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/

25 August 2017
Version 1.375

Title word cross-reference

(2, 2) [KSSY12, LTC+15b]. (\(k, n\)) [YC11].
(n, t, n) [LHYZ12]. (t, n) [QD16, ZPWY12].
0 [XHX+17]. 1 [XHX+17]. 1, 2, 3 [SMDS11].
11 [LJ17]. 13 [Blo15]. 2 [DBPS12, EAA+16].
ESS12, JR13, MCDB12, PGLL10, WY12].
22 [MNP12]. 2\(k\) [Sun16]. 3
[AP10, CG12b, DWWZ12, FWS13, GZHD12].
GH11a, KWS+12, LJ17, LJ15, MKH+12.
RS16, SS10b, SS12a, SGS14, WSSO12.
tWmC12, YT11a, YI14, YPRL17]. 32 \times 32
[SAA14]. 3 \times 3 [AMVZ12]. 4
[COP14, DWZ12, HLYS14]. \$49.00 [Sch15a].
8 [LPO+17]. \$9 [APPVP15]. = [JUW10]. 2
[YNX+16]. 3 [LHM14]. \(\alpha\) [TTL10]. c
[KRDH13]. d [QD16]. d \times d [KA17]. \(\ell\)
[ZTL15]. \(F_p + \nu F_p\) [WGF16]. \(\gamma\) [DZW12].
GF(\(2^x\)) [SF12]. GF(\(2^n\)) [SKH15]. GF(\(2^n\))
[LBOX12]. \(K\)
[FXP12, FR16, CHX13, ZHT16].
L(1/4 + o(1)) [Jou13]. M [MMSD13, ÖŠ11].
\(F_{36509}\) [AMORH13]. \(F_q\) [SS13]. \(\mathcal{NP}\) [HN10].
GF(\(q\)) [LPS10]. LWE [BV14]. \(\mu\) [Jia14a]. N
[FR16]. \(n \times k(k \geq n/2)\) [MC11]. \(O(d13^2)
[KA17]. \(O(n^2)\) [KS11]. P [DG17]. \(\pm 1\)
[HZW+14]. \(q\) [GMS11]. \(S\) [LJ15]. t
[HJM+11, Oba11]. w [Kre13].

- [RS14]. -band [MMSD13]. -Bit [LPO+17].
-boxes [LJ15]. -Cheater [Oba11]. -D
[MCDB12]. -dimensional [DWWZ12, QD16].
-Diversity [ZTL15]. -Encoded [DG17].
-Encoding [XHX+17]. -Means [KRDH13].
-Multiple [LTC+15b]. -NN [ZHT16].

.onion [Boy16].

/ [Ran10, Ran14, Ran16].

0.13um [KLM+12].


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

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


SGGCR\textsuperscript{+16}. Ad-Hoc [PD14]. Adam [Bar12]. Adaptive [CT11a, zGXW12, GLG12, HZW\textsuperscript{+14}, HLAZ15, KD12a, Lin15, PWLL13, SOS15, CLP\textsuperscript{+13b}, dCCSM\textsuperscript{+12}, dCCSB\textsuperscript{+16}, EEAZ13, FXP12, GKCK11, GLM\textsuperscript{+16}, KS11, LHM14, LWW\textsuperscript{+10}, PC14, SH11, Wan13, WKH11]. Adaptively [HP14, OT12]. adder [MS13a]. Adding [CFVP16, CSL\textsuperscript{+14}]. Additive [ZDL12]. Additively [PKTK12]. address [PSJ\textsuperscript{+13}]. addresses [AZH11]. Addressing [SVG16, SRB\textsuperscript{+12}]. Adelson [BBB16b]. Adelson-Velskii [BBB16b]. adjacency [SA15]. adjacent [Kre13]. Administering [Pal16]. Adoption [LKKL13, YWK10b]. Advanced [Böh10, DR10, TC10, DDFR13, GLIC10, Kra12, MKRM10, NdMMW16, SKK10]. Advances [PHWM10, WP15, Abe10, GILL10, LW11a, PJ12, Rab10]. Advantage [WSSO12]. Adversarial [BAG12, BJR\textsuperscript{+14}]. Adversaries [BC14, XTK10]. Adversary [Yon12, KS11, LXLY12, ZPFW12]. Advertisement [Ano16g, AMHJ10]. Advertisements [AHS13]. AES [BW16, BBBP13, BKR11, BB10, DGPP10, HF14b, LB13, Mar10, MM14b, PBCC14, SY15a]. AES-Like [BW16]. AET [HTC\textsuperscript{+15}]. Affiliation [XLM\textsuperscript{+12}, XGLM14, XZLW15]. Affiliation-Hiding [XLM\textsuperscript{+12}, XGLM14, XZLW15]. Affine [BCEM15, GZHD12, ZWM14]. affine-transformation-invariant [BGHZ12]. Afraid [Par12a]. Africa [BL10]. Africrypt [BL10]. Against [Ano17b, BVS\textsuperscript{+13}, BL15, CW12b, CMA14, GDCG16, HCETP\textsuperscript{+12}, Sch13, SGH15, SLY\textsuperscript{+16}, WSA15, ASBdS16, BBBP13, BV1R12, BPR14a, BPR14b, BF1K16, BSR\textsuperscript{+14}, BK12b, Bud16, Che15, CG14a, CGCS12, DHLAW10, EWS14, FTV\textsuperscript{+10}, zGXW12, GSC17, JHHN12, LGL\textsuperscript{+12}, LLY\textsuperscript{+12a}, LWJC14, MD12b, MNP12, NDNR13, OF11, SEY14, SY15b, SD12, TLL13, WHN\textsuperscript{+12}, Yon12, ZLQ15]. Age [Bla12, SR14, Sto12]. Aged [Ree15]. Alienation [WH14, LG14, HZ14, KB11, LLLS13, ND14, Nos14, hSZZ15, TLL12, WXX\textsuperscript{+17}, XCL13, XMHD13, YZZ\textsuperscript{+14}, ZWQ\textsuperscript{+11}, ZTT16, ZCC15, OHJ10]. Aided [BGK12, BCGK12, BGB12, GMSV14, Vua10, ABBD13, LLY15, SSAF11]. APISteG [AGLW16]. Air [AUMT16]. aircraft [XWWZ16]. AK [XHC\textsuperscript{+12}]. AK-PPM [XHC\textsuperscript{+12}]. AKA [LLLS13]. AKF [KH15]. al [LLW16, LLSW16, MWZ12, PLPW13, SBS\textsuperscript{+12}, Mac14, Ke15]. al-Qaeda [Mac14, Ke15]. al. [ABJ13, SPLHCB14]. Alan [Cs12, Don14, LCKBJ12]. Algebra [Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14]. Algebraic [SK11, Tum15, Wat10, Bul10a, CFR11, SA14, YTM\textsuperscript{+14}]. Algorithm [Ano11b, AK14, BGJT14, CNR14, jCPB\textsuperscript{+12}, ESS12, GKS17, JHL12, JSZ12, JH112, JLL16, KB10, LL11, LT14a, NdMMW16, NV10, RR11, RVRSCM12, WHZ12, YPR17, Y16, ZSW\textsuperscript{+12}, Ant14, BGJT13, BMB16, CG12b, Chm10, EEAZ13, JK13, Jou13, KY10, KHM13, LC17, LR15, MS12a, MM14b, MNM\textsuperscript{+16}, MN14, PGLL10, PA10, PC14, SH11, SL10, SWW\textsuperscript{+17}, jT12b, TLT10, WGZ\textsuperscript{+12}, XTK10, ZL12, ÁCZ16, ZOC10]. Algorithmic [AY12]. Algorithmics [Gas13]. Algorithms [AMKA17, AB10b, BCG12a, BJ10, CN12, KRDH13, MR14a, TKM12, YS15, ZW15, AGHP14, Fri10a, Mac12, NACL12, NC13,
Almost [FFL12, GDCC16, Oba11], Almost-Tight [GDCC16], Altera [SMOP15], alternate [ZLW+12], Alternating [BKLS12, KDH15], AMBTC [KSSY12], America [AB10a, Bha16], American [Sch15a], Americans [ABJ13], among [BP11, MPJ+16, SS17], amount [EEAZ13], Amplification [ABF12, HMR14], Analog [KOP12, BBB+16a, BC14, BS12, CKLM13, CCKM16, CCW+10, CSTR16, CJC11, CHS15, Kup15, LW11a, LWKP12, MNS11, OO12, SEHK12, SS13, XJW+16, YWK10b, YTS12, ZH15, ZM16, Abe10, BBBP13, CZ15b, GLIC10, HH15, Jia14b, LGKY10, LWKP14, NAL17, XHH12, YY11, ZWQ+11], Application-Level [CCW+10], Applications [AMVZ12, Ana14, BKPW12, BCG+12b, BJCHA17, BS12, CZLC12a, CZLC12b, CPS16, DK15, FSK10, GKM16, GRL12, HvSi12, HN10, JWJ+17, Nac12, NV10, PJ12, RQD+15, SCPSN10a, SCPSN10b, Sha10, Ter11, TYK+12, WH17, YR11, Ano11a, CFR11, CSZ+11, CDA14, Dur15, EBFK13, FES10, Fri10a, Gil10, KO16, LWZG10, LR15, LBOX12, LTT10, MS13c, MM14b, PHWM10, PKA15, SWW+17, ZZ15], Applied [BS11, KP10, MR10, Xie12], Applying [Bar12], Approach [CTC+15, Chi16, HLAZ15, HILW12, KKA15, MKN13, MZ17, PS14, RP12, SLGZ12, Sia12, SH15, SC12, TCN+17, TLW12, Vie12, VCK15, WYCF14, ZW15, AL15, AT10, BSS11, CLZ+17, CO11, CML16, DZS+12, GGH+16b, KL13, LGFCCRP14, MCP15, NC13, SE16, WMYR16], Approaches [GWM16, LC15, SBV14, MKH+12],
Appropriate [SP15b]. Approximate [CN12, JSCM17, SGS14]. AppSec [RQD+15]. April
[FHR14, DWZ12, Gen10]. Arbitrary-State [FHR14]. Arbitration [Küp15]. Arbitrator
[WSA15]. Architect [GW14]. Architectural [MD12b, VCK+12, ZWT13]. Architecture
[BCE+10, HKL+14, KCR11, LGR14, MCDB12, MJGS12, MC11, NdMMW16, RMP10, SWM+10, SLII1, VDB+16, AL15, Ano13b, BVI12, LXMW12, MJS13, SSS11, SSPL+13, SAAB10]. architecture-independent [BVIB12]. Architectures [AMKA17, BGG+13, BJCHA17, CMO+16, CHS15, MKAA17, FPBG14, HL14, MK11, Nov10]. Area [GMVV17, HC17, LZCK14, WH17, LMJC11, Nov10]. Area-Time [HC17]. Areas [MV12, JY14]. Arguments [BCI+13]. ARX [PH12a]. Arithmetric [AIK14, Fre10, GHI11a, HSA14, IEE13, KHF10, PG12, DTZZ12, MO14]. Array
[BL12, MCDB12, NWF14]. Arrays
[LB13, TRD11, KM10a]. Art
[ABJ13, BDK11]. ARX [KN10]. Asa
[Bai12]. ASIACRYPT [LW11a, Abe10].ASIC [MKAA17]. Asking [DL15]. ASM [Vle12]. ASM-Based [Vle12]. ASP.NET
[DR11]. Assessing [CBL13]. Assignment
[LMS16]. Associated [Sar10b]. associative
[BS15]. Associativity [AB12]. Assumption
[LZC12a, LZC14, ZG10]. Assumptions
[CZF12, DN12, KM10c, PDN15, ABW10]. Assurance
[BMBV10, Bar15, KMP+11, RBNN15, WL11]. Assured
[Tan15a, WMYR16]. Asymmetric
[HG12, XLM+12, XGML14, XZLW15, ZWQ+11, CSS+13]. asymmetric-histogram [CSS+13]. asymptotic [DTZZ12, TD14]. Asymptotically [LPS12]. Attack
[Ano15c, BMS12, Bro17, CJP12, DSB15, FXP+17, zGXW12, GV14b, GDCC16, HCTETP+12, HLAZ15, JL1H12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LWKP12, LWPF12, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, CJP15, DDFR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LHYH14, LWKP14, MB11, MNP12, NZL+15, SX16, WYL13]. Attackers [BL15]. Attacks
[ARP12, Ano17b, BGK12, BFK16, BKK14, Che15, CMA14, DGI12, DHLAW10, DHB16, EWS14, GPT14, Hay13, JSP+16, JW17+17, KNR10, LLLC11, LWW12, LWCJ14, LCL17b, MD12b, P315+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, WW14, WHN+12, XNG+14, YCM+13, ZLQ15, BBQP13, BVIB12, BR1+14, dCCSM+12, DCA+12, DJL+12, Dara16, EA12, FTV+10, FIO15, GPP+16, GBN11, KM10a, KPS10, LWKE11, NSDR13, OF11, PX13, TS16, TY16b, TLL13, WWBC14, XW11D12]. attempt [Fel13]. ATtiny [EGG+12]. Attribute
[AAC+16, AHL+12, BFK+10, Boy13, CD16, FHR14, GZZ+13, GSW+16, Gli12, GV12, HSM12, Her14, KGP12, LW11b, LW11c, LW12, LJHC12, LY+13, LHL+14, LAL+15, LHL15, LW16, OT12, PB12, RVH+16, Rao17, SSS12, WLL15, WLL16, XCM13, XWL16, XHX+17, ZPM+15, ZQQ15, ZHW15, HKHK13, LCL+15, LFWS15, LYL15, LJW+17, RD17, XWS17, YCT15, ZWM14, ZML17]. Attribute-Based
[AAC+16, BFK+10, Boy13, CD16, FHR14, GZZ+13, GSW+16, GV15, HSMY12, LW11b, LW11c, LW12, LJHC12, LY+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSS12, WLL15, WLL16, XCM13, XWL16, XHX+17, ZPM+15, ZQQ15, ZHW15, HKHK13, LCL+15, LFWS15, LYL15, LJW+17, RD17, XWS17, YCT15, ZWM14, ZML17].
Attribute-Hiding [OT12, ZWM14].
Attributes [CG12a, Yon11, LCL+17a].
Attribution [XHC+12, FNP+15].
Auction [Con10, HJM+11].
Audience [DTE17].
Audio [DA12, FM15, GCK12, HGT15, KD12a, KD12b, LSL12b, TC10, gWpNyY+14, XNG+14, XNRG15, ZS12, LSQ11a, SKEG14, yWpNyL11, YQH12].
Audit [YNR12b].
Auditing [LMD16, TCN+17, YYS+16, YXA+16].
August [AB10a, JY14, MV12, Rab10].
Austin [IEE13].
Authentic [HLT+15, SZMK13].
Authenticate [HM12].
Authenticated [Alo12, BCO13, BDMLN16, CLY14, CCS14, CRE+12, DS11, EAA12, ESS12, FFL12, GTR11, GL12, HCL12, HL10a, HCL+14, HEC+12, LH11b, LCCJ13, LTT10, MR14a, MMY12, MHKS14, MSU13, PTT16, Sar10b, Smit11b, TW14, XLM+12, XHC+12, XGLM14, XZW15, YS12, YLW13, YRT+16, Yon12, ZPZ+16, ZXH16, AIB+16, CTL13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HL11, HPY10, ISC+16, LWS10, LH111, LML+13, NCL13, Nos11, Nos14, PPTT15, SMBA10, TCS14, Tso13, TKHHK14, WZMI12a, WZM12b, WTT12, XWXC14, XCL13, YC12, YZZ+14, ZT16, ZG10, ZZC15].
Authenticating [BS12, CHX13, GRL12, OKG+12, RPG12, WY12, ZCSW15, LFGCGCRP14, PGLL10].
Authentication [ASO14, AAZ+16, ACAT+15, AUMT16, BL12, BGE+12, BCM12, BSSV12, BCD+12, Bis17, BF11, Boy16, BKJP12, BSV12, CCGPDMG12, CTC+15, CC14, CCW+10, CJ13, CD12, CJ12, CLH13, DL15, DBPS12, DPW12, DKP12, FLH13, FR16, FMTR12, FD11, GHS14, Gli2, GI12, GM14, GU13, GMV17, GCK12, HZC+12, HvS12, HLLC11, Har13, Hay13, HBCC13, HM10, HCPB12, HETTPL+12, HKL+12, HXC+11, HLC11, IGR+16, JN12, JCMI12, JAE10, KP12, KRM+10, KSD+17, KPC+11, KLY+12, KTA12, KGP12, Kim15, KPKS12, KLM+12, KO16, KH10, LCL11, LLG15, LLCL15, LNZ+13, LZCK14, LNX15, LLZ+12, MWZ12, MEFO12, MKH+12, MBC15, MRRT17, MRS+17, May15, MLBL12, Mor12, MSKRI17, MPM+17, N11, NR12, NLLJ12, NLY15, OdH12, O012, O12, PCGD14, PPRT12, PDT12, PWVT12, RS11, RWI14, RSN14, Saa12a, SBS+12, Sar12, SGIC16, Sch15b].
Chain [EAA+16, KPW13, QZL+16a, QZL+16b, YFT17, CR12]. chaining [EA11].
chains [HLYS14, JCHS16]. Challenge [AD12, GHS14, YDH+15, ZCC15].
Challenges [CN12, FS15, Fra15, LLGJ16, MRS+17, SBV14, KJN+16, WS14]. change [ZWT13].
changed [Mac12]. Channel [ASN11, CDK+10, CBL13, EWS14, GWM16, GPT14, KOP12, LGR14, NDC+13, PRC12, SG15, TT12, ADG16, BVB12, DMWS12, DJL+12, JLT+12, MFP13]. Channels [ASN12, BGN17, DKMR15, EPAG16, KW14, Vua10, DMV14, LGR14, NDC+13, PRC12, SG15, TT12, ADG16, BVB12, DMWS12, DJL+12, JLT+12, MFP13].
Chaos-Based [RR11, RVRSCM12, LW13c, ZLW+12].
Chaotic [BCGH11, Ye10, GCH15, ISC+16, KLW+16, LW10, NES+14, WGZ+12, ZT14].
Chaotic [BCGH11, Ye10, GCH15, ISC+16, KLW+16, LW10, NES+14, WGZ+12, ZT14].
Chapman [Ful10]. Character [SS12b].
Characteristic [BGJT14, SR10, BGJT13, Jou13].
Characterization [ALR13, BS13b, DPCM16, YZLC12, DDD14]. Characterizing [Ash14, JR13, MPJ+16].
Chattarjee [Kat13]. cheat [WS12].
Check [GST12]. Check-before-Output [GST12]. Checkability [LHL+14].
Checkable [IW14]. Checking [FYMY15, SYY+17, XYA+16].
China [BYL10, IEE11a, LTW11, Yan10]. Chinese [HF14a]. Chip [Bis17, MDAB10, BAB+13, BGG+13].
Choquet [SH11, SM11, SNM14]. Chosen [FSGW12, zGXW12, HLW12, HPY10, LCT+14, LZC12a, LLML12, MH14, RS10, WWHL12, GLM+14, GH12, LZC14].
Chosen-Ciphertext [RS10, FSGW12, LCT+14, GH12, LZC14].
Church [ABJ13]. CHURNs [RBNB15].
Cipher [BW16, BFMT16, BC+12b, CMLS15, CGCS12, DG12, DWZ12, Fis15, FXP+17, GLLSN12, GCS+13, HZ11, IOM12, JKP12, KR11, KWS+12, LPS12, LWZ12, LJ17, LWKP12, LWPF12, MRTV12, MHC12, MS12b, OGK+14, PH12a, PRC12, WSSO12, WHN+12, AMS+10, BNY14, CR12, HKT11, Hol12, Jeo13, KD15, Lew10, LC13, LHH14, LWKP14, MNP12, PL16, Rec15, RS14, Sar11, WYL14, WWBC14, LGL+12].
Ciphers [ABS+12, BMS12, BKLS12, Bru12, CWP12, DGJS12, DJG+14, EGG+12, EKP+13, GT12, GST12, GNL12, IS12, KPC+14, Kl10, LCLW17, LGLL12, LJ16, MD12b, NN12, Pud12, Sls12, SEHK12, Vua10, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KMO10a, LWK11, MHT10, MHV15, QGL13, SKK10, TQL+14, WB12].
Ciphertext [BDPS12, CWWL12, zGXW12, HLW12, JMG+16, KA17, LZC12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XMMC13, XW116, ZH15, FSGW12, GLM+14, GH12, HPY10, HKII13, KTT12, LCT+14, LFWS15, LZC14, RD17, SGM16, XS17, LAL+15, LHL+15]. Ciphertext-only [KA17].
Ciphertext-Policy [Rao17, XMLC13, XWL16, ZH15, LFWS15, XWS17, LAL+15, LHL+15].
Circle [SC10].
Circuit [Kar12, MTY11, XWS17, XWL16, Lai12, MS13a].
Circuit-Size [MTY11].
Circuits [AIK14, AS17, BR14, GGH+16a, GHII1a, GVW15, SSI0b, SS12a].
Circumventing [BAG12]. CISSP [STC11].
Citizen [Ano16d]. Claims [SKGY14].
Class [BCG12a, SY15a, XYXY11, BJ16,
Classes [ÁCZ16]. Classical [JEA+15, MSU13, SSU12, CR12, RK11].

Classification [HPC10, KAHKB17, SGP+12]. Classifiers [KGV16, LCM+17].

Claudius [Hol12]. CLEFIA [LWZ12, TSLL11, TS16, WB12].

CLEFIA-128 [TSLL11]. CLEFIA-type [WB12].

Client [ASM12, CTC+15, FD11, RAZS15, Vle12, FA14a, FA14b, hSSZ15, WT10a].

Client-Based [ASM12]. Client-Centric [Vle12]. client-server [FA14b, hSSZ15].

Cloud [AJA16, BCQ+13, CWL+14, CWL16, CDFZ16, CXT+14, CLW16, DXA14, FCMI4, FPY15, JLS12, KMSMI5, KKA15, KIP15, LA15, LYZ+13, LGR14, LLC+15, LNYX15, PSM17, Pet12, RSGG15, SKH17, TV15, Vle12, WWW17, XNKG15, XWSW16, XMLC13, XWLJ16, XJW+16, YDY+16, YHL16, YXA+16, ZDL12, ZLDC15, ZYG16, AaBT16, AZPC14, ASO14, AAZ+16, BK12b, CFVP16, CLH16, CZ15b, FH13, HSM13, Jeo13, KKA14, KKM+13, KKM+14, LKX+14, LZY+16, LAL+15, LW13a, LYL15, LHL15, LCY+16, LZCI7, MLMI6, NB13, PP11, RAO17, SYY+17, SLM10, SKB+17, SWW+16, SWW+17, TLMMI3, WL12, WMX+17, XXX15, YYS+16, YWT+12, ZDW+16, ZHT16].


Cloudier [CCE16].

Clouds [BCQ+13, RSN14, HFT16, IC17, JKL+16, LFWS15, LL16a, YN+16].

Clustered [DS11]. Clustering [KRDH13, VS15].

CMAC [SKK10]. Co [MBR15].

Co-Processor [MBR15]. coal [KO16].

cocktail [OHJ10]. Code [AD12, Bud16, CCL+13, Cop10a, Fox13, HG12, KSY12, PY+13, SS13, War11, ABB13, Ant14, Bha16, Bri11, CCLL11, GIJ+12, MCP15, McG11, Moo14, OF11, PA10, Wes15].

Code-Based [HG12, SS13, MCP15].

code-breaking [Ant14, Bri11].


codebreakers [Ano11c, Bud16, Smi11a]. Codebreaking [Bai12, Cop10b, McK10, McK11].

Coded [She14]. Codes [BBC+13, Bay10, DBPS12, FMM14, GMN15, GRI15, HCT17, KWT14, MBR15, OTDI0, SEIY14, ST14, TL12, WGF16, WSS12, Xie12, YTP11, Yek10, ATI+10, Bul10a, CZ15a, Cti13a, Hea15, LTT10, MG15, OSI11, Tan15b, YSJ14, Ayu12, Low12].

Codevelopment [DF16].

Coding [Che11, CCL14, CCA14, DH17, Hes12, LCLL15, Per13, AZF+12, Bul10b, DTZZ12, JZS+10, KM11, NDNR13, OF11, Tan15b, YTM+14, Kim15].

CoDiP2P [NCCG13]. Coercion [CW12b].

Cognitive [PP11, Kim11, RP12].

Coin [ALR13, CLP13a, DSMM14, M14, BB14, Wag16].

Coins [Fok12].

COIP [BCF16]. COIP-Continuous [BCF16].

Colbert [Dew11].

Collaboration [CRE+12, PCPK14].

Collaboration-Preserving [CRE+12].

collaborative [LT14b, HB13].

collect [Sch15c].

Collision [BK12a, ZL12, AKY13, SKP15, SBK+17].

Collison-based [ZL12].

Collision-Resistant [BK12a].

Collusion [MMSD13, RVH+16, FLZ+12, GMRT+15].

Collusion-resistant [GMRT+15].

Collusions [GVW12].

Color [BCPV11, DD13, FR16, LW10, MR16, YWNN15, SNM14, yWpyWypN13, WZG+12, YSC16].

