CLLL11, GIJ+12, MCP15, McG11, McK12, Moo14, OF11, PA10, Wes15].  
Code-Based [HG12, SS13, Sen17, MCP15].  
code-breaking [Ant14, Bri11].  
Code-cracking [War11].  
Codebreakers [An11c, Bud16, Maf16, McK12, Smi11a].  
Codebreaking [Bai12, RS18, Cop10b, McK10, McK11].  
Coded [She14].  
Codes [Ano19a, BBC+13, Bay10, BKST18, DBPS12, DPW18, FMNV14, GMNS15, Giri15, HC17, KW14, MBR15, ODT10, SEY14, ST14, TLW12, WGF16, WSS12, Xie12, YTP11, Yek10, ATI+10, Bu10a, CZ15a, Chi13a, Fag17, Hea13, LTT10, MG15, ÖS11, Tan15b, YJS14, Ayu12, Low12].  
Code-development [DF16].  
Coding [Che11, CWL16, CJ13, CG14a, DG17, Hes12,
MAL10, PMZ13, PP10b, TCN\textsuperscript{+17}, WHZ12, ZSP\textsuperscript{+19}, Ara13, CMMS17, DTZZ12, LK14, Li10, LPZJ15, PP11, QZ14, RSMA19, SI12]. compression-based [SI12]. Compression/Decompression [PP10b]. 

Compression [CCZC13]. Compromise [YNR12b, GBNM11, PX13]. Compromised [DSSDW14, ZYL\textsuperscript{+10}]. Compromising [BC14]. Compromise [YNR12b, GBNM11, PX13]. Compromised [DSSDW14, ZYL\textsuperscript{+10}]. Compromising [BC14]. Compulsory [QRW\textsuperscript{+18}]. Comput [HYS18]. Computability [Gas13]. Computable [LGH\textsuperscript{+17}, FWS13]. Computation [ARH14, Ash14, Bee17, BDOZ11, Fri10b, GST12, GVW12, GHKL11, HP14, HC17, IEE11a, Jin10, KW14, KMO14, LHM\textsuperscript{+15}, LQD\textsuperscript{+16}, MMP14, Mal13, NSMS14, PST13, SVVCV15, SQZ\textsuperscript{+17}, TM18, Wat10, ABDP15, AB10b, BHH19, LDDAM12, PHGR16, TG12, vDKS11]. Computational [BCO13, GKS17, RD17, TBCB15, HRS13, SDM14]. Computations [ARM15, CK18, KHP116, Nac16, ADM116, BK12, LR15, SSA111, TLMM13]. 

Comput [Vai12]. Computer [BGK12, BCGK12, BGB12, BDD19, Bul10b, DF16, Gas13, IEE10, IEE11b, IEE13, LL15,Orm16, Ter11, Vua10, ABB13, DK12, FPGP14, PHWM10, Stai1b]. 

Computer-Aided [BGK12, BCGK12, BGB12, ABB13]. Computers [Mos18, Cop10b, LCKBJ12, Mac12, Mvo11, PHWH10]. Computing [ACM10, ACM11, AJA16, Aoo17e, BCG\textsuperscript{+12b}, Cer14, CGB\textsuperscript{+10}, DXA14, EAA12, FES10, Gen10, KMSM15, KP17, LCK11, LT14a, LYZ\textsuperscript{+13}, LLC\textsuperscript{+10}, LLGJ16, LNX15, MLO17, OS16, PAF18, Pet12, RS18, SJWH\textsuperscript{+17}, SLMO10, Vai11, Vcl12, XMLC13, XWL16, YE12, YHL16, ZLDC15, AaBT16, AAZ\textsuperscript{+16}, And13, CZI5b, CSTR16, DLK\textsuperscript{+16}, DWZ12, HSM13, HYS18, Jea13, JSMG18, KKA14, KKM\textsuperscript{+13}, KKM\textsuperscript{+14}, KSB\textsuperscript{+17}, KH18, LKX\textsuperscript{+14}, LYL15, LHL15, MS12a, NR17, Nam19, NCCG13, PPA18, PP11, PPA15, QZDJ16, QR\textsuperscript{+18}, Rao17, Tan12b, WSC14, Wan18, WDKV19, WLS14, WL19, XXX15, XWV\textsuperscript{+18}, YHHM18, YWK\textsuperscript{+10a}, YQL17, YY11, ZWS\textsuperscript{+18}, ZLY\textsuperscript{+19}, ZSW\textsuperscript{+18b}, YXA\textsuperscript{+18}]. conceal [EEAZ13]. Concept [TMC15]. Conceptual [PMZ12, SPM\textsuperscript{+13}, TSH14]. Concrete [BS14]. Concurrent [CLP13a, FCM14, GJO\textsuperscript{+13}, MKRM10, OOR\textsuperscript{+14}, AKG13, SRB\textsuperscript{+12}, X LW16]. condition [TD14]. Conditional [HBCC13, KPW13, LLG15, LSLW15, MLO17, XJW\textsuperscript{+16}, FSGW11, FSGW12, HWDL16, HYF18, IOV\textsuperscript{+18}, LCT\textsuperscript{+14}, PZBF18, SKB\textsuperscript{+17}, Tan12b]. Conditionally [ZJ14]. Conditions [Ano17d]. Conference [BC11, CGB\textsuperscript{+10}, Che11, Cra12, Dan12, Dun12b, FB12, GLIC10, IEE11a, JY14, LCK11, LW11a, LNW11, Lin14b, PJ12, SNJ11, Sah13, Yan10, AB10a, Abe10, BYL10, BL10, Gil10, GG10, HWG10, Kia11, LH10a, Pie10, Rab10, vDKS11]. Confidential [HS11, AZPC14]. 

KHPP16, KMO14, LP11, Pan14, ZMW16, AHL+12, DWZ12, LCT+14, SGM16.

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

**constants** [DWZ12]. **Constrained**
[BSJ15, CSH+18, EAA12, JMG+16, YNR12a, Yon12, DMV15, KAS15, LLZ+16, LCL+17a]. **Constraints**
[CKKM16]. **Construct**
[SGY11, WT13]. **Constructed**
[Ye10, ZH15]. **Constructing**
[CDSLY14, ZSW+12, HRV10]. **Construction**
[BWLA16, DF11, EM12, FZT14, GWWC15, HHP17, KMO14, MSas12, Rog16, Sar10b, ST14, WZ15, WCL+18, WMS+12, XHX+17, LFZ+17, MSas13, SA14, YWL+17, YT11b, YKC+12, ZCLL14]. **Constructions**
[BCF+14, DQFL12, HL10b, KOTY17, SNJ11, SES+16, CZ15a, CGKO11, NAL17, Zim10]. **Constructive**
[Mau12, WB12]. **constructs** [BP10]. **Containing**
[XWDN12]. **contemporaries** [LCKBJ12]. **Contemporary** [Opp11]. **Content**
[ADR18, BCP14a, MHT+13, PMZ13, PZPS15, WHZ12, WZXL12, YT12, XXZ+11, GPN+12]. **Content-based** [MHT+13]. **contents** [MSM+18b, SKS+18]. **contest** [Cra14]. **Contests**
[WXY+17]. **Context**
[Fra16, ZCSW15]. **contextual** [Svo14]. **Continual**
[BKKV10, XZY+12, YZ12, YCZY12]. **Continual-Leakage** [YZ12]. **Continually**
[DLWV11]. **Continuous** [ACAT+15, BCF16, DLHLAW10, uHAN+18, FMVN14, MSKRJ17, PYP10, Sch15b, SRT12, Yam12, ZY17a, ZYM18, BTW15, PLGMCdF18]. **Continuous-Tone** [Yam12]. **Contract**
[MMP19, Men13b]. **contrast** [DDD14, GLW13, LXL10a, MM14a]. **Contributory**
[WQZ+16]. **Control**
[ATS15, BFK+10, DLZ+16b, HHS+15, HLC+18, LGM+16, LGLK17, MM17, MK12b, NA10b, QZL+16a, RSN14, SGC14, TBCB15, XMLC13, YTH17, ACK+10, AMHJ10, CLH+16, CO11, Cra11, FNWLI8, FS18, GHD19, JAS+11, LCL+17a, LCL+15, NZM10, QCX18, Sch15c, SA15, Tan12b, Wan18, XHH12, ZML17, ZVH14, ZWS+18, ZFH+18, ZZL+18]. **Controllable**
[FH13, ZLDC15, ZHT16]. **Controlled**
[FMTR12, WP17, Har16]. **Controller**
[GMVV17]. **Controllers** [AMH+16]. **controls** [CGH11]. **controvery** [McG11]. **conundrum** [Eve12]. **Conversations**
[WBC+10]. **Converse** [KPKS12]. **Conversion** [BJ10]. **Convertible**
[CLL16, LH11b, HL11, LHH11, XWSC14]. **Convolution** [DWZ18]. **convolutional** [MG15]. **Cookie** [FVJ19]. **cookies** [DCAT12]. **Cooperative**
[LLZ+12, SJWH+17, ZLDC15, WQZ+13]. **Coordinate** [YKK18]. **Coppersmith**
[Dra16]. **coprocessor** [ABC+12, BGG+13, IBM13b]. **coprocessors** [GCVR17]. **Copy**
[BT12, MHT+13]. **Copyright** [SJ12, GJ13]. **Core** [LB13, YWF18, YS15, RS17, HLYS14]. **Cores** [MGG+19]. **cornerstone** [Tan17b]. **Correct**
[PST13, Lan11]. **CorrectDB** [BS13a]. **correcting** [AT1+10, LT10, MCP15]. **Correction**
[LSC+15, yWXY+18, Chi13a, Sun16]. **Correctness** [YGS+17, WS13]. **Correlated**
[RS10, Jia16, ZPZ+16]. **Correlation**
[BW12, FFA+18, LD13, SDM+12, WWBC14, XHH12, YCL17]. **correlations** [Sar14]. **Correspondence** [SY14]. **corresponding** [DWZ12]. **Corrigendum**
[HYS18, WZM12a]. **cosmography** [Pet11]. **Cost** [ABC+17, AMH+16, CML15, CJP12, GI12, HLT+15, Man13, NVM+17, WMX+17, CZ14, CJP15, LEW19, Sar10a, YL11]. **Cost-effective** [HLT+15, WMX+17]. **Costas** [TRD11]. **Costs** [KHP16]. **couldn't** [Bha16]. **Countdown** [Zet14]. **Counter**
[ARP12, KMJ18, Fay16]. **Counterexample** [KPW13]. **Counterfeit**
[ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, Ano19a, App14, AAB17, ACM17, ARM15, Bar12, BGK12, Bar15, BRT12, BCGN16, Bon12, BF19, BKKV10, BJ10, Buc10, BLM17, BLM18, BCF+14, CNR14, CT18, CJFH14, Cas10, CGMO14, Che17, CST+17, CFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, FHLD19, Feh10, FSK10, Fid18, FBM12, Fre10, GO17, GFBF12, G13, GPT12, GLW12, Ham17, Hes12, HG12, HKR+18, JS18, JT12a, KM10c, KP10, KAK18, LSL12a, Lin17, LWL10b, LGYW12, LMHH14, LGH+17, LWHS17, LPO+17, MO12, MS10, Mau12, Men13a, MR14c, Mic10b, MST18, MV12, MM17, NNA10, NS12, Orm16, PP10a, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16, Sch18, Sen10, SS13]. Cryptography [Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16, Sta11a, Ste15a, VS16, WWL+14, WY12, Wes16, Yan12, Yan11, YTS12, YL17, ZZCJ14, ZAC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBD13, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Böi12, BSR+14, BS12, BBB16b, CFR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSL14, DDD14, Dav11, D13, Dur15, Far14, GCVR17, Har15, HH15, HZW17, Hof16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Li1112, LY14, MCN+18, MS13b, MDD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSAF11, Sta11b, Stil11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA+18, YDH+15]. Cryptology [BC11, Bro11, Dun12b, LW11a, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPGP14, Gil10, GG10, Kia11, LH10a, MZ17a, Pal16, Pie10, Rab10, HWG10, LT11, Kob10]. Cryptomania [Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16, Sta11a, Ste15a, VS16, WWL+14, WY12, Wes16, Yan12, Yan11, YTS12, YL17, ZZCJ14, ZAC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBD13, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Böi12, BSR+14, BS12, BBB16b, CFR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSL14, DDD14, Dav11, D13, Dur15, Far14, GCVR17, Har15, HH15, HZW17, Hof16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Li1112, LY14, MCN+18, MS13b, MDD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSAF11, Sta11b, Stil11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA+18, YDH+15]. cryptography [YR11, ZWX+18, vDKS11, Che11, LZJX10, Nac12, Cou12, Full10, Gas13, Low12, Mei10, Mur10, Ter11]. cryptography-based [BOB13]. Cryptography-Related [Cil11]. Cryptology [BC11, Bro11, Dun12b, LW11a, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPGP14, Gil10, GG10, Kia11, LH10a, MZ17a, Pal16, Pie10, Rab10, HWG10, LT11, Kob10]. Cryptomania [Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16, Sta11a, Ste15a, VS16, WWL+14, WY12, Wes16, Yan12, Yan11, YTS12, YL17, ZZCJ14, ZAC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBD13, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Böi12, BSR+14, BS12, BBB16b, CFR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSL14, DDD14, Dav11, D13, Dur15, Far14, GCVR17, Har15, HH15, HZW17, Hof16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Li1112, LY14, MCN+18, MS13b, MDD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSAF11, Sta11b, Stil11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA+18, YDH+15]. cryptography [YR11, ZWX+18, vDKS11, Che11, LZJX10, Nac12, Cou12, Full10, Gas13, Low12, Mei10, Mur10, Ter11]. cryptography [YR11, ZWX+18, vDKS11, Che11, LZJX10, Nac12, Cou12, Full10, Gas13, Low12, Mei10, Mur10, Ter11].

Dash [KCC17]. Data [Ano13c, ADL12, Bar12, BJL16, BCD+12, BJL12, BW12, BKL18, CWL+14, CMLS15, CCW+10, CSV15, CNT+14, CLW16, DDS12, Dan12, DR12, DK16a, DMS+16, DA12, DCA18, DLZ+16b, EKB+16, FMY15, FP15, FRS+16, GTT11, HSM14, HLC+18, HLT+15, HK14, IBM13a, KRD13, KGV16, LLP19, LLZ+17, LWCJ14, LLZ+12, LZO+12b, MLO17, Mal13, MMS17b, MM14b, NNM10, NR12, PD14, PSM17, PBC+17, PH12b, PNR17, QZL+16a, QZ18, RCP+18, Rea16, RS14, SGG18, SAKM16, Sar10b, SMS18, SP15b, SKH17, Sia12, SL10, TCM+17, Tan15a, Vai12, V515, W2CC18, XNK15, XWSW16, YDY+16, YMC+17, XZYL16, ZPXX17, ZTL15, ZLW+17, AP10, AS14, Ana14, Ano11a, Ara13, ADH17, ALL+18, B119, B119, BTP15, BC18, B1V13, CDG12, C1H+16, C1F+10, CD18, DFJ+10, DTZ12, DRD11, ED17, F18, GHD19, Gen10, GLB+18, GZS+18, HSM13, HIK+15, HMK12, HHI6]. data [HYS18, HAY18, H1CC14, Kim16, KH18, K1W16, L1N14, LT14b, L1K+14, L1Z+16, L17b, L1H+18, LFS15, L1W+16, L1C17, L1L+18, L1L6a, L1H+16, M1K14, Nam19, O108, OSS16, Q1X18, Sch15c, SYY+17, SAR18b, S1Y+17, Tan17b, TMK11, T1M23, W1H13, W1L14, W1W13, W1S14, W1W19, XXX15, XVW+18, X1W+18, Y1S+16, Y1Q17, X1A+16, YNX+16, Z1K17, ZMM+10, Z1W+13, Z1H+16, Z2L+18, AEH17, HLYS14, Sch15c]. Data-Centric [DLZ+16b]. Data-Classifiers [KGV16]. Data-Compression [DA12]. Data-Minimizing [BCD+12]. Data-Oriented [NN10]. Database [BTHJ12, SBV14, W1L+18, BL11, JHC14, L1W13a, PRZ12, Suc12, YXD18].

Databases [FCM14, HC10, JKH12, K15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12].

datacenters [PRN+19]. Dataset [SP13].
datas [LV10].


Databases [FCM14, HP10, JKH12, K15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12].

Datacenters [PRN+19]. Dataset [SP13].

datas [LV10].


Databases [FCM14, HP10, JKH12, K15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12].

Datacenters [PRN+19]. Dataset [SP13].

datas [LV10].


Databases [FCM14, HP10, JKH12, K15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12].

Datacenters [PRN+19]. Dataset [SP13].

datas [LV10].

definition [LWL10a, WSC14, YKC+12]. Definitions [GLW12, Mau12, CGKO11, KM14, KGO10, XWXC14]. Degeneracy [WH18]. Degradation [MMS+17a].
Degree [KA18] degrees [MZ17a]. Delay [CCKM16, GMNS15, LFX+18, LBR12, JLT+12, XW13]. Delegatable [WZ11]. Delegated
[MZHY15, TMC15]. Delegation [FMTR12, SSW12, XWLJ16, YZ12, YAM+15, JSMG18, NAL17, XWS17, ZM14].
Demonstrating [HLC16]. Deniability [TCS14]. Deniable [DF11, zGXW12, HLLC11, HS11, Jia14b, JXLZ15, LXJ14].
Denial [Goo12]. Designer [KMY18]. Designing [CDK+10, DZS+18, FLW12, MRT10, PSD15, SR10]. Designs [BGK12, PCY+17, KDH15].
Detecting [BKBK14, Ess17, GAS+16, HLW12, KW14, SH15, YSC+15, LWLW11]. Detection [AMKA17, ATS15, CBO+18, DSB15, DF11, GZH17, HDWH12, KU14, LGL+12, LC15, MKRM10, MAKA17, NDC+13, NMS14, SAJ16, SBV14, SP15a, SRAA17, SG14, TM18, YFT17, AKKY17, AOT13, BM13, HB13, JC13, KLC+10, Maz13, MHT+13, WYL13].
Detective [Cho10]. Detector [LTKP16]. Detector-Based [LTKP16]. Determine [FSWF11, Sto12]. Determining
[NN12, Scr18]. Deterministic [MPRS12, NIS12, XXZ12, DTZZ12].
Deterring [WGJT10]. DEUCE [YNQ15]. develop [Ham19]. Developed [Har16].
Device [ABCL17, CFXY17, DFKC17, HSUS11, KLM+12, SRK+17, TYK+12, GM16, KKG14, Kim16, Par12b, SHBC19, VV19, XHH12].
Devices [AAC+16, CSY+18, DLWW11, EGG+12, GPT12, GdM16, GMSV14, HH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, WK16, WT10b, XJR+17, Aia15, CLP+13b, CFL13, CTL12, Chi13a, FRT13, GTSS19, IB11, KPP16, LKAT12, MvO11, MV15, OYHSB14, SHBC19, TG17, ZPZ+16]. DFA [WH17]. DFA-Resistant [WH17]. DFT [DDFR13]. DHA [AKY13]. DHA-256 [AKY13]. DHTs [YKGK13]. Diagram
Doesn’t [RS11, SS12a]. dog [Ran14]. Doing [JCM12]. Domain
[AGW15, BDFK12, BBM15, CLY14, DG17, LA15, MR16, PDMR12, SGY11, WLZL12, gWpNyY+14, AMK12, BGAD12, GJ13, IG11, LXCMI1, LPZJ15, LBR12, PWW10, QMC17, SCKH10, wWpWyYpN13, YZL+18, YWK+10a, YCM+13]. Domain-Specific
[BDFK12]. Domains
[LQD+16, LRWV14, KGO10, NES+14].
domination [GJMP15]. Don’t
[BCK17, FHV16]. Dopant [BRPB13].
Dopant-Level [BRPB13]. DoS-resistant
[HCC10]. dots [Li12]. Double [AK14, ARM15, Lin15, LEW19, PKTK12, Sas12].
Double-SP [Sas12]. Doubling [Zha12].
Doublly [CFZ12, CW14b]. Doubly-Spatial
[CFZ12]. Douglas [Ber16a]. Down
[Ano17e, McG11]. Download [ZGC16].
[SRK+17]. DRAMs [LSC+15]. DRBG
[YGS+17]. Drift [GKSBI7, JZS12].
Drift-Compensated [GKSBI7]. Driscoll
[Bur11, Joh15]. Drive
[SYC+17, Mac12, SYW17]. Drive-Thru
[SYC+17, SYW17]. Driven
[BMP12, DLMM+18]. DriverGuard
[CDD13]. DRM [Pet12]. DSA [Dra16].
DSP [MS13c]. DSPs [DGPI0]. DSS
[Ano12a]. DSSH [YLS12]. DTKI [YCR16].
DTLS [AP13]. DTRAB [FTV+10]. Dual
[BWR12, CCG+16, CMG+18, HF14b, NLYZ12, PAF18, BW13, CFN+14].
Dual-Mode [PAF18]. Dual-Rail [HF14b].
Dummy [GST12]. duplication [LWI11].
Durable [LY15]. Durfee [TK19]. During
[FGR+17, AB13, RS17]. DWT
[LD13, SJ12]. dyadic [MO14]. Dynamic
[ABB19, EKB+16, FHR14, HH15, KHY18, LHM+15, MWZ12, MM12, NKWF14, PPS12a, PNRC17, SSW12, SY14, SKV12, SGC14, VMV15, XNKG15, XWSW16, XZY+12, XWZ+18, ZXYL16, CTL12, CSTR16, DSCS12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KH18, KBP17, LXMW12, LHM14, LZC17, NPH+14, PSJ+13, SES+16, SSS11, SGM16, XHM14, YZL+18, YD17, ZSMS18, ZZL+18].
dynamic-identity [JZS+10]. dynamical
[jT12b]. Dynamics
[RSCX18, AABT16, LTC+15a, Li12].
dynamics-based [AABT16]. dyslexic
[Bha16].
e-commerce [Ano11a]. E-exam [Mor12].
E-health
[WMX+17, IC17, YZL+18, JKL+16].
E-Learning [Yon11]. e-mail [BTW15].
e-passport [LB18, LY14]. E-Voting
[KV18, LGPRH14]. E2 [WY14].
EAC [LJX10]. Each [YLL+12]. EAP
[FL13, HZC+14, ZCLL14]. EAP-based
[HZC+14, ZCLL14]. Early
[Bel18, Bro11, And13]. Earth [Har14].
easier [MBF+13]. Easy
[Bel16, SMD11, Tay14, Wu16, ZDW+16].
Eat [DSSD14]. Eavesdropping
[CWL16, Han12, YSJL14]. EC
[Dra16, CFN+14, CCG+16, CMG+18]. ECC
[BSSV12, JM+16, KRH18]. ECC-Based
[BSSV12]. ECDSA [BB+16a, HB16].
ECG [PLGMCD18]. ECG-based
[PLGMCD18]. Echo [DLMM+18, HGT15].
Echo-Based [HGT15]. economy [Sir16].
Ecosystems [LDB15, MMP19]. EDAK
[ABB19]. EdDSA [JL16]. Edge [AHM+18, DF16, KA18, MD15, PRN+19, Sun16].
Edge-centric [AHM+18]. Edition
[Cor14a, KAB10]. Editorial [OK18].
Editors [BD19, LLK18]. Education
[LRWV14]. Edwards [JL16, LT14a, YTS12].
Edwards-curve [JL16]. EFADS [WLS14].
Effect [PLGMCD18, WB12]. Effective
[HLT+15, KRH13, WMY+17]. Effectively
[YMC+17]. Effects
[MAL10, SKV12, SHBC19]. Efficiency
[ABF12, Chi16, DG17, FRS+16, HRV10, LLML12, LCL+17a, MS13b, WXLY16].
[RAZS15, Ran14]. **Encrypted**

[ADR18, BTHJ12, CWL+14, CWL16, Cor14a, DBW12, DCA18, FCM14, FRS+16, Gen13, GLG12, GZH17, HTZR12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kaw15, KG16, LA15, LGLK17, LQD+16, Lop12, Mur16, NBP17, NNAM10, PBC+17, QLL17, SAKM16, Sia12, TM18, Vai12, WBC+10, XWS16, YDY+16, ZDL12, ZXYL16, ZVG16, ZLW+17, AHM+18, AZH11, BTPLST15, BGP+17, BKV13, BL11, CH11, Cri16, CDL18, DKL+16, DRD11, ED17, FTV+10, Gen10, GZS+18, HH16, KH18, LGLK17, LQD+16, LW13a, OSSK16, PRZB12, SEXY18, SWW+17, Suc12, TKMZ13, WR15, WL19, XYW+18, YXD18, YQOL17, ZLY10, ZHT16].

**Encryption** [CC10, Mar10c, dRSdlVC12, LFGCGCRP14, Pow14].

[ADM12, AV12, AEH17, Alol2, AAC+16, Ano13c, Ano14, Ano15c, Ano17d, AKP12, ABE12, AS16, BV5+13, BWA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12, BS14, BV18, Bla16, BKL12, BPS12, BHJP14, BDMN16, Boy13, BV11, BV14, BG14, CV14, CMO+16, CCL16, CWWL12, CN12, CFZ12, CLHC12, Che15, Che18, CGL+12, Chi12, Chu16, CRE+12, Con18, CNT12, CLW16, CD16, DR10, DN12, DJF+10, DSB18, Des10b, DOS15, Dsn12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJHH12, Fcl19, FFL12, Fuc11, GWWC15, GGH+16a, GGH17, GM13, GZS+13, GSW+16, GH11a, GH11b, GHS12, GHS12, GDC16, GV12, GVW15, GM14, GL12, GKS17, Gue16, HSMY12, HLLG18, HZ11, HG12, Hor19, HC17, HTC+15, HLH19, HP12, IAD10, JLS12, JHL12, Jia14a, JR14, Kam13, KB10, KME+12, KMY18, KTT12].

**Encryption** [KOS16, KKA15, KFOS12, KHPP16, KJM18, KS12, LMGC17, LMG+18, Lau17, Led16, LLSW16, LLPY19, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LLC+15, LTZY16, LLL17a, LFX+18, LLLH18, LSLW15, LH11b, LSQ18, LB13, LY15, LW16, LYY+18, LLM12, LLH18, MZHY15, MLO17, MMP14, MR14a, MTY11, MSM18a, MVVR12, MMS17b, MRL+18, MBF18, MPRS12, MT12, MRK10, MSa12, Nac16, NMMW16, NTY12, NMS14, NAL17, OT12, OKG+15, PM13, PR12, PB12, PDNH15, PRGBSAC19, Per13, PTK12, PBS12a, PYS18, PMZ12, PCY+17, PRSV17, RVH+16, RCP+18, RZP+15, RM18, RSSB12, RDZ+16, RVRCM12, SGG18, Saa12a, SSW12, Sar10b, Sch15a, SLGZ12, SZE14, Sh14, Sml11b, Sta12, SGH15, SMOP15, Tan11, TCN+17, TICL15, TMC15, Tan17b, TDT13, TKR14, TT12, Unr15, Vai11, VSR12, VOG15, Wal18, WHC+15, WP17, WDCL18, WSS12, Wat12, WLC12].

