Title word cross-reference

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

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p_k)
[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LYL01, YCH02]. (tn)
[PW05, SC05a]. + [Abe01]. {0, 1}
[LBGZ01, LBGZ02]. 1 [Wu02]. $125
[And04]. 128 [AIK04, PCG01]. 13
[HSL02]. $15.00 [Imr03]. 2
[Bih00, BGN05, CY02, CKL03, DN07, Gau02, GHK06, GIKR02, HKA05, KLR09, SC02b, Ver02, Wen03]. 2000 ± 10
[Man01]. 2^{28} [Bih02]. 2^k [MFFT05]. 2^m
[KLY02, KKY02]. 3 [BP04, Ben00, ChLYL09, CT09, Lav09, OMT02, WH09, ZTP05].
$35.00 [Top02]. $49.99 [Gum04]. $5
[SCF01]. 5 [Pat04]. $51.48 [Pap05]. 512
[CDL00]. 7 [Gri01, Pat03a]. (2,128) [WB02].
6 [AIK04]. ABC [PS04b]. d [BD00b]. E_0
[FL01a]. f_8 [KSHY01]. g(x) [Shp02]. g_c(x, 1)
[SZP02]. GF(2) [CP03]. GF(2^m)
[OTIT01, RMP08]. GF(p^m) [BGK03].
GF(p) [ZP01]. k [BJS02, CT08b, GFC08, HKS00, QPV05, WL02]. l [QP05]. 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) [SGGB00]. μ
[LN04]. n
[CT08b, Gon06, HKS00, LKJL01, TM01]. N^{0.292} [BD00b]. NC^o [AIK06]. p [FL06].
[ACM08]. 41st [IEE00a]. 42nd [IEE01a]. 43rd [IEE02]. 44th [IEE03]. 45th [IEE04]. 46th [IEE05a]. 47th [IEE06]. 48th [IEE07]. 49th [IEE08]. 4th [BCKK05, BC05b, DWML05, DRS05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, KN03, MS05a, NP02a]. 5 [BCJ+06, Wac05]. 50th [IEE09b]. 512 [AD07, GLG+02]. 5th [CV04, KJR05, LL03, LLT+04, Li05, NP02a, Syv02, WKP03]. 64 [LKH+08, WWCW00]. 6th [BDZ04, Boy01, Chr00, DFPS06, PC05a, RS05, Sch01d, ST01d, Wri03]. 8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800 [BG07a, Hir09]. 800-90 [BG07a, Hir09]. 802.11b [SIRO4]. 802.11g [Coc02a]. 82 [Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02, SMP+09, VY01, Vau05a, WK06, Zhe02b]. 9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04]. 90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1 [GM00b]. ‘98 [Wi09]. ‘99 [DN00b]. 9th [CCMR02, CSY09, DR02e, DKU05, Lai03, NH03, Pat03b, FY05, YDKM06]. = = [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05]. A5 [BD00a, BSW01, PS01c]. A5/1 [BD00a, BSW01, PS01c]. AAFG1 [Hug02]. Aarhus [Cra05a]. Abadi [MW04]. Abelian [CF02, PHK+01, RS02]. Abstention [JJL02]. Abstract [CM00, Cou04, DIRR05, HLvA02, HIW01, 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 [EHKHO4]. Accelerator [MGBS01, RS04, TS00, XB01, DP+02].

Access [ANRS01, AN02e, BNPW03, CM02, DS06, HC08, MS03b, Ril02, Sma03a, Sm00a, ZGLX05, AW05, AW08, AFB05, BA06, BNP08, Che08b, DFM04, Hos08b, HY03, YI06, JW06, KNS05, LKZ+04, MF07, MSP+08, PS02a, STY07, WL05, WC01b]. access-control [BNP08]. accessible [Pau02a]. accountability [WABL+08]. Accounting [La08]. Accumulator [GTH02]. Accumulators [CL02a]. accurate [ZY08]. Achieve [CFS01]. Achievement [Coc01a]. Achievements [VDKP05]. achieving [PS04c]. ACISP [YG01c]. ACM [AC01a, ACM03a, ACM03b, ACM03c, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, MS05b, Bar06b, FMA02, Ra06]. ACNS [GKS05, IKY05, JY04, ZHY03]. acoustic [ZTT05]. Acquiring [SETB08]. across [Dav07, ZBLvB05]. Act [Kha05, Uni00a, Uni00e, Uni00d, Uni00g, Uni00h]. Actel [DV08]. Action [SE01]. Active [BC05a, BACS02, BP02, LJL05, MA00a, MA00b, Tad02, BPS08]. Active-Content [MA00a, MA00b]. activities [AJ08, SN07]. actually [Hau06]. Ad [BSS02, KH05, WT02, Cha05b, DHMR07, LHC08, LKZ+04, PCD07, SLP07, TW07, ZC09, MAA04]. 'ad-Durayhim’s [MAaT04]. Ad-hoc [BSS02, WT02, DHMR07, ZC09]. Adaptation [SSZ08]. Adapting [MJD01]. Adaptive [CM00, CTL04, CL08, Coc02a, CS02, CS03b, DSS01, ERF+05, FMY01, JMV02, KCJ+01, KL01, LP01, MP05, Nov01, Pie05, ZWC02, AAPP07, Che07, DP04, MB08, WNQ08, XMST07, YZDW07].
Adaptively
[AF04b, CHK05, FMY02, JL00].
Adaptively-Secure [CHK05]. Added
[Ano02b, St.00]. Adding [FBWC02].
Addison [Puc03]. Addition
[KT00, LPZ06, PP06a]. Additive
[FMY01, MF01]. Additive-Sharing
[FMY01]. Address
[IIT03, Nik02a, Nik02b, FXAM04, RW07].
Address-Bit [IIT03]. Addressing
[HTW07]. Adi [Coc03]. Adic
[GHK+06]. adjacent [JT01b]. Adjustment [BSNO00].
Adlan [MAaTxx]. Adleman
[BB79, Coc03, SP79]. Administration
[USE00c, USE00a, Ris06, WL04a]. administrative [Cra05b]. Admitting
[HSZI00]. Advance [CZB+01]. Advanced
[DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Swe08, Tan01, Ase02, Bar00c, Ili00, Bur03, CMM06, Coc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Har00, Her09, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sye00, WBRF00, Wri01, YW06]. Advances
[Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPST07, ELV01, Kil01a, Oka00, P6i01, Pre00, TIS07, Yum02a, Kat01, Bih03, CCM04, Cra05a, Fra04, Knn02, Lai03, Loe04b, LLI+04, Li05, LSI+05, Men07, Roy05, Sho05a, Zhe02b]. Advantage [SZ01]. advantages [CDS07]. adventures [Hro09].
Adversarial [CLR09, GSS08, MNS08].
Adversarial-knowledge [CLR09].
Adversaries [CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT+08, ZDO5]. Adversary
[Aba00, Gor06, RW02]. AES
[CGH+00b, DRS05, FIP01a, Her09, Pha04, AG01, An00a, AL00b, BDK+09, CG03, Coo02b, DB00b, DR02a, DR02b, DLP+09, DRO1, Don01, Dra00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, ICM00, IK00, IL01, JI00, KS09, Ke05, KFS000, KV01, LP02a, Len01, MHM+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03b, RRY00, SKKS00, SM03b, Sch00b, SKW+00, SW00a, SL00, WW00, WB00, WOL01, WWGP00, WW00].
AES-CBC [Fe06]. AES-like [DL+09].
AES-related [Sch00b]. Affine
[Ben00, CT09, Fel06, HH09].
Affine-Transformation-Invariant [CT09].
AFIS [Zir07]. African [WD01b]. after
[Ber03, McL06]. again [Fox00]. Against
[CS05b, DM07b, FKSW00, KS00a, KKS00a, KKS01, Mes00, Mes01, MFL05, MH04, P06b, Pro01, RK05, AG01, Ava03, Ban05, BPR00, BP02, BBN+09, BBB+02, BCP02b, CM00, CS03b, DB04, D06, Des00b, Des00c, Egl00, EBS01, FP01, Fry00, Geb04, HN02, HLL+01, HG07, Hsu05b, HLC08, In05, ISW03, IIT03, JKS02, J00b, JT01a, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, Mit00, M02, MG08, N00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PQ03b, RS01, SK01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sho00b, SKU+00, SKI01, SLL+00, Tad02, TV03, VHF01, XH05, YJ00, YKL02a, YKLM02b, YKLM03, ZS07].
Age
[Mar08b, Lev01]. Agency
[AJ08, Ban02, K01]. Agent
[HQ05, KC02, PDJH09, RdS01, RC01, Rot01, ZYM05, KXD00, SMS+08, SH00].
Agent-Based [HQ05, SSM+08]. Agents
[WHI01, Hau06, LSA+07]. Ages
[Eag05, Kin01]. Aggregate
[BGLS03, WK05]. Aggregated [ZS05].
Aggregation [Her06, CCM09, MS09].
Aggressive [Wy05]. AGM [Gau02].
Agreement
[AAG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB+04, AKR04, CY05, CY05, Che04a, CY05, CJ04, CJL05, HWW03, KPT04, KRY05, KKL05, LKK03a, LKK03b, LL04a, LL05a, LK05b, LK05c, LK05d, LLY06, LLS+09, LLR02, PQ03a, PQ06, Sh05, SW05, SC05b, Tsa06, Tse07, VK08, YW05, ...]
YS02, YSH03, Yi04, YRY05b, ZC04, LLR06].

agricultural [Lov01]. Aided [NS01b, HLL02]. aim [Pau02a]. Aimed [SFDF06]. Airport [Sas07], airwaves [Dav07]. Ajtai [GK05]. Aks [Che03]. Al [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx]. 

al-fusul [MAaT05]. al-Ka [MAaT07]. Al-Kindi [MAaT03, MAaTxx]. al-mutargima [MAaT05]. Alan [Pet08]. Alcatraz [LSVS09]. Alchemy [Pag03]. Alert [AJ08]. Alerts [NCRX04]. Alexandria [MS05b]. Algebra [Couv, CD01a, Lan04a, CKY07, Fau09, HW03a, HWR09, Sh05b]. Algebraic [AK03, Bar09, Can06b, CMR06, CM03, Cov03, CSF05, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mas04, MN01, MR02a, MR02b, PDMS09, Bul09, CKN06, CDL06, Iwa08, May09]. algebraically [RBF08], algebra [BDFP02]. Algorithm [ANS05, AEMR09, Bar00a, Bar00c, Bi09, BSC01a, ChLYL09, CU01, CJ03a, CJS01, CTLL01, CG03, CH07c, CKM00, CT03, CP03, DR01, DG00, Dhe03, EYCP00, FBW01, FMS01, GMM01, HTS02, HM02c, HZS05, JKK01, KBD03, KMM06, KY02c, KTL02, KV01, LP06, MM01b, MM01c, MS02e, NMS01, OS01, PZL09, PTB07, Ram01, RS01, SS01a, SQ00, WJ05, W07, WR07, WS01, Jin07, OS06, OP03, Puc03, QS01, SST06, Shao01c, Sma03b, SDNM06, SQ01, SWT07, YSS01, ZC00, ZGLX05, AveH00, AW05, AW08, BDO1, AKH03b, BSDV08, BRK03b, BUo05, BG06, BR05, BCJ06, CKL09, CW07, CS05a, DKS08, GW08, GM04, GTZ04, Has01b, Hir09, Hro05, Htu01, JET04, JWS05, KS00, Kor09, LKH08, LMW05, LW05a, LKJL01, Lu07]. analysis [Mea04, MT07, MRST06, OS00, PSG09].
Analyzing [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04]. Analytic [Shp03, Nie04].

Analyzing [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04]. Analytic [Shp03, Nie04].

Application-Aware [IKP+07].

Applications
[AF04b, AC02, AGT01, Anu04, BLST01, BH05, Bar06b, BI05a, BK+03, BS00a, Bih03, BGOY08, BSS02, BL08, CC04a, CD00a, CV02, CGH01, CZ05, CHSS02, CS09, Cra05a, CDI05, DJ01, DK02, DK07, DA03, DFPS06, FR02, GS08, GKK+09, GJKR03, Gen04a, GRW06, Go01a, Go04, HRS02, HN06, Has01a, HSS04, HR05, HJW05, J01b, KY01, KMM+06, KLOG4, KMO01, KBM09, KKIM01, Knu02, MAA07, MM07b, Nie02c, Nie02d, PS07, RSN+01, Sch06b, Shp03, SXY01, SPGG06, Vau02, Wya02, XYL09, YZ00, Zha02, ÁCTZ05, Ate04, AH05, AFGH06, BG08, BGL+03, CCCY01, CM05b, CS09, CK+08, DY09a, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gal02, GVC+08, GKK+07, GB09, HHSS01, Has02, Hen01, HKPR05, Jac00, KV+09, KNS05, La00, Lee04a].

applications
[LJ05a, LPW06, LB05, MY01, MA06, MC04, MSV04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SSS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPH06, WW08, WA06, WV00, YS04, ZBP05]. Applied
[HW03a, HWR09, SL07, GV09, GNP05, IKY05, JY04, ZY03]. Applying
[Elb09, KC02, Lan00d, LSV07, SQ01, SPMLS02, TND+09, vDKST06].

Appointed [CL01a]. apprehension [AJ08].

Approach
[BKM07, CGF809, CR01, CW09, CB01, DJLT01, Kra03, Lai07, LL05c, Lut03, OMT02, PBD00, Pau02a, Pre02a, SKG09, VH09, VVS01, Vitr03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLMM05, GG+08, Har05a, J01, JW01, Lyc02, MT09, Mar05b, MI09, Mos06, NN03, SL07, SN04, SW06b, ZLX99, ZSZ01, ZL04b, ZL04a]. Approaches
Approximation [CLZ02, Kuk01, WL02].
Approximations [BDQ04, Apress [Ter08].
April [Ano00d, 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, LKM+05, LZ04, LXM+05, Lut02, MP01c, MFS+09, Rot02a, SMTM01, SM03b, SLG+05, Uzn04, Che00, CC05c, DHL06, Ion05, LHL03b, MPPM09, SKW+07, SRL07, SH05, Tan01, WWA01].
Architectures [BGK+03, KLY02, RM02, SM02, Con04, DP04, GKS05, Ndm04, RH00, WH02b].
arival [SGMV09].
Archives [RC01].
archiving [DMSW09].
area [BP03a, Cal00c].
Areas [HH04, MZ04, PT06, VY01, AMW07, Buc00a, HH05, HAO0, NH03, ST01d].
Arent’t [Bau01a, Bau01b].
Arguments [HNO+09].
ARITH [BS03, BC01, IEE05b].
ARITH-15 [BC01].
ARITH-16 [BS03].
ARRIVAL-17 [IEE05b].
Arithmetic [BS03, BIP05, BGK+03, BCDH09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDV+01, SR06, GPS05, PS04a, SOIG07].
arithmetics [Lam91].
ARM7 [DV08, XB01].
armies [Ano03b].
Army [Boy03].
Arne [Bec02].
array [DZL01].
Arrays [ABM08, BS00a, GC01a, HWW05, PP06a].
Arrived [Law05].
arsenal [Blu09].
Art [An07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Eri03, Eri08, MS02d].
Article [Che08b].
Artifacts [EHK+03].
Artificial [Cop04b, MMYH02].
Arun [For04].
ASI [MJD01].
ASIC [WOL01].
ASIP [SKW+07].
asks [An08a].
ASM [MK05a].
Aspect [Kos01a].
Aspects [BLMS00, CMR06, Pel06, DLP+09, Rup09].
Aspiration [Ash03].
assembly [Gou09].
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, LHL04].
ASSL [VH09].
associated [XLMS06].
asociativity [HR08].
Assumption [CS00, DN00a, FOPS01, KMZ03, ZD05].
Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT+00, Nao03, SB02, Mic02a].
Assurance [LXM+05, AL04, BJ02, FOP06, Gha07, Jen09].
Assurances [Bar06b].
Astrology [Pag03].
Astronomy [MYC01].
Asymmetric [CH07b, Man01, SY01a, SBZ02, WH01, 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 [Ahm08, CKQ03, CS05b, CS03b, Des00b, Fil00, FV03, GHJV00, GHJV01, HQ01, Hug02, HW01, JI00b, KCP01, KSO0a, KML+02, KM01c, LY07, LNL+08, LV04, LM05, Luc02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, PQ03b, RMS05, SGM09, Sch01b, Sho00b, Sma03b, VHP01, YKL02a, 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, Luc00, TMMM05, BF06a].

**Attacking-Based** [TMMM05].

**Attacks**

[ARR03, AG01, AK03, BC05a, BPR00, BP02, BM000, BBB+02, BDK+09, BU02, BM03b, BCP02b, BM01c, Can06b, CS07b, CT08a, CJS01, CKM00, CJP00, CM03, Cout3, CWR09, CD01b, DPV01, DFS04, DJ06, DS08, DM07b, FKSW00, FOB05, FP01, Fry00, Fur02b, Gen04a, Gir06, GK02, HSH+08a, HNZI02, HR04a, HSH+01, HLC08, ISW03, JKS02, JJ00d, KKS00a, KKS01, KJC+01, KI01a, Law09a, LLS05a, IJS05, LJ05b, MPO06, MP06, MF01, Mes00, Mes01, Mö02, MG08, OT03a, OT03b, OOP03, O035, Ove06, PKB01, PDMS09, RS01, SKQ01, Sem00, SWT07, Tad02, VY07, WYY05a, WYY05d, WLZZ05, YYDO01, YY01, YGO1b, wV01, BPS08, B055, BCS08, BZ03, CKL+09, CS05a, DK08, Ges04, HSH+08b, HSH+09, Has01b, Hsu05b, HL05b, Ino05, IM06, JD01, KS05a, KTC03, LPV+09].

**attacks** [LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RG05, Schro0c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07, WL04b, Yan07, YS02, ZSJN07].

**attractors** [HHYW07].

**Attribute** [LY05, RSA00c, IY05].

**Attributes** [SS01b].

**Auction** [AS01a, Ano01a].

**Auctioning** [RCG+05].

**Auctions** [Bra01b].

**Audio**

[Arn01, C05c, DRL09, MH05, WNY09, WWL+02, X01, WQ00, BS01b, KJR05, KN03].

**Audio-** [KJR05].

**Audio-and**

[BS01b, KN03].

**Augmented**

[CS07e, You01].

**Augmenting** [AL04].

**August**

[AM07, Be00, B+02, Bon03, Fra04, HH04, HH05, HAO0, JQ04, KKP02, KI01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch04b, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a].

**Australia**

[Boy01, IZ00].

**DKU05, Pf01, Jef08**. **Authentic**

[DGMS03, Zur01, SS01b].

**Authenticate**

[Bau03a, Bau03b].

**Authenticated**

[AGT01, BN00a, BPR00, BU02, BC04b, BMN01, BMP00, BCP01, CPF04, Chi08, DG03, DA03, EP02, GKK07, GL03, GTT03, HS07, KOY01, KY03, KRA03, Lee01, LHT09, MPS00, Mac01, MSJ02, MND+04, NA07, Nam02, Ng05, Pol01, SK00, Vau05b, WC01a, YPPK09, Yi04, ZCY02, BKN04, BCP07, CYY05, CYH05, Che04a, CLC08, CJ04, CJL05, GL06a, GM05, HTJ08, HWW02, HWWM03, Hsu05a, Hwa05, HL05c, HL05d, KOY09, KRY05, LKK03a, LKY03b, LL04a, LLL05, LKY05c, LKY05d, LHC08, LLR02, LRR06, LKP05a, Mi08, PQ03a, PQ06, RBB03, Sei05, SW05, SC05b, TLH05, T01a, Tse07, WH02a, XY04, WYW05, YC09a, YS02, YSH03, YRY05b, YPK08, ZC04, ZAX05, ZW05b, ZL05].

**Authenticating**

[AIP01, CG09, Fur05, JW05, PM08, RCB00, YSS+01, Lin01a].

**Authentication**

[AAK09, AP09, ANR01, Ano01b, Ano01c, Ano01e, Ano02d, AHK02, ANL01, BH06, BAC02, BCL+05b, BCG+02, BM03a, BH00a, BCC01, BDhKB09, BR02, BDF05, BDF01b, BM03c, BL02, BLDT09, BWE+00, CV03, CGP08, CS07b, CLK01a, CLK01b, CC05b, CC09, CJ03c, CWY05, CT09, Cin02, Cir01, CKG+02, CKJ+04, Cou01, CMB+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FM00b, Fre03, FSS01, Gan01a, Gar03a, GMW05, GSV02, GD02, GT02, Gut04c, Had00, HSHI01, HSHI02, HSHI06, HKW06, HY01, Hoe01, HS01b, HP00, HL07, ISS08, Jab01, JP02a, JP07, JP02b, KJR05, KC09b, KH05, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LTT+04, LB04, LLL05c, LSH03b, LM00, LH+08, Lys07, MM01a, Mal02, MJ04, MD04, JR03, MGC02, MNT06, Nao02, Nik02a, Nik02b, OKE02, OH08].

**Authenticating** [PB00, Par04, PC05, PK01, Qu01, RKZD02, Ric07, Ril02, 8]
[DPV04]. Barken [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, IR02].

Based [Ano01c, ANR01, AF03, AJO08, BDG01, BKLS02, BNPS02, BN02, Ben00, BRS02, BF01b, BF03, BB04, Bon07, BCHK07, BGH07, BPR08, BD03, BMN01, Boy03, BQR01, BLM01c, BSNO00, BRTM09, CGFSHG09, ČvTMH01, CK02a, CGMM02, CF01b, CC02a, CV03, CPP04, CCD07, CS07b, CLT07, CHSS02, CHM02, CZK05, CM05a, CTH08, CGK02, Coc01b, Cou01, CFS01, CS00, DN00a, DKMR05, DT03, EHK03, EM03, FL06, FM02a, FMY01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GP06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HC08, HH09, Igl02, Jam00, KBD03, KLM06, KJR05, KKG03, KY02a, Kwo03a, KHHK05, LHL03a, LF03, LKY05a, LKY05b, LHY05, LD01, LTH05, LPM05, LW05a, LWZH05, LYG07, LLW08a, LLW08b, LCC05, LSA07, LCZ05c, LCZ05a, LLC06a, Mic01, MR09, MI09, Mit00, MB08, MCO4, MPPM09, MV03b, NZCC05, NC09, NNSK05, OS09, PCSV07, PW05, PBMB01, PSC09, PS08a, Pel06, PSM08, PC00, PLJ05a, PLJ05b, based [QCB05a, Reg03, Reg04, RG09, RCG05+09, Seo02, SG07, Sco04, Seo05, SPG02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SCS05a, mSgFlL05, SSM08, SW05, SH00, SK01b, SCL05, SLCO5, Smu02, SCS05c, TWNA08, Tsa05, UHA09, UEBEP09, VS01, VKS09, WAF00, WL07, WP07, WQ08, WHH05, Whi09, WW00, W02b, WW05, XMST07, YW04, YCW08, YS04, hY08, YJ00, YPSZ01, YRY05c, YPKL08, YY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRMS05, NZS05]. Bases [AAC01, ADDS06, BKP09, B02, ČvTMH01, EBC00, FJ03, FLA03, CCT08, Fau09, ZT03]. Basic [Gol01b, Gol01a, Gol04, Kat05b, Puc03, Ste02, Bon00]. Basics [Leh06, Lut02].

Basing [BPR08, CHL02, AGGM06, AGGM10]. Basis [RMH03b, Vav03, vW01, GPS05, LS05b, RMH03a]. Batch [Ara02, HLT01, PBD07, Sha01d, BLH06, HLH00]. Batching [SB01]. Battery [CBSU06].
Bay [Cal00c]. Bayes [Goo00]. BB84 [IHa02a]. BC [IEE02]. BCH [MLC01]. BDD [KLN06, Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pan02a, CNPQ03, YJ00, vT01]. Beach [IEE00a]. beat [Lev01]. because [AJ08]. Become [Ort00]. Been [Nic01]. BeepBeep [Dri02]. before [Uni00a, Uni00b, Uni00c, Uni00e, YJ00]. Beginning [Dew08, Hoo05]. Beginnings [Bud00b]. Begins [MP00]. Behavior [Vav03]. BEHEMOTH [Bar00c]. behind [Hen06b]. Beijing [FLY06, LST05]. Being [ASW01, ES00a]. beleid [dL00]. Belgium [DR02c, Pre00, QS00]. Belief [BPST02]. believing [Buh06]. Bell [BZ02, Eke02]. Benchmark [Ase02, TLY04, LDH06, YLT06]. Bendy [Sas07]. Benefit [YKL02a]. benefits [CH00]. Benford [NM09]. Bergen [Ytr06]. Berkeley [IEE06]. Berlin [FLA03]. Bermuda [Bl03]. Bernard [DNRS03]. Berners [Coc02b]. Berners-Lee [Coc02b]. Best [Bau01a, Bau01b, MFS09, Gol08, Ste02]. BestCrypt [Bau02b]. Bethesda [ACM09]. Better [FV03, PM00, RR02, SKQ01, HLLL03, Pau03]. BetterBASIC [ASW01]. Between [DKMR05, Ket06, Ngu05, NN06, Fa09, GKM00, MS09c, PCG01, RMH03b, SM03b, SXY01, VKS09, ATSV00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, Pri00, RMP08, SWR05, UHA09, WW08, ZFK04]. Bit-Fixing [KZ07, KZ03]. Bit-Locker [Kor09]. Bits [BS01d, SZ01, HN04, Shp02]. Bitslice [DFV01]. Black [Aro01i, CF02, CFS05, DI05, DRR05, DS08, KY01d]. Black-Box [Aro01i, BS02, CF02, CFS05, DI05, DRR05, KY01d]. Blackmailing [PS01b]. Bletchley [Sal00b, Cop05, Cop06, HS01a, Sal05a, SE01, Sni01b, Wei06]. Blind [AO00, BP00a, BSC01b, CL01b, JK01b, LL07, Na05, Pau02b, SP08, ZTP05, ZK02, Fa03, HC04a, JLL01, JLL04, LHY05, LCZ05b, MS09a, SV08a, SHT05, WH05, ZC05]. blindness [AvdH00]. Blink [Sas07]. Block [AIK01, BS02, BR02, BSC01a, CVTM01, Can01b, CLL00, CP02, CMB05, Cro01, DR00a, Dwo03, EYCP00, Flu02a, HSH01, JKK01, KCP01, KHY01, KKG03, LRW02, MV00, MS02e, NP01, OMS01, Pat01, PS06, Pl01, RM05, SM03b, SY02, SK01, SK01, WC01, XH03, YG01b, Bal08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kato05, KJ01, LDH06, LCP04, KKH08, MM05, PSP08, RBB03, SSM09].
buys [Zaf00]. Buzzes [Coc02b]. Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGR07, LLR02, LLR06, PI06]. Byzantine-Resistant [CNV06].

C [Ter08, Zol01, III00, Oiw09, RMPJ08, Sea05, Sea09, VM03, WK01, Wel05]. C# [Ter08, Zol01, III00, Oiw09, RMPJ08, Sea05, Sea09, VM03, WK01, Wel05].

C-testable [RMPJ08]. C2C [HTJ08]. CA [ACM03b, Joy03b, KKP02, Men05, Men07, Nac01, Oka04, Poi06, Pre02c, USE02a, USE02b]. CAA [MGC02]. Cache [BTTF02, Klc07, OST05, OST06, TSS+03, Ino05, WL07]. cache-based [WL07]. Caches [GSVC02, LLK05]. Caernarvon [TKP+08]. Caesar [Cha02, Yon06].

CAIDA [Pli00]. Cairo [EBC+00]. CalLC [Sil01]. calculus [MRST06]. Calcutta [Roy00].

Calibrating [SDMN06]. Calif [ACM03c]. California [ACM03a, ACM07, Bel00, Bon03, Fra04, IEE00a, Kil01a, Sch01c, Sch04a, Sch05a, Sho05a, USE00b, USE02c, Wi109, Yun02a, IEE06]. Call [An004a, An007b, An007a, MD04]. Calls [WG05, An008c, WC05]. Cambridge [ACM10, Chr00, Chr01, CCMMR02, CCMMR05, IEE03, JQ04, Kat05b, Kil05, Nao04, Pag03, Puc03, Rot07].

Camellia [AIK+01, HQ01, KM02, LHL+02, SM03b, SKI01, XH05]. Camera [CGK+02]. Camera-Based [CGK+02]. Can [BB02, CZB+01, Dav01c, Lai08, Ros07, Ver06b, CNPQ03, CG05, SBB05, Zir07].

Canada [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, YY01]. Candidate [III00, EYCP00, NIS00, SKW+00, SL00]. Candidates [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC00a, WB00]. 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 [IEE05b]. Card [BCST00, CMG+01, CL07, DF01, DFPS06, RE03, RS01, SR01, Ano00k, Ano01, AJ01b, Bor00, BGL+03, Bur00, Cal00c, Car01, CCCY01, Cha05a, Cla00b, Con00, CH00, DFCW00, GMG00, Ham01a, Has02, Hen01, Hus01, Jac00, LSA+07, LC05a, Lu07, QS00, RE00, SP02, Smi00, VK08, Zaf00, Che00, FGL02, Pau02b, SKK00, TY03].

card-based [LSA+07]. CARDIS [DFPS06]. CARDIS'98 [QS00]. Cards [And04, AJ01b, Bel01, CK06, DJLT01, HBdJ01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NFQ03, QSO1, Sak01, Sha01c, TBL01, VPG01, YKMY01, Ano04b, Ano04c, AJ01a, BPR01, BCH05, Bur00, DFH01, DFPS07, Fin03, GUQ01, HHSS01, Hsu05b, KLY03, LKY05a, Ler02, LCS09, MY01, Poh01, PB01, Pre07, SVD07, TIS07, Ano03a, BJvdB02, CL04d, CCK04b, Che00, Gro03, HL05b, Ku04, KC05, LHY02, Sco04, SCF01, YY04].

CardS4 [GN01]. Care [Mad00, RC06, An003a]. carefully [Cha00b]. Carlo [Bii09, Sug03]. cars [LPW06].

Cartilage [MYC01]. Cartography [SGM09, SWR05]. Cascade [DG+04].

Cascaded [Jou04]. Case [ABK00, An005a, BBGM08, BU02, BCP01, CNS02, GS07a, Nie02b, OST05, Vau01, BKN04, BF06a, BK05, CSK+08, HRS08, KWDB06, Mic02a, Mic02b, OST06, Pei09, STY07, SKW+07, SPH06, ZW01].

case/average [Mic02b]. cases [ABHS09]. Cash [PS01b]. Cathedral [USE02a]. Cats [Pen01b].

Caught [Wei00]. cause [SB05]. Causes [Mur01]. Cautionary [GMP01a].

Cayley [Lan91]. Cayman [Syv02]. CBC [BBKN01, BPR05, BR00b, DGH+04, Fer06, JMV02, Kl03, Vau01, Vau02]. CBIDs [MC04]. CCA [KOMM01, MII01b]. CCA2 [BST02, Lin03, RG09]. CCA2-Secure [Lin03]. CCG [TL06]. CCM [Dwo03].
CCS [Mart02b, MS05b]. CDH [CM05a].
CDH-Based [CM05a]. Cell
[Fox00, MYC01, SHL07]. Cell-phone-free
[Fox00]. Cellular [La00, LZ04, MGC02,
PZL09, SBZ04, Bao04, ETM05, KK03,
SHH07, Wan04a, dRMS05, Wue09]. Center
[AUW01, CH01a, CYH04, LPM05].
Centered [BKM07, CMB+05]. 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, CMG+01, RdS01,
Bra01a, LCK04, ZSM05]. Certification
[An01k, CHM+02, RSA00b, BGB09,
BD04b, KB09].
Certified [ANR01, CSV07, NZCG05, BCL05a, BCW05,
CWH00, CCH05, CJ05, HW04, HW05, HL04,
LL06, LWK05a, NZS05, Shao04b, Shao05b,
THL05, Tsa05, 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
[Cla00a, GV09, Nao03, Sta03, SVEG09].
Chang [CWJT01, ZC05].
Chang-Wu [CWJT01].
change [CYH05].
Changes [Mur01].
Changing [BST03].
Channel [BU02, CHV03, Law09a, LCK03, MH02,
NM005, OT03a, OT03b, Sch06a, SYLC05,
ARR03, BP03a, BG07b, Buh06, CNPQ03,
KSW00, LCZ05b, PSP+08, WL07,
YTWY05].
Channels [AIP01, CK02b, Nam02, Vau05b, LH04].
Chaos [JK01b, SK01b, WZW05, JK01a,
LMC+03, MC03, PSG+09].
Chaos-Based
[ZZW05, SK01b, JK01a, PSG+09].
Chaotic
[LLL+01, SXY01, USSR02, Vav03, AMRP00,
ÁMP04, GhdGSS00, GB09, HHYW07,
HLWZW09, JK01b, LMC+03, LYG07,
MA02, PBMB01, PS01a, PZL09, SPG02,
SL09, UHA+09, VKS09, WG02, WW08,
kWpLwW01, WLW04, YZEE09].
Chapman
[Kat05b, Was08a].
chapter [MAaT05, Tat05].
Characteristic
[Gau02, GPS06, KT00, Ver02, GPS05].
Characterization
[AJ08, Nam02, XH03, BGM04, KY00, QVP05, XLS06].
Characterizations
[Pa05].
Characterizing
[BTW05, BT08].
Charging
[BACS02, RH02].
Chatter
[Kee05].
Chaum
[BNPS02, KLN+06, WH05].
Chauvin
[Ma03a].
Charging
[CCL09, OK06, LZ05a, PRS04, PZ01a, PZ02a, ZP01].
Check [Kir01b].
Checkable
[BPS02].
Checking
[BPS02, JZ00, PRS04].
checklists [Sha01a].
Checks [FM02a].
Checksums
[St01, SGPH98].
Cheju
[Kim01].
Chemical
[EIG01, Chen [LW05c].
Chemnich
[CV04, RD01, Roy05].
CHES
[JQ04, KP02, KP01, KN01, RS05,
WP03].
CHESS
[LKHL09].
CHESS-64
[LKHL09].
Chicago
[ACMO4b, Top02, Con00].
Chien
[YYY05b].
Children
[Pau02a, Syc00].
China
[B+02, DWMLZ05, FLY06, JY00,
GGH+08, RG05].
checklists [Sha01a].
Checks [FM02a].
Checksums
[St01, SGPH98].
Cheju
[Kim01].
Chemical
[EIG01, Chen [LW05c].
Chemnich
[CV04, RD01, Roy05].
CHES
[JQ04, KP02, KP01, KN01, RS05,
WP03].
CHESS
[LKHL09].
CHESS-64
[LKHL09].
Chicago
[ACMO4b, Top02, Con00].
Chien
[YYY05b].
Children
[Pau02a, Syc00].
China
[B+02, DWMLZ05, FLY06, JY00,
GGH+08, RG05].
checklists [Sha01a].
Checks [FM02a].
Checksums
[St01, SGPH98].
Cheju
[Kim01].
Chemical
[EIG01, Chen [LW05c].
Chemnich
[CV04, RD01, Roy05].
CHES
[JQ04, KP02, KP01, KN01, RS05,
WP03].
CHESS
[LKHL09].
CHESS-64
[LKHL09].
Chicago
[ACMO4b, Top02, Con00].
Chien
[YYY05b].
Children
[Pau02a, Syc00].
China
[B+02, DWMLZ05, FLY06, JY00,
GGH+08, RG05].
checklists [Sha01a].
Checks [FM02a].
Checksums
[St01, SGPH98].
Cheju
[Kim01].
Chosen-Plaintext [DN02a, KM01c, Ki01a].

Cincinnati [BD08].

Cinematic [CAC03].

Cipher [AIK+01, BRS02, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DP050, DF07, Dwo03, EYCP00, FF01a, Flh02a, GBM02, HCJ02, HQ01, KYHC01, KHD01, LKHL09, MSN07, NPV01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY+02, SYX01, SBEW01, SKI01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BVP+04, GPX08, GGG05a, Hey03, KHO00, LKH+08, Mac00, PSP+08, RBB03, Sal00b, SHH07, WW08, Wins05b, WF02, XH05].

Ciphers [AAG+00, BBKN01, BS00b, BR01, BKM07, CvTMH01, Can01b, CF01b, Can06b, CJS01, Chu02, CHJ02, CP02, CM03, Cou09, DPV01, Eaq05, Fil00, FF01a, Fil02, Gol01d, HR00, HR04a, HSH+01, Jam00, Jan06, Kan01, KCP01, KKG03, LRW02, MV00, Oni01, PP06a, Plt01, RMS05, Sar02, SM03b, SKU+00, Wal00, Wri05, ??02, YG01b, ZC00, Bai08, Bar06a, Bel07a, Ber07, Bod99, DLP+09, DY01, Dun06, DK08, Egh00, GP06, HW03a, HWR09, Hey03, JKR01b, Jun05, Kat05a, KSW00, Kin01, LMS07, LDH06, Lun09, Max06, MIO09, MWM01, Pin06, SJH04, Smi01b, SL07, SB05, TT00, Wag03, YI00, You06, Kat05b].

Ciphertext [BBK03a, BCHK07, CKN03, CF01b, CS07c, CHJ+01a, CHJ+01b, CS02, CS03b, Des00b, DK05, FP01, JKR02, JJO00b, KS00a, KY01a, KCJ+01, KM03, KUR01, Man01, Nov01, PV06b, Shoo00b, BM050, CHP+09, IM06, KG09, Poi00].

Ciphertexts [AFI06, BGW05, BGN05, Gen04b, JJO00a].

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

Circuits [Bl05a, FLM+03, Gol03, ISW03, MD05, PBTV07, You01, GLC+04].

Circumvention [Kha05].

Cirencester [Hon01, Pat03b, Sma05].

CISM [PPV96].

CISC [FLY06].

citizens [Ano03a].

clamping [Ano03a].

Clandestine [Wri05].

Class [Car02, KM01a, KKH03, NN06, OP01a, Plt01, SBZ02, DKL00b, Fox00, HM00, Uni01].

Classes [CY02, RSA00c].

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

Classification [HMS04, PBD00, Uni01].

client [RSA09a].

Cleaner [TR09a, TR09b].

Cleaning [Lut03].

Clear [Lut03].

Close [DM07b].

clauses [SV08a].

cloud [CKS09].

Clouds [GS01, VS01].

Cluster [Haf01, KCD07, SEF+06, TLC06, TW07].

Cluster-Based [KCD07].

Clusters [MFS+09].

CM [CMK00, GHK+06].

CMS [BWBL02, DKU05].

Co [Bud00b, Nd05, ACM01b].

Co-Design [Nd05].

Co-operation [Bud00b].

Coalition [ACJT00].

Coalition-Resistant [ACJT00].

coarse [Rhi03].

Coast [Boy01].

Cod [IEE05b].

Code [Ark05, BR04, CD00b, CV03, Cer04b, FIP02a, FF01b, HSZI01, Imr03, KY01e, Lai08, OS09, Reo01, Rey01, Sal00a, Sin02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MJ05, RSA09a, SM00c, SM05, SM07a, Sin99, Sin00, Sve08, AAG+00, SE01].

Code-based [BR04, OS09, BGB09].

Codebook [CTH08, YWWS09, WJP07].

Codebook-linked [YWWS09].

Codebreaker [Hau03, Plt06].

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

Codebreaking [Bud00a, Bud00b, Sin01b,
Alv00, Bud02, Cop05, Cop06]. **codec**

[Che08a]. **Coded** [MLC01]. **Codes**

[Bee05, BP06, Big08, Bod99, BQR01, CC09, Chu02, CDG05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ??02, YYDO01, Yek07, Bel07a, aSM01, Bul09, DB04, DKL00b, DW05, DW01, Gar03a, HW09, Kov01, Lam07, Lun09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02]. **codeword**

[AJ08]. **Coding**

[Buc00a, CS05c, HHL00, Joy00, LLL01, MZ02, Pat03b, RK06, Sal05c, Sma05, TW02, TW06b, Yru06, Che07, DW05, Gar04, Hon01, PPV96, Scho0a, Sch01c, S+03, Sch04a, Sch04b, Scho0a, Seo05, Seo99, TW05, Irw03]. **Coefficient**

[CH01b, KT00]. **Cohen**

[Was03a]. **Coherent** [TPPM07]. **Coin**

[Lin01b]. **Coin-Tossing** [Lin01b]. **Coins**

[HR04b]. **Cold**

[ShS08a, AJO8, HS+08b, HS+09]. **cold-boot** [HS+08b, HS+09].

**collaboration**

[ED03, PCSM07, SBG05, SBG07]. **collaborative** [LLY07]. **collapse** [SBB05].

**Collection** [GMM08, Bro05a]. **Collections**

[Kuh00]. **Collective** [BBB02]. **collide** [GNP05]. **Collision** [DG02, ITO05, WYY05a, WYY05d, GM00a, Sem00]. **Collision-Resistant** [IKO05]. **Collisions**

[BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c]. **Collusion**

[BGW05, HNZI02, Zan01]. **Color**

[WKP03]. **Color**

[CTL04, Che07, Che08a, CTY09, FGD01, AEEdR05, CDD07, Yan02, YCL07]. **Colorado** [BC01, Sch04b, USE004]. **Colored** [CDD07]. **Colossus**

[Cop04a, Cop05, Cop06, Lav06, Sal00b, Sal00a, Sal05a, Sal05x]. **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, An03e]. **Coming**

[Dan01]. **Comment** [SCS05b, WY05, WLW04]. **Comments** [AS01c, CGH00b, JW01, MNFG02, SKW00, CJT04]. **Commerce**

[CLK01b, GS02a, Kir01a, Sta00, Uni01, ZYM05, BM03a, FB01, Gra01, MY01, SN07, YCO9a]. **commercial** [LCC05, YLR05]. **Commitment** [DN02b, DMS00, FF00, CAC06, HR07, KKL09]. **Commitments**

[BN00b, CF01a, DFS04, FM02a, Gen04a, HNO09]. **Committee** [Uni00a, Uni00b]. **committing** [DN00a, Nid02b]. **commodity**

[CGL08a, CGL08b, CGL08c]. **Common** [Pas03, TG07]. **Commonwealth** [PY05]. **communicating** [Hut01]. **Communication**

[AK02a, ANRS01, BJK08, BBK03a, BIW08, Big08, Col03, Fis05, GKK+09, LLS+09, Mar07, NA07, PL01, Sch06b, SKR02, Wir05, vDW05, BJK04, BC05b, CC05c, CGP03, EY09, GKK+07, GG05b, GC05, HYS03, JZ09, JRS09, KPS02, LPM05, Lin02, MP08, PBMB01, Par04, RH03, SNW01, UP05, WWA01]. **Communication-Efficient** [Fis05, LLS09]. **Communications**

[CG00a, Gau02, JRB06, MS02e, SW00a, WW00, FGM03, JL03, Sma01, WB00]. **Companies** [Ste00].

**Company** [ASW01, Zaf00]. **Comparative**

[DPR01, GLG02, Kat05b]. **Comparing** [HU05, KLN06]. **Comparison** [CG00a, GC01a, Gau02, JRB+06, MS02e, SW00a, WW00, FGM03, JL03, Sma01, WB00]. **Compendium** [Lut02]. **Compensated**
[AAK09]. competition [Cla00b]. compiler [DFG00, Oiw09]. Compilers [Lut02]. complement [YC09b]. Complementary [AS01c]. Complete [Bar00a, Bee05, Bud00a, FGMO01, GCKL08, HMS04, KY00, MS09c, Sal07, TWM+09, Bud02]. Completeness [HG03, MW04, ABHS09, PT08]. Complex [JKK+01, LKLK05]. Complexity [BYJK08, BLM01, BDTK08, CB01, DN00a, FBW01, GKK07, GKK+09, HR04a, Lut02, Nie02b, RMH03b, Ros00, Rot05, Slp03, BYJK04, CDD00, GKK+07, GIKR01, Gor05, JZ09, Mic02a, MP08, RMH03a, Rot02b, Rot03, Slp99, SPHH06, TW06a, SV08a, Fal07, Rot07].

