Title word cross-reference

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

$(k, n) + 1$ [LCZ05c]. $(\lambda, \omega)$ [VDKST06]. $(p_k)$ [BINP03]. $(t, n)$ [CHY05a, HL05c, Kog02, LKL+01, YCH04, CLT07]. $(tn)$ [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, CLK+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 $\pm$ 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]. $g^2$ [Shp02]. $g_e(x, 1)$ [SZP02]. $GF(2)$ [CP03]. $GF(p^m)$ [OTIT01, RMPJ08]. $GF(p)$ [AIK06]. $(p)$ [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. $l$ [QPV05]. $M + 1$ [AS01a]. $F_q$ [CY02]. $Z_n$ [GRO05]. $GF(2)$ [GS03, KTT07]. $GF(2^m)$ [BBGM08, KTT07, KWP06, RMH03a, RS04]. $GF(2^m)$ [KKH03]. $SL_2(F_{2^n})$ [SGGB00]. $\mu$ [LN04]. $n$ [CT08b, Gon06, HKS00, LKJL01, TM01]. $N^{0.292}$ [BD00b]. $NC^0$ [AIK06]. $p$ [FL06].
p^q [LKYL00]. p^x [CHH01]. Q [Yas08]. r [JY01]. w [DwWmW05, OT03b]. x^w [Gon06]. y [OS01].

-Aadic [GHK+06]. -Bit [AIK+01, CDL+00, PCG01]. -Connected [BJLS02]. -Coordinate [OS01]. -coverings [SC02b]. -decompositions [vDKST06].
-DNF [BGN05]. -Metric [LBRZ01, LBRZ02]. -NNAF [DwWmW05]. -out-of- [CT08b]. -Polynomials [FL06, CHH01]. -Round [BP04, Bi00, GIKR02, CKL+03]. -Source [KLR09]. -st [AS01a]. -Steiner [WL02]. -Threshold [CLT07, Kog02]. -way [LKJ01].

.NET [For04, TG04].
/dev/random [BH05]. /evolution [Pat02a]. /MOM [DJL01].

0 [And04, BC04a, Gum04, Imr03, Puz04, WYY05]. 0-07-225242-7 [Gum04]. 0-13-10051-X [For04]. 0-226-74110-8 [Top02]. 0-262-14075-6 [Pag03]. 0-321-20217-1 [Puz04]. 0-385-49532-3 [Imr03]. 0-470-84402-7 [And04]. 0-03-Bit [GS07a]. '05 [ACM05c, MS05b, ZC09]. '07 [ACM07]. '08 [ACM08]. '09 [ACM09, EIE09a].

1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05b, WYY05c, Was08a]. 1-5848-518-1 [Was08a]. 1-Connected [BJLS02]. 1-out-of-n [AOS02]. 1.82Gbits [KV01]. 1.82Gbits/sec [KV01]. 101 [Sei00a]. 10118-3 [ISO04]. 106 [Uni00c, Uni00d, Uni00g]. 106-1 [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 [JJ02, 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]. 1920s [Bur02]. 1960s [Bur02]. 1982 [AJ08]. 1987 [Kha05]. 1993 [PPV96]. 1999 [Lee03b, Uni00a, Uni00b, Uni00f, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Uni01].

19th [BCD09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH+00b, Eke02, Iw03, KH08, KI01a, Sch00b, Wit01, YG01c]. 2001 [ACM01a, BC01, GJSS01, Lee03a, Pem01b]. 2002 [B+02, IEE02, RSA03a, Yun02a]. 2003 [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, WKP03]. 2004 [ACM04b, ZC04]. 2005 [ACM05a, ACM05b, ACM05c, ANS05, HYZ05b, ISO05, Roy05, Ter08, Yr06]. 2006 [ACM06]. 2007 [ACM07, An006b, SM07b]. 2008 [ACM08, Dep08, YRS+09]. 2009 [ACM09, May09]. 20th [Bel00]. 21 [AJ01b]. 21264 [WB00]. 21st [Jef00, Kii01a]. 21th [IEE09]. 22 [TZ01]. 22nd [Yun02a]. 23rd [Bon03]. 24th [Cra05a, Fra04]. 25th [Luc00]. 25th [Sh05a]. 26 [DB04]. 26th [EBC+02]. 27th [Men07]. 29. [Eke02]. 29th [FLA+03].

3 [Duw03, Imr03]. 3-515-07640-9 [Eag05]. 3-540-66778-4 [Duw03]. 3-Key [Kel05]. 3.0 [Flu02b, Hei01, SQ01]. 305 [ECM00a]. 306 [ECM00b]. 30th [Coc02a]. 314pp [Duw03]. 3278 [BWBL02]. 33rd [ACM01a]. 36th [ACM04b]. 37th [ACM05c]. 39th [ACM07]. 3D [LZP+04]. 3GPP [KSHY01, SM02]. 3rd [ACM05a, USE00a].
Adaptively
[AF04b, CHK05, FMY02, JL00].
Adaptively-Secure [CHK05]. Added
[Ano02b, St.00]. Adding [FBWC02].
Addison [Puc03]. Addition
[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].
Addison [Puc03]. Administration
[USE00c, USE00a, Ris06, WL04a].
admirable [Cra05b]. Admitting
[HSZI00]. Advance [CZB′01]. Advanced
[DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK′03b, DFCW00, ISTE08, Swe08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Har00, Her09, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sye00, WBRF00, Wri01, YW06].
Advances [Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS07, ELv01, Kil01a, Oko00, Pě01, Pre00, TIS07, Yun02a, Kat01, Bih03, CC04a, Cra05a, Fra04, Km02, Lai03, Lee04b, LLT′04, Li05, LST′05, Men07, Roy05, Sho05a, Zhe02b]. Advantage [SZ01].
advantages [CDS07]. adventures [Hro09]. Adversarial [CLR09, GSS08, MNS08]. Adversarial-knowledge [CLR09].
Adversaries [CM00, JQ01, KSR02, Lu02, RK05, SKR02, GXT′08, ZD05]. Adversary [Ab00a, Gor06, RW02].
AES [CGH′00b, DRS05, FIP01a, Her09, Pha04, AG01, An00a, AL00b, BBK′09, CG03, Coc02b, DR00b, DR02a, DR02b, DLP′09, DPR01, Dau01, Dma00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, IK00, IK01, JH00, KS09a, Kel05, KS00, KV01, LPO2a, Len01, MHM′02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQQ03b, RRY00, SKKS00, SM03b, Sch00b, SKW′00, SW00a, SL00, WW00, WB00, WOL01, WWP00, WWCW00].
AES-CBC [Fer06]. AES-like [DLP′09]. AES-related [Sch00b]. Affine
[Ben00, CT09, Fel06, HH09].
Affine-Transformation-Invariant [CT09].
AFIS [Zir07]. African [WD01b]. after
[Ber03, McL06]. against [Fox00]. Against
[CS05b, DM07b, FKS00, KS00a, KKS00a, KKS01, Mes00, Mes01, MP05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Bau05, BPR00, BB02, BBN′09, BBB′02, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egl00, EBS01, FP01, Fry00, Geb04, HNZI02, HLL′01, Hsu05b, HLC08, Ino05, ISW03, IIT03, JKS02, JJO06b, JT01a, Kan01, KM02, KML′02, LM08, LPV′09, Lu02, Mit00, Mo02, MG08, NRR00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC′02, PSP′08, PS01b, PQ03b, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sho00b, SKU′00, SKI01, SLL′00, Tad02, TV03, VHP01, XH05, YJ00, YKLM02a, YKLM02b, YKLM03, ZSJN07].
Age [Mar08b, Lev01]. Agency
[AJ08, Bam02, Kov01]. Agent
[HQ05, KC02, PDZH09, RD01, RC01, Rot01, ZYM05, KX00, SSM′08, SH00]. Agent-Based [HQQ05, SSM′08]. Agents
[WHI01, Hau06, LSA′07]. Ages
[Eag05, Kin01]. Aggregate
[BGLS03, WK05]. Aggregated [ZSN05].
Aggregation [Her06, CCMT09, MS09b]. Aggressive [WY05]. AGM [Gau02]. Agreement
[AAG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB′04, AK10T04, CYY05, CYY05, Che04a, CY05, CJ04, CJL05, HWWM03, KPT′04, KRY05, KHKL05, LKKY03a, LKKY03b, LL04a, LL05a, LKY05b, LKY05c, LKY05d, LLY06, LLS′09, LLR02, PQ03a, PQ06, Shi05,
SW05, SC05b, Tsa06, Tse07, VK08, YY05, YS02, YSH03, Yi04, YRY05b, ZC04, LRR06. 

agricultural [Lov01]. Aided [NS01b, HLL +02]. aim [Pau02a]. Aimed [SFDF06]. Airport [Sas07]. airwaves [Dav07]. Ajtai [GK05]. A KS [Che03]. A [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx]. al-fusul [MAaT05]. al-Ka [MAaT07]. Al-Kindi [MAaT03, MAaTxx]. Al-Kindii [GK05]. AKS [Che03]. Al [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx].
[Mea04, MT07, MRST06, OS00, Psg+09, PS05b, SK01b, WLT05a, WFP05, XH05, XMST07, YCW+08, YC08, ZWWL01, ZL04c, ZDW06]. **Analytic** [Shp03, Nie04].

**Analyzing** [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04].

**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, ELv03, Fra04, IEE00a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Kil01a, MZ04, Men07, Sho05a, USE01b, USE01a, USE02c, VY01, Yun02a, ACM00, Bel00, HA00, Jef08, NH03, ST01d].

**Anomaly** [RCG+05].

**Anonymity** [GM03, IKOS06, MP02, SS01b, EY09, LV07, Par04].

**Anonymization** [FXAM04, RW07].

**Anonymous** [ABC+05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL+08, SOO02, Wan04a, YAO9, ZJ09, G030a, EY09, LHC08, Sae02, Sha03c, WCJ05, YTYW03, ZC09].

**ANSI** [HI00, Kel05, Oiw09].

**ANSI-C** [Oiw09].

**Answers** [PT08].

**Anthony** [Pag03].

**Anti-Circumvention** [Kha05].

**anti-virus** [Ano05b].

**anticipation** [Goc00].

**Any** [Fis01b, HNO+09, CDM00, DFMO4, DMS00, HR07, Poi00].

**Anyone** [Ros07].

**Anytime** [DKST09].

**Apache** [Hadd01].

**API** [MWM01, Mor03].

**APIs** [BM01c].

**Appendix** [Kel05].

**Applet** [ZFK04].

**applets** [Bis03a].

**Applicability** [Wya02, TM01].

**Application** [AD10, ACS02, Bai01b, Boy01, CL02a, CKQ03, Dam07, Dhe03, GHK+06, HF00, IKP+07, JX05, Jon04, Lai03, Lec04b, LLS05b, LXM+05, NP07, Oka00, Pfo1, PQ03b, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TWNA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG09, CMKT00, CP07, DIM08, FP00, JRS09, Lav09, MT07, MPH06, MK05a, NZS05, RSS04, SSST06, TC00].

**Application-Aware** [IKP+07].

**Applications** [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, Bl05a, BGK+03, BS00a, Bih03, BGY08, BSS02, BLO8, CC04a, CD00a, CV02, CGH01, CZ05, CHSS02, CSY09, Cra05a, CD10, DJ01, DK02, DK07, DA03, DFPS06, FR02, GS08, GKK+09, GJKR03, Gen04a, GRW06, GL01a, GL04, HRS02, HNN06, Har06, Has01a, HSS04, HR05, HJJ05, JT01b, JY01, KMM+06, KGL04, KMO01, KRM01, Knu02, MA07, MM07b, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Shp03, SXY01, SPGQ06, Vau02, Yna02, XYL09, YZ00, Zha02, ACTZ05, Ate04, AH05, AFGH06, BG08, BGL+03, CCCY01, CM05b, CS09, CSK+08, DY09a, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gal02, GVC+08, GKK+07, GB09, HHSS01, Has02, Hen01, HKPR05, Jac00, KV+09, KNS05, LA00, Lee04a].

**applications** [LJ05a, LPW06, LB05, MY01, Ma06, MC04, MSV04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SSS06, Sch00a, Sch01c, St03, Sch04a, Sch04b, Sch05a, SPHP06, WW08, WA06, VWV0, YS04, ZBP05].

**Applied** [HW03a, HWR09, SL07, GV09, GNP05, IKY05, JY04, ZYH03].

**Applying** [Elb09, KC02, Lan00d, LMS07, SQ01, SPM08, TN+09, vDKST06].

**Appointed** [CL01a].

**Apprehension** [AJ08].

**Approach** [BKM07, CGF09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lrut03, QMT02, PBD00, Pau02a, Pre02a, SKG09, VH09, VSSV01, Vir03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJ01, DLMM05, GGH+08, Har05a, J01, JW01, LYC02, MT09, Mar05b,
[MI09, Mos06, NN03, SLP07, SN04, SW00b, ZLX99, ZS01, ZL04b, ZL04a]. Approaches [CGMM02, AvdH00, DG05, Fri07, Has01b, KXD00]. approval [Wan04b].

Approximation [CLZ02, Kuk01, WL02]. Approaches [BDQ04]. Apress [Ter08].

April [Ano00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH00b, DFPS06, Joy03b, Km02, Mat02, NIS00, Nac01, Sch01d, SMP09, YDKM06]. APSS [ZSV05].

Arabic [MAaTxx]. Arbitrarily [RW03b]. Arbitrary [AR01, BR00b, BR01, CKN00, CHL01b, CF02, Tee06].

Arbitrary-Length [AR01, BR00b, CKN00, CHL01b]. Architectural [ASK07, ABM00, BMA00a, BMA00b, BMA00c, CW02, Gro03, KV01, LTM00, ZYLG05, Ano05b]. Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LKM05, LZ04, LXM05, Lut02, MP01c, MFS09, Rot02a, SM01m, SM03b, SLG05, Uzu04, Ch00, CC05e, DHL06, Io05, LHL03b, MMPM09, SKW07, SH07, SH05, Tan01, WW01].

Architectures [BGK03, KLY02, RM02, SM02, Con04, DP04, GKS05, NdM04, RH00, WH02b]. 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 [HNO09]. ARITH [BS03, BC01, IE05b]. ARITH-15 [BC01]. ARITH-16 [BS03].

ARITH-17 [IE05b]. Arithmetic [BS03, BIP05, BGK03, BCDH09, BC01, CT03, Gro03, IE05b, KM07, KIr03, PPV96, RDJ01, SR06, GPS05, PS04a, SOIG07]. arithmetics [Lam91]. ARM7 [DV08, XB01]. armies [Ano03b]. Army [Boy03]. Arne [Bec02]. array [DZL01].

Arrays [ABM08, BS00a, GC01a, HW05, PP06a]. Arrived [Law05]. arsenal [Blu09]. Art [An07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Eri03, Eri08, MS02d].

Article [Che08b]. Artifacts [EHK03]. Artificial [Cop04b, MMHY02, Arun [For04]. ASCI [MJD01]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DNO0b, KIO1a]. ASIC [WOL01].

ASIP [SKW07]. asks [Ano08a]. ASM [MK05a]. Aspect [Kos01a]. Aspects [BLMS00, CMR06, Pel06, DLP09, Rup09]. Aspiration [Ash03]. assembly [Gou09]. assessing [CDD05]. assessment [CC05e, DMS07]. assets [KH03, NRR00]. Assignment [BRTM09, HC08, CHC04, DFMO04, Hwa00, TP07, WC01b, hY08]. assignments [SWR05]. Assisted [ECG07, XS03, BB05, LHL04]. ASSL [VH09]. associated [XLMS06]. associativity [HR08]. Assumption [CS00, DN00a, FOP01, KM03, ZD05].

Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT09, Nao03, SBZ02, Mic02a]. Assurance [LXM05, AL04, BJ02, FOP06, Gha07, Jen09]. Assurances [Bar06b].

Astrology [Pag03]. Astronomy [MYC01]. Asymmetric [CH07b, Man01, SY01a, SBZ02, WH01, YG01a, GJ04, Lee01, OP01b].

Asymptotically [vDW04]. Asynchronous [CKPS01, FML03, KSR02, SKR02, ZSV05]. at-targama [MAaT05]. Atlanta [IE09b].

ATM [Pat02a, Pat02b, Zee00]. Atomic [CN06]. Attached [RCL00].

Attachments [Pic07]. Attack [Ahm08, CKQ03, CS05b, CS03b, Des00b, Fi00, VF03, GHJ00, GHJ01, HQ01, Hug02, HW01, JJO0b, KCP01, KS00a, KML02, KM01c, LY07, LNL08, LV04, LM05, Lu02a, Man01, MH04, MSU05, Nov01, OM09, PF06a, PQ03b, RMS05, SG09, Sch01b, Sho00b, Sma00b, VHP01, YKL02a, ZC04, AS05, DKL00a, Duj08].
Duj09, GM00a, HAU04, Hes04b, HG07, Iwa08, JJO2, KS09a, KM04a, LM08, Law09b, LS05b, Mir05, OS00, SIR04, XH05. Attack-Resistant [LNL+08]. attacker [BDSV08]. Attackers [JMV02]. Attacking [FMP03, KPR03, Luc00, TMMM05, BF06a]. Attack-Based [TMMM05]. Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, BMM00, BBB+02, BDK+09, BU02, BM03b, BCP02b, BM01c, Can06b, CS07b, CT08a, CJS01, CKM00, CJNP00, CM03, Cou03, CWR09, CD01b, DPV01, DFS04, DJ06, DS08, DM07b, FKS00, FOH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GKO2, HSH08a, HNZI02, HR04a, HSH01, HLC08, ISW03, JJO0d, KKS00a, KS00b, KKS01, KCJ+01, KI01a, Law09a, LLS05a, LJS05b, LJS06, LJS07, LJS08, LJS09, RS01, SK01, Sen00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZ05, YYDO01, YY01, YG01b, vW01, BPS08, Bau05, BCS08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH08b, HSH09, Has01b, Hsu05b, HLU05b, Ino05, IM06, JD01, KS05a, KTC03, LPV+09]. attacks [LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RG05, Sch00c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07a, WL04b, Yan07, YS02, ZJSN07]. attractors [HHYW07]. Attribute [LY05, RSA00e, IY05]. Attributes [SS01b]. Auction [AS01a, Ano01a]. auctioning [RCG+05]. Auctions [Bra01b]. Audio [Arn01, CS05c, DRL09, MH05, WNY09, WWL+02, XFZ01, WNQ08, BS01b, KJR05, KN03]. Audio- [KJR05]. Audio-and [BS01b, KN03]. Augmented [CS07e, You01]. Augmenting [AL04]. August [AMW07, Bel00, B+02, Bon03, Fra04, HHI04, HH05, HA00, JQ04, KPK02, Kli01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch04b, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a]. Australia [Boy01, IZ00]. Austria [DKU05, Pf01, Jef08]. Authentic [DGMS03, Dur01, SS01b]. Authenticate [Bau03a, Bau03b]. Authenticated [AGT01, BN00a, BPR00, BU02, BC04b, BM01, BPM00, BCP01, CPF04, Chi08b, DG03, DA03, EP02, GKK07, GL03, GTVC03, HS07, KOY01, KY03, Kra03, Lee01, LHT09, MPS00, Mac01, MS02, MND+04, NA07, Nam02, Ngu05, Poh01, SK00, Vau05b, WC01a, YPPK09, Yi04, ZWCT02, BKN04, BCP07, CY05, CYH05, Che04a, CL008, CJ04, CJL05, DG06, GL06a, GMR05, HTJ08, HWW02, HTW03, Hsu05a, Hua05, HL05c, HL05d, KOY09, KY05, LKK03a, LKKY03b, LKL04a, LLL04, LLY05a, LKY05c, LKY05d, LHC08, LL02, LRR02, LWK05a, Mi08, PQ03a, PQ06, RB03, Sei05, SW05, SC05b, TLH05, TJ01a, Tse07, WH02a, XY04, YW05, YC09a, YS02, YES03, YRY05b, YPKL08, ZC04, ZAX05, ZW05b, ZL05]. Authenticating [AAP01, Chi08a, CGV09, Fur05, JW05, PM08, RCB00, YSS01, Lin01a]. Authentication [AAK09, AP09, ANRS01, An001b, An01e, An02d, AHKM02, ANL01, BH06, BACS02, BCL+05b, BCC+02, BM03a, BA00a, BKR00, BCC01, BDhKB09, BR02, BDFP05, BDF01b, BM03c, BL02, BLDT09, BWE+00, CV03, CG08, CS07b, CLK01a, CLK01b, CC05b, CC09, CJ03c, CW05, CT09, Cim01, Cir01, CGK+02, CJ+04, Cou01, CMB+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FM00b, Freq03, FSSF01, Gan01a, Gar03a, GM05, GSC02, GD02, GT02, Gut04c, Had00, HSZ01, HSH02, HSH06, HKW06, HY01, Hoe01, HS01b, HP00, HL07, ISSZ08, Jab01, JP02a, JP07, JP02b, KJR05, K09b, KH05, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LIT+04, LB04, LL05c, LSH03b, LM00, LHL+08, Lys07, MM01a, Mal02, MJ04, MD04, MR03, MG02, MNT06, Nao02,
Nik02a, Nik02b, OKE02]. Authentication [OHB08, PBD00, Par04, PBC05, PK01, Qu01, RKZD02, Ric07, Ril02, SNWX01, SR01, Sch04c, Sch05b, Sei00b, SY01b, SGB02, Smi00, Smi01c, Smi02, SE09, SK06, Str01b, SJ05, SYLC05, SC01, TK03, TZT09a, TZT09b, Tsa01, VN04, WLLL09, WC09, Way01, Way02a, Wei06, WB08, WT02, WS03, WL07b, WLT05b, WHL05, XYL09, YI01, YEP+06, YSR01, YLLL02, YKW01, Za00, ZJ04, ZBLvB05, AvdH00, AF04a, All06, Ano00k, Ano00l, AAKD09, AL04, Bad07, Bel04, BGP02, BSSM+07, BFG04, BFG05, BS01b, BBG+02, BDFP02, BFM07, Cer04a, CC01, CCK04a, CC04b, CCK04b, CC05c, CY05, CCS08, CWJT01, CJT01, CJ03b, CH07a, CL09, Coc01a, CMvdV06, Dal01, DY09a, DGK+04, DG05, DW05, FGM03, Gan08, GLC+04, GTY08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Hsu06, HLY02, LLH02, LHL03a, LF03, LKY04, LW04, LHL04, LKY05a, LLY06, LL+09, L05, LST+05, LCX08, LW05a, LLH06, LFW04, LHL03b, LT04, LC04a, Lin07, LN04, LL08a, LLW08b, LC05a, LC05b, Luk01, LS09c, MAB06, MIt00, MR00, ME08b, MP07, NC09, NLD08, PY08, PCS03, PCC03, PI06, Pei04, Pot03, Pot07, RG06, SNW01, SG07, SN07, Sh05c, Sco04, Sei05, Sh105c, SSM+08, Sh105, SL05a, St00, Ste05a, SW02, SCS05b, SC05c, SCS05c, SFS05, SY06, TM06, TB02, TOEO00, TIS07, TW07, TAL05, UBE09, VM03, VK08, Vol05, Wac05, Wan04a, WL050a, WDN09, WL04b, WHHT08, XWL08b, YY04, YWC05, YTWY05, YCYW07, YYW08, YC09b, YS04, YRY04, YRY05a, YRY05c, YY05b, Ybf04, ZL04a, ZK05, ZSN05, Zha06, ZDW06, ZSN07, dB07, CS08b, ECM00a]. Authenticator [CKY07]. Authenticity [AB01, Bla02a, CBD+05, GJ03, GOR02b, HG03, RW03b, Sch01a, Mit02]. Author [An000b, An001d]. Authorisation [SN07]. Authorities [CHS02, HWW04, WH02b]. Authority [Con00, JLL02, CCH05, KB09]. Authorization [BACS02, CJK+04, LSZ05, ZK02, YT09, GJJ05, JEZ04, Lin07, SRJ01, WL04a, WB05, YbJ04]. Authorship [Top02], auto [YY00]. auto-recoverable [YY00]. Automata [LZ04, MGC02, Wue09, Bar04, CC05d, K03, Lah00, LQ08, Mon03, SB04, SHH07, TC00, dRMS05]. automate [Burt02]. Automated [CDR01, LLW05, LLW09, HJW05, IY05, LS05b]. Automatic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05]. automorphism [Pae03]. automotive [LPW06]. Autonomic [VH09, Che05b]. autopsize [Car00]. auxiliary [Dam00, DKL09]. availability [CBD+05]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average [KMT01, CGHG06]. average-case [Mic02b]. avoid [Tyn05]. avoided [CNPQ03]. Award [RSA03a, Bar00b, Coc03]. Awarded [Coc02b]. Aware [IKP+07, OHB08, CBSU06, Zee00]. Awareness [HLM03, BK05]. Away [Coc03, Ols00, Tey06]. Awkward [TvdKB+01]. Axiomatization [dH08]. B [SPK08, YG01a]. B-Spline [SPK08]. B2B [Zho02]. Babbage [Bar00a]. Back [CZB+01, KCD07, SF07, An000g]. Back-End [KCD07]. Backdoors [CS03c]. Backup [Str02]. backward [HCD08a, HCD08b]. backward-and-forward [HCD08a, HCD08b]. Bacon [GG05a]. bad [BBN+09]. bail [An001g]. Bait [Luc02a]. Balancing [Hf01, Lut02]. Ballot [Cha04]. Baltimore [ACM05b, ACM05c, GL05]. Banach [AUW01]. Bandwidth
bandwidth-efficient [SLP07].

**Bandwidth-Optimal** [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a].

**Bandwidth-Optimal** [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a].

Barcode [Che08b]. Bare [DPV04]. Barken [Sty04]. Barret [Gro01].

**barriers** [Kov01]. **base** [DIM08, IR02].

Based [Ano01c, ANR01, AF03, AJ008, BDG+01, BKL02, BNPS02, BN02, Ben00, BRS02, BF01b, BF03, BB04, Bon07, BCHK07, BGH07, BPR+08, BD03, BMN01, Boy03, BQR01, BM01c, BSN000, BRTM09, CGFSHG09, CvTMH01, CK02a, CGMM02, CF01b, CC02a, CV03, CPP04, CDC07, CS07b, CLT07, CHSS02, CHM+02, CZZK05, CM05a, CTH08, CGK+02, Coc01b, Cou01, CFS01, CS00, DN00a, DMK005, DTD03, EHK+03, EM03, FL06, FM02a, FM01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HC08, HH09, Ig02, Jam00, KBD03, KLN+06, KJ05, KKG03, KY02a, KL05, Ke03, KY01c, KY02b, KC09b, KK02, KC02, KCD07, KPR03, KM05, Kra02a, Ku02, KWP06, KT00, LLI02, LP03, LKLK05, LHT09.

**Based** [LZ01, LZ04, LL05c, LPZ06, LY07, LLRW07, LW00, LSK03, LS05, LLS05b, LQD07, MP000, Mar02a, Mar08b, MNP01, Miy01, MG02, MII01a, MSU05, NMO05, Nak01, Nam02, NBD01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP000, PZL09, Ri02, RE02, RH02, RS00, RS03, RS08, RMC01, Sal05b, Sch01a, SSF09, Sha02, Sha01e, SOO01, SXY01, Sma03a, SBEW01, SGB01, TM005, TLL02, TST09a, TZTO9b, VMS05, Van05b, Ver06a, VHP01, VK07, WR02, WY02, WZW05, WG05, WC03, WH09, WBD01, WC04, XLY09, YM01, YT09, YYD001, YSS+01, YKW01, YLH05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWCY02, vDW04, AAP07, AA08, AN02b, App05, AAKD09, BB09, BR04, BF08, BS01b, Bla01b, BM05, BLP06, BGL+03, BDO09b, Buh06, CGH06, CG06, CL02b, CL04d, CL00, CCH04, CY05, Che05a, CCS08]. **based** [CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CJL06, CJL05, Che08b, CYH+07, CVFZ06, CCD+04, CTT07, CHT02, CC04c, Cra05b, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EKH04, FXA04, FWL08, GMR08, GW08, GL06a, GHG0500, GS01, GPS05, GGS+09, GB09, HMO, HLL+02, HCD08a, HCD08b, HL09, Has00, Her07, HPS01, HG05a, Hsu05a, HLwWZ09, Hio09, HP01, HLL03, HL05d, IM06, JK01a, JK01b, JW06, JZC05, JLL01, KG09, hKL005, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KLC03, Ku04, KCC05, Kwo03a, KHKL05, LHC03a, LF03, LKY05a, LKY05b, LH05, LD01, LTH05, LPM05, LW05a, LWZH05, LLY07, LL08, LW08b, LCC05, LAS+07, LCZ05c, LCZ05a, LLC06a, LLC06b, MS09c, Mic01, MR09, MJ09, Mit00, MB08, MC04, MPPM09, MV03b, NZCG05, NC09, NSN05, OS09, PCSM07, PW05, PBMB01, PSE+09, PS08a, Pel06]. **based** [PSP+08, FC00, PLJ05a, PLJ05b, QCB05a, Reg03, Reg04, RG09, RCC+05, Sae02, SG07, Sco04, Se05, SPG02, Sh03a, Sh03d, SC05a, Sha05c, Sha05d, SC05a, mSGFtL05, SSM+08, SW05, SH00, SK01b, SCL05, SLC05, SU02, SC05c, SY06, TWNA08, Ts05, UHA+09, UBE09, VS01, VK05, WA0F00, WL07a, WJP07, WNQ08, WHH05, WH09, WW01, WH02b, WY05, XMST07, YW04, YCW+08, YWWD08, YS04, hY08, YJ00, YPS01, YRY05c, YPKL08, YW00, ZC04, ZC09, ZD06, ZCL05, ZYW07, dRMS05, N205]. **Bases** [AAC+01, ADDS06, BKP09, B+02, CvTMH01, EBC+00, FJ03, FLA+03, CCT08, Fan09, ZT03]. **Basic** [Go01b, Go01a, Go04, Kat05b, Puc03, Ste02, Bon00]. **Basics** [Le06, Lut02].
Basing [BPR+08, CHL02, AGGM06, AGGM10].

Basis [RMH03b, Vav03, vW01, GPS05, LS05b, RMH09a].

Batching [Ara02, HLT01, PBD07, Scha01d, BLH06, HLH00].

Battery [CBSU06].

Bay [Cal00c].

Bayes [Goo00].

Black [Ina02a].

BCH [IEE02].

BCH [MLC01].

Bi-linear [Cou04, PJK01].

Bi-directional [BS00a, LSKC05].

Biased [B02, BM00, RR02, SKQ01].

Biometrics-Based [Cou04, PJK01].

Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01].

Beach [IEE00a].

Beg [Lev01].

because [AJ08].

Become [Ort00].

BeepBeep [Dri02].

before [Un00a, Un00b, Un00c, Un00h, YJ00].

Beginning [Dew08, Hoo05].

Beginnings [Bud00b].

Begins [MP00].

Behavior [Vav03].

BEHEMOTH [Bar00c].

behind [Hen06b].

Bel [Goo00].

Belief [BPST02].

believing [Bu00].

Bel [BZ02, Eke02].

Benchmark [Ase02, TLY04, LDH06, YLT06].

Bendy [Sus07].

Benefit [YKL02a].

benefits [CH00].

Benford [NM09].

Bergen [Ytr06].

Berkeley [IEE06].

Berlin [FLA+03].

Bermuda [Bl03a].

Bernard [DNR03].

Bennis [Coc02b].

Bennis-Lee [Coc02b].

Best [Bau01a, Bau01b, MFS+09, Gol08, Ste02].

BestCrypt [Bau02b].

Bethesda [ACM09].

Better [V03, P00, RR02, SKQ01].

HLLL03, Pau03].

BetterBASIC [ASW+01].

Between [DKMR05, Ket06, Ngu05, NN06, Fau09, GKM+00, GC05, MSV04, Pau01, RW03a, SK06].

Beurling [Bec02].

Beyond [Gor06, LMW05, Mar08a, Sch03, See04, Sty04].

BGP [ZSN05, vW00].

Bi [Cou04, PJK01].

Bi-directional [PJK01].

Bi-linear [Cou04].

Bias [CL02c, Sd00].

Biased [BS00a, LSKC05].

BiBa [RR02].

Bibliography [Bee05].

Bidiagonal [BR09].

Bidiagonal-Singular [BR09].

big [RR03a].

BigNum [SR06].

Bilateral [CT08a].

Bilinear [BGLS03, BMS03, CL04a, HAMS04, KK02, LC05b, VK08].

Bill [Gen00a].

billing [S+08].

Binarization [LSK05].

Binary [ADJ09, HMM01, LSKC05, OSSST04, SKG09, WCT05, ACTZ05, BG08, BG09, FSGV01, GB09].

Binary-Ternary [ADJ09].

BIND [Kle07].

Binding [DN02b].

BioAW [MJ04].

Biometric [AHKM02, Dal01, EM03, WHH01, KJ05, LTT+04, PK01, SR01, SAS07, Way01, Way02a, Wea06, BS01b, KN03, Li05, LST+05, MR00, Sni00, MJ04, TB02, ZJ04].

Biometrics [Ash03, Bjo05, MR03, Rii02, Str01a, BSS+07, BCP+03, Bu06].

Biometrics-Based [Rii02].

Biomolecular [B09].

Birds [MLM03].

birth [Bu06, SE01].

Birthday [Wag02].

Bisimulation [BP02].

Bit [AIK+01, BK06a, BL08, CGH01, CDL+00, DMS00, GS07a, IT03, KZ07, LNS02, MS09d, PCG01, RMH03b, SM03b, SXY01, VK09, ATSV00, Bar00a, BK07, GXP08, KZ03, KKL09, Luc00, Pri00, RMP08, SWR05, UHA+09, WW08, ZFK04].

Bit-Fixing [KZ07, KZ03].

bit-substitution [GXP08].

Bit-Locker [Kor09].

Bits [BS01d, SZ01, HN04, Slp02].

Bitslice [DPV01].

Black [An01i, CF02, CF05, DI05, DRR05, DS08, KY01d].

Black-Box [An01i, BR02, CF02, CF05, DI05, DRR05, KY01d].

Blackmailing [PS01b].

Bletchley [Sal00b, Cop05, Cop06, HS01a, Sal05a, SE01, Sni01b, Wei06, Win00].

Blind [AO00, BNPS02, BB00a, BSC01b, CL01b, JKK+01, LY07, Naf05, Pan02b, SP08, ZTP05, ZK02, Fan03, HC04a, JLL01, JL04, LHY05, LC05b, MS09a, SV08a, SHT05, WH05, ZC05].

blindness [Avh00].

Blink [S07b].

Block [AIK+01, BKR00, BR02, BR02, BSC01a, CvTMH01, Can01b, CLLL00, CP02, CMB+05, Cro01, DR00a, Dwo03, EYCP00,
Flu02a, HSH+01, JKK+01, KCP01, KYHC01, KKG03, LLRW07, LRW02, MV00, MS02e, NPV01, OMSK01, Pat01, PS06, Plid01, RMS05, SM03b, SYY+02, SKU+00, SKI01, WCJ09, XH01b, YG01b, Bai08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kat05a, KJ01, LDH06, LCP04, LKH08, MMJ05, PSP08, RBB03, SHJR04, SHH07, WF02, XH05, YI00.

Block-Based [LLRW07]. Block-Cipher [BR02, RBB03]. Block-Cipher-Based [BRS02]. Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. blockciphers [Fur01]. Blocks [Jou02]. Blockwise [JMV02]. Bluetooth [GBM02, LV04, LMV05]. Blunders [Bur01]. Blur [VHP01]. Blur/Deblur [VHP01]. Blurring [LSKC05, SK06]. Board [CGBS01]. boat [DB04]. Body [Ban02, TG07]. BOEL [Fin02]. Boethius [Eag05]. bolstered [Ano01b]. bombe [Wil01a, Tur04]. Bombs [Ano02i, LBA00]. bombs [Lov01]. Bond [CAC03]. Boneh [ASK05, Hes04a]. Bonn [DRS05]. Book [And04, Duw03, Eag05, Fal07, For04, Gas01, Gum04, Imm03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Rec01, Rot07, Sal03b, See04, Shp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wal00, Was08a, Kat05b, Lam07, Lun09, MAaT05, Sin99, Sin00, AAG+00].

Books [Dr.00c, Rec01]. Bookshelf [Lut02, Lut03, Wil01b]. Bookworm [Sal03b]. Boolean [Car02, CT03, CS09, MS02b, QPV05, SM00a, SM00b, SM03a, WV00].

Boomerang [KK00a, KKS01, KML+02]. Boot [HSH+08a, HSH+08b, HSH+09]. Border [MJF07]. Borders [PGT07].

Boston [USE01b, USE01a]. bot [Ano08b]. Botschaften [Sch09]. bottleneck [WL02]. bottlenecks [HTW07]. Bound [CY08, DGN03, KMT01, HILL03, HY08, GW00]. Boundaries [PGT07]. Bound [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vad03, DFSS05].

Bounded-Quantum-Storage [DFSS08]. Bounding [DM07b]. Bounds [BDF01b, BP03b, DIRR05, Di01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GGK03, JZ09, KS05b, PS02a, Shp99].

Bouwmeester [Duw03]. Box [Ano01i, BR02, CFS05, Di05, DRR05, DS08, FM02b, KY01d, Kil01b, SMT01, JnBuXgXm05]. Boxes [Bih00, BCDM00, ZC00]. BP [Wei00, Wei05]. Braid [AAFG01, CJ03a, GM02a, Hug02, KLC+00, LLH01, LP03, MS05, Cho08b, Hen06a].

Braille [Pau02b]. Branch [AKS06].

Braunches [Fe06]. Break [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breakers [CD00b]. Breaking [BKN04, DKFX05, GO03, GK02, Kov01, KR03, Kih08, Sal00a, Wri05, Fie09, Gar01, SE01, Smi01b, SL07, Swe08]. breaks [OS00].

Breakthrough [Coc02a, LR01, Pau02a]. Brief [Bon07, Cos03, Kir01a, Boo05, Gra01].

Briefs [MP00, PM00, Pau02a, Pau02b, Pau03, Pau09]. Bright [Ano01i, LNP02].

Bristol [DFCW00].

British [ACMO08, Fie09, Fra01, Syv02, Bud00b].

Broadband [MP00, SHL07, MJF+08].

Broadcast [AFI06, BGW05, CKPS01, CNV06, DS03, FW04, GS00, GKK007, GRW06, HSO02a, HLL05, LNP02, SNW01, Woc00, ASW00, KSW06, Kre05, Mar05b, NLD08, RG09, WDLN09, LN04].

broadcasting [TJ01b, WH02b].

Broke [Urb01, KS04]. Broken [Ahn08].

Brooks [Bar00b]. BRSIM [BP08]. BRSIM/UC [BP08]. BRSIM/UC-soundness [BP08].

Bruce [Sty04, See04]. Bruges [Pre00].

Brumley [AS05].

Buchmann
[Lee03a]. Buffer [FOBH05, Fry00, Ino05]. Bug [BCS08, Bor00]. bugs [GLJ06]. Building [Jou02, Kun07, Mar02a, And08, Bra01a, FB01, LS05b, McG06, MPH06, PQ06, DB04]. buitenlands [dL00]. Bulletin [Cer04b]. Bulletproof [Cha05b]. bundles [GT02]. Bug [ABM08]. Bug [Arn01]. Bush [Ris06]. business [HHSS01, Poh01]. Buy [PLW07]. Buyer [MM01a]. buys [Zaf00]. Buzzes [Coc02b]. Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGC05, LHR06, PI06]. Byzantine-Resistant [CNV06]. C [Ter08, Zol01, III00, Oiw09, RMPJ08, Sea05, Sea09, VM03, WK01, Wel05]. C# [MJ03]. C-testable [RMPJ08]. C2C [HTJ08]. CA [ACM04b, Joy03b, KKP02, Men05, Nac01, Oka04, Po06, Pre02c, USE02a, USE02b]. CAA [MGC02]. Cache [BTTF02, Kl07, OST05, OST06, TSS03]. CAIDA [Pri00]. Cairo [BEC04]. CalLC [Sil01]. calculus [MRST06]. Calcutta [Roy00a]. Calibrating [SDMN06]. Calif [ACM03c]. California [ACM03a, ACM07, Bel00, Bon03, Fra04, IEE00a, Kil01a, Sch01c, Sch04a, Sh05a, Sh06a, USE00b, USE02c, Wil99, Yuf02a, IEE06]. Call [An04a, An07b, An07a, MD04]. Calls [WG05, An08c, WC05]. Cambridge [ACM10, Chr00, Chr01, CCM02, CCM05, IEE03, JQ04, Kat05b, Kil05, Nac04, Pag03, Pac03, Rot07]. Camellia [AIK01, HQ01, KMO2, HLS02, SM03b, SK01, XH05]. Camera [CGK02]. Camera-Based [CGK02]. Can [BB02, CBZ01, Dav01c, Lai08, Ros07, Ver06b, CNP03, CG05, SBB05, Zir07]. Canada [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [II00, EYP00, NIS00, SKW00, SL00]. Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b]. cannot [Gav08]. canonical [TP07]. CANS [DW05]. Canterbury [CZ05]. Cantor [WP05]. Capabilities [BKTW01, AL04, ABD01]. Capability [MH05]. capable [ETMP05]. Capacity [ChLYL09, S01, ME08a, Wan05]. Cape [IE05]. Card [BCST00, CMG01, CL07, DF01, DFS06, RE03, RS01, SR01, An00k, An00l, AJ01b, Bor00, BGL03, Bur00, Cal00c, Car01, CCCY01, Cha05a, Con00, CHOO, DFC00, GMG00, HO1a, Has02, Hen01, Hus01, Jac00, LSA07, LC05a, Lu07, Q00, RE00, SP02, Sm00, VK08, Zaf00, Che00, FGL02, Pan02b, SK00, TV03]. card-based [LZ07]. CARDIS [DFS06]. CARDIS’98 [Q00]. Cards [An04, AJ01b, Bel01, CK06, DJL01]. HBD01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NFQ03, Q01, Sak01, Sh01c, TBD01, VPG01, YMY01, An04b, An04c, AJ01a, BPR01, BCH05, Bur00, DFH01, DFPST07, Fin03, GU01, HHS00, Hsu05b, KLY03, LK05a, Ler02, LCS09, MY01, Poh01, PB01, Pre07, SVF07, TIS07, YW08, An03a, BJD02, CL04d, CCK04b, Che00, Gro03, HLO5b, Ku04, KC05, LHY02, S04, SC01, YW04]. CardS4 [GN01]. Care [Mad00, RC06, An03a]. care fully [Cha00b]. Carlo [BI09, Sug03]. cars [LPW06]. Cartilage [MYC01]. Cartography [SGM09, SW05]. Cascade [DGH04]. Cascaded [Jou04]. Case [ABK00, An05a, BBGM08, BU02, BCP01, CNS02, GOS7a, NC02b, OST05, Vau01, BKN04, BF06a, BK05, CS08, HRS08, KWD06, Mic02a, Mic02b, OST06, Pe09, ST07, SKW07, SPH06, ZWW01]. case/average [Mic02b]. cases [ABHS09].
Chosen [BCHK07, CKN03, CHJ +01a, CHJ +01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JKS02, JJ00b, KS00a, KY01a, KCJ +01, KMZ03, KM01c, Ki01a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH +09, KG09].

Chosen-Ciphertext [BCHK07, CKN03, CHJ +01a, CHJ +01b, Des00b, DK05, FP01, JKS02, JJ00b, KCJ +01, KMZ03, Nov01, PV06b, Poi00, CHH +09, KG09].

Chosen-Plaintext [DN02a, KM01c, Ki01a].

CHW [CHC04]. CIA [Mah04, Ris06]. Cincinnati [BD08]. Cinematic [CAC03]. Cipher [AIK +01, BKR00, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DPS05, DF07, Dwo03, EYCP00, FF01a, Flu02a, GG05a, GBM02, HCJ02, HQ01, KYHC01, KHD01, LKHL09, MSNH07, VP01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SY01, SBEW01, SK101, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BVP +04, GPX08, HAU04, Hey03, KH08, Kid00, LH08, Mac00, PSP +08, RBB03, Sal00b, SHH07, WW08, Win05b, WF02, XH05].

Ciphers [AAG +00, BBKN01, BS00b, BR01, BKM07, CVTMH01, Can01b, CF01b, Can06b, CJS01, Ch01a, CHJ02, CP02, CM03, Cou03, DPV01, Eq05, Fil00, F010a, Fil02, Gol01d, HR00, HR04a, HSH +01, Jam00, Jan06, Kan01, KC01a, KPG01, LRW02, MV00, Oni01, PP06a, Pl01, RMS05, Sar02, SM03b, SKU +00, Wall00, Wr05, ??02, YG01b, ZC00, Bai08, Bar06a, Bel07a, Ber07, Bod99, DLP +09, DY01, Dum06, DK08, Egh00, GPC06, HW03a, HWR09, Hey03, J010b, Jun05, Kat05a, KSH00, Kin01, LMSV07, LDH06, Lun09, Max06, Mi09, MW001, Pin06, SHJR04, Smi01b, SL07, SB05, TT00, Wag03, Yi01, You06, Kat05b].

Ciphertext [BBK03a, BCHK07, CKN03, CF01b, CS07c, CHJ +01a, CHJ +01b, CS02, CS03b, Des00b, DK05, FP01, JKS02, JJ00b, KS00a, KY01a, KCJ +01, KMZ03, Kur01, Man01, Nov01, PV06b, Sho00b, BMW05, CHH +09, IM06, KG09, Poi00].

Ciphertext-Only [BBK03a].

Ciphertexts [AFI06, BGW05, BGN05, Gen04b, J00a].

Circuit [EHK +03, GSS08, HR05, MG08, KS05b].