**Encryption** [WDDW12, WZ15, WWHL12, WMS+12, WQZ+16, XNKG15, XY18, XXZ12, XJW13, XWL16, XJW+16, XHH+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YK+11, YFF+12, YCZ12, YKDL12, ZOC10, ZPM+15, ZSQ+19, ZDL12, ZYT13, ZWTM15, ZQ15, ZMW16, ZMM17, ZHW15, ZYM+18, ZWS+18, ZHZ+19, AHS14, ATKH+17, AKKY17, Ana14, Ano13b, Ano15e, Ano16f, ABR12, AMH10, ACD+15, AHL+12, BLL+19, BAAS13, BC18, BG14, BS12, BGP+17, CPPT18, CFVP16, CFZ+10, CW14b, CLH+16, CMMS17, CZ5b, CS11, Chn10, CW12a, CDF+10, CM13, CGK11, DL16a, DD17, DTZ12, Eve12, Eve16, FAF+18, FH13, FSGW11, FSGW12, FM+18, Fay16, GMOGCCCI5, GH13, GHS13, GLM+16, GH12, GLL+18, GZAX19, HGWY11, HZQ14, HZL18, HWD16, HZWS18, HZT13, HLR11, HLY11, HTF16, HTC17, HYS18, HYF18, HKHK13, JCHS16, Jia14b, JSMG18, JHCC14, JSM+18, Kam16, KHMB13, KKM+14, LLL16].

**Encryption** [LCL+17a, LCL+15, LFZ+17, LCT+14, LFWS15, LLM+19, LPds10,
LHH11, LW10, LW13b, LZC14, LPZJ15, LCY+16, LZC17, LJW+17, LJWY18, LLL+18, LDZW19, LL16a, IW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSas13, NES+14, Nam19, PPAS18, Pet12, QRW+18, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, Sar11, SYL13, SE14, SE16, SH11, SN11, SM14, SLZ12, SY15b, Sha13, SGFCRM+18, SLM10, SKB+17, Spa16, SGP+17, SGM16, Tam15, TPL16, jT12b, WGTJ10, WY10, WWYZ11, WWYY11, WHY+12, WDL13, WLFX17, Wan18, WGG+12, WLS14, WCC18, XWZW16, XWC14, XSWC10, XXX15, XWS17, XWZ+18, YT11b, yYqWqZC13, Yan14, YZCT17, YHHM18, YCT15, YLZ+16, YL11, ZWQ+11, ZZ11, ZLW+12, ZJK+14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZYC+17, ZCL+19, ZKL12, ZL12, ZDW+16, ZYT17, Zhi13, Wan14, LAL+15, Sar18a, Kat13, encryption-based [BC18, XWZ+18], Encryption/Decryption [KB10].

Encryption [zGZW12, LG12, SLY+16, RD17].

Encyclopedia [VT11]. End [Ano15c, BRR+15, BGP+17, CFE16, Chu16, RST15a, RST15b, Chi13a]. End-to-End [CFE16, RST15a, RST15b, Ano15c, BRR+15, BGP+17]. endomorphism [FWS13]. Endomorphisms [AK14, LGH+17], enemies [Fag17]. Enemy [BC14, CAC14]. Energetic [PDMR12].

Energy [Ano15d, AZF+12, ABC+17, Bla16, JEA+15, LSC+15, MP12, PAF18, TLCF16, TCN+17, VN17, CZ14, ZT16]. Energy-Efficient [MP12, TLCF16]. Energy-Harvesting [ABC+17].


engagement [LSBN14], engaging [ISC+16], engine [BS13a]. Engineering [Bel18, FSK10, GHD19, LKL18, MS18a, MP12, PGLL10, TQL+14]. Engines [LB13, BGG+13]. enhance [CZ14, SLM10].

Enhanced [DTE17, KY10, KKM+13, MS17, SGG18, TV15, YCC16, AMN18, ACK+10, DLK+16, GM16, LNK13, YQOL17].

Enhancement [FSX12b, LA15, NNA10, CHS11].

Enhancements [Che18, FSX12c].

Enhancing [CSW12, IA15, Lan13, YS15].

Enigma [KM15, KM16, LHA+16, Ore14, Ano16c, Bur11, Kap11, Kap13, McG11, MC12].

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

Enrollment [YWZ+12]. ensuing [SS17].

Entanglement [Ano15d, JEA+15].

Entanglement-Based [JEA+15].

Enterprise [TGC16, Din10, NB13].

Enterprises [KCR11]. Entities [GZ12].

Entity [BCM12, BCM13].

Entropy [DSSDW14, DK16b, KPW13, VS16, YGFL15, BNY14]. Entropy-Based [YGFL15, eTTS [YL17], enumerators [OS11].

Environment [AARJ12, BCGN16, KKA15, MLO17, MRS+17, RQD+15, SGG18, SAM+19, TV15, YMA17, FHZW18, GAI+18, HLYS14, KKM+14, Kim16, NR17, Par12b, SKB+17, WL12, WCFW18, WT10a, XXX15, YWK+10a].

Environments [HLKL15, LQY10, PAS13b, TMGP13, XLP+18, CLHJ13, CTL13, KPP16, KAS15, LNK+18b, LW13a, LCY+16, NACLR12, SCY15, Tan12b, VDO14]. Eof [Gup15].

ePassport [ABHC+16]. Ephemerizer [Tan15a]. Epistemic [Sch12c]. EPR [UUN11].


Era [Mos18, QCX18, ABJ13]. Ergodic [IAD10].

Erratum [YFK+12]. Error [KW14, LSC+15, MCP15, TLCF16, ATI+10, CH13a, LTT10]. Error-correcting [MCP15, LTT10]. Errors [TM18, CSS+13].

Establishment [ASN12, Ano11b, BCO13, DL12, NYR+14, GTSS19, SZMK13, ZPZ+16, ZW+18].

Estimation [BCF16, GSN+16]. Estonian [Ano17c]. Ethernet [KCR11]. EU [PH12b].

EUROCRYPT [PJ12, Gil10].

even [AAE+14, ERLM16, FHM+12]. Even [ARH14, LPS12, Ana14, DKS12].

Even-Mansour [TKM12].

Exam [Bla12, SR14]. evident [MN10]. Evolution [LQY10, Tay17, BvOS15].

Exact [TKM12]. exam [Mor12]. examination [VCK+12]. Examining [SP13]. Example [KD12b].

Exchange [CLY14, CST+17]. DG15, FVS17, GZ12, HC12, LY16, MSU13, TYM+17, WSA15, WT10b, YS12, YLW13, YRT+16, Yon12, ZXI16, AKG13, AIB+16, FHH10a, FA14b, FIO15, GBNM11, GLM+11, Jia14b, KMTG12, IWS10, LML+13, SEXY18, TCS14, Tso13, TKHK14, WHJ17, WZM12a, WZM12b, WT10a, WTT12, XW12, YC12, ZWAI18, ZG10].

Excitation [SOS15]. Exclusive [Men13b]. Execution [AAR12, RQD+15, YS15].

existing [FMA+18, HT13]. Expanding [MS16, Sch15b]. Expansion [LTC+15b].

TSC16a, BABB+13, Die12, JK13, Pet11].

Expectations [DY13]. Expected [DMV15, KOTY17]. Experience [AD12].

Experiences [JAE10]. Experimental [LCW+16, DHH+13]. Experimentally [LHA+16]. Experts [Sto12]. Explicit [AQD12, FHS13, FIO15, ZLC15].

exploitability [CFN+14]. exploitation [MAK+12, NCCG13]. Exploiting [ACK+10, BDGH15, VDB+16, ZPZ+16].


exponentially [RK11]. exponentiation [VN17]. exponents [SM10b]. Exposing [ERLM16, FVJ19, OF12, YQH12, YSC+15].

Exposure [BVS+13, TK19]. expression [WR15]. Extend [TMC15]. Extended [BFMT16, DGP10, Gre17, HZW+14, HBG+17, SH15, YAM12, YSC16].

Extending [ZSW+12]. Extensible [YZ12].

Extension [ARH14, EKP+13, GFBF12, GT12, RW12, SFG11, HTC17, ZXL+14].

Extensions [FVJ19, LWL10b]. Extensive [FVJ19]. external [ZZK17]. Extract [AN12]. Extract-Transform-Load [AN12].

Extractability [BCP14b]. Extractable [CZL12b, CZL14, GHWH17].

Extraction [BWLA16, GST13, GPT14, PCK14, GPP+16]. Extractor [USH19].

extractors [ZMor10]. extraordinary [Hol12].

extreme [GJ13]. Extruded [CJFH14]. Eye [ERLM16, SM13, Tox14].

F5 [LLY+12b]. Fa [FMS12a]. Fabric [BHH19]. fabricating [WW13].

Fabrication [VDB+16].

Fabrication-Induced [VDB+16]. Face [AQD12, XHH12]. Facial [KR312].

facilitate [Ch13a]. Facsimile [Ano16d].

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

Factoring [APPVP15, LML12, MM13].

Factorization [CJ12, FS15, KFL+10].
Kuz11, YAM+15, Mes15, TPL16.  
Failing  
{Cer14}.  
Fails  {ABD+15}.  
Failure  
{WCL+18}.  
Fair  {ALR13, CSV15, DSMM14, DG15, WSA15, SEXY18}.  
Fair-Exchange  
{DG15}.  
Fairness  
{ALR13, Ash14, GHKL11, Wag16, MV16b}.  
Fake  {KU14}.  
Fallen  {HCPLSB12}.  
False  
{LLZ+12, CDGC12}.  
Families  
{BSS+13, KU12}.  
Family  {ARH+18, BMS12, BKST18, DGIS12, DJG+15, FLS+10, FFL12, GNL12, LYY+18, MFG16, YCL17}.  
Fanin  
{SS12a}.  
Fast  {BLAN+16, Bru12, CHS15, DSB18, GSN+16, LGLK17, NR12, PRSV17, WHZ12, WBA17, WQZ+13, ZHW+16, FHH10a, KHM13, MBB11}.  
FastAD  
{SMBA10}.  
Faster  
{CN12, HVL17, TH16, ZSP+19, Ant14}.  
Fault  
{AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JT12a, LGL+12, LCLW17, LGLL12, MKRM10, MKAA17, PH12a, RZZ+15, SEY14, YGD+17, BBBP13, PBC14, WMYR16}.  
Fault-Based  
{BBB+16a}.  
Fault-resistant  
{PBC14}.  
Fault-tolerant  
{WMYR16}.  
FBI  
{Bha16}.  
FC  
{DDS12, Dan12}.  
FEAD  
{ZWM14}.  
Feasibility  
{AAC+16, FKS+13, WHC+15}.  
Feature  
{Ber18, SGP+12, FTV+10, GJ13, MHT+13}.  
Features  
{Y14, ZTL15, FNP+15, LCM+17, LTC+15a}.  
Feauveau  
{Ara13}.  
February  
{Ano10, DDS12, Dan12, Dn12b, Kiat11, Lin14b}.  
FedCohesion  
{CCFM12}.  
Federated  
{BS13b, CCFM12, CSL+14, SAM+19, BMB10, JAS+11, TODQ18}.  
Federated-IoT-enabled  
{TODQ18}.  
Federation  
{SS10a, NB13}.  
Federations  
{MMS+17a, MLB16}.  
Feedback  
{HZ11, Hey17, PYM+15, SKGY14, ZH15, LWK11}.  
Feedback-Based  
{PYM+15}.  
FEIPS  
{DG15}.  
Feistel  
{BFMT16, KDH15, Sas12, SEHK12}.  
FESSD  
{LGLK17}.  
FHE  
{CK18}.  
FHE-Based  
{CK18}.  
FHSD  
{SP15a}.  
FI  
{YNR12a}.  
FI-BAF  
{YNR12a}.  
Fiat  
{BDSG+13}.  
Fibonacci  
{FM15, LLP+18}.  
Fibonacci-number  
{LLP+18}.  
Fidelity  
{BCP14a}.  
Field  
{CLF+17, GHP13, HSA14, SS12a, TGC16, ZAG19}.  
Fields  
{ARH14, BGJT14, HVL17, AA14, BGJT13, CZ15a, LBOX12, Ø11}.  
Fight  
{Ano16e, Wu16}.  
File  
{DMS+16, LY16, TLC15, ZGC16, YHH18}.  
Filling  
{BWR12}.  
Filter  
{Kaw15, ATKH+17}.  
filtered  
{HTC17}.  
filtered-equality-test  
{HTC17}.  
Filtering  
{LLZ+12, CDGC12}.  
Financial  
{Ano11b, Ber12, DDS12, Dan12}.  
Finding  
{Hof16, Ste15a}.  
Fine  
{CDD13, YTH17, ZML17, CLH+16, FSGW11}.  
Fine-Grained  
{CDD13, YTH17, ZML17, CLH+16}.  
Fine-Grained-State-Machine  
{CHS15}.  
Firms  
{Ano15e}.  
First  
{Ano17d, BH15, DR10, LFX+18, MS17, PC16, Wil18, AB10a, BCV12, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14}.  
First-Generation  
{BH15}.  
First-Order  
{LFX+18}.  
Fischlin  
{ABGR13}.  
Fistful  
{MPJ+16}.  
fit  
{KGO10}.  
Fix  
{DLV16, HLV10}.  
Fixed  
{Chm10, Lim11}.  
Flag  
{MBB+18}.  
Flame  
{Goo12}.  
Flaw  
{Moo12, SH15, Ste15a}.  
Flaw-Finding  
{Ste15a}.  
Flaws  
{DR11, FVJ19, HLV10}.  
FlexDPDP  
{EKB+16}.  
Flexible  
{LGY12, PAF18, BGG+13, WLS14, ZL12, ZFH+18}.  
Flexlist  
{EKB+16}.  
Flexlist-Based  
{EKB+16}.  
Fog  
{YNR12a}.  
Flows  
{ATS15, WXL+17, KL13, LWY12, PPR+12, SRB+12}.  
Flowers  
{Hal17}.  
Flow  
{CDD13, HKB14, WYL13}.  
fly  
{PS14}.  
Fog
[ACZ16, ALR13, BBC+14, BKK14, BKPW12, BK12a, CPS16, DSM14, DQFL12, FY11, LVV11, NR12, Rja12, RW12, SMS14, SLY+16, Tan12a, YTP11, AY14a, BDP11, CG12b, CQX18, CW12a, ESR14, Gen10, HRV10, Li10, QZDJ16, WT13].

Fundamentals [Joh10]. Further [HCL+14, WHY+12]. Fus [FMS12a]. Fusion [ABCL17].

Future [AYS15, BCE+12, BKBK14, Bon12, CDFZ16, GCK12, HYS18, Mon13, Ano13d, FPBG14, Mac12, PPA18, PHWM10, MJS13]. Future-proof [Mon13].

Fuzzy [KRDH13, NC12, SH11, USH19, XJWW13, Alp18, KHM13, MMSD13, SM11, SNN14].

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

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

gadgets [Gal13]. Gait [XJR+17, XJR+17].

Gait-Based [XJR+17]. Gait-Key [XJR+17].

Gallai [SS10b].

Galois [CFR11, CLF+17, HSA14]. gambling [Ana14].

Game [MZA+13, LPZ15, SD10, SKEG14]. game-theoretic [SD10, SKEG14]. Gap [LRVW14, TMGP13, PPA18]. Gaps [SPM+13, DKL+16].

Garble [AIK14].

Garbling [App13].

Gates [App13].

Gateway [WZM12a, WZM12b, WLI11, WXK+17].

Gateway-oriented [WZM12a, WZM12b].

Gaussian [HRK+18, RMR19, YWL+17].

GCD [KI11].

GCHQ [Ald11].

GCM [KK10].

GCM/GMAC [KK10].

GDLP [MMZ12].

Gear [ASH13].

Geckos [GSC17].

geese [Bai12].

GenePrint [HQY+16].

Gener [HYS18].

General [Bar16, CJXX19, FHJ12, GBF12, Gue16, HP12, KOTY17, LPL15, PB12, SJWH+17, YFF12, ABDP15, Bai12, DGJN14, HQZH14, LWS10, WS12, YCI11, ZYC+17].

General-Purpose [Gue16, ABDP15, DGJN14].

Generalisation [LR15].

Generalised [Hes12].

Generalization [GMNS15].

Generalized [BFMT16, LPL15, PC14, TY16b, Ye14, ZÁC17, ADG16, BNST17, KL11, NC13, YMSH10].

Generated [ADD10, LCL17b, NN12, XYXY11, AGHP14, LW13b].

Generating [Ano16e].

Germany [FBM12, GLIC10, Sen10, Wat10].

Gesture [LCL17b, SHBC19].

gesture-based [SHBC19].

Get [AUMT16, GCS AddP11].

Ghost [CD11].

GHH [GH11b].

Girod [GMNS15].

GLARM [LLZ+16]. glimpse [Mic10a].

Global
Globally [CCS14]. Glyph [XZZ18]. GMAC [SKK10].

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

Goes [BCD 12, RY10]. Goldreich [Lin17].

Goldstrike [BH15]. Goliath [Sch15c].

Gong [LW16]. Good [DQFL12, FY11, LSBN14, RY10, SA14, WT13]. goodbye [HU15].

Google [Har14, Loe15, VGN14].

Goppa [MBR15]. Gordon [GW14].

GOST [LC13, WYW14]. Government [Ano15e].

GPG [Ran14]. GPGPU [RVRSCM12].

GPGPUs [TLCF16]. GPU [BCGH11, GCH15, HBBRMN+16, JHCC14, MBB11, ZOC10].

GPU [VKP17]. Graded [BR14].

grail [Wat15, Mic10a].

Grain [BMS12, FSGW11].

Grained [CDD13, YTH17, CLH16, ZML17].

Graph [ATS15, GTT11, WH18, GJMP15].

graph-based [GJMP15].

Graphical [BCV12, CTL12, LTC+15a].

graphical-based [CTL12].

Hand [BCF12, KU12, KA18, Lai17, PMZ12, BBGT12].

Gray [DA10, UUN13].


Green [dCCSB+16, ZTZ16].

Grey-box [LRW13].

Grid-Based [PL15, WS12].

Grids [SC10, CT11b, GLW13, Shy15, JAE10].

Gröbner [EVP10, FES10, Tam15].

Gros [Dan12].

Ground [KP17].

Group [AEHS15, BSV12, CGY+13, CLM16, DT13, FSV17, HL10a, Har13, LLZ+16, LCCJ13, TW14, XLM+12, XGLM14, XLW15, ZHX16, AKK+17, CML+18, GBNM11, HCCCI11, HPY10, IOV+18, LLLS13, LWS10, LLM+19, RS15, WDLZ13, WTT12, YZL+18, ZZKA17, ZWQ+11].

Group-based [LLZ+16, CML+18].

Grouping [LNZ+13].

Groups [Abe12, GZ12, XNKG15, YS12, YKNS12, MZ17a, WQZ+13, ZZ15].

Grover [JL18].

GRS [TD14].

GSR [LC17].

Guaranteed [TBCB15].

Guerrillas [Has16].

Guess [FWSF11, Fok12].

Guessing [Che15, LCL17b, XJWW13, FIO15].

Guest [Gup15, BdD19, LLK18].

Guidance [BD15].

Guide [STC11, Han12].

H.264 [JSZS12, JHHN12, LLHS12, LW13c, MU12, WDDW12, ZLDD12, ZLDD14].

H.264/AVC [JSZS12, JHHN12, LW13c].

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

H.265 [GKS17].

H.265/HEVC [GKS17].

Hack [DV16, Foli16, Ran10, Ran14, Ran16].

Hacker [ZGC16].

Hacking [GHS14, Hea15, JEA+15, Sta13].

Hacks [Ran10].

Hand [GPT14, BSS11].

Handover [HH12, LBR12, CLM+12, CML+18, ZBR11, ZCLL14].

Handshake [KK12, KK13, WZ11].

Handwriting [SKV12].

Handwritten [GdM16, ASVE13].

Hankel [Ye10].

Hans [Mur10].

Haptic [ASVE13].

Hard [KPC+11, Mar10c, ZWTM15, RPG12].

Hard-to-Invert [ZWTM15].

Hardcover [Joh10].

Harder [KTA12, Sch16].

Hardness [BHKN13, SS13].

Hardware [AW15, AW17, BRPB13, BDMLN16, BJCHA17, CMLRHS13, DZS+18, DOS15, ERRMG15, GP17, GCVR17, GCS+13].
Hardware-Assisted [LLKA19]. Hardware-Based [HLN +10]. Hardware-Enabled [YSF +18]. Hardware-Enforced [Set16]. Hardware-Intrinsic [SN10, NS10]. Hardware/Software [MRL +18].

Hardwarees [SKH15]. Hardy [Xie12]. Harmonic [YWNW15]. Harnessing [DFKC17]. Harvesting [ABC+17, ZGC16]. HAS-160 [WLC12]. Hash [Ano12, AMPH14, BHH+15, BKST18, BK12a, CLP13a, jCPB+12, CZLC12a, CZLC12b, CZLC14, CJP12, DCM18, EAA+16, FLS+10, GI12, HCPLSB12, Hul13, HRS16, HBG+17, MKF+16, MCF17, MKA17, NTY12, NR12, NXB13, PTT16, Rja12, SGY11, WSO12, ZM17, ZHZ+19, AY14a, AKY13, AP11, CJP15, ESRI14, KKG14, PPB16, RS14, SPLHCB14, SXL16, WYW14]. Hash-Based [BHH+15, GI12, HCPLSB12, Hul13, HRS16, HBG+17, MKF+16, MCF17, MKA17, NXB13, CJP12, CJP15, PPB16, SPLHCB14].


Hierarchy [NA10b, VN16]. High [AW17, ASBdS16, Ano17d, ARM15, Bar15, BDL+11, DM15, DG17, FHL19, GL12, GCS+13, HZ11, KMP+11, KPC+16, KAK18, LTKP16, LCK11, LLY+18, LPO+17, MS13b, MS13c, PCPK14, WYCF14, WL11, XNRG15, XL+18, ABB13, GZH12, GCVR17, KL13, MAK+12, RS17, WLH13, WXYL16, WZL13, WKLH11].


