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]. (pk)

[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LZZ01, YCH04, CLT07]. (tn)

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

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

[And04]. 128 [AIK+01, PCG01]. 13

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

[BD00b]. $35.00 [Top02]. $49.99 [Gum04]. $5

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

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

0 [AIK04]. ABC [PS04b]. d [BD00b]. E0

[FL01a]. f8 [KSH01]. g(x) [Shp02]. gε(x, 1)

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

[OTIT01, RMP08]. GF(pm) [BGK+03].

[FL06]. GF(p) [PZ01]. H2A [CBB05]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. l

[QPV05]. M + 1 [AS01a]. F4 [CY02]. Zn

[Gro05]. GF(2) [GS03, KTT07]. GF(2m)

[BBG08, KTT07, QPV05, RMH03a, RS04].

[KKH03]. SL2(F2n) [SGGB00]. μ

[LN04]. n

[CT08b, Gon06, HKS00, LKJL01, TM01]. Nn0.1 [BD00b]. NC0 [AIK06]. p [FL06].
$p^q$ [LKYL00]. $p^r$ [CHH01]. $Q$ [Yas08]. $r$
[JJ01]. $w$ [DwWmW05, OT03b]. $x^n$ [Gon06].
y [OS01]. $Z_n$ [LWL09].

-Adic [GHK+06]. -Bit
[AIK+01, CDL+00, PCG01]. -Connected
[BJLS02]. -Coordinate [OS01]. -coverings
[SC02b]. -decompositions [vDKST06].
-DNF [BGN05]. -Metric
[AIK+01, CDL+00, PCG01]. -Connected
[BJLS02]. -Coordinate [OS01]. -coverings
[SC02b]. -decompositions [vDKST06].

.Round
[FL06, CHH01]. -Round
[BP04, Bih00, GHK+06]. -Steiner
[WL02]. -Threshold
[CLT07, Kog02]. -way
[LKJL01].

.NET [For04, TG04].
/dev/random [BH05]. /evolution
[Pat02a]. /MOM [DJLT01].

0 [And04, BC04a, Gum04, Imr03, Puz04,
WYY05d]. 0-07-222742-7 [Gum04].
0-13-100851-X [For04]. 0-226-74410-8
[Top02]. 0-262-14075-6 [Pag03].
0-321-20217-1 [Puz04]. 0-385-49532-3
[Imr03]. 0-470-84403-7 [And04]. 024-Bit
[GS07a]. 05 [ACM05a, MS05b, ZC09]. 07
[ACM07]. 08 [ACM08]. 09
[ACM09, IEE09a].

1 [BD00a, BSW01, FOP06, GM00b,
GLG+02, HKR01, MP06, PS01c, Puz04,
Uni00c, Uni00d, Uni00g, WYY05b, WYY05c,
Was08a]. 1-58488-518-1 [Was08a].
1-Connected [BJLS02]. 1-out-of-n
[AOS02]. 1.82Gbits [KV01].
1.82Gbits/sec [KV01]. 101 [Sei00a].
1011B-3 [ISO04]. 16
[Uni00c, Uni00d, Uni00g]. 106-1
[Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a].
109-bit [Pri00]. 10th [Coc02a, Joh03,
Lee04b, MZ04, Sma05, dCdVSG05]. 11-15
[AUW01]. 11th [CCMR05, HY05b, HH04,
HH05, RM04, Roy05, USE02b]. 12 [TPS01].
128 [JJ02, WFLY04]. 128-Bit [SM05b].
12th [GH05, MS05b, PT06]. 13-15
[ACM05b]. 130 [LM08]. 14th
[AMW07, AAC+01, Bir07]. 150-Kilometer
[Das08]. 155 [LMP+01]. 15th [M04, BC01].
160 [KSF00]. 16th [BS03]. 17th [IEE05b].
186 [Nat00]. 186-2 [Nat00]. 18th [KM07].
1905-1 [ISO05]. 192-bit [Luc00]. 1930s
[Kha05]. 1993 [PPV96]. 1999
[Lee03b, Uni00a, Uni00f, Uni00c,
Uni00e, Uni00d, Uni00g, Uni01h, Uni01j].
19th [BCD09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000
[CGH+00b, Eke02, Irw03, KH08, KI01a,
Sch00b, Wit01, YG01c]. 2001
[ACM01a, BC01, GJSS01, Lee03a, Pem01b].
2002 [B+02, IEE02, RSA03a, Yun02a]. 2003
[ACM03a, ACM03b, ACM03c, BS03, Bon03,
FLA+03, WK03]. 2004 [ACM04b, ZC04].
2005 [ACM05a, ACM05b, ACM05c, ANS05,
HY05b, ISO05, Roy05, Ter08, Ytr06]. 2006
[ACM06]. 2007 [ACM07, Ano06b, SM07b].
2008 [ACM08, Dew08, YRS+09]. 2009
[ACM09, May09]. 20th [Bel00]. 21 [AJ01b].
21264 [WB00]. 21st [Jef08, Kilo1a]. 21th
[IEE09a]. 22 [McK04, TTTZ01]. 22nd
[Yun02a]. 23rd [Bon03]. 24th
[Cra05a, Fra04]. 256-bit [Luc00]. 25th
[Sh05a]. 26 [DB04]. 26th [EBC+00]. 27th
[Men07]. 29. [Eke02]. 29th [FLA+03].

3 [Duw03, Imr03]. 3-15-07640-9 [Eag05].
3-540-66784-4 [Duw03]. 3-Key [Kel05].
3.0 [Flu02b, Hei01, SQ01]. 305 [ECM00a].
306 [ECM00b]. 30th [Coc02a]. 314pp
[Duw03]. 3278 [BWBL02]. 33rd [ACM01a].
36th [ACM04b]. 37th [ACM05c]. 39th
[ACM07]. 3D [LZP+04]. 3GPP
[KSH01, SM02]. 3rd [ACM05a, USE00a].
4 [Duw03]. 4-round [DLP+09]. 40th
[ACM08]. 41st [IEE00a]. 42nd [IEE01a].
43rd [IEE02]. 44th [IEE03]. 45th [IEE04].
46th [IEE05a]. 47th [IEE06]. 48th [IEE07].
49th [IEE08]. 4th
[BCKK05, BC05c, 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 [Bla03,
Des02, HA00, JQ04, LL04c, MMV06, Oka00].

7 [And04, Gum04]. 7-round [Pha04]. 7.2
[TvdKB+01]. 77 [AL04]. 7th
[BCJ+06, Wac05].

8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800
[BG07a, Hir09]. 800-90 [BG07a, Hir09].
802.11b [SIR04]. 802.11g [Coc02a].
802.11i [HSD+05]. 802.15.4 [Mi808]. 82
[Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02,
SMP+09, VY01, Vau05a, WK06, Zhe02b].

9 [CGF+02, Gan08]. 9/11 [Ark05, Mah04].
90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1
[GM00b]. '98 [Wil09]. '99 [DN00b]. 9th
[CMMR02, CSY09, DR02e, DKU05, Lai03,
NH03, Pat03b, PY05, YDKM06].

= [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05]. A5
[BD00a, BSW01, PS01c]. A5/1
[BD00a, BSW01, PS01c]. AAFG1 [Hug02].
AAs [LCP04]. Aarhus [Cra05a]. Abadi
[MW04]. Abelian [CF02, PHK+01, RS02].
Abstention [JLL02]. Abstract
[CMM00, Con04, DRR05, HLvA02, HJW01,
JL00, MSJ02, MP02, Mas04, Wag02, BJN00,
BCDM00, CD00a, CC04c, FKS+00, GHJV00,
GTZ04, HT04, HP01, Iwa08, IK00, Jon08,
KK05a, KM00, LM08, Mes00, Pei09, Yas08].
Abstracting [Bla01a, Mon03]. abstraction
[BLP06]. abstractions [BG07a]. Abstracts
[Sch00b]. Accelerating [ESG+05]. acceleration [EHKH04]. Accelerator
[CGBS01, RS04, TS00, XBO1, DPT+02].
Acceptance [CFR02]. Access
[ANRS01, Ano02e, BNPW03, CGMM02,
DS06, HC08, MS03b, Ril02, Sma03a, Sun00a,
ZGLX05, AW05, AW08, AFB05, BA06,
BNP08, Che08b, DFM04, Hos06b, HW03c,
HY03, IY06, JW06, KNS05, LKZ+04, MF07,
MSP+08, PS02a, STY07, WL05, WC01b].
access-control [BNP08]. accessible
[Pau02a]. accountability [WABL+08].
Accounting [Lai08]. Accumulator
[GTH02]. Accumulators [CL02a].
accurate [ZY08]. Achieve [CFRS01].
Achievement [Coc01a]. Achievements
[VDK05]. achieving [PS04c]. ACISP
[YG01c]. ACM [ACM01a, ACM03a,
ACM03b, ACM03c, ACM05b, ACM05c,
ACM06, ACM07, ACM08, ACM09, ACM10,
MS05b, Bar00b, FMA02, Raj06]. ACNS
[GKS05, IY05, JYZ04, ZYH03]. acoustic
[ZT05]. Acquiring [SETB08]. across
[Dav07, ZBLvB05]. Act [Kha05, Uni00a,
Uni00c, Uni00d, Uni00g, Uni00h]. Actel
[DV08]. Action [SE01]. Active
[BC05a, BACS02, BP02, LKL05, MA00a,
MA00b, Tad02, BPS08]. Active-Content
[MA00a, MA00b]. activities [AJ08, SN07].
actually [Hau06]. Ad
[BS02, WT02, Cha05b, DHM07,
KVD07, LHC08, LKZ+04, PCSV07, SLPP07,
TW07, ZC09, MAsT04]. 'ad-Durayhim's
[MAaT04]. Ad-hoc
[BS02, WT02, DHM07, ZC09].
Adaptation [ISSZ08]. Adapting [MJ01].
Adaptive
[CM00, CBB05, CTL04, CL08, Coc02a, CS02,
CS03b, DSS01, EFY+05, FMY01, JM02,
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].

dependent [JT01b]. Adjustment [BSN00].

Adrian [MAaTxx]. Adleman
[BST97, Coc03, SP97]. Administration
[USE00c, USE00a, Ris06, WL04a].

administration [Cra05b]. Admitting
[HSZI00]. Advance [CBZ+01]. Advanced
[CF07, DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Swe08, Tan01, Ase02, Bar00c, HI00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sye00, WBRF00, Wri01, YW06]. Advances
[Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS07, ELv01, Kil01a, Oka00, Pfo01, Pre00, TI07, Yum02a, Kat01, Bih03, C04a, Cra05a, Fra04, Kuo02, Lai03, Lee04b, LLT+04, Li05, LST+05, Men07, Roy05, Sho05a, Zhe02b]. Advantage [SZ01].

advantages [CDS07]. adventures [Hro09].

Adversarial [CLR09, GSS08, MNS08].

Adversarial-knowledge [CLR09].

Adversaries [CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05]. Adversary
[Aba00, Gor06, RW02]. AES
[CGH+00b, DRS05, FIP01a, Her09a, Pha04, AG01, Ano00a, AL00b, BDK+09, CG03, Coc02b, DR00b, DR02a, DR02b, DLP+09, DPR01, Dan01, Dra00, EECP00, Fer06, FM02b, GC00a, HW03b, IBM00, IK00, IK01, Joh00, KS09a, Kel05, KFSS00, KV01, LP02a, Len01, MMH+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03b, RRY00, SKKS00, SM03b, Sch00b, SKW+00, SW00a, SL00, WW00, WB00, WOL01, WWGP00, WWCW00].

AES-CBC [Fe06]. AES-like [DLP+09].

AES-related [Sch00b]. Affine
[Ben00, CT09, Fel06, HH09].

Affine-Transformation-Invariant [CT09].

AFIS [Zir07]. African [WDO1b]. after
[Ber03, McL06]. again [Fox00]. Against
[CS05b, DM07b, FKS00, KS00a, KKS00a, KKS01, Mes00, Mes01, MSPS05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Bau05, BPR00, BP02, BBN+09, BBB+02, BC02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Eg00, EBS01, FP01, Fry00, Gb04, HNZI02, HLL+01, HG07, Hsu05b, HLC08, In050, ISW03, IIT03, JKS02, J100b, JTI01, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, Mit00, Mol02, MOG08, NRR00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PC03b, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sho00b, SKU+00, SKI01, SLL+00, Tad02, TV03, VHP01, XH05, Y010, YML02a, YML02b, YML03, ZCW04, ZSJN07]. Age [Mar08b, Lev01].

Agency
[AJ08, Ban02, K0v01]. Agent
[HQ05, KC02, PDZH09, RDS01, RC01, Rot01, ZYM05, KXD00, SSM+08, SH00].

Agent-Based [HQ05, SSM+08]. Agents
[WHI01, Hau06, LSA+07]. Ages
[Eag05, Kiv01]. Aggregate
[BGLS03, WK05]. Aggregated [ZSN05].

Aggregation
[Her06, CCMT09, MS09b]. Aggressive
[Wy05]. AGM [Gau02].

Agreement
[AAFG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB+04, AKNRT04, CYY05, CYY05, Che04a, CY05, CJ04, CJL05, HWWM03, Ju04, KPT04, KRY05, KHKL05, LKYY03a, LKYY03b, LL04a, LLL04, LL05a, LKY05b, LKY05b, LKY05b].
LKY05c, LKY05d, LLY06, LLS^+09, LLR02, PQ03a, PQ06, SW06, Shi05, SW05a, SC05b, Tsa06, Tse07, VK08, YW05, YC09b, YS02, YSH03, Yi04, YRY05b, ZC04, LLR06.

Agricultural [Lov01]. Aided [NS01b, HLL^+02]. Aim [Pau02a]. Aimed [SFD06]. Airport [Sas07]. Airways [Dav07]. Ajtai [GK05]. AKS [Che03]. Al [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx].

Alerts [NCRX04]. Alchemy [Pag03]. Alcatraz [LSVS09]. Alchemy [Pag03]. Alert [AJ08]. Alarms [NCRX04]. Alexandria [MS05b]. Algebra [Cou01, CD01a, Lan04a, CK07, Fau09, HW03a, HWR09, Sho05b].

Algebraic [AK03, Bar09, Can06b, CMR06, CM03, Cou03, CS05f, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mas04, MN01, MR02a, MR02b, PDMS09, Bul09, CKN06, CDL06, Iwa08, May09].

Algebraically [RBF08]. Algebras [BDFP02]. Algorithm [ANS05, AEMR09, Bar00a, Bar00c, Bi09, BSC01a, ChLYL09, CU01, CJS01, CTL01, CG03, CC06, CH07c, CKM00, CT03, CP03, DR01, DG00, Dhe03, EYCP00, FBW01, FMS01, GMM01, HT02, HM02c, HZSL05, JKK^+01, KBD03, KMM^+06, KY02c, KLB^+02a, KTT07, KV01, LPZ06, MM01b, MM01c, MS02e, NMS01, OS01, PZ09, PB07, Ram01, RS01, SS01a, SPG06, WH05, Wes01, Wie00, AJ08, App05, BF06a, Bla00, C099a, CH01, CKY05, CYH^+07, CCH01, FOP09, Fer06, FSG01, GPH08, Jon08, KJ01, Kwo02, Kwo03b, LCP04, LLLZ06a, LLLZ06b, MN14, OS07, SCS05a, SM08, SZ02, TM01, WL02, WN05, Wuo09, YRY05c, And03, SA02].

Algorithmic [Hro09, Jou09, Has01b]. Algorithms [AD07, A009c, AB09, BKLS02, III00, BWBL02, CPhX04, CLR01, Dama07, DWN01, FW09, Gau02, GL06b, Har06, Har09, Int00, JP03, Kel05, Lee03b, LR07, LP02b, PBB02, Pre02a, Pre02b, SL00, TLYL04, TV03, WBR00, WGW00, AHK03b, Ano01j, AH05, CKL^+09, CCM01, GH05G, GPC08, HW03a, HWR09, HH06, Hro05, JK01a, MCHN05, Pre07, Rho03, TC05, XLMS06, ZLS07, Zir07, dH08].

Alien [Wil01b]. All-or-Nothing [Des00c, SR00]. Alley [DR01, Wie00]. Allied [Hau03, Hau06]. Allocation [CCM05, LZ09]. Allowing [JLL02]. Almost [AP09, BS00a, Jut01, Mar02b]. Alpha [WB00, Wu02]. Alphal [KHD01]. Alterna [Ano02a]. Alternating [Wer02, HKP05].

Alternative [Bad07, Gar03a, Han00, BMW02b]. Always [BB79]. am [Eke02, SU07]. Anamli [BC05c, CGP03]. Amenability [WW00]. America [DB04]. American [GL05, Kat05b, Alv00, Na05]. Americans [WD01b]. among [BN00a, KT00, SKU^+00, Win05c].

Amongst [Pen01b]. Amplification [CHS05, LT05, RK05, SV08b]. Amplified [KK00a, KKS01, KML^+02]. Amplifier [Pl01]. Amsterdam [Knu02]. Analyses [BPR05, Des00a, Pau01]. Analysing [BL02].

Analysis [AR08, ABR01, AKS06, AD07, Ano01c, AIK^+01, ARC^+01, Ava03, BN00a, BDhKB09, BRS02, BF05, Bor01, BSL02, Cry00, CK02a, CS03b, DPV01, Dra00, FL01a, FGM00a, Gir06, Gol01c, GH05G, GPR06, HZSI01, HKR01, HSS04, Hey03, HM02c, IT03, JK01a, JQY01, JT01a, JQY01, hKLS00, KMS02, LCK03, LKHL09, LY05, LWK00, LH07, MOP06, Mar02b, Mas04, MS01, MM01, Mea01, Mes00, Mes01, MAaTxx, MG08, NP02b, N002, OS06, ÖOP03, Puc03, Q01, SSST06, Sha01c, Sma03b, SDM06, SQ01, SWT07, YSS^+01, ZC00, ZGL05, A0H00, AW05, AW08, Abd01, AHK03b, As04b, BDS08, BBK^+03b, Bjo05, BG07a, BR05,
Lai07, LL05c, Lut03, OMT02, PBD00, Pau02a, Pre02a, SKG09, VH09, VVS01, Vir03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLM05, GGH+08, Har05a, JJ01, JW01, KVD07, LG09, LYC02, MT09, Mar05b, Mio09, Mos06, NN03, SLP07, SK03, SN04, SW00b, ZLX99, ZSZ01, ZL04a. Approaches [CGMM02, AvdH00, DG05, Fri07, Has01b, KXD00].

Difficulty [Wan04b].

Approximation [CLZ02, Kuk01, WL02].

Approximations [BDQ04].

Apress [Ter08].

April [Ano00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH+08b, DFPS06, Joy03b, Knu02, Mat02, NIS00, Nac01, Sch01d, SMM+09, YDKM06]. APSS [ZSV05].

Arabic [MAaTxx].

Arbitrarily [RW03b].

Arbitrary [AR01, BR00b, BR01, CKN00, CHJ+01b].

Arbitrary-Length [AR01, BR00b, CKN00, CHJ+01b].

Architectural [ASK07, ABM00a, BMA00b, BMA00c, CW02, Gro03, KV01, LTM+00, ZYL05, Ano05c]. Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LKM+05, LST04, LXM+05, Lut02, MP01c, MFS+09, Rot02a, SMT01, SM03b, SLG+05, Uzn04, Che00a, CC05e, DLH06, Ino05, LHL03b, MPP09, SKW+07, SHL07, SH05, Tan01, WWA01].

Architectures [BGK+03, KLY02, RM02, SM02, Con04, DP04, GKS05, NdM04, RH00, WH02b]. archival [SGMV09]. Archives [RC01].

archiving [DMSW09]. area [BP03a, Cal00c]. Areas [HH04, MZ04, PT06, VY01, AMW07, Buc00a, HH05, HA00, NH03, ST01d].

Aren’t [Bau01a, Bau01b]. Arguments [HNO+09]. ARITH [BS03, BC01, IEE05b].

ARITH-15 [BC01]. ARITH-16 [BS03].

ARITH-17 [EE05b]. Arithmetic [BS03, BIP05, BGK+03, BCD09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDJ+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 [Bhu09]. Art [An07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Eri03, Eri08, MS02d].

Article [Che08b]. Artifacts [EHK+03]. Artificial [Cop04b, MMYH02]. Arun [For04]. ASCI [MJD01]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DNM00b, KI01a]. ASIC [WOL01].

ASIP [SKW+07]. asks [Ano08a]. ASM [MK05a]. Aspect [Kos01a]. Aspects [BLMS00, CMR06, Pe06, An03, DLP+09, Rup09].

Aspiration [Ash03]. assembly [Gon09]. assessing [CDD+05]. assessment [CC05e, DMS07]. assets [KH03, NRR00].

Assignment [BRT09, HC08, CHC04, CJ03c, DFM04, HW03c, Hwa00, Lin01a, TP07, WC01b, yH08]. assignments [SWR05].

Assisted [ECD+07, XS03, Art04, BB05, LH04a].

ASSL [VH09]. associated [XLM06]. associativity [HRS08]. Assumption [CS00, DN00a, FOP01, KMZ03, ZD05].

Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT+00, Nac03, SBZ02, Mic02a].

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

Astrology [Pag03]. Astronomy [MYC01].

Asymmetric [CH07b, Man01, SY01a, SBZ02, WHI01, YG01a, GJ04, Lee01, OP01b].

Asymptotically [vDW04]. Asynchronous [CKPS01, FLM+03, SKR02, SKR2, ZSV05]. at-targama [MAaT05]. Atlanta [Vie09b].

ATM [Pat02a, Pat02b, Zea00]. Atomic [CN06]. Attached [RCBL00].

Attachments [Ric07]. Attack [Ahm08, CKQ03, CS05b, CS03b, Des00b, Fil00, FV03, 
GHJV00, GHJV01, HQ01, Hug02, HW01, JI00b, KCP01, KS00a, KML+02, KM01c, LY07, LNL+08, LV04, LMV05, Luc02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, PQ03b, RMS05, SG00, Sch01b, Sho00b, Sma03b, VHP01, YKLM02a, ZC04, ASK05, Ade09, DKL+00a, Du09, Duj09, GM00a, HAU04, Hes04b, HG07, Iwa08, JJ02, KS09a, KM04a, LM08, Law09b, LS05b, Mir05, OS00, SIR04, XH05, ZCW04.

Attack-Resistant [LNL+08]. attacker [BDSV08]. Attackers [JMV02]. Attacking [FMP03, KPR03, Luc00, TMMM05, BF06a]. Attacking-Based [TMMM05]. Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, BMM00, BB+B+02, BDK+09, BU02, BM03b, BCP02b, BM01c, Can00b, CS07b, C203, CT08a, CJS01, CKM00, CIJ00, CM03, Cou03, CWR09, CD01b, DPV01, DFS04, DJ06, DS08, DM07b, FK09, FOH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GKO2, HSH+08a, HNZ02, HR04a, HSH+01, HLC08, ISW03, JKS02, JJ00d, KK00a, KS00b, KKS01, KCJ+01, KLO1a, Law09a, LLS05a, LWS05, LJ05b, MOP06, MP06, MFO1, McK04, Mes00, Mes01, Mel02, MG08, OT03a, OT03b, OOP03, OST05, Ove06, PK09, PDMS09, RS01, SK01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZ05, YYY01, Y01, Y02, vW01, BPS08, Bau05, BCS08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05b, HLU05, In005, IM06, JD01, KS05a]. attacks [KTC03, LPV+09, LSH00, MMLJ05, NS05a, NLD08, OST06, PQ03a, RG05, Sch00c, Sch01f, Sh05, SL06, SK05b, SW00b, WL07a, WL04b, Yan07, Y02, ZSJN07].

Attitudes [FD00, CF05]. attractors [HHY07]. Attribute [LY05, RSA00e, IY05]. Attributes [SS01b].

Auction [AS01a, An01a]. auctioning [RCG+05]. Auctions [Bra01b]. Audio [Ar01, CS05c, DRL09, MH05, WNY09, WWL+02, XZF01, WNQ08, BS01b, KJR05, KN03]. Audio- [KJR05]. Audio-and [BS01b, KN03]. Augmented [CS07c, You01]. Augmenting [AL04].

August [AMW07, Be00, B+02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KKP02, Kil01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch00b, Sch00c, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Y02a]. Australia [Boy01, IZ00].

Austria [DKU05, P01, Jef08]. Authentic [DGMS03, Dur01, SS01b]. Authenticate [Bau03a, Bau03b]. Authenticated [AGT01, BN00a, BPR00, BU02, BC04b, BM01, BMP00, BCP01, CPP04, Ch08e, DG03, DA03, EP02, GKO07, GL03, GTT03, HS07, KOY01, KY03, K03, LHT09, MPS00, Mac01, JS02, MN04, NA07, Nam02, Ng05, Pol01, SK00, Vau05b, WCO1a, YPP09, Y04, ZWC02, BKN04, BCP07, CYY05, CY05, Che04a, CL08, CJ04, CUL05, DG06, GL06a, GRM05, HT08, HWW02, HWW03, HSu05a, Hwa05, HL05c, HL05d, J04, K09, KRY05, LKK03a, LKK03b, LL04a, LL04b, LL05a, LK05c, LK05d, LHC08, LL02, LL06, LW05a, Mis08, PQ03a, PQ06, RBB03, Se05, SW05a, SC05b, TLH05, T01a, Tse07, WL06, WH02a, XY04, YW05, YC09a, Y02, YSH03, YRY05b, YPK08, ZC04, ZAX05, ZW05b, ZL05].

Authenticating [AIP01, Chi08a, CGV09, Fur05, JW05, PM08, RCBL00, YSS+01, Lin01b].

Authentication [AAK09, AP09, ANRS01, An01b, An01c, An01e, A02d, AHMK02, AN01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, BKR00, BCC01, BC02, BC05b, BDK09, BR02, BDFP05, BDF01b, BM03c, BL02, BLDT09, BPE+00, CV03, CG08, CS07b, CC01b, CC01b, CC05b, CC09, CJT02, CJ03d, CWY05, CT09, C01, CR01, CFRR02, CGK+02,
Authentication

Authorisation

Authorities

Authorization

Authenticity

Available

Auto-recoverable

Automata

Automorphisms

Autopsie

Auxiliary

Availability

Auto-numerical

Average
[KMT01, CGHG06]. \textbf{average-case} [Mic02b]. \textbf{avoid} [Tyn05]. avoided \cite{CNPQ03}. \textbf{Award} [RSA03a, Bar00b, Coc03]. \textbf{Awarded} [Coc02b]. \textbf{Aware} \cite{IKP07, OHB08a, CBSU06, OHB08b, Zea00}. \textbf{Awareness} [HLM03, BK05]. \textbf{Away} [Coc03, Ols00, Tee06]. \textbf{Awkward} [TvdKB01]. \textbf{Axiomatization} [dH08]. \textbf{B} [SPK08, YG01a]. \textbf{B-Spline} [SPK08]. \textbf{B2B} [Zho02]. \textbf{Babbage} [Bar00a]. \textbf{Back} [CZB01, KCD07, SF07, Ano00g]. \textbf{Back-End} [KCD07]. \textbf{Backdoors} [CS03c]. \textbf{Backup} [Str02]. \textbf{backward} [HCD08a, HCD08b]. \textbf{backward-and-forward} [HCD08a, HCD08b]. \textbf{Bacon} [GG05a]. \textbf{bad} [BBN09]. \textbf{bail} [Ano01g]. \textbf{Bait} [Luc02a]. \textbf{Balancing} [Hof01, Lut02]. \textbf{Ballot} [Cha04]. \textbf{Baltimore} [ACM05b, ACM05c, GL05]. \textbf{Banach} [AUW01]. \textbf{Bandwidth} [CG1+02, YY01, SLP07]. \textbf{bandwidth-efficient} [SLP07]. \textbf{Bandwidth-Optimal} [YY01]. \textbf{Bangalore} [MMV06]. \textbf{Banking} [HKW06]. \textbf{Barbara} [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a]. \textbf{Barcode} [Che08b]. \textbf{Bare} [DPV04]. \textbf{Barkan} [Sty04]. \textbf{Barret} [Gro01]. \textbf{barriers} [Kov01]. \textbf{base} [DIM08, IR02]. \textbf{Based} [Ano01c, ANR01, AF03, AJO08, BDG+01, BKL02, BNPS02, BN02, Ben00, BRS02, BF01b, BF03, BB04, Bon07, BCKH07, BHG07, BPR+08, BD03, BM01, Boy03, BQR01, BM10c, BSN00, BRTM09, CGFSH09, CvTMH01, CK02a, CMGM02, CF01b, CC02a, CV03, CPP04, CCD07, CS07b, CC01b, CLT07, CHSS02, CHM+02, CJK05, CM05a, CTH08, CGK+02, Coc01b, Cou01, CFS01, CS00, DN00a, DKMR05, D03, EHK+03, EM03, FL06, FM02a, FMY01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HC08, HH09, Igl02, Jam00, KBD03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05, KY01c, KY02b, KCO9b, KK02, KC02, KCO7, KPR03, KM05, Kra02a, Ku02, KWP06, KT00, LLL02, LP03, LKL05]. \textbf{Based} [LHT09, LZ01, LZ04, LL05c, LPZ06, LY07, LLRW07, LWK00, LSC03, LH05, LSO5, LLS05b, LCD07, MPS00, Mar08a, Mar08b, MNP01, Miy01, MGC02, Mii01a, MSU05, NMO05, Nak01, Nam02, NBD01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP06a, PZL09, PMRZ00, Rii02, RE02, RH02, RS00, RS03, RS08, RMC01, Sal05b, Sch01a, SSFC09, Shao2, Shao1e, SOO01, SXY01, Sma03a, SBEW01, SGB01, TMMM05, TYY, TZZ09a, TZZ09b, VMSV05, Vau05b, Ver06a, VHP01, VK07, WRW02, WY02, WZW05, WG05, WC09, WH09, WBD01, WC04, XYL09, YK01Y, YY01, YSS01, YK01Y, YL05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWCY02, vDW04, AAPP07, AA08, Ano02b, Ano05b, App05, AAK09, BGB09, BBC+09, BR04, BFG08, BS01b, Bla01b, BMW05, BLP06, BGL+03, BDS09b, Buh06, CGHG06, CG06, CL02b, Co09a, CL04d]. \textbf{based} [CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c, CJ01, CJ02, CL06, CJL05, Cho08b, CYN20, CCD+04, CT07, CHT02, CC04c, Cra05b, DS09, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EHK04, FLZ02, FXAM04, FLL08, GM09, GW08, GSK09, GL06a, GHS00, GS01, GPS05, GSG+09, GB09, HM00, HLL+02, HCD08a, HCD08b, HRL09, Has00, Her07, Her09b, HPS01, HG05a, Hsu05a, HLwWZ09, Hii00, HP01, HLL03, HL05d, sHCP09, IM06, JK01a, JK01b, J06, JPL04, JZC05, JLL01, KG09, hKLS00, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KLC03, Ku04, KCC05, Kwo03a, KHKL05, LHL03a, LP03, LKY05a, LKY05b, LHY05, jLC07, LG09, LD01, LTH05, LPM05, LW05a, LWZH05, LYGL07, ZG06, CL02b, CO09a, CL04d].
LLW08a, LLW08b, LCC05, LSA+07,
LCZ05c, LCZ05a, LLC06a, LLC06b, MW06,
MS09c, Mic01, MR09, Mi09, Mit00, MB08.
based [MC04, MPPM09, MV03b, NZCG05,
NC09, NSNK05, OS09, PCSM07, PW05,
PBMB01, FSG+09, PS08a, Pel06, PSP+08,
PC00, Pha06, PLJ05a, PLJ05b, QC03a,
Reg03, Reg04, RG09, RCG+05, Se02, SG07,
Sc04, Sei05, SP02, Sha03c, Sha03d,
SC05a, Sha05c, Sha05d, SLH03, SCS05a,
mSFtL05, SSM+08, SW05a, SH00, SK01b,
SCL05, Sun02, SCS05c, SY06,
TNG04, TWA08, Ts0a8, Ts0a5, UHA+09,
UBE09, VS01, WAF00, WLT03,
WL07a, WJP07, WQ08, WLLH05, W09,
W00, W02b, WY05, WC05, XMST07,
Y09a, YCW+08, YWWD08, Y09b, YS04,
h09, Y00, YPSZ01, YR05c, YPKL08,
YY00, ZC04, ZC09, ZDWO6, ZCL05,
ZY07, dRMS05, ZS05. Bases
AAC+01, ADDS06, BKP09, B+02,
CtT09, F00, F03, FLA+03,
CCT08, F009, ZT03. Basic
[Go01b, Go01a, Go04, Kat05b, Puc03,
St02, Bon00]. Basics
[Lh06, Lut02].
Basing
[BPR+08, CHL02, AGM06, AGM10].
Basis [RMH03b, Vav03, vW01, GPS05,
LR05b, RMH03a]. Batch
[AR02, HLT01,
PBB07, Sh01d, BLH06, HLL00]. Batching
[SB01]. Battery
[CBSU06]. Battle
[Bd000a, Bd02, SM00c, SM05, SM07a].
battles [Ca00d]. Bay [Ca00c]. Bayes
[Go00]. BB84 [Ina02a]. BC [EE02]. BCH
[MLC01]. BDD [KLN+06, Kra02a].
BDD-Based [Kra02a]. Be
[Bar00a, Pan02a, CNQ03, YJ00, vT01].
Beach [EE00a]. beat [Lev01]. because
[AJ08]. Become [Ort00, Wai04]. Been
[Nic01]. BeepBeep [Dr02]. before [Uni00a,
Uni00b, Uni00f, Uni00e, Uni00h, YJ00].
Beginning [Dew08, Hoo05]. Beginnings
[Bd000b]. Begins [MP00]. Behavior
[Vav03]. BEHEMOTH [Bar00c]. behind
[Hea06b]. Beijing [FY06, LST+05]. Being
[ASW+01, ES00a]. beleid [DL00]. Belgium
[DR02c, Pre00, Q500]. Belief [BPST02].
believing [Buh06]. Bell [BZ02, Eke02].
Benchmark
[As02, TLYL04, LDH06, YLT06]. Bendy
[Sas07]. Benefit [YKM02a]. benefits
[CH00]. Benford [NM09]. Bergen [Yfr06].
Berkeley [EE06]. Berlin [FLA+03].
Bermuda [Bla01]. Bernward [DNR03].
Berner [Coc02b]. Berners [Coc02b].
Best
[Bau01a, Bau01b, MFS+09, Go08, St02].
BestCrypt [Bau02b]. Bethesda [ACM09].
Better
[FV03, PM00, RR02, SKQ01,
HLL03, Pan03, Rie00]. BetterBASIC
[ASW+01]. Between
[DKM05, Ket06, Ngu05, NWN06, Fan09,
GKM+00, GC05, MSV04, Pan01, RW03a,
Sch02, Sch04d, SK06]. Beurling [Bec02].
Beyond [Gor06, Hei03, LMW05, Mar08a,
Sch03, See04, Sty04]. BGP
[ZSN05, vOWK07]. Bi [Cou04, PKJ01].
Bi-directional [PKJ01]. Bi-linear [Cou04].
Bias [CL02c, Se100]. Blased
[BS00a, LSKC05]. BiBa [RR02].
Bibliography [Bee05]. Bidiagonal [BR09].
Bidiagonal-Singular [BR09]. big [RR03a].
BigNum [SR06]. Bilateral [CT08a].
Bilinear
[BGLS03, BMS03, CL04a, HNS02,
KK02, DSGP06, LCO05, VK08]. Bill
[Gen00a]. billing [SSM+08]. Binarization
[LSK05]. Binary [AD109, HHN01,
LSK05, OSSST04, SKG09, WC09,
ACTZ05, BG08, BG09, FSGV01, GB09].
Binary-Ternary [AD109]. BIND [Kle07].
Binding [DN02b]. BioAW [MJ04].
Biometric
[AKH02, Da01, EM03].
WH01, KJR05, LT+04, PZR00, PK01,
SR01, Sas07, Way01, Way02a, Wea06,
B001b, Gui06, JP06, KN03, Li05, LST+05,
MR00, RFR07a, RFR07b, RFR07c, Smi00,
MJ04, BJ02, ZJ04]. Biometric-Based
[PMR00]. Biometrics
Biometrics-Based [Ril02]. Biomolecular [Bi09]. Birds [MLM03]. Birth [Bud06, SE01]. Birthday [Wag02]. Bisimulation [BJP02]. Bit [AIK+01, BK06a, BLO8, CGH01, CDL+00, DMS00, MS09d, PCTG01, RMH03b, SM03b, SXY1, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, Pri00, RMPJ08, SWR05, UHA+09, WW08, ZFK04].

Bit-Fixing [KZ07, KZ03]. Bit-Substitution [GPX08]. Bit-Locker [Kor09]. Bits [BS01d, SZ01, HN04, Shp02]. Bitslice [DPV01]. Black [Ano01i, CF02, CFS05, DI05, DIRR05, DS08, KY01d]. Black-Box [Ano01i, BRS02, CF02, CFS05, DI05, DIRR05, KY01d]. Blackmailing [PS01b]. Bletchley [Sal00b, Cop05, Cop06, HS01a, Sal05a, SE01, Smi01b, Wei06, Win00]. Blind [AO00, BNPS02, BR02, BSC01a, CvTMH01, Can01b, CMB+05, Cro01, DR00a, Dwo03, EYCP00, Flu02a, HSH+01, JKK+01, KCP01, KYHC01, KKK03, LLRW07, LRW02, MV00, MS02e, NP01, OMSK01, Pat01, PS06, Pi01, RMS05, SM03b, SYY+02, SKU+00, SKI01, WC09, XH03, YG01b, Bai08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kat05a, KJ01, LDH06, LCP04, LKh+08, MJM05, PSP+08, RBB03, SHJ04, SHH07, WF02, XH05, YI00].

Block-Based [LLRW07, BCC+09]. Block-Cipher [BR02, RBB03]. Block-Cipher-Based [BRS02]. Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. Blocks [Jou02]. Blockwise [JMV02]. Blockwise-Adaptive [JMV02]. Bluetooth [GBM02, LV04, LMV05]. Blunders [Bur01]. Blur [VHP01]. Blur/Deblur [VHP01]. Blurring [LSKC05, SK06]. Board [CBG02]. boat [DB04]. Body [Bam02, TG07]. BOEL [Fat02]. Boethius [Eag05]. bolstered [Ano01h]. bombe [Wil01a, Tur04]. Bombes [Ano02i, LBA00]. bombs [Lov01]. Bonds [CA03]. Boneh [ASK05, Hes04a]. Book [An04, Du03, E05, Fal04, For04, Gas01, Gum04, In03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Re01, Rot07, Sal03b, S04, Shp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wall00, Was08a, Kat05b, Lam07, Lun09, MAA05, Ros00b, Sin99, Sin00, AAG+00]. Books [Che00b, Dr.00c, Ros00b, Re01]. Bookshelf [Lut02, Lut03, Wil01b]. Bookworm [Sal03b]. Boolean [Car02, CT03, CS09, MS02b, PQS05, SM00a, SM00b, SM03a, WV00]. Boom [An04a]. Boomerang [KKS00a, KKS01, KML+02]. Boot [HS+08a, HSH+08b, HSH+09]. Border [MJF07]. Borders [PGT07]. Boston [USE01b, USE01a]. Bot [Ano08b]. Botschaften [Sch09]. bottleneck [WL02]. bottlenecks [HTW07]. Bound [CY08, DGN03, KMT01, HLLL03, hY08, GW00]. Boundaries [PGT07]. Bound [Che04b, DFS08, DIS02, Din01, Din05, Lu02, MPPSW05, MTS04, Vad03, DFS05]. Bound-Quantum-Storage [DFS08]. Bounding [DM07b]. Bounds [BDP01b, BP03b, DIRR05, Di01, GGT05, RW03a, SWX01, SM00b, Shp03, Wall01, WW05, GT00, GKK03, ZJ09, KS05b, PS02a, Shp99]. Bowmeester [Duw03]. Box [An01i, BR02, CF02, CFS05, DI05, DIRR05, DS08, FM02b, KY01d, Kil01b, SMTM01, JmBdXgXm05]. Boxes [Bih00, BCDM00, ZC00]. BP
Braid [AAFG01, CJ03a, GM02a, Hug02, KLC⁺00, LLH01, LP03, MSU05, Cho08b, Hen06a].

Braille [Pau02b]. Branch [AKS06].

Branch [Fel06]. Branches [Fel06]. Break [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breakers [CD00b]. Breaking [Ano09a, BKN04, Das08, DKFX05, GO03, GKr02, Kov01, KR03, Kil08, Sal00a, Wri05, Fie09, Gar01, SE01, Smi01b, SL07, Swe08].

breaks [OS00]. Breakthrough [Coc02a, LR01, Pau02a].

Brief [Bon07, Cos03, Kir01a, Boo05, Gra01]. Briefs [MP00, PM00, Pau02a, Pau02b, Pau03, Pau09]. Bright [Ano01i, LNP02]. Bristol [DFCW00]. Britain [Gui06].

British [ACM08, Fie08, Fra01, Syv02, Bud00b]. Broadband [MP00, SLH07, MJF⁺08].

Broadcast [AFI06, BGW05, CKPS01, CNV06, DS03, FW04, GSW00, GKK007, GRW06, HS02a, HLL05, SNP02, SNW01, Woo00, ASW00, KSW06, Kre05, Mar05b, NLD08, RG09, WDLN09, LN04].

broadcasting [TJ01b, WH02b]. Broke [Urb01, KS04]. Broken [Ahn08]. Brooks [Bar00b]. BRSIM [BP08]. BRSIM/UC [BP08]. BRSIM/UC-soundness [BP08].

Bruce [Hei03, Sty04, See04]. Bruges [Pre00]. Brunley [ASK05]. Brute [Cur05, SGA07]. Brutus [CJM00]. BSD [Lin02, ASW⁺01, Lin02]. BSDCon [USE02a]. Bubble [Ber03]. Buchmann [Lee03a]. Buffer [FOBH05, Fry00, Ino05].

Bug [BCS08, Bor00]. bugs [GJL06].

Building [Jou02, Kmt07, Mar02a, And08b, Bra01a, FB01, LS05b, Mg06, MHPD06, PQ06, DB04]. buitenlands [dl00].

Bulletin [Cer04b]. Bulletproof [Cha05b]. bundles [GT02]. Burrows [ABM08].

Burying [Arn01]. Bush [Ris06]. business [HHSS01, Pol01]. Buy [PLW07]. Buyer [MM01a]. buys [Zaf00]. Buzzes [Coc02b].

Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGR07, LLR02, LLR06, P106]. Byzantine-Resistant [CNV06].

C [Ter08, Zol01, III00, Iw09, Oik09, RMPJ08, Sea05, Sea09, VM03, WK01, We05]. C# [MJ03]. C-testable [RMPJ08]. C²C [HTJ08]. CA [ACM03b, Joy03b, KKP02, Men05, Men07, Nac01, Oka04, Poi06, Pre02c, USE02a, USE02b]. CAA [MCG02]. Cache [BTTF02, Kle07, OST05, OST06, TSS⁺03, Ino05, WLR07]. cache-based [WL07a].

Caches [GSVC02, LLK05]. Caernarvon [TPK⁺08]. Caesar [Chu02, Yon06].

CAIDA [Pri00]. Cairo [EBC⁺00]. CaLaC [Sil01]. calculus [MRST06]. Calcutta [Roy00a]. Calibrating [SDMN06]. Calif [ACM03c]. California [ACM03a, ACM07, Bel00, Bon03, Fra04, IE00a, Kil01a, Sch01c, Sch04a, Sch05a, Sh05a, USE06b, USE02c, Wil99, Yon02a, IE006]. Call [Ano04b, Ano07b, Ano07a, MD04].

Calls [WG05, Ano08c, WC05]. Cambridge [ACM10, Chr00, Chr01, CCMR02, CCMR05, IE003, JQ04, Kat05b, Kil05, Nao04, Pag03, Puc03, Rot07]. Camellia [AIK⁺01, HQ01, KM02, LHL⁺02, SM03b, SK01, XH05].

Camera [CGK⁺02, Gei03]. Camera-Based [CGK⁺02]. Can [BB02, CZB⁺01, Dav01c, Lai08, Ras07, Ver06b, CNP03, CG05, SBB05, Zir07].