Complexity-Theoretic [CB01].

Compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BSL02, Hei01, TEM+01]. composability [PS04c]. Composable [AF04b, BOHL+05, BLDT09, CF01a, CK02b, DN02b, DN03, NMO05, RK05, Can01a, CLOS02].

Composite [CQS01, GMP01a, RDJ+01, Zhe01].

Composition [BJP02, BN00a, CR03, CV02, Pie05, Sho00a, Can06a, LLR02, LLR06, Puc06].

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

comprehensive [DLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08].

Compressibility [HN06]. Compression [ABM08, BD03, HSKC01, Kei02, LHS05, RS08, Sal07, SDFH00, WWL+02, WC03, FS08, Gar04, La00, LJ05a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TTTZ01, Zir07].

Compression-Encryption-Hiding [BD03].

Compromise [Ahm08, Lai08]. Compromised [ZYN08]. computability [Pet08]. Computable [Vad03].

Computation [ACS02, Bai01b, BCL+05b, BI05a, BIM00, BJLS02, CC00, CD00, CDN01, CDG+05, CDI05, DN03, DI05, DM00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, Jef08, KO04, KLML05, KSR02, Lin01b, PS05, WW05, Ano02g, AB09, BEZ00, BEZ01, CLOS02, CLC08, CDD00, DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WHH05, WY05, SM07b, Duw03].

computation-efficient [CLC08].

Computational [CCL09, DLP+09, GH02, HG03, KLR09, KK06, Rup09, SM07b, WvD02, AUW01, IKOS08, Lam01, Lau08a, Nie02a, Sho05b, SHJR04].

Computationally [MPSW05].

Computations [HL05a, ML05, RHM04, SBZ04, TC05].

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

Computer [BS03, Bi03, Bro05a, BCDH09, BC01, CSW+08, CZK05, CGK+02, Coo02a, Coo03, HY05b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Iee00, JBR05, KM07, Le06, Lut02, MYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Tyn05, Cas02, DFGH04, Fan09, FPO06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Sha06, SLO6, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coc03].

computerized [LM+03, Pau02].

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

Computing [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BB09, CG00a, CK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Lut03, May04, PHM03, Sch06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Wri00, Yan00, YKMB08, Cha07, Che05b, CHT02, DHL06, HV09, HKPR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sei05, Wil99, YLR05, Lut03].

Compuware [Ano02d]. conceal [BB79].
Concealing [DMS00]. Concealment [DA03]. Concept [ARC01]. concepts [AB09, Kra07, SWSR05, MC04]. concerning [HW03b]. Concerns [MP00]. concrete [KNS05]. Concurrency [JL00]. Concurrent [BP02, DPV04, Gen04a, KKG03, Ros00a, Dam00].

Conditional [LMV05, WN02]. Conditions [IK05]. Conference [ACM03a, ACM04a, Ano06b, AAC01, AJ01b, Bel00, B+02, BZ02, BS01b, Bih03, Bla03, Bon03, Boy01, Buc00a, CC04a, CV04, CGP03, CGH+00b, Cra05a, DKU05, DFCW00, DFPFS06, EBC+00, ELyS01, FLY06, Fra01, FMA02, Fra04, FLA+03, HR06, HYZ05b, IEE09a, IKY05, JYJ04, JM03, Joy03b, Jue04, KJR05, Kil01a, Kim02, KN03, Kn02, Lai03, LL03, Lee04b, LTT+04, LL04c, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Nao1, Nao04, Ok00, Ok04, Pato3b, Pem01b, Pfe01, Poi06, Pre00, Pre92, RD01, Roy00a, Roy05, Sho05a, Sil01, SM07b, Sma05, Syv02, USE00c, USE00a, USE01a, USE01b, USE02c, Wil99, Won01, Wri03, Yun02a, YDKM06, ZJ04, Zhe02b, ZHY03, AUW01, BC05b, DV05, DWML05, DRS05, Hon01, Kil05, Li05, PC05a, PY05, PP96, Q500, Son00, WK06].

Confidences [Gan01a]. Confidentiality [Dwo03, Pem01a, YC08]. configurable [MBS04]. Configuration [Sha02, Mos06].

Confirmation [SK00]. Confirmner [CM00, GM03]. Confiscation [DBS01]. Conformance [LBR00, RSA00].

confounded [Bel07a]. confusion [She01].

congestion [SBB00]. Congress [Un00a, Un00b, Un00f, Un00e, Un00h].

congruences [Ste08]. Congruential [CS05b, LS05a, SB05].

conic [LCC05, LCZ05a]. Conjecture [CU01].

Conjugacy [CJ03a]. Conjugate [Igl02].

Connected [BJLS02, HFB01]. Connection [HR00, Jam00, Goo00, Mic02b].

Connection-Polynomials [Jam00].

Connections [WRW02]. Conquer [SKQ01].

conscious [DMSW09]. Consensus [CNV06]. Considerations [DBS+06, Hei07, Rub01, Sch07, SVEG09].

Considering [WA07]. Consistency [ABC+05, JEZ04].

Constant [App07, Bli05a, CS07c, CD01a, DPV04, DN02b, DJ05, Lin01b, Sun00a, IK05].

Constant-Depth [Bli05a]. Constant-Round [DPV04, DI05, Lin01b].

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

constraints [CC05d, LPM05, SN04].

Construct [CDMP05]. constructed [Tsa05]. Constructible [NNT05].

Constructing [Des00b, Fig01b, Vadd03, Wen03, JZCW05, NS01a, ZL05].

Construction [BBKN01, BB00b, Car02, CMK07, Lin03, Nie02c, SM00a, TNM00, YWD08, DW05, SC02c].

Constructions [BS00a, BR00b, BS02, GMW05, GGM05, GM02c, Jon04, PR08, PZ02b, SNWX01, SM00b, GT00, GP08, IK03, NR04, PR05, Reg03, Req04, vDKST06].

constructive [GGH+08]. consumption [Mis08].

Contact [YKMY01, Car00]. Contact-Less [YKMY01].

Contactless [And04, K02a, Cla00b, Fin03].

Contemporary [Ahm07, Opp05, SVEG09].

Content [AAK09, CGJ+02, HHJS04, MA00a, MA00b, RE02, XMST07, YKW01, ATS04, DY09a, SG07].

Content-adaptive [XMST07].

Content-Based [RE02, YKW01, SG07]. Content-triggered [HHJS04].

Contest [Bar00b]. Context [DJL01, FPS01, SN04].

continue [Lov01].

continued [Dan02]. Contra [Mah04].

contract [WK05]. Contrast [BDDS03, HKS00, HT06, K03, CDFM05].

Contrast-optimal [HKS00].

Contrast-Sensitive [HT06]. Control [ABEL05, ANRS01, B07, CGMM02, H08, L05, Sma03a, ZGLX05, BNP08, DFM04, DPT+02, JW06, KNS05, LKZ+04].
MD04, MSP+08, PS04b, STY07, WC01b].

Control-flow [ABEL05]. Controlled [GVC+08, IMM01, AW05, AW08, LAPS08].

Controlling [HY03, MS03b, MS02d, WL05].

Controls [Har01a, Har01b]. conventional [CJ04, YW05, YRY05b]. Converging [Pot07]. Conversation [GK04].

courses [VAYY09]. Conversion [CD05, Ket06]. Conversions [KL01b].

Convertible [Chi08, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b]. Convolution [PG05]. cookbook [VM03]. cookies [Cha05a]. Cool [Ano00d]. Coordinate [OS01]. COPACOBANA [GKN+08]. Copenhagen [TBJ02]. Copley [USE01b, USE01a]. coprocessing [ML05].

Correcting [MZ02, NN06, YYDO01, ZYR01]. Correction [BQR01, CTBA+01, Din05, LN08, LW05b, MPSW05, TEM+01, Gar04]. Correctness [PBD05, Bel07b, HSD+05, dH08].

Correlated [FWW04]. Correlation [BSC01b, CJS01, Gol01c, JJO0d, LV04, LMOV05, MH04, Nyb01, SY01a, WRW02, ZC00, GQ05b, JJO2a]. Correlations [KM00, KM01b]. corruption [XNK+05].

COS [FF01a, WB02]. Cost [CDF01, FBW01, PD07, Sta05, YEP+06, CL09, SHJR04, YLR05]. Cost-Effective [PD07]. cost-ineffectiveness [YL05].

could [Clao0b, Faul02b]. Counter [DIS02, QS01, SLG+05, SL06, MJ05].

Counter-Measures [QS01]. Countering [PP06b, SK05b]. Countermeasure [IT03, MM09, OT03a, PKBD01, YKLM02a].

Countermeasures [Av03, Fry00, GM00b, MOP06, OST05, Has01b, JDJ01, Man08, OST06]. Counters [KMO01]. counterterrorism [Na05].

Counting [Gau02, Kuh00, Hig08]. Couple [SXY01]. coupled [LF03]. course [AA04b, GV09, GL05]. courses [Gha07].

Cover [GA05, Gut02a, LNP02, NN03, RS00]. coverings [SC02b]. Covert [Col03]. Cozens [Sal03b]. CPCMS [Sha02]. CPI [ECG+07].

CPOL [BZP05]. CPUs [ESG+05]. Crack [Sin02, Ano08b]. Crackberries [Sta05]. Cracked [AAG+00, Nic01, Pri00]. Crackers [Ols00, SE01, SE02, NRR00]. Cracking [DZ01, BZ03, Cur05]. Crackproof [Sal03b]. Cracks [Bar00a, Ste05c]. Cramer [Luc02b, VMSV05].

CRC [Kato05b, Spr03, SGPH05]. Creation [MV01, Top02, MB08]. Creator [Coc01a].

Credentials [CL02a, CL04a, LLW05, LLW09]. Credit [CNB+02]. Crete [ACM01a]. crime [Cas02, KB00, Lau08b].

criminal [Men03]. criminals [Win05c]. Criteria [Can01b, IBM00]. criterion [QP05].

Critical [LKM+05, SE09, CS07a, Gor05]. cron [Oue05]. Cropping [SDH00]. Cross [Ban02b, SM08, LCX08, SLP07].

cross-authentication [LCX08]. cross-disciplinary [SM08]. cross-layer [SLP07]. Cross-Platform [Ban02b].

crowd [Fox00]. CRT [FMP03, Kuh02a, May02].

CRT-Exponent [May02]. crypt [Per03].

Crypanalyses [Kan01, SKU+00].

Crypanalyst [ASK07, AMR00, An03, Ano07b, Ano07a, BDG+01, Bae04, BLH06, BP03a, BBK03a, Bar06a, BP01a, BD00a, Biho00, BFM02, BDK02a, BDK02b, BS01, BDD03, BD00b, BCCN01, CGS08G09, CV02, CC01, CL01b, CYY05, CK05, CKB+02, CW01, CJ03, Ch06, Cho08b, CH02, CP02, Cout04, CGJ+02, DG00, DGP07a, DGP07b, DGP09, DGP09b].
DN00b, FJ03, FKS\(^+00\), FKL\(^+01b\), FKL\(^+01a\), Fin06, Flu02a, Flu02b, Fur01, Fur02a, Fur02b, GS07a, GM02a, GJSS01, GS02c, GM02b, GM00b, GM02, GC00b, Gra02a, GS09, GKN\(^+08\), HPC02, HQR01, HAU04, Hen06a, HLL\(^+01\), HSM\(^+02\), HHK\(^+04\), Hsu05a, HLH00, Hwa00, JK02a, JJ00c, JJ01, JmBdXm05, Jou09, Joy03a, KM02, KW03, KS00b, KRY05, KV02, KRS\(^+02\), KKS00b, Kra02a, KC05, Küh01, Küh02b, KHKL05, LC03, 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, Pel06, PS06, PS01c, QCBB05a, Sch06a, Sco04, Sha03c, Sha05a, STK02, SGB01, SK08, SK01, SHH07, TIGD01, TM06, TLH05, TJ01, TSS\(^+03\), Wag00, Wag03, WL05, WBD01, WBD02, Wu02, XY04, YSD02, YW05, YKL02a, YKL02b, YRY05a, YY05a, You01, YG01a, YG01c, ZYR01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, AMRP04, BF01a, Bai08, Bar09, BS01c, Buh06, Bul09, Bur02, CV05, CKN06, CKL\(^+03\), Dun06, Egh00, EBS01, Eke09, Fie09, GPG06, Goo00, Jun05, KSWH00, Kuh01, LMSV07, Max06, MAA03, MAA04, MAA05, MAA06, MAA07, Nybo1, Pha04, RSQ03, Rup09, SK01a, Sel00, Sin09, SL07, SCS05b, SLL\(^+00\), Swe08, TC00, TM01, WLH04, WF02, YI00, YY00, YKL03, Kat05b]. Cryptanalyst [Wil06]. Cryptanalytic [BS00b, KFS00, Oec03, QSR\(^+02\), Yan07, Wil01a]. Cryptic [Wir05]. CRYPTIM [Ust01b]. CRYPTO [Bra04, Men07, Sho05a, Ahm08, Ano01j, Ano03c, Bau01a, Bau01b, Bu01, CCM01, CNB\(^+02\), Lev01, Lev02, Mar08a, Mar02b, MC04, Pem01b, SYL05, TR09a, TR09b, Yun02b, Bec02, BK05, HGN03, Web02, Bel00, Bon03, Kih01a, Yun02a, Sei00a]. Crypto-algorithms [Ano01j, CCM01]. Crypto-based [MC04]. Crypto-CCS [Mar02b]. Crypto-integrity [Yun02b]. Crypto-systems [Ano01j, CCM01]. Cryptoanalysis [HSR02, LD01]. CryptoAPI [Bon00]. Cryptoclub [BP06]. Cryptocomplexity [Rot05, Fu07]. Cryptocoprocessor [HV04]. Cryptographer [Joy03b, Nak01, Oka04, Pol06, Pre02c, Men05]. Cryptographers [Coc03, KLN\(^+06\), Tsa07, Bel07a, Haut03]. Cryptographic [AC02, AADK05, AL00a, ADH\(^+07\), Ase02, BLST01, BDF\(^+01a\), Bar00a, BGK\(^+03\), Bih03, Bla01a, Box01, BDP02, Bra01b, BM01c, BL08, Bure06, CC04a, Can01b, Car02, CCD01, CHL02, CKY07, CB01, Cra05a, CS09, CO09, DD02, DHMR07, DF04, DWN01, DHR00, DV08, DFG01, FIP01b, FS00, Fis01a, FGA00a, Fre01, GMP01a, Gar05, GSS08, GGKT05, GK02, GTH02, Gor02a, GL00, GU01, Gut00, Gut02b, Gut04a, HTS02, HN06, Har06, Has01a, HL05a, HC08, Ig02, IY00, Ito01, IMM01, JT05, KMO01, KY01, KY02b, Kil01b, KS06a, Knu02, Kis02, Law08a, LN08, LS05a, LK01, MS02a, MOP06, Mea01, MNP01, MRL\(^+02\), MMH02, Mor03, MK05b, MS05, NIS01a, NIS01b, Nao03, Nd05, Ngu05, Nie04, OTI01, OP01a, PKBD01, PR08, PJDH09, Pem01b, Pfu01, Pin03, PS02b]. Cryptographic [Pot06, Pre00, Pre02a, Pre02b, RSA04d, RSA01, RR00, RRS06, Rot01, RSN\(^+01\), SM00a, SS01a, SGM09, Sha02, Shp03, Shy02, SFDF06, SR06, SL09, TLY04, TW08, TBDL01, Uzu04, WK03, WN02, WBL01, WCO1, You01, Zha08, ÂMR04, ACT05, ALV02, AV04, BGB09, BDSV08, Bla01b, BP05, BG08, BG09, BDN02, BD04a, BGL\(^+03\), BM06, BR05, Can01a, Can06a, CHC04, Coh03, CC05d, CDL06, DP04, Dug04, DFG00, FS03a, FSGV01, GT00, GPV08, GJ04, GM04, GB09, HY03, IK03, IYK02, IYK03, JW01, KAM08, KSF00, KP03, LMT05, Lau05, LL05, LLW09, ML05, Mea04,
MT07, Mic02b, MRST06, Mon03, NN03, NdM04, NdM06, PS04a, PSC+09, PR05, Pre07, Pri00, Puc06, QPV05, Reg03, Reg04, RMH04, RBF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, kWpLwW01.
cryptographic [WLW04, XLMS06, YLT06, ZLK99, ZWL01, ZLO4b, dH08, BWBL02, JQ04, KKP02, KP01, KNP01, RS05].
Cryptographically [ADD09, AHS08, BJP02, BFCZ08, BB00b, FR08, MS02b, RGX06, Aam03, AW05, AW08, Laut08a, SM03a].
Cryptographically-masked [AHS08].
CryptoGraphics [CK06].
cryptographie [RSA09a].
Cryptology [LSY01].
cryptography [HMV04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irw03, IS06, IS08, JY04, JL00, JT01b, JT01a, Jue04, Kak06, KLR09, KZ07, KGS07, Kat05b, KB06, KBM09, KPMF02, KWDB06, KY01c, Kir01a, KMS02, KZ02, KS03, KP06, Lam01, LGS01, LSY01, Lee03b, LLL+01, Lie05, LDM04, LW05b, LP02b, Lut03, Lys08, MNT+00, MP02, Mao01, Mao04, MZ04, Mao01, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pe06, PM02, PBB02, Poi02, PTC06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGG08, Sti95, Sti01, Sti02, Sti06c, SJ05, Syv02, TSO00, TW06a, TG04, TW02, TW06b, Tro08, TR09a, TR09b, Uni01, USS02, VY01, VM02].
Cryptography [WPS01, Wei04, WK01, Wl05, Wie00, WvD02, Wri00, YWC08, Ytr06, YC01, YDKM06, ZYH03, vDW04, Imr03, AMW07, AUW01, Ano02a, Ano02g, ABDS01, Beat09b, BBD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BEZ00, BEZ01, BGM04, BEM+07, Buc06a, Buc01, Buc04, BLR09, BMA00a, BMA00b, BMA00c, CCT08, CDFM05, CDD07, Cos00, CDD07, Dif01, DIM08, DwWnW05, DOPS04, DKL09, DW09, Du03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK07, Gek04, GRTZ02, Gol99, GG05b, GHPT05, GPS05, GNP05, HH05, HIL+00, HKPR05, HA00, Hig08, HKS00, Hoo05, HG05b, HLWZ09, IF00, IM06, JK01b, Jan08b, Joy00, KZ03, KLO8, Kat01, Kil05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Lop06, Mau04, May01, McA08, MBS04, MM07a, Mol07, NP02a].
cryptography [Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, Pin06, Reg05, Reg09, Rot02b, Rot03, Roy00b, Rup09, STY07, SBRZ04, SC06, SH05, Shp99, Si05, Sin99, Sin00, Sma04, ST01d, SK01b, TW05, UHA09, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wri03, YCO9a, YCO9, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sio01, 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, CMG07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Lai03, LL04c, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka04, Pot06, Rot05, RS02, Sha03b, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bih03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam91, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, PC05a, Poi06, Pre02c, RD01, Roy00a, Roy05, Sho05a, 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, NSNK05, NBD01, Ove06, PHK+01, YG01a, YG01c, Zhe02a, Zhe06, Bau04, CL02b, CCH04, Cho06, CFVZ06, CHH01, Dan02, DHL06, EKRM01, GHGSS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04b, LL06, LKYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SPG02, SCS05a, SP79, SLC05, Sun00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, hY08].

Cryptosystems
[Aki09, Ava03, BDG+01, BKLS02, BPS00, BM00, CHSS02, CCW02, DDG+06, DKKY02, ESG+05, FJ03, Fel06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KMY02, KI01b, KMY04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vad03, WY02, XB01, ZLK02, Ban05, BF06a, BB79, CHC01, CMKT00, EBS01, EHKH04, GH08, GBK01, HM00, Has00, Has01b, Huih00, HP01, KW00, Kos01c, LD01, Luk01, Mic01, Mis06, OS00, Pei09, PLJ05b, SSST06, Sha05c, Sm01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WW00, YY00, ZS01, vT01].

cryptovirology [YY04]. CRYPTREC
[IY00]. CSCW [ZP05]. CT [Joy03b, Men05, Nac01, Oka04, Pot06, Pre02c, ZC09].

CT-RSA [Joy03b, Men05, Nac01, Oka04, Pot06, Pre02c, ZC09]. CTO [An03e]. CTS [Con00]. Cuban [AJ08]. Cube
[DS08, PDMS09]. Cube-Type [PDMS09]. culture [Gil07]. Cumulative [WP03]. cure [RD09]. cure-all [RD09]. Current
[DHF01, PRS04, LPW06]. curriculum
[FOP06]. Curve
[ANS05, ADI09, An05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BM01, CQS01, CFA+06, GPP08, HYZ05a, HMY01, HM02c, JTO1b, JTO1a, KMB09, KPMF02, KWS02, LW02, Mä02, Kir03, OTIT01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, W08a, WPS01, XB01, YY01, ZLK02, BS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, CHH01, Dan02, DHL06, EKRM01, GHGSS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04b, LL06, LKYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SPG02, SCS05a, SP79, SLC05, Sun00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, hY08].

Curve-Based [KW06, Pel06]. Curves
[AHRH08, Bai01a, BB00b, CY02, Ga01, GLV01, Gau02, GHK+06, Kid02, PWGP03, Ver02, CMKT00, Hus04, LWZH05, MP01b, MSV04, Sim02, SC02b, Was08b, Wen03, Yas08]. customer [Lin01a]. CVS
[DFG01]. Cyber [FNRC05, WW04, Man05]. Cyberinsurance [BP07]. Cybersecurity
[PLW07]. cyberspace [Mit02]. cycles
[ABHS09, BPS08]. Cyclic [PG05, Mic02a]. Czech
[MJ04].

D [Dw03, Ben00, ChLY09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05]. D.R
[Irw03]. daemons [Mos06]. Danmgår
[CDMP05]. dark [Bla09]. darkening
[CDD07]. DARPA [Coc01a]. Data
[ACM03a, ACM04a, ABM08, An02a, AAC+01, BG02, B+02, BNPW03, Bro05b, Che01a, CTL01, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, Kös02, Män05].
Lan00b, LP00, LHS05, LS08, Lut03, MND+04, MS03b, MFS*09, NM09, OS05, Per05, RKZD02, RK06, Sal03a, Sal07, Sin01a, SDMN06, TZD05, TPPM07, VDKP05, WS05, WY02, WN02, kc01, vW01, AG09, AHK03b, AKSX04, Arn01, Bla00, BNP08, CCMT09, Cer04a, CHe04a, CHe04b, CHe05a, GPH98, SETB08, WMDR08, YLC*09, YC08, ZSJN07, Zir07, Cur05, DK08, Lin02, Pap05].

Data-Hiding [VDKP05].

Data/image [S*03].

Database [ACM03c, ACM05b, BI05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Mau04, PS08h, PBVB01].

Database-service-provider [HILM02].

Databases [AK02b, CDM*05, DN04, AHK03a, CDD*05, CKY07, GA03, MSP09, MNT06, NS05b, ÜG08, YPPK09].

Datenverschlüsselung [Lin02].

Dedicated [DN04].

Details [AY09, AS05i, BPS*07, CA08, CH08, CK10, CK10b, CL04c, SC02c, BR09, CL04c, SC02c, decomposing vDKST06].

Decomposition [BSP*07, CL04c, SC02c, Decomposing vDKST06].

Decipherability [aSM01, Sav04].

Deciphering [Eri02, KB07, Ark05, Lov01, NS01a].

Decision [DJ06, GR04, KM04a].

Decisive [CUC01].

Decisions [Coc02a, Coc02a, Decisions CUC01].

Defeating [CSK*08].

Defective [BTTF02, Dav01b, Dav01c, KLR09].

Defending [NRR00, Pro01].

Defense [GK02, HW01, Mir05, Wy05, BV02].

Defenses [SL06].

Definition [YWD08, SN00].

Definitions [Uni01, AH05].

Definitive [BS01a, BSB05, Gar03b].

Defining [YRS08].

Degenerate [Ber09a].

Degradation [BSC01a].

Degree [CV02, QVP05].

Degrees [Sat06].

Déjà [DP00].

DeKaRT [Go03].

Delacorte [Imr03].

Delay [WR02, NS01a].

Delays warning [WM03].

Delays warning [WM03].

Delays warning [WM03].

Delays warning [WM03].

Delays warning [WM03].

Demonstrably [HL06].

Demystifying [RR04].

Deniability [Pas03].

Deniable
[Nao02, CCK04a, CSK08, DG05, LC05b, YRY05c, Zha06]. Denial [Mah04, Nik02a, Nik02b, PKBD01, Ril02, Mir05].

Denial-of-Service [Nik02a, PKBD01].

Denmark [Cra05a, TBJ02].

Denver [ACM01b, Sch04b, USE00d].

Department [Bol02, Eri01].

Dependable [NABG03, And08].

Dependent [Gol03, WS05, BPS05, BPS08].

deployed [BDET00].

Deploying [BH00b, GSB04]. Deployment [CL07, KDO01, Mur01, Sin01a, App05, JRR09].

Dept [Uni01].

Depth [BI05a].

Derandomization [BOV03, BOV07].

Derivation [DGH04].

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, AIC01, ARC01, Bar00b, Can01b, CCDP01, Cim02, CB01, CS03b, CMB05, CLZ02, DR02a, DR02b, DF07, EHK03, FF01a, FZH05, GSS08, Geb04, Gut02b, Gut04a, HRL09, Hro05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04b, LB05, MKP09, MP00, Nd05, NS02, Rhi03, SJT09, SPG02, SRQL03, Uzu04, WZW05, WW08, WLLL09, ARJ08, CMS08, GG05b, Gut04c, HC04a, Htu01, KSF00, MI09, MWM01, SVEG09, YCW08, YC08].

Design/CPN [AADK05].

designated [LV07].

Designing [HBC08, TCR03, C02, CG05, Lan00c].

Designs [Bee05, CC02a, Bai08, Des00a, WL07].

Desktop [Mun08, BDET00].

Desmedt [CHH09].

Desynchronization [CDTT05].

Detached [Sha01c].

Detailed [Lut03].

Details [Scr01].

Detect [FOB05].

Detecting [CMS09, FGD01, JQYY01, Har07a, LHL04].

Detection [AS01b, AD07, BB00a, BKM07, CH01b, CZK05, JT05, KG03, SK01, SY01a, SLT01, ST01c, TZD05, TMMM05, WO05, YI01, Zan01, Bej06, BBK03, HLL02, Men03, NN02, WMS08, YW06, ZGTG05].

Detection/Correction [SKQ01].

Detector [BSC01b, DNP07].

Determined [KKH03].

Determining [KS03, LQ08, OS07].

Deterministic [BK06a, Her06, KZ03, KZ07, May04, BK07].

dev [BH05].

Developers [An06a, Dev00, MK05b, Nis03a].

Developing [MV03b, Cra05b, Gal02, HL06].

Development [An02e, CNB02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a].

Developments [An03e, Pre07, Sha04a].

develops [Pau02b].

Deviates [Run55, Ran01].

Device [Ric07, ST03b, WPS01].

Devices [BCH00, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KHD01, MV01, MRL02, SCF01, WC01a, Ano06a, CMS08, DMT07, Tse07, ZYW07].

Devil [Blu01c].

DFT [Che08a].

DH [Lys02].

DHIES [ABR01].

Development [CM09].

Dictionary [BPR00, BCP02b, CS07b, D06, Pho01, NS05a].

did [MH09].

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

Dies [Bar00a, Coc01a].

difference [PBMB01, dW02].

Different [LS08, WWTH08].

Different [CGMM02, Sma01].

Differential [Av03, BMM00, BF00a, BFMR02, BD02a, Cr00, CV02, CK02, CKL03, Eke09, Fur02a, Gra02a, HLM01, HSM02, HHK04, IIT03, JT01a, Kan01, KM02, KCP01, VLC02, MP06, MMT09, MHL02, MG08, PSC02, PQ03b, SK01a, SKU00, SKL01, YSD02, vW01, BF01a, CUS08, Che08a, DLP09, Egl00, EBS01, Pha04, SLL00, 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, CRKT08, FS01b, GR04, Ki01b, KK02, KM04a, Kra03, Kra05, Mis08, Ts06, YYY05c].
diffuser [Fer06].
diuser [She01].
diusing [She01].
digest [MSP09].
Digit [KWP06, Tan07a, BG09, HKPR05, Kir01b].
digital [ANS05, AvdH00, AR00, AS08, Ano01f, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BSO9b, Ca00b, CCH05, CC09, Che01b, CFS01, CM02, CM08, 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, Mek01, PL01, PJH01, PCG01, PZL09, PBM+07, Ram01, Rds01, RS01, Sam09, Sch00d, Sch06b, Sc01, Sha01e, SC02a, Sh08, SL01, Sng01, TJ03, US02, VHP01, VK07, WNY09, Wm05a, WBD01, Wu01, WV01, WC03, WC04, Wym02, XFZ01, XYL09, YWWS09, YYDO01, YYZ01, ZWC02, Zho02, AAPP07, AA08, Ano00i, Ate04, BL06, Bra01a, Ca00a, CS08a, CWH00, CL00, CJ05, Che07, Die00, FB01, GGG03, Gil07, HRL09, HLL00, HHC05, KP00, Lev01].
digital [LLC06b, MK08, NRR00, PC05b, PL05a, PBV08, QC05b, Sha01d, Sha04b, Sh05d, SCL05, TCC02, TND+09, UP05, WQ08, WHL03, XC05, XM0T07, An009, Ano13, BCK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].
Digital-Audio [WNY09].
Digital-Signature [Eng00]. Digits [Che04b, Ran55, Ran01]. Dimension [DDG+06, TZ09a, TZ09b].
Dimensionality [SBG02]. dimensions [CLR09]. Dining [KLN+06]. diplomacy [Alv00].
directional [PJK01]. Directions [Sha01b, DFH01].
director [Mad04]. directories [C+02, Pet03]. directory [C+02]. disabled [Pau02a]. disadvantage [CD07].
Disappear [Per05]. Disappearing [Way02b, Way09]. disappointed [Ste00].
Disaster [WCZ05]. disciplinary [SM08].
disclosure [JMO7, Swi05]. Discovery [Bi09, HLL+02, SGB07, SGA07]. Discrete [CS03a, CNS02, Che04b, COW20, Gen00b, GV05, GPP08, KOC09b, LW02, LJO05, VK07, HNO4, HW03a, HWR09, Hsu05a, HLU0d, JL03, JLL01, HLL0a, HLY05, LTH05, PL05a, QCB05a, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SLC05, SCS05c, Yas08].
discretized [MA02]. Discryption [Har07b].
discursive [Mit02]. Discussion [Ano01a, Ano01b, Ano01c, Ano01d, Ano01e, Ano01f, Ano01g, Ano01h, Ano01i, Ano01k, KLB+02a, Mal02, Nik02b].
Dishonest [GKK07]. disjoint [Gut04c].
Disk [Cro01, Har07b, Si06, CS08a, Fer06].
dismantles [Hil06]. dispatches [Kee05].
displayed [CGV09]. Displays [Kuh02a].
Disputed [CAC06]. Distance [CGF09, CPHX04, DM07b, DW01].
distinguished [HWW04, WH02b].
Distinguishing [HSR+01]. Distortion [BG08, CS05c]. Distortion-Free [BG08].
Distortions [HH09, SDF01]. Distributed [BCS02, BT02, CL01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJK03, GS02c, GTH02, LLY06, SC01, WT02, And08, AFG06, BDE00, CO09, FMY02, KKL09, LN04, LW08a, M+08, FS08a, Raj06, WZB05, YbJ04].
Distribution [BDF+01a, BOH0+05, BSB000, FSO1b, Ina02a, Ina02b, Ku02, LLL02, NAO7, Sch01a, YI01, ATS04, BA07, CY014, GL06b, MP08, SLP07, Sh01p, Sh04b, WHHT08, YS04, ZLG01].
Distributions [CY08]. Diversity [Kun01]. Divide [SKQ01].
Division [HZZ05, Tan07a, Che08b, MN14]. Divisor [KMO1a]. DL [HRL09, PL05a, Sch01f, Sch01e, WMD08].
DL-based [HRL09, PLJ05b].
DL-encryption [Sch01f]. DL-keys [Sch01e].
DL-STD M [WMDR08]. DLP [MSV04].
DM [Eag05]. DNA [GPX08]. DNF [BGN05]. D [Kle07]. Do
[Bur06, HSR +01, HR04b, Win01, BB79].
Dobb’s [Dr.00c]. Document [ISO05, PJH01, ST01c, VHP01, CDS07, CL04c].
Documents [PJK01, AW05, AW08, DGK+04, GA03, ÚG08]. Does
[AB01, Pie05, Con09]. Doing [BM01a].
Dolev [BPS08, BDNN02, ZD05]. Domain [AS08, Bar00c, BSCO1a, BSCO1b, BSL02, CKJ+04, Cor00b, Cor02, DOP05, DNP07, GW01, ISSZ08, Kuh02a, Lan00d, LZ01, MM01a, OMT02, PBC05, SOHS01, SDFH00, ZLK02, BR06, CS05a, DSP01, EKRMA01, Zir07]. Domains
[BR01, CLK01a, CLK01b, Van01]. Domingo [CKN06]. Dominic [Rot07]. Dominica [PY05]. domino [LLLZ06a, LLLZ06b].
don’t [Win05c]. Don’ts [FSSF01]. DONUT [CLLL00]. Door [SF07]. Doors
[Eri02]. DOS-Resistant [Ano01e, ANL01]. Double [ADDS06, CY08, CMJP03, Cooke02a, Dim08, GH08, GB09, Hau06, JIW05].
double-base [DIM08]. Double-Gate [Cooke02a]. Double-Size [CMJP03].
double-trapdoor [JOW05]. Doubling [FO03]. Douglas [Spr03]. Down
[BBPV00, Cooke02b, Ano00g, Ano03c, Ano03a, Pot03, PBVB01, Ste05c]. Downwards
[FO03]. DPA [SGBP01, TV03]. DPA-Based [SGBP01]. Dr [Ano03e]. Dr. [Dr.00c]. draft
[Ste00, Dwo03]. drastic [Sug03]. drawn
[vOT08]. DRBG [Hir09]. Dress [Ahn08].
drinks [Ano03c]. Drive [NP07, Kor09].
DSA [MR01a, SA02, Shao1d, TvdKB+01]. DSA-type [Sha01d]. DSEA
[LLLZ06a, LLLZ06b]. DSP
[Geb04, WWGP00]. DSP-embedded
[Geb04]. DSPs [WWGP00]. DSS
[Ano09, Ano13, FIP00, Nat00]. DTD
[PK02]. Dual
[KHY04, LKLK05, SF07, WCJ09, ST03a].
dual-field [ST03a]. Dual-Pair [WCJ09].
Dual-Tree [LKLK05]. Dumb [Eri01].
Dummies [Cob04]. Dump [KCJ+01].
Dunaynir [MTH05], d’une [Car00].
Durahim [MAaTxx]. Durayhim’s
[MAaT04]. during [AJ08, Bec02, WA07].
Dust [KGS07]. Dutch [dL00]. Duty
[ZGLX05]. Dwork [DRNS03, GKH05, Zha06].
DWT [LHS05, PBC05]. DWT-Based
[LHS05]. Dynamic
[AFB05, BN08, BCP01, BCP02a, BF07, CL02a, CW09, CDF+04, CTT07, GTH02, HQ05, Pat01, SUG03, TT01, BBG+02, GL06b, LCP04, LYY06, LCK04, LCC05, RG05, Yi04].
dynamic-key [LCP04]. dynamics
[BGPS02, MR00].
E-business [Poh01, HHSS01].
E-Commerce
[Kir01a, BM03a, Gra01, SN07, Sta00, MY01].
E-Goods [NZCCG01]. e-Government
[RM02]. E-Learning [CAC06]. e-mail
[LL04b, NZS05, All06, ANR01, KS00a, Law05]. e-payment [Has02]. E-Security
[NJJ01]. E-smart [A01b]. e-voting
[JCT03, Cha04]. E-Wallet [ETZ00]. E0
[TVL04]. E2 [SUK+00]. Early
[ASW+01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Sm04, ZGTG05]. Easier [Pau09].
Easy [GR04, Hos06b]. Eavesdropping
[Kuh02a, Kee05]. eBook
[Ano02d, WWL+02]. EC [SF07]. ECC
[BWB12, CL09, Mi08, Ts05].
ECC-based [CL09, Ts05]. ECC2K
[LMO4]. ECC2K-130 [LMO4]. ECCV
[MJ04, TBJ02]. ECDSA [ANS05]. Eclipse
[Coc02b]. ECMA-305 [ECM00a].
ECMA-306 [ECM00b]. economics [Blc07].
ECPP [Che03]. ed [Gun04, Nis03a]. Edge
[Sta05]. Edinburgh [RS05, Pem01b]. Edit
[CGFSHG09]. editing [MAaTxx]. Edition
[Cho08a, Irw03, Spr03]. Editor
[MFS+09, Sak01, KP03, SK06]. Editorial
27

[Er01, Er02, FOP06]. Editors
[BK06b, PTP07, SJT09, SGK08]. EDK
[An02e]. Eds
[Duw03, Pag03]. Education
[Puz04, RC06, CAC03]. Effect [AEV+07].
Effective [CDR01, PD07, Sen03, SL06].
Effects [BBGM08, Har00, GJ04, SN07].
Efficiency [III00, GGKT05, SLG+05, GT00,
GGK03, KT06, YTH04]. Efficient
[ACS02, ABRW01, AEMR09, Bai01b,
BIN03, BKLS02, BR00a, BGP02,
BSDV08, BSK+03, BS00a, BF01c, BGH07,
BB00b, BCDM00, CKPS01, CL02a,
CCMT09, CCD07, CL01b, CPX04, CM05a,
CJL05, CT08b, CKK03, Cou01, Dam00,
DN03, Dhe03, FF00, Fis05, FS01c, GLV01,
GC01b, GTH02, GST04, GBKP01, HCJ02,
HSZ01, Has01a, HS00, HW04, HZS05,
HL07, Hiih00, HS07, KOY01, KOY09, KLY02,
KO03, KKH01, KKH03, LSY01, LCK01,
LKY05a, LKY05b, LCO5a, Mac01, MV03a,
MP01c, MN14, Nd05, NSNK05, OS01, PC03,
PB05, Ram01, RSQ03, RDJ+01, SM01,
SM03a, SRQL03, SSNGS00, TC05, WHL05,
WYY05d, WH01, WC01a, XBO1, XS03,
YWD08, YLH05, YW05, YZ05, YZ07].
efficient [LPV+09, LSL+09, LC04, LHH04,
LC02, Mic02a, MSP09, NR04, PCC03,
RGL05, RBB03, SL07, SLK05, Shao5b,
SC05a, WK05, XC05, Yan02, YTW05,
YC09a, ZSN05, ZYW07]. Efficiently
[IKNP03, NNT05, AGKS07]. efforts [Web00].
Egg [Pau02a]. Eggs [Wei06, Wei05].
EGPGV [MFS+09]. Egypt
[EBC+00, Imr03, Sin00]. Eighth
[ACM06, B+02, ELvS01, IEE01b]. Einstein
[MNT+00]. EJB [TEM+01]. Erkert
[Duw03]. El-Gamal [EKRA01]. Election
[JLL02, Cal00b]. Elections [Cha04, Pw01].
Electromagnetic [SGM09, QS01].
Electronic [Ble07, CL01b, CM02, Dur01,
H0f01, ISO05, IY00, KMO01, KS02, Lan04b,
LLL02, Mad00, MNFG02, Rub01, RMC01,
Str01a, YKMY01, ZYM05, AvdH00,
AAKD09, Cal00a, EY09, FB01, HJW05].

element [MS02d]. Elementary
[Sis09, Ste08, Tat05]. Elephant [Fer06].