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

Highly [SZDL14, ACD+15, DT13]. HIGHT [CWP12, WWBC14]. hijacking [DCAT12].
HILL [KPW13, KA17]. HIMMO
[GMRT+15]. Hindering [BTPLST15].
HISS [DT13]. histogram [CSS+13, Lin14a].
Historians [Cer14]. Historical
[Hai17, Han12]. History
[ABJ13, Ano19a, Cer14, Cop10a, LT14b, MeK10, McK11, SE16, Smi15a].
history-free [SE16]. Hitler [Hea15, Moo14].
HMAC [GWM16, MAK+12, YGS+17].
HMAC-DRBG [YGS+17].
HMAC-SHA256 [GWM16].
HMAC-DRBG [YGS+17].
HMAC-SHA256 [GWM16].
Holden [Ano17b]. Hole
[Ano15d, BKKV10, PC16]. Holocaust
[Han12]. holy [Wat15, Mic10a]. home
[KPP16, Cor14a]. Homogeneous
[HT11]. Homomorphic
[AKP12, BV11, BV14, BGV14, CMO+16, CN12, CJI13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHPS12, KOS16, KGV16, Kim15, Lau17, LCLL15, MLO17, MSM18a, MRL+18, MBF18, Nac16, PKTK12, RCP+18, Tan15b, Vai11, WHC+15, XWZ+18, AKKY17, BDOZ11, BC18, CIXX19, CW12a, GH13, GHPS13, GLM+16, LL16, SXY18, Tam15, WSC14, ZXJ+14, ZYC+17].
Homomorphism [Bra13]. Honey
[JR14]. hop
[RWLL14, LCT+14]. Hop-by-Hop
[RWLL14]. Hopf [Kuz11]. horse
[BSR+14]. host
[LKKL13, der10]. hostile
[CDA14]. HotCalls [WBA17]. House
[Ano16h, Bha16]. HP
[CBG+10]. Hromkovic
[Gas13]. HTTP
[BHCdFR12]. Huang
[LLSW16]. Huffman [Sun16]. Hui
[FMS12a]. Hui-Yuan
[FMS12a]. Human
[HHS+15, IA15, DMT12, LW+10, PYH+18]. Humans
[RBNB15]. Hummingbird
[ESS12]. Hummingbird-
[ESS12]. Hunt
[Bha16]. hunted
[McG11]. HVS
[RMG18]. HWMP
[BOB13]. Hybrid
[ADI11, ARM15, JHW+19, KBL11, KKA15, LP12, NGAuHQ16, OO12, Per13, SGG18, SRT12, XWLJ16, SAM+19, EEAZ13, KP18, WXLY16, WS14, XWS17, BOB13]. Hybrid-Double
[ARM15]. hybrid-indexed
[WXYL16]. hybridization
[MMSD13]. Hyderabad
[GG10]. Hyper
[BL14, WZG+12]. Hyper-and-elliptic-curve
[BL14]. hyper-chaotic
[WZG+12]. Hyperchaotic
[MGOGCC15]. hyperelliptic
[FWS13, Kre13]. hypergeometric
[YL11]. Hyperledger
[BHH19]. i-NVMM
[CS11]. I/O
[CDD13]. i2b2
[RCP+18]. IB
[CZL14]. IBC
[BOB13]. IBC-HWMP
[BOB13]. IBM
[ABC+12, ACD+15, BAB+13, IKL+14, JSM+18]. ICA
[tWmC12]. ICICTA
[IEE11a]. ICISC
[LIH+10]. ICs
[GSFT16]. ID
[Ano17c, CTL13, CDPLCA16, EZ15, HCC10, IB11, KGO10, LGMC17, LY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, TPL16, TT12, TTH15, Wan18, WT10b, WTT12]. ID-based
[MM12, LGMC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WTT12]. ID-card
[Ano17c]. ID2S
[YRT+16]. IDEA
[BNY14]. Ideal
[LPO+17, WCL+18, HKT11, yYqWqZC13]. idealness
[TD14]. ideas
[Mac12]. idempotent
[Dur15]. Identical
[Bow11]. Identifiable
[Oba11]. Identification
[FSX12b, FSX12c, FSX12a, VAG15, YGFL15, YKK18, AGIW16, CTPH13, CJP12, CP15, EA12, HQY+16, KI11, KL13, NLYZ12, YTM+14]. identified
[AZH11]. identifier
[MJS13]. identifiers
[Cer18]. Identifying
[CSV15, SVG16, ZCS15]. identities
[GLM+11]. Identity
[AYH+18, AQD12, ASM12, ASVE13, Ano15b, ACAT+15, ASS15, BWLA16, BCF16, BHG12, BKPK12, BDFK12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CZL12a, CZL12b, CHLC12, CZLC12, CGL+12, CGY+13,
[BCP14a, Ara13]. **Images** [BCPV11, BBM15, CLF11, FR16, GL10, LC15, LLY+12b, MR16, NC12, Yam12, dRSdiVC12, AMK12, DD13, HWYW14, LW13b, MM14a, MKH+12, UUN13, WLH13, WZLW13]. **imaging** [WW13]. **IMFlexCom** [PAF18]. **IMI** [PN10]. **imitation** [Hai17]. **Impact** [Alo12, BLS12, DM15, SF12]. **Impartial** [BCF16]. **Imperceptibility** [HGT15]. **Imperceptible** [Lin14a]. **Imperfect** [ABD+15, BHvOS15]. **impersonation** [AATM18, GBNM11]. **Implants** [Mic16, SSPL+13]. **Implausibility** [GGHW17]. **Implementation** [BW16, BKLS18, BSJ15, BDMLN16, EGG+12, FHLD19, GP17, GL12, GPT12, GCS+13, HF14b, KB10, KG1V6, MFG16, MAS16, NdMMW16, QLL17, RMP10, VKP17, ZPM+15, AMN18, BDP+12, GH13, HBRBMN+16, KY10, KSH18, MM14a, MNNW15, NES+14, PBC114, SK14, SAAB10, SF12]. **Implementations** [BFCZ12, BFK16, BDG15, BJ10, Bru12, CMLRHS13, CBL13, ERRMG15, LGH+17, MLCH10, Ton16, YZLC12, ABBD13, ABF+14, BFG+14, BJR+14, CFN+14, CGH17, LBOX12, RSM19, Sta11b, ZSW+18a]. **Implementing** [Dav11, GH11b, HTZ12, LTC+15a, SG15, SL10, VOG15, SA16b]. **Implications** [DK16a, OSH16]. **implicit** [DWZ12]. **Imply** [ALR13, LRW17]. **Importance** [YL17, MLMSMG12]. **Important** [TC10]. **Impollibility** [ACM+17, BCF+14, Mat14]. **Impossible** [Blo15, CWP12, LIF16, TSSL11, WYL14, WW12, MNP12, SDM10, SDM14]. **improbable** [TS16a]. **Improve** [AQD12]. **Improved** [Ber18, BCP14a, Chi12, CGKO11, FVK17, GLLSN12, IK15, JHL12, KZG10, LT14a, LW12, LJF16, LH11, LCCJ13, LC15, LLML12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GLW13, HWW12, Nam19, PWLL13, SDM10, XHH12, WJ14]. **Improvement** [FRS+16, LFX+18, MWZ12, PLPF13, AN15, BMB16, CHS11, Far14, LNM+11]. **improvements** [EA12, HRV10, Tso13]. **Improving** [AB15, BCM+15, Ch16, FMS12b, GMS11, HLC11, HMC12, Sar10a, SS11, YWF18, YKB10]. **IMS** [IG11, MEFO12]. **In-Memory** [PAF18]. **In-Order** [ZBPF18]. **Incentive** [SJWH+17, YTH17]. **Incentive-Aware** [YTH17]. **Incident** [CCG+16, CMG+18]. **Indicial** [FD11]. **Inconsistencies** [YSC+15]. **inconsistent** [OF12]. **Increase** [NNAM10]. **Increasing** [AEH17, CLZ+17, PKS18]. **Incremental** [KKM+14, MPRS12, CS11]. **Incrementing** [KS15]. **IND-CCA** [AHS14]. IND-CCA2 [Gal13, MVVR12]. **indefinite** [Svo14]. **Independent** [FCM14, MTY11, MRRM10, YE12, ZTL15, BIV12, DDD14, VV19]. **Index** [LHHR10, PSS+13, ZXYL16, Jor13, LH112, LW13a]. **Index-Based** [ZXYL16, LLHS12]. **indexed** [WXLY16]. **Indexing** [HCDM12]. **India** [BC11, CGB+10, GG10]. **Indicator** [KU12]. **Indicators** [YT12, Pal16]. **Indirect** [ABS+12]. **Indistinguishability** [AS16, BV18, FMYM15, GGH14, GGH+16a]. **Indistinguishable** [LG12]. **Individual** [LMB12]. **INDOCRYPT** [BC11, GG10]. **Induced** [VDB+16]. **induction** [BBBP13]. **industrial** [GHD19]. **Industry** [Ano11b, QZL+16a, Cha13c, Men13b, ZSMS18]. **Infective** [GST12]. **Inference** [Bro11, DBPS12, NC12]. **Inferring** [BPSD17]. **Influence** [RSCX18]. **Information** [AQD12, ABCL17, Bai10, BF11, CVM14, CDGC12, CGB+10, CST+17, CBL13, De11, DP12, FHKP17, FHS13, HHH+13, IF16, JHNN12, LG12, LW11a, Low12, MA17, MAL10, NTKG17, SG14, ST11, TWZ11, WSS12, XSS18, Yan10].
Mei10, Men13a, Sch15a, SOG15, Sta11b, CM13, Buc10, Led16, Sch15a, Ful10, Mur10. Intraduction
[NSMS14, SAJL16, SBV14, YKC+12]. Intrusion-resilient [YKC+12], Intrusive
[AARJ12, MFH13]. Invariance
[yWpNyL11]. Invariant
[CSW12, NKFW14, RS16, WYW+13, YWWN15, GZHD12, LXXM11]. Invariants
[NKFW14, CDSL+14, KK10, MZ17a, TLL13]. Invention [Orm16]. Invents [Ant14].
Inverse [JS18, RMER19]. Inversion
[KHHH14]. Invert [ZWTM15]. Inverted
[ZXYL16]. Invertible [SLY+16, UUN13]. Investigating [SPM+13]. Investigations
[Bla16, Har14]. Invisibility [BN14]. Invisible
[Keb15, Mac14, SYL13]. InvisiMem
[AN17]. INVISIOS [AARJ12]. Invited
[SS19]. Involution [Bru12]. Involving
[HLCL11]. IoT
[AATM18, CCM17, CSH+18, FQM18, GAI+18, MMP19, NVM+17, SGC16,
TODQ18, TG17, WCFW18, WXX+17, YFT18, YTH17, ZCW15, ZLY+19]. IoT-Based
[YTH17, ZLY+19]. IoT-Enabled [SGC16]. IoTs
[SAJL16, ZSW+18a]. IP
[AGLW16, AZH11, PJ18, PA10, RS17,
SP15a, TJDZ12, WBC+10]. IP-SEC [PA10]. IPE
[ZM16]. iPhone [Wi16]. IPs
[GSFT16, NDG+17]. IPv6 [KP12]. IRC
[HB13]. IRC-based [HB13]. IRIF
[JKHe12]. Irregular [YLW+17]. ISBN
[Ano15b, Ano17b, Bai12, Joh10, Mur10,
[Dan12]. ISO
[BCM12, BCM13, T516a, WWBC14].
ISO/IEC [BCM12, BCM13]. Isogenies
[Y+17]. Isogeny
[BF19, KAK18, LNL+19, ZSP+19]. Isogeny-Based
[BF19, KAK18, ZSP+19]. Isolated
[YS15]. Isolating [LG12]. ISSAC
[Wat10]. Issue
[Ano13d, Ano16a, Ano16b,
Ano16h, CSYY18, GO17, LW13a, LLK18,
WX13, PHWM10, Sim15b]. Issues
[ABHC+16, PZPS15, JAE10, KJN+16,
MHV15]. ISTE [Ano15b]. Italian
[Sac14]. Italy [Cra12]. items [YD17]. Iterate
[HHR11]. Iterated [LPS12]. Iteration
[CCZ13]. Iterative [QJC+18, SXL16].
ITUbee [FXP+17]. iVector [RSR+19].
iVector-Based [RSR+19].
CNT12, Cou12, CMA14, DWZZ12, DL12, EAA+16, FZT13, FVS17, FB12, GFBF12, GT12, GZZ+13, GSW+16, GST13, GPT14, Gir15, GKS17, GZ12, GLB+18, HSMY12, HLLG18, HC12, HL10a, HCL+14, HTX+15, HEC+12, HLH19, Jia14a, JE+15, KP12, KTT12, KFOS12, Kim15, LSSL16, LCLL15, LGY10, LY16, LH11b, LSQ18, LCCJ13, LYY+18, LBR12, LHL18, TMY+13, TM12, WP17, WSS12, WLC12, WZ15, WCL+18, WWHL12, YZ15, Yon12, YKC+11, YFK+12, ZSP+19, ZXX16, ZY17a, AA14, ATK17, APX+18, ABB+14, AKG13, AIB+16, ABW10, AN15, BS15, BGAD12, BB14, BJ16, BSW12, BG+13, BBA16, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLCZ10, DLK+16, DGI12, Dur15, FHH10a, FA14b, FIO15, FHZ18, GMRT+15, GPP+16, GH16, GBNM11, GLM+11, GTSS19, HPC12, HZWW17, HWB12, HL11, HLSY14, HCT17, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSMG18, KDH15, KMT12, KKH19, KI18, KLIW+16, KD+17, LLLL13, LLP+18, LWS10, LIK+17, LPdS10, LW13b, LZC14, LML+13, MNP12, MRT10, NACLR12, NCL13, Nos11, Nos14, RG10, RWZ13, RPSL10, SES+16, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZ15, SA15, SGP+17, SVT10, TK19, TCS14, TLL12. key [Tso13, TKHK14, VV19, VN17, WWYZ11, WDKV19, WZM12a, WZM12b, WT10a, WTT12, WQZ+13, WXK+17, XW12, XW13, XCL13, XMHD13, XHM14, YTL11b, YC12, Yan14, YZZ+14, YHHS16, YZL+18, YLZ+16, ZPZ+16, ZWQ+11, ZZ11, ZCC15, ZT16, ZXW+18, ZXWA18, ZCL+19, ZG10, ZZZ15, ZY17b, ZWS+18, ZHT16, CLW16, OHJ10, XJ+17]. Key-Aggregate [CCT+14, PSM17, GLB+18, CLW16]. Key-Agreement [WSS12, APK+18]. Key-Alternating [BKLS12]. Key-Based [Xio12]. key-correlations [Sar14]. key-delegation [JSM18]. Key-Code [BGO13]. Key-Extraction [GPT14]. key-hash [KKG14]. Key-Insulated [FZT13, LH11b, HL11, RG10, RWZ13, WWYZ11]. Key-Length [GT12]. Key-Length-Based [PNRC17]. Key-Policy [GZ13+13, GSW+16, HSMY12, RVH+16]. Keyed [KE19, MMS17b, YHHM18]. Keyed-Function [MMS17b]. KEYing [TW14, BCPV11]. Keyless [PDM12, ZXW+18]. keyrings [MBB11]. Keys [ASN11, BF12, Bro17, CC10, HDW12, MS16, PSM17, TW14, ZM16, CMG+18, HL14, IK15, LLY15, LH13, LW10, LL+18, RWZ13]. keystream [SM11]. Keystroke [AaBT16, SP13, CTL12, LTC+15a]. Keyword [CWL+14, Che15, HCDM12, HLH19, LSSL18, WDC18, XWS16, XJWW13, ZXYL16, BL11, CLH+16, FSGW12, GZS+18, LK+14, OSS16, SY15b, WHY+12, WXLY16, WXY+18, YZCT17]. Keywords [CWL12, ZS11]. KGC [YT11a]. kid [Tan17a]. King [ABJ13]. kiss [HU15, KYEV+18, Ros11]. KLEIN [GNL12]. Klepto [XY18]. Knapsacks [Dun12a]. Knaves [CEL+19]. Knebl [Mur10]. Knights [CEL+19]. knocking [KSB+17]. Know [BC14, CAC14, XTK10]. Knowledge [CLP13a, COP+14, GJO+13, GOS12, IW14, MX13, MBC+18, MT12, OOR+14, Pan14, TSH14, Ano11a, KPP16, LLM+19]. Known [DWWZ12, JLH12, SEHK12]. Known-Key


Library
[ACZ16, Bee17, BLS12, FLW12, KRH18].

Life
[MKN13, SCMS18, McK10, McK11, War11].

Lifecycle
[Tan15a].

Lifetime
[HSUS11].

Lifting
[LSL12b].

Light
[JEA15].

lightning
[Ran10].

Lightweight
[AMKA17, AARJ12, BSS13, BFMT16, BKL13, BM11, CGCGPDMG12, CWP12, CCF17, DS11, ESS12, EKP13, FQZF18, GNL12, GAI18, GMV17, GMSV14, HZW18, HCETPL12, IS12, IOM12, KE19, MO12, MFG16, MPM17, PCDG14, She14, ZYW13, ZLY19, AMN18, AATM18, AKKY17, BLL19, Bor10, BBB16b, CL11, FLL14, GTSS19, KDH15, LLZ16, MCN18, MNP12, MHV15, MHY18, P18, PSo13, SGJ18, Tan12b, TG17, WLZ16, WGF16, YCL17, BBEPT14, Bul10a, FES10, GMOGCCC15, Her10, HCCC11, LWK11, OS11, SA14, XSWC10].

Like
[BW16, ERLM16, CGCS12, HLH19, KO16, LJ15, LJ16, RS14].

Lilliput
[BFMT16].

Limited
[DFKC17].

Limited-Use
[DFKC17].

Limits
[AS16, GV14a, KS12].

Lindell
[Ful10].

Line
[FFL12, YMWS11].

Linear
[BCI13, BW12, CGCS12, CMA14, EKP13, FGMP12, LGLL12, LJ15, LJ16, LF16, WGF16, YCL17, BBEP14, Bul10a, FES10, GMOGCC15, Her10, HCCC11, LWK11, OS11, SA14, XSWC10].

Linear/Linear
[JS18, DWZ12].

link-state
[Ham12].

Links
[PRGBC19].

Linux
[Fel13].

Lisp
[GUI10].

LISISAP
[VS11].

Listening
[Lan17].

 LIVE
[ZZCJ14].

Live
[ACz11, MeK12].

Load
[AN12, FXP12, PR19].

Loc
[CDPLCA16].

Loc/ID
[CDPLCA16].

Local
[pNyWyY14, TMK11, VGA15, WYW13, LMJC11, LWY+10, PTK14].

Locality
[Kaw15, NGCG13].

Localization
[SRAA17, GAI18, NC13, SCY15].

Locally
[Yek10].

locating
[ZYL10].

Location
[Kim11, PDS15, PKA15, WPZM16, CHX13, Har14, NZL15, PC14, YXA18].

Location-based
[Kim11, CHX13, NZL15].

Location-dependent
[PKA15].

Location-Privacy
[PSP15].

Locations
[KD12a, Alp18].

loci
[FES10].

locating
[ZYL10].

Locality
[Kaw15, NGCG13].

Listening
[LMJC11, LWW10, PTK14].

Low-Bandwidth
[GST13, NR11].

Low-Bit-Rate
[LKAT12].

Low-complexity
[DJL12].

Low-Cost
[ABC17, CI12, Man13, NVM17, LEW19].

Low-Distortion
[FHS13].

Low-end
[Chi13a].

Low-Latency
[BGC12].

Low-Overhead
[AWSS17].

Low-Power
M [Orm16, HvS12]. M-Identity [HvS12].
MA [ACM10]. MAC
[Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN16]. MacGuffin [LGL+16]. Machine
[AGHP14, Ano16c, CHS15, Sch12a, ABBD13, GJ13, Gup15, LLA+16, LH+16, QMC17, RY10, TTL10, War11, WS14].
Machine-generated [AGHP14].
Made [Orm16, Sma16]. magic [PHN+12].
Magnetic [VBD+16]. Magnifying [DKL+16]. mail [BTW15]. Main
[AMH+16, LY15, ZHZ+19, CS11].
Maintaining [WP15]. Make [Ay12].
makes [Ken11]. Making
[BG14, dCCSB+16, Gel13, LA10, ZDV+16].
Malaysia [HWG10]. Malicious [AAE*14, BL15, TM18, VQA15, BK12b, WTT12].
malleability [KTT12]. Malleable
[CKLM13, DPW18, MSAa12, CG14a, FMNV14, LP11, MSAa13, OOR+14, Pas13a].
Mallory [FHM+12]. Malware
[ATS15, GAF+15, JC13, Goo12]. man
[And13, Bat10, Kap13, Moe14].
Management [ASM12, ABB19, BD15, Bar16, BS13b, CCFM12, CSL+14, GOPB12, KP12, KKA14, Lop15b, MKF+16, PN10, TMGP13, Vle12, YZ+12, YSS14, ZJ11, ZTSR12, BBMS10, BB16b, CFL13, Cha13c, dCCSM+12, dCCSB+16, Dn10, KH18, MLMSMG12, MGP10, PLCGS11, Sch11, SR10, SA15, SWW+16, WSC14, WDKV19, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b]. Manager
[KK15, Kim16]. Managing [MD15, BC18]. MANET [KTU16]. MANETs [Yan14].
Manhattan [SS10c]. manipulation [OF12].
Mansour [DKS12, LPS12]. Manual [Sac14].
Manuale [Sac14]. Manuscript [Ano16d].
Many [LB13, HRS13, ZQWZ10].
Many-Core [LB13], many-to-one [ZQWZ10]. Map [XYXYX11, ISC+16, LZY+16, LWK+18, PC14, SE18, ZT14].
map-based [LWK+18]. Maple [G+13].
Mapping [CBL13, MS17, MM14a]. Mappings [MC11, CDPLCA16].
MapReduce [LJLC12]. Maps
[Ye14, BAAS13, KLW+16, LW10]. March
[Ano10, Cra12, DDS12, Dan12, Dn12b, IEE11a, Pie10, Sah13, WZ12a]. Marche [CCFM12]. Margareet [Led16, Sch15a].
Marian [Kap13]. market [YWK10b].
marking [PJ18]. Markov [CR12, FVK17].
Marotto [SE18]. Marshall [Don14].
Martin [ABJ13, Hof16]. Maryline
[Ano15b]. Mashup [HTZR12].
Mashup-Providing [HTZR12]. Masked
[WH17]. Masking
[HF14b, PYM+13, USH19]. Mass
[BPR14a, BPR14b]. Masses [Ano15c].
Master [Dew11, Mar10a]. Matching
[Lin15, Tan12a, MR14c, MHT+13, PTTT15, SS17, YZL+18]. MathCW [Bee17]. Mathematical
[Bee17, FGPGP14, Ham17, IBM13a, Mei10, Sch15a, Wes16, KM14, OO10, Sta11b]. Mathematical-Function [Bee17]. Mathematician [Ano17e].
Mathematicians [Azc11]. Mathematics
[Ano17b, Ay12, Led16, Sch15a, Ter11, CM13, Kra12, PHW10, Wes16].
MATLAB [TRD11]. Matrices
[AMVZ12, BNA15, AKG13, FES10]. Matrix
[BFT16, IAD10, LYY18, SK12a, TDID13, Ye10, Cha13b, LLM19, TK14].
Matrix-vector [LLM19]. Matter
[Rau15, SS12a, DKA14]. Max [And13].
Maximizing [DBPS12]. Maxims [Kob10].
May [BL10, FBM12, GI10, Se10]. maze
[LLC10]. mbedTLS [YG817]. MC
[HIDFGPC15]. MC-2D [HIDFGPC15].
MclIEEE [DN12, GV14b, MBR15, MT12, MG15, OTD10, SWM10, VOG15]. McOE
[FF12]. MDPC [HC17, VOG15]. ME
[XHH12]. mean [TTL10]. Meaningful
[LTC15b, SA16a]. Means
[KRDIH13, AMH10, Kaml6, Pal16]. Measure [DDD14]. Measure-independent
DDD14]. measurement [VGN14].
Measurements [DTE17]. measuring
[DMWS12]. Mechanical [RSCX18, Mat19].
Mechanism [ABB19, KD12b, LL15, LLY18, Lin15, PTK12, Sa12a, SMOP15, ZHS19, CL11, FPX12, PLPW13, PSJ13, WB12, YXA16, ZW14]. Mechanisms
[CBO18, JSK17, SGG18, FHH10a, KSA16, MMZ12, PLGMC18]. Media
[KBL11, Fri10a]. Mediated
[Fra16, YHK10]. Medical
[KBL11, UUN11, AIA18, AMK12, KSA16, KLC10]. Medicine [MA17, LWK18].
MEDISN [KLC10]. Meet
[LTJ17, LWKP12, LWPF12, LWKP14]. Meet-in-the-Middle
[LTJ17, LWKP12, LWPF12, LWKP14]. Meeting [Hof16]. Meets [RBHP15, BSR14, MZA13, PHY18, SM13].
Members [YWZ12]. Membership
[FHR14]. MemGuard [CZ14]. Memorial
[Ano11c]. Memoriam [Gre11]. Memories
[AWSS17, BDGH15, RM18, SM18, YNQ15]. Memory
[AN17, ASBD16, AMH16, BKKV10, DLZ16a, DHLAW10, GKM16, GM13, Gue16, HT13, HF14b, KMJ18, LGLK17, LY15, PAF18, SB18, TLGF16, ZH19, BAB13, CZ14, CS11, CVG13, VCK12, ZWT13]. Memory-less [GM13]. memoryless [BJ16]. Memristor [MCS15]. Memristor-Based
[MCS15]. men
[McK10, McK11, McK12, MPJ16].
mercurial [CS11]. Merkle [XZW18].
Mesh [BOB13, YLY18, YI14, CG12b, HGW11, HCCC11, WDBL11, XCH14, YHHS16, ZZCJ14]. Meshes [SG14].
Meshram [PLPW13]. Message [ABS12, DPKW12, HLLC11, Jia17, KHHH14, PSS13, PS12b, PA10, RW1I14, CJXX19, CMMS17, EEAZ13, Jia16, LC17, YMM13].
Message-Based [PS12b]. Messages
[Gen13, YLL12, BMM12, BTW15, KPS10, LCM17, SA15]. Messaging
[BFK10, Wu17]. messy [BBDL17].
Metaheuristic [HCETPL12].
Metamorphic [ATS15]. metaphors
[Mat19]. metering [WMYR16]. Meters
[DM15]. Method
[AGW15, Ara13, BBB16a, FLH13, GLLSN12, GMNS15, HHS15, LyWZ12, LP12, LD13, LBR12, MU12, OWHS12, PS14, SAA15, SY15a, SP15a, SZDL14, USH19, WZXL2, WZCC18, XNG14, XNRG15, YYY15, AGLW16, AIA18, BBL19, CSS13, Dra16, FVK17, KHHH14, LLC10, LT13, LT14b, LPZ15, MO14, PWW10, SI12, WT13, YWT12]. Methodology
[CBL13, ZZKA17]. Methods
[BKMK14, KOB10, LW12, KSB17, KVvE18, O010, TMK11, TPKT12]. Metric
[YGF15, DMWS12]. Metrics
[CVM14, BC18]. Mexico [AB10a]. Meyer
[Bur11, Joh15]. Microarchitectural
[MSI18]. Microarchitecture [ZBP18].
Microcontroller [GL12].
Microcontrollers [LPO17]. Microcosmic
[WWC11]. Microprocessors [SK12b].
Microsoft [Le15]. Mid [AUMT16].
Mid-Air [AUMT16]. Middle
[LTJ17, LWKP12, LWPF12, LWKP14].
MiddleBox [FGR +17]. Midway [Car11].
Might [Hur16]. Migration [SJS12].
MIKEY [TW14]. Military [HK14]. Miller [Sch15a, LL11, LT14a, Led16, LR15].
Millionaire [KGS17]. Mind [WP15].
mines [KO16]. Minimal [ARH +18, BDH11, MZ17a]. Minimalism [DKS12].
Mitigating [EPAG16, HRS16]. Mitigation [BRS17, LGR14, DJL +12]. miTLS [BFK16].
MitM [TY16b]. mix [WGJT10]. mix-networks [WGJT10]. Mixed [ST16]. mMTC [CML +18]. Mo [RBS +17]. Mobile [BCD +12, FD11, GPT12, GdM16, HvS12, HLLK15, KP12, KKA15, LH12, May15, NRZQ15, Sch15b, SFE10, Sch14, SAA12b, WPZM16, WT10b, XHH12, XNKG15, XHC +12, YHL16, Yon11, ZLDD12, Aia15, AAZ +16, ALL +18, CLP +13b, CTL12, CSSW11, CT13, uHAN +18, FHH10a, FA14b, FHZW18, GM16, GH16, HZHW17, HZW18, HL14, IB11, Kem11, KKA14, KKM +13, KKM +14, KKG14, KSB +17, LH13, OYHSB14, Par12b, hSZZ15, SSAF11, SKB +17, SHBC19, TKHK14, WSC14, WT10a, YHHM18, YNX +16, ZLDD14, ZDW +16, ZC12, MFB +13, SLL10]. mobile-cloud [KKM +13]. mobiles [GCSAddP11]. Mobility
[CLH13, LNK +18a, CL11, GH16, LH11a, MYYR13, YLS12, ZX11]. Mode
[HZ11, Mar10c, PAF18, gWpNyY +14, WLC12, ZHZ +19, Fay16]. Model
[AW15, AW17, App13, CT18, CLP13a, GLG12, GJO +13, GJJ15, GJZ17, HZX15, IA15, JHW +19, Kar12, KP17, LHM +15, LZC +12b, MVVR12, PYM +15, PNRC17, SZS14, SPM +13, TCB15, WW +11, WWHL12, XZY +12, Yon12, ZHL15, BL11, CK11, CDPLCA16, DFJ +17, HKT11, HTC17, KSV13, LST12, LCV +16, LL16b, MGP10, Mas17, MM13, NB13, WYL13, WZM12a, WZM12b, YC12, ZCL +19, TCL15]. Model-based [IA15]. Model-Predictive
[TCB15]. Modeling
[CJFH14, GBNM11, LTKP16, MKN13, PAS13b, Ana14, CDGC12, MH +18]. Modelling
[LLSW16]. modified
[CTHP13, EEAZ13, MM14b]. Modular
[Abe12, LNL +19, VN17]. modulation
[KPB17]. Moduli [APPVP15]. Modulus
[CNT12, LyWZZ12, SEY14, KFL +10]. Moment
Money [RBS +17]. Monitoring
[BCE +10, ASO14, AKP +18, KO16]. Monitors [IF16]. monopolizable
[DJL +12]. Monte [CR12, FVK17]. Montréal [JY14]. Morphing
[MBC15]. Morphology
[IA15]. MorphoSys [MD12a]. Morris
[Gre11]. most
[Ald11, ESR14, GJ +12]. Motion
[GZH17, JHHN12, AP10, SYW17]. Mouse
[ZPW16, HT11]. mouse-based [HT11]. Movement
[ERLM16, ZPW16]. Mozilla
[Loe15]. MP3 [YQH12]. MPC
[GGHR14, RSMA19]. MPEG [YYO15]. MPEG-4 [YYO15]. MPSS
[SL10]. MRAM
[DSB16, PAF18, VDB +16]. MRAM-Based [VDB +16]. MrCrypt
[TLMM13]. MSP430 [KSH18]. MSP430X
[GL12]. MST_1tn3 [StV10]. Much [DL15]. Muhammad [ABJ13]. Multi
[ASS15, BBEPT14, BRT12, CWL +14, Chi12,
GVW12, GJZ17, HYS11, HC12, HRS16, IG11, KTI12, KMO14, LyWSZ10, MZHY15, MEFO12, MLBL12, NGAuHQ16, OKG+12, OSSK16, SK12b, TWZ+12, TYM+17, Wan14, WOLP15, XWSW16, YWW10, Ye14, ZC13, ZQK15, ZLDC15, BGG+13, CLP+13b, CFVP16, CJXX19, CG12b, CLHJ13, CW14a, HCCC11, HLC12, ISC+16, JCHS16, KM11, LXK+14, LCT+14, LH13, LWY12, Mas17, QMC17, SCY15, SWW+16, SSS11, TLL12, WDZL13, WXK+17, XLWZ16, XHM14, YCC16, ZZKA17].

