Title word cross-reference

#1 [Man01, RSA02]. #10 [RSA00b]. #11 [RSA01, Clu03]. #13 [RSA03b]. #15 [RSA00d, RSA00c]. #9 [RSA00e].

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p_k) [BINP03]. (t, n)

[CHY05a, HL05c, Kog02, LZL+01, YCH04].

(tn) [PW05, SC05a]. + [Abe01]. {0, 1}

[LBGZ01, LBGZ02]. 1 [Wu02]. $125$

[And04]. 128 [AIK+01, PGC01]. 13

[HSL+02]. $15.00$ [Imr03]. 2

[Bih00, BGN05, CY02, CKL+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 ± 10

[Mau01]. 2^{28} [Bih02]. 2^k [MFFT05]. 2^m

[ABCD02, KKY02]. 3 [BP04, Ben00, ChLYL09, CT09, Lav09, OMT02, WH09, ZTP05].

$35.00$ [Top02]. $49.99$ [Gum04]. $5$

[SCF01]. 5 [Pat04]. $51.48$ [Pap05]. 512

[CDL+00]. 7 [Gri01, Pat03a], (2,128) [WB02].

[AIK04]. ABC [PS04b]. d [BD00b]. E_0

[FL01a]. f_8 [KSHY01]. g^{2^2} [Shp02]. g_e(x, 1)

[SZP02]. GF(2) [CP03]. GF(2^m)

[OTIT01, RMPJ08]. GF(p^m) [BGK+03].

GF(p)[PZ01]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. l [QPV05]. M + 1

[AS01a]. F_q [CY02]. Z_n [Gro06]. GF(2)

[GS03, KTT07]. GF(2^m)

[BBGM08, KTT07, KW06, RMH03a, RS04].

GF(2^n) [KKH03]. SL_2(F_{2^m}) [SGGB00]. µ

[LN04]. n

[CT08b, Gon06, HKS00, LKJL01, TM01]. N^{0.292} [BD00b]. NC^0 [AIK06]. p [FL06].
\( p^q \) [LKYL00]. \( p^r \) [CHH01]. \( Q \) [Yas08]. \( r \) [JY01]. \( w \) [DwWmW05, OT03b]. \( x^v \) [Gon06]. \( y \) [OS01].

-Adic [GHK+06]. -Bit [AIK+01, CDL+00, PCG01]. -Connected [BJLS02]. -Coordinate [OS01]. -coverings [SC02b]. -decompositions [vDKST06]. -DNF [BGN05]. -Metric [LBGZ01, LBGZ02]. -NNAF [DwWmW05]. -out-of [CT08b]. -Polynomials [FL06, CHH01]. -Round [BP04, Bih00, GIKR02, CKL+03]. -Source [KLR09]. -st [AS01a]. -Steiner [WL02]. -Threshold [Kog02]. -way [LKJL01].

-.NET [For04, TG04].

/dev/random [BH05]. /evolution [Pat02a]. /MOM [DJLT01].

0 [And04, BC04a, Gum04, Imr03, Puz04, WYY05d]. 0-07-222742-7 [Gum04]. 0-13-100851-X [For04]. 0-226-74410-8 [Top02]. 0-262-14075-6 [Pag03]. 0-321-20217-1 [Puz04]. 0-385-49532-3 [Imr03]. 0-470-84402-7 [And04]. 024-Bit [GOS7a]. '05 [ACM05c, MS05b, ZC09]. '07 [ACM07]. '08 [ACM08]. '09 [ACM09, IEE09a]. 1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05b, WYY05c, Was08a]. 1-58488-518-1 [Was08a]. 1-Connected [BJLS02]. 1-out-of-n [AOS02]. 1.82GBits [KV01]. 1.82GBits/sec [KV01]. 101 [Sei00a]. 10118-3 [ISO04]. 106 [Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a]. 109-bit [Pri00]. 10th [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. 11-15 [AUW01]. 11th [CCMR05, HYZ05b, HH04, HH05, RM04, Roy05, USE02b]. 12 [TPS01]. 128 [JJ02a, WFLY04]. 128-Bit [SM03b]. 12th [GH05, MS05b, PT06]. 13-15 [ACM05b]. 130 [LM08]. 14th [AMW07, AAC+01, Bir07]. 155 [LMP+01]. 15th [MJ04, BC01]. 160 [KF00]. 16th [BS03]. 17th [IEE05b]. 186 [Dat00]. 186-2 [Dat00]. 18th [KM07]. 19005-1 [ISO05]. 192-bit [Luc00]. 1962 [AJ08]. 1987 [Kha05]. 1993 [PPV96]. 1999 [Lee03b, Uni00a, Uni00b, Uni00f, Uni00c, Uni00d, Uni00g, Uni00h, Uni01]. 19th [BCDH09]. 1V [CGBS01].

2 [Dat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH+00b, Eko02, Irw03, KH08, KI01a, Sch00b, Wit01, YG01c]. 2001 [ACM01a, BC01, GJSS01, Lee03a]. 2002 [B+02, IEE02, RSA03a, Yun02a]. 2003 [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, WKP03]. 2004 [ACM04b, ZC04]. 2005 [ACM05a, ACM05b, ACM05c, ANS05, HYZ05b, ISO05, Roy05, Ter08, Ytr06]. 2006 [ACM06]. 2007 [ACM07, Ano06a, SM07]. 2008 [ACM08, Dew08, YRS+09]. 2009 [ACM09, May09]. 20th [Bel00]. 21 [AJ01b]. 21264 [WB00]. 21st [Jef08, Kii01]. 21th [IEE09a]. 22 [TTZ01]. 22nd [Yun02a]. 23rd [Bon03]. 24th [Cra05a, Fra04]. 256-bit [Luc00]. 25th [Sho05a]. 26 [DB04]. 26th [EBC+00]. 27th [Men07]. 29. [Eke02]. 29th [FLA+03].

3 [Duw03, Imr03]. 3-515-07640-9 [Eag05]. 3-540-66778-4 [Duw03]. 3-Key [Kel05]. 3.0 [Flu02b, Hei01, SQ01]. 305 [ECM00a]. 306 [ECM00b]. 30th [Coc02a]. 314pp [Duw03]. 3278 [BWBL02]. 33rd [ACM01a]. 36th [ACM04b]. 37th [ACM05c]. 39th [ACM07]. 3D [LZP+04]. 3GPP [KSHY01, SM02]. 3rd [ACM05a, USE00a].

4 [Duw03]. 4-round [DLP+09]. 40th [ACM08]. 41st [IEE00a]. 42nd [IEE01a]. 43rd [IEE02]. 44th [IEE03]. 45th [IEE04].
Addison [Puc03]. Addition [KT00, LPZ06, PP06a]. Additive [FMY01, MF01]. Additive-Sharing [FMY01]. Address [IIT03, Nik02a, Nik02b, FXAM04, RW07]. Address-Bit [IIT03]. Addressing [HTW07]. Adjacent [JT01b]. Adjustment [BSNO00]. Adlan [MAaTxx]. Adleman [BB79, Coc03, SP79]. Administration [USE00c, USE00a, Ris06, WL04a]. Administrative [Cra05b]. Admitting [HSZI00]. Advance [CZB+01]. Advanced [DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Swe08, Tan01, Bar00c, III00, Burr03, CMR06, Coc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Han00, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, WBRF00, YW06]. Advances [Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPST07, ELvS01, Kil01a, Ok000, Pi001, Pre00, TIS07, Yun02a, Kat01, Bii03, CC04a, Cra05a, Fra04, Kno02, La03, Lee04b, LTb04, Li05, LST+05, Men07, Roy05, Sh00a, Zhe02b]. Advantage [SZ01]. advantages [CDS07]. adventures [Hro09]. Adversarial [CLR09, GSS08, NS08]. Adversarial-knowledge [CLR09]. Adversaries [CM00, JQY01, KR02, Lu02, SK05, SKR02, GXT+08, ZD05]. Adversary [Aba00, Gor06, RW02]. AES [CGH+00b, DRS05, FIP01a, Pha04, AG01, AL00b, BDG+09, CG03, Coc02b, DR00b, DR02a, DR02b, DLP+09, DFR01, Dan01, Dra00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, IK00, IK01, Joh00, KS09, Ke05, KFSS00, KV01, LP02a, Len01, MHH+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03, RR00, SKKS00, SM03b, Sch00b, SKW+00, SW00a, SL00, WW00, WB00, WOL01, WWGP00, WWCW00]. AES-CBC [Fer06]. AES-like [DLP+09]. AES-related [Sch00b]. Affine [Ben00, CT09, Fe06]. Affine-Transformation-Invariant [CT09]. AFIS [Zir07]. after [Ber03, McL06]. again [Fox00]. Against [CS05a, DM07b, FKSW00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, Av03, Bau05, BPR00, BP02, BBN+09, BB+02, BCP02b, CM00, CS03b, DB04, Des00b, Des00c, Egl00, EBS01, FP01, Fry00, Geb04, HNZI02, HLL+01, HG07, Hsu05b, HLC08, Ino05, ISW03, IIT03, JKS02, JJ00b, JT01a, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, Mit00, Möll02, MG08, NRR00, NLD08, OK05, OS00, OT03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PQ03, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sh000b, SKU+00, SKI01, SLL+00, Tad02, TV03, VHP01, XH05, YJ00, YKLM02a, YKLM02b, YKLM03, ZS01]. Age [Mar08b, Lev01]. Agency [Aja08, Bam02]. Agent [HQ05, KC02, PDJ09, Rs01, RC01, Rot01, ZYM05, KXD00, SSM+08, SH00]. Agent-Based [HQ05, SSM+08]. Agents [WHI01, Haut06, LSA+07]. Ages [Eag05, Kin01]. Aggregate [BGL03, WK05]. Aggregated [ZSN05]. Aggregation [Her06, CCMT09, MS09b]. Aggressive [Wyl05]. AGM [Gau02]. Agreement [AAFG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB+04, AKNRT04, CYY05, Che04a, CY05, CJ04, CJL05, HWWM03, KPT04, KRY05, KKH05, LKK03a, LKK03b, LQ04a, LLL04, LL05a, LKY05b, LKY05c, LKY05d, LLR02, Shi05, SW05, SC05b, Ts06, Tse07, VY05, YW05, YS02, YR04, YRY05b, ZC04, LLR06]. agricultural [Lov01]. Aided [NS01b, HLL+02]. Aim [Pau02a]. Aimed [SFD06]. Airport [Sas07]. Ajtai [GK05]. AKS [Che03]. Al [MA00a, Hwa05, Irw03, KJ05]. MAaT05, MAaT07, PKH05, XY04.
annoyances [Tyn05]. annoying [Tyn05].
Annual [ACM01a, ACM02, ACM04b, ACM05c, ACM06, ACM07, ACM08, Bon03, Cra05a, ELvs01, Fra04, IEE00, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Kil01a, MZ04, Men07, Sho05a, USE01b, USE01a, USE02c, VY01, Yun02a, ACM00, Bel00, HA00, Jef08, NH03, ST01d].
anomaly [RCG+05]. Anonymity [GM03, IKOS06, MP02, SS01b, EY09, LV07, Par04].
anonymization [FXAM04, RW07].
Anonymous [ABC+05, CL02a, CL04a, HSHI02, HSHI06, KT01, HLL+08, SOO102, Wan04a, YT09, ZJ09, BP03a, EY09, LHC08, Sae02, Shao3c, WCJ05, YTW05, ZC09].
ANSI [II100, Ke105, Oiw09]. ANSI-C [Oiw09]. Answers [PT08]. Anthony [Pag03].
Anti [Kha05, Ano05b]. Anti-Circumvention [Kha05]. anti-virus [Ano05b].
anticipation [Goo00]. Any [Fis01b, HNO+09, CDM00, DFM04, DMS00, HR07, Poi00]. Anyone [Ros07]. Anytime [DJLT01].
Anywhere [DJLT01]. Apache [Had00]. API [MWM01, Mor03]. APIs [BM01c].
Appendix [Ke105]. Applet [ZFK04]. applets [Bis03a]. Applicability [Wya02, TM01].
Application [AD109, ACS02, Bai01b, Boy01, CL02a, CKQ03, Dam07, Dhe03, GKH+06, HF00, IKP+07, JX05, Jou04, Lai03, Lee04b, LSL05b, LXM+05, NP07, Oka00, Pbh01, PQ03, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TWNA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG09, CMK00, CP07, DIM08, FP00, JRS09, Lax09, MT07, MPH06, MK05a, RSS04, SSST06, TC00].
Application-Aware [IKP+07].
Applications [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, BJ05a, BGK+03, BSS02, Bih03, BG0Y08, BSS02, BL08, CC04a, CD00, CV02, CGHG01, CZ05, CHSS02, CS09, Cra05a, CDM01, DJ02, DK07, DA03, DFP06, FR02, GSS08, GKK+09, GJRK03, Gen04a, GRW06, G0L01a, G0L04, HRS02, H060, Has01a, HSS04, HR05, HJW05, JTO1b, JY01, KMM+06, KGL04, KMO01, KBM09, KKIM01, Knm02, MM07b, Nie02c, Nie02d, PS02h, RSN+01, Sch06b, Shp03, SXY01, SPGQ06, Vau02, Wya02, XYL09, YZ00, Zea0a, Zho02, ACTZ05, Ate04, AH05, AFH06, BG08, BGL+03, CCCC01, CM05b, CS09, CHK+08, DYO09, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gale02, GVC+08, GKK+07, GB09, HHSS01, Has02, Hen01, HKPR05, Jac00, KV+09, KNS05, La00, Lee04a, LJ05a]. applications [LPW06, LB05, MY01, Ma106, MC04, MSV04, Nie04, PW08, PBD07, PC00, Q0S00, Ros06b, SS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPH06, WW08, WA06, WV00, YS04, ZBP05]. Applied [HW03a, HWR09, SL07, GV09, GNP05, IKY05, JYZ04, ZHY03]. Applying [Elb09, KC02, Lan00d, LMSV07, SQ01, SPM002, vDKST06]. Appointed [CL01a]. apprehension [AJ08]. Approach [BKM07, CGFSHG09, CDR01, CW09, CB01, DJLT01, Kra03, Lai07, LL05c, Lh03, OMT02, PBD00, Pan02a, Pre02a, SKG09, VH09, VVS01, Vir03, XYL09, YKMB08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLM05, GGH+08, Har05a, JI01, JW01, LYO02, MT09, Mar05b, MI09, Mos06, NN03, SL0P7, SN04, SW00b, ZLX09, ZS01, ZL04b, ZL04a]. Approaches [CGMM02, AvdH00, DG05, Has01b, KXD00].
approval [Wan04b]. Approximation [CLZ02, Kuk01, WL02]. Approximations [BDQ04]. Apress [Ter08]. April [Ano00b, Buc00a, Chr00, Chr01, CC0M02, CF05, CGH+00b, DFP06, Joy03b, Knm02, Mat02, NIS00, Nac01, Sch01d, SM+09, YDKM06]. APSS [ZSV05]. Arabic [MAdTxx].
Arbitrarily [RW03b]. Arbitrary [AR01, BR00b, BR01, CKN00, CHJ+01b, CF02]. Arbitrary-Length [AR01, BR00b, CKN00, CHJ+01b].
Architectural [ASK07, ABM00, BMA00a, BMA00b, BMA00c, CW02, Gro03, KV01, LTM+00, ZYL05, Ano05b]. Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LKM+00, LTM+00, ZYLG05, Ano05b]. Architectures [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LKM+00, LTM+00, ZYLG05, Ano05b].

Archival [SGMV09]. Archives [RC01]. Archiving [DMSW09]. area [BP03a, Caio04]. Areas [HH04, MZ04, PT06, VY01, AMW07, Buc00a, HH05, HA00, NH03, ST01d]. Aren’t [Bau01a, Bau01b]. Arguments [HNO+09]. ARITH [BS03, BC01, IEE05b]. ARITH-15 [BC01]. ARITH-16 [BS03]. ARITH-17 [IEE05b].

Arithmetic [BS03, BCDH09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDJ+01, SR06, GFS05, P004a, SOIG07].

Arithmetics [Lam91]. ARM7 [DV08, XB01]. Army [Boy03]. Arne [Bec02]. area [DZL01]. Arrays [ABM08, BS00a, GC01a, HIV05, P006a]. Arrived [Law05]. arsenal [Blu09]. Art [And07, Bis03b, Col03, Mar05a, MZ02, CS07a, DSM07, Eri03, Eri08, MS024].

Article [Che08b]. Artifacts [EHK+03]. Artificial [Cop04b, MMYH02]. Arun [For04]. ASCII [MJ001]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DN00b, Ki01a]. ASIC [WOL01].

ASIP [SKW+07]. ASM [MK05a]. Aspect [Kos01a]. Aspects [BLMS00, CMR06, Pel06, DL09+09, Rup09].

Aspiration [Ash03]. assembly [Gon09]. assessing [CDD+05]. assessment [CC05e, DMS07]. assets [KH03, NRR00]. Assignment [BRTM09, CHC04, DF04, Hwa00, TP07, WC01b, hY08]. assignments [SWR05]. Assisted [ECG+07, XSO3, BB05, LHL04]. ASSL [VI09]. associated [XLMS06]. associativity [HRS08]. Assumptions [CS00, DN00a, FOPS01, KZ03, ZD05].

Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT+00, Nao03, SB02, Mic02a]. Assurance [LXM+05, AL04, BJ02, FOP06, Gha07, Jen09]. Assurances [Bar06b].

Astrology [Pag03]. Astronomy [MYC01]. Asymmetric [CH07b, Man01, SY01a, SBB02, WHI01, YG01a, Lee01, OP01b]. Asymptotically [vDW04].

Asynchronous [CKPS01, FML+03, KSR02, SKR02, ZSV05]. at-targama [MAt05]. Atlanta [IEE09b].

ATM [Pat02a, Pat02b, ZEA00]. Atomic [CNV06]. Attached [RCBL00]. Attachments [Ric07]. Attack [Ahm08, CKQ03, CS05a, CS03b, Des00b, F000, FV03, GJH00, GJH01, HQ01, Hug02, HW01, J00b, KCP01, KS00a, KML+02, KM01c, LY07, LNL+08, LV04, LM05, Luc02a, Man01, MHR04, MSU05, Nov01, OM09, PV06a, PQ03, RMS05, SGM09, Sch01b, Sho08, Sma03b, VHP01, YKLM02a, ZC04, ASK05, DKL+00a, Duj08, Duj09, GM00a, HAU04, Hes04b, HG07, Iwa08, J02a, KS09, KM04a, LM08, Law09b, LS05b, MIR05, OS00, SIR04, XH05].

Attack-Resistant [LNL+08]. attacker [BDSV08]. Attackers [JMV02]. Attacking [FMP03, KPR03, Luc00, TMM05, BF06a].

Attacking-Based [TMM05]. Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, BM00, BDK+09, BU02, BM03b, BCP02b, BM01c, Can006b, CS07b, CT08a, CJS01, CKM00, CJNP00, CM03, Con03, CWR09, CD01b, DPH01, DFS04, D08, DM07b, FKS00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gil06, G02, HSH+08a, HD02, HR04a, HSH+01, HLC08, ISW03, JKS02, J00d, KKS00a, KS00b, KKS01, KCJ+01, KL01a, Law09a,
LLS05a, LWS05, LJ05b, MOP06, MP06, MF01, Mes00, Mes01, Mö102, MG08, OT03a, OT03b, [OOP03, OST05, Ove06, PKBD01, PDM09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZZ05, YYDO01, YY01, YG01b, vW01, Bau05, BZ03, CKL09, DK08, Geb04, HSH08b, HSH09, Has01b, Hsu05b, HL05b, Ino05, IM06, JDD01, KS05a, KTC03, LPV09, LSH00, MMJ05, NS05a, NLD08].

attacks

[OST06, RG05, Sch00c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07, WL04b, Yan07, YS02, ZSJN07].

attractors

[HHYW07].

Attribute

[LY05, RSA00e, IY05].

Attributes

[SS01b].

Auction

[AS01a, Ano01a].

Auctioning

[RCG05].

Auctions

[Bra01b].

Audio

[Arn01, CS05b, MH05, WNY09, WWL02, XFZ01, WNQ08, BS01b, KJR05, KN03].

Audio-and

[BS01b, KN03].

Augmented

[CS07c, You01].

Augmenting

[AL04].

August

[AMW07, Bel00, B+02, Bon03, Fra04, HH04, HN05, HA00, JQ04, KKP02, Ki01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch04b, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a].

Austria

[Boy01, IZ00].

Authentication

[Sch04c, Sch05b, Sci00b, SY01b, SBG02, Smi01c, Smi02, SE09, SK06, Str01b, SJ05, SYLC05, SC01, TK03, TST09a, TST09b, Tsa01, VN04, WLLL09, Way01, Way02a, Wea06, WKB08, WT02, WS03, WLT05b, XYL09, Y101, YEP06, YSR01, YLLL02, YKW01, ZJ04, ZBLvB05, AvdH00, AF04a, All06, AAKD09, AL04, Bel04, BGP02, BFG04, BFG05, BS01b, BBG02, BDPF02, Cer04a, CC01, CCK04a, CLO4d, CC04b, CCK04b, CC05c, CY05, CCS08, CWJT01, CJT01, CJ03b, CH07a, CL09, Coc01a, CMD06, DAI01, DY09a, DG05, DW05, FGM03, GAN08, GLC04, GS09, GUQ01, HM02a, Hsu05b, HSY03, HLL04, HL05b, KLY03, KJY05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LLH02,
Miy01, MGC02, Mü101a, MSU05, NMO05, Nak01, Nam02, NBD01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP06a, Rif02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sa105b, Sch01a, SSFC09, Sha02, Sha01e, SOO01, SXY01, Sma03a, SBEW01, SGB01, TMM01, TYLY01, TZT09a, TZT09b, VMSV05, Vau05b, Ver06a, VHP01, VK07, WRW02, WY02, WZW05, WG05, WH09, WBD01, XYL09, YKM01, YT09, YPD01, YSS01, YKW01, YLH05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWCY02, vDW04, App05, AAKD09, BGB09, BR04, BFG08, BS01b, Bla01b, BMW05, BL06, BGL03, BDS09b, Buh06, CGHG06, CL02b, CL04d, CL00, CCH04, CY05, Che05a, CCS08, CGL08a, CGL08b, CGL08c, CJT01, CL09, CJL05, Cho08b, CYH07, CFVZ06, CCD04, CTT07, CHT02, CC04c, Cra05b, DPT02.

Based [DHL06, DV08, DW01, EHKH04, FXAM04, FW01, GMR08, GW08, GLO6a, GhGDS00, GS01, GPS05, GB09, HM00, HLL02, HCD08a, HCD08b, HRL09, Hsu05a, HLL03, HLL02, HKL09, Hsu05a, HLL03, HLH00, HLL03, HL05d, IM06, JK01a, JK01b, JW06, JWZ05, JLT01, KG09, hKLS00, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KCL03, Ku04, KCC05, Kwo03a, KHKL05, LHL03a, LKY05a, LKY05b, LHY05, LD01, LTH05, LPM05, LW05a, LWZH05, LYG07, LLW08a, LLW08b, LCC05, LSA07, LCZ05c, LCZ05a, LLC06a, LLC06b, Mel01, MR09, M009, MB08, M004, MMP09, MV03b, NZCG05, NC09, NSN05, OS09, PCS07, PW05, PBMO01, PSG09, PS08a, Pel06, P80+08, PC00, PLJ05a, PLJ05b, QCB05a, Reg03, Reg04, RG09, RCG05, Sae02, SG07, Sco04, Sei05, SPG02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SCS05a, mSgFtL05, SSM08+08].

Based [SW05, SH00, SK01b, SL05, SLC05, Sun02, SCS05c, TWNA08, Tsa05, UHA09, UBER09, VSO1, VKS09, WAF00, WL07, WJP07, WQ08, WH02b, YW05, XMST07, YW04, YCW08, YS04, hY08, YJ00, YPS01, YRY05c, YPKL08, YY00, ZC04, ZC09, ZWD06, ZCL05, ZYW07, dRMS05]. Bases [AAC+01, ADD06, BKP09, B0+02, CvTMH01, EBC0+00, FJ03, FLA03, CCT08, Fan09, ZT03]. Basic [Go10b, Go10a, Go04, K05b, Puc03, Ste02, Bon01]. Basics [Leh06, Lut02].

Basing [BPR08, CHL02, AGG06, AGG10]. Basic [RMH03b, Vav03, vW01, GPS05, LS05b, RMH03a]. Batch [Ara02, HLT01, PBD07, Sha01d, BLH06, HLH00]. Batching [SB01]. Battery [CBSU06]. Battle [Bud00a, Bud02, SM00c, SM05]. Bay [Cal00c]. Bayes [Goo00]. BB84 [I0a2].

BC [IEE02]. BCH [MLC01]. BDD [Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01]. Beach [IEE00a]. beat [Lev01]. because [AJ08]. Become [Ort00]. Been [Nic01].

BeepBeep [Dri02]. before [Uni01a, Uni00b, Uni00c, Uni000, YJ00]. Beginning [Dew08, Hoo05]. Beginnings [Bud00a].

Begins [MP00]. Behavior [Vav03]. BEHEMOTH [Bar00c]. Beijing [FLY06, LST0+05]. Being [ASW0+01, ES00a]. beleid [dL00]. Belgium [DR02c, Pre00, Q500]. Belief [BPS02]. believing [Buh06]. Bell [BZ02, Eke02]. Benchmark [TYLY04, LDH06, YLT06].

Bendy [Sas07]. Benefit [YKL02a]. benefits [CH00]. Benford [NM09]. Bergen [Ytr06]. Berkeley [IEE06]. Berlin [FLA03]. Bermuda [Bla03]. Bernard [DNS03]. Berners [Coc02]. Berners-Lee [Coc02b]. Best [Bau01a, Bau01b, MFS0+09, Go10b, Ste02].

BestCrypt [Bau02b]. Bethesda [AC09]. Better [FV03, PM00, RR02, SKQ01, HLLL03, Pau03]. BetterBASIC [ASW0+01].

Between
[DKMR05, Ket06, Ng05, NN06, Fan09, GKM+00, GC05, MSV04, RW03a, SK06]. Beurling [Bec02]. Beyond [Gor06, LMW05, Mar08a, Sch03, See04, Sty06]. BGP [ZSN05, vOWK07]. Bi [Con04, PJK01]. Bi-directional [PJK01]. Bi-linear [Cou04]. Bi-directional [PJK01]. Bi-linear [Cou04]. Bias [CL02c, Sel00]. Biased [BS00a, LSKC05]. BiBa [RR02]. Bibliography [Bee05]. Bidiagonal [BR09]. Bidiagonal-Singular [BR09]. big [RR03a]. BigNum [SR06]. Bilateral [CT08a]. Bilinear [BGLS03, BMS03, CL04a, HMS04, KK02, LC05b, VK08]. billing [SSM+08]. Binarization [LSKC05]. Binary [ADI09, HHM01, LSKC05, OSSST04, SKG09, ACTZ05, BG08, BG09, FSGV01, GB09]. Binary-Ternary [ADI09]. BIND [Kle07]. Binding [DN02b]. BioAW [MJ04]. Biometric [AHKM02, Dal01, EM03, HH01, KJ05, LT+04, PK01, SR01, Sas07, Way01, Way02a, Wea06, BS01b, KN03, Li05, LST+05, MR00, MJ04, TB02, ZJ04]. Biometrics [Ash03, Bjo05, JR03, Ri02, Str01a, BC+03, Bu06]. Biometrics-Based [Ri02]. Biomolecular [Bi09]. Birds [MLM03]. birth [SE01]. Birthday [Wag02]. Bismutation [BGP02]. Bit [AIK+01, BK06a, BL08, CGH01, CDL+00, DMS00, G07a, IT03, KZ07, LS02, MS09c, PCG01, RMH03b, SM03b, SXY01, VK09, ATSVY00, Bar06a, BK07, GP08, KZ03, KKL09, Luc00, Pri00, RMP08, SW05, UHA+09, WW08, ZFK04]. Bit-Fixing [KZ07, KZ03]. bit-substitution [GP08]. BitLocker [Kor09]. Bits [BS01d, SZ01, HN04, Shp02]. Bitlice [DPV01]. Black [An01g, CF02, CF05, DI05, DRR05, DS08, KY01d]. Black-Box [An01g, BR02, CF02, CFS05, DI05, DRR05, KY01d]. Blackmailing [PS01b]. Bletchley [Sal00b, Cop05, Cop06, Sal05a, SE01, Smi01b, Win00]. Blind [AO00, BNPS02, BB06a, BSC01b, CL01b, JKK+01, LY07, Nafo05, PA02b, SPK08, ZTP05, ZK02, Fan03, HC04a, JLI01, JLI04, LH05, LC05b, MS09a, SV08a, SHT05, WHH05, ZC05]. blindness [AvdH00]. Blink [Sas07]. Block [AIK+01, BS02, BR02, BSC01a, CVTMH01, Can01b, CLLL00, CP02, CM+05, Cre01, DR06a, Dwo03, EYCP00, F02a, HSH+01, JKK+01, KCP01, KHH01, KKH03, LRW02, MV00, MS02e, NP01, OMSK01, Pat01, PS06, Pli01, RMS05, SM03b, SYY+02, SK01, XH03, YG01b, Bai08, BF06a, DY01, Dnm06, Gho00, GPX08, Hey03, JK01b, Jun05, K05a, KJ01, LDDH06, LC04, LKH+08, MMJ05, P08+08, RBB03, SHJ04, SH07, WF02, XH05, YI00]. Block-Cipher [BR02, RBB03]. Block-Cipher-Based [BR02]. Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. blockciphers [Fur01]. Blocks [Jou02]. Blockwise [IM02]. Blockwise-Adaptive [IM02]. Bluetooth [GBM02, LV04, LMV05]. Blunders [Bur01]. Blur [VHP01]. Blur/Deblur [VHP01]. Bluring [LSKC05, SK06]. Board [CGBS01]. boat [DB04]. Body [Bam02, TG07]. BOEL [Fin02]. Boethius [Eag05]. bombe [Wil01a, Tur04]. Bombes [An02e]. bombs [Lov01]. Bonds [CAC03]. Boneh [ASK05, Hes04a]. Bonn [DRS05]. Book [And04, Duw03, E05, Fal07, For04, Gas01, Gum04, Inc03, Irw03, Jan08, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Re01, Rot07, Sal03b, See04, Sh04a, Sin02, Spr03, Sty04, Ter08, Top02, Uru04, Wal00, Was08a, Kat05b, Lam07, Lun09, MAaT05, Sin09, Sin00, AAG+00]. Books [Dr00c, Re01]. Bookshelf [Lut02, Lut03, Wil01b]. Bookworm [Sal03b]. Boolean [Car02, CT03, CS09, MS02b, QP05, SM00a, SM00b, SM03a, WV00]. Boomerang [KKS00a, KKS01, KML+02].
Boot [HSH+08a, HSH+08b, HSH+09].
Border [MJF07]. Borders [PGT07].
Boston [USE01b, USE01a]. Botschaften [Sch09]. bottleneck [WL02]. bottlenecks [HTW07]. Bound [CY08, DGN03, KMT01, HLLL03, hY08, GW00]. Boundaries [PGT07]. Bounded [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vad03, DFSS05]. Bounded-Quantum-Storage [DFSS08]. Bounding [DM07b]. Bounds [BDF01b, BP03b, DIRR05, Di 01, GGT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKK03, JZ09, PS02a, Shp99]. Bouwmeester [Duw03]. Box [Ano01g, BRS02, CF02, CFS05, DI05, DIRR05, DS08, FM02b, KY01d, Kil01b, SMTM01, JmBdXgXm05]. Boxes [Bih00, BCDM00, ZC00]. BP [Wei00, Wei05]. Braid [AAFG01, CJ03a, GM02a, Hug02, KLC+00, LLH01, LP03, Cho08b, Hen06]. Braille [Pau02b]. Branch [AKS06]. Branches [Fel06]. Break [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breaking [BKN04, DKFX05, GO03, GKO2, KR03, Kih08, Sal00a, Wri05, Fie09, Gar01, SE01, Sm01b, SL07, Swe08]. breaks [OS00]. Breakthrough [Coo02a, LR01, Pan02a]. Brief [Bon07, Cos03, Boo05, Gra01]. Briefs [MP00, PM00, Pau02a, Pau02b, Pau03, Pau09]. Bright [Ano01g, LNP02]. Bristol [DFCW02]. British [ACM08, Fie09, Fra01, Syv02, Bud00b]. Broadband [MP00, SHL07, MJF+08].
Broadcast [AFI06, BGW05, CKPS01, CV06, DS03, FWW04, GSW00, GKK007, GRW06, HS02a, HLL05, LNP02, SNWX01, Woo00, ASW00, KSW06, Kre05, Mar05b, NLD08, RG09, WDLN09, LN04]. Broadcasting [TJ01b, WH02b]. Broke [Urb01, KS04]. Broken [Ahn08]. Brooks [Bar00b]. Bruce [Sty04, See04]. Bruges [Pre00]. Brumley [ASK05]. Brute [Cur05, SGA07]. Brutus [CJM00]. BSD [Lin02, ASW+01, Lin02]. BSDCon [USE02a]. Bubble [Ber03]. Buchmann [Lee03a]. Buffer [FOBH05, Fry00, Ino05]. bug [Bor00]. bugs [GJL06]. Building [Jou02, Knu07, Mar02a, And08, Bra01a, FB01, LS05b, McGregor, MPH06, DB04]. buitenlands [dL00]. Bulletin [Cer04b]. Bulletproof [Cha05b]. bundles [GT02]. Burrows [ABM08]. Burying [Arn01]. Bush [Ris06]. business [HHSS01]. Buy [PLW07]. Buyer [MM01a]. Buzzes [Coc02b]. Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGR07, LLR02, LLR06, P106]. Byzantine-Resistant [CNV06].
Canada [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00].

Cambridge [CZ05].

Cantor [WPP05].

Capabilities [BDTW01, AL04, ABDS01].

Capability [MH05].

Capable [ETMP05].

Capacity [ChLYL09, Sug01, ME08a, Wan05].

Card [IEE05b].

Cards [And04, AJ01b, Bel01, CK06, DJLT01, HBdJL01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NFQ03, Q501, Sak01, Sha01c, TBDL01, VPG01, YKMY01, Ano04b, Ano04c, AJ01a, BPR01, BCHJ05, Bur00, DFH01, DFPS07, Fin03, GU01, HHS01, Hsu05b, KLY03, LKY05a, Ler02, LCS09, MY01, PB01, Pr07, SVD07, TIS07, Ano03a, BJvdB02, CL04d, CCK04b, Che00, Gro03, HL05b, Kuo04, KC05, LHY02, Sco04, SCF01, YW04].

Card-based [LSA07].

CARDIS [DFPS06].

CARDIS’98 [QS00].

Card-based [BBKN01, BPR05, BR00b, DGH04, Fer06, JMV02, KI03, Vau01, Vau02].

CBIDs [MC04].

CCA [KOMM01, Mül01b].

CCA2 [BST02, Lin03, RG09].

CCGrid [KCOM05].

CCM [Dwo03].

CDH [CM05a].

CDH-Based [CM05a].

Cell [Fox00, MYC01, SHL07].

Cell-phone-free [Fox00].

Cellular [La000, LZ04, MGC02, SBZ04, Bao04, ETMP05, K03, SHH07, Wan04a, dRMS05, Wue09].

Center [AUW01, CH01a, CYH04, LPM05].

Centered [BBKN01, CMB05].

Central [CHL02].

Centralized [BP01, PRS04, Vau01, Vau02].

Certification [An01i, CHM02, RSA00b, BGB09, BD04b, KB09].

Certified [ANR01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LKW05a, Sha04b, Sha05b, TlH05, Tsa05, JJC03, WH03].

Cerven [Sab03b].

CFS [It01].

ChaCha [Ber08].

Chain [YT09, YZ00, Wue09].

Chaining [BB01], chaining [PCC03], challenge [LMO8, LW05a, PRS04], challenge/response [LV05a].

Challenges [Cla00a, GV09, Nao03, Sta03, SVE09].

Chang [CWJT01, ZC05].

Chang-Wu [CWJT01].

Changes [Mur01].

Changing [BST03].

Channel [BU02, CHV03, Law09a, LCK03, Mö02, NMO05, OT03a, OT03b, Sch06a, SYL05].

case/average [Mic02b].

Cash [PS01b].

Cathedral [USE02a].

Caught [Wei00].

cause [SBB05].

Causes [Mur01].

Cautionary [GMP01a].

Cayley [Lam91].

Cayan [Svy02].

CBC [BBKN01, BPR05, BR00b, DGH04, Fer06, JMV02, KI03, Vau01, Vau02].

CBIDs [MC04].

CCA [KOMM01, Mül01b].

CCA2 [BST02, Lin03, RG09].

CCM [Dwo03].

CCS [Mar02b, MS05b].

CDH [CM05a].

CDH-Based [CM05a].

Cell [Fox00, MYC01, SHL07].

Cell-phone-free [Fox00].

Cellular [La000, LZ04, MGC02, SBZ04, Bao04, ETMP05, K03, SHH07, Wan04a, dRMS05, Wue09].

Center [AUW01, CH01a, CYH04, LPM05].

Centered [BBKN01, CMB05].

Central [CHL02].

Centralized [BP01, PRS04, Vau01, Vau02].

Certification [An01i, CHM02, RSA00b, BGB09, BD04b, KB09].

Certified [ANR01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LKW05a, Sha04b, Sha05b, TlH05, Tsa05, JJC03, WH03].

Cerven [Sab03b].

CFS [It01].

ChaCha [Ber08].

Chain [YT09, YZ00, Wue09].

Chaining [BB01], chaining [PCC03], challenge [LMO8, LW05a, PRS04], challenge/response [LV05a].

Challenges [Cla00a, GV09, Nao03, Sta03, SVE09].

Chang [CWJT01, ZC05].

Chang-Wu [CWJT01].

Changes [Mur01].

Changing [BST03].

Channel [BU02, CHV03, Law09a, LCK03, Mö02, NMO05, OT03a, OT03b, Sch06a, SYL05].
ARR03, BP03a, BG07b, Buh06, CNPQ03, LCZ05b, PSP*08, WL07, YTWW05].

Channels
[AIP01, CK02b, Nam02, Vau05b, LH04].

Chaos
[JK01b, SK01b, WZW05, JK01a, LMC*03, McN03, PSG*09]. Chaos-Based
[WZW05, SK01b, JK01a, PSG*09].

Chaotic
[LLL*01, SXY01, USY02, Vav03, AMRP00, AMRP04, GHGSS00, GB09, HHYW07, HLW07, YTWY05].

Chapman
[Kat05b, Was08a].

Chapters
[MA05aT05, Tat05].

Characteristic
[Gau02, GPS06, KT00, Ver02, GPS05].

Characterization
[AJO08, Nam02, XH03, BGM04, KY00, QPV05, XLMS06].

Characterizations
[Pas05].

Characterizing
[BTW05, BTW08].

Charging
[BACS02, RH02].

Chatter
[Kee05].

Chaum
[BNPS02, WHH05].

Chaumian
[Mö03a].

Cheating
[OKS06, PZ01, PZ02a, ZP01]. check
[Kir01]. Checkable
[BPST02]. Checking
[BL02, JY00, GGH*08, RG05].

Checks
[Sha01a]. Checksums
[Sto01, SGPH98]. Cheju
[Kim01].

Chemical
[EIG01].

Children
.CV04, RD01, Roy05].

CHES
[JQ04, KKP01, KP01, KP02, RS05, WK03]. CHESS
[KLHL09]. CHESS-64
[KLHL09].

Chicago
[ACM04b, Top02, Con00].

China
[B*02, DWML05, FLY06, JY04, LLT*04, Li05, LST*05, ZJ04, ZYH03, TTZ01].

Chinese
[LLT*04, Li05, Sch01b, CAC06, YKLM03].

Chip
[BNPW03, DV08, MM01b, MM01c, MP00, Fox00, ISTE08, An04b].

Chip-Secured
[BNPW03]. Chipkarten
[An04b]. Chips
[An00b, Pau02b]. Choice
[Jam00].

Chosen
[BCHK07, CKN03, CHJ*01a, CHJ*01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JKS02, JJ06b, KS00a, KY01a, KCJ*01, KMZ03, KM01c, Ki01a, Man01, Nov01, PV06b, Poi00, Sho00b, BM05, CHH*09, KG09].

Chosen-Ciphertext
[BCHK07, CKN03, CHJ*01a, CHJ*01b, Des00b, DK05, FP01, JKS02, JJ06b, KCJ*01, KMZ03, Nov01, PV06b, Poi00, CHH*09, KG09].

Chosen-Plaintext
[DN02a, KM01c, Ki01a].

CHW
[CHC04].

Cincinnati
[BD08].

Cinematic
[CAC03].

Cipher
[AIK*01, BR02, Cer04b, CLL00, Cro01, CL02c, DR00a, DG00, DWP05, DF07, Dwo03, EYP00, FF01a, Flu02a, GBM02, HCJ02, HQ01, KYC01, KGD01, LKHL09, MSNN07, NPV01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY*02, SXY01, SBEW01, SBEW01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, GPX08, GGM05a, Hey03, KH08, Kid00, LKH*08, PV08, RBB03, Sal00b, SHH07, W08, Win05b, WF02, CH05].

Ciphers
[AAG*00, BBKN01, BS00b, BR01, BK00, ČvTM01, Can01b, CF01b, Can06b, CJS01, Chu02, CH02, CP02, CM03, Cou03, DPV01, Eag05, Fil00, FF01a, Fil02, Go01d, HR00, HR04a, HSH*01, Jam00, Jan06, Kan01, KCP01, KKG03, LRW02, MV00, Oni01, PP06a, Pli01, RMS05, Sar02, SM03b, SKU*00, Wal00, Wri05, ? 02, YG01b, ZC00, Bai08, Bar06a, Bel07, Ber07, Bod99, DL09, DY01, Dun06, DK08, Egh00, GGP06, HW03a, HWR09, Hey03, JK01b, Jun05, Kat05a, Kin01, LMS07, LDH06, Lun09, Max06, MI09, MWM01, Pin06, SHJR04, Sni01b, SL07, SB05, TT00, Wag03, YI00, You06, Kat05b].

Ciphertext
[BBK03a, BCHK07, CKN03, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JKS02, JJ06b, KS00a, KY01a, KCJ*01, KMZ03, KM01c, Ki01a, Man01, Nov01, PV06b, Poi00, Sho00b, BM05, CHH*09, IM06, KG09, Po00]. Ciphertext-Only
[BBK03a].
Ciphertexts
[AFI06, BGW05, BGN05, Gen04b, JJ00a].

Circuit
[EHK +03, GSS08, HR05, MG08].

Circuits
[BI05a, FML +03, Gol03, ISW03, MD05, PBTW07, You01, GLC+04].

Circumvention
[Kha05].

Cirencester
[Hon01, Pat03b, Sma05].

CIRM
[PPV96].

CISC
[FLY06].

citizens
[Ano03a].

clamping
[Ano03a].

Clandestine
[Wri05].

Class
[Car02, KM01a, KKH03, NN06, OP01a, Pli01, SBZ02, DKL00b, Fox00, HM00, Uni01].

Classes
[CY02, RSA00e].

Classical
[BYJK08, Gav08, GW00, LW05b, NA07, BYJK04, JZ09].

Classification
[HMS04, PBD00, Uni01].

clauses
[SV08a].

cle
[RSA09a].

Cleaner
[TR09a, TR09b].

Cleaning
[Lut03].

cleanup
[Lov01].

Client
[ANRS01, Ano01e, ANL01, FSSF01, PS05, WKB08, HTJ08, YS04].

Client-Server
[ANRS01, PS05].

client-to-client
[HTJ08].

Clients
[JRFH01, RKZD02].

Clip
[FGL02].

clock
[Pau02b].

Clocked
[CGFSHG09, MH04].

Close
[DM07b].

closing
[Lau08b, PWGP03].

cloud
[CKS09].

Clouds
[GS01, VS01].

Cluster
[Höf01, KCD07, SEF +06, TLC06, TW07].

Cluster-Based
[KCD07].

Clusters
[MFS +09].

CM
[CMKT00, GHK +06].

CMS
[BWBL02, DKU05].

Co
[Bud00b, Nd05, ACM01b].

Co-Design
[Nd05].

Co-operation
[Bud00b].

Coalition
[ACJT00].

Coalition-Resistant
[ACJT00].

coarse
[Rh03].

Coast
[Boy01].

Cod
[IIE05b].

Code
[Ark05, BR04, CV03, Cer04b, FIP02a, FF01b, HSZ101, Imr03, KY01e, Lai08, OS09, Ree01, Rey01, Sal00a, Sin02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MMJ05, RSA09a, SM00c, SM05, Sin99, Sin00, Swe08, AAG+00, SE01].

Code-based
[BR04, OS09, BGB09].

codebook
[WJP07].

Codebreaker
[Hau03, Pin06].

Codebreakers
[Bec02, Gan01b, Gas01, Kah67a, Kah67b, Kah74, Kah96].

Codebreaking
[Bud00a, Bud00b, Sin01b, Bud02, Cop05, Cop06].

codec
[Che08a].

Coded
[MLC01].

Codes
[Bee05, BP06, Big08, Bod99, BQR01, Chu02, CDG+05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, YM02, YYD001, Yek07, Bel07, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HWR09, Lam07, Lam09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02].

codemod
[AJO8].