Circuits [BI05a, FML +03, Gol03, ISW03, MD05, PBTW07, Y01, GLC +04].

Circumvention [Kha05].

Cirencester [Hon01, Pat03b, Sm05].

CIRM [PPV96].

CISC [FLY06].

Citizens [An03a].

Clean [DS00].

Cleaning [L04].

Class [Car02, KM01a, KKH03, NN06, OP01a, Pl01, SBZ02, DKL00b, Fox00, HM00, Uni01].

Classes [CY02, RSA00c].

Classical [BYJK08, Gav08, GW00, LW05b, NA07, BYJK04, J09].

Classification [HMS04, PD00, Uni01].

Classical [RSA09a].

Cleaner [TR09a, TR09b].

Cleaning [Lut03].

Client [ARNS01, An01e, ANL01, FSSF01, PS05, WKB08, Bad07, HT08, LF03, YS04].

Client-Server [ARNS01, PS05].

Client-to-client [HT08].

Clients [JRFH01, RKZD02].

Clinton [Gen00a].

Clip [FG02].

Cliques [PQ06].

Cliques-type [PQ06].

Clock [Pan02].

Closed [CGFSH09, MH04].

Closing [DM07b].

Cloud [CS09].

Clouds [GS01, VS01].

Cluster [Hof01, KCD07, SEF +06, TLC06, TW07].

Cluster-Based [KCD07].

Clusters [MFS +09].

CM [CMK00, GHK +06].

CMS [BWBL02, DUK05].

Co [Bud00b, Nd05, ACM01b].

Co-Design [Nd05].

Coalition [ACJT00].

Coalition-Resistant [ACJT00].

Coarse [Rhi03].

Coast [Boy01].

Cod [IEE05b].

Code [Ar05, BK00, BR04, CD00b, CV03, Cer04b, FIP02a, FF01b, HSZ01, I0r03, KY01e, Lai08, OS09, Ree01, Rey01, Sal00a,
Sin02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MMJ05, RSA09a, SM00c, SM05, SM07a, Sin99, Sin00, Swe08, AAG+00, SE01].

Code-based [BR04, OS09, BGB09].

Codebook [CTH08, YWWS09, WJP07].

Codebook-linked [YWWS09].

Codebreaker [Hau03, Pin06].

Codebreakers [Bec02, Gan01b, Gas01, HS01a, Kah67a, Kah67b, Kah74, Kah96].

Codebreaking [Bud00a, Bud02, Cop05, Cop06].

Codec [Che08a].

Codecs [LLRW07].

Coded [MLC01].

Codes [Bee05, BP06, Big08, Bod99, BQR01, CC09, Chu02, CDG+05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ??02, YYD001, Yek07, Bel07a, aSM01, Bu09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HWR09, Kov01, Lam07, Luen09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02].

Codeword [AJ08].

Coding [Buc00a, CS05c, HHL+00, Joy00, LLL+01, MZ02, Pat03b, RK06, Sal05c, Sm05, TW02, TW06b, Ytr06, Che07, DW05, Gar04, Hon01, PPV96, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sea05, Sea09, TW05, Iwu03].

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].

Collaborative [LLY06].

Collection [GMM08, Bro05a].

Collections [Kuh00].

Collective [BBB+02].

Collision [DG02, IK005, MS09c, WYY05a, WYY05d, GM00a, Sem00].

Collision-Resistant [IK005].

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

Collusion [BGW05, HNLI02, Zan01].

Cologne [WK03].

Color [CTL04, Che07, Che08a, CTY09, FGD01, AEE05, 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, Gur02, GHTP05, GB09].

Combinatorial [GMW05, SLTB+06, Hen06a].

Combinatorics [Lee03b, Combined [LLS05a].

Combiner [Sar02, LL06].

Combiners [AK03].

Combining [Abe04].

Comes [Mar08b, An03c].

Coming [Dan01].

Commemoration [BZ02].

Comment [SCS05b, W05, WLY04].

Comments [AS01c, CGH+00b, JW01, MNFG02, SKW+00, CJT04].

Commerce [CLK01b, GS02a, Kir01a, Sta00, Uni01, ZYM05, BM03a, FB01, Gra01, MY01, SN07, YM09a].

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+09, LLS+09, Mar07, NA07, PL01, Sch06b, SKR02, Wri05, vDW04, BYJK04, BC05b, CC05c, CGP03, EY09, GKK+07, GG05b, GC05, HYS03, JZ09, JRS09, KPS02, LPM05, Lin02, MP08, PBMB01, Par04, RH03, SNW01, U05, WWA01].

Communication-Efficient [Fis05, LLS+09].

Communications [GN06, HJ07, Ig02, Kra01, Lan00a, Lan04b, LCK01, Loll, MS05b, Sal01b, Vau05b, VMC02, BP03a,
Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSKC01, Kei02, LHS05, RS08, Sal07, SDFH00, WWL+02, WC03, FS08, Gar04, La00, LJ05a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Compression-Encryption-Hiding [BD03].

Compromise [Ahm08, Lai08].

Compromised [ZYN08].

computability [Pet08].

Computable [Vad03].

Computation [ACS02, Bai01b, BCL+05b, BI05a, BIMO0, BJLS02, CC00, CDM00, CDN01, CDG+05, CDI05, DN03, DI05, DM00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, Jef08, KO04, KLML05, KSR02, Lin01b, PS05, WW05, An002g, AB09, BEZ00, BEZ01, CLOS02, CLC08, CDD00, DwWinW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WLHH05, WY05, SM07b, Duw03].

computation-efficient [CLC08].

Computational [CCL09, DLP+09, GH02, HG03, KLR09, KK06, Rup09, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WLHH05, WY05, SM07b, Duw03].

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

Compute [MFS+09]. Computed [FBW01].

Computer [BS03, Bis03b, Bro05a, BCDH09, BC01, CSW+08, CZK05, CGK+02, Coc02a, Coc03, HYZ05b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Ifr00, JBR05, KM07, Leh06, Lut02, MYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Tyn05, Cas02, DFGH04, Fan09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Shu06, SL06, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coc03].

computerized [LMC+03, Pau02b].

Computers [Coc03, Ett02, TSS+03, Cop05,
Computing

[ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBKD00, CGH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Lu03, May04, PFM03, Sch06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Wro00, Yan00, YKMB08, Cha07, Che05b, CHTD02, DHL06, HV09, HKPR05, LMC+03, Mi09, PP03, PP07, Raj06, RP00, Sei05, Wil99, YLR05, Lu03].

Computware [Ano02d].

conceal [BB79].

Concealing [DMS00].

Concealment [DA03].

Concept [ARC+01], concepts [AB09, Kra07, SWR05, MC04], concerning [HW03b].

Concerns [MP00], concrete [KNS05].

Concrete [KNS05].

Concurrency [JL00].

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

Conditional [LMV05, WN02].

Conditions [IK05], Conference

[ACM03a, ACM04a, Ano06b, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bih03, Bla03, Bon03, Boy01, Buc00a, CCO04a, CV04, CGP03, CGH00b, Cra05a, DKU05, DFCW00, DFPS06, EBC+00, ELvS01, FLY06, Fra01, FMA02, Fra04, FLA+03, HR06, HY05b, IEE09a, IKY05, JY04, JM03, Joy03b, Jue04, KJR05, Kij01a, Kim02, KN03, Knu02, Lai03, Lee04b, LIM+04, LL04c, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Nae01, Nao04, Oka00, Oka04, Pat03b, Pen01b, Phu01, Pio06, Pre00, Pre02c, RD01, Roy00a, Roy05, Sho05a, Shi01, SM07b, Sma05, Syv02, USE00c, USE00a, USE01b, USE01a, USE02c, Wil99, Won01, Wro03, Yun02a, YDK06, Z04, Zhe02b, ZHY03, AUW01, BC05b, DV05, DWML05, DRS05, Ha01, Kil05, Li05, PC05a, PY05, PPV06, QS00, Son00, WK06].

Confidences [Gan01a].

Confidentiality

[Dwo03, Pen01a, YC08]. configurable

[MBS04].

Configuration [Sha02, Mos06].

Confirmation [SK00].

Confrimer

[CM00, GM03].

Confiscation [DBS01].

Conformance [LBR00, RSA00c].

confounded [Bel07a].

confusion [She01].

congestion [SBB05].

Congress

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

congruences [Ste08].

Congruential

[CS05b, LS05a, SB05].

conic

[LCC05, LCZ05a].

Conjecture [CU01].

Conjugacy [CJ03a].

Conjugate [Igl02].

Connected [BJLS02, HS01].

Connection

[HR00, Jam00, Goo00, Mic02b].

Connection-Polynomials [Jam00].

Connections [WRW02].

Conquer [SKQ01].

conscious [DMSW09].

Consensus

[CNV06].

Considerations

[DBS+06, Hei07, Rub01, Sch07, SVEG09].

Considering [WA07].

Consistency

[ABC+05, JEZ04].

consistent [RG06].

Constant

[App07, BI05a, CD01a, DPV04, DN02b, DT05, Lin01b, Sun00a, IKOS08].

Constant-Depth

[BI05a].

Constant-Round

[DPV04, DT05, Lin01b].

Constrained

[BCH+00, DBS+06, HS01b, MRL+02, Zhe02a, Has00, RAL07].

constraints

[CC05d, LPM05, SN04].

Construct

[CDMP05].

constructed

[Tsa05].

Constructible

[NNT05].

Constructing

[Des00b, Fis01b, Vad03, Wen03, JZCW05, NS01a, ZL05].

Construction

[BBKN01, BB00b, Car02, CMKT00, Lin03, Nie02c, SM00a, TNM00, YW08D, DW05, SC02c].

Constructions

[BS00a, BR00b, BRS02, GM05, GKT05, GM02c, Jou04, PR08, PZ02b, SNWX01, SM00b, GT00, GPV08, IK03, IK06, NR04, PR05, Reg03, Reg04, vDKST06].

constructive

[GGH+08].

consumption

[Mis08].

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]. Contest [Bar00b]. Context [DJLT01, FPS01, SN04]. continued [Lov01]. continued [Dan02]. Contra [Maih04]. contract [WK05]. Contrast [BDDS03, HKSO, HT06, KS03, CDFM05]. Contrast-optimal [HKSO]. Contrast-Sensitive [HT06]. Control [ABEL05, ANRS01, BW07, CGMM02, HC08, LY05, Sma03a, ZGLX05, BNP08, DFM04, DPT+02, JW06, KNS05, LKZ+04, MD04, MSP+08, PS04b, STY07, WC01b]. Control-flow [ABEL05]. Controlled [GVC+08, IMM01, AW05, AW08, LAPSO]. Controlling [HY03, MS03b, MS02d, WL05]. Controls [Har01a, Har01b]. conventional [CJ04, YW05, YRY05b]. Converging [Pot07]. Conversation [MK04]. conversations [VAVY09]. Conversion [CDI05, Kett06]. Conversions [Kio1b]. Convertible [Chi08b, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b]. Convolution [PG05]. cookbook [VM03]. cookies [Cha05a]. Cool [Ano00d]. Coordinate [OS01]. COPACOBANA [GK+N08]. Copenhagen [TBJ02]. Copley [USE01b, USE01a]. coprocessing [ML05]. Coprocessor [Gut00, It00, LS01b, OTIT01, AV04]. Coprocessors [Sm02]. Copy [LTM+00]. copying [SV08a]. Copyright [Kha05, LLL02, PBB02, XFZ01, ZTP05, Gil07, Kwo03a]. CORBA [TEM+01]. Core [BF00a, Din07, DV08, HMS04, TPS01]. Corfu [SM07b]. Corner [Mar08a, TR09a, TR09b]. corners [Bha09]. Corporate [HW01, KH03]. Correcting [MZ02, NN06, YYDO01, ZYR01]. Correction [BQR01, CTBA+01, Din05, LN08, LW05b, MPSW05, SKQ01, TEM+01, Gar04]. Correctness [PBD05, Bel07b, HSD+05, dH08]. Correlated [FWW04]. Correlation [BSC01b, CJS01, Gol01c, JJ00d, LV04, LMV05, MH04, Nyb01, SY01a, WRW02, ZC00, GG05, JJ02]. Correlations [KM00, KM01b]. corruption [XNK+05]. COS [FF01a, WB02]. Cost [CDF01, FBW01, PD07, Sta05, YEP+06, CL09, SHJR04, YLR05]. Cost-Effective [PD07]. cost-ineffectiveness [YLR05]. could [Cl00b, Pan02b]. Counter [DIS02, QS01, SLG+05, SLO6, MMJ05]. Counter-Measures [QS01]. Countering [PP06b, SK05b]. Countermeasure [ITT03, MMMT09, OT03a, PKBD01, YKLM02a]. Countermeasures [Ava03, Fry00, GM00b, MOP06, OST05, Has01b, JDJ01, Man08, OST06]. Counters [KMO01]. counterterrorism [Na05]. Counting [Gaut02, Kuh00, Hig08]. Couple [SYX01]. coupled [LF03]. course [AA04b, GV09, GL05]. courses [Gha07]. Cover [GA05, Gut02a, LNP02, NN03, RS00]. coverage [DS00]. coverings [SC02]. Covert [Col03]. Cozents [Sal03b]. CPCMS [Sha02]. CPI [ECG+07]. CPN [AADK05]. CPOL [BZP05]. CPUs [ESC+05]. Crack [Sin02, Ano08b]. Crackberries [Sta05]. Cracked [AAG+00, Nic01, Pri00]. Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZL01, BZ03, Cur05]. Crackproof [Sal03b]. Cracks [Bar00a, Ste05c]. Cramer [Luc02b, VMS05]. CRC [Kat05b, Spr03, Was08a, SGP08]. Creation [MV01, Top02, MB08]. Creator [Coc01a]. Credentials [CL02a, CL04a, LLW05, LLW09]. Credit [CNB+02]. Crete [ACM01a]. crime [Cas02, KB00, Lauer08b]. criminals [Win05c]. Criteria [Can01b, IBM00]. criterion [QP05]. Critical [LKM+05]. SE09, CS07a, Gor05]. cron [Oue05]. Cropping [SDFH00]. Cross
[Bau02b, SM08, LCX08, SLP07].
cross-authentication [LCX08].
Cross-disciplinary [SM08]. cross-layer [SLP07]. Cross-Platform [Bau02b]. crowd [Fox00]. CRT [FMP03, Kuh02a, May02].

CROSS-EXponent [May02]. crypt [Per03].
Cryp
tanalyses [Kan01, SKU00].

Cryptanalysis
[ASK07, AMRP00, And03, Ano07b, Ano07a, BDG+01, Bau04, BLH06, BP03a, BBK03a, Bar06a, BP01a, BD00a, Bih00, BMFR02, BDK02a, BDK02b, BSW01, BDD03, BD00b, BCCN01, CGFSG09, CV02, CC01, CL01b, CY05, CKY05, CKK+02, CWJT01, CJT03, Cho06, Cho08b, CHJ02, CP02, Cou04, CJS+02, DG00, DGP07a, DGP07b, DGP09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Fin06, Flu02a, Flu02b, Flu01, Fur02a, Fur02b, GS07a, GM02a, GJS01, GS02c, GM02b, GM00b, GB02, GC00b, Gra02a, GS09, GKN+08, HPC02, HQR01, HAuR04, Hen06a, HLL+01, HSM+02, HHK+04, Hsu05a, HL00, Hwa00, JK02a, J00c, J01, JnBdXgXm05, Jou09, Joy03a, KM02, KW03, KS00b, KRY05, CK02, KRS+02, KKS00b, Kra02a, KC05, Kuh01, Kuh02b, KHKK05, LC03, LHL+02, LP03, Lee03c, LKY04, LL05a, LR07, LBGZ01, LBGZ02, LLH04].

Cryptanalysis
[LL05c, LLCL08, LW05c, MS03a, May02, MG01, AADK05, AL00a, Ano09b, ADH+07, Ase02, BLST01, BDF+01a, Bar00a, BGK+03, Bli03, Bla01a, Bor01, BD02, Bra01b, BM01c, BL08, Bur06, CCC04a, Coo01b, Car02, CDP01, CHL02, CKY07, CB01, CRA05a, CS09, CO09, DD02, DHMR07, DFM04, DS00, DWN01, DHR00, DV08, DFG01, FIP01b, FS00, Fis01a, FGM00a, Fri01, GMP01a, Gar05, GSS08, GGKT05, G02, GTH02, Gor02a, GL00, GU01, Gut00, Gut02b, Gut04a, HTS02, HN06, Har06, Has01a, HLA05a, Hoc08, Igl02, YIV00, It01, IMM01, J05, K001, KY01b, KY02b, K101b, K306a, K309b, Knu02, K101b, K001, KS06a, KLJ01, M02a, MOP06, Mea01, MNP01, MRL+02, MHL02, Mor03, MK05b, MS05, NIS01a, NIS01b, Nao03, Nd05, Ngu05, Nie04, OTT01, OP01a,
PKBD01, PR08, PZDH09, Pem01b, Pf01]

Cryptographic
[Pin02, Pin03, PS02b, Pot06, Pre00, Pre02a, Pre02b, RSA00d, RSA01, RR00, RRS06, Rot01, RSN+01, SM00a, SS01a, SG09, Sha02, Shp03, Sf02, SFDF06, SR06, SL09, TLYL04, TWNA08, TBLD01, Uzu04, WK03, WN02, WBL01, WC01b, You01, Zha08, AMRP04, ASTZ05, ALV02, AV04, BGB09, BDSV08, Bla01b, BP05, BG08, BG09, BDNN02, BD04a, BGL03, BMV06, BR05, Can01a, Can06a, CHC04, Coh03, CC05d, CDL06, DP04, Dug04, DFG00, FS03a, FSGV01, GT00, GPV08, GJ04, GM04, GB09, HY03, IK03, IK06, IYK02, IYK03, JW01, KAM08, KSF00, KS05b, KP03, LMTV05, Lau05, LW09, ML05, Mea04, MT07, Mic02b, MR06, Mon03, NdM04, ND06, PS04a, PSM+09, PR05, Pre07, Pri00, Puc06, QPV05, Reg03, Reg04, Ren09, RHM04, RBF08].

cryptographic [RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, kWpLwW01, WLW04, XLMS06, YLT06, ZLX09, ZW0101, ZL04b, dH08, BWBL02, JQ04, KKP02, KP01, KNP01, RS05].

Cryptographically [ADD09, AHS08, BJ02, BFCZ08, BB00b, FR08, MS02b, RGX06, Aam03, AW05, AW08, Lau08a, SM03a].

Cryptographically-masked [AHS08].

CryptoGraphics [CK06]. cryptographic [RSA08a]. Cryptographie [RSA08b].

[ANS05, AF04b, AD09, AA04b, Ano00c, Ano01, Ano02b, Ano02f, Ano02h, Ano04a, Ano05a, Ano07b, Ano07a, AA0G01, AIK04, AIK06, App07, AEAO05, ABM00, Bai01a, Bai01b, BINF03, BDZ04, BOV07, BBGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BW02, Bla02b, BDDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, BK006b, BKM07, Buc00b, BD08, BP01b, BRTM09, CPS07, Cer04b, CCL09, CSW+08, CQS01, CPD06, Cob04, CFA+06, Cop00, Cor06, Dr.00c, Dan07, DFSS08, DFSS05, DD00, DFGH04, DK02, DK07, Des02, DT03, DY09b, DSS01, DNN00, DNN03, Dre00, DP08, EPP+07, EP05, E1109, E1104, ECG+07, Ett02, FS03b, Gal01, Gal02, GHK+06, GKK+09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Grio1, Grio5, HR06, HH04, HMI01].

Cryptography
[HM04, HSS01, HPS08, Hon01, IEE00b, IXY05, Irw03, IK06, IK08, JI00, JI01b, JI01a, Jue04, Kak06, KLR09, KZ07, KG07, Kat05b, KK06, KBM09, KPM02, KWB06, KY01c, Kiri01a, KMS02, KM05, KS02, KS03, KW06, Lam01, LG01, LSY01, Lee03b, LLL+01, Lie05, LDM04, LW05b, LP02b, Lut03, Ly08, MNT+00, MP02, MA01, MA04, MZ04, MA01, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Murl01, 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, Sti95, Sti01, Sti02, Sti06c, SJ05, Syv02, TSO00, TW06a, TG04, TW02, TW06b, Tro08, TR09a, TR09b, Uni01, USS02, VY01].

Cryptographic
[VMC02, WPS01, Wei04, WK01, We05, Wie00, WvD02, Wri00, YW08, Yt06, YC01, YDM06, ZY03, vD04, Im03, AM07, AUW01, Ano02a, Ano02g, ABD01, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BEZ00, BEZ01, BGM04, BEM+07, Buc00a, Buc01, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CCT08, CDFM05, CDD07, Cos00, Cre00, D04, Di01, DCM08, Dw02, DOP05, DKL09, DW09, Duw03, Eke02, FX04, FP09, Fra01, FP00, GV09, GL05, GKK+07, Geb04, GRTZ02, Gol99, GG05b, GH05, GPS05, GNP05, HH05, HHL+00, HKP05, HAI00, Hig08, HKS00, Hoo05, HG05b, HLW09, ...]
IZ00, IM06, JK01b, Jan08b, Joy00, KZ03, KL08, Kat01, Ki05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Lop06, Mau04, May01, McA08, MBS04, MM07a, Mol07, cryptography [NP02a, Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00, Pin06, Reg05, Reg09, Rot02b, Rot03, Roy00b, Rup09, STY07, SBZ04, Ser06, SH05, Shp99, Sil09, Sin00, Smo04, ST01d, SK01b, TW05, UHA+09, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wri03, YY04, YC07, vT05, For04, HCO2, Kat05b, Pat03b, Sil01, Smo05, Bee05, Lee03a, Ree01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08], cryptography-based [FXAM04].

Cryptologic [BS00a]. Cryptological [Lew00]. Cryptologie [dL00]. Cryptologists [WD01b]. Cryptology [Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Lu03, LL04c, Lu02, MMV06, Neu04, NS01c, Ngu01, Oka04, Po06, Rot05, RS02, Sha03b, Zhe02b, dL00, Ban00, Ban02a, Bau07, Bel00, Bhi03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kii01a, Kim02, Lam01, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, PC05a, Pi01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sh05a, Son00, Won01, WK06, Yun02a, vT00, DWML05].

CryptoManiac [WWA01]. Crypton [ACK+02, MG01]. Cryptosystem [BST02, FL06, GG01, GK05, GHW01, Hug02, KM01a, KY02c, KLC+00, LHT09, dVP06, Luc02b, NSN05, NB01, Ove06, PH+01, YG01a, YG01c, Zhe02a, Zhe06, Bao04, CL02b, CCH04, Che05a, Cho06, CFVZ06, CH01, Dan02, DHI06, EKRAM01, GHGSS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04b, LL06, LKYL00, Lo00, LS01c, OP01b, Pa03, Po00, SPG02, SCS05a, SP79, SLC05, Sun00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, hY08].

Cryptosystems [Aki09, Ava03, BDG+01, BKL02, BPS00, BMM00, CHS02, CCW02, DD+06, DXX02, ESG+05, FJ03, Fe06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KKY02, KI01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWG03, ST02a, SQA01, SKG01, Ste01, Vad03, Wya02, XBO1, ZLK02, Ban05, BF06a, BB79, CH01, CMKT00, EBS01, EHK04, GH08, GBKP01, HM00, Has00, Has01b, Hbi00, HP01, KW00, Kos01c, LD01, Luk01, Mic01, Mis06, OS06, Pe09, PLJ05b, SSST06, Sh05a, Sm01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WV00, YY00, ZS01, vT01], cryptovirology [YY04]. CRYPTREC [IY00]. CSCW [ZP05]. CT [Joy03b, Men05, Nac01, Oka04, Po06, Pre02c, ZC09]. CT-RSA [Joy03b, Men05, Nac01, Oka04, Po06, Pre02c, ZC09]. CTO [Ano03e]. CTS [Con00]. Cuban [AJ08]. Cube [DS08, PDM09]. Cube-Type [PDM09].

culture [Gil07]. Cumulative [WP03]. cure [RD09]. cure-all [RD09]. Current [DFH01,PRS04,LPW06]. curriculum [FO06]. Curve [ANS05, ADI09, AN005a, Avo03, BIN03, Bar00a, BGM08, BM00, BWBL02, BS01d, BM01, CS01, CFA+06, GPP08, HYZ05a, HMM04, HM02c, JT01b, JT01a, KMB09, KMF02, KSS02, KWP06, LW02, Mö01, Kir03, OT01, OS01, PWG03, Pe06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XBO1, YYZ01, ZLK02, BSS04, BSS05, BGM4, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHK04, GBKP01, Has01b, Has05a, HL05a, JW06, LL04b, Mis06, OS00, ST02a, SSST06, SH05, Sm01, SCL05, SLC05, TC05, Ver01, Wol04, WPP05, YC09a, ZS01, ZL05, vT01].

Curve-Based [KWP06, Pe06]. Curves [AHHR08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK+06, Kid02, PWG03, Ver02, CMKT00, Hus04, LWZH05, MP01b,
MSV04, Sil05, Sim02, SC02b, Was08b, Wen03, Yas08]. customer [Lin01a]. CVS [DFG01]. Cyber [FNRC05, WW04, Mau05]. Cyberinsurance [BP07], Cybersecurity [PLW07], cyberspace [Mit02], cycles [ABHS09, BPS08]. 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, BS00b, BNPW03, Bro05b, Che01a, CTLLO1, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, Küs02, Lan00b, LLRW07, LP00, LHSM06, LS08, Lut03, MND+04, MS03b, MFS+09, NM09, OS05, Per05, RKZD02, RK06, Sal03a, Sal07, Sin01a, SDMN06, TZZD05, TCPPM07, VKKP05, WS05, WY02, WY02, kc01, VW01, AG09, AHK03b, AKSX04, Ano02c, Arn01, Bha00, BNP08, CCMT09, Cer04a, CLRO9, CPG+04, DZL01, DGMS03, FS04, HILM02, LLK05, MJ03, Mal06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGPH08, SETB08, WMDR08, YLC+09, YC08, ZSJV07, Zir07, Cur05, DK08, Lin02, PAP05]. Data-Hiding [VKKP05]. data/image [Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, B05a, BBPV00, KS02, SVEG09, Ga02, HILM02, Mau04, PS08b, PBV01]. database-service-provider [HILM02]. Databases [AK02b, CDM+05, DN04, AHK03a, CDD+05, CKY07, GA03, MS009, MNT06, NS05b, ÜG08, YPPK09].

Datamining [DN04]. Datenverschlüsselung [Lin02]. David [Gas01, PAP05, Bar05, EAG05]. Day [SE01, CSW05, Win05c]. Days [Adl03, Riv03, Smo04]. DC [USE01c]. DCT [BSC01a, BSC01b, CH01b, KT00, LY07, LSC03]. DCT-Based [LY07, LSC03]. DDH [Lys02]. DDO [LKH+08]. DDO-64 [LKH+08]. Dead [Gut02a]. deaf [Pau02b]. Dealer [DK01, Sun00a]. Dealing [BH00a]. Debate [Jol01, Mad00]. Debian [YRS+09, Ahm08]. Deblur [VHP01]. Debugger [Ano02d]. Debugging [Ano02d]. Dec [IEE09a]. decades [Luv01]. decades-old [Luv01]. December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, Lai03, Lee04b, LLT+04, LI05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b].

Decentralized [MSP+08]. deception [CS07a, Mah04, MS02d]. Decidability [Küs02]. Deciding [Bau05]. Decimal [BJvdB02]. Decimation [Bau05]. Decipherable [AS01, Sav04]. Deciphering [Eri02, KB07, Ark05, Luv01, NS01a]. Decision [DJ06, GR04, KM04a].

Decisional [CU01]. Decisions [Coc02a, Sch07]. Decodable [Yek07]. Decoding [KY02b, LBZL01, LBZL02, Rai00, AGKS07, Bul09]. decomposing [FP09]. Decomposition [BR09, CL04c, SC02c]. decompositions [vDkST06]. Decorrelation [CLL00, Vau01]. decrypt [Bih02].

Decrypt [Bau00, Bau02a, Bau07, MB01]. Decryption [Bau00b, BST02, CS03a, CDD07, FSP01, HGN+03, Int00, KCJ+01, Ano08a, DZL01, GH08, MI03, OS07, Shp04b, SWH+09, WH09]. Decryptor [TPS01, Zol01]. DeCSS [Coc02a]. Dedicated [ISO04]. Deep [CMS08].

Defeating [CSK+08]. Defective [BTTF02, Dav01b, Dav01c, KLR09]. Defending [NRR00, Pro01]. Defense [GK02, HW01, Mir05, Wy05, Bol02]. defenses [SL06]. defined [Yas08].

Definition [YWD08, SN100]. Definitions
[Uni01, AH05]. **Definitive**  
[BS01a, BSHb05, Gar03b]. \textit{defying} [HRS08].  
**Degenerate** [Ber09a]. **Degradation**  
[BSC01a]. **Degree** [CV02, QPV05].  
**Degrees** [Sat06]. **Déjà** [DP00]. **DeKaRT** [Gol03]. **Dekker** [Irw03].  
**Delacorte** [Imr03]. **Delay** [WRW02, NS01a]. **Delayed** [JM07].  
**delegated** [CL04c]. **Delegation** [WN02, ZP05].  
**Delhi** [JM03, RM04]. **Delivers** [Ano02e]. **Delivery** [NZCG05, RMCG01, DY09a, NZS05].  
**Delphi** [TEM +01, Hei01]. **Demand** [BD03, CMB +04, SEF +06].  
**Democracies** [CZB +01]. **Democracy** [CTBA +01]. **Demography** [Coc03]. **Demons** [Mos06].  
**demonstrably** [HL06]. **demystifying** [RR04]. **Deniability** [Pas03]. **Deniable** [Nab02, CCK04a, CSK +08, DG05, LCO5b, YRY05c, Zha06].  
**Denial** [Mah04, Nik02a, Nik02b, PKBD01, Ri02, Mif05]. **Denial-of-Service** [Nik02a, PKBD01].  
**Denmark** [Cra05a, TBJ02]. **Denver** [ACM01b, Sch04b, USE00d].  
**Dependable** [NAG03, And08]. **Dependent** [Gol03, WS05, BPS05].  
**deployed** [BDET00]. **Deploying** [BH00b, GSB +04]. **Deployment** [CL07, KDO01, Mro01, App05, JRR09].  
**Dept** [Uni01]. **Depth** [Bil05a]. **Derandomization** [BOV03, BOV07]. **Derivation** [DGH +04].  
**Deriving** [BJP02, CSW05]. **DES-encrypted** [Bih02]. **DES-like** [Egh00, EBS01].  
**Desch** [LBA00]. **Describing** [PS06]. **Description** [Lav06, MH05]. **Descriptors** [DPN07, SP04].  
**Design** [Abd01, AADK05, Ano02e, ADD09, AIK +01, ARC +01, Bar00b, Can01b, CDDP01, Cim02, CB01, CS03b, CMB +05, CLZ02, DR02a, DR02b, DF07, EHK +03, FF01a, FZH05, GSS08, Geb04, Gut02b, Gut04a, HRL09, Hro05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04b, LB05, MKP09, MP00, Nd05, NSS02, Rhi03, SJ09, SPG02, SRQL03, Uzu04, WZ05, WW08, WLLL09, ARJ08, CMS08, GG05b, Gut04c, HC04a, Hut01, KSF00, MI09, MWM01, SVEG09, YCW +08, YC08].  
**Design/CPN** [AADK05]. **designated** [LV07]. **Designing** [HBC +08, TCR03, C +02, CG05, Lan00c]. **Designs** [Bec05, CC02a, Bai08, Des00a, WL07a].  
**Desktop** [Mro08, BDET00]. **Desmedt** [CHH +09]. **Desynchronization** [CDTT05].  
**Detached** [Sha01c]. **Detailed** [Lut03]. **Details** [Scr01]. **Detect** [FOBH05]. **Detecting** [CMS09, GFD01, JQYY01, Har07a, LHL04]. **Detection** [AS01b, AD07, BB00a, BKM07, CH01b, CJK05, JT05, KKK03, SKQ01, SY01a, SLT01, ST01c, TZZD05, TMM05, WG05, YI01, Zan01, Bej06, BBK +03b, HLL +02, Men03, NNO2, WMS08, YW06, ZGT05]. **Detection/Correction** [SKQ01]. **Detector** [BSC01b, DNP07]. **Determined** [KHH03]. **Determining** [KS03, LQ08, OS07]. **Deterministic** [BK06a, Her06, KZ03, KZ07, May04, BK07]. dev [BH05]. **Developers** [Ano06c, Dew08, MK05b, Nis03a]. **Developing** [MV03b, Cra05b, Gal02, HL06]. **Development** [Ano02e, CMB +02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a]. **Developments** [Ano03e, Pre07, Sha04a]. **develops** [Pau02b]. **Deviates** [Ran55, Ran01]. **Device** [Ric07, ST03b, WPS01]. **Devices** [BCH +00, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KHD01, MV01, MRL +02, SCF01, WCO01, Ano06a, CMS08, DMT07, Tse07, ZYW07]. Devill [Bla01c]. **DFT** [Che08a]. DH [Lys02]. **DHIES** [ABR01]. **DHP** [MSV04]. **Diablerets** [Vau05a]. **Diagnosis** [Ano04a, BK06b, XNK +05]. **Diagnostics** [NM09]. **Diagonal** [PJH01, PJK01]. Dickson [SZP02]. **Dictionaries** [AGT01].
Dictionary [BPR00, BCP02b, CS07b, DJ06, Pho01, NS05a]. did [MH09]. Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b]. Dies [Bar00a, Coc01a]. difference [PBMB01, dW02]. Different [LS08, WWTH08].

Dies [Bar00a, Coc01a].

Dierence [PBMB01, dW02]. Dierencing [LS08, WWTH08]. Dierent [CGMM02, dW02]. Dierential [Ava03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKL+03, Eke09, Fur02a, Gra02a, HLL+01, HSM+02, HHK+04, IIT03, JT01a, Kan01, KM02, KCP01, LHL03, MP06, MMT09, MHL+02, MG08, PSC+02, PQ03b, SK01a, SKU+00, SKI01, vW01, BF01a, CUS08, DLP+09, Egh00, EBS01, Pha04, SSL+00, TM01].

Dierential-Linear [BDK02a]. Dierentials [BF00b]. Dicult [Bud00b, MT02]. Dicult-to-pass [MT02].

Die [Jan08a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKRT08, FS01b, GR04, Kil01b, KK02, KM04a, Kra03, Kra05, Mis08, Tsa06, YRY05c].

Differenser [Fer06]. diffusing [She01]. digest [MSP09]. Digit [KWP06, Tan07a, BG09, HKP05, Kir01b].

Digital [ANS05, AvdH00, AR00, AS08, Ano1f, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Ca00b, CCH05, CC09, Che01b, CFS01, CM02, CMB+08, CZB+01, CGJ+02, DSP01, EIG01, Eng00, EH03, HSZ00, HSZ01, HS01b, HHGP+03, HW01, HLT05, JBR05, KZ01, Kal01, KO02, Kuh00, Kwo02, Kwo03b, LZX+01, LLL+01, Lin01a, LL01, Lut03, Mad00, MM01a, MM02, Meh01, PL01, PJH01, PCG01, PZL09, PBM+07, Ram01, Rd01, RSO1, Sam09, Sch00d, Sch06b, Sc01, Sha01c, SC02a, Shi08, SL01, Sug01, TJ03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03, WC04, Wya02, XFZ01, XYL09, YWWS09, YYDO01, YYZ01, ZWC02, Zho02, AAP07, AA08, Ano01, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CJO5, Che07, Die00, FB01, GGK03, Gil07, HRL09, HLH00, HHC05, KP00, Lev01].

digital [LLC06b, MKY08, NRR00, PC05b, PLJ05a, PBV08, QC05b, Sha01d, Sha04b, Sha05d, SCL05, TCC02, TEN+09, UP05, WNQ08, WHL03, XC05, XMST07, Ano09a, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].

Digital-Audio [WNY09].

Digital-Signature [Eng00]. Digits [Che04b, Ran55, Ran01]. Dimension [DDG+06, TZT09a, TZT09b]. Dimensionality [SBG02].

dimensions [CLR09]. Dining [KLN+06].

Diplomacy [Alv00]. Direct [BMW05, KG09].

directional [PJK01]. Directions [Sha01b, DFH01]. directly [JZCW05].

direct [BMW05, KG09].

disadvantage [CDS07].

Disappearance [Per05]. Disappearing [Way02b, Way09].

disappointed [Ste00].

Disaster [WC05].

disciplinary [SM08].

disclosure [JM07, Swi05].

Discovery [Bi09, HLL+02, SBG07, SGA07]. Discrete [CS03a, CNS02, Che04b, CCH05, Gen00b, GV05, GPP08, KC09b, LW02, LJ05, VK07, HN04, HW03a, HWR09, Hsu05a, HLO5d, JLO3, JLL01, LHL03a, LHY05, LTH05, PLJ05a, QC05a, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SLC05, SCS05c, Yas08].

discretized [MA02].

Discription [Har07b].

discursive [Mit02].

discussion [Kee05].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].

disjoint [Gut04c].
Distortions [HH09, SDF01]. Distributed
[BCS02, BT02, CLK01a, CS08b, CD01a,
DS03, EP05, FM02a, FS01a, GJKR03,
GSVC02, GTH02, LLY06, SCF01, WT02,
And08, AFGH06, BDET00, CO09, FMY02,
KKL09, LN04, LLW08a, MSP +08, P508a,
Ra06, WZB05, YbJ04]. Distribution
[BCS02, BT02, CLK01a, CS08b, CD01a,
DS03, EP05, FM02a, FS01a, GJKR03,
GSVC02, GTH02, LLY06, SCF01, WT02,
And08, AFGH06, BDET00, CO09, FMY02,
KKL09, LN04, LLW08a, MSP +08, P508a,
Ra06, WZB05, YbJ04]. Distribution
[BCS02, BT02, CLK01a, CS08b, CD01a,
DS03, EP05, FM02a, FS01a, GJKR03,
GSVC02, GTH02, LLY06, SCF01, WT02,
And08, AFGH06, BDET00, CO09, FMY02,
KKL09, LN04, LLW08a, MSP +08, P508a,
Ra06, WZB05, YbJ04]. Distribution
[BCS02, BT02, CLK01a, CS08b, CD01a,
DS03, EP05, FM02a, FS01a, GJKR03,
GSVC02, GTH02, LLY06, SCF01, WT02,
And08, AFGH06, BDET00, CO09, FMY02,
KKL09, LN04, LLW08a, MSP +08, P508a,
Ra06, WZB05, YbJ04].
[LV04]. **E2** [SKU+00]. Early
[ASW+01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Smo04, ZGTG05]. **Easier** [Pau09].
**Easy** [GR04, Hos06b]. Eavesdropping
[Kuh02a, Kec05]. **eBook**
[Ano02d, 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]. **ECP** [Che03]. ed [Gum04, Nis03a]. Edge
[Sta05]. Edinburgh [RS05, Pen01b]. Edit
[CGFSHG09]. editing [MAaTxx]. Edition
[Cho08a, Irv03, Spr03]. Editor
[MFS+09, Sak01, KP03, SK06]. Editorial
[Er01, Er02, FOP06]. Editors
[BK06b, PTP07, JT09, GKL08]. EDK
[Ano02e]. Eds [Duw03, Pag03]. Education
[Puz04, RC06, CAC03]. Effect [AEV+07].
**Effective** [CDR01, PD07, Sen03, SL06].
**Effects** [BBGM08, Har00, JG04, SN07].
**Efficiency** [II00, GGKT05, SLG+05, GT00, GKK03, KT06, YTH04]. **Efficient**
[ACS02, ABRW01, AEMR09, Bai01b, BINP03, BKL02, BR00a, BGHP02, BDSV08, BGK+03, BS00a, BF01c, BGH07, BBB00, BCD00, CKPS01, CL02a, CCMT09, CCD07, CL01b, CPhX04, CM05a, Chi08a, CJK05, CT05b, CKK03, Cou01, Dam00, DN03, Den03, FF00, Fis05, FS01c, GLV01, GC01b, GTH02, GST04,GBK01, HCJ02, HSZ01, Has01a, HS00, HV04, HZS05, HL07, Hii00, HS07, KOY01, KOY09, KLY02, K003, KH03, LSY01, LCK01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, MN04, NSK05, OS01, PCS03, PB05, Ram01, RSL03, RDJ+01, SM01, SM03a, SRL03, SNS00, TC05, WHL05, WYY05d, WHI01, WC01a, XB01, XS03, YWD08, YHL05, Zan01, Zho06, ÁCTZ05, AF05, Bli01b, CC04b, CC05c, CY05, CH05, CL08, DWE08, DWWM05, FP09, FSGV01, HHG06, HC04a, JW06].
**efficient** [KHYM08, LPV+09, LLS+09, LCK04, LLH04, LYC02, Mic02a, MSP09, NR04, PCC03, RG05, RBB03, SLP07, SKW+07, S205b, SC05a, WK05, X05, Yan02, YTW05, YC09a, ZSN05, ZYW07].
**Efficiently** [IKNP03, NNT05, AGKS07].
effect [Wei00], efforts [Pau02a]. Eggs
[Wei01, Wei05]. **EGPGV** [MFS+09]. Egypt
[EB+00, IM03, Sin00]. Eighth
[ACM06, B+02, ELV01, IEE01b]. Einstein
[MNT+00]. **EJB** [TEM+01]. Ekert
[Duw03]. El-Gamal [EKRA01]. Election
[JLL02, CA00b]. Elections [Cha04, PV01].
**Electromagnetic** [SGM09, Q501].
**Electronic** [Ble07, CL01b, CM02, Dur01, Hoo01, ISO05, IY00, KMO01, KS02, Lan04b, LLL02, Mad00, MNFG02, Rub01, RMC01, Str01a, YKMY01, ZYM05, AvdH00, AAKD09, Cal00a, EY09, FB01, HJW05].
**Element** [MS02d]. Elementary
[Sin09, Ste08, Tat05]. Elephant [Fer06].
**Eleven** [All03]. El-Gamal [BJN00, CL02b, CWH00, HL04, LHT09, SJ00].
**El-Gamal-like** [CWH00, HL04]. Elizabeth
[Bud06]. Elliptic
[ADI09, Ano05a, Bai01a, BINP03, Bar00a, BBGM08, BMM00, BS01d, BMN01, BB00b, CQ01, CQR+06, GLV01, Gau02, GP08, HY05a, HMM01, HM02c, HS04, JT01b, JT01a, KBBM09, KPM09, Kid02, KS02, LW02, MP01b, MIS02, Kir03, OTT01, SO01, OT03b, PWGP03, RSA03b, RS04, RS01, Sat06, S05, Was08a, Was08b, WPS01, XB01, YYY01, vT01, BSS04, BSS05, BM04, BG07a, CCBH04, CHe05a, CF06, DIM08, DwWM05, EH04, GBKN01, HS05a, HL05d, JW06, LL04b, LWZH05, MS06, MVS04, O05, S00, ST03a, STST06, SH05, Sim02, Sma01, SC02b, SCL05, SL05, TC05, Ver01, YC09a, Yas08, ZS01, ZL05, ANS05, BWBL02]. **Ellis** [Coc01a]. Elmau
[IEE01b]. Else
[FL01b]. **EMA** [QS01]. Email
[ES00b, Gart03a, Luc06]. Email-Based
[Gar03a]. emanations [ZZT05]. Embedded [Ano01c, Ano02d, Ano02e, BBGM08, Dri02, DV08, GSS08, JT05, JQ04, KKP02, LPW06, NdM04, RS05, SPGQ06, WK03, YSS+01, ARJ08, BGM04, Fox00, Geb04, KV04, N09, KP01, KNP01, KP03, MBS04, Nis03a, TQ07, Fin02]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, KCO9a, Wan05].
encryption [Sch01f, SR00, SVEG09, Shp04b, Ste00, SP03, SWH09, Tan01, TTZ01, TOEO00, TM01, TLH05, Uni00b, UP05, VKS09, WG02, Wei00, WN95, WH02a, XY04, Yan02, YGZ05, YZEE09, YC07, ZLG01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CHKO08, CHJ01a, RR04, Uni00f, Wue09, Jan08a].

decryption/cipher [HAuR04].

decryption/decryption [OS07].

Encryptor [LMP01, TPS01, Ano00a].

Encryptor/Decryptor [TPS01].

Encyclopedia [Bid03, vT05].

End [KCD07, Per03, SKKS00, WWGP00, YSR01, SU07].

End-to-End [YSR01].

Ended [Kus02].

Endomorphisms [GLV01].

Endpoint [Kad07].

Enemies [DM07b].

Energy [GC01b, Ino05, LPV09, SLP07, Mis08].

Energy-efficient [LPV09].

Energy-security [Ino05].

Enforcement [GN06].

enforces [BP05].

enforcing [GMM08, HRS08].

Engine [Fri01, MMH02, DP04, SLM07].

engineer [Pau02b, SN04].

Engineering [GM08, HRS08].

Enhanced [JKW01, ZGLX05, OP01b, TWL05, WHH05, ZSM05].

enhanced-security [OP01b].

Enhancement [CJ05, LSH03a, LSH03b, YW04].

enhancements [ADH07].

Enriching [BDK02a, MS05a, SE09, Sui00b, DY01].

enigma [Rob02, Rob09, BCB05, Cas06, Chu02, Cop04b, DB04, GO03, Goo00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Wil01a, Win05b, Win00].

Enigma [Kap05].

Enough [CNB02, Pat03a, YJ00].

Enrolment [WHH01].

Entangled [Bar00c, LB04].

Enterprise [BH00b, C+02, HM05, MJF07, App05, TCR03].

Entropic [DS05b].

Entropy [DS05b, EHMS00, LH07, JRS09].

