Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/
01 March 2018
Version 3.315

Title word cross-reference

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

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p_k)
[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LZL+01, YCH04, CLT07]. (tn)
[PW05, SC05a]. + [Abe01]. {0, 1}
[LBGZ01, LBGZ02]. 1 [Wu02]. $125
[And04], 128 [AIK+01, PCG01]. 13
[HLST+02]. $15.00 [Imr03]. 2
[Bih00, BGN05, CY02, CKL+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 ± 10
[Mau01]. 2^{28} [Bih02]. 2^k [MFFT05]. 2^m
[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]. (2,126) [WB02].
0 [AIK04]. ABC [PS04b], d [BD00b]. E_0
[FL01a]. f_8 [KSHY01]. g^{-2} [Shp02]. g_r(x, 1)
[SZP02]. GF(2) [CP03]. GF(2^m)
[OTTT01, RMPJ08], GF(p^m) [BGK+03], GF(pt) [PZ01]. k [BJLS02, CT08b, GPC08, HK00, 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^n) [KKH03]. SL_2(F_2^n) [SG00b]. µ
[LN04]. n
[CT08b, Gon06, HK00, LKJ01, TM01]. N_0.292 [BD00b]. NC[0] [AIK06]. p [FL06].
41st [IEE00a]. 42nd [IEE01a]. 43rd [IEE02]. 44th [IEE03]. 45th [IEE04]. 46th [IEE05a]. 47th [IEE06]. 48th [IEE07]. 49th [IEE08]. 4th
[BCKK05, BC05b, DWML05, DRS05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, KN03, MS05a, NP02a].
5 [BCJ +06, Wac05]. 50th [IEE09b]. 512 [AD07, GLG +02]. 5th [CV04, KJR05, LL03, LLT +04, Li05, NP02a, Syv02, WKP03].

7 Round [Pha04]. 7.2 [TvdKB +01]. 7.7 [AL04]. 7th [BDZ04, Boy01, Chr00, DFPS06, PC05a, RS05, Scho1d, ST01d, Wri03].

8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800 [BG07a, Hir09]. 800-90 [BG07a, Hir09]. 802.11b [SIRO4]. 802.11g [Coc02a]. 802.15.4 [Miš08]. 82 [Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02, SMP +09, VY01, Vaut05a, WK06, Zhe02b].

9 [CGP +02, Gan08]. 9/11 [Ark05, Mah04]. 90 [BG07a, Hir09]. 9796-1 [GM00b]. 9796-1 [GM00b]. '98 [Wll09]. '99 [DNo05]. 9th
[CCMR02, CSY09, DR02e. DKU05, Lai03, NH03, Pat03b, PY05, YDKM06].

= [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05]. A5 [BD00a, BSW01, PS01c]. A5/1 [BD00a, BSW01, PS01c]. AAFFG1 [Hug02]. Aarhus [Cra05a]. Abadi [MW04]. Abelian
[CFC02, PHK +01, RS02]. Abstention [JLL02]. Abstract
[CM00, Cou04, DIRR05, HLvA02, HJW01, JL00, MSJ02, MP02, Mas04, Wag02, BJN00, BCDM00, CD00a, CC04c, FKS +00, GHJV00, GTZ04, HT04, HP01, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Pei09, Yas08]. Abstracting [Bla01a, Mon03]. abstraction [BLP06]. abstractions [BG07b]. Abstracts
[Sch00b]. Accelerating [ESG +05]. acceleration [EHKH04]. Accelerator
[CGBS01, RS04, TS000, XB01, DPT +02]. Access
[ANRS01, Ano02e, BN05, CGMM02, DS06, HC08, MS03b, Ril02, Sma03a, Sun00a, ZGLX05, AW05, AW08, AFB05, BA06, BN08, Che08b, DFM04, Hos06b, HY03, IY06, JW06, KNS05, LKZ +04, MF07, MSP +08, PS02a, STY07, WL05, WC01b]. access-control [BN05]. accessible [Pau02a]. accountability [WABL +08]. Accounting
[Lai08]. Accumulator
[GTH02]. Accumulators [CL02a]. accurate [ZY08]. Achieve [CFS01]. Achievement [Coc01a]. Achievements
[VDK05]. achieving [PS04c]. ACISP
[YG01c]. ACM
[ACM01a, ACM03a, ACM03b, ACM03c, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, MS05b, Bar00b, FMA02, RA06]. ACNS
[GKS05, IY05, JY04, ZYH03]. acoustic
[ZST05]. Acquiring [SETB08]. across
[Dav07, ZBLvB05]. Act
[Kha05, Uni00a, Uni00c, Uni00d, Uni00g]. Actel
[DV08]. Action
[SE01]. Active
[BC05a, BAC02, BP02, LIL05, MA00a, MA00b, Tad02, BPS08]. Active-Content
[MA00a, MA00b]. activities
[AJ08, SN07]. actually
[Hau06]. Ad
[BS02, KH05, WT02, Cha05b, DHR07, LHC08, LKZ +04, PC07, SLP07, TW07, ZC09, MA04]. 'ad-Durayhim’s
[MA04]. Ad-hoc
[BSS02, WT02, DHR07, ZC09]. Adaptation
[ISSZ08]. Adapting
[MJD01]. Adaptive
[CM00, CT04, CL08, CQ02a, CS02, CS03b, DSS01, EFY +05, FMY01, JMV02, KCJ +01, KLL01, LP01, MP05, Nov00, Pie05, ZWC02, AAP07, Che07, DP04, MB08, WN08, XMST07, YZD07].


Adaptively
[AF04b, CHK05, FMY02, JL00].
Adaptively-Secure [CHK05]. Added
[Ano02b, St.00]. Adding [FBWC02].
Addison [Puc03]. Addition
[KT00, LPZ06, PP06a]. Additive
[FMY01, MF01]. Adding [FBWC02].
Addition [KT00, LPZ06, PP06a]. Additive
[FMY01, MF01]. Additive-Sharing
[FMY01]. Address
[IIT03, Nik02a, Nik02b, FXAM04, RW07].
Address-Bit [IIT03]. Addressing
[HTW07]. Adi [Coc03]. Adic [GHK06].
adjacent [JT01b]. Adjustment [BSNO00].
Adlan [MAaTxx]. Adleman
[BB79, Coc03, SP79]. Administration
[USE00c, USE00a, Ris06, WL04a].
administrative [Cra05b]. Admitting
[HSZI00]. Advance [CZB01]. Advanced
[DFPS06, Lan00a, MM01c, Mor05, Sch06a, BBK03, DFCW00, ISTE08, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sye00, WBRF00, Wri01, YW06]. Advances
[Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS07, ELvS01, Kil01a, Oka00, Pre01, Pre00, TT07, Yun02a, Kat01, Bl003, CC04a, Cra05a, Fra04, Knn02, Lai03, Lee04b, LLI04, Li05, LST04, Men07, Roy05, Sho05a, Zhe02b]. Advantage [SZ01].
adventures [Hro09]. Adversarial
[CL09b, GSS08, MNS08].
Adversarial-knowledge [CLR09].
Adversaries [CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT04, ZD05]. Adversary
[Aba00, Gor06, RW02, AE05].
AES [CGH00b, DRS05, FIP01a, Her09, Pha04, AG01, Ano00a, AL00b, BBK03, CG03, Coc02b, DR00b, DR02a, DLP09, DPR01, Dau01, Dra00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, IMK00, ILO00, ILO01, Joh00, KS09, KLo05, KSFSS00, KV01, LP02a, Len01, MHM02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03b, RRY00, SKK00, SM03b, Sch00b, SKW00, SW00a, SL00, WW00, WB00, WOL01, WWGP00, WWCW00]. AES-CBC [Fer06]. AES-like [DLP09]. AES-related [Sch00b]. Afine
[Ben00, CT00, Fel06, HH09].
Afini-Transformation-Invariant [CT00].
AFIS [Zir07]. African [WD01b]. after
[Ber03, Mc06]. again [Fox00]. Against
[CS05b, DRS05, FKSW00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPPSW05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Ban05, BPR00, BP02, BBN09, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egh00, EBS01, FP01, Fry00, Geb04, HNZI02, HLL01, Hsu05b, HLC08, Ino05, ISW03, IIT03, JKS02, J000b, JT01a, Kan01, KM02, KML02, LM08, LPV09, L02, Mit00, M02, MG08, NRR00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC02, P08, P01b, PQ03b, RS01, SKQ01, Sch01b, SF00, SD01, Sem00, Sho00b, SKU00, SH01, SLL00, Tad02, TV03, VHP01, XH05, YJ00, YKL02a, YKL02b, YKL03, ZSJN07]. Age
[Mar08b, Lev01]. Agency
[AJ08, Ban02, Kov01]. Agent
[HQ05, KC02, PDJ09, RD01, RC01, Rot01, ZYM05, KXD00, SSM08, SH00]. Agent-Based
[HQ05, SMS08]. Agents
[WHI01, Hau06, LSA07]. Ages
[Eag05, Kin01]. Aggregate
[BGLS03, WK05]. Aggregated [ZSN05].
Aggregation [Her06, CCMT09, MS09b].
Aggressive [Wyl05]. AGO [Gau02].
Agreement
[AF01, CT00a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB04, AKN04, CYY05, CYH05, Che04a, CY05, CQ04, CQ05, HWWM03, KPT04, KRY05, KK05, LKK03a, LKK03b, L04a, LLL04, LLL05a, LKY05c, LKY05d, LKY06, LLS09, LRR02, PQ03a, PQ06, SH05, SW05, SC05b, Tsa06, Tse07, VK08, YW05, YW06].
YS02, YSH03, Yi04, YRY05b, ZC04, LLR06. agricultural [Lov01]. Aided [NS01b, HLL+02]. aim [Pau02a]. Aimed [SFDF06]. Airport [Sas07]. airwaves [Dar07]. Ajtai [GK05]. A KS [Che03]. Al [MAaTxx, Hwa05, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx]. al-fusul [MAaT05]. al-Ka [MAaT07]. Al-Kindi [MAaT03, MAaTxx]. Al-Kindi [MAaT05]. Al-Ka [MAaT07]. Al-Kindi [MAaT03, MAaTxx]. al-mutargima [MAaT05]. Alan [Pet08]. Alcatraz [LSVS09]. Alchemy [Pag03]. alert [AJ08]. alerts [NCRX04]. Alexandria [MS05b]. Algebra [Cou01, CD01a, Lan04a, CKY07, Fau09, HW03a, HWR09, Sh05b]. Algebraic [AK03, Bar09, Can06b, CMR06, CM03, Cou03, CS05, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mas04, MN01, MR02a, MR02b, PSM09, Bul09, CKN06, CDL06, Iwa08, May09]. algebraically [RBF08]. algorithms [BDFP02]. Algorithm [ANS05, AEMR09, Bar09, Can06b, CMR06, CM03, Cou03, CS05, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mas04, MN01, MR02a, MR02b, PSM09, Bul09, CKN06, CDL06, Iwa08, May09]. almost [AP09, BS00a, Dut01, Mar02b]. Alpha [WB00, Wu02]. Alphal [KHD01]. Altera [An02e]. Alternating [Wer02, HKPR05]. Alternative [Bad07, Gar03a, BMW02b]. always [BB79]. am [Eke02, SU07]. Analyses [BPR05, Des00a, Pau01]. Analysing [BL02]. Analysis [ARJ08, ABR01, AKS06, AD07, An01c, AIK01, ARC01, Ana03, BN00a, BDKB09, BR02, BF05, Bor01, BSL02, Cry00, CK02a, CS03b, DPV01, Dra00, FL01a, FGM00a, Gir06, GHT05, GLG02, GPR06, HSI01, HKR01, HSS04, Hey03, HM02c, IIT03, JK01a, JQY01, JT01a, JQY01, hKLS00, KMS02, LCK03, LKH09, LHY05, LWK00, LW05a, LKJL01, Lu07]. analysis [Mea04, MT07, MRST06, OS00, PSG09].
PS08b, SK01b, WLT05a, WPP05, XH05, XMST07, YCW+08, YC08, ZWWL01, ZL04c, ZDW06. Analytic [Shp03, Nie04].

Analyzing [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04]. anatomy [Bam02]. Anchor [Ree01]. Ancient [Imr03, Sin00, Mol05, Pin06]. Andrei [Puz04]. Andrew [Puz04]. Anguilla [Fra01]. Anniversary [Sal01b, Coc02a]. annotated [Pet08]. annoyances [Tyn05]. annoying [Tyn05]. Annual [ACM01a, ACM02, ACM04b, ACM05c, ACM06, ACM07, ACM08, Bon03, Cra05a, ELvS01, Fra04, IEE00a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IE08, IE09b, Kill01a, MZ04, Men07, Sho05a, USE01b, USE01a, USE01c, VY01, Yun02a, ACM00, Bel00, HA00, Jef08, NH03, ST01d]. anomaly [RCG05]. Anonymity [GM03, IKOS06, MP02, SS01b, EY09, LV07, Par04]. anonymization [FXAM04, RW07]. Anonymous [ABC05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL+08, SOOI02, Wan04a, YT09, ZJ09, BP03a, EY09, LHC08, Sae02, Sha03a, WC05, TWY05, ZC09]. ANSI [III00, Kel05, Oiw09]. ANSI-C [Oiw09]. Answers [PT08]. Anthony [Pag03]. Anti [Kha05, Ano05b]. Anti-Circumvention [Kha05]. anti-virus [Ano05b]. anticipation [Goo00]. Any [Fis01b, HNO+09, CDM00, DFM04, DMS00, HR07, Poi00]. Anyone [Ros07]. Anytime [DJLT01]. Anywhere [DJLT01]. Apache [Had00]. API [MW01, Mor03]. APIs [BM01c]. Appendix [Ke05]. Applet [ZFK04]. applets [Bis03a]. Applicability [Wya02, TM01]. Application [AD09, ACS02, Bai01b, Boy01, CL02a, CKQ03, Dam07, Dhe03, GHK+06, HF00, IKP+07, JX05, Jou04, Lai03, Lee04b, LLS05b, LXM+05, NP07, Oka00, Pfi01, 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, AG01, And04, BLST01, BH05, Bar06b, BI05a, BGK+03, BS00a, Bih03, BGOY08, BSS02, BLO8, CC04a, CD00a, CV02, CGH01, CZ05, CHSS02, CS09, Cra05a, CD01, DJ01, DKO2, DK07, DA03, DFPS06, FR02, GSS08, GKK+09. GJKR03, Gen04a, GRW06, Go01a, Gol04, HRS02, HN06, Har06, Has01a, HSS04, HR05, HJW05, JTO1b, JY01, KMM+06, KLG04, KMO01, KBM09, KK01, Maa07, MM07b, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Shp03, SY01, SPQ06, Vau02, Wya02, XYL09, ZY00, Zha02, ATOZ05, ATOE04, AH05, AFGH06, BG08, BGL+03, CCCC01, CM05b, CS09, CSK+08, DY09a, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gal02, GVC+08, GKK+07, GB09, HSS01, Has02, Hen01, HKPR05, Jac00, KVN+09, KNS05, La00, Lee04a]. applications [LJ05a, LPW06, LB05, MY01, Mal06, MC04, MSV04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SSS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPH06, WW08, WA06, WV00, YS04, ZBP05]. Applied [HW03a, HWR09, SL07, GV09, GNP05, IKY05, JY04, ZH03]. Applying [Elb09, KC02, Lam04, LMS07, SQ01, SPML02, TND+09, vDKST06]. Appointed [CL01a]. apprehension [AJ08]. Approach [BKM07, CGFSH09, CDR01, CW09, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, PBD00, Pau02a, Pre02a, SKG09, VH09, VVS01, Vri03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLMM05, GGH+08, Har05a, J01, JW01, LYM02, MT09, Mar05b, ML09, Mos06, NN03, SL07, SN04, SW00b, ZLX99, ZSQ01, ZL04b, ZL04a]. Approaches
Approvals [CGMM02, AvdH00, DG05, Fri07, Has01b, KXD00].
Approximation [CLZ02, Kuk01, WL02].
Approximations [BDQ04].
April [An00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH^00b, DFPS06, Joy03b, Knu02, Mat02, NIS00, Nac01, Sch01d, SMP^09, YDKM06].
APSS [ZSV05].
Arabic [MAaTxx].
Arbitrarily [RW03b].
Arbitrary [AR01, BR00b, BR01, CKN00, CHJ^01b, CF02, Tee06].
Arbitrary-Length [AR01, BR00b, CKN00, CHJ^01b].
Architectural [ASK07, ABM00, BMA00a, BMA00b, BMA00c, CW02, Gro03, KV01, LTM^00, ZYLG05, Ano05b].
Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LTM^00, ZYLG05].
Architectures [BGK^03, 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].
Arête [Bau01a, Bau01b].
Arguments [HNO^09].
ARITH [BS03, BC01, IEE05b].
ARITH-15 [BC01].
ARITH-16 [BS03].
ARITH-17 [IEE05b].
Arithmetic [BS03, BIP05, BGK^03, BCDH09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDJ^01, SR06, GPS05, PS04a, SOIG07].
arithmetics [Lam01].
ARM7 [DV08, XB01].
armies [Ano03b].
Army [Boy03].
Arne [Bec02].
array [DZL01].
Arrays [ABM08, BS00a, GC01a, HW05, PP06a].
Arrived [Law05].
arsenal [Blu09].
Art [And07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Eri03, Eri08, MS02d].
Article [Che08b].
Artifacts [EHK^03].
Artificial [Cop04b, MMYH02].
Arum [For04].
ASCII [MJD01].
ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Roy01, Oka00, DN00b, KI01a].
ASIC [WOL01].
ASIP [SKW^07].
asks [An00a].
ASM [MK05a].
Aspect [Kos01a].
Aspects [BLMS00, CMR06, Pel06, DLP^09, Rup09].
Aspiration [Ash03].
assessing [CDD^05].
assessment [CC05e, DMS07].
assets [KH03, NRR00].
Assignment [BRTM09, HC08, CHC04, DFM04, Hwa00, TP07, WC01b, hY08].
assignments [SWR05].
Assisted [ECG^07, XS03, BB05, HLH04].
ASSL [VH09].
associated [XLMS06].
associativity [HRS08].
Assumption [CS00, DN00a, FOPS01, KMZ03, ZD05].
Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT^00, Nao03, SBZ02, Mic02a].
Assurance [LXM^05, AL04, BJ02, FOP06, Gha07, Jen09].
Assurances [Bar06b].
Astrology [Pag03].
Astronomy [MYC01].
Asymmetric [CH07b, Man01, SY01a, SBZ02, WHI01, YG01a, GJ04, Lee01, OP01b].
Asymptotically [vDW04].
Asynchronous [CKPS01, FML^03, KSR02, SKR02, ZSV05].
at-targama [MAaT05].
Atlanta [IEE09b].
ATM [Pat02a, Pat02b, Zea00].
Atomic [CVN06].
Attached [RCBL00].
Attachments [Ric07].
Attack [Ah08, CKQ03, CS05b, CS03b, Des00b, Fil00, FV03, GHJ00, GHJ01, HQ01, Hug02, HW01, J00b, KCP01, KS00a, KML^02, KM01c, LY07, LNL^08, LV04, LM05, Luc02a, Man01, MHH04, MSU05, Nov01, OM09, PV06a, PQ03b, RMS05, SGM09, Sch01b, Sho00b, Sma03b, VHP01, YKLM02a, ZC04, ASK05, DKL^00a, Duj08, Duj09, GM00a, HAU04, Hes04b, HG07, Iwa08, JJ02a, KS09, KM04a, LM08, Law09b].
LS05b, Mir05, OS00, SIR04, XH05].

**Attack-Resistant** [LNL+08]. attacker [BDSV08]. Attackers [JMV02]. Attacking [FMP03, KPR03, TMMM05, BF06a].

**Attacking-Based** [TMMM05]. Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, BMM00, BB+02, BDK+09, BU02, BM03b, BP02b, BM01c, Can06b, CS07b, CT08a, CJS01, CKN00, CM03, Coo3, CWR09, CD01b, DP01, DFS04, DJ06, DS08, DM07b, FKS00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GK02, HSH+08a, HNZI02, HR04a, HSH+01, HLC08, ISW03, JKS02, JJ00d, KKS00a, KKS01, KCJ+01, KI01a, Law09a, LLS05a, LJ05b, MOP06, MP06, MF01, Mes00, Mes01, Mo02, MG08, OT03a, OT03b, OOP03, OST05, Ove06, PKBD09, PDM09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZZ05, YYYDO01, YY01, YG01b, vW01, BPS08, Bau05, BCS08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05b, HL05b, Ino05, IM06, JDJ01, KOS05a, KTC03, LPV+09].

attacks [LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RGA05, Scho0c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07, WL04b, Yan07, YS02, ZSJN07].

**attractors** [HHYW07].

**Attribute** [LY05, RSA00e, IY05]. Attributes [SS01b].

**Auction** [AS01a, Ano01a]. auctioning [RCG+05].

**Auctions** [Bra01b].

**Audio** [Arn01, CS05c, DRL09, MH05, WNY09, WWL+02, XFZ01, WNQ08, BOS01b, KJR05, KN03].

**Augmented** [CS07c, You01].

**Australia** [Boy01, IZ00].

**Authentic** [DGMS03, Dur01, SS01b].

**Authenticate** [Bau03a, Bau03b].

**Authenticated** [AGT01, BN00a, BPR00, BU02, BC04b, BM01b, BMP00, BC01, CPP04, Ch08, DG03, DA03, EP02, GKK007, GL03, GTC03, HS07, KOY01, KY03, Kra03, Lee01, LHT09, MPS00, Mac01, MSJ02, MND+04, NA07, Nam02, Nu05, Poh01, SK00, Vau05b, WC01a, YPP09, Yi04, ZCY02, BKN04, BCP07, CYY05, CYH05, Che04a, CLC08, C04, CJ05, GL06a, GMR05, HTJ08, HWW02, HWW03, HS05a, Hva06, H05c, H05d, KOY05, K05, LKY03a, LK03b, L04a, L05a, LKY05c, L05d, LHC08, LL02, LL05a, LW05a, Mis08, P03a, P06, RBB03, Se05, SW05, SC05b, TLL05, T01a, Tse07, WH02a, XY04, YW05, YC09a, YS02, YSH03, YRY05b, YPKL08, ZC04, ZAX05, Z05b, ZL05].

**Authentication** [AIP01, CGV09, Fur05, JW05, PM08, RCBL00, YSS+01, Lin01a].

**Authentication** [AAK09, AP09, ANRS01, Ano01b, Ano01c, Ano01e, An02c, AHKM02, ANL01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, BCC01, BDhKB09, BR02, BDF05, BDF01b, BM03c, BL02, BLD09, BWE+00, CV03, CGP08, CS07b, CLK01a, CLK01b, CC05b, CC09, CJ03c, CWY05, CT09, Cim02, Cir01, CGK+02, CJK+04, Col01, CMB+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, Gan01a, Gar03a, GM05, GSV02, GD02, GTO2, Gut04c, Had00, HSH01, HSH02, HSH06, HKW06, HY01, Hoe01, HS01b, HP00, HL07, ISS08, Jab01, J02a, JP07, JP02b, KJR05, K09b, KH05, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LTL+04, LB04, LL05c, LSH03b, LM00, LHL+08, Lys07, MM01a, Mal02, MJ04, MD04, JR03, MG02, MNT06, Nao02, Nik02a, Nik02b, OKE02, OH08].

**PK01, Qu01, RKZD02, Ric07, Ril02,**

**Authorized** [DKU05, Pf01, Jef08].

**Authenticate** [Bau03a, Bau03b].

**Authenticated** [AGT01, BN00a, BPR00, BU02, BC04b, BM01b, BMP00, BC01, CPP04, Ch08, DG03, DA03, EP02, GKK007, GL03, GTC03, HS07, KOY01, KY03, Kra03, Lee01, LHT09, MPS00, Mac01, MSJ02, MND+04, NA07, Nam02, Nu05, Poh01, SK00, Vau05b, WC01a, YPP09, Yi04, ZCY02, BKN04, BCP07, CYY05, CYH05, Che04a, CLC08, C04, CJ05, GL06a, GMR05, HTJ08, HWW02, HWW03, HS05a, Hva06, H05c, H05d, KOY05, K05, LKY03a, LK03b, L04a, L05a, LKY05c, L05d, LHC08, LL02, LL05a, LW05a, Mis08, P03a, P06, RBB03, Se05, SW05, SC05b, TLL05, T01a, Tse07, WH02a, XY04, YW05, YC09a, YS02, YSH03, YRY05b, YPKL08, ZC04, ZAX05, Z05b, ZL05].

**Authenticating** [AIP01, CGV09, Fur05, JW05, PM08, RCBL00, YSS+01, Lin01a].

**Authentication** [AAK09, AP09, ANRS01, Ano01b, Ano01c, Ano01e, An02c, AHKM02, ANL01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, BCC01, BDhKB09, BR02, BDF05, BDF01b, BM03c, BL02, BLD09, BWE+00, CV03, CGP08, CS07b, CLK01a, CLK01b, CC05b, CC09, CJ03c, CWY05, CT09, Cim02, Cir01, CGK+02, CJK+04, Col01, CMB+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, Gan01a, Gar03a, GM05, GSV02, GD02, GTO2, Gut04c, Had00, HSH01, HSH02, HSH06, HKW06, HY01, Hoe01, HS01b, HP00, HL07, ISS08, Jab01, J02a, JP07, JP02b, KJR05, K09b, KH05, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LTL+04, LB04, LL05c, LSH03b, LM00, LHL+08, Lys07, MM01a, Mal02, MJ04, MD04, JR03, MG02, MNT06, Nao02, Nik02a, Nik02b, OKE02, OH08].

**PK01, Qu01, RKZD02, Ric07, Ril02,**

**Autonomous**.
authentication [KJY05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LLH02, LHL03a, LF03, LKY04, LW04, LHL04, LKY05a, LLY06, LLS+09, Li05, LST+05, LCX08, LW05a, LFW04, LHL03b, LT04, LC04a, Lin07, LN04, LLW08a, LLW08b, LC05a, LC05b, Luk01, MS09c, MABI06, Mit00, MR00, ME08b, MP07, NC09, NLD08, PY08, PCS03, PCC03, PI06, Pei04, Pot03, Pot07, SNW01, SG07, SN07, Sch05c, Sco04, Sei05, Sh05c, SSM+08, Shi05, SLO5a, St.00, Ste05a, SW02, SCS05b, SC05c, SCS05c, SZS05, TM06, TBJ02, TOEO00, TIS07, TW07, TWL05, UBE09, VM03, VK08, Vo05, Wan04a, WLT05a, WDLN09, WL04b, WHHT08, YW04, YWC05, YTW07, YCY07, YC09b, YS04, YRY04, YRY05a, YRY05c, YY05b, Ybj04, ZL04a, ZK05, ZSN05, Zha06, ZSN07, dB07, CS08b, ECM00a, ECM00b, LSH03a].

authenticator [CKY07].

authority [KJY05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LLH02, LHL03a, LF03, LKY04, LW04, LHL04, LKY05a, LLY06, LLS+09, Li05, LST+05, LCX08, LW05a, LFW04, LHL03b, LT04, LC04a, Lin07, LN04, LLW08a, LLW08b, LC05a, LC05b, Luk01, MS09c, MABI06, Mit00, MR00, ME08b, MP07, NC09, NLD08, PY08, PCS03, PCC03, PI06, Pei04, Pot03, Pot07, SNW01, SG07, SN07, Sch05c, Sco04, Sei05, Sh05c, SSM+08, Shi05, SLO5a, St.00, Ste05a, SW02, SCS05b, SC05c, SCS05c, SZS05, TM06, TBJ02, TOEO00, TIS07, TW07, TWL05, UBE09, VM03, VK08, Vo05, Wan04a, WLT05a, WDLN09, WL04b, WHHT08, YW04, YWC05, YTW07, YCY07, YC09b, YS04, YRY04, YRY05a, YRY05c, YY05b, Ybj04, ZL04a, ZK05, ZSN05, Zha06, ZSN07, dB07, CS08b, ECM00a, ECM00b, LSH03a].

Authentication [KJY05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LLH02, LHL03a, LF03, LKY04, LW04, LHL04, LKY05a, LLY06, LLS+09, Li05, LST+05, LCX08, LW05a, LFW04, LHL03b, LT04, LC04a, Lin07, LN04, LLW08a, LLW08b, LC05a, LC05b, Luk01, MS09c, MABI06, Mit00, MR00, ME08b, MP07, NC09, NLD08, PY08, PCS03, PCC03, PI06, Pei04, Pot03, Pot07, SNW01, SG07, SN07, Sch05c, Sco04, Sei05, Sh05c, SSM+08, Shi05, SLO5a, St.00, Ste05a, SW02, SCS05b, SC05c, SCS05c, SZS05, TM06, TBJ02, TOEO00, TIS07, TW07, TWL05, UBE09, VM03, VK08, Vo05, Wan04a, WLT05a, WDLN09, WL04b, WHHT08, YW04, YWC05, YTW07, YCY07, YC09b, YS04, YRY04, YRY05a, YRY05c, YY05b, Ybj04, ZL04a, ZK05, ZSN05, Zha06, ZSN07, dB07, CS08b, ECM00a, ECM00b, LSH03a].
Sho05a, Yun02a. **Barcode** [Che08b]. **Bare** [DPV04]. **Barken** [Sty04]. **Barret** [Gro01]. **barriers** [Kov01]. base [DIM08, IR02]. **Based** [Ano01c, ANR01, AF03, AJO08, BDG+01, BKLS02, BNS02, BN02, Ben00, BRS02, BF01b, BF03, BB04, Bon07]. BCHK07, BGH07, BPR+08, BD03, BMN01, Boy03, BQR01, BM05c, BSN000, BRTM09, CGFSG09, ČvTMH01, CK02a, CGM02, CF01b, CC02a, CV03, CPP04, CDD07, CS07b, CLT07, CHSS02, CHM+02, CZK05, CM05a, CTH08, CGK+02, Coc01b, Con01, CFS01, CS00, DN00a, DKMR05, DT03, EHK+03, EM03, FL06, FM02a, FMY01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HC08, HH09, Igl02, Jam00, KBD03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05, KY02b, KC09b, KC02, KCD07, KPR03, Kra02a, Ku02, KWP06, KT00, LL02, LP03, LKLK05, LHT09, LZ01]. **Based** [LZ04, LL05c, LPZ06, LY07, LWK00, LHS05, LSZ05, LL05b, LCD07, MPS00, Mar08a, Mar08b, MNP01, Miy01, MG02, Mi01a, MSU05, NMO05, Nak01, Nam02, NBD01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP06a, PZL09, Ri02, RE02, RH02, RS00, RS03, RS08, RMC01, Sal05b, Sch01a, SSFC09, Sha02, Sha01e, SOOJ02, SXY01, Sma03a, SBEW01, SGB01, TMM05, TYY02, TZT09a, TZT09b, VMSV05, Vau05b, Ver06a, VH01, VK07, WRW02, WY02, WZ05, WG05, WCJ09, WH09, WBD01, WC04, XYL09, YKMY01, YT09, YYD01, YSS+01, YKV01, YLH05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWYC02, vDW04, AAP07, AA08, An02b, App05, AAK09, BGB09, BR04, BFG08, BS01b, Bha01b, BMW05, BLP06, BGL+03, BDS09b, Buh06, CGH06, CG06, CL02b, CL04d, CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c]. **Based** [CJT01, CL09, CJL06, CJL05, Che08b, CYH+07, CFVZ06, CDD+04, CTT07, CHT02, CC04c, Cra05b, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EHKH04, FXAM04, FWL08, GMR08, GW08, GL06a, GHD+00, GS01, GPS05, GGS+09, GB09, HM00, HLL+02, HCD08a, HCD08b, HRL09, Has00, Her07, HPS01, HG05a, Hsu05a, HLwWZ09, Hih00, HP01, HLL03, HL05d, IM06, JK01a, JK01b, JW06, JZCW05, JLL01, KG09, hKLS00, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KCL03, Ku04, KCC05, Kwo03a, KHKL05, LHL03a, LF03, LKY05a, LKY05b, LHY05, LD01, LTH05, LPM05, LW05a, LWZH05, LYGL07, LLW08a, LLW08b, LCC05, LSA+07, LCZ05c, LCZ05a, LLL06a, LCC06b, MS09c, Mic01, MR09, Mi09, Mit00, MB08, MC04, MPPM09, MV03b, NZCG05, NC09, NSNK05, OS09, PCS07, PW05, PBMB01, PSC+09, PS08a, Pel06, PSP+08, PC00, PL05a]. **based** [PLJ05b, QCBO5a, Reg03, Reg04, RG09, RCG+05, Sae02, SG07, Sco04, Sei05, SPG02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SC05a, nSgFtL05, SSM+08, SW05, SH00, SK01b, SCL05, SMO02, SCS05c, TWNA08, Tsa05, HUA+09, UBE09, VS01, VKS09, WAF00, WL07, WJP07, WNW08, WLLH05, Whi09, WV00, WH02b, WY05, XMST07, YW04, YCW+08, YS04, hY08, YJ00, YPSZ01, YRY05e, YPKL08, YY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRMS05, NZS05]. **Bases** [AAC+01, ADDS06, BK09, B+02, ČvTMH01, EBC+00, FJ03, FLA+03, CCT08, Fau09, ZT03]. **Basic** [Gol01b, Gol01a, Gol04, Kat05b, Puc03, Ste02, Bon00]. **Basis** [Leh06, Lut02]. **Basing** [BPR+08, CHL02, AGGM06, AGGM10]. **Basis** [RMH03b, VaV03, vW01, GPS05, LS05b, RMH03a]. **Batch** [Ara02, HL01, PBD07, Sha01d, BLH06, HLH00]. **Batching** [SB01]. **Battery** [CBSU06]. **Battle**
Bay [Cal00c]. Bayes [Goo00]. BB84 [Ina02a]. BC [IEE02]. BCH [MLC01]. BDD [KLN+06, Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01]. Beach [IEE00a]. beat [Lev01]. because [AJ08]. Become [Ort00]. Been [Nic01]. BeepBeep [Dri02]. before [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YJ00]. Beginning [Dew08, Hoo05]. Beginnings [Bud00b]. Begins [MP00]. Behavior [Vav03]. BEHEMOTH [Bar00c]. behind [Hen06b]. Beijing [FLY06, LST+05]. Being [ASW+01, ES00a]. beleid [dL00]. Belgium [DR02c, Pre00, QS00]. Belief [BPST02]. believing [Buh06]. Bell [BZ02, Eke02]. Benchmark [Ase02, TLYL04, LDH06, YLT06]. Bendy [Sas07]. Benefit [YKLM02a]. benefits [CH00]. Benford [NM09]. Bergen [Ytr06]. Berkeley [IEE06]. Berlin [FLA+03]. Bermuda [Bla03]. Bernard [DNRS03]. Berners [Coc02b]. Berners-Lee [Coc02b]. Best [Bau01a, Bau01b, MFS+09, Gol08, Ste02]. BestCrypt [Bau02b]. Bethesda [ACM09]. Better [FV03, PM00, MR02, SK01, HLL00, Pau03]. BetterBASIC [ASW+01]. Between [DKMR05, Ket06, Ngu05, NN06, Fau09, GKM+00, GC05, MSV04, Pau01, SK03, SKI01, WCJ09, XH03, YG01b]. Bi [Cou04, PJK01]. Bi-directional [PJK01]. Bi-linear [Cou04]. Bias [CL02c, Ser00]. Biased [BS00a, LSKC05]. BiBa [RR02]. Bibliography [Bee05]. Bidiagonal [BR09]. Bidiagonal-Singular [BR09]. big [RR03a]. BigNum [SR06]. Bilateral [CT08a]. Bilinear [BGLS03, BMS03, CL04a, HMS04, KK02, LC05b, VK08]. Bill [Gen00a]. billing [SSM+08]. Binarization [LSKC05]. Binary [AD09, HHM01, LSKC05, OSSST04, SKG09, WCJ09, ÁCTZ05, BG08, BG09, FSGV01, GB09]. Binary-Ternary [AD09]. BIND [Kle07]. Binding [DN02b]. BioAW [MJ04]. Biometric [AHKM02, Dal01, EM03, HWH01, KJR05, LLT+04, PK01, SR01, Sas07, Way01, Way02a, Wea06, BS01b, KN03, Li05, LST+05, MR00, Smi00, MJ04, TBJ02, ZJ04]. Biometrics [Ash03, Bjo05, JR03, Ri02, Str01a, BSSM+07, BCP+03, Buh06]. Biometrics-Based [Ri02]. Biomolecular [Bi09]. Birds [MLM03]. birth [Bud06, SE01]. Birthday [Wag02]. Bismulation [BJP02]. Bit [AIK+01, BK06a, BL08, CGH01, CDL+00, DMS00, GS07a, IIT03, KZ07, LNS02, MS09d, PCG01, RMH03b, SM03b, SY01, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, Pri00, RMPJ08, SWR05, UHA+09, WW08, ZFK04]. Bit-Fixing [KZ07, KZ03]. bit-substitution [GPX08]. BitLocker [Kor09]. Bits [BS01d, SZ01, HN04, Shp02]. Bitslice [DPV01]. Black [Ano01i, CF02, CFS05, DI05, DRR05, DS08, KY01d]. Black-Box [Ano01i, BR02, CF02, CFS05, DI05, DRR05, KY01d]. Blackmailing [PS01b]. Bletchley [Sal00b, Cop05, Cop06, HS01a, Sal05a, SE01, Smi01b, Wei06, Win00]. Blind [AO00, BNPS02, BB00a, BSC01b, CL01b, JKK+01, LY07, Na05, Pau02b, SPK08, ZTP05, ZK02, Fan03, HC04a, JLL01, JL04, LH05, LCZ05b, MS09a, SV08a, SHT05, WHH05, ZC05]. blindness [AvdH00]. Blink [Sas07]. Block [AIK+01, BR02, BS01a, ČVTMH01, Can01b, CLLL00, CP02, CMB+05, Cro01, DR00a, Do03, EYC00, Fhu02a, HSH+01, JKK+01, KCP01, KYHC01, KKG03, LRW02, MV00, MS02a, NPV01, OSMK01, Pat01, PS06, Pli01, RMS05, SM03b, SY+02, SKU+00, SKI01, WC09, X03, YG01b, BaI08, BF06a, DYM01, Dun06, Egh00, GPX08, Hey03, JKK01b, Jun05, Kat05a, KJ01, LDH06, WGD06].
Block-Cipher-Based [BRS02].
Block-DCT [BSC01a].
Blockcipher [GM02c, OS07].
Blockciphers [Fur01].
Blocks [Jou02].
Blockwise [JMV02].
Blockwise-Adaptive [JMV02].
Bluetooth [GBM02, LV04, LMV05].
Blunders [Bur01].
Blur [VHP01].
Blur/Deblur [VHP01].
Blurring [LSKC05, SK06].
Board [CGBS01].
boat [DB04].
Body [Bam02, TG07].
BOEL [Fin02].
Boethius [Eag05].
bolstered [Ano01h].
bombe [Wil01a, Tur04].
Bombes [Ano02i, LBA00].
bombs [Lov01].
Bonds [CAC03].
Boneh [ASK05, Hes04a].
Bonn [DRS05].
Book [And04, Duw03, Eag05, Fal07, For04, Gas01, Gum04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Ree01, Rot07, Sal03b, See04, Shp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wal00, Was08a, Kat05b, Lam07, MAaT05, Sin99, Sin00, AAG].
Books [Dr.00c, Ree01].
Bookshelf [Lut02, Lut03, Wil01b].
Bookworm [Sal03b].
Boolean [Car02, CT03, CS09, MS02b, QPV05, SM00a, SM00b, SM03a, SM03b, WV00].
Boomerang [KKS00a, KKS01, KML].
Boot [HSH, HSH, HSH].
Border [MJF07].
Borders [PGT07].
Boston [USE01b, USE01a].
bot [Ano08b].
Botschaften [Sch09].
bottleneck [WL02].
bottlenecks [HTW07, Bonn [CGBS01]].
Bound [CY08, DGN03, KMT01, HLLL03, hY08, GW00].
Boundaries [PGT07].
Bounded [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, hY08, GW00, GGK03, JZ09, PS02a, Shp99].
Bounded-Quantum-Storage [DFSS08].
Bounding [DM07b].
Bounds [BDF01b, BP03b, DIRR05, Di01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GGK03, JZ09, PS02a, Slg09].
[HHSS01, Poh01]. **Buy** [PLW07]. **Buyer** [MM01a], **buys** [Zaf00]. **Buzzes** [Coc02b]. **Bytecode** [Coo02, Ler02]. **Byzantine** [CNV06, HGR07, LLR02, LLR06, PI06]. **Byzantine-Resistant** [CNV06].

C [Ter08, Zo10, III00, Oiw09, RMP08, Sea05, Sea09, VM03, WK01, We05]. C# [MJ03]. C-testable [RMP08]. C2C [HTJ08]. CA [ACM03b, Joy03b, KKP02, Men05, Men07, Nao04, Oka04, Pre02c, USE02a, USE02b]. **CAA** [MGC02]. Cache [BTTF02, Klc07, OST05, OST06, TSS+03, Ino05, WL07], cache-based [WL07]. Caches [GSVC02, LLK05]. Caernarvon [TKP+08]. Caesar [Chu02, You06]. CAIDA [Pri00]. Cairo [EBC+00]. CalLC [Sil01]. calculus [MRST06]. Calcutta [Roy00a]. Calibrating [SDMN06]. Calif [ACM03c]. California [ACM03a, ACM07, Bel00, Bum03, Fra04, IEE00a, Kil01a, Sch01c, Sch04a, Sch05a, Sh005a, USE00b, USE02c, Wil99, Yun02a, IEE06]. Call [Ano04a, Ano07b, Ano07a, M04d]. Calls [WG05, Ano08c, WCJ05]. Cambridge [ACM10, Chr00, Chr01, CC002, CCM05, EIE03, JQ04, Kat05, Kil05, Nao04, Pag03, Puc03, Rot07]. Camellia [AIK+01, HQ01, KM05, HHL+02, SM03b, SKI01, X05].

Camera [CGK+02]. Camera-Based [CGK+02]. Can [BB02, CBZ+01, Dav01c, Lai08, Ros07, Ver06b, CNPQ03, CG05, SBB05, Zir07]. Canada [ACM02, ACM08, AMW07, HH04, H05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. **Candidate** [I00, EYCP00, NIS00, SKW+00, SL00]. Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WBO0]. Cannes [AJ01a, AJ01b]. cannot [Gav08]. canonical [TP07]. CANS [DWML05]. Canterbury [CZ05]. Cantor [WPP05]. Capabilities [BDTW01, AL04, ABDS01]. Capability [MH05]. capable [ETMP05]. Capacity [ChLYL09, Sug01, ME08a, Wan05]. Cape [IIE05b]. Card [BCST00, CMG+01, CL07, DF01, DFPS06, RE03, RS01, SR01, Ano00k, Ano00l, AJ01b, Bor00, BGL+03, Bur00, Cal00c, Car01, CCCY01, Cha05a, Cla00b, Con00, CH00, DFCW00, GMG00, HM01a, Has02, Hen01, Hus01, Jac00, LSA+07, LC05a, Lu07, Q00, RE00, SP02, Smi00, VK08, Zaf00, Che00, FGL02, Pan02b, SKKS00, TV03]. card-based [LSA+07]. **CARDIS** [DFPS06]. **CARDIS’98** [Q00]. Cards [And04, AJ01b, Bel01, CK06, DLT01, HBdJJ01, JSJK01, JY01, L000d, MOP06, MV01, MN01, MG08, NFQ03, Q00, Sak01, Sha01c, TBL01, VPG01, YMY01, Ano04b, Ano04c, AJ01a, BPR01, BCH05, Bur00, DFH01, DFPST07, Fin03, GU01, HHSS01, Hsu05b, KLY03, LKY05a, Ler02, LCS09, MY01, Poh01, PB01, Pre07, SVDF07, TIS07, Ano03a, BJvdB02, CL04d, CCK04b, Che00, Gro03, HL05b, Ku04, KC05, LHY02, Sco04, SCF01, YW04].