Eleven [All03]. ElGamal [BJN00, CL02b,
CWH00, HL04, LHT09, SJ00].
ElGamal-like [CWH00, HL04]. Elizabeth
[Bud06]. Elliptic
[ADI09, An05a, Bai01a, BNP03, Bar00a,
BBGM08, BM00, BS01d, BMN01, BB00b,
CS01, CFA+06, GLV01, Gau02, GP08,
HY05a, HHH01, HMM04, HM02c, Hus04,
JT01b, J01a, KMO09, KPF02, Kid02,
KSZ02, LW02, MP01b, Mf02, Krs03,
OTT01, OS01, OT3b, PG03, RSA03b,
RS04, RS05, Sat06, Si05, Was08b, Was08b,
WPS01, XBO1, YYY01, v01, BSS04, BSS05,
BM04, BG07a, CCH04, Che05a, CFV06,
DIM08, Dw05, EH04, GBKP01, Hsu05a,
HL05d, JW06, LL04, LW05, Mis06,
MVS04, OS01, ST03a, SST06, SH05,
Sim02, Sma01, SC02b, SLC05, SLC05, TC05,
Ver01, YC09a, YC09d, ZSZ01, ZL05, ANS05,
BWW02]. Ellis [Coc01a]. Elmau
[IEE01b]. Else [FL01b]. EMA [QS01]. Email
[ES00b, Gar03a, Luc06]. Email-Based
[Gar03a]. emanations [ZT05]. Embedded
[An01c, An02d, An02e]. BBGM08, Br02,
D08, GSS08, JT05, J004, KK02, LPW06,
Nd05, RS05, SPG06, WW03, YSS+01,
ARJ08, BM04, F00x, Gb04, KV+09,
KP01, KNP01, K03, M04, Nis03a,
TCP+08, XQ07, Fin02]. Embedding
[A009, JX05, JG07, Sal03b, WY02, WC04,
KC09a, Wam05]. Embrace [CNB+02].
Embracing [An03c]. EMD [BR06].
Emperor [Sin01b]. Empirical
[HW03b, Goo00], empirically [SS03].
Empiness [DIS02]. Emulux
[CZ+01, CTBA+01]. Enabled
[Por06, CCC01, DY09a]. Enabling
[Web02]. encapsulation [CH+09, KG09].
Encipher [BR00a]. Enciphering
Encode [BR00a, BKN04, Ano08c].
Encode-Then-Encrypt [BR00a].
Encode-then-Encipher [BR00a].
encoded [WMS08]. Encoding
[JT01b, RS00, Lin02]. encounter [Win05c].
Encrypt [BKN04, BR00b, Dav01c, Pet05, Dav01b].
Encrypted [BBK03a, BGHP02, BGLS03,
CD01b, Hug04, Lan04a, LH07, RMCG01,
Sta02b, Van01, WRW02, Whi09, Woo00,
Ano06a, Bih02, BNP08, CCM07, CDD09,
CSK08, FJ04, HILM02, Hes04a, LSH00,
MW04, Pet03, ÜG08]. Encrypted
[Pro00, RC01, Zho06]. Encryption
[ABC05, Abe01, AS01a, Abe04, AP09,
AB01, ADR02, Ano03, Ano01f, Ano01g,
Ano01h, Ase02, ANR01, AFI06, AF03,
Bar00c, HI00, Baut02, BN00a, BR00a,
BBM00, BB04, BGW05, BB03, BNPW03,
BB02, Bur03, CD00a, CS03a, CK03, CHK05,
Che01a, CTL01, Chi08, Cho08a, CMR06,
Cla00a, Coc02b, Coc01b, CJNP00, CHJ01b,
CD01, CS02, CS03b, Cr01, Cur05, DS03,
DR01, DR02b, DR02c, DN00a, DN03,
Dan01, DJ06, Des00a, Des00b, Des00c,
DL98, DR02d, DA02, DFK03, DK05,
DS05b, Dri02, FIP01a, FL01a, GC01a,
GWS00, Gen03, GRW06, GH05, CD02,
GMM01, Gutxx, HSH08a, HS02a, HY05a,
HSH10, HK01, HW05, Har07b, Har00,
Hei07, Her09, HS00, HR05, HG03,
HL02, HGNP03, HLL05]. Encryption
[HLC08, ISSZ08, Joh03, Jol01, JK02b, JGG02,
JMV02, JKR01, Jut01, KB03, KSHY01,
KS00a, KY01a, Kha05, KKJ07, K0s01a,
Kra01, Kur01, KD04, Lai07, Lan00a, Lan00b,
LP03, LHT09, LY07, Lin03, LNP02, LMV05,
LCD07, Mna01, Mar07, Mar08a, Mar08b,
MF01, MM01c, MP01a, MP00, MP05,
Mö03a, Mor05, Mö01a, MS09c, NIS00,
Nan02, NZCG05, NZS05, NP02b, Nie02b,
PV06b, PM00, Pau09, Pem01a, PZL09,
PDM09, Pha04, Por01, PS00, Pre01, RM04,
RK06, RDJ01, Sam01, Sch00b, SJ00, Siv06,
SB00, CAC06, SRQL03, SPGQ06, SBZ02,
Sye00, TV03, Uni00a, Uni00c, Uni00e,
Uni00d, Uni00g, Uni00h, Ust01b, VMS05,
WZW05, WBRF00, Wri01, YEP06, YW06,
ASW00, Abd01, ABH09, AKSX04,
AMR00, ABW09, Ano00c, Ano00c, Ano00f,
Ano00g, Ano00h, Ano00j, Ano02a, Ano03e,
Ano06d]. encryption
[App05, Ate04, AcM05, AFGH06, BPS08,
BKN04, BR04, BB01+09, Ber09a, BBK03b,
Bir07, Bla00, BJ00, Bro05, CB06, CS08a,
CBSU06, CH01, CKRT08, DL01, DL07,
DRS05, DW01, Fer06, PB01, Fox00, FMS05,
GMR08, GGG03, Gen09a, Gen09b,
GKM00, Gou09, Gu05, Gut04c, HSH08b,
HSH09, HS02b, HYYW07, HCD08a,
HCD08b, AHA04, HW02, Hsu05a,
Hua05, HLC05, HLC05d, IM06, JK01a, JK01b,
JX05, JWA05, JJ01b, KY05, JCD07,
KCD07, Per03, SKKS00, WWGP00, YSR01, SU07].
End-to-End [YSR01]. Ended [Küss02].
Endomorphisms [GLV01]. Endpoint [Kad07]. Enemies [DM07b]. Energy [GC01b, Ino05, LPV+09, SLP07, Mis08]. Energy-efficient [LPV+09].
Energy-security [Ino05]. enforce [SN04]. Enforcement [GN06]. enforcing [BP05]. Enforcing [GMM08, HRS08].
Engine [Fri01, MMH02, DP04, SHL07]. engineer [Pau02b, SN04]. engineering [CNB+02, MNT+00, MYC01, Pem01b, Roy00, SM07b, TR09a, TR09b, VH09, And08, EC05, Jeon09, Man08].
engeenrs [Pri00]. engines [PM08]. Enhance [ZWC02]. Enhanced [JKRW01, ZGLX05, OP01b, TWL05, WHH05, ZSM05].
enhanced-security [OP01b]. Enhanced-security [LPV+09].
Enhancement [CJ05, LSH03a, LSH03b, YW04].
enhancements [ADH+07]. Enhancing [BDK02a, MS05a, SE09, Sm00b, DY01].
enigma [Rob02, Rob09, BCB+05, Cas06, Chu02, Cop04b, DB04, GO03, Goo00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Wil01a, Win05b, Win00]. Enigma [Kap05].
Enough [CNB+02, Pat03a, YJ00].
Enrolment [HWH01]. Entangled [Bar00c, LB04]. Enterprise [BH00b, C+02, HM05, MJF07, App05, TCR03].
Entropic [DS05b]. Entropy [DS05b, EHMS00, LH07, JRS09].
Environment [BST03, DeL07, HS01b, LSV090, IM06, KKL09, KB00, Rhi03, Wh09, ZBP05].
Environmental [PS05]. Environments [CJK+04, LKHL09, BGR04, MNS08, SB05, SBG07, SN04, YC09a, YhJf04]. ephemeral [Mis08].
Ephemeralizer [Per05].
EPOC [JQY01]. ePOST [MPHD06]. EPR [Ina02b]. Equation [FJ03]. Equations [CP02, DDC+06, GS03, PBMB01].
Equipping [DMT07]. Equitability [DBS01]. equivalent [Fis01a, LQ08, MSV04]. Equivalent [Fer00, KOMM01, May04, SIR04].
Era [MP00, Uni00c, Bur00, Uni00f]. eraune [PCS03]. Erasures [JL00]. ERP [LSZ05].
Erratum [AGMM10, Kwo03b, LLLZ06a]. Erroneous [CH01b, MNT+00]. Error [BBK+03b, BQR01, Din05, KKG03, LM02, LM06, MPSW05, MZ02, NN06, SK01, Y01, YY00, ZY01, Zol01].
Erasures [JL00]. Error-Prone [MLC01].
Errors [AD07, AL07, Reg05, Reg09].
escape [Blu09, Fur05]. Escrow [AK02a, Ano01a, CL01a, DBS01, LCK01, ATSVY00, CL02b, LCC05].
Escrowed [PS01b]. eServer [AV04]. ESORICS [dCdVSG05]. espionage [Bud06]. essays [MAaT07]. Essential [Cop04b, Dr.00c, MR02a, MR02b].
essentials [HHL+00]. establishing [Kov03, KH03].
Establishment [BM03c, NIS03b, HMvdLM07, LF03, SL05a].
Estimation [EFY+05, JX05, KLB+02a, LNL+08, Sel00].
ethical [Har05b]. Euclidean [CPhX04, CMJP03, CLZ02, WL02]. EULA [WWL+02]. EUR [Eag05]. EUROCRYPT [Bh03, CC04a, Cra05a, Knu02, Pfi01, Pre00, GJSS01].
Eurographics [MFS+09].
Europe [Pag03]. European [AL06, CZ05, KGL04, Pre01, dCdVSG05, Ano00f, Che08b, Die00, Pre02a].
EUROPKI [AL06, CZ05, KGL04]. EV [HTJ08]. EV-C2C-PAKE [HTJ08].
Evaluate [Pre02a]. Evaluating [BGN05, NTW07].
Evaluation [BSC01a, EYCP00, FS00, FML+03, IKM00, IY00, J00a, Kan01, Kir03, SSKS00, BZP05, FXAM04, FS03a, LCP04, MCH05, RC05, RN00a, RN00b].
Evaluations [LM02].
Evangelizing [Coc01a]. evasion [Blu09].
even [Bh02, OS00, Win05c]. EventGuard [SL05b]. ever [Fur05]. Everlasting [DR02d].
Every [TH01, DKK07, Win05c].
Everything [CTBA+01]. Everywhere [CTBA+01].
Fan [YRY05c]. fare [GMG00]. Fascinating [Sch09]. FASME [RM02]. Fast [AL00b, ABM00, BDTW01, BST02, CJS01, CQS01, Cor00a, Cout03, Cro01, FS02, GC01a, GD02, GMM01, GPC08, HGG07, HR04a, JJ00d, KKM01, KK03, KKJ+07, LSY01, LS05b, MSNH07, Kir03, NS05a, NSS02, OKE02, OT03b, PG06, RR02, Tsa06, UHA+09, Yan05, ABB+04, BMA00a, BMA00b, BMA00c, JAW+00, J02a, Lu05, PBBM01, WWA01, Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d].

Faster [Bar00c, CMJP03, GLV01, KS09, LV04, Oec03, Ban05, Why05]. faszinierende [Sch09]. Fat [MYC01, TvdKB+01]. Fault [An04a, BM00, BK06b, BM07, DS03, Gir06, PV06a, PQ03b, YKL02b, HGR07, Lin07, Pl06, RMY04, YJ00, YKL03, ZL04a]. fault-based [YJ00], fault-tolerant [HGR07, Lin07, RMH04]. Faults [GSS08, VS08]. Favre [MFS+09]. FBI [Mad04]. FC [Bla03, Fra01, Jue04, PY05, Syv02, Wri03].

Fear [See04, Sty04, Sch03]. Feasibility [APV05, BDET00]. feasible [LM08]. Feature [GW01, Gut02a, HH09, LNP02, LLC06a, NN03]. Features [PK01, SBG02].

February [DR02c, Fra01, GH05, Joh03, Jue04, Kil05, Kim01, Men05, NP02a, Nao04, Oka04, PY05, Po06, Pre02c, RM04, Syv02, USE02a, Wil99]. Federated [DeL07, GTY08]. Feedback [CGFSHG09, CM03, Cout03, Igl02, Hey03, SPG02]. FeedForward [BP01a]. Feel [PM00]. Feeling [Buh06]. Feistel [Cou04, Kan01, LMSV07, On01, Pat04].

Feldman [AF04b]. Ferrer [CKN06]. Fetal [MYC01]. fetch [HTW07], Fi [Sty04, Bar03]. Fiat [VS08]. fiction [An03e]. FIDES [ISTE08]. Field [FJ03, GC01a, RDJ+01, CKY07, GMG00, Has00, J03, ST03a]. Fields [Bai01a, BT02, CU01, Che04b, CQS01, CFS05, HCK09, HHM01, KKH03, Lov01, MNP01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sim02, Sma01].

Fifth [ACM03b, SM07b]. Fighting [DGN03, SZ03]. File [CCDP01, GJS05, J01, LK01, BDET00, CSK+08, HTW07, Hos06b, ISO05, MKW00, MSP+08]. Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pet05]. Filesystems [WBL01].

Filter [LBGZ01, LBGZ02, MSNH07, Sar02, CMS08]. Filter-Combiner [Sar02]. Filtered [MH04]. Filtering [SDFH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00]. Finalists [EYCP00, IKM00, IK00, Mes00, Mes01, SKKS00, SW00a, WW00]. Financial [An05, Gri01, HMYH02, CL04d, MMJP03, UBEP09]. fingerprint-based [CL04d].

Fingerprinting [KT01, CTT07]. Fingerprints [TK03, KLY03, Sco04]. Fingers [MMH02]. Finite [BDET00]. Feasible [APV05, BDET00]. feasible [LM08].

February [DR02c, Fra01, GH05, Joh03, Jue04, Kil05, Kim01, Men05, NP02a, Nao04, Oka04, PY05, Po06, Pre02c, RM04, Syv02, USE02a, Wil99]. Federated [DeL07, GTY08]. Feedback [CGFSHG09, CM03, Cout03, Igl02, Hey03, SPG02]. FeedForward [BP01a]. Feel [PM00]. Feeling [Buh06]. Feistel [Cou04, Kan01, LMSV07, On01, Pat04].

Feldman [AF04b]. Ferrer [CKN06]. Fetal [MYC01]. fetch [HTW07], Fi [Sty04, Bar03]. Fiat [VS08]. fiction [An03e]. FIDES [ISTE08]. Field [FJ03, GC01a, RDJ+01, CKY07, GMG00, Has00, J03, ST03a]. Fields [Bai01a, BT02, CU01, Che04b, CQS01, CFS05, HCK09, HHM01, KKH03, Lov01, MNP01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sim02, Sma01].

Fifth [ACM03b, SM07b]. Fighting [DGN03, SZ03]. File [CCDP01, GJS05, J01, LK01, BDET00, CSK+08, HTW07, Hos06b, ISO05, MKW00, MSP+08]. Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pet05]. Filesystems [WBL01].

Filter [LBGZ01, LBGZ02, MSNH07, Sar02, CMS08]. Filter-Combiner [Sar02]. Filtered [MH04]. Filtering [SDFH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00]. Finalists [EYCP00, IKM00, IK00, Mes00, Mes01, SKKS00, SW00a, WW00]. Financial [An05, Gri01, HMYH02, CL04d, MMJP03, UBEP09]. fingerprint-based [CL04d].

Fingerprinting [KT01, CTT07]. Fingerprints [TK03, KLY03, Sco04]. Fingers [MMH02]. Finite [BDET00]. Feasible [APV05, BDET00]. feasible [LM08].
[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, WW01]. **Floating** [NS05c]. **Floating-Point** [NS05c]. **Flow** [BDNN02, ABEL05, FR08, ME08a, TWM⁺09]. **Flows** [ECM00a, AHS08, Cer04a, LAU02, SL05a]. **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]. **Forecasts** [Rai00]. **Forecasting** [WWL⁺02]. **Forensic** [PS08b, Cas02, Kor09]. **forensically** [ME08b]. **Forensics** [JBR05, CS04, CS08a, CDS07, MS09a, MKY08, MAC⁺03]. **Forest** [FBW01]. **Forgery** [CH01a, CKN00, LS01a, SLT01, HSW09]. **Forgotten** [Eag05, Kin01, OC03]. **Form** [AD09, CH07c, OS01, LKY00, Mic01]. **Formal** [BG09, Be07b, BCH05, BCJ⁺06, CL05, DKS08, GOR02b, HG03, Lan00d, Mea01, YWD08, ABHS09, JW01, Mea04, Pau01, ZLX99, ZL04b]. **Formalizing** [HM01a]. **Formally** [BPJ02]. **format** [ISO05, RG05]. **format-string** [RG05]. **Formation** [RW03a, Luk01]. **Formats** [GIS05]. **Former** [Mad04]. **Forms** [JT01b, LLL04]. **Formula** [Kog02]. **Formulae** [CH07b, WPP05]. **Formulas** [BGN05]. **Formulations** [AHHR08]. **Forum** [CZB⁺01, CTBA⁺01, CNB⁺02, CMB⁺05]. **forums** [Hil06]. **Forward** [AR00, AFI06, BY03, CHK03, IR01, HCD08a, HCD08b, ZYW07]. **Forward-Secure** [AR00, AFI06, CHK03, IR01]. **Forward-Security** [BY03]. **Forwarding** [KCD07, Kra02b]. **FOSS** [Bo102]. **Found** [Bar00a]. **Foundation** [LT03]. **Foundations** [DKK07, Gol01b, Gol01a, Gol04, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Nie02d, Sal05d, Kat05b, Puc03]. **Founder** [Bar00a, An03e]. **Four** [LXM⁺05]. **Four-Layer** [LXM⁺05]. **Fourier** [Che07, DSP01, DNP07, KC09b, LPZ06, SP04]. **Fourteenth** [USE00c]. **Fourth** [ACM02, ACM05b, DWCW00]. **FPGA** [An02e, CC02a, CB01, CG03, CNP03, EYCP00, EHKH04, KMM⁺06, KY09, KBM09, KR⁺02, LP02a, MM01b, MM01c, OTT01, OP03, Pat01, PBWT07, QSR⁺02, TULL02, TP01, USS02, WW00]. **FPAGAs** [AD07, DPR01, MM09, RS01, SNG03, SLG09, SK05a]. **Fractal** [AA04a, JLS03, WC03]. **Fraction** [Wal03]. **fractional** [DSP01, SSST06]. **fractions** [Dan02]. **Fragile** [CC09, CH01b, CT09, Nak01, FJK01, LYL07, SY01b]. **Frame** [LHS05]. **Frames** [WW05]. **Framework** [ANRS01, GL03, GOR02b, Hunt05, NO05, NP07, PS06, RS00, Shy02, ZY08, AHK03b, CCF01, CP07, CC04c, DMSW09, GJ05, GL06a, GM04, JE04, KNS05, MS09b, MBS04, YCW⁺08, HF00]. **France** [ACM04a, ACM05a, AJ01a, AJ01b, GH05, KN01, NP02a, PPV96, KM07]. **Francis** [Bud06]. **Francisco** [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b]. **FranzSteiner** [Eag05]. **fraud** [An03a]. **Fred** [Bar00b]. **Free** [AP09, An02e, Bau01a, Bau01b, BGI08, C01a, CNV06, DG02, HS00, HM01b, JP03, Jut01, Fox00, KS06b, SBG05, Bo102]. **FreeBSD** [CC02a, Mur02, Siv06]. **Freedom** [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, Mi03]. **FREENIX** [USE01b, USE02c]. **French** [Wri03]. **Frequencies** [DD02]. **Frequency**
Frequency-Domain [OMT02]. Frey [Was08a], friar [GG05a]. Friendly [CTY09, CRSP09, Hsu05b, HL05b, SZS05, WLT05a].

FrontPage [WWL +02]. FSE [Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d]. FTC [Ste05c]. fuels [Mad04].

Full [Cor00b, DOP05, LKHL09, WYY05b, WYY05c, BL04, CS08a, HS02b, LKH+08, Oiw09]. full-encryption [HS02b].

Full-Round [LKHL09, LKH+08]. Fully [BL08, FS01a, Gen09b, KPMF02, RG09, Gen09a]. Function [BR02, CDM05b, Fis01b, Fluo02b, GIS05, HNO+09, HPC02, JH00a, Kan01, Kii01b, Nie02c, RB01, Yan05, CHY02b, CJ04, HR07, LW04, LPM05, WWTH08, YW05, YRY05b].

Functional [ECM00a, WA06]. Functionalities [PS05]. functionality [ETMP05]. Functions [AEMR09, BBDK00, Bon01, Can01b, CV02, Car02, Che01c, DN02a, DGN03, DNR03, Fil02, FIPR05, GLG+02, HSM04, HR04b, Jou04, Kii01b, LTW05, Lys02, PR01, RR08, SM00a, SM00b, SS01a, Sho00a, Sho00b, Ver02, WP03, WFL04, Wer02, AGGM06, AGGM10, ALV02, CS09, KHC+08, HRS08, ISO04, KKO7, LLH02, LYK04, MS02b, Mic02a, Mic02b, NR04, PW08, QPV05, SM03a, WH09, YRY04, ZW05a, RRS06].

Fundamentals [And04, PHS03, Shi08, Way01, vT00, Fin03]. Funds [Coc01a]. Further [JS05, LL04a, LL05c, MP07, YRY05a].

Fusion [KZ09, TDZ05, ZS05, BG09]. fusul [MAA+05]. Future [ASW+01, An002f, Joh00, LNP02, NFQ03, Sch00e, HP00, LPW06]. Fuzzing [SG07].

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

G [Coc03, For04, WAs08a]. Gaitherburg [SMP+09]. Gamal [EKRA01]. Game [BHR00, LM02, CAC06, BR04, Gou09]. game-like [Gou09]. game-playing [BR04]. Gamers [MP00]. Games [KN08]. Ganesh [For04]. Ganzúa [GPG06]. Gap [OP01a, PWGP03, RW03a]. Gap-Problems [OP01a]. Gate [Coc02a, GC01a]. gates [TWM+09]. Gauging [PvS01]. Gauss [KKH03]. Gaussian [EKRA01, JL03].

Gbps [TPS01]. GCD [JP03]. GCD-Free [JP03]. GCM [KS09]. Geeks [McN03]. Geheimsschreiber [Joy00, UW00]. GEM [CHJ+01a, JM02].

General [AB09, CDM00, DN00a, ESG+05, GM01b, Kog02, Lin03, MND+04, Sal01a, YC01, YI06, JL03, LJ05a]. General-Purpose [ESG+05].

Generalisation [DJ01]. Generalization [YYZ01, HWW02]. Generalizations [LD04, LS08]. Generalized [KSR02, Mic02a, TC01, TJ01a, WAG02, WLH05, KYL00, Shio05]. Generate [HSR+01, Wer02, FSGV01]. Generated [ADD09, MRL+02, RB08]. Generating [BMK00, BCDM00, GG01, MK+06, SS03].

Generation [ACS02, BH05, BK06a, CS03c, ESG+05, GJKR03, GL01, GW01, JG01, MR01a, Ram01, TL07, TV03, WP03, WHL05, Web08, WS02, An004c, BK07, BG08, BF01c, ISTE08, LS05b]. Generator [ADD09, BP01a, DI05, Diet03, DGP07a, DGP07b, DV08, EHK+03, G000b, GM02a, Gol01c, GPR06, Int03, Kel05, LMHCETR06, LV04, SXY01, SFDF06, TWA08, TZZ09a, TZZ09b, ZKL01, Aam03, ACX05, Be08, BG08, BG09, BG07a, DGP09, GB09, HG05a, HLW09, JAW+00, KHK08, KSF00, Pan07, PSS+09, PSSP+08, PC00, RGG06, SR07, SB05, UHA+09, WW08, VKS09].

Generators [BST03, BK06a, BL08, C01b, CS05b, Fin06, Kral02a, LGZ01, LGZ02, LS05a, MH04, RSN+01, Vav03, BK07, BGPG05, CO09, SK01b, Tsa06, ZYEE09]. generators-part [SK01b]. Generic [BN00a, DOP05, GKT05, HLL05, Mar02b, MV01, GT00, MPO8, Sch01f, Sch01e, XLMS06, CHJ+01a]. Genetic [HSIR02, LMHCETR06, CV05, SC05a, WJP07].
Gennaro [Miy01].
Gennaro-Krawczyk-Rabin [Miy01].
gentle [RR03a]. Gentry [Hes04a]. Genus [CY02, GHK+06, Wen03]. Geometric [GTTC03, HH09, LLS05a, LL05c, LJ05b, SDF01, CJT01]. Geometrical [LWS05].
geometry [PPV96, WW06]. George [Gum04]. Georgia [IEE09b].
German [Sch09, Ano04b, Mor05, Sal00b, Sal00a, Win05b]. Germany [DRS05, Duw03, FLA+03, WKP03, IEE01b].
Geschichte [Sch09]. Get [Coc01a, WD01a, Cla00b]. gets [Bor00].
Getting [PM00]. GF [BINP03, KPMF02, KLY02, KKY02]. GH [GHW01]. GHS [Hes04b]. giant [Lam07].
Gibson [Ove06]. Giesbrecht [CHH01].
Gigabit [CGBS01]. Gigabits [HTS02].
Give [CNB+02]. Given [Wal03]. Giving [Tee06, Wu01].
Global [Ahm08, LWS05, Por06, Ano00h, BK00, Kee05, KB00].
Globus [MJD01]. GN [SC05b].
GN-authenticated [SC05b]. Gnaana [For04]. GNU [Coc01a]. GnuPG [JKS02, St10b]. GNY [Tee06]. Go [Bur06, CZB+01].
Goals [PHM03]. goes [Pan07].
Gold [Boy01, For04, Tsa07].
Goldreich [Kat05b, Lee03b, Puc03, AC02].
Gong [GG01].
Good [CB01, Kid02, MP06, GG05b, vOT08].
Goodness [CMB+05]. Goods [NZCG05].
Google [Con09, Law09b]. Googling [Con09]. GOST [SK01a]. got [Car01].
Goubin [Sma03b]. Governance [TPPM07].
Government [Y00, RM02, Lev01, LCS09].
Governments [An000g]. GPG [Bau01a, Bui01b, Luc06].
GPT [Ove06]. GQ [BP02]. graduate [GV09].
Grafton [Pag03]. grain [Rhi03].
Grained [SS01b]. Grand [Svy02]. granted [An000h].
Graph [CGBSHG09, GTTC03, HM02b, VVS01, YKW01, CTT07].
Graph-Based [CGBSHG09, HM02b, CTT07]. graphical
vOT08]. Graphics
[CK06, DNP07, MFS+09]. Graphs
[NNT05, Ust01b, WGL00]. Gravritlenko [Puz04].
Gray [FGD01, Har05b].
Gray-Scale [FGD01]. grayscale [YCL07].
greatest [Bel07a]. Greece [ACM01a, KGL04, SM07b]. greedy [HKPR05].
Green [TR09a, TR09b].
GREMLIN [H601]. Grenoble [ACM05a].
grey [BDN00, SCS05a]. Grid [ACM05a, MJD01, SEF+06, TLC06, ZBP05, Cha07, CJK+04].
GridOne [YC09b]. Grids [CTY09, MPPM09].
grip [But06]. Gröbner [CTCT08, FJ03, Bau09].
Group [ANRS01, AAFG01, ACJT00, BBS04, BCP01, BCP02a, BCP02b, CD00a, CvTMH01, Cho01a, HSH02, HSH06, HWW04, Hug02, JP02b, KY03, Kin02, LZL+01, MSU05, SOOI02, SWH05, Ste01, Tan07b, VMSV05, Wer02, AKSN04, BCP07, CLO4b, CYH04, CH05, CWNT04, CHT04, Cho08b, ED03, He02, Hen06a, HWW02, KS05a, KPT04, KKL09, LL06, LLY06, LPM05, LWW05, NS05b, PQ03a, PQ06, RH03, SNW01, Sha05a, T01a, Tse07, WGL00, WHHT08, YLC+09, YY05a, ZC04, ZK04]. group-by [YLC+09].
Group-Oriented [LZL+01, HWW04, CH05, CWNT01, LLY06, TJ01a, WHHT08].
Groups [BS02, CV03, CF02, Dre00, GM02a, GNT04, KM01a, LLY06, Pae03, Yi04].
Groupbook [SEK01, SEK02].
Guide [An000b, Cha05b, Ciu02].
Guadeloupe [Wri03]. Guanajuato [Buc00a].
Guangzhou [LLL+04, L05].
Guessing [AGK07, Bau05, Shi05, YS02, DLM05].
Guest [KP03, Sak01, BK06b, MFS+09, PTP07, SJT09, SGK08].
Guide [An000c, BS01a, BSB05, BCP+03, B01b, HM04, Poo03, Vac06, Wei04, And08, Bon00, Br05b, C+02, Che00, Gar03b, Kov03, Lum09, Mol05, SL06].
Guidebook [SEK01, SEK02].
Guided [ZY08, Pet08].
guidelines [Die00], Guildford [KN03].
Gummy [MMYH02], Guo [LLLZ06a, LLLZ06b], Gutmann [Uzu04].

H [Was08a], H.R. [Uni00d, Uni00h], H.R. [Uni00a, Uni00e], H64 [GM001].
Hack [MYC01, Sin02, SL06], hacked [Ano02c].
hacker [Gol08, Har05b], Hackers [SEK01, SEK02, Ano01h, BDO4b, NRR00, Win05c].
Hacking [Eri03, Eri08, Gum04, Man08, MSK03, SSS06, VGM04, Puz04, Har05b].
hacks [Sti06b, Sti06a], Hadamard [HSW05], Hagenberg [Jef08], Half [HS02b].
Halfspaces [KS06a], Hall [Bar00c, For04, Kat05b, Was08a, MAaT05].
Hall/CRC [Kat05b], Half/CRC [Kat05b, Was08a], Halmstad [BS01b].
Hamming [GK02], hamper [Lov01].
Hand [WBL01], Handbook [And04, Cas02, CFA+06, Jan06, MMJP03, RE03, AB09, Fin03, Har05b, KB00, KB03, MJ03, RE00, dLB07, Was08a].
Handheld [BMK00, Ano06a], Handhelds [MP00].
Handle [RC06], Handling [KL05, Lut03].
Handoff [OKE02], Hands [KLB+02b, Shu06].
Handshake [SB01].
Handshakes [Ver06a], Handwritting [Ano02d], Hankerson [Irw03].
Haptic [PBM+07], Haptics [Pau02a].
Hard [Har07b, HSS04, Lai07, CGHG06, GPV08].
Hard-Core [HSS04], Hard-Disk [Har07b].
Hard-Line [Lai07], hard-on-average [CGHG06].
hardcore [Sch01c], hardcore [Eag05, Pap03, Top02, Pap05].
Harddisk [Por01], hardening [Mos06].
Hardness [CHS05, CNS02, KYS02b, KS06a, LTW05, SV08b, AGG06, SU07, AGGM10].
Hardware [Ano02b, Ano07b, Ano07a, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GKO2, GPS05, GLG+02, Gro01, GPP08, KMM00, ISW03, JQ04, KKP02, NEX05, PS01c, RS05, RS04, SOTD00, SMT01, SM02, SM03b, SRQ03, SGK08, TSO00, TB01, WKP03, WBRF00, XH03, XBO1, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK+03b, EKHK04, GC00a, HBC+08, KP01, KN01, KR03, ND04, RA07, SOIG07, VS08, Hol04, YKLM03, YW06].
Hardware-based [Ano02b].
hardware-constrained [RA07].
hardware/software [ARJ08].
Harley [WPP05], Harn [GG01].
Hash [Ano08d, Ano12, AE09, BBKN01, BRS02, BDS09b, Bu06, Co00b, Cor02, CDMP05, CS02, DOP05, FIP02b, Fil02, GISO5, GLG+02, HPC02, HR04b, ISO04, Jou04, KM+06, MD05, RRS06, RR08, RB01, SSO1a, Sho00a, Sho00b, SK05a, WFLY04, Yn05, YZ00, BR06, KCL03, Ku04, KCC05, LLH02, KKY04, LW04, Mic02b, Wa00, YRF04, FIP02a, ZW05a].
Hash-based [BDS09b, KCL03, Ku04, KCC05].
Hash-CBC [BBKN01], Hash-Function [BRS02], Hash-functions [ISO04].
Hashes [Sch01a, GNP05].
Hashing [IKO05, SGG00, WS03].
HAVAL [WFLY04], HAVAL-128 [WFLY04].
HAVEGE [SS03], HB [MP07], HB-family [MP07], HCI [HKMB08].
headlines [Hen06a].
Health [Mad00, Ano03a, CCC01]. health-care [Ano03a].
Healthcare [BTTF02], health-care [Ano03a].
Healthcare [BTTF02], health-care [Ano03a].
health-care [BTTF02], health-care [Ano03a].
Herriot [Coc03]. Hersonissos [ACM01a]. Hessenberg [SSFC09].

Heterogeneous [BCS02, KHYM08, ZBLvB05]. Heterogenous [Hof01].

Heuristic [SS03]. HFE [FJ03, CHH01, Fel06]. HFE-Cryptosystems [Fel06].

HIBE [CS07c]. Hidden [HGNS03, KW03, LNS02, GMR05, Lun09, Shp05, FJ03, Sch09]. Hide [PH03, Shp05]. Hide-and-seek [Shp05].

Hiding [BD03, CLT07, Col03, DN02b, GA05, HNO09, LHS05, LS08, MH05, MMT09, VDK05, WC03, HR07, JDJ01, KP00, RSP05, Way02b, Way09, YCL07].

Hierachy [HC08]. Hierarchical [GS02b, HNZI02, HL02, MN01, YLH05, 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, CIIJ06, CGJ02, DS05b, FZH05, Gro01, HNZI02, HV04, Int00, JKR01, KMM06, Ken02b, KB00, Kra05, KT01, MM01b, NFO03, RW07, SKKS00, SOTD00, SM02, SGM09, SLG05, TL07, Uni00e, Wie00, WWGP00, YKMY01, Zhe01, BVP04, BZF05, BGL03, Jen09, KC09a, Uni00d, WWTH08, Zir07].

High-assurance [Jen09]. High-Bandwidth [CGJ02].

High-Dynamic-Range [CW09]. High-End [SKKS00, WWGP00]. High-Performance [Kra05, NFO03, BZF05]. High-Speed [Ano00d, Ano02d, Gro01, JKR01, KMM06, SOTD00, SM02, Wie00, YKMY01, RW07, BGL03].

High-technology-crime [KB00]. High-Throughput [HV04]. Higher [CV02, KCP01, BF01a]. Highly [CV02].

Hijacking [Ste05c]. Hill [Gum04, USE02a]. Hilton [KJR05]. HIPAA [AEV07].

Historic [Pet08]. Historical [RE02, MWW01]. History [BP03b, Ifr00, Pag03, Sal01a, Sin01b, CAC06, Top02, AJ08, Boo05, HSW09, Jan08b, KNS05, Na05, Nis03a, Pin06, Ris06, RH00, Wil01a, dLB07].

History-based [KNS05]. Hit [Bi05].

HMAC [FIP02a, DGH04, Hir09]. HMQV [Kra05]. Hoare [DH08].

Hoax [CBZ01, CTBA01]. hoc [SSS02, Cha05b, DHMR07, KH05, LHC08, LKZ04, PCSM07, SLP07, TW07, WT02, ZC09]. Hold [PM00].

Holier [MYC01]. Holistic [RM02].

Homage [JP02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03].

Homegrown [Str02]. Homeland [Man02, Man05, RR03b]. homogeneous [MF07, PS02a]. Homomorphic [AS01a, Aki09, CDN01, DN03, HS00, Cho06, Gen09a, Gen09b].

homomorphism [CKN06]. homophonic [Sav04].

Honeynets [Din07]. Hong B+02, ZJ04, Cl00b]. honor [OC03]. hook [JEZ04]. hooks [GJJ05].

hop [NC09, ZJ07]. hop-by-hop [ZJ07].

Horizon [Coc02b]. host [Shu06]. hostile [ABB04].

Hosts [H601, ZS08]. Hot [IEE01b].

Hotel [USE01b, USE01a, USE02a]. HotOS [IEE01b].

HotOS-VIII [IEE01b]. hours [Fox00].

House [Uni00a, Uni00d, Uni00f, Uni00e, Uni00h].

Hsu [BCW05, HL05b]. HTML [CNB02].

HTTP [Zha00]. Huang [ZC05]. Hug [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 [ZYR01]. HWWM [LKY05c].

HWWM-authenticated [LKY05c].

Hybrid [ADl09, KD04, LZ04, PK01, CJ03b, HG07, LPM05, TM06].

Hyderabad [MS02c].

Hype [Way02a].

Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic
Hyper-Encryption

Hyperelliptic

Ava03, CY02, CFA+06, HSS01, PWGP03,
Ver02, Was08a, ZLK02, CMKT05, Wen03,
Wol04, WPP05.

hypotheses [KW00].

I-tracings [RE02]. i.e [NP02a, Wil99]. IA

IA-64 [WWCW00]. IACBC

[Ava03, CY02, CFA+06, HSS01, PWGP03,
Ver02, Was08a, ZLK02, CMKT05, Wen03,
Wol04, WPP05].

hypotheses [KW00].
Implement [HQ05]. Implementation
[AD07, AG01, Ase02, Ash03, ARC+01, BBD+02, CCBP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EH03, FW09, FB01, FD01, GO01a, Gir06, HTS02, HHMN01, JKS02, KMM+06, KMS01, KTT07, KRS+02, KV01, LP02a, MKP09, MM01c, MN01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTT01, Pat01, PBTW07, QSR+02, RDJ+01, SM01, Sha01e, SK05a, SQRL03, USS02, Vir03, WZW05, W00, WOL01, XB01, Zaa00, B004, BRB+03b, C+02, CNPQ03, DKL+00a, GHDG00, GBKP01, HEE00, HP01, Hut01, KY09, LL04b, LCX08, LB05, Rhi03, SM03a, SVDF07, W004, YW06, ZFK04]. Implementations
[AL00b, BIP02, III00, CTLL01, CGBS01, EPP+07, GLG+02, MM01b, MP01a, RS01, WWCW00, ASK05, BFCZ08, BFG07, B008, FR08, RAL07, SQRL03]. Implemented [TSS+03]. Implementing
[Dw04, Kor09, LM08, LD04, MWS08, NDJ01, Pet03, Sm01a, SR06, C+02, CW02].

Implications
[Kun01, LJ05a, MF01, Bj005, Fri07]. Implies [KY01e]. Imply [Pic05].

Importance
[An00a, BKJ01]. Important [SM00a]. imposed [XLMS06].

Impossibilities
[CHL02]. Impossibility
[APV05, BPR+08, Fis01b, PQ06]. Impossible
[B00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SK01]. improve [Pau02a, CAC06]. Improve-ment
[CAC06]. Improved
[AF006, BPR05, BB05, BF00b, CL01b, CKK+02, CJ04, DN00a, DG02, Fan03, FKS+00, FKL+01b, FK+01a, GM08, Gen00b, HK09, HKA+05, JQYY01, Kin00, KT06, Kuh02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02e, PR08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].

Improvement
[AS01c, AJO08, Che04a, CZK05, CCW02, Di01, HWWM03, HW003, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Sha04b, Sha05b, WHLH03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK+04a, CL04c, CHY05a, Hsu05a, JSW05, JIliD05, X005, KJ05, LL04a, LW05c, S05, TO01, WLT05a, YW04, YWC05, YRY05a, ZC09].

Improvements
[BBM00, HW002, JL03, NP02b, YCYW07, CH07a, SQRL03]. Improving
[ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SK01, SB01, Sm02, XQ07, YEP+06, YGZ05].

Incentives
[Sw05]. Incident
[JBR05, Tom06]. Including [SR01].

Incomputable
[Ver06b]. inconsistencies
[MS09a]. Incorporating
[MSF+09]. incorrectness
[CHC04]. Increase
[PBTW07]. Increasing
[CS05c].

Incremental
[BKY02, LKL05].

IND-CCA
[Mu01b]. IND-CCA2
[BST02].

Independence
[BP03b]. Independent
[BS00a, BSL02, Kin02]. Index
[An000b, An01a]. indexing
[YPPK09].

India
[CV04, JM03, MM06, MS02c, RD01, Roy00a, RM04, Roy05, An03c]. Indies
[Fra01, Sys02, Wri03]. individual
[TW07].

INDOCRYPT
[CV04, JM03, MM06, MS02c, RD01, Roy00a]. Induced
[Vau02].

Industrial
[USE00b]. Industry
[ANS05, Mad00, Ort00]. ineffectiveness
[YLR05]. Infeasibility
[FS08]. Influence
[Mar02b, CDD+05]. Infinite
[TZT09a, TZT09b, Vau01]. Influencing
[Bl01c]. Inform
[Kwo03b, San05].

Information
[AP09, BW07, BIM00, BZ02, Big08, BB03, BJ02, Boy01, CGM07, DMO00a, ELV01, Hay06, HQ05, HW01, IS004, JD01, JG07, KP00, Kel02, KLB+02b, KO00, Lai03, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].
input-flow [FR08]. Information-Theoretic [VDKP05, vW01]. Information-Theoretically [DM00b]. Infrastructure [AHKM02, AL06, BC04b, BWE+00, CL07, ES00a, FL01b, KGL04, Sin01a, BHM03, BDS+09a, Ben01a, CZ05, FB01, Gor05, LCK04, MWS08, Ben02]. Infrastructures [HCDO02, Lin00b, PHM03, WBD01, Bra01a, LAPS08, SN07]. INIDP04 [LDM04]. initial [DK08]. Initiative [Coc01a, Cal00b]. initiatives [Mau05]. injection [MMJ05, ZSJN07]. Injectable [DKXY02]. Insulated [DKXY02]. Integer [CH07c, GMP01a, KKIM01, EKRA01]. Integrated [KW02, WH09]. Integrated [ECM00a, ECM00b, GMG00, Lut03, GLC+04, LK01, SSM+08, SN04]. Integrating [Wit01]. Integration [Ito00, CJL06, Sug03]. Integrity [An02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel [Coc02a, MP00]. Intellectual [Qu01, WY02]. Intelligence [Cop04b, AJ08]. Intelligent [Cos03]. Inter [WR02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WR02]. interaction [Gav08]. Interactions [Fau09]. Interactive [DG00, CHK05, DDO+01, Fis01b, Fis05, HNZI02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00]. 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, An00d, AAO+01, AJ01b, BDZ04, Bel00, B+02, BBD09, BS01b, Bli03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL00, Chr00, Chr01, CCMR02, CCMR05, CS09, CG05, Cra05a, DR02c, Des02, DUK05, DFP06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HY05b, IEE09a, IZ00, IKY05, JY04, Jef08, Jok03, JMO3, JQ04, Juc04, KGP02, KCR04, KR05, Kii01a, Kimm02, KN03, Knu02, KP01, KNP01, Lai03, LL03, Lee04b, LST+05, LL04c, MM06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pfi01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Sch01d, Sho05a, Sil01, SM07b, Syv02, TB02, TLC06, Un00a, VY01, Vau05a, WK03, Wil99, Won01, Wri03, Yun02a].
International [YDKM06, ZJ04, Zhe02b, ZH03, AMW07, AUW01, Ano00e, AJ01a, BCKK05, Bir07, BC05b, CKL05, DSY05, DWML05, DRS05, GKS05, HH04, HH05, HA00, Hon01, PC05a, PY05, PV05, Q500, Sma05, Son00, ST01d, WK06, Ytr06].

Internet [SMP09, ABB04, Ben01a, Ben02, Cal00a, Cha02a, Cha00a, Coc03, DP04, DGM03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MCN03, MA00a, Mir05, PM00, PLW07, PvS01, Pho01, PHL03, Rub01, SB05, SE01, SE02, Sto01, Tsa01, TWL05, Uri01, WC05, Wri05, ZG05, kc01].

Interoperability [Hil00, TEM01, BHM03]. interoperable [BFGT08].

Interpolation [LW02, YG01b, FWTC05, KT06].

Interpolations [Sat06]. Interpretation [Mas04, CC04c]. interpretation-based [CC04c]. Intersections [KS06a]. Interstate [RM02].

Intersecting [Jan00]. Intrinsic [ZWC02]. introduced [Ano00a].

Introducing [JL00]. Introduction [Ben02, Ber09b, Bis03a, BK06b, Buc00b, Buc01, Buc04, DK02, DK07, Fa07, Hay06, HK08, HC02, KL08, MAA07, Mol01, Neu04, PTP07, PM02, Pho03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGK08, TW02, TW05, TW06b, CS07a, CM05b, Gar01, HW08, Hro05, KP03, Mol07, RR03a, RP00, Sh05b, TW06a, Kat05b, Rot07, Lee03a].

Intrusion [CZ05, DFK03, DP07, JT05, TZZ05, TM05, WG05, HLL02, MAC03, NCR04, NN02, YbJF04, IR02].

Intrusion-Resilient [DFK03, DP07, IR02]. intrusion-tolerant [YbJF04]. intrusions [Be06]. invalid [CTJ04].

Invariant [Ben00, CT09, HH09, ZLZ07]. Invariants [WH09]. Invasion [ASW01]. invasions [Tyn05]. Invention [Ir00]. Inventors [Bar00c]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, FFMT05].

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, DR05]. involutional [SHH07]. IP [Ano00a, CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSEC [Vau02, CG05, Dav01a, KMM06, SW07, FS00, FS03a, XL06].

IPSec-Compliant [CG05]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06].

Irregular [MH04]. Irregularly [CG09]. Irreversibility [WZC02].

ISBN [An04, Duw03, Ego05, For04, Gum04, Im03, Pag03, Puz04, Top02].

Island [CSY09, KLO4, Kmo01, Lee04b, IE07].


Isomorphisms [CPP04]. Israel [Jol01].

ISSAC [Jef08]. issue [FOP06]. FOP06. Issues [BDF01, BH00a, Hil00, KRV01, Mea01, PB07, SE06, MK08, Pat02b].

ISW'97 [You01]. IT-Architectures [RM02]. Italy [AAC01, AL06, BCKK05, BC05b, CGP03, dCD05, IEE04].