Environment [BST03, DL07, HS01b, LSVS09, IM06, KKL09, KB00, Rh03, Whi09, ZBP05].

Environmental [PS05].

Environments [CJ+04, LKH09, BGM04, MNS08, SBB05, SBB07, SN04, YC09a, YbfJ04].

ephemeral [Mis08].

Ephemeralizer [Per05].

EPOC [JQY01].

ePOST [MPHD06].

ERP [Ina02b].

Equation [FJ03].

Equations [CP02, DDG06, GS03, PBMB01].

Equipping [DMT07].

Equitability [DBS01].

Erasure [BBK+03b, BQR01, Din05, KKG03, LW05b, LM02, MLC01, MPSW05, MZ02, NN06, SKQ01, Y101, YYDO01, ZYR01, Zo01, Gar04, LHL04, YW06].

Error-Correcting [NN06, ZYR01].

Error-Prone [MLC01].

Errors [AD07, AL07, Reg05, Reg09].

escape [Bhu09, Fur05].

Escrow [AK02a, An001a, CL01a, DBS01, LCK01, ATSVY00, CL02b, LCC05].

Escrowed [PS01b].

eServer [AV04].

eSORICS [dCdVSG05].

Espionage [Bud06].

Essays [MAaT07].

Essential [Cop04b, Dru00c, MR02a, MR02b].

Essentials [HHL+00, Irv03].

estimating [Kov03, KH03].

Establishment [BM03c, NIS03b, HMvdLM07, LF03, SL05a].

Estimation [EFY+05, JX05, KLb+02a, LNL+08, Sel00].

ethical [Har05b].

Euclidean [CPhX04, CMJP03, CLZ02, WL02].

EULA [WWL+02].

EUR [Eag05].

EUROCRYPT [Bih03, CC04a, CRA05a, Knu02, Pfi01, Pre00].
Factoring-Based [PV06b]. factorisation [GG08]. Factorization [CDL00, Lam91].

Facts [GO03]. Fade [CAC03]. Fail [JQYY01, SSNGS00]. Fail-stop [SSNGS00].

Failures [DFG01, GMM01, GPC08, HGG07, HR04a, JH04d, KKIM01, KK03, KKJ07, LSY01, LS05b, MSN07, Kir03, NS05a, NSSF02, OKE02, OT03b, PG05, RR02, Tsa06, UHA09, Yan05, ABB04, BMA00a, BMA00b, BMA00c, JAW00, JH04, Joh05, Mat04, RM04, Sch00b, Sch01h].

Faster [Bar00c, CMJP03, GLV01, KS09a, LV04, Oec03, Ban05, Why05].

Faster-Tolerant [WL07b, HGR07, Lin07, RMH04]. Faults [GSS08, VS08]. Favre [MFS09]. FBI [Mad04]. FC

[Bla03, Fra01, Jue04, PY05, Syv02, Wri03]. Fear [Sec04, Syv02, Sch03]. Feasibility [APV05, BDET00]. feasible [LM08].

Feature [GW01, Gut02a, HH09, LNP02, LLC06a, NN03]. Features [PK01, SBG02].

February [DR02c, Fra01, GH05, Joh03, Jue04, Kil05, Kim01, Men05, NF02a, Nao04, Ok04, PY05, Poi06, Pre02c, RM04, Syv02, USE02a, Wl09].

Federated [DeL07, GTY08]. Feedback [CGFSHC09, CM03, Cou03, Ig02, Hey03, SP02]. FeedForward [BP01a]. Feel [PM00]. Feeling [Bth06]. Feistel [Con04, Kan01, LMS07, Oni01, Pat04].

Feldman [AF04b]. Ferrer [CKN06]. Fatal [MYC01]. fetch [HTW07]. Fi [Sty04, Bar03]. Fiat [VS08]. fiction [An03e]. FIDES [ISTE08]. Field [FJ03, GC01a, RDJ01, CKY07, GMG00, Has00, JL03, ST03a].

Fields [Bai01a, BT02, CU01, Che04b, CQS01, CFS05, HCK09, HHM01, KKH03, Lov01, MNP01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sma01].

Fifth [ACM03b, SM07b]. Fighting [DGN03, SZ03]. File [CCDP01, GIS05, Ito01, LK01, BDET00, CSK08, HTW07, Hos06b, ISO05, MKKK00, MP06, SY05, WYY05b, ZT03, SW00b].

Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pett05]. Filesystems [WBL01].

Filter [LBGZ01, LBGZ02, MSN07, Sar02, CMS08]. Filter-Combiner [Sar02]. Filtered [MH04].

Filtering [SDFH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00].

Finalists [EYC00, IKM00, IK00, IK01, Mes00, Mes01, SKK00, SW00a, WWCC00].

Finally [Coc02b]. Financial [AN05, Gru01, Pen01b, Wri03, Bla03, Fra01, Jue04, PY05, Syv02]. Find [LH07].

Finding [HR04b, MP06, WYY05b, WYY05c, ZT03, SW00b].

FINDsomeone.com [Gra98]. Fine [SS01b]. Fine-Grained [SS01b]. Fingerprint [An02d, HHY07, HBF09, KHY04, MMYH02, CL04d, MMJP03, UBE09].

finger-print-based [SL04d]. Fingerprinting [KT01, CT07].
NP07, PS06, RS00, Shy02, ZYN08, AHK03b, CCCY01, CP07, CC04c, DMSW09, GJ05, GL06a, GM04, JEZ04, KNS05, MS09b, MBS04, YCW08, HF00. France [ACM04a, ACM05a, A101a, A102b, GH05, KNP01, NP01a, PPV96, KM07]. Francis [Bud06]. Francesco [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b]. FranzSteiner [Eag05]. fraud [Ano03a]. Fred [Bar00b]. Free [AP09, Ano02e, Bau01a, Bau01b, BGI08, Coc01a, CNV06, DG02, HS00, HM01b, JP03, Jut01, Fox00, KS06b, SG05, Bo102]. FreeBSD [Coc01a, Mur02, Siv06]. Freedom [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, Mil03]. FREENIX [USE01b, USE02c]. French [Wri03]. Frequencies [DD02]. Frequency [OMT02, Sak01, SOHS01, CS05a]. Frequency-Domain [OMT02]. Frey [Was08a]. Friar [GG05a]. Friendly [CTY09, CRSP09, Hsu05b, HH05b, HF01, LL05b, LS05b]. FrontPage [WWL02]. FSE [Bar07, DR02, GH05, JOh03, Mat02, RM04, Sch03b, Sch04a]. FTC [Ste05c]. fuels [Mad04]. Full [Cor00b, DOP05, LKH09, WYY8b, WYY8c, B104, CS08a, HS02b, LKH08, Oiw09]. full-encryption [HS02b]. Full-Round [LKH09, LKH08]. Fully [BL08, FSO1a, Gen09b, KPMF02, RG09, Gen09a]. Function [BR02, CMDP05, FIs01b, Fluo02b, GIS05, HNO09, HPC02, J200a, Kan01, Kil01b, Nie02c, RB01, Yan05, CHY05b, CJO4, HR07, LW04, LPM05, WWTH08, YW05, YRY05b]. Functional [ECM0a, WA06]. Functionalities [PS05]. functionality [ETMP05]. Functions [AEMR09, BBDK00, Bon01, Can01b, CV02, Car02, Che01c, DNO02a, DGN03, DRNS03, Fil02, FIPR05, GLG04, HSO04, HR04b, Jou04, Kil01b, LTV05, Lys02, PR01, RR08, SM00a, SM00b, SS01a, Sh00a, Sh00b, Ver02, WP03, WFLY04, Wer02, AGGM06, AGGM10, ALV02, CS09, GVC08, HRS08, ISO04, KK07, KS05b, LLH02, LKY04, MS02b, MS09c, Mic02a, Mic02b, RR04, PW08, QPV05, SM03a, Whi09, YRY04, ZW05a, RRS06]. Fundamentals [And04, PHS03, Sh08, Way01, VT00, Fin03]. Funds [Coc01a]. Further [JS05, LL04, LL05c, MP07, YRY05a]. Fusion [KZ09, TZD05, ZS05, BG09]. fusul [MAaT05]. Future [ASW01, Ano02f, JOh00, LNP02, NFQ03, Sch04e, HP00, LPW06]. Fuzzing [SGA07]. fuzzy [HS02b, NC09]. fuzzy-based [NC09]. G [Coc03, For04, Was08a]. Gaitherburg [SMP09]. Gamal [EKRM01]. Game [DHR00, LM02, CAC06, BR04, Go09]. game-like [Go09]. game-playing [BR04]. Gamers [MP00]. Games [KN08]. Ganesh [For04]. Ganzúa [GPG06]. Gap [OP01a, PWGP03, RW03a]. Gap-Problems [OP01a]. Gate [Coc02a, GC01a]. gates [TWM09]. Gauging [PvS01]. Gauss [KKH03]. Gaussian [EKRM01, JL03]. Gbps [TPS01]. GCD [JP03]. GCD-Free [JP03]. GCM [KS09a]. geeks [McN03]. Geheimsschreiber [Joy00, UW00]. GEM [CHJ+01a, JMV02]. General [AB09, CDM00, DN00a, ESG05, GM01b, KOG02, LNO03, MND04, SAd01a, YC01, YI06, JL03, LL05a]. General-Purpose [ESG05]. Generalisation [DJ01]. Generalization [YYZ01, HHW02]. Generalizations [LD04, LS08]. Generalized [KSR02, Mic02a, TC01, TJ01a, WAG02, WKL05, LKY00, Sh05]. Generate [HRS01, Wel02, FSGV01]. Generated [ADD09, MRL02, RBF08]. Generating [BMK00, BCDM00, GG01, MFK06, SS03]. Generation [ACS02, BH05, BK06a, CS03c, ESG05, GJKR03, GL01, GW01, JC01, MR01a, Ram01, TC07, TV03, WP03, WKL05, WBL08, WS02, Ano04c, BK07, BG08, BF01c, IS08, LS05b]. Generator
[ADD09, BP01a, DI05, Dic03, DGP07a, DGP07b, DV08, EHK+03, Gen00b, GM02a, Gol1c, GPR06, Int03, Kei05, LMHCETR06, LV04, SXY01, SFDF06, TWNA08, TTT09a, TTT09b, ZKL01, Aam03, ACTZ05, Bel08, BG08, BG09, BG07a, DGP09, GB09, HG05a, HlwWZ09, JAW+00, KH08, KS00, Pan07, PG+09, PS+08, PC00, RGX06, SR07, SB05, UHA+09, WW08, VKS09].

Generators [BST03, BK06a, BL08, CF01b, CS05b, Fink06, Kra02a, LBGZ01, LBGZ02, LS05a, MHO4, RSN+01, Vav03, BK07, BGPGS05, CO09, LBGZ02, LS05a, MHO4, RSN+01, Vav03, BK07, BGPGS05, CO09, SK01b, TS09, WW08, VKS09].

Generators-part [SK01b].

Generic [BN00a, DOP05, GGKT05, HLL05, MAr02b, MV01, GT00, Sch01f, Sch01e, XLM06, CHT+01a].

Generic [HTSI02, LMHCETR06, CV05, SCS05a, WJP07].

Gennaro [Miy01].

Gennaro-Krawczyk-Rabin [Miy01].

Gentle [RR03a].

Gentry [Hes04a].

Genus [CY02, GHK+06, Wen03].

Geometric [GTTC03, HH09, LLS05a, LL05c, LJ05b, SDF01, CJT01].

Geometrical [LWS05].

Geography [PPV96, WW06].

George [Gum04].

Georgia [IEEE09b].

German [Sch09, Ano04b, Liu02, Mor05, Sala0b, Sala0a, Win05b].

Germany [DRS05, Dwr03, FLA+03, Vw03, WK03, IE01b].

Geschichte [Sch09].

Get [Coc01a, WDO1a, Cpa00b].

gets [Bor00].

Getting [PM00].

GF [BP003, KPMF02, KLY02, KKY02].

GH [GHW01].

GHS [Hss04b].

Giant [Lam07].

Gibson [Ove06].

Giesbrecht [CHH01].

Gigabit [CGBS01].

Gigabits [HTS02].

Give [CB01].

Giving [PM00].

GF [BINP03, KPMF02, KLY02, KKY02].

GH [GHW01].

GHS [Hss04b].

Giant [Lam07].

 Gibson [Ove06].

Giesbrecht [CHH01].

Gigabit [CGBS01].

Gigabits [HTS02].

Give [CB01].

Giving [PM00].

Globus [MJD01].

GN [SC05b].

GN-authenticated [SC05b].

Gnana [For04].

GNU [Coc01a].

GnuPG [JKS02, Sti06b].

GNU [Coc01a].

GNY [Coc01a].

Goals [PHM03].

Gold [Boy01, For04, Tsa07].

Goldreich [Kat05b, Lee03b, Puc03, AC02].

Gong [GG01].

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

Goodness [CB03b].

Goods [NZCG05].

Google [Con09, Law09b].

Googling [Con09].

Got [Car01].

Goubin [Sma03b].

Governance [TPM07].

Government [Tyt00, RM02, Lev01, LCS09].

Governments [Ano00g].

GP [Bau01a, Bap01b, Luc06].

GPS [CKQ03].

GPT [Ove06].

Graduate [GV09].

Grafton [Pag03].

Gran [Rhi03].

Grained [SS01b].

Grand [Syv02].

Granted [Ano00h].

Graph [CGFS09, GTC03, HM02b, VWS01, YW01, CT07].

Graph-Based [CGFS09, HM02b, CT07].

Graphical [vOT08].

Graphics [Ct06, DNP07, MFS+09].

Graphs [NNT05, Ust01b, WGL00].

Gravrelen [Puz04].

Gray [FGD01, Har05b].

Gray-Scalar [FGD01].

Grayscale [YCL07].

Greatest [Bel07a].

Greece [ACM01a, KGL04, SM07b].

Greedy [HKPR05].

Green [TR90a, TR90b].

GREMLIN [Ht01].

Grenoble [ACM05a].

Grey [BDN00, SCS05a].

Grid [ACM05a, MJD01, SEF+06, TLC06, ZB05, Ch07, CJK+04].

GridOne [YCL09].

Grids [CTY09, MPP09].

Grip [Buh06].

Gröbner [CCT08, FJ03, Fau09].

Group [ANRS01, AAF01, ACJ00, BBS04, BCP01, BCP02a, BCP02b, CD00a, CTV01, CH01a, HSH02, HSH06, HWW04, Hug02, JP02b, KY03, Kin02, LPL01, MS05, SO02, SWH05, Ste01, Dan07b, VWS05, Wer02, AKNR04, BCP07, CL04b, CYH04, CHC05, CWWT01, CWT04, Ch08b, ED03, He02, Hen06a, HWW02, K505a, KPT04, KKKL09, LL06, LHL04, LPM05, LWW05, NS05b, PQ03a, PQ06, RHO3, SN01, Sha05a, Tjo01a, Tse07, WGL00, WHHT08, YLC+09, YY05a, YZZ04].

group-by [YLC+09].
Group-Oriented [LZL +01, HWW04, CHC05, CWJT01, LL06, TJ01a, WHHT08].

Groups [BSS02, CV03, CF02, Dre00, GM02a, GST04, KM01a, KLC+00, LLH01, LP03, Luc02b, MN01, PHK+01, GR04, HM00, LLY06, Pae03, Yi04].

GSM [BBK03a, BD00a, Cha05b, Cin02].

Guadeloupe [Wri03].

Guanajuato [Buc00a].

Guangzhou [LLT+04, Li05].

Guessing [AGKS07, Bau05, Shi05, YS02, DLMM05].

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

Guide [Ano06c, BS01a, BS05, BCP+03, BP01b, HMV04, Poo03, Vac06, Wei04, And08, Bon00, Bro05b, C+02, Che00, Gar03b, Kuv03, Lun09, Mol05, SL06].

Guides [SK01, SEK02].

Guidebook [SEK01, SEK02].

Guided [ZY08, Pet08].

guidelines [Die00].

Guildford [KN03].

Gummy [MMYH02].

Guo [LLLZ06a, LLLZ06b].

Gutmann [Uzu04].

H [Was08a].

H.R [Uni00d, Uni00e].

H64 [GMM01].

Hacker [Gol08, Har05b].

Hacking [Eri03, Eri08, Gun04, Man08, MSK03, SSS06, VGM04, Puz04, Har05b].

Hacks [Sti06b, Sti06a].

Hadamard [HWW05].

Hagenberg [Jef08].

Half [HS02b].

Halvespaces [KS06a, KS09b].

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

Hall/CRC [Kat05b, Was08a].

Halmstad [BS01b].

Hamming [GK02].

Hand [Lov01].

Handbook [RK06].

Hand [OKE02].

Hands [KLB+02b, Shu06].

Hands-on [KLB+02b, Shu06].

Handshake [SB01].

Handshakes [Ver06a].

Handwriting [Bau02d].

Hankerson [Irw03].

Haptic [PBM+07].

Haptics [Pau02a].

Hard [Har07b, HM04, Lai07, CGH06, GPV08].

Hard-Core [HMS04].

Hard-Disk [Har07b].

Hard-Line [Lai07].

hard-on-average [CGH06].

hardcore [Sch01e].

hardcover [Eag05, Pag03, Top02, Pap05].

Haddrick [Por01].

Hardware [Ano02b, Ano07b, Ano07a, BM01a, Dit03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG+02, Gro01, GPP08, IK00, ISW03, JQ04, KKP02, ND05, PS01c, RS05, RS04, SOT00, SM10, SM20, SM03b, SR03, SGK08, TS00, TDL01, WK03, WRB00, XH03, X01, YKLM02b, Z02a, ARJ08, An000a, BK0+03b, EKH04, GC00a, HBC+08, KP01, KNP01, KD04, RAL07, SOI07, VS08, W04, YKLM03, YW06].

Hardware-based [Ano02b].

hardware-constrained [RAL07].

hardware/software [ARJ08].

Harley [WPP05].

Harn [GG01].

Hash [An08d, An12, AEMR09, BBKN01, BRS02, BDS09b, Bur06, Cor00b, Cor02, CDMP05, CS02, DOP05, FIP02b, F02, GIS05, GLG+02, HCP02, HR04b, ISO04, J04, KMM+06, MD05, RRS06, RR08, RB01, SS01a, Sh00a, Sho00b, SK06a, WFLY04, Yan05, YZ00, BR06, KCL03, Ku04, KCC05, LHH02, LKY04, LW04, MS09c, Mic02b, Wag00, YRY04, FIP02a, Z05a].

Hash-based [BDS09b, KCL03, Ku04, KCC05].

Hash-CRC [BBKN01].

Hash-Function [BRS02].

Hash-functions [ISO04].

Hashes [Sch01a, GNP05].

Hashing [IK05, SGGB00, WS03].

HAVA [WFLY04].

HAVAL-128 [WFLY04].

HAVEGE [SS03].

HB [MP07].

HB-family
LLS05a, LZ01, LWS05, LY07, LJ05b, LSC03, LSKC05, PZL09, RS00, SDFH00, SDF01, SSFC09, SYL05, TZ01, TH01, TC01, UP05, VKS09, VK07, WY02, WL05b, YZEE09, AAPP07, AQ08, CC02b, CH01, Che07, Che08a, KC09a, LLCL08, Lin00a, LT04, LYGL07, LLC06b, MS09a, MB08, PBV08, Sch00a, Sch01c, S＋03, Sch04b, Sch05a, mSgFtL05, TL02, Wan05, WMS08, YCYW07, YCL07, ZLZS07].

Imagery-Feature [GW01].
image-identification [PBV08]. Images [CTL04, CC08, CW09, DP00, FGD01, LS08, PJH01, PBC05, RE02, WCJ09, WC04, YWWS09, AAPP07, AEErD05, BN00, FWTC05, HHYW07, TCC02, TND＋09].

Imaginary [HJW01, HM00, Huh00]. Imai [DDG＋06, YG01a]. Imbalanced [ZWCY02]. Immune [HJW01, HM00, Huh00]. Imbalanced [ZWCY02]. Immunization [HR05]. Impact [Ber03, HGNC＋03, JKRW01, MMYH02, Wri00, CS08a]. Perfect [CP07, DOPS04]. Impersonation [BP02, Hsu05b]. implant [Fox00].

Implement [HQ05]. Implementation [AD07, AG01, Ase02, Ash03, ARC＋01, BBD＋02, CDDP01, CGP08, CG03, CPS01, CS05a, Cor00a, EYCP00, EHK＋03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HMM01, JKRS02, KMM＋06, KMS01, KTT07, KRS＋02, KV01, LP02a, MKP09, MM01c, MN01p, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBWT07, QSR＋02, RDJ＋01, SM01, Sha01e, SK05a, SQRL03, USS02, Vir03, WZW05, WW00, WLO01, XB01, Zea00, BI04, BBK＋03b, C＋02, CNPQ03, DKL＋00a, GldGS00, GBKP01, Hi0h01, HP01, Hup01, KY09, LL04b, LCX08, LB05, Rh＋03, SM03a, SVDF07, WLO04, YW06, ZFK04].

Implementations [AL00b, BJ02, II00, CTTTL01, CGBS01, EPP＋07, GLG＋02, MM01b, MP01a, RS01, WW00, AS05, BFCZ08, BFTG08, BG07b, FR08, RAL07, RSLQ03].

Implemented [TSS＋03]. Implementing [Dwi04, Kor09, LM08, LDM04, MWS08, NDJB01, Pet03, SSM01a, SR06, C＋02, CW02].

Implications [Kun01, LJC05a, MFI01, Bjo05, Fri07]. Implies [KY01e]. Imply [Pie05].

Importance [AN02b, KCJ＋01, TIGD01]. Important [SM00a]. imposed [XLMS06]. Improbabilities [CHL02]. Impossibility [AP05, BPR＋08, Fis01b, PQ06].

Impossible [BF00a, BF00b, CKK＋02, HSM＋02, MHL＋02, Pha04, SKU＋00, SKI01]. improve [Pau02a, SIC06].

Improvement [CAC06]. Improved [AFGH06, BPR05, BB05, BF00b, CL01b, CJK＋02, CJ04, DN00a, DG02, Fan03, FKS＋00, FKL＋01b, FKL＋01a, GMR08, Gen00b, HCK9, HKA＋05, JQY01, Kin00, KT06, Ku02, Kiu02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02e, P08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].

Improvement [AS01c, AJ00b, Che04a, CKZ05, CCW02, DI01, HWWM03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT＋00, NP07, Sha04b, Sha05b, WHHL03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CH05a, Hsu05a, JSW05, JmBDX05, KJY05, LL04a, LW05c, SZE05, TO01, WLT05a, YW04, YWC05, YRY05a, ZC09].

Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, SQRL03].

Improving [ASK05, Dim07, ESBS01, KMT01, LHC08, LS01b, Mic01, SKQ01, SB01, Sun02, XQ07, YEP＋06, YGZ05].

incentives [Swi07]. Incident [JBR05, Tom06]. Including [SR01].

Incomputable [Ver06b]. inconsistencies [MS09a]. Incorporating [MFS＋09].
incorrectness [CHC04]. Increase [PBTW07]. Increasing [CS05c].
Incremental [BKY02, LKLK05].
IND-CCA [MiKi01b]. INDC-CCA2 [BST02].
Independence [BP03b]. Independent [BS00a, BSL02, Kin02]. Index
[Ano00b, Ano01d]. Indexing [YPPK09].
India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano00c]. Indies
[Fra01, Syv02, Wri03].
India [CV04, JM03, MMV06, MS02c, RD01, Roy00a]. Induced [Vau02].
Industrial [USE00b]. Industry [ANS05, Mad00, Ort00]. ineectiveness
[YLR05]. Infeasibility [FS08]. Inference
[Mar02b, CDD05]. Infinite
[TZT09a, TZT09b, Vau01]. Influencing
[Blak01c]. Inform [Kwo03b, San05].
Information [AP09, BW07, BIM00, BZ02, Big08, BB03, BJ02, Boy01, CGM07, CC06, DM00b, ECM00a, ELvS01, Hay06, HQ05, HW01, ISO04, JD01, JG07, KP00, Kei02, KLB02b, KO00, Lai03, Lee04b, LW05b, LL01, MH05, Oka00, PP06b, RSA00d, RS01, Roy05, Sch06b, Son00, Sta06, Ste02, TG07, VDKP05, WABL08, Yek07, Zhe02b, ZS05, vW01, ABHS09, ABW09, Arn01, Bid03, BK00, BEZ00, BEZ01, Bro05b, Duw03, FR08, FOP06, Gar04, Ghah07, IY05, KN08, KB00, Kov03, MS09b, ME08a, PS02a, Smu02, TWM09, Way02b, Way09, dLB07, CS09, FLY06, GW00, Kim02, LL03, LL04c, PC05a, Won01, WK06]. information-flow [FR08].
Information-Theoretical [VDKP05, vW01].
Information-Theoretically [DM00b].
Infrastructure [AHKM02, AL06, BC04b, BWE00, CL07, ES00a, FL01b, GKL04, Sin01a, BH03, BDS09a, Ben01a, C105, FB01, Gor05, LCK04, MWS08, Ben02].
Infrastructures [HCD00, Lin00b, PHM03, WB01, Bra01a, LAPS08, SN07]. INIDP04
[LDM04]. initial [DK08]. Initiative
[Coc01a, Cal00b]. initiatives [Mau05]. injection [MMJ05, ZSN07]. Injective
[CMDV06, KOs01c]. Innovation [Sam09]. innovations [Web02]. Innovative [MM07a].
Innsbruck [Pfi01]. Input
[CAC06, TC00, DKL09, VM03].
Input-trees [TC00]. Insecure
[Vau05b, Wal01, BJN00, LLH06, XWL08].
Insecurity
[Blak02b, DOP05, Lai08, Man02, NS01b].
insertion [MB08]. insertion-extraction
[MB08]. Insider
[CS09, Tad02, KSM05, Mah04]. Insights
[Kun01]. Inspired [CC09]. Installation
[USE00a]. instance [FS08]. Instances
[GG01, HN06]. Instant [BBK03a, RR05].
Instantiated [RR08]. Instantiation
[BF05]. Instruction [BBG08, EP05, KTT07, Bnu06, HTW07, MMJ05].
Instruction-Level [EP05].
Instruction-Set [BBG08]. Instructions
[LS01]. instrumentation [MPPM09].
insubvertible [ACdM05]. Insulated
[DKX02]. Integer [Gro03, JL03, MN14].
Integers
[CH07c, GP01a, KKM01, EKRA01]. Integral
[KW02, WH09]. Integrated
[ECM00a, ECOM00b, GMG00, Lut03, GLC04, LK01, SSM08, SN04].
Integrating
[Wit01]. Integration
[It00, CJL06, Sug03]. Integrity
[An02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHLR04, Yun02b]. Intel
[Coc02a, MP00]. Intellectual
[Qu01, WY02]. Intelligence
[Cop04b, AJ08]. Intelligent [Cos03]. Inter
[WRW02, ECOM00b]. Inter-Exchange
[ECM00b]. Inter-Packet [WRW02].
interaction [Gav08]. Interactions [Fau09].
Interactive
[DG00, MS09c, CHK05, DDO01, Fis01b, Fis05, HNZ02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00, MS09c].
Interception [CHV03]. interdomain
[MABI06, vOWK07]. interesting [SWR05].
Interface [RSA01]. Interference
[FGM00a, FGM00b, GA05, BR05].
Interlaken [CC04a]. Interleaved [ZSJV07, NC09]. intermediaries [JA02].

Internal [Har07b, Bej06]. International [ACM03a, ACM04a, ACM05a, ACM09, ACM10, Ano00d, AAC99, AJ01b, BDZ04, Be11, B+02, BBD09, BS01b, Bih03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCMR02, CCMR05, CSY09, CPG03, Cra05a, DR02c, Des02, DNU05, DFPS06, EBC99, Fra01, FMA02, Fra04, FLA03, GH05, IEE09a, ZZ00, IZY05, JYZ04, Je08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, KLO1a, Kim01, Kim02, KN03, KCO1, KP01, KN01, Lai03, LL03, Lee04b, LST99, LL94c, MMV06, MJ04, MS05a, Mat02, MS04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pfi01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Scho1d, Sho05a, Sil01, SM07b, Syv02, TB02, TCO06, Ulo00a, VV01, Van05a, WKP03, Wi09, Won01, Wri03, Yun02a.

International [YDKM06, ZJ04, Zhe02b, ZY03, AMW07, AUW01, Ano00e, AJ01a, BCKK05, Bir07, BC05b, CCM05, CV05, DWML05, DRS05, GKS05, HH04, HH05, HA00, Hon01, May09, PC05a, PY05, PPV96, QS00, Sma05, Son00, ST01d, WK06, Ytr06].

Internet [SMP09, ABB04, Ben01a, Ben02, Cal00a, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HK06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, Pvo01, Pho01, PFM03, Rub01, SBB05, SEK01, SEK02, Sto01, Tsa01, TWL05, Uro01, WCJ05, Wri05, ZHT05, k01]. Internet-wide [SBB05].

Interoperability [Hil00, TEM99, BHM03]. interoperable [BFGT08]. Interpolation [LW02, YGO1b, FWTC05, KT06].

Interpolations [Sat06]. Interpretation [Mas04, CC04c]. interpretation-based [CC04c]. Intersections [KS06a, KS09b].

Interstate [RM02]. intranet [Jan00].

Intrinsic [ZWC02]. introduced [Ano00a].

Introducing [JL00]. Introduction

[Ben02, Ber09b, Bis03a, BK06b, Buc00b, Buc01, Buco4, CLR01, DK02, DK07, Fal07, Hay06, HPS08, HC02, KL08, MA007, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGK08, TW02, TW05, TW66, Big08, CS07a, CM05b, Gar01, HW98, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06a, Kat05b, Rot07, Lee03a].

Intrusion [CZK05, DKf99, DP07, JT05, TZD05, TMM05, W05, HLL99, MAC99, NCRX04, NNO2, YbJ04, IR02].

Intrusion-Resilient [DFK99, DP07, IR02]. intrusion-tolerant [YbJ04]. intrusions [Bej06]. invalid [CJT04]. Invariant

[Ben00, CT09, HH09, ZL03]. Invariants [WH09].

Invasion [ASW98]. invasions [Tyn05].

Invention [Ifr00]. Inventors [Bar00c]. Invincible [Hao00a, JP01, MFF05].

Inversion [BNPS02, KKY02, KTT07, SPG02].

Inversion/Division [KKY02]. inversive [SB05]. Investigating [BW07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03].

Invitation [Bar02]. Invited

[FGM00a, Lan00d, DRS05]. involutional [SSH07].

IP [An00a, CD01b, FXA04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSec

[Vau02, CGBS01, Dav01a, KMM99, SKW99, FS00, FS03a, XLMS06].

IPSec-Compliant [CGBS01]. IPTables

[GC05]. IPv6 [Nik02a, Nik02b]. Iran [Maho04]. Iran [Cos03]. Iris [LJ06].

Irregular [MH04]. Irregularly [CGFS99]. Irreversibility [ZWC02].

ISBN [And04, Duw03, Eaq05, For04, Gum04, Imr03, Pag03, Puz04, Top02].

Island

[CS09, KGL04, Kim01, Lee04b, IEE07].

ISSAC [Jef08]. Issue [FOP06, FOP06]. Issues [BDF01, BH00a, KRV01, Mea01, PBM²+07, SEF²+06, MKY08, Part02b].

ISW'97 [You01]. IT-Architectures [RM02]. Italy [AAC01, AL06, BCKK05, BC05b, CGP03, dCdVSG05, IEE04].

Itanium [CHT02, Int00a]. Itanium-based [CHT02]. Iterated [Jou04, Oni01].

Iteration [Che03]. IV [Sch01c, HSH²+01]. IWBRS [LST²+05]. IWDW [BCKK05, CKL05, KCR04, PK03].

J2EE [BTTF02]. Jack [Coc03]. James [Top02]. jamming [LPV²+09]. Jan [YRY05b]. January [Des02, GL05, Vau05a, Wri03]. Japan [An0001, Mat02, Oka00, Coo02b, Smi01b].

Japanese [YJ00]. Java [An040b, Mar05a, WBL01, An002e, An040a, An040c, AJ01a, BC0502, Bi0303a, BJvDB02, CMM²+01, Che00, CCM05, Coo02, DPT²+02, DILT01, Dra00, EM03, Gal02, GW08, G0101, Has02, Hoo05, Ham05, LA00, Ler02, LDM04, Mar02a, MWM01, Nis03a, R01, Rot02a, SA02, SL00, Str01b, SJ05, Vir03, We04, Win01, Zea00, ZFK04].

Java-Based [EM03, DPT²+02, GW08]. Java-Lösung [An040b]. JAVA-Ring [WBL01].

JavaCard [AJ01a]. JavaCards [Cim02].

JavaScript [TEM²+01]. java.crypto [Win01]. JBis²+07 M [MP01a]. JCCM [CMG²+01].

Jean [MFS²+09]. Jezu [CSY09, Lee04b]. Jeng [QCB05b]. Jeness [Sal03b]. JICC [HYZ05b]. Jin [Coo01a].

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

Johannes [Lee03a]. John [An040, BZ02, NH03, Rot07, Coo03]. Joins [Bar00c, Con00]. Joint [ADI09, ADR02, CR03, HYZ05b, HYZ05a, Puc03, M09].


Julius [Chn02]. July [ACM01a, CZ05, Jef08, KJR05, May09, PVP96, Roy00b, Sch01c, S²+03, Uni00a, Uni00b, Uni00c, Uni00d, ZJ04]. Jump [MP00]. June [ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BS03, BS01b, BCDH09, BC01, C0502, FMA02, IEE05b, IKY05, JYZ04, KGL04, KN03, KM07, PVP96, TB0J02, USE01b, USE01c, USE02c].

Just [ABB²+04, An060a, Gut02a, Car01].


Keeping [SEK01, SEK02]. KEM [NM05]. Kerberos [BCJ²+06, C001a, Gar03b, Hil00, Ito00, LLW08a, MJ01, MPP00, Rub00, Smi01a, Wac05, WD01a, Wit01].

Kerchoffs [KMZ03]. Kernel [Int00, Mor03, BK05, HB06]. Key [AN05, ASW00, AK02a, An01j, An09b, AAF01, AEAQ05, AL06, AF03, ABM00, BC05a, BPS08, BH06, BDG²+01, BDZ04, Bar00a, BPS00, BPR00, BBM00, BBPD01, BY03, BOHL²+05, Ben02, LBM01, Bih00, BBB²+02, DDK²+09, BR00b, BM03b, BDTW01, BM010, BM03c, BPM00, BBCP01, BCP02a, BCP02b, BM01c, BST02, CK02a, CK02b, CHK03, CHK05, CPP04, Che01a, CT08a, CHKO08, CCW02, CCM01, CMM00, CS02, CS03b, CS03c, DPK04, DJ01, DPS05, Des00c, DBS01, Des02, DG03, DY09b, DKXY02, DK²+03, DGH²+04, DBS²+06, ESG²+05, EP05, ES00a, FL06, FKS00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Go03, GH01, GC01b, GSB²+04, Gut04b, HNZI02, HCDG02, HLM03, Hoe01, HR05, HG03, HC08, HJW01, HS07, HLC08, IEE00b, Ina02a, Ina02b, JL08, Jou02, JG01,
DPV04, DFS04, DDO+01, Eri02, Fis05, Gen04a, GK05, HNO+09, KS06b, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00, Ros06a, TG07, BDSV08, CLR09, Dam00, Hro09, IKOS07, JRR09, PBD07, KK07].

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

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

Kobitz [AHRH08, Has01b]. Kolmogorov [Sch01a]. Kommunikation [Lin02]. Kong [B+02, ZJ04, Cla00b]. Konstantin [Puz04].

Korea [CSY09, CKL05, KCR04, Kim01, Kim02, LL03, Lee04b, LL04c, May09, PC05a, PK03, Son00, Won01, WK06].

Körner [Mor03]. Kościszko [OC03]. Krawczyk [Miy01]. Kryptanałyse [Mor05]. Kuala [DY05].

Kunning [ZYH03]. Kurosawa [CHH+09]. Kurtz [Gum04]. Kyoto [Oka00].

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

Laboratory [Bru06, LBA00]. Lagrange [FWTC05].

Laid [Wei06, Wei05]. Lam [Wag00].

Lamar [LHMCE96]. lamp [McN03].

LAN [Bar03, Pau03, SZ08, Sty04].

Lanczos [BF06a]. Landau [Jan08a].

Landscape [Ahm07]. Language [ARC+01, DDD02, Gou09, Jen09, MW04, WAF00].

language-based [WAF00]. languages [Lun09, Rob02, Rob09]. Laos [Lov01].

Laptop [PTG07]. Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, EIA+03, G001, H000, P005, S001, ST03b, USE00a, BP03a, CKY05, C03b, Has00, HMvdLM07, HY03, PS08a, S03a, TM06, WL05].

Large-scale [CDR01, BH00a, BP03a, HMvdLM07, PS08a].

Larger [Car02]. LAPRBS [CPhX04].

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

latency [RSP05]. Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HPS01, HG07, IM06, Mic01, Reg03, Reg04].

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

lattice-reduction [HG07]. Lattices [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Sph05, Sli01]. Launched [Bar00b, Ano00].

Launches [Ano02d]. lava [McN03].

Law [GN06, MFG02, Ste05c, NM09]. Layer [LXM+05, LPV+09, SLP07, ZL04c]. Layers [Gri01].

Laying [Lut03]. Lazy [CCM05].

LDAP [Bau03a, Bau03b, BH00b]. Lead [Tsa07].

Leak [RST01]. Leakage [CKN01, DP08, Ke02, RS01, ABHS09, CKN04, IY05].

Leakage-Resilient [DP08]. Learned [GBS+04].

Learning [KS06a, LY07, CAC06, BKW03, KS09b, Mal06, Reg05, Reg09, SM08, Whi09].

Least [SZ01]. lecture [Rot02b, Rot03, Adl03, RSA03a, Riv03, Sha03b].

Lee [Sty04, C02b, KRY05, KCL03, KHKL05, LKY05d, SCS05b, ZK05].

Left [Dhe03, HKPR05]. left-to-right [HKPR05].

Legal [Coc02a]. Legislation [Eng00].

legislative [AvdH00]. legitimate [Lin01a].

Leighton [Rub00]. Leighton-Micali [Rub00].

Length [AR01, BR00b, CKN00, CHJ+01b, M03a, RK06].

Length-preserving [Mes03a]. Leonard [Coc03]. Less [YKMY01, BD00b]. Lessons [GBS+04, KS00].

Lest [HSH+08a, HSH+08b, HSH+09]. Lets [Pau02a].

Lev [Kwo03b]. Letters [ASW+01, BTTF02, MNT+00, TEM+01, TvdKB+01, WWL+02].

Leuven [BBD09, DR02c]. Level [EP05, MV00, TV03, BDN00, DHL06, KVN+09, SS03].

Levels [KM05, CUS08, Voi05]. Leveraging [BRTM09].

LEVIATHAN [CL02c]. Levin [AC02]. LFSR [Jam00, JZCW05].

LFSR-Based [Jam00]. LHL [Pei04, YRY05a]. LHL-key [Pei04, YRY05a].

Li [JW01, KCL03, SZZ05, QC05a, SC05b, ZK05].

Liaw [TJ01b].

Liberty [Lan04b, An00]. librarian [PBV08]. Libraries [Fin02, MK05b].
Library [KSZ02, Lau05, Law09b]. Libre [Jen09]. license [Ano00h]. Lies [Gan01b, Sch00d, Swa01, Ste05c]. Life [Cop04b, GSBJ04]. Lifecycle [HL06]. Lifetime [Coc01a, CPG04]. Lifting [CNS02]. Light [WT02]. Light-Weight [WT02]. Lightweight [EPP07, Mal02, CH07a, CL09, MP07]. Like [Coc02a, PSC02, VMSV05, BCDM00, CPL05, Egh00, EBS01, Gui09, HSL04, SKU00, SLL00]. LILI [JJ02]. LILI-128 [JJ02]. Limitations [Gua05, Fis01a]. Limited [AK02a, LCD07, Buh06, Tse07]. Limiting [CCK04b]. Limits [CWR09]. Lin [CC02b, CHY05c, KTC03, YY05b]. Line [Cho08a, DL98, Jan08a, Lu02, SK06, YLLL02, Bau05, MCS02, DL07, Luk01, Shi05]. Linear [BDK02a, BDK02b, BDQ04, CGFSHG09, C05b, CHJ02, Cou01, CM03, Cou03, CD01a, CDG05, FM02a, FM02b, GS03, GMB02, HLI01, Hug02, JI00d, Kan01, KMT01, Kin02, KM01c, KRS02, KY01e, LLI01, LS05a, NPV01, PSC02, PG05, PZ02a, SNWX01, STK02, WF02, YSD02, BD04a, Bul09, CLK03, Cou04, GHPT05, Kuk01, LLI04, Reg05, Reg09, RSL03, Se00, SLL00, TM01]. Linearization [DDG06]. Linearly [ADD09]. Lines [SP04]. Linguistic [CDR01]. link [LPV09]. link-layer [LPV09]. linkages [ZAX05]. linked [YWWS09]. Linking [GW00]. Linux [Lin02, ASW01, FR02, Fon02, Fri01, GJ05, Gau08, GPR06, JEZ04, Lin02, Mor03, Pri00, Shu06, St02b, Sta05]. LISA [USE00c]. list [AGK07]. little [Lam07, Sch05c]. Live [Lov01]. Lived [GW00]. lives [FRN05]. living [BCB05]. LLL [CKY05, NS05c]. Load [CC08, Höf01]. Loads [GH02]. Loan [SOOI02]. Loaning [Bl01c]. Local [NABG03, Lav09]. Locality [MFS09]. Localization [WT05b, CKL09]. Locally [Vad03, Yek07]. Location [HY01, KZ01, LNL08, Buh06, SG07]. Locations [Kra02b]. Log [Gen00b, HN04]. Logarithm [CNS02, Che04b, CCG02, GV05, GPP08, LW02, Hsu05a, HL05d, JLL01, LHY05, Sch01e, SCL05, SLC05, Yas08]. Logarithmic [EGK08]. Logarithms [C03a, JL03, LHL03a, LTH05, PLJ05a, QC05a, Sha05c, Sha05d, SCS05c]. Logging [Fox00, MT09]. Logic [BPST02, Cop04b, KB03, KS06b, Li01, Nie02d, SQ01, SC01, Tec06, TV03, BDS02, BD04a, DZ01, SW02, WZ05]. Logic-Based [KBD03]. Logical [Kra07, SP03, Zha08]. Logics [IK03, IK06]. Login [LL05c, CCK04b, CT01]. Logistic [KJ01]. Logo [LZ09]. London [Pag03, Top02]. Long [ABRW01, Dur01, GS00, Gro03, PC01, Zho06, BM06, IS05, SG09]. Long-Lived [GW00]. Long-Term [ABRW01, Dur01, BM06, IS05, SG09]. Look [Bon07, Has00, Lut03, Syc00, Hen06b]. Look-up [Has00]. Looking [ASW01, Ano01i, Cha00b]. looks [Nis03a]. Lookup [MFFT05]. loop [KVN09]. loop-level [KVN09]. Loopholes [Ste01]. Lorenz [GHdG00, S00a]. Lorenz-based [GHdG00]. Losing [Sta05]. LosLobos [Pri00]. Loss [LHS05, Mit00]. Lossy [AIP01, HSK01, PW08]. Lost [PY06, Rob02, Rob09]. Lösung [An04b]. lot [Cha00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [QS00]. Louvain-la-Neuve [QS00]. Low [An00d, BM01b, CH07c, G04, HNZI02, HGR07, JO02, KBM09, RM03b, RM03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09, Fan03, HLL03, LCS04a, WMM05, WY05, ZYW07]. low-computation [Fan03, LCS04a]. low-cost [CL09]. Low-end [SU07]. Low-Exponent [SZ01]. Low-power [HGR07]. Low-Power [An00d, JP02a, KB09, CO09, ZYW07].
Low-State [GST04]. Low-Weight [CH07c].
Lower [BDF01b, BP03b, DIRR05, GT00, GGK03, PS02a, Shp03, WW05, KS05b, Shp99]. LSB [CS05e, FGDO1, WMS08]. LSB-encoded [WMS08]. LSD [HS02a]. Lu [QCB05b].
Luby [MP03, Pat03a]. LC [LNS02].
Luminy [PPV96]. Lumpur [DV05]. Lund [Joh03]. LUT [CC02a, TL07]. Luxembourg [Bir07]. Lyndon [GS01, VS01]. Lynn [Hes04a].
LZ [AL04]. LZ-77 [AL04].