Coding
[Buc00a, CS05b, HHL+00, Joy00, LLL+01, MZ02, Pat03b, RK06, Sal05c, Sma05, TW02, Ytr06, Che07, DW05, Gar04, Hon01, PPV96, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sea05, Sea09, TW05, Irw03].

Coefficients
[CH01b, KT00].

Cohen
[Was08a].

Coherent
[TPPM07].

Coin
[Lin01b].

Coin-Tossing
[Lin01b].

Coins
[HR04b].

Cold
[HSV+08a, AJ08, HSV+08b, HSV+09].

cold-boot
[HSV+08b, HSV+09].

collaboration
[ED03, PCSM07, SBG05, SBG07].

collapse
[SBB05].

Collection
[GMM08, Bro05a].

Collections
[Kuh00].

Collective
[BBB+02].

collide
[GNP05].

Collision
[DG02, IK005, WYY05a, WYY05d, GM00a, Sem00].

Collision-Resistant
[IK005].

Collisions
[BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c].

Collusion
[BG05, HNZI02, Zan01].

Cologne
[WKB03].

Color
[Che07, Che08a, FGD01, AEE055, CDD07, Yan02, YCL07].

Colorado
[BC01, Sch04b, USE00d].

Coloured
[CDD07].

Colossus
[Cop04a, Cop05, Cop06, Lav06, Sal00b, Sal00a, Sal05a, Salxx].

Colour
[RS00].

Coloured
[AADK05].

Columbia
[ACM08].

column
[Raj06].

Combination
[CF01b, Gau02, GHPT05, GB09].

Combinatorial
[GMW05, SLTB+06, Hen06].
Combinatorics [Lee03b]. Combined [LLS05a]. Combiner [Sar02, LL06].
Combiners [AK03]. Combining [Abe04]. Comes [Mar08b]. Coming [Dan01].
Commemoration [BZ02]. Comment [SCS05b, WY05, WLW04]. Comments
[AS01c, CGH+ 00b, JW01, MNFG02, SKW+00, CJT04]. Commerce
[CLK01b, GS02a, Sta00, Uni01, ZYM05, BM03a, FB01, Gra01, MY01, SN07, YC09].
commercial [LCC05, YLR05]. Commitment [DN00b, CF01a, DFS04, FM02a, Gen04a, HNO+09]. Committee
[Uni00a, Uni00b]. committing [DN00a, Nie02b]. commodity
[CGL+08a, CGL+08b, CGL+08c]. Common
[Pas03, TG07]. Commonwealth [PY05]. communicating [Hut01]. Communication
[AK02a, ANRS01, BYJK08, BBK03a, BIW08, Big08, Col03, Fis05, GKK+07].
Comparative [DPR01, GLG+02, Kat05b].
Comparing [HU05]. Comparison [GC00a, GC01a, Gau02, RBL+06, MS02a, SW00a, WW00, FGM03, JL03, Sma01, WB00].
Compendium [Lut02]. Compensated
[AAK09]. competition [Cla00b]. compiler
[DFG00, Oiw09]. Compilers [Lut02]. Complementary [AS01c]. Complete
[Bar00a, Bee05, Bud00a, FGMO01, GCKL08, HSM04, KY00, MS09c, Sal07, TWM+09, Bud02]. Completeness [HG03, PT08].
Complex [JJK+01, LKL05]. Complexity
[BYJK08, BLM01, BDK+09, CKRT08, CB01, DN00a, FBW01, GKKO07, GKK+09, HR04a, Lut02, Nie02b, RMH03b, Ros00, Rot05, Shp03, BYJK04, CDD00, GKK+07, GIKR01, Gor05, JZ09, Mic02a, MP08, RMH03a, Rot02b, Rot03, Shp99, SPHH06, TW06, SV08a, Fa07, Rot07]. Complexity-Theoretic [CB01].
compliance [LMW05]. Compliant
[CGBS01, RV09]. Component
[BSL02, Hei01, TEM+01]. composability
[PS04c]. Composable [AF04b, BOHL+05, BLDT09, CF01a, CK02b, DN02b, DN03, NMO05, RK05, Can01a, CL05a]. Composite
[CQS01, GMP01a, RDJ+01, Zhe01]. Composition
[BJP02, BN00a, CR03, CV02, Pie05, Sho00a, Can06a, LLR02, LLR06, Pue06].
compositional [GM04]. Compostela
[BS03]. Compound [SB05]. Compress
[Gen04b]. Compressed [ISSZ08, SB04].
Compressed-Domain [ISSZ08]. Compressibility
[HN06]. Compression
[ABM08, BD03, HSKC01, Ke02, LHS05, RS08, Sal07, SDFH00, WWL+02, FS08, Gar04, Lai04a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TT01, Zir07]. Compression-Encryption-Hiding
[BD03]. Compromise
[Ahm08, Lai08]. Compromised
[ZYN08]. computability
[Pet08]. Computable [Vad03].
Computation
[ACS02, Bai01b, BCL+05b, BL05a, BIM00, BJLS02, CC00, CDM00, CDM01, CDG+05, CD05, DN03, DI05, DM00b, FS02, FGMO01, FW04, GIKR02, HCK09, Has01a, HM01b, Jef08, KO04, KLML05, KSR02, Lin01b, PS05, WW05, Ano02d, AB09, BEZ00, BEZ01, CLOS02, CL08, CDD00,
DwWmW05, Fan03, GCKL08, HT04, HLL03,
IKOS07, LMSV07, LC04a, May09, Mis06,
SH05, WLH05, WY05, SM07, Duw03.

\begin{itemize}
\item \textbf{Computation-efficient} [CLC08].
\item \textbf{Computational} [DLP\textsuperscript{+}09, GH02, KL09, KK06,
Rup09, SM07, WvD02, AUW01, IKOS08,
Lam01, Lau08a, Nie02a, Sho05, SHJR04].
\item \textbf{Computationally} [MPSW05].
\item \textbf{Computations} [HL05a, ML05, Lam01, Lau08a, Nie02a, Sho05b, SH05, WLHH05, WY05, SM07, Duw03].
\item \textbf{Compute} [MFS\textsuperscript{+}09].
\item \textbf{Computed} [FBW01].
\item \textbf{Computer} [BS03, Bis03b, Bro05a, BCDH09, BC01,
CSW\textsuperscript{+}08, CZK05, CGK\textsuperscript{+}02, Coc02a, Coc03,
HYZ05b, IEE00a, IEE01a, IEE02, IEE03,
IEE04, IEE05a, IEE05b, IEE06, IEE07,
IEE08, IEE09b, IEE09b, JEE10b, JEE10c,
Lam01, Lau08a, Nie02a, Sho05, SHJR04].
\item \textbf{Computer-Science} [Coc03].
\item \textbf{computerized} [LMC\textsuperscript{+}03, Pau02b].
\item \textbf{Computers} [Coc03, Ett02, TSS\textsuperscript{+}03, Cop05,
Cop06, RH00].
\item \textbf{Computing} [ACM00, ACM01a, ACM01b, ACM02,
ACM03b, ACM04b, ACM05a, ACM05c,
ACM06, ACM07, ACM08, ACM09, ACM10,
ASW\textsuperscript{+}01, BBDDK00, CGH00a, CLK1\textsuperscript{a},
Coc03b, EP02, JP03, LKHL09, Lut03,
May04, PHM03, Sch06b, SKG09, SCF01,
Sim02, SEF\textsuperscript{+}06, Sta03, TIC06, VHG09, Ver02,
WC01a, Yan00, YKMB08, Cha07, Che05b,
CHT02, DHL06, HV09, HKPR05, LMC\textsuperscript{+}03,
MI09, PP03, PP07, Raj06, RP00, Sei05,
Wil99, YLR05, Lut03].
\item \textbf{Compunware} [An02b].
\item \textbf{conceal} [BB79].
\item \textbf{Concealing} [DMS00].
\item \textbf{Concealment} [DA03].
\item \textbf{Concept} [ARC\textsuperscript{+}01].
\item \textbf{concepts} [AB09, Kra07, SWR05, MC04].
\item \textbf{concerning} [HW03b].
\item \textbf{Concerns} [MP00].
\item \textbf{Concrete} [KNS05].
\item \textbf{Concurrency} [JL00].
\item \textbf{Concurrent} [BP02, DPV04, Gen04a,
KKG03, Ros00, Ros06a, Dam00].
\item \textbf{Conditional} [LMV05, WN02].
\item \textbf{Conditions} [IKO05].
\item \textbf{Conference} [ACM03a, ACM04a,
Ano06a, AAC\textsuperscript{+}01, AJ01b, Be00, B\textsuperscript{+}02,
BZ02, BS01b, Bli03, Bla03, Bon03, Boy01,
Buc00a, CC04a, CV04, CGP03, CGH\textsuperscript{+}00b,
Cra05a, DKU05, DFCW00, DFPS06,
EBC\textsuperscript{+}00, ELvS01, FLY06, Fra01, FMA02,
Fro04, FLA\textsuperscript{+}03, HR06, HYZ05b, IEE09a,
IKY05, JYZ04, JM03, Joy03b, Jue04,
KJR05, Kili0a, Kim02, KN03, Knut02, Lai03,
LL03, Le04b, LLT\textsuperscript{+}04, LL04c, MMV06,
MS05b, MS02c, Men05, Men07, NIS00,
Nac01, Nao01, Oka00, Oka04, Pat03b, Pf01,
Poi06, Pre00, Pre02b, RD01, Roy00a, Roy05,
Sho05a, Sil01, SM07, Sma05, Syv02, USE00c,
USE00a, USE01b, USE01a, USE02c, W109,
Won01, W103, Yun02a, YDKM06, ZJ04,
Zhe02b, ZHY03, AUW01, BC05b, DV05,
DWML05, DRS05, Hon01, Kili05, Lii05,
PC05a, PY05, PPV96, QS00, Son00, WK06].
\item \textbf{Confidences} [Gan01a].
\item \textbf{Confidentiality} [Dwo03, YC08].
\item \textbf{configurable} [MBS04].
\item \textbf{Configuration} [Sha02, Mos06].
\item \textbf{Confirmation} [SK00].
\item \textbf{Conformer} [CM00, GM03].
\item \textbf{Confiscation} [DBS01].
\item \textbf{Conformance} [LB00, RSA00c].
\item \textbf{confounded} [Bel07].
\item \textbf{confusion} [She01].
\item \textbf{congestion} [SB05].
\item \textbf{Congress} [Uni00a].
\item \textbf{congruences} [Ste08].
\item \textbf{Congruential} [CS05a, LS05a, SB05].
\item \textbf{conic} [LCC05, LCZ05a].
\item \textbf{Conjecture} [CU01].
\item \textbf{Conjugacy} [CJ03a].
\item \textbf{Conjugate} [Ig02].
\item \textbf{Connected} [BJLS02, Ho01].
\item \textbf{Connection} [HR00, Jam00, Goo00, Mic02b].
\item \textbf{Connection-Polynomials} [Jam00].
\item \textbf{Connections} [WRW02].
\item \textbf{Conquer} [SKQ01].
\item \textbf{conscious} [DMSW09].
\item \textbf{Consensus} [CNV06].
\item \textbf{Considerations} [DBS\textsuperscript{+}06, Hei07, Rub01, Sch07, SVEG09].
\item \textbf{Considering} [WA07].
\item \textbf{Consistency} [ABC\textsuperscript{+}05, JEZ04].
\item \textbf{Constant} [App07, BI05a, CS07c, CD01a, DPV04].
DN02b, DI05, Lin01b, Sun00a, IKOS08].
Constant-Depth [BI05a].
Constant-Round [DPV04, DI05, Lin01b].
Constrained [BCH00, DBS06, HS01, MRL02, Zhe02a, Has00, RAL07].
constraints [CC05d, LPM05, SN04].
Construct [CDMP05].
Constructed [Tsa05].
Constructible [NNT05].
Constructing [Des00b, Fis01b, Vad03, Wen03, JZCW05, NS01a, ZL05].
Construction [BBKN01, BB00b, Car02, CMKT00, Lin03, Nie02c, SM00a, TNM00, YWD08, DW05].
Constructions [BS00a, BR00b, BR02, GMW05, GGKT05, GM02c, Jou04, PR08, PZ02b, SNWX01, SM00b, GT00, GPV08, IK03, NR04, PR05, Reg03, Reg04, vDKST06].
constructive [GGH08].
consumption [Miˇs08].
Contact [YKMY01, Car00].
Contact-Less [YKMY01].
Contactless [And04, KS02, Cla00b, Fin03].
Contemporary [Ahm07, Opp05, SVEG09].
Content [AAK09, CGJ02, HHJS04, MA00a, MA00b, RE02, XMST07, YKW01, ATS04, DY09a, SG07].
Content-adaptive [XMST07].
Content-Based [RE02, YKW01, SG07].
Content-triggered [HHJS04].
Context [Bar00b].
Context [DJLTO1, FPS01, SN04].
continue [Lov01].
continued [Dan02].
Contra [Mah04].
contract [WK05].
Contrast [BDDS03, HKS00, HT06, KS03, CDFM05].
Contrast-optimal [HKS00].
Contrast-Sensitive [HT06].
Control [ABEL05, ANRS01, BW07, CGMM02, LY05, Sma03a, ZGLX05, BN08, DFM04, DPT02, JW06, KNS05, LKZ04, MD04, MSP08, PS04b, ST07, WC01b].
Control-flow [ABEL05].
Controlled [GVC08, IMM01, AW05, AW08, LAPS08].
Controlling [HY03, MS03b, MS02d, WL05].
Controls [Har01a, Har01b].
conventional [CJ04, YW05, YRY05b].
Conversation [GK04].
conversations [VAVY09].
Conversion [CDI05, Ket06].
Conversions [KI01b].
Convertible [Chi08, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b].
Convolution [PG05].
cookbook [VM03].
cookies [Cha05a].
Cool [Ano00b].
Coordinate [OS01].
COPACOBANA [GKN08].
Copenhagen [TBJ02].
Copley [USE01b, USE01a].
coprocessing [ML05].
Coprocessor [Gut00, Ito00, LS01b, OTIT01, AV04].
Coprocessors [Smi02].
Copy [LTM00].
copying [SV08a].
Copyright [Kha05, LLL02, PBB02, XFZ01, ZTP05, Gil07, Kwo03a].
CORBA [TE01].
Core [BF00a, Dim07, DV08, HMS04, TPS01].
Corfu [SM07].
Corner [Mar08a, TR09a, TR09b].
corners [Bhu09].
Corporate [HW01, KH03].
Correcting [MZ02, NN06, YYDO01, ZYR01].
Correction [BQR01, CTBA01, Din05, LN08, LW05b, MSPW05, TEM01, Car00].
Correctness [PBD05, HSD05, DHO8].
Correlated [FWW04].
Correlation [BSC01b, CS01, Gol01c, JJ00d, LV04, LM05, MH04, Nyb01, SY01a, WRW02, ZC00, GG05b, JJ02a].
Correlations [KM00, KM01b].
corruption [XNK05].
COS [FF01a, WB02].
Cost [CDF01, FBW01, PD07, Sta05, YEP06, CL09, SHJR04, YLR05].
Cost-Effective [PD07].
cost-ineffectiveness [YLR05].
could [Cla00b, Pau02b].
Counter [DIS02, QS01, SLG05, SL06, MMJ05].
Counter-Measures [QS01].
Countering [PP06b, SK05b].
Countermeasure [HT03, MMT09, OT03a, PKBD01, YKL02a].
Countermeasures [AVA03, Fry00, GM00b, MOP06, OS05, Has01b, JDJ01, Man08, OS06].
Counters [KMO01].
counterterrorism [Naf05].
Counting [Gau02, Kuh00, Hig08].
Couple [SXY01].
course [AA04b, GV09, GL05].
courses [Gha07].
Cover
[GA05, Gut02a, LNP02, NN03, RS00].

coverings [SC02b, Cover [Col03].

Covert [Col03].

Cozens [Sal03b].

CPCMS [Sha02].

CPI [ECG+07].

CPOL [BZP05].

CPUs [ESG+05].

Crack [Sin02].

Crackberries [Sta05].

Cracked [AAG+00, Nic01, Pri00].

Crackers [Ols00, SEK01, SEK02, NRR00].

Cracking [DZL01, BZ03, Cur05].

Crackproof [Sal03b].

Cracks [Bar00a, Ste05c].

Cramer [Luc02b, VMSV05].

CRC [Kat05b, Spr02, SGPH98].

Creation [MV01, Top02, MB08].

Creator [Coc01a].

Credentials [CL02a, CL04a, LLW05, LLW09].

Credit [CNB+02].

Cret [ACM01a].

crime [Cas02, KB00, Lau08b].

criminal [Men03].

criminals [Win05c].

Criteria [Can01b, IBM00].

criterion [QPV05].

Critical [LKM+05, SE09, CS07a, Gor05].

cron [Oue05].

Cropping [SDFH00].

Cross [Bau02b, SM08, LCX08, SLP07].

cross-authentication [LCX08].

Cross-disciplinary [SM08].

cross-layer [SLP07].

Cross-Platform [Bau02b].

crowd [Fox00].

CRT [FMP03, Kuh02a, May02].

CRT-Exponent [May02].

crypt [Per03].

Cryptanalyses [Kan01, SKU+00].

Cryptanalysis [ASK07, AMRP00, Ano03, Ano07b, Auc07a, BDG+01, Bau04, BLH06, BP03a, BBK03a, Bar06a, BP01a, BD00a, Bih00, BFMR02, BDK02a, BDK02b, BSW01, BDD03, BD00b, BCCN01, CGFSHG09, CV02, CC01, CL01b, CYY05, CKY05, CKK+02, CWJT01, CJT03, Cho06, Ch08b, CJH02, CP02, Cou04, CGJ+02, DG00, DGP07a, DGP07b, DGP09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Finc06, Fln02a, Fln02b, Fur01, Fur02a, Fur02b, G507a, GM02a, GJSS01, GS02c, GM02b, GM00b, GM02b, GC00b, Gra02a, GS09, GKN+08, HPC02, HQR01, HAuR04, Hen06, HLL+01, HSM+02, HHK+04, Hsu05a, HLH00, Hwa00, JK02a, J003c, JC01, JnbdXgXm05, Jou09, Joy03a, KM02, KW03, KS00b, KRY05, KW02, KRS+02, KKS00b, Kra02a, KC05, Kuh01, Kuh02b, KHKL05, LC03, LHL+02, LP03, Lee03c, LKY04, LL05a, LR07, LBGZ01, LBGZ02, LLH04].

Cryptanalysis [LL05c, LLCL08, LW05c, MS03a, May02, MG01, MHL+02, Mor05, NP01, PSC+02, PK05, Pei04, Pel06, PS06, PS01c, QC05a, Sch06a, Sco04, Sha03c, Sha05a, STK02, SGB01, SKG08, SK01, SH07, TIGD01, TM06, TLH05, TJ01b, TSS+03, Wag00, Wag03, WL05, WBD01, WB02, Wu02, XY04, YSD02, YW05, YKLM02a, YKLM02b, YRF05a, YY05a, You1, YG01a, YG01c, ZVR01, ZKL01, ZC05, ZK05, Z05, ZC09, dW02, AMRP04, BF01a, Bai08, Bar09, BS01c, Buh06, Bul09, CV05, CK06, CKL+03, Dun06, Egh00, EBS01, Eke09, Fio09, GPG06, Goo00, Jun05, Kuk01, LMSV07, Max06, MAAT03, MAAT04, MAAT05, MAAT06, MAAT07, N02, Ph04, SQ03, Rupp09, SK01a, Sel00, Sin09, SL07, SCS05b, SLL+00, Swe08, TC00, TM01, WLW04, W02, Y100, YJ00, YKLM03, Kat05b].

cryptanalyst [Wil06].

cryptanalytic [BS00b, KFSS00, Oec03, QSR+02, Yan07, Wil01a].

cryptic [Wri05].

CRYPTIM [Ust01b].

CRYPTO [Fra04, Men07, Sho05a, Ahm08, Ano01h, Bau01a, Bau01b, Bur01, CCM01, CBB+02, Lev01, Lev02, Mar08a, Mar02b, MC04, SYL05, TR09a, TR09b, Yun02a, Ecc02, BK05, HGNS03, Web02, Bel00, Bon03, Kili01a, Yun02a, Sel00a].

Crypto-algorithms [An01h, CCM01].

Crypto-based [MC04].

Crypto-CCS [Mar02b].

Crypto-integrity [Yun02b].

Crypto-systems [An01h, CCM01].

Cryptoanalysis [HSIR02, LD01].

CryptoAPI [Bon00].

Cryptoclub [BP06].

Cryptocomplexity [Rot05, Fall07].

Cryptocomputer [HV04].

Cryptographer [Joy03b, Nac01, Oka04, Po06, Pre02b, Men05].

Cryptographers [Coc03, Tsa07, Bel07, Hau03].
Cryptographic
[AC02, AADK05, AL00a, ADH+07, BLST01, BDF+01a, Bar00a, BGK+03, Bih03, Bla01a, Bor01, BDP02, Bra01b, BM01c, BL08, Bur06, CC04a, Can01b, Car+02, CCDP01, CHL02, CB01, Cra05a, CS09, CO09, DD02, DHMR07, DFMO4, DWN01, DHR00, DV08, DFG01, FIP01b, FSN01a, FGM00a, Fri01, GMP01a, Gar05, GSS08, GGKT05, GK02, GTH02, Gor02a, GL00, GUQ01, Gut00, Gut02b, Gut04a, HTS02, HN06, Har06, Has01a, HLO5a, Igl02, IV00, Ito01, IMM01, JT05, KMO01, KY01b, KY02b, KI01b, KS06, Knut02, Kisu02, Law09a, LN08, LS05a, LKKL01, MS02a, MOP06, Mea01, MNP01, MRL+02, MMH02, Mor03, MK05b, MS05, NIS01a, NIS01b, N004, ND05, Ng05, Nic04, OTT01, OP01a, PKBD01, PR08, PJDH09, PA01, Pin02, Pin03, PS02b, Pre00, Pre02a, RSA00d, RSA01].

Cryptographic
[RR00, RRS06, Rot01, RSN+01, SM00a, SS01a, SGM09, Sha02, Shp03, Shy02, SFDF06, SR06, SL09, TLYL04, TWA08, TBL01, Uzu04, UK003, WN02, WBL01, Wc01b, You01, Zha08, AMRP04, ACTZ05, ALV02, AV04, BGD09, BDSV08, Bla01b, BP05, BG08, BG09, BDN02, BD04a, BGL+03, BM06, Can01a, Can06a, CHC04, CC05d, DP04, DFG00, FS03a, FSVG01, GT00, GPV08, GM04, GB09, HY03, I003, IKY02, IYK03, JW01, KSF00, KP03, LM010, Lai05, LLV05, LLV09, ML05, Mea04, MT07, Mi02b, MRST06, Mon03, NN03, NDM04, ND06, PS04a, PSG+09, PR05, Pre07, Pri00, Puc06, QPV05, Reg03, Reg04, RM04, RF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, kWpLW01, WL04, XLS06, YLT06, ZLX99, ZWVL01, ZL04b, dH08, BWB02, JQ04, KPK02, KP01, KNP01].

Cryptographic [RS05].
Cryptographically
[ADD09, AHS08, BFC02, BFCZ08, BB00b, FR08, MS02b, RGX06, Aam03, AW05, AW08, Lau08a, SM03a].

Cryptographically-masked [AHS08].

CryptoGraphics [CK06].
cryptographic [RSA09a].

Cryptography
[ANS05, AF04b, ADI09, AA04b, An00c, An01g, An04a, An05a, An07b, An07a, AAFG01, AIK04, AIK06, App07, AEQ05, ABM00, Bia01b, Bia01b, BIP03, BDZ04, BOV03, BOV07, BGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BWBL02, Bla02b, BDDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, BK06b, BKM07, Buc00b, BD08, BP01b, BRTM09, CPS07, Cer04b, CSW+08, CQS01, CPD06, C004, CFA+06, C000, Cor06, Dr.00c, Dam07, DFS08, DFS05, DD00, DFGH04, DK02, DK07, Des02, DT03, DY09b, DSS01, DDN00, DDD03, Dre00, DP08, EPP+07, EP05, Elb09, Ell04, ECG+07, Ett02, FS03b, Gal01, Gal02, GHK+06, GKK+09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, GRI01, Gro05, HR06, HH04, HHM01, HM04, HSS01, HSP08, Hon01].

Cryptography
[IIE00b, IKY05, Irw03, IKOS06, IKOS08, JYZ04, JLO0, JT01b, JT01a, Jue04, KLR09, KZ07, KGS07, Kat05b, KK06, KBM09, KPM02, KW08, KY01c, KSM02, KZ02, KS03, KW06, Lam01, LG01, LSY01, Lee03b, LLL+01, Liet05, LMD04, LW05b, LP02b, Lut03, LS08, MNT+00, MP02, Mao01, Mao04, MZ04, Mau01, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pel06, PM02, PB02, Poi02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGK08, Sti05, Sti01, Sti0, Sti06c, SJ05, Syv02, TSO00, TW06, TG04, TW02, Tro08, TR09a, TR09b, Uni01, USS02, VY01, VMC02, WPS01, Wei04, WK01, Wel05, Wei00, WvD02, YWC08].

Cryptography
[Ytr06, YC01, YDKM06, ZYH03, vDW04, Imr03, AMW07, AUW01, Ano02a, Ano02d, ABDS01, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BEZ00, BEZ01, BGM04, BEM07, Buco0a, Buc01, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CCT08, CDFM05, CDD07, Cos00, DD04, Dif01, DIM08, DwWmW05, DOPS04, DKL09, DW09, Dwu03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK07, Geb04, GRTZ02, Gol99, GG05b, GH05b, GPS05, GNP05, HH05, HLwWZ09, IZ00, IM06, JK01b, Joy00, KZ03, KL08, Kat01, Kil05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Mau04, May01, McA08, MBS04, MM07a, Mol07, NP02a, Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00, Pin06, Reg05, Reg09, Rot02b].

Cryptography
[Rot03, Roy00b, Rup09, ST07, SBZ04, Ser06, SH05, Sph99, Sil05, Sin09, Sin00, Smo04, ST01d, SK01b, TW05, UHA09, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Wri03, YC09, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Ree01, Wal00, Was08a, MP01b, Sph04a, Kat05b, Spr03, Ter08].
cryptography-based [FXAM04].

Cryptologic [BS00a]. Cryptological [Lew00].

Cryptology [dL00]. Cryptology
[Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Kin02, Lau03, LL04c, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka01, Po01, Rot05, RS02, Sha03b, Zhe02b, dL00, Ban00, Ban02a, Bel00, Bib03, Boo05, Boy01, CV04, Cra05a, DVO5, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam01, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka01, PC05a, Po01, Pre00, Pre02b, RD01, Roy00a, Roy05, Sh05a, Son00, Won01, WK06, Yun02a, vT00, DWML05].

CryptoManiac [WWA01]. Crypton [CKK02, MG01]. Cryptosystem
[BST02, FL06, GG01, GK05, GH01, Hug02, KM01a, KY02c, KLC00, LHT09, dVP06, Luc02b, NSNK05, NBD01, Ove06, PHK01, YG01a, YG01c, Zhe02a, Bao04, CL02b, CCH04, Che05a, Cho06, CFVZ06, CHH01, Dan02, DHL06, EKRM01, GH01, GS00, GC00b, GMW01, Hen06, Iwa08, JW06, KY09, LL04b, LL06, LKYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SP02, SCS05a, SP79, SL05, Sm00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, hY08].

Cryptosystems
[Aki09, Ava03, BDG01, BKLS02, BPS00, BMM00, CHSS02, CCW02, DDG06, DKXY02, ESG05, FJ03, Fe06, FP01, HK01, IZ00, Jou02, JQY01, KY02a, Kim01, KLY02, KKY02, Kl01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SK09, Ste01, VAD03, Wya02, XB01, ZLK02, Ban05, BF06a, BB79, CH01, CMKT00, EBS01, EHKH04, GH08, GBKP01, HM00, Has00, Has01b, Huh00, HP01, WK00, Kos01c, LD01, Luk01, Mic01, Mis06, OS00, Pe09, PLJ05b, SST06, Sh05c, Sma01, TO01, TC05, Ts05, Ver01, Why05, Wol04, WPP05, WV00, YY00, ZZ01, vT01].

cryptovirology [YY04]. CRYPTREC
[IY00]. CSCW [ZP05]. CT [Joy03a, Men05, Nac01, Oka04, Po06, Pre02b, ZC09].

CT-RSA [Joy03b, Men05, Nac01, Oka04, Po06, Pre02b, ZC09].

Cuban [AJ08]. Cube [DS08, PDMS09].

Cube-Type [PDMS09]. culture [Gil07].

Cumulative [WP03]. cure [RD09]. cure-all [RD09]. Current [DFH01, PRS04, LPW06].

curriculum [FOP06]. Curve
[ANS05, ADI09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BMM00, BWBL02, BS01d, BM01, CQS01, CFA06, GP08, HY05a, HH01, HM04, HM02c, JT01b, JT01a, KBM09, KP0F02, KS02, KWP06, LW02, M02, M03, MT01, OS01, PWGP03, Pel06, RAO03b, R04, R05, Sat06, Was08a,
Curve-Based [KWP06, Pel06]. Curves [AHRH08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK +06, Kid02, PWGP03, Ver02, CMKT00, Has04, LWZH05, MP01b, MSV04, Si05, Sim02, SC02b, Was08b, Wen03, Was08].


D [Duw03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05]. D.R [Irw03]. daemons [Mos06]. Damgård [CDMP05]. dark [Biu09]. darkening [CDD07]. DARPA [Coc01a]. Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BNPW03, Bro05b, Che01a, CTL01, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, Kiøs02, Lan00b, LP00, LHS05, Lut03, MND+04, MS03b, MF5+09, NM09, OS05, Per05, RKZD02, RK06, Sal03a, Sal07, Sin01a, TZDZ05, TPPM07, VDK05, WS05, WY02, WN02, ke01, vW01, AG09, AKH03b, AKSX04, Arn01, Bia00, BN08, CCM09, Cer04a, CLR09, CPG+04, DZL01, FS04, HILM02, LLK05, MJ03, Mal06, Men03, MI05, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGPH08, SETB08, WMDR08, YLC+09, YC08, ZJN07, Zir07, Cur05, DK08, Lin02, Pap05]. Data-Hiding [VDKP05]. data/image [S+03]. data/image [Sch00a, Sch01c, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, BI05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Man04, PS08b, PBV01].

database-service-provider [HILM02]. Databases [AK02b, CD+05, DN04, AHK03a, CDD+05, GA03, MSP09, MNT06, NS05b, ÜG08, YPPK09]. Datamining [DN04]. Datenverschlüsselung [Lin02].

David [Gas01, Pap05, Bar05, Eaz05]. Day [SE01, SW05, Win05c]. Days [Ad03, Riv03, Sm04]. DC [USE01c]. DCT [BSC01a, BSC01b, Ch01b, KT00, LYT07]. DCT-Based [LY07]. DDH [Lys02]. DDO [LK+08]. DDO-64 [LK+08]. Dead [Gut02a]. deaf [Pau02b]. Dealer [DK01, Sun00a]. Dealing [BH00a]. Debate [Jol01]. Debian [YRS+09, Ahm08]. Debugger [Ano02b]. Debugging [Ano02b].

Dec [IE09a]. decades [Lov01]. decades-old [Lov01]. December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kin02, Lai03, Lee04b, LTT+04, Li05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b].

Decentralized [MSP+08]. deception [CS07a, Mal04, MS02d]. Decidability [Kus02]. Deciding [Bau05]. Decimal [BJvdB02]. Decimisation [BZ03].

Decimation [Fil00]. decipherable [Sav04].

Deciphering [Eri02, KB07, Ark05, Lov01, NS01a]. decision [GR04, KM04a]. Decisional [Cu01]. Decisions [Coc02a, Sch07].

Decodable [Yek07]. Decoding [KY02b, LBGZ01, LBGZ02, Rai00, AGKS07, Bul09]. decomposing [FP09]. Decomposition [BR09, CL04c]. decompositions [vDKST06]. Decorrelation [CLLL00, Vau01]. decrypt [Biu02].

Decrypted [Bau00, Bau02a, MB01].

Decryption [Bar00b, BST02, CS03a, CCD07, FPS01, HGMP+03, Int00, KCJ+01, DZL01, GH08, Mil03, Shp04b, SWH+09].

Decryptor [Zol01]. DeCSS [Coc02a].
Dedicated [ISO04]. Deep [CMS08].
Defeating [CHK+08]. Defective
[BTTF02, Dav01b, Dav01c, KLR09].
Defending [NRR00, Pro01]. Defense
[GK02, HW01, Mirc05, Wy01, Bol02].
defenses [SL06]. defined [Yas08].
Definition [YWD08, SNI00]. Definitions
[Uni01, AH05]. Definitive
[BS01a, BSB05, Gar03b]. defyng [HRS08].
Degenerate [Ber09a]. Degradation
[BSC01a]. Degree [CV02, QPV05].
Degrees [Sat06]. DÉJÀ [DP00]. DeKaRT
[Go03]. Dekker [Irw03]. Delacorte
[Imr03]. Delay [WRW02, NS01a]. Delayed
[JM07]. delegated [CL04c]. Delegation
[WN02, ZP05]. Delhi [JM03, RM04].
Delivers [An002c]. Delivery
[NZCG05, RMCG01, DY09a]. Delphi
[TEM+01, Hei01]. Demand
[BD03, CMB+05, SEF+06]. Democracies
[CBZ+01]. Democracy [CTBA+01].
Demography [Coc03]. Demons [Mos06].
demonstrably [HL06]. demystifying
[RR04]. Deniability [Pas03]. Deniable
[Nao02, CCK04a, CHK+08, DG05, LC05b, YRY+05c, Zha06].
Denial [Mah04, Nik02a, Nik02b, PKBD01, Ril02, Mirc05].
Denial-of-Service [Nik02a, PKBD01].
Denmark [Cra05a, TB02]. Denver
[ACM01b, Sch04b, USE004]. Department
[Bol02, Eri01]. Dependable
[NABG03, And08]. Dependent
[Go03, WS05]. deployed [BDET00].
Deploying [BH00b, GS+04]. Deployment
[CL07, KDO01, Mur01, Sin01a, App05, JRR09]. Dept [Uni01]. Depth [Bi05a].
Derandomization [BOV03, BOV07]. Derivation
[DGH+04]. Deriving
[BJP02, CSW05]. DES-encrypted [Bih02].
DES-like [Egh00, EBS01]. Describing
[PS06]. Description [Lav06, MH05].
Descriptors [DN07, SP04]. Design
[Abd01, AADK05, An002c, ADD09, AIK+01, ARC+01, Bar00b, Can01b, CCDP01, Cim02, CB01, CS03b, CMB+05, CLZ02, DR02a, DF07, EHK+03, FF01a, FZH05, GSS08, Geb04, Gut02b, Gut04a, HRL09, Hro05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04b, LB05, MKP09, MP00, Nd05, NSS02, Rhi03, SJ09, SPG02, SRQL03, Uzu04, WZ05, WW08, WLLL09, ARJ08, CMS08, DR02b, GG05b, HC04a, Hut01, KS00, M109, MWM01, SVEG09, YCW+08, YC08]. Design/CPN [AADK05]. designated
[LV07]. Designing
[HBC+08, TCR03, C+02, CG05, Lan00a].
Designs
[Bee05, CC02a, Bai08, Des00a, WL07].
desktop [BDET00]. Desmedt [CHH+09].
Desynchronization [CDT05]. Detached
[Sha01a]. Detailed [Lut03]. Detect
[FBOH05]. Detecting
[CMS09, FGD01, JQYY01, Har07a, LHL04].
Detection
[AS01b, AD07, BB00a, BKM07, CH01b, Czik05, JT05, KKG03, SKQ01, SY01a, SLT01, ST01c, TZD05, TMMMO5, WG05, YI01, Zan01, Bej06, BBK+03b, HLL+02, Men03, NN02, WMS08, YW06, ZGTOG05].
Detection/Correction [SKQ01]. Detector
[BSC01b, DNP07]. Determined [KKH03].
Determining [KS03, LQ08, OS07].
Deterministic
[BK06a, Her06, KZ03, KZ07, May04, BK07].
development [BH05]. Developers
[An006b, Dev08, MK05b, Nis03a].
Developing
[MV03b, Cra05a, Gal02, HL06].
Development
[An002c, CNB+02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a].
developments
[Pre07, Sha04a]. develops
[Pau02b]. Deviates
[Ran55, Ran01]. Device
[RIC07, ST03b, WPS01]. Devices
[BCH+00, Dam07, EP02, GST04, Hei07, JPO2a, JW05, Kha05, KHD01, MV01, MRL+02, SCF01, WC01a, CMS08, DMT07, Tse07, ZYW07].
Devil
[Bla01c]. DFT [Ch08a]. DH
[Lys02].
DHIES
[ABR01]. DHP
[MSV04].
Diablerets
[Vau05a]. Diagnosis
Diagnostics [NM09]. Diagonal [PJJH01, PJK01]. Dictionary [SZP02]. Dictionaries [AGT01].

Dictionaries [BPR00, BCP02b, CS07b, Pho01, NS05a].

Died [MH09]. Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b].

Dies [Bar00a, Coc01a]. difference [PBMB01, dW02]. differencing [WWTH08].

Different [CGMM02, Sma01]. Differential [Ava03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eke09, Fur02a, Gra02a, HLL+01, HSM+02, HHH+04, IIT03, JT01a, Kan01, KM02, KPC01, LHL+02, MP06, MM03, MHL+02, MG08, PSC+02, PQ03, SK01a, SKU+00, SKI01, YSD02, vW01, BF01a, CUS08, Che08a, DLP+09, Egh00, EBS01, Pha04, SLL+00, TM01].

Differential-Linear [BDK02a].

Differentials [BF00b]. Difficult [Bud00b, MT02]. Difficult-to-pass [MT02].

Diffie [Jan08, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CUI01, CJO03a, CKRT08, FSO01b, GR04, KI01b, KK02, KM04a, Kra03, Kra05, Mio08, TSA06, YRY05c].

diffuser [She01]. digest [MSP09]. Digit [KWP06, Tan07a, BG09, HKPR05, Kir01].

Digital [AN05, AvoH00, AR00, AS08, Ano01f, Ano02b, ABRW01, Bar00a, Bar06b, BL08, BSD09b, Cal00a, CHH05, Che01b, CFS01, CMB02, CMB+08, CZB+01, CGJ+02, DSO01, EIG01, Eng00, EHK+03, HSZ00, HSZ10, HS01, HHHG+03, HW01, HLT01, JBR05, KZ01, Kal01, KC02, Kuh00, Kw02, Kwo03b, LZ+01, LLL+01, LIO0a, LIO1, Lut03, MMM0a, MM02, Meh01, PL01, PJJH01, PCG01, PBM+07, Ram01, Rs01, Sato09, Sch00d, Sch06b, Sha01e, SC02a, Shi08, SLT01, Sugo01, TJC03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, Wya02, XFZ01, XYL09, YYDO01, YYZ01, ZWC02, Zwa02, Ate04, BLH06, Bra01a, Ca00b, CS08a, CWH00, CL00, CJO5, Che07, FB01, GGK03, Gil07, HRL09, HLH00, HHC05, KP00, Lev01, LLL06b, MKY08, NRR00, PC05b, PLJ05a, QC05b, Sha01d, Sha04b, Sha05d, SCL05, TCC02, UP05].

digital [WNQ08, WHLH03, XC05, XMST07, Ano09, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, KCR04, Nat00, PK03, SA02].

Digital-Audio [WNY09].

Digital-Signature [Eng00].

digits [Che04b, Ran55, Ran01]. Dimension [DD+06, TZZ09a, TZZ09b].

Dimensionality [SBG02], dimensions [CLR09]. Direct [BM05, KG09].

directional [PJJH01]. Directions [Sha01b, DFH01]. directly [JZCW05].

directories [C+02, Pet03]. directory [C+02].

disabled [Pau02a]. disadvantage [CDS07]. Disappear [Per05].

Disappearing [Way02b, Way09]. Disaster [WCZ05]. disciplinary [SM08]. disclosure [JM07, Swi05].

Discovery [Bi09, HLL+02, SBG07, SGA07]. Discrete [CS03a, CNS02, Che04b, CWW02, Gen00, GV05, GPP08, LW02, LLL05, VK07, HNO4, HW03a, HWR09, Hwu05a, HLU05, JL03, JLL01, LHL03a, LH05, LTH05, PLJ05a, QC05b, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SCS05c, Yas08].

discretized [MA02]. Discription [Har07b].

discursive [Mit02]. Discussion [Ana01a, Ana01b, Ana01c, Ana01g, Ana01h, Ana01e, Ana01i, KLB+02a, Mal02, Nik02b].

Dishonest [GKK007]. Disk [Cro01, Har07b, Siv06, CS08a, Fer06].

dispatches [Kee05]. displayed [CGV09].

Displays [Kuh02a]. Disputed [CAC06].

Distance [CGFSHG09, CPHX04, DM07b, DW01].

distinguished [HWW04, WH02b].

Distinguishing [HSR+01]. Distortion [BGI08, CS05b]. Distortion-Free [BGI08].
Distortions [SDF01]. Distributed [BCS02, BT02, CLK01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJKR03, GSVC02, GTH02, SCF01, WT02, And08, AFGH06, BDET00, CO09, FMY02, KKL09, LN04, LLW08a, MSP+08, PS08a, Raj06, WZB05, YbJf04].

Distribution [BDF+01a, BOHL+05, BBB+02, BSNO00, FS01b, Ina02a, Ina02b, Ku02, LLL02, NA07, Sch01a, YI01, ATS04, CYH04, GL06b, MP08, SL07, Shp01, Shp04b, WHHT08, YS04, ZLG01]. Distributions [CY08].

Diversity [Kun01]. Divide [SKQ01]. Division [Tan07a, Che08b]. Divisor [KM01a]. DL [HRL09, PLJ05b, Sch01f, Sch01e, WMDR08]. DL-based [HRL09, PLJ05b].

DL-encryption [Sch01f]. DL-keys [Sch01e]. DL-STDM [WMDR08]. DLP [MSV04]. DM [Eag05]. DNA [GPX08]. DNF [BGN05]. DNS [Kle07]. Do [Bur06, HSR+01, HR04b, Win01, BB79].

Dobb's [Dr.00c]. Document [ISO05, PJH01, ST01c, VHP01, CDS07, CL04c]. Documents [PJK01, AW05, AW08, GA03, ÜG08]. Does [AB01, Pie05, Con09]. Doing [BM01a].

Dolev [BDNN02, ZD05]. Domain [AS08, Bar00c, BSC01a, BSC01b, BSL02, CJK+04, Cor00b, Cor02, DOP05, DPN07, GW01, ISSZ08, Kuh02a, Lan00d, LZ01, MM01a, OMT02, PBC05, SOHS01, SDFH00, ZLK02, BR06, DSP01, EKRM01, Zir07].

Domains [BR01, CLK01a, CLK01b, Vau01]. Domingo [CKN06]. Dominic [Rot07]. Dominican [PY05]. domino [LLL06a, LLL06b]. don't [Win05c].

Don'ts [FSSF01]. DONUT [CLLL00]. Door [SF07]. Doors [Eri02].

DOS-Resistant [An001c, ANL01]. Double [ADD06, CY08, CMJP03, Coc02a, DIM08, GH08, GB09, HAu06, JSW05]. double-base [DIM08]. Double-Gate [Coc02a].

double-Size [CMJP03]. double-trapdoor [JSW05]. Doubling [FV03]. Douglas [Spr03]. Down [BBPV00, Coc02b, An003b, An003a, PBVB01, Ste05c]. Downwards [FV03]. DPA [SGB01, TV03]. DPA-Based [SGB01]. DRAFT [Dwo03].

dracatic [Sug03]. drawn [vOT08]. DRBG [Hir09]. Dress [Ahn08]. drinks [An003b]. Drive [NP07, Kor09]. DSA [MR01a, SA02, Sha01d, TvdKB+01].

DSA-type [Sha01d]. DSEA [LLLZ06a, LLLZ06b]. DSP [Geb04, WWP00]. DSP-embedded [Geb04]. DSPs [WWP00]. DSS [An009, An10, FIP00, Nat00]. DTD [PCK02]. Dual [KH04, LKL05, SF07, ST03a]. dual-field [ST03a]. Dual-Tree [LKL05]. Dumb [Eri01]. Dummies [Cob04].

Dump [KCJ+01]. Dunaynir [MAaT05]. d’une [Car00]. Durahim [MAaT05]. Durahim’s [MAaT04]. during [AJ08, Bec02, WA07]. Dust [KGS07]. Dutch [dl00]. Duty [ZGLX05]. Dwork [DNR03, GK05, Zha06].

DWT [LHS05, PBC05]. DWT-Based [LHS05]. Dynamic [AFB05, BNP08, BCP01, BCP02a, CL02a, CW09, CCD+04, CTT07, GTH02, HQ05, Pat01, Sug03, TT01, BBG+02, GL06b, LCP04, LCK04, LCC05, RG05, Yi04].

dynamic-key [LCP04]. dynamics [BGP02, MR00].

e-business [HHSS01]. e-commerce [BM03a, Gra01, SN07, Sta00, MY01].

E-Goods [NZCG05]. e-Government [RM02]. E-Learning [CAC06]. e-mail [LL04b, All06, ANR01, KS00a, Law05].

e-payment [Has02]. E-Security [NDJB01]. E-smart [AJ01b]. e-voting [CJT03, Cha04].