Itanium [CHT02, Int00]. Itanium-based [CHT02]. Iterated [Jou04, On01].

Iteration [Che03]. IV [Sch01c, HSH01].

IWBR [LST05]. IWDW [BCK05, CKL05, KCR04, PK03].

J2EE [BTTF02]. Jack [Coc03]. James [Top02]. jamming [LPV09]. Jan [YRY05b].

January [Des02, GL05, IZ00, Vau05a, Wri03]. Japan [An00d, Mat02, Oka00, CSo02b, Sm01b].

Japanese [Y00]. Java [An04b, Mar05a].
WBL01, Ano02e, Ano03a, Ano04b, Ano04c, AJ01a, BCS02, Bis03a, BJvdB02, CMG+01, Che00, CMM05, Coo2, DPT+02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hum05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Virt03, Wei04, Win01, Zee00, ZFK04. Java-Based [EM03, DPT+02, GW08]. Java-Lösung [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]. JICC [HYZ05b]. Jim [Coc01a]. Job [MYC01]. jobs [Oue05]. Joel [Gum04]. Johannes [Lee03a]. John [And04, BZ02, NH03, Rot07, Coc03]. Joins [Bar00c, Con00]. Joint [ADI09, ADR02, CR03, HYZ05b]. Just [ABB+04, Ano06a, Gut02a, Car01]. Kahn [Gas01]. Kaikan [Ano00d]. Kaspersky [Ano08a]. KASUMI [KYHC01, KSHY01, SM02]. Katholieke [BBDD09]. Katz [Bar00a]. Keccak [BDPV09]. Keep [DM07b, Lys08, FS04]. Keeping [SEK01, SEK02]. KEM [NMO05]. Kerberos [BCJ+06, Coc01a, Gar03b, Hii00, Ito00, LLW08a, MJ01, MPPM09, Rub00, Smi01a, Vac05, WD01a, Wit01]. Kerckhoffs [KMZ03]. Kernel [Int00, Mor03, BK05, HB06]. Key [ANS05, ASW00, AK02a, Ano01j, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BPS08, BH06, BDG+01, BDZ04, Bar00a, BPS00, BPR00, BM00, BBDF01, BY03, BOHL+05, Ben02, LBM01, Bih00, BBB+02, BDK+09, BR00b, BM03b, BDTW01, BMN01, BM03c, BFP00, BCP01, BCP02a, BCP02b, BM01c, BST02, CK02a, CK02b, CHK03, CH05, CPP04, Che01a, CT08a, CHKO08, CCW02, CMM01, CKM00, CS02, CS03b, CS03c, DP04, DJ01, DPS05, Des00c, DBS01, Des02, DG03, DY09b, DKXY02, DFK+03, DGH+04, DBS+06, ESG+05, EP05, ES00a, FL06, FKS00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Gol03, GHW01, GC01b, GSB+04, Gut04b, HN02, HCD02, HLM03, Hoe01, HR05, HG03, HC08, HIJW01, HS07, HLC08, IEE00b, Ina02a, Ina02b, JL08, Jou02, JG01, Jue04, KGL04, KOY01, KY03, Kat05b]. Journey [LBA00]. Journal [LLLZ06a]. Journey [FF01b]. Jr [Kat05b]. Judiciary [Uni00b]. Julius [Cho02]. July [ACM01a, CZ05, Jef08, KJR05, May09, PPV96, Roy00b, Sch01c, S+03, Uni00a, Uni00b, Uni00e, Uni00d, ZJ04]. Jump [MP00]. June [ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BS03, BS01b, BCDH09, BC01, CZ05, FMA02, IEE05b, IK05, JYZ04, KGL04, KN03, KM07, PPV96, TB02, USE01b, USE01a, USE02c]. Just [ABB+04, Ano06a, Gut02a, Car01].
Cho06, CHH+09, CJL05, Cre00, DFM04, DMT07, DW09, EKRMA01, ED03, EHKH04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GMR05, GKM+00, GS01, GL06b, GMW01, HCD08a, HCD08b, HAU04, HHG06, HLLL03, HTJ08, HG05b, HWW03, HvdLM07, Hwa00, HLLL04, IZ00, Iwa08, IM06, Jan08b, JRR09, JW06, JXW05, KY00, KS05a, KYY09, KAM08, KG09, Kim01, KPY04, KRY05, Ko00, KV00, Kos01c, KHK05, LHL03a, LF03, LKK03a, LKK03b, LCP04, LL04a, LW04, LLL04, LL05a, LKY05b, LKY05c, LKY05d, LLY06, LL05b, LKY05b, LKY05c, LKY05d, LLY06, LLS+09, LCK04, LPM05, LHC08, LKL01, LSH00, L001c, LCC05, Lop06, MWS08, MKW00, MP08, Mis08, Ml0b, NP02a, PS00, PI04, Pei04, PR03a, PQ06, PC09, PSM08, PLJ05b, Pot06, Pri00, RH03, SN00, SLP07, SR01, SB04, Sh05c, Sh05b.

Key-Based [Sha01e]. Key-Dependent
[Gal03, BPS08]. Key-Exchange
[AB04, CK02a, KS05a]. Key-Insulated
[DKXY02]. Key-management
[CW05]. Key-Privacy
[BBDP01]. Key-Recycling
[PS05]. Key-Share [CT08a].
Key-Sharing [HNZI02, WBD01].
Keyboard [ZT05]. Keyczar [Law09b].
keyed [Küh08, SR00, FIP02a].
Keyed-Hash [FIP02a]. keying
[ABB+04, Che08a, EGK08]. Keyless [Qu01].
Keys [AOS02, APV05, AF06, BT02, BMK00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, Lu00, MN01, MRL+02, Omi01, PS00, Sm01c, Str02, TvdK+01, BCL05a, BCW05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH+08b, HSH+09, HW04, HY03, HL04, KAM08, LLW08b, LS01c, LWK05a, ML05, NN03, Sch01e, Sha04b, Sha05b, SB05, TLH05, TJC03, WHO3, YRS+09].
Keystream [AMR04, Kra02a, LV04, MH04, WL04, P01a]. Keystroke
[MR00, BGP02]. Keystrokes [SWT07].
Keyword [FIPR05]. KG [HLC08]. KG
[Z07]. KHAZAD [PQ03b]. KIAS
[May09]. Kid [CAC06]. Kikai [An004].
Kikai-Shinko-Kaikan [An004]. kill
[Lov]. Killing [Lov]. kind [DW01].
Kindi [MAa03, MAaTxx]. King [Eag05].
Kingdom [DFC00]. Kingston
[HA00, PT06]. Kit [An02e]. Klaus
[And04]. Kleptographic [YY01]. knapsack
[Kos01c, LCL05]. knapsacks [Mic02a].
Knife [Boy03]. Know
[CMB+05, Ros07, Con09, DKK07, Win05c].
Knowing [CH01a]. Knowledge
[Abe01, Abe04, AS01b, APV05, BP04, Con01, DPV04, DFS04, DDO+01, Eri02, Fis05, Gen04a, GK05, HNO+09, KS06b, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00, Ros06a, TG07, BCSV08, CLR09, Dam00, Hro09, IK05, JRR09, PBD07, KK07]. Knowledge-of-Exponent [BP04]. Known
[CMB+05, DNO2a, Fur02b, HSH01, Bao04, YTH04]. Known-IV [HSH+01].
Known-Plaintext
[DN02a, Fur02b, CKN06]. knows [Fox00].
Koblitz [AHRH08, Has01b]. Kolmogorov
[Sch01a]. Kommunikation [L02]. Kong
[B+02]. JZ04, Cla00b]. Konstantin [Puz04].
Korea [CS09, CTK05, KCR04, Kim01, Kim02, LL03, Lee04b, LL04e, Buy09, PC05a, PK03, Son00, Won01, WK06].
Korner
[Mor03]. Kościuszk [OC03]. Krawczyk
[Miy01]. Kryptoanalyse [Mor05]. Kuala
[DV05]. Kunming [Z03]. Kurosawa
[CHH+09]. Kurtz [Gum04]. Kyoto
[Oka00].
L [Sem00]. L-collision [Sem00].
Laboratory [Bru06, LBA00]. Lagrange [FWTC05], Laid [Wei06, Wei05]. Lam [Wag00]. Lamar [LMHCETR06]. lamp [McN03]. LAN [Bar03, Pan03, SZ08, Sty04]. Lanczos [BF06a], Landau [Jan08a]. Landscape [Ahm07]. Language [ARC+01, DD02, Gou09, Jen09, MW04, WAF00]. language-based [WAF00]. languages [Lun09, Rob02, Rob09]. Laos [Lov01]. Laptop [PGT07]. Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, GGO1, Kuh00, PG05, SM01, ST03b, USE00a, BPO3a, CKY05, CJO3b, Has00, HMvLM07, HY03, PS08a, SM03a, TM06, WL05].

Large-Scale
[CDR01, BH00a, BPO3a, HMvLM07, PS08a].

Larger [Car02]. LARPBS [CPbX04].

Lasers [Ilg02, UHA+09]. late [Sch05c]. latency [RSP05]. Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HPS01, HG07, IM06, Mic01, Reg03, Reg04].

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

lattice-reduction [HG07]. Lattices [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Shp05, SI01]. Launched [Bar00b, Ano00]. Launches [Ano02d]. lava [McN03]. Law [GN06, MNFG02, St05c, NM09]. Layer [LX0+05, LPV+09, SLP07, ZLO4c]. Layers [Gri01]. Laying [Lut03]. Lazy [CCM05].

LDAP [Bau03a, Bau03b, BH00b]. Lead [Tsa07]. Leak [RST01]. Leakage [CKN01, DP08, Kel02, RS01, ABHS09, CNK04, IY05].

Leakage-Resilient [DP08]. Learned [GSB+04]. Learning [KS06a, LY07, CAC06, BKW03, Mal06, Reg05, Reg09, SM08, Whi09]. Least [SZ01].

lecture [Rot02b, Rot03, Adl03, RSA03a, Riv03, Sha03b]. Lee [Sty04, Coc02b, KRY05, KCL03, KHKL05, LKY05d, SCS05b, ZK05].

Left [Dhe03, HKPR05]. left-to-right [HKPR05]. Legal [Coc02a]. Legislation [Eng00]. legislative [AvdH00]. legitimate [Lin01a].

Leighton [Rub00]. Length [AR01, BR00b, CKN00, CHJ+01b, MD03a, RK06].

Length-Preserving [MD03a]. Leonard [Coc03]. Less [YKMY01, BD00b]. Lessons [GBS+04, KFSS00]. Lest [HSH+08a, HSH+08b, HSH+09]. Lets [Pau02a]. Lett [Kwo03b]. Letters [ASW+01, BTTF02, MNT+00, TEM+01, TvdKB+01, WWL+02]. Leuven [BBD09, DR02c]. Level [EP05, MV00, TV03, BDN00, DHL06, KVR+09, SS03].

levels [CUS08, Voi05]. Leveraging [BRTM09]. LEVIATHAN [CL02c]. Levin [AC02]. LFSR [Jan00, JZCW05].

LFSR-Based [Jan00]. LHL [Pei04, YRY05]. LHL-key [Pei04, YRY05a]. Li [JW01, KCL03, SZS05, QCB05a, SCS05b, ZK05]. Liaw [TJ01b].

Liberty [Lan04b, Ano00]. librarian [PBV08]. Libraries [Fin02, MK05b].

Library [KSZ02, Lan05, Law09b]. Libre [Jen09]. license [Ano00]. Lies [Gan01b, Sch00d, Swao1, Ste05c]. Life [Cop04b, GSB+04]. lifecycle [HL06].

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

Like [Coc02a, PSC+02, VMS05, BCDM00, CWH00, DLP+09, Egh00, EBS01, Go09, HSL+02, HL04, SKE+00, SLE+00]. LILI [JJO2a]. LILI-128 [JJO2a]. Limitations [Gua05, Fis01a]. Limited [AK02a, LCD07, Buh06, Tse07]. limiting [CCK04]. Limits [CWR09]. Lin [CC02b, CH05a, KTC03, YY05a]. Line [Cho08a, DL98, Jan08a, Lai07, Lu02, SK06, YLL02, Bau05, BCS02, DL07, Luk01, Shi05].

Linear [BDK02a, BD02b, BDQ04]. CGFSHG09, CS05b, CHJ02, Cou01, CM03, Cou03, CDM00, CD01a, CDG+05, FM02a, FM02b, GS03, GBM02, HLL+01, Hug02, JJO0d, Kan01, KMT01, Kin02, KM01c,
Linearization [DDG+06]. Linearly [ADD09]. Lines [SP04]. Linguistic [CDR01]. link [LPV+09]. link-layer [LPV+09]. linkages [ZAX05]. linked [YWWS09]. Linking [GW00]. Linux [Lin02, ASW+01, Ano01i, Cla00b]. Login [Fox00, MT09]. Logic [BPST02, Cop04b, KBD03, KS06b, Lit01, Nie02d, SQ01, SC01, Tee06, TV03, BDNN02, BD04a, DZL01, WZB05, dH08]. Logic-Based [KBD03]. Logical [Kra07, SP03, Zha08]. Logics [IK03]. Login [LL05c, CCK04b, CJT01]. Logistic [KJ01]. Logo [LZ09]. London [Pag03, Top02]. Long [ABRW01, Dur01, GSW00, Gro03, PCG01, Zho06, BMV06, ISO05, SGMV09]. Long-Lived [GSW00]. Long-Term [ABRW01, Dur01, BMV06, ISO05, SGMV09]. Look [Bon07, Has00, Lut03, Sye00, Hen06b]. Look-up [Has00]. Looking [ASW+01, Ano01i, Cla00b]. looks [Nis03a]. Lookup [MFFT05]. loop [KV+09]. loop-level [KV+09]. Loopholes [Ste01]. Lorenz [GHdGSS00, Sal00a]. Lorenz-based [GHdGSS00]. Losing [Sta05]. LosLobos [Pri00]. Loss [LHS05, Mit00]. Lossy [AIP01, HSKC01, PW08]. Lost [PY06, Rob02, Rob09]. Lösung [Ano04b]. lot [Cla00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [QS00]. Low [Ano00d, BM01b, CH07c, GTO03, HGRO7, JPO2a, KMB09, RMH03b, RMH03a, SU07, SHJ04, SZ01, WC01a, CL09, CO09, Fan03, HLL03, LC04a, WLH05, WY05, ZYW07]. Low-computation [Fan03, LC04a]. low-cost [CL09]. Low-end [SU07]. Low-Exponent [SZ01]. Low-overhead [HGR07]. Low-Power [Ano00d, JPO2a, KMB09, CO09, ZYW07]. Low-State [GTO04]. Low-Weight [CH07c]. Lower [BD01b, BP03b, DRR05, GT00, GGK03, PS02a, Shp03, WW05, Shp09]. LSB [CS05c, FGD01, WMS08]. LSB-encoded [WMS08]. LSD [HS02a]. Lu [QCB05b]. Luby [MP03, Pat03a]. LUC [LNS02]. Luminy [PPV96]. Lumpur [DV05]. Lund [Joh03]. LUT [CC02a, TL07]. Luxembourg [Bir07]. Lyndon [GS01, VS01]. Lynn [Hes04a]. LZ [AL04]. LZ-77 [AL04].
measurement-based [FXAM04].
Measures [CB01, QS01]. Measuring [Siv06]. Mechanising [Be101]. Mechanism [LXM+05, WY02, 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 [Cla00a, HG07]. meet-in-the-middle [HG07]. meeting [Jef08]. Meets [Way02a]. Melbourne [IZ00]. Member [CTH08]. Membership [NBD01, Fis01a]. Memoir [Bar05]. Memorable [KOY01]. Memoria [DNRS03]. Memory [AK03, AJO08, CCM05, DK08, DGN03, HNZ02, HBDJL01, KJC+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05]. Memory-Bound [DGN03]. memory-safe [Oiw09]. Memoryless [Sar02]. MEMS [ECG+07]. MEMS-Assisted [ECG+07]. ment [CA06]. menu [Mea04]. Mercy [Flu02a, Cro01]. Merkle [CDMP05, JLSM03]. Mersenne [Ano03d]. Mesh [LPZ06, ZTP05, KB09, LZP+04, YPSZ01]. Meshes [BG08, Lav09]. Message [BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGMO0b, GTZ04, Jut01, OMO9, SNR04, WS03, Zol01, BPS08, CH05, Cj05, Gav08, HW05, MD04, Shao4b, TJC03, Wu01, ZF05, ZAX05]. Messages [Ara02, AR01, BR00b, CHJ+01b, DS05b, Sch09, Wri05, Zho06, Alv00, Ano08c, BCG+02, Bih02, BB79, Lm09, SP79]. messaging [Opp01, RR05]. meta [SM08, PLJ05a, QCB05b, Shao5d]. Meta-He [PLJ05a, QCB05b, Shao5d]. meta-learning [SM08]. metadata [CDS07, FJ04]. metamorphic [CSW05]. Metaphor [CNB+02]. Metering [BC04b]. Method [BDTW01, GHK+06, GL00, Gro01, HRS02, HQ05, JKK+01, Mol02, OKE02, OT03a, OT03b, SOHS01, TIGD01, TS00, WH09, WNY09, ZL05, AMRP04, DwWu04, Gut04c, JLV03, MSP09, MFK+06, Wg02, WWTH08, kWPW01, WlW04, YC09b, YCL07, CHJ+01a]. Methodologies [SPMLS02, ND04]. Methodology [VMS05, HM02a]. Methods [BCDM00, FD01, Kin00, Lm00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Bau00, Bau02a, Bau07, BGM04, BCHJ05, CM05b, GKS05, JZCW05, LMSV07, Mal06, SSST06, Shp99, YW06]. Metric [LBGZ01, LBGZ02]. Metrics [LZ01, NP07]. Mexico [Buc00a]. MGC'05 [ACM05a]. Miami [Des02]. Micali [Rub00]. Michael [Ter08]. Micro [ASK07, Eng00, Ste05c]. Micro-Architectural [ASK07]. microcontrollers [GBK01]. Microelectronics [IEE09a]. Microprocessor [Web08]. Microprocessors [LKM+05]. Microscopic [MYC01]. Microsoft [Bau00, Scr01, Ste05b, Weh00]. Middle [Eag05, Gen04a, HG07, Kin01]. Middleware [ACM05a, KRV01, LGS01, MBS04]. Migration [Pat02a]. Mikhailovsky [Puz04]. Milan [dCdVSG05]. military [Ark05]. Million [Ran55, Ran01, Ano03a]. MIME [Dav01b, Dav01c, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau06b]. Mine [For04]. Minimal [FBW01, FGMO01, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LPM05]. Mining [LP00, Lut03, HLL+02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [CC05e]. MinRank [Cou01]. Minutiae [UEP09]. Minutiae-based [UEP09]. Misbehaving [JQY01, SBB05]. Misinformation [CZB+01]. Missed [TvdKB+01]. MIST [Wal03]. Mistakes [Ste05b]. MISTY
LCZ05b, LW05c, NC09, PW05, SC05a, TWL05, TYH04, YCH04.
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-Property [ZS05]. Multiagent [ZS05].
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 [LLL04]. Multiagent-Based [ZS05]. multibit [TND+09].
Multicast [AIP01, BPS00, BDF01b, ASW00, GIKR01, GL06b, JA02, KB09, MP08, PCS03, YC08].
Multicollisions [Jou04]. Multi-level [LN04].
Multimedia [AAK09, FMS05, GA05, HL07, Sun05, WLLL09, DY09a, DKA05, Lf00, SG07, YC08].
Multimodal [PY08]. Multiparty [BG08, CDN01, DN03, DI05, GIKR02, OZL08, CDD00, HT04, IKOS07].
multipath [SK05b]. Multiple [AIK+01, Ara02, BDQ04, CL01a, CL01b, CHSS02, Che08b, DK05, Har00, HZSL05, HLT01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJO4, DM07a, HLH00, KC09a, MN14, Sha01d, SW05, TCC02, YW05, YH03, YRY05b].
multiple-key [Che04a, CJO4, SW05, YW05, YH03, YRY05b]. Multiple-Precision [HZSL05, MN14].
Multiple-watermarking [Che08b]. Multiples [HR00].
Multiplication [AHRH08, ADDS06, BK09, CMJP03, CH07c, Dhe03, GL01, HM02c, KKKM01, M02, NMSK01, OS01, Tan07a, Wal01, BINP03, DwWM05, FP00, GD05, Has00, Mis06]. Multiplications [Har06, OT03b]. Multiplcative [Has01a, KO03, MFFT05]. Multiplier [HKA+05].
Multipliers [CMJP03, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07]. multiprocessor [ISTE08].
Multi-purpose [Boy03]. Multireceiver [HSZ01]. Multiresolution [hKLS00, YPSZ01]. Multiset [aSM01].
Multisignature [Tad02, CWH00, CL04c, CCH04, He02, LC04b, LKW05b, YY05a, ZK04].
multisignatures [CL00, WH02b]. Multithreaded [Zha00]. Multivariable [DS05a].
Multivariate [DY09b, BGP09, FP09]. Municipal [MJF+08]. Music [MNS01, XMST07].
mutargima [MAaT05]. Mutation [Lut02].
Mutual [JP02a, KH05, CCS08, VK08].
Mutually [WC01a]. MYCRYPT [DV05].
mysterious [Bel07a]. Mystery [Rug04, GG05a]. Myths [GO03, kc01].

N [Mar05a, AOS02, KOMM01]. NAF [OT03b]. Names [Coc01a, Sha02, Ark05, CGV09].
Naming [Ano01b, BH00b]. Nanotechnology [RR03a, RR03b].
Naor [Zha06]. Napoleon [Urb01]. narrowing [MT07]. NASA [Ano02c, Wi99]. Nation [Lan04a].
National [BWE+00, Jo01, LCS09, AJ08, Bam02].
National-Scale [BWE+00]. Natural [ARC+01, Top02, WMS08]. Nature [Pag03].
Naval [LBA00, Goo00]. Nazi [Hau06, KS04]. NC [AIK04]. nCipher [Ano03e]. NCP [SQ01]. NCR [LBA00].
Near [BC04a, DPS05]. Near-Collisions
Necessary [LCK03, MN01]. Necessity [SBZ02]. Nederlanden [dL00]. Need [Coc01a, HR04b, Sty04]. Needs [CZB+01, DKK07]. Negotiation [DBS+06, HJJS04, IY05, LLW05, LLW09]. Nema [Kid00]. NESSIE [Pre01, Mac00, Pre02a, Pre02b, SGB01, DPVR00]. nested [LCK04]. Net [CAC03, Ano08b, LKJL01]. Nederland [Knu02]. Nets [AADK05]. Netspionage [BK00]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Kos07, VM03]. Networks [AEAO05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZD02, Sin01a, WT02, Zee00, ZYN08, WLY05, YLT06, ECM00a, ECM00b]. Network-Attached [RCBL00]. network-based [HLL+02].
noninterference [DFG00].
noninvertibility [HRS08]. Nonlinear [BP01a, BI05b, CV02, Che01c, LBGZ01, LBGZ02, SM00a, ZC00, BPGGS05, 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, HW05, OZL08].
Numbers [HSR +01, HBF09, Ifr00, MN01, ST03b, AG09, HW98, KB39, Kir01b, MFK +06, SS03, Shp05, Tip27]. numeric [AKSX04]. Numerical [WWL +02]. numerically [Sav04]. Numerous [CC08]. NURBS [Ben00].

Number-Notation [Eag05, Kin01]. Number-theoretic [NR04]. Numbers [HSR +01, HBF09, Ifr00, MN01, ST03b, AG09, HW98, KB39, Kir01b, MFK +06, SS03, Shp05, Tip27]. numeric [AKSX04]. Numerical [WWL +02]. numerically [Sav04]. Numerous [CC08]. NURBS [Ben00].

NPRCryptBench [YLTO6]. NSA [RC05]. NSS [GJSS01, HP01]. NT [Str01b, USE00a]. NT/2000 [USE00a].
NTRU [GJSS01, GS02c, HP01, HGHP +03, HGNP +03, HG07, JJ00b, NP02b]. NP-hardness [AGGM06, AGGM10].
NPCryptBench [YLTO6]. NSA [RC05]. NSS [GJSS01, HP01]. NT [Str01b, USE00a]. NT/2000 [USE00a].
NTRU [GJSS01, GS02c, HP01, HGHP +03, HGNP +03, HG07, JJ00b, NP02b]. NP-hardness [AGGM06, AGGM10].
NTRUSign [HHG06, KY09].
NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Die03, DG07a, DGP07b, DV08, Eag05, EHK+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kef05, Ket06, KM01b, LMHCETR06, LNS02, MN01, NR04, RSN +01, SP05, Sch06b, Shp99, Shp03, SFDF06, TWNA08, TL07, T7Z09a, T7Z09b, Vav03, Wal00, Yan00, YKLM02b, Aam03, AUW01, BK07, Bel08, BPGGS05, BG08, BG09, BG07a, BGL +03, CNPQ03, CO09, DIM08, DG09, FP00, HG05a, HGNS03, HLwWZ09, HP01, JAW +00, JLO3, KH08, KS00, Kin01, Lam01, Mit00, Nie02a, Nic04, Pan07, PSS +09, PSSP +08, PC00, RGX06, Sho05b, Shp05, Sim02, Ste08, SR07, SK01b, T005, Wag03, Was08b, YZEE09].
Number-Notation [Eag05, Kin01]. Number-theoretic [NR04]. Numbers [HSR +01, HBF09, Ifr00, MN01, ST03b, AG09, HW98, KB39, Kir01b, MFK +06, SS03, Shp05, Tip27]. numeric [AKSX04]. Numerical [WWL +02]. numerically [Sav04]. Numerous [CC08]. NURBS [Ben00].

Notes [KSF00]. Nothing [Des00c, SR00]. Novice [Dew08, Gou09]. Novo [Bi09]. November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].

November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].

November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
November [ACM01b, ACMO05a, BZ02, CKL05, Eke02, EIE00a, IEIE02, LA03, LL04c, MS05b, PK03].
On-Demand [SEF+06]. On-Line [Lu02, BCS02, Luk01].

One [AK02a, BYJK08, CHL02, Che03, DIS02, Di01, DW01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, KI01a, KO03, KO00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00c, Uni00h, YZ02, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, Di03, DS02, GKK+07, HR07, HRS08, JZ09, KO07, KKKP05, KO03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, YW05, YRY05b, ZW05a].

One-Time [HM02b, LDM04, RR02, CCK04b, DS02, LC04a].

One-variable [SV08a].

One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sho00a, YZ02, AK02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, GKK+07, HR07, HRS08, JZ09, KO07, KKKP05, KO03, LW04, LPM05, LQ08, Mic02a, Poi00, SVDF07, SW05, YW05, YRY05b, ZW05a].

One-Wayness [KI01a, PV06b].

Online/Offline [ST01b].

Ontario [HA00, ST01d, VY01].

Oracle [ABR01, Abe01, Abe04, BF05, Chi08, Gra02b, Nie02b, Pas03, Ano02c].

Oracles [BNPS02, BB04, KG09, RG09].

Order [AKX04, Bai01a, CV02, KCP01, KCJ01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Coh03, JZCW05, KSS06b, PQV05].

Order-Specified [Tad02].

organizing [KWP06, OKS06].

options [Fri07, Pot03].

Oracle [ABR01, Abe01, Abe04, BF05, Chi08, Gra02b, Nie02b, Pas03, Ano02c].

Origin [MABI06, MD04].

Organizational [PTP07, BJ02].

[DJ06, WV01].

OS [PS01c].

On-Demand [SEF+06].

On-Line [Lu02, BCS02, Luk01].

One [AK02a, BYJK08, CHL02, Che03, DIS02, Di01, DW01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, KI01a, KO03, KO00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00c, Uni00h, YZ02, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, Di03, DS02, GKK+07, HR07, HRS08, JZ09, KO07, KKKP05, KO03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, YW05, YRY05b, ZW05a].

One-Time [HM02b, LDM04, RR02, CCK04b, DS02, LC04a].

one-variable [SV08a].

One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sho00a, YZ02, AK02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, GKK+07, HR07, HRS08, JZ09, KO07, KKKP05, KO03, LW04, LPM05, LQ08, Mic02a, Poi00, YW05, YRY05b, ZW05a].

One-Wayness [KI01a, PV06b].

Ongoing [Sam09].

Onion [CL05].

Online [BDF+01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAY09, Voi05, FNR05, Fox00, Pan07, Tyn05, PT08].

One-Time [ST01b].

Only [BBK03a, CF01b, GL01, Hoe01, VY07, BC3DM00, FKS+00, GHJV00, Jia08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Yas08].

Ontario [HA00, ST01d, VY01].

OOSCD [CZB+01].

Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Kiis02, Lin02, Mea01, PM00, VDKP05, Ano03c, ETMP05, McA08, Bar00b, Lin02].

Open-Ended [Kiis02].

Open-Source [Joh05].

Open-Source [Bol02, Gut00, McA08].

OpenCard [HF00].

Opening [CAC03].

OpenSSH [Bau01c, Sta02b, TVdB+01, Hos06a, Mss06].

OpenSSL [Fri01, Res01a, Res01b, Sti06a, VMC02, YRS+09, Bel08].

Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL+08a, CGL+08b, CGL+08c, DGP09, KWDB06, MPHD06, SET08, TKP+08].

Operation [BR02, BKM07, Dwo03, EP02, Gol01d, HSH+01, JKR01, KY01a, Bdu00b, RBB03, Win00].

Operation-Centered [BKM07].

Operational [WA07, GMG00].

Operations [BIP05, IM01, KDO01, KS05b, LS01b, Ark05, Dug04].

operators [Bau01a, BDDS03, CH+01b, CDF01, CF02, DPS05, DNP07, GMW05, IR01, KOO4, KS03, LZ09, Man01, MPSW05, MP08, SNR04, YY01, vDW04, BCD06, HSK05, LSH03a, LSH03b].

optimality [NK06].

Optimised [TL07].

Optimistic [CC00, DLY08].

Optimization [Ken02a, Kre05, KV01, SMM01, TLY04, WPP05].

optimized [LC03].

optimizing [Dwi04].

Optimum [KWP06, OKS06].

options [Fri07, Pot03].

Oracle [ABR01, Abe01, Abe04, BF05, Chi08, Gra02b, Nie02b, Pas03, Ano02c].

Orders [AKS04, Bai01a, CV02, KCP01, KCJ01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Coh03, JZCW05, KSS06b, PQV05].

Order-Specified [Tad02].

ordered [HY03, WL05].

Ordering [Mea04].

Orders [HJW01, PS02b, HM00, Huh00].

Ore [CHH01].

Oregon [ACM00, BCDH09].

Organization [JG07, MP00, C+02].

Organizational [PTP07, BJ02].

organized [AUV01].

Oriented [HR00, LSL+01, SKU+00, ZCC01, CHC05, CWJT01, DHL06, HW04, LL06, LWZH05, MWM01, Sae02, Sha03c, TJ01a, WHHT08].

Origin [MABI06, MD04].

Original [JQY01].

Originators [Cop04a].

Origins [Cop04a].

Orleans [USE00c].

Orsay [DPT+02].

OS- [CRSP09].

oscillator
oscillator-based 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]. PA-RISC [Cor00a, WWCW00]. Package [Win01]. Packed [FH07]. Packet [BR09, WRW02, WLZZ05, CMS08]. Pad [LD04, DSO2]. Padding [AR01, BCCN01, CJNP02, KO03, LS01a, Man01, Vau02]. Padding [NP02b].

PadLock [Lud05]. PadLock-wicked [Lud05]. Page [IEE00b]. PageRank [GPC08]. pages [Fal07, Rot07], paging [SZ08]. Paillier [CGHG01, DJJ01, NSN05, ST02]. Pair [WCJ09].

Pairing [BKLS02, BF01b, BF03, CHSS02, GPS06, HCD08a, HCD08b, Kir03, PV06a, SKG09, Sna03a, GPS05, Lee04a, PC05b, VAVY09].

Pairing-Based [BKLS02, GPS06, PV06a, HCD08a, HCD08b, GPS05]. Pairings [Bon07, BGH07, Jout02, SB04, ZK02, CJL05, LWZH05, LC05b, SW05, VK08]. pairs [LYGL07, Shp01]. Pairwise [CLL00, FM02a, HMvdLM07]. PAKE [HTJ08]. Palm [BDhKB09, WPS01, Wil99, Ano02d].

Palmprint [KZ09]. PAM [FR02, Sei00b]. Panama [BDPV09]. Panel [FL01b].

Panopticon [YN01]. Paper [CC09, MFS+09, Pet08]. Papers [Ano04a, Ano07b, Ano07a, Sch00b, Ytr06, Wil99, Bla03, Chr01, CCM02, CCM05, CSY09, CGP03, DR02c, GH05, Jo03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PK03, PT06, RM04, S010, AMW07, AJ01a, Bir07, BC05b, CZ05, CKL05, DR05, HH04, HH05, PC05a, PY05, WK06, Wri03]. Paradigm [BN00a, CS02, G03, KD04, YC01, BKN04, Can01a].

Paradigms [Des00b, Swa01, Hro05]. Paradise [USE00b]. Paradox [Che01b]. Parallel [AHRH08, App07, AEMR09, CB04, CNTL01, CNPQ03, CNB+02, D07, D06b, JL08, KY02c, Lin01b, MFS+09, PS04a, RMH03b, S01a, BF06a, FP00, OS07, RMPJ08]. parallelism [KVN+09]. Parallelizable [BR02, M02]. parallelizing [Fri01a]. Parallizable [LKK03a, LKK03b]. parameter [Wue09]. Parameterizable [KPMF02].

parameterization [LZP+04]. Parameters [ZL02]. Parametric [Vir03]. Paranoid [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gu05, Oue05, Ste05a, Luc06].

Parascript [Ano02d]. Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a].

Paris [ACM04a, GH05, KN01, NP02a]. Parity [DRL09, KKG03, You01, BKW03].

Parity-Based [KKG03, DRL09]. Park [Cop05, Cop06, HS01a, Sal00b, Sal05a, SE01, Smi01b, Wei06, Win00]. Part [Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05]. Partial [BM03b, Cor02, Her06, ABH09, CP07].

Partial-Domain [Cor02]. Partially [AO00, MSP09, Bao04, Fan03, HC04a, HY03, H03, W05, WLHH05, WM05, 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, FGMO01, FWW04, GCKL08, HM01b, JW01, LLL04, LLS+09, LSH00, YC09a, ZLX99]. Pass [SK00, MT02]. passe [Car00]. Passes [Coc03]. Passing [Vir03]. Passive [Sha01c, VV07, RW07]. Passive-Only [VV07]. Password [BMN01, BMP00, CHVV03, CPP04, CS07b, DG03, GL03, GMR05, Har01a, Har01b, Jabb01, KOY01, LSH03a, LSH03b, MPS00, Mac01, MSJ02, Ngu05, SBW01, WHL05, YS04, ZWCY02, CC01, CC04b, CCK04b, CYH05, Fur05, GL06a, HTJ08, JM07, KLY03, KJY05, KTC03, KCL03, Ku04, KCC05, KHKL05, LFV04, LC04a, Sco04, Shi05, YW04, YWC05, YS02, YPKL08, ZDW06]. Password-Authenticated [BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, SBW01, WHL05, YS04, ZWCY02, CC01, CC04b, CCK04b, CYH05, Fur05, GL06a, HTJ08, JM07, KLY03, KJY05, KTC03, KCL03, Ku04, KCC05, KHKL05, LFV04, LC04a, Sco04, Shi05, YW04, YWC05, YS02, YPKL08, ZDW06]. Password-Based [CPP04, CS07b, GL03, GMR05, Har01a, Har01b, Jabb01, KOY01, LSH03a, LSH03b, MPS00, Mac01, MSJ02, Ngu05, SBW01, WHL05, YS04, ZWCY02, CC01, CC04b, CCK04b, CYH05, Fur05, GL06a, HTJ08, JM07, KLY03, KJY05, KTC03, KCL03, Ku04, KCC05, KHKL05, LFV04, LC04a, Sco04, Shi05, YW04, YWC05, YS02, YPKL08, ZDW06]. Password-guessing [Shi05]. Passwords [GL01, KOY01, Per03, Smi01c, Ano03b, FZ06, KOY01, NS05a, RD09, vOT08]. Patarin [Bih00]. Patent [MP00]. Path [GXT+08, CCD+04, Dev08, ZSN05]. path-based [CCD+04]. Path-quality [GXT+08]. Pattern [ABM08, BDhKB09, BLP06, BCCN01, LS01a, TIGD01, Buh06, LYGL07]. Pattern-based [BLP06]. Patterns [DD02, MP06, WCJ09]. 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, MPH06, PI06, WCJ05, Yi04]. Peer-to-Peer [HR02, RH02, ATS04, MPH06, PI06, WCJ05]. PeerAccess [WZB05]. Peinado [YRY05a]. PEM [Dav01b]. average-case [Mic02c]. cellular [SSM+08]. cipher [HAuR04]. Correction [SKQ01]. CPN [AADK05]. CRC [Kat05b, Was08a]. Data [BSB00b]. Deblur [VHP01]. decryption [OS07]. Decryptor [TPS01]. Division [KKY02]. evolution [Pat02a]. Hardware [Nd05]. HMAC [RR08]. IEC [ISO04]. image [Sch00a, Sch01c, Sch04a, Sch04b, Sch05a]. Memory [BS00b]. MOM [DJLT01]. multisignature [Wu01]. Offline [ST01b]. response [LV05a]. 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, Guo05, Oue05, Ste05a]. Pennsylvania [IEE05a, IEE08]. People [ASW+01, CG05, Lov01]. Perceptual [BPM+07]. Perceptually [EFY+05]. Perfect [AJ008, CLE509, DN02b, DSS01, Sun00a, DM07a, SC02c, ZD05]. Perfectly [DMS00, KR02, SNR04]. Perform [Kin00]. Performance [ACM01b, BH00a, DOR01, Dra00, EYP00, FZH05, Int00, Ken02a, Ken02b, Kra05, LWK00, MM01b, NFQ03, PWGP03, PBTW07, SKKS00, SW00a, SB01, Siv06, SL00, SGPH98, WBRF00, WWCW00, WS02, XH03, YEP+06, Zaa00, AKNRT04, BVP+04, BZP05, KCL+09, CRSP09, GCO0a, HMO2a, JRB+06, LW05a, NTW07, YZ05]. performance-friendly [CRSP09]. periodic [XQ07]. Periods [KKH03]. Perl [Sal03b]. Permutation [DMS00, HSR+01, IYK02, KKG03, KO03, LSY01, DP02, IYK03]. Permutations [BPR+08, CHL02, KO00]
Persistent [AGT01, ST06]. Person [KJR05, LLT+04, PK01, BS01b, KN03, Li05, LST+05, PY08]. Personal [Bar05, EHMS00, SEK01, SEK02, Tu05, UP05]. personalized [GPC08]. Perspective [LL01]. Perspectives [BMV06, SM08]. Perturbation [BDhKB09, JW05, LKHL09, Lut03, Lut03]. PET [MS05a]. Peter [For04, Uzu04]. Petersburg [GKS05]. petitions [Cal00b]. Petri [LKJL01, AADK05]. PGP [McL06, Ano00h, BCH+00, Dav01b, Dav01c, JKS02, Luc06, Opp01]. PGV [BRS02]. pharaohs [Pin06]. Phase [CDF01, Ig02, KLB+02a, Che07, Che08a]. Phase-Conjugate [Ig02]. phase-shift [Che08a]. Phil [Bar00a]. Philadelphia [IEE09a]. Philosophy [Cop04b]. phasing [Bel04]. Phone [CAC03, Fox00]. Photonic [TWNA08]. Photonic-based [TWNA08]. Photons [Bar00c]. Physical [CGMM02, LR07, YKL02a, GVC+08, UHA+09]. Physicist [BZ02]. physicists [RP00]. Physics [MYC01, Sch06b, BEZ00, BEZ01, Duw03]. Pi [OS08]. PIC [Fin02], pick [Cla00b]. Picks [PM00]. PicoDBMS [PBVB01]. Picturing [Pau03]. Piecewise [LLL+01]. Pigeon [Pem01b]. piling [Kuk01]. piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03]. PIPE [CBD+05]. Pipelined [MD05, Mis06]. PIR [BIM00]. Pirates [KY01d]. PISN [ECM00a, ECM00b]. Pittsburgh [IEE05a]. Pixel [LS08, WCJ09, BCD06, LYGL07, WWTH08]. pixel-pairs [LYGL07]. Pixel-Value [LS08, WWTH08]. PKC [BDZ04, Des02, Kim01, NP02a, Vau05a, IZ00, Kl01a, Kl01b, ZC04]. PKC’98 [HPC02]. PKCS [Ch03, Man01, RSA00c, RSA00b, RSA00d, RSA00e, RSA01, RSA02, RSA03b]. PKCS#1 [CJNP00]. PKCS#11 [DKS08]. PKCS#7 [Dav01b]. PKI [AL06, CZ05, KGL04, Ahm08, ES00b, ES00a, Gar03a, Gut02a, Hoo05, NDJB01, Ort00, St.00]. PKIX [FL01b]. PKP [JJ01]. PKWare [Bar00a]. Place [USE01b, USE01a, GS07b, IEE09a]. placement [GGJ05, JEZ04]. Plain [Col03]. Plaintext [DN02a, Furt02b, GK05, HLM03, Jo01, Ke02, KM01c, Kl01a, MF01, CKN06]. Plaintexts [BR00a]. Plan [CAC06, CGP+02, Gau08]. plan [WL02]. Planning [WCZ05]. plans [Ark05]. Platform [Bau02b, MMH02, PJDH09, ARJ08, ISTE08]. Platforms [AIK+01]. Play [WD01a]. Playing [Shp05, BR04]. Please [Per03]. Pluggable [Sei00b]. plus [Cop04b]. PODS [ACM03c, ACM05b]. poetry [MAaT06]. pogromca [Kap05]. Point [GLV01, M601, NS05c, USE00b, WW06]. point-sampled [WW06]. Points [BGJ08, Gau02, Cla00b]. poised [CH00]. Poisoning [Kle07]. Poland [AUW01, Bih03]. Polarization [HR05]. Poles [KS04]. Policies [AEV+07, ZP05, BNP08, LJY04, RN00a, RN00b]. Policy [Bla01c, HQ05, Ano00e, BFG08, BZP05, DFM04, Gor05, RVS09, Uni00b, RR04]. policy-based [BFG08]. policy-compliant [RVS09]. Polish [Kap05]. Politics [Cho08a, DL98, Jan08a, DL07]. polyalphabetic [GPG06]. Polygonal [Ben00, BB00a, BGI08, SP04]. polymorphic [CSW05]. Polynomial [AF03, BIP05, BG+01, Bul09, CU01, CJO3a, CH07c, CLZ02, DSM0a, Gon06, HR00, KJO05, KYS1c, KTT07, LW02, May04, P101, RMH03b, Sat06, LFW04, MRST06, SZP02]. Polynomial-Time [CLZ02, KJO5, Pli01, MRST06]. Polynomials [BLST01, DS08, FL06, Jam00, JJ00d, Lan04a, CHH01, FP09, GS09]. Pon [QCB05b]. Pool [BTTF02]. Popular
Knu07, LP00, Pap05, PBD05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YWD08, Be04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZYL05, ZSM05, MS05a, Jan08a].