M [DNRS03]. M8 [TM01]. MA [ACM10, JQ04, Kil05, KP01, Nao04, Pag03]. MAC [BKN04, CKM00, Ki03, LPV+09, Vau01, Kra03]. MacDES [CKM00].
Machine [LBA00, Mal06, Pro00, Cas06, Kid00, Pau02b, SWR05, WQN08, Win05b, HM01a, Pet08].
Macraigor [Ano02d]. MACs [BPR05, BR00b, BM01c, Sem00]. Made [Ste05b]. Madison [FMA02]. Maelstrom [MYC01]. Magic [DNRS03, Bur02, Hro09].
Magyarik [dVP06]. Mail [ANR01, Cos03, KS00a, Law05, LO04b, NZS05, All06].
Mainframe [Web08]. mainstream [Bjo05]. Maintaining [MJF07, Zho02].
Maintenance [NABG03]. Maiorana [Car02]. Majesty [Bud06]. Majority [GKK007, SV08b]. Make [BP06, Ber03, Sin02]. Makes [Pan09].
Making [CRSP09, Gar01, Lut03, Mit00, Oec03, Per05, Wri05]. Malaysia [DV05].
Malaysian [Kha05]. Malicious [HLC08, SZ03, YY04, Tsa06]. malleable [DW09, FF00, PR05]. Malware [LH07, SZ03]. Man [Gen04a, Urb01].
Man-in-the-Middle [Gen04a].
Management [ACM03a, ACM04a, Ano02d, Ano02e, BP07, BW07, ELv001, FMA02, GKO4, Gut04b, KB06, Lin00b, Scr01, Sha02, Woa00, Wya02, AW00, AJS08, AFB05, CG06, Cha05a, GT08, ISO05, Jun00, JW06, KHYM08, KAM08, LM05, LPM05, LR01, LK01, MKKW00, Pot06, RH03, SRJ01, Sen03, UP05]. manager [KH03, Sha01a].
Managing [MA00a, MA00b, NDJB01, Oue05, PTP07, PBB02, Tot00, BJ02, Kow03, KH03].
Mandrake [TvdKB+01]. MANETs [STY07, DF07]. manipulation [SWR05].
Manuscript [GG05a, Rug04]. 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 [Irw03]. March [BDZ04, Bir07, Bla03, HR06, PY05, Sil01, Uni00g, Uni00h, Ytr06]. Marian [Kap05].
Marjan [BCB+05]. Markers [FBW01].
Market [Bar00a, Ano01h, Swi05]. Marketplace [PL07, VN04]. Markov [KW03]. Marks [Ano01c, YSS+01].
Markup [Uni00a, Uni00d, Uni00e]. Marrakech [IEE09a]. Marriott [USE01b, USE01a]. MARS [BF00a, BCDM00, Fer00, IBM00, IK00, KKS00a, KS00b, KKS01, SOTD00].
MARS-like [BCDM00]. Mary [Ree01, Sin99]. Maryland [ACM05b, ACM05c, ACM09, SMP+09, GL05]. masked [AHS08, Lau08a]. Masking [CH02, CT03, GK02, Lav09].
Massachusetts [IEE05b, USE01b, USE01a, IEE03]. masses [Pot06]. massively [FP00].
massively-parallel [FP00]. Match [JJ00a, WC04, LLC06a]. Matching [ABM08, Len01, UBE09, Voi05].
materialized [MSP09]. Materials [SLT01].
Math [SR06, Mc03]. Mathematical [AUW01, Cas06, FF01b, GL05, HPS08, Kat05b, You06, GKS05, Sin09].

Mathematics
[BP06, Lew00, Nie02d, Sch05a, Wal00, Gar04, Sch00a, Sch01c, S+03, Sch04a, Sch04b].

Mathématiques [RSA09b, PPV96].

Matrices [TL07, CFVZ06, LMTV05].

Matrix [CV03, BFL06a, OS07].

Matroids [CDG+05].

Matsumoto [DDG+06, YG01a].

Mature [Tro08].

Max [Di 01].

maximal [Hüü00, HJW01].

Maximum [KMT01, ZC00, DW01].

May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bih03, CC04a, Cra05a, DRS05, IEE01b, Kn02, KN01, MJ04, MS00a, PM00, P+01, Pre00, TLC06, Uni00f, Uni00c, YKLM02a, Pau02a, YJ00].

Mbps [LMP+01].

McClure [Gun04].

McEliece [CFS01, KI01a, KI01b, Loi00, LS01c, Sun00b].

McEliece-Based [CFS01].

McEliece [CFS01].

McEliece [CFS01, KI01a, KI01b, Loi00, LS01c, Sun00b].

McEliece-Based [CFS01].

McFarland [Car02].

McGraw [Gun04].

McGraw-Hill [Gun04].

MD4 [DG02, WFLY04].

MD5 [Eke09, WFL04].

Me [CAC03, CNB+02].

Mean [Bar00c, KLML05, Ver06b].

Means [LMHCETR06, Nis03a].

measure [Lav09].

Measurement [Ano02e, kp01, CO09, FXAM04, RW07].

measurement-based [FXAM04].

Measures [CB01, QS01].

Measuring [Siv06].

Mechanising [Bel01].

Mechanism [LXM+05, WY02, CL08, GH08, LCP04, ME08b, WAF00].

Mechanisms [BACS02, CJK+04, Lin00a, MD04, Mir05].

mechanized [dH08].

Media [Hei07, Ano02a].

Median [Cap01].

Mediated [DT03, CG06].

mediator [SBG05].

mediator-free [SBG05].

medical [AL07].

Medicine [MYC01].

Meet [Cl00a, HG07].

meet-in-the-middle [HG07].

meeting [Je08].

Meets [Way02a].

Melbourne [IZ00].

Member [CTH08].

Membership [NBD01, Fis01a].

Memoir [Bar05].

Memorable [KOY01].

Memoriam [DNR03].

Memory [AK03, AJ008, BS00b, CCM05, DK08, DGN03, HNZI02, HBdJL01, KCJ+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05].

Memory-Bound [DGN03].

memory-safe [Oiw09].

Memoryless [Sar02].

MEMS [ECC+07].

MEMS-Assisted [ECC+07].

ment [CAC06].

menu [Mea04].

Mercy [Flu02a, Cro01].

Merkle [CDMP05, JLS03].

Mersenne [Ano03d].

Mesh [LPZ06, ZTP05, KB09, LZP+04, YPSZ01].

Mesches [BGI08, Lav09].

Message [BKR00, BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SN04, WS03, Zol01, BPS08, CCH06, CJ05, Gav08, HW05, MD04, MS09c, Sha04b, TJ03, Wu01, ZF05, ZAX05].

Messages [Ara02, AR01, Br00b, CHJ+01b, DS05b, Sch09, Wri05, Zho06, Alv00, An08c, BCG+02, Bil02, BB79, Lun09, SP79].

messaging [Opp01, RR05].

meta [SM08, PLJ05a, QC05b, Sha05d].

Meta-He [PLJ05a, QC05b, Sha05d].

meta-learning [SM08].

metadatum [CDS07, FJ04].

metamorphic [CSW05].

Metaphor [CNB+02].

Metering [BC04b].

Method [BDTW01, GHK+06, GL00, Gro01, HRS02, HQ05, JKK+01, Mö02, OKE02, OT03a, OT03b, SOHS01, TIGD01, TSO00, WH09, WNY09, ZL05, ÁMRP04, DwW05, Gut04c, JL03, MFP09, MFK+06, WG02, WWT08, kWpLwW01, WL04, YCO09, YCL07, CHJ+01a].

Methodologies [SPML02, ND04].

Methodology [VMS05, HM02a].

Methods [BCDM00, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TMM00, Vir03, Bau00, Bau02a, Bau07, BGM04, BCHJ05, CM05b, GKS05, JZC05, LMSV07, Mal06, SSST06, Shp99, YW06].

Metric [LBG01, LBG02].

Metrics [LZ01, NP07].

Mexico [Buc00a].

MGC'05 [ACM05a].

Micali [Des02].

Miccai [Rub00].

Michael [Ter08].

Micro [ASK07, Eng00, Ste05c].
Micro-Architectural [ASK07].

microcontrollers [GBK01].

Microelectronics [IEE09a].

Microprocessor [Web08].

Microprocessors [LKM+05]. Microscopic [MYC01]. Microsoft [Bon00, Scr01, Ste05b, Weh00]. Middle [Eag05, Gen04a, HG07, Kin01]. Middleware [ACM05a, KRV01, LGS01, MBS04].

Migration [Pat02a]. Mikhailovsky [Puz04]. Milan [dCdVSG05]. military [Ark05]. Million [Ran55, Ran01, Ano03a]. MIME [Dav01b, Dav01c, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [Eag05, Gen04a, HG07, Kin01]. Minimalist [Tro08]. Miniming [LPM05]. Mining [LP00, Lut03, HLL+02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [CC05e]. MinRank [Con01]. Minutiae [UBE09]. Minutiae-based [UBE09]. Misbehaving [JQY01, SBB05]. Misinformation [CZB+01]. Missed [TvdKB+01]. MIST [Wal03]. Mistakes [Ste05b]. MISTY [KYHC01, Kih01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Kih02b]. Mithra [Fre03]. Mitigating [NLD08]. Mix [JH00a]. Mixed [SKR02]. Mixes [Mol03a]. Miyazaki [WHLH03]. MMM [GKS05]. MMM-ACNS [GKS05]. Mnemosyne [RH02, HR02]. Mobile [Cha05a, Dim07, GN06, JP02a, KZ01, KB07, KC02, KHO01, LCK01, Mal02, PP06a, PKZD02, RdS01, RC01, Rot01, SH00, ZYM05, CC05c, CJO3b, DHMR07, HP00, HYS03, ISTE08, KXD00, LC03, LC04a, Lin07, LKZ+04, Par04, Pau02a, SSM+08, SL05a, TM06, TW07, Tse07, Wan04a, YC00a]. mobile-commerce [YCO9a]. mod [TM01]. Modal [GN01]. Mode [BR02, Dwo03, HR03, HKR01, KSHY01, SLG+05, WB02, Hey03, RBB03, ZLO4c]. Model [Abe01, Abe04, BH05, BPST02, BL02, CLK01a, CS07c, CPhX04, CHi08b, CT09, DPV04, DFS08, Din01, Din05, ECM00a, Gra02b, HLC08, KLN+06, KW03, LJL05, MN0+04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SFDF06, TZDZ05, Vad03, WCZ05, WT02, WvD02, ZGLX05, ZP05, ZS05, BKW09, CUS08, Dam00, DFS05, GMR08, HILM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SRJ01, TP07, DY09a]. Model-Based [Sal05b]. Modeling [AAD05, CDD+05, HMvLM07, KS05a, ZP05, Laf00, SS04]. modelled [BG08]. Modelling [HCD002, JP07, Puc03]. Models [Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01a, SC02b, vOT08]. Modern [Gol99, Mao04, Pag03, SM07b, Swe08, Bud06, Fur01, IM06, KL08, Mol05, SE01, Lut03, Lee03b]. Modes [DGH+04, Dwo03, GD02, Gol01d, HSH+01, JM02, JKR01, Jut01, KY01a]. Modified [CH04, HPC02, JO01, K101a, ST02, Che08a, CJ0101, HWWM03, LL04a, LL05a, kWP04W01]. modifying [CSV07]. Modular [BIP05, BKP09, CMJP03, CH07c, Dhe03, FP00, Gro01, Har06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wal01, WLO4a, HSD+05]. Modulation [AS01c, Che07]. Module [Ano02d, LM00, SGM09, ARJ08, BG09, Jan08b]. Modules [FIP01b, NS01b, GJ05, JE04, SE01b]. Moduli [Bai01b, GMP01b, Wal01]. Modulo [ACS02, Gnt06, Gro03, MF05, THe01, Wan05]. Modulus [Ano1k, CGH00a, CDL+00, S0101, WY02, WS02, LKYL00, WWH08]. Modulus-Based [WY02]. Mollin [Kat05b]. MOM [AJL01]. 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]. Monterey [USE02c].
Montgomery [CH07c, HKA+05, NMSK01, OS01, PS04a, TSO00, Wal01, WS03].
Montgomery-Form [OS01]. Montpellier
[KM07]. Montréal [ACM02]. Morocco
[IEE09a]. MorphoSys [Tan01]. MOSS
[Dav01b]. Most [GG05a, Shp02, Tyn05].
Mothballed [Bar00c]. Motif [Bi09].
Motion [EFY+05, hKLS00, WMDR08].
Mountain [JYZ04]. mouse [HLWZ09]. MP
[MP07]. MP3 [DRL09]. MPEG
[LHS05, MLco01, SG07, YZD007].
MPEG-4 [SG07]. MRF [Che01a]. MRN
[TIGD01]. MSXML [tem+01, Hei01]. Mu [CTJ03].
much [Con09]. Multi
[ARR03, BBM00, BR06, CCD07, CJK+04, CDM00, CDG+05, DLY08, DJL01, FGMO01, FWW04, Gen04a, HM01b, HS07, JLL02, Kur01, LV07, LLL04, Tsa01, ZJ09, BSSM+07, CLOS02, CC05a, CHY05a, CHY05b, DLZ01, FWTC05, GMLS02, HHYW07, HWH05, HC04b, HL04, LHL03b, LCZ05b, LW05c, NC09, PW05, SC05a, TWL05, TYH04, YCH04].
Multi-applications [DJL01].
Multi-Authority [JLL02]. Multi-channel
[ARR03]. Multi-designated [LV07].
Multi-Domain [CJK+04]. multi-factor
[BSSM+07]. multi-hop [NC09].
multi-linear [LL04]. Multi-party
[CDM00, CDG+05, FGMO01, FWW04, HM01b, LLL04, CLOS02].
Multi-property-preserving [BR06].
Multi-Proxy
[ZJ09, HC04b, LW05c, TYH04].
Multi-Receiver [CCD07]. Multi-recipient
[Kur01]. multi-scroll [HHYW07].
multi-secret [CC05a, CHY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server
[Tsa01, LHL03b, TWL05]. Multi-Servers
[HS07]. multi-signature [HHW05, HC04b, HL04, LCZ05b, LW05c, TYH04].
multi-stage [CHY05b]. Multi-trapdoor
[Gen04a]. Multi-user
[BBM00, DLY08, GMLS02]. multi-valued
[DZL01]. Multiagent [ZS05].
Multiagent-Based [ZS05]. multibit
[TND+09]. Multicast
[AIP01, BPS00, BDF01b, ASW00, GIKR01, GL06b, JA02, KB09, MP08, PCS03, YC08].
Multicollisions [Jou04]. Multilevel
[LN04]. Multimedia [AAK09, FMS05, GA05, HLO7, LRL07, SLO06, WLLL09].
DY09a, DU05, Laf00, Ren09, SG07, YC08].
Multimodal [PY09]. Multiparty
[BGOY08, CDN01, DNO3, DIO5, GIKR02, OZL08, CDD00, HTH04, KOS07]. multipath
[SK05b]. Multiple [AK+01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, DK05, Har00, HZSL05, HLT01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJ04, DMO7a, HL00, KC09a, MN14, Sha01d, SW05, TCC02, WY05, YSH03, YRY05b].
multiple-key [Che04a, CJO4, SW05, WY05, YSH03, YRY05b]. Multi-Precision
[HZSL05, MN14]. Multiple-watermarking
[Che08b]. Multiples [HR00].
Multiplication [AHR08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02c, KKK10, MLO02, NMSK01, OS01, Tan07a, Wal01, BIN03, DwWmW05, FP00, GD05, Has00, Mis06]. Multiplications
[Har06, OT03b]. Multiplicative
[Has01a, K003, MFT05]. Multiplier
[HKA+05]. Multipliers
[CMJP03, KWP06, RMM03b, WS05, HGNS03, RMP08, RMM03a]. Multiply
[KTT07]. multiprocessor [ISTE08].
Multipurpose [Boy03]. Multireceiver
[HSZI01]. Multiresolution
[hKLS00, YPS01]. Multiset [ASM01].
Multisignature
[Tad02, CWH00, CL04c, CCH04, He02, LC04b, LWK05b, Wu01, YY05a, ZY04].
multisignatures [CL00, WH02b].
Multithreaded [Zha00]. Multivariable [DY09b, BGP09, FP09]. Municipal [MJS+08]. Music [MNS01, XMST07].

__mutargima__ [MA05a]. Mutation [Lut02].

Mutual [JP02a, KH05, CCS08, VK08, YWWD08]. __Mutually__ [WC05a]. MYCRYPT [DV05].

__mysterious__ [Bel07a]. Mystery [GG05a, Rug04]. Myths [GO03, Kc01].

N [Mar05a, AOS02, KMM01]. NAF [OT03b]. Names [Coc01a, Sha02, Ark05, CGV09]. Naming [Ano01b, BH00b]. Nanotechnology [RR03a, RR03b].

Naor [Zha06]. Napoleon [Urb01]. narrowing [MT07]. NASA [Ano02c, Wi99]. Nation [Lan04a].

National [BWE+00, Jo01, LCS09, AJ08, Ban02]. National-Scale [BWE00]. Nature [Pag03]. Naval [LBA00, Goo00]. Nazi [Hau06, KS04]. NC [AIK04]. nCipher [Ano03a]. NCP [SQ01]. NCR [LB00].

Near [BC04a, DPS05]. Near-Collisions [BC04a]. Necessary [LCK03, MN01]. Necessity [SBZ02]. Nederlanden [dL00]. Need [Coc01a, HR04b, Sty04]. Needs [CZB+01, DKK07]. Negotiation [DBS06, HJLS04, IY05, LLWO, LLW09].

Nema [Kid00]. NESSIE [Pre01, Mac00, Pr02a, Pr02b, SGB01, DPVR00]. nested [LCK04]. Net [CAC03, Ano08b, LKL01].

Netherlands [Kmu02]. Nets [ADK05]. Netspionage [BK00]. Network [Ano02d, Ano03b, Bar03, BGOY08, Con04, CLZ02, Dim07, FBWC02, Gum04, Har05a, IKY05, JYZ04, KKG03, KPS02, Ken02b, LMP+01, Lu07, Mal02, NN02, PZDH09, PZL09, Poo03, RCBL00, RC05, Sty04, TLYL04, VMC02, YC01, ZYH03, ZS05, Bru06, CJ03b, CMS08, Coc01a, DWML05, GKS05, HLL+02, LC03, LPV+09, ME08a, MSK03, Mis08, Pri00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wy05, YLT06, ECM00a, ECM00b].

Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Ros07, VM03]. Networks [EAQ05, BJS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PRL01, RKZD02, Sin01a, WT02, ZEA00, ZYN08, ZWC02, AJ08, BBG+02, BC05b, CCMT09, CP03, CBD+05, DHRM07, ETMP05, HJ07, Hmvl07, JRR09, KXTZ09, KY08, KB09, LDH06, LHC08, LW05a, LLH06, Lin07, LN04, Lop06, LKZ+04, MWS08, MJF+08, MS09b, NC09, NL08, PCSV07, PS08a, Pat02b, SL07, SSM+08, TP07, TM06, TCR03, TW07, WDL09, XWL08, YC07, ZSJN07, ZBLB05, Ano02d, CS08b].

Neural [KMS02, PZL09, PR01, YC01, YC07]. Neural-Network [YC01]. Neveu [QSO00]. Nevada [EL00, IEE01a]. Never [Wei00, Hau06]. Newfoundland [NH03]. Newman [Pag03]. Newmanry [Sal01a].

News [Ano03c, Bar00a, Bar00b, Bar00c, Cla00a, Coc01a, Coc02a, Coc02b, Coc03, Eng00, Fox00, MYC01, MP00, PM00, Pau02a, Pau02b, Pau03, Pau09, Pri00].

CAC03, CAC06, Sta05, Raj06]. Newton [KT06]. Next [ES05+05, MC06, TV03, Web08, BD04b, ISTE08, RR03a].

Next-Generation [ES05+05, Web08]. NFA [DS02]. NFS [Sta02a]. Nice [DS06, JJ00c].

Nicko [Ano03c]. Nimbus [Fur02a, Mac00]. nine [Tat05]. Ninth [USE00d]. NIST [BG07a, Dra00, Hr09, Ke05, RR06, SF07].

NIST-Recommended [Ke05]. NMAC [RR08]. NMAC/HMAC [RR08]. NNAF [DwWm05]. No [Sta05, Sty04, Uni00g, Wei06, Wei05, CC05b].

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

Nodes [ZYN08, RAL07]. NOEKEON [DPVR00]. Noise [BKW03, GA05].
MPSW05, SDMN06, MS09a, PC00].

noise-based [PC00]. Noise-tolerant [BKW03]. noisy [HGNS03]. Nominative [PL01]. Non [BR05, CHK05, CZB01, DN00a, DDO01, DW09, FF00, Fis01b, Fis05, FGM00a, FGM00b, HNZI02, HJW01, IYK02, IYK03, JT01b, Kos01c, KOO00, MSTZ04, Nie02b, PHK01, Pas05, SPK08, WBL01, DM07a, DS02, Huh00, HLL04, IM06, KKL09, KHL09, LSA07, PR05, RP00, SC05c].

Non-adjacent [JT01b]. Non-committing [DN00a, Nie02b]. Non-Cryptographic [WBL01, IYK02, IYK03]. Non-injective [Kos01c]. Non-interactive [CHK05, DDO01, Fis01b, Fis05, HNZI02, HJW01, MSTZ04, Pas05, KKL09, KHL09].

Non-interference [BR05]. Non-malleable [BW09, FF00, PR05]. Non-maximal [HJW01, Huh00]. Non-OOSD [CBZ01].

Non-perfect [DM07a]. non-physicists [RP00]. non-quantum [IM06].

Non-repudiation [HLL04, LSA07, SC05c]. Non-trivial [KO00]. Non-Uniform [SPK08]. nonce [CY05, LKY05a].

nonce-based [CY05, LKY05a]. Nonces [BR00a]. Noncontact [Sak01].

noninterference [DFG00]. noninvertibility [HRS08]. Nonlinear [BP01a, BI05b, CV02, Che01c, LBZ01, LBZ02, SM00a, ZC00, BGPG05, CFVZ06, KH08]. Nonlinearity [SM00b].

Nonnalleable [ABW09, DNN00, DNN03, PR08]. nonreputable [TYH04, YTH04].

nonreputation [HW05, OZL08]. Nonsecurity [Sch07]. Nonuniform [CU01].

Normal [Ran55, Ran01, GPS05, Mic01, RMH03a].

Normalization [VK07]. Norway [Ytr06].

Nose [Fox00]. Notarized [GTY08].

Notation [Eag05, Kin01].

Note [CWY05, FS02, 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, HC08, MP01c, WCJ09, AJ08, BG08, CSS08, GB09, HG05a, SP02, SCS05a, MShF05].

November [ACM01b, ACM05a, BZ02, CLK05, Eke02, IEE00a, IEE02, Lai03, LL03, LL04c, MS05b, PK03].

novice [Dew08, Gou09]. Novo [Bou09].

NP [AGGM06, FS08, HN06, AGGM10]. NP-hardness [AGGM06, AGGM10].

NPCryptBench [YLT06]. NSA [RC05].

NSS [GJSS01, HPS01]. NT [Str01b, USE00a]. NT/2000 [USE00a].

NTRU [GJSS01, GS02c, HPS01, HG05a, HG07, JJ00b, NP02b].

NTRUEncrypt [HG06, KY09].

NTRUSIGN [HG06, HG06, HWH08, ZJ09].

NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CDO1a, CFS05, Di03, DGP07a, DGP07b, DV08, Ead05, EHK03, Fin06, Gou06, GPR06, Hig08, Int03, Kat05b, Ke05, Ket06, KM01b, LMHCET06, LNS02, MNP01, NR04, RSN01, SP05, Sch06b, Shp99, Shp03, SFDF06, TWA08, TL07, TMT09a, TMT09b, Vav03, Wal00, YW00, YKL02b, Aam03, AUW01, BK07, Bel08, BGPG05, BG08, BG09, BG07a, BGL03, CNPQ03, CO09, DIM08, DGP09, FPP00, HG05a, HGNS03, HLWZ09, HP01, JAW00, JL03, K08, KS00, Kin01, Lam01, Mit00, Nie02a, Nie04, Pan07, PSG09, PSG08, PC00, RGX06, Sh05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Was08b, YZEE09].

Number-Notation [Eag05, Kin01].

Number-theoretic [NR04]. Numbers [HRS01, HBF09, IPR00, MN01, ST03b, AG09, HW98, KB39, Kru01b, MFK06, SS03, Shp05, Tip27]. numeric [AKS04].

Numerical [WWL02]. numerically [Sav04]. Numerous [CC08].

NURBS
optimality [NK06]. Optimised [TL07].

Optimistic [CC00, DLV08]. Optimization [Ken02a, Krc05, KV01, SMTM01, TLYL04, WPP05]. optimized [LC03]. optimizing [Dwi04].

Optimum [KWP06, OKS06]. options [Fri07, Pot03]. Oracle [ABR01, Abe01, Abe04, BF05, Chi08b, Gra02b, Nie02b, Pas03, Ano02c]. Oracles [BNPS02, BB04, KG09, RG09].

Order [AKSX04, Bai01a, CV02, KCP01, KCI01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Coh03, JZCW05, KS06b, QPV05]. Order-Specified [Tad02].

oriented [HY03, WL05]. Ordering [Mea04]. Orders [HJW01, PS02b, HM00, Hii00].

Organizational [PTP07, BJ02]. organized [AUW01]. Oriented [HR00, LZX01, SKU00, ZCC01, CHC05, CWJ01, DHL06, HWW04, LL06, LWZH05, MWM01, Sae02, Sha03c, TJ01a, WHHT08].

Origin [MAB06, MD04]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Orsay [DPT02].

oscillator [BGL03, GB09]. oscillator-based [BGL03]. oscillators [SPG02]. Other [BF05, Ngu05, Wri05, Cla00b].

Otherworldly [MYC01]. Ottawa [AMW07, MZ04]. our [Sta05]. ourselves [Fur05]. Outbound [Smi02]. Output [Dic03, YJ00].

OutputSource [HL05a].

outsourced [MSP09, MNT06, YPPK09, YLC09].

overcoming [CHC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, Ino05].

overhead [HGR07, IK0808, RSP05].

overheads [XLMS06].

overlays [SK05b].

Overshadow [CGL08a, CGL08b, CGL08c]. overview [SEV09]. Ownership [AS01b, Nik02a, Nik02b, CL08, Lin01a].

Page [Puc03, AKS02, KR03]. P1363 [IEE00b].

P2P [BRTM09, STY07, WJ02, YLR05].

P2Ps [LHL08]. PA [Cor00a, WWCW00].

PA-RISC [Cor00a, WWCW00]. Package [Win01].

Packet [BR09, WRW02, WLZ05, CMS08].

Padding [AR01, BCC01, CKN00, CJNP02, KO03, LS01a, Man01, Vau02].

PadLock [Lud05].

Pagination [GPC08].

Pages [Fal07, Rot07].

Paradigm [BN00a, CS02, Gol03, KDP04, BKN04, Can01a].

Panoramic [YN01].

Paper [CC09, MFS09, Pet08].

Papers [Ano04a, Ano07b, Ano07a, Sch00b, Ytr06, Wil09, Bla03, Chr01, CMMR02, CMMR05, 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].

Paradigms [Des00b, Swa01, Hro05].
Paradise [USE00b]. Paradox [Che01b].
Parallel [AHRH08, App07, AEMR09, CPhX04, CTLLO1, CNPQ03, CNB+02, Dam07, DM00b, JL08, KY02c, Lin01b, MFS+09, PS04a, RMH03b, SS01a, BF06a, FP00, OS07, RMPJ08]. parallelism [KVN+09]. Parallelizable [BR02, Mäö02]. parallelizing [Fis01a]. Parallizable [LKKY03a, LKKY03b]. parameter [Wue09]. Parameterizable [KPMF02]. parameterization [LZP+04]. Parameters [ZLK02]. Paris [ACM04a, GH05, KNP01, NP02a]. Parity [DRL09, KKG03, You01, BKW03]. Parity-Based [KKG03, DRL09]. Park [Cop05, Cop06, HS01a, Sal00b, Sal05a, SE01, Smi01b, Wei06, Win08]. Part [Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05]. Partial [BM03b, Cor02, Her06, ABHS09, CP07]. Partial-Domain [Cor02]. Partially [AO00, MSP09, Bao04, Fan03, HC04a, HY03, HLL03, WL05, WLHH05, WY05, ZC05]. Participatory [CTBA+01]. parties [LKY05b]. Partition [CTH08, WJP07]. Partitioned [DN04]. partitioning [BF06a, Che07]. partitions [Sav04]. Party [KO04, Lin01b, MR01a, WW05, WV01, CLO02, CLO08, CDM00, CDG+05, FGM01, FW004, GCKL08, HM01b, JW01, LLL04, LLS+09, LSH00, YC09a, ZLX99]. Pass [SK00, MT02]. passe [Car00]. Passes [Coc03]. Passing [Vir03]. Passive [Sha01c, VV07, RW07]. Passive-Only [VV07]. Password [BMN01, BMP00, CHV03, CPP04, CS07b, DG03, GL03, GMR05, Har01a, Har01b, Jab01, KOY01, LSH03a, LSH03b, MPS00, Mac01, MSJ02, Ngu05, SBEW01, SY06, WIL05, YS04, ZWCY02, CC01, CC04b, CCK04b, CYH05, DG06, Fur05, GL06a, HT08, JM07, KLY03, KJI05, KTC03, KCL03, Ku04, KCC05, KHL05, LIL06, LFW04, LC04a, Sco04, Shi05, XwWL08, YW04, YWC05, YS02, YPKL08, ZDW06]. Password-Authenticated [BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HT08]. Password-Based [CPP04, CS07b, GL03, SBEW01, SY06, YS04, GL06a, KHL05, ZDW06]. password-guessing [Shi05]. Passwords [GL01, KOY01, Per03, Smi01c, An03c, FZ06, KOY09, NS05a, RD09, YWWD08, vOT08]. Patarin [Bih00]. Patent [MP00]. Path [GXT+08, CCD+04, Dew08, ZSN05]. path-based [CCD+04]. Path-quality [GXT+08]. Pattern [ABM08, BDhKB09, BLP06, BCC01, LS01a, TIGD01, Bau06, LYGL07]. Pattern-based [BLP06]. Patterns [DD02, MP06, WCJ09]. Pay [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06]. Pay-as-you-watch [Joy03a]. pay-as-you-watch [Joy03a]. payload [KC09a]. Payment [MV01, RMCG01, YKMY01, Has02, HP00, SH00]. PC [BSW01, Ste05c]. PCIXCC [AV04]. PCKS#7 [Dav01c]. PCPs [FS08]. PCs [BD06]. PDF [IS05, CNB+02, ISO05]. PDF/A [ISO05]. PDF/A-1 [ISO05]. Pearson [Puz04]. Pebbling [DNW05]. Pedersen [GJKR03]. Peer [HR02, RH02, ATS04, LLY06, MPH06, PI06, WCJ05, Yi04]. Peer-to-Peer [HR02, RH02, ATS04, MPH06, PI06, WCJ05]. PeerAccess [WZB05]. Peinado [YRY05a]. PEM [Dav01b]. Penguin [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a]. Pennsylvania [IEE05a, IEE08]. People [ASW+01, CG05, Lov01]. Perceptual [PBM+07]. Perceptually [EFY+05].
Perfect [AJO08, CLLL00, DN02b, DSS01, Sun00a, DM07a, SC02c, SY06, ZD05].
Perfectly [AJO08, CLLL00, DN02b, DSS01, Sun00a, DM07a, SC02c, SY06, ZD05].

Perform [Kin00]. Performance [ACM01b, BHO0a, DPR01, Dra00, EYCP00, FZH05, Int00, Ken02a, Ken02b, Kra05, LWK00, MM01b, NFQ03, PWGP03, PBTW07, SKKS00, SW00a, SB01, Siv06, SL00, SGPFI98, WBRF00, WWCCW00, WS02, XH03, YEP+06, Zea00, AKNRT04, BVP+04, BZP05, CKL+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTW07, YGZ05].
performance-friendly [CRSP09].
periodic [XQ07].
Periods [KKH03]. Perl [Sal03b].
Permutation [DMS00, HSR+01, IYK02, KKG03, KO03, LSY01, DP02, IYK03].
Permutations [BPR+08, CHL02, KO00, MP03, KKKP05, WV00].
Persistent [AGT01, ST06]. Person [KJR05, LLT+04, PK01, BS01b, KN03, Li05, LST+05, PY08].
Personal [Bar05, EHMS00, SEK01, SEK02, PKP, Pioneer [Coc03].
Personalized [GPC08].
Perspective [LL01]. Perspectives [BMV06, SM08].
Perturbation [HWH08, ZY08]. Pervasive [BDKB09, JW05, LKHL09, Lut03, Lut03].
PET [MS05a].
Petersburg [GKS05]. petitions [Cal00b].
Petri [LKJL01, AADK05].
Petro [ML06, Ano00b, BCH+00, Dav01b, Dav01c, JKS02, Luc06, Opp01].
PGV [BRS02].
pharaohs [Pin06]. Phase [CDF01, Iglo2, KLB+02a, Che07, Che08a].
Phase-Conjugate [Iglo2]. phase-shift [Che08a].
Phil [Bar00a].
Philadelphia [IEE08].
Phil [ML06].
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 [Clu00b].
Picks [PM00]. PicoDBMS [PBVB01].
PicoDMBS [BBVP00]. Picturing [Pau03].
Piecewise [LLL+01].
piling [Kuk01]. piling-up [Kuk01].
PIN [BZ03]. Pioneer [Coc03]. PIPE [CBD+05].
PipeLineed [MD05, Mis06].
Piper [BIM00].
Pirates [KY01d]. PISN [Ecm00a, Ecm00b].

Pixel [DS08, WCJ09, BCD06, LYGL07, WWTH08].

pixel-pairs [LYGL07].

Pixel-Value [DS08, WWTH08].

PKC [BDZ04, Des02, Kim01, NP02a, Van05a, IZ00, KI01a, KI01b, ZC04].

PKC'98 [HPC02].

PKCS [Chu03, Man01, RSA00c, RSA00b, RSA00d, RSA00e, RSA01, RSA02, RSA03b].
PKCS#1 [CJNP00].

PKCS#11 [DKS08].

PKCS#7 [Dav01b].

PKI [AL06, CZ05, KGL04, Ahm08, ES00b, ES00a, Gar03a, Gut02a, Hoo05, NDJB01, Ort00, St00].

PKIX [FL01b].

PKP [JJ01].

PKWare [Bar00a].

Place [USE01b, USE01a, GS07b, IEE09a].

placement [GJJ05, JEZ04].
Plain [Col03].

Plaintext [DN02a, Fur02b, GK05, HLM03, Jo01, KI01a, KM01c, KI01a, MF01, CKN06].

Plaintexts [BR00a].

Plan [CAC06, CGP+02, Gun08]. plane [WL02].

Planning [WCZ05]. plans [Ark05].

Platform [Bau02b, MMH02, PZDH09, ARJ08, ISTE08].

Platforms [AIK+01].

Play [WD01a].

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

Pluggable [Sei00b]. plus [Cop04b].

PODS [ACM03c, ACM05b].

poetry [MAaT06].

pogromca [Kap05].

Point [GLV01, M502, NS05c, USE00b, WW06].

point-sampled [WW06].

Points [BGJ08, Gau02, Cla00b]. poised [CH00].

Poisoning [Kle07].

Poland [AUW01, Bih03].

Polarization [HR05].
Poles [KS04].

Policies [AEV+07, ZP05, BNP08, LJY04, RN00a, RN00b].

Policy...
[Bla01c, HQ05, Ano00e, BFG08, BZP05, DFM04, Gor05, RVS09, Uni00b, RR04].

**policy-based** [BFG08]. **policy-compliant** [RVS09].

**Polish** [Kap05].

**Politics** [Cho08a, DL98, Jan08a, DL07].

**polyalphabetic** [GPG06]. **Polygonal** [Ben00, BB00a, BGI08, SP04].

**polymorphic** [CSW05]. **Polynomial** [AF03, BIP05, BDG01, Bul09, CU01, CJ03a, CH07c, CLZ02, DS05a, Gon06, HR00, KL05, KY01c, KTT07, LW02, May04, Pli01, RMH03b, Sat06, LFW04, MRST06, SZP02].

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

**Polynomials** [BLST01, DS08, FL06, Jam00, JJ00d, Lan04a, CH01, FF09, GS09].

**Pon** [QCB05b].

**Pool** [BTTF02].

**Popular** [RR08, CAC06].

**Port** [Kra02b].

**Portable** [Hei07, Wan04a].

**Portfolio** [Ano02e].

**Portland** [ACM00, BCDH09].

**Possessing** [CC08].

**Possession** [Tee06].

**Possibility** [SF07, BGI01, DOPS04].

**Possible** [Mur01].

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

**Post-Quantum** [AKS06, Ano00d, Ava03, BI05b, BNPS02, Cry00, DPV01, DBS06, Gir06, Has01b, HM02c, HBF09, IIT03, JP02a, QY01, KBM09, KLY02, MOP06, Mas04, MS01, MMMT09, Mes00, Mes01, MG08, OS00, OS06, ÔØ03, PSG09, Sha01c, Sma03b, WS05, WC01a, vW01, CBSU06, CO09, Geb04, Mit02, OS08, XH05, ZYW07].

**Power-Analysis** [ÔØ03].

**power-attacks** [Geb04]. **power-aware** [CBSU06].

**Power-Sum** [KL02].

**Power-Up** [HBF09].

**Pp** [Eag05, Pag03, Top02].

**PPC** [ASW01].

**PPK** [YDKM06].

**pq** [KOMM01].

**PQCrypto** [BD08].

**Practical** [Ano01c, AR01, Ash03, ACJT00, BDK09, BF05, BLMS00, CS03a, Cap01, CDR01, Chi08a, CS03b, DK01, Dre00, FS03b, GSS03, GIS05, GH02, HQR01, HJW01, Ina02a, Ina02b, IT03, Kan01, LM05, LCD07, Lutt03, LWK05a, MM02, MSU05, OM09, PBD00, Poi02, Poo03, Roy00b, Sug01, Wei04, YSS01, Bro05b, DKL00a, Har05a, KSW06, Luc06, Mos06, MSV04, Sha01a].

**Practice** [AL06, BD20, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti95, Sti02, Sti06c, Lut03, Spr03].

**practices** [Ste02].

**practitioners** [PP09].

**pragmatic** [BMW02b].

**Pre** [Ad03, AA08].

**pre-processing** [AA08].

**Precise** [Wal01].

**Precision** [HZLS05, SR06, LMC03, MN14].

**Precomputation** [SLG05].

**predecryption** [RSP05].

**Predicate** [Be08].

**Predicting** [AG09, BPGS05].

**Predistribution** [HMvdLM07, JRR09, TP07].

**Prefix** [CGM07].

**Prepadding** [FXAM04, RW07].

**Prefix-preserving** [FXAM04, RW07].

**Prehistory** [Ifr00].

**Preliminary** [KS00b, KKS00b].

**Prentice** [For04].

**Prentice-Hall** [For04].

**Preprocessing** [BIM00, CCK03].

**presence** [BIW08, GXT08, MI08, VS08].

**Preservation** [Che01b, Dur01, Bro05a, ISO05].

**Preserve** [NNT05].

**Preserving** [DN04, KPS05c, LP00, Mä03a, YWD08, AKS04, BR06, BSMS07, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07].

**President** [Gen00a].

**Press** [Inar03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03].

**Pressure** [HWH01].

**pretty** [vOWK07].

**Prevent** [FOBH05].

**Preventing** [CS07b, CL09, HSW09, ID05, 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 [Ano03k, Sze01, Ste08, AKS02]. Primitive [CFS05, YK02, IMM01, ST01a, ST02, YK03]. Primitives [BDFP02, CHL02, FGMO01, Ngu05, RR00, BDFP05, Gar05, JZCW05, RAL07]. principal [ZL04b]. Principle [CZK05]. Principles [ACM03c, ACM05b, DK02, DK07, KL08, MAA07, SB07, Sta02a, Sta06]. Print [Kra02b]. Printed [SLT01]. Printer [Bar00a]. Priority [WWL+02]. Privacy [Ano00i, AEV+00, BBDP01, BSS+00, CDM+05, Cho08a, DL98, DL07, DFKX05, DN04, KS02a, GMM08, HY01, KS05c, Knu07, LP00, MP00, Pap05, PB05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YW08, Be04, Bjo05, BA06, Brah01a, CLR09, CKN06, HJW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZYL05, ZSM05, MS05a, Jan08a]. Privacy-Enabled [Por06]. privacy-enhanced [ZSM05]. Privacy-Enhancing [SE09]. Privacy-Preserving [DN04, KS05c, YW08, BA06, HJW05, Pin02, Pin03]. Private [AF04a, AF06, BDF+01a, BIM00, BY03, BS09, BIL02, BGW05, IS03, KO00, OS05, SDMN06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PL05b, Sun02, YRS+09, ZY08, ECM00a, ECM00b]. Private-Key [BY03, KY00, PL05b, Sun02]. prize [Fox00, Coc02b, MNT+00]. PRNG [HSS04, Mur02, SF07]. Proactive [DBS01, FMY01, JSM05, ZSV05]. Probabilistic [CCW02, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLMM05, G099, JZCW05, KY00, MRST06, PBMB01, dH08, Neu04]. Probability [KMT01, MNT+00, DLP+09]. Probing [ISW03]. Problem [AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK+02, Con01, CLZ02, DIS02, DHR00, FL06, Gen03, GV05, GPP08, KK02, LNS02, NBD01, Wag02, BKW03, CCG06, CJT04, DLMM05, HGNS03, Hsu05a, LHY05, LD01, Luk01, Pei09, Shp05, SCL05, WL02, Whi09, Yas08, KMT04a]. problem-solving [Whi09]. Problems [BI05a, Can06b, MV03a, OP01a, TvdK+01, VDKP05, HL05d, KXD00, LMTV05, LMC+03, RSS04]. Procedure [LY07]. Procedures [DJ06, BBK+03b]. Proceedings [ACM00, ACM02, ACM04a, ACM05a, AAC+01, Bon03, EBC+00, FMA02, FLA+03, SM07b, USE00c, USE00b, USE00a, USE00d, USE01b, USE01c, USE01a, USE02a, USE02c, USE02b, WK03, Yun02a, ACM05c, ACM07, ACM08, ACM09, EUW01, AJ01b, BS03, Be00, B+02, Boy01, Buc00a, BC01, HA00, Hon01, IEE00a, IEE01a, IZ00, Kil01a, MS05b, Oka00, PPV96, P010, Pre00, QS00, RD01, Roy00a, SMP+09, ST01d, VY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BDZ04, BS01b, BCDH09, BD08, CC04a, CV04, Chr00, Des02, DFPS06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE05b, IEE07, IEE08, IEE09b, JY04, Jef08, JM03, Joy03b, JQ04, KJR05, KLG04, Kim01, Kim02, KM03, Knu02, KP01, KN07, La03, Lee04b, LTT+04, MMV06, MJ04, May09, MS02c]. Proceedings [Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sma05, Svy02, TJ02, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZYH03, BCC05, Cra05a, DV05, DWML05, DKU05, GKS05, IKY05, Kil05, Li05, LST+05, Men07, Poi06, Sho05a, Son00, dCdV05]. Process [Kwo03b, MNT+00, BKFP02, HL06, MRST06, VKS09]. Processes [BDP02, ALV02, BDNN02, Whi09]. Processing [ISSZ08, KLB+02b, PCK02,
AA08, AA04a, YPSZ01]. Processor
[Ano02e, BBGM08, EP05, FBWC02, FZH05, GC01b, Int00, KBD03, KPMF02, TYLL02, ST03a, SHL07]. Processors
[TLYL04, CW02, CRSP09, Geb04, LJ05a, YGZ05, YLT06, ZYLG05]. Procurement
[Lad06]. produce [Zir07]. producing [Zir07]. product [KSWH00, Sun02].

Products
[ACS02, Ano02d, Ano02e, Knu07, Ano00c]. professional [Dew08, vT00]. proficiency [Dew08]. Profile [PJH01, RSA00c]. Profiles
[MV01, PJK01]. Program [Hö01, Bec02, GGH08, Kov03, KH03, CS08b].

Programmable
[Dam07, GC01a, HV04, Svi02]. Programmer
[Wil01b, Bon01, Che00, DKK07]. Programmers
[Coc01a, Wei04, Gou09]. Programming
[ASW01, Ano02d, Coc03, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03].

Programs
[BGI01, Ark05, SLTB06]. Progress
[KK06, KFSS00, RD01, Roy00a, CV04, DV05, JM03, MMV06, MS02c]. Project
[Fri01, IY00, MNT00, Pau02a, Saixx, Gou09, LR01, Lov01, MWM01, Sha01a, Coc01a, Coc02b, IY00, Pre02b].

projects [Gha07]. Prolog [Bl01a, Bl01b].

Promise
[Ano02f]. promises [Pau02a]. promte [WK05]. Promotes [Bar00b].

Prone
[MCL01]. Proof
[Abe01, Abe04, AS01b, ARC01, BDP02, Cor02, GK05, SOIG07, SPMLS02, Tee06, BR05, GM04, HSD05, LMW05, PBD07].

proof-of-compliance [LMW05].

Proof-of-Concept [ARC01]. proofing [CT02]. Proofs
[BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, Goll99, HG05b, SV08b, dH08].

Propagation
[LJL05, QPV05]. Properties
[ABC05, BM01c, KY01b, LLL01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].

Property
[LPZ06, Qu01, Uni00h, WY02, BR06, JRS09].

Proposal
[DPVR00, Mac00]. Proposed
[Coc02a, GM00b, HPC02, Ki01a, You01, YG01c, JK01a, ZDW06]. Protect
[ETZ00, BBN09, WK05]. protected
[CYH05, PKH05, ZCL05]. Protecting
[Des00c, EHMS00, KY01d, Kra01, LKM05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYLG05].

Protection
[CGJ02, DKFX05, ECG07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL08a, CGL08b, CGL08c, CT02, Gor05, Kov03, KH03, Kwo03a, LL05b].

Protection [JT01a]. Protocol
[Ano01a, Be101, BPT02, BL02, CK02a, CJ03c, CWY05, Cim02, ECM00b, Fre03, GJKR03, GL00, HS07, JP02b, JRFH01, JT05, KLN06, Kuk06, Kra05, Ku02, LCK01, Mea01, MS05, NS01b, Ru00, RMCG01, SK00, Tan07b, TZT09a, TZT09b, WHL05, YSR01, BP03a, Bl01b, BDFP05, BK05, CS04, CCK04a, CC04b, CY05, CC05c, CYH05, Che04a, CLC08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, GTZ04, HT08, HWWM03, HHC05, KH08, KKL09, KTC03, LC03, LF03, LKYY03a, LKYY03b, LW04, LHL04, LKY05b, LKY05c, LHC08, LSH03a, LC05b, Lku01, MS03a, Par04, Pau01, RG06, Shi05, SW05, SIP04, TM06, Tsa06, Tse07, W05, Wilt05a, WHHT08, YW05, YT05, YC09a, YS02, YSH03, YRY05b, YRY05c, YPK08, ZW01, ZL04c, ZDW06, ZY07, LSH03b].

