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, PCG01]. 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 [Man01]. 2^{28} [Bih02]. 2^k [MFFT05]. 2^m [KLY02, 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]. 0 [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^n) [BGK+03]. GF(p) [PZ01]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. l [QPV05]. M + 1 [AS01a]. F_q [CY02]. Z_n [Gri05]. GF(2) [GS03, KTT07]. GF(2^m) [BBGM08, KTT07, KWP06, RMH03a, RS04]. GF(2^n) [KKH03]. SL_2(F_{2^n}) [SGGB00]. μ [LN04]. n [CT08b, Gon06, HKS00, LKJL01, TM01]. N^{0.292} [BD00b]. NC^0 [AIK06]. p [FL06].
p^r q^r [LKYL00]. p^s [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]. -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 [BP04, Bih00, GIKR02, CKL+03]. 0-9 [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]. 101118-3 [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 [KSF00]. 16th [BS03]. 17th [IEE05b]. 186 [Nat00]. 186-2 [Nat00]. 18th [KM07]. 19005-1 [ISO05]. 192-bit [Luc00]. 1962 [AJ08]. 1987 [Kha05]. 1993 [PPV96]. 1999 [Lee03b, Uni00a, Uni00f, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Uni01]. 19th [BCDH09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH+00b, Eke02, Irw03, KH08, KI01a, Sch00b, Wi01, YG01c]. 2001 [ACM01a, BC01, GJS01, Lee03a]. 2002 [B+02, IEE02, RSA03a, Yun02a]. 2003 [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, WK03]. 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, Kilo1a]. 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 [LP+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].
46th [IEE05a]. 47th [IEE06]. 48th [IEE07]. 49th [IEE08]. 4th
[BCKK05, BC05b, DWML05, DRS05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, 
KN03, MS05a, NP02a].

5 [BCJ+06, Vac05]. 50th [IEE09b]. 512
[AD07, GLG+02]. 5th [CV04, KJR05, LL03, 
LLT+04, Li05, NP02a, Syv02, WKP03].

64 [LKH+08, WWCW00]. 6th [Bla03, Des02, HA00, JQ04, LL04c, MMV06, Oka00].

7 [And04, Gum04]. 7-round [Pha04]. 7.2
[TVdKB+01]. 77 [AL04]. 7th [BDZ04, Boy01, Chr00, DFPS06, PC05a, 
RS05, Sch01d, ST01d, Wri03].

8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800
[BG07a, Hir09]. 800-90 [BG07a, Hir09].

802.11b [SIR04]. 802.11g [Coc02a]. 802.15.4
[Mia08]. 82 [Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02, 
SMP+09, VY01, Vau05a, WK06, Zhe02b].

9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04].
90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1
[GM00b]. '98 [Wii09]. '99 [DN00b]. 9th
[CCMR02, CSY09, DR02c, Dку05, Lai03, 
NH03, Pat03b, PY05, YDK06].

= [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05]. A5
[BD00a, BSW01, PS01c]. A5/1
[BD00a, BSW01, PS01c]. AAFG1 [Hug02].
Aarhus [Cra05a]. Abelian
[CF02, PHK+01, RS02]. Abstention
[JLL02]. Abstract
[CM00, Cou04, DIRR05, HLvA02, HJW01, 
JL00, MSJ02, MP02, Mas04, Wag02, BJN00, 
BCDM00, CD00, CC04c, FKS+00, GHJV00, 
H04, HP01, Iwa08, IK00, Jon08, KKS00a, 
KM00, LM08, Mes00, Pei09, Yas08].

Abstracting [Bla01a, Mon03]. abstraction
[BLP06]. abstractions [BG07b]. Abstracts
[Sch00b]. Accelerating [ESG+05].
acceleration [EHKH04]. Accelerator
[CGBS01, RS04, TS00, XB01, DPT+02].
Access [ANRS01, An02c, BNPW03, 
CGMM02, MS03b, Ril02, Sma03a, Sun00a, 
ZGLX05, AW05, AW08, AF05, BA06, 
BN08, Che08b, DFM04, Hos06b, HY03, 
IT06, JW06, KNS05, LKZ+04, MF07, 
MSP+08, PS02a, STY07, WL05, WC01b].
access-control [BN08]. accessible
[Pau02a]. accountability [WABL+08].
Accounting [Lai08]. Accumulator
[GTH02]. Accumulators [CL02a].
accurate [ZY08]. Achieve [CFS01].
Achievement [Coc01a]. Achievements
[VDPK05]. achieving [PS04c]. ACISP
[YG01c]. ACM [ACM01a, ACM03a, 
ACM03b, ACM03c, ACM05b, ACM05c, 
ACM06, ACM07, ACM08. ACM09, ACM10, 
MS05b, Bar00b, FMA02, Raj06]. ACNS
[GKS05, IKA05, JYZ04, ZYH03]. acoustic
[ZZT05]. Acquiring [SETB08]. across
[ZBLvB05]. Act [Kha05, Uni00a, Uni00c, 
Uni00d, Uni00g, Uni00h]. Actel
[DV08]. Action [SE01]. Active [BC05a, BACS02, 
BP02, LJL05, MA00a, MA00b, Tad02].
Active-Content [MA00a, MA00b].
activities [AJ08, SN07]. actually [Hau06].
Ad [BSS02, KH05, W02, Ch05b, 
DHMR07, LHC08, LKZ+04, PCSM07, 
SLP07, TW07, ZC09, MAaT04].
'ad-Durayhim's [MAaT04]. Ad-hoc
[BSS02, WD02, DHMR07, ZC09].
Adaptation [ISSZ08]. Adapting [MJ01].
Adaptive
[CM00, CL08, Coc02a, CS02, CS03b, DSS01, 
EFY+05, FMY01, JMV02, KCJ+01, KLL01, 
LP01, MP05, Nov01, Pie05, ZWC02, Che07, 
DP04, MB08, WNQ08, XMST07, YZD07].
Adaptively
[AF04b, CHK05, FMY02, J00].
Adaptively-Secure [CHK05]. Adding
Addison [Puc03]. Addison [KT00, LPZ06, PP06a]. Additive [FMY01, MF01]. Additive-Sharing [FMY01]. Address [IIT03, Nik02a, Nik02b, FXAM04, RW07]. Address-Bit [IIT03]. Addressing [HTW07]. Adi [Coc03]. Adic [GHK+06]. 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, DJS05, FIP01a, GC01a, Har00, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, WFR00, YW06]. Advances [Aki09, Be00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPST07, Elv01, Ki01a, Ok00, Pi01, Pre00, TIS07, Yun02a, Kat01, Bih03, CC04a, Cra05a, Fra04, Knu02, Lai01, Lee04b, LLT+04, Li05, LST+05, Men07, Roy05, Sh05a, Zhe02b]. Advantage [SZ01]. advantages [CDS07]. adventures [Hro09]. Adversarial [CLR09, GSS08, MNS08]. Adversarial-knowledge [CLR09]. Adversaries [CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05]. Adversary [Ab00, Gor06, RW02]. AES [CGH+00b, DRS05, FIP01a, Pha04, AG01, AL00b, BDK+09, CG03, Coc02b, DR00b, DR02a, DRS05, DLP+09, DRS05, Dan01, Dra00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, IKM00, IK00, Jh00, KS09, Ke05, KFS00, KV01, LP02a, Len01, MM+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03, RY00, SKKS00, SM03b, Sch00b, SKW+00, S00a, SL00, WW00, WB00, WOL01, WWGP00, WWCW00]. AES-CBC [Fer06]. AES-like [DLP+09]. AES-related [Sch00b]. Affine [Ben00, CT09, Fel06]. Affine-Transformation-Invariant [CT09]. AFIS [Zir07]. after [Ber03, McL06]. again [Fox00]. Against [CS05a, DM07b, FKW00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Bau05, BPR00, BP02, BBN+09, BBB+02, BCP02b, CM00, CS03b, DB04, Des00b, Des00c, Egl00, EBS01, FP01, Fry00, Geb04, HNZI02, HLL+01, HG07, Hsu05b, HLC08, Ino05, ISW03, IIT03, JKS02, J00b, JT01a, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, Mit00, Mol02, MG08, NRR00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PQ03, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sen00, Sh00b, SKU+00, SKI01, SL+00, Tad02, TV03, VHP01, XH05, YJ00, YKLM02a, YKLM02b, YKLM03, ZSJD07]. Age [Mar08b, Lev01]. Agency [Aj08, Bam02]. Agent [HQ05, KC02, PJDH09, RDS01, RC01, Rot01, ZYM05, XKD00, SSM+08, SH00]. Agent-Based [HQ05, SSM+08]. Agents [WHI01, Haut06, LSA+07]. Ages [Eag05, Kin01]. Aggregate [BGLS03, WK05]. Aggregated [ZSN05]. Aggregation [Her06, CCMT09, MS09b]. Aggressive [Wly05]. AGM [Gau02]. Agreement [AAFG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB+04, AKNRT04, CYY05, Che04a, CY05, CJ04, CJL05, HWWM03, KPT04, KRY05, KHKL05, LKK03a, LKK03b, L04a, LLL04, LLL05, LKY05b, LKY05c, LKY05d, LRR02, Shi05, SW05, SC05b, Tsa06, Tse07, VK08, YY05, Y02, Y04, YRY05b, ZC04, LRR06]. agricultural [Lov01]. Aided [NS01b, HLL+02]. aim [Pau02a]. Aimed [SFDF06]. Airport [Sas07]. Ajtai [GK05]. AKS [Che03]. AI [MAaTxx, Hwa05, Irw03, KJ05, MAaT05, MAaT07, PKH05, XY04].
al-fusul [MAaT05]. al-Ka [MAaT07].
Al-Kindi [MAaT03, MAaTxx].
Al-mutargima [MAaT05].
Alan [Pet08].
Alcatraz [LSVS09].
Alchemy [Pag03].
alert [AJ08]. alerts [NCRX04].
Alexandria [MS05b].
Algebra [Cou01, CD01a, Lan04a, Fau09, HW03a, HWR09, Sho05b].
Algebraic [AK03, Bar09, CMR06, CM03, Cou01, CS05, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mai04, MN01, MR02a, MR02b, PDMS09, Bul09, CKN06, Iwa08, May09]. algebraically [RBF08].
algebras [BDFP02].
Algorithm [ANS05, AEMR09, Bar00a, Bar00c, Bi09, BSC01a, ChLYL09, CU01, CJ03a, CJS01, CTT01, CG03, CH07c, CKM00, CT03, CP03, DR01, DG00, Dhe03, EYC00, FBW01, FMS01, GM01, HTS02, HM02c, JK+01, KBD03, KMM+06, KY02c, KLB+02a, KTT07, KV01, LPZ06, MM01b, MM01c, MS02e, NMSK01, OS01, PBTW07, Ram01, RS01, SS01a, SPGQ06, WHL05, Wes01, Wie00, AJS08, App05, BF06a, Bla00, CHC01, CKY05, CYH+07, CHH01, FP09, Fer06, FSGV01, GPX08, Jon08, KJ01, Kwo02, Kwo03b, LCP04, LLLZ06a, LLLZ06b, OS07, SCS05a, SM08, SPZ02, TM01, WL02, WN95, Wie09, YRY05c, And03, SA02].
Algorithmic [Hro09, Jou09, Has01b].
Algorithms [AD07, AB09, BKL02, II00, BWBL02, CPhX04, Dun07, DW01, FW09, Gau02, GL06b, Har06, Har00, Int00, JP03, Kel05, Lee03b, LR07, LP02b, PBB02, Pre02a, SL00, TLY04, TV03, WBRF00, WWGP00, AHK03b, An01, AH05, CLK+09, CCM01, GHT05, GPC08, HW03a, HWR09, HGH06, Hro05, JKM01a, MCHN05, Pr07, Rhi03, TC05, XLMS06, ZLZS07, Zir07, dH08].
Alien [Wil01b]. All-or-Nothing [Des00c, SR00].
Alley [DR01, Wie00].
Allied [Hau03, Hau06]. Allocation [CCM05, LZ09]. Allowing [JLL02]. Almost [AP09, BS00a, Jut01, Mar02b]. Alpha [WB00, Wu02]. Alphal [KHD01]. Altera [An01c]. Alternating [Wer02, HKPR05].
Alternative [Gar03a, BW02b]. always [BB79]. am [Eko02, SU07]. Almalfi [BC05b, CGP03]. Amenability [WW00].
America [DB04]. American [GL05, Kat05b, Na05]. among [BN00a, KT00, SKU+00, Win05c].
Amplification [CHS05, LTW05, RK05, SV08b]. Amplified [KK00a, KKS01, KML+02]. Amplifier [Pli01]. Amsterdam [Knu02]. Analyses [BPR05, Des00a].
Analysis [ARJ08, ABR01, AKS06, AD07, An01, AIC+01, ARC+01, Av03, BN00a, BDhKB09, BRS02, BF05, Bor01, BSL02, Cry00, CK02a, CS03b, DPV01, Dra00, FL01a, FGM00a, Gir06, Gol01c, GHT05, GL+02, GPR06, HSS01, HKR01, HSS04, Hey03, HM02c, IIT03, JK01a, JQYY01, JT01a, JQYY01, hKLS00, KMS02, LC03, LKH09, LY05, LWK00, LH07, MOP06, Mar02b, Mas04, MS01, MMT09, Mea01, Mes00, Mes01, MAaTxx, MG08, NP02b, NSS02, OS06, ÖP003, Puc03, QS01, SSS06, Shao11c, Sma03b, SQ01, SWT07, YSS+01, ZC00, ZGLX05, AvdH00, AW05, AW08, Abd01, AHK03b, BSV08, BBK+03b, Bjo05, BG07a, BCJ+06, CLK+09, CW07, DKS08, GW08, GM04, Has01b, Hir09, Hro05, Hut01, JEZ04, JWS05, KSF00, Kor09, LKH+08, LW05, LW05a, LKJL01, Lu07, Mea04, MT07, MRST06, OS00].
analysis [PSG+09, PS08b, SK01b, WLT05a, WPP05, XH05, XMST07, YCW+08, YC08, ZWWL01, ZL04c, ZDW06].
Analytic [Shp03, Nie04]. Analyzing [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04].
anatomy [Bam02]. Anchor [Ree01].
Ancient [Imr03, Sin00, Mol05, Pin06].
Andrei [Puz04]. Andrew [Puz04].
Anguilla [Fra01]. Anniversary [Sal01b, Coc02a]. annotated [Pet08].
annoyances [Tyn05]. annoying [Tyn05].

Annual [ACM01a, ACM02, ACM04b, ACM05c, ACM06, ACM07, ACM08, Bon03, Cra05a, ELYS01, Fra04, IEEE02, IEEE03, IEEE04, IEEE05a, IEEE06, IEEE07, IEEE08, IEEE09b, Kil01a, MZ04, Men07, Sh05a, 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, LHL+08, SOOI02, Wan04a, YT09, ZJ09, BP03a, EY09, LHC08, Sae02, Sha03c, WJC05, YTWY05, ZC09]. ANSI [III00, Kel05, 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 [Ke05]. Applet [ZFK04]. applets [Bis03a]. Applicability [Wya02, TM01]. Application [AD09, ACS02, Bai01b, Boy01, CL02a, CKQ03, Dam07, Dhe03, GHK+06, HF00, IKP+07, JX05, Jou04, Lai03, Lee04b, LLS05b, LXM+05, NP07, Oka00, PFI01, PQ03, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TWNA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG09, CMKT00, CP07, DIM08, FP00, JRS05, Lax09, MT07, MPH06, MK05a, RSS04, SSST06, TC00]. Application-Aware [IKP+07].

Applications [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, BJ05a, BGK+03, BS00a, Bih03, BGOY08, BSS02, BL08, CC04a, CD00, CV02, CGHG01, C205, CHSS02, CSY09, Cra05a, CD015, DJ01, DK02, DK07, DA03, DFPS06, FR02, GSS08, GKK+09, GJKR03, Gen04a, GRW06, Gol01a, Gol04, HRS02, HO06, Har06, Has01a, HSS04, HR05, HJW05, JT01b, JY01, KMM+06, KGL04, KMO01, KBM09, KKIM01, Knu02, MM07b, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Sh03, SXY01, SPGQ06, Vau02, Wya02, XYL09, YZ00, Zee0a, Zho02, ACTZ05, Ate04, AH05, AFHG06, BG08, BGL+03, CCCC01, CM05b, CS09, CHK+08, DY09a, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gal02, GCC+08, GKK+07, GB09, HHS01, Has02, Hen01, HKPR05, Jac00, KV+09, KNS05, Lao00, Lee04a, LJ05a]. applications [LPW06, LB05, MY01, Mal06, MC04, MS04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SSS06, 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, SPMLS02, vDKST06]. Appointed [CL01a]. apprehension [AJ08]. Approach [BKM07, CEGSHG09, CDR01, CW09, CB01, DJLT01, Kra03, Lai07, LL05c, Lut03, OMT02, PBD00, Pan02a, Pre02a, SKG09, VH09, VVS01, Virt03, XYL09, YKMB08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLM05, GGH+08, Har05a, JJ01, JW01, LYC02, MT09, Mar05b, MI09, Mos06, NN03, SLP07, SN04, SW00b, ZLX99, ZSZ01, ZL04b, ZL04a]. Approaches [CGMM02, AvdH00, DGO5, Has01b, KXD00]. approval [Wan04b]. Approximation [CL02, Kuk01, WL02]. Approximations [BDQ04]. Apress [Ter08]. April [An00b, Buc00a, Chr00, Chr01, CCMMR02, CCMMR05, CGH+00b, DFPS06, Joy03b, Knu02, Mat02, NIS00, Nac01, Sch01d, SMP+09, YDKM06]. APSS [ZSV05]. Arabic [MAaTxx]. 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, LKM05, DHL06, Ino05, LHL03b, MPP09, SKW07, SHL07, SH05, Tan01, WWA01].

Architectures [BGK+03, KLY02, RM02, SM02, Con04, DP04, GKS05, NdM04, RH00, LZ04, LXM05, Lut02, MP01c, MFS09, Rot02a, SMT01, SM03b, SLG+05, Uzu04, Che00, CC05e, DHL06, Ino05, LHL03b, MPP09, SKW07, SHL07, SH05, Tan01, WWA01].

Archival [SGMV09]. Archives [RC01].

Archiving [DMSW09]. area [BP03a, Cal00c]. Areas [HH04, MZ04, PT06, VY01, AMW07, Buc00a, HH05, HA00, NH03, ST01d]. Aren’t [Bau01a, Bau01b]. Arguments [HNO+09]. ARITH [BS03, IE05b]. ARITH-15 [BC01]. ARITH-16 [BS03]. ARITH-17 [IE05b].

Arithmetic [BS03, BCDH09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDJ+01, SR06, GFS05, PS04a, SOIG07].

arithmetics [Lam91]. ARM7 [DV08, XB01]. Army [Boy03]. Arne [Bec02]. array [DZL01]. Arrays [ABM08, BS00a, GC01a, HW05, PP06a].

Arrived [Law05]. arsenal [Blu09]. Art [And07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Er03, Er08, MS02d].

Article [Che08b]. Artifacts [EHK+03].

Artificial [Cur04b, MMY02]. Arun [For04]. ASCII [MJ001]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DN00b, KL01a]. ASCII [WOL01].

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

Aspiration [Ash03]. assembly [Gou09]. assessing [CDD+05]. assessment [CC05e, DMS07]. assets [KH03, NRR00]. Assignment [BRTM09, CHC04, DFM04, Hwa00, TP07, WC01b, yY08]. assignments [SWR05]. Assisted [ECG+07, X03, BB05, LHL04]. ASSL [VH09]. associated [XLM06].

associativity [HR08]. Assumption [CS00, DN00a, FOPS01, KMZ03, ZD05].

Assumptions [ABR01, BP04, BCP2a, FS01a, KLR09, Lin03, MNT+00, Na0a, SB02, Mi02a].

Assurance [LXM+05, AL04, BJ02, FOP06, Gha07, Jen09]. Assurances [Bar06b].

Astrology [Pag03]. Astronomy [MYC01].

Asymmetric [CH07b, Man01, SY01a, SB02, WH01, YG01a, Lee01, OP01b].

Asymptotically [vDW04]. Asynchronous [CKPS01, FML+03, KSR02, SKR02, ZSV05].

at-targama [MAaT05]. Atlanta [IE09b].

ATM [Pat02a, Pat02b, Zea00]. Atomic [CN06].

Attached [RCB00].

Attachments [Ric07]. Attack [Ahm08, CKQ03, CS05a, CS03b, Des00b, Fil00, FV03, GHJV00, GHJV01, HQ01, Hug02, HW01, J006, KPC01, KS00a, KML+02, KM01c, LY07, LNL+08, LV04, LMV05, Luc02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, PQ03, RMS05, SGM09, Sch01b, Sho0b, Sma03b, VHP01, YKLM02a, ZC04, ASK05, DKL+00a, Dj08, Du09, GM00a, HA04, Hes04b, HG07, Iwa08, J002, KS09, KM04a, LM08, Law09b, LS05b, Mir05, OS00, SI04, XH05].

Attack-Resistant [LNL+08]. attacker [BDSV08]. Attackers [JMV02].

Attacking [FMP03, KPR03, Lue00, TMM05, BF06a].

Attacking-Based [TMM05].

Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, MMP00, BBB+02, BD+09, BU02, BM03b, BCP2b, BM01c, Can06b, CS07b, CT08a, CJS01, CM00, CJNP00, CM03, Con03, CWR09, CD01b, DP01, DFS04, DS08, DM07b, FKSW00, FOHB05, FP01, Fry00, Fur02b, Gen04a, Gir06, G02, HSH+08a, HNZI02, HR04a, HSH+01, HLC08, ISW03, JKS02, J006d, KKS00a, KSS0b, KKS01, KCJ+01, KL01a, Law09a,
LLS05a, LWS05, LJ05b, MOP06, MP06, MF01, Mes00, Mes01, Möl02, MG08, OT03a, OT03b, [OOP03, OST05, Ove06, PKB01, PDMS09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZZ05, YYDO01, YY01, YG01b, vW01, Bau05, BZ03, CKL +09, DK08, Geb04, HSH +08b, HSH +09, HAS01, Hsu05b, HL05b, Ino05, IM06, JDJ01, KS05a, KTC03, LPV +09, 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 [RCG +05].

Auctions [Bra01b]. Audio [Arn01, CS05b, MH05, WNY09, WWL +02, XF02, WNQ08, BS01b, KJR05, KN03].

Audio- [KJR05]. Audio-and [BS01b, KN03].

Augmented [CS07c, You01]. Augmenting [AL04].

August [AMW07, Bel00, B +02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KKP02, Ki01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch04b, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a].

Australia [Boy01, IZ00]. Austria [DKU05, P601, Je08].

Authentic [Dur01, SS01b]. Authenticate [Bau03a, Bau03b].

Authenticated [AGT01, BN00a, BPR00, BU02, BC04b, BMN01, BMP00, BCP01, CPP04, Ch08, DG03, DA03, EP02, GKK07, GL03, GTTC03, HS07, KOY01, KY03, Kra03, Lee01, LH09, MPS00, Mac01, MS02, MND +04, NA07, Nam02, Ngu05, SK00, Van05b, WCY02, BKN04, BCP07, CYY05, Ck04a, CLC08, CJ04, CJL05, GL06a, GMR05, HT08, HWW02, HWW03, Hsu05a, Hwa05, HL05c, HL05d, KOY09, KRY05, LKKY03a, LKKY03b, LL04a, LL05a, LKY05c, LKY05d, LHC08, LLR02, LLR06, LHK05a, Mi08, RB03, Sei05, SW05, SC05b, TLH05, TJ01a, Tse07, WH02a, XY04, YW05, YC09, YS02, YRY05b, YPKL08, ZC04, ZAX05, ZW05b, ZL05].

Authenticating [AIP01, CGV09, JW05, PM08, RCC00, YSS +01, Lin01a].

Authentication [AAK09, AP09, ANRES01, Ano01b, Ano01c, Ano01e, Ano02b, AHKM02, ANL01, BH06, BACS02, BCL +05b, BCG +02, BM03a, BH00a, BCC01, BDK09, BR02, BDFP05, BDF01b, BL02, BLDT09, BRE +00, CV03, CS07b, CLK01a, CLK01b, CC05b, CJ03c, CW05, CT09, Cim02, Cir01, CGK +02, CJK +04, Cou01, CMB +05, DP00, Dwo03, ETZ00, EM03, FIP02a, FM06b, Fr03, FSS01, Gan01a, Gar03a, GM07, GSV02, GD02, GT02, Had00, HZ01, HSH02, HSH06, HKW06, HY01, Hac01, HS01, HL07, ISS08, Jab01, JP02a, JP02b, KJR05, KH05, Kha01, Ku02, KZ09, Law05, Li01, LLT +04, LB04, LL05c, LSH03b, LM00, LHL +08, Lys07, MM01a, Mal02, MJ04, MD04, JR03, MG02, MN06, Nao02, Nik02a, Nik02b, OKE02, OHH08, PBDD0, Par04, PBC05, PK01, Qu01, RIK02, Ric07, Ri02, SNWX01, SR01].

Authentication [Sch04c, Sch05b, Sei00b, SY01b, SBG02, Smi01c, Smi02, SE09, SK06, Str01b, SJ05, SYL05, SC01, TK03, T309a, T309b, Ts01, VN04, WLLL09, Way01, Way02, Wei06, WKB08, WT02, WS03, WLT05b, XYL09, Y101, YEP +06, YSR01, YLL02, YKW01, ZJ04, ZBL05, Abd01, AF04a, All06, AAKD09, AL04, Be04, BGP02, BFG04, BFG05, BS01b, BBG +02, BDFP02, Cer04a, CC01, CCK04a, CL04d, CC04b, CCK04b, CC05c, CY05, CSS08, CWJ01, CT01, CJ03b, CH07a, CL09, Coc01a, CMD06, Da01, DY09a, DG05, DW05, FGM03, Gan08, GLC +04, GS09, GUQ01, HM02a, Hsu05b, HYS03, HLL04, HL05b, KLY03, KJ05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LL02,
Miy01, MGC02, Mül01a, MSU05, NM005, Nak01, Nam02, NBO01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP06a, Ril02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sal05b, Sch01a, SSFC09, Sha02, Sha01c, SO0I02, SXY01, Sma03a, SBEW01, SGB01, TMMM05, TYZ09a, TYZ09b, VMSV05, Vau05b, Ver06a, VHP01, VK07, WRW02, WY02, WZW05, WG05, WH09, WBD01, XYL09, YKMY01, YT09, YYYG01, YSS+01, YKW01, YLH05, ZK02, ZG05, ZP05, ZJ09, ZS05, ZWXY02, vDW04, App05, AAKD09, BGB09, BR04, BFG08, BS01b, Bla01b, BMW05, BLP06, BGL03, BDS09b, Buh06, CGHG06, CL02b, CL04d, CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CJL05, Cho08b, CYH07, CFVZ06, CCD04, CTT07, CHT02, CC04c, Cra05b, DPT02, [DHL06, DV08, DW01, EHKH04, FXAM04, FWL08, GM08, GLO6a, GHGSS00, GS01, GPS05, GB09, HM00, HLL+02, HCD08a, HCD08b, HRL09, Has00, Her07, HPS01, HG05a, Hsu05a, HLWZ09, Hui00, HP01, HLL03, HLO5d, IM06, JK01a, JK01b, JW06, JZCW05, JLL01, KG09, hKLS00, KLY03, KPT04, KN03, KHL09, KWW0, KNS05, KCL03, Ku04, KCC05, Kwo03a, KHKL05, LHL03a, LF03, LKY05a, LKY05b, LHY05, LD01, LTH05, LPM05, LW05a, LWZH05, LYGL07, LLW08a, LLW08b, LCC05, LCS+07, LCZ05c, LCZ05a, LLC06a, LLC06b, Mic01, MR09, MI09, Mit00, MB08, MO04, MPP03, MV03b, NZCG05, NC09, NSNK05, OS09, PCSM07, PW05, PBMB01, PSC09, PS08a, Pel06, PSP+08, PC00, PLJ05a, PLJ05b, QCB05a, Reg03, Reg04, RG09, RGC+05, Sax02, SGO7, SCo04, Sci05, SPG02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SCS05a, mSgtL05]. based [SSM+08, SW05, SH00, SK01b, SCL05, SLC05, Sun02, SCS05c, TWNA08, Tsa05, UHA+09, UBE09, V801, VKS09, WAF00, WL07, WJP07, WNQ08, WLHH05, WV00, WH02b, WY05, XMST07, YW04, YCW+08, YS04, hY08, JY00, YPSZ01, YRY05c, YPKL08, YYY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRMS05]. Bases [AAC+01, ADDS06, BKP09, B+02, CvTMH01, EBC+00, FJ03, FLA+03, CCT08, Fau09, ZT03]. Basic [Go01b, Go01a, Go04, Kat05b, Puc03, Ste02, Bon00]. Basics [Leh06, Lut02]. Basing [BPR08, CHL02, AGGM06, AGGM10]. Bases [RMH03b, V03, GPS05, LS05b, RMH03a]. Batch [Ara02, HLT01, PB07, Shao1d, BLH06, HL00]. Batching [SB01]. Battery [CBSU06]. Battle [Bud00a, Bud02, SM00c, SM05]. Bay [Cal00c]. Bayes [Goo00]. BC [IEE02]. BCH [MLC01]. BDD [Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pau02a, CNPQ03, YJ000, vT01]. Beach [IEE00a]. beat [Lev01]. because [AJO8]. Become [Ort00]. Been [Nic01]. BeepBeep [Dri02]. before [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YJ000]. Beginning [Dew08, Hoo05]. Beginnings [Bud00b]. Begins [MP00]. Behavior [Vav03]. BEHEMOTH [Bar00c]. Beijing [FLY06, LST+05]. Being [ASW+01, ES00a]. beleid [dL00]. Belgium [DR02c, Pre00, QS00]. Belief [BPST02]. believing [Buh06]. Bell [BZ02, Eke02]. Benchmark [TLYL04, LDH06, YLT06]. Bendy [Sas07]. Benefit [YKLM02a]. benefits [CH00]. Benford [NM09]. Bergen [Yr06]. Berkeley [IEE06]. Berlin [FLA+03]. Bermuda [Bl03]. Bernard [DN05]. Berners [Coc02b]. Berners-Lee [Coc02b]. Best [Ban01a, Ban01b, MFS+09, Go08, Ste02]. BestCrypt [Ban02b]. Bethesda [ACM09]. Better [V03, PM00, RR02, SKQ01, HL00, Pau03]. BetterBASIC [ASW+01]. Between [DKMR05, Ket06, Ngu05, NN06, Fau09].
GKM+00, GC05, MSV04, RW03a, SK06.

Beurling [Bec02]. Beyond [Gor06, LWM05, Mar08a, Sch03, See04, Sty04], BGP [ZSM05, vOWK07], Bi [Cou04, PJK01]. Bi-directional [PJK01]. Bi-linear [Cou04]. Bias [CL02c, Scl00]. 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, Da01, EM03, HWH01, KJR05, LLT+04, SR01, Sase07, WS01a, Wea06, BS01b, KN03, Li05, LST+05, MR00, MJ04, TB01, ZJ04]. Biometrics [Ash03, Bjo05, JR03, Ril02, Str01a, BCP03, Buh06]. Biometrics-Based [Ril02]. Biomolecular [Bi09]. Birds [MLM03]. Birth [SE01]. Birthday [Wag02]. Bismulation [BJP02]. Bit [AIK+01, BK06a, BL08, CGH01, CDL+00, DMS00, GS07a, IIT03, KZ07, LNS02, MS09e, PCC01, RMH03b, SM03b, SXY01, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, Pri00, RPM08, SWR05, UHA+09, WW08, ZFK04]. Bit-Fixing [KZ07, KZ03]. bit-substitution [GPX08]. BitLocke [Kor09]. Bits [BS01d, SZ01, HN04, Shp02]. Bitslice [DPV01]. Black [ANO1g, CF02, CFS05, DI05, DIRR05, DSO8, KYO1d]. Black-Box [ANO1g, BRS02, CF02, CFS05, DI05, DIRR05, KY01d]. Blackmailing [PS01b]. Bletchley [Sal00b, Cop05, Cop06, Sal05a, SE01, Sni01b, Win00]. Blind [AO00, BNPS02, BB00a, BSC01b, CL01b, JKK+01, LY07, Na05, Pau02b, SPK08, ZTP05, ZK02, Fan03, HC04a, JLL01, JL04, LHY05, LC05b, MS09a, SV08a, SHT05, WHH05, ZC05]. blindness [AvdH00]. Blink [Sas07]. Block [AIK+01, BRS02, BR02, BSC01a, CvT01]. Can01b, CLL00, CP02, CMB+05, Cro01, DR00a, Dwo03, EYCP00, Fhu02a, HSH+01, JKK+01, KCP01, KYHC01, KKG03, LRW02, MV00, MS02e, NPV01, OMSK01, Pat01, PS06, Pli01, RMO05, SM03b, SY0+02, SKU+00, SK10, XH03, YG01b, Bai08, BF06a, DY01, Dua06, Egh00, GPX08, Hey03, JKK+01, Jun05, Kat05a, KJ01, LDH06, LCP04, LH0+08, MJM05, PSP0+08, RBB03, SHJ04, SHH07, WF02, XH05, YI00]. Block-Cipher [BR02, RBB03]. Block-Cipher-Based [RBB03]. Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. blockciphers [Fur01]. Blocks [Jon02]. Blockwise [JMV02]. Blockwise-Adaptive [JMV02]. Bluetooth [GMBO, LV04, LMV05]. Blunders [Bra01]. Blur [VHP01]. Blur/Deblur [VHP01]. Blurring [LSK05, SK06]. Board [CBGS01]. boat [DB04]. Body [Bam02, TG07]. BOEL [Fm02]. Boethius [Eag05]. bombe [Wil01a, Tur04]. Bombes [Ame02e]. bombs [Lov01]. Bonds [CAC03]. Boneh [ASK05, Hes04a]. Bonn [DSS05]. Book [An04, Du05, Eaw05, Fal07, For04, Gas01, Gum04, Imr03, Irw03, Jan08, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Re01, Rot07, Sal03b, See04, Shp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wal00, Was08a, Kat05b, Lam07, Lun09, MAaT05, Sin09, Sin00, AAG+00]. Books [Dr.00c, Ree01]. Bookshelf [Lut02, Lut03, Wil01b]. Bookworm [Sal03b]. Boolean [Car02, CT03, CS09, MS02b, QPV05, SM00a, SM00b, SM03a, VW00]. 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, bY08, GW00]. Boundaries [PGT07].
Bounding [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vad03, DFFS05].
Bounding-Quantum-Storage [DFSS08].
Bounded [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vad03, DFFS05].
Bounded-Quantum-Storage [DFSS08].
Bounding [DM07b].
Bounds [BDF01b, BP03b, DIRR05, Di 01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKK03, JZ09, PS02a, Shp99].
Bouwmeester [Duw03].
Boxes [Bih00, BCDM00, ZC00].
Braille [Pau02b].
Branches [Fel06].
Break [BP06, Sin02, HM04, WA06].
Breaker [Rey01].
Breathing [BP06, Sin02, HM04, WA06].
Breach [Os00].
Bright [Ano01g, LNP02].
Brilliant [Ano01g, LNP02].
Brissac-Quercy [Pre00].
Broken [Ahm08].
Broken [Ahm08].
Browsers [Bar00b].
Bruce [Sty04, See04].
Bruges [Pre00].
Brumley [ASK05].
Brute [Cur05, SGA07].
Brutus [CJM00].
BSD [Lin02, ASW+01, Lin02].
BSEDCON [USE02a].
Budd [Ber03].
Buchmann [Lec03a].
Buffer [FOBH05, Fry00, Ino05].
bug [Bo00].
bugs [GJL06].
Building [Jou02, Kmu07, Mar02a, And08, Bra01a, FB01, LS05b, MG06, MPH06, DB04].
buitenlands [dL00].
Bulletin [Cer04b].
Bulletproof [Cha05b]. bundles [GT02].
Burrows [ABM08].
Bush [Ris06].
business [HHH01].
Buy [PLW07].
Buyer [MM01a].
Buzzaes [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]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].

Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b].

Cannes [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [III00, EYCP00, NIS00, SKW00].
[AFI06, BGW05, BGN05, Gen04b, JJ00a].
Circuit [EHK+03, GSS08, HR05, MG08].
Circuits [BI05a, FML+03, Gol03, ISW03, MD05, PTB07, 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, HTJ09, Lam07, LS01, YS04].
Client-Server [ANRS01, PS05].
Client-to-client [HTJ09].
Clients [JRFH01, RKZD02].
Clip [FGL02].
clock [Pau02b].
Clock [CGFSHG09, MH04].
Close [DM07b].
closing [Lau08b, PWGP03].
cloud [CKS09].
Clouds [GS01, VS01].
Cluster [Hö01, KCD07, SEF+06, TLC06, TW07].
Cluster-Based [KCD07].
Clusters [MFS+09].
CM [CMKT00, GHK+06].
CMS [WBWL02, DUK05].
Co [Bud00b, Nd05, ACM01b].
Co-Design [Nd05].
Co-operation [Bud00b].
Coalition [ACJT00].
Coalition-Resistant [ACJT00].
coarse [Rhi03].
Coast [Boy01].
Cod [IEE05b].
Code [Ark05, BR04, CV03, Cer04b, FIP02a, FF01b, HSZ01, Im03, KY01e, Lai08, OS09, Re01, Rey01, Sal00a, Sin02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MMD05, 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].
code [Che08a].
Coded [MLC01].
Codes [Bec05, BP06, Big08, Bod99, BQR01, Chu02, CDG+05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, YY02, YDD001, Yek07, Be07, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HWR09, Lam07, Lam09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02].
codeword [AJ08].
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 [HSH+08a, AJ08, HSH+08b, HSH+09].
cold-boot [HSH+08b, HSH+09].
collaboration [ED03, PCSM07, SBG05, SBG07].
collapse [SBB05].
Collection [GMM08, Bro05a].
Collections [Kuh00].
Collective [BBB+02].
collide [GPN05].
Collision [DG02, IK005, WYY05a, WYY05d, GM00a, Sem00].
Collision-Resistant [IK005].
Collisions [BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c].
Collusion [BGW05, HNZI02, Zan01].
Cologne [WKP03].
Color [Che07, Che08a, FGD01, AEEdR05, CDD07, Yan02, YCL07].
Colorado [BC01, Sch04b, USE00d].
Colored [CDD07].
Colossus [Cop04a, Cop05, Cop06, Lav06, Sal00b, Sal00a, Sal05a, Salxx].
Colour [RS00].
Coloured [AADK05].
Columbia [ACM08].
column [Raj06].
Combination [CF01b, Gau02, GHPT05, GB09].
Combinatorial [GW05, 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 [DN02b, DMS00, FF00, CAC06, HR07, KKL09]. Commitments [BN00b, 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]. communicating [DN00a, Nie02b]. commodity [CGL +08a, CGL +08b, CGL +08c]. Common [Pas03, TG07]. Communication-Efficient [Fis05]. Communications [GN06, HJ07, Igl02, Kra01, Lan00a, Lan04b, LCK01, LL01, MS05b, Sal01b, Vao05b, VMC02, BP03a, CYH04, HW002, LC04a, Sal05c, Ser06, SL05a, Wil99, WGL00, YTW05, YK05]. Community [SK06]. commutativity [HRS08]. commuting [CKRT08]. Compact [CG03, JT01b, SMTM01, Y09, ZL02, JAW +00, Mic02a]. Company [ASW +01]. Comparative [DPR01, GLG +02, Kat05b]. Comparing [HU05]. Comparison [GC00a, GC01a, Gao02, JRB +06, MS02e, SW00a, WW00, FGM03, JL03, Sma01, WB00]. Compendium [Lut02]. Compensated [AAK09]. competition [Cha00b]. compiler [DFG00, Oiw09]. Compilers [Lut02]. Complementary [AS01c]. Complete [Bar00a, Bee05, Bud00a, FGMO01, GCKL08, HMS04, KY00, MS09c, Sal07, TWW +09, Bud02]. Completeness [HG03, PT08]. Complex [JKK +01, LKL05]. Complexity [BYJK08, BLM01, BDK +09, CKRT08, CB01, DN00a, FBW01, GKKO07, GKK +09, HR04a, Lut02, Nie02b, RMH03b, Ross00, Rot05, Shp03, BYJK04, CDD00, GKK +07, GIKR01, Gor05, JZ09, Mic02a, MP08, RMH03a, Rot02b, Rot03, Shp99, SPHH06, TW06, SV08a, Far07, Rot07]. Complexity-Theoretic [CB01]. compliance [LMW05]. Compliant [CGBS01, RV09]. Component [BSL02, Hei01, TEM +01]. composability [PS04]. Composable [AF04b, BOHL +05, BLDT09, CF01a, CDD02, DN02b, DN03, NMO05, RK05, Can01a, CLO02]. Composite [CQS01, GMP01a, RDJ +01, Zhe01]. Composition [BJP02, BN00a, CR03, CV02, Pie05, Sho00a, Can06a, LWR02, LRR06, Puc06]. compositional [GM04]. Compostela [BS03]. Compound [SB05]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, HS00, Ke02, LHS05, RS08, Sal07, SDFH00, WWL +02, FS08, Gar04, Lai00, L05a, Sch00a, Sch01c, S +03, Sch04a, Sch04b, Sch05a, TT00, Zir07]. Compression-Encryption-Hiding [BD03]. Compromise [Ahm08, Lai08]. Compromised [ZYN08]. computability [Pet08]. Computable [Vad03]. Computation [ACS02, Bai01b, BCL +05b, Bl05a, BIM00, BJLS02, CC00, CD00, CDN01, CDG +05, CD05, DN03, D105, DM00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HMO1b, Jf08, KO04, KLML05, KSR02, Lin01b, PS05, WW05, A020d, AB09, BEZ00, BEZ01, CLO02, CLO08, CDD00,
DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WLHH05, WY05, SM07, Dw03, Computation-efficient [CLC08].