**CardS4** [GN01]. Care [Mad00, RC06, Ano03a]. carefully [Cla00b]. Carlo [Bi09, Sug03]. cars [LPW06]. Cartilage [MYC01]. Cartography [SGM09, SWR05]. Cascade [DGH+04]. Cascaded [Jou04]. Case [ABK00, Ano05a, BBGM08, BU02, BCP01, CNS02, GS07a, Nie02b, OIS05, Vau01, BKN04, BF06a, BK05, CSK+08, HRS08, KWDB06, Mic02a, Mic02b, OST06, Pei09, ST07, SKW+07, SPH06, ZWDL01]. case/average [Mic02b]. cases [ABHS09]. Cash [PS01b]. **Cathedral** [USE02a]. Cats [Pen01b]. Caught [Wei00]. cause [SB05]. Causes [Mur01]. Cautionary [GMP01a]. Cayley [Lam91]. Cayman [Svy02]. CBC [BBKN01, BPR05, BR00b, DGH+04, Fer06, JMV02, KI03, Vau01, Vau02]. CBIDs [MC04]. CCA [KOMM01, Mü01b]. CCA2 [BST02, Lin03, RG09]. CCA2-Secure
14

[102x646]Lin03. **CCGrid** [TLC06]. **CCM** [Dwo03]. **CCS** [Mar02b, MS05b]. **CDH** [CM05a]. **CDH-Based** [CM05a]. **Cell** [Fox00, MYC01, SHL07]. **Cell-phone-free** [Fox00]. **Cellular** [Laf00, LZ04, MGC02, PZL09, SBZ04, ETMP05, KK03, SIH07, Wan04a, dRMS05, Wue09]. **Center** [AUW01, CH01a, CYH04, LPM05]. **Centered** [BKM07, CMB05]. **Central** [CHL02]. **Centralized** [Wac05]. **Centre** [PPV96]. **century** [Kob00, Lan00c, PRS04, Gan01b, Lan00a]. **CERT** [Sea09]. **certicom** [LM08]. **Certificate** [BLM01, Gen03, GMR08]. **Certificate-Based** [Gen03, GMR08]. **Certificateless** [HLC08, HRL09]. **Certificates** [BDTW01, CMG01, RdS01, Bra01a, LCK04, ZSM05]. **Certification** [ANR01, CHM02, RSA00b, BGB09, BD04b, KB09]. **Certified** [ANR01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LWK05a, NZS05, Sha04b, Sha05b, TLH05, Tsau05, TJC03, WH03]. **Cerven** [Sal03b]. **CFS** [Ito01]. **ChaCha** [Ber08]. **Chain** [YT09, YZ00, Wue09]. **chain-rules** [Wue09]. **Chained** [BCC01]. **chaining** [PCC03]. **challenge** [LM08, LW05a, PRS04]. **challenge/response** [LW05a]. **Challenges** [C1a00a, GV09, Nao03, Sta03, SVEG09]. **Chang** [CWJT01, ZC05]. **Chang-Wu** [CWJT01]. **change** [CYH05]. **Changes** [Mru01]. **Changing** [BST03]. **Channel** [BU02, CHVV03, Law09a, LCK03, M¨ol02, NMO05, OT03a, OT03b, Sch06a, SYLC05, ARR03, BP03a, BG07b, Buh06, CNPQ03, KSWH00, LCZ05b, MS09e, PSP+08, WL07, YTWV05]. **Channels** [AIP01, CK02b, Nam02, Vau05b, LH04]. **Chaos** [JK01b, SK01b, WZ05, JK01a, LMC+03, McN03, PSG+09]. **Chaos-Based** [WZ05, SK01b, JK01a, PSG+09]. **Chaotic** [LLL+01, SXY01, USS02, Vav03, AMRP00, AMRP04, GHdGSS00, GB09, HHYW07, HLwWZ09, JK01b, LMC+03, LYGL07, MA02, PBMB01, PS01a, PZL09, SPG02, SL09, UHA+09, VKS09, WG02, WW08, kWpLwW01, WLW04, YZEE09]. **Chapman** [Kla05b, Was08a]. **chapters** [MAaT05, Tat05]. **Characteristic** [Gau02, GPS06, KT00, Ver02, GPS05]. **Characterization** [AJ008, Nam02, XH03, BGM04, KY00, QPV05, XLMS06]. **Characterizations** [Pas05]. **Characterizing** [BTW05, BTW08]. **Charging** [BACS02, RH02]. **Chatter** [Kee05]. **Chau** [BNPS02, KLN+06, WHH05]. **Chaumian** [M¨ol03a]. **Cheating** [CCL09, OKS06, PZ01, PZ02b, PZ02a, ZP01]. **check** [Kir01b]. **Checkable** [BPST02]. **Checking** [BL02, JP07, KLN+06, YJ00, GGH+08, RG05]. **checklists** [Sha01a]. **Checks** [FM02a]. **Checksums** [Sto01, SGPH98]. **Cheju** [Kim01]. **Chemical** [EIJ01]. **Chen** [LW05c]. **Chennai** [CV04, RD01, Roy05]. **CHES** [JQ04, KKP02, KP01, KN01, RS05, WK03]. **CHESS** [LKHL09]. **CHESS-64** [LKHL09]. **Chicago** [ACM04b, Top02, Con00]. **Chien** [YRY05b]. **Children** [BCHK07, CKN03, CHJ+01a, CHJ+01b, Des00b, DK05, FP01, IM06, KS00a, KY01a, KCJ+01, KMZ03, KM+01, Ki01a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH+09, KOG09]. **Chinese** [LT+04, Li05, Sch01b, CAC06, YKLM03]. **Chip** [BNPW03, DV08, MM01b, MM01c, MP00, Fox00, ISTE08, Ano04b]. **Chip-Secured** [BNPW03]. **Chipkarten** [Ano04b]. **Chips** [Ano04d, Pau02b]. **Choice** [Jam00]. **Chosen** [BCHK07, CKN03, CHJ+01a, CHJ+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JK02, J00b, K500a, KY01a, KCJ+01, KMZ03, KM01c, Ki01a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH+09, KOG09]. **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, BRS02, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DPS05, DF07, Dwo03, EYCP00, FF01a, Flu02a, GBM02, HCJ02, HQ01, KHYC01, KHD01, LKHL09, MSNH07, NPV01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY⁺02, SXY01, SBEW01, SK101, WB02, Wu02, XH03, ZCC01, BGP09, BB00a, BVP⁺04, GPX08, GG05a, Hey03, KH08, Kid00, LKH⁺08, Mac00, PSP⁺08, RBB03, Sal00b, SHH07, WW08, Win05b, WF02, XH05].

**Ciphers** [AAG⁺00, BBKN01, BS00b, BR01, BKM07, ČvTMH01, Can01b, CF01b, Can06b, CJS01, Chu02, CHJ02, CP02, CM03, Cou03, DPV01, Eaq05, Fil00, FF01a, Fil02, Gol03, HR00, HR04a, HSH⁺01, Jan00, Jan06, Kan01, KCP01, KKG03, LRW02, MV00, Oni01, PP06a, Pl01, RMS05, Sar02, SM03b, SKU⁺00, Wai00, Wri05, ??02, YG01b, ZC00, Bai08, Bar06a, Be07a, Ber07, Bod99, DLP⁺09, DY01, Dun06, DK08, Egh00, GP06, HW03a, HWR09, Hey03, J01b, Jun05, Kat05a, KSWH00, Kin01, LMSV07, LDH06, Lun09, Max06, MI09, MWM01, Pin06, SJHR04, Smi01b, SL07, SB05, TT00, Wag03, YI00, You06, Kat05b].

**Ciphertext** [BBK03a, BCHK07, CKN03, CF01b, CS07c, CHJ⁺01a, CHJ⁺01b, CS02, CS03b, Des00b, DK05, FP01, JKS02, JJ00b, KS00a, KY01a, KJ01, KMZ03, Kur01, Man01, Nov01, PV06b, Sh000b, BM05, CHH⁺09, IM06, KG09, Poi00].

**Ciphertext-To-Only** [BBK03a].

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

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

**Circuits** [BI05a, FMI⁺03, Gol03, IS03, MD05, PBWT07, You01, GLC⁺04].

**Circumvention** [Kha05]. **Cirencester** [Hon01, Pat03b, Sma05]. **CIRM** [PPV96].

**CISC** [FLY06]. **citizens** [An03a]. **claims** [DS00]. **clamping** [An03a]. **Clandestine** [Wri05].

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

**Classes** [Cy02, RSA00c]. **Classical** [BYJK08, Gav08, GW00, LW05b, NA07, BYJK04, JZ09].

**Classification** [HMS04, PBD00, Uni01].

**Cle** [RSA09a]. **Cleaner** [TR09a, TR09b].

**Cleaning** [Lut03]. **cleanup** [Lov01].

**Client** [ANRS01, An01e, ANL01, FSSF01, PS05, WKB08, Bad07, HTJ08, LF03, YS04].

**Client-Server** [ANRS01, PS05].

**client-to-client** [HTJ08].

**Clients** [JRF01, RKK02]. **Clinton** [Gen00a].

**Clip** [FGL02]. **Cliques** [PQ06].

**Cliques-type** [PQ06]. **clock** [Pau02b].

**Closed** [CGFSHG09, MH04]. **Close** [DM07b].

**Closing** [Lau08b, PWGP03].

**cloud** [CKS09]. **Clouds** [GS01, VS01].

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

**Cluster-Based** [KCD07].

**Clusters** [MFS⁺09]. **CM** [CMKT00, GHK⁺06]. **CMS** [BWBL02, DKL05].

**Co** [Bud00b, Nd05, ACM01b]. **Co-Design** [Nd05].

**Coalition** [ACJT00]. **Coalition-Resistant** [ACJT00].
Codebreaking [Bud00a, Bud00b, Sin01b, Alv00, Bud02, Cop05, Cop06]. codec [Che08a]. Coded [MLC01]. Codes [Bee05, BP06, Big08, Bod99, BQR01, CC09, Chu02, CDG+05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ?702, YYDO01, Yek07, Bel07a, aSM01, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HW09, Kov01, Lam07, Lun09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Smi01b].

Coded MLG [MLC01]. Codes [Bee05, BP06, Big08, Bod99, BQR01, CC09, Chu02, CDG+05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ?702, YYDO01, Yek07, Bel07a, aSM01, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HW09, Kov01, Lam07, Lun09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Smi01b].

codeword [AJ08]. Coding [Buc00a, CS05c, HHL+00, Joy00, LLL+00, MZ02, Pat03b, RK06, Sal05c, Smi05, TW02, TW06b, Ytr06, Che07, DW05, Gar04, Hou01, PPV96, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sea05, Sea09, TW05, Irw03].

Coefficients [CH01b, KT00]. Cohen [Was08a]. Coherent [TPPM07]. Coin [Lin01b]. Coin-Tossing [Lin01b]. Coins [HR04b]. Cold [HSH+08a, AJ08, HSH+08b, HSH+09].

cold-boot [HSH+08a, AJ08, HSH+08b, HSH+09]. collaboration [ED03, PCSM07, SBG05, SBG07].

collaborative [LLY06]. collapse [SBB05]. Collection [GMM08, Bro05a]. Collections [Kuh00]. Collective [BBB+02]. collide [GNP05]. Collision [DG02, IK005, MS09c, WYY05a, WYY05d, GM00a, Sen00].

Collision-Resistant [IK005]. Collisions [BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c].

collision [BGW05, HNZI02, Zan01]. Cologne [WKP03]. Color [CTL04, Che07, Che08a, CTY09, FG01, AEEdR05, CDD07, Yan02, YCL07].

Colorado [BC01, Sch04b, USE00d]. Colored [CDD07]. Colossus [Cop04a, Cop05, Cop06, Lav06, Sal00b, Sal00a, Sal05a, Salxx]. Colour [RS00].

Coloured [AADK05]. Columbia [ACM08]. column [Raj06]. Combination [CF01b, Gau02, GHPT05, GB09].

Combinatorial [GMW05, SLTB+06, Hen06a].

Combinatorics [Lec03b]. Combined [LLS05a]. Combiner [Sar02, LL06].

Combiners [AK03]. Combining [Abe04].

Comes [Mar08b, An003e]. Coming [Dan01].

Commemoration [BZ02].

Comment [SCS05b, WY05, WLY04].

Comments [AS01c, CGH+06b, JW01, MNFG02, SW+00, CJT04].

Commerce [CLK01b, GS02a, Kir01a, Sta00, Uni01, ZYM05, BM03a, FB01, Gra01, MY01, SN07, YC09a].

commercial [LCC05, YLR05].

Commitment [DN02b, DMS00, FF00, CAC06, HR07, KKL09]. Commitments [BN00b, CF01a, DFM04, 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, ANR01, 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, SN01, UP05, WWA01].

Communication-Efficient [Fis05, LLS+09].

Communications [GN06, HJ07, Igl02, Kra01, Lan00a, Lan04b, LCK01, LL01, MS05b, Sal01b, Vau05b, VM02a, B0P03a, CYH04, HWV02, LC04a, Sal05c, Ser06, SL05a, Wl09, WGL00, YTWY05, DKU05].

Community [SK06]. commutativity [HRS08]. commuting [CRK08].

Compact [CG03, JT01b, SMTM01, YT09, ZLK02, JAW+00, Mic02a]. companies [Ste00].

Company [ASW+01, Zaf00]. Comparative [DPR01, GLG+02, Kat05b]. Comparing [HU05, KLN+06].

Comparison [GC00a, GC01a, Gau02, JRB+06, MS02e, SW00a, WW00, FGM03, JL03, SMA01, WB00].
Compendium [Lut02]. Compensated [AAK09], competition [Cla00b], compiler [DFG00, Oiw09], Compilers [Lut02].

complement [YCO99]. Complementary [AS01c]. Complete [Bar00a, Bee05, Bud00a, FGMO01, GCKL08, HMS04, KY00, MS09d, Sal07, TWM+09, Bud02]. Completeness [HG03, MW04, ABHS09, PT08]. Complex [Cla00b, Bud02]. Completeness [HG03, MW04, ABHS09, PT08]. Complexity [Lut02].

Complexity-Theoretic [CB01]. complex [JKK+01, LKLK05]. Complex [JKK+01, LKLK05]. Completeness [HG03, MW04, ABHS09, PT08]. Complexity [Lut02].

Complexity Theoretic [CB01].

compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BSL02, Hei01, TEM*01].

composability [PS04c]. Composable [AF04b, BOHL+05, BLDT09, CF01a, CK02b, DN02b, DN03, NM005, RK05, Can01a, CLOS02].

Composite [CQ001, GMC01a, RDJ+01, Zhe01].

Composition [BJP02, BN00a, CR03, CV02, Pie05, Sh00a, Can06a, LHR02, LLR06, Puc06].

compositional [GM04]. Compostela [BS03]. Compound [SB05].

comprehensive [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04].

Compressed-Domain [ISSZ08].

Compressibility [HN06]. Compression [ABM08, BD03, HSCK01, Kei02, LHS05, RS08, Sal07, SFH00, 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, BIM00, BJLS02, CC00, CDM00, CDN01, CDG+05, CDI05, DNO3, DIO5, DMO0b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, Jef08, K004, KLML05, KSR02, Lin01b, PS05, WW05, An002g, AB09, BE00, BE01, CLOS02, CL08, CDD00, DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WHH05, WY05, SM07b, Duw03].

computation-efficient [CLC08].

Computational [CCL09, DLP+09, G02, HG03, KLR09, KK06, Rup09, SM07b, WvD02, AUW01, IKOS08, Lam01, Lau08a, Nie02a, Sh05b, SHJR04].

Computationally [MPSW05].

Computations [HL05a, ML05, RM04, SBZ04, TC05].

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

Computer [BS03, Bis03b, Bro05a, BCDH09, BC01, CSW+08, CZK05, CGK+02, Cc02a, Coc03, HYZ05b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Ifr00, JBR05, KM07, Le06b, Lut02, MYC01, MS05b, MAC+03, N02d, RC06, SB07, T105, Cas02, DFGH04, Fau09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Sh06, SLO6, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coc03].

computerized [LMC+03, Pau02b].

Computers [Coc03, Ett02, TSS+03, Cop05, Cop06, RH00].

Computing [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBK00, CG00a, CL01a, Cop04b, EP02, J003, LBA00, LKHL09, Lut03, May04, PHM03, Sh06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TL06, VHO9, Ver02, WC01a, Wri00, Yan00, YK08, Cha07, Che05b, CHT02, DHL06, HV09, HKR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sc05, W109, YL05, Lut03].
DFM04, DPT+02, JW06, KNS05, LKZ+04, MD04, MSP+08, PS04b, STY07, WC01b.

**Control-flow** [ABEL05]. **Controlled** [GVC+08, IMM01, AW05, AW08, LAPS08]. **Controlling** [HY03, MS03b, MS02d, WL05]. **Controls** [Har01a, Har01b]. **conventional** [CJ04, YW05, YRY05b]. **Converging** [Pot07]. **Conversation** [GK04].

**Controlled** [GVC+08, IMM01, AW05, AW08, LAPS08]. **Controlling** [HY03, MS03b, MS02d, WL05]. **Controls** [Har01a, Har01b]. **Converging** [Pot07]. **Conversation** [GK04].
Cho06, Cho08b, CHJ02, CP02, Cou04, CGJ +02, DG00, DGP07a, DGP07b, DGP09, DN00b, FJ03, FKS +00, FKL +01b, FKL +01a, Fin06, Fhu02a, Fhu02b, Fur01, Fur02a, Fur02b, GS07a, GM02a, GJS01, GS02c, GM02b, GM00b, GBM02, GC00b, Gra02a, GS09, GKN +08, HPC02, HQR01, HAuR04, Hen06a, HLL +01, HSM +02, HIK +04, Hsu05a, HLH00, Hwa00, JK02a, JJ00c, JJ01, JnBdXgXm05, Jou09, Joy03a, KM02, KW03, KS00b, KRY05, KW02, KRS +02, KKS00b, Kra02a, KC05, Küh01, Küh02b, KHKL05, LCo3, LHL +02, LP03, Lee03c, LKY04, LL05a, LR07, LBGZ01, LBGZ02, LLH04].

Cryptanalysis [LL05c, LLCL08, LW05c, MS03a, May02, MG01, MHL +02, Mor05, NPV01, PSC +02, PKH05, Pei04, Pei06, PS06, PS01c, QCB05a, Sch06a, Sco04, Sha03c, Sha05a, STK02, SGB01, SK00, SHH07, TIGD01, TM06, TLI05, TJI01b, TSS +03, Wag00, Wag03, WL05, WBD01, WB02, Wu02, XY04, YSD02, YW05, YKLM02a, YKLM02b, YRY05a, YY05a, YOu01, YG01a, YG01c, ZY01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, ÅMRP04, BF01a, BAI08, Bar09, BS01c, Bu06, Bu09, Bur02, CV05, CK06, KCL +03, DUN06, Egh00, EBS01, Eke09, Fie09, GPG06, Goo00, Jun05, KSS00, Kuk01, LMK08, Max06, MAA03, MAA04, MAa05, MAa06, MAa07, Nyb01, Pha04, RSA03, Rup09, SK01a, Sel00, Sin09, SL07, SCS05b, SL07, Sze08, TC00, TM01, WIL04, WF02, YL00, YY00, YKLM03, Kat05b].

Cryptanalyst [Wil06].

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

Cryptic [Wri05].

CRYPTIM [Ust01b].

CRYPTO [Fra04, Men07, Sho05a, Ahn08, Ano01j, Ano03e, Bau01a, Bau01b, Bur01, CCM01, CNB +02, Lev01, Lev02, Mar08a, Mar02b, MC04, Pem01b, SYLC05, TR09a, TR09b, Yun02b, Bec02, BK05, HGS03, Web02, Bel00, Bon03, Kil01a, Yun02a, Sei00a].

Crypto-algorithms [Ano01j, CCM01].

Crypto-based [MC04].

Crypto-CCS [Mar02b].

Crypto-integrity [Yun02b].

Crypto-systems [Ano01j, CCM01].

Crytoanalysis [HIS02, LD01].

CryptoAPI [Bon00].

Cryptoclub [BP06].

Cryptocomplexity [Wri05].

CRYPTO [Fra04, Men07, Sho05a, Ano03e].

CryptoAPI [Bon00].

Cryptocomplexity [Wri05].

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

Cryptic [Wri05].

CRYPTIM [Ust01b].

CRYPTO [Fra04, Men07, Sho05a, Ahn08, Ano01j, Ano03e, Bau01a, Bau01b, Bur01, CCM01, CNB +02, Lev01, Lev02, Mar08a, Mar02b, MC04, Pem01b, SYLC05, TR09a, TR09b, Yun02b, Bec02, BK05, HGS03, Web02, Bel00, Bon03, Kil01a, Yun02a, Sei00a].

Crypto-algorithms [Ano01j, CCM01].

Crypto-based [MC04].

Crypto-CCS [Mar02b].

Crypto-integrity [Yun02b].

Crypto-systems [Ano01j, CCM01].

Crytoanalysis [HIS02, LD01].

CryptoAPI [Bon00].

Cryptoclub [BP06].

Cryptocomplexity [Wri05].

CRYPTO [Fra04, Men07, Sho05a, Ano03e].

CryptoAPI [Bon00].

Cryptocomplexity [Wri05].
IYK02, IYK03, JW01, KAM08, KSF00, KP03, LMTV05, Lau05, LLW05, LLW09, ML05, Mea04, MT07, Mic02b, MRST06, Mon03, NN03, NdM04, NdM06, PS04a, PSG09, PR05, Pri00, Puc06, QPV05, Reg03, Reg04, Ren09, RMH04, RBF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b.

cryptographic
[kWpLwW01, WLW04, XLMS06, YLT06, ZLX99, ZWWL01, ZL04b, dH08, BWBL02, JQ04, KKP02, KP01, KNP01, RS05].

Cryptographically
[ADD09, AHS08, BJF02, BFCZ08, BB00b, FR08, MS02b, RGX06, Aam03, AW05, AW08, Lau08a, SM03a].

Cryptographically-masked [AHS08].

CryptoGraphics [CK06].
cryptographie [RSA09a].

Cryptography
[ANS05, AF04b, ADI09, AA04b, Ano00e, Ano01, Ano02b, Ano02f, Ano02h, Ano04a, Ano05a, Ano07b, Ano07a, AAFG01, AIK04, AIK06, App07, AEAO05, ABM00, Bai01a, Bai01b, BINP03, BD04, BOV03, BOV07, BBGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BWB02, Bha02b, BDDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, BK06b, BKM07, Buc00b, BD08, BP01b, BRTM09, CPS07, Cer04b, CCL09, CSW08, CQ01, CPD06, Cob04, CFA06, Cop00, Cor06, Dr00c, Dam07, DFS05, DFS05, DDO0, DFG04, DK02, DK07, Des02, DT03, DY09b, DSS01, DD00, DD03, Dre00, DP08, EPP07, EP05, Eib09, Eli04, ECG07, Ett02, FS03b, Gal01, Gal02, GHK06, GKK09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Gri01, Gro05, HR06, HH04, HHM01].

Cryptography
[HMV04, HSS01, HPS08, Hon01, JEE00b, IKY05, Irw03, IKOS06, IKOS08, JY04, JL00, JT01b, JT01a, Jue04, Kak06, KLR09, KZ07, KCS07, Kat05b, KK06, KBM09, KPMF02, KWDB06, KY01c, Kir01a, KMS02, KZ02, KS03, KWP06, Lam01, LG01, LSY01, Lee03, LLL01, Lie05, LDM04, LW05b, LP02b, Lu03, Lys08, MNT00, MP02, Mao01, Mao04, MZ04, Man01, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pe06, PM02, PBB02, Poi02, PT06, Puc03, RASA0a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGK08, Sti05, Sti01, Sti02, Sti06c, SJ05, Syv02, TSO00, TW06a, TG04, TW02, TW06b, Tre08, TR09a, TR09b, Uni01, USS02, TY01, VMC02].

Cryptography
[WPS01, Wei04, WK01, Wel05, Wie00, WvD02, Wri00, YWC08, Ytr06, YC01, YDKM06, ZY03, dW04, Im03, AMW07, AUW01, Ano02a, Ano02g, ABDS01, Ber09b, BD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BE00, BEM07, Buc00a, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CCO07, CDF05, CDD07, Cos00, Cre00, CDD07, Dif01, DMO0, DWW05, DOPS04, DKL09, DW09, Duv03, Eke02, FXM04, FP09, Fra01, FP00, GV09, GL05, GKK07, Geb04, GRTZ02, Gol99, GG05b, GHP05, GPS05, GNP05, HH05, HHL00, HKR05, HA00, Hig08, HSK00, Hoo05, HG05b, HLLW09, IZ00, IM06, JK01b, Jan08b, Joy00, KZ03, KL08, Kat01, Kil05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Lop06, Maur04, May01, McA08, MBS04, MM07a, Mol07, NP02a].
cryptography
[Nis03a, NH03, Opp05, OS09, PP09, PY05, PC00, Pin06, Reg05, Reg09, Rot02b, Rot03, Roy00b, Rup09, STY07, SBZ04, Ser06, SH05, Shp99, Si05, Sin09, Sin00, Sm04, ST01d, SK01b, TW05, UHA09, Vas05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Wli09, Wri03, YC09a, YY04, YCO7, vT05, For04, HC02, Kat05b, Pab03b, Si01, Sma05, Bee05, Lee03a, Rec01, 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, Lai03, LL04c, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka04, Poi06, Rot05, RS02, Sha03b, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bin03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam01, LL03, Lee04b, Men05, Men07, Nac01, Oka00, P05a, P601, Pre00, Pre02c, RD01, Roy05, Sh05a, Son00, Won01, WK06, Yun02a, vT00, DWML05].

CryptoManiac [WWA01]. Crypton [CKK02, MG01]. Cryptosystem [BST02, FL06, GG01, GK05, GHW01, Hug02, KM01a, KY02c, KLC+00, LHT09, dvP06, Luc02b, NSN05, NBD01, Ove06, PH+01, YG01a, YGO1c, Zhe02a, Zho06, Bao04, CLO2b, CCH04, Che05a, Cho06, CFV06, CHH01, Dan02, DHL06, EKRMA01, GhdGSS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04b, LL06, KLYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SPG02, SCS05a, SP79, SLC05, Sun00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, yH08].

Cryptosystems [Aki09, Ava03, BDG01, BKLS02, BP000, BM00, CHSS02, CCW02, DG+06, DKXY02, ESG+05, FJ03, Fel06, FP01, HJW01, IZ00, Jou02, JQY01, KY02a, Kim01, KLY02, KKY02, Kl01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vad03, Wya02, XB01, ZL02, Ban05, BF06a, BB79, CH01c, CMKT00, EBS01, EHHK04, GHO8, GBK01, HM00, Has00, Has01b, Hüh00, HP01, KW00, Kos01c, LD01, Luk01, Mic01, Mis06, OS00, Pei09, PLJ05b, SSS06, Sha05c, Sma01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WV00, Y000, ZSZ01, vT01].

cryptovirology [YY04]. CRYPTREC [Y00]. CSCW [ZP05]. CT [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09]. CT-RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09]. CTO [Ano03c]. CTS [Con00]. Cuban [AJ08]. Cube [DS08, PDMS09]. Cube-Type [PDMS09]. culture [Gil07]. Cumulative [WP03]. cure [RD09]. cure-all [RD09]. Current [DFH01, PRS04, LPW06]. curriculum [FOP06]. Curve [ANS05, ADI09, Ano05a, Ava03, BNP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BM01, CQS01, CFA+06, GPP08, HYZ05a, HMM0, HMO2c, JT01b, JT01a, KMM09, KMF02, KSZ02, KWP06, LW02, Mö02, K03, OTIT01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, X01, YYZ01, ZL02, BSS04, BSS05, BG04, BG07a, CCHO4, Che05a, CFV06, DIM08, DwWmW05, EKK04, GKP01, Has01b, Hsu05a, HL05, JW06, L04b, Mis06, OS00, ST03a, SSST06, S05, Sma01, SLC05, SLC05, TC05, Ver01, Wol04, WPP05, Y009a, ZSZ01, ZL05, vT01].

Curve-Based [KWP06, Pel06]. Curves [ARA08, Bai01a, BB06b, CY02, Gal01, GL01, Gau02, GHK+06, Kid02, PWGP03, Ver02, CMKT00, H04, LWZH05, MP01b, MS04, Sil05, Sim02, SC02b, Was08b, Wen03, Yas08]. customer [Lin01a]. CVS [DFG01]. Cyber [FNRC05, WW04, Mau05]. Cyberinsurance [BP07]. Cybersecurity [PLW07]. cyberspace [Mit02]. cycles [ABH09, BPS08]. Cyclic [PG05, Mic02a]. Czech [MJ04].

D [Du03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05]. D.R [Irw03]. demons [Mos06]. Damgård [CDMP05]. dark [Bla09]. darkening [CDD07]. DARPA [Coc01]. Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BNP03,
Bro05b, Che01a, CTLLO1, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, K"us02, Lan00b, LP00, LHS05, LS08, Lut03, MND+04, MS03b, MFS+09, NM09, OS05, Per05, RKZD02, RK06, Sal03a, Sal07, Sin01a, SDMN06, TZDO5, TPPM07, VDKP05, WS05, WY02, WN02, kc01, vW01, AG09, AHK03b, AKSX04, Ano02c, Arn01, Bla00, BNP08, CCMT09, Cer04a, CLR09, CPG+04, DZL01, DGMS03, FS04, HILM02, LLK05, MJ03, Mal06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGPH98, SETB08, WMDR08, YLC+09, YC08, ZSJN07, Zir07, Cur05, DK08, Lin02, Pap05]. **Data-Hiding** [VDKP05].

**Database** [ACM03c, ACM05b, BI05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Man04, PS08b, PBV01].

**Database-service-provider** [HILM02].

**Databases** [AK02b, CD05, DN04, AHK03a, CDD+05, CKY07, GA03, MSP09, MNT06, NS05b, UG08, YPPK09].

**Datamining** [DN04].

**Datenverschlüsselung** [Lin02]. **David** [Gas01, Pap05, Bar05, Eag05].

**Days** [SE01, CSW05, Win05c].

**DC** [USE01c]. **DCT** [BSC01a, BSC01b, CH01b, KTO00, LY07].

**DCT-Based** [LY07]. **DDH** [Lys02]. **DDO** [LKH+08]. **DDO-64** [LKH+08]. **Dead** [Gut02a].

**Dealer** [Pau02b].

**Deal** [DK01, Sun00a]. **Dealing** [BH00a].

**Debate** [Jo01, Mad00].

**Debian** [YRS+09, Ahm08].

**Debugger** [Ano02d]. **Debugging** [Ano02d].

**Dec** [IIE09a].

**decades-old** [Lov01].

**December** [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, Lai03, Lee04b, LTT+04, Li05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b].

**Decentralized** [MSP+08].

**deception** [CS07a, Mah04, MS02d].

**Decidability** [K"us02].

**Deciding** [Bau05].

**Decimal** [Bau05].

**DDH** [Lys02].

**DDO** [LKH+08].

**Dead** [Gut02a].

**deaf** [Pau02b].

**Dealer** [DK01, Sun00a].

**Dealing** [BH00a].

**Debate** [Jo01, Mad00].

**Debian** [YRS+09, Ahm08].

**Definition** [YWD08, SNI00].

**Definitions** [Uni01, AH05].

**Definitive** [BS01a, BSB05, Gar03b].

**Defying** [HRS08].

**Degenerate** [Ber09a].

**Degradation** [BSC01a].

**Degree** [CV02, QPV05].

**Degrees** [Sat06].

**Déjà** [DP00].

**DeKaRT** [Go03].

**Dekker** [Irw03].

**Delacorte** [Irw03].

**Delay** [WRW02, NS01a].

**Delayed** [JM07].

**delegated** [CL04c].

**Delegation** [WN02, ZP05].

**Delhi** [JM03, RM04].

**Delivers** [Ano02e].

**Delivery** [NZCG05, RMCG01, DY09a, NZS05].

**Delphi** [TEM+01, He01].

**Demand** [BD03, CMB+05, SEF+06].

**Democracies** [CZB+01].

**Democracy** [CTBA+01].
Demography [Coc03]. Demons [Mos06]. demonstrably [HL06]. demystifying [RR04]. Deniability [Pas03]. Deniable [Nao02, CCK04a, CSK+08, DG05, LC05b, YRY05c, Zha06]. Denial [Mah04, Nik02a, Nik02b, PKBD01, Rii02, Mir05]. Denial-of-Service [Nik02a, PKBD01]. Denmark [Cra05a, TBJ02]. Denver [ACM01b, Sch04b, USE00d]. Department [Bol02, Eri01]. Dependable [NABG03, And08]. Dependent [Gol03, WS05, BPS08]. deployed [BDET00]. Deploying [BH00b, GSB+04]. Deployment [CL07, KDO01, Mur01, Sin01a, App05, JRR09]. Dept [Uni01]. Depth [BI05a]. Derandomization [BOV03, BOV07]. Derivation [DGH+04]. Deriving [BJP02, CSW05]. DES-encrypted [Bih02]. DES-like [Egh00, EBS01]. Desch [LBA00]. Describing [PS06]. Description [Lav06, MH05]. Descriptors [DNP07, SP04]. Design [Abd01, AADK05, Ano02e, ADD09, AIK+01, ARC+01, Bar00b, Can01b, CDP01, Cm02, 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, SPO02, SRQ03, Uz04, WZ05, WW08, WLLL09, ARJ08, CMS08, GSG05b, Gut04c, HC04a, Hut01, KSF00, MI09, MWM01, SYE09, YCW+08, YC08]. Design/CPN [AADK05]. designated [LV07]. Designing [HBC+08, TCR03, C+02, CG05, Lan00c]. Designs [Bee05, CC02a, Bai08, Des00a, WL07]. Desktop [Mun08, BDET00]. Desmedt [CHH+09]. Desynchronization [CDTT05]. Detached [Sha01c]. Detailed [Lut03]. Details [Scr01]. Detect [FOBH05]. Detecting [CMS09, FGD01, JQYY01, Har07a, LHL04]. Detection [AS01b, AD07, BB00a, BKM07, CH01b, CZK05, JT05, KKG03, SKQ01, SY01a, SLT01, ST01c, TZD05, TMM05, WG05, YI01, Zan01, Bej06, BBK+03b, HLL+02, Men03, NN02, WMS08, YW06, ZGTG05]. Detection/Correction [SKQ01]. Detector [BSC01b, DN07]. Determined [KKH03]. 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, CNB+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, KDO01, MV01, MRL+02, SCF01, WC01a, Ano06a, CMS08, DMT07, Tse07, ZYW07]. Devil [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]. Differentiating [LS08, WWTH08]. Different [CGMM02, Sma01]. Differential [Ava03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eke09, Fur02a, Gra02a, HLL+01, HSM+02, HHK+04, IIT03, JT01a, Kan01, KM02, KCP01, LHL+02, MP06, MM09, MHL+02, MG08, PSC+02, PQ03b, SK01a, SU+00, SKI01, YSD02].
vW01, BF01a, CUS08, Che08a, DLP +09, Egh00, EBS01, Pha04, SLL +00, TM01. 
**Differential-Linear** [BDK02a].
**Differentials** [BF00b].
**Difficult** [Bud00b, MT02].
**Difficult-to-pass** [MT02].
**Diffie** [Jan08a, ABR01, ASW +01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKRT08, FS01b, GR04, Ki01b, KK02, KM04a, Kra03, Kra05, Miš08, Tsa06, YRY05c].
**diffuser** [Fer06].
**diffusing** [She01].
**digest** [MSP09].
**Digit** [KWP06, Tan07a, BG09, HKPR05, Kir01b].
**Digital** [ANS05, AvdH00, AR00, Ano01f, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00b, CCH05, CC09, Che01b, CFS01, CMB02, CMB +08, CZB +01, CGJ +02, DSP01, EIG01, Eng00, EHK +03, HSZ00, HSZ01, HS01b, HHGP +03, HW01, HLT01, JBR05, KZ01, Kal01, KC02, Kuh00, Kwo02, Kwo03b, LZL +01, LLL +01, Lin01a, LL01, Lut03, Mad00, MM01a, MM02, Meh01, PL01, PJH01, PCG01, PZL09, PB +07, Ram01, Rd01, RS01, Sam09, Sch00d, Sch06b, Scr01, Sha01e, SC02a, Shi08, SLT01, Sug01, TJC03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03, WC04, Wy02, XFL01, XYL09, YWWS09, YYDO01, YZZ01, ZWC02, Zho02, AAP07, AA08, Ano00i, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CJ05, Che07, Die00, FB01, GGGK03, GI07, HRL09, HLH00, HHC05, KP00, Lev01].
**digital** [LLC06b, MKY08, NR00, PC05b, PLJ05a, PBV08, QC05b, Sha01d, Sha05d, SCL05, TCC02, TND +09, UP05, WNQ06, WHLH03, XC05, XMST07, Ano09, 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].
**Direct** [BMW05, KG09].
**directional** [PJK01].
**Directions** [Sha01b, DFLH01].
**directly** [ZJCW05].
**Director** [Mad04].
**directories** [C +02, Pet03].
**directory** [C +02].
**disabled** [Pau02a].
**disadvantage** [CDS07].
**Disappear** [Per05].
**Disappearing** [Way02b, Way09].
**disappointing** [Ste00].
**Disaster** [WCZ05].
**disciplinary** [SM08].
**discipline** [JJ07, Swi05].
**Discovery** [Bi09, HLL +02, SBB07, SGA07].
**Discr** [CS03a, CNS02, Che04b, CCW02, Gen00b, GV05, GPP08, KC09b, LW02, JLR05, VK07, HN04, HW03a, HWR09, Hsu05a, HL05d, JL03, JLL01, LHL03a, LHY05, LTH05, PLJ05a, QC05b, Sch01e, Sha05c, Sha05d, SWRO5, SCL05, SL05, SCS05c, Yas08].
**discretized** [MA02].
**Discryption** [Har07b].
**discursive** [Mit02].
**Discussion** [Ano01a, Ano01b, Ano01c, Ano01d, Ano01e, Ano01f, Ano01g, Ano01h, KL+02a, Mal02, Nik02b].
**Dishonest** [GKK07].
**disjoint** [Gut04c].
**Disk** [Cro01, Har07b, Siv06, CS08a, Fer06].
**dismantles** [Hil06].
**dispatches** [Kee05].
**displayed** [CGV09].
**Displays** [Kuh02a].
**Disputed** [CAC06].
**Distance** [BDF +01a, BOHL +05, BBD +02, BSN000, FS01b, In02a, In02b, Ku02, LLL02, NA07, Sch01a, YL01, ATS04, Bad07, CYH04, GL06b, MP08, SLP07, Shp01, Shp04b, WHHT08, YS04, ZLG01].
**Distributions** [CY08].
**Diversity** [Kun01].
**Divide** [SKQ01].
**division** [VW01].
**Divisive** [BMW05, KG09].
**Division** [Ber05].
**divorced** [JHS02].
**divorce** [JHS02].
**distinguish** [HWW04, WH02b].
**Distinguishing** [HSR +01].
**Distributed** [BG01, CS05c].
**Distortion-Free** [BG01].
**Distortions** [HH09, SDF01].
**Distributed** [BC02, BT02, CL01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJK03, GSL02, GTH02, LL06, SC01, WT02, And08, AFGH06, BDE06, CO09, FMY02, KKL09, LN04, LLW08a, MSP +08, PS08a, Raj06, WZ05, YB04].
**Distribution** [BDF +01a, BOHL +05, BB +02, BSN000, FS01b, In02a, In02b, Ku02, LLL02, NA07, Sch01a, YL01, ATS04, Bad07, CYH04, GL06b, MP08, SLP07, Shp01, Shp04b, WHHT08, YS04, ZLG01].
[Por06, CCCY01, DY09a]. Enabling [Web02]. encapsulation [CHH+09, KG09]. Encipher [BR00a]. Enciphering [HR03, KT01]. Encode [BR00a, BKN04, Ano08c].
Encipher-Then-Encipher [BR00a].
Encipher-then-Encrypt-and-MAC [BKN04]. encoded [WMS08]. Encoding [JT01b, RS00, Lin02].
Encrypt [BKN04, BTTF02, Dav01c, Pet05, Dav01b]. Encrypted [BBK03a, BGHP02, BGLS03, CD01b, Hug04, Lan04a, LH07, RMCG01, Sta02b, Van01, WRW02, Whi09, Woo00, Ano06a, Bih02, BNP08, CCMT09, CDD+05, CSK+08, FJ04, HILM02, Hes04a, LSH00, MW04, Pet03, ÜG08].
Encrypting [Pro00, RC01, Zho06]. Encryption [ABC+05, Abe01, Abe04, AP09, AB01, ADR02, And03, Ano01f, Ano01g, Ano01h, Ase02, AFI06, AF03, Bar00c, II00, Bau02b, BN00a, BR00a, BMM00, BBDP01, BU02, BF01b, BF03, BB04, BGW05, BCHK07, BGH07, BPR+08, BB03, BNPW03, BD03, BKY02, Bur03, CD00a, CS03a, CHK03, CHK05, CGH01, Che01a, CTL01, Chi08, Cho08a, CMR06, Cla00a, Coc02b, Coc01b, CJN00, CH01b, CDN01, CS02, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DKF+03, DK05, DS05b, Dri02, FIP01a, FL01a, GC01a, GS000, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HSH+08a, HS02a, HY05a, HSH02, HSH06, HKR01, HW06, Har07b, Har00, Hei07, Her09, HS00, HR05, HG03, HL02, HGNP+03, HLL05]. Encryption [HLC08, ISSZ08, Joh03, Jol01, JK02b, JJ02b, JMV02, JKRW01, Jun01, KBD03, KSHY01, KS00a, KY01a, Kha05, KKJ+07, Kos01a, Kra01, Kur01, KD04, La07, Lan00a, Lan00b, LP03, LHT09, LY07, Lin03, LNP02, LMV05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, Mö03a, Mor05, Mü01a, MS09d, NIS00, Nam02, NZCG05, NZS05, NP02b, Nie02b, PV06b, PM00, Pau09, Pem01a, PZL09, PDM09, Pha04, Por01, PS00, Pre01, RM04, RK06, RDI+01, Sam01, Sch00b, SJ00, Siv06, SB00, SAC06, SRQL03, SPG06, SBZ02, Sye00, TV03, Uni00a, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Ust01b, VMSV05, WZW05, WBRF00, Wri01, YEP+06, YW06, ASW00, Abd01, AHS09, AKSX04, AMRP00, ABW09, Ano00e, Ano00c, Ano00f, Ano00g, Ano00h, Ano00j, Ano02a, Ano03c, Ano06d].
encryption [App05, Ate04, ACdM05, AFGH06, BPS08, BKN04, BR04, BB04, BBK+03b, Bir07, Blao0, BJ00, Bao0, BNP08, CCMT09, CDD+05, CSK+08, FJ04, HILM02, Hes04a, LSH00, MW04, Pet03, ÜG08].
Encrypting [Pro00, RC01, Zho06]. Encryption [ABC+05, Abe01, Abe04, AP09, AB01, ADR02, And03, Ano01f, Ano01g, Ano01h, Ase02, ANR01, AFI06, AF03, Bar00c, II00, Bau02b, BN00a, BR00a, BMM00, BBDD01, BU02, BF01b, BF03, BB04, BGW05, BCHK07, BGH07, BPR+08, BB03, BNPW03, BD03, BKY02, Bur03, CD00a, CS03a, CHK03, CHK05, CGH01, Che01a, CTL01, Chi08, Cho08a, CMR06, Cla00a, Coc02b, Coc01b, CJN00, CH01b, CDN01, CS02, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DKF+03, DK05, DS05b, Dri02, FIP01a, FL01a, GC01a, GS000, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HSH+08a, HS02a, HY05a, HSH02, HSH06, HKR01, HW06, Har07b, Har00, Hei07, Her09, HS00, HR05, HG03, HL02, HGNP+03, HLL05].
encryption [SR00, SVEG09, Shp04b, Ste00, SP03, SWH+09, Tan01, TTT01, TOEO00, TM01, TLH05, Uni00b, UP05, VKS09, WG02, Wh00, WN95, WH02a, XY04, Yan02, YGZ05, YZEE09, YC07, ZLG01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CH008, CHJ+01a, RR04, Uni00e, Wue09, Jan00a]. encryption/cipher [HAuR04].
encryption/decryption [OS07].
Encryptor [LMP+01, TPS01, Ano00a].
ever [Fur05]. Everlasting [DR02d]. Every [TH01, DKK07, Win05c]. Everything [CTBA^+01]. Everywhere [Ber00]. Evidence [Ver01, Bro05a, HW03b].