Naïve [ZLW+17]. Name [YCM+13]. Named [LLZ+17]. National [Fid18, ABJ13]. Natural [ZCWS15]. nature
[ASN11, YMA17, ZHH17]. Noised [JLS12]. Noisy [ASN12, HZW14]. Non
[AS17, AMH16, BCI13, CG14a, CPS16, DJL12, DPW18, EKP13, FHKP17,
FMNV14, GZX19, HKB14, KTT12, LLG15, MFH13, MSas12, OOR14, Pas13a, QJC18,
RM18, RMG18, Svo14, SM18, WGMW12, YNQ15, YKDL12, ZLDD12, AY14a, BS15,
CS11, ESR14, GIJ12, Lan11, LP11, MSas13, SES16, SX16, XSSC10, Yan14].
non-adjacent [Kre13]. non-associative [BS15]. Non-Black-Box [CPS16].
Non-blind [HKB14, RMG18]. Non-Boolean [AS17]. non-browser [GIJ12].
non-compliant [Lan11]. Non-contextual [Svo14]. non-cryptographic [AY14a, ESR14].
nor-non-interactive [BCI13, Pas13a, Yan14]. Non-intrusive [MFH13]. non-iterative [SXL16].
Non-Linear [EK13, XSSC10]. Non-Linear/Linear [EK13]. Non-malleability [KTT12].
Non-Malleable [DPW18, MSas12, CG14a, FMNV14, OOR14, Pas13a, LP11, MSas13].
Non-monopolizable [DJL12]. Non-perfect [FKHP17]. Non-Privatization [LLG15].
Non-stationary [ZLDD12]. Non-tamper [WGMW12]. Non-transferable [GZ19].
Non-uniform [QJC18]. Non-uniformly [YKDL12]. Non-Volatile
[AMH16, RM18, SM18, YNQ15, CS11]. NonInteractive
[KOS16, GOS12, MBC18]. Nonlinear
[CCM15, KW14, LW13a, Lid12]. Nonvolatile [ZHZ19]. Norm [FHS13].
Normal [RMERM19, TY16a]. Normalization [KLY12, SJ12].
Normalized [YGL15]. Normal [Low12].
Note [HY11, Gal13, Hwa11, Lim11]. nothing [Cer15]. Notions
[KFOS12, SNJ11, Sar12, BP11]. Novel
[CLHC12, DCM18, KRKH13, LLG15, LYWZZ12, LHL11b, MJGS12, MCS15,
SWM10, SC12, V16, WHZ12, WZXL12, YZX12, Ye14, ZZM17, BOB13, CH10,
DDFR13, GPLZ13, HCCC11, JXLZ15, LXCM11, LMJC11, LH13, LW10,
LML13, MRT10, NZL15, PZBF18, SY17, Sun16, T17, JT12b, WYL13,
WZG12, YWT12, ZBR11]. November
[Kap11, LCK11, Yan11]. NSA
[ABJ13, Ano13b, AHS13, Bud16, Men13b, Sta13, Tox14]. NSDG [SSPC12]. NTT
[BS15]. NTRUEncrypt [DW18, KY10]. NTRUESign [Wan10].
NUT-Based [MCDB12]. Nuclear [Hcl17].
Number
[ADI11, BKLS12, CDK10, DSB18, Fok12,
Ham17, KA18, LTP16, LCLW17, MFG16,
NIS12, NAM10, Sha10, SRAA17, SRK17,
CFY10, CP13, LLP18, LGKY10, Lim11,
MS12a, MRT10, SH11, Sti11, XSSC10].
Numbering [DNS11]. Numbers
[BCGH11, CK18, FM15, Shp10, AZH11,
Ana14, GCH15, SMDS11, ZOC10]. numeral
[GKCK11]. Numerical [CMIL16].
Numerology [GG11]. NVMM [CS11].
O [CDD13]. Obfuscated
[LMS16, OWS12, ZM16]. Obfuscating
[BGI10, BGI12]. Obfuscation [ABCL17,
AS16, AWSS17, BBC14, BV18, BCP14b,
BR14, C15b, DRS16, EMW14, FKV15,
GHR14, G16a, GH17, MH14,
BBGT12, CFVP16, G16b, OSSK16].
Obfuscation-Based [ABCL17]. Obfuscators [PSD15]. ObfusMem
[AWS17]. Object [BCK17]. Objects
[L18, ZC15, HST14, SMBA10,
WW13]. Oblivious
[DN12, W18, CGH11, RYF13].
Obscurity [Edw14]. observation
[WHY12]. Observations [HCL14].
Obtaining [BB10]. Occasion [Nat12].
October [CGB10, IEE10, IEE11b].
Octonions [BS15]. odd [GJMP15]. Oded
Outsourcing [DR12, LJLC12, LHL+14, LJWY18, SKB+17, SWW+16].
Over-the-Air [VOGB18, ZXW+18]. Overcoming
[BKKV10, DY13].
Overhead [AWSS17, Bai10, CCW+10, GHS12, RM18, ZJ11, RS17].
Overlay [CHS15, MJS13].
Oversight [Bla16].
overview [AA14, BDP+12]. own [Zha15a]. owners [GZS+18]. Ownership
[FMTR12, RR11, HWYW14, KH18].
Oxford [Che11, Wes16]. Ozarow [ADG16].

P2P [dCCSM+12]. P3 [HK18]. Packet
[FRG+17, JTZ+17, VKPI17, XHC+12, MV16b, PJ18, PX13, XWDN12].
Packets [Bis17]. Pads [NA10a, BM15]. Paillier
[Lin15]. Pairing [Bon12, CWWL12, CST+17, KZG10, KHPP16, LGPRH14, Meni3a, MSt18, YTS12, BP18, Con12, KSH18, LL16a, LR15, YT11b, ZY17b].
Pairing-Based
[Bon12, CST+17, KZG10, LGPRH14, Meni3a, MSt18, YTS12, Con12, KSH18].
pairing-free [LL16a, YT11b].
pairing-friendly [BP18]. Pairings
[ASS15, Hof15, IL15, LT14a, HWB12, QXYWX16, RS15, UK18]. pairs [MCP15].
Pairwise [DL12, YM16]. Palash [Kat13].
Palm [IEE11b]. Pan [GOPB12].
Pan-European [GOPB12]. Panacea
[Hor19]. Paper
[TSH17, Ano16g, SK14, YFK+12]. Papers
[Ano16a, Ano16b, Ano16h, LW13a, XW13, DDS12, Dan12, MV12, BYL10, LY14, LH10a, vDKS11]. Paradigm
[ABGR13, BS12, Mau12, MP12, TAP19, WQZ+13]. Parallel
[Bull10a]. Paranoia [Cor14a]. Park
[Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, McK11, McK12, Pen11a, Smi11a, Smi15b, Smi15a, Bai12]. Part
[BLM18, VM14, BD15, Bar16]. Partial
[DLV16, GFBF12, LG12, SGS14, TK19, WDDW12, Bax14]. Partially [KB10].
participants [KSu13, WTT12]. participating [CH10]. particle [ZSMS18]. Parties
[YCR16, Kup13]. Partitioned
[FVS17]. Partitioning [ADR18, AP11]. Party
[Ash14, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, OSH16, QZL+16b, Tym+17, ZM16, ED19, FIO15, GVW12, HPC12, HWB12, LyWSZ10, LML+13, Tso13, THK14, Xlw16, XCL13, YC12, ZZ+14, Zzc15, GHKL11].
Passau [GLIC10]. PASSERINE [Saa12a]. Passion
[Hof15]. Passive [DHB16, GSC17, SB17, BM13, uHAN+18, Llw11, MK12a].
passport [LZJX10]. Password
[ASBdS16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, Yrt+16, XZHL16, ABK13, AIKC18, CTL12, DSCS12, FA14a, FIO15, FH16, GPLZ13, HCC10, IOV+18, KMTG12, LWS10, LNK13, MM12, Mvo11, Tso13, THK14, WZM12a, WZM12b, YC12, ZXMLA18].
Password-Authenticated
[HCL+14, YRT+16, ZHL16, LWS10, WZM12a, WZM12b]. Password-Based
[BRT12, CLY14, FVS17, WgMW12, DSCS12, FA14a, FIO15, IOV+18, TKH14].
Password-Only [YLW13, KMTG12]. Passwords
[BHvOS15, LCL17b, BCV12, Che13, GPLZ13]. Past [Bon12]. Patchwork
[NXH+17, XNG+14]. Patchwork-Based
[NXH+17, XNG+14]. Path [DMS+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13].
Patient [ZLDCC15, ZVG16].
POB [SRAA17]. Podolsky [HR13]. Point [AK14, MH14, ZC13, ZM16].
Point-To-Point [ZC13].
Point/Polynomial [ZM16]. Pointers [Lop12, PYM+13]. Points
[SC12, Chm10, Lim11]. Poisoning [HLAZ15, YCM+13]. Polar
[YWNW15, PGLL10, YKK18]. Polarities [XNP+18].
policies [Cra11, DFJ+10, LHM14]. Policy [FVJ19, GZZ+13, GSW+16, HSMY12, MK12b, RVH+16, Rao17, SVG16, XMLC13, XWLJ16, ZHW15, FSGW11, FS18, HZL18, HHHK13, JSMG18, LJJW18, LDZW19, QRW+18, TY16a, WXS17, LAL+15, LHL15]. Polish [Kap11].
Polynomial [Ano11b, BGJT14, DWZ18, ERRMG15, FS15, HVL17, NKF14, WSSO12, ZM16, AAT16, BGJT13, Bul10a, Bul10a]. Polynomial-Advantage [WSSO12].
Polynomials [CMLRHS13, SS12b, TWZ11, LPdS10].
Portable [Bee17, LA10]. posed [Lan10].
Position [BCF+14, CGMO14, MS17, YXA+18]. Position-Based [BCF+14, CGMO14].
Positioning [HK15]. Possession [EKB+16, ZPXX17, SYY+17]. possibility [BGI+10, BGI+12]. Possible [BF12, Fra15, Om16]. Post
[LLK18, MKAA17, Y+17, ZCC15, YDH+15, Sen10, Yan11]. Post-challenge [ZCC15].
Post-Quantum [LLK18, MKAA17, Y+17, YDH+15, Sen10, Yan11]. postcamera [Lin14a]. Postfix [HEK18]. Postquantum
[Ano16a, Ano16b, BLM17, BLM18, Lau17, MGG+19, YZCT17]. posture [SHBC19].
Potential [Cil11, VS16, ZW15]. Power [ARP12, AS16, HHR11, MMP14, MD12b, MAS16, SAI16, SDM+12, TQL+14, WT10b, YAM+15, ZH15, ZJ11, FAA+18, LGKY10, LKAT12, QGGL13, RITF+11].
PPFM [MS17]. PPM [XHC+12]. PQCrypto [Sen10, Yan11]. Practical
[AK11, BHH+15, BDH11, CLSW12, CGH17, Cra11, DZY10, EA12, FSS12, FSK10, HSA14, HPO+15, HRR+18, LW16, LIQY18, MFB18, PPTT15, RW23, TSH17, WHLH16, XW13, YZCL12, ZYD10, ZLW+17, AMS+10, BS13a, CNF+14, JAK+16, LFZ+17, PHGR16, WR15, YKGK13, ZSW+18a]. practicality [NDNR13, Zha15a]. Practice
[ABD+15, CDFZ16, FM12, PW12, Rog16, RBHP15, RST15a, RST15b, SN10, SAKM16, NS10, Sta11a].
Practice-Oriented [Rog16]. Practitioners [PP10a]. Pre [YW1+17, YHHS16]. pre-distribution [YHHS16]. Pre-image [YW1+17]. Preaveraging [GWM16].
PRECISE [HYF18]. precision [MN14, SK12b]. Precomputation [GKM16]. Predicate [KHPP16, NMS14, YKNS12, ZYT13, FH13, HFT16].
Predictability [DK16b]. prediction [CSS+13]. Predictive [TBCB15].
[BPC14a, LLG15, VSV15, Yon11, LVR10, TMLS12]. preserve [BAG12]. preserved
[SWW+17]. Preserving
[ABCL17, BJL16, BHKN13, BJL12, CWL+14, CRE+12, GZZ+13, HMY12, HLLC11, HXC+11, HMK14, HK18, KS12, LMGC17, LNYX15, LQD+16, MGH18, NSMS14, OMR16, PR12, PD14, PSS+13, PPRT12, Pet12, RVH+16, RSR+19].
IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLIC10, IE11a, Kial11, Lin14b, Sah13.

Processing [SAKM16, TKMZ13, VKPI17, BKV13, HKW+15, MS13b, PRZB12, WS14].

Processor [BKV13, CLF+17, HKL+14, LB13, MBR15, YS15, ABDP15, BAB+13, BGG+13, KSH18, SSPL+13, Tar10].

Processors [AD12, CCM+15, OT12, YKNS12, Cha13b, DDM17].

Products [LMG+18, RS10].

Professional [STC11].

Profiles [BCF16].

Profiling [DP12].

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

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

Progress [AB10a, BL10, BC11, GG10].

Progressive [SA16a].

Project [SPG+19, ACK+10, SS10c, W118].

Project-Based [SPG+19].

Protocol [APPVP15].

Program [MZ17b, Wal18, CLZ+17, GGH+16b, MFH13].

Programmable [CLF+17].

Programming [Bee17, Bcem15, SY14, ASEV13, HL10].

Programs [BG1+10, BGI+12, CL16].

Progress [AB10a, BL10, BC11, GG10].

Progressive [SA16a].

Project [SPG+19, ACK+10, SS10c, W118].

Project-Based [SPG+19].

Property [HEC+12, PR12, Rja12].

Properties [CCK12, CCCK16, DPFL12, FY11, JS18, JW13, KU12, Sch12c, CLCZ10, WT13].

Proof [HEC+12, PR12, Rja12].

Proofs [BGK12, CSGK12, BGB12, BC1+13, BSDG+13, CLZC12b, IW14, LN13+13, Man1, NTY12, Sav13b, WPZM16, AGHP14, KPP+16, KKK+16, Li10].

Propagate [GWM16].

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

Properties [CCK12, CCCK16, DPFL12, FY11, JS18, JW13, KU12, Sch12c, CLCZ10, WT13].

Proof [HEC+12, PR12, Rja12].

Proportions [Ber12].

Propose [BFMT16].

proposed [Bax14].

Protect [CTC+15, YMC+17, YMB12, CDF+10, dCCSM+12].

Protected [BDGH15, SG15].

Protecting [BCP14a, GSFT16, LLFY19, Mar10b, RCP+18, SCY15, Wat14b, ATKH+17, CDA14].

Protection [CDD13, GST12, Lop12, NGAuH16, NDG+17, RR11, SEY14, SJ12, AT1+10, HLYS14, KKM+13, LvRY10, RS17, TLL13, YWT+12].

PROTECTION-KEY [HLYS14].

Protocol [BL12, BC14, BCM+15, BSSV12, BFK16, CC14, CCM17, FLH13, FMT12, Fra16, GI12, HvS12, HC12, HL10a, HCP13, HC12, HCT12, HKL+12, JTH+16, JIHL+19, KMO14, LNZ+13, LCG13, LNXY15, MBC15, MR10, PSS+13, SBS+12, SGC16, TYK+12, WT10b, JXR+17, YS12, YWF18, YWZ+12, ZXZ+11, AATM18, AKG13, AIB+16, AIAK18, AN15, BDM18, BGAD12, CSD18, CCSW11, CJP15, DCL+16, EA12, FA14b, FIO15, GMSW14, GLM+11, HPC12, HWB12, HL14, IC17, IOV+18, JK+16, JXZL15, Kim11, KO16, LLLS13, LDDAM12, LKKL13, LWS10, LMXW12, LE10, LY14, LML+13, NCL13, NLYZ12, OHJ10, Par12b, SPLHC14, SB17, SGJ+18, SWW+16, SSS11, SSLP+13, TG17, Ts13, TJKH14, VS11, WCFW18, WZM12a, WZM12b, WLS14, WM16, WT10a, WTT12, WCH18, XCL13, XHM14, YC12, YZZ+14, YMM13, ZWQ+11, ZT16, ZC+17, ZXW+18, XW18, ZG10, ZC15, ZR11, BO13, CJP12, LFGCCCR14].

Protocol [Ste15b].

Protocols [API3, ABHC+16, BMP12, CCK12, CCK16, CCF17, CCD15, Con10, CM11, Fra15, GRL12, GM11, GRL10, HLLC11, HL10b, KOS16, LY16, MS16, MT12, Mur16, NYR+14, NSMS14, PS14, SBS+12, Sch12c, SO12, TM12, Xio12, YRT+16, Aia15, An13b, ACM12, CML+18, CR10, CLCZ10, DGGJ14, FTP+10, GBMN11, GLR13, HSH11, Ham12, HDPC13, HZWW17, HST14, KJN+16, KUSU13, KKK+16, LKKL13, MN10, NR11, Nos11, Nos14, SD10, YSL+10].

Prototyping [KPC+16].

Provable [BKLS12, CC14, EKB+16, Rog16, YMSH10, ZX11, ZPXX17, FA14a, HRS13, LH11, WB12, XCL13].

Provably [BCGAPM12, BCM12, BCM13, BHP14, FH110a, GLL+18, IL15, LH11a, LL16b, PS17, ...]
WMS+12, XJWW13, YC12, YZZ+14, ZG10, ABBD13, FIO15, SXY16, XWXC14. prove [DGJN14]. provenance [CDLI18, ZOSZ17].
Provide [Ano15a], Provided [KS12].
Providence [Sch15a], provider [DFJ+17].
providers [AKK+17, BK12b, YWK10b].
Providing [DLN13, HTZR12, KS18, MLM16]. Proving [Sar14, AGH+17].
Proxy [ASS15, GSW+16, GJJ15, GJZ17, GZXA19, HGWW11, HZX15, KP12, LSLW15, LAL+15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW+16, YMWS11, YCM+13, BGP+17, CLH+16, FSGW11, FSGW12, GH12, HWDL16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, LL16b, QMW17, SLZ12, SKB+17, Tia15, WHY+12, Wan18, WLS14, XWXC14, YZCT17, ZLY10, ZDW+16].
Proxy-invisible [SYL13].
Ps [HDWH12].
Pseudo [NN12, XYXYX11, CFY+10, KM10a, MG15, PLsVe10, SH11, SM11, XSWC10, Zim10].
Pseudorandom [AS17, BCGH11, BK12a, Kla10, MFG16, CP13, GCH15, HRV10].
Pseudorandomness [Sha10a]. PSMPA [ZLDC15]. PSO [TLL13]. PSPACE [JJUW10]. Public [Ano11b, ABW10, BVS+13, BB14, BKLS12, BKVK10, CT18, CLP13a, Che15, CNT12, Con12, FBM12, GKS17, HCTC+15, HLH19, IM14, JLT+12, KFSO12, LLSW16, LpD10, LSQ18, LZC14, LLH18, MZH15, MPM14, MTY11, Mat14, MPR12, Muf16, NTY12, Orn16, PDNH15, RSBGN12, RW12, RBHP15, SGG18, Saa12a, Sch19, SK12b, SVM+10, Sia12, SC12, SLY+16, SGP+17, SVT10, TMC15, TT12, WP17, WZ15, WWHL12, Wil18, XNKG15, XXZ12, Xio12, XJWW13, YL17, YKC+11, YFK+12, YMC+17, ZY17a, AA14, ATKH+17, BS15, BSW12, Dur15, HZWW17, HL14, HTC17, LSNB14, LLY15, LFWS15, LH13, LL16a, RPSL10, SES+16, SY15b, VN17, YT11b, YYS+16, ZZ11, ZCC15, ZCL+19, ZY17b, FB12].
Public-Coin [CLP13a, Mat14].
Public-Key [BVS+13, BKKV10, GKS17, KFSO12, LLH18, MPM14, MPRS12, NTY12, Orm16, PDNH15, RSBGN12, RW12, SK12b, SVM+10, Sia12, XNKG15, XJWW13, YKCC+11, YFK+12, ZY17a, ABW10, IM14, LpD10, LzC14, BSW12, RPSL10, SES+16, VN17, ZCC15, ZY17b].
Publication [ZTL15]. Publicly [NMP+13, YNR12a]. Publish [MYYR13].
Publish/Subscribe [DLZ+16b, OFMR16, PRSV17, SLI11, TKR14, YSM14].
Puzzle [IBM13a]. Puzzles [RSBG12, dCCSM+12, dCCSB+16]. Py [DGIS12]. Py-Family [DGIS12]. pyramid [MHT+13].
### Quadratic

* [AZPC14, HDWH12]. Quadratic
  
* [KRDH13, SEY14, YDH15]. Quadraticity
  
* [MS12b]. Quality
  
* [CSW12, NN12, YCM13, SS11, WZLW13, WKH11]. Quantitative
  
* [BL15, MLBL12, MV16b, HM10]. Quantization
  
* [KRDH13, SEY14, YDH15]. Quadraticity
  
### Quality

* [CSW12, NN12, YCM13, SS11, WZLW13, WKH11]. Quantitative
  
* [BL15, MLBL12, MV16b, HM10]. Quantization
  
### Random

* [IOM12]. RAM [RYF13]. Ramanujan
  
* [KK10]. Ramifications [ALR13]. Random
  
### Randomness

* [AY14a, Ana14, ABF12, ACM17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11]. Range
  
* [DCA18, HMCK12, JCHS16]. Rank
  
* [SS10b, FES10]. Ranked
  
### Re-authentication

* [LBR12, FXP12, LMJC11]. Re-encryption
  
* [BR12, GW16, GZX19, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PRSV17, WY10, XJW16, BGP17, CFZ10, CLH16, CZ15b, FSWG11, FSWG12, FXP12, GH12, HWD16, HYP18, KKM14, LMJC11, LCT14, LFWS15, LL16a, SYL13, SLZ12, SKB17, Tia15, WJG10, WHY12, Wan18, WLS14, XXX15, YZCT17, ZDW16, LAL15]. Re-encryption
  
* [BR12, FXP12, LMJC11]. Re-Encryption
  
* [GCS13, Loc15, Rec15, RS14, Sar14]. RC4-like [RS14]. Re
  
### Re-Encryption

* [BR12, FXP12, LMJC11]. Re-Encryption
  
* [GCS13, Loc15, Rec15, RS14, Sar14]. RC4-like [RS14]. Re
  
* [AY14a, Ana14, ABF12, ACM17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11]. Range
  
* [DCA18, HMCK12, JCHS16]. Rank
  
* [SS10b, FES10]. Ranked
  
### Rationality

* [GLR10, GLR13]. RBAC
  
* [VN16]. RC4
  
* [GCS13, Loc15, Rec15, RS14, Sar14]. RC4-like [RS14]. Re
  
* [AY14a, Ana14, ABF12, ACM17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11]. Range
  
* [DCA18, HMCK12, JCHS16]. Rank
  
* [SS10b, FES10]. Ranked
  
* [AY14a, Ana14, ABF12, ACM17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11]. Range
  
* [DCA18, HMCK12, JCHS16]. Rank
  
* [SS10b, FES10]. Ranked
  
### Re-encryption

* [BR12, FXP12, LMJC11]. Re-Encryption
  
* [GCS13, Loc15, Rec15, RS14, Sar14]. RC4-like [RS14]. Re
  
### Randomness

* [AY14a, Ana14, ABF12, ACM17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11]. Range
  
* [DCA18, HMCK12, JCHS16]. Rank
  
* [SS10b, FES10]. Ranked
  
* [AY14a, Ana14, ABF12, ACM17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11]. Range
  
* [DCA18, HMCK12, JCHS16]. Rank
  
* [SS10b, FES10]. Ranked
NAL17, PRSV17, XJW⁺16, ABR12, GZX19, LSC12, Pet12, SYL10, BGP⁺17, CFZ⁺10, CLH⁺16, CZI15b, FSGW11, FSGW12, GHI12, HWDL16, HYF18, KKM⁺14, LCT⁺14, LFWS15, LL⁺16a, SYL13, SLZ12, SKB⁺17, WJGT10, WHY⁺12, Wan18, WLS14, XXX15, YZCT17, ZDW⁺16, LAL⁺15]. re-signatures [Tia15].


---

LNM, CHS11, HU15, KKG14, LH10c, LNY11, LNK13, LWK+18, LH13, MM12, Sar10a, WQZ+13, YSL+10]. remotely [Wat14b, YHHM18]. Removing [HKPK13]. 
Renewal [MMHY]. renewed [GPLMZ].

rental [LY14]. Reordering [Ao12]. Repair [SEK+19]. Repairing [BCM12, BCM13].
repository [RSM15]. Representation [AGW15, BFMT16, MHT+13].
Representation-Based [AGW15].
Representatives [Bla16]. reproducible [CW12a]. Repudiation [LLG15].
Repurposing [GY13]. Reputation [BL15, LHM+15, PAS13b, MPG10].
Reputation-Based [PAS13b]. Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13]. Requirements [OS16].
requiring [KHHH14]. ReSC [YFT18].
Rescue [TSH17]. Research [BA18, CDFZ16, SG19+19, WP15, GLIC10, Hof16, Pal15, Ven14]. Researchers [Con12, Edw14, Wall18, Win17].
reset [RY10]. Resettable [CPS16]. Resettably-Sound [COP+14].
Resilience [NTY12, GL+18]. Resilience [YM16].
Resilient [AV12, BKKV10, FPS12, LTZ16, LD13, NRY+14, Pan14, PNS15, ZXY+12, YZ12, YNR12b, YCZ12, ZYT13, ZWTM15, ZM17, ZY17a, ZYM18, CQX18, DLZ16a, GV14a, KPS10, MMMS13, SGG+17, Wan18, YSFL14, YKC+12, YLZ+16, YZ17b].
Resistance [CGCS12, RRC12, WLZL12, ZJ11, DLN13, FJIO15]. Resistant [BK12a, CDK+10, GV14b, HF14b, WHZ12, WG112, WH17, YPR117, GMRT+15, HCC10, PBCC14, VCK+12, WTT12, YKKG13]. resisting [SXL16, Tam15].
Resource-efficient [SZMK13, XZW16].
Respiratory [RSCX18]. Response [GHS14, HLKL15, ZHW+16, MRRT17].
Resprinting [TBCB15]. restoration [WHZ12]. restricted [CHL16]. result [ACK+10, ED17]. Results [DGSI12, LFLF16, Hof16, KGO10].
Rethinking [Che13, HU15, LSG16, MV16a].
Retrieval [BBB+16a, BTH12, CJP12, DS19, HK14, JMG+16, JKH12, Yek10, ZZ1+11, CJ15P, SWW+17]. returned [War11]. reusable [RS17]. Reuse [ABF12].
Reveal [Sta13]. Revealed [Ano15d].
Revealing [BT12, KK12, KK13]. reverse [TQL+14]. reversed [KHY18].
Reversibility [FSX12a, HWW14].
Reversible [CLF11, CSS13, HHS+15, MM17, MR16, NC12, AMK12, CT11a, HLC16, JK13, MM14a, NC13, PWLL13, PC14, TK14, WOLS12]. Reversibly [MKH+12].
Review [Ano15b, Ano17b, Ay12, Ayu12, Bai12, Bar12, Cou12, Dew11, Ful10, Gas13, Joh10, Kat13, Ke15, Kob10, Led16, Lop15b, Low12, Mei10, Mou15, Mur10, Sch15a, Sha10, Ter11, Xie12, JAS+11, MM12, TPK12].
Reviewed [Sch15a]. Reviews [SR14].
Revised [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDSK11]. Revising [BT12].
revision [LT14b]. Revisited [CL14, DCPW12, DKS12, GWWC15, KFO15, LL11, Lop15a, PKTK12, Sar12, Tan12a, BCL14, HKT11, HYWS11, TS16a, ZCL+12].
Revisiting [TLW12, WSA15].
Revocability [WHLH16]. Revocable [AEHS15, CD16, QZ18, SE14, SE16, SRS14, SZDL14, TCL15, TT12, Unr15, FLL+14, LDZW19, WLFX17, WTT12]. Revocation [AEHS15, LLC+15, LW16, Loh15b, RDZ+16, XMLC13, YWZ+12, ATK11, LJWY18].
Revoking [TAKS10]. Revolutionized [Orn16].
RFID [CJP15, AATM18, BL12,
BSSV12, BM11, CGCGPDMG12, CCF17, CJP12, Cho14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, GAI+18, HSH11, HBPC13, HQY+16, HCPLSB12, HCETPL+12, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLSvdLE10, QZL+16a, QZL+16b, SBS+12, SPLHCB14, TG17, WH17, WCFW18, YFT18.

RFID-Enabled
[YFT18, QZL+16a, QZL+16b]. **RFID/NFC** [Mic16]. **RFIDs** [KOP12]. **RGB** [SNM14, ST16]. RI [Sch15a]. Rich [CS12].

Richman [Xie12]. Riddle
[Bro17, SR12a, BBG+17, LHA+12, Sch11]. Rightful
[RR11]. Rights
[LRVY10].

Rigorous
[DK17]. Ring
[GHPS12, HKL+12, XY18, YKS10, YLA+13, ZJ14, DZ14, Hwa11]. Ring-LPN
[HKL+12]. Ring-LWE
[XY18]. Rings
[YM16]. RISC
[ZBPFI18]. rise
[Ano14, Mat19]. Risk
[Zha15b, PKN15].
risks
[Lan10, SS17]. RKA
[SLY+16].

RKA-Secure
[SLY+16]. RLCPS
[DSS12].