Colossal [Hai17].

Colossus [Cop10a, Cop10b].

Coloured [PS14].

Column [FS15].

combating [FTV10].

combinational [MS13a].

Combin [PP10b].

Combining [Chi13a, CDF+10].

Coming [SO15].

Comment [LCLL15].

Comments [IC17, Kim15, hSSZ15, TCL15, XWS17].

Commerce [Bla16, HVS12, Orm16, Ano11a].
Commitments [Pas13a, CSZ+11, LP11].
Committee [Bla16].
Common [CN12, DHB16, ESR14].
Communication [BPSD17, CCM17, CCW+10, FMS12b, Gas13, GPVCDiBR012, K14, Low12, OKG+12, Wan13, ZC13, ZHW+16, ADG16, DKL+16, HCCCI11, HLYS14, HPY10, KRM*10, KTU16, LT13, LyWSZ10, RK11, SSAF11, SSPL+13, Ts13, YKGK13, Zhu13, vDKS11].
communication-efficient [Tso13, Zhu13].
Communication-resource-aware [Wan13].
Communications [JTZ+16, KSD+17, OO12, SMS14, Edw17, FHH10a, FGCGCRP14, LLZ+16, RS15, WDZL13].
Community [BPS16].
Commutative [CLHC12, SLGZ12].
Commutativity [ABR12].
Commuting [Fuc11, AKG13].
Compact [CFOR12, CKLM13, EGG+12, MAS16, VSR12, ZMW16].
Companion [KR11].
Comparable [XHX+17].
Comparative [DDR+16, MHV15, NR11].
Comparison [CGCS12, DWB12, HPC10, KU12, ST14, HM10, LCM+17].
compartmented [EZ15]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16].
Compression [CNT12, DA12, PMZ13, PP10b, TCN+17, WHZ12, CMMS17, DTZZ12, K14, Li10, LPZJ15, PP11, QZ14, SI12].
compression-based [SI12]. Compression/Decompression [PP10b].
Compromise [YNR12b, GBNM11, PX13].
Computability [Gas13].
Computable [LGH+17, FWS13].
Computation [ARH14, Ash14, BDOZ11, Fri10b, GST12, GVW12, GHKL11, HP14, HC17, IEE11a, KW14, KMO14, LHM+15, LQD+16, MPP14, Mal13, NSMS14, PST13, SVCV15, Wat10, ABPD15, AB10b, LDDAM12, PHGR16, TG12, vDKS11].
Computational [BCO13, RD17, TBCB15, HRS13, SDM14].
Computations [ARM15, KHP16, Nac16, ADMM16, BK12b, LR15, SSAF11, TLMM13].
Computer [BGK12].
conceal [EEAZ13]. Concept [TMC15].
Conceptual [PMZ12, SPM+13, TSH14].
Concrete [BS14]. Concurrent
[CLP13a, FCM14, GJO+13, MRM10,
OOR+14, AKG13, SRB+12, XLWZ16].
condition [TD14]. Conditional
[HBCC13, KPW13, LLG15, LSLW15,
XJW+16, FSGW11, FSGW12, HDWL16,
LCT+14, SKB+17, Tan12b]. Conditionally
[ZJ14]. Conference
[BC11, CGB+10, Che11, Cra12, Dan12,
Dun12b, FBM12, GLIC10, IEE11a, JY14,
LCK11, LW11a, LTW11, Lin14b, PJ12,
SNJ11, Sah13, Yan10, AB10a, Abe10,
BYL10, BL10, Gil10, GG10, HWG10, Kia11,
LH10a, Pie10, Rab10, vDKS11]. Confidential
[HS11, AZPC14]. Confidentiality
[BFK+10, HLLC11, OFMR16, WDDW12,
Bia12, CHX13, ZHT16]. Confidentiality-Preserving
[OFMR16]. Configurable [CVG+13]. Configuration
[Bis17]. Configurations
[BWLA16, DF11, EM12,
FZT14, GWWC15, KMO14, MSas12, Rog16,
Sar10b, ST14, WZ15, WMS+12, XHX+17,
Msas13, SA14, YK12, YKC+12, ZCLL14].
Constructions
[BCF+14, DQFL12, HL10b, SNJ11, SES+16,
CZ15a, CGKO11, NAL17, Zim10].
Constructive
[BCF+14, DQFL12, HL10b, SNJ11, SES+16,
CZ15a, CGKO11, NAL17, Zim10].
Constructive
[Mau12, WB12]. constructs
[BP10]. Containing
[XWDN12]. contemporaries
[LCXB12].
Continual
[BKKV10, XZ12, YCZ12].
Continual-Leakage
[YZ12]. Continually
[DLWW11]. Continuous
[ACAT+15, BCF16, DHLAW10, FMNV14,
MSKRJ17, PYP10, Sch15, Yan12].
Continuous-Tone
[Yam12]. contract
[Men13]. contrast
[DDD14, GLW13, LW10a, MM14a].
Contributory
[WQZ+16]. Control
[ATS15, BCF10, DLZ+16b, HHS+15,
LMG+16, MCK12b, NA10b, QZL+16a,
RSM14, SGC14, TBCB15, YCZ12].
ACK+10, AMHJ10, CLH+16, CO11, Cra11,
JAS+11, LCL+17a, LCL+15, NZM10,
Sch15c, SA15, Tan12b, XHH12, ZML17].
Controllable
[FH13, ZLDC15, ZHT16].
Controllable
[FH13, ZLDC15, ZHT16].
Controlling
[FMTR12, Har16]. Controllers
[AMH+16]. controls
[CGH11]. controversy
[McG11].
Conversations
[BFC+10]. Conversations
[KPKS12]. Conversion
[BP10]. Convertible
[LH11b, HL11, LHH11, XWXC14].
Convolutional
[MG15]. cookies
[DCAT12].
Cooperative [LLZ+12, ZLDC15, WQZ+13].
Coppersmith [Dra16], coprocessor [ABC+12, BGG+13, IBM13b].
coprocessors [GCVR17], Copy [YT12, MHT+13]. Copyright [SJ12, GJ13].
Core [LB13, YS15, RS17, HLYS14]. Correct [PST13]. CorrectDB [BS13a].
correcting [ATI+10, LTT10, MCP15]. Correctness [WS13].
Corrigendum [WZM12a]. cosmography [Pet11].
Cost [ABC+17, AMH+16, CMS15, CJP12, GI12, HLT+15, Man13, WMX+17, CZ14, CJP15, Sar10a, YL11].
Cost-Effective [HTL+15, WMX+17].
Costs [KHPP16]. couldn’t [Bha16]. Countdown [Zet14].
Counter [ARP12, Fay16].
Counterexample [KPW13]. Counterfeit [YFT17]. Counterfeiting [Ano16e].
counterfeits [GSN+16]. Countermeasure [BBB+16a, MD12b].
Countermeasures [BGN17, EWS14, PZPS15]. counting [LLY+12a].
Coupling [SMS14]. cover [UUN13]. Covert [EPAG16, JTT+16, NSA15, LT13, LywS10, SRB+12].
CovertBand [NTKG17]. Cozzens [Led16, Sch15a]. CP [TY16a]. CPM [PYM+13].
Creativity [WP15].
cultural [JMW+16, KKM+13]. XMHD13].
Credentials [CG12a, SSW12]. Credible [ZW15].
CRM [LHM+15]. Cropping [SR12b].
Cross [CLY14, DSB15, LHM+15, MV16a, YGFL15, ZXH16, ZTSR12, SS17, der10].
cross-matching [SS17]. Cross-Site [DSB15].
Cryptanalysis [BW12, Bor10, CWP12, CGCS12, DG12, DJG+15, Far14, GST13, Gor10, Hin10, IO12, Jec13, Kh10, KN10, KWS+12, LH10b, LNM+11, LFJ16, LJ16, MWZ12, NXB13, OTo10, PSOMPL13, SPLHB14, SM10a, SM10b, TY16a, TG17, Vua10, Wag10, WYYZ11, WYY11, WSO12, WYY14, XQL11, YMW11, AP11, BMB16, BKR11, Bul10a, Bul10b, Con12, Eiss10, Her10, KD1H3, LLVM16, LFW+16, Nov10, RTF+11, SDM10, SDM14, Sun11, SvT10, Tam15, TSL11, WYL14, WWBC14, AY12].
Cryptanalyzing [ZLW+12]. CryptDB [PRZB12]. Crypto
[Goo12, Pfl10, Rab10, SCSN10a, SCSN10b, W11, BS+14, BGG+13].
Cryptoclass [Ayu12]. cryptograms [Shy15]. Cryptographer
[Dun12b, K1a11, Pie10]. Cryptographers [Ano16d, BPS16, Goo12]. Cryptographic
[Abe12, AMKA17, AD12, AVMZ12, App15, BMP12, CGK12, BGB14, Bar15, BCM+15, BIKK14, BLS12, BDP11, BFCZ12, BG1H15, B1a2, BKL+13, BSJ15, BNA15, CCK12, CCCK16, CFE16, jCP+12, CBL13, Cor14b, Des10a, DQFL12, DR11, Eiss17, FKS+13, FY11, FLW12, Gir15, GM11, GL10, GGG11, Har16, HN10, HHH+13, HST14, HSA14, IBM13b, JR13, KOP12, LV11, Loe15, MVV12, MP12, MKAA17, MK12b, NIS13, NA10a, PTT16, PFS12, PS14, P12, RMP10, RSGB12, Rja12, RH1P15, SK11, SEY14, SF1K15, Sch12c, Sev16, GSY11, SP15b, SDM+12, SR14, SO12, TW12, Tom16, VYZ12, YNR12a, YNR12b, YS15, ABDP15, AY14a, ABB+14, ABF+14, ABC+12, BFG+14, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DJN14, EBFK13, ESR14, GHG+16b, Gil10, GLR13, KAS15, KKK+16].

cryptographic [LGKY10, MS13c, MMZ12, MM13, Mes15, MN10, NDNR13, Pal15, PLPW13, PSdO+13, QZD16, SD10, WT13, WMX+17, YSM14, Zim10, Sha10].

Cryptographic-Key [SK11].

Cryptographical [KU12].

Cryptographically [ADD10, BCGH11, BJL12, MC11, NDG+17, PLSvLE10, SVCV15, GCH15, HJM+11, SA14].

Cryptography [ACZ16, Ano15b, Ano15c, Ano16a, Ano16g, App14, ARM15, Bar12, BGK12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BCF+14, CNR14, CJFH14, Cas10, CGMO14, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, FSK10, FBM12, Fr10, GFBF12, G13, GP12, GPT12, GLW12, Ham17, Hes12, HGI12, JTT12a, KM10c, KP10, LSL12a, Lin17, LWL10b, LWHS17, LPO+17, Mau12, MR14c, Mic10b, MV12, NNA10, NS12, Orm16, PP10a, PPH12, PG12, RW12, RGG16, SY14, SG15, SOG15, Sch16, Sen10, SS13, SK12b, SA16a, Sim15, SGE14, Sm16, Sta11a, Ste15a, VS16, W12, Wes16, Yan12, Yan11, YTS12, ZZCJ14, vTJ11, AMORH13, AAT16, AAA14, ABBD13, Ano11a].

cryptography [ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BAB+13, Blo12, BSR+14, BSW12, BBB16b, CFR11, Cha13b, Cho14, CSTR16, Con12, CDSL14, DDD14, Dav11, DDI3, Dur15, Far14, GCV17, Har15, Hof16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Krc13, LLLK10, Lin14b, LWL10a, Lid12, LLY14, MSL13b, M12a, MCP15, Mic10a, NLYZ12, Nov10, Opp11, PHMO10, PP11, RY10, Sah13, SK14, SSAF11, Sta11b, Sti11, Svo14, VDO14, VN17, WYK12, YT11a, YSC16, YDH+15, Y11r, vDKS11, Che11, LZJX10, Nac12, Cou12, Ful10, Gas13, Low12, Me10, Mu10, Ter11].

cryptography-based [BOB13].

Cryptography-Related [Cil11]. Cryptol [Lau12]. Cryptology [BC11, Bro11, CCM10, G13, G14, FES10, FGPGP14, Gil10, GG10, H11, Har15, HH15, HOF16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Krc13, LLLK10, Lin14b, LWL10a, Lid12, LLY14, MSL13b, M12a, MCP15, Mic10a, NLYZ12, Nov10, Opp11, PHMO10, PP11, RY10, Sah13, SK14, SSAF11, Sta11b, Sti11, Svo14, VDO14, VN17, WYK12, YT11a, YSC16, YDH+15, Y11r, vDKS11, Che11, LZJX10, Nac12, Cou12, Ful10, Gas13, Low12, Me10, Mu10, Ter11].
Disreputable [ABJ13].

Distinguishers [SEHK12, ZSW+12, AY14b, AP11].

Distinguishing [KM0a].

Dissection [HK14].

Disruption [Dun12a].

Disruption-Tolerant [HK14].

Diversity [UUN13].

NACLR12, YHHS16, YL11].

dithered dCCSB YKKL12, ZLDC15, BLV17, CSTR16, BB14, BGP [SS12b, MN14].

Divisors [CN12].

Document-centric [BPP10]. Documents [Bl12, HCDM12, Sta13, ZDL12, CH11, GA11, SR14].

Does [LRW17]. Doesn’t [RS11, SS12a]. dog [Ran14].

Doing [JCM12].

Document [AGW15, BDFK12, CLY14, DG17, LA15, MR16, PDR12, SGY11, WLZL12, gWpNyY+14, AMK12, BGAD12, GJJ13, IGI1, LXCMI11, LPZJ15, LBR12, PWW10, SCKH10, yWpWypN13, YWK+10a, YCM+13].

Domain-Specific [BDFK12].

Domains [LQD+16, LRW14, KGO10, NES+14].

domination [GJM15]. don’t [FHV16].


Double [AK14, ARM15, Lin15, PTKT12, Sas12].

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

Doubl [CFZ12, CW14b]. Doubly-Spatial [CFZ12].

Douglas [Ber16a].

Down [Ano17b, McG11].

Download [ZGC16].

DPA [ZJ11].

DRAMs [LSC+15].

Drift [GKSB17, JSZS12].

Drift-Compensated [GKSB17].

Drive [SYC+17, Mac12, SYW17].

Drive-Thru [SYC+17, SYW17].

Driven [BMP12].

DriverGuard [CDD13].

DRM [Pet12].

DSA [Dra16].

DSP [MS13c].

DSPs [DP10].

DSS [Ano13a].

DSH [YLS12].

DTKI [YCR16].

DTLS [AP13].

DTRAB [FTV+10].

Dual [BWR12, CCG+16, HF14b, NLYZ12, BW13, CFN+14].

Dual-Rail [HF14b].

Dummy [GST12].

duplication [LWLW11].

Durable [LY15].

During [ABJ13, RS17].

DWT [SJ12].

dyadic [MO14].

Dynamic [EKB+16, FHR14, HH15, LHM+15, MWZ12, MM12, NKWF14, PPS12a, PNRC17, SSW12, SY14, SKV12, SGC14, VMV15, XNKG15, XWSW16, XZY+12, ZXYL16, CTL12, CSTR16, DSCS12, EA11, GLM+11, JJS+10, KKM+13, KPBP17, LXMW12, LHM14, LZX17, NPJ+14, PSJ+13, SES+16, SSS1, SGM16, YD17].

dynamic-identity [JJS+10].

dynamics [AaBT16, LTC15a, Lüd12].

dynamics-based [AaBT16].

dyslexic [Bha16].

e-commerce [Ano11a].

e-exam [Mor12].

E-health [WMX+17, IC17, JK11].

E-Learning [Yon11].

E-passport [LJX10].

e-rental [LY14].

E-Voting [GPRH14].

E2 [WYL14].

EAC [LJX10].

Each [YLL+12].

EAP [FLH13, HZC+14, ZCL14].

EAP-based [HZC+14, ZCL14].

Early [Bro11, And13].

easier [MBF+13].

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

Eat [DSSDW14].

Eavesdropping [CW16, PX13, YSL14].

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

ECC [SBC15, MWC14].
ECC-Based
ECDSA
Echo
Economy
EdDSA
Edition
Education
Edwards
Effective
Eects
Eciency
Ecient
Ecological
Echo-Based
Economic
Economies
Edwards-curve
Echoes
Eight
Eighth
Eight-round
Einfuhrung
Effort
Effort-Release
EHealth
eID
eight
Einführung
Elebirt
Election
Electrocardiography
Electromagnetic
Electronic
Elementary
Elements
Elevation
Elliptic
ELmD
Embed
Embedded
Embedding
Embeddings
Emerigable
Emerged
Emergence
Emergency
Emerging
Empirical
Employees
Enable
Enabled
Enabled/disabled
Enciphering
Encoded
Encoding
Encounter
Encrypted
Encapulating
Encapsulated
Encapsulator
HTZR12, HCDM12, IBM13a, JSCM17, Kaw15, KGV16, LA15, LQD16, Lop12, Mur16, NBZP17, NNAM10, QLL17, SAKM16, Sia12, Vai12, WBC10, XSW16, YDY16, ZDL12, ZYX16, AZH11, BTPLST15, BGP17, BKV13, BL11, CH11, Cri16, DKL16, DRD11, ED17, FTV10, Gen10, LXX14, LZY16, LW13a, PRZB12, SWW17, Suc12, TKMZ13, ZLY10, ZHT16.

Encryption [CC10, Mar10, dRSdlVC12, LFGCGCRP14, Pow14].

Encryption [ADM12, AV12, Alo12, AAC16, Ano15b, AKP12, ABF12, AS16, BVS13, BWLA16, BPR14a, BPR14b, Bel16, BDOZ11, BPR14b, Bel16, BDOZ11, BWR12, BS14, Bla16, BKLS12, BDPS12, BHJP14, BDMN16, Boy13, BV11, BV14, BGV14, CVM14, CMO16, CWWL12, CN12, CZF12, CLHC12, Ch15, CGL12, Chi12, Chu16, CRE12, CNT12, CLW16, CD16, DR10, DN12, DFJ10, Des10b, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJJH12, FUL12, Fuc11, GWWC15, GGH16a, GM13, GZZ13, GSW16, GH11a, GH11b, GHS12, GHPS12, GDCC16, GV12, GWV15, GL14, GL12, Gue16, HSMY12, HZ11, HG12, HC17, HTC15, HP12, JLS12, Jia14a, JR14, Kam13, KB10, KME12, KTT12, KOS16, KKA15, KFOS12, KHP16, KS12, Led16, LLSW16, LW11b, LW11c, LW12, LLLC12, LY12, LHL14, LLC15, LTZY16, LSLW15, LH11b, LB13, LY15]. Encryption [CW12a, CDF10, CM13, CGKO11, DDL16a, DDM17, DTTZ12, FH13, FG112, FSFW12, Fay16, GMOGCC15, GH13, GHPS13, GLM16, GI12, HG12, HG12, HZW14, HWDL16, HT13, HR11, HL11, HT16, HKHK13, JCHS16, Jia14b, JHCC14, Kam16, KMB13, KMK14, LL16, LXL17a, LXL15, LXL14, LFWS15, LPdS10, LHH11, LW10, LW13b, LZX14, LPZ15, LCY16, LZX17, LJW17, LIL16a, LW13c, LCS12, MMS17b, Mes15, Mon13, MS13, NES14, Pet12, Ran16, RG10, RWW13, RFS10, SES16, Sar11, SYL13, SE14, SE16, SH11, SN11, SNM14, SLZ12, SY15b, SLM10, SKB17, Spal16, SGM16, Tan15, TPL16, jT12b, WGJ10, WY10, WWWY11, WWWY11, WHY12, WZD13, WZG12, WXZ16, WXWC14, XSWC10, XXX15, XWS17, YT11b, yYqWqZC13, YCT15, YLZ16, YL11, ZWQ11, ZZZ1, ZLW12, ZXJ14, ZWM14, ZT14, ZCC15, ZML17, Z12, ZD16, ZHT13, Wan14, LAL15, Kat13]. Encryption/Decryption [KB10]. Encryptions [zGXW12, LG12, SLY16, RD17].

Explicit [AQD12, FHS13, FIO15, ZZC15].

Exploitability [CFN14]. exploitation
[MAK12, NCCG13]. Exploiting
[ACK10, BDGH15, VDB16, ZPZ16].

Exploits [ZGC16]. Exploration
[AUM16, ABDP15, RYF13]. Exploring
[Cil11, FNP15, TLCF16, WHC15].

exponent [SM10a]. exponentially
[RK11]. exponentiation
[VN17].

F5 [LLY12b]. Fa [FMS12a]. fabricating
[WW13]. Fabrication
[VDB16].

Fabrication-Induced [VDB16]. Face
[AQD12, XHH12]. Facial [KRB12].
facilitate [Chi13a]. Facsimile
[Ano16d].

Factor [HXC11, LLC11, AIB16, CLP13b, DMWS12, HC12, IC17, JKL16, JMW16, Lit14, WW14].

Factoring
[APPVP15, LML12, MM13].

Factorization
[Cou12, FS15, Kuz11, YAM15, Mes15, TPL16]. Failing
[Cer14].

Fails [ABD15]. Fair
[ALR13, CSV15, DSMM14, DG15, WSA15].

Fair-Exchange [DG15]. Fairness
[ALR13, Ash14, GHKL11, Wag16, MV16b].

Fake [KU14]. Fallen
[HCPLSB12]. False
[LLZ12, CDGC12]. Families
[KU12].

Family
[BMS12, DGIS12, DJG15, FLG10, FFL12, GNL12, MFG16]. Fanin
[SS12a].

Fast
[BLAN16, Bru12, CHS15, GSN16, NR12, WHZ12, WQZ13, ZHW16].

FHH10a, KHMB13, MBB11]. FastAD
[MISA10]. Faster
[CN12, HVL17, TH16, Ant14].

Fault
[AMKA17, BMS12, BBB16a, FXP17, GST12, JWJ17, JKP12, JT12a, LGL12, LCLW17, LGLL12, MKRM10, MKA17, PH12a, RZZ15, SEY14, YGD17, BBP13, PBCC14, WMYR16].

Fault-Based
[BBB16a]. fault-resistant
[PBCC14]. fault-tolerant
[WMYR16]. FBI
[Bha16].

Feedback-Based
[ZGC16]. Feedback
[BWLA16, GST13, GPT14, PCPK14, GPP16]. extractors
[Zim10].

extraordinary
[Hol12]. extreme
[GJ13].

Extract
[AN12].

Extract-Transform-Load
[AN12].

Extractability
[BCP14b]. Extractable
[CLLC12b, CLC14]. Extraction
[BWLA16, GST13, GPT14, PCPK14, GPP16]. extractors
[Zim10].

F5
[LLY12b]. Fa [FMS12a]. fabricating
[WW13]. Fabrication
[VDB16].

February
[Ano10, DDS12, Dan12b, Kia11, Lin14b].

FedCohesion
[CCFM12].

FedCohesion-Based
[ZGC16]. FedCohesion
[CCFM12]. Feedback
[BWLA16, GST13, GPT14, PCPK14, GPP16]. extractors
[Zim10].

Fidelity
[BCP14a]. Field
[GHPS13, HSA14, SS12a, TGC16]. Fields
[ARH14, BGJT14, HVL17, AA14, BGJT13, CZ15a, LBOX12, ÖS11].

Fighting
[Ano16e, Wu16].

Filter
[DKH15, KDH15, SML12, SEHK12]. FHSD
[SP15a]. FI
[YNR12a]. FI-BAF
[YNR12a].

Fiat
[BDSG13]. Fibonacci
[FM15].

Fidelity
[BCP14a]. Field
[GHPS13, HSA14, SS12a, TGC16]. Fields
[ARH14, BGJT14, HVL17, AA14, BGJT13, CZ15a, LBOX12, ÖS11].

Fine
[CDD13, ZML17, CLH16, FSGW11].

Finding
[Hof16, Ste15a]. Fine
[Ano11b, Ber12, DAS12, Dan12]. Finding
[Hof16, Ste15a]. Fine
[CDD13, ZML17, CLH16, FSGW11].
Fine-Grained [CDD13, ZML17, CLH+16].

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

Finger [KLY+12], Fingerprint
[MR14b, KKi14], Fingerprinting
[ZS12, FLZ+12, RS17], Finite
[BGJT14, CHS15, GMNS15, HVL17, AA14, BGJT13, CZ15a, LBOX12, OSI11].

Finite-State-Machine [CHS15]. First
[DR10, PC16, AB10a, BCV12, Kim11,
LCKBJ12, Mic10a, SBK+17, Zet14].

Fischlin [ABGR13]. f'itful [MPJ+16]. fit
[KGO10]. Fix [DLV16, HLV10]. Fixed
[Chn10, Lim11]. Flame [Goo12]. Flaw
[Moo12, SH15, Ste15a]. Flaw-Finding
[Ste15a]. Flaws [DR11, HLV10].

FlexDPDP [EKB+16]. Flexible
[LGWY12, BGG+13, ZL12]. Flexlist
[EKB+16]. Flexlist-Based [EKB+16]. flip
[Wag16]. Flow
[ATS15, KL13, LWY12, PPR+12, SRB+12].

Flowers [Hai17]. Flows
[CDD13, HKB14, WYL13]. fly [PS14].