Evolution [DF01, Ree01, SP02, Sin99, Sin00]. evolutionary [LMSV07]. Evolved [LMHCTR06]. Exact [Cor00b]. example [Nis03a].

Exchange [BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JL08, KOY01, KY03, MPS00, Mac01, MSJ02, Ngu05, VPG01, WC01a, WV01, ZWCV02, BBG^+02, BCP07, CLC08, CWJT01, GL06a, GMR05, HTJ08, KS05a, KOY09, LW04, LHC08, LSH00, MS03a, Mis08, YC09a, YPKL05, ZYW07, CPP04, CP07, ECM00b]. exchanging [KN08].

Exclusive [GRW06]. Executing [HILM02, LJ05a]. Execution [Coo02]. Exhaustive [Des00c]. Existing [MV01, BDET00]. Expanded [Cho08a, Irw03]. Expanding [DN01, BCD06, HKPR05].

Expected [KL05, RK06, DLP^+09]. Experience [Sas07, BCHJ05]. Experiences [MPHD06, USE00a]. Experimental [BG09, CGBS01, OOP03, WS02, RSQ03, Sna04].

Experimentation [Hum05]. Experimenting [LSVS09]. experiments [Bru06]. expert [Ano01g]. Expiration [MP00, Sch05b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOBH05]. exploitation [Eri03, Eri08, KYN^+09]. Exploiting [CK06, ETMP05, HR00, HM04, ZWC02].

Exploits [MJF07, CSW05]. exploration [SKW^+07]. Exploratory [Lut03]. Exponent [BP04, BM01b, DN00b, May02, SZ01, CKY05, Dj08, GD05, Shp04b].

Exponential [BYJK04, BYJK08, CY08, GKK^+07, GKK^+09, Shp05]. Exponentiation [KKH03, SK07, CKRT08, HGNS03]. Exponents [FS02, FS01b]. export [Ano00b]. Exposed [Gum04, MK03, SSS06]. exposing [YY04].

Expositive [MAaT05]. Exposure [BM03b, DSS01, KZ07, CDD^+05, KZ03]. Exposure-Resilient [DSS01, KZ07, KZ03]. expressions [MW04]. Extended [ABDS01, BPS00, CM00, Cou04, DIRR05, HL08, HJW01, J00, MSJ02, MP02, OST05, W02, BJN00, CD00a, HT04, HP01, Mis06, Pei09, QPV05, LJK01]. Extending [ADD06, IKNP03, Ove06, S03b, SS01a].

Extension [Bai01a, YWD08, BR06, CMD06]. Extensions [ABC^+05, BBGM08, CS07c, HM02b, R02a, W04]. Extracting [Cer04a]. Extraction [DG04^+04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lu02, Vad03, DW09, KZ03, Sha04a].

Extraordinary [Top02]. Extreme [Ano02d]. Extrusion [Bej06]. Eye [Sas07, CAC03]. Eye-Opening [CAC03].
[Fie09, Wei06, Wei00, Wei05]. Fit [CCM05].
Five [SW00a, MS02b, Rot02b, Rot03].
five-lecture [Rot02b, Rot03]. Fix [TEM*01].
Fixed [AR01, BCCN01, CKN00, LS01a, Shp04b, SP79].
Fixed-Length [AR01, CKN00].
Fixed-Pattern [BCCN01, LS01a].
Fixing [KZ07, KZ03].
FL [Des02, Jue04].
Flash [ST06, SGB01].
Flat [SV08a].
Flaws [Gra02a, SPMLS02, Vau02, SL05a].
Flexibility [LP02a].
Flexible [CMG+01, CLK01b, DGK+04, OT03a, Tsa01, BA06, KC05, LHY02, WWA01].
Floating [NS05c].
Floating-Point [NS05c].
Flow [BDNN02, ABEL05, FR08, ME08a, TWM*09].
Flows [ECM00a, AHS08, Cer04a, Lau08a].
Flying [Fox00].
FOCS [IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07].
FOKSTRAUT [BH00a].
Foo [Puz04, VGM04].
Food [MNT+00].
Fool [RW02].
Footsteps [Lav06].
force [Cur05, SGA07].
forces [AJ08].
Ford [Mar05a].
Forecast [RAi00].
Forecasting [WWL+02].
Forensic [PS08b, Cas02, Kor09]. forensically [ME08b].
Forensics [JBR05, CS04, CS08a, CDS07, MS09a, MKY08, MAC+03].
Forest [FBW01].
Forgery [CH01a, CMM00, LS01a, SLT01, HSW09].
Forgotten [Eag05, Kin01, OC03].
Form [AD09, CH07c, OS01, LKYL00, Mic01].
Formal [BGB09, Bel07b, BCHJ05, BCJ+06, CL05, DKS08, GOR02b, H03, Lan00d, Mea01, YWD08, ABHS09, JW01, Mea04, Pau01, SW02, ZLX99, ZL04b]. Formalizing [HM01a].
Formally [BJP02]. format [ISO05, RG05]. format-string [RG05].
Formation [RW03a, Luk01].
Formats [GIS05].
Former [Mad04].
Forms [JT01b, LLL04].
Formula [Kog02].
Formulae [CH07b, WPP05].
Formulas [BGN05].
Formulations [AHRH08].
Forum [CZB+01, CTBA+01, CNB+02, CMB+05].
forums [Hill06].
Forward [AR00, AFI06, BY03, CHK03, IR01, HCD08a, HCD08b, ZYW07].
Forward-Secure [AR00, AFI06, CHK03, IR01].
Forward-Security [BY03].
Forwarding [KCD07, Kra02a].
FOSS [Bol02].
Found [Bar00a].
Foundation [Lut03].
Foundations [DKK07, Gol01b, Gol01a, Gol04, IE00a, IE01a, IE02, IE03, IE04, IE05a, IE06, IE07, IE08, IE09b, Nie02d, Sal05d, Kat05b, Puc03].
Founder [Bar00a, Ano03e].
Four [LXM+05].
Four-Layer [LXM+05].
Fourier [Che07, DSP01, DNP07, KC09b, LPZ06, SP04].
Fourteenth [USE00c].
Fourth [ACM02, ACM05b, DFCW00].
FPGA [Ano02e, CC02a, CGBS01, C03, CNPQ03, EYCP00, EHK04, KMM+06, KY09, KMB09, KRS+02, LP02a, MM01b, MM01c, OTIT01, OOP03, Pat01, PBTW07, QSR+02, TLYL02, TPS01, US02, WW00].
FPGAAs [AD07, DPR01, MMT09, RSQ03, SGM09, SK05a].
Fractal [AA04a, JLS03, WC03].
Fraction [Wal03].
fractional [DSP01, SSST06].
fractions [Dan02].
Fragile [CC09, CH01b, CT09, Nak01, PJK01, LYGL07, SY01b].
Frame [LHS05].
Frames [HHW05].
Framework [ANRS01, GL03, GOR02b, Hun05, NMO05, NP07, PS06, RS00, Shy02, ZYN08, AHKO3b, CCCY01, CP07, CC04e, DMSW09, GJ05, GL06a, GM04, JEZ04, KNS05, MS09b, MBS04, YCW+08, HF00].
France [ACM04a, ACM05a, AJ01a, AJ01b, GH05, KN01, NP02a, PPV96, KM07].
Francisco [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b].
FranzSteiner [Eag05].
fraud [Ano03a].
Fred [Bar00b].
Free [AP09, Ano02e, Bau01b, Bau01b, BG08, C01a, CVN06, DG02, HS00, HM01b, JP03, Jut01, Fox00, KS06b, SBG05, Bol02].
FreeBSD [Coc01a, Mur02, Si06].
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, HL05b, SZS05, WLT05a].

**FrontPage** [WWL02]. FSE [Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d]. FTC [Ste05c].

**fuels** [Mad04].

**Full** [Cor00b, DOP05, LKHL09, LKH08, Oiw09]. full-encryption [HS02b].

**Full-Round** [LKHL09, LKH08]. Fully [BL08, FS01a, Gen09b, KPMF02, RG09, Gen09a].

**Function** [BR502, CDMP05, Fis01b, Fl02b, GIS05, HNO09, HPC02, J000a, K0101, Kil01b, Nie02c, RB01, Yan05, CHY05b, CJ04, HR07, LW04, LPM05, WWT08, YW05, YRY05b].

**Functional** [ECM00a, WA06].

**Functionalities** [PS05]. functionality [ETMP05]. Functions [AEMR09, BBDK00, Bon01, Can01b, CV02, Car02, Che01c, DN02a, DGN03, DNR03, FL02, FIPR05, GLG09, HMO04, HR04b, J0001, K0101, LT05, Lys02, PR01, RR08, SM00a, SM00b, S01a, Sho00a, Sho00b, Ver02, WP03, WFL04, Wer02, AGGM06, AGGM10, ALV02, CS09, GVC09, HRS08, ISO04, K007, LHH02, LKY04, MS02b, MS09c, Mic02a, Mic02b, NR04, PW08, QPV05, SM03a, Whi09, YRY04, ZW05a, RRS06].

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

**Funds** [Coc01a]. Further [JS05, LLL04a, LL05c, MP07, YRY05a].

**Fusion** [K09, TDTZ05, ZS05, BG09]. fusul [MAaT05].

**Future** [AS01, An002f, Joh00, LNP02, NF003, Sch00e, HP00, LPW06]. Fuzzing [SGA07].

fuzzy [HS02b, NC09]. fuzzy-based [NC09].

G [Coc03, For04, Was08a]. Gaitherburg
MV01, GT00, MP08, Sch01f, Sch01e,
XLMS06, CHJ+01a. Genetic [HSIR02,
LHMCETR00, CV05, SCS05a, WJP07].
Gennaro [Miy01].
Gennaro-Krawczyk-Rabin [Miy01].
gentle [RR03a]. Gentry [Hes04a]. Genus
[CY02, GHK+06, Wer03]. Geometric
[GTTC03, HH09, LL05a, LL05c, LJ05b,
SDF01, CJT+01]. Geometrical [LWS05].
geometry [PPV96, WW06]. George
[Gum04]. Georgia [Tee09a]. German
[Sch09, Ano04b, Lim02, Mor05, Sal00b,
Sal00a, Win05b]. Germany
[DRS05, Duw03, FLA+03, WK03, IEO01b].
Geschichte [Sch09]. Get
[Coc01a, WD01a, Cla00b]. gets [Bor00].
Getting [PM00]. GF
[BIN03, KPM02, KLY02, KKY02]. GH
[GHW01]. GHS [Hes04b]. giant [Lam07].
Gibson [Ove06]. Giesbrecht [CHH01].
Gigabit [CGBS01]. Gigabits [HT02].
Give [CNB+02]. Given [Wai03]. Giving
[Tee06, Wu01]. Global [Ahn08, LWS05,
Por06, Ano00b, BK00, Kee05, KB00].
Globus [MJD01]. GN [SC05b].
GN-authenticated [SC05b]. Ghana
[For04]. GNU [Coc01a]. GnuPG
[JKS02, Sti06b]. GNY [Tee06]. Go
[Bur06, CZB+01]. Goals [PHM03]. goes
[Pan07]. Gold [Boy01, For04, Tsa07].
Goldreich [Kat05b, Lee03b, Puc03, AC02].
Gong [GG01]. Good
[CBO1, Kid02, MP06, GG05b, vT01].
Goodness [CMB+05]. Goods [NZCG05].
Google [Con09, Law09b]. Googling
[Con09]. GOST [SK01a]. got [Car01].
Goubin [Sna03b]. Governance [TPM07].
Government [YY00, RM02, Lev01, LCS09].
Governments [Ano00g]. GPG
[Bau01a, Bau01b, Luc06]. GPS [CKQ03].
GPT [Ove06]. GQ [BP02]. graduate
[GV09]. Grafter [Pag03]. grain [Rhi03].
Grained [SS01b]. Grand [Syy02]. granted
[Ano00h]. Graph [CGFS09, HTT+03,
HM02b, VVS01, YK01, CTT07].
Graph-Based
[CGFS09, HM02b, CTT07]. graphical
[vTO08]. Graphics
[CK06, DNP07, MFS+09]. Graphs
[NNT05, Ust01b, WGL00]. Gravilenko
[Pru04]. Gray [FG01, Har05b].
Gray-Scal[e [FG01]. grayscale [YCL07].
greatest [Be07a]. Greece
[ACM01a, KGL04, SM07b]. greedy
[HKP05]. Green [TR09a, TR09b].
GREMLIN [Hfi01]. Grenoble [ACM05a].
grey [BDN00, SCS05a]. Grid
[ACM05a, MJ01, SEF+06, TLC06, ZBP05,
Cha07, CJK+04]. GridOne [YC09b]. Grids
[CTY09, MMPM09]. grip [Buh06]. Gröbner
[CCT08, FJ03, Fan09]. Group
[ANRS01, AAF01, ACJ00, BBO04, BCP01, BCP02a,
BCP02b, CD00c, CV01, CH01a,
HSH10, HSH10, HW04, Hug02, JP02b,
KY03, Kin02, LLI+01, MSU05, SOU02,
SWH05, Ste01, Tan07b, VMS05, Wer02,
AKR04, BCP07, CLO4b, CH04, CH05,
CWJ+01, CJ+04, Ch00b, ED03, He02,
Hen06a, HW02, KSM05, KPT04, KKKL09,
LL05, LLI04, LPM05, LWK05b, NS05b,
PQ03a, PQ06, RH03, SNW01, Sha05a,
TJ01a, Tse07, WLL00, WHT08, YLC+09,
YY05a, ZC04, ZX04]. group-by
[YLC+09].
Group-Oriented
[LZL+01, HW04]. CHC05, CWJ+01, LL06, TJO1a, WHT08].
Groups [BS02, CV03, CF02, Dc00,
GM02a, GST04, KM01a, KLC+00, LL01,
LP03, Lu02b, MN01, PHK+01, GR04,
HM00, LLY06, Pa03, Yi04]. GSM
[BBK03a, BD00a, Cha05b, Cin02].
Guadeloupe [Wri03]. Guanjiaatu
[Buc00a]. Guangzhou [LLT+04, Li05].
Guessing
[AGYS07, Bau05, Shi05, YS02, DLMM05].
Guest [KP03, Sak01, BK06b, MFS+09,
TP07, SJ09, SK08]. Guide
[Ano06c, BS01a, BS05, BCP+03, BP01b,
HM04, Poo03, Vac06, Wei04, And08,
Helps [DF01, Pri00]. Helsinki [Bur00].
Henseil [CNS02]. Her [Bud06]. Here [Bur06, Law05]. Hermite [Mic01]. heroes [OC03]. Herriot [Coc03]. Hersonissoes [ACM01a]. Hessenberg [SFC09].
Heterogeneous [BCS02, KHYM08, ZBLvB05].
Heterogenous [HCf01]. heuristic [SS03].
HFE [FJ03, CHH01, Fei06].
HFE-Cryptosystems [Fel06]. HIBE [CS07c]. Hidden [HGN03, KW03, LNS02, GMR05, Lm09, Shp05, FJ03, Sch09]. Hide [PH03, Shp05]. hide-and-seek [Shp05].
Hiding [BD03, CLT07, Cct03, DN02b, GA05, HNO+09, LHS05, LS08, MH05, MMMT09, VDKP05, WC03, HR07, JDJ01, KP00, RSP05, Way02b, Way09, YCL07].
Hierarchy [HC08]. Hierarchical [GS02b, HNLZ01, HL02, MN01, YLLH05, BD04b, Che07, JW06, KAM08, WC01b, hY08].
hierarchies [AFB05, Cer04a, HY03, WL05].
hierarchy [CMdV06, Hwa00, JA02].
Hierocrypt [OMSK01]. Hieroglyphs [Wri05].
High [ACM01b, Ano00d, Ano02d, ChLYL09, CW09, CJL06, CGJ*02, DSO5b, FZH05, Gro01, HNZ02, HV04, Int00, JKRW01, KMM*06, Ken02b, KB00, Kra05, KTO1, MMO1b, NFQ03, R07, SKK00, SOTD00, SM02, SGM09, SLG*05, TL07, Uni00c, W00, WCGP00, YKMY01, Zhe01, BVP*04, BZP05, BGL*03, Jen09, KCO09a, Uni00f, WWTH08, Zir07]. high-assurance [Jen09].
High-Bandwidth [CGJ*02].
High-Dynamic-Range [CW09]. High-End [SKKS00, WCGP00]. High-Performance [Kra05, NFQ03, BZP05].
High-Speed [An000d, An02d, Gro01, JKRW01, KMM*06, SOTD00, SM02, W00, YKMY01, RW07, BGL*03].
High-technology-crime [KB00].
High-Throughput [HV04]. Higher [CV02, KCP01, BF01a]. Highly [CV02].
hijacking [Ste05c]. Hill [Gum04, USE02a].
Hilton [KJR05]. HIPAA [AEV+07].
historic [Pet08]. Historical.
RE02, MWM01. History [BP03b, Ifr00, Pag03, Sal01a, Sin01b, CAC06, Top02, AJ08, Boo05, HSW09, Jan08b, KNS05, Na05, Nis03a, Pm06, R10, RH00, Wil01a, dLB07].
history-based [KNS05]. hit [Bo05].
HMAC [FIP02a, DGH*04, H09]. HMVQ [Kra05]. Hoare [dH08]. Hoax [CZB*01, CTBA*01]. hoc [BSS02, Cha05b, DHMR07, KH05, LHC08, LKZ*04, PCSM07, SLP07, TW07, WT02, ZC09]. Hold [PM00]. Holier [MYC01]. Holistic [RM02].
Homage [JP02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03].
Homegrown [Str02]. Homeland.
Man02, Mau05, RR03b. homogeneous [MF07, PS02a]. Homomorphic.
AS01a, Aki09, CNO01, DN03, HS00, Cho06, Gen09a, Gen09b. homomorphism.
CKN06]. homophonic [Sav04].
Honeynets [Dim07]. Hong [B+02, ZJ04, Cla00b]. honor [OC03]. hook [JEZ04]. hooks [GJJ05]. hop [NC09, ZSJN07]. hop-by-hop [ZSJN07].
Horizontal [Coc02b]. host [Shu06]. hostile [ABB*04]. Hosts [H601, S08]. Hot [IEE01b].
Hotel [USE01b, USE01a, USE02a]. HotOS [IEE01b]. HotOS-VIII [IEE01b]. hours [Fox00].
House [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Hsu [BCW05, HL05c]. HTML [CNB*02].
HTTP [Zhu00]. Huang [ZC05]. Huge [MSNH07, NNT05]. Hull [KMT01].
Human [Dre00, GL01, JW05, KOY01, Man08, MS02d]. Human-Memorable [KOY01].
Hundred [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Hunting [GJL06]. Hwang [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KCL03, LW05c, QCB05a, WL05, ZYR01].
Hwang-Rao [ZYM01]. HWWM [LKY05c].
HWWM-authenticated [LKY05c].
Hybrid [ADI09, KD04, LZ04, PK01, CJ03b,
Hyderabad [MS02c], Hype [Way02a], Hyper [DR02d, Lu02, PZL09], Hyper-chaotic [PZL09], Hyper-Encryption [DR02d, Lu02], Hyperelliptic [Ava03, CY02, CFA+06, HSS01, PWGP03, Ver02, Was08a, ZLK02, CMKT00, Wen03, Wol04, WPP05], hypotheses [KW00].

I-tracings [RE02], i.e. [NP02a, Wil99], IA [WWCW00], IA-64 [WWCW00], IACBC [JMV02], IBE [ABC+05], IBM [AV04, ADH+07, CGH+00b, Web08, Weh00], IBB [AV04, ADH+07, CGH+00b, Web08, Weh00], Ibn [MAaT04, MAaT05, MAaTxx, MAaT07], Ibn-Adlan [MAaTxx], Ibn-Al-Durahim [MAaTxx], iButton [HWH01], IC [BGL+03, PC00], ICBA [ZJ04], ICCMSE [SM07b], ICISC [Kim02, LL03, LL04c, PC05a, Won01, WK06], ICISC’99 [Son00], ICM [IEE09a, IEE09a], ICs [Bar00c], Id [JZ09, BRTM09, CCD07, CL07, CS07c, CL00, GS02b, GTY08, HC08, KLY03, KHL09, Ku02, LCS09, Sco04, SW05, SCL05, WBD01, WH02b, YLH05, ZK02, ZC04, ZC09], Ide [Ano02d], Idea [Cos03, RR03a, CTLL01, HTS02], Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b], Ideas [Gha07, Eri01], Identification [BP02, BLD09, Gar03a, GLC+04, KK02, Kir01b, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZC09], identifiers [MC04], Identifying [HBF09, LLS05b, ZYN08, DMS07], identities [Kwo02, Kwo03b], Identity [App05, BF01b, BF03, BB04, BCHK07, BGH07, BPR+08, Boy03, BRTM09, CL01a, CHM+02, Coc01b, DT03, GK04, Her06, Her07, HY01, HL02, KC02, LCD07, Mar08a, Mar08b, PCSM07, SMP+09, BM05, CG06, CIL05, GG08, KG09, LWZH05, RG09, Sa02, Sha03c, Wan04b, Win05a, YCW+08, ZY07], Identity-Based [BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, LCD07, Mar08a, Mar08b, App05, Her07, PCSM07, BM05, CG06, CIL05, KG09, LWZH05, Sa02, Sha03c, YCW+08, ZY07], IDSFM [TZDZ05], IDtrust2009 [SM09], IEEE [BS03, BCDH09, BC01, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, KM07, HSD+05, Hug04, Mis08, PH03, ZD06], IEM [RC05], IFIP [DKU05, DFS06, DFW00, ELvS01], II [Ban05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Hau03, Hau04, HK09, OC03, Res01a, Res01b, Sal00a, ZT03], III [Sch00a, Ano00d, Bau03b], IKE [CK02a, Kra03], I’ll [PLW07], Illinois ACM04b, Illusions [Koc02], illustrated [Lun09], Im [BGI+01, DOPS04, RR05], IMA [Pat03b, Sma05, Hon01], Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, CL07, CC09, GW01, KBD03, KCB09, LL05a, L01, LWS05, LY07, Lj05b, LSKC05, PZL09, RS00, SDFH00, SDF01, SSFC09, SYLC05, TTTZ01, TH01, TC01, UP05, VKS09, VK07, W02, WLT05, YZ09, AAP07, A00, CC02b, CH01, Che07, Che08a, KK09a, LCL08, Lin00a, LT04, LY07, LLC06b, MS09a, MB08, PBV08, S+03, mSgFtL05, TL02, Wan05, WMS08, YCYW07, YCL07, ZLZS07]. Image-Feature [GW01], image-identification [PBV08], Images [CTL04, CC08, CW09, DP00, FD01, LS08, PJH01, PBC05, RE02, WCI09, WC04, YW09, AAP07, AEdR05, BDN00, FWT05, HYY07, TCC02, TND+09], Imaginary [HJW01, HM00, Hb00], Imai [DDG+06, YG01a], Imbalanced [ZW07].
Immersive [Coc01a]. Immune [CZK05, PZ02b, YKLM02b, ZP01, YKLM03].

Immunization [HR05]. Impact [Ber03, HGNP +03, JKRW01, MMYH02, Wri00, CS08a]. Imperfect [CPS07, DOPS04]. Impersonation [BP02, Hsu05b]. implant [Fox00]. Implement [HQ05]. Implementation [AD07, AG01, Ase02, Ash03, ARC +01, BBD +02, CDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK +03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HHM01, JKS02, KMM +06, KMS01, KTT07, KRS +02, KV01, LPO2a, MKP09, MM01c, MNP01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBTW07, QSR +02, RDJ +01, SM01, Sha01e, SK05a, SRQ03, USS02, Vir03, WZ05, WW00, WOL01, XB01, Zee00, BI04, BBK +03, BI05b, CNP03, DKL +00a, GHdGS00, GBKP01, Hii00, HP01, Hut01, KY09, LL04b, LCX08, LB05, Rhi03, SM03a, SVDF07, Wol04, YW06, ZFK04]. Implementations [AL00b, BJ00, III00, CTTL01, CGBS01, EPP +07, GLG +02, MM01b, MP01a, RS01, WWCW00, ASK05, BFCZ08, BFGT08, BG07b, FR08, RAL07, RSQ03]. Implemented [TSS +03]. Implementing [Dwi04, K09, LM08, LDM04, MWS08, NDJ01, Pet03, Smi01a, SR06, C +02, CW02].

Implications [Kun01, LJ05a, MF01, Bjo05, Fri07]. Implies [KY01e]. Imply [Pie05]. Importance [Ano02b, KJ +01, TGD01]. Important [SM00a]. imposed [XLS06]. Impossibilities [CHL02]. Impossibility [AP05, BPR +08, Fis06, PQ06]. Impossible [BF00a, BF00b, CKK +02, HSM +02, MHL +02, Pha04, SKU +00, SK01]. improve [Pau02a, CAC06]. Improve-ment [CAC06]. Improved [AFGH06, BPR05, BB05, BF00b, CL01b, CKK +02, C304, DN00a, DG02, Fan03, FKS +00, FKL +01b, FKL +01a, GMR08, Gen00b, HCK09, HKA +05, JQYY01, Kin00, KT06, Ku02, Küh02b, LW04, LL06, Mic02b, Miy01, M04, K03, MS02e, PR08, ST01b, SWH05, SC05c, TN00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].

Improvement [AS01c, AJ08, Che04a, CZK05, CCW02, Di 01, HWWM03, HWW03, Ha05, LKY05c, LKY05d, LTH05, MNT +00, NP07, Sha04b, Sha05b, WHL03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JSW05, Jmu05, Jmu06, Jmu07, KY05, LL04a, LW05c, SLS05, TO01, WLT05a, YW04, YWC05, YRY05a, ZC09]. Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, RSQ03]. Improving [ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SK01, SB01, Sun02, XQ07, YEP +06, YGZ05]. incentives [Swi05]. Incident [JBR05, Tom06]. Including [SR01].

Incomputable [Ver06b]. inconsistencies [MS09a]. Incorporating [MFS +09]. incorrectness [CHC04]. Increase [PBTW07]. Increasing [CS05c]. Incremental [BKY02, LKLK05]. IND-CCA [Mi01b]. IND-CCA2 [BST02]. Independence [BP03b]. Independent [BS00a, BSL02, Kin02]. Index [An00b, An01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, An03c]. Indies [Fra01, Syv02, Wri03]. individual [TW07].

INDCRYPT [CV04, JM03, MMV06, MS02c, RD01, Roy00a]. Induced [Vau02]. Industrial [USE00b]. Industry [ANS05, Mad00, Ort00]. ineffectiveness [YLR05]. Infeasibility [FS08]. Inference [Mar02b, CDD +05]. Infinite [TZT09a, TZT09b, Vau01]. Influencing [Bla01c]. Inform [Kwo03b, San05].

Information [AP09, BW07, BIM00, BZ02, Big08, BB03,
Information-flow [FR08].
Information-Theoretic [VDKP05, vW01].
Information-Theoretically [DM00b].
Infrastructure [AHKM02, AL06, BC04b, BWE00, CL07, ES00a, FL01b, KGL04, Sin01a, BHM03, BDS09a, Ben01a, CZ05, FB01, Gor05, LCK04, MWS08, Ben02].
Infrastructures [HCDO02, Lin00b, PHM03, WBD01, Bra01a, LAPS08, SN07].
INIDP04 [LDM04]. initial [DK08]. Initiative [Coc01a, Cal00b]. initiatives [Mau05].
injection [MMJ05, ZSJN07]. Injectable [CmVe06, Kos01c]. Innovation [Sam09].
innovations [Web02]. Innovative [MM07a].
Innsbruck [Pfi01]. Input [CAC06, TC00, DKL09, VM03].
Input-trees [TC00]. Insecure [Vau05b, Wal01, BJN00]. Insecurity [Bla02b, DOP05, Lai08, Man02, NS01b].
insertion [MB08]. insertion-extraction [MB08]. Insider [CMS09, Tad02, KS05a, Mah04].
Insights [Kun01]. Inspired [CC09]. Installation [USE00a]. instance [FS08]. Instances [GG01, HN06]. Instant [BBK03a, RR05].
Instantiated [RR08]. Instantiation [BF05]. Instruction [BBGM08, EP05, KTT07, Bru06, HTW07, MMJ05].
Instruction-Level [EP05]. Instruction-Set [BBGM08]. Instructions [LSY01]. instrumentation [MPPM09].
isubvertible [ACdM05]. Insulated [DKXY02]. Integer [Gro03, JL03, MN14].
Integers [CH07c, GMP01a, KKKM01, EKRMA01].
Integral [KW02, WH09]. Integrated [ECM00a, ECM00b, GMG00, Lut03, GLC+04, LK01, SSM+08, SN04].
Integrating [Wit01]. Integration [Ito00, CJL06, Sug03]. Integrity [Ano02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel [Coc02a, MP00]. Intellectual [Qu01, WY02].
Intelligence [App04b, AJ08]. Intelligent [Cos03]. Inter [WRW02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WRW02].
interaction [Gav08]. Interactions [Fau09].
Interactive [DG00, MS09c, DDO01, Fis01b, Fis05, HNZI02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00, MS09c].
Interception [CHVV03]. interdomain [MABI06, vOWK07]. interesting [SWR05].
Interface [RSA01]. Interference [FGM00a, FGM00b, GA05, BR05].
Interlaken [CC04a]. Interleaved [ZSJN07, NC09]. intermediaries [JA02].
Internal [Har07b, Bej06]. International [ACM03a, ACM04a, ACM05a, ACM09, ACM10, Ano00d, AAC+01, A101b, BDZ04, Bel00, B+02, BBB09, BS01b, Bi03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCM02, CCM05, CSY09, CGP03, Cra05a, DR02c, Des02, DKU05, DFPS06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JYZ04, Jef08, Jih03, JM03, JQ04, Je04, KKP02, KCR04, KJR05, Kli01a, Kim01, Kim02, KN03, Kn02, KP01, KNP01, Lai03, LL03, Lee04b, LST+05, LL04c, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pfi01, Pre00, PT06, RD01, 39
International [YDKM06, ZJ04, Zhe02b, ZYH03, AMW07, Ano00e, AJ01a, BCKK05, Bir07, BC05b, CKL05, DV05, DWS05, GKS05, HH04, HH05, HA00, Hon01, MAY09, PC05a, PY05, PPV96, QS00, Sma05, Son00, ST01d, WK06, Ytr06].

Internet [SMP+09, ABB+04, Ben01a, Ben02, Cal00a, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HK06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, PVs01, Pho01, PHM03, Rub01, SSB05, SEK01, SEK02, Sto01, Tsa01, TW05, WC05, WC05, ZGTG05, kc01]. Internet-wide [SBB05].

Interoperability [Hil00, TEM+01, BHM03].

Interoperable [BFGT08].

Interpolation [LW02, YG01b, FWTC05, KT06].

Interpolations [Sat06]. Interpretation [Mas04, CC04c]. interpretation-based [CC04c]. Intersections [KS06a]. Interstate [RM02]. Intranet [Jan00]. Intrinsic [ZWC02]. introduced [Ano00a].

Introducing [JL00]. Introduction [Ben02, Ber09b, Bis03a, BK06b, Buc00b, Buc01, Buc04, DK02, DK03, Fai07, Hay06, HPS08, HCS02, KLO8, MA007, Mol01, Neu04, PT07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGK08, TW02, TW05, TW06b, Big08, CS07a, CM05b, Gar01, HW98, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06a, Kat05b, Rot07, Lee03a].

Intrusion [CZK05, DFK+03, DP07, JT05, TZZ05, TMM05, WG05, HLL+02, MAC+03, NCRX04, NNO2, Ybf04, IR02].

Intrusion-Resilient [DFK+03, DP07, IR02]. intrusion-tolerant [Ybf04]. intrusions [Bej06]. invalid [CJT04]. Invariant [Ben00, CT09, HH09, ZLZS07]. Invariants [WH09]. Invasion [ASW+01]. invasions [Tyn05]. Invention [Ifr00]. Inventors [Bar00c]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, MFT05].

Inversion [BNPS02, KKY02, KTT07, SPG02]. Inversion/Division [KKY02]. inversive [SB05]. Investigating [BW07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08, WD01b, WC04]. Invitation [Bar02]. Invited [FGM00a, Lan00d, DRS05]. involutional [SHH07]. IP [Ano00a, CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSec [Vau02, CGBS01, Dav01a, KMM+06, SKW+07, FS00, FS03a, XLM06].

IPSec-Compliant [CGBS01]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFSHG09]. Irreversibility [ZWC02].

ISBN [And04, Duv03, Ead05, For04, Gum04, Ire03, Pag03, Puz04, Top02].


ISSAC [Jef08]. issue [FOP06, FOP06].

Issues [BDF+01a, BH00a, Hill00, KRV01, Mea01, PMB+07, SEF+06, MKY08, Pat02b].

ISW97 [You01]. IT-Architectures [RM02]. Italy [AAC+01, AL06, BCKK05, BC05b, CGP03, dCDSVG05, IEE04].

Itanium [CCH20, Int00]. Itanium-based [CCH20]. Iterated [Jou04, Oni01].

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

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

J2EE [BTTF02]. Jack [Coc03]. James [Top02]. jamming [LPV+09]. Jan
[YRY05b]. January
[Des02, GL05, Vau05a, Wri03]. Japan
[Ano00d, Mat02, Oka00, Coc02b, Smi01b]. Japanese
[IZ00]. Java
[Ano04b, Mar05a, WBL01, Ano02e, Ano03a, Ano04b, AJ01a, BCS02, Bis03a, BJvdB02, CMG+01, Che00, CCM05, Coc02, DPT’02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Lai08, LB00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, S 03, Vir03, Wei04, Win01, ZEA00, ZFK04]. Java-Based
[EM03, DPT’02, GW08]. Java-L¨osung
[Ano04b]. JAVA-Ring
[WBL01]. JavaCard
[AJ01a]. Javacards
[Cim02]. JavaScript
[TEM+01]. javax.crypto
[Win01]. JBits
[MP01a]. JCCM
[CMG+01]. Jean
[MFS+09]. Jeju
[CSY09, Lee04b]. Jeng
[QCB05b]. Jenness
[Sal03b]. John
[MYC01]. jobs
[Oue05]. Joel
[Gum04]. Johannes
[Lee03a]. Joint
[Bar00c, Con00]. Joint
[ADl09, ADR02, CR03, HY05b, HY05a, Puc03, MI09]. J¨org
[Fal07]. Jose
[Po06, Pre02c]. Joseph
[LBA00]. Journal
[LLLZ06a]. Journey
[FF01b]. Jr
[Kat05b]. Judiciary
[Uni00h]. July
[Chu02]. Julius
[ACM01a, CZ05]. Je08, KJR05, May09
[PVP96, Roy00b, Sch01c, S+03, Uni00a, Uni00b, Uni00e, Uni00d, ZJ04]. Jump
[MP00]. June
[ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BS03, BS01b, BCDH09, BC01, CZ05, FMA02, IEE05b, IKY05, JYZ04, KGL04, KN03, KM07, PVP96, TB02, USE01b, USE01a, USE02c]. Just
[ABB+04, Ano06a, Gut02a, Car01]. Kahn
[Gas01]. Kaikan
[Ano00d]. Kaspersky
[Ano08a]. KASUMI
[KYHC01, KSHY01, SM02]. Katholieke
[BBD09]. Katz
[Bar00a]. Keccak
[BDPV09]. Keep
[DM07b, Lys08, FS04]. Keeping
[SEK01, SEK02]. KEM
[NMO05]. Kerberos
[BCJ+06, Coc01a, Gar03b, Hi00, It00, LLW08a, MJD01, MPPM09, Rub00, Smi01a, Wac05, WD01a, Wri01]. Kerckhoffs
[KMZ03]. Kernel
[Int00, Mor03, BK05, HB06]. Key
[ANS05, ASW00, AK02a, Ano01j]. AAFG01, AEAQ05, AL06, AF03, AM00, BC05a, BPS08, BH06, BDG+01, BDZ04, Bar00a, BPS00, BPR00, BMM00, BBDP01, BY03, BOHL+05, Ben02, BL01, Bih00, BBB+02, BDK+09, BR00b, BM03b, BDTW01, BMM01, BM03c, BM02, BCP01, BCP02a, BCP02b, BM01c, BST02, C02a, CK02b, CHK03, CHK05, CPP04, C01a, CT08a, CHKO08, CCW02, CCM01, CM00, CS02, CS03b, CS03c, DPV04, DJ01, DPS05, Des00c, DBS01, Des02, DG03, DY09b, DKXY02, DFK+03, DHG+04, DBS+06, ESG+05, EP05, ES00a, FL06, FKSW00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Gol03, GH01, GC01b, GSB+04, Gut04b, HNZ02, HCD002, HL03, Hoe01, HR05, HG03, HC08, HJW01, HS07, HL08, IE00b, I00a2, Ina02b, JL08, Jon02, JG01, Jue04, KGL04, KOY01, KY03, Kat05b]. Key
[Ke05, Ke00, KKM01, KM01a, KLY02, KKY02, KY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, Ku02, KMM01, KY01e, KU01, I03, LCK01, LL02, LP03, LV00, Len01, Lin03, Lin00b, M005, Mac01, MSJ02, MHM+02, May04, MR01b, MR01c, M01a, M01b, M01c, M01d, M01e, Mur00, NIS03b, NA07, Nug05, N01b, N02, OT00, P00, PR01, P02, P03, R04, R05, R06, R07, R08, S007, T01, V007, Wal03, WZW05, WHI01, WC01a, WS00, WBD01, Wya02, YKM01, Y01, YG01c, YDKM06, Zhe02a, ZW02, ABH09, AJS08, AUW01, AKN04, AFB05, BHM03, Bad07, BBN+09, Ben01a, BB79, BG08, BBG+02.
BD00b, Bra01a, BCP07, BMA00a, BMA00b, BMA00c, BD04b, CCT08, CL02b, C205, CY05, CY05b, Che04a, CHC04, CY05.

key [CLC08, CKRT08, CWJT01, CJ04, Che06, CHI+09, CJI05, Cre00, DFM04, DMT07, DW09, EKRM01a, ED03, EHKK04, FMY02, FP00, GMLS02, Gal02, GL06a, GMR05, GKM00, GS01, GL06b, GMW01, HCD08a, HCD08b, HAU04, HHC06, HLLL03, HTJ08, HG05b, HWWM03, HMvdLM07, Hwa00, HLL04, IZ00, Iwa08, IM06, Jan08b, JRR09, JW06, JXW05, JZCW05, KY00, KS05a, KOY09, KHY08, KAM09, Kim01, KPT04, KRY05, Kob00, KW00, Kos01c, HKHL05, LHL03a, LF03, LKY03a, LKY03b, LCP04, LL04a, LW04, LLI05a, LKY05b, LKY05c, LKY05d, LLY06, LLS08, LCK04, LPM05, LHC08, LKJI01, LSH00, LSI01c, LCC05, Lop06, MWS08, MKK00, MP08, Mi08, Mi01b, NP02a, PS08a, PA06, Pei09, Pei04, PQ03a, PQ06, PC09, PSP08, PLJ05b, Pot06, Pri00, RH03, SN00, SLP07, SRJ01, SBZ04, Sha05c, Sh05.

dkey [SL05a, SW05, Shp04a, SC05b, SIR04, SLC05, Sun00b, Sun02, SZP02, SC05b, SC05c, SC05a, TP07, TO01, Tsa06, Tsa05, Tse07, VS01, Vau05a, VK08, WDN09, War00, WGL00, WV00, WC01b, Wu01, WL04b, WHHT08, XH05, YW05, YC09a, YS02, YSH03, YS04, hY08, Yj04, YR05a, YRY05b, YY05a, YPKL08, ZLG01, ZC04, ZK05, ZSM05, ZYW07, ABB°04, GL05].

Key-Based [Sha01e]. Key-Dependent [Gol03, BPS08]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKY02]. key-management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DP05]. Key-Share [CT08a]. Key-Sharing [HNZJ02, WBD01]. Keyboard [ZZT05]. Keyczar [Law09b]. keyed [Küh08, SR00, FIP02a]. Keyed-Hash [FIP02a]. keying [ABB°04, Che08a, EGK08]. Keyless [Qu01]. Keys [AOS02, APV05, AFI06, BT02, BMK00, BW05, CHM+02, EHMS00, Fer00, HSH°08a, Luke00, MN01, MRL°02, Oni01, P00, Sni01c, Str02, TvdKB+01, BCL05a, BCW05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH°08b, HSH°09, HW04, HY03, HL04, KAM08, LL00b, LS01c, LW05a, ML05, NN03, Sch01e, Sha04b, Sha05b, SB05, TLH05, TJC03, WH03, YRS°09]. Keystream [ÅM04, Kra02a, LV04, MH04, WL04, PS01a]. Keystroke [MR00, BGP02]. Keystrokes [SWT07].

Keyword [FIPR05]. KGK [HL08]. KG [ZY07]. KHAZAD [PQ03b]. KIASS [May09]. Kid [CAC06]. Kikai [Ano00d]. Kikai-Shinko-Kaikan [Ano00d]. kill [Lov01]. Killing [Lov01]. kind [DW01].

Kindi [MAaT03, MAaTxx]. Kind [Eag05].

Kingdom [DFCW00]. Kingston [HA00, PT06]. Kit [Ano02e]. Klaus [And04]. Kleptographic [YY01]. knapsack [Kos01c, SL05]. knapsacks [Mic02a].

Knife [Boy03]. Know [CMB°05, Ros07, Con09, DKK07, Win05c].

Knowing [CH01a]. Knowledge [Abe01, Abe04, AS01b, APV05, BP04, Cou01, DP04, DFS04, DDO°01, Eri02, Fis05, Gen04a, GK05, HNO°09, KS06b, LMS05, LHL°08, MR01b, XV03a, Pas05, Ros00, Ros06a, TG07, BSV08, CLR09, Dm00, Hro09, IKS07, 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].

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

Korea [CSY09, CK05, CR04, Kim01, Kim02, LL03, Lee04b, LL04c, May09, PC05a, PK03, Son00, Won01, WK06]. Korner [Mor03]. Kościszko [OC03]. Krawczyk [Miy01]. Kryptoanalyse [Mor05]. Kuala
Kunming [ZYH03]. Kurosawa [CHH+09]. Kurtz [Gum04]. Kyoto [Oka00].

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

Laboratory [Bru06, LBA00]. Lagrange [FWTC05]. Laid [Wei06, Wei05]. Lam [Wag00]. Lamar [LMHCTR06]. lamp [McN03]. LAN [Bar03, Pau03, SZ08, Sty04].