Canada [ACM02, ACM08, AMW07, HH04, HH05, HA00, IE002, MS05a, MZ04, NH03, PT06, ST01d, YV01]. Candidate [II00, 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 [BDD01, AL04, ABDS01]. Capability [MH05]. capable [ETMP05]. Capacity [ChLYL09, Sug01, ME08a, Wan05]. Cape [IE05b]. capital [SW05b]. capture
Card [BCST00, CMG+01, CL07, CJT02, DF01, DFPS06, RE03, RS01, SR01, Ano00k, Ano00l, Ano05b, AJ01b, Bor00, BGL+03, Bur00, Cal00c, Car01, CCCY01, Chao05a, Chao08b, Con00, CH00, DFCW00, GMG00, HM01a, Has02, Hen01, Hus01, Jac00, LSA+07, LC05a, Lu07, QS00, RE00, SP02, Smi00, VK08, Zaf00, Che00a, FGL02, Pau02b, SKKS00, TV03]. card-based [LSA+07]. CARDIS [DFPS06]. CARDIS'98 [QS00]. Cards [And04, AJ01b, Bel01, CK06, DJLT01, HBdJL01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NFQ03, QS01, Sak01, Sha01c, TBDL01, VPG01, YKMY01, Ano04c, Ano04e, AJ01a, BPR01, BCHJ05, Bur00, DFH01, DFPS07, FCZ05, Fm03, GUQ01, Gui06, HHS01, Hsu05b, Jua04, KLY03, LKY05a, Ler02, LCS09, MY01, Pha06, Pol01, PB01, Pre07, SVDF07, SLH03, TIS07, WC03b, YWD08, Ano03a, BJvdB02, CL04d, CCK04b, Che00a, Gro03, HL05b, Kuh04, KC05, LHY02, Sce04, SCF01, YW04a]. CardS4 [GN01]. Care [Mad00, RC06, Ano03a]. carefully [Cla00b]. Carlo [Bi09, Sug03]. carrying [Art04]. cars [LPW06]. Cartilage [MYC01]. Cartography [SGM09, SWR05]. Cascade [DGH+04]. Cascaded [Jou04]. Case [ABK00, Ano05a, BBGM08, BU02, BCP01, CNS02, GS07a, Nie02b, OST05, Van01, BKN04, BF06a, BK05, CSK+08, HRS08, KWDB06, Mic02a, Mic02b, OST06, Pe09, STY07, SKW+07, SPH06, ZWWL01]. case/average [Mic02b]. cases [ABHS09]. Cash [PS01b]. Cathedral [USE02a]. Cats [Pem01b]. Caught [Wei00]. cause [SBB05]. Causes [Mur01]. Cautionary [GMP01a]. Cayley [Lam91]. Cayman [Svy02]. CBC [BBKN01, BPR05, BR00b, DGH+04, Fer06, JMV02, KI03, Vau01, Vau02]. CBIDs [MC04]. CCA [KOMM01, Miö01b]. CCA2 [BST02, Lin03, RG09]. CCA2-Secure [Lin03]. CCGrid [TLC06]. CCM [Dwo03]. CCS [Mar02b, MS05b]. CDH [CM05a]. CDH-Based [CM05a]. Cell [Fox00, MYC01, SHL07]. Cell-phone-free [Fox00]. Cellular [Laf00, LZ04, MGC02, PZL09, Ric00, SBZ04, Bau04, ETMP05, KK03, SHH07, Wan04a, dRMS05, Wue09, SSN+08]. Center [AUW01, CH01a, CYH04, LPM05]. Centered [BKMO07, 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 [HL08, RHL09]. Certificates [BDTW01, CMG+01, RdS01, Bra01a, LCK04, ZSM05]. Certification [Ano01k, CHM+02, RSA00b, BGB09, BD04b, KB09]. Certified [ANR01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CJO5, HW04, HW05, HL04, LL06, LWK05a, NZS05, Sha04b, Sha05b, TLH05, Tsa05, TC03, WH03]. Cerven [Sal03b]. CFS [Ito01]. ChaCha [Ber08]. Chain [YT09, YZ00, Wue09]. chain-rules [Wue09]. Chained [BCC01, BC05b]. Chaining [BKRO0, CBB05, PCC03]. challenge [LM08, LW05a, PRS04]. challenge/response [LW05a]. Challenges [Cla00a, GV00, Nao03, Sta03, SVE09]. Chang [CWJT01, ZC05]. change [CYH05]. Changes [Mur01]. Changing [BST03]. Channel [BU02, CHVV03, Law09a, LCK03, Mšl02, NMO05, OT03a, OT03b, Sch06a, SYLC05, ARR03, BP03a, BGb07, Buh06, CNPQ03, KSWH00, LCZ05b, MS09c, PSP+08, WL07a, YTWT05]. Channels [API01, CK02b, Namo02, Vau05b, LH04]. Chaos [JK01b, SK01b, WZW05, JK01a, LMC+03, McN03, PSG+09]. Chaos-Based [WZW05, SK01b, JK01a, PSG09]. Chaotic [LLL+01, Mül06, SXY01, USS02, Vav03, AMRP00, ÄMR04, GHdGSS00, GB09].
HHYW07, HLwWZ09, JK01b, LMC+03, LYGL07, MA02, PBMB01, PS01a, PZL09, SPG02, SL09, UHA+09, VKS09, WG02, WW08, kWpLwW01, WLV04, YZEE09.

Chapman [Kat05b, Tat05]. Characteristic [Gau02, GPS06, KTO0, Ver02, GPS05]. characteristics [RFR07a, RFR07b, RFR07c].

Characterization [AJO08, Nam02, XH03, G02, KY00, QPV05, XLS06]. Characterizations [Pas05].

Characterizing [BTW05, BTW08]. Charging [BACS02, RH02]. Chatter [Kee05].

Chaum [BNPS02, KLN+06, WZH05]. Chaumian [Mol03a]. Cheating [CCL09, OKS06, PZ01, PZ02b, PZ02a, ZP01].

Check [Kir01b]. Checkable [BPST02]. Checking [BL02, JP07, KLN+06, YJ00, GGH+08, RG05].

Checks [FM02a]. Checksums [Sto01, SGPH98]. Cheju [Kim01].

Chemical [EIG01]. Chen [LW05c].

Chennai [CV04, RD01, Roy05]. Chernobyl [Rie03]. CHES [JJQ04, KKP02, KP01, KN01, RS05, WK03]. CHESS [LKHL09].

CHESS-64 [LKHL09]. Cheswick [Che05b].

Chicago [ACM04b, Top02, Con00]. Chien [YRY05b]. Children [Pau02a, Sye00].

China [B+02, DWML05, FLJ06, JTY04, LLI+04, Li05, LST+05, ZJ04, ZYH03, An00c, TZX01]. Chinese [LLT+04, Li05, Sch01b, CAC06, YKL03].

Chip [Ade09, BNWP03, DV08, MM01b, MM01c, MP00, Fox00, ITE08, An00c].

Chip-Secured [BNWP03]. Chipkarten [An004c]. Chips [An000d, Pau02a]. Choice [Jan00].

Chosen [BCH07, CKN03, CH+01a, CH+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JK02, J006b, KS00a, KY01a, KCJ+01, KMZ03, KM01c, K101a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH+09, KG09, ZCW04].

Chosen-Ciphertext [BCHK07, CKN03, CH+01a, CH+01b, Des00b, DK05, FP01, JK02, J006b, KCJ+01, KMZ03, Nov01, PV06b, Poi00, CHH+09, KG09].

Chosen-Plaintext [DN02a, KM01c, KI01a]. CHW [CHC04, CIA [Mah04, Ris06].

Cincinnati [BD08]. Cinematic [CAC03].

Cipher [AIK+01, BKR00, BS02, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DRS05, DF07, Dwo03, EYCP00, FF01a, Flu02a, G05a, GBM02, HJC02, H01, KYH01, KH01, LKH09, MSN07, NP01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY+02, SXY01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BV+04, GPX08, Han04, Hey03, KH08, Kid00, LKH+08, Mac00, PSP+08, RBB03, Sal00b, SHH07, WW08, Win05b, WF02, XH05].

Ciphers [AAG+00, BBKN01, BS00b, BR01, BKM07, CvTMH01, Can01b, CF01b, Can06b, CJS01, Ch02, C02, CP02, CM03, Con03, DPV01, E05, Fi00, FF01a, Fil02, Gol01d, Gol01e, HR00, HR04a, HSH+01, Jam00, Jan06, Can01, KCP01, KKG03, LRW02, MV00, On01, PP06a, Pli01, RMS05, Sar02, SM03b, SKU+00, Wal00, Wri05, ??02, YG01b, ZC00, Bai08, Bar06a, Bel07a, Ber07, Bod99, DLP+09, DY01, DS09, Dun06, DK08, Egh00, GP06, HW03a, HWR09, Hey03, JK01b, Jun05, Kat05a, KSW00, Kin01, LMS07, LDH06, Lun09, Max06, M90, MWM01, Pin06, SHJR04, SK03, Sm01b, SL07, SB05, TT00, Wag03, Yi00, You06, Kat05b].

Ciphertext [BBK03a, BCH07, CKN03, CF01b, CS07c, CH+01a, CH+01b, CS02, CS03b, Des00b, DK05, FP01, JK02, J006b, KS00a, KY01a, KCJ+01, KMZ03, Kur01, Man01, Nov01, PV06b, Sho00b, BW05, CHH+09, IM06, KG09, Paul00].

Ciphertext-Only [BBK03a]. Ciphertexts [AF06, BGW05, BGN05, Gen04b, J00a].

Circuit [EHK+03, GSS08, HR05, MG08, KS05b].
Circuits [BI05a, FML+03, Gol03, ISW03, MD05, PBTW07, You01, GLC+04].

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

CISC [FLY06]. citizens [Ano03a]. claims [DS00].

clamping [Ano03a]. Clandestine [Wri05].

Class [Car02, KM01a, KKH03, NN06, OP01a, Phi01, SBZ02, DKL00b, Fox00, HM00, Uni01]. Classes [CY02, RSA00c]. Classical [BYJK08, Gav08, GW00, LW05b, NA07, BYJK04, JZ09]. Classification [HMS04, PBD00, Uni01].

clauses [SV08a].

cle [RSA09a]. Cleaner [TR09a, TR09b].

Cleaning [Lut03]. cleanup [Lov01]. Client [ANRS01, Ano01e, ANL01, FSSF01, PS05, WKB08, Bad07, HTJ08, LF03, YS04].

Client-Server [ANRS01, PS05]. client-to-client [HTJ08]. Clients [JRFH01, RKZD02, WLI06]. Clinton [Gen00a]. Clip [FGL02]. Cliques [PQ06].

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

Clocked [CGFSH09, MH04]. Close [DM07b]. closing [Lau08b, FWGP03].

cloud [CS09]. Clouds [GS01, VS01].

Cluster [Höf01, KCD07, SEF+06, TCL06, TW07]. Cluster-Based [KCD07]. Clusters [MFS+09]. CM [CMKT00, GHK+06]. CMS [BWL02, DKU05]. Co [Bud00b, Nd05, ACM01b].

Co-Design [Nd05]. Co-operation [Bud00b]. Coalition [ACJT00]. Coalition-Resistant [ACJT00].

coarse [Rhi03]. Coast [Boy01]. Cod [IEE05b].

Code [Ark05, BKR00, BR04, CD00b, CV03, Cer04b, FIP02a, FF01b, HSZ01, Imm03, KY01e, Lai08, OS09, Re01, Rey01, Sal00a, Sin02, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HLO3, KS04, Lev01, MMJ05, Mnl02, Ros00b, RSA09a, SM00c, SM05, SM07a, Sin99, Sin00, Swe08, AAG+00, SE01]. Code-based [BR04, OS09, BGB09].

Codebook [CTH08, YWWS09, WJP07].

Codebook-linked [YWWS09]. Codebreaker [Han03, Pin06]. Codebreakers [Bec02, Gan01b, Gas01, HS01a, Kah67a, Kah67b, Kah74, Kah96].

Codebreaking [Bud00a, Bud00b, Sin01b, Alv00, Bud02, Cop05, Cop06]. Codebuster [Ano04d]. codec [Che08a]. Codes [LLR07].

Coded [MLC01]. Codes [Bee05, BP06, Big08, Bod99, BQR01, CC09, Chu02, CDG+05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ??02, YYYD01, Yek07, Bel07a, aSM01, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HRW09, Kov01, Lam07, Lun09, Min03, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02].

codeword [AJ08]. Coding [Buc00a, CS05c, HHL+00, Joy00, LLL+01, MZ02, Pat03b, RK06, Sal05c, Sma05, TW02, TW06b, Ytr06, Che07a, DW05, Gar04, Hon01, PPV96, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sea05, Sea09, TW05, Irw03].

Coefficients [CH01b, KT00]. coffin [Rie03].

Cohen [Was08a]. Coherent [TPPM07].

Coin [Lin01c]. Coin-Tossing [Lin01c].

Coins [HR04b]. Cold [HSH+08a, AJ08, HSH+08b, HSH+09].

cold-boot [HSH+08a, HSH+09].

collaboration [ED03, PCS07, SBG05, SBG07].

collaborative [LLY06]. collapse [SBB05].

Collection [GMM08, Bro05a]. Collections [Kuh00]. Collective [BBB+02]. collide [GNP05].

Collision [DG02, IK05, MS09c, WYY05a, WYY05d, GM00a, Sem00].

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

Collusion [BGW05, HNZI02, Zan01]. Cologne [WKP03].

Color [CTL04, Che07a, Che08a, CTY09, FGD01, AEE05b, CO09a, CDD07, Yan02, YCL07].

Colorado [BC01, Sch04b, USE00d].

Colored [CDD07]. Colossus
LHS05, RS08, Sal07, SDFH00, WWL\textsuperscript{+}02, WC03a, FS08, Gar04, Laf00, Lj05a, Sch00a, Sch01c, S\textsuperscript{+}03, Sch04a, Sch04b, Sch05a, TTZ01, Zir07.

**Compression-Encryption-Hiding** [BD03].

**Compromise** [Ahm08, Lai08].

**Compromised** [ZYN08].

**Comput** [McK04].

**Computability** [Pet08].

**Computable** [Vad03].

**Computation** [ACS02, Bai01b, BCL\textsuperscript{+}05b, BI05a, BIM00, BJLS02, CC00, CDM00, CDG\textsuperscript{+}05, CDI05, DN03, DI05, DM00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, KO04, KLML05, KSR02, Lin01c, PS05, WW05, Ano02g, AB09, BE200, BEZ01, CLOS02, CLC08, CD00, DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WHH05, WW05, Ano02g, AB09, Kra07, SWR05, MC04].

**computation-efficient** [CLC08].

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

**Computationally** [MPSW05].

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

**Compute** [MFS\textsuperscript{+}09].

**Computed** [FBW01].

**Computer** [BS03, Bis03b, Bro05a, BCDH09, BC01, CSW\textsuperscript{+}08, CC02a, Coc03, HY0205b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, frr00, JBR05, KM07, Lte06, Lut02, MYC01, MS05b, MAC\textsuperscript{+}03, Nie02d, RC06, SB07, Tyn05, Cas02, Che05b, DFGH04, Fau09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Shu06, SL06, SE01, dCdVSG05, GKS05, dCdVSG05].

**Computer-Science** [Coc03].

**computerized** [LMC\textsuperscript{+}03, Pau02b].

**Computers** [Coc03, Ett02, TSS\textsuperscript{+}03, Cop05, Cop06, Heg09, RH00].

**Computing** [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW\textsuperscript{+}01, BBDK00, CGH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Ltt03, May04, PHM03, Sch06b, SKG09, SCF01, Sim02, SEF\textsuperscript{+}06, Sta03, TLC06, VH09, Ver02, WC01a, Wri00, Yan00, YKMB08, Cha07, Che05c, CHT02, DHL06, HV09, HKPR05, LMC\textsuperscript{+}03, MI09, PP03, PP07, Raj06, RP00, Sei05, WHH06, Wil99, YLR05, Lut03].

**Compueware** [Ano02d].

**conceal** [BB79].

**Concealing** [DMS00].

**Concealment** [DA03].

**Concept** [ARC\textsuperscript{+}01].

**concepts** [AB09, Kra07, SWR05, MC04].

**concerning** [HW03b].

**Concurrent** [BP02, DPV04, Gen04a, KKG03, Ros00a, Ros06a, Dam00].

**Conditional** [LMV05, WN02].

**Conditions** [IKO05].

**Conference** [ACM03a, ACM04a, Ano06b, AAC\textsuperscript{+}01, AJ01b, Bel00, B\textsuperscript{+}02, BZ02, BS01b, Bli03, Bla03, Bon03, Boy01, Buc00a, CC04a, CV04, CGP03, CGH\textsuperscript{+}00b, Cra05a, DKU05, DFCW00, DFPS06, EBC\textsuperscript{+}00, ELV00, FLY06, Fra01, FMA02, Fra04, FLA\textsuperscript{+}03, HR06, HY05b, IEE09a, IKY05, JYZ04, JMc03, Joy03b, Jue04, KJ05, Kiloa1, Kino2, KN03, Knu02, Lai03, LL03, Lee04b, LTT\textsuperscript{+}04, LL04c, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Nac01, Nao04, Oka00, Oka04, Pat03b, Pen01b, Pfl01, Poi06, Pre00, Pre02c, RD01, Roy00a, Roy05, Sho05a, Sil01, SM07b, Sma05, Syv02, USE00c, USE00a, USE01b, USE01a, USE02c, Wil99, Won01, Wri03, Yun02a, YDKM06, JZ04, Zhe02b, ZY03, AUW01, BC05c, DV05, DWML05, DR05, Hon01, Kil05, Li05, PC05a, PY05, PPV96, QS00, Son00, WK06].

**Confidences** [Gan01a].

**Confidentiality** [Dwo03, Pen01a, YC08].

**configurable** [MBS04].

**Configuration** [Sha02, Mos06].

**Confirmation** [SK00].

**Confierner** [CM00, GM03].

**Confiication** [DBS01].

**Conformance** [LBR00, RSA00c].
MPSW05, SKQ01, TEM+01, Gar04].

**Correctness**

[PBD05, Bel07b, HSD+05, dH08].

**Correlated** [FWW04].

**Correlation** [BSC01b, CJ01, Gol01c, JJ00d, LV04, LMV05, MH04, Nyb01, SY01a, WRW02, ZC00, GG05b, JJ02].

**Correlations** [KM00, KM01b].

**Corruption** [XNK+05].

**COS** [FF01a, WB02].

**Cost** [CDF01, FBW01, PD07, Sta05, YEP+06, CL09, SHJ04, SK03, YLR05].

**Cost-Eective** [PD07].

**Cost-ineffectiveness** [YLR05].

**Could** [Min03, Cla00b, Pau02b].

**Count** [Che07b].

**Counter** [DIS02, QS01, SLG+05, SL06, MMJ05].

**Counter-Measures** [QSO1].

**Countermeasures** [PP06b, SK05b].

**Countermeasure** [IT03, MMT09, OT03a, PKBD01, YKL02a].

**Countermeasures** [Ava03, Fry00, GM00b, MOP06, OST05, Has01b, JDJ01, Man08, OST06].

**Counters** [KMO01].

**counterterrorism** [Na05].

**Counting** [Gau02, Kuh00, Hig08].

**Couple** [SXY01].

**Courses** [Gha07].

**Cover** [GA05, Gut02a, LNP02, NN03, RS00].

**coverage** [DS00].

**Cropping** [SDFH00].

**Crowd** [Fox00].

**CRT** [FMP03, Kuh02a, May02].

**Cryptanalyses** [HW03c, Kan01, SKU+00].

**Cryptanalysis** [ASK07, AMRP00, And03, An07b, An07a, BDG+01, Bao04, BLH06, BP03a, BKK03a, Bar06a, BP01a, BD00a, Bih00, BFMR02, BDK02a, BDK02b, BSW01, BDD03, BD00b, BCCN01, CGFSG09, CV02, CC01a, CC01b, CL01b, CY05, CKY05, CKK+02, CJT01, CJT03, Cho06, Cho08b, CHJ02, CP02, Cou04, CGJ+02, DG00, DGP07a, DGP07b, DG09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Fin06, Flu02a, Flu02b, Fru01, Fru02a, Fru02b, GS07a, GM02a, GJS01, GS02c, GM02b, GBM02, GC00b, Graf02a, GS09, GKN+08, HPC02, HQR01, HAU04, H504, HLL+01, HSM+02, HK+04, Hsu05a, HLH00, Hwa00, JN02a, JN02b, Jou09, Joy03a, KM02, KW03, KS00b, KRY05, KW02, KRS+02, KSK00b, K02a, KC05, Kii01, Kii02b, KHKL05, LC03, LHL+02, LP03, Lee03c, LKY04, LL05a, LR07, LB01, LB02].

**Cryptanalysis** [LLH04, LL05c, LLCL08, LW05c, MS03a, May02, MG01, MHL+02, Mort05, NPV01, PSC+02, PKH05, Piel04, Pei06, Pha06, PH06, PS01c, QC05a, Sch06a, Sci04, Sha03c, Sha05a, STK02, SGB01, SGK08, SKE01, SHH07, TIGD01, TM06, TLH05, TJO1b, XSS+03, Wag00, Wag03, WLT03, WL05, WBD01, WBD02, Wu02, XWL08, XY04, YSD02, YW04b, YW05, YKL02a, YKL02b, YRY05a, YYY05a, You01, YG01a,
YG01c, ZYR01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, AMRP04, BF01a, Bai08, Bar09, BS01c, Buo06, Buo09, Bur02, CV05, CKN06, CKL+03, Dun06, Egh00, EBS01, Eke09, Fie09, GPG06, Goo00, Jun05, KSWH00, Kuk01, LMSV07, Max06, MAaT03, MAaT04, MAaT05, MAaT06, MAaT07, Nyb01, Pha04, RSQL03, Rup09, SK01a, Sel00, Sin09, SL07, SCS05b, SSL+00, Swe08, TC00, TM01, WLW04, WF02, YI00, YJ00, cryptanalysis [YKLM03, Kat05b].

Cryptanalyst [Wil06].

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

Cryptic [Wri05].

CRYPTIM [Ust01b].

CRYPTO [Fra04, Men07, Sho05a, Ahm08, Ano01j, Ano03f, Bao01a, Bao01b, Bur01, CC0501, CNB+02, Lev01, Lev02, Mar08a, Mar02b, MC04, Pem01b, SYLC05, TR09a, TR09b, Yun02b, Bec02, BK05, HGN03, Web02, Bel00, Bon01, Kil01a, Yun02a, Seio00a].

Crypt-algorithms [Ano01j, CCM01].

Crypto-based [MC04].

Crypto-CCS [Mar02b].

Crypto-integrity [Yun02b].

Crypto-systems [Ano01j, CCM01].

Crytoanalysis [HSIR02, LD01].

CryptoAPI [Bon00].

Cryptoclub [BP06].

Cryptocomplexity [Rot05, Fal07].

Cryptocprocessor [HV04].

Cryptographer [Joy03b, Nac01, Oka04, Poi06, Pre02c, Men05].

Cryptographers [Coc03, Heg09, KLN+06, Tsa07, Bel07a, Hau03].

Cryptographic

[AC02, AADK05, AL00a, Ano09c, Adh+07, Ase02, BLST01, BDF+01a, Bar00a, BGK+03, Bih03, Bia01a, Bor01, BDP02, Bra01b, BM01c, BLO8, Bur06, CC04a, Car01b, Car02, CDP01, CHL02, CKY07, CB01, Cra05a, CS09, C0909b, DD02, DMR07, DFM04, D00, DVN01, DHR00, DV08, DFG01, FIP01b, FS00, Fis01a, FGM00a, Fri01, GMP01a, Gar05, GS080, GGG05, G010d, G02, GTH02, Gor02a, GL00, GUG01, Gut00, Gut02b, Gut04a, HTS02, HN06, Har06, Has01a, HL05a, HC08, Ig02, IY00, Ito01, IMM01, JT05, KMO01, KY01b, KY02b, Kil01b, KS06a, KS09b, Knu02, Kus02, Law09a, LN08, LS05a, LKJ01, MS02a, MOP06, Mea01, MNP01, MRL+02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Nao03, Ndm05, Ngu05, Nie04, OTIT01, OPO1a, FKB01D, FRO8, PZDH09, Pem01b, Pf01].

Cryptographic

[Pin02, Pin03, PS02b, Pot06, Pre00, Pre02a, Pre02b, RSA00d, RSA01, RR00, RRS06, Rot01, RSN+01, SM00a, SS01a, SGM09, Sha02, Shp03, Shy02, SFDF06, SWV00, SR06, SL09, TLY04, TWA08, TBD01, Uzu04, WK03, WN02, WBL01, WC01b, You01, Zha08, AMRP04, ACT05, ALV02, AV04, BGB09, BDSV80, Bla01b, BP05, BG08, BG09, BDNN02, BD04a, BGL+03, BM06, BR05, Can01a, Can06a, CHC04, Coh03, CC05d, CDL06, DP04, Dug04, DFG00, FS03a, FSG01, GT00, GPV08, GJ04, GM04, GB09, HW03c, HY03, IK03, IK06, IYK02, IYK03, JW01, KAM08, KS05b, KP03, LMT05, Lau05, LLW05, LLW09, ML05, Mea04, MT07, Mic02b, MRST06, Mon03, NN03, NdM04, NdM06, PS04a, PSG+09, PR05, Pre07, Puc06, QPV05, Reg03, Reg04, Ren09, RMH04].

Cryptographic

[RBF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, TNG04, kWpLwW01, WLW04, XLM06, YLT06, ZLS09, ZWWL01, ZL04b, dH08, BWB02, JQ04, KKP02, KP01, KNP01, RS05].

Cryptographically

[ADD09, AH05, BJB02, BFC08, BB00b, FR08, MS02b, RGX06, Ano03, AW05, AW08, Lau08a, SM03a].

Cryptographically-masked [AH05].

CryptoGraphics [CK06].

Cryptographic

[ANS05, AADK05, AL00a, ANo09c, Adh+07, Ase02, BLST01, BDF+01a, Bar00a, BGK+03, Bih03, Bia01a, Bor01, BDP02, Bra01b, BM01c, BLO8, Bur06, CC04a, Can01b, Car02, CDP01, CHL02, CKY07, CB01, Cra05a, CS09, C0909b, DD02, DMR07, DFM04, D00, DVN01, DHR00, DV08, DFG01, FIP01b, FS00, Fis01a, FGM00a, Fri01, GMP01a, Gar05, GS080, GGG05, G010d, G02, GTH02, Gor02a, GL00, GUG01, Gut00, Gut02b, Gut04a, HTS02, HN06, Har06, Has01a, HL05a, HC08, Ig02, IY00, Ito01, IMM01, JT05, KMO01, KY01b, KY02b, Kil01b, KS06a, KS09b, Knu02, Kus02, Law09a, LN08, LS05a, LKJ01, MS02a, MOP06, Mea01, MNP01, MRL+02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Nao03, Ndm05, Ngu05, Nie04, OTIT01, OPO1a, FKB01D, FRO8, PZDH09, Pem01b, Pf01].
BBGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BWBL02, Bla02b, BDDS03, Bon00, Bon07, BPR01, Boy03, BLM00, BK06b, BKM07, Buc00b, BD08, BO1b, BRTM09, CPS07, Cer04b, CCL09, CSW08, CQS01, Cop04, CFA06, Cop00, Cor06, Dr00c, Dam07, DFS08, DD00, Das08, DDF04, DKO02, Des02, DT03, DY09b, DSS01, DDN00, Dre00, DP08, EPP07, EP05, Ell04, ECG07, Ett02, FS03b, Gal01, Gal02, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Grit01, Gro05, HR06, HH04.

Cryptography
[HHM01, HMV04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irm03, IK06, IK09, JYZ04, JLO0, JTO1b, JTO1a, Jue04, Kao06, KLR09, KZ07, KG07, Kat05b, KK06, KMB09, KPMF02, KWD06, KY01c, Kir01a, KMS02, KM05, KSZ02, KS03, KWP06, Lam01, LG01, Lee03b, LLL01, Lie05, LDM04, L05b, LP02b, Lut03, Lys08, MN00, MP02, Mao01, Mao04, MZ04, Mao01, MAA07, MB01, Mr09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pel06, PM02, PBB02, Poi02, PTO6, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS05, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sth02a, SGK08, Sti95, Sti01, Sti02, Sti06c, SJ05, Syv02, TS00, TW06a, TG04, TMM01, TW02, TW06b, Tro08, TR09a, TR09b].

Cryptography
[Uni01, U02, YY01, VMC02, WPS01, Wei04, WK01, Wei05, Wei00, WV02, Wri00, YW00, YW06, Y06, Y01, YDK06, ZY03, vDW04, Imr03, AMW07, AN03, AU01, An02a, An02g, AB01, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bal03, BD00, BCD06, BEZ00, BEZ01, BGM04, BEM07, Buc00a, Buc01, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CTO08, CJ03c, CDFM05, CDD07, Cos00, Cre00, DD04, Diff01, DIM08, DwW05, DOPS04, DKL09, DW09, Duh03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK07, Geb04, GRTZ02, Gol09, GG05b, GHT05, GPS05, GNP05, HH05, HHL00, He03, HKPR05, HA00, Hig08, HKS00, Ho05, HG05b, HLW09, IZ00, IM06, JK01b, Jan08b, Joy00, KZ03, KL08, Kat01, Kil05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Lin01a, Lop06].

cryptography
[Mau04, May01, Mc08, MBS04, MM07a, Mol07, NP02a, Nis03a, NH03, Opp05, OS09, PP05, PY05, PC09, PC00, Pin06, Pip03, Reg05, Reg09, Rot02b, Rot03, Roy00b, Rup09, ST07, Sch02, Sch04d, SBZ04, Ser06, SH05, Shp09, Sil05, Sin03, Sin00, Sma04, ST01d, SK01b, TW05, UHA09, Van03, Van05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wri03, YC09a, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Rec01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08, Ros00b].
cryptography-based
[FXAM04].

Cryptologic
[BS00a].

Cryptological
[Lew00].

Cryptology
[W01b].

Cryptologists
[BD00].

Cryptography
[Bar02, Bon03, CG07, CCO04a, Cr07, FLY06, Fra04, JM03, Kn02, Lai03, LL04c, L02, MMV06, Neu04, NS01, Ng01, Oka04, Poi06, Rot05, RS02, Sha03b, Zhe02b, dL00, Bao00, Bao02a, Bau07, Bel00, Bib03, Boy05, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam91, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, P05a, Pi01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sh005a, Son00, Wao01, WK06, Yun02a, vT00, DWML05].

CryptoManiac
[WW01].

Crypton
[CKK02, MG01].

Cryptosystem
[BST02, FL06, GG01, GK05, GHW01, Hug02, KM01a, KY02c, KLC00, LHT09, dV06, Luc02b, NSN05, NBD01, Ove06, PH04, YG01a, YG01c, Zhe02a, Zho06, Bao04].
CL02b, CCH04, Che05a, Cho06, CFVZ06, CHH01, Dan02, DHL06, EKRMA01, GH04SS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04b, LL06, LKYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SP02, SCS05a, SP79, SLC05, Sun00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, YC09b, hY08].

Cryptosystems
[Aki09, Ava03, BDG +01, BKLS02, BPS00, BMM00, CHSS02, CCW02, DDG +06, DKXY02, ESG +05, FJ03, Fel06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, Kl01b, KM04b, Kos01b, LZO4, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWG03, ST01a, SKQ01, SKG09, Ste01, Vad03, Wya02, XB01, ZLK02, Ban05, BF06a, BB79, CHC01, CMKT00, EBS01, EHKK04, GH08, GBKP01, HM00, Has00, Has01b, Hih00, HP01, KW00, Kos01c, LD01, Luk01, Mic01, Mis06, OS00, Pei09, PLJ05b, SSST06, Sha05c, Sma01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WV00, YY00, ZSZ01, vT01].

Cryptovirology [YY04]. CRYPTREC [IY00]. CSCW [ZP05]. CSP [SB09]. CT [Joy03b, Men05, Nac01, Oka04, Pei06, Pre02c, ZC09]. CT-RSA [Joy03b, Men05, Nac01, Oka04, Pei06, Pre02c, ZC09]. CTO [Ano03f]. CTS [Con00]. Cuban [AJ08].

Cube [DS08, PDMS09]. Cube-Type [PDMS09]. culture [Gil07]. Cumulative [LG04, WP03]. cure [RD09]. cure-all [RD09]. Current [DFH01, PRS04, LPW06].

curriculum [FOP06]. Curve
[ANS05, ADI09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BMN01, CQS01, CFA +06, GPP08, HY05a, HM01, HV04, HM02c, JT01b, JT01a, KRM09, KPMF02, KSSZ02, WPW06, LW02, Mj02, Kir03, OTT01, OS01, PWG03, PEL06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, X01, YY01, ZLK02, BSS04, BSS05, BG04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWinW05, EHKH04, GBKP01, Has01b, Hsu05a, HL05d, JW06, LL04b, LWL09, Mis06, OS00, ST03a, SSST06, SH05, Sma01, SCL05, SLC05, TC05, Van03, Ver01, Wol04, WPP05, YC09a, YC09b, ZSZ01, ZL05, vT01].

Curve-Based [KWP06, Pel06]. Curves [AHR08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK +06, Kid02, PWG03, Ver02, CMKT00, Hus04, LWZH05, MP01b, MSV04, Sil05, Sim02, SC02b, Was08b, Wen03, Yas08]. customer [Lin01b]. CVS [DFG01]. Cyber [FNRC05, WW04, Man05].

Cyberinsurance [BP07]. Cybersecurity [PLW07]. cyberspace [Mit02]. cycles [ABHS09, BP07]. Cyclical [YY04]. Cyclic [PF05, Mic02a].

Czech [MJ04].

D [Duw03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05].

D.R [Ir03]. dad [Che05b]. demons [Mos06].

Damgård [CDMP05]. dark [Br09].

darkening [CDD07]. DARPA [Coe01a].

Data [ACM03a, ACM04a, ABM08, Ano02a, AAC +01, BGHP02, B +02, BS00b, BNPW03, Bro05b, Che01a, CTLLO1, DBS01, EBC +00, Elb09, FMA02, FLA +03, GA05, GMM08, GTTC03, HLL +02, Ken02a, Ken02b, Kus02, Lan00b, LLRW07, LP00, LHS05, LS08, Lut03, MND +04, MS03b, MFS +09, NM09, OS05, Per05a, RKZD02, RK06, Sal03a, Sal07, Sin01a, SK03, SDMN06, TZDZ05, TPPM07, VDKP05, WS05, WW02, WN02, kc01, vw01, AM06, AG09, Ade09, AHK03b, AIXS04, Ano02c, Arn01, Bla00, BN08, CCMT09, Cer04a, CO09a, CLR09, CPG +04, DZL01, DGMS03, FS04, HILM02, LLK05, MJ03, Mal06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S +03, Sch04a, Sch04b, Sch05a, SGPH98, SETB08, WMDR08, YLC +09, YC08, ZSJN07, Zir07, Cur05, DK08, Lin02, Pap05]. Data-Hiding [VDK05]. data/image [Sch00a, Sch01c, S +03, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, B105a, BBPV00, KS02,
SVEG09, Gal02, HILM02, Mau04, PS08b, PBVB01. database-service-provider [HILM02]. Databases [AK02b, CDM+05, DN04, AHK03a, CDD+05, CKY07, GA03, MSP09, MNT06, NS05b, ÜGO8, YPPK09]. 
Datamining [DN04]. Datenverschlüsselung [Lin02]. David [Gas01, Pap05, Bar05, Eag05]. Day [SE01, CSW05, Win05c]. Days [Adl03, Riv03, Smo04]. DC [USE01c]. DCT [BSC01a, BSC01b, CH01b, KT00, LY07, LSC03]. DCT-Based [LY07, LSC03]. DDH [Lys02]. DDO [LK+08]. DDO-64 [LK+08]. Dead [Gutt02a, deaf [Pau02b]. Dealer [DK01, Sun00a]. Dealing [BH00a, BC05b]. Debate [Jo01, Mad00]. 
Decimalisation [Kus02]. 
Deciding [An02d]. Decoding [An02d]. Dec [IEE09a]. decades-old [Lov01]. December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, La03, Lee04b, LLT+04, Li05, MM06, MS02e, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b]. 
Decentralized [MSP+08]. deception [CS07a, Mah04, MS02d]. Decidability [Kü02]. Deciding [Bau05]. Decimal [BJv02]. Decimation [BF00a]. Decipherable [aSM01, Sav04]. Deciphering [Eri02, KB07, Ark05, Lov01, NS01a]. Decision [DJ06, GR04, KM04a]. Decisions [CU01]. Decoding [KY02b, LB02, LB02, Ral00]. AGKS07, Bal09]. decomposing [FP09]. Decomposition [BR09, CL04c, SC02e]. decompositions [vDKST06]. Decomrelation [CLL00, Vau01]. decrypt [Bii02]. 
Decrypted [Bau00, Bau02a, Bau07, MB01]. 
Decryption [Bar00b, BST02, CS03a, CCD07, FPS01, HGNN+03, Int00, KCJ+01, Ano08a, Che01e, DZL01, GH08, Mil03, OS07, Shp04b, SWH+09, Wli09]. Decryptor [TPS01, Zol01]. DeCSS [Coc02a]. Dedicated [ISO04]. Deep [CMS08]. Defeating [CSK+08]. Defective [BTTF02, Dav01b, Dav01c, KLR09]. 
Defending [NRR00, Pro01]. Defense [GK02, HW01, Mir05, Wy05, Bol02]. defenses [SL06]. defined [Yas08]. Definition [YWD08, SNI00]. Definitions [Uni01, AH05]. Definitive 
BS01a, BS05, BSB05, Gar03b, defying [HRS08]. Degenerate [Ber09a]. Degradation [BSC01a]. Degree [CV02, QPV05]. 
Degrees [Sat06]. Déjà [DP00]. DeKaRT [Go03]. Dekker [Irw03]. Delacorte 
Imr03. Delay [WRW02, NS01a]. Delayed 
JM07. delegated [CL04c]. Delegation 
WN02, ZP05, MW06]. Delhi [JM03, RM04]. Delivers [An02e]. Delivery 
[NZC05, RMC01, DY09a, NZS05]. Delphi [TEM+01, Hei01]. Demand 
[BD03, CMB+05, SEF+06]. Demilitarized 
[Kum07]. Democracy [CZB+01]. Democracy [CTBA+01]. Demography [Coc03]. Demons [Mos06]. demonstrably 
HL06. demystifying [RR04]. Deniability [Pas03]. Deniable 
[Nao02, CCK04a, CSK+08, DG05, LC05b, YRY05c, Zha06]. Denial 
[Mah04, Nik02a, Nik02b, PKBD01, Ril02, Mir05]. Denial-of-Service 
[Nik02a, PKBD01]. Denmark 
[Cra05a, TJ02]. Denver 
[ACM01b, Sch04b, USE00d]. Department 
[Bo02, Eri01]. Dependable 
[NAB03, And08b]. Dependent 
[Go03, WS05, BPS08, SK03]. deployed 
[BD00]. Deploying [BH00b, GSB+04]. Deployment 
[CL07, KDO01, Mur01, Sin01a, App05, JRR09]. Dept [Uni01]. 
Depth [BII05a]. Derandomization 
[BOV03, BOV07]. Derivation [DGH+04]. Deriving [BJP02, CV05]. DES-encrypted [Bii02]. DES-like
Describing [Lav06, MH05]. Descriptors [DNP07, SP04]. Design [Abd01, AADK05, Ano02e, ADD09, AIK+01, ARC+01, Bar00b, Can01b, CDP01, Cim02, CB01, CS03b, CMB+05, CLZ02, DR02a, DR02b, DS09, DF07, EHK+03, FF01a, FZH05, GSS08, Gru04, Gut04a, HRL09, Hro05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04b, LB05, MKP09, MP00, Nd05, NSS02, Rhi03, STJ09, SPG02, SRLQ03, Uzu04, WZW05, WW08, WLLL09, ARJ08, Ade09, CMS08, GGG05b, Gut04c, HC04a, Htu01, KSF00, MI09, MWM01, SVEG09, YCW+08, YC08]. Design/CPN [AADK05]. designated [LV07]. Designing [HBC+08, TCR03, C+02, CG05, Lan00c]. Designs [Bee05, CC02a, Bai08, Des00a, WL07a]. Desktop [Mun08, BDET00]. Desmedt [CHH+09]. Desynchronization [CDTT05]. Detached [Sha01c]. Detailed [Lut03]. Details [Scr01]. Detect [FOBH05]. Detecting [CMS09, FGD01, JQYY01, Har07a, LHL04a]. Detection [AS01b, AD07, BB00a, BK07, CH01b, CZK05, JT05, KG03, SQ01, SY01a, SLT01, ST01c, TZZD05, TMM05, WG05, YI01, Zan01, Bej06, BBK+03b, HLL+02, Men03, NN02, WMS08, WW06, ZGTG05]. Detection/Correction [SKQ01]. Detector [BSC01b, DNP07]. Determined [KKH03]. Determining [KS03, LQ08, OS07]. Deterministic [BK06a, Her06, KZ03, KZ07, May04, BK07]. dev [BH05]. Developers [Ano06c, Dew08, MK05b, Nis03a]. Developing [MV03b, Cra05b, Gal02, HL06]. Development [Ano02e, CNB+02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a]. Developments [Ano03f, Pre07, Sha04a]. develops [Pau02b]. Deviates [Ran55, Ran01]. Device [Ric07, ST03b, WPS01]. Devices [BCH+00, CFRR02, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KH01, MV01, MRL+02, SCF01, WC01a, Ano06a, CMS08, CF07, DMT07, SCF09, Tse07, YC09b, ZYW07]. Devil [Bla01c]. DFT [Che08a]. DH [Lys02]. DHIIES [ABR01]. DHP [MSV04]. Diablerets [Van05a]. Diagnosis [Ano04b, BK06b, XNK+05]. Diagnostics [NM09]. Diagonal [PJJH01, PJK01]. Dickson [SZP02]. Dictionaries [AGT01]. Dictionary [BPR00, BCP02b, CS07b, DJ06, Pho01, NS05a]. did [MH09]. Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01a, Sch04a, Sch05a, USE00b]. Dies [Bar00a, Coc01a]. difference [PBMB01, dW02]. Different [LS08, WWTH08]. Different [CGMM02, Sna01]. Differential [Ava03, BMM00, BF00a, BFR02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eke09, Fur02a, Gra02a, HLL+01, HSM+02, HHK+04, IIT03, JT01a, Kan01, KM02, KCP01, LHL+02, MP06, MM09, MHL+02, MG08, PSC+02, PQ03b, SK01a, SNE+00, SKI01, YSD02, vW01, BF01a, CUS08, Che08a, DLP+09, Egh00, EBS01, Pha04, SSL+00, TM01]. Differential-Linear [BDK02a]. Differentials [BF00b]. Difficult [Bud00b, MT02]. Difficult-to-pass [MT02]. Diffie [Jan08a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02b, BCP07, CY08, CU01, CJ03a, CTKRT08, FS01b, GR04, Kil01b, KKK04a, Kra03, Kra05, Mi08, Tsa06, YRY05c]. diffuse [Wal04]. diffuser [Ger06]. diffusing [She01]. digest [MSP09]. Digits [KWP06, Tan07a, BG09, HKPR05, Kir01b]. Digital [ANS05, AvdH00, AR00, AS08, Ano01f, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00b, CCH05, CC09, Che01b, CFS01, CMB02, CMB+08, CZB+01, CGJ+02, DSP01, EIG01, Eng00, EHK+03,
HSZI00, HSZI01, Han00, HS01b, HHGP+03, HW01, HTL01, JBR05, KZ01, Ka01, KC02, Kuh00, Kwo02, Kwo03b, LZZ+01, LLL+01, Lin01b, LWL09, LL01, Lu03, Mad00, MM01a, MM02, Mch01, PL01, PJO01, PCG01, PZL09, PBM+07, Ram01, RdS01, RS01, San09, Sch00d, Sch06b, Scr01, Sha01e, SC02a, Shi08, SLT01, Suy01, TMM01, TJC03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wn01, WV01, WC03a, WC04, Wys02, XZ01, XYL09, YWWS09, YY01, ZWC02, Zhao2, ZCW04, XAPP07, AA08, Ano00i, Ano01, Ano01, Ate04, BLH06, Bra01a, Ca00a, CS08a, CWH00, CL00, C105, Che07a, Che00b, Die00, FB01, GGK03.

digital [Gil07, HRL09, HLC07, HLH00, HHC05, KP00, LG04, LG09, Lev01, LLC06b, MKY08, NRR00, PC05b, PLJ05a, PBV08, QCB05b, Ree03, Sha01d, Sha04b, Sha05d, SCL05, TCC02, TN0+09, U005, W008, WHL03, WC05, XC05, XMST07, Ano09b, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].

Digital-Audio [NY09].

Digital-Signature [Eng00].

Digits [Che04b, Ran55, Ran01].

Dimension [DDG+06, TZT09a, TZT09b].

Dimensionality [SGB02].

dimensions [CLR09].

Dining [KLN+06].

diplomacy [Alv00].

Direct [BMW05, KG09].

directional [PJK01].

directions [Sha01b, DFH01].

directly [JZCW05].

director [Mad04].

directories [C+02, Pet03].

directory [C+02].

disabled [Pau02a].

Disappear [Per05a].

Disappearing [Way02b, Way09].

disappointed [Ste00].

Disaster [WC05].

disciplinary [SM08].
disclosure [JM07, Swi05].

disclosure [B09, HLL+02, SBG07, SGA07].

Discrete [CS03a, CNS02, Che04b, CCW02, Gen00b, GV05, GP08, KC09b, LW02, LJJ05, VK07, HN04, HW03a, HWR09, Hsu05a, HU05d, JJ03, JLL01, LHL03a, LHY05, LTH05, PLJ05a, QCB05a, Sch01e, Shao5c, Shao5d, SWR05, SCL05, SLC05, SCS05c, Y08].

discretized [MA02].

Discription [Har07b].

discursive [Mit02].

Discussion [Ano01a, Ano01b, Ano01c, Ano01i, Ano01j, Ano01e, Ano01k, KLB+02a, Mal02, Nik02b].

Dishonest [GKK07].

disjoint [Gut04c].

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

dismantles [Hil06].

dispatches [Kee05].

displayed [CGV09].

Displays [Kuh02a].

Disputed [CAC06].

Distance [CGFSG09, CPIX04, DM07b, DW01].

distinguished [HWW04, WH02b].

Distinguishing [HR+01].

Distortion [BGI08, CS05c].

Distortion-Free [BGI08].

Distortions [HH09, SDF01].

Distributed [BCS02, BT02, CLK01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJKR03, GSV02, GTH02, LLY06, SCF01, WT02, And08b, AF06, BDE00, C009b, FMY02, KKL09, LN04, LLW08a, S0+08, PS08a, Raj06, WZ05, YbJ04].

Distribution [BDF+01a, BOH+05, BBB+02, BS0000, FS01b, Ina02a, Ina02b, Ku02, LL02, NA07, Sch01a, Y01, AST04, AS04b, Bad07, CYP04, GL06b, MP08, SLP07, Shp01, Shp04b, SY06, WH08, Y04, ZLG01].

Distributions [CY08].

diversity [Kun01].

Divide [SKQ01].

Division [HZS05, KKY02, Tan07a, Che08b, MN14].

Divisor [KM01a].

DL [HLR09, PLJ05b, Sch01f, Sch01e, WMDR08].

DL-based [HLR09, PLJ05b].

DL-encryption [Sch01f].

dL-keys [Sch01e].

DL-STDMD [WMDR08].

DLP [MSV04].

DM [Eag05].

DNA [GPX08].

DNF [BGN05].

DNS [Her09b, Kle07].

DNS-based [Her09b].

do [Bur06, HSR+01, HR04b, Win01, BB79].

Dobby’s [Dr.00c].

Document [ISO05, PJ01, ST01c, VHP01, CDS07, CL04c].

Documents [PJK01, AW05, AW08, DGK+04, GA03, ÚG08].