Foolproof [FFL12]. Force
[JR14, CJP12, CJP15]. Forensics
[CFXY17, AKM+11, QZ14, SM13]. forged
[HREJ14]. forgeries [YQH12]. Forgery
[LC15, BM13, LWLW11]. forgotten
[And13]. form [DWZ12, Kre13]. Formal
[ACF16, EWS14, HAS14, KGO10, PLCGS11,
ZW15, Aia15, XWXC14]. Formalized
[YZC16]. formats [ZT14]. forms [TY16a].

formula [DWZ12]. FORTIS [GSFT16].

Forum [Ran15]. Forward
[ABD+15, BV15, FS16, GSFT16,
HLT+15, KME+12, KX10, LTH+15,
NMS14, WLH15, XW12, Yon12, YKC+11,
BM11, TCS14, YFK+12]. Forward-Secure
[BV15, KME+12, LTH+15, NMS14,
WLH15, YKC+11, YFK+12].

ForwardDiffSig [BAL10]. forwarding
[PN17]. Found [Moo12]. Foundations
[Des10a, IEE10, IE11b, Lin17, SN10, NS10,
Sta11b, Ter11]. Four [LyW12].

Four-Pixel [LyW12]. Fourier
[GJ13, yWpWyN13]. Fourth [Kob10].

FOX [LJF16]. FPGA [AMKA17, BCE+10,
BDGH15, CFZ+10, CHS15, GFBF12,
HF14b, MM14a, MAK+12, ZLQ15].

FPGA/ASIC [CFZ+10]. FPGAAs
[DG10, SMOP15, VMV15]. Fractal
[JT+16, KM11]. fraction [IK15].

fractional [BW13, VM14]. Fragile
[CHHW12, MCD12, SSA13, CCL11,
PGL10, WHZ12]. fragment [BBP10].

Fragmentation [BDPS12, CDF+10]. frame
[YQH12]. Frames [DG17, IM14].

Framework [BJL16, CD12, DG17, HXC+11,
KPC+16, LLG15, LSC+15, LY15, LQD+16,
MSU13, SK11, SYC+17, TSH14, VPK17,
ZJ14, BHCDFR12, KKGK10, KM14,
MMS+17a, MBF+13, PSdO+13, PLCGS11,
PKA15, SD10, SA16b, SYW17]. frameworks
[LSBN14]. France [Kap11].

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

Frank [AB13, Joh10]. frankencerts
[BJR+14]. Fraud [Ber12]. Fred [Xie12].

Free [App13, Boy16, IL15, TWZ+12,
TTH15, ZLH+12, ATK11, LL16a, SA12,
SE16, YT11b]. Free-View [TWZ+12].

FreeBSD [MMN15]. Freestart [SKP15].

French [Ant14]. Frequency
[KAHKB17, LT16, LW14, TC10,
CJP12, CJP15, EA12, NLYZ12].

Frequency-Based [LWC14]. Freshness
[RBN15]. Friendly [FRA16, SZDL14,
AC12, KLW+16, RD17, WOLS12].

Frontside [DDR+16]. FSR [MD12b].

FSR-Based [MD12b]. Fugue [AP11].
Full [ALR13, HEC+12, LW12, VS16, WLC12,
BKR11, DMM17, LC13, Ran16, SWW+17,
SKP15, Tam15, TY16b]. full-hiding
[DMM17]. full-text [SWW+17]. Fully
[AKP12, BV11, BV14, BGV14, CMO+16,
CN12, CZF12, CNT12, DOS15, GHI1a,
GHI1b, GHS12, HLLC11, LSLW15, LSC12,
MV12, Nac16, NCCG13, PBY12, SGH15,
Vai11, WHC+15, ZZ12, GH13, ZXJ+14,
ZML17]. **Fully-Homomorphic** [GH11b].

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

**Fun** [APPV15]. **Function** [AMPH14, FLS+10, LyWZZ12, SLY11, WSSO12, AKY13, AP11, CMMS17, LK14, LP11, RS14, Sar11, SXL16, TQL+14, WYW14].

**Functional** [AS16, BSW12, Boy13, GGH+16, GVW12, LQD+16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14].

**Functionalities** [JR13].

**Functions** [ACZ16, ALR13, BBC+14, BIKK14, BKPW12, BK12a, CPS16, DSSM14, DQFL12, FY11, IVV11, NR12, Rja12, RW12, SML14, SLX+16, Tan12a, TQL+14, WYW14].

**Fundamentals** [Joh10].

**Further** [HCL+14, WHY+12].

**Fus** [FMS12a].

**Future** [BCE+12, BKBK14, Bon12, CDFZ16, GCK12, Mon13, Ano13b, FPBG14, Mac12, PHWM10, MJS13].

**Future-proof** [Mon13].

**Fuzzy** [KRDH13, NC12, SH11, XJWW13, KHMB13, MSD13, SM11, SNM14].

**G** [HLYS14].

**G2C** [BMP12].

**GA** [MMSD13].

**GA-fuzzy** [MMSD13].

**gadgets** [Gel13].

**Gait** [XJR+17, XJR+17].

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

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

**Gallai** [SS10b].

**Galois** [CFY+10, LGKY10, MRT10, PLSvdLE10, SH11, SM11, XSWC10].

**Generators** [AS17, LTKP16, MFG16, NIS12, PFS12, CP13, HRV10, MG15, Sti11, Zim10].

**Generic** [BWLA16, BR14, Chl16, GWWC15, HXC+11, Sar10b, SY15a, ZCLL14, HQY+16, YT11b].

**Generically** [MHKS14].

**Genetic** [JK13, ASVE13, EEAZ13, PTK14].

**Genius** [Hai17].

**Gentry** [GH11b].

**Genuine** [HR13].

**Genus** [FWS13].

**Geodesics** [ZZCJ14].

**Geographic** [LC17].

**Geolocation** [FPY15].

**Geometric** [DSB16, GT11, WLZL12, YNNW15, CLZ+17, GZHD12].

**Geometrical** [TLL13].

**Geometrically** [WYW+13].

**Geometry** [tWmC12, CFR11, CZ15a].

**German** [BDFK12, Blu02, Buc10, Cop10a].

**Germany** [FBM12, GLIC10, Sen10, Wat10].

**Gesture** [LCL17b].

**Gestures** [AUMT16, GCSAddP11].

**Get** [GPT14, Sch11].

**Getting** [ESS15].

**Ghost** [CDA14].

**GHZ** [CCL+13].

**GHZ-State** [CCL+13].

**Girod** [GMNS15].

**GLARM** [LLZ+16].

**glimpse** [Mic10a].

**Global** [CLP13a, CLH13, MRS+17, GH16,
LH11a, TMK11, ZX11. Globally [CCS14].
GMAC [SKK10]. Goal [BMP12].
Goal-Driven [BMP12]. Goes [BCD+12, RY10]. Goldreich [Lin17].
Goliath [Sch15c]. Gong [LLW16]. Good [DQLF12, FY11, LSNB14, RY10, SA14, WT13]. Google [Loe15, VGN14].
Goppa [MBR15]. Gordon [Lin17].
NXB13, CJP12, CJP15, PPB16, SPLHCB14.
Hash-Based [GI12, HCPLSB12, MKAA17, NXB13, CJP12, CJP15, PPB16, SPLHCB14].
Hashing [AAE+14, ASBdS16, BHKN13, BKL+13, Kaw15, CP13]. Haskell [Rus15].
hatching [WKY12]. HB [HSH1]. HDH [PDH15].
Health [LYZ+13, LHL15, Rao17, ZVG16, IC17, WXM+17, JKL+16].
Healthcare [BN14, HLLKL15, ZLDC15, AS14, Kim16].
Hearing [Bla16]. Heartbeat [IA15].
Heartbleed [DKA+14, Ven14]. hedging [RY10]. Heights [Gen13]. held [Cho10].
helper [Sm11a]. helper [RWZ15]. HeNB [CLM+12]. Herodotus [Keb15, Mac14].
Heterogeneous [SP15b, SZMK13, SCKH10].
Heuristic [BGJT14]. HEVC [DG17]. HIBE [LW11c].
Hickory [NN15]. Hidden [FMS12b, PSS+13, YLL+12, ZYT13, BDK11, LCL+17a, Sch15c, Sm15].
Hiding [GGH+16b, GL10, JH1N12, MK12b, OT12, XLM+12, XGLM14, ZZWL15, DDM17, KWH16, LXY12, LT14b, UUN11, WHL13, WZWL13, ZWM14].
hiera [Lac15].
Hierarchical [ADM12, BSSV12, FSX12a, LSLW15, NMS14, NLY15, OT12, WYML16, ZMW16, ZHW+16, DCS12, KPB17, NZM10, RG10, SE14, SE16, WWYZ11].
Hierarchy [NA10b, VN16]. High [ASBDs16, ARM15, Bar15, BDL+11, DM15, DG17, GL12, GCS+13, HZ11, KMP+11, KPC+16, LTKP16, LCK11, LPO+17, MS13b, MS13c, PCPK14, WYCF14, WL11, XNRG15, ABBD13, GZHD12, GCVR17, KL13, MAK+12, RS17, WHL13, WXYL16, WZWL13, WKH11].
High-Level [KPC+16, ABBD13]. High-Performance [GCS+13, LPO+17, GCVR17].
high-throughput [MAK+12]. Higher [LWK12, PRC12, gWPnyY+14, ZSW+12, LWKP14].
Higher-Order [LWK12, PRC12, ZSW+12, gWPnyY+14, LWKP14].
Highly [SZDL14, ADC+15, DT13].
HIGHT [CPW12, WWBC14]. hijacking [DCAT12].
HILL [KPP13, KA17]. HIMMO [GMRT+15]. Hindering [BTPLST15].
HISS [DT13]. histogram [CSS+13, Lin14a].
Historians [Cer14]. Historical [Hai17].
History [ABJ13, Cer14, Cop10a, LT14b, Mc10, MK11, SE16, Sm15]. history-free [SE16].
Hitler [Hea15, Moo14]. HMAC [GMW16, MAK+12].
HAMAC-SHA256 [GMW16].
HN [PD14, She14, XHC+12, KM10b, LXJ14, SGGR+16].
Hoffstein [Mei10].
Hole [Ano15c, BKKV10, PC16].
Holy [Mic10a]. home [KPP16, Cor14a].
Homogeneous [HT11]. Homomorphic [AKP12, BV11, BV14, BGV14, CMO+16, CN12, CJ13, CNT12, DOS15, GH11a, GH11b, GHS12, GHP21, KOS16, KG16, Kin15, LCLL15, Nac16, PKTK12, Tan15b, Vai11, WHC+15, BDO11, RWL12, GHA13, GHPS13, GLM+16, LLW16, Tam15, ZXJ+14].
Homomorphism [Bra13]. Honey [JR14].
Hop [RWLL14, LCT+14]. Hop-by-Hop [RWLL14].
House [Ano16g, B1a16]. HP [CBG+10].
Hromkovic [Gas13]. HTTP [BHCdFR12].
Huang [LSSW16]. Huffman [Sun16].
Hui-Yuan [FMS12a].
Human [HHS+15, IA15, DMT12, LW+10].
Humans [RBNB15]. Hummingbird [ESS12].
Hummingbird- [ESS12].
hunt [Bha16]. hunted [McG11].
HWMP
[BOB13]. Hybrid
[ADI11, ARM15, KBL11, KKA15, LP12, NGAuH16, O012, Per13, XWLJ16, EEAZ13, WXLY16, WS14, XWS17, BOB13]. Hybrid-Double [ARM15].
hybrid-indexed [WXLY16]. hybridization [MMSD13]. Hyderabad [GG10]. Hyper [BL14, WGZ12].
Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL12, Chi2, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GOPB12, HYW14, HZC12, HSM13, HSM14, HX15, HYWS11, KKA14, KRB12, Kuz11, LMB12, LSL12a, LKAT12, LJJ14, LSL15, LSL15, LH11b, LSL12, MBF13, MGJS12, MR10, OdH12, Par12a, PSS13, PSJ13, PWVT12, RDZ16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, SPPC12, SKGY14, SWW16, SGH15, TKR14, Tia15, TH16, TMGP13, Vle12, WY10, W14, XZ12, XQL11, XJW16, YXZ12, YTM14, You11, YK11, YFK12, YCZ12, Z12, ZM16, ZW16, ZW16, ZT12, ZT12, Z12].
Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL12, Chi2, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, HY13, GJJ15, GJZ17, HZC12, HSM13, HSM14, HX15, HYWS11, KKA14, KRB12, Kuz11, LMB12, LSL12a, LKAT12, LJJ14, LSL15, LSL15, LH11b, LSL12, MBF13, MGJS12, MR10, OdH12, Par12a, PSS13, PSJ13, PWVT12, RDZ16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, SPPC12, SKGY14, SWW16, SGH15, TKR14, Tia15, TH16, TMGP13, Vle12, WY10, W14, XZ12, XQL11, XJW16, YXZ12, YTM14, You11, YK11, YFK12, YCZ12, Z12, ZM16, ZW16, ZW16, ZT12, ZT12, Z12].
Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL12, Chi2, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, HY13, GJJ15, GJZ17, HZC12, HSM13, HSM14, HX15, LSL12a, LSL15, LSL15, LH11b, LSL12, LSL12, LSL12, MBF13, MGJS12, MR10, OdH12, Par12a, PSS13, PSJ13, PWVT12, RDZ16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, SPPC12, SKGY14, SWW16, SGH15, TKR14, Tia15, TH16, TMGP13, Vle12, WY10, W14, XZ12, XQL11, XJW16, YXZ12, YTM14, You11, YK11, YFK12, YCZ12, Z12, ZM16, ZW16, ZW16, ZT12, ZT12, Z12].
Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL12, Chi2, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, HY13, GJJ15, GJZ17, HZC12, HSM13, HSM14, HX15, LSL12a, LSL15, LSL15, LH11b, LSL12, MBF13, MGJS12, MR10, OdH12, Par12a, PSS13, PSJ13, PWVT12, RDZ16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, SPPC12, SKGY14, SWW16, SGH15, TKR14, Tia15, TH16, TMGP13, Vle12, WY10, W14, XZ12, XQL11, XJW16, YXZ12, YTM14, You11, YK11, YFK12, YCZ12, Z12, ZM16, ZW16, ZW16, ZT12, ZT12, Z12].
YKC+12, YXA+16, ZZ21, LZJX10, Kat13.
IEEE802.16e [HLCL11]. if [ABJ13, Rus15]. IFP [GLIC10]. IFP [MMZ12]. Igor [Sha10]. II [SCPSN10b, SMOP15]. III [SMOP15]. Illegal [ABJ13]. Illumination [KLY+12]. Illustrated [GHS14]. Illustrated [Cop10a]. Im [BGI+10, BGI+12]. IMA [Che11]. IMACC [Che11]. Image [BAAS13, BWR12, CJFH14, DA10, JKH+Y12, KPS10, LA15, MBC15, PWW10, RSL6, RVRS1C12, SH11, SM11, SJ12, SGP+12, SSA13, WHZ12, WXZL12, WYW+13, WYCF14, WK1Y2, YLL+12, YWNN15, Ye10, Ye14, YH16, ZXZ+11, BWA13, BM13, CT11a, CW14a, EA11, GKC11, HLC16, KLM11, LXC11, LW10, LWL11, LW13b, LPZJ15, M014, NES+14, PTK14, Sch12a, SM13, SMN14, Sm16, JTh12, TLL10, TLL13, UUN11, UUN13, yWpWyypN13, WGZ+12, WKh11, WOLS12, XSWC10, YC11, YCC16, YSC16, ZLW+12, ZT14, ZL12].
Image-Guided [CJFH14]. ImageMagick [Tay14]. Imagery [BCP14a]. Images [BCP11, CLF11, FR16, GL10, LC15, LLY+12b, MR16, NC12, Yan12, dRsdVC12, AMK12, DD13, HWYW14, LW13b, MM14a, MKH+12, UUN11, WLM13, ZW1L13].
Implementation [BW16, BSJ15, BDML16, EGG+12, GL12, GPT12, GCS+13, HF14b, KB10, KG1V16, MFG16, MAS16, NdMMW16, QL17, RMP10, VKPI17, ZPM+15, BDP+12, GH13, HBBRNM+16, KY10, MM14a, MNNW15, NES+14, PBCC14, SK14, SAAB10, SF12].
Implementations [BCFZ12, BFK16, BDGH15, BJ10, Bru12, CMLRHS13, CBL13, ERRMG15, LGH+17, MLB10, Tom16, YZLC12, ABBD13, ABF+14, BFG+14, BJ1R+14, CFN+14, LBOX12, Sta11b].
Improved [BCP14a, Chi12, CGK01, GLLS12, IK15, JHL12, KZG10, LTI14a, LWL12, LJF16, LHI11, LCC13, LC15, LML12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GLV13, PWL13, SD10, XHH12, Wan14].
Improvement [FRS+16, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNX+11]. improvements [EA12, HRV10, Tso13].
Indexing [HCDM12]. India [BC11, CGB+10, GG10]. Indicator [KU12]. Indicators [YT12, Pal16]. Indirect [ABS+12]. Indistinguishability
YWNW15, GZHD12, LXCM11]. Invariants [NKWF14, CDSLY14, KK10, TLL13].
Invention [Orm16]. inverts [Ant14].
inversion [KHHH14]. Invert [ZWTM15].
Inverted [ZXYL16]. Invertible
[SLY+16, UUN13]. Investigating
[SPP+13]. Investigations [Bla16].
Invisibility [BN14]. Invisible
[Keb15, Mac14, SYL13]. INVISIOS
[AARJ12]. Involution [Bru12]. Involving
[HCLL11]. IoT [CCM17, SGC16, TG17,
WXK+17, YFT17, ZCWS15]. IoT-Enabled
[SGC16]. IoTs [SAJL16]. IP
[AGLW16, AZH11, PA10, RS17, SP15a,
TJZF12, WBC+10]. IP-SEC [PA10]. IPE
[ZM16]. iphone [Wu16]. IPs
[GSFT16, NDG+17]. IPv6 [KP12]. IRC
[HB13]. IRC-based [HB13]. IRIW
[JKHrYe12]. ISBN
[Joh10]. Islet [Dan12]. ISO
[BCM12, BCM13, TS16, WWBC14]. ISO/
IEC [BCM12, BCM13]. Isolated
[YS15]. Isolating [LG12]. ISSAC
[Wat10]. Issue
[Ano13b, Ano16a, Ano16b, Ano16g, LW13a,
XW13, PHWM10]. Issues [ABHC+16,
PZPS15, JAE10, KJN+16, MHV15]. Italy
[Cra12]. items [YD17]. Iterate [HRH11].
Iterated [LPS12]. iterative [SXL16].
ITUbee [FXP+17].

K2 [PS12]. Kalyna [OGK+15]. Karatsuba
[BCL14]. Karhunen [BCPV11]. KASE
[CLW16]. Katz [Ful10, Mou15]. KDM
[MTY11]. Keccak [BDP+12]. keep [Rus15].
Keeping [CG14b, Man13, Gup15]. KEM
[CZLC14]. Kerberos [SCKH10, TW14].
Key
[ASN12, Ano11b, BN14, BVS+13,
BL12, BBO+16a, BCO13, BKL12, BF11,
BKKV10, BB10, CVM14, CLY14, Che15,
CJ13, Chi16, CCT+14, CNT12, Cou12,
CMA14, DWZ12, DL12, EAA+16, FZT13,
FMB12, GFBF12, GT12, GZZ+13, GSW+16,
GST13, GPT14, Gir15, GZ12, HSMY12,
HC12, HIL10a, HCL+14, HCT+15, HEC+12,
Jia14a, JEA+15, KP12, KTT12, KFOS12,
Kim15, LLSW16, LCL15, LQY10, LY16,
LH11b, LCCJ13, LBR12, MZHY15, MVV12,
MMP14, MTY11, MYMY12, MPSR12,
MNS11, MSU13, NNA10, NYR+14, NTY12,
Orn16, PSM17, PDNH15, PCPK14, Pud12,
PNRC17, RVH+16, RSBGN12, RW12,
Saa12a, SK11, SNJ11, SEHK12, SK12b,
SMW+10, Sia12, SGGH15, SLY+16, TMC15,
TM12, WSS12, WLC12, WZ15, WWHL12,
WT10b, XNKG15, XXZ12, Xio12, XLM+12,
XJWWW13, XGLM14, XZLW15, XJR+17,
YM16, YZ+12, YS12, YLW13, YRT+16,
Yon12, YKC+11, YFK+12, ZH16, AA14].
key
[ABB+14, AKG13, AIB+16, ABW10,
AN15, BS15, BGAD12, BB14, BJ16, BSW12,
BGG+13, BBB16b, CFL13, Cha13a, CLZ+17,
CTL13, CML16, CLCZ10, DLK+16, DGIS12,
Dur15, FHH10a, FA14b, FIO15, GMRT+15,
GPP\textsuperscript{+16}, GH16, GBNM11, GLM\textsuperscript{+11}, HPC12, HL11, HLYS14, IM14, ISC\textsuperscript{+16}, IB11, JSK\textsuperscript{+16}, JLT\textsuperscript{+12}, Jia14b, KDH15, KKG14, KLM\textsuperscript{+16}, LLLS13, LWS10, LPdS10, LW13b, LZX14, LML\textsuperscript{+13}, MNP12, MRT10, NACL12, NCL13, Nos11, Nos14, RG10, RWZ13, RPSL10, SES\textsuperscript{+16}, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZ15, SA15, SvT10, TCS14, TLL12, Tso13, TKHK14, VN17, WWY11, WZM12a, WZM12b, WT10a, WTT12, WQZ\textsuperscript{+13}, WXK\textsuperscript{+17}, WX12, XW13, XCL13, XMHD13, YT11b, YC12, YZZ\textsuperscript{+14}, YHHS16, YLZ\textsuperscript{+16}, ZPZ\textsuperscript{+16}, ZWQ\textsuperscript{+11}, ZZ11, ZCC15, ZT16, ZG10, ZCC15, ZHT16, CLW16, OHJ10, XJR\textsuperscript{+17}.

Key-Aggregate [CCT\textsuperscript{+14}, PSM17, CLW16].

Key-Agreement [WSS12].

Key-Alternating [BKLS12].

Key-Based [Xio12].

Key-correlations [Sar14].

Key-Establishment [BCO13].

Key-Extraction [GPT14].

Key-Hash [KKG14].

Key-Insulated [FZT13, LH11b, HL11, RG10, RWZ13, WWY11].

Key-Length [GT12].

Key-Length-Based [PNRC17].

Key-Policy [GZZ\textsuperscript{+13}, GSW\textsuperscript{+16}, HSMY12, RH16].

KEYing [TW14, BCPV11].

Keyless [PMR12].

key-payments [MBB11].

Keys [ASN11, BF12, Bro17, CC10, HDWH12, MS16, PSM17, TW14, ZMW16, HL14, IK15, LLY15, LH13, LW10, RWZ13].

keystream [SM11].

Keystroke [AaBT16, SP13, CTL12, LTC\textsuperscript{+15a}].

Keyword [CWL\textsuperscript{+14}, Che15, HCDM12, XWS16, XJW13, ZXY16, BL11, CLH\textsuperscript{+16}, FS12, LKB\textsuperscript{+14}, SY15b, WHY\textsuperscript{+12}, WX16].

Keywords [CWWL12, ZZ11].

KGC [YT11a].

King [ABJ13].

KISS [Ros11].

KLEIN [GNL12].

Knapsacks [Dun12a].

Knebl [Mur10].

Know [BC14, CAC14, XTK10].

Knowledge [CLP13a, COP14, GJO\textsuperscript{+13}, GOS12, IW14, MX13, MT12, OOR\textsuperscript{+14}, Pan14, TSH14, Ano11a, KPP16].

Known [DWWZ12, JHL12, SEHK12].

Known-Key [DWWZ12, SEHK12].

Kobitz [BJ10].

Kode [NN15].

Korea [LH10a, LW11a].

KP [FIJ12, HQZH14].

KP-ABE [FJJH12, HQZH14].

Kristie [Keb15].

Kryptologie [Bl12].

Kryptographie [Buc10].

Kuala [HWG10].

Kurtosis [YYO15].

L [Low12, Xci12].

Labs [Ven14].

Labyrinth [Fox13].

Lacks [BDG13].

LAKE [BCO13].

Landis [BBB16].

Languages [MX13, Wat12].

LANs [FLH13].

Lapin [HKL\textsuperscript{+12}].

Laptop [GPT14].

Large [AN12, DM15, JLS12, JKHeY12, KR11, LU12, LW16, LQ16, MC11, SP13, dCCSB\textsuperscript{+16}, EE13, FX12, GS\textsuperscript{+16}, LBOX12, SR10].

Large-Scale [DM15, JKHeY12, LQ16, dCCSB\textsuperscript{+16}, FX12, GS\textsuperscript{+16}, SR10].

LARK [DS11].

Laser [DDR\textsuperscript{+16}, FNP\textsuperscript{+15}, L11].

Last [Hof15, Hof16].

Latency [BCG\textsuperscript{+12b}].

Lateral [SCY15].

Latin [AB10a].

LatinCrypt [AB10a].