Lanczos [BF06a]. Landscape [Ahm07]. Language [ARC+01, DD02, Gou09, Jen09, MW04, WAF00].

Language-based [WAF00]. languages [Lun09, Rob02, Rob09].

Laptop [PGT07]. Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, GG01, Kuh00, PG05, SM01, ST03b, USE00a, BP03a, CKY05, C303b, Has00, HMvdLM07, HY03, PS08a, SM03a, TM06, WL05].

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

Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, GG01, Kuh00, PG05, SM01, ST03b, USE00a, BP03a, CKY05, C303b, Has00, HMvdLM07, HY03, PS08a, SM03a, TM06, WL05].

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

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

Latency [RSP05]. Lattice-based [Sync01c, Gou09, Gen09b, Mic02a, Reg05, Kuo09, Sip05, Si01].

Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HS01, HG07, IM06, Mic01, Reg03, Reg04].

Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HS01, HG07, IM06, Mic01, Reg03, Reg04].

Lattice-based [MR09, HS01, IM06, Reg04].

lattice-reduction [HG07]. Lattices [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Kuo09, Sip05, Si01].

Launched [Bar00b, An000]. Launches [An00d]. lava [Mc03].

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, ABH09, CK04, IY05].

Leakage-Resilient [DP08]. Learned [GSP+04]. Learning [KS06a, LY07, CAC06, BKW03, Ms06, Reg05, Reg09, SM08, Wh09].

Least [SZ01]. lecture [Rot02b, Rot03, Ad03, RSA03a, Riv03, Sha03b].

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

Left [Dhe03, HPKR05]. left-to-right [HPR05]. Legal [Coc02a]. Legislation [Eng00]. legislative [AvdH00]. legitimate [Lin01a].

Leighton [Rub00]. Leighton-Micali [Rub00]. Length [AR01, BR00b, CKN00, CHJ+01b, MS03a, RK06].

Length-Preserving [ML03a]. Leonard [Coc03].

Less [YKY01, BD00b]. Lessons [GBS+04, KFSS00].

Lester [RSP05]. Let [HSP+08a, HSP+08b, HSP+09]. Lets [Pau02a].

Letters [ASW+01, BTTF02, MNT+00, TEM+01, TvdKB+01, WML+02].

Leuven [BBD09, DR02c].

Legalisation [AVD00].

legislative [AvdH00].

Leigh [Gan01b, Sch00d, Swa01, Ste05c].

Life [Cop01a, CPG+04].

Lifeline [Coc01a, CPG+04].

Lifeline [Coc01a, CPG+04].

Lifting [CNS02].

Light [WT02].

Light-Weight [WT02].

Lightweight [EP0+07, MA02, CH07a, CL09, MP07].

Like [Coc02a, PSC+02, VMS05, BCDM00, CW00, DLP+09, Egh00, EBS01, Gun09, HSL+02, HL04, SKU+00, SLL+00].

LILLI [JJ02a].

LILLI-128 [JJ02a].

Limitations [Gua05, Fis01a]. Limited [AK02a, LCD07, Bul06, Tse07].

Limiting [CCR04b].

Limits [CWR09].

Lin [CC02b, CHY05a, KTC03, Y05b].

Line [Cho08a, DL98, Jan08, Lai07, Lu02, SK06, YLL02, Bau05, BCS02, DL07, Luk01, Shi05].

Linear [BDK02a, BDK02b, BDQ04].
Mean [Bar00c, KLML05, Ver06b]. Means [LMHCETR06, Nis03a]. measure [Lav09]. Measurement [Ano02e, kc01, CO09, FXAM04, RW07]. measurement-based [FXAM04]. Measures [CB01, QS01]. Measuring [Siv06]. Mechanising [Bel01]. Mechanism [LXM+05, CL08, GH08, LCP04, ME08b, WAF00]. Mechanisms [BACS02, CJK+04, Lin00a, MD04, Mir05]. mechanized [dH08]. Media [Hei07, Ano02d]. Median [Cap01]. Mediated [DT03, CG06]. mediator [SBG05], mediator-free [SBG05], medical [AL07]. Medicine [MYC01]. Meet [Cha00a, HG07]. meet-in-the-middle [HG07]. meeting [Jef08]. Meets [Way02a]. Melbourne [IZ00]. Member [CTH08]. Membership [NBD01, Fis01a]. Memoir [Bar05]. Memorable [KOY01]. Memoriam [DNRS03]. Memory [AK03, AJ008, CCM05, DK08, DGN03, HNZJ02, HBdJL01, KCJ+01, Oec03, OT03b, Oiw09, Pau02a, ST06, XNK+05, YGZ05]. Memory-Bound [DG03]. memory-safe [Oiw09]. Memoryless [Sar02]. MEMS [ECG+07]. MEMS-Assisted [ECG+07]. ment [CAC06]. menu [Mea04]. Mercy [Flu02a, Cro01]. Merkle [CDMP05, JLS03]. Mersenne [Ano03d]. Mesh [LP206, ZTP05, KB09, LZP+04, YPSZ01]. Mesches [BG08, Lav09]. Message [BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SNR04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, MD04, MS09c, Sha04b, TJ03, Wu01, ZF05, ZAX05]. Messages [Ara02, AR01, BR00b, CHJ+01b, DS05b, Sct09, Wri05, Zho06, Alv00, Ano08c, BCG+02, Birh02, BB79, Lm09, SP79]. messaging [Opp01, RR05]. meta [SM08, PLJ05a, QCBO5b, Sha05d]. Meta-He [PLJ05a, QCB05b, Sha05d]. meta-learning [SM08], metadata [CDS07, FJ04]. metamorphic [CSW05]. Metaphor [CBN+02]. Metering [BCO4b]. Method [BDTW01, GHK+06, GL00, Gro01, HRS02, HQ05, JKK+01, Măroiu, OKE02, OT03a, OT03b, SOHS01, TIGD01, TSO00, WH09, WNY09, ZL05, ARMP04, DwWmW05, Gut04c, JL03, MSP09, MFK+06, WGI02, WWT08, kWpLwW01, Wll04, YCO9b, YCL07, CHJ+01a]. Methodologies [SPM05]. Methodology [VMS05, HM02a]. Methods [BCDM00, FDO1, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Bau00, Bau02a, Bau07, BG04, BCIJ05, CM05b, GKS05, JZC05, LMSV07, Mal06, SSS07, Shp09, YW06]. Metric [LBZ01, LBGZ02]. Metrics [LBGZ01, LBGZ02]. Mexico [Buc00a]. MGC'05 [ACM05a]. Miami [Des02]. Micali [Rub00]. Michael [Ter08]. Micro [ASK07, Eng00, Ste05c]. Micro-Architectural [ASK07]. microcontrollers [GBK01]. Microelectronics [IEE09a]. Microprocessor [Web08]. Microprocessors [LKM+05]. Microscopic [MYC01]. Microsoft [Bon00, Scr01, Ste05b, Wh00]. Middle [Eag05, Gen04a, HG07, Kin01]. Middleware [ACM05a, KR01, LGS01, MBS04]. Migration [Pat02a]. Mikhailovsky [Puz04]. Milan [dCdV05]. military [Ark05]. Million [Ran55, Ran01, Ano03a]. MIME [Dav01b, Dav01c, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [FBW01, FGM001, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LPM05]. Mining [LP00, Lut03, HLL+02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [Co05c]. MinRank [Cou01]. Minutiae [UBEP09].
Minutiae-based [UBE09]. Misbehaving [JQY01, SBB05]. Misinformation
[CBF01]. Missed [TvdK09]. MIST [Wal03]. Mistakes [Ste05b]. MISTY
[KYHC01, Küh01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Küh02b].

Mithra [Fre03]. Mitigating [NLD08]. Mix [JJ00a]. Mixed [SKR02]. Mixes
[Möl03a]. Miyazaki [WHLH03]. MMM [GKS05]. MMM-ACNS [GKS05].

Mnemosyne [RH02, HR02]. Mobile [Chau05a, Dim07]. GN06, JP02a, KZ01, KB07, KCH01, LCK01, Mal02, MM02, PL01, RKZD02, Ri01, RC01, Rot01, SH00, ZYM05, CC05c, CJ03b, DHMR07, HP00, HYS03, ISTE08, KXD00, LC03, LC04a, Lin07, LKZ04, Par04, Pau02a, SSM08, SL05a, TM06, TW07, Tse07, Wan04a, YC09a].

mobile-commerce [YC09a]. mod [TM01]. Modal [GN01]. Mode
[BR02, Dwo03, HR03, HK01, KSHY01, SLG05, WB02, Hey03, RB03, ZL04c].
Model [Abe01, Abe04, BH05, BFK06, BR02, CJK01a, CPhX04, Ch08, CT09, DPV05, DFSS08, DLT00, Din05, ECM00a, Gra02b, HLC08, KLN06, KW03, JL05, MND04, MNFG02, MR01b, MR01c, MTS04, Pas03, SA02, Sal05b, Sar02, SDFD06, TZD05, Vad03, WC05, Wt02, WvD02, ZGLX05, ZP05, ZS05, BWD03, CUS08, Dan00, DFSS05, GMR08, HILM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SRJ01, TP07, DY09a]. Model-Based
[Sal05b]. Modeling [AADK05, CD05, HMvdLM07, KS05a, ZP05, La00, SS04].
modelled [BG08]. Modelling
[HCD02, JP07, Pu03]. Models
[Ben00, BBO0a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01a, SC02b, vOT08].
Modern [Gol09, Mao04, Pag03, SM07b, Swe08, Bud06, Fur01, IM06, KLO8, Mol05, SE01, Lut03, Lee03b]. Modes
[DGH04, Dwo03, GD02, Gol01d, HSH01, JM02, JKRW01, Jut01, KY01a]. Modified
[CHC04, HPC02, JY01, K101a, ST02, Che08a, CTO1, HW03, LL04a, LL05a, kWP0W01]. modifying [CSV07].

Modular [BIP05, BPK09, CM03, CH07c, Dhe03, FP00, Gro01, H06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wal01, WL04a, HST05]. Modulation
[AS01c, Che07]. Module [An00, LM00, SGM09, AR08, BG09, Jan08b]. Modules
[FIP01b, NIS01b, GJ05, JZ04, Se00b].

Moduli [Bai01b, BMP01b, Wal01]. Modulo
[BF01a, Küh02b]. Modulation [AS01c, Che07]. Module [An00, LM00, SGM09, AR08, BG09, Jan08b]. Modules
[FIP01b, NIS01b, GJ05, JZ04, Se00b].

Modular-Base [WY02]. Mollin [Kw05a]. MONA [KMS05]. Mondriaan [BF06a]. Money [An01a, YKM01]. monitor
[MK05a]. Monitored [PS05]. Monitoring
[AK02a, BCS02, Pol06, Be06, GXT08, ZGTG05]. Monitors [JT05]. Monks
[Eas05, Kin01]. monoalphabetic [GPG06]. monopoly
[GHdG00]. Monotones
[WW05]. Monte [Bi09, Sug03]. Monterey
[USE02c]. Montgomery
[CH07c, HKA05, NMS01, OS01, PS04a, TSO00, Wal01, WS03]. Montgomery-Form
[OS01]. Montpellier [KM07]. Montréal
[AC02]. Morocco [IEE09a]. MorphoSys
[Tan01]. MOSS [Dav01b], most
[GG05a, Shp02, Tyn05]. Mothballed
[Bar00c]. Motif [Bi09]. Motion
[EF05, hKLS00, WMR08]. Mountain
[JY04]. mouse [HLwZ09]. move [Jac00]. movement [HLwZ09]. MP [MP07]. MP3
[DL09]. MPEG
[LH05, LMC01, SG07, YZD07]. MPEG-4 [SG07]. MRF [Che01a]. MRM
[TIG01]. MSP03 [GBK01]. MSXML
[TEM01, Hei01]. Mu [CT03]. much
[Con09]. Multi
[ARR03, BFM00, BR06, CDB07, CJK04, CD00, CDG05, DLY08, DJL01, FG001, FWW04, Gen04a, HM01b, H07].
Multi-applications [DJLT01].

Multi-Authority [JLL02].

Multi-channel [ARR03].

Multi-designated [LV07].

Multi-Domain [CJK 04].

multi-factor [BSSM +07].

multi-hop [NC09].

multi-linear [LLL04].

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 [HWH05, HC04b, HL04, LCZ05b, LW05c, TYH04].

multi-stage [CHY05b].

Multi-trapdoor [Gen04a].

Multi-user

[BBM00, DLY08, GMLS02].

multi-valued

[DDZ01].

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, HL07, Sun05, WLLY09, DY09a, DKL05, La00, Ren09, SG07, YC08].

Multimodal [PY08].

Multi-party

[BGYO08, CDN01, DN03, DI05, GIKR02, OZL08, CDD00, HT04, IKOS07].

multipath

[SK05b].

Multiple [AIK +01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, DK05, Har00, HZSL05, HL01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJ04, DM07a, HLH00, KC09a, MN14, Sha01d, SW05, TCC02, YW05, YSH03, YRY05b].

multiple-key

[Che04a, CJ04, SW05, YW05, YSH03, YRY05b].

Multiple-Precision

[HZSL05, MN14].

Multiple-watermarking

[Che08b].

Multiples [HR00].

Multiplication

[AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02c, KKM01, Mo02, NMSK01, SO01, Tan07a, Wal01, BIN03, Dw05W05, FP00, GD05, Has00, Mis06].

Multiplications

[Har06, OT03b].

Multiplicative

[Has01a, KO03, MFFT05].

Multiplier

[HKA +05].

Multipliers

[CMJP03, KP06, RHM03b, WS05, HGS03, RMPJ08, RHM03a].

Multiply

[KTT07].

multiprocessor [ISTE08].

Multipurpose

[Boy03].

Multireceiver [HSZ01].

Multi-resolution

[hKLS00, YPS01].

Multiset [aSM01].

Multisignature

[Tad02, CWH00, CL04c, CCH04, He02, LC04b, LW05a, YW05, YZ04].

multisignatures [CL00, WH02b].

Multithreaded [Zha00].

Multivariable

[DS05a].

Multivariate

[DY09b, BG09, FP09].

Municipal

[MJF +08].

Music [MNS01, XMST07].

mutargima

[MAaT05].

Mutation

[Lut02].

Mutual

[JP02a, KH05, CC08, VK08].

Mutually

[WC01a].

MYCRYPT [DV05].

mysterious

[Bel07a].

Mystery

[Rug04, GG05a].

Myths [GO03, kc01].

N [Mar05a, AOS02, KOMM01].

NAF [OT03b].

Names

[Coc01a, Sha02, Ark05, CV09].

Naming

[An01b, BH00b].

Nanotechnology

[RR03a, RR03b].

Naor

[Zha06].

Napoleon

[Urb01].

narrowing

[MT07].

NASA

[An02c, Wil99].

Nation [Lan04a].

National

[BWE +00, Jol01, LCS09, AJ08, Bamb02].

National-Scale

[BWE +00].

Natural

[ARC +01, Top02, WMS08].

Nature [Pag03].
Naval [LBA00, Goo00]. Nazi [Hau06, KS04]. NC [AIK04]. nCipher [Ano03c, NCP [SQ01]. NCR [LBA00]. Near [BC04a, DPS05]. Near-Collisions [BC04a]. Necessary [LC03, MN01]. Necessity [SBZ02]. Nederlanden [dL00]. Need [Coc01a, HR04b, Sty04]. Needs [CZB +01, DKK07]. Negotiation [DBS +06, HHJS04, IY05, LLW05, LLW09]. Nema [Kid00]. NESSIE [Pre01, Mac00, Pre02a, Pre02b, SGB01, DPVR00]. nested [LCK04]. Net [CAC03, Ano08b, LKJL01]. Netherlands [Knu02]. Nets [AADK05]. Netspionage [BK00]. Network [Ano02d, Ano03b, Bar03, BGOY08, Con04, CLZ02, Dim07, FBWC02, Gum04, Har05a, IY05, JYZ04, KKK03, KPS02, Ken02b, LMP +01, Lu07, Mal02, NN02, PJDH09, Poo03, RCBL00, RC05, Sty04, TLYL04, VMC02, YC01, ZHY03, ZS05, Brn06, C303b, CMS08, Coc01a, DWML05, GKS05, HLL +02, LC03, LPV +09, ME08a, MSK03, Miš08, Pr00, RAL07, Sch00c, Sta02a, TIS07, Vac06, WyI05, YLT06, ECM00a, ECM00b].

Network-Attached [RCBL00]. network-based [HLL +02]. Networked [Sch00d, LB05]. Networking [ACM01b, Ros07, VM03]. Networks [AEAQ05, BJLS02, CGM07, DBS +06, Fin06, GPC08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL +08, NABG03, PR01, RKZD02, Sin01a, WT02, Zea00, ZYN08, ZWYC02, AJS08, BBG +02, BC05b, CCMT09, CGP03, CBD +05, DHMR07, ETMP05, HJ07, HMvdLM07, JRR09, KXTZ09, KHYM08, KB09, LDH06, LHC08, LW05a, Lin07, LN04, Lop06, LKZ +04, MWS08, MJF +08, MS09b, NC09, NLDO8, PCSM07, PSS08a, Pat02b, SLP07, SSM +08, TP07, TM06, TCR03, TW07, WDLN09, YC07, ZSJN07, ŽBLvB05, Ano02d, CS08b].

Neutral [KMS02, PZL09, PR01, YC01, YC07]. Neural-Network [YC01]. Neuve [QS00]. Nevada [ELvS01, 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, Pan02a, Pan02b, Pau03, Pau09, Pri00, CAC03, CAC06, Sta05, Ra06]. Newton [KT06]. Next [ESG +05, Mel06, TV03, Web08, BD04b, ISTE08, RR03a]. Next-Generation [ESG +05, Web08]. NFA [DIS02]. NFS [Sta02b]. Nice [DS06, JJ00c]. Nicko [Ano03c]. Nimbus [Fur02a, Mac00].

nine [Tat05]. Ninth [USE00d]. NIST [BG07a, Dra00, Hir09, Kel05, RRS06, SF07]. NIST-Recommended [Kel05]. NMAC [RR08]. NMAC/HMAC [RR08]. NNAF [DwWmW05].

No [Sta05, Sty04, UnI00g, Wei06, Wei05, CC05b]. Nobel [MNT +00]. Node [BRTM09, Fox00]. Nodes [ZYN08, RAL07]. NOEKEON [DPVR00]. Noise [BK03, GA05, MPSW05, SDMN06, MS09a, PC00]. noise-based [PC00]. Noise-tolerant [BK03]. noisy [HGN03]. Nominative [PL01].

Non [BR05, CHK05, CZB +01, DN00a, DDO +01, DW09, FF00, Fis01b, Fis05, FGM00a, FGM00b, HNZI02, HWJ01, IYK02, IYK03, JTO11, Kos01c, KO00, MSTS04, Nie02b, PHK +01, Pas05, SPK08, WBL01, DM07a, DS02, Hüh00, HLL04, IM06, KKL09, KHL09, LSA +07, PR05, RP00, SC05c].

Non-adjacent [JTO11]. Non-committing [DN00a, Nie02b]. Non-Cryptographic [WBL01, IYK02, IYK03]. Non-injective [Kos01c]. Non-interactive [CHK05, DDO +01, Fis01b, Fis05, HNZI02, HWJ01, MSTS04, Pas05, KKL09, KHL09]. Non-interference [BR05]. Non-malleable [DW09, FF00, PR05]. Non-maximal [HWJ01, Hüh00]. Non-OOSD [CZB +01]. non-perfect [DM07a]. non-physicists [RP00].

non-quantum [IM06]. non-repudiation [HLL04, LSA +07, 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, LBGZ01, LBGZ02, SM00a, ZC00, BGPGS05, CFVZ06, KH08]. Nonlinearity [SM00b]. Nonmalleable [ABW09, DDN00, DDN03, PR08]. nonrepudiable [TYH04, YTH04]. nonrepudiation [HW05, OZL08]. Nonsecurity [Sch07]. Nonuniform [CU01]. Normal [Ran55, Ran01, GPS05, Mic01, RMH03a]. Normalization [VK07]. Norway [Ytr06]. Nose [Fox00]. 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, CCS08, GB09, HG05a, SPG02, SC05a, mSgFtL05]. November [ACM01b, ACM05a, BZ02, CKL05, Eke02, IEE00a, IEE02, Lai03, LL03, LL04c, MS05b, PK03], novice [Dew08, Gou09]. Novo [Bi09]. NP [AGGM06, FS08, HN06, AGGM10]. NP-hardness [AGGM06, AGGM10]. NPCryptBench [YLT06]. NSA [RC05]. NSS [GJSS01, HP01]. NT [Str01b, USE00a]. NT/2000 [USE00a]. NTRU [GJSS01, GS02c, HPS01, HGHP+03, HGHP+03, HG07, JJO00b, NP02b]. NTRUEncrypt [HHG06, KY09]. NTRUSIGN [HHGP+03, HG06, HH08, ZJ09]. NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Die03, DGP07a, DGP07b, DV08, Eag05, EHK+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05, Ket06, KM01b, LMHETR06, LNS02, MNP01, NR04, RSN+01, SP05, Sch06b, Shp99, Shp03, SDFD06, TWNA08, TL07, TTZ09a, TTZ09b, Vav03, Wal00, Yan00, YKL02b, Aam03, AUW01, BK07, Bel08, BGPGS05, BG08, BG09, BG07a, BGL+03, CNP003, CO09, DIM08, DGP09, FP00, HG05a, HGN03, HLwWZ09, HP01, JAW+00, JL03, KH08, KSF00, Kin01, Lam01, Mit00, Nie02a, Nie04, Pan07, PSG+09, Psp+08, PC00, RGX06, Sh05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Wag03, Was08b, YZEE09]. Number-Notation [Eag05, Kin01]. Number-theoretic [NR04]. Numbers [HSR+01, HBF09, Fr00, MN01, ST03b, AG09, HG08, KB39, Kir01b, MFK+06, SS03, Shp05, Tip27]. numeric [AKSX04]. Numerical [WWL+02]. numerically [Sav04]. Numerous [CC08]. NurBS [Ben00]. NUSH [WF02]. NY [HR06, IK05, KJR05, Sch01d, YDKM06, NIS00]. Nyberg [Ara02]. O [Kat05b, Puc03]. OAEP [Man01, BF05, BF06b, Bon01, FOPS01, Sh01]. Obfuscated [NS05b]. Obfuscating [BG1+01]. obfuscation [CT02]. Object [RSA00e, DHL06, MWM01, ST06]. object-oriented [DHL06, MWM01]. Objects [CCM05, ZTP05, PB01, WHI09]. Oblivious [CT08b, Din01, FPR05, INP03, SDF01, GKM+00, KKL09]. obscurity [MN03]. Observability [JQYY01]. observers [JL04]. Obstacles [KM04a]. Obtaining [Bar06b, BP03b]. OCB [NB03]. occur [Web02]. Ocean [MYC01]. October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST+05, TTZ01, USE00b, ZY03]. Octopus [Cla00b]. Oded [Lee03b]. odyssey [Gol08]. Oedipus [Lav06]. Off [AJ08,
Origin [MABI06, MD04]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Orsay [DPT+02]. Ors [CRSP09]. Oscillator [BGL+03, GB09]. Oscillator-based [BGL+03]. Oscillators [SPG02]. Other [BF05, Ngu05, Wri05, Cla00b]. Otherworldly [MYC01]. Ottawa [AMW07, MZ04]. Our [Sta05]. Ourselves [Fur05]. Outbound [Smi02]. Output [Dic03, YJ00]. Outsource [HL05a]. Outsourced [MSP09, MNT06, YPPK09, YLC+09]. Overcoming [CHC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, Ino05]. Overhead [HGR07, IKOS08, RSP05]. Overheads [XLMS06]. Overlay [SL05b, YC08]. Overlays [SK05b]. Overshadow [CGL+08a, CGL+08b, CGL+08c]. Overview [SVEG09]. Ownership [AS01b, Nik02a, Nik02b, CL08, Lin01a].

P [Puc03, AKS02, KR03]. P1363 [IEE00b]. P2P [BRTM09, STY07, WN02, YLR05]. P2Ps [LHL+08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. Package [Win01]. Packet [BR09, WRW02, WLZZ05, CMS08]. Pad [LDM04, D502]. Padding [AR01, BCCN01, CKN00, CJNP02, KO03, LS01a, Man01, Vau02]. Paddings [NP02b]. PadLock [Luc05]. PadLock-wicked [Luc05]. Page [IEE00b]. PageRank [GPC08]. Pages [Fal07, Rot07]. Paging [SZ08]. Paillier [CGH01, DJ01, NSNK05, ST02]. Pair [WJC09]. Pairing [BKLS02, BF01b, BF03, CHS02, GPS06, HCD08a, HCD08b, Kir03, PV06a, SKG09, Sma03a, GPS05, Lee04a, PC05b, VAVY09]. Pairing-Based [BKLS02, GPS06, PV06a, HCD08a, HCD08b, GPS05]. Pairings [Bon07, BGH07, Jon02, SB04, ZK02, CJL05, LWZH05, LC05b, SW05, VK08]. Pairs [LYGL07, Shp01]. Pairwise [CLLLO0, FM02a, HMvdLM07]. PAKE [HT08]. Palm [BDhKB09, WPS01, Wli09, Ano02d]. Palmprint [KZ09]. PAM [FR02, Sei00b]. Panama [BDPV09]. Panel [FL01b]. Panoptic [YN01]. Paper [CC09, MFS+09]. Papers [Ano04a, MFS+04, Sch00b, Ytr06, Wli09, Bla03, Chr01, CMRR02]. CSY09, CGP03, DR02c, GH05, Joh03. Jue04, KKK02, KCR04, LL03, LL04c, MS05a, Mar02, MZ04, NH03, PK03, PT06, RM04, Sil01, AMW07, AJ01a, Bir07, BC05b, CZ05, CKL05, DRS05, HH04, HH05, PC05a, PY05, WK06, Wri03]. Paradigm [BN0a0, CS02, GL03, KDO4, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Paradise [USE00b]. Paradox [Che01b]. Parallel [AHR08, App07, AEMR09, CPhX04, CTL01, CNPQ03, CNB+02, Dan07, DM00b, JK08, KY02c, Lin01b, MFS+09, FP00, RM03b, SS01a, BF06a, FP00, OS07, RMP08]. parallelism [KVN+09]. Parallelizable [BR02, Mö02]. paralleling [Fis01a]. Parallelizable [LKKY03a, LKKY03b]. parameter [Wue09]. Parameterizable [KP01]. parameterization [LZP+04]. Parameters [ZLK02]. Parametric [Vir03]. Paranoid [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Sr05a, Luc06]. Parascript [Ano02d]. Parasitic [ETZ00]. Parents [Pan02a]. Parents-to-Be [Pan02a]. Paris [ACM04a, GHP05, KNP01, NP02a]. Parity [DRL09, KKG03, Yon01]. Park [Cop05, KKG03, DRL09]. Partial [Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05].
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, CLOS02, CLC08, CDM00, CDG+05, FGM001, FW04, GCKL08, HM01b, JW01, LLL04, LLS+09, LSH00, YC09a, ZLX99].

Pass [SK00, MT02]. passe [Car00]. Passes [Coc03]. Passing [Vir03]. Passive [Sha01c, VV07]. Passive-Only [VV07]. Password [BMN01, BMP00, CHVV03, CPP04, CS07b, DG03, GL03, GMR05, Har01a, Har01b, Jab01, KOY01, LSH03a, LSH03b, MPP00, Mac01, MSJ02, Ngu05, SBEW01, WHL05, YS04, ZWCV02, CC01, CC04b, CC04b, CYH05, Fur05, GL06a, HTJ08, JM07, KLY03, KJI05, KTC03, KCL03, Ku04, KCC05, KHKL05, LFW04, LC04a, Sco04, Shi05, YW04, YWC05, YS02, YPKL08, ZD06].

Password-Authenticated [BMP00, DG03, KOY01, MSJ02, Ngu05, HTJ08]. Password-Based [CPP04, CS07b, GL03, SBEW01, YS04, GL06a, KHKL05, ZD06].

password-guessing [Shi05]. Passwords [GL01, KOY01, Per03, Sni01c, Ano03c, FZ06, KOY09, NS05a, RD09, vOT08].

Patarin [Bih00]. Patent [MP00]. Path [GXT+08, CCD+04, Dev08, ZSN05].

path-based [CCD+04]. Path-quality [GXT+08].

Pattern [ABM08, BDik09, BL06, BCCN01, LS01a, TIGD01, Bu06, LYG07].

Pattern-based [BL06]. Patterns [DD02, MP06, WC09]. Pavol [Sal03b]. pay [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 [BDET00]. PDA [GW08]. PDF [ISO05, CNB+02, ISO05]. PDF/A [ISO05].

PDF/A-1 [ISO05]. Pearson [Puz04]. Pebbling [DNW05]. Pedersen [GJKR03]. Peer [HR02, RH02, ATS04, LLY06, MPHD06, PI06, WC05, Y04]. Peer-to-Peer [HR02, RH02, ATS04, MPHD06, PI06, WC05]. PeerAccess [WZB05]. Peinado [RYR05a]. PEM [Dav01b]. average-case [Mic02b]. cellular [SSM+08], cipher [Hau04]. Correction [SKQ01]. CPN [AADK05]. CRC [Kat05b, Was08a]. Data [BS00b]. Deblur [VHP01]. decryption [OS07]. Decryptor [TSP01]. Division [KKY02]. evolution [Pat02a]. Hardware [Nd05]. HMAC [R08]. IEC [ISO04]. image [Sch00a, Sch01c, Sch04a, Sch04b, Sch05a]. Memory [BS00b]. MOM [Dlt01].

multisignature [Wu01]. Offline [ST01b]. response [LW05a]. sec [KV01]. SGID [Tot00]. software [AR08]. TLS [BPST02, CHVV03, KPR03, OHB08].

UC-soundness [BPS08]. WG11.2 [ELvS01]. WG8.8 [DFCW00]. Penguin [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gu05, Oue05, Ste05a].

Pennsylvania [IEE05a, IEE08]. People [ASW+01, CG05, Lov01]. Perfectly [PBM+07]. Perceptually [EFY+05].

Perfect [AJO08, CLLL00, DN02b, DSS01, Sun00a, DM07a, SC02c, ZD05]. Perfectly [DMS00, KSR02, SNR04]. Perform [Kin00].

Performance [ACM01b, BH00a, DPR01, Dra00, EYCP00, FZH05, Int00, Ken02a, Ken02b, Kra05, LWK00, MM01b, NFQ03, PWGP03, PBTW07, SKKS00, SW00a, SB01, Siv06, SL00, SGPH08, WBRF00, WWCW00, WS02, XH03, YEP+06, Zea00, AKNRT04, BVP+04, BZP05, CKL+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTW07, YGZ05]. performance-friendly [CRSP09].
Permutation [DMS00, HSR+01, IYK02, KKG03, KO03, LSY01, DP02, IYK03].

Permutations [BPR+08, CHL02, KO00, MO03, KKKP05, WV00]. Persistent
[AGT01, ST06]. Person [KJR05, LLT+04, PK01, BS01b, KN03, Li05, LST+05, PY08].

Perspective [KKG03, KO03, LSY01, DP02, IYK03]. Place [USE01b, USE01a, GSS07b, IEE09a]. placement [GJJ05, JEZ04]. Plain [Co03]. Plaintext [DN02a, Furt02, GK05, HLM03, Jo01, Kel02, KM01c, MF01, CKN06].

Plaintexts [BR00a]. Plan [WCZ05]. plans [Ar05]. Platform [Bau02b, MMH02, PJDH09, ARJ08, ISE08].

Platforms [AIK+01]. Play [WD01a]. Playing [Shp05, BR04]. Please [Per03].

Pluggable [Sei00b]. plus [Cop04b]. PODS [ACM03c, ACM05b]. poetry [MAaT06].

pogromca [Kap05]. Point [GLV01, Mel02, NS05c, USE00b, WW06]. point-sampled [WW06]. Points [BG10, Gau02, Cla00b]. poised [CH00].

Poisoning [Kle07]. Poland [AUW01, Bih03]. Polarization [HR05].

Poles [KS04]. Policies [AEV+07, ZP05, BN08, LJ04, RN00a, RN00b]. Policy [Bl01c, HQ05, Ano00e, BFG08, BZP05, DF04, Gor05, RVS09, Uni00b, RR04].

policy-based [BF08]. policy-compliant [RVS09]. Polish [Kap05]. Politics [Cho08a, DL98, Jan08a, DL07].

polyalphabetic [GPG06]. Polygonal [Ben00, BB00a, BG08, SP04].

polymorphic [CSW05]. Polynomial [AF03, BIP05, BDG+01, Bu09, CU01, CJ03a, CH07c, CLZ02, DS05a, Gou06, HR00, KL05, KY01c, KTT07, LW02, May04, PI01, RMH03b, Sat06, LFW04, MRST06, SZP02].

Polynomial-Time
Polynomials [BLST01, DS08, FL06, Jam00, JJ00d, Lan04a, CHH01, FP09, GS09]. Pon [QCB05b]. Pool [BTTF02]. Popular [RR08, CAC06]. Port [Kra02b]. Portable [Hei07, Wan04a]. Portfolio [Ano02e]. Portland [ACM00, BCDH09]. Possessing [CC08]. Possession [Kra02b]. Possibility [Tee06]. Possible [Mur01]. Post [BBD09, BLRS09, Ber09b, HHG06, BD08]. Post-Quantum [BBD09, BLRS09, Ber09b, HHG06, BD08, BBD09]. postage [Ble07]. Poster [TSO00, RN00b]. Potential [Kid02]. Potentially [Wal01]. POTSHARDS [SGMV09]. Power [AKS06, Ano00d, Ava03, BI05b, BNPS02, Cry00, DV08, GB06, Has01b, HM02c, HBF09, IIT03, JP02a, JQY01, KBM09, KLY02, MOP06, Mas04, MIMM09, Mes00, Mes01, MG08, OS00, OS06, ÔÔP03, PSG+09, Sha01c, Sma03b, WS05, WCO1a, vW01, CBSU06, CO09, Geb04, Mit02, OS08, XH05, ZY07]. Power-Analysis [ÔÔP03]. power-attacks [Geb04]. Power-Sum [KLY02]. Power-Up [HBF09]. PP [Eag05, Pag03, Top02]. PPK [KOMM01]. PQCrypt [BD08]. Practical [Ano01c, AR01, Ash03, ACJT00, BDK+09, BF05, BLMS00, CS03a, Cap01, CD0R01, CS03b, DK01, Dre00, FS03b, GSS03, GIS05, GH02, HQR01, HJW01, Ina02a, Ina02b, IIT03, Kan01, LMV05, LCD07, Lut03, LWK05a, MM02, MSU05, OM09, PB00, Pel06, Po02, Poo03, Roy00b, Sug01, Wei04, YSS+01, Bro05b, DKL+00a, Har05a, KSW06, Luc06, Mos06, MSV04, Sha01a]. Practice [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti95, Sti02, Sti06c, Lut03, Spr03]. practices [Ste02]. practitioners [PP09]. pragmatic [BMW02b]. Prague [MJ04]. Pre [Adl03, AA08]. pre-processing [AA08]. Precise [Wal01]. Precision [HZSL05, SR06, LMC+03, MN14]. Precomputation [SLG+05]. predecryption [RSP05]. Predict [Dic03]. predictable [Be08]. Predicting [AG09, BPGS05]. Prediction [AKS06, SLG+05]. predictive [vOT08]. predistribution [HMvdLM07, JRR09, TP07]. Preface [CGM07]. Prefix [FXAM04, RW07]. Prefix-preserving [FXAM04, RW07]. Prehistory [Fr00]. Preliminary [KS00b, KKS00b]. Prentice [For04]. Prentice-Hall [For04]. Preparations [FJ04]. Prepared [ASW+01]. Preprocessing [BIM00, CKK03]. presence [BIW08, GXT+08, Mio08, VS08]. Preservation [Che01b, Dur01, Bro05a, ISO05]. Preserve [NNT05]. Preserving [DN04, KS05b, LP00, Mio03a, YWD08, AKS04, BR06, BSSM+07, BA06, FXAM04, GA03, HW05, LCK04, Pin02, Pin03, RW07, HJ07]. President [Gen00a]. Press [Ina03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03]. Pressure [HWH01]. pretty [vOWK07]. Prevent [FOBH05]. Preventing [CS07b, CCL09, HSW09, IY05, RG05, DMS07]. Prevention [JT05, PZ01, PZ02a]. Price [AS01a, Bra01b]. Primality [BT02, Che03]. Prime [ACS02, Bai01a, Har07a, Pau02a, WS03, JL03, dW02]. Prime-detecting [Har07a]. Primer [KL+02b, Lad06]. Primes [An03d, Dur01, HLLL03, Ste08, AKS02]. Primitive [CSFS05, IYK02, IMM01, ST01a, ST02, IYK03]. Primitives [BDFP02, CHL02, FMO01, Ng05, RR00, BDFP05, Gar05, JZCW05, RAL07]. principal [ZL04b]. Principle [CZK05]. Principals [ACM03c, ACM05b, DK02, DK07, KL08, MAA07, SB07, Sta02a, Sta06]. Print [Kra02b]. Printed [SLT01]. Printer
Privacy-Enabled [Por06].
privacy-enhanced [ZSM05].
Privacy-Enhancing [SE09].
Privacy-Preserving [DN04, KS05b, YWD08, BA06, HJW05, Pin02, Pin03].
Private [AF04a, AFI06, BDFP02, BY03, BSW09, BJLS02, BGW05, ISW03, KO00, OS05, SDMM06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PL05b, Sun02, YRS09, ZY08, ECM00a, ECM00b].
Private-Key [BY03, KY00, PLJ05b, Sun02].
prize [Fox00, Coc02b, MNT00].
PRNG [HSS04, Mur02, SF07].
Proactive [DBS01, FMY01, JS05, ZSV05].
Probabilistic [CCW02, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLM05, Go99, JWC05, KY00, MRST06, PBBM01, dH08, Neu04].
Probability [KMT01, MNT00, DLP09].
Probing [ISW03].
Problem [AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK02, Cou01, CLZ02, DIS02, DHR00, FL06, Gen03, GV05, GPP08, KK02, LNS02, NB01, Wag02, BKW03, CGH06, CJT04, DLM05, HN03, Hu05a, LHY05, LD01, Luk01, Pei09, SLP05, SL05, WL02, Whi09, Yas08, KM04a].
problem-solving [Whi09].
Problems [BB05a, Can06b, MV03a, OP01a, TVdKB01, VDKP05, HL05d, KXD00, LMT05, LMC03, RSS04].
Procedure [LY07].
Procedures [DJ06, BBK03b].
Proceedings [ACM00, ACM02, ACM04a, ACM05a, AAC01, Bon03, EBC00, FMA02, FLA03, SM07b, USE00c, USE00b, USE00a, USE00d, USE01b, USE01c, USE01a, USE02a, USE02c, USE02b, WKP03, Yun02a, ACM05c, ACM07, ACM08, ACM09, AUW01, AJ01b, BS03, Be00, B+02, Boy01, Bu00a, BC01, HA00, Hon01, IEEE00a, IEEE01a, IZ00, Ki01a, MS05b, Oka00, PPV06, Pi01, Pre00, Q000, RD01, Roy00a, SMP09, ST01d, VY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BDZ04, BS01b, Bih03, BCD09, BD08, CC04a, CV04, Crh00, Des02, DFP06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEEE02, IEEE03, IEEE04, IEEE05b, IEEE07, IEEE08, IEEE09b, JY04, Je08, JM03, Jo03b, JQ04, KJR05, KGL04, Kim01, Kim02, KN03, Knu02, KP01, KN01, KM07, Lai03, Lee04b, LIT04, MMV06, MJ04, May09, MS02c].
Proceedings [Men05, Nac01, N02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sma05, Syv02, TB02, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZH03, BCKK05, Cra05a, DV05, DWM05, DKU05, GKS05, IKY05, Ki05, Li05, LST05, Men07, Poi06, Sh05a, Son00, dCdV05].
Process [Kwo03b, MNT00, BDF02, HL06, MRST06, VKS09].
Processes [BDP02, ALV02, BDNN02, Whi09].
Processing [ISSZ08, KLB02, PCK02, AA08, AA04a, YPS01].
Processor [An02e, BBGM08, EP05, FBWC02, FZH05, GC01b, Int00, KBD03, KPM02, TLY02, ST03a, SHL07].
Processors [TLYL04, CW02, CRS09, Geb04, LJ05a, YZ05, YLT06, ZYL05].
Procurement [Lad06].
produce [Zir07].
producing [SOIG07].
product [KSWH00, Sun02].
Products [ACS02, An02d, An02e, Knu07, An00c].
GGH\textsuperscript{+}08, Kov03, KH03, CS08b].

Programmable
[Dam07, GC01a, HV04, Smi02).

Programmer
[Wil01b, Bon00, Che00, DKK07).

Programmers
[Coc01a, Wei04, Gou09).

Programming
[ASW\textsuperscript{+}01, Ano02d, Coc03, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJo1a, AJo1b, CW07, Nis03a, VM03).

Programs
[BGI\textsuperscript{+}01, Ark05, SLTB\textsuperscript{+}06).

Progress
[KK06, KFSS00, RD01, Roy00a, CV04, DV05, JM03, MMV06, MS02c).

Project
[Fri01, IY00, MNT\textsuperscript{+}00, Pau02a, Salxx, Gou09, LR01, Lov01, MWM01, Sha01a, Coc01a, Coc02b, IY00, Pre02b).

projects
[Gha07).

Prolog
[Bla01a, Bla01b).

Promise
[Ano02f).

promises
[Pau02a).

promote
[WK05).

Promotes
[Bar00b).

Prone
[MLC01).

Proof
[ABC\textsuperscript{+}05, BM01c, KY01b, LLL\textsuperscript{+}01, MS02a, NNT05, SM00a, BD04a, CDLO6, FMG03).

Property
[LPZ06, Qu01, Uni00b, WY02, BR06, JS09).

Proposal
[DPVR00, Mac00). Proposed
[Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDWO6). Protect
[ETZ00, BBN\textsuperscript{+}09, WK05) protected
[CYH05, PKH05, ZCL05). Protecting
[Des00c, EHMS00, KY01d, Kra01, LKM\textsuperscript{+}05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYL05].

Protection
[CGJ\textsuperscript{+}02, DKFX05, ECG\textsuperscript{+}07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL\textsuperscript{+}08a, CGL\textsuperscript{+}08b, CGL\textsuperscript{+}08c, CT02, Gor05, Kov03, KH03, Kw03a, LL05b].

Protection
[JT01a). Protocol
[Ano01a, Bel01, BPST02, BL02, CK02a, CJ03c, CWY05, Cym02, ECM00b, Fre03, GJKR03, GL00, HS07, JP02b, JRFH01, JT05, KLN\textsuperscript{+}06, Kaka06, Kra05, Ku02, LCK01, Mea01, MSU05, NIS01b, Rub00, RMCG01, SK00, Tan07b, TZT09a, TZT09b, WHL05, YSR01, BP03a, Bla01b, BDFP05, BK05, CS04, CCK04a, CC04b, CYY05, CC05c, CYH05, Che04a, CLC08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, GTZ04, HTJ08, HWWM03, HHC05, KH08, KKL09, KTC03, LC03, LF03, LKKY03a, LKKY03b, LW04, LHLO4, LK05, LK05c, LHC08, LSH03a, LC05b, Luk01, MS03a, Par04, Pau01, Shi05, SW05, SR04, TM06, Tsa06, Tse07, WK05, WLT05a, WHHT08, YW05, YTWH05, YC09a, YS02, YSH03, YRY05b, YRY05c, YPKL08, ZWRL01, ZL04c, ZDW06, ZYW07, LSH03b]).