E-Wallet [ETZ00]. E0 [LV04]. E2 [SKU+00]. Early [ASW+01, Nik02a, Nik02b, Pag03, Riv03, Snu04, ZGT05]. Easier [Pau09]. Easy [GR04, Hos06b].

Eavesdropping [Kuh02a, Kee05]. eBook [An002b, WWL+02]. EC [SF07]. ECC
[BWBL02, CL09, Mis08, TSA05].

**ECC-based** [CL09, TSA05]. **ECC2K** [LM08]. **ECC2K-130** [LM08]. **ECCV** [MJ04, TB02]. **EDCSA** [ANS05]. **Eclipse** [Coc02b]. **ECMA-305** [ECM00a]. **ECMA-306** [ECM00b]. **economics** [Ble07].

**ECC2K** [LM08]. **ECCV** [MJ04, TB02]. **ECDSA** [ANS05]. **Eclipse** [Coc02b]. **ECMA-305** [ECM00a]. **ECMA-306** [ECM00b]. **economics** [Ble07].

**ECC2K** [LM08]. **ECCV** [MJ04, TB02]. **ECDSA** [ANS05]. **Eclipse** [Coc02b]. **ECMA-305** [ECM00a]. **ECMA-306** [ECM00b]. **economics** [Ble07].
Embrace [CNB+02]. Embracing [Web02]. Embracing [Ano03b]. EMD [BR06]. Emperor [Smi01b]. Empirical [HW03b, Goo00]. empirically [SS03]. Emptiness [DIS02]. Emulex [CZB+01, CTBA+01]. Enabled [Por06, CYY01, DY09a]. Enabling [Web02]. encapsulation [CHH+09, KG09]. Encipher [BR00a]. Enciphering [HR03, KT01]. Encode [BR00a, BKN04]. Encode-Then-Encipher [BR00a]. Encode-then-Encrypt-and-MAC [BKN04]. encoded [WMS08]. Encoding [JT01b, RS00, Lin02]. encounter [Win05c]. Encrypt [BKN04, BTTF02, DAV01, Pet05, Dav01b]. Encrypted [BBK03a, BGHP02, BGLS03, CD01b, Hug04, Lan04a, LH07, RMCG01, Sta02b, Vau01, WRW02, Woo00, Biih02, BN08, CCM09, CDD+05, CH+08, FJ04, HILM02, Hes04a, LSH00, Pet03, UG08]. Encrypting [Por06, RC01]. Encryption [ABC+05, Abe01, AS01a, Abe04, AP09, AB01, ADR02, Ano03, Ano01f, AN01, AFI06, AF03, Bar00c, III00, Bau02b, BN00a, BR00a, BBM00, BBDP01, BC02, BF01b, BF03, BB04, BGW05, BCHK07, BGH07, BPR+08, BB03, BNPW03, BD03, BKY02, Bur03, CD00, CS03a, CHK03, CHK05, CCM01, Che01a, CTLL01, Chio8, Chio8a, CM06, Cla00a, Coo02b, Cox01b, CJNP00, CHJ+01b, CD01, CS02, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DF+03, DK05, DS05, Dri02, FIP01a, FL01a, GC01a, GS00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HSH+08a, HS02a, HZX05a, HSHI02, HSHI06, HKR01, HWW05, HAR0, Hei07, HS00, HR05, HG03, HL02, HGNP+03, HLL05, HLC08, ISSZ08, Joh03, Jol01, JK02b]. Encryption [JJ02b, JMV02, JKRW01, Jut01, KB03, KSY01, KS00a, KY01a, Kha05, KK+07, Kos01a, Kra01, Kur01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, Lin03, LNP02, LM05, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, Mö03a, Mor05, Mül01a, MS09c, NIS00, Nam02, NZCG05, NP02b, Nie02b, PV06b, PM00, Pau09, PDMS09, Pha04, Por01, PS00, Pre01, RM04, RK06, RJD+01, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQL03, SPPQ06, SBZ02, TV03, Un00a, Un00c, Un00e, Un00g, Un00h, Ust01b, VMS05, WZW05, WBRF00, YEP+06, YW06, ASW00, Abd01, AKSX04, AMRP00, ABW09, Ano00c, Ano02a, App05, Ate04, AC05, AFGH06, BKN04, BR04, BNN+09, Ber09a, BBK+03b, Bir07, Bla00, BJN00, Bro05b, CS08a, CBSU06, CHC01, CKRT08, DZ01, DL07. encryption [DR05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GGG03, Gen09a, Gen09b, GKM+00, Gou09, Gu05, HSH+08b, HSH+09, HS02b, HHHW07, HCD08a, HCD08b, HAN04, HW02, Hsu05a, Hwa05, HL05c, HL05d, IM06, JK01a, JK01b, JXW05, JS05, JZCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Küh08, Lab00, LV07, Lee01, LCP04, LJo05a, LMC+03, LLL06a, LLZ06b, LLCL08, LB05, Lu02, Lud05, LK01, LWK05a, Mar05b, Mat02, Mül01b, NK06, OS07, PBMB01, PS01a, Pau02a, Pau03, RG09, Rho03, RB03, RSP05, SN00, SKW+07, Sch00a, Sch01c, S03, Sch04a, Sch04b, Sch05a, Sch01d, Sch01f, SR00, SVEG09, Sp04b, SWH+09, Tan01, TTZ01, TO000, TM01, TLH05, Un00b, UP05, VKS09, WG02, WN95, WH02a, XY04, Yan02, YGZ05, YZ009, YC07, ZLG01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05]. Encryption [CHKO08, CHJ+01a, RR04, Un00f, Wue09, Jan08]. encryption/cipher [HAU04]. encryption/decryption [OS07]. Encryptor [LMP+01, TPS01]. Encryptor/ Decryptor [TPS01]. Encyclopedia [Bid03, vT05]. End [KCD07, Per03, SKKS00, WWGP00, YSR01, SU07].
End-to-End [YSR01]. Ended [Küs02].
Endomorphisms [GLV01]. Endpoint [Kad07]. Ennemies [DM07b]. Energy [GC01b, Ino05, LPV+09, SLP07, Mis08].
Energy-efficient [LPV+09]. Energy-security [Ino05]. enforce [SN04].
Enforcement [GN06]. enforces [BP05]. Enforcing [GMM08, HRS08].
Engine [Fri01, MMH02, DP04, SHL07]. engineer [Pau02b, SN04]. Engineering [CNB+02, MNT+00, MYC01, Roy00b, SM07, TR09a, TR09b, VH09, And08, EC05, Jen09, Man08]. engineers [Pri00]. engines [PM08].
Enhance [ZWC02]. Enhanced [JKRW01, ZGLX05, OP01b, TWL05, WHH05, SLP07, Mis08].
enhanced-security [OP01b].
Enhancement [CJ05, LSH03a, LSH03b, YJ00]. enhancements [ADH+07]. Enhancing [BDK02a, MS05a, App05, TCR03].
enigma [Rob02, Cas06, Chu02, DB04, GO03, Goo00, Joy00, KS04, SM00c, SM05, SE01, Wil01a, Win05b, Win00].
Enough [CNB+02, Pat03a, YJ00].
Enrolment [HWH01].
Entangled [Bar00c, LB04]. Enterprise [BH00b, C+02, HM05, MZF07, App05, TCR03]. Entropic [DS05].
Environ [HWH01].
Environment [BST03, DeL07, HS01, LSVS09, IM06, KKL09, KB00, Rhi03, ZBP05].
Environmental [PS05]. Environments [CJK+04, LKHL09, BGM04, MN08, SB05, SB07, SN04, YC09, YJ04].
ephemeral [Mis08]. Ephemerizer [Per05]. EPPOC [JQY01]. ePOST [MPHD06]. EPR [Ina02b].
equation [FJ03]. Equations [CP02, DDG+06, GS03, PBMB01].
equipping [DMT07]. Equityability [DBS01].
equivalence [Fis01a, LQ08, MSV04]. Equivalent [Fer00, KOMM01, May04, SIR04]. Era [MP00, Uni00c, Bur00, Uni00f]. erasure [PCS03]. Erasures [JL00]. ERP [LSZ05].
Erratum [AGGM10, Kwo03b, LLLZ06a].
Erroneous [CH01b, MNT+00]. Error [BBK+03b, BQR01, Dinh05, KKG03, LW05b, LM02, MSL01, MPSW05, MZ02, NN06, SK01, YI01, YD001, ZYR01, Zol01, Gar04, LHL04, YW06]. Error-Correcting [NN06, ZYR01]. Error-Prone [MCL01].
Errors [AD03, AL07, Reg05, Reg09]. escape [Bhu09]. Escrow [AK02a, Ano01a, CL01a, DBS01, LCK01, ATSVY00, CL02b, LCC05].
Escrowed [PS01b]. eServer [AV04].
ESORICS [dCdVSG05]. essays [MA07].
Essential [Cop04b, Dr.00c, MR02a, MR02b]. essentials [HHL+00, Irw03]. establishing [Kov03, KH03]. Establishment [NIS03b, HMvdLM07, SL05a]. Estimation [EFY+05, JX05, KLB+02a, LNL+08, Sel00].
ethical [Har05b]. Euclidean [CPhX04, CMJP03, CLZ02, WL02]. EULA [WWL+02]. EUR [Eag05]. EUCRYPT [Bih03, CC04a, Cra05a, Knu02, Pre00, GJSS01].
Eurographics [MFS+09].
Europe [Pag03].
European [AL06, CZ05, KGL04, Pre01, dCdVSG05, Che08b, Pre02a].
EUROPKI [AL06, CZ05, KGL04]. EV [HTJ08].
Evaluate [Pre02a]. Evaluating [BGN05, NTW07]. Evaluation [BSC01a, EYCP00, FS00, FML+03, IKM00, YJ00, JTT00a, Kan01, Krs00, SKK050, BZP05, FXAM04, FS03a, LCP04, MCHN05, RC05, RN00a, RN00b]. Evaluations [LM02].
Evangelizing [Coc01a]. evasion [Bhu09].
even [Bih02, OS00, Win05c]. EventGuard [SL05a]. Everlasting [DR02d]. Every [TH01, DKK07, Win05c]. Everything [CTBA+01]. Everywhere [Ber00].
Evidence [Ver01, Bro05a, HW03b].
Evolution [DF01, Ree01, SP02, Sin99, Sin00].
evolutionary [LMSV07]. Evolved [LMHCETR06]. Exact [Cor00b]. examines [Nis03a]. example [Bla00, GC05, Zir07].
Exchange [BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JL08, KOY01, KY03, MPS00, Mac01, MSJ02, Ngu05, VPG01, WC01a, WV01, ZWCY02, BBG +02, BCP07, CLC08, CWJT01, GL06a, GMR05, HTJ08, KS05a, KOY09, LW04, LHC08, LSH00, MS03a, Miˇs08, YC09, YPKL08, ZYW07, CPP04, CP07, ECM00b], exchanging [KN08]. Exclusive [GRW06]. Executing [HILM02, LJ05a]. Execution [Coo02]. Exhaustive [Des00c]. Existing [MV01, BDET00]. Expanded [Cho08a, Irw03]. Expanding [DN02a]. expansible [LLW08a]. Expansion [DN02b, BCD06, HKPR05]. expansions [HKPR05]. Expected [KL05, RK06, DLP*09]. Experience [Sas07, BCHJ05]. Experiences [MPHD06, USE00b]. Experimental [BG09, CGBS01, ¨OOP03, WS02, RSQL03, Smo04]. Experimentation [Hun05]. Experimenting [LSVS09]. experiments [Bru06]. Expiration [MP00, Sch05b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOBH05]. exploitation [Eri03, Eri08, KVN*09]. Exploiting [CK06, ETMP05, HR00, HM04, ZWC02]. Exploits [MJF07, CSW05]. exploration [SKW*07]. Exploratory [Lut03]. Experiment [BP04, BM01b, DN00b, May02, SZ01, CKY05, Duj08, GD05, Shp04b]. Exponential [BP04, BM01b, DN00b, May02, SZ01, CKY05, Duj08, GD05, Shp04b]. Exposure [BP04, BM01b, DN00b, May02, SZ01, CKY05, Duj08, GD05, Shp04b]. Exponential [BYJK04, BYJK08, CY08, GKK*07, GKK*09, Shp05]. Exponentiation [KKH03, SK07, CKRT08, HGNS03]. Exponents [FS02, FS01b]. Exposed [Gun04, MSK03, SS06]. exposing [YY04]. Exposive [MAaT05]. Exposure [BM03b, DSS01, KZ07, CDD*05, KZ03]. Exposure-Resilient [DSS01, KZ07, KZ03]. Extended [ABDS01, BPS00, CM00, Cou04, DIRR05, HLvA02, HJW01, JL00, MSJ02, MP02, OST05, Wag02, BJN00, CD00, HT04, HP01, Mis06, Pei09, QPV05, LKJL01]. Extending [ADDS06, IKNP03, Ove06, Sal03b, SS01a]. Extension [BAI01a, YWD08, BR06, CMDV06]. Extensions [ABC*05, BBGM08, CS07c, HM02b, Rot02a, Wei04]. Extracting [Cer04a]. Extraction [DGH*04, RW03a, MB08]. Extractors [Fis05, KLR09, KZ07, Lu02, Vad03, DW09, KZ03, Sha04a]. Extraordinary [Top02]. Extreme [Ano02b]. Extrusion [Be06]. Eye [Sas07, CAC03]. Eye-Opening [CAC03].
PBMB01, WWA01, Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d. Faster [Bar00c, CMJP03, GLV01, KS09, LV04, Oec03, Ban05, Why05]. Faszinierende [Sch09]. Fat [MVC01, TvdKB+01]. Fault [Ano04a, BMM00, BK06b, BKM07, DS03, Gir06, PV06a, PQ03, YKLM02b, HGR07, Lin07, PI06, RMH04, YJ00, YKLM03, ZL04a]. fault-based [YJ00]. fault-tolerant [HGR07, Lin07, RMH04]. Faults [GSS08, VS08]. fault-based [YJ00]. Faults [GSS08, VS08]. Fawzi [MYC01, TvdKB+01]. Feasible [LM08]. Feature [GW01, Gut02a, LNP02, LLC06a, NN03]. Features [PK01, SBG02]. February [DR02c, Fra01, GH05, Joh03, Jue04, Kil05, Kim01, Men05, NP02a, Nao04, Oka04, PY05, Poi06, Pre02b, RM04, Syv02, USE02a, Wil99]. Federated [DeL07]. Feedback [CGFSHG09, CM03, Cou03, Igl02, ST03a]. FeedForward [BP01a]. Feel [PM00]. Feeling [Buh06]. Feistel [Cou04, Kan01, LMS07, Oni01, Pat04]. Feldman [AF04b]. Ferrer [CKN06]. Fetal [MYC01]. fetch [HTW07]. Fi [Sty04, Bar03]. Fiat [VS08]. FIDES [ISTE08]. Field [FJ03, GC01a, RDJ+01, GMG00, Has00, JL03, ST03a]. Fields [Bai01a, BT02, CU01, Che04b, CQS01, CFS05, HCK09, HM01, KKH03, Lov01, MNP01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sim02, Sma01]. Fifth [ACM03b, SM07]. Fighting [DGN03, SZ03]. File [CCDP01, GIS05, Ito01, LK01, BDE00, CHK+08, HTW07, Hos06b, ISO05, MKK00, MSP+08]. Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pet05]. Filesystems [WBL01]. Filter [LBGZ01, LBGZ02, MSNH07, Sar02, CMS08]. Filter-Combiner [Sar02]. Filtered [MH04]. Filtering [SDFH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00]. Finalists [EYCP00, IKM00, IK00, IK01, Mes00, Mes01, SKKS00, SW00a, WW00]. Finally [Coc02b]. Financial [ANS05, Gri01, Wri03, Fra01, Jue04, PY05, Syv02]. FINDsomeone.com [Gra98]. Fine [SS01b]. Fine-Grained [SS01b]. Fingerprint [Ano02b, HLY07, HBF09, KHY04, MMY02, CL04d, MJP03, UBP09]. fingerprint-based [CL04d]. Fingerprinting [KT01, CTT07]. Fingers [TK03, KLY03, Sco04]. Finger [MMY02]. Finite [BLST01, BR01, CU01, Che04b, CQS01, HCK09, WW05, KKH03, MM07b, PHK+01, RS08, Ver02, Gar04, Has00, LMC+03, LQ08, NS01a, RMH04, Sma01, SLTB+06, TC00]. Finkenzeller [And04]. FIPS [Nat00]. Firewall [LJ04]. First [Bar00a, BBD09, CM02, CM+05, FLY06, KGL04, MNP01, Nao04, NNT05, ÖOP03, PK03, QSR+02, Roy00a, USE00b, Wil09, ZJ04, ZHY03, AJ01a, Cha00b, Coo02a, DV05, RH00, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, Lan00a]. Fish [Fie09, Wei00, Wei05]. Fix [CCM05]. Five-lecture [Rot02b, Rot03]. five-lecture [Rot02b, Rot03]. Fix [TEM+01]. Fixed [AR01, BCC01, CKN00, LS01a, Shp04b, SP09]. Fixed-Length [AR01, CKN00]. Fixed-Pattern [BCC01, LS01a]. Fixing [KZ07, KZ03]. FL [Des02, Jue04]. flash [ST06, SGB01]. Flat [SV08a]. Flaws [Gra02a, SPM02, Vau02, SL05a]. Flexibility [LP02a]. Flexible [CMG+01, CLK01b, OT03a, Tsao01, BA06, KC05, LHY02, WW00]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM+09]. Flows [ECM00a, AHS08, Cer04a, Lau08a]. Flying [Fox00]. FOCS [IEE02, IEE03, IEE04].
IEE05a, IEE06, IEE07. FOKSTRAUT
[BH00a]. Foo [Puz04, VGM04]. Food
[MNT°00]. Fool [RW02]. Footsteps
[Lav06]. force [Cur05, SGA07]. forces
[AJ08]. Ford [Mar05a]. Forecast [Rai00].
Forecasting [WWL°02]. Forensic
[PS08b, Cas02, Kor09]. forensically
[ME08b]. Forensics [JBR05, CS08a, CDS07, MS09a, MKY08, MAC°03]. Forest
[FBW01]. Forgery
[CH01a, CCM00, LS01a, SLT01, HSW09]. Forgotten
[Eag05, Kin01, OC03]. Form
[ADI09, CH07c, OS01, LKYL00, Mic01]. Formal
[BGB09, BCHJ05, BCJ°06, CL05, DKS08, GOR02b, HG03, Lan00d, Mea01, YWD08, JW01, Mea04, ZLX99, ZL04b]. Formalizing
[HM01a]. Formally
[BJP02]. format
[ISO05, RG05]. format-string
[RG05]. Formats
[GIS05]. Formats
[JTO1b, LLL04]. Formula
[Kog02]. Formulae
[CH07b, WPP05]. Formulas
[BGN05]. Formulations
[AHRH08]. Forum
[CBZ°01, CTBA°01, CNB°02, CMB°05]. Forward
[AR00, AF106, BY03, CHK03, IR01, HCD08a, HCD08b, ZYW07]. Forward-Secure
[AR00, AF106, CHK03, IR01]. Forward-Security
[BY03]. Forwarding
[KCD07, Kra02b]. FOSS
[Bo102]. Found
[Bar00a]. Foundation
[Lut03]. Foundations
[DKK07, Gol01b, Gol01a, Gol04, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Nie02d, Sal05d, Kat05b, Puc03]. Founder
[Bar00a]. Four
[LX0°01]. Four-Layer
[LX0°01]. Fourier
[Che07, DSP01, DNP07, LPZ06, SP04]. Fourteenth
[USE00c]. Fourth
[ACM02, ACM05b, DFCW00]. FPGA
[Ano02c, CC02a, CGB01, CG03, CNPQ03, EYCP00, EKKH04, KMM°06, KY09, KBM09, KR02°02, LP02a, MM01b, MM01c, OTIT01, OOP03, Pat01, PBTW07, QSR°02, TYLL02, TPS01, USS02, WW00]. FPGA
[AD07, DPR01, MM09, RSQ03, SG09, SK05a]. Fractal
[AA04a, MLMS03]. Fraction
[Wal03]. fractional
[DSP01, SSST06]. fractions
[Dan02]. Fragile
[CH01b, CT09, Nak01, PKJ01, LYGL07, SY01b]. Frame
[LHS05]. Frames
[HW005]. Framework
[ANRS01, GL03, GOR02b, Hun05, NMO05, NP07, PS06, RSO, Syh02, ZYN08, AHK03b, CCCC01, CP07, CC04c, DMSW09, GJJ05, GL06a, GM04, JER04, KNS05, MS09b, MBS04, YCW°08, HF00]. France
[ACM04a, ACM05a, AJ01a, AJ01b, GH05, KNP01, NP02a, PPV96, KM07]. Francisco
[Cal00c, Joy03b, Men05, Nca01, Oka04, USE02a, USE02b]. FranzSteiner
[Eag05]. fraud
[An00a]. Fred
[Bar00b]. FreeBSD
[AP09, An002c, Bau01a, Bau01b, BGI08, Coc01a, CNV06, DG02, HS00, HM01b, JP03, Jut01, Fox00, SGB05, Bol02]. Freedom
[Uni00a, Uni00c, Uni00d, Uni00e, Uni00f, Mi003]. FREENIX
[USE01b, USE02c]. French
[Wri03]. Frequencies
[DD02]. Frequency
[OMT02, Sak01, SOHS01]. Frequency-Domain
[OMT02]. Frey
[Was08a]. friar
[GG05a]. friendly
[CRSP09, Hsu05b, HL05b, SZS05, WLT05a]. FrontPage
[WWL°02]. FSE
[BI07, DR02c, GH05, Jho03, Mat02, RM04, Sch00b, Sch01d]. FTC
[St05c]. Full
[Cor00b, DOP05, LKLH09, WYY05b, WYY05c, BI04, CS08a, HS02b, LKH°08, Oiw09]. full-encryption
[HS02b]. Full-Round
[LKHL09, LKH°08]. Fully
[BL08, FS01a, Gen09b, KPMF02, RG09, Gen09a]. Function
[BR02, CDMP05, Fis01b, Fhu02b, GIC05, HNO°09, HPC02, JJO0a, Kan01, KI01b, Nie02a, RB01, Yan05, CHY05b, CJ04, HR07, LW04, LPM05, WWH08, YW05, YRY05b]. Functional
[ECM00a, WA06]. Functionalities
[PS05]. functionality
Functions
[AEMR09, BBDK00, Bon01, Can01b, CV02, Car02, Che01c, DN02a, DGN03, DNRS03, Fil02, FIPR05, GLG+02, HMS04, HR04b, Jou04, Ki01b, LTW05, Lys02, PR01, RR08, SM00a, SM00b, SS01a, Sho00a, Sho00b, Ver02, WP03, WFLY04, Wer02, AGGM06, AGGM10, ALV02, CS09, GVC+08, HR08, ISO04, KK07, LLH02, LKY04, MS02b, Mic02a, Mic02b, NR04, PW08, QPV05, SM03a, YRY04, ZW05a, RRS06].

Fundamentals
[And04, PHS03, Shi08, Way01, vT00, Fin03].

Funds
[Coc01a].

Further
[JS05, LL04a, LL05c, MP07, YRY05a].

Fusion
[KZ09, TZDZ05, ZS05, BG09].

Fuzzy
[MAaT05].

Future
[ASW01, Joh00, LNP02, NFQ03, Sch00e, LPW06].

Fuzzing
[SGA07].

fuzzy
[HS02b, NC09].

fuzzy-based
[NC09].

G
[Coc03, For04, Was08a].

Gaitherburg
[SMP+09].

Gamal
[EKRMA01].

Game
[DHR00, LM02, CAC06, BR04, Gou09].

Game-like
[Gou09].

Game-playing
[BR04].

Gamers
[MP00].

Ganesh
[KN08].

Gauss
[KKH03].

Gaussian
[EKRMA01, JL03].

Gbps
[TPS01].

GCD
[JP03].

GCD-Free
[JP03].

GCM
[KS09].

Geeks
[McN03].

Geheimschreiber
[Joy00, UW00].

GEM
[CHJ+01a, JMV02].

General
[AB09, CDM00, DN00a, ESG+05, GMP01b, Kog02, Lin03, MND+04, Sal01a, YC01, IY06, JL03, JL05a].

General-Purpose
[ESG+05].

Generalisation
[DJ01].

Generalization
[YYZ01, HWW02].

Generalizations
[LD04].

Generated
[ADD09, MRL+02, RBF08].

Generating
[BMK00, BCDM00, GG01, MFK+06, SS03].

Generation
[ACS02, BH05, BK06a, CS03c, ESG+05, GJKR03, GL01, GW01, JG01, MR01a, Ram01, TL07, TV03, WP03, WHLH05, Web08, WS02, Ano04c, BK07, BG08, BF01c, ISTE08, LS05b].

Generator
[ADD09, BP01a, DI05, Di03, DGP07a, DGP07b, DV08, EHK+03, Gen00, GM02a, Gol01c, GPR06, Int03, Ke10, LMHCTR06, LV04, SX01, SDFD06, TWNA08, TZZT9a, TZZT9b, ZK01, Aam03, ACTZ05, Be10, BG08, BG07a, DGP09, GB09, HG05a, HlwWZ09, JAW+00, KH08, KSF00, Pan07, PGG+09, PPS+08, PC00, RGX06, SR07, SB05, UHA+09, WW08, VKS09].

Generators
[BST03, BK06a, BL08, CF01b, CS05a, Fin06, Kra02a, LBGZ01, LBGZ02, LS09a, MH04, RSN+01, Vav03, BK07, BGP08, C009, SK01b, Ts06, YZEE09].

generators-part
[SK01b].

Generic
[BK06a, DGP09, GJKR03, CV05, SCS05a, WJP07].

Genarro
[Miy01].

Genarro-Krawczyk-Rabin
[Miy01].

gentle
[RR03a].

Genus
[HSIR02, LMHCETR06, CV05, SCS05a, WJP07].

Gennaro
[Miy01].

German
[Sch09, Ano04b, Lin02, Mor05, Sal00b, Sal00a, Win05b].

Germany
[DRS05, Duw03, FLA+03, WKP03, IEE01b].

Geschichte
[Sch09].

Get
[Coc01a, WD01, Cla00b].

Giving
[PM00].

GF
[BINP03, KPMF02, LKY02, KKY02].

GH
[GH01].

GHS
[HS04a].

giant
[Lam07].

Gibson
[Ove06].

Giesbrecht
[CHH01].

Gigabit
[GGS01, HGS01].

Gigabits
[HTS02].

Give
[CNB+02].

Given
[Wal03].

Giving

Global [Wu01].

Globus [MJD01]. GN [SC05b].
GN-authenticated [SC05b].

Gnana [For04].

GNU [Coc01a].

GNU Privacy Guard [For04].

GnuPG [JKS02, Sti06b].

Go [For04].

Gold [PHM03].

Goldreich [Kat05b, Lee03b, Puc03, AC02].

Gong [GG01].

Good [CB01, Kid02, MP06, GG05b, vT01].

Goodness [CMB+05].

Goods [NZCG05].

Google [Con09, Law09b].

Googling [Con09].

GOST [SK01a].

Goubin [Sma03b].

Governance [TPPM07].

Government [IY00, RM02, Lev01, LCS09].

GPG [Bau01a, Bau01b, Luc06].

GPS [CKQ03].

GPT [Ove06].

GQ [BP02].

Graduate [GV09].

Grafton [Pag03].

Grained [SS01b].

Grand [Syv02].

Graph [CGFSHG09, GTTC03, HM02b, VVS01, YKW01, CTT07].

Graph-Based [CGFSHG09, HM02b, CTT07].

Graphical [vOT08].

Graphics [CK06, DNP07, MFS+09].

Graphs [NNT05, Ust01b, WGL00].

Gravilenko [Puz04].

Gray [FGD01, Har05b].

Gray-Scale [FGD01].

grayscale [YCL07].

Greedy [Bel07].

Greece [ACM01a, KGL04, SM07].

Greedy [Bel07].

Greek [TR09a, TR09b].

GREMLIN [Hof01].

Grenoble [ACM05a].

grey [BDN00, SCS05a].

Grid [ACM05a, MJD01, SEF+06, TLC06, ZBP05, Cha07, CJK+04].

grids [MPPM09].

Grip [Buh06].

Gröbner [CCT08, FJ03, Fau09].

Group [ANRS01, AAFG01, ACJT00, BBS04, BCP01, BCP02a, BCP02b, CD00, ČtTMH01, CH01a, HSHI02, HSHI06, HW04, Hug02, JPT0b, KY03, Kin02, LYL+09, MSU05, SOOJ02, SWH05, Ste01, Tan07b, VMSV05, Wer02, AKNRT04, BCP07, CL04b, CU04, CHC05, CWVT01, CTV04, Cho08b, ED03, Heo02, Hen06, HWW02, KS05a, KPT04, KKL09, LL06, LLLH04, LPM05, LWWK05b, NS05b, RH03, SNW01, Sha05a, TJ01a, Tse07, WGL00, WHHT08, YLC+09, YY05a, ZC04, ZXL+04].

Group-by [YL+09].

Group-Oriented [LZL+09, HW04, CH05, CWVT01, LL06, TJO1a, WHHT08].

Groups [BSS02, CV03, CF02, DRE00, GM02a, GST04, KM01a, KLC+00, LLH01, LP03, Luc02b, MN01, PHK+01, GR04, HM00, Pao03, YI04].

GSM [BBK03a, BD00a, Cha05b, Cim02].

Guadeloupe [Wri03].

Guangzhou [LLT+04, Li05].

Guessing [AGK07, Bau05, Shi05, YS02, DLMM05].

Guest [KP03, Sak01, BK06b, MFS+09, PTP07, SJT09, SGK08].

Guide [Ano06b, BS01a, BSB05, BCP+03, BP01b, HM04, PO03, Vac06, Wei04, And08, Bon00, Bro05b, C+02, Che00, Gar03b, Kov03, Lun09, Mo05, SL06].

Guidebook [SEK01, SEK02].

Guided [ZY08, Pet08].

Guildford [KN03].

Gummy [MMYH02].

Guo [LLLZ06a, LLLZ06b].

Gutmann [Uzu04].

H [Was08a].

H.R [Uni00d, Uni00h].

H64 [GMP01].

Hack [MYCO1, Sin02, SL06].

hacker [Gol08, Har05b].

Hackers [SEK01, SEK02, BD04b, NRR00, Win05c].

Hacking [Eri03, Eri08, Gym04, Man08, MSK03, SSOJ06, VGM04, Puz04, Har05b].

hacks [Sti06b, Sti06a].

Hadamard [HW05].

Hagenberg [Jef08].

Half [HS02b].

Half-encryption [HS02b].

Halfspaces [KS06].

Hall [Bar00c, For04, Kat05b, Was08a, MAaT05].

Hall/CRC [Kat05b].

Hall/CRC [Kat05b, Was08a].

Halmstad [BS01b].

Hamming [GK02].

hamper [Lov01].

Hand [WBL01].

Handbook [And04, Cas02, CFA+06, Jan06, MMJP03, RE03, AB09, Fin03, Har05b, KB00, KH03].
High-assurance [Jen09].

High-Bandwidth [CGJ+02].

High-Dynamic-Range [CW09].

High-End [SKKS00, WWGP00].

High-Performance [Kra05, NFQ03, BZP05].

High-Speed [Ano00b, Ano02b, Gro01, JKRW01, KMM+06, SOTD00, SM02, Wie00, YKMY01, RW07, BGL+03].

High-technology-crime [KB00].

High-Throughput [HV04].

Higher [CV02, KCP01, BF01a].

Highly [CV02].

hijacking [Ste05c].

Hill [Gum04, USE02a].

Hilton [KJR05].

HIPAA [AEV+07].

historic [Pet08].

Historical [RE02, MWM01].

History [BP03b, Ifr00, Pag03, Sal01a, Sin01b, CAC06, Top02, AJ08, Boo05, HS09, KNS05, Nis03a, Pin06, Ris06, RH00, Wil01a].

history-based [KNS05].

hit [Bjo05].

HMAC [FIP02a, DGH+04, Hir09].

HMQV [Kra05].

Hoare [dH08].

Hoax [CSS02, Cha05b, DHMR07, TW07, WT02, ZC09].

Holier [MYC01].

Holistic [RM02].

Homage [JP02b].

Home [IEE00b, SEK01, SEK02, CAC03, Pet03].

Homegrown [Str02].

Homogeneous [MF07, PS02a].

Homomorphic [AS01a, Aki09, CDN01, DN03, HS00, Cho06, Gen09a, Gen09b].

homomorphism [CKN06].

homophonic [Sav04].

Honeynets [Dim07].

Hong [B+02, JZ04, Cla00b].

honor [OC03].

hook [JE204].

hooks [GJJ05].

hop [NC09, ZSJN07].

hop-by-hop [ZSJN07].

Horizon [Co02b].

host [Shu06].

hostile [ABB+04].

Hosts [H+01, SZ08].

Hot [IEE01b].

Hotel [USE01b, USE01a, USE02a].

HotOS [IEE01b].

HotOS-VIII [IEE01b].

hours [Fox00].

House [Uni00a].

Hsu [BCW05, HL05c].

HTML [CNB+02].

HTTP [Zha00].

Huang [ZC05].

Huge [MSNH07, NNT05].

Hull [KMT01].

Human [Dre00, GL01, JW05, KOY01, Man08, MS02d].

Human-Memorable [KOY01].

Hundred [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].

Hunting [GJL06].

Hwang [SCS05b, Hsu05a, HL05d, KTC03, KCL03, LW05c, QCB05a, WL05, ZYR01].

Hwang-Rao [ZJR01].

HWWM [LKY05c].

HWWM-authenticated [LKY05c].

Hybrid [AD09, KD04, LZ04, PK01, CJ03b, HG07, LPM05, TM06].

Hyderabad [MS02c].

Hype [Way02a].

Hyper [DR02d, Lu02].

Hyper-Encryption [DR02d, Lu02].

Hyperelliptic [Av03, CY02, CFA+06, HSS01, PWGP03, Ver02, Was08a, ZLK02, CMKT00, Wen03, Wol04, WPP05].

hypotheses [KW00].

I-tracings [RE02].

i.e [NP02a, Wil99].

IA [WWCW00].

IA-64 [WWCW00].

IACBC [JMV02].

IBE [ABC+05].

IBM [AV04, ADH+07, CGH+00b, Web08].

Ibn [MAaT04, MAaT05, MAaTxx, MAaT07].

Ibn-Adlan [MAaTxx].

Ibn-Al-Durahim [MAaTxx].

iButton [HWH01].

IC [BGL+03, PC00].

ICBA [ZJ04].

ICCMSE [SM07].

ICISC [Kim02, LL04c, PC05a, Won01, WK06].

ICISC’99 [Son00].

ICM [IEE09a, IEE09a].

ICs [Bar00c].

Id [JZ09, BRTM09, CCD07, CL07, CS07c, CL00, GS02b, KLY03, KHL09, Ku02, LCS09, Sco04, SW05, SCL05, WBD01, WH02b, YLH05, ZK02, ZC04, ZC09].

Id-Based [JZ09, CCD07, GS02b, Ku02, WBD01, YLH05, ZK02, CL00, KLY03, KHL09, Sco04, SW05, SCL05, WH02b, ZC04, ZC09].

IDE [An02b].

Idea [Cos03, RR03a, CTLL01, HTS02].

Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b].

Ideas [Gha07, Eri01].
Identifiers [MC04]. Identifying [HBF09, LLS05b, ZYN08, DMS07]. identities [Kwo02, Kwo03b]. Identifying [HBF09, LLS05b, ZYN08, DMS07]. identities [Kwo02, Kwo03b]. Identity [App05, BF01b, BF03, BB04, BCHK07, BGH07, BPR+08, Boy03, BRTM09, CL01a, CHM+02, Coc01b, DT03, GKO4, Her06, Her07, HY01, HL02, KC02, Mar08a, Mar08b, PCSM07, SMP+09, BM05, CJL05, GG08, KG09, LWZH05, RG09, Sae02, Sha03c, Wan04b, Win05a, YCW+08, ZYW07]. Identity-Based [BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, Mar08a, Mar08b, App05, Her07, PCSM07, BM05, CJL05, KG09, LWZH05, Sae02, Sha03c, YCW+08, ZYW07]. IDSFM [TZDZ05]. IDtrust2009 [SMP+09]. IEEE [BS03, BCDH09, BC01, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, KM07, HSD+05, Hug04, Mist08, PHM03, ZDW06]. IEM [RC05]. IFIP [DKU05, DFPS06, DFCW00, ELvS01]. II [Ban05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Hau03, Hau09, OC03, Res01a, Res01b, Sal00a, ZT03]. III [Sch00a, Ano00b, Bau03b]. IEE [CK02a, Kra03]. I'll [PLW07]. Illinois [ACM04b]. Illusions [Koc02]. illustrated [Lun09]. Im [BGI+01, DOPS04, RR05]. IMA [Pat05b, Sma05, Hon01]. Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, GW01, KBD03, LLS05a, LZO1, LWS05, LY07, LJ05b, LSCK05, RS00, SDFH00, SDF01, SFSC09, SYLC05, TTTZ01, TH01, TC01, UP05, VKS09, VK07, WY02, WLT05b, YZEE09, CC02b, CHC01, Che07, Che08a, KC09, LLC08, Lin00a, LT04, LYGL07, LLC06b, MS09a, MB08, S+03, mSgFtL05, TL02, Wan05, WMS08, YCYW07, YCL07, ZLZS07]. Image-Feature [GW01]. Images [CW09, DP00, FGD01, PZH01, PBC05, RE02, AEEr05, BDN00, FWT05, HHYW07, TCC02]. Imaginary [HJW01, HM00, Hüh00]. Imai [DDG+06, YG01a]. Imbalanced [ZWCY02]. Immersive [Coc01a]. Immune [MC04]. Imaging [CW09, DP00, FGD01, PZH01, PBC05, RE02, AEEr05, BDN00, FWT05, HHYW07, TCC02]. Impersonation [BP02, Hsu05b]. implant [Fox00]. Implementation [HQ05]. Implementations [AL00b, BJP02, III00, CTLL01, CGBS01, EPP+07, GLG+02, MM01b, MP01a, RS01, WWCW00, ASK05, BFCZ08, BFGT08, BG07b, FR08, RALT07, RSLQ03]. Implemented [TSS+03]. Implementing [Dwi04, Kor09, LM08, LDM04, MWS08, NDJB01, Pet03, Smi01a, SR06, C+02, CW02]. Implications [Kun01, LJ05a, MF01, Bjo05]. Implies [KY01e]. Imply [Pie05]. Importance [KJC+01, TIGD01]. Important [SM00a]. imposed [XLMS06]. Possibilities [CHL02]. Possibility [APV05, BPR+08, Fis01b]. Impossible [BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SK01]. improve [Pau02a, CAC06]. Improve-ment [CAC06].
Improved [AFGH06, BPR05, BB05, BF00b, CL01b, CKK+02, CJ04, DN00a, DG02, Fan03, FKS+00, FKL+01b, FKL+01a, GMR08, Gen00, HCK09, HKA+05, JQYY01, Kin00, KTO6, Ku02, Küh02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02e, PR08, ST01b, SWH05, SC05c, TNM00, ZKL01, vBKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].

Improvement [AS01c, AJ008, Che04a, CZK05, CCW02, Di 01, HWWM03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Cha05b, Sha05b, WHLH03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JSW05, JmBdXgXm05, KJY05, LL04a, LW05c, SZS05, TO01, WLT05a, YW04, YWC05, YRY05a, ZC09].

Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, SRQL03].

Improving [ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SK01, SB01, Sun02, XQ07, YEP+06, YGZ05].

Incentives [Swi05].

Incident [JBR05, Tom06].

Including [SR01].

Incomputable [Ver06b].

Inconsistencies [MS09a].

Incorporating [MFS+09].

Increase [PBTW07].

Increasing [CS05b].

Incremental [BKYO2, LKLK05].

IND-CCA [Mi01b].

IND-CCA2 [BTO02].

Independence [BP03b].

Independent [BS00a, BSL02, Kin02].

Index [Ano00a, Ano01d].

Indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03b].

Indies [Fra01, Syv02, Wri03].

individual [TW07].

INDOCRYPT [CV04, JM03, MMV06, MS02c, RD01, Roy00a].

Induced [Vau02].

Industrial [USE00b].

Industry [ANS05, ort00].

ineffectiveness [YL05].

Infeasibility [FS08].

Inference [Mar02b, CDD+05].

Infinite [TZT09a, Tzt09b, Vau01].

Influencing [Bla01c].

Inform [Kwo03b, San05].

Information [AP09, BW07, BIM00, BZ02, Big08, BB03, BJ02, Boy01, CGM07, DM00b, ECM00a, ELvS01, Hay06, HQ05, HW01, ISO04, JD01, JGG07, KP00, KR02, KLB+02b, KO00, Lai03, Lee04b, LW05b, LL01, MH05, Oka00, PP06b, RSA00d, RS01, Roy05, Sch06b, Son00, Sta06, Ste02, TG07, VDKP05, WABL+08, Yek07, Zhe02b, ZS05, vW01, ABW09, Arn01, Bid03, BK00, BEZ00, BEZ01, Bro05b, Duw03, FR08, FOP06, Gar04, Gha07, IY05, KN08, KB00, Kov03, MS09b, ME08a, PS02a, Son02, TWM+09, Way02b, Way09, CSY09, FL06, GW06, Kim02, LL03, LL04c, PC05a, Won01, WK06].

information-flow [FR08].

Information-Theoretic [VDKP05, vW01].

Information-Theoretically [DM00b].

Infrastructure [AHKM02, AL06, BC04b, BWE+00, CL07, ES00a, FL01b, KGL04, Sin01a, BHM03, BDS+09a, Ben01a, CZ05, FB01, Gor05, LCK04, MWS08, Ben02].

Infrastructures [HDO002, Lin00b, PHM03, WBD01, Bra01a, LAP08, SN07].

INIDP04 [LDM04].

initial [DK08].

Initiative [COC01a, Cal00a].

initiatives [Mau05].

Injection [MMJ05, ZSN07].

Injective [C MdV06, Kos01c].

Innovation [San09].

innovations [Web02].

Innsbruck [Pfi01].

Input [CAC06, TC00, DKL09, VM03].

Input-trees [TC00].

Insecure [Vau05b, Wal01, BJN00].

Insecurity [Bla02b, Dop05, Lal08, Man02, NS01b].

insertion [MB08].

insertion-extraction [MB08].

Insider [CMS09, Tad02, KS05a, Mah04].

Insights [Kun01].

Installation [USE00a].

instant [FS08].

Instances [GG01, HN06].

Instant [BBK03a, RR05].

Instantiated [RR08].

Instantiation [BF05].

Instruction [BBGM08, EP05, KTT07, Brn06, HTW07, MMJ05].

Instruction-Level [EP05].

Instruction-Set [BBGM08].

Instructions [Bla01c].
LSY01. instrumentation [MPPM09]. insubvertible [AcDM05]. Insulated [DKXY02]. Integer [Gro03, JL03]. Integers [CH07c, GM01a, KKM01, EKRA01]. Integral [KW02, WH09]. Integrated [EC00a, ECM00b, GMG00, Lut03, GLC+04, LK01, SSM+08, SN04]. Integrating [Wi01]. Integration [Ito00, CJL06, Sug03]. Integrity [Ano02c, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel [Coc02a, MP00]. Intellectual [Qu01, WY02]. Intelligence [Cop04b, AJ08]. Intelligent [Cos03]. Inter [WRW02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WRW02]. interaction [Gav08]. Interactions [Fau09]. Interception [CHVV03]. interdomain [MABI06, vOWK07]. interesting [SWR05]. Interface [RSA01]. Interference [FG00a, FG00b, GA05]. Interlaken [CC04a]. Interleaved [ZSJN07, NC09]. intermediaries [JA02]. Internal [Har07b, Bej06]. International [AC03a, ACM04a, ACM05a, ACM09, ACM10, Ano00b, AAC+01, AJ01b, BD04, Bel00, B+02, BB09, BS01b, Bia03, Bia03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCMR02, CCMR05, CS09, CG03, Cra05a, DR02c, Des02, DK05, DFPS06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JY04, Jef08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, Kli01a, Kim01, Kim02, KN03, Km02, KP01, KNP01, Lai03, LL03, Lee04b, LST+05, LL04c, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pfi01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Sch01d, Sho05a, Sil01, SM07, Syv02, TBJ02, TLC06, Uni00a, Vy01, Vau05a, WKP03, Wil99, Won01, Wir03, Yun02a]. International [YDKM06, ZJ04, Zhe02b, ZYH03, AMW07, AUW01, Ano00c, AJ01a, BCKK05, Bir07, BC05a, CKL05, DV05, DVML05, DRS05, GKS05, HH04, HH05, HA00, Hon01, May09, PC05a, PY05, PPV96, QS00, Sma05, Son00, ST01d, WK06, Ytr06]. Internet [SMP+09, ABB+04, Ben01a, Ben02, Cal00b, Chu02, Clao0a, Coc03, DP04, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, MC03, MA00a, Mir05, PM00, PLW07, Pv01, Pho01, PHM03, Rub01, SBB05, SE01, SE02, Sto01, Tsa01, TWL05, Uri01, WCJ05, Wir05, ZGT05, k01]. Internet-wide [SBB05]. Interoperability [Hil00, TEM+01, BHM03]. interoperable [BFGT08]. Interpolation [LW02, YG01b, FWTC05, KT06]. Interpolations [Sat06]. Interpretation [Mas04, CC04b, interpretation-based [CC04c]. Intersections [KS06]. Interstate [RM02]. intranet [Jan00]. Intrinsic [ZWC02]. Introducing [JL00]. Introduction [Ben02, Ber09b, Bis03a, BK06b, Bu00c, Bu01, Bu04, DK02, DK07, Fal07, Hay06, HPS08, HC02, KL08, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGK08, TW02, TW05, Big08, CSo7a, CM05b, Gar01, HW98, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06, Kat05b, Rot07, Lee03a]. Intrusion [CZK05, DFK+03, DP07, JT05, TZZD05, TMM05, WGO5, HLL+02, MAC+03, NCRX04, NN02, YbF04, IR02]. Intrusion-Resilient [DFK+03, DP07, IR02]. intrusion-tolerant [Ybf04]. intrusions [Bej06]. invalid [CJT04]. Invariant [Ben00, CT09, ZLZ07]. Invariants [WH09]. Invasion [ASW+01]. invasions [Tyn05]. Invention [If06]. Inventors [Bar06]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, MFFT05].
**Inversion**
[BNPS02, KKY02, KTT07, SPG02].