Lattice [ADM12, Ano11b, BS15, EM12, FGM10, HP15, LP17, PG12, AT16, DR16].

Lattice-Based [ADM12, Ano11b, BS15, EM12, HP15, LP17, PG12, AT16].

Lattices [Boy13, TH16, XXZ12, ZQQ15, Kri13, Tia15, XLM16, yYqWqZC13].

launch [Zet14].

Law [Bl12, SR14, Wu16, AOT13].

Layer [LHM\textsuperscript{+15}, ZHX16, HQ\textsuperscript{+16}, LKL13].

Layered [BS14, GRL12, JCHS16, ZC12].

LBlock [KDH13, MNP12].

LGDM [BBC\textsuperscript{+13}].

Leader [TKM12].

leak [BBG\textsuperscript{+17}].

Leakage [AV12, BKKV10, CBL13, DH16, FSP12, HH13, IL15, LT16, NTK17, NTY12, Pan14, SGH15, TTH15, XY15, YZLC12, YZ12, YC12, YZT13, ZWT15, ZM16, DLZ16a, DMWS12, GV14a, YL16, ZWM14, ZCC15].

Leakage-Free
Leakage-Resilience [IL15, TTH15]. Leakage-Resilient [NTY12]. Leakage-tolerating [ZWM14]. Leakage-Resilient [AV12, FPS12, LTZY16, Pan14, XZY+12, ZYT13, DLZ16a, GV14].


AAZ$^{+16}$, CLP$^{+13b}$, CTL12, CCSW11, CTL13, FHH10a, FA14b, GM16, GH16, HL14, IB11, KKA14, KKM$^{+13}$, KKM$^{+14}$, KKG14, LH13, OYHSB14, Par12b, hSZZ15, SSAF11, SKB$^{+17}$, THK14, WT10a, YNX$^{+16}$, ZD$^{+16}$, ZC12, MBF$^{+13}$, SLL10].


Mode [HZ11, Mar10, gWPnY$^{+14}$, WLC12, Fay16].

Model [App13, CLP13a, GLG12, GJO$^{+13}$, GJJ15, GJZ17, HZX15, IA15, Kar12, LHM$^{+15}$, LZC$^{+12b}$, MVVR12, PYM$^{+15}$, PNRC17, SJS14, SPM$^{+13}$, TBCB15, WWC$^{+11}$, WWHL12, XZ$^{+12}$, You12, ZHL15, BL11, CDPLCA16, HKT11, KSSU13, LSTZ12, LCY$^{+16}$, LL16b, MGPI0, Mas17, MM13, NB13, WYL13, WZM12a, WZM12b, YC12, TCL15]. Model-based [IA15].

Model-Predictive [TBCB15]. Modeling [CJFH14, GBNM11, LTKP16, MKN13, PNAS13b, Ana14, CDGC12]. Modelling [BL15, ACF16].


Modular [Abe12, VN17], modulation [KB17]. Moduli [APPVP15]. Modulus [CNT12, LyW12, SEY14]. Moment [PTK14, GJ13, TPKT12, yWPnY11].


MP3 [YQH12]. MPC [GGHR14]. MPEG [YYO15]. MPEG-4 [YYO15].

MPSS [SLL10]. MRAM [DSB16, VDB$^{+16}$]. MRAM-Based [VDB$^{+16}$]. MrCrypt [TLMM13].

MSP$^{40X}$ [GL12]. MST$^{_1tn3}$ [SwT10]. Much [DL15]. Muhammad [ABJ13].

Multi [ASS15, BBEPT14, BRT12, CWL$^{+14}$, Chi12, GVW12, GJ17, HC12, IG11, KTT12, KMO14, LyWS10, MZH15, MEFO12, MLBL12, NGAuH16, OKG$^{+12}$, SK12b, TWZ$^{+12}$, Wan14, WOLP15, XWSW16, YWW10, Ye14, ZC13, ZQ15, ZLCD15, BGG$^{+13}$, CLP$^{+13b}$, CFVP16, CG12b, CLJH13, CW14a, CZ15b, GOMGCCR15, GPVcBRO12, KL14, KL11, HCC11, HLC12, ISC$^{+16}$, JCHS16, KM11, LXMW12, LKX$^{+14}$, LCT$^{+14}$, LH13, LWY12, Mas17, SCY15, SWW$^{+16}$, SSS11, TLL12, WDZL13, WXX$^{+17}$, XLWZ16, YCC16]. multi-agent [GPVcBRO12]. multi-authenticated [KL11]. Multi-Authority [ZQQ15].


multi-gateway [WXW17]. multi-hop [LCT$^{+14}$]. Multi-instance [BRT12].

Multi-Keyword [CW12, XWSW16, LKX$^{+14}$].


multi-scale [CG12b]. multi-scroll
[GMOGCCC15]. Multi-Secret
[zc13, CW14a, HCCC11, HLC12].
Multi-Segment [WOLP15]. multi-server
[CLHJ13, HL14, ISC’16, LXMW12, LH13,
SS11, TTL12]. Multi-Signature [ASS15].
multi-stage [Mas17]. multi-use [CZ15b].
Multi-User [MZYH15, OKG’12]. multibit
[KPS10]. Multicast [CC14, BAL10,
HGWW11, LTT10, NAICL12].
Multicoupon [HIDFGPC15]. Multidevice
[DPCM16]. Multidimension [AJA16].
Multidimensional
[Her10, WWBC14, HMC12]. Multifactor
[MNY12]. Multigigabit [PP10b].
multihop [ADF12]. Multilevel
[FMS12b, HF14a, NSA15]. Multimedia
[NSA15, PMZ13, PZPS15, PYM’15,
WLY’15, ZW15, Zha15, ZSA12, HM10,
HWYW14, LLLK10, WN13, XZW16,
TW14]. Multimodal
[GM16, ATI’10, MHT’13]. Multipartite
[HR13]. Multiparty [BD011, CCL’13,
Fri10b, ADMM16, LDD12]. Multiple
[DSB15, Dun12a, FR16, KBL11, LTC’15b,
LQD’16, NDC’13, SY14, SC10, Sta12,
LWZG10, LTC’15a, LZC17, MN14, RWZ13,
TKHK14]. Multiple-Parameter
[NDC’13]. multiple-precision [MN14].
Multiple-Secret [SC10]. Multiplication
[AK14, CMO’16, HVL17, SK12b, YTS12,
AAT16, SKH15, SF12]. multiplicative
[KHH14]. Multipliers [ARM15].
Multireceiver [HH10b]. multisecret
[FGMP12]. Multitone [GL10].
Multivariate [ST16, YDH’15].
multiwavelet [PW10]. Munich [Wat10].
Music [NTKG17, W16]. musical [Ana14].
Mutt [Ran14]. Mutual
[CJP12, GH12, GM14, Kim16, SBS’12,
WT10b, CJP15, Cho14, CL11, FH110a,
Far14, GH16, HDPC13, IB11, KLW’16,
SPLHCB14, TG17, XMHD13]. MVP
[CD12]. mvSERS [HKL15]. My [GPT14].
Name [YCM’13]. Names
[ABJ13, MPJ’16]. National [ABJ13].
Natural [ZCWS15]. nature [KL13]. Naval
[Don14]. Nazis [Hea15]. NDSS [An10].
nearest [LRV10]. nearest-neighbor
[LRV10]. nearly [PHGR16]. necessary
[TD14]. needs [Sch12b]. Negligible [DF11].
neighbor [LRV10]. Neighborhood
[DA10]. Neighboring [LSQ11b, LC15].
Neil [Pea11]. Neon [ZMM’10]. nested
[FH10a]. Net [LHF12]. Nets [PS14].
Nets-based [PS14]. Network
[An10, Bis17, CW16, CJ13, CLH13,
DRS16, Hay13, HDW12, Kim15, LCLL15,
LY16, LTW11, MJGS12, NNAM10,
NRZQ15, SG16, She14, TLW12, VKPI17,
VFV17, VCA15, VKC15, WP15, YZLC12,
YSJL14, AKM’11, AL15, An11a, AZF’12,
CL11, DLK’16, FPBG14, HWG10, HB13,
HKB4, JZS’10, LH11a, LKLL13, MA13,
MJS13, NDNR13, OF11, PI16, RCW15,
SCKH10, Sta11a, Tan15b, WY13, WS14,
YLS12, Ste15b]. network-based [YLS12].
Network-Coded [She14].
Network-on-Chip [Bis17]. Networking
[LCK11, ZHL15, Kim11, LCM’17].
Networks [ABC’17, BN14, BPSD17,
BFMT16, CS14, DS11, DF16, FMS12b,
GMVV17, HZC’12, HBCC13, HK14, KH10,
LLC11, LL15, LHMM’15, LZC14, LWC14,
LLZ’12, MPM’17, NSA15, NVR’14, OQ12,
OKG’12, PYM’15, PCPK14, RWL14,
SWYP12, She14, SP15b, Sm11b, SL11,
TCN’17, WLY’15, XHC’12, YML16, ZC13,
ZW15, Zha15, ZLDD12, ZSA12, Aia15,
AS04, AIB’16, AD12, BDK11,
BLAN’16, BBI16b, CDGC12, CLM’12,
CLSW12, CL11, DSCS12, DK12, DLN13,
EEAZ13, FA14b, GH16, HGWW11, HZC’14,
HCC11, HM11, HTS’10, JLT’12,
JM16’16, KML10b, KL’10, KO16,
KLW’16, LLL12, LC17, LMJC11, LX14,
QM17, RGP12, SGGC’16, SA12,
SZMK13, hSZZ15, SKK10, TKHK14,


'Nobody [Sto12]. Node [NYR+14, OKG+12, LC17, PX13, SAAB10]. Node-Capture [NYR+14]. Nodes [VGA15, ZYL+10]. Noise [ASN11]. Noised [JLS12]. Noisy [ASN12, HZW+14]. Non [AS17, AMH+16, BCI+13, CG14a, CPS16, DJL+12, EKP+13, FNV14, HKB14, KTT12, LLG15, MFH13, MSas12, OOR+14, Pas13a, Svo14, WgMW12, YNQ15, YKKL12, ZLDD12, AY14a, BS15, CS11, ESR114, GIJ+12, Kre13, LP11, MSas13, SES+16, SXL16, XSWC10]. Non-adjacent [Kre13].


Non-Malleable [MSas12, CG14a, FNV14, OOR+14, Pas13a, LP11, MSas13]. Non-monopolizable [DJL+12]. Non-Repudiation [LLG15].


November [Kap11, LCK11, Yan11]. NSA [ABJ13, AHS13, Bud16, Men13, Sta13, Tox14]. NSDG [SSPC12]. NTOW [BS15].


Numerical [CML16]. Numerology [GG11].

NVMM [CS11].

O [CDD13]. Obfuscated [LMS16, OWHS12, ZM16]. Obfuscating [BGI+10, BGI+12]. Obfuscation [AS16, BBC+14, BCP14b, BR14, CZ15b, DRS16, EMW14, FKV15, GGH14, GGH+16a, MH14, BBGT12, CFVP16, GGH+16b].

Obtaining [BB10]. Occasion [Nac12].
October [CGB+10, IEE10, IEE11b].
Off [GPT14, GHS14, YMS11].
Off-Line [YMS11]. Off-Path [GHS14].
Offering [Par12b]. Offers [Paul0]. Office [Mor12]. Official [Kiip15]. Offline [An015a, GAS+16, LJJW+17, RSM15].
Offline/online [LJW+17]. Offloading [JHCC14]. Offs [ASBdS16, BS14, SR10].
Offsets [YQH12]. Old [GY13]. on-chip [BAB+13].
On-Line [FFL12].
On-siteDriverID [SGGCR+16].
On-the-fly [PS14]. One [CP16, DSMM14, DCAT12, FD11, HP14, HG12, Mat14, NA10a, PC16, XW12, XYYYY11, XZLW15, Yon12, BM15, FHH10a, HR10, LP11, LW10, LW13b, LML+13, RK11, Rus15, SM10a, TCS14, QWZ10].
One-Dimensional [XYXYX11].
One-Round [XZLW15, Yon12, XW12, TCS14].
One-Sided [HP14]. One-Time [NA10a, DCAT12, BM15, FHH10a, LW10, LW13b, LML+13]. One-Time-Password [FD11]. One-Way [CP16, DSMM14, Mat14, HR10, LP11, RK11].
Onion [KZG10]. Online [BPSSD17, JMG+16, KSD+17, PSM17, SKGY14, WXY+17, ZHL15, CC10, LKAT12, SYW17].
One/Offline [JMG+16, LKAT12]. Only [BB10, YNR12b, YLW13, Bul10a, KA17, Sar11].
open
[ABF+14, MV15, Pow14, Win17, ZWQ+11].
opensource [ABF+14, Pow14].
OpenCL [ABDP15]. Opening [GDCC16, LZ12a, LZC14]. Openings [SP13]. openness [Bla12].
Operations
[Cil11, SEY14, YWW10, LZY+16].
Opportunities [Mic10b]. opportunity [Sch11].
Optimal [AS17, DSSD14, PDN15, PPS12b, Cha13a, DDD14, PPTT15]. Optimality [SDM+12]. Optimally [DSMM14, GT12].
Optimally-Fair [DSMM14]. Optimised [CMO+16]. Optimising [EVP10].
Optimum [Obe11, YFF12]. Optional [PC16]. OR-Proof [FSX12]. oracle
[GLM+16, HKT11].
Orcas [FZT14, FSX12, GSW+16, QXL11, YS12, YKC+11, YLA+13, LLY15, RG10, SYL13, WYYY11, YFK+12].
Order [KS12, IYK12, PRC12, YK12, ZDL12, ZSW+12, AY13, LW13a, LC1+16, LWK14, gWpNyY+14, YL11].
Order-Preserving [KS12, YKL12, YL11].
organisational [Sm15]. Organization [RSGG15]. Orientated [TJZF12].
Oriented [NNAM10, Rog16, RSGG15, WW12, WZ12a, WZ12b].
Orthogonal [tWmC12].
Oscillator [YKBS10].
OSN [BCF16].
OSNs [PZPS15]. outliers [Sch12].
Output [DK16, GST12, NR12, PBCC14].
Outright [AB13]. Outsourced [FRS+16, LLC+15, LDQ+16, PD14, RDZ+16, DFJ+10].
Overcoming [BKKV10, DY13].
Overhead [CC+10, GHS12, ZJ11, RS17].
Overview [CHS15, MJS13].
Ozarow [ADG16].
**P2P** [dCCSm+12]. Packet
[JTZ+16, VPKI17, XHC+12, MV16b, PX13, XWDN12]. Packets [Bis17]. Pads

**Pairing** [Bon12, CWWL12, KZG10, KHP16, LGPRH14, YTS12, Con12, LL16a, LR15, YT11b]. Pairing-Based
[Bon12, KZG10, LGPRH14, YTS12, Con12].
pairing-free [LL16a, YT11b]. Pairings
[ASS15, Ho15, IL15, LT14a, QYWXY16, RS15]. pairs [MCP15]. Pairwise
[DL12, YM16]. Palash [Kat13]. Palm

**Papers** [Ano16a, Ano16b, Ano16g, LIW3a, XW13, DDS12, Dan12, MV12, BYL10, YJ14, LH10a, vdKSS11]. Paradigm
[ABGR13, BSV12, Mau12, MP12, WQZ+13].

**Parallel** [App14, ARM15, CGB+10, LY16, LB13, MCDB12, MC11, NdMMW16, SMD11, YE12, CSTR16, MRT10, RG10, RWZ13, WWYZ11]. Parameter [NDC+13],
parametric [Bull0a]. Paranoia [Cor14a].

**Park** [Ano16c, Bri11, Cop10a, Cop10b, GW14, Mck10, Mck11, Pea11, Smi11a, Smi15, Bai12]. part [VM14]. Partial
[DLV16, GFBF12, LG12, SGS14, WDDW12, Bax14]. Partially [KB10]. participants
[KSU13, WTT12]. participating [CH10].

**Parties** [YCR16, Kip15]. Partitioning

**Passau** [GL1C10]. PASSERINE [Saa12a].

**Passion** [Hof15]. Passive
[DHB16, GsC17, BM13, LWW11, MK12a]. passport [LZJX10]. password
[ASBdS16, BRT12, CLY14, DM15, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WGMW12, YLW13, YRT+16, ZK1H16, ABK13, CTL12, DSCS12, FA14a,
FIO15, FHV16, HCC10, LWS10, LMK113, MM12, Mvo11, Tso13, TKHK14, WZM12a, WZM12b, YC12].

**Password-Authenticated**
[HCL+14, YRT+16, ZKH16, LWS10, WZM12a, WZM12b]. Password-Based
[BRT12, CLY14, WGMW12, DSCS12, FA14a, FIO15, TKH14]. Password-Only
[YLW13]. Passwords
[BHV10, LCL17b, BCV12, Che13]. Past
[Bon12]. Patchwork [XNG+14].

**Patchwork-Based** [XNG+14]. Path
[DMSS+16, GHS14, NLLJ12, ZW15, YRF+13].

**Patient** [ZLDC15, ZVG16].

**Patient-Centric** [ZVG16].

**Patterns** [Ano16e, BPSD17, WOLP15, BDK11]. pay
[CCSW11]. pay-TV [CCSW11]. Payload
[CHHW12, AZH11]. Payment
[DG15, SYC+17, SYW17]. Payments
[RBHP15, MP+16], PC [YE12].

**PC-Based** [YE12]. PCIe
[IBM13b]. PCM
[LY15]. PCM-based [LY15]. PCPs [MX13].

**PCs** [GPT14, GPP+16]. PDGC [CGB+10].

**Peaks** [TC10]. pearl [Rus15]. Pecherskii
[Kuz11]. peer [NCCG13, ZYW+13]. peer-to-peer [NCCG13, ZYW+13].
[Run10, Run14, Run16].

**ASIC** [CFZ+10].

**AVC** [JSZ12, JHH12, LIW12].

**Decompression** [PP10b]. Decryption
[KB10]. disabled [HFT16]. HEVC
[GKSB17]. ID [CDPLCA16]. IEC
[BCM12, BCM13]. Linear [EKP+13]. LTE
[DLK+16]. Offline [JMG+16, LKA12].
online [LJW+17]. or [YLA+13].

**Polynomial** [ZM16].

**Stateful** [NTY12].

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

**SVC** [MU12, WDDW12, ZLDD12]. Taylor
[Joh10]. TLS [BJR+14, DAV11]. TLS-based
[PP11]. Per-File [DMS+16]. Perceived
[CSW12]. perceptual [MK11]. PEREA
[ATK11]. Perfect [Pas13a, Sch13, CZ15a, LLC10, Lew10, XW12]. perfectly [ADG16].
Performance [Alo12, AB15, CGL+12, CCG10, DLK+16, DBPS12, EGG+12, ESRI14, FPBG14, GLG12, GCS+13, HKL+14, LCK11, LPO+17, MHC12, SKV12, TPKT12, WDDW12, Xio12, ZLDD12, ABDP15, GCVR17, MMS+17a, MS13c].

Potential [SWW].

Power
[ARP12, AS16, HHR11, MMP14, MD12b, MAS16, SAJJ16, SDM+12, TQL+14, WT10b, YAM+15, ZH15, ZJ11, LGKY10, LKAT12, QGGL13, RITF+11].

POWER7 [BAB+13].

PowerEN [HKL+14].

Powerful [IF16].

PowerP [Joh10, Sch15a, CGCS12].

PP-1 [CGCS12].

PPM [XHC+12].

PQRandom [Sen10, Yan11].

Practical
[ATK11, CLSW12, Cra11, DZY10, EA12, FPS12, FSK10, HSA14, HPO+15, LW16, PPTT15, RWZ13, WHLH16, XW13, YZLC12, ZYD10, AMS+10, BS13a, CFN+14, JSK+16, PHGR16, YJKG13].

practicality [NDNR13].

Practice
[ABD+15, CDFZ16, FM12, PWVT12, Rog16, RBHP15, RST15a, RST15b, SN10, SAKM16, NS10, Sta11a].

Practice-Oriented [Rog16].

Practitioners [PP10a].

pre [YHHS16].

pre-distribution [YHHS16].

Preaveraging [GWM16].

precision [MN14, SK12b].

Precomputation [GK16].

Predicate
[KHPP16, NMS14, YKNS12, ZYT13, FH13, HFT16].

Predictability [DK16].

prediction [CSS+13].

Predictive
[TBCB15].

Predictors [EPAG16].

Predistribution [YM16].

Preimage [Li10].

Preseeding [Ran16].

Presence [BDPS12].

Present
[Bon12, LJ16, WH17].

PRESENT-like [LJ16].

Preservation
[BCP14a, LLG15, VSV15, Yon11, LVRY10, TMLS12].

preserve [BG12].

preserved [SWW].

Preserving
[BJL16, BHK13, BJL12, CWL+14, CRE+12, GZZ+13, HSMY12, HLCC11, HXC+11, HMKH14, KS12, LNXY15, LQD+16, NSMS14, OFMR16, PR12, PD14, PSS+13, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, WPZM16, YKKL12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AIB+16, BLV17, FH13, GH16, GA11, HSH11, IC17, JKL+16, LW13a, LCY+16, SYY+17, Tan12b, TSH14, YMM13, YNZ+16, YL11, ZWY+13].

Prevent
[HLAZ15, PYM+13, JSK+16].

Preventing
[DCAT12, SKEG14, WS12].

Prevention
[CWL16].

Primality [Cou12].

PRIME
[ACK+10, GM13].

Primitive
[App15, MCS+15].

Primitives
[BSJ15, EAM+12, HLN+10, SP15b, ABPD15, BSR+14, Gor10].

PRINCE [BCG+12b].

principle [WW14].

Principles
[DK15, FSK10, Fri00a, Sta11a].

print [KPS10].

print-scan [KPS10].

Printer
[EMW14, FNP+15].

Prior [NA10a].

Priority
[LMS16, Bia12].

Prisoners
[Mac14, Keb15].

Privacy
[AKM+11, ACM12, ABHC+16, BN14, BC16, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DTE17, ESS15, GZZ+13, HSMY12, HBC13, HXC+11, JN12, KMI0b, KS12, LSBN14, LLG15, LNXY15, LQD+16, MYLY13, NSM14, PD14, PSS+13, PPRT12, PZP15, PSD15, Pet12, RVH+16, RWLL14, RBHP15, SS17, Set16, SDDL14, SOF12, TMLS12, TMG13, WPZM16, WMY16, YMM13, Yon11, ZHW+16, ZM16, ZHW15, ZLDC15, ZHL15, ZTL15, ACK+10, BP11, BAG12, CDF+10, DZS+12, FH13, HSH11, IC17, JKL+16, Kam16, KKGK10, KM14, MA+13, MGP0, PX13, Sav16, Sch11, SLZ12, SYY+17, SCY15, SWW+17, Tan12b, WW17, WS13, YSY+16, YNZ+16, ZWY+13].

Privacy-protected
[WMY16].

Privacy-Aware
[BCF16, MGP10].

Privacy-Based
[BS13b].

Privacy-Enhanced
[DT17, ACK+10].

Privacy-friendly
[ACM12].

Privacy-Preservation
[LLG15].

privacy-protected
[SWW].

Privacy-Preserving
[BJL16, BJL12, CWL+14, GZZ+13, HSMY12, LNXY15, LQD+16, NSM14, PD14, PPRT12, Pet12, RVH+16, RBHP15,
SZDL14, WPZM16, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, BLV17, HSH11, SYY+17, Tan12b, ZYW+13.

Private [GM13, Jia14a, QZL16, Sia12, Yek10, ZMW16, XZYL16, HJM+11, IK15].

private-keys [IK15]. privileged [WDZL13].

PRNG [DK16]. Proactive
[SLL10, WMYR16]. Probabilistic
[BFG+14, Rao10, KU13].

Probabilistically [IW14]. Probability
[DF11, HLC16]. Probability-based
[HLC16]. probable [Sav13b]. probe
[Edw14]. Problem [LLGJ16, NA10b, TKM12, Mes15, MR14c, RH10, VM14].

Problems [Dun12a, Fra15, GTT11, KRDH13, KPC+11, SK14, TPL16, WS14].

Procedure [CS14, OS12]. Proceedings
[LCK11, WAT10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Dun12b, FBMI2, Gii10, GG10, HWGI10, IEE10, IEE11b, IEE13, LW11a, LTW11, Pie10, Pj12, Rah10, Sen10, Yan10, Yan11, AB10a, BL10, GLIC10, IEE11a, Kia11, Lin14b, Sah13].

Processing [SAKM16, TKMZ13, VPK17, BKV13, HWK+15, MS13b, PRZB12, WS14].

Processor
[HKL+14, LB13, MBR15, YS15, ABDP15, BAB+13, BGC+13, SSPL+13, Tar10].

Processors [GFBF12, Gue16, RYF+13].

Product [ADM12, CCM+15, OT12, YKNS12, Cha13b, DMM17]. Products
[RS10]. Professional [STC11]. Profiles
[BCF16]. Profiling [DP12]. Profit
[APPVP15]. Program
[MZ17, CLZ+17, GGH+16b, MFH13].

Programming
[BCEM15, SY14, ASVE13, HL10].