Protocols
[AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Bor01, BM01b, BM03c, Bra01b, BLD09, CKPS01, CT08a, CMMR02, CMMR05, Cir01, CN06, DJ06, DF01, Fis01b, FGM00a, GMP01a, GIV01, Gor02a, J07, JW05, KS00a, KY03, KL08, Kra03, Ku02, MS02a, MNP01, PB00D, PR08, PJDH09, Rot01, Shy02, SC01, Tee06, AA04b, AKNR04, Bar06a, Bau05, Bel07b, BDSV08, BFGT08, BP05, BL06, BD04a, BR05, Can01a, Can06a, CP07, CRKT08, CWW07, CH07a, Cho08b, Chr00, Chr01, CJ00M, Coh03, CC05d, CD06L, DFG00, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LP0V09, LL04, LLY06, LLS09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SL05a, SR00, SW00b, YS04, ZLX09, ZL04b, PDMS09, Puc03].

ProtoMon
[JT05).

Provability
[GOR02b). Provably
[HM02b, HLL\textsuperscript{+}01, HSL\textsuperscript{+}02, KSH01,
Provability
[AO00, ACJT00, BMP00, BCP01, BCP07,
CHK08, DG03, HLvA02, HvAL09, HL07,
HS07, JMvM02, M¯øl03a, NSNK05, NSS02,
VMSV05, XS03, ZCL05, BKN04, CCMT09].
Provenance [HSW09].
Provers [MV03a].
Provide [AB01, Sch01a].
Providence [IEE07, Sil01].
Provider [LDM04, HILM02].
Provides [MV03b].
Providing [BACS02, BDS09a, DeL07, Lin07, Par04].
Proving [Che03, Sch01a].
Provision [Kha05].
Proxy [AH05, BCL05a, DKFX05, LCK03, LCZ05b,
PL01, RdS01, Sha03d, ZJ09, AFGH06,
CCH04, DY09a, HWW03, HW04, HW05,
HW05, HC04b, KHL09, LL05b, LH05,
LCZ05c, LW05c, PKH05, Sha05b, SHT05,
TY04, YTH04, ZCL05].
proxy-enabled [DY09a].
proxy-protected [PKH05, ZCL05].
pseudo- [BH05, FW05, Gen00b, LHL08, MP03, SXY01,
TTZ09a, TTZ09b, WP03, BG09, GB09, MFK06, NR04,
PSP08, RGX06, SL09, WW08, YZEE09].
Pseudo-Random
[LLL05, MP03, WP03, Gen00b, SXY01,
MFK06, NR04, RGX06, SL09, WW08].
Pseudo-Signatures [BH05].
Pseudo-signatures [FW04].
pseudonoise [HG05a]. pseudonym [CG06].
pseudoprimes [ZT03]. Pseudorandomness
[GM02c, IK00, IK01, KYHC01, LHL01,
Lee03b, MV00, Shp03, Gol99]. Psychology
[MYC01]. PUD [Nat00]. Public [ANS05,
AUW01, APV05, An01j, AEQ05, AF03,
BC05a, BDG01, BDZ04, Bar00c, BPS00,
BBM00, BBDP01, BLM01, Bii00, BDTW01,
BST02, CHK03, CHK05, CDM05,
CHM02, CHK08, CCW02, CT09, CCM01,
CS02, CS03b, DPV04, DJ01, Des02, DY09b,
DKXY02, DFK03, ESG05, ES00a, ED03,
FL06, FL01b, GMLS02, GH01, GC01b,
GSB04, Gut04b, HCD002, HR05, HG05b,
HR04b, HJW01, HLC08, IEE00b, IZ00,
Jou02, Kat05b, KKM01, KM01a, Kim01,
KLY02, KKY02, KYY02c, KLC00, Ki01b,
KM04b, Kos01a, Kos01b, KOM01, KY01e,
Kur01, LLL02, LP03, LV00, Len01, LPZ06,
Lin03, Lin00b, MR01b, MR01c, Møl03a,
Mol03b, Møl01a, NP02a, NBD01, NSS02,
OTU00, PHK01, Pei09, PR01, Poi02,
PHM03, Qu01, RSA00a, RKZ02, ST01a,
ST02, Sin01a, Sni01c, Ste01, TS000, TT01,
Vau05a, WZW05, WH01].
Public
[WV00, Wyat02, YKMY01, YG01c,
YDMK06, Zhe02a, AG09, BHM03, BCL05a,
BC05, BBN09, Ben01a, BB79, Bra01a,
BD04b, Cal00b, CCT08, CL02b, CWH00,
CCH05, CJ05, CKRT08, Ch06, Cre00,
DMT07, EKRMA01, EHKH04, FMY02,
FP00, Gau02, GH08, GKM00, GS01, Gor05,
GMW01, HCD08a, HCD08b, HH06, HW04,
LL04, Iwa08, IM06, Jan08b, JXW05,
JZCW05, KPS02, Kob00, KW00, Kos01c,
LF03, LKY05b, LCK04, LIW08b, LS01c,
Lop06, LWK05a, MWS08, Møl01b, PIP06,
PC09, SNIO0, SRJ01, Sh04b, Sha05b,
Shp04a, SL05, Sun00b, SZP02, SC05c,
TO01, TLH05, Tsa05, TJ03, VS01,
WDLN09, War00, Wa01, WH03, WL04b,
Hy08, YRS09, ZSM05, AL06, BDZ04,
Ben02, CZ05, Des02, GL05, KL04, Kim01,
NP02a, Vau05a, YDMK06].
Public-Key
[An01j, AEQ05, BC05a, BMM00,
BBDP01, BLM01, BST02, CHK03, CHK05,
CCM01, CS02, CS03b, DPV04, DJ01,
DKXY02, DFK03, ESG05, ES00a, ED03,
FL06, FL01b, GMLS02, GH01, GC01b,
GSB04, Gut04b, HCD002, HR05, HG05b,
HR04b, HJW01, HLC08, IEE00b, IZ00,
Jou02, Kat05b, KKM01, KM01a, Kim01,
KLY02, KKY02, KYY02c, KLC00, Ki01b,
KM04b, Kos01a, Kos01b, KOM01, KY01e,
Kur01, LLL02, LP03, LV00, Len01, LPZ06,
Lin03, Lin00b, MR01b, MR01c, Møl03a,
Mol03b, Møl01a, NP02a, NBD01, NSS02,
OTU00, PHK01, Pei09, PR01, Poi02,
PHM03, Qu01, RSA00a, RKZ02, ST01a,
ST02, Sin01a, Sni01c, Ste01, TS000, TT01,
Vau05a, WZW05, WH01].
TS000, TT01, WHI01, YDKM06, AUW01, ED03, HG05b, Pei09, BHM03, BBN+09, BD04b, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HG06, Iwa08, Jan08b, JXW05, JZCW05, Kos01c, LF03, LS01c, Lop06, MWS08, Müll01b, SNI00, Shp04a, SLC05, Sun00b, TO01, ZSM05, GL05].

Public-Key-Based [YKMY01].
Publication [Top02, DGMS03].
Publications [Bee05].
Published [MS03b].
Publishing [Ano02d].
puce [Car00].
PUFs [MKP09].
Purpose [Ano07b, Ano07a, ESG05, GS07a, GPP08, SGK08, LJ05a].
Purposes [LS05a, FSGV01, PBV08].
Push [Pau03].
puzzle [LF03].
PUFs [MKP09].

Quantifier [KS06b].
Quantifier-free [KS06b].
Quantitative [Bai08, ME08a].
Quantization [DRL09, WC04].
Quantum [AC02, ATSVY00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL+05, BBD09, BJ02, BB+02, BB03, BLMS00, BXM+07, Coc03, DFP04, DFP05, DFS08, DMS00, EII04, Ett02, GKK+09, GH02, GW00, GRTZ02, HV09, Hay06, Im03, Ina02a, Ina02b, Kak06, KK06, KLB+02b, LB04, LW05b, NA07, OTU00, PC09, Re01, RK05, Ser06, SR07, TO01, Wi199, Wri00, Y100, Y101, ZLQ01, ABW09, Ano03c, Ano06d, BYJK04, BCG+02, Ber09b, BEZ00, BEZ01, BLRS09, DFSS05, Duw03, Eke02, GKK+07, Gav08, HHG06, IM06, JZ09, JRS09, JAW+00, Joy00, K07, KH08, KKKP05, LQ08, May01, NK06, Pn06, RP00, Sin99, Sin00, Smo04, UHA+09, BZ02, BD08, BB09].
quantum-storage [DFSS05].

quarter [Kob00].
quarter-century [Kob00].
quartz [Ano00b].
QUARTZ [PCG01].
Quasi [MD05].
Quasi-Pipelined [MD05].
Quasigroup [MSN07].
Québec [ACM02].
Queen [Ree01, Sin99].
Queenstown [Zhe02b].
queries [CKK03, Fis01a, GPC08].
Query [GA03, PT08, PCK02, BKW03, PM08, YLC+09].
Query-preserving [GA03].
quoting [FJ04, UG08].
question [OC03].
Questions [Ett02, Joh00, Jac00].
Queues [WWL+02].
quiche [CUS08].
quick [Dew08].

R [Kat05b, Pag03, Spr03, Bih00].
R&D [Mau05].
Rabbit [BVP+04].
Rabin [Bon01, Gen04b, Miy01].
Rackoff [MP03, Pat03a].
radar [GG05b].
Radiations [SGM09].
radical [Web02].
Radio [Sak01].
RadioGatun [BDPV09].
Radix [HKA+05, JY01].
Radix [HKA+05, JY01].
rails [Fox00].
Rainbow [DS05a].
Raises [MP00].
Raising [Cos03].
ramp [YI06].
Ramping [Coc02b].
Random [Abe01, Abe04, BCT03, BK06a, BK05, BB04, BL08, CTY09, Chi08, Die03, DGP07a, DGP07b, DV08, EH+03, Gra02b, GPR06, HSR+01, HBF09, Int03, JRR09, Kel05, LLS+01, LMM+02, Lys02, MP03, Mir02, NNT05, Nie02b, Pas03, Pat04, Ran55, Ran01, RSN+01, SDFD06, TWNA08, TL07, Tip27, TZT09a, TZT09b, Vav03, VDK09, WP03, BK07, Be08, BG08, BG09, BG07a, BGL+03, CJL06, CO09, DGP09, Fis01a, GYC+08, Gen00b, GB09, HG05a, HLWZ09, HMvdLM07, JAW+00, KH08, KB39, KG09, M09, MFK+06, NR04, Pan07, PSG+09, PSP+08, PC00, Reg05, Reg09, RG09, RGX06, SS03, SXY01, 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 [Sun00a, DW01, Sim02]. Ransom
[BSN00, Bur00]. Region [BR09, CPS07, Pas03, RS00, Salt07, vT00].
Reference [BR09, CPS07, Pas03, RS00, Salt07, vT00]. Reference-Watermarking [BR09].
Refined [Sma03b]. Regarding [GMP01a]. Regex [BTTF02]. Region
[BSN00, Bur00]. Region-Based [BSN00]. register [HTW07]. Registers
[CGFSHG09]. Registration [HLM03]. regression [mSgFtL05]. regulations
[And04, Ano02i, Duw03, Eaq05, Fal07, Gas01, Gum04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, Pag03, Pap05, Puz04, Rec01, Rot07, See04, Spr03, Ter08, TvdKB +01, Top02, Was08a, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wal00]. Reviews
[For04, Kid00, Sal03b, Sty04]. Revised
[Bla03, BC05b, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GS02c, GH05, HH04, HH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PT06, RM04, Slo01, Ytr06, AMW07, Aj01a, BK07, Bir07, CKL05, DR08, DRS05, Irw03, PY05, WK06, Wri03]. Revisited
[ABC +05, Ano02h, BM01b, CDMP05, Knu00b, NS05c, OSSST04, Hes04b, ZZT05]. Revisiting
[AEAQ05, Har01a, Har01b, JMV02]. Revocation
[BDTW01, CL02a, Gen03, GST04, NNL01, TT01, ZSM05, KTO6, KSW06, LHH05, SW02]. revoke [NN03]. revolution [Bor00, Con00]. Revolutionary
[CMB +05]. Rewriting [Cir01, HR04a]. RFC [BWBL02]. RFID
[And04, AL07, ACdM05, BLDT09, CCMR05, CH07a, CL09, FW09, Fin03, KJK +07, OS06, Ros06b, SE09, TZT09a, TZT09b]. Rhee
[Küh08]. Rhode [IEE07]. RI [Sil01]. Right
[Dhe03, GS07b, HPKR05]. rightful
[CL08, Lin01a]. Rights
[Bor00a, BNPW03, Dre00, Scr01, Wya02, BA06, UP05]. Rijndael
[BB02, MP01a, SKU +00, Wer02, CKK +02, CGB01, DR00a, DR00b, DR01, DR02b, FKS +00, FKL +01b, FKL +01a, FSW01, FD01, GM00a, JmBdXgXm05, KTO6, KMT01, KV01, Luc00, MM01b, MH02, PSC +02, RDJ +01, SMTM01, SRL03]. Rijndael-Like [PSC +02]. Ring
[BSS02, Nao02, WBL01, ZK02, Her07]. Rings [BLST01]. RIPEMD
[DG02, WFLY04]. RISC
[Cor00a, Gro03, WWCW00]. RISC-Based
[Gro03]. Risk [WA07, Vo05]. Risks
[ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, PVS01, Sch00c]. Rivest
[BB79, Coc03, SP79]. RMI
[JR +06, Mar02a]. RNS
[B104, BKP09, NMSK01]. Road
[BDPV09, HR04b, PB01]. Roadmap
[Coc02b]. Roaming
[CAC03, YWD08, SS +08]. Robots
[Coc01a]. Robust [BB00a, BR09, CJ03c, CWY05, DDO +01, HH09, hKLS00, Lin00a, LHS05, LLC06b, PKJ01, SG07, SOH01, SDFH00, SDF01, VK07, WNY09, WL04b, WMDR08, YPSZ01, ZTP05, LCZ05c, LKZ +04, Mhit00, MB08, TND +09, YY05b]. Robustness
[CS05c, HM01b, Rot01, CKL +09]. Rogaway
[MW04]. Roger [GG05a]. Roger
[BB79, Coc03]. root
[Pet05]. rootkit
[Blu09]. Rootkits
[HBB06]. Roots
[Gon06, HCK09, CAC06]. Roseau
[IIEE04]. Ronald [Coc03]. root
[Pet05]. rootkit
[Bhh09]. Rootkits
[HB06]. Roots
[Gon06, HCK09, CAC06]. Roseau
[PY05]. Rotation
[RB08]. Rothe
[Fal07]. Rough
[Naz02, WG05]. roughness
[Lav09]. Round
[II00, BP04, Bih00, BF00a, BDK02b, Che03, DPV04, DI05, Dra00, FKS00w, GKK007, GIKR02, HSR +01, Kan01, KO04, KKS00a, KS00b, KKS01, KML +02, KKS00b, LKHL09, Lin01b, MP03, MHL +02, NPV01, RR00, Ros00, STK02, WBRF00, Wer02, YSD02, CV05, CLC08, CKL +03, DL +09, GIKR01, HSL +02, Kii01, LK +08, MR01b, Pha04, SW05]. round- [CLC08]. Round-Complexity
[Ros00]. Round-Optimal
[KO04]. Rounds
[BDK +09, CD01a, HSI02, KM01b, Luc00, Pat03a, Pat04, GM00a, SK01a]. Routing
[BGOY08, CL05, Ken02a, KB09, LAPS08, LHC08, MABI06, PS08a, RV09, vOWK07]. RSA
[Joy03b, Men05, Nac01, Oka04, Poi06,
Pre02c, Shp04a, Wal00, Adl03, Ano01k, Ano02e, AR01, BI04, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BJ00, BF01c, Bon01, BCCN01, BP01b, CNS02, CDL+00, CW02, Che01a, CKY05, CNPQ03, CKN00, CJNP02, CS00, CS03c, CD01b, DK01, DT03, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gro01, HN04, Her07, HLLL03, HLH00, HLL03, Int00, Jan08b, JS05, Jon08, JK02b, JJ02b, JG01, Kal01, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, May04, Miy01, Mol03b, MP01c, NZCG05, NZS05, NS01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Sha03a, Shp04b, SZ01, Str02]. RSA [SWH+09, TIGD01, TT00, Ver06a, Wal01, Wal03, WQWZ01, War00, WLHH05, Wie00, WS02, PY05, XC05, Yan07, hY08, YKLM02b, YKL03, YPKL08, YY00, You06, ZC09, Zhe01, ZWCY02, dW02]. RSA-based [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLLL03, NZCG05, Sei05, WLHH05, PY05, YPKL08, YY00]. RSA-Encrypted [CD01b]. RSA-Primitive [ST01a]. RSA(R) [An006b]. RSES [LLC08]. RST [ZLS07]. Rueppel [Ara02]. Rules [Bla01a, Ano00c, Bla01b, GM04, Ste02, Wue09]. Running [ZL04c]. Running-mode [ZL04c]. Runtime [PBTW07]. Russia [KGS05]. Ryan [Puc03]. Rye [KR05]. Ryu [KJ05]. S [BZ02, Kat05b, Puc03, Bih00, BCDM00, Dav01b, Dav01c, FM02b, JmBdXgXm05, Opp01, STM01, ZC00]. S-Box [FM02b, SMTM01, JmBdXgXm05]. S-boxes [BCDM00, ZC00]. S/MIME [BZ02, Kat05b, Puc03, Bih00, BCDM00, Dav01b, Dav01c, Opp01]. SAC [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR+01, HSS04, ST01d, VY01]. SAC’99 [HA00]. SAFE [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Oiw09]. Safe-Prime [ACS02]. Safeguard [LXM+05]. Safeguarding [Sty04, Bar03]. safer [An000f, NPV01, BDD03]. safety [HM01a]. SAFKASI [WAF00]. Salomon [Pap05]. Salsa20 [Ber07, Ber08]. Salt [PKBD01]. Salzburg [DKU05]. Samba [BH00a]. SAML [RR04]. Samos [KLG04]. sampling [WW06]. sampling [KB39, Sug03, Tip27]. San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Ok04, Poi06, Pre02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c]. sans [Car00]. Santa [Bel00, Bon03, Fra04, Kil01a, Men07, Shi05a, Yun02a]. Santiago [BS03]. Sanxin [LSZ05]. SARS [BA02]. SASAS [BS01c]. SAT [AKL+06]. Satan [Mea04]. satisfying [LPV05]. Saturation [Luc02a]. saving [Lev01]. Savings [AC03]. SAX2 [TEM+01, He01]. Say [Sta05]. says [Mad04]. SBLH [JK02a]. SBoxes [WOL01]. SC-CFS [It01]. SC2000 [SYY+02]. SC2001 [ACM01b]. Scalable [CP02, HKA+05, HLL05, KY03, KHYM08, SPG06, LLH08b, ST03a]. Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. Scale [BWE+00, CDR01, FGD01, BP03a, BH00a, HmvdLM07, PS08a]. Scaling [BBPV00, Coc02b, SDFH00, SDF01, PBVB01]. Scambray [Gum04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Os00]. Scenarios [BF05]. scene [SG07]. Skeptical [Pem01]. Schedule [MHM+02]. Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BNPS02, BR09, BS01d, BMS03, CL01a, CHK03, CGHG01, CYH01, CTL04, CC09, CH01b, CM05a, Coc01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJSS01, GS02c, HS02a, HNZ02, HY01, HT06, HC08, Ig02, JS0K1].
KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LCD07, Miy01, Mül01a, OKS06, PL01, RK06, Scr01, SOO02, SWH05, SGG00, SYL05, SSNGS00, Tad02, TC01, Tsa01, TT01, WQW01, WZW05, WBD01, YWWS09, YG01a, YLH05, ZJ09, AEEdR05, BCL05a, BCW05, BKN04, BBG02, CL02b, CC01, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CHY05a, CHY05b, CL00, CHC04, CCH04, CY05, CHS05, Che05a, Che08a, Che08b, CCS08, CKN06, CJT01, DW01, FXAM04, FWL08, FWT05, Gen09a, GS09, Hes04a, HPS01, HWW03, HWW04, Hsu05a, HWH05, Hsu05b].

Scheme [HC04a, Hwa00, HYS03, HLL04, Hwa05, HL05c, HL05d, HL05b, JW06, JSW05, KC09a, KLY03, KRY05, KSW06, KHL09, KCL03, Ku04, KC05, KCC05, KHL05, LHY02, LHL02, LHL03a, LKY04, LL04a, LJ04y, LL05a, LKY05a, LKY05d, LL05b, LMC+03, LHI04, LTH05, LLCL08, LHL03b, LC04a, LGY07, LCC05, LC04b, LC05a, LH05, LCZ05b, LCZ05c, LCZ05a, LWK05b, MSP09, NC09, PW05, PBMB01, PCC03, PC05b, PS01a, Pe04, Sae02, Sco04, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, mSgFl05, SCS05b, SC05c, SCS05c, SZS05, TLH05, TWL05, TY04, V080, Wan04b, WL05, WK05, WJP07, WDL09, WHH05, WC01b, WH02a, WHL03, WH03, WL04b, XC05, YTH04, YW04, YCH04, hY08, YRY04, YRY05a, YY05a, YY05b, YbJ04c, ZC04, ZX04, ZC05, ZK05, ZW05a, ZAX05, ZC09, ZL05, dRMS05]. Schemes [AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CPD06, CKNO, Cor02, CJNP02, Con04, CS04, CS03b, CDG+05, CL02, DN00a, DN02b, DS06, DN06b, FF00, HSZI00, HWW05, HM02b, HLL05, Kin02, Koa01a, KS03, KOMM01, LZL+01, LP01, MV00, NIS03b, Nam02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SBZ02, SPMLS02, Sun00a, VMSV05, WCJ09, XS03, YWC08, YYY01, Yek07, YYZ01, ZTP05, ZYR01, Abd01, AFGH06, BCD06, CWH00, CC05b, CHT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGK03, HCD08a, HCD08b, Han04, He02, HSK00, HW04, HW05, HC04b, HL04, IY06, IY06, JW05, KJ05, Kir01b, KT06, Kre05, Küh08, LWZH05, LWK05a, LW05c, MF07, Müll01b, NK06, PS02a, PKH05, QC05a, QC05b, SN00, Sha03d, Shao05b, SCL05, SC02c, SHT05]. schemes [Ts05, Wu01, XY04, YWC05, YCW+08, ZF05, ZCL05, vDKST06].

Schloss [IEE01b], Schneider [Puc03], Schneier [Sec04, Sty04], Schnorr [BP02]. School [Coc02a]. Schools [PM00]. Science [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Im03, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04]. Scientific [CHT02, MH09, Lau08b]. Scientists [Coc01a, MH09]. SCN [BC05b, CGP03]. Scots [Rec01, Sin99]. Scream [HCJ02]. Scribbner [Gas01]. Scripts [Uri01, Oue05, Rob02, Rob09]. scroll [GB09, HHYW07]. SD [ECM00a]. SDK [Ano02d, Bar00c]. SDL [HL06]. SEA [SPQ06]. SEAL [Fht02b]. Seamless [OKE02]. Search [Bi05a, Des00c, FIPR05, KB07, LM02, TIGD01, WYY05a, WYY05d, FZ06, PM08]. Searchable [ABC+05, AFI06]. Searches [PGT07]. Searching [BSW09, GTTC03, OS05]. Seattle [ACM06, S+03, USE00a]. Second [ACM03c, Bra01b, BD08, C205, GW01, HTS02, JY04, KCR04, Kl05, KP01, NM09, RD01, ACM00, Iw03, Son00, Spr03]. Second-Order [NM09]. Second-Price [Bra01b]. Secord [Top02]. Secrecy [Bla02a, GH02, Im03, Lau05, Rec01, RW03a, Sin01b, BDNN02, BLP06, BD04a, Mol05, Sin99, Sin00, ZYW07]. Secret [ACS02, Alv00, BBDK00, BTW05, Bi05b].
Can06a, CGHG01, Cer04b, CC02b, CSW+08, Che05b, CM05a, CH07a, CS09, Cha03, Coc01a, CK06b, Cor00b, Cor02, CGP+02, CG05, Dr.00c, Dal01, DN02a, DKMR05, DeL07, DJ06, Des00c, Dim07, DR02d, DSS01, DK05, DS05b, DBS+06, Elb09, ELvS01, FIP01b, FBWC02, FW09, FY06, For04, FML+03, FMV01, GS02a, GSS03, Gum04, Gut02b, Gut04a, Gutxx, HM00, HSZI01, Hei07, HM02b, Hir09, HLL+01, HGNP+03, HQ05, HL05c, HL05d, ISO04, Ina02a, Ina02b, Int00, IKY05, IKP+07, JYZ04, JP07, JP02b, JSW05, JG07, Jo01, JBR05, JK02b].

security

[JJ02b, JMV02, JQY01, Kan01, KM02, KSY01, KL05, Ken02a, KB06, KMZ03, KDO01, Koc02, KHL09, Kos01a, Kov01, KX000, Lad06, Lai03, Lan00a, Lan04b, LGS01, LKH+08, LKHL09, Leh06, Len01, LNS02, LL04c, LSH03a, LSH03b, Lin02, LWK05b, LP01, MJF07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Mü01a, NIS01b, NDJJ01, NP07, Oka00, OP01a, Ort00, PV06b, PSC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PTP07, PP07, Pho01, Pie05, Pii01, Poi02, PHM03, Poo03, PF03, PS05, Puc03, Puc06, QCB05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sal03a, SJ09, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch01f, See04, Sha05d, SLG+05, SL05a, Shp02, SEF+06, SEK01, SEK02, SK06, Sta03, SB07, Ste05b, SBZ02].

Security

[Sty04, SK01, Sun05, Swi05, Tan07b, TH07, TG04, TPPM07, Uni00a, USE00d, USE01c, USE02b, Uni00c, Uni00e, Uni00d, Uni00g, Uzu04, Vau02, VMC02, WLT05a, WBL01, WWL+02, WA07, YEP+06, YWD08, Zan01, ZWC02, ZDW06, Zhe02b, ZH03, ZS05, AA04b, Ano05b, AJ01a, AJ01b, BPS08, Bai08, Bau05, Bej06, Bel07b, BR04, BGP09, BFT08, BFG08, Bjo05, Ble07, BJ02, BMW05, BG07a, Bru06, BMV06, Can01a, C+02, Cha07, Cha05b, CKL+09, CKRT08, CJL06, CJM00, Con09, Con04, CC05e, DP04, DKK07, DY01, DFGH04, Des00a, DWML05, DUK05, DMS07, Egh00, FXAM04, FR08, FOP06, GH08, GJL06, GJJ05, Gha07, GJ03, Gor05, GKS05, GM01, GC05, Gut04c, HN04, HCD08a, HCD08b, Har05a, Hen01, Hes04a, HM05, HLS+02, HL06, HG05b, Ino05, JEZ04, Jun00, Kad07, KY00].

security

[KPS02, Kim02, Kov03, KH03, Kw03a, LC03, LL03, LJY04, LL05b, LPW06, LMC+03, LM05, LLLZ06a, LLLZ06b, LHC08, MJ03, Ma06, Man08, Man05, Man04, May01, MKK00, MSK03, Mg06, Men03, MS02d, MK05a, MPPM09, OP01b, Pa03, PSG+09, PC05a, Pat02a, PY05, PP06a, Fau00, PHS03, Poi00, PS04c, RC05, Ros06b, RN00a, RN00b, SN00, Sal05d, Sch03, Sen03, SL07, Shu06, SPPH06, Son00, SH00, Sta02b, Sta06, Ste02, Sun00b, SHT05, SL+00, Ts05, Uni00f, Vac06, Vo05, VOS08, WAF00, WA06, Won01, WK06, XQ07, YY04, YY05, ZS01, ZW05b, ZSN05, dB07, dCVD005, vWKO7, vT05, AG09, Ano02e, BC05b, BP01b, Chr00, Chr01, CCMR02, CCMR05, CGP03, JRB+06, Lin02, RR04, Uni00h, ZL04c, Pap05].

Security-related [Gutxx].

security-sensitive [SPPH06]. seed [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Shp05]. seeking [Mos06].

Seeks [CAC06]. Seems [Coc02a]. Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01, Y01, Ytr06, AMW07, Bir07, BC05b, CZ05, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bur03, dB07]. Selection [IBM00, JKK+01, RS00, SM08]. Selective-ID [CS07c]. Selectively [Ch08]. Self [GMM08, HW05, KY01d, PS01b, PBC05, Sch06b, WH06, WLT05b, ZKL01].
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]. Shacham [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 [BTW05, BI05b, BTW08, BGP02, CD00a, CLT07, CC08, CTY09, CDM00, CF02, CFS05, CDG05, CDI05, Di01, Di03, DS06, DP07, FM02a, FPS01, FMY01, HN01Z2, Kin02, Kog02, KS03, LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, SZ01, Sun00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CH05a, CHY05b, CDD00, DD04, DM07a, DKL00b, FWTC05, GIKR01, HT04, HKS00, IY06, LT04, MP07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDkST06]. shc [Gua05]. Sheets [MNS01]. shell [Dwi04, Gua05, BS01a, BSB05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [YW05c]. Shift [CGFSHG09, Che08a, Shin [Kii08, Kii08]. Shines [Coc02b]. Shinko [An000d]. Ships [An002e]. Shops [An001c, YSS+01]. Shor [KLB+02a]. Shores [KKP02]. Short [An001k, AFI06, BS04, 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, WHL05, ZKL01]. SHS [An008d, An012]. Shuffle [FS01c, NSNK05, Sas07]. Shuffles [Mir02]. Shuffling [PBD05]. shut [Gil07]. SiBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [An001i, BU02, KSWH00, Law09a, LL01, Mål02, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP+08, WL07]. Side-Channel [BU02, Law09a, Mål02, CNPQ03, PSP+08]. Side-Match [WC04]. Siena [BCKK05]. sieve [CM05b, J03]. 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 [BTTTF02, Dav01c]. SIGn-and-MAc [Kra03]. Signal [An002e, GGA05b, Shao1e, CLK+09, LLLZ06a, LLLZ06b, Kov01]. Signalling [ECM00b]. signals [Ren09]. Signature [AN05, AK00, A00, ADR02, An01c, An01f, An009, An013, Ara02, Ar01, ACJT00, Bar06b, BNPS02, BG00Y8, BMS03, BOS09b, CM00, CD00a, CL04a, CK02a, CGP08, CH01a, Che02, CM05a, Cor02, CF01, CS00, DS05a, DFKX05, Eng00, FIP00, Gen00a, GJS01, GS02c, HY05a, HSZ00, HM02b, JSJK01, K02, Kuh00, LZ0+01, LP01, MV01, M01, Nat00, NZ05G0, PL01, PCK02, Pre01, RS01, SA02, ST01b, S00102, SW05, SPM0502, Str01a, SYLC05, SSNGS00, TNM00, WQW01, WBD01, XYL09, Y00D01, Y0S01, Y0Z01, YL05, Z0K2, Z0J9, Zhe01, AvdH00, BCL05a, BCW05, C100b, CWH00, CL04b, CYH04, CCH05, CJ05, Che05a, CJT04, GGK03, HLL+02, His04a, HPS01, HWW02, HWW03, HW04, HWW05, HWW05, HWW05, HC04a, HWW05, HC04b, LL04, Kwo02, Kwo03b, LH04, LH05, LL05b, LLH04, LTH05, LWZH05, LHH05]. signature [LCZ05b, LCZ05c, LCZ05a,
LW05c, PKH05, PC05b, QCB05a, QCB05b, Sae02, Sha03c, Sha03d, Sha04b, Sha05a, Sha05b, Sha05d, SCL05, SHT05, TJC03, TYH04, Wao04b, WK05, WLHH05, WHH05, Wu01, WHL03, WH03, WY05, XCM05, YTH04, ZC05, ZF05, ZW05a, ZCL05, RR04.

Signature-Based [CK02a].
Signature-Embedded [Ano01c, YSS+01].
Signature-Tree [TNM00].
Signature/multisignature [Wu01].
Signatures [AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCCN01, CD00a, CL01b, CNV06, CBZ+01, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZ01, Her06, HM02b, HS01b, HHGP+03, HLT01, IR01, IR02, JS05, KZ01, LCK03, L501a, Lys02, MR01a, Mad00, MM02, MNFG02, PCG01, Ram01, RR02, Rs01, Wao01, XS03, Zha02, Ano00i, Ate04, AH05, BLH06, BB05, BMW02b, BMW02a, BLRS09, Cal00a, CKK03, Die00, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HLH00, JLL01, JL04, KKKL09, LV07, LS05b, MJ05, PLJ05a, PBV08, Sch01f, Sha01d, NZS05].

Signcryption [Boy03, MLM03, Zhe01].
Signed [FL01b, OSSST04, Sch01a, SJ00].
Signer [DKFX05, CJT04, LL05b, WK05, IR02].
Signer-Base [IR02]. signer-verified [CJT04]. Signers [LZL+01, Sae02, Sha03c, YTH04].
Significant [SZ01, MS02b, Shp02]. Signing [Ano00j, IR01, RR02, HW04, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAKD09. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imr03, Ree01]. Simple [AKS06, CYS05, CJS01, CJS03, CWY05, CS03c, DT03, FS01, G06, HM02c, HLT01, MS01, Nam02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKK03a, LKK03b, LF04, XH05]. Simpler [Lin03]. Simplicity [MS01. Simplification [DJ01]. Simplifications [JS05]. Simplified [Bon01]. Simplifying [Gut04b]. Simply [Oni01]. Simply-Iterated [Oni01]. Simulatability [HU05]. simulatable [Lau05]. Simulation [DKMR05, KL05, CPG+04]. Simulation-Based [DKMR05, KL05]. Simulations [WBRF00]. simultaneously [Wu01]. Singapore [BDZ04, TLC06]. Singh [Inr03, Ree03]. Single [GIS05, KO00, MM01b, MM10c, ZLZZ05, SV08a]. Single-Chip [MM01b, MM01c]. Single-Packet [WZLZZ05]. Single-Server [KO00]. Singular [AS08, Bao11b, BR09]. SINGOBIOGRAPHIES [LTT+04, Li05]. SIP [NTW07, PM00, ZS08]. Site [AECV+07, Cocc02a]. Sites [Ros07]. situation [AJ08]. six [Bel07a]. Sixth [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, TLC06]. Size [CS07c, CMJP03, HNZ02]. Skein [AEMR09]. Sketching [MNS08, SLTB+06]. Skipjack [Gra02a, HSL+02, SLL+00]. Skipjack-like [HSL+02, SLL+00]. SKLOIS [FLY06]. Sky [MYC01]. SLAAC [CGBS01]. SLEAC-1V [CGBS01]. Slide [Fur02b]. Small [CCM05, ELvS01, Fin02, GPS06, MNT+00, May02, OTO03, RK06, SM02, Sch01e, SPGQ06, Wal03, YLC+09, Duj08, dW02]. Small-Project [MNT+00]. Smaller [Bar00c]. Smart [Ano04, Ano03a, AJ01b, Bel01, BCST00, Car01, CL07, DF01, DFCW00, DJLT01, HBDJ01, Hen01, HQ05, Jac00, JSJK01, JY01, L00d, LSA+07, MOP06, MV01, MG08, NFQ03, Poh01, Q00, Q01, RE00, RE03, RS01, Sak01, SR01, Sha01c, SP02, TBDL01, VPG01, YKMY01, An00k, An00l, An004c, AJ01a, Bor00, BPR01, BCH05, BGL+03, Bur00, Cal00c, CCCY01, Cha05a, Cla00b, Coa00, CH00, DMT07, DFH01, DFPS07, Fin03, GM00, GUQ01, HHS01, Hsu05b, Hus01, KLY03, LKY05a, Ler02, LC05a, Lu07, MY01, PB01, Pre07, SVF07, Sm00, TIS07, VK08, Zaf00, BJvdB02, CL04d, CCK04b, Che00, DFP06, FGL02,
smart-card [GMG00, SKKS00, SCF01, TV03, YW04].
Smartcard [HWH01, KRV01, RMCG01, Uri01, PBVB00, CGMM02, DM07b, HRS02, It001, KSW06, An004b, RM02]. smarter [Car01, Cl00b]. Smartly [MS01]. Smooth [PS02b, GMR05]. SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. Sniff [An002e]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWH05, Sac02, Sh03c]. Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Ahm07, And07, An002c, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HMM01, Hoe01, Job03, Knu07, KSS02, Lad06, Law09a, LSY01, LLLZ06a, LSV09, LTM00, MNT00, MSNH07, MKY08, McG06, Nd05, PM00, PS01c, RM04, Sch01a, Sch00b, Ste00, USE00b, VH09, VVS01, WHL05, Wol04, ZCC01, An000b, An000j, Bir07, CT02, CCD04, CTT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, Mat02, McA08, MCHN05, Pau03, Sch01d, SS03, WL07, WA06, Sal03b, Bol02]. Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [Hoe01]. Software-Oriented [ZC01]. Software/Hardware [Nd05]. SOI [An002e, NFQ03]. SOISIC [An002e]. Solaris [An006c, BH00b]. Solomon [KY02b]. Solution [Cap01, DHR00, LLS05b, Poh01, Str02, TvdKB01, LSH00]. Solutions [An004b, MV01, Jan00, MSK03, MV03b, St.00, Gump04]. Solve [CU01, GS03]. Solving [CJT04, GPP08, Wil01a, Bul09, Whi09].

Some
[AG01, BDF01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HAnR04, He02, JK01a, RSS04, SHT05, ZF05]. Someren [An003e]. Something [FL01b]. sometimes [FR05]. Sons [An004]. Sorry [San05]. sorts [An003e]. Soul [Bl01c]. Sound [BJP02, FR08]. Soundness [ABH09, PV04, MR01c, BPS08, LA08]. Source [Bar00c, Bol02, Gut00, HBF09, KL09, PM00, RK06, TEM01, An003c, BGL03, McA08, RV09, SB05, Bar00b, Lin02]. Sources [KZ07, WL05]. Southampton [Bl03]. Soviet [AJ08]. SP [BG07a, Hir09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPARK [Jen09]. Sparse [BLST01, BD01b, GS03, BF06a]. Spatial [MM01a, SDFH00, SL09, YPPK09]. Spatial-Domain [SDFH00]. Spatio [CDTT05]. Spatio-Temporal [CDTT05]. speakables [BZ02]. Speaker [LM00]. Speaks [VN04]. Spec [Bar00c]. Special [An004a, An007b, An007a, BK06b, GS05, GS07a, GPP08, SGK08, KP03, FOP06]. Special-Purpose [An007b, An007a, GS07a, GPP08, SGK08]. Specialized [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00a, LKJL01, RSA00c, Mea04]. Specifications [IEE00b, BD05, BD04a]. Specified [Tad02, He02, LWK05b, YY05a, ZY05]. Specifying [BJvdB02, Cir01]. Speck [KGS07]. Spectr [GMM01]. Spectr-H64 [GMM01]. spectra [MS02b]. Spectral
STL [Zol01]. STOC [ACM05c, ACM07, ACM08, ACM09].
Stochastic [MG01]. Stock [Bar00a]. Stone [MLM03]. Stones [WRW02]. stop [SSNGS00, Win05c]. Storage [DFSS08, Din01, Din05, HR02, Har07b, Hug04, MSTS04, RCBL00, Ric07, RH02, Vad03, AFGH06, DFS05, HGR07, LPM05, SGMV09]. Store [CTBA+01]. Storing [ST06]. Story [Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kar01, Sch09, Bud02, DB04, Hau06, Hig04, HS01a, Win00].
Strategic [AJ08]. Strategies [Cir01, KL05, SKQ01, Dwi04]. Strategy [DR02a, TPPM07, KC09a]. Stream [BCC01, BSW09, BS00b, BL02, CF01b, Can06b, CJS01, CHJ02, CM03, Cou03, CL02c, DF07, Fil00, FF01a, Gol01d, GBM02, HCCR03, HR00, HR04a, Jam00, KHD01, MSN07, PP06a, SM01, Sar02, SXY01, WB02, W01, ZC00, ZCC01, BGP09, Ber07, B00a, BG08, BVP+04, DK08, KO08, Max06, MI09, P03, PC03, SB05, WW08]. Stream-Cipher [SXY01, WW08]. Streaming [OS05]. Streams [AIP01, YLC+09]. Strength [CB01, JX05, Oni01, CKL+09].
Strengthening [Loi00, MHM+02]. String [CP07, DFS04, Pas03, Dam00, RG05]. Strings [Vau05b]. Strong [ADD09, BB00b, CS00, DKFX05, KCJ+01, KW00, LSH03a, LSH03b, Lu02, Pau09, SBZ02, W02, CC04b, HRS08, K03, Ku04, LL05b, SS03, ZT03, ZFK04]. Strong-Password [LSH03a, LSH03b, W02, CC04b, K03, Ku04]. Strongly [Y06]. Structural [BS01c, LBR00]. Structure [DN07, EIG01, H01, HLL+01, MR02a, MR02b, GT07, HSL+02, MF07, PS02a, SG07, SLL+00, XMST07]. Structured [BRTM09, C03]. Structures [An02e, DS06, GTTC03, HCD002, KCP01, K02, MND+04, MFFT05, PSC+02, PQ03b, Sun00a, XH03, Hen06a, Y06, SW05].
struggle [Bur02]. Stuart [Gum04]. students [AA04b, PP09]. Studies [Pag03, SPH06]. Study [BBGM08, Car02, DPR01, DP00, KKJ+07, WC05, BKN04, BF06a, DY09a, KW06, SK+07, ZW01]. Sturgeon [Wei05, Wei00, Wei06].
Stuttgart [Eag05]. style [BPS08, dH08]. Subcommittee [Uni00f, Uni00h]. Subdivision [LD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro05, GMR05]. subliminal [LH04].
subsampling [LL06b], subscribe [SL05b]. subsets [Sch01e]. substitute [Bh02]. Substitution [KK03, GPX08, RBF08, WL04b]. Substitution-Permutation [K03]. Subsystem [HL07, MB04]. Subtleties [Lai08]. subverting [HB06]. Success [An06d]. successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Sufficient [KO05, KO06]. Suffix [ABM08]. SUID [Tot00]. SUID/Sqid [Tot00]. Suitable [AIK+01, CQS01, KTT07, LKH09, SP05, W03]. Suite [RSN+01, SBEW01, YLT06]. Suited [WWGP00]. Sun [Che04b, KLY02].
Sum-of-Digits [Che04b]. Sums [CY08, Shp05]. Sunspots [CP07]. Super [Lam07, CAC06, Hos06b]. supercluster [Pri00]. Supercomputer [Coc01a].
Supersingular [Gal01, R02, Ver01]. Supplemental [BD01]. Supplementary [ECM00a, ECM00b]. Supplies [Sha01c]. Support [ABM00, Gro03, LT+00, PJDH09, S02, An05b, BMA00a, BMA00b, BMA00c, ED03, mSGFL05, SSM+08, WNQ08, ZYLG05].
Supporting [CLK01a, SW02]. Suppression [GA05]. Sure [Tom06]. surface [Iwa08, SDL07]. Surfaces [SPK08]. surveillance [CS09]. Survey [EPP+07, KM04b, LDH06, ATS04, An00e].
TC-6 [DKU05]. TC11 [ElvS01]. TC8 [DFCW00]. TC8/WG8.8 [DFCW00]. TCB [SPHH06]. TCC [HR06, Kil05, Nao04]. TCP [CD01b, Ols00, SBB05]. TEA [CV05, HSR+01, HSIR02, HHH+04, MHL+02, WN95]. Teaching [McA08, Shi08, GV09, Jan08b]. Tech [Kir01a, TvdKB+01, Uni00c, Gra01, Uni00f]. Technical [BHM03, GS07b, Lan00c, Scr01, TL02, USE01b, USE01a, USE02c]. Technique [CC02a, Pau09, PQ03b, SC02a, WC03, vW01, CL00, Che08b, Pan03, Ren09]. Techniques [AIP01, BSW09, Bib03, BBPV00, BDP02, CC04a, Cra05a, DBS+06, Dun06, Gal03, KLN+06, Ken02b, Knu02, KO03, MKP09, NCRX04, PJK01, Pfi01, Pre00, Shi08, YKW01, AB09, BMW05, BR05, Che08a, DY01, DHMR07, DY09a, Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08]. Technologie [RSA09b]. Technologies [MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZWC02, ATS04, PB01, TTZ01]. Technology [CZK05, Cra00a, GSB+04, MP00, NFQ03, Pag03, TV03, AL07, Ble07, Car01, Cas02, Che00, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b]. Tektronix [Ano02c]. TelCorrelo [LM00]. telegram [Tuc66]. Teelogic [Ano02c]. Telephone [KZ01]. Telephony [Ano02c, PM00, CGV09]. teleportation [BEZ00, BEZ01, Duw03]. Telling [Gan01b]. template [LLC06a, UBE09]. Temporal [CDTT05, KXTZ09]. Ten [ESE00a]. Tenth [USE01c]. Term [ABRW01, Dur01, BMV06, ISO05, SGMV09, WDL09]. Terminal [ECM00a, ECM00b]. terminals [ISTE08]. termination [BP05]. terms [LMT05]. Ternary [AD09, DKL00b]. Terrorism [PP06b]. terrorists [Mad04, Win05c]. TESLA [LN04]. Test [BT02, HSS04, Lan00b, LN08, RSN+01, Way02a, DSS0, GMG00, Kat05a, KKKP05, RSS04]. testable [RMPJ08]. Testing [HI00, CGBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03]. Tests [MT02, NM09, GT02, Gut04c]. Text [Lut02, PJH01, PM08]. textbook [BJN00, PP09]. Thank [CMB+05]. Theft [CMS09]. Their [AGT01, CD00a, Gen04a, JKRW01, LLL+01, WLZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, TO01, WV00]. Them [WD01a, Tee06]. Theorem [AC02, Eke02, GN01, Sho00a, Sch01b, YKLM03]. theorems [MW04, Nyb01]. Theoretic [CB01, DHR00, Kat05b, Nie02b, VVS01, VDKP05, vW01, Mar05b, NR04, Shp99, Wag03]. Theoretical [SGB01, PRS04]. Theoretically [AP09, DM06b]. Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bib03, Boy01, CC04a, Cra05a, Des02, Fal07, HR06, Hay06, IZ00, Irw03, Kin01, Knu02, Lai03, Lee04b, Lut03, MNT+00, Mao04, NP02a, Nao04, Oka00, PY06, Pfi01, Pre00, Rot05, Roy05, Sch06b, Shp03, Spr03, TW02, TW06b, Van05a, Wai00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cas06, Cos00, DW05, Gar04, HHL+00, HW98, Joy00, Kil05, La00, Lam01, PPV96, Rot02b, Rot03, SCS05a, Sho05b, Ste08, Sti95, Sti02, Sti06c, Tat05, TW05, Was08b, HR06, KXTZ09, Kil05, Nao04, Nie02a, Nie04]. There [Bar00b, GW00]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Sch03]. Third [AL06, BS01b, CGP03, HR06, IKY05, KNP01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QSO0, CGH+00b]. third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM00]. Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thirty-Fourth [ACM02]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT+00]. Thoughts [Joh00]. Threat
threatened [Por06, SS04, BK00, Geb04]. threats [CNPQ03]. Three [BR00b, Kak06, LSH00, MAaT06, AJ08, CLC08, FGM03, GPS05, LKY05b, LLS+09, MF07, MAaTxx, SPPH06, YC09a, ZL04b]. Three-Key [BR00b]. Three-party [LSH00, CLC08, LLS+09, YC09a].

three-principal [ZL04b]. Three-Stage [Kak06]. Three-party [LSH00, CLC08, LLS+09, YC09a].

thresholding [WL07]. Time [GBKP01, Di01].