**Inversion/Division** [KKY02].

**inversive** [SB05].

**Investigation** [BW07].

**investigative** [Cas02].

**investigator** [Men03].

**investigation** [Cas02].

**Investigative** [BW07].

**investigator** [Men03].

**Invisibility** [Cas02].

**Invisible** [SB05].

**Invitation** [Cas02].

**Invited** [Cas02].

**involutional** [SHH07].

**IP** [CD01b, FXAM04, HL07, Lin07, MV03b, RW07].

**IP-based** [MV03b].

**IPAKE** [CPP04].

**IPSEC** [Vau02, CGBS01, Dav01a, KMM +06, SKW +07, FS00, FS03a, XLMS06].

**IPSec-Compliant** [CGBS01].

**IPTables** [GC05].

**IPv6** [Nik02a, Nik02b].

**Iran** [Mah04].

**Ire** [Cos03].

**Iris** [CJL06].

**Irregular** [MH04].

**Irregularly** [CGFSHG09].

**Irreversibility** [ZWC02].

**ISBN** [And04, Duw03, Eag05, For04, Gum04, Imr03, Pag03, Puz04, Top02].

**Island** [CSY09, KGL04, Kim01, Lee04b, IEE07].

**ISO** [GM00b].

**ISO/IEC** [ISO04].

**ISO9979** [TM01].

**ISO9979-20** [TM01].

**Isolated** [LSVS09, MMMT09].

**Isomorphism** [BW07].

**Isomorphisms** [BW07].

**Israel** [Jol01].

**ISSAC** [Jef08].

**issue** [FOP06, FOP06].

**Issues** [BDF +01a, BH00a, Eaq05, For04, Gum04, Inr03, Pag03, Puz04, Top02].

**IT-Architectures** [RM02].

**Italy** [AAC +01, AL06, BCKK05, BC05b, CGP03, dCdVSG05, IEE04].

**Itanium** [CHT02, Int00].

**Itanium-based** [CHT02].

**Iterated** [Jou04, Onl01].

**Iteration** [Che03].

**IV** [Sch01c, HSH +01].

**IWBRs** [LST +05].

**IWDS** [BCKK05, CLK05, KCR04, PK03].

**J2EE** [BTTF02].

**Jack** [Cos03].

**James** [Top02].

**jamming** [LPV +09].

**Jan** [YRY05b].

**January** [Des02, GL05, IZ00, Vau05a, Wri03].

**Japan** [Ano00b, Mat02, Oka00, Coc02b, Smi01b].

**Japanese** [Y00].

**Java** [Ano04b, Mar05a, WBL01, Ano02c, Ano03a, Ano04b, Ano04c, AJ01a, BC02, Bis03a, BJvdB02, CMG +01, Che00, CCM05, Coo02, DPT +02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hum05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, St01b, SJ05, Virt03, Wei04, Win01, Zee00, ZFK04].

**Java-Based** [EM03, DPT +02, GW08].

**Java-Löösung** [Ano04b].

**JAVA-Ring** [WBL01].

**JavaCard** [AJ01a].

**Javacards** [Cim02].

**JavaScript** [TEM +01].

**javax.crypto** [Win01].

**JBits TM** [MP01a].

**JCCM** [CMG +01].

**Jean** [MFS +09].

**Jewel** [CSY09, Lee04b].

**Jenness** [Sal03b].

**Ji** [Coc01a].

**Job** [MYC01].

**jobs** [Oue05].

**Joel** [Gum04].

**Johannes** [Lee03a].

**John** [And04, BZ02, NH03, Rot07, Cos03].

**Join** [Bar00c, Con00].

**Joint** [ADI09, ADR02, CR03, HYZ05b, HYZ05a, Puc03, Mat09].

**Jörg** [Fal07].

**Jose** [Poi06, Pre02b].

**Journal** [LLLZ06a].

**Journey** [FF01b].

**Jr** [Kat05b].

**Julius** [Chu02].

**July** [ACM01a, C05, Fe08, KJR05, May09, PPV96, Roy00b, Sch01c, S +03, Uni00a, Uni00b, Uni00e, Uni00d, ZJ04].

**Jump** [MP00].

**June** [ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BS03, BS01b, BCD09, BC01, C05, FMA02, IEE05b, IKY05, JZ04, K04, KLD04, K03, KM07, PPV96, TB02, USE01b, USE01a, USE02c].

**Just** [ABB +04, Gut02a, Car01].

**Kahan** [Gas01].

**Kaizen** [Ano00b].

**KASUMI** [KHYC01, KSHY01, SM02].

**Katholieke** [BB09].

**Katz** [Bar00a].

**Keccak** [BDPV09].

**Keep** [DM07b, Lys08, FS04].

**Keeping** [SEK01, SEK02].

**KEM** [NMO05].

**Kerberos** [BCJ +06, Coc01a, Gar03b, Hil00, It00, LLW08a, MJ01, MP00, Rub00, Smi01a, Wac05, WD01, W07].

**Kerckhoffs**
[KMZ03], Kernel
[Int00, Mor03, BK05, HB06]. Key
[ANS05, ASW00, AK02a, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BH06, BDG+01, BDZ04, Bar00a, BPS00, BPR00, BBM00, BBDP01, BY03, BOHL+05, Ben02, BLM01, Bil00, BBB+02, BDK+09, BR00b, BM03b, BDTW01, BMN01, BMP00, BCP01, BCP02a, BC02b, BM01c, BST02, CK02a, CK02b, CHK03, CHK05, CPP04, Che01a, CT08a, CHK00, CCM01, CMM00, CS02, CS03b, CS03c, DPV04, DJ01, DPS05, Des00c, DBS01, Des02, DG03, DY09b, DKXY02, DFK+03, DGH+04, DBS+06, ESG+05, EP05, ES00a, FL06, FKS00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Gol03, GH01w, GC01b, GSB+04, Gut04b, HNZI02, HCD002, HLM03, Hoe01, HR05, HG03, HJW01, HS07, HLC08, IEE00b, Ina02a, Ina02b, JL08, Jou02, JG01, Jue04, KGL04, KOY01, KY03, Kat05b, Kel05, Kel00, KKM01]. Key
[KM01a, KLY02, KY02c, KLC+00, Kl01b, KM04b, Kos01a, Kos01b, Ku02, KOMM01, KY01e, Kur01, KI03, LCK01, LLL02, LP03, LV00, Len01, Lin03, Lin00b, MPP00, Mac01, MSJ02, MHM+02, May04, MR01b, MR01c, Mil03a, Mol03b, Mil01a, Mur00, NIS03b, NA07, Ngu05, NBD01, NSS02, OTU00, Ort00, PHK+01, PR01, Poi02, PHM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sha01e, Sin01a, SK00, Ste01, ST01c, TSO00, Tan07b, TT01, VV07, Wal03, ZZW05, WH01, WC01a, Woo00, WBD01, Wya02, YKMY01, YI01, YG01c, YDKM06, Zhe02a, ZWCT05, AS08, AUW01, AKNR04, AF05, BHM03, BBN+09, Ben01a, BB79, BG08, BBC+02, BD00b, Bra01a, BCP07, BMA00a, BMA00b, BMA00c, BD04b, CCT08, CL02b, C05, CYY05, Che04a, CHC04, CY05, CLC08, CKRT08, CWJT01, CJ04, Cho06, CHH+09, CJL05]. Key
[DFM04, DMT07, DW09, EKRMA01, ED03, EHK04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GMR05, GKM+00, GS01, GL06b, GW01, HCD08a, HCD08b, HAN04, HH06, HLLL03, HTJ08, HG05b, HWWM03, HMvdLM07, Iwa00, HLL04, IZ00, Iwa08, IM06, JRR09, JW06, JXW05, JZCW05, KY00, KS05a, KOY09, KHYM08, KG09, Kim01, KPT04, KRY05, Kob00, KW00, Kos01c, KHKL05, LHL03a, LKKY03a, LKKY03b, LCP04, LL04a, LL04, LL05a, LKY05b, LKY05c, LKY05d, LCK04, LPM05, LHC08, LKJ01, LSH00, LS01c, LCC05, MW08, MKKW00, MP08, Mi08, Muli01b, NP02a, PS08a, Plo06, Pei09, Pei04, PC09, PSM+08, PLJ05b, Pri00, RH03, SN100, SL07, SR01, SBZ04, Shao5c, Shio5, SL05a, SW05, Shp04a, SC05b, SI04, SLC05, Sun00b, Sun02, SZP02, SC05b, SC05c, SCS05c, TP07, TO01, Tsao6, Tsao5, Tse07]. key
[VS01, Van05a, VK08, WDL09, War00, WGL00, WV00, WCO1b, Wuo1, WL04b, WHHT08, XH05, YW05, YC09, YS02, YS04, hY08, Yi04, YRY05a, YRY05b, YY05b, YPKL08, ZZ05, ZC05, ZSM05, ZYW07, ABB+04, GL05]. Key-Based [Sha01c]. Key-Dependent [Go03]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKXY02]. key-management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DPS05]. Key-Share [CT08a]. Key-Sharing [HNZI02, WBD01]. Keyboard [ZZT05]. Keyczar [Law09b]. keyed [Küh08, SR00, FIP02a]. Keyed-Hash [FIP02a]. keying [ABB+04, Che08a, EGK08]. Keyless [Qu01]. Keys [AOS02, APV05, AFI06, BT02, BMK00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, Lux00, MN01, MRL+02, Oni01, P000, Smi01c, Str02, TvdKB+01, BCL05a, BCW05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH+08b, HSH+09, HW04, HY03, HL04, LL08b, LS01c, LWK05a, ML05, NN03, Sch01e, Shao4b, Sha05b, SB05,
TLH05, TJC03, WH03, YRS+09.

Keystream [AMRP04, Kra02a, LV04, MH04, WLW04, PS01a]. Keystroke [MR00, BG02]. Keystrokes [S1W70].

Keyword [FIPR05, KGC [HLC08, KGS [ZYW07], KHAZAD [PQ03], KIAS [May09], Kid [CAC06, Kidik [Ano00b].

Kikai-Shinko-Kaikan [Ano00b]. kill [Lov01]. Killing [Lov01].

Kindi [MAaT03, MAaTxx]. Kindi [MAaT03, MAaTxx].

Kingdom [DFCW00].

Kingston [HA00, PT06].

Kit [Ano02c].

Klaus [And04].

Kleptographic [YY01].

Knapsack [Kos01c, SLC05].

Knife [Boy03].

Know [CMB+05, Ros07, Con09, DKK07, Win05c]. Knowing [CH01a].

Knowledge [Abe01, Abe04, AS01b, APV05, BP04, Con01, DP04, DFS04, DDD01, Eri02, Fis05, Gen04a, GK05, HNO+09, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00, Ros06a, TG07, BDSV08, CLR09, Dam00, Hro09, IKOS07, JRR09, PBD07, KK07].

Knowledge-of-Exponent [BP04]. Known [CKN06, CBMB+05, DN02a, Fur02b, HSH+01, Bao04, YTH04]. Known-IV [HSH+01].

Known-Plaintext [DN02a, Fur02b, CKN06]. knows [Fox00].

Koblitz [AHHR08, Has01b]. Kolmogorov [Sch01a]. Kommunikation [Lin02].

Kong [B+02, ZJ04, Cia00b]. Konstantin [Paz04].

Korea [CSY09, CKL05, KCR04, Kim01, Kim02, LL03, Lee04b, LL04e, May09, PC05a, PK03, Son00, Won01, WK06].

Korner [Mor03]. Kościszko [OC03]. Krawczyk [Miy01]. Kryptanalyse [Mor05]. Kuala [DV05]. Kunming [ZYH03]. Kurosawa [CHH+09].

Kurtz [Gun04]. Kyoto [Oka00].

L [Sem00]. L-collision [Sem00].

Laboratory [Brau06]. Lagrange [FWT05].

Laid [Wei05]. Lam [Wag00]. Lamar [LMHCETR06]. lamp [McN03].

LAN [Bar03, Pau03, SZ08, Sty04]. Lanczos [BF06a]. Landau [Jan08]. Landscape [Aht07]. Language [ARC+01, DD02, Gon09, Jen09, WAF00]. language-based [WAF00]. languages [Lun09, Rob02]. Laos [Lov01]. Laptop [PCT07]. Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, GG01, Kul00, PG05, SM01, ST03b, USE00a, BP03a, CKY05, CJO3b, Has00, HMvdLM07, HY03, PS08a, SM03a, TM06, WL05].

Large-Scale [CDR01, BH00a, BP03a, HMvdLM07, PS08a]. Larger [Car02]. LARPBS [CPhX04].

Lasers [Igl02, UHA+09]. late [Sch05c]. latency [RSP05].

Lattices [CD01b, HHGP+03, MV03a, MR09, BLRS09, HPS01, HG07, IM06, Mic01, Reg03, Reg04].

Lattice-based [MR09, HPS01, IM06, Reg04].

lattice-reduction [HG07]. Lattices [NS01c, Ng01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Sh05, Si01].

Launched [Bar00b]. Launches [Ano02b]. lava [McN03].

Law [GN06, MNFG02, Ste05c, NM09]. Layer [LXM+05, LPV+09, SL07, ZL04c]. Layers [Gri01]. Laying [Lut03]. Lazy [CCM05].

LDAP [Bau03a, Bau03b, BH00b]. Lead [Tsa07]. Leak [RST01]. Leakage [CK01, DP08, Koc02, RS01, CNK04, IY05].

Leakage-Resilient [DP08]. Learned [G02+04]. Learning [KS07, LY07, CAC06, BKW03, MAL06, Reg05, Reg09, SM08].

Least [SZ01]. lecture [Rot02b, Rot03, AD03, RAS03a, Riv03, Sha03b].

Lee [Sty04, Coc02b, KRY05, KCL03, KHKL05, LKY05d, SCS05b, ZK05].

Left [Dhe03, HKPR05]. left-to-right [HKPR05]. Legal [Coc02a]. Legislation [Eng00].

legislative [AvdH00]. legitimate [Lin01a].

Leighton [Rub00]. Leighton-Micali [Rub00]. Length [AR01, BR00b, CKN00, CHJ+01b, Møl03a, RK06].

Length-Preserving [Møl03a]. Leonard
Less [YKMY01, BD00b]. Lessons [GSB+04, KFSS00]. Lest
[HSN+08a, HSN+08b, HSN+09]. Lets [Pau02a]. Lett [Kwo03b]. Letters
[ASW+01, BTTF02, MNT+00, TEM+01, TvdKB+01, WWL+02]. Leuven
[BBD09, DR02c]. Level [EP05, MV00, TVH03, BDH00, KVW+09, S0S3]. levels [CUS08]. Leveraging [BRTM09]. LEVIATHAN [CL02c]. Levin
[AC02]. LFSR [Jam00, JZCW05]. LFSR-Based [Jam00]. LHL [Pei04, YRY+05a]. LHL-key [Pei04, YRY+05a]. Li [JW01, KLC03, S05S, QCB05a, SCS05b, ZK05]. Liaw [TJ01b]. Liberty [Lan04b, An00c]. Libraries
[Fin02, MK05b]. Library [KS02, Lan05, Law09b]. Libre [Jen09]. Lies [Gan01b, Sch00d, S0a01, Ste05c]. Life [C04b, GSB+04]. lifecycle [HL06]. Lifetime [Coc01a, CPG+04]. Lifting [CBS02]. Light [WT02]. Light-Weight [WT02]. Lightweight
[EPP+07, Mal02, CH07a, CL09, MP07]. Like [Coc02a, PSC+02, VMSV05, BCDM00, C00H00, DLP+09, E00h00, EBS01, Gou09, HSL+02, H0L04, SKU+00, SLL+00]. LILI
[J302a]. LILI-128 [J302a]. Limitations [Gua05, Fis01a]. Limited
[AK02a, Buh06, Tse07]. limiting [CCK04b]. Limits [CWR09]. Lin
[CC02b, CHY05a, KTC03, YY05b]. Line [Cho08a, DL98, Jan08, Lai07, Lu02, SK06, YLL02, Bau05, BCS02, D01L, Luk01, S05]. Linear
[BK02a, B02b, BDQ04, CGFSG09, CS05a, CHJ02, C0u01, C03M, C003, CD00, CD01a, CDG+05, FM02a, FM02b, G03S, GB02, HLL+01, Hug02, J00dJ, Kan01, KMT01, Kin02, KM01c, KRS+02, KY01e, LLL+01, L05S, N0P01, PSC+02, PG05, PZ02a, SNWX01, STK02, WF02, YSD02, BD04a, Bui09, CKL+03, C0u04, GHPT05, Kuk01, LLL04, Reg05, Reg09, RSQL03, S00L, SLL+00, TM01]. Linearization [DDG+06]. Linearly
[ADD09]. Lines [SP04]. Linguistic
[CDR01]. link [LPV+09]. link-layer
[LPV+09]. linkages [ZAX05]. Linking
[GW00]. Linux [Lin02, ASW+01, FR02, Fin02, Fri01, GJJ05, G00P06, GZ04, GRP06, JZ04, Lin02, Mor03, Pri00, Shu06, Sta02b, Sta05]. LISA [USE00c]. list [AGKS07]. little
[Lam07, Sch05c]. Live [Lov01]. Lived
[GSW00]. lives [FRN05]. LLL
[CKY05, NS05c]. Load [H010]. Loads
[GH02]. Loan [SOI02]. Loaning [Bla01c]. Local
[NABG03, Lav09]. Locality
[MFS+09]. Localization
[WLT05b, KCL+09]. Locally
[Vad03, Yek07]. Location
[HY01, KZ01, LNL+08, Buh06, S07]. Locations
[Kra02b]. Log [Gen00, H04]. Logarithm
[CNS02, Che04b, CCW02, GV05, GPP08, LO2, HS05a, H0L05d, LHL01, WH05, Sch01e, S01C, S05C, L05C, S05S, Y05a]. Logarithmic
[EGK08]. Logarithms
[CS03a, JL03, LHL03a, L05T, PLJ05a, QCB05a, Sh05c, Sha05d, SCS05c]. Logging
[Fox00, MT09]. Logic
[BPS02, Cop04b, KBD03, L011, Nie02d, SQ01, S01C, TV03, BD02, BD04a, DZ01, WZ05, DH08]. Logical-Based [KBD03]. Logical
[Kra07, Zha08]. Logics
[IK03]. Login
[LL05c, CCK04b, C01T1]. Logistic
[KJ01]. Logo
[LZ09]. London
[Pag03, Top02]. Long
[ABRW01, Dur01, GSW00, Gro03, PCG01, BMV06, IS05, SGMV09]. Long-Lived [GSW00]. Long-Term
[ABRW01, Dur01, BMV06, IS05, SGMV09]. Look
[Bon07, Has00, Lut03]. Look-up
[Has00]. Looking
[ASW+01, An01g, Cla00b]. looks [Nis03a]. Lookup
[MFFT05]. loop [KVW+09]. loop-level [KVW+09]. Loopholes
[Ste01]. Lorenz [GHdGSS00, Sal00a]. Lorenz-based
[GHdGSS00]. Losing [Sta05]. LosLobos
[Pri00]. Loss [LS05, MIT00]. Lossy
[AIP01, HSKC01, PW08]. Lost
[PY06, Rob02]. Lösung [Ano04b]. Lot [Cla00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [QS00].

Louvain-la-Neuve [QS00]. Low [Ano00b, BM01b, CH07c, GST04, HNZJ02, HGR07, JP02a, KBo09, RMH03b, RMH03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09, Fan03, HLL03, LC04a, WLLH05, WY05, ZYW07].

low-computation [Fan03, LC04a].

low-cost [CL09].

Low-End [SU07].

Low-Exponent [SZ01].

Low-overhead [HGR07].

Low-Power [Ano00b, JP02a, KBo09, CO09, ZYW07].

Low-State [GST04].

Low-Weight [CH07c].

Lower [BDF01b, BP03b, DIRR05, GT00, GGK03, PS02a, Slp03, WW05, Slp99].

LSB [CS05b, FGD01, WMS08].

LSB-encoded [WMS08].

LSD [HS02a].

Luc [QCB05b].

Luby [MP03, Pat01a].

Luminy [PPV96].

Lumpur [DV05].

Lund [Joh03].

LUT [CC02a, TL07].

Luxembourg [Bir07].

Lyndon [GS01, VS01].

Lynn [Hes04a].

LZ [AL04].

LZ-77 [AL04].
Match [JJ00a, LLC06a]. Matching [ABM08, Len01, UBE09]. Materialized [MSP09]. Materials [SLT01]. Math [SR06, McN03]. Mathematical [AUW01, Cas06, GL05, HPS08, Kat05b, You06, GKS05, Sin09].

Mathematics [SR06, McN03]. Math [BP06, Lew00, Nie02a, Sch00a, Sch01d, S+03, Sch04a, Sch04b]. Mathematiques [RSA09b, PPV96]. Matrices [TL07, CFVZ06, LMTV05]. Matrix [CV03, BF06a, OS07]. Matroids [CDG+05]. Matsumoto [DDG+06, YG01a].

Mature [Tro08]. Max [Di 01]. maximal [Hüh00, HJW01]. maxims [Bau00, Bau02a]. Maximum [KMT01, ZC00, DW01]. May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bih03, CC04a, Cra05a, DRS05, IEE01b, Knu02, KNP01, MJ04, MS05a, P000, P001, Pre00, TLC06, Uni00f, Uni00e, YKLM02a, P002a, YJ00]. Mbps [LMP+01]. McClure [Gum04]. McEliece [CFS01, KI01a, KI01b, Loi00, LS01c, Sun00b]. McEliece-Based [CFS01]. McFarland [Car02]. McGraw [Gum04]. McGraw-Hill [Gum04]. MD4 [DG02, WFLY04]. MD5 [Eke09, WFLY04]. Me [CAC03, CNB+02]. Mean [Bar00c, KLLM05, Ver06b]. Means [LMHCETR06, Nis03a]. measure [Lav09]. Measurement [An002c, kc01, CO09, FXAM04, RW07]. measurement-based [FXAM04]. Measures [CB01, Q501]. Measuring [Siv06]. Mechanising [Be01]. Mechanism [LXM+05, WY02, CL08, GH08, LCP04, ME08b, WAF00]. Mechanisms [BACS02, CJK+04, Lin00a, MD04, Mir05]. mechanized [dH08]. Media [Hei07, An02b]. Median [Cap01].

Mediated [DT03]. mediator [SBG05]. mediator-free [SBG05]. medical [AL07]. Medicine [MYC01]. Meet [Cla00a, HG07]. meet-in-the-middle [HG07]. meeting [Jef08]. Meets [Way02a]. Melbourne [IZ00]. Membership [NBD01, Fis01a]. Memoir [Bar05]. Memorable [KOY01]. Memoriam [DNRS03]. Memory [AK03, AJ00, CCM05, DK08, DGN03, HNZI02, HBDJL01, KCJ+01, Oec03, OT03b, QSR+02, R005, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05]. Memory-Bound [DG03]. memory-safe [Oiw09]. Memoryless [Sar02]. MEMS [ECG+07]. MEMS-Assisted [ECG+07]. menu [Mea04]. Mercy [Fnu02a, Cro01]. Merkle [CDMP05, JLS03]. Mersenne [An003c]. Mesh [LPZ06, ZTP05, KB09, LZP+04, YPSZ01]. Meshes [BG08, Lav09]. Message [BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, F000, Jut01, O009, SNR04, W03, Zol00, C05, C05, Gav08, HW05, MD04, Sha04b, TJC03, Wu01, ZF05, ZAX05]. Messages [Ara02, AR01, BR00b, CHJ+01b, DS05, Sch09, Wri05, BCG+02, Bih02, BB79, Lun09, SP79]. messaging [Opp01, RR05]. meta [SM08, PLJ05a, QCB05, Sha05d]. Meta-He [PLJ05a, QCB05, Sha05d]. meta-learning [SM08]. metadata [CD07, FJ04]. metamorphic [CSW05]. Metaphor [CNB+02]. Metering [BC04b]. Method [BDTW01, GHK+06, GL00, Gro01, HR02, HQ05, JKKA+01, Me02, OKE02, OT03a, OT03b, SOHS01, TIGD01, TS000, WH09, WNY09, ZL05, AMR04, DwWN05, JL03, MSP09, MFK+06, WG02, WWTH08, kWpLwW01, WLW04, YCL07, CHJ+01a]. Methodologies [SPML02, NdM04]. Methodology [VMS05, HM02a]. Methods [BCDM00, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07, TNM00, Vir03, Bau00, Bau02a, BGM04, BCHJ05, CM05b, GKS05, JZCW05, LMSV07, Mal06, SSST06, Shp99, YW06]. Metric [LB01, LB02]. Metrics [LZ01, NP07]. Mexico [Buc00a]. MGC’05
[AK02a, BCS02, Por06, Bej06, GXTG05]. Monitors [JT05]. Monks [Eag05, Kin01]. monoalphabetic [GPG06]. monolithic [GhdGSS00]. Monotones [WW05]. Monte [Bi09, Sug03]. Monterey [USE02c]. Montgomery [CH07c, HKA+05, NMSK01, OS01, PS04a, TS00, Wal01, WS03]. Monterey-Form [OS01]. Montpellier [KM07]. Montr´eal [ACM02]. Morocco [IEE09a]. MorphoSys [Tan01]. MOSS [Dav01b]. most [GG05a, Shp02, Tyn05]. Mothballed [Bar00c]. Motif [Bi09]. Motion [EFY+05, hKLS00, WMDR08]. Mountain [JYZ04]. mouse [HLwWZ09]. move [Jac00]. movement [HLwWZ09]. MP [MP07]. MPEG [LHS05, MLC01, YZDW07]. MPEG-4 [SG07]. MRF [Che01a]. MRN [TIGD01]. MSP430x33x [GBKP01]. MSXML [TEM+01, Hei01]. Mu [CJT03]. much [Con09]. Multi [ARR03, BBM00, BR06, CJK+04, CJK+05, DLY08, DIII01, FGM001, FW004, Gen04a, HM01b, HS07, JLL02, Kur01, LV07, LLL04, Tsa01, ZJ09, CLOS02, CC05a, CHY05a, CHY05b, DZL01, FWTC05, GMLS02, HHYW07, HWH05, HC04b, HL04, LH03b, LCZ05b, LW05c, NC09, PW05, SC05a, TWL05, TYH04, YCH04]. Multi-applications [DIII01]. Multi-Authority [JLL02]. Multi-channel [ARR03]. Multi-designated [LV07]. Multi-Domain [CJK+04]. multi-hop [NC09]. multi-linear [LII04]. Multi-party [CDM00, CDG+05, FGM001, FW004, HM01b, LII04, CLOS02]. Multi-property-preserving [BR06]. Multi-Proxy [ZJ09, HC04b, LW05c, TYH04]. Multi-Receiver [CCD07]. Multi-recipient [Kur01]. multi-scroll [HHYW07]. multi-secret [CC05a, CHY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server [Tsa01, LHL03b, TWL05]. Multi-Servers [HS07]. multi-signature [HWH05, HC04b, HL04, LCZ05b, LW05c, TYH04]. multi-stage [CHY05b]. Multi-trapdoor [Gen04a]. Multi-user [BBM00, DLY08, GMLS02]. multi-valued [DZL01]. Multiagent [ZS05]. Multiagent-Based [ZS05]. Multicast [AIP01, BPS00, BDF01b, ASW00, GIKR01, GL06b, JA02, KB09, MP08, PCS03, YC08]. Multicollisions [Jou04]. Multilevel [LN04]. Multimedia [AAK99, FMS05, GA05, HL07, Sun05, TTL09, DY09a, DUK05, LA00, SG07, YC08]. Multimodal [PY08]. Multiparty [BG008, CDN01, DN03, DI05, GKR02, OZL08, CDD00, HT04, IKOS07]. multipath [SK05b]. Multiple [AIK+01, Ara02, BDQ04, CL01a, CKL01b, CHSS02, Che08b, DK05, Har00, HLT01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJ04, DIII07a, HL00, KC09, Sha04d, SW05, TCC02, YW05, YRY05b]. multiple-key [Che04a, CJ04, SW05, YW05, YRY05b]. Multiple-watermarking [Che08b]. Multiples [HR00]. Multiplication [AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GL01, HM02c, KKIM01, Mòl02, NMSK01, OS01, Tan07a, Wal01, BNP03, DwWmW05, FP00, GD05, Has00, Mis06]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KO03, MFFT05]. Multiplier [HKA+05]. Multipliers [CMJP03, KWP06, RH03b, WS05, HGN03, RMP08, RH03a]. Multiply [KTT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver [HSZ01]. Multiresolution [hKLS00, YPS01]. Multisignature [Tad02, CWH00, CL04c, CCH04, He02, LC04b, LWK05b, YY05a, ZX04]. multisignatures [CL00, WH02b]. Multithreaded [Zha00]. Multivariate [DY09b, BGP09, FP09]. Municipal
mutargima [MAaT05]. Mutation [Lut02].
Mutual [JP02a, KH05, CCS08, VK08].
Mutually [WC01a]. MYCRYPT [DV05].
mysterious [Bel07]. Mystery [Rug04, GG05a].

N [Mar05a, AOS02, KOMM01]. NAF [OT03b].
Names [Coc01a, Sha02, Ark05, CGV09]. Naming [Ano01b, BH00b].
Nanotechnology [RR03a, RR03b]. Naor [Zha06].
Napoleon [Urb01]. narrowing [MT07]. NASA [Wil99].
National [BWE+00, Jol01, LCS09, AJ08, Bam02].
National-Scale [BWE+00]. Natural [ARC+01, Top02, WMS08].
Nature [Pag03]. naval [Goo00]. Nazi [Hau06, KS04]. NC [AIK04].
NCP [SQ01]. Near [BC04a, DPS05]. Near-Collisions [BC04a].
Necessary [LCK03, MN01]. Necessity [SBZ02].
Nederlanden [dL00]. Need [Coc01a, HR04b, Sty04]. Needs [CZB+01, DKK07].
Negotiation [DBS+06, HHJS04, IY05, LLW05, LLW09].
Nema [Kid00]. NESSIE [Pre01, Pre02a, SGB01]. nested [LCK04].
Net [CAC03, LJKL01]. Netherlands [Knu02].
 Nets [AADK05]. Netspionage [BK00].
Network [Ano02b, Bar03, BGOY08, Con04, CLZ02, Dim07, FBWC02, Gum04, Har05a, IKY05, JY04, KKK03, KPS02, Ken02b, LMP+01, Lu07, Mal02, NN02, PJDH09, Poo03, RCBL00, RC05, Sty04, TLYL04, VMC02, YC01, ZHY03, ZS05, Bru06, CJ03b, CMS08, Coc01a, DWML05, GKS05, HLL+02, LC03, LPV+09, ME08a, MSK03, Mi08, Pri00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wyl05, YLT06, ECM00a, ECM00b].
Network-Attached [RCBL00].
network-based [HLL+02]. Networked [Sch00d, LB05].
Networking [ACM01b, Ros07, VM03]. Networks [AEAQ05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zea00, ZYN08, ZWCMY02, AJS08, BBG+02, BC05b, CCMT09, CGP03, CBD+05, DHRM07, ETM05, HJ07, HMvdLM07, JRR09, KXTZ09, KYHM08, KB09, LHD06, LHC08, LW05a, Lin07, LN04, LKZ+04, MWS08, MJF+08, MS09b, NC09, NLD08, PCSM07, PS08a, Pat02b, SLP07, SSM+08, TP07, TM06, TCR03, TW07, WDLN09, YC07, ZSJN07, ZBLvB05, Ano02b, CS08b]. Neural [KMS02, PR01, YC07].
Neural-Network [YC01]. Neuve [QS00].
Nevada [ELvS01, IEE01a]. Never [Wei00, Hau06].
Newfoundland [NH03]. Newman [Pag03]. Newmanry [Sal01a].
News [Ano03b, Bar00a, Bar00b, Bar00c, Cla00a, Coc01a, Coc02a, Coc02b, Coc03, Eng00, Fox00, MYC01, MP00, PM00, Pan02a, Pan02b, Pan03, Pan09, Pri00, CAC03, CAC06, Sta05, Raj06].
Newton [KT06]. Next [ESG+05, McL06, TV03, Web08, BD04b, ISTE08, RR03a].
Next-Generation [ESG+05, Web08]. NFA [DIS02].
NFS [Sta02b]. NICE [JJ00c]. Nimbus [Fur02a]. nine [Tat05]. Ninth [USE00d]. NIST [BG07a, Dra00, Hir09, Kel05, RRS06, SF07].
NIST-Recommended [Kel05]. NMAC [RR08].
NMAC/HMAC [RR08]. NNAF [ DwWmW05]. No [Sta05, Sty04, Uni00g, Wei05, CC05b].
Nobel [MNT+00]. Node [BRTM09, Fox00].
Nodes [ZYN08, RAL07]. Noise [BKW03, GA05, MPSW05, MS09a, PC00]. noise-based [PC00]. Noise-tolerant [BK03]. noisy [HGNS03]. Nominative [PL01].
Non [CH05, CZB+01, DN00a, DDO+01, DW09, FF00, Fis01b, Fis05, FGM00a, FGM00b, HNZI02, HJW01, IYK02, IYK03, JT01b, Kos01c, KOO, MSTS04, Nic02b, PHK+01, Pas05, SPK08, WBL01].
DM07a, DS02, Hüh00, HLL04, IM06, KKL09, KHL09, LSA+07, PR05, RP00, SC05c.

Non-adjacent [JT01b]. Non-committing [DN00a, Nie02b]. Non-Cryptographic [WBL01, IYK02, IYK03]. Non-injective [Kos01c]. Non-interactive [CHK05, DDO+01, Fis01b, Fis05, HNZI02, HJW01, MSTS04, Pas05, KKL09, KHL09].

Non-malleable [DW09, FF00, PR05].

Non-OOSD [CZB+01]. non-perfect [DM07a]. non-physicists [RP00].

Non-quantum [IM06].

Non-trivial [KO00].

Non-Uniform [SPK08].

nonce [CY05, LKY05a]. nonce-based [CY05, LKY05a]. Nonces [BR00a].

Noncontact [Sak01]. noninterference [DFG00].

noninvertibility [HRS08].

Nonlinear [BP01a, BI05b, CV02, Che01c, LBGZ01, LBGZ02, SML0a, ZC00, BGPGS05, CFVZ06, KH08].

Nonlinearity [SM00b].

Nonmalleable [ABW09, DDN00, DDN03, PR08].

nonrepudiable [TYH04, YTH04].

nonrepudiation [HW05, OZL08].

Nonsecurity [Sch07]. Nonuniform [CU01].

Normalization [VK07].

Nose [Fox00].

Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Dic03, DGP07a, DGP07b, DV08, Eag05, EHKO03, Fin06, Gou09, Nov06, H08, Hig08, Int03, Kat05b, Ket06, KM01b, LMHCETR06, LNS02, MNP01, NR04, RSN+01, SP05, Sch06b, Shp99, Shp03, SDF06, TWA08, TL07, TZW09a, TZW09b, Vav03, Wall06, Yan00, YKLM02b, Am03, AUW01, BK07, Bel08, BGPGS05, BG08, BG09, BG07a, BGL+03, CNP03, CO09, DIM08, DGP09, FP00, G05a, HGNS03, HlwWZ09, HP01, JAW+00, J03, KH08, KS00, Kin01, Lam01, Mit00, Nie02a, Nie04, Pan07, PSG+09, SPF+08, PC00, RGX06, Sh05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Was08b, YZEE09].

Number-Notation [Eag05, Kin01].

Number-theoretic [NR04]. Numbers [HSL+01, HBF09, Ifr00, MN01, ST03b, AG09, HW98, KB39, Kir01, MFK+06, S03, Shp05, Tip27]. numeric [AKS04].

Numerical [WWL+02]. numerically [Sav04].

NURBS [Ben00]. NUSH [WF02].

NY [HR06, IKY05, KJR05, Sch01d, YDKM06, NIS00].

Nyberg [Ara02].

O [Kat05b, Puc03]. OAEP [Man01, BF05, BF06b, Bon01, FOPS01, Sh01].

Obfuscated [NS05b]. Obfuscating [BGI+01]. Object [RSA00e, DHL06, MWM01, ST06].

Object-oriented [DHL06, MWM01].

Object [CCM05, ZTP05, PB01].

Oblivious [CT08b, Din01, FIPR05, IKNP03,
obscurity [MN03]. Observability [JQYY01]. observers [JL04]. Obstacles [KM04a]. Obtaining [Bar06b, BP03b]. OCB [RBB03]. October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST0+05, TTZ01, USE00b, ZYH03]. Octopus [Clao0b]. Oded [Lee03b]. odyssey [Gol08]. Oedipus [Lav06]. Off [AJO08, Coc02b, Oec03, Shi05, YLLL02, Bau05]. Off-Line [YLLL02, Shi05, Bau05]. Offering [YC08]. Office [Uni01]. Offer [Kov03]. Offline [WV01]. Offs [PS01c]. OH [BB00c]. oil [RD09]. old [Lov01]. On-Demand [SE06]. On-Line [Lu02, BCS02, Luk01]. One [AK02a, BYJK08, CHL02, Che03, DI01, DW01, DMS00, Fis01b, GKK0+99, HNO0+99, HM02b, HR05, KIO1a, KO03, KO00, LT0W05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YZ00, YKL02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, DI03, DS02, GKK0+97, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVFD07, SV08a, SW05, YW05, YRY05b, ZW05a]. One-Time [HM02b, LDM04, RR02, CCK04b, DS02, LC04a]. one-variable [SV08a]. One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK0+99, HNO0+99, HR05, KIO3, KO00, LTW05, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, GKK0+97, HR07, HRS08, JZ09, KK07, KKK05, KK03, LW04, LPM05, LQ08, Mic02a, Poi00, YW05, YRY05b, ZW05a]. One-Wayness [KI01a, PV06b]. Ongoing [Sam09]. Onion [CL05]. Online [BDF0+01a, BBKN01, Fis05, LCS09, Or00, Rey01, ST01b, VAVY09, FNRC05, Fox00, Pan07, Tyn05, PT08]. Online/Offline [ST01b]. Only [BBK03a, CF01b, GL01, Hoe01, VV07, BCDM00, FKS0+00, GHJV00, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Yas08]. Ontario [HA00, ST01d, VY01]. OSSC [CZB+01]. OSSD [CZB+01]. Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Kus02, Lin02, Mei01, PM00, VDKP05, Ano03b, ETMP05, MaA08, Bar00b, Lin02]. Open-Ended [Kus02]. Open-Secret [Joh05]. Open-Source [Bol02, Gut00, McA08]. OpenCard [HF00]. Opening [CAC03]. OpenSSH [Bau01c, Sta02b, TvdKB01, Hos06a, Mos06]. OpenSSL [Fri01, Res01a, Res01b, Sti06a, VMC02, YRS0+99, Bel08]. Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL0+98a, CGL0+98b, CGL0+98c, DGP09, KWD06, MPHD06, SETB08, TKP0+08]. Operation [BR02, BK07, Dw03, EP02, Gol04, HSH0+01, JKR01, KY01a, Bau00b, RBB03, Win00]. Operation-Centered [BK07]. Operational [WA07, GMG00]. Operations [BIP05, IMM01, KDO01, KS05b, LS01b, Ark05]. operator [Wan05]. Operators [CH00]. opinion [BHM03, GS07b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Bau02b]. Optimal [Bai01a, BDDS03, CHJ0+01b, CDF01, CF02, DPS05, DNP07, GMW05, IR01, KO04, KS03, LZ09, Man01, MPSW05, MP08, SNR04, YY01, vDW04, BCD06, HK00, LSH03a, LSH03b]. optimality [NK06]. Optimised [TL07]. Optimistic [CC00, DLY08]. Optimization [Ken02a, Kre05, KV01, SMTM01, TLYL04, WPP05]. optimized [LC03], optimizing [Dwi04]. Optimum [KWP06, OKS06]. Oracle [ABR01, Abe01, Abe04, BF05, Chi08, Gra02b, Nic02b, Pas03, Ano02c]. Oracles [BNPS02, BB04, KG09, RG09]. Order [AKSX04, Bai01a, CV02, KCP01, KJC0+01, Kra01, Luc02b, NNT05, NM09, Sty04].

performance-friendly [CRSP09]. periodic [XQ07]. Periods [KKH03]. Perl [Sal03b]. Period [KKH03]. Perl [Sal03b]. Permutation [BPR08, CHL02, KO00, MP03, KKKP05, WV00]. Persistent [AGT01, ST06]. Person [KJR05, LLT04, PK01, BS01b, KN03, Li05, LST05, PY08]. Personalized [GPC08]. Perspect [LL01]. Perspectives [BM06, SM08]. Perturbation [HWH08, ZY08]. Perturbation [HWH08, ZY08]. Pervasive [BDaK09, JW05, LKHL09, Lut03, Lut03]. Perturbation [HWH08, ZY08]. Periodic [XQ07]. Periodic [XQ07]. Periods [KKH03]. Perl [Sal03b]. Permutation [BPR08, CHL02, KO00, MP03, KKKP05, WV00]. Persistent [AGT01, ST06]. Person [KJR05, LLT04, PK01, BS01b, KN03, Lio5, LST05, PY08]. Persistent [AGT01, ST06]. Person [KJR05, LLT04, PK01, BS01b, KN03, Lio5, LST05, PY08]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutation [DMS00, HSR01, IYK02, KKG03, KO03, LSY01, DP02, IYK03].
CJ03a, CH07c, CLZ02, Gon06, HR00, KL05, KY01c, KTT07, LW02, May04, Pli01, RMH03b, Sat06, LFWM04, MRST06, SZP02. Polynomial-Time [CLZ02, KL05, Pli01, MRST06]. Polynomials [BLST01, DS08, FL06, Jam00, JJ00d, Lan04a, CHH01, FP09, GS09]. Pon [QC05b]. Pool [BTTF02]. Popular [RR08, CAC06]. Portable [Hei07, Wan04a]. Portfolio [Ano02c]. Portland [ACM00, BCDH09]. Possibility [SF07, BGI01, DOPS04]. Possible [Mur01]. Post [BBD09, BLRS09, Ber09b, HHG06, BD08, BBD09]. Post-Quantum [BBD09, BLRS09, Ber09b, HHG06, BD08, BBD09]. postage [Ble07]. Poster [TSO00, RN00b]. Potential [Kid02]. Potentially [Wal01]. POTSHARDS [SGMV09]. Power [AKS06, Ano00b, Ava03, BL05b, BNPS02, Cry00, DPV01, DBK+06, Gir06, Has01b, HMO2c, HBF09, IIT03, JP02a, JQY01, KBM09, KLY02, MOP06, Mas04, MS01, MMMT09, Mes00, Mes01, MG08, OS00, OS06, OOP03, PGX+09, Sha01c, Sma03b, WS05, WC01a, vW01, CBSU06, CO09, Geb04, Mit02, OS08, XH05, ZYW07]. Power-Analysis [OOP03]. power-attacks [Geb04]. power-aware [CBSU06]. Power-Sum [KLY02]. Power-Up [HBF09]. Pp [Eag05, Pag03, Top02]. PPC [ASW+01]. PPY [YDKM06]. pq [KOMM01]. PQCrypto [BD08]. Practical [Ano01c, AR01, ASCH03, ACJT00, BDK+09, BF05, BLMS00, CS03a, Cap01, CDR01, CS03b, DK01, Dreu00, FS03b, GSS03, GIS05, GH02, HQR01, IJW01, Ina02a, Ina02b, IIT03, Kan01, LMOV05, Lut03, LWK05a, MM02, MSU05, OM09, PBD00, Pel06, Poi02, Poo03, Roy00b, Sug01, Wei04, YSS+01, Bro05b, DKL+00a, Har05a, KSW06, Luc06, Mos06, MSV04, Sha01a]. Practice [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti95, Sti02, Sti06c, Lut03, Spr03]. practices [Ste02]. practitioners [PP09]. pragmatic [BMW02b]. Prague [MJ04]. Pre [Adl03]. Precise [Wal01]. Precision [SR06, LM+03]. Precomputation [SLG+05]. predecryption [RSP05]. Predict [Die03]. predictable [Be08]. Predicting [AG09, BGPS05]. Prediction [AKS06, SLG+05]. predictive [vOT08]. predistribution [HMvdLM07, JRR09, TP07]. Preface [CGM07]. Prefix [FXAM04, RW07]. Prefix-preserving [FXAM04, RW07]. Prehistory [Fr00]. Preliminary [KS00b, KKS00b]. Prentice [For04]. Prentice-Hall [For04]. Preparations [FJ04]. Prepared [ASW+01]. Preprocessing [BIM00, CKK03]. presence [BIW06, GTX+08, Mii08, VS08]. Preservation [Che01b, Dur01, Bro05a, IS05]. Preserve [NNT05]. Preserving [DN04, KS05b, LP00, Mii03a, YWD08]. AKSX04, BR06, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07]. Press [Imr03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03]. Pressure [HWH01]. pretty [vOWK07]. Prevent [FOBH05]. Preventing [CS07b, HSW09, IY05, RG05, DMS07]. Prevention [JT05, PZ01, PZ02a]. Price [AS01a, Bra01b]. Primality [BT02, Che03]. Prime [ACS02, BAI01a, Har07a, Pau02a, WS03, JL03, dW02]. Prime-detecting [Har07a]. Primer [KLB+02b, Lad06]. Primes [Ano03c, SZ01, HLLL03, Ste08, AKS02]. Primitive [CFS05, IYK02, IMM01, ST01a, ST02, IYK03]. Primitives [BDFP02, CHL02, FGM001, Ngu05, RR00, BDFP05, Gar05, JZCW05, RAL07]. principal [ZL04b]. Principle [CZK05]. Principles [ACM03c, ACM05b, DK02, DK07, KL08, SB07, Sta02a, Sta06]. Print
[Kra02b]. Printed [SLT01]. Printer [Bar00a]. Priority [WWL+02]. Privacy [AEV+07, BBPD01, CDM+05, Cho08a, DL98, DL07, DKFX05, DN04, GS02a, GMM08, HY01, KS05b, Knu07, LP00, MP00, Pap05, PBD05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YWD08, BeI04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Ty05, WK05, ZYL05, ZSM05, MS05a, Jan08]. Privacy-Enabled [Por06]. privacy-enhanced [ZSM05]. Privacy-Enhancing [SE09]. Privacy-Preserving [DN04, KS05b, YWD08, BA06, HJW05, Pin02, Pin03]. Private [AF04a, AFI06, BDFP02, BIM00, BY03, BSW09, BJLS02, BGW05, ISW03, KO00, OS05, ST01c, Wal03, Yek07, BD00b, Cal00a, HLLL03, KY00, KPS02, PLJ05b, Sun02, YRS+09, ZY08, ECM00a, ECM00b]. Private-Key [BY03, KY00, PLJ05b, Sun02]. prize [Fox00, Coc02b, MNT+00]. PRNG [HSS04, Mur02, SF07]. Proactive [DBS01, FMY01, JS05, ZSV05]. Probabilistic [CCW02, CPD06, DJ01, Kuh00, Lee03b, CP07, DLMM05, GoI09, JZCW05, KY00, MRST06, PBMB01, dH08, Ne04]. Probability [KMT01, MNT+00, DLP+09]. Probing [ISW03]. Problem [AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK+02, Cou01, CLZ02, DIS02, DHR00, FL06, Gen03, GV05, GPP08, KK02, LNS02, NBD01, Wav02, BK03, CGH06, CJT04, DLMM05, HGN03, Hsu05a, LH05, LD01, Luk01, Pe09, Shp05, SCL05, WL02, Yas08, KM04a]. Problems [BI05a, Can06b, MO03a, OP01a, TvdKB+01, VDK05, HL05d, KX00, LMT05, LMC+03, RSS04]. Procedure [LY07]. procedures [BBK+03b]. Proceedings [ACM00, ACM02, ACM04a, ACM05a, AAC+01, Bon03, EBC+00, FMA02, FLA+03, SM07, USE00c, USE00b, USE00a, USE00d, USE01b, USE01c, USE01a, USE02a, USE02c, USE02b, WK03, Yun02a, ACM05c, ACM07, ACM08, ACM09, AUW01, AJ01b, BS03, Be00, B+02, Boy01, Buc00a, BC01, HA00, Hon01, IEE00a, IEE01a, IZ00, Kil01a, MS05b, Oka00, PPV96, Pfi01, Pre00, QS00, RD01, Roy00a, SMP+09, ST01d, VY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BDZ04, BS01b, Bi03, BCDH09, BD08, CC04a, CV04, Chr00, Des02, DFPS06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE05b, IEE07, IEEE08, IEEE09, JY04, Je08, JM03, Joy03b, JQ04, KJ05, KGL04, Km01, Km02, KN03, Knu02, KP01, KN01, KM07, Lai03, Lee04b, LLT+04, MMV06, MJ04, May09, MS02c]. Proceedings [Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02b, RS05, Sch01d, Sma05, Syv02, TB02, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZYH03, BCK05, Cra05a, DV05, DWML05, DKU05, GKS05, IK05, Kil05, Li05, LST+05, Men07, Poi06, Sho05a, Sun00, DCvSG05]. Process [Kw03b, MNT+00, BDFP02, HL06, MRST06, VKS09]. Processes [BDP02, AL02, BDN02]. Processing [ISSZ08, KLB+02b, PCK02, AA04a, YPSZ01]. Processor [An02c, BBGM08, EP05, FBWC02, FZ05, GC01b, Int00, KBD03, KPMF02, TYLL02, ST03a, SHL07]. Processors [TLYL04, CW02, CRSP09, Gb04, L05a, YG05, YL06, ZYL05]. Procurement [Lad06]. produce [Zir07]. producing [SOIG07]. product [Sun02]. Products [ACS02, An02b, An02c, Km07]. professional [Dew08, vT00]. proficiency [Dew08]. Profile [PZH02, RSA01]. Profiles [MV01, PJ01]. Program [Höfo1, Bec02, GGH+08, Kvo03, KH03, CS08b]. Programmable [Dam07, GC01a, HV04, Sm02]. Programmer
Programmers [Coc01a, Wei04, Gou09].