Programs [BGI+10, BGI+12]. Progress
[AB10a, BL10, BC11, GG10]. Progressive
[SA16a]. Project [ACK+10, SS10c].

projective [CZ15a]. Prominent [ABJ13].

Promise [Pau10, PWVT12]. promised
[HSL11]. Proof [BDG+13, Bla12, CZLC12a, CZLC14, FSX12c, Kuz11, LW12, NLY15, SR14, Ste15a, Mon13, PPTT15].

Proofs [BGK12, BCGR12, BGB12, BCI+13, BSG+13, CZLC12b, IW14, LNJ+13, Mau12, NTY12, Sav13b, WPZM16, AGH14, KPP16, KKK+16, Lit10].

Propagate [GWM16]. Propagation
[WWC+11, YZL12]. Properties
[CCK12, CCK16, DQFL12, FY11, JR13, KU12, Sch12c, CLCZ10, WT13]. Property
[HEC+12, PR12, Rja12]. Proportions
[Ber12]. Propose [BFMT16]. proposed
[Bax14]. Protect
[CTC+15, BVI12, CDF+10, dCSSM+12].

Protected [BDGH15, SG15]. Protecting
[BCP14a, GSFT16, SCY15, CDA14].

Protection [CDD13, GST12, Lop12, NGAu16, NGD+17, RR11, SEY14, SJ12, ATI+10, HLY14, KKM+13, LVRY10, RS17, TLL13, YWT+12]. protection-key
[HLYS14]. Protocol [BL12, BC14, BCM+15, BSSV12, BFK16, CC14, CCM17, FLH13, FMTR12, Fra16, GI12, HS12, HC12, HL10a, HCP12, HCETPL+12, HKL+12, JTT+16, KMO14, LNZ+13, LCCJ13, LNXY15, MBC15, MR10, PSS+13, SBS+12, SGC16, TYK+12, WTI0b, XJR+17, YS12, YWZ+12, ZZ+11, AKG13, AIB+16, AN15, BGA12, CC11, CJP15, DLK+16, EA12, FA14b, FIO15, GMSW14, GLM+11, HPC12, HL14, IC17, JKL+16, Kim11, KO16, LLLS13, LDD12, LKLL13, LWS10, LXM12, LY14, LML+13, NCL13, NLYZ12, OHJ10, Par12b, SLP12B14, SWW+16, SSS11, SSPL+13, TG17, Tso13, Tikh14, WZM12a, WZM12b, WMY16, WT10a, WTI12, XCL13, YC12, YZZ+14, YMM13, ZWQ+11, ZZ12, ZG10, ZZC15, ZN11, BOB13, CJ12, LFCCCRP14, Ste15b].

Protocols [AP13, ABHC+16, BMP12, CCK12, CCK16, CCD15, Con10, CMI1, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KOS16, LY16, MS16, MT12, Mur16, NRY+14, NSMS14, PS14, SBS+12, Sch12c, SOF12, TM12, Xia12, YRT+16, Aia15].
ACM12, CR10, CLCZ10, DGJN14, FTV⁺¹⁰, GBNM11, GLR13, HSH11, HDPC13, HST14, KJD⁺¹⁰, KSU13, KKK⁺¹⁰, LKML13, MN10, NR11, Nos11, Nos14, SD10, YSL⁺¹⁰.

Prototyping [KPC⁺¹⁶].

Provable [BKLS12, CC14, EKB⁺¹⁶, Rog16, YMSH10, ZX11, FA14a, HRS13, LHH11, WB12, XCL13].

Provable [BCGAPM12, BCM12, BCM13, BHJP14, FHH10a, IL15, LHH11a, LL16b, PSM17, WMS⁺¹², XJW⁺¹³, YC12, YZZ⁺¹⁴, ZG10, ABBD13, FIO15, SXL16, XWXC14].

prove [DGJN14].

Provide [Ano15a].

Provided [KS12].

Providence [Sch15a].

providers [BK12b, YWK10b].

Providing [DLN13, HTZR12, MLM16].

Proving [Sar14].

Proximity [IW14].

Proxy [ASS15, GSW⁺¹⁶, GJJ15, GJZ17, HGWW11, HZ15, KP12, LSLW15, LAL⁺¹⁵, LSC12, MBC15, NAL17, Pet12, SYL13, WY10, WYML16, XJW⁺¹⁶, YMSW11, YCM⁺¹³, BGP⁺¹⁷, CLI⁺¹⁶, FSGW11, FSGW12, GH12, HWDL16, KKM⁺¹⁴, LCT⁺¹⁴, LFWS15, LL16a, LL16b, QMW17, SLZ12, SKB⁺¹⁷, Tia15, WHY⁺¹², XWXC14, ZLY10, ZDW⁺¹⁶].

Proxy-invisible [SYL13].

Ps [HDWH12].

Pseudo [NN12, XYXYX11, CFY⁺¹⁰, KM10a, MG15, PLsvdLE10, SH11, SM11, XSWC10, Zim10].

Pseudo-Random [XYXYX11, CFY⁺¹⁰, KM10a, MG15, PLsvdLE10, SH11, SM11, XSWC10, Zim10].

Pseudonymous [BDFK12].

Pseudoprime [DW12].

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

Pseudorandomness [Sha10].

PSMPA [ZLDC15].

PSO [TLL13].

PSpace [JJUW10].

Public [Ano11b, ABW10, BVS⁺¹³, BB14, BKLS12, BKKV10, CLP13a, Che15, CNT12, Cou12, FBM12, HTC⁺¹⁵, IM14, JLT⁺¹², KFOS12, LLSW15, LPS10, LZC14, MZHY15, MPP14, MTY11, Mat14, MPRS12, NTY12, Orm16, PDNH15, RSBGN12, RW12, RBHP15, Saa12a, SK12b, SWM⁺¹⁰, Sia12, SC12, SLY⁺¹⁶, SvT10, TMC15, TT12, WZ15, WWHL12, XNKG15, XXZ12, Xio12, XJWW13, YKC⁺¹¹, YFK⁺¹², AA14, BS15, BSW12, Dur15, HL14, LSBN14, LLY15, LFWS15, LH13, LL16a, RPSL10, SES⁺¹⁶, SY15b, VN17, YT11b, YYS⁺¹⁶, ZZ11, ZCC15, FB12].

Public-Coin [CLP13a, Mat14].

Public-Key [BVS⁺¹³, BKKV10, KFOS12, MMP14, MPRS12, NTY12, Orm16, PDNH15, RSBGN12, RW12, SK12b, SWM⁺¹⁰, Sia12, XNKG15, XJWW13, YKC⁺¹¹, YFK⁺¹², ABW10, IM14, LPS10, LZC14, BSW12, RPSL10, SES⁺¹⁶, VN17, ZCC15].

Publication [ZTL15].

Publicly [NMP⁺¹³, YNR12a].

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

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

published [MYFYR13].

Publisher [Ful10, Mur10].

Publishing [VSV15].

Puebla [AB10a].

PUF [CCKM16, CCM17, DSB16, KPKS12, KLM⁺¹², MVV12, VDB⁺¹⁶].

PUF-Based [CCM17, KPKS12, MVV12].

Pufferfish [KM14].

PUFKY [MVV12].

PUFs [IGR⁺¹⁶].

pulse [MRRT17].

pulse-response [MRRT17].

punctured [MG15].

puppet [Lac15].

Purpose [GFBF12, Gue16, ABDP15, DGJN14, KM11].

purposes [ABB⁺¹⁴].

Pushdown [CCD15].

Pushing [FHV16].

Puzzle [IBM13a].

Puzzles [RSBG12, dCCSM⁺¹², dCCSB⁺¹⁶].

Py [DGIS12].

Py-Family [DGIS12].

pyramid [MHT⁺¹³].

Q&A [Hof15, Hof16].

Q3 [Ven14].

Qaeda [Mac14, Keb15].

QC [JY14, HC17, VOG15].

QC-MDPC [HC17].

QIP [JJUW10].

QS [AZPC14, HDWH12].

Quadratic [KRDH13, SEY14, YDH⁺¹⁵].

Quadraticity
Quality [CSW12, NN12, YCM+13, SS11, WZLW13, WKH11]. Quantitative [BL15, MLBL12, MV16b, HM10].


Random-Grid [KS15]. Randomization [Gas13]. Randomized [ARP12, GT12, HHR11, SR12b, BWA13].

Randomness [AY14a, Ana14, ABF12, BWLA16, MS10, MS16, DTZ12, FRT13, RY10, TC11].

range [HMCK12, JCHS16]. Rank [SS10b, FES10]. Ranked [CWL+14, XWSW16, LKX+14].

range [HMCK12, JCHS16]. Rank [SS10b, FES10]. Ranked [CWL+14, XWSW16, LKX+14].

Random-Grid [KS15]. Randomization [Gas13]. Randomized [ARP12, GT12, HHR11, SR12b, BWA13].

Randomness [AY14a, Ana14, ABF12, BWLA16, MS10, MS16, DTZ12, FRT13, RY10, TC11].

range [HMCK12, JCHS16]. Rank [SS10b, FES10]. Ranked [CWL+14, XWSW16, LKX+14].

range [HMCK12, JCHS16]. Rank [SS10b, FES10]. Ranked [CWL+14, XWSW16, LKX+14].

range [HMCK12, JCHS16]. Rank [SS10b, FES10]. Ranked [CWL+14, XWSW16, LKX+14].
WLZL12, YE12, CC14, MK11, AY14a.
Redistributed [LXCM11]. Reduced [BW12, DWWZ12, KNR10, LWZ12, LJF16, LWPF12, AKY13, AY14b, LF16]. Reduced-Round [LWZ12, AY14b, LF16]. Reduction [ABR12, LCIW17, LSC+15]. Reductions [BHKN13, DW12]. Reference [LLHS12, IM14]. Refinement [BCEM15].
Rekeying [DT13, QLL17, CLSW12, DS11]. Rekeying-Aware [QLL17]. Related [Cil11, CMA14, DGI12, Pud12, WLC12, MNP12].
Related-Key [CMA14, Pud12, WLC12, DGI12]. Relational [HPC10, RP12, BFG+14, BL11, GA11, JK13, PYP10]. Relations [BP11, FHS13, HLR11, KGO10]. Release [KFO12, RSBGN12, Unr15, WSS12].
remapping [PSJ+13]. Remarks [SSU12]. Remote [BCE+10, CS14, FYMY15, LZCK14, Sar12, SY+17, VM15, WgMdZ12, WgMW12, CHS11, IB11, KKG14, LH10, LNM+11, LNKL13, LH13, MM12, Sar10a, WQZ+13, YSL+10].
Removing [HKK13]. Renewal [MMY12].
Representation-Based [AGW15]. Representatives [Bla16]. reproducible [CW12a]. Repudiation [LLG15].
Repurposing [FY13]. Reputation [BL15, LHM+15, PAS13b, MGP10]. Reputation-Based [PAS13b]. Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13]. Requirements [OS16].
Researchers [Con12, Edw14, Win17]. reset [RY10]. Resettable [CPS16]. Resettably [COP14]. Resettably-Sound [COP14].
Resilience [NTY12]. Resiliency [YM16].
Resilient [AV12, BKKV10, FPS12, LTZY16, NY1+14, Pan14, PSD15, XZY+12, YZ12, YNR12b, YCZY12, ZYT13, ZWT15].
Resistance [CGCS12, PRC12, WLZL12, ZJ11, DLN13, FIO15].
Resistant [BK12a, CDK+10, GV14b, HF14b, WHZ12, WgMW12, WH17, YPR117, GMRT+15, HCC10, PBCC14, VCK+12, WTT12, YKGGK13]. Resisting [SXL16, Tan15].
Response [GHS14, HLKL15, ZHW+16, MRRT17]. Resprinting [TBCB15]. Review [AY12, Ayu12, Bai12, Bar12, Cou12, Dew11, Ful10, Gas13, Joh10, Kat13, Keh15, Kob10, Led16, Lop15b, Low12, Mei10, Mou15, Mur10, Sch15a, Sha10, Ter11, Xie12, JAS+11, MM12, TPKT12].
Revising [Sch15a]. Reviews [SR14]. Revised [DLS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. Revising [BT12].
Revocation [TLW12, WSA15]. Revocability [WHLH16]. Revocable [AEHS15, CD16, SE14, SE16, SZS14, SZDL14, TCKL15, TT12, Unr15, FLL+14, WTT12].
Revolutionized [Orm16]. RFID [CJP15, BL12, BSSV12, BM11, CGCGPDMG12, CJP12, Cho14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, HSH11, HDPC13, HQY+16, HCPLSB12, HCETPL+12, LNZ+13, MO12, MK12a, PPH12, PLsVE10, QZL+16a, QZL+16b, SBS+12, SPLHC14, TG17, WH17].
RNTS [PSOMPL13]. roaming [SCKH10, ZK11]. Robbery [SPW+16].
Rob [Gre11]. Robotic [SPW+16].
Robust [BCGAPM12, BCG12a, CFOR12, GKS17, HZC+12, JSZS12, LSL12b, LSR13, MR16, MU12, MS16, MC11, pNyWyY+14, OCG11, RR11, SJ12, SC12, TCKL16, TK14, TTT10, WLDB11, WgMDZ12, gWpNyY+14, XNG+14, YWNW15, YYO15, AP10, CLM+12, EAA+16, GZRD12, HZC+14, LW10, RS17, yWPnyY11, yWPWyYpN13, YSL+10].
Robustness [HGT15, YKBS10]. Rochefort [Car11].
Ron [ARH14], Rosen [HR13], Rosenhain [CDSLY14], ZVG16.

Round [KN10, KNR10], Round [jCPB12, COP14, DWWZ12, GGHR14, KMO14, LWZ12, LJ17, Pan14, XZLW15, Yon12, AY14b, Blo15, LP11, LF+16, Sun11, TSL11, TQL+14, TCS14, LW12].

Round-Reduced [DWWZ12], Rounds [GST12, Sas12, LYHH14, MNP12]. Router [Bis17, SA15]. Routing [KZG10, WLY+15, LSG16, LC17], RSA [Dun12b, Kial11, Pie10, APPVP15, BBBP13, Bro17, CLSW12, Chm10, GM13, GST13, Her14, Hin10, HLYS14, IK15, KHHH14, Lim11, Moo12, SM10a, SM10b, SLM10, Win17, YX+16]. RSA-1024 [Bro17, Win17], RSA/1024 [FLL+14], rubber [BSR14]. Rule [KPW13, NC12, TW12, McG11]. Rule-Based [TW12], Rumor [FKOV15]. Run [IF16], Run-Time [IF16], RunStream [KPC+16], Runtime [CLP+13b], Russian [McG11].

s [Sch15a, NN12, RMP10, SS11], S-box [RMP10], S-Boxes [NN12, SS11], SA [LHM14], SAC [JY14, MV12], SAEL [DLK+16], SAE/LTE [DLK+16], Safe [RQD+15, Gel13], Safely [HM12], Safety [OS16, BMM12, KO16], Salsa20 [MAS16].

sampling [Ana14], San [ACM11, Ano10, Dun12b, Kial11, Lin14b, Pie10], Sanitizable [PH12b], Sanjit [Kat13], Santa [Rab10], Sanya [LTW11], SARFUM [BCE+10], Sarkar [Kat13], satphone [DHW+13], SAW [CFH+13], sawtooth [Ye14], SC’11 [LCK11], SCA [HFr14b], SCA-Resistant [HFr14b], scalability [YC11].

Scalar [CCT+14, DT13, FMTR12, HIFDGPC15, KGV16, LYZ+16, MBR15, QZL+16a, GSN+16, MMN+16, WDLZ13, YC11, KCR11, KS11], Scalar [YTS12, SK15]. Scale [DM15, GU13, JKHeY12, LQD+16, CG12b, dCCSB+16, FXP12, GSN+16, SR10], Scan [LWK11, DDFR13, KPS10].

Scan-based [LWK11], Scenarios [DSB15], Schedules [Pud12], scheduling [MV16b], Schema [AN12], Scheme [ASS15, BHI12, BS14, BKJP12, CML15, CCW+10, CLHC12, CHHW12, CLH13, CSW12, DA10, DS11, DKS12, FR16, FGM10, GZZ+13, GH11b, GJJ17, GLW12, HIDFPGPC15, HMR12, HP12, IL15, JSZS12, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KLM+12, LSL12b, LHF12, LTH+15, LTZY16, LH11b, LGWY12, LTC+15b, LGPRH14, MWZ12, MVVR12, MMN12, MS12, NXB13, NLLJ12, NLY15, Pet12, PDT12, RVH+16, SK12a, SJ12, SGP+12, SD12, She14, ST16, SP15b, SSA13, TDTD13, TWZ11, WY10, WgMdZI12, WgMW12, gWpNyY+14, WH15, XWSW16, XHC+12, XJWW13, YM16, Yam12, YZX+12, Ye10, Ye14, YMSW11, ZP+15, ZC13, ZQQ15, ZLDD12, AHS14, BOB13, BAL10, BMM12, BBB16b, CCL11, CLSW12, CH10, CT11a, CLHJ13, CW14a, CTHP13, Cho14, DSCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, GZHD12, GJ13, GMRT+15, GLM+16, GH16, HBBRNM+16, HL11, HCC11, HLC16], scheme [HCC10, Hwa11, IB11, JLT+12, JZS+10, JM16+16, KI11, KPP16, KD15, KK13, KHMB13, KKM+13, KKM+14, KKG14, Kini16, KLW+16, KWH16, KL11, LXY12, LLZ+16, LSR13, LH10c, LJJX10, LNM+11, LMJ11, LC12, LLH13, LNKL13, LFWS15, LH13, LWH10, LWL10, LW13b, LZC14, LL16a, LL16b, LWH12, MMS17b, MK12a, MS13, Nos14, QMW17, RP10, SGCR+16, SM11, Tan12b, TY16a, TK14, DT14, TLL13, TLL12, UUN11, WY11, WWYY11, yWpNyL11, WHL13, WDLZ13, WZ11, WKK11, WOLS12, WXY+17, XHH12, XWZW16, WX14, XXX15, XMHD13, YC11, YCC16, YWK+10a,
Secure [WXLY16, WLH15, WWHL12, WMS+12, tWmC12, XWSW16, XJWW13, YNR12a, YNR12b, YKC+11, YAM+15, YGD+17, ZXZ+11, ZDL12, ZVG16, ZHT16, ZBR11, AHS14, ABD13, ACF16, ACD+15, BOB13, BSR+14, CCLL11, CLHJ13, CW14a, CS11, FHH10a, FLL+14, FSGW12, FA14b, FIO15, Gal13, GCH15, HGWW11, HWZ+15, HLYS14, HPY10, IB11, JZS+10, KPP16, KKA14, KRM+10, KTUI16, LLLS13, LDDAM12, LH11a, LLW16, LSR13, LCT+14, LL+15, LL16a, LL16b, LBOX12, MR14c, NACL12, NAL17, PSLvdLE10, Rao17, RG10, RYF+13, RITF+11, RS15, SGGCR+16, SYL13, SWW+16, SSS11, SSPL+13, SXL16, Tar10, TLMM13, TLL12, WMX+17, WXWC14, XXX15, YC12, YqWqZC13, YZZ+15, YY11, YLS12, YMSH10, ZLY10, ZCLL14, ZZ15, ZG10, ZZ12, ZCL12, Zhu13, Ano12, OKG+12, YSS14, YFK+12].

Secure-TWS [OKG+12].

Security [WXLY16, WWS19, XWSW16, XJWW13, YAM+15, YGD+17, ZXZ+11, ZDL12, ZVG16, ZHT16, ZBR11, AHS14, ABD13, AC16, ACD+15, BSR13, CCLL11, CLHJ13, CW14a, CS11, FHH10a, FLL+14, FSGW12, FA14b, FIO15, Gal13, GCH15, HGWW11, HWZ+15, HLYS14, HPY10, IB11, JZS+10, KPP16, KKA14, KRM+10, KTUI16, LLLS13, LDDAM12, LH11a, LLW16, LSR13, LCT+14, LL+15, LL16a, LL16b, LBOX12, MR14c, NACL12, NAL17, PSLvdLE10, Rao17, RG10, RYF+13, RITF+11, RS15, SGGCR+16, SYL13, SWW+16, SSS11, SSPL+13, SXL16, Tar10, TLMM13, TLL12, WMX+17, WXWC14, XXX15, YC12, YqWqZC13, YZZ+15, YY11, YLS12, YMSH10, ZLY10, ZCLL14, ZZ15, ZG10, ZZ12, ZCL12, Zhu13, Ano12, OKG+12, YSS14, YFK+12].

Securely [CC10, LHL+14, MS16, WXY+17, der10].

Security [BK12b, CMLS15, NPH+14, PMZ13, SFE10, SL11, Ste15b, TKR14, YT12, CR10, SA15, Tox14].

Security [ABJ13, ASBS16, Ano13b, Ano15a, ABF12, AN15, ABH+16, BCB+10, BCM+15, BRT12, BPR14a, BPR14b, BLS12, BCG16, BPS12, BP10, CFST17, CFE16, CHS11, CFXY17, CCD15, CPS16, CM11, DDS12, Dan12, DR12, FSX12b, FSP12c, GZZ+13, GSC17, HC12, HLW12, HX+11, HLC11, HL+15, HLN+10, IS12, IGR+16, JN12, Jint14a, KBL11, KFOS12, KSD+17, KD12b, LPS12, LST12, LW11a, LR14, LW12, LT11, LP12, LR17, LZC12a, LDB+15, LMS16, MYT11, MK13, MCS+15, MH14, Man12, MV16a, MLBL12, MPM+17, Nac12, NAM10, NDG+17, Nos11, Nos14, Orm16, OS16, Pas13a, PZPS15, PDNH15, PS14, PL16, PDT12, PNRC17, RQD+15, RZW12, Rog16, RS10, SN10, SNJ11, SBS+12, Sar12, Sch13, SD12, Shi11, SLM10, STC11, SMOP15, SCGW+14, Tso13, TV15, WYCF14, WSA15, WSS12].

Security [WS14, Yan10, YZLC12, YSS14, Yon11, Zha15, vTJ11, AB10a, Abe10, ABGR13, Ano11a, BYL10, BSS11, BDL+11, BLV17, BM11, CO11, CTHP15, CLOC10, CVG+13, DLK+16, DHW+13, Edw14, FHM+12, FA14a, Fi15, GM16, GLM+16, GMS11, GH12, HWDL16, HWG10, HLR11, HRS13, HLV10, KSA16, KKK+16, Lan10, Lan13, LH10a, LXMW12, LH11, LZC14, LSG16, MZA+13, Men13, MM14b, NS10, NLC13, NLYZ12, OYHS14, PHWM10, QYWX16, Rec15, RPSL10, RH10, SA12, SLZ12, SY15b, Sr16, Sta11a, UUN11, VCK+12, XCL13, WX12, YKC+12, Bar12].

Security-Aware [LMS16].

security-modified [MM14b].

Security-Aware [LMS16].

Security [MM14b].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security [MM14b].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].