Computational [DLP+09, GH02, KLR09, KK06, Rup09, SM07, WvD02, AUW01, IKOS08, Lam01, Lau08a, Nie02a, Sho05b, SHJR04].

Computationally [MPSW05].

Computations [HL05a, ML05, RMH04, SBZ04, TC05].

Compute [MFS+09, FBW01].

Computer [BS03, Bis03b, BCDH09, BC01, CSW+08, CZK05, CGK+02, Coo02a, Coo03, HYZ05b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Ir00, JBR05, KM07, Le06, Lut02, MYC01, MS05b, Mac03, Nie02d, RC06, SB07, Tyn05, Cas02, DFGH04, Fan09, FOP06, GKS05, Lov01, Mal06, PR04, PS03, Sal05c, Sal05d, Sch06, SL06, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coo03].

computerized [LMC+03, Pau02b].

Computers [Coo03, Ett02, TSS+03, Cop05, Cop06, RH00].

Computing [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBDK00, CGH00a, CLK01a, Cop04b, EP02, JP03, LP03, LKHL09, Lut03, May04, PM03, Sch06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Yan00, YKMB08, Cha07, Che05b, CHT02, DHL06, HV09, HKPR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sei05, Wil99, YLR05, Lut03].

Compumware [An02b, concea [BB79], Concealing [DMS00], Concealment [DA03], Concept [ARC+01], concepts [AB09, Kra07, SWR05, MC04], concerning [HW03b], Concerns [MP00], concrete [KN05].

Concurrent [BP02, DPV04, Gen04a, KKG03, Ros00, Ros06a, Dam00].

Conditional [LMV05, WN02].

Conditions [IKO05].

Conference [ACM03a, ACM04a, Ano06a, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bla03, Bon03, Boy01, Bu00a, CC04a, CV04, CGP03, CGH+00b, Cra05a, DUK05, DFCW00, DFPS06, EBC+00, Elv01, FLY06, Fra01, FMA02, Fra04, FLA+03, HR06, HYZ05b, IEE09a, IY05, JY04, JM03, Joy03b, Jue04, KJR05, Kil01a, Kim02, KN03, Knt02, Lai03, LL03, Lee04b, LL+04, LL04c, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Nac01, Nao01, Oka00, Oka04, Pat03b, Pfi01, Poi06, Pre00, Pre02b, RD01, Roy00a, Roy05, Sho05a, Sil01, SM07, Sma05, Syv02, USE00c, USE00a, USE01b, USE01a, USE02c, Wil99, Won01, Wun03, Yun02a, YDKM06, ZJ04, Zhe02b, ZHY03, AUW01, BC05b, DV05, DWML05, DRS05, Hon01, Kil05, Lit05, PC05a, PY05, PPV96, Q500, Son00, WK06].

Confidences [Gan01a].

Confidentiality [Dwo03, YC08].

configurable [MBS04].

Configuration [Shu02, Mos06].

Confirmation [SK00].

Confirmmer [CM00, GM03].

Confiscation [RB01].

Conformance [LB00, RSA00c].

conflated [Bel07].

confusion [She01].

congestion [SSB05].

Congress [Uni00a].

congruences [Ste08].

Congruential [CS05a, LS05a, SB05].

conic [LCC05, LCZ05a].

Conjecture [CU01].

Conjugacy [CJ03a].

Conjugate [Ig02].

Connected [BJLS02, Ho01].

Connection [HR00, Jam00, Goo00, Mic02b].

Connection-Polynomials [Jam00].

Connections [WRW02].

Conquer [SKQ01].

conscious [DMSW09].

Consensus [CNV06].

Considerations [DWS+06, Hei07, Rub01, Sch07, SVEG09].

Considering [WA07].

Consistency [ABC+05, JZ04].

Constant [App07, BL05a, CS07c, CD01a, DPV04].
DN02b, DI05, Lin01b, Sun00a, IKOS08].
Constant-Depth [BI05a].
Constant-Round [DPV04, DI05, Lin01b].
Constrained [BCH^00, DBS^06, HS01, MRL^02, Zhe02a, Has06, 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, BRS02, GMW05, GGKT05, GM02c, Jou04, PR08, PZ02b, SNWX01, SM00b, GT00, GPV08, IK03, NR04, PR05, Reg03, Reg04, vDKST06].
constructive [GGH^08].
consumption [Miˇs08].
Contact [YKMY01, Car00].
Contact-Less [YKMY01].
Contactless [And04, KS02, Cla00b, Fin03].
Contemporary [Ahm07, Opp05, SVEG09].
Content [AAK09, CGJ^02, HHJS04, MA00a, MA00b, RE02, XMST07, YKW01, ATS04, DY09a, SG07].
Content-adaptive [XMST07].
Content-Based [RE02, YKW01, SG07].
Content-triggered [HHJS04].
Context [Bar00b].
Context [DJLT01, FPS01, SN04].
continue [Lov01].
continued [Dan02].
Contr [WK05].
Contrast [BDDS03, HKS00, HT06, KOS03, CDFM05].
Contrast-optimal [HKS00].
Contrast-Sensitive [HT06].
Control [ABEL05, ANRS01, BW07, CGMM02, LY05, Sma03a, ZGLX05, BN08, DFMO4, DPT^+02, JW06, KNS05, LZK^+04, MD04, MSP^+08, PS04b, ST07, WC01b].
Control-flow [ABEL05].
Controlled [GVC^08, IMM01, AW05, AW08, LAPS08].
Controlling [HY03, MS03b, MS02d, WL05].
Controls [Har01a, Har01b].
conventional [CJ04, YW05, YRY05b].
Conversation [GK04].
conversations [VAVY09].
Conversion [CDI05, Ketz06].
Conversions [KI01b].
Convertible [Chi08, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b].
Convolution [PG05].
cookbook [VM03].
cookies [Cha05a].
Cool [Ano00b].
Coordinate [OS01].
COPACOBANA [GKN^08].
Copenhagen [TBJ02].
Copley [USE01b, USE01a].
coprocessing [ML05].
Coprocessor [Gut00, It00, LS01b, OTIT01, AV04].
Coprocessors [Smi02].
Copy [LTM^+00].
copying [SV08a].
Copyright [Kha05, LLL02, PBB02, XFZ01, ZTP05, Gil07, Kwo03a].
CORBA [TEM^+01].
Core [BF00a, Dim07, DV08, HMS04, TPS01].
Corfu [SM07].
Corner [Mar08a, TR09a, TR09b].
corners [Bhu09].
Corporate [HW01, KH03].
Correcting [MZ02, NN06, YYDO01, ZYR01].
Correction [BQR01, CTBA^+01, Dim05, LN08, LW05b, MPSW05, TEM^+01, Gar04].
Correctness [PBD05, HSD^+05, DHO8].
Correlated [FWW04].
Correlation [BSC01b, CJS01, Gol01c, JJ00d, LV04, LM05, MH04, Nyb01, SY01a, WRW02, ZCO0, GG05b, JJJ02a].
Correlations [KM00, KM01b].
corruption [XKN^+05].
COS [FF01a, WB02].
Cost [CDF01, FBW01, PD07, Sta05, YEP^+06, CL09, SHJR04, YLR05].
Cost-Effective [PD07].
cost-ineffectiveness [YLR05].
could [Cla00b, Pau02a].
Counter [DIS02, QS01, SLG^+05, SL06, MM05].
Counter-Measures [QS01].
Countering [PP06b, SK05b].
Countermeasure [IT03, MMMT09, OT03a, PKBD01, YKLM02a].
Countermeasures [Av03, Fry00, GM00b, MOP06, OST05, Has01b, JDJ01, Man08, OST06].
Counters [KMO01].
counterterrorism [Naf05].
Counting [Gau02, Hig08].
Coupe [SXY01].
coupled [LF03].
course [AA04b, GV09, GL05].
courses [Gha07].
Cover [GA05, Gut02a, LNP02, NN03, RS00].
coverings [SC02b].
Cover [Col03].
Covert [ECG+07].
CPCMS [Sha02].
CPI [EG+07].
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, Spr03, SGPH98].
Creation [MV01, Top02, KB08].
Creator [Coc01a].
Credentials [CL02a, CL04a, LLW05, LLW09].
Credit [CBN+02].
Crete [ACM01a].
crime [Cas02, KB00, Lau08b].
criminal [Men03].
criminal [Win05c].
criminal [Win05c].
criminal [Win05c].
criterion [QPV05].
critical [LKM+05, SE09, CS07a, Gor05].
cron [Oue05].
Cropping [SDFH00].
crowd [Fox00].
CRT [FMP03, Kuh02a, May02].
CRT-Exponent [May02].
crypt [Per03].
cryptanalyses [Kan01, SKU+00].
cryptanalysis [ASKE02, AMRP00, Ano03, Ano07b, Ano07a, BDG+01, Bao04, BLH06, BP03a, BK03a, Bar06a, BP01a, BD00a, Bih00, BMFR02, BDK02a, BDK02b, BSW01, BDD03, BD00b, BCCN01, CGFSHG09, CV02, CC01, CL01b, CYY05, CKY05, CKK+02, CWJT03, CJT03, Ch06, Ch08b, CHJ02, CP02, Cou04, CGJ+02, DG00, DGP07a, DGP07b, DG09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Fin06, Fl02a, Fl02b, Fur01, Fur02a, Fur02b, GS07a, GM02a, GJ02a, GJ02b, GM00b, GM02b, GC00b, Gra02a, GS09, GKN+08, HPC02, HQR01, HA04, Hen06, HLL+01, HSM+02, HHK+04, Hsu05a, HLH00, Hwa00, JK02a, J00c, J01, JnBxGxXm05, 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, LWR05c, MS03a, May02, MG01, MHL+02, Mor05, NP01, PSC+02, PKH05, Pei04, Pel06, PS06, PS01c, QC05a, Sch06a, Sco04, Sha03a, Sha05a, STK02, SG01, SGK08, SKI01, SHH07, TIGD01, TM06, TLH05, TJ01b, TSS+03, Wag00, Wag03, WL05, WBD01, WB02, Wu02, XY04, YSD02, YW05, YKLM02a, YKLM02b, YRY05a, YY05a, You1, YG01a, YG01c, ZYR01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, AMRP04, BF01a, Bai08, Bar09, BS01c, Buh06, Bul09, CV05, CK06, CKL+03, Dm06, Egh00, EBS01, Eke09, Fie09, GPG06, Goo00, Jun05, Kuk01, LMSV07, Max06, MAAT03, MAAT04, MAAT05, MAAT06, MAAT07, Na01, Pha04, RSQ03, Rup09, SK01a, Sel00, Sin09, SL07, SC05b, SLL+00, Swe08, TC00, TM01, WLW04, WF02, YL00, YJ00, YKLM03, Kat05b].
cryptanalyst [Wil06].
cryptanalytic [BS00b, KFSS00, Oec03, QSR+02, Yan07, Wil01a].
cryptic [Wri05].
cryptanalytic [Fra04, Men07, Sho05a, Ahm08, Ano01h, Bau01a, Bau01b, Bur01, CCM01, CNB+02, Lev01, Lev02, Mar08a, Mar02b, MC04, SYLC05, TR09a, TR09b, Yun02b, Bec02, BK05, HGN03, Web02, Bel00, Bon03, Kil01a, Yun02a, Se00a].
crypto-algorithms [Ano01h, CCM01].
crypto-based [MC04].
crypto-CCS [Mar02b].
crypto-integrity [Yam02b].
crypto-systems [Ano01h, CCM01].
cryptoanalysis [HSI02, LD01].
cryptoAPI [Bon00].
cryptoclub [BP06].
cryptocomplexity [Rot05, Fal07].
cryptocomputer [HLV04].
cryptographer [Joy03b, Nac01, Oka04, Pol06, 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, Car02, CCDP01, CHL02, CB01, Cra05a, CS09, CO09, DD02, DHMR07, DF04, DWN01, DHR00, DV08, DFG01, FIP01b, FS01a, FGM00a, Fri01, GMP01a, Gar05, GSS08, GGKT05, GK2, GTH02, Gor02a, GL00, GUQ01, Gut00, Gut02b, Gut04a, HST02, HN06, Har06, Has01a, HLN05, Igl02, IV00, It001, IMM01, JT05, KMO01, KY01b, KY02b, Ki01b, KS06, Knu02, Ki002, Law09a, LN08, LS05a, LKJJ01, MS02a, MOP06, Mea01, MNP01, MRL+02, MMH02, Mor03, MK05b, MSU05, N01a, N01b, No0, Ngu05, Nie04, OTTI01, OP01a, PKBD01, Pre00, Pre02a, RSA00d, RSA01].

Cryptographic
[RRA00, RR06, Rot01, RSN+01, SM00a, SS01a, SGM09, Sha02, Shp03, Shy02, SFDF06, SH06, SL09, TLY04, TWNA08, TB0L01, Uzu04, WKP03, WN02, WBL01, WC01b, You01, Zha08, AMRP04, ACTZ05, ALV02, AV04, BGG09, BDSV08, Bla01b, BP05, BG08, BG09, BDN02, BD04a, BGL+03, BM006, Can01a, Can06a, CHC04, CC05d, DP04, DFG00, FS03a, FSGV01, GT00, GPV08, GM04, GB09, HY03, IK03, IYK02, IY03, JW01, KSF00, KP03, LMTV05, Lau05, LLV05, LLW09, ML05, Mea04, MT07, Mic02b, MRST06, Mon03, NN03, NDM04, ND06, PS04a, PSG+09, PR05, Pre07, Pri00, Puc06, QP05, QG05, Reg03, Reg04, RMH04, RBF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, kWPwW01, WLW04, XLM06, YL06, ZLX99, ZWWL01, ZL04b, dH08, BWBL02, QJ04, KKP02, KP01, KN01].

Cryptographic [RS05].
Cryptographically
[ADD09, AHS08, BFCZ08, BB00b, FR08, MS02b, RGX06, Am003, AW05, AW08, L008a, SM03a].

Cryptographically-masked [AHS08].

CryptoGraphics [CK06].
cryptographie [RSA09a].

Cryptography
[ANS05, AF04b, ADI09, AA04b, An00c, An01g, An00a, An005a, An007b, An007a, AAFG01, AIK04, AIK06, App07, AE0Q05, AB000, B001a, B001b, BNP03, BD04, BO03, BO07, BBG08, BM01a, BR00a, BY03, Ber00, Ber03, Bg08, BWBL02, Bla02b, BDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, Bkm06b, Bkm07, Buc00b, BD08, BP01b, BRTM09, CPS07, Cer04b, CSW+08, CQSO1, CPD06, Cob04, CFA+06, C0, Cor06, Dr.00c, Dam07, DFSS08, DFS05, DD00, DFG04, DK02, DK07, Des02, DT03, DY09b, DSS01, DNN00, DNO3, Dre00, DP08, EPP+07, E05, Elb09, Eli04, ECG+07, Ett02, FS03b, Gal01, Gal02, GHK+06, GKK+09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GCO1b, Gra01, GPS06, GN06, Gri01, Gro05, HR06, HH04, HHM01, HVM04, HSS01, HP080, Hon01].

Cryptography
[IEE00b, I05, Irw03, IKOS06, IKOS08, JYZ04, JL00, JT01b, JT01a, Jue04, KLR09, KZ07, KGS07, Kat05b, KKH06, KBM09, KPMF02, KD06, KY01c, KMS02, KZS02, KS03, KWP06, Lam01, LG01, LSY01, Lee03b, LLL+01, Le05, LD04, LW05b, LP02b, Lut03, Lys08, MNT+00, MP02, Mao01, Maa04, MZ04, Mau01, MB01, MR09, MS03b, M01, M03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pel06, PM02, PBB02, Poi02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SG08, Sti05, Sti01, Sti02, Sti06c, SJ05, Syv02, TSO00, TW06, TG04, TW02, Tro08, TR09a, TR09b, Un01, USS02, VY01, VMC02, WPS01, Wei04, WK01, Wel05, Wie00, Wv0D02, YWC08].
[Ytr06, YC01, YDKM06, ZYH03, vDW04, Imr03, AMW07, Auo02a, Auo02d, ABDS01, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BZ00, BZ01, BGM04, BEM+07, Buc00a, Buc01, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CCT08, CDFM05, CDD07, Cos00, DD04, Dif01, DIM08, DwWmW05, DOPS04, DKL09, Duw03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK+07, Geb04, GRTZ02, Gol99, GG05b, GHPT05, GPS05, GNP05, HH05, HHL+00, HKPR05, HAA0, Hig08, HKS00, Hoo05, HG05b, HLwWZ09, IZ00, IM06, JK01b, Joy00, KZ03, KL08, Kat01, Kil05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Mau04, May01, McA08, MBS04, MM07a, Mol07, Nis03a, NH03, Opp05, OS09, PY05, PC09, PC00, Pin06, Reg05, Reg09, Rot02b].

cryptography [Rot03, Roy00b, Rup09, STY07, SBZ04, Ser06, SH05, Shp99, Sil05, Sin99, Sin00, Smo04, ST01d, SK01b, TW05, UHA+09, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Wr03, YC09, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Ree01, Wa00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08].
cryptography-based [FXAM04].

Cryptologic [BS00a]. Cryptological [Lew00].

Cryptology [dL00]. Cryptology [Bar02, Bon03, CMG07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Liu03, LL04c, Lut02, MMV06, Neu04, Nis01c, Ng01, Ok04, Po06, Rot05, RS02, Sha03b, Zhe02h, dL00, Ban00, Ban02a, Bel00, Bih03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam01, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, PC05a, Pf01, Pre00, Pre02b, RD01, Roy00a, Roy05, Sh05a, Son00, Won01, WK06, Yun02a, vT00, DWML05].

CryptoManiac [WWA01]. Crypton [CKK+02, MG01]. Cryptosystem [BST02, FL06, GG01, GK05, GHW01, Hug02, KM01a, KY02c, KLC+00, LHT09, dVP06, Luc02b, NSNK05, NBD01, Ove06, PHK+01, YG01a, YG01c, Zhe02a, Bao04, CL02b, CCH04, Che05a, Cho06, CFVZ06, CHH01, Dan02, DTH06, EKRM01, GHdGSS00, GS01, GC00b, GMW01, Hen06, Iwa08, JW06, KY09, LL04b, LL06, LKY00, Loi00, LS01c, OP01b, Pae03, Poi00, SPG02, SCS05a, SP79, SLC05, Sum00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, hY08].

Cryptosystems [Aki09, Ava03, BDG+01, BKLS02, BPS00, BMM00, CHSS02, CWW02, DDG+06, DKXY02, ESG+05, FJ03, Fe06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KLi01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, SSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vao02, Wao02, X01, ZL02, Ban05, BFO6a, BB79, CHC01, CMK00, EBS01, EKK04, GHO8, GBKP01, HM00, Has00, Has01b, H¨uh00, HP01, KV00, Kos01c, LD01, Luk01, Mic01, Mis06, OS00, Pe09, PLJ05b, SST06, Sha05c, Sma01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WV00, YYY00, ZSS01, vT01].
cryptovirology [YY04].

CRYPTREC [IY00]. CSCW [ZP05]. CT [Joy03b, Men05, Nac01, Oka04, Po06, Pre02b, ZC09].

CT-RSA [Joy03b, Men05, Nac01, Oka04, Po06, Pre02b, ZC09]. CTS [Con00]. 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, An05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BMN01, CQS01, CFA+06, GPP08, HYZ05a, HMM01, HMV04, HM02c, JT01b, JT01a, KMB09, KMF02, KSS02, KWP06, LW02, MOL02, Kir03, OTT01, OS01, PWGP03, Pid06, RSA03b, RS04, RS01, Sat06, Was08a, vT01].
WPS01, XB01, YYZ01, ZLK02, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHKH04, GBKP01, Has01b, Hsu05a, HL05d, JW06, LL04b, Mis06, OS00, ST03a, SSST06, SH05, Sma01, SCL05, SLC05, TC05, Ver01, Wl04, WPP05, YC09, ZSZ01, ZL05, vT01.

Curve-Based [KWP06, Pel06]. Curves [AHRH08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK +06, Kid02, PWGP03, Ver02, CMKT00, Hsu04, LWZH05, MSV04, Sim02, SC02b, Was08b, Wen03, Was08].

customer [Lin01a].

CVS [DFG01]. Cyber [FNRC05, WW04, Mau05]. Cybersecurity [BP07].

Cyberspace [Mit02]. Cyclic [PG05, Mic02a]. Czech [MJ04].

D [Duw03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05]. D.R [Irw03]. daemons [Mos06]. Damgård [CDMP05]. dark [Bhu09]. darkening [CDD07]. DARPA [Coc01a]. Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BNPW03, Bro05b, Che01a, CTLL01, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GM08, GTTC03, HLL+02, Ken02a, Ken02b, Kïus02, Lan00b, LP00, LHS05, Lut03, MND+04, MS03b, MFS+09, NM09, OS05, Per05, RKZD02, RK06, Sal03a, Sal07, Sin01a, TZDZ05, TPPM07, VDKP05, WS05, WY02, WN02, koe1, vW01, AG09, AKH03b, AKSX04, Arn01, Bla00, BNP08, CCMT09, Cer04a, CLR09, CPG+04, DLZ01, FS04, HILM02, LLLK05, MJ03, Mal06, Men03, MI05, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGPH08, SETB08, WMDR08, YLC+09, YC08, ZSIN07, Zir07, Cur05, DK08, Lin02, Papol05]. Data-Hiding [VDKP05]. data/image [S+03]. data/image [Sch00a, Sch01c, Sch04a, Sch04b, Sch05a].

Database [ACM03c, ACM05b, Bl05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Mau04, PS08b, PV01].

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

Datamining [DN04]. Datenverschlüsselung [Lin02].

David [Gas01, Pap05, Bar05, Eaq05]. Day [SE01, CSW05, Win05c]. Days [Adl03, Riv03, SMO04]. DC [USE01c]. DCT [BSC01a, BSC01b, CH01b, KT00, LY07].

DCT-Based [LY07]. DDH [Lys02]. DDO [LKHM+08]. DDO-64 [LKHM+08]. Dead [Gut02a]. deaf [Pau02b]. Dealer [DK01, Sun00a].

Dealing [BH00a]. Debate [Jol01]. Debian [YRS+09, Ahm08].

Debugger [Ano02b]. Debugging [Ano02b].

Dec [IEEE09a]. decades [ Lov01].

decades-old [Lov01].

December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, Lai03, Lee04b, LTT+04, L05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, SMA05, Son00, USE00c, Uni01, Won01, WK06, ZL05].

Decentralized [MSP+08]. deception [CS07a, Mal04, MS02d]. Decidability [Küs02].

Deciding [Bau05]. Decimal [BzvdB02]. Decimation [Fil00]. decipherable [Sav04].

Deciphering [Eri02, KB07, Ank05, Lov01, SNOa].

decision [GR04, KM04a]. Decisional [Cu01].

Decisions [Cor02a, Sch07].

Decodable [Yek07]. Decoding [KY02b, LBGZ01, LBGZ02, Rain01, AGK07, Bul09].

decomposing [FP09].

Decomposition [BR09, CL04c]. decompositions [vDKST06].

Decorrelation [CL09, Vau01]. decrypt [Bli02].

Decrypted [Bau00, Bau02a, MB01].

Decryption [Bar00b, BST02, CS03a, CCD07, FPS01, HGND+03, Int00, KCJ+01, DL01, GH08, Mil03, Shp04b, SW+09].

Decryptor [Zol01]. DeCSS [Coc02a].
Diagnostics [NM09]. Diagonal [PJH01, PJK01]. Dickson [SZP02]. Dictionaries [AGT01].

Dictionary [BPR00, BCP02b, CS07b, Pho01, NS05a]. did [MH09]. Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b]. Dies [Bar06a, Coc01a]. difference [PBMB01, dW02]. differencing [WWTH08].

different [CGMM02, Sma01]. Differentials [BF00b]. Difficult [Bud00b, MT02]. Difficult-to-pass [MT02].

Diff [Jan08, ABR01, ASW01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CRKRT08, F01b, GR04, KI01b, KK02, KM04a, Kra03, Kra05, Mi08, TA06, YR05c]. Diffuser [Fer06].

diffusing [She01]. digest [MSP09]. Digit [KWP06, Tan07a, BG09, HKP05, KJ01].

Digital [ANS05, AvdH00, AR00, AS08, Ano11f, Ano02b, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00a, CCH05, CEA01, CFS01, CMB02, CM02, CZB01, CGJ02, DSP01, EIG01, Eng00, EHK03, HZ00, HSZ00, HZ01, HZ02, HZ03, HZ04, C101, KZ01, KA01, KC02, Kuh00, Kwo02, Kwo03b, LZ01, LLL01, Lin01a, LL01, L03, MM01a, MM02, Me01, PL01, PJH01, PGC01, PBM07, RAM01, RD01, RS01, Sam09, Sch00d, Sch06b, Sch01e, SC02a, Shi08, SLT01, Sug01, TJ03, US02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, Wya02, XFZ01, XYL09, YY00, YY01, YYZ01, ZWC02, Zho02, Aet04, BLH06, Bra01a, Cal00b, CS08a, CWH00, CL00, CJ05, Che07, FB01, GG03, Gl07, HLR09, HLH00, HHC05, KP00, Lev01, LLL06b, MKY08, NRR00, PC05b, PL05a, PB08, QCB08, Sha01d, Sha04b, Sha05d, SCL05, TCC02].

digital [UP05, WNQ08, WHLH03, X05, XMST07, Ano09, Ano13, BCKK05, CDS07, CKL05, FIP00, F000, KCR04, Nat00, PK03, SA02]. Digital-Audio [WNY09].

Digital-Signature [EN00]. Digits [Che04b, Ran55, Ran01]. Dimension [DDG06, TZT09a, TZT09b].

Dimensionality [SBG02]. dimensions [CLR09]. Direct [BMW05, KG09].

directional [PJH01]. Directions [Sha01b, DFH01]. digitally [JZC05].
directories [C02, P03]. directory [C02]. disabled [Pau02a].
disadvantage [CDS07]. Disappear [Per05].

Disappearing [Way02b, Way09]. Disaster [WCZ05]. disciplinary [SM08]. disclosure [J07, Swi05].

Discovery [Bi09, HLL02, SBG07, SGA07]. Discrete [CS03a, CNS02, Che04b, CCW02, Gen00, GV05, GPP08, LW02, LJ05, VK07, HN04, HW03a, HWR09, Hsu05a, H05d, JL03, LL01, LHL03a, LHY05, LTH05, PL05a, QCB05a, Sch01e, Sha05c, Sha05d, SR05, SCL05, SCL05c, SCS05c, Y08].

discretized [MA02]. Discription [Har07b].
discursive [Mit02]. Discussion [An01a, An01b, An01c, An01g, An01h, An01e, An01i, KLB02a, Mal02, N02b].

Dishonest [GKK007]. Disk [Cro01, Har07b, Siv06, CS08a, Fer06].
dispatches [Kee05]. displayed [CGV09]. Displays [Kuh02a]. Disputed [CAC06].

Distance [CGFSHG09, CPH04, DM07b, DW01].

distinguished [HWW04, WH02b].

distinguishing [HSR01]. Distortion
[Ano02b, WWL+02]. **EC** [SF07]. **ECC** [BWBL02, CL09, Mis08, Tsa05]. **ECC-based** [CL09, Tsa05]. **ECC2K** [LM08]. **ECC2K-130** [LM08]. **ECCV** [MJ04, TBJ02]. **ECDSA** [ANS05]. **Eclipse** [Coc02b]. **ECMA-305** [ECM00a]. **ECMA-306** [ECM00b]. **Economics** [Ble07]. **ECPP** [Che03]. **ed** [Gum04, Nis03a]. **Edge** [Sta05]. **Edinburgh** [RS05]. **Editing** [CGFSGH09]. **Edition** [Cha04]. **Editors** [BK06b, PTP07, SJT09, SGK08]. **EDK** [Ano02c]. **Eds** [Duw03, Pag03]. **Education** [Puz04, RC06, CAC03]. **Effect** [AEV+07]. **Effective** [CDR01, PD07, Sen03, SL06]. **Effects** [BBGM08, Har00, SN07]. **Efficiency** [II00, GGT05, SLG+05, GT00, GKO03, KT06, YTH04]. **Efficient** [ACS02, ABRW01, AEMR09, Bai01b, BINP03, BKLS02, BR00a, BGP02, BDSV08, BGG+03, BS00a, BF01c, BGF07, BB00b, BCDM00, CKPS01, CL02a, CCMT09, CCD07, CL01b, CPX04, CM05a, CJL05, CTO8b, CKK03, Cou01, Dam02, DN03, Dhe03, FF00, Fis05, FS01c, GLV01, GCO1b, GTH02, GST04, GBK01, HCJ02, HSZ101, Has01a, HS00, HW04, HL07, Hl00, HS07, KOY01, KOY09, KLY02, KO03, KHD01, KKH03, LSY01, LCK01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, Nd05, NS05, OS01, PCS03, PBD05, Ram01, RSQ03, RDJ+01, SM01, SM03a, SRQ03, SSNG00, TC05, WHL05, WYY05d, WHL01, WC01a, XBO1, XSO3, YWD08, YHL05, Zan01, ACTZ05, AFB05, Bla01b, CC04b, CC50c, CY05, CHC05, CL08, GFW08, DwWmW05, FP09, FSG01, HGH06, HCO04a, JW06, KHYM08, LPV+09, LCK04, LLH04]. **efficient** [LYC02, Mic02a, MSP09, NR04, PCC03, RG05, RBB03, SLP07, SKW+07, Shao5b, SC05a, WK05, XC05, Yn02, YTV05, YC09, ZSN05, ZYW07]. **Efficiently** [IKNP03, NNT05, AGKS07]. **Efforts** [Pau02a]. **Eggs** [Wei05]. **EGPGV** [MFS+09]. **Egypt** [EB+00, Irn03, Sin00]. **Eighth** [ACM06, B+02, ElvS01, IEE01b]. **Einstein** [MNT+00]. **EJB** [TEM+01]. **Ekert** [Duw03]. **El-Gamal** [EKRM01]. **Election** [JLL02, Cal00a]. **Elections** [Cha04, PwS01]. **Electromagnetic** [SGM09, QS01]. **Electronic** [Ble07, CL01b, CM02, Dhe01, Hof01, ISO05, IY00, KMO01, KS02, Lan04b, LLL02, MNFG02, Rb01, RMCG01, Str01a, YKM01, ZYM05, Avh00, AAK09, Cal00b, EY09, FB01, HJ05]. **element** [MS02d]. **Elementary** [Sin09, Ste08, Tat05]. **Elephant** [Fe06]. **Eleven** [All03]. **ElGamal** [BJN00, CL02b, CWH00, HL04, LHT09, SJ00]. **ElGamal-like** [CWH00, HL04]. **Elliptic** [ADL09, Ano05a, Bai01a, BINP03, Bar00a, BBGM08, BMM00, BS01d, BMN01, BB00b, CQS01, CFA+06, GLV01, Gau02, GP00, HY05a, HMM01, HW04, HM02c, Hus04, JT01b, JT01a, KMB09, KMF02, Kid02, KS02, LW02, MP01b, Mi02, Kir03, OTI01, OS01, OT03b, PWG03, RSA03b, RS04, RS01, Sat06, SI05, Was08a, Was08b, WPS01, XBO1, YYZ01, vT01, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFV06, DIM08, DwWmW05, EHK04, GBK01, Hs05a, HL05d, JW06, LLL04b, LWZH05, Mis06, MSV04, OS00, ST03a, SSST06, SH05, Sim02, Sma01, SC02b, SLC05, TLC05, TC05, Ver01, YC09, Yas08, ZS01, ZL05, ANS05, BBW02]. **Ellis** [Coc01a]. **Elmaw** [IEE01b]. **Else** [FL01b]. **EMA** [QS01]. **Email** [ES00b, Gar03a, Luc06]. **Email-Based** [Gar03a]. **emanations** [ZZT05]. **Embedded** [Ano01c, Ano02b, Ano02c, BBGM08, DR02, DV08, GSS08, JOT05, JQ04, KKP02, LPW06, NdM04, RS05, SPG06, WKP03, YSS+01, ARJ08, BGM04, Fox00, Gb04, KV+09, KP01, KNP01, KP03, MBS04, Nis03a, TKP+08, XQ07, Fin02]. **Embedding**
[AAK09, JX05, JG07, Sal03b, WY02, KC09, Wan05]. Embrace [CNB+02]. Embracing [Ano03b]. EMD [BR06]. Emperor [Smi01b]. Empirical [HW03b, Goo00]. empirically [SS03]. Emptiness [DIS02]. Emulex [CZB+01, CTBA+01]. Enabled [Por06, CCCY01, DY09a]. Enabling [Web02]. encapsulation [CHH+09, KG09]. Encipher [BR00a]. Enciphering [HR03, KT01]. Encode [BR00a, BKN04]. Encode-Then-Encipher [BR00a]. Encode-then-Encrypt-and-MAC [BK04]. encoded [WMS08]. Encoding [JT01b, RS00, Lin02]. encounter [Win05c]. Encrypt [BK04, BTTF02, Dav01c, Pet05, Dav01b]. Encrypted [BBK03a, BGHP02, BLG03, CD01b, Hug04, Lan04a, LH07, RMCG01, Sta02b, Vau01, WRW02, Wu00, Shi02b, BNP08, CCMT09, CDD05, CHH07, HLM02, Hes04a, LSH00, Pet03, ÜG08]. Encrypting [Pro00, RC01]. Encryption [ABC+05, Abe01, AS01a, Abe04, AP09, AB01, AD02, And03, Ano01f, ANR01, AFI06, AF03, Bar00c, HI00, Ban02b, BN00a, BR00a, BBM00, BBPD01, BU02, BF01b, BF03, BB04, BGW05, BCHK07, BGH07, BPR+08, BB03, BNPW03, BD03, BKY02, Bur03, CD00, CS03a, CHK03, CHK05, CGH01, Cho01a, CTL01, Cli08, Cho08a, CMR06, Cla00a, Coc02b, Coc01b, CNJP00, CHJ+01b, CD01, CS01a, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DKF+03, DS05, Dri02, FIP01a, FL01a, GC01a, GSW00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx. HSH+08a, HS02a, HYZ05a, HSH02, HSH06, HKR01, HW05, Har07b, Har00, Hei07, HS00, HR05, HG03, HL02, HGNP+03, HLL05, HLC08, ISSZ08, Jol03, Jol01, JK02b]. Encryption [JJ02b, JMV02, JKRW01, Jut01, KBD03, KSHY01, KS00a, KY01a, Kha05, KKJ+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, Mü01a, MS09c, NIS00, Nam02, NZCG05, NP02b, Nie02b, PV06b, PM00, Pau09, PDS09, Pha04, For01, PS00, Pre01, RM06, RDJ01, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQL03, SPMQ06, SBZ02, TV03, Uni00a, Uni00c, Uni00d, Uni00g, Uni00h, Ust01b, VMSV05, WZW05, WBRF00, YEP+06, YW06, AS00, Abd01, AKBX04, AMR00, ABW09, Ano00c, Ano02a, App05, Ate04, AcD05, AFGH06, BK04, BR04, BBN+09, Ber09a, BBK+03b, Bir07, Blu00, BJN00, Bro05b, CS08a, CBSU07, CH01, CKRT08, DZL01, DL07]. encryption [DRS05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GKK03, Gen09a, Gen09b, GKM+00, Gou09, Gua05, HSH+08b, HSH+09, HS02b, HNYW07, HCD08a, HCD08b, HAU04, HW02, Hsu05a, Hwa05, HL05c, HL05d, IM06, JK01a, JK01b, JWW05, JX05, JZCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kru05, Küh08, La00, LV07, Lee01, LCP04, LJ05a, LMC+03, LLLZ06, LLLL06b, LLLC08, LB05, Lu02, Lud05, LK01, LWK05a, Mar05b, Mat02, Mü01b, NK06, OS07, PBMB01, PS01a, Pau02a, Pau03, RG09, Rho03, RBB03, RSP05, SN00, SKW+07, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sch01d, Sch01f, SR00, SVEG09, Shp04b, SWH+09, Tan01, TTZ01, TOEO00, TM01, TLH05, Uni00b, UP05, VKS09, WG02, WN95, WH02a, XY04, Yan02, YGZ05, YZEE09, YC07, ZL01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05]. Encryption [CKH08, CHJ+01a, RR04, Uni00f, Wue09, Jan08]. encryption/cipher [HAU04]. encryption/decryption [OS07]. Encryptor [LMP+01, TPS01]. Encryptor/Decryptor [TPS01]. Encyclopedia [Bid03, vT05]. End [KCD07, Per03,
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, Miš08, 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 [LLLW08a]. Expansion [DN02b, BCD06, HKPR05]. expansions [HKPR05]. Expected [KL05, RK06, DLP+09]. Experience [Sas07, BCHJ05]. Experimental [BG09, CGBS01, ¨OOP03, WS02, RSQL03, Smo04]. Experimentation [Bru06]. Experimenting [LSVS09]. experiments [MPHD06, USE00b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOBH05]. exploitation [Eri03, Eri08, KYV+09]. Exploiting [CK06, ETMP05, HR00, HM04, ZWC02]. Exploits [MJF07, CSW05]. exploration [SKW+07]. Exploratory [Lut03]. Exponent [BP04, BM01b, DN00b, May02, SZ01, CKY05, Duj08, GD03, Sph04b]. Exponential [BYJK04, BYJK08, CY08, GKK+07, GKK+09, Shp05]. Exponentiation [KKH03, SK07, CKRT08, HGNS03]. Exponents [FS02, FS01b]. Exposed [Gum04, MSK03, SS06]. exposing [YY04]. Expositive [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, CMe006]. Extensions [ABC+05, BBGM08, CS07c, HM02b, Rot02a, Wei04]. Extracting [Cer04a]. Extraction [DG07+04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lu02, Vad03, DW09, KZ03, Sha04a]. Extraordinary [Top02]. Extreme [Bai02b]. Extrusion [Bej06]. Eye [Sas07, CAC03]. Eye-Opening [CAC03].
Faster [Bar00c, CMJP03, GLV01, KS09, LV04, Oec03, Bui05, Why05]. faszinierende [Sch09].