Does
[AB01, Pie05, Con09, Wal04]. Doing [BM01a]. Dolev [BPS08, BDNN02, ZD05]. Domain [AS08, Bar00c, BSC01a, BSC01b, BSL02, CJK+04, Cor00b, Cor02, DOP05, DN07, GW01, ISSZ08, Kuh02a, Lan00d, LZ01, MM01a, OMT02, PBC05, SOHS01, SDFH00, ZLK02, BR06, CS05a, DSP01, EKRMA01, Zir07]. 

Domains [BR01, CLK01a, CLK01b, Vau01]. Domingo [CKN06]. Dominic [Rot07]. Dominica [PY05]. don’t [Win05c]. Don’ts [FSSF01]. DONUT [CLLL00]. Door [SF07]. Doors [Eri02]. DOS-Resistant [Ano01e, ANL01]. Double [ADDS06, CY08, CMJP03, Coc02a, DIM08, GH08, GB09, Hau06, JSW05]. double-base [DIM08]. Double-Gate [Coc02a]. Double-Size [CMJP03]. double-trapdoor [JSW05]. Doubling [FV03]. Douglas [Spr03]. Down [BBPV00, Coc02b, Ano00g, Ano03c, Ano03a, Pot03, PBVB01, Ste05c]. Downwards [FV03]. DPA [SGB01, TV03]. DPA-Based [SGB01]. Dr [Ano03f]. Dr. [Dr.00c]. drafted [Sug03]. drawn [vOT08]. DRBG [Hir09]. Dress [Ahn08]. drinks [Ano03c]. Drive [NP07, Kor09]. DSA [MR01a, SA02, Sha01d, TvdKB+01]. DSA-type [Shah14]. DSEA [LLLZ06a, LLLZ06b]. DSP [Geb04, WWGP00]. DSP-embedded [Geb04]. DSPs [WWGP00]. DSS [Ano09b, Ano13, FIP00, Nat00]. DTD [PCK02]. Dual [HLC07, KHY04, LK05, SF07, WC09, ST03a]. dual-field [ST03a]. Dual-Pair [WC09]. Dual-Tree [LK05]. Dual-wrapped [HLC07]. Dumb [Eri01]. Dummies [Cob04]. Dump [KCJ+01]. 

Dunaynir [MAaT05], d’une [Car00]. Durahim [MAaTxx]. Durahyhm’s [MAaT04]. during [AJ08, Bec02, WA07]. Dust [KGS07]. Dutch [dl00]. Duty [ZGLX05]. DVD [Gei03, Per05b]. Dwork [DNRS03, GK05, Zha06]. DWT [LHS05, PBC05]. DWT-Based [LHS05]. Dynamic [AFB05, BNP08, BCP01, BCP02a, FM07, CL02a, CW09, CCD+04, CTT07, GTH02, HQ05, Pat01, Sug03, TT01, BB+02, GL06b, HW03c, LCP04, LLV06, LCK04, LCC05, RG05, Yi04]. dynamic-key [LCP04]. dynamics [BGP02, shC09, JL07, MR00]. dynamics-based [shC09, JL07].

E-business [Poh01, HHSS01]. E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01]. E-Goods [NZCG05]. e-Government [RM02]. E-Learning [CAC06]. e-mail [Che01f, LL04b, NZS05, Smi03, All06, ANR01, KS00a, Law05]. e-mails [LG09]. e-payment [Has02]. E-Security [NDJB01]. E-smart [AJ01b]. E-Vote [Che07b]. e-voting [CJT03, Cha04]. E-Wallet [ET00]. E0 [LV04]. E2 [SKU+00]. Early [ASW+01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Cal00d, Smo04, ZG05]. Easier [Pau09]. Easy [GR04, Hos06b]. Eavesdropping [Kuh02a, Kee05]. 

ebanking [WDCJ09]. eBook [Ano02d, WWL+02]. EC [SF07]. ECC [BWBL02, CL09, Mis08, Ts05]. ECC-based [CL09, Ts05]. ECC2K [LM08]. ECC2K-130 [LM08]. ECCV [MJ04, TBJ02]. ECDSA [ANS05]. Eclipse [Coc02b]. ECMA-305 [ECM00a]. ECMA-306 [ECM00b]. economics [Ble07]. ECPP [Che03]. ed [Gum04, Nis03a]. Edge [St05]. Edinburgh [RS05, PEN01b]. Edit [CGF09]. editing [MAtx]. Edition [Cho08a, Irw03, Spr03]. Editor [Eri01]. Eri02, FOP06]. Editors [BK06b, PTP07, SJT09, SGK08]. EDK [Ano02e]. Eds [Duw03, Pag03]. Education [Puz04, RC06, CAC03]. Effect [AEV+07]. Effective [CDR01, PD07, Sen03, SL06]. Effects [BBG08, Ha00, GJ04, SN07].
Efficiency [III00, GGKT05, SLG+05, GT00, GGK03, KT06, YTH04]. Efficient [ACS02, ABRW01, AEMR09, Bai01b, BINP03, BKL02, BR00a, BGHP02, BSDV08, BGR+03, BS00a, BF01c, BGH07, BB00b, BCDM00, CKPS01, CL02a, CCMT09, CCD07, CL01b, CPX04, CM05a, CTJ02, Ch08a, CJL05, CT08b, CKK03, Cou01, Dan00, DN03, Dhe03, FF00, Fis05, FS01c, GLV01, GC01b, GTH02, GST04, GBKP01, HCJ02, Has01a, HS00, HW04, HZSL05, HL07, Hüh00, HS07, Jua04, KOY01, KOY09, KLY05, KH01, KHK03, LSY01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, BM01, Nd05, NSKN05, OS01, PC03, PB00, Ram01, RSQ03, RDJ+01, SM01, SW06, SRQL03, SSGS00, Tsa08, TC05, WHL05, WYY05d, WH01, WC01a, XB01, XS09, YW08d, YLH05, Zan01, Zho06, ACTZ05, AFB05, Bla01b, CC04b, CC05c, CY05, CH05, CLC08, DS09, Dew08, DwWmW05, FP09].

ecient [FSGV01, HHG06, HC04a, J06, LPV+09, LLS+09, LCK04, LLH04, LYC02, Mic02a, MSP09, NR04, PCC03, RG05, RB03, SL07, SK+07, Sha05b, SC05a, WK05, X01, YTW05, YC09a, ZS05, YWZ07].

Eciently [IKNP03, NNT05, AGK07]. eort [Weh00]. eorts [Pau02a]. Eggs [Wei06, Wei05].

EGPGV [MFS+09]. Egypt [EB0, IB02, ELvS01, IEE01b]. Eighth [ACM06, B+02, ELvS01, IEE01b]. Einstein [MNT+00]. EJB [TEM+01]. Ekert [Duw03]. El-Gamal [EKRA01]. Election [JLL02, Cal00b]. Elections [Cha04, PV01]. Electrical [Wal04]. Electromagnetic [SGM09, QS01].

Element [MS02d]. Elementary [Sin09, Ste08, Tatt]. Elephant [Fer06].

Eleven [All03]. ElGamal [BJN00, CL02b, CWH00, HL04, LHT09, J00]. ElGamal-like [CWH00, HL04].

Ellis [Coc01a]. Elmau [IEE01b]. Else [FL01b].

clude [Che01f]. EMA [QS01]. Email [ES00b, Gar03a, Her09b, Luc06].

Email-Based [Gar03a]. emanations [ZIT05]. Embedded [An01c, A02a, DR02, BGM08, Dri02, DV08, GSS08, J05, JQ04, KP02, LPW05, ND04, RS05, SPQ06, WKP03, YS+01, AR08, BGM04, FO04, GB04, KV+09, KP01, KNP01, KP03, MBS04, N03a, TKP+08, XQ07, F02].

Embrace [CNB+02]. Embracing [An03c]. EMD [BR06]. Emperor [Sm01b]. Empirical [HW03b, Goo00]. empirically [SS03].

Emptiness [DIS02]. Emulex [CZB+01, CTB+01]. Enabled [For06, CCGY01, DY09a]. Enabling [Web02]. encapsulation [CHI+09, KG09].

Encipher [BR00a]. Enciphering [HR03]. Encode [HH03].
[BR00a, BKN04, Ano08c].

**Encode-Then-Encipher** [BR00a].

**Encode-then-Encrypt-and-MAC** [BKN04]. **encoded** [WMS08]. **Encoding** [JT01b, RS00, Lin02]. **encounter** [Win05c].

**Encountering** [Wol03]. **Encrypt** [BKN04, BTTF02, Dav01c, Pet05, Dav01b].

**Encrypted** [BBK03a, BGHP02, BGLS03, CD01b, Hug04, Lan04a, WRW02, Whi09, Woo00, AMB06, Ano06a, Bih02, BNP08, CCMT09, CDD05, CSK08, FJ04, HILM02, Hes04a, LHL04b, LSH00, MW04, Pet03, ÜG08]. **Encrypting** [Pro00, RC01, Zho06]. **Encryption** [ABC05, Abe01, AS01a, Abe04, AP09, AB01, ADR02, Ano01f, Ano01g, Ano01h, Ase02, ANR01, AFI06, AF03, Bar00c, III00, Bau02b, BN00a, BR00a, BMM00, BBDP01, BU02, BF01b, BF03, BB04, BGW05, BCHK07, BH07, BPR08, BB03, BNPW03, BD03, BKY02, Bur03, Cal00d, Cal00e, CD00a, CS03a, CHK03, CHK05, CGHF01, Che01a, CTLL01, Chi08e, Cho08a, CMR06, Cla00a, Coc02b, Coc01b, CNKP00, CHJ01b, CDN01, CS02, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DFK03, DK05, DS05b, Dri02, FIP01a, FL01a, GC01a, GSW00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HSH08a, HS02a, HYZ05a, HSH02, HSH06, HKR01, HWW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03, HL02]. **Encryption** [HGNP03, HLL05, HLC08, ISSZ08, Joh03, Jol01, JK02b, JK02c, JM02, JKRW01, Jut01, KBD03, KSHY01, KSO0a, KY01a, Kha05, KKJ07, Kos01a, Kra01, Kur01, KDO4, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LLRW07, Lin03, LNP02, LM05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, Mö03a, Mor05, Mü01a, MS09d, NISO0, Nam02, NZCG05, NZS05, NP02b, Nie02b, PV06b, PM00, Pau09, Pem01a, PZL09, PDM09, Pha04, Por01, PS00, Pre01, RM04, RK06, RJD08, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQL03, SPGQ06, SBZ02, Sy0e, TV03, Uni00a, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Ust01b, VMSV05, WZW05, WBRF00, Wri01, YEP06, YW06, ASW00, Abd01, ABHS09, AKSX04, AMRP00, ABW09, Ano00a, Ano00c, Ano00f, Ano00g, Ano00h, Ano00j]. **encryption** [Ano02a, Ano03f, Ano06d, App05, Ate04, ACD05, AFGH06, BPS08, BKN04, BR04, BBN09, Ber09a, BBK03b, Bir07, Bla00, BJN00, Bro05b, CG06, CS08a, CBSU06, CHC01, CRKRT08, DZL01, DL07, DR05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GG03, Gen09a, Gen09b, GKM00, Gou09, Gua05, Gut04c, HSH08b, HSH09, HS02b, HYY07, HCD08a, HCD08b, HAU04, HWW02, Hsu05a, Hwa05, HL05c, HL05d, IM06, JK01a, JK01b, JW05, JSW05, JZCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Kü08, La00, LV07, Lee01, LPC04, LJD05, LMC03, LLL06a, LLLZ06b, LLC08b, LB05, Lu02, Lvd05, LK01, LKW05a, Mad04, Marin, Mat02, Mü01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pan03, RGO1, Rho03, RBB03, RSP05, SN00, SKW07, Sch00a, Sch01c, S03, Sch04a, Sch04b]. **encryption** [Sch05a, Sch01d, Sch01f, SR00, SVEG09, Sh04b, SK03, Ste00, SP03, SWH09, Tan01, T01, TOE00, TM01, TLH05, Uni00b, UP05, VSK09, WG02, Wei00, WN95, Wol03, WH02a, XY04, Yan02, YG05, YZEE09, YC07, ZLG01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CHKO08, CHJ01a, RR04, Uni00f, Wue09, Jan08a].

**encryption/cipher** [HAAU04].

**encryption/decryption** [OS07].

**Encryptor** [LMP01, TPS01, Ano00a].

**Encryptor/Decryptor** [TPS01].

**Encyclopedia** [Bid03, vT05].

*End*
[KCD07, Per03, SKKS00, WWGP00, YSR01, AMB06, SU07]. 
**End-to-End** [YSR01, AMB06]. 
[End] [Küs02]. 
**Endomorphisms** [GLV01]. 
**Endpoint** [Kad07]. 
**Enemies** [DM07b]. 
**Energy** [GC01b, Ino05, LPV]+09, SLP07, Mis08]. 
**Energy-efficient** [LPV]+09]. 
**Energy-security** [Ino05]. 
**Engineer** [Pau02b, SN04]. 
**Engineering** [CNB]+02, MNT00, MYC01, Pem01b, Roy00b, SM07b, TR09a, TR09b, VH09, And08b, EC05, Jen09, Man08, Wal04]. 
**Enhance** [ZWC02]. 
**Enhanced** [JKRW01, LHL04b, ZGLX05, CZ03, McK04, OP01b, TWL05, WH05, ZSM05]. 
**Enhancements** [ADH]+07]. 
**Enhancing** [BDK02a, MS05a, SE09, Sun00b, 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, An03d, 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, LSVS09, IM06, KKL09, KB00, Rh03, Whi09, ZBP05]. 
**Environmental** [PS05]. 
**Environments** [CJ04, LKHL09, BM04, MNS08, SBG05, SBG07, SN04, YC09a, YbJf04]. 
**ephemeral** [Mis08]. 
**Ephemeron** [Per05a]. 
**EPOC** [QY01]. 
**ePOST** [MPHD06]. 
**EPR** [Ina02b]. 
**Equation** [FJ03]. 
**Equations** [CP02, DDG]+06, GS03, PBMB01]. 
**Equipping** [DMT07]. 
**Equitability** [DBS01]. 
**equivalence** [Fis01a, LQ08, MSV04]. 
**Equivalent** [Fer00, KOMM01, May04, SIR04]. 
**Era** [MP00, Uni00c, Bur00, Uni00f]. 
**erasure** [PCS03]. 
**Erasures** [JL00]. 
**ERP** [LSZ05]. 
**Erratum** [AGGM10, Kwo03b, LLLZ06a, MK04]. 
**Erroneous** [CH01b, MNT]+00]. 
**Error** [BBK]+03b, BQR01, Din05, KKG03, LW05b, LM02, MLC01, MPSW05, MZ02, NN06, SKQ01, YI01, YD01, ZRY01, Zo01, Gar04, LHL04a, YW06]. 
**Error-Correcting** [NN06, ZRY01]. 
**Error-Prone** [MC01]. 
**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, Irw03]. 
**establishing** [Kov03, KH03]. 
**Establishment** [BM03c, NIS03b, HMvdLM07, LF03, SL05a]. 
**Estimation** [EFY]+05, JX05, KLB]+02a, LNL]+08, Sel00]. 
**ethical** [Har05b]. 
**Euclidean** [CPLX04, CMJP03, CLZ02, WL02]. 
**EULA** [WWL]+02]. 
**EUR** [Eag05]. 
**EUROCRYPT** [Bh03, CC04a, Cra05a, Tin01, Pre00, GJSS01]. 
**Eurographics** [MFS]+09]. 
**Europe** [Pag03]. 
**European** [AL06, CZ05, GKL04, Pre01, dCdVSG05, Ano00f, Che08b, Die00, Pre02a]. 
**EUROPKI** [AL06, CZ05, GKL04]. 
**EV** [HTJ08]. 
**EV-C2C-PAKE** [HTJ08]. 
**Evaluate** [Pre02a]. 
**Evaluating** [BG05, NTW07]. 
**Evaluation** [BSC01a, EYC00, FS00, FSL]+03, IM00, NY00, J000a, Kan01, Kir03, SKKS00, BZP05, FXAM04, FS03a, LCP04, MCH05, RC05, RN00a, RN00b]. 
**Evaluations** [LM02]. 
**Evangelizing** [Coc01a]. 
**evasion** [Blu09].
even [Biih02, OS00, Win05c]. EventGuard [SL05b]. events [SB90]. ever [Fur05]. Everlasting [DR02d]. Every [Che07b, TH01, DKK07, Win05c]. Everyone [Han00]. Everything [CTBA+01]. Everywhere [Ber00]. Evidence [Ver01, Bro05a, HW03b]. Evolution [DF01, Ree01, Pat02a, Ros00b, SP02, Sin99, Sin00]. evolutionary [LMSV07]. Evolved [LMHCETR06]. Exact [Cor00b]. examines [Nis03a]. example [Bla00, GC05, Zir07]. Exchange [BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DGY03, DLY08, GL03, J08, KOY01, KY03, MPS00, Mac01, MSJ02, Ngu05, VPG01, W01, WV01, ZW01, BBG02, BCP07, CLC00, CWJ01, DG06, GL06a, GMR05, HTJ08, KS05a, KOY09, LHL04b, LW04, LFHT07, LHC08, LSH00, MS03a, Mis08, WLH06, YC09a, YPKL08, ZYW07, CPP04, CP07, ECM00b]. exchanging [KN08]. Exclusive [GRW06]. Executing [HILM02, LJ05a]. Executive [Des00c]. Existing [MV01, BDET00]. Expanded [Cho08a, Irw03]. Expanding [DN02a]. expansible [LLW08a]. Expansion [DN02b, BCD06, HKPR05]. expansions [HKPR05]. Expected [KL05, RK06, DLP+09]. Experience [Sas07, BCHJ05]. experiences [MPHD06, USE00b]. Experimental [BG09, CGBS01, ÖOP03, WS02, RSQL03, Sm040]. Experimentation [Hun05]. Experimenting [LSVS09]. experiments [Bru06]. expert [An01g, Che05b]. Expiration [MP00, Sch05b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOBH05]. exploitation [Eri03, Eri08, KV09]. Exploiting [CK06, ETMP05, HR00, HM04, ZWC02]. Exploits [MJF07, CSW05]. exploration [SKW+07]. Exploratory [Lut03]. Exponent [BP04, BM01b, DN00b, May02, SZ01, CKY05, Duj08, GD05, Shp04b]. Exponential [BYJK04, BYJK08, CY08, GKK+07, GKK09, Shp05]. Exponentiation [KKH03, SK07, CTR08, HGNS03]. Exponents [FS02, FS01b]. export [An00h]. Exposed [Gum04, MSK03, SSS06]. exposing [YY04]. Expositive [MAaT05]. Exposure [BM03b, DSS01, KZ07, CDD05, KZ03]. Exposure-Resilient [DSS01, KZ07, KZ03]. expressions [MW04]. Extended [ABDS01, BPS00, CM00, Con04, DIRR05, HLvA01, HL00, MSJ02, MP02, OST05, Wag02, BJN00, CD00a, HT04, HP01, Mis06, Pei09, QPKV05, LKJL01]. Extending [ADD06, IKNP03, Ove06, Sal03b, SS01a]. Extension [Bai01a, YWD08, BR06, CMdV06]. Extensions [ABC+05, BBG08, CS07c, HM02b, Rot02a, Wei04]. Extracting [Cer04a]. Extraction [DHG+04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lu02, Vad03, DW09, KZ03, Sha04a]. Extraordinary [Top02]. Extreme [Ree03, An002d]. Extrusion [Bej06]. Eye [Sas07, CAC03]. Eye-Opening [CAC03].

F5 [Wes01]. Face [KZ09, NH02, PK01, SBG02, TZZ09b, PY08]. FaceHashing [TNG04]. Faces [NS01c, Ngu01]. facets [Rot02b, Rot03]. fact [An03f]. Factor [DN02b, Sas07, BSSM07, Hen06b, Sch05c, St.00, Ste05a, YW0D08, dBo07]. Factoring [BN02, KY02a, KLM02a, KOMM01, May04, PV06b, ST03b, LTH05, LCZ05c, Mi01b, PLJ05a, QCB05a, Sha03d, Sha05d, ZLC05]. Factoring-Based [PV06b]. factorisation [GG08]. Factorization [CDL+00, Lam09]. Facts [GO03]. Fad [CAC03]. Fail [JQYY01, SNSG00]. Fail-stop [SSNG00]. Failures [DFG01, HGNP+03]. Fair
[CC00, DLY08, GC01a, JLL01, JL04, LMS05, PS00, VPG01, WV01, LSA+07, MS03a].

Fair-Zero [LMS05]. Fairness [GCKL08].

faithfulness [GTZ04]. False [ZSJN07].

Falsification [OM09]. Fame [Bar00c].

Family [CQS01, Flu02b, NPV01, SK05a, You1, Ber07, FNRC05, GKP01, MP07].

Fan [YRY05c]. Fare [GMG00].

Fascinating [Sch09]. FASME [RM02].

Fast [AL00b, ABM00, BDTW01, BST02, CJS01, CC06, CQS01, Cor00a, Cou03, Cro01, FS02, GC01a, GD02, GMM01, GPC08, HG07, HR04a, JJo0d, KKIM01, KK03, KKJ+07, LSY01, LS05b, MSNH07, Kir03, NS05a, NSS02, OKE02, OT03b, PG05, RR02, Tsa06, UHA+09, Yan05, ABB+04, BMA00a, BMA00b, BMA00c, JAW+00, JJo2, Lud05, PBMB01, WW01, Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d].

Faster [Bar00c, CMJP03, GLV01, KS09a, LVo04, Oec03, Ban05, Why05].

faszinierende [Sch09]. Fat [MYC01, TvdKB+01].

Fault [Ano04b, BMM00, BK06b, BMK07, DS03, Gir06, PV06a, PQ06b, WL07b, YKLM02b, HGR07, Lin07, P06, RMH04, YJo0, YKLM03, ZL04a]. fault-based [YJo0].

Fault-Tolerant [WL07b, HG07, Lin07, RMH04]. Faults [GS00, VS08]. Favre [MFS+09]. FBI [Mad04].

FC [Bla03, Fra01, Jue04, PY05, Syv02, Wri03].

Fear [Hei03, Sec04, Sty04, Sch03].

Feasibility [APV05, BDET00]. feasible [LM08].

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

February [DR02c, Fra01, GH05, Joh03, Jue04, Gil05, Kin01, Men05, NPa02a, Nao04, Oka04, PY05, Poi06, Pre02c, RM04, Syv02, USE02a, Wi99].

Federated [DeL07, GTY08]. Feedback [CGFSHG09, CM03, Cou03, Igl02, Hey03, SPG02]. FeedForward [BP01a]. Feel [PM00]. Feeling [Buh06]. Feistel [Cou04, Kan01, LMSV07, Oni01, Pat04].

Feldman [AF04b]. Ferrer [CKN06]. Fetal [MYC01]. fetch [HTW07]. Fi [Sty04, Bar03]. Fiat [VS08].

fiction [Ano03f]. FIDES [ISTE08]. Field [FJ03, GC01a, RDJ+01, CKY07, GMG00, Has00, JL03, ST03a].

Fields [Bai01a, BT02, CU01, Che04b, CQS01, BFS05, HCK09, HHM01, KKH03, Lov01, MN01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Simg0, Sma01].

Fifth [ACM03b, SM07b]. Fighting [DGN03, SZ03]. File [CCDP01, GIS05, Ito01, LK01, BDET00, CSK+08, HTW07, H0s06b, ISO05, MKW00, MPG08].

Files [T00, CHe02, Lov01]. Filesystem [Bau02b, Pet05].

Filesystems [Bau02b]. Filter [LBGZ01, LBGZ02, MSNH07, Sar02, CMS08].

Filter-Combiner [SB02]. Filtered [MH04].

Filtering [SDH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00].

Finalists [EC00, ICM00, IK00, IK01, Mes00, Mes01, SKK00, SW00a, WW00].

Finally [Coc02b].

Financial [ANS05, G00, Pen01b, Wri03, Bla03, Fra01, Jue04, PY05, Syv02]. Find [IH07].

Finding [HR04b, MP06, WY05b, WYY05c, ZT03, SW00b].

FINDSOMECOM [Gra98]. Fine [SS01b].

Fine-Grained [SS01b]. Fingerprint [Ano02d, HH05, HBF09, KHY04, MM02, CL04d, MJ03, UBE09].

fingerPrint-based [CL04].

Fingerprinting [KT01, CTT07].

Fingerprints [TK03, KLY03, Sco04].

Fingers [MM02].

Finite [BLST01, BR01, CU01, Che04b, CQS01, HCK09, HW05, KKH03, MM07b, PHK+01, RS08, Ver02, Gar04, Has00, LMC+03, LQ08, NS01a, RMH04, Sma01, SLTB+06, TC00].

Finkenzeller [And04]. FIPS [Nat00].

Firewall [LJY04]. firm [Zaf00]. First [Bar00a, BBD09, Coh03, CM02, CMB+05, FLY06, KGL04, KS06b, MNP01, Nao04, PUB01].

Firmware [Zaf00].
NNT05, ÖOP03, PK03, QSR +02, Roy00a, USE00b, Wil99, ZJ04, ZYH03, AJ01a, Cla00b, Coc02a, DV05, LBA00, RH00, Uni00b, Uni00f, Uni00e, Uni00h, Lan00a.

First-order [Coh03, KSN06b]. Fish [Fie09, Wei06, Wei00, Wei05]. Fit [CCM05]. Five [SW00a, MS02b, Rot02b, Rot03]. Fix [TEM +01]. Fixed [AR01, BCCN01, CKN00, LS01a, Shp04b, SP79]. Fixed-Length [AR01, CKN00]. Fixed-Pattern [BCCN01, LS01a]. Fixing [KZ07, KZ03]. FL [Des02, Jue04], flash [ST06, SGB01]. Flat [SV08a]. Flaws [Gra02a, SPMLS02, Vau02, SL05a]. Flexibility [LP02a]. Flexible [CMG +01, CLK01b, DGK +04, OT03a, Tsa01, BA06, KC05, LHY02, WWA01]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM +09]. Flows [ECM00a, AHS08, Cer04a, Lau08a]. Flying [Fox00]. FOCS [IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07], foes [Rie00]. FOKSTRAUT [BH00a]. Foo [Puz04, VGM04]. Food [MNT +00]. Fool [RW02]. Footsteps [Lav06]. force [Cur05, SGA07]. forces [AJ08]. Ford [Mar05a]. Forecast [Rai00]. Forecasting [WWL +02]. Forensic [PS08b, Cas02, Kor09]. forensically [ME08b]. Forensics [JBR05, CS04, CS08a, CDS07, MS09a, MKY08, MAC +03]. Forest [FBW01]. Forgery [CH01a, CCM00, LS01a, SUT01, HSW09]. Forgotten [Eng05, Kin01, OC03]. Form [AD09, CH07c, OS01, LKLY00, Mic01]. Formal [GBG09, Bel07b, BCH05, BJC +06, CLO5, DKS08, GOR02b, HG03, Lan00d, Mea01, YWD08, ABHS09, JW01, Mea04, Pau01, SW02, ZLX99, ZL04b]. Formalizing [HM01a]. Formally [BJP02]. format [ISO05, RG05]. format-string [RG05]. Formation [RW03a, Luk01]. Formats [GIS05]. Former [Mad04]. Forms [JT01b, LLL04]. Formula [Kog02]. Formulae [CH07b, WPP05]. Formulas [BGN05]. Formulations [AHRH08]. Fort [SM03]. Forum [CZB +01, CTBA +01, CNB +02, CMB +05]. forums [Hi06]. Forward [AR00, AFIO6, BY03, CHK03, IR01, HCD08a, HCD08b, SY06, ZYW07]. Forward-Secure [AR00, AFIO6, CHK03, IR01]. Forward-Security [BY03]. Forwarding [KCD07, Kra02b]. FOSS [Bo02]. Found [Bar00a]. Foundation [Lut03]. Foundations [DKK07, Gol01b, Gol01a, Gol04, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Nie02d, Sal05d, Kat05b, Puc03]. Founder [Bar00a, Ano03f]. Four [LXM +05]. Four-Layer [LXM +05]. Fourier [Che07a, DSP01, DNP07, KC09b, LP06, SP04]. Fourteenth [USE00c]. Fourth [ACM02, ACM05b, DFCW00]. FPGA [Ano02e, CC02a, CGBS01, CG03, CNPQ03, EYCP00, EHKH04, KMM +06, KY09, KBM09, KRS +02, LP02a, MM01b, MM01c, OTIT01, OOP03, Pat01, PBTW07, QSR +02, TYLL02, TPS01, USS02, WW00]. FPGAs [AD07, DPR01, MMT09, RSL03, SGM09, SK05a]. Fractal [AA04a, JLS03, WCC03]. Fraction [Wal03]. fractional [DSP01, SS06]. fractions [Dan02]. Fragile [CC09, CH01b, CT09, Nak01, PJK01, LYL07, SY01b]. Frame [LHS05]. Frames [HHW05]. Framework [ANRS01, GL03, GOR02b, Hum05, NMO05, NP07, PS06, RS00, Shy02, ZYN08, AHK03b, Ayo06, CCCY01, CP07, CCC04, DMSW09, GJ05, GL06a, GM04, JEZ04, KNS05, MS09b, MBS04, YCW +08, HFF00]. France [ACM04a, ACM05a, AJ01a, AJ01b, GH05, KN01, NP02a, PPV96, KM07]. Francis [Bud06]. Francisco [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b].
Franz Steiner [Eag05]. fraud [Ano03a].
Fred [Bar00b]. Free
[AP09, Ano02e, Bau01a, Bau01b, BGI08, Coc01a, CNV06, DG02, HS00, HM01b, JP03, Jut01, Fox00, KS06b, SBG05, Bol02].
FreeBSD [Coc01a, Mu02, Siv06].
Freedom [Uni00a, Uni00e, Uni00d, Uni00g, Uni00b, Min03]. FREENIX
[USE01b, USE02c].
French [Wri03].
Frequencies [DD02].
Frequency [OMT02, Sak01, SOHS01, CS05a].
Frequency-Domain [OMT02].
Frey [Was08a].
Friar [GG05a].
Friendly
[CTY09, CRSP09, Hsu05b, HL05b, SZS05, WLT05a, WC03b, YW04b].
FrontPage
[WWL+02]. FSE
[Bi07, DR02c, GH05, Jou03, Mat02, RM04, Sch00b, Sch01d].
FTC
[Ste05c].
fuels
[Mad04].
Full
[Cor00b, DOP05, LKHL09, WYY05b, WYY05c, B104, CS08a, HS02b, LKH+08, Oiw09].
full-encryption
[HS02b].
Full-Round
[LKHL09, LKH+08].
Fully
[BL08, FSO1a, Gen09b, KPMF02, RG09, Gen09a].
Function
[BR02, CDMP05, Fis01b, Flu02b, GIS05, HNO+09, HPC02, J00a, Kan01, Ki01b, Nie02c, RB01, Yan05, CHY05b, C04, HR07, LW04, LPM05, Ta08, WWTH08, YW05, YRY05b].
Functional
[ECM00a, WA06].
Functionality
[ETM05].
G
[Coc03, For04, Was08a].
Gaitherburg
[SMP+09].
Gamal
[EKRMA01].
Game
[DHR00, LM02, CAC06, BR04, Go09, HCBLETRG06].
game-like
[Go09].

game-playing
[BR04].
Gamers
[MP00].
Games
[KN08, HCBLETRG06].
Ganesh
[For04].
Ganzúa
[GPG06].
Gap
[OP01a, PWGP03, RW03a, Sch02, Sch04d].
Gap-Problems
[OP01a].
Gate
[Cor02a, GC01a].
gates
[TWM+09].
Gauging
[PvS01].
Gauss
[KKH03].
Gaussian
[EKRMA01, JL03].
Gbps
[TPS01].
GCD
[JP03].
GCD-Free
[JP03].
GCM
[KS09a].
geeks
[Mc03].
Geheimschreiber
[Joy00, UW00].
GEM
[CHJ+01a, JMV02].
gems
[Six05].
General
[AB09, CDM00, DN00a, ESG+05, GMP01b, Kog02, Lin03, MND+04, Sal01a, YC01, HCBLETRG06, YI06, JL03, LJ05a].
General-Purpose
[ESG+05].
Generalisation
[DL04].
Generalizations
[LY01, HW02].
Generating
[BMK00, BCDM00, GG01, MFK+06, SS03].
Generation
[ACS02, BH05, BK06a, CS03c, ESG+05, GJKR03, GL01, GW01, JG01, MR01a, Ran01, TL07, TV03, WP03, WHLH05, Web08, WS02, Ano04e, BK07, BG08, BF01c, ISTE08, LS05b, TNG04, Van03].
Generator
[ADD09, BP01a, D105, Die03, DGP07a, DGP07b, DV08, EHK+03, Gen00b, GM02a].
Generators [BST03, BK06a, BL08, CF01b, CS05b, Fin06, Kra02a, LBGZ01, LBGZ02, LS05a, MH04, RSN01, Vav03, BK07, BGPGS05, CO09b, SK01b, Tsa06, YZEE09].

Generic [BN00a, DOP05, GGKT05, HLL05, Mar02b, MV01, GT00, MP08, Sch01f, Sch01e, XLMS06, CH05, SCS05a, WJP07].

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

Gennaro [Miy01].

Gennaro-Krawczyk-Rabin [Miy01].

gentle [RR03a].

Gentry [Hes04a].

Genus [CY02, GHK+06, Wen03].

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

Geometrical [LWS05].

geometry [PPV96, WW06].

George [Gum04].

Georgia [IEE09b].

German [Sch09, Ano04c, Lin02, Mor05, Sal00b, Sal00a, Win05b].

Germany [DRS05, Duw03, FLA+03, WKP03, IE01b].

Geschichte [Sch09].

Get [coc01a, WD01a, Cla00b]. gets [Bor00].

Getting [Kar02, PM00].

GF [BINP03, KPMF02, KLY02, KKY02].

GH [GHW01].

GHS [Hes04a]. giant [Lam07].

Gibson [Ove06].

Giesbrecht [CHH01].

Gigabit [CGBS01].

Gigabits [HTS02].

Give [CNB+02].

Given [Wal03].

Giving [Tee06, Wu01].

Global [Ahm08, LWS05, Por06, Ano00b, BK00, Kec05, KB00].

Globus [MJ01].

GN [SC05b].

GN-authenticated [SC05b].

Gnana [For04].

GNU [Coc01a].

GnuPG [JKS02, Sto06b].

GNY [Tee06].

Go [Bur06, CzB+01, HCBLTRG06].

Goals [PHM03].

Gold [Boy01, For04, Tsao07].

Goldreich [Kat05b, Lee03b, Puc03, AC02].

Gong [GG01].

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

Goodness [CMB+05].

Goods [NZCG05].

Google [Con09, Law09b].

Googling [Con09].

GOST [SK01a].

got [Car01].

Goubin [Sma03b].

Governance [TPPM07].

Government [IY00, RM02, Lev01, LCS09].

Governments [Ano00g].

GPG [Bau01, Bau01b, Luc06].

GPS [CKQ03].

GPT [Ove06].

GQ [BP02].

graduate [GV09].

Grafton [Pag03].

granted [Ano00h].

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

Graph-Based [CGFSHG09, HM02b, CTT07].

Graphical [vOT08].

Graphics [CK06, DNP07, MFS+09].

Graphs [NNT05, Ust01b, WGL00].

Gravvilenko [Puz04].

Gray [FGD01, Har05b].

Gray-Scale [FGD01].

grayscale [YCL07].

greatest [Bel07a].

Greece [ACM01a, KGL04, SM07b]. greedy [HKPR05].

Green [TR09a, TR09b].

GREMLIN [H01].

Grenoble [ACM05a].

grey [BDN00, SCS05a].

Grid [ACM05a, MJ01, SEF+06, TLC06, ZBP05, Cha07, CJK+04].

GridOne [YCO9c].

Grids [CTY09, MMPM09].

grip [Buh06].

Gröbner [CCT08, FJ03, Fau09].

Group [ANRS01, AAFG01, ACJT00, BBS04, BCP01, BCP02a, BCP02b, CD00a, CvTMH01, CH01a, HSHI02, HSHI06, HW02, Hug02, JP02b, KY03, Kin02, LZL+01, MSU05, SOO02, SWH05, Ste01, Ten07b, VMSV05, Wer02, AKNRT04, BCP07, CL04b, CYH04, CHC05, CWJ01, CTT04, Cha00b, ED03].

He03, Hen06a, HW02, KS05a, KPT04, KKKL09, LL06, LLH04, LPM05, LWK05b, NS05b, PQ03a, PQ06, RH03, SNW01, Sha05a, TJu01a, Tse07, WGL00, WHHT08, YLC+09, YY05a, ZC04, ZX04].

group-by [YLC09].

Group-Oriented [LZL+01, HW02].
GHz [Ano09a, BBK03a, BD00a, Cha05b, Cim02].

Guadeloupe [Wri03].

Guanajuato [Buc00a].

Guangzhou [LLT04, Li05].

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

Guest [KP03, Sak01, BK06b, MFS09, PTP07, SJT09, SGK08].

Gui [LG09].

Guide [Ano06c, BS01a, BSB05, BCP03, BP01b, HMV04, Poo03, Vac06, Wei04, Gar03b, Kvo03, Lun09, Mol05, SL06].

Guidebook [SEK01, SEK02].

Guided [ZY08, Pet08].

Guidelines [MMZ00, Die00].

Guildford [KN03].

Gummy [MMYH02].

Guo [LLLZ06a, LLLZ06b].

Gutmann [Uzu04].

H [Was08a]. H.R [Uni00d, Uni00h]. H.R. [Uni00a, Uni00e]. H64 [GMM01]. Hack [MYC01, Sin02, SL06].

hacked [Ano02c].

Hacking [Eri03, Eri08, Gnu04, Man08, MS03b, SRQL03, SGK08, TSO00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK*03b, DS09, EH04, HC00a, HBC*08, KP01, KN01, KP03, NdM04, RAF07, SOIG07, VS08, Wol04, YKLM03, YW06].

Hardware [Ano02b, Ano07b, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPs05, GLG*02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, ND05, PS01c, RS05, RS04, SOTD00, SMT01, SM02a, SRQL03, SGK08, TSO00, TEDL01, WKP03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK*03b, DS09, EH04, HC00a, HBC*08, KP01, KN01, KP03, NdM04, RAF07, SOIG07, VS08, Wol04, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07].

hardware/software [ARJ08].

Harley [WPP05].

Harn [GG01].

Hash [Ano08d, Ano12, AEMR09, BBK01, BRS02, BDS09b, Bur06, CBB05, Cor00b, Cor02, CDMP05, CS02, DOP05, FIP02b, FI02, GIS05, GLG*02, HPC02, HR04b, ISO04, Jou04, KMM*06, MD05, RRS06, RR08, RB01, SS01a, Sh00a, Sho02b, SK05a, WFLY04, Yan05, YZ00, BR06, DS09, KCL03, Ku04, KCC05, LLH02, LKY04, LW04, MS09, Mic02b, Ts008, W00a, YRY04, FIP02a, Z05a].

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

Hash-CBC [BBK01].

Hash-chaining [CBB05].

Hash-Function [BRS02].

Hash-functions [ISO04].

Hashes [Sch01a, GPN05].

Hasing [IK05, SGGB00, WS03].

HAVAL [WFLY04].

HAVAL-128 [WFLY04].
Horizon [Coc02b]. Host [Shu06]. hostile [ABB+04]. Hosts [Hsf01, SZ08]. Hot [IEE01b]. Hotel
[USE01b, USE01a, USE02a]. HotOS [IEE01b]. HotOS-VIII [IEE01b]. hours [Fox00]. House
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hsu [BCW05, HL05c]. HTML [CNB+02]. HTTP
[Zha00]. Huang [ZC05]. Huge [MSNH07, NNT05]. Hull [KMT01]. Human
[Dre00, GL01, JW05, KOY01, Man08, MS02d, RFR07a, RFR07b, RFR07c].

Human-Memorable [KOY01]. Hundred
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hunting [GJL06]. Hwang [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KCL03, IW05c,
QCB05a, WL05, YRY05d, ZYR01]. Hwang-Rao [ZYR01]. HWWM [LKY05c]. HWWM-authenticated [LKY05c].

Hybrid
[AD109, CBB05, KD04, LZ04, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hyderabad
[MS02c]. Hype [Way02a, Che01d]. Hyper
[DR02d, Lu02, PZL09]. Hyper-chaotic
[PZL09]. Hyper-Encryption
[DR02d, Lu02]. Hyperelliptic
[Ava03, CY02, CFA+06, HSS01, PWGP03,
Ver02, Was08a, ZLK02, CMKT00, Wen03,
Wol04, WPP05]. Hyperencryption
[Che01d]. hyperlinking [Che01c]. hypotheses [KW00].

I-tracings [RE02]. i.e [NP02a, Wi99]. IA
[WWCW00]. IA-64 [WWCW00]. IACBC
[JMV02]. IBE [ABC+05]. IBM
[AV04, ADH+07, CGH+00b, Web08, Web00]. Ibn
[MAaT04, MAaT05, MAaTxx, MAaT07]. Ibn-Adlan [MAaTxx]. Ibn-Al-Durahim
[MAaTxx]. iButton [HW01]. IC
[BGL+03, PC00]. ICBA [ZJ04]. ICCMSE
[SM07b]. ICISC
[Kim02, LL03, LL04c, PC05a, Won01, WK06]. ICISC’99 [Son00]. ICM [IEE09a, IEE09a]. ICs [Bar00c]. ID [Gui06, ZJ09, BRTM09,
CDD07, CL07, CS07c, CL00, GS02b, GTY08,
HC08, KLY03, KHL09, Ku02, LCS09, Sco04,
SW05a, SCL05, WBD01, WH02b, YCO09b,
YLM05, ZK02, ZC04, ZC09]. Id-Based
[ZJ09, CDD07, GS02b, HC08, Ku02,
WBD01, YLM05, ZK02, CL00, KLY03,
KHL09, Sco04, SW05a, SCL05, WH02b,
YCO09b, ZC04, ZC09]. IDE [An02d]. Idea
[Cos03, RR03a, CTL01, HTS02]. Ideal
[BTW05, BTW08, CDFM05, Lan00d, Gen09b]. Ideas [Gha07, Eri01].

Identification
[BP02, BLDT09, Gar03a, GLC+04, KK02,
Kir01b, Lys07, Sak01, SK06, Zhe01, And04,
Dul01, Fin03, PBV08, YCW+08, ZCO9].

identifiers [MC04]. Identifying
[HBF09, LLS05b, ZYO08, DMS07].

identities [Kwo02, Kwo03b]. Identity
[App05, BF01b, BF03, BB04, BCHK07,
BGH07, BPR+08, Boy03, BRTM09, CL01a,
CHM+02, Coc01b, DTM03, GKO4, Her06,
Her07, HY01, HL02, KC02, LCD07, Mar08a,
Mar08b, PCMS07, SMP+09, BW05, CG06,
CJL05, GG08, Gui06, KG09, LWZH05,
RG09, Sae02, Sha03c, Wal04, Wan04b,
Win05a, YCW+08, ZY007].

Identity-Based
[BF01b, BF03, BCHK07, Boy03, BRTM09,
DT03, Her06, HL02, KC02, LCD07, Mar08a, Mar08b, App05, Her07,
PCMS07, BW05, CG06, CJL05, KG09,
LWZH05, Sae02, Sha03c, YCW+08, ZY007].

IDSFM [TZDZ05]. IDtrust2009
[SMP+09]. IEC [ISO04]. IEEE
[BS03, BCD09, BC01, IEE01a, IEE02,
IEE03, IEE04, IEE05a, IEE05b, IEE06,
IEE07, IEE08, IEE09b, KM07, HSD+05,
Hug04, Mis08, PHM03, ZDW06]. IEM
[RC05]. IFIP
[DKU05, DFPS06, DFC00, ELvS01]. II
[Bau05, Bau01a, Bau01b, Bau01c, Bec02,
Bud00a, Bud02, Bau03, Kvo01, MH09,
OC03, Res01a, Res01b, Sal00a, ZT03]. III
[Sch00a, An00d, Bau03b]. IKE
I'll [PLW07]. Illinois [ACM04b]. Illusions [Koc02]. illustrated [Lun09]. Im [BGI+01, DOPS04, RR05]. IMA [Pat03b, Sma05, Hon01]. Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, CLT07, CC09, CC06, GW01, KB03, KC09b, LLS05a, L201, IWS05, LY07, LJ05b, LSC03, LSKC05, PZL09, RS00, SDFH00, SDF01, SSFC09, SYLC05, TTTZ01, TH01, TC01, UP05, VKS09, VK07, WY02, WL07b, YZZ09, AAP07, AA08, CC02b, CHC01, Che07a, Che08a, GSK09, HLC07, KC09a, LCLC08, Lin00a, LT04, LYG07, LLL06b, MS09a, MB08, PBV08, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, mSFL05, TL02, Wan05, WMS05, WC05, YCYW07, YCL07, ZLS07]. Image-Feature [GW01]. image-identification [PBV08]. Images [CTL04, CC08, CW09, DP00, FG01, LG01, LS08, PJ01, PBC05, RE02, WC09, WC04, YWWS09, AAP07, AEE09, BD00, FWT05, HHYW07, TCC02, TN09]. Imaginary [HJW01, HM00, Huh00]. Imbalanced [DDG06, YG01a]. Imbalanced [ZWC02]. Imbalanced [ZWC02]. Immersive [Coc01a]. Immune [CZK05, PZ02b, YKLM02b, ZP01, YKLM03]. Immunization [HR05]. Impact [Ber03, HGNP+03, JKRW01, MMYH02, Wri00, CS08a]. Imperfect [CPS07, DOPS04]. Impersonation [BP02, Hsu05b]. implant [Fox00]. Implement [HQ05]. Implementation [AD07, AG01, Ase02, Ash03, ARCO+01, BBD+02, CDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK+03, FW09, FB01, FD01, GC01a, Gir06, HT02, HLM01, JKS02, KMM+06, KMS01, KTT07, KRS+02, KV01, LP02a, MMZ00, MKP09, MM01c, MN01, MP01c, Mur02, Nov01, NMSK01, Ow09, OTT01, Pat01, PBWT07, QSR+02, RJJ+01, SM01, Sha01e, SK05a, SQRL03, USS02, Vir03, WZW05, WW00, WOL01, XB01, Zea09, BI04, BBK+03b, C+02, CNPQ03, DS09, DKL+00a, GHAG00, GKP01, Huh00, HP01, Hut01, KY09, LL04b, LCX08, LB05, Rh03, SM03a, SVDF07, Wol04, YW06, ZFK04]. Implementations [AL00b, BDP02, HP00, CTLL01, CG01b, EPP+07, GLG+02, MM01b, MP01a, RS01, WWCW00, ASK05, BFCZ08, BFGT08, BG07b, FR08, RAL07, RSQ03]. Implemented [TSS+03]. Implementing [Dwi04, Kor09, LMD04, MWS08, NDJB01, Pet03, Sni01a, SR06, C+02, CW02]. Implications [Kun01, LJ05a, MF01, Aya06, Bjo05, Fri07]. Implies [KY01e]. Imply [Pie05]. Importance [An02b, KCJ+01, TID01]. Important [SM00a]. imposed [XLMS06]. Possibilities [CHL02]. Impossibility [AP05, BPR+08, Fis01b, PQ06]. Impossible [BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SK01]. impostor [LC07]. improve [Pau02a, CAC06]. Improvement [CAC06]. Improved [AFGH06, BPR05, BB05, BF00b, CL01b, CKK+02, CJ04, D00a, DG02, Fan03, FKS+00, FKL+01b, FKL+01a, GMR08, Gen00b, HCK09, HKA+05, JQY01, Kin00, KT06, Ku02, Kuh02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02e, PR08, ST01b, SW05, SC05c, TN00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YR05a, ZW05a]. Improvement [AS01c, AJO08, Che04a, CzK05, CC02, D01, HWW03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Sha04b, Sha05b, WHL03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JSW05, JnI05, X05b, LY05b, LL04a, LW05c, SZS05, TO01, WLT05a, YW04a, YWC05, YRY05a, YRY05b, ZC09]. Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, WYZ04, YRY05b, ZC09].
Improving incentives [Swi05].