Privacy-Enabled [Por06].
privacy-enhanced [ZSM05].
Privacy-Enhancing [SE09].
Privacy-Preserving [DN04, KS05b, YWD08, BA06, HJW05, Pin02, Pin03].

Private [AF04a, AFI06, BDFP02, BIM00, BY03, BSW09, BILS02, BGW05, ISW03, KO00, OS05, SDMN06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PLJO5b, Sun02, YRS*09, ZY08, ECM00a, ECM00b].

Private-Key [BY03, KY00, PLJ05b, Sun02].

prize [Fox00, Coc02b, MNT*00].

PRNG [HSS04, Mur02, SF07].

Proactive [DBS01, FMY01, JS05, ZSV05].
Probabilistic
[CCW02, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLM05, Go99, JZC05, KY00, MRST06, PBMB01, dH08, Neu04].

Probability [KMT01, MNT*00, DLP*09].

Probing [ISW03].
Problem
[AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK*02, Con01, CLZ02, DIS02, DHR00, FL06, Gen03, GV05, GPP08, KK02, LNS02, NBD01, Wag02, BKW03, CGHG06, CJT04, DLM05, HGNS03, Hsu05a, LHY05, LD01, Luk01, Pei09, Shp05, SCL05, WL02, Whi09, Yas08, Km04a]. problem-solving

[Whi09]. Problems
[BI05a, Can06b, MV03a, OP01a, TvdKB*01, VDKP05, HL05d, KX00, LM05, LMC*03, RSS04].

Procedure [LY07]. Procedures

[DJ06, BBK*03b]. Procedings

[AC00, ACM02, ACM04a, ACM05a, AAC*01, Bon03, EBC*00, FMA02, FLA*03, 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, B001, HA00, Hon01, IEE00a, IEE01a, IZ00, Kil01a, MS05b, Oka00, PPV06, PF01, Pre00, Q00, R001, Roy00a, SMP*09, ST01d, VY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BDZ04, BS01b, Bh03, BCDH09, BD08, CC04a, CV04, Chr00, Des02, DFPS06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE04, IEE05b, IEE07, IEE08, IEE09b, JY04, Jd08, JM03, Joy03b, JQ04, KJ05, KGL04, Kim01, Kim02, KN03, Kn02, KP01, KN01, KM07, Lai03, Lee04b, LLT*04, MMV06, MJ04, May09, MS02c].

Proceedings [Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sma05, Syv02, TBJ02, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZY03, BCKK05, Cra05a, DV05, DWML05, DKU05, GKS05, IK05, Kit05, L05, LST*05, Men07, P006, Sh05a, S00, dCdV05].

Process
[Kwo03b, MNT*00, BDFP02, HL06, MRST06, VKS09]. Processes

[BDP02, ALV02, BDNN02, Whi09].

Processing [ISSZ08, KLB*02b, PCK02, AA08, AA04a, YPSZ01]. Processor

[Ano02e, BBGM08, EP05, FBWC02, FZ05, GC01b, Int00, KBD03, KPMF02, TY02, ST03a, SHL07].

Processors

[TLY04, CW02, CRSP09, Geb04, LJ05a, YGZ05, YLT06, ZYL05].

Procurement

[Lad06]. produce [Zir07]. producing

[SO107]. product [KSW00, Sun02].

Products

[ACS02, Ano02d, Ano02e, Knu07, An00c].

professional [Dew08, vT00]. proficiency

[Dew08]. Profile

[PH01, RSA00c]. Profiles

[MG01, PJK01]. Program

[Hö01, Bec02, GGH*08, K003, KH03, CS08b].

Programmable

[Dan07, GC01a, HV04, Sm02].

Programmer
Programmers [Coc01a, Wei04, Gou09].
Programming [ASW01, Ano02d, Coc03, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03].
Programs [BGI01, Ark05, SLTB06].
Progress [KK06, KFSS00, RD01, Roy00a, CV04, HMHC06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03].
Projects [Fri01, IY00, MNT00, Pau02a, Salxx, Gou09, LR01, Lov01, MWM01, Sha01a, Coc01a, Coc02b, IY00, Pre02b].
Proposals [Gha07].
Prolog [Bla01a, Bla01b].
Promise [Ano02f].
promises [Pau02a].
promote [WK05].
Promotes [Bar00b].
Prone [MLC01].
Proof [Abe01, Abe04, AS01b, ARC01, BDP02, Cor02, Gk05, SOIG07, SPML02, Tee06, BR05, GMI04, HSD05, LMW05, PBD07].
proof-of-compliance [LMW05].
Proof-of-Concept [ARC01].
Proofs [BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie03b, BGB09, BR04, Goli99, HG05b, SV08b, DHO8].
Propagation [LJL05, QPV05].
Properties [ABC05, BM01c, KY01b, LLL01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].
Property [LPZ06, Qu01, Uni00b, WY02, BR06, JRS09].
Proposal [DPVR00, Mac00].
Proposed [Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06].
Protect [ETZ00, BBN09, WK05].
protected [CYH05, PKH05, ZCL05].
Protecting [Des00c, EHSM00, KY01d, Kra01, LKM05, LW05b, ML05, NN03a, Sha01c, vW01, Bro05b, LLY04, LS05b, ZLY05].
Protection [CGJ02, DKF05, ECG07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL08a, CGL08b, CGL08c, Gor05, Kovo3, KH03, Kwoo3a, LL05b].
Protections [JT01a].
Protocol [An001a, Bel01, BPST02, BL02, CK02a, CJ03c, CW05, Cim02, ECM00b, Fre03, GJKR03, GL00, HS07, JP02b, JRFH01, JT05, KLN06, Kak06, Kra05, Ku02, LCK01, Mea01, MU05, NS01b, Rub00, RMC01, SK00, Tan07b, TST09a, TZT09b, WHT05, YSR01, BP03a, Bla01b, BDFP05, BK05, CS04, CCK04a, CC04b, CYY05, CC05c, CH05, Che04a, CJC08, CJ03b, CJ04, CJL05, DFO4, GM04, GTZ04, HT08, HWMM03, HHC05, KH08, KKL09, KTC03, LC03, LF03, LKY03a, LKY03b, LW04, LH04, LKY05b, LKY05c, LHC08, LSH03a, LC05b, Lvk01, MS03a, Par04, Pau01, Shi05, SW05, SIR06, TM06, Tse06, Tse07, WK05, WLT05a, WHHT08, YW05, YTW05, YC09a, YS02, YSH03, YRY05, YRY05c, YPKL08, ZWLU01, ZL04c, ZDW06, ZYW07, LSH03].
Protocols [AADD05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Bor01, BMN01, BM03c, Bra01b, BLTD09, CKPS01, CT08a, CCM02, CCMR05, CIR01, CNV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GV01, Gor02a, JP07, JW05, KS00a, KY03, KL08, Kra03, Kusi02, MS02a, MP01, PB00, PR08, PJDH09, Rot01, Shy02, SC01, Tee06, AA04b, AKNRT04, Bar06a, Bau05, Bel07b, BDSV08, BFGT08, BP05, BLP06, BD04a, BR05, Can01a, Can06a, CP07, CRKT08, CJ01a, CH07a, Chuo8b, Chr00, Chr01, CJM00, Coh03, CC05d, CDL06, DFG00, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV09, LLL04, LLY06, LLS09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SL05a, SR00, SW00b, YS04, ZLX99, ZL04b, PDMS09, Puc03].
ProtoMon [JT05].
Provability [GOR02].
Provable [HM02b, HLL01, HSL02, KSH01, PB05, SLL00, BGP09].
Provably [AO00, AC00, BMP00, BCP01, BCP04, CHKO08, DG03, HlvA02, HvAL09, Hl07, HS07, JMY02, MJ03a, NSSK05, NSS02, VMSV05, XS03, ZCL05, BKN04, CCM02].
Provenance [HSW09].
Provers [MV03a].
Provide [AB01, Sch01a]. Providence [IEE07, Sil01]. Provider [LDM04, HILM02]. providers [MV03b]. Provides [OT03b]. Providing [BACS02, BDS+09a, DeL07, Lin07, Pan04]. Proving [Che03, FS01c, GN01, Tee06]. Proxy [Kha05]. proxy-enabled [DY09a]. proxy-protected [PKH05, ZCL05]. psBGP [vOWK07]. Pseudo [BH05, FWW04, Gen00b, LLL+01, LHL*+08, MP03, SXY01, TST09a, TST09b, WP03, BGO9, GB09, MFK*06, NR04, PSP*08, RXG06, SL09, WW08, YZEE09]. Pseudo-Random [LLL+01, MP03, WP03, Gen00b, SXY01, MFK*06, NR04, RGX06, SL09, WW08]. Pseudo-Ransom [BH05]. Pseudo-signatures [FWW04]. pseudonoise [HG05a]. pseudonym [CG06]. pseudoprimes [ZT03]. Pseudorandom [CDI05, DNO2a, DI05, DP02, Finn06, Fh02b, FIPR05, GMO2a, IYK02, LMH01, Nie02c, Aam03, BPGPS05, IYK03, KSF00]. Pseudorandomness [GM02c, IK00, IK01, KYHC01, LLH01, Lee03b, MV00, Shp03, Go099]. Psychology [MYC01]. PUB [Nat00]. Public [ANS05, AUW01, APV05, Ano01j, AEAQ05, AF03, BCO5a, BDG*01, BDZ04, Bar00c, BPS00, BBM00, BBPD01, BLM01, Bli00, BDTW01, BST02, CHK03, CHK05, CDM*05, CHM*02, CHKO08, CCW02, CT09, CCM01, CS02, CS03b, DV04, DJ01, Des02, DY09b, DKXY02, DFK*03, ESG*05, ES00a, ED03, FL06, FL01b, GMS02, GH01v, GC01b, GSB*04, Gut04b, HCD002, HR05, HG05b, HR04b, HJW01, HLC08, IEE00b, IZ00, Jou02, Kat05b, KKM01, KM01a, Kim01, KLY02, KKY02, KY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Mu03a, Mol03b, Mi01a, NP02a, NBD01, NSS02, OTU00, PHK*01, Pei09, PR01, Poi02, PNM03, Qu01, RSA00a, RKS+02, ST01a, ST02, Sin01a, Sm01c, Ste01, TS000, TT01, Vau05a, WZW05, WH01]. Public [WV00, Wya02, YKMY01, YG01c, YDKM06, Zhe02a, AG09, BHM03, CL05a, BC05, BBO+09, Ben01a, BB79, Bra01a, BD04b, Cal00b, CCT08, CL02b, CWH00, CCH05, CJO5, CKRT08, Chen06, Cre00, DMT07, EKRMA01, EHH04, FMY02, FPU0, Gal02, GH08, GKM+00, GS01, Gor05, GMW01, HCD08a, HCD08b, HHG06, HH04, Ila04, Iwa08, IM06, Jan08b, JXW05, JZCW05, KPS02, Kob00, KV00, Kos01c, LF03, LKY05b, LCK04, LW08b, LSL01c, Lop06, LWK05a, MWS08, Mi01b, PI06, PC09, SN00, SR01, Sha04b, Sha05b, Ship04a, SLC05, Sun00b, SZP02, SC05c, TO01, TL05, Tsa05, TJC03, VS01, WDLN09, War00, Wu01, WH03, WL04b, hY08, YRS*09, ZSM05, AL06, BDZ04, Ben02, CZ05, Des02, GL05, KGO4, Kim01, NP02a, Vau05a, YDKM06]. Public-Key [Ano01j, AEAQ05, BC05a, BBM00, BBPD01, BLM01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DV04, DJ01, DFK*03, ESG*05, ES00a, FL06, GHW01, GC01b, HR05, IEE00b, Kat05b, KKM01, KM01a, KLY02, KKY02, KY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Mu03a, Mol03b, Mi01a, NP02a, NBD01, NSS02, OTU00, PHK*01, Pei09, PR01, Poi02, PNM03, Qu01, RSA00a, RKS+02, ST01a, ST02, Sin01a, Sm01c, Ste01, TS000, TT01, Vau05a, WZW05, WH01]
SLC05, Sun00b, TO01, ZSM05, GL05].
Public-Key-Based [YKMY01].
Publication [Top02, DGM03].
Publications [Bee05], publique [RSA09a], publish [SL05b], publish-subscribe [SL05b]. Published [MS03b]. Publishing [An02d]. puce [Car00]. PUFs [MKP09].
Purpose [An07b, An07a, EGG05, GS07a, GPP08, SGK08, LJ05a]. Purposes [LS05a, FSVG01, PBV08]. Push [Pau03].
puzzle [LF03]. Puzzles [ANL01, CHS05].
Q [BFMR02, CH01b]. Q&A [Str01b, Win01]. QCQC [Wil99]. QCQS [Wil99]. QDSL [CUS08]. QNX [An02d].
QoS [JKRW01, Zea00]. QoS-aware [Zea00].
QSIG [ECM00b]. QSIG-WTMAU [ECM00b]. Q'tron [YC07]. QUAD [BGP09]. Quadratic [BT02, Coc01b, HJW01, SP05, CCS08, HM00, Hiih00, HP01, LD01].
Quality [BW07, TL07, DMSW09, GXT08, KC09a, WWTH08]. quality-conscious [DMSW09].
Quantifier [KSS06b]. Quantifier-free [KSS06b]. Quantitative [Bai08, ME08a].
Quantization [DRL09, WC04]. Quantum [AC02, ATVY00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL05, BBD09, BZ02, BBB02, BB03, BLM00, BEM07, Coc03, DFS04, DFP05, DFS08, DMS00, EJJ04, Ett02, GKK09, GH02, GW00, GRTZ02, HV09, Hay06, Inur03, Ina02a, Ina02b, Kak06, KK06, KL05, LB04, LW05b, NA07, OTU00, PC09, Ree01, RK05, Ser06, SR07, TO01, Wil99, Wri00, Y100, Y101, ZL0G01, ABV09, Ano03e, Ano06d, BYJK04, BCG02, Ber09b, BEZ02, BEZ01, BLRS09, DFS05, Du0v03, Eke02, GKK07, Gav08, HHG06, IM06, JZ09, JRS09, JAW00, Joy00, KK07, KH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Sin99, Sin00, Sm04, UHA09, BZ02, BD08, BBD09].
quantum-storage [DFSS05].
quarter [Kob00]. quarter-century [Kob00]. quarters [Cla00b]. QUARTZ [PCG01].
Quasi [MD05]. Quasi-Pipelined [MD05]. Quasigroup [MSNH07]. Québec [ACM02].
Queen [Ree01, Sin99]. Queenstown [Zhe02b]. queries [CKK03, Fis01a, GPC08].
Query [GA03, PT08, PCK02, BKW03, PM08, YLC09]. Query-preserving [GA03]. querying [FJ04, UG08]. question [OC03].
Questions [Ett02, Joh00, Jac00]. Queues [WWL02]. queuing [CUS08].
quick [Dew08].
R [Kat05b, Pag03, Spr03, Bih00]. R&D [Mau05]. Rabbit [BVP04]. Rabin [Bon01, Gen04b, Myi01].
Rackoff [MP03, Pat03a]. radar [GG05b].
Radiations [SGM09]. radical [Web02].
Radio [Sak01]. RadioGatún [BDPV09].
Radix [HKA05, JY01]. Radix- [HKA05, JY01]. rails [Fox00]. Rainbow [DS05a].
Raises [MP00]. Raising [Cos03].
ramp [UY06]. Rampung [Coc02b]. Random [Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CTO09, Chio08, Dic03, DGP07a, DGP07b, DVO8, EHK03, Gra02b, GPR06, HSR01, HBF09, Int03, JRR09, Kel05, LLL01, LM02, Lys02, MP03, Mir02, NNT05, Pab02, Pas03, Pat04, Ran55, Ran01, RSN01, SFD06, TWNO08, TL07, Tip27, TTT09a, TTT09b, Var03, VKS09, WP03, BK07, Bel08, BG08, BG09, BG07a, BGL03, CJL06, CO09, DGP09, Fis01a, GVC08, Gen00b, GB09, HGO5a, HLLWZ09.HMvLM07, JAW00, KHO8, KB39, KG09, MI09, MFK06, NR04, Pan07, PSG09, PSP08, PC00, Reg05, Reg09, RC09, RGX06, SS03, SXY01, SR07, SK01b, Sug03, SL09, UHA09, WW08, YZEE09, BH05].
Random-Error [LM02].
random-self-reductions [Fis01a].
Randomats [San01]. randomization [WHH05].
randomization-enhanced [WHH05].
Randomized [Sem00, Hro05].
Randomness
[DD00, DD04, DGH+04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN+04, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03].

Range [CW09]. Rank [Sun00a, DW01, Sim02]. Ransom [BH05].

Rao [ZYR01]. rapid [OP01b]. Rate [KT01, L209, PS02a, Sun02]. Rates [GH02].

Ratio [D1 01]. Rational [HT04]. ratios [Zir07]. RBAC [LSZ05, SN04, ZP05].

RBAC-Based [LSZ05]. RC4 [FMS01, Mir02, VV07]. RC6 [GHJV00, GHJV01, IK01, KM00, KM01b, RRY00, STK02]. RCES [LLCL08].

RCES/RSES [LLCL08]. re [AH05, AFGH06, KHL09]. re-encryption [AFGH06, KHL09]. re-signatures [AH05].

Reachability [AL00a, MT07]. REACT [OP01b]. Reactive [Shy02]. Real [BSW01, Dri02, GSB+04, JBR05, SP05, Sta05, YKMB08, GM04, HP01, Lie05, SL07, SGPH08, YZDW07]. Real-Time [Dri02, GM04, YZDW07]. Reality [Coc01a]. Really [CZB+01, Wei00, Dav01c]. reap [CH00]. reason [Lau08b]. reasoning [IK03].

Rebalanced [SWH+09]. Rebalanced-RSA [SWH+09]. rebels [Lev01]. Rebuild [Sal05a]. Receipt [HS00].

Receipt-Free [HS00]. Receipts [Cha04]. Receive [Coc03]. Receiver [CCD07].

Receivers [NNL01, SBB05]. recently [JK01a]. Reception [Top02]. Recipes [VM03]. Recipient [ANR01, Kur01].

Recipients [Coc01a]. recoding [SSST06]. Recognition [Ano02d, LLT+04, LST+05, TST90b, HS02b, Li05, MMJP03].

Recommendation [Bar06b, BK06a, BK07, Dwo03, NIS03b]. Recommended [Kel05]. Reconfigurable [BNPW03, PGT07]. Reconfiguring [FD01, FH05, GC01b, KBD03, LZ04, MKP09, MMH02, SJJ09, SKG09, SRQL03, CMS08, DHL06, GC00a, HBC+08, Rhi03].

Reconfiguration [PBTW07]. Reconsidered [Sho01]. Reconstructing [CDF01, FL06, PS01a]. Reconstruction [AF03, CF01b, CDF01, JJ00d, KY01c].

Records [Dur01]. Recoverable [NZCG05, NZS05, SGMV09, YY00].

Recovery [BDK+09, BM01c, CKM00, OS01, PBC05, TC01, VV07, WCZ05, WLT05b, CCH05, CJ05, HW05, LKJL01, PSP+08, Sha04b, SIR04, TJC03, Wu01, ZF05].

Recursive [WHHT08]. Recycling [DFS05, TR09a, TR09b]. Red [Sas07].

Red-Eye [Sas07]. redistribution [KB09].

Redondo [IEE00a]. Reduced [BDK02b, CC08, CS05c, FKSW00, HQ01, HSR+01, KKS00a, KSS00b, KKS01, KML+02, KM01b, KKS00b, MHL+02, NP01, STK02, SK10, YSD02, CV05, Küh01, SK01a].

Reduced-Round [FD01, FZH05, GC01b, KBD03, LZ04, MKP09, MMH02, SJJ09, SKG09, SRQL03, CMS08, DHL06, GC00a, HBC+08, Rhi03].

Redundability [DM00b]. Reducing [AL07, BIM00, SPH06]. Reduction [CM05a, CH07c, Dhe03, Gro01, HGG07, Kid02, PG05, ALV02, HG07, Sug03].

reductions [Fis01a]. Redundancy [AB01, BR00a, FM02b, YLR05].

Redundant [MF01, Tan07a, PS04a]. Redwood [KKP02]. Reed [KY02b].

Reference [BR09, CPS07, Pas03, RS00, Sal07, vT00].

Reference-Watermarking [BR09].

Refined [Sma03b]. Regarding [GMP01a].

Regex [BTTF02]. Region [BSNO00, Bur00]. Region-Based [BSNO00]. register [HTW07]. Registers [CGFSHG09]. Registration [HLM03].

regression [mSgFtL05]. regulations [AN00, Cla00b]. Rehearsal [Ahm08].

reinforce [SWR05]. Rejewski [BCB+05, Kap05]. Related [BDF+01a, Can06b, CY08, FKSW00, Kil01b, KML05, Sat06, Buc00a, Gutxx, HAnR04, Hen06a, Scho0b]. Related-Key [FKSW00].
Reviews
For04, Kid00, Sal03b, Sty04.
Revised
Bla03, BC05b, Chr01, CC0MR02, CC0MR05, CSY09, CGP03, DRO2c, GS02c, GH05, HH04, HH05, Jhe03, Jhe04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, FK03, PT06, RM04, Sii01, Ytr06, AMW07, Ajo01a, BK07, Bir07, CZ05, CKL05, DR05, 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, NNN01, TT01, ZSM05, KT06, KSW06, LH05.
revoke
NN03.
revolution
Bor00, Con00.
Revolutionary
CMB+05.
Rewriting
Cir01, HR04a. RFC [BWBL02]. RFID
And04, AL07, AC0M05, BLDT09, CCSI08, CH07a, CLO09, FW09, Fin03, KKJ+07, OSt06, Ros06b, SE09, TZT09a, TZT09b.
Rhee
Kuh08. Rhode [IE07]. RI [Sil01]. Right
Dhe03, GS07b, HKPR05. righful
[CL08, Lin01a]. Rights [Bar00a, BNPW03, Dreh00, Scro01, Wy01, BA06, UP05].
Rijndael
BB02, MP01a, SKU+00, Wer02, CKK+02, CGBS01, DR00a, DR00b, DR01, DR02b, FKS+00, FKL+01b, FKL+01a, FS01, FD01, GM00a, JmBdXgXm05, KY01b, KM01, KVC01, Luc00, MM01b, DM02, PSC+02, RDD+01, SMTM01, SRQ03.
Rijndael-Like
PSC+02. Ring
[BSS02, Nao02, WBL01, ZK02, Her07].
Rings
[BLST01]. RIPEMD
DG02, WFLY04. RISC
[Cor00a, Gro03, WWCC00]. RISC-Based
[Med03]. Risk
[WA07, Voi05]. Risks
[ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jau00, MN03, Psv01, Sch00c]. Rivest
[BB79, Coc03, SP79]. RMI
[BJ04, BKP09, NMSK01]. Road
[BDPV09, HR04b, PB01]. Roadmap
[Coc02b]. Roaming
[CAC03, YWD08, SSM+08]. Robots
[Coc01a]. Robust
[BB00a, BR09, CJ03c, CWY05, DDO+01, HH09, hKLS00, Lin00a, LHS05, LCC06b, PKJ01, SG07, SOH01, SDFH00, SDF01, VK07, WNY09, WL04b, WMDR08, YPSZ01, ZTP05, LCZ05c, LKZ+04, Mit00, MB08, TND+09, YY05b].
Robustness
[CS05c, HM01b, Rot01, CKL+09]. Rogaway
[WM04]. Roger [GG05a]. Role
[SBG02, YT00, ZGLX05, Cer04a, Cra05b, Gor05, Mau04]. Role-Based
[YT09, ZGLX05, Cra05b]. Roles
[LLL+01, Vix02]. Roma
[AAC+01]. Rome
[IE04]. Ronald [Coc03]. root
[Pet05]. rootkit
[Blu09]. Rootkits
[HB06]. Roots
[Go06, HCK09, CAC06]. Roseau
[PY05]. Rotation
[RBF08]. Rothe
[Fal07]. Rough
[Naz02, WG05]. roughness
[Lav09]. Round
[HI00, BP04, Bih00, BF00a, BDK02b, Che03, DPV04, Dri05, Dra00, FKS00, GKK007, GI02, HSR+01, Kan01, KO04, KKS00a, KS00b, KKS01, KML+02, KK500b, LKHL09, Lin01b, MP03, MHL+02, NV01, RR00, Ros00, STK02, WBRF00, Wer02, YSD02, CV05, CLC08, CKL+03, DLP+09, GI01, HLS+02, Kuh01, LKH+08, MR01b, Pha04, SW05]. round
[RCL08]. Round-Complexity
[Ros00]. Round-Optimal
[KO04]. Rounds
[BDK+09, CD01a, HSIR02, KM01b, Luc00, Pat03a, Pat04, GM00a, SK01a]. Routing
[BDG08, CL05, Ken02a, KB09, LAP08, LHC08, MABI06, PS08a, RVS09, vOWK07]. RSA
[Joy03b, Men05, Nac01, Oka04, Poi06, Pref02c, Shp04a, Wal00, AdI03, Ano01k, Ano02e, AR01, BI04, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BJ000, BF01c, Bon01, BCC01, BP01b, CNS02, CDL+00, CW02, Che01a, CKY05, CNTQ03,
CKN00, CJNP02, CS00, CS03c, CD01b, DK01, DT03, Duj08, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gro01, HN04, Her07, HLLL03, HLH00, HLL03, Int00, Jan08b, JS05, Jon08, JK02b, JJ02b, JG01, Kat01, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, Miy01, Mol03b, MP01c, NZCG05, NZS05, NS01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Sha03a, Shp01, Shp04b, SZ01, Str02, RSA [SWH09, TIGD01, TT00, Ver06a, Wal01, Wal03, WQWZ01, War00, WLHH05, Wie00, WS02, WY05, XC05, Yan07, hY08, YKLM02b, YKLM03, YPKL08, YY00, You06, ZC09, Zhe01, ZWCY02, dW02, RSA-based [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLLL03, NZCG05, Sei05, WLHH05, WY05, YPKL08, YY00], RSA-Encrypted [CD01b], RSA-Primitive [ST01a], RSA(R) [Ano06b], RSES [LLCL08], RST [ZLZS07], Rueppel [Ara02], Rules [Bla01a, Ano00c, Bla01b, GM04, Ste02, Wue09], Running [ZL04c], Running-mode [ZL04c], Runtime [PBTW07], Russia [KS05], Ryan [Puc03], Rye [KJR05], Ryu [KCC05], S [BZ02, Kat05b, Puc03, Bi00, BCDM00, Dav01b, Dav01c, FM02b, JnBdXgXm05, Opp01, SMTM01, ZC00], S-Box [FM02b, SMTM01, JnBdXgXm05], S-boxes [BCDM00, ZC00], S/MIME [Dav01b, Dav01c, Opp01], SAC [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR01, HSS04, ST01d, VY01], SAC99 [HA00], SAFE [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Oiw09], Safe-Prime [ACS02], Safeguard [LXM05], Safeguarding [Sty04, Bar03], safer [Ano00f, NPV01, BDD03], safety [HM01a], SAFKASI [WAF00], Salomon [Pap05], Salsa20 [Ber07, Ber08], Salt [PKBD01], Salzburg [DKU05], Samba [BH00a], SAML [RR04], Samos [KGL04], sampled [WW06], sampling [KB39, Sug03, Tip27], San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Ok04, Poi06, Prea02, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c], sans [Car00], Santa [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a], Santiago [BS03], Sanxin [LSZ05], SAR [BS01c], SAT [KLN+06], Satan [Me04], satellite [CC05c, HYS03], Satisfy [PHM03], satisfying [QP05], Saturation [Luc02a], saving [Le01], Savings [C03], SAX2 [TEM01, He01], Say [Sta05], says [Mad04], SBLH [JK02a], SBoxes [WOL01], SC-CFS [It01], SC2000 [SY00, YS02], SC2001 [AC01b], Scalable [CPh04, HAK05, HY03, KHY08, SPGQ06, LLW08b, ST03a], Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06], Scale [BWE00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a], Scaling [BBPV00, Coc02b, SDFH00, SDF01, PVB01], Scambray [Gum04], Scan [MYC01, BD03, KBD03], SCAN-Based [BD03], Scaring [Ol00], Scenarios [BF05], scene [SG07], Sceptical [Pen01b], Schedule [MHM02, XH05], Scheduling [FMS01, XQ07], Scheme [AR00, AK02a, ACJ00, AF03, BNPS02, BR09, BS01d, BMS03, CL01a, CHK03, CGHG01, CYH01, CT04, CC09, CH01b, CM05a, Coc01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJS01, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LCD07, Miy01, Mi01a, OKS06, PL01, RK06, Sc01, SO012, SW05, SGGB00, SYL00, SNSS01, Ta02, TC01, Tsa01, TTT01, WQWZ01, WZW05, WBD01, YWWS09].
Jan06, Joh05, JLL02, Kah67a, Kah67b, Kah06, Kin02, Kog02, KS03, LD04, LTO4, LM02, May04, MN01, NABG03, NN06, OKS06, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sun02a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, AJ08, AEEdR05, Ano02c, Ano08c, Bam02, BCB05, Cal01, CC05a, CHY05a, CHY05b, CJL06, CK04, CDD00, DD04, DM00a, Di 03, Duj08, FNRC05, FWTC05, FZ06, Gal02, GIKR01, HT04, HJK07, HKS00, IY06]. Secret [Kar01, Kee05, KB09, Lam07, Lun09, MF07, MI09, Na005, PS02a, PW05, Ris06, Sch01e, SBZ04, SC05a, Sm01b, SC02c, Wan05, Win06, YCH04, ZSV05, vDKST06, Hil06]. Secret-Ballot [Cha04]. Secret-code [DW01]. Secret-Key [HR05, RW03a].

Secret-Sharing [BI05b, CDM00, CDI05, DKL00b]. Secretly [CC08]. Secrets [BH06, BBD02, CMS09, CP07, Cop04b, Di 01, Gan01b, Gum04, KMS01, LKM05, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM01, VGM04, AGK07, Ano03b, Ano08b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DLMM05]. Section [Ano04a, Ano07a, BK06b, SGK08, TL02, KP03]. Sector [Cox01, MV01]. Secure [AR00, A000, AF04b, AG01, AP09, Ano01k, ACJT00, AFI06, BDF01b, BST03, BCL05b, Bar03, BCI05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CHK03, CK05, CG08, CW07, CQS01, CHJ01a, CHJ01b, CDM00, CD01a, CS02, CS03b, CDG05, CDG05, Des00b, DG03, DMO0b, ES00b, FGM01, FB01, FP01, FOPS01, GPSC08, GIKR02, GJK03, Gen04a, GD05, HSZ00, HSZ01, HSH02, HSI06, HRS02, Har07b, HKW06, HKL02, HxAL09, HR04b, HL07, Hut01, HLC08, IR01, Ito00, IFH01, JJJ00a, JLO0, JM02, KMM06, KY01a, KO04, KLML05, KC02, KH05, KKL09, KL01b, Kos01a, Kos01b, Kra01, Kra05, KSR02, LCK01, LLL02, LCK03, LW00, Lin01b, Lin03, Lin02, MKP09, Mar02a, Mar07, MV01, Mlo03a, MJ01, NMO05, Nam02, N05, NS05]. Secure [NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RvS09, Rd01, ST00a, Sea05, SDF07, SBG05, Sni02, SKR02, SNR04, SBEW01, Sty04, Tad02, VMSV05, Vau05b, VMC02, VM03, WLL09, WBL01, WGL00, WH05, XS03, ZYM05, Zho06, Aam03, Abd01, AEEdR05, AL07, AFGH06, BDS09a, BDF05, BCP07, CLOS02, CCMT09, CCO4b, CCO4b, CRSP09, CHH09, CG05, Dw04, FM02, Geb04, GIKR01, GCKL08, HSW09, HL03, HL06, HJW05, HBC08, In05, ITE08, IK07, IY06, KOY09, KG09, LL04b, LH04, LHC08, LC04a, LCZ05b, MT09, ML05, Mil01b, OS00, PCSM07, PBMB01, PQ06, PSP08, RH03, RG09, RGX06, Sea09, SBEW09, TCR03, Tse07, Ver01, VK08, WWA01, YGZ05, YTWY05, hY08, YRY04, ZBP05, ZCL05, vV07, Ano08d, Ano12, BS01a, BSB05, CHK08, FIP02h]. Secured [BNPW03, Ito01, UP05]. Securely [HL05a, LLK05]. Securing [Abe01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, IS03, LAPS08, LL05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. Security [AW05, AW08, Ahm07, AJ08, ADR02, And07, And08, Ano02b, Ano06c, AHM02, BP07, BW07, Bam02, BS00, BM00, BP02, BNPS02, BY03, BPR05, BOH05, BBE02, Bis03b, BLa02a, BF06b, BTW01, BUK07, Boy01, BLS00, CG07, CK02a, CN03, Can06a, CGH01, Cer04b, CC02b, CSW08, Che05b, CM05a, CH07a, CSY09, Ch03, Coo01a, CK06, Cor00b, Cor02, CGP02, CG05, Dr00c, Dal01, DN02a, DKMR05, De07, DJ06, Des00c, Dim07, DR02d, DSS01, DK05, DS05b, DBS06, Elb09, ELvS01.
Security [JJ02b, JMV02, JQY01, Kan01, KM02, KSHY01, KL05, Ken02a, KB06, KM03, KDO01, KHL09, Kos01a, Kov01, KXD00, Lad06, Lan00a, Lan04b, LGS01, Lee04b, LKH+08, LKHL09, Leh06, Len01, LNS02, LQ05, Lin02, LXM+05, LWK05b, LP01, MJF07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Miü01a, NIS01b, NDJB01, NP07, Oka00, OP01a, Ort00, PV06b, PSC+02, PTP07, PP03, PTO05, Puc03, Puc05, Puc06, QCB05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sal03a, SJA07, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch01f, Se04, Sh05d, SLG+05, SL05a, Shp02, SEF+06, SEK01, SEK02, SK06, Sta03, SJA07, Ste05b, SB02].

Security-related [Gutxx].

security-sensitive [SPH06]. seed [TP07, KJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Shp05]. seeking [Mos06].

Seeks [CAC06]. Seems [Coc02a]. Selected [BP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, VY01, Ytr06, AMW07, Bir07, BC05b, CZ05, CCL05, DR05, HH04, HH05, PC05a, Wil09, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bur03, dB07]. Selection [IBM00, JKK+01, RS00, SM08]. Selective [CS07c, LS01a, LM02]. Selectively-ID [CS07c]. Selectively [Chi08]. Self [GMM08, HW05, KY01d, P01b, PB05, Sch06b, WHL05, WL05b, ZKL01, BCL05a, BCW05, CSV07, CWH00, CCH05, CJC05, Fis01a, HW04, Lee04a, LH06, LS05b, LWK05a, PC05b, Sh04b, Sh05b, TLH05, TSC02, WZ03, Wy05].

Self-certified [HW05, BCL05a, BCW05, CWH00, CCH05, CJC05, CJC05, Fis01a, HW04, Lee04a, LH06, LS05b, LWK05a, PC05b, Sh04b, Sh05b, TLH05, TSC02, WZ03, Wy05].
self-defense [Wyl05], Self-Enforcing [GMM08], Self-Escrowed [PS01b], Self-Localization [WLT05], self-modifying [CSV07], self-pairing [Lee04a, PC05b], self-protecting [LS05b], Self-Shrinking [WHLH05, ZKL01], Self-Similarity [Sch06b], Selling [Bla01c], semantic [PBV08, SNI00, Sch00c, Coc01a], Semantically [KI01b, ST01a], Semantics [Li01, Mar02b, BFG04, BFG05], Semi [Fer00, Nak02, PC05b], Semi-Equivalent [Fer00], Semi-fragile [SY01b], Semiconductor [Coc02b, Igl02, UHA +09], Seminal [Cop04b], semipublic [YC07], Sender [CMB +05, TJ01a], Sensation [Top02], Sensible [Sch04c], Sensibly [See04, Sty04, Sch03], Sensitive [HT06, Bro05b, SPHH06], Sensitivity [SDMN06], Sensor [AEAQ05, CS08b, DBS +06, Fin06, GPČS08, LNL +08, NABG03, PJDH09, ZYN08, AJS08, CCMT09, HMvdLM07, JRR09, KXTZ09, KHYM08, LDH06, LPV +09, LN04, Lop06, MWS08, MS09b, NC09, NLD08, PS08a,RAL07, TP07, WDLN09, ZSJN07], Seoul [CKL05, KCR04, Kim02, LL03, LL04c, May09, PC05a, PK03, Son00, Won01, WK06], Separable [CD00a], Separating [MKKKW00, Nie02b], Separation [BYJK08, GKK +09, Ke00, Lys02, Mur00, ZGLX05, BYJK04], separations [GKK +07], September [AUW01, AAC +01, AJ01a, BCKK05, BC05b, CS09, CGP06, DV05, DUK05, DFCW00, EBC +00, ELvS01, FLA +03, GKS05, QS00, RS05, SM07b, WKPO3, cdCVV05, AJ08], September19 [AJ01b], September19-21 [AJ01b]. Sequence [HWH01, MS02e, WHLH05, ÁCTZ05, GB09, SL09, WG02, YZEE09]. Sequences [ADD09, BI09, FSGV01, HG05a, JZCW05]. Sequential [GSS08, SNW00, RMH03a, WH02b], Serial [CTLL01, KWP06, Uni00g, Mit00], Serpent [BDK02b, ABK00, IK00, IK01, KKS00a, KKS01, KKS00b, Osv00, Pat01], Server [ANRS01, BMK00, Dew08, KO00, LWK00, NS01b, PS05, TMMM05, XS03, Zha00, BB05, LHL04, LKY05b, LHL03b, NTW07, Ts0a1, TWL05, YS04], Server-Aided [NS01b], Server-Assisted [XS03], serverless [BDET00], Servers [BIM00, HS07, Jab01, KCD07, Mar02a, TEM +01, LS05b, PT08], Service [BACS02, BH00a, CLK01a, DeL07, KZ01, Lan04a, LDM04, Nik02a, Nik02b, PKBD01, CUS08, HILM02, KWDB06, LB05, Mir05, MV03b, SRJ01, SSM +08, ÚG08, Coc02b, Híl06]. Services [ANS05, BCS02, DJLT01, ECM00a, ECM00b, Ksu07, Ts0a1, Uni00b, BDS +09a, BFG04, BFG05, BFG08, CCCY01, HM05, JRJ +06, MPPM09, MV03b, RR04, SBG07, SL05b, TWL05, WA06, BH00b], serving [LLK05], Session [GL01, OHB08, CS04, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00b], Session-Aware [OHB08], Session-Key [GL01], Sessions [KPR03], Set [BBGM08, GRW06, JRFH01, KS05b, WG05, aSM01, BDET00, Che07, CCC05d, DM00a, Mar05b, Sta00], Setup [MYC01], Sets [CSF05, EIG01, TW07], Setting [BBM00, DLY08, LP01, PGT07, GMLS02], settings [Lee01], setup [PS04c], Seven [Luc00], seventh [AAC +01], Several [KS00a, LO4, Ts0a5, ZT03], SFLASH [GM02b, SGB01], SGI [Bar00c], SHA [AD07, BC04a, GLG +02, HKR01, MP06, SK05a, TYYL02, 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], Shamam [Hes04a], Shamir
Shamir’s [LD04]. Shape [Gan01b, Gil07].

Shapes [OMT02]. SHARC [DMSW09].

Share [CT08a, CDI05, FS04, AEEdR05].

Shared [ACS02, BH06, BBKD00, BT02, CGH00a, TEM01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01]. Sharing [BTW05, BI05b, BTW08, BGHP02, CD00a, CLT07, CC08, CYT09, CDM00, CF02, CFS05, CDG05, CDI05, Di01, Di03, DS06, DP07, FM02a, FPS01, FMY01, HNZI02, KIN02, Kog02, KS03, LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, SZ01, Sun00a, TC01, TCC02, WN02, WBD01, ZP01, CGHG06, CC05a, CHY05a, CHY05b, DD07a, DKL00b, FTWC05, GIKR01, HT04, HK500, IT06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCWH07, ZSV05, dRMS05].

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

Shift [CGFH09, Che08a]. Shin [Küh08, Küh08]. Shines [Coc02b]. Shinko [An000d]. Ships [An002c]. Shops [An001c, YSS01]. Shor [KLB02a].

Shores [KKP02]. Short [An0001k, AFI06, BBS04, BGW05, DN000b, Gra02b, LS01b, PM02, RR02, RW02, Vau005b, GL05, WDLN09, Sco02b, Sch01c]. short-term [WDLN09]. Shortcuts [Sha03a]. Shortened [Kur01]. shortest [Pei09]. ShortPK [WDLN09]. Shoup [Luc02b, VMSV05]. shows [AJ08].

Shrinking [Gol01c, WHLH05, ZKL01]. SHS [An008d, An012]. Shuff [FS01c, NSN05, Sas07]. Shuffles [Mir02].

Shuffling [PBD05]. Shut [Gil07]. SIBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [An001i, BU02, KSWH00, Law09a, LL01, Möl02, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP08, WL07]. Side-Channel [BU02, Law09a, Möl02, CNPQ03, PSP08].

Side-Match [WC04]. Siena [BCKKK05]. sieve [CM05b, JL03]. sieves [Har07a]. SIGABA [Lee03c]. SIGACT [ACM03c, ACM05b, Raj06]. SIGART [ACM03c, ACM05b]. Sight [Col03]. SIGMA [Kra03]. SIGMOD [ACM03a, ACM03c, ACM05b, ACM04a, FMA02].

SIGMOD-SIGACT-SIGART [ACM03c, ACM05b]. Sign [BSC01b, BTTF02, Da01c, Kra03, Da01b]. Sign-and-Encrypt [BTTF02, Da01c]. Sign-and-MAC [Kra03]. Signal [An002e, GG05b, Sha01e, CKL09]. Shorted [NSCG05, PL01, PCK02, Pre01, RS01, SA02, ST01b, SO012, SWH05, SPML02, Str01a, SYLC05, SSNG00, TNM00, WQW01, WBD01, XYL09, YDQ01, YSY01, YLH05, ZKD02, ZJ09, Zhe01, AvdH00, BCL05a, BCW05, Cyl00b, Cyl04b, CY04, CCH05, J05, CCH05, Che05a, CJT04, GGK03, HLL02, Hes04a, HP001, HW020, HW030, HW040, HH050, HC04a, HLL03, HC04b, HL04, Kwo02, Kwo03b, LH04, LHY05, LL05b, LLY04, LWZ05, LLH05].