RLWE
[XZJ+14]. RNG
[CGH17]. RNGs
[DSSDW14]. RNTS
[PSOMPL13].

roaming
[SCHH10, ZX11]. Robbery
[SPW+16]. Robert
[Gre11]. Robotic
[SPW+16, VOGB18]. Robust
[BCGAPM12, BCG12a, FOR12, GKS17, HZC+12].

JSZS12, LSL12b, LSR13, MR16, MU12, MS16, MC11, pNyWyY+14, OCDG11, RR11, RMG18, SJ12, SC12, SZTZ18, TLF16, TK14, TTL10, WLDB11, WgMdZ1Z12, gWpNyY+14, XNG+14, YWN15, YYO15, AP10, AIA+18, CLM+12, EAA+16, GZHD12, HZC+14, HZL18, IOV+18, KIH19, LNk+18a, LW10, PKS18, RS17, yWpNyL11, yWpWyVpN13, YSL+10, ZHH+17].

Robustness
[HGT15, YKS10, AEH17]. ROCA
[Ano17f]. Rochefort
[Car11]. Rock
[Crit6]. Rock-solid
[Crit6]. Rodney
[DSS12]. Rogozin
[Kuz11]. Role
[PH12b, ZVG16, ZHV14]. Role-Based
[ZVG16, ZHV14]. Ron
[LHA+12]. Room
[Smi11b, Pea11]. Root
[ARH14]. ROP
[ZHS+19]. Rosen
[HR13]. Rosenhain
[CDSLY14]. rotation
[LWL11].

Rotational
[KN10, KRN10]. Roulette
[Ber17]. Round
[Ber17, jCPB+12, COP+14, DWWZ12, GGHR14, KOT17, KMO14, LWZ12, LJ17, Pan14, TYM+17, XZL15, Yon12, YJ14b, ABM+12, Blo15, LP11, LFW+16, Sun11, TSSL11, TQL+14, TC14, XW12].

Round-Reduced
[DWWZ12]. Rounds
[GST12, Sas12, LYHH14, MNP12]. Router
[Bis17, SA15]. Routing
[Han12, KZH10, WLY+15, LSG16, LC17].

RSA
[Dun12b, KJ11, Pie10, APPVP15, BBBP13, Bro17, BNST17, CLSW12, Chm10, GM13, GST13, Her14, Hin10, HLYS14, IK15, KHHH14, KFL+10, Lim11, Moe12, SM10a, SM10b, SL10, TK19, Win17, YHK+10, YXA+16]. RSA-1024
[Bro17, Win17].

RSEL
[FL+14]. RST
[LD13]. rubber
[BSR+14]. Rule
[KPW13, NC12, TW12, McG11].

Rule-Based
[TW12]. Rumor
[FKOV15]. Run
[CEL+19, IF16]. Run-Time
[IF16].

RunStream
[KPC+16]. Runtime
[CLP+13b]. Rupture
[KA18]. Russian
[McG11].
Schneier [Sev16]. Scholarship [SPG<sup>+</sup>19]. Scholarship-for-Service [SPG<sup>+</sup>19].


Scope [Bai12]. Score [GCSAddP11]. Scoring [OSSK16]. Scrambling [LLL17a].


SE-AKA [LLLS13]. Seals [MN10]. Seam [LC15]. Seam-Carved [LC15]. Search [AHN<sup>+</sup>18, CWL<sup>+</sup>14, Che15, DCA18, FR<sup>+</sup>16, GTT11, HCDM12, HLH19, LSQL18, TMC15, WDCL18, WW12, XWSW16, XJW13, ZXY16, BL11, CLH<sup>+</sup>16, FH13, FSGW12, GZS<sup>+</sup>18, HH16, OSSK16, SY15b, WHY<sup>+</sup>12, WXLY16, XWY<sup>+</sup>18, YXDI16, YQOL17, ZZ11].

Searchable [BHJP14, CWWL12, CLW16, CGKO11, FJJHJ12, PBC<sup>+</sup>17, PCY<sup>+</sup>17, XNKG15, ZZQ<sup>+</sup>19, DLZ16a, DRD11, HQZH14, HTC17, JCWH16, LSC17, LLL<sup>+</sup>18, RPSL10, WXLY16, WCCH18, YZCT17].

Searches [Sia12, WR15]. searching [GP<sup>+</sup>12]. Seattle [LCK11, KCR11].


Secret [ADD16, AARJ12, Ash14, AMH<sup>+</sup>16, BVS<sup>+</sup>13, BWLA16, BCGH11, BCG12a, BCQ<sup>+</sup>13, BWA13, BJL12, BHJP14, BFS11, Bru12, BDH11, BEM15, CFOR12, CCM17, CZF12, CZLC14, Che15, CMA14, DM18, DL15, DMS<sup>+</sup>16, DG15, DLZ<sup>+</sup>16b, Edw17, FLH13, Fri10b, FD11, FSX12a, zGXW12, GKM16, GGH14, GFBF12, GT12, GV14b, GHKL11, GM14, GZS<sup>+</sup>18, Hv512, HSM14, HLLG18, Har16, HL10b, HP14, HTZR12, HMCK12, HLC<sup>+</sup>18, HLKL15, HIS18, HK14, HLH19, IL15, Jac16, JHW<sup>+</sup>19, KW14, KME<sup>+</sup>12, KYEV<sup>+</sup>18, Kip15, KH10, LJS<sup>+</sup>14, LL15, LH12, LYZ<sup>+</sup>13, LTH<sup>+</sup>15, LTZ16, LSLW15, LLGJ16, LSQL18, LY15, LHL15, LMLL12, LSC12, MLO17, MMP14, Mal13, MVVR12, MMS17b, MK12a, MKAA17, NBZP17, NDG<sup>+</sup>17, NR12, NMS14, NNSMS14, PB12, PSM17, Per13, PBC<sup>+</sup>17, PRN<sup>+</sup>19, QZL<sup>+</sup>16b, QZDJ16, QZZ18, RMP10, Rea16, RSGG15, SAM<sup>+</sup>19, SNJ11, ST19, SZS14].


Searchable [BHJP14, CWWL12, CLW16, CGKO11, FJJHJ12, PBC<sup>+</sup>17, PCY<sup>+</sup>17, XNKG15, ZZQ<sup>+</sup>19, DLZ16a, DRD11, HQZH14, HTC17, JCWH16, LSC17, LLL<sup>+</sup>18, RPSL10, WXLY16, WCCH18, YZCT17].

Searches [Sia12, WR15]. searching [GP<sup>+</sup>12]. Seattle [LCK11, KCR11].


Secrecy [ADD16, AARJ12, Ash14, AMH<sup>+</sup>16, BVS<sup>+</sup>13, BWLA16, BCGH11, BCG12a, BCQ<sup>+</sup>13, BWA13, BJL12, BHJP14, BFS11, Bru12, BDH11, BEM15, CFOR12, CCM17, CZF12, CZLC14, Che15, CMA14, DM18, DL15, DMS<sup>+</sup>16, DG15, DLZ<sup>+</sup>16b, Edw17, FLH13, Fri10b, FD11, FSX12a, zGXW12, GKM16, GGH14, GFBF12, GT12, GV14b, GHKL11, GM14, GZS<sup>+</sup>18, Hv512, HSM14, HLLG18, Har16, HL10b, HP14, HTZR12, HMCK12, HLC<sup>+</sup>18, HLKL15, HIS18, HK14, HLH19, IL15, Jac16, JHW<sup>+</sup>19, KW14, KME<sup>+</sup>12, KYEV<sup>+</sup>18, Kip15, KH10, LJS<sup>+</sup>14, LL15, LH12, LYZ<sup>+</sup>13, LTH<sup>+</sup>15, LTZ16, LSLW15, LLGJ16, LSQL18, LY15, LHL15, LMLL12, LSC12, MLO17, MMP14, Mal13, MVVR12, MMS17b, MK12a, MKAA17, NBZP17, NDG<sup>+</sup>17, NR12, NMS14, NNSMS14, PB12, PSM17, Per13, PBC<sup>+</sup>17, PRN<sup>+</sup>19, QZL<sup>+</sup>16b, QZDJ16, QZZ18, RMP10, Rea16, RSGG15, SAM<sup>+</sup>19, SNJ11, ST19, SZS14].

SSAF11, SVG16, SYW17, SYC+17, SMS14, SZDL14, SGH15, SLy+16, SR12b, SM18, TB18, TCl15, TWZ11, TG12, TGC16, VMV15, WgMW12, WKB16, WXLY16, WLY17, WDC11, WHL15, WBA17, WWH12, WMS+12, tWmC12, XWS16, XJW13, XLP+18, YNR12a, YNR12b, YTH17, YHK+10, YKC+11, YAM+15, YGD+17, ZZX+11, ZDL12, ZVH14, ZVG16, ZHT16, ZLW+17, ZHZ+19, ZBR11, AHS14, APK+18, ABBD13, ACF16, AKK+17, ACD+15, BOB13, BHH19, BSR+14, CCLL11, CSD18, CLJH13, CW14a, CS11, CDL18, FHH10a, FLL+14, FSGW12, FA14b, FIO15, FSl18, Gal13, GAI+18, GLL+18, GCH15, HGWW11, HWK+15, HLYS14, HTC17, HPY10, IB11, JZS+10, KPP16, KKA14, KRM+10, KTU16, KDW+17, LLLS13, LDLAM12, LH11a, LLW16, LSR13, LWW+18, LCT+14, LAL+15, LL16a, LL16b, LBOX12, MR14c, MHY+18, NRI17, NACL12, NAL17, PSO+12, PL Swedish10, Rao17, RG10, RYF+13, RITF+11]. secure [RL15, SGGR+16, SYL13, SWW+16, SS11, SSPL+13, SXL16, Tan10, TLM13, TLL12, VS11, WLZ+16, WMX+17, WDKV19, WCH18, WLI19, WXSC14, XXX15, YC12, yYqWgC13, YZ+14, YZCT17, YQOL17, YYY11, YLS12, YMSH10, ZLY10, ZCLL14, ZZ15, ZYC+17, ZG10, ZZ12, ZX11, ZY17b, ZC12, Zhu13, ZSW+18b, Ano12, DSLB18, HRK18, OKG+12, YSS14, YFK+12]. Secure-TWS [OKG+12]. Secure [LC17, SG18]. SecureLR [JW19]. Securely [CC10, KP17, LH+14, MS16, WYY+17, BC18, der10]. Securing [BK12b, CML15, CST+17, NPH+14, PMZ13, SFE10, SMK18, SLJ11, Stat5b, TKR14, YMA17, YT12, CR10, Din10, SKS+18, SA15, Tox14]. Securities [WWL+14]. Security [ABJ13, AHN+18, ASBdS16, Ano13d, Ano15a, Ano15d, ABF12, AN15, ABHC+16, AYS15, BCR+10, BAI8, BCM+15, BTR12, BPR14a, BPR14b, BLS12, BCGN16, BDPS12, Bra15, BDH11, BP10, CFST17, CFE16, CHS11, CFXY17, CCD15, CPS16, CM11, DDS12, Dan12, DR12, DK16a, DFK17, FMA+18, Fid18, FSX12b, FSX12c, GZZ+13, GSC17, HC12, Hel17, Her19, HB17, HSUS11, HLW12, HXC+11, HLC11, HLT+15, HLN+10, IS12, IKR+16, JN12, Jia14a, KBL11, KS18, KFG12, KSD+17, KD12b, LPS12, LST12, LW11a, LB14, LLPY19, LW12, LLZ+17, LTW11, LSQE18, LP12, LRW17, LZC12a, LDB+15, LMS16, LLH18, MTY11, MKN13, MCS+15, MH14, Mau12, MV16a, MG+19, MLB12, MPM+17, Nac12, NNAM10, NDC+17, NVM+17, Nos1, Nos1, OSH16, ORM16, OS16, Pas13a, PZPS15, PDHN15, PS14, PL16, PDT12, FNRC17]. Security [RCP+18, RQD+15, RWZ12, Rog16, RS10, SG18, SN10, SNJ11, SBS+12, Sar12, Sch13, SD12, Shi11, SLM10, STC11, Sti19, SMOP15, SCGW+14, Tso13, TV15, Wal18, WYCF14, WSA15, WSS12, WCL+18, WS14, Yan10, YZLC12, YSF+18, YGS+17, YSS14, Yon11, Zha15b, ZY17a, vTJ11, AM18, AB10a, Abe10, ABGR13, ABM+12, Ano11a, AD17, BYL10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTIP13, CLC10, CVG+13, DLK+16, DHW+13, Edw14, FHM+12, FA14a, Fei19, Fis15, GH19, GM16, GLM+16, GMS11, GH12, HWD16, HWG10, HLR11, HRS13, HLV10, KSA16, KKK+16, Lan10, Lan13, LH10a, LXMW12, LHH11, LZC14, LSG16, MZA+13, Men13b, MM14b, MSY+18b, NS10, Nam19, NCL13, NLYZ12, OK18, OYH14B, PHWM10, QYW16, Rec15, RPSL10, RH10, SA12, Ser12, SLZ12, SY15b, Sir16, Sta11a, Tan17b, TODQ18, UUN11]. security [VCK+12, WCFW18, XCL13, Zha15a, XW12, YKC+12, Bar12]. Security-Aware [LMS16, GH19]. security-enhanced [AM18]. security-modified [MM14b]. SEDURA [LY15]. Seed [AS17, LYHH14, Sun11]. seeing [Tox14].
seen [Goo12]. Segment [WOLP15].
Segmentation [WYW+13, ZZCJ14]. selectable [GLM+11]. Selected [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12]. Selection [KD12a, RP12, SEY14, FXP12]. Selective [BTHJ12, GDC16, LW12, LSC+15, LZC12a, LLH18, LSC14, LW13c].
Selective-Opening [LLH18]. Self [Cer18, CLL16, CHHW12, CSV15, DM18, HZ11, LCL+17a, LLPY19, LH12, LHM14, PRGBSAC19, SAA15, SM12, TAP19, WHZ12, XWXC14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11].
Sensitive [Kaw15, RQD+15, Tan15a, QCX18]. Sensitivity [YGD+17, LW+10]. Sensor [ABC+17, BN14, CS14, DS11, KH10, LLC11, LLZ+12, NNAM10, NYR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YM16, ASO14, APK+18, AIB+16, AIKC18, ADZF12, BLAN+16, BBB16b, CDGC12, CLSW12, DSCS12, DLN13, HTC+10, JNUH17, JMW+16, KLC+16, KLW+16, KDW+17, LC17, LNK+18b, PL16, SZMK13, SKK10, Wan13, WW14, WXK+17, XWDN12, XMHD13, ZYL+10]. Sensors [DL12, LK+17]. Sensory [SXC14]. Seoul [LH10a, LW11a]. separation [MJIS13].
Sequence [PFS12, WGWZ+12]. Sequences [ADD10, Kla10, NN12, XNP+18, XYZ11, HLC12, VM14].
Sequential [GLR10, GLR13, LLY15, WYL13]. Series [BJL16, Die12]. Serpent [PC16]. Server [BCO13, Che15, GMSV14, LSQL18, LYL15, YLW13, ATKH+17, CSD18, CLHJ13, FA14b, FHZW19, HDPC13, HL14, ISC+16, KMTG12, LXMW12, LH13, SY15b, hSZZ15, SSSAF11, SSS11, TLL12, WT10a, XHM14].
Service [BBK14, CCS14, Hay13, LDB+15, LBR12, NRZQ15, RSG15, SPG+19, SPC12, St15, VS16, AabT16, KPP16, LHL+18, LW13a, MMP19, ML616, Par12b, Wu17, YW140b, ZX11, YCM+13].
Service-Based [LDB+15]. Service-Oriented [RSG15]. Services [Ano11b, DL+16b, MEF12, OO12, ZHL15, AZPC14, CSD18, CHX13, GAI+18, IMB17, IG11, NZL+15, PPI11, WDK19, XX15].
Session [BS12, BJKP12, CFST17, SH12, AN15, DCAT12, SHBC19]. Session-Based [BJK12]. Set [Cor14b, EKP+13, YZ12, Con12, TMK11]. set-valued [TMK11]. sets [SF12]. Setting [BKLS12, HHP17, MZHY15, TYM+17, XXZ12, ZHL15]. Settings [GZ12]. setup [Jia16]. Several [Sas12, ZT14]. SGX [WBA17]. SHA [AAE+14, ABM+12, App15, jCPB+12, LC17, MAK+12, SKP15]. SHA-1
ABB+14, ADH17, BM13, BGG+13, FMA+18, HT13, KJN+16, KAS15, MMP19, MA17, Maz13, MHV15, NRI11, PPA18, WWW17.

Survival [YCM+13, MMS+17a], Synchronizing [CFST17]. SVP [MU12, WDDW12, ZLDD12, ZLDD14]. Synchronized [KRB15, DG15, GOPB12, Har16, HHS+16, ADI11, Ano10, CZLC12a, CZLC14, Cor14b, HYS18, WZM12, LY16, LNZ+13, MR14b, OŚ12, PRSV17, QZL+16b, RST15a, BGG+17, BGG+19, IAD10, JN12, JWJ+17, YK18, Taylor16]. Symmetric-Key [BBC+12]. Sylvester [SS10b]. Symmetry [SGS14]. Symmetry-Based [KRB12]. System [KRB10, ACM11, Ano10, IEE10, IEE11b, IEE13, Wat10, Ano11a]. System-Level [JWJ+17]. System-on-Chip [HZS+19]. Systematic [CCG+16, CBL13, PC16]. Systems [AN12, AB15, BL15, BS13b, BTCPL6, BB10, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HLN+10, HK18, LMD16, LQY10, LY16, LNZ+13, MR14b, OŚ12, PRSV17, QZL+16b, RST15a, BST15b, SFS+15, SFK15, SV+16, SKH17, SGC14, SDM+12, STC11, TKR14, YNR12a, AT10, ATI+10, CFVP16, CFZ+10, CLZ+17, dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DZS+12, EIS10, FXP12, GOMGC15, GHD19, GSN+16, GPVcBRO12, HZW18, JSK+16, JHCC14, KSA16, LCL+15, LWK+18, MLMSMG12, MGP10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRB+12, WS14, YSM14, ZVH14, Zhu13, MA17, Ano11a]. SYSTOLIC [MCDB12]. SYSTOLIC-ARRAY [MCDB12]. SZK [MX13].

Technique [HEK18, KBL11, ZLDD14, BBBP13, CPPT18, GCSÁddP11, Nam19, SM12, SSKS+18, TS16a, ZWS+18].

Techniques [Bis17, DA12, GOS12, HPC10, HL10b, LW12, Mor12, PJ12, AB10b, BM13, FGPGP14, Gil10, HT13, KHF10, LH11a, OO18, VN17, WMX+17, Joh10].

Technologies [SJZG19, JAE10, JAS+11, Lan10, MMP19].

Technology [Ano19b, CGB+10, Fol16, IEE11a, Wu16, Ham19, IMB17].

Telecare [LWK+18, MA17]. Telephony [SKEG14].

Television [DTE17]. Tell [Cer14].

Template [NGAuHQ16, SKV12, ATI+10, GCS AddP11].

Templates [DWB12, AHM+18].

temporal [JMW+16, XMHD13].

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

Tenant [TV15].

terahertz [WW13]. Term [SKV12, CFVP16].

termination [SRB+12].

TERMinator [MTM18].

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

Testable [RMP10].

tester [RPSL10, SY15b].

Testing [Cou12, SS12a, AY14a, BJR+14]. Tests [GLG12, MS12b, Sim15a].

Texas [IEE13].

Text [GdM16, SMK18, XZZ18, CR12, SI12, SWW+17].

Text-dependent [GdM16].

Textbook [PP10a]. Texture [TSH17].

Theft [Ber12, Ber17, BTPMLST15].

Their [CZLC12b, CK18, FVJ19, JS18, JSK+17, NR12, CQX18, Hof16, IK15, KK10, Mat19, Sti11].

them [HLV10, JSK+16, Rus15].

Theological [SS10c].

Theorem [Lau12, HF14a].

Theorem-based [Lau12].

Theoretic [CVM14, MAL10, WSS12, CDGC12, SD10, SKEG14].

Theoretical [KL13, ZZ15, Gas13].

Theoretically [TWZ11].

Theories [ABR12].

Theory [ACM10, ACM11, CCKM16, CDFZ16, CDFS10, Cra12, FGM10, FBMI2, FS15, Res12, LW11a, Lin14b, Nac12, Per13, PJ12, RBHP15, RST15a, RST15b, Sah13, SAKM16, Sha10, Wes16, Yun10, Abe10, AB10b, BuI10b, CFR11, Gil10, LPZJ15, MZA+13, McG11, YTM+14, Cra12, Lin14b, Sah13, vDKS11].

theory-based [LPZJ15].

There [Cer15, Mc10, Mc11, SM13].

Thin [Chi16].

things [FQZF18, AAC+16, CLF+17, Ham19, HZL18, JKAU19, LNK+18b, LGH+17, NLLJ12, NLY15, PLGMCdF18, SB17, SS19, WCCH18, YCT15].

Third [jCPB+12, OSH16, QZL+16b, Sen10, BL10, ED19, Kip13]. Third-Party [OSH16, QZL+16b].

Third-Round [jCPB+12].

Thirteen [AP13].

Thou [BDK11].

Threat [CSY18, ALL+18, Ven14]. Threats [AJA16, ERLM16, GSC17, LJS+14].

Three [CZ15a, HXC+11, LLY+18, LZC+12b, PC16, Shi11, YKNS12, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].

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

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

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

Threshold [CT11b, Cil11, FGM10, GLW13, HYS11, LWL10b, SSU12, Sta12, Tan11, WYC14, WLH15, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, HH15, OO10, QD16, SES+16, Shy15, SG16, TD14, ZXJ+14, ZPY12].

thresholding [PC14].

through [Sch12b]. Throughput [MAK+12].

Thr [SYC+17, SYW17].

Thwart [LJS+14].

Thwarting [XTK10].

Ticket [XHCH14].

Ticket-based [XHCH14]. tickets [LMJC11]. tied [Men13b].

Ties [PYM+15]. Tight [GDCC16, LPS12, LLH18].

Tightly [HLLG18].

Time
[ASBdS16, Ano17d, App14, AYS15, BJL16, Che17, FD11, GSC17, HC17, HGT15, IF16, JWJ+17, JEA+15, KME+12, LCL+17a, LFX+18, NA10a, Nov10, PNRC17, Ste15b, WLZL12, YE12, AY14a, Ano15d, BM15, CC14, DCAT12, FHH10a, GPLZ13, HU15, LW10, LW13b, LML+13, MK11, Ano16g].

[SB18, BTPLST15]. **Trends**
[Fri12, GCK12, ZMS14, JAE10]. Triangular
[AMVZ12]. **Tricks** [GY13]. Trigger [SS19].
trimmed [TTL10]. **TRIMS** [MGP10].
**Triple** [LW13b, MS12a]. **triple-base**
[MS12a]. **Triple-image** [LW13b]. **Triplet**
[JS18]. triumphant [McG11]. **Trivium**
[MS12b, SR12a]. **TRNGs** [YKS10].
**Trojan** [NDC+13]. **Trojans** [BRPB13].
True [FRT13, LTKP16, Fag17]. **TrueErase**
[DMS+16]. **Truly** [LA10]. **Truncated**
[KWS+12, WW12]. **Trust** [Bar15, BCK17, Gli12, GM14, GSFT16,
IGR+16, KMSM15, KGP12, PYM+15,
PH12b, PAS13b, Rau15, TMGP13, TV15,
WLY+15, Zha15b, CO11, KGO10,
MLMSG12, MGP10, Sch12b, YT11a].
**Trusted** [AWSS17, EAA12, FPY15, YCR16,
ED19, HTC+10, Küp13, ZXLW15].
**trustworthy** [KM10b]. **TPP** [ATK11].
**TTP-free** [ATK11]. **TTPs**
[KGO10, TAKS10]. **Tulip** [JB11]. **Tunnel**
[VDB+16, ZBR11]. **Tunnel-based** [ZBR11].
**tunnels** [Cri16]. **Tunny** [Cop10a]. **Turing**
[Orn16, Bli12, Car10, CS12, Don14, Hai17,
Hel17, KSU13, LCKBJ12]. **Turtle**
[WZCC18]. **Tutorials** [Lin17]. **Tutte**
[Hai17]. **TV** [CCSW11]. **Tweakable**
[CMLRHS13, LST12, MLCH10, Sar11,
Zha12], **tweet** [BTW15]. **twelve** [BCV12].
**twice** [BM15]. **TWINE** [KDH13, TY16b].
**Twins** [Bow11]. **Two** [Ash14, Brn12,
CTL13, DZ14, ED19, GGH14, GLW12,
HL10b, HP14, KMTG12, KOS16, KU12,
LLC11, Lit14, NSMS14, OTD14, YSL+10,
YWL13, ZM16, AN15, CSD18, CHS11,
DHW+13, FIO15, HPC12, HWDL16,
HW12, JLT+12, JMW+16, Ken11, Lit10,
McG11, QYW16, Rus15, SM10b, hSZ15,
WW14, Wat14a, YT11b, ZZC15, GHKL11].
**two-channel** [JLT+12]. **Two-Factor**
[LLC11, ED19, Lit14, JMW+16, Ken11,
WW14, Wat14a]. **Two-Party** [Ash14,
HL10b, HP14, KOS16, NSMS14, ZM16,
FIO15, HPC12, HWB12, ZZC15, GHKL11].
**Two-Round** [GGHR14]. **Two-Server**
[YLW13, KMTG12, CSD18]. **Twofish**
[MD12a]. **TWS** [OKG+12]. **Type**
[AKP12, CFL13, PFS12, SH15, BNS17,
SYL13, WB12]. **Type-based**
[CFL13, SYL13]. **Type-Flaw** [SH15].
**Types** [BCEM15].

**U.S.** [Maf16]. **Ubiquitous** [OS16, Par12b].
**UESDE** [YZ12]. **UHF** [HQY+16, PPH12].
**UK** [Che11, PJ12, vDKS11, Ano15e].
**Ukraine** [OGK+15]. ultra
[AATM18, GW14, TG17, WCFW18].
**ultra-lightweight**
[AATM18, TG17, WCFW18].
**ultralightweight**
[ACM12, GMSW14, SB17]. **UMTS**
[OHJ10, TM12]. un-traceability [Chi13a].
**Unattended** [BN14]. unauthentic
[MLMSG12]. **Unauthorized** [CBO+18].
**Unbounded** [LW11c, YZ12]. unbreakable
[Bha16]. Uncalibrated [SGP+12].
**uncensored** [Ald11]. **Uncertainty**
[FHS13, BBGT12]. Unclonable [Ano16e].
**Unconditional** [Jia14a]. Unconditionally
[CFOR12, LHF12, SNJ11].
**Unconditionally-Secure** [CFOR12].
**uncorrelated** [MSM+18b]. Uncovering
[FMS12a, WBC+10]. **Unciphered**
[Rao10]. **Undeniable** [BH12].
**Underbelly** [Her19]. underfeeding
[BBBP13]. **underhanded** [Cra14].
**Understanding** [EPAG16, PP10a, Bar12].
**Undetectable** [CEL+19]. **Undisturbed**
[YCL17]. **Unexpanded** [SA16a].
**Unforgeable** [HH17]. Unidirectional
[LSC12, DKL+16]. **Unified** [ZSW+12].
Uniform [HZS+19, QIC+18]. uniformly
[YYKL12]. Unilaterally [GRL12].
**Unintended** [Ess17, SS19]. union
[BBDL+17, Bud16]. Unique
[SSPC12, SOS15]. Unit
[PP10b, Sta13, MS13a, MS13b, MS13c].