Tickets [FGL02, KS02]. Tie [SZS05b]. tier [TW07]. Tight [CM05a, Di01].

Time [AK02a, App07, AJ008, BPST02, BS00b, BSW01, CU01, CJO3a, CVN06, CLZ02, Dri02, GPcS08, HM02b, Ina02b, KL05, Kuh02a, LP02a, Lan00b, LJL05, LDM04, May04, Oec03, Pil01, QSR+02, RR02, CAC03, CCK04b, CLO0, DS02, GS07b, GM04, HHC05, LC04a, MRST06, NS05a, YZD07, yO8, DK08].

time-bound [yO8]. Time-Domain [Kuh02a].

Time-Free [CVN06]. Time-Limited [AK02a]. Time-Memory [AJ008, Oec03, QSR+02].

Time-Memory-Data [DK08].

Time-Reversed [Ina02b]. time-space [NS05a]. time-stamping [HHC05].

Time/ Memory/Data [BS00b]. Timed [BN00b, CHKO08, JF07, LKJL01, MA01, HGNS03, Zha06]. Timed-Release [CHK008, MA01, HGNS03].

times [AJ08, CCK04b, Mol005]. timestamp [YW04]. timestamp-based [YW04]. Timestamping [MSTS04]. Timing

[CKQ03, CWR09, Law09b, Sch01b, SWT07, ASK05, DKL+00a, KS09, OS00].

timing-attack [KS09]. Tiny [Bar00b, WN95, And03]. Tipsy [TvdKB+01]. Tissue [MYC01]. Title [ZHY03]. TLS [HSD+05, JK02b, JJ02b, SBEW01, BFCZ08].

TIMAC [KI03]. TMS320C6x [WGP06].

today [Lie05, Nis03a]. Together [WD01a].

Token [Fri01, RSA00d, RSA01, CS04].

Tokyo [An00d]. Told [ES00a].

Tolerance [An04a, BKo6b, ZL04a].

Tolerant [DS03, HSKC01, BKW03, HGR07, Lin07, PI06, RH04, YbJF04].

Tolerating [KSR02, SKR02]. too [Sch05c, vT01]. took [IEE09a].

Tool [An02d, An02e, KI101, GPG06]. Toolkit [NIS01a, Sha01a].

Tools [An02d, An02e, Bar00b, Golo1b, Ken02b, Ust01b, Bai08, Cas02, CT02, GC05, NCRX04, SETB08, Kat05b, Puc03]. toolset [Jen09].

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

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

Topics [HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oka04, Po016, Pre02c].

topology [Hjo07].

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 [HLL01, WH05, WLHH05, WY05].

Traceable [LZL+01, CCH04].

traceback [CS04].

Tracing [KY01d, KY01e, LLL02, NN01, SNW00, TT01, WRW02, WLZZ05, WH01].

tracings [RE02].

Track [Fox00, Joy03b, Nac01, Oka04, Po016, PHM03, Pre02c, USE01b].

USE02c, Men05, CAC03, CAC06].

Tracking [WCJ05, FNRC05, SZ08, TWM+09].

Trade
Two-Block [KCP01]. two-channel
[MS09c]. Two-factor
[Hen06b, Sch05c, St.00, Ste05a, dB07].
Two-Key [KI03]. two-level
[DH06]. Two-Party [KO04, Lin01b, MR01a, WW05, CLOS02, GCKL08, JW01, ZLX99].
Two-Pass [SK00]. Two-tier [TW07].
Two-Way [DIS02]. TWOBLOCK [Yan05].
Two-Fish [BF00b, FKSW00, IK00, Kel00, Knu00a, Knu00b, Luc02a, Mur00, SKW +00].
Type [CKQ03, Dug04, H"of01, KYHC01, PDMS09, RMS05, Vir03, GGO8, PQ06, Sha01d].
Type-based [Dug04]. Type-Passing [Vir03]. typed [BG07b, FR08]. Types [Gor02a, GJ04, RSA00e, BFM07, Lau05].
Typical [BSC01a]. typing [GJ03]. Tzeng [QCB05a, Hsu05a, HL05d].
U [DB04]. U-boat [DB04]. U.K. [CAC06].
U.S [Uni01]. U.S. [Bol02, PM00, Uni00b].
Ubiquitous [Sto03, LKZ +04]. UCOn [LY05, PS04b]. UK
[CZ05, Chr00, Chr01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01].
Ultimate [Di01]. ultra
[Bar02, CH07a, DB04, Cal01, Win00]. ultra-lightweight [CH07a]. ultra-secret
[Bar02]. Ultrafast [FF01a]. UltraSONIC
[MMMH02]. UMTS [Cha05b, HL07].
Unauthorized [Ano02e]. Unbalanced
[FMP03, May02, HLLL03]. Unbelievable
[Len01]. Unborn [Pau02a]. Unbounded
[RW02, WvD02]. Unbreakable [Ver06b].
Uncertain [See04, Sty04, Sch03].
UNCITRAL [MNFG02]. uncompletable
[NS01a]. Unconditional
[HM01b, May01, Pas05, RW03b, WW05].
Unconditionally
[HSZI00, HSZI01, HSHI02, HSHI06].
Uncovering [MNT +00]. Uncrackable
[Ano03c]. undeciphered [Rob02, Rob09].
Undeniable
[GMP01b, GM03, JSJK01, Miy01, WQWZ01, CHC05, LH04, LCZ05a, SSM +08].
undergraduate [AA04b, Gha07].
undergraduates [DFGH04].
Understanding [CPG +04, Cra05b, Elb09, Gor06, PP09, Sun05, Un09]. undetectable
[BMW02b]. Unexpectedly [Bar00a].
Unforgeable [BY02, KY01a]. Unicode
[MJF07]. Unified
[CZB +01, HKA +05, MFS +09, SM03b].
Uniform [SPK08, TL07, SU07]. uniformity
[Shp01, Shp04b]. Unimodular [CV03].
Unique [Lam91, Lys02, TH01]. United
[DFCW00, Jol01]. Universal [BOHL +05, CR03, CJSNP02, CS02, If06, KKKP05, KO03, Pli01, Sho00a, SP79, Cal00c, PS04c].
 universality [DS02]. Universally
[AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DNO2b, DN03, NMO05, RK05].
Universally-Composable [AF04b].
Universiteit [BBDO9]. University
[Kat05b, Puc03, Rot07, Top02]. UNIX
[CCDP01, Har01a, Har01b, Ho01, Wit01, GSS03]. UNIX-Type [Hö01]. Unknown
[CT08a, Luc02b, CSM05, HJ07]. Unknowns
[CMB +05]. unleash [McN03]. Unleashing
[Lop06]. unlinkability [WH05].
Unpredictability [BS02]. unprotected
[ASK05]. Unravelling [Ano03c]. unsolved
[Bel07a, GG05a]. untold [DB04].
untraceability [CL09, LHY05, Par04].
Untraceable [ACM05]. Untrusted
[BMK00, CGK +02, LS09, LLK05, ZBP05].
unusual [GG05a]. Unveiled [Bar00a].
Update [TEM +01]. Updated [Cho08a].
upgrade [Pau02a, Pau02b]. Upgrades
[Ano02e]. upon [DFG01, PQ03a].
UPPAAL [BBDO2]. Upper
[BP03b, DRR05, KMT01]. Upwards
[BF03]. URSA [LKZ +04]. US$54 [Dw03].
USA [ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKE05, Joy03b, JQ04, Jue04, KKP02, KJR05, KIt05, KP01, Men05, Men07, Nac01, Nao04, Oka04, Poi06, Pre02c,
78

Sch01d, Sho05a, Sil01, YDKM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FMA02, IEE01a, IEE05a, IEE05b, IEE08, IEE09b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SMP+09, USE00c, USE00b, USE00a, USE01c, USE01a, USE02c, Wis99, Yun02a.

usability [CG05]. Usage [LY05, PS04b]. Use [Bai01a, BWBL02, Bol02, BQR01, CPS07, Dre00, ISO05, Kra03, LC04, Pan09, PBTW07, Str01a, WS05, Win01, CG05, OS07]. used [CDL06, MSV04]. useful [SM03a]. Usenet [Coc01a]. USENIX [Coc01a]. User [Ano00k, BGP02, CL01b, CMB+05, DP00, Had00, HY01, KZ09, LSZ05, JR03, OH08, PS01b, Pohl01, Saso07, SSM+08, Str01a, Tsa01, BM00, CL04d, DLY08, GMLS02, Hsu05b, HL05b, KC05, LAPS08, LHY02, LHL02, LKY04, LKY05a, LHL03b, LC05a, LC01, Pur04, SS03, SZ05, TWL05, WLT05a, YS04, YR04, ZYLG05, vOT08]. User-Centered [CMB+05]. user-controlled [LAPS08]. user-drawn [vOT08]. user-friendly [SZ05, WLT05a]. user-level [SS03]. Users [LS05b]. Uses [Bau01c, RSQ03]. ushers [Bur00]. Using [AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01i, ADDS06, BJP02, BHO6, BK06a, Bau01a, Bau01b, BP06, BPST02, BR09, BT02, BM00, BMP00, BLO2, Che01a, CL04d, CGBS01, CCG02, CCM01, CH07c, Cir01, DI05, DPR01, DP00, DWN01, DGH+04, EFY+05, FJ03, FMP03, Frie01, GC01a, GL01, GSB+04, HHGP+03, H050, HJ01, Jab01, JKK+01, JSJ01, KKY01, Kel05, KMO1a, KLC+00, KTT07, Kru02b, KZ09, Lan04a, Len01, LB04, LS05a, LM02, LH07, MS02a, MS09a, ML03, MS03b, MM05, NZCG05, NM09, OT03a, PHK+01, PJH01, PJK01, PCK02, PK01, Sho00b, SK05a, Sm03a, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VPG01, WY02, W01, WC03, XFZ01, YKMY01, YL02, YS+01, ZZWL01, Zhe01, ASW00, AL07, BCL05a, BCW05, BK07, CG06, CDS07, CWH00, CL04d]. using [CCK04b, CCH05, CHY05b, CKY05, CJ05, Che07, CKY07, Che08a, Che08b, CJ04, CCK03, Cos00, DZL01, Dan02, DFG00, FWTC05, GC00a, GMR05, Gen09b, GS09, HHSS01, HW05, HAU04, HTW07, Hr09, HW04, HY03, HL04, JR09, KOY09, KC09a, KYY03, KB09, KKL09, KKJ+07, KSW06, KR03, Knu04, KC05, LHY02, LL02, LKY04, LCP04, LL04b, LW04, LKY05a, LL05, LW09, LF04, LC05a, LCC06a, LK05a, MT07, Mic01, NS05a, Pe03, PS04a, PY08, PCS03, PC03b, PC05b, RC05, Sco04, Sha04b, Sha05b, SHH07, Tan07a, TL05, Tso05, TJ03, VK08, Wan04b, W05, Wan05, WGL00, WH03, YW04, YW05, YC09a, YRY04, YRY05b, YZ05a, ZF04]. utility [Gua05]. Utilizing [Str02].

V [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00c]. v2.1 [RSA02]. v2.11 [RSA01]. V5 [It000]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABR01, BM01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [PM00]. Value [BR09, GIS05, LS08, BMW02a, DK08, WTH08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadhrajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Lue02b, NSNK05, Ber08, Duj08, Duj09]. Variants [BDK+09, DG02, KS00b, C05, Sha04b, TJC03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDhKB09]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pe09, mSGFL05, WNQ08]. vectors [LHL04]. Vegas [ELvS01, IEE01a]. Vein [BDhKB09]. Vendors [Pau03, MV03b]. Venona [Ben01b, Ben04]. Verenigde [dL00]. Veridicom [Ano02d]. Verifiable [ANR01, Ate04, CD00a, CS03a,
CHS05, Cha04, JLL02, JG01, Lys02, NZCG05, NZS05, NSNK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a. 
Verifiably [BGLS03, Hes04a]. 
verifiably-encrypted [Hes04a]. 
Verification 
[AAK05, Ara02, BPST02, BP05, GMV01, G1], Gut02b, Gut04a, HW01, Hoe01, Str01a, BD04a, CC05b, CJL06, Coh03, DS00, HL05c, JW01, Ler02, MD04, MT07, MSP09, PBD07, TYH04, W04b, Wa01, YLC09, ZL04b, CS08b, Uz04a. 
Verified [BJP02, BFGT08, BFCZ08, CJK04]. 
[Bl02, BLP06, HLH00, SV08a, Sha01a]. 
Versions [Bol02, HPC02, OST05, SKI01, Mis06]. 
Verification [BFG08, BJvdB02, CJM00, HLT01, IR01], PT08, RR02, BL06, BLP06, HLH00, SV08a, Sha01a]. 
[BJP02, BFGT08, BFCZ08, CJK04]. 
[Bl02, BLP06, HLH00, SV08a, Sha01a]. 
versions [Bol02, HPC02, OST05, SKI01, Mis06]. 
Verifiers [CL01a, He02, LV07, LWK05b, YYY05a, ZP04]. 
Verify [MS02a]. 
Verifying [BFG08, BJvdB02, CJM00, HLH01, IR01, PT08, RR02, BL06, BLP06, HLH00, SV08a, Sha01a]. 
[BJP02, BFGT08, BFCZ08, CJK04]. 
[Bl02, BLP06, HLH00, SV08a, Sha01a]. 
Verifications [Bol02, HPC02, OST05, SKI01, Mis06]. 
Verstehen [Sch09]. 
Versus [Mad00, Rub00, WWL02, ASW01, BJLS02, DBS01, WPP05]. 
Vertically [DN04]. 
Very [AAC01, B+02, CG03, EBC00, FLA03, H001, PM02, PBMB01, Zir07]. 
Vestiges [Top02]. 
[VI] [Sch04a]. 
via [AGK07, An00b, ACD05, BD09, Car02, C03, CPG04, FBWC02, Fox00, HHYW07, HL03, J006a, KT06, ML05, PG05, RG05, SB01, SLG05, ZG01, Lu05]. 
Victoria [ACM08, IZ00]. 
Victorian [Top02]. 
victory [Han03]. 
Vid [CAC06]. 
Video [BDF+01a, BD03, CT05, EY+05, ISS208, KBD03, KJ05, KLI01, LHS05, MLC01, SC02a, BS01b, JA02, KN03, UP05]. 
Video-Based [KJ05, BS01b, KN03]. 
Videos [YHDW07]. 
Vienna [BZ02]. 
Vietnam [Lov01]. 
View [Bar00a, Mah04, Sin09]. 
Views [Bar00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03]. 
Vigenère [DG00]. 
VII [Sch04b]. 
VIII [IEE01b, Sch05a]. 
Virginia [MS05b]. 
Virtual [An00c, HM01b, Pro00, YSS01, BDS09a, ML05, ZBP05]. 
virtualization 
[CGL08a, CGL08b, CGL08c]. 
virtualization-based 
[CGL08a, CGL08b, CGL08c]. 
Virtues [Tro08]. 
Virus [Gor06, An00b]. 
Visible [HT06]. 
Vista [Fe06]. 
Visual [BDN00, BDDS03, BCD06, CCL09, CTY09, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, ZP05, ABDS01, CDF05, CDD07, DD04, HKS00, L009, PY08, Yan02, YC07, Bon00, Zol01]. 
Visualization [XYL09, MFS09]. 
Viterbi [LBMG01, LBMG02]. 
Vladimirov [Puz04]. 
VLDV [EBC00, FLA03]. 
VLDV [B+02]. 
VLSI [KV01]. 
VMS [CA05a]. 
Voice [An001, PK01, VN04]. 
VolIP [An00c, SZ08, VAV09, WC05]. 
vol [Kat05b, Lee03b]. 
volatile [SB01, SLG05, ZG01, Lu05]. 
Volume [Go04]. 
Vortrag [Eke02]. 
Voter [Cha04]. 
Voter-Verifiable [Cha04]. 
Voting [Cha04, FPS01, HS00, J005, JLL02, KMO01, Rub01, CT03, HJW05]. 
Voyнич [Rug04]. 
VPN [KMM06]. 
VPNs [Dav01a]. 
VQ [WJP07]. 
VQ-based [WJP07]. 
Vs [CTBA01, Di 01, Di 03, SU07, WW04]. 
VSS [AF04b, CDF01, FM02a]. 
Vu [DP00]. 
vulnerabilities 
[CSW05, DMS07, SV05, XNK05]. 
vulnerability [KHL09, SAG07, YRS09]. 
WA [ACM06]. 
WACs [Kov01]. 
Wagner [DP06]. 
Wagstaff [Kat05b]. 
Wahab [MAaT07]. 
Walking [Fox00]. 
Wallet [ETZ00, JL04]. 
Walsh [MS02b]. 
Walsingham [Bu06]. 
WAN [H001]. 
WAN-Cluster [H001]. 
Wang [SZ05]. 
WAP [JRF01]. 
War [Bec02, Bu00a, Bu02, Hau03, Kov01, MH09, OC03, AJ08, DB04, R006, L001]. 
Warfare [HW01, WW04]. 
warrior [PC04].
Wars [RR03b]. Warsaw [AUW01, Bih03].
Washington [S’03, USE00a, USE01c].
wasn’t [Bur02]. WaSP [Coc02b]. WASSA [Ano05b]. Watch [MA00a, Joy03a].
Waterloo [HH04, HH05, ST01d].
Watermark [AS01b, GMV01, JX05, KHY04, Kwo03a, Mel01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zan01, AA08, CL08, LYGL07, LLC06a].
Watermark-based [Kwo03a].
Watermark-Fingerprint [KHY04].
Watermarked [ST01c]. Watermarking [AS08, AK02b, AHK03b, AS01c, Arn01, ARC’+01, BR09, BSC01a, BSC01b, BSL02, BQR01, BSNO00, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB’+08, DWN01, DNP07, EFY’+05, EIG01, GW01, HT06, HH09, JK’+01, KCR04, hKL05, KLL01, Kun01, KT00, L09, LSL05a, LKL05, L01, LZ’+04, LWS05, LP06, LJ05b, LL01, LSKC05, MM01a, MNS01, Nak01, OMT02, PJ01, PJK01, PR01, PBM’+07, Q01, San09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SPK08, VVS01, VHP01, VK07, WCJ09, WH09, WNY09, WWL’+02, WLT05b, XF01, YWWS09, ZTP05, ZWC02, AHK03a, AAP07, BCKK05, CC02b, Che08b, CYH’+07, CCD’+04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, HHC05, JDJ01, JA02, KPO0, LDD07, Lin00a, Lin01a, LLC06a, LLCC06b, MB08, MCH05, PK03, Ren09, mSGFl05].
watermarking [WJP07, WNQ08, Way02b, Way09, WMDR08, XMST07, YZDW07, YPS01, ZLZS07].
Watermarks [Ben00, BB00a, MLC01, Sug01, WC03, WC04, YLLL02, MB08, TND’+09].
Watershed [FBW01].
Watershed-from-Markers [FBW01].
WAV [XFZ01]. WAV-Table [XFZ01].
Wavelet [BR09, GW01, LKLK05, L01, Nak01, VK07, AAP07, AA08].
wavelet-based [AAP07, AA08].
Wavelet-Domain [LZ01], WAVES [LBA00]. Way [BYJK08, BM01a, CHL02, DIS02, DMS00, Fis01b, GKK’+09, HNO’+09, HR05, K003, KO00, LTW05, Sh00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK’+07, HR07, HR05, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LKL01, Mic02a, Poi00, YW05, YRY05b, ZW05a].
Wayness [KI01a, PV06b]. Ways [BB02]. WCC [Ytr06]. WDDL [MMMT09].
Weak [HS03, LS01c, RW03b, DW09, GG08, KOY09, KW00].
Weakly [HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00].
Weakness [AS08, AK02b, AHK03b, AS01c, Arn01, ARC’+01, BR09, BSC01a, BSC01b, BSL02, BQR01, BSNO00, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB’+08, DWN01, DNP07, EFY’+05, EIG01, GW01, HT06, HH09, JK’+01, KCR04, hKL05, KLL01, Kun01, KT00, L09, LSL05a, LKL05, L01, LZ’+04, LWS05, LP06, LJ05b, LL01, LSKC05, MM01a, MNS01, Nak01, OMT02, PJ01, PJK01, PR01, PBM’+07, Q01, San09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SPK08, VVS01, VHP01, VK07, WCJ09, WH09, WNY09, WWL’+02, WLT05b, XF01, YWWS09, ZTP05, ZWC02, AHK03a, AAP07, BCKK05, CC02b, Che08b, CYH’+07, CCD’+04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, HHC05, JDJ01, JA02, KPO0, LDD07, Lin00a, Lin01a, LLC06a, LLCC06b, MB08, MCH05, PK03, Ren09, mSGFl05].
Weights [AS08, AK02b, AHK03b, AS01c, Arn01, ARC’+01, BR09, BSC01a, BSC01b, BSL02, BQR01, BSNO00, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB’+08, DWN01, DNP07, EFY’+05, EIG01, GW01, HT06, HH09, JK’+01, KCR04, hKL05, KLL01, Kun01, KT00, L09, LSL05a, LKL05, L01, LZ’+04, LWS05, LP06, LJ05b, LL01, LSKC05, MM01a, MNS01, Nak01, OMT02, PJ01, PJK01, PR01, PBM’+07, Q01, San09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SPK08, VVS01, VHP01, VK07, WCJ09, WH09, WNY09, WWL’+02, WLT05b, XF01, YWWS09, ZTP05, ZWC02, AHK03a, AAP07, BCKK05, CC02b, Che08b, CYH’+07, CCD’+04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, HHC05, JDJ01, JA02, KPO0, LDD07, Lin00a, Lin01a, LLC06a, LLCC06b, MB08, MCH05, PK03, Ren09, mSGFl05].
[Puz04, Sty04, VGM04, FMA02, Bar03]. Wi-Fi [Sty04, Bar03]. Wi-Foo [Puz04, VGM04]. wicked [Lud05]. Wide [DR02a, SBB03]. Width [OT03b]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b]. Wiley [And04, Gra01, Kir01a]. Wiener [Duj08, Duj09]. WIESSE [USE00b].
REFERENCES

[CV05, HHK+04, MHL+02]. XTR
[LW02, LV00, LNS02, Ver01].

Yahalom [Pau01]. Yang
[KJY05, WL05, YWC05]. Yang-Shieh
[YWC05]. Yao [BPS08, BDNN02, ZD05].
Yao-style [BPS08]. Yarrow
[KSF00, Mur02]. Yarrow-160 [KSF00].
Yaschenko [Kat05b]. YCH [SC05a]. YCN
[Hwa00]. Year [Naz02, Bur00]. Years
[Ahm08, CM02]. Yellow [JY04]. Yen
[LLLZ06a, LLLZ06b]. Sen-Guo [LLLZ06a].
Yesterday [Coc02a]. Yi [Wag00]. Yi-Lam
[Wag00]. Yokohama [Mat02]. Yoo
[KCC05, KHKL05]. Yoon [KCC05]. York
[HR06, IKY05, NIS00, Sch01d, YDKM06].
Young [FF01b]. You’re [ES00a, Nic01].
You’ve [Nic01]. Yuck [Sas07]. Yuen
[KL08].

Z [Wue09]. Z-parameter [Wue09]. z10
[Web08]. z9 [ADH+07]. Zealand [Zhe02b].
Zeilinger [Duw03]. Zero [AS01b, APV05,
BP04, Cou01, DPV04, DFS04, DDO+01,
HNO+09, IKOS07, LMS05, LHL+08, MR01b,
MV03a, Pas05, Ros00, Ros06a, CSW05,
Dam00, PBD07, KK07]. zero-day [CSW05].
Zero-Knowledge [AS01b, BP04, Cou01,
DFS04, HNO+09, LHL+08, MR01b, MV03a,
Pas05, Ros00, Ros06a, IKOS07, Dam00,
PBD07]. Zeta [Ver02]. Zhang [JW01,
YY05a]. Zhou [PKH05]. Zimmermann
[McL06, Tuc06]. ZK [PBD05]. Zodiac
[HSM+02]. [AA04a]

References


Al-Akaidi:2004:FSP

Aly:2004:CSP

Agreste:2008:NAP
REFERENCES


REFERENCES


REFERENCES


[Abe04] Masayuki Abe. Combin-


Ansper:2001:ELT


Ambainis:2009:NEQ


Adcock:2002:QGL


Ateniese:2005:URT


Ateniese:2000:PPS

Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Bellare [Bel00], pages 255–??
REFERENCES

ACM:2000:PTS


ACM:2001:PAAN


ACM:2001:SHP


ACM:2002:PTF


ACM:2003:PAS


ACM:2003:PTF


ACM:2003:PTS

[ACM03c] ACM, editor. *Proceedings of the Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium on
ACM:2004:PAS


ACM:2004:PAA


ACM:2005:MPI


ACM:2005:PTF


ACM:2005:SPA


ACM:2006:PTE


ACM:2007:SPA

ACM, editor. STOC ’07: proceedings of the 39th Annual ACM Symposium on
Algesheimer:2002:ECM

Alvarez:2005:EBS

Ahmad:2007:ADE
Imtiaz Ahmad and A. Shoba Das. Analysis and detection of errors in implementation of SHA-512 algorithms on FPGAs. The
REFERENCES

Anyanwu:2009:DCS

Avanzi:2006:ESM

Arnold:2007:CSE

Adikari:2009:HBT

Adleman:2003:TLP

An:2002:SJS
Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature


[AF04a] Martín Abadi and Cédric Fournet. Private authentication. *Theoretical Com-
REFERENCES

Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. [AG09]

Attrapadung:2006:FSS


Akkar:2001:IAS


Acquisti:2009:PSS

Alessandro Acquisti and


Rakesh Agrawal, Peter J. Haas, and Jerry Kiernan. A
system for watermarking relational databases. In ACM [ACM03a], page 674. ISBN 1-58113-634-X. LCCN ????


Armington:2002:BAI


REFERENCES


Al-Ibrahim:2001:AMS


Al-Ibrahim:2001:AMS


Attali:2001:JSC

REFERENCES


Attali:2001:SCP

Aid:2008:NSA

Avoine:2008:CIT

Al-Jarrah:2008:NKM

Abe:2002:KES
REFERENCES

CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL [Aki09]

Agrawal:2002:WRD


Armknecht:2003:AAC


Akinwande:2009:AHC


Amir:2004:PGK


Agrawal:2002:PP


Acicmez:2006:PSB

Onur Aciicmez, Çetin Kaya Koç, and Jean-Pierre Seifert. On the power of simple branch prediction analysis. Technical report, School

**REFERENCES**


**Agrawal:2004:OPE**


**Amadio:2000:RPC**


**Aoki:2000:FIA**


**Atallah:2004:ALA**


REFERENCES

1. Adams:2007:SAC


3. Anderson:2004:BRR


5. Anderson:2008:SEG

6. Aura:2001:RAC
REFERENCES

Anonymous:2000:AIH


Anonymous:2000:AIah


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


Anonymous:2001:ANT

Anonymous:2001:AWB


Anonymous:2001:AIgb


Anonymous:2001:RAC


Anonymous:2001:EDS


Anonymous:2001:EER


Anonymous:2001:EMB


Anonymous:2001:LBS

Anonymous. Looking on the bright side of black-box cryptography (transcript of discussion). *Lec-
REFERENCES


Anonymous. Products: Palm Digital Media’s eBook publishing tools; Veridicom’s fingerprint authentication module; high-speed de-


Anonymous. Review of US bombes. *IEEE An-
Anonymous: 2003: TMC
[Ano03a]

Anonymous: 2003: NAW
[Ano03b]

Anonymous: 2003: NUP
[Ano03c]

<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>1750</td>
<td>L. Euler</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. Welch, Jr.</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>1997</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>Armengaud et al. (GIMPS)</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud et al. (GIMPS)</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>C. T. Clarkson, Woltman, and theigner (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 Boone (GIMPS)</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich, George Woltman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo (GIMPS)</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, George Woltman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, George Woltman, Scott Kurowski, and others</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>
2004. CODEN ????  ISSN 0965-2590.


Anonymous:2008:KAD

Anonymous:2008:RCB

Anonymous:2008:RES

Anonymous:2008:SHS

Anonymous:2009:DSS

Anonymous:2012:SHS

Anonymous:2013:DSS
Anonymous. Digital Signature...

Ateniese:2001:SRC


ANSI:2005:AXP


Abe:2000:PSP

REFERENCES

Abe:2002:SVK


Alomair:2009:ITS


Appenzeller:2005:IBE


Applebaum:2007:CCP


Alwen:2005:IFR


Abdalla:2000:NFS

REFERENCES


REFERENCES


Arnold:2001:AWB


Agrawal:2003:MCA


Abe:2001:SPA


Adelsbach:2001:ZKW


Agung:2001:ICI

[AS01c] I. Wiseto Agung and Peter Sweeney. Improvement and comments on image wa-


REFERENCES


[Blanton:2006:SRF] [Bai08] Thomas Baignères. *Quant-
REFERENCES

Quantitative security of block ciphers: designs and cryptanalysis tools. Thèse, Faculté informatique et communications IC, Programme doctoral Informatique, Communications et Information, Institut de systèmes de communication ISC (Laboratoire de sécurité et de cryptographie LASEC), École polytechnique fédérale de Lausanne EPFL, Lausanne, Switzerland, 2008. 243 pp.


[Ban00a] Nicholas Baran. News and views: 108-bit elliptic curve cryptographic key found; new algorithm cracks the stock market; first complete Babbage printer unveiled; XrML view to be digital rights standard; PKWare founder [phil katz] dies unexpectedly. Dr. Dobb’s Journal of Software Tools, 25(7):18, July 2000. CODEN DDJOEB. ISSN 1044-789X.

[Ban00b] Nicholas Baran. News and views: More on tiny transistors; Open Source repository launched; design contest promotes new software tools; and 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/.

[Ban00c] 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.

Barr:2002:IC


Barken:2003:HSY


Barron:2005:DWP


Barkan:2006:CCP


Barker:2006:ROA


Bard:2009:AC


Bauer:2000:DSM

Friedrich Ludwig Bauer. Decrypted secrets: methods


REFERENCES


REFERENCES


[BBB09] Daniel J. (Daniel Julius) Bernstein, Johannes Buchmann, and Erik Dahmen, editors. *Post-quantum cryptography: [First Interna-
REFERENCES

124


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


REFERENCES


REFERENCES


[BCH00] Michael Brown, Donny Cheung, Darrel Hanker-
REFERENCES


[102x681] REFERENCES

129


Breunesse:2005:FMS


Boneh:2007:CCS


Butler:2006:FAK


Barni:2005:DWI


Bao:2005:PSS


Barak:2005:SCA

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

[130]


Bresson:2001:PAG


Bresson:2002:GDH


Bresson:2003:GB

REFERENCES


REFERENCES

Bourbakis:2003:SBC


Bozzano:2004:AVS


Burmester:2004:HPK


Buchmann:2008:PQC


Biryukov:2003:CS

REFERENCES


Blundo:2003:COT


Bolosky:2000:FSD


Bao:2001:SPD


Boneh:2001:LBM


Bodei:2002:PAP


Bodei:2005:APS

C. Bodei, P. Degano, R. Focardi, and C. Priami. Authentication primitives for secure protocol specifica-
REFERENCES

134


Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES variants with


[BDQ04] Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On multiple linear approximations. In Franklin [Fra04], pages 1–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN
REFERENCES

Baldwin:2009:PSS


Buchmann:2009:HBD


Bertolotti:2008:ERA


Boneh:2001:MFR


Bao:2004:PKC

REFERENCES


REFERENCES


[Ben02] Messaoud Benantar. *Introduction to the Public Key...
REFERENCES


REFERENCES


REFERENCES


REFERENCES

0167-8191 (print), 1872-7336 (electronic).


REFERENCES

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

Biham:2002:DCQ


Brown:2007:SAN


Bugliesi:2007:SIT


Blaszczyk:2008:NMT


Blaszczyk:2009:EVT


Barthe:2009:FCC

Gilles Barthe, Benjamin Grégoire, and Santiago Zanella.
REFERENCES


Boneh:2007:SEI


Bennett:2002:ESE


Bogomjakov:2008:PMD


Bertoni:2003:EAA

REFERENCES


REFERENCES


[BH00a] Robert Beck and Steve Holstead. FOKSTRAUT and Samba — dealing with authentication and performance issues on a large-scale Samba service. In USENIX [USE00c], page ?? ISBN 1-880446-13-8. LCCN ????
Bialaski:2000:SLN

Barak:2005:MAP

Badra:2006:KEA

Backhouse:2003:TOT

Bajard:2004:FRI

Barkol:2005:SCC
REFERENCES


REFERENCES


Beimel:2000:RSC

[BIM00]


Biryukov:2007:FSE

David Bishop. Introduction

Bishop:2003:ICJ


Bajard:2005:AOP


Bajard:2003:EMG

Bajard:2000:RSC

Beimel:2000:RSC


Bajard:2005:AOP


Bajard:2003:EMG

Bajard:2000:RSC

Beimel:2000:RSC


Bajard:2005:AOP


Bajard:2003:EMG

Bajard:2000:RSC

Beimel:2000:RSC


[Barkol:2008:CPR]


[Blaser:2002:PCC]


[Boneh:2000:WTE]


[Bjorn:2005:BHM]

REFERENCES

151

Backes:2002:DCS

Boni:2000:NGT

Burnside:2005:CCP

Barker:2006:RRN

Breveglieri:2006:GEI
L. Breveglieri and I. Koren. Guest Editors’ introduction:
REFERENCES


Barker:2007:RRN


Barreto:2002:EAP


Breveglieri:2007:OCA


Bellare:2004:BPR


Bajard:2009:SRB

REFERENCES


REFERENCES

Blanchet:2001:ECP


Blanchet:2002:SAS


Blaze:2001:LYS


Blaze:2002:CI


Blaze:2003:FCI


Burmester:2009:UCR

[BLDT09] Mike Burmester, Tri Van...

Bleumer:2007:EPS


Bao:2006:CIB


Berbecaru:2001:CPK


Brassard:2000:SAP


Bozga:2006:PBA

L. Bozga, Y. Lakhnech, and M. Périn. Pattern-

**Buchmann:2009:PQC**


**Banks:2001:CAS**


**Blunden:2009:RAE**


**Batina:2001:AWD**


**Blomer:2001:LSE**

Johannes Blömer and Alexander May. Low secret exponent RSA revisited. Lecture Notes in Computer Science, 2146:4–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
REFERENCES


Burke:2000:ASFb


Burke:2000:ASFc


Boneh:2000:GRK


Biehl:2000:DFA


Boyd:2001:ECB


Boyko:2000:PSP

[MP00] Victor Boyko, Philip MacKen-


[BN00a] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations


**REFERENCES**


[Bon03] Dan Boneh, editor. *Advances in Cryptology—CRYPTO*
REFERENCES


REFERENCES


REFERENCES

Bellare:2002:GSI

Barbancho:2003:CAC

Buchbinder:2003:LUB

Bellare:2004:KEA

Blanchet:2005:VCP
REFERENCES

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


[BPR08] D. Boneh, P. Papakonstantinou, C. Rackoff, Y. Vahilis, and B. Waters. On the im-


Black:2000:CMA


Black:2001:CAF


Black:2002:BCM


Bellare:2004:CBG

REFERENCES


Black:2002:BBA


Bierbrauer:2000:AIW


Butler:2009:LIB


Biryukov:2000:CTM


Brustoloni:2006:LEN


Barrett:2001:SSS

Daniel J. Barrett and Richard E. Silverman. SSH: The


REFERENCES


REFERENCES


REFERENCES

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

Buchmann:2002:ICP


Barak:2003:TRN


Biryukov:2001:RTC


Biehl:2002:NDP

REFERENCES


REFERENCES


[Buh06] Ileana Buhan. Feeling is believing: a location limited channel based on grip pattern biometrics and cryptanalysis. CTIT technical report 06-29, Centre


REFERENCES

for Telematics and Information Technology, University of Twente, Enschede, The Netherlands, 2006. 10 pp.


Bulygin:2009:PSS


Burmansson:2000:TCY


Burnett:2001:CB


Bury:2003:SAE


Burke:2002:IWA


Boesgaard:2004:RNH

Baker:2007:ISU


Blake-Wilson:2002:RUE


Butler:2000:NSA


Bellare:2003:FSP


Bar-Yossef:2004:ESQ


Bar-Yossef:2008:ESQ

REFERENCES


Carrington:2002:EDS


Staff:2003:NTC

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

Staff:2006:NTS

REFERENCES


[Can06b] Anne Canteaut. Open problems related to algebraic attacks on stream ciphers. In Ytrehus [Ytr06], pages 120–134. ISBN 3-540-35481-
REFERENCES


[CB01] Juan David González Cobas and José Antonio López

Cooper:2005:AAP


Chandramouli:2006:BPA


Cachin:2000:OFS


Chan:2001:CRP


Carline:2002:NWT

REFERENCES


Chang:2002:SLI
REFERENCES

820–832, August 15, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chang:2005:EAP


Comon:2005:TAO


Crandall:2005:SAM


Chen:2008:SNI


Chang:2009:FDI


Chan:2001:WEF

REFERENCES

Collberg:2004:DPB


Chen:2004:TPM


Chai:2007:EIB


Chang:2005:DSM


Cattaneo:2001:DIT


Chang:2004:IDA


Chang:2004:SOT

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

**Chang:2009:PCC**


**CCL09**

**Christianson:2001:PKC**


**CCM01**

**Choi:2005:JMA**


**CCL09**

**Christianson:2002:SPI**


**CCM05**

**Christianson:2005:SPI**

Bruce Christianson, Bruno Crispo, James A. Malcolm,


Massimo Caboara, Fabrizio Caruso, and Carlo Traverso. Gröbner bases for public key cryptography. In Jeffrey [Jef08], pages 315–324. ISBN 1-59593-904-0. LCCN ???.


Carpenter:2000:CB


Cramer:2001:SDL


Cimato:2007:CVC

S. Cimato, R. De Prisco,
REFERENCES


REFERENCES


Cramer:2001:MCT

[CDR01]

Chapman:2001:PEA

[CDTT05]

Chen:2005:NVW

[Cer04a]

Ceravolo:2004:ERH
REFERENCES

Certicom:2004:CCC


Cer04b

Certicom, 5520 Explorer Drive, 4th Floor Mississauga, Ontario, L4W 5L1 Canada. Published quarterly.

Canetti:2001:UCC


Cramer:2002:OBB


Cohen:2006:HEH


Cohen:2006:HEH


Cohen:2006:HEH

REFERENCES

192

How to achieve a McEliece-based digital signature scheme.