Security-Aware [LMS16].
[WHZ12, PGLL10]. **Semi-homomorphic**
[BDOZ11]. **Semi-trusted** [XZLW15].
**Semi-trusted** [SS10c].
**Semi-trusted** [XZLW15].
**Semi-trusted** [Dur15].
**Semi-paper** [WZ15].
**Sensational** [YGFL15].
**Sensing** [Kar12, RPG12, XWZW16, Fay16].
**Sensitive** [Kaw15, RQD+15, Tan15a].
**Sensitivity** [YGD+17, LWW+10].
**Sensor** [ABC+17, BN14, CS14, DS11, KH10, LLC11, LLZ+12, NAM10, NYR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YM16, ASO14, AIB+16, ADF12, BLAN+16, BB16b, CDGC12, CLSW12, DSCS12, DLN13, HTC+10, JM+16, KLC+10, KO16, KLW+16, LC17, PL16, SZMK13, SKK10, Wam13, WW14, WXK+17, XWDN12, XMHD13, ZYL+10].
**Sensors** [DL12].
**Sensory** [SGC14].
**Seoul** [LH10a, LW11a].
**Separation** [MJS13].
**Sequence** [PFS12, WGZ+12].
**Sequences** [ADD10, Kla10, NN12, XYXYX11, HLC12, VM14].
**Sequential** [GLR10, GLR13, LLY15, WYL13].
**Series** [BJL16, Die12].
**Serpent** [PC16].
**Server** [BCO13, Che15, GMS14, LLL15, YLW13, CLHJ13, FA14b, HDPC13, HL14, ISC+16, LMXW12, LH13, SY15b, hSZZ15, SSAF11, SSS11, TLL12, WT10a].
**Server-Aided** [GMS14, LLY15, SSAF11].
**Server-Designation** [Che15].
**Server-Side** [BCO13].
**Servers** [DRD11].
**Service** [BKBK14, CCS14, Hay13, LDB+15, LBR12, NRZQ15, RSGG15, SSPC12, VS16, AaBT16, KPP16, LW13a, MLM16, Par12b, YWK10b, ZXL11, YCM+13].
**Service-Based** [LDB+15].
**Service-Oriented** [RSGG15].
**Services** [AaBT16, DLZ+16, MEF012, OO12, ZHL15, AZPC14, CHX13, IG11, NZL+15, PP11, XXX15].
**Session** [BS12, BKJP12, CFST17, SRS12, AN15, DCA12].
**Setting** [BKJP12].
**Set** [Cor14b, EKP+13, YZ12, Con12, TMK11].
**set-valued** [TMK11].
**set** [SF12].
**Setting** [BKLS12, MZHY15, XXZ12, ZHL15].
**Settings** [GZ12].
**setup** [Jia16].
**Several** [Sas12, ZT14].
**SHA** [AAE+14, App15, jCPB+12, LC17, MAK+12, SKP15].
**SHA-1** [AAE+14, SKP15].
**SHA-256** [App15, MAK+12].
**SHA-3** [jCPB+12, LC17].
**SHA-1** [SA12].
**Shared** [CFOR12, KU14, SA16a, WY12].
**Sharing** [BFM12, BBEPT14, CCM15, CFOR12, CCL+13, CHT+14, CLW16, DR12, EM12, FR16, HL10a, HRS13, HLT+15, KU14, KSSY12, KS15, LYZ+13, LPL15, Lin15, LCCJ13, LTC+15b, NS12, Ob11, PSM17, SC10, SSS12, TL12, TWZ11, WYCF14, WKB16, WGF16, XNK15, XZY+12, YFF12, YWZ+12, ZC13, CT11b, CW14a, EZ15, EA11, FGMP12, GJMP15, GL13, HF14a, HBBRN+16, HCCC11, HLC12, KI11, KTU16, KPB17, LX12, LT13, LFWS15, LAL+15, LyWS10, LHY12, LHL15, LL16a, G17, O10, Q16, R17, T14, U11, U13, WK11, WS12, WOLS12, YC11, YCC16, ZCL+12, ZZ15, YW12, SSS10].
**Shell** [YSS14, Tay14].
**Shenzhen** [IEE11a].
**Shield** [NDG+17, KGV16].
**Shift** [AKP12, ZH15, LW11].
**Shift-Type** [AKP12].
**Shift** [YYW10, CSS+13].
**Shih** [Joh10].
**Shopping** [AHS13].
**Shor** [MMN+16].
**Short** [BGH12, CWWL12, MR12, SKV12, WQZ+16, XGLM14, LLY15, RD17, ZQW12].
**Short-Output** [NR12].
**Shorter** [PPB16, TH16].
**shown** [Ana14].
**shows** [Goo12].
**Shparlinski** [Sha10].
**Shredder** [AMH+16].
**Shredding** [AMH+16].
**SHS**
LRW13, LRW17, LWW+10, Maz13, PHN+12, SI12, Sun16, WKH11, WOLS12, ZMS14.

Stego [YLL+12], Stego-Image [YLL+12].

Stellenbosch [BL10], step [AKY13], STES [CMLS15], Steven [Led16, Sch15a], Still [RAZS15], stolen [Bha16], Stopping [Sav13a], StopWatch [LGR14], Storage [BCQ+13, CWL16, CCT+14, CLW16, GLG12, HSM14, JSCM17, Kip15, LCK11, LMD16, LWJCJ14, QLL17, SKH17, XNKG15, ZDL12, ZVG16, AY14a, BP10, CFVP16, CFZ+10, CLH+16, CDF+10, FH13, HSM13, LBOX12, Sar10a, SY+17, SWW+16, SW+17, WS13, YLL+12].

Steganography [BHR16], Steganography-Image [BHR16].

Stellenbosch [BL10], step [AKY13], STES [CMLS15], Steven [Led16, Sch15a], Still [RAZS15], stolen [Bha16], Stopping [Sav13a], StopWatch [LGR14], Storage [BCQ+13, CWL16, CCT+14, CLW16, GLG12, HSM14, JSCM17, Kip15, LCK11, LMD16, LWJCJ14, QLL17, SKH17, XNKG15, ZDL12, ZVG16, AY14a, BP10, CFVP16, CFZ+10, CLH+16, CDF+10, FH13, HSM13, LBOX12, Sar10a, SY+17, SWW+16, SW+17, WS13, YLL+12].

Structural [BMK12].

Structure-Independent [MKRM10], Structured [PMZ12], Structures [GT11, HH+13, LH16, LPL15, PB12, DDFR13, MKS14, Shy15, WS12, ZZ15].

STT [VDB+16], Students [PP10a], Study [DDR+16, SY15a, STC11, CCG10, EBFK13, HSM15, SS17, VGN14], Stuxnet [Zet14], Style [GHPS12, GHPS13].

Subcommittee [Bla16], submarine [LWJG10], submarines [McG11], Subscribe [BGP+17, SLI11], Subset [BS14, RP12, ZZ11], subspaces [ZWM14].

Substructure [MRT10], Succinct [BCI+13, CKLM13].

Suitable [Jeo13, SKB+17], suite [NACL12], Sumo [BS12], Sun [Cer15], Supervised [CTC+15], Supply [ZQ+16a, ZQ+16b, YFT17].

Support [SZC11], support [CZ14, PKA15, TTL10, VCK+12, ZMM+10, ZBR11], Supporting [FMTR12, HCDM12], surfaces [CDSL14], Surprises [Bow11], Surreptitiously [SFRK15], Surveillance [BPR14a, BPR14b, Lan10].

Survey [ABHC+16, BGN17, BCTPL16, BHP14, BJCHA17, HPC10, KSD+17, LGM+16, MR14b, MS10, NV10, OFMR16, SKH17, TRD11, AZZ+16, VCK+12, ZMM+10, ZBR11], Support [FMTR12, HCDM12], surfaces [CDSL14], Surprises [Bow11], Surreptitiously [SFRK15], Surveillance [BPR14a, BPR14b, Lan10].

Survey [ABHC+16, BGN17, BCTPL16, BHP14, BJCHA17, HPC10, KSD+17, LGM+16, MR14b, MS10, NV10, OFMR16, SKH17, TRD11, AZZ+16, VCK+12, ZMM+10, ZBR11], Support [FMTR12, HCDM12], surfaces [CDSL14], Surprises [Bow11], Surreptitiously [SFRK15], Surveillance [BPR14a, BPR14b, Lan10].

Survey [ABHC+16, BGN17, BCTPL16, BHP14, BJCHA17, HPC10, KSD+17, LGM+16, MR14b, MS10, NV10, OFMR16, SKH17, TRD11, AZZ+16, VCK+12, ZMM+10, ZBR11], Support [FMTR12, HCDM12], surfaces [CDSL14], Surprises [Bow11], Surreptitiously [SFRK15], Surveillance [BPR14a, BPR14b, Lan10].
Synchronization
[BL12, WXY+17, XNG+14]. synchronized
[ACM12]. Synchronizing [HZ11]. SYN
[MHC12]. Syndromes [BBC+13]. Synergy
[KRB12]. Synergy-Based [KRB12].
synthesis [RS17]. Syst [WZM12a]. System
[ADI11, Ano10, CZLC12a, CZLC14, Cor14b,
CRST15, DG15, GOPB12, Har16, HHS+15,
JN12, JWJ+17, KMP+11, Lop12, MLBL12,
NSMS14, QLL17, SLI11, YE12, YXZ+12,
ZPW16, ZLDC15, ZVG16, BBG+13, Bul10a,
CH11, CTL12, CZ14, CS11, GKC11K,
HWK+15, HJM+11, HLS14, LLLK10, Lit14,
LTC+15a, MS12a, MNNW15, PSONPL13,
SSPL+13, WXM+17, WGW+12, XWZW16,
ZMM+10, ZML17, KKA14, Dew11].

System-Level [JWJ+17]. Systematic
[CCG+16, CBL13, PC16]. Systems
[AN12, AB15, BL15, BS13b, BCTPL16,
BB10, CWW16, CRE+12, DLZ+16b, GI12,
HXU+11, HCL+14, HLN+10, LMD16,
LQY10, LY16, LNZ+13, MR14b, OŠ12,
QZL+16b, RST15a, RST15b, SBS+12,
SKR15, Sev16, SKH17, SGC14, SDM+12,
STC11, TKR14, YNR12a, AT10, AT1+10,
CFVP16, CFZ+10, CLZ+17, dCCSM+12,
dCCSB+16, CGH11, CVG+13, CDA14,
DZS+12, Eis10, FXP12, GNOGCC15,
GSN+16, GPVCD10, JSK+16, JHCC14,
KSA16, LCL+15, MLMSM12, MGP10,
MFI13, NLYZ12, SS10a, SR10, SRB+12,
WS14, YSM14, ZH13, MA17, Ano11a].

Systolic [MCD12]. Systolic-Array
[MCD12]. SZK [MX13].

Table [CCL+13, AY14a, LDDAM12].
Tables [PTT16]. Tag [NNAM10, PPH12,
CJP15, SPLHB14, CJP12]. Tags
[MO12, HSH11, HDPC13, HQY+16, MK12a,
PLSvLE10, TG17]. Taipei [Yan11].
Taiwan [Yan11]. Takes [Ano16c]. Talking
[FD11]. Tamed [NXB13]. taming
[BBDL+17]. tamper
[MN10, NC13, WGM12]. tamper-evident
[MN10]. Tampered [SSA13]. Tampering
[CG14a]. TAO [Sta13]. Taormina [Cra12].
tap [ADG16]. Targeted [ABJ13]. Tasks
[ABel2, FKS+13]. Taxonomy
[AJA16, GAF+15, KMSM15, MA17]. TCC
[Cra12, Lin14b, Sah13]. TEA [CWP12].

Teaching [GY13]. Team
[LJS+14, Pf110, An114]. Tear [Boy16].
Tear-Free [Boy16]. TEASE [ZB11].

Technical [Sir16, Wag16, JW14, Suc12].

Technique
[KBL11, BPP13, GCSÁdd11, TS16].
Techniques [Bis17, DA12, GOS12, HPC10,
HL10b, LV12, Mor12, PJ12, AB10b, BM13,
FGPG14, Gil10, HT13, KHF10, LH11a,
VN17, WXM+17, JH10]. technologies
[JR10, JAS+11, Lan10]. Technology
[CGB+10, Fol16, IEE11a, WU16]. Telecare
[MA17]. Telephony [SKEG14]. Television
[DTE17]. Tell [Cer14]. Template
[NGAaH16, SKV12, AT1+10, GCSÁdd11].
Templates [DWB12]. temporal
[MWM+16, MHT+13, XHM13].
temporal-credential-based
[MWM+16, XHM13]. Tenant [TV15].
terahertz [WW13]. Term
[SKV12, CFVP16]. termination [SRB+12].
Ternary [ADI11]. Test [HTC+15, JEA+15,
LLSW16, MZH15, SS10b, Ano16f].

Testable [RMP10]. tester
[RPSL10, SY15]. Testing
[Cou12, SS12a, AY14a, BJF+14]. Tests
[GLG12, MS12b, Sim15]. Texas [IEEE13].

Text [Gd16, CR12, SI12, SWW+17].
Text-dependent [Gd16]. Textbook
[PP10a]. Theft [Ber12, BTPL15]. Their
[CSLC12b, NR12, Hof16, IK15, KK10, Sti11].
them [HLV10, JSK+16, RS15].

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

Theoretic
Theoretically [KL13, ZZ15, Gas13].

Three-Factor

Three-Dimensional [LZC+12b].

Three-Phase

Throughput [MAK+12]. Thru [SYC+17, SYW17]. Thwart [LS+14].


Time [GDCC16, LPS12].

Time-Area [Nov10]. Time-Memory [ASBSD16]. Time-Series [BJL16].

Time-Specific [KME+12]. Time-Spread [HGT15].

Timed [Jia14b, KFOS12, Tan15a, Unr15, WSS12].

Timed-Ephemerizer [Tan15a].

Timed-Release [KFOS12, Tan15a, WSS12].

Timing [BGN17, GV14b, Hay13, LGR14, SRB+12].

Tiny [ZOC10]. Titan [PP10b]. Titan-R [PP10b]. TLS [AP13, BBDL+17, BFCZ12, CFN+14].

Today [Ber16a, Mac12].

Toeplitz [Ye10].

Token [TYK+12, ZM16, Jac16].

token-based [Jac16]. Token-Leakage [ZM16]. tokens [DCAT12].

Tokyo [Sah13].

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

Tolerating [ZM14].

Tone [Yam12].

Too [DL15, DDSW14, Ros11].

Tool [ASM12, DKMR15].

Toolbox [AHS13, TRD11].

Toolkit [BJL12].

Tools [Abe12, BKBK14, Ste15a]. Top [SS12a, SS10c, Sta13, CHX13].

Top-CHX13. Top-Panin [SS12a]. Top-Secret [SS10c].

Topics [SCPS10a, SCPS10b, AB10b, Dun12b, Kia11, Pie10].

Topology [HHMK14].

Topology-Preserving [HHMK14].

Tor [LLY+12a].

Toronto [MV12].

Tossing [ALR13, DSMM14, Fok12, BB14].

Touch [SPW+16, CTL12]. TPM [GY13].

TQC [vDKS11]. Trace

[ABR12, PS14, AA14, WGJ16].

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

Traceback [LWY12, WYL13].

traces [MYR13].

Tracing [LW16, FPS12b, MFH13, PPR+12].

Track [Dun12b, Kia11, Pie10].

Trade [ASBSD16, BS14, SR10].

Trade-OFFs [ASBSD16, BS14, SR10].

Tradeoff
Unconditional [Jia14a]. Unconditionally [CFOR12, LHF12, SNJ11].

Unconditionally-Secure [CFOR12].

Uncovering [FMS12a, WBC¹+10].

Undeciphered [Rao10].

Underfeeding [BBBP13].

Underhanded [Cra14].

Understanding [EPAG16, PP10a, Bar12].

Unexpanded [SA16a].

Unidirectional [LSC12, DKL¹+16].

Unified [ZSW¹+12].

Uniformly [YKKL12].

Unilaterally [GRL12].

Unintended [Ess17].

Union [BBDL¹+17, Bud16].

Unique [SSPC12, SOS15].

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

Units [ABDP15].

Universal [ASM12, BJL12, NR12].

Universally [DN12].

University [CGB¹+10, Wes16].

Unlimited [IBM13a].

Unlocking [VS16].

Unmanned [XWZW16].

Unprovable [Pas13a].

Unsigncryption [EZ15].

Unstructured [CML16].

Untold [Pea11].

Untraceability [YHL16].

Untraceable [JMW¹+16].

Untrusted

[LQY10, MS16, DRD11, MVo11, WS13].

Updatable [LCL¹+17a].

Update [BCE¹+10, LQY10].

Upper [ÂMVK12].

URLs [AY14a].

USA [Dun12b, IEE13, Kia11, Lin14b, Ple10, Rab10, ACM10, ACM1, IEE10, IEE11b].

Usability [RAZS15].

Usable [DL15, TGC16].

Validating [GJ¹+12].

Validity [BCF16].

VANETs [BMM12, CGCGPDMG12, LLG15, YMM13].

Variability [VDB¹+16].

Variable [CHHW12, CMMS17, DTZZ12].

variable-interval [DTZZ12].

Variables [BB10].

Variants [ASS15, BB10, Hin10].

Variation


Verification [App15, ABR12, BL15, CCK12, CCC16, CM11, EWS14, Ess17, GLLSN12, GdM16, GMSV14, Lin15, MV16a, OSH12, PNRC17, SOF12, Tom16, Vet10, ZPW16, AHP14, ARB+14, ASVE13, BFG+14, GPN+12, KKK+16, MR14c, NPH+14, SD10, YNX+16].


Very [BFM12, Jou13]. via [BKHNN13, BCI+13, BR14, CDSLY14, CLW16, GT12, GST13, GVV12, LT13, LT14b, MH14, PTK14, QZDJ16, RS10, SE16, S efficienciesplus11, SKEG14, TBCB15, tWmC12, Yon11, ZOC10, Zim10].


Video [BWR12, DG17, GKS17, JSZ12, OSH12, TWZ+12, WLZL12, YE12, YTI12, Cri16, LLHS12, MK11, OCG11, XZW16].


Voynich [Ano16d, Bax14]. vs [FKOV15].

Vulnerabilities [BKJP12, MAS16, PTD12, RY10]. Vulnerability [MKNN13, TM12, VKC15, DMWS12, MYYR13]. Vulnerable [Ano15c].

vVote [CRST15].


warrior [Bud16]. wartime [McK10, McK11]. was [Goo12, LHA+12].

Watermark [CHHW12, EMW14, KBL11, LJC+12b, MCDB12, SJ12, YE12, ZS12, HB13, TLL13, WYL13].

Watermarking [BCGAM12, BF12, BCPV11, CG12b, CHHW12, DG17, FM15, Fra15, Fra16, GKS17, HPC10, HGT15, HHH14, JSZ12, Jok10, JKHy12, KD12a, LSL12b, LP12, MR16, MU12, NGAH16, NC12, pNyWY1+14, OWHS12, RS16, RP12, RR11, SAA15, SLGZ12, SSA13, TWZ+12, TC10].
Weaker Weakening GJMP15, RH10]. [LY15].


Web-Based [CD12]. web-content [GPN12]. WebCallerID [HCM11].


WG [GLIC10, DJG15, ERRMG15]. WG-ERRMG15]. Wherefore [BDK11]. Whit [LHA12]. White [BW16, BCGN16, Mic10b, DD13, YSC16].


Wiretapping [Lan10]. Wiring [HTZR12]. Wise [CG14a, SSA13]. WISP [PPH12].

Without [ASS15, CCL13, FZT14, GSW16, LTC15b, NA10a, YLA13, AZH11, BT12, BF11, BGV14, CCW10, FSX12a, GH11a, GST12, GLM16, HDP13, ISC16, LLY15, LGWY12, RG10, SYL13, SLZ12, TAK10, WWYY11, XQL11, YS12, YKC11, YFK12]. WLAN [KAHK17]. women

[Hea15, McK10, McK11]. Word [WW12].


[Ano16, BFK16, BPS16, FKS13, KM10c, Tom16, Con12, GJJ12, Goo12, LCKBJ12, Pet11, Sch15c, Zet14]. world-class [Goo12].

Worm [WWC11]. Worst [Bikk14].

writing [LT14b]. wrong [LHA+12]. WSN [DL12]. WSNs [ZY+10]. Wu [LLLK10]. WW2 [Don14]. Wyner [ADG16].


References

Akyildiz:2014:OTB


Abo-alian:2016:KDB


Ambrosin:2016:FAB


Albertini:2014:MHE

Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Malicious hashing: Eve’s variant of SHA-1. In Joux and Yousef [JY14], pages 1–19. ISBN 3-
REFERENCES


[AB10b] Abdalla:2010:PCL


[AB10b] Atallah:2010:ATC

Mikhail Atallah and Marina Blanton, editors. Algorithms and theory of computation handbook. Special topics and techniques, volume 2 of Chapman and Hall/CRC applied algo-
REFERENCES


Giuseppe Ateniese, Giuseppe Bianchi, Angelo T. Capossele, Chiara Petrioli, and Dora Spenza. Low-cost standard signatures

**[Adrian:2015:IFS]**


**[Agosta:2015:OPP]**


**[Abe:2010:ACA]**


**[Abe:2012:TBG]**


**[Arriaga:2012:JSS]**

Afonso Arriaga, Manuel Barbosa, and Pooya Farshim. On the joint security of

**Almeida:2014:COS**


**Ananth:2013:SFP**


**Avoine:2016:SSP**


**Aid:2013:DIO**


**Acar:2013:SPA**

Tolga Acar, Mira Belenkiy,

Arapinis:2012:RET


[ABR12]

Applebaum:2010:PKC


[ABW10]

Arias-Cabarcos:2015:BIP


[ACAT+15]

Arnold:2015:NGH


[ACD+15]

**Amoah:2016:FMA**


**Ardagna:2010:ECP**


**Avoine:2012:PFS**

REFERENCES


Adikari:2011:HBT


Abdalla:2012:LBH


Andrychowicz:2016:SMC


Attrapadung:2015:RGS


Akinyele:2014:MGA


Abdullaziz:2016:AAI

Ahani:2015:SRB


Attrapadung:2012:ABE


Appelbaum:2013:SSG


Aiash:2015:FAA


Amin:2016:DAP

Ruhul Amin, SK Hafizul Islam, G. P. Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer*


Frederik Armknecht, Stefan Katzenbeisser, and Andreas Peter. Shift-type homomorphic encryption and its application to fully homomorphic encryption. Lecture Notes in Computer Sci-
AlTawy:2013:SOC


Aiash:2015:IAA


Alomair:2012:AEH


Asharov:2013:FCF


Awad:2016:SSZ


Arsalan:2012:IRW


Ahir:2017:LAR


Adj:2013:WDC


Aumasson:2014:HFB


Ahmadian:2010:PDS


Alvarez:2012:CAB

Rafael Álvarez, Francisco


Anonymous: 2015: BSU


Anonymous: 2015: CEB


Anonymous: 2015: QCS


Anonymous: 2016: CPSd


Anonymous: 2016: CPS e


Anonymous: 2016: EMT

Anonymous. The Enigma machine takes a quantum leap. *R&D Maga-

**Anonymous:2016:FVM**


**Anonymous:2016:GUP**


**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:MBH**

Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF


AlFardan:2013:LTB


Applebaum:2013:GXG


Applebaum:2014:CCP

Benny Applebaum. Cryptography in Constant Parallel Time. Information Security and Cryp-
REFERENCES


Ahmadi:2012:SKE


Asaar:2015:IBM


Alsulaiman:2013:IVB


Altman:2010:AAP


Argyropoulos:2010:BTP

[ATI+10] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, Yannis Damousis, Michael G. Strintzis, Martin Braun, and Serge Boverie. Biometric template protection

**Au:2011:PPT**


**Alam:2015:ACF**


**Aslan:2016:DEM**


**Abdalla:2012:LRS**


**Alzala-Yamajako:2012:RAC**


**Ahmad:2014:RTN**

Tahir Ahmad and Usman Younis. Randomness testing of non-cryptographic hash functions for real-time hash table based storage and look-up of URLs. *Journal of Network and Computer Applications*, 41(??):197–205, May 2014. CO-
AlTawy:2014:IDR


Ayub:2012:BRB


Apavatjrut:2012:EEA


Alshammari:2011:CET


Alavi:2014:RQE


Behnia:2013:IEB

S. Behnia, A. Akhavan, A. Akhshani, and A. Sam-sudin. Image encryption based on the Jacobian elliptic maps. The Journal of Systems and Software, 86(9):2429–2438, Septem-
REFERENCES

Blander:2013:IPP


Brennan:2012:ASC


Bailin:2012:ERG


Bercearu:2010:FSM


Barbay:2012:BRB


Barthe:2015:HAC

REFERENCES


REFERENCES

DEN ???? ISSN 1550-4832.

Boumerzoug:2016:LKM


Barenghi:2013:FIT


Barak:2014:OEF


Beurdouche:2017:MSU

References

Beimel:2014:MLS

Bernstein:2017:SRD

Boldi:2012:IUG

Bernstein:2011:PCI

Basin:2014:KYE

Bichsel:2012:DMA
Patrik Bichsel, Jan Camenisch, Bart De Decker, Jorn Lapon, and Vincent Naessens. Data-minimizing authentication goes mobile. Lecture Notes in Computer
Badrignans:2010:SSA


Balfanz:2012:FA


Bugliesi:2015:ART


Buhrman:2014:PBQ


Bahri:2016:CCO


Bahi:2012:SCS

Jacques M. Bahi, Jean-François Couchot, and Christophe Guyeux. Steganography: a class of secure and robust algo-
References

Borghoff:2012:PLL

Baelde:2012:TPR

Bahi:2011:ECS

Barthe:2012:CA

Beunardeau:2016:WBC

Bitansky:2013:SNI
Nir Bitansky, Alessandro

---


Borghoff:2012:PLL

Baelde:2012:TPR

Bahi:2011:ECS

Barthe:2012:CA

Beunardeau:2016:WBC

Bitansky:2013:SNI
Nir Bitansky, Alessandro

**Bernstein:2014:CKR**


**Basin:2012:PRI**


**Basin:2015:ISC**


**Bicakci:2013:LSS**

Kemal Bicakci, Bruno Crispo, and Gabriele Oligeri. LAKE: a server-side authenticated key-establishment with low computational workload. *ACM Transactions on Internet Technology (TOIT)*, 13(2):5:1–
REFERENCES

5:??, December 2013. CO-DEN ???. ISSN 1533-5399 (print), 1557-6051 (electronic).

[Botta:2014:PCI]

[Boyle:2014:EO]

[Basso:2011:BWC]

[Bessani:2013:DDS]

[Blasco:2016:SWB]

[Biddle:2012:GPL]
Bender:2012:DSP


Bhasin:2015:EFB


Backstrom:2011:WAT


Bernstein:2011:HSH


Bossuet:2016:EPA


Bendlin:2011:SHE

REFERENCES

http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_11.

[Bertoni:2011:CSF]

[Berto

[Berto

[BDP11]

[Berton

[Bertoni:2012:KIO]

[Boldyrev

[BDPS12]

[Bonito:2013:WFS]

[Bellot

[Bellovin:2016:EEE]

[Berghel:2012:ITF]
REFERENCES


205, January 2014. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). POPL ’14 conference proceedings.