Signature [LCZ05b, LCZ05c, LCZ05a, LC05c, PKH05, PC05b, QC05a, QC05b, Sae02, Sha03c, Sha03d, Sha04b, Sha05a, Sha05d, SCL05, SHT05, TJ03, TYH04, Wan04b, WK05, WLHH05, W0H05, Wh01, W0HH03, W0H03, WY05, X05, Y0H04, Z05, ZP05, 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, CV06, CBZ+01, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZI01, Her06, HM02b, HS01b, HHGP+03, HLT01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00, MM02, MNFG02, PCG01, Ram01, RR02, Rds01, VW01, Xs03, Zho02, An00i, Ate04, AH05, BLH06, BB05, BMW02b, BMW02a, BRLS09, Cal00a, CKK03, Die00, DMT07, Fan03, FWWW04, FB01, GMLS02, HRL09, Her07, HHL00, JLL01, JL04, KKKL09, LV07, LS05b, MMJ05, 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 [An00j, IR01, RR02, HWW04, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imr03, Rec01]. Simple [AKS06, CYH05, CJS01, CJJ03c, CWY05, CS03c, DT03, FSW01, Gir06, HM02c, HLT01, MS01, NAM02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKYYYY03a, LKK03b, LFW04, 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 [Imr03, Rec01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a]. Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09].
SINOBIOMETRICS [LLT+04, Li05]. SIP [NTW07, PM00, SZ08]. Sir [Bud06]. Site [AEV+07, Coc02a]. Sites [Ros07]. situation [AJ08]. six [Bel07a]. Sixth [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, TLC06]. Size [CS07c, CMJP03, HNZI02].
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 [An00j, IR01, RR02, HWW04, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imr03, Rec01]. Simple [AKS06, CYH05, CJS01, CJJ03c, CWY05, CS03c, DT03, FSW01, Gir06, HM02c, HLT01, MS01, NAM02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKYYYY03a, LKK03b, LFW04, 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 [Imr03, Rec01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a]. Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09]. SIM [LLT+04, Li05]. SIP [NTW07, PM00, SZ08]. Sir [Bud06]. Site [AEV+07, Coc02a]. Sites [Ros07]. situation [AJ08]. six [Bel07a]. Sixth [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, TLC06]. Size [CS07c, CMJP03, HNZI02].
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 [An00j, IR01, RR02, HWW04, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imr03, Rec01]. Simple [AKS06, CYH05, CJS01, CJJ03c, CWY05, CS03c, DT03, FSW01, Gir06, HM02c, HLT01, MS01, NAM02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKYYYY03a, LKK03b, LFW04, 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 [Imr03, Rec01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a]. Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09].
[CMG+01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, Ano04b, RM02], smarter [Car01, Cla00b]. 
Smartly [MS01]. Smooth [PS02b, GM05]. SMS [Coes02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. Sni [Ano02e]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sae02, Sha03c]. Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Ahm07, And07, Ano02e, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HHM01, Hoe01, Joh03, Knu07, KSZ02, Lad06, Law09a, LSY01, LLLZ06a, LSVS09, LTM+00, MNT+00, MSNH07, MKY08, McG06, Nd05, PM00, PS01c, RM04, Sch01a, Sch00b, Ste00, USE00b, VH09, VVS01, WHLH05, W01, ZC01, Ano00b, Ano00j, Bir07, CCD+04, CTT07, CC04c, DMS07, GP05, HM04, HL06, Jen09, Mat02, McA08, MCHN05, Pan03, Sch01d, SS03, WL07, WA06, Sal03b, Bol02]. Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [Hoe01]. Software-Oriented [ZC01]. Software/ Hardware [Nd05]. SOI [Ano02e, NFQ03]. SOISIC [Ano02e]. Solaris [Ano00c, BH00b]. Solomon [Kye02]. Solution [Cap01, DHR00, LLS05b, Poh01, Str02, TvdKB+01, LSH00]. Solutions [Ano04b, MV01, Jan00, MS03, MV03b, St.00, Gum04]. Solve [CU01, GS03]. Solving [CJT04, GP08, Wil01a, Bul09, Whi09]. Some [AG01, BDF+01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, Hau00, He02, J01a, RSS04, SHT05, ZF05]. Someren [Ano03e]. Something [FL01b]. sometimes [FNRC05]. Sons [And04]. Sorry [San05]. sorts [Ano03e]. Soul [Blao1c]. Sound [BjP02, FR08]. Soundness [ABHS09, DPV04, MR01c, BPS08, Lau08a]. Source [Bar00c, Bol02, Gut00, HBF09, KLR09, PM00, RK06, TEM+01, Ano03c, BGL+03, Ma08, RVS09, SB05, Bar00b, Lin02]. Sources [KZ07, WLZZ05, KZ03]. Southampton [Bl03]. Soviet [AJ08]. SP [BG07a, Hi09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPA-Based [Nov01]. Space [BGH07, Lu02, MSNH07, NS05a]. Space-Bounded [Lu02]. Space-Efficient [BGH07]. Spain [BS03, DFPS06]. Spam [CMB+05, DGN03, Vix02]. Spammer [Bel04]. SPARK [Jen09]. Sparse [BLST01, BDG+01, FS01b, GS03, BF06a]. Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09]. Spatial-Domain [SDFH00]. Spatio [CTDT05]. Spatio-Temporal [CTDT05]. speakables [BZ02]. Speaker [LM00]. Speaks [VN04]. Spec [Bar00c]. Special [Ano04a, Ano07b, Ano07a, BK06b, GIS05, GS07a, GPP08, SGK08, KP03, FOP06]. Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08]. specialized [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00, LKJL01, RSA00, Mea04]. Specifications [IE00b, BDFP05, BD04a]. Specified [Tad02, He02, LKW05b, YY05a, ZK04]. Specifying [BJvdB02, Cir01]. Spек [KG07]. Spect [GMM01]. Specter [GMM01]. spectra [MS02b]. Spectral [PV05, SK07]. Spectrum [BQR01, LY07, PM00]. Speech [ML+02, AA04a, PY08]. Speech-Generated [ML+02]. SpeechStudio [Ano02e]. Speed [An00d, An02d, Gno01, JKRW01, KMM+06, Lut02, SOTD00, SM02, Wi00, YKMY01, BGL+03, RW07, RMCG01].
Speeding [Osv00, SWH+09, TC05].
Speedup [YKL02b, YKL03]. Speedy [Cre00]. spherical [LZP+04]. Spider [Tur04].
Spies [Gan01b, Win05c, Han06, NRR00]. SPIHT [Che08a]. SPIN [MS02a]. Spline [SPK08].
Splitting [GMM05, LLK05]. SPN [HLL+01, Kan01, PQ03b]. SPNs [CKL+03].
spot [Naf05]. Spread [BQR01]. Spring [Pap05]. Spring-Verlag [Pap05]. Springer [Fal07, Lee03a, Lee03b, Pho01].
Springs [Wil99]. spying [FNRC05]. spymaster [Bud06]. spyware [Ste05c]. SQL [Dew08, HLM02]. Squadron [OC03].
Square [HCK09, HQ01]. Squaring [CH07b, NSS02]. SRAM [HBF09]. SSC2 [HQR01, ZCC01].
SSH [All03, BS01a, BSB05, BKN05, LLK05]. SSH-Connected [Hof01]. SSHFS [Hos06b].
SSL [ASK05, BPST02, CHVV03, JRB+06, KCD07]. SSL/TLS [HQR01, ZCC01].
Stand [CAC03]. Standard [Ano08d, Ano09, Ano12, Ano13, Bar00a, BCP02a, FIP00, FIP01a, FIS01a, Her09, Hug04, HLC08, IEE02b, MM01c, MP01a, Nat00, PM00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, BBK+03b, DRS05, GMR08, Sea09, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02a, Coc02b, Cur05, DR01, DR02b, Dan01, FIP02b, GCO01a, Har00, Lan00a, Lan00b, Lan04a, Mor05, NIS00, SB00, Sta00, Sve00, WBRF00, Wri01, YY06].
Standardized [Man01]. Standards [Ano01f, Bur06, CL07, Coc02b, Hus01, RSA00a, Tsa06]. Standing [Lan00b]. State [And07, CR03, GST04, HBF09, MSNH07, Ris06, TL07, Kar01, Mit00].
State-transition [TL07]. statecraft [dL00]. Stateless [ANR01, NNL01, SK05b]. Stateless-Recipient [ANR01]. States [LB04, Jol01]. static [CW07]. Statistical [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, LZ01, LLL+01, MV03a, Neu04, Pro01, RSN+01, BKW03, Hey03]. Statistically [Fis01b, HR07, HNO+09]. Statistically-hiding [HR07].
Statistically-Secret [Fis01b]. Statistics [CKN01, CNK04, KLML05]. Status [Pre01, Sha03b]. statute [Cal00b]. STDM [WMDR08]. Stealing [Gan01b]. Stefan [AUW01]. Steganalysis [Pro01, Sal05b, WW04]. Steganografie [Sch09]. Steganographic [CT04, HR02, MJF07, RH02, RS00, Wes01, KC09a, LYG02, WTH08, YCL07]. Steganography [BC05a, BGI08, CYH01, ChLYL09, CDR01, CW09, CTH08, Cal03, CMB+08, CS05c, DIRR05, DRL09, FGD01, Fri07, Gal03, HLvA02, HVAL09, Hum05, HSKC01, LSY08, PH03, Sal05b, Sch09, Sha01e, Shi08, SWR05, Wan05, WW06, CDS07, Che07, Che08a, GGS+09, JD01, KPO0, LT04, WW04, WMS08, WAY02b, Way09, YCY07].
Stego [KC09a]. stego-image [KC09a]. Steiner [WL02]. Step [DRL09, KK0905, MP07, SL06].
step-by-step [SL06]. Step-out [KKK09]. Stepping [WRW02]. steps [Bil02].
Stereotypes [GO03]. Stern [CGP08, CS05b]. sticker [GPX08]. Sticks [Sam01]. still [Ano00f]. Stinson [Spr03].
STL [Zol01]. STOC [ACM05c, ACM07, ACM08, ACM09]. Stochastic [MG01]. Stock [Bar00a]. Stone [ML03]. Stones [WRW02]. stop [SSNS00, Win05c]. Storage [DFSS08, Dn01, Din05, HR02, Har07b, Hug04, MTS04, RCB00, Ric07, RH02, Vado03, AFGH06, DFSS05, HGR07, LPM05].
Symbiosis [DF01]. symbol [SVDF07].
Symbolic [Bor01, Jef08, Mar02b, May09, MT07, MP05, ALV02]. symbols [Lun09].
Symmetric [Ano01j, ABM00, BU02, BKM07, CvTMH01, CCM01, Des00b, EP05, FW09, Fil02, RR00, Ust01b, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01].
Symmetric-Key [Ano01j, ABM00, CCM01, EP05, RR00, BMA00a, BMA00b, BMA00c].
symmetric [RBF08].
Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, An000d, BS03, BCDH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Jef08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05].
synchronisation [CMdV06].
Synchronization [GPCS08].
synchronize [Pau02b].
Synchronous [CH01b, Sar02].
synopses [YLC+09]. Syntax [BWBL02, RSA00b, RSA00d].
Synthesis [XZF01, SOIG07, UBEF09].
syslogs [ME08b].
System [An000d, An002c, ANR01, BIP05, BCST00, Bi00, CDP01, CHM+02, CSW+08, CGJ+02, DJ01, DGP07a, DGP07b, DV08, EM03, FL01, It001, Joh05, K02, KHY04, LV00, LS05, LXM+05, MA00a, MA00b, Miy01, MFK+06, MFS+09, RH02, SR01, Sha02, SOI02, Ste05b, TK03, TZO09, USE00a, WG05, WA07, YKMY01, YKL02b, ZYM05, AHK03a, AMR00, An000j, ADH+07, AAKD09, Bu00, BDET00, Bu01, CC02b, CCH05, CJL06, CPG+04, Coc01a, Cre00, CO09, DZL01, DPT+02, DIM08, DGP09, FP00, GG08, GM00, Gou09, HLL+02, Joy03a, KWDB06, KXD00, Kwo03a, LL40b, LKJL01, Lin00a, LK01, MKKW00, RCG+05, Sal00b, SCS05a, SGMV09, SETB08, TKP+08, Wan04a, dB07].
systematic [DW05, ZL04a]. Systemic [KB06].

Table [An003d, MFTT05, XZF01, BZ03, CC05b, Has00]. table-based [Has00].
Tables [AJO08, KB39, RBF08].
Tags [KKJ+07].
Tagging [BP05]. Tags [OS06, ACdM05].
Taiwan [Lai03, An003a].
Takagi [LKYL00].
Takagi-cryptosystem [LKYL00].
Takaragi [WHLH03].
Taking [CD07, Lai07, PM00].
Talkbot [Rot07].
Talk [FGM00a, Lan00d].
tamer [Kap05].
Taming [Aba00, Lov01].
Tamper [LTM+00].
tampering [PS08b].
tandem [DPT+02].
tank [Pau03].
tar [Str02].
targama [MAaT05].
target [BD04b].
Targets [MV01, Pau03].
Tarragona [DFPS06].
tasks [XQ07].
Tate [Jou02, SKG09].
TATSU [TSO00].
natting [CSK+08].
TC [DKU05].
TC-11 [DKU05].
TC-6 [DKU05].
TCB [DFCW00].
TC8 [DFCW00].
TC8/WG8.8 [DFCW00].

Tech [McA08, Shu06, GV09, Jan08b].
Tek [Kir01a, TvdKB+01, Uni00c, Gra01, Uni00f].
Technical [BHM03, GS07b, Lan00c, Scr01, ...
TL02, USE01b, USE01a, USE02c.

Technique [CC02a, Pan09, PQ03b, SC02a, WC03, vW01, CL00, Che08b, Pau03].

Techniques [AIP01, BSW09, Bih03, BBPV00, BDP02, CC04a, Cra05a, DBS+06, Dun06, Gal03, KLN+06, Ken02b, Knu02, KO03, MKF09, NCRX04, PJK01, 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, Cla00a, GSB+04, MP00, NFQ03, Pag03, TV03, AL07, Ble07, Car01, Cas02, Che00, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b].

Tektronix [Ano02e].

TelCorreo [LM00].

telegram [Tuc66].

Telephone [KZ01].

Telelogic [Ano02e].

Telephony [Ano02e, PM00, CGV09].

television [Tuc66].

Temporal [CDTT05, KXTZ09].

Tenth [USE01c].

Term [ABRW01, Dur01, BMV06, ISO05, SGMV09, WDNL09].

Terminal [ECM00a, ECM00b].

terminals [ISTE08].

termination [BP05].

Ternary [AD09, DKL00b].

Terrorism [AN00].

Telling [Gan01b].

template [LLC06a, UBEF09].

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

testable [RMPJ08].

Testing [III00, CGBS01, FI02, Lut02, Lut03, SB00, WA06, Lut03].

Tests [MT02, NM09, GT02, Gut04c].

Text [Lut02, PJH01, PM08].

textbook [BJN00, PP09].

Thank [CMS09].

Their [AGT01, CD00a, Gen04a, JKRW01, LLL+01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, TO01, VW00].

They [WD01a, Tee06].

Theorem [AC02, Eke02, GN01, Sho00a, Sch01b, YKLM03].

theorems [MW04, Nyb01].

Theoretic [CB01, DHR00, Kat05b, Nie02b, VVS01, VDKP05, vW01, Mar05b, NR04, SLP99, Wag03].

Theoretical [SGB01, PRS04].

Theoretically [AP09, DM00b].

Theory [ACM00, ACM01a, ACM02b, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bih03, Boy01, CC04a, Cra05a, Des02, FaI07, HR06, Hay06, IZ00, IRw03, Kim01, Ku02, Lai03, Lee04b, Lu03, MNT+00, Mao04, NP02a, Nao04, Oka00, PW06, Pfi01, Pre00, Rot05, Roy05, Sch06b, SLP03, Spr03, TW02, TW06b, Vau05a, Wal00, WG05, Yan00, YDKM06, Zhe02b, AUV01, AB09, Buc00a, Cas06, Cos00, DW05, Gar04, HHL+00, HW98, Joy00, Ki05, Lai00, Lam01, PPV96, Rot02b, Rot03, SCR05a, Sh05b, Ste08, StI95, StI02, StI06c, Tat05, TW05, Was08b, HR06, KXTZ09, Ki05, Nao04, Nie02a, Nie04].

There [Bar00b, GW00].

thieves [NRR00].

Think [Pan03].

Thinking [See04, Sty04, CSG00].

Third [AL06, BS01b, CGP03, HR06, IY05, KNP01, MS02c, NIS00, W01, W01, CKL05, GKS05, IZ00, JZCW05, Q00, CG+00].

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 [Por06, SS04, BK00, Geb04].

threatened [An00].

threats [CNP03].

Three [BR00b, Kak06, LSH00, Man06, AJ08, CL08, FGM03, GPS05, LKY05, LLS+09, MF07, MANx, SPH06, YC09a, ZL04b].

Three-Key [BR00b].

Three-party [LHS00, CL08, LLS+09, YC09a].

three-principal [ZL04b].

Three-Stage [Kak06].

Threshold [AF04b, AIP01].
BTW05, BTW08, BDDS03, BSS02, CCD07, CLT07, CDN01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, Kin00, Kin02, Kog02, LZZ01, LCZ05a, LP01, MSJ02, Nie02c, STY07, WQWZ01, Wan04b, WH03, XS03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, HWW02, HWW03, HW05, JLL01, JL04, LCC05, LCZ05c, SCL05, TYH04, WHLH03, XC05, YTH04.

Throughput [HV04, LS01b]. thwattering [WL07].

TI [GBKP01]. tib [MAaT07].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07].

Tight [CM05a, Di 01]. Time [AK02a, App07, AJ008, BPST02, BS00b, BSW01, CU01, CJ03a, CNV06, CLZ02, Dr102, GPC08, HM02b, Ina02b, KL05, Kuh02a, LP02a, Lam00b, JLJ05, LDM04, May04, Oec03, Pli01, QSR+02, RR02, CAC03, CCK04b, CL00, DS02, GSO7b, GM04, HHC05, LC04a, MRST06, NS05a, YZD07, hY08, DK08].

time-bound [hY08]. Time-Domain [Kuh02a].

Time-Free [CNV06]. 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, CHK008, JP07, LKJ01, Mao01, HGS00, Zha06].

Timed-Release [CHK008, Mao01, HGS00].

times [AJ08, CCK04b, Mol05].

timestamp [YW04].

timestamp-based [YW04].

Timestamping [MSTS04].

Timing [CKQ06, CWR09, Law09b, Sch01b, SWT07, ASK05, DLK+00a, KS09, OS00].

timing-attack [KS09].

Tiny [Bar00b, WN95, And03].

Tipsy [TvdKB+01].

Tissue [MYC01].

Title [ZHY03].

TLS [HSD+05, JK02b, JJ02b, SBEW01, BFCZ08].

TMAC [K103].

TMS320C6x [WWGP00].

today [Lie05, Nis03a].

Together [WD01a].

Token [Fri01, RSA00d, RSA01, CS04].

Tokyo [An000d].

told [ES00a].

Tolerance [An04a, BK06b, ZL04a].

Tolerant [DS03, HSKC01, BKV03, HGR07, Lin07, PI06, RH04, YbJf04].

Tolerating [KSR02, SKR02].

too [Sch05c, vT01].

took [IEE09a].

Tool [An02d, An02e, KI01b, GPG06].

Toolkit [NIS01a, Sha01a].

Tools [An02d, An02e, Bar00b, Gf01b, Kog02, Ken02b, Ust01b, Bal08, Cas02, GC05, NCRX04, SET08, Kat05b, Puc03].

toolset [Jen09].

Top [Cal01, Fox00, Jan06, MV00, AJ08, GCP08].

top- [GPC08].

Top-Level [MV00].

Topics [HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oka04, Poi06, Pre02c].

topology [HJ07].

Tori [GV05, CPS06].

Toronto [MS05a, VY01].

torsion [KM04a].

Torsion-subgroup [KM04a].

torus [DK08].

Torsion-based [DK08].

Tossing [Lin01b].

totality [HRS08].

Touch [Pau02a].

tour [Pet08].

Town [KJ05].

Trace [Bor01, LNS02, NN03].

trace-and-revoke [NN03].

Traceability [HLL03, HW05, W1H05, WY05].

Traceable [LZZ01, CCH04].

traceback [CS04].

Tracing [KY01d, KY01e, LLL02, NN03, SNW00, TT01, WRW02, WLZ05, WH10].

tracings [RE02].

Track [Fox00, Joy03b, Nac01, Oka04, Poi06, Ph03, Pre02c, USE01b, USE02c, Men05, CAC03, CAC06].

Tracking [WCJ05, FNC05, SZ08, TMW+09].

Trade [AJ008, CMS09, Oec03, PS01c, Uni00f].

Trade-Off [AJ008, Oec03].

Trade-Offs [PS01c].

Tradeoff [LP02a, QSR+02, CW02, Ino05, NS05a, DK08].

Tradeoffs [BS00b, CTLL01, SRQ03, SU07].

Trading [PV06b, SWH+09].

Traffic [FGL02, MIS08, Fie09].

Trail [DR02a].

Train [DR02a].

Training [Coc02a].

Traitor [KY01d, KY01e, LLL02, SNW00, TT01].
WHI01]. Transacted [HBdJL01].
Transaction [RH02, AAKD09].
Transaction-Based [RH02], transactional [ST06], transactions [Cal00b, Cal00a].
Transcript [Ano01a, Ano01b, Ano01c, Ano01i, Ano01j, Ano01e, Ano01k, Mal02, Nik02b]. Transfer [CT08b, Din01, GKM +00, KKL09].
Transferability [HSZI00]. Transfers [IKNP03]. Transform [ABM08, BR09, CPhX04, KC09b, LKLK05, Nak01, SSFC09, VK07, BR06, Che07, OP01b, SR00, LPZ06].
Transformation [CT09, HLL05, DSP01]. Transformations [Fel06, KYY00, LMTV05, Pag03].
transforms [Laf00]. Transient [Ric07, VS08]. Transistor [Coc02a]. Transistors [Bar00b]. Transit [Con00, Cal00c]. Transition [Ase02, TL07]. Transitive [BN02]. Translation [GGS +09, PY06]. Translation-based [GGS +09]. TransLink [Cal00c].
Transmission [MLC01, SNR04, SVDF07]. Transparent [CCDP01, For01, Lin00a]. transport [Bar00b]. Trapdoor [BPR +08, Fis01b, KO03, KO00, Gen04a, JSW05, PW08]. Trapdoors [GPV08].
Travel [Bur00]. Traversal [JLMS03]. Trawling [Knu00a, Knu00b, treatise [Bl00, MAaT03, MAaT04, MAaT07].
treatises [MAaT06, MAaT07]. Treatment [CL05, DK08]. Tree [CC05d, GST04, JLM03, KPT04, LKL05, LM02, TN00, Mon03, PCC03, WL02].
Tree-Based [GST04, KPT04]. trees [Che02, Che07, TC00]. Trends [Ahm08, KB07, Or00, Nd06, PR04]. tricks [All03]. triggered [HHJS04].
tripartite [SW05]. Triple [HSH +01, BR04, CGBS01, Cor00a, FZH05, Ke05, LMP +01].
Triple-DES [Cor00a, LMP +01]. Triples [FS01b]. Tripwire [TvdKB +01]. trivial [KO00]. troubleshooting [HJW05]. True [BST03, Cha04, DV08, EHK +03, HBF09, Pan07, SFDF06, BG08, BG09, GB09, Hau06, HLW09, Ste05c, vT01, VKS09].
Truecrypt [CSK +08]. truly [BGL +03]. Truncated [CS05b, KM02, LHL +02, SKU +00, SKI01, GS09]. Trust [CHSS02, HCD02, Lin00b, LHL +08, Mit02, SMP +09, Dav01c, HJJS04, LY05, LCK04, LL05, LM05, LLW09]. Trusted [DK01, WH01, WV01, AR08, PS04c, ZYL05].
Trusting [CKS09]. trustworthy [CCH05]. Truth [MNT +00]. Tseng [Hwa05, XY04, ZAX05]. TTM [GC00b].
Tuesday [Uni00a, Uni00c, Uni00c]. tunable [LB05]. Tunny [Sal01a]. Turin [AL06].
Turing [Bar00b, RSA03a, Adl03, Coo03, Cop04b, Goo06, Pe08, Riv03, Sha03b].
Turkey [Bor00]. Turkish [DD02]. Turn [Tsa07]. Turning [DJLT01]. tutorial [Can06a, Puc06, Rot02b, Rot03, vT00].
Tweakable [DS08, HR03, LRW02]. Twentieth [Gan01b]. Twenty [ACM03c, ACM05b, AAC +01, B +02, Lan00a].
Twenty-Eighth [B +02]. Twenty-first [Lan00a]. Twenty-Fourth [ACM05b]. Twenty-Second [ACM03c].
Twenty-seventh [AAC +01]. Twin [Ram01]. TWIRL [ST03b]. Two [Ahm08, BDG +01, DIS02, FD01, Hen06b, HSI02, HSS01, HU05, HLT01, HL05b, JZC05, KCP01, KO04, KTC03, KI03, Lin01b, MR01a, MLM03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, St00, Ste05a, Ste01, TW07, WW05, XS03, YYDO01, CLO02, DHL06, GC008, JW01, LMTV05, MC03, MCH05, Pau01, ZLX99, dB07].
Two-Block [KCP01]. Two-factor [Hen06b, Sch05c, St00, Ste05a, dB07].
Two-Key [KI03]. two-level [DHL06].
Two-Party [KO04, Lin01b, MR01a, WW05, CLO02, GCKL08, JW01, ZLX99].
Two-Pass [SK00]. Two-tier [TW07]. Two-Way [DIS02]. TWOBLOCK [Yan05].
Twofish [BF00b, FKSW00, IK00, Ke00, Knu00a, Lcm02, Mdr00, SKW +00].
77

Type
[CKQ03, Dug04, H6501, KYHC01, PDMS09, RMS05, Vir03, GG08, 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 [Sta03, LKZ+04]. UCON [LY05, PS04b]. UK [CZ05, Chr00, Chr01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01].

Ultimate [Di01]. ultra [Bam02, CH70a, DB04, Cal01, Win00]. ultra-lightweight [CH70a]. ultra-secret [Bam02]. Ultrafast [FF01a]. UltraSONIC [MMH02].

Unauthorized [Ano02e]. Unbalanced [FMP03, May02, HLLL03]. Unbelievable [Len01]. Unborn [Pau02a]. Unbounded [RW02, WvD02]. Unbreakable [Ver06b].

Uncertain [See04, Sty04, Sch03]. UNCITRAL [MNFG02]. uncompletatable [NS01a]. Unconditional [HM01b, May01, Pas05, RW03b, WW05].

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

Undeniable [GMP01b, GM03, JSJK01, Miy01, WQWZ01, CHC05, LH04, LCZ05a, SSM+08]. undergraduate [AA04b, Gha07].

undergraduates [DFGH04]. Understanding [CPG+04, Cra05b, Elb09, Gor06, PP09, Sun05, Lun09]. undetachable [BMW02b]. Unexpectedly [Bar00a].

Unforgeable [BKY02, KY01a]. Unicode [Mf070]. 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, CJNP02, CS02, Ifr00, KKKP05, KO03, Pli01, Sho0a, SP79, Cal00c, PS04c]. universality [DS02]. Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DN02b, DN03, NMO05, RK05]. Universally-Composable [AF04b].

Universiteit [BBD09]. University [Kat05b, Puc03, Rot07, Top02]. UNIX [CCDP01, Har01a, Har01b, H6501, Wit01, GSS03]. UNIX-Type [H6501]. Unknown [CT08a, Luc02b, CSW05, HJ07]. Unknowns [CMB+05]. unleash [McN03]. Unleashing [Lop06]. unlinkability [WHH05].

Unpredictability [BS01d]. unprotected [ASK05]. Unravelling [Ano03c]. unsolved [Bel07a, GG05a]. untold [DB04].

untraceability [CL09, LHY05, Par04]. Untraceable [ACdM05]. Untrusted [BMK00, CGK+02, LSVS09, LLK05, ZBP05]. unusual [GG05a]. Unveiled [Bar00a].

Update [TEM+01]. Updated [Cho08a]. upgrade [Pau02a, Pau02b]. Upgrades [Ano02e]. upon [DFG01, PQ03a].

UPPAAL [BBD+02]. Upper [BP03b, DIRR05, KMT01]. Upwards [FV03]. US$54 [Duw03].

USA [ACM03b, ACM04b, ACM05c]. ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KKP02, KJR05, K105, KP01, Men05, Men07, Nac01, Nao04, Oka04, Pol06, Pre02c, Sch01d, Sho0a, Sil01, YDKM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FMA02, IEE01a, IEE05a, IEE05b, IE008, IE009b, K101a, MS05b, NS00, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SM+09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, Wil99, Ymu02a]. usability [CG05]. Usage [LY05, PS04b]. Use [Ba01a, BWBL02, Bol02, BQR01, CPS07, Dre00].

ISO05, Kra03, LCK04, Pau09, PBTW07,
used [CDL06, MSV04]. useful [SM03a]. UserNet [Coc01a]. USENIX [Coc01a]. User [Ano00k, BGP02, CL01b, CMB+05, DP00, Had00, HY01, KZ09, LSZ05, JR03, OHB08, PS01b, Poh01, Sas07, SSM+08, Str01a, Tsai01, BBM00, CL04d, DLY08, GMLS02, Hsu05b, HL05b, KC05, LAPS08, LH02, LKY04, LKY05a, LHL03b, LC05a, LK01, Par04, SS03, SS05, TWL05, WLT05a, YS04, YRY04, ZyLG05, vOT08].

User-Centered [CMB+05]. user-controlled [LAPS08]. user-drawn [vOT08]. user-friendly [SZS05, WLT05a]. Uses [Bau01c, RSQL03]. ushers [Bur00]. Using [AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01c, Ano01j, AD006, BJ02, BH06, BK06a, Bau01a, Bau01b, BP06, BPS02, BR09, BT02, BM00, BPS00, BL02, Che01a, CLLL00, CGBS01, CCW02, CCM01, CH07e, Cir01, DI05, DPR01, DP00, DW01, DGH+04, EFY+05, FJ03, FMP03, Fri01, GC01a, GL01, GSB+04, HGHP+03, HQ05, HJW01, Jah01, JKK+01, JSJ01, KOY01, Kel05, KM01a, KLC+00, KTT07, Krr02b, Kz09, Lan04a, Len01, LB04, LS05a, LM02, LH07, MS02a, MS02a, MLM03, MS03b, MMJ05, NZCG05, NM09, OT03a, PHK+01, PJH01, PJK01, PCK02, PK01, Sh00b, SK05a, Sm03a, SP04, Ste01, ST01c, TS00, TL07, TK03, TT01, VPG01, WY02, Wit01, WC03, XZ01, YKMY01, YLLL02, YSS+01, ZWWL01, Zhe01, AS00, AL07, BCI05a, BCW05, BK07, CG06, CSS07, CWH00, CL04d]. using [CCK04b, CCH05, CHY05b, CKY05, CKY05, Che07, CKY07, Che08a, Che08b, CJ04, CCK03, Cos00, DZL01, Dan02, DF00, FWT05, GC00a, GM05, Gen09b, GS09, HHSS01, HWW05, HAU04, HTW07, Hr09, HW04, HY03, HL04, JRR09, KOY09, KO09a, KLY03, K09b, KKL09, KKK+07, KS06, KR03, KU04, KC05, LH02, LH02, LKY04, LCP04, LL04b, LW04, LKY05a, LLW05, LLI09, LW04, LC05a, LCC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, RC05, Sco04, Sha04b, Sha05b, SH07, Tan07a, TLL05, Tsa05, TJC03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04, YW05, YC09a, YRY04, YRY05b, YZ009, YC07, ZW05a, ZFK04].

utility [Gua05]. Utilizing [Str02].

v [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00c]. v2.1 [RSA02]. v2.11 [RSA01]. V [Its00]. V5.1a [CSk+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BLM01, KCI+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [FM00]. Value [BR09, GSS05, LS08, BMW02a, DK08, WWTH08]. valued [DL01, MS02a]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadharajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSN05, Brr08, Duj08, Duj09]. Variants [BDK+09, DG02, KS00b, CJ05, Sha04b, TJC03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDhK09]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SB02, WC04, Pei09, mSgFl05, WQ08]. vectors [LH04]. Vegas [ELvS01, IEE01a]. Vein [BDhK09]. Vendors [Pau03, MV03b]. Venona [Ben01b, Ben04]. Verenigde [dL00]. Veridicom [Ano02d]. Verifiable [ANR01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Ly02, NZCG05, NZS05, NSN05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a]. Verifiably [BDL03, Hes04a]. verifiably-encrypted [Hes04a]. Verification [AADK05, Ara02, BPS02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJL06, Coh03, HL05c, JW01, Ler02, MD04, MT07, MSP09].
PBD07, TYH04, Wan04b, Wu01, YLC+09, ZLX99, ZLO4b, CS08b, Uze04]. Verified [BJP02, BFGT08, BFCZ08, CJT04]. verifier [Bla01b, LKY05b], verifier-based [LKY05b]. Verifiers [CL01a, He02, LV07, LWK05b, YY05a, ZX04]. Verify [MS02a]. Verifying [BFG08, BJvdB02, CJM00, HLT01, IR01, PT08, RR02, BLM06, BLP06, HLM00, SV08a, Sha01d]. Verlag [Eag05, Lee03a, Lee03b, Pap05]. Version [Bol02, HPC02, OST05, SKI01, Mis06]. Versions [HSR+01, NPV01, Ano00f, CV05]. Versteckte [Sch09]. Versus [Mad00, Rub00, WWL+02, ASW+01, BJLS02, DBS01, WPP05]. Vertically [DN04]. Very [AAC+01, B+02, CG03, EBC+00, FLA+03, Hfi01, PM02, PBM01, Zir07]. Vestiges [Top02]. VI [Sch04a]. via [AGKS07, Ano00k, ACm05, BDPV09, Car02, Che03, CPG+04, FBWC02, Fox00, HHYW07, HLM03, J00a, KT06, ML05, PG05, RC05, SB01, SLG+05, ZLG01, Lud05]. Victoria [ACM08, ZLO0]. Victorian [Top02]. victory [Hau03]. Vid [CAC06]. Video [BDF+01a, BD03, CDTT05, EFY+05, ISSZ08, KBD03, KJR05, KLL01, LHS05, MLC01, SC02a, BS01b, JA02, KN03, UP05]. Video-Based [KJR05, BS01b, KN03]. videos [YZDW07]. Vienna [BZ02]. Vietnam [Lov01]. View [Bar00a, Mah04, Sin09]. Views [Bar00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03]. Vigenère [DG00]. VII [Sch04b]. VIII [IEE01b, Sch05a]. Virginia [MS05b]. Virtual [Ano00c, HM01a, Pro00, YSS+01, BDS+09a, ML05, ZBP05]. virtualization [CGL+08a, CGL+08b, CGL+08c]. virtualization-based [CGL+08a, CGL+08b, CGL+08c]. Virtues [Tro08]. Virus [Gor06, Ano05b]. Visible [HT06]. Vista [Fer06]. Visual [BDN00, BDDS03, BCD06, CCL09, CTY09, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, ZP05, ABDS01, CDFM05, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Zol01]. Visualization [XYL09, MFS+09]. Viterbi [LBGZ01, LBGZ02]. Vladimir [Puz04]. VLDB [EBC+00, FLA+03]. VLDP [B+02]. VLSI [KJR05, BS01b, KN03]. voIP [Ano05c, SZ08, VAVY09, WJC05]. Volt [Kat05b, Lee03b]. volatile [SET08]. Volume [Gol04]. Vortrag [Eke02]. Voter [Cha04]. Voter-Verifiable [Cha04]. Voting [Cha04, FPS01, HS00, Joh05, JLL02, KMO01, Rub01, CJT03, HJW05]. Voynich [Rug04]. VPN [KMM+06]. VPs [Dav01a]. VQ [WJP07]. VQ-based [WJP07]. Vs [CTBA+01, Di01, Di03, SU07, WW04]. VSS [AF04b, CDF01, FM02a]. Vu [DP00]. vulnerabilities [CSW05, DMS07, Swi05, XNK+05]. vulnerability [KHL09, SGA07, YRS+09]. WA [ACM06]. WACs [Kov01]. Wagner [dVP06]. Wagstaff [Kat05b]. Wahab [MA+07]. Walking [Fox00]. Wallet [ETZ00, JL04]. Walsh [MS02b]. Walsingham [Bud06]. Warn [H601]. WAN-Cluster [H601]. Wang [SZS05]. WAP [JRFH01]. War [Bec02, Bud00a, Bud02, Hau03, Kov01, MH09, OC03, Aj08, DB04, Ris06, Lov01]. 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, Mok01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zan01, AA08, CL08, LYGL07, LCL06a]. Watermark-based [Kwo03a].
Watermark-Fingerprint [KHY04].
Watermarked [ST01c]. Watermarking [AS08, AK02b, AHK03b, AS01c, Arn01, ARC^+01, BR09, BSC01a, BSC01b, BSL02, BQR01, BNS00, CC02a, CH01b, CDT05, CT09, CM02, CMB^+08, DWN01, DNP07, EFY^+05, EIG01, GW01, HT06, HH09, JKK^+01, KCB04, kLS00, KLL01, Kun01, KT00, L090, LLS05a, LKK05, L01, LZP^+04, IWS05, LJP06, L05b, LL01, LS05c, MM01a, MNS01, Nak01, OMT02, PJK01, PK01, PBM^+07, Qu01, Sam09, SOHS01, SFDH00, SFD01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SP08, VVS01, VMDR08, XMST07, YZDW07, YPSZ01, ZLZ07].

Watermarks [Ben00, BB00a, MLC01, Sug01, WC03, WC04, YLLL02, MB08, TN^+09].

Watershed [FBW01].

Watershed-from-Markers [FBW01]. WAV [XFZ01], WAV-Table [XFZ01].

Wavelet [BR09, GW01, LK05, L01, Nak01, VK07, AAPP07, AA08].

wavelet-based [AAPP07, AA08].

Wavelet-Domain [LZ01]. WAVES [LBA00]. Way [BYJK08, BM01a, CHL02, DIS02, DSM00, Fis01b, GKK^+09, HN0^+09, HR05, KO30, KO00, LT0W05, Sh00a, YZ00, AK02a, AGG06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK^+07, HR07, HRS08, JZ09, KK07, KKK05, KK03, LW04, LP05, LQ08, KKJ01, Mic02a, Po00, YW05, YRY05b, ZW05a]. Wayness [KI01a, PV06b]. Ways [BB02].

[tr06]. WDDL [MMMT09]. Weak [HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00]. Weakening [ZD05].

Weakly [BS00a, CHS05]. Weakness [SW05, SZS05, YPKL08]. Weaknesses [FMS01, He02, KCL03, KCC05, SGGB00].

Weapons [RR03]. Weather [WWL^+02].

Web [Mar05a, BFG05, BFG08, Hili06, An01c, An02e, An03c, AEV^+07, BFG04, BC04b, CCC01, Coc01a, Coc02a, Coc02b, CZB^+01, DeL07, DMS09, FSS01, G02a, GSVC02, HM05, JRB^+06, KCD07, LWK00, LLS05b, LX^+05, MPPM09, PM00, RO04, Sam09, SSS06, Sch01a, SBG07, TMM05, WA06, YSS^+01]. Web-Based [An01c, Sch01a, YSS^+01]. Web-enabled [CCY01].

webcam [McN03].

WebFountain [An03c]. Webrelay [Zha00]. Weight [CH07c, GK02, WT02].

Weighted [BTW05, BTW08, SC02c, YZ00].

Web [BF01b, BF03, J002, Kir03]. Well [WWGP00]. Welschenbach [Ter08]. Welsh [Rot07]. went [AJ08]. WEP [SIR04]. were [Hau06].

Wesley [Puc03]. West [Fra01, Jue04, Syv02, Wri03]. Westbridge [An02a]. Western [CZB^+01]. Wet [CC09].

Weyl [Sug03]. WG [DFPS06]. WG11.1 [ELV01]. WG11.1/WG11.2 [ELV01].

Wheeler [ABM08, Bar05]. Where [Bur06, Pem01a]. While [Tee06]. WHIM [JA02]. WHIRLPOOL [RB01]. Whisper [NAG03]. Whitening [Oni01]. Whitfield [Jan08a].

whole [CPG^+04]. Wi [Puz04, Sty04, VG04, FMA02, Bar03].

Wi-Fi [Sty04, Bar03]. Wi-Foo [Puz04, VG04]. wicked [Lud05]. Wide [DR02a, SBB05]. Width [OT03b]. Width-OT03b. Wiener [Duj08, Duj09]. WIESS [USE00b].

Wiley [And04, Gra01, Kir01a].

Will [Orr00, Cla00b, Fr005]. William [Pag03]. Williams [Mü01]. Window [OT03a, SSST06]. Windows [USE00a, DGP07a, DGP07b, DGP09, Fer06].
REFERENCES

[Ahm08, CM02]. Yellow [JYZ04]. Yen [LLLZ06a, LLLZ06b]. Yen-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]. [AA04b] You've [Nic01]. Yuck [Sas07]. Yuen [KH08].

Z [Wue09]. Z-parameter [Wue09]. z10
[Web08]. z9 [ADH+07]. Zealand [Zhe02b].
Zeilinger [Duv03]. 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, Tuc66]. ZK [PBD05]. Zodiac [AA08]

References

XXX:2002:CC

Al-Akaidi:2004:FSP


Agreste:2008:NAP

Apers:2001:PTS
Peter M. G. Apers, Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Kotagiri Ramamohanarao, and Richard T. Snodgrass, editors. Proceedings of the Twenty-seventh International Con-
REFERENCES

ference on Very Large Data
Kauffman Publishers, Los Altos, CA 94022, USA,

Al-Azzoni:2005:MVC

[AADK05] Issam Al-Azzoni, Douglas G.
Down, and Ridha Khedri. Modeling and verification of
cryptographic protocols using coloured Petri nets and
design/CPN. Nordic Journal of Computing, 12(3):
200–228, Fall 2005. CODEN NJ
COFR. ISSN 1236-6064.

Anshel:2001:NKA

[AAFG01] Iris Anshel, Michael Anshel,
Benji Fisher, and Dorian Goldfeld. New key
agreement protocols in braid group cryptography.
Lecture Notes in Computer Science, 2020:
CODEN LNCS/19.
ISSN 0302-9743 (print), 1611-3349
(electronic). URL http://link.springer-
ny.com/link/service/series/0558/
bibs/2020/20200013.htm;
http://link.springer-
ny.com/link/service/series/0558/papers/2020/20200013.
pdf.

Almgren:2000:HWC

[AAG+00] Fredrik Almgren, Gunnar
Andersson, Torbjörn
Granlund, Lars Ivansson,
and Staffan Ulfberg. How
we cracked the Code Book
iphers. Technical report,
????, ?????, October
11, 2000. 40 pp. URL
http://frode.home.cern.
ch/frode/crypto/codebook
solution.pdf; http://
www.simonsingh.com/cipher.
htm. See [Sin99].

Ababneh:2009:CSE

[Sufyan Ababneh, Rashid
Ansari, and Ashfaq Khokhar.
Compensated signature em-
bedding for multimedia con-
tent authentication. Journal of Data and Information
Quality (JDIQ), 1(3):17:1–
17:??, December 2009. CO-
DEN ????. ISSN 1936-1955.

Ashraf:2009:SBE

[AAKD09] Manzur Ashraf, Syed Muf-
zul Aziz, M. Lutful Kabir,
and Biswajit K. Dey. A SIM-
based electronic transaction
authentication system. Interna-
tional Journal of Computer
Systems Science and Engineering, 24(4):
??, July 2009.
CODEN CSSEEI.
ISSN 0267-6192.