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]

[CGK+02]

[Chen:2008:OVBa]

[Crosby:2002:CHB]
[CGJ+02]

[Clarke:2002:UCP]

[CGH01]

[CGHG06]

[CGL+08a]

[Crosby:2002:CHB] [CGJ+02]

Chen:2008:OVBB


Chen:2008:OVBC


Caballero-Gil:2007:PSC


Canovas:2002:DSB

REFERENCES


REFERENCES

Chen:2001:SFW  

Chien:2007:SUL  

Chung:2007:ASF  

Chung:2007:MRA  

Chaum:2004:VSB  

Chan:2005:MCM  
REFERENCES

Chandra:2005:BWS


Chakrabarti:2007:GCS


Chang:2001:NEA


Chen:2004:MCK


Chen:2005:EUG


Chen:2000:JCT


Chen:2001:DEU

Chaur-Chin Chen. Data encryption using MRF with
an RSA key. *Lecture Notes in Computer Science*, 2195:399–??, 2001. [Che02]

Chen:2001:PDP


Chen:2001:NVR


Cheng:2003:PPO


Chen:2004:IAM


Robert S. Coulter, George Havas, and Marie Henderson. Giesbrecht’s algorithm, the HFE cryptosystem and Ore’s \( p^t \)-

Choi:2009:KDK


Chien:2008:SCA


Coron:2001:GGC


Coron:2001:OCC

REFERENCES

Coppersmith:2002:CSC


Canetti:2003:FSP


Canetti:2005:ASN


Cheon:2008:PST


Chang:2002:IBO

Chao:2009:HCS


Chen:2002:CPK


Choi:2006:CHP


Christianson:2000:SPI


Chowdhury:2008:CBG

REFERENCES

Christianson:2001:SPI

Canetti:2005:HAW

Chen:2002:AMT

Cornea:2002:SCI

Churchhouse:2002:CCJ
Robert F. Churchhouse. Codes and Ciphers: Julius Caesar, the Enigma, and the Internet. Cambridge University Press, Cambridge,
REFERENCES


Canvel:2003:PIS


Chang:2005:ILW


Chang:2005:NMS

Chang:2005:NMS


Cimato:2002:DAP


Cirstea:2001:SAP

REFERENCES


Cheon:2003:PTA


Chien:2003:HA1


Chien:2003:RSA


Chien:2004:IAM


Chen:2005:EDS


Cornwall:2004:AAM

[LCAK+04] Linda A. Cornwall, Jens Jensen, David P. Kelsey, Ákos Frohner, Daniel Kouřil, Franck Bonnassieux, Sophie Nicoud, Károly Lőrentey, Joni Hahkala, Mika Si-


[Coron:2002:UPS] Jean-Sébastien Coron, Marc

Chepyzhov:2001:SAF


Chien:2001:MRL


Chien:2002:SAI

[Ran Canetti and Hugo Krawczyk. Security analysis of IKE’s signature-based key-exchange protocol. In]{[CK02a]}
REFERENCES


[Canetti:2002:UCN]


[Cheon:2002:IID]


[Chung:2003:EPX]


[Chun:2003:DLC]

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


Cox:2005:DWT


Chen:2009:SRP


Coppersmith:2000:KRF


Coron:2000:FLA

REFERENCES


REFERENCES


Chevalier:2008:CRS

Cachin:2009:TC

Chen:2005:CLR

Chen:2007:CRA

Chen:2000:IBD

Camenisch:2001:IES


REFERENCES

Chang:2004:CGS

Chang:2004:IDM

Chang:2004:RFB

Chien:2009:EBL

Chandramouli:2007:ISS

Camenisch:2005:FTO
REFERENCES

October 2009. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

[Clark] Clark:2000:TNE


[Clark] Clark:2000:LNC

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.

[Chen] Chen:2008:RCE


[Chang] Chang:2001:FAM


Dong Hyeon Cheon, Sang Jin Lee, Jong In Lim, and Sung Jae Lee. New block

Canetti:2002:UCT

Chen:2009:AKD

Chang:2007:SIH
CODEN FUMAI.J. ISSN 0169-2968 (print), 1875-8681 (electronic).

Clulow:2003:SP

Czumaj:2002:PTA
http://link.springer-ny.com/link/service/series/0558/bibs/2380/23800973.htm;
REFERENCES


Camenisch:2000:CSS


Chevallier-Mames:2005:ECB


Cox:2002:FYE


Courtois:2003:AAS


Cojocaru:2005:ISM

[CMB02] Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom. Digital watermarking. Morgan Kaufmann series in multimedia information and systems. Morgan Kaufmann
REFERENCES


[CMB+05] 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).


[CMJP03] Benoît Chevallier-Mames, Marc Joye, and Pascal Paillierinst. Faster double-size

Chao:2000:CHC


Cid:2006:AAA


Caputo:2009:DIT


Crawford:2002:FEE

Coron:2004:SSL


Ciet:2003:PFI


Catalano:2002:HHL


Correia:2006:CAB


Czernik:2009:CRN

Cobb:2004:CD


Cochran:2001:NVS


Cocks:2001:IBE


Cochran:2002:NVSa


Cochran:2002:NVWB

REFERENCES


Coppersmith:2000:C


Copeland:2004:COO


Copeland:2004:ETS


Copeland:2005:CSB


Copeland:2006:CSB


Corella:2000:FIT

REFERENCES

Coron:2000:ESF


Coron:2002:SPP


Coron:2006:WC


Cosgrave:2000:NTC


Costlow:2003:BIM


Courtois:2001:EZK

REFERENCES

 Courtois:2003:FAA


 Courtois:2004:FSB


 Courtois:2002:CBC


 Courtois:2003:AXA

REFERENCES

Chatzikokolakis:2007:FAP


Cimato:2006:PVC


Chow:2004:UDL


Chen:2004:SEP


Catalano:2004:IIP


Jason Crampton. Understanding and develop-

Crenshaw:2000:SPK


Crowley:2001:MFL


Chhabra:2009:MSP


CRI:2000:DPA


Cramer:2000:SSB


Cramer:2002:UHP

REFERENCES


Cvejic:2005:IRL


Capaldi:2007:ADI


Chakrabarti:2007:PBA


Chatterjee:2007:CSC


Casey:2008:IFD


Chang:2008:DAP

REFERENCES

[Cusick:2009:CBF]

[CSK+08]

[Cai:2007:CSM]

[Crandall:2005:DUV]

[Chen:2008:CCS]

[Chung:2009:ISA]
REFERENCES

Collberg:2002:WTP

Coron:2003:NAS

Chen:2008:BUK

Chu:2008:EOT

Chou:2009:ATI

Crawford:2001:FPV
Diane Crawford, Thomas Tiahrt, Moti Ben-Ari, Matt

**Chiang:2008:CPB**


**Chang:2004:ASS**


**Cheung:2001:TPS**


**Collberg:2007:DGB**


**Chen:2009:FCV**

REFERENCES


REFERENCES

Canteaut:2004:PCI

Canda:2001:SBC

Chang:2002:ATI

Chess:2007:SPS
Brian Chess and Jacob West. Secure programming with static analysis. Addison-Wesley software security series. Addison-Wesley.


Y. Choie and D. Yun. Isomorphism classes of hyper-

Chen:2005:ENB


Chang:2008:EBD


Chang:2001:NSS


Chang:2000:SAG


Chang:2005:SAK


[CZK05] 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
REFERENCES

Dodis:2003:CAA

Dale:2001:BSA

Damgaard:2000:ECZ

Damaj:2007:PAD

Danielyan:2001:AAE

Danas:2002:CUS

Davis:2001:ISV

Davis:2001:DSA
Don Davis. Defective Sign & Encrypt in S/MIME,
REFERENCES


Davis:2001:DSE


Davis:2007:AAA


DeBrosse:2004:SBU


DeBorde:2007:STF


Desmedt:2001:ERD


Doyle:2006:SCK

Barry Doyle, Stuart Bell, Alan F. Smeaton, Kealan McCusker, and Noel E. O’Connor. Security considerations and key negotiation techniques for power
constrained sensor networks.  
CODEN CMPJA6.  
ISSN 0010-4620 (print), 1460-2067 (electronic).  
URL http://
comjnl.oxfordjournals.org/cgi/content/abstract/49/4/443;

Sabrina de Capitani di Vimercati, Paul Syverson, 
and Dieter Gollmann, editors.  
Computer security — ESORICS 2005: 10th European symposium on research in computer security, 
Milan, Italy, September 12–14, 2005: proceedings, 
volume 3679 of Lecture Notes in Computer Science.  
CODEN LNCSD9.  
ISSN 0302-9743 (print), 1611-3349 (electronic).  
LCCN ????.

Annalisa De Bonis and Alfredo De Santis.  
Randomness in visual cryptography.  
Lecture Notes in Computer Science, 1770:626–??, 2000.  
CODEN LNCSD9.  
ISSN 0302-9743 (print), 1611-3349 (electronic).  
URL http:
//link.springer-ny.com/link/service/series/0558/
bibs/1770/17700626.htm;
http://link.springer-ny.com/link/service/series/
0558/papers/1770/17700626.pdf.

Mehmet Emin Dalkılıç and Gökhan Dalkılıç.  
On the cryptographic patterns and frequencies in Turkish language.  
Lecture Notes in Computer Science, 2457: 144–??, 2002.  
CODEN LNCSD9.  
ISSN 0302-9743 (print), 1611-3349 (electronic).  
URL http://
//link.springer.de/link/service/series/0558/bibs/
2457/24570144.htm; http://link.springer.de/link/
service/series/0558/papers/2457/24570144.pdf.

Annalisa De Bonis and Alfredo De Santis.  
Randomness in secret sharing and visual cryptography schemes.  
CODEN TCSCDI.  
ISSN 0304-3975 (print), 1879-2294 (electronic).

Adama Diene, Jintai Ding, Jason E. Gower, Timothy J. 
Hodges, and Zhijun Yin.  
Dimension of the linearization


Desai:2000:SAN


Dewson:2008:BSS


Dhem:2001:HSS


Delgado:2007:SCD

REFERENCES

URL http://proceedings.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=APCPCS00009639000002000965000001&
idtype=cvips.

Domingo-Ferrer:2000:SCR


Domingo-Ferrer:2001:CDS


Durante:2000:CAC


Durante:2001:CWR


DePalma:2004:CCS

REFERENCES


Dodis:2003:IRP


DeSantis:2004:CKA


Domingo-Ferrer:2006:SCR


Domingo-Ferrer:2007:ASC


Damgaard:2004:ZKP

Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstand-ing quantum attacks. In Franklin [Fra04], pages 254–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN ???
REFERENCES


REFERENCES

DiRaimondo:2005:NAD


Dodis:2004:REK


Devanbu:2003:ADP


Devanbu:2004:FAX


Dorrendorf:2007:CRNa

Leo Dorrendorf, Zvi Guterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system.
REFERENCES


[DHMR07] Vanesa Daza, Javier Herranz, Paz Morillo, and Carla

**DHR00**

**DiCrescenzo:2003:SOS**

**Damgaard:2005:CRM**

**DiCrescenzo:2001:SOS**

**DiCrescenzo:2000:CSG**
Giovanni Di Crescenzo. Sharing one secret vs. sharing many secrets. In *Secure Networks: Proceedings of the Second Workshop*, pages 112–??. CODEN ????. ISSN ????.
REFERENCES


REFERENCES


[DJ06] St´ephanie Delaune and Florent Jacquemard. Decision procedures for the security of protocols with probabilistic encryption against offline

[DK02] Donsez:2001:TMA


[DK05] [DK01]


Delfs:2002:ICP


Dodis:2005:CCS

REFERENCES


REFERENCES

abstract.html; http://www.elsevier.nl/cgi-ng/10/41/16/180/21/34/article.pdf.


REFERENCES

Diffie:1998:PLP


Diffie:2007:PLP


deLeeuw:2000:CSD


deLeeuw:2007:HIS


DelLungo:2005:GSP


Daemen:2009:CAE

REFERENCES


Dowd:2007:ASS


Denev:2009:SFQ


Ding:2007:ESD


CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Damgaard:2000:INC


Durfee:2000:CRS

REFERENCES


REFERENCES

Doncel:2007:ODS

Dwork:2003:MFM

Dwork:2005:PPW

Dodis:2004:IPC
REFERENCES

[Dh00]

[De02]

[Da04]

[DP07]

[DP08]

[DPR01]
REFERENCES


[DR01] Joan Daemen and Vincent Rijmen. Algorithm al-


REFERENCES

Daemen:2002:FSE


Ding:2002:HEE


Dray:2000:NPA

Dreyfus:2000:PUC


Driscoll:2002:BER

[Dr02] Kevin Driscoll. BeepBeep: Embedded real-time encryption. Lecture Notes in
REFERENCES


Diqun:2009:QSP


DelRey:2005:SSS


Dobbertin:2005:AES


Devanbu:2000:CVT


Dodis:2002:NUO

REFERENCES

org/iel5/8411/26517/01181962. pdf?isnumber=26517&prod-
CNF&arnumber=1181962&arSt=
+376&ared=+385&arAuthor=
jp?isnumber=26517&arnumber=
1181962&count=82&index=
38. IEEE Computer Society
Order Number PR01822.

[DS03] Paolo D’Arco and Douglas R. Stinson. Fault toler-
ant and distributed broadcast encryption. In Joye
[Joy03b], pages 263–280. CODEN LNCS9D. ISBN 3-
540-00847-0. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25 CS22 2003. URL http:
//link.springer-ny.com/link/service/series/0558/
issn=0302-9743&volume=2612.

[DS05a] J. Ding and D. Schmidt. Rainbow, a new multivari-
able polynomial signature scheme. Lecture Notes in
Computer Science, 3531: 164–175, 2005. CODEN
LNCSA9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).

[DS05b] Yevgeniy Dodis and Adam

Smith. Entropic security and the encryption of
high entropy messages. In Kilian [Kil05], pages 556–
CODEN LNCSD9. ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743 (print), 1611-3349 (elec-
issn=0302-9743&volume=3378; http://www.springerlink.

[DS06] Cunsheng Ding and Arto
Salomaa. Secret sharing schemes with nice access
structures. Fundamenta Informaticae, 73(1–2):51–63,
October 2006. CODEN FU-
MAAJ. ISSN 0169-2968 (print), 1875-8681 (elec-
tronic).

[DS08] Itai Dinur and Adi Shamir.
Cube attacks on tweakable black box polyno-

mials. Technical report, Computer Science Depart-
ment, The Weizmann In-
stitute, Rehobot 76100, Is-
org/cube-attacks.pdf.

[DSP01] Igor Djurovic, Srdjan Stankovic
and Ioannis Pitas. Dig-

(Dodis:2001:PAS)


(DS01)


(Duggan:2004:TBC)


(Dujella:2008:VWA)


(Dujella:2009:VWA)


(Dunkelman:2006:TCB)

Orr Dunkelman. *Techniques for cryptanalysis of block ci-

**Duranti:2001:LTP**


**Duwell:2003:BRB**


**Dawson:2005:PCM**


**Drutarovsky:2008:CSC**


**Levy-dit-Vehel:2006:WC**


**Du:2001:OKS**

Wei Zhang Du and Xin Mei Wang. One kind of secret-


REFERENCES


[DwWmW05] Qiong Dai, Xiao Xiang Zou, and Zhu Kai Luo. Cracking a data encryption and decryption system using multivalued logic array. *Chinese
REFERENCES


REFERENCES


ECMA:2000:EPIb


[EGK08]


Echizen:2005:PAV


Eghlidos:2000:SLB


Elmallah:2008:LK


Epstein:2003:DIT

REFERENCES


Elbirt:2009:UAC


Elliott:2004:QC


Everitt:2003:JBI


English:2000:MNDb


England:2002:AOO

Elbirt:2005:ILD


Eisenbarth:2007:SLC


Erickson:2001:EDD


Erickson:2008:HAE


Ellison:2000:TRP


Ellison:2000:IRRa

Eberle:2005:ANG


Enck:2005:EOF


Ettinger:2002:QQC


Elbirt:2000:FIP


Edman:2009:AES


Ebringer:2000:PAP


Ebringer:2000:PAP
REFERENCES


REFERENCES


N. Ferguson. Semi-equivalent keys in MARS. In ????, editor, Third AES Candidate Conference, page ?? ????.


REFERENCES


REFERENCES


[Fil00] Eric Filiol. Decimation attack of stream ciphers.
REFERENCES

Finnigin:2006:CPN

FIPS:2000:DSS

FIPS:2001:AES

FIPS:2001:SRC
REFERENCES


REFERENCES


**Fluhrer:2002:CMB**


**Fluhrer:2002:CSP**


**Feng:2006:ISC**


**Fehr:2002:LVD**

REFERENCES

[Fuller:2002:LRA]

[Franklin:2002:PAS]

[Fournier:2003:SEA]

[Fouque:2003:AUR]

[Fluhrer:2001:WKS]
REFERENCES


REFERENCES

Frincke:2006:ESI


Fujisaki:2001:ROS


Fox:2000:NTFb


Freking:2000:MMR


REFERENCES


REFERENCES

Ferguson:2000:CEI

Fouque:2001:FDT

Friedlander:2001:DDH

Furukawa:2001:ESP

Fischer:2002:NFC

Ferguson:2003:CEI
Niels Ferguson and Bruce

Ferguson:2003:PC

Fundulaki:2004:SYD

Fuster-Sabater:2001:EAG

Fu:2001:DCA

Ferguson:2001:SAR
REFERENCES


[FW09] Martin Feldhofer and Johannes Wolkerstorfer. Hardware implementation of symmetric algorithms for RFID

**Fan:2008:RSB**


**Feng:2005:NMS**


**Fitzi:2004:PSB**


**Fan:2004:PPI**


**Furnell:2006:RPS**

REFERENCES


Ganti:2008:PAL


Garrett:2001:MBC


Garfinkel:2003:KDG


Garman:2003:KDG


Garrett:2004:MCT


Garrett:2005:CP


Gasarch:2001:BRBa

William Gasarch. Book review: The Codebreak-

Gaudry:2002:CCS


Gavinsky:2008:CIC


Guine:2009:NTR


Guajardo:2001:EIE


Golic:2002:LCB

REFERENCES


REFERENCES


Gennaro:2000:IPR
REFERENCES


[Gen04b] Craig Gentry. How to compress Rabin ciphertexts and signatures (and more). In Franklin [Fra04], pages 179–?? CODEN LNCSD9.


REFERENCES


REFERENCES


Gonzales:2000:LBC


Gilbert:2000:SAR


Gilbert:2001:SAR


Gaudry:2006:ACM


Grabner:2005:ALC

Peter J. Grabner, Clemens Heuberger, Helmut Prodinger, and Jörg M. Thuswaldner.

**Gong:2001:GPK**


**Gennaro:2001:RCV**


**Gennaro:2002:RSM**


**Gillespie:2007:WSC**


**Giraud:2006:RIR**


**Gebhardt:2005:NPV**

M. Gebhardt, G. Illies, and W. Schindler. A note on the practical value of single hash function collisions for special
file formats. In NIST Cryptographic Hash Workshop 2005, page ?? ??, ???. [GJKR03]
2005. ISBN ?? LCCN ???.

Gordon:2003:ATS


Gordon:2004:TEA


Ganapathy:2005:APA


Gentry:2001:CNS


Gennaro:2003:SAP


Gallagher:2006:HSB


REFERENCES

Garay:2007:RCA

[102x681]


Gertner:2000:RBP

[129x436]


Guneysu:2008:CC

[128x243]


Gorodetsky:2005:CNS


Goubault-Larrecq:2000:MAC

Goldreich:2001:SKG


Gennaro:2003:FPB


Garrett:2005:PKC


Gennaro:2006:FPB


Goshi:2006:ADM


Gassend:2004:IAI


Rosario Gennaro and Daniele Micciancio. Cryptanalysis
REFERENCES


[Gilbert:2002:CS]

[Gilbert:2002:NRP]

[Galbraith:2003:IAU]

[Gorrieri:2004:SFR]

[Giuliano:2000:ISC]
Genevieve Giuliano, James E. Moore II, and Jacqueline Golob. Integrated smart-


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


References

Galindo:2008:ICB


Gopalakrishnan:2001:PWV


Grosek:2001:SPK


Ge:2005:CCO


Gore:2001:CMT


Gratzer:2006:CLE


REFERENCES

Goldreich:2004:FCV

Goldstein:2008:BHO

Gonda:2006:NMR
J. Gonda. The number of the modulo \( n \) roots of the polynomial \( x^v - x^v \) and the RSA. J.UCS: Journal of Universal Computer Science, 12(9):1215–1228, ????. 2006. CODEN ???. ISSN 0948-6968. URL http://www.jucs.org/jucs_12_9/the_number_of_the.
REFERENCES

Good:2000:TAE


Gordon:2002:TCP


Gordon:2005:NSC


Goulding:2009:ESA


Gupta:2008:FAT

Manish Gupta, Amit Pathak, and Soumen Chakrabarti. Fast algorithms for top-k personalized PageRank


REFERENCES


REFERENCES


Grossschadl:2001:HSR


Grossschadl:2003:ASL


Grosch:2002:QC

Gisin:2002:QC


GonzalezVasco:2001:CPK


Garfinkel:2002:WSP


Gentry:2002:HIB


Gentry:2002:CRN


Geiselmann:2003:HSS

REFERENCES


Goodrich:2002:EDD


Goodrich:2003:ADS


Goodrich:2008:NFI


Guttman:2004:FAP


Guar:2005:PPL


Gumz:2004:BRH

Guillou:2001:CAP


Gutmann:2000:OSC


Gutmann:2002:CFP


Gutmann:2002:DVC


Gutmann:2004:CSA


Gutmann:2004:SPK

REFERENCES

Gutman:2004:ATD


Gutmann:20xx:ESR


Granger:2005:DLP


Garera:2009:CTG


Gassend:2008:CPR


Gisin:2000:LCQ

guoxiang:2001:ifb


gebotsys:2008:eaaw


Goldberg:2008:pqm


heys:2000:sac


Haddad:2000:AUA


Harvey:2000:EMA


Hare:2001:RUPa

Hare:2001:RUPb


Harrington:2005:NSP


Harris:2005:GHE


Hars:2006:MIA


Harman:2007:PDS


Hars:2007:DIH


Hasan:2000:LTB


Hasan:2001:ECM

[Has01a] M. A. Hasan. Efficient computation of multiplicative inverses for cryptographic applications. In Burgess and

Hasan:2001:PAA


Hassler:2002:JCP


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 SIGS23. ISSN 0097-8418. NOTE FROM ACM: It has been determined that the authors of this article plagiarized the contents from a previously published paper. Therefore ACM has shut off access to this paper.

Hayashi:2006:QIT

REFERENCES


Hwang:2004:NMP


Huang:2008:NCK


Han:2008:PBPa


Han:2008:PB Pb


Henderson:2002:MTS


Halevi:2002:SSE


Han:2009:ICS

Dong-Guk Han, Dooho Choi,


REFERENCES

Herranz:2006:DIB

Herranz:2007:IBR

Heron:2009:AES

Hess:2004:SVE

Hess:2004:GAR

Heys:2003:ASC

Hassler:2000:OFA
REFERENCES

Horvitz:2003:WKA


Horan:2005:NRN


Howgrave-Graham:2003:PKC


Horvitz:2003:WKA


Horan:2005:NRN


Howgrave-Graham:2003:PKC


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2003:IDF

REFERENCES


Howgrave-Graham:2003:HNP


Hendricks:2007:LOB


Handschiuh:2004:SAC


Handschiuh:2005:SAC

Helena Handschuh and M. Anwar Hasan, editors. Selected areas in cryptog-
REFERENCES


**Hong:2004:DCT**


**Hankerson:2000:CTC**


**Hankerson:2001:SIE**


**Hamann:2001:SBA**


**Han:2007:FIE**

Higgins:2008:NSC


Hill:2000:KII


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], pages 216–227. ISBN ???? LCCN ???? ACM order number 475020.

Hirose:2009:SAD


Hinkelmann:2007:CUN


Huhnlein:2001:TPN


Hofmeister:2000:COS


Hiltgen:2006:SIB


Horwitz:2002:THI


Howard:2003:WSC


Hwang:2004:REL


Hohenberger:2005:HSO

Hwang:2005:TAU

Hwang:2005:SHW

Hwang:2005:STH

Howard:2006:SDL

Huang:2007:EPS

Hwang:2008:CPK
Hwang:2000:CBV

Hong:2001:PSA

Han:2002:DMA

Hwang:2003:TRB

Hwang:2004:KAS

Hwang:2005:GTS
Hong:2003:BBP


Herzog:2003:PAK


Hwang:2001:TSB


Hopper:2002:PSS


Hu:2009:TRN

Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU


Harbitter:2002:MAP


Hevia:2002:PSG


Hitchcock:2002:NEC


Hoglund:2004:ESH


Hollar:2005:EWS


Holenstein:2004:CCB


Hankerson:2004:GEC


Huang:2007:MPK


Hastad:2004:SAR

REFERENCES


REFERENCES

Honary:2001:CCI


Hook:2005:BCP


Hoskins:2006:SSE


Horn:2000:APF


Huhnlein:2001:ICB


Han:2002:CMV


REFERENCES

**Hawkes:2000:EMC**


**Hand:2002:MPP**


**Halevi:2003:TEM**


**Hawkes:2004:RVC**


**Hsiao:2004:FCP**

[HR04b] Chun-Yuan Hsiao and Leonid Reyzin. Finding collisions on a public road, or do secure hash functions need secret coins? In Franklin [Fra04], pages 92–?? CODEN LNCS389. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-

[Holenstein:2005:OWS]

[Haitner:2007:SHC]

[Harn:2009:DDB]

[Hromkovic:2005:DAR]
Hromkovic:2009:AAH


Haneberg:2002:MSS


Hemaspaandra:2008:EDA


Hirt:2000:ERF


Hinsley:2001:CIS


Hoffstein:2001:MAD

REFERENCES


REFERENCES

Halderman:2008:LWRa


Halderman:2008:LWRb


Halderman:2009:LWR


Hanaoka:2002:USA


Hanaoka:2006:USA

REFERENCES


Hess:2001:TTH


Hernandez:2004:STN


Hsu:2005:UFR


Hasan:2009:PHF


Hanaoka:2000:USD

REFERENCES


Stephen Roderick Hines, Gary Tyson, and David Whalley. Addressing instruction fetch bottlenecks
REFERENCES


**Hofheinz:2005:CTN**


**Hughes:2004:ISE**


**Huhnlein:2000:EIC**


**Hunt:2005:JFE**


**Husemann:2001:SSC**


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


REFERENCES


[Hwa05] Hsu:2004:EPS


[Hwa05] Hsu:2005:SCT


[Hwa05] Hwang:2000:CYK


[Hwa05] Hwang:2005:ITA

REFERENCES

Henderson:2001:IEV


Hsu:2005:NPM


Hsu:2002:IGT


Hsu:2003:ITP


Hardy:2009:AAC

REFERENCES

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

Hsu:2004:GOS


Harkins:2005:ESU


Hwang:2003:CAL


Yeh:2008:STB


IEEE:2000:ASF


IEEE:2001:ISF


IEEE:2001:EIW


IEEE:2002:PAI


IEEE:2003:PAI

REFERENCES


IEEE:2004:PAI


IEEE:2006:AIS


IEEE:2005:PIS


IEEE:2006:AIS

IEEE Society Order Number P2720.


REFERENCES


REFERENCES

Iwata:2000:PAF  

[IK00]

Iwata:2001:PAF  

[IK01]

Impagliazzo:2003:LRA  

Ichikawa:2000:HEA  
Ishai:2006:CA

Ishai:2007:ZKS

Ishai:2008:CCC

Iyer:2007:TAA

[IKNP03]

[IKOS06]
Klemperer, and Reza Fari-
var. Toward application-
aware security and reliabil-
ity. *IEEE Security & Pri-
February 2007. CODEN ????
ISSN 1540-7993 (print), 1558-4046 (elec-
tronic).

Ioannidis:2005:ACN

[IKY05] John Ioannidis, Angelos
Keromytis, and Moti Yung,
editors. *Applied Cryptog-
raphy and Network Secu-
ritv: Third International
Conference, ACNS 2005,
New York, NY, USA, June
7–10, 2005, proceedings*,
volume 3531 of *Lecture
Notes in Computer Science*.
Springer-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
ISBN 3-540-26223-7 (soft-
cover). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN TK5102.85
A26 2005. URL http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=

Izmerly:2006:CCA

[IM06] Oleg Izmerly and Tal Mor.
Chosen ciphertext attacks on
lattice-based public key en-
cryption and modern (non-
quantum) cryptography in

Izotov:2001:COC

[IMM01] Boris V. Izotov, Alexan-
der A. Moldovyan, and
Nick A. Moldovyan. Con-
trolled operations as a cryp-
tographic primitive. *Lec-
ture Notes in Computer Science*, 2052:230–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2052/20520230.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2052/20520230.
pdf.

Imrey:2003:BRC

[Imr03] Lee Imrey. Book review:
*The Code Book: The Scie-
nce of Secrecy from An-
cient Egypt to Quantum Cryp-
tography* by Simon Singh, Dela-
corte Press, 2000, $15.00,
Queue: Tomorrow’s Com-
puting Today*, 1(9):76, De-
cember/January 2003. CO-
DEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).
Inamori:2002:SPB


Inamori:2002:SPT


Inoue:2005:EST


Intel:2000:IIP


Intel:2003:IRN


Itkis:2001:FSS


Itkis:2002:SSB

Gene Itkis and Leonid Reyzin. SiBIR: Signer-

Irwin:2003:BRBb


ISO:2004:IIIb


Iqbal:2008:CDV


Inoue:2008:FAC

Ishai:2003:PCS


Itoi:2000:SCI


Itoi:2001:SFS


Iwami:2008:AIA


Imai:2000:CPC


Irwin:2005:PAI

Iwamoto:2006:SSR


Iwata:2002:NCP


Iwata:2003:NCP


Imai:2000:PKC


Judge:2002:WWM


Jablon:2001:PAU

REFERENCES


REFERENCES

1993 / Gehan Gunasekara.

Janeczko:2006:TSH

Jankowski:2008:BRBb

Jankvist:2008:TMH

Jennewein:2000:FCQ

Jones:2005:RDF

Johnson:2001:ICS

Jeffrey:2008:PAM


REFERENCES


REFERENCES


JKS02


JL00


JL03

REFERENCES

Juang:2004:FBT


Jeong:2008:PKE


Juang:2001:FBT


Juang:2002:VMA


Jakobsson:2003:FMT


Johansson:2003:PCI

Thomas Johansson and Subhamoy Maitra, editors. Progress in Cryptology—
REFERENCES


REFERENCES

Johansson:2003:FSE [Joh03]

Johnson:2005:OSV [Joh05]

Jolish:2001:EDP

Jones:2008:RAA [Jon08]

Joux:2002:WTP [Jou02]
REFERENCES


**Joux:2004:MIH**


**Joux:2009:AC**


**Joyner:2000:CTC**


**Joye:2003:CPY**


**Joye:2003:TCC**

Jakobsson:2002:MAL


Jaulmes:2002:SHG


Joye:2003:GFA


Jakubowska:2007:MCT


Joye:2004:CHE

Marc Joye and Jean-Jacques Quisquater, editors. Cryptographic Hardware and


Matjaz B. Juric, Ivan Rozman, Bostjan Brumen, Matjaz Colnaric, and Marjan Hericko. Comparison of performance of Web services, WS-Security, RMI,

Jin:2001:WCS

Jaworski:2009:RKP

Jain:2009:PQR

Jarecki:2005:FSP

Jongkook:2001:NUS
REFERENCES


REFERENCES

Junod:2005:SCB

Pascal Junod. Statistical cryptanalysis of block ciphers. Thèse sciences, Faculté Informatique et communications IC, Section des systèmes de communication (Institut de systèmes de communication), EPF Lausanne, Lausanne, Switzerland, 2005. 267 pp. URL http://library.epfl.ch/theses/?nr=3179.

Jutla:2001:EMA


Juels:2005:APD


Jeng:2006:EKM


Jin:2005:EAW


Joye:2001:NMM


Jain:2009:NBC


Jiang:2005:TMD

Zhengtao Jiang, Yang Zhan, Dan Chen, and Yumin Wang. Two methods of directly constructing probabilistic public-key encryption primitives based on third-order LFSR sequences. Applied Mathematics and
REFERENCES


Kadrich:2007:ES


Kahn:1967:CSSa


Kahn:1967:CSSb


Kahn:1974:C


Kahn:1996:CSS


Kah:2006:TSQ


Kaliski:2001:RDS


Kayem:2008:RCK

REFERENCES

[**Kanda:2001:PSE**]

[**Kapera:2005:MRP**]

[**Karski:2001:SSS**]

[**Katzenbeisser:2001:RAR**]
Stefan Katzenbeisser. Recent advances in RSA cryptography, volume 3 of Advances in information security. Kluwer Academic [KB39]

[**Katz:2005:CBR**]

[**Kendall:1939:TRS**]
Maurice G. (Maurice George)

Kovacich:2000:HTC


Kiely:2006:SSM


Kamvar:2007:DTM


Kim:2009:DCA


Kachris:2003:RLB


Keller:2009:ECC

Maurice Keller, Andrew Byrne, and William P. Marlane. Elliptic curve cryptography on FPGA for low-power applications. *ACM Transactions on Reconfigurable Technology and Sys-
REFERENCES

tems (TRETS), 2(1):2:1–2:??, March 2009. CO-
DEN ??? ISSN 1936-7406 (print), 1936-7414 (elec-
tronic).

claffy:2001:IMM

[kc01] kc claffy. Internet measure-
ment: Myths about Internet data, 2001. URL http://
tems Administration Conference, December 2–7, 2001, 
Town and Country Resort Hotel, San Diego, CA.

Kim:2002:SMA

[KC02] Seongyeol Kim and Ily-
ong Chung. A secure mo-
 bile agent system apply-
ing identity-based digital 
signature scheme. Lecture Notes in Computer Sci-
ence, 2510:588–??, 2002. CODEN LNCSD9. ISSN 
0302-9743 (print), 1611-3349 (electronic). URL http://
link.springer.de/link/service/series/0558/bibs/2510/25100588.htm; http://
link.springer.de/link/service/series/0558/papers/2510/25100588.pdf.

Kieu:2009:HSI

[KC09a] The Duc Kieu and Chin-
Chen Chang. A high 
steo-image quality stegano-
graphic scheme with re-
versibility and high payload 
using multiple embedding 
strategy. The Journal of Sys-
tems and Software, 82(10): 
1743–1752, October 2009. 
CODEN JSSODM. ISSN 
0164-1212 (print), 1873-1228 
(electronic).

Kieu:2009:IAB

[KC09b] The Duc Kieu and Chin-
Chen Chang. An im-
ge authentication based 
on discrete Fourier trans-
form. Fundamenta Infor-
maticae, 97(4):369–379, De-
cember 2009. CODEN FU-
MAAJ. ISSN 0169-2968 
(print), 1875-8681 (elec-
tronic).

Ku:2005:WYR

[KC05] Wei-Chi Ku and Shuai-Min 
Chen. Cryptanalysis of a 
flexible remote user authen-
tication scheme using Smart 
Cards. Operating Systems 
Review, 39(1):90–96, Jan-
uary 2005. CODEN OS-
RED8. ISSN 0163-5980 
(print), 1943-586X (elec-
tronic).
Kim:2007:SBE

Kim:2001:SAC

Ku:2003:WLL

Kang:2001:NHO

Kalker:2004:DWS
REFERENCES


[Keller05] Sharon S. Kellar. NIST-Recommended Random Number Generator Based on
ANSI X9.31 Appendix A.2.4

Kenyon:2002:DNR

Kenyon:2002:HPD

Kettani:2006:CBN

Kelsey:2000:CPL
J. Kelsey, N. Ferguson, B. Schneier, and M. Stay. Cryptanalytic progress: Lessons for AES. In ?????, editor, Third AES Candidate Conference, page ?? ?????, ?????, April 2000. ISBN ????. LCCN ????.

Kiltz:2009:DCC

Katsikas:2004:PKI
REFERENCES

Kaps:2007:CSD


Kovacich:2003:MHC


Kim:2005:SMA


Kato:2008:QSC


Khaw:2005:EDA


Komninos:2001:ESC


REFERENCES

0558/papers/2274/22740237.pdf.


Kim:2002:ISC

REFERENCES


[Kir03] Peter L. Montgomery Kirsten Eisenträger, Kristin Lauter. Fast elliptic curve arithmetic and improved Weil pairing

Kocarev:2001:LMB


Kanade:2005:AVB


Koj:2005:IVA


Kim:2002:NIS


Klein:2003:FOW

REFERENCES


REFERENCES

403


Kelsey:2000:ABA


Khesel:2001:ABA


Kohno:2000:PCR


Kohno:2001:PCR

Nam-Yeun Kim, Dae-Ghon Kho, and Kee-Young Yoo. Inversion/division systolic architecture for public-key cryptosystems in GF($2^m$). Lecture Notes in Computer
Katz:2005:HEP

Katz:2008:IMC

Knill:2002:FPE

Knill:2002:QIP

Ko:2000:NPK
Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo

Klein:2007:BDC

[Bel00]


Kong:2001:AVW


Kiltz:2005:SCM


Kacprzak:2006:CBS


Kalai:2009:SEU

Y. T. Kalai, Xin Li, and A. Rao. 2-source extractors under computational assumptions and cryptography
with defective randomness. In IEEE [IEE09b], pages
IEEE Computer Society order number P3850.

Kim:2002:EPS

[KLY02] Nam-Yeun Kim, Won-Ho Lee, and Kee-Young Yoo.
Efficient power-sum systolic architectures for public-key
cryptosystems in GF(2^m).
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
link/service/series/0558/bibs/2387/23870153.htm;
http://link.springer-ny.com/link/service/series/
0558/papers/2387/23870153.pdf.

Kim:2003:IBP

[KLY03] Hyun-Sung Kim, Sung-Woon Lee, and Kee-Young
Yoo. ID-based password authentication scheme using smart cards and fingerprints.
CODEN OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).

Knudsen:2000:CRA

[KM00] Lars Knudsen and Willi Meier. Correlations in RC6 (abstract only). In
NIST [NIS00], page 9. ISBN ???? LCCN ????
encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf;

Knudsen:2001:CRR

[Knudsen:2001:CRR]

L. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds.
In Schneier [Sch01d], page ??
CODEN LNCSD9. ISBN 3-
Koblitz:2004:OTS

Koblitz:2004:SPK
epubs.siam.org/sam-bin/dbq/article/43919.

[408]

Kornerup:2007:PIS


Kim:2002:ABA


Kakarountas:2006:HSF


Katz:2001:CCA


Klarlund:2001:MIS


REFERENCES

Kol:2008:GEI

Koc:2001:CHEb

Krukow:2005:FCR

Knudsen:2000:TT

Knudsen:2000:TTR

Knudsen:2002:ACE


REFERENCES


Kocher:2002:IS


Koga:2002:GFR


Kurosawa:2001:ICP


Kornblum:2009:IBD


Koshiba:2001:NAS


Koshiba:2001:SRS

Koskinen:2001:NIK


Kovach:2001:BCB


Kovacic:2003:ISS


Katz:2001:EPA


Katz:2009:ESA


Katzenbeisser:2000:IHT

[KP00] Stefan Katzenbeisser and Fabien A. P. Petitcolas, editors. *Information hiding*


REFERENCES


[Kra02b] Rory Krause. Using SSH port forwarding to print at remote locations. Linux Journal, 94:60–62, 64, February 2002. CODEN LIJOFX. ISSN 1075-
Krawczy:2003:SSM


Krawczyk:2005:HHP


Kramer:2007:LCC


Kreitz:2005:OBE


Koeune:2002:FIL

REFERENCES


REFERENCES


Kasper:2009:FTA


Kelsey:2000:YND

REFERENCES

Protecting a mobile agent’s route against collusions / Dirk Westhoff . . . [et al.] — Photuris: design criteria / William Allen Simpson. [KSW06]


Kuribayashi:2000:WSB


Kuribayashi:2001:NAF


Kogan:2006:IER


Ku:2002:IIB


Kobayashi:2007:AIG


Ku:2003:TSA


Kukorelly:2001:PAL


Kun01


Kurosawa:2001:MRP


Kusters:2002:DCP


Kuo:2001:AOS


Kejariwal:2009:ELL

Arun Kejariwal, Alexander V. Veidenbaum, Alexandru Nicolau, Milind Girkar, Xinmin Tian, and Hideki Saito. On the exploitation of

**Koshiba:2000:SEP**


**Knudsen:2002:IC**


**Karlof:2003:HMM**


**Keromytis:2006:COS**


**Kwon:2002:DSA**


**Kwok:2003:WBC**

Sai Ho Kwok. Watermark-

**Kwon:2003:EDS**


**Kumar:2006:ODS**


**Wong:2001:MCC**


See comment and reply [AMRP04, WLW04].

**Kun:2000:SMA**


**Kamat:2009:TPW**


**Katz:2000:CCS**

REFERENCES


[KY09] A. A. Kamal and A. M. Youssef. An FPGA implementation of the NTRU-

Kang:2001:PMT


Kabatnik:2001:LSD


Kamp:2003:DEB


Kamp:2007:DEB


Kumar:2009:UAU

Ajay Kumar and David Zhang. User authentication using fusion of face


REFERENCES


Landau:2004:PNS


Landau:2004:SLE


Laud:2005:STS


Laud:2008:CSC


Laughlin:2008:CRC


Lavington:2006:FCD

IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

**Lavoué: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


Laufer:2000:SSC


Laih:2003:COP


Lin:2004:SOT


Lu:2004:XMS

[Eric Jui-Lin Lu and Rai-Fu Chen. An XML mul-
REFERENCES


**[Lu:2005:ERU]**


**[LC05a]**

**[Lu:2005:NDA]**


**[LC05b]**


**[LCC05]**


**[LCD07]**


**[LCK01]**


Levi:2004:UNC

Lee:2004:DEB

Lim:2009:OPG

Li:2008:CAM

Lu:2005:TUS

Lu:2005:PBM

Lu:2005:RTP
RongXing Lu, ZhenFu Cao, and HaoJin Zhu. A robust $(k,n)+1$ threshold proxy signature scheme based on

**Li:2001:CCB**


**[LD01]**

**Lai:2004:SGS**


**[LD04]**


**[LDD07]**


**[LDH06]**


**Lindquist:2004:JCS**


**Lee:2001:AES**


**Lee:2003:BRBa**
Lee:2003:BRBb


Lee:2003:CS


Lee:2004:SPM


Lee:2004:ACA


Lehtinen:2006:CSB


Lenstra:2001:USM

[Len01] Arjen K. Lenstra. Unbelievable security, matching AES security using public key systems. Lec-


[LHC08] Chua-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. [LHL03a] Cheng-Chi Lee, Min-Shiang

Lin:2003:NRU


Lee:2004:SAA


Lu:2008:PTZ


Liu:2005:DBV


Lee:2009:NCA


Lee:2002:FRU

Lee:2005:NBS


Li:2001:NSA


Li:2005:ABPa


Lieman:2005:CRW


Lin:2000:RTI


Linn:2000:TMM

REFERENCES


Lingmann:2002:DSK [LJ05a]


[LKJL01] Shin-Young Lim, Jeong-Ho Ko, Eun-Ah Jun, and Gang-Soo Lee. Specification and

Lee:2003:PSAa


Lee:2003:PSAb


Lee:2005:NIIW


Lee:2005:ENB


Lee:2004:CUA


Lee:2005:APC

Lee:2005:EVB

Lee:2005:IHA

Lim:2000:GTC

Luo:2004:UUR

Lu:2001:DWC
REFERENCES


Lee:2003:ISC


Lee:2004:FIM


Lee:2004:DIS


Lim:2004:ISC


Lee:2005:CMA

Keon-Jik Lee and Byeong-


Lee:2001:PBG

Lee:2002:RUA

Li:2001:SPD

Lee:2002:SEC


[LSS05b] Sanya Liu, Zhenyu Liu, and Zhongren Su. Securing Web application system: a solution based on SMS for
identifying users. In Han et al. [HYZ05b], pages 104–??.

[LLS+09]

[LLT+04]

[Li:2004:ABP]

[Liu:2008:DEA]

[Liu:2008:SAM]
REFERENCES


Li:2009:ATN


Lee:2006:DCK


Linares:2000:SAM


Lorenz:2002:SSG


Lavasani:2008:IFA


Li:2003:SCE

[LMC+03] Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the sebu-
Lamenca-Martinez:2006:LNP


Leitold:2001:MTN


Lepinski:2005:FZK


Laskari:2005:TTC


REFERENCES


Li:2002:HNP


Loidreau:2000:SMC


Lopez:2006:UPK


Lovering:2001:TKF


Lindell:2000:PPD

Lysyanskaya:2001:AST

Labbe:2002:AIF

Luccio:2002:AC

Lee:2003:CPK

Li:2005:MCK

Law:2009:EEL
Yee Wei Law, Marinuthu Palaniswami, Lodewijk Van Hoesel, Jeroen Doumen,
Pieter Hartel, and Paul Havinga. Energy-efficient
link-layer jamming attacks
against wireless sensor net-
work MAC protocols. ACM
Transactions on Sensor Net-
works, 5(1):6:1–6:??, February 2009. CODEN ????
ISSN 1550-4859 (print),
1550-4867 (electronic).