Faster [Bar00c, CMJP03, GLV01, KS09, LV04, Oec03, Bui05, Why05]. faszinierende [Sch09].
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]. Foor [RG05]. Footsteps [Lav06], force [Cur05, SGA07], forces [AJ08]. Ford [Mar05a]. Forecast [Rai00]. Forecasting [WWL+02]. Forensic [PS08b, Cas02, Kor09]. forensically [ME08b]. Forensics [JBR05, CS04, CS08a, CDS07, MS09a, MKY08, MAC+03]. Forest [FBW01]. Forgery [CH01a, CKM00, LS01a, SLT01, HSW09]. Forgotten [Eag05, Kin01, OC03]. Form [ADI09, CH07c, OS01, LKYL00, Mic01]. Formal [BGB09, BCHJ05, BCJ+06, CL05, DKS08, OR02b, HG03, Lan00d, Mea01, YWD08, JW01, Mea04, ZLX09, ZL04b]. Formalizing [HM01a]. Formally [BJP02]. format [ISO05, RG05]. format-string [RG05]. Formation [RW03a, LK01]. Formats [GIS05]. Forms [JT01b, LLL04]. Formula [Kog02]. Formulas [BN05]. Formulations [AHRH08]. Forum [CZB+01, CTBA+01, CNB+02, CMB+05]. Forward [AR00, AF06, BY03, CHK03, IR01, HCD08a, HCD08b, ZYW07]. Forward-Secure [AR00, AF06, CHK03, IR01]. Forward-Security [BY03]. Forwarding [KCD07, Kra02b]. FOSS [Bo02]. Founder [Bar00a]. Foundation [Lut03]. Foundations [DK07, Gol01b, Gol01a, Gol04, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Nic02d, Sal05d, Kat05b, Puc03]. Founder [Bar00a]. Four [LXM+05]. Four-Layer [LXM+05]. Fourier [Cle07, DSP01, DNP07, LPZ06, SP04]. Fourteenth [USE00c]. Fourth [ACM02, ACM05b, DFCW00]. FPGA [Ano02c, CC02a, CGBS01, CG03, CNPQ03, EYCP00, EHHK04, KMM+06, KY09, KMB09, KRS+02, LP02a, MM01b, MM01c, OTT01, OP03, Pat01, PBTW07, QR+02, TYYL02, TPS01, USS02, WW00]. FPGAs [AD07, DPR01, MM07, RSQ03, SGM09, SK05a]. Fractal [AA04a, JLM03]. Fraction [Wai03]. fractional [DSP01, SST06]. fractions [Dan02]. Fragile [CH01b, CT09, Nak01, PJK01, LY01, SY01b]. Frame [LHS05]. Frames [HWW05]. Framework [AN01, GL03, GOR02b, Hur05, NMO05, NP07, PS06, RN00, SHY02, ZYN08, AH03b, CWC01, CP07, C04e, DMSW09, GJ05, GL06a, GM04, JE04, KNS05, MS09b, MBS04, YCW+08, HF00]. France [ACM04a, ACM05a, AJ01a, AJ01b, GH05, KN01, NP02a, PPV96, KM07]. Francisco [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b]. FranzSteiner [Eag05]. fraud [Ano03a]. Free [Bar00b]. FreeBSD [Coc01a, Mur02, Siv06]. Freedom [Un00a, Un00c, Un00d, Un00g, Un00h, M103]. FREENIX [USE01b, USE02c]. French [Wri03]. Frequencies [DD02]. Frequency [OMT02, Sak01, SOHS01]. Frequency-Domain [OMT02]. Frey [Was08a]. friar [GG05a]. friendly [CRSP09, Hsu05b, HSL05, SZS05, WLT05a]. FrontPage [WWL+02]. FSE [Bir07, DR02c, GH05, Jo03, Mat02, RM04, Sch00b, Sch01d]. FPC [Ste05c]. Full [Cor00b, DOP05, LKH09, WWY05c, B104, CS08a, HS02b, LKH+08, Oi09]. full-encryption [HS02b]. Full-Round [LKH09, LKH+08]. Fully [BL08, FS01a, Gen09b, KPM02, RG09, Gen09a]. Function [BR02, CDMP05, Fis01b, Fhu02b, GIS05, HNO+09, HPC02, JJ00a, Kan01, Kil01b, Nic02c, RB01, Yan05, CHY05b, CJO4, HR07,
LW04, LPM05, WWTH08, YW05, YRY05b].

Functional [ECM00a, WA06].

Functionalities [PS05], functionality [ETMP05].

Functions [AEMR09, BBDK00, Bon01, Can01b, CV02, Car02, Che01c, DN02a, DGN03, DNRS03, Fil02, FIPR05, GLG+02, HSM04, HR04b, Jou04, Kil01b, LTW05, Lys02, PR01, RR08, SM00a, SM00b, SS01a, Sho00a, Sho00b, Ver02, WP03, WFLY04, Wer02, AGGM06, AGGM10, ALV02, CS09, GVC+08, HRS08, 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].

fusul [MAaT05].

Future [ASW+01, Joh00, LNP02, NFQ03, Sch00e, LPW06].

Fuzzing [SGA07], fuzzy [HS02b, NC09].

fuzzy-based [NC09].

G [Coc03, For04, Was08a]. Gaitherburg [SMP+09]. Gamal [EKRA01]. Game [DHR00, LM02, CAC06, BR04, Gou09].

game-like [Gou09]. game-playing [BR04].

Gamers [MP00]. Games [KN08]. Ganesh [For04].

Ganzúa [GPG06].

Gap [OP01a, PWGP03, RW03a]. Gap-Problems [OP01a].

Gate [Coc02a, GC01a]. gates [TWM+09].

Gauging [PvS01].

Gaussian [EKRA01, JL03].

Gbps [TPS01]. GCD [JP03].

GCD-Free [JP03].

GCM [KS09]. geeks [McN03].

Geheimsschreiber [Joy00, UW00].

GEM [CHJ+01a, JM02].

General [AB09, CDM00, DN00a, ESG+05, GMP01b, Kog02, Lin03, MND+04, Sal01a, YC01, YJ06, JL03, JJJ05a]. General-Purpose [ESG+05].

Generalisation [DJo1]. Generalization [YYZ01, HWW02]. Generalizations [LD04]. Generalized [KSR02, Mic02a, TC01, TJ01a, Wag02, WHL05, LKYL00, Shi05].

Generate [HSR+01, Wer02, FSGV01].

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, WHL05, Web08, WS02, Ano04c, BK07, BG08, BF01c, ISTE08, LS05b]. Generator [ADD09, BPR01a, DI05, DiC03, DGP07a, DGP07b, DV08, EHK+03, Gen00, GM02a, Gol01c, GPR06, Int03, Ke105, LMHCETR06, LV04, SX01, SFDF06, TWNA08, TTT09a, TTT09b, ZKL01, Aam03, ACTZ05, Be108, BG08, BG07a, DGP09, GB09, HG05a, HLwW09, JAW+00, KH08, KSF00, Pan07, PGP07a, PSP+08, PC00, RGOX06, SR07, SB05, UHA+09, WW08, VKS09].

Generators [BST03, BK06a, BL08, CF01b, CS05a, Fin06, Kra02a, LBGZ01, LBGZ02, LS05a, MHO4, RSN+01, Vav03, BK07, BGPG05, CO09, SK01b, Tsa06, YZEE09].

generators-part [SK01b]. Generic [BN00a, DOP05, GKT05, HLL05, Mar02b, MV01, GT00, MP08, Sch01f, Sch01e, XLMS06, CHJ+01a]. Genetic [HSIR02, LMHCETR06, CV05, SCS05a, WJP07].

Gennaro [Miy01].

Gennaro-Krawczyk-Rabin [Miy01].

gentle [RR03a].

Gentry [Hes04a].

Genus [CY02, GHK+06, Wen03].

Geometric [GTTC03, LL05c, LJ05b, SDF01, CJT01].

Geometrical [LWS05].

geometry [PPV96, WW06].

George [Gum04].

Georgia [IEE09b].

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

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

Geschichte [Sch09].

Get [Coc01a, WD01, Cla00b].

gets [Bor00].

Getting [PM00]. GF [BIN03, KMPF02, KLY02, KKY02].

GH [GHW01].

GHS [HES04b].

GIANT [Lam07].
Gibson [Ove06]. Giesbrecht [CHH01].
Gigabit [CGBS01]. Gigabits [HTS02].
Give [CNB+02]. Given [Wal03]. giving [Wu01].
Global
[Ahn08, LWS05, Por06, BK00, Kee05, KB00].
Globus [MJD01]. GN [SC05b].
GN-authenticated [SC05b]. Gnana [For04]. GNU [Coc01a]. Gnupg
[JKS02, Sti06b]. Go [Bur06, CZB+01].
Goals [PHM03]. goes [Pan07]. Gold
[Boy01, For04, Tsa07]. 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]. got [Car01].
Goubin [Sma03b]. Governance [TPPM07].
Government [LY00, RM02, Lev01, LCS09].
Pgp [Bau01a, Bau01b, Luc06]. GPS
[CKQ03]. Gpt [Ove06]. QG [BP02].
Graduate [GV09]. Grafton [Pag03]. grain
[Rhi03]. Grained [SS01b]. Grand [Syv02].
Graph [CGFSHG09, GfTTC03, HM02b, VVS01, YKW01, CT07]. Graph-Based
[CGFSHG09, HM02b, CT07]. Graphical
[vOT08]. Graphics
[CK06, DNP07, MFS+09]. Graphs
[NNT05, Ust01b, WGL00]. Gravrilenko
[Puz04]. Gray [FGD01, Har05b].
Gray-scale [FGD01]. grayscale [YCL07].
greatest [Bel07]. Greece
[ACM01a, KGL04, SM07]. greedy
[HKPR05]. Green [TR09a, TR09b].
GREMLIN [H601]. Grenoble [ACM05a].
grey [BDN00, SCS05a]. Grid
[ACM05a, MJD01, SEF+06, TLC06, ZBP05, Cha07, CJK+04]. grids [MPM09]. Grip
[Buh06]. Gröbner
[CCT08, FJ03, Fau09].
Group [ANR01, AAFG01, ACJT00,
BBS04, BCP01, BCP02a, BCP02b, CD00,
CvTMH01, CH01a, HSH02, HSH06,
HW04, Hug02, JP02b, KY03, Kin02,
LZL+01, MSU05, SOO102, SWH05, Ste01,
Tan02b, VMSV05, Wer02, AKNRT04,
BC07, CL04b, CYH04, CH05, CWJT01,
CJT04, Cho08b, ED03, He02, Hen06,
HW02, KS05a, KPT04, KKKL09, LL06,
LLH04, LPM05, LWK05b, NS05b, RH03,
SNW01, Sha05a, TJ01a, Tse07, WGL00,
WHHT08, YLC+09, YY05a, ZC04, Z04].
group-by [YLC+09]. Group-Oriented
[LZL+01, HW04, CH05, CWJT01, LL06,
TJ01a, WHHT08]. Groups
[BSS02, CV03, CF02, Dre00, GM02a, GST04,
KM01a, KLC+00, LLH01, LP03, Luc02b,
MN01, PHK+01, GR04, HM00, Pae03, YI04].
GSM [BBK03a, BD00a, Cha05b, Cim02].
Guadeloupe [Wri03]. Guanajuato
[Buc00a]. Guangzhou [LL+04, Li05].
Guessing
[AGKS07, Bau05, Shi05, YS02, DLMM05].
Guest [KP03, Sak01, BK06b, MFS+09,
PTP07, SJT09, SGK08]. Guide
[An06b, BS01a, BSB05, BCP+03, BCP01b,
HM04, Poo03, Vac06, Wei04, And08,
Bau00, Bro05b, C0+02, Che00, Gar03b,
Kov03, Lu09, Mal05, SL06]. Guidebook
[SEK01, SEK02]. Guided [ZY08, Pet08].
Guildford [KNI03]. Gummy [MMY02].
Guo [LLLZ06a, LLLZ06b]. Gutmann
[Uza04].

H [Was08a]. H.R [Un00a, Un00b]. H.R.
[Un00a, Un00c]. H64 [GMM01]. Hack
[MYC01, Sin02, SL06]. hacker
[Go08, Har05b]. Hackers
[SEK01, SEK02, BD04b, NRR00, Win05c].
Hacking [Eri03, Eri08, Gum04, Man08,
MSK03, SSS06, 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
Handbook [And04, Cas02, CFA+06, Jan06, MMJP03, RE03, AB09, Fin03, Har05b, KB00, KH03, MJ03, RE00, Was08a]. Handheld [BMK00]. Handhelds [MP00]. Handle [RC06]. Handling [KL05, Lut03]. Handoff [OKE02]. Hands [KLB+02b, Shu06]. Hands-on [KLB+02b, Shu06]. Handshake [SB01]. Handshakes [Ver06a]. Handwriting [Ano02b]. Hankerson [Irw03]. Haptic [PBM+07]. Haptics [Pau02a]. Hard [Har07b, HMS04, Lai07, CGHG06, GPV08]. Hard-Core [HMS04]. Hard-Disk [Har07b]. Hard-Line [Lai07]. hard-on-average [CGHG06]. hardcore [Scho1e]. hardcover [Eag05, Pag03, Top02, Pap05]. Harddisk [Por01]. Hardness [CHS05, CNS02, KY02b, HS06, LTW05, SV08b, AGGM06, SU07, AGGM10]. Hardware [Ano07b, BNN+01, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, Gk02, GPS05, GLG+02, Gro01, GPP08, Ikm00, IS03, JQ04, KKP02, Nd05, FS01c, RS05, RS04, SORTD00, SMTM01, SM02, SM03b, SRQL03, Sgk08, TSO00, TBL01, WK03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, BBK+03b, EHHK04, GC00a, HBC+08, KP01, KN01, KP03, Nd04, RAL07, SOIG07, VS08, Wo04, YKLM03, YW06]. hardware-constrained [RAL07]. hardware/software [ARJ08]. Harley [WPP05]. Harp [G01]. Hash [Ano08, Ano12, AEMR09, BBKN01, BRS02, BDS09b, Burt06, Cor06b, Cor02, CDMP05, CS02, DOP05, FI02, Fil02, GIS05, GLG+02, HPC02, HR04b, ISO04, Jou04, KMM+06, MD05, RRR06, RR08, RB01, SS01a, Sh000a, Sh000b, SK05a, WFLY04, Yan05, YZ00, BR06, KCL03, Ku04, KCC05, LLH02, LKY04, LW04, Mic02b, Wg00, YRY04, FI02a, ZW05a]. Hash-based [BDS09b, KCL03, Ku04, KCC05]. Hash-CBC [BBKN01]. Hash-Function [BRS02]. Hash-functions [ISO04]. Hashes [Sch01a, GNP05]. Hashing [IKO05, SGGB00, WS03]. HAVAL [WFLY04]. HAVALE-128 [WFLY04]. HAVEGE [SS03]. HB [MP07]. HB-family [MP07]. HB-MP [MP07]. HCI [YKMB08]. health [Ano03a, CCCY01]. health-care [Ano03a]. Healthcare [BTTF02, heap]. Hearing [Uni00c, Uni00g, Uni00b, Uni00f, Uni00h]. hearings [Uni00b]. Hedge [Sho00b]. Hedged [BNN+09]. Heimdal [WD01]. held [Buc00a, PPV96, Uni00b]. Hellman [KM04, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, Cj03a, CKRT08, FS01b, GR04, K01b, KK02, Kra03, Kra05, Mis08, Tsa06, YRY05c]. Helped [Gan01b]. Helps [DF01, Pri00]. Helsinki [Bur00]. Hensel [CNS02]. Here [Bur06, Law05]. Hermite [Mic01]. heroes [OC03]. Heyerdahl [Coc03]. Hersonissos [ACM01a]. Hessenberg [SSFC09]. Heterogeneous [BCS02, KHYM08, ZBLvB05]. Heterogenous [H501]. heuristic [SS03]. HFE [FJ03, CHH01, Fe06]. HFE-Cryptosystems [Fe06]. HIBE [CS07]. Hidden [HGN03, KV03, LNS02, GM05, L09, S05, FJ03, Sch09]. Hide [FJ03, S05]. hide-and-seek [S05]. Hiding [BD03, Col03, DN02b, GA05, HNO+09, LHS05, MH05, MM09, VDKP05, HR07, JD01, KP00, RSP05, W02b, W09, YCL07]. Hierarchical [GS02b, HNZI02, HL02, MN01, YLH05, BD04b, Che07, JW06, WC01b, hY08]. hierarchies [AFB05, Cer04a, HY03, WL05]. hierarchy [CMdV06, Hwa00, JA02]. Hierocrypt [OMSK01]. Hieroglyphs [Wri05]. High [ACM01b, Ano00b, Ano02b, ChLYL09, C09, CJL06, CGJ+02, DS05, FZH05, Gro01, HNZI02, HV04, Int00, JKRW01, KMM+06, Ken02b, KB00, Kra05, KT01, MM01b, NFQ03, RW07, SKKS00].
[BTW05, BTW08, CDFM05, Lan00d, Gen09b]. **Ideas** [Gha07, Eri01].

**Identification**

[BP02, BLDT09, Gar03a, GLC+04, KK02, Kir01, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZC09].

**identifiers** [MC04]. **Identifying** [HBF09, LLS05b, ZYN08, DMS07].

**Identity** [BP02, BLDT09, Gar03a, GLC+04, KK02, Kir01, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZC09].

**Identity-Based** [BP02, BLDT09, Gar03a, GLC+04, KK02, Kir01, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZC09].

**IDFSM** [TZDZ05]. **IDtrust2009** [SMP+09]. **IEEE** [BS03, BCDH09, BC01, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, KM07, HSD+05, Hug04, Mis08, PHM03, ZDW06]. **IEM** [RC05].

**IFIP** [DKU05, DFPS06, DFCW00, ELvS01]. **II** [Ban05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Hai03, MOH09, OC03, Res01a, Res01b, Sal00a, ZTO03]. **III** [Scho00a, Anoo0b, Bau03b]. **IKE** [C02a, Kru03]. **I’ll** [PLW07]. **Illinois** [ACM04b]. **Illusions** [Koc02].

**Image** [APT00, AS01c, BSC01a, BSC01b, BQR01, CYH01, GW01, KB03, LLS05a, LZ01, LWS05, LY07, LJ05b, LSKC05, RS00, SHF00, SDF01, SSFC09, SYL05, TTD01, TH01, TC01, UP05, VS09, VK07, WY02, WLT05b, YZEE09, CC02b, CHC01, Che07, Che08a, KC09, LLCL08, Lin00a, LT04, LYGL07, LLC06b, MS09a, MB08, PBV08, S+03, mSgFl05, TL02, Wan05, WMS08, YCYW07, YCL07, ZLZ07].

**Image-Feature** [GW01]. **image-identification** [PBV08]. **Images** [CW09, DP00, FGD01, PJ01, PB05, RE02, AEER05, BD00, FWTC05, HYW07, TCC02]. **Imaginary** [HJW01, H00, H00].

**Imai** [DDG+06, YG01a]. **Imbalanced** [ZWCY02]. **Immunize** [CZK05, PZ02b, YKLM02b, ZP01, YKLM03]. **Immunization** [HR05]. **Impact** [Ber03, HGPN03, JKRW01, MMYH02, CS08a].

**Imperfect** [CPS07, DOPS04]. **Implied** [KY01e]. **Imply** [Pie05].

**Importance** [KCJ+01, TIGD01]. **Important** [SM00a]. **imposed** [XLMS06].

**Impossibilities** [CHL02].
Impossible [BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SKI01]. 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, JQY01, Kin00, KT06, Ku02, Küh02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02c, PR08, ST01b, SWH05, SC05c, TMM00, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].

Improvement [AS01c, AJO08, Che04a, CZK05, CCW02, Di01, HWWM03, HW03, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Shao4b, Shao5b, WHL03, YRY05b, YRY05c, ZYM05, ZAX05, BL06, CK04a, CL04c, CHY05a, Hsu05a, JSW05, JmbDgXm05, KJJ05, LL04a, LW05, LZ05, SS05, T001, WLT05a, YW04, YWC05, YRY05a, ZC09].

Improvements [BBM00, HW02, JL03, NP02b, YCYW07, CH07a, SRQL03].

Improving [ASHK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SKQ01, SB01, Sun02, XQ07, YEP+06, YGZ05]. incentives [Swi05]. Incident [JBR05, Tom06]. Including [SR01].

Incomputable [Ver06b]. inconsistencies [MS09a]. Incorporating [MFS+09].

incorrectness [CHC04]. Increase [PBTW07]. Increasing [CS05b].

Incremental [BKY02, L03, PBK05, TP06b].

IND-CCA [Mii01b]. IND-CCA2 [BST02].

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 [TZZ09a, TZZ09b, Vau01].

Influencing [Bla01c]. Inform [Kwo03b, San05].

Information [AP09, BW07, BM00, BZ02, Big08, BB03, BJ02, Boy01, CGM07, DM00b, ECM00a, ELv01, Hay06, HQ05, HW01, ISO04, JG07, KP00, Ke02, KLB+02b, K00, Lai03, Lee04b, LW05b, L01, MH05, Oka00, PP06b, RSA00d, RS01, Roy05, Sch06b, Son00, Sta06, Ste02, TG07, VDK05, WABL+08, Yek07, Zhe02b, ZS05, vW01, AB09, A00, Bid03, BK00, BEZ00, BEZ01, BR05b, Dv03, FR08, FPO06, Gar04, Gha07, IY05, KN08, KB00, Kov03, MS09b, ME08b, PS02a, Sun02, Tw09, Way02b, Way09, CSY09, FLY06, GW00, Kim02, LL03, LL04c, PC05a, W01, WK06].

information-flow [FR08].

Information-Theoretic [VDK05, vW01].

Information-Theoretically [DM00b].

Infrastructure [AKM02, AL06, BC04b, BWE+00, CL07, ES00a, FL01b, KGL04, Sin01a, BHM03, BDS+09a, Ben01a, CZ05, FB01, Gor05, LCK04, MWS08, Ben02].

Infrastructures [HDC02, L00b, PHM03, WBD01, Bra01a, LAPS08, SN07].

INIDP04 [L04].

initial [DK08]. Initiative [Coc01a, Cal00a]. initiatives [Mau05].

Injection [MMJ05, ZSN07].

Injective [CM06, Kos01c].

Innovative [Sam09].

innovations [We02].

Innsbruck [Pfi01].

Input [CAC06, TC00, DKL09, VM03].

Input-trees [TC00].

Insecure [Vau05b, Wal01, BJ00].

Insecurity [Bla02b, DPO05, Lai08, Man02, NS01b].

insertion [MB08].

insertion-extraction [MB08].

Insider [CMS09, Tad02, KS05a, Mah04].

Insights [Kun01].

Installation [USE00a]. instance [FS08].

Instances [GG01, HN06].

Instant [BBK03a, RR05].

Instantiated [RR08].
Invariants [WH09]. Invasion [ASW+01]. invasions [Tyn05]. Invention [Ifr00]. Inventors [Bar00c]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, MFFT05].

Inversion
[BNPS02, KKY02, TTT07, SPG02]. Inversion/Division [KKY02]. Inversion [CGH00a, Has01a, JP03]. Inversion [IWBRS]. Inversion [BNPS02, KKY02, TTT07, SPG02].

Inversion
[BNPS02, KKY02, TTT07, SPG02]. Inversion/Division [KKY02]. Inversion [CGH00a, Has01a, JP03]. Inversion [IWBRS]. Inversion
[BNPS02, KKY02, TTT07, SPG02]. Inversion/Division [KKY02]. Inversion [CGH00a, Has01a, JP03]. Inversion [IWBRS]. Inversion
[BNPS02, KKY02, TTT07, SPG02]. Inversion/Division [KKY02]. Inversion [CGH00a, Has01a, JP03]. Inversion [IWBRS].

Investigating
[WB07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08]. Invitation [Bar02]. Invited [FGM00a, Lan00d, DRS05].

involutional [SHH07]. IP [CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSEC [Vau02, CGBS01, Dau01a, KMM+06, SKW+07, FS00, FS03a, XLMS06].

IPSec-Compliant [CGBS01]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFSH09]. Irreversibility [ZWC02].

ISBN [And04, Dwu03, Eag05, For04, Gum04, Inm03, Pag03, Puz04, Top02]. Island [CSV09, KGL04, Kim01, Lee04b, IEE07].


Isomorphisms [CPP04]. Israel [Jo01].

ISSAC [Je08b]. issue [FOP06, FOP06]. Issues [BDF+01a, BH00a, Hil00, KRV01, Mea01, PB+07, SEF+06, MKY08, Fat02b].

ISW’97 [You01]. IT-Architectures [RM02]. Italy [AAC+01, AL06, BCKK05, BC05b, CGP03, dCdVSG05, IEE04].

Itanium [CHT02, Int00]. Itanium-based [CHT02]. Iterated [Jou04, Oni01].

Iteration [Che03]. IV [Sch01c, HSH+01].

IWBRIS [LST+05]. IWDW [BCKK05, CKL05, KCR04, PK03].

[Des02, GL05, IZ00, Vau05a, Wri03]. Japan
[Ann00b, Mat02, Okx00, Coc02b, Smi01b].

Japanese
[IY00]. Java [Ano04b, Mar05a, WBL01, Ano02c, Ano03a, Ano04b, Ano04c, AJ01a, BCS02, Bis03a, BJvdB02, CMG+01, Che00, CCM05, Coo02, DPT+02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hun05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Vir03, Wei04, Win01, Zea00, ZFK04]. Java-Based
[EM03, DPT+02, GW08]. Java-Lösung
[Ano04b]. JAVA-Ring [WBL01].

JavaCard [AJ01a]. Javacards [Cim02].

JavaScript
[TEM+01]. java.crypto [Win01]. JBits2M
[MP01a]. JCCM
[CMG+01]. Jean
[MFS+09]. Jeju
[CSY09, Lee04b]. Jeng
[QCB05b]. Jenness
[Sal03b]. JICC
[HYZ05b]. Jim
[Coc01a].

Job
[MYC01]. jobs
[Oue05]. Joel
[Gum04].

Johannes
[Lee03a]. John
[And04, BZ02, NH03, Rot07, Coc03]. Joins
[Bar00c, Con00]. Joint
[ADI09, ADR02, CR03, HYZ05b, HYZ05a, Puc03, M09].

Jörg
[Fal07]. Jose
[Pio06, Pre02b]. Journal
[LLLZ06a]. Journey
[FF01b]. Jr
[Kat05b].

Julius
[Cha02]. July
[ACM01a, CZ05, Jef08, KJR05, May09, PPV96, Roy00b, Sch01c, S+03, Uni00a, Uni00b, Uni00c, Uni00d, ZJ04]. Jump
[MP00]. June
[ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM07, ACM09, ACM10, AL06, BS03, BS01b, BCDH09, BC01, CZ05, FMA02, IE05b, IKY05, JYZ04, KGL04, KN03, KM07, PPV96, TB02, USE01b, USE01a, USE02c].

Just
[ABB+04, Gut02a, Car01].

Kahn
[Gas01]. Kaikan
[Ano00b].

KASUMI
[KYH01, KSH01, SM02].

Katholieke
[BB09]. Katz
[Bar00a].

Kecceck
[BDVP09].

Keep
[DM07b, Lys08, FS04].

Keeping
[SEK01, SEK02]. **KEM** [NMO05].

**Kerberos** [BCJ+06, Coc01a, Gar03b, Hil00, Ito00, LLW08a, MJ01, MPPM09, Rub00, Smi01a, Wac05, WD01, Wit01]. **Kerckhoffs** [KMZ03].

**Kernel** [Int00, Mor03, BK05, HB06].

**Key** [ANS05, ASW00, AK02a, Ano01b, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BH06, BDG+01, BDZ04, Bar00a, BPS00, BPR00, BBM00, BBDP01, BM03b, BDTW01, BM01c, BCP01, BCP02a, BCP02b, BM01c, BST02, CK02a, CK02b, CHK03, CHK05, CPP04, Che01a, CT08a, CHKO08, CCM01, CKM00, CS02, CS03b, CS03c, DPV04, DJ01, DSM05, Des00c, DBS01, Des02, DG03, DY09b, DKXY02, DFK+03, DGH+04, DBS+06, ESG+05, EP05, ES00a, FL06, FKSW00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Go03, GH01, GC01b, GSB+04, Guf04b, HNZI02, HCD08a, HCD08b, HLLL03, HTJ08, HG05b, HWWM03, HMvdLM07, Hwa00, HLL04, IZ09, Iwa08, IM06, JRR09, JW06, JXX05, JZCW05, KY00, KOY01, KY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, Ku02, KOMM01, KY01e, Kur01, KI03, LCK01, LLL02, LP03, LV00, Len01, Lin03, Lin00b, MPP00, Mac01, MSJ02, M+00, May04, MR01b, MR01c, Ml03a, Mu01a, Muto00, N003b, NA07, Ngu05, NBD01, NSS00, OT000, Or000, PHK+02, PR01, Poi02, PM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sa01e, Sin01a, SK00, Ste01, ST01c, TSO00, Tan07b, TT01, VV07, Wal03, WZW05, WH01, WCO0a, Wo00, WBD01, Wy02, YKMY01, YI01, YG01c, YDM06, Zhe02a, ZWY02, AJ08, AUW01, AKNR04, AFB05, BHM03, BBN+09, Ben01a, BB79, BG08, BGG+02, BD00b, Bra01a, BCP07, BMA00a, BMA00b, BMA00c, BD04b, CCT08, CL02b, CZ05, CYY05, Che04a, CHC04, CY05, CLC08, CKRT08, CJ04, Cho06, CHH+09, CJL05]. **key** [DFM04, DMT07, DW09, EKRMA01, ED03, EH00, FM02, FP00, GML02, Ga01, GH08, GL06a, GRM05, GKM+00, GS01, GL06b, GMW01, HCD08a, HCD08b, HAN04, HGH06, HLL03, HTJ08, HG05b, HWWM03, HMvdLM07, Hwa00, HLL04, IZ09, Iwa08, IM06, JRR09, JW06, JXX05, JZCW05, KY00, KS05a, KOY09, KY01e, KY02c, KLC+00, LFK03, LLL04, LLL05a, LKY05b, LKY05c, LKY05d, LCP04, LHC08, LKJL01, LSH00, LS01c, LCC05, MWS08, MMK00, MP08, Mi08, Ml01b, NP02a, PS08a, P106, Pe09, Pe04, PC09, PS08a, PLJ05b, Pri01, RH03, SN00, SL07, SRJ01, SBZ04, Sh05e, Sh05g, SL05a, SW05, Shp04a, SC05b, SIR04, SLC05, Sun00b, Sun02, SP02, SC05b, SC05c, CCS05c, TP07, TO01, Ts06, Ts05]. **key** [Tse07, VS01, Vau05a, VK08, WDLN09, War00, WGL00, WV00, WC01b, Wu01, WL04b, WHHT08, XH05, YY05, YC09, YS02, YS04, YY05b, YY05b, YPKL08, ZL01, ZC04, ZK05, ZSM05, ZYW07, ABB+04, GL05].

**Key-Based** [Sha01e]. **Key-Dependent** [Go03]. **Key-Exchange** [BH06, CK02a, KS05a]. **Key-Insulated** [DKXY02]. **key-management** [JW06]. **Key-Privacy** [BBPD01]. **Key-Recycling** [DP05]. **Key-Share** [CT08a]. **Key-Sharing** [HNZI02, WBD01]. **Keyboard** [ZZT05]. **Keyczar** [Law09b]. **keyed** [Kuh08, SR00, FIP02a]. **Key-Hash** [FIP02a]. **keying** [ABB+04, Che08a, EGK08]. **Keyless** [Qu01]. **Keys** [AOS02, AF05, AF106, BT02, BMD00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, Lc00, MN01, MRL+02, On01, PS00, Sma01c, Str02, TvdKB+01].
Leighton [Rub00]. Leighton-Micali [Rub00]. Length [AR01, BR00b, CKN00, CHJ+01b, Mō03a, RK06].

Length-Preserving [Mō03a]. Leonard [Coc03]. Less [YKMY01, BD00b]. Lessons [GBS+04, KFSS00]. Lest [HSH+08a, HSH+08b, HSH+09].

Letters [AR01, BR00b, CKN00, CHJ+01b, Mō03a, RK06]. Level [EP05, MV00, TV03, BDN00, DHL06, KVN+09, SS03].

Levels [CUS08]. Leveraging [BRTM09]. LEVIATHAN [CL02c]. Levin [AC02].

LFSR [Jam00, JZCW05]. LFSR-Based [Jam00]. LHL [Pei04, YRY05a]. LHL-key [Pei04, YRY05a]. Li [JW01, KCL03, SZS05, QCB05a, SCS05b, ZK05].

Liaw [TJ01b]. Liberty [Lan04b, Ano00c]. librarian [PBV08]. Libraries [Fin02, MK05b]. Library [KSZ02, Lau05, Law09b]. Libre [Len09]. Lies [Gan01b, Sch00d, Swa01, Ste05c]. Life [Cop04b, GBS+04]. lifecycle [HL06].

Lifetime [Coc01a, CPG+04]. Lifting [CNS02]. Light [WT02]. Light-Weight [WT02]. Lightweight [EPP+07, Mal02, CH07a, CL09, MP07].

Like [Coc02a, PSC+02, VMS05, BCDM00, CWW00, DLP+09, Egh00, EBS01, Gou09, HSL+02, HL04, SKU+00, SLL+00].

LILI [JJ02a]. LILI-128 [JJ02a]. Limitations [Gua05, Fis01a]. Limited [AK02a, Buh06, Tse07]. limiting [CCK04b].

Limits [CWR09]. Lin [CC02b, CHY05a, KTC03, YY05b]. Line [Cho08a, DL98, Jan08, Lai07, Lu02, SK06, YLLL02, Baut05, BCS02, DL07, Luk01, Shi05].

Linear [BDK02a, BDK02b, BDQ04, CGFSHG09, CS05a, CHJ02, Cou01, CM03, Cou03, CDM00, CD01a, CDG+05, FM02a, FM02b, GS03, GBM02, HLL+01, Hug02, JJ00d, Kan01, KMT01, Kin02, KM01c, KRS+02, KY01c, LLL+01, LS05a, NPV01, PSC+02, PG05, PZ02a, SNWX01, STK02, WF02, YSD02, BD04a, Bu09, CKB+03, Cou04, GHPT05, Kuk01, LLL04, Reg05, Reg09, RSQ03, Se00, SLL+00, TM01].

Linearization [DD+06]. Linearly [ADD09]. Lines [SPA04]. Linguistic [CD01]. link [LPV+09]. link-layer [LPV+09]. linkages [ZAX05]. Linking [GW00]. Linux [Lin02, ASW+01, FR02, Fin02, Fri01, GJ05, Gan08, GPR06, JEZ04, Lin02, Mor03, Pri00, Shu06, Sta02b, Sta05].

LISA [USE00c]. list [AGKS07]. little [Lam07, Sch05c]. Live [Lam07, Lov01]. Lived [GSW00]. lives [FNRC05]. living [BCB+05].

LLL [CKY05, NS05c]. Load [HL06]. Loads [GH02]. Loan [SONO02]. Loaning [Bla01c].

Local [NABG03, Lau09]. Locality [MFS+09]. Localization [WLT05b, CL09]. Locally [Vad03, Yek07].

Location [HY01, KZ01, LNN+08, Buh06, SG07]. Locations [Kra02b]. Log [Gen00, HN04]. Logarithm [CNS02, Che04b, CCW02, GV05, GPP08, LW02, Hsu05a, HL05d, JLL01, LH05, Sch01c, SCL05, SLC05, YAS08].

Logarithmic [EGK08]. Logarithms [CS03a, JL03, LHL03a, LTH05, PLS05, QCB05a, Sha05c, Sha05d, SCS05c]. Logging [Fox00, MT09]. Logic [BPST02, Cop04b, KBD03, Li01, Nie02d, SQ01, SC01, TV03, BDNN02, BD04a, DZL01, WZB03, dH08].

Logic-Based [KBD03]. Logical [Kra07, Zha08]. Logics [IK03]. Login [LL05c, CCK04b, CJT01]. Logistic [KJ01].

Logo [LZ09]. London [Pac03, Top02]. Long [ABRW01, Dur01, GSW00, Gro03, PCC01, BMV06, ISO05, SGMV09].

Long-Lived [GSW00]. Long-Term [ABRW01, Dur01, BMV06, ISO05, SGMV09]. Look [Bon07, Has00, Lut03]. Look-up [Has00]. Looking [ASW+01, Ano01g, Cla00b]. looks [Nis03a].

Lookup [MFFT05]. loop [KVN+09].
loop-level [KVN+09]. Loopholes [Ste01]. Lorenz [GHDGSS00, Sal00a]. Lorenz-based [GHdGSS00]. Losing [Sta05]. LosLobos [Pri00]. Loss [LHS05, Mit00]. Lossy [AIP01, HSKC01, PW08]. Lost [PY06, Rob02, Rob09]. Lösung [Ano04b]. LosLobos [Pri00]. Loss [LHS05, Mit00]. Lossy [AIP01, HSKC01, PW08]. Lost [PY06, Rob02, Rob09]. Lösung [Ano04b]. lot [Cla00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [Lud00]. Louvain-la-Neuve [QS00]. Low [Ano00b, BM01b, CH07c, GST04, HNZI02, HGR07, JP02a, KMB09, RMH03b, RMH03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09, Fan03, HLL03, LC04a, WLHH05, WY05, ZYW07]. Low-computation [Fan03, LC04a]. Low-cost [CL09]. Low-end [SU07]. Low-Exponent [SZ01]. Low-overhead [HGR07]. Low-Power [Ano00b, JP02a, KMB09, CO09, ZYW07]. Low-State [GST04]. Low-Weight [CH07c]. Lower [BDF01b, BP03b, DIU05, GT00, GGK03, PS02a, Shp03, WW05, Shp99]. LSB [CS05b, FGD01, WMS08]. LSB-encoded [WMS08]. LSD [HS02a]. Lu [QC305b]. Luby [MP03, Pat03a]. LUC [LNS02]. Luminy [PPV96]. Lymph [DV05]. Lund [Joh03]. LUT [CC02a, TL07]. Luxembourg [Bir07]. Lyndon [GS01, VS01]. Lynn [Hes04a]. LZ [AL04]. L.Z.-77 [AL04].