Aamodt:2003:CSP

[AMod03] Ken S. Aamodt. A cryp-
tographically secure pseudo-
dorandom number genera-
University, West Lafayette,
IN, USA, December 2003.
147 pp. URL http://
catalog.lib.purdue.edu/
Find/Record/1380784;
Agreste:2007:IAW

An:2001:DER

Abadi:2000:TA

Aiello:2004:JFK
Abdalla:2005:SER

Abe:2001:SEP

Abe:2004:CEP
Abadi:2005:CFI


Adao:2009:SCF


Anderson:2000:CS


Austin:2000:ASF


Adjeroh:2008:BWT


Abdalla:2001:ODH


[ACM00] ACM, editor. Proceedings of the thirty second annual


REFERENCES


[ACM2004:PAA]


[ACM2005:MPI]


[ACM2005:PTF]


[ACM2005:SPA]


[ACM2006:PTE]


[ACM2007:SPA]


[ACM2008:SPA]
ACM:2009:SPA


ACM:2010:PAI


Algesheimer:2002:ECM


Álvarez:2005:EBS


Ahmad:2007:ADE


Anyanwu:2009:DCS

[ADD09] Matthew N. Anyanwu, Lih-Yuan Deng, and Dipankar Dasgupta. Design of cryptographically strong gener-

**Avanzi:2006:ESM**


**Arnold:2007:CSE**


**Adikari:2009:HBT**


**An:2002:SJS**


**Arazi:2005:RPK**

Benjamin Arazi, Itamar Elhanany, Ortal Arazi, and


Masayuki Abe and Serge Fehr. Adaptively secure Feldman VSS and applications to universally-composable threshold cryptography. In Franklin [Fra04], pages 317–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (elec-
REFERENCES


Atallah:2005:DEK


Ateniese:2006:IPR


Attrapadung:2006:FSS


Akkar:2001:IAS


Acquisti:2009:PSS


Akavia:2006:BOW

Adi Akavia, Oded Goldreich, Shafi Goldwasser, and
REFERENCES


Armington:2002:BAI


Ahmad:2007:CSS


Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB

REFERENCES

Applebaum:2004:CNS


Applebaum:2006:C


Al-Ibrahim:2001:AMS


Attali:2001:JSC


Attali:2001:SCP

Isabelle Attali and Thomas Jensen, editors. Smart card programming and security: International Conference on Research in Smart Cards, Es- smart 2001, Cannes, France, September19-21, 2001: proceedings, volume 2140 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Hei-
REFERENCES

Aid:2008:NSA

Avoine:2008:CIT

Al-Jarrah:2008:NKM

Abe:2002:KES

Agrawal:2002:WRD
REFERENCES

Armknecht:2003:AAC

Akinwande:2009:AHC

Amir:2004:PGK

Agrawal:2002:PP

Acicmez:2006:PSB

Agrawal:2004:OPE
Amadio:2000:RPC


Aoki:2000:FIA


Atallah:2004:ALA


Atzeni:2006:PKI


Anshel:2007:RME

REFERENCES

**Allen:2003:EST**


**Allman:2006:MAW**


**Alvarez:2000:SMC**


**Amadio:2002:SRP**


**Alvarez:2000:CCE**


**Alvarez:2004:KCC**


**Adams:2007:SAC**

REFERENCES

Andem:2003:CTE


Anderson:2004:BRR


Anderson:2007:SSS


Anderson:2008:SEG


Aura:2001:RA


Anonymous:2000:AIH


Anonymous:2000:AIah

[Ano00b] Anonymous. Author index. In Bellare [Bel00], pages 545–?? ISBN 3-540-
Anonymous:2000:CRR

Anonymous:2000:CCI

Anonymous:2000:CLI

Anonymous:2000:EES

Anonymous:2000:GBE

Anonymous:2000:PESa

Anonymous:2000:PTD
REFERENCES


REFERENCES

Anonymous:2001:AIgb


Anonymous:2001:EER


Anonymous:2001:EMB


Anonymous:2001:LBS


Anonymous:2001:EDS


Anonymous:2001:PKC

Anonymous. Public-key crypto-systems using symmetric-

Anonymous:2001:SCS


Anonymous:2002:DEC


Anonymous:2002:IHB


Anonymous:2002:NSD


Anonymous:2002:PPD


Anonymous. For Taiwan’s 22 million citizens, Java Smart
CODEN PCMGEP. ISSN 0888-8507.

[Anonymous:2003:NAW]


[Anonymous:2003:NUP]

CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic).

[Anonymous:2003:TMP]

<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>1950</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>L. Euler</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>4433</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. Swansea</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</td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td>Anonymous</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>Anonymous</td>
</tr>
<tr>
<td>32</td>
<td>756839</td>
<td>1992</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud et al. (GIMPS)</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, Woltman, &amp; Kurowski (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>2009</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>
REFERENCES

2004. CODEN ???? ISSN 0965-2590.

Anonymous:2005:CEC [Ano05a]

Anonymous:2005:WAS [Ano05b]

Anonymous:2006:JHD [Ano06a]

Anonymous:2006:RC [Ano06b]

Anonymous:2006:SSD [Ano06c]

Anonymous:2006:SQE [Ano06d]

Anonymous:2007:CPSH [Ano07a]

Anonymous:2007:CPSf [Ano07b]
Anonymous:2008:KAD


Anonymous:2008:RCB


Anonymous:2008:RES


Anonymous:2008:SHS


Anonymous:2009:DSS


Anonymous:2012:SHS


Anonymous:2013:DSS

REFERENCES

Ateniese:2001:SRC

Amir:2001:FAA

ANSI:2005:AXP

Abe:2000:PSP


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

Agarwal:2008:DWS


Asenjo:2002:AES


Ashburn:2003:PBA


Aciicmez:2005:IBB


Aciicmez:2007:MAC


Blanchet-Sadri:2001:MSD

Abdalla:2000:KMR


Androutsellis-Theotokis:2004:SPP


Allison:2001:LLE


Aharono\textsc{v}:2000:QBE


Alster:2001:PKC

Arnold:2004:IPN


Avanzi:2003:CAD


Aalberts:2000:DSB


Abadi:2005:SA


Abadi:2008:SA


Bernstein:2002:VPT

Philip A. Bernstein et al., editors. *VLDP 2002: proceedings of the Twenty-Eighth International Conference on Very Large Data Bases*, Hong Kong SAR, China,
REFERENCES


Blanton:2006:SRF


Bagnulo:2002:PAA


Badra:2007:AWC


Baier:2001:ECP


Baier:2001:ECS

Baigneres:2008:QSB

Bamford:2002:BSA

Banks:2005:TFC

Bao:2004:CPK

Baran:2000:NVB
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.

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

Baran:2000:NVR

[Bar00c] 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


Barkan:2003:HSY


Barron:2005:DWP


Barkan:2006:CCP


Barker:2006:ROA


Bard:2009:AC


REFERENCES

Baudet:2005:DSP


Bauer:2007:DSM


Blakley:1979:RSA


Benedens:2000:TBD


Buchmann:2000:ECC


Barkan:2002:HMW

REFERENCES


Bernstein:2009:PQC


Beimel:2000:CFS


Bellare:2001:KPP


Blumenthal:2002:SAD


Bartolini:2008:EIS


Barkan:2003:ICO

[BBK03a] Elad Barkan, Eli Biham, and Nathan Keller. In-

**Bertoni:2003:EAD**


**Bertoni:2003:EAD**


**Bellare:2009:HPK**

REFERENCES

Bobineau:2000:PSD


Boneh:2004:SGS


Blundo:2004:SIA

REFERENCES


[BCCN01] Eric Brier, Christophe Clavier, Jean-Sébastien Coron, and David Naccache. Cryptanalysis of RSA signatures with
fixed-pattern padding. In Kilian [Kil01a], pages 433--??
no.2139. UK £47.00. URL
http://link.springer-ny:
com/link/service/series/|
0558/bibs/2139/21390433.| |
htm; http://link.springer-
ny.com/link/service/series/|
0558/papers/2139/21390433.| |

Blundo:2006:VCS

Carlo Blundo, Stelvio Cimato,
and Alfredo De Santis. Visual
encryption schemes with optimal pixel expan-
sion. Theoretical Com-
puter Science, 369(1–3):169–
CODEN TCSCDI. ISSN
0304-3975 (print), 1879-2294
(electronic).

Bruguera:2009:PIS

Javier D. Bruguera, Mar-
ius Cornea, Debjit Das-
Sarma, and John Harrisi-
on, editors. Proceedings of
the 19th IEEE Symposium
on Computer Arithmetic,
June 8–10, 2009, Portland,
Oregon, USA. IEEE Com-
puter Society Press, 1109
Spring Street, Suite 300,
Silver Spring, MD 20910,
USA, 2009. ISBN 0-7695-
3670-0. ISSN 1063-6889.
URL http://www.ac.usc.
es/arith19/.

Burnett:2000:EMG

L. Burnett, G. Carter,
E. Dawson, and W. Mil-
lan. Efficient methods for
generating MARS-like S-
boxes (abstract only). In
NIST [NIS00], page 10.
ISBN ???. LCCN ???.
gov/encryption/aes/round2/
conf3/aes3conf.htm; http:
//csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-1.pdf;
http://csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-2.pdf;
http://csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-3.pdf;
http://csrc.nist.gov/
encryption/aes/round2/
conf3/papers/AES3Proceedings.
pdf.

Barnum:2002:AQM

H. Barnum, C. Crepeau,
D. Gottesman, A. Smith,
and A. Tapp. Authen-
tication of quantum mes-
ages. In IEEE [IEE02],
pages 449–458. CODEN
ASFPDV. ISBN 0-7695-
1822-2. ISSN 0272-5428.
LCCN QA267. URL http:
//ieeexplore.ieee.org/
ie15/8411/26517/01181969.| |
pdf?isnumber=26517&prod=|
CNF&arNumber=1181969&arSt=|
+449&ared=+458&arAuthor=|
Barnum%2C+H.%2B+Crepeau%
2C%2B+Gottesman%2C+
D.%2B+Smith%2C+A.%2B+Tapp%
REFERENCES


REFERENCES


REFERENCES


Bresson:2007:PSA


Bellavista:2002:JLD


Baiham:2008:BA


Betarte:2000:SSC


Bao:2005:RWH


Biham:2000:CAG

REFERENCES

Boneh:2000:CRP


Bourbakis:2003:SBC


Bozzano:2004:AVS


Burmester:2004:HPK


Buchmann:2008:PQC


Biryukov:2003:CS

REFERENCES


Bodei:2002:PAP

Chiara Bodei, Pierpaolo Degano, Riccardo Focardi, and Corrado Priami. Primitives for authentication in...
REFERENCES


REFERENCES


REFERENCES


**Biryukov:2004:MLA**


**Baldwin:2009:PSS**


**Buchmann:2009:HBD**


**Bertolotti:2008:ERA**


**Boneh:2001:MFR**


**Bao:2004:PKC**

REFERENCES


REFERENCES


[0558/papers/2140/21400019.pdf]


REFERENCES


Benantar:2002:IPK


[Ben02] [Ber03]


Benson:2001:VS

[Ben04] [Ber03]

[Bersen:2003:CAB]


[Bernstein:2007:SFS]

REFERENCES

Bernstein:2008:CVS


Bergmann:2009:DKR


Bernstein:2009:IPQ


Bouwmeester:2001:PQI


Bouwmeester:2000:PQI


Biham:2000:IDR

**REFERENCES**


**Babbage:2001:MHO**


**Boneh:2001:IBE**


**Boneh:2001:EGS**


**Boneh:2003:IBE**


**Boldyreva:2005:ARO**

Bisseling:2006:MSM


Boldyrev:2006:SO


Bhargavan:2005:SWS


Bhargavan:2008:VPB


Bhargavan:2008:VII

REFERENCES

December 2008. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).


[BG09] Marta Blaszczyk and Richard A. Guinee. Experimental validation of a true random binary digit generator fusion with a pseudo random number generator for cryptographic module application. In *IET Irish Signals and Systems Confer-
Barthe:2009:FCC


Boneh:2007:SEI


Bennett:2002:ESE


Barak:2001:IPO


Bogomjakov:2008:PMD

Bertoni:2003:EAA


Bucci:2003:HSO


Boneh:2003:AWE


Branovic:2004:WCE


Boneh:2005:EDF


[BGW05] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Shoup [Sho05a], pages 258–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic).
REFERENCES


**Beck:2000:FSD** [BH00a]


**Bialaski:2000:SLN** [BH00b]


**Barak:2005:MAP** [BH05]


**Badra:2006:KEA**


**Backhouse:2003:TOT**


**Bajard:2004:FRI**

REFERENCES


Biham:2002:HDE


Biham:2003:ACE


Beimel:2000:RSC


Bajard:2005:AOP


Biryukov:2007:FSE

[Bir07] Alex Biryukov, editor. Fast software encryption: 14th in-
Bishop:2003:ICJ


Bishop:2003:CSA


Blaser:2002:PCC


Boneh:2000:WTE

REFERENCES


[BK06a] Elaine Barker and John Kelsey. Recommendation


[BKN04] Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: a case study of the encode-then-encrypt-

**Bajard:2009:SRB**


**Blum:2003:NTL**


**Buonanno:2002:IUE**


**Broadfoot:2002:ASA**


**Bucci:2008:FDR**


**Black:2000:TDE**

Michael Andrew Black. A treatise on data encryption and an example of the
REFERENCES

black algorithm. Thesis (M.A.), University of California, Santa Barbara, Santa Barbara, CA, USA, 2000.

Blanchet:2001:ACP


Blanchet:2001:ECP


Blaze:2001:LYS


Blancchet:2002:SAS


Blaze:2002:CI


Blaze:2003:FCI

REFERENCES


Burmester:2009:UCR


Bleumer:2007:EPS


Bao:2006:CIB


Berbecaru:2001:CPK


Brassard:2000:SAP

[BLMS00] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Security aspects of practical quantum cryptography. Lec-
REFERENCES


Bozga:2006:PBA


Buchmann:2009:PQC


Banks:2001:CAS


Blunden:2009:RAE


Batina:2001:AWD

REFERENCES


REFERENCES


REFERENCES

Boyko:2000:PSP

Boneh:2003:VTS

Boneh:2003:PAU
REFERENCES


[BNPS02] Mihir Bellare, Chanathip Namprernpre, David Pointcheval, and Michael Semanko. The power of RSA inversion oracles and the security of chaum’s RSA-based blind

[Bouganim:2003:CSD]

[Bodycombe:1999:CC]

[Ben-Or:2005:UCS]

[Bollinger:2002:UFO]

[Bondi:2000:CVB]

[Boneh:2001:SOR]
Dan Boneh. Simplified OAEP for the RSA and Rabin functions. In Kilian [Kil05a], pages 275–??. ISBN 3-540-42456-3 (paperback). LCCN QA76.9.A25...
REFERENCES

C79 2001; QA267.A1 L43
no.2139. UK£47.00. URL
http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390275.htm;


Barak:2003:DC


Barak:2007:DC


Boyd:2001:ACA


Boyen:2003:MIB


Bedi:2001:CNF

REFERENCES

Burnett:2001:RSO

Bellare:2002:GSI

[BP01b]

[BP02]

Bellare:2003:CAC

Buchbinder:2003:LUB

Bellare:2004:KEA

Barbancho:2003:CAF

Buchbinder:2003:LUB

Bellare:2004:KEA
REFERENCES

Blanchet:2005:VCP


Beissinger:2006:CUM


Baer:2007:CIS


Bellare:2000:AKE


Borst:2001:CSC


Bellare:2005:ISA

Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. In Shoup [Sho05a, pages
REFERENCES


Boneh:2008:IBI

BPR+08


Baudron:2000:ENS

BPS00


Benerecetti:2002:VST

BPST02


Brandao:2001:UEC

BQR01

REFERENCES

Bellare:2000:ETE


Black:2001:CAF


Black:2002:BCM

REFERENCES

Bellare:2004:CBG


Bugliesi:2005:NIP


Bellare:2006:MPP


Bhatnagar:2009:RRW


Brands:2001:RPK


Brandt:2001:CPS


Brown:2005:CEC

REFERENCES


REFERENCES


REFERENCES


[BSL02] Stéphane Bounkong, David Saad, and David Lowe. Independent component anal-
REFERENCES


Bhargav-Spantzol:2007:PPM


Buchmann:2002:ICP


Biryukov:2001:RTC


Bethencourt:2009:NTP


BSW09]

REFERENCES

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

Biehl:2002:NDP


Boyer:2002:LDS


Beimel:2005:CIW


Beimel:2008:CIW


Black:2002:SCA


Buchmann:2000:CTC

Johannes Buchmann, editor. Coding theory, cryptography, and related areas: proceedings of an International Conference on

**Buchmann:2000:IC**


**Buchmann:2001:IC**


**Buchmann:2004:IC**


**Budiansky:2000:BWC**


**Budiansky:2000:DBU**


**Budiansky:2002:BWC**


**Budiansky:2006:HMS**

REFERENCES


REFERENCES

Boesgaard:2004:RNH

Baker:2007:ISU

Blake-Wilson:2002:RUE

Butler:2000:RSA

Bellare:2003:FSP

Bar-Yossef:2004:ESQ
Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In ACM [ACM04b],
Bar-Yossef:2008:ESQ


Bertlmann:2002:QUB


Bond:2003:DTA


Borders:2005:CHP


Carrington:2002:EDS


Staff:2003:NTC

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

Staff:2006:NTS

[CACM Staff. News track: Super game plan; E-learning roots disputed; Chinese history; U.K. seeks popular science input; encryption...

**REFERENCES**

**CALACIT:2000:SID**


**CADOJ:2000:DSE**


**CAMTC:2000:TSC**


**Calvocoressi:2001:TSU**


**Canetti:2001:UCC**


**Canteaut:2001:CFD**


**Canetti:2006:SCC**

REFERENCES


(Car00) Bruno Carriere. Le passe sans contact: autopsie d’une puce. La vie du rail et des transports, pages 43–48, November 2000.

(Car01) Amy Carter. Smart card technology just got smarter. Metro, 97(9), December 2001.


REFERENCES

php/C/30. The front cover of this issue displays eight pages of Alan Turing’s description of the Enigma machine. The issue is a special tribute to Kurt Gödel for the centenary of his birth.

Cobas:2001:CTA

Cooper:2005:AAP

Chandramouli:2006:BPA

Cachin:2000:OFS

Chan:2001:CRP

Carline:2002:NWT
Dylan Carline and Paul Coulton. A novel watermarking technique for LUT based FPGA designs. Lec-
REFERENCEs

ture Notes in Computer Science, 2438:1152–??, 2002.
CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/
link/service/series/0558/bibs/2438/24381152.htm;

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


REFERENCES

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


REFERENCES

Collberg:2004:DPB


Chai:2007:EIB


Cattaneo:2001:DIT


Chen:2004:TPM


Chang:2005:DSM


Chang:2004:IDA

REFERENCES

Chang:2004:SOT

Chang:2009:PCC

Choi:2005:JMA

Christianson:2002:SPI

Christianson:2001:PKC
Christiansson:2005:SPI


Castelluccia:2009:EPS


Chen:2008:NMA


Caboara:2008:GBP

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 ????

Choi:2002:IPP


Camenisch:2000:VEG

Jan Camenisch and Ivan Damgård. Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes (extended abstract). In Advances in cryptology—ASIACRYPT 2000 (Kyoto),

**Carpenter:2000:CB**


**Cramer:2001:SDL**


**Cramér:2000:CVS**


**Ceselli:2005:MAI**

REFERENCES


REFERENCES


REFERENCES

28114-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25
C79 2005; QA76.9 .A25;
QA76.9 C79 2005; QA76.9
C794 2005; QA76.9; In-
ternet. URL http://
\www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

and Jesper B. Nielsen. Multi-
party computation from
threshold homomorphic en-
cryption. In Advances in
cryptology—EUROCRYPT
2001 (Innsbruck), volume
2045 of Lecture Notes in
Comput. Sci., pages 280–
300. Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
many / London, UK / etc.,
\link.springer-ny.com/
link/service/series/0558/
bibs/2045/20450280.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2045/20450280.
pdf.

[CDR01] Mark Chapman, George I.
Davida, and Marc Rennhard.
A practical and effective ap-
proach to large-scale auto-
mated linguistic steganog-
raphy. Lecture Notes in
Computer Science, 2200:
156–??, 2001. CODEN
LNCSDE9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
\link.springer-ny.com/
link/service/series/0558/
bibs/2200/22000156.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2200/22000156.
pdf.

[Castiglione:2007:TAD] A. Castiglione, A. De Santis,
and C. Soriente. Taking ad-
evantages of a disad-
antage: Digital forensics and
steganography using docu-
ment metadata. The Jour-
nal of Systems and Software,
CODEN JSSODM. ISSN
0164-1212 (print), 1873-1228
(electronic).

[Chen:2005:NVW] Zhenyong Chen, Junhui
Deng, Long Tang, and Zesh-
eng Tang. A novel video
watermarking resistant to
spatio-temporal desynchro-
nization. In Han et al.
[HYZ05b], pages 532–??
ISBN 981-270-153-2. LCCN
??? URL http://
eproceedings.worldscinet.
com/9812701532/9812701532.
don31.html.

hierarchies from authentica-
tion data flows. Interna-
tional Journal of Computer
Systems Science and Engi-
neering, 19(3):??, May 2004.
REFERENCES

CODEN CSSEEI. ISSN 0267-6192.

Certicom:2004:CCC


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

Canetti:2001:UCC


Canetti:2001:COR


Cramer:2002:OBB


Cohen:2006:HEH


REFERENCES

Candebat:2006:SPM

Chodowiec:2001:ETG

Copp
er:2000:ICT
REFERENCES

CGHG01

CGJ+02

CGK+02

Caballero-Gil:2006:SSB
REFERENCES

Chen:2008:OVBa


Chen:2008:OVBb


Canovas:2002:DSB

REFERENCES


[CH01a] Chin-Chen Chang and Kuofeng Hwang. Towards the forgery of a group signature without knowing the group center’s secret. Lecture Notes in Computer


REFERENCES

198


REFERENCES

Chen:2001:DEU


Chen:2001:PDP


Cheon:2001:NVR


Chen:2002:SFS


Cheng:2003:PPO


Chen:2004:IAM


[CHH01] Robert S. Coulter, George Havas, and Marie Hen-
REFERENCES


CORON:2001:GGC


CORON:2001:OCC


[CHK05] Ran Canetti, Shai Halevi, and Jonathan Katz. Adaptively-secure, non-interactive public-key encryption. In Kilian [Kil05], pages 150–?? CODEN LNCSD9.


REFERENCES


[Chu02] 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


Cimato:2002:DAP


Cirstea:2001:SAP


[Cornwall:2004:AAM] Linda A. Cornwall, Jens Jensen, David P. Kelsey, Ákos Frohner, Daniel Kouril, Franck Bonnassieux, Sophie Nicoud, Károly Lőrentey, Joni Hahkala, Mika Si-

Choie:2005:EIB


Chin:2006:HSI


Coron:2000:NAP


Coron:2002:UPS

Jean-Sébastien Coron, Marc


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


Canetti:2002:UCN


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


Coppersmith:2000:KRF


Coron:2000:FLA


Chen:2009:SRP

REFERENCES


REFERENCES


Chevalier:2008:CRS

Cachin:2009:TC

Chen:2005:CLR

Chen:2007:CRA

Chen:2000:IBD

Camenisch:2001:IES
REFERENCES

Chang:2001:CIU


Camenisch:2002:DAA


Cao:2002:TKE


Crowley:2002:BLS


Camenisch:2004:SSA


REFERENCES


[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.


Canetti:2002:UCT


Chen:2009:AKD


Clulow:2003:SP


Czumaj:2002:PTA

REFERENCES


[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).


Diane Crawford, Srinivas Nedunuri, Adrian Bowyer, Arnd Weber, Greg A. Woods, and Mark Adler. Forum: Embrace the engineering metaphor; credit for crypto’s parallel development; enough PDF: Give me HTML. Communications of the Association for Computing Machinery, 45(8):11–14, August 2002. CODEN CACMA2. ISSN ????
Coron:2004:SSL


Ciet:2003:PFI


Catalano:2002:HHL


Correia:2006:CAB


Czernik:2009:CRN


[Cobb:2004:CD]

[Coc01a]

[Coc01b]

[Cochran:2002:NVW]

[Cochran:2002:NVWb]
REFERENCES


Coppersmith:2000:C


Copeland:2004:COO


Copeland:2004:ETS


Copeland:2005:CSB


Copeland:2006:CSB


Corella:2000:FIT

Francisco Corella. A fast implementation of DES and Triple-DES on PARISC 2.0. In USENIX [USE00b], page ?? ISBN 1-880446-15-4. LCCN
REFERENCES

Coron:2000:ESF

Coron:2002:SPP

Coron:2006:WC

Cosgrave:2000:NTC

Costlow:2003:BIM

Courtois:2001:EZK
REFERENCES


Courtois:2003:FAA

Courtois:2003:AXA


REFERENCES

Canetti:2007:CSH


Ciet:2001:SFC


Canetti:2003:UCJ


Cramer:2005:ACE


Crampton:2005:UDR

[JCR05b] Jason Crampton. Understanding and develop-


Camenisch:2003:PVE

Cramer:2003:DAP

Crepeau:2003:SBR

Carrier:2004:STP

Collberg:2005:SWF

Contini:2005:SAA
Scott Contini and Igor E. Shparlinski. On Stern’s attack against secret truncated


REFERENCES


REFERENCES

0302-9743 (print), 1611-3349 (electronic). LCCN ????. URL http://www.springerlink.com/content/978-3-642-00306-6.


Chu:2008:EOT


Chou:2009:ATI


Crawford:2001:FPV


[CT09]
REFERENCES

Chiang:2008:CPB


Chang:2004:ASS


Cheung:2001:TPS


Collberg:2007:DGB


Chen:2009:FCV


Cheng:2001:NPT

REFERENCES


REFERENCES

Casu:2004:LG
Julio César Hernández Cast

Canda:2001:SBC

Chess:2007:SPS

Cheng:2009:NAS
REFERENCES

Chang:2000:ELD

Chien:2001:CCW

Crosby:2009:OLR

Chien:2005:NRS

Choie:2002:ICH


REFERENCES

[Chang:2005:CIA]

[Chadwick:2005:PKI]

[Crawford:2001:FHC]

[Cheng:2005:RIC]

[Doedis:2003:CAA]
REFERENCES


[Dav01c] Don Davis. Defective sign-and-encrypt: Can you really

Dav07

DB04

DeBorde:2007:STF

Desmedt:2001:ERD

Doyle:2006:SCK
REFERENCES


diVimercati:2005:CSE


DeBonis:2004:RSS


Diene:2006:DLE


Dolev:2000:NC

Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. SIAM Journal on Computing, 30
REFERENCES


REFERENCES


[Domingo-Ferrer:2000:SCR] Josep Domingo-Ferrer, David Chan, and Anthony Watson, editors. Smart card re-

Durante:2000:CAC

Durante:2001:CWR

DePalma:2004:CCS

Domingo-Ferrer:2001:CDS

Dodis:2003:IRP
Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko

DeSantis:2004:CKA


Domingo-Ferrer:2006:SCR


Domingo-Ferrer:2007:ASC


Damgaard:2004:ZKP

REFERENCES


REFERENCES

Do:2004:REK


Devanbu:2004:FAX


Devanbu:2003:ADP


Dwork:2003:MBF


Dorrendorf:2007:CRNa


Dorrendorf:2007:CRNb

[DGP07b] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas.

**[Dorrendorf:2009:CRN]**


**[DGP09]**


**[dH08]**


Dierickx:2000:EGD


Diffie:2001:UC


Dimitriadis:2007:IMC


Dimitrov:2008:DBN


Ding:2001:OTB


Ding:2005:ECB

Yan Zong Ding. Error correction in the bounded storage model. In Kil-

Ded:2005:ULB


Dang:2002:EPT


Dang:2002:EPT


Dang:2002:EPT

Dang:2002:EPT


Delaune:2006:DPS


[DK07] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*, volume 1 of Infor-
REFERENCES


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

### REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title and Details</th>
</tr>
</thead>
</table>


Y. Dodis, P. J. Lee, and D. H. Yum. Optimistic
References


[DeSantis:2000:SSS]

[DM07a]

[Drimer:2007:KYE]

[Dumais:2000:PCQ]
REFERENCES


[Dowd:2007:ASS]

[Denev:2009:SFQ]

[Ding:2007:ESD]

[Damgaard:2000:INC]

[Durfee:2000:CRS]

[Damgaard:2002:EPF]
Ivan Damgård and Jesper Buus Nielsen. Expanding pseudorandom functions; or:


REFERENCES

[Doncel:2007:ODS]

[Dwork:2003:MFM]

[Dwork:2005:PPW]

[Dodis:2005:GIF]

[Dodis:2004:IPC]
REFERENCES

Computer Society Order Number P2228.

Dhamija:2000:DVU


DeMatteis:2002:PP


Dandalis:2004:ACE


Dziembowski:2007:IRS


Dziembowski:2008:LR


Dandalis:2001:CSP


Damgaard:2005:QCN

Ivan Damgård, Thomas Brochmann, Pedersen, and Louis Sal-

**Delbourg:2002:JBC**


**Daemen:2001:BCP**


**Crescenzo:2004:CRR**


**Daemen:2000:NPN**


**Daemen:2000:BCR**

REFERENCES


REFERENCES

Daemen:2002:FSE


Dray:2000:NPA


Ding:2002:HEE


Dreyfus:2000:PUC


Driscoll:2002:BER


Yevgeniy Dodis, Amit Sahai, and Adam Smith. On perfect and adaptive security...


[Duj08]

Ding:2003:SIB


[DT03]

Duggan:2004:TBC


[Dug04]

Dujella:2008:VWA


[Duj09]

Dujella:2009:VWA


[Dun06]

Duranti:2001:LTP

REFERENCES


REFERENCES

0938-1279 (print), 1432-0622 (electronic).


REFERENCES

ElAbbadi:2000:VPI

Eghlidos:2001:IRL

Eilam:2005:RSR


English:2007:MAC

ECMA:2000:EPIa
REFERENCES


REFERENCES

Ernst:2004:FBH


Ellison:2000:PSK


Eggers:2001:DWC


Ekert:2002:BTQ


Ekeraa:2009:DCM


El-Kassar:2001:GPK


Elbirt:2009:UAC

Elliott:2004:QC


English:2000:MNDb


England:2002:AOO


Elbirt:2005:ILD

REFERENCES


REFERENCES

Eberle:2005:ANG


Enck:2005:EOF


Edman:2009:AES


Edman:2009:AES


Elbirt:2000:FIP

REFERENCES


Fischer:2001:TMR


Fischlin:2000:ENM


Felke:2006:ATH


Filiol:2001:NUS


Ferguson:2000:SEK

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

Ferguson:2006:AEC


Ferguson:2006:ACE

REFERENCES


US$13.95.


REFERENCES


REFERENCES


REFERENCES

282


REFERENCES


Ferguson:2000:TRR


Fluhrer:2001:AES


Fox:2001:PPK


Faure:2006:NPK


Freytag:2003:VPI

Fluhrer:2002:CMB


Fluhrer:2002:CSP


Feng:2006:ISC


Fehr:2002:LVD


Fuller:2002:LRA

REFERENCES


REFERENCES


REFERENCES


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

Faugere:2009:EAD


Fournet:2008:CSI


Frankel:2001:FCI

REFERENCES


REFERENCES


REFERENCES


Ferguson:2003:PC


Fundulaki:2004:SYD


Fortnow:2008:IIC


Fuster-Sabater:2001:EAG


Fu:2001:DCA


Ferguson:2001:SAR

Furman:2001:CSM


Furman:2002:DCN


Furuya:2002:SAK


Furnell:2005:AOW


Fouque:2003:DAW


Feldhofer:2009:HIS

Martin Feldhofer and Johannes Wolkersstorfer. Hardware implementation of symmetric algorithms for RFID security. In Paris Kitsos

**Fan:2008:RSB**


**Feng:2005:NMS**


**Fitzi:2004:PSB**


**Fan:2004:PPI**


**Furnell:2006:RPS**

REFERENCES


**Gaudry:2002:CCS**


**Gavinsky:2008:CIC**


**Guinee:2009:NTR**


**Guajardo:2001:EIE**


**Golic:2002:LCB**

Gaj:2000:CHP

[KGC00a] Kris Gaj and Pawel Chodowiec. Comparison of the hardware performance of the AES candidates using reconfigurable hardware. In NIST [NIS00], pages 40–56. ISBN ???. LCCN ???.

Goubin:2000:CTC


Gaj:2001:FIF


Goodman:2001:EER


Guerrero:2005:ECB


REFERENCES


REFERENCES

Giuliani:2001:GLI


Goldstone:2005:FCR


Golomb:2005:SDG


Gambino:2008:ITW


Goldwasser:2008:CAP


Gennaro:2003:LBE


Gonzales:2000:LBC


Gilbert:2001:SAR


Gilbert:2000:SAR


Gaudry:2006:ACM


Grabner:2005:ALC

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


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


 References


REFERENCES

Goldreich:2001:SKG

[GL01] Oded Goldreich and Yehuda Lindell. Session-key generation using human pass-
words only. In Kil-ian [Kil01a], pages 408–??, ISBN 3-540-42456-3 (paper-

Gennaro:2006:FPB

[GL03] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenti-

Garrett:2005:PKC

[GL05] Paul Garrett and Daniel Lieman, editors. Public-key cryptography: American Mathematical Society short course, January 13–14, 2003, Baltimore, Mary-
land, volume 62 of Proceedings of symposia in applied mathematics [AMS short course lecture notes].


Gennaro:2006:FPB

[GL06a] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenti-

Goshi:2006:ADM

[GL06b] Justin Goshi and Richard E. Ladner. Algorithms for dy-
namic multicast key distri-
bution. ACM Journal of Ex-
perimental Algorithmics, 11: 1.4:1–1.4:??, ???? 2006. CO-
DEN ??? ISSN 1084-6654.

Gassend:2004:IAI

[GLC+04] Blaise Gassend, Dainhy Lim, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. Identification and authen-
tication of integrated cir-
REFERENCES

Grembowski:2002:CAH

Gallant:2001:FPM

Gilbert:2000:CAR

Girault:2000:CCP

Gennaro:2002:CPG
[GM02a] Rosario Gennaro and Daniele Micciancio. Cryptanalysis

**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-

**Galbraith:2002:PKS**


**Gootts:2001:FEA**


**Golle:2008:DCS**


**Galbraith:2001:CNR**


**Galbraith:2001:RBU**


**Gentry:2005:PAK**

Craig Gentry, Philip MacKenzie, and Zulfikar Ramzan. Password authenticated key exchange using hidden smooth subgroups. In Meadows and Syverson [MS05b], pages
REFERENCES

Gallindo:2008:ICB


Gopalakrishnan:2001:PWV


Grosek:2001:SPK


Ge:2005:CCO


Gore:2001:CMT


Gratzer:2006:CLE

REFERENCES

**Gutmann:**2005:WHC

**Gaj:**2003:FME

**Goldreich:**1999:MCP

**Goldreich:**2001:FCBb

**Goldreich:**2001:FCBa

**Golic:**2001:CAS
REFERENCES

Golic:2001:MOS


Goldreich:2004:FCV

URL http://www.loc.gov/catdir/description/cam021/00049362.html; http://www.loc.gov/catdir/toc/cam023/00049362.html. See also volume 1 [Gol01b].

Golic:2003:DNP

CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42.

Goldstein:2008:BHO


Gonda:2006:NMR

CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_12_9/the_number_of_the.


REFERENCES


REFERENCES

Grossschadl:2001:HSR

Grossschadl:2003:ASL

Groth:2005:CS

Gisin:2002:QC

Gentry:2006:EES
REFERENCES

LCCN QA76 .S974 2006.

Gonzalez Vasco:2001:CPK

Garfinkel:2002:WSP

Gentry:2002:CRN

Geiselmann:2003:HSS
Geiselmann:2007:SPH


Goodell:2007:TOR


Grassl:2009:CAS


Guida:2004:DUP


Gaubatz:2008:SCD

G. Gaubatz, E. Savas, and B. Sunar. Sequential circuit design for embedded cryptographic applications resilient to adversarial faults. *IEEE


REFERENCES


Guttman:2004:ATD


Gutmann:20xx:ESR


Granger:2005:DLP


Gisin:2000:LCQ


**Guoxiang:2001:IFB**


**Gebotys:2008:EAW**


**Goldberg:2008:PQM**

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


**Heys:2000:SAC**


**Haddad:2000:AUA**


**Harvey:2000:EMA**


**Hare:2001:RUPa**

REREFERENCES


Hasan:2001:PAA


Hassler:2002:JCP


Haufler:2006:SWN


Hayat:2004:CSE

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

Hoglund:2006:RSW

Huffmire:2008:DSS

Hartel:2001:TMS

Holcomb:2009:PSS

Humphries:2002:IC

Huang:2004:NDE
Hwang:2004:NMP


Huang:2008:NCK


Han:2008:PBPa


Han:2008:PBPb


Henderson:2002:MTS


Halevi:2002:SSE


Han:2009:ICS

[Dong-Guk Han, Dooho Choi,

**He:2002:WSM**


**Hei:2001:DXS**


**Heikkila:2007:ESC**


**Hendry:2001:SCS**


**Henderson:2006:CBG**


**Henry:2006:TFA**


**Herzberg:2002:SX**

Herranz:2006:DIB


Herranz:2007:IBR


Heron:2009:AES


Hess:2004:SVE


Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA


Horvitz:2003:WKA


Horan:2005:NRN


Howgrave-Graham:2003:IDF

Howgrave-Graham:2003:HNP


Hendricks:2007:LOB


Handscharh:2004:SAC


Handscharh:2005:SAC

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


Higgins:2008:NSC


Hill:2000:KI


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

Huang:2005:ASE


Harris:2005:IUS


Kim:2000:RMW


Heuberger:2005:AGE

Clemens Heuberger, Rajendra Katti, Helmut Prodinger, and Xiaoyu Ruan. The alternating greedy expansion and applications to computing digit expansions from left-to-right in cryptography. Theoretical Computer Science, 341(1-3):55–72, September 5, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Handschuh:2001:ASE

[HKS00]
Thomas Hofmeister, Matthias Krause, and Hans U. Simon.

[Hiltgen:2006:SIB]

[HL03]

[Howard:2003:WSC]

[Hwang:2004:REL]

[Hohenberger:2005:HSO]
Hwang:2005:TAU


Hwang:2005:SHW


Hwang:2005:STH


Howard:2006:SDL


Hwang:2007:EPS


Hwang:2008:CPK

REFERENCES

Hwang:2000:CBV


Hong:2001:PSA


Han:2002:DMA


Hwang:2003:TRB


Hwang:2004:KAS


Hwang:2005:GTS

REFERENCES

Hong:2003:BBP

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

Herzog:2003:PAK


Hopper:2002:PSS


Hu:2009:TRN

CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).

Hwang:2001:TSB

REFERENCES


Hoglund:2004:ESH

Hollar:2005:EWS

Holenstein:2004:CCB

Hankerson:2004:GEC

Huang:2007:MPK

Haastad:2004:SAR
REFERENCES


REFERENCES

0558/papers/2074/20740801.pdf.


REFERENCES


REFERENCES


[Hawkes:2000:EMC]


[Hsiao:2004:FCP] 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 LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-
REFERENCES

Holenstein:2005:OWS


Halevi:2006:TCT


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

Halevy:2002:LBE


Han:2002:HEF


Hwang:2007:PEA


He:2005:MCP


Hong:2001:KIA

REFERENCES

Halderman:2008:LWRa


Halderman:2008:LWRb


Halderman:2009:LWR


Hanaoka:2002:USA


Hanaoka:2006:USA

REFERENCES


**Hernandez:2002:GCT**


**Hwang:2001:LCT**


**Hong:2002:PSR**


**Hong:2002:IDC**


**Hernandez:2001:DTR**

REFERENCES


Stephen Roderick Hines, Gary Tyson, and David Whalley. Addressing instruction fetch bottlenecks
by using an instruction
register file. ACM SIG-
PLAN Notices, 42(7):165–
174, July 2007. CODEN
SINODQ. ISSN 0362-1340
(print), 1523-2867 (print),
1558-1160 (electronic).

Hofheinz:2005:CTN

[Dennis Hofheinz and Do-
minique Unruh. Comparing
two notions of simulatibil-
ity. In Kilian [Kil05], pages
86–?? CODEN LNCD9.
ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
T44 2005. URL http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3378; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b106171.

Hughes:2002:LAA

[James Hughes. A linear alge-
braic attack on the AAFG1
braid group cryptosystem.
Lecture Notes in Computer
CODEN LNCD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/1
bibs/2384/23840176.htm;
http://link.springer-
ny.com/link/service/series/1
0558/papers/2384/23840176.
pdf.

Hughes:2004:ISE

[Jim Hughes. IEEE stan-
dard for encrypted stor-
age. Computer, 37(11):
110–??, November 2004.
CODEN CPTRB4. ISSN
0018-9162 (print), 1558-0814
(electronic). URL http:
//csdl.computer.org/dl/
mags/co/2004/11/ry110.
htm; http://csdl.computer.
org/dl/mags/co/2004/11/
ry110.pdf.

Huhnlein:2000:EIC

[Detlef Hühnlein. Efficient
implementation of cryptosys-
tems based on non-
maximal imaginary quadratic
orders. Lecture Notes in
Computer Science, 1758:
147–162, 2000. CODEN
LNCD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Hunt:2005:JFE

[K. Hunt. A Java framework
for experimentation with
steganography. SIGCSE
Bulletin (ACM Special Inter-
est Group on Computer Sci-
ence Education), 37(1):282–
286, 2005. CODEN SIGSD3.
ISSN 0097-8418.

Husemann:2001:SSC

[Dirk Husemann. Standards
in the smart card world.
Computer Networks (Ams-
derdam, Netherlands: 1999),
CODEN ???? ISSN
REFERENCES

Husemoller:2004:EC

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

Huth:2001:SCS

Hodjat:2004:HTP

Hallgren:2009:QC

Hopper:2009:PSS

Hardy:1998:ITN


REFERENCES

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


Hsu:2004:GOS


Harkins:2005:ESU


Hwang:2003:CAL


Yeh:2008:STB

REFERENCES

Hwang:2003:ASM


Han:2005:PJIb


Han:2005:PJI


Huang:2005:EMP


IBM-MARS-Team:2000:MAS

IEEE:2000:ASF


IEEE:2000:IPH


IEEE:2001:ISF


IEEE:2002:PAI

REFERENCES


IEEE:2004:PAI


IEEE:2005:PIS


IEEE:2005:AIS


IEEE:2006:AIS

IEEE:2007:PAI


IEEE:2008:PAI


IEEE:2009:ISI


Itoi:2001:SIS


[Ifrah:2000:UHN]

[Iglesias:2002:NSB]

[Bassham:2000:ETA]

[Itoh:2003:PCA]
REFERENCES

Iwata:2000:PAF


Iwata:2001:PAF


Impagliazzo:2003:LRA


Ichikawa:2000:HEA

Ishai:2003:EOT


Ishai:2005:SCC


Ishai:2006:CA


Ishai:2007:ZKS


Ishai:2008:CCC


Iyer:2007:TAA


Inamori:2002:SPB


Quatum computation and quantum cryptography.


Inamori:2002:SPT


Quatum computation and quantum cryptography.


Itkis:2001:FSS


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

Intel:2000:IIP


Intel:2003:IRN


Itkis:2002:SSB

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


Iwamoto:2006:SSR


Iwata:2002:NCP


Iwata:2003:NCP


Imai:2000:PKC


Judge:2002:WWM


Jablon:2001:PAU


Jacson:2000:SCQ


Jambunathan:2000:CCP


Janczewski:2000:IIS

REFERENCES

1993 / Gehan Gunasekara.


REFERENCES

Hagenberg, Austria. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-59593-904-0. LCCN ????.