Bobba:2010:ABM

Bhargavan:2016:MVP

Beimel:2012:SSS

Berger:2016:EGF

Battistello:2012:TBA
REFERENCES


Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete log-


REFERENCES


Behnia:2012:SEI


Bosc:2014:SPS


Bonneau:2015:PEI


Biagioli:2012:CCS


Beimel:2014:CCW

Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. Lecture Notes in
REFERENCES

Biswa:2017:SA

Brumley:2010:CAI

Boche:2016:DSK

Bouraoui:2017:HAE

Bogdanov:2012:UTC

Benhamouda:2016:NFP
Fabrice Benhamouda, Marc Joye, and Benoit Libert. A new framework for privacy-preserving aggregation of time-series data. *ACM Transactions*
REFERENCES

100

Brubaker:2014:UFA

Boldyrev:2012:NPG

Bouti:2012:SCB

Bhuyan:2014:DDD

Braun:2012:ULA

Brakerski:2010:OHB
Z. Brakerski, Y. T. Kalai,
REFERENCES


Suvarna Bothe, Panagio-

Bernstein:2010:PCA


Byun:2011:SMC


Bai:2012:SSR


Bernstein:2014:HEC


Bidgoly:2015:MQV


Blanchette:2012:BPC

REFERENCES

276 pp. LCCN K2269.5 B58 2012.

Blaze:2016:UHR


Benzaid:2016:FAW


Blomer:2012:TKG


Blondeau:2015:IDA


Bernstein:2012:SIN


Bestavros:2017:PSU

REFERENCES


Burmester:2011:LRA


Birajdar:2013:DIF


Bard:2015:PRO

Gregory V. Bard and Theodore McDonough. Plaintext recovery for one-time pads used twice. ACM Communications in Computer Algebra, 49(1):17–18, March 2015. CODEN ????

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

Benamara:2016:ICA


Baldwin:2010:AFI


Biswas:2012:IBA


REFERENCES


[BP10] Randal Burns and Zachary Peterson. Security con-


REFERENCES


[Brakerski:2014:VBB]

[Brakerski:2013:WHB]

[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


Bellare:2012:MIS


Brumley:2012:SFI


Bergsma:2012:PAW


Bajaj:2013:CSE


Birrell:2013:FIM


Bhattacharjee:2014:CAT

REFERENCES

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

Bagheri:2015:NNA


Boorghany:2015:CIL


Bojinov:2014:NMC


Batina:2012:HEB


Broustis:2012:GAN

REFERENCES


REFERENCE

1. Bhatnagar:2013:BIW

2. Bai:2016:ALC


Feng Bao, Moti Yung, and Dongdai Lin, editors. *Information security and cryptography: 5th international conference, INSCRYPT 2009*, Beijing, China, December 12–15,
REFERENCES


REFERENCES

Chadha:2016:A

Chretien:2015:SPP

Carota:2012:FFI

Chou:2010:PSO

Checkoway:2016:SAJ

Chadha:2012:A
Rohit Chadha, Ştefan Ciobăca, and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. Lecture Notes in
References

Chatterjee:2016:TAD


Chou:2013:UGS


Chang:2011:SFW


Cascudo:2015:SSN


Chatterjee:2017:PBS


Cho:2014:DGA

Michael Cheng Yi Cho, Pokai Chen, and Shi-

Chen:2011:EAA


Chu:2014:KAC


Chen:2010:ALD


Chiasson:2012:MWB


Cui:2016:RDA


Criswell:2014:VGP

John Criswell, Nathan Dautenhahn, and Vikram

**Cheng:2013:DVB**


**Ciriani:2010:CFE**


**Ciriani:2010:TPA**


**Choo:2016:CCT**


**Cao:2012:ITM**

REFERENCES


Carter:2013:SSA


Centenaro:2013:TBA


Checkoway:2014:PED


Cevallas:2012:USR


Carstensen:2011:AAA


Calzavara:2017:SWJ

Stefano Calzavara, Riccardo Focardi, Marco Squarcina, and Mauro Tempesta. Surviving the Web: a journey into Web session security. *ACM Computing Surveys*, 50
REFERENCES

Celesti:2016:ALT

Choo:2017:EDF

Chang:2010:PRN

Chen:2010:IFA

Camenisch:2012:EAA

Che:2012:WAM

Cheraghchi:2014:NMC

Corrigan-Gibbs:2014:KS

Chaudhuri:2010:PIC
Pranay Chaudhuri, Sukumar Ghosh, Raj Kumar Buyya, Jian-Nong Cao, and Oeepak Oahiya, editors. Proceedings of the 2010 1st International Conference on Parallel Distributed and Grid Computing (PDGC), Jaypee University of Information Technology Waknaghat,


Caballero-Gil:2012:LAR

Chmiel:2012:EPC

Coull:2011:ACO
Scott E. Coull, Matthew Green, and Susan Hohenberger. Access controls for oblivious and anonymous


[Chang:2013:MPQ] Mei-Chu Chang. On a matrix product question in

**Chen:2011:CCI**


**Chen:2012:SRF**


**Chen:2012:IAM**


**Chen:2015:SSS**


**Cheswick:2013:RP**


**Chien:2012:IAM**

Chien:2013:CRC


Chirgwin:2013:ABB


Chien:2016:GAI


Chirgwin:2013:ABB


Chou:2014:EMA


Chen:2011:SEI

Tien-Ho Chen, Han-Cheng Hsiang, and Wei-Kuan


REFERENCES


See cryptanalysis [SPLHC14].


REFERENCES

Chang:2011:RSB


Chong:2013:ASG


Chen:2016:RPR


Chen:2012:NCB


Chen:2013:TSE


Cao:2012:SRH

REFERENCES


Canetti:2013:PCC	Cui:2016:KAS


CLP13a	CLW16

CLP+13b	CLY14

CLZ17
REFERENCES


[CMA14] Hui Cui, Yi Mu, and Man Ho Au. Signcryption secure against linear related-key attacks.

[Cozzens:2013:MEE]

[Chakraborty:2013:EHI]
REFERENCES


REFERENCES

Chin:2011:ACS

Conitzer:2010:AP

Constandin:2012:RSN

Copeland:2010:CBG

Copeland:2010:CSB

Chung:2014:RRS

Cordova:2014:EBS
Tim Cordova. Encrypted

**Corthesy:2014:SSD**


**Coutinho:2012:RPT**


**Claessen:2013:SPN**


**Chung:2016:NBB**


**Chevalier:2010:CSC**


**Chen:2012:DCC**

Jian Chen and Jeffrey S. Rosenthal. Decrypting classical cipher text using Markov chain Monte Carlo. *Statistics and
REFERENCES

Crampton:2011:PEC

Cramer:2012:TCT

Crav:2014:UCC

Clear:2012:CPA

Crichlow:2016:RSE

Culnane:2015:VVV
Chris Culnane, Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague. vVote:
a verifiable voting system. 


Chhabra:2011:NSN


Clark:2012:RLA


Chapin:2014:SRP


Chadwick:2014:AFI


Chen:2013:RWM


Ciegis:2016:ADP

Raimondas Ciegis, Vadi-mas Starikovicius, Natal-ija Tumanova, and Minvydas Ragulskis. Application of distributed parallel computing for dynamic

**Chong:2015:SID**


**Chow:2012:EPV**


**Chen:2011:IBT**


**Chen:2011:ARI**


**Chen:2011:TVS**


**Calzavara:2015:SLA**


**Chin:2013:SMB**

Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng, and Raphael C.-W. Phan. On

Chang:2012:GBP


Chou:2013:TIB


Crenne:2013:CMS


Calmon:2014:ITM


Choi:2012:LT


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

**Chen:2012:CKS**


**Chen:2014:MLC**


**Chen:2012:FSD**


**Chen:2015:OMU**

REFERENCES

Chen:2012:AIB


Chen:2012:IBE


Chen:2014:CSI


Dharwadkar:2010:SSG


Djebbar:2012:ASB


Danezis:2012:FCDb

REFERENCES


[DD13]


[DDArco:2014:MIC]


REFERENCES


derhans:2010:USC


Desmedt:2010:CF


Desmedt:2010:ES


Desmedt:2010:CF


Durmuth:2011:DEN


DuPont:2016:ECC

Quinn DuPont and Bradley Fidler. Edge cryptography and the codevelopment of computer networks and cybersecurity. IEEE Annals of the History of Com-

DeCapitaniDiVimercati:2010:EPR


Dutta:2017:EFC


Dupressoir:2014:GGP


Ding:2012:CLS


Djuric:2015:FSF


Ding:2012:NRR

[L. Ding, J. Guan, and W. l. Sun. New results of related-key attacks on all Py-family of stream ciphers. J.UCS: Journal of Universal Computer Science, 18(12):1741–??, ???? 2012. CODEN ???? ISSN ...
Drimer:2010=DBP


Dubeuf:2016=EPA


Dodis:2010=CAC


Driessen:2013=ESA


Diem:2012=UES


Drosou:2012=SAH

Ding:2015:CWF


Domnitser:2012:NMC


Dolev:2012:ATC


Delfs:2015:ICP


Dorre:2016:ELO


Durumeric:2014:MH

[DKA+14] Zakir Durumeric, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicholas Weaver, Johanna Amann, Jethro Beekman, Mathias Payer, et al. The matter of
Heartbleed. In ????, editor, ACM Internet Measurement Conference, page ??.


REFERENCES

DeLuca:2015:SUS


Degefa:2016:PSE


Dong:2013:PRS


Dai:2016:MLR


DiPietro:2016:CLD


Dodis:2011:SSC


Duan:2016:SDC

Li Duan, Dongxi Liu,


REFERENCES


[Duong:2011:CWC] Thai Duong and J. Rizzo. Cryptography in the Web:
The case of cryptographic design flaws in ASP.NET. Unknown, May 2011.

Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE


Dixon:2016:NTO


delRey:2012:EDI


Dini:2011:LLA

REFERENCES

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

Das:2015:DCS


Das:2016:MPU


Das:2012:DPB


Dachman-Soled:2014:COF


Dodis:2014:HEY

Dini:2013:HHS


Drosatos:2017:PET


Deng:2012:VIA


Dunkelman:2012:MEK


Dunkelman:2012:TCC


Durcheva:2015:SAI

Mariana Durcheva. Some applications of idempotent semirings in public key cryptography. *ACM Com-
REFERENCES


REFERENCES


REFERENCES


Edwards:2017:NSQ
El-Emam:2013:EEAZ13

Eisenbarth:2012:EEG12

Ebansarkhani:2012:EM12

Eisenbarth:2010:CCE
Embar:2014:PWO


Evtyushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC


Engels:2012:HLA

REFERENCES


Farash:2014:SEI

[FA14b]

Farash:2014:CIE

[Far14]

Fischlin:2012:PKC

[FBM12]

Fay:2016:ICM

[Fay16]

Ferretti:2014:DCI
Luca Ferretti, Michele Colajanni, and Mirco Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. IEEE Transactions on Parallel and Distributed Systems, 25(2):437–446, February 2014. CODEN ITDSEO.
REFERENCES

ISSN 1045-9219 (print), 1558-2183 (electronic).

Fuglerud:2011:SIA

Fehr:2010:QC

Faugere:2010:CLR

Fleischmann:2012:MFA

Feng:2010:CTS
REFERENCES


FAN:2014:ASA


Fawzi:2013:LDN


Florencio:2016:PSD


Farash:2015:PSE


Fisher:2015:CS


Fei:2012:GTK

Han Fei, Qin Jing, Zhao Huawei, and Hu Jiankun. A general transformation from KP-ABE to searchable encryption. *Lecture
Fan:2015:SVS


Fehr:2013:FCC


Fan:2013:CEM


Ferguson:2010:SHF


Forler:2012:DAC

Christian Forler, Stefan Lucks, and Jakob Wenzel.

[Feng:2012:CAO]


[FLZ+12]


[Fallahpour:2015:AWB]


[FM15]


[Fraczek:2012:MSI]

Albert Fernández-Mir and Rolando Trujillo-Rasua. A scalable RFID au-

\textbf{Ferreira:2015:LPA} \hfill \textbf{Folkkink:2012:TCG}


\textbf{Folkkink:2012:TCG} \hfill \textbf{Folger:2016:TQH}


\textbf{Folger:2016:TQH} \hfill \textbf{Fox:2013:RLQ}


\textbf{Fox:2013:RLQ} \hfill \textbf{Faigl:2014:PEC}


\textbf{Faigl:2014:PEC} \hfill \textbf{Folger:2016:TQH}

REFERENCES


[Fri10a] Jessica Fridrich. Steganography in digital media:

Friksen:2010:SMC


Friksen:2012:MTS


Fridrich:2012:MTS


Fang:2011:ICP

Lining Fang, Willy Susilo, Chunpeng Ge, and Jiandong Wang. Interactive conditional proxy re-encryption with fine grain policy. The Journal of Systems and Software, 84 (12):2293–2302, December 2011. CODEN JS-SODM. ISSN 0164-1212

Fraschiger:2013:TRR


Forbes:2015:CTC

REFERENCES


[Fang:2012:CCS]


[Ferguson:2010:CED]


[Feng:2011:GDA]


[Fujioka:2012:SHI]


[Fujioka:2012:SEP]
Fadlullah:2010:DCA


Fuchsbaeur:2011:CSV


Feng:2013:ECE


Fanyang:2012:SAK

REFERENCES


Christophe Guyeux, Raphaël Couturier, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic
REFERENCES


Gupta:2012:CDF


Gupta:2013:HPH


Guerra-Casanova:2011:SOT


Granado-Criado:2017:HCH


Gong:2016:ATI


Guerin:2016:TDU

Nilson Donizete Guerin, Jr., Flavio de Barros Vi-

[Geller:2013:MIS]

[Gentry:2010:CAF]

[Gentry:2013:EMH]


[GG10]
Grigg:2011:CCN


Garg:2016:CIO


Garg:2016:HSS


Guo:2012:EBP

Lifeng Guo and Lei Hu. Efficient bidirectional proxy re-encryption with direct chosen-ciphertext se-

Garg:2014:TRS


Gen
ty:2011:FHE


Gen
ty:2011:IGF


Guo:2012:EBP


REFERENCES

Gilad:2014:PHI


Godor:2012:HBM


Georgiev:2012:MDC


Gilbert:2010:ACE


Giry:2015:BCK


Gao:2013:LCA

Guangyong Gao and Guoping Jiang. A lossless copyright authentication scheme based on Bessel–Fourier moment and extreme learning machine


[GL12] Dieter Gollmann, Jean-Louis Lanet, and Julien Iguchi-Cartigny, editors. *Smart card research and applications*.

Gagne:2012:AVB


Guo:2011:EDA


Gong:2016:HES


Gradwohl:2010:SRC


Gradwohl:2013:SRC

Ronen Gradwohl, Noam Livne, and Alon Rosen. Sequential rationality in cryptographic protocols. ACM Transactions on Economics and Computa-
REFERENCES

Guo:2012:ETD


Guo:2013:TVS


Goyal:2011:SCP


Garmany:2013:PPR


Gotzfried:2014:MAT


Gofman:2016:MBE


Giambruno:2015:GGB

Laura Giambruno, Sabrina

García-Martínez:2015:HEB


García-Morchon:2015:HCR


Guo:2011:ISS


Guo:2014:SAS


Gao:2014:URA

REFERENCES


[Groza:2017:LCL]


[Gong:2012:KNF]


[Goodin:2012:CBS]


[Goodrich:2012:EVW]

**Genkin:2016:PKE**


**Gonzalez-Pardo:2012:CID**


**Greengard:2011:MRM**


**Grimes:2015:CCT**

Gibson-Robinson:2012:AAL


Guha:2017:RTS


Guin:2016:FCS


Gong:2016:FSC


Gierlichs:2012:ICD


Genkin:2013:RKE

Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. Technical and web report, Technion and Tel Aviv University and Weizmann In-


[Gebotys:2016:PCP] Catherine H. Gebotys, Brian A. White, and Edgar Mateos. Preaveraging and carry propa-


REFERENCES


Hernandez-Becerril:2016:GIS


He:2013:HEH


Hao:2012:SAM


Hu:2017:ATE


Hwang:2010:RIB

Hsu:2011:NLM


Hore:2012:IED


Hernandez-Castro:2012:MTA


Huang:2014:FOS


Hsu:2011:WLC


Hernandez-Castro:2012:AFH

Julio Cesar Hernandez-Castro, Pedro Peris-Lopez, Masoumeh Safkhani, and Nasour Bagheri. Another fallen hash-based RFID authentication protocol. *Lec-
REFERENCES

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

[HDPC13]

[HEC+12]

Heninger:2012:MYP
Nadia Heninger, Zakir Durumeric, Eric Wus-
trow, and J. Alex Hal-
derman. Mining your Ps and Qs: Detection
of widespread weak keys in network devices. In
????, editor, Proceedings of the 21st USENIX Security
Symposium, August 2012, pages 205–220. USENIX,
Berkeley, CA, USA, 2012. ISBN ???.

[HHDWH12]

[Herranz:2014:ABS]

Hwang:2012:ABA
Jung Yeon Hwang, Sung-wook Eom, Ku-Young
Chang, Pil Joong Lee, and DaeHun Nyang. Anonymity-
based authenticated key agreement with full bind-
ing property. Lecture Notes in Computer Sci-
ence, 7690:177–191, 2012. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-
com/chapter/10.1007/978-3-642-35416-8_13/.

[Hea15]

Nick Heath. Hacking the Nazis: The secret story
of the women who broke Hitler’s codes. TechRe-
public, ??(??):??, March
26, 2015. URL http://
www.techrepublic.com/
article/the-women-who-
helped-crack-nazi-codes-at-bletchley-park/.

[Heath:2015:HNS]
REFERENCES

www.sciencedirect.com/
science/article/pii/S0304397514000772.


REFERENCES

**Han:2011:PEB**


**Harn:2015:DTS**


**Huber:2014:TPW**


**Haitner:2011:PRI**


**Hong:2015:RSM**

REFERENCES


REFERENCES

www.sciencedirect.com/science/article/pii/S0898121212001198

Heyse:2012:LEA


Heil:2014:APH


Holenstein:2011:ERO


Harn:2010:AGK


Hazay:2010:EST


Hsu:2011:NIB

[Chien-Lung Hsu and Han-Yu Lin. New identity-based key-insulated convertible...

Hsieh:2014:AMU


Hmood:2015:ACA


Hu:2012:VMS


Hu:2016:PBR


Huang:2011:ISL

REFERENCES

Huang:2015:MSE

Harn:2011:FDM

Humire:2010:SPR

Herranz:2011:RBS

Huang:2015:CEA

Howard:2010:DSS
Michael Howard, David LeBlanc, and John Viega. 24 deadly sins of software security: programming flaws and how to
REFERENCES

Hohenberger:2012:DDQ


Huang:2014:SWC


Hefeeda:2010:ASM


Herzberg:2012:TJA


Hore:2012:SMR


Hoang:2012:ESB

Viet Tung Hoang, Ben Morris, and Phillip Rogaway. An enciphering scheme based on a


REFERENCES


**Han:2014:GTK**  

**He:2013:GME**  

**Haitner:2010:EIC**  
REFERENCES

Hwang:2011:CD


Homma:2014:TFD


Halevi:2011:TBH


Han:2013:IBD


Han:2014:IBS


Han:2012:PPD


Heather:2014:CPE

James Heather, Steve Schneider, and Vanessa Teague. Cryptographic protocols with everyday objects. Formal Aspects

Shi:2015:CTS

Hamdy:2011:HPB

Henson:2013:MES

Hu:2010:TTW

Huang:2015:PAP

Herbert:2012:SMP


Zhian He, Wai Kit Wong, Ben Kao, David Wai Lok Cheung, Rongbin Li, Siu Ming Yiu, and Eric Lo. SDB: a secure query processing

**Hsu:2014:VWR**


**Huang:2011:GFT**


**Huang:2011:IBS**


**Heys:2011:PSC**


**Han:2012:ERI**


**Han:2014:ERI**

Qi Han, Yinghui Zhang,

Han:2014:ATS


Islam:2015:MBA


Islam:2011:MES


IBM:2013:DMP

enables unlimited analysis of encrypted data. See patent [GH13].


8. ISSN 1063-6889. LCCN QA76.9.C62 S95 2013.

**Imanimehr:2016:HPR**


**Islam:2011:MDA**


**Iyengar:2016:SPS**


**Imai:2015:IRR**


**Islam:2015:LFP**


**Ioannou:2014:PKC**

REFERENCES


[Jie:2010:AAI] Wei Jie, Junaid Arshad, and Pascal Ekin. Authen-

**Jie:2011:RGA**


**[JAS+11]**

**Prins:2011:DCA**


**[JB11]**

**Jho:2016:SSE**


**[JCHS16]**


**[JCM12]**

**Chang:2012:TRR**


**[JEA+15]**

REFERENCES

December 18, 2015. CODEN SACDAF. ISSN 2375-2548. URL http://advances.sciencemag.org/content/1/11/e1500793.


REFERENCES


Jain:2016:APQ


Jiang:2012:DCA


Joye:2012:FAC


Tong:2012:NBD


Jiang:2016:CVI


Juels:2014:INC

Ari Juels and Bonnie Wong. The interplay of neuroscience and cryptog-

[JZS+10]  

[KA17]  

[KAHKB17]  
Kamp:2013:MES


Kamp:2016:MEM


Kapera:2011:SPD


Kapera:2013:MRM


Karafyllidis:2012:QGC


Kong:2015:CSM


Katz:2013:RIB

Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kim:2011:SSE


Koz:2012:ASE


Kraetzer:2012:PCS


Karakoc:2013:BCL

Karakoc:2015:AKA

Keblusek:2015:BRK

Kikuchi:2012:SSN

Khedr:2016:SSH
Alhassan Khedr, Glenn Gulak, and Vinod Vaikuntanathan. SHIELD: Scal

**Kwon:2010:SEB**


**Khazaei:2010:NBS**


**Kastner:2010:AOT**


**Kim:2014:MBM**


**Khalil-Hani:2013:BEB**


**Kim:2016:EPE**

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


Konstantinou:2010:RCI


Kawai:2012:SHS


Kawai:2013:SHS


Khalil:2014:CIM


Khan:2015:CMB


Kim:2012:INS


Keller:2010:DAS


Khomejani:2010:PCT


Koblitz:2010:BNW


Kiani:2011:MPD

Kifer:2014:PFM

Koblitz:2015:RWE

Koblitz:2016:RWE

Kasamatsu:2012:TSE

Kiyoshima:2014:CRB

Karger:2011:LLB

Kanwal:2015:TTM
[Ayesha Kanwal, Rahat Masood, Muhammad Awais Shibli, and Rafia Mumtaz. Taxonomy for trust

Khovratovich:2010:RCA


Khovratovich:2010:RRA


Kumari:2016:APW


Khameane:2016:BBU

REFERENCES

Kollmitzer:2010:AQC


Kang:2012:AKM


Kumar:2017:TAU

Vireshwar Kumar, Jung-Min (Jerry) Park, and Kaigui Bian. Transmitter authentication using hierarchical modulation in dynamic spectrum sharing. *Journal of Network and Computer Applications*, 91(??):52–60, August 1, 2017. CODEN JN-

Kiltz:2011:EH


Khalid:2016:RHL


Kocabas:2012:CPB

Ünal Kocabas, Andreas Peter, Stefan Katzenbeisser,

**Kang:2016:DSA**


**Keskinarkaus:2010:IWD**


**Krenn:2013:CCR**


**Knudsen:2011:BCC**


**Krantz:2012:EAM**


**Kostinger:2012:SBL**

Martin Köstinger, Peter M.
REFERENCES


Kannan:2013:NQF


Krenn:2013:AWI


King:2011:BBB


Kolesnikov:2012:LPP


Kumar:2015:RGB

Sachin Kumar and Ra-

**Kocabas:2016:ESM**


**Kiljan:2017:SAC**


**Kim:2012:SSS**


**Klingler:2013:UPT**


**Kim:2012:SAH**


**Kawachi:2012:SKE**

Akinori Kawachi, Hirotoshi Takebe, and Keisuke...

Kobayashi:2016:ASC


Kupcu:2013:DTT


Kupcu:2015:OAS


Kuznetsov:2011:APP

A. Kuznetsov. Analytic proof of Pecherskii–Rogozin identity and Wiener–Hopf factorization. The-
REFERENCES


Karpovsky:2014:DSS


Kuo:2016:SDD


Koyama:2012:NTD


Kamal:2010:EIN


Kate:2010:PBO


Lu:2010:MSc

REFERENCES


REFERENCES

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


[LCCJ13] Liu:2013:IA Yining Liu, Chi Cheng, Jianyu Cao, and Tao Jiang. An improved authenticated group key transfer proto-


[LC17] Liu:2013:IA Yining Liu, Chi Cheng, Jianyu Cao, and Tao Jiang. An improved authenticated group key transfer proto-


Liu:2016:LCR

Liang:2015:CPA

Lancrenon:2012:IPI

Liu:2017:ECC

Lan:2010:RNG

Li:2012:FDM
Wei Li, Dawu Gu, Zhiqiang Liu, Ya Liu, and Xiaohu Huang. Fault detection of the MacGufin Cipher against differential fault attack. *Lecture Notes in Computer Sci-
Liu:2012:LFA


Labati:2016:BRA


Lopez-Garcia:2014:PBB

Lourdes López-García, Luis J. Domínguez Perez, and Francisco Rodríguez-Henríquez. A pairing-based blind signature e-voting scheme.