Programming [ASW+01, Ano02b, Coc03, LMHCETR06, Res01a, Res01b, Sawa01, Uro01, Aj01a, Aj01b, CW07, Ni03a, VM03].

Programs [BGI+01, Ark05, SLTB+06].

Progress [KK06, KFSS00, RD01, Roy00a, CV04, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Ni03a, VM03].

Projects [Fri01, IY00, MNT+00, Pau02a, Salxx, Gou09, LR01, Lov01, MWM01, Sha01a, Coc01a, Coc02b, IY00, Gha07].

Prolog [Bla01a, Bla01b].

Promises [Pau02a].

Promote [WK05].

Promotes [Bar00b].

Prone [MLC01].

Proof [Abe01, Abe04, AS01b, ARC+01, BDP02, Cor02, Gk05, SOJG07, SMPLS02, GM04, HSD+05, LMW05, PB07].

proof-of-compliance [LMW05].

Proof-of-Concept [ARC+01].

Proofs [BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, Go09, HG05b, SV08b, dH08].

Propagation [LJL05, QPV05].

Properties [ABC+05, BM01c, KY01b, LLL+01, MS02a, NNT05, SM00a, BD04a, FGM03].

Property [LPZ06, Qu01, Uni00b, WY02, BR06, JRS09].

Proposed [Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06].

Protection [ETZ00, BBN+09, WK05].

protected [PKH05, ZCL05].

Protecting [Des00c, EHS00, KY01d, Kra01, LKM+05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYL05].

Protection [CGJ+02, DFKX05, ECG+07, FBW02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, Gor05, Kvo03, KH03, Kwo03a, LL05b].

Protocols [JT01a].

[Ano01a, Bel01, BP02, BL02, CK02a, CJ03c, CW05, Cim02, ECM00b, Fre03, GJKR03, GL00, HS07, JP02b, JRFH01, JT05, Kra05, Ku02, LCK01, Mea01, MSU05, NS01b, Rub00, RMCG01, SK00, Tan07b, TZ09a, TZ09b, YSR01, BP03a, Bla01b, BDFP05, BK05, CS04, CCK04a, CC04b, CYY05, CC05c, Che04a, CLC08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, HT08, HW003, HHC05, KH08, KKL09, KTC03, LC03, LKYY03a, LKYY03b, LW04, LHL04, LK05b, LK05c, LH08, LSH03a, LC05b, Luk01, MS03a, Par04, Sh05, SW05, SIR04, TM06, Tsa06, Tse07, WK05, WL05a, WH008, YW05, YTYW05, YC09, YS02, YRY05b, YRY05c, YPKL08, ZW01, ZL04c, ZDW06, ZYW07, LSH03b].

Protocols [AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Br01, BM01, Bra01b, BLD09, CKPS01, CT08a, CCM02, CCM05, Cir01, CNV06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, JW05, KS00a, KY03, KL08, Kra03, Ki02, MS02a, MN01, PBD00, PR08, PJDH09, Rot01, Sh02, SC01, AA04b, AK01, Bar06a, Bau05, BLS08, BF04, BP05, BLP06, BR04a, Can01a, Can06a, CP07, CK01, CW01, CH07a, Cho08b, Chr00, Chr01, CJM00, CC05d, DFG00, GUQ01, HM02a, JW01, KS05a, LPV+09, LLL04, Mea04, MT07, MR06, Mon03, MP07, PR05, Puc06, SV08a, SL05a, SR00, SW00b, YS04, ZL09, ZL04b, PDM09, Puc03].

ProtoMon [JT05].

Provability [GOR02b].

Provable [HM02b, HLL+01, HSL+02, KSY01, PBD05, SLL+00, BGP09].

Provably [AO00, AET00, BMD00, BCP01, BCP07, CHKO08, DG03, HLV02, HLA09, HL07, HS07, JMV02, M03a, NSN05, NSS02, VMS05, XS03, ZCL05, BKN04, CC04].

provenance [HSW09].

Provers [MV03a].

Provide [AB01, Sch01a].

Provider [IEE07, Si01].

Providers [LD04, HLM02], providers [MV03b].

Provides [OT03b].

Providing [BACS02, BDS+09a, DeL07, Lin07, Par04].

Proving [Che03, SF01c, GN01].

Provision [Kha05].

Proxy [AH05, BCL05a, DFKX05,
proxy-enabled [DY09a]. proxy-protected [PKh05, Zcl05]. psBGP [YVWK07].

pseudo [BH05, FWW04, Gen00, LLL01, LW05c, Gen00, FXY01, LHL08, MP03, SXY01, MFK06, NR04, WP03, BG09, GB09, MFK06, NR04, PSP08, RGX06, SL09, WW08, YZEE09].
Pseudo-Random [LLL01, MP03, WP03, Gen00, SXY01, MFK06, NR04, WP03, BG09, GB09, MFK06, NR04, PSP08, RGX06, SL09, WW08].
Pseudo-Ransom [BH05].
Pseudo-signatures [FWW04].
pseudonoise [HG05a]. pseudoprimes [ZT03]. Pseudorandom [CDI05, DN02a, DI05, DP02, Fin06, Flu02b, FIPR05, GM02a, IYK02, LMHCETR06, Nie02c, RSN01, Aam03, BGPGS05, IYK03, KSF00].
Pseudorandomness [GM02c, IK00, KY01e, KI01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Mol03b, Mülo1a, NPO2a, NBD01, NSS02, OTU00, PHK01, Pei09, PR01, Po01, PFM03, Q001, RSA00a, RKZD02, ST01a, ST02, Sin01a, Smi01c, Ste01, TSO00, TT01, Vau05a, WZ05, WHI01].
Public [WV00, Wy02, YKMY01, YG01c, YDK06, Zhe02a, AG09, BM03, BCL05a, BCW05, BBN+09, Ben01a, BB79, Bra01a, BD04b, Cal00a, CCT08, CL02h, CWH00, CCH05, CJ05, CKRT08, Cho06, DMT07, EKRAM01, EHHK04, FM02, FP00, Gal02, GH08, GKM00, GS01, Gor05, GMW01, HCD08a, HCD08b, HG06, HW04, HL04, Iwa08, IM06, JW05, JZCW05, KP02, Kob00, KW00, Kos01c, LKY05b, LCK04, LLW08b, LSO1c, LWK05a, MWS08, Mülo1b, PI06, PC09, SN00, SR01, Sha04b, Sha05b, Shp04a, SLC05, Sun00b, SZP02, SC05c, TO01, TLH05, Ts05, TJC03, VSO1, WDLN09, War00, Wu01, WH03, WL04b, hY08, YRS09, ZSM05, AL06, BDZ04, Ben02, C05, Des02, GL05, KGL04, Kim01, NP02a, Vau05a, YDKM06].
Public-Key [An01ih, AE005, BC05a, BM00, BB01, BLM01, B0502, CH03, CHK05, CMC01, CS02, CS03b, DPV04, DJ01, D009b, DXX02, DFK03, ESG+05, ES00a, FL06, GHW01, GC01b, HR05, IEE00b, Kat05b, KKIM01, KM01a, KLY02, KK02, KY02c, KL+00, KI01b, K04b, Kos01a, Kos01b, K0M01, Kos01c, M0303b, Mölo3a, Mülo1a, NPO2a, NBD01, NSS02, OTU00, PHK+01, Pei09, PR01, Po01, PFM03, Q001, RSA00a, RKZD02, ST01a, ST02, Sin01a, Smi01c, Ste01, TSO00, TT01, Vau05a, WZ05, WHI01].
Publication [Top02]. Publications [Bee05].
publique [RSA09a]. publish [SL05b]. publish-subscribe [SL05b]. Published [MS03b]. Publishing [An02b]. puce [Car00]. PUFs [MKP09]. Purpose [An07b, An07a, ESG+05, GS07a, GPP08, SGK08, L05a]. Purposes [LS05a, FSGV01]. Push [Pau03]. Puzzles
RCES/RSES [LLCL08]. re
[AH05, AFGH06, KHL09]. re-encryption
[AFGH06, KHL09]. re-signatures [AH05].
Reachability [AL00a, MT07]. REACT
[OP01b]. Reactive [Shy02]. Real
[BSW01, Dri02, GSB+04, JBR05, SP05,
Sta05, YKMB08, GM04, HP01, Lie05, SL07,
SGPH98, YZDW07]. Real-Time
[Dri02, GM04, YZDW07]. Reality [Coc01a].
Really [CZB+01, Wei00, Dav01c]. reap
[CH00]. reason [Lau08b]. reasoning [IK03].
Rebalanced [SWH+09]. Rebalanced-RSA
[SWH+09]. rebels [Lev01]. Rebuild [Salxx].
Rebuilding [Sal05a]. Receipt [HS00].
Receipt-Free [HS00]. Receipts [Cha04].
Receive [Coc03]. Receiver [CCD07].
Receivers [NNL01, SBB05]. recently
[JK01a]. Reception [Top02]. Recipes
[VM03]. Recipient [ANR01, Kur01].
Recipient [Coc01a]. recoding [SSST06].
Recognition [Ano02b, LLT+04, LST+05,
TZT09b, HS02b, Li05, MMJP03].
Recommendation [Bar06b, BK06a, BK07, Dwo03, NIS03b].
Recommended [Kel05]. Reconciling
[BNPW03, PGT07]. Reconfigurable
[FD01, FZH05, GC01b, KBD03, LZ04,
MKP09, MHH02, SJT09, SKG09, SRQLO3,
CMS08, DHL06, GC00a, HBC+08, Rhio3].
Reconfiguration [PBTW07].
Reconsidered [Sho01]. Reconstructing
[CDF01, FL06, PS01a]. Reconstruction
[AF03, CF01b, CDF01, JJ00d, KY01c].
Records [Dur01]. Recoverable
[NZCG05, SGMV09, YY00]. Recovery
[BDK+09, BM01c, CKM00, OS01, PBC05,
TC01, VV07, WCZ05, WLT05b, CCH05,
CJ05, HW05, LKJL01, PSP+08, Sha04b,
SIR04, TJC03, Wu01, ZF05]. Recursive
[WHHT08]. Recycling
[DS05, TR09a, TR09b]. Red [Sas07].
Red-Eye [Sas07]. redistribution [KB09].
Redondo [IEE00a]. Reduced
[BDK02b, CS05b, FKSW00, HQ01, HSR+01,
KKS00a, KS00b, KKS01, KML+02, KM01b,
KKS00b, MHL+02, NPV01, STK02, SK01,
YSD02, CV05, Küh01, SK01a]. Reduced-Round [FKSW00, KKS00a,
KS00b, KKS01, KML+02, KKS00b, NPV01,
YSD02, CV05, Küh01]. Reducibility
[DM00b]. Reducing
[AL07, BIM00, SPH00]. Reduction
[CM05a, CH07c, Dhe03, Gro01, HGG07,
Kid02, PG05, ALV02, HG07, Sug03].
reductions [Fis01a]. Redundancy
[AB01, BR00a, FM02b, YL005].
Redundant [MF01, Tan07a, PS04a].
Redwood [KKP02]. Reed [KY02b].
Reference
[BR09, CPS07, Pas03, RS00, Sal07, vT00].
Reference-Watermarking [BR09].
Refined [Sma03b]. Regarding [GMP01a].
Regex [BTTF02]. Region
[BSNO00, Bur00]. Region-Based
[BSNO00]. register [HTW07]. Registers
[CGFSHG09]. Registration [HLM03].
regression [mSgFl05]. regulations
[Cha00b]. Rehearsal [Ahm08]. reinforce
[SWR05]. Related [BDF+01a, Can06b,
CY08, FKSW00, Kii01b, KLM05, Sat06,
Buc00a, Gutxx, HAN04, Hen06, Sch00b].
Related-Key [FKSW00]. Relation
[ABC+05, NN06]. Relational
[AK02b, AHH03a, AHH03b, GA03, PT08].
Relationships [BN00a, Uni00a, Uni00c, Zha08].
Relationship [Ngo05, GKM+00].
Related-Key [FKSW00]. SKU+00].
relative [JRS09, Müh01b]. Relaxing
[CKN03, PS05]. Relay [DM07b, Zha00].
Release [CHKO08, Mao01, HGNS03].
Released [Bar00c]. Releases
[BR00c, AJ08]. Reliability
[IKP+07, WK05]. Reliable
[JR03, MPH06]. reloaded [SL06].
Remainder [Sch01b, YKLM03]. Remarks
[BCW05, CL04d, SCS05c]. Remember
[HSH+08a, HSH+08b, HSH+09]. Remote
[CRW09, Kra02b, LL05c, Rub01, TK03].

WKB08, CC01, CL04d, CJT01, Hsu05b, HL05b, KC05, LHY02, LLH02, LKY05a, LHL03b, LC05a, SZS05, WL07a.
remotely [Küh08, SR00]. Removal [LLS05a]. Removing [JL00]. rencontres [PPV96]. Renewable [TOEO00].
Removals [LLS05a]. Removing [JL00]. rencontres [PPV96]. Renewable [TOEO00].
Renewable [TOEO00]. Repairing [DKFX05, GM00b, HL04, ZJ09, BKN04]. replace [Gav08]. replication [BIW08].
Reply [WLW04]. Report [DFG01, Pre01, Sal01a, Sha03b, BCHJ05].
Repository [Bar00b]. Representation [BJvdB02, FSW01, JLMS03, JY01, RN00a, RN00b, ZLK02, BDSV08, BA06, PS04a, SWR05]. Representations [OSSST04].
Representative [CTBA+01]. Representatives [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Republic [MJ04, dL00]. Republiek [dL00].
repudiation [HLL04, LSA+07, SC05c]. reputation [KNS05, RCG+05]. reputation-systems [KN05]. Request [RSA00b]. require [SV08a]. Required [Sun00a, Lov01, Wan05].
Requirements [FIP01b, HH01, Kin02, NIS01b, Mea04]. Rescue [ASW+01]. Research [AJ01b, CZ05, CZK05, DFPS06, KGL04, LXM+05, RC06, Sch00e, TMM05, DFCW00, JXW05, MH09, QS00, dCvV05].
Researchers [Pau02b]. Restartable [DPV04, MR01b]. Residue [TIGD01, YKLM02b, CNPQ03, FP00, LD01].
Residues [Coc01b, Zhe01, CCS08]. Resiliency [Joh00]. Resilient [Che01c, DSS01, DFK+03, DP07, DP08, GSS08, KZ07, SM00b, KZ03, IR02]. Resist [HM02c]. Resistance [HNZ02, Mö02, EBS01]. Resistant [An001e, ACJ07, AN01, AN05, CDT05, CNV06, Gir06, IK005, LLS05a, LWS05, LTM+00, LNL+08, KS09, PC09, WL04b, YS02]. Resolution [SGM09]. resolving [Lin01a]. Resort [USE00b]. Resource [MRL+02, Tse07].
Resource-Constrained [MRL+02]. resource-limited [Tse07]. Resources [Gutxx, FOP06]. Response [JBR05, XNK+05]. Responsibilities [Vix02]. Resting [Gut02a]. restricted [ASW00]. Restudy [FWL08]. Results [APV05, GM02c, OOP03, RR08, Way02a, YRS+09, CV05, CKRT08, DM07a, GM000, PM08].
Rethinking [Bra01a, KMZ03].
Retreat [FKSW00]. Retrieval [BIM00, KO00, RE02, Yek07]. Retractive [DS01]. retrofitting [CGL+08a, CGL+08b, CGL+08c]. Reversal [Cap01, DIS02]. Reversal-Bounded [DIS02]. Reversals [MS02e]. Reverse [Coo02, EC05, Wue09]. Reversed [Ina02b]. reversibility [KC09]. Reversible [Go03].
Reversing [EC05, YWC08, YNI01, CDFM05]. Review [And04, An02e, Duw03, Ead05, Fon07, Gas01, Gun04, Im03, Irw03, Jan08, Lee03a, Lee03b, Mar05a, Pag03, Pap05, Puz04, Roe01, Rot07, See04, Spr03, Ter08, TvdKB+01, Top02, Uzu04, Was08a, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wa00].
Reviews [For04, Kid00, Sal03b, Sty04].
Revised [Bla03, BC05b, Chr01, CCMR02, CCMR05, CS09, CGP03, DR02c, GS02c, GH05, HH04, HH05, Joh03, Jue04, KKP02, KRC04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PT06, RM04, SL01, Ytr06, AMW07, AJ01a, BK07, Bir07, CZ05, CKL05, DR05, IR03, PY03, WK06, WR03].
Revisited [ABC+05, BM01b, CDMP05, Knu00b, NS05c, OSSST04, Res04b, ZTT05]. Revisiting [AEAQ05, Har01a, Har01b, JMV02].
Revocation [BDTW01, CL02a, Gen03, GSO04, NNL01, TT01, ZSM05, KT06, KSW06, LHH05].
revocation [NN03]. revolution [Bor00, Con00]. Revolutionary [CMB+05]. Rewriting [Cir01, HR04a]. RFC [BWBL02].
Revolutionary [CMB+05]. Rewriting [Cir01, HR04a]. RFC [BWBL02].
REVOLUTIONARY [CMB+05]. Rewriting [Cir01, HR04a]. RFC [BWBL02].
And04, AL07, ACDM05, BLD09, CCS08,
[Küh08]. Rhode [IEE07]. RI [Sil01]. Right [Dhe03, GS07b, HKPR05]. rightful [CL08, Lin01a]. Rights [Bar00a, BNPW03, Dre00, Wya02, BA06, UP05].

Rijndael [BB02, MP01a, SKU+00, Wer02, CKK+02, CGBS01, DR00a, DR00b, DR01, DR02b, FKS+00, FKL+01b, FSW01, FD01, GM00a, JmBdXm05, KY01b, KMT01, KV01, Luc00, MM01b, MMH02, PSC+02, RDJ+01, SMTM01, SRQL03].

Rijndael-Like [PSC+02].

Ring [BSS02, Nao02, WBL01, ZK02, Her07]. Rings [BLST01]. RIPEMD [DG02, WFLY04].

RISC [Cor00a, Gro03, WWCW00]. RISC-Based [Gro03].

RISC-Based [Cor00a, Gro03, WWCW00].

Risk [WA07]. Risks [ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, PV01, Sch00c].

Rivest [BB79, Coc03, SP79].

RMI [JRB+06, Mar02a]. RNS [BI04, BKP09, NMSK01]. Road [BDPV09, HR04b, PB01]. Roadmap [Cor02b].

Roaming [CAC03, YWD08, SSM+08]. Robots [Cor01a].

Robust [BB00a, BR09, CJ03c, CW05, DDO+01, hKL00, Lin00a, LHS05, LLC06b, PJ01, SG07, SOH01, SDFH00, SDF1, VK07, WNY09, WL04b, WMDR08, YPSZ01, ZTP05, LC05c, LKZ+04, Mit00, MB08, YY05b].

Robustness [CS05b, HM01b, Rot01, CKL+09]. Roger [GG05a].

Role [SBG02, YT09, ZGLX05, Cer04a, Cra05b, Gor05, Mau04].

Role-Based [YT09, ZGLX05, Cra05b].

Roles [LLL+01, Vix02]. Roma [AAC+01].

Rome [IEE04]. Ronald [Cor03]. root [Pet05].

rootkit [Blu09]. Rootkits [HB06].

Roots [Gon06, HCK09, CAC06]. Rootx [PY05].

Rotation [RBF08]. Rothe [Fal07].

Rough [Naz02, WG05]. roughness [Lav09].

Round [II00, BP04, Biho00, BF00a, BDK02b, Che03, DP04, DL05, Dra00, FKS00, GKKO07, GIRO02, HSR+01, Kan01, KO04, KS00a, KS00b, KS01, KML+02, KSS00b, KHL09, Lin01b, MP03, MHL+02, NPP01, RR00, Ros06, STK02, WBRF00, Wer02, YSD02, CV05, CLC08, CKL+03, DLP+09, GIRO1, HSL+02, Küh01, LKH+08, MR01b, Pha04, SW05].

round- [CLC08]. Round-Complexity [Ros00]. Round-Optimal [KO04]. Rounds [BDK+09, CD01, HSI02, KM01b, Luc00, Pat03a, Pat04, GM00a, SK01a].

Routing [BG08, CL05, Ken02a, KB09, LAP08, LHC08, MBAI06, PS08a, RVS09, vOW07].

RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02b, Shp04a, Wal00, Adl03, Ano01i, Ano02c, AR01, BI04, BL06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BN00, BF01c, Bon01, BCC01, BP01b, CNS02, CDL+00, CW02, Che01a, CK05, CN03, CKN00, CNP02, CS00, CS03c, CD01b, DK01, DT03, Duj08, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gro01, HN04, Her07, HL03, HL00, HL03, Int00, JS05, Jon08, JK02b, J02b, J01, Kal01, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May04, Miy01, Mol03b, MP01c, NZC05, NS01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Shao03a, Shp01, Shp04b, SZ01, Str02, SWH+09, TIG01].

RSA [TT00, Ver06a, Wal01, Wal03, WQW01, War00, WHL00, Wic00, WS02, W05, XC05, Yan07, YKLM02, YKLM03, YPK08, YY00, Y06, ZC09, Zhe01, ZWCY02, dW02].

RSA-Based [BNPS02, GMP01b, KPR03, Ver06a, HL03, NZC05, Sei05, WHL05, W05, YPK08, YY00].

RSA-Encrypted [CD01b].

RSA-Primitive [ST01a]. RSA(R) [Ano06a].

RSES [LLCL08]. RST [ZLZ07].

Rueppel [Ara02]. Rules [Bla01a, Bla01b, GM04, Ste02, Wue09].
Running [ZL04c]. Running-mode [ZL04c].
Runtime [PBTW07]. Russia [GKS05].
Ryan [Puc03]. Rye [KJR05]. Ryu [KCC05].
S [BZ02, Kat05b, Puc03, Bih00, BCDM00, Dav01b, Dav01c, FM02b, JnBdXgXx05, Opp01, SMTM01, ZC00]. S-Box [FM02b, SMTM01, JnBdXgXx05]. S-boxes [BCDM00, ZC00]. S/MIME [Dav01b, Dav01c, Opp01]. SAC [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR+01, HSS04, ST01d, VY01]. SAC'99 [HA00]. SAFE [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Oiw09]. Safe-Prime [ACS02]. Safeguarding [Sty04, Bar03]. SAFER [NPV01, BDD03]. safety [HM01a]. SAFKASI [WAF00]. Salsa20 [Ber07, Ber08]. Salt [PKBD01]. Salzburg [DKU05]. Samba [BH00a]. SAML [RR04]. Samos [KGL04]. sampled [WW06]. sampling [KB39, Sug03, Tip27]. San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Oka04, Poi06, Pre02b, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c]. sans [Car00]. Santa [Bel00, Bon03, Fra04, Kii01a, Men07, Sh05a, Yun02a]. Santiago [BS03]. Sanxin [LSZ05]. SAR [B+02]. SASAS [BS01c]. Satan [Mee04]. satellite [CC05c, HYS03]. Satisfy [PHM03]. satisfying [QP05]. Saturation [Luc02a]. saving [Lev01]. Savings [CAC03]. SAX2 [TEM+01, Hei01]. Say [Sta05]. SBLH [JK02a]. SBoxes [WOL01]. SC-CFS [It001]. SC2000 [SYy+02, YSD02].
SC2001 [ACM01b]. Scalable [CPhX04, HKA+05, HLY05, KIY05a, KXY05d, LC05b, LM+03, LHY04, LTH05, LL05a, LMC+03, LLH04, LL05c, L05b, LC05a, LD04, LYGL07, LCC05, LC04b, LC05a, LHH05, LC05b, LC05c, LCZ05a, LKW05b, MSC09, NC09, PW05, PMMB01, PC03c, P05b, P01a, Pei04, Sae02, S04a, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, mSgFl05, SCS05b, SC05c, SC05c, SZS05, TLH05, TML05, TYH04, VK08, VS08, Wan04b, WL05, WK05, WJP07, WDLN09, WHH05, WC01, WH02a, WHLH03, WH03, WL04b, XC05, YTH04, YW04, YCH04, hY08, YRY04, YRY05a, Y05a, YBY05, YbJf04, ZC04, Coc02b, SDFH00, SDF01, PBVB01].
Scambray [Gum04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Ols00]. Scenarios [BF05]. scene [SG07]. Schedule [MHH+02, XH05].
Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BNPS02, Br09, BS01d, BMS03, CL01a, CHK03, CGH01, CHY01, CHH01b, CM05a, Coc01b, CFS01, CDM00, DFK05, F01c, GJS001, GS02c, HS02a, HNZ02, HY01, HT06, Igl02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, Miy01, Milk01a, OKS06, PL01, RK06, SOO02, SWH05, SGGB00, SYLC05, SSNS00, Tad02, TC01, Ts01, TT01, WQW01, WZW05, WBD01, YG01a, YLH05, Z09, AEE005, BCL05a, BCAW05, BKN04, BBG02, CL02b, CC01, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CH05a, CHY05b, CL00, CHC04, CCH04, CY05, CHC05, Che05a, Che07, Che08a, Che08b, CC08, CK06, CJ01T01, DW01, FXAM04, FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HWW03, HWW04, Hs05a, HWH05, Hsu05b, HC04a, Hwa00, HY03, HLL04, Hwa05, HLY05, H05d]. scheme [HL05b, JW06, JSW05, KC09, KLY03, KRY05, KSW06, KHL09, KCL03, Kn04, KC05, KCC05, KHKL05, LHY02, LLH02, LMC05c, LHY04, LLY04, LLY05a, LKY05a, LKY05d, LMC+03, LHY04, LTH05, LL05a, LMC05b, LC04a, LYGL07, LCC05, LC04b, LC05a, LHH05, LC05b, LC05c, LCZ05a, LKW05b, MSP09, NC09, PW05, PMMB01, PCC03, PC05b, P01a, Pei04, Sae02, S04a, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, mSgFl05, SCS05b, SC05c, SC05c, SZS05, TLH05, TML05, TYH04, VK08, VS08, Wan04b, WL05, WK05, WJP07, WDLN09, WHH05, WC01, WH02a, WHLH03, WH03, WL04b, XC05, YTH04, YW04, YCH04, hY08, YRY04, YRY05a, Y05a, YBY05, YbJf04, ZC04,
Schemes [AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00, CL04a, CT08b, CPD06, CKN00, Cor02, CJNP02, Cou04, CS00, CS03b, CDG05+, CLZ02, DN00a, DN02b, Des00b, DN00b, FF00, HSZI00, HW005, HM02b, HLI05, Kin02, Kos01a, KS03, KOMM01, LZ2a+, LP01, MV00, NIS03b, Nam02, NN01, NN06, OP01a, Pat04, Pre01, ST01b, SBZ02, SPMLS02, Sun00a, VMS05, XSO3, YWCO8, YYD001, Yek07, YYYZ01, ZTP05, ZYR01, Abd01, AFGH06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGK03, HCD08a, HDC08b, HAnR04, He02, HKS00, HW04, HW05, HCO4b, HL04, IY06, JXW05, KIY05, Kir01, KT06, Kre05, Kuhl08, LWZH05, LWK05a, LW05c, MF07, Mi001b, NK06, PS02a, PKH05, QCB05a, QCB05b, SN00, Sha03d, Sha05b, SCL05, SHT05, Tsa05, Wu01, XY04, YWCO5].
schemes [YCW08, ZF05, ZCL05, vDKST06].
Schloss [IEE01b]. Schneider [Puc03]. Schneier [See04, Sty04]. Schnorr [BP02]. School [Coc02a]. Schools [PM00]. Science [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Imr03, Nie02d, Pag03, Sch06b, SM07, Sin01b, CAC06, PRS04].
Scientific [CHT02, MH09, Lau08b]. Scientists [Coc01a, MH09]. Second-Order [NM09]. Second-Price [Bra01b]. Second [AC03c, Bra01b, BD08, CZ05, GW01, HTS02, JYZ04, KCR04, Ki05, KP01, NM09, RD01, ACM00, Irw03, Sin00, Spr03].

Searchable [ABC+05, AF06]. Searches [PGT07]. Searching [BSW09, GTTC03, OS05]. Seattle
ACJT00, AFI06, BDF+01a, BST03, BCL+05b, Bar03, BS105a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CK02b, CHK03, CHK05, CW07, CQ0101, CHJ+01a, CHJ+01b, CDM00, CD01a, CS02, CS03b, CDG05, CDI05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, F0PS01, GP0808, GIKR02, GJKR03, Gen04a, GD05, HSZ100, HSZ101, HSH06, HRS02, Har07b, HKW06, HLvA02, HvAL09, HR04b, HL07, Hutt01, HLC08, IR01, Ito00, IFH01, JJ00a, JL00, JMV02, KMM+06, KY01a, KO04, KLM05, KC02, KH05, KKL09, KI01b, Kos01a, Kos01b, Kra01, Kra05, KSR02, LCK01, LLL02, LCK03, LWK00, Lin01b, Lin03, Lin02, MKP09, Mar02a, Mar07, MV01, Mi03a, MJD01, NMO05, Nam02, Nd05, NSN05, NS02, OK06]. Secure [OKE02, OT03b, Opp01, PS08a, RV09, RsD01, ST01a, Sea05, SVDF07, SB05, Sni02, SKR02, SN04, SBE01, Sty04, Tad02, VMS05, Vau05b, VM02, VM03, WLLL09, WBL01, WGL00, XSM03, ZYM05. Aan03, Abd01, AEEdR05, AL07, AGF06, BDS+09a, BDFP05, BCP07, CLOS02, CC04b, CCK04b, CRS09, CH09, CG05, Dwi04, FMY02, Geb04, GIKR01, GCKL08, HS09, HL03, HL06, HJ05, HBC+08, Ino05, ISTE08, IO07, KY06, KOY09, KGO9, LL04b, LH04, LHC08, LC04a, LCZ05b, M09, MLI01b, OS00, PC0707, PBM01, P0SP+08, RH03, RG09, RGX06, Sea09, SB07, SGMV09, TKP+08, TCR03, Tse07, Ver01, VK08, WWA01, YZG05, YT05, Y08, YRY04, ZBP05, ZCL05, vW0K07, Ano08, Ano12, BS01a, BS05, CHK08, FIP02b]. Secured [BNPW03, It0101, UP05]. Securely [HL05a, LL05]. Security [AW05, AW08, A0m07, AJ08, AD02, And07, And08, An06b, AK02, B070, BW07, Bam02, BPS00, BB00, BP02, BNPS02, BY03, BPR05, BOH1+05, BBI+02, Bis03b, Bla02a, BF06b, BDTW01, BCHK07, Boy01, BLS00, C0M07, CK02a, CKN03, Ca06a, CHG01, Cer04b, CC02b, CS+08, Che05b, CM05a, CH07a, CSY09, Ch03, C0c01a, CK06, Cor00b, Cor02, CGP+02, CG05, Dr.00c, Dal01, DN02a, DMR05, DeL07, Des00c, Dim07, DR02d, DSS01, DK05, DS05, D08+06, El09, E0L01, F0P01b, FBWC02, FW09, F0Y06, For04, FLM+03, FMY01, G02a, G0303, Gum04, G02b, Gut04a, Gutxx, HM00, HSZ101, He07, HM02b, Hir09, HLL+01, HGN0+03, HQ05, HL05c, HL05d, ISO04, In02a, In02b, Int00, IY05, IKP+07, JY04, JP02b, JSW05, J07, Jol01, JBR05, J0K02b, J0K02b, JMV02, JQY01, Kan01]. Security [KM02, KSH01, K05, Ken02a, KB06, KM03, KDO01, Koc02, KHL09, Kos01a, KKD00, L06, Lai03, Lan00a, Lan04b, LGS01, Lee04b, LKH+08, LKHL09, Leh06, Len01, LNS02, L04c, LSH03a, LSH03b, Lin02, LXM+05, LWK05, LP01, MJF07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Mli01a, NIS01b, ND01, NP07, Oka00, OP01a, Or00, PV06b, PSC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PTP07, PP07, Ph01, Pie01, Pli01, Pol02, PM03, Poo03, PF03, PS05, Puc03, Puc06, QC05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sa03a, ST09, Sch04d, Sch00e, Sch07, Sch08, SJ00, Sch01f, See04, Sh05d, SLG+05, SL05a, Shp02, SEF+06, SEK01, SEK02, SK06, Sta03, SB07, Ste05b, SZ02, Sty04, SK01, Sun05, Swi05, Tan07b]. Security [TG07, TG04, TPPM07, U00a, USE00d, USE01c, USE02b, U00c, U00e, U00d, U00g, Uzn04, Vau02, VM02, WLT05a, WBL01, WWL+02, WA07, YEP+06,
64

YWD08, Zan01, ZWC02, ZDW06, Zhe02b,
ZYH03, ZS05, AA04b, Ano05b, AJ01a,
AJ01b, Bai08, Bau05, Bej06, BR04, BGP09,
BFGT08, BFG08, Bjo05, Ble07, BJ02,
BMW05, BG07a, Bru06, BMV06, Can01a,
C+ 02, Cha07, Cha05b, CKL+ 09, CKRT08,
CJL06, CJM00, Con09, Con04, CC05e, DP04,
DKK07, DY01, DFGH04, Des00a, DWML05,
DKU05, DMS07, Egh00, FXAM04, FR08,
FOP06, GH08, GJL06, GJJ05, Gha07, Gor05,
GKS05, GMW01, GC05, HN04, HCD08a,
HCD08b, Har05a, Hen01, Hes04a, HM05,
HSL+ 02, HL06, HG05b, Ino05, JEZ04,
Jan00, Kad07, KY00, KPS02, Kim02, Kov03,
KH03, Kwo03a, LC03, LL03, LJY04, LL05b].
security [LPW06, LMC+ 03, LMW05,
LLLZ06a, LLLZ06b, LHC08, MJ03, Mal06,
Man08, Mau05, Mau04, May01, MKKW00,
MSK03, McG06, Men03, MS02d, MK05a,
MPPM09, OP01b, Pae03, PSG+ 09, PC05a,
Pat02a, PY05, PP06a, Pau03, PHS03, Poi00,
PS04c, RC05, Ros06b, RN00a, RN00b,
SNI00, Sal05d, Sch03, Sen03, SHL07, Shu06,
SPHH06, Son00, SH00, Sta02a, Sta06, Ste02,
Sun00b, SHT05, SLL+ 00, Tsa05, Uni00f,
Vac06, VS08, WAF00, WA06, Won01, WK06,
XQ07, YW04, YY05b, ZSZ01, ZW05b,
ZSN05, dCdVSG05, vOWK07, vT05, AG09,
Ano02c, BC05b, BP01b, Chr00, Chr01,
CCMR02, CCMR05, CGP03, JRB+ 06,
Lin02, RR04, Uni00h, ZL04c, Pap05].
Security-related [Gutxx].
security-sensitive [SPHH06]. seed
[TP07, KKJ+ 07]. Seeing [Wal03]. Seek
[Coc01a, PH03, Shp05]. seeking [Mos06].
Seeks [CAC06]. Seems [Coc02a]. Selected
[BKP09, Bar00c, CCMR05, CSY09, GH05,
HA00, MS05a, Neu04, PT06, RSA00e,
ST01d, VY01, Ytr06, AMW07, Bir07,
BC05b, CZ05, CKL05, DRS05, HH04, HH05,
PC05a, Wil99, WK06, AMW07, HH04,
HH05, MZ04, NH03, PT06]. Selecting
[Bur03]. Selection
[IBM00, JKK+ 01, RS00, SM08]. Selective

[CS07c, LS01a, LM02]. Selective-ID
[CS07c]. Selectively [Chi08]. Self
[GMM08, HW05, KY01d, PS01b, PBC05,
Sch06b, WHLH05, WLT05b, ZKL01,
BCL05a, BCW05, CSV07, CWH00, CCH05,
CJ05, Fis01a, HW04, HL04, Lee04a, LL06,
LS05b, LWK05a, PC05b, Sha04b, Sha05b,
TLH05, Tsa05, TJC03, WH03, Wyl05].
Self-certified
[HW05, BCL05a, BCW05, CWH00, CCH05,
CJ05, HW04, HL04, LL06, LWK05a, Sha04b,
Sha05b, TLH05, Tsa05, TJC03, WH03].
self-defense [Wyl05]. Self-Enforcing
[GMM08]. Self-Escrowed [PS01b].
Self-Localization [WLT05b].
self-modifying [CSV07]. self-pairing
[Lee04a, PC05b]. self-protecting [LS05b].
Self-Shrinking [WHLH05, ZKL01].
Self-Similarity [Sch06b]. Selling [Bla01c].
semantic [SNI00, Sch00c, Coc01a].
Semantically [KI01b, ST01a]. Semantics
[Li01, Mar02b, BFG04, BFG05]. Semi
[Fer00, Nak01, SY01b]. Semi-Equivalent
[Fer00]. Semi-fragile [SY01b].
Semiconductor [Coc02b, Igl02, UHA+ 09].
Seminal [Cop04b]. semipublic [YC07].
Sender [CMB+ 05, TJ01a]. Sensation
[Top02]. Sensible [Sch04c]. Sensibly
[See04, Sty04, Sch03]. Sensitive
[HT06, Bro05b, SPHH06]. Sensor
[AEAQ05, CS08b, DBS+ 06, Fin06, GPČS08,
LNL+ 08, NABG03, PJDH09, ZYN08, AJS08,
CCMT09, HMvdLM07, JRR09, KXTZ09,
KHYM08, LDH06, LPV+ 09, LN04, MWS08,
MS09b, NC09, NLD08, PS08a, RAL07,
TP07, WDLN09, ZSJN07]. Seoul
[CKL05, KCR04, Kim02, LL03, LL04c,
May09, PC05a, PK03, Son00, Won01, WK06].
Separable [CD00]. Separating
[MKKW00, Nie02b]. Separation
[BYJK08, GKK+ 09, Kel00, Lys02, Mur00,
ZGLX05, BYJK04]. separations [GKK+ 07].
September
[AUW01, AAC+ 01, AJ01a, BCKK05, BC05b,


September 19 [AJ01b]. September 19-21 [AJ01b]. Sequence [HWH01, KWP06, Uni00g, Mit00]. Sequential [GSS08, SNW00, RMH03a, WH02b]. Server [ANRS01, BMK00, Dew08, KO00, LWK00, NS01b, PS05, TMMM05, ´ACTZ05, GB09, SL09, WG02, YZEE09]. Servers [BDET00]. Servers-Aided [XS03]. Servers-Assisted [KS00a, LD04]. Serverless [BDET00]. Server-Assisted [KS00a, LD04]. Serverless [BDET00]. Servers [BIM00, HS07, Jab01, KCD07, Mar02a, TEM+01, LS05b, PT08]. Service [BACS02, BH06, BBDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYL05]. Shares [TT01]. Sharing [BTW05, Bi05b, BTW08, BG05, BD05, CDM00, CF05, CF06, CS03, JRFH01, KS05b, WG05, BDET00, Che07, CC05d, DM00a, Mar05b, Sta00]. Session [LLK05]. Session-Aware [OHB08]. Session-Key [GL01]. Sessions [KPR03]. Set [BBG08, GRW06, JRFH01, KS05b, WG05, BDET00, Che07, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01]. Sets [CS03, EIG01, TW07]. Setting [BBM00, DLY08, LP01, PGT07, GMLS02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC+01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SGB01]. SGI [Bar00c]. SHA [AD07, BC04a, GLG+02, HKR01, MP06, SK05a, TULL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG+02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TULL02]. SHA-512 [AD07, GLG+02]. SHA1 [WYY05a]. SHACAL [KML+02]. Shacham [Hes04a]. Shamir [BB79, SP79, Coc03, PW05, VS08]. Shamir’s [LD04]. Shape [Gan01b, Gil07]. Shapes [OMT02]. SHARC [DMSW09]. Share [CT08a, CI05, FS04, AEEEdR05]. Shared [ACS02, BH06, BBDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYL05]. Shares [TT01]. Sharing [BTW05, Bi05b, BTW08, BG05, BD05, CDM00, CF05, CF06, CS03, JRFH01, KS05b, WG05, BDET00, Che07, CC05d, DM00a, Mar05b, Sta00]. Shift [CGFSGH09, Che08a]. Shin [KHH08, KHH08]. Shines [Coc02b]. Shinko [An00b]. Ships [An02c]. Shops [An01c, YSS+01]. Shor [KLB+02a]. Shores [KKP02]. Short [An01a, AI06, BBS04, BG05, DN00b, Gra02b, LS01b, PM02, RR02, RW02, Vau05b, GL05, WDLN09, Coc02b, Sch01e]. short-term [WDLN09]. Shortcuts [Sha03a]. Shortened [Kur01]. shortest [Pel09]. ShortPK [WDLN09]. Shoup [Luc02b, VMSV05]. shows [AJ08]. Shrinking [Gol01c, WHLH05, ZKL01]. SHS
Shuffle [Mir02]. Shuffle [FS01c, NSNK05, Sas07]. Shuffles [FS01c, NSNK05, Sas07]. Shuffling [PBDO5]. Shut [Gil07]. SiBIR [IR02]. Sic [IEE09a]. sichere [Lin02]. Side [Ano01g, BU02, Law09a, LL01, M¨ol02, OT03a, OT03b, Sch06a, CNPQ03, PSP+08, WL07]. Side-Channel [BU02, Law09a, M¨ol02, CNPQ03, PSP+08]. Side-Channel [BU02, Law09a, M¨ol02, CNPQ03, PSP+08]. Side-Channel [BU02, Law09a, M¨ol02, CNPQ03, PSP+08].