Protocols
[AADK05, AL00a, AAFG01, BP04, Bl01a, Bl02a, Bor01, BM01, BM03c, Bra01b, BLDT09, CKPS01, CT08a, CCMR02, CCMR05, Cir01, CNV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, JP07, JW05, KS00a, KY03, KL08, Kra03, Kıs02, MS02a, MN01, PB00, PR08, PZDH09, Rot01, Shy02, SC01, Tee06,
AA04b, AKNRT04, Bar06a, Bau05, Bel07b, BDSV08, BFGT08, BP05, BLP06, BD04a, BR05, Can01a, Can06a, CP07, CKRT08, CWJT01, CH07a, Cho08b, Chr00, Chr01, CJM00, Coh03, CC05d, CDL06, DFG00, GJ03, GJO4, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV09, LLL04, LLY06, LLS09, Mec04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SR00, SW06, SY06, YS04, ZLX09, ZL04b, PDS09, Puc03.

ProtoMon [JT05]. Provability [GOR02b]. Provably [HM02b, HLL01, HSL02, KSHY01, PBD05, SLL00, BGP09]. Provably [AO00, ACJT00, BMP00, BCP01, BCP07, CHKO08, DG03, DG06, Hlav02, Hv09, HL07, HS07, JM02, Mo03a, NS05, NSS02, VMS05, Xso4, ZL05, BKN04, CCMT09]. provenance [HSW09]. Provers [MV03a]. Provide [AB01, Sch01a]. Providence [IEE07, Sil01]. Provider [LDM04, HILM02]. providers [MV03b]. Provides [OT03b]. Providing [BACS02, BDS09a, Del07, Lin07, Par04]. Proving [Che03, FS01c, GNO1, Tee06]. Provision [Kha05]. Proxy [AH05, BC05a, DFKX05, LCK03, LC05b, PL01, Rds01, Sha03d, ZJ09, AFGH06, CCH04, DY09, HW03, HW04, HW05, HW05, HC04b, KHL09, LL05, LHH05, LC05c, LW05c, PKH05, Sha05b, SHT05, TY04, YTH04, ZL05]. proxy-enabled [DY9a]. proxy-protected [PKH05, ZLC05]. psBGP [vOWK07].

Pseudo [BH05, FWW04, Gen00b, LLL01, LHL08, MP03, SX01, TTT09, TTT09b, WP03, BG09, GB09, MF06, NR04, PPO8, RGX06, SL09, WW08]. Pseudo-Random [LLL01, MP03, WP03, Gen00b, SX01, MF06, NR04, RGX06, SL09, WW08]. Pseudo-Ransom [BH05].

Pseudo-signatures [FWW04]. pseudonoise [HG05a]. pseudonym [CG06]. pseudoprimes [ZT03]. Pseudorandom [CD05, DN02a, DI05, DP02, Fin06, Fhu02b, FIPR05, GM02a, IY02, LHMC06, NRC02c, RSN01, Aam03, BGPG05, IY03, KSF01]. Pseudorandomness [GM02c, IK00, IK01, KYC01, LL01, Lee03b, MV00, Shp03, Go99]. Psychology [MYC01]. PUB [Nat00]. Public [ANS05, AUW01, APV05, An01j, AEAQ05, AF03, BC05a, BDG01, BDZ04, Bar00c, BPS00, BB00, BD01, BL01, Bih00, BDTW01, BST02, CHK03, CHK05, CM05, CHM02, CHK08, Chi08a, CCW02, CT09, CCM01, CS02, CS03b, DPV04, DJ01, Des02, DY09, DKXY02, DFK03, ESG05, ES00a, ED03, FL06, FL01b, GML02, GH01, GC01b, GUS04, GUS04b, HCD02, HR05, HG05b, HR04b, HJW01, HLC08, IEE06, IZ00, Jno02, Kat05b, KKM01, Kno01a, Kim01, KLY02, KKY02, KY02c, KLC00, KI01b, KM04b, Kos01a, Kos01b, KOM01, KY01e, Kuo01, LL02, LP03, LV00, Len01, LPS06, Lin03, Lin00b, MR01b, MR01c, Mo03a, Mo03b, Mu01a, NP02a, NBD01, NSS02, OTU00, PH01, Pei09, PR01, Poi02, PHM03, Qu01, RSA00a, RKZD02, ST01a, ST02, Sin01a, Sni01c, Ste01, TSO00, TTO01, Vau05a, WZW05]. Public [WYH01, WVO0, Wya02, YK01, YG01c, YDK06, Zhe02a, AG09, BHM03, BCL05a, BCW05, BBN09, Ben01a, BBT99, Bra01a, BD04b, Cal00b, CCT08, CL02b, CW00, CCH05, CJ05, CR08, Cho06, CRE00, DMT07, EKRM01, EHH04, FMY02, FP00, Gal02, GH08, GKM00, GS01, Gor05, GWM01, HCD08a, HCD08b, HHG06, HW04, HL04, Iwa08, IM06, Jno08b, JXW05, JZCW05, KPS02, Kob00, KW00, Kos01c, LF03, LKY05b, LCK04, LL08b, LS01c, Lop06, LKW05, MWS08, Mu01b, PI06, PC09, SN00, SR01, Sha04b, Sha05b, Shp04a, SL05, Sun00b, SZP02, SC05c, TO01, TLH05, Tsa05, TJC03, VS01, WDL09, War00, Wu01, WH03, WL04b,
hY08, YRS+⁰⁹, ZSM05, AL06, BDZ04, Ben02, CZ05, Des02, GL05, KGL04, Kim01, NP02a, Vau05a, YDKM06. Public-Key
[Ano01j, AEAQ05, BC05a, BM00, BBDP01, BLM01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DPV04, DJ01, 
DFK⁺⁰³, ESG⁺⁰⁵, ES00a, CH01, KLY02, KKY02c, KLC⁺⁰⁰, KI01b, KM01a, KY01e, Kur01, LP03, Lin03, Lin00b, MR01b, 
MR01c, Mō03a, Mol03b, NSS02, OTU00, Poi02, RSA00a, ST01a, ST02, Sin01a, TS00, TT01, WH01, YDKM06, AUV01, 
ED03, HG05b, Pei09, BHM03, BDN04, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HHG06, Iwa08, Jan08b, 
JXW05, JZCW05, Kos01c, LF03, LS01c, Lop06, MWS08, Mō03a, SN00, Shp04a, SLC05, Sun00b, TO01, ZSM05, GL05].
Public-Key-Based
[YKMY01]. Publication
[Top02, DGMS03]. Publications
[Bee05]. publish, publiques
[SL05b]. publish-subscribe
[SL05b]. Published
[MS03b]. publishing
[Ano02d]. puce
[Car00]. PUFs
[MK09]. Purpose
[Ano07b, Ano02c, Ano02d, Ano02e, Ano02f, Ano02g, Ano02h, BYJK08, BOHL⁺⁰⁵, BBD09, BZ02, 
BBB⁺⁰², BB03, BLMS00, BEM⁺⁰⁷, Coo03, DFS04, DPS05, DFFS08, DMS00, Ellis04, Ett02, GKK⁺⁰⁹, GH02, GW00, GRTZ02, 
HV09, Hay06, In01a, In02b, Kah06, KK06, KLB⁺⁰²b, LB04, LW05b, NA07, OTU00, PC09, Rec01, RK05, Ser06, SR07, 
TO01, Wi09, Wri00, Y00, Y10, ZLG01, ABW09, An03b, An06b, BYJK04, BCG⁺⁰², Ber09b, BEZ00, BEZ01, BLRS09, 
DFSS05, Duv03, Eke02, GKK⁺⁰⁷, Gav08, HHG06, IM06, JZ09, JRS09, JAW⁺⁰⁰, Joy00, Ko07, KO08, KKKP05, LQ08, 
May01, NK06, Pin06, RP00, Sin99, Sin00, Smo04, UHA⁺⁰⁹, BZ02, BD08, BD09].
quantum-storage
[DFSS05]. quarter
[Ko00]. quarter-century
[Ko00]. quarters
[Zhe02b]. QUARTZ
[PCG01]. Quasi
[MD05]. Quasi-Pipelined
[MD05]. Quasigroup
[MSNH07]. Québec
[ACM02]. Queen
[Rec01, Sin99]. Queenstown
[Zhe02b]. queries
[CKK03, Fis01a, GPC08]. Query
[GA03, PT08, PCK02, BKW03, PM08, YLC⁺⁰⁹]. Query-preserving
[GA03]. querying
[FJ04, UG08]. question
[OC03]. Questions
[Ett02, Joh00, Jac00]. Queues
[WWL⁺⁰²]. queuing
[CUS08]. quick
[Dew08]. R
[Kat05b, Pag03, Spr03, Bih00]. R&D
[Mau05]. Rabbit
[BVP⁺⁰⁴]. Rackoff
[MP03, Pat03a]. radar
[GG05b]. Radiations
[SNG09]. radical
[Web02]. Radio
[Sak01]. RadioGatún
[BDPV09]. Radix
[HKA⁺⁰⁵, JY01]. Radix-
[HKA⁺⁰⁵, JY01]. rails
[Fox00]. Rainbow
[DS05a]. Raises
[MP00]. Raising
[Cos03]. ramp
[Y06]. Ramp [CC02b]. Random
[An01]. ABCB04, BSM03, BK06a, BF05, BF04, BL08, CTY09, Chi08b, Dic03, DGP07a,
DGP07b, DV08, EH K+03, Gra02b, GPR06, HSR +01, HBF09, Int03, JRR09, Kel05, LLL +01, LM02, Lys02, MP03, Mir02, NNT05, Nie02b, Pas03, Pat04, Ran55, Ran01, RSN +01, SFDF06, TWNA08, TL07, Tip27, TZZ09a, TZZ09b, Vav03, VKS09, WP03, BK07, Bel08, BG08, BG09, BG07a, BGL +03, CJL06, CO09, DGP09, Fis01a, GVC +08, Gen00b, GB09, HG05a, HLW8W09, HMvLM07, JAW +00, KH08, KB09, MI09, MFK +06, NR04, Pan07, PSS +09, PSP +08, PC00, Reg05, Reg09, RG09, RGX06, SS03, SX01, SR07, SK01b, Sug03, SL09, UHA +09, WW08, YZEE09, BH05].

Random-Error [LM02].
random-self-reductions [Fis01a].
Randomats [Sam01]. randomization [WHH05]. randomization-enhanced [WHH05]. Randomized [Sem00, Hro05]. Randomness [DD00, DD04, DGH +04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN +09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03].
Range [CW09].
Rank [Sun00a, DW01, Sim02]. Ransom [BH05].
Rao [ZYR01]. rapid [OP01b]. Rate [KT01, LZ09, PS02a, Sun00a].
Ratio [Di01]. 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].
re [AH05, AFGH06, KHL09]. re-encryption [AH05].
re-signatures [AH05].
Reachability [AL00a, MT07]. REACT [OP01b]. Reactive [Shy02]. Real [BSW01, Dri02, GSB +04, JBR05, SP05, Sta05, YKMBO8, GM04, HP01, Lie05, SL07, SGPH98, YZDW07]. Real-Time [Dri02, GM04, YZDW07]. Reality [Coc01a].
Really [CZB +01, Wei00, Dav01c].
reap [CH00]. reason [Lau08b]. reasoning [IK03, IK06]. Rebalanced [SWH +09].
Rebalanced-RSA [SWH +09]. rebels [Lev01]. Rebuild [Salxx]. Rebuilding [Sal05a]. Receipt [HS00]. Receipt-Free [HS00].
Receipts [Cha04]. Receive [Coc03]. Receiver [CCD07]. Receivers [NNL01, SBB05]. recency [SW02]. recently [JK01a]. Reception [Top02]. Recipes [VM03]. Recipient [ANR01, Kur01].
Recipients [Coc01a]. recoding [SSST06]. Recognition [A02d, LLT +04, LST +05, TZT09b, HS02b, Li05, MMJP03].
Recommendation [Bar06b, BK06a, BK07, Dwo03, NIS03b]. Recommended [Kel05]. Reconciling [BNPW03, PGT07]. Reconfigurable [FD01, FZ05, GC01b, KBD03, L204, MK09, MMH02, SJT09, SKG09, SRQL03, CMS08, DHL06, GC00a, HBC +08, RH03].
Reconfiguration [PBTW07].
Reconsidered [Sho01]. Reconstructing [CWF01, FL06, PS01a]. Reconstruction [AF03, CF01b, CDF01, JJ00d, KY01c].
Records [DUR01]. Recoverable [NZCG05, NZS05, SGMV09, YY00].
Recovery [BDK +09, BM01c, CCM00, OS01, PBC05, TC01, VV07, WC05, WL05b, CCH05, CJ05, HW05, KJKL01, PSS +08, Sha04b, SIR04, TJ03, Wu01, ZF05].
Recursive [WHHT08]. Recycling [DPS05, TR09a, TR09b]. Red [Sas07].
Red-Eye [Sas07]. redistribution [KB09].
Redondo [IEE00a]. Reduced [BDK02b, CC08, CS05c, FKS00, HQ01, HSR +01, KKS00a, KKS00b, KKS01, KML +02, KM01b, KKS00b, MHL +02, NP01, STK02, SKI01, YSD02, CV05, Küh01, SK01a].
Reduced-Round [FK00, KKS00a, KKS00b, KKS01, KML +02, KKS00b, NP01, YSD02, CV05, Küh01].
Reducibility [DM00b]. Reducing [AL07, BMM00, SPH06]. Reduction [CM05a, CH07c, Dhe03, Gro01, HGG07,
Results [APV05, GM02c, OOP03, RR08, Way02a, YRS09, CV05, CKRT08, DM07a, GMG00, PM08].

Rethinking [Bra01a, KMZ03].

Reevaluation [Kuh08]. Rhode [IEE07]. RI [Sil01].

Right [Dhe03, GS07b, HKPR05].

rightful [CL08, Lin01a]. Rights [Bar00a, BNPW03, Dre00, Scr01, Wya02, BA06, UP05].

Rijndael [BB02, MP01a, SKU+00, Wer02, CKK+02, CGBS01, DR00a, DR00b, DR01, DR02b, FKS+00, FKL+01b, FKL+01a, FSW01, FD01, GM00a, JmBdXm05, KY01b, K07, KV01, Luc00, MM01b, MMH02, PSC+02, RDJ+01, SMTM01, SRQL03].

Rijndael-Like [PSC+02].

Ring [Rhee].

Rings [BLST01]. RIPEDM [DG02, WFLY04]. RISC [Cor00a, Gro03, WWCW00]. RISC-Based [Gro03].

Risk [WA07, Voi05].

Rights [ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, Pr01, Sch00c].

Rivest [BB79, Coc03, SP79].

RMI [JRB+06, Mar02a].

RNS [Bi04, BK09, NMSK01].

Road [BDPV09, HR04b, PB01]. Roadmap [Coc02b].

Roaming [CAC03, YWD08, SSM+08].

Robots [Coc01a].

Robust [BB00a, BR09, C03c, CWY05, DDO+01, HH09, hKL00, Lin00a, LHS05, LLC06b, PJK01, SG07, SOHS01, SDFH00, SDF01, VK07, WNY09, WLO4b, WMDR08, YPSZ01, ZTP05, LCZ05c, LKZ+04, Mt00, MB08, TND+09, YY05b].

Robustness [CS05c, HM01b, Rot01, CKL+09].

Rogaway [MW04].

Roger [GG05a].

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

Role-Based [YT09, ZGLX05, Cra05b].

Roles [LLL+01, Vixt02].

Roma [AAC+01].

Rome [IEE04].

Ronald [Coc03].

root [Pet05].

rootkit [Bhu09].

Rootkits [HB06].

Roots [Gon06, HCK09, CAC06].

Roseau [PY05].

Rotation [BBF08].

Rothe [Fal07].

Rough [Naz02, W05].

roughness [Lav09].

Round [HI00, BP04, Bih00, BF00a, BDK02b, Che03].
Round-Complexity [Ros00].
Round-Optimal [KO04].
Rounds [BDK09, CD01a, HSIR02, KM01b, Luc00, Pat03a, Pat04, GM00a, SK01a].
Routing [BGYO08, CL05, Ken02a, KB09, LAPS08, LH08, MABI06, PS08a, RVS09, vOWK07].
RSA [Joy03b, Men05, Oka04, PRE02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, C00c].
S-Box [FM02b, SMTM01, JmBDXgXm05].
S-boxes [BCDM00, Z00].
S/MIME [Dav01b, Dav01c, Opp01].
SAFE [Uni00a, Uni00b, Uni00c, Uni00d, Uni00e, Uni00f, ACS02, LBR00, Lys08, Oiw09].
Safe-Prime [ACS02].
Safeguard [LXM05, Sty04, Bar03].
safeguard [LXM05, Sty04, Bar03].
safety [HM01a].
SAFKASI [WAF00].
Salsa20 [Ber07, Ber08].
Salzburg [DKU05].
Samba [BH00a].
SAML [RR04].
sampl [WW06].
sampling [KB39, Sug03, Tip27].
San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Oka04, PRE02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, C00c].
sans [Car00].
Santa [Bel00, Ben03, Fram04, Kil01a, Men07, Sho05a, Yun02a].
Santiago [BS03].
Sanxin [LSZ05].
SAR [B+02].
SASAS [BS01c].
SAT [KLN+06].
Sat [Mea04].
satellite [CC05c, HY03].
satisfy [PHM03].
satisfying [PP05].
Saturation [Luc02a].
saving [Lev01].
Savings [CAC03].
SAX2 [TEM+01, Hei01].
Say [Sta05].
says [Mad04].
SBLH [JK02a].
SBox [WOL01].
SC-CFS [IT01].
SC2000 [SSY+02, YSD02].
SC2001 [ACM01b].
Scalable [CPH04, HKA+05, HLL05, KY03, KHYM08, SPQ06, LLW08b, ST03a].
Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWMW05, Mis06].
Scale
[BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a]. Scaling [BBP00, Coc02b, SDHF00, SDF01, PBVB01].

Scambray [Gum04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Ols00]. Scenarios [BF05]. scene [SG07]. Sceptical [Pem01b]. Schedule [MHM+02, XH05]. Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJ00, AF03, BNPS02, BR09, BS01d, BMS03, CL01a, CHK03, CGHG01, CYH01, CTL04, CC09, CH01b, CM05a, C0c01b, CDF01, CDM00, DS05a, DKE05, FS01c, GJSS01, GS02c, HS02a, HNZ01, HY01, HT06, HC08, Igl02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LCD07, Miy01, Mii01a, OK06, PL01, RK06, Scr01, SOO02, SWH05, SGG00, SYL05, SSNS00, Tad02, TC01, Tsa01, TT01, WQW01, WZ05, WBD01, YWWS09, YG01a, YLH05, ZJ09, AEE05, BCL05a, BCW05, BN04, B0BB02, CL02b, CC01, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CHV05a, CHY05b, CL00, CHC04, C0CH04, CY05, CHC05, Che05a, Che07, Che08a, Che08b, CCS08, KCH06, CT01, D0W01, FAX04, FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HWW03, HWW04, Hsu05a, HWW05, Hsu05b].

scheme [HC04a, Hwa00, HIV03, HLL04, HIV04, HLL05, HLL05c, HLL05d, JW06, JSH05, KC09a, KLY03, KRY05, KWS06, KHL09, KCL03, Ku04, K05, KCC05, KHK05, LH02, LLH02, LHL03a, LKY04, LL04a, LJY04, LL05a, LKY05a, LKY05d, LL05b, LMC+03, LHH04, LHT05, LLCL08, LLH06, LHL03b, LHC04a, LLY07, LCC05, LC04b, LC05a, LHH05, LCZ05b, LCZ05c, LCZ05a, LW05b, MSP09, NC09, PW05, PBMB01, PCC03, PC05b, PS01a, Pe04, Sae02, Sco04, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, mSgFt05, SCS05b, SC05c, SCS05c, SSS05, TLH05, TWL05, TYH04, VK08, VS08, Wan04b, WL05, WK05, WJP07, WDLN09, WHH05, WC01b, WH02a, WHL03, WH03, WL04b, XwWL08, XC05, YTH04, YW04, YCH04, hY08, YRR04, YRR05a, YY05a, YY05b, YbJ04, ZC04, Z04, ZC05, ZK05, ZW05a, ZAX05, Z09, ZL05, dRRM05].

Schemes [AR01, BP02, BU02, BD03, BDDS03, BF05, BGOY08, B0DS09b, CM00, CD00a, CL04a, CGP08, CT08b, CP06, CKN00, Cor02, CJNP02, Cou04, CS01, CS03b, CDG+05, CLZ02, DN00a, DN02b, D0s03b, DS05, DN00b, FF00, HZ01, HWW05, HM02b, HLL05, Kin02, KOS01a, KS03, KOM01, LZL+01, LP01, MV00, NIS03b, Nam02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SB42, S0PLS02, Sun00a, VMS05, WCJ09, XS03, YYC08, YYD001, Yek07, YYJ01, ZTP05, ZYR01, Abd01, AFGH06, BCD06, CWH00, CC05b, CJT03, CDFM05, D0D4, DM00a, DF0M, D0s03b, GGK03, HCD08a, HCD08b, HAU04, He02, HKS00, HW04, HW05, H0C04b, HLL04, IY06, JXW05, KJY05, KIr01b, KTO0, K06, K0h08, LWZ05, LW05a, LW05c, MF07, Mii01b, NK06, PS02a, PKH05, QCB05a, QCB05b, SN00, Sha03d, Sha05b, SCL05, S0C02c, SHT05].
schemes [Tsa05, Wu01, XY04, YWC05, YCW*08, ZJ05, ZL05, ZDKST06].

Schloss [EE01b]. Schneider [Puc03]. Schneier [See04, Sty04]. Schnorr [BP02]. School [Coc02a]. Schools [PM00]. Science [Bis03b, C0c03, EEE00a, EEE01a, EEE02, IE03, IE04, IE05a, IE06, IE07, IE08, IE09b, Im03, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04]. Scientific [CHT02, MH09, Lan08b].

Scientists [Coc01a, MH09]. SCN [BC05b, CGP03]. Scots [Ree01, Sin99]. Scream [HCJ02]. Scribner [Gas01]. Scripts [Uri01, Oue05, Rob02, Rob09]. scroll [GB09, HHY07]. SD [ECM00a]. SDK [Ano02d, Bar00c]. SDL [HL06]. SEA
[SPGQ06]. SEAL [Flu02b]. Seamless [OKE02]. Search [BI05a, Des00c, FIPR05, KB07, LM02, TIDG01, WYY05a, WYY05d, FZ06, PM08]. Searchable [ABC05, AFI06]. Searches [PGT07]. Searching [BSW09, GTC03, OS05]. Seattle [ACM06, S+05, USE00a]. sec [KV01]. Second [ACM03c, Bra01b, BD08, CZ05, GW01, HTS02, JY04, KCR04, Kil05, KP01, NM09, RD01, ACM00, Irw03, Son00, Spr03]. Second-Order [NM09]. Second-Price [Bra01b]. Secord [Top02]. Secrecy [Bla02a, GH02, Imr03, Lau05, Ree01, RW03a, Sin01b, BDNN02, BLP06, BD04a, Mol05, Sin99, Sin00, SY06, ZYW07]. Secret [ACS02, Alv00, BBDK00, BTW05, BI05b, BTW08, BP06, BM01b, CGHG06, CG060a, CH01a, CLT07, Cha04, CTY09, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG0505, CDI01, Di 01, DKL00b, DS06, DN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah96b, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, MN01, NABB03, NN06, OK060, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sin00a, TL02, Top02, TC01, UW00, Ver06a, Wir05, ZYR01, ZP01, vW01, AJ08, AEDR05, Ano08c, Bar02b, BCB035, Cal01, CC05a, CHY05a, CHY05b, CJI06, CNK04, CDD00, DD04, DB04, DM00a, Di 03, DW01, Duj08, FNRC05, FWTC05, FZ06, Gal02, GIKR01, HT04, HJ07]. secret [HK00, IY06, Kee05, KB09, Lam07, Lam09, MF07, MII09, Na05, PS02a, PW05, Ris06, Sch01e, SBZ04, SC05a, Smi01b, SC02c, Wan05, Win00, YCH04, ZSY05, dRMS05, vDKST06, Hii06]. Secret-Ballot [Cha04].

secret-code [DW01]. Secret-Key [HR05, RW03a]. Secret-Sharing [BI05b, CDM00, CDI05, DKL00b]. Secretly [CC08]. Secrets [BH06, BBD02, CMS09, CP07, Cop04b, Di 01, Gan01b, Gum04, KMS01, LKM0505, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM01, VGM04, AGKS07, An03b, An08b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DLM05]. Section [An04a, An07a, BK06b, SGK07, TL02, KP03]. Sector [Cro01, MV01]. Secure [AR00, AO00, AF04b, AG01, AP09, An01k, ACJT00, AFI06, BDF01a, BST03, BCL05b, Bar03, BI05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CPKS01, CM00, CG06, CK02h, CHK03, CHK05, CGP08, CW07, CQS01, CHJ01a, CHJ01b, CDM00, CDI01, CS02, CS03b, CDG0505, CDI05, Des00b, DG03, DM00b, ES00b, FGM001, FB01, FP01, FOPS01, GPC08, GIKR02, GJKR03, Gen04a, GD05, HZ001, HZ002, HSH06, HRS02, Har07b, HK060, HLV02, HVA09, HR04b, HL07, Hut01, HLC08, IR01, It000, IFH01, JI00a, JL00, JVM02, KMM06, KY01a, KO04, KLM0505, KQ02, KH05, KKL09, KL01b, Kos01a, Kos01b, Kra01, Kra05, KSR02, LCK01, LLL02, LCK03, LW001, Lin01b, Lin03, Lin02, MKP09, Mar02a, Mar07, MV01, Mol03a, MJD01, NAM02, Na05, NSNK05]. Secure [NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RV09, RD01, ST01a, Seo05, SVDF07, SBG05, Smi02, SKR02, SNR04, SBEW01, Sty04, Tad02, VMS05, Vuu05b, VMC02, VM03, WLL09, WBL01, WGL00, WH05, XS03, ZYM05, Zho06, Aam03, Abd01, AEE050, AL07, AFG06, BDS09a, BDFP05, BCP07, CLOS02, CCMT09, CC04b, CCK04b, CRS09, CHH09, CG05, DG06, Dwi04, FMY02, Geb04, GIKR01, GCKL08, HSW09, HL03, HL06, HJW05, HBC08, Ino05, ISTE08, IK0807, IY06, KOY09, KG09, LL04b, LLL04, LHC08, LC04a, LCZ05b, MT09, ML05, Mii01b, OS00, PCS07, PBMB01,
PQ06, PSP+08, RH03, RG09, RGX06, Sea09, SBG07, SGMV09, TKP+08, TCR03, Tse07, Ver01, VK08, WWA01, YGZ05, YTMY05, hY08, YRY04, ZBP05, ZCL05, vOWK07, Ano08d, Ano12, BS01a, BSB05, CHKO08, CH008, FIP02b. Secure [BNPW03, Ito01, UP05]. Securely [HL05a, LLK05]. Securing [Abe01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. Security [AW05, AW08, Ahm07, AJ08, ADR02, And07, And08, Ano02b, Ano06c, AHKM02, BP07, BW07, Bam02, BPS00, BBM00, BKR00, BP02, BNPS02, BY03, BPR05, BOHL+05, BBP+02, Bis03b, Blu02a, BF06b, BDTW01, BCH07, Boy01, BLMS00, CGM07, CK02a, CKN03, Can06a, CGHG01, Cer04b, CCO2b, CSW+08, Che05b, CM05a, CH07a, CS09, Cho03, Coo01a, CK06, Coo02b, CGP+02, CG05, Dr.00c, Dal01, DN02a, DMR05, DeL07, DJ06, Des00c, Dim07, DR02d, DSS01, DK05, DS05b, DBS+06, Elb09, ELv01, FIP01b, FBWC02, FW09, FLY06, For04, FLM+03, FM04, GS02a, GS03, Gum04, Gut02b, Gut04a, Gutxx, HM00, HSZ01, Hei07, HM02b, Hin09, HLL+01, HGNP+03, HQ05, HL05c, HO04, IS04, Ina02a, Ina02b, Int00, IKY05, IKP+07, JY04, JP07, JP02b, JW05, JQ07, JoL01, JBR05]. Security [JK02b, JK02c, JMV02, JQY01, Kan01, KM02, KSHY01, KL05, Ken02a, KB06, KM03a, KDO01, KM05, Koc02, KHL09, Kos01a, Kov01, KX000, Lad06, Lai03, Lan00a, Lan04b, LGS01, Lee04b, LKH+08, LKHL09, Leh06, Len01, LNS02, LL04c, LSH03a, LSH03b, Lin02, LXM+05, LWK05b, LP01, MJF07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Müll01a, NISO1b, NDJ01, NP07, Oak00, OP01a, Ort00, PV06b, PSC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PTP07, PP07, Pho01, Pie05, Pli01, Poi02, PHM03, Poo03, PF03, PS05, Puc03, Puc06, QCB05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sal03a, SJ09, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch00f, See04, Sha05d, SLG+05, SL05a, Sph02, SEF+06, SEK01, SEK02, SK06, Sta03, SB07]. Security [Ste05b, SBZ02, Sty04, SKI01, Sun05, Swi05, Tan07b, TG07, TG04, TPR07, Uni00a, USE00d, USE01c, USE02b, Uni00c, Uni00e, Uni00d, Uni00g, Uzu04, Vau02, VMC02, WLT05a, WBL01, WWL+02, WA07, YEP+06, YWD08, Zan01, ZWC02, ZDW06, Zhe02b, ZHY03, ZS05, AA04b, Ano05b, AJ01a, AJ01b, BP08, BAI05, Ban05, Bel06, Bel07b, BR04, BGP09, BFGT08, BFG08, Bjo05, Ble07, BJ02, BM05, BG07a, Br06, BMV06, Can01a, C+02, Cha07, Cha05b, CKL+09, CR08, CJS06, CMM00, Con09, Con04, CC05e, DP04, DKK07, DY01, DFGH04, Des00a, DWM05, DK05, DMS07, Egl00, FXAM04, FR08, FOP06, GH08, GJL06, GJ05, Gha07, GJ03, Gor05, GKS05, GMW01, GC05, Gut04a, HM04, HCD08a, HCD08b, Har05a, Hen01, Hes04a, HM05, HSL+02, HL06, HGL05b, Ino05, JEC04, Jan00]. Security [Kad07, KY00, KPS02, Kim02, Kov03, KH03, Kwo03a, LC03, LL03, LJ04, LL05b, LPW06, LMC+03, LM05, LLL06a, LLL06b, LHC08, MJ03, Ma06, Man08, Man05, Man04, May01, MKKW00, MS03, Mc06, Men03, MS02d, MK05a, MPPM09, OP01b, Paet03, PS+09, PC05a, Pat02a, PY05, PP06a, Pau03, PHS03, Poi00, PS04c, RC05, Ros06b, RN00a, RN00b, SN00, Sal05d, Sch03, Sen03, SHL07, Shu06, SH00, Sta02a, Sta06, Ste02, Sun00b, SHT05, SSL+00, Tsa05, Uni00f, Vac06, Voi05, VOS08, WA00, WA06, Won01, WK06, XQ07, YW04, YY05b, ZSZ01, ZZW05b, ZSN05, dB07, dCdVSG05, vOWK07, vTO5, AG09, Ano02e, BC05b, BP01b, Chr00, Chr01, CC02, CC02, CG03, JBR+06, Lin02, RR04, Uni00h, ZL04c, Pap05].
Security-related [Gutta].
security-sensitive [SPHH06]. seed
[TP07, KKK+07]. Seeing [Wal03]. Seek
[Coc01a, PH03, Shp05]. seeking [Mos06].
Seeks [CAC06]. Seem [Coc02a]. Selected
[EE09, CSY09, HAO00, MS05a, Neu04, PT06, RSA00e,
St01d, YV01, Ytr06, AMW07, Bir07,
BC05b, CZ05, DRS05, HH04, HH05,
PC05a, Wil09, WK06, AMW07, HH04,
HH05, MZ04, NH03, PT06]. Selecting
[BDK02b, ABK00, IK00, IK01, KKS00a,
KKS01, KKS00b, Os00, Pat01]. Server
[ANRS01, BMK00, Dew08, KO00, LWK00,
NS01b, PS05, TMM05, XS03, Zha00,
BB05, LHL04, LKY05b, LHL03b, NTW07,
Tsa01, TWL05, YS04]. Server-Aided
[NS01b]. Server-Assisted [XS03]. serverless
[BDET00]. Servers
[BIM00, HS07, Jab01, KCD07, Mar02a,
TEM+01, LS05b, PT08]. Service [BACS02,
BH00a, CLK01a, DeL07, KZ01, Lan04a,
LM04, Nik02a, Nik02b, PKBD01, CUS08,
HLM02, KWDB06, LB05, Mir05, MV03b,
SRJ01, SSM+08, ÜG08, Coc02b, Hili06].
Services
[ANS05, BCS02, DJLT01, ECM00a,
ECM00b, Knu07, Sour01, Uni00b, WL07b,
BDS+09a, BFG04, BFG05, BFG08, CCCY01,
HM05, JRB+06, MPPM09, MV03b, RR04, SBG07, SL05b, TWL05, WA06, BH00b.

serving [LLK05]. Session [GL01, OHB08, CS04, RN00b, Uni00a, Uni00b, Uni100f, Uni00e, Uni00b]. Session-Aware [OHB08]. Session-Key [GL01]. Sessions [KPR03]. Set [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDET00, Che07, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01]. Sets [CFS05, EIG01, TW07]. Setting [BBM00, DLY08, LP01, PGT07, GMLS02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC+01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SGB01]. SGI [Bar00c]. SGID [Tot00]. SHA [AD07, BC04a, GLG+02, HKR01, MP06, SK05a, TYLL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG+02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TYLL02]. SHA-512 [AD07, GLG+02]. SHA1 [WYY05a]. SHACAL [KML+02]. Schacham [Hes04a]. Shamir [BB79, SP79, Coc03, PW05, VS08]. Shamir’s [LD04]. Shape [Gan01b, Gil07]. Shapes [OMT02]. SHARC [DMSW09]. Share [CT08a, CDI05, FS04, AEEdR05]. Shared [ACS02, BH06, BBDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01]. Sharing [BT05, BI05b, BTW08, BGHP02, CD00a, CLT07, CC08, CTY09, CDMA00, CF02, CS05, CDG+05, CDI05, DI 01, DI 03, DS06, DP07, FM02a, FPS01, FMY01, 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, DLK00b, FWTC05, GIKR01, HT04, HKS00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDKST06]. she [Gua05]. Sheets [MNS01]. shell [Dwi04, Gua05, BS01a, BSB05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [YWC05]. Shift [CGFSH09, Che08a]. Shin [Kühb08, Kühb08]. Shines [Coc02b]. Shinko [Ano00d]. Ships [Ano02e]. Shops [Ano01c, YSS+01]. Shor [KLB+02a]. Shores [KKP02]. Short [Ano01k, AF06, BBS04, BGW05, DN00b, Gra02b, LS01b, PM02, RR02, RW02, Vau05b, GL05, WDLN09, Coc02b, Sch01e]. short-term [WDLN09]. Shortcuts [Sha03a]. Shortened [Kur01]. shortest [Pei09]. ShortPK [WDLN09]. Shoup [Luc02b, VMSV05]. shows [AJ08]. Shrinking [Gol01c, WHLH05, ZKL01]. SHS [Ano08d, Ano12]. Shuffle [FS01c, NSNK05, Sas07]. Shuffles [Mir02]. Shuffling [PBD05]. shut [Gil07]. SiBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [Ano01i, BU02, KSWH00, Law09a, LL01, Möl02, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP+08, WL07a]. Side-Channel [BU02, Law09a, Möl02, CNPQ03, PSP+08]. Side-Match [WC04]. Siena [BCKK05]. sieve [CM05b, JL03]. sieves [Har07a]. SIGABA [Lee03c]. SIGACT [ACM03c, ACM05b, Raj06]. SIGART [ACM03c, ACM05b]. Sight [Col03]. SIGMA [Kra03]. 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 [Ano02e, GG05b, Sha01e, CKL+09, LLLZ06a, LLLZ06b, Koy01]. Signalling [ECM00b]. signals [Ren09]. Signature [ANS05, AAK09, AR00, ADR02, Ano01c, Ano01f, Ano00a, Ano13, Ara02, ARO1, ACJT00, Bar06b, BNPS02, BOGY08, BMS03, BDS09b, CM00, CD00a, CL04a, CK02a, CGP08, CH01a, Che02, CM05a,
Cor02, CFS01, CS00, DS05a, DKFX05, Eng00, FIP00, Gen00a, GJSS01, GS02c, HY05a, HSZI00, HM02b, JSJK01, KC02, Kuh00, LZX01, LP01, MV01, Miy01, Nat00, NZCG05, PL01, PCK02, Pre01, RS01, SA02, ST01b, SOII02, SWH05, SPMLS02, Str01a, SYLC05, SSNGS00, TN00, WQWZ01, WBD01, XYL09, YYDO01, YSS01, YLH05, ZK02, Z09, Zhe01, AvdH00, BCL05a, BCW05, Cal00b, CWH00, CL04b, CYH04, CCH05, CJ05, CHC05, Che05a, CJT04, GGG03, HLL02, Hes04a, HPS01, HWW02, HWW03, HW04, HWW04, HWW05, HW05, HC04a, HL04, Kwo02, Kwo03b, LH04, LHD05, LL05b, LLH04, LTH05, LWZH05, LHH05].

signature [LCZ05b, LCZ05c, LCZ05a, LW05c, PKH05, PC05b, QCB05a, QCB05b, Sae02, Sha03c, Sha03d, Sha04b, Sha05a, Sha05b, Sha05d, SCL05, SHT05, TJ03, TY04, Wan04b, WK05, WLHH05, WH05, Wu01, WHLH03, WH03, WY05, XC05, YTH04, ZC05, ZF05, ZW05a, ZCL05, RR04].

Signature-Based [CK02a].

Signature-Embedded [An00c, YSS01].

Signature-Tree [TN00].

signature/multisignature [Wu01].

Signatures [AO00, AOS02, ABRW01, BN02, BGLS03, BS04, BSS02, BCCN01, CD00a, CL01b, CNV06, CZB04, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZI01, Her06, HM02b, HS01b, HHGP04, HL01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00, MM02, MNFG02, PC01, Ram01, RR02, Rd01, VW01, XS03, Zho02, An00i, Ate04, AH05, BLH06, BO05, BM02b, BM02a, BLRS09, Ca00a, CKK03, Die00, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HL00, JLL01, JL04, KKCL09, LV07, LS05b, MJ05j, PL05a, PBV08, Sch01f, Sha01d, NZ05].

Signcryption [Boy03, MLM03, Zhe01].

Signed [FL01b, OSSS04, Sch01a, SJ00].

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

Signer-Base [IR02].

Signer-verified [CJT04].

Signers [LZL01, Sae02, Sha03c, YTH04].

Significant [SZ01, MS02b, Shp02].

Signings [AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCCN01, CD00a, CL01b, CNV06, CZB04, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZI01, Her06, HM02b, HS01b, HHGP04, HL01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00, MM02, MNFG02, PC01, Ram01, RR02, Rd01, VW01, XS03, Zho02, An00i, Ate04, AH05, BLH06, BO05, BM02b, BM02a, BLRS09, Ca00a, CKK03, Die00, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HL00, JLL01, JL04, KKCL09, LV07, LS05b, MJ05j, PL05a, PBV08, Sch01f, Sha01d, NZ05].

Simpler [Lin03].

Simplicity [MS01].

Simplifications [DJ01].

Simplifying [Gut04b].

Simply [On01].

Simply-Iterated [On01].

Simulatability [HU05].

Simulatable [Lau05].

Simulation-Based [DKMR05, KL05].

Simulations [WBRF00].

simultaneously [Wu01].

Singapore [BDZ04, TL06].

Singh [Im03, Ree01].

Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a].

Single-Chip [MM01b, MM01c].

Single-Packet [WLZZ05].

Single-Server [KO00].

Sinegular [AS08, Bai01b, BR09].

SINOBIOLOGIC [LLT04, Li05].

SIP [NTW07, PM00, SZ08].

Sir [Bud06].

Site [AEV07, Co02a].

Sites [Ros07].

situation [AJ08].

six [Bel07a].

Sixth [Un00a, Un00b, Un00f, Un00e, Un00h, TL06].

Size [CS07c, CMJ03, HN02, Kal03].

Sizes [An00b].

Skein [AEMR09].

Sketching [MNS08, SLTB06].

Skipjack [Gra02a, HSL02, SLL01].

Skipjack-like [HSL02, SLL01].

SKLOIS [FLY06].

Sky [MYC01].

SLAAC [CGBS01].

SLAAC-1V [CGBS01].

Small [CCM05, ELvS01, Fia02, GPS06, MNT00, May02, OT03b, RK06, SM02, Sch01e].
Small-Project [MNT+00]. Smaller [Bar00c]. Smart [And04, Ano03a, AJ01b, Bel01, BCST00, Car01, CL07, DF01, DFCW00, DJLT01, HBdJL01, Hen01, HQ05, Jac00, JSJK01, JY01, Lan00d, LSA+07, MOP06, MV01, MG08, NFQ03, Poh01, Q500, Q501, RE00, RE03, RS01, Sak01, SR01, Sha01c, SP02, TBDL01, VPG01, YKMY01, Ano00k, Ano00l, Ano04c, AJ01a, Bor00, BPR01, BCHJ05, BGL+03, Bur00, Cal00c, CCCY01, Cha05a, Cla00b, Con00, CH00, DMT07, DFH01, DFPST07, Fin03, GMG00, GUQ01, HHS01, Hsn05b, Hsu01, KLY03, LKY05a, Ler02, LC05a, Lu07, MY01, PB01, Pre07, SVDF07, Smi00, TIS07, VK08, YWWD08, Za00, BJvdB02, CL04d, CCK04b, Che00, DFP06, FGL02, Gro03, HL05b, Kc04, KC05, LHY02, Pau02b, SKKS00, Sco04, SCF01, TV03, YW04].

smart-card [GMG00]. Smartcard [HWH01, KRV01, RMCG01, Uri01, PBVB01, BBP00, CGMM02, DM07b, HRS02, It001, KS02]. Smartcard-Based [RMCG01, CMG02]. smarter [Car01, Cla00b]. Smartly [MS01]. Smooth [PS02b, GMR05]. SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. Sniff [And02e]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sa02, Sha03c]. Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Ah07, And07, Ano02e, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HHH01, Hoe01, JH03, Knu07, KSZ02, Lao06, Law99a, LSY01, LLZ06a, LSVS09, LTM+00, MNT+00, MSH07, MKY08, MG06, Nd05, PM00, PS01c, RM04, Sch01a, Sch00b, Ste00, USE00b, V09, VVS01, W005, W010, ZCC01, ARJ08, Ano00h, Ano09j, Bir07, CT02, CCD+04, CT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, Mat02, Mc08, MCH05, Pau03, Sch01d, SS03, WL07a, WA06, Sal03b, B0702].

Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [Hoe01]. Software-Oriented [ZCC01]. Software/hardware [Nd05]. SOI [And02e, NFQ03]. SOIIISC [Ano04c]. Solaris [Ano04c, B00b]. Solomon [KY02b]. Solution [Cap01, THR00, LLS05b, Poh01, Str02, TVdKB+01, LSH00]. Solutions [Ano04b, MV01, Jan00, MSK03, M03b, St.00, Gum04]. Solve [CU01, G803]. Solving [CJT04, GPP08, W101a, Bul09, Wh09]. Some [AG01, BDF+01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HAU04, He02, JK01a, RSS04, SHT05, ZF05]. Someren [Ano03c]. Something [FL01b]. sometimes [FNRC05]. Sons [And04]. Sorry [San05]. sorts [Ano03e]. Soul [Bla01c]. Sound [BJP02, FR08]. Soundness [ABHS09, DP04, M01c, BPS08, Lan08a]. Source [Bar00, Bol02, G004, HBF09, KLR09, PM00, RK06, TEM+01, Ano03c, BGL+03, Mc08, RVS09, SB05, Bar00b, Lin02]. Sources [KZ07, WLLZ05, KZ03].