Lee:2010:ISC

Donghoon Lee and Seokhie Hong, editors. Information, security and cryptography – ICISC 2009: 12th international conference,
REFERENCES

Lee:2010:CGC

Li:2010:EBB

Lee:2011:PSE

Lin:2011:NIB

Liao:2013:NMS
REFERENCES

**Lenstra:2012:RWW**


**Lum:2016:QEM**


**Lin:2011:ICA**


**Li:2012:BVS**


**Li:2014:SOA**

[LHL⁺14] Jin Li, Xinyi Huang, Jing-wei Li, Xiaofeng Chen, and Yang Xiang. Securely outsourcing attribute-based encryption with checkability. *IEEE Transactions on Parallel and Distributed
Liu:2015:SSP


Lian:2014:SSA


Lin:2015:CND


Liu:2012:ESS


Li:2010:PAP


Lim:2011:NAN

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

Lin:2014:IVW


Litton:2014:TFA


Liu:2015:LBD

Huacui Liu and Chenhui Jin. Lower bounds


REFERENCES


Lee:2016:CAM [LLSW16] Hyung Tae Lee, San Ling, Jae Hong Seo, and Huaxiong Wang. CCA2 attack and modification of Huang et al.’s public key encryption with authorized equal-


[LNY16] Chengzhe Lai, Rongxing Lu, Dong Zheng, Hui

Lambert-Mogiliansky:2012:EIIL


Le:2016:ADS


Liu:2014:SCS


Li:2011:NRA


Lv:2013:NTP

Lukasiewycz:2016:SAO


Li:2013:ESC


Liu:2013:GPB


Liu:2015:SAB


Liu:2013:GPB


Loeb:2015:MGM

REFERENCES


Lima:2010:PKE


Lian:2015:GRG


Liu:2015:GTB


Liu:2016:PPO


REFERENCES


Kaitai Liang, Willy Susilo, Joseph K. Liu, and Duncan S. Wong. Efficient and fully CCA se-


**Lysyanskaya:2010:AEC**


**Lin:2011:CNS**


**Li:2016:LRC**


**Ludge:2012:NLD**


**Lucchese:2010:RPT**

Claudio Lucchese, Michail Vlachos, Deepak Rajan, and Philip S. Yu. Rights
REFERENCES


http://link.springer.com/content/pdf/10.1007/978-3-642-20465-4_30.

[**Lewko:2012:NPM**]


[**Liu:2013:SIP**]


[**Liu:2013:TIE**]


[**Liu:2013:CBS**]


[**Liu:2013:DAB**]


[**Liu:2014:DAF**]

Hongbo Liu, Hui Wang, Yingying Chen, and Dayong Jia. Defending against frequency-based attacks on distributed data storage in wireless networks.
Liu:2017:EEC

Liu:2011:SBA

Lu:2014:HOM

Liu:2010:NDC

Liu:2010:SET


[Li:2012:IIA]


[Li:2014:IBD]


[Li:2014:EMK]


REFERENCES


Liao:2012:NSM


Liao:2010:MPC


Li:2013:SSS


Liu:2012:SOCa


Luo:2012:LVT


Liu:2014:PKE

Shengli Liu, Fangguo Zhang, and Kefei Chen. Public-key encryption scheme with selective opening chosen-ciphertext security

**Liu:2017:ESS**


**Liu:2014:CRA**


**Li:2016:BMA**


**Masdari:2017:STA**

Mohammad Masdari and Saffiyeh Ahmadzadeh. A survey and taxonomy of the authentication schemes


REFERENCES

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

Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP


Maurer:2012:CCN


Mayron:2015:BAM


Mazurczyk:2013:VSD


Milo:2011:FGB

[MBB11] Fabrizio Milo, Massimo Bernaschi, and Mauro

Mao:2015:PUA


Mukhopadhyay:2011:PEA


Madanayake:2012:BPS

McGrayne: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 ???.

Marquez-Corbella:2015:ECP

Mathew:2015:NMB

Majzoub:2012:MRH

Mansouri:2012:ACA
Shohreh Sharif Mansouri and Elena Dubrova. An architectural countermeasure against power analysis attacks for FSR-based
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-29912-4_5/.

**Murdoch:2010:CPB**


**Maachaoui:2012:MLA**


**Meiklejohn:2010:BRB**


**Menn:2013:ESC**


**Meshram:2015:EIB**


**Mandal:2016:DIW**

Kalikinkar Mandal, Xinxin Fan, and Guang Gong.

Moreno:2013:NIP


Moufek:2015:MCB


Marmol:2010:TPA


Matsuda:2014:CCS


Meziani:2012:IPS


Miller:2014:ADS

Andrew Miller, Michael Hicks, Jonathan Katz,
and Elaine Shi. Authent-
icated data structures,
generically. ACM SIG-
PLAN Notices, 49(1):411–
423, January 2014. CO-
DEN SINODQ. ISSN 0362-
1340 (print), 1523-2867
(print), 1558-1160 (elec-
tronic). POPL ’14 confer-
ence proceedings.

Luntian Mou, Tiejun
Huang, Yonghong Tian,
Menglin Jiang, and Wen
Gao. Content-based copy
detection through multi-
omodal feature representa-
tion and temporal pyramid
matching. ACM Transac-
tions on Multimedia Com-
puting, Communications,
and Applications, 10(1):
CODEN ???? ISSN 1551-
6857 (print), 1551-6865
(electronic).

Bassam J. Mohd, Thaier
Hayajneh, and Athana-
sios V. Vasilakos. A sur-
vey on lightweight block ci-
phers for low-resource de-
cives: Comparative study
and open issues. Journal
of Network and Computer
Applications, 58(??):73–93,
December 2015. CODEN
JNCA. ISSN 1084-8045
(print), 1095-8592 (elec-
tronic). URL http://

Daniele Micciancio. A first
glimpse of cryptography’s
Holy Grail. Communications
of the Association for
Computing Machinery, 53
(3):96, March 2010. CO-
DEN CACMA2. ISSN
0001-0782 (print), 1557-
7317 (electronic).

Wil Michiels. Opportunities
in white-box cryptography.
IEEE Security &
Privacy, 8(1):64–67, Jan-
uary/February 2010. ISSN
1540-7993 (print), 1558-
4046 (electronic).

P. Martinez-Julia and A. F.
Gómez-Skarmeta. A novel
identity-based network ar-
chitecture for next genera-
tion Internet. J.UCS:
Journal of Universal Com-
puter Science, 18(12):
1643–??, ???. 2012. CO-
DEN ????. ISSN 0948-
6968. URL http://www.
jucs.org/jucs_18_12/a_novel_identity_based.

Pedro Martinez-Julia and
Antonio F. Skarmeta. Beyond
the separation of iden-
tifier and locator:
Building an identity-based

Mohanty:2011:RTP


Moessner:2012:SAS


Muller:2012:HPC


Mozaffari-Kermani:2017:FD


Malik:2012:AIC

Marconato:2013:VLC


Mozaffari-Kermani:2010:CSI


Montecchi:2012:QSE


Mancillas-Lopez:2010:RHI


Mendez:2016:PES


Manzanares-Lopez:2012:ICU

[MLMSMG12] Pilar Manzanares-Lopez, Josemaria Malgosa-Sanchez, and Juan Pedro Muñoz-Gea. The importance

**Madhusudhan:2012:DIB**


**Meshram:2013:IBC**


**Mait:2014:FIR**


**Mondal:2014:DSM**


**Moldovyan:2012:BBD**

REFERENCES


REFERENCES

Moran:2010:BCP
Tal Moran and Moni Naor. Basing cryptographic protocols on tamper-evident
CODEN TCSDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Mukhopadhyay:2014:EMP
Debapriyay Mukhopadhyay and Subhas C. Nandy. Efﬁcient multiple-precision
integer division algorithm. Information Processing Letters, 114(3):152–157,
March 2014. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Monz:2016:RSS
Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl,
Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, and
(6277):1068–1070, March 4, 2016. ISSN 0036-8075.
URL http://science.sciencemag.org/content/351/6277/1068.

McKusick:2015:DIF
Marshall Kirk McKusick, George V. Neville-Neil, and Robert N. M. Watson. The design and implementation of the FreeBSD operating system. Addison-Wesley,
xxx + 886 pp. LCCN QA76.774.F74 M35 2015.

Minier:2012:RKI
Marine Minier and María Naya-Plasencia. A related key impossible differen-
tial attack against 22 rounds of the lightweight block cipher LBlock. Infor-
mation Processing Letters, 112(16):624–629, August 31, 2012. CODEN IFPLAT.
ISSN 0020-0190 (print), 1872-6119 (electronic).


REFERENCES


[MR10] Aybek Mukhamedov and Mark D. Ryan. Identity escrow protocol and...


Piotr Mroczkowski and Janusz Szmidt. The cube attack on stream cipher Trivium and quadraticity tests. Fundamenta Informaticae, 114(3-4):309–318, August 2012. CODEN FUMAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

REFERENCES


**Morozov:2012:ZKP**


**Malkin:2011:ECS**


**Mu:2010:BRB**


**Murdoch:2016:IDP**


**Miri:2012:SAC**

Ali Miri and Serge Vaudenay, editors. *Selected Areas in Cryptography:*
REFERENCES


REFERENCES


REFERENCES


[NCL13] Liang Ni, Gongliang Chen, and Jianhua Li. Escrowable identity-based authenticated key agreement


[Nes: EIC] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Naglaa F. Soliman, Alaa M. Abbas, Osama S. Faragallah, Noura Semary, Mohiy M. Hadhoud, Saleh A. Alshebeili, and Fathi E. Abd El-Samie. Efficient implementation of chaotic image encryption in trans-

**Nafea:2016:HMB**


**NIST:2012:RRN**


**NIST:2013:CSS**


**Nguyen:2014:DDI**


**Ning:2012:DPB**


**Ning:2015:APB**

REFERENCES

292


REFERENCES

CODEN PPLTEE. ISSN 0129-6264.

Navin:2010:ETU


Novotny:2010:TAE


Nichols:2014:CSS


Nguyen:2011:APB


Nose:2011:SWA


Nose:2014:SWS


**Nguyen:2012:SOU**


**Niu:2015:CRS**


**Naccache:2010:THI**


**Nojoumian:2012:SRS**


**Natarajan:2015:MAD**


**Niksefat:2014:ZPP**

Salman Niksefat, Babak Sadeghiyan, Payman Mohassel, and Saeed Sadeghian. ZIDS: a privacy-preserving

Nandakumar:2017:CAI


Nguyen:2012:LRS


Nguyen:2010:LAS


Nie:2013:CHB


Newell:2014:NCR

Andrew Newell, Hongyi


Rolf Oppliger. Contemporary cryptography.


REFERENCES


Ortiz-Yepes:2014:BSA


Praba:2010:MAC


Pal:2015:SDC


Pal:2016:ACC


Pandey:2014:ACR


Parent:2012:WAI


Park:2012:APO

Pass:2013:USP


[Pas13a]

Pasanata:2013:MDR


[PAS13b]

Paulson:2010:SDO


[Pau10]

Pandit:2012:EFS


[PB12]

Park:2014:FRI


[PBCC14]

Pun:2014:GIT

Chi-Man Pun and Ka-Cheng Choi. Generalized integer transform based reversible watermarking algorithm using efficient location map encoding

[PC14]


March/April 2010. CODEN ????. ISSN 1540-7993 (print), 1558-4046 (electronic).


Papas:2012:MLR


Park:2010:SIC


Pieprzyk:2010:TCC


Pointcheval:2012:ACE


Pedro Peris-Lopez, Enrique San Millán, Jan


**Paar:2010:UCT**


**Papadopoulos:2010:TRM**


**Park:2011:ACC**


**Pereira:2016:SHB**


**Pendl:2012:ECC**


**Pyun:2012:IBF**

Young June Pyun, Younghee Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing interactive traffic. *Computer Networks (Amster-
REFERENCES

Pathak:2012:PPS


Phan:2012:DDB


Phan:2012:MBT


Papadopoulos:2015:PAP


Pandey:2012:PPS


Piret:2012:PBC

Gilles Piret, Thomas Rocher, and Claude Carlet. PI-
REFERENCES


**Popa:2012:CPQ**


**Priemuth-Schmid:2012:ASV**


**Permpoonpatalarp:2014:FTG**


**Perazzo:2015:DRL**


**Pereira:2013:SLC**

REFERENCES

Phatak:2013:SIN


Patranabis:2017:PSK


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC


Papakostas:2014:MBL

references


Kanthakumar Pongaliur and Li Xiao. Sensor node source privacy and packet recovery under eavesdropping and node compromise attacks. ACM Transactions on Sensor Networks, 9(4):50:1–50:??, July 2013. CODEN ????. ISSN 1550-
Philippaerts:2013:CMC


Pei:2015:SWT


Papadopoulos:2010:CAR


Qin:2016:VTQ


Qu:2013:DPA


Saiyu Qi, Yuanqing Zheng, Mo Li, Yunhao Liu, and Jinli Qiu. Scalable industry data access control in RFID-enabled sup-

Qi:2016:SPR


Qi:2016:SPR

Rabin:2010:ACC


Rankin:2010:HLH


Rao:2010:PAA


Rao:2017:SEC

REFERENCES

Rauscher:2015:FMT

Ruoti:2015:WJS

Rupp:2015:CTM

Radke:2015:CFA

Rabbachin:2015:WNI

Rao:2017:CFA
REFERENCES


Ren:2016:IBE

Reardon:2016:SDD

Reeve:2015:ARC


Ren:2010:CSH

Roh:2010:BSW

Robert-Inacio:2011:SAP
REFERENCES

[Rjasko:2012:BBP]

[Regev:2011:QOW]
Oded Regev and Bo’az Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In ACM [ACM11], pages 31–40. ISBN ????? LCCN ????? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

[Rogaway:2016:POP]

[Rose:2011:KBT]

[Rao:2012:SSA]

[Rifa-Pous:2012:AHD]
Helena Rifa-Pous and Carles Garrigues. Authenticating hard decision sens-
REFERENCES


[RPSL10] Rhee:2010:TSS


REFERENCES


REFERENCES


Saeed:2016:IID

Saleh:2016:PED

Sarier:2012:SNB

Sarkar:2010:SGC

Sarkar:2011:TES
Sarkar:2014:PEK


Sasaki:2012:DSW


Savage:2013:NSL


Savage:2013:PP


Savage:2015:NVS


Savage:2016:NKP


Stevens:2017:AFS

REFERENCES


Schnoor:2012:DES

Schneier:2013:HDD

Schaefer:2015:BRB
REFERENCES


REFERENCES

330


References


REFERENCES


REFERENCES


Shu:2014:DAS

Saxena:2016:API

Sanchez-Garcia:2016:SSA

Sun:2015:FSW

Susilo:2016:EDT

Shankar:2012:BDF
Deepa D. Shankar, T. Gireeshkumar, K. Praveen, R. Jithin,
REFERENCES


[SH15] Song:2015:ADT

REFERENCES

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

**Shen:2014:LES**


**Shim:2011:SA**


**Shparlinski:2010:NWP**


**Suoranasta:2012:ASM**


**Shyu:2015:VCR**


**Satir:2012:CBT**

Siad:2012:NAP


Simion:2015:RST


Sirer:2016:TPS


Shakeri:2012:RZW


Sabri:2011:AFS


Sachnev:2012:IME

REFERENCES


REFERENCES


REFERENCES


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


REFERENCES

[Smith:2015:HHB]

[Swierczynski:2015:PSE]

[Safavi-Naini:2011:USC]
Seyedzadeh:2014:RCI


Suriadi:2012:PCV


Schaumont:2015:IEP


Suresh:2015:AGU


Serwadda:2013:ELK


Shiaeles:2015:FII


Siraj A. Shaikh and


N. Saxena and C. Se-

[Saxena:2012:BIT]

[Shparlinski:2012:CSD]

[Sendrier:2013:HCE]
Sadhy:2017:PRE


Singh:2013:QBF


Smith:2011:SMC


Sood:2011:SDI

Sandeep K. Sood, Anil K. Sarje, and Kuldip Singh. A secure dynamic identity based authentication protocol for multi-server arch-
REFERENCES

Stallings:2011:CNS

Sahai:2012:DCC

Shen:2016:RMM

Schaer:2012:EI

Schillewaert:2014:CCA

Spiez:2012:RCT

Spiez:2012:RCT

Sahai:2012:DCC

Shen:2016:RMM

Schaer:2012:EI

Stallings:2011:CNS

Schaer:2012:EI

Sahai:2012:DCC

Shen:2016:RMM

Schaer:2012:EI
REFERENCES


REFERENCES


Stolte:2012:EDA


Suciu:2012:SED


Sung:2011:DCE


Sun:2016:NEB


Shen:2015:CSC


Song:2016:IAR


REFERENCES

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


[Tamayo:2015:AFH]

[Tan:2012:SLM]

[Tan:2012:LCP]

[Tang:2015:ETE]

[Tang:2015:HAC]

[Tarnovsky:2010:DSP]
REFERENCES


Theofanos:2016:SUE


Tian:2016:IBS


Tian:2015:IBP


Tu:2014:EPB


TERROVITIS: 2012: PPD


TOMB: 2016: AVR


TANG: 2014: PAB

REFERENCES

Taylor:2011:CAS


Tezcan:2016:IID


Tao:2014:CFS


Tang:2011:IDC


Tso:2013:SAI


Tseng:2012:ERI


[TRD11]

[TSLL11]

[Tso13]

[TSH14]
 REFERENCES


Tartary:2011:EIT


Tian:2012:SSB


Tan:2016:CCA


Tolba:2016:GMA


Trammel:2012:DTP


Unruh:2015:RQT
Ulutas:2011:MIS


Ulutas:2013:ISI


Vaikuntanathan:2011:CBN


Vaikuntanathan:2012:HCE


Valamehr:2012:IRM


Vatajelu:2016:SMB


vanDam:2011:TQC

Wim van Dam, Vivian M.

Visegrady:2014:SCV


VenafiLabs:2014:VLQ


Vetter:2010:ABV


Venkatkrishnan:2017:DRB


Vernize:2015:MNI


Viennot:2014:MSG

REFERENCES

221–233, June 2014. CODEN ????. ISSN 0163-5999 (print), 1557-9484 (electronic).


Vollala:2017:EEM


VonMaurich:2015:IQM


Vassilev:2016:ESU


Vivek:2012:CSE


Vlachos:2015:DPC


vanTilborg:2011:ECS

REFERENCES

Vuagnoux:2010:CA


Wagstaff:2010:C


Wagner:2016:TPF


Wang:2010:NSB


Wang:2013:CRA


Wang:2014:IIA

REFERENCES

Ward:2011:CCM


Watt:2010:IPI


Waters:2012:FER


Wang:2012:PCE


Wright:2010:USP


Wei:2012:NTB


[Wang:2012:SPB]


[Wei:2012:NCI]


[Wei:2016:PAB]


[Wu:2012:DAA]


[BBG+17]
Wang:2012:MCE


Wei:2012:IRK

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

Wang:2011:RBM


Wang:2013:HCL


Wei:2015:FST


Wu:2015:TRM


Xiaotian Wu, Duanhao Ou, Qiming Liang, and Wei Sun. A user-friendly secret image sharing scheme with reversible steganography based on cellular


[Williams:2013:APC] Peter Williams and Radu Sion. Access privacy and

**Whitworth:2014:SPC**


**Wang:2015:RSA**


**Watanabe:2012:ITT**


**Wang:2012:PAC**


**Wu:2010:EUA**


**Wu:2010:IBM**

Tsu-Yang Wu and Yuh-Min Tseng. An ID-based mutual authentication and


Wang:2014:ATF


Wen:2014:MZC


Wang:2011:MMW


Weng:2012:NCC


Werner:2017:CIM


[Wang:2011:CIB]


[Wang:2016:SHI]


[Wu:2017:EAK]


[Wang:2017:SRS]

REFERENCES

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

Weir:2012:AVC

Wang:2014:NAI

Weir:2012:IHV

Wang:2013:NSW

Wei:2014:IDC

Wei:2016:APS
Wang:2013:BSB


Wang:2014:CGR


Wen:2011:DSH


Wei:2015:CPK


Weng:2013:VWI


Wei:2012:CSO

See [WZM12b].


[XHCH14] Li Xu, Yuan He, Xiaofeng Wang:2012:NIS


[XHCH14] Li Xu, Yuan He, Xiaofeng


Xu:2016:CIB


Xu:2013:PKE


Xue:2013:TCB


Xie:2013:ECP

X. Xie, H. Ma, J. Li, and X. Chen. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing. *J.UCS: Journal of Universal Com-

---

REFERENCES

(print), 1550-4867 (electronic).

Xiang:2016:EMP


Xue:2013:TCB
REFERENCES


[XWS17] See comments [XWS17].

Xia:2016:SDM

Xie:2014:SCP

Xiao:2016:REM

Xiong:2015:SRE

Xie:2012:DPK


REFERENCES


Yang:2011:PQC


Yang:2011:GSS


Yang:2012:PST


Yang:2016:EBB


Yuan:2013:PVQ

Lihua Yuan, Chao-Chih Chen, Prasant Mohapatra, Chen-Nee Chuah, and Krishna Kant. A proxy view of quality of Domain Name Service, poisoning attacks and survival strategies. ACM Trans-
REFERENCES


[Yan:2016:DEB] Zheng Yan, Wenxiu Ding,

**Ye:2010:ACC**


**Yamada:2012:PBR**


**Ye:2014:NIE**


CO DEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

**Yekhanin:2010:LDC**


**Yoshida:2012:OGT**


**Yu:2012:EPF**

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


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


**Yi:2013:ETS**  

**Yu:2016:CBE**  

**Yagan:2016:WSN**  

**Ying:2013:PPB**  

**Yu:2010:PSI**  

**Yu:2011:CLE**  
Yong Yu, Yi Mu, Guilin Wang, and Ying Sun. Cryptanalysis of an offline electronic cash scheme...


Yoneyama:2012:ORA


Yang:2017:SAS


Yang:2012:EMA


Yengisetty:2011:AVC


Yi:2016:IPA


Yang:2012:SAK

REFERENCES


**Yumbul:2015:EEP**


**Yang:2015:EPS**


**Yang:2016:ECV**


**Yao:2014:NCR**


**Yeh:2010:TRR**


**Yuen:2014:TCT**

REFERENCES

Ylonen:2014:SAA


Yang:2011:CCK


Yang:2011:CPK


Yamada:2012:UEW


Yang:2014:IBI


Yang:2011:ACD


Yasuda:2012:ASM

Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Saku-

**Yao:2010:IDA**


**Yang:2015:RCI**


**Wang:2011:RDA**


**Wang:2013:RBC**

Yu:2012:NWM

Yu:2012:SME

Yu:2016:CDI

Yang:2010:CRS

Yesilyurt:2015:RWM
Murat Yesilyurt, Yildiray Yalman, and A. Turan Ozcerit. A robust water- marking method for MPEG-4 based on kurtosis. The Computer
Yang:2013:ECS


Yang:2016:EPA


Yang:2012:LUC


Yang:2012:BPN


Yang:2012:NIB

Geng Yang, Qiang Zhou, Xiaolong Xu, Jian Xu, and Chunming Rong. A novel identity-based key management and encryption scheme for distributed system. Lecture Notes in Computer Science, 7672:
REFERENCES


Yang:2014:PST


Zhu:2012:JLS


Zhang:2011:TNT


Zhang:2013:RMS


Zhang:2015:PCL


Zhu:2012:TCS

Zhifang Zhang, Yeow Meng

Zhang:2014:GCS

Zhang:2015:IAI

Zetter:2014:CZD
Zhao:2010:PSA


Zhou:2016:HFD


Gao:2012:DES


Zadeh:2015:ASP


Zhang:2012:LDC


Zhang:2015:STR


Zhu:2015:IDM

Hui Zhu, Cheng Huang,


**Zhang:2015:RBA**  


**Zhang:2012:CCB**  


**Zhang:2016:TLT**  


**Zhang:2017:FGA**  

Zhang:2010:NSS


Zielinska:2014:TS


Zhang:2016:CAH


Zafar:2010:GRN


Zavattoni:2015:SIA


Zheng:2016:EUV

Zhao:2012:SSS


Zenger:2016:AKE


Zmudzinski:2012:WEU


Zhao:2012:SSM

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

**Zhang:2012:EHO**


**Zhang:2014:NCM**


**Zhu:2015:PPD**


**Zwattendorfer:2012:CBL**


**Zhang:2016:EEA**

Zhou:2016:SRB


Zhang:2015:FAA


Zhang:2014:LFL


Zhang:2011:AGK


Zilberberg:2013:PCM


Zhang:2015:FER

[ZWTF15] Mingwu Zhang, Chunzhi Wang, Tsuyoshi Tak-


Jun Zhang, Yang Xiang, Wanlei Zhou, Lei Ye, and Yi Mu. Secure image retrieval based on visual content and watermarking protocol. *The Computer*
REFERENCES


Zheng:2010:PS


Zhang:2011:EPK


Zhao:2012:FCS


Zhang:2013:BLR


**Zheng:2015:EPT**


**Zhuang:2014:SCA**