Signature-Based [CK02a]. Signature-Embedded [Ano01c, YSS+01]. Signature-Tree [TNM00]. Signature/Signature-Based [CK02a]. Signature-Embedded [Ano01c, YSS+01].

Signature [ANS05, AAK09, AR00, ADRO2, Ano01c, Ano01f, Ano09, Ano13, Ara02, AR01, ACJT00, Bar06b, BNPS02, BGOY08, BMS03, BDS09b, CM00, CD00, CL04a, CK02a, CH01a, Che02, CM05a, Cor02, CFS01, CS00, DFKX05, Eng00, FIP00, GJ00, GS02c, HY05a, HS01, HM02b, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, MM02, MNFG02, PCG01, Ram01, RR02, Rds01, WV01, XZ01, Z02, Ate04, AH05, BLH06, BB05, BMW02b, BNPS02, BLRS09, Cal00b, CKK03, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HLH00, J01, J04, KKKL09, LV07, LS01b, MMJ05, PJ05a, Sch01f, Sh01d].

Signature-Based [CK02a]. Signature-Embedded [Ano01c, YSS+01]. Signature-Tree [TNM00]. signature/signature-Based [Wu01].

Signature-Based [CK02a]. Signature-Embedded [Ano01c, YSS+01]. Signature-Tree [TNM00]. signature/Signature-Based [Wu01].

Signature [ANS05, AAK09, AR00, ADRO2, Ano01c, Ano01f, Ano09, Ano13, Ara02, AR01, ACJT00, Bar06b, BNPS02, BGOY08, BMS03, BDS09b, CM00, CD00, CL04a, CK02a, CH01a, Che02, CM05a, Cor02, CFS01, CS00, DFKX05, Eng00, FIP00, GJ00, GS02c, HY05a, HS01, HM02b, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, MM02, MNFG02, PCG01, Ram01, RR02, Rds01, WV01, XZ01, Z02, Ate04, AH05, BLH06, BB05, BMW02b, BNPS02, BLRS09, Cal00b, CKK03, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HLH00, J01, J04, KKKL09, LV07, LS01b, MMJ05, PJ05a, Sch01f, Sh01d].
simulatable [Lau05]. Simulation [DKMR05, KL05, CPG+04]. Simulation-Based [DKMR05, KL05]. Simulations [WBRF00]. simultaneously [Wu01]. Singapore [BDZ04, TLC06]. Singh [Imr03, Ree01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a]. Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09]. SINOBIOMETRICS [LLT+04, Li05]. SIP [NTW07, PM00, SZ08]. Sit [AEV+07, Coc02a]. Sites [Ros07]. situation [AJ08]. Six [Bel07]. Sixth [Uni00a, Uni00b, Uni00f, Uni00h, TLC06]. Size [CS07c, CMJP03, HNZI02]. Skein [AEMR09], Sketching [MNS08, SLTB+06]. Skipjack [Gra02a, HSL+02, SLL+00]. Skipjack-like [HSL+02, SLL+00]. SKLOIS [FLY06]. Sky [MYC01]. SLAAC [CGBS01]. SLAAC-1V [CGBS01]. Slide [Fur02b]. Small [CCM05, ELvS01, Fin02, GPS06, MNT+00]. Smaller [Bar00c]. Smart [And04, Ano03a, AJ01b, Bel01, BCST00, Car01, CL07, DF01, DFCW00, DJLT01, HbdJL01, Hen01, HQ05, Jac00, JSSJ01, JY01, Lan00d, LSA+07, MOP06, MV01, MG08, NFQ03, QS00, QS01, RE00, RE03, RS01, Sak01, SR01, Sha10c, SP02, TBDL01, VPG01, YKMY01, An04c, AJ01a, Bor00, BPR01, BCHJ05, BGL+03, Bur00, Cal00c, C CCY01, Cha05a, Cha06b, Con00, CH00, DMT07, DFH01, DFFST07, Fin03, GMG00, GU01, HHS01, Hsu05b, Hus01, KLY03, LKY05a, Lcr02, LC05a, Lu07, MY01, PB01, Pre07, SVDF07, TIS07, V08K, BVdDB02, CL04d, CCK04b, Che00, DFPS06, FGL02, Gro03, HL05b, Ku04, KC05, LHY02, Pau02b, SKKS00, Sco04, SCFO1, TV03, YW04]. smart-card [GMG00]. Smartcard [HWH01, KRV01, RMCG01, Uri01, PBVB01, BBPV00, CGMM02, DM07b, HRS02, It001, KS02]. Smartcard-Based [RMCG01, CGMM02]. Smartcards [CMG+01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, Ano04b, RM02]. smarter [Car01, Cla00b]. Smartly [MS01]. Smooth [PS02b, GMR05]. SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. Sniff [Ano02c]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sae02, Sha03c]. Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Akm07, And07, Ano02c, Bar00b, BC04b, Coc01a, DR02c, DF01, GH05, HJC02, HM01, Hoe01, Jeh03, Kun07, KS02, Lad06, Law09a, LSY01, LLLZ06a, LSVS09, LTM+00, MNT+00, MSNH07, MKY08, Mc06, Nd05, PM00, SW07, SM02, YL07, ZW04]. Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [Hoe01]. Software-Oriented [ZCC01]. Software/Hardware [Nd05]. SOI [Ano02c, NFQ03]. SOISCIC [Ano02c]. Solaris [Ano06b, BH00b]. Solomon [KY02b]. Solution [Cap01, DHR00, LLS05b, Str02, TvdKB+01, LSH00]. Solutions [Akm04b, MV01, Jan00, MSK03, MV03b, Gum04]. Solve [CU01, GS03]. Solving [CJT04, GPP08, Wil01a, Bu09]. Some [AG01, BDF+01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Han04, He02, JK01a, RSS04, SHT05, ZF05]. Something [FL01b]. sometimes [FNRC05].
Sons [And04]. Sorry [San05]. Soul [Bla01c].
Sound [BJP02, FR08]. Soundness [DPV04, MR01c, Lau08a]. Source [Bar00c, Bol02, Gut00, HBF09, KLR09, PM00, RK06, TEM+01, Ano03b, BGL+03, McA08, RVS09, SB05, Bar00b, Lin02].
Sources [KZ07, WLZZ05, KZ03].
Southampton [Bla03]. Soviet [AJ08]. SP [BG07a, Hir09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPA-Based [Nov01].
Space [BGH07, Lu02, MSNH07, NS05a].
Space-Bounded [Lu02]. Space-Efficient [BGH07]. Spain [BS03, DFP06]. Spam [CMB+05, DGN03, Vix02]. Spamming [Bel04]. SPARK [Jun09]. Sparse [BLST01, BDG+01, FS01b, GS03, BF06a].
Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09]. Spatial-Domain [SDFH00]. Spatio [CDTT05]. Spatio-Temporal [CDTT05]. speakables [BZ02]. Speaker [LM00]. Speaks [VN04].
Spec [Bar00c]. Special [Ano04a, Ano07b, Ano07a, BK06b, GIS05, GS07a, GPP08, SGK08, KP03, FOP06].
Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08]. specialized [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00a, LJKL01, RSA00c, Mee04].
Specifications [IEE00b, BDFP05, BD04a].
Specified [Tad02, He02, LWK05b, YY05a, ZX04].
Specifying [BJvdB02, Cir01]. Speck [KGS07]. Spectr [GMM01]. Spectr-H64 [GMM01]. spectra [MS02b]. Spectral [QP05, SK07]. Spectrum [BRQ01, LY07, PM00]. Speech [MRL+02, AA04a, PY08].
Speech-Generated [MRL+02].
SpeechStudio [Ano02c]. Speed [Ano00b, Ano02b, Gro01, JKRW01, KMM+06, Lut02, SOTD00, SM02, Wie00, YKMY01, BGL+03, RW07, RMCG01].
Speeding [Osv00, SWH+09, TC05]. Speedup [YKLM02b, YKLM03]. spherical [LZP+04]. Spider [Jur04]. Spies [Gan01b, Win05c, Han06, NRR00].
SPIHT [Che08a]. SPIN [MS02a]. Spline [SPK08].
Splitting [GMW05, LLK05]. SPN [HLL+01, Kan01, PQ03]. SPNs [CKL+03].
spot [Na05]. Spread [BQR01]. Spring [Pap05]. Spring-Verlag [Pap05]. Springer [Fal07, Lee03a, Lee03b, Pho01]. Springs [Wil99]. spying [FNRC05]. spyware [Ste05c]. SQL [Dev08, HLM02].
Squadron [OC03]. Square [HCK09, HQ01]. Squaring [CH07b, NSS02]. SRAM [HBF09].
SSC2 [HQR01, ZCC01]. SSH [All03, BS01a, BS05, BKN04, Dwi04, H601, Hos06b, Kra02b, Naz02, Oue05, SWT07, Str02].
SSH-Connected [H601]. SSHFS [Hos06b].
SSL [ASK05, BPS02, CHV03, JRB+06, KCD07, KPR03, Kra01, LLK05, LWK00, Net04, OBB08, SB01, SQ01, Vau02, ZFK04].
SSL/TLS [BPS02, CHV03, KPR03, OHB08]. SST [Gau02]. St [GKS05, NH03, AS01a]. stage [CHY05b]. stamp [CL00]. stamping [HHC05]. Stamps [KZ01]. Stand [CAC03].
Standard [Ano08, Ano09, Ano12, Ano13, Bar00a, BCP02a, FIP00, FIP01a, FS01a, Hug04, HLC08, IEE00b, MM01c, MP01a, Nat00, PM00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, BBK+03b, DRS05, GMR08, Sea09, Tan01, Bar00c, HI00, Bur03, CRM06, Coco02a, Coco02b, Cur05, DR01, DR02b, Dan01, FIP02b, GC01a, Har00, Lan00a, Lan0ob, Lan04a, Mor05, NIS00, SB00, Sta00, WBRF00, YY06].
Standardized [Man01]. Standards [Ano01f, Bur06, CL07, Coco02b, Hsu01, RSA00a, Tsa06]. Standing [Lan00b]. State [And07, CR03, GST04, HBF09, MSNH07, Ris06, TL07, Kar01, Mit00].
State-transition [TL07]. statecraft [dL00]. Stateless [ANR01, NNL01, SK05b].
Stateless-Recipient [ANR01]. States [LB04, Jol01]. static [CW07]. Statistical [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, LZ01, LLL+01, MV03a, Neu04, Pro01, RSN+01, BKW03, Hey03].

Statistically [Fis01b, HR07, HNO+09]. Statistically-hiding [HR07]. Statistically-Secret [Fis01b]. Statistics [CKN01, CNK04, KLML05]. Status [Pre01, Sha03b]. statute [Cal00a]. STDM [WMDR08]. Stealing [Gan01b]. Stefan [AUW01]. Steganalysis [Pro01, Sal05b, WW04]. Steganografie [Sch09]. Steganographic [HR02, MJF07, RH02, RS00, Wes01, KC09, LYC02, WWTH08, YCL07].

Steganography [BC05a, BGI08, CYH01, ChLYL09, CDR01, CW09, Col03, CMB+08, CS05b, DIRR05, FGD01, HLV-A02, HvAL09, Hun05, HSKC01, PH03, Sal05b, Sch09, Sha01c, Shi08, SWR05, Wan05, WW06, CDS07, Che07, Che08a, JD01, KP00, LT04, WW04, WMS08, Way02b, Way09, YCYW07]. stego [KC09]. stego-image [KC09]. Steiner [WL02]. Step [KKKL09, MP07, SL06]. step-by-step [SL06]. Step-out [KKKL09]. Stepping [Bii02]. steps [Bii02]. Stereotypes [GO03]. Stern [CS05a]. sticker [GPX08]. Sticks [Sam01]. Stinson [Spr03]. STL [Zol01]. STOC [ACM05a, ACM07, ACM08, ACM09].

Stochastic [MG01]. Stock [Bar00a]. Stone [MLM03]. Stones [WRW02]. stop [SSNGS00, Win05c]. Storage [DFSS08, Din01, Din05, HR02, Har07b, Hug04, MSTS04, RCBL00, Ric07, RH02, VAD03, AFGH06, DFSS05, HGR07, LPM05, SGMV09]. Store [CTBA+01]. Storing [ST06]. Story [Ben01b, Bud00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, Win00]. strategic [AJ08]. Strategies [Cir01, KL05, SKQ01, Dwi04]. Strategy [DR02a, TPPM07, KC09]. Stream [BCC01, BS09, BS00b, BL02, CF01b, Can06b, CJS01, CHJ20, CM03, Cou03, CL02c, DF07, Fil00, FF01a, Gol01d, GBM02, HJCJ02, HR00, HR04a, Jam00, KHD01, MSNH07, PP06a, SM01, Sar02, SXY01, WB02, Wu02, ZC00, ZC01, BGP09, Ber07, BD00a, BG08, DK08, KH08, Max06, MI09, PC03, PC03, SB05, WW08].

Stream-Cipher [SXY01, WW08]. Streaming [OS05]. Streams [AIP01, YLC+09]. Strength [CB01, JX05, Oni01, CKL+09]. Strengthening [Loi00, MHM+02]. String [CP07, DFS04, Pas03, Dam00, RG05]. Strings [Vau05b]. Strong [ADD09, BB00b, CS00, DKFX05, KCJ+01, KW00, LSH03a, LSH03b, Lu02, Pan09, SBZ02, CC04b, HRS08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04]. Strong-Password [LSH03a, LSH03b, CC04b, KTC03, Ku04]. Strongly [IY06]. Structural [BS01c, LBR00]. Structure [DNP07, EIG01, HH01, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SLL+00, XMST07]. Structured [BRTM09, CKK03]. Structures [An02c, GTTC03, HCO02, KCP01, Kius02, MND+04, MFF05, PSC+02, PQ03, Sun00a, XH03, Hen06, IY06, SWR05].

Stuart [Gum04]. students [AA04b, PP09]. Studies [Pag03, SPH06]. Study [BBGM08, Car02, DPR01, DP00, KKJ+07, WCZ05, BKN04, BF06a, DY09a, KWDB06, SKW+07, ZWWL01]. Sturgeon [Wei05, Wei00]. Stuttgart [Eag05]. style [dH08]. Subdivision [LDD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro05, GMR05]. subliminal [LH04]. subsampling [LLC06b]. subscribe [SL05b]. subsets [Sch01e]. substitute [Bii02]. Substitution [KKG03, GPX08, RBF08, WL04b].
Substitution-Permutation [KKG03].
Subsystem [HL07, MBS04]. Subtleties [Lai08]. Subverting [HB06]. Successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Sufficient [IKO05, Kos01b, KO00, MN01]. Suffix [ABM08]. SUID [Tot00]. SUID/S gid [Tot00]. Suitable [AIK+01, CQS01, KTT07, LKHL09, SP05, Wbn03]. Suite [RSN+01, SBEW01, YLT06]. Suited [WWGP00]. Sum [Che04b, KLY02]. Sum-of-Digits [Che04b]. Sums [CY08, Shp05]. Sunspots [CPS07]. Super [Lam07, CAC06, Hos06b]. Supercluster [Pri00]. Supercomputer [Coc01a]. Supersingular [Gal01, CQS01, KTT07, LKHL09, SP05, Wbn03]. Supersymmetric [Che04b]. Symmetry [RBF08]. Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, Ano00b, BS02, BCDH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, JFl08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05]. Synchronisation [CmdV06]. Synchronization [GPcS08]. synchronize [Pau02b]. Synchronos [CH01b, Sar02]. Synopsis [YL+09]. Syntax [FWB02, RSA00b, RSA00c]. Systems [ME08b]. System [Ano02b, Ano02c, ANR01, BIP05, BCST00, Bh01, CCDP01, CHM+02, CJS+02, DJ01, DGP07a, DGP07b, DV08, EM03, FL01a, Ito01, Joh05, KC02, KH04, LV00, LSS05, LSS05, LXM+05, MA00a, MA00b, Miy01, MKF+06, MFS+09, RH02, SO01b, S002b, Ste05b, TK03, TZZ09b, USE00a, WG05, WA07, YKM01, YKL02b, ZYM05, AHH03a, AMRP00, ADH+07, AAKP09, Biu09, BDET00, Bu09, CC02b, CCH05, CJL06, CPG+04, C001a, Co09, DZL01, DPT+02, DIM08, DGP09, FP00, GG08, GMG00, Gou09, HLL+02, Jov03a, KWDB06, KX00, K003a, L04b, LKJL01, Lin00a, LK01, M001, MKK00, RCG+05, Sa00b, SCS05a, SGMV09, SETB08, TKP+08, WA04a]. Systematic [DW05, ZL04a]. Systemic [KB06]. Systems [ACM03c, ACM05b, ANR01, Ano02c, BCST00, BRTM09, CP02, ELv01, Fe06, GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST+05, LLLL09, L05b, Lu03, Mar02b, MMYH02, NABB03, R05, R102, SM01, S007, ST09, SY01, USE00c, USE00b, Vav03, VHP01, WK03, ARJ08, And08, Ano01b, Bid03, Ble07, CUS08, CC05c, CCGS08, CGL+08a, CGL+08b, CGL+08c, CCM01, CNPQ03, CHT02, CG05, CHK+08, DY09a, EY09.
Table [Ano03c, MFFTO5, XFZ01, BZ03, CC05b, Has00].

Tables [AJO08, KB39, RBF08].

Tag [KKJ07].

Tags [OS06, ACdM05].

Taipei [Lai03].

Taiwan [Lai03, Ano03a].

Takagi-cryptosystem [LKYL00].

Takagi-cryptosystem [LKYL00].

Takaragi [WHLH03].

Takagis cryptosystem [LKYL00].

Taking [CDS07, Lai07, PM00].

Talbot [Rot07].

Talk [FGM00a, Lan00d].

Taming [Aba00, Lov01].

Tamper [LTM+00].

tampering [PS08b].

Tandem [DPT+02].

tank [Pau03].

Tar [Str02].

Targama [MAaT05].

Target [BD04a].

Targets [MV01, Pau03].

Tarragona [DFPS06].

Tasks [XQ07].

Tate [Jou02, SKG09].

Tatsu [TSO00].

Tattling [BP05].

Technique [CC02a, Pau09, PQ03, SC02a, vW01, CL00, Che08b, Pau03].

Techniques [AIP01, BSW09, Bih03, BBP00, BPD02, CC04a, Cra05a, DBS+06, Dun06, Ken02b, Knu02, KO03, MKP09, NCRX04, PJK01, Pf01, Pre00, Sh08, YK01, AB09, BWMO5, Che08a, DY01, DHMR07, DY09a, Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08].

Technologie [RSA09b].

Technologies [MS05a, PP06b, Sam09, SE09, V909, Way01, Way02a, ZWC02, ATS04, PB01, TTZ01].

Technology [CZK05, Cla00a, GSB+04, MP00, NFQ03, Pag03, TV03, AL07, Ble07, Car01, Cas02, Che00, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b].

Tektronix [Ano02c, TC-11].

Telegram [LM00].

Telenet [El06].

Telenet [El06].

Telephone [KVZ01].

Telephony [Ano02c, PM00, CGV09].

Teleportation [BEZ00, BEZ01, Duw03].

Telling [Gan01b].

Template [LTM06a, UEP09].

Temporal [CDTT05, KXTZ09].

Ten [ES00a].

Tenth [LTM06a].

Terminal [ECM00a, ECM00b].

terminals [ISTE08].

termination [BP05].

Terror [AD09, DKL00b].

Terrorism [PP06b].

terrorists [Win05c].

TESLA [LN04].

Test [BT02, HSS04, Lan00b, LN08, RSN+01, Way02a, GMG00, Kat05a, KKKP05, RSS04].

testable [RMP08].

Testing [IH00, CGBS01, Fil02, Lat02, Lat03, SB00, WA06, Lat03].

Tests [MT02, NM09, GT02].

Text [LS02, PJH01, PM08].

textbook [BJN00, PP09].

Thank [CMB+05].

Theft [CMS09].

Their [AGT01, CD00, Gen04a, JKRW01, LLL+01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SST06, TO01, VW00].

Them [WD01].

Theorem [AC02, Eke02, GN01, Sh00a, Sch01b, YKL00].

theorems [Ny01].

Theoretical [CB01, DHR00, Kat05b, Nie02b, VVS01, VDKP05, vW01, Mar05b, Shp99, Wag03].

Theoretically [SGB01, PRS04].

Theoretically [AP09, DM00b].

Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bih03, Boy01, CC04a, Cra05a, Des02, Fu07, HR06, Hay06, IZ00, Irw03, Kim01, Knu02, La03, Lee04b, Lat03, MNT+00, Mao04].
transforms [Laf00]. Transient [Ric07, VS08]. Transistor [Coc02a]. Transistors [Bar00b]. Transit [Con00, Cal00c]. transition [TL07]. Transitive [BN02]. Translation [PY06]. TransLink [Cal00c]. Transmission [MLC01, SNR04, SVDF07]. Transparent [CCDP01, Por01, Lin00a]. transport [Bor00]. Trapdoor [BPR08, Fis01b, KO03, KO00, Gen04a, JSW05, PW08]. Trapdoors [GPV08], Travel [Bur00]. Traversal [JLMS03]. Trawling [Knu00a, Knu00b]. treatise [Bla00, MAA03, MAA04, MAA07]. treatises [MAA06, MAA07]. Treatment [CL05, DK08]. Tree [CC05d, GST04, KPT04, LKLK05, LM02, TMW04]. trees [Che02, Che07, TC00]. Trends [Ahn08, KB07, Ort00, Ndm06, PRS04]. tricks [All03]. triggered [HHJS04]. tripartite [SW05]. Triple [HS05, BR04, CGBS01, Cot00a, FZH05, Ke105, LMP01]. Triple-DES [Cor00a, LMP01]. Triples [FR01b]. Tripwire [TvdKB01]. trivial [KO00]. troubleshooting [HHJS05]. True [BST03, Chao4, DV08, EHK03, HBF09, Pan07, SFDF06, BG08, BG09, GB09, Han06, HLwWZ09, Ste05c, vT01, VKS09]. Truecrypt [CHK08]. truly [BGL03]. Truncated [CS05a, KM02, LHL03]. Truncation [CS05a, KM02, LHL03]. Trust [CHSS02, HCD02, Lin00b, LHL03, Mita02, SMP09, Dav01c, HHJS04, JY05, LCK04, LLW05, LMW05, LLW09]. Trusted [DK01, WHI01, WV01, ARJ08, PS04c, ZYLG05]. Trusting [CKS09]. trustworthy [CCH05]. Truth [MNT00]. Tseng [Hwa05, XY04, ZAX05]. TTM [GC00b]. Tuesday [Unio0a, Unio0b, Unio0c]. tunable [LB05]. Tunny [Sal01a]. Tunin [AL06]. Turing [Bar00b, RSA03a, Ad03, Coc03, Cop04b, Goo00, Pet08, Riv03, Sha03].
unusual [GG05a]. Unveiled [Bar00a]. Update [TEM+01]. Updated [Cho08a].
upgrade [Pau02a, Pau02b]. Upgrades [Ano02c]. upon [DFG01]. UPPAAL [BBD+02].
[BMK00, CGK+02, LSVS09, LLK05, ZBP05].
[USA] ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KPP02, KJR05, Kil05, KP01, Men05, Men07, Nac01, Nao04, Oka04, Pre02b, Poi06, Pre02b, Sch01d, Sho05a, Sil01, YDKM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FMA02, IEE01a, IEE05a, IEE05b, IEE08, IEE09b, Ki01a, MS05b, NIS00, Sch00a, Sch01c, S03, Sch04a, Sch04b, Sch05a, SMP+09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, WI99, Yun02a. usability [CG05]. Usage [LY05, PS04b]. Use [Bai01a, BWBL02, Bol02, BQR01, CPS07, Dre00, ISO05, Kra03, LCK04, Pau09, PBTW07, Str01a, WS05, Win01, CG05, OS07]. used [MSV04]. useful [SM03a]. UseNet [Coc01a]. USENIX [Coc01a]. User [BG002, CL01b, CMR+05, D000, Had00, HY01, KZ09, LS05, JR03, OHO08, PS01b, Sas07, SSM+08, Str01a, Tsa01, BBM00, CL04d, DLY08, GMSL02, Hsu05b, HL05b, KC05, LAP08, LHY02, LL02, LKY04, LKY05a, LHL03b, LC05a, LC01, Par04, SS03, SZS05, TWL05, WLT05a, YS04, YRY04, ZYLG05, v0T08]. User-Centered [CMR+05]. user-controlled [LAPS08].
user-drawn [vOT08]. user-friendly [SZS05, WLT05a]. user-level [SS03]. Users [LLS05b]. Uses [Bau01c, RSQ03]. ushers [Bur00]. Using [A01a, A01c, AADK05, AIP01, Ano01a, Ano01c, Ano01h, ADDS06, BJ02, BH06, BK06a, Bau01a, Bau01b, BP06, BPS02, BR09, BT02, BM00, BMP00, BL02, Che01a, CLLL00, CGBS01, CCW02, CCM01, CHO07c, Cir01, DI05, DPR01, DP00, DWN01, DGH+04, EFY+05, FJ03, FMP03, Fri01, GC01a, GL01, GSB+04, HHGP+03, HQ05, HJW01, Jab01, JKK+01, JSJK01, KOY01, Kel05, KM01a, KLC+00, KTT07, Kra02b, KZ09, Lan04a, Len01, LB04, LS05a, LM02, LH07, MS02a, MS09a, MLM03, MS03b, MMJ05, NZCG05, NM09, OT03a, PHK+01, PJH01, PKJ01, PC02, PK01, Sho00b, SK05a, Sma03a, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VP01, WY02, Wit01, XFZ01, YKMY01, YLL02, YSS+01, ZWWL01, Zhe01, ASW00, AL07, BCL05a, BCW05, BK07, CDS07, CWH00, CL04d, CCK04b, CCH05]. using [CH05b, CKY05, CJ05, Che07, Che08a, Che08b, CJ04, CKK03, Cos00, DZL01, Du02, DFG00, FWT05, GC00a, GMR05, Gen09b, GS09, HHS01, HW05, HA04, HT07, Hir09, HW04, HY03, HL04, JRR09, KOY09, KOY09, KLY03, KB09, KKL09, KKJ+07, KSW06, KR03, Ku04, KC05, LH02, LLH02, LKY04, LCP04, LL04b, LW04, LKY05a, LLW05, LLW09, LW04, LC05a, LL06, LWK07, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, FCC03, PS05b, Sco04, Sha04b, Sha05b, SHHO7, Tan07a, TL05, Tsa05, TJC03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YY04, YC09, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. utility [Gua05]. Utilizing [Str02].

V [K05b, Puz04, S03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00c]. v2.1 [RSA02]. v2.11 [RSA01]. V5 [It00]. V5.1a [CHK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BLM01, KJC+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [PM00]. Value [BR09, GIS05, BM02a, DK08, WW08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadhrajan [MS03a]. variable [SV08a].
Variables [HR04a]. Variant [Luc02b, NSNK05, Ber08, Duj08, Duj09]. Variants [BDK+09, DG02, KS00b, CJ05, Sha04b, TJ03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDhKB09]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, Pei09, mSgFtL05, WNQ08]. vectors [LHL04]. Vegas [ELvS01, IEE01a]. Vein [BDhKB09]. Vendors [Pau03, MV03b]. Venona [Ben01b]. Verenigde [dL00]. Veridicom [Ano02b]. Verifiable [ANR01, Ate04, CD00, CS03a, CHS05, Cha04, JLL02, JG01, Lys02, NZCG05, NSNK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a]. Verifiability [BGLS03, Hes04a]. verifiably-encrypted [Hes04a]. Verification [AADK05, Ara02, BPST02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJL06, HL05c, JW01, Ldr02, MD04, MT07, MS09, PBD07, TYH04, Wan04b, Wu01, YLC+09, ZLX99, ZL04b, CS08b, Uzu04]. Verified [BJP02, BFGT08, BFCZ08, CJT04]. verifier [Bla01b, LKY05b]. verifier-based [LKY05b]. Verifiers [CL01a, He02, LV07, LWK05b, YY05a, ZX04]. Verify [MS02a]. Verifying [BFG08, BvdB02, CJM00, HL07, IR01, PTO8, RR02, BL06, BL06P, HLH00, SV08a, Sha01d]. Verlag [Eag05, Lee03a, Lee03b, Pap05]. Version [Bol02, HPC02, OST05, SKI01, Mis06]. Versions [Hsr01, NPV01, CV05]. Versteckte [Sch09]. Versus [Rub00, WWL+02, ASW+01, BJLS02, DBS01, WPP05]. Vertically [DN04]. Very [AAC+01, B+02, CG03, EBC+00, FLA+03, H601, PM02, PBMB01, Zir07]. Vestiges [Top02]. VI [Sch04a]. via [AGKS07, ACmM05, BDPV09, Car02, Che03, CPG+04, FWBC02, Fox00, HHYW07, HLM03, JJO0a, KT06, ML05, PG05, RG05, SB01, SLG+05, ZLG01, Lud05]. Victoria [ACM08, IZ00]. Victorian [Top02]. victory [Hau03]. Vid [CAC06]. Video [BDF+01a, BD03, CDTT05, EFY+05, ISSZ08, KBD03, KJR05, KLL01, LHS05, ML01, SC02a, BS01b, JA02, KN03, UP05]. Video-Based [KJR05, BS01b, KN03]. videos [YZDW07]. Vienna [BZ02]. Vietnam [Lov01]. View [Bar00a, Mah04, Sin09]. Views [Bar00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03]. Vigenère [DG00]. VII [Sch04a]. VIII [IEEE01b, Sch05a]. Virginia [MS05b]. Virtual [Ano01c, HM01a, Pro00, YSS+01, BDS+09a, ML05, ZBP05]. virtualization [CGL+08a, CGL+08b, CGL+08c]. virtualization-based [CGL+08a, CGL+08b, CGL+08c]. Virtues [Tro08]. Virus [Gor06, Ano05b]. Visible [HT06]. Vista [Fer06]. Visual [BDN00, BDDS03, BCD06, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, ZP05, ABDS01, CDFM05, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Zol01]. Visualization [XYL09, MFS+09]. Viterbi [LBGZ01, LBGZ02]. Vladimirov [Puz04]. VLLDB [EBC+00, FLA+03]. VLDV [B+02]. VLSI [KV01]. VMSS [SC05a]. Voice [PK01, VN04]. VoIP [SZ08, VAVY09, WC05]. vol [Kat05b, Lee03b]. volatile [SETB08]. Volume [Go04]. Vortrag [Eke02]. Voter [Cha04]. Voter-Verifiable [Cha04]. Voting [Cha04, FPS01, HS00, Joh05, JLL02, KMO01, Rub01, CJT03, HJW05]. Voyncich [Rug04]. VPN [KMM+06]. VPNSs [Dave01a]. VQ [WJP07]. VQ-based [WJP07]. Vs [CTBA+01, Di 01, Di 03, SU07, WW04]. VSS [AF04b, CDF01, FM02a]. Vu [DP00]. vulnerabilities [CSW05, DMS07, Swi05, XNK+05]. vulnerability [KHL09, SGA07, YRS+09]. WA [ACM06]. Wagner [VP06]. Wagstaff
[Jan08]. Who [CZB+01, Urb01, Hau06]. whole [CPG+04]. Wi [Puz04, Sty04, VGM04, FMA02, Bar03]. Wi-Fi [Sty04, Bar03]. Wi- Fi [Puz04, VGM04]. wicked [Lud05]. Wide [DR02a, SBB05]. Width [OT03b]. Wiener [Duj08, Duj09]. WIESS [USE00b]. Wiley [And04, Gra01]. Will [Ort00, Cla00b]. William [Pag03]. Williams [Mul01a]. Window [OT03a, SSST06]. Windows [USE00a, DGP07a, DGP07b, DGP09, Fer06, HB06, WD01, Wit01]. Wins [Bar00b]. Wired [Gil07, SIR04]. Wireless [AEAQ05, Bar03, BCI+00, ECM00b, Fin06, KH05, KHD01, LNL+08, Puz03, PJDH09, Puz04, Sn01a, Sty04, SYL05, VGM04, YSR01, ZYN08, ZWCV02, BPO3a, BBG+02, CCMT09, Cha05b, GW08, GGO5b, JRR09, KXTZ09, KB09, LDH06, LPV+09, LW05a, Lin07, MJF+08, NC09, NLD08, PCSM07, Par04, Pat02a, Pat02b, SLP07, SZ08, TP07, Vac06, Wan04a, YTW05, CS08b, ECM00a, PDM09]. Wiretapping [Cho08a, DL98, Jan08, DL07]. WISA [CS09]. Within [MR02a, CHM+02, MR02b]. Without [BCL+05b, Bha01c, BB04, BGO7, Har06, NA07, CH01a, CCK04b, CYH04, CCH05, CJ04, CDD07, CN06, D01K, KG09, Ku04, LVO7, LW04, LKYO5b, LL06, LCZ05b, Lys07, MP02, Mar07, P04c, RG09, WH01, YW05, YRY05b, ZW05a]. Withstanding [DF04]. Wits [Bud00a, Bud02]. WLAN [SSM+08]. WLAN/ cellular [SSM+08]. Woes [BTTF02]. Women [FF01b]. won [Hau03]. Worcester [KP01]. Word [HR00, SKU+00]. Word-Oriented [HR00, SKU+00]. Wordlengths [PG05]. words [GS01, Max06, NS01a, VS01]. Work [DFG01, DNW05, Fox00]. Working [DFCW00, ELvS01, KB00]. workload [BGM04]. Works [Net04]. Workshop [ACM05a, An05b, AL06, BDZ04, BBD09, BD08, CZ05, Chr00, Chr01, CCMR02, CCMR05, CSY09, DR02c, Des02, GH05, IEE01b, IZ00, Joh03, JQ04, KKP02, KCR04, KGL04, Kim01, KP01, KNP01, LST+05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RRS06, RM04, Sch00b, Sch01d, TB02, USE00b, YY01, Vau05a, WKP03, Yrr06, AMW07, AJ01a, BCKK05, Bir07, CKL05, GKS05, HH04, HH05, HA00, ST01d]. World [Ber03, HW01, Nik02a, Nik02b, Sch00d, Sty04, YKMB08, Aro05, Bel07, GG05a, HH06, Hus01, KPS02, Kee05, Lie05, Lun09, Rob02, Sch03, SL07, Bec02, Bud00a, Bud02, Hau03, M09, OC03, Sty04, Sec04]. Worlds [Wil01b]. Worm [LJL05, CSW05]. Worms [ZGTG05]. Worst [CCM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case [HRS08, Mic02a, Mic02b, Pei09]. worst-case/ average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. Wrapper [Os00]. Write [BB02]. Writers [Gor06]. Writing [HL03, Jan06, Kah67a, Kah67b, Kah96, Gas01]. Writings [Cop04b]. WS [JRB+06, RR04]. WS-Policy [RR04]. WS-Security [JRB+06, RR04]. WSDL [Bar00c]. WTLS [Vau02]. WTMAU [ECM00a, ECM00b]. WTMAU-SD [ECM00a]. Wu [BCW05, CHY05a, CWJT01, HL05c, MS03a, YY05b]. Wu-Lin [YY05b]. Wuhan [TTZ01]. WW [Sal00a].

X [For04]. X. 509 [SJ05]. X.9.31 [Kel05]. X9.62 [ANS05]. Xbox [Ste05b]. XCB [GD02]. XECB [GD02]. Xia [CJT04, Sha05a]. Xiamen [DWM05]. Xiao [JW01, YY05a]. Xilinx [Ana02c]. XIV [USE00c]. xix [Top02]. XL [CP03]. XML [Hei01, TEM+01, AW05, AW08, Ana02c, BNP08, CKK03, Dav01b, Dav01c, FJ04, FL01b, GA03, Her02, LC04b, PCK02, RR04, UG08, Uri01, UST01a]. XMT [SG07]. XrML [Bar00a]. XTEA [CV05, HHK+04, MHL+02]. XTR
REFERENCES

[LW02, LV00, LNS02, Ver01].

Yang [KJY05, WL05, YWC05].
Yang-Shieh [YWC05].
Yao [BDNN02, ZD05].
Yarrow [KSF00, Mur02].
Yarrow-160 [KSF00].
Yaschenko [Kat05b].
YCH [SC05a].
Year [Naz02, Bur00].
Yellow [JYZ04].
Yen [LLLZ06a, LLLZ06b].
Yen-Guo [LLLZ06a].
Yesterday [Coc02a].
Yi [Wag00].
You're [ES00a, Nic01].
You've [Nic01].
Yuck [Sas07].
Yuen [KH08].

Z [Wue09]. Z-parameter [Wue09]. z10 [Web08]. Zeta [Ver02].
Zeilinger [Dzw03]. Zero [AS01b, APV05, BP04, Con01, DPV04, DFS04, DDO +01, HNO +09, IKOS07, LMS05, LHL +08, MR01b, MV03a, Pas05, Ros00, Ros06a, CSW05, Dan00, PBD07, KK07].
Zero-Knowledge [AS01b, BP04, Con01, DFS04, HNO +09, LHL +08, MR01b, MV03a, Pas05, Ros00, IKOS07, Dam00, PBD07].
Zeta [Ver02].
Zhang [JW01, YY05a].
Zimmermann [McL06, Tuc66].
ZK [PBD05].

References

Al-Akaidi:2004:FSP


Aly:2004:CSP


Apers:2001:PTS

REFERENCES

Al-Azzoni:2005:MVC


Anshel:2001:NKA


Ababneh:2009:CSE


Ashraf:2009:SBE


Aamodt:2003:CSP


An:2001:DER

Atallah:2009:ATC

REFERENCES


Abadi:2000:TA


[ABB+04] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In Shoup [Sho05a], pages 205–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; In-
REFERENCES


Austin:2000:ASF


Adjeroh:2008:BWT


Abdalla:2001:ODH


Adjeroh:2008:BWT


Ambainis:2009:NEQ


REFERENCES


Alvarez:2005:EBS


Ahmad:2007:ADE


Anyanwu:2009:DCS


Avanzi:2006:ESM


Arnold:2007:CSE

T. W. Arnold, A. Dames, M. D. Hocker, M. D.
REFERENCES


Adikari:2009:HBT


Adleman:2003:TLP


An:2002:SJS


Arazi:2005:RPK


Alvarez:2005:SSS


Atighehchi:2009:EPA

Anton:2007:HEW


Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR

REFERENCES

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

Attrapadung:2006:FSS


Akkar:2001:IAS


Acquisti:2009:PSS


Akavia:2006:BOW


Akavia:2010:EBO


Alon:2007:GSE

Noga Alon, Venkatesan Guruswami, Tali Kaufman, and Madhu Sudan. Guessing secrets efficiently via list
REFERENCES


Anagnostopoulos:2001:PAD


Ateniese:2005:PRS


Agrawal:2003:WRD


Armington:2002:BAI


Ahmad:2007:CSS

Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB


Applebaum:2004:CNS


Applebaum:2006:C

Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC⁰. *SIAM Journal on Com-
REFERENCES


Al-Ibrahim:2001:AMS


Attali:2001:JSC


Attali:2001:SCP


Aid:2008:NSA

REFERENCES


**Amir:2004:PGK**


**Agrawal:2002:PP**


**Aciicmez:2006:PSB**


**Agrawal:2004:OPE**


**Amadio:2000:RPC**


**Aoki:2000:FIA**

Atallah:2004:ALA


Atzeni:2006:PKI


Anshel:2007:RME


Allen:2003:EST


Allman:2006:MAW


Amadio:2002:SRP

REFERENCES

Alvarez:2000:CCE

Alvarez:2004:KCC

Adams:2007:SAC

Andem:2003:CTE

Anderson:2004:BRR

Anderson:2007:SSS

Anderson:2008:SEG
[Ross Anderson. Security engineering: a guide to building dependable distributed...]

Andem:2003:CTE

Aura:2001:RAC


Anonymous:2000:CCI


Anonymous:2000:CLI


Anonymous:2000:AAPb


Anonymous:2000:ANT

Anonymous: 2001: AWB


Anonymous: 2001: AIgb


Anonymous: 2001: EDS


Anonymous: 2001: LBS

Anonymous:2001:PKC


Anonymous:2001:SCS


Anonymous:2002:DEC


Anonymous:2002:PPD


Anonymous:2002:PSS

Anonymous. Products: SOISIC ships design kit for SOI structures; systems and software development tools from Telelogic; RSA Security’s Web access management system; Altera’s free embedded processor portfolio; signal integrity measurement tools from tektronix; Oracle upgrades Java development tool; Xilinx delivers EDK...
Anonymous:2002:QCQ


Anonymous:2002:RUB


Anonymous:2003:TMC


Anonymous:2003:NUP


Anonymous:2003:TMP

Mersenne primes are primes of the form $M(n) = 2^p - 1$. The known members of this set in order of increasing $p$ (not of discovery), year of discovery, and discoverer, are:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>Year</th>
<th>Discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1913</td>
<td>E. Fauquembergue</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1876</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson &amp; D. Slowinski</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>1988</td>
<td>W. N. Colquitt &amp; L. Welsh</td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>756839</td>
<td>1992</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud et al. (GIMPS)</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, Woltman, Kruppa et al. (GIMPS)</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala et al. (GIMPS)</td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>2001</td>
<td>M. Cameron (GIMPS)</td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>M. Shafer (GIMPS)</td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2004</td>
<td>Josh Findley (GIMPS)</td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2005</td>
<td>Martin Nowak (GIMPS)</td>
</tr>
<tr>
<td>43</td>
<td>30402457</td>
<td>2005</td>
<td>Curtis Cooper &amp; Steven G. Lucas (GIMPS)</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven G. Lucas (GIMPS)</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich (GIMPS)</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo (GIMPS)</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, George Woltman, et al. (GIMPS)</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, George Woltman et al. (GIMPS)</td>
</tr>
</tbody>
</table>
Anonymous:2004:CPS

Anonymous:2004:NGJ

Anonymous:2004:CEC

Anonymous:2005:RC

Anonymous:2005:SSD

Anonymous:2007:CPSf

Anonymous:2006:SSD

**Anonymous:2008:SHS**


**Anonymous:2013:DSS**


**Ateniese:2001:SRC**

0558/papers/2271/22710182.pdf.

**Amir:2001:FAA**


**ANSI:2005:AXP**


**Abe:2000:PSP**


**Alomair:2009:ITS**

REFERENCES

15/information_theoretically_secure_encryption.

Appenzeller:2005:IBE


Applebaum:2007:CCP


Alwen:2005:IFR


Abdalla:2000:NFS


Arboit:2001:FLM


Araki:2002:NRS

Shunsuke Araki. A Nyberg–Rueppel signature for multi-

Atallah:2001:NLW


Aaraj:2008:ADH


Agrawal:2003:MCA


Arkin:2005:CND


Arnold:2001:AWB

Abe:2001:SPA


Agung:2001:ICI


Agarwal:2008:DWS


Ashburn:2003:PBA

REFERENCES


Acicmez:2005:IBB


Acicmez:2007:MAC


Abdalla:2000:KMR


Androussellis-Theotokis:2004:SPP


Aharonov:2000:QBE

Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In
REFERENCES


Martín Abadi and Bogdan Warinschi. Security

Abadi:2008:SAC


Bernstein:2002:VPT


Blanton:2006:SRF


Bagnulo:2002:PAA


Baier:2001:ECP


Baier:2001:ECS

Harald Baier. Efficient computation of singular moduli with application in cryptography. *Lecture Notes in Computer Science*, 2138:
REFERENCES


[Bar00b] Nicholas Baran. News and views: More on tiny tran-
sistors; Open Source repository launched; design contest promotes new software tools; and then there’s a decryption contest; Fred Brooks wins ACM Turing Award. Dr. Dobb’s Journal of Software Tools, 25(3):18, March 2000. CODEN DDJOEB. ISSN 1044-789X. URL http://sourceforge.net/.