Incident [JBR05, Tom06]. Including [SR01]. Incomputable [Ver06b].

Inconsistencies [MS09a]. Incorporating [Ver06b].

Incorrectness [CHC04].

Increase [PBTW07]. Increasing [CS05c].

Incremental [BKY02, LKLK05].

IND-CCA [Mul01b]. IND-CCA2 [BST02].

Independence [BP03b]. Independent [BS00a, BSL02, Kin02, GSK09]. Index [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indies [Fra01, Syv02, Wri03].

Indexing [Ano00b, Ano01d]. indexing [YPPK09].

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

Infrastructures [HCD002, Lin00b, PBM03, WBD01, Bra01a, LAPS08, LOP04, SN07].

INIDP04 [LDM04]. initial [DK08].

initiation [YW05]. Initiative [Coc01a, Cal00b]. initiatives [Mau05].

insertion [MB08]. insertion-extraction [MB08].

insertion-extraction [MB08].

Insider [CMS09, Tad02, KS05a, Mal04].

Integrity [Ano02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b].

Intel [Coc02a, MP00]. Intellectual [Qu01, WY02].

Intelligence
Intelligent [Cos03]. Inter [WRW02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WRW02]. interaction [Gav08]. Interactions [Fau09]. Interactive

[BC05b, DG00, MS09c, CHK05, DDO+01, Fis01b, Fis05, HNZJ02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00, MS09c].

Interception [CHVV03]. interdomain [MABI06, vOWK07]. interesting [SWR05]. Interface [RSA01]. Interference [FGM00a, FGM00b, GA05, BR05].

[BC05b, DG00, MS09c, CHK05, DDO+01, Fis01b, Fis05, HNZJ02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00, MS09c].

Interception [CHVV03]. interdomain [MABI06, vOWK07]. interesting [SWR05]. Interface [RSA01]. Interference [FGM00a, FGM00b, GA05, BR05].

Interception [CHVV03]. interdomain [MABI06, vOWK07]. interesting [SWR05]. Interface [RSA01]. Interference [FGM00a, FGM00b, GA05, BR05].

Internal [Har07b, Bej06]. International [ACM03a, ACM04a, ACM05a, ACM09, ACM10, AN03, An00d, AAC+01, AJO1b, BDZ04, Bel00, B+02, BBD09, BS01b, Bi03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCMR02, CCMR05, CSY09, CGP03, Cra05a, DR02c, Des02, DKL05, DFP06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JYZ04, Je08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, Ki01a, Kim01, Kim02, KN03, Kn02, KP01, KN01, Lai03, LL03, Lee04b, LST05, LL04c, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pf01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Sch014, Sho05a, Sil01, SM07b, Syv02, TB02, TLL06, Uni00a, VY01, Van05a, WKP03, Wl99, Won01, Wri03].

International

[YM02a, YDKM06, ZJ04, Zhe02b, YZ03, AMW07, AUW01, An00c, AJ01a, BCKK05, Bir07, BC05c, CKL05, DV05, DWML05, DRS05, GSK05, HH04, HH05, HAO0, Hon01, May09, PC05a, PY05, PPV96, QS00, Sma05, Son00, ST01d, WK06, Ytr06].

Internet

[SMP+09, ABB+04, Ben01a, Ben02, Cal00a, Che05b, Chu02, Cla00a, Coc03, DP04, DGM03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, MC03, MA00a, Mir05, PM00, PLW07, PVS01, Pho01, PH03, Ru01, SBB05, SEK01, SEK02, Sto01, Tsa01, TNL05, U01, W01, WC05, Wri05, ZGT05, ke01].

Internet-wide [SBB05]. Interoperability [Hil00, TEM+01, BHM03]. interoperable [BFTG08]. Interpolation [LW02, YG01b, FWT05, KT06].

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

Interstate [RM02]. intranet [Jan00]. Intrinsic [SWC02]. introduced [An00a].

Introducing [JL00]. Introduction [B02, Bej09b, Bis03a, BK06b, Buc00b, Buc01, Bu04, CLR01, DK02, DK07, Fa07, Hay06, HPS08, HC02, MAA07, Mo01, Neu04, PT07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SHT09, SGK08, TW02, TW05, TW06b, Bug08, CS07b, CM05b, Gar01, HW98, H005, K030, M007, R03a, R000, Sh005b, TW06a, Kat05b, Rot07, Lee03a].

Intrusion [CZK05, DFK+03, DP07, JT05, TZZ05, TMM05, WG05, HLL+02, MAC+03, NCRX04, NN02, Yb03, JR02].

Intrusion-Resilient [DFK+03, DP07, IR02]. intrusion-tolerant [Yb04]. intrusions [Bej06]. intrusive [AM06, RFR07b, RFR07c].

invalid [CJT04]. Invariant [Ben00, CT09, HH09, ZLZ07]. Invariants [WH09]. Invasion [ASW+01]. invasions [Tyn05].

Invention [B04, F00, Sav05a]. Invaders [Bar00c].

Investigating [AMB06, BW07]. investigation [Cas02]. Investigative

[Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08, W01b, WC04].

Invitation [Bar02]. Invited [SBB05, ECM00b].
ions [Min03]. IP [Ano00a, CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSEC [Vau02, CBG05, Duv02a, KMM+06, SKW+07, FS00, FS03a, XLMS06]. IPSec-Compliant [CBGS01]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFSHG09]. Irreversibility [ZWC02]. ISBN [And04, Duw03, Eag05, For04, Gum04, Imr03, Pug04, Top02]. Island [CSY09, KGL04, Kim01, Lee04b, IEE07]. ISO [GM00b]. ISO/IEC [ISO04]. ISO9979 [TM01]. ISO9979-20 [TM01]. Isolated [LSVS09, MMMT09]. Isomorphism [CY02]. Israel [Jol01]. ISSAC [Jef08]. issue [FOP06, FOP06]. Issues [BDF+01a, BH03a, Hi00, KR01, Mea01, PB07, SEF+06, MK08, Pat02b]. ISW’97 [You01]. IT-Architectures [RM02]. Italy [AAC+01, AL06, BCKK05, BC05c, CGP03, dCdVSG05, IEE04]. Itanium [CHT02, Int00]. Itanium-based [CHT02]. Iterated [Jou04, Oni01]. Iteration [Che03]. IV [Sch01c, HSH+01]. IWBRIS [LST+05]. IWDW [BCKK05, CKL05, KCR04, PK03]. J2EE [BTTF02]. Jack [Coc03]. James [Top02]. jamming [LPV+09]. Jan [YRY05b]. January [Des02, GL05, ZIO00, Vau05a, Wri03]. Japan [An00d, Mat02, Oka00, Coc02b, Smi01a, Smi01b]. Japanese [YIO00]. Java [An004c, Mar05a, WBL01, Ano02a, Ano03a, Ano04c, Ano04e, AJ01a, BCS02, Bis03a, BJvdB02, CMG+01, Che00a, CCM05, Coo02, DPT+02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hum05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Virt03, Wei04, Win01, Zea00, ZFK04]. Java-Based [EM03, DPT+02, GW08]. Java-Lösung [An004c]. JAVA-Ring [WBL01]. JavaCard [AJ01a]. JavaCards [Cim02]. JavaScript [TEM+01]. javascript [Win01]. JBits TM [MP01a]. JCCM [CMG+01]. Jean [MFS+09]. Jeju [CSY09, Lee04b]. Jeng [QBC05b]. Jenness [Sal03b]. JICC [HY05b]. Jim [Coc01a]. Job [MYC01]. jobs [Oue05]. Joel [Gum04]. Johannes [Lee03a]. John [And04, BZ02, NH03, Rot07, Coc03]. Joins [Bar00c, Con00]. Joint [AD109, ADR02, CR03, HY05b, HY05a, Puc03, MI09]. Jörg [Fal07]. Jose [Po06, Pre02c]. Joseph [LBA00]. Journal [LLLZ06a]. Journey [FF01b]. Jr [Kat05b]. Judiciary [Uni00h]. Julius [Chat02]. July [ACM01a, CZ05, Jef08, KJJ05, 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, JY04, KL04, KN03, KM07, PPV96, TBJ02, USE01b, USE01a, USE02c]. Just [ABB+04, Ano06a, Gut02a, Car01]. Kahn [Gas01]. Kaikan [An00d]. Kaspersky [An008a]. KASUMI [KHC01, KHY01, SM02]. Katholieke [BB09]. Katz [Bar00a]. Keccak [BDPV09]. Keep [DM07b, Lys08, FS04]. Keeping [SEK01, SEK02]. KEM [NMO05]. Kerberos [BCJ+06, C01a, Gar03b, Hid00, Ito00, LLW08a, MDJ01, MP00, Rub00, Smi01a, Wac05, WD01a, Wit01]. Kerckhoffs [KM03]. Kernel [Int00, Mor03, BK05, HB06]. Key [ANS05, ASW00, AK02a, Ano01j, Ano09c, AAFG01, AE050, AL06, AF03, AB00, BC05a, BPS08, BH06, BDG+01, BDZ04, Bar00a, BPS00, BPR00, BMM00, BBD01, BY03, BOHL+05, Ben02, BLM01, Bi00].
Long-Lived [GSW00]. Long-Term
[ABRW01, Dur01, BMV06, ISO05, LG04, SGMV09]. Look
[Bon07, Has00, Lut03, Sye00, Hen06b]. Look-up [Has00]. Looking
[ASW+01, Ano01i, Cla00b]. looks [Nis03a].
Lookup [MFFT05]. loop [KVN09]. loop-level [KVN09]. Loopholes [Ste01].
Lorenz [GHdGSS00, Sal00a]. Lorenz-based [GHdGSS00]. Losing
[Sta05]. LosLobos [Pri00]. Loss [LHS05, BC05b, Mit00]. Lossy
[AIP01, HSKC01, PW08, Asl04a]. Lost
[PY06, Rob02, Rob09]. Lösung [An004c].
Lot [Cla00b]. Lotteries [FPS01]. Louisiana
[USE00c]. Louvain [QSO00].
Louvain-la-Neuve [QSO00]. Low
[Ano00d, BM01b, CH07c, GST04, HNZI02, HR07, JP02a, KBM09, RMH03b, RMH03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09b, Fan03, HLL03, LC04a, SK03, WLHH05, WH06, WY05, ZY07].
low-computation [Fan03, LC04a].
low-cost [CL09]. Low-end [SU07].
Low-Exponent [SZ01]. Low-overhead
[HGR07]. Low-Power
[Ano00d, JP02a, KBM09, CO09b, ZY07].
Low-State [GST04]. Low-Weight [CH07c]. Lower
[BD01b, BP03b, DIR05, GT00, GGK03, PS02a, Shp03, WW05, KS05b, Shp99]. LSB
[CS05e, FG01, WMS08]. LSB-encoded
[WMS08]. LSD [HS02a]. Lu [QCB05b].
Luby [MP03, Pto03a]. LUC [LN02].
Luminy [PPV96]. Lumpur [DV05]. Lund
[Joh03]. lurk [Rie00]. LUT [CC02a, TL07].
Luxembourg [Bir07]. Lyndon
[GS01, VS01]. Lynn [Hes04a]. LZ [AL04].
LZ-77 [AL04].

M [DNRS03]. M8 [TM01]. MA
[ACM10, JQ04, Kil05, KP01, Nao04, Pag03]. MAC [BKN04, CKM00, Kl03, LPV09, Vau01, Kra03]. MacDES [CKM00].
Machine
[LBA00, Mal06, Pro00, Cas06, Kid00, Pau02b, SWR05, WNQ08, Win05b, HM01a, Pet08].
Macraigor [An02d]. MACs
[BR05, BR00b, BM01c, Sem00]. Made
[Ste05b]. Madison [FMA02]. Maelstrom
[MYC01]. Magic [DNRS03, Bur02, Hro09].
Magyarik [dVF06]. Mail
[ANR01, Cos03, KS00a, Law05, CHE01f, LL04b, NZS05, Smi03, All06]. mails [LG09].
Mainframe [Web08]. mainstream [Bj05]. Maintaining
[MJF07, Zho02]. Maintenance [NABG03]. Maiorana
[Car02]. Majesty [Bud06]. Majority
[GGK01, SV08b]. Make
[BP06, Ber03, Sin02]. Makes [Pau09].
Making [Che07b, CRSP09, Gar01, Lut03, Mit00, Mul02, Oec03, Per05a, Wi05].
Malaysia [DV05]. Malaysian
[HLC08, SZ03, YY04, Tsa06].
malleable [DW09, FF00, PR05]. Malware
[LH07, SZ03]. Man [Gen04a, Urb01].
Man-in-the-Middle [Gen04a]. Management
[ACM03a, ACM04a, An02d, An02e, BP07, BW07, ELvS01, FMA02, GKO4, Gut04b, KB06, Lin00b, Scr01, Sha02, TMM01, Woo00, Wya02, ASW00, AJS08, AFB05, C05g, Cha05a, GTY08, ISO05, Jan00, JW06, KYM08, KM08, LMW05, LMP05, LR01, LK01, MKW00, Po06, RH03, SR01, Sen03, UP05]. manager
[KH03, Sha01a]. Managing
[MA00a, MA00b, NDJB01, Oue05, PTP07, PBB02, Tot00, BJ02, Kov03, KH03].
Mandrake [TvdKB01]. MANETs
[STY07, DF07]. manipulation [SWR05].
Manuscript [GG05a, Rug04]. manuscripts
[MAaTxx]. Many
[BB02, Di01, MP03, Di03, SVDF07]. Many-Round [MP03]. many-to-one
[SVDF07]. map
[KJ01, Lee04a, PC05b, SL09]. Maple
[Cos00, TT00]. mapping [Tan01]. Maps
[BGLS03, BMS03, CL04a, LLL+01, WP03, JK01b, MA02]. Maqasid [MAaT05].
Marcel [Irw03]. March [BDZ04, Bir07, Bla03, HR06, PY05, SIl01, Uni00g, Uni00h, Ytr06]. Marian [Kap05]. Marjan [BCB +05]. Markers [FBW01]. Market [Bar00a, Ano01b, Swi05]. Marketplace [PLW07, VN04]. Markov [KW03]. Marks [Ano01c, YSS +01]. Markup [Uni00a, Uni00d, Uni00e]. Marrakech [IEE09a]. Marriott [USE01b, USE01a]. MARS [BF00a, BCDM00, Fer00, IBM00, IK00, KKS00a, KS00b, KKS01, SOTD00]. MARS-like [BCDM00]. Mary [Ree01, Ros00b, Sin99]. Maryland [ACM05b, ACM05c, ACM09, SMP +09, GL05]. Mass [And08a].massively [AHS08, Lau08a]. Masking [CHJ02, CT03, GKO2, Lav09]. Massachusetts [IEE05b, USE01b, USE01a, IEE03]. masses [Pot06]. massively-parallel [FP00]. Match [JJ00a, WC04, LCC06a]. Matching [ABM08, Len01, UBEF09, Vo05]. materialized [MSP09]. Materials [SLT01]. Math [SR06, McNo3]. Mathematical [AUW01, Cas06, FF01b, GL05, HPS08, Kat05b, You06, GKS05, Sin09]. Mathematics [BP06, Lew00, Nie02d, Sch05a, Wal00, Gar04, Sch00a, Sch01c, S +03, Sch04a, Sch04b]. MatheMatiques [RSA09b, PPV96]. Matrices [TL07, CFVZ06, LMTV05]. Matrix [CV03, BF06a, OS07]. Matroids [CDG +05]. Matsumoto [DDG +06, YG01a]. Mature [Tro08]. Max [Di 01]. maximal [Hüh00, HJW01]. maximizing [GK09]. maxims [Bau00, Bau02a, Bau07]. Maximum [KMT01, ZC00, DW01]. May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bih03, CC04a, Cra05a, DRS05, IEE01b, Kn02, KN01, MJ04, MS05a, PM00, Pfo01, Pre00, TLC06, Uni00f, Uni00e, YKLM02a, Pau02a, YJ00]. Mbps [LMP +01]. McClure [Gum04]. McEliece [CF01, KI01a, KI01b, Loi00, LS01c, Sun00b]. McEliece-Based [CF01]. McFarland [Car02]. McGraw [Gum04]. McGraw-Hill [Gum04]. MD4 [DG02, WFLY04]. MD5 [Eke09, WFLY04]. Me [CAC03, CNB +02]. Mean [Bar00c, KLML05, Ver06b]. Means [LMHCET06, Nis03a]. measurement [Lav09]. Measurement [Ano02e, Hei07, CBB05, Ano02d]. media-streaming [CBB05]. Media [Cap01]. Mediated [DT03, CG06]. mediator [SBG05]. mediator-free [SBG05]. medical [AL07]. Medicine [MYC01, Moo01]. Meet [Cia00a, HG07]. meet-in-the-middle [HG07]. meeting [Jef08]. Meets [Way02a]. Melbourne [IZ00]. Member [CTH08]. Membership [NBD01, Fis01a]. Memoir [Bar05]. Memorable [KOY01]. Memoriam [DNR03]. Memory [AK03, AO08, BS00b, CCM05, DK08, DGN03, HNZ02, HDDJ01, KCJ +01, Oec03, OT03b, QSR +02, RSP05, YEP +06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK +05, YGZ05]. Memory-Bound [DGN03]. memory-safe [Oiw09]. Memoryless [Sar02]. MEMS [ECG +07]. MEMS-Assisted [ECG +07]. ment [CAC06]. menu [Mea04]. Mercy [Flu02a, Cro01]. Merkle [CDMP05, JLMS03]. Mersenne [Ano03e]. Mesh [LPZ06, ZTP05, KB09, LZP +04, YPSZ01]. Mesbes [BGI08, Lav09]. Message
[BKR00, BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SNR04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, Kar02, MD04, MS09c, Sha04b, TJC03, Wu01, ZF05, ZAX05, ZCW04]. Messages [Ara02, AR01, BR00b, CHJ01b, DS05b, Sch09, Wri05, Zhou06, Al00, An00c, BCG02, Bh02, BB79, LM09, SP79]. Messaging [Opp01, RR05]. Meta [SM08, PLJ05a, QCB05b, Sha05d]. Meta-He [PLJ05a, QCB05b, Sha05d]. Meta-learning [SM08]. Metadata [CDS07, FJ04]. Metamorphic [CSW05]. Metaphor [CNB02]. Metering [BC04b]. Method [BDTW01, GHK06, GL00, Gro01, HRS02, HQ05, JKK01, LL02, Mol02, OKE02, OT03a, OT03b, SOHS01, TIGD01, TSO00, WH09, WNY09, ZL05, AMRP04, DwWmW05, Gut04c, JZCW05, LMSV07, LFHT07, Mal06, SSST06, Sh09, YW06]. Methodologies [SPMLS02, NdM04]. Methodology [VMSV05, HM02a, HCBLETRG06]. Methods [BCDM00, CFRR02, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Baun0, Bau02a, Bau07, BM04, BCHJ05, CM05b, GK05, JZCW05, LMSV07, LFHT07, Mal06, SSST06, Sh09, 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 [GBKP01]. Microelectronics [IEEE09a]. Microprocessor [Web08]. Microprocessors [LKM05]. Microscopic [MYC01]. Microsoft [Bon00, Scr01, Ste05b, Web00]. Middleware [ACM05a, KRK01, LGS01, MBS04]. Migration [Pat02a]. Mikhailovsky [Puz04]. Milan [dCdV05]. military [Ark05]. Million [Ran55, Ran01, An00a]. MIME [Dav01b, Dav01c, LG09, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [FW01, FGM01, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LP05]. Mining [LP00, Lut03, HLL02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [CC05c]. MinRank [Con01]. Minutiae [UBEP09]. Minutiae-based [UBEP09]. Misbehaving [JQY01, SBB05]. Misinformation [CBZ01]. Missed [TvdKB01]. MIST [Wa03]. Mistakes [Ste05b]. MISTY [KYH01, Kih01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Kih02b]. Mithra [Fret03]. Mitigating [NLD08]. Mix [J00a]. Mixed [SKR02]. Mixes [M03a]. Miyazaki [WHL03]. MMM [GK05]. MMM-ACNS [GK05]. Mnenosyne [RH02, HR02]. Mobile [Cha05a, CFRR02, Dim07, GN06, J02a, KZ01, KB07, KC02, KHD01, LCK01, Mal02, MM02, PL01, RZ02, R01, R01, SH00, ZY05, CC05c, CJ03b, CF05, CF07, DHRM07, HP00, HYS03, ShCP09, ISTE08, KVD07, KX00, LC03, LC04a, Lin07, LKZ04, Par04, Pan02a, SSM08, SL05a, TM06, TW07, Tse07, Wan04a, YC09a, YC09b]. mobile-commerce [YC09a]. mod [TM01]. Modal [GN01]. Mode [BR02, Dwo03, HR03, HCR01, KSHY01, SLG05, WB02, Hey03, RBB03, ZL04c]. Model [Abe01, Abe04, BH05, BPS02, BL02, CLK01a, CS07c, CPH04, Chi08e, CT09, DP04, DFS008, Din01, Din05, ECM00a, Gra02, HLC08, KL06, KW03, LIL05, MND04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SDF06, TSDZ05, Vad03, WCZ05, WT02, W02, ZGL05, ZP05, ZS05, BKW03]
CUS08, Dan00, DFSS05, GMR08, HILM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SRJ01, TP07, DY09a. **Model-Based** [Sal05b]. **Modeling** [AADK05, CDD +05, HMvdLM07, KS05a, ZP05, Lafo00, SS04]. **modelled** [BG08]. **Modelling** [HCDO02, JP07, Puc03]. **Models** [Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01b, SC02b, vOT08]. **Modern** [Gol99, Mao04, Pag03, SM07b, Swe08, Bud06, Fur01, IM06, KL08, Mol05, SE01, Lut03, Lee03b]. **Modiﬁed** [CHC04, HPC02, JY01, Ki01a, ST02, Che08a, CJT01, HWWM03, LL04a, LL05a, kWpLWw01]. **modifying** [CSV07]. **Modular** [BIP05, BKP09, CMJP03, CH07c, Dhe03, F00p, Gro01, Har06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wa01, WL04a, HSD +05]. **Modulation** [AS01c, Che07a]. **Module** [Ano02d, BM00, SGM09, ARJ08, BG09, Jan08b]. **Modules** [FIP01b, NIS01b, GJJ05, JEZ04, Sci00b]. **Moduli** [Bai01b, GMP01b, Wa01]. **Modulo** [ACS02, Gon06, Gro03, MFFT05, Zhe01, Wan05]. **Modulus** [Ano01k, CGH00a, CDL +00, S01, WY02, WS02, LKYL00, WWTH08]. **Modulus-Based** [WY02]. **Mollin** [K05b]. **MOM** [DLC01]. **MONA** [K01b]. **Mondriaan** [BF06a]. **Money** [An00a, YKMY01, JP06]. **monitor** [MK05a]. **Monitored** [PS05]. **Monitoring** [AK02a, BCS02, Por06, Be06, GXT +08, ZGTG05]. **Monitors** [JT05]. **Monks** [Eag05, Kin01]. **monoaalphabetic** [GP06]. **monolithic** [GhdGS06]. **Monotones** [WW05]. **Monsters** [And08a]. **Monte** [B09, Sug03]. **Montereys** [USE02c]. **Montgomery** [CH07c, HKA +05, NMSK01, OS01, PS04a, TSO00, Wa01, WS03]. **Montgomery-Form** [OS01]. **Montpellier** [KM07]. **Montréal** [ACM02]. **Morocco** [IEE09a]. **MorphoSys** [Tan01]. **MOSS** [Dav01b]. **Most** [GG05a, Shp02, Tyn05]. **Mothballed** [Bar00c]. **Motif** [Bi09]. **Motion** [EFY +05, HKLS00, WDWM08]. **Mountain** [JZ04]. **mouse** [HLWw09]. **move** [Jac00]. **movement** [HLwW09]. **MP** [MP07]. **MP3** [DLR09]. **MPEG** [LHS05, MLP01, SG07, YZDW07]. **MPEG-4** [SG07]. **MRF** [Che01a]. **MRM** [TIGD01]. **MSP430x33x** [GBK01]. **MSXML** [TE01]. **Mu** [CJT03]. **Much** [Che01d, Con09]. **Multi** [ARR03, BM00, BR06, CCD07, CJK +04, CD00, CDG +05, DL08, DJL01]. **FGMO01, FW04, Gen04a, HM01b, HS07, JLL02, Kur01, LV07, LLL04, Ts01, Z09, BSSM +07, CLO02, CC05a, CHY05a, CHY05b, DZL01, FWT05, GMLS02, HHY07, HWH05, HC04b, HL04, LLL03b, LCZ05b, LW05c, NC09, PW05, SC05a, Ts0a, TWL05, TYH04, YCH04]. **Multi-applications** [DJL01]. **Multi-Authority** [JLL02]. **Multi-channel** [ARR03]. **Multi-designated** [L07]. **Multi-Domain** [CJK +04]. **multi-factor** [BSSM +07]. **multi-hop** [NC09]. **multi-linear** [LL04]. **Multi-party** [CD00, CDG +05, FGM01, FW04, HM01b, LL04, CLO02]. **Multi-property-preserving** [BR06]. **Multi-Proxy** [Z09, HC04b, LW05c, TYH04]. **Multi-Receiver** [CCD07]. **Multi-recipient** [K01]. **multi-scroll** [HHY07]. **multi-secret** [CC05a, CHY05a, FWT05, PW05, SC05a, YCH04]. **Multi-server** [Ts0a, LL03b, Ts08, TWL05]. **Multi-Servers** [HS07]. **multi-signature** [HWH05, HC04b, HL04, LCZ05b, LW05c, TYH04]. **Multi-stage** [CHY05b]. **Multi-trapdoor** [Gen04a]. **Multi-user** [BM00, DL08, GMLS02]. **multi- valued** [DL01]. **Multiagent** [Z05]. **Multiagent-Based** [Z05]. **multibit**
Multicollisions [Jou04]. Multilevel [LN04]. Multimedia [AAK09, FMS05, GA05, HL07, LLRW07, Sm05, WLLL09, DY09a, DKU05, La00, Ren09, SG07, YC08].

Multipath [SK05b]. Multiple [AIK01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, Dk05, Har00, HZSL05, HL07, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJ04, DM07a, HL00, KC09a, MN14, Sha01d, SW05a, TCC02, YW05, YSH03, YRY05b]. Multipair [BCC02, BGOY08, CDN01, DN03, DI05, GIKR02, OZL08, PMRZ00, CDD00, HT04, IKOS07].

Multiple-key [Che04a, CJ04, SW05a, YW05, YSH03, YRY05b]. Multipath-watermarking [Che08b]. Multiples [HR00]. Multiplication [AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02e, KIKM01, M02, NMSK01, OS01, Tan07a, Wa01, BNP03, DwWmW05, FP00, GD05, Has00, Mis06]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KO03, MFFT05]. Multiplier [HKA05]. Multipliers [CMJP03, KWP06, RH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07]. multithreaded [Zha00].

Multiverse [Boy03]. Multireceiver [HSZ01]. Multiresolution [hKLS00, YPSZ01]. Multiset [aSM01].

Multisignature [Tad02, CWH00, Cl04c, CCH04, He02, LWL09, LC04b, LWK05b, Wu01, YY05a, ZX04]. multisignatures [CL00, WH02b].

Multithreaded [Zha00]. Multivariable [DS05a]. Multivariate [DY09b, BGP09, FP09]. Municipal [MJJ08]. museums [Six05]. Music [MNS01, XMST07]. mutargima [MAAT05]. Mutation [Lut02]. Mutual [JP02a, KH05, CCS08, SW06, VK08, YWWD08, YC09b].

Mutually [WC01a]. My [Che05b]. MYCRYPT [DV05]. mysterious [Bel07a]. Mystery [GG05a, Rug04]. Myths [GO03, kc01].

N [Mar05a, AOS02, KOMM01]. NAF [OT03b]. Names [Coc01a, Sha02, Ark05, CGV09]. Naming [An01b, BH00b]. Nanotechnology [RR03a, RR03b]. Naor [Zha06]. Napoleon [Urb01]. narrowed [Sch04d]. narrowing [MT07]. NASA [An02c, Wil99]. Nation [Lan04].

National-Scale [BWE00]. Natural [ARC01, Top02, WMS08]. Nature [Pag03]. Naval [LBA00, Goo00]. Nazi [Han06, KS04]. NC [AIK04]. nCipher [An03f]. NCP [SQ01]. NCR [LBA00].

Near [BC04a, DPPS05]. Near-Collisions [BC04a]. Necessary [LCK03, MN01].

Necessity [SBZ02]. Nederlanden [dL00]. Need [Coc01a, HR04b, Sty04]. Needs [CZB01, DKK07]. Negotiation [DBS06, HHJS04, IY05, LLW05, LLW09].

Nema [Kid00]. NESIE [Pre01, Mac00, Pre02a, Pre02b, SGB01, DPPR00]. nested [LCK04]. Net [CACC03, An01b, LKJL01].

Netherlands [Kmu02]. NetHost [AMB06]. NetHost-Sensor [AMB06]. Nets [AADK05]. Netspionage [KBO0]. Network [An02d, An03b, Bar03, BGOY08, Con04, CLZ02, Dim07, FWBC02, Gum04, Har05a, IKY05, JYZ04, KKG03, KPS02, Ken02b, LMP01, Lu07, Ma02, NN02, PZDH09, PZL09, Poo03, RCBL00, RC05, Sty04].

TLYL04, VMC02, YC01, ZYH03, ZS05, Bru06, CJ03b, CMS08, Coc01a, DWML05, GKS05, HLL02, LC03, LPV09, MW06, ME08a, MSK03, MS08, Pr00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wyl05, YLT06, ECM00a, ECM00b].
Ros00a, MF07, PC05b, Yan02, Zha06.

Notes [KSF00]. Noting [Des00c, SR00].

Notions [BPS00, BN00a, CK02b, DKMR05, HU05, Kos01a, Des00a, KY00, PS04c].

Novel [BBC+09, CC02a, CYH01, CDDT05, CW09, HC08, MP01c, WCJ09, AJS08, BG08, CCS08, DSGP06, GB09, HG05a, SPG02, SCS05a, mSgFtL05, WC05].

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

Novice [Dew08, Gou09].

Novo [Bi09].

NP [AGGM06, FS08, HN06, AGGM10].

NP-hardness [AGGM06, AGGM10].

NPCryptBench [YLT06]. NSA [RC05].

NSF [Han00].

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

NTRU [GJSS01, GS02c, HPS01, HGHP+03, HGNP+03, HG07, JH00b, NP02b].

NTRUEncrypt [HHG06, KY09].

NTRUSIGN [HHGP+03, HHG06, HW08, ZJ09].

NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Die03, DG07a, DG07b, DV08, Eag05, EH08+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05, Ket06, KM01b, LMHCTR06, LNS02, MN01, NR04, RSN+01, SP05, Sch06b, Shp99, Shp03, SDFD06, TWNA08, TL07, TZZ09b, Vav03, Wal00, Yan00, YKLM02b, Aam03, AUW01, BK07, Be08, BGPG05, BG08, BG09, BGL+03, CNPQ03, CO09b, DIM08, DGP09, FP00, HG05a, HGNS03, HLxW09, HP01, JAW+00, JL03, KH08, KSF00, Kin01, Lam01, Mit00, Nie04, Pan07, PSG+09, PSP+08, PC00, RGX06, Sho05b, Shp05, Sim02, Stein, SR07, SK01b, Tzt05, Wagt03, Was08b, YZEE09].

Number-Notation [Eag05, Kin01].

Number-theoretic [NR04]. Numbers [HSR+01, HBF09, ffr00, MN01, ST03b, AG09, HW08, KB39, Kir01b, MFK+06, SS03, Shp05, Tip27]. numeric [AKSX04].

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

Numerous [CC08]. NURBS [Ben00].

NUSH [WF02]. NY [HR06, IKY05, KJR05, Sch01d, YDKM06, NIS00].

Nyberg [Ara02].

O [Kat05b, Puc03]. OAEP [Man01, BF05, BF06b, Bon01, FPS01, Sho01].

Obfuscated [NS05b]. Obfuscating [BG1+01]. obfuscation [CT02]. Object [RSA00e, DHL06, MWM01, ST06].

object-oriented [DHL06, MWM01].

Objects [CCM05, ZTP05, PB01, Whi09].

Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GDK+00, KKL09]. obscurity [MN03].

Observability [JQYY01].

observers [JL04]. Obstacles [KM04a].

Obtaining [Bar06b, BP03b]. OCB [RBB03]. occur [Web02]. Ocean [MYC01].

October [AJ08, BD08, CK05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST+05, TTZ01, USE00b, ZYH03].

Octopus [Cl00b]. Oded [Lee03b]. odyssey [Gol08].

Oedipus [Lav06].

Off [AJO08, Coc02b, Oec03, Sh10, YLLL02, Bau05].

Off-Line [YLLL02, Sh10, Bau05]. Offering [YY08].

Office [Uni01]. officer [Kov03].

Official [BP01b, Coc02b].

OffLine [DJ06, ST01b, VW01].

Offs [PS01c]. OH [BD08]. oil [RD09]. old [Lov01].

On-Demand [SEP+06]. On-Line [Lu02, BCS02, Luk01].

One [AK02a, BYJK08, CHL02, Che03, DIS02, Di 01, DW01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, KI01a, KO03, KO00, LTKW05, LDM04, MLM03, PV06b, PG05, PL05b, RR02, Sh00a, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, Di 03, DS02, GKK+07, HR07, HRS08, HLTJ09, JZ09, KKK07, KKKP05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Pol00, SVDF07, SV08a, SW05a, Tsa08].
One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLTJ09, LC04a]. One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLTJ09, LC04a].

One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLTJ09, LC04a]. One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLTJ09, LC04a].

One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK07, HNO09, HRTJ09, KO03, KO00, LTW05, Sh00a, YZ00, AK02a, AGGM06, AGGM10, BLYJ04, CHY05b, CJ04, GKK07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LJQ05, Mic02a, Poi00, Tsa08, YW05, YRY05b, ZW05a]. One-Wayness [KI01a, PV06b].

Ongoing [Sam09]. Onion [CL05]. Online/Oline [ST01b]. Online/Oline [ST01b].

Only [BBK03a, CF01b, GL01, Hoe01, VV07, BCDM00, FKS00, GHJV00, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Yus08]. Ongoing [Sam09]. Onion [CL05].

Ontario [HA00, ST01d, VY01]. OOSCD [CZB01]. OOSCD [CZB01].

Open [Bar00c, BDF01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAVY09, Voi05, FNRC05, Fox00, Pan07, Tyn05, PT08]. Open Card [HF00].

Open-Ended [Kis02]. Open-Secret [JOh05]. Open-Source [Bol02, Gut00, McA08]. Open-Source [Bol02, Gut00, McA08].

Opening [CAC03]. Opening [CAC03]. Opening [CAC03].

OpenSSL [Fri01, Res01a, Res01b, Sti06a, Val00, YRS09, Bel08]. Operating [BCST00, DPG07a, DPG07b, IEE01b, SR01, CGL+08a, CGL+08c, DPG09, KWD006, MHP06, SETB08, TKP08].

Operation [BR02, BKM07, Dvo03, EP02, Gol01e, HSH01, JKRW01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BKM07]. Operational [WA07, GMG00].

Operations [BIP05, IM01, KDO01, KS05c, LS01b, Ark05, Dug04]. operator [Wan05]. Operators [CH00]. opinion [BHM03, GS07b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Pau02b]. Optimal [Bai01a, BDDS03, CHJ+01b, CDF01, CF02, DPS05, DNP07, GMW05, IR01, KO04, KS03, LZ09, Man01, MPSW05, MP08, SNR04, YY01, vDW04, BCD06, HKS00, LSH03a, LSH03b]. optimality [NK06]. Optimised [TL07].

Optimistic [CC00, DLY08]. Optimization [Ken02a, Kre05, KV01, SMT01, TLYL04, WPP05]. optimized [LC03]. optimizing [Dwi04]. Optimum [KWP06, OKS06].

options [Fri07, Pot03]. Opt [Han00]. Oracle [ABR01, Abe01, Abe04, BF05, Ch08e, Gra02b, Nie02b, Pas03, Ano02e].

Oracles [BNPS02, BB04, KG09, RG09]. Order [AKSX04, Bai01a, CV02, KCP01, KCJ+01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Coh03, JZCW05, KS06b, QPV05]. Order-Specific [Ted02]. ordered [HY03, WL05]. Ordering [Mee04]. Orders [HJW01, PS02b, HM00, Hih00]. Ore [CHH01]. Oregon [ACM00, BCDH09].

Organization [JG07, MMZ00, MP00, C+02]. Organizational [PTP07, BJ02]. organized [AUW01]. Oriented [HR00, LSL+01, SKU+00, ZCC01, CHC05, CWJT01, DHL06, HWW04, LL06, LWZH05, MWM01, Saef02, Sh03c, TJo01a, WHHT08].

Origin [MA010, MD04]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Orsay [DPT+02]. OS [CRSP09]. oscillator [BGL+03, GB09].

oscillator-based [BGL+03]. oscillators [SPG02]. OSNP [HLTJ09]. Other [BF05, Ngu05, Wri05, Cla00b].

Other worldly [MYC01]. Ottawa [AMW07, MZ04]. our [Sta05]. ourselves [Fur05]. Outbound [Smi02]. Output [De03, YJ00]. Outsource [HL05a].

outsourced [MSP09, MNT06, YPPK09, YLC+09]. overcoming [CHC04]. Overdefined
Overflow [FOBH05, Fry00, Ino05].

overhead

[GR07, Ikon08, RSP05].

overhead

[XLMS06].

overlays

[SK05b].

Overshadow

[CGL+08a, CGL+08b, CGL+08c].

overview

[SVEG09].

Ownership

[AS01b, Nik02a, Nik02b, CL08, Lin01b].

P

[Puc03, AKS02, KR03].

P1363

[IEE00b].

P2P

[BRTM09, STY07, WN02, YLR05].

P2Ps

[LHL+08].

PA

[Cor00a, WWCW00].

PA-RISC

[Cor00a, WWCW00].

PACA

[Art04].

Package

[Win01].

Packed

[LH07].

Packet

[BR09, WRW02, WLZZ05, BC05b, CMS08].

Pad

[LD04, DS02].

Padding

[AR01, BCCN01, CJN02, KO03, LS01a, Man01, Vau02].

Paddings

[NP02b].

PadLock

[Lud05].

PadLock-wicked

[Lud05].

Page

[IEE00b].

PageRank

[GPC08].

pages

[Fal07, Rot07].

paging

[SZ08].

Paillier

[CGH01, DJ01, SNK05, ST02].

Pair

[WCJ09].

Pairing

[BKLS02, BF01b, BF03, CHSS02, GPS06, HC08a, HC08b, KM05, Kir03, PV06a, SKG09, Sma03a, GPS05, Lee04a, PC05b, VAVV09].

Pairing-Based

[BKLS02, GPS06, KM05, PV06a, HC08a, HC08b, GPS05].

Pairings

[Bon07, BGH07, Jou02, SB04, ZK02, CJL05, DSGP06, LWZH05, LC05b, SW05a, VK08].

Pairs

[LYGL07, Slp01].

Pairwise

[CLL00, FM02a, HMLVLM07].

PAKE

[HTJ08].

Palm

[BDhKB09, WPS01, W1999, A002].

Palmprint

[KZ09].

PAM

[FR02, Sei00b].

Panama

[BDPV09].

Panel

[FL01b].

Panoptic

[Y01].

Paper

[CC09, MFS+09, Pet08].

Papers

[An004b, An007b, An007a, Sch00b, Ytr06, W1999, Bla03, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, ZM04, NH03, PK03, PT06, RM04, S1901, AM07, AJ01a, B1907, BC05c, C205, CKL05, DRS05, HH04, HH05, PC05a, PY05, WK06, Wt03].

Paradigm

[BN00a, CS02, Go03, KD04, YC01, BKN04, Can01a].

Paradigms

[Des00b, Swa01, Har05].

Paradise

[USE00b].

Paradox

[Che01b].

Parallel

[AHRH08, App07, AEMR09, CPhX04, CTL01, CNP03, CNB+02, Dam07, DM00b, J08, KY02c, Lin01c, MFS+09, PS04a, RMH03b, SS01a, BF06a, FP00, OS07, RMP08].

Parallelism

[KVN+09].

Parallelizable

[BR02, M6l02].

parallelizing

[F01a].

Parallellizable

[LKK03a, LKK03b].

Parameter

[Wue09].

Parameterizable

[KPM02].

parameterization

[LZP+04].

Parameters

[ZL02].

Parametric

[Vir03].

Paranoid

[Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, G05a, Oue05, Ste05a, Luc06].

Parascript

[A002d].

Parasitic

[ETZ00].

Parents

[Pan02a].

Parents-to-Be

[Pan02a].

Paris

[ACM04a, GH05, KNP01, N02a].

Parity

[DRL09, KKG03, Yt01, BKW03].

Parity-Based

[KKG03, DRL09].

Park

[Cop05, Cop06, HS01a, Sa00b, Sa05a, SE01, Smi01b, Wei06, Win00].

Part

[Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05].

Partial

[BM03b, Cor02, Her06, ABHS09, CP07].

Partial-Domain

[Cor02].

Partially

[A000, MS09, Bao04, Fan03, HC04a, HY03, HLL03, WL05, WLLH05, WY05, ZC05].

Participatory

[CTB+01].

parties

[LKY05b].

Partition

[CTH08, WJP07].

Partitioned

[DN04].

partitioning

[BF06a, Che07a].

partitions

[Sav04].

Party

[K004, Lin01c, MR01a, WW05, WY01, CLOS02, CLK08, CDM00, CDG+05, FGMO01, FWW04, GCKL08, HM01b, JW01, LHL04b, LLL04, LLS+09, LSH00, YC09a, ZLX99].

Pass

[SK00, MT02].
Passive [Sha01c, VV07, RW07]. Passive-Only [VV07]. Password [BMN01, BMP00, CHV03, CPP04, CS07b, CC01b, DG03, GL03, GMR05, Har01a, Har01b, Jab01, KOY01, LSH03a, LSH03b, MP000, Mac01, MSJ02,Ngu05, SBEW01, SY06, WHL05, YS04, ZWCY02, CC01a, CC04b, CCK04b, CYH05, DG06, FLZ02, Fur05, GL06a, HTJ08, JM07, JPL04, Jua04, KLY03, KJY05, KTC03, KCL03, Ku04, KCC05, KHKL05, LLH06, LW04, LH03, LC04a, Pha06, Sco04, SLH03, Shi05, WLT03, XwWL08, YW04a, YWC05, YS02, YPKL08, ZDW06]. Password-Authenticated [BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HTJ08]. Password-Based [CPP04, CS07b, GL03, SBEW01, SY06, GL04, ZWCY02, Pha06, ZDW06]. password-guessing [Shi05]. Passwords [GL01, KOY01, Per03, Smi01c, Ano03c, FZ06, KOY09, NS05a, RD09, YW04a, YW04b, ZDW06]. Password-Authenticated [BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HTJ08].