Southampton [Bla03]. Soviet [AJ08]. SP [BG07a, H09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPA-Based [Nov01]. Space [BG07, Lu02, MSH07, N05a]. Space-Bounded [Lu02]. Space-Efficient [BG07]. Spain [BS03, DFP06]. Spam [CMB+05, DGN03, V06]. Spanning [Bel04]. SPARK [Jen09]. Sparse [BLST01, BDG+01, FS01b, G803, B06a]. Spatial [MM01a, SGM09, SDFH00, L00a].
Spatial-Domain [SDFH00]. Spatio [CDTT05].
Spatio-Temporal [CDTT05]. speakebles [BZ02]. Speaker [LM00]. Speaks [VN04].
Spec [Bar00c]. Special [Ano04a, Ano07b, Ano07a, BK06b, GIS05, GS07a, GPP08, SKG08, KP03, FOP06].
Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08].
specialed [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00a, LKJL01, RSA00c, Mea04].
Specifications [IEE00b, BDFP05, BD04a]. Specified [Tad02, He02, LWK05b, YY05a, ZX04].
Specifying [BJvdB02, Cir01]. Speck [KGS07]. Spectr [GMM01]. Spectr-H64 [GMM01]. spectra [MS02b].
Spectral [QPV05, SK07]. Spectrum [BQR01, LY07, PM00]. Speech [MRL+02, AA04a, PY08].
Speech-Generated [MRL+02]. SpeechStudio [Ano02e]. Speed [Ano00d, Ano02d, Gro01, JKRW01, KMM+06, Lut02, SOTD00, SM02, We00, YKMY01, BGL+03, RW07, RMCG01].
Speeding [Osv00, SWH+09, TC05]. Speedup [YKL02b, YKL03]. Speedy [Cre00]. spherical [LZP+04]. Spider [Tur04].
Spies [Gan01b, Win05c, Hau06, NRR00]. SPIHT [Che08a]. SPIN [MS02a]. Spline [SPK08].
Splitting [GMW05, LLK05]. SPN [HLL+01, Kan01, PQ03b]. SPNs [CKL+03].
spot [Naf05]. Spread [BQR01]. Spring [Pap05]. Spring-Verlag [Pap05]. Springer [Fal07, Lee03a, Lee03b, Pho01].
Springs [Wil99]. spying [FRN05]. spymaster [Bud06]. spyware [Ste05c]. SQL [Dew08, HILM02]. Squadron [OC03].
Square [HCK09, HQ01]. Squaring [CH07b, NSS02]. SRAM [HBF09]. SSC2 [HQR01, ZCC01].
SSH [All03, BS01a, BSB05, BKN04, Dw04, H601, Hos06b, Kra02b, Naz02, Oue05, SWT07, Str02].
SSH-Connected [H601]. SSF [Hos06b].
SSL [ASK05, BPST02, CHV03, JRB+06, KCD07, KPR03, Kra01, LLK05, LWK00, Net04, OHB08, SB01, SQ01, Vau02, ZFK04].
SSL/TLS [BPST02, CHV03, KPR03, OHB08]. SST [Gau02]. St [GKS05, NH03, A01a]. Stack [Pot03]. Stage [Kak06, CHY05b]. stamp [CL00]. stamping [HHC05]. Stamps [KZ01]. Stand [CAC03]. Standard [Ano08d, Ano09a, Ano12, Ano13, Bar00a, BCP02a, FIP00, FIP01a, FSo01, Her09, Hug04, HLC08, IEE00b, MM01c, MP01a, Nat00, PM00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, BBK+03b, DRS05, GMR08, Sea09, Tan01, Ase02, Bar00c, H00, Bur03, CMR06, Coc02a, Coc02b, Cur05, DR01, DR02b, Dan01, FIP02b, GC01a, Har00, Lan00a, Lan00b, Lan04a, Mor05, NIS00, SB00, Sta00, Sve00, WBR00F, Wri01, YW06].
Standardized [Man01]. Standards [Ano01f, Bur06, CL07, C02b, Hus01, RSA00a, Tsa06]. Standing [Lan00b]. State [And07, CR03, GST04, HBF09, Kar01, MSNH07, R06, TL07, Mit00].
State-transition [TL07]. statecraft [dL00]. Stateless [ANR01, NNL01, SK05b].
Stateless-Recipient [ANR01]. States [LB04, Jo01]. static [CW07].
Statistical [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, L01, LLL+01, MV03a, Neu04, Pro01, RSN+01, BKW03, Hey03].
Statistically [Fis01b, HR07, HNO+09].
Statistically-hiding [HR07].
Statistically-Secret [Fis01b]. Statistics [CKN01, CNK04, KLML05]. Status [Pre01, Sha03b]. statute [Cal00b]. STDM [WMDR08]. Stealing [Gan01b]. Stefan [AUV01]. Steganalysis [Pre01, Sal05b, WW04].
Steganografie [Sch09]. Steganographic [CTL04, HR02, MJF07, RH02, RS00, Wes01].
KC09a, LYC02, WWTH08, YCL07].

Steganography
[BC05a, BGI08, CYH01, ChLYL09, CDR01, CW09, CTH08, Col03, CMB+08, CS05c, DIRR05, DRL09, FGDO1, Fri07, Gal03, HLvA02, HvAL09, HSKC01, LS08, PH03, Sal05b, Sch09, Sha01e, Shi08, SWR05, Wan05, WW06, CDS07, Che07, Che08a, GGS09, JDJ01, KP00, LT04, WW04, WMS08, Way02b, Way09, YCYW07]. stego
[KC09a].

Step[WL02].

Step-by-step
[SL06].

Step-out
[KKKL09].

Stepping
[WRW02].

Stereotypes
[GO03].

Stern
[CGP08, CS05b].

sticker
[GPX08].

Sticks
[Sam01].

Still
[Ano00f].

Stinson
[Spr03].

STL
[Zol01].

STOC
[ACM90c, ACM97, ACM08, ACM09].

Stochastic
[MG01].

Stock
[Bar00a].

Stone
[MM03].

Stories
[ST06].

Story
[Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, HS01a, Win00].

strategic
[AJ08].

Strategies
[Cir01, KL05, SKQ01, Dwi04].

Strategy
[DR02a, TPP07, KC09a].

Stream
[BCC01, BS00b, BL02, CF01b, Can06b, CJS01, CHJ02, CM03, Cou03, CL02c, DF07, FI000, FO10a, Gol01d, GBM02, HCJ02, HR00, HR04a, JAm00, KHD01, MSNH07, PP06a, SM01, Sar02, SXY01, WB02, Wu02, ZC00, ZZC01, BGP09, Ber07, BD00a, BG08, BVP+04, DK08, KH08, Max06, MI09, PC03, PC03, SB05, WW08].

Stream-Cipher
[SXY01, WW08].

Streaming
[OS05].

Streams
[AIP01, YLC+09].

Strength
[CB01, JX05, Oni01, CKL+09].

Strengthening
[Loi00, MHH+02].

String
[CP07, DFS04, Pas03, Dam00, RG05].

Strings
[Vau05b].

Strong
[ADD09, BB00b, CS00, DKFX05, KCJ+01, KW00, LS03a, LSH03b, Lo02, Pau09, SBZ02, WHL05, CC04b, HR08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04].

Strong-Password
[LSH03a, LSH03b, WHL05, CC04b, KTC03, Ku04].

Strongly
[BY06].

Structural
[BRR+01, LBR00].

Structure
[DNP07, EIG01, Hs01, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SSL+00, XMST07].

Structured
[BRTM09, CKK03].

Structures
[An02e, DS06, GTTC03, HCD002, KCP01, Kü02, MND+04, MFF05, PS+02, PQ03b, Sun00a, XH03, Hen06a, IY06, SWR05].

Struggle
[Bur02].

Stuart
[Gum04].

Students
[AA04b, PP09].

Studies
[Pag03, SPHH06].

Study
[BBGM08, Car02, DPR01, DP00, KKJ+07, WC05, BKN04, BF06a, DY09a, KWDB06, SKW+07, ZWWL01].

Sturgeon
[Wei05, Wei06, Wei06].

Stuttgart
[Eag05].

Style
[BPS08, dH08].

Subcommittee
[Uni00f, Uni00h].

Subdivision
[LDD07].

Subgroup
[NBD01, KM04a].

Subgroups
[Gro05, GRM05].

subliminal
[LH04].

subsampling
[LLC06b].

subscribe
[SL05b].

subsets
[Sch01e].

substitute
[Bih02].

Substitution
[KKG03, GPO8, RFB08, WLO4b].

Substitution-Permutation
[KKG03].

Subsystem
[HL07, MBS04].

Subtleties
[Lai08].

subverting
[HB06].

Success
[An06d].

successful
[KH03].

Succinct
[BA06, FS08].

Sued
[Nic01].

Sufficient
[IKO05, Kos01b, KO00, MN01].

Suffix
[ABM08].

SUID
[Tot00].

SUID/SID
[Tot00].

Suitable
[AIK+01, CQ01, KTT07, LKHL09, SP05, Wen03].

Suite
[RSN+01, SBEW01, YLT06]. **Suit**ed [WWGP00]. **Sum** [Che04b, KLY02]. **Sum-of-Digits** [Che04b]. **Sums** [CY08, Shp05]. **Sunspots** [CP07]. **Super** [Lam07, CAC06, Hos06b]. **superccluster** [Pri00]. **Supercomputer** [Coc01a]. **Supercomputer** [Coc01a]. **Supersingular** [Gal01, RS02, Ver01]. **Supplemental** [TBDL01]. **Supplementary** [ECM00a, ECM00b]. **Supplies** [Sha01c]. **Support** [ABM00, Gro03, LTM+00, PZDH09, SBG02, Ano00d, BMA00a, BMA00b, BMA00c, ED03, mSgFtL05, SSM+08, WnQ08, ZYL05]. **Supporting** [CLK01a, SW02]. **Surveillance** [LCS09]. **Survivable** [CLZ02]. **Susan** [Jan08a]. **SVD** [CYH+07, FWL08]. **SVD-based** [CYH+07, FWL08]. **SVGrid** [ZBP05]. **Sweden** [BS01b, Joh03]. **Swiss** [Bec02]. **Switzerland** [CC04a, Vau05a]. **Symbiosis** [DF01]. **symbol** [SVDF07]. **Symbolic** [Bor01, Jef08, Mar02b, May09, MT07, MP05, ALV02]. **symbols** [Lun09]. **Symmetric** [Ano01j]. **Symmetric-Key** [Ano01j]. **Systematic** [KB06]. **Systems** [ACM03c, ACM05b, AnRS01, Ano02e, BCS02, BRTM09, CP02, ELs01, Fe06, GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST+05, LLLZ06a, LJ05b, Lut03, Mar02b, MYV02, NAB03, RS05, Ril02, Sm01, Sas07, STJ09, SXY01, USE00c, USE00b, Vav03, VHP01, WKP03, ARJ08, Ano09, Ano01j, Bid03, Ble07, CUS08, CC05c, CCS08, CGL+08a, CGL+08b, CGL+08c, CCM01, CNPQ03, CHT02, CG05, CSK+08, DY09a, EY09, FMY02, FP00, HP00, HBC+08, Hut01, HY03, KAM08, KP01, KNP01, KP03, Koe03, KR03, KNS05, MBS04, MSP+08, NAM06, Nas03a, PBMB01, Par04, PI06, WnQ08, ZYL05, ZSV05, Ano02d, Lut03]. **Systolic** [KLY02, KKY02, MP01c].
Table [Ano03d, MFFT05, XFZ01, BZ03, CC05b, Has00]. table-based [Has00].

Tables [AJO08, KB39, RBF08]. Tag [KKJ07]. tagging [BP05]. Tags [OS06, AC04b]. Taipei [Lai03]. Taiwan [Lai03, Ano03a]. Takagi [LKYL00].

Takagi-cryptosystem [LKYL00]. Takaragi [WHLH03]. Taking [CDS07, Lai07, PM00]. Talbot [Rot07]. Talk [FGM00a, Lan00d].

tamer [Kap05]. Taming [Aba00, Lov01]. Tamper [LTM00, CT02]. tamper-proofing [CT02]. tampering [PS08b]. tandem [DPT02]. tank [Pau03].

tar [Str02]. targama [MAaT05]. target [BD04b]. Targets [MV01, Pau03].

Tarragona [DFPS06]. tasks [XQ07]. Tate [Jou02, SKG00]. TATSU [TSS00]. tatting [CSK08].

tc [DKU05]. TC-11 [DKU05]. TC-6 [DKU05]. TC11 [ELvS01]. TC8 [DFCW00].

TCC [HR06, Kil05, Nao04]. TCP [CD01b, Ols00, SBB05].

TCCB [SBB05]. Test [BT02, HSS04, Lan00b, LN08, RSN+01, Way02a, DS00, GMG00, Kat05a, KKKP05, RSS04]. testable [RMPJ08].

Testing [III00, CGBS01, Fil02, Lut03, SB00, WA06, Lut03]. Tests [MT02, NM09, GT02, Gut04c]. Text [Lut02, PJH01, PM08]. textbook [BJN00, PP09]. Thank [CMB05]. Theft [CMS09].

Their [AGT01, CD00a, Gen04a, JKRW01, LLL+01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, TO01, WV00]. Them [WD01a, Teo06]. Theorem [AC02, Eke02, GN01, Sh00a, Sch00, YKL03].

theorems [MW04, Nyb01]. Theoretic [CB01, DHR00, Kat05b, Nio02b, VVS01, VDKP05, wW01, Mar05b, NR04, Shp09, Wag03]. Theoretical [SGB01, PRS04].

Theoretically [AP09, DM00b]. Theory [AC00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bii03, Boy01, CC04a, Cra05a, Des02, Fa07, HR06, Hay06, IZ00, Rd01a, Kim01, Knu02, Lai03, Lee04b, Lau05b, MNT+00, Mao04, NPS02a, Nao04, Ok00a, PY06, Pf01, Pre00, Rot05, Roy05, Sch06b, Shp03, Spr03, TW02, TW06b, Vau05a, WAl00, WG05, Yan00, YDK06, Zhe02b].
There [Bar00b, GW00]. thieves [NRR00].

Thinking [Pau03]. Thinking [See04, Sty04, CS07a, Sch03]. Third [AL06, BS01b, CGP03, HR06, IKY05, KNP01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QS00, CGH00b].

Thirty [ACM03b, ACM06, ACM00].

Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thiry-Fourth [ACM02]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT00]. Thoughts [Joh00].

Thought [MYC01]. Thought [NRR00].

Thoughts [Joh00].

Thoughts [Joh00].

Thoughts [Joh00].

Thoughts [Joh00].

Thoughts [Joh00].

Thoughts [Joh00].
[HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oku04, Poj06, Pre02c]. 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 [Pau02a]. tour [Pet08]. Town [KJR05]. Trace [Bor01, LNS02, NN03]. trace-and-revoke [NN03]. Traceability [BL03, HW05, WLWH05, WY05]. Traceable [LZL+01, CCH04]. traceback [CS04]. Tracing [KY01d, KY01e, LLL02, NNL01, SWN00, TT01, WRW02, WLZZ05, WH01]. tracings [RE02]. Track [Fox00, Joy03b, Nac01, Oku04, Poj06, PHM03, Pre02c, USE01b, USE02c, Men05, CAC03, CAC06]. Tracking [WCJ05, FNRC05, SZ08, TW+09]. Trade [AJO08, CMS09, Oec03, PS01c, Uni00f]. Trade-O [AJO08, Oec03]. Trade-Os [PS01c]. Tradeoff [LP02a, QSR+02, CW02, Ino05, NS05a, DK08]. Tradeoffs [BS00b, CTL01, SRQ+03, SU07]. Trading [PV06b, SW+09]. Traffic [FGL02, Mis08, Fei09]. Trail [DR02a]. train [Pri00]. Training [Coc02a]. Trader [KY01d, KY01e, LLL02, SWN00, TT01, WH01]. Transacted [HBDJL01]. Transaction [RH02, AKD09]. Transaction-Based [RH02]. transactional [ST06]. transactions [Cal00b, Cal00a]. Transcript [An01a, An01b, An01c, An01i, An01j, An01k, Mal02, Nik02]. Transfer [CT08b, Din01, GKM+00, KKL09]. Transferability [HSZ00]. Transfers [IKNP03]. Transform [ABM08, BR09, CPhX04, KC09b, LKLK05, Nak01, SSFC09, VK07, BR06, Che07, OP01b, SR00, LPZ06]. Transformation [CT09, HLL05, DSP01]. Transformations [Fel06, KYHC01, LMTV05, Pag03]. transforms [Laf00]. Transient [Ric07, VS08]. Transistor [Coc02a]. Transistors [Bar00b]. Transit [Con00, Cal00c]. Transition [Asc02, TL07]. Transitioning [An09b]. Transitive [BN02]. Translation [GGS+09, PY06]. Translation-based [GGS+09]. TransLink [Cal00c]. Transmission [MLC01, SNR04, SVDF07]. Transparent [CCDP01, Por01, Lin00a]. transport [BR00]. Trapdoor [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]. treats [MAaT06, MAaT07]. Treatment [CL05, DK08]. Tree [CC05d, GST04, JLS03, KPT04, LKLK05, LM02, TNM00, Mon03, PCC03, WL02]. Tree-Based [GST04, KPT04]. trees [Che02, Che07, TC00]. Trends [Ahn08, KB07, Or00, NdM06, PRS04]. tricks [All03]. triggered [HHJS04]. tripartite [SW05]. Triple [HS0+01, BR04, CBGS01, Cor00a, FZH05, Ke05, LMP+01]. Triple-DES [Cor00a, LMP+01]. Triangles [FS01b]. Tripwire [Tvk0+01]. trivial [KO00]. troubleshooting [HWJ05]. True [BST03, Cha04, DV08, EHK+03, HBF09, Pan07, SFDF06, BG08, BG09, GB09, Hau06, HlWZ09, Ste05c, vT01, VKS09]. Truecrypt [CSK08]. truly [BGL+03]. Truncated [CS05b, KM02, LHL+02, SKU+00, SKI01, GS09]. Trust [CHSS02, HCOD02, Lin00b, LHL+08, Mit02, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, LLW09]. Trusted [DK01, WH01, WV01, AR08, PS04c, ZYL05]. Trusting [CKS09]. trustworthy [CCH05]. Truth [MNT+00]. Tseng [Hwa05, XY04, ZAX05]. TTM [GC00b]. Tuesday [Uni00a, Uni00f, Uni00c]. tunable [LB05]. Tunny [Sal01a]. Turin [AL06].
Turing [Bar00b, RSA03a, Adl03, Coo03, Cop04b, Goo00, Pet08, Riv03, Sha03b].
Turkey [Bor00].
Turkish [DD02].
Turn [Tsa07].
Turning [DJLT01].
Tweakable [DS08, HR03, LRW02].
Twentieth [Gan01b].
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].
TWIRL [Kal03, ST03b].
Two [Ahm08, BDG+01, DIS02, FD01, Hen06b, HSIR02, HSS01, HU05, HLT01, HL05b, JZCW05, KCP01, KO04, KTC03, KI03, LIN01b, MR01a, ML003, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, Ste05a, Ste1, TW07, WW05, X05, YYWD08, YYDO01, CLOS02, DHL06, GCKL08, JW01, LMT05, MS09c, MCHN05, Pau01, ZLX99, dB07].
Two-Block [KCP01].
two-channel [MS09c].
two-factor [Hen06b, Sch05c, St.00, Ste05a, YYWD08, dB07].
two-level [DHL06].
two-Party [KO04, Lin01b, MR01a, WW05, CLOS02, GCKL08, JW01, ZLX99].
two-Pass [SK00].
two-tier [TW07].
two-Way [DIS02].
TWOBLOCK [Yan05].
Twofish [BF00b, FKSW00, IK00, Kel00, Knu00a, Knu00b, Luc02a, Mur00, SKW+00].
type [CKQ03, Dug04, Him01, KYHC01, PDMS09, RMS05, Vir03, GG08, PQ06, Shaftid].
type-based [Dug04].
type-Passing [Vir03].
typed [BG07b, FR08].
types [Gor02a, GJ03, RXA00e, BFM07, Llan05].
typical [BSC01a].
typing [GJ03].
Tzeng [QCB05a, Hsu05a, HL05d].
U [DB04].
U-boat [DB04].
U.K. [CAC06].
U.S [Uni01].
UB [Bol02, PM00, Uni00b].
Ubiquitous [Stat03, LHK+04].
UC-soundness [BPS08].
UCON [LY05, PS04b].
UK [CZ05, Chr00, Chr01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sm05, Hon01].
Ultimate [Dif01].
ultra [Ban02, CH07a, DB04, Cal01, Win00].
ultra-lightweight [CH07a].
ultra-secret [Ban02].
Ultrafast [FP01a].
UltraSONIC [MMH02].
UMTS [Cha05b, HL07].
Unauthorized [Ano02c].
Unbalanced [FMP03, May02, HLLL03].
Unbelievable [Len01].
Unborn [Pau02a].
Unbounded [RW02, WV02].
Unbreakable [Ver06b].
Uncertain [Sec04, Sty04, Sch03].
UNCITRAL [MNFG02], uncompletable [NS01a].
Unconditional [HM01b, May01, Pas05, WW03b, WW05].
Unconditionally [HSZ00, HSZ01, HSHI02, HSHI06].
Uncovering [MNT+00].
Uncrackable [Ano03c].
Undeciphered [Rob02, Rob09].
Undeniable [GMP01b, GM03, JSJK01, Miy01, WQ01, CH05, LH04, LCZ05a, SSM+08].
undergraduate [AA04b, Gha07].
undergraduates [DFG04].
Understanding [CPG+04, CRA05b, Elb09, Gor06, PP09, Sun05, Lmn09].
undetachable [BMW02b].
Unexpectedly [Bar00a].
Unforgeable [BKY02, KY01a].
Unicode [MJF07].
Unified [CBZ+01, HKA+05, MFS+09, SM03b].
Uniform [SP08, TL07, SU07].
uniformity [Shp01, Shp04b].
unimodular [CV03].
Unique [Lam91, Lys02, TH01].
United [DFCW00, JL01].
Universal [BOHL+05, CR03, CJP02, CS02, Ifr00, KKKP05, KO03, Pli01, Sh00a, SP99, Cal00c, PS04c].
universal [DS02].
Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DN02b, DNS05, NMO05, RK05].
Universally-Composable [AF04b].
Universiteit [BBDO9].
University [Kat05b, Puc03, Rot07, Top02].
UNIX [CDP01, Har01a, Har01b, H601, Wit01].
[Man01, RSA00e]. v2.1 [RSA02]. v2.11
[RSA01]. V5 [It00]. V5.1a [CSK+08]. Vail
[BC01]. valid [Wan04b]. valid-signature
[Wan04b]. Validation [ABRW01, BLM01,
KCI+01, BG09, ME08b, VM03]. Validity
[Zho02]. Valuable [PM00]. Value [BR09,
GJS05, LS08, BMW02a, DK08, WWTH08].
valued [DZL01, MS02b]. Vancouver
[IEE02]. Varadharajan [CJ03].
Varadrajan [MS03a]. variable [SV08a].
Variables [HR04a]. Variant
[Luc02b, NSN05, Ber08, Duj08, Duj09].
Variants [BDK+09, DG02, KS00b, CJ05,
Sha04b, TJ03]. Varieties [RS02].
Variety [AOS02]. Vascular [BdhKB09]. vault
[SHL07]. Vector [AS08, Che03c, DNP07,
SBG02, WC04, Pei09, mSgFlL05, WNQ08].
vectors [LHL04]. Vegas [ELvS01, IEE01a].
Vein [BdhKB09]. Vendors
[Pau03, MV03b]. Venona [Ben01b, Ben04].
Verenigde [dL00]. Veridicom [An02d].
Verifiable [ANR01, Ate04, CD00a, CS03a,
CHS05, Cha04, JLL02, JG01, Lys02,
NZC05, NZS05, NSN05, NN06, CHY05a,
CDD00, GKH01, KKL09, SC05a].
Verifiably [BGLS03, Hes04a].
verifiably-encrypted [Hes04a].
Veriﬁcation
[AAK05, Ara02, BPST02, BP05, GMV01,
GL00, Gut02b, Gut04a, HWH01, Hoe01,
Str01a, BD04a, CC05b, CJL06, Cohl03, DS00,
HL05c, JWO1, Ler02, MD04, MT07, MSP09,
PBB07, TYH04, Wan04b, Wu01, YLC08,
ZLK99, ZL04b, CS08b, Uzu04].
Veriﬁed
[BJP02, BFGT08, BFCZ08, CJT04].
Verifier
[Bla01b, LKY05b]. veriﬁer-based
[LY05b]. Veriﬁers
[CL01a, He02, LV07, LWK05b, YY05a, ZX04].
Verify
[MS02a]. Verifying
[BFG08, BJvdB02, CJM00, HLTO1, IR01,
PT08, RR02, BLH06, BLP06, HLH00,
SV08a, Sha01d]. Verlag
[Eag05, Lee03a, Lee03b, Pap05]. Version
[Bol02, HPC02, OST05, SKI01, Mis06].
Versions
[HSR+01, NPV01, An00f, CV05].
Versteckte [Sch09]. Versus
[Mad00, Rub00, WWS+02, ASW+01,
BJLS02, DBS01, WPP05]. Vertically
[DN04]. Very
[AAC01, B+02, CG03, EBC+00, FLA+03,
Höf01, PM02, PBM01, Zir07]. Vestiges
[Top02]. VI [Sch04a]. via
[AGK07, An00k, AC05, BDP09,
Car02, Che03, CGP+04, FBWC02, Fox00,
HHY07, HML03, J00a, KT06, ML05,
PG05, RG05, SB01, SLG+05, ZL01, L05].
Victoria
[ACM08, IZ00]. Victorian
[Top02]. victory [Hau03]. Vid [CAC06].
Video
[BD+01, BD03, CD00c, EFY+05,
ISS08, KBD03, KJ05, LHS05,
MLC01, SC02a, BS01b, JA02, KN03, UP05].
Video-Based
[KJR05, BS01b, KN03]. videos
[YZD07]. Vienna [BZ02].
Vietnam
[Lov01]. View
[Bar00a, Mah04, Sin09]. Views
[Bar00a, Bar00b, Bar00c, C01a, C02a,
C02b, C03]. Vigenère
[DG00]. Villes
[IEE01b, Sch05a]. VIII
[Sch04b]. VII
[IEE01b, Sch05a]. Virginia
[MS05b]. Virtual
[An01c, HM01a, Pr00,
YS+01, BD+09a, ML05, ZBP05].
virtualization
[CGL08a, CGL08b, CGL08c].
virtualization-based
[CGL08a, CGL08b, CGL08c]. Virtues
[Tro08]. Virus
[G06, An05b]. Visible
[HT06]. Vista
[Fer06]. Visual
[BDN00, BDDS03, BCD06, CCL09, CTO09,
CPO06, DD00, Kog02, K03, RD09,
WMS08, YWC08, YC01, ZP05, ABS01,
CDFM05, CDD07, DD04, HKS00, La09,
PY08, Yan02, YC07, Bon00, Zol01].
Visualization
[XY09, MFS+09]. Viterbi
[LBGZ01, LBGZ02]. Vladimir
[Puz04]. VLDB
[EBC+00, FLA+03]. VLDP
[B+02]. VLSI
[KV01]. VMSS
[SC05a]. Voice
[An00l, PK01, V04]. VoIP
[An08c, ZS08, VAY09, WJC05]. vol
[Kat05b, Lee03b]. volatile
[SETB08].
Wiretapping [Cho08a, DL98, Jan08a, DL07]. WISA [CSY09]. Within [MR02a, CHM02, MR02b]. Without [BCL05b, Bla01c, BB04, BGH07, Har06, NA07, Ano03b, CH01a, CCK04b, CYH04, CCH05, CTH08, C04, CDD07, CNV06, DK01, KG09, Ku04, LV07, LW04, LKY05b, LL06, LCZ05b, Lys07, MP02, Mar07, PS04c, RG09, WH01, YW05, YRY05b, ZW05a]. Withstanding [DFS04]. Wits [Bud00a, Bud02]. WLAN [SSM08]. WLAN/cellular [SSM08]. Woes [BTTF02]. Women [FF01b]. won [Hau03]. Worcester [KP01]. Word [HR00, SKU00]. Word-Oriented [HR00, SKU00]. Wordlengths [PG05]. words [GS01, Max06, NS01a, VS01]. Work [DFG01, DNW05, Fox00]. Working [DFCW00, ELvS01, KB00]. workload [BGM04]. Works [Net04]. Workshop [ACM05a, Ano05b, AL06, BDZ04, BBD09, BD08, C05, Chr00, Chr01, CCMR02, CCMR05, CSY09, DR02c, Des02, GH05, IEE01b, IZ00, Joh03, JQ04, KKP02, KCR04, KGL04, Kim01, KP01, KNP01, LST05, MJ04, MS05a, Mat02, NH03, PK03, PT06, RS05, RPM04, Sch00b, Sch01d, TBJ02, USE00b, VY01, Vau05a, WK03, Ytr06, AMW07, AJ01a, BCKK05, Bir07, CKL05, GSK05, HH04, HH05, HA00, ST01d]. World [Ber03, GG05a, HW01, Nik02a, Sch00d, Sty04, YKMB08, Ano03b, Ar05, Bel07a, HHG06, Hus01, KPS02, Kee05, Lie05, Lun09, Rob02, Rob09, Hau03, SL07, Bec02, Bud00a, Bud02, M04, Sch01d, TBJ02, USE00b, VY01, Vau05a, WK03, Ytr06, AMW07, AJ01a, BCKK05, Bir07, CKL05, GSK05, HH04, HH05, HA00, ST01d]. Worlds [Wil01b]. Worm [LJK05, CSW05]. Worms [ZGTG05]. Worst [CCM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case [HRS08, Mic02a, Mic02b, Pei09]. worst-case/average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. Wrapper [Ols00].
References

Al-Akaidi:2004:FSP


Aly:2004:CSP

Alaaeldin A. Aly and Shakil Akhtar. Cryptography and security protocols course for undergraduate IT students.
REFERENCES


Agreste:2008:NAP


Apers:2001:PTS


Al-Azzoni:2005:MVC


Anshel:2001:NKA


Almgren:2000:HWC


www.simonsingh.com/cipher.htm. See [Sin99].


REFERENCES

Abadi:2000:TA

Abdalla:2005:SER

Ateniese:2001:ECV
REFERENCES

ng/10/41/16/186/20/29/
article.pdf.


[ABM00] Todd Austin, Jerome Burke, and John McDonald. Architectural support for fast symmetric-key cryptography. ACM SIGPLAN Notices, 35(11):178–189,
REFERENCES


0558/bibs/1880/18800255.html; http://link.springer-ny.com/link/service/series/[ACM00]
0558/papers/1880/18800255.pdf.


REFERENCES


REFERENCES


[ACM09] ACM, editor. STOC ’09: proceedings of the 2009 ACM International Symposium on Theory of Com-


[ACTZ05] Rafael Álvarez, Joan-Josep Climent, Leandro Tortosa,

**Ahmad:2007:ADE**


**Anyanwu:2009:DCS**


**Avanzi:2006:ESM**


**Arnold:2007:CSE**


**Adikari:2009:HBT**

REFERENCES

[BCDH09], pages 76–83.
URL http://www.ac.usc. es/arith19/.


REFERENCES

Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR


Attrapadung:2006:FSS

REFERENCES

Akkar:2001:IAS

Acquisti:2009:PSS

Akavia:2006:BO

Akavia:2010:EBO

Alon:2007:GSE

Anagnostopoulos:2001:PAD
REFERENCES

bibs/2200/22000379.htm;
http://link.springer-
y.com/link/service/series/0558/papers/2200/22000379.pdf.


REFERENCES

Attali:2001:JSC


Attali:2001:SCP


Aid:2008:NSA


Avoine:2008:CIT


Al-Jarrah:2008:NKM

Omar Al-Jarrah and Ramzy Saifan. A novel key management algorithm in sensor
REFERENCES


REFERENCES


REFERENCES

Atzeni:2006:PKI

Anshel:2007:RME

Allman:2006:MAW

Alvarez:2000:SMC

Amadio:2002:SRP

Allen:2003:EST

Amadio:2000:CCP
REFERENCES

PYLAAG. ISSN 0375-9601 (print), 1873-2429 (electronic).


See [kWpLwW01, WLW04].


Aura:2001:RA


Anonymous:2000:AIIa


Anonymous:2000:AIIah


Anonymous:2000:CRR


Anonymous:2000:CCI


Anonymous:2000:CLI


Anonymous:2000:EES

Anonymous:2000:GBE


Anonymous:2000:PESa


Anonymous:2000:PTD


Anonymous:2000:SES


Anonymous:2000:UAS


Anonymous:2000:VAS


Anonymous:2001:AAPb

REFERENCES


Anonymous:2001:EMB


Anonymous:2001:LBS


Anonymous:2001:PKC


Anonymous:2001:SCS


Anonymous:2002:DEC


Anonymous:2002:IHB

Anonymous:2002:NSD


Anonymous:2002:PPD


Anonymous:2002:PFQ


Anonymous:2002:QCQ

Anonymous:2002:QCR


Anonymous:2002:RUB


Anonymous:2003:TMC


Anonymous:2003:NAW


Anonymous:2003:NUP


Anonymous:2003:TMP

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1913</td>
<td>E. Fauquembergue</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1876</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>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. Woltman</td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>756839</td>
<td>1992</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud et al. (GIMPS)</td>
</tr>
<tr>
<td>36</td>
<td>2979221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala et al. (GIMPS)</td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>2001</td>
<td>M. Cameron (GIMPS)</td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>M. Shafer (GIMPS)</td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2004</td>
<td>Josh Findley (GIMPS)</td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2005</td>
<td>Martin Nowak (GIMPS)</td>
</tr>
<tr>
<td>43</td>
<td>30402457</td>
<td>2005</td>
<td>Curtis Cooper &amp; Steven Gagel</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven Gagel</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>
<tr>
<td>49</td>
<td>74207281</td>
<td>2016</td>
<td>Curtis Cooper (GIMPS)</td>
</tr>
<tr>
<td>50</td>
<td>77232917</td>
<td>2018</td>
<td>Jon Pace (GIMPS)</td>
</tr>
</tbody>
</table>
Anonymous:2003:UCD


Anonymous:2004:CPS


Anonymous:2004:CJL


Anonymous:2004:NGJ


Anonymous:2005:CEC


Anonymous:2005:WAS


Anonymous:2006:JHD


Anonymous:2006:RC

Anonymous:2006:SSD


Anonymous:2006:SQE


Anonymous:2007:CPSh


Anonymous:2007:CPSf


Anonymous:2008:KAD


Anonymous:2008:RCB


Anonymous:2008:RES


Anonymous:2008:SHS

REFERENCES


Anonymous:2012:SHS

Anonymous:2001:SR

Anonymous:2009:DSS

Anonymous:2013:DSS

Anonymous:2009:TCA

Anonymous:2012:SHS

Anonymous:2001:FAA

**ANSI:2005:AXP**


**Abe:2000:PSP**


**Abe:2002:SVK**


**Alomair:2009:ITS**


**Appenzeller:2005:IBE**

Guido Appenzeller. Identity-based encryption from algo-
REFERENCES


REFERENCES


REFERENCES


[Ate04] Giuseppe Ateniese. Verifiable encryption of digital signatures and applications. *ACM Transactions on Inform-
Androutsellis-Theotokis:2004:SPP


Aharonov:2000:QBE


Alster:2001:PKC


Arnold:2004:IPN


Avanzi:2003:CAD

REFERENCES


REFERENCES


[Ban05] William D. Banks. Towards faster cryptosystems, II. In Garrett and Lieman [GL05],

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.

Nicholas Baran. News and views: More on tiny transistors; 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/.


REFERENCES


[Bau01c] Mick Bauer. Paranoid penguin: The 101 uses of...
REFERENCES


REFERENCES


[BB05] Kemal Bicakci and Nazife Baykal. Improved server...

**Biham:2002:SQK**


**Behrmann:2002:UIS**


**Bernstein:2009:PQC**


**Beimel:2000:CFS**

REFERENCES

Blumenthal:2002:SAD


Bartolini:2008:EIS


Barkan:2003:ICO


Bertoni:2003:EAD


Bellare:2001:OCH

Mihir Bellare, Alexandra Boldyreva, Lars Knudsen,

**Bellare:2000:PKE**


**Bellare:2009:HPK**


**Bobineau:2000:PSD**


**Boneh:2004:SGS**


**Burgess:2001:ISC**

N. Burgess and L. Ciminiera, editors. *15th
REFERENCES


Biham:2004:NCS


Blundo:2004:SIA


Backes:2005:PKS


Blundo:2005:SCN

Brzeziński:2005:MRL


Bergadano:2001:CSA


Blundo:2006:VCS


Bruguera:2009:PIS


Brier:2001:CRS

REFERENCES

2009. URL http://www.ac.usc.es/arith19/


REFERENCES

Butler:2006:FAK

Barni:2005:DWI

Bao:2005:PSS

Barak:2005:SCA

Bresson:2001:PAG
REFERENCES


Betarte:2000:SSC


Bao:2005:RWH


Biham:2000:CAG


Boneh:2000:CRP


Bourbakis:2003:SBC


Bozzano:2004:AVS

REFERENCES

JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

**Burmester:2004:HPK**


**Buchmann:2008:PQC**


**Blundo:2003:COT**


**Bolosky:2000:FSD**

Bao:2001:SPD


Bodei:2005:APS


Bao:2001:CTS


Bhattacharyya:2009:VPA

[DhKB09] D. Bhattacharyya, P. Das, T. h. Kim, and S. K. Bandy-

**Biham:2002:EDL**


**Biham:2002:LCR**


**Biryukov:2009:KRA**


**Blundo:2000:VCG**


REFERENCES


L. Bello. openssl — predictable random number
REFERENCES


Thomas A. Berson. Cryptography everywhere. *Lec-
REFERENCES


2. Berson:2003:CAB


5. Bernstein:2009:IPQ

   Dirk Bouwmeester, Artur K. Ekert, and Anton Zeilinger. The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation. Springer-Verlag, Berlin, Germany / Heidelberg, Ger-
REFERENCES


REFERENCES


[BFG04] Karthikeyan Bhargavan, Cédric Fournet, and Andrew D.
REFERENCES


REFERENCES

[144]


Dan Boneh, Craig Gentry, Ben Lynn, and Ho-"{v}av Shacham. Aggregate


REFERENCES


for pseudo-ransom generation with applications to 
\texttt{/dev/random}. In Meadows and Syverson [MS05b], pages
order number 459050.

\section{REFERENCES}

\begin{thebibliography}{9}

\bibitem[BH06]{BH06} Mohamad Badra and Ibrahim Hajjeh. Key-exchange aut-
CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

\bibitem[BHM03]{BHM03} James Backhouse, Carol Hsu, and Aidan McDonnell. Tech-
nical opinion: Toward public-key infrastructure interoperability.
\textit{Communications of the Association for Computing Machinery},
46(6):98–100, June 2003. CODEN CACMA2. ISSN 0001-0782 (print),
1557-7317 (electronic).

\bibitem[BI04]{BI04} J.-C. Bajard and L. Imbert. A full RNS implement-
ation of RSA. \textit{IEEE Transactions on Computers},
53(6):769–774, June 2004. CODEN ITCOB4. ISSN 0018-9340 (print),
&arnumber=1288551.

\bibitem[BI05a]{BI05a} Omer Barkol and Yuval Ishai. Secure computa-
tion of constant-depth circuits with applications to database search problems.
In Shoup [Sho05a], pages 395–?? ISBN 3-540-28114-2. ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
C79 2005; QA76.9.A25;
QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; Internet. URL http://
3621.

\bibitem[BI05b]{BI05b} Amos Beimel and Yuval Ishai. On the power of non-
linear secret-sharing. \textit{SIAM Journal on Discrete Mathematics},
CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146
(electronic). URL http://
epubs.siam.org/sam-bin/dbq/article/41286.

\bibitem[Bi09]{Bi09} Chengpeng Bi. A Monte Carlo EM algorithm for De
Novo Motif discovery in biomolecular sequences. \textit{IEEE/ACM Transactions on
CODEN ITCBcy. ISSN 1545-5963

\end{thebibliography}
REFERENCES

Bidgoli:2003:EIS


Biggs:2008:CII


Biham:2000:CPR


Biham:2002:HDE


Biham:2003:ACE


Beimel:2000:RSC

Amos Beimel, Yuval Ishai, and Tal Malkin. Reduc-


REFERENCES


[BJvdB02] Cees-Bart Breunesse, Bart

[BK00]

[BK05]

[BK07]

[BK06b]

[BK06a]
<table>
<thead>
<tr>
<th>REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Barreto:2002:EAP</strong></td>
</tr>
<tr>
<td><strong>Breveglieri:2007:OCA</strong></td>
</tr>
<tr>
<td><strong>Bellare:2004:BPR</strong></td>
</tr>
<tr>
<td><strong>Bajard:2009:SRB</strong></td>
</tr>
<tr>
<td><strong>Bellare:2000:SCB</strong></td>
</tr>
<tr>
<td><strong>Blum:2003:NTL</strong></td>
</tr>
</tbody>
</table>
REFERENCES

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

Buonanno:2002:IUE


Broadfoot:2002:ASA


Bucci:2008:FDR


Black:2000:TDE

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

Blanchet:2001:ACP


Blanchet:2001:ECP

REFERENCES

shop, page 82. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. ISBN ???? LCCN ???? URL ????.

Blaze:2001:LYS


Blancchet:2002:SAS


Blaze:2002:CI


Blaze:2003:FCI


Burmester:2009:UCR

REFERENCES


REFERENCES

issn=1433-2779&volume=8&issue=1&spage=57.

**Buchmann:2009:PQC**


**Banks:2001:CAS**


**Blunden:2009:RAE**


**Batina:2001:AWD**


**Blomer:2001:LSE**


**Brincat:2001:KRA**

[BM01c] Karl Brincat and Chris J.

**Basu:2003:AC**


**Blomer:2003:NPK**


**Boyd:2003:PAK**


**Burke:2000:ASFa**


**Burke:2000:ASFb**

REFERENCES

RED8. ISSN 0163-5980 (print), 1943-586X (electronic).


REFERENCES


REFERENCES


Boneh:2000:TC


Bellare:2002:PRI


Bellare:2002:TSB


Bouganim:2003:CSD


Bouganim:2008:DAC

Luc Bouganim, François Dang Ngoc, and Philippe Pucheral. Dynamic access-control policies on XML encrypted data.


REFERENCES


Barak:2003:DC


Barak:2007:DC

REFERENCES

Boyd:2001:ACA


Boyen:2003:MIB


Bedi:2001:CNF


Burnett:2001:RSO


Bellare:2002:GSI

Mihir Bellare and Adriana Palacio. GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In Yung [Yun02a], pages 162–177. CODEN LNCSD9. ISBN 3-540-44050-X (paperback). ISSN 0302-9743
REFERENCES

(165)


[BP03a]


[BP04]

Buchbinder:2003:LUB


[BP05]

Blanchet:2005:VCP


[BP06]

Beissinger:2006:CUM

REFERENCES


[Backes:2008:KDM]


[BPST02]


/Bellare:2000:ETE


[Brandao:2001:UEC]


[Benerecetti:2002:VST]


Mihir Bellare and Thomas Ristenpart. Multi-property-preserving hash domain ex-

[Bhatnagar:2009:RRW]

[Brands:2001:RPK]

[Bra01a]

[Brands:2001:RPK]

[Brown:2005:CEC]

[Black:2002:BBA]
REFERENCES

Butler:2009:LIB

Brustoloni:2006:LEN

Bierbrauer:2000:AIW

Biryukov:2000:CTM

Barrett:2001:SSS
REFERENCES


REFERENCES


REFERENCES


[Blake:2004:AEC]


REFERENCES

Barak:2003:TRN

[BST03]

Biryukov:2001:RTC

[BW01]

Bethencourt:2009:NTP

[Biehl:2002:NDP]

[BTTF02]

Boyer:2002:LDS
John Boyer, Andrew D. Todd, Jason Trenough, and Doug Farrell. Letters: Defective sign-and-encrypt and healthcare woes and

Beimel:2005:CIW


Beimel:2008:CIW


Black:2002:SCA


Buchmann:2000:CTC


Buchmann:2000:IC


Buchmann:2001:IC

Johannes Buchmann. *Introduction to cryptography*. Un-

Buchmann:2004:IC


Budiansky:2002:BWC


Budiansky:2006:HMS


Buhans:2006:FBL

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

Bulygin:2009:PSS

REFERENCES


Wade H. Baker and Linda Wallace. Is information security under control?: Investigating quality in information
REFERENCES


[Butler:2000:NSA]

[Bellare:2003:FSP]
Mihir Bellare and Bennet Yee. Forward-security in private-key cryptography. In Joye [Joy03b], pages 1–18.

[Bertlmann:2002:QUB]
Reinhold A. Bertlmann and Anton Zeilinger, editors. *Quantum [Un]Speakables: From Bell to Quantum Information: Conference in Commemoration of the Physicist*...
REFERENCES


CAMTC:2000:TSC


Calvocoressi:2001:TSU


Canetti:2001:UUCS


Canetti:2006:SCC


Cantraut:2001:OPR

REFERENCES


Carriere:2000:PSC

Carter:2001:SCT

Carlet:2002:LCC

Casey:2002:HCC

Casselman:2006:MTE

Cobas:2001:CTA
REFERENCES

0558/papers/2178/21780233.pdf.

Cooper:2005:AAP


Chandramouli:2006:BPA


Cachin:2000:OFS


Chan:2001:CRP


Carline:2002:NWT


Chan:2002:SLI


REFERENCES

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

CC05d

CC05e

Chen:2008:SNI

Chang:2009:FDI

Chan:2001:WEF

Chuang:2006:USF
REFERENCES

Collberg:2004:DPB


Chen:2004:TPM


Chai:2007:EIB


Chang:2005:DSM


Cattaneo:2001:DIT


Chang:2004:IDA


Chang:2004:SOT

[CCK04b] Ya-Fen Chang, Chin-Chen Chang, and Jui-Yi Kuo. A

Chang:2009:PCC


Christianson:2001:PKC


Choi:2005:JMA


Christianson:2002:SPI


Christianson:2005:SPI

Bruce Christianson, Bruno Crispo, James A. Malcolm,


REFERENCES


[CDD00]

Carpenter:2000:CB


[CDD01a]

Cramer:2001:SDL


[CDD+05]

Cimato:2007:CVC


[CDD07]

Ceselli:2005:MAI


[Cavallar:2000:FBR] Stefania Cavallar, Bruce

Cortier:2006:SAP


Cramer:2000:GSM


Chawla:2005:TPP


Coron:2005:MDR

REFERENCES


REFERENCES

Certicom:2004:CCC


Canetti:2001:UCC


Canteaut:2001:COR


Cramer:2002:OBB


Cohen:2006:HEH


Courtios:2001:HAM

Nicolas T. Courtios, Matthieu Finiasz, and Nicolas Sendrier.
REFERENCES


Chodowiec:2003:VCF


Cranor:2005:SUD

Candebat:2006:SPM

Chodowiec:2001:ETG

Caballero-Gil:2009:GBA

Catalano:2000:CIS

Coppersmith:2000:ICT
REFERENCES


Catalano:2001:BSP


[CGH01]

Caballero-Gil:2006:SSB


[CGHG06]

Crosby:2002:CHB


[CGJ02]

Chen:2008:OVBa

[Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmaniam, Carl A.]