Nicholas Baran. News and views: RSA algorithm in the public domain; Woz joins the Inventors Hall of Fame; entangled photons mean faster, smaller ICs; BEHEMOTH mothballed; Advanced Encryption Standard selected; SGI releases SDK as open source; WSDL spec released. Dr. Dobb’s Journal of Software Tools, 25(12):18, December 2000. CODEN DDJOEB. ISSN 1044-789X.


Gregory V. Bard. Algebraic cryptanalysis. Springer-Ver-
References


REFERENCES

Bauer:2003:PPAb


Baudet:2005:DSP


Blakley:1979:RSA


Benedens:2000:TBD


Buchmann:2000:ECC


Barkan:2002:HMW

REFERENCES

Bouda:2003:EQI


Boneh:2004:SIB


Behrmann:2002:UIS


Bicakci:2005:ISA


Biham:2002:SQK


Bernstein:2009:PQC

Daniel J. (Daniel Julius) Bernstein, Johannes Buchmann, and Erik Dahmen, editors. *Post-quantum cryptography: [First Interna-
REFERENCES


Bertoni:2003:EAD


Bellare:2000:PKE


Bellare:2009:HPK


Bobineau:2000:PSD

Christophe Bobineau, Luc Bouganim, Philippe Pucheral, and Patrick Valduriez. PicoDMBS: Scaling down

**Boneh:2004:SGS**


**Burgess:2001:ISC**


**Biham:2004:NCS**


**Blundo:2004:SIA**


**Backes:2005:PKS**

REFERENCES


REFERENCES

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

Bruguera:2009:PIS


Burnett:2000:EMG


Barnum:2002:AQM


Brown:2000:PCW


Breunesse:2005:FMS

C.-B. Breunesse, N. Cataño,
REFERENCES


[BCP01] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval.
REFERENCES


[Bell02] Paolo Bellavista, Antonio Corradi, and Cesare Stefanelli. Java for on-line distributed monitoring of heterogeneous systems and services. *The Computer*
Betarte:2000:SSC


Bao:2005:RWH


Bihm:2000:CAG


Boneh:2000:CRP


Bourbakis:2003:SBC


Bozzano:2004:AVS

Marco Bozzano and Giorgio Delzanno. Automatic verifi-

Burmester:2004:HPK


Buchmann:2008:PQC


Biryukov:2003:CS


Blundo:2003:COT


Bolosky:2000:FSD

William J. Bolosky, John R. Douceur, David Ely, and Marvin Theimer. Feasibility of a serverless distributed file system deployed on an existing set of desktop PCs.
REFERENCES


REFERENCES

Bhattacharyya:2009:VPA

Biham:2002:EDL

Biham:2002:LCR

Biryukov:2009:KRA

Blundo:2000:VCG
REFERENCES


REFERENCES


REFERENCES


Dagmar Bruss, Gábor Erdélyi, Tim Meyer, Tobias Riege, and Jörg Rothe. *Quantum cryptography: a sur-
References

[Ben00]

[Ben01a]

[Ben01b]

[Ben02]

[Ber00]

[Ber03]
REFERENCES

Bernstein:2007:SFS


Bernstein:2008:CVS


Bergmann:2009:DKR


Bernstein:2008:CVS


Bouwmeester:2000:PQI


Bouwmeester:2001:PQI


Biham:2000:IDR

Eli Biham and Vladimir Furman. Impossible differential on 8-round MARS’ core.
In NIST [NIS00], pages 186–194. ISBN ???. LCCN ???.

Eli Biham and Vladimir Furman. Improved impossible differentials on Twofish. [BF00b]
Lecture Notes in Computer Science, 1977:80–??, 2000. CODEN LNCSD9. ISSN

Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In Kilian [Kil01a], pages 213–?? ISBN
UK £47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390213.htm;

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

Steve Babbage and Laurent Frisch. On MISTY1 higher order differential cryptanalysis. Lecture Notes in Computer Science, 2015:22–36,


[BFG08] Karthikeyan Bhargavan, Cédric Fournet, and Andrew D.
REFERENCES


REFERENCES


[BGLS03] Bertoni:2003:EAA


[BGM04] Bucci:2003:HSO


[BGN05] Boneh:2005:EDF

REFERENCES


[BGW05] Dan Boneh, Craig Gentry, and Brent Waters. Col-


J.-C. Bajard and L. Imbert. A full RNS implementation of RSA. IEEE Transactions on Computers,
REFERENCES


Biham:2002:HDE


Biham:2003:ACE


Beimel:2000:RSC


Bajard:2003:EMG


Bajard:2005:AOP

Jean-Claude Bajard, Laurent Imbert, and Thomas Plantard. Arithmetic operations in the polynomial modular number system. In IEEE [IEE05b], page ??
REFERENCES

ISBN ???? LCCN ???? URL
http://arith17.polito.
it/final/paper-168.pdf. [BIW08]

Biryukov:2007:FSE


[BJ02]

Bishop:2003:ICJ


[BJS02]

Bishop:2003:CSA


Barkol:2008:CPR


[BIW08]

Boyce:2002:IAM


[BJ02]

Blaser:2002:PCC


[BJJS02]

Boneh:2000:WTE

Dan Boneh, Antoine Joux,


Matthew Burnside and Angelos D. Keromytis. The case for crypto protocol awareness inside the OS kernel. *ACM SIGARCH Computer


REFERENCES

Bellare:2004:BPR


Bajard:2009:SRB


Blum:2003:NTL


Buonanno:2002:IUE


Broadfoot:2002:ASA


Bucci:2008:FDR

Blaze:2001:LYS

Blanchet:2002:SAS

Blaze:2002:CI

Black:2000:TDE
Michael Andrew Black. A treatise on data encryption and an example of the black algorithm. Thesis (M.A.), University of California, Santa Barbara, Santa Barbara, CA, USA, 2000.

Blanchet:2001:ACP

Blanchet:2001:ECP
REFERENCES


REFERENCES

ny.com/link/service/series/0558/papers/2200/22000183.pdf.


Batina:2001:AWD


Blomer:2001:LSE


Brincat:2001:KRA


Basu:2003:AC


Blomer:2003:NPK

REFERENCES


REFERENCES


Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based


REFERENCES


Bouganim:2003:CSD


Bodycombe:1999:CC


Ben-Or:2005:UCS


Bollinger:2002:UFO


Boneh:2001:SOR

REFERENCES


REFERENCES


Boaz:2007:DC


Bedi:2001:CNF

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Black:2000:CMA


Black:2001:CAF


Black:2002:BCM


Bellare:2004:CBG


Bellare:2006:MPP

Mihir Bellare and Thomas Ristenpart. Multi-property-preserving hash domain extension and the EMD transform. In ?????, editor, Advances in Cryptology — ASI-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[BSC01a]

[Bo:2001:EID]

[BSC01b]

[BSL02]

[Bounkong:2002:ICA]

[Bounkong:2002:ICA]

[BSN00]

[Brisbane:2000:RBW]
Bresson:2002:TRS


Blake:2004:AEC


Buchmann:2002:ICP


Barak:2003:TRN

Boaz Barak, Ronen Shaltiel, and Eran Tromer. True random number generators secure in a changing environment. In Walter et al. [WKP03], pages 166–180. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-

[Biehl:2002:NDP]

Biehl:2002:NDP


[Biryukov:2001:RTC]

Biryukov:2001:RTC


[Bethencourt:2009:NTP]

Bethencourt:2009:NTP


[Boyer:2002:LDS]

Boyer:2002:LDS

[BTW05] Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In Kilian [Kil05], pages 600–??. CODEN LNCSD9. ISBN 3-540-24573-1 (soft-cover). ISSN 0302-9743 (print), 1611-3349 (elec-
REFERENCES

Beimel:2008:CIW

Black:2002:SCA

Buchmann:2000:CTC

Buchmann:2001:IC

Buchmann:2004:IC
REFERENCES


Budiansky:2000:BWC


[Bud00a]

Budiansky:2000:DBU


[Bud00b]

Budiansky:2002:BWC


[Bud02]

Buhan:2006:FBL

Ileana Buhan. Feeling is believing: a location limited channel based on grip pattern biometrics and cryptanalysis. CTIT technical report 06-29, Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands, 2006. 10 pp.

[Buh06]

Bulygin:2009:PSS


[Bul09]

Burmansson:2000:TCY


[Bur00]

Burnett:2001:CB


[Bur01]

Burr:2003:SAE

REFERENCES


**Burr:2006:CHS**


**Baker:2007:ISU**


**Blake-Wilson:2002:RUE**


**Bellare:2003:FSP**


**Bar-Yossef:2004:ESQ**

REFERENCES

[Bar-Yossef:2008:ESQ]

[Bertlmann:2002:QUB]

[Bond:2003:DTA]

[Borders:2005:CHP]

[Carrington:2002:EDS]

[Staff:2003:NTC]
CACM Staff. News track: Cinematic watermark; eye-opening education; roaming time; stand by me; savings bonds fade to net; phone home. *Communications of the Association for Computing Machinery*, 46(7):9–10, July 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

[Staff:2006:NTS]
CACM Staff. News track: Super game plan; E-learning roots disputed; Chinese history; U.K. seeks popular science input; encryption commitment; Improve-ment news; vid kid. *Communications of the Association for Computing Machinery*,

[CADOJ:2000:DSE]


[Canetti:2001:UCS]


[Canteaut:2001:CFD]


[Canetti:2006:SCC]


REFERENCES

The issue is a special tribute to Kurt Gödel for the centenary of his birth.

Cobas:2001:CTA

Cooper:2005:AAP

Chandramouli:2006:BPA

Cachin:2000:OFS

Chan:2001:CRP

Carline:2002:NWT
Dylan Carline and Paul Coulton. A novel watermarking technique for LUT based FPGA designs. Lecture Notes in Computer Science, 2438:1152–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
REFERENCES


REFERENCES


[CCD07] Zhenchuan Chai, Zhenfu Cao, and Xiaolei Dong. Efficient ID-based multi-receiver threshold decryption. *International Jour-
REFERENCES


**Choi:2005:JMA**


**Christianson:2002:SPI**


**Christianson:2005:SPI**


**Castelluccia:2009:EPS**

REFERENCES


[CD01b] P. A. Crouch and J. H. Davenport. Lattice attacks on RSA-encrypted IP and TCP.
REFERENCES

*Cramer:2000:CVS*
Ronald Cramer, Ivan Damgård, and Stefan Dziembowski. [CDD00]

*Ceselli:2005:MAI*
Alberto Ceselli, Ernesto Damiani, Sabrina De Capitani Di Vimercati, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. [CDFM05]

*Cimato:2005:ICV*
REFERENCES


REFERENCES


REFERENCES

[Castiglione:2007:TAD]

[Chen:2005:NVW]

[Ceravolo:2004:ERH]

[Certicom:2004:CCC]
Certicom, 5520 Explorer Drive, 4th Floor Mississauga, Ontario, L4W 5L1 Canada. Published quarterly.

[Canetti:2001:UCC]

[Canteaut:2001:COR]
REFERENCES


[Chodowiec:2003:VCF] Paweł Chodowiec and Kris
REFERENCES


Cranor:2005:SUD [CG05]


Chodowiec:2001:ETG [CGBS01]


Caballero-Gil:2009:GBA


Catalano:2000:CIS

Coppersmith:2000:ICT


Catalano:2001:BSP


Caballero-Gil:2006:SSB


Crosby:2002:CHB

REFERENCES

0558/papers/2320/23200192.pdf.


REFERENCES

amp;idtype=cvips.

Canovas:2002:DSB


Cox:2002:SP9


Cimato:2003:SCN


Chow:2009:ADN


Crotch-Harvey:2000:OPR

Trevor Crotch-Harvey. Operators are poised to reap

**Chang:2001:TFG**


**Chen:2001:SFW**


**Chien:2007:SUL**


**Chung:2007:ASF**


**Chung:2007:MRA**


**Chaum:2004:VSB**


REFERENCES

Chen:2000:JCT


Chen:2001:DEU


Chen:2001:PDP


Chen:2001:NVR


Chen:2002:SFS


Cheng:2003:PPO


[Che08b] Wen-Yuan Chen. Multiple-watermarking scheme of the European Article Number Barcode using similar code
REFERENCES


REFERENCES


Coppersmith:2002:CSC


Canetti:2003:FSP


Canetti:2005:ASN


Czeskis:2008:DED


Cheon:2008:PST

Jung Hee Cheon, Nicholas Hopper, Yongdae Kim, and Ivan Osipkov. Provably

**Chang:2002:IBO**


**Chao:2009:HCS**


**Chen:2002:CPK**


**Choi:2006:CHP**


**Choo:2008:PLP**

Chowdhury:2008:CBG


Christianson:2000:SPI


Christianson:2001:SPI


Canetti:2005:HAW


Chen:2002:AMT

Cornea:2002:SCI


Churchhouse:2002:CCJ


Canvel:2003:PIS

[CHVV03] Brice Canvel, Alain Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a SSL/TLS channel. In Boneh

Chang:2005:ILW


Chang:2005:NMS


Cimato:2002:DAP


[Cir01]


[CJ04] Hung-Yu Chien and Jinn-Ke Jan. Improved authen-

Chen:2005:EDS


Chen:2005:EDS


Choie:2005:EIB


Chin:2006:HSI


Clarke:2000:VSP

REFERENCES

[102x681] REFERENCES

198


REFERENCES


REFERENCES


REFERENCES


[Cachin:2001:SEA] Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup. Secure and ef-
icient asynchronous broadcast protocols. In Kilian [Kil01a], pages 524–??.
C79 2001; QA267.A1 L43
no.2139. UK £47.00. URL

Julien Cathalo, François Koeune, and Jean-Jacques Quisquater. A new type
of timing attack: Application to GPS. In Walter et al. [WKP03], pages 291–303.
CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
link/service/series/0558/tocs/t2779.htm; http://www.springerlink.com/

Yannick Chevalier, Ralf Küsters, Michaël Rusinowitch, and Mathieu Turnuанi.
Complexity results for security protocols with Diffie–
Hellman exponentiation and commuting public key en-
cryption. ACM Transactions on Computational Logic, 9
CODEN ????? ISSN 1529-
3785 (print), 1557-945X (electronic).

Christian Cachin, Idit Keidar, and Alexander Shraer.
Trusting the cloud. ACM SIGACT News, 40(2):81–
86, June 2009. CODEN SIGNDM. ISSN 0163-5700
(print), 1943-5827 (electronic).

Chien-Yuan Chen, Cheng-Yuan Ku, and David C.
Yen. Cryptanalysis of large RSA exponent by using the
LLL algorithm. Applied Mathematics and Computation,
169(1):516–525, October 1, 2005. CODEN AMHCBQ. ISSN 0096-3003
(print), 1873-5649 (electronic).

An ID-based digital multisignatures scheme with time
stamp technique. International Journal of Computer Systems Science and


[CL08] Chin-Chen Chang and Pei-Yu Lin. Adaptive watermark mechanism for rightful own-


[CN00b] Julie Clark. Looking for new contactless points: Hong Kong’s Octopus smart card could get a lot smarter, but it will have to pick its way carefully through regulations and competition from other quarters first.
REFERENCES

Cheon:2000:NBC

Canetti:2002:UCT

Chen:2009:AKD

Clulow:2003:SP

Czumaj:2002:PTA


REFERENCES


[CMB+05] Diane Crawford, Marius Mătioc, Steven M. Bellovin, Richard Hubert, Andrew D. Wolfe, Jr., David Foulier, and Andrew R. Kilner. Forum: To block spam, demand sender authentication; not revolutionary (thank goodness); how to know the known from the unknowns; user first in user-centered design. *Communications of the Association for Computing Machinery*, 48(3):11–13, March 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


[Crawford:2005:FBS] Diane Crawford, Marius Mătioc, Steven M. Bellovin, Richard Hubert, Andrew D. Wolfe, Jr., David Foulier, and Andrew R. Kilner. Forum: To block spam, demand sender authentication; not revolutionary (thank goodness); how to know the known from the unknowns; user first in user-centered design. *Communications of the Association for Computing Machinery*, 48(3):11–13, March 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES

Chevallier-Mames:2003:FDS


Chao:2000:CHC


Chao:2008:DNP


Caputo:2009:DIT


Crawford:2002:FEE

Diane Crawford, Srinivas Nedumuri, Adrian Bowyer, Arnd Weber, Greg A. Woods, and Mark Adler. Forum: Embrace the en-

REFERENCES

gineering metaphor; credit for crypto’s parallel development; enough PDF: Give me HTML. Communications of the Association for Computing Machinery, 45(8):11–14, August 2002. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Coron:2004:SSL

Ciet:2003:PFI

Catalano:2002:HHL

Correia:2006:CAB

Czernik:2009:CRN
[CO09] Pawel Czernik and Jakub Oliszyna. Cryptographic random number generators for low-power distributed measurement system. Proceedings of the SPIE — The International Society for Op-
REFERENCES

Cobb:2004:CD

Cocks:2001:IBE

Cochran:2001:NVS

Cochran:2002:NVW
Shannon Cochran. News and views: WaSP [Web


REFERENCES


REFERENCES

[Cor00b] Jean-Sébastien Coron. On the exact security of full domain hash. In Bellare [Bel00], pages 229–??.

[Cor02] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626.

[Cor03] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626.


[Cor00] Jean-Sébastien Coron. On the exact security of full domain hash. In Bellare [Bel00], pages 229–??.

[Cor02] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626.

[Cor03] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626.


[Cor00] Jean-Sébastien Coron. On the exact security of full domain hash. In Bellare [Bel00], pages 229–??.

[Cor02] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626.

[Cor03] Jean-Sébastien Coron. Security proof for partial-domain hash signature schemes. In Yung [Yun02a], pages 613–626.

REFERENCES

215

Courtois:2003:FAA

Courtois:2004:FSB

Courtois:2002:CBC

Courtois:2003:AXA
REFERENCES

Chatzikokolakis:2007:FAP


Cimato:2006:PVC


Chow:2004:UDL


Catalano:2004:IIP

REFERENCES


[CRA05b] Jason Crampton. Understanding and develop-

Canetti:2007:CSH

Canetti:2003:UCJ


Crampton:2005:UDR


Cramer:2005:ACE

Jason Crampton. Understanding and develop-


REFERENCES


REFERENCES


REFERENCES

Chu:2008:EOT


Chou:2009:ATI


Crawford:2001:FPV


Cheung:2001:TPS


Collberg:2007:DGB


Cheng:2001:NPT

[CU01] Qi Cheng and Shigenori Uchiyama. Nonuniform polynomial time algorithm to solve decisional Diffie–Hellman problem in finite fields under conjecture. *Lec-
REFERENCES

Curtin:2005:BFC


Chaitanya:2008:QQM


Canteaut:2002:DCH


Canteaut:2004:PCI

[CV04] Anne Canteaut and Kapeeswaran Viswanathan, editors. Progress in cryptology: INDOCRYPT 2004: 5th International Confer-

Castro:2005:NRG


Chang:2002:ATI


Chess:2007:SPS

Cheng:2009:NAS


Chang:2000:ELD


Chien:2001:CCW


Crosby:2009:OLR


Chien:2005:NRS


Choie:2002:ICH


elsevier.com/gej-ng/10/23/20/80/37/33/abstract.html.
Chen:2005:ENB


Chang:2008:EBD


Chang:2001:NSS


Chang:2004:TSSb


Chang:2005:CIA

REFERENCES

cember 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).


REFERENCES


Jim DeBrosse and Colin B. Burke. The secret in Build-
References

229


Desmedt:2001:ERD

Yvo Desmedt, Mike Burmester, and Jennifer Seberry. Equi-
tability in retroactive data confiscation versus proac-

Doyle:2006:SCK

Barry Doyle, Stuart Bell, Alan F. Smeaton, Kealan McCusker, and Noel E. O’Connor. Security consider-

DiVimercati:2005:CSE

Sabrina de Capitani di Vimercati, Paul Syverson, and Dieter Gollmann, editors. Computer security — ESORICS 2005: 10th Euro-
pean symposium on research in computer secu-

DeBonis:2000:RVC

Dalkili:2002:CPF


DeBonis:2004:RSS


Diene:2006:DLE


Dolev:2000:NC


Dolev:2003:NC


DeSantis:2001:RNI

DeLooze:2007:PWS


Desai:2000:EES


Desai:2000:NPC


Desai:2000:SAN


Desmedt:2002:PKC


REFERENCES


[DFPS06] Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors. *Smart Card
REFERENCES


Domingo-Ferrer:2007:ASC


Damgaard:2005:CBQ


Damgaard:2008:CBQ


Dalkilic:2000:ICA

REFERENCES


DiRaimondo:2005:NAD

DiRaimondo:2003:PST


Dwork:2003:MBF


REFERENCES


Ding:2005:ECB


Dedici:2005:ULB


Dang:2002:EPT


Damgaard:2001:GSS


Donsez:2001:TMA

Didier Donsez, Sébastien


Orr Dunkelman and Nathan Keller. Treatment of the ini-


REFERENCES


Delaune:2008:FAP


Dittmann:2005:CMS


Dodis:2002:KIP


Diffie:1998:PLP


deLeeuw:2000:CSD

thesis has been carried out under the auspices of the research school IPA (Institute for Programming research and Algorithmics). In Dutch and English.

Diffie:2007:PLP


DelLungo:2005:GSP


DeSantis:2000:SSS


Dodis:2000:PRI

Yevgeniy Dodis and Silvio Micali. Parallel reducibility for information-
theoretically secure computation. In Bellare [Bel00],
pages 74–?? ISBN 3-540-67907-3. ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
link/service/series/0558/bibs/1880/18800074.htm;

DeSantis:2007:NRN

Alfredo De Santis and Barbara Masucci. New results
on non-perfect sharing of multiple secrets. The Journal of Systems and Software,
80(2):216–223, February 2007. CODEN JS-
SODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Drimer:2007:KYE

Saar Drimer and Steven J. Murdoch. Keep your enemies close: Distance bounding against
Smartcard relay attacks. Report ??, Computer Laboratory, University of Cambridge, Cambridge,
in USENIX Security Symposium, August 2007, pages
87–102.

Dumais:2000:PCQ

Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment
from any quantum one-way permutation. Lecture Notes in Computer Science, 1807:
300–??, 2000. CODEN LNCSD9. ISSN 0302-
link/service/series/0558/bibs/1807/18070300.htm;

Dowd:2007:ASS

Mark Dowd, John McDonal, and Justin Schuh. The art of software security assessment: identifying and
(paperback). xxi + 1174 pp. LCCN QA76.9.A25

Denev:2009:SFQ

Dimitar Denev, Arturas Mazeika, Marc Spaniol, and
Gerhard Weikum. SHARC: framework for quality-conscious
Web archiving. Proceedings of the VLDB Endowment,
REFERENCES

CODEN ???. ISSN 2150-8097.


REFERENCES


Damgaard:2003:UCE


Dwork:2003:MFM


Dwork:2005:PPW

Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work.
REFERENCES


**Dziembowski:2007:IRS**

**Dziembowski:2008:LRC**

**Dandalis:2001:CSP**

**Damgaard:2005:QCN**

**Delbourg:2002:JBC**

**Daemen:2001:BCP**
Joan Daemen, Michael


*Crescenzo:2004:CRR*


*Daemen:2000:BCR*


*Daemen:2000:RA*


*DDJ:2000:DDE*


*Daemen:2001:AAR*

Joan Daemen and Vincent Rijmen. Algorithm alley: Rijndael: The Advanced Encryption Stan-


Jim Dray. NIST performance analysis of the final round Java AES candidates. In
NIST [NIS00], pages 149–160. ISBN ???? LCCN ????

[Dreyfus:2000:PUC]

[Driscoll:2002:BER]


[Dobbertin:2005:AES]
REFERENCES


See [BEZ01].

Dawson:2005:PCM


DV05


Levy-dit-Vehel:2006:WC


Du:2001:OKS


dW02

Ding:2005:CTC


Dodis:2009:NME


Dwivedi:2004:ISS


Desmedt:2005:CNS


Dittmann:2001:UCW


Dworkin:2003:DRB

Morris Dworkin. DRAFT recommendation for block

Ding:2005:NME


Dawu:2001:TES


Deng:2009:SCA


Ding:2009:MPK


Dai:2001:CDE


Eagleton:2005:BRD

ElAbbadi:2000:VPI


Eghlidos:2001:IRL


Eilam:2005:RSR


English:2007:MAC


ECMA:2000:EPIa


ECMA:2000:EPIb

[ECM00b] ECMA. ECMA-306: Private Integrated Services Network (PISN) — Inter-Exchange Signalling Protocol — Wireless Terminal Au-
REFERENCES


M. Ernst, B. Henhapl, S. Klupsch, and S. Huss. FPGA based hardware acceleration for elliptic curve public key cryptosystems.
REFERENCES

Ellison:2000:PSK


Eggers:2001:DWC


Ekert:2002:BTQ


Ekeraa:2009:DCM


El-Kassar:2001:GPK


Elbirt:2009:UAC


Elliott:2004:QC

Chip Elliott. Quantum cryptography. *IEEE Se-
REFERENCES


Thomas Eisenbarth, Christof Paar, Axel Poschmann,


References

Enck:2005:EOF


Ettinger:2002:QQC


Ebringer:2000:PAP


Edman:2009:AES


Elbirt:2000:FIP


Faliszewski:2007:BRB

Piotr Faliszewski. Book review: *Complexity The-


V. Fischer and M. Druatarovský. Two methods of Rijndael implementation in reconfigurable hardware. Lecture Notes in Computer Science, 2162:77–??, 2001. CODEN LNCSDE9. ISSN
REFERENCES


[Fer00] N. Ferguson. Semi-equivalent keys in MARS. In ?????, editor, Third AES Candidate Conference, page ??, ?????, ?????. April 2000. ISBN ???? LCCN ????


Frenkiel:2002:CCS

Focardi:2000:ITN

Focardi:2000:MAT

Focardi:2003:CTA

Fitzi:2001:MCP

**Field:2009:BCB**


**Filiol:2000:DAS**


**Filiol:2002:NST**


**Finley:2002:BSE**


**Finkenzeller:2003:RHF**


**Finnigin:2006:CPN**

[Fin06] Kevin M. Finnigin. Crypt-


REFERENCES

Freedman:2005:KSO


Fischlin:2001:CLP


Fischlin:2001:ICN


Fischlin:2005:CEN


Faugere:2003:ACH

Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner


REFERENCES


Ferguson:2000:TRR


Fluhrer:2001:AES


Faure:2006:NPK


Freytag:2003:VPI


Fluhrer:2002:CMB

REFERENCES


[Franklin:2002:PAS] Michael Franklin, Bongki Moon, and Anastassia Ailamaki, editors. Proceedings of the ACM SIGMOD International Conference on Man-
REFERENCES


Borivoje (Borko) Furht, Edin Muharemagic, and Daniel Socek. Multimedia


[FOPS01] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA–OAEP is secure under the RSA assumption. In Kilian [Kil01a], pages 260–??.
REFERENCES


REFERENCES


REFERENCES


Fremberg:2003:MAP


Friberg:2001:UCH


Frykholm:2000:CAB


Ferguson:2000:CEI


Fouque:2001:FDT

REFERENCES


[Fundulaki:2004:SYD] Irini Fundulaki and Arnaud Sahuguet. “share your data,


REFERENCES

Furuya:2002:SAK

Fouque:2003:DAW

Feldhofer:2009:HIS

Fan:2008:RSB

Feng:2005:NMS
REFERENCES


[Galbraith:2002:CID] Nicholas Galbraith. Cryptography for Internet and


[Gar04] Paul B. Garrett. The mathematics of coding the-


REFERENCES

Golic:2002:LCB


Goubin:2000:CTC


Gaj:2000:CHP


Gaj:2001:FIF


Goodman:2001:EER

James Goodman and Anantha Chandrakasan. An energy efficient reconfigurable public-key cryptogra-

**Guerrero:2005:ECB**


**Gordon:2008:CFS**


**Gligor:2002:FEA**


**Gennaro:2005:SMS**


**Gebotys:2004:DSC**


**Gennaro:2000:IPR**

Rosario Gennaro. An improved pseudo-random generator based on discrete log. In Bellare [Bel00], pages 469–??. ISBN 3-540-
REFERENCES


REFERENCES

Gentry:2009:FHEb

Giuliani:2001:GLI

Goldstone:2005:FCR

Golomb:2005:SDG

Gambino:2008:ITW

Goldwasser:2008:CAP

Gennaro:2003:LBE
Rosario Gennaro, Yael Gertner, and Jonathan Katz.
REFERENCES


Gennaro:2005:BEG


Gilbert:2002:SCL


Gilbert:2005:FSE


Galindo:2008:SPK


Ghafarian:2007:IPU

in Computer Science Education (ITiCSE’07).


REFERENCES

DEN 1549-6325 (print), 1549-6333 (electronic).

**Gong:2001:GPK**


**Gennaro:2001:RCV**


**Gebhardt:2005:NPV**


**Giraud:2006:RIR**


**Gillespie:2007:WSC**

REFERENCES


Ganapathy:2005:APA


Gennaro:2003:SAP


Gentry:2001:CNS


Gomulkiewicz:2002:HWA

Goldsmith:2004:CAI


Goldwasser:2005:PPK


Gavinsky:2009:ESO


Garay:2007:RCA


Gertner:2000:RBP

Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan. The relationship between public key encryption and oblivious transfer. In IEEE
REFERENCES


REFERENCES


REFERENCES

Gilbert:2002:NRP

Galbraith:2003:IAU

Gorrieri:2004:SFR

Giuliano:2000:ISC

Galbraith:2002:PKS

Goots:2001:FEA
REFERENCES

(Golle) Philippe Golle, Frank McSherry, and Ilya Mironov. [GMM08]

(Galbraith) Steven D. Galbraith, Wenbo Mao, and Kenneth G. Paterson. [GMP01a]

(Galindo) David Galindo, Paz Morillo, and Carla Ràfols. [GMR08]

(K. Gopalakrishnan) K. Gopalakrishnan, Nasir Memon, and Poorvi L. Vora. [GMV01]
REFERENCES

computer.org/mu/books/mu2001/pdf/u4066.pdf;


REFERENCES

Goldreich:1999:MCP


Goldreich:2001:FCBb


Goldreich:2001:FCBa


Golic:2001:CAS


Golic:2001:MOS


Golic:2003:DNP

Jovan D. Golić. DeKaRT: a new paradigm for key-dependent reversible cir-

Goldreich:2004:FCV


Goldstein:2008:BHO


[Goldreich:2004:FCV]

Good:2000:TAE


Good:2000:TAE

Gonda:2006:NMR


[Goldstein:2008:BHO]

Gordon:2002:TCP

REFERENCES


REFERENCES


Güneysu:2008:SPH


Gutterman:2006:ALR


Granger:2005:HSN


Granger:2006:SCA


Gentry:2008:THL


Geng:2008:DSA


Galbraith:2004:EDD

Grasser:1998:FC


Graff:2001:CCW


Granboulan:2002:FDC


Granboulan:2002:SSR


Grigg:2001:FCL


Grossschadl:2001:HSR

REFERENCES


[GS02a] Simson Garfinkel and Gene Spafford. *Web Security, Privacy & Commerce*. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, second edi-
REFERENCES


Geiselmann:2003:HSS

Geiselmann:2007:SPH

Goodell:2007:TOR
Grassl:2009:CAS

Guida:2004:DUP

Garfinkel:2003:PUI

Gaubatz:2008:SCD

Goodrich:2004:ETB
REFERENCES

Giles:2002:ADW


Garay:2000:LLB


Gennaro:2000:LBE


Goodrich:2002:EDD

[GTTC03] Michael T. Goodrich, Roberto Tamassia, Nikos Triandopoulos, and Robert Cohen. Authenticated data structures for graph and ge-

Guttman:2002:ATS


Goodrich:2003:ADS


Guar:2005:PPL


Gumz:2004:BRH


Guillou:2001:CAP


Gutmann:2000:OSC


Gutmann:2002:CFP


Gutmann:2002:DVC

Peter Gutmann. The De-

Gutmann:2004:CSA


Gutmann:2004:SPK


Gutmann:20xx:ESR


GV5


Garera:2009:CTG

Sujata Garera and Jorge Vasconcelos. Challenges in teaching a graduate course in applied cryptography. SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education), 41(2):103–107, June 2009. CODEN SIGSD3. ISSN 0097-8418.

Gassend:2008:CPR

Blaise Gassend, Marten Van Dijk, Dwaine Clarke, Emina Torlak, Srinivas Devadas, and Pim Tuyls. Controlled
CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).


REFERENCES

Hare:2001:RUPa


Hare:2001:RUPb


Harrington:2005:NSP


Harris:2005:GHE


Hars:2006:MIA


Harman:2007:PDS


Hars:2007:DIH

Hasan:2000:LTB


Hasan:2001:ECM


Hasan:2001:PAA


Hasan:2002:JCP


Haufler:2003:CVH


Haufler:2006:SWN


Hayat:2004:CSE

Khwaja Amer Hayat, Umar Waqar Anis, and S. Tauseef ur Rehman. Cryptanalysis of some encryption/cipher schemes using related key attack. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36 (4):85–87, December 2004. CODEN SIGSD3. ISSN 0097-8418. NOTE FROM ACM: It has been determined that the authors of this article plagiarized the
Hayashi:2006:QIT


Hoglund:2006:RSW


Huffmire:2008:DSS


Hartel:2001:TMS


Holcomb:2009:PSS


Humphries:2002:IC

REFERENCES


[Han:2009:ICS] Dong-Guk Han, Dooho Choi,
&arnumber=4663058.


Herranz:2007:IBR


Hess:2004:SVE


Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA


Horvitz:2003:WKA

References

Horan:2005:NRN


Howgrave-Graham:2003:IDF


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2005:PKC


Howgrave-Graham:2003:HNP

Hendricks:2007:LOB

Handschuh:2004:SAC

Handschuh:2005:SAC

Hwang:2005:TSP
Min-Shiang Hwang, Kuo-


REFERENCES


Hirose:2009:SAD


Hinkelmann:2007:CUN


Huhnlein:2001:TPN


Huang:2005:ASE


Harris:2005:IUS


Kim:2000:RMW

REFERENCES


[HL06] Michael Howard and Steve Lipner. The security develop-

Huang:2007:EPS


Hwang:2000:CBV


Hong:2001:PSA


Han:2002:DMA

Hwang:2003:TRB


Hwang:2004:KAS


Hwang:2005:GTS


Hwang:2001:TSB


Hong:2003:BBP


Herzog:2003:PAK

REFERENCES

Hopper:2002:PSS


Hu:2009:TRN


Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU


REFERENCES


REFERENCES


Hoepman:2001:SKA


Hofinger:2001:LBE


Honary:2001:CCI


Hook:2005:BCP


Hoskins:2006:SO


Hu:2005:USA


Hawkes:2001:PCS


Hand:2002:MPP


Halevi:2003:TEM

REFERENCES


Haitner:2007:SHC


Harn:2009:DDB


Hromkovic:2005:DAR


Hromkovic:2009:AAH


Haneberg:2002:MSS


Hemaspaandra:2008:EDA


Hirt:2000:ERF

Hirt, Martin and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In Advances in cryptology—EUROCRYPT
REFERENCES


Hoffstein:2001:MAD


Halevy:2002:LBE


Han:2002:HEF


Hwang:2007:PEA


He:2005:MCP

Changhua He, Mukund Sundararajan, Anupam Datta, Ante Derek, and John C. Mitchell. A modular correctness proof of IEEE 802.11i and TLS. In Meadows and
REFERENCES


REFERENCES

Hanaoka:2006:USA

Hernandez:2002:GCT

Hwang:2001:LCT

Hong:2002:PSR

Hong:2002:IDC
Hernandez:2001:DTR


Hess:2001:TTH


Hernandez:2004:STN


Hsu:2005:CIT


Hsu:2005:UFR

Hasan:2009:PHF


Hanaoka:2000:USD


Halpern:2004:RSS


Huang:2006:CSV


Hongfeng:2008:ECP


Hamalainen:2002:GPS

Antti Hämäläinen, Matti Tommiska, and Jorma Skyttä.
REFERENCES


Hines:2007:AIF


Hofheinz:2005:CTN


Hughes:2002:LAA


Hughes:2004:ISE


Huhnlein:2000:EIC

Detlef Hühnlein. Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders. *Lecture Notes in
REFERENCES


With appendices by Stefan Theisen, Otto Forster, and Ruth Lawrence.


REFERENCES

Hopper:2009:PSS

Hardy:1998:ITN

Hutchinson:2001:IWC

Hardy:2003:AAC

Hellekalek:2003:EEC

Hsu:2004:EPS

Hsu:2005:SCT
Chien-Lung Hsu and Tzong-Sun Wu. Self-certified

**Hwang:2000:CYK**


**Hwang:2005:ITA**


**Hsu:2005:NPM**


**Hu:2008:NNP**


**Hardy:2009:AAC**

Hsu:2002:IGT


Harkins:2005:ESU


Hsu:2003:ITP


Hirose:2001:UAS

References

Hwang:2003:CAL

Yeh:2008:STB

Hwang:2003:ASM

Han:2005:PJ1

Han:2005:PJI

IBM-MARS-Team:2000:MAS
IEEE:2000:ASF


IEEE:2000:IPH


IEEE:2001:ISF


IEEE:2001:EIW


IEEE:2002:PAI


IEEE:2003:PAI


IEEE:2007:PAI


IEEE:2008:PAI


IEEE:2009:PAI


Itoi:2001:SIS

Ifrah:2000:UHN


Iglesias:2002:NSB


Bassham:2000:ETA


Itoh:2003:PCA


Iwata:2000:PAF

Tetsu Iwata and Kaoru
Kurosawa. On the pseudorandomness of AES finalists — RC6, Serpent, MARS and Twofish (abstract only). In NIST [NIS00], page 9. ISBN ???? LCCN ????.


Iwata:2001:PAF


Impagliazzo:2003:LRA

REFERENCES

Ishai:2003:EOT


Ishai:2005:SCC


Ishai:2006:CA


Ishai:2007:ZKS


Iyer:2007:TAA

Ioannidis:2005:ACN


Izmerly:2006:CCA


Imrey:2003:BRC


Inamori:2002:SPB

Hitoshi Inamori. Security of practical BB84 quantum key distribution. Al-
DEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL http://
www.springerlink.com/openurl.asp?genre=article&
issn=0178-4617&volume=
34&issue=4&page=366. Quant-
tum computation and quantum cryptography.

**Inamori:2002:SPT**

www.springerlink.com/openurl.asp?genre=article&
issn=0178-4617&volume=

**Inoue:2005:EST**

[Ino05] Koji Inoue. Energy-security tradeoff in a secure cache architecture against buffer overflow attacks. *ACM SIGARCH Computer Ar-

**Intel:2000:IIP**

developer.intel.com/design/ia-64/downloads/itaniumssl_seg_103.htm.

**Intel:2003:IRN**

developer.intel.com/design/chipsets/rng/docs.htm.

**Itkis:2001:FSS**

[IR01] Gene Itkis and Leonid Reyzin. Forward-secure signatures with optimal signing and verifying. In Kil-
ny.com/link/service/series/0558/bibs/2139/21390332.htm; http://link.springer-

**Itkis:2002:SSB**

[IR02] Gene Itkis and Leonid Reyzin. SiBIR: Signer-
Base Intrusion-Resilient signatures. In Yung [Yun02a], pages 499–514. CODEN
REFERENCES


Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hard-


Janeczko:2006:TSH


Jankowski:2008:BRBb


Jennewein:2000:FCQ


Jones:2005:RDF


Johnson:2001:IHS


Jeffrey:2008:PAM


Jennings:2009:SLL

Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC


CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).


[JJS02] Kahil Jallad, Jonathan Katz, and Bruce Schneier. Implementation of chosen-
REFERENCES


Jarecki:2000:AST


Joux:2003:IGN


Juang:2004:FBT

Jeong:2008:PKE


Juang:2001:FBT


Juang:2002:VMA


Jakobsson:2003:FMT


Johansson:2003:PCI

REFERENCES


REFERENCES


REFERENCES


Jaulmes:2002:SHG


Joye:2003:GFA


Joye:2004:CHE


Joye:2001:PMA

Marc Joye, Jean-Jacques Quisquater, and Moti Yung. On the power of misbehav-

Joye:2001:OAD

Juric:2006:CPW

Jin:2001:WCS

Jaworski:2009:RKP
Jain:2009:PQR

Jarecki:2005:FSP

Jiang:2005:SAI

Joye:2001:PAD
Joye:2001:CEN


Joglekar:2005:PEM


Juels:2004:FCI


Junod:2005:SCB


Jutla:2001:EMA

REFERENCES

link/service/series/0558/
bibs/2045/20450529.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2045/20450529.

Ji:2001:CAF

Dongyao Ji and Yuming
Wang. Comments on “An
approach to the formal ver-
ification of the two-party
cryptographic protocols” by
Zhang, Li and Xiao. Oper-
ating Systems Review, 35(1):
6–7, January 2001. CODEN
OSRED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic). See [ZLX99].

Juels:2005:APD

Ari Juels and Stephen A.
Weis. Authenticating perva-
sive devices with human pro-
tocols. In Shoup [Sho05a],
pages 293–?? ISBN 3-540-
28114-2. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2005; QA76.9 .A25;
QA76.9 C79 2005; QA76.9;
C794 2005; QA76.9; Inter-
net. URL http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

Jeng:2006:EKM

Fuh-Gwo Jeng and Chung-
Ming Wang. An efficient
key-management scheme for
hierarchical access control
based on elliptic curve cryp-
tosystem. The Journal of
Systems and Software, 79
CODEN JSSODM. ISSN
0164-1212 (print), 1873-1228
(electronic).

Jin:2005:EAW

Cong Jin and Kailua Xu.
Estimation and application
of the watermark embed-
ding strength. In Han
et al. [HYZ05b], pages 147–
LCCN ?? URL http://
eproceedings.worldscinet.
com/9812701532/9812701532.
0031.html.

Jiang:2005:RNP

Zhengtao Jiang, Mingsen Xi-
ang, and Yumin Wang. A
research on new public-key
encryption schemes. Applied
Mathematics and Compu-
tation, 169(1):51–61, Oc-
tober 1, 2005. CODEN
AMHCBQ. ISSN 0096-3003
(print), 1873-5649 (elec-
tronic).

Joye:2001:NMM

Marc Joye and Sung-Ming
Yen. New minimal modified
radix-r representation with
applications to smart cards.
Lecture Notes in Computer
CODEN LNCS9D. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
REFERENCES


Jakobsson:2004:ACN

Jiang:2005:TMD

Kadrich:2007:ES

Kahn:1967:CSSa

Kahn:1967:CSSb
David Kahn. The Codebreakers: the Story of Secret Writ-
REFERENCES


Kendall:1939:TRS


Kovacich:2000:HTC


Kiely:2006:SSM


Kamvar:2007:DTM


Kim:2009:DCA


Kachris:2003:RLB

REFERENCES


Ku:2005:WYR


KCL03


Kim:2007:SBE


KCD07


Kalker:2004:DWS

Ton Kalker, Ingemar J. Cox, and Yong Man Ro, editors. Digital Watermarking: Second International Workshop, IWDW 2003, Seoul, Korea,

Kurosawa:2004:NPH

King:2001:SAD

Keefe:2005:CDS

Kelsey:2000:KST

Kelsey:2002:CIL
REFERENCES


REFERENCES


[KH05] Kovacich:2003:MHC


[KH05] Khaw:2005:EDA
REFERENCES


Kobara:2001:SSM


Kurosawa:2003:TTK


Kidwell:2000:SNC


Kida:2002:PGR


Kilian:2001:ACC

REFERENCES


REFERENCES


King:2000:IMP


King:2001:CMF


King:2002:RG1


Kirtland:2001:INC


Montgomery:2003:FEC

Peter L. Montgomery Kirsten Eisenträger, Kristin Lauter. Fast elliptic curve arithmetic and improved Weil pairing evaluation. In Joye [Joy03b],


[KK06] A. Kawachi and T. Koshiba. Progress in quantum com-


0558/papers/2259/22590245.pdf.

**Ko:2007:SRT**


**Kim:2009:SVN**


**Klonowski:2009:SGS**


**Kawachi:2005:UTQ**


**Kaliski:2002:CHE**

REFERENCES


Kelsey:2000:ABA
John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent (abstract only). In NIST [NIS00], page 10. ISBN ???? LCCN ????

Kohno:2000:PCR
Tadayoshi Kohno, John Kelsey, and Bruce Schneier. Preliminary cryptanalysis of reduced-round Serpent. In NIST [NIS00], pages 195–214. ISBN ???? LCCN ????