M [DNRS03]. M8 [TM01]. MA [ACM10, JQ04, KI05, KP01, Nao04, Pag03]. MAC [BKN04, CKM00, KI03, LPV+09, Vau01, Cra03]. MacDES [CKM00]. Machine [Mal06, Pro00, Cas06, Kid00, Pau02b, SWR05, WQ05, Win05b, HM01a, Pet08]. Macraigor [Ano02b]. MACs [BPR05, BR00b, BM01c, Sem00]. Made [Ste05b]. Madison [FMA02]. Maelstrom [MYC01]. Magic [DNRS03, Hro09]. Magyaryik [dVP06]. Mail [ANR01, Cos03, KS00a, Law05, LL04b, All06]. Mainframe [Web08]. mainstream [Bjo05]. Maintaining [MJF07, Zho02]. Maintenance [NABG03]. Maiorana [Car02]. Majority [GKK007, SVS08b]. Make [BP06, Ber03, Sin02]. Makes [Pau09]. Making [CRSP09, Gar01, Lut03, Mit00, Oec03, Per05, Wri05]. Malaysia [DV05]. Malaysian [Kha05]. Malicious [HLC08, SZ03, YR04, Tsa06]. malleable [DW09, FF00, PR05]. Malware [LH07, SZ03]. Man [Gen04a, Urb01]. Man-in-the-Middle [Gen04a]. Management [ACM03a, ACM04a, Ano02b, Ano02c, BP07, BW07, ELYS01, FMA02, GK04, Gut04b, KB06, Lin00b, Sha02, Woo00, Wy02, ASW00, AJS08, AFB05, Cha05a, ISO05, Jan00, JW06, KHYM08, LMW05, LPM05, LR01, LK01, MKKW00, RH03, SRJ01, Sen03, UP05]. manager [Kh03, Sha01a]. Managing [MA00a, MA00b, NDJB01, Oue05, PTP07, PBB02, To00, BJ02, Kov03, KH03]. Mandrake [TvdKB+01]. MANETs [STY07, DF07]. manipulation [SWR05]. manuscript [GG05a, Rup04]. manuscripts [MAaTxx]. Many [BB02, Di01, MP03, Di03, SVDF07]. Many-Round [MP03]. many-to-one [SVDF07]. map [KJ01, Lee04a, PC05b, SL09]. Maple [Cos00, TT00]. mapping [Tan01]. Maps [BGLS03, BMS03, CL04a, LLL+01, WP03, JK01b, MA02]. Maqasid [MAaT05]. Marcel [Ir03]. March [BDZ04, Bir07, Bla03, HR06, PY05, SIl01, Uni00g, Uni00h, YBr06]. Marian [Kap05]. Marjan [BCB+05]. Markers [FBW01]. Market [Bar00a, Swi05]. Marketplace [PLW07, VN04]. Markov [KW03]. Marks [Ano01c, YSS+01]. Markup [Uni00a, Uni00d, Uni00c]. Marrakech [IEE09a]. Marriott [USE01b, USE01a]. MARS [BF00a, BCDM00, FCR00, IBM00, IK00, KSS00a, KS00b, KS001, SOTD00]. MARS-like [BCDM00]. Mary [Ree01, Sin09]. Maryland [ACM05b].
ACM05c, ACM09, SMP+09, GL05]. masked [AHS08, Lau08a]. Masking [CHJ02, CT03, GK02, Lav09].
Massachusetts [IEE05b, USE01b, USE01a, IEE03]. massively [FP00]. massively-parallel [FP00]. Match [JJ00a, LLC06a]. Matching [ABM08, Len01, UBE09]. materialized [MS09]. Materials [SLT01].
Massively [FP00]. Match [JJ00a, LLC06a]. Matching [ABM08, Len01, UBE09]. materialized [MS09]. Materials [SLT01].
Mathematics [BP06, Lew00, Nie02d, Sch00a, Sch01c, S+03, Sch04a, ST06, XNK+05, YGZ05].
Math´ematiques [RSA09b, PPV96]. Matrices [TL07, CFVZ06, LMTV05].
Matrix [CV03, BF06a, OS07]. Matroids [CDG+05]. Matsumoto [DDG+06, YG01a].
Mature [Tro08]. Max [Di 01]. maximal [H¨uh00, HJW01]. maxims [Bau00, Bau02a].
Maximum [KMT01, ZC00, DW01]. May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bih03, CC04a, Cra05a, DRS05, IEE01b, Knu02, KN01, MJ04, MS05a, FM00, Pif01, Pre00, TLC06, Uni00f, Uni00e, YKL02a, Pau02a, YJ00]. Mbps [LMP+01]. McClure [Gum04]. McEliece [CF501, KI01a, Ki01b, Loi00, LS01c, Sun00b]. McEliece-Based [CF501]. McFarland [Car02].
McGraw [Gum04]. McGraw-Hill [Gum04]. MD4 [DG02, WFLY04]. MD5 [Eke09, WFLY04]. Me [AC03, CB03, CNB+02]. Mean [Bar00c, KLML05, Ver06b]. Means [LMHCETR06, Nis03a]. measure [Lav09].
Measurement [An002c, kc01, CO09, FXAM04, RW07]. measurement-based [FXAM04].
Measures [CB01, KQ01]. Measuring [Siv06]. Mechanising [Be01]. Mechanism [LXM+05, WY02, CL08, GH08, LCP04, ME08b, WAF00]. Mechanisms [BACS02, CJK+04, Lin00a, MD04, Mir05]. mechanized [dH08]. Media [Hei07, An002b]. Median [Cap01]. Mediated [DT03]. mediator [SBG05]. mediated-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, AJ08, CCM05, DK08, DGN03, HNZI02, HDbJL01, KCH+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05]. Memory-Bound [DGN03]. memory-safe [Oiw09]. Memoryless [Bar02]. MEMS [ECG+07]. MEMS-Assisted [ECG+07].
ment [CAC06]. menu [Mea04]. Mercy [FL02a, Cro01]. Merkle [CDMP05, JLMS03]. Mersenne [An003c]. Mesh [LPZ06, ZTP05, KB09, LZP+04, YPSZ01]. Meshes [BG108, Lav09]. Message [BR02, BWBL02, BDF01b, CV03, C02c, FIP02a, FGM00b, Jut01, OM09, SN04, WS03, Zol01, CCH05, Cj05, Gav08, HW05, MD04, Sha04b, TJC03, Wai01, ZF05, ZAX05].
Messages [Ara02, AR01, BR00b, C1J+01, DS05, Sch09, Wri05, BCD02, Bih02, BB79, Lmn09, SP79]. messaging [Opp01, RR05]. meta [SM08, PL05a, QC05b, Sha05d]. Meta-He [PLJ05a, QC05b, Sha05d].
meta-learning [SM08]. metadata [CD05, FJ04]. metamorphic [CS05]. Metaphor [CNB+02]. Metering [BC04b].
Method [BDTW01, GHK+06, GL00, Gro01, HRS02, Hq05, JKK+01, Mlo02, OKE02, OT03a, OT03b, SOH01, TGD01, TSO00, WH09, WNY09, ZL05, AMRP04, DWW05, JL03, M, MFK+06, WG02, WWT08, kWPW01, WLW04, YCL07, CHJ+01a]. Methodologies [SPM02, ND04]. Methodology [VMS05, HM02a]. Methods [BCDM00, FD01, Kin00, Lan00d,
Mea01, Neu04, Sal05b, Sch06a, SM07, TNM00, Vir03, Ban00, Bau02a, BGM04, BCHJ05, CM05b, GKS05, JZCW05, LMSV07, Mal06, SSST06, Shp99, YW06].

Metric [LBGZ01, LBGZ02]. Metrics [LZ01, NP07]. Mexico [Buc00a]. MGC’05 [ACM05a]. Miami [Des02]. Micali [Rub00]. Michael [Ter08]. Micro [ASK07, Eng00, Ste05c]. Micro-Architectural [ASK07]. microcontrollers [GBK01]. Microelectronics [IEE09a]. Microprocessor [Web08]. Microprocessors [LKM+05]. Microscopic [MYC01]. Microsoft [Bon00, Ste05b]. Middle [Eag05, Gen04a, HG07, Kin01]. Middleware [ACM05a, KRV01, LGS01, MBS04]. Migration [Pat02a]. Mikhailovsky [Puz04]. Milan [cdVSG05]. military [Ark05]. Million [Ran55, Ran01, Ano03a]. MIME [Dav01b, Dav01c, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [FBW01, FGM01, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LPM05]. Mining [LP00, Lut03, HLL+02, Mal06, Men03, PIn02, PIn03, ZY08]. MinPASS [HS01]. Minos [CC05e]. MinRank [Cou01]. Minutiae [UBE09]. Minutiae-based [UBE09]. Misbehaving [JQV01, SBB05]. Misinformation [CBZ+01]. Missed [TvdKB+01]. MIST [Wal03]. Mistakes [Ste05b]. MISTY [KYHC01, Küh01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Küh02b]. Mithra [Fre03]. Mitigating [NLD08]. Mix [JJ00a]. Mixed [SKR02]. Mixes [Mö03a]. Miyazaki [WHL03]. MMM [GKS05]. MMM-ACNS [GKS05]. Mnemosyne [RH02, HR02]. Mobile [Cha05a, Dim07, GN06, JP02a, KZ01, KB07, KC02, KHD01, LCK01, Mal02, MM02, PL01, RKZD02, RdS01, RC01, Rot01, SH00, ZYM05, CC05c, CJ03b, DHMR07, HYS03, ISTE08, KXD00, LC03, LC04a, Lin07, LKZ+04, Par04, Pau02a, SSM+08, SL05a, TM06, TW07, Tse07, Wan04a, YC09]. mobile-commerce [YC09]. mod [TM01]. Modal [GN01]. Mode [BR02, Dwo03, HR03, HKR01, KSHY01, SLG+05, WB02, Hey03, RBB03, ZL04c]. Model [Abe01, Abe04, BH05, BPST02, BL02, CLK01a, CS07c, CPhX04, Chi08, CT09, DPV04, DFS08, Din01, Din05, ECM00a, Gra02b, HLC08, KW03, LJL05, MND+04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SFDF06, TZDZ05, Vad03, WCZ05, WT02, WvD02, ZGLX05, ZP05, ZS05, BKW03, CUS08, Damm00, DFS05, GM008, HLM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SRJ01, TP07, DY09a]. Model-Based [Sal05b]. Modeling [AADK05, CCD+05, HMvLM07, KS05a, ZP05, Laf00, SS04]. modelled [BG08]. Modelling [HCD002, Puc03]. Models [Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01a, SC02b, vOT08]. Modern [Gol99, Mao04, Pag03, SM07, Swe08, Fur01, IM06, KL08, Mol05, SE01, Lut03, Lee03b]. Modes [DGH+04, Dwo03, GD02, Gol01d, HSH+01, JMV02, JKR01, Jut01, KY01a]. Modified [CHC04, HPC02, JY01, KJ01a, ST02, Che08a, CJT01, HWW03, LL04a, LL05a, kWPvLwW01]. modifying [CSV07]. Modular [BIP05, BK09, CM030, CH07c, Dhe03, FP00, Gro01, Har06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wal01, WL04a, HSD+05]. Modulation [AS01c, Che07]. Module [Ano02b, LM00, SGM09, ARJ08, BG09]. Modules [FIP01b, NIS01b, GJ05, JEZ04, Se00b]. Moduli [Bai01b, GMP01b, Wal01]. Modulo [ACS02, Gon06, Gro03, MFFT05, Zhe01, Wan05]. Modulus
[Ano01i, CGH00a, CDL+00, SZ01, WY02, WS02, LKY00, WWTH08].
Modulus-Based [WY02]. Mollin [Kat05b]. MONA [KMS01]. Mondriaan [BF06a]. Money [Ano01a, YKMY01]. monitor [MK05a]. Monitored [PS05]. Monitoring [AK02a, BCS02, Por06, Bej06, GXT+08, ZGTG05]. Monitors [JT05]. Monks [Eag05, Kin01]. monoalphabetic [GPG06]. monolithic [GHdGSS00]. Monotones [WW05]. Monte [Bi09, Sug03]. Montereau [USE02c]. 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]. MPEG [LHS05, MLC01, SG07, YZDW07]. MPEG-4 [SG07]. MPEG-4[SG07]. MPEG [Che01a]. MRF [Che01a]. MRM [TIGD01]. MSP430x33x [GBKP01]. MSXML [TEM+01, Hei01]. Mu [CJT03]. much [Con09]. Multi [ARR03, BBM00, BR06, CCD07, CJK+04, CDM00, CDG+05, DLY08, DLJT01, FGM001, FW004, Gen04a, HM01b, HS07, JLL02, Kur01, LV07, LLL04, Tsa01, ZJ09, CLOS02, CC05a, CHY05a, CHY05b, DLZ01, FWCT05, GMMS02, HHYW07, HHW05, HC04b, HL04, HLL03b, LCZ05b, LW05c, NC09, PW05, SC05a, TW05, TY04, YCH04]. Multi-applications [DLJT01]. Multi-Authority [JLL02]. Multi-channel [ARR03]. Multi-designated [LV07]. Multi-Domain [CJK+04]. multi-hop [NC09]. multi-linear [LLL04]. Multi-party [CDM00, CDG+05, FGM001, FWWT04, HMO1b, LLL04, CLOS02]. Multi-property-preserving [BR06]. Multi-Proxy [ZJ09, HC04b, LW05c, TY04]. Multi-Receiver [CCD07]. Multi-recipient [Kur01]. multi-scroll [HHYW07]. multi-secret [CC05a, CHY05a, FWWT05, PW05, SC05a, YCH04]. Multi-server [Tsa01, LHL03b, TWL05]. Multi-Servers [HS07]. multi-signature [HWH05, HC04b, HL04, LCZ05b, LW05c, TY04]. multi-stage [CHY05b]. Multi-trapdoor [Gen04a]. Multi-user [BBM00, DLY08, GMLS02]. multi-valued [DLZ01]. Multiagent [ZS05]. Multiagent-Based [ZS05]. Multicast [AIP01, BPS00, BDF01b, ASW00, GIKR01, GL06b, JA02, KB09, MP08, PCS03, YC08]. Multicollisions [Jou04]. Multilevel [LN04]. Multimedia [AAK09, FMS05, GA05, HL07, Sun05, WLL09, DY09a, DKU05, Lao00, SG07, YC08]. multimodal [PY08]. Multiparty [BG09, CDN01, DI05, GIKR02, OZL08, CDDS00, HTO4, IKOS07]. Multipath [SK05b]. Multiple [AIK+01, Ara02, BDQ04, CLK01a, CLK01b, CHDSS02, Che08b, DK05, Har00, HLT01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJO4, DM07a, HL000, KC09, Sha01d, SW05, TCC02, YW05, YRY05b]. multiple-key [Che04a, CJO4, SW05, YW05, YRY05b]. Multiple-watermarking [Che08b]. Multiples [HR00]. Multiplication [AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02c, KKIM01, ML02, NMSK01, OS01, Tan07a, WA01, BIP03, DwWmW05, FP00, GD05, HS00, Miss06]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KO03, MFFT05]. Multiplier [HK40+5]. Multipliers [CMJP03, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver [HSZ01]. Multiresolution...
Multisignature
[CL00, WH02b]. Multithreaded [Zha00]. Multivariate
[DY09b, BGP09, FP09]. Municipal
[MJF+08]. Music [MNS01, XMST07].
multisignatures [CL00, WH02b].
multisignatures [CL00, WH02b].

Multithreaded [Zha00]. Multivariate
[DY09b, BGP09, FP09]. Municipal
[MJF+08]. Music [MNS01, XMST07]. Mutually
[WC01]. MYCRYPT [DV05].
mysterious [Bel07]. Mystery [Rug04, GG05a].
Mystery [Rug04, GG05a]. Myths [GO03, kc01].

Municipal [MJF+08]. Music [MNS01, XMST07].

Mysterious [Bel07]. Mystery [Rug04, GG05a]. Myths [GO03, kc01].
Napoleon [Urb01]. Narrowing [MT07]. NASA
[Wil99]. Nation [Lan04a]. National
[BWE+00]. National-Scale [BWE+00].
Natural [ARC+01, Top02, WMS08]. Nature [Pag03].

Naval [Goo00]. Nazı [Hau06, KS04]. NC
[AIK04]. NCP [SQ01]. Near
[BC04a, DPS05]. Near-Collisions [BC04a].
Necessary [LCK03, MN01]. Necessity
[SBZ01]. 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, LKLJ01]. Netherlands
[Knu02]. Nets [ADK05]. Netspionage
[BK00]. Network
[Ano02b, Bar03, BGOY08, Con04, CLZ02,
Dim07, FBWC02, Gum04, Har05a, IKY05,
JYZ04, KKK03, KPS02, Ken02b, LMP+01,
Lu07, Mal02, NN02, PJDH09, Poo03,
RCBL00, RC05, Sty04, TLYL04, VMCO2,
YC01, ZYH03, ZS05, Bn06, CJ03b, CMS08,
Coc01a, DWML05, GKS05, HLL+02, LC03,
LPV+09, ME08a, MSK03, Mi080, Pri00,
RAL07, Sch00c, Sta02a, TIS07, Vac06,
Wy05, YLT06, ECM00a, ECM00b].
Network-Attached [RCBL00].

Networked [HLL+02]. Networks
[AAQ05, BJLS02, CGM07, DBS+06, Fin06,
GPCS08, Gor05, JKR01, KZ01, Ken02a,
KH05, LNL+08, NABG03, PR01, RZD02,
Sin01a, WT02, Zea00, ZYN08, ZWCY02,
AJ08, BBG+02, BC05b, CCMT09, CGP03,
CBD+05, DHMR07, ETMP05, HJ07,
HMDL07, JRR09, KXTZ09, KYHM08,
KB09, LDH06, LHC08, LW05a, Lin07, LN04,
LKZ+04, MWS08, MJF+08, MS09b, NC09,
NL08, PCSM07, PS08a, Pat02b, SLP07,
SSM+08, TP07, TM06, TCR03, TW07,
WDLN09, YC07, ZSJ07, ŽBLvB05,
Ano02b, CS08b]. Neural
[KMS02, PR01, YC01, YC07].

Neural-Network [YC01]. Neveu
[QS00]. Nevada [ElvS01, IE01a]. Never
[Wei00, Han06]. Newfoundland [NH03].

Newman [Pag03]. Newmanry [Sal01a].
News [Ano03b, Bar00a, Bar00b, Bar00c,
Cla00a, Coc01a, Coc02a, Coc03, Coc03,
Eng00, Fox00, MYC01, MP00, PM00,
Pau02a, Pau02b, Pau03, Pau09, Pri00,
CAX03, CAC06, Sta05, Raj06]. Newton
[KT06]. Next [ESG+05, Mcl06, TV03,
Web08, BDO4b, ISTE08, RR03a].

Next-Generation [ESG+05, Web08]. NFA
[DIS02]. NFS [Sta02b]. NICE [J00c].
Nimbus [Fur02a]. Nine [Tat05]. Ninth
[USE00d]. NIST
[BG07a, Dra00, Hri09, Ke05, RRS06, SF07].

NIST-Recommended [Ke05]. NMAC
[RR08]. NMAC/HMAC [RR08]. NNAF
[SwMwW05]. No
[Sta05, Sty04, Uni00g, Wei05, CC05b].

Nobel [MNT+00]. Node [BRTM09, Fox00].

Nodes [ZYN08, RAL07]. Noise
[SW03, AG05, MPSW05, MS09b, PC00].
noise-based [PC00]. Noise-tolerant
[BKW03]. noisy [HGNS03]. Nominative [PL01]. Non [CHK05, CZB+01, DN00a, DDO+01, DW09, FF00, Fis01b, Fis05, FGM00a, FGM00b, HNZI02, HJW01, IYK02, IYK03, JT01b, Kos01c, KO00, MSTS04, Nie02b, PHK+01, Pas05, SPK08, WBL01, DM07a, DS02, H"uh00, 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-maximal [HJW01, H"uh00]. Non-OOSD [CZB+01]. non-perfect [DM07a]. non-physicists [RP00]. non-quantum [IM06]. non-repudiation [HLL04, LSA+07, PR05]. non-trivial [KO00]. Non-Uniform [SP05]. nonce [CY05, LKY05a]. nonce-based [CY05, LKY05a]. Nonces [BR00a].

Noncontact [Sak01]. noninterference [DFG00]. noninvertibility [HR08]. Nonlinear [BP01a, BI05b, CV02, Che01c, LBGZ01, LBGZ02, SM00a, ZC00, BGPGS05, CFVZ06, KH08].

Nonmalleable [ABW09, DDN00, DDN03, PR08]. nonrepudiable [TYH04, YTH04]. nonrepudiation [HW05, OZL08].

Nonsecurity [Sch07]. Nonuniform [CU01].

Normal [Ran55, Ran01, GPS05, Mic01, RMH03a]. Normalization [VK07]. Norway [Ytr06].

Nose [Fox00]. Notation [Eag05, Kin01].

Note [CWY05, FSO2, GMP01a, GIS05, KCP01, Ros00, MF07, PC05b, Yan02, Zha06]. Notes [KSF00]. Nothing [Des00c, SR00].

Notions [BPS00, BN00a, CK02b, DKMR05, HU05, Kos01a, Des00a, KY00, PS04c]. Novel [CC02a, CYH01, CDTT05, CW09, MP01c, AJS08, BG08, CCS08, GB09, HG05a, SPG02, SCS05a, nSGFTL05].

November [ACM01b, ACM05a, BZ02, CKL05, Eke02, IEE00a, IEE02, Lai03, LL03, LL04c, MS05b, PK03].

novice [Dew08, Gou09]. Novo [BI09].

NP [AGGM06, FS08, HN06, AGGM10].

NP-hardness [AGGM06, AGGM10].

NPCryptBench [YLT06]. NSA [RC05].

NSS [GJSS01, HP01]. NT [Str01b, USE00a]. NT/2000 [USE00a].

NTRU [GJSS01, GS02c, HPS01].

NTRUEncrypt [HHGP+03, HGNP+03, HG07, JJ00b, NP02b].

NTRUSEN [HHGP+03, HG07, JZ09].

NTRUSIGN [HHGP+03, HG07, JZ09].

NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, DFS05, Dic03, DGP07a, DGP07b, DV08, EAG05, EHK+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05, Ket06, KM01b, LMHCETR06, LNS02, MN01, NR04, RSN+01, SP05, Sch06b, Shp99, Shp03, SFDF06, TWNA08, TL07, TZN09a, TZN09b, Vav03, Wal00, Yan00, YKLM02b, Aam03, AUW01, BK07, Bel08, BGPGS05, BG08, BG09, BG07a, BGL+03, CNPQ03, CO09, DIM08, DGP09, FP00, HG05a, HGNS03, HLYWZ09, HP01, JAW+00, JL03, KH08, KSF00, Kin01, Lam01, Mit00, Nie02a, Nie04, Pan07, PSC+09, PSP+08, PC00, RGX06, Shp05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Wag03, Was08b, YZEE09].

Number-Notation [Eag05, Kin01].

Number-theoretic [NR04]. Numbers [HRS+01, HBF09, Ifr00, MN01, ST03b, AG09, HW08, KB39, Kir01, MFK+06, SS03, Shp05, Tip27].

numeric [AKSX04].

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

NURBS [Ben00].

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

Nyberg [Ara02].

O [Kat05b, Puc03].

OAEP [Man01, BF05, BF06b, Bon01, FOPS01, Sho01].
Obfuscated [NS05b]. Obfuscating [BGI–01]. Object [RSA00c, DHL06, MWM01, ST06]. object-oriented [DHL06, MWM01]. Objects [CCM05, ZTP05, PB01]. Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GKM+00, KKL09]. obscurity [MN03]. Observability [JQYY01]. observers [JL04]. Obstacles [KM04a]. Obtaining [Bar06b, BP03b]. OCB [RBB03]. occur [Web02]. Ocean [MYC01]. October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST+05, TTZ01, USE00b, ZYH03]. Octopus [Cla00b]. Oded [Lee03b]. odyssey [Gol08]. Oedipus [Lav06]. Off [AJO08, Coc02b, Oec03, Shi05, YLLL02, Bau05]. Off-Line [YLLL02, Shi05, Bau05]. Offering [YC08]. Office [Uni01]. officer [Kov03]. Official [BP01b, Coc02b]. Offline [WV01]. Offs [PS01c]. OH [BD08]. oil [RD09]. old [Lov01]. On-Demand [SEF+06]. On-Line [Lu02, BCS02, Luk01]. One [AK02a, BYJK08, CHL02, Che03, DIS02, Di 01, DW01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, KIO1a, KO03, KO00, LTW05, LMD04, ML03, PV06b, PG05, PLJ05b, RR02, Shoo0a, Uni00a, Uni00b, Uni00e, Uni00h, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, Di 03, DS02, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, YW05, YRY05b, ZW05a]. One-Time [HM02b, LMD04, RR02, CCK04b, DS02, LC04a]. one-variable [SV08a]. One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Shoo0a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, Mic02a, Poi00, YW05, YRY05b, ZW05a]. One-Wayness [KI01a, PV06b]. Ongoing [Sam09]. Onion [CL05]. Online [BDF+01a, BBKN01, Fis05, LCS09, Orto0, Rey01, ST01b, VAVY09, FNRC05, Fox00, Pan07, Try05, PT08]. Online/Offline [ST01b]. Only [BBK03a, CF01b, GL01, Hoe01, VV07, BCDM00, FKS+00, GHJV00, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Yas08]. Ontario [HA00, ST01d, VY01]. OOSCD [CZB+01]. OOSD [CZB+01]. Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Kius02, Lin02, Mea01, PM00, VDKP05, Ano03b, ETMP05, Mca08, Bar00b, Lin02]. Open-Ended [Kius02]. Open-Secret [Joh05]. Open-Source [Bol02, Gut00, McA08]. OpenCard [HF00]. Opening [CAC03]. OpenSSH [Bau01c, Sta02b, TvdKB+01, Hos06a, Mos06]. OpenSSL [Fri01, Res01a, Res01b, Sti06a, VMC02, YRS+09, Bei08]. Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL+08a, CGL+08b, CGL+08c, DGP09, KWDB06, MPH06, SETB08, TKP+08]. Operation [BR02, BKM07, Dwo03, EP02, Gol01d, HSH+01, JKRW01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BKM07]. Operational [WA07, GMG00]. Operations [BIP05, IMM01, KDO01, KS05b, LS01b, Ark05, operator [Wan05]. Operators [CH00]. opinion [BHM03, GS07b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Pau02b]. Optimal [Ba01a, BDDS03, CHJ+01b, CDF01, CF02, DPS05, DN07, GMW05, IR01, KO04, KS03, LZ09, Man01, MPW05, MP08, SNR04, YY01, vD04, BCD06, HKS00, 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, Nie02b, Pas03, Ano02c].
Oracles [BNPS02, BB04, KG09, RG09].
Order [AKXS04, Bai01a, CV02, KCP01, KCJ+01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, JZCW05, QPV05].
Order-Specified [Tad02].
ordered [HY03, WL05].
Ordering [Mea04].
Orders [HJW01, PS02b, HM00, Hüh00].
Ore [CHH01].
Oregon [ACM00, BCDH09].
Organization [JG07, MP00, C+02].
Organizational [PTP07, BJ02].
organized [AUW01].
Oriented [HR00, LZL+01, SKU+00, ZCC01, CHC05, CWJT01, DHL06, HWW04, LL06, LWZH05, MWM01, Sae02, Sha03c, TJO1a, WHHT08].
Origin [MABI06, MD04].
Original [JQY01].
Origins [Cop04a].
Orleans [USE00c].
Orsay [DPT+02].
OS- [CRSP09].
oscillator [BGL+03, GB09].
oscillator-based [BGL+03].
oscillators [SPG02].
Other [BF05, Ngu05, Wri05, Cla00b].
Otherworldly [MYC01].
Ottawa [AMW07, MZ04].
our [Sta05].
Outbound [Smi02].
Output [Dic03, YJ00].
Outsource [HL05a].
outsourced [MSP09, MNT06, YPPK09, YLC+09].
overcoming [CHC04].
Overdefined [CP02].
Overflow [FOBH05, Fry00, Ino05].
overhead [HGR07, IKOS08, RSP05].
overheads [XILMS06].
overlay [SL05b, YC08].
overlays [SK05b].
Overshadow [CGL+08a, CGL+08b, CGL+08c].
overview [SVEG09].
Ownership [AS01b, Nik02a, Nik02b, CL08, Lin01a].
P [Puc03, AKS02, KR03].
P1363 [IEE00b].
P2P [BRTM09, STY07, WN02, YLR05].
P2Ps [LHL+08].
PA [Cor00a, WWCW00].
PA-RISC [Cor00a, WWCW00].
Package [Win01].
Packet [BR09, WRW02, LWZZ05, CMS08].
Pad [LD04, DS02].
Padding [AR01, BCCN01, CKN00, CJNP02, KO03, LS01a, Man01, Van02].
Paddings [NP02b].
PadLock [Lud05].
PadLock-wicked [Lud05].
Page [IEE00b].
PageRank [GPC08].
pages [Fal07, Rot07].
paging [SZ08].
Paillier [CGHG01, DJ01, NSNK05, ST02].
Pairing [BKLS02, BF01b, BF03, CHSS02, GPS06, HCD08a, HCD08b, Kir03, PV06a, SKG09, Sma03a, GPS05, Lee04a, PC05b, VAVY09].
Pairing-Based [BKLS02, GPS06, PV06a, HCD08a, HCD08b, GPS05].
Pairings [Bon07, BGH07, Jou02, SB04, ZK02, CJKL05, LWZH05, LC05b, SW05, VK08].
pairs [LYGL07, Shp01].
Pairwise [CLL00, FM02a, HMvdLM07].
PAKE [HTJ08].
Palm [BDhKB09, WPS01, Wil09, Ano02b].
Palmprint [KZ09].
PAM [FR02, Sei00b].
Panama [BDPV09].
Panel [FL01b].
Panopticion [YN01].
Paper [MFS+09, Pet08].
Papers [Ano04a, Ano07b, Ano07a, Sch00b, Ytr06, Wil99, Bla03, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PK03, PT06, RM04, Sil01, AMW07, AJ01a, Bir07, BC05b, CZ05, CKL05, DR05, HH04, HH05, PC05a, PY05, WK06, Wri03].
Paradigm [BN00a, CS02, Gol03, KD04, YC01, BKN04, Can01a].
Paradigms [Des00b, Swa01, Hro05].
Paradise [USE00b].
Paradox [Che01b].
Parallel [MRH08, App07, AEMR09, CPhX04, CTL01, CNP03, CNB+02, Dam07, DM00b, JL08, KY02c, Lin01b, MFS+09, PS04a, RMH03b, SSO1a, BF06a, FP00, OS07, RMPJ08].
parallelism [KVN+09].
Parallelizable [BR02, MDS02].
parallelizing [Fis01a].
Parallizable [LKY03a, LKKY03b].
parameter [Wuc09].
Parameterization [KPM02].
parameterization [LZP+04].
Parameters [ZLK02]. Parametric [Vir03]. Paranoid
[Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Parascript [Ano02a]. Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a].
Parasitic [ETZ00]. Parascript [Ano02b]. Paranoid [Bau01a, Bau01b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Parasitic [ETZ00]. Parascript [Ano02b].
Parasitic [ETZ00]. Paranoid [Bau01a, Bau01b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Parasitic [ETZ00]. Parascript [Ano02b].
Parasitic [ETZ00]. Paranoid [Bau01a, Bau01b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Parasitic [ETZ00]. Parascript [Ano02b].
Parasitic [ETZ00]. Paranoid [Bau01a, Bau01b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Parasitic [ETZ00]. Parascript [Ano02b].
Parasitic [ETZ00]. Paranoid [Bau01a, Bau01b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Perfect [AJO08, CLLL00, DN02b, DSS01, Sun00a, DM07a, ZD05]. Perfectly [DMS00, KSR02, SNR04]. Perform [Kin00].

Performance [ACM01b, BH00a, DPR01, Dra00, EYCP00, FZH05, Int00, Ken02a, Ken02b, Kra05, LWK00, MM01b, NFQ03, PWGF03, PBTV07, SKKS00, SW00a, SB01, Siv06, SL00, SGPH98, WBRF00, WWCW00, WS02, XH03, YEP+06, ZEA00, AKNRT04, BZP05, CKL+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTW07, YGZ05].

performance-friendly [CRSP09].

Periodic [XQ07]. Periods [KKH03]. Perl [Sal03b].

Permutation [DMS00, HS+01, IYK02, KKG03, KO03, LSY01, DP02, IYK03].

Permutations [BPR+08, CHL02, KO00, MP03, KKKP05, VW00]. Persistent [AGT01, ST06]. Person [KJR05, LL+04, PK01, BS01b, KN03, Li05, LST+05, PY08].

Personal [Bar05, EHM00, SEK01, SEK02, TY05]. personalized [GPC08].

Perspective [LL01]. Perspectives [BMV06, SM08]. Perturbation [HWH08, ZY08]. Pervasive [BDhKB09, JW05, LKHL09, Lut03, Lut03].

Petersburg [GKS05]. petitions [Cal00a].

Petri [LKJL01, AADK05]. PGP

[McL06, BCH+00, Dav01b, Dav01c, JKS02, LUC06, Opp01]. PGV [BR02]. pharaohs [Pin06].

Phase [CDF01, Ig02, KL+02a, Che07, Che08a].

Phase-Conjugate [Ig02]. phase-shift [Che08a]. Phil [Bar00a]. Philadelphia [IEE08].

Philip [McL06]. Philosophy [Cop04b]. phishing [Bel04]. Phone [CAC03, Fox00]. Photonic [TWN08].

Photonic-based [TWN08]. Photons [Bar00c]. Physical [CGMM02, LR07, YKLM02a, GVC+08, UHA+09]. Physicist [BZ02]. physicists [RP00].

Physics [MYC01, Sch06b, BEZ00, BEZ01, Duw03]. Pi [OS08]. PIC [Fin02]. pick [Cla00b].

Picks [PM00]. PicoDBMS [PBVB01].

PicoDMBS [BBPV00]. Picturing [Pau03]. Piecewise [LL+01]. piling [Kuk01].

piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03]. PIPE [CBD+05]. Pipelined [MD05, Mis06]. PIR [BMI00]. Pirates [KY01d].

PISK [ECM00a, ECM00b]. Pittsburgh [IEE05a]. pixel [BCD06, LYGL07, WWTH08]. pixel-pairs [LYGL07].

pixel-value [WWTH08]. PKC [BDZ04, Des02, Kim01, NP02a, Vau05a, IZ00, KI01a, KI01b, ZC04]. PKC98 [HPC02]. PKCS

[Ch03, Man01, RSA00c, RSA00b, RSA00d, RSA00e, RSA01, RSA02, RSA03b].

PKCS#1 [CNJ00]. PKCS#11 [DKS08].

PKCS#7 [Dav01b]. PKI

[AL06, CZ05, KGL04, Ahm08, ES00b, ES00a, Gar03a, Gut02a, Hoo05, NDJ01, Orl00].

PKIX [FL01b]. PKP [JJ01]. PKWare [Bar00a]. Place

[USE01b, USE01a, GSO7b, IEE09a]. placement [GJ05, JEZ04]. Plain [Co03].

Plaintext [DN02a, Fur02b, G05, HLM03, Jo01, Kel02, KM01c, KI01a, MF01, CKN06].

Plaintexts [BR00a]. Plan

[CAC06, CPG+02, Gau08]. plane [WL02]. Planning [WCZ05]. plans [Ark05].

Platform

[Bar02b, MM02, PJ09, AJ08, ISE08]. Platforms [AI+01]. Play [WD01].

Playing [Shp05, BR04]. Please [Per03].

Pluggable [Sei05]. plus [Cop04b]. PODS [ACM03c, ACM05b]. poetry [MA06].

pogromca [Kap05]. Point

[GLV01, M02, NS05c, USE00b, WW06]. point-sampled [WW06]. Points

[BGI08, Gau02, Cla00a]. poised [CH00].

Poisoning [Kle07]. Poland

[AUW01, Bi03]. Polarization [HR05].

Poles [KS04]. Policies [AEV+07, ZP05, BNP08, LJ04, RN00a, RN00b]. Policy

[Bl01c, HQ05, AN00c, BFG08, BZP05, DFM04, Gor05, RVS09, Uni00b, RR04]. policy-based [BFG08]. policy-compliant
Polish [Kap05]. Politics [Cho08a, DL98, Jan08, DL07].

Polyalphabetic [GP06]. Polygonal [Ben00, BB00a, BGI08, SP04].

Polymorphic [CSW05], Polynomial [AF03, BIP05, BDG+01, Bul09, CU01, CJ03a, CH07c, CLZ02, Gon06, HR00, KL05, KY01c, KTT07, LW02, May04, Pli01, RMH03b, Sat06, LFW04, MRST06, SPZ02].

Polynomial-Time [CLZ02, KL05, Pli01, MRST06].

Polynomials [BLST01, DS08, FL06, Jam00, JJ00d, Lan04a, CHH01, FP09, GS09].

Pon [QCB05b].

Pool [BTTF02].

Popular [RR08, CAC06].

Port [Kra02b].

Portable [Hei07, Wan04a].

Portfolio [Ano02c].

Portland [ACM00, BCDH09].

Possibility [SF07, BGI+01, DOPS04].

Possible [Mur01].

Post [BBD09, BLRS09, Ber09b, HHG06, BD08].

Post-Quantum [BBD09, BLRS09, Ber09b, HHG06, BD08, BBD09].

Postage [Ble07].

Poster [TSO00, RN00b].

Potential [Kid02].

Potentially [Wal01].

POTSHARDS [SGMV09].

Power [AKS06, Ano00b, Av03, BI05b, BNPS02, Cry00, DPV01, DBS+06, Gir06, Has01b, HM02c, HBF09, IIT03, JP02a, JQY01, KMB09, KLY02, MOP06, Mas04, MS01, MMMT09, Mes00, Meso1, MG08, OS00, OS06, ÖO03, PSC+09, Sha01c, Sma03b, WS05, WC01a, vW01, CBSU06, CO09, Geb04, Mit02, OS08, XH05, ZYW07].

Power-Analysis [ÖO03]. power-attacks [Geb04]. power-aware [CBSU06].

Power-Sum [KLY02]. Power-Up [HBF09].

PP [Eag05, Pag03, Top02]. PPC [ASW+01].

PPK [YDKM06]. pq [KOMM01].

PQCrypto [BD08]. Practical [An01c, AR01, Ash03, ACJT00, BDK+09, BF05, BLMS00, CS03a, Cap01, CDR01, CS03b, DKO1, DRE00, FS03b, GSS03, GIS05, GH02, HQ01, HW01, IMA02a, INIT03, Kan01, LMV05, Lut03, LWO5a, 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, EZ00, Kim01, Mao04, NP02a, PY06, SB07, Van05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti95, Sti02, Sti06c, Lut03, Spr03]. practices [Ste02].

practitioners [PP09]. pragmatic [BM02a].

Practice [SU04]. Pre [Adl03].