[CGL+08a]

Chen:2008:OVBB


Chen:2008:OVBC


Caballero-Gil:2007:PSC


Canovas:2002:DSB


[CH01a] Chin-Chen Chang and Kuo-Feng Hwang. Towards the forgery of a group signature without knowing the group center’s secret. Lecture Notes in Computer Science, 2229:47–??, 2001. CODEN LNCS69. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:
REFERENCES


REFERENCES

Chandra:2005:BWS

[Cha05b]

Chakrabarti:2007:GCS

[Cha07]

Chang:2001:NEA

[CHC01]

Chen:2004:MCK


Chen:2005:EUG


Chen:2000:JCT


Chen:2001:DEU

[Che01a] Chau-Chin Chen. Data encryption using MRF with
REFERENCES

Chen:2001:PDP


Chen:2001:NVR


Chen:2002:SFS


Cheng:2003:PPO


Chen:2004:IAM

REFERENCES


[CHH01] Robert S. Coulter, George Havas, and Marie Henderson. Giesbrecht’s algorithm, the HFE cryptosystem and Ore’s $p$-

**Choi:2009:KDK**


**Chien:2008:EPA**


**Chien:2008:SCA**


**Coron:2001:GGC**


**Coron:2001:OCC**

Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen. Optimal chosen-ciphertext secure encryption of arbitrary-length messages. Lecture Notes in Computer
Coppersmith:2002:CSC


Canetti:2003:FSP


Cheon:2008:PST


Chang:2002:IBO

REFERENCES

Chao:2009:HCS

Chen:2002:CPK

Choi:2006:CHP

Choo:2008:PLP

Chowdhury:2008:CBG

Christianson:2000:SPI
REFERENCES


REFERENCES

406 pp. LCCN QA76.8.I83
URL http://www.intel.
com/intelpress/sum_scientific.htm.

[Chu02]

[CHVV03]

[Cin02]

[CHY05a]

[Cir01]
Horatiu Cirstea. Specifying authentication protocols us-
REFERENCES

ing rewriting and strategies. 

**Cheon:2003:PTA**


**Cheien:2003:PTA**


**Chien:2004:IAM**


**Chien:2005:EDS**


**Chien:2005:EDS**

REFERENCES

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

**Cornwall:2004:AAM**


**Choie:2005:EIB**


**Clarke:2000:VSP**


**Coron:2000:NAP**

REFERENCES

Coron:2002:UPS


Chepyzhov:2001:SAF


Chien:2001:MRL


Chien:2003:CMV


Chien:2004:SIS

REFERENCES

December 2004. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).


[CKK03] Yon Dohn Chung, Jong Wook Kim, and Myoung Ho Kim. Efficient preprocessing of XML queries using structured signatures. Information Processing Letters,
REFERENCES

Chun:2003:DLC


Chen:2009:SRP


Coppersmith:2000:KRF


Coron:2000:FLA

REFERENCES


[Coron:2001:SSL]

[CKN01]

Canetti:2003:SEA

[CKN03]


Cachin:2001:SEA


Cathalo:2003:NTT

Julien Cathalo, François Koene, and Jean-Jacques

code...
REFERENCES


[Camenisch:2001:IES] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with ap-
REFERENCES

pointed verifiers. In Kilian [Kil01a], pages 388–??
no.2139. UK £47.00. URL
http://link.springer-ny.com/
link/service/series/0558/
bibs/2139/21390388.
htm; http://link.springer-
ny.com/link/service/series/
0558/papers/2139/21390388.

[CL01b] Chin-Chen Chang and Iuon-Chang Lin. Cryptanalysis of the improved user
efficient blind signatures. Lecture Notes in Computer
CODEN LNCS-D9. ISSN
0302-9743 (print), 1611-3349
link/service/series/0558/
bibs/2229/22290042.htm;
http://link.springer-ny.com/link/service/series/
0558/papers/2229/22290042.
pdf.

[CL02a] Jan Camenisch and Anna
Lysyanskaya. Dynamic ac-
cumulators and application
to efficient revocation of
anonymous credentials. In
Yung [Yun02a], pages 61–
76. CODEN LNCS-D9.
ISBN 3-540-44050-X (pa-
perback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
tocs/t2442.htm; http://www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2442.

[Cao:2002:TKE] Zhen Fu Cao and Ji Guo
Li. A threshold key escrow scheme based on ElGa-
amal public key cryptosystem. Chinese Journal of Computers = Chi suan chi hsueh
CODEN JIXUDT. ISSN
0254-4164.

[Crowley:2002:BLS] Paul Crowley and Stefan Lucks. Bias in the
LEVIATHAN stream cipher. Lecture Notes in Computer
CODEN LNCS-D9. ISSN
0302-9743 (print), 1611-3349
link/service/series/0558/
bibs/2355/23550211.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2355/23550211.
pdf.

[Camenisch:2002:DAA] Jan Camenisch and Anna
Lysyanskaya. Dynamic ac-
cumulators and application
to efficient revocation of
anonymous credentials. In
Yung [Yun02a], pages 61–
76. CODEN LNCS-D9.
ISBN 3-540-44050-X (pa-
perback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
tocs/t2442.htm; http://www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2442.

[Camenisch:2004:SSA] Jan Camenisch and Anna
Lysyanskaya. Signature
schemes and anonymous cre-
dentials from bilinear maps.
In Franklin [Fra04], pages


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.


**Cheon:2000:NBC**


**Canetti:2002:UCT**


**Chen:2009:AKD**


**Chang:2007:SIH**


**Clulow:2003:SP**

Czumaj:2002:PTA


Camenisch:2000:CSS


Cox:2002:FYE


Courtois:2003:AAS


Chevallier-Mames:2005:ECB


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).


REFERENCES


Chao:2000:CHC


Cid:2006:AAA


Cho:2008:DNP

REFERENCES

Caputo:2009:DIT


Crawford:2002:FEE


Coron:2004:SSL


Ciet:2003:PFI


Catalano:2002:HHL


Correia:2006:CAB


Shannon Cochran. News and views: School of Adaptive Computer Training; it seems like yesterday... [10th an-
niversary of the first Web
site]; double-gate transistor
breakthrough; 802.11g Stan-
dard proposed; 30th an-
iversary of the [Intel] 4004;
DeCSS legal decisions. *Dr.
Dobb’s Journal of Software
Tools*, 27(2):18, February
2002. CODEN DDJOEB.
ISSN 1044-789X. URL

[Coh03]

Shannon Cochran. News
and views: WaSP [Web
Standards Project] buzzes
off; Eclipse Project on
the horizon; semiconductor
roadmap: Ramping up, scal-
ing down; AES [Advanced
Encryption Standard]: Its
finally official; SMS [Short
Message Service] shines on;
Berners-Lee awarded Japan
Prize. *Dr. Dobb’s Journal
of Software Tools*, 27(3):
14, March 2002. CODEN
DDJOEB. ISSN 1044-789X.

[Coc03]

Ernie Cohen. First-order
verification of cryptographic
protocols. *Journal of Com-
puter Security*, 11(2):189–
216, 2003. CODEN
JCSIET. ISSN 0926-227X
(print), 1875-8924 (elec-
tronic).

[Col03]

Eric Cole. *Hiding in Plain
Sight: Steganography and
the Art of Covert Com-
munication*. John Wiley
and Sons, Inc., New York,
NY, USA, 2003. ISBN 0-
471-44449-9. xviii + 335
pp. LCCN QA76.9.A25 C598
2003. US$35.00.

[Con00]

Toulla Constantinou. Chicago
smart: Chicago Transit Au-
thority (CTS) joins “smart
card” revolution. *Mass tran-
sit*, 26(7):52–53, December
2000.

[Con03]

Sean Convery. *Network se-
curity architectures*. Net-
working technology series.
Cisco Press, Indianapolis,
IN, USA, 2004. ISBN
1-58705-115-X. xxxix +
739 pp. LCCN TK5105.59.
ISBN with [TCR03].
REFERENCES


[Copeland:2006:CSB]

[Corella:2000:FIT]

[Coron:2000:ESF]

[Coron:2002:SPP]

[Coron:2006:WC]

[Cosgrave:2000:NTC]
Costlow:2003:BIM


Courtois:2001:EZK


Courtois:2003:FAA


Courtois:2004:FSB


Courtois:2002:CBC

REFERENCES


REFERENCES


REFERENCES


Cramer:2002:UHP

Cramer:2003:DAP

Camenisch:2003:PVE

Creppeau:2003:SBR

Carrier:2004:STP
REFERENCES

Collberg:2005:SWF


Contini:2005:SAA


Cvejic:2005:IRL


Capaldi:2007:ADI


Chakrabarti:2007:PBA


Chatterjee:2007:CSC


Casey:2008:IFD

Eoghan Casey and Gerasimos J. Stellatos. The impact of full disk encryption
REFERENCES


Chang:2008:DAP


Cusick:2009:CBF


Czeskis:2008:DED


Cai:2007:CSM


Crandall:2005:DUV


Chen:2008:CCS

REFERENCES

jucs_14_3/cryptography_in_computer_system.

Chung:2009:ISA

Collberg:2002:WTP

Coron:2003:NAS

Chen:2008:BUK

Chu:2008:EOT
REFERENCES


Chou:2009:ATI


Crawford:2001:FPV


Chiang:2008:CPB


Chang:2004:ASS


Cheung:2001:TPS


Collberg:2007:DGB

Christian S. Collberg, Clark Thombarson, and Gregg M. Townsend. Dynamic graph-

Chen:2009:FCV


Cheng:2001:NPT


Curtin:2005:BFC


Chaitanya:2008:QQM


Canteaut:2002:DCH

REFERENCES


Chang:2002:ATI


Chess:2007:SPS


Chien:2001:CCW


Crosby:2009:OLR

Chien:2005:NRS


Choi:2002:ICH


Chen:2005:ENB


Chang:2008:EBD


Chang:2001:NSS


Chang:2004:TSSb

Ting-Yi Chang, Chou-Chen Yang, and Min-Shiang Hwang. A threshold signature scheme for group communications without a shared distribution center. *Future Generation Computer
REFERENCES


REFERENCES

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/citations/journals/cacm/2001-44-2/p11-crawford/. See [Sch00c].

Cheng:2005:RIC

[Xiaorong Cheng, Huilan Zhao, and Jitian Kou. Research and improvement on computer intrusion detection technology based on immune principle. In Han et al. [HYZ05b], pages 167–?? ISBN 981-270-153-2. LCCN ???. URL http://eproceedings.worldscinet.com/9812701532/9812701532.0031.html.]

CZK05

[Cheng:2005:RIC]

Cheng:2005:RIC

[Damgaard:2000:ECZ]

Dale:2001:BSA

[Damjoeb. ISSN 1044-789X. URL http://www.ddj.com/.]

Damgaard:2000:ECZ


Dalpha:2001:AAE

[Damaj:2007:P]

Damaj:2007:PAD


Danielyan:2001:AEE

[Dan01]

Danielyan:2001:AEE

[Dan01]

REFERENCES


REFERENCES


Doyle:2006:SCK [DD00]


DiVimercati:2005:CSE [DD02]


DeBonis:2000:RVC


Dalkılıç:2002:CPF

DeBonis:2004:RSS


Diene:2006:DLE


Dolev:2000:NC


Dolev:2003:NC


Desai:2000:ESS

[Des00a] Anand Desai. *Encryption schemes: security notions, designs and analyses*. Vita thesis (Ph.D.), University of


REFERENCES


Delgado:2007:SCD

  idtype=cvips.

Domingo-Ferrer:2000:SCR


Durante:2000:CAC


Durante:2001:CWR

DePalma:2004:CCS


Domingo-Ferrer:2001:CDS


Dodis:2003:IRP


DeSantis:2004:CKA


Domingo-Ferrer:2006:SCR


DiRaimondo:2003:PST


DiRaimondo:2005:NAD


DiRaimondo:2006:PST


Devanbu:2004:FAX


Devanbu:2003:ADP

Premkumar Devanbu, Michael Gertz, Charles Martel, and Stuart G. Stubblebine.

**Dwork:2003:MBF**


**Dorrendorf:2007:CRN**


**Dorrendorf:2007:CRNb**


**Dorrendorf:2007:CRNa**


**Dhem:2003:EMR**

Jean-François Dhem. Efficient

**Dhem:2003:EMR**


Deng:2006:OOC

Yan-Xiang Deng, Chao-Jang Hwang, and Jiang-Lung Liu. An object-oriented cryp-
tosystem based on two-level reconfigurable computing ar-

Daza:2007:CTM

Vanesa Daza, Javier Herranz, Paz Morillo, and Carla Ráfols. Cryptographic tech-
niques for mobile ad-hoc networks. Computer Networks (Amsterdam, Nether-

Dodis:2000:CSG


DiCrescenzo:2001:SOS


DiCrescenzo:2003:SOS

Giovanni Di Crescenzo.

Damgaard:2005:CRM


Dierickx:2000:EGD


Dif01


Dimitriadis:2007:IMC


Dimitrov:2008:DBN

Vassil Dimitrov, Laurent Imbert, and Pradeep K.
REFERENCES


Ding:2001:OTB


Ding:2005:ECB


Dedic:2005:ULB


Dang:2002:EPT

Zhe Dang, Oscar H. Ibarra, and Zhi-Wei Sun. On the emptiness problem for two-way NFA with one reversal-bounded counter. Lec-


Delaune:2006:DPS


Donsez:2001:TMA


Damgaard:2001:PTR
REFERENCES


[DKK07] Neil Daswani, Christoph Kern, and Anita Kesa-


REFERENCES

[Dittmann:2005:CMS]

[Dodis:2002:KIP]

[Diffie:1998:PLP]

[Diffie:2007:PLP]

[Die:1998:PLP]

[deLeeuw:2000:CSD]

[Diffie:2007:HIS]
Karl de Leeuw and J. A. Bergstra, editors. *The history of information security:*


DeSantis:2007:NRN

Drimer:2007:KYE

Dumais:2000:PCQ

Dowd:2007:ASS

Denev:2009:SFQ

Ding:2007:ESD
REFERENCES


REFERENCES

issn=0302-9743&volume=3621.


DODis:2004:IPC


DeMatteis:2002:PP


Dandalis:2004:ACE


Dziembowski:2007:IRS

[DP07] S. Dziembowski and K. Pietrzak. Intrusion-resilient secret shar-
REFERENCES

Dziembowski:2008:LRC


Dandalis:2001:CSP


Damgaard:2005:QCN


Delbourg:2002:JBC


Daemen:2001:BCP

REFERENCES


**Crescenzo:2004:CRR**


**Daemen:2000:NPN**


**Daemen:2000:RA**


**DDJ:2000:DDE**


**Daemen:2001:AAR**


Dra:2000:NPA


Dre:2000:PUC


Dri:2002:BER


Dob:2005:AES


Devanbu:2000:CVT

Dods:2002:NUO

Dodis:2005:RNM

Dodis:2005:ESE

DS00

DS02

DS03

DS05a

DS05b
REFERENCES


Ding:2006:SSS


Dinur:2008:CAT


Dodis:2001:PAS


Djurovic:2001:DWF


Ding:2003:SIB

REFERENCES


Drutarovsky:2008:CSC

M. Drutarovsky and M. Var- 
chola. Cryptographic sys-

tem on a chip based on Ac-
tel ARM7 soft-core with em-
bedded true random num-
DDECS 2008, 11th IEEE 
Workshop on Design and Di-
agnostics of Electronic Cir-
cuits and Systems, pages 1-
6. IEEE Computer Society 
Press, 1109 Spring Street, 
Suite 300, Silver Spring, MD 
20910, USA, 2008. URL 

org/stamp/stamp.jsp?tp=
&arnumber=4538778.

Levy-dit-Vehel:2006:WC

Françoise Levy dit Ve-
hel and Ludovic Perret. 
On the Wagner–Magyarik 
cryptosystem. In Ytre-
hus [Ytr06], pages 316–329. 
ISBN 3-540-35481-6. LCCN 

Du:2001:OKS

Wei Zhang Du and Xin Mei 
Wang. One kind of secret-
code encryption scheme 
based on maximum rank dis-
tance codes. Chinese Jour-
nal of Computers = Chi suan

chi hsheh pao, 24(6):650– 
653, 2001. CODEN JIX-
UDT. ISSN 0254-4164.

Benne de Weger. Crypt-
analysis of RSA with small 
prime difference. Applica-
able algebra in engineering, 
communication and comput-
ing, 13(1):17–28, 2002. CO-
DEN AAECWE. ISSN 
0938-1279 (print), 1432-0622 
(electronic).

Cunsheng Ding and Xuesong 
Wang. A coding theory 
construction of new system-
atic authentication codes. 
Theoretical Computer Sci-
ence, 330(1):81–99, January 
31, 2005. CODEN TC-
SCDI. ISSN 0304-3975 
(print), 1879-2294 (electronic).

Yevgeniy Dodis and Daniel 
Wichs. Non-malleable ex-
tractors and symmetric key 
cryptography from weak se-
crets. In ACM [ACM09], 
pages 601–610. ISBN 1-
60558-613-7. LCCN QA75.5 
A22 2009.

Himanshu Dwivedi. Im-
plementing SSH: strategies
REFERENCES


Desmedt:2005:CNS


Dittmann:2001:UCW


Dworkin:2003:DRB


Ding:2005:NME

[yong ding, kwok woong, and yu min wang. a w-nnaf method for the efficient computation of scalar multiplication in elliptic curve cryptography. applied mathematics and computation, 167(1):81–93, august 5, 2005. coden amhcbq. isbn 0096-3003 (print), 1873-5649 (electronic).]
REFERENCES

Dawu:2001:TES


Deng:2009:SCA


Ding:2009:MPK


Dai:2001:CDE


Eagleton:2005:BRD


ElAbbadi:2000:VPI


Eghlidos:2001:IRL

[EBS01] Taranee Eghlidos, Albrecht Beutelspacher, and Babak Sadeghiyan. Improving

**Eilam:2005:RSR**


**English:2007:MAC**


**ECMA:2000:EPIa**


**ECMA:2000:EPIb**


**Ellison:2003:PKS**


**Echizen:2005:PAV**

Isao Echizen, Yasuhiro Fujii, Takaaki Yamada,


Joachim J. Eggers, Wolf-


**Everitt:2003:JBI**


**English:2000:MNDb**


**England:2002:AOO**


**Elbirt:2005:ILD**


**Eisenbarth:2007:SLC**


**Erickson:2001:EDD**


**Erickson:2002:EDD**

REFERENCES

URL http://www.ddj.com/

[Ericsson:2003:HAE]

[Ericsson:2008:HAE]

[Ellison:2000:TRP]

[Ellison:2000:IRRa]


[Encck:2005:EOF]

[Ettinger:2002:QQC]
Mark Ettinger. 20 questions, quantum computers, and
REFERENCES


Ebringer:2000:PAP


Edman:2009:AES


Elbirt:2000:FIP


Faliszewski:2007:BRB


Fan:2003:ILC


Ferguson:2000:SEK | N. Ferguson. Semi-equivalent keys in MARS. In ????, editor, Third AES Candidate Conference, page ??, ????.
REFERENCES

Ferguson:2006:ACE

Fischlin:2000:ENM

Filiol:2001:NUS

Flannery:2001:CYW

Fridrich:2001:DLS

Frenkiel:2002:CCS
REFERENCES


[FGM03] Riccardo Focardi, Roberto Gorrieri, and Fabio Martinelli. A comparison of three authentication properties. [Fil00]


[Fil00] Eric Filiol. Decimation


[FIP01a] FIPS. *Advanced Encryption Standard (AES)*. National Institute for Standards and
REFERENCES


REFERENCES

[Fischlin:2001:CLP]

[Fischlin:2001:ICN]

[Fischlin:2005:CEN]

[Faugere:2003:ACH]

[Feng:2004:PEX]
Ferguson:2001:ICRa

Ferguson:2000:TRR

Fluhrer:2001:AES
REFERENCES


REFERENCES


REFERENCES

[102x681] REFERENCES

289


Faugere:2009:EAD


Faugere:2009:EAD
Fernandes:2002:SAL


Fournet:2008:CSI


Frankel:2001:FCI


Franklin:2004:ACC


Fremberg:2003:MAP

Daniel Fremberg. The

Friberg:2001:UCH


Friberg:2001:UCH

Ferguson:2000:CEI


Fouque:2001:FDT


Friedlander:2001:DDH

REFERENCES


Furukawa:2001:ESP


Fischer:2002:NFC


Ferguson:2003:CEI


Ferguson:2003:PC


Fundulaki:2004:SYD


Fortnow:2008:1IC

REFERENCES


REFERENCES


[FW05] Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger. Pseudo-
signatures, broadcast, and multi-party computation from correlated randomness. [FZH05]
In Franklin [Fra04], pages 562–??. CODEN LNCSD9.

Fan:2004:PPI


Furnell:2006:RPS


Fu:2005:DHP


Gross-Amblard:2003:QPW


Gang:2005:CN1


Galbraith:2001:SCC


REFERENCES

computer.org/dl/mags/sp/2003/06/j6020.pdf.


[Gas01] William Gasarch. Book review: The Codebreak-


REFERENCES


Gaj:2000:CHP


Goubin:2000:CTC


Gaj:2001:FIF


**Goodman:2001:EER**

[GC01b]


**Guerrero:2005:ECB**

[GC05]


**Gordon:2008:CFS**


**Gligor:2002:FEA**


**Gennaro:2005:SMS**

Gebotys:2004:DSC

Gengler:2000:UPC

Gennaro:2000:IPR

Gentry:2003:CBE

Gentry:2004:HCR
Craig Gentry. How to compress Rabin ciphertexts and signatures (and more). In Franklin [Fra04], pages 179–?? CODEN LNCSDD.
REFERENCES

ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN [GG01]

Gennaro:2006:RC

Gentry:2009:FHEa

Gentry:2009:FHEb

Giuliani:2001:GLI

Goldstone:2005:FCR

Golomb:2005:SDG
Solomon W. (Solomon Wolf) Golomb and Guang Gong. Signal design for good correlation for wireless commu-
REFERENCES

Gambino:2008:ITW

Goldwasser:2008:CAP

Gennaro:2003:LBE

Gennaro:2005:BEG

Grothoff:2009:TBS

Gilbert:2002:SCL
REFERENCES


[GIKR02] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. On 2-round secure multiparty computation. In Yung [Yun02a],
305

REFERENCES


REFERENCES

Gennaro:2003:SAP


Gallagher:2006:HSB


Gentry:2001:CNS


Gomulkiewicz:2002:HWA


Goldsmith:2004:CAI


Goldwasser:2005:PPK

Shafi Goldwasser and Dmitriy Kharchenko. Proof of plain-
text knowledge for the Ajtai–Dwork cryptosystem. In Kilian [Kil05], pages 529–?


References


American Mathematical Society, Providence, RI, USA, 2005. ISBN 0-8218-3365-
0. LCCN QA76.9.A25 PS2 2005. URL http://

[GLG+02] Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen,
Peter Bellows, Jaroslav Fiandr, Tom Lehman, and
Brian Schott. Comparative analysis of the hardware im-
plementations of hash functions SHA-1 and SHA-512.
Lecture Notes in Computer Science, 2433:75–??, 2002.
CODEN LNCSND. ISSN 0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/ link/service/series/0558/|
bibs/2433/24330075.htm; |
http://link.springer-
ny.com/link/service/series/|
0558/papers/2433/24330075.pdf.

[GL06a] Rosario Gennaro and Yehuda
Lindell. A framework for
password-based authenti-
cated key exchange. ACM
Transactions on Information and System Security,
CODEN ATISBQ. ISSN
1094-9224 (print), 1557-7406
(electronic).

[GL06b] Justin Goshi and Richard E.
Ladner. Algorithms for dy-
namic multicast key distri-
bution. ACM Journal of Ex-
perimental Algorithmics, 11:
1:4:1–1:4:??, ???. 2006. CO-
DEN ????? ISSN 1084-6654.

[GLC04] Blaise Gassend, Daihyun
Lim, Dwaine Clarke, Marten
van Dijk, and Srinivas De-
vadas. Identification and
authentication of integrated
circuits. Concurrency and
Computation: Practice and
Experience, 16(11):1077–1098,
September 2004. CO-
DEN CCPEBO. ISSN
1532-0626 (print), 1532-0634
(electronic).

[GM00a] Henri Gilbert and Marine

Gallant:2001:FPM

Robert P. Gallant, Robert J.
Lambert, and Scott A. Van-
stone. Faster point multipli-
cation on elliptic curves with
efficient endomorphisms. In
Kilian [Kil01a], pages 190–??
ISBN 3-540-42456-3 (paper-
back). LCCN QA76.9.A25
C79 2001; QA267.A1 L43
no.2139. UK £47.00. URL
http://link.springer-ny.com/ link/service/series/|
0558/bibs/2139/21390190.htm; |
http://link.springer-
ny.com/link/service/series/|
0558/papers/2139/21390190.pdf.

Gilbert:2000:CAR


REFERENCES

Galbraith:2003:IAU


Gorrieri:2004:SFR


Giuliano:2000:ISC


Galbraith:2002:PKS


Goots:2001:FEA


Golle:2008:DCS

REFERENCES

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

Galbraith:2001:CNR


Galbraith:2001:RBU


Gentry:2005:PAK


Galindo:2008:ICB


Gopalakrishnan:2001:PWV


Grosek:2001:SPK

REFERENCES

Ge:2005:CCO


Gore:2001:CMT


Gratzer:2006:CLE


Gutmann:2005:WHC


Gaj:2003:FME


Goldreich:1999:MCP

REFERENCES

Goldreich:2001:FCBb


Goldreich:2001:FCBa


Golic:2001:CAS

REFERENCES

Goldreich:2004:FCV


Goldstein:2008:BHO


Gonda:2006:NMR


Good:2000:TAE


Gordon:2002:TCP


Gurgens:2002:APF


//link.springer.de/link/service/series/0558/papers/2437/24370227.pdf.

Gorman:2005:NSC


Gordon:2006:UA


Goulding:2009:ESA


Gupta:2008:FAT


Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT


Guneysu:2008:SPH

Tim Güneysu, Christof Paar, and Jan Pelzl. Special-purpose hardware for solving the elliptic curve discrete logarithm problem. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 1(2):8:1–
Gutterman:2006:ALR


Granger:2005:HSN


Granger:2006:SCA


Gentry:2008:THL


Geng:2008:DSA


Galbraith:2004:EDD


Grasser:1998:FC


Gra:2001:CCW

Jon Graff. Cryptography and e-commerce: a Wiley tech

[Granboulan:2002:FDC]

[Granboulan:2002:SSR]

[Grigg:2001:FCL]

[Grossschadl:2001:HSR]

[Grossschadl:2003:ASL]
REFERENCES

Groth:2005:CS


Gisin:2002:QC


GonzalezVasco:2001:CPK


Gentry:2002:HIB


Gentry:2006:EES

[GRW06] Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. Lecture Notes in Computer Sci-
REFERENCES


REFERENCES

Guida:2004:DUP


Garfinkel:2003:PUI


Gaubatz:2008:SCD


Goodrich:2004:ETB


Giles:2002:ADW


Goodrich:2008:NFI


Guttman:2004:FAP


Guar:2005:PPL


Gumz:2004:BRH


Guillou:2001:CAP


Gutmann:2000:OSC


Gutmann:2002:CFP


Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford. Path-quality monitor-
REFERENCES


Heys:2000:SAC

Haddad:2000:AUA


Harvey:2000:EMA


Hare:2000:RUPb


Harrington:2005:NSP


Harris:2005:GHE


Hare:2001:RUPb


Hars:2006:MIA

Harman:2007:PDS


Hars:2007:DIH


Hasan:2000:L


Hasan:2001:ECM


Hasan:2001:PAA


Hassler:2002:JCP


Haufler:2003:CVH

REFERENCES


[Hayat:2004:CSE] Khawaja Amer Hayat, Umar Waqar Anis, and S. Tauseef ur Rehman. Cryptanalysis of some encryption/cipher schemes using related key attack. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36 (4):85–87, December 2004. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). 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.


Henderson:2002:MTS


Halevi:2002:SSE


Han:2009:ICS


He:2002:WSM


Heijl:2001:DXS


Heikkila:2007:ESC

REFERENCES

July/August 2007. CODEN ???. ISSN 1540-7993 (print), 1558-4046 (electronic).

Hendry:2001:SCS


Henderson:2006:CBG


Henry:2006:TFA


Herzb erg:2002:BX


Herranz:2006:DIB


Herranz:2007:IBR


Heron:2009:AES

REFERENCES


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2003:HNP


REFERENCES

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


[Hankerson:2001:SIE] Darrel Hankerson, Julio López

Hamann:2001:SBA


Han:2007:FIE


Higgins:2008:NSC


Hilley:2006:SSD


Hacigumus:2002:ESE

Hakan Hacigümüş, Bala Iyer, Chen Li, and Sharad Mehrotra. Executing SQL over encrypted data in the database-service-provider model. In Franklin et al. [FMA02],
REFERENCES


Heuberger:2005:AGE


Hofmeister:2000:COS


Hiltgen:2006:SIB


Horwitz:2002:THI


Hanschuh:2001:ASE


Hiltgen:2006:SIB


Horwitz:2002:THI


Michael Howard and Steve Lipner. *The security develop-


REFERENCES

**Hwang:2003:TRB**


**Hwang:2004:KAS**


**Hwang:2005:GTS**


**Hong:2003:BBP**


**Herzog:2003:PAK**


**Hwang:2001:TSP**

REFERENCES

Hopper:2002:PSS

Hu:2009:TRN

Hamdy:2000:SCB

Hartel:2001:FSJ

Hirt:2001:RFU


REFERENCES

Hankerson:2004:GEC

Huang:2007:MPK

Haastad:2004:SAR

Harnik:2006:CNI

Haitner:2009:SHC

Hanaoka:2002:HNI
REFERENCES


Hoepman:2001:SKA


Hofinger:2001:LBE


Honary:2001:CCI


Hook:2005:BCP


Hoskins:2006:SO

REFERENCES


[He:2001:SAR] Yeping He and Sihan Qing. Square attack on reduced


Hawkes:2004:RVC


Hsiao:2004:FCP


Holenstein:2005:OWS


Halevi:2006:TCT


[Haitner:2007:SHC]

[Harn:2009:DDB]

[Hromkovic:2009:AAH]

[Haneberg:2002:MSS]

[Hemaspaandra:2008:EDA]

[Hromkovic:2005:DAR]
REFERENCES

Hirt:2000:ERF


Hinsley:2001:CIS


Halevy:2002:LBE


Han:2002:HEF


Hwang:2007:PEA

REFERENCES

He:2005:MCP

Hong:2001:KIA

Halderman:2008:LWRa

Halderman:2008:LWRb

Halderman:2009:LWR
J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Applebaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. Communications of the Associa-
REFERENCES


Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim, and Jongsu Kim. Prov-
Hong:2002:IDC


Hess:2001:TTH


Hernandez:2004:STN


Hsu:2005:CIT

Chien-Lung Hsu. Cryptanalysis and improvement of the


[Huang:2006:CSV] Biao-Bing Huang and Shao-

**Hongfeng:2008:ECP**


**Hamalainen:2002:GPS**


**Hines:2007:AIF**


**Hofheinz:2005:CTN**


**Hughes:2002:LAA**

REFERENCES

Hughes:2004:ISE


Huhnlein:2000:EIC


Hunt:2005:JFE


Husemann:2001:SSC


Husemoller:2004:EC


Huth:2001:SCS


Hodjat:2004:HTP

[HV04] Alireza Hodjat and Ingrid Verbauwhede. High-
REFERENCES


REFERENCES


(print), 1557-9654 (electronic).

**Hardy:2009:AAC**


**Hsu:2002:IGT**


**Harkins:2005:ESU**


**Hsu:2003:IMA**


Huang:2005:EMP


IEEE:2000:ASF


IEEE:2000:IPH


IBM-MARS-Team:2000:MAS


IEEE:2001:ISF


IEEE, editor. *Proceedings: 46th Annual IEEE Symposium on Founda-


REFERENCES


IEEE:2009:PAI


IEEE09b

Itoi:2001:SIS


[IFH01]

ifrah:2000:UHN


Iglesias:2002:NSB


Bassham:2000:ET

Lawrence E. Bassham III. Efficiency testing of ANSI C implementations of round 2 candidate algorithms for the
Advanced Encryption Standard. In NIST [NIS00], pages 136–148. ISBN ????


REFERENCES

**Impagliazzo:2003:LRA**


**Impagliazzo:2006:LRA**


**Ichikawa:2000:HEA**


**Ishai:2003:EOT**


**Ishai:2005:SCC**

Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Sufficient conditions


Izmerly:2006:CCA

Izotov:2001:COC

Imrey:2003:BRC

Inamori:2002:SPB

Inamori:2002:SPT
Inoue:2005:EST


Intel:2000:IIP


Intel:2003:IRN


Itkis:2001:FSS


ITkis:2002:SSB


Irwin:2003:BRBb


ISO:2004:IIB

ISO. ISO/IEC 10118-3:2004: Information tech-

ISO:2005:IDM


Iqbal:2008:CDV


Inoue:2008:FAC


Ishai:2003:PCS


Itoi:2000:SCI


[IYK03] Tetsu Iwata, Tomonobu


Janczewski:2000:IIS


Janeczko:2006:TSH


Jankowski:2008:BRBb


Jankvist:2008:TMH

REFERENCES

Jennewein:2000:FCQ [Jef08]

Jones:2005:RDF [JBR05]

Johnson:2001:IHS [JG01]

Jeffrey:2008:PAM

Jennings:2009:SLL [Jen09]

Jaeger:2004:CAA [JEZ04]

Juels:2001:RKG
Ari Juels and Jorge Guajardo. RSA key generation
REFERENCES


[JJ00d] Éliane Jaulmes and Fredrik Jönsson. Fast correlation attacks through reconstruction of linear polynomials. In Bellare [Bel00], pages 300–??. ISBN 3-540-67907-3. ISSN 0302-9743
Jaulmes:2001:CPN


Jonsson:2002:FCA


Jakimoski:2001:ASR


Jakimoski:2001:CCB


Jakimoski:2002:CS


Jonsson:2002:SRE

Jonsson:2002:SRT


Jung:2001:EMO


Jallad:2002:ICC


Jang:2001:BWA

REFERENCES


Jarecki:2000:AST

Joux:2003:IGN

Juang:2004:FBT

Jeong:2008:PKE

Juang:2001:FBT
W.-S. Juang, C.-L. Lei, and H.-T. Liaw. Fair

Juang:2002:VMA


Johansson:2003:PCI


Jakobsson:2007:DPD

REFERENCES


[Joh05] Thomas K. Johnson. An


REFERENCES


Marc Joye:2003:GFA

Joye:2004:CHE

Joye:2001:PMA


REFERENCES


[JT05] S. P. Joglekar and S. R. Tate. ProtoMon: Embedded monitors for cryptographic protocol intrusion detection and...


[JW05] Ari Juels and Stephen A. Weis. Authenticating pervasive devices with human pro-


REFERENCES


REFERENCES

Kaliski:2001:RDS

Kaliski:2003:TRK

Kayem:2008:RCK

Kanda:2001:PSE

Kapera:2005:MRP

Karski:2001:SSS

Katzenbeisser:2001:RAR
REFERENCES


**Katos:2005:RTB**


**Katz:2005:CBR**


**Kendall:1939:TRS**


**Kovacich:2000:HTC**


**Kiely:2006:SSM**


**Kamvar:2007:DTM**


**Kim:2009:DCA**

[KB09] Jongtack Kim and Saewoong Bahk. Design of certification authority using secret


REFERENCES

RED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Kieu:2009:HSI


Kieu:2009:IAB


Ku:2005:WYR


Kim:2007:SBE


Ku:2003:WLL


Ku:2001:SAC

REFERENCES


Kang:2001:NHO

[177x646]


Kalker:2004:DWS

[177x646]


Kurosawa:2004:NPH

[177x646]


King:2001:SAD

[177x646]


Keefe:2005:CDS

[177x646]

Patrick Radden Keefe. Chatter: dispatches from the secret world of global eaves-
REFERENCES


Kellar:2005:NRR


Kenyon:2002:HPD


Kenyon:2002:DNR


Kettani:2006:CBN
REFERENCES


REFERENCES

Kato:2008:QSC

Khaw:2005:EDA

Komninos:2001:ESC

Kwon:2005:CLK

Koo:2009:SVN

Kirovski:2004:DWF
REFERENCES


Kausar:2008:SEK


Kobara:2001:NCP


Kurosawa:2003:TTK


Kidwell:2000:SNC

Peggy A. Kidwell. The Swiss Nema cipher machine
REFERENCES


**Kid02**

**Kil01**

**Kim01**

**Kilt01**
Kim:2001:CMF


King:2002:RG1

REFERENCES

Kirkby:2001:CCW

Kirtland:2001:INC

Montgomery:2003:FEC

Kocarev:2001:LMB

Kanade:2005:AVB
REFERENCES

Kawachi:2006:PQC

Kashefi:2007:SZK

Klein:2003:FOW

Karri:2003:PBC

Kim:2005:IYA

Kim:2002:NIS

Karri:2003:PBC

Kawachi:2006:PQC

Kashefi:2007:SZK

Klein:2003:FOW

Karri:2003:PBC

Kawachi:2006:PQC

Kashefi:2007:SZK

Klein:2003:FOW
REFERENCES


Kwon:2003:EEC


Khachatrian:2001:FMI


Klono\l{w}ski:2009:SGS


Kawachi:2005:UTQ


Kojima:2001:UTQ


**Kim:2009:SVN**

**Kaliski:2002:CHE**

**Kelsey:2000:ABA**

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


Kelsey:2001:ABA


Katz:2005:HEP


Katz:2008:IMC


Kim:2002:IDS

Knill:2002:FPE

Knill:2002:QIP

Ko:2000:NPK

Klein:2007:BDC

Kong:2001:AVW


REFERENCES

NIST [NIS00], page 9.
ISBN ???? LCCN ????

[Kim:2001:NPK]

[Knudsen:2001:CPL]

[Kanda:2002:SCA]


Kakarountas:2006:HSF


Katz:2001:CCA


Klarlund:2001:MIS


Klimov:2002:ANC


Keliher:2001:IUB

Liam Keliher, Henk Meijer, and Stafford Tavares. Improving the upper bound on
the maximum average linear
hull probability for Rijndael.

Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/2259/22590112.htm;
http://link.springer-
ny.com/link/service/series/0558/
papers/2259/22590112.pdf.

Kim:2003:RCC

Seungjoo Kim, Masahiro
Mambo, and Yuliang Zheng.
Rethinking chosen-ciphertext
security under Kerckhoff's
assumption. In Joye
[Joy03b], pages 227–243.
CODEN LNCSD9. ISBN 3-
540-00847-0. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C822 2003. URL http://
link.springer-ny.com/
link/service/series/0558/
tocs/t2259.htm; http://
link.springer-ny.com/
link/service/series/0558/
papers/2259/22590112.pdf.

Kol:2008:GEI

Gillat Kol and Moni Naor.
Games for exchanging infor-
mation. In ACM [ACM08],
pages 423–432. ISBN 1-
60558-047-3. LCCN QA76.6

Koc:2001:CHEb

Çetin K. Koç, David Nacc-
cache, and Christof Paar,
editors. Cryptographic hard-
ware and embedded systems
— CHES 2001: Third Inter-
national Workshop, Paris,
France, May 14–16, 2001:
Proceedings, volume 2162
of Lecture Notes in Com-
puter Science and Lecture
Notes in Artificial Intelli-
telligence. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2001. CODEN
LNCSD9. ISBN 3-
540-42521-7. ISSN 0302-9743
REFERENCES

[412]

Krukow:2005:FCR


Knutson:2007:BPS


Kushilevitz:2000:OWT

Eyal Kushilevitz and Rafail Ostrovsky. One-way trapdoor permutations are sufficient for non-trivial single-server private information retrieval. Lecture Notes in Computer Science, 1807:104–??, 2000. CODEN LCNSDR. ISSN 0302-9743 (print), 1611-3349.

Knutson:2000:TT


Knutson:2000:TTR


Knutson:2002:ACE


[KO03]


[K004]


[Koblitz:2000:TQC]


[Kocher:2002:IS]


[Koga:2002:GFR]
REFERENCES

Kurosawa:2001:ICP


Kornblum:2009:IBD


Koshiba:2001:NAS


Koshiba:2001:SRS


Koskinen:2001:NIK


Kovach:2001:BCB

[Kov01] Karen Kovach. *Breaking codes, breaking barriers: the WACs of the Signal Secu-
Kovacic:2003:ISS


Katz:2009:ESA


Katzenbeisser:2000:IHT


Koc:2001:CHEa

REFERENCES


Koc:2003:GEI


Kerins:2002:FPE


Klima:2003:ARB

[KPR03] Vlastimil Klíma, Ondřej Pokorný, and Tomáš Rosa.


Kaufman:2002:NSP


Kim:2004:TBG

**REFERENCES**

**Krishna:2003:BUP**


**Krawczyk:2001:OEA**


**Krawczyk:2003:SSM**


**Krause:2002:BBC**


**Krause:2002:USP**


**Krawczyk:2005:HHP**

[Kra05] Hugo Krawczyk. HMQV: a high-performance secure
REFERENCES

Diffie–Hellman protocol. In
Shoup [Sho05a], pages 546–
?? ISBN 3-540-28114-
2. ISSN 0302-9743 (print),
1611-3349 (electronic). LCCN
QA76.9.A25 C79 2005; QA76.9
.A25; QA76.9 C79 2005;
QA76.9 C794 2005; QA76.9;
Internet. URL http://
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

[Kra07]
Simon Kramer. Logical
concepts in cryptography.
ACM SIGACT News, 38
CODEN SIGNDM. ISSN
0163-5700 (print), 1943-5827
(electronic). URL http://
//doi.acm.org/10.1145/
1345189.1345205.

[Kre05]
Gunnar Kreitz. Optimization
of broadcast encryption
schemes. Examensarbete,
Numerisk analys och
datalogi, Kungliga Tekniska
högskolan, Stockholm, Swe-

[KRS+02]
François Koeune, Gael
Rouvroy, François-Xavier
Standaert, Jean-Jacques
Quisquater, Jean-Pierre David,
and Jean-Didier Legat. An
FPGA implementation of
the linear cryptanalysis.
Lecture Notes in Computer

[Kat:2000:CCA]
Jonathan Katz and Bruce
Schneier. A chosen ci-

[Keh:2001:ISM]
Roger Kehr, Michael Rohs,
and Harald Vogt. Issues
in smartcard middleware.
Lecture Notes in Computer
CODEN LNCSN9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
//link.springer-ny.com/
link/service/series/0558/
bibs/2041/20410090.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2041/20410090.

[Kim:2005:CLL]
Kee-Won Kim, Eun-Kyung
Ryu, and Kee-Young Yoo.
Cryptanalysis of Lee–Lee au-
thenticated key agreement
scheme. Applied Mathemat-
ics and Computation, 163
CODEN AMHCBQ. ISSN
0096-3003 (print), 1873-5649
(electronic).
REFERENCES


Kelsey:2000:MAP


Kuramitsu:2002:ETC


Krause:2003:DOC


Kozaczuk:2004:EHP


Katz:2005:MIA

Jonathan Katz and Ji Sun Shin. Modeling insider at-

Kiltz:2005:TCL


Kissner:2005:PPS


Klivans:2006:CHL


Kurkowski:2006:QFF


Kasper:2009:FTA


Klivans:2009:CHL

REFERENCES

Kelsey:2000:YND


Kang:2001:PSK

Ju-Sung Kang, Sang-Uk

**[Kumar:2002:APS]**


**[KSZ02]**


**[Kogan:2006:PRS]**


**[Kuribayashi:2000:WSB]**

Minoru Kuribayashi and Hatsukazu Tanaka. A watermarking scheme based on the characteristic of addition among DCT coefficients.
Kuribayashi:2001:NAF

Kogan:2006:IER

Kobayashi:2007:AIG

Ku:2002:IIB
REFERENCES

Ku:2004:HBS

[102x681] REFERENCES
[0x0]424

Kuhn:2000:PCL


Kuhn:2001:CRR


Kuhn:2002:OTD


Kuhn:2002:ICM


Kuhn:2008:BSS


Kukorelly:2001:P

Kundur:2001:WDI


Kurosawa:2001:MRP


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


[KY01a] Jonathan Katz and Moti Yung. Unforgeable encryp-


Katz:2002:TCB


Katz:2003:SPA


Kiayias:2002:CHB


Kim:2002:PAA


Kang:2001:PMT

[KYHC01] Ju-Sung Kang, Okyeon Yi,
REFERENCES


[Lam01] Kwok Yan Lam. Cryptography and computational number theory, volume 20 of Progress in computer science


Landau:2000:TOD


Landau:2000:ITS


Landau:2004:PNS

REFERENCES

Landau:2004:SLE

Landau:2008:CSC

Laughlin:2008:CR

Lavington:2006:FCD

Lavoûe:2009:LRM
Lawton:2005:MAH


Lawson:2009:SCA


Lawson:2009:TAG


Li:2004:QAU


Lindskog:2005:DIT


Lee:2000:UBN


Leveiller:2001:CNF

Leveiller:2002:CNF

Sabine Leveiller, Joseph Boutros, Philippe Guillot, and Gilles Zémor. Cryptanalysis of nonlinear filter generators with \( \{0,1\} \)-metric Viterbi decoding. Lecture Notes in Computer Science, 2288:50–??, 2002.