Kohn:2001:ABA

Kim:2002:IDS
Nam-Youn Kim, Dae-Ghon Kho, and Kee-Young Yoo. Inversion/division systolic architecture for public-key cryptosystems in GF(2\(^m\)). Lecture Notes in Computer Science, 2433:289–??, 2002. CODEN LNCSD9. ISSN
REFERENCES


Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju sung Kang, and Choonsik Park. New public-

Klein:2007:BDC


Kong:2001:AVW


Kiltz:2005:SCM


Kalai:2009:SEU


Kim:2002:EPS

REFERENCES


REFERENCES


Kim:2002:ABA


Kakarountas:2006:HSF


Katz:2001:CCA


Klarlund:2001:MIS


Klimov:2002:ANC

Keliher:2001:IUB


Kim:2003:RCC


Kittler:2003:AVB


Kol:2008:GEI


Koc:2001:CHEb

Çetin K. Koç, David Naccache, and Christof Paar, editors. Cryptographic hardware and embedded systems — CHES 2001: Third Inter-

Krukow:2005:FCR


Knudsen:2000:TT


Knudsen:2000:TTR


Knutson:2007:BPS

### REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>
Koga:2002:GFR


Kurosawa:2001:ICP


Koshiba:2001:NAS


Koshiba:2001:SRS


Koskinen:2001:NIK

[Jukka A. Koskinen. Non-injective knapsack public-key cryptosystems. Theoretical Computer Science,]
REFERENCES


Koc:2003:GEI


Kerins:2002:FPE


Klima:2003:ARB


Kaufman:2002:NSP


Kim:2004:TBG

Yongdae Kim, Adrian Perrig, and Gene Tsudik. Tree-based group key agreement. *ACM Transactions on Information and System Security,*
REFERENCES


REFERENCES

[399]


Krawczyk:2005:HHP

Hugo Krawczyk. HMQV: a high-performance secure
Diffie–Hellman protocol. In Shoup [Sho05a], pages 546–
?? ISBN 3-540-28114-2. ISSN 0302-9743 (print),
.A25; QA76.9 C79 2005;
QA76.9 C794 2005; QA76.9;
Internet. URL http:
issn=0302-9743&volume=
3621.

Kramer:2007:LCC

Simon Kramer. Logical
concepts in cryptography.
ACM SIGACT News, 38
CODEN SIGNDM. ISSN
0163-5700 (print), 1943-5827
(electronic). URL http:
//doi.acm.org/10.1145/
1345189.1345205.

Kreitz:2005:OBE

Gunnar Kreitz. Optimization
of broadcast encryption
schemes. Examensar-
bete, Numerisk analys och
datalogi, Kungliga Tekniska
högskolan, Stockholm, Swe-

Koeune:2002:FIL

Francois Koeune, Gael
Rouvroy, Francois-Xavier
Standaert, Jean-Jacques
Quisquater, Jean-Pierre David,
and Jean-Didier Legat. An
FPGA implementation of
the linear cryptanalysis.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/1
bibs/2438/24380845.htm;
http://link.springer-

Kehr:2001:ISM

Roger Kehr, Michael Rohs,
and Harald Vogt. Issues
in smartcard middleware.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/1
bibs/2041/20410090.htm;
http://link.springer-

Kim:2005:CLL

Kee-Won Kim, Eun-Kyung
Ryu, and Kee-Young Yoo.
Cryptanalysis of Lee–Lee au-
thenticated key agreement
scheme. Applied Mathematics
and Computation, 163
CODEN AMHBQ. ISSN
REFERENCES

0096-3003 (print), 1873-5649 (electronic).

Katz:2000:CCA


Kelsey:2000:MAP


Kuramitsu:2002:ETC


Krause:2003:DOC


Kozaczuk:2004:EHP

REFERENCES

www.loc.gov/catdir/toc/fy051/2004040636.html.

Katz:2005:MIA


Kissner:2005:PPS


Klivans:2006:CHL


Kasper:2009:FTA


Kelsey:2000:YND


Kuhn:2002:ICM


Kuhn:2008:BSS


Kukorelly:2001:PAL


Kundur:2001:WDI


Kurosawa:2001:MRP


Kusters:2002:DCP

REFERENCES


[Huang:2001:AOS]

[Kejariwal:2009:ELL]

[Koshiba:2000:SEP]

[Knudsen:2002:IC]

[Karlof:2003:HMM]
REFERENCES


Kiayias:2001:SPP


Kurosawa:2001:LCI


Katz:2002:TCB


Kiayias:2002:CHB


Kim:2002:PAA

Hyun-Sung Kim and Kee-Young Yoo. Parallel algorithm and architecture for public-key cryptosystem. Lecture Notes in Computer Science, 2510:145–??, 2002. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349


J. Kamp and D. Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. In IEEE [IEE03], pages

Kamp:2007:DEB

Jesse Kamp and David Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryp-

Kumar:2009:UAU


Ladd:2006:SPS


Kamp:2007:DEB

Jesse Kamp and David Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptog-

Laih:2003:ACA

Chi Sung Laih, editor. *Advances in Cryptology—ASIACRYPT 2003: 9th International Conference on the Theory and Applica-
REFERENCES

[Laird:2007:THL]

[Lai:2008:JIA]

[Lamont:1991:UFC]

[Lam:2001:CCN]

[Lambert:2007:SLG]

[Landau:2000:CST]

[Landau:2000:STT]
REFERENCES

Landau:2000:TOD


[Landau:2000:ITS]

Lanet:2000:ITS


Landau:2004:PNS


[Landau:2004:SLE]

Laud:2005:STS

[Lau05] Peeter Laud. Secrecy types for a simulatable cryptographic library. In Meadows and Syverson [MS05b], pages 413–417.
REFERENCES


REFERENCES

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

**Lindskog:2005:DIT**


**Leveiller:2001:CNF**


**Laufer:2000:SSC**


**Laih:2003:COP**


**Lin:2004:SOT**

Min-Hui Lin and Chinch Chen Chang. A secure


REFERENCES


REFERENCES

Lu:2005:RTP


Li:2001:CCB


Lai:2004:SGS


Lavoue:2007:SSW


Law:2006:SBB


Lindquist:2004:JCS


Lee:2001:AES


Lee:2003:BRBa

REFERENCES

CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Buc01, Buc04].

Lee:2003:BRBb


Lee:2003:CS


Lee:2004:SPM


Lee:2004:ACA


Lehtinen:2006:CSB

REFERENCES

Lenstra:2001:USM


Leroy:2002:BVJ


Levy:2001:CHC


Lewand:2000:CM


Liaw:2004:SPA


Lang:2001:CMS

REFERENCES


REFERENCES

Lin:2003:NRU


[177x571][LHL03b]

Lee:2004:SAA


[177x399][LHL04]

Lu:2008:PTZ


[177x252][LHL+08]

Liu:2005:DBV


[177x240][LHS05]

Lee:2009:NCA


[177x232][LHY05]

Lee:2002:FRU


[177x218][LHY02]
REFERENCES

problem for untraceability. 

**Li:2001:NSA**


**Li:2005:ABPa**


**Lieman:2005:CRW**


**Lin:2000:RTI**


**Linn:2000:TMM**

Lin:2001:DWM


Lindell:2001:PCT


Lingmann:2002:DSK


Lindell:2003:SCC


Lin:2007:PFT


Lee:2005:IEC

REFERENCES


[LKJL01] Shin-Young Lim, Jeong-Ho Ko, Eun-Ah Jun, and Gang-Soo Lee. Specification and analysis of n-way key recovery system by Extended Cryptographic Timed Petri...


Lee:2003:ISC


Lee:2004:FIM


Lee:2004:DIS


Lim:2004:ISC


Lee:2005:CMA

Keon-Jik Lee and Byeong-Jik Lee. Cryptanalysis of the modified authenticated key agreement scheme. *Ap-
REFERENCES

Lee:2005:SSP

Li:2005:FCR

Lee:2006:ISC

LL05b]

LL06]

LL05c]

LLH01]
REFERENCES

3-540-42456-3 (paperback).
UK£47.00. URL http://link.springer-ny.com/
link/service/series/0558/[LLL⁺]bibs/2139/21390486.htm;
pdf.

Lee:2002:RUA

[LLH02] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang. A
remote user authentication scheme using hash functions.
CODEN OSRED8. ISSN 0163-5980 (print), 1943-
586X (electronic).

Li:2004:CES

[LLH04] Li-Hua Li, Chi-Yu Liu, and Min-Shiang Hwang. Crypt-
analysis of an efficient secure group signature scheme.
CODEN OSRED8. ISSN 0163-5980 (print), 1943-
586X (electronic).

Lesniewski-Laas:2005:SSS

[LLK05] Chris Lesniewski-Laas and M. Frans Kaashoek. SSL
splitting: Securely serving data from untrusted caches.
Computer Networks (Amsterdam, Netherlands: 1999),
48(5):763–779, August 5, 2005. CODEN ????? ISSN
1389-1286 (print), 1872-7069 (electronic).

Li:2001:SPD

Shujun Li, Qi Li, Wen-ming Li, Xuanqin Mou, and
Yuanlong Cai. Statistical properties of digital piece-
wise linear chaotic maps and their roles in cryptography
and pseudo-random coding. Lecture Notes in Computer
Science, 2260:205–??, 2001. CODEN LNCSD9. ISSN
link/service/series/0558/[LLL]bibs/2260/22600205.htm;
pdf.

Lee:2002:SEC

[LLL02] Hyung-Woo Lee, Sung-Min Lee, and Im-Yeong Lee. Se-
cure electronic copyright distribution with public key
based traitor tracing. Lecture Notes in Computer Science,
2455:324–??, 2002. CODEN LNCSD9. ISSN
link/service/series/0558/[LLL]bibs/2455/24550324.htm;
pdf.
Lee:2004:MPA


Li:2006:ESY


Lee:2005:IWR


Liu:2005:SWA

REFERENCES


REFERENCES


[Leitold:2001:MTN] Herbert Leitold, Wolfgang Mayerwieser, Udo Payer,


Ninghui Li, John C. Mitchell, and William H. Winsbor-


[Loi00] Pierre Loidreau. Strengthen-

Lovering:2001:TKF


Lindell:2000:PPD


Lysyanskaya:2001:AST


Labbe:2002:AIF


Luccio:2002:AC

REFERENCES

Lee:2003:CPK

Li:2005:MCK

Li:2006:PMW

Li:2008:DEO
Lvzhou Li and Daowen Qiu. Determining the equivalence for one-way quantum finite automata. Theoretical Computer Science, 403 (1):42–51, August 20, 2008. CODEN TCSCDI. ISSN

Lee:2003:CPK

Lemke:2006:ESC

Li:2005:MCK

Li:2006:PMW

Li:2008:DEO
Lvzhou Li and Daowen Qiu. Determining the equivalence for one-way quantum finite automata. Theoretical Computer Science, 403 (1):42–51, August 20, 2008. CODEN TCSCDI. ISSN
Lientz:2001:BTP


Lemke-Rust:2007:MAP


Liskov:2002:TBC


Lenstra:2001:SFR


Lindemann:2001:ICT


Loidreau:2001:WKM

REFERENCES


[LSHC05] Haiping Lu, Yun Q. Shi, Alex C. Kot, and Lihui Chen. Binary image watermarking through blurring and biased binarization. International Journal of Image

Li:2005:ABP


Liang:2009:AIE


Lin:2004:SIS

Li:2005:ISS


Lie:2000:ASC


Lin:2005:HAO


Lu:2002:HEA


Lu:2007:NSC


Lucs:2000:ASR

REFERENCES

Lucas:2002:SAB


Lucas:2002:VCS


Lucas:2006:PGE


Ludvig:2005:PWF


Luk'yanov:2001:PFA


Lunde:2009:BCU

Paul Lunde, editor. The book of codes: understanding the world of hidden messages: an illustrated guide to signs, symbols, ciphers,


Laguillaumie:2007:MDV


Lange:2002:PIE


Liang:2005:PAC


Loepp:2005:PIC


Lyuu:2005:CIH


Lee:2004:IAK


Lin:2000:PAS

[LWK00] Xiaodong Lin, Johnny W. Wong, and Weidong Kou. Performance analysis of secure Web server based on

Lv:2005:PCA


Lv:2005:SMS


Li:2005:IWR


Lin:2005:NIB


Lixin:2005:FLA


Li:2005:AAU


[LZ01] K. H. Leung and Bing Zeng. Wavelet-domain image wa-


REFERENCES

Masuda:2002:CDC


Mrayati:2003:AKT


Mrayati:2004:IAD


Mrayati:2005:IDB


Mrayati:2006:TTC


Mrayati:2007:TTC


Mrayati:20xx:AET

Introduction by Chaker Faham.


REFERENCES


REFERENCES


Maurer:2001:C [May01]


Maurer:2004:RCD [May02]


Maximov:2006:SWC


Mayers:2001:USQ


May:2002:CUR

service/series/0558/papers/2442/24420242.pdf.


http://arith17.polito.it/final/paper-149.pdf.

**McCamant:2008:QIF**


**Monteiro:2008:AVM**


**Meadows:2001:OIF**


**Meadows:2004:OSM**


**Mehrabi:2001:DW**


**Mena:2003:IDM**


REFERENCES


&Marti-Farre:2007:NSS


&Mueller:2006:SMG


&Muller:2009:BPE


&Minier:2001:SCC

REFERENCES


Moon:2002:IDC


May:2002:SKS


Mihaljevic:2009:ASC


Micciancio:2001:ILB


Micciancio:2002:GCK

REFERENCES

Micciancio:2002:ICH


Millen:2003:FD


Mironov:2002:RSO


Mirkovic:2005:IDS


Mishra:2006:PCS


Misić:2008:TEC

Jelena Mišić. Traffic and energy consumption of an IEEE 802.15.4 network in the presence of authenticated, ECC Diffie–Hellman ephemeral key exchange. Computer Networks (Amsterdam, Netherlands: 1999), 52(11):2227–2236, August 8,
Mitchell:2000:MSN


Mitra:2002:TAD


Miyazaki:2001:ISG


MacDonald:2003:CDS


Maltoni:2004:BAE


Moore:2001:AGK

Patrick C. Moore, Wilbur R. Johnson, and Richard J. De-

Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS


Moyle:2005:CLD


Mazieres:2000:SKM


Majzoobi:2009:TDI


MM01b  M. McLoone and J. V. McCanny. High performance single-chip FPGA Rijndael algorithm implementations. *Lecture Notes in Computer*
REFERENCES


McLoone:2001:SCF


Mana:2002:PMD


Moldovyan:2007:IC


Mullen:2007:FFA


Moreira:2002:RCE

REFERENCES

Milenkovic:2005:UIC

Maltoni:2003:HFR

McEvoy:2009:IWH

Maitra:2006:PCI

Matsumoto:2002:IAG


Monsignori:2001:WMS


Mironov:2008:SAE


MacAndrew:2000:LPT


Mykletun:2006:AIO


Mollin:2001:IC


Moller:2002:PEC


REFERENCES

URL http://deposit.ddb.de/cgi-bin/dokserv?id=2739575&prov=M&dok_var=1&dok_ext=htm.


Moshopoulos:2001:NSA


Malkhi:2002:ACE

REFERENCES


REFERENCES


[MR02a] S. Murphy and M. J. B. Robshaw. Essential algebraic structure within the AES. Report, Information
REFERENCES


REFERENCES


Markowitch:2003:CWV

Miklau:2003:CAP

Martin:2005:PET

Meadows:2005:CPA

Mahdian:2009:UNI

Manulis:2009:SMF
Mark Manulis and Jörg Schwenk. Security model

Myers:2009:BEC


Shen:2005:NIW


MacKenzie:2002:TPA


McClure:2003:HEN


Matsumoto:2007:FSC

Makoto Matsumoto, Mutsu Saito, Takujii Nishimura, and Mariko Hagita. A fast stream cipher with huge state space and quasigroup filter for software. In Adams et al. [AMW07], pages 246–
   LCCN ????

**Miltchev:2008:DAC**


**Mouratidis:2009:PMD**


**Moran:2004:NIT**


**Myasnikov:2005:PAB**


**Muzereau:2004:EBD**


**Marsaglia:2002:SDP**


S. Murphy. The key separation of Twofish. Comments on AES round 2 submitted to NIST., March 2000.

REFERENCES


REFERENCES


REFERENCES


Nedjah:2005:SHC


Nash:2001:PIM


Nedjah:2004:ECH


Nedjah:2006:NTC


Netscape:2004:HSW


Neuenschwander:2004:PSM

REFERENCES


REFERENCES


Nievergelt:2002:FLM

Niederreiter:2004:BRC

Nikander:2002:DSAa

Nikander:2002:DSAb

NIST:2000:TAE
NIST, editor. *The Third Advanced Encryption Standard Candidate Conference,*


[NIST:2003:RKE]

[Nagaj:2006:OQE]

[Ning:2008:MAA]
REFERENCES

ISSN 1550-4859 (print), 1550-4867 (electronic).

**Nigrini:2009:DDU**


**Nagao:2005:UCS**


**Northcutt:2002:NID**


**Naor:2003:CFP**


**Nozaki:2001:IRA**

Nikov:2006:RBV


Naor:2001:RTS


Naor:2005:ECH


Novak:2001:SBA


Naccache:2002:PKC


[NS01a] Jean Néraud and Carla

[NS05a]

Nguyen:2001:ISA


[NS05b]

Nguyen:2005:FPL


[NSN05]

Nguyen:2005:PSE


[NSS02] Mototsugu Nishioka, Hisayoshi Satoh, and Kouichi Saku-
rai. Design and analysis of fast provably secure public-

[NZCG05] A. Nenadic, N. Zhang, B. Cheetham, and C. Goble. RSA-based certified delivery of E-goods using verifiable and recoverable signature en-


[Oec03] Philippe Oechslin. Making a faster cryptanalytic time-
memory trade-off. In Boneh [Bon03], pages 617–630. CO-
REFERENCES


Oppliger:2008:STS


Oiwa:2009:IMS


Okamoto:2000:ACA


[OHB08]

[Oiw09]

[Oka00]

[OKE02]


Ohzahata:2002:FAM

Satoshi Ohzahata, Shige-

Ogata:2006:OSS


Ols00


Ohigashi:2009:PMF


Ohkuma:2001:BCH


Ohbuchi:2002:FDA


Onions:2001:SSI

Paul Onions. On the strength of simply-iterated

Ors:2003:PAA


Opp:2005:CC

REFERENCES

Ortiz:2000:ITW

Okeya:2000:PAB

Okeya:2001:EEC

Ostrovsky:2005:PSS

Oren:2006:PAR

Obimbo:2007:PAD
Charlie Obimbo and Be-


Katsuyuki Okeya, Katja Schmidt-Samoa, Christian Spahn, and Tsuyoshi Takagi. Signed binary representations revisited. In Franklin [Fra04], pages 123–?? CODEN LNCS9D.


Dag Arne Osvik. Speeding up Serpent. In NIST
REFERENCES


[OTU00] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryp-

**Ouellette:2005:PPM** [Oue05]


**Overbeck:2006:EGA** [Ove06]


**Onieva:2008:MNS** [OZL08]


**Paeng:2003:SCU** [Pae03]


**Page:2003:BRW** [Pag03]


**Panditaratne:2007:TRN** [Pan07]

REFERENCES

Papanikolaou:2005:BRBa


Park:2004:APP


Pass:2003:DCR


Pass:2005:UCN


Patterson:2001:DFI


Patiyoot:2002:MSE

D. Patiyoot. Migration /
REFERENCES

Patiyoot:2002:SIW


Patarin:2003:LRR


Paterson:2003:CCI


Patarin:2004:SRF


Paulson:2002:NBPb

[Linda Dailey Paulson. News

Paulson:2002:NBR


Paulson:2003:NBV


Paulson:2009:NBT


Praca:2001:SCS


Piva:2002:MCW

Alessandro Piva, Franco
REFERENCES


S. Papadimitriou, T. Boumtis, S. Mavroudi, and A. Bez-

Perez:2007:URR


Pucheral:2001:PSD


Peikari:2004:SW


Park:2005:ISC

REFERENCES


REFERENCES


[Per03] Tom Perrine. The end of crypt() passwords ... please? *login: the USENIX Association newsletter*, 28(6):??, December 2003. CODEN LOGNEM. ISSN 1044-
Perlman:2005:EMD


Petullo:2003:IEH


Petullo:2005:EYR


Petzold:2008:ATG


Potter:2003:S


Pfitzmann:2001:ACE

service/series/0558/tocs/t2045.htm.

Phatak:2005:FMR


Power:2007:SBB


Provos:2003:HSI


Phan:2004:IDC

Raphael C.-W. Phan. Impossible differential crypt-


Paeng:2001:NPK


Polk:2003:IIC

REFERENCES


[Pin06] Stephen Pincock. Codebreaker: the history of codes and ciphers, from the ancient pharaohs to quantum cryptography. Walker,
REFERENCES


Pecho:2009:APW


Park:2001:RFW


Poh:2001:HBP


Petitcolas:2003:DWF

[Fabien A. P. Petitcolas and Hyoun Joong Kim, editors. Digital watermarking: First Interna-
REFERENCES


Park:2001:PTU

Park:2001:CSC

Park:2005:CZA

Pliam:2001:PTU
Pon:2005:MDS


Pon:2005:OPK


Pfleeger:2007:IBC


Paulson:2000:NBU


Piper:2002:CVS


Pang:2008:AQR


Pointcheval:2000:CCS

REFERENCES

Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP


Pornin:2001:THE


Porras:2006:PEG


Pfleeger:2003:SC

Charles P. Pfleeger and Shari Lawrence Pfleeger. Se-

Paul:2006:SSC

Popp:2006:CTT

Pfleeger:2007:SC

Paar:2009:UCT

Pellikaan:1996:AGC

Piret:2003:DFA
Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In Walter et al. [WKP03], pages 77–88. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
Picard:2001:NNF


Pass:2005:NIC


Preneel:2000:ACE


Preneel:2001:NES

REFERENCES

Preneel:2002:NEA


Preneel:2002:TCC


Preneel:2007:SRD


Price:2000:NCH


Provos:2000:EVM


Provos:2001:DAS

Niels Provos. Defending against statistical steganalysis. In USENIX [USE01c],
REFERENCES


Paun:2004:CTT


Pfitzmann:2001:SEC


Poupard:2000:FER


Pornin:2001:SHT


Parker:2001:RKC
REFERENCES


REFERENCES


Phan:2006:FDB


Park:2008:SRB


Pavlou:2008:FAD


Park:2002:SRL


Pareschi:2009:PAC


Petit:2008:BCB

C. Petit, F. Staudeart, O. Pereira, T. Malkin, and M. Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In ?????, editor, *ASIAN ACM Symposium on Information,
REFERENCES


Roman:2007:SCP

Ramesh:2001:TAE

Rand:1955:MRD

Rijmen:2001:WHF

Rogaway:2003:OBC

Rand:2001:MRD
REFERENCES


REFERENCES


[Rey01] Robert Reynard. Secret code breaker online. World-Wide


[Rhi03] Jason P. Rhinelander. Design and implementation of encryption algorithms in a coarse grain reconfigurable environment. Thesis (M. Eng.), Memorial University of Newfoundland,
REFERENCES


Riedl:2002:FSH


Ruiz:2001:SPS


Roy:2004:FSE


Reyhani-Masoleh:2003:LCS

[RMH03a] Arash Reyhani-Masoleh and M. Anwar Hasan. Low complexity sequential normal basis multipliers over GF(2^m). In Bajard and Schulte [BS03], pages 188–
Reyhani-Masoleh:2003:LCB


Reyhani-Masoleh:2004:TFT


Rahaman:2008:CTB


Ryabko:2005:NTA


Ryutov:2000:RESa


Ryutov:2000:RESb

REFERENCES


REFERENCES


REFERENCES

Roychowdhury:2000:PCJ


Roy:2005:ACA


Rieffel:2000:IQC


Ramzan:2000:RSS


Reyzin:2002:BTB


Robshaw, and Yiqun Lisa Yin. RC6 as the AES. In NIST [NIS00], pages 337–342. ISBN ????. LCCN ????

Rosenbaum:2000:SFR

Rubin:2002:SAV

Rubin:2003:TBC
REFERENCES


RSA Laboratories. PKCS #15: Conformance Profile Specification. RSA Data Security, Inc., Redwood City, CA, USA, August 1, 2000. 8 pp. URL


REferences

69213-4. LCCN ????
URL http://d-nb.info/997902213/34; http://
/nbn-resolving.de/urn:nbn:de:111-20091103138; http://www.springerlink.com/content/r61844.

URL http://d-nb.info/997902213/34; http://
/nbn-resolving.de/urn:nbn:de:111-20091103138; http://www.springerlink.com/content/r61844.

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title and Publication Details</th>
</tr>
</thead>
</table>
REFERENCES


**Russell:2002:HFU**


**Renner:2003:NBS**


**Renner:2003:UAP**


**Ramaswamy:2007:HSP**


**Schmalz:2003:MDI**

REFERENCES


References


Salomon:2003:DPS


Salomon:2005:CDC


Salomon:2005:FCS


Sallee:2005:MBM


Sale:2005:RCB

Anthony E. Sale. The rebuilding of Colossus at Bletchley Park. IEEE An-
Salomon:2007:DCC


Sale:20xx:CRP


Samid:2001:ESR


Samtani:2009:WTO


Santini:2005:WSI


Sarkar:2002:FCM

Sasse:2007:REB


Satoh:2006:DPI


Savelli:2004:NDC


Soto:2000:RTA


Shacham:2001:ISH


Scott:2004:CP


Stoklosa:2005:CIC

Janusz Stoklosa and Jaroslaw Bubicz. Compound inversive


Jun Shao and Zhenfu Cao. A new efficient (tn) veri...

**Stephanides:2005:GAK**


**Sun:2005:IPK**


**Siegelin:2001:SCD**


**Schmalz:2000:MAD**


**Schneier:2000:AAR**

REFERENCES

Schneier:2000:IRS


Schneier:2000:SLD


Schneier:2000:SRF


Scharinger:2001:ASK

Josef Scharinger. Application of signed Kolmogorov hashes to provide integrity and authenticity in Web-based software distribution.

Schindler:2001:TAA


Schmalz:2001:MDI

Schneier:2001:FSE  [Sch01d]


Schneier:2003:BFT  [Sch03]


Schmalz:2004:MDIa  [Sch04a]

Schmalz:2004:MDIb


Schneier:2004:SA


Schramm:2006:AMS


Schmalz:2005:MDI


Schneier:2005:AE


Schneier:2005:TFA

REFERENCES


555

REFERENCES

0096-3003 (print), 1873-5649 (electronic).


[SCS05c] [SDFH00]


Sarah Spiekermann and


Seifert:2005:ACR

Speed:2001:PIS

Speed:2002:PIS

Semanko:2000:CAA

Sennewald:2003:ESM

Sergienko:2006:QCC

Sutherland:2008:AVO
Iain Sutherland, Jon Evans,

Shumow:2007:PBD


Simka:2006:MTR


Sakr:2007:RCB


Sutton:2007:FBF


Steinwandt:2001:TDB

REFERENCES


Shapiro:2002:CCM

 Urdu http://www.usenix. [Sha03d]
org/publications/library/
proceedings/usenix02/tech/
freenix/shapiro.html.

Shamir:2003:RS

Adi Shamir. RSA shortcuts. In Joye [Joy03b], page 327. CODEN LNCS9D. ISBN 3-
540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25
link/service/series/0558/
tocs/t2612.htm; http://www.springerlink.com/
openuurl.asp?genre=issue&
issn=0302-9743&volume=
2612.

Shamir:2003:TLC

Adi Shamir. Turing Lecture on cryptography: a status report. World-
Wide Web slide presenta-
tion, video, and audio., 2003. URL http://www.acm.org/
turingawardlecture/RSA/.

Shao:2003:CIB

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

Shao:2003:PSS


Shaltiel:2004:RDE

Ronen Shaltiel. Recent developments in extractors. In Păun et al. [PRS04], page ?? ISBN 981-238-
783-8 (set), 981-238-966-0 (vol. 1), 981-238-965-2 (vol. 2). LCCN QA76 .C878
cs.haifa.ac.il/~ronen/
online_papers/online_papers.
html; http://www.cs.
haifa.ac.il/~ronen/online_papers/survey.ps.


Kyungah Shim. Off-line password-guessing attacks on the generalized key agreement and password authen-

**Shih:2008:DWS**


**Sierra:2004:LCC**


**Shimizu:2007:CBE**


**Shoup:2000:CTU**


**Shoup:2000:UHF**


**Shoup:2001:OR**

Victor Shoup. OAEP
reconsidered. In Kilian [Kil01a], pages 239–??.
C79 2001; QA267.A1 L43
no.2139. UK £47.00. URL
com/link/service/series/
0558/bibs/2139/21390239. [Shp99]
htm; http://link.springer-
ny.com/link/service/series/
0558/papers/2139/21390239.
df.

[Sho05a] Victor Shoup, editor. Ad-
vances in cryptography: CRYPTO
2005: 25th Annual Inter-
national Cryptology Confer-
ence, Santa Barbara, Cal-
ifornia, USA, August 14–
18, 2005: proceedings, vol-
ume 3621 of Lecture Notes in
Computer Science. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
2005. ISBN 3-540-
28114-2. ISSN 0302-9743
(print), 1611-3349 (elect-
tronic). LCCN QA76.9.A25
C79 2005; QA76.9 .A25;
QA76.9 C79 2005; QA76.9
C794 2005; QA76.9; In-
ternet. URL http:/
/www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

[Sho05b] Victor Shoup. A com-
putational introduction to
number theory and algebra.
Cambridge University Press,
0-521-85154-8 (hardcover),
0-521-61725-1 (paperback).
svi + 517 pp. LCCN QA241

theoretic methods in
cryptography: complexity
lower bounds, volume 17 of
Progress in computer science
and applied logic. Birkhäuser
Verlag, Basel, Switzerland,
1999. ISBN 3-7643-5888-
2 (Basel), 0-8176-5888-2
(Boston). viii + 180 pp.
LCCN QA267.7.S57 1999.

uniformity of distribution of
the RSA pairs. Mathematics
of Computation, 70(234):
801–808, April 2001. CO-
DEN MCMPAF. ISSN 0025-
5718 (paper), 1088-6842
(electronic). URL http:/
/www.ams.org/journal-
getitem?pii=S0025-5718-
00-01274-6; http://www.
ams.org/mcom/2001-70-234/
S0025-5718-00-01274-6/
S0025-5718-00-01274-6.
dvi; http://www.ams.
org/mcom/2001-70-234/S0025-
5718-00-01274-6/S0025-
5718-00-01274-6.pdf;
http://www.ams.org/mcom/
2001-70-234/S0025-5718-
00-01274-6/S0025-5718-
00-01274-6.ps; http:/
/www.ams.org/mcom/2001-


REFERENCES


[Sin99] Simon Singh. The code book: the evolution of secrecy from Mary, Queen of Scots, to


Sivonen:2006:MPF


Schnorr:2000:SSE


Sucurovic:2005:JCX


Schaumont:2009:GEI


Song:2000:TPA


Seki:2001:DCR


REFERENCES

[570]

Sano:2000:PEA

Schindler:2001:IDC

Sugita:2000:RAD
REFERENCES

like RIJNDAEL, E2. In NIST [NIS00], pages 242–256. ISBN ?? LCCN ???.

Scharwaechter:2007:AAE

Schneier:2000:CTA

Stebenz:2000:PAC


REFERENCES

Sebag-Montefiore:2000:EBC

Sarkar:2001:EIL

Sarkar:2003:EIC

Satoh:2002:SHS

Satoh:2003:UHA
Akashi Satoh and Sumio Morioka. Unified hardware architecture for 128-bit block ciphers AES and Camellia. In Walter et al. [WKP03], pages 304–318. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
REFERENCES

Sebag-Montefiore:2005:EBC


Simos:2007:CMS


Smith-Miles:2008:CDP


Smart:2001:CDF


Smart:2003:ACU


[SoHS01] David Sánchez, Agustín Orfila, Julio César Hernández, and José María Sierra. Robust new method in frequency domain watermarking. Lecture Notes in Computer Science, 2200:


Lenin Singaravelu, Calton Pu, Hermann Härting, and Christian Helmuth. Reducing TCB complexity for...

**Sun:2008:BWN**


**Stern:2002:FAP**


**Song:2001:ANL**


**Shin:2000:ANT**


**Sanchez-Reillo:2001:IBA**

Raul Sanchez-Reillo. Including biometric authentication in a smart card operating system. *Lec-
REFERENCES

StDenis:2006:BMI

Stipcevic:2007:QRN

Samarati:2001:AMP

Standaert:2003:EIR

Sarkar:2001:PAE
Stubblebine:2001:AAF

Seznec:2003:HUL

Swiderski:2004:TM

Seddik:2009:IWB

Shi:2008:UAU

Susilo:2000:NEF
REFERENCES

Scambray:2006:HEW


Schmidt-Samoa:2006:AFW


Sakurai:2001:NSS


Shamir:2001:IOO


Stern:2001:ADW

REFERENCES


[ST03d]

[ST03b]


[ST06]
Michal Spivak and Sivan Toledo. Storing a persistent transactional object heap on flash memory. ACM SIGPLAN Notices, 41(7):22–33, July 2006. CODEN SIN-
ODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

**Stallings:2000:SSC**


**Stallings:2002:CNS**


**Standboge:2002:ENO**


**Stajano:2003:SCU**


**Stanik:2005:NLO**


**Stamp:2006:ISP**


**Steinwandt:2001:LTP**

[Ste01] Rainer Steinwandt. Loop-holes in two public key cryptosystems using the modular group. *Lecture
REFERENCES


Stefanek:2002:ISB


Steele:2005:PPT


Steil:2005:MMM


Stern:2005:MLF


Stein:2008:ENT


Stinson:1995:CTP

REFERENCES


[Str01a] Bruno Struif. Use of bio-

**Strunk:2001:JQJ**


**Strubinger:2002:HBS**


**Stytz:2004:BRW**


**Saxena:2007:TCP**


**Shaltiel:2007:LEU**


**Sugihara:2001:PCD**

REFERENCES


[SV08b] Ronen Shaltiel and Emanuele Viola. Hardness amplification proofs require majority. In ACM [ACM08], pages
REFERENCES


random bit generator based on coupled chaotic systems and its applications in stream-cipher cryptography.


**Seo:2001:CDA**


**Shi:2001:NSF**


**Sun:2005:CSS**


**Syverson:2002:FCI**

Skoudis:2003:MFM


Sarikaya:2008:SPT


Sun:2002:NAD


Sun:2005:WIW

November 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).


REFERENCES


[Tsai:2001:GSI] Chwei-Shyong Tsai and Chin-Chen Chang. A generalized secret image shar-

**Theoharidou:2007:CBK**


**Tirkel:2001:UWE**


**Tabatabaian:2001:NSP**

REFERENCES


Tippett:1927:RSN

Torres:2007:ANS

Tseng:2001:GGO

Tseng:2001:CLB

Tseng:2003:DSM

Tico:2003:RAS

Toll:2008:CSE
References


[TM01] Toshio Tokita and Tsutomu Matsumoto. On applicability
REFERENCES


Justin Troutman and Vincent Rijmen. Crypto corner: Green cryptography: Cleaner engineering through recycling, part 2. IEEE
Troutman:2008:VMM


Tsaur:2001:FUA


Tsaur:2005:SSS


Tsaban:2006:FGD


Tsang:2007:WCT


Tseng:2007:SAG

REFERENCES

Takano:2000:PTH

[TSO00] Kohji Takano, Akashi Satoh, and Nobuyuki Ohba. Poster 5: TATSU — hardware accelerator for public-key cryptography using Montgomery method. In Anonymous [Ano00b], page ??

Tsunoo:2003:CIC


Tahir:2000:RCM


Tzeng:2001:PKT


Tian:2001:ICE


Tuchman:1966:ZT

[Tuc66] Barbara W. Tuchman. *The Zimmermann telegram*. MacMil- [Kah96] describes this book as “recount[ing] the political effects of the most important cryptogram solution in history”.

[Tue66]
**REFERENCES**

**Turing:2004:BS**


Text prepared by Ralph Erskine and Philip Marks and Frode Weierud from the only two surviving copies of Turing’s typescript.

**Tiri:2003:SEA**


**Toft:2001:LTT**


**Trappe:2002:ICC**


**Trappe:2005:ICC**

REFERENCES

Talbot:2006:CCI


Tsai:2007:TTA


Tsaur:2005:EUA


Tiwari:2009:CIF

[TWM+09] Mohit Tiwari, Hassan M. G. Wassel, Bita Mazloom, Shashidhar Mysore, Frederick T. Chong, and Timothy Sherwood. Complete in-

formation flow tracking from the gates up. ACM SIGPLAN Notices, 44(3):109–120, March 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Thamrin:2008:PBR


Tzeng:2004:NTM


Ting:2002:FBS

[TYLL02] Kurt K. Ting, Steve C. L.


Tamer Uz, George Bebis, Ali Erol, and Salil Prab-


**Uhl:2005:IVE**


**Urban:2001:MWB**


**Urien:2001:PIS**


**USENIX:2000:PLI**


**USENIX:2000:PFW**


**USENIX:2000:PFSa**

[USE00c] USENIX, editor. *Proceedings of the Fourteenth Sys-
REFERENCES

USENIX:2000:PNU


USENIX:2001:PUA


USENIX:2001:PFT


USENIX:2002:PUS

REFERENCES


Conference on Coding Theory, Cryptography and Number Theory held at the U.S. Naval Academy during October 25–26, 1998.


REFERENCES


Vavraiv:2003:RNG


Voloshynovskiy:2005:ITD

Sviatoslav Voloshynovskiy, Frederic Deguillaume, Oleksiy Koval, and Thierry Pun.

**vanDijk:2006:ICS**


**vanDijk:2004:AOC**


**Verheul:2001:EXM**


**Vercauteren:2002:CFZ**


**Vergnaud:2006:RBS**


**Vernitski:2006:CUM**


[VK07] Cabir Vural and Serap Kazan. Image normalization...
REFERENCES

Vo:2008:SMA


Volos:2009:IEP


Viega:2003:SPC


Viega:2002:NSO

REFERENCES

Vasco:2005:NCS


Vaughan-Nichols:2004:VAS


vanOorschot:2007:IRS


Vogt:2001:USC


Vasco:2001:CPK

[VS01] Maríá Isabel González Vasco and Rainer Steinwandt. Clouds over a public key cryptosystem based on Lyndon words. Informa-
REFERENCES

Voyiatzis:2008:SFS

vanTilborg:2000:FCP

vanTilborg:2001:ECC
Henk van Tilborg. Elliptic curve cryptosystems; too good to be true? Nieuw

Vaudenay:2007:POK

Venkatesan:2001:GTA
Ramarathnam Venkatesan, Vijay Vazirani, and Saurabh Sinha. A graph theoretic approach to software watermarking. Lecture Notes in Computer Sci-


 REFERENCES


REFERENCES

001-0782 (print), 1557-7317 (electronic).


REFERENCES

Walter:2001:PBM


Walter:2003:STM


Wang:2004:AWA


Wang:2004:TVS


Wang:2005:SCR

REFERENCES


**Wardlaw:2000:RPK**


**Washington:2008:BRB**


**Washington:2008:ECN**


**Wayman:2001:FBA**


**Wayman:2002:BAT**


**Wayner:2002:DCI**


**Wayner:2009:DCI**

REFERENCES


[WBRF00] Bryan Weeks, Mark Bean,


REFERENCES


[WFLY04] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive,
Wang:2002:CSE

[WG02]

Wang:2005:RST

[WG05]

Wong:2000:SGC

[WGL00]

Wu:2002:CAE

[W02a]

Wu:2002:IBM

[W02b]

Wu:2003:TSS

[W03]

Wang:2009:NWM
Yu-Ping Wang and Shi-Min Hu. A new watermarking method for 3D models based on integral in-

Wen:2005:URE


Wu:2008:RPG


Watanabe:2001:EAP


Whyte:2005:TFC

REFERENCES


Wiener:2000:AAH

Williams:1999:QCQ

Wilson:2001:SEH

Wilcox:2001:SEH

Williams:2006:C

Winchester:2000:USI

Wincelberg:2001:JQH
REFERENCES

Windley:2005:DI


Winkel:2005:GEC


Winkler:2005:SAU


Withers:2001:IWU


Wang:2007:VBW


Welschenbach:2001:CCC


Wang:2005:ECSb

Won:2006:ISC


Weigold:2008:RCA


Walter:2003:CHE


Wang:2002:AAB


Wedde:2004:MAA

Horst F. Wedde and Mario Lischka. Modular authorization and administration.
REFERENCES


Wu:2004:RKA

Wang:2005:CHY

Wang:2007:NCD

Wen:2005:TRB

Wang:2009:DSM

Wang:2005:SAI

Wu:2005:IAW
Qiong Wu, Guohui Li, and Dan Tu. An image authentication watermarking

Wong:2004:RCK


See [kWpLwW01, AMRP04].

Wang:2005:TSP


Wu:2008:RWM


Watters:2008:VDL


Wheeler:1995:TTE


Watanabe:2002:CCD

REFERENCES

Wang:2008:NAD

Wang:2009:RDA

Wolkerstorfer:2001:AIA

Wollinger:2004:SHI

Won:2001:ISC


REFERENCES

[WS02]

[WRS03]
Weimerskirch:2002:DLW


Wu:2002:CSCb


Wuensche:2009:CAE


Wu:2000:PKC


Wu:2001:FED

Chuan-Kun Wu and Vijay Varadharajan. Fair exchange of digital signatures with offline trusted third party.
Woodruff:2002:CUC


Wang:2004:CWS


Wolf:2005:NML

REFERENCES


Wincelberg:2002:LIE


Wang:2008:HQS


Wang:2002:WEM


Wu:2005:CTR


Wyant:2002:APK

REFERENCES


[Wang:2005:DIC] Xuebing Wang, Linhua Zhang, and Yong Wu. Design and implementation of
a chaos-based public key encryption scheme. In Han et al. [HZY05b], pages 79–?? ISBN 981-270-153-2.

Xu:2001:EIE


Xu:2005:ETR


Xu:2001:CPW


Xiao:2003:HPC


Xiao:2005:SPA

Lu Xiao and Howard M. Heys. A simple power analysis attack against the key schedule of the Camellia block cipher. Information Processing Letters, 95(3):409–412, August 16, 2005. CODEN IFPLAT. ISSN
REFERENCES

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


Xu:2009:AVB


Yan:2000:NTC


Yan:2002:NEC


Yang:2005:TFN


Yuan-bo:2004:ITA


Yue:2001:GNN

REFERENCES


[YG01b] A. M. Youssef and G. Gong. On the interpolation at-...

Youssef:2001:CPK


Yang:2005:IME


Yamamura:2000:QCB


Yamamura:2001:EDA


Yi:2004:AKA

Yen:2000:CBO

Yen:2002:CAO

Yen:2002:RSR

Yaridi:2008:HAC

Yamamoto:2001:PKB
Hideo Yamamoto, Tetsutaro Kobayashi, Masahiro

Yu:2001:TCB


Yi:2009:SSG


Yu:2005:EHI


Yoo:2002:LAU


Yurkewych:2005:CIR

REFERENCES


Yue:2006:NCB


Young:2001:RP


Youssef:2001:CAF


Young:2006:MCC


Youn:2008:WRB


Yang:2009:AIO


Yin:2001:RMW

Yilek:2009:WPK

Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, and Stefan Savage.

Yoon:2004:SUA


Yoon:2005:CFI


Yoon:2005:ICJ


Yoon:2005:IFA


Yeh:2002:SAK

REFERENCES

OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).


Yang:2004:ENT


Ytrehus:2006:CCI


Yang:2005:SEA


Yung:2002:ACC


Yung:2002:CI


REFERENCES


Young:2000:RBA


Young:2001:BOK


Young:2004:MCE


Yoon:2005:CZX


Yoon:2005:SWL


Ye:2001:ATD


REFERENCES

Zhang:2005:ITA


Zivkovic:2005:AAH


Zhao:2005:SSV

Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. In ACM [ACM05a], pages 1–6. ISBN 1-59593-269-0. LCCN ????

Zhang:2000:MCA


Zhang:2004:AIB


Zhang:2005:CHC


Zhang:2009:CII

Fangguo Zhang and Xiaofeng Chen. Cryptanalysis and improvement of an ID-based ad-hoc anonymous identification scheme
REFERENCES


Zhang:2001:SOS


Zhou:2005:PSP


Zhao:2006:SAP


Zeadally:2000:IPQ


Zunino:2005:WPE


ZF05

Zhenfeng Zhang and Dengguo Feng. Cryptanalysis of some signature schemes with message recovery. Applied Mathematics and Com-
REFERENCES


REFERENCES


Zheng:2002:NPK


Zheng:2002:ACA


Zhou:2002:MVD


Zirkind:2007:ADC

Zhang:2004:BAF


Zhang:2009:IBR


Zhang:2002:IBB


Zhang:2005:CLH


Zenner:2001:ICS

Erik Zenner, Matthias Krause, and Stefan Lucks. Improved cryptanalysis of the self-shrinking generator. Lec-
REFERENCES


REFERENCES

bibs/2384/23840203.htm;

**Zhang:1999:AFV**


**Zheng:2007:SRI**


**Zolman:2001:SEM**


**Zhang:2001:CIS**


**Zhang:2005:DMC**


**Zhou:2005:MBI**


**Zhu:2007:IHH**

transactions on Sensor Networks, 3(3):14:1–14:??, August 2007. CODEN ????
ISSN 1550-4859 (print), 1550-4867 (electronic).


Zhang:2003:FSP


Zafeiriou:2005:BRW

Stefanos Zafeiriou, Anastasios Tefas, and Ioannis Pitas. Blind robust watermarking

**ZHANG:2005:ISS**


**ZHANG:2005:SCA**


**ZHAO:2002:EII**


**ZHU:2002:PAK**


**ZHANG:2001:USC**

REFERENCES

Zhang:2004:NMS


Zhong:2008:GPT


Zhou:2003:ACN


Zhang:2005:ASP


Zhang:2005:ISM


Zhang:2008:FIC


Zhou:2003:ACN


Zhong:2008:GPT


Zhang:2005:ASP


Zhang:2005:ISM


Zhang:2008:FIC


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