Path-based [BLP06]. Patterns [DD02, MP06, WCJ09, jLC07]. Peer-assisted [Art04]. Peer-to-Peer [HR02, RH02, ATS04, MHPD06, PI06, WCJ05]. PeerAccess [WZB05]. Peinado [YRY05a]. PEM [Dav01b]. Penguin [Ban01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gu05, Oue05, Ste05a]. Pennsylvania [IEE05a, IEE08]. People [ASW+01, CG03, Lov01]. Perceptions [WDCJ09]. Perceptual [PBM+07]. Perceptually [EFY+05]. Perfect [AG00, CLLL00, DS01, Sun00a, DM07a, SC02c, SY06, ZD05]. Perfectly [DMS00, KSR02, SNR04]. Perform [Kin00]. Performance [ACM01b, BH00a, DFM01, Dra00, EY00, FZH05, Int00, Ken02a, Ken02b, Kra05, LK00, MM01b, NFQ03, PW03, PB07, SKKS00, SW00a, SB01, Siv06, SL00, SGP09, WBRF00, WW00, WS02, XH03, YEP06, Zea00, AKNRT04, BVP04, BZP05, CL03, CRSP09, GC00a, HM02a, JR06, LW05a, NTW07, SK03, YG05]. performance-friendly [CRSP09]. periodic [XQ07]. Periods [KK03]. Perl [Sal03b]. Permutation [DMS00, HSR01, IY02, KK03, Ko03, LSY01, DP02, IY03]. Permutations [BPR08, CHL02, K00, MP03, KKK05, WV00]. Persistent [AGT01, ST06]. Person [KJR05, LTT04, PK01, BS01b, KN03, Li05, LST05, PY08]. Personal [Bar05, EM00, SEK01, SEK02, Tyn05, UP05, Wal09]. Personalised [TNG04]. personalize [GPC08]. Perspective [LL01]. Perspectives [BMV06, SM08]. Perturbation [HH08, ZY08]. Pervasive [BDhKB09, JW05, LKLH09, Lut03, Lut03]. PET [MS05a]. Peter [For04, Uzu04]. Petersburg [GKS05]. petitions [Cal00b]. Petri [LKJL01, AADK05]. PGP [McL06, An00h, BCH00, Dav01b, Dav01c, JKS02, Luc06, Opp01]. PGV [BRS02]. pharaohs [Pin06]. Phase [CDF01, Ip02, KLB02a, Che07a, Che08a]. Phase-Conjugate [Ip02]. phase-shift
PSG\textsuperscript{+}09, Sha01c, Sma03b, WS05, WC01a, vW01, CBUSU06, CO09b, Geb04, Mit02, OS08, WLH06, XH05, ZYW07.

**Power-Analysis** [ÖOP\textsuperscript{03}], **power-attacks** [Geb04].

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

\textbf{Pp} [Eag05, Pag03, Top02]. **PP** [ASW\textsuperscript{+}01].

**PPK** [YDKM06]. \textbf{pq} [KOMM01].

**PQCrypto** [BD08].

**Practical** [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, XKTZ09, Sta02a, Sta06, Sti05, Sti02, Sti06c, Lut03, Spr03]. \textbf{practices} [CF05, Ste02]. **practitioners** [PP09].

**pragmatic** [BMW02b].

**Prague** [MJ04].

**Pre** [Adl03, AA08]. \textbf{pre-processing} [AA08].

**Precise** [Wal01]. **Precision** [HZSLO5, SR06, LMC\textsuperscript{+}03, MN14].

**Precomputation** [SLG\textsuperscript{+}05].

**predecryption** [RSP05]. **Predict** [Dic03].

**predictable** [Be08]. **Predicting** [AG09, BGPGS05].

**Prediction** [AKS06, SLG\textsuperscript{+}05]. **predictive** [vOT08].

**prediction** [HMvdLM07, JRR09, TP07]. **Prefix** [CGM07].

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

**Prehistory** [Ir00]. **Preliminary** [KSO0b, KKS0b].

**Prentice** [For04].

**Prentice-Hall** [For04]. \textbf{Preparations} [FJ04]. \textbf{Prepared} [ASW\textsuperscript{+}01].

**Preprocessing** [BIM00, CKK03]. **presence** [BIW08, GXT\textsuperscript{+}08, Ms08, VS08].

**Preservation** [Che01b, Dur01, Bro05a, ISO05, LG04].

**Preserve** [NTT05]. **Preserving** [DN04, KS05c, LP00, Mi03a, YWD08, AKSX04, BR06, BSSM\textsuperscript{+}07, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07].

**President** [Gen00a]. **Press** [Imr03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03].

**Pressure** [HWH01]. **pretty** [vOWK07].

**Prevent** [FOBH05]. **Preventing** [CS07b, CCL09, HSW09, IY05, RG05, DMS07].

**Prevention** [JT05, PZ01, PZ02a, Ge03, Sni03]. **Price** [AS01a, Bra01b].

**Primality** [BT02, Che03].

**Prime** [ACS02, Bai01a, Har07a, Pan02a, WS03, JL03, dW02]. **Prime-detecting** [Har07a].

**Primer** [KL+02b, Lad06].

**Primes** [An003c, SZ01, HLL03, Ste08, AKS02].

**Primitive** [CF05, IY02, IMM01, ST01a, ST02, IY03]. **Primitives** [BDFP02, CHL02, FGMO01, Gol01d, Ngu05, RR00, BDFP05, Gar05, JZCW05, RAL07].

**principal** [ZL04b]. **Principle** [CZK05].

**Principles** [ACM03c, ACM05b, DK02, DK07, KL08, MA007, SB07, Sta02a, Sta06].

**Print** [Kra02b]. **Printed** [SLT01]. **Printer** [Bar00a].

**Priority** [WWL\textsuperscript{+}02].

**Privacy** [An000i, AEV\textsuperscript{+}07, BBDP01, BSSM\textsuperscript{+}07, CDM\textsuperscript{+}05, Che08a, DL98, DL07, DFKX05, DN04, GS02a, GMM08, HY01, KS05c, Knu07, LP00, M007, M005, Pap05, PB05b, PP06b, Por06, PGT07, RW03b, R05, Ros07, Sal03a, SE09, Tom06, YWD08, Bel04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZYL05, ZSM05, MS05a, Jan08a].

**Privacy-Enabled** [Por06].

**privacy-enhanced** [ZSM05].

**Privacy-Enhancing** [SE09].

**Privacy-Preserving** [DN04, KS05c, YWD08, BA06, HJW05, Pin02, Pin03].

**Private** [AF04a, AF106, BDF\textsuperscript{+}01a, BIM00, BY03, BS09, BJLS02, BGW05, ISW03, PO04].
KO00, OS05, SDMN06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PLJ05b, Sun02, YRS+09, ZY08, ECM00a, ECM00b]. Private-Key [BY03, KY00, PLJ05b, Sun02]. prize [Fox00, Coc02b, MNT +00]. PRNG [HSS04, Mur02, SF07]. Proactive [DBS01, FMY01, JS05, ZSV05]. Probabilistic [CCW02, CP07, DLM05, Go19, JZCW05, KY00, KPS02, PLJ05b, Sun02, YRS]. Probability [KMT01, MNT +00, DLP +09]. Probing [ISW03]. Problem [AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK +02, Cou01, CLZ02, DIS02, DHR00, FL06, Gen03, GV05, GP08, KK02, LNS02, NBD01, Wag02, BKM03, CGH06, CT04, DLM05, HGN03, Hsu05a, LHY05, LD01, Luk01, Pei09, Slp05, SCL05, WL02, WH09, Yas08, Knu02a]. problem-solving [WH09]. Problems [BI05a, Can06b, MV03a, OP01a, TvdKB +01, VDKP05, HL05d, KXD00, LMT05v, LMC +03, RSS04]. Procedure [LY07]. Procedures [DJ06, BBK +03b]. Proceedings [ACM00, ACM02, ACM04a, ACM05a, AAC +01, Bon03, EBC +00, FMA02, FLA +03, SM07b, USE00c, USE00b, USE00a, USE00d, USE01b, USE01c, USE01a, USE02a, USE02c, USE02b, WKP03, Yun02a, ACM05c, ACM07, ACM08, ACM09, AUV01, AJ01b, BS03, Be100, B +02, Boy01, Buc00a, BC01, HA00, Hon01, IEE00a, IEE01a, IEE02a, IEE04b, IEE05b, IEE05, IEE07, IEE08, IEE09b, JY04, JF08, JM03, Joy03b, JQ04, KJ05, KGL04, Kim01, Kim02, KN03, Kn02, KP01, KNP01, KM07, Lai03, Lee04b, LTT +04, MMV06, MJ04, May09, MS02c]. Proceedings [Men05, Nac01, NPO2a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sm05, Syv02, TB02, Van05a, Won01, YDKM06, ZJ04, Zhe02b, ZY03, BCKK05, Cra05a, DV05, DWML05, DUK05, GKS05, IKY05, KI05, LI05, LST +05, Men07, Poi06, SH05a, Son00, dCdvSG05]. Process [Kwo03b, MTT +00, BDFP02, HL06, MRST06, VKS09]. Processes [BDP02, ALV02, BDNN02, WH09]. Processing [ISSZ08, KLB +02b, PCK02, AA08, AA04a, Ayo06, VPSZ01]. Processor [An002e, BBGM08, EP05, FBWC02, FZH05, GC01b, Int00, KBD03, KMPF02, TLYL02, ST03a, SHL07]. Processors [LY07]. Procurement [Lad06]. produce [Zir07]. producing [SOIG07]. product [KSWH00, Sun02]. Products [ACS02, An002d, An002e, Kn07, An000c]. profession [Wal04]. professional [Dew08, T00]. proficiency [Dew08]. Profile [PJA01, RAS00]. Profiles [MV01, PJK01]. Program [H01, Bec02, GGH +08, K03, KH03, CS08b]. Programmable [Dam07, GC01a, HV04, SMI02]. Programmer [Wil01b, Bon00, Che00a, DKK07]. Programmers [Coc01a, Wei04, Gou09]. Programming [ASW +01, An002d, Coc03, LHMCTR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, NIS03, VM03]. Programs [BGI +01, Ark05, SLTB +06]. Progress [KK06, KFSS00, RD01, Roy00a, CV04, DV05, JM03, MMV06, MS02c]. Project [Fri01, IY00, MTT +00, Pau02a, Salxx, Gou09, LR01, L01, WMW01, Sha01a, Coc01a, Coc02b, IY00, Pre02b]. projects [Gha07]. Prolog [Bla01a, Bla01b]. Promise [An002f]. promises [Pau02a].
promote [WK05]. Promotes [Bar00b].
Prove [MLC01]. Proof
[Ab01c, Ab00a, AS01b, ARC+01, BD02, Cor02, GK05, SOIO7, SPMS02, Tee06, BR05, Chi08b, Chi08c, Chi08d, GM04, HSD+05, LMW05, PBD07].
proof-of-compliance [LMW05].
Proof-of-Concept [ARC+01]. proofing
[CT02]. Proofs
[BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, Go09, HG05b, SV08b, dH08].
Propagation
[ARC+01].
Proofs
[BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, Go09, HG05b, SV08b, dH08].
Proposal
[ABC+05, BM01c, KY01b, LLL+01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].
Property
[ABC+05, BM01c, KY01b, LLL+01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].
Proposal
[DPVR00, Mac00]. Proposed
[Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06].
Protect
[ETZ00, BBN+09, WK05].
Protected
[CYH05, PKH05, ZCL05].
Protection
[Des00c, EHMS00, KY01d, Kra01, LKM+05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYL05].
Propagate
[CGJ+02, DFKX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VH01, WY02, XFZ01, ZTP05, CL08, CGL+08b, CGL+08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].
Properties
[BD04a, BR05, Can01a, Can06a, CP07, CKRT08, CWJT01, CH07, Cho08b, Chro01, CJM00, Coh03, CC05d, CDL06, DFG00, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV+09, LLL04, LL06, LLS+09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ06a, Puc06, SY06, WLH06, YS04, ZLX99, ZL04b, PDMS09, Puc03].
ProtoMon
[JT05]. Provability
[GOR02b].
Provable
[HM02b, HLL+01, HSL+02, KSH01, PB05, PSL+00, BGP09].
Provably
[AO00, ACJT00, BPT00, BCP01, BCP07, CHKO08, DG03, DG06, HL+02, HV09, HL0, HS07, JMV02, Mi03a, NSN05, NSS02, VMS05, WLH06, X03, ZCL05, BKN04, CMCT09]. provenance
[HSW09].
Provers
[A01, Sch01a].
Provider
[AB01, Sch01a].
Provision
[IEE07, Sil01].
Provision
[AB01, Sch01a].
Providers
[LD04, HLM02]. providers
[MV03b].
Provides
[OT03b].
Providing
[BACS02, BDS+09, DeL07, Lin07, Par04].
Proving
[Char03, FSO1c, GN01, Tee06].
Proxy
[AH05, BL05a, DFKX05, LCK03, LC05b, PL01, Rd01, Sha03d, Z09, AFG06].
Purposes [LS05a, FSGV01, PBV08]. Push [Pan03]. puzzle [LF03]. Puzzles [Ano01a, ANL01, CHS05].

Q [BFMR02, CH01b]. Q&A [Str01b, Win01]. QCQC [Wil99]. QCQS [Wil99]. QDSL [CUS08]. QNX [Ano02d]. 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, GXT+08, KC09a, WWTH08]. quality-conscious [DMSW09]. Quantiifer [KS06b]. Quantifier-free [KS06b]. Quantitative [Bai08, ME08a]. Quantization [DRL09, WC04, WC05]. Quantum [AC02, ATSVY00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL++05, BBD09, BZ02, BBB++02, BB03, BLMS00, BEM+07, Coc03, DFS04, DPS05, DFSS08, Das08, DMS00, Eto04, Eti02, GKK+09, GH02, GW00, GRTZ02, HV09, Hay06, Inr03, Ina02a, Ina02b, Kak06, KK06, KLB+02b, LB04, LW05b, Moo07, NA07, OTU00, PC09, Rec01, RK05, Ser06, SR07, T001, Wil99, Wti00, Y100, Y101, ZLG01, ABW09, Ano03f, Ano06d, BYJK04, BCG+02, Ber09b, BEZ00, BEZ01, BLRS09, DFSS05, Duw03, Eke02, GKK+07, Gav08, Heg09, HGH06, IM06, JZ09, JRS09, JAW+00, Joy00, KK07, KH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Ros00b, Sin99, Sin00, Smo04, UHA+09, BZ02, BD08, BB09]. quantum-storage [DFSS05]. quarter [Kob00]. quarter-century [Kob00]. quarters [Cla00b]. QUARTZ [PCG01]. Quasi [MD05]. Quasi-Pipelined [MD05]. Quasigroup [MSNH07]. Québec [ACM02]. Queen [Rec01, Ros00b, Sin99]. Queenstown [Zhe02b]. queries [CKK03, Fis01a, GPC08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC+09]. Query-preserving [GA03]. querying [FJ04, UG08]. question [OC03]. Questions [Ett02, Joh00, Jac00]. Queues [WWL+02]. queuing [CUS08]. quick [Dew08].

R [Che05b, Kat05b, Pag03, Spr03, Bih00]. R&D [Mau05]. Rabbit [BVP+04]. Rabin [Bon01, Gen04b, Miy01]. Rackoff [MP03, Pat03a]. radar [GG05b]. Radiations [SGM09]. radical [Web02]. Radio [Sac01]. RadioGatún [BDPV09]. Radix [HKA+05, JY01]. Radix-rails [Fox00]. Rainbow [DS05a]. Raises [MP00]. Raising [Cos03]. ramp [Y06]. Ramping [Coc02b]. Random [Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CTY09, Chi08e, Di03, DGP07a, DGP07b, DV08, EHK+03, Gra02b, GPR06, HSR+01, HBF09, Int03, JRR09, Kel05, LLL+01, LM02, Lys02, MP03, Mir02, NNT05, Nie02b, Pas03, Pat04, Ran55, Ran01, RSN+01, SFDF06, TWNA08, TL07, Tip27, TTT09a, TZT09b, Vav03, VKS09, WP03, BK07, Bl08, BG08, BG09, BG07a, BGL+03, CJL06, CO09b, DGP09, Fis01a, GVC+08, Gen00b, GB09, HG05a, HLWZ09, HDMI07, JAW+00, KH08, KB39, KG09, MI09, MKF+06, NR04, Pas07, PSG+09, PSP+08, PC00, Reg05, Reg09, RG09, RGX06, SS03, SXY01, SR07, SK01b, Sug03, SL09, UHA+09, WW08, YZEE09, BH05]. Random-Error [LM02]. random-self-reductions [Fis01a]. Randomnats [Sam01]. randomization [WHH05]. randomization-enhanced [WHH05]. Randomized [Sem00, Hro05]. Randomness [DD00, DD04, DGH+04, FW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN+09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03]. Range [CW09]. Rank [Sun00a, DW01, Sim02]. Ransom [BH05].
Rao [ZYL01]. rapid [OP01b]. Rate [KT01, LZ09, PS02a, Sun02]. Rates [GH02].
Ratio [Di 01]. Rational [HT04]. ratios [Zir07]. raw [CO09a]. RBAC
[LSZ05, SN04, ZP05]. RBAC-Based [LSZ05]. RC4 [FMS01, Mir02, VV07]. RC6
[GHV00, GHJV01, IK00, IK01, KM00, KM01b, RRY00, STK02]. RCES [LLCL08].
RCES/RSES [LLCL08]. RCES [GH02]. Rational [HT04]. ratios [Zir07]. raw
[CO09a]. RBAC [LSZ05, SN04, ZP05]. RBAC-Based [LSZ05]. RC4 [FMS01, Mir02, VV07]. RC6
[GHV00, GHJV01, IK00, 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, OJ04, JBR05, SP05, Sta05, YKMB08, GM04, HP01, Lie05, SL07, SGP08, YZDW07]. Real-Time
[Dri02, GM04, YZDW07]. Reality [Coc01a]. Really [CZB01, Wei00, Dav01c].
reason [Lau08b]. reasoning [IK03, IK06]. Recalculated [SW02]. recent
[JK01a]. Reception [Top02]. Recipes [VM03]. Recipient [ANR01, Kur01].
Recipients [Coc01a]. recoding [SSST06]. Recognition [Ano02d, LLT04, LST05, TZT09b, HS02b, Li05, MMJP03].
Recommendation [Bar06b, BK06a, BK07, Dwo03, NIS03b]. Recommended [Kel05]. Reconfiguring
[BNPW03, PGT07]. Reconfigurable [FD01, FHZ05, GC01b, KBD03, LZ04, MKP09, MMH02, SJT09, SKG09, SRQL03, CMS08, DHL06, GC00a, HBC+08, Rhi03].
Reconfiguration [PTTW07].
Reconsidered [Sho01]. Reconstructing [CDF01, FL06, PS01a]. Reconstruction
[AF03, CF01b, CDF01, JJO06d, KY01c].
Records [Dur01]. Recoverable [NZCG05, NZS05, SGMV09, YYY00].
Recovery [BDK+09, BM01c, CKM00, MMZ00, OS01, PBC05, SVW00, TC01, VW07, WCZ05, WLT05b, CCH05, CJ05, HW05, LKL01, PSP+08, Sha04b, SIR04, TJ03, Wu01, ZF05]. Recursive
[WHHT08]. Recycling [DPS05, TR09a, TR09b]. Red [Saw07].
Red-Eye [Saw07]. redistribution [KB09]. Redondo [IEE00a]. Reduced
[BDK02b, CC08, CS05c, FKS00, HQ01, HSR+01, KKS00a, KS00b, KKS01, KML+02, KM01b, KKS00b, MHL+02, NV01, STK02, SK01, YSD02, CV05, KHH01, SK01a]. Reduced-Round [FKS00, KKS00a, KS00b, KKS01, KML+02, KKS00b, NV01, YSD02, CV05, KHH01]. Reducibility
[DM00b]. Reducing [AL07, BIM00, SPPH06]. Reduction [CM05a, CH07c, Dhe03, Gro01, HGG07, Kid02, PG05, ALV02, HG07, Sug03]. reductions [Fis01a]. Redundancy
[AB01, BR00a, MOM02, YLR05]. Redundant [MF01, Taa07a, PS04a].
Redwood [KKP02]. Reed [KY02b]. Reference
[BR09, CPS07, Pe03, RS00, Sal07, vT00]. Reference-Watermarking [BR09].
Refined [Sma03b]. Regarding [GMP01a]. Regex [BTTF02]. Region
[BN00a, Pau01, Uni00a, Uni00f, Uni00e, Uni00g]. Region-Based
[BN00a, register [HTW07]. Registers [CGFS09]. Registration [HLM03].
regression [mSgFtL05]. Regulations [TM01, Ano00g, Cha00b]. Rehearsal
[Ah08]. reinforce [SWR05]. Reiwe [CB6+05, Kap05]. Related
[BD06b, Can06b, CY08, FKS00, Kil01b, KLM05, Sat06, Buc00a, Gutxx, HAU04, Hen06a, Scho00b]. Related-Key [FKS00]. Relation
[ABC05, NN06]. Relational
[AK02b, AHP03a, AHP03b, CKY07, GA03, PT08]. Relations [BN00a, Pau01, Uni00a, Uni00f, Uni00e, SP03, Zha08]. Relationship
[NG05, GKM+00]. Relationships
[DKMR05, SKU+00]. relative
[JRS09, Mü01b]. relaxes [Ano00c].
Relaxing [CKN03, PS05]. Relay
[DM07b, Zha00]. Release
[CHK08, Mao01, HGNS03]. Released
[Bar00c, Ano01g]. Releases [Bar00c, AJ08].
Reliability [IKP+07, WK05]. Reliable
[MR03, MPHD06]. reload [SL06].
Reminders [Che01f]. Remainder
[Sch01b, YKLM03]. remedy [FZ06].
Remember
[HSH+08a, HSH+08b, HSH+09]. Remote
[CKN03, PS05]. Remanufacturing
[BCW05, CL04d, SCS05c]. remedy [FZ06].
Replacement [DKFX05, GM00b, HL04, ZJ09, BKN04].
replace [Gav08]. Replacing
[FZ06, KAM08]. replication [BIW08].
Reply [WLW04]. Report [DFG01, Pem01b, Pre01, Sol01a, Sha03b, BCHJ05].
Repository [Bar00b]. Representation
[BJvdB02, FSW01, JLMS03, JY01, RN00a, RN00b, ZKL02, BDSV08, BA06, PS04a, SWR05]. Representations [OSSST04].
Representative [CTBA+01].
Representatives
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Republic [MJ04, dL00]. Republican
[HL04, LSA+07, SC05c]. reputation
[KN05, RCG+05]. reputation-systems [KN05]. Request
[RSA00b]. require [SO08b]. Required
[Sun00a, Lov01, Wan05]. Requirements
[FIP01b, HWH01, Kin02, NIS01b, Mei04].
Rescue [ASW+01]. Research [Pip03].
Research [AJ01b, CZ05, CZK05, DFPS06, KGL04, LXM+05, RC06, Sch00e, TMMM05, DFCW00, JXW05, MH09, QS00, dCdVSG05]. Researchers [An00b, An00c, Pau02b].
Resettability [DPV04, MR01b]. Residue
[TIGD01, YKLM02b, CNPQ03, FP00, LD01]. Residues [Coc01b, Zhe01, CCS08].
Resiliency [Job00]. Resilient
[Che01c, DSS01, DK+03, DP07, DP08, GSS08, KZ07, SM00b, KZ03, IR02]. Resist
[HM02c]. Resistance
[HNZ+02, MÖ02, EBS01]. Resistant
[An01e, ACJT00, ANL01, BGW05, CDTT05, CN06, Gir06, IOK05, LLS05a, LWS05, LTM+00, LNL+08, KS09a, PC09, WLO04b, YS02, MS09c]. Resolution
[SGM09]. resolving [Lin01b]. Resort
[USE00b]. Resource
[MRL+02, Tse07]. Resource-Constrained [MR+02].
resource-limited [Tse07]. Resources
[Butxx, FOP06]. Response
[JBR05, LW05a, XNK+05]. Responsibilities [Vix02]. Resting
[Gut02a]. restricted [ASW00]. Restriction
[CTH08]. Restudy [FWL08]. Results
[APV05, GM02c, OOP03, RR08, Way02a, YRS+09, CV05, CKRT08, DM07a, GMG00, PM08]. Rethinking [Bra01a, KZ03].
Retraining [JLC07]. Retreat [FKSW00].
Retrieve [BIM00, KO00, RE02, YK07].
Retroactive [DS01]. retrofitting
[CGL+08a, CGL+08b, CGL+08c]. reunion
[LBA00]. Revealed [Ga03]. Reversal
[Cap01, DIS02]. Reversal-Bounded
[DI02]. Reversals [MS02e]. Reverse
[Coo02, EC05, Wue09]. Reversed [Che02]. reversibility [KC09a]. Reversible [Ga03].
Reversing
[EC05, YWC08, YN01, CDFM05]. Review
[And04, An00i, Du03, Eeg05, Fal07, Gas01, Gun04, Im03, Izw03, Jan08a, Lee03a, Lee03b, Mar05a, Pag03, Pap05, Puz04, Ree01, Rot07, See04, Spr03, Ter08, TvdKB+01, Top02, Uzu04, Was08a, Her09b, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wal00]. Reviews
[For04, Kid00, Sal03b, Sty04]. **Revised**
[Bla03, BC05c, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GS02c, GH05, HH04, HH05, Jol03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MQ04, NH03, PC05a, PK03, PT06, RM04, Sil01, Ytr06, AMW07, A01a, BK07, Bir07, CZ05, CKL05, DR05, Irw03, PY05, WK06, Wri03]. **Revised**
[ABC+05, Ana02b, BM01b, CDP05, Kmh00b, NS05c, OSSST04, Hes04b, OH08b, ZTT05]. **Revisiting**
[AEAQ05, Har01a, Har01b, JMV02]. **Revocation**
[BDTW01, CL02a, Gen03, GST04, NNL01, TT01, ZSM05, KT06, KSW06, LHH05, SW02]. **revoke** [NN03]. **Revolutionary**
[CMB+05]. **Rewriting** [Cir01, HR04a]. **RFC** [BWBL02]. **RFID** [And04, AL07, ACD05, Ay06, BLD09, CCS08, CH07a, CL09, FW09, Fin03, KJK+07, OS06, Ros06b, SE09, TTT09a, TTT09b].

**Rhee** [Kiu08]. **Rhode** [IEE07]. **RI** [Sil01]. **Right** [Dhe03, GS07b, HKP05]. **rightful** [CL08, Lin01b]. **Rights** [Bar00a, BNPW03, Dre00, Scr01, TMM01, Wy02, B06, UP05].

**Rijndael**
[BB02, MP01a, SKK+00, W02, CKK+02, CG01, DR00a, DR00b, DR01, DR02b, FKS+00, FLK+01b, FLK+01a, FSW01, FD01, GM00a, JmBdXm05, KV01b, K101, KV01, Luc00, MM01b, MMH02, PSC+02, RDJ+1, SMTM01, SRQ03].

**Rijndael-Like** [PSC+02]. **Ring** [BSS02, Nao02, WBL01, ZK02, Her07].

**Rings** [BLST01]. **RIPEMD**
[DG02, WF04]. **RISC** [Cor00a, Gro03, WCC00]. **RISC-Based** [Gro03].

**Risk** [WA07, Vo05]. **Risks**
[ES00a, Kuh02a, Ros07, Be014, B02, ES00b, Jan00, MN03, P+01, Sch00c]. **Rivest**
[BB79, Coc03, SP79]. **RMI**
[JB06, Mar02a]. **RNS**
[BI04, KP09, NMSK01]. **Road**
[BDPV09, HR04b, PB01]. **Roadmap**
[Coc02b]. **Roaming**
[CAC03, YWD08, SS+08]. **Robotic**
[Kum07]. **Robots** [Coc01a]. **Robust**
[BB00a, BR09, CJ034, CWY05, DDK+01, FCZ05, HH09, hKLS00, Lin00a, LHS05, LL06b, PJK01, SO01, SDFH00, SDF01, WY09, WLS04, WM08, YPS01, ZTP05, KA09, LZ05c, LKZ+04, Mit00, MB08, TN+09, YY05b].

**Robustness**
[CS05c, HM01b, Rot01, CKL+09]. **Rogaway**
[MW04]. **Roger** [GG05a]. **Role**
[SBG02, Y09, ZLX05, Cer04a, Cra05b, Gor05, Man04]. **Role-Based**
[Y09, ZLX05, Cra05b]. **Roles**
[LLL+01, Vix02]. **Roma** [AAC+01]. **Rome**
[IEE04]. **Ronald** [Coc03]. **root** [Pet05].

**Rootkit** [Bh09]. **Rootkits** [HB06]. **Roots**
[Go06, HCK09, CAC06]. **Roseau** [PY05].

**Rotation** [RB08]. **rotations** [SK03]. **Rothe** [Fal07]. **Rough** [Naz02, WG05].

**Roughness** [Lav09]. **Round**
[II00, BP04, Bi00, BF00a, BD02b, Che03, DP04, D05, Dra00, FKS00, GKK07, GIKR02, HSY+01, Kan01, K04, KSS00a, KS00b, KKS01, KML+02, KSS00b, LKL09, Lin01c, MP03, MHL+02, NP01, RR00, Ros00a, STK02, WR00, Wer02, YS02, CV05, CL08, CKL+03, DLP+09, GIKR01, HLS+02, K01, LKH+08, MR01b, Ph04, SW05]. **round-** [CL08].

**Round-Complexity** [Ros00a]. **Round-Optimal** [K04]. **Rounds**
[BDD+09, CD01a, HS02, KM01b, Lu00, Pa03a, Pa04, GM00a, SK01a]. **Routing**
[BGO08, CL05, Kon02a, KB09, LAPS08, LHC08, MABI06, PS08a, RVS09, vOWK07].

**RSA** [Joy03b, Men05, Oka04, Poi06, Prec02c, Sh04a, W00, Ad03, An01k, An02e, AR01, BI04, BLH06, Bar06c, BM01a, BP02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BJ00, BF01c, Bon01, BCC01, BP01b, CNS02, CDL+00, CW02, Che01a, CKY05, CNQP03,
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, JK02c, JG01, Kal01, Kal03, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, May04, Miy01, Mol03b, MP01c, NZCG05, NZS05, NS01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Sha03a, Shp01, Shp04b, SZ01]. RSA [Str02, SWH09, TIGD01, TT00, Ver06a, Wal01, Wal03, WQQW01, War00, WLHH05, Wie00, WS02, WY05, XG05, Yan07, yH08, YKL02b, YKL03, YPKL08, YY00. You06, ZC09, Zhe01, ZWCY02, dW02]. RSA-based [NS05, 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, Bih00, BCDM00, Dav01b, Dav01c, FM02b, JnBlXqXm05, LG09, Opp01, SMTM01, ZC00]. S-Box [FM02b, SMTM01, JnBlXqXm05]. S-boxes [BCDM00, ZC00]. S/MIME [Dav01b, Dav01c, LG09, Opp01]. SAC [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR01, HSS04, ST01d, VY01]. SAC’99 [HA00]. SAFE [Uni00a, Uni00e, Uni00d, Uni00g, Uni00b, ACS02, LBR00, Lys08, Oiw09]. Safe-Prime [ACS02]. Safeguard [LXM05]. Safeguarding [Sty04, Bar03]. safer [An000f, NPV01, BDD03]. safety [HM01a]. SAFKASI [WAF00]. Salomon [Pap05]. Salsa20 [Ber07, Ber08]. Salt [PKBD01]. Salzburg [DKU05]. Samba [BH00a]. SAML [RR04]. Samos [KGL04]. sampled [WW06]. sampling [KB39, Sug03, Tip27]. San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Oko04, Po01, Pre02c, Sch00a, Sch01, Sch01a, Sch05a, USE00b, USE02a, USE02b, Cal00c]. sanity [Sk003]. sans [Car00]. Santa [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a]. Santiago [BS03]. Sanxin [LSZ05]. SAR [B+02]. SASAS [BS01c]. SAT [KLN+06]. Satan [Mea04]. satellite [CC05c, HYS03]. Satisfy [PHM03]. satisfying [QPV05]. Saturation [Luc02a]. saving [Lev01]. Savings [CAC03]. SAX2 [TEM’01, Hei01]. Say [Sta05]. says [Mad04]. SBLH [JK02a]. SBoxes [WOL01]. SC-CFS [Ito01]. SC2000 [SYY+02, YSD02]. SC2001 [ACM01b]. Scalable [CPhX04, HKA05, HLY05, KYS03, KHYM08, SPQG06, LW08b, ST03a]. Scalar [AHR08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. Scale [BWE’00, CDR01, FGD01, BF03a, BH00a, HMvdLM07, PS08a]. Scaling [BBPV00, Cc02b, SDFH00, SDF01, PBVB01]. Scambrazy [Gun04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Ols00]. Scenarios [BF05]. scene [SG07]. Sceptical [Pen01b]. Schedule [MMH+02, XF05]. Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BBC’09, BPS02, BR09, BS01d, BMS03, CL01a, CHK03, CHG01, CC01b, CYH01, CTL04, CC09, CH01b, CM05a, Cc01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJJ01, GS02c, HYS02a, HNZI02, HY01, HT06, HC08, Ig02, JSS01, KK02, KC02, KC07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LCD07, Miy01, Mill01a, OKS06, PL01, RK06, Sc01, SOO02, SW05, SGGB00, SYLC05, SNNG01, Tad02, TC01, Tsa01, TTO1, WQQW01, WZ05, WBD01, YWWS09.
YG01a, YLH05, ZJ09, AEEdR05, Asl04a, BCL05a, BCW05, BKN04, BBG+02, CL02b, CBBH05, CC01a, CC05a, CL04b, CL04c, CL04d, CCK04b, CY04, CHY05a, CHY05b, CL00, CHC04, CCH04, CY05, CHC05, Che05a, Che07a, Che08a, Che08b, CCS08, CKN06, CJT01, Chi08b, Chi08c, Chi08d, DSGP06, DW01, FLZ02, FXAM04, FCZ05b.

scheme [FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HWW03, HWW04, Hsu05a, HWH05, Hsu05b, HLC07, HC04a, Hwa00, HYS03, HLL04, Hwa05, HL05c, HL05d, HL05b, JH06, JASW05, KC09a, KLY03, KRY05, KSW06, KHL09, KCL03, Ku04, KC05, KCC05, HKHL05, LHY02, LL02, LHH03, LMKY05a, LL04a, LRY04, LLY05a, LKY05a, LKY05d, LL05b, LMC+03, LL04, LTH05, LLCL08, LL06, LHL03b, LH03, LC04a, LYG07, LCC05, LC04b, LCC05a, LLH05, LCLZ05b, LCZ05c, LCZ05a, LW05b, MSP09, NCO9, PW05, PBMB01, PCC03, PC05b, P901a, Pei04, Sae02, Sco04, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, SLH03, mSGFtL05, SCS05b, SC05c, SC05c, SFS05, TLL05, Tsao8, TWL05, TY04, V05, VS08, WLT03, Wan04b, WL05, WK05, WJP07, WDL09, WHH05, WC01b, WH02a, WHHL03, WH03, WCO3b, WCO4b, WC05, XWXL08, XC05, YW04b, YTH04, YW04a, YCH04, YW05, YCO9b, hY08, YRY04, YR05a, YY05a, YRY05d].

scheme [YY05b, YbJ04, ZC04, ZF04, ZC05, ZK05, ZW05a, ZAX05, ZC09, ZL05, dRMS05].

Schemes [AR01, BP02, BU02, BDSS03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CPD06, CKN00, Cor02, CJP02, Con04, CS00, CS03b, CD+05, CL02, DN00a, DN02b, Des00b, DS06, DN00b, FF00, HSZ00, HWW05, HM02b, HLL05, KIn02, Kos01a, KS03, KOM01, LZL+01, LP01, MV00, NIS03b, Nam02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SBZ02, SPML02, Snm00a, VMSV05, WCJ09, X03, YWC08, YY0D01, Yek07, YYZ01, ZT05, ZY01R, Abdo1, AFGH06, BCD06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGG03, HCD08a, HCD08b, HANR04, He02, HKS00, HW03c, HW04, HW05, HC04b, HL04, IY06, JPL04, JX05, KJ05, Kir01b, KT06, Kre05, Kul00, LWH05, LWF05, LW05c, MF07, Mü01b, NKO, PS02a, PKH05, Pho06, QC05b, QCB05a, SN01, Shao3d, Shao5b].

Schemes [SCL05, SC02c, SHT05, Tsao5, Wu01, XY04, YW05c, YWC05, YCW+08, ZF05, ZCL05, vDKST06].

Schloss [IE001b], Schneider [Puc03].

Schneier [Hei03, See04, Sty04].

Schnorr [BP02].

School [Coc02a].

Schools [PM00].

Science [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Imr03, Nie02d, Pag03, Sch06b, SM07b, Sin01b, MAC06, PR04, Six05].

Scientific [CST02, HM09, Bau08].

Scientists [Coc01a, MH09].

SCN [BC05a, CGP03].

Scots [Roe01, Ros00b, Sin99].

Scream [HCJ02].

Scribner [Gas01].

Scripts [Uri01, Oue05, Rob02, Rob09].

scroll [GB09, HHYV07].

SD [ECM00a].

SDK [Aho02d, Bar00c].

SDL [HL06].

SEA [SPG06].

Seamless [OKE02].

Search [BL05a, Des00c, FIPR05, KB07, LM02, TGD01, WYY05a, WYY05d, FZ06, PM08].

Searchable [ABC+05, AF106].

Searches [PGT07].

Searching [BSW09, GTTC03, OS05].

Seattle [ACM06, S+03, USE00a].

sec [KV01].

Second [ACM03c, Bra01b, BD08, CZ05, GW01, HTS02, JY04, KCR04, Ki05, KPH01, NM09, RD01, ACM00, Irw03, Rie03, Son00, Spr03].

Second-Order [NM09].

Second-Price [Bra01b].

Secord [Top02].

Secrecy [Bla02a, GH02, Imr03, Lau05, Ree01].
Secret

[ACS02, Alv00, Ano03d, BBDK00, BTW05, BI05b, BTW08, BP06, BM01b, CGGH06, CGH00a, CH01a, CTY09, CS05b, CK01d, CD00, CF02, CFS05, CDI05, DI01, DKL00b, D06, DN00b, DP07, EHMS00, FM02a, FS02, Fi01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah67b, Kah96, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, MN01, NABG03, NN06, OKS06, PZ01, PZ02b, PW03a, PW03b, Rey01, RST01, Sin01b, Sin00a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, AJ08, AEEdR05, Ano02c, Ano08c, Bam02, BCB05, BCL05, BCL07, BDD00, BCL00b, Bl04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CHK3, CHK05, CGP08, CW07, CQS01, CHJ+01a, CHJ+01b, CDM00, CD01a, CS02, CS03b, CDG+05, CD05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, FP01, FOPS01, GP08, GIKR02, GJKR03, Gen04a, GD05, HSZ00, HSZ01, HSHI02, HSHI06, HR02, Har07b, HKW06, HL02, Hv09, HR04b, HL07, HT09, Hut01, HLC08, IR01, Ito00, IFH01, J00a, J00b, JMV02, KMM06, KY01a, K04, KLM05, KC02, KH05, KKL09, KI01b, Kos01a, Kos01b, Kra01, Kra05, KRS02, LCK01, LLL02, LCK03, LWK00, Lin01c, Lin03, Lin02, LL02, MK09, Mar02a, Mar07, MV01, Mo03a, MJ01D, NM05, Nam02, Nd05].

Secure

[BNP03, Ito01, UP05]. Securely

[HL05a, LLK05].

Section

[Ano04b, Ano07a, BK06b, SG08, TL02, KP03].

Secret

[MeK04].

Secure

[AR00, AO00, AF04b, AG01, AP09, An001k, ACJT00, AFI06, BDF+01a, BST03, BCL+05b, Bar03, Bl05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CHK3, CHK05, CGP08, CW07, CQS01, CHJ+01a, CHJ+01b, CDM00, CD01a, CS02, CS03b, CDG+05, CD05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, FP01, FOPS01, GP08, GIKR02, GJKR03, Gen04a, GD05, HSZ00, HSZ01, HSHI02, HSHI06, HR02, Har07b, HKW06, HL02, Hv09, HR04b, HL07, HT09, Hut01, HLC08, IR01, Ito00, IFH01, J00a, J00b, JMV02, KMM06, KY01a, K04, KLM05, KC02, KH05, KKL09, KI01b, Kos01a, Kos01b, Kra01, Kra05, KRS02, LCK01, LLL02, LCK03, LWK00, Lin01c, Lin03, Lin02, LL02, MK09, Mar02a, Mar07, MV01, Mo03a, MJ01D, NM05, Nam02, Nd05].

Secure

[NSNK05, NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RV09, Rd01, ST01a, Sea05, SV07, SB05, Sm02, SK02, SN04, SBEW01, Sty04, Tad02, VMS05, Vau05b, VM03, WLL09, WBL01, WGL00, WHL05, XS03, YW05, ZMY05, Zhou06, Ann03, Ab01, AEEdR05, AL07, AFGH06, BDS+09a, BDFP05, BC07, CLO02, CC04b, CCK04b, CR09, CHI+09, CG05, DG06, Dwi04, FMY02, Geb04, GIKR01, GCKL08, HSW09, HL03, HL06, HJ09, HBC+08, In05, ISTE08, IKOS07, I06, KOY09, KG09, LL04b, LL04H, LHC08, LH03, LC04a, LCZ05b, MT09, ML05, Mii01b, OS00, PCM07, PB01, PQ06, PSP+08b, RH03, RG09, RG06, Sea09, SB07, SG09, TKP+08, TCR03, Tse07, Ver01, VK08, WLH06, WWA01, YG05, YT05, Y08, YRY04, ZBP05, ZC05, ZCW04, vOWK07, An008d, An012, BS01a, BSB05, CHK008].

Secure

[FIP02b].

Secured

[BNP03, Ito01, UP05].

Securely

[HL05a, LLK05].

Securing

[Ab01, Cal00a, CY01, D01a, FR02, HHH01, Hor02, Hos06a, ISW03, LAP08, LLS05b, Mos00, Mos01, RR04, SL05b, TV03,
Kwo02, Kwo03b, LPW06]. Security
[AW05, AW08, Ahm07, AJ08, ADR02,
And07, And08b, Ano2b, Ano06c, AHKM02,
Ayo06, BP07, BW07, Bam02, BPS00,
BRM00, BKRO0, BP02, BNP02, BY03,
BPR05, BOHL+05, BBB+02, Bis03b,
Bla02a, BF06b, BDTW01, BCH07, Boy01,
BLMS00, CGM07, CK02a, CKN03, Can06a,
CGHG01, Cer04b, CC02b, CSW08, Che05c,
CM05a, CH07a, CSY09, Chu03, Coc01a,
CK06, Cor00b, Cor02, CGP+02, CG05,
Dr.00c, Dal01, DN02a, DKMR05, Del07,
DJ06, Des00c, Dim07, DRO2d, DSS01, DK05,
DS05b, DBS+06, Elh09, ELvS01, FIP01b,
FBWC02, FW09, FY06, For04, FML+03,
FMY01, GS02a, GSS03, Gum04, Gut02b,
Gut04a, Gutxx, HM00, HSZI01, Hei07,
HM02b, Hir09, HLL+01, HGPNP03, HQ05,
HL05c, IS04, Ina02a, Ina02c, Int00,
IKY05, IKP07, JYZ04, JP07, JP02b,
JSW05, JG07, Jol01]. Security
[JB05, JK02b, JK02c, JMV02, JQY01,
Kan01, KM02, KSHY01, KL05, Ken02a,
KB06, KMD03, K0001, KM05, Koc02,
KL09, Kos01a, Kov01, KX0001, Lad06,
Lai03, Lan00a, Lan04b, LGS01, Lee04b,
LKH+08, LKHL09, Lek06, Len01, LNS02,
L04c, LSH03a, LSH03b, Lin02, LXM+05,
LWK05b, LP01, MJ07, MS02a, MS09b,
MP03, MF01, MS05b, MV01, MN03, MP05,
Mi010a, NS01b, NDJ01, NP07, Oka00,
OP01a, Ort00, PV06b, PSC02, Pat03a,
Pat04, Pat02b, PD07, PC04, PP03, PP07,
PP07, Pho01, Pie05, Pin01, Po02, PHM03,
Poo03, PF03, PS05, Puc03, Puc06, QC03b5,
RR00, RR03b, RR05, RC01, Rot02a, Roy05,
Rub01, RC06, ST02, Sal03a, SJ09, Sch00d,
Sch00e, Sch07, Sch08, SJO0, Sch01f, See04,
Sha05d, SLH03, SLG+05, SL05a, Shb02,
Sko03, SEF+06, SEK01, SEK02]. Security
[SK06, St03a, SB07, Ste05b, SBZ02, Sty04,
SK01, Sun05, Sw05, Tan07b, TG07, TG04,
TMM07, Uni00a, USE00d, USE01c,
USE02b, Uni00c, Uni00e, Uni00d, Uni00g,
Uzu04, Vau02, VM02, WLT05a, WBL01,
WWL+02, WA07, YEP+06, YWD08, Zan01,
ZWC02, ZD06W, Zhe02b, ZHY03, ZS05,
AA04b, Ano05c, AJ01a, AJ01b, BPS08,
Bai08, Bao05, Be06, Bel07b, BR04, BGP09,
BFGT08, BF08, Bjo05, Ble07, BJ02,
BM05, BG07a, Br06, BPM06, Can01a,
C+02, Cha07, Cha05b, CKL+09, Che00b, 
Che05b, CKT08, Chia08b, Chia08c, Chia08d,
CJ06, CMM00, Con09, Con04, CC05c, DP04,
DKK07, DYO1, DFGH04, Des00a, DW05L,
DK05, DMS07, Eth00, FAXM04, FR08,
FOP06, GH08, GJ06, GJ05, Gha07, GJ03,
Gor05, GKS05, GMW01, GC05, Gut04c,
HN04, HCD08a, HCD08b, Har05a, Hei03].
security
[Hen01, Hen04a, HM05, HSL+02, HL06,
HG05b, Ino05, JEO4, Jan00, Kad07, KY00,
KPS02, Kim02, KVD07, Kov03, KH03,
Kwo03a, LC03, LL03, LJ04, LL05b, LP06W,
L0C+03, LM05, LLLZ06a, LLLZ06b,
LHC08, MJ03, Mal06, Man08, Man05,
Man04, May01, MKK00, MSK01, MG06,
Men03, MS02d, MK05a, MPP09, OP01b,
Pat03, PSC09, PO05a, Pat02a, PY05,
PP06a, Pan03, PHS03, Pip03, Po00, PS04c,
Rie00, RC05, Ros06b, RNO0a, RN00b, SNI00,
Sal05d, Sch03, Sch02, Sch04d, Sen03, SH07,
Shu06, SPH06, Son00, SH00, St02a, St06,
Ste02, Sun00b, SHT00, SL0700, Tsa05,
Uni00f, Vac06, Van03, Voi05, VS08, WAF00,
WDC09, WA06, Won01, WK06, XQ07,
YW04a, YY05b, ZS01, ZW05b, ZS05,
ZH06, ZD07, dCVD05S, vVOW07, vTO05, AG09,
Ano02e, BC05c, BP01b, Chr00]. Security
[Chr01, CCM02, CCM05, CGP03,
JR06+06, Lin02, RR04, Uni00h, ZL04c,
Pap05]. Security-related [Gutxx].
security-sensitive [SPH06]. seed
[TP07, KKJ+07]. Seeing [Wal03]. Seek
[Coc01a, PH03, Sph05]. seeking [Mos06].
Seeks [CAC06]. Seens [Coc02a]. Selected
[BKP09, Bar00c, CCM05, CSY09, GH05,
HA00, MS05a, Neu04, PT06, RAS00e,
Selecting [Bur03, dB07].
Selection [IBM00, JKK +01, RS00, SM08].
Selective [CS07c, LS01a, LM02].
Selective-ID [CS07c]. Selectively [Chi08e].
Self [GMM08, HW05, KY01d, PS01b, PBC05, Sch06b, WHLH05, WLT05b, ZKL01, BCL05a, BCW05, CSV07, CHW00, CCH05, CJ05, Fis01a, HW04, HL04, Lee04a, LL06, LS05b, LWK05a, PC05b, Sha04b, Sha05b, TLH05, Tsa05, TJC03, WH03, Wyl05].
Self-certiﬁed [HW05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HL04, LL06, LWK05a, Sha04b, Sha05b, TLH05, Tsa05, TJC03, WH03].
self-defense [Wyl05]. Self-Enforcing [GMM08]. Self-Escrowed [PS01b].
Self-Localization [WLT05b].
self-modifying [CSV07], self-pairing [Lee04a, PC05b], self-protecting [LS05b].
Self-Shrinking [WHLH05, ZKL01].
Self-Similarity [Sch06b]. Selling [Bla01c].
semantic [PBV08, SNI00, Sch00c, Coc01a]. Semantically [KI01b, ST01a]. Semantics [Li01, Mar02b, BFG04, BFG05, SW02].
Semi [Fer00, Nak01, SY01b]. Semi-Equivalent [Fer00]. Semi-fragile [LY01b].
Semi-fragile [LY01b].
Semicluster [Boud06b].
Sensing [Top02]. Sensibly [Sch04c]. Sensibly [See04, Sty04, Hei03, Sch03].
Sensitive [HT06, Bro05b, SPHH06]. Sensitivity [SDMN06, GSK09].
Sensor [AEAQ05, CS08b, DBS +06, Fin06, GPČS08, LNL +08, NAB03, PDZH09, ZYN08, AJ08, CCMT09, HMDvLM07, JRR09, KXTZ09, KHYM08, LDH06, LPV +09, LN04, Lop06, MWS08, MS09b, NC09, NL08, PS08a, RAL07, TP07, WDLN09, ZSJN07, AMB06].
Sentry [Kum07]. Seoul
Set [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDET00, Che07a, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01].