VANETs [PZBF18, WLZ+16, Wu17]. **Variability** [VDB+16, SHBC19]. **Variable** [CHHW12, CMMS17, XNP+18, DTZZ12]. **variable-interval** [DTZZ12]. **Variables** [BB10]. **Variant** [AAE+14, MVVR12, ZXWA18]. **Variants** [ASS15, BB10, Hin10]. **Variation** [DWZ12]. **Variations** [DSB16, SJZG19]. **Varied** [GZ12]. **varieties** [LR15]. **Varying** [GKCK11]. **Vault** [PBC+17, KHMB13]. **VBF** [ACZ16]. **VBTree** [WL19]. **VDTNs** [PSS+13]. **Vector** [ÁCZ16, FHL19, HMKH14, JHNN12, KAW15, MH14, PTK14, QZDJ16, RS10, SE16, SSSA11, SKEG14, TBCB15, tWmC12, YWF18, Yon11, ZOC10, Zim10]. **Vichy** [Kap11]. **Vicious** [NN15]. **Vie** [ADR18, BHKN13, BCI+13, BR14, CDSLY14, CLW16, GT12, GST13, GVW12, JHW+19, LT13, LT14b, LEW19, LLKA19, MH14, PTK14, QZDJ16, RS10, SE16, SSSA11, SKEG14, TBCB15, tWmC12, YWF18, Yon11, ZOC10, Zim10]. **Vichy** [Kap11]. **Vicious** [NN15]. **win** [Pea11]. **Video** [BWR12, DG17, GKB17, JSZS12, OŚ12, TWZ+12, WLZL12, YE12, YT12, Cri16, LLHS12, MK11, OCGD11, XWZW16]. **Videos** [GZH17, JSCM17]. **Vietnam** [ABJ13]. **View** [RS16, TWZ+12, YCM+13, ZGC16]. **View-Invariant** [RS16]. **Views** [VGA15, TG12]. **Virtual** [BR14, HB17, RY10, VDO14, CDA14]. **Virtualization** [CDD13, QZDJ16]. **Virtualization-Based** [CDD13, QZDJ16]. **Virus** [WOLP15]. **Visible** [Cas10, HWYW14, LZC+12b, WZL13, Lin14a]. **vision** [BSW12, LW+10]. **Visual** [BB10]. **VMOR** [MSI18]. **Voice** [JTZ+16, WBC+10, LGCC15, RJZ14, TJC12]. **Voice-over-IP** [TJZF12]. **VoIP** [BGAD12, M13, SS10a, ZZT16]. **Volatile** [AMH+16, RM18, SM18, YNQ15, CS11]. **voltage** [BB10]. **volume** [WLDB11]. **voluntary** [WGJ10]. **Voting** [Ber16a, CFE16, CRST15, CEL+19, KV18, LHF12, LGPRH14, RST15a, RST15b, Sch10]. **Voynich** [An10d, Bax14]. **vs** [Bur11, FKO15, Mar10b]. **Vulnerabilities** [BKJP12, HSUS11, MAS16, PTD12, RY10]. **Vulnerability** [MKN13, TM12, VCK15, Wall18, An17, DMWS12, MYJR13]. **Vulnerable** [An10d]. **vVote** [CRST15].
W [Mar10a, Xie12, Hül13]. W-OTS [Hü13].
WA [LCK11], Waknaghaf [CGB+10].
Walker [Xie12], Wallets [Chi13b]. Wallis [Wes16], War [Has16, Mun17, Bud16, Car11, Smi11a].
Warbler [MFG16], warriors [Bud16].
wartime [McK10, McK11]. was [Goo12, LHA+12]. Watermark [CHHW12, DMM+18, EMW14, Jin10, KBL11, LZC+12b, MCDB12, QJC+18, SJ12, YE12, ZS12, HB13, TLL13, WYL13].
Watermark-Driven [DMM+18].
Watermarking
[BCGAPM12, BF12, BCPV11, BDB14, BM15, CG12b, CHHW12, CCZC13, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HEK18, HGT15, HHMK14, JSZS12, Joh10, JKHeY12, KD12a, LSL12b, LLY+18, LP12, LD13, MM17, MR16, MU12, NGAuH16, NC12, NXH+17, pNyWyY+14, OWHS12, RS16, RP12, RR11, RMG18, SAA15, SLGZ12, SSA13, TR18, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, gWpNyY+14, WXL+17, yWXY+18, tWmC12, XNG+14, XNRG15, XNP+18, YWNW15, YPRI17, YK18, YYO15, ZXZ+11, ZWZ17, AP10, AIA+18, AMK12, BW13, BWA13, CCLL11, CT11a, CSS+13, GHZD12, GA11, HK14, HWYW14, JK13, KPS10, KJN+16, KM11, LSR13, LXCMM11, LLHS12, Lin14a, LLY12, MMSD13, MM14a, MO14, MK11, NC13, PTK14, PWLL13, PWLW10, PGLL10, PKS18, PC14, PPR+12, RS17, SKS+18, TAY14, TK14, TTL10, TPKT12, WLDB11, yWpWyN11, Wan13, yWpWyYpN13, WZLW13].
watermarking
[YWT+12, ZZKA17, ZSMS18].
Watermarking-Encryption [SLGZ12], Watermarks [GL10, YTL12]. WAVE [BMM12]. WAVE-enabled [BMM12].
Wavelet [AGW15, LSL12b, MR16, Ara13, AMK12, BW13, LXCMM11, MO14, yWpNyYL11].
Wavelet-Domain [MR16]. wavelets
[MMSD13]. Way [CP16, DSM14, Mat14, HRV10, LP11, RK11]. WBAN [KS18].
WBANs [KIH19]. Weak [BF11, DY13, HDWH12, PYM+15, Pud12, JGIM15, RH10]. Weakening [SFKR15].
[BCTPL16, XJR+17, GTS19, LIK+17]. Wearout [DFK17]. web [GP+12, IMB17, KRM+10, KGO10, ATKH+17, BS12, BKJP12, CTC+15, CFST17, CD12, DR11, Fra16, HCM11, SP15a, SPM+13, ZGC16].
Welchman [GW14]. Well [JCM12]. were [McK10, McK11]. Western [Han12]. WG [GLC10, DJG+15, ERRMG15, ZAG19].
WG- [ERRMG15]. WG-16 [ZAG19].
Where [CMG+18]. Wherefore [BDK11].
Whit [LHA+12]. White [BW16, BCGN16, Mic10b, DD13, YSC16, ZSW+18a].
White-Box
[BW16, BCGN16, Mic10b, ZSW+18a].
Whitfield [Hof16]. who [Bat10, Bha16, Car11, Fag17, Hea15, Kap13, McK10, Mck11, Mck12, Moo14, XTK10].
Wicked [SGH15]. Widespread [HDWH12].
 wildcard [HH16]. Wilderness [Ac11].
Will [Mos18]. win [Smi11a]. window
[Win17]. windows [BBG+17], Wine [Che17]. Wineskin [Che17]. wins [Ano16g].
wire [ADG16, ZZCJ14]. wire-tap [ADG16].
Wireless
[ABC+17, BN14, BOB13, CBO+18, CS14, DPCM16, DS11, FLH13, HZC+12, HBC13, KH10, LLC11, LHM+15, LZCK14, LWCJ14,
LLZ+12, NNAM10, PCPK14, RCW15, RWLL14, SWYP12, SP15b, TCN+17, YM16, ZLDD12, APK+18, A1b+16, AIKC18, ADF12, BLAN+16, BABB16b, CDGC12, CML+18, CLSW12, CL11, DSCS12, HGWW11, HZC+14, HZWW17, HCC11, HTC+10, HLYS14, JM16, KP18, KO16, KLW+16, KDW+17, LC17, LMJC11, LNK+17, LNK+18b, NDNR13, PL16, QMW17, SA12, SGJ+18, SZMK13, SCKH10, SSK10, TDKH14, Wan13, WW14, WXK+17, XHCH14, XMHD13, YHHS16, ZBR11, ZCCL14, ZLDD14, ZHH+17.

wiretapping [Lan10]. Wiring [HTZR12]. Wise [CG14a, SSA13]. WISP [PPH12]. Withholding [BRS17]. Without [ASS15, CCL+13, FZT14, GSW+16, GKS17, LTC+15b, NA10a, YLA+13, AZH11, BT12, BF11, BGV14, CCW+10, DCA18, FSX12a, GH11a, GST12, ISC+16, LLY15, LGWY12, RG10, SYL13, SLZ12, TAKS10, WWYY11, XQ1L11, XM1H14, YS12, YKC+11, YFK+12, ZY17b, ZYM18].


workbench [CFH+13]. workflows [BPP10]. working [Wat14b]. Workload [BCO13]. Workshop [MV12, Sen10, Yan11]. Workshops [DDS12]. World [ANO16h, ANO17d, BFK16, BPS16, FKS+13, KM10c, LLK18, MDMJ17, Tom16, Con12, GIJ+12, Goo12, LCKBJ12, Pet11, Sch15c, Zet14, Mun17]. world-class [Goo12].


Write [LLPY19, YNQ15, ZHZ+19]. Write-Efficient [YNQ15]. writing [LT14b]. wrong [LHA+12, UK18]. WSN [DL12]. WSNs [ABB19, ZYL+10]. Wu [LLLK10].


Z [JSM+18]. z13 [ACD+15]. Zero [AMH+16, BW12, CLP13a, COP+14, GJO+13, GOS12, IW14, LLM+19, MX13, MBC+18, MT12, OOR+14, Pan14, SJ12, WCL+18, YCL17, Zet14, AIA+18, KPP16, TLL13, WWBC14]. Zero-Correlation [BW12, YCL17, WWBC14]. Zero-Cost [AMH+16]. Zero-Knowledge [CLP13a, GOS12, IW14, MX13, MBC+18, MT12, Pan14, LLM+19, KPP16].


References

REFERENCES


[AAT16] Sedat Akleylek, Erdem Alkim, and Zaliha Yüce Tok. Sparse polynomial multiplication for lattice-based cryptography with small complexity. *The Journal of Su-
REFERENCES


REFERENCES

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

[ABB⁺14]

[Almeida:2013:CCA]

[Athmani:2019:EED]

[Arnold:2012:ICC]

[Ateniese:2017:LCS]
Giuseppe Ateniese, Giuseppe Bianchi, Angelo T. Capossele, Chiara Petrioli, and Dora Spenza. Low-cost standard signatures
REFERENCES


**Ambrosin:2017:OBB**


**Adrian:2015:IFS**


**Agosta:2015:OPP**


**Abe:2010:ACA**


**Abe:2012:TBG**

Masayuki Abe. Tools over bilinear groups for


REFERENCES


Acar:2013:SPA


Andreeva:2012:SAS


Arapinis:2012:RET


AlMashrafi:2012:AIM


Applebaum:2010:PKC

Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions.
REFERENCES

In ACM [ACM10], pages 171–180. ISBN 1-60558-817-2. LCCN QA 76.6 [ACF16]
Arias-Cabarcos:2015:BIP
Patricia Arias-Cabarcos, Florina Almenarez, Ruben Trapero, Daniel Diaz-Sanchez, and Andres Marin.

[ACAT+15]

Arnold:2015:NGH

[ACD+15]

Amoah:2016:FMA
Raphael Amoah, Seyit Camtepe, and Ernest Foo.

[ACK+10]

Ardagna:2010:ECP
Claudio A. Ardagna, Jan Camenisch, Markus Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio.

[ACM10]

ACM:2011:PAI


Avoine:2012:PFS


Austrin:2017:ICT


Aczel:2011:SWL


Álvarez-Cubero:2016:AVL


Aizatulin:2012:VCC

Anyanwu:2010:DCS


Ayday:2012:DAA


Aliberti:2016:RPS


Attasena:2017:SSC


Adikari:2011:HBT


Abdalla:2012:LBH

Andrychowicz:2016:SMC


Araldo:2018:CEC


Ahmed:2017:IRD


Attrapadung:2015:RGS


Antonopoulos:2017:DIS


Akinuye:2014:MGA

REFERENCES

Abdullaziz:2016:AAI

Ahani:2015:SRB

Attrapadung:2012:ABE

Ali:2018:ECM

Akhhtar:2018:BSI

Appelbaum:2013:SSG
J. Appelbaum, J. Horchert, and C. Stöcker. Shopping for spy gear: Cata-
log advertises NSA tool-
box. Der Spiegel, ??(??):??, 
December 29, 2013. URL 
http://www.spiegel.de/
international/world/catalog-
reveals-nsa-has-back-
doors-for-numerous-devices-
a-940994.html.

[AHS14] 
Murat Ak, Turgut Hanoy-
mak, and Ali Aydin 
Selçuk. IND-CCA se-
cure encryption based on 
a Zheng–Seberry scheme. 
Journal of Computational 
and Applied Mathematics, 
259 (part B)(??):529–535, 
March 15, 2014. CODEN 
JCAMDI. ISSN 0377-0427 
(print), 1879-1778 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0377042713003403.

[AIA+16] 
Mahdi Aiash. A formal 
analysis of authentication 
protocols for mobile de-
vice in next generation 
networks. Concurrency 
and Computation: Prac-
tice and Experience, 27 
(12):2938–2953, August 25, 
2015. CODEN CCPEBO. 
ISSN 1532-0626 (print), 
1532-0634 (electronic).

[Ala18] 
Zulfiqar Ali, Muham-
mad Imran, Mansour 
Alsulaiman, Muhammad 
Shoaib, and Sana Ul-
lah. Chaos-based ro-
 bust method of zero-
watermarking for medical 
signals. Future Gen-
eration Computer Systems, 
88(??):400–412, Novem-
ber 2018. CODEN FG-
SEVI. ISSN 0167-739X 
(print), 1872-7115 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0167739X18304709.

[AIA+16] 
Ruhul Amin, SK Hafizul 
Islam, G. P. Biswas, Muham-
mad Khurram Khan, Lu Leng, 
and Neeraj Kumar. De-
sign of an anonymity-
 preserving three-factor au-
thenticated key exchange 
protocol for wireless sen-
sor networks. Computer 
Networks (Amsterdam, Nether-
lands: 1999), 101 
CODEN ????? ISSN 1389-
1286 (print), 1872-7069 
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1389128616000207.

[AIK14] 
Benny Applebaum, Yuval 
Ishai, and Eyal Kushile-
vitz. How to garble arith-
metic circuits. SIAM Jour-
nal on Computing, 43(2): 
905–929, ???. 2014. CO-
DEN SMJCAT. ISSN 
0097-5397 (print), 1095-
7111 (electronic).
Amin:2018:UAP


Alhanahnah:2016:MTI


Azarderakhsh:2014:NDP


Almulla:2013:CKE


Anada:2017:CGS


Alabdulatif:2017:PPA

REFERENCES


[ALL+18] Man Ho Au, Kaitai Liang,


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


REFERENCES


REFERENCES

Anonymous:2015:CEB


Anonymous:2015:QCS


Anonymous:2015:UGB


Anonymous:2016:CPSd


Anonymous:2016:CPSe


Anonymous:2016:EMT


Anonymous:2016:FVM


Anonymous:2016:GUP


Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

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

Anonymous:2017:BRM

Anonymous:2017:CCS

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

Anonymous:2017:HDQ


Anonymous:2017:MBH


Anonymous:2017:RV


Anonymous:2019:HCC

REFERENCES


[APK+18] Rifaqat Ali, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah,

**Applebaum:2013:GXG**


**Applebaum:2014:CCP**


**Albrecht:2015:FBR**


**Al-Qarni:2012:EI**


**Appel:2015:VCP**

Arai:2013:MDH


Adj:2014:SRC


AlTawy:2018:TCM


Azarderakhsh:2015:PHS


Ambrose:2012:RII


Asharov:2016:LPI

REFERENCES


Andrade:2016:LEP


Asaro:2014:TCC


Al-Sinani:2012:UCB


Ahmadi:2011:SKC


Ahmadi:2012:SKE

REFERENCES


Asaar:2015:IBM


Alsulaiman:2013:IVB


Altman:2010:AAP


Argyropoulos:2010:BTP


Au:2011:PPT

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

Al-Tariq:2017:SFP


Alam:2015:ACF


Alaslan:2016:DEM


Abdalla:2012:LRS


Altaf:2015:LPM


Altaf:2017:LHL


Apavatjr:2012:EEA


Alshammari:2011:CET


Behnia:2013:IEB


Blaner:2013:IPP


Elaine Barker. Recommendation for key management. Part 1: Gen-


REFERENCES

Boumerzoug:2016:LKM

Barenghi:2013:FIT

Baldi:2013:ULC

Barak:2014:OEF

Beurdouche:2017:MSU
REFERENCES

Beimel:2014:MLS

Bernstein:2017:SRD

Boldi:2012:IUG


REFERENCES

Bochur:2018:HEB


Balagurusamy:2019:CA


Bichsel:2012:DMA


Badrignans:2010:SSA


Balfanz:2012:FA

REFERENCES

2012. ISSN 1540-7993 (print), 1558-4046 (electronic).


[Bahri:2016:CCO] Leila Bahri, Barbara Carmi-
nati, and Elena Ferrari. COIP-continuous, operable, impartial, and privacy-aware identity validity estimation for OSN profiles. ACM Transactions on the Web (TWEB), 10(4):23:1–23:??, December 2016. CO-


REFERENCES


[BCL14] Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja


Basin:2012:PRI


Basin:2013:PRI


Basin:2015:ISC


Bicakci:2013:LSS


Botta:2014:PCI

REFERENCES

Boyle:2014:EO

Basso:2011:BWC

Bessani:2013:DDS

Blasco:2016:SWB

Biddle:2012:GPL

Barker:2015:RKM
REFERENCES


[BDE11] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou R3579X?: anonymized social networks, hidden patterns, and structural steganography. *Communications of the Association*
REFERENCES


REFERENCES

Keccak-implementation-3.2.pdf.

**Boldyreva:2012:SSE**

**Bitansky:2013:WFS**

**Bellovin:2016:EEE**

**Bellovin:2018:UAE**

**Bellovin:2019:LI**
REFERENCES


REFERENCES


[Bos:2019:ACI]

[BF19]

[Bhargavan:2012:VCI]

[BF16]

[Bhargavan:2016:MVP]

[Bobba:2010:ABM]

[BFK16]
Beimel:2012:SSS


[BFM12]

Berger:2016:EGF


[BFMT16]

Boldyreva:2014:MEW


[BG14]

Battistello:2012:TBA


[BGAD12]

Barthe:2012:CACb


[BGB12]

Bossuet:2013:AFS

REFERENCES

41:??, August 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).


Borcea:2017:PEE


Bhattacharjee:2016:SWC


Blasco:2012:FAS


Behnia:2012:SEI

Rouzbeh Behnia, Swee-Huay Heng, and Che-Sheng Gan. Short and efficient identity-based un-


REFERENCES


**Benhamouda:2016:NFP**


**Brubaker:2014:UFA**


**Bouti:2012:SCB**


REFERENCES

org/content/57/4/537.
full.pdf+html.

Braun:2012:ULA

Brakerski:2010:OHB

Bogdanov:2012:KAC

Bogdanov:2013:SDS
ISSN 1545-5963 (print), 1557-9964 (electronic).

Bellare:2012:IBL


Bothe:2013:EPS


Byun:2011:SMC


**Bai:2012:SSR**


**Bernstein:2017:SCS**


**Blanc-hette:2012:BPC**


**Blaze:2016:UHR**


**Benzaid:2016:FAW**

Chaïka Benzaid, Karim Lounis, Ameer Al-Nemrat,
REFERENCES


Bai:2019:LMD


Buc:2017:PCU


Buchmann:2018:PCP


Buchmann:2018:PCP

Baires:2015:IDM


Blomer:2012:TKG

Blondeau:2015:IDA

REFERENCES


[BMBS10] Adrian Baldwin, Marco Casassa, Mont, Yolanta Beres, and...

**Biswas:2012:IBA**


**Backes:2012:GCP**


**Banik:2012:DFA**


**Babamir:2014:AKP**


**Buckley:2015:RVV**


**Bunder:2017:GAR**

Martin Bunder, Abderrahmane Nitaj, Willy Susilo,

[Biryukov:2014:DEA]

[Ben-Othman:2013:IHN]

[Bohme:2010:ASS]

[Boneh:2012:PBC]

[Borghoff:2010:CLC]


Bellare:2014:SSEa

Bellare:2014:SSEb

Boneh:2016:BCR

Balsa:2017:TIC

Brakerski:2014:VBB

Brakerski:2013:WHB
Bradbury:2015:BSB


Briggs:2011:SDC


Broemeling:2011:AES


Brook:2017:LSR


Becker:2013:SDL

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

Benaloh:2015:EEV


Bag:2017:BBW

Bellare:2012:MIS


Brumley:2012:SFI


Bergsma:2012:PAW


Bajaj:2013:CSE


Birrell:2013:FIM


Bhattacherjee:2014:CA


Bagheri:2015:NNA

REFERENCES


REFERENCES


Brocardo:2015:AVM


Buchmann:2010:EKG


Bulygin:2010:AOP


Bulygin:2010:CA


Burke:2011:AMD

Brakerski:2011:EFH


Brakerski:2014:EFH


Bitansky:2018:IOF


Bayrak:2012:AII


Baek:2013:SPK


Bogdanov:2012:ZCL


Bhatnagar:2013:BIW


REFERENCES

the Association for Computing Machinery, 57(5): 8, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Caldwell:2013:INP


Carter:2010:TB


Carlson:2011:JRW


Casselman:2010:VC


Cobb:2013:LMS


Chang:2018:DMU


Cachin:2010:EKS

Christian Cachin and Jan Camenisch. Encrypting keys securely. IEEE Se-


REFERENCES


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


Chatterjee:2017:PBS


Cho:2014:DGA


Chen:2011:EAA


Chu:2014:KAC


Chen:2010:ALD


Chen:2013:WSB

Guoming Chen, Qiang Chen, Dong Zhang, and
REFERENCES


De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. The-145
ory of Privacy and Anonymity, chapter 18, pages 1–35. Volume 2 of Atallah and Blanton [AB10b], second ed-

Choo:2016:CCT

Kim-Kwang Raymond Choo, Josep Domingo-Ferrer, and Lei Zhang. Cloud cryptography: Theory, prac-
science/article/pii/S0167739X16300942.

Cao:2012:ITM


Chari:2010:DSC

uni-trier.de/”ley/db/conf/cardis/cardis2010.
html#ChariDKPRRRSST10.

Cui:2018:ABC

Hui Cui, Robert H. Deng, and Yingjiu Li. Attribute-based cloud storage with secure provenance over en-
www.sciencedirect.com/
science/article/pii/S0167739X17322835.

Coras:2016:AML

Florin Coras, Jordi Domingo-Pascual, Darrel Lewis, and Albert Cabellos-Aparicio. An analytical model for Loc/ID mappings caches.
REFERENCES


Costello:2014:Cas

Culnane:2019:KKR

Ceruzzi:2014:HFT

Cerf:2015:CTN

Cerf:2018:CSA

Chang-Fong:2016:CSC
REFERENCES


Carter:2013:SSA

Centenaro:2013:TBA

Checkoway:2014:PED

Cevалlos:2012:USR

Carstensen:2011:AAA
REFERENCES


REFERENCES

Cheraghchi:2014:NMC


Corrigan-Gibbs:2014:KS


Chaudhuri:2010:PIC


Caballero-Gil:2012:LAR


Chmiel:2012:EPC


Coull:2011:ACO

Scott E. Coull, Matthew Green, and Susan Hohenberger. Access controls for oblivious and anonymous

**Cohney:2017:PSR**


**Curtmola:2011:SSE**


**Cheng:2012:PAI**


**Chandran:2014:PBC**


**Cheng:2013:NIB**


**Chen:2010:NUP**

REFERENCES


[Chen15] Yu-Chi Chen. SPEKS: Secure server-designation...


Chirgwin:2013:ABB


Chien:2016:GAI


Chmielowiec:2010:FPR


Choudary:2010:SCD


Chou:2014:EMA


Chen:2011:SEI


Cooke:2015:FSM

[CHS15] Patrick Cooke, Lu Hao, and Greg Stitt. Finite-state-machine overlay architectures for fast FPGA

Chu:2016:BEE


CHX13


Cilardo:2011:EPT


Cao:2014:SCI


Cho:2012:CBF


See cryptanalysis [SPLICB14].

**Cho:2015:CBF**


**Chandra:2011:AST**


**Chung:2018:ERN**


**Chase:2013:SMN**


**Chang:2019:GTS**

Chuang:2011:LMA


Colin:2016:CTC


Comon-Lundh:2010:DSP


Chang:2011:RSB


Chen:2017:PGF


Chong:2013:ASG


Chen:2016:RPR

Zhenhua Chen, Shundong Li, Qiong Huang, Yilei

Chen:2012:NCB


Chen:2013:TSE


Chande:2016:NSC


Cao:2012:SRH


Canetti:2013:PCC

REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-36594-2_5/


REFERENCES

540-78636-8 (e-book), 3-642-43053-8. ISSN 1619-7100 (print), 2197-845X (electronic). xiii +
172 + 59 pp. LCCN QA76.9.A25 C74 2012;
QA76.9.D35. URL http://
/www.springerlink.com/
content/978-3-540-78636-
8.

[CM13] Margaret B. Cozzens and
Steven J. Miller. The
mathematics of encryption:
an elementary introduc-
tion, volume 29 of Math-
ematical world. Ameri-
can Mathematical Society,
Providence, RI, USA, 2013.
ISBN 0-8218-8321-6 (pa-

[CML16] Hui Cui, Yi Mu, and
Man Ho Au. Signcryp-
tion secure against lin-
er related-key attacks.
The Computer Journal,
57(10):1472–1483, Octo-
ISSN 0010-4620 (print),
1460-2067 (electronic).
URL http://
comjnl.oxfordjournals.
org/content/57/10/1472.

[CMG+18] Stephen Checkoway, Ja-
acob Maskiewicz, Christina
Garman, Joshua Fried,
Shaanan Cohney, Matthew
Green, Nadia Heninger,
Ralf-Philipp Weinmann,
Eric Rescorla, and Hovav
Shacham. Where did I
leave my keys?: lessons
from the Juniper Dual
EC incident. Communica-
tions of the Associa-
tion for Computing Ma-
chinery, 61(11):148–155,
November 2018. CO-
DEN CACMA2. ISSN
0001-0782 (print), 1557-
7317 (electronic). URL
https://cacm.acm.org/
magazines/2018/11/232227/
fulltext.

[CMA14] Patrick J. Coles, Eric M.
Metodiev, and Norbert
Lütkenhaus. Numeri-
cal approach for unstruc-
tured quantum key dis-
tribution. Nature Com-
munications, 7:11712, May
2016. CODEN NCAOBW.
ISSN 2041-1723 (elec-
tronic). URL http://
www.nature.com/ncomms/
2016/160520/ncomms11712/
full/ncomms11712.html;
http://www.scientificcomputing.
com/news/2016/05/computing-
secret-unbreakable-key.