Lin:2004:SOT


Lu:2005:ER

Rongxing Lu and Zhenfu Cao. Efficient remote user authentication scheme using...

Lu:2005:NDA


Long:2005:DTC


Lu:2007:NPL


Lee:2001:SEK


Lee:2003:APS


Levi:2004:UNC

[LC04] Albert Levi, M. Ufuk Caglayan, and Cetin K. Koc. Use of nested certifi-

**Lee:2004:DEB**


**Lim:2009:OPG**


**Li:2008:CAM**


**Lu:2005:TUS**


**Lu:2005:PBM**


**Lu:2005:RTP**


**Li:2001:CCB**

Zi Chen Li and Yi Qi Dai. Cryptanalysis of cryptosystems based on the quadratic

**Lai:2004:SGS**


**Lavoue:2007:SSW**


**Law:2006:SBB**


**Lindquist:2004:JCS**


**Lee:2001:AES**


**Lee:2003:BRBa**


**Lee:2003:BRBBb**

REFERENCES

0163-5700 (print), 1943-5827 (electronic). See [Gol99].


REFERENCES


REFERENCES

[102x681] //link.springer-ny.com/
link/service/series/0558/1
bibs/2229/22290408.htm;
http://link.springer-
y.com/link/service/series/1
0558/papers/2229/22290408.
pdf.

[LHH05] Narn-Yih Lee and Pei-Hsiu
Ho. Convertible undeniable
signature with subliminal
channels. Applied Mathemat-
ics and Computation, 158(1):
CODEN AMHCBQ. ISSN
0096-3003 (print), 1873-5649
(electronic).

[LH04] Lee:2004:CUS

[177x574] [LH07] Robert Lyda and James
Hamrock. Using entropy
analysis to find encrypted
and packed malware. IEEE
Security & Privacy, 5(2):
CODEN ???? ISSN
1540-7993 (print), 1558-4046
(electronic).

[LH07] Lyda:2007:UEA

[311x473] [LHL03a] Chua-Ta Li, Min-Shiang
Hwang, and Yen-Ping Chu.
Improving the security of
a secure anonymous rout-
ing protocol with authenti-
cated key exchange for ad
hoc networks. International
Journal of Computer Sys-
tems Science and Engineer-
ing, 23(3):??, May 2008.
CODEN CSSEMI. ISSN 0267-
6192.

[LHL03a] Li:2008:ISS

[386x461] [LHL+02] Seonhee Lee, Seokhie Hong,
Sangjin Lee, Jongin Lim,
and Seonhee Yoon. Trun-
cated differential cryptanal-
ysis of Camellia. Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/1
bibs/2288/22880032.htm;
http://link.springer-
y.com/link/service/series/1
0558/papers/2288/22880032.
pdf.

[LHL03a] LHL+02

[423x425] [LHH05] Eric Jui-Lin Lu, Min-Shiang
Hwang, and Cheng-Jian
Huang. A new proxy sig-
nature scheme with revoca-
tion. Applied Mathemat-
ics and Computation, 161(3):
CODEN AMHCBQ. ISSN
0096-3003 (print), 1873-5649
(electronic).

[LH05] Lu:2005:NPS

[386x449] [LHC08] Cheng-Chi Lee, Min-Shiang
Hwang, and Li-Hua Li.
A new key authentication
scheme based on discrete log-
arithms. Applied Mathemat-
ics and Computation, 139(2–
CODEN AMHCBQ. ISSN
0096-3003 (print), 1873-5649
(electronic).

[LHC08] Lee:2003:NKA
REFERENCES

Lin:2003:NRU


Lee:2004:SAA


Lu:2008:PTZ


Liu:2005:DBV


Lee:2009:NCA


Lee:2002:FPU


Lee:2005:NBS

Li:2001:NSA


Lieman:2005:CRW


Lin:2000:RTI


Linn:2000:TMM


Lin:2001:DWM

Phen-Lan Lin. Digital watermarking models for resolving

**Lindell:2001:PCT**

Lindell:2003:SCC


**Lin:2007:PFT**

Lin:2002:DSK

Lingmann:2002:DSK


**Lindell:2001:PCT**

Lindell:2000a:SCC


**Lingmann:2002:DSK**

Lingmann:2002:DSK

Lingmann:2002:DSK


**Lin:2007:PFT**

Lin:2007:PFT

Lin:2007:PFT


**Lee:2005:IEC**

Lee:2005:IEC

Lee:2005:IEC


REFERENCES


REFERENCES

Lee:2005:EVB


Lee:2005:IHA


Lee:2005:ILL


Lim:2000:GTC


Luo:2004:UUR


Lu:2001:DWC


Lee:2003:ISC

[LL03] Pil Joong Lee and Chae Hoon
REFERENCES


Lee:2004:FIM


Lee:2004:DIS


Lim:2004:ISC


Lee:2005:CMA

REFERENCES


REFERENCES

Lee:2002:RUA


Li:2004:CES


Liao:2006:PAS


Lesniewski-Laas:2005:SSS


Li:2001:SPD


Lee:2002:SEC


[LLL04] Young-Ran Lee, Hyang-Sook Lee, and Ho-Kyu Lee. Multi-party authenticated key
agreement protocols from multi-linear forms. Applied Mathematics and Compu-
tation, 159(2):317–331, December 6, 2004. CODEN AMHCBQ. ISSN 0096-3003
(print), 1873-5649 (electronic).

LCCN QA75.5 .A22 2002. ACM order number 508020.

[LRR06] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the composition of authenti-
CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).


Hongjun Liu, Ping Luo, and Daoshun Wang. A distributed expansible authentication model based

[Liu:2008:SAM]


[LLW08b]


[LLW09]


[Linares:2000:SAM]


[Lorenz:2002:SSG]

REFERENCES

Lavasani:2008:IFA

Li:2003:SCE

Lepinski:2005:FZK

Lamenca-Martinez:2006:LNP

Leitold:2001:MTN
Laskari:2007:AEC


Laskari:2005:TTC


Lu:2005:CCA


Liu:2004:MBA


Levieil:2008:CTC


Liu:2008:ARL

[LNL+08] Donggang Liu, Peng Ning, An Liu, Cliff Wang, and


REFERENCES


Li:2005:MCK


Law:2009:EEL


Lemke:2006:ESC


Li:2006:PMW


LQ08


Lientz:2001:BTP


Lemke-Rust:2007:MAP


Liu:2008:GPV


Liu:2008:GPV

Lin:2000:TPE


Lin:2000:TPE

Lin:2003:SEOa


Lin:2003:SEOa

Lin:2003:SEOb


Lin:2003:SEOb

Lu:2005:BIW

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


REFERENCES

Li:2005:ISS


Lie:2000:ASC


Lin:2005:HAO


Lu:2002:HEA


Lu:2007:NSC


Lucks:2000:ASR

REFERENCES

//csrc.nist.gov/encryption/aes/round2/conf3/papers/
AES3Proceedings-1.pdf; [Luc06]

Lucas:2002:SAB

Lucas:2002:VCS

Lucas:2006:PGE

Ludvig:2005:PWF

Lukyanov:2001:PFA

Lunde:2009:BCU
Paul Lunde, editor. The book of codes: understanding the world of hidden messages: an illustrated guide to signs, symbols, ciphers, and secret languages. University of California Press,
REFERENCES


[LV07] Fabien Laguillaumie and


Xiaodong Lin, Johnny W. Wong, and Weidong Kou. Performance analysis of secure Web server based on SSL. *Lecture Notes in Computer Science*, 1975: 249–??, 2000. CODEN LNCS9. ISSN 0302-

Lv:2005:PCA


Lv:2005:SMS


Li:2005:WMT


Li:2005:FLA


Li:2005:AAU


Anna Lysyanskaya. Unique signatures and verifiable random functions from the DH-DDH separation. In Yung [Yun02a], pages 597-612. CODEN LNCS9D.

K. H. Leung and Bing Zeng. Wavelet-domain image watermarking based on statistical metrics. *Lecture Notes in Computer Sci-

Li:2004:CAB


Lao:2009:ORA


Li:2001:GOT


Li:2004:WMS


Michener:2000:IWM


Michener:2000:MSA

Masuda:2002:CDC


Maurer:2007:ICP


Mrayati:2003:AKT


Mrayati:2004:IAD


Mrayati:2005:IDB


Mrayati:2006:TTC


Mrayati:2007:TTC


Alexis Warner Machado. The Nimbus cipher: a proposal for NESSIE. Report ??, ????, ????, Septem-
ber 2000.


REFERENCES

Mahle:2004:DDI

Malcolm:2002:LAM

Maloof:2006:MLD

Manger:2001:CCA

Mann:2002:HI

Mann:2008:HHS

Mao:2001:TRC
REFERENCES


Mao:2004:MCT


Marques:2002:BSJ


Martinelli:2002:SSA


Mares:2005:BRA


Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI

Luther Martin. Crypto corner: Identity-based encryption and beyond. IEEE
REFERENCES


Martin:2008:IBE


Mastreni:2004:APA


Matsui:2002:FSE


Maurer:2001:C


Maurer:2004:RCD


Maughan:2005:HSC

REFERENCES

Maximov:2006:SWC


Mayers:2001:USQ


May:2002:CUR


May:2004:CRS


May:2009:PIS


Mel:2001:CD


Mohanty:2008:IWB

[Saraju P. Mohanty and Bharat K. Bhargava. Invisible watermarking based on creation and robust insertion-extraction of image

**[MBS04]**


**[MC04]**


**[MCHN05]**


**[McA08]**

McNichol:2003:HTM


Martin:2004:AMC


Macchetti:2005:QPH


McCaman:2008:QIF


Monteiro:2008:AVM


Meadows:2001:OIF


Meadows:2004:OSM

Catherine Meadows. Ordering from Satan’s menu: a survey of requirements specification for formal anal-
REFERENCES


Thomas Messerges. Securing the AES finalists against power analysis at-
tacks (abstract only). In NIST [NIS00], page 10. ISBN ???. LCCN ???.


Messerges:2001:SAF


McGrew:2001:AAE

[MF01] David A. McGrew and Scott R. Fluhrer. Attacks on additive encryption of redundant plaintext and implications on Internet security.


Marti-Farré:2007:NSS


Matula:2005:TLS


Mueller:2006:SMG

[MFK+06] Maik Mueller, Michael Friedrich, Klaus Kiefer, Ralf Miko, and Juergen Schneider. System and method for

Muller:2009:BPE


Minier:2001:SCC


Muresan:2008:PCA


Mukherjee:2002:CAB


Molland:2004:ICA

Håvard Molland and Tor Helleseth. An improved correlation attack against irregular clocked and filtered keystream generators. In Franklin [Fra04], pages 373–??, 2004. CODEN LNCSDD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN
REFERENCES


Ma:2005:NCD

Maas:2009:SRW

May:2002:SKS

Mihaljevic:2009:ASC

Moon:2002:IDC


[Mir05] Jelena Mirkovic, editor. Internet denial of service: attack and defense mechanisms. The Radia Perlman series in computer networking and security. Prentice-Hall PTR, Upper Saddle River, NJ 07458, USA,
REFERENCES


REFERENCES

Maltoni:2004:BAE


Moore:2001:AGK


Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS


Moyle:2005:CLD

REFERENCES


REFERENCES


Mullen:2007:FFA
Gary L. Mullen and Carl
Mummert. Finite Fields
and Applications, volume 41
of Student mathematical li-
brary. American Mathematical
Society, Providence, RI,
USA, 2007. ISBN 0-8218-
4418-0 (paperback). ix + 175
pp. LCCN QA247.3 .M85
2007.

Moreira:2002:RCE
Emmanuel A. Moreira,
Paul L. McAlpine, and Si-
mon D. Haynes. Rijn-
dael cryptographic engine
on the UltraSONIC recon-
figurable platform. Lecture
Notes in Computer Scien-
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
l ink/service/ser ies/0558/
bibs/2438/24380770.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2438/24380770.
pdf.

Milenko vic:2005:UIB
Milena Milenković, Aleksan-
dar Milenković, and Emil
Jovanov. Using instruction
block signatures to counter
code injection attacks. ACM
SIGARCH Computer Ar-
117, March 2005. CODEN
CANED2. ISSN 0163-5964
(print), 1943-5851 (elec-
tronic).

Maltoni:2003:HFR
Davide Maltoni, Dario Maio,
Anil K. Jain, and Salil
Prabhakar. Handbook of
fingerprint recognition.
Springer professional com-
puting. Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
many / London, UK / etc.,
xii + 348 pp. LCCN HV6074
H25 2003. US$59.95. In-
cludes DVD-ROM.

McEvoy:2009:IWH
Robert P. McEvoy, Colin C.
Murphy, William P. Mar-
nane, and Michael Tunstall.
Isolated WDDL: a hiding
countermeasure for differen-
tial power analysis on FP-
GAs. ACM Transactions
on Reconfigurable Technol-
ogy and Systems (TRETS),
CODEN ???: ISSN
1936-7406 (print), 1936-7414
(electronic).

Maitra:2006:PCI
Subhamoy Maitra, C. E. Ven-
Madhavan, and Ramarath-
nam Venkatesan, editors.
Progress in Cryptology —
INDOCRYPT 2005: 6th In-
ternational Conference on
Cryptology in India, Ban-

Matsumoto:2002:IAG


Mizuki:2001:NSN


Mercuri:2003:IRS


Mukhopadhyay:2014:EMP


Martel:2004:GMA

[MND+04] Charles Martel, Glen Nuckolls, Premkumar Devanbu,

Martínez-Nadal:2002:CUM


Monsignori:2001:WMS


Mironov:2008:SAE


MacAndrew:2000:LPT

Tim MacAndrew, Robert H. Norman, Jeff Templon, Kevin W. Wall, Shari Lawrence Pfleeger, Joseph C. Sligo, Christopher Jack, and Terry Ritter. Letters: Probability theory and software engineering; food

**Mykletun:2006:AIO**


**Mollin:2003:RPK**


**Mollin:2005:CGS**

Richard A. Mollin. *Codes: the guide to secrecy from...*


Orren Merton and Linda Dail-ley Paulson. News briefs:

McMillan:2001:JIA


Mihaiescu:2001:BRE


Moshopoulos:2001:NSA


Malkhi:2002:ACE

Dahlia Malkhi and Elan Pavlov. Anonymity without ’cryptography’ (extended abstract). *Lecture
Maurer:2003:SMR


Micciancio:2005:ASS


Matusiewicz:2006:FGD


Munilla:2007:HMF


Micciancio:2008:OCC


Mislove:2006:EBO

Alan Mislove, Ansley Post, Andreas Haeberlen, and Peter Druschel. Experiences in building and operating ePOST, a reliable peer-to-peer application. Operating
REFERENCES


Moralis:2009:KSA


Monrose:2000:KDB


MacKenzie:2001:TPG


Micali:2005:OEC


Micciancio:2009:LBC


Monrose:2002:TSG


Mitchell:2006:PPT


Maitra:2002:CSB

REFERENCES

Menezes:2002:PCI


Mitnick:2002:ADC


Muthukrishnan:2002:IAS


Markowitch:2003:CWV


Miklau:2003:CAP

[MS03b] Gerome Miklau and Dan Suciu. Controlling ac-


[MS09d] S. Myers and A. Shelat. Bit

Shen:2005:NIW


MacKenzie:2002:TPA


McClure:2003:HEN


Matsumoto:2007:FSC

Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. A fast stream cipher with huge state space and quasigroup filter for software. In Adams et al. [AMW07], pages 246–263. ISBN 3-540-77360-6. LCCN ????.

Miltchev:2008:DAC

REFERENCES

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

**Mouratidis:2009:PMD**

**Moran:2004:NIT**

**Myasnikov:2005:PAB**

**Muzereau:2004:EBD**

**Marsaglia:2002:SDP**

**Meseguer:2007:SRA**
José Meseguer and Prasanna Thati. Symbolic reachability analysis using narrowing


REFERENCES


REFERENCES


Matsui:2004:SAC


Nagy:2007:AQK


Naik:2003:DSW


Naccache:2001:TCC


REFERENCES

Naor:2004:TCF


NIST:2000:FPD


Nazario:2002:RYS


Nieto:2001:PKC


Nghiem:2009:FBI

REFERENCES

Ning:2004:TTO


Nedjah:2005:SHC


Nash:2001:PIM


Nedjah:2004:ECH


Nedjah:2006:NTC


Netscape:2004:HSW


This is a tutorial of how the Secure Sockets Layer (SSL) protocol works.

Neuenschwander:2004:PSM

Daniel Neuenschwander. *Probabilistic and Statistical Methods in Cryptology: An Introduction by Selected Top-


[Ngu01] Phong Q. Nguyen. The two faces of lattices in cryp-

[Ngu05] Minh-Huyen Nguyen. The relationship between password-


[NH03] Kaisa Nyberg and Howard Heys, editors. Selected ar-
eas in cryptography: 9th
annual International Work-
shop, SAC 2002, St. John’s,
Newfoundland, Canada, Aug-
st 15–16, 2002: Re-
vised Papers, volume 2595
of Lecture Notes in Com-
puter Science. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2003. CO-
DEN LNCSD9. ISBN 3-540-
00622-2. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
S22 2002. URL http://link.springer-de/
link/service/series/0558/
tocs/t2595.htm; http://www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2595. Also available via the
World Wide Web.

[Nic01] John Nicholson. You’ve been
cracked ... and now you’re
sued. :login: the USENIX
Association newsletter, 26
(2):??, April 2001. CODEN
LOGNEM. ISSN 1044-6397.
URL http://www.usenix.
org/publications/login/
2001-04/pdfs/nicholson.
pdf.

[Nie02a] Harald Niederreiter. Book
review: Cryptography and
computational number the-
ory. Mathematics of Com-
putation, 71(239):??, July
2002. CODEN MCM-

[Nie02b] Jesper Buus Nielsen. Sepa-
rating random oracle proofs
from complexity theoretic
proofs: The non-committing
encryption case. In Yung
[Yun02a], pages 111–126.
CODEN LNCSD9. ISBN
3-540-44050-X (paperback).
ISSN 0302-9743 (print),
1611-3349 (electronic). LCCN
QA76.9.A25 C79 2002. URL
http://link.springer-de/
link/service/series/0558/
bibs/2442/24420111.htm;
http://link.springer.de/
link/service/series/0558/
papers/2442/24420111.pdf

[Nie02c] Jesper Buus Nielsen. A
threshold pseudorandom

Nievergelt:2002:FLM


Nievergelt:2002:FLM


Nievergelt:2002:FLM


Niederreiter:2002:FLM


NIST:2000:TAE


NIST:2001:CT


NIST:2001:SRC


Nisley:2003:ELH


NIST:2003:RKE


Nagaj:2006:OQE


REFERENCES


REFERENCES


Nguyen:2002:AIN


Nichols:2000:DYD

Elizabeth A. Nichols and Gunnar Peterson. A metrics framework to drive application security improve-


Nakahara:2001:LCR


Naor:2004:NTC


Nichols:2007:MFD

REFERENCES


REFERENCES

Nguyen:2005:PSE


Nishioka:2002:DAF


Nahum:2007:ESS


Nyberg:2001:CTC


Nenadic:2005:RBC


Nenadic:2005:RBV


[NSN05]
[NTW07]
Olson:2003:QHK


Oechslin:2003:MFC


Oppliger:2008:STS


Oiwa:2009:IMS


Okamoto:2000:ACAA


Okamoto:2004:TCC

REFERENCES


Ohzahata:2002:FAM


Ohigashi:2009:PMF


Ohkuma:2001:BCH


[OP01b] Tatsuaki Okamoto and David Pointcheval. REACT: rapid enhanced-security asymmetric cryptosystem transform. Lecture Notes in Computer Science, 2020:
REFERENCES

159–175, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES

QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; In-
ternet. URL http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

Oren:2006:PAR
Yossi Oren and Adi Shamir.
Power analysis of RFID
tags. Technical report, Fac-
yulty of Mathematics and
Computer Science, Weiz-
mann Institute, POB 26, Re-
hovot 76100, Israel, 2006.
URL http://www.wisdom.
weizmann.ac.il/~yossio/
rfid/.

Obimbo:2007:PAD
Charlie Obimbo and Be-
hzad Salami. A parallel
algorithm for determining
the inverse of a matrix for
use in blockcipher encryp-
tion/decryption. The Jour-
nal of Supercomputing, 39
CODEN JOSUED. ISSN
0920-8542 (print), 1573-0484
(electronic). URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=0920-8542&volume=
39&issue=2&spage=113.

Oury:2008:PP
Nicolas Oury and Wouter
Swierstra. The power of Pi.
ACM SIGPLAN No-
tices, 43(9):39–50, Septem-
ber 2008. CODEN SIN-
ODQ. ISSN 0362-1340
(print), 1523-2867 (print),
1558-1160 (electronic).

Overbeck:2009:CBC
Raphael Overbeck and Nico-
las Sendrier. Code-based
cryptography. In Bernstein
et al. [BBD09], pages 95–146.
ISBN 3-540-88701-6 (hard-
cover), 3-642-10019-8 (soft-
cover). LCCN QA76.9.A25
P67 2009.

Okeya:2004:SBR
Katsuyuki Okeya, Katja
Schmidt-Samoa, Christian
Spahn, and Tsuyoshi Tak-
agi. Signed binary rep-
resentations revisited. In
Franklin [Fra04], pages 123–
37. CODEN LNCSD9.
ISBN 3-540-22668-0. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
10.1007/b99099. URL http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3152; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b99099.

Osvik:2005:CA
Dag Arne Osvik, Adi
Shamir, and Eran Tromer.
Cache attacks and coun-
termeasures: the case of
AES: (extended version).
Technical report, Depart-
ment of Computer Sci-
ence and Applied Mathe-
ematics, Weizmann Insti-
tute of Science, Rehovot 76100,
REFERENCES


[Otita01] Souichi Okada, Naoya Torii,

[Ove06]


[OTU00]


[Oue05]


[Ove06]


[OZL08]


[Pae03]

REFERENCES


**Panditaratne:2007:TRN**


**Papanikolaou:2005:BRBa**


**Park:2004:APP**


**Pass:2003:DCR**


**Pass:2005:UCN**


REFERENCES

Patarin:2004:SRF


Paulson:2001:RBS


Paulson:2002:NBPb


Paulson:2002:NBV


Paulson:2003:NBV

Paulson:2009:NBT

Praca:2001:SCS

Piva:2002:MCW

Piva:2005:SRA

Park:2000:CAP

Peng:2005:SES
Kun Peng, Colin Boyd, and Ed Dawson. Simple and efficient shuffling with provable correctness and ZK privacy. In Shoup [Sho05a], pages 188–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 2005; QA76.9 .A25; QA76.9 C79 2005; QA76.9 C794 2005; QA76.9; In-
REFERENCES


Nikolaos Petrakos, George W. Dinolt, James Bret Mich-

**Peinado:2004:CLK**


**Peikert:2009:PKC**


**Pelzl:2006:PAC**


**Pemble:2001:CEW**


**Pemble:2001:SPA**


**Perrine:2003:ECP**


**Perlman:2005:EMD**

REFERENCES

/Petullo:2003:IEH


/Petullo:2005:EYR


/Petzold:2008:ATG


/Potter:2003:S


/Pfitzmann:2001:ACE


/Phatak:2005:FMR


**Pathak:2006:BFT**


**Pietrzak:2005:CDI**


**Pinkas:2002:CTP**


**Pinkas:2003:CTP**


**Pincock:2006:CHC**


**Park:2001:NDW**

Ji Hwan Park, Sook Ee Jeong, and Young Huh. A new digital watermark-
REFERENCES


Park:2001:RFW


Poh:2001:HBP


Petitcolas:2003:DWF


Park:2001:CSC

REFERENCES


Plam:2001:PTU


Pon:2005:CZA


Pon:2005:DNP


Pon:2005:OPK
REFERENCES

Pfleeger:2007:IBC

Paulson:2000:NBU

Piper:2002:CVS

Pang:2008:AQR

Pohlmann:2001:SCA

Pointcheval:2000:CCS

Pointcheval:2002:PSP
REFERENCES

Pointcheval:2006:TCC


Poo:2003:NSP


Potter:2003:WAO


Potter:2006:CKM


Porras:2006:PEG


Porin:2001:THE

Potter:2007:CWW


Pfleeger:2003:SC


Pfleeger:2007:SC


Paar:2009:UCT


Pellikaan:1996:AGC

R. Pellikaan, M. Perret, and S. G. Vladut, editors. *Arithmetic, geometry, and cod-


[Pre02c] Bart Preneel, editor. *Topics in cryptology, CT-RSA 2002: the Cryptographers’ Track at RSA Conference*


REFERENCES

Parker:2001:RKC

Pfitzmann:2001:SEC

Pornin:2001:SHT

Padro:2002:LBI

Pomerance:2002:SOC


REFERENCES

2008. CODEN ????. ISSN 1539-9087 (print), 1558-3465 (electronic).

Pavlou:2008:FAD


Park:2002:SRL


Pareschi:2009:PAC


Petit:2008:BCB


Preneel:2006:SAC

Pang:2008:VCR

Pfeeger:2007:GEI

Pucella:2003:JRB

Pucella:2006:SCC

Pucella:2007:Ib

Puzmanova:2004:RWF

Page:2006:FAP


[PY05] Andrew S. Patrick and Moti Yung, editors. *Financial

Paterson:2006:LTT


Palanivel:2008:MPA


Pieprzyk:2001:CPS


Pieprzyk:2002:CPL


Pieprzyk:2002:CCI

Josef Pieprzyk and Xian-Mo Zhang. Constructions of cheating immune secret sharing. Lecture

Pecho:2009:APW


Peng:2009:DIE


Qian:2005:CLT


Quisquater:2005:SCR

REFERENCES


Roman:2007:SCP


Ram01


Rand:2001:MRD


Rijmen:2001:WHF


Rogaway:2003:OBC


Rijmen:2008:RSA

Vincent Rijmen, Paulo S. L. M. Barreto, and Décio L. Gazzoni Filho. Rotation symmetry in alge-

Roth:2001:EJA

Rogers:2005:NSE

Rubin:2006:CSE

Reed:2000:ANA

Rubin:2005:ARS

Rangan:2001:PCI
REFERENCES


[RdS01] Renaud:2009:VPC


[RDJ+01] Rankl:2000:SCH


[RE00] Riley:2002:CBR

REFERENCES


Regev:2003:SCH


Regev:2009:LLE


Ren:2009:CWT


Rescorla:2001:IOPa

REFERENCES

Rescorla:2001:IOPb


Rigenburg:2005:PFS


Rotondi:2006:CHA


Ren:2009:FCS


Rojas:2000:FCH


Roescoe:2002:TBC

REFERENCES


Rafaeli:2003:SKM

[Sand issues pdf]


Rafaeli:2003:SKM


Rhinelander:2003:DIE


Rhinelander:2003:DIE


Rich:2007:ATS


Rich:2007:ATS


Rila:2002:DAB


Risa:2006:SWS

Risen:2006:SWS


Rivest:2003:TLE


Renner:2005:UCP

REFERENCES


REFERENCES

Ruiz:2001:SPS

Reyhani-Masoleh:2003:LCS

Reyhani-Masoleh:2004:TFT

Rahaman:2008:CTB

Ryabko:2005:NTA
B. Y. Ryabko, V. A. Monarev, and Y. I. Shokin.

Ryutov:2000:RESa


Ryutov:2000:RESb


Robinson:2002:LLE


Robinson:2009:LLE


Rosen:2000:NRC


Rosen:2006:CZK

REFERENCES

R657 2006. URL http://www.springerlink.com/content/u1171. With Additional Background by Oded Goldreich.


[Rot05] Jörg Rothe. Complexity Theory and Cryptology: an Introduction to Cryptocomplexity. Texts in theoretical com-

Rothe:2007:BRB


Roy:2000:PCI


Roychowdhury:2000:PCJ


Roy:2005:ACA


Rieffel:2000:IQC


Rechberger:2008:NRN


Rechberger:2006:NCW


Rivest:2000:RA


Rosenbaum:2000:SFR


Romer:2001:ILA

Tanja Römer and Jean-Pierre Seifert. Information leakage attacks against

[Rubin:2002:SAV]

[Rubin:2003:TBC]

[Rao:2005:CHE]


Rivest:2003:TAL


RSA:2003:PEC


Rousseau:2009:CCP


Rousseau:2009:MT


Rukhin:2001:STS


Rogers:2005:MPH


Rouvroy:2003:EUF


Rivest:2001:HLS


Rubin:2000:KVL

REFERENCES


[RW03b] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an


REFERENCES


[Sal05a] Anthony E. Sale. The rebuilding of Colossus at Bletchley Park. IEEE An-


REFERENCES

Samtani:2009:WTO

Santini:2005:WSI

Sarkar:2002:FCM

Sasse:2007:REB

Satoh:2006:DPI

Savelli:2004:NDC

Soto:2000:RTA
Juan Soto and Lawrence E. Bassham. Randomness testing of the Advanced Encryption Standard finalist candidates. NIST internal report 6483, National Institute for Standards and Technology, Gaithersburg,
REFERENCES

Shacham:2001:ISH


Scott:2004:CP


Stoklosa:2005:CIC


Stallings:2007:CSP


Sherwood:2005:MTR


Steiner:2001:SPB


REFERENCES


Da-Zhi Sun and Zhen-Fu Cao. Improved public key authentication scheme for non-repudiation. *Applied Mathematics and Com-
REFERENCES

Siegelin:2001:SCD


Schmalz:2000:MAD


Schneier:2000:AAR


Schneier:2000:IRS


Schneier:2000:SLD


Scharinger:2001:ASK


Schindler:2001:TAA


Schmalz:2001:MDI


Schneier:2001:FSE


Schneier:2005:AE


Schneier:2005:TFA


Schramm:2006:AMS


Schroeder:2006:NTS


Schneier:2007:NCS


Schneier:2008:SS

Bruce Schneier. Schneier on Security. John Wiley and Sons, Inc., New York,
REFERENCES


Da-Zhi Sun, Zhen-Fu Cao, and Yu Sun. Remarks on a new key authentication scheme based on discrete logarithms. Applied Mathematics and Computation, 167
Seb:2001:OIW

Sebe:2000:SDI

Smith:2006:CNS

Smith:2001:ADB

Spiekermann:2009:ACR

Seacord:2005:SCC
Robert C. Seacord. Secure coding in C and C++. Addison-Wesley,
REFERENCES


Seacord:2009:CCS

Seetharaman:2004:BRB

Smith:2006:SID

Seifried:2000:C

Seifried:2000:PPA

Seifert:2005:ACR

Speed:2001:PIS
[Timothy Speed, Juanita Ellis, and Steffano Korper. The Personal Internet Security Guidebook: Keeping Hackers and Crackers out of Your
REFERENCES

*Speed:2002:PIS*  

*Sennewald:2003:ESM*  

*Selcuk:2000:BEL*  

*Semanko:2000:CAA*  

*Sutherland:2008:AVO*  

*Shumow:2007:PBD*  
REFERENCES

//rump2007.cr.yp.to/15-
shumow.pdf.

**Simka:2006:MTR**


**Sakr:2007:RCB**


**Steinwandt:2001:TDB**


**Steinwandt:2000:WHS**


REFERENCES

133, March 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

**Shailer:2001:PMT**


**Shamir:2001:NDC**


**Shao:2001:BVM**


**Sharp:2001:IKB**


**Shapiro:2002:CCM**

Jonathan S. Shapiro. CPCMS: a configuration management system based on cryptographic names. In

Shamir:2003:RS


Shamir:2003:TLC


Shao:2003:CIB


Shao:2004:IDS


Shao:2005:CXY


Sierra:2004:LCC

Shimizu:2007:CBE

Shoup:2000:CTU

Shoup:2000:UHF

Shoup:2001:OR

Shoup:2005:ACC


[Shp03] Igor E. Shparlinski. Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds


REFERENCES


[Sil01]:01:CLI

[Sil05]:05:ECC


[Sim01a] A. K. Singh. Deployment of public-key infrastructure...
REFERENCES

in wireless data networks.


References


Sucurovic:2005:JCX


Schaumont:2009:GEI


Song:2000:TPA


Seki:2001:DCR


Stojanovski:2001:CBRa


Sklavos:2005:ISH


Stavrou:2005: CAS

Stabell-Kulo:2006:ESC

Saldamli:2007:SME

Shu:2009:RCA

Sugita:2001:SRV

Sano:2000:PEA
REFERENCES

595


Schindler:2001:IDC


Srinathan:2002:ASC


Sugita:2000:RAD


Schneier:2000:CTA

[SKW00] Bruce Schneier, John Kelsey, Doug Whiting, David Wag-


Skoudis:2006:CHR


Stamp:2007:ACB


Sun:2009:CPR


Su:2005:KPK


Shi:2005:HEC


Sung:2000:PSS


Salido:2007:EBE

December 2007. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

**Song:2001:DWF**


**Sarkar:2000:CNB**


**Sarkar:2000:NBC**


**Sarkar:2000:CNB**


**Sebag-Montefiore:2000:EBC**

Sarkar:2001:EIL


Satoh:2002:SHS


Sarkar:2003:EIC


Satoh:2003:UHA


Sebag-Montefiore:2005:EBC


REFERENCES


Shigetomi:2002:ALS


Song:2000:ISC


REFERENCES

Singaravelu:2006:RTC


Sun:2008:BWN


Steen:2002:FAP


Springer:2003:BRB


Song:2001:ANL


Shin:2000:ANT

REFERENCES


**Sanchez-Reillo:2001:IBA**

[R01]


**Samarati:2001:AMP**

[R01]


**Standaert:2003:EIR**

[R03]


**StDenis:2006:BMI**

[R06]


**Stipcevic:2007:QRN**

[R07]

REFERENCES

Sarkar:2001:PAE


Stubblebine:2001:AAF


Seznec:2003:HUL


Swiderski:2004:TM


Seddik:2009:IWB


Shi:2008:UAU

Susilo:2000:NEF


Scambry:2006:HEW


Schmidt-Samoa:2006:AFW


StPierre:2000:TFA


Sakurai:2001:NSS


Shamir:2001:IOO

Stern:2001:ADW
[ST01c]

Stinson:2001:SAC
[ST01d]

Sakurai:2002:SMP
[ST02]

Satoh:2003:SDF
[ST03a]

Shamir:2003:FLN
[ST03b]
Adi Shamir and Eran Tromer. Factoring large numbers with the TWIRL device. In Boneh [Bon03], pages 1-26. CODEN
REFERENCES


Spivak:2006:SPT

Stallings:2000:SSC

Stallings:2002:CNS

Standboge:2002:ENO

Stajano:2003:SCU

Stanik:2005:NLO
REFERENCES


REFERENCES


Shimoyama:2002:MLC


Stone:2001:CI


Struif:2001:UBU


Strunk:2001:JQJ


Strubinger:2002:HBS


Stytz:2004:BRW

Saxena:2007:TCP

Shaltiel:2007:LEU

Sugihara:2001:PCD

Sugita:2003:DRW

Sun:2000:DRR

Sun:2000:ESM

Sun:2002:HIR
Hung-Min Sun. Improving the information rate of a private-key cryptosystem based on product codes. Informatica (Vilnius), 13(1):


Francesc Sebè, Alexandre Viejo, and Josep Domingo-Ferrer. Secure many-to-one symbol transmission for implementation on smart cards.


REFERENCES


[SWH+09] Hung-Min Sun, Mu-En Wu, M. Jason Hinek, Cheng-
REFERENCES


Swire:2005:SMI


Stevenson:2005:SCI


Song:2007:TAK


Shujun:2001:PRB


Seo:2001:CDA

REFERENCES

Shi:2001:NSF


Sun:2005:CSS


Syed:2000:CLA


Sun:2006:PBA


Syverson:2002:FCI


Shimoyama:2002:BCS

SYY+02 Takeshi Shimoyama, Hi-toshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun


REFERENCES


 REFERENCES


REFERENCES


[Tabatabaian:2001:NSP] Seyed J. Tabatabaian, Sam Ikeshiro, Murat Gunussoy,

**Tippett:1927:RSN**


**Torres:2007:ANS**


**Tseng:2001:GGO**


**Tseng:2001:CLB**


**Tseng:2003:DSM**


**Tico:2003:RAS**

REFERENCES

2003. CODEN ????. ISSN 0219-4678.


REFERENCES


REFERENCES

bibs/1965/19650156.htm;

[TROUTMAN:2009:CCGA]

[TROUTMAN:2009:CCGB]

[TRO08]

[TSAUR:2001:FUA]

[TSAUR:2005:SSS]

[TSAFAN:2006:FGD]

[TSAANG:2007:WCT]
Patrick P. Tsang. When cryptographers turn lead into gold. IEEE Secu-
REFERENCES


[TSS00] Kohji Takano, Akashi Satoh, and Nobuyuki Ohba. Poster 5: TATSU — hardware accelerator for public-key cryptography using Montgomery method. In Anonymous [Ano00d], page ??


[TZT01] Jun Tian, Tieniu Tan, and Liangpei Zhang, editors. Image compression and en-

Tuchman:1966:ZT


Turing:2004:BS


Tiri:2003:SEA

Kris Tiri and Ingrid Ver-...


[TWNA08] N. M. Thamrin, G. Witjaksono, A. Nuruddin, and

Tzeng:2004:NTM


Ting:2002:FBS


Tynan:2005:CPA


Tian:2005:NDF


Tong:2009:RAPa

REFERENCES


Tong:2009:RAPb


Uz:2009:MBT

Uz:2009:MBT


Unay:2008:SQE


Uchida:2009:FPR


USC:2000:HRS

United States Congress. H.R. 850, the Security and Freedom through Encryption (SAFE) Act: Markup before the Committee on International Relations, House of Representatives, One Hundred Sixth Congress, first
REFERENCES


[Uni00g] United States Congress.House Committee on the Judiciary. 106-1 Hearing: Security And Freedom Through Encryption (SAFE) Act, Serial No.
REFERENCES


[UP05] Andreas Uhl and Andreas Pommer. Image and video encryption: from digital
REFERENCES


USENIX:2002:PBF


USENIX:2002:PUS


USENIX:2002:PFT


Vasyl Ustimenko. CRYP-TIM: Graphs as tools for symmetric encryption.


REFERENCES

Vaudeny:2001:DID


Vaudeny:2002:SFI


Vaudeny:2005:PKC


Vaudeny:2005:SCI


[Ver02] Frederik Vercauteren. Computing zeta functions of hyperelliptic curves over finite
fields of characteristic 2. In
Yung [Yun02a], pages 369–384. CODEN LNCSD9.
ISBN 3-540-44050-X (paperback). ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25

Damien Vergnaud. RSA-based secret handshakes. In


Andrew A. Vladimirov, Konstantin V. Gavrilenko, and
Andrei A. Mikhailovsky. Wi-Foo: The Secrets of Wireless Hacking. Addison-Wesley,


Sviatoslav Voloshynovskiy, Alexander Herrigel, and
Thierry Pun. Blur/deblur attack against document protection systems based on

Mirko Viroli. A type-passing

**Vixie:2002:SRR**


**Vural:2007:IND**

idtype=cvips.

**Vo:2008:SMA**


**Volos:2009:IEP**


**Viega:2003:SPC**

John Viega and Matt Messier. *Secure programming cookbook for C and C++: Recipes for cryptography, authentication, networking, input validation and more*. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA
REFERENCES


REFERENCES

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

vanOorschot:2007:IRS


Vogt:2001:USC


Vasco:2001:CPK


Voyiatzis:2008:SFS


vanTilborg:2000:FCP


vanTilborg:2001:ECC

vanTilborg:2005:ECS


Vaudenay:2007:POK


Venkatesan:2001:GTA


vonWillich:2001:TIT


Vaudenay:2001:SAC

REFERENCES

0. LCCN QA76.9.A25 S22 2001.


David Wagner. A generalized birthday problem:

Wagstaff:2003:CNT


Walsh:2000:BRM


Walter:2001:PBM


Walter:2003:STM


REFERENCES

Wayman:2001:FBA


Wayman:2002:BAT


Wayner:2002:DCI


Wayner:2009:DCI


Weiss:2000:CA


Wu:2002:CSCa


[Williams:2001:ICA] Jeannette Williams and Yolande Dickerson. *The In-

Wang:2009:SST


Weaver:2006:BA


Weber:2002:ECH


Webb:2008:IZN


Wehde:2000:IME


Weierud:2000:SFB


WG02 Xiang Sheng Wang and Juan Ren Gan. A chaotic sequence encryption method.


REFERENCES

[Wu:2002:IBM]

[WHT08]


[Wen:2005:URE]

[Watanabe:2001:EAP]


REFERENCES


REFERENCES

Winkler:2005:SAU


Withers:2001:IWU


Wang:2005:ECSb


Welschenbach:2001:CCC


Wang:2005:ECSb


Won:2006:ISC

Thomas Weigold, Thorsten Kramp, and Michael Baentsch.


Shyh-Yih Wang and Chi-Sung Laih. Cryptanalysis of Hwang–Yang scheme...


REFERENCES


[Watters:2008:VDL] Xiang-Yang Wang, Pan-Pan Niu, and Wei Qi. A new adaptive digital audio watermarking based on sup-

Wang:2009:RDA


Wolkerstorfer:2001:AIA


Wollinger:2004:SHI


Won:2001:ISC


Wool:2000:KME

REFERENCES

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

Wang:2003:SGP

Wollinger:2005:CVH

Weimerskirch:2001:ECC

Wang:2001:TUR

Wright:2000:IQC
REFERENCES


REFERENCES


[Walter:2005:DDP]

[Weimerskirch:2002:DLW]

[Wu:2000:PK]
Chuan-Kun Wu and Vijay Varadharajan. Public key cryptosystems based on Boolean permutations and their applications. International Journal of Computer

[Wuensche:2009:CAE]

[Wu:2000:DPK]
REFERENCES


REFERENCES

Wang:2006:SPS


Wang:2008:DCP


Worley:2000:AFP


Wollinger:2000:HWH

Thomas J. Wollinger, Min Wang, Jorge Guajardo, and Christof Paar. How well are high-end DSPs suited for the AES algorithms? AES algorithms on the TMS20C6x DSP. In NIST [NIS00], pages 94–105. ISBN ???. LCCN ???.

WW06


WW08


WWA01

REFERENCES


Wincelberg:2002:LIE


Wang:2002:WEM


Wang:2008:HQS


Wang:2005:CTR


Wyant:2002:APK

Wyler:2005:ANS


Wang:2005:CSCA


Wang:2005:FCFa


Wang:2005:FCFb


Wang:2005:ECSa


Winslett:2005:PLD

REFERENCES


[Xiang:2008:CPA] Tao Xiang, Kwok wo Wong, and Xiaofeng Liao. Cryptanalysis of a password authentication scheme over in-

**Xie:2004:CTA**


**Xu:2009:AVB**


**Yang:2002:NEC**


**Yang:2005:TFN**


**Yan:2000:NTC**


**Yang:2007:CAR**


**Yasuda:2008:DLP**


**Yuan-bo:2004:ITA**

Guo Yuan-bo and Ma Jianfeng. An intrusion-tolerant


REFERENCES

Yang:2004:MSS


Yu:2007:NSM


Yang:2008:NFD


Yekhanin:2007:LDC


Yung:2006:PKC


REFERENCES

Yen:2003:RSC


Yardi:2008:HAC


Yamamoto:2001:PKB


Yu:2005:EHI


Yu:2009:SSG

Jia Yu, Daxing Li, and Rong Hao. An efficient

Yoo:2002:LAU


Yurkewych:2005:CIR


Yue:2006:NCB


Young:2001:RP


Yousef:2001:CAF


Young:2006:MCC

REFERENCES

0-8218-3730-3. viii + 159 pp. LCCN ???.

Youn:2008:WRB


Yang:2009:AIO


Yin:2001:RMW


Yilek:2009:WPK


Yoon:2004:SUA


Yoon:2005:CFI

Yo
[2005:ICJ]

Yo
[2005:IFA]

Yeh:2002:SAK

Yeh:2003:IAM
Yang:2001:EEA


Yoshiura:2001:AWB


Yao:2009:CAR


Yang:2004:ENT


Ytrehus:2006:CCI


REFERENCES


REFERENCES


REFERENCES

Zhang:2005:ITA


Zivkovic:2005:AAH


Zhao:2005:SSV

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

Zhang:2004:AIB


Zhang:2005:CHC

REFERENCES

Zhang:2009:CII


Zhang:2001:SOS


Zunino:2005:WPE


Zhou:2005:PSP


Zhao:2006:SAP


Zeadally:2000:IPQ

Zhang:2005:CSS


Zhen:2004:IBS


Zhang:2005:AES


Zou:2005:MED


Zhang:2000:WMH


Zhao:2006:NDN


Zhang:2008:CLR


Zheng:2001:ISS

Yuliang Zheng. Identification, signature and sign-

Zheng:2002:NPK


Zheng:2002:A


Zhou:2002:MVD


Zhong:2006:E

REFERENCES 690

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


Zhang:2005:CLH


Zhang:2004:AFV


Zhang:2004:RMA


Zhao:2005:MCE


Zhang:2001:QKD

Yong-Sheng Zhang, Chuan-Feng Li, and Guang-Can Guo. Quantum key distribution via quantum encryption. *Physical Review A (Atomic, Molecular,


REFERENCES

[Zafeiriou:2005:BRW]

[Zhang:2005:ISS]


Zhao:2002:EI1

Zhu:2002:PAK
REFERENCES


Zhang:2001:USC


Zhong:2008:GPT


Zhou:2003:ACN


Zhang:2005:ASP


Zhang:2005:ISM

[ZYM05] Peng Zhang, Chengqing Ye, and Xueying Ma. Improvement of secure mobile agent system in elec-