Jennings:2009:SLL


Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


REFERENCES


References


Jallad:2002:ICC


Jarecki:2000:AST


Joux:2003:IGN

REFERENCES

http://www.ams.org/mcom/  
2003-72-242/S0025-5718-  
02-01482-5/S0025-5718-  [JLL02]  
02-01482-5.ps; http:/  
www.ams.org/mcom/2003-  
72-242/S0025-5718-02-01482-  
5/S0025-5718-02-01482-5.tex.

Juang:2004:FBT


Juang:2002:VMA


Jeong:2008:PKE


Juang:2001:FBT


Juang:2002:VMA


Johansson:2003:PCI

[Thomas Johansson and Subhamoy Maitra, editors. Progress in Cryptology—
Jakobsson:2007:DPD


Jing-mei:2005:CRB


Joux:2002:BAA


Johnson:2000:AFR

REFERENCES


REFERENCES


Jakobsson:2002:MAL


Jaulmes:2002:SHG


Joye:2003:GFA


Jakubowska:2007:MCT


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

**Jin:2001:WCS**  

**Jaworski:2009:RKP**  

**Jarecki:2005:FSP**  

**Jongkook:2001:NUS**  
REFERENCES


Pascal Junod. *Statistical cryptanalysis of block ciphers*. Thèses 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.


et al. [HYZ05b], pages 147–??, ISBN 981-270-153-2.


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


Kaliski:2001:RDS


Kayem:2008:RCK

Kanda:2001:PSE


Kapera:2005:MRP


Karski:2001:SSS


Katzenbeisser:2001:RAR


Katz:2005:CBR


Kendall:1939:TRS

Maurice G. (Maurice George)
REFERENCES


**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. Marname. Elliptic curve cryptography on FPGA for low-power applications. *ACM Transactions on Reconfigurable Technology and Sys-
REFERENCES


Kim:2007:SBE


Kim:2001:SAC


Ku:2003:WLL


Kang:2001:NHO


Kalker:2004:DWS

REFERENCES

Kurosawa:2004:NPH


King:2001:SAD


Kellar:2005:NRR

Sharon S. Kellar. NIST-Recommended Random Number Generator Based on
References


Kenyon:2002:DNR


Kenyon:2002:HPD


Kettani:2006:CBN


Kelsey:2000:CPL


Kiltz:2009:DCC


Katsikas:2004:PKI

Kaps:2007:CSD


Kovacic:2003:MHC


Kim:2005:SMA


Kato:2008:QSC


Khaw:2005:EDA


Komninos:2001:ESC

Kwon:2005:CLK


Koo:2009:SVN


Kirovski:2004:DWF


Kobara:2001:NCP


Kausar:2008:SEK

Kobara:2001:SSM


Kurosawa:2003:TTK


Kidwell:2000:SNC


Kida:2002:PGR


Kilian:2001:ACC


Kiltz:2001:TBC

E. Kiltz. A tool box of cryptographic functions related to the Diffie-Hellman function. Lecture Notes


REFERENCES

King:2000:IMP

King:2001:CMF

King:2002:RGI

Kirkby:2001:CCW

Kirtland:2001:INC

Montgomery:2003:FEC
Peter L. Montgomery Kirsten Kirsebom, Kristin Lauter. Fast elliptic curve arithmetic and improved Weil pairing.

Kocarev:2001:LMB


Kanade:2005:AVB


Krink:2005:IYA


Kim:2002:NIS


Klein:2003:FOW

REFERENCES


REFERENCES


Ko:2007:SRT

amp;idtype=cvips.

Klowski:2009:SGS


Kawachi:2005:UTQ


Kim:2009:SVN


Kaliski:2002:CHE

REFERENCES

Kelsey:2000:ABA

Kohno:2000:PCR

Kelsey:2001:ABA

Kim:2002:IDS
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
REFERENCES


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
REFERENCES


Klein:2007:BDC


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

Kim:2002:EPS


Kim:2003:IBP


Knudsen:2000:CRA


Knudsen:2001:CRR


Knudsen:2001:NPK

L. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds. In Schneier [Sch01d], page ?? CODEN LNCS-D9. ISBN 3-
REFERENCES

Knudsen:2001:CPL

Kanda:2002:SCA

Koblitz:2004:OTS

Koblitz:2004:SPK


REFERENCES


REFERENCES

openurl.asp?genre=issue&
issn=0302-9743&volume=
2688.

Kol:2008:GEI


Koc:2001:CHEb


Knu00a

Knudsen:2000:TT


Knudsen:2000:TTR


Knudsen:2002:ACE


Kruko:2005:FCR


Krukow:2005:FCR
Knutson:2007:BPS

Kushilevitz:2000:OWT

Komano:2003:EUP

Koblitz:2000:TQC
REFERENCES


REFERENCES

Koskinen:2001:NIK


Kovach:2001:BCB


Kovacich:2003:ISS

Gerald L. Kovacich. *The information systems security officer’s guide: establishing and managing

Katz:2009:ESA


Katzenbeisser:2000:IHT

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


Kaufman:2002:NSP


Kim:2004:TBG


Krishna:2003:BUP


Krawczyk:2001:OEA


Krause:2002:BBC


Krause:2002:USP

Rory Krause. Using SSH port forwarding to print at remote locations. *Linux Journal*, 94:60–62, 64, February 2002. CODEN LIJOFX. ISSN 1075-
REFERENCES


Kehr:2001:ISM


Kim:2005:CLL


Katz:2000:CCA


Kelsey:2000:MAP


Kuramitsu:2002:ETC

REFERENCES


REFERENCES

**Kasper:2009:FTA**


**Kelsey:2000:YND**

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


[CODEN ATISBQ] ISSN 1094-9224 (print), 1557-7406 (electronic).
**REFERENCES**


[KVN+09] Arun Kejariwal, Alexander V. Veidenbaum, Alexandru Nicolau, Milind Girkar, Xinmin Tian, and Hideki Saito. On the exploitation of
REFERENCES

424


[Koshiba:2000:SEP]


[KWDB06]


[Kwok:2003:WBC]


Karolof:2003:HMM


Kwon:2002:DSA


**Kwon:2003:EDS**


**Kumar:2006:ODS**


**Kamat:2009:TPW**


**Katz:2000:CCS**


REFERENCES

p245-katz/p245-katz.pdf;

ACM order number 508000.

Katz:2001:UEC


Kavut:2001:SCP


Kiayias:2001:PRB


Kurosawa:2001:LCI


Kil01a

Katz:2002:TCB

Katz:2002:TCB

Katz:2003:SPA

Kiayias:2002:CHB

Kamal:2009:FIN
A. A. Kamal and A. M. Youssef. An FPGA implementation of the NTRU-


[KZ09] 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

REFERENCES

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


Lu:2005:ND


Long:2005:DTC


Lu:2007:NPL


Lee:2001:SEK


Lee:2003:APS

REFERENCES

Levi:2004:UNC

Lee:2004:DEB

Lim:2009:OPG

Li:2008:CAM

Lu:2005:TUS

Lu:2005:PBM

Lu:2005:RTP
Rong Xing Lu, Zhen Fu Cao, and Hao Jin Zhu. A robust \((k,n) + 1\) threshold proxy signature scheme based on...

**Li:2001:CCB**


**Lai:2004:SGS**


**Lavoue:2007:SSW**


**Law:2006:SBB**


**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-
REFERENCES

Leroy:2002:BVJ


Levy:2001:CHC


Levy:2002:C


Lewand:2000:CM


Lee:2003:PKB


Liaw:2004:SPA

REFERENCES


Lin:2003:NRU


Lee:2004:SAA


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

John Linn. Trust models and management in public-key infrastructures. Technical report, RSA Data Security, Inc., Redwood City,
REFERENCES


Lin:2001:DWM

Lindell:2001:PCT

Lingmann:2002:DSK

Lindell:2003:SCC

Lin:2007:PFT

Lee:2005:IEC
B. K. Lee and L. K. John. Implications of executing compression and encryp-
REFERENCES

Licks:2005:GAI


Li:2005:AWP


Lee:2009:SAF


Lim:2001:SAW

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

Ludwig:2001:FSE


Lee:2008:SAF


REFERENCES


REFERENCES


[LL03]


[LL04a]


[LL04b]


[LL04c]


[LL05a]

Keon-Jik Lee and Byeong-
REFERENCES


bibs/2455/24550324.htm;
http://link.springer-
ny.com/link/service/series/1
0558/papers/2455/24550324.pdf.

Lee:2004:MPA

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

Li:2006:ESY


Lee:2005:IWR


Liu:2005:SWA

[LLS05b] 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–?? ISBN 981-270-153-2.


[Li:2009:ATN] Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the secu-

[LAMS05]


[LMP01] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and

Lu:2005:CCA


Li:2005:BPC


Liu:2004:MBA


Levieil:2008:CTC


Liu:2008:ARL


Lotspeich:2002:CFB


REFERENCES


Yee Wei Law, Marinuthu Palaniswami, Lodewijk Van Hoesel, Jeroen Doumen,

Lemke:2006:ESC


Lemke-Rust:2007:MAP


Li:2006:PMW


Li:2008:DEO


Lientz:2001:BTP


Lisko:2002:TBC

REFERENCES

Lenstra:2001:SFR


Lindemann:2001:ICT


Loidreau:2001:WKM


Li:2005:ULC


Liang:2005:FA


Liu:2008:GPV


Lopez:2007:SCB


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. ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743 (print), 1611-3349 (elec-
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3378; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b106171.

Lu:2002:HEA

Chi-Jen Lu. Hyper-encryption
against space-bounded ad-
versaries from on-line strong
extractors. In Yung [Yun02a].
pages 257–271. CODEN
LNCS9. ISBN 3-540-
44050-X (paperback). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
QA76.9.A25 C79 2002. URL
http://link.springer.de/
link/service/series/0558/
bibs/2442/24420257.htm;
http://link.springer.de/
link/service/series/0558/
papers/2442/24420257.pdf.

Lu:2007:NSC

HongQian Karen Lu. Net-
work smart card review and
analysis. Computer Net-
works (Amsterdam, Nether-
lands: 1999), 51(9):2234–
2248, June 20, 2007. CO-
DEN ???. ISSN 1389-1286 [Luc02b]
(print), 1872-7069 (elec-
tronic).

Lucks:2000:ASR

Stefan Lucks. Attacking
seven rounds of Rijndael un-
der 192-bit and 256-bit keys.
In NIST [NIS00], pages 215–
gov/encryption/aes/round2/
conf3/aes3conf.htm; http://
csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-1.pdf;
http://csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-2.pdf;
http://csrc.nist.gov/encryption/aes/round2/
conf3/papers/AES3Proceedings-3.pdf;
http://csrc.nist.gov/encryption/

Lucks:2002:SAB

Stefan Lucks. The saturation
attack — A bait for Twofish.
Lecture Notes in Computer
Science, 2355:1–??, 2002.
CODEN LNCS9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/2355/23550001.htm;
http://link.springer-
ny.com/link/service/series/0558/papers/2355/23550001.
pdf.

Lucks:2002:VCS

Stefan Lucks. A vari-
ant of the Cramer-Shoup
cryptosystem for groups
Lucas:2006:PGE


Ludvig:2005:PWF


Lukyanov:2001:PFA

Lenstra:2000:XPK


Lu:2004:FCA


Laguillaumie:2007:MDV


Lange:2002:PIE


Lee:2004:IAK

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

Li:2005:AAU

Li:2007:NBA

Lou:2002:ESA

Liu:2007:IFW
REFERENCES

[465]

Lysyanskaya:2002:USV


Lysyanskaya:2007:AI


Lysyanskaya:2008:CHK


Leung:2001:WDI


Li:2004:CAB


Lao:2009:ORA

REFERENCES

Li:2001:GOT


Li:2004:WMS


Michener:2000:MSA


Masuda:2002:CDC


Maurer:2007:ICP


Mrayati:2003:AKT

M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. Al-Kindi’s treatise on cryptanalysis, volume 1 of Arabic origins of cryptography. KFCRIS & KACST,
REFERENCES


MacKenzie:2001:MEP


Moha: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-
Manger:2001:CCA


Mao:2004:MCT


Mann:2008:HHS

Martinelli:2002:SSA


Mares:2005:BRA


Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI


Martin:2008:IBE


Mastroeni:2004:APA

REFERENCES

[Matsui:2002:FSE]

[Maurer:2001:C]

[Maurer:2004:RCD]

[Maughan:2005:HSC]

[Maximov:2006:SWC]

[Mayers:2001:USQ]

[May:2002:CUR]
REFERENCES


[MC04] Gabriel Montenegro and Claude Castelluccia. Crypto-based identifiers (CBIDs): Concepts and applications. ACM Transactions on Infor-
REFERENCES

McAndrew:2008:TCO

McGraw:2006:SSB

Myles:2005:ETS

McLaughlin:2006:PZW

McNichol:2003:HTM

Martin:2004:AMC
Macchetti:2005:QPH


McCaman:2008:QIF


Monteiro:2008:AVM


Meadows:2001:OIF


Meadows:2004:OSM


Mehrabi:2001:DW


Mena:2003:IDM

REFERENCES


Menezes:2005:TCC


Menezes:2007:ACC


Messerges:2000:SAF


Messerges:2001:SAF

REFERENCES

McGrew:2001:AAE

Marti-Farre:2007:NSS

Matula:2005:TLS

Mueller:2006:SMG

Müller: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


[Mis08] Jelena Mišić. Traffic and energy consumption of an IEEE 802.15.4 network in the presence of authenticated, ECC Diffie–Hellman ephemeral key exchange.
REFERENCES


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

McDonald:2008:SID


Malone-Lee:2003:TBO


McGregor:2005:PCK


Maitra:2001:SDD


McLoone:2001:HPS

McLoone:2001:SCF


Moldovyan:2007:IC


Mullen:2007:FFA


Moreira:2002:RCE

REFERENCES


//link.springer-ny.com/
link/service/series/0558/]
bibs/2438/24380770.htm;
http://link.springer-ny.com/link/service/series/]
0558/papers/2438/24380770.pdf.


REFERENCES


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


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

REFERENCES

Mangard:2006:PAA

Morris:2003:KKL

Moritz:2005:KAE

Moses:2006:DSD

Merton:2000:NBG

McMillan:2001:JIA
REFERENCES


<table>
<thead>
<tr>
<th>References</th>
<th>Title</th>
<th>Authors</th>
<th>Publication Details</th>
</tr>
</thead>
</table>
REFERENCES

Micali:2005:OEC

Monrose:2000:KDB

MacKenzie:2001:TPG

Micali:2001:MRR

Micali:2001:SPK
Silvio Micali and Leonid Reyzin. Soundness in the public-key model. In Kilian [Kil01a], pages 542–??
REFERENCES


Murphy:2002:EASa


Murphy:2002:EASb


Micciancio:2009:LBC


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


REFERENCES


uiarchive.cso.uiuc.edu/ 
pub/etext/gutenberg/; [102x681] [177x646] [177x634] [177x622] [177x610] [177x598] [177x586] [177x574] [182x562] [189x534] [308x550] [199x504] [290x504] [102x486] [311x486] [386x489] [386x477] 496 
http://www.loc.gov/catdir/bios/mh051/2004351501. 


REFERENCES

**Muzereau:2004:EBD**

**Marsaglia:2002:SDP**

**Meseguer:2007:SRA**

**Ma:2009:NAS**

**Muller:2001:SWB**

**Muller:2001:SIC**
REFERENCES


REFERENCES


Alison McCook, Philip Yam,

**Morelos-Zaragoza:2002:AEC**


**Nagy:2007:AQK**


**Naik:2003:DSW**


Naor:2003:CA


Naor:2004:TCF


NIST:2000:FPD


Nazario:2002:RYS


Nieto:2001:PKC

Juan Manuel González Nieto, Colin Boyd, and

Nghiem:2009:FBI


Ning:2004:TTA


Nedjah:2005:SHC


Nash:2001:PIM


Nedjah:2004:ECH


Nedjah:2006:NTC

Nadia Nedjah and Luiza de Macedo Mourelle, edi-

Netscape:2004:HSW


Neuenschwander:2004:PSM


Neve:2003:STF


Nguyen:2001:TFLb


Nguyen:2005:RBP

Minh-Huyen Nguyen. The relationship between password-authenticated key exchange


[Nis03a] E. Nisley. Ed looks at the history of cryptography and

**NIST:2003:RKE**


**Naga:2006:OQE**


**Ning:2008:MAA**


**Nigrini:2009:DDU**


**Nagao:2005:UCS**


**Nozaki:2001:IRA**

[NMSK01] H. Nozaki, M. Motoyama, A. Shimbo, and S. Kawamura. Implementation of


Jorge Nakahara, Jr., Bart Preneel, and Joos Vandewalle. Linear cryptanal-

**Naor:2004:NTC**


**Nichols:2000:DYD**


**Neraud:2001:CFD**


**Nguyen:2001:ISA**


**Nguyen:2001:TFLa**

REFERENCES


REFERENCES


REFERENCES

259–269, June 2009. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

**Okamoto:2000:ACA**


**Okamoto:2004:TCC**


**Ohzahata:2002:FAM**


**Ogata:2006:OSS**


**Olson:2000:SCT**

Adam Olson. Scaring crackers away with TCP wrapper.
REFERENCES

Ohigashi:2009:PMF

Ohkuma:2001:BCH

Ohbuchi:2002:FDA

Onions:2001:SSI

Ors:2003:PAA
REFERENCES

openurl.asp?genre=issue&
issn=0302-9743&volume=
2779; http://www.springerlink.
com/openurl.asp?genre=
volume&dois=doi:10.1007/
b13240.

Okamoto:2001:GPN

Tatsuaki Okamoto and
David Pointcheval. The gap-
problems: A new class of
problems for the security
of cryptographic schemes.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1992/19920104.htm;
http://link.springer-
ny.com/link/service/series/

Okamoto:2001:RRE

Tatsuaki Okamoto and
David Pointcheval. REACT:
rapid enhanced-security asym-
metric cryptosystem trans-
form. Lecture Notes in
Computer Science, 2020:
159–175, 2001. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Oppliger:2001:SMP

Rolf Oppliger. Secure
messaging with PGP and
S/MIME. Artech House
computer security series.
Artech House Inc., Norwood,
MA, USA, 2001. ISBN 1-
58053-161-X. xxiii + 305
pp. LCCN TK5102.85 .067
artechhouse.com/Detail.
asp?strIsbn=978-1-58053-
161-0.

Oppliger:2005:CC

Rolf Oppliger. Contempo-
rary cryptography. Artech
House computer security se-
ries. Artech House Inc., Nor-
wood, MA, USA, 2005. ISBN
1-58053-642-5. xxv + 503
pp. LCCN Z103 .066
artechhouse.com/Detail.
asp?strIsbn=978-1-58053-
642-4.

Ortiz:2000:ITW

Sixto Ortiz Jr. Industry
trends: Will PKI become
a key to online security?
Computer, 33
CODEN CPTRB4. ISSN
0018-9162 (print), 1558-0814
(electronic). URL http://
dlib.computer.org/co/
books/co2000/pdf/rz013.
pdf.

Okeya:2000:PAB

Katsuyuki Okeya and Kouichi
Sakurai. Power analysis
breaks elliptic curve
cryptosystems even secure
against the timing attack.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
REFERENCES


Raphael Overbeck and Nicolas Sendrier. Code-based cryptography. In Bernstein et al. [BBD09], pages 95–146. ISBN 3-540-88701-6 (hard-
REFERENCES

Okeya:2004:SBR


Osvik:2005:CA


Osvik:2000:SS


Okeya:2003:MFC


Raphael Overbeck. Extending Gibson’s attacks on the GPT crypotosystem. In Ytrehus [Ytr06], pages 178–188.
REFERENCES


Rafael Pass. On deniability in the common ref-

Pass:2005:UCN


Patiyoot:2002:MSE


Patiyoot:2002:SIW


Patarin:2003:LRR

REFERENCES


REFERENCES

January 2005. CODEN ???.
ISSN 0219-4678.


REFERENCES


Poulos:2008:TSE


Pucheral:2001:PSD


Petrie:2000:NBI


Peikari:2004:SW


Park:2005:ISC


Jung Min Park, Edwin K. P.

Pan:2007:IBS


Peeters:2007:CES


Petrakos:2009:CTA


Peinado:2004:CLK


Peikert:2009:PKC


Pelzl:2006:PAC


Pemble:2001:CEW


REFERENCES

Pfitzmann:2001:ACE


Phatak:2005:FMR


Phan:2004:IDC


Paeng:2001:NPK

Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seong-taek Chee, and Choonsik Park. New public key cryptosystem using finite non Abelian groups. In Kil-

Polk:2003:IIC


Phoha:2001:SDI


Pieprzyk:2003:FCS


Pathak:2006:BFT


Pietrzak:2005:CDI


Pinkas:2002:CTP

[Benny Pinkas. Cryptographic techniques for privacy-preserving data mining. ACM SIGKDD Explor-
REFERENCES

Pinkas:2003:CTP

Pincock:2006:CHC

Pecho:2009:APW

Park:2001:ND

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 for mobile communication.
REFERENCES


Pliam:2001:PTU


Pon:2005:OPK


Pfleeger:2007:IBC


Paulson:2000:NBU

Piper:2002:CVS


Pang:2008:AQR


Pohlmann:2001:SCA


Pointcheval:2000:CCS


Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP

REFERENCES


REFERENCES


Popp:2006:CTT


Pfleeger:2007:SC


Paar:2009:UCT


Pellikaan:1996:AGC


Pereira:2003:SAU


Piret:2003:DFA

Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In Walter et al. [WKP03], pages 77–88. CODEN LNCS-D9. ISBN 3-540-40833-9. ISSN
Pereira:2006:IBS


Pass:2005:NIC


Pass:2008:NIC


Preneel:2000:ACE


Preneel:2001:NES

Bart Preneel. New European Schemes for Signature,
Integrity and Encryption (NESSIE): a status report. 
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:
//link.springer-ny.com/link/service/series/0558/[Pre02c]

**Preneel:2002:NEA**

//link.springer-ny.com/link/service/series/0558/[Pre02c]

**Preneel:2002:NPT**


**Preneel:2002:TCC**


**Preneel:2007:SRD**


Birgit Pfitzmann and Ahmad-Reza Sadeghi. Self-escrowed cash against user blackmailing. *Lecture Notes in
REFERENCES


Pucella:2006:SAC


Pucella:2007:IB


Puzmanova:2004:RWF


Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI

Deborah M. Phillips and Hans A. von Spakovsky. Gauging the risks of Internet elections. Communications of the Association for Computing Machinery, 44(1):73, January 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-
REFERENCES


Pang:2005:NMS


Peikert:2008:LTF


Pelzl:2003:HCC


Patrick:2005:FCD


Paterson:2006:LTT


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

**Qian:2005:SPL**


**Qian:2005:SPL**


**Quisquater:2000:SCR**


**Quisquater:2002:CTM**


**Quisquater:2002:CTM**

REFERENCES


REFERENCES


REFERENCES


proxy certificates. Lecture Notes in Computer Science, 2033:206–??, 2001. [RE03]


[Reg05] Oded Regev. On lattices, learning with errors, random

Regev:2009:LLE


Rescorla:2001:IOPa


Rescorla:2001:IOPb


Reynard:2001:SCB


Ringenburg:2005:PFS


Ren:2009:FCS


Rose:2006:CSP


Rojas:2000:FCH

[RH02] Timothy Roscoe and Steven Hand. Transaction-based 
charging in mnemosyne: a peer-to-peer steganographic 
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://
/link.springer.de/link/service/series/0558/bibs/2376/23760335.htm; http://
/link.springer.de/link/service/series/0558/papers/2376/23760335.pdf.

[RH03] Sandro Rafaeli and David Hutchison. A survey of 
key management for secure group communication. ACM 
CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

[Rhi03] Jason P. Rhinelander. Design and implementation of encryption algorithms 
in a coarse grain reconfigurable environment. Thesis (M. Eng.), Memorial 
University of Newfoundland, St. Johns, Newfoundland, Canada, 2003.

Rich:2007:ATS

Donald Rich. Authentication in transient storage device attachments. Computer, 

Rila:2002:DAB

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://
/link.springer.de/link/service/series/0558/bibs/2437/24370019.htm; http://
/link.springer.de/link/service/series/0558/papers/2437/24370019.pdf.

Risen:2006:SWS

7066-5. 240 pp. LCCN ????

Rivest:2003:TLE

REFERENCES

[553] Renner:2005:UCP

[RK06] Ruan:2006:NSC


[RM02] Riedl:2002:FSH

Bimal Roy and Willi Meier, editors. Fast Software Encryption: 11th International Workshop, FSE 2004: Delhi, India, February 5--7, 2004: Revised Papers, volume 3017 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Ger-
REFERENCES


Ruiz:2000:SPS

Reyhani-Masoleh:2003:LCS

Reyhani-Masoleh:2003:LCB

Reyhani-Masoleh:2004:TFT

Rahaman:2008:CTB
H. Rahaman, J. Mathew,


[RMS05] Ryabko:2005:NTA


[RN00a] Ryutov:2000:RESa


[RN00b] Ryutov:2000:RESb


[Ros00] Rosen:2000:NRC

REFERENCES


[Rot03] Jörg Rothe. Some facets of complexity theory and cryptography: a five-lecture
REFERENCES


Rieffel:2000:IQC


Ramzan:2000:RSS


Reyzin:2002:BTB


Ratner:2003:NGI


Ratner:2003:NHS


Rosenberg:2004:SWS

REFERENCES


**Rittinghouse:2005:IIM**


**Rechberger:2008:NRN**


**Rechberger:2006:NCW**


**Rivest:2000:RA**


**Rosenbaum:2000:SFR**


Rubin:2002:SAV


Rubin:2003:TBC


Riley:2004:HAE


Rao:2005:CHE


[RS01] RSA Laboratories. PKCS #11 v2.11: Cryptographic Token Interface Standard. RSA Data Security, Inc.,
REFERENCES


Rivest:2003:TAL


Rousseau:2009:MT


Rukhin:2001:STS

Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David


Rubin:2000:KVL


Rubin:2001:SCR


Rugg:2004:CMV


Rupp:2009:CAC


Raghavan:2009:SPC


Russell:2002:HFU


Renner:2003:NBS

REFERENCES


[Sak01] Ken Sakamura. Guest editor’s introduction: Radio frequency identification

**Sal01b**


**Sale:2000:CBP**


**Sale:2001:GRT**


**Sal00a**


**Sal00b**


**Sal01a**

Sale:2005:RCB

Sallee:2005:MBM

Salomon:2005:CDC

Salomon:2005:FCS

Salomon:2007:DCC

Sale:20xx:CRP


Soto:2000:RTA


Shacham:2001:ISH


Scott:2004:CP


Stoklosa:2005:CIC


Stallings:2007:CSP


Sherwood:2005:MTR

REFERENCES


REFERENCES

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


REFERENCES


Bruce Schneier. *Secrets and Lies: Digital Security in a...*
REFERENCES


Schneier:2000:SRF


Scharinger:2001:ASK


Schmalz:2001:MDI


Schneier:2001:FSE


Schindler:2001:TAA


Schnorr:2001:SGH


Schnorr:2001:SDE


Schneier:2003:BFT


Schmalz:2004:MDIa


Schmalz:2004:MDIb


Schneier:2004:SA

Bruce Schneier. Sensible authentication. ACM


Schneier:2008:SS

Schmeh:2009:VBF

Su:2005:IBT

Scott:2004:CIB

Screamer:2001:MDR

Shen:2005:NCB

Sun:2005:CCL
Sun:2005:RNK

Sebe:2001:OIW

Sebe:2000:SDI

Smith:2006:CNS

Smith:2001:ADB

Spiekermann:2009:ACR
Seacord:2005:SCC

Seacord:2009:CCS

Seetharaman:2004:BRB

Smith:2006:SID

Seifried:2000:C

Seifried:2000:PPA

Seifert:2005:ACR
REFERENCES


[Sem00] Michael Semanko. L-collision attacks against randomized MACs. In Beller [Bel00], pages 216–?

[SETB08] Iain Sutherland, Jon Evans, Theodore Tryfonas, and Andrew Blyth. Acquiring volatile operating system data tools and techniques. Operating Systems Review,
Shumow:2007:PBD


Simka:2006:MTR


Sakr:2007:RRC


Sutton:2007:FBF


Steinwandt:2001:TDB

0558/papers/2200/22000280.pdf.

**Steinwandt:2000:WHS**


**Steinwandt:2008:GEI**


**Sauvage:2009:ERF**


**Storer:2009:PSR**


**Stone:1998:PCC**


**Sonntag:2000:MAS**

Michael Sonntag and Rudolf Hörmanseder. Mobile agent security based on payment.
REFERENCES


Shirase:2005:AEC

Shailer:2001:PMT

Shamir:2001:NDC

Shamir:2001:PSC

Shao:2001:BVM

Sharp:2001:IKB
REFERENCES


URL http://www.acm.org/turingawardlecture/RSA/


[Sha04b] Zuhua Shao. Improvement of digital signature with


Shao:2005:CXY


Shao:2005:IEP


Shao:2005:NKA


Shao:2005:SMD


Shepherd:2001:CDC


Sung:2007:CIB


Shim:2005:LPG

REFERENCES

Shih:2008:DWS

Sierra:2004:LCC

Shimizu:2007:CBE

Shoup:2000:CTU

Shoup:2000:UHF

Shoup:2001:OR
Victor Shoup. OAEP reconsidered. In Kilian
REFERENCES


Shoup:2005:ACC


Shoup:2005:CIN


Shparlinski:1999:NTM


Shparlinski:2001:UDR

Shparlinski:2002:SMS
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shparlinski:2003:CAA

Shparlinski:2004:BRR

Shparlinski:2004:UDD
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Shparlinski:2005:PHS

Sun:2005:SSP
REFERENCES

Shamba:2006:THL


Shyamasundar:2002:ACP


Silberman:2005:ECC


Simon:2002:CRE


Singh:1999:CBE

Simon Singh. The code book: the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography. Doubleday, New York, NY, USA,
References


**Singh:2000:CBE**


**Singh:2001:DPK**


**Sinkov:2009:ECM**


**Stubblefield:2004:KRA**


**Sivonen:2006:MPF**

Timo Sivonen. Measurement...


[SK01b] T. Stojanovski and L. Ko-
REFERENCES


[Sklavos:2005:ISH]

[Stavrou:2005:CAS]

[Stabell-Kulo:2006:ESC]

[Saldamli:2007:SME]

[Shu:2009:RCA]

[Sugita:2001:SRV]

Sano:2000:PEA

Srinathan:2002:ASC

Sugita:2000:RAD
REFERENCES


Schneier:2000:CTA  [SKW+00]


Scharwaechter:2007:AAE  [SKW+07]


Sterbenz:2000:PAC  [SL00]


Shim:2005:SFA  [SL05a]

Kyungah Shim and Young-
REFERENCES


Srivatsa:2005:SPS


Skoudis:2006:CHR


Stamp:2007:ACB


Sun:2009:CPR


Su:2005:KPK


Shi:2005:HEC


REFERENCES

Sebag-Montefiore:2000:EBC


Sarkar:2003:EIC


Satoh:2002:SHS


Satoh:2003:UHA

REFERENCES


Sebag-Montefiore:2005:EBC


Sebag-Montefiore:2007:EBC


Simos:2007:CMS


Smith-Miles:2008:CDP


Smart:2001:CDF


Smart:2003:ACU

[NPS03a] Nigel P. Smart. Access control using pairing based cryptography. In Joye [Joy03b], pages 111–121. CODEN LNCS9D. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25...


REFERENCES

599


REFERENCES


REFERENCES


Akashi Satoh, Nobuyuki Ooba, Kohji Takano, and


REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-n...[SR00]

Shin:2000:ANT


Sanchez-Reillo:2001:IBA


StDenis:2006:BMI


Stipcevic:2007:QRN


Samarati:2001:AMP


Standaert:2003:EIR

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

[Sarkar:2001:PAE]

[SS01a]

Stubblebine:2001:AAF

[Sarkar:2001:PAE]

Seznec:2003:HUL

[SS01a]

Swiderski:2004:TM

[Sedick:2009:IWB]
Hassen Seddik, Mounir Sayadi, Farhat Fnaiech, and Mohamed Cheriet. Image watermarking based on the Hessenberg transform. In-
Shi:2008:UAU


[SSM+08]

Susilo:2000:NEF


[SSNGS00]

Scambray:2006:HEW


Schmidt-Samoa:2006:AFW


[SSST06]

StPierre:2000:TFA


[St.00]

Sakurai:2001:NSS

Shamir:2001:IOO


Stern:2001:ADW


Stinson:2001:SAC


Sakurai:2002:SMP

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

Steil:2005:MMM


Stern:2005:MLF


Stein:2008:ENT


Stinson:2001:C


Stinson:2002:CTP


Stieber:2006:OH


Stieber:2006:GH

REFERENCES

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

Stinson:2006:CTP

Shimoyama:2002:MLC

Struif:2001:UBU

Strunk:2001:JQJ

Strubinger:2002:HBS

[Sti06c]

[Str01a]

[Str01b]


REFERENCES


REFERENCES

Schneier:2000:PCF


Sun:2000:AFA


Shim:2005:WIB


Swaine:2001:PPSa


Swenson:2008:MCT


Song:2005:ISG

REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>

Syed:2000:CLA


Sun:2005:CSS


Syverson:2002:FCI


Shimoyama:2002:BCS


REFERENCES


Tao:2000:ITF


Tsai:2001:GSI


Tsaur:2005:EAS


Tsai:2002:SMS


Trudel:2003:DSE


Teepe:2006:PPA

REFERENCES


REFERENCES


REFERENCES


Tang:2006:CHA


Tian:2005:RWS


Tosilis:2009:ARM


Tousidou:2000:IMS


Tanaka:2001:QPK


Tochikubo:2000:RAE

Tomaszewski:2006:YSY


Topham:2002:BRJ


Totsch:2000:MSS


Tague:2007:CSA


Trope:2007:CSD


Trimberger:2001:GED


Troutman:2009:CCGa

Justin Troutman and Vincent Rijmen. Crypto corner: Green cryptography:

[Troutman:2009:CCGb]


[Troutman:2008:VMM]


[Tsaur:2001:FUA]


[Tseng:2007:SA]

Yuh-Min Tseng. A secure authenticated group key agreement protocol for resource-

Takano:2000:PTH

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

Tsunoo:2003:CIC


Tzeng:2001:PKT


Tian:2001:ICE

REFERENCES

**Tuchman:1966:ZT**


**Turing:2004:BS**


**Toft:2001:LTT**


**Trappe:2002:ICC**

REFERENCES


Tzeng:2004:NTM


Ting:2002:FBS


Tyanan:2005:CPA


Tian:2005:NDF


Tong:2009:RAPa

REFERENCES

Tong:2009:RAPb


Uz:2009:MBT


Unay:2008:SQE


Uchida:2009:FPR


USC:2000:HRS

REFERENCES


REFERENCES

USHCJ:2000:SFT


USPTO:2001:CCP


Uhl:2005:IVE


Urban:2001:MWB


Urien:2001:PIS


USENIX:2000:PLI

REFERENCES

proceedings/lisa-nt2000/.  

USENIX:2000:PFW


USENIX:2000:PFSa


USENIX:2000:PNU


USENIX:2001:PUA


USENIX:2001:PFT


USENIX:2001:PTU

REFERENCES


USENIX:2002:PBF


USENIX:2002:PUS


USENIX:2002:PFT


USENIX:2002:PBF


USENIX:2002:PUS


USENIX:2002:PFT


Utami:2002:FID


Urien:2001:XS


Ustimenko:2001:CGT

Ulfving:2000:GS


Uzn:2004:BRC


[Vav03] D. D. Vavriv. Random number generators on the basis of systems with chaotic


REFERENCES


REFERENCES


pp. LCCN QA76.73.C15 V53 2003.

**Viega:2002:NSO**


**Vasco:2005:NCS**


**Vaughan-Nichols:2004:VAS**


**Voice:2005:OAM**


**vanOorschot:2008:PMU**


**vanOorschot:2007:IRS**


[WA06] James A. Whittaker and Mike Andrews. *How to break Web software: func-

Woody:2007:COS


Weitzner:2008:IA


Wachsmann:2005:CAK


Wallach:2000:SSM


Wagner:2000:CYL


Wagner:2002:GBP

REFERENCES


REFERENCES


REFERENCES

Wu:2003:HDW


Wu:2004:EIW


Wang:2005:TAP


Wang:2009:NWA


Wang:2005:SDR


Westerlund:2001:HWK


Williams:2001:ICA

REFERENCES

Wang:2009:SST


Weaver:2006:BA


Weber:2002:ECH


Weierud:2000:SFB


Weiss:2004:JCE


Weiss:2004:JCE

REFERENCES

Weierud:2005:BSF


Weierud:2005:BPS


Welschenbach:2005:CCC


Wernsdorf:2002:RFR


Weng:2003:CHC


Westfeld:2001:FSA

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Withers:2001:IWU


Wang:2007:VBW


Welschenbach:2001:CCC


Wang:2005:ECSb


Won:2006:ISC


Weigold:2008:RCA

REFERENCES


REFERENCES


Wen:2005:TRB


Wang:2009:DSM


Wang:2005:SAI


Wu:2005:IAW


Wong:2004:RCK


Wang:2005:TSP

REFERENCES

Wu:2008:RWM


Watters:2008:VDL


Wetterstorfer:2001:AIA

[WOL01] Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger. An ASIC implementation of the AES SBoxes. *Lecture Notes in
REFERENCES


[Wol04]


[WPP05] T. Wollinger, J. Pelzl, and C. Paar. Cantor versus Harley: optimization and


**Weimerskirch:2001:ECC**


**Wang:2001:TUR**


**Wright:2000:IQC**


**Wright:2001:AES**


**Wright:2003:FCI**


André Weimerskirch and Gilles Thonet. A distributed


David P. Woodruff and Marten van Dijk. Cryp-
REFERENCES

663

Weaver:2000:CAC


Wang:2004:CWS


Wolf:2005:NML


Wang:2006:SPS


Wang:2008:DCP

Xing-Yuan Wang and Xiao-Juan Wang. Design of

**Wu:2001:CFF**


**Worley:2000:AFP**


**Wollinger:2000:HWH**


**Wincelberg:2002:LIE**

David Wincelberg, Sy Wong, Dan Leach, Paul Keister, and Robert Masta. Letters: Inside eBook security; numerical weather forecasting; FrontPage EULA; prior-

[Wang:2008:HQS]

[WY02]

[Wu:2005:CTR]

[Wyan:2002:APK]

[Wyler:2005:ANS]
REFERENCES


[Wang:2005:FCFa]

[Wang:2005:FCFb]

[Wang:2005:DIC]

[Xu:2001:EIE]
Sheng-Bo Xu and Lejla Batina. Efficient implementation of elliptic curve cryptosystems on an ARM7 with hardware accelerator. Lecture Notes in Computer
Xiao:2003:HPC

Xiao:2005:SPA

Xenakis:2006:GCO
Xu:2007:CAD


Xu:2005:ADR


Xie:2007:ISP


Xu:2003:TEP


Xie:2004:CTA


Xu:2009:AVB


Yan:2000:NTC

S. Y. Yan. *Number The-


Yiu:2008:ODC


Yang:2009:ETP


Yang:2009:CGA


Yang:2004:MSS


Yu:2007:NSM


Yang:2008:NFD

Yang:2007:IIS


Yung:2006:PKC


Yekhanin:2007:LDC


Yan:2006:ICP


Youssef:2001:CIM


Youssef:2001:IAB

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

**Youssef:2001:CPK**


**Yang:2005:IME**


**Yamamura:2000:QCB**


**Yang:2005:EDA**


**Yi:2004:AKA**

Yen:2000:CBO


Yen:2002:CAO


Yen:2002:RSR


Yardi:2008:HAC


Yamamoto:2001:PKB

[Hideo Yamamoto, Tetsutaro Kobayashi, Masahiro...

[YLH05]

Yu:2001:TCB


[YLLL02]

[YLH05]

Yu:2001:TCB


[YLH05]

Yu:2005:EHI

[YLH05]


[YLH05]

Yu:2005:EHI


[YLH05]

Yoo:2002:LAU

REFERENCES


REFERENCES

Yilek:2009:WPK


Yoon:2004:SUA


Yoon:2005:ICJ


Yoon:2005:IFA


Yeh:2002:SAK

REFERENCES


[Yeh:2004:PBU]


[Yanami:2002:DLC]


[Yang:2001:EEA]


[Yoshiura:2001:AWB]


[Yeh:2004:PBU]


[YSH03]
Yao:2009:CAR


Yang:2004:ENT


Ytrehus:2006:CCI


Yang:2005:SEA


Yung:2002:ACC


Yung:2002:CI


Yang:2005:CIA


Yang:2004:ISE


Yang:2008:VCS


Yen:2006:SED


Yang:2005:IYS


Yang:2004:ISE


Yang:2008:VCS


**REFERENCES**

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

**Yoon:2005:SWL**


**Ye:2001:ATD**


**Yen:2000:WOW**


**Ye:2007:NAW**


**You:2001:GEC**


**Youssef:2009:IEU**

M. I. Youssef, M. Zahara,
&arnumber=5233974.

Zafar:2000:ACB


Zane:2001:EWD


Zhao:2005:SSV

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

Zhang:2000:MCA

Muxiang Zhang and Agnes Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. In Bellare [Beh00], pages 501–?? ISBN 3-540-67907-3. ISSN 0302-9743

Zhang:2005:ITA


Zivkovic:2005:AAH

Zhang:2004:AIB

Zhang:2005:CHC

Zhang:2009:CII

Zhang:2001:SOS

Zhou:2005:PSP

Zunino:2005:WPE
REFERENCES

Zhao:2006:SAP

Zeadally:2000:IPQ

Zhang:2005:CSS

Zhen:2004:IBS

Zhang:2005:AES

Zou:2005:MED

Zhang:2000:WMH
Peter Zhang. Webrelay: A multithreaded HTTP relay

Zhao:2006:NDN


Zhang:2008:CLR


Zheng:2000:ISS


Zheng:2002:NPK


Zheng:2002:ACA

Zhou:2002:MVD


Zhong:2006:ESC


Zirkind:2007:ADC


Zhang:2004:BAF


Zhang:2009:IBR

Jianhong Zhang and Cheng Ji. An id-based and repairing NTRUSign-based anonymous multi-proxy signature scheme. In IEEE, editor, Proceedings of the International Conference on Com-
REFERENCES


REFERENCES

Zhang:2004:RMA


Zhao:2005:MCE


Zhang:2001:QKD


Zhang:2002:CRD


Zhang:1999:AFV


Zheng:2007:SRI


Zolman:2001:SEM

REFERENCES

CODEN CCUJEX. ISSN 1075-2838.

Zhang:2001:CIS


Zhang:2005:DMC


Zhou:2005:MBI


Zhu:2007:IHH


Zhang:2005:RPE


Zhao:2005:APA


Zhou:2005:APS

Lidong Zhou, Fred B. Schneider, and Robbert Van Renesse. APSS: proactive secret sharing in asynchronous systems. ACM
REFERENCES


Zhang:2001:ASE


Zhang:2003:FSP


Zafeiriou:2005:BRW


Zhang:2005:ISS


Zhang:2005:SCA


Zhao:2002:EI

Xianfeng Zhao, Weinong Wang, and Kefei Chen. Ex-


REFERENCES


Zhang:2005:ASP


Zhang:2005:ISM


Zhang:2008:FIC


Zeng:2001:CHR


Zhu:2007:EIB