Sets [CFS05, EIG01, TW07]. Setting [BBM00, DLY08, LP01, PGT07, GMLS02].

settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SGB01].

SGI [Bar00c]. SGID [Tot00]. SHA [AD07, BC04a, GLG02, HKR01, MP06, SK05a, TYLL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TYLL02]. SHA-512 [AD07, GLG02]. SHA1 [BC04a, WYY05d].

SHACAL [KML02]. Shacham [Hes04a]. Shamir [BB79, SP79, Coc03, PW05, VS05]. Shamir's [LD04]. Shape [Gan01b, Gil07]. Shapes [OMT02]. SHARC [DMSW09]. Share [CT08a, CDI05, FS04, AEEdR05].

Shared [AC02, BH06, BBDK00, BT02, CGH00a, TEM01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01]. Sharing [BTW05, BI05b, BTW08, BGP02, CD00a, CFTT07, CC08, CTY09, CDM00, CFT02, CFS05, CDG05, CDI05, Di01, Di03, DS06, DP07, FM02a, FP01, FM01, HN02, Ki02, Kog02, KS03, LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, SZ01, Sun00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CD000, DD04, DM07a, DKL00b, FWT05, GIK01, HT04, HK00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDKST06].

she [Gua05]. Sheets [MNS01]. shell [Dwi04, Gua05, BG01a, BS05]. Sheltering [MYC01]. Shen [KTC03]. Shiek [McK04, CZ03, WYC05]. Shift [CGFSHG09, Che08a]. shifting [Cal00c].

Shin [Kuh08, Kuh08]. Shines [Coc02b]. Shinko [Ano00d]. Ships [Ano02c].

Shops [Ano01c, YSS01]. Shor [KLB02a]. Shores [KKP02]. Short [Ano01k, AFI06, BBS04, BGW05, DN00b, Gra02, LS01b, PM02, RR02, RW02, Vau05b, GL05, WDLN09, C002b, Sch01e].

short-term [WDLN09]. Shortcuts [Sha03a, Shortened [Ku01]. shortest [Pei09]. ShortPK [WDLN09]. Shoup [Luc02b, VMS05]. show [Smi03]. shows [AJ08].

Shrinking [Go01c, WHL05, ZKL01]. SHS [Ano08d, Ano12]. Shuffle [FS01c, NSN05, Sas07]. Shuffles [Mir02].

Shuffling [PBD05]. shut [Gil07]. SIBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [An001i, BU02, KSW00, Law09a, LL01, M602, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP08, WL07a]. Side-Channel [BU02, Law09a, M602, CNPQ03, PSP08].

Side-Match [WC04]. Siena [BCK05]. sieve [CM05b, JL03]. sieves [Har07a].

SIGABA [Lee03c]. SIGACT [AC03c, ACM05b, RA06]. SIGART [AC03c, ACM05b, Sigh [Col03]. SIGMA [Kra03]. SIGMOD [AC03a, ACM05b, ACM04a, FMA02].

SIGMOD-SIGACT [AC03c, ACM05b]. Sign [BCS01b, BTTF02, Dav01c, Kra03, Dav01b]. Sign-and-Encrypt [BTTF02, Dav01c].

SGn-and-MAC [Kra03]. Signal [An002c, GG05b, Sha01e, CKL09, LLL06a, LLL06b, SBS09, Kov01].

Signalling [EC00b]. signals [Ren09].

Signature [ANS05, AAK09, AR00, ADM02, Ano01c, Ano01f, Ano09b, Ano13, Ara02, AR01, ACJ00, Bar06b, BNPS02, BGOY09, BMS03, BDS09b, CM00, CD00a, CL04a, CK02a, CGP08, CH01a, Che02, CM05a, Cor02, CFS01, CS00, DS05a, DKFX05, Eng00, FIP00, Gen00a, GJSS01, GS02c, HY05a, HSL00, Han00, HMR02, JSK01, KC02, Kuh00, LZL01, LP01, MV01, Miy01, Nat00, NZCG05, PL01, PCK02, Pre01, RS01].
SA02, ST01b, SOOI02, SWH05, SPMLS02, Str01a, SYLC05, SSNG500, TMN00, WQWZ01, WBD01, XYL09, YYDO01, YSS+01, YYZ01, YLH05, ZK02, ZJ09, Zhe01, AvdH00, BCL05a, BCW05, Cal00b, CWH00, CL04b, CYH04, CCH05, CJ05, CHC05, Che05a, CJT04, GGG03, HLL02, Hes04a, HPS01, HWW02, HWW03, HW04, HWW04, HW05, HC04a, HLL03, HC04b, HLL04, Kw02, Kw03b, LH04, LHY05, LL05b, LLH04, LTH05, LWZH05. signature
LHH05, LCZ05b, LCZ05a, LW05c, PKH05, PC05b, QC05a, QC05b, Sae02, Sha03c, Sha03d, Sha04b, Sha05a, Sha05b, Sha05d, SCL05, SHT05, TJC03, TYH04, Wan04b, WK05, WLLH05, WH05, Wu01, WHL03, WH03, WY05, X05, YTH04, ZC05, ZF05, ZW05a, ZCL05, ZCW04, RR04. Signature-Based [CK02a].
Signature-Embedded [Ano01c, YSS+01].
Signature-Tree [TNM00].
signature/multisignature [Wu01].
Signatures
AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCC01, CD00a, CL01b, CN06, C30+01, DK01, GMP01b, GM03, GP04b, Gra02b, HS01, Her06, HM02b, HS01b, HHGG+03, HLT01, IR01, IR02, JS05, KZ01, Ka01, LK03, LS01a, Lys02, MR01a, Ma00, MM02, MNFG02, PCG01, Ram01, RR02, Rds01, W001, XS03, Zho02, An006i, Ate04, AH05, BHL06, BB05, BM02b, BMW02a, BLRS09, Cal00a, CKK03, Die00, DM07, Fan03, FW04, FB01, MGLS02, HRL09, Her07, HL00, JLL01, JL04, KKL09, LV07, LG04, LG09, LS05, MM05, PL05a, PV08, 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 [An009], IR01, RR02, HW04, WK05, WH02b. signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imm03, Ree01]. Simple
[AKS06, CYH05, CJS01, CJ03d, CWY05, CC06, CS03c, DT03, FSW01, Gir06, HM02c, HL01, MS01, Nam02, PD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKK03a, LKK03b, LFW04, X05, YRY05d]. Simpler [Lin03]. Simplicity [MS01].
Simplification [DJ01]. Simplications [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 [BD04, TLC06]. Singh [Imm03, Ree01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a].
Single-Chip [MM01b, MM01c].
Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09].
SINOBIOMETRICS [LLT+04, Li05]. SIA [NTW07, PM00, SZ08]. Sir [Bud06]. Site [AEV+07, Coc02a]. Sites [Che04d, Ros07]. situation [AJ08]. six [Bel07a]. Sixth
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, TLC06]. Size
[CS07c, CMJP03, HNZI02, Kal03]. Sizes [An009c]. Skein [AEMR09]. Sketching [MNS08, SLTB+06]. Skipjack
[Gra02a, HSL+02, SLT+00]. Skipjack-like
[HSL+02, SLT+00]. SKLOIS [FLY06]. Skys [MC01]. SLAAC [CGB01]. SLAAC-1V [CGB01].
Slide [Fur02b]. Small
[CMM05, ELS01, Fin02, GPS06, MNT+00, May02, OT03b, RK06, SM02, Sch01e, SPQ06, Wal03, YLC+09, Duj08, dW02]. Small-Project [MNT+00]. Smaller
Smart [And04, Ano03a, Ano05b, AJ01b, Bel01, BCST00, Car01, CL07, CJT02, DF01, DFCW00, DJLT01, HBdJL01, Hen01, HQ05, Jac00, JSJK01, JY01, Lan00d, LSA + 07, MOP06, MV01, MG08, NFQ03, Poh01, QS00, QS01, RE00, RE03, RS01, Sak01, SR01, Sha01e, SP02, TBDL01, VP01, YKMY01, Ano00k, Ano00l, Ano04e, AJ01a, Bor00, BPR01, BCHJ05, BGL + 03, Cal00c, CCCC01, Cha05a, Cla00b, Con00, CH00, DM07t, DFH01, DFPST07, FCZ05, Fin03, GM00, GU01, HHSS01, Hu05b, Hu01, Jua04, KLY03, LKY05a, LKY05b, LKY05c, Ler02, LC05a, Lu07, MY01, Pha06, Pb01, Pre07, SVDF07, SLH03, Sm00, TIS07, VK08, WC03b, YY04b, YWDD08, Za00, BJVDB02, CL04d, CCK04b, Che00a, DFP06, FGL02, Gro03, HL05b, Ku04, KC05, KY05a, MC06, Pau02b, SSKS00, Sc00, SCF01, TBDL01, VPG01, YKMY01, Ano00k, Ano00l, Ano04e, AJ01a, Bor00, BPR01, BCHJ05, BGL + 03, Cal00c, CCCC01, Cha05a, Cla00b, Con00, CH00, DM07t, DFH01, DFPST07, FCZ05, Fin03, GM00, GU01, HHSS01, Hu05b, Hu01, Jua04, KLY03, LKY05a, LKY05b, LKY05c, Ler02, LC05a, Lu07, MY01, Pha06, Pb01, Pre07, SVDF07, SLH03, Sm00, TIS07, VK08, WC03b, YY04b, YWDD08, Za00, BJVDB02, CL04d, CCK04b, Che00a, DFP06, FGL02, Gro03, HL05b, Ku04, KC05, KY05a, MC06, Pau02b, SSKS00, Sc00, SCF01, TBDL01, VPG01, YKMY01.

Smart-card [GMG00]. Smartcard [HWH01, KRV01, RMCG01, Uri01, PBVB01, BBPV00, CGMM02, DM07b, HRS02, Ito01, KS02]. Smartcard-Based [CMG + 01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, Ano04c, RM02]. Smarter [Car01, Cla00b]. Smartly [MS01]. Smooth [PS02b, GMR05]. SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. sneak [Ade09]. Sniff [Ano02e]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sae02, Sha03c]. Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Ahn07, And07, Ano02c, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HMM01, He01, Joh03, Knu07, KSZ02, Lad06, Law09a, LSY01, LLLZ06a, LLS09, LTM + 00, MNT + 00, MSNS07, MKNG08, MG06, N005, PM00, PS01c, RM04, Sch01a, Sch00b, Ste00, USE00b, VH09, VVS01, WLLH05, Wo04, ZCC01, ARJ08, Ano00h, Ano00j, Bir07, Che01c, CT02, CCH + 04, CTT07, CC04c, DMS07, GPS05, HMO4, HL06, Jen09, KA09, Mat02, Mc08, MCHN05, Pau03, Sch01d, SS03, WL07a, WA06, Sal03b, Bol02]. Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [Hoe01]. Software-Oriented [ZCC01]. Software/Headware [Nd05]. SOI [Ano02e, NFQ03]. SOISIC [Ano02c]. Solaris [Ano06c, BHO0b]. Solomon [KY02b]. Solution [Cap01, CJT02, DHR00, LL05b, Poh01, Str02, TVdK + 01, LSH00]. Solutions [Ano04c, MV01, Jan00, MSK03, MV03b, St.00, Gum04]. Solve [CU01, GSD03]. Solving [CJT04, GPP08, W01a, Bul09, Wh09]. Some [AG01, BDF + 01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HAN04, He02, JK01a, RSS04, SHT05, ZF05]. Someren [Ano03f]. Something [FL01]. Sometimes [FRN05]. Sons [And04]. Sorry [San05]. sorts [Ano03f]. Soul [Bla01c]. Sound [BP02, FR08]. Soundness [ABHS09, DP04, MR01c, MPS08, LA08a]. Source [Bar00c, Bol02, Gut00, HP09, KLR09, PM00, RK06, TEM + 01, Ano03c, BCL + 03, CBB05, MC08, RV09, SB05, Bar00b, Lin02]. Sources [KZ07, WLZZ05, KZ03]. Southampton [Bla03]. Soviet [AJ08]. SP [BG07a, Hir09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPA-Based [Nov01]. Space [BGH07, Lu02]. Space-Bounded [Lu02]. Space-Efficient [BGH07]. Spain [BS03, DFP06]. Spam [CMB + 05, DGN03, Vix02]. Spamming [Bal04]. SPARK [Jen09]. Sparse [BLST01, BDG + 01, FS01b, GS03, BF06a]. Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09]. Spatial-Domain
Spatio-Temporal [CTTT05].

Spatio-Temporal speakables [BZ02].

Speakers [VN04].

Spec [Bar00c]. Special [Ano04b, Ano07b, Ano07a, BK06b, GIS05, GS07a, GPP08, SGK08, KP03, FOP06].

Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08].

Specialized [Wan04b].

Specific [HCK09, Zir07].

Specification [BCST00, ECM00a, LKJL01, RSA00c, Mea04].

Specifications [IEE00b, BDFP05, BD04a].

 Specification [BCST00, ECM00a, LKJL01, RSA00c, Mea04].

Specificity [GSK09].

Specified [Tad02, He02, LWK05b, YY05a, ZX04].

Specifying [BJvdB02, Cir01, SBS09].

Speck [KGS07]. Spectr [GMM01].

Spectr-H64 [GMM01].

spectra [MS02b].

Spectral [QPV05, SK07].

Spectrum [BQR01, LY07, PM00].

Speech [MRL+02, AA04a, PY08].

Speech-Generated [MRL+02].

SpeechStudio [Ano02e].

Speech-generated [H601].

SSL [ASK05, BPST02, CHVV03, JRB+06, KCD07, KPR03, Kra01, LLK05, LWK00, Net04, OHB08a, OHB08b, SB01, SQ01, Van02, ZFK04].

SSL/SSS [BPST02, CHVV03, KPR03, OHB08a, OHB08b].

SST [Gau02].

Stack [Pot03].

Stage [Kak06, CHY05b].

stamp [CL00].

stamping [HHC05].

Stamps [KZ01].

Stand [CAC03].

Standard [Ano08d, Ano09b, Ano12, Ano13, Bar00a, BCP02a, FIP00, FIP01a, FS01a, Her09a, Hug04, HLC08, IE00b, MM01c, MP01a, Nat00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, BBK+03b, DR05, GMR08, Sea09, Tan01, Ase02, Bar00c, HI00, Bur03, CMR06, Coc02a, Coc02b, Cur05, DR01, DR02b, Dan01, FIP02b, GC01a, Har00, Lan00a, Lan00b, Lan04a, Mor05, NIS00, B00, Sta00, Sy00, WBRF00, Wri01, YW06].

Standardized [Man01].

Standards [Ano01f, Bur06, CL07, Coc02b, Hus01, RSA00a, Tsa06].

Standing [Man01b].

State [And07, CR03, G04, HBF09, Kar01, MSNH07, Ris06, TL07, Mit00].

State-transition [TL07], statecraft [dL00].

Stateless [ANR01, NNL01, SK05b].

Stateless-Recipient [ANR01].

States [LB04, Jo01].

static [CW07].

Statistical [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, LZ01, LL+01, MV03a, Neu04, Pro01, RSN+01, BKW03, GSK09, Hey03].

Statistically [Fis01b, HR07, HNO+09].

Statistically-hiding [HR07].

Statistically-Secret [Fis01b].

Statistics [CNK01, CNK04, KLML05].

Status [Pre01, Sha03b].

statute [Cal00b].

STDM [WMDR08].

Stealing [Gan01b].

Stefan [AUW01].

Steganalysis [Pro01, Sal05b, GSK09, WW04].

Steganografie [Sch09].

Steganographic [CTL04, HR02, LL02, MJF07, RH02, RS00, Wes01, KG09a, LY02, WW08, YCL07].
Steganography
[BC05a, BG10, CHLY09, CDR01, CW09, CTH08, Co10, CM10, CS05, DDIR05, DRL09, FGD01, Fri07, Gal03, HCBLETR06, Hlva02, HAG09, Hun05, HSKC01, LS08, PH03, Sal05, Sch09, Sha01, Shi08, SWR05, Van05, WW06, CDS07, CO09a, Che07a, Che08a, GGS09, JD01, KP00, LT04, WW04, WM08, Way02b, Wy09, YCYW07]. stego[KC09a]. stego-image[KC09a]. Steiner[WL02]. Step[DRL09, KKKL09, MP07, SL06]. step-by-step[SL06]. Step-out[KKKL09]. Stepping[WRW02]. sterile[Bih02]. Stereotypes[GO03]. Stern[CGP08, CS05b]. sticker[GPX08]. Sticks[Sam01]. still[Ano00f, Rie00]. Stinson[Spr03]. STL[Zol01]. STOC[ACM05c, ACM07, ACM08, ACM09]. Stochastic[MG01]. Stock[Bar00a]. Stone[MLM03]. Stones[WRW02]. stop[SSNGS00, Win05c]. Storage[DFSS08, Din01, Din05, HR02, Hart07b, Hug04, MSTS04, RCBL00, Ric07, RH02, Vao03, AFG06, DFS05, HGR07, LP05, SGMV09]. Store[CTBA01]. Storing[ST06]. Story[Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Han06, Hig08, HS01a, Win00]. strategic[AJ08]. Strategies[Cir01, KL05, SKQ01, Dwi04]. Strategy[DR02a, TP07, KCC09a]. Stream[BCCO1, BC05b, BS00b, BL02, CF01b, Can06b, CJ01, CH03, CM03, Coo13, CL02c, DF07, Fl00, FF01a, Gol01d, Gol10e, GBM02, HCJ02, HR00, HR04a, Jam00, KH01, MSNH07, PP06a, SM01, Sar02, SXY01, WB02, Wu02, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, BVP04, DS09, DK08, KH08, Max06, MI09, PCS03, PCC03, SB05, WW08]. Stream-Cipher[SXY01, WW08]. Streaming[OS05, CBB05]. Streams[AIP01, CO09a, YLC09, ZCW04]. Strength[CB01, JX05, Oni01, CKL09]. Strengthening[Loi00, MHH02]. String[CPS07, DFS04, Pas03, Dam00, RG05]. Strings[Vau05b]. Strong[ADD09, BB00b, CS00, DFK05, KJ01, KW00, LSH03a, LSH03b, Lu02, Far09, SBS02, WKL05, CC04b, HRS08, KT03, Ku04, LL05b, SS03, ZT03, ZFK04]. Strong-Password[LH03a, LSH03b, WKL05, CC04b, KT03, Ku04]. Strongly[IY06]. Structural[BS01c, LBR00]. Structure[DP07, EIG01, H301, HLL01, MR02a, MR02b, GT02, HSL02, MF07, PS02a, SG07, SLL00, XMT07]. Structured[BRTM09, CK03]. Structures[Ano02e, DS06, GT03, HCDO02, KCP01, Kus02, MND04, MFF05, PSC04, PQ03b, Sun00a, XH03, Hen06a, IY06, SWR05]. struggle[Bur02]. Stuart[Gun04]. students[AA04b, PP09]. Studies[Pag03, LFHT07, SPHH06]. Study[BBGM08, Car02, DFR01, DP00, KJ07, WC05, BKN04, BF06a, DY09a, KWD06, SK04, ZWWL01]. Subgroup[NBD01, KM04a]. Subgroups[GRO05, GMR05]. subliminal[LH04]. subsampling[LLC06a]. subscribe[SL05b]. Subscriber[CFRR02]. subscription[MW06]. subscription-based[MW06]. subsets[Sch01]. substitute[Bih02]. Substitution[KKG03, GP05, RF08, WL04b]. Substitution-Permutation[KKG03]. Subsystem[HL07, MBS04]. Subtleties[Lai08]. subverting[HB06]. Success[Ano06d]. Successful[KH03]. Succinct[BA06, FS08]. Sued[Nic01]. Sufficient[KO05, KO01, MTO1]. Suffix[ABM08]. SUID[Tot00]. SUID/SGID
Suitable [AIK+01, CQS01, KTT07, LKHL09, SP05, Wen03].

Suite [RSN+01, SBEW01, YLT06]. Suited [WWGP00].

Sum [Che04b, KLY02].

Sum-of-Digits [Che04b].

Sums [CY08, Shp05]. Sun [Che04b, KLY02].

Sunspots [CPS07].

Super [Lam07, CAC06, Hos06b]. supercluster [Pri00].

Supercomputer [Coc01a, Wal09].

Supersingular [Gal01, RS02, Ver01].

Supervision [FDIR00].

Supplemental [TBDL01].

Supplementary [ECM00a, ECM00b].

Supplies [Sha01c].

Support [ABM00, Gro03, LTM+00, PZDH09, SBG02, Ano05c, BMA00a, BMA00b, BMA00c, ED03, mSgFlt05, SSM+08, WQN08, ZYL05].

Supporting [CLK01a, SW02].

Supporting [CLK01a, SW02].

Survey [Che01f, LCS09].

Survey [EPP+07, FDIR00, KM04b, LDH06, ATS04, Ano00e, BEM+07, CF05, CDL06, EY09, LOP04, Men04, Mü01b, OZL08, PC09, Pre07, RH03, RAL07, Sch01f, ÜG08, ZLZ07].

Survivable [CLZ02].

Survivable [CLZ02].

Symbiotic [Jan08a]. SVD [BBC+09, CYH+07, FWL08].

SVD [BBC+09, CYH+07, FWL08].

SVD-based [CYH+07, FWL08].

SVD Grid [ZBP05].

Sweden [BS01b, JH03]. Swedish [BEC02].

Swiss [DZ00, Kid00].

Switzerland [CC04a, Vau05a].

Symbiosis [DF01].

Symbol [SVD07]. Symbolic [Bor01, JEF08, Mar02b, May09, MT07, MP05, ALV02].

Symbols [Lum09].

Symmetric [Bor01, JEF08, Mar02b, May09, MT07, MP05, ALV02].

Symmetric [Bor01, JEF08, Mar02b, May09, MT07, MP05, ALV02].

Symmetric-Key [Ano01j].

Symmetric-Key [Ano01j].

Symmetry [RBF08].

Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, Ano00d, BS03, BCDH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, JEF08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05].

synchronization [CMdV06].

Synchronisation [GPCS08, SW02].

Synchronizes [Pau02b]. Synchronous [CH01b, Sar02].

Supernovae [YLC+09].

Syntax [BWBL02, RSA00b, RSA00d].

Synthesis [XF01, SOIG07, UBE09].

Syslogs [ME08b].

Survivable [CLZ02].

Survivable [CLZ02].

Systems [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, Ano00d, BS03, BCDH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, JEF08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05].
[ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bih03, Boy01, CC04a, Cra05a, Des02, Fal07, HR06, Hay06, IR00, Irw03, Kin01, Kin02, Lai03, Lee04b, Lut03, Mao04, NP02a, Nao04, Oka00, PY06, Pri01, Pre00, Rol05, Roy05, Sch06b, Shp03, Spr03, TW02, TW06b, Vau05a, Wal00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cas06, Cos00, Dw05, Gar04, HHL00, HW98, Joy00, Kil05, Laf00, Lam01, PPV96, Rot02b, Rot03, SCS05a, Sho05b, Ste08, Sti95, Sti02, Sti06c, Tat05, TW05, Was08b, HR06, KXTZ09, Kil05, Nao04, Nie02a, Nie04].

There [Bar00b, GW00].

Think [Pau03].

Thinking [See04, Sty04, CS07a, Hei03, Sch03].

Third [AL06, BS01b, CGP03, HR06, IKY05, KNP01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QS00, CGH00b]. third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM00].

Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thiry-Fourth [ACM02]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT00]. Thoughts [Jo00]. Threat [Por06, SS04, BK00, Geb04]. threatened [An00b]. threats [CNP03]. Three [BR00b, Kak06, LSH00, MAaT06, AJ08, CLC08, FG03, GPS05, LHL04b, LKY05b, LLS09, MF07, MAaTxx, SPH06, YC09a, ZL04b]. Three-Key [BR00b]. Three-party [LSH00, CLC08, LHL04b, LLS09, YC09a].

three-principal [ZL04b]. three-stage [ZL04b].

Threshold [Kak06].

AF04b, AIP01, BTW05, BTW08, BDDS03, BS02, CCD07, CLT07, CDN01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, KS05b, Kin00, Kin02, Kog02, LZZ01, LSC03, LCL05a, LP01, MSJ02, Nie02c, STY07, WQWZ01, Wan04b, WH03, XS03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, CHE05a, DG06, HWW02, HWW03, HW05, JLL01, JL04, LCC05, LCZ05c, SCL05, TYH04, WHH03, XC05, YTH04].

Throughput [HV04, LS01b]. thwarting [WL07a]. thwarts [Ade09, SW05b]. TI [GBKP01]. tib [MAaT07]. Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07].

Tight [CM05a, Dl01]. Time [AK02a, App07, AJO08, BPST02, BS00b, BS01, CU01, CJ03a, CN06, CLZ02, Dri02, GPC08, HM02b, Ina02b, KL05, Kuh02a, LP02a, Lan00b, LLL05, LDM04, May04, Oec03, Ple01, QSR02, RR02, CAC03, CCK04b, CL00, DS02, GS07b, GM04, HLTJ09, HHC05, LC04a, MRST06, NS05a, YZD07, hY08, DK08].

time-bound [hY08]. Time-Domain [Ku02a]. Time-Free [CN06]. Time-Limited [AK02a]. Time-Memory [AJ08, Oec03, QSR02].

Time-Memory-Data [DK08].

time-reversed [Ina02b]. time-space [NS05a]. time-stamping [HC05].

Time/Memory/Data [BS00b]. Timed [BN00b, CHK08, JP07, LKJL01, Mao01, HGN03, Zha06].

Timed-Release [CHK08, Mao01, HGN03]. times [AJ08, CCK04b, Mol05].

Timestamp [CC01b, FLZ02, SLH03, WLT03, YW04a].

Timestamp-Based [CC01b, FLZ02, SLH03, WLT03, YW04a].

Timestamping [MST04]. Timing [CKQ03, CWR09, Law09b, Sch01b, SWT07, ASK05, DKL00a, KS09a, OS00].

timing-attack [KS09a].

Tiny [Bar00b, Min03, WN95, And03].

Tipsy [TvdKB01].

Tissue [MYC01]. Title [ZYH03].

TLS [BPST02, CHV03, HSD05, JK02b, JK02c, KPR03, OH80a, OH80b, SBEW01, BFC08].

TMAC [KI03].

TMS320C6x [WWGP00]. today [Lie05, Nis03a]. Together [WD01a]. Token [Fri01, RSA00d, RSA01, CS04]. tokens [WDC09].

Tokyo [Ano00d]. Told [ES00a].
Tolerance [Ano04b, BK06b, ZL04a].
Tolerant [DS03, HSKC01, WL07b, BKW03, HGR07, Lin07, PI06, RMH04, Ybj04].
Tolerating [KSR02, SKR02].
Toggling [Sch05c, vT01].
Tools [Ano02d, Ano02e, Kil01b, GPG06].
Toolkit [NIS01a, Sha01a].
Tools [Ano02d, Ano02e, Bar00b, Gol01b, Ken02b, Ust01b, Bai08, Cas02, CT02, GC05, NCRX04, SETB08, Kat05b, Puc03].
Toolset [Jen09].
Top [Cal01, Fox00, Jan06, MV00, AJ08, GPC08].
Tophandle [GPC08].
Top-Level [MV00].
Topics [HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oka04, Poi06, Pre02c].
Totality [HR08].
Touch [Pau02a, JP06].
Toughest [Min03].
Tour [Pet08].
Town [KJR05].
Trace [Bor01, LNS02, NN03].
Trace-and-revoke [NN03].
Traceability [HLL03, HW05, WLHH05, WY05].
Traceable [LZL01, CCH04].
Traceback [CS04].
Tracing [KYO1d, KY01e, LLL02, NNL01, SNW00, TTO1, WRW02, WLZZ05, WH01].
Tracings [RE02].
Track [Fox00, Joy03b, Nac01, Oka04, Poi06, PHS03, Pre02c].
Trade-off [AJ008, CSM09, Oec03, PS01c, Uni00f].
Trade-Off [AJ008, Oec03].
Trade-Offs [PS01c].
Tradeoff [LP02a, QSR+02, CW02, Ino05, NS05a, DK00].
Tradeoffs [BS00b, CTL01, SRQ03, SU07].
Trading [PV06b, SWH09].
Traffic [FGL02, Mis08, Fie09].
Trail [DR02a].
Train [Fro00].
Training [Coc02a].
Traitor [KYO1d, KY01e, LLL02, SNW00, TTO1, WH01].
Transacted [HBdJL01].
Transaction [RH02, AAKD09].
Transaction-Based [RH02].
Transactional [ST06].
Transactions [Ca00b, Ca00a].
Transcript [Ano01a, Ano01b, Ano01c, Ano01i, Ano01j, Ano01e, Ano01k, Mal02, Nik02b].
Transfer [CT08b, Din01, GKM00, KKL09].
Transferability [HSZI00].
Transfers [IKNP03].
Transform [AB08, BBC09, BR09, CPhX04, KC09b, LKLK05, Nak01, SSFC09, VK07, BR06, Che07a, OP01b, SR00, LPZ06].
Transformation [CT09, HLL05, DSP01].
Transformations [Fel06, KHC01, LMTV05, Pag03].
Transforms [La00].
Translative [HLL03, VS08].
Transistor [Coc02a].
Transistors [Bar00b].
Transitive [BN02].
Translation [GGS09, PY06].
Translation-based [GGS09].
Translation-based [GGS09].
TransLink [Ca00c].
Transmission [MLC01, SNR04, SVD07, SMI03].
Transparent [CCDP01, Por01, Lin00a].
Transport [Bor00].
Trapdoor [BPR08, Fis01b, KO03, KKO00, Gen04a, JS05, PW08].
Trapdoors [GP08].
Trapping [Min03].
Travel [Bur00].
Traversal [JLMS03].
Trawling [Knu00b, Knu00a].
Treatise [Bla00, MAaT03, MAaT04, MAaT07].
Treatises [MAaT06, MAaT07].
Treatment [CL05, DK08].
Tree [CC05d, GST04, JMS03, KPT04, LKLK05, LM02, TN00, Mon03, PCC03, WL02].
Tree-Based [GST04, KPT04].
trees [Che02, Che07a, TC00].
Tricks [All03].
triggered [HJW05].
trivial
Tripwire [TvdKB01].
trivial
True
[BST03, Cha04, DV08, EHK+03, HBF09, Pan07, SFDF06, BG08, BG09, GB09, Hau06, HLwWZ09, Ste05c, vT01, VKS09].

Truecrypt [CSK+08, truly [BGL+03].

Truncated [CS05b, KM02, LHL+02, SKU+00, SKI01, GS09].

Truncated [CSK09].

Trust [CS05b, KM02, LHL+02, SKU+00, SKI01, GS09].

Trusted [CHSS02, HCDO02, Lin00b, LHL+08, Mit02, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, LMW05, LLW09].

Trusted [DK01, WHI01, WV01, ARJ08, PS04c, ZYL05].

Trusting [CKS09].

trustworthy [CCH05, SK03].

Truth [MNT+00].

Tseng [Hwa05, XY04, ZAX05].

TTM [GC00b].

Tuesday [Uni00a, Uni00f, Uni00e].

tunable [LB05].

Tunny [Sal01a].

Turin [AL06].

Turkey [Bor00].

Turkish [DD02].

Turn [Tsa07].

Turning [DJLT01].

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

TV [Smi03].

Tweakable [DS08, HR03, LRW02].

Twentieth [Gan01b].

Twenty [ACM03c, ACM05b, AAC+01, B+02, Lan00a].

Twenty-Eighth [B+02].

Twenty-first [Lan00a].

Twenty-Second [ACM03c].

Twenty-seventh [AAC+01].

Twin [Ram01].

TWINRL [Kal03, ST03b].

Two [Ahm08, BDG+01, DIS02, FD01, Hen06b, HSR02, HSS01, HU05, HL05b, JZCW05, KCP01, KO04, KTC03, KI03, Lin01c, MR01a, MLM03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, St.00, Ste05a, Ste01, TW07, WW05, X503, YWWD08, YYDO01, CLOs02, DHL06, GCKL08, HW03c, JW01, LMTV05, MS09c, MC03, MCHN05, Pan01, Pha06, ZLX99, dB07].

Two-Block [KCP01].

Two-channel [MS09c].

Two-factor [Hen06b, Sch05c, St.00, Ste05a, YWWD08, dB07].

Two-Key [KI03].

Two-level [DHL06].

Two-Party [KO04, Lin01c, MR01a, WW05, CLOs02, GCKL08, JW01, ZLX99].

Two-Pass [SK00].

Two-tier [TW07].

Two-Way [DIS02].

TWOBLOCK [Yan05].

Twofish [BF00b, FSKW00, IK00, Kel00, Knu00a, Knu00b, Luc02a, Mur00, SKW+00].

Type [CKQ03, Dug04, H601, KYHC01, PDMs09, RMS05, Vir03, GG08, PQ06, Sha014].

Type-based [Dug04].

Type-Passing [Vir03].

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].

UC-soundness [BPS08].

UCON [LY05, PS04b].

UK [CZ05, Ch00, Ch01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01].

Ultimate [Dif01].

Ultra [Bam02, CH07a, DB04, Cal01, Win00].

ultra-lightweight [CH07a].

ultra-secret [Bam02].

Ultrafast [FF01a].

UltraSONIC [MMH02].

Ultrawideband [Bra06].

UMTS [Cha05b, HL07].

Unauthorized [Ano02c].

Unbalanced [FMP03, May02, HLL03].

Unbelievable [Len01].

Unborn [Pau02a].

Unbounded [RW02, WvD02].

Unbreakable [Ver06b, Mlu02].

Uncertain [See04, St04, Hein03, Sch03].

UNCITAL [MNFG02].

uncompletable [NS01a].

Unconditional [HM01b, May01, Pas05, RW03b, WW05].

Unconditionally [HSZI00, HSZI01, HSHI02, HSHI06].

Uncovering [MNT+00].

Uncrackable [An03c].

undeciphered [Rob02, Rob09].

Undeniable [GMP01b, GM03, JSJK01, Miy01, WQWZ01, CHC05, LH04, LCO50a, SSM+08].

undergraduate [AA04b, Gha07].

undergraduates [DFGH04].

Understanding [AN03, CPG+04, Cra05b, Elb09, Gor06, LG09, PP09, Sun05, Lun09].

undetachable [BMW02b].

Unexpectedly
Bar00a. **Unforgeable** [BKY02, KY01a].

Unhooking [Moo01]. **Unicode** [MJF07].

Unified

[CZB+01, HKA+05, MFS+09, SM03b].

**Uniform** [SPK08, TL07, SU07]. uniformity [Shp01, Shp04b].

**Unimodular** [CV03].

Unique [Lam91, Lys02, TH01]. United

[DFCW00, Jol01]. **Universal**

[BOHL+05, CR03, CJNP02, CS02, Ifr00, KKKP05, KO03, Pli01, Sho00a, SP79, Cal00c, PS04c].

uniformity [SPK08, TL07, SU07].

Universe

[AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, CS02, Ifr00, KKKP05, KO03, Pli01, Sho00a, SP79, Cal00c, PS04c].

Universally

[AF04b]. Universally-Composable

[AF04b].

**Universiteit** [BBD09]. University

[Kat05b, Puc03, Rot07, Top02]. UNIX

[CCDP01, Har01a, Har01b, Hof01, Wit01, GSS03]. UNIX-Type

[Hof01].

Unknown [CT08a, Luc01a, CKB02b, CLOS02, DN02b, DN03, NMO05, RK05].

Universally-Composable [AF04b].

Unrecognizably [Wal04]. **Unsolved**

[GG05a, Bel07a]. untold [DB04].

untraceability [CL09, LHY05, Par04].

**Untraceable** [ACdM05]. Untrusted

[BMK00, CGK+02, LSVS09, LSK05, ZBP05].

Unusual [GG05a]. **Unveiled** [Bar00a].

Update [Das08, TEM+01, Heg09].

Updated [Cho08a]. updating [LH03].

upgrade [Pau02a, Pau02b]. Upgrades

[Ano02e]. upon [DFG01, PQ03a].

UPPAAL [BBD+02]. Upper

[BP03b, DIR05, KMT01]. Upset [Bra06].

Upwards [FV03]. **URSA** [LKZ+04].

**US$54** [Duw03]. USA

[ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KKP02, KJR05, Kil05, KP01, Men05, Men07, Nac01, Nao04, Oka04, Poi06, Pre02c, Sch01d, Sho05a, SI01, YDM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FMA02, IEE01a, IEE05a, IEE05b, IEE08, IEE09b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SMP+09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, Wil99, Yum02a]. **usability**

[CG05, WDC09]. **Usage** [LY05, PS04b].

Use

[Bai01a, BWBL02, Bol02, BQR01, CPS07, Dre00, ISO05, Kra03, LCK04, Pau09, PTW07, Str01a, WS05, Win01, CG05, OS07]. used [CDL06, MSV04]. useful

[SM03a]. **Usenet** [Coc01a]. **USENIX**

[Coc01a]. **User**

[Ano00k, BGP02, CL01b, CMB+05, DPO0, FDIR00, Had00, HY01, KZ09, LSZ05, MR03, OHB08a, PS01b, Poh01, Nas07, Semester08, Str01a, Tsa01, WDC09, BBM0, CL04d, CH08b, CH08c, CH08d, CF07, DSGP06, DLY08, GMLS02, HW03c, Hsu05b, HL05b, KCC05, LAPS08, LHY02, LLHO02, LKY04, LKY05a, LHL03b, LOK05a, LOK1, OHB08b, Par04, SS03, SZS05, TWL05, WLT05a, WC03b, YW04b, YS04, YRY04, YRY05d, ZYL05, vOT08].

User-Centered

[CMB+05].

user-controlled [LAPS08]. user-drawn

[vOT08]. **user-friendly** [SZS05, WLT05a].

user-level [SS03]. Users [LLS05b, CF05].

Uses

[Bau01c, RSQ03]. ushers [Bur00].

Using

[AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01c, Ano01j, ADDS06, BPI01, BH06, BK06a, BBC+09, Bua01a, Bua01b, BP06, BPS02, BUR09, BTO2, BMK00, BNP00, BL02, Cle01a, CLL00, CGBS01, CCW02, CCM01, CC06, CH07c, Cir01, DI05, DPR01, DP00, DWN01, DGH+04, EFY+05, F030, FMP03, Fri01, GC01a, GL01, GSB+04, HHGP+03, HQ05, HJW01, Jab01, JKK+01, JSJK01, KOSY01, Kel05, KM01a, KLC+00, KTT07, Kra02b, KZ09, Lao04a, Len01, LB04, LS05a, LM02, LH07, MS02a, MS09a, MLM03, MS03b, MMJ05, NZCG05, NM09, OT03a, PPK+01, PJH01, PJK01, PCK02, PK01, Sho00b, SK05a, Sma03a, SVW00, SP04, Ste01, ST01c, TSO00, TL07, TK03, TTT01, VPG01, WY02, Wit01, WC03a, XFZ01, YKM01, YLLL02,
YSS+01, ZWWL01, Zhe01, ASW00, AL07, BCL05a, BCW05, BK07, CG06. using [CD07, CWH00, CL04d, CCK04b, CCH05, CHY05b, CK05, Che07a, CKY07, Che08a, Che08b, CJ04, CKK03, Cos00, DZL01, Dan02, DSGP06, DS09, DFG00, FWT05, GC00a, GMR05, Gen09b, GS09, HHSS01, HWW05, HAuR04, HTW07, Hir09, HW04, HLTJ09, HY03, HL04, JRR09, Jua04, KOY09, KLY03, KB09, KKL09, KK07, KSW06, KR03, Ku04, KC05, LHY02, LLH02, LKY04, LCP04, LL04b, LW04, LKY05a, LLW05, LLW09, LFW04, LC05a, LLC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SHH07, Tan07a, TLH05, Tsa05, TJ03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04a, YW05, YC09a, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. utilising [RFR07a, RFR07b, RFR07c]. utility [Gua05]. Utilizing [Str02].

V [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00e]. v2.1 [RSA01]. V5 [ito00]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BLM01, KCI+01, BC01]. Validity [Zho02]. Valuable [PM00]. Value [BR09, GIS05, LS08, BMW02a, DK08, WWTH08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadharajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSNK05, Ber08, Duj08, Duj09]. Variants [BDK07, DG02, KSO0b, CJ05, Sha04b, TJ03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDhKB09]. vast [Wai04]. vault [SCHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pei09, nSgfT05, WNQ08, WC05]. vectors [LHL04a]. Vegas [ELvS01, IEE01a]. Vein [BDhKB09]. Vendors [Pau03, MV03b]. Venona [Ben01b, Ben04]. venture [SW05b]. Verenigde [dl00]. Veridicom [Alo02d]. Verifiabile [ANR01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Lys02, NZCG05, NZS05, NNSK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a]. verifiably [BGLS03, Hes04a]. verifiably-encrypted [Hes04a]. Verification [AADK05, Ara02, BPST02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJL06, Col03, DS09, HL05c, JW01, Ler02, MD04, MT07, MSP09, PBD07, Tsa08, TYH04, Wan04b, Wu01, YLC+09, ZLX99, ZL04b, CS08b, Uzu04]. Verified [BJP02, BFGT08, BFCZ08, CJT04]. verifier [Bla01b, LKY05b]. verifier-based [LKY05b]. Verifiers [CL01a, He02, LV07, LWK05b, YY05a, ZO04]. Verify [MS02a]. Verifying [BFG08, BJvdB02, CJM00, HLTI01, IR01, PT08, RR02, BLH06, BLP06, HLH00, SV08a, Sha01d]. Verlag [Eag05, Lee03a, Lee03b, Pap05]. Versions [BS02, HPC02, OST05, SKI01, Mis06]. Versus [Mad00, Rub00, WWL+02, ASW+01, BJLS02, DBS01, WPP05]. Vertically [DN04]. Very [AAC+01, B+02, CG03, EBC+00, FLA+03, HOI+01, PM02, PBMB01, Zir07]. Vestiges [Top02]. VI [SCH04a]. via [AGKS07, An00k, ACD05, BDPV09, Car02, Che03, CPG+04, FBWC02, Fox00, HYV07, HLM03, J00a, KT06, ML05, PG05, RG05, SB01, SLG+05, ZLGD01, Lud05]. Victoria [ACM08, IZ00]. Victorian [Top02]. victory [Hau03]. Vid [CAC06]. Video [BDF+01a, BD03, CDTT05, EFY+05, ISSZ08, KBD03, KJR05, KLL01,
LHS05, MLC01, SC02a, BS01b, CO09a, JA02, KN03, UP05. Video-Based [KJRI05, BS01b, KN03]. videos [YZDW07]. Vienna [BZ02]. Vietnam [Lov01]. View [BAR00a, Mah04, Sin09]. Views [BAR00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03]. Vigènère [DG00]. VII [SCH04b]. VIII [IEE01b, Sch05a]. Virginia [MS05b]. Virtual [ANO01c, HM01a, PPR00, 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, AN05c]. Visible [HT06]. Vista [FER06]. Visual [BDN00, BDDS03, BCD06, CCL09, CTY09, CPD06, DD00, KOG02, KS03, RD09, WMS08, YWC08, YC01, ZP05, ABDS01, CDFM05, CDD07, DD04, HKSS00, LAX09, PY08, Yan02, YC07, Bon00, ZOL01]. Visualization [XYL09, MFS+09]. Vital [WAL04]. Viterbi [LBGZ01, LBGZ02]. Vladimir [PZU04].

VLDB [EBC+00, FLA+03]. VLDP [B+02]. VLSI [KV01]. VMSS [SC05a]. Voice [AN001, PK01, VN04]. VoIP [ANO08c, SZ08, VAY09, WCJ05]. vol [KAT05b, LEC03b]. volatile [SETB08].