Precise [Wal01].

Precision [SR06, LMC+03].

Precomputation [SLG+05]. predecoration [RSP05].

Predict [Di03]. predictable [Be08].

Predicting [AG09, BGPGS05]. Prediction [AKS06, SLG+05]. predictive [vOT08].

predistribution [HMvdLM07, RRR09, TP07].

Prefix [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 [BIW08, GXT+08, Mi08, V08].

Preservation [Che01b, Dur01, Bro05a, ISO05]. Preserve [NNT05].

Preserving [DN04, KS05b, LP00, Mö03a, YWD08, AKS04, 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 [An03c, SZ01, HLLL03, Ste08, AKS02].

Primitive [CFS05, IYK02, IMM01, ST01a].
Primitives
[BDFP02, CHL02, FGMO01, 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, BBDP01, CDM +05, Cho08a, DL98, DL07, DKFX05, DN04, GMM08, HY01, KS05b, Knu07, LP00, MP00, Pap05, PBD05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YWD08, Bel04, Bjo05, Bra01a, CLR09, CKN06, HIW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZYLG05, ZSM05, MS05a, Jan08]. Privacy-Enabled [Por06]. privacy-enhanced [ZSM05]. Privacy-Enhancing [SE09].

Privacy-Enhancing [ZSM05].

Privacy-Enabled [Por06].

Procurement [Lad06]. produce [Zir07]. producing [SOIG07]. product [Sun02]. Products [ACS02, Ano02b, Ano02c, Knu07]. professional [Dew08, vT00]. proficiency
Profiles [PJH01, RSA00c]. Profiles [MV01, FJK01]. Program [Höö01, Bec02, GGH+08, Kov03, KH03, CS08b]. Programmable [Dan07, GC01a, HV04, Sni02]. Programmer [Wil01b, Bon00, Che00, DKK07]. Programmers [Coc01a, Wei04, Gou09]. Programming [ASW+01, Ano02b, Coc03, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03]. Programs [BGI+01, Ark05, SLTB+06]. Progress [KK06, KFSS00, RD01, Roy00a, CV04, DV05, JM03, MMV06, MS02c]. Project [Fri01, IY00, MNT+00, Pau02a, Salxx, Gou09, LR01, Lov01, MWM01, Sha01a, Coc01a, Coc02b, IY00]. projects [Gha07]. Prolog [Bla01a, Bla01b]. promises [Pau02a]. promote [WK05]. Promotes [Bar00b]. prone [MLC01]. Proof [Abe01, Abe04, AS01b, ARC+01, BD02, Cor02, Gou09]. Proof-of-compliance [LMW05]. Proof-of-Concept [ARC+01]. Proofs [BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, Gol09, HG05b, SV01, dH08]. Propagation [LJL05, QPV05]. Properties [ABC+05, BM01c, KY10b, LLL+01, MS02a, NNT05, SM00a, BD04a, FGM03]. Property [LPZ06, Qu01, Uni00b, WY02, BR06, JRS09]. Proposed [Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDWO6]. Protect [ETZ00, BBN+09, WK05]. protected [PKH05, ZCL05]. Protecting [Des00c, EHMS00, KY10d, Kra01, LKM+05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LIY04, LS05b, ZYL05]. Protection [CGJ+02, DKFX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, Gor05, Kov03, KH03, Kwo03a, LL05b]. Protections [JT01a]. Protocol [Ano01a, Bel01, BPS02, BL02, CK02a, CJ03c, CWY05, Cim02, ECM00b, Fre03, GJKR03, GL00, HS07, JP02b, JRFH01, JT05, Kra05, Ku02, LCK01, Mea01, MSU05, NS01b, Rub00, RMCG01, SK00, Tan07b, TST09a, TST09b, YSR01, BP03a, Bla01b, BDFP05, BK05, CS04, CCKA04, CC04b, CY05, CC05c, Che04a, CLC08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, HT08, HWWM03, HHC05, HK08, KKL09, KTC03, LC03, LF03, LK00, LK00b, LW04, LHL04, LKY05b, LKY05c, LHC08, LSH03a, LC05b, Luk01, MS03a, Par04, Shi05, SW05, SIR04, TM06, Tse07, WK05, WLT05a, WHHT08, YW05, YTWH05, YC09, YS02, YRY05b, YRY05c, YPKL08, ZWW01, ZL04c, ZDW06, ZYW07, LSH03b]. Protocols [AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, BZ01, BMN01, Bra01b, BLD09, CJK01, CT08a, CMMR02, CMMR05, Cir01, CNV06, DFG01, Fis01b, FGM00a, GMP01a, GM01, Gor02a, JW05, KS00a, KY03, KL08, Kra03, Kis02, MS02a, MN01, PB00, PR08, PJDH09, Rot01, Shy02, SC01, AA04b, AKNRT04, Bar06a, Bau05, BDSV08, BFGT08, BP05, BL06, BD04a, Can01a, Can06a, CP07, CKRT08, CWJ01, CH07a, Ch00b, Chr00, Chr01, CJM00, CC05d, DFG00, GU01, HM02a, JW01, KS05a, LPV+00, LLL04, Mea04, MT07, MRST06, Mon03, MP07, PR05, Puc06, SV01a, SL05a, SR00, SW00b, SY04, ZLX09, ZL04b, PDS09, Puc03]. ProtoMon [JT05]. Provability [GOR02b]. Provably [HM02b, HLL+01, HSL+02, KSH01, PDF05, SLL+00, BGP09]. Provides [AB01, Sch01a]. Providence
[IEE07, Sil01]. **Provider** [LDM04, HLM02]. **providers** [MV03b]. **Provides** [OT03b].

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

**Proving** [Che03, FS01c, GN01]. **Proxy** [LDM04, HILM02].

**Proving** [Kha05]. **Proxy** [AH05, BCL05a, DKFX05, LCK03, LCZ05b, PL01, Rds01, Sha03d, ZJ09, AFGH06, CCh04, DY09a, HW03, HW04, HWH05, HW05, HC04b, KHL09, LL05b, LHH05, LCZ05c, LW05c, PKH05, Sha05b, SHT05, YTH04, ZCL05]. **Proxy-enabled** [DY09a]. **Proxy-protected** [PKH05, ZCL05].

**Pseudo** [BH05, FW08, Gen00, LLL+01, LHL+08, MP03, SXY01, TAZ09a, TAZ09b, WP03, BG09, GB09, MFK+06, NR04, Psp+08, RGX06, SL09, WW08, YZen09]. **Pseudo-Random** [LLL+01, MP03, WP03, Gen00, SXY01, MFK+06, NR04, RGX06, SL09, WW08]. **Pseudo-Random** [BH05]. **Pseudo-signatures** [FW04]. **Pseudonoise** [HG05a]. **Pseudoprimes** [ZT03]. **Pseudorandom** [CDI05, DN02a, DJ05, DP02, Fin06, Fhu02b, FIPR05, GM02a, IYK02, LMCET06, Nie02c, RSN+01, Aam03, BGG05, SXY01, MFK+06, NR04, RGX06, SL09, WW08]. **Pseudorandomness** [GM02c, IK00, IK01, KYHC01, LLH01, Lear03b, MV00, Shi03, Gol99]. **Psychology** [Myc01]. **Publication** [Nat00]. **Public** [ANS05, AUW01, APV05, Ano01h, AEAQ05, AF03, BC05a, BDG+01, BDZ04, Bar00c, BPS00, BBM00, BBDP01, BLM01, Bi00, BDW01, BST02, CHK03, CHK05, CDM+05, CHM+02, CHK08, CCW02, CT09, CCM01, CS02, CS03b, DPV04, DJ01, Des02, DY09b, DKKXY02, DFK+03, ESG+05, ES00a, ED03, FL06, FL01b, GL02, GW01, GC01b, GSB+04, Gtu04b, HCD002, HR05, HG05b, HR04b, HJW01, HLC08, IEE00b, IZ00, Jou02, Kat05b, KKM01, KM01a, Kim01, KLY02, KKY02, KY02c, KLC+00, KL01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Mål03a, Mol03b, Mål04a, NPO2a, NBD01, NSS02, OTU00, PHK+01, Pei09, PR01, Po02, PHM03, Qu01, RSA00a, RKZ02, ST01a, ST02, Sin01a, Sm01c, Ste01, ST00, TT01, Vau05a, WZW05, WHH01]. **Public** [WV00, Wy90, YKMY01, YG01c, YDKM06, Zhe02a, AG09, BHM03, BCL05a, BCW05, BBN+09, Ben01a, BB79, Bra01a, BD04b, Ca00a, CCT08, CL02b, CWH00, CCH05, CJ05, CKRT08, Cho06, DMT07, EKRMA01, EHK04, FMY02, FP00, Ga02, GH08, GKM+00, GS01, Gor05, GMW01, HCD08a, HCD08b, HHG06, HW04, HL04, Iwa08, IM06, JXW05, JZC05, KPS02, Kob00, KW00, Kos01c, LF03, LKY05b, LCK04, LLL08b, LSL01, LWW05a, MÅ01b, P06, PC09, SN00, SRJ01, Sha04b, Sha05b, Shp04a, SLC05, Sun00b, SZP02, SC05c, TO01, THC05, Tsa05, TJ03, VS01, WDL09, War00, Wu01, WH03, WL04b, hY08, YRS+09, ZSM05, AL06, BDZ04, Ben02, CZ05, Des02, GL05, KLG04, Kim01, NP02a, Vau05a, YDKM06]. **Public-Key** [Ano01h, AEAQ05, BC05a, BBM00, BBDP01, BLM01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DPV04, DJ01, DFK+03, ESG+05, ES00a, FL06, GW01, GC01b, HR05, IEE00b, Kat05b, KKM01, KM01a, KLY02, KKY02, KY02c, KLC+00, KL01b, KM04b, Kos01a, Kos01b, KY01, Kur01, LP03, Lin03, Lin00b, MR01b, MR01c, Mål03a, Mol03b, NSS02, OTU00, Po02, RSA00a, ST01a, ST02, Sin01a, ST00, TT01, WH01, YDKM06, AUW01, ED03, HG05b, Pei09, BHM03, BBN+09, BD04b, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HHG06, Iwa08, JXW05, JZC05, Kos01c, LF03, LS01c, MWS08, Mål01b, SN00, SLC05, Sun00b, TO01, ZSM05, GL05]. **Public-Key-Based** [YKMY01]. **Publication** [Top02]. **Publications** [Bee05]. **publique** [RSA09a].
publish [SL05b]. publish-subscribe [SL05b]. Published [MS03b]. Publishing [Ano02b]. puce [Car00]. PUFs [MKP09].

Purpose [Ano07b, Ano07a, ESG05, GS07a, GPP08, SGK08, LJ05a]. Purposes [LS05a, FSGV01, PBV08]. Push [Pau03].

puzzle [LF03]. Puzzles [Ano01e, ANL01, CHS05]. Q [BFMR02, CH01b]. Q&A [LS05a, FSGV01, PBV08]. Push [Pau03].

Radix [HKA05, JY01]. Random [BGP09]. Randomized [Sem00, Hro05]. Randomness [DD00, DD04, DGH04, FWW04, Gen06, MT02, JLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03].

Rao [ZYR01]. rapid [OP01b]. Rate [BH05]. Ransom [BH05]. Random [BGP09]. Randomized [Sem00, Hro05]. Randomness [DD00, DD04, DGH04, FWW04, Gen06, MT02, JLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03].

Range [CW09]. Rank [Sun00a, DW01, Sim02]. Ransom [BH05]. Random [BGP09]. Randomized [Sem00, Hro05]. Randomness [DD00, DD04, DGH04, FWW04, Gen06, MT02, JLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03].
[KT01, LZ09, PS02a, Sun02]. Rates [GH02].
Ratio [Di 01]. Rational [HT04]. ratios [Zir07].
RBAC [LSZ05, SN04, ZP05].
RBAC-Based [LSZ05]. RC4
[FMS01, Mir02, VV07]. RC6
[GHJV00, GHJV01, IK00, IK01, KM00, KM01b, RRY00, STK02]. RCES [LLCL08]. RCES/RSES [LLCL08].
Rational [HT04]. 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
[Dr02, GM04, YZDW07]. Reality [Coc01a].
Really [CZB+01, Wei00, Dav01c]. reason [Lau08b]. reasoning [IK03].
Red-Eye [Sas07]. Red [Sas07].
Redondo [IEE00a]. Reduced
[BDK02b, CS05b, FKSW00, HQ01, HSR+01, KK00a, KS00b, KK01, KML+02, KM01b, KS00b, MHL+02, NPV01, STK02, SKI01, YSD02, CV05, Küh01, SK01a].
Reduced-Round [FKSW00, KK00a, KS00b, KK01, KML+02, KK00b, NPV01, YSD02, CV05, Küh01]. Reducibility
[DM00b]. Reducing
[AL07, BIM00, SPH06]. Reduction
[CM05a, CH07c, Dhe03, HG07, Kid02, PG05, ALV02, HG07, Sug03].
reductions [Fis01a]. Redundancy
[AB01, BR00a, FM02b, YLR05]. 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
[BSN00, Bur00]. Region-Based
[BSN00]. register
[HTW07]. Registers
[CGFSHG09]. Registration
[HL03]. regression
[mSfL05].
regulations
[Cla00b]. Rehearsal
[Ahm08]. reinforce
[SWR05]. Rejewski
[BCB+05, Kap05].
Related
[BD01a, Can06b, CY08, FKSW00, Kil01b, KLML05, Sat06, Buc00a, Gutxx, HAU04, Hen06, Sch00b].
Related-Key
[FKSW00]. Relation
[ABC+05, NN06]. Relational
[AK02b, AHK03a, AHK03b, GA03, PT08].
Relations
[BN00a, Uni00a, Uni00e, Zha08].
Relationship
[NG05, GKM+00].
Relationships
[DKM05]. SKU+00].
relative
[JRS09, Möü01b]. Relaxing
[CKN03, PS05]. Relay
[DM07b, Zha00].
Release
[CHKO08, Mao01, HGNS03].
Released [Bar00c]. Releases [Bar00c, AJ08]. Reliability [IKP+07, WK05]. Reliable [JR03, MPHD06]. reloaded [SL06].
Remainder [Sch01b, YKL03]. Remarks [BCW05, Cl04d, SCS05c]. Remember [HSH+08a, HSH+08b, HSH+09]. Remote [CWR09, Kra02b, LL05c, Rub01, TK03, WK08b, CC01, Cl04d, CJT01, Hsu05b, HL05b, KC05, LHY02, LHY05a, LHL03b, LC05a, SZS05, WLT05a].
Remotely [Küh08, SR00]. Removal [LLS05a]. Removing [JL00].
rencontres [PPV96]. Renewable [Bar00b].
Reply [WLW04]. Report [DFG01, Pre01, Sala01a, Sh03b, BCHJ05].
Repository [Bar00b]. Representation [BJvdB02, FSW01, JLMS03, JY01, RN00a, RN00b, ZL02, BDSV08, BA06, PS04a, SWR05]. Representations [OSSST04]. Representative [CTBA+01].
Representatives [Uni00a, Uni00b, Uni00f, Uni00c, Uni00h].
Republic [MJ04, dL00]. Republiek [dL00].
reputation [HLL04, LSA+07, SC05c]. reputation [KNS05, RCG05]. reputation-systems [KNS05]. Request [RSA00b]. require [SV08b]. Required [Sun00a, Lov01, Wan05]. Requirements [FIP01b, HH01, Kin02, NIS01b, Mea04].
Rescue [ASW+01]. Research [AJ01b, CZ05, CZ05, DFPS06, KGL04, LXM+05, RC06, Sch00e, TMM05, DFCW00, JXW05, MH09, Q500, dCDS05].
Researchers [Pau02b]. Resettable [DP04, MR01b]. Residue [TIGD01, YKL02b, 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, M602, EB01]. Resistant [Ano01e, ACJT00, ANL01, BGW05, CDTT05, CNV06, Gir06, IK05, 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, XK+05]. Responsibilities [Vix02]. Resting [Gut02a]. restricted [ASW00]. Restudy [FWL08]. Results [AP05, GM02c, OOP03, RR08, Way02a, YRS+09, CV05, CKRT08, DM07a, GMG00, PM08]. Rethinking [Bra01a, KMZ03].
Retreat [FKS00]. Retrieval [BIM00, KO00, RE02, Yek07]. Retroactive [DS01]. retrofitting [CGL+08a, CGL+08b, CGL+08c]. Reversal [Cap01, D02]. Reversal-Bounded [DIS02]. Reversals [MS02e]. Reverse [Coo02, EC05, Wue09]. Reversed [Ina02b]. reversibility [KO09]. Reversible [Go03].
Reversing [EC05, YWC08, YN01, CDFM05]. Review [And04, Ano02e, Duw03, Ego05, Fal07, Gas01, Gum04, Imr03, Ian08, Lee03a, Lee03b, Mar05a, Pago03, Pap05, Puz04, Rec01, Rot07, See04, Spr03, Ter08, TvdKB+01, Top02, Uzu04, Was08a, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Sph04a, Wal00].
Reviews [For04, Kid00, Sala03b, Sty04].
Revised [Bla03, BC05b, Chr01, CMMR02, CMMR05, CY09, CGP03, DR02c, GS02c, GH05, HH04, HH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PTO6, RM04, Sil01, Ytr06, AMW07, A01a, BK07, Bir07, CZ05, CKL05, DRS05, Irw03, PY05, WK06, Wri03].
Revisited [ABC+05, BM01b, CDMP05, Knu00b, NS05c, OSSST04, Has04b, ZZT05].
Revisiting...
Revocation
[BDTW01, CL02a, Gen03, GST04, NNL01, TT01, ZSM05, KT06, KSW06, LHH05].
revoke [NN03]. revolution [Bor00, Con00].
Revolution [CMB+05]. Rewriting [Cir01, HR04a].
Revolutionary [Bor00, Con00].
Rewriting [Cir01, HR04a].
RFC [BWBL02]. RFID [And04, AL07, ACdM05, BLDT09, CCS08, CH07a, CL09, FW09, Fin03, KKJ+07, OS06, Ros06b, SE09, TZZT09a, TZZT09b].
Rhee [K¨uh08].
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, FKL+01a, FS01, FD01, GM00a, JmBdXgXm05, KY01b, KMK01, KY01, LK00, MM01b, MMH02, PSC+02, RDJ+01, SMTM01, SRQ03].
Rijndael-Like [PSC+02].
Ring [BSS02, Nao02, WBL01, ZK02, Her07].
Rings [BLST01]. RIPEMD [DG02, WFLY04].
RISC [Cor00a, Gro03, WWCW00].
RISC-Based [Gro03].
Risk [WA07].
Risks [ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, Pv01, Sch00c].
Rivest [BB79, Coc03, SP79].
RMI [JB06, Mar02a].
RNS [BI04, BKP09, NMSK01].
Road [BDPV09, HR04b, PB01].
Roadmap [Cog02b].
Roaming [CAC03, YWD08, SSM+04].
Robots [Cog01a].
Robust [BB00a, BR09, CJ03c, CW05, DDO+01, hKL00, Lin00a, LHS05, LLC06b, PJK01, SG07, SOH01, SDFH00, SDF01, VK07, WNY09, WL04b, WMDR08, YPSZ01, ZTP05, LCZ05c, 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 [Bor00, Con00].
Root [Pet05].
rootkit [Blu09].
Rootkits [HB06].
Roots [Gon06, HCK09, CAC06].
Roseau [PY05].
Rotation [RBF08].
Rothe [Fal07].
Rough [Naz02, WG05].
roughness [Lav09].
Round [II00, BP04, Bih00, BF00a, BDK02b, Che03, DPV04, DI05, Dra00, FKS00, GKK007, GIKR02, HSR+01, Kan01, KO04, KKS00a, KS00b, KKS01, KML+02, KKS00b, LKHL09, Lin01b, MP03, MHL+02, NPV01, RR00, Ros00, STK02, WBF00, Wer02, YSD02, CV05, CLC08, CKL+03, DLP+09, GIKR01, HSL+02, Kiih01, LKH+08, MR01b, Pha04, SW05].
round- [CLC08].
Round-Complexity [Ros00]. Round-Optimal [KO04].
Rounds [BDK+09, CD01a, HSR02, KM01b, Luc00, Pat03a, Pat04, GM00a, SK01a].
Routing [BGOY08, CL05, Ken02a, KB09, LAP08, LHC08, MBA06, PS08a, RV09, vOWK07].
RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02b, Shp04a, Wal00, Adl03, Ano01i, Ano02c, AR01, BI04, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BN00, BF01c, Bon01, BCCN01, BP01b, CN02, CDL+00, CW02, Che01a, Cky05, CNP03, CK00, CJK02, CS00, CS03c, CD01b, DK01, DT03, Duj08, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gor01, HN04, Her07, HLL03, HL00, HLL03, In00, JS05, Jon08, JK02b, J02b, JG01, Kal01, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, Miy01, Mol03b, MP01c, NZCG05, NS01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Se03a, Shp01, Shp04b, SZ01, Str02, SWH+09, TIGD01].
RSA [TT00, Ver06a, Wal01, Wal03, WQWZ01, War00, WLHH05, Wie00, WS02, WY05, XC05, Yan07, hY08, YKLM02b, YKLM03, YPKL08, YY00, Yoo06, ZC09, Zhe01,
RSA-Based [BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZCG05, Sei05, WLHH05, WY05, YPKL08, YY00]. RSA-Encrypted [CD01b]. RSA-Primitive [ST01a, RSA(R) [BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZCG05, Sei05, WLHH05, WY05, YPKL08, YY00]. RSA-Encrypted [CD01b]. RSA-Primitive [ST01a]. RSA(R) [Ano06a]. RSES [LLCL08]. RST [ZLZS07]. 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, JmBdXgXm05, Opp01, SMTM01, ZC00]. S-Box [FM02b, SMTM01, JmBdXgXm05]. 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]. Safeguard [LXM+05]. Safeguarding [Sty04, Bar03]. SAFER [NPV01, BDD03]. safety [HM01a]. SAFKASI [WAF00]. Salomon [Pap05]. Salsa20 [Ber07, Ber08]. Salt [PKBD01]. Salzburg [DU05]. Samba [BH00a]. SAML [RR04]. Samos [KLG04]. 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, Kil01a, Men07, Sho05a, Yun02a]. Santiago [BS03]. Sanxin [LSZ05]. SAR [B+02]. SASAS [BS01c]. Satan [Mea04]. 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 [Ito01]. SC2000 [SYY+02, YSD02]. SC2001 [ACM01b]. Scalable [CPlX04, HKA+05, HLL05, KY03, KYH08, SPG06, LLW08b, ST03a]. Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. Scale [BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a]. Scaling [BBP00, Coc02b, SDFH00, SDF01, PBVB01]. Scambray [Gun04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Ols00]. Scenarios [BF05]. scene [SG07]. Schedule [MMH+02, XH05]. Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BNPS02, BR09, BS01d, BMS03, CL01a, CHK03, CGH01, CRY01, CH01b, CM05a, Coc01b, CFS01, CDM00, DFKX05, FS01c, GJSS01, GS02c, HS02a, HNZ02, HY01, HT06, Igl02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, Miy01, Mii01a, OKS06, PL01, RK06, SOO02, SWH05, SGG00, SYL05, SSNG00, Tad02, TC01, Tas01, TT01, WQW01, WZW05, WBD01, YG01a, YLH05, Z09, AEEdR05, BCL05a, BCW05, BKN04, BBG+02, CL02b, CC01, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CH05a, CH05b, CL00, CH04, CCH04, CY05, CH05c, Che05a, Che07, Che08a, Che08b, CCK04, CKN06, CHT01, DW01, FXAM04, FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HWW03, HWW04, Hsu05a, HWW05, Hsu05b, HCO4a, Hwa00, HY03, HLL04, Hwa05, HLL05c, HLL05d]. scheme [HL05b, JW06, JSW05, KC09, KLY03, KRY05, KSW06, KHL09, KCL03, Ku04, KC05, KCC05, HKHL05, LHY02, LHH02, LHL03a, LKY04, LL04a, LJY04, LL05a, LKY05a, LKY05d, LL05b, LM+03, LLH04, LTH05, LLCL08, LHL03b, LC04a, LYGL07, LCC05, LC04b, LC05a, LHH05, LCZ05b, LCZ05c, LCZ05a, LWK05b, MSP09, NC09, PW05, PBMB01, PCC03, PC05b, PS01a,
Pei04, Sae02, Sco04, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, mSgFtL05, SCS05b, SC05c, SCS05c, SZS05, TLH05, TWL05, TYH04, VK08, VS08, Wan04b, WL05, WK05, WJP07, WDLN09, WHH05, WC01b, WH02a, WHLH03, WH03, WL04b, XC05, YTH04, YW04, YCH04, hY08, YRY04, YRY05a, YY05a, YY05b, YbJ04, ZC04, ZO04, ZK05, ZK05, ZA05, ZCA05, ZL05, dRMS05].

Schemes [AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00, CL04a, CT08b, CPD06, CKN00, Cor02, CNJ02, CON04, CS00, CS03b, CDG05, CLZ02, DN00a, DN00b, Des00b, DN00b, FF00, HSZI00, HW05, HM02b, HLL05, Kin02, Kos01a, KS03, KOMM01, LTL05, LP01, MV00, NIS03b, Nan02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SB02, SPMLS02, Sun00a, VMS05, SX03, YWC08, YYD001, Yek07, YYY01, ZTP05, ZYR01, Abd01, AFGH04, BCD06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGK03, HCD08a, HCD08b, HAnR04, He02, HK00, HW04, HW05, HCO04b, HLO4, IIY06, JXW05, KJY05, Kir01, KTO05, Kre05, Küh08, LWZH05, LWK05a, LW05c, MF07, Mii01b, NK06, PS02a, PKH05, QC05a, QC05b, SN00, Sha03d, Sha05b, SCL05, SHT05, Ts05, Wu01, XYQ04, YWC05]. schemes [YCW08, ZF05, ZCL05, vDKST06].

Schloss [IEE01b, Schneider [Puc03].

Schneier [See04, Sty04]. Schmorr [BP02].

School [Coc02a]. Schools [PM00].

Science [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Im03, Nic02d, Pag03, Sch06b, SM07, Sin01b, CAC06, PRS04].

Scientific [CHT02, MH09, Lau08b].

Scientists [Coc01a, MH09].

SCN [BC05b, CGP03].

Scots [Rec01, Sin99].

Scream [HCJ02].

Scribner [Gas01].

Scripts [Uri01, Oue05, Rob02, Rob09].

scroll [GB09, HHYW07].

SD [ECM00a].

SDK [Ano02b, Bar03c]. SDL [HL06]. SEA [SPG06]. SEAL [Hu02b]. Seamless [OKE02]. Search [Bl05a, Des00c, FIPR05, KB07, LM02, TIGD01, WYY05a, WYY05d, PM08].

Searchable [ABC05, AFI06]. Searchings [PGT07].

Seattle [BSW09, GTTC03, OS05].

Second [ACM06, S03, USE00a].

Second-Order [NM09].

Second-Price [Bra01b].

Second-Order [NM09].

Secret [ACS02, BBDK00, BTW05, Bl05b, BTW08, BP06, BM01b, CGH06, CGH00a, CH01a, Cha04, CS05a, CKN01, CMD00, CDF01, CF02, CFS05, CDG05, CD05, Di01, DKL00b, DN00b, DP07, EHS00, FM02a, FS02, Fis01b, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah67b, K06, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, MN01, NAG03, NN06, OKS06, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sin00a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, AJ08, AEE05, Bam02, BCB05, CA01, CCA05a, CHY05a, CHY05b, CJO4, CND04, CDD00, DD04, DB04, DM00a, Di03, DW01, Duj08, FNRC05, FWTC05, G002, GIKR01, HT04, Hcj07, HKS00, IY06, Kar05, Kee05, KB09, Lam07, Lun09, MF07, MI09, Naf05].

Secrets [PS02a, PW05, Ris06, Sch01e, SBZ04, SC05a, Sm01b, Wan05, Win00, YCH04, ZSV05, dRMS05, vDKST06].

Secret-Ballot [Cha04].

Secret-code [DW01].

Secret-Key [HR05, RW03a].

Secret-Sharing [Bl05b, CDM00, CD05, DKL00b].

Secrets [BH06, BBD02, CMS09, CP07, Cop04b, Di01, Gan01b, Gum04, KMS01, LKM05].
Lys08, Pag03, Puz04, Sch00d, Swa01, TEM+01, VGM04, AGKS07, Bam02, Bau00, Bau02a, Cop05, Cop06, DM07a, Di 03, DW09, EC05, FS04, GD04, MSK03, Ste08, TCC02, DLMM05. Section [Ano04a, Ano07a, BK06b, SGK08, TL02, KP03]. Sector [Ano04a, Ano07a, BK06b, SGK08, TL02, KP03].
SLG\textsuperscript{+05}, SL05a, Shp02, SEF\textsuperscript{+06}, SEK01, SEK02, SK06, Sta03, SB07, Ste05b, SBZ02, Sty04, SKI01, Sun05, Swi05, Tan07b].

**Security**

[TG07, TG04, TPPM07, Uni00a, USE00d, USE01c, USE02b, Uni00c, Uni00d, Uni00g, Uzu04, Vau02, VMC02, WLT05a, WBL01, WLL\textsuperscript{+02}, WA07, YEP\textsuperscript{+06}, YWD08, Zau01, ZWC02, ZD06, Zhe02b, ZYH03, ZS05, AA04b, Ano05b, Ajo01a, Ajo01b, Bao08, Bau05, Bej06, BR04, BGP09, BFGT08, BFG08, Bjo05, Ble07, BJ02, BMW05, BGO\textsuperscript{+07a}, Brou06, BMV06, Can01a, C\textsuperscript{+02}, Cha07, Cha05b, CKL\textsuperscript{+09}, CKRT08, CJL06, CJM00, Con09, Con04, CC05e, DP04, DKK07, DY01, DFGH04, Des00a, DWML05, DKKU05, DMS07, Egh00, FXAM04, FR08, FOP06, GH08, GJJ05, Gha07, Gor05, GKS05, GMW01, GC05, HN04, HCD08a, HCD08b, Hen01, Hes04a, HM05, HSL\textsuperscript{+02}, HL06, HG05b, Ino05, JFZ04, Jan00, Kad07, KY00, KPS02, Kim02, Kow03, Kli03, Kwo03a, LC03, LL03, LJY04, LL05b].

security [LPW06, LMC\textsuperscript{+03}, LMW05, LLL06a, LLL06b, LHC08, MJ03, Mal06, Man08, Man05, Mau04, May01, MKWW00, MS03, McG06, Mem03, MSQ24, MK05a, MPPM09, OP01b, Pae03, PSCG\textsuperscript{+09}, PC05a, Pat02a, PY05, PP06a, Pus03, PHS03, Poi00, PS04c, RC05, Ros06b, RNo04, SN00, Sal05d, Sch03, Sen03, SHL07, Shu06, SPH06, Son00, SH00, Sta02a, Sta06, Ste02, Sun06b, SHT05, SLL\textsuperscript{+00}, Tsa05, Un000f, Vac06, VS08, WA00, WA06, Won01, WK06, XQ07, YY05b, ZS010, ZW05b, ZSN05, dCdVGS05, vOWK07, vT05, AG09, Ana02c, BC05b, BP01b, chr00, Chr01, CCM02, CCMR05, CGP03, JRB\textsuperscript{+06}, Lin02, RR04, Uni00h, ZL04c, Pup05].

**security-related** [Gut03].

**security-sensitive** [SPH06].

**seed** [TP07, KJ\textsuperscript{+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, Wi99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06].

**Selection** [Bur03].

**Select** [IBM00, JK\textsuperscript{+01}, RS00, SM08].

**Selective** [CS07e, LS01a, LM02].

**Selective-ID** [CS07e].

**Selectively** [Chi08].

**Self** [GMM08, HW05, KY01d, PS01b, BPC05, Sch06b, WHL05, WLT05b, ZKL01, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, HL04, Lee04a, LL06, LS05b, LWK05a, PC05b, Sha04b, Sha05b, TLH05, Tsa05, TJ03, WH03, Wyl05].

**Self-certified** [HW05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HL04, LL06, LWK05a, Sha04b, Sha05b, TLH05, Tsa05, TJ03, WH03].

**Self-Enforcing** [Wyl05].

**Self-Escrowed** [PS01b].

**Self-Localization** [WLT05b].

**self-modifying** [CSV07].

**self-pairing** [Lee04a, PC05b].

**self-protecting** [LS05b].

**Self-Shrinking** [WHL05, ZKL01].

**Self-Similarity** [Sch06b].

**Selling** [Bla01c].

**semantically** [PBV08, SNI00, Sch00c, Coc01a].

**Semantically** [KI01b, ST01a].

**Semantics** [Li01, Mar02b, BFG04, BFG05].

**Semi** [Fer00, Nak01, SY01b].

**Semi-Equivalent** [Fer00].

**Semi-fragile** [SY01b].

**Semiconductor** [Coc02b, Ig02, UHA\textsuperscript{+09}].

**Sens** [Cop04b].

**semi-public** [YC07].

**Sender** [MB05, TJ01a].

**Sensation** [Top02].

**Sensible** [Sch04c].

**Sensibly** [See04, Sty04, Sch03].

**Sensitive** [HT06, Bro05b, SPH06].

**Sensor** [AEQA05, CS08b, DBS\textsuperscript{+06}, Fin06, GP\textsuperscript{+08}, LNL\textsuperscript{+08}, NABG03, PJDH09, ZYN08, AJ08, CCMT09, HMDL07, JRR09, KXTZ09, KHY08, LDH06, LPV\textsuperscript{+09}, LN04, MW08, MS09b, NC09, NLD08, PS08a, RA07, 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, CSY09, CGP03, DV05, DKU05, DFCW00, EBC+00, ELvS01, FLA+03, GKS05, QS00, RS05, SM07, WKP03, dCdVSG05, AJ08].

September 19 [AJ01b]. September 19-21 [AJ01b]. Sequence [HWH01, MS02e, WHLH05, ÁCTZ05, GB09, SL09, WG02, YZEE09]. Sequences [ADD09, Bi09, FSGV01, HG05a, JZCW05].

Sequential [HWH01, MS02e, WHLH05, ÁCTZ05, GB09, SL09, WG02, YZEE09]. Sequential [CD00, EIG01, TW07].

Serial [BIM00, HS07, Jab01, KCD07, Mar02a, TEM+01, LS05b, Pat01]. Server [ANRS01, BMK00, Dew08, Ko00, LWK00, NS01b, PS05, TMM05, XS03, Zhang00, BB05, LHL04, LKY05b, LHL03b, NTW07, Tsao1, TWL05, YS04]. Server-Assisted [NS01b]. Server-Assisted [NS01b].

Serverless [BDET00]. Servers [BIM00, HS07, Jab01, KCD07, Mar02a, TEM+01, LS05b, Pat01]. Service [BACS02, BH06, BBDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01].

Services [ANS05, BCS02, DJLT01, ECM00a, ECM00b, Km07, Tsao1, Uni00b, BDS+09a, BFG04, BFG05, BFS08, CCCY01, HM05, JRB+06, MPM09, MV03b, RR04, SGB07, SL05b, TWL05, WA06, BH00b]. serving [LLK05].

Session [GL01, OHB08, CS04, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Session-Aware [OHB08]. Session-Key [GL01]. Sessions [KPR03]. Set [BBGM08, GRW06, JRFH01, KS05b, WG05, BDET00, Che07, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01]. Sets [CS005, EIG01, TW07]. Setting [BBM00, DLY08, LP01, PGT07, GMLS02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC+01]. Several [KS00a, LD04, Tsao5, ZT03]. SFLASH [GM02b, SGB01].

SGI [Bar00c]. SHA [AD07, BC04a, GLG+02, HKR01, MP06, SK05a, TYL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG+02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TYL02].

SHA-1 [GLG+02, HKR01, MP06, WYY05b, WYY05c]. SHA-3 [SK05a]. SHA-512 [AD07, GLG+02, HKR01, MP06, WYY05b, WYY05c]. SHA1 [WYY05a]. SHACAL [KML+02].

Shacham [Has04a]. Shamir [BB79, SP79, Coc03, PW05, VS08]. Shamir's [LD04]. Shape [Gan01b, Gil07].

Shapes [OMT02]. SHARC [DMSW09]. Share [CT08a, CD05, FS04, AEEadR05].

Shared [ACS02, BH06, BBDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01].

Sharing [BTW05, Bi05b, BTW08, BGH02, CD00, CDM00, CF02, CS05, CDG+05, CD05, Di01, Di03, DP07, FM02a, FPS01, FM01, HNZI02, Kin02, Kog02, KS03, LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, SZ01, Sun00a, TC01, TCC02, WN02, WB01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CDD00, DD04, DM07a, DKL00b, FWT05, GIKR01, HT04, HKS00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDKST06].

She [Gua05]. Sheets [MNS01]. shell [Dwi04, Gua05, BS01a, BSB05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [YWC05].

Shift [CGFSHG09, Che08a]. Shin [Küh08, Küh08]. Shines [Coc02b]. Shinko [An00b]. Ships [An02c]. Shops [An01c, YSS+01]. Shor [KL+02a].

Shores [KKP02]. Short [KPR03].
short-term [WDLN09].

Shor [Luc02b, VMSV05]. shows [AJ08].

Shortcuts [Sha03a].

Shortened [Kur01].

shortest [Pei09]. ShortPK [WDLN09]. Shoup [Luc02b, VMSV05]. shows [AJ08].

Shrinking [Gol01c, WHLH05, ZKL01]. SHS [Ano08, Ano12]. Shuff [FS01c, NSNK05, Sas07]. Shuffles [Mir02].

Shuffling [PBD05]. shut [Gil07]. SiBIR [IR02].

SiC [IEE09a]. sichere [Lin02].

sieve [CM05b, JL03]. sieves [Har07a]. SIGABA [Lee03c].

SIGACT [ACM03c, ACM05b, Raj06]. SIGART [ACM03c, ACM05b]. SIGMOD [ACM03a, ACM03c, ACM05b, ACM04a, FMA02]. SIGMOD-SIGACT-SIGART [ACM03c, ACM05b]. Sign [BSC01b, BTTF02, Dav01c, Kra03, Dav01b]. Sign-and-Encrypt [BTTF02, Dav01c].

SIGN-and-MAC [Kra03]. Signal [Ano02c, GG05b, Sha01e, CKL+09, LLLZ06a, LLLZ06b]. Signalling [ECM00b].

Signature [ANS05, AAK09, AR00, ADR02, 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, GJSS01, GS02c, HY05a, HSZII00, HM02b, JSSJK01, KC02, Kuh00, LLL+01, LP01, MV01, Miy01, Nat00, NZCG05, PL01, PCK02, Pre01, RS01, SA02, ST01b, SOOI02, SWH05, SPMLS02, Str01a, SYLC05, SSNGS00, TNN00, WQWZ01, WBD01, XYL09, YYD01, YSS+01, YYZ01, YLH05, ZK02, ZJ09, Zhe01, AvdH00, BCL05a, BCW05, Ca00a, CWH00, CL04b, CYH04, CCH05, CJ05, CHC05, Che05a, CJT04, GKG03, HLL+02, Hes04a, HPS01, HWW02, HWW03, HWW04, HWW04, HW05, HW05, HC04a, HLL03, HC04b, H04, Kwo02, Kwo02b, LH04, LHY05, LL05b, LLH04, LTH05, LWZH05, LHH05, LCZ05b, LCZ05c, LCZ05a, LW05c].

signature [PKH05, PC05b, QCB05a, QCB05b, Sha02, Sha03c, Sha04b, Sha05a, Sha05b, Sha05d, SCL05, SHT05, TJC03, TYH04, Wan04b, WK05, WLHH05, WHH05, Wu01, WWH03, WH03, WY05, XCO05, YTH04, ZC05, ZF05, ZW05a, ZCL05, RR04].