[JCMG+18] Jin Cao, Maode Ma, Hui
Li, Yulong Fu, and Xue-
feng Liu. EGHR: Efficient
group-based handover au-
thentication protocols for
mMTC in 5G wireless net-
woks. Journal of Net-


REFERENCES

[CNRS:2014:NAS]

[Coron:2012:PKC]

[Chin:2011:ACS]

[Conitzer:2010:AP]

[Constantin:2012:RSN]

[Connolly:2018:FE]

[Copeland:2010:CBG]
B. Jack Copeland. Colossus: Breaking the German


Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, and Ivan Visconti. 4-round resettably sound zero knowledge. [Cou12]


Koen Claessen and Michal H. Palka. Splittable pseudorandom number gener-


Jason Crampton. Practical and efficient cryptographic enforcement of interval-

**Cramer:2012:TCT**


**Crichlow:2016:RSE**


**Culnane:2015:VVV**


**Chhabra:2011:NSN**

Siddhartha Chhabra and Yan Solihin. i-NVMM: a secure non-volatile main memory system with incremental encryption. *ACM
REFERENCES


Clark:2012:RLA

Chapin:2014:SRP

Chattaraj:2018:NTS

Chauhan:2018:BBA

Chadwick:2014:AFI

Chen:2013:RWM
Xianyi Chen, Xingming

Chen:2017:SIE


Chen:2012:EPV


Chen:2018:SIA


Chow:2015:SID


Chow:2012:EPV

Chen:2011:IBT


Chen:2011:ARI


Chen:2011:TVS


Canard:2018:CPK


Calzavara:2015:SLA


Chin:2013:SMB


Chang:2012:GBP

REFERENCES

Chou:2013:TIB

Crenne:2013:CMS

Calmon:2014:ITM

Choi:2012:LTF

Chung:2012:CBI

Chen:2014:SBB
Chien-Chang Chen and

Chen:2014:DSE


Cao:2014:PPM


Chen:2016:EPN


Chen:2012:CKS


Chen:2012:IDC
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-30428-6_15/

Chen:2014:MLC


Chen:2015:TCP


Cheng:2015:OMU


Chen:2012:FSD


Chen:2012:AIB


Chen:2012:IBE

REFERENCES


2. Dharwadkar:2010:SSG

3. Djebbar:2012:ASB

4. Danezis:2012:FCDb

5. Davies:2011:IST

6. Diong:2012:DAU
Mouhamadou L. Diong, Patrick Bas, Chloé Pelle, and Wadih Sawaya. Document authentication using 2D codes: Maximizing

**Dou:2018:OHR**


**DCAT12**


**Cordeiro:2012:IMB**


**Ding:2018:NPH**

Kaimeng Ding, Shiping Chen, and Fan Meng. A novel perceptual hash al-

**DePrisco:2013:CVC**


**DaArco:2014:MIC**


**DaRolt:2013:NDS**


**Datta:2017:SFH**


**Castro:2016:FVB**


**Danezis:2012:FCDa**

George Danezis, Sven Dietrich, and Kazue Sako, editors. *Financial Cryptography and Data Security:*
REFERENCES


[DF16] Quinn DuPont and Bradley Fidler. Edge cryptography and the codevelopment of computer networks and

DeCapitaniDiVimercati:2010:EPR


DeCapitanidiVimercati:2017:AMM


Deng:2017:LLH

[DFKC17] Zhaoxia Deng, Ariel Feldman, Stuart A. Kurtz, and Frederic T. Chong. Lemonade from lemons: Harnessing device wearout to create limited-use secu-

Ding:2012:CLS


Djuric:2015:FSF


Dutta:2017:EFC

[Tanima Dutta and Hari Prabhat Gupta. An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC)-


[Drimer:2010:DBP] Saar Drimer, Tim Gîniesyu, and Christof Paar. DSPs, BRAMs, and a pinch of logic: Extended recipes for AES on FPGAs. ACM Transactions on Reconfigurable Technology and Sys-


REFERENCES

November 2013. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).


REFERENCES

Delfs:2015:ICP


Delimitrou:2016:SID


Dorre:2016:ELO


Doychev:2017:RAS


Durumeric:2014:MH


Dolev:2016:MCG

REFERENCES


[DLS16] Fikadu B. Degefa, Donghoon Lee, Jiye Kim, Younsung Choi, and Dongho Won.


REFERENCES


**DiPietro:2016:CLD**


**Djaziri-Larbi:2018:WDA**


**Dodis:2011:SSC**


**Dai:2016:MLR**


**Dong:2013:PRS**


**Duan:2016:SDC**

Li Duan, Dongxi Liu, Yang Zhang, Shiping Chen, Ren Ping Liu, Bo Cheng, and Junliang Chen. Secure
REFERENCES


DeCarneDeCarnavalet:2015:LSE


Daneshgar:2018:SSS


Diesburg:2016:TLA


Dimitrakakis:2015:ELA


Demme:2012:SCV


David:2012:UCO

REFERENCES


REFERENCES

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


Deng:2018:SFE


Dachman-Soled:2014:COF


Drosatos:2017:PET

Deng:2012:VIA


Dunkelman:2012:MEK


Dunkelman:2012:TCC


Durcheva:2015:SAI


David:2012:PRE


Dorn:2012:ECE


Dong:2012:KKD


Dong:2012:NDI


Dai:2018:OPC


Dong:2012:KDD

[DWZ18] Lunzhi Deng and Jiwen Zeng. Two new identity-based threshold ring sig-


Imran Erguler and Emin Anarim. Practical attacks and improvements to an efficient radio frequency identification authentication protocol. *Concurrency and Computation: Practice and Experience*,
REFERENCES


Ekberg:2012:AEP


Ehdaie:2016:HCR


Esiner:2017:QRI


Esiner:2019:TFA


Edwards:2014:NRP

REFERENCES

Machinery, 57(8):11–13, August 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Edwards:2017:NSQ

El-Emam:2013:NSA

Eisenbarth:2012:CIP

Esiner:2016:FFB

Engels:2013:NLL

ElBansarkhani:2012:ELB
[EM12]

Embar:2014:PWO
[EMW14]

Evtyushkin:2016:UMC
[EPAG16]

Eberz:2016:LLE
[ERLM16]

El-Razouk:2015:NHI
[ERRMG15]

Estebanez:2014:PMC
[ESRI14]
REFERENCES

Engels:2012:HLA

Ebadi:2015:DPN

Essex:2017:DDU

Everett:2012:EC

Everett:2016:SES

Eibach:2010:OGB


Jason Fagone. *The woman who smashed codes: a true story of love, spies, and the unlikely heroine who


http://link.springer.com/chapter/10.1007/978-3-642-34047-5_12/.

REFERENCES


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


[Fan:2014:RRS] Kai Fan, Jie Li, Hui Li, Xiaohui Liang, Xuemin (Sherman) Shen, and Yintang Yang. RSEL: revocable secure efficient lightweight RFID authen-


[Feng:2012:CAO] Hui Feng, Hefei Ling, Fuhao Zou, Weiqi Yan, and Zhengding Lu. A collusion attack optimization strat-

**Fallahpour:2015:AWB**


**Ferrag:2018:SCN**


**Feng:2012:USD**


**Farwa:2018:FAI**

REFERENCES

Fraczek:2012:MSI  
W. Fraczek, W. Mazurczyk, and K. Szczypiorski.  
Multilevel steganography: Improving hidden communication in networks.  
CODEN ???.  
ISSN 0948-6968.  

Fernandez-Mir:2012:SRA  
Albert Fernández-Mir and Rolando Trujillo-Rasua.  
A scalable RFID authentication protocol supporting ownership transfer and controlled delegation.  
CODEN LNCSD9.  
ISSN 0302-9743 (print), 1611-3349 (electronic).  
URL http://link.springer.com/chapter/10.1007/978-3-642-25286-0_10/.

Ferreira:2015:LPA  
Anselmo Ferreira, Luiz C. Navarro, Giuliano Pinheiro, Jefersson A. dos Santos, and Anderson Rocha.  
Laser printer attribution: Exploring new features and beyond.  
ISSN 0379-0738.  
See also [?].

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.  
CODEN JS-SODM.  
ISSN 0164-1212 (print), 1873-1228 (electronic).  

Fokkink:2012:TCG  
Robbert Fokkink.  
Tossing coins to guess a secret number.  
CODEN AMMYAE.  
ISSN 0002-9890 (print), 1930-0972 (electronic).  

Folger:2016:TQH  
Tim Folger.  
Technology: The quantum hack.  
CODEN SCAMAC.  
ISSN 0036-8733 (print), 1946-7087 (electronic).  
URL http://www.nature.com/
REFERENCES


[Fathimal:2016:SSS] P. Mohamed Fathimal and...


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Authors</th>
<th>Journal/Conference Details</th>
<th>URL</th>
</tr>
</thead>
</table>
REFERENCES


Fuchsbaure:2011:CSV

Fulton:2010:BRB

Franken:2019:ECP

Fathi-Vajargah:2017:IMC

Fiore:2017:PGP

Feng:2013:ECE
Jun Feng, Xueming Wang, and Hong Sun. Efficiently computable endomorphism for genus 3 hyperelliptic curve cryptosystems. Information Process-
Fanyang:2012:SAK


Fu:2017:DFA


Feng:2011:VBF


Fan:2015:IRD


Fan:2013:KIS


Fan:2014:NCI

REFERENCES

208

(GomezPardo:2013:ICM) [G13]

(Gross-Amblard:2011:QPW) [GA11]

(Gregio:2015:TTM) [GAF+15]

(Gope:2018:LPP) [GAI+18]

(Galindo:2013:NIC) [Gal13]

(Gasarch:2013:RBC) [Gas13]
William Gasarch. Review of Theoretical Computer Science: Introduction to Automata, Computability,


Craig Gentry. Encrypted messages from the heights

[Gaspar:2012:SEF]

[GG11]

[Garg:2016:CIO]

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


[Gen11b] Coding is a phrase used in the context of data transmission and signal processing.


Grigoriev:2017:YMP  

Gaj:2017:DCR  

Guo:2010:HMW  

Gouvea:2012:HSI  

Guo:2018:KAA  

Gorawski:2012:EAS  


Gong:2016:HES  

Gradwohl:2010:SRC  

Gradwohl:2013:SRC  

Guo:2012:ETD  

Guo:2013:TVS  

Goyal:2011:SCP  

Garmany:2013:PPR  
Behrad Garmany and Tilo Müller. PRIME: Pri-


**Guo:2011:ISS** Fuchun Guo, Yi Mu, and Willy Susilo. Improving security of $q$-SDH based digi-

**Guo:2014:SAS**


**Gao:2014:URA**


**Groza:2017:LCL**


**Gong:2012:KNF**


**Garay:2017:SIA**

REFERENCES

**Goodin:2012:CBS**

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

**Garcia:2012:ERP**


**Gorski:2010:CDS**


**Groth:2012:NTN**


**Glowacz:2017:IDW**


**Gong:2013:NOT**


**Goodrich:2012:EVW**

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

[Genkin:2016:PKE]

[GPT12]

[Gre17]

[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.

Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Guha:2017:RTS


Guin:2016:FCS


Gong:2016:FSC


Gierlichs:2012:ICD

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

Genkin:2013:RKE


Ge:2016:KPA


Gazi:2012:EOS


Gupta:2019:LAU


Goodrich:2011:EAD

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

[Grosse:2013:AS] 

[Gueron:2016:MEG] 

[Gupta:2015:GEM] 

REFERENCES


REFERENCES


[Guo:2012:AKE]

[Guo:2017:EMD]

[Gao:2012:RHC]

[Guo:2018:SMK]

[Guo:2019:NTP]

[Ge:2013:SAP]
Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang. Secu-


REFERENCES


Hernandez-Becerril:2016:GIS

Hulsing:2017:XEH

Hao:2012:SAM

Hu:2017:ATE

REFERENCES

Hernandez-Becerril:2016:GIS


He:2013:HEH


Hu:2017:ATE


REFERENCES


Hernandez-Castro:2012:AFH

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

Heath:2015:HNS

Hw

Hamad:2018:DWU
Safwat Hamad, Ahmed Elhadad, and Amal Khalifa. DNA watermarking using...
REFERENCES


Hellman:2017:TLC


Hermelin:2010:MLC


Herranz:2014:ABS


Herardian:2019:SUC


Hess:2012:GJC


Heys:2017:SCF


Harn:2014:MTS

[HF14a] Lein Harn and Miao Fuyou. Multilevel threshold secret sharing based on the
REFERENCES


Hoang:2014:IMD


Hua:2015:TSE


Heyse:2012:TOC


Harn:2015:DTS

[HH15] Lein Harn and Ching-Fang Hsu. Dynamic threshold secret reconstruction

Huang:2016:EDP


Han:2011:PEB


**Hu:2016:EWS**


**Hayashi:2013:AEI**


**Huber:2014:TPW**


**Huang:2017:BBC**


**Haitner:2011:PRI**


**Hong:2015:RSM**

Wien Hong, Gwoboa Horng, Chih-Wei Shiu, Tung-Shou Chen, and Yu-Chi Chen. Reversible steganographic


REFERENCES


[HL10a] L. Harn and Changlu Lin. Authenticated group key transfer protocol based
REFERENCES


[Hazay:2010:EST]

[Hsu:2011:NIB]

[Hsieh:2014:AMU]

[Hmood:2015:ACA]

[Hu:2012:VMS]

[HL10b]

[HL11]
REFERENCES


REFERENCES


Han:2018:TSE

Huang:2015:CEA

Howard:2010:DSS

Hohenberger:2012:DDQ
Susan Hohenberger, Allison Lewko, and Brent Waters. Detecting dangerous queries: a new approach for chosen ciphertext security. Lecture Notes in Computer Sci-
 REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-32009-5_1/.

[Hof16]

Hirt:2014:BA


[HMR14]

Harnik:2010:CIC


[HN10]

Hoffmann:2016:LBQb


[Hof15]

Hoffmann:2015:LBQb


[Hol12]

Horsman:2019:CPE


[Hof19]

Hyla:2012:CBE

Tomasz Hyla and Jerzy Pejaś. Certificate-based encryption scheme with general access structure. Lecture Notes in Computer
REFERENCES


Jinsong Han, Chen Qian, Panlong Yang, Dan Ma,


REFERENCES


Herranz:2013:SMS


Hulsing:2016:MMT


Haitner:2010:EIC


Hwang:2011:CDA


Hubballi:2018:NTC


Homma:2014:TFD

N. Homma, K. Saito, and T. Aoki. Toward formal design of practical cryptographic hardware based on Galois field arith-
Halevi:2011:TBH


Han:2013:IBD


Han:2014:IBS


Han:2012:PPD


Heather:2014:CPE


Ho:2011:EIB

Shi:2015:CTS

Hamdy:2011:HPB

Henson:2013:MES

Hu:2010:TTW

Huang:2015:PAP

Huang:2017:SSS


REFERENCES


**Holbl:2012:ITP**


**He:2016:STI**


**Heng:2010:CNS**


**He:2015:SSQ**

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

**Hsu:2014:VWR**

Huang:2011:GFT


Huang:2018:PIB


See [?].

Huang:2011:IBS


Heys:2011:PSC

REFERENCES


Han:2012:ERI


Han:2014:ERI


Han:2018:ERA

Qi Han, Yinghui Zhang, and Hui Li. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. *Future Generation Computer Systems*, 83(??):269–277, June 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL 

Huang:2019:ILA


Han:2014:ATS


IEEE:2011:PIA


IEEE:2013:PIS


IImanimehr:2016:HPR


Islam:2011:MDA


Iyengar:2016:SPS


Imai:2015:IRR


[IG11]
REFERENCES

Islam:2015:LFP

Ioannou:2014:PKC

I:2017:ETB

I:2018:REP

Isobe:2012:SCL

Isobe:2012:SAL
[IS12] Takanori Isobe and Ky-

Irshad:2016:EAM


Jie:2010:AAI


Jie:2011:RGA

REFERENCES

January 2011. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Prins:2011:DCA

Jain:2013:MSD

Jho:2016:SSE

Jakobsson:2012:AWD

Chang:2012:TRR

Jogenfors:2015:HBT

Jeong:2013:CBC


S王朝:2014:UIS

S王朝:2014:TEA

S王朝:2014:MAC

S王朝:2014:MAC


[JKHeY12] Jong Yun Jun, Kunho Kim, Jae-Pil Heo, and Sung eui Yoon. IRIW: Image retrieval based image watermarking for large-scale


0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32344-7_2.}


[263] Jiang:2016:UTC


[266] Johnson:2010:BRF

Neil F. Johnson. Book review: Frank Y. Shih, Digital Watermarking and
Johnson:2015:NGA


Joux:2013:NIC


Juels:2014:HEE


Jaiyeola:2018:IPN

Jevdjic:2017:ASC


Jain:2016:APQ


Judmay:2017:BCI


Jiang:2018:CPA

REFERENCES


[WJ17] Wei Jiang, Liang Wen, Ke Jiang, Xia Zhang, Xiong Pan, and Keran Zhou. System-level design to detect fault injection at-

Jin:2015:NCD


Jou:2014:SAC


Jiang:2010:EDI


Khazaei:2017:COA


Kurkcu:2018:CBE

Kornycky:2017:RFT


Koziel:2018:HPS


Kapera:2011:SPD


Kapera:2013:MRM


Karafyllidis:2012:QGC


Kamp:2013:MES


Kamp:2016:MEM

Kong:2015:CSM


Katz:2013:RIB


Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP


Kim:2011:SSE

Changhoon Kim, Matthew Caesar, and Jennifer Rexford. SEATTLE: a Scalable Ethernet Architecture for Large Enterprises. *ACM Transactions on Computer

Kraetzer:2012:PCS


Karakoc:2013:BCL


Kumari:2017:DSU


Keblusek:2015:BRK


Kemshall:2011:WMT


Kleinjung:2010:FBR


Kikuchi:2012:SSN


Kramer:2010:FDC

Kim:2012:SLT


Khedr:2016:SSH


Kwon:2010:SEB


Koo:2018:PPD


Khamaei:2010:NBS


Kastner:2010:AOT

Kim:2014:MBM


Khalil-Hani:2013:BEB


Kim:2016:EPE


Kai:2011:CIS


Kiayias:2011:TCC


Kompara:2019:REM

Kim:2011:LBA


Kim:2015:CEH


Kim:2016:MAS


Khan:2016:BSW


Konstantinou:2010:RCI


Kawai:2012:SHS

Kawai:2013:SHS

Khalil:2014:CIM

Khan:2015:CMB

Khan:2014:MEK

Karopoulos:2010:FIP

Kubota:2016:SAV
Takahiro Kubota, Yoshi-


REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Conference/Journal</th>
<th>Publisher</th>
<th>Pages</th>
<th>ISBN</th>
<th>LCCN</th>
</tr>
</thead>
<tbody>
<tr>
<td>[KME+12]</td>
<td>Kohei Kasamatsu, Takahiro Matsuda, Keita Emura,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Kline:2018:CAR


Kiyoshima:2014:CRB


Karger:2011:LLB


Kanwal:2015:TTM


Katz:2012:TSP

Kavun:2018:SAE


Khovratovich:2010:RCA


Khovratovich:2010:RRA


Kumari:2016:APW


Koblitz:2010:BRB


Kasper:2012:SCA


Khameasemanan:2016:BBU

REFERENCES

279


[KPB17] Vireshwar Kumar, Jung-Min (Jerry) Park, and Kaigui Bian. Transmitter authentication using hierarchical modulation in

**Kiltz:2011:EAH**


**Khalid:2016:RHL**


**Kocabas:2012:CPB**


**Kang:2016:DSA**


**Keskinarkaus:2010:IWD**


K:2018:AAF


K:2010:RCB


Kolesnikov:2012:LPP


Kumar:2015:RGB


Karthiga:2018:PSA

Kocabas:2016:ESM

[102x644] Ko
[216x644] cabas:2016:ESM

Khan:2017:TPK

[202x644] K
[216x644] an:2017:TPK

Kiljan:2017:SAC

[202x644] K
[216x644] iljan:2017:SAC

Kwon:2018:EIP

[202x644] K
[216x644] won:2018:EIP

Kim:2012:SSS

[202x644] K
[216x644] im:2012:SSS

Klingler:2013:UPT

[202x644] K
[216x644] lingler:2013:UPT
Kim:2012:SAH


Kawachi:2012:SKE


Kobayashi:2016:ASC


Klisowski:2012:CCP


Kai:2014:FSD


Kupcu:2013:DTT

Alptekin Küçüç. Distributing trusted third parties. ACM SIGACT News, 44
Kupcu:2015:OAS


Kuznetso:2011:APP


Kshetri:2018:BEV


Kiljan:2018:ETA


Karpovsky:2014:DSS


Kuo:2016:SDD

Koyama:2012:NTD


Kamal:2010:EIN


Kreutz:2018:KPS


Kuo:2018:DRA


Kate:2010:PBO


Lu:2010:MSC


Lathey:2015:IEE

REFERENCES

[38:??, January 2015. CO-DEN ???? ISSN 1551-6857 (print), 1551-6865 (electronic).

Lackey:2015:UHP


Liang:2015:SEC


Langley:2013:EDC


Lan17


Launchbury:2012:TBC


Landau:2010:SSR

Lauter:2017:POL


Liu:2013:PAE


Luo:2012:ESI


Lupu:2012:IBK


Lu:2013:CSA


Liu:2015:IAC

Laxmi:2017:GGS


Liu:2013:IAG


Lathrop:2011:SPI


Lavington:2012:ATH


Li:2015:NAC


Lee:2017:SUE

Kwangsu Lee, Seung Geol

[LCLW17]

Liu:2017:GAU


[LCL17b]

Li:2015:CEH


[LCLL15]

Liang:2014:CCS

Kaitai Liang, Cheng-Kang Chu, Xiao Tan, Duncan S. Wong, Chunming Tang, and Jianying Zhou. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. *Theoretical Computer Sci-
REFERENCES

Liu:2016:EQQ

Liu:2016:NOP

Lotz:2015:SCS

Launchbury:2012:ELT
REFERENCES


Liang:2015:CPA


Li:2018:CIC


Liu:2017:ECC


Lan:2010:RNG


REFERENCES

Liu:2012:FVC


Lee:2010:ISC


Lee:2010:CGC


Lin:2011:NIB


Lin:2011:ICA


Li:2010:AIS


Li:2014:SOA


Lian:2014:SSA

Yanling Lian, Xinyi Huang, and Yi Mu. SA3: Self-adaptive anonymous au-


[Li:2014:IVW] Pei-Yu Lin. Impercepti-

Lindell:2014:TCT


Lin:2015:LBD


Liu:2016:LCP


Li:2017:MMA


Li:2016:IRI


Li:2017:SQS


Li:2012:OEA


Laszka:2014:STC
REFERENCES


Cheng-Chi Lee, Chun-Ta Li, and Shun-Der Chen. Two attacks on a two-factor user authentication in wireless sensor networks. Parallel Processing Letters,
REFERENCES


[LLK18] Zhe Liu, Patrick Longa, and Çetin Kaya Koç. Guest Editors’ introduction to the special issue on cryptographic engineering in a post-quantum world: State


REFERENCES


**Liu:2019:SBC**


**Li:2017:CIS**


**Li:2017:CCD**


**Liu:2018:VSE**


**Li:2018:CIE**


**Li:2010:DCY**

Chengqing Li, Shujun Li,

Lai:2013:SAS


Libert:2019:ZKA


Lai:2018:EQK


Lee:2019:CSS

REFERENCES

Lee:2016:CAM

Lee:2016:AGA

Lee:2015:SAS

Luo:2012:FSI

Ling:2012:NCC

Li:2018:WMH
REFERENCES

49–64, July/September 2018. CODEN IEMU/E4. ISSN 1070-986x (print), 1941-0166 (electronic).

Lu:2012:BBE


Lai:2016:GGB


Li:2017:CBS


Lambert-Mogiliansky:2012:EII


Le:2016:ADS


Lai:2018:IBB


REFERENCES


REFERENCES


**[Liu:2015:GTB]**


**[Liu:2016:PPO]**


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

**[Libert:2010:KES]**


**[Lubicz:2015:GMA]**


**[Lukowiak:2014:CEB]**

REFERENCES

2:??, March 2014. CODEN ??? ISSN 1946-6226.


REFERENCES


[LTC+15a] Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang, Wang-Jui Tsai, and Pokai Zhong. Implementing multiple biometric features for a recall-based graph-

**Liu:2015:MSG**


**Lao:2016:BFD**


**Lysyanskaya:2010:AEC**


**Lin:2011:CNS**

REFERENCES


[Li:2016:LRC]

[Ludge:2012:NLD]

[Lud12]

[Lafitte:2011:CBF]

[Liu:2010:CIE]


Liu:2013:TIE


Liu:2013:CBS


Liu:2016:PAB


Liu:2014:DAF


Liu:2017:EEC


Liu:2011:SBA

Xiong Li, Fan Wu, Muhammad Khurram Khan, Lili

Lu:2012:HOM


Liu:2010:NDC


Liu:2010:SET


Liu:2011:PIA

Lu:2012:MMA

Li:2010:GCP

Lou:2010:NAS

Luo:2012:ICB

Li:2012:IIA

Lin:2010:DSM
Dai-Rui Lin, Chih-I Wang, Zhi-Kai Zhang, and D. J. Guan. A digital signature with multiple subliminal channels and its

**Li:2011:NIW**


**Li:2014:IBD**


**Li:2014:EMK**


**Lai:2012:RHB**


**Li:2012:ESD**

REFERENCES


Liao:2010:MPC


Liu:2018:SKR


Li:2013:SSS


Liu:2012:SOCa


Luo:2012:LVT


Liu:2014:PKE


REFERENCES

MacCormick:2012:NAC  [MAC+12]

With a foreword by Christopher M. Bishop.

Macrakis:2014:PLS  [MAL10]

Maffeo:2016:UNC  [MAL13]

Michail:2012:EHT  [MAC+12]

Moskowitz:2010:ITE  [MAL10]

Malkin:2013:SCB  [MAL13]
REFERENCES


Mangard:2013:KSL


Martin:2010:FWL


Martin:2010:PCC


Martin:2010:XMA


Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP

REFERENCES


Matthiessen:2019:RCM

Maurer:2012:CCN

Mazurczyk:2013:VSD

Milo:2011:FGB

Mao:2015:PUA
REFERENCES

Matias:2018:NNZ


Malone:2013:MOD


Migliore:2018:PPF


Massolino:2015:OSC


Mukhopadhyay:2011:PEA


Madanayake:2012:BPS

McGrew:2017:IDH

McGraw:2011:TWH

McKay:2010:SLB

McKay:2011:SLB
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 ???

Mahmood:2018:ECC

Marquez-Corbella:2015:ECP
Irene Marquez-Corbella and Ruud Pellikaan. Error-correcting pairs: a new approach to code-based crypt-
REFERENCES


Arsalan Mosenia, Xiao-Mansfield-Devine:2015:MIC

Mansfield-Devine:2015:MIC

Mosenia:2017:PTS

Mosenia:2017:PTS

**Maachaoui:2012:MLA**  

**Meiklejohn:2010:BRB**  

**Menezes:2013:IPB**  

**Menn:2013:ESC**  

**Meshram:2015:EIB**  

**Mandal:2016:DIW**  
REFERENCES


Miller:2014:ADS


Mou:2013:CBC


Mohd:2015:SLB


Micciancio:2010:FGC


Michiels:2010:OWB

REFERENCES

Michael:2016:RNI


Midgley:2010:SEE


Martinez-Julia:2013:BSI


Muller:2012:HPC

Mozaari-Kermani:2017:FD


Mozaari-Kermani:2010:CSI


Moiz:2016:SMH


Malik:2012:AIC


Marconato:2013:VLC

Montecchi:2012:QSE

Mancillas-Lopez:2010:RHI

Mendez:2016:PES

Manzanares-Lopez:2012:ICU

Ma:2017:LBI

Madhusudhan:2012:DIB
R. Madhusudhan and R. C.

Meshram:2013:IBC


Maity:2014:FIR


Mondal:2014:DSM


Maity:2017:ODC


Mulholland:2017:DCD

REFERENCES


[MMS17c] Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. A simple authentication encryption scheme. Concurr-

Maity:2013:CRS


Matsuo:2012:MAK


Meshram:2012:IBC

Chandrashekhari Meshram, Suchitra A. Meshram, and Mingwu Zhang. An ID-based cryptographic mech-


Monz:2016:RSS


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

McKusick:2015:DIF


Minier:2012:RKI


Mizuki:2011:ASN


Maimut:2012:LCR


Minamoto:2014:BDI


[DMP+18] Donghyun Min, Donggyu Park, Jinwoo Ahn, Ryan Walker, Junghhee Lee, Sungyong Park, and


Marasco:2014:SAS


Micali:2014:CMS


Manimehalai:2016:NRR


Migliore:2018:HSC


Martinovic:2017:AUP


Matsumoto:2017:ACG

Moghadam:2010:DRN


Mendel:2012:DAL


Maitra:2012:NAC


Maitra:2013:DSM


Maitra:2013:HEM

(print), 1943-5851 (electronic).