Volume [GOL04]. Vortrag [EK02]. Vote [CHE07b]. Voter [CHA04]. Voter-Verifiable [CHA04]. Voting [CHA04, FPS01, HS00, JOH05, JLL02, KMO01, RUB01, CTD03, HJW05]. Vouchness [RUG04]. VPN [KMM+06]. VPNS [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 [DV06]. Wagstaff [KAT05b]. Wahab [MAAT07]. Walking [FOX00]. Wallet [ETZ00, JL04]. Walsh [MS02b].

Walsingham [BUD06]. WAN [H6IO1]. WAN-Cluster [H6IO1]. Wang [SJS05]. Wants [HAN00]. WAP [JRFH01]. War [BEC02, BUD00a, BUD02, HAN03, KVO01, MH09, OC03, AJ08, DB04, RIS06, LOVE01]. Warfare [HW01, WW04]. warrior [PC04].

Wars [RR03b, CAL04d, CAL04e]. Warsaw [AUW01, BIH03]. Washington [S+03, USE00a, USE01c]. wasn’t [BUR02].

WaSP [COC02b]. WASSA [AN05c]. Watch [MA00a, Sav05a, Sav05b, JOY03a]. Watercolor [HH04, HH05, ST01d]. Watermark [AS01b, GMV01, JX05, KHY04, KWO03a, MEH01, PBB02, RE02, SY01a, CAC03, TH01, WY02, ZAN01, AA08, CL08, LYGL07, LLC06a].

Watermark-based [KWU03a].

Watermark-Fingerprint [KHY04].

Watermarked [ST01c]. Watermarking [AS08, AK02b, AKH03b, AS01c, ARU01, ARC+01, BBC+09, BR09, BSC01a, BSC01b, BSL02, BQR01, BSN00, CC02a, CH01b, CDT05, CT09, CM02, CM03, CM08, DW01, DNP07, EFC+05, EI01, GW01, HT06, HH09, JKK+01, KCR04, HKL00, KLL01, KUN01, KT00, LZ09, LL05a, LKL05, LZO1, LZX+04, IWS05, LPZ06, LJ05b, LSC03, LL01, LSKC05, MM01a, MNS01, NAK01, OTM02, PJH01, PJK01, PR01, PBM+07, QU01, SAMS09, SS001, SDFH00, SDF01, SSFC09, SC02a, SY01b, SHI08, SP04, SLT01, SPK08, VV01, VHP01, VK07, WCJ09, WH09, WY09, WWL+02, WTL05b, XFZ01, YWWS09, ZTP05, ZWC02, AKH03a, APP07, BCKK05, CC02b, CHE08b, CYH+07, CCD+04, CS05a, CC04c, CMB02, CLK05, DSP01, FWL08, FMS05, GA03, HLC07, HHC05, JJO01, JA02, KA09, KPO01, LDD07, LIN00a, LIN01b, LLC06a, LLC06b, MB08, MCH05].

watermarking [PK03, REN09, MSFTL05, WJP07, WNO08, WAT02b, WAT09, WC05, WMD08].

XIMST07, YZW07, YPSZ01, ZLZ07].
Watermarks
[Ben00, BB00a, MLC01, Sug01, WC03a, WC04, YLLL02, MB08, TND+09].
Watershed [FBW01].
Watershed-from-Markers [FBW01].
WAV [XFZ01]. WAV-Table [XFZ01].
Wavelet [BR09, GW01, LKLK05, LZ01, Nak01, AAP07, AA08].
wavelet-based [AAP07, AA08].
Wavelet-Domain [LZ01]. WAVES [LBA00].
Way [BYJK08, BM01a, CHL02, DIS02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sho00a, ZY00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KKK, LW04, LPM05, LQ08, LKJL01, Mic02a, Poi00, Tsa08, WW05, YW05, YRY05b, ZW05a].
Wayness [KI01a, PV06b]. Ways [BB02].
WCC [Ytr06]. WDDL [MMMT09].
Weak [HG03, LS01c, RW03b, DW09, GO08, KO00, KW00]. Weakening [ZD05].
Weakly [BS00a, CHS05]. Weakness [SW05a, SZS05, YPKL08]. Weaknesses [FMS01, He02, KCL03, KCC05, SGGB00].
Weapons [RR03b]. Weather [WWL+02].
Web [Che01d, Mar05a, BFG05, BFG08, Hil06, Ano01c, Ano02e, Ano03c, AEV+07, BFG04, BC04b, CCCY01, Coc01a, Coc02a, Coc02b, CZB+01, Del07, DMSW09, FSSF01, GSO2a, GSVCC02, HM05, JRB+06, KCD07, LKW00, LLS05b, LXM+05, MMPM09, PM00, RR04, Sam09, SSS06, Sch01a, SBG07, TMMM05, WA06, YSS+01].
Web-Based [Ano01c, Sch01a, YSS+01].
Web-enabled [CCCY01]. webcam [McN03].
WebFountain [Ano03c].
Webrelay [Zha00]. Weight [CH07c, GK02, WT02]. Weighted [BTW05, BTW08, SC02c, YZ00]. Weil [BF01b, BF03, Jou02, Kir03]. Well [WWGP00].
Welschenbach [Ter08]. Welsh [Rot07].
wed [AJ08]. WEP [SIR04]. were [Hau06]. Wesley [Puc03]. West
[Fra01, Jue04, Syv02, Wri03]. Westbridge
[Ano02e]. Western [CZB+01]. Wet [CC09].
Weyl [Sug03]. WG [DFPS06]. WG11.1
[ELvS01]. WG11.1/WG11.2 [ELvS01]. WG11.2 [ELvS01]. WG8.8 [DFCW00].
Wheeler [ABM08, Bar05]. Where
[Bur06, Fen01a]. While [Tee06]. WHIM
[JA02]. WHIRLPOOL [RB01]. Whisper
[NAB03]. Whitening [On01]. Whitfield
[Jan08a]. Who [CZB+01, Urb01, Hau06].
whole [CPG+04]. Wi
[Puz04, Sty04, VG04, FMA02, Bar03].
Wi-Fi [Syo04, Bar03]. Wi-Foo
[Puz04, VG04]. wicked [Lud05]. Wide
[DR02a, SBB05]. Width [OT03b]. Width-
[OT03b]. Wiener [Duj08, Duj09]. WIESS
[USE00b]. Wiley [And04, Gra01, Kir01a].
Will [Or00, Cla00b, Fur05]. William
[Che05b, Pag03]. Williams [Mü01a].
Window [OT03a, SSST06]. Windows
[USE00a, DGP07a, DGP07b, DGP09, Fer06, HB06, WD01a, Wit01]. Wins [Bar00b].
Wired [Gil07, Pot07, SIR04]. Wireless
[AEQ05, Bar03, BCH+00, ECM00b, Fin06, KH05, KHD01, LNL+08, Pan03, PZD09, Pot03, Puz04, Sin01a, Sty04, SYL05, VG04, YSR01, ZYN08, ZWCY02, Bad07, BP03a, BBG+02, CCCT09, Cha05b, GW08, GG05b, HLT09, JRR09, KXTZ09, KB09, LD06, LPV+09, LFHT07, LW05a, Lin07, Lop06, MJF+08, Moo01, NC09, NLD08, PCS07, Par04, Pat02a, Pat02b, Pot07, SPL07, SZ08, TP07, Vac06, Van03, Van04a, YTW05, CS08b, ECM00a, PDMS09].
Wiretapping
[Cho08a, DL98, Jan08a, DL07]. WISA
[CSY09]. Within
[MR02a, CHM+02, MR02b]. Without
[BCL+05b, Bla01c, BB04, BGM07, Har06, NA07, Ano03b, CH01a, CCK04b, CYH04, CCH05, CTH08, CJ03c, CJ04, CDD07, CN06, DK01, KG09, Kuo4, LV07, LHL04b, LW04, LKY05b, LL06, Lin01a, LCZ05b, Lys07, MP02, Mar07, PS04c, RG09, Tsa08,
Withstanding [DFS04]. Wits [Bud00a, Bud02]. WLAN [SSM+08].
WLAN/cellular [SSM+08]. Woes [BTTF02]. Women [FF01b, won] [Hau03].
Worchester [KP01]. Word [HR00, SKU+00]. Word-Oriented [HR00, SKU+00].
Wordlengths [PG05]. words [GS01, Max06, NS01a, VS01]. Work [DFG01, DNW05, Fox00].
Working [DFCW00, ELvS01, KB00]. workload [BGM04]. Works [Net04].
Workshop [ACM05a, Ano05c, AL06, BDZ04, BBD09, BGD04, Ch00, Chr01, CCMR02, CCMR05, CSY09, DR02c, Des02, GH05, IEE01b, IZ00, JQ04, KKP02, KCR04, KGL04, Kim01, KP01, KNP01, LST05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RRS06, RM04, Sch00b, Sch01d, TB02, USE00b, VY01, Van05a, WK03, Yr06, AMW07, AJ01a, BCKK05, Bir07, CKL05, GKS05, HH04, HH05, HA00, ST01d]. World [Ber03, GG05a, HW01, Nik02a, Nik02b, Sch00d, Sty04, YKMB08, Ano03b, Arko05, Bel07a, Che00b, Hei03, HHG06, Hus01, KPS02, Koe05, Lie05, Um09, Rob02, Rob09, Sch03, SL07, Bec02, Bud00a, Bud02, Hau03, Kof01, MH09, OC03, Sty04, See04]. Worlds [Wil01b]. Worm [LJL05, CSW05]. Worms [ZGT05].
Worst [CCM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case [HRS08, Mic02a, Mic02b, Pei09]. worst-case/average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. wrapped [HLC07]. Wrapper [Ols00]. Write [BB02]. Writers [Gor06]. Writing [HL03, Jan06, Kah07a, Kah07b, Kah96, Gas01]. Writings [Cop04b].
WS [JRB+06, RR04]. WS-Policy [RR04]. WS-Security [JRB+06, RR04]. WSDL [Bar00c]. WTLS [Vau02]. WTMAU [ECM00a, ECM00b]. WTMAU-SD [ECM00a]. Wu [BCW05, CHY05a, CWJTO1, HL05c, MS03a, YY05b]. Wu-Lin [YY05b]. Wuhan [TTZ01]. WW [Sal00a].
WWII [WD01b].
X [For04]. X.509 [SJ05]. X.9.31 [Ke05]. X.9.62 [ANS05]. Xbox [Ste05b]. XCBC [GD02]. XECB [GD02]. Xia [CTJ04, Sha05a]. Xiamen [DWML05]. Xiao [JW01, YY05a]. Xilinux [Ano02e]. XIV [USE00c]. xix [Top02]. XL [CP03]. XML [Hei01, TEM+01, AW05, AW8, Ano02e, BN08, CKK03, Dav01b, Dav01c, DGK+04, FJ04, FL01b, GA03, Her02, LC04b, PCK02, RR04, ÜG08, Uri01, UST01a]. XMT [SG07]. XrML [Bar00a]. XTEA [CV05, HHK+04, MHL+02]. XTR [LW02, LV00, LNS02, Ver01].
Yahalom [Pan01]. Yang [McK04, CZ03, KJY05, WL05, YWC05].
Yang-Shieh [YWC05]. Yao [BPS08, BDNN02, ZD05]. Yao-style [BPS08]. Yarrow [YCF00, Mur02].
Yarrow-160 [KSF00]. Yaschenko [Kat05b].
YCH [SC05a]. YCN [Hwa00]. Year [Naz02, Bur00]. Years [Ahn08, CM02, Ros04]. Yellow [JYZ04].
Yen [LLLZ06]. Yen-Guo [LLLZ06]. Yesterday [Coc02a]. Yi [Wag00]. Yi-Lam [Wag00]. Yokohama [Mat02].
You [KCC05, KHKL05]. Youn [KCC05]. York [HR06, IKY05, NIS00, Sch01d, YDKM06].
Young [FF01b]. You’re [ES00a, Nic01]. You’ve [Nic01]. Yuck [Sas07]. Yuen [KH08].
Z [Wue09]. Z-parameter [Wue09]. z10 [Web08]. z9 [ADH+07]. Zealand [Zhe02b].
Zeilinger [Duw03]. Zero [AS01b, APV05].
Zimmerling [Duw03]. Zero [AS01b, APV05]. BP04, Cont1, DPV04, DFS04, DDO+01, HNO+09, IKOS07, LMS05, LHL+08, MR01b, MV03a, Pus05, Ros06a, Ros06a, CSM05, Dam00, PBD07, KK07]. zero-day [CSW05].
Zero-Knowledge [AS01b, BP04, Cont01,
REFERENCES

DFS04, HNO+09, LHL+08, MR01b, MV03a, Pas05, Ros00a, Ros06a, IKOS07, Dam00, PBD07. Zeta [Ver02]. Zhang [JW01, YY05a]. Zhou [PKH05]. Zimmermann [McL06, Tuc66]. ZK [PBD05]. Zodiac [HSM+02]. Zone [Kum07].

References

XXX:2002:CC


Al-Akaidi:2004:FSP


Aly:2004:CSP


Agreste:2008:NAP


Apers:2001:PTS


Al-Azzoni:2005:MVC

Issam Al-Azzoni, Douglas G. Down, and Ridha Khedri. Modeling and verification of cryptographic

**[Anshel:2001:NKA]**


**[AAG+00]**


**[Ababneh:2009:CSE]**


**[Ashraf:2009:SBE]**


**[Aamodt:2003:CSP]**


**[Agreste:2007:IAW]**

REFERENCES


Atallah:2009:ATC


Abdalla:2005:SER

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


Abe:2001:SEP


Abe:2004:CEP


Abadi:2005:CFI

Martín Abadi, Mihai Budiu, Úlfar Erlingsson, and Jay Ligatti. Control-flow integrity. In Meadows and Syverson [MS05b], pages...


REFERENCES


<table>
<thead>
<tr>
<th>Reference ID</th>
<th>Description</th>
</tr>
</thead>
</table>
REFERENCES


REFERENCES

Anyanwu:2009:DCS


Avanzi:2006:ESM


Adeec:2009:CDT


Arnold:2007:CSE


Adikari:2009:HBT


Adleman:2003:TLP


An:2002:SJS

Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On

**Arazi:2005:RPK**


**Alvarez:2005:SSS**


**Atighehchi:2009:EPA**


**Anton:2007:HEW**


**Augot:2003:PKE**


Acquisti:2009:PSS


Alon:2007:GSE


Anagnostopoulos:2001:PAD


Ateniese:2005:PRS

Giuseppe Ateniese and Susan Hohenberger. Proxy re-signatures: new definitions, algorithms, and applications. In Meadows and Syverson [MS05b], pages
Agrawal:2003:SWR


Agrawal:2003:WRD


Armington:2002:BAI


Ahmad:2007:CSS


Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF

REFERENCES

Aoki:2001:CBB


Applebaum:2006:C


Al-Ibrahim:2001:AMS


Attali:2001:JSC

Isabelle Attali and Thomas Jensen, editors. Java on smart cards: programming and security: first international workshop,
REFERENCES


REFERENCES


[Aks02] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. Report,


REFERENCES

Atzeni:2006:PKI


Anshel:2007:RME


Allen:2003:EST


Allman:2006:MAW


Alvarez:2000:SMC


Amadio:2002:SRP


Abimbola:2006:NSI

A. A. Abimbola, J. M. Munoz, and W. J. Buchanan. NetHost-Sensor: Investigating the capture of end-to-end encrypted intrusive data. *Computers*
REFERENCES

Alvarez:2000:CCE

Alvarez:2004:KCC

See [kWpLwW01, WLW04].

Andem:2003:CTE

Adams:2007:SAC

Aljifri:2003:ILA

Anderson:2004:BRR
REFERENCES


Anderson:2007:SSS

Anderson:2008:MMM

Anderson:2008:SEG

Aura:2001:RAC
Tuomas Aura, Pekka Nikander, and Jussipekka Leivo.


Anonymous:2000:AIH

Anonymous:2000:AIah

Anonymous:2000:CRR
Anonymous. China relaxes rules on encryption prod-
REFERENCES

106


**Anonymous:2000:CCI**


**Anonymous:2000:CLI**


**Anonymous:2000:EES**


**Anonymous:2000:GBE**


**Anonymous:2000:GPE**


**Anonymous:2000:PTD**


**Anonymous:2000:SES**

Anonymous:2000:UAS


Anonymous:2000:VAS


Anonymous:2001:AAPb


Anonymous:2001:AWB


Anonymous:2001:RA

Anonymous:2001:EDS

Anonymous:2001:EER

Anonymous:2001:EMB

Anonymous:2001:PKC


Anonymous:2002:PSS


Anonymous:2002:PFQ


Anonymous:2002:QCQ


Anonymous:2002:QCR


Anonymous:2002:RUB

Anonymous:2003:TMC


Anonymous:2003:NAW


Anonymous:2003:NUP


Anonymous:2003:SEY


Anonymous:2003:TMP


Mersenne primes are primes of the form $M(n) = 2^p - 1$. The known members of this set in order of increasing $p$ (not of discovery), year of discovery, and discoverer, are:
<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1461</td>
<td>Anonymous</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1833</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1866</td>
<td>E. Fauquembergue</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>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>13</td>
<td>127</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>2203</td>
<td>1957</td>
<td>L. Euler</td>
</tr>
<tr>
<td>15</td>
<td>4423</td>
<td>1961</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>16</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>17</td>
<td>110503</td>
<td>1988</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>18</td>
<td>132049</td>
<td>1996</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>19</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>20</td>
<td>21701</td>
<td>1978</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>21</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>22</td>
<td>3217</td>
<td>1957</td>
<td>H. Riesel</td>
</tr>
<tr>
<td>23</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>24</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>25</td>
<td>9689</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>26</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>27</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>28</td>
<td>216091</td>
<td>1985</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>29</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>30</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson</td>
</tr>
<tr>
<td>31</td>
<td>45856</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>48623</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>33</td>
<td>61001</td>
<td>1996</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>34</td>
<td>75683</td>
<td>1992</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>35</td>
<td>85943</td>
<td>1994</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>36</td>
<td>1257787</td>
<td>1996</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>37</td>
<td>1398269</td>
<td>1996</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>38</td>
<td>2976221</td>
<td>1997</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>39</td>
<td>3021377</td>
<td>1998</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>40</td>
<td>364271</td>
<td>1999</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>41</td>
<td>42643801</td>
<td>2009</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>42</td>
<td>43112609</td>
<td>2008</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>43</td>
<td>57885161</td>
<td>2013</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>44</td>
<td>6120731</td>
<td>2014</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>45</td>
<td>71563217</td>
<td>2016</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>46</td>
<td>74207281</td>
<td>2016</td>
<td>D. Tuckerman</td>
</tr>
<tr>
<td>47</td>
<td>82589933</td>
<td>2018</td>
<td>D. Tuckerman</td>
</tr>
</tbody>
</table>


**Anonymous:2004:Cf**


**Anonymous:2004:NGJ**


**Anonymous:2005:CEC**


**Anonymous:2005:SCB**


**Anonymous:2005:WAS**


**Anonymous:2006:JHD**


**Anonymous:2006:RC**


**Anonymous:2006:SSD**

REFERENCES


REFERENCES

**Anonymous:2009:BG**


**Anonymous:2009:DSS**


**Anonymous:2009:TCA**


**Anonymous:2012:SHS**


**Anonymous:2013:DSS**


**Ateniese:2001:SRC**

Amir:2001:FAA


ANSI:2005:AXP


Abe:2000:PSP


Abe:2002:SVK


Alomair:2009:ITS

REFERENCES


Shunsuke Araki. A Nyberg–Rueppel signature for mul-


Rashmi Agarwal and M. S. Santhanam. Digital watermarking in the singular

**Asenjo:2002:AES**


**Ashburn:2003:PBA**


**Aslan:2004:HSM**


**Aslan:2004:LAA**


**Aciicmez:2007:MAC**


**Aciicmez:2005:IBB**

REFERENCES


Abdalla:2000:KMR


Allison:2001:LLE


Ateniese:2004:VED


Androutsellis-Theotokis:2004:SPP


Aharonov:2000:QBE

REFERENCES


REFERENCES


[BA06] Marina Blanton and Mikhail Atallah. Succinct representation of flexible and privacy-preserving access
REFERENCES


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/.

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

Barr:2002:IC

Barken:2003:HSY

Barron:2005:DWP
REFERENCES

oxfordjournals.org/cgi/reprint/48/6/650.


REFERENCES


[BB00a] Oliver Benedens and Christoph Busch. Towards blind detection of robust water-

**Buchmann:2000:ECC**


**Barkan:2002:HMW**


**Bouda:2003:EQI**


**Boneh:2004:SIB**


**Bicakci:2005:ISA**

Biham:2002:SQK


Basso:2009:NBB


Beimel:2002:UIS

Bellare:2001:KPP


Blumenthal:2002:SAD


Bartolini:2008:EIS


Barkan:2003:ICO


Bertoni:2003:EAD

REFERENCES


Bellare:2001:OCH


Bellare:2000:PKE


Bobineau:2000:PSD


Boneh:2004:SGS

REFERENCES


REFERENCES


REFERENCES


Blundo:2006:VCS

Bruguera:2009:PIS

Barnum:2002:AQM

Burnett:2000:EMG
REFERENCES

[BCJ+06] 135


REFERENCES


Bresson:2007:PSA


Bellavista:2002:JLD


Bao:2005:R


Biham:2000:CAG

REFERENCES


REFERENCES


[BDFP02] Chiara Bodei, Pierpaolo Degano, Riccardo Focardi, and Corrado Priami. Primitives for authentication in
REFERENCES


REFERENCES


Biryukov:2004:MLA


Baldwin:2009:PSS


Buchmann:2009:HBD


Bertolotti:2008:ERA


Boneh:2001:MFR


Bao:2004:PKC

Feng Bao, Robert Deng, and Jianying Zhou, editors. Public Key Cryptography—PKC 2004: 7th International Workshop on Practice and Theory in Public Key Cryptography, Singapore, March 1–4, 2004:
REFERENCES


Beckman:2002:CAB


Bejtlich:2006:EDS


Bellare:2000:ACC


Bella:2001:MPS

REFERENCES


REFERENCES


Benson:2001:VS

Benantar:2002:IPK

Benson:2004:VS

Berson:2000:CE

Berson:2003:CAB

Bernstein:2007:SFS
Daniel J. Bernstein. The Salsa20 family of stream ciphers. Report, Department of Mathemat-


REFERENCES


REFERENCES


REFERENCES

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


REFERENCES


[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evalu-
References

Evaluating 2-DNF formulas on ciphertexts. In Kilian [Kil05], pages 325–??
CODEN LNCSD9.


REFERENCES


REFERENCES

0001-0782 (print), 1557-7317 (electronic).


Biham:2000:CPR


Biham:2002:HDE


Biham:2003:ACE


Beimel:2000:RSC


Bajard:2003:EMG

REFERENCES


REFERENCES


[BK00] William Boni and Ger-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[BLST01] William D. Banks, Daniel Lieman, Igor E. Shpar- 
linski, and Van Thuong To. Cryptographic appli- 
cations of sparse polynomi- 
als over finite rings. Lecture 
Notes in Computer Science, [BM01b] 2015:206–??, 2001. CO- 
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http:
//link.springer-ny.com/ 
link/service/series/0558/
bibs/2015/20150206.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2015/20150206.
pdf.

[Blu09] Bill Blunden. The rootkit 
arsenal: escape and eva-
sion in the dark corners of 
the system. Wordware Pub-
lishing, Plano, TX, USA, 
2009. ISBN 1-59822-061-
6 (paperback). xxvii + 
908 pp. LCCN QA76.9.A25
B585 2009.

[BM01a] Lejla Batina and Geke 
Muurling. Another way 
of doing RSA crypto-
graphy in hardware. Lecture 
Notes in Computer Science, 
2260:364–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http:
//link.springer-ny.com/ 
link/service/series/0558/
bibs/2260/22600063.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2260/22600063.
pdf.
REFERENCES

[Basu:2003:AC]

[Blomer:2003:NPK]

[Boyd:2003:PAK]

[Burke:2000:ASFa]

[Burke:2000:ASFb]

[Burke:2000:ASFc]
Jerome Burke, John McDonald, and Todd Austin. Architectural support for fast symmetric-key cryptography. ACM SIGPLAN Notices, 35(11):178-189,
REFERENCES

November 2000. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).


Buchmann:2006:PCL


Borselius:2002:VTS


Borselius:2002:PAU

Niklas Borselius, Chris J. Mitchell, and Aaron Wilson. A pragmatic alternative to undetectable sig-

Boyen:2005:DCC


Bellare:2000:AER


Boneh:2000:TC

Dan Boneh and Moni Naor. Timed commitments.
REFERENCES


REFERENCES

Ben-Or:2005:UCS


Bollinger:2002:UFO


Bondi:2000:CVB


Boneh:2001:SOR


Boneh:2003:ACC

REFERENCES


REFERENCES


Barbancho:2003:CA


Buchbinder:2003:LUB


Bellare:2004:KEA


Blanchet:2005:VCP


Beissinger:2006:CUM

REFERENCES


REFERENCES


REFERENCES


[BR00b] Black:2000:CMA

[BR01] Black:2001:CAF

[BR02] Black:2002:BCM

[BR04] Black:2004:CBG

[BR04] Bellare:2004:CBG

[BR05] Bugliesi:2005:NIP


REFERENCES

(print), 1875-8924 (electronic).

Bellare:2006:MPP


Bhatnagar:2009:RRW


Brackenridge:2006:IUU


Brown:2005:CEC


Brown:2005:DEP

ISBN 0-9549513-0-1. ???.

**Black:2002:BBA**


**Bierbrauer:2000:AIW**


**Butler:2009:LIB**


**Biryukov:2000:CTM**


**Bru06**

José Carlos Brustoloni. Laboratory experiments for network security instruction.

**Brustoloni:2006:LEN**

REFERENCES


REFERENCES


REFERENCES

[BSSM+07] Abhilasha Bhargav-Spanetz, Anna C. Squicciarini, Shimon Modi, Matthew Young, Elisa Bertino, and Ste-


 REFERENCES


[Buh06] Ileana Buhan. Feeling is believing: a location limited channel based on grip pattern biometrics and cryptanalysis. CTIT technical report 06-29, Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands, 2006. 10 pp.


REFERENCES

Boesgaard:2004:RNH


Baker:2007:ISU


Blake-Wilson:2002:RUE


Butler:2000: NSA


Bellare:2003:FSP


Bar-Yossef:2004:ESQ

Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communic-
REFERENCES


Bar-Yossef:2008:ESQ


Bertlmann:2002:QUB


Bond:2003:DTA


Borders:2005:CHP


Carrington:2002:EDS


Staff:2003:NTC

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

Staff:2006:NTS

CACM Staff. News track: Super game plan; E-learning
roots disputed; Chinese history; U.K. seeks popular science input; encryption commitment; *Improve*ment news; vid kid. *Communications of the Association for Computing Machinery*, 49 (11):9–10, November 2006. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

**CALACIT:2000:SID**


**CADOJ:2000:DSE**


**CAMTC:2000:TSC**


**Caloyannides:2000:EWE**


**Caloyannides:2000:EWS**


**Calvocoressi:2001:TSU**


**Canetti:2001:UCS**


**Canteaut:2001:CFD**

A. Canteaut. Cryptographic functions and design criteria for block ciphers. *Lec-
REFERENCES


[Cas02] Eoghan Casey, editor. Handbook of computer crime in-


REFERENCES

---

Chandramouli:2006:BPA


---

Cachin:2000:OFS


---

Chan:2001:CRP


---

Chan:2001:CTB


---

Carline:2002:NWT


---

Chan:2002:SLI


---

Cachin:2004:ACE

Christian Cachin and Jan Camenisch, editors. Ad-
REFERENCES


REFERENCES


REFERENCES


Chai:2007:EIB

Cattaneo:2001:DIT

Chen:2004:TPM

Chang:2005:DSM

Chang:2004:IDA

Chang:2004:SOT
REFERENCES

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

Chang:2009:PCC

Christianson:2001:PKC

Choi:2005:JMA

Christianson:2002:SPI

Christianson: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


Carpenter:2000:CB


Cramer:2001:SDL


Ceselli:2005:MAI

REFERENCES


REFERENCES

**Cavallar:2000:FBR**


**Cortier:2006:SAP**


**Chawla:2005:TTP**


**Cramer:2000:GSM**


**Coron:2005:MDR**

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle–Damgård revisited: How to construct a hash function. In Shoup [Sho05a],


P. Ceravolo. Extracting role hierarchies from authentication data flows. International Journal of Computer
REFERENCES


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


REFERENCES


**Chodowiec:2003:VCF**


**Cranor:2005:SUD**


**Candebat:2006:SPM**


**Chodowiec:2001:ETG**


**Caballero-Gil:2009:GBA**

P. Caballero-Gil, A. Fúster-

Catalano:2000:CIS


Coppersmith:2000:ICT


Catalano:2001:BSP


Caballero-Gil:2006:SSB

P. Caballero-Gil and C. Hernández-Goya. Secret sharing based

**Crosby:2002:CHB**


**Chen:2008:OVBa**


**Chen:2008:OVBb**

<table>
<thead>
<tr>
<th>REFERENCES</th>
<th></th>
</tr>
</thead>
</table>
REFERENCES


[CH07a] Hung-Yu Chien and Chen-

Chung:2007:ASF


Chung:2007:MRA


Chaum:2004:VSB


Chan:2005:MCM


Chandra:2005:BWS


Chakrabarti:2007:GCS

Chen:2000:JCT


Cherry:2000:SLD


Chen:2001:DEU


Chen:2001:PDP

REFERENCES

Cheon:2001:NVR


Cherry:2001:REM


Chen:2002:SFS


Cheng:2003:PPO

REFERENCES

Chen:2004:IAM


Cheng:2004:BSD


Chen:2005:TSS


Chen:2007:CIS


Cherry:2005:MEV


Chen:2008:CIS


Chen:2008:MWS


Coulter:2001:GAH


Chien:2008:EP


Chien:2008:PA


Chien:2008:PAu

REFERENCES


Chien:2008:PAUc


Chien:2008:SCA


Coron:2001:OCC


Coron:2001:GGC


Coppersmith:2002:CSC

Don Coppersmith, Shai Halevi, and Charanjit Jutla. Cryptanalysis of stream ci-

Canetti:2003:FSP


Canetti:2005:ASN


Cheon:2008:PST


Chang:2002:IBO


Chao:2009:HCS

REFERENCES


REFERENCES

Christianson:2001:SPI


Canetti:2005:HAW


Chen:2002:AMT


Cornea:2002:SCI


Churchhouse:2002:CCJ

REFERENCES

215


REFERENCES

Cheon:2003:PTA


Cheien:2003:RSA


Chien:2003:HAP


Chien:2003:NHA


Chien:2004:IAM


Chen:2005:EDS

REFERENCES


Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier. New attacks on PKCS#1 v1.5 encryption. *Lecture Notes in Computer Science*, 1807:
Coron:2002:UPS


Chepyzhov:2001:SAF


Chien:2001:MRL


Chien:2002:EPS


Chung:2003:EPX


Chun:2003:DLC


Cox:2005:DWT


Chen:2009:SRP


Coppersmith:2000:KRF

REFERENCES

Coron:2000:FLA


Coron:2001:SSL


Canetti:2003:RCC


Cheon:2006:KPC


Cachin:2001:SEA

Christian Cachin, Klaus Kursawe, Frank Petzold,

Cathalo:2003:NTT


Chevalier:2008:CRS


Cachin:2009:TC


Chen:2005:CLR


Chen:2007:CRA

REFERENCES


REFERENCES


REFERENCES

issn=0302-9743&volume=
3621.

Chandramouli:2007:ISS

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

96, March/April 2007. CODEN ???. ISSN 1540-7993
(print), 1558-4046 (electronic).

Chang:2008:AWM

[CL08] Chin-Chen Chang and Pei-
Yu Lin. Adaptive watermark mechanism for right-
ful ownership protection. *The Journal of Systems and
Software*, 81(7):1118–1129, July 2008. CODEN JS-
SODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Chien:2009:EBL

[CL09] Hung-Yu Chien and Chi-
Sung Laih. ECC-based lightweight authentication
protocol with untraceability for low-cost RFID. *Journal
of Parallel and Distributed Computing*, 69(10):848–853,
October 2009. CODEN JPDCER. ISSN 0743-7315
(print), 1096-0848 (electronic).

Clark:2000:TNE

[Cla00a] David Clark. Technology
news: Encryption advances to meet Internet challenges.

Chen:2008:RCE

[CLC08] Tzung-Her Chen, Wei-Bin
Lee, and Hsing-Bai Chen. A round-
and computation-
efficient three-party authen-
ticated key exchange proto-
col. *The Journal of Sys-
tems and Software*, 81(9):
CODEN JSSODM. ISSN
0164-1212 (print), 1873-
1228 (electronic).

Chang:2001:ASM

Kyung-Ah Chang, Byung-
Rae Lee, and Tai-Yun
Kim. Authentication service model supporting mul-
tiple domains in distributed computing. *Lecture Notes in Computer Science*, 2073:
413–??, 2001. CODEN LNCSD9. ISSN 0302-
REFERENCES


Chang:2001:FAM


Cheon:2000:NBC


Canetti:2002:UCT


Cormen:2001:IA


Chen:2009:AKD

Bee-Chung Chen, Kristen Leefvre, and Raghu Ramakrishnan. Adversarial-knowledge dimensions in data privacy. VLDB Journal: Very Large Data Bases, 18(2):429-467, April 2009. CODEN VLDBFR. ISSN
REFERENCES

Chang:2007:SIH


Clulow:2003:SP


Czumaj:2002:PTA


Camenisch:2000:CSS


Cox:2002:FYE

REFERENCES

Courtois:2003:AAS

Chevallier-Mames:2005:ECB

Cojocaru:2005:ISM

Cox:2002:DW

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

Cox:2008:DWS
I. J. (Ingemar J.) Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker. *Digital Watermarking and Steganography*. The Morgan

Cremers:2006:ISE


Campo:2001:JFC


Chevallier-Mames:2003:FDS


Chao:2000:CHC

Cid:2006:AAA

Cho:2008:DNP

Caputo:2009:DIT

Cra 2002:FEE

Coron:2004:SSL

Ciet:2003:PF1
Catalano:2002:HHL


Correia:2006:CAB


Cetin:2009:NSA


Czernik:2009:CRN


Cobb:2004:CD

REFERENCES


Cohen:2003:FOV


Cole:2003:HPS


Constantinou:2000:CSC


Convery:2004:NSA


Conti:2009:GSH


Cook:2002:REJ


Coppersmith:2000:C

D. Coppersmith. Cryptography. IBM Journal
REFERENCES

of Research and Development, 44(1/2):246–250, January/March 2000. CO-
DEN IBMJAE. ISSN 0018-

DEN IAHCEX. ISSN 1058-
org/dl/mags/an/2004/04/
a4038.pdf.


Francisco Corella. A fast implementation of DES and Triple-DES on PAR-
REFERENCES


**Cimato:2006:PVC**


**Chow:2004:UDL**


**Chen:2004:SEP**


**Catalano:2004:IIP**


[237]
REFERENCES

Canetti:2007:CSH
[102x625]


Ciet:2001:SFC
[102x453]


Canetti:2003:UCJ
[102x192]


Crampton:2005:UDR
[102x192]


Cramer:2005:ACE

Jason Crampton. Under-

Crenshaw:2000:SPK


Cro:2001:MFL


Chhabra:2009:MSP


CRI:2000:DPA


Cramer:2000:SSB


Cramer:2002:UHP


Cramer:2000:SSB


REFERENCES


[CS07c] Katharine Chang and Kang G. Shin. Distributed Authentication of Program Integrity

**Cusick:2009:CBF**


**Czeskis:2008:DED**


**Cai:2007:CSM**


**Crandall:2005:DUV**


**Chen:2008:CCS**


**Chung:2009:ISA**

Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors. *Information Security Applications: 9th International Workshop,*
REFERENCES


Collberg:2002:WTP


Coron:2003:NAS


Chen:2008:BUK


Chu:2008:EOT


Chou:2009:ATI

Chang-Min Chou and Din-Chang Tseng. Affine-transformation-invariant public fragile watermarking for

**Crawford:2001:FPV**


**Chiang:2008:CPB**


**Chang:2004:ASS**


**Cheung:2001:TPS**


**Collberg:2007:DGB**


REFERENCES


Fu-Chi Chang and Chia-Jiu Wang. Architectural tradeoff in implementing RSA processors. ACM
REFERENCES


[CYH01]


REFERENCES

Chang:2005:SAK


Chung:2007:SBW


Chang:2005:CIA


Chen:2003:AEY


Chadwick:2005:PKI


[Dal01]

Cheng:2005:RIC


[CZK05]

Dale:2001:BSA


[DA03]


[Dam00]

Damaj:2007:P


dB07


Desmedt:2001:ERD


Doyle:2006:SCK


diVimercati:2005:CSE

Annalisa De Bonis and Alfredo De Santis. Randomness in visual cryptog-
REFERENCES

Dalkilic:2002:CPF

DeBonis:2004:RSS

Diene:2006:DLE
Adama Diene, Jintai Ding, Jason E. Gower, Timo
ty J. Hodges, and Zhijun Yin. Dimension of the linearization equations of the Matsumoto–Imai cryptosystems. In Ytre

Dolev:2000:NC

Dolev:2003:NC

DeSantis:2001:RNI
Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. Robust

DeLooze:2007:PWS

DeLooze:2007:PWS
[DeL07]

Desai:2000:ESS

Desai:2000:ESS
[Des00a]

Desai:2000:NPC

Desai:2000:NPC
[Des00b]

Desmedt:2002:PKC
REFERENCES


Antonio Durante, Riccardo Focardi, and Roberto Gorrieri. A compiler for analyzing cryptographic protocols using noninterference. *ACM Transactions on
REFERENCES


Durante:2001:CWR


DePalma:2004:CCS


Domingo-Ferrer:2001:CDS


Dodis:2003:IRP


DeSantis:2004:CKA

[DFM04] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Ma-
REFERENCES


[DFS04]

Domingo-Ferrer:2006:SCR


[DFPS06]

Domingo-Ferrer:2007:ASC


[DFSS08]

Damgaard:2004:ZKP


[DFSS05]

Damgaard:2005:CBQ


[DFPST07]

Damgaard:2008:CBQ

Dalkilic:2000:ICA


Debaert:2002:RRI


DiRaimondo:2003:PST


DiRaimondo:2005:NAD


DiRaimondo:2006:PST


Dodis:2004:REK

Yevgeniy Dodis, Rosario Gennaro, Johan Håstad,

REFERENCES

2008. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Devanbu:2003:ADP


Devanbu:2003:FAX


Dorrendorf:2007:CRNb


Dorrendorf:2007:CRNa

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


REFERENCES


Dierickx:2000:EGD

Diffie:2001:UC

Dimitriadis:2007:IMC

Dimitrov:2008:DBN

Ding:2001:OTB
Ding:2005:ECB


Dedic:2005:ULB


Dang:2002:EPT


Dang:2002:EPT


Delaune:2006:DPS

Stéphanie Delaune and Florent Jacquemard. Decision procedures for the security of protocols with probabilistic encryption against offline dictionary attacks. Jour-
REFERENCES


REFERENCES

Delfs:2007:ICP


Dunkelman:2008:TIV


Du:2005:BRS


Daswani:2007:FSW


Dhem:2000:PIT


Ding:2000:SSC

REFERENCES

Do dis:2009:CAI


Datta:2005:RBN


Delaune:2008:FAP


Dittmann:2005:CMS


Dodis:2002:KIP

REFERENCES


REFERENCES

article&issn=0010-485X&volume=85&issue=1&spage=85

**Dodos:2008:OFE**


**DeSantis:2000:SSS**


**Dodos:2000:PRI**


**DeSantis:2007:NRN**


**Drimer:2007:KYE**


**Dumais:2000:PCQ**

Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any
REFERENCES


Durfee:2000:CRS

REFERENCES


REFERENCES


REFERENCES

Dhamija:2000:DVU

DeMatteis:2002:PP

Dandalis:2004:ACE

Dziembowski:2007:IRS

Dziembowski:2008:LRC

Dandalis:2001:CSP

[Damgaard:2005:QCN]


[Crescenzo:2004:CRR]


[Daemen:2000:NPN]


[Delbourg:2002:JBC]


[Daemen:2000:NPN]


[Delbourg:2002:JBC]

REFERENCES


Joan Daemen and Vincent Rijmen. Rijndael for AES. In NIST [NIS00], pages 343–347. ISBN ???? LCCN ???.


REFERENCES


[DR02c]


[DR02d]


[Dre00]

Suelette Dreyfus. The practical use of cryptography in human rights groups, 2000. URL
REFERENCES


Driscoll:2002:BER


Diqun:2009:QSP


delRey:2005:SSS


Dobbertin:2005:AES


Devanbu:2000:CVT

REFERENCES


REFERENCES


Duggan:2004:TBC


Dujella:2008:VWA


Dujella:2009:VWA


Dunkelman:2006:TCB


Duranti:2001:LTP


Duwell:2003:BRB

Dawson:2005:PCM


Drutarovsky:2008:CSC


Levy-dit-Vehel:2006:WC


Du:2001:OKS


deWeger:2002:CRS


Ding:2005:CTC


Dodis:2009:NME

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

Dwivedi:2004:ISS


DWN01

30849-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25
issn=0302-9743&volume=3810.

Dittmann:2001:UCW


Dworkin:2003:DRB


Ding:2005:NME

Yong Ding, Kwok wo Wong, and Yu min Wang. A w-
REFERENCES


**Dawu:2001:TES**


**[Eag05]**


**ElAbbadi:2000:VPI**


**Eghlidos:2001:IRL**


**Eilam:2005:RSR**


**English:2007:MAC**

Jennifer English, David Coe, Rhonda Gaede, David Hyde, and Jeffrey Kulick. MEMS-assisted cryptography for CPI protection.


**ECMA:2000:EPIa**


**ECMA:2000:EPIb**


**Ellison:2003:PKS**

Carl Ellison and Steve Dohrmann. Public-key sup-

Echizen:2005:PAV


Eghlidos:2000:SLB


Elmallah:2008:LK


Epstein:2003:DIT


Ernst:2004:FBH


Ellison:2000:PSK

Carl Ellison, Chris Hall, Randy Milbert, and Bruce Schneier. Protecting secret

Eggers:2001:DWC


Ekert:2002:BTQ


Ekerea:2009:DCM


El-Kassar:2001:GPK


Elbirt:2009:UAC


Elliott:2004:QC

REFERENCES


<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Year</th>
<th>ISBN</th>
<th>Title</th>
<th>Edition</th>
<th>Publisher</th>
<th>Pages</th>
<th>URL</th>
</tr>
</thead>
</table>
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Flannery:2001:CYW

Fridrich:2001:DLS

Frenkiel:2002:CCS

Focardi:2000:ITN

Focardi:2000:MAT
REFERENCES


[Focardi:2003:CTA]

[Fitzi:2001:MCP]

[Filiol:2000:DAS]

[Filiol:2002:NST]

[Finley:2002:BSE]
REFERENCES

Finkenzeller:2003:RFH

Finnigin:2006:CPN

FIPS:2000:DSS

FIPS:2001:AES

FIPS:2001:SR

FIPS:2000:BRS
REFERENCES


FIPS:2002:KHM


FIPS:2002:SHS


Freedman:2005:KSO


Fischlin:2001:CLP


Fischlin:2001:ICN

Marc Fischlin. On the impossibility of constructing non-interactive statistically-secret protocols from any trapdoor one-way function. Lecture Notes in Computer Science, 2271:79–??, 2001. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349
REFERENCES


REFERENCES


Ferguson:2000:ICR


Fox:2001:PPK


Ferguson:2000:TRR

N. Ferguson, J. Kelsey, B. Schneier, and D. Wagner. A TwoFish retreat: Related-key attacks against reduced-round TwoFish. TwoFish technical report 6, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, February 14, 2000. ???.

Fluhrer:2001:AES


REFERENCES


REFERENCES


Fluhrer:2001:WKS


Furht:2005:MEW


Frankel:2001:ASA

REFERENCES


REFERENCES


REFERENCES

Fernandes:2002:SAL

Fournet:2008:CSI

Frankel:2001:FCI

Franklin:2004:ACC

Frembberg:2003:MAP
REFERENCES


Friberg:2001:UCH


Frith:2007:SAO


Frykholm:2000:CAB


Ferguson:2000:CEI


Fouque:2001:FDT


Friedlander:2001:DDH

REFERENCES

epubs.siam.org/sam-bin/dbq/article/36174.


Furukawa:2001:ESP


Fischer:2002:NFC


Fundulaki:2004:SYD


Ferguson:2003:PC


Ferguson:2003:CEI

[Ferguson:2003:CEI] Niels Ferguson and Bruce Schneier. A cryptographic evaluation of IPsec. Un-


Furnell:2005:AOW

Fouque:2003:DAW

Fan:2008:RSB

Feng:2005:NMS
0164-1212 (print), 1873-1228 (electronic).

**Fitzi:2004:PSB**

**Fan:2004:PPI**

**Furnell:2006:RPS**

**Fu:2005:DHP**

**Gross-Amblard:2003:QPW**

**Gang:2005:CNI**

**Galbraith:2001:SCC**
Steven D. Galbraith. Supersingular curves in cryp-


Garman:2003:KDG


Garrett:2004:MCT


Gasarch:2001:BRBa


Gaudry:2002:CCS


Gavinsky:2008:CIC

REFERENCES

Guinee:2009:NTR


Guajardo:2001:EIE


Golic:2002:LCB


Goubin:2000:CTC

Gaj:2001:FIF


Goodman:2001:EER


Guerrero:2005:ECB


Gordon:2008:CFS


Gligor:2002:FEA

Gennaro:2005:SMS

Gebotys:2004:DSC

Geier:2003:LCC

Gengler:2000:UPC

Gentry:2003:CBE

Gennaro:2004:MTC
Rosario Gennaro. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-
the-middle attacks. In Franklin [Fra04], pages 220–??. CODEN LNCSD9.
ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN
volume&id=doi:10.1007/b99099.

Gentry:2004:HCR
Craig Gentry. How to compress Rabin ciphertexts and signatures (and more). In
Franklin [Fra04], pages 179–??. CODEN LNCSD9. ISBN 3-540-22668-0. ISSN
0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL
volume&id=doi:10.1007/b99099.