Signature-Based [CK02a].

Signature-Embedded [Ano01c, YSS+01].

Signature-Tree [TMN00]. signature/multisignature [Wu01].

Signatures [AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCCN01, CD00, CL01b, CNV06, CBZ+01, CK01, GMP01b, GM03, Gen04b, Gra02b, HSZII01, Her06, HM02b, HS01, HHGP+03, HTL01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, MM02, MFNG02, PCCG01, Ram01, RR02, RdS01, WV01, XSO3, Zho02, Ate04, AH05, BLH06, BB05, BMW02b, BMW02a, BLRS09, Cal00b, CKK03, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HLH00, JL01, J04, KKKL09, LV07, LS05b, MMJ05, PLJ05a, PBV08, Sch01f, Sha01d].

Signcryption [Boy03, MLM03, Zhe01].

Signed [FL01b, OSSST04, Sch01a, SJ00].

Signer [DKFX05, CJT04, LL05b, WK05, IR02].

Signer-Base [IR02]. signer-verified [CJT04]. Signers [LZL+01, Sae02, Sha03c, YTH04].

Significant [SZ01, MS02b, Shp02]. Signing [IR01, RR02, HWW04, WK05, WH02b].

signs [Lum09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Scho06b].

Simon [Imr03, Ree01]. Simple [AKS06, CJS01, CJS03c, CYW05, CS03c].
Solve [CU01, GS03]. Solving [CJT04, GPP08, Wil01a, Bul09]. Some [AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau04, He02, JK01a, RSS04, SHT05, ZF05].

Solve [CU01, GS03]. Solving [CJT04, GPP08, Wil01a, Bul09]. Some [AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau04, He02, JK01a, RSS04, SHT05, ZF05].

Solving [CJT04, GPP08, Wil01a, Bul09]. Some [AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau04, He02, JK01a, RSS04, SHT05, ZF05].

Solving [CJT04, GPP08, Wil01a, Bul09]. Some [AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau04, He02, JK01a, RSS04, SHT05, ZF05].

Solving [CJT04, GPP08, Wil01a, Bul09]. Some [AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau04, He02, JK01a, RSS04, SHT05, ZF05].

Solving [CJT04, GPP08, Wil01a, Bul09]. Some [AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau04, He02, JK01a, RSS04, SHT05, ZF05].
NIS00, SB00, Sta00, WBRF00, YW06.

**Standardized** [Man01]. **Standards** [Ano01f, Bur06, CL07, Coc02b, Hus01, RSA00a, Ts06]. **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]. **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, BG08, CYH01, ChLYL09, CDR01, CW09, Col03, CMB+08, CS05b, DIRR05, FGD01, HLvA02, HvAL09, Hum05, HSRC01, PH03, Sal05b, Scha01, Shl08, 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** [WRW02]. **steps** [Bih02]. **Stereotypes** [GO03]. **Stern** [CS05a]. **sticker** [GPX08].

**Sticks** [Sam01]. **Stinson** [Spr03]. **STL** [Zol01]. **STOC** [ACM05c, 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, Kah07a, Kah07b, Kah06, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, Win00].

**strategic** [AJ08]. **Strategies** [Cir01, KL05, SKQ01, DW04]. **Strategy** [DR02a, TPPM07, KC09]. **Stream** [BCC01, BS00b, BL02, CF01b, Can06b, CJS01, CHJ02, CM03, Cour03, CL02c, DF07, Fil00, FO01a, Goul01d, GBM02, HC02, HR00, HR04a, Jam00, KHD01, MSNH07, PP06a, SM01, Sar02, SYX01, WB02, Wu02, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, DK08, KH08, Max06, MI09, PCS03, PCC03, SB05, WW08].

**Stream-Cipher** [SYX01, WW08]. **Streaming** [OS05]. **Streams** [AIP01, YLC+09]. **Strength** [CB01, JX05, Ono01, CKL+09].

**Strengthening** [Loi00, HM+02]. **String** [CPS07, DFS04, Pas03, Dam00, RG05].

**Strings** [Vau05b]. **Strong** [ADD09, BB00b, CS00, DF05, KCI+01, KW00, LSH03a, LSH03b, Lu02, Pau09, SBZ02, CCO4b, HRS08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04].

**Strong-Password** [LH03a, LSH03b, CC04b, KTC03, Ku04].

**Strongly** [IY06]. **Structural** [BS01c, LBR00]. **Structure** [DN07, EIG01, HSL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SSL+00, XMS07]. **Structured** [BRTM09, CKK03]. **Structures** [An02c, GTTC03, HDO02, KCP01, Küs02, MND+04, MF07, PSC+02, PQ03, Sun00a, XH03, He06, IY06, SW05].

**Stuart** [Gum04]. **students** [AA04b, PP09]. **Studies** [Pag03, SPH06]. **Study** [BBGM03, Car02, DPR01, DP00, KJ+07, WC05, BKN04, BF00a, DY09a, KW06, SKW+07, ZWW01]. **Sturgeon**
Subdivision [LDD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro05, GMR05].

subsampling [LLC06b]. subscribe [SL05b]. subsets [Sch01e]. substitute [Bih02]. Substitution [KKG03, GPX08, RBF08, WL04b]. Substitution-Permutation [KKG03]. Subsystem [HL07, MBS04]. Subtleities [Laï08]. subverting [HB06]. successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Sufficient [IKO05, Kos01b, KO00, MN01]. Suffix [ABM08]. SUID [Tot00]. SUID/SGID [Tot00]. Suitable [AIK+01, CQS01, KTT07, LKH09, SP05, Wen03]. Suite [RSN+01, SBEW01, YLT06]. Suited [WWGP00]. Sum [Che04b, KLY02]. Sum-of-Digits [Che04b]. Sums [Lam07, CAC06, Hos06b]. supercluster [Při00]. Supercomputer [Coc01a].

Supersingular [Gal01, RS02, Ver01]. Supplemental [TBDL01]. Supplementary [ECM00a, ECM00b]. Supplies [Sha01c].

Support [ABM00, Gro03, LTM+00, PJDH09, SBG02, Ano05b, BMA00a, BMA00b, BMA00c, ED03, mSgFl05, SSM+08, WNQ08, ZYL05].

Supporting [CLK01a]. Suppression [GA05]. Sure [Tom06]. surface [Iwa08, LDD07]. Surfaces [SPK08].

surveillance [LCS09]. Survey [EPP+07, KM04b, LDH06, ATS04, Ano00c, BEM+07, EY09, Mea04, Müi01b, OZL08, PC09, Pre07, RH03, RAL07, Sch01f, ÚG08, ZLZ07].

Survivable [CLZ02]. Susan [Jan08]. SVD [CYH+07, FWL08]. SVD-based [CYH+07, FWL08]. SVGrid [ZBP05].

Sweden [BS01b, Joh03]. Swedish [Bec02].

Swiss [Boy03, Kid00]. Switching [CT03].

Switzerland [CC04a, Vau05a]. Symbiosis [DF01]. symbol [SVDF07].

Symbolic

[Wei05, Wei00]. Stuttgart [Eag05]. style [dH08]. Subdivision [LDD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro05, GMR05].

subsampling [LLC06b]. subscribe [SL05b]. subsets [Sch01e]. substitute [Bih02]. Substitution [KKG03, GPX08, RBF08, WL04b]. Substitution-Permutation [KKG03]. Subsystem [HL07, MBS04]. Subtleities [Laï08]. subverting [HB06]. successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Sufficient [IKO05, Kos01b, KO00, MN01]. Suffix [ABM08]. SUID [Tot00]. SUID/SGID [Tot00]. Suitable [AIK+01, CQS01, KTT07, LKH09, SP05, Wen03]. Suite [RSN+01, SBEW01, YLT06]. Suited [WWGP00]. Sum [Che04b, KLY02]. Sum-of-Digits [Che04b]. Sums [Lam07, CAC06, Hos06b]. supercluster [Při00]. Supercomputer [Coc01a].

Supersingular [Gal01, RS02, Ver01]. Supplemental [TBDL01]. Supplementary [ECM00a, ECM00b]. Supplies [Sha01c].

Support [ABM00, Gro03, LTM+00, PJDH09, SBG02, Ano05b, BMA00a, BMA00b, BMA00c, ED03, mSgFl05, SSM+08, WNQ08, ZYL05].

Supporting [CLK01a]. Suppression [GA05]. Sure [Tom06]. surface [Iwa08, LDD07]. Surfaces [SPK08].

surveillance [LCS09]. Survey [EPP+07, KM04b, LDH06, ATS04, Ano00c, BEM+07, EY09, Mea04, Müi01b, OZL08, PC09, Pre07, RH03, RAL07, Sch01f, ÚG08, ZLZ07].

Survivable [CLZ02]. Susan [Jan08]. SVD [CYH+07, FWL08]. SVD-based [CYH+07, FWL08]. SVGrid [ZBP05].

Sweden [BS01b, Joh03]. Swedish [Bec02].

Swiss [Boy03, Kid00]. Switching [CT03].

Switzerland [CC04a, Vau05a]. Symbiosis [DF01]. symbol [SVDF07].

Symbolic [Bor01, Jef08, Mar02b, May09, MT07, MP05, ALV02]. symbols [Lam09]. Symmetric [Ano01b, ABM00, BU02, BKM07, ČvTMH01, CCM01, Des00b, EP05, FW09, Fli02, RR00, Ust01b, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01].

Symmetric-Key [Ano01b, ABM00, CCM01, EP05, RR00, BMA00a, BMA00b, BMA00c]. symmetry [RBF08]. Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, Ano00b, BS03, BCDH09, BC01, CCGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Jef08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05]. synchronisation [CmdV06].

Synchronization [GPCS08]. synchronize [Pau02b]. Synchronous [CH01b, Sar02].

synopses [YLC+09]. Syntax [BWBL02, RAST00, RASA004]. Synthesis [XFP01, SOIG07, UBEP09].

syslogs [ME08b]. System [Ano02b, Ano02c, ANR01, BIP05, BCST00, Bih00, CCDP01, CHM+02, CSM+08, CGJ+02, DJ01, DGP07a, DGP07b, DV08, EM03, FL01a, Ito01, Joh05, KC02, KHY04, LV00, LSB05, LL05b, LXM+05, MA00a, MA00b, Mly01, MFK+06, MFS+09, RH02, SR01, Sha02, SOO02, Ste05b, TK03, TZ09b, USE00a, WG05, WA07, YKM01, YKLM02b, ZYM05, AHK03a, AMRP00, ADH+07, AAKD09, Bnh09, BDET00, Bu09, CC02b, CCH05, CGL06, CPG+04, Coc01a, CO09, DZL01, DPT+02, DIM08, DGP09, FP00, GG08, GMG00, Gou09, HLU+02, Joy03a, KWDB06, KXD00, Kwo03a, LLO4b, LKJL01, Lin00a, LK01, MKKW00, RCG+05, Sa00b, SCS05a, SGMV09, SETB08, TKP+08, Wan04a].

systematic [DW05, ZL04a]. Systemic [KB06]. Systems [ACM03c, ACM05b, ANRS01, Ano02c, BCS02, BRTM09, CP02, ELvS01, Fe106, GS03, GRW06, IEE01b,
Systolic [KLY02, KKY02, MP01c].

Table [Ano03c, MFFT05, XFZ01, BZ03, CC05b, Has00].

Tag [BP05].

Tags [OS06, ACdM05].

Taipei [Lai03].

Taiwan [Ano03a].

Takagi [LKYL00].

Takagi-cryptosystem [LKYL00].

Takaragi [WHLH03].

Taking [CDS07, Lai07, PM00].

Talbot [Rot07].

Talk [FGM00a, Lan00d].

tamer [Kap05].

Taming [Aba00, Lov01].

Tamper [LTM+00].

tampering [PS08b].

tandem [DPT+02].

tank [Pau03].

tar [Str02].

targama [MAaT05].

Target [MV01, Pau03].

Tarragona [DFPS06].

tasks [XQ07].

Tate [Jou02, SG09].

TATSU [TS00].

tattling [CHK+08].

TC [DKU05].

TC-11 [DKU05].

TC-6 [DKU05].

tc [ELvS01].

TC8 [DFCW00].

TC8/WG8.8 [DFCW00].

TCB [SPHH06].

TCC [HR06, Kil05, Nao04].

TCP [CD01b, Ols00, SBB05].

TEA [CV05, HSR+01, HSRI02, HHH+04, MHL+02, WN95].

Teaching [McA09, Snm06, Gy09].

Tech [TvdKB+01, Uin00c, Gra01, Un00f].

Technical [BHM03, GS07b, Lan00c, TL02, USE01b, USE01a, USE02c].

Technique [CC02a, Pau09, PQ03, SC02a, VW01, CL00, Che08b, Pau03].

Techniques [AIP01, BSW09, Bih03, BBPV00, BDP02, CC04a, Cra05a, DBS+06, Dun06, Ken02b, Kun02, KO03, MKP09, NCRX04, PJK01, Pfl01, Pre00, Shi08, YKW01, AB09, BM05, Che08a, DY01, DHMR07, DY09a, Gal02, ISO04, KP00, Man08, Pin02, Pin03, PV01, SET08, Swe08].

Technologie [RSA09b].

Technologies [MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZWC02, ATS04, PB01, TTTZ01].

Technology [CB01, DHR00, Kat05b, Nie02b, VVS01, VDK05, vW01, Mar05b, NR04, Shp99, Wag03].

Theoretical
Theoretically [AP09, DM00b]. Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, BiH03, Boy01, CC04a, Cra05a, Des02,Fal07, HR06, Hay06, IZ00, Irw03, Kin01, Knu02, LaI03, Lee04b, Lut03, MNT00, Mao04, NP02a, Nao04, Oka00, PY06, Pf01,Pre00, Rot05, Roy05, Sch06b, Shp03, Spr03, TW02, Vau05a, Wal00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cos00, DW05, Gar04, HHL00, HW98, Joy00, Kil05, Lam01, PPV96, Rot02b, Rot03, SCS05a, Sho05b, Ste08, Sti95, Sti02, Sti06c, Tat05, TW05, Was08b, HR06, KXTZ09, Kil05, Nao04, Nie02a, Nie04].

There [Bar00b, GW00]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Sch03]. Third [AL06, BS01b, CGP03, HR06, IKY05, KNP01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QSO0, CGH00b].

third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM00].

Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thirty [ACM02]. Thirly [ACM02].

Thirty-Fourth [ACM02]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT00]. Thoughts [Joh00]. Threat [Por06, SS04, BK00, Geb04]. threats [CNPQ03]. Three [BR00b, LSH00, MAaT06, AJ08, CLC08, FGM03, GPS05, LKY05b, MF07, MAaTxx, SP006, YC09, ZL04b].

Three-Key [BR00b]. Three-party [LSH00, CLC08, YC09]. three-principal [ZL04b]. Threshold [AF04b, AIP01, BT05, BTW08, BDDS03, BSS02, CCD07, CND01, DK01, DNO3, DG03, FG01a, FP01, JL00, KY02a, Kin00, Kin02, Kog02, LZX03, LCZ05a, LPO1, MJ02, Nie03c, ST07, WQWZ01, Wan04b, WH03, XS03, BC005, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, HWW02, HW03, HW05, JLL01, LC04, LCC05, LCZ05c, SCL05, TYH04, WHLH03, XCO5, YTH04]. Throughput [HV04, LS01b]. thwarting [WL07]. TI [GBK01]. tib [MA07]. Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01]. Time [AK02a, App07, AJO08, BPST02, BS00b, BSW01, CU01, CJO03a, CV06, CLZ02, Dri02, GP08, HM02b, Ina02b, KL05, Kuh02a, LP02a, Lan00b, LLL05, LDM04, May04, Oec03, Pli01, QSR02, RR02, CAC03, CCK04b, CL00, DS02, GS07b, GM04, HHC05, LC04a, MRST06, NS05a, YZDW07, hY08, DK08].

Time-Domain [Kuh02a]. Time-Free [CNV06]. Time-Limited [AK02a]. Time-Memory [AJ008, Oec03, QSR02]. Time-Memory-Data [DK08]. Time-Reversed [Ina02b]. time-space [NS05a]. time-stamping [HHC05].

Time/Data [BS00b]. Timed [BN00b, CHK08, LKJ01, MA01, HGNS03, Zha06].

Timed-Release [CHK008, MA01, HGNS03]. times [AJ08, CCK04b, Mol05].

time-stamp [YW04].

timestamp [YS05a]. timestamp-based [YW04].

Timestamping [MSTS04]. Timing [CKQ03, CWR09, Law99, Sch01b, SWT07, AS05, DKL00a, K09, OS00].

timing-attack [KSR08]. Tiny [Bar00b, WN95, An03].

Tipsy [TvdKB01]. Tissue [MYC01].

Title [ZYH03]. Tls [HSD05, JK02b, JJ02b, SBEW01, BFCZ08].

TMAC [KI03]. TMS230C6x [WWGP00].

today [Lie02, Nis03a]. Together [WD01].

Token [Fri01, RAS00d, RSA01, CS04].

Tokyo [An00b]. Told [ES00a].

Tolerance [An04a, BK06b, ZL04a]. Tolerant [DS03, HS01, BKW03, HGR07, Lin07, P06, RM04, Yb04].

Tolerating [KSR02, SKR02]. too [Sch05c, V01]. took [IE09a].

Tool
[Ano02b, Ano02c, Kil01b, GPG06]. Toolkit [NIS01a, Sha01a]. Tools [Ano02b, Ano02c, Bar00b, Gol01b, Ken02b, Ust01b, Bai08, Cas02, GC05, NCRX04, SETB08, Kat05b, Puc03]. toolset [Jen09].

Top [Cal01, Fox00, Jan06, MV00, AJ08, GPC08].

top- [GPC08]. Top-Level [MV00].

Topics [HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oka04, Poi06, Pre02b]. topology [HJ07]. Tori [GV05, GPS06].

Top-Level [MV00].

topology [HJ07].

Tori [GV05, GPS06].

Toronto [MS05a, VY01].

torsion [KM04a].

torsion-subgroup [KM04a]. Torus [RS03, RS08, vDW04]. Torus-Based [RS03, RS08, vDW04].

Tossing [Lin01b].

totality [HRS08]. Touch [Pet02a]. tour [Pet08]. Town [KJR05].

trace-and-revoke [NN03]. Traceability [HLL03, HV05, WLHH05, WY05].

Transcript [Ano01a, Ano01b, Ano01c, Ano01g, Ano01h, Ano01e, Ano01i, Mal02, Nik02b]. Transfer [CT08b, Din01, GKM+00, KKL09].

Transferability [HSZI00]. Transfers [IKNP03]. Transform [ABM08, BR09, CPhX04, LKLK05, Nak01, SSFC09, VK07, BR06, Che07, OP01b, SR00, LPZ06].

Transformation [CT09, HLL05, DSP01].

Transformations [Fel06, KYHC01, LMTV05, Pag03].

transforms [La00]. Transient [Ric07, VS08]. Transistor [Coc02a].

Transistors [Bar00b]. Transit [Con00, Cal00c]. transition [TL07].

Transitive [BN02]. Translation [PY06].

TransLink [Cal00c]. Transmission [MLC01, SNR04, SVDF07]. Transparent [CCDP01, For01, Lin00a]. transport [Bao00].

Trappedoor [BPR+08, Fis01b, KO03, KO00, Gen04a, JSW05, PW08]. Trapdoors [GPV08]. Travel [Bur00]. Traversal [JLMS03].

Trawling [Knu00a, Knu00b]. treatise [Bla00, MAaT03, MAaT04, MAaT07].

treatises [MAaT06, MAaT07]. Treatment [CL05, DK08].

Tree [CC05d, GST04, JLMV03, KPT04, LKLK05, LM02, TNM00, Mon03, PCC03, WL02].

Tree-Based [GST04, KPT04]. trees [Che02, Tco07]. Trends [Ahm08, KB07, Or00, NdM06, PR04].

tricks [All03]. triggered [HJJ05].

tripartite [SW05]. Triple [ISH+01, BR04, CGBS01, Cor00a, FZH05, Kel05, LMP+01].

Triple-DES [Cor00a, LMP+01]. Triples [FS01b].

Tripwire [TvdKB+01]. trivial [KO00]. troubleshooting [HJW05].

True [BST03, Cha04, DVO8, EKH+03, HBF09, Pan07, SFD06, BGO8, BG09, GB09, Han06, HLMWZ09, Ste006, vT01, VKS09].

Truncate [CH08]. truly [BGL+03].

Truncated [CS05a, KM02, LHL+02, SKU+00, SKI01, GS09].

Trust [CHSS02, HCD02, Lin00b, LHL+08, MIT02, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, LMW05, LLW09].

Trusted [DK01,
WHI01, WV01, ARJ08, PS04c, ZYLG05.

Trusting [CKS09]. trustworthy [CCH05].

Truth [MNT00]. Tseng [Hwa05, XY04, ZAX05]. TTM [GCO08].

Tuesday [Uni00a, Uni00f, Uni00e]. tunable [LB05]. Tunny [Sal01a]. Turin [AL06].

Turing [Bar00b, RSA03a, Adl03, Coc03, Cop04b, Goo00, Pet08, Riv03, Sha03b].

Turkey [Bor00]. Turkish [DD02]. Turn [Tsa07].

Turning [DJLT01]. tutorial [Can06a, Puc06, Rot02b, Rot03, vT00].

Tweakable [DS08, HR03, LRW02].

Twenty [ACM03c, ACM05b, AAC+01, B+02, Lan00a]. Twenty-Eighth [B+02]. Twenty-first [Lan00a]. Twenty-Fourth [ACM05b]. Twenty-Second [ACM03c].

Twenty-seventh [AAC+01]. Twin [Ram01].

Two-Block [KCP01]. Two-factor [Sch05c, Ste05a]. Two-Key [K103].

two-level [DHL06]. Two-Party [KO04, Lin01b, MR01a, MLM03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, Ste05a, Ste01, TW07, WW05, XS03, YYDO01, CLOS02, DHL06, GCKL08, JW01, LMVT05, McN03, MCHN05, ZLX09].

Two-Tier [TW07]. Two-Way [DI02].

TWOBLOCK [Yan05]. Twofish [BF00b, FKSW00, IK00, Kego00a, Knu00b, Luc02a, Mur00, SKW*00].

Type [CKQ03, Hs01, KYHC01, PDMS09, RMS05, Vir03, GG08, Sha01d]. Type-Passing [Vir03].

typed [BG07b, FR08].

Typical [Gor02a, RSA00e, Lan05]. Typical [BSC01a]. Tzeng [QCB05a, Hsu05a, HLU05d].

U [DB04]. U-boat [DB04]. U.K. [CAC06].

U.S [Uni01]. U.S. [Bol02, PM00, Uni00b]. Ubiquitous [Sta03, LKZ+04]. UCON [LY05, PS04b].

UK [CZ05, Chr00, Chr01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01].

Ultimate [Di01]. ultra [Bam02, CH07a, DB04, Cal01, Win00].

ultra-lightweight [CH07a]. ultra-secret [Bam02]. Ultrafast [FF01a]. UltraSONIC [MMH02]. UMTS [Cha05b, HL07].

Un Authorized [An02e]. Unbalanced [FMP03, May02, HLL03]. Unbelievable [Len01]. Unborn [Pau02a]. Unbounded [RW02, WvD02]. Unbreakable [Ver06b].

Uncertain [See04, Sty04, Sch03].

UNCITRAL [MNFG02]. uncompletable [NS01a]. Unconditional [HM01b, May01, Pas05, RW03b, WW05].

Unconditionally [HSZI00, HSZI01, HSHI02, HSHI06]. Uncovering [MNT+00]. Uncrackable [An03b]. undeciphered [Rob02, Rob09].

Undeniable [GMP01b, GM03, JSJK01, Miy01, WQWZ01, CHC05, LH04, LCZ05a, SSM+08].

undergraduate [AA04b, Gha07].

undergraduates [DFGH04].

Understanding [CPG+04, Cra05b, Elb09, Gor06, PP09, Sun05, Lun09]. undetachable [BMW02b]. Unexpectedly [Bar00a].

Unforgeable [BKY02, KY01a]. Unicode [MJF07].

Unified [CBZ+04, HKA+05, MFS+09, SM03b].

Uniform [SPK08, TL07, SU07]. uniformity [Shp01, Shp04b]. Unimodular [CV03].

Unique [Lam91, Lys02, TH01]. United [DFCW00, JL01]. Universal [BOHL*05, CR03, CINP02, CS02, Ifo00, KKKP05, KO03, Pli01, Sho00a, SP79, Cal00c, PS04c].

universality [DS02]. Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DN02b, DN03, NMO05, RK05].

Universally-Composable [AF04b]. Universiteit [BBD09]. University [Kat05b, Puc03, Rot07, Top02]. UNIX [CCDP01, Har01a, Har01b, Hö01, Wit01].
UNIX-Type [Hö01]. Unknown [CT08a, Luc02b, CSW05, HJ07]. Unknowns [CMB+05]. unleash [McN03].
unlinkability [WHH05]. Unpredictability [BS01d]. unprotected [ASK05]. unsolved
[Bel07, GG05a]. untold [DB04].
untraceability [CL09, LHY05, Par04]. Untraceable [ACdM05]. Untrusted
[BMK00, CGK+02, LSVS09, LLK05, ZBP05]. unusual [GG05a]. Unveiled [Bar00a].
Update [TEM+01]. Updated [Cho08a]. upgrades [Ano02c]. upon [DFG01]. UPPAAL
[BBB+02]. Upper [BP03b, DIRR05, KMT01]. Upwards [FV03]. URSA [LKZ+04]. US$54
[Duw03]. USA [ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM09, BDO8, Des02,
Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KKP02, KJR05, Ki05, KP01, Men05,
Men07, Nac01, Nao04, Ok04, Oio06, Pre02b, Sch01d, Sh05a, Sio1, YDKM06, ACM10,
Bel00, Bon03, BCDH09, ELvS01, FMA02, IEE01a, IEE05a, IEE05b, IEE08, IEE09b,
Ki01a, MS05b, NIS00, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SMP+09, USE00c,
USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, Wi99, Yun02a]. usability
[CG05]. Usage [LY05, PS04b]. Use [Bai01a, BWB02,博02, BQR01, CPS07, Dre00,
ISO05, Kra03, LCK04, Pau09, PBTW07, Str01a, WS05, Win01, CG05, OS07]. used
[MSV04]. useful [SM03a]. UseNet [Coc01a]. USENIX [Coc01a]. User
[BGP02, CL01b, CMB+05, DP00, Had00, HY01, KZ09, LSZ05, JR03, OHO8, PS01b,
Sao7, SSM+08, Str01a, Ts01a, BMB00, CL0d4, DLY08, GMLS02, Hsu05b, HL05b,
KC05, LAPS08, LHY02, LLH02, LKY04, LKY05a, LHL03b, LC05a, LC01, Par04,
SS03, SZS05, TWWL05, WLT05a, YS04, YRY04, ZYL05, vOT08]. User-Centered
[CMB+05]. user-controlled [LAPS08]. user-drawn [vOT08]. user-friendly
[SZS05, WLT05a]. user-level [SS03]. Users
[LLS05b]. Uses [Bau01c, RSQL03]. ushers
[Bur00]. Using [AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01c, Ano01h, ADDS06,
BJP02, BH06, BK06a, Bau01a, Bau01b, BP06, BPT02, BR09, BT02, BMK00,
BMP00, BL02, Che01a, CLLL00, CGBS01, CCW02, CCM01, CH07c, Cir01, Di05,
DPR01, DP00, DW01, DGH+04, EFY+05, FJ03, FMP03, Fri01, GC01a, GL01, GS+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, PJK01, PCK02,
PK01, Sho00b, SK05a, Sma03a, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VPG01,
WY02, Wit01, XZ01, YKMY01, YLLL02, YSS+01, ZW01, Zhe01, ASW00, AL07,
BCL05a, BCW05, BK07, CDS07, CWH00, CL04d, CCK04b, CCH05]. using
[CHY05b, CKY05, CJ05, Che07, Che08a, Che08b, CJ04, CJK03, Cos00, DZL01,
Dun02, DFG00, FWTC05, GC00a, GMR05, Gen09b, GSO9, HHSS01, HW05, HAU04,
HTW07, Hir09, HW04, HY03, HL04, JRR09, KOY09, KC09, KLY03, KB09, KKL09,
KKJ+07, KSW06, KR03, Ku04, KC05, LHY02, LLLH02, LKY04, LCP04, LLL04b,
LW04, LKY05a, LLW05, LLW09, LF0W04, LC05a, LLC06a, LWK05a, MT07, Mic01,
NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, RC05, Sco04, Sha04b, Sha05b,
SHH07, Tan07a, TLH05, Ts05, TJC03, VK08, Wan04b, WK05, Wan05, WGL00,
WH03, YW04, YC09, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. utility
[Gua05]. Utilizing [Str02].
V [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0
[Man01, RSA00c]. v2.1 [RSA02]. v2.11 [RSA01]. V5 [It000]. V5.1a [CHK+08]. Vail
valid [Wan04b], valid-signature [Wan04b].
Validation [ABRW01, BLR01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02].
Valuable [PM00]. Value [BR09, GIS05, BMW02a, DK08, WWTH08].
valued [DZL02, MS02b].
Validation [ABRW01, BLM01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02].
Valuable [PM00]. Value [BR09, GIS05, BMW02a, DK08, WWTH08].
valued [DZL02, MS02b].
Valuable [PM00].
Validation [ABRW01, BLM01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02].
Valuable [PM00]. Value [BR09, GIS05, BMW02a, DK08, WWTH08].
valued [DZL02, MS02b].
Valuable [PM00].
Validation [ABRW01, BLM01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02].
Valuable [PM00]. Value [BR09, GIS05, BMW02a, DK08, WWTH08].
valued [DZL02, MS02b].
Valuable [PM00].
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 [dVP06]. Wagstaff [Kat05b]. Wahab [MAaT07]. Walking [Fox00]. Wallet [ETZ00, JL04]. Walsh [MS02b]. WAN [Höf01]. WAN-Cluster [Höf01]. Wang [SZS05]. WAP [JRFH01]. Walking [Fox00]. Wallet [ETZ00, JL04]. Walsh [MS02b]. WAN [Höf01]. WAN-Cluster [Höf01]. Wang [SZS05]. WAP [JRFH01].

Vulnerabilities [CSW05, DMS07, Swi05, XNK+05]. Vulnerability [KHL09, SGA07, YRS+09].

Washington [S*03, USE00a, USE01c]. WaSP [Coc02b]. WASSA [Ano05b]. Watch [MAa00a, Joy03a]. Waterloo [HH04, HH05, ST01d]. Watermark [AS01b, GMV01, JX05, KHY04, Kwo03a, Meh01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zan01, CL08, LYGL07, LLC06a].

Watermark-based [Kwo03a]. Watermark-Fingerprint [KHY04]. Watermarking [ST01c]. Watermarking [AS08, AK02b, AHK03b, AS01c, Arn01, ARC+01, BR09, BSC01a, BSC01b, BSL02, BQR01, BSN000, CC02a, CH01b, CDTT05, CT09, CM02, CMB+08, DWN01, DNP07, EFY+05, EIG01, GW01, HT06, JK+01, KCR04, hKLS00, KLL01, Kun01, KT00, LZ09, LLS05a, LLLK05, LZ01, LZP+04, IWS05, LPZ06, LL01, LSDK05, MM01a, MNS01, Nak01, OMT02, PJJH01, PJK01, PR01, PBM+07, Qu01, Sam09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SMT01, SPK08, VVS01, VHP01, VK07, WH09, WNY09, WWL+02, WLT05b, XFZ01, ZTP05, ZWC02, AHK03a, BBK05, CC02b, Che08b, CYH+07, CCD+04, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, HHC05, JDJ01, JA02, KP00, LDD07, Lin00a, Lin01a, LLC06a, LLC06b, MB08, MCHN05, PK03, mSGFtL05, WJP07, WQ08, Way02b, Way09, WMDR08, XMST07, YZDW07, YPSZ01]. Watermarking [ZLZ07].

Watermarks [Ben00, BB00a, MLC01, SUG01, YLLL02, MB08]. Watershed [FBW01]. Watershed-from-Markers [FBW01]. WAV [XFZ01]. WAV-Table [XFZ01].

Wavelet [BR09, GW01, LLLK05, LZ01, Nak01, VK07]. Wavelet-Domain [LZ01]. Way [BYJK08, BM01a, CLH02, DIS02, DMS00, Fis01b, GKK+07, HNO+09, HR05, KO03, K000, LT05, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cha00b, GKK+07, HR07, HRS08, JZ09, KK07, KKK05, KK03, LW04, LPM05, LQ08, LLKL01, Mc02a, Poi00, YW05, YRY05b, ZW05a]. Wayness [KI01a, PV06b]. Ways [BB02]. WCC [Ytr06]. WDDL [MMMT09]. Weak [HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00]. Weakening [ZD05]. Weakly [BS00a, CHS05]. Weakness [SW05, SZS05, YPKL08]. Weaknesses [FMS01, He02, KCL03, KCC05, SGGB00]. Weapons [RR03b]. Weather [WWL+02].

Web [Mar05a, BFG05, BFG08, Ano01c, Ano02c, Ano03b, AEV+07, BFG04, BC04b, CCY01, C01a, Coc02a, Coc02b, CZB+01, Del07, DMSW09, FSS01, GS02a, GSV02, HM05, JRB+06, KCDT07, LWW00, LLS05b, LXM+05, MPPM09, PM00, RR04, Sam09, SS06, Sch01a, SBG07, TMM05, WA06, YSS+01].

Web-based [CCY01]. Web-enabled [CCY01]. webcam [McN03]. WebFountain [Ano03b].

Webrelay [Zha00]. Weight [CH07c, GK02, WT02]. Weighted [BTW05, BTW08, YZ00]. Weil [BF01b, BF03, Jou02, Kir03]. Well [WWGP00]. Welschenbach [Ter08]. Welsh [Rot07]. went [AJ08]. WEP [SIR04]. were
[Hau06]. Wesley [Puc03]. West [Fra01, Jue04, Syv02, Wri03]. Westbridge [Ano02c]. Western [CZB+01]. Weyl [Sug03]. WG [DFPS06]. WG11.1 [ELvS01]. WG11.1/WG11.2 [ELvS01]. Wheeler [ABM08, Bar05]. Where [Bar06]. WHIM [JA02]. WHIRLPOOL [RB01]. Whisper [NABG03]. Whitening [Oni01]. Whitfield [Jan08]. Who [CZB+01, Urb01, Hau06]. whole [CPG+04]. Wi-Fi [Sty04, VGM04, FMA02, Bar03]. Wi-Foo [Puz04, VGM04]. wicked [Lud05]. Wide [DR02a, SBB05]. Width [OT03b]. Wiener [Duj08, Duj09]. WIESS [USE00b]. Wiley [And04, Gra01]. Will [Ort00, Cla00b]. William [Pag03]. Williams [Mii01a]. Window [OT03a, SSST06]. Windows [USE00a, DGP07a, DGP07b, DGP09, Fer06, HB06, WD01, Wit01]. Wins [Bar00b]. Wired [Gil07, SIR04]. Wireless [AAE05, Bar03, BCH+00, ECM00b, Fin06, KH05, KHD01, LNL+08, Pau03, PJDH09, Puz04, Sin01a, Sty04, SYLC05, VGM04, YSR01, ZYN08, ZW02, BP03a, BBG+02, CCM09, Cha05b, GW08, GG05b, JRR09, KTXT09, KB09, LDH06, LPV+09, LW05a, Lin07, MJF+08, NC09, NLD08, PSCM07, Par04, Pat02a, Pat02b, SLP07, SZ08, TP07, Vac06, Wan04a, YT05, CS08b, ECM00a, PDMS09]. Wiretapping [Ch08a, DL98, Jan08, DL07]. WISA [CSY09]. Within [MR02a, CHM+02, MR02b]. Without [BCL+05b, Bla01c, BB04, BH07, Har06, NA07, CH01a, CCK01b, CYH04, CCH05, CJ04, CDD07, CNV06, DK01, KG09, Ku04, LV07, LW04, LKY05, LL06, LCZ05b, Lys07, MP02, Mar07, PS04c, 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 [BG04]. Works [Net04]. Workshop [ACM05a, Ano05b, AL06, BDZ04, BBD09, BD08, C205, Chr00, Chr01, CCMR02, CCMR05, CSY09, DR02c, Des02, GH05, IEE01b, JZ00, JQ04, KKP02, KCR04, KGL04, Kim01, KP01, KNP01, LST+05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RR06, RM04, Sch00b, Sch01d, TB02, USE00b, YY01, Vau05a, WK03, Ytr06, AMW07, AJ01a, BCKK05, Bir07, CKL05, GKS05, HH04, HH05, HA00, ST01d]. World [Ber03, HW01, Nik02a, Nik02b, Sch00d, Sty04, YKMB08, Ark05, Bel07, GG05a, HH06, Hus01, KPS02, Kee05, Lie05, Liu09, Rob02, Rob09, Sch03, SL07, Bec02, Bud00a, Bud02, Hau03, MH09, OC03, Sty04, See04]. Worlds [Wii01b]. Worm [LJL05, CSW05]. Worms [ZGTG05]. Worst [CCM05, HR05, Mic02a, Mic02b, Pei09]. worst-case [HR05, Mic02a, Mic02b, Pei09]. worst-case/average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. Wrapper [Ols00]. 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, CWJ01, HL05c, MS03a, YY05b]. Wu-Lin [YY05b]. Wuhan [TTZ01]. WW [Sal00a]. X [For04]. X.509 [SJ05]. X.931 [Kel05]. X.99.62 [ANS05]. Xbox [Ste05b]. XCBC [GD02]. XECB [GD02]. Xia [CJT04, Sha05a]. Xiamen [DWML05].
References

Al-Akaidi:2004:FSP

Aly:2004:CSP

Apers:2001:PTS
Peter M. G. Apers, Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Kotagiri Zimmermann [McLo06, Tuc66]. Zero-Knowledge [AS01b, BP04, Cou01, DFS04, HNO°09, LHL°08, MR01b, MV03a, Pas05, Ros00, Ros06a, CSW05, Dam00, PBD07, KK07]. z10 [AAC°01]. Zeta [Ver02]. Zhang [JW01, YY05a]. Zhou [PKH05]. Zimmermann [McLo06, Tuc66]. ZK [PBD05]. Zodiac [HSM°02].

References

XXX:2002:CC

Al-Akaidi:2004:FSP

Aly:2004:CSP

Apers:2001:PTS
Peter M. G. Apers, Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Kotagiri Zimmermann [McLo06, Tuc66]. Zero-Knowledge [AS01b, BP04, Cou01, DFS04, HNO°09, LHL°08, MR01b, MV03a, Pas05, Ros00, Ros06a, CSW05, Dam00, PBD07, KK07]. z10 [AAC°01]. Zeta [Ver02]. Zhang [JW01, YY05a]. Zhou [PKH05]. Zimmermann [McLo06, Tuc66]. ZK [PBD05]. Zodiac [HSM°02].