**Maitra:2013:HPM**


**Miller:2016:RPS**


**Mukherjee:2017:EPP**


**Myers:2012:BCM**


**Myers:2013:BBC**


**Marton:2010:RDC**

Mashimo:2018:VMS


Mosenia:2017:CCA


Martins:2018:SFH


Muhammad:2018:ISU


Miret:2018:PBC


Mosca:2013:QKD

REFERENCES


Murphy:2010:BRB


Murdoch:2016:IDP


Miri:2012:SAC


Min:2016:RSC


Mishra:2016:AFP


Mannan:2011:LPD

Mohammad Mannan and P. C. van Oorschot. Leveraging personal devices for stronger password authentication from untrusted computers. *Journal of
REFERENCES


Maes:2012:PFF

Mathew:2012:EIC

Ma:2012:CIS

Ma:2013:PVP

Marko:2017:MDI
Frantisek Marko and Alexandr N.


REFERENCES

Naskar:2012:FIR

Naskar:2013:GTL

Naranjo:2013:FDA

Ni:2013:EIB

Narasimhan:2013:HTD
REFERENCES

Ngo:2017:CSS

Nedjah:2016:PYP

Nafea:2016:HMB

Newell:2013:PCD

Naeem:2014:EIC


[MNP+13] Juan González Nieto, Mark Manulis, Bertram Poetter-

Nieto:2014:FSH


Nag:2010:KD


Navin:2010:ETU


Namasudra:2017:NSA


Niu:2015:CRS


Naccache:2010:THI


Nojoumian:2012:SRS


Natarajan:2015:MAD


Niksefat:2014:ZPP


REFERENCES


Xuyun Nie, Zhaochu Xu, and Johannes Buchmann. Cryptanalysis of hash-based tamed transformation and minus signature scheme. Lecture Notes in Computer Scien-
REFERENCES


Gabriele Oligeri, Stefano Chessa, Roberto Di Pietro, and Gaetano Giunta. Robust and efficient authentication of video stream


REFERENCES

Ogiela:2018:EBI

Oliveira:2012:STA

Ogiela:2018:LTC

Ohtake:2012:AAH

Ogiela:2010:UML

Orlandi:2014:SCN
Claudio Orlandi, Rafail Ostrovsky, Vanishree Rao, Amit Sahai, and Ivan Visconti. Statistical concur-


Olson:2016:SIT


Orencik:2016:MKS


Otmani:2010:CTM


Ogiela:2018:VCA


Ohzeki:2012:NWM

Kazu Ohzeki, YuanYu Wei, Yutaka Hirakawa,

**Ortiz-Yepes:2014:BSA**


**Praba:2010:MAC**


**Parveen:2018:IEE**


**Pal:2015:SDC**


**Pal:2016:ACC**


**Pandey:2014:ACR**


Poh:2017:SDV


Park:2014:FRI


Pun:2014:GIT


Paul:2016:TSO


Papadopoulos:2014:LQA


Premnath:2014:EHR


**Poh:2017:SSE**


**Pang:2014:PPA**


**Paul:2012:KSS**


**Pereira:2015:PKE**


**Pippal:2012:SVU**


**Pearson:2011:NWC**

Joss Pearson, editor. *Neil Webster’s cribs for vic-


[PHWM10] Jong Hyuk Park, Sajid Hussain, Guilin Wang, and Yi Mu. Special issue of computers and mathematics with applications on

Pieprzyk:2010:TCC [Pie10]

Pointcheval:2012:ACE [PJ12]

Patel:2018:LLA [PJ18]

Premarathne:2015:LDD [PKA15]
Pramila:2018:ICA


Peter:2012:AHE


Phuc:2016:SAS


Perez:2011:FDS


Peris-Lopez:2018:EAC


Pang:2013:IMA

Liaojun Pang, Huixian Li, Qingqi Pei, and Yu-

Peris-Lopez:2010:CSP


Poh:2012:SEC


Pande:2013:SMC


Poursakidis:2010:TPC


Puthal:2017:DDK

Niu:2014:RDW


Powers:2014:OSCa


Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC


P:2018:ABE


Pereira:2016:SHB

Geovandro C. C. F. Pereira, Cassius Puodzius, and Paulo S. L. M. Bar-

**Pathak:2012:PPS**


**Phan:2012:DDB**


**Phan:2012:MBT**

Papadopoulos:2015:PAP


Pandey:2012:PPS


Piret:2012:PBC


Perez-Resa:2019:SSE


Puthal:2019:SAL


Polyakov:2017:FPR

[Yuriy Polyakov, Kurt Rohloff, Gyana Salu, and Vinod Vaikuntanathan. Fast proxy re-encryption for publish/subscribe sys-


Patranabis:2017:PSK


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC


Papakostas:2014:MBL

(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0096300313012046

**Papamanthou:2016:AHT**

**Pudo:2012:RKA**

**Pei:2013:ARW**

**Poller:2012:EIC**

**Peng:2010:IWM**

**Pongaliur:2013:SNS**
REFERENCES

Pagnin:2018:HDB


Philippaerts:2013:CMC


Pei:2015:SWT


Papadopoulos:2010:CAR


Phuong:2018:CBE


Pournaghi:2018:NNE

www.sciencedirect.com/science/article/pii/S1389128618300227


REFERENCES


Qiu:2017:AAS


Qiu:2017:PSB


Qiao:2018:CTC


Quaglia:2018:SV


Qin:2016:STI


Qian:2014:IAF

Zhenxing Qian and Xin-

Qiang:2016:SCF


Qi:2016:SID


Qi:2016:SPR


Qin:2018:BRO


Rabin:2010:ACC


Rankin:2010:HLH

Kyle Rankin. Hack and
REFERENCES


Rankin:2014:HEY


Rankin:2016:HSP


Rao:2010:PAA


Rao:2017:SEC


Rauscher:2015:FMT


Ruoti:2015:WJS


Rupp:2015:CTM

[Andy Rupp, Foteini Baldimtsi,]

Radke:2015:CFA


Reaves:2017:MBM


Raisaro:2018:PPS


Rabbachin:2015:WN1


Rao:2017:CFA


Ren:2016:IBE


Reardon:2016:SDD


Reeve:2015:ARC


Ren:2010:CSH


Roh:2010:BSW


Robert-Inacio:2011:SAP

REFERENCES


REFERENCES


[RPG12] RPG12


Rosen:2010:CCS


Reeder:2011:WPD


Rivest:2014:SSR


Rossi:2015:IBS


Rana:2016:DBV


Roy:2017:LOS


Roetteler:2018:QCC

REFERENCES


Rahulamathavan:2019:PPI


Ryan:2015:EEVa


Rahulamathavan:2016:UCA


Rodriguez-Vazquez:2012:SCB

Juan José Rodríguez-Vázquez, Sixto Romero-Sánchez, and Miguel Cárdenas-Montes. Speeding up a chaos-based image encryption algorithm using GPGPU. *Lecture Notes in Computer Science*, 6927:592–599, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-
REFERENCES


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


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


Palash Sarkar. Tweaking enciphering schemes using


Savage:2013:NSL


Savage:2013:PP


Savage:2015:NVS


Savage:2016:NKP


Safkhani:2017:PSD


Shwartz:2018:DMI


Stevens:2017:AFS

REFERENCES

first-sha1-collision.html.

Safkhani:2012:SMA


Santos:2014:ACD


Shyu:2010:VMS


Srinivasan:2012:RAP


Syta:2014:SAA


Schoenmakers:2010:VS

Berry Schoenmakers. Voting Schemes, chapter 15, pages 1–21. Volume 2 of Atallah and Blanton [AB10b], second edition,
REFERENCES

Schwartz:2011:IMP


Schaathun:2012:MLI


Schneier:2012:LOE


Schnoor:2012:DES


Schneier:2013:HDD


Schaefer:2015:BRB

REFERENCES


REFERENCES


[SD12] Jing Shen and Yusong Du. A password authentication scheme against Smart Card


CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-34062-8_5/.

**Shakiba:2010:IID**


**Souissi:2012:OCP**

http://link.springer.com/chapter/10.1007/978-3-642-30955-7_15/.

**Shakiba:2014:CCI**


**Seo:2014:RHI**


**Seo:2016:RHI**


**Salman:2018:BMM**

S. M. Salman and A. A. Elsadany. On the bifurcation of Marotto’s map and its application in im-

**Sasaki:2012:IKK**


**Staples:2019:SAB**


**Sendrier:2010:PQC**


**Serrato:2012:IAN**


**Sakai:2016:CDN**

Yusuke Sakai, Keita Emura, Jacob C. N. Schuldt, Goichiro Hanaoka, and Kazuo Ohta. Construc-

**Sethumadhavan:2016:HEP**


**Severance:2016:BSB**


**Seo:2018:AOF**


**Savas:2014:SMQ**


**Su:2012:IIN**


**Shabtai:2010:SAP**

[SFE10] Asaf Shabtai, Yuval Fledel,

**Schneier:2015:SWC**


**Sasdric:2015:ICS**


**Shu:2014:DAS**


**Saxena:2016:API**


**Silva-García:2018:SBG**


**S:2018:EDS**

Prabu S, Gpinath Ganapathy, and Ranjan Goyal.

**Sanchez-Garcia:2016:SSA**


**Sun:2015:FSW**


**Shen:2018:CAL**


**Susilo:2016:EDT**


**Shankar:2012:BDF**

Deepa D. Shankar, T. Gireesh Kumar, K. Praveen, R. Jithin, and Ashji S. Raj. Block dependency feature based classification scheme for uncalibrated image ste-
References

Sun:2017:PKE


Sipiran:2014:SCA


Shaolan:2011:EDE


Seyedzadeh:2011:IEA


Song:2015:ADT

Shallit:2010:BRB


Shaw:2013:DE


Syed:2019:TGB


Shen:2014:LES


Shim:2011:SA


Shparlinski:2010:NWP

Suoranta:2012:ASM


Shyu:2015:VCR


Satir:2012:CBT


Siad:2012:NAP


Simion:2015:RST


Simmonds:2015:DI


Sirer:2016:TPS

[Sir16] Emin Gün Sirer. Technical perspective: The state (and security) of the


[Shin:2017:CGI]

Shin:2017:CGI


[SJWH+17]

[Sherman:2019:OVB]

Sherman:2019:OVB


Shin:2017:SSD

Szalachowski:2010:CCG

Stevens:2015:FCF

Singh:2018:MWT

Scheidat:2012:STT

Schmitz:2012:NAC
Srivatsa:2011:ESA


Schultz:2010:MMP


Somani:2010:IDS

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

Sun:2016:RSP

Shi-Feng Sun, Joseph K. Liu, Yu Yu, Baodong Qin, and Dawu Gu. RKA-secure public key encryp-


Shao:2012:AKP


Sarkar:2010:CRM


Sarkar:2010:CRT

Santanu Sarkar and Subhamoy Maitra. Cryptanalysis of RSA with two decryption exponents. *Infor-
Seyedzadeh:2011:IES


Sengupta:2012:SAI


Sencar:2013:DIF


Swami:2018:AAS


Smart:2016:CMS

Stanton:2010:FAD

Salmon:2011:PRN
John K. Salmon, Mark A. Moraes, Ron O. Dror, and David E. Shaw. Parallel random numbers: as easy as 1, 2, 3. In Lathrop et al. [LCK11], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????

Smith:2011:SSX

Smith:2011:RBA

Swierczynski:2015:PSE

Stankovski:2014:CFE
Tomislav Stankovski, Pe-

Sharma:2018:CSS


Sadeghi:2010:THI


Safavi-Naini:2011:USC


Seyedzadeh:2014:RCI


Suriadi:2012:PCV

Suriadi Suriadi, Chun Ouyang, and Ernest Foo. Privacy compliance verification in cryptographic protocols. Lecture Notes in Computer Science, 7400:


[Spa16] Eugene H. Spaafford. The strength of encryption. *Communications of the
REFERENCES


Schilling:2012:ATU


Sur:2012:SSU


Stanton:2014:BRB


Singh:2017:SCB


Stefan:2012:ACT

REFERENCES


[SSAF11] Matthew Smith, Christian Schridde, Björn Agel,


REFERENCES


Schaffer:2012:EII


Schillewaert:2014:CCA


Shen:2016:RMM


Sethumadhavan:2019:SA


Stallings:2011:CNS


Stanoyevitch:2011:ICM


Stanek:2012:TEM

Sta:2013:ITD

Stew:2011:CCI

Steel:2015:APF

Stenn:2015:SNT

Stipcevic:2011:QRN

Stickney:2015:CBS

Stiles:2019:HSB
D. Stiles. The hardware security behind Azure Sphere. IEEE Micro,
REFERENCES


**Stolte:2012:EDA**


**Suciu:2012:SED**


**Sung:2011:DCE**


**Sun:2016:NEB**


**Shen:2015:CSC**


**Song:2016:IAR**


**Svozil:2014:NCC**

Karl Svůzil. Non-contextual chocolate balls versus value indefinite quantum cryptography. *Theoretical
REFERENCES


REFERENCES

Shen:2017:RDP


Sui:2014:DAH


Shi:2013:REA


Sun:2017:CPP


Shen:2014:ERC

REFERENCES

Sun:2018:RPP

Tsang:2010:BRR

Tamayo:2015:AFH


REFERENCES

Tang:2015:ETE

Tang:2015:HAC

Tankard:2017:BNK

Tankard:2017:ECB

Toth:2019:SSD

Tarnovsky:2010:DSP

Taylor:2014:WSE

Taylor:2017:EBH
Michael Bedford Taylor. The evolution of Bitcoin hardware. Computer, 50
Talbi:2018:SIW

Tilli:2015:GCR

Tuan:2010:AWB

Taylor:2011:DR

Tang:2015:CER

Tian:2014:DFS


Tiplea:2014:NSC


Tao:2013:SMS


Terai:2011:BRB


Tassa:2012:SDC


Tewari:2017:CNU

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

Theofanos:2016:SUE

Tian:2016:IBS

Tian:2015:IBP

Tian:2012:TOE

Thabit:2014:RR

Takayasu:2019:PKE
Tu:2014:EPB


Tani:2012:EQA


Tu:2013:PAQ


Tariq:2014:SBL


Tan:2016:ESE


Tsaur:2012:ESM

Woei-Jiunn Tsaur, Jiahong Li, and Wei-Bin Lee. An efficient and secure multi-server authentication scheme with key agreement. *The
**REFERENCES**


**Tsai:2013:ZWS**


**Tetali:2013:MSA**


**Tang:2012:RSS**


**Tsay:2012:VUL**


**Tsoutsos:2018:EDM**

REFERENCES


Toxen:2014:NSS


Tsougenis:2012:PEM


Tan:2016:BIB


Taylor:2011:CAS


Tezcan:2016:IID

REFERENCES

[Tschorsch:2016:BBT]

[Tao:2014:CFS]

[Toreini:2017:TRP]

[Tang:2011:IDC]

[Tso:2013:SAI]

[Tseng:2012:ERI]

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


Christophe Tartary, Hua-xiong Wang, and Yun Zhang. An efficient and information theoretically secure rational secret sharing scheme based on symmetric bivariate polynomials. *International Journal...
Tian:2012:SSB


Tian:2016:ORA


Tolba:2016:GMA


Tolba:2016:DTP


Tolba:2016:GMA


Ehatisham-ul-Haq:2018:CAS

[uHAN+18] Muhammad Ehatisham ul Haq, Muhammad Awais Azam, Usman Naeem,


**Vaikuntanathan:2012:HCE**


**vanDam:2011:TQC**


**Valamehr:2012:IRM**


**Visegrady:2014:SCV**


**VenaLabs:2014:VLQ**


Vleju:2012:CCA


Vivek:2014:CSC


Vliegen:2015:SRD


Veloudis:2016:NPH


Vollala:2017:EEM


VonMaurich:2015:IQM

REFERENCES


[Vua10] Martin Vuagnoux. Computer Aided Cryptanalysis from Ciphers to Side Chan-
Vazirani:2019:FDI


Wagsta:2010:C


Wagner:2016:TPF


Walter:2018:RCS


Wang:2010:NSB


Wang:2013:CRA

Wang:2014:IIA


Wang:2018:LRI


Ward:2011:CCM


Watt:2010:IPI


Waters:2012:FER


Watts:2014:ICB


Watts:2014:PYI

Steve Watts. Protecting your identity when


King-Hang Wang, Chien-Ming Chen, Weicheng Fang, and Tsu-Yang Wu. On the security of a new...

Wei:2018:GCQ


Wang:2018:SEA


Wei:2012:NTB


Wazid:2019:DSK


Wang:2013:SES

Guojun Wang, Qiushuang Du, Wei Zhou, and Qin Liu. A scalable encryption scheme for multi-privileged group communications. The Journal of Supercomputing, 64(3):1075–1091, June 2013. CO-


REFERENCES

Wei:2016:PAB

Wu:2012:DAA

Wang:2012:FOP

Williams:2018:FPD

Winder:2017:ROS
Davey Winder. Researchers open sliding


REFERENCES

IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).


REFERENCES


Wang:2015:HAD


Wu:2012:UFS


Wendzel:2015:CME


Wang:2017:PPK


Wang:2016:SEP


Wu:2013:FTR

Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, and Jesús A.

Wu:2016:CBE


Wei:2015:TPE


Wu:2012:RGB


Williams:2013:APC


Whitworth:2014:SPC


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

construct Boolean functions with good crypto-
graphic properties. Information Processing Letters,
113(14–16):567–571, July/August 2013. CODEN IF-
PLAT. ISSN 0020-0190 (print), 1872-6119 (elec-
science/article/pii/S0020019013001348.

search of truncated impossible differentials for
word-oriented block ciphers. Lecture Notes in
Computer Science (Amsterdam, Netherlands:
1999), 56(12):2994–3006, August 16, 2012. CO-
DEN ????? ISSN 1389-1286 (print), 1872-7069 (elec-
science/article/pii/S1389128612001995.

[Wu:2016:LTN] Felix Wu. Law and technology: No easy an-
swers in the fight over
iPhone decryption. Communications of the As-
sociation for Computing Machinery, 59(9):20–22,
September 2016. CODEN CACMA2. ISSN 0001-0782
(print), 1557-7317 (electronic). URL http://
cacm.acm.org/magazines/2016/9/206250/fulltext.

Wu:2012:RIB

[Tsung-Yang Wu, Yuh-Min
Tseng, and Tung-Tso Tsai.
A revocable ID-based au-
thenticated group key ex-
change protocol with resis-
tant to malicious partici-
pants. Computer Networks
(Amsterdam, Netherlands:
1999), 56(12):2994–3006,
August 16, 2012. CO-
DEN ????? ISSN 1389-1286
(print), 1872-7069 (elec-
science/article/pii/S1389128612001995.

push messaging service in
VANET clouds. The Jour-
nal of Supercomputing, 73
CODEN JOSUED. ISSN
0920-8542 (print), 1573-
0484 (electronic).

Wu:2012:AST

[WW12] Shengbao Wu and Ming-
sheng Wang. Automatic
search of truncated im-
possible differentials for
word-oriented block ciphers. Lecture Notes in
Computer Science, 7668:
283–302, 2012. CODEN
LNCS9. ISSN 0302-9743 (print), 1611-
com/chapter/10.1007/978-3-642-34931-7_17/.

[WW13] Karl D. D. Willis and And-
rew D. Wilson. InfraS-
tructs: fabricating informa-
tion inside physical ob-

Wang:2014:ATF


Wen:2014:MZC


Wang:2011:MMW


Weng:2012:NCC


Wahaballa:2014:MLS

REFERENCES

Werner:2017:CIM

Wang:2011:CIB

Wang:2011:CHI

Wang:2017:FWA


[WYL13] Xiaogang Wang, Ming Yang, and Junzhou Luo.
REFERENCES


**Wei:2014:IDC**


**Wei:2016:APS**


**Wang:2013:BSB**


**Wei:2014:IDC**


**Wen:2011:DSH**


**Wei:2015:CPK**

Puwen Wei and Yuliang Zheng. On the construction of public key encryption


REFERENCES

Xiong:2013:NIB

Xu:2014:AHA

Xu:2012:APA

Xu:2014:TBH

Xue:2014:LDP


Xu:2013:PKE


Xu:2012:AHA


Xue:2018:SNN


Xiang:2016:EMP


Xue:2013:TCB


Xie:2013:ECP


[XSWC10] Hong Xin, Zhu Shujing, Chen Weibin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In *2010 International Conference on Computer Appli-
IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010.


[XWLJ16] See [XWS16].


[XWXC14] Qi Xie, Guilin Wang, Fubiao Xia, and Deren Chen. Self-certified proxy convertible authenticated encryption: formal definitions and a provably secure scheme. Concurrency

Xiao:2016:REM

[Xiong:2015:SRE]

[XXYXY11]


[Xie:2012:DPK]

[XXZ12]


[Xxing-Yuan:2011:PRS]

[XXYXY11]


[Xu:2015:ORA]

[XXZ12]

Xiong:2012:CLR


Xiao:2018:FEI


Yoo:2017:PQD


Yamaguchi:2012:EVC


Yu:2015:SDS


Yang:2010:PII

REFERENCES

Yang:2011:PQC


Yang:2014:BEB


Yang:2011:GSS


Yang:2012:PST


Yang:2016:EBB


Yi:2017:ZCL

[WYCL17] Wentan Yi, Shaozhen Chen, and Yuchen Li. Zero-correlation linear crypt-

Yuan:2013:PVQ


Yu:2016:DNF


Yao:2015:LAB


Yuan:2012:IBE


Yu:2017:PDA

Meng-Day (Mandel) Yu and Srinivas Devadas. Pervasive, dynamic authentication of physical items. *Communications of the Association for Computing Machinery*, 60(4):32–39, April 2017. CODEN CACMA2. ISSN 0001-0782
Yasuda:2015:MQC


Yan:2016:DEB


Ye:2010:ACC


Yamada:2012:PBR


Ye:2014:NIE


Yekhanin:2010:LDC

Yoshida:2012:OGT

Yu:2012:EPF

Yang:2017:CCS

Yang:2018:RRE

Yuce:2017:AFI

Yang:2015:SHI
Ye:2017:VCS

Ye:2016:IEA

Yu:2010:IBF

Yang:2016:EHA


Yu:2011:FSI


Yu:2012:IRI


Young:2013:TPC

Yang:2018:AIW


Yum:2011:ACO


Yum:2012:OPE


Yoshino:2012:SIP


Yi:2017:ICM


Yuen:2013:ELT


Yum:2012:OPE


Yoshino:2012:SIP

REFERENCES


Yang:2012:WSI


[YLZ+12]

You:2012:DDS


[YLZ12]

Yi:2013:ETS


[YMA17]

Yu:2016:CBE


[YLZ+16]

Yagan:2016:WSN


[YM16]

Yakubu:2017:SSN

Abukari M. Yakubu, Namunu C. Maddage, and Pradeep K. Atrey. Se-

**Yu:2017:AAC**


**Ying:2013:PPB**


**Yu:2010:PSI**


**Young:2015:DWE**


**Yavuz:2012:BFB**

[YNR12a] Attila A. Yavuz, Peng Ning, and Michael K. Reiter. BAF and FI-


Yang:2012:EMA


Yin:2017:QPE


Yengisetty:2011:AVC


Yi:2016:IPA


Yang:2012:SAK


Yumbul:2015:EEP

Kazim Yumbul and Erkay Savas. Enhancing an embedded processor core for efficient and isolated execution of cryptographic algorithms. The Computer Journal, 58(10):2368–2387,
REFERENCES


**Yang:2015:EPS**


**Yang:2016:ECV**


**Yang:2018:HEP**


**Yao:2014:NCR**


**Yeh:2010:TRR**


**Yuen:2014:TCT**

REFERENCES

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

Ylonen:2014:SAA

Yang:2011:CCK

Yang:2011:CPK

Yang:2014:IBI

Yamada:2012:UEW

Yeh:2017:SIB
Yang:2011:ACD


Yasuda:2012:ASM


Yang:2018:IAC


Yao:2010:IDA


Yao:2010:ASP


Yan:2017:PIS

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

Yang:2015:RCI


Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


Yang:2010:CRS


Wang:2018:CIW

[Xiang yang Wang, Huan Xu, Si yu Zhang, Lin lin Liang, Pan pan Niu, and Hong ying Yang. A color image watermarking approach based on synchronization correction. Fundamenta Informaticae, 158]
Yu:2012:SME

Ye:2018:ISS

Yesilyurt:2015:RWM
Murat Yesilyurt, Yildiray Yalman, and A. Turan

Yang:2013:ECS

Yang:2016:EPA

Yang:2012:LUC

Yang:2017:SKS

Yang:2018:CDD
Yang Yang, Xianghan Zheng, Ximeng Liu, Shangping Zhong, and Victor Chang. Cross-domain dynamic anonymous authenticated group key management with symptom-

**Yang:2012:BPN**


**Yang:2012:NIB**


**Zufiria:2017:GLM**


**Zidaric:2019:HOA**

Nusa Zidaric, Mark Aagaard, and Guang Gong. Hardware optimizations and analysis for the WG-16 cipher with tower field arithmetic. *IEEE Transactions on Computers*, 68
REFERENCES


Zoni:2018:CSC


Zhang:2011:TNT


Zh:2012:JLS


Zhang:2013:RMS


Zhang:2015:PCL


Zhang:2012:TCS

Zhifang Zhang, Yeow Meng Chee, San Ling, Mulan Liu, and Huaxiong Wang.


REFERENCES


[Zhang:2019:REU] Jun Zhang, Rui Hou, Wei Song, Sally A. Mckeee, Zhen Jia, Chen Zheng, Mingyu Chen, Lixin Zhang, and Dan Meng. RAGuard: an efficient and user-transparent hardware mechanism against...

Zh:2016:SCI


[ZHBT16] Zh:2016:TSC


Zhang:2016:PPV


Zhu:2013:TSC


Zhou:2015:EPP


Zuo:2019:WDH
REFERENCES

Zimand:2010:SEC


Zhang:2011:FBP


Zeng:2014:NFC


Zhou:2012:CBF


Zhou:2015:PPS


Zhao:2012:IAS

Zhao:2014:TAH


Zhang:2012:EEF


Zhang:2015:RBA


Zhang:2012:CCB


Zhu:2017:PSN


Zhou:2019:LIB


Zhang:2016:TLT


[ZM16] Zhang:2017:FGA


Zielinska:2016:CAH

Leyou Zhang, Yi Mu,


Zhou:2017:IBB


Zenger:2016:AKE


Zhang:2015:MAA


Zhang:2010:EMO


Zmudzinski:2012:WEU


Zhao:2012:SSM

Zheng:2018:GDP


Zanon:2019:FKC


Zhou:2018:TPW


Zuo:2018:CSA


**Zhang:2015:FAA**  

**Zhang:2014:LFL**  

**Zhou:2018:QT**  

**Zilberberg:2013:PCM**  
REFERENCES

June 2013. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).


Zhou:2011:PSA


Zhang:2016:PAG


Zhang:2014:EFH


REFERENCES


[ZZ11] Bo Zhang and Fangguo Zhang. An efficient public key encryption with

Zhao:2012:FCS


Zhao:2015:EPT

Zheng:2015:EPT


Zh:2014:SAC


Zhang:2015:ITS

Zheng:2015:EPT

Zhang:2015:ITS


Zh:2014:SAC


Zaidan:2017:NDW

Zhu:2018:CA


Zhang:2017:NLR


Zeng:2019:SAE