[LR01] Kerstin Lemke, Christof
Paar, and Marko Wolf, edi-
tors. Embedded security in
cars: securing current and
future automotive IT appli-
cations. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2006. ISBN 3-540-
28384-6. x + 273 pp. LCCN

[LPW06] Li Li, Zhigeng Pan, and
David Zhang. A pub-
lisch mesh watermarking al-
gorithm based on addition
property of Fourier Trans-
form. International Jour-
nal of Image and Graphics
(IJIG), 6(1):35–??, January
2006. CODEN ????
ISSN 0219-4678.

[LPZ06] Lvzhou Li and Daowen Qin.
Determining the equivalence
for one-way quantum fi-
nite automata. Theoretical
Computer Science, 403
CODEN TCSCDI. ISSN
0304-3975 (print), 1879-2294
(electronic).

[LQ08] Liskov:2002:TBC
Moses Liskov, Ronald L.
Rivest, and David Wagner.
Tweakable block ciphers.
In Yung [Yun02a], pages
31–46. CODEN LNCSD9.
ISBN 3-540-44050-X (pa-
erback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2002. URL http://
link.springer.de/link/
service/series/0558/bibs/
2442/24420031.htm; http:
//link.springer.de/link/
service/series/0558/papers/
2442/24420031.pdf.
References


Lin:2000:TPE


Lin:2003:SEOa


Lin:2003:SEOb


Lu:2005:BIW


Li:2005:ABPb


Liang:2009:AIE

Zhenkai Liang, Weiqing Sun,


Henry Lin, Luca Trevisan, and Hoeteck Wee. On hardness amplification of one-way functions. In
REFERENCES

Kilian [Kil05], pages 34–??  CODEN LNCSD9.

Lu:2002:HEA


Lu:2007:NSC


Lucks:2000:ASR


Lucks:2002:SAB


Lucks:2002:VCS

Stefan Lucks. A variant of the Cramer–Shoup cryptosystem for groups
of unknown order. Lecture Notes in Computer Science, 2501:27–??, 2002. [Lun09]


Michael J. Lutz. Bookshelf: Laying the foundation for pervasive computing [Pervasive Computing]; integrated approach to data handling [Exploratory Data Mining and Data Cleaning]; mak-


[Lee04] Narn-Yih Lee and Chien-Nan Wu. Improved authentication key exchange protocol without using one-way

**Liang:2005:PAC**


**Loepp:2005:PIC**


**Lyuu:2005:CIH**


**Lin:2000:PAS**


**Lv:2005:PCA**


**Lv:2005:SMS**

REFERENCES

[Li:2005:IWR]

[LY05]

[LY07]

[Lou:2002:ESA]

[Liu:2007:IFW]
REFERENCES

Lysyanskaya:2002:USV


Lysyanskaya:2007:AI


Lysyanskaya:2008:CHK


Leung:2001:WDI


Li:2004:CAB


Lao:2009:ORA


Mrayati:2004:IAD

Mrayati:2005:IDB

Mrayati:2006:TTC

Mrayati:2007:TTC

Mrayati:20xx:AET

McDaniel:2006:OAI

Machado:2000:NCP
MacKenzie:2001:MEP


Mohay:2003:CIF


Madsen:2004:FFD


Mahle:2004:DDI


Malcolm:2002:LAM


Maloof:2006:MLD

Marcus A. Maloof, editor. Machine learning and data mining for computer security: methods and applica-
REFERENCES

Manger:2001:CCA

Man01
Mao:2001:TRC

Man02
Mann:2002:HI

Man08
Mann:2008:HHS
REFERENCES


Matsui:2002:FSE

Maurer:2001:C

Maurer:2004:RCD

Maughan:2005:HSC

Maximov:2006:SWC

Mayers:2001:USQ

May:2002:CUR
Alexander May. Cryptanalysis of unbalanced RSA with small CRT-exponent. In Yung [Yun02a], pages 242–256. CODEN LNCS0D9.
REFERENCES


Mel:2001:CD


Mohanty:2008:IWB


McKinnon:2004:CCS


Montenegro:2004:CBI

Gabriel Montenegro and Claude Castelluccia. Cryptobased identifiers (CBIDs): Concepts and applications. ACM Transactions on Inform...
REFERENCES

McAndrew:2008:TCO


McGraw:2006:SSB


Myles:2005:ETS


McLaughlin:2006:PZW


McNichol:2003:HTM


Martin:2004:AMC

REFERENCES


**Menezes:2005:TCC**


**Messerges:2000:SAF**


**Messerges:2001:SAF**

REFERENCES

McGrew:2001:AAE

Marti-Farre:2007:NSS

Matula:2005:TLS

Mueller:2006:SMG

Muller:2009:BPE

Minier:2001:SCC
Marine Minier and Henri Gilbert. Stochastic crypt-

Muresan:2008:PCA

Mukherjee:2002:CAB

Molland:2004:ICA

Ma:2005:NCD

Maas:2009:SRW
REFERENCES

Moon:2002:IDC

May:2002:SKS

Mihaljevic:2009:ASC

Micciancio:2001:ILB

Micciancio:2002:GCK
REFERENCES

Micciancio:2002:ICH


Millen:2003:FD


Mironov:2002:RSO


Mirkovic:2005:IDS


Mishra:2006:PCS


Misić:2008:TEC

Jelena Mišić. Traffic and energy consumption of an IEEE 802.15.4 network in the presence of authenticated, ECC Diffie–Hellman ephemeral key exchange.
Mitchell:2000:MSN


Mitra:2002:TAD


Miyazaki:2001:ISG


MacDonald:2003:CDS


Maltoni:2004:BAE


Moore:2001:AGK


Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS


Moyle:2005:CLD


Mazieres:2000:SKM


Majzoobi:2009:TDI

REFERENCES


McLoone:2001:SCF


Mana:2002:PMD


Moldovyan:2007:IC


Mullen:2007:FFA


Moreira:2002:RCE

REFERENCES


REFERENCES


This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.


REFERENCES


Meyer:2001:FIC

Monsignori:2001:WMS

Mironov:2008:SAE

MacAndrew:2000:LPT

Mykletun:2006:AIO

Mollin:2001:IC
Richard A. Mollin. *An Introduction to Cryptography*. 

Moller:2002:PEC


Moller:2003:PSP


Mollin:2003:RPK


Mollin:2005:CGS


Mollin:2007:IC


Monniaux:2003:ACP

Mangard:2006:PAA

Stephan Mangard, Elisa-beth Oswald, and Thomas Popp. Power Analysis At-tacks and Countermeasures for Cryptographic Smart Cards, volume 450 of Ad-\v{v}ances in Information Security. Springer-Verlag, Berlin, Germany / Heidelberg, Ger-

Morris:2003:KKL


Moritz:2005:KAE

REFERENCES


REFERENCES


REFERENCES


[MR01c] Silvio Micali and Leonid Reyzin. Soundness in the public-key model. In Kilian [Kil01a], pages 542–??
REFERENCES


Monrose:2002:TSG


Mitchell:2006:PPT


Mayer-Sommer:2001:SAS

Rita Mayer-Sommer. Smartly

Maggi:2002:USV


Maitra:2002:CSB


Menezes:2002:PCI


Mitnick:2002:ADC

REFERENCES


Muthukrishnan:2002:IAS

Markowitch:2003:CWV

Miklau:2003:CAP

Martin:2005:PET

Meadows:2005:CPA
REFERENCES


McClure:2003:HEN


Matsumoto:2007:FSC

Makoto Matsumoto, Mitsuo Saito, Takuki 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 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????.

Miltchev:2008:DAC


Mouratidis:2009:PMD


Moran:2004:NIT


Myasnikov:2005:PAB

Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. A practical attack on a braid group

Muzereau:2004:EBD

A. Muzereau, N. P. Smart, and F. Vercauteren. The equivalence between the DHP and DLP for elliptic curves used in practical applications. LMS Journal of Computation and Mathematics, 7:50–??, 2004. CODEN ????? ISSN 1461-1570.

Marsaglia:2002:SDP


Meseguer:2007:SRA


Ma:2009:NAS


Muller:2001:SWB

Muller:2001:SIC


Munro:2008:DE


Murphy:2000:KST

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

Murray:2001:CDC


Murray:2002:IYP


Moriai:2000:PTL


Meister:2001:PPG

Gisela Meister and Michael Vogel. Protection profiles and generic security targets for smart cards as secure signature creation devices — existing solutions for the payment sector. Lecture Notes in Computer Science, 2140:179–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349.
REFERENCES

Micciancio:2003:SZK


[MV03a]

Morelli:2001:JAH


[MV03b]

Micciancio:2004:CTA


[MW04]

Morelli:2003:DIB


[MWM01]

Malan:2008:IPK


[MWS08]

MRaihi:2001:CAS


[MY01]
REFERENCES


[Naik:2003:DSW] Vinayak Naik, Anish Arora,


REFERENCES

Naor:2002:DRA


Naor:2003:CAC


NIST:2000:FPD


Nazario:2002:RYS

Jose Nazario. A rough year for SSH. Linux Jour-
Nieto:2001:PKC


Nghiem:2009:FBI


Ning:2004:TTA


Nedjah:2005:SHC


Nash:2001:PIM


Nedjah:2004:ECH

Nadia Nedjah and Luiza de Macedo Mourelle, editors. Embedded cryptographic hardware: methodologies and architectures.
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Nikander:2002:DSAA


Nikander:2002:DSAB


NIST:2000:TAE


NIST:2001:CT


NIST:2001:SRC

[NIS01b] NIST. Security requirements for cryptographic modules.
REFERENCES


REFERENCES

Nozaki:2001:IRA

Northcutt:2002:NID

Naor:2001:RTS

Nikov:2006:RBV

Naor:2005:ECH
Moni Naor, Asaf Nussboim, and Eran Tromer. Efficiently constructible huge graphs that preserve first order properties of random graphs.
REFERENCES

In Kilian [Kil05], pages 66–??  
CODEN LNCSD9. 
ISBN 3-540-24573-1 (softcover). ISSN 0302-9743  
(print), 1611-3349 (electronic). LCCN QA76.9.A25  
openurl.asp?genre=issue&issn=0302-9743&volume=  
3378; http://www.springerlink.com/openurl.asp?genre= 

Roman Novak. SPA-based adaptive chosen-ciphertext attack on RSA implementation. Lecture Notes in  


REFERENCES

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


[NS01c] Phong Q. Nguyen and Jacques Stern. The two faces

Narayanan:2005:FDA


Narayanan:2005:ODG


Nguyen:2005:FPL


Nguyen:2005:PSE


Nishioka:2002:DAF


Nahum:2007:ESS

Nyberg:2001:CTC


Nenadic:2005:RBC


Nenadic:2005:RBV


Olson:2003:QHK


Oechslin:2003:MFC


Oppliger:2008:STS

REFERENCES

0018-9162 (print), 1558-0814 (electronic).


Olson:2000:SCT


Ohigashi:2009:PMF


Ohkuma:2001:BCH


Ohbuchi:2002:FDA


Onions:2001:SSI


Ors:2003:PAA

Siddika Berna Örs, Elisabeth Oswald, and Bart Preneel. Power-analysis attacks on an FPGA — first experimental results. In Walter et al. [WKP03], pages 35–50. CODEN LNCS-D9.
REFERENCES


REFERENCES

Okeya:2000:PAB


Okeya:2001:EEC


Orent:2006:PAR


Obimbo:2007:PAD


Oury:2008:PP

REFERENCES


[OT03a] Katsuyuki Okeya and Tsuyoshi Takagi. A more flexible


Overbeck:2006:EGA

Onieva:2008:MNS

Paeng:2003:SCU

Page:2003:BRW

Panditaratne:2007:TRN

Papanikolaou:2005:BRBa

Park:2004:APP
Chang-Seop Park. Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems. Computer Networks (Amsterdam, Netherlands: 1999),
REFERENCES


[Pau02a] Linda Dailey Paulson. News briefs: Project promises accessible technology for the disabled; two efforts aim to upgrade mobile memory; new haptics approach lets parents-to-be “touch” their unborn children; prime breakthrough may improve encryption. Computer, 35 (10):26, October 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814


REFERENCES

CODEN IJBEE4. ISSN 0218-1274.


REFERENCES


REFERENCES


[Pen01a] Matthew Pemble. Confidentiality: From encryption, to
CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electronic). URL http://

**Pemble:2001:SPA**

**Perrine:2003:ECP**
Tom Perrine. The end of *crypt()* passwords ... please? ;login: the USENIX Association newsletter, 28 (6):??, December 2003. CODEN LOGNEM. ISSN 1044-6397. URL http://www.

**Perlman:2005:EMD**

**Pett:2003:IEH**

**Per05**

**Petzold:2008:ATG**

**Potter:2003:S**
Bruce Potter and Bob Fleck. *802.11 Security*. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617
REFERENCES


Pfitzmann:2001:ACE


Phatak:2005:FMR


Power:2007:SBB


Provos:2003:HSI


Phan:2004:IDC


Paeng:2001:NPK

Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik
REFERENCES


[Pin02] Benny Pinkas. Cryptographic techniques for

**Pinkas:2003:CTP**


**Pincock:2006:CHC**


**Pecho:2009:APW**


**Park:2001:NDW**


**Park:2001:RFW**

REFERENCES


Poh:2001:HBP


Petitcolas:2003:DWF


Park:2001:CSC


Park:2005:CZA


Park:2001:DNP

Hee-Un Park and Im-Yeong Lee. A digital nominative proxy signature scheme


REFERENCES

Piper:2002:CVS


Pang:2008:AQR


Pohlmann:2001:SCA


Pointcheval:2000:CCS


Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP

REFERENCES


[PP06a] Souradyuti Paul and Bart Preneel. On the (in)security


Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In Walter et al. [WKP03], pages 77–88. CODEN LNCS9. ISBN 3-540-40833-9. ISSN
Pereira:2006:IBS


Picard:2001:NNF


Pass:2005:NIC


Pass:2008:NIC


Preneel:2000:ACE


Preneel:2001:NES

Bart Preneel. New European Schemes for Signature,
REFERENCES


Preneel:2002:NEA


Preneel:2002:NPT


Preneel:2002:TCC


Preneel:2007:SRD

Price:2000:NCH


Provos:2000:EVM


Provos:2001:DAS


Paun:2004:CTT


Poupard:2000:FER


Parker:2001:RKC


Pfitzmann:2001:SEC

Birgit Pfitzmann and Ahmad-Reza Sadeghi. Self-escrowed cash against user blackmailing. *Lecture Notes in
Pornin:2001:SHT


Padro:2002:LBI


Pomerance:2002:SOC


Page:2004:PCA


Park:2004:UUC

REFERENCES

Prabhakaran:2004:NNS


Prabhakaran:2005:RES


Phan:2006:FDB


Park:2008:SRB


Pavlou:2008:FAD


Park:2002:SRL

service/series/0558/papers/2501/25010176.pdf.

Pareschi:2009:PAC


Petit:2008:BCB


Preneel:2006:SAC


Pang:2008:VCR


Pfleeger:2007:GEI


Pucella:2003:JRB

[Ruc03] Riccardo Pucella. Joint re-

Pucella:2006:SCC


Pucella:2007: Ib


Puzmanova:2004:RWF


PV06a

Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI

REFERENCES

Pang:2005:NMS


PW05

Peikert:2008:LTF


PW08

Pelzl:2003:HCC


PY05

Patrick:2005:FCD


PWGP03

Paterson:2006:LTT

REFERENCES


Haifeng Qian, ZhenFu Cao, and Haiyong Bao. Cryptanalysis of Li–Tzeng–Hwang’s improved signature schemes.

**Qian:2005:SPL**


**Quisquater:2000:SCR**


**Quisquater:2002:CTM**


**Quisquater:2001:EAE**


**Quisquater:2002:CTM**


Rand:2001:MRD


Roman:2007:SCP


Rand:2001:MRD

Rand Corporation. *A Million Random Digits With
REFERENCES


REFERENCES


[RdS01] Artur Romão and Miguel Mira da Silva. Secure mobile agent digital signatures with
proxy certificates. Lecture Notes in Computer Science, 2033:206–??, 2001. [RE03]


Oded Regev. On lattices, learning with errors, random
REFERENCES

linear codes, and cryptography. In ACM [ACM05c],
84–93. ISBN 1-58113-960-8. LCCN QA75.5 A22
2005.

Oded Regev. On lattices,
learning with errors, random
linear codes, and cryptography. Journal of the ACM,
56(6):34:1–34:40, September 2009. CODEN JA-
COAH. ISSN 0004-5411
(print), 1557-735X (elec-
tronic).

Jian Ren. A cryptographic
watermarking technique for multimedia signals. Advances in Computational
Mathematics, 31(1–3):267–
281, October 2009. CODEN ACMHEX. ISSN 1019-7168
(print), 1572-9044 (elec-

Eric Rescorla. An intro-
duction to OpenSSL pro-
gramming, Part I of II.
Linux Journal, 89:74, 76–78,
CODEN LIJOFX. ISSN
1075-3583 (print), 1938-3827
(electronic).

Eric Rescorla. An intro-
duction to OpenSSL pro-
gramming, Part II of II.

Robert Reynard. Secret code
breaker online. World-Wide
codebreaker.dids.com/.

Michael F. Ringenburg and
Dan Grossman. Prevent-
ing format-string attacks via
automatic and efficient dy-
namic checking. In Meadows
and Syverson [MS05b], pages
354–363. ISBN 1-59593-226-
7. LCCN QA76.9.A25. ACM
order number 459050.

Yanli Ren and Dawu Gu.
Fully CCA2 secure iden-
tity based broadcast encryp-
tion without random or-
acles. Information Process-
ning Letters, 109(11):527–533,
May 16, 2009. CODEN IFPLAT.
ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

Gregory Gordon Rose, Alexan-
der Gantman, and Lu Xiao.
Cryptographically secure


[Ris06] James Risen. State of war: the secret history of the CIA


[Roy04] Bimal Roy and Willi Meier,


[RMH04] Arash Reyhani-Masoleh and M. Anwar Hasan. Towards fault-tolerant cryptographic...


[Alon Rosen. A note on the round-complexity of concurrent zero-knowledge. In Bellare [Bel00], pages]
REFERENCES


Jörg Rothe. Some facets of complexity theory and


REFERENCES


Rieffel:2000:IQC


Ratzman:2000:RSS


Ratzman:2003:NGI


Ratzman:2003:NHS

REFERENCES


REFERENCES

Rosenbaum:2000:SFR

Romer:2001:ILA

Rubin:2002:SAV


Rubin:2003:TBC

Riley:2004:HAE
REFERENCES


Rao:2005:CHE


Rubin:2008:CFF


RSA:2000:PKC


RSA:2000:PVCa


RSA:2000:PCP


RSA:2000:PVCb


RSA:2000:PVS

RSA Laboratories. *PKCS #9 v2.0: Selected Object Classes and Attribute Types*. RSA Data Security, Inc., Redwood City,


REFERENCES

http://www.springerlink.com/content/r61844.


REFERENCES


[RW03a] Renato Renner and Stefan Wolf. New bounds in secret-

**Renner:2003:UAP**


**Ramaswamy:2007:HSP**


**Schmalz:2003:MDI**


**Saini:2002:JMD**


**Saeednia:2002:IBS**

REFERENCES


Peter H. Salus. Book reviews: The bookworm: Reviews of Pawel Cerven’s

Sale:2005:RCB


Sallee:2005:MBM


Salomon:2005:CDC


Salomon:2005:FCS


Salomon:2007:DCC

REFERENCES


[Sav04] A. Savelli. On numerically decipherable codes and their

**Soto:2000:RTA**


**Shacham:2001:ISH**


**Scott:2004:CP**


**Stoklosa:2005:CIC**


**Stallings:2007:CSP**


**Sherwood:2005:MTR**

Rob Sherwood, Bobby Bhat-

**References**


[SBEW01] [SBG02] [SBG05]


[SBEW01] [SBG02] [SBZ02]

REFERENCES


[SC05b] George Stephanides and Nicolae Constantinescu. The
REFERENCES


**Sun:2005:IPK** [Sch00b]


**Siegelin:2001:SCD** [SC05c]


**Schmalz:2000:MAD** [Sch00a]


**Schneier:2000:AAR**


**Schneier:2000:IRS**

Schneier:2000:SLD


Schneier:2000:SRF


Scharinger:2001:ASK


Schindler:2001:TAA


Schmalz:2001:MDI


Schneier:2001:FSE


**Schnorr:2001:SGH**


**Schnorr:2001:SDE**


**Schneier:2003:BFT**


**Schmalz:2004:MDIa**


**Schmalz:2004:MDIb**

Schneier:2004:SA


Schmalz:2005:MDI


Schneier:2005:TFA


Schramm:2006:AMS


Schroeder:2006:NTS

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title and Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sun:2005:CCL</strong></td>
<td>Da-Zhi Sun, Zhen-Fu Cao, and Yu Sun. Comment: cryptanalysis of Lee–Hwang–Li’s key authentica-</td>
</tr>
</tbody>
</table>

Sun:2005:RNK


Sebe:2001:OIW


Sebe:2000:SDI


Smith:2001:ADB

Spiekermann:2009:ACR

Seacord:2005:SCC

Seacord:2009:CCS

Seetharaman:2004:BRB

Smith:2006:SID

Seifried:2000:C

Seifried:2000:PPA


[SETB08] Iain Sutherland, Jon Evans,

Shumow:2007:PBD


Simka:2006:MTR


Sakr:2007:RCB


Sutton:2007:FBF


Steinwandt:2001:TDB

REFERENCES

link/service/series/0558/bibs/2200/22000280.htm;

Steinwandt:2000:WHS


Steinwandt:2008:GEI


Sauvage:2009:ERF


Storer:2009:PSR


Stone:1998:PCC

REFERENCES

Sonntag:2000:MAS


Shirase:2005:AEC


Shailer:2001:PMT


Shamir:2001:NDC


Shamir:2001:PSC


Shao:2001:BVM


Sharp:2001:IKB

References

Shapiro:2002:CCM

Shamir:2003:RS

Shao:2003:CI

Shao:2003:PS

Shaltiel:2004:R
REFERENCES


[Shi05] Kyungah Shim. Off-line password-guessing attacks on the generalized key agreement and password authen-

**Shih:2008:DWS**


**Sierra:2004:LCC**


**Shimizu:2007:CBE**


**Shoup:2000:CTU**


**Shoup:2000:UHF**


**Shoup:2001:OR**

Victor Shoup. OAEP


REFERENCES


Shyamasundar:2002:ACP


Silverman:2001:CLI


Simon:2002:CRE

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


Sivonen:2006:MPF


Schnorr:2000:SSE


Sucurovic:2005:JCY


Schaumont:2009:GEI


Song:2000:TPA


Seki:2001:DCR

REFERENCES

Stojanovski:2001:CBRa


Sklavos:2005:ISH


Stavrou:2005:CAS


Stabell-Kulo:2006:ESC


Saldamli:2007:SME


Shu:2009:RCA


Sugita:2001:SRV

[SKI01] Makoto Sugita, Kazukuni Kobara, and Hideki Imai. Security of reduced version of the block cipher Camellia against truncated and impossible differential cryptanalysis. Lecture Notes in Computer Sci-
REFERENCES

Sano:2000:PEA


[SKKS00]

Srinathan:2002:ASC


[SKR02]

Sugita:2000:RAD


[SKU+00]
Schneier:2000:CTA

[SKW+00] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, and Niels Ferguson. Comments on Twofish as an AES candidate. In NIST [NIS00], pages 355–356. ISBN ????. LCCN ???.

Sterbenz:2000:PAC

REFERENCES

**Shim:2005:SFA**


**Srivatsa:2005:SPS**


**Skoudis:2006:CHR**


**Stamp:2007:ACB**


**Sun:2009:CPR**


**Su:2005:KPK**


**Shi:2005:HEC**


[SM00b] Palash Sarkar and Subhamoy Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In Bellare [Bel00], pages 515–?? ISBN 3-540-67907-3. ISSN 0302-9743
REFERENCES

Sebag-Montefiore:2000:EBC


Sarkar:2003:EIC

&arnumber=1190582.

Satoh:2003:UHA


Satoh:2002:SHS


[SM00c]

[SM01]

[SM03a]

[SM03b]
REFERENCES


Sebag-Montefiore:2005:EBC

Sebag-Montefiore:2007:EBC

Simos:2007:CMS

Smith-Miles:2008:CDP

Smart:2001:CDF

Smart:2003:ACU
REFERENCES


[Smi01c] Richard E. Smith. *Authentication: From Passwords*
REFERENCES

599

[Smith:2002:OAP]

[Smo04]

[SMP+09]

[Satoh:2001:CRH]

[SN04]
Schlager:2007:EAA


Sakai:2000:NDS


Srinathan:2004:OPS


Safavi-Naini:2000:STT


Safavi-Naini:2001:BAG


Safavi-Naini:2001:LAC

REFERENCES


Sanchez:2001:RNM


Slind:2007:PPS


Song:2000:ISC


Shigetomi:2002:ALS


Satoh:2000:HSM

Akashi Satoh, Nobuyuki Ooba, Kohji Takano, and


S. M. Shahruz, A. K. Pradeep, and R. Gurumoorthy. Design of a novel cryp-


REFERENCES


[SRQL03] François-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier

Sarkar:2001:PAE

Stubblebine:2001:AAF

Seznec:2003:HUL

Swiderski:2004:TM

Seddik:2009:IWB
Hassen Seddik, Mounir Sayadi, Farhat Fnaiach, and Mohamed Cheriet. Image watermarking based on the Hessenberg transform. In-
REFERENCES


Shi:2008:UAU

Susilo:2000:NEF

StPierre:2000:TFA

Sakurai:2001:NSS

Schmidt-Samoa:2006:AFW

Scambray:2006:HEW

[ST01b] Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In Kilian [Kil01a], pages 355–??.
http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390355.htm;

CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370258.htm;


CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2384/23840436.htm;
REFERENCES

Satoh:2003:SDF


Shamir:2003:FLN


Spivak:2006:SPT


Stallings:2000:SSC


Stallings:2002:CNS


Standboge:2002:ENO


Stajano:2003:SCU

REFERENCES

Stanik:2005:NLO

Stamp:2006:ISP

Sterlicchi:2000:SCD

Steinwandt:2001:LTP

Stefanek:2002:ISB

Steele:2005:PPT
REFERENCES


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

**Stinson:2006:CTP**


**Shimoyama:2002:MLC**


**Stone:2001:CI**


**Struif:2001:UBU**


**Strunk:2001:JQJ**


**Strubinger:2002:HBS**

REFERENCES

2002. CODEN SYADE7. ISSN 1061-2688.

**Stytz:2004:BRW**


**Saxena:2007:TCP**


**Shaltiel:2007:LEU**


**Sugihara:2001:PCD**


**Sugita:2003:DRW**


**Sun:2000:DRR**

REFERENCES


Sun:2000:ESM


Sun:2002:IIR


Sun:2005:UMS


Seidl:2008:FOV


Shaltiel:2008:HAP


Sebe:2007:SMO


Shmueli:2009:DEO

REFERENCES


[Sun:2000:AFA]


[Shim:2005:WIB]

[Swaine:2001:PPSa]

[Stubblebine:2002:ALF]

[Swenson:2008:MCT]
REFERENCES

enhancements/fy0808/2007051636-t.html; http://www.loc.gov/catdir/enhancements/fy0810/2007051636-b.html

Song:2005:ISG


Sun:2009:TDS


Swire:2005:SMI


Stevenson:2005:SCI


Song:2007:TAK


Shujun:2001:PRB

REFERENCES

Seo:2001:CDA


Shi:2001:NSF


Syed:2000:CLA


Sun:2005:CSS


Syverson:2002:FCI


Shimoyama:2002:BCS

[SYY+02] Takeshi Shimoyama, Hi-
toshi Yanami, Kazuhiro Yokoyama, Masahiko Take
enaka, Kouichi Itoh, Jun Yajima, Naoya Torii, and
Hidema Tanaka. The block cipher SC2000. Lecture
Notes in Computer Science, 2355:312–??, 2002.
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
link/service/series/0558/2355/23550312.htm;
http://link.springer-ny.com/link/service/series/
0558/papers/2355/23550312.pdf.

Ron Steinfeld and Yuliang Zheng. An advantage of low-
exponent RSA with modulus primes sharing least
significant bits. Lecture Notes in Computer Science,
2020:52–??, 2001. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL http://
link.springer-ny.com/
link/service/series/0558/2020/20200052.htm;
http://link.springer-ny.com/link/service/series/

Ed Skoudis and Lenny Zeltser. Malware: Fighting
Malicious Code. Prentice Hall series in computer
networking and distributed systems. Prentice-Hall PTR,
0-13-101405-6. 512 (est.) pp. LCCN QA76.9.A25 S58

Behmet Sarikaya and Xiao Zheng. SIP paging and
tracking of wireless LAN hosts for VoIP. IEEE/ACM
CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Qi Sun, Qi Fan Zhang, and Guo Hua Peng. A new
algorithm for the Dickson polynomial $g_e(x,1)$ public
key cryptosystem. Sichuan Daxue Xuebao, 39(1):18–23,
2002. CODEN SCTHAO. ISSN 0490-6756.

Da-Zhi Sun, Ji-Dong Zhong, and Yu Sun. Weakness
and improvement on Wang–Li–Tie's user-friendly remote
authentication scheme. Applied Mathematics and Com-
CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).
Tada:2002:OSM


Tang:2001:AES


Tang:2007:MMU


Tang:2007:SGK


Tattersall:2005:ENT


Trichina:2001:SCH

REFERENCES


pp. Duplicate ISBN with [Con04].

**Teepe:2006:PPA**


**Todd:2001:LSS**


**Terai:2008:BRB**


**Thorsteinson:2004:NSC**


**Theoharidou:2007:CBK**


**Tirkel:2001:UWE**

Tabatabaian:2001:NSP


Tippett:1927:RSN


Torres:2007:ANS

Joaquin Torres, Antonio Izquierdo, and Jose Maria Sierra. Advances in network smart cards authentication.

Tseng:2001:GGO


Tseng:2001:CLB


Tseng:2003:DSM

**REFERENCES**

**Tico:2003:RAS**


**Toll:2008:CSE**


**Thien:2002:TSS**


**Thomas:2007:HQU**


**Turner:2006:SIS**


**Tsai:2005:CAE**


**Tan:2004:OBC**

[TLYL04] Zhangxi Tan, Chuang Lin, Hao Yin, and Bo Li. Optimization and benchmark of

Tokita:2001:ADC


Tang:2006:CHA


Tian:2005:RWS

[TMM05] Junfeng Tian, Guofu Ma, Shengfu Ma, and Yahui Meng. Research on Web server attacking-based intrusion detection. In Han et al. [HYZ05b], pages 159–?

Toussidou:2000:IMS


Tanaka:2001:QPK

[TO01] Keisuke Tanaka and Tat-suaki Okamoto. Quan-
New developments of the theory of computation and algorithms (Japanese) (Kyoto, 2001).


Tsang:2007:WCT

Tseng:2007:SAG

Takano:2000:PTH
Kohji Takano, Akashi Satoh, and Nobuyuki Ohta. Poster 5: TATSU — hardware accelerator for public-key cryptography using Montgomery method. In Anonymous [Ano00d], page ??.

Tsunoo:2003:CIC

Tahir:2000:RCM

Tzeng:2001:PKT
Tian:2001:ICE


Tuchman:1966:ZT


Turing:2004:BS


Tiri:2003:SEA


Toft:2001:LTT

George Toft, Hugo van der Kooij, Mick Bauer, Chris Hendrickson, Stephanie Black, Adrian Ho, Markus Hogger, Ian Abbott, and Robin Rowes. Letters: Tech tipsy; awkward solution; Mandrake 7.2 review; OpenSSH and DSA keys; missed the


[TW2009CIF] Mohit Tiwari, Hassan M. G. Wassel, Bita Mazloom, Shashidhar Mysore, Fred-

Thamrin:2008:PBR


Tzeng:2004:NTM


Ting:2002:FBS


Tynan:2005:CPA


Tian:2005:NDF

Junfeng Tian, Weidong Zhao, Ruizhong Du, and Zhe Zhang. A new data fusion model of intrusion detection—IDSFM. In Han et al. [HYZ05b], pages 73–?? ISBN 981-270-153-2. LCCN ???? URL http://eproceedings.worldscinet...


IEEE Computer Society
Press, 1109 Spring Street,
Suite 300, Silver Spring, MD
20910, USA, 2009. URL
org/stamp/stamp.jsp?tp=
&arnumber=5192510.

[Uni00a]
United States Congress.
H.R. 850, the Security and
Freedom through Encryption
(SAFE) Act: Markup before
the Committee on Interna-
tional Relations, House of
Representatives, One Hun-
dred Sixth Congress, first
session, Tuesday, July 13,
1999. United States Govern-
ment Printing Office, Wash-
ington, DC, USA, 2000.
ISBN 0-16-060340-4, 0-16-
060340-4. iii + 102 pp.
LCCN KF27.I53 106th.

[Uni00b]
United States Congress.House
Committee on Armed Ser-
VICES. U.S. encryption policy:
hearing before the Committee
on Armed Services, House of
Representatives, One Hun-
dred Sixth Congress, first
session: hearings held July
1, 13, 1999. Washington,
DC, USA, 2000. iv + 195

[Uni00c]
United States Congress.House
Committee on International
Relations. 106-1 Hearing:
Encryption Security in a
High Tech Era, May 18,
1999. Washington, DC,
USA, 2000. Shipping List #: 2000-0319-P. Shipping List
Date: 07/31/2000.

[Uni00d]
United States Congress.House
Committee on International
Relations. 106-1 Markup:
H.R. 850, The Security And
Freedom Through Encryp-
tion (SAFE) Act, July 13,
1999. Washington, DC,
USA, 2000. Shipping List #: 2000-0214-P. Shipping List
Date: 04/20/2000.

[Uni00e]
United States Congress.House
Committee on International
Relations. H.R. 850, the Se-
curity and Freedom through
Encryption (SAFE) Act: mark up before the Commit-
tee on International Re-
lations, House of Repre-
sentatives, One Hundred
Sixth Congress, first ses-
sion, Tuesday, July 13,
1999. Washington, DC,
Shipping list no.: 2000-0214-
P.
REFERENCES


USHCJ:2000:HSF


USHCJ:2000:SFT


USPTO:2001:CCP


Uhl:2005:IVE


Urban:2001:MWB


Urien:2001:PIS

REFERENCES


USENIX:2000:PLI


USENIX:2000:PFW


USENIX:2000:PFSa


USENIX:2000:PNU


USENIX:2001:PUA


USENIX:2001:PFT

[USE01b] USENIX, editor. Proceed-
 REFERENCES


REFERENCES


Ustimenko:2001:CGT


Ulfving:2000:GS


Uzun:2004:BRC


Vacca:2006:GWN


Vadhan:2003:CLC

[Vad03] Salil P. Vadhan. On con-
REFERENCES


Vaudenay:2001:DID


Vaudenay:2002:SFI


Vaudenay:2005:PKC

REFERENCES


Verheul:2001:EXM


Vercauteren:2002:CZF


Vergnaud:2006:RBS


Vernitski:2006:CUM


Vladimirov:2004:WFS


Vassev:2009:STA


Voloshynovskiy:2001:BDA

Sviatoslav Voloshynovskiy, Alexander Herrigel, and Thierry Pun. Blur/deblur attack against document
REFERENCES


REFERENCES


Viega:2003:SPC


Viega:2002:NSO


Voice:2005:OAM

Chris Voice. Online au-

**vanOorschot:2008:PMU**


**vanOorschot:2007:IRS**


**Vogt:2001:USC**


**Vasco:2001:CPK**


**Voyiatzis:2008:SFS**


**vanTilborg:2000:FCP**

Henk C. A. van Tilborg. *Fundamentals of cryptography: a professional reference and

[vanTilborg:2001:ECC]


[vanTilborg:2005:ECS]


[VVS01]


[vonWillich:2001:TIT]

REFERENCES

[0558/papers/2260/22600044.pdf]


REFERENCES


Walter:2003:STM

Wang:2004:AWA

Wang:2004:TVS

Wang:2005:SCR

Wardlaw:2000:RPK

Washington:2008:BRB
REFERENCES

Washington:2008:ECN


Wayman:2001:FBA


Wayman:2002:BAT


Wayner:2002:DCI


Wayner:2009:DCI


Weiss:2000:CAC


[WC01a] Duncan S. Wong and Agnes H. Chan. Efficient and mutually authenticated key exchange for low power com-

**Wu:2001:CKA**


**Wu:2003:HDW**


**Wu:2004:EIW**


**Wang:2005:TAP**


**Wang:2009:NWA**


**Wang:2005:SDR**


**Wang:2005:SDR**
REFERENCES

Westerlund:2001:HWK


Williams:2001:ICA


Wang:2009:SST


Weaver:2006:BA


Weber:2002:ECH


Webb:2008:IZN


Wehde:2000:IME


Weierud:2000:SFB

Frode Weierud. Sturgeon, the FISH BP never really


Welschenbach:2005:CCC


Weng:2003:CHC
REFERENCES

Wernsdorf:2002:RFR


Westfeld:2001:FSA


Wu:2002:LCN


Wang:2000:SGC

REFERENCES


[WHI01] Yuji Watanabe, Goichiro Hanaoka, and Hideki Imai. Efficient asymmetric public-key traitor tracing without trusted agents. *Lecture Notes in Computer Sci-

[Whi09]


[WHL05]


[Whyte:2005:TFC]


[Wie00]
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Wang:2005:CHY


Wang:2007:NCD


Wen:2005:TRB


Wang:2005:SAI


Wu:2005:IAW


Wong:2004:RCK

W. K. Wong, L. P. Lee, and K. W. Wong. Reply to the comment “Keystream cryptanalysis of a chaotic crypto-
REFERENCES


See [kWpLwW01, ´AMRP04].

Wang:2005:TSP


Wu:2008:RWM


Watters:2008:VDL


Wheeler:1995:TTE


Watanabe:2002:CCD


Wang:2008:NAD

REFERENCES


Wollinger:2005:CVH


Weimerskirch:2001:ECC


Wang:2001:TUR


Wright:2000:IQC


Wright:2001:AES

Marie A. Wright. The Advanced Encryption Standard. *Network Secu-
REFERENCES


[Wright:2003:FCI]

[Wang:2002:IPD]

[Wright:2002:EPS]

[Wrixon:2005:CCO]

[Whiting:2003:MPH]
REFERENCES

662

Walter:2005:DDP


Weimerskirch:2002:DLW


Wu:2002:CSCb


Wuensche:2009:CAE


Wu:2000:PKC

Wu:2001:FED


Woodruff:2002:CUC


Weaver:2000:CAC


WW04


Wolf:2005:NML

REFERENCES


Wyler:2005:ANS

gress Publishing, Inc., Rock

Wang:2005:CSA

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-

Wang:2005:ECSa

Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient collision search attacks on SHA-0. In Shoup [Sho05a], pages 1–?? ISBN 3-540-

Wang:2005:FCFa

Wang:2005:FCFb

Wang:2005:FCFb

Winslett:2005:PLD

Marianne Winslett, Charles C. Zhang, and Piero A. Bon
tti. PeerAccess: a logic for distributed autoriza
tion. In Meadows and Syver
REFERENCES


[XH05] Lu Xiao and Howard M. Heys. A simple power analysis attack against the key schedule of the Camellia

Xenakis:2006:GCO


Xu:2007:CAD


Xu:2005:ADR


Xie:2007:ISP


Xu:2003:TEP


Xie:2004:CTA

Qi Xie and Xiu Yuan Yu. Cryptanalysis of Tseng et al.’s authenticated encryption schemes. Applied Mathematics and Computation, 158(1):1–5, Octo-
REFERENCES

Xu:2009:AVB

[XYL09]

Yan:2000:NTC

[Yan00]

Yang:2002:NEC

[Yan02]

Yang:2005:TFN

[Yan05]

Yan:2007:CAR

[Yas08]

Yasuda:2008:DLP

[Yuan-bo:2004:ITA]

Yuan-bo:2004:ITA

[YbJf04]

Yue:2001:GNN

[YC01]


Yang:2008:NFD


Yang:2007:IIS


Yang:2006:PKC


Yekhanin:2007:LDC


Yan:2006:ICP


Youssef:2001:CIM

[A. Youssef and G. Gong. Cryptanalysis of Imai and Matsumoto scheme B asymmetric cryptosystem. *Lec-
REFERENCEs

ture Notes in Computer Science, 2247:214–??, 2001. [YGZ05]

Youssef:2001:IAB [YG01b]


Youssef:2001:CPK [YG01c]


Yang:2005:IME


Yamamura:2000:QCB


Yamamura:2001:EDA

Yi:2004:AKA


Yen:2000:CB


Yen:2002:CAO


Yen:2003:RSC


Yardi:2008:HAC

Sarita Yardi, Pamela Kro-

**Yamamoto:2001:PKB**


**Yu:2001:TCB**


**Yi:2009:SSG**


**Yu:2005:EHI**


**Yoo:2002:LAU**

REFERENCES


[YPPK09] Yin Yang, Stavros Papadopoulos, Dimitris Papadias, and George Kollios. Authenticated indexing for outsourced spatial databases. VLDB Journal: Very Large Data Bases,
Yin:2001:RMW


Yilek:2009:WPK


Yoon:2004:SUA


Yoon:2005:CFI


Yoon:2005:ICJ


Yoon:2005:IFA

REFERENCES

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

Yeh:2002:SAK

Yeh:2004:PBU

Yanami:2002:DLC

Yeh:2003:IAM

Yen:2001:EEA

Yoshiura:2001:AWB
Hiroshi Yoshiura, Takaaki Shigematsu, Seiichi Susaki, Tsukasa Saitoh, Hisashi Toyoshima, Chikako Kurita,


REFERENCES

Yang:2008:VCS


Yang:2008:FSD


Yang:2009:CLW


Young:2000:RBA


Young:2001:BOK


Young:2004:MCE


[Ye:2007:NAW] Dengpan Ye, Changfu Zou,
REFERENCES


[ZBP05] Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. In ACM [ACM05a],

[ACM05a]
REFERENCES


Zunino:2005:WPE


Zhao:2006:SAP


Zeadally:2000:IPQ


Zhang:2005:CSS


Zhen:2004:IBS


Zhang:2005:AES


Zou:2005:MED

[ZGTG05] Cliff C. Zou, Weibo Gong, Don Towsley, and Lixin Gao. The monitoring and early detection of Internet

**Zhang:2000:WMH**


**Zha00**


**Zha06**


**Zha08**


**Zhe01**


**Zhe02a**

REFERENCES


REFERENCES


REFERENCES


[ZLZS07] Dong Zheng, Yan Liu, Jiying Zhao, and Abdulmotealeb El Saddik. A survey of RST invariant image water-

**Zolman:2001:SEM**


**Zhang:2001:CIS**


**Zhang:2005:DMC**


**Zhou:2005:MBI**


**Zhu:2007:APA**

Meiyuan Zhao, Sean W. Smith, and David M. Nicol. Aggregated path authentication for efficient BGP security. In Meadows and Syver-
REFERENCES


[ZW05b] Jianhong Zhang and Yunmin Wang. On the security of a convertible au-

Zhao:2002:EII  
**[ZWC02]**  

Zhu:2002:PAK  
**[ZWCY02]**  

Zhang:2004:NMS  

Zhong:2008:GPT  

Zhou:2003:ACN  
Jianying Zhou, Moti Yung, and Yongfei Han, editors. *Applied Cryptography and
REFERENCES


Zhang:2005:ASP


Zhang:2005:ISM


Zhang:2008:FIC


Zeng:2001:CHR


Zhu:2007:EIB

Robert W. Zhu, Guomin Yang, and Duncan S. Wong.