References

XXX:2002:CC
REFERENCES


Al-Azzoni:2005:MVC


Anshel:2001:NKA


Almgren:2000:HWC


Ababneh:2009:CSE


Ashraf:2009:SBE


Aamodt:2003:CSP

REFERENCES


An:2001:DER


Atallah:2009:ATC


Abadi:2000:TA


Aiello:2004:JFK


Abdalla:2005:SER

Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascale Paillier, and Haixia Shi. Searchable encryption revisited: Consistency prop-


Anderson:2000:CS


Austin:2000:ASF


Adjamoh:2008:BWT


Ansper:2001:ELT


Ambainis:2009:NEQ

Andris Ambainis, Jan Bouda, and Andreas Winter. Non-malleable encryption of


REFERENCES


REFERENCES

ACM:2005:PTF


[ACM05b] ACM:2005:PTF


[ACM05c] ACM:2005:SPA


[ACM06] ACM:2006:PTE

ACM:2007:SPA


ACM:2008:SPA


[ACM08] ACM:2008:SPA

ACM:2009:SPA


ACM:2010:PAI

References

Algesheimer:2002:ECM


Alvarez:2005:EBS


Ahmad:2007:ADE


Anyanwu:2009:DCS


Avanzi:2006:ESM

Roberto Avanzi, Vassil Dimitrov, Christophe Doche, and Francesco Sica. Extending scalar multiplication using double bases. Lecture Notes in Computer Science, 4284:
Arnold:2007:CSE


Adikari:2009:HBT


Arazi:2005:RPK


Alvarez:2005:SSS


REFERENCES

Ateniese:2006:IPR


Attrapadung:2006:FSS


Akkar:2001:IAS


Acquisti:2009:PSS


Akavia:2006:BOW


Akavia:2010:EBO


Ahmad:2007:CSS


Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB


Applebaum:2004:CNS

Applebaum:2006:C


Al-Ibrahim:2001:AMS


Attali:2001:SCP


Attali:2001:JSC


Aid:2008:NSA

Matthew M. Aid and Thomas R. Johnson. National Security Agency releases history of cold war intelligence activities: Soviet strategic forces went on alert three times during

Avoine:2008:CIT


Al-Jarrah:2008:NKM


Abe:2002:KES


Agrawal:2002:WRD


Armknecht:2003:AAC

Akinwande:2009:AHC


Amir:2004:PGK


Agrawal:2002:PP


Acicimez:2006:PSB


Agrawal:2004:OPE


Amadio:2000:RPC

REFERENCES


Atallah:2004:ALA


Atzeni:2006:PKI


Anshel:2007:RME


Allen:2003:EST


Allman:2006:MAW

Amadio:2002:SRP


Alvarez:2000:CCE


Alvarez:2004:KCC


Andem:2003:CTE


Anderson:2004:BRR


Anderson:2007:SSS

REFERENCES


[Ano01a]


[Ano01b]


[Ano01c]

REFERENCES


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 Telel-
REFERENCES


[Ano03a]

Anonymous:2002:QCQ


[Ano02d]

Anonymous:2002:RUB


[Ano03a]

Anonymous:2003:TMC


[Ano03a]

Anonymous:2003:NUP


[Ano03a]

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>1957</td>
<td>H. Riesel</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. Wiehl</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>Armstrong 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, Kerby</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</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmoe</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, George</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, George</td>
</tr>
</tbody>
</table>

REFERENCES

- http://www.mersenne.org/
- http://www.mersenne.org/prime.htm
- http://www.mersenne.org/various/57885161.htm
- http://www.utm.edu/research/primes/index.html
- http://www.utm.edu/research/primes/notes/3021377/
Anonymous:2004:CPS

Anonymous:2004:CJL

Anonymous:2004:NGJ

Anonymous:2005:CEC

Anonymous:2005:WAS

Anonymous:2006:RC

Anonymous:2006:SSD

Anonymous:2007:CPSh

Anonymous:2007:CPSf
[Ano07b] Anonymous. Call for papers: Special-purpose hard-

**Anonymous:2008:SHS**


**Anonymous:2013:DSS**


**Ateniese:2001:SRC**

REFERENCES


References


Shunsuke Araki. A Nyberg–Rueppel signature for multi-

**Atallah:2001:NLW**


**Aaraj:2008:ADH**


**Arkin:2005:CND**


**Arnold:2001:AWB**


**Agrawal:2003:MCA**

REFERENCES


Abe:2001:SPA


Adelsbach:2001:ZKW


Agung:2001:ICI


Agarwal:2008:DWS


Ashburn:2003:PBA

REFERENCES


[ATSVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In...
REFERENCES


Alster:2001:PKC


Arnold:2004:IPN


Avanzi:2003:CAD


Aalberts:2000:DSB


Abadi:2005:SAC

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


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

1075-3583 (print), 1938-3827 (electronic).


REFERENCES


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


[BBPV00] Christophe Bobineau, Luc Bouganim, Philippe Pucheral, and Patrick Valduriez. PicoDMBS: Scaling down
REFERENCES


Blundo:2005:SCN
[BC05b]

Bergadano:2001:CSA
[BCC01]

Brier:2001:CRS
[BCCN01]
REFERENCES

Blundo:2006:VCS


Bruguera:2009:PIS


Burnett:2000:EMG


Barnum:2002:AQM


Brown:2000:PCW

Michael Brown, Donny Cheung, Darrel Hanker-

Breunesse:2005:FMS


Boneh:2007:CCS


Butler:2006:FAK


Barni:2005:DWI


Bao:2005:PSS


Barak:2005:SCA

Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. In Shoup [Sho05a], pages 361–?? ISBN 3-540-28114-2. ISSN 0302-9743
Bresson:2001:PAG


Bresson:2002:DGD


Bresson:2002:GDH


Bolle:2003:GB


Bresson:2007:PSA

Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably secure authenticated group Diffie–Hellman key exchange. ACM Transactions on Information and
REFERENCES


REFERENCES


REFERENCES


[BDDG01] Feng Bao, Robert H. Deng, Willi Geiselmann, Claus Schnorr, Rainer Steinwandt,
REFERENCES


Bhattacharyya:2009:VPA


Biham:2002:EDL


Biham:2002:LCR


Biryukov:2009:KRA

Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES variants with up to 10 rounds. Report, University of Luxembourg, Luxembourg; École Normale Supérieure, 45 rue d’Ulm, 75230 Paris, France; Einstein Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel; Computer Science department, The Weizmann Institute, Rehovot 76100, Israel, November 8, 2009. URL
REFERENCES

Blundo:2000:VCG

Bodei:2002:FLD

Boreale:2002:PTC

Bertoni:2009:RPK

Biryukov:2004:MLA

Baldwin:2009:PSS
Adrian Baldwin, Chris Dal-
REFERENCES

[102x681] REFERENCES

129


[417x204] [Boneh:2001:MFR]

Dan Boneh, Xuhua Ding, Gene Tsudik, and Chi Ming Wong. A method for fast revocation of public key certificates and security capabili-

[407x562] [Bec02] Bengt Beckman. Codebreakers: Arne Beurling and the Swedish crypto program during World War II. American


[Bel07] Richard Belfield. The six unsolved ciphers: inside the mysterious codes that have confounded the world’s greatest cryptographers. Ulysses, Berkeley, CA, USA, 2007. ISBN 1-56975-628-7 (paper-
REFERENCES

Bello:2008:OPR


Bruss:2007:QCS


Benedens:2000:AIW


Benantar:2001:IPK


Benson:2001:VS


Benantar:2002:IPK


Berson:2000:CE

REFERENCES


**Biham:2000:IDR**

[BF00a] Eli Biham and Vladimir Furman. Impossible differential on 8-round MARS’ core. In NIST [NIS00], pages 186–194. ISBN ???. LCCN ???.


**Biham:2000:IID**


**Boneh:2001:IBE**


**Boneh:2001:EGS**

REFERENCES

Boneh:2003:IBE


Boldyreva:2005:ARO


Bisseling:2006:MSM

Rob H. Bisseling and Ildikó Flesch. Mondriaan sparse matrix partitioning for attacking cryptosystems by a parallel block Lanczos algorithm — a case study.


Boldyreva:2006:SO


Bhargavan:2004:SWS


Bhargavan:2008:CVI

Bhargavan:2005:SWS


Bhargavan:2008:VPB


Bhargavan:2008:VII


Biham:2002:DCQ


Brown:2007:SAN


Bugliesi:2007:SIT


Blaszczyk:2008:NMT

[BG08] M. Blaszczyk and R. A. Guiney. A novel modelled true random binary
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[BB03] James Backhouse, Carol Hsu, and Aidan McDonnell. Technical opinion: Toward

Bajard:2004:FRI


Barkol:2005:SCC


Beimel:2005:PNS


Bi:2009:MCE


Bidgoli:2003:EIS


Biggs:2008:CII

Biham:2000:CPR


Biham:2002:HDE


Biham:2003:ACE


Beimel:2000:RSC


Bajard:2003:EMG

J.-C. Bajard, L. Imbert, C. Negre, and T. Plantard. Efficient multiplication in $\text{GF}(p^k)$ for elliptic curve cryptography. In Bajard and
REFERENCES


Bajard:2005:AOP


Biryukov:2007:FSE


Bishop:2003:ICJ


Bishop:2003:CSA


Barkol:2008:CPR


Boyce:2002:IAM


Blaser:2002:PCC
REFERENCES


William Boni and Gerald L. Kovacich. Netspi-

**Burnside:2005:CCP**


**Barker:2006:RRN**


**Barreto:2002:EAP**


**Barker:2007:RRN**

REFERENCES


Bucci:2008:FDR


Blanchet:2001:ECP


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


Blaze:2001:LYS


Blanchet:2002:SAS


Blaze:2002:CI

Matt Blaze. Cryptography and insecurity. In USENIX
REFERENCES


[BLM01] Diana Berbecaru, Antonio
Blunden:2009:RAE  

Batina:2001:AWD  

Blomer:2001:LSE  

Blomer:2003:NPK  
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Bellare:2002:PRI


Ben-Or:2005:UCS


Bouganim:2003:CSD


Bollinger:2002:UFO


Bondi:2000:CVB


Bodycombe:1999:CC


Bon00]
REFERENCES

459 pp. LCCN QA76.73.B3 B665 2000.


Barak:2003:DC


Barak:2007:DC


Boyen:2003:MIB

REFERENCES


REFERENCES


Blanchet:2005:VCP


Beissinger:2006:CUM


Baer:2007:CIS


Bellare:2000:AKE


Borst:2001:CSC


REFERENCES


[BR04] M. Bellare and P. Rogaway. Code-based game-
REFERENCES


Butler:2009:LIB


Brustoloni:2006:LEN


Bierbrauer:2000:AIW


Biryukov:2000:CTM


Barrett:2001:SSS

REFERENCES


[BS01b] Bigun:2001:AVB


[BS01d] Biryukov:2001:SCS

[BS01c]


Boneh:2001:UBE


[BS03] Bajard:2003:ISC
REFERENCES


REFERENCES


REFERENCES

Barak:2003:TRN

Biryukov:2001:RTC

Bethencourt:2009:NTP

Biehl:2002:NDP

Boyer:2002:LDS
Beimel:2005:CIW

Beimel:2008:CIW

Black:2002:SCA

Buchmann:2000:CTC

Buchmann:2000:IC

Buchmann:2001:IC
Johannes Buchmann. *Introduction to cryptography*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
REFERENCES


REFERENCES

Town and Country Resort Hotel, San Diego, CA.

Burr:2003:SAE


Burr:2006:CHS


Baker:2007:ISU


Blake-Wilson:2002:RUE


Butler:2000: NSA


Bellare:2003:FSP

Bar-Yossef:2004:ESQ


Bar-Yossef:2008:ESQ


Bertlmann:2002:QUB


Bond:2003:DTA


Borders:2005:CHP


Carrington:2002:EDS


Staff:2003:NTC

[CAC03] 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).
REFERENCES


[Can06a] Ran Canetti. Security and composition of cryp-


Carter:2001:SCT

Carlet:2002:LCC

Casey:2002:HCC

Casselman:2006:MTE
Cobas:2001:CTA

Cooper:2005:AAP

Chandramouli:2006:BPA

Cachin:2000:OFS

Chan:2001:CRP
REFERENCES

173

CODEN IJCMAT. ISSN 0020-7160.


REFERENCES

Chan:2005:STM


Chang:2005:ASN


Chang:2005:EAP


Comon:2005:TAO


Crandall:2005:SAM


Ch:2001:WEF


Collberg:2004:DPB

REFERENCES


REFERENCES

Christianson:2001:PKC

Choi:2005:JMA
Choi:2002:SPI

Christianson:2005:SPI

Castelluccia:2009:EFS
Claude Castelluccia, Aldar
C-F. Chan, Einar Mykle-
tun, and Gene Tsudik. Ef-
fficient and provably secure
aggregation of encrypted
data in wireless sensor net-
works. ACM Transactions
on Sensor Networks, 5(3):
20:1–20:??, May 2009. CO-
DEN ???. ISSN 1550-4859
(print), 1550-4867 (elec-
tronic).

[CD00]

Chen:2008:NMA

Yalin Chen, Jue-Sam Chou,
and Hung-Min Sun. A
novel mutual authentication
scheme based on quadratic
residues for RFID systems.
Computer Networks (Ams-
terdam, Netherlands: 1999),
52(12):2373–2380, August
22, 2008. CODEN ????.
ISSN 1389-1286 (print),
1872-7069 (electronic).

[CCTS08]

Caboara:2008:GBP

Massimo Caboara, Fabrizio
Caruso, and Carlo Traverso.
Gröbner bases for public key
 cryptography. In Jeffrey
[Jeff08], pages 315–324. ISBN
1-59593-904-0. LCCN ????

[CCW02]

Choi:2002:IPP

Dug-Hwan Choi, Seungbok
Choi, and Dongho Won.
Improvement of probabilistic
public key cryptosystems us-
ing discrete logarithm. Lecture
Notes in Computer Science,
2288:72–??, 2002. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/1
bibs/2288/22880072.htm;
http://link.springer-
ny.com/link/service/series/1
0558/papers/2288/22880072.
pdf.

[CCW02]

Camenisch:2000:VEG

Jan Camenisch and Ivan
Damgård. Verifiable encryp-
tion, group encryption, and
their applications to separ-
able group signatures and
signature sharing schemes
(extended abstract). In Ad-
vances in cryptology—
ASIACRYPT 2000 (Kyoto),
volume 1976 of Lecture Notes
in Comput. Sci., pages 331–
345. Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
many / London, UK / etc.,
2000. URL http://
link.springer-ny.com/
link/service/series/0558/1
bibs/1976/19760331.htm;
http://link.springer-
ny.com/link/service/series/
pdf.

[CCS08]

Cramer:2001:SDL

Ronald Cramer and Ivan
Damgård. Secure distributed
linear algebra in a constant
number of rounds. In Kil-
lian [Kil01a], pages 119–??
ISBN 3-540-42456-3 (paper-
back). LCCN QA76.9.A25
C79 2001; QA267.A1 L43
no.2139. UK£47.00. URL
REFERENCES


Cimato:2005:ICV


Cramer:2005:CMS


Cramer:2005:SCP


Cavallar:2000:FBR


[Chawla:2005:TPP]


[CDMP05]


[Cramer:2001:MCT]


[Chapman:2001:PEA]

References


REFERENCES


[CFVZ06] Joan-Josep Climent, Francisco Ferrández, José-Francisco


Chodowiec:2003:VCF


Chodowiec:2001:ETG


Cranor:2005:SUD


Caballero-Gil:2009:GBA

REFERENCES

Catalano:2000:CIS


Coppersmith:2000:ICT


Caballero-Gil:2006:SSB


Crosby:2002:CHB

Scott Crosby, Ian Goldberg, Robert Johnson, Dawn Song, and David Wagner. A cryptanalysis of the high-


[Chen:2008:OVBa]


[Chen:2008:OVBa]

REFERENCES


[CH07c] Jaewook Chung and M. Anwar Hasan. Montgomery reduction algorithm for modular multiplication using low-weight polynomial form in-


REFERENCES

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

[189]

Chen:2005:EUG

[CHC05]

Chen:2000:JCT

[Che00]

Chen:2001:DEU

[Che01a]

Chen:2001:PDP

[Che01b]

Chen:2001:NVR

[Che01c]

Chen:2002:SFS

[Che02]

Cheng:2003:PPO
Qi Cheng. Primality proving via one round in

Chen:2005:TSS


Cheng:2004:BSD


volume&id=doi:10.1007/b99099.

Chen:2007:CIS


Chen:2008:CIS

Wen-Yuan Chen. Color image steganography scheme using DFT, SPIHT codec, and modified differential

[Chen:2008:MWS]


[CHH01]


[CHJ+01a]

REFERENCES


Coron:2001:OCC


Coppersmith:2002:CSC


Canetti:2003:FSP


Canetti:2005:ASN


Czeskis:2008:DED

Alexei Czeskis, David J. St. Hilaire, Karl Koscher, Steven D. Gribble, Tadayoshi Kohno, and Bruce Schneier. Defeating encrypted and deniable file systems: Truecrypt V5.1a and the case of the tattling OS and applications.
REFERENCES


REFERENCES


Chowdhury:2008:CBG


Christianson:2000:SPI


[Cho08b] Christianson:2001:SPI


Canetti:2005:HAW

REFERENCES


[CHY05b] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang.

Cimato:2002:DAP


Cirstea:2001:SAP


Cheon:2003:PTA


Chien:2003:HAP


Chien:2003:RSA


REFERENCES

198


REFERENCES


Cheon:2002:IID


Chung:2003:EPX


Chun:2003:DLC

Kilsoo Chun, Seungjoo Kim, Sangjin Lee, Soo Hak Sung, and Seonhee Yoon. Differential and linear cryptanalysis for 2-round SPNs.


Cox:2005:DWT


Chen:2009:SRP

REFERENCES

Coppersmith:2000:KRF

Coron:2000:FLA

Coron:2000:FLA

Canetti:2003:RCC

Cheon:2006:KPC
Jung Hee Cheon, Woo-Hwan Kim, and Hyun Soo Nam.


REFERENCES

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


[CL02c] Paul Crowley and Stefan Lucks. Bias in the LEVIATHAN stream cipher.
REFERENCES


[CL07] Ramaswamy Chandramouli and Philip Lee. Infrastructure standards for smart...


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. *ITS international*, 6(2):77–78, March/April 2000. [Cla00b]


REFERENCES

Chang:2001:FAM


Cheon:2000:NBC


Canetti:2002:UCT


Chen:2009:AKD


Clulow:2003:SP


Czumaj:2002:PTA

Artur Czumaj, Andrzej Lin-

**Camenisch:2000:CSS**


**Cox:2002:FYE**


**Courtois:2003:AAS**


**Chevallier-Mames:2005:ECB**


**Cojocaru:2005:ISM**

Alina Cojocaru and Maruti Ram Murty. *An introduction to sieve methods and their ap-

Cox:2002:DW


Crawford:2005:FBS

Diane Crawford, Marius Matioc, Steven M. Bellovin, Richard Hubert, Andrew D. Wolfe, Jr., David Foulser, 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).

Cox:2008:DWS


Cremers:2006:ISE


Campo:2001:JFC

REFERENCES


Chevallier-Mames:2003:FDS


Chao:2008:DNP


Caputo:2009:DIT

Crawford:2002:FEE


Coron:2004:SSL


Ciet:2003:PFI


Catalano:2002:HHL


Correia:2006:CAB


Czernik:2009:CRN

[CO09] Pawel Czernik and Jakub Olaszyna. Cryptographic ran-


Cochran:2002:NVW


Cochran:2003:NVC


Cole:2003:HPS


Constantinou:2000:CSC


Convery:2004:NSA


Conti:2009:GSH


Cook:2002:REJ

REFERENCES


[Cor00a] Francisco Corella. A fast implementation of DES
Coron:2000:ESF


Coron:2006:WC


Cosgrave:2000:NTC


Costlow:2003:BIM


Courtois:2001:EZK

Courtois:2003:FAA


Courtois:2004:FSB


Courtois:2003:AXA

REFERENCES

Chatzikokolakis:2007:FAP


Cimato:2006:PVC


Chow:2004:UDL


Chen:2004:SEP


Catalano:2004:IIP

REFERENCES

volume&id=doi:10.1007/b99099.

[Canetti:2007:CSH]

[Ciet:2001:SFC]


[Canetti:2003:UCJ]
Crampton:2005:UDR


Crowley:2001:MFL


Chhabra:2009:MSP


CRI:2000:DPA


Cramer:2000:SSB


Cramer:2002:UHP


Camenisch:2003:PVE

REFERENCES


www.jucs.org/jucs_11_1/increasing_robustness_of_LSB.

**Capaldi:2007:ADI**


**Chakrabarti:2007:PBA**


**Chatterjee:2007:CSC**


**Casey:2008:IFD**


**Chang:2008:DAP**


**Cusick:2009:CBF**


**Cai:2007:CSM**


References

Chu:2008:EOT


Chou:2009:ATI


Crawford:2001:FPV


Cheung:2001:TTP


Collberg:2007:DGB


Cheng:2001:NPT

Qi Cheng and Shigenori

---

Curtin:2005:BFC


---

Chaitanya:2008:QQM


---

Canteaut:2002:DCH


---

Cary:2003:MAC

REFERENCES


**Cheng:2009:NAS**


**Chang:2000:ELD**


**Chien:2005:NRS**


**Crosby:2009:OLR**


**Choie:2002:ICH**

Y. Choie and D. Yun. Isomorphism classes of hyperelliptic curves of genus 2

**Chen:2005:ENB**


**Chang:2008:EBD**


**Chung:2007:SBW**


**Chang:2005:CIA**

Ting-Yi Chang, Chou-Chan Yang, and Ya-Wen Yang.

**Chadwick:2005:PKI**


**Crawford:2001:FHC**


**Cheng:2005:RIC**


**Dodis:2003:CAA**


**Dale:2001:BSA**

Richard Dale. Biometric se-
security: It’s all about identification and authentication. 


**Damgaard:2000:ECZ**


**Danaj:2007:PAD**


**Danielyan:2001:AAS**


**Danas:2002:CUS**


**Davis:2001:ISV**


**Davis:2001:DSA**


**Davis:2001:DSE**


[DeBrosse:2004:SBU]

[Desmedt:2001:ERD]

[DiVimercati:2005:CSE]

[Doyle:2006:SCK]
Barry Doyle, Stuart Bell, Alan F. Smearton, Kealan McCusker, and Noel E. O’Connor. Security considerations and key negoti-
REFERENCES

bibs/1770/17700626.htm;


DeLooze:2007:PWS


Desai:2000:ESS


Desai:2000:NPC


Desmedt:2002:PKC

REFERENCES


REFERENCES

Durante:2001:CWR


DePalma:2004:CCS


Domingo-Ferrer:2001:CDS


DeSantis:2004:CKA


DKF+03


DFH01

REFERENCES

Domingo-Ferrer:2006:SCR


Domingo-Ferrer:2007:ASC


Damgaard:2004:ZKP


Damgaard:2005:CBQ


Damgaard:2008:CBQ


Dalkilic:2000:ICA

[DG00] Mehmet E. Dalkilic and Cengiz Gunog. An interactive cryptanalysis algorithm for the Vigenère cipher. Lea-
REFERENCES


REFERENCES

Dorrendorf:2007:CRNa

Dorrendorf:2007:CRNb

Dorrendorf:2009:CRN

denHartog:2008:TMC

Dhem:2003:EMR
Deng:2006:OOC


Daza:2007:CTM


DiCrescenzo:2001:SOS


DiCrescenzo:2003:SOS


Dambgard:2005:CRM

Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. In Shoup [Sho05a], pages 378–??.
Dichtl:2003:HPO


Diffie:2001:UC


Dimitriadis:2007:IMC


Dimitrov:2008:DBN


Ding:2001:OTB

Yan Zong Ding. Oblivi-


Datta:2005:RBN


Delaune:2008:FAP


Dittmann:2005:CMS


Dodis:2002:KIP


Diffie:1998:PLP


deleeuw:2000:CSD

[Karl de Leeuw. Cryptology and statecraft in the
REFERENCES

Dutch Republic [Cryptologie en buitenlands beleid in de Republiek der Verenigde Nederlanden]. Ph.D. thesis, Universiteit van Amsterdam, Amsterdam, The Netherlands, 2000. viii + 190 pp. The work in this thesis has been carried out under the auspices of the research school IPA (Institute for Programming research and Algorithmics). In Dutch and English.


REFERENCES


REFERENCES


[DN02a] Ivan Damgård and Jesper Buus Nielsen. Perfect

[DN02b]


Cynthia Dwork, Moni Naor, Omer Reingold, and Larry Stockmeyer. Magic functions: In memoriam: Bernard
REFERENCES


**Dwork:2005:PPW**


**Dodis:2005:PPW**


**Dhamija:2000:DVU**


**DeMatteis:2002:PP**


**Daemen:2001:BCP**


**Crescenzo:2004:CRR**


**Daemen:2000:BCR**


**Daemen:2000:RA**


**DDJ:2000:DDE**

REFERENCES

250

Daemen:2001:AAR

Daemen:2002:AWT

Daemen:2002:DRA

Daemen:2002:FSE

Ding:2002:HEE
REFERENCES

Dray:2000:NPA


Dreyfus:2000:PUC


Driscoll:2002:BER


delRey:2005:SSS


Dobbertin:2005:AES

REFERENCES

252

0302-9743 (print), 1611-3349 (electronic). LCCN ????
URL http://www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=3373.

**Dodis:2002:NUO**

Y. Dodis and J. Spencer.
On the (non)universality of
the one-time pad. In IEEE
[IEE02], pages 376–385. CO-
DEN ASFPDV. ISBN 0-
7695-1822-2. ISSN 0272-
5428. LCCN QA267. URL
org/iel5/8411/26517/01181962.
pdf?isnumber=26517&prod-
CF&arnumber=1181962&arSt-
+376&ared=385&arAuthor=
Dodis,Y.+Spencer,J.;
http://ieeexplore.ieee.org/xpls/abs_all.
.jsp?isnumber=26517&arnumber=
1181962&count=82&index=38.
IEEE Computer Society
Order Number PR01822.

**Dodis:2005:ESE**

Yevgeniy Dodis and Adam
Smith. Entropic security and the encryption of
high entropy messages. In
Kilian [Kil05], pages 556–??
CODEN LNCSD9. ISBN 3-
540-24573-1 (softcover).
ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
T44 2005. URL http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3378; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b106171.

**Dinur:2008:CAT**

Itai Dinur and Adi Shamir.
Cube attacks on tweak-
able black box polyno-
mials. Technical report,
Computer Science Depart-
ment, The Weizmann In-
itute, Rehobot 76100, Is-
rael, September 13, 2008.
URL http://cryptome.
org/cube-attacks.pdf.

**Djurovic:2001:DWF**

Igor Djurovic, Srdjan Stankovic,
and Ioannis Pitas. Digital
watermarking in the fractional Fourier transfor-
mation domain. *Journal of Network and Com-
puter Applications*, 24(2):
Dodzi:2001:PAS


Ding:2003:SIB


Dujella:2008:VWA


Dujella:2009:VWA


Dunkelman:2006:TCB


Duranti:2001:LTP


See [BEZ01].


Benne de Weger. Cryptanalysis of RSA with small...
REFERENCES


Ding:2005:CTC


Ding:2005:CTC

DOD:2009:NME


Dwivedi:2004:ISS


Dwivedi:2004:ISS

Desmedt:2005:CNS


Desmedt:2005:CNS

Dittmann:2001:UCW


REFERENCES


ElAbbadi:2000:VPI


Eghlidos:2001:IRL


Eilam:2005:RSR


English:2007:MAC


ECMA:2000:EPIa

REFERENCES


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Elmallah:2008:LK


Eghlidos:2000:SLB


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB

REFERENCES


Elliott:2004:QC


English:2000:MNDb


England:2002:AOO


Elbirt:2005:ILD

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

Eisenbarth:2007:SLC

Erickson:2001:EDD

Erickson:2002:EDD

Erickson:2003:HAE

Erickson:2008:HAE

Ellison:2000:TRP

Ellison:2000:IRRa


Faliszewski:2007:BRB

Fan:2003:ILC

Faugere:2009:IBC

Ford:2001:SEC

Feghali:2002:SAP
Fischer:2001:TMR


Felke:2006:ATH


Ferguson:2000:SEK


Ferguson:2006:ACE


Fischlin:2000:ENM


Filiol:2001:NUS


Flannery:2001:CYW

REFERENCES


REFERENCES


REFERENCES


**FIPS:2002:SHS**


**Freedman:2005:KSO**


**Fischlin:2001:CLP**


REFERENCES


REFERENCES


REFERENCES


Franklin:2002:PAS


Fournier:2003:SEA


Fouque:2003:AUR


Fluhrer:2001:WKS

REFERENCES


[DFO06] D. Frincke, S. Oudekirk, and B. Popovsky. Editorial: Special issue on resources for the computer security and information assurance curricu-
Fujisaki:2001:ROS


Forbes:2004:BRN


Fox:2000:NTFb


Freking:2000:MMR


Fouque:2001:TCS

Pierre-Alain Fouque and David Pointcheval. Threshold cryptosystems secure against chosen-ciphertext at-

Faugere:2009:EAD


Fouque:2001:SDC


Fournet:2008:CSI


Frankel:2001:FC1

REFERENCES


REFERENCES

Fouque:2001:FDT

Friedlander:2001:DDH

Furukawa:2001:ESP

Fischer:2002:NFC

Ferguson:2003:CEI

Ferguson:2003:PC
REFERENCES


Fundulaki:2004:SYD


Fortnow:2008:IIC


Fuster-Sabater:2001:EAG


Fu:2001:DCA


Ferguson:2001:SAR


Furman:2001:CSM


Furman:2002:DCN

Vladimir Furman. Differential cryptanalysis of Nimbus.
REFERENCES

Furuya:2002:SAK


Fouque:2003:DAW


Fan:2008:RSB


Feng:2005:NMS

Jen-Bang Feng, Hsien-Chau


REFERENCES

Galbreath:2002:CID

Garfinkel:2003:EBI

Ganti:2008:PAL

Garrett:2001:MBC

Gannon:2001:SST

Ganger:2001:AC

Gal02

Gar01

Garfinkel:2003:EBI

Garman:2003:KDG
Jason Garman. Kerberos: the definitive guide. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA,


Gaudry:2002:CCS


Gavinsky:2008:CIC


Guinee:2009:NTR

REFERENCES

Guajardo:2001:EIE

Golic:2002:LCB

Gaj:2001:FIF

Goodman:2001:EER [GD02]

Guerrero:2005:ECB [GD05]

Gennaro:2005:SMS [Geb04]

Gebotys:2004:DSC [GCKL08]
Catherine H. Gebotys. Design of secure cryptography against the threat of power-attacks in DSP-embedded...

**Gennaro:2000:IPR**


**Gentry:2003:CBE**


**Gentry:2004:HCR**


**Gennaro:2006:RC**

REFERENCES


Goldwasser:2008:CAP


Gennaro:2003:LBE


Gennaro:2005:BEG


Gilbert:2005:FSE


Galindo:2008:SPK


Gebhardt:2005:NPV


Ganapathy:2005:APA


Gennaro:2003:SAP


Gallagher:2006:HSB


Gentry:2001:CNS


Gomulkiewicz:2002:HWA

Marcin Gomulkiewicz and Mirosław Kutyłowiski. Hamming weight attacks on cryptographic hardware —
REFERENCES

breaking masking defense. 
CODEN LNCS.D9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://
link.springer.de/link/service/series/0558/bibs/1
2502/25020090.htm; http://
link.springer.de/link/service/series/0558/papers/1
2502/25020090.pdf.

Goldsmith:2004:CAI

[Goldsmith:2004:CAI]
Clair W. Goldsmith and Rob Kolstad. A conversation about identity management. 
;login: the USENIX Association newsletter, 29(5): ??, October 2004. CODEN 
LOGNEM. ISSN 1044-6397. URL http://www.usenix.
org/publications/login/2004-10/pdfs/interview.
pdf.

Goldwasser:2005:PPK

Goldwasser:2005:PPK
Shafi Goldwasser and Dmitriy Kharchenko. Proof of plaintext knowledge for the Ajtai–
Dwork cryptosystem. In Kilian [Kil05], pages 529–??, CODEN LNCS.D9. ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743 (print), 1611-3349 (elec-
issn=0302-9743&volume=3378; http://www.springerlink.
com/openurl.asp?genre=


Gavinsky:2007:ESO

Dmitry Gavinsky, Julia Kempe, Iordanis Keren-
dis, Ran Raz, and Ronald de Wolf. Exponential separa-
tions for one-way quantum communication complexity, 
with applications to cryptography. In ACM [ACM07], 

Gavinsky:2009:ESO

Dmitry Gavinsky, Julia Kempe, Iordanis Keren-
dis, Ran Raz, and Ronald de Wolf. Exponential sep-
taration for one-way quantum communication complex-
ity, with applications to cryptography. SIAM 
CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 
(electronic).

Garay:2007:RCA

Garay:2007:RCA
J. A. Garay, J. Katz, Chi-Yuen Koo, and R. Os
trovsky. Round complexity of authenticated broad-
cast with a dishonest majority. In IEEE [IEE07], 
ieee.org/servlet/opac?punumber=4389466. IEEE
Computer Society order number P3010.

**Gertner:2000:RBP**


**Guneysu:2008:CC**


**Goubault-Larrecq:2000:MAC**


**Goldreich:2001:SKG**

REFERENCES


REFERENCES


REFERENCES

Gopalakrishnan:2001:PWV


Grosek:2001:SPK


Ge:2005:CCO


Gore:2001:CMT


Gratzer:2006:CLE


Gutmann:2005:WHC

REFERENCES

Gaj:2003:FME


Goldreich:2001:FCHB


Goldreich:1999:MCP


Golic:2001:CAS


Golic:2001:MOS


**Garcia-Pasquel:2006:GCT**


**Guneysu:2008:SPH**


**Gutierrez:2006:ALR**


**Granger:2005:HSN**


**Granger:2006:SCA**


**Gentry:2008:THL**


**Geng:2008:DSA**

Xiutang Geng, Linqiang Pan, and Jin Xu. A DNA sticker algorithm for bit-substitution in a block cipher. *Journal of Parallel...*

**Galbraith:2004:EDD**


**Grasser:1998:FC**


**Graff:2001:CCW**


**Granboulan:2002:SSR**


**Granboulan:2002:FDC**


**Grossschäd:2001:HSR**

Johann Großschäd. High-speed RSA hardware based
REFERENCES


Grossschadl:2003:ASL


Groth:2005:CS


Gisin:2002:QC


Gentry:2006:EES


GonzalezVasco:2001:CPK

REFERENCES

(Garfinkel:2002:WSP)


(Gentry:2002:HIB)


(Gentry:2002:CRN)


(Geiselmann:2003:HSS)


(Geiselmann:2007:SPH)

REFERENCES


REFERENCES


Giles:2002:ADW


Garay:2000:LLB


Goodrich:2002:EDD

Goodrich:2003:ADS


Guar:2005:PPL


Gumz:2004:BRH


Gutmann:2000:OSC


Gutmann:2002:CFP

REFERENCES


Gutmann:2002:DVC


Gutmann:2004:CSA


Gutmann:2004:SPK


Gutmann:20xx:ESR


Granger:2005:DLP


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 SIGS3D. ISSN 0097-8418.


[HA00] Howard Heys and Carlisle Adams, editors. Selected ar-
references


Ian Harvey. The ef-
ffects of multiple algorithms in the Advanced Encryption Standard. In NIST [NIS00], pages 269–278.
ISBN ???. LCCN ???.


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 contents from a previously published paper. Therefore ACM has shut off access to this paper.

**Hayashi:2006:QIT**


**Hoglund:2006:RSW**


**Huffmire:2008:DSS**


**Hartel:2001:TMS**


**Holcomb:2009:PSS**

REFERENCES


Humphries:2002:IC


Huang:2004:NDE


Hwang:2004:NMP


Han:2008:PBPa


Han:2008:PBPb


Henderson:2002:MTS


Halevi:2002:SSE

Han:2009:ICS


He:2002:WSM


Heikkila:2007:ESC


Hendry:2001:SCS


Henderson:2006:CBG


Herzberg:2002:SX

Herranz:2006:DIB


Herranz:2007:IBR


Hess:2004:SVE


Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA


Horvitz:2003:WKA


<table>
<thead>
<tr>
<th>REFERENCES</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Howgrave-Graham:2003:HNP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Handschuh:2004:SAC</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Handschnuh:2005:SAC</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Hendricks:2007:LOB</strong></td>
<td></td>
</tr>
</tbody>
</table>


Hankerson:2000:CTC


Hankerson:2001:SIE


Han:2007:FIE


Higgins:2008:NSC


Hill:2000:KII

Hacigumus:2002:ESE


Hirose:2009:SAD


Hinkelmann:2007:CUN


Huhnlein:2001:TPN


Huang:2005:ASE


Harris:2005:IUS

[HKA+05] David Harris, Ram Krishnamurthy, Mark Anders, Sanu Mathew, and Steven Hsu. An improved unified scalable radix-2 Montgomery multiplier. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL

Kim:2000:RMW


Heuberger:2005:AGE


Handschuh:2001:ASE


Hiltgen:2006:SIB


Horwitz:2002:THI

Jeremy Horwitz and Ben

Howard:2003:WSC

Hwang:2004:REL

Hohenberger:2005:HSO
Susan Hohenberger and Anna Lysyanskaya. How to securely outsource cryptographic computations. In Kilian [Kil05], pages 264–?? CODEN LNCSD9.

Hwang:2005:TAU

Hwang:2005:SHW

Hwang:2005:STH
Shin-Jia Hwang and Hao-Chih Liao. Security of Tzeng–Hwang’s authenticated encryption scheme...

[Howard:2006:SDL]


[Huang:2007:EPS]


[Hwang:2000:CBV]


REFERENCES


REFERENCES

no.2139. UK£47.00. URL
http://link.springer-ny.com/link/service/series/0558/bibs/21390101.htm;


[HMS04] Thomas Holenstein, Ueli

Hankerson:2004:GEC


Huang:2007:MPK


Haitner:2009:SHC


Hanaoka:2002:HNI

Goichiro Hanaoka, Tsuyoshi

Haastad:2004:SAR


Harnik:2006:CNI


Hoepman:2001:SKA


Hofinger:2001:LBE


Honary:2001:CCI


Hook:2005:BCP

REFERENCES


Hu:2005:USA


Hawkes:2001:PCS


Hand:2002:MPP


Halevi:2003:TEM

REFERENCES

[Hawkes:2004:RVC]

[Hsiao:2004:FCP]

[Holenstein:2005:OWS]

[Halevi:2006:TCT]
Haitner:2007:SHC


Haneberg:2002:MSS


Hemaspaandra:2008:EDA

REFERENCES


[He:2005:MCP] Changhua He, Mukund Sun-

Hong:2001:KIA

Halderman:2008:LWRb

Halderman:2009:LWR

Hanaoka:2002:USA
Goichiro Hanaoka, Junji Shikata, Yumiko Hanaoka, and Hideki Imai. Unconditionally secure anonymous encryption and group authentication. Lecture Notes in Computer Science,
REFERENCES

Hanaoka:2006:USA


Hernandez:2002:GCT


Hwang:2001:LCT


Hong:2002:PSR


Hong:2002:IDC

REFERENCES


[Hsu:2005:UFR] Chien-Lung Hsu. A user friendly remote authentication scheme with smart cards...


[Hasan:2009:PHF](#)

[Hanaoka:2000:USD](#)


[Halpern:2004:RSS](#)


[Huang:2006:CSV](#)


[Hongfeng:2008:ECP](#)

REFERENCES

**Hamalainen:2002:GPS**

**Hines:2007:AIF**

**Hofheinz:2005:CTN**
Dennis Hofheinz and Dominique Unruh. Comparing two notions of simulatability. In Kilian [Kil05], pages 86–??, CODEN LNCSDD.

**Hughes:2002:LAA**

**Hughes:2004:ISE**
Huhnlein:2000:EIC


Hunt:2005:JFE


Husemann:2001:SSC


Husemoller:2004:EC


Huth:2001:SCS


Hodjat:2004:HTP

REFERENCES


REFERENCES


REFERENCES


**Hsu:2002:IGT**


**Hsu:2003:ITP**


**Hsu:2004:GOS**


**Harkins:2005:ESU**


**Hsu:2003:IMA**


**Hirose:2001:UAS**

REFERENCES


Hwang:2003:CAL


Yeh:2008:STB


Hwang:2003:ASM


Han:2005:PJI


Han:2005:PJIb


IBM-MARS-Team:2000:MAS

IEEE:2000:ASF


IEEE:2000:IPH


IEEE:2001:ISF


IEEE:2001:EIW


IEEE:2002:PAI


IEEE:2003:PAI

IEEE:2004:PAI


IEEE:2005:AIS


IEEE:2005:PIS


IEEE:2006:AIS


REFERENCES

Ifrah:2000:UHN


Iglesias:2002:NSB


Bassham:2000:ETA


Itoh:2003:PCA

REFERENCES

Iwata:2000:PAF


Iwata:2001:PAF


Ichikawa:2000:HEA

REFERENCES

Ishai:2003:EOT

Ishai:2005:SCC

Ishai:2007:ZKS

Ishai:2008:CCC

Iyer:2007:TAA
Ravishankar K. Iyer, Zbigniew Kalbarczyk, Karthik

Ioannidis:2005:ACN


Imrey:2003:BRC


[IR02] Gene Itkis and Leonid Reyzin. SiBIR: Signer-
REFERENCES


Ishai:2003:PCS


Itoi:2000:SCI


Itoi:2001:SCS


Iwami:2008:AIA


Imai:2000:CPC


Irwin:2005:PAI


REFERENCES

link/service/series/0558/bibs/2020/20200344.htm;

[Jac00] Chris Jackson. Smart card questions move from technology to applications. Railway

[Jam00] K. Jambunathan. On choice of connection-polynomials for LFSR-based stream ciphers. Lecture Notes in
link/service/series/0558/bibs/1977/19770009.htm;

[Jan00] Lech Janczewski. Internet and intranet security management: risks and solutions. Idea Group Pub.,

1993 / Gehan Gunasekara.

Janeczko:2006:TSH


Jankowski:2008:BRBb


Jennewein:2000:FCQ


Jones:2005:RDF


Johnston:2001:IHS


Jeffrey:2008:PAM


Jennings:2009:SLL

REFERENCES

Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC


[JJ00d] Johansson:2000:FCA


Jakimoski:2001:ASR


Jakimoski:2001:CCB

Goce Jakimoski and Ljupco Kocarev. Chaos and cryptography: block encryption


[Jakimovski:2002:CS]

[Jonsson:2002:SRE]

[Jang:2001:BWA]

[Jung:2001:EMO]

[Jallad:2002:ICC]
Kahil Jallad, Jonathan Katz, and Bruce Schneier. Implementation of chosen-

**Jarecki:2000:AST**


**Joux:2003:IGN**


**Juang:2004:FBT**

REFERENCES

Jeong:2008:PKE


Juang:2001:FBT


Juang:2002:VMA


Jakobsson:2003:FMT


Johansson:2003:PCI

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-
REFERENCES

Joye:2001:OAD

Matyas:2003:TRU

Juric:2006:CPW

Jin:2001:WCS

Jaworski:2009:RKP


REFERENCES

[102x681]copyright 
[102x681]link/service/series/0558/
bibs/2045/20450529.htm; 
http://link.springer- 
ny.com/link/service/series/
0558/papers/2045/20450529. pdf.

**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. Operating 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 pervasive devices with human pro-
tocols. In Shoup [Sho05a], pages 293–?? ISBN 3-540- 
28114-2. ISSN 0302-9743 (print), 1611-3349 (elec-
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 crypt-
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-
ing strength. In Han et al. [HYZ05b], pages 147–?? ISBN 981-270-153-2. 

**Jiang:2005:RNP**

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

**Joye:2001:NMM**

Marc Joye and Sung-Ming 
CODEN LNCSD9. ISSN 
0302-9743 (print), 1611-3349 
REFERENCES

link/service/series/0558/bibs/2274/22740375.htm;

Jakobsson:2004:ACN [JZCW05]

Jain:2009:NBC [Kah67a]

Jiang:2005:TMD [Kah67b]

Kadrich:2007:ES [Kad07]

Kahn:1967:CSSa [Kah67a]

Kahn:1967:CSSb [Kah67b]
David Kahn. The Codebreakers: the Story of Secret Writ-
REFERENCES


[Kah74] David Kahn. The Codebreak-


[Kat01] Stefan Katzenbeisser. Recent advances in RSA cryptography, volume 3 of Advances in in-


[Kat05b] Jonathan Katz. Comparative book review: Cryptography: An Introduction, by V. V. Yaschenko (American Mathematical Society, 2002); Cryptanalysis of Number Theoretic Ci-
REFERENCES

CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL http://doi.acm.org/10.1145/1067309.1067316. See [Gol01b, Wag03, Mol03b].

Kendall:1939:TRS


Kovacich:2000:HTC


Kiely:2006:SSM


Kamvar:2007:DTM


Keller:2009:ECC


Kachris:2003:RLB


Kim:2009:DCA


claffy:2001:IMM


[KC05]


[KC09]


[KCC05]


[Kang:2001:NHO]


[KCD07]

REFERENCES

Kurosawa:2004:NPH


King:2001:SAD


Keefe:2005:CDS

Kelsey:2000:KST

Kettani:2006:CBN
Houssain Kettani. On the conversion between number systems. IEEE transactions on circuits and systems. 2, Analog and digital signal
REFERENCES


REFERENCES

[KHD01]

[KHKL05]

[KHL09]

[KHY04]

[KHYM08]

[Kobara:2001:NCP]

[Kobara:2001:SSM]

[Kurosawa:2003:TTK]
REFERENCES


Kidwell:2000:SNC


Kidwell:2000:SNC

Kida:2002:PGR


Kida:2002:PGR

Kilian:2001:ACC


Kilian:2001:ACC

Kiltz:2001:TBC


Kiltz:2001:TBC

Kim:2001:PKC


Kim:2001:PKC

Kilian:2005:TCS


Kilian:2005:TCS

Kim:2002:ISC

REFERENCES


King:2000:IMP

King:2001:CMF

King:2002:RG1

Kirtland:2001:INC
Joseph Kirtland. Identification numbers and check digit schemes. Classroom re-


Montgomery:2003:FEC

Kocarev:2001:LMB

Kanade:2005:AVB
Takeo Kanade, Anil Jain, and Nalini K. Ratha, editors. Audio- and Video-Based Biom

Kim:2005:IYA
Kee-Won Kim, Jun-Cheol Jeon, and Kee-Youn Yoo. An improvement on Yang et


REFERENCES


reduced-round Serpent. In NIST [NIS00], pages 195–214. ISBN ????, LCCN ???.

Kelsey:2001:ABA
J. Kelsey, T. Kohno, and B. Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Schneier [Sch01], page ??, CODEN LNCSD9. ISBN 3-540-41728-1. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kim:2002:IDS

Katz:2008:IMC

Knill:2002:FPE

Knill:2002:QIP
REFERENCES

383


Kim:2001:NPK

Knudsen:2001:CPL

Knudsen:2001:CRL
[KM04]

Koblitz:2004:SPK

Kornerup:2007:PIS
Peter Kornerup and Jean-Michel Muller, editors. *Proceedings of the 18th IEEE Symposium*
REFERENCES


Kim:2002:ABA


KMM06


Keliher:2001:IUB


KMO01


Klarlund:2001:MIS


Klimov:2002:ANC


Katz:2003:CAC

Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng. Rethinking chosen-ciphertext security under Kerckhoffs’ assumption. In Joyce
REFERENCES


Kittler:2003:AVB


Kol:2008:GEI


Koc:2002:CHEb


Krukow:2005:FCR


Knudsen:2000:TTR


Knudsen:2002:ACE

Knutson:2007:BPS


Kushilevitz:2000:OWT


Komano:2003:EUP


Kurosawa:2001:ICP

Kornblum:2009:IBD


Koshiba:2001:NAS


Koshiba:2001:SRS


Katzenbeisser:2000:IHT


Koc:2001:CHEa

Çetin K. Koç and Christof Paar, editors. Cryptographic hardware and embed-
REFERENCES


Krause:2002:BBC

Krause:2002:USP

Krawczyk:2003:SSM

Krawczyk:2005:HHP

Kramer:2007:LCC

Kreitz:2005:OBE

Koeune:2002:FIL

Kehr:2001:ISM
REFERENCES


Kim:2005:CLL

Katz:2000:CCA

Kelsey:2000:MAP

Kuramitsu:2002:ETC

Krause:2003:DOC

Kozaczuk:2004:EHP

Kissner:2005:PPS

Kissner:2005:PPS
REFERENCES

Klivans:2006:CHL


Kasper:2009:FTA


Kelsey:2000:YND


Kang:2001:PSK


Ku:2002:IIB


Ku:2004:HBS


Kuhn:2000:PCL


Kuhn:2001:CRR


Kuhn:2002:OTD


Kuhn:2008:BSS


Kukorelly:2001:PAL


Kundur:2001:WDI


Kurosawa:2001:MRP

REFERENCES


Kusters:2002:DCP

Kuo:2001:AOS

Kejariwal:2009:ELL

Koshiba:2000:SEP

Knudsen:2002:IC

Karlof:2003:HMM

Keromytis:2006:COS
Kwon:2002:DSA

Kwok:2003:WBC

Kwon:2003:EDS

Kwon:2003:EDS

Kumar:2006:ODS

Kamat:2009:TPW

Katz:2000:CCS
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Landau:2004:SLE]


[La00d]


[Landau:2004:PNS]


[Laughlin:2008:CRC]


[Lavoue:2009:LRM]


[Laughlin:2008:CRC]


[Laughlin:2008:CRC]


[Laughlin:2008:CRC]


[Laughlin:2008:CRC]

Lawton:2005:MAH


Lawson:2009:SCA


Lawson:2009:TAG


Li:2004:QAU


Lindskog:2005:DIT


Leveiller:2001:CNF


Laufer:2000:SSC


Laih:2003:COP

Lin:2004:SOT

Lu:2004:XMS

Lu:2005:ERU

Long:2005:DTC

Lee:2001:SEK

Li:2008:CAM


Lu:2005:TUS


Lu:2005:PBM


Lu:2005:RTP


Li:2001:CCB


Lai:2004:SGS


Law:2006:SBB


Lindquist:2004:JCS


Lee:2001:AES


Lee:2003:BRBa

REFERENCES


REFERENCES


Lee:2003:NKA


Lin:2003:NRU


Lee:2004:SAA


Lu:2008:PTZ


Liu:2005:DBV


Lee:2005:NBS


Li:2001:NSA


Li:2005:ABPa

S. Z. Li, editor. *Advances in biometric person authentication: 5th Chinese conference on biometric recognition*, SINOBIO-
REFERENCES

Lieman:2005:CRW

Lin:2000:RTI

Lindell:2001:PCT

Lindell:2003:SCC

Lin:2007:PFT


REFERENCES


[LL05c] Ying Li and Jintao Li. Further cryptanalysis of a remote login authentication scheme based on geometric approach. In Han et al. [HYZ05b], pages 143-?? ISBN 981-270-153-2.
REFERENCES

Lee:2006:ISC

Lu:2006:FBW

Li:2004:CES

Li:2001:SPD

Lee:2002:RUA

Lee:2006:ISC

Lu:2006:RDI

Lesniewski-Laas:2005:SSS


Lamenca-Martinez:2006:LNP

Leitold:2001:MTN

Lepinski:2005:FZK

Laskari:2007:AEC

Laskari:2005:TTC

Lu:2005:CCA

Li:2005:BPC

Liu:2004:MBA
Ponggang Liu and Peng Ning. Multilevel $\mu$TESLA: Broadcast authentication for dis-


Lemke-Rust:2007:MAP


Liskov:2002:TBC


Lenstra:2001:SFR


Lindemann:2001:ICT


Loidreau:2001:WKM


Li:2005:ULC


Liang:2005:FAG


Lopez:2007:SCB


Lin:2000:TPE

REFERENCES

Lin:2003:SEOa

Lin:2003:SEOb

Lu:2005:BIW

Li:2005:ABPb

Liang:2009:AIE

Lee:2001:EPI

Liu:2005:RBU

Lin:2004:SIS

Li:2005:ISS
REFERENCES

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

[LT00]

[LTW05]

[Lu02]

[Lu07]

[Lucks:2000:ASR]

[Lucks:2002:SAB]

[Lucks:2002:VCS]
Lucas:2006:PGE


Ludvig:2005:PWF


Lukyanov:2001:PFA


Lunde:2009:BCU


Lutz:2002:BBS


Lutz:2003:BLF


Lenstra:2000:XPK


Lu:2004:FCA

REFERENCES


[Loepp:2005:PIC]


[Haifeng Li, Shuxun Wang, and Weiwei Song. Image watermarking resistant to global geometrical attacks. In Han et al.
REFERENCES


Lin:2005:NIB


[LWZH05]

[LXM+05]


Li:2005:AAU


Li:2007:NBA


LYC02


Lysyanskaya:2007:AI


Lysyanskaya:2008:CHK


Lysyanskaya:2002:USV


Lysyanskaya:2007:AI


Lysyanskaya:2008:CHK

REFERENCES

[LZ01]

[Li:2004:CAB]

[Lao:2009:ORA]

[Li:2001:GOT]

[Mrayati:2003:AKT]

[Mrayati:2004:IAD]
M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Ibn ’ad-Durayhim’s treatise on cryptanalysis*, volume 3 of *Arabic origins of cryptology*. KFCRIS & KACST,


Maloof:2006:MLD


Mao:2004:MCT


Manger:2001:CCA


Marques:2002:BSJ


Martinelli:2002:SSA


Mares:2005:BRA

Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI


Martin:2008:IBE


Mastroeni:2004:APA


Matsui:2002:FSE


Mayers:2001:USQ

Mohanty:2008:IWB

McKinnon:2004:CCS

Montenegro:2004:CBI

McAndrew:2008:TCO

McGraw:2006:SSB


Mel:2001:CD
Myles:2005:ETS


McLaughlin:2006:PZW


McNichol:2003:HTM


Martin:2004:AMC


Macchetti:2005:QPH


McCamant:2008:QIF


Monteiro:2008:AVM


Meadows:2001:OIF


Meadows:2004:OSM


Mehrabi:2001:DW


References


REFERENCES

Ma:2005:NCD


Ma:2009:SRW

Maas:2009:SRW


Moon:2002:IDC


Micciancio:2001:ILB

Micciancio:2002:GCK


Micciancio:2002:ICH

REFERENCES


Moore:2001:AGK


Moore:2005:CLD


Mabry:2007:USE


Mabry:2009:TDI


McDonald:2008:SID


McGregor:2005:PCK

REFERENCES


REFERENCES


Moreira:2002:RCE

Milenkovic:2005:UIB

Maltoni:2003:HFR

McEvoy:2009:IWH

Maitra:2006:PCI

Matsumoto:2002:IAG

Mizuki:2001:NSN
REFERENCES


REFERENCES


[Moritz:2005:KAE] Hannes Moritz. Kryptoanalyse des Advanced Encryption Standard. (German) cryptanal-

**Moses:2006:DSD**


**Morton:2000:NBG**


**McMillan:2001:JIA**


**Mihăilescu:2001:BRF**


**Moshopoulos:2001:ASA**


**Malkhi:2002:CAC**


**Maurer:2003:SMR**

REFERENCES

Micciancio:2005:ASS


Matusiewicz:2006:FGD


Munilla:2007:HMF


Micciancio:2008:OCC


Mislove:2006:EOB


Moralis:2009:KSA


Micali:2005:OEC


Monrose:2000:KDB

REFERENCES

FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.elsevier.com/gej-ng/10/19/19/41/27/30/abstract.html.

MacKenzie:2001:TPG


Micali:2001:MRR


Micali:2001:SPK


Murphy:2002:EASa


Murphy:2002:EASb


Micciancio:2009:LBC


Monrose:2002:TSG


Mitchell:2006:PPT

REFERENCES

14, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Mayer-Sommer:2001:SAS


Maggi:2002:USV


Maitra:2002:CSB


Menezes:2002:PCI


Mitnick:2002:ADC


Muthukrishnan:2002:IAS


Markowitch:2003:CWV

REFERENCES

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

Miklau:2003:CAP

Martin:2005:PET

Meadows:2005:CPA

Mahdian:2009:UNI

Manulis:2009:SMF

Myers:2009:BEC

Shen:2005:NIW

MacKenzie:2002:TPA

 McClure:2003:HEN
Stuart McClure, Joel Scambray, and George Kurtz. Hacking exposed: net-


[Meseguer07] José Meseguer and Prasanna Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. Higher-Order and Sym-
REFERENCES

Ma:2009:NAS


Muller:2001:SWB


Muller:2001:SIC


Moricai:2000:PTL


Meister:2001:PPG


Micciancio:2003:SZK

[MV03a] Daniele Micciancio and Salil P. Vadhan. Statistical zero-knowledge proofs with effi-
cient provers: Lattice problems and more. In Boneh [Bon03], pages 282–298. CO-
asp?genre=issue&issn=0302-9743&volume=2729; http://www.springerlink.com/

Morrow:2003:DIB
Monique Morrow and Kateel Vijayananda. Developing IP-based services: solutions for
service providers and vendors. Morgan Kauf-
mann Publishers, Los Altos, CA 94022, USA,

MWM01
Ralph Morelli, Ralph Walde, and Gregg Mar-
cuccio. A Java API for historical ciphers:
an object-oriented design project. SIGCSE
Bulletin (ACM Special Interest Group on
Computer Science Education), 33(1):307–311,
March 2001. CODEN SIGSD3. ISSN 0097-
8418.

Malan:2008:IPK
David J. Malan, Matt Walsh, and Michael D.
Smith. Implementing public-key infrastructure
for sensor networks. ACM Transactions
2008. CODEN ????. ISSN 1550-4859 (print),
1550-4867 (electronic).

MRaihi:2001:CAS
David M’Raïhi and Moti Yung. E-commerce
applications of smart cards. Computer
Networks (Amsterdam, Netherlands: 1999),
nl/gej-ng/10/15/22/61/28/31/abstract.
html; http://www.elsevier.nl/gej-ng/
10/15/22/61/28/31/article.pdf.

McCook:2001:NSS
Alison McCook, Philip Yam, and Graham P.
Collins. News scan: The not so sheltering
sky: computer; Hack job; tissue engineer-
ing: Fat into cartilage; psychology: Holier
than thou; astronomy: Otherworldly ocean;
physics: Microscopic maelstrom; medicine:
Fetal cell setback. Scientific American,
MAC. ISSN 0036-8733 (print). 1946-7087
2001/0501issue/0501inbrief.html.

Morelos-Zaragoza:2002:AEC
Robert Morelos-Zaragoza. The Art of Error
Correcting Coding. John Wiley and Sons,
471-49581-6. xvi + 221 pp. LCCN ????
UK£45.00, US$95.00. URL http://www.
loc.gov/catdir/description/wiley035/
2002280749.html; http://www.loc.gov/
catdir/toc/wiley023/2002280749.html.

Matsui:2004:SAC
Mitsuru Matsui and Robert Zuccherato, ed-
itors. Selected Areas in Cryptography: 10th
Annual International Workshop, SAC 2003,
Ottawa, Canada, August 14–15, 2003, Re-
vised Papers, volume 3006 of Lecture Notes
in Computer Science. Springer-Verlag, Berlin,
Germany / Heidelberg, Germany / Lon-
ISBN 3-540-21370-8. ISSN 0302-9743
(print). 1611-3349 (electronic). LCCN ????
URL http://link.springer-ny.com/link/
service/series/0558/tocs/t3006.htm;
asp?genre=issue&issn=0302-9743&volume=


REFERENCES


REFERENCES


REFERENCES


Nakahara:2001:LCR


Naor:2004:NTC


Nichols:2000:DYD


Néraud:2001:CFD


Nguyen:2001:ISA


Nguyen:2001:TFLa


Narayanan:2005:FDA


Narayanan:2005:ODG


Nguyen:2005:FPL

Nenadic:2005:RBC


Olson:2003:QHK


Oechslin:2003:MFC


Oppliger:2008:STS


REFERENCES
REFERENCES

Oiwa:2009:IMS


Okamoto:2000:ACA


Okamoto:2004:TCC


Ogata:2006:OSS


Olson:2000:SCT


Ohigashi:2009:PMF


Ohkuma:2001:BCH


Dag Arne Osvik, Adi Shamir, and Eran Tromer. Cache attacks and countermeasures:


Linda Dailey Paulson. News briefs: Project promises accessible technology for the disabled; two efforts aim to upgrade mobile mem-
ory; new haptics approach lets parents-to-be “touch” their unborn children; prime breakthrough may improve encryption.


Paulson:2002:NBR


Paulson:2003:NBV


Paulson:2009:NBT


Piva:2002:MCW


Piva:2005:SRA


Park:2000:CAP

REFERENCES


[PC04] Cyrus Peikari and Anton Chuvakin. Security warrior. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street,


Pan:2007:IBS

REFERENCES


REFERENCES


Pathak:2006:BFT

Pietrzak:2005:CDI

Pinkas:2002:CTP

Pinkas:2003:CTP

Pincock:2006:CHC

Pecho:2009:APW

Park:2001:NDW

Park:2001:RFW


[PLJ05b] Shun-Fu Pon, Erl-Huei Lu, and Albert B. Jeng. One private-key for all DL-based cryp-

Pfleeger:2007:IBC


Paulson:2000:NBU


Piper:2002:CVS


Pang:2008:AQR


Pornin:2001:THE


Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP


Poi00

REFERENCES


Porras:2006:PEG


Pfleeger:2003:SC


Paul:2006:SSC


Popp:2006:CTT


Pfleeger:2007:SC


Paar:2009:UCT


Pellikaan:1996:AGC


Piret:2003:DFA


Pareschi:2009:PAC

Pang:2008:VCR

Pfleeger:2007:GEI

Pucella:2003:JRB

Pucella:2006:SCC

Pucella:2007:Ib
Puzmanova:2004:RWF


Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI


Pang:2005:NMS


Peikert:2008:ITF


Pelzl:2003:HCC


Patrick:2005:FCD

REFERENCES

475


Paterson:2006:LTT


Paterson:2006:LTT

Palanivel:2008:MPA


Palanivel:2008:MPA

Pieprzyk:2001:CPS


Pieprzyk:2001:CPS

Pieprzyk:2002:CPL


Pieprzyk:2002:CPL

Pieprzyk:2002:CCI


Pieprzyk:2002:CCI

Qian:2005:CLT


Qian:2005:CLT

Qian:2005:SPL


Qian:2005:SPL

Quisquater:2000:SCR


Quisquater:2000:SCR

Quisquater:2005:SCC


Quisquater:2005:SCC

Quisquater:2001:EAE


[Rai00]

Quisquater:2002:CTM


Qu:2001:KPW


[RAL07]

Raikhel:2000:DF


Rand:1955:MRD


Rand:2001:MRD

REFERENCES

0-8330-3047-7. xxv + 400 + 200 pp. LCCN QA276.25 .M55 2001. See also [Ran55].

**Rijmen:2001:WHF**


**Rogaway:2003:OBC**


**Rijmen:2008:RSA**


**Roth:2001:EJA**


**Rogers:2005:NSE**


**Rubin:2006:CSE**


**Reed:2000:ANA**


**Rubin:2005:ARS**


**Rangan:2001:PCI**


References


REFERENCES


Ryutov:2000:RESb

Robinson:2002:LLE

Robinson:2009:LLE

Rosen:2006:CZK

Rosenberg:2006:RAS

Rosenblum:2007:WAC

Roth:2001:RSC

Roth:2002:JSA
REFERENCES

Rothe:2002:SFC


Rothe:2003:SFC


Rothe:2005:CTC


Rothe:2007:BRB


Roy:2000:PCI


Roy:2005:ACA


Rieffel:2000:IQC

REFERENCES


REFERENCES


[R00]

[R01]

[R02]

[R03]

[R04]

[R05]


REFERENCES


REFERENCES


Saini:2002:JMD


Saeednia:2002:IBS


Sakamura:2001:GEI


Sale:2000:CBP


Sale:2001:GRT


Salus:2001:CA


Salomon:2003:DPS


Salus:2003:BRBb

REFERENCES

Sale:2005:RCB


Salomon:2007:DCC


Sallee:2005:MBM


Sale:20xx:CRP


Salomon:2005:CDC


Samid:2001:ESR


Salomon:2005:FCS


Samtani:2009:WTO


Salomon:2005:ESR


Santini:2009:WTO


Santini:2005:WSI

Simone Santini. We are sorry to inform you...

Sarkar:2002:FCM

Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung [Yun02a], pages 533–548. CODEN

Samtani:2009:WTO


Santini:2005:WSI

Simone Santini. We are sorry to inform you...

Sarkar:2002:FCM

Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung [Yun02a], pages 533–548. CODEN


[SSB05] Rob Sherwood, Bobby Bhattacharjee, and Ryan Braud. Misbehaving TCP receivers can cause Internet-wide congestion collapse. In


**Steiner:2001:SPB**


**Smeraldi:2002:SVF**


**Shehab:2005:SCM**


**Shehab:2007:WSD**


**Steinfeld:2002:NSA**


**Seredynski:2004:CAC**


**Syverson:2001:LAP**


**Shen:2002:NDW**


REFERENCES

495


Schmalz:2004:MDIa

Schmalz:2004:MDIb

Schneier:2004:SA

Schweiger:2006:AMS

Schroeder:2006:NTS
REFERENCES


REFERENCES


REFERENCES


[Sak07] Ziad Sakr and Nicolas D. Georganas. Robust content-based MPEG-4 XMT scene structure authentication and multimedia content location. ACM Transactions on Multimedia
REFERENCES


Shirase:2005:AEC

Shailer:2001:PMT

Shao:2001:BVM

Sharp:2001:IKB

Shapiro:2002:CCM

Shamir:2003:RS

Shamir:2003:TLC
Adi Shamir. Turing Lecture on cryptology: a status report. World-Wide Web slide presen-
REFERENCES


Shao:2003:CIB


Shao:2005:IEP


Shao:2005:NKA


Shao:2005:SMD


Shepherd:2001:CDC


Sung:2007:CIB

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

Shih:2008:DWS

Sierra:2004:LCC

Shimizu:2007:CBE

Shoup:2000:ACC

Shoup:2000:UHF

Shoup:2005:ACC
REFERENCES

Shoup:2005:CIN

Shparlinski:2003:CAA

Shparlinski:2002:SMS

Shparlinski:2004:BRR

Shparlinski:2004:UDD

Shparlinski:2002:SMS
REFERENCES


Sun:2005:SSP

Shumba:2006:THL

Shyamasundar:2002:ACP

Silverman:2001:CLI

Silverman:2005:ECC

Simon:2002:CRE

Singh:1999:CBE

Singh:2000:CBE

Singh:2001:DPK
REFERENCES


REFERENCES


Schindler:2001:IDC


Srinathan:2002:ASC


Sugita:2000:RAD


Schneier:2000:CTA


Scharwaechter:2007:AAE


Sterbenz:2000:PAC

Andreas Sterbenz and Peter Lipp. Performance of the AES candidate algo-


Javier Salido, Loukas Lazos, and Radha Poovendran. Energy and bandwidth-efficient key distribution in wireless ad hoc networks:

**REFERENCES**

**Song:2001:DWF**


**Sarkar:2000:CNB**


**Sarkar:2000:NBC**


**Sarkar:2000:EIL**


**Satoh:2002:SHS**

REFERENCES


REFERENCES

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


**Song:2000:ISC**


**Shigetomi:2002:ALS**


**Satoh:2000:HSM**


**Shelfer:2002:SCE**


**Solachidis:2004:WPL**


**Schielzeth:2005:RQN**


**Shahruz:2002:DNC**


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


Shim:2000:NEF


Scambray:2006:HEW


Stinson:2001:SAC

of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Hei-

Kouichi Sakurai and Tsuyoshi Takagi. On the security of a modified public-
key primitive. Lecture Notes in Computer Science, 2384:436–??, 2002. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-

A. Satoh and K. Takano. A scalable dual-field elliptic curve cryptograph-
stamp/stamp.jsp?tp=&arnumber=1190586.

Adi Shamir and Eran Tromer. Factorizing large numbers with the TWIRL de-


William Stallings. Cryptography and network security: principles and practice. Prentice-

James Standboge. Encrypted NFS with OpenSSH and Linux. Sys Admin: The Jour-
ISSN 1061-2688.

REFERENCES


REFERENCES

Stinson:2002:CTP


Stieber:2006:OH


Stieber:2006:GH


Shimoyama:2002:MLC


Stone:2001:CI


Struif:2001:UBU


Strunk:2001:JQJ


Strubinger:2002:HBS


Stytz:2004:BRW


Ronen Shaltiel and Emanuele Viola. Hardness amplification proofs require majority. In ACM
REFERENCES


Hsing-Min Sun, Mu-En Wu, M. Jason Hinek, Cheng-Ta Yang, and Vincent S. Tseng. Trad-

[Swi05]

[Swi05a]

Stevenson:2005:SCI


[SXY01]

Shujun:2001:PRB


Shi:2001:NSF


Sun:2005:CSS

REFERENCES


Shimoyama:2002:BCS

Steinfeld:2001:ALE

Skoudis:2003:MFM

Sarikaya:2008:SPT

Sun:2002:NAD

Tada:2002:OSM

Tang:2001:AES

Tang:2007:MMU
Ping Tak Peter Tang. Modular multiplication using redundant digit division. In Kornerup

[Tan07b]

[Tat05]

[TC01]

[TCC02]
REFERENCES

Trudel:2003:DSE

Todd:2001:LSS

Terai:2008:BRB

Thorsteinsson:2004:NSC

Theoharidou:2007:CBK

Tirkel:2001:UWE

Tabatabaian:2001:NSP

Tippett:1927:RSN

Torres:2007:ANS
Tseng:2001:GGO


Tseng:2001:CLB


Tseng:2003:DSM


Tico:2003:RAS


Toll:2008:CSE


Thien:2002:TSS


Thomas:2007:HQU


Turner:2006:SIS


Tsai:2005:CAE


Tan:2004:OBC

REFERENCES

Tokita:2001:ADC

Tang:2006:CHA

Tian:2005:RWS

Tousidou:2000:IMS


Takahashi:2002:QPK

Takahashi:2001:QPK

Tochikubo:2000:RAE

Tomaszewski:2006:YSY

Topham:2002:BRJ

Totsch:2000:MSS
REFERENCES


REFERENCES

[Tseng:2007:SAG]

[Takano:2000:PTH]
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]

[Turing:2004:BS]
REFERENCES


REFERENCES


[Unay:2008:SQE] Ozan Unay and Taflan I. Gündem. A sur-

Uchida:2009:FP


USC:2000:HRS


USHCAS:2000:UEP


USHCJ:2000:HSF

[United States Congress. House Committee on the Judiciary. 106-1 Hearing: Security And
REFERENCES


REFERENCES


Ustimenko:2001:CGT


Ulfving:2000:GS


Uzun:2004:BRC


Vacca:2006:GWN


Vadhan:2003:CLC


Vaudenay:2001:DID


Vaudenay:2002:SF1

Serge Vaudenay. Security flaws induced by CBC padding — applications to SSL, IPSEC, WTLS .... Lecture Notes in Computer Science, 2332:534–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print),


Verheul:2001:EXM


Vercauteren:2002:CZF


Vergnaud:2006:RBS


Vernitski:2006:CUM


Vladimirov:2004:WFS


Vassev:2009:STA


Voloshynovskiy:2001:BDA


Viroli:2003:TPA

REFERENCES

Vural:2007:IND


Vo:2008:SMA


Volos:2009:IEP


Viega:2003:SPC


Viega:2002:NSO


Vasco:2005:NCS


Vaughan-Nichols:2004:VAS

vanOorschot:2008:PMU

vanOorschot:2007:IRS

Vogt:2001:USC

Vasco:2001:CPK

Voyiatzis:2008:SFS

vanTilborg:2000:FCP

vanTilborg:2001:ECC

vanTilborg:2005:ECS

Vaudenay:2007:POK
REFERENCES


Venkatesan:2001:GTA


Wittaker:2006:HBW


Woody:2007:COS


Weitzner:2008:IA


Wachsmann:2005:CAK


Wallach:2000:SSM


[vW01]


Vaudenay:2001:SAC

Wagner:2000:CYL

Wagner:2002:GBP

Walter:2001:PBM

Walter:2003:STM

Wang:2004:AWA
Wang:2004:TVS


Wang:2005:SCR


Wayward:2000:RPK


Washington:2008:BRB


Washington:2008:ECN


Wayman:2001:FBA


Wayman:2002:BAT


Wayner:2002:DCI


Wayner:2009:DCI


Weiss:2000:CAC

REFERENCES

Wu:2002:CSCa

Wu:2001:CDS

WBD01

Wong:2001:EMA

Weeks:2000:HPS

Wu:2001:CKA

Wong:2001:EMA

Wong:2001:EMA

Wong:2001:EMA

Wong:2001:EMA

Wong:2001:EMA

Wong:2001:EMA

Weis:2001:SYH

Wang:2005:TAP
Xinyuan Wang, Shiping Chen, and Sushil Jajodia. Tracking anonymous peer-to-peer VoIP calls on the Internet. In Meadows and Syverson [MS05b], pages 81–91. ISBN 1-59593-226-
7. LCCN QA76.9.A25. ACM order number 459050.


REFERENCES


[WHL00] Tzong-Sun Wu and Chien-Lung Hsu. Convertible authenticated encryption scheme. *The
REFERENCES


[Wu:2002:IBM]


[Wu:2003:TSS]


[Wu:2003:IMT]


Wiener:2000:AAH


Winterbotham:2000:USI


Williams:1999:QCQ


Wilcox:2001:SEH


Windley:2005:DI


Winkel:2005:GEC


Winkler:2005:SAU

REFERENCES

Withers:2001:IWU


Wang:2007:VBW


Welschenbach:2001:CCC


Wang:2005:ECSb


Won:2006:ISC


Weigold:2008:RCA


Walter:2003:CHE


Wang:2002:AAB


REFERENCES

Wedde:2004:MAA

Wu:2004:RKA

Wang:2005:CHY

Wang:2007:NCD

Wen:2005:TRB

Wang:2009:DSM

Wang:2005:SAI

Wang:2005:IAW

Wong:2004:RCK

Wang:2005:TSP


REFERENCES

Wool:2000:KME

[Woo00]

Wang:2003:SGP

[WP03]

Wollinger:2005:CVH

[WPP05]

Weimerskirch:2001:ECC

[WP01]

Wang:2001:TUR

[WPS01]

Wrixon:2005:CCO
Fred B. Wrixon. Codes, Ciphers and Other Cryptic and Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet. Black Dog & Leventhal Publishers, New York, NY, USA,


REFERENCES

Wu:2000:PKC

Wu:2001:FED

Woodruff:2002:CUC

Wang:2004:CWS

Wolf:2005:NML

Wang:2006:SPS

Wang:2008:DCP

Wu:2001:CFF


Worley:2000:AFP


Wollinger:2000:HWH


Wincelberg:2002:LIE


Wang:2008:HQS


Wang:2002:WEM


Wu:2005:CTR

Wyant:2002:APK

Wyler:2005:ANS

Wang:2005:CSA

Wang:2005:FCFa

Wang:2005:FCFb

Wang:2005:ECSa

Winslett:2005:PLD


Xu:2001:EIE


Shouhuai Xu and Ravi Sandhu. Two efficient and provably secure schemes for server-assisted threshold signatures. In Joye [Joy03b], pages 355–372. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743 (print),
REFERENCES


Yiu:2008:ODC


Yang:2009:ETP


Yang:2008:NFD


Yung:2006:PKC


Yekhanin:2007:LDC


Yan:2006:ICP

Yan:2007:NSM

Yan:2008:NFD

Yu:2007:NSM

Yu:2008:ODC

Yu:2009:ETP

Yu:2004:MSS

Yu:2007:NSM

Yu:2008:NFD

Yu:2009:ETP

Yu:2007:NSM

Yu:2008:NFD

Yu:2009:ETP

Youssef:2001:CIM


Youssef:2001:IAB


Youssef:2001:CPK


Yen:2000:CBO


Yang:2005:IME


Yamamura:2000:QCB


Yamamura:2001:EDA


Yi:2004:AKA


Yen:2000:CBO


Jia Yu, Daxing Li, and Rong Hao. An efficient hierarchical ID-based signature scheme. In Han et al. [HYZ05b], pages 92–?? ISBN 981-270-153-2. LCCN ????
REFERENCES


Yoo:2002:LAU

Yurkewych:2005:CIR

Yue:2006:NCB

Young:2006:MCC

Young:2008:WRB

Yang:2009:AIO

You:2001:RMW

Youssef:2001:CAF

Young:2001:RP

You:2001:CAF


Yoshiura:2001:AWB


Yao:2009:CAR


Yang:2004:ISE


Yung:2002:ACC


**Yang:2005:CIA**


**Yang:2005:IYS**


**Yang:2005:VCS**


**Yang:2005:YWC**

Yang:2005:YWC


**Yang:2008:FSD**


**Young:2000:RBA**


**Young:2001:BOK**

REFERENCES

Yoon:2005:CZX


Yoon:2005:SWL


Ye:2001:ATD


You:2001:GEC


Youssef:2009:IEU


Zane:2001:EWD

REFERENCES


[ZBP05] 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 ????


REFERENCES


Zhao:2006:SAP


Zeadally:2000:IPQ


Zhang:2005:CSS


Zhao:2006:NDN


Zhang:2008:CLR


Zheng:2001:ISS

REFERENCES

Zhang:2002:BAF

Zhang:2009:IBR

Zirkind:2007:ADC

Zheng:2002:NPK

Zheng:2002:ACA

Zhou:2002:MVD

Zirkind:2007:ADC

Zheng:2002:NPK

Zheng:2002:ACA

Zhou:2002:MVD

Zhirkind:2007:ADC
REFERENCES


Zhang:2004:AFV

Zhang:2004:RMA


Zhao:2005:MCE

REFERENCES


REFERENCES

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

Zhang:2001:ASE


Zhang:2003:FSP


Zafeiriou:2005:BRW


Zhu:2002:PAK


Zhang:2005:ISS


Zhang:2005:SCA


Zhu:2002:PAK

REFERENCES

Zhang:2004:NMS

Zhang:2005:ASP

Zhang:2005:ISM

Zhang:2008:FIC

Zeng:2001:CHR

Zhu:2007:EIB