Gennaro:2006:RC
67, March/April 2006. CODEN ???. ISSN 1540-7993 (print), 1558-4046 (electronic).

Gentry:2009:FHEa
Craig Gentry. A fully homomorphic encryption scheme. Ph.d. thesis, Department
of Computer Science, Stanford University, Stanford, CA, USA, 2009. x + 199
pp. URL http://crypto.stanford.edu/craig/;

Giuliano:2001:GLI
Kenneth J. Giuliani and Guang Gong. Generating large instances of the Gong–
Harn cryptosystem. Lecture Notes in Computer Science, 2260:317–??, 2001. CO-
bibs/2260/22600317.htm;

Goldstone:2005:FCR
Lawrence Goldstone and Nancy Bazelon Goldstone. The Friar and the Cipher:
Roger Bacon and the Unsolved Mystery of the Most
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Gordon:2004:TEA

Ganapathy:2005:APA

Gennaro:2003:SAP

Gallagher:2006:HSB

Gentry:2001:CNS

Gomulkiewicz:2002:HWA
Marcin Gomulkiewicz and Mirosław Kutylowski. Hamming weight attacks on cryptographic hardware — breaking masking defense.
REFERENCES

http://link.springer.de/link/service/series/0558/bibs/2502/25020090.htm;

Goldsmith:2004:CAI


Goldwasser:2005:PPK


Gavinsky:2007:ESO


Gavinsky:2009:ESO


Garay:2007:RCA

Computer Society order number P3010.


[GLG+02] Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, and Brian Schott. Comparative analysis of the hardware implementations of hash functions SHA-
REFERENCES


Rosario Gennaro and Daniele Micciancio. Cryptanalysis of a pseudorandom generator based on braid groups. Lecture Notes in Computer Science, 2332:1-??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:


REFERENCES

Galbraith:2002:PKS


Goots:2001:FEA


Golle:2008:DCS


Gentry:2005:PAK


Galbraith:2001:CNR


Galbraith:2001:RBU

REFERENCES


Gaj:2003:FME

Goldreich:1999:MCP

Goldreich:2001:FCBb

Goldreich:2001:FCBa

Golic:2001:CAS
ny.com/link/service/series/0558/papers/2139/21390440.pdf.


**Gupta:2008:FAT**


**Ganeriwal:2008:STS**


**García-Pasquel:2006:GCT**


**Guneysu:2008:SPH**


**Guterman:2006:ALR**


**Granger:2005:HSN**

R. Granger, D. Page, and M. Stam. Hardware and software normal basis arithmetic for pairing-based cryptography in characteristic three. *IEEE
Granger:2006:SCA


Grass:1998:FC


Gra:2001:CCW


Granboulan:2002:FDC

References


[GS02c] Craig Gentry and Mike Szydlato. Cryptanalysis of

Geiselmann:2003:HSS

Geiselmann:2007:SPH

Goodell:2007:TOR

Grassl:2009:CAS

Guida:2004:DUP
REFERENCES


Geetha:2009:BIS

Garnkel:2003:PUI

Gaubatz:2008:SCD

Goodrich:2004:ETB

Giles:2002:ADW
REFERENCES

http://link.springer.de/link/service/series/0558/bibs/2502/25020126.htm;


**Goodrich:2008:NFI**


**Guttman:2004:FAP**


**Guar:2005:PPL**


**Guizzo:2006:BIC**


**Gutmann:2004:BRH**


**Guillou:2001:CAP**


**Gutmann:2000:OSC**

Peter Gutmann. An open-source cryptographic co-processor. In *USENIX [USE00d], page ?? ISBN*
REFERENCES

Gutmann:2002:CFP

Gutmann:2002:DVC

Gutmann:2004:CSA

Gutmann:2004:SPK

Gutmann:2004:ATD

Gutmann:20xx:ESR

Granger:2005:DLP


Garera:2009:CTG

Sujata Garera and Jorge Vasconcelos. Challenges in teaching a graduate course in applied cryptography. SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education), 41(2):103–107, June 2009. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Gassend:2008:CPR


Gisin:2000:LCQ


Guoxiang:2001:IFB

Gebotys:2008:EA


Goldberg:2008:PQM


Heys:2000:SAC


REFERENCES


REFERENCES


Hassler:2002:JCP


Hau
er:2003:CVH

[Hau03] Hervie Hau

Haufler:2006:SWN


Hayat:2004:CSE

[HAuR04] Khawaja Amer Hayat, Umar Waqar Anis, and S. Tauseef ur Rehman. Cryptanalysis of some encryption/cipher schemes using related key attack. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36(4):85–87, December 2004. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). NOTE FROM ACM: It has been determined that the authors of this article plagiarized the contents from a previously published paper. Therefore ACM has shut off access to this paper.

Hayashi:2006:QIT


Hoglund:2006:RSW

[HB06] Greg Hoglund and James

REFERENCES


Humire:2008:DSS

Huffmire:2008:DSS

Hartel:2001:TMS

Hartel:2001:TMS

Huang:2004:NDE

Hwang:2004:NMP
Shin-Jia Hwang and Chin-Chin Chen. New multiproxy multi-signature schemes. Applied Mathematics and
Huang:2008:NCK


Hernandez-Castro:2006:SGG


Han:2008:PBPa


Han:2008:PBPb


Henderson:2002:MTS


Halevi:2002:SSE


Han:2009:ICS

Hei01

Hei03

Hei07

Hen01
Mike Hendry. Smart card security and applications.

**Henderson:2006:CBG**


**Henry:2006:TFA**


**Herzberg:2002:SX**


**Herranz:2006:DIB**


**Herranz:2007:IBR**


**Heron:2009:AES**


**Herranz:2009:DBE**

REFERENCES


REFERENCES

Howgrave-Graham:2005:PKC


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2003:IDF


Hasenplaugh:2003:HNP

REFERENCES


Hendrick:2007:LOB


Handsich:2004:SAC


Handsich:2005:SAC


Hung:2009:FBA

Kuo Lung Hung and Shin-Wei He. Feature based affine invariant watermarking robust to geometric distortions. Fundamenta Informaticae, 92(1-2):131–143, January 2009. CODEN FU-MAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Hwang:2005:TSP

Min-Shiang Hwang, Kuo-

**Hoffstein:2006:NNE**


**Hoffstein:2003:NDS**


**Hess:2004:CTT**


**Hong:2004:DCT**

Hankerson:2001:SIE


Hamann:2001:SBA


Han:2007:FIE


Higgins:2008:NSC


Hill:2000:KII


Hilley:2006:SSD

REFERENCES


Kim:2000:RMW


Heuberger:2005:AGE


Handscho:2001:ASE


Hofmeister:2000:COS

Horwitz:2002:THI


Howard:2003:WSC


Hwang:2004:REL


Hohenberger:2005:HSO


Hwang:2005:TAU


Hwang:2005:SHW


Hwang:2005:STH

Shin-Jia Hwang and Hao-


Herzog:2003:PAK


Hwang:2001:TSB


Huang:2009:OSW


Hopper:2002:PSS


Hu:2009:TRN

0960-0779 (print), 1873-2887 (electronic).

Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU


Harbitter:2002:MAP


Hevia:2002:PSG


Hitchcock:2002:NEM

REFERENCES


Hoglund:2004:ESH


Hollar:2005:EWS


Holenstein:2004:CCB


Hankerson:2004:GEC


Huang:2007:MPK


Haastad:2004:SAR

Johan Håstad and Mats Näslund. The security of all RSA and discrete log bits. Journal of the ACM,
REFERENCES


Siegfried Höfinger. Load balancing for the electronic structure program GREMLIN in a very heterogeneous SSH-connected WAN-cluster of UNIX-type hosts. *Lecture Notes in Computer Science*, 2074: 801–??, 2001. CODEN LNCSD9. ISSN 0302-
REFERENCES


[Bhos06a]


[Bhos06b]


[Horn2000:APF]


[Huhnlein2001:ICB]


REFERENCES

Han:2002:CMV


Hoffstein:2001:NNL


Hoffstein:2008:IMC


He:2001:SAR


Hu:2005:USA


Hawkes:2001:PCS

Philip Hawkes, Frank Quick, and Gregory G. Rose. A practical cryptanalysis of SSC2. *Lecture Notes in Computer Science*, 2259:
REFERENCES


Hawkes:2000:EMC


Hand:2002:MPP


Halevi:2003:TEM


Hawkes:2004:RVC

REFERENCES


Hromkovic:2005:DAR


Hromkovic:2009:AAH


Haneberg:2002:MSS


Hinsley:2001:CIS

F. H. (Francis Harry) Hinsley and Alan Stripp, editors.
REFERENCES


Hoffstein:2001:MAD


Halevy:2002:LBE


Han:2002:HEF


Hwang:2007:PEA


He:2005:MCP


Hong:2001:KIA

Deukjo Hong, Jaechul Sung, Seokhie Hong, Wonil Lee,

Halderman:2008:LWRa


Halderman:2009:LWR


Hanaoka:2002:USA

REFERENCES


Hernandez:2001:DTR


Hernandez:2004:STN


Hess:2001:TTH


Hsu:2005:CIT


Hsu:2005:UFR

REFERENCES

Hasan:2009:PHF


Hanaoka:2000:USD


Hanaoka:2001:EUS


Halpern:2004:RSS


Huang:2006:CSV


Hongfeng:2008:ECP

Hamalainen:2002:GPS


Hines:2007:AIF


Hofheinz:2005:CTN


Hughes:2002:LAA


Hughes:2004:ISE


Huhnlein:2000:EIC

Detlef Hühnlein. Efficient implementation of cryp-

[Hunt:2005:JFE]


[Husemann:2001:SSC]


[Husemoller:2004:EC]


[Huth:2001:SCS]


[Hodjat:2004:HTP]


[Hallgren:2009:QC]

Sean Hallgren and Ulrich Vollmer. Quantum...


REFERENCES


REFERENCES

0018-9448 (print), 1557-9654 (electronic).


REFERENCES

**Hirose:2001:UAS**

**Hwang:2003:ASM**

**Hwang:2003:CAL**

**Yeh:2008:STB**

**Han:2005:PJIb**

**Han:2005:PJI**


IEEE:2005:AIS


IEEE:2005:PIS


IEEE:2006:AIS


IEEE:2007:PAI


IEEE:2008:PAI

puter Society order number P3436.

[IEEE:2009:ISI]
IEEE, editor. 

[IEEE:2009:PAI]
IEEE, editor. 

[Ito:2001:SIS]
Naomaru Itoi, Tomoko Fukuzawa, and Peter Honeyman. Secure Internet smartcards. 

[Ifr:2000:UHN]

[Igl:2002:NSB]
A. Iglesias. A new scheme based on semiconductor lasers with phase-conjugate feedback for cryptographic communications. 
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title and Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iwata:2000:PAF</td>
<td>Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of AES finalists — RC6, Serpent, MARS and Twofish (abstract only). In NIST [NIK00], page 9. ISBN ????, LCCN ???. URL [URL7], [URL8], [URL9], [URL10].</td>
</tr>
</tbody>
</table>
REFERENCES

bibs/1978/19780231.htm;

Impagliazzo:2003:LRA

isnumber=27770&prod=CNF&arnumber=1238211&arSt=p
372&ared=+383&arAuthor=Impagliazzo%2C+R.%3B+Kapron%2C+B.M.;
http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=27770&arnumber=1238211&count=66&index=
38. IEEE Computer Society Order Number PR02040.

Impagliazzo:2006:LRA


Ichikawa:2000:HEA


Ishai:2003:EOT

REFERENCES


Izmerly:2006:CCA


Izmerly:2006:CCA

Izotov:2001:COC


Inamori:2002:SPB


**Inoue:2005:EST**


**Intel:2000:IIP**


**Intel:2003:IRN**


**Itkis:2001:FSS**


**Itkis:2002:SSB**


**Irwin:2003:BRBb**


Itoi:2000:SCI

Itoi:2001:SCS

Iwami:2008:AIA

Imai:2000:CPC

Irwin:2005:PAI

Iwamoto:2006:SSR

Iwata:2002:NCP
Tetsu Iwata, Tomonobu Yoshino, and Kaoru Kurosawa. Non-cryptographic primitive for pseudorandom permutation. Lecture


REFERENCES


[Jan08a] Richard Jankowski. Book review: *Privacy on the Line: The Politics of Wiretap-
REFERENCES


Jankvist:2008:TMH


Jennnewein:2000:FCQ


Jones:2005:RDF


Johnson:2001:IHS


Jeffrey:2008:PAM


Jennings:2009:SLL


Jonsson:2002:SRE


Jonsson:2002:SRT


Jang:2001:BWA


Jung:2001:EMO


Jallad:2002:ICC

Kahil Jallad, Jonathan


Wen-Shenq Juang and Horng-Twu Liaw. Fair blind threshold signatures in wallet with observers.
REFERENCES


Jeong:2008:PKE

Lee:2007:RKD

Juang:2001:FBT

Juang:2002:VMA

Jakobsson:2003:FMT

Johansson:2003:PCI
Thomas Johansson and Subhamoy Maitra, editors. Progress in Cryptology—
REFERENCES


Jakobsson:2007:DPD


Jing-mei:2005:CRB


Joux:2002:BAA


Johnson:2000:AFR

REFERENCES

Johansson:2003:FSE


Jolish:2001:EDP


Jones:2008:RAA


Joux:2002:WTP

Antoine Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. Lecture
Joux:2004:MIH


Joux:2009:AC


Joyner:2000:CTC


Joye:2003:CPY


Joye:2003:TCC


Jakobsson:2002:Mal


Jaulmes:2002:SHG


Joye:2003:GFA


Jain:2006:TMB


Jakubowska:2007:MCT

Gizela Jakubowska and Wojciech Penczek. Modelling and checking timed authen-
REFERENCES

Jiang:2004:FAP


Joye:2004:CHE


Joye:2001:PMA


Joye:2001:OAD

REFERENCES

Juric:2006:CPW

Jin:2001:WCS

Jaworski:2009:RKP

Jarecki:2005:FSP

Jongkook:2001:NUS
Lee Jongkook, Ryu Shiryong, Kim Jeungseop, and Yoo Keeyoung. A new undeniable signature scheme using smart cards. Lecture Notes in Computer Science,
Jiang:2005:SAI


Joye:2001:PAD


Joye:2001:CEN


Joye:2001:CEN


Juang:2004:EPA

REFERENCES

Juels:2004:FCI


Juels:2005:APD


Junod:2005:SCB


Jutla:2001:EMA


Ji:2001:CAF


Juels:2005:APD
REFERENCES

Jeng:2006:EKM

Jin:2005:EAW

Jiang:2005:RNP

Joye:2001:NMM

Jakobsson:2004:ACN
REFERENCES


### REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>
Karski:2001:SSS


Kariya:2002:GM


Katzenbeisser:2001:RAR


Katos:2005:RTB


Katz:2005:CBR


Kendall:1939:TRS


Kovacic:2000:HTC

Kiely:2006:SSM


Kamvar:2007:DTM


Kim:2009:DCA


Kachris:2003:RLB


Keller:2009:ECC


Kac:2001:IMM

try Resort Hotel, San Diego, CA.

Kim:2002:SMA


Ku:2005:CFR


Kieu:2009:IAB


Ku:2005:WYR


Kieu:2009:HSI


Kim:2007:SBE

REFERENCES


Sharon S. Kellar. NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms. National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, January 31, 2005. 4 pp. URL http://
REFERENCES


REFERENCES


Kilian:2005:TCS


Kim:2001:PKC


Kim:2002:ISC

REFERENCES

[King:2000:IMP]

[King:2001:CMF]

[King:2002:RGI]

[Kirkby:2001:CCW]

[Kirtland:2001:INC]

[Montgomery:2003:FEC]
Kocarev:2001:LMB


Kanade:2005:AVB


Kim:2005:IYA


Kim:2002:NIS


Klein:2003:FOW


Kawachi:2006:PQC

A. Kawachi and T. Koshiha.


Ko:2007:SR


Klowski:2009:SGS


Kawachi:2005:UTQ


Kim:2009:SVN


Kaliski:2002:CHE

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(2m). Lecture Notes in Computer Science, 2433:...


Ko:2000:NPK


Klein:2007:BDC


Kong:2001:AVW


Kiltz:2005:SCM


Kaczprzak:2006:CBS

Kalai:2009:SEU


Knudsen:2000:CRA


Kim:2002:EPS


Kim:2001:NPK


Kim:2003:IBP

REFERENCES

Knudsen:2001:CRR

L. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds. In Schneier [Sch01d], page ??.

Knudsen:2001:CPL


Kanda:2002:SCA


Koblitz:2004:OTS

REFERENCES


REFERENCES


Klarlund:2001:MIS


Klimov:2002:ANC


Kim:2003:RCC


[KNu00a] L. Knudsen. Trawling Twofish. Reports in informatics, University of

\textbf{Knudsen:2000:TTR}

L. Knudsen. Trawling Twofish — revisited. In \textit{???.}, editor, \textit{Third AES Candidate Conference}, page \textit{???.}, \textit{???.}, \textit{???.}, April 2000. ISBN \textit{???.} LCCN \textit{???.}

\textbf{Knudsen:2002:ACE}


\textbf{Kushilevitz:2000:OWT}


\textbf{Komano:2003:EUP}

Katz:2004:ROS


Koblitz:2000:TQC


Kocher:2002:IS

Paul Kocher. Illusions of security, 2002. URL [Kor09]

Kurosawa:2001:ICP


Kornblum:2009:IBD

menting BitLocker drive encryption for forensic analysis. Digital Investigation, 5 (3):75–84, ????. 2009. URL ????. [Kos01c]

Koshiba:2001:NAS


Koshiba:2001:SRS

[Kos01b]


Koskinen:2001:NIK


Kovach:2001:BCB


Kovacic:2003:ISS

Katz:2001:EPA


Katz:2009:ESA


Katzenbeisser:2000:IHT


Koc:2001:CHEa


Koc:2003:GEI

REFERENCES

Kerins:2002:FPE


Klima:2003:ARB


Kaufman:2002:NSP


Kim:2004:TBG


Krishna:2003:BUP


Krawczyk:2001:OEA

[Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How
secure is SSL?). In Kilian [Kil01a], pages 310–
?? ISBN 3-540-42456-
3 (paperback). LCCN
QA76.9.A25 C79 2001; [Kra03]
QA267.A1 L43 no.2139.
UK £47.00. URL http://
//link.springer-ny.com/
link/service/series/0558/
| bibs/2139/21390310.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2139/21390310.|
pdf.

Krause:2002:BBC

[Kra02a]
Matthias Krause. BDD-
based cryptanalysis of keystream
| generators. Lecture Notes
in Computer Science. 2332: |
222–??, 2002. CODEN |
LNCS.D9. ISSN 0302-
9743 (print), 1611-3349 |
(electronic). URL http://
//link.springer-ny.com/
link/service/series/0558/
| bibs/2332/23320222.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2332/23320222.| pdf.

Krause:2002:USP

[Kra02b]
Rory Krause. Using |
SSH port forwarding to |
| print at remote locations. |
Linux Journal, 94:60-62, 64, |
February 2002. CODEN |
LIJOFX. ISSN 1075-3583 |
(print), 1938-3827 (elec-
tronic). URL http:// |
| noframes.linuxjournal.|

Krawczy:2003:SSM

Hugo Krawczy. SIGMA: |
The “SIGn-and-Mac” ap-
| proach to authenticated |
| Diffie–Hellman and its |
use in the IKE proto-
cols. In Boneh [Bon03], |
pages 400–425. CODEN |
| LNCSD9. ISBN 3-540-
40674-3. ISSN 0302-9743 |
| (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25 |
| C79 2003. URL http://
//link.springer-ny.com/
link/service/series/0558/
| tocs/t2729.htm; http://
www.springerlink.com/
openurl.asp?genre=issue&
| issn=0302-9743&volume= |
2729; http://www.springerlink.| com/openurl.asp?genre= |
| volume&id=doi:10.1007/ |
b11817.

Krawczyk:2005:HHP

Hugo Krawczyk. HMQV: |
a high-performance secure |
| Diffie–Hellman protocol. |
In Shoup [Sho05a], pages |
546–?? ISBN 3-540-
28114-2. ISSN 0302-9743 |
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25 |
C79 2005; QA76.9 .A25; |
QA76.9 C79 2005; QA76.9 |
C794 2005; QA76.9: In-
| ternet. URL http://
//www.springerlink.com/
openurl.asp?genre=issue&
| issn=0302-9743&volume= |
3621.
REFERENCES

Kramer:2007:LCC


Kreitz:2005:OBE


Koeune:2002:FIL


Kehr:2001:ISM


KRS+02


Katz:2000:CCA

REFERENCES

Kelsey:2000:MAP

John Kelsey and Bruce Schneier. MARS attacks! preliminary cryptanalysis of reduced-round MARS variants. In NIST [NIS00], pages 169–185. ISBN ????. LCCN ???. URL

Krause:2003:DOC


Kozaczuk:2004:EHP


Katz:2005:MIA

Kiltz:2005:TCL  

Kissner:2005:PPS  

Klivans:2006:CHL  
REFERENCES


[KSHY01] Ju-Sung Kang, Sang-Uk Shin, Dowon Hong, and Okyeon Yi. Provable security of KASUMI and 3GPP

Kumar:2002:APS


Kogan:2006:PRS


Kuribayashi:2000:WSB

REFERENCES


REFERENCES

**Ku:2004:HBS**


**Kuhn:2000:PCL**


**Kuhn:2001:CRR**


**Kuhn:2002:OTD**


**Kuhn:2008:BSS**


**Kukorelly:2001:P**

REFERENCES

IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Kumagai:2007:RSK


Kundur:2001:WDI


Kurosawa:2001:MRP


Kusters:2002:DCP


Kuo:2001:AOS


Komninos:2007:ALS

Komninos, Nikos, Dimitrios D. Vergados, and Christos Douligeris. Au-
REFERENCES


Kejariwal:2009:ELL


Koshiba:2000:SEP


Knudsen:2002:IC


Karlof:2003:HMM


Keromytis:2006:COS

REFERENCES


Kwon:2002:DSA


Kwok:2003:WBC


Kwon:2003:EDS


Kumar:2006:ODS


Wong:2001:MCC


Kun:2000:SMA


Kamat:2009:TPW

Pandurang Kamat, Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Temporal privacy in wireless sensor

Katz:2000:CCS


Katz:2001:UEC


Kavut:2001:SCP


Kiayias:2001:PRB


Kiayias:2001:SPP

Kurosawa:2001:LCI


Katz:2002:TCB


Kiayias:2002:CHB


Kim:2002:PAA


Katz:2003:SPA

Jonathan Katz and Moti Yung. Scalable protocols for


A. A. Kamal and A. M. Youssef. An FPGA implementa-

[KZ03]


Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyun-
sook Cho. Pseudorandomness of MISTY-type trans-
formations and the block cipher KASUMI. Lecture
Notes in Computer Science, 2119:60–??, 2001. CO-
DEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). URL http: //link.springer-ny.com/ link/service/series/0558/ [KZ01]
bibs/2119/21190060.htm; http://link.springer-


M. Kabatnik and A. Zugenmaier. Location stamps for digital signatures: a
new service for mobile telephone networks. Lecture
Notes in Computer Science, 2094:20–??, 2001. CO-
DEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http: //link.springer-ny.com/ link/service/series/0558/ [KZ01]
bibs/2094/20940020.htm; http://link.springer-

[KZ03]


J. Kamp and D. Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptog-
ography. In IEEE [IEE03], pages 92–101. CODEN ASFPDV. ISBN 0-7695-
REFERENCES


[Lan00c] Susan Landau. Technical opinion: designing cryptography for the new century. *Communications of


Laud:2008:CSC


Laughlin:2008:CRC


Lavington:2006:FCD


Lavoué:2009:LRM


Lawton:2005:MAH


Lawson:2009:SCA


Lawson:2009:TAG


Li:2004:QAU

REFERENCES


REFERENCES

Laih:2003:COP

Lin:2004:SOT

Lu:2004:XMS

Lu:2005:ND

Long:2005:DTC

Lu:2007:NPL
Lee:2001:SEK


Lee:2003:APS


Lee:2004:DEB


Lim:2009:OPG


Li:2008:CAM

Zhongwen Li, Qiong Chen, and Yang Xiang. A cross-authentication model and implementation. International Journal of Computer Systems Science and Engi-
REFERENCES

neering, 23(3):??, May 2008. CODEN CSSEEI. ISSN 0267-6192.

Lu:2005:TUS


Lu:2005:PBM


Lu:2005:RTP


Li:2001:CCB


Lai:2004:SGS


Lavoué:2007:SSW


Law:2006:SBB


REFERENCES

issue&issn=0302-9743&volume=1
3329; http://www.springerlink.com/openurl.asp?genre=

Lehtinen:2006:CSB


Lenstra:2001:USM


Lenstra:2001:USM

[Leh06]

Levy:2001:CHC


Lewand:2000:CM

Lee:2003:PKB


Lei:2007:CSA


Liaw:2004:SPA


Lekkas:2004:CNL


Levi:2009:ULM


Lang:2001:CMS

REFERENCES


http://link.springer-
REFERENCES


[LHT09] Cheng-Chi Lee, Min-Shiang Hwang, and Shiang-Feng

Lee:2002:FRU


Lee:2005:NBS


Li:2001:NASA


Li:2005:ABPa


Lieman:2005:CRW

REFERENCES


C & L, Böblingen, Germany, 2002. ISBN 3-932311-87-8 (??invalid checksum??). 476 (est.) pp. LCCN ????


[LK01] Stefan Ludwig and Winfried Kalfa. File system encryption with integrated user management. *Operating
Lee:2008:SAF

Lee:2009:SAF

Lim:2001:SAW

Lee:2003:PSAa

Lee:2003:PSAb

Lee:2005:NIW


REFERENCES

Lim:2000:GTC


Luo:2004:UUR


Lee:2003:ISC


Lu:2001:DWC


Lou:2002:SMS

REFERENCES


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


[LLH04] Li-Hua Li, Chi-Yu Liu, and Min-Shiang Hwang. Crypt-


REFERENCES

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

Li:2006:ESY


Li:2006:SYG


Lindell:2002:CAB


Lian:2007:MDE


Lee:2005:IWR


Liu:2005:SWA

Sanya Liu, Zhenyu Liu, and Zhongren Su. Securing Web application system: a solution based on SMS for identifying users. In Han

Lee:2009:CET


Li:2004:ABP


Li:2005:ATN


Liu:2008:DEA


Liu:2008:SAM

REFERENCES


Li:2009:ATN

Lee:2006:DCK

Linares:2000:Sam

Lorenz:2002:SSG

Lavasani:2008:IFA

Li:2003:SCE
Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and


**Lu:2005:CCA**


**Lu:2005:CCA**


**Liu:2004:MBA**


**Leviell:2008:CTC**


**Liu:2008:ARL**


**Lotspiech:2002:CFB**

Jeffrey Lotspiech, Stefan Nusser, and Florian Pe-


REFERENCES

Lindell:2000:PPD


Lysyanskaya:2001:AST


Labbe:2002:AIF


Luccio:2002:AC


Lee:2003:CPK


REFERENCES


ervations of attack signatures: a basis for building self-protecting servers.

[Liu:2008:GPV]

[LS08]

[LSC03]


[Lin:2003:SEOa]

[Lin:2003:SEOb]

[Lu:2005:BIW]
Haiping Lu, Yun Q. Shi, Alex C. Kot, and Lihui
REFERENCES


Li:2005:ABPb


Liang:2009:AIE

Zhenkai Liang, Weiqing Sun, V. N. Venkatakrishnan, and R. Sekar. Alca-traz: An isolated environment for experimenting with untrusted software. ACM Transactions on Informa-

Lee:2001:EPI


Liu:2005:RBU


Lin:2004:SIS

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

Li:2005:ISS


Lie:2000:ASC


Lu:2007:NSC


Lu:2005:HAO


Lucs:2000:ASR

Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys.

Lucks:2002:SAB


Ludvig:2005:PWF


Lukyanov:2001:PFA

REFERENCES


REFERENCES

Laguillaumie:2007:MDV


Lange:2002:PIE


Lee:2004:IAK


Liang:2005:PA


Loepp:2005:PIC


Lyuu:2005:CIH

REFERENCES

739, August 5, 2005. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Lin:2000:PAS

Lv:2005:PCA

Lv:2005:SMS

Lin:2009:DMG

Li:2005:IWR

Lin:2005:NIB
REFERENCES

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

[LXM+05] Xu Lixin, Zhang Xincheng,
He Min, Wu Xianglin, and
Qingyun Ru. A four-layer
architecture for Web applica-
tion system security as-
surance: a safeguard mech-
anism research. In Han
et al. [HYZ05b], pages 87–
LCCN ?? ?? URL http://
eproceedings.worldscinet.
com/9812701532/9812701532.
0031.html.

[LYGL07] Shao-Hui Liu, Hong-Xun
Yao, Wen Gao, and Yong-
Liang Liu. An image frag-
ile watermark scheme based
on chaotic image pattern
and pixel-pairs. Applied
Mathematics and Computation,
185(2):869–882, February
15, 2007. CODEN AMHCBQ.
ISSN 0096-3003 (print),
1873-5649 (electronic).

[Lys02] Anna Lysyanskaya. Unique
signatures and verifiable
random functions from the
DH–DDH separation. In
Yung [Yun02a], pages 597–
612. CODEN LCSD9.
ISBN 3-540-44050-X (pa-
perback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2002. URL http://
link.springer.de/link/
service/series/0558/bibs/1
2442/24420597.htm; http://
link.springer.de/link/
service/series/0558/papers/1
2442/24420597.pdf.

[LY05] Zude Li and Xiaojun Ye.
Attribute analysis of usage
control (UCON). In Han
et al. [HYZ05b], pages 59–
LCCN ?? ?? URL http://
eproceedings.worldscinet.
com/9812701532/9812701532.
0031.html.

[LY07] Weihai Li and Yuan Yuan.
A new blind attack pro-
cedure for DCT-based
image encryption with spec-
trum learning. International
Journal of Image and
Graphics (IJIG), 7(3):481–
496, July 2007. CODEN
???? ISSN 0219-4678.

[LYC02] D-C Lou, T-L Yin, and M-C
Chang. An efficient stegan-
ographic approach. Interna-
tional Journal of Computer
Systems Science and En-
gineering, 17(4/5):??, July/
September 2002. CODEN
CSSEEI. ISSN 0267-6192.

[Lou:2002:ESA] 

[Lys07] Anna Lysyanskaya. Authen-
tication without identifica-

[Lou:2002:ESA]
REFERENCES

487

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

**Lysyanskaya:2008:CHK**

[102x681]REFERENCES

Anna Lysyanskaya. Cryptography: How to keep
secrets safe. *Scientific
American*, 299(3):88–95, [LZ09]
September 2008. CO-
DEN SCAMAC. ISSN
0036-8733 (print), 1946-
7087 (electronic). URL
http://www.nature.com/
scientificamerican/journal/
nature.com/scientificamerican/journal/v299/n3/pdf/scientificamerican0908-
88.pdf.

**Leung:2001:WDI**

K. H. Leung and Bing Zeng.
Wavelet-domain image wa-
termarking based on sta-
tistical metrics. *Lecture
Notes in Computer Science*,
2195:788–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2195/21950788.htm;
http://link.springer-
y.com/link/service/series/
0558/papers/2195/21950788.
pdf.

**Li:2004:CAB**

Hua Li and Chang N.
Zhang. A cellular automata
based reconfigurable archi-
tecture for hybrid crypto-
systems. *The Computer
ISSN 0010-4620 (print),
1460-2067 (electronic).

**Lao:2009:ORA**

Yuanwei Lao and Yuan F.
Zheng. Optimal rate alloca-
tion for logo watermarking.
*International Journal of Im-
age and Graphics (IJIG)*, 9
(1):1–25, January 2009. CO-
DEN ????. ISSN 0219-4678.

**Li:2001:GOT**

Zi-Chen Li, Jun-Mei Zhang,
Luo, William Song, and Yi-Qi Dai. Group-
oriented \((t, n)\) threshold dig-
ital signature schemes with
traceable signers. *Lecture
Notes in Computer Science*,
2040:57–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2040/20400057.htm;
http://link.springer-
y.com/link/service/series/
0558/papers/2040/20400057.
pdf.

**Li:2004:WMS**

Li Li, David Zhang, Zhi-
geng Pan, Jiaoying Shi, Kun
Zhou, and Kai Ye. Water-
marking 3D mesh by spher-
Maurer:2007:ICP


Mrayati:2003:AKT


Mrayati:2004:IAD


Mrayati:2005:IDB

M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, editors. *Ibn Dunaynir’s book: Expositive chapters on cryptanalysis*: (Maqasid al-fusul al-mutargima an hall


[MAC+03] George M. Mohay, Alison Anderson, Byron Collie,


References

Mann:2002:HI


Mann:2008:HHS


Mao:2001:TRC


Mao:2004:MCT


Marques:2002:BSJ


Martinelli:2002:SSA

REFERENCES

Mares:2005:BRA


Martin:2005:STA


Mastroeni:2004:APA


Matsui:2002:FSE


Martin:2008:IBE


Martin:2008:CCI

Maurer:2001:C


Maurer:2004:RCD


Maughan:2005:HSC


Maximov:2006:SWC


Mayers:2001:USQ


May:2002:CUR


May:2004:CRS

Alexander May. Computing the RSA secret key is deterministic polynomial time equivalent to factoring. In Franklin [Fra04], pages 213–?? CODEN LNCSD9.
May:2009:PIS


May:2009:PIS

[May09]


Mel:2001:CD

[MB01]


Mohanty:2008:IWB


McKinnon:2004:CCS


Montenegro:2004:CBI


McAndrew:2008:TCO
REFERENCES


REFERENCES


[Men03] Jesús Mena. Investigative data mining for security and criminal detection. Butterworth-

Menezes:2005:TCC


Menezes:2007:ACC


Messerges:2000:SAF


Messerges:2001:SAF

McGrew:2001:AAE


Marti-Farré:2007:NSS


Matula:2005:TLS


Mueller:2006:SMG


Muller:2009:BPE

Minier:2001:SCC


Muresan:2008:PCA


Mukherjee:2002:CAB


Molland:2004:ICA


Ma:2005:NCD


Maas:2009:SRW


Mihaljevic:2009:ASC

Micciancio:2001:ILB

Micciancio:2002:GCK
REFERENCES


REFERENCES


Moore:2001:AGK


Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS


Moyle:2005:CLD


Mazieres:2000:SKM


[MM07b] Gary L. Mullen and Carl
REFERENCES


Moreira:2002:RCE


Milenkovic:2005:UIB


Maltoni:2003:HFR


McEvoy:2009:IWH


Maitra:2006:PCI

REFERENCES


**Matsumoto:2002:IAG**


**Maclean:2000:OIG**


**Mizuki:2001:NSN**


**Mercuri:2003:IRS**


**Mukhopadhay:2014:EMP**

REFERENCES

1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013002627. This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.


[Mironov:2008:SAE] Ilya Mironov, Moni Naor, and Gil Segev. Sketching in

MacAndrew:2000:LPT


Mykletun:2006:AIO


Mollin:2001:IC


Moller:2002:PEC


Moller:2003:PSP

Mollin:2003:RPK


Mollin:2005:CGS


Mollin:2007:IC


Monniaux:2003:ACP

David Monniaux. Abstracting cryptographic protocols with tree automata.


Moore:2001:UMW


Moore:2007:CQK


Mangard:2006:PAA

REFERENCES

Morris:2003:KKL


Moritz:2005:KAE


Moses:2006:DSD


Merton:2000:NBG


McMillan:2001:JIA


Mihailescu:2001:BRE

REFERENCES

[Moshopoulous:2001:NSA]

[Malkhi:2002:ACE]

[Maurer:2003:SMR]

[Micciancio:2005:ASS]

[Matusiewicz:2006:FGD]
Krystian Matusiewicz and Josef Pieprzyk. Finding

Munilla:2007:HMF


Micciancio:2008:OCC


Misllov:2006:EBO


Moralis:2009:KSA


Micali:2005:OEC

Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error correction against computationally bounded noise. In Kilian [Kil05], pages 1–?? CODEN LNCSD9. ISBN 3-540-24573-1 (softcover). ISSN 0302-9743
REFERENCES


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


Murphy:2002:EASb


Matyas:2003:TRU


Micciancio:2009:LBC


Monrose:2002:TSG


Mitchell:2006:PPT


Mayer-Sommer:2001:SAS

Rita Mayer-Sommer. Smartly analyzing the simplicity and the power of simple power
analysis on smartcards. Lecture Notes in Computer Science, 1965:78–??, 2001. CO- 
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:// 
link.springer-ny.com/ link/service/series/0558/ 
bibs/1965/19650078.htm; http://link.springer- 
ny.com/link/service/series/1 
0558/papers/1965/19650078.}

Maggi:2002:USV

Paolo Maggi and Riccardo Sisto. Using SPIN to verify security properties of cryptog- 
tographic protocols. Lecture Notes in Computer Science, 2318:187–??, 2002. CO- 
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:// 
link.springer-ny.com/ link/service/series/0558/ 
bibs/2318/23180187.htm; http://link.springer- 
ny.com/link/service/series/1 
0558/papers/2318/23180187.}

Maitra:2002:CSB

Subhamoy Maitra and Palash Sarkar. Cryptographically significant Boolean functions with 
five valued Walsh spectra. Theoretical Computer Science, 276(1–2):133–146, 
April 6, 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (elec- 
tronic). URL http://www.elsevier.com/gej-
ng/10/41/16/247/27/33/ 
abstract.html.

Menezes:2002:PCI

ence on Cryptology in India, Hyderabad, India, December 16–18, 2002: Proceed- 
ings, volume 2551 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, 
ISBN 3-540-00263-4 (soft-cover). ISSN 0302-9743 (print), 1611-3349 (elec-
link.springer-ny.com/ link/service/series/0558/ 
tocs/t2551.htm; http://www.springerlink.com/ openurl.asp?genre=issue& 
issn=0302-9743&volume=2551. Also available via the World Wide Web.

Mitnick:2002:ADC

Kevin D. (Kevin David) Mitnick and William L. Simon. The art of deception: controlling the human element of secu-

4, 0-7645-4280-X (paper-
REFERENCES


Muthukrishnan:2002:IAS


Markowitch:2003:CWV


Miklau:2003:CAP


Martin:2005:PET


Meadows:2005:CPA

REFERENCES

Mahdian:2009:UNI


Manulis:2009:SMF


Mashatan:2009:ITC


Myers:2009:BEC


Shen:2005:NIW


MacKenzie:2002:TPA

McClure:2003:HEN


Matsumoto:2007:FSC

Makoto Matsumoto, Mitsuo Saito, Takuji Nishimura, and Mariko Hagita. A fast stream cipher with huge state space and quasigroup filter for software. In Adams et al. [AMW07], pages 246–263. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ????.

Miltchev:2008:DAC


Mouratidis:2009:PMD


Moran:2004:NIT


Myasnikov:2005:PAB

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

Muzereau:2004:EBD


Marsaglia:2002:SDP


Meseguer:2007:SRA


Ma:2009:NAS


Muller:2001:SWB

Muller:2001:SIC


Mullins:2002:MUC


Mullins:2006:CC


Munro:2008:DE


Murphy:2000:KST

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

Murray:2001:CDC


Murray:2002:IYP


Moriai:2000:PTL

REFERENCES

Meister:2001:PPG

Micciancio:2003:SZK

Micciancio:2004:CTA

Ma:2006:ADS
REFERENCES

Morelli:2001:JAH

Malan:2008:IPK

MRaihi:2001:CAS

McCook:2001:NSS

Morelos-Zaragoza:2002:AEC

Matsui:2004:SAC
Mitsuru Matsui and Robert Zuccherato, editors. *Selected Areas in Cryptography: 10th Annual International
REFERENCES


Nagy:2007:AQK


Naik:2003:DSW


Naccache:2001:TCC


Naftali:2005:BSS

Nakai:2001:SFW


Namprempre:2002:SCB


Naor:2002:DRA


Naor:2003:CAC


Naor:2004:TCF

Moni Naor, editor. Theory of Cryptography: First Theory of Cryptography Conference, TCC 2004, Cam-


[NCRX04] Peng Ning, Yun Cui, Douglas S. Reeves, and Dingbang Xu. Techniques and tools for analyzing intru-
REFERENCES

527


Neve:2003:STF

Amaury Nève, Denis Flan-  
dre, and Jean-Jacques  
Quisquater. SOI techn-  
nology for future high-  
performance smart cards.  
IEEE Micro, 23(3):58–67,  
May/June 2003. CODEN  
IEMIDZ. ISSN 0272-1732  
(print), 1937-4143 (elec-

[Ng05]

[HF02]

[NHO2]

bibs/2259/22590313.htm;  
http://link.springer-
ny.com/link/service/series/|
0558/papers/2259/22590313.|  

Nguyen:2001:TFLb

Phong Q. Nguyen. The  
two faces of lattices in cryp-
tology. Lecture Notes in  
Computer Science, 2259:  
313–??, 2001. CODEN  
LNCSD9. ISSN 0302-9743  
(print), 1611-3349 (elec-

[Ho3]

[NH03]

Nyberg:2003:SAC

Kaisa Nyberg and Howard  
Heys, editors. Selected areas  
in cryptography: 9th annual  
International Workshop,  
SAC 2002, St. John’s, New-

[NHO2]

http://csdl.computer.  
org/dl/mags/mi/2003/03/  
m3058.pdf.

[Ng01]

Nguyen:2005:RBP  
Minh-Huyen Nguyen. The  
relationship between pass-
word-authenticated key  
exchange and other crypto-
graphic primitives. In Kilian  
[Kil05], pages 457–??  
CODEN LNCSD9. ISBN  
3-540-24573-1 (softcover).  
ISSN 0302-9743 (print),  
1611-3349 (electronic).  
LCCN QA76.9.A25 T44  
2005. URL  
http://www.springerlink.  
com/openurl.asp?genre=
volume&id=doi:10.1007/  
b106171.

[NH02]

[NH03]

http://www.springerlink.  
com/openurl.asp?genre=
volume&id=doi:10.1007/  
b97045.

[HF02]

[Ho3]

[Ng01]

[Ng05]  
[HF02]  
[Ho3]  
[NH03]

http://library.lanl.gov/cgi-
bin/getfile?27-08.pdf.

[HF02]  
[Ho3]  
[NH03]

Nyberg:2003:SAC

Kaisa Nyberg and Howard  
Heys, editors. Selected areas  
in cryptography: 9th annual  
International Workshop,  
SAC 2002, St. John’s, New-

Nicholson:2001:YBC


Niederreiter:2002:BRC


Nielsen:2002:SR


Nielsen:2002:TPF

[102x156] Jesper Buus Nielsen. A threshold pseudorandom function construction and

Nievergelt:2002:FLM


Niederreiter:2004:BRC


Nikander:2002:DSAa


Nikander:2002:DSAb

Pekka Nikander. Denial of service, address ownership, and early authentication in the IPv6 world (transcript of discussion). Lecture Notes in Computer Science, 2467:22–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
REFERENCES


NIST:2000:TAE


NIST:2001:CT


NIST:2001:SRC


Nisley:2003:ELH


NIST:2003:RKE


[NN03] Dalit Naor and Moni Naor. Cover feature: Protect-

Nikon:2006:RBV


Naor:2001:RTS


Novak:2001:SBA


Naccache:2002:PKC

David Naccache and Pascal Paillier, editors. Public


Nichols:2000:D


Neraud:2001:CFD


Nguyen:2001:ISA


Nguyen:2001:TFLa


Narayanan:2005:FDA


Narayanan:2005:ODG

[NS05b] Arvind Narayanan and Vitaly Shmatikov. Obfuscated databases and group privacy. In Meadows and Syverson [MS05b], pages 102–111. ISBN 1-59593-
REFERENCES


(print), 1611-3349 (electronic).

verifiable shuffle based on a variant of the Paillier cryptosystem. *J.UCS: Journal of

fast provably secure public-key cryptosystems based on a modular squaring. *Lecture
Notes in Computer Science*, 2288:81–??, 2002. CODEN LNCSD9. ISSN 0302-9743

349–350, June 2007. CODEN ???? ISSN 0163-5999
(print), 1557-9484 (electronic).

CODEN DAMADU. ISSN 0166-218X (print), 1872-6771 (electronic).

0948-6968. URL http://www.jucs.org/jucs_11_1/rsa_based_certified_delivery.
REFERENCES


Oiwa:2009:IMS
REFERENCES


REFERENCES

2000. CODEN SYADE7. ISSN 1061-2688. URL http://www.samag.com/

Ohigashi:2009:PMF

Toshihiro Ohigashi and Masakatu Morii. A practical message falsification attack on WPA. Technical report, Hiroshima University, 1-4-2 Kaga

Ohkuma:2001:BCH


Ohbuchi:2002:FDA


Onions:2001:SSI


Ors:2003:PAA

REFERENCES


REFERENCES


REFERENCES


Okeya:2004:SBR

OST05

OST06

Osvik:2000:SS

Osvik:2005:CAC

Osvik:2006:CAC

Okeya:2003:MFC


Raphael Overbeck. Extending Gibson’s attacks on the GPT cryptosystem. In Ytrehus [Ytr06], pages 178–188.
Oniev:2008:MNS

Paeng:2003:SCU

Page:2003:BRW

Panditaratne:2007:TRN

Papanikolaou:2005:BRBa

Park:2004:APP
REFERENCES

Pass:2003:DCR


Pass:2005:UCN


Patiyo:2002:MSE


Patiyo:2002:SIW


Patarin:2003:LRR

REFERENCES


Paterson:2003:CCI


Patarin:2004:SRF


Paulson:2001:RBS


Paulson:2002:NBPa


Alessandro Piva, Franco Bartolini, and Roberto Piva:2002:MCW


Alessandro Piva, Franco Bartolini, and Roberto Bartolini:2005:SRA

Park:2000:CAP


Peng:2005:SES


Peng:2007:BZK


Prattichizzo:2007:PIH


Papadimitriou:2001:PSE

Perez:2007:URR


Poulos:2008:TSE


Pucheral:2001:PSD


Petrie:2000:NBI


Peikari:2004:SW


Park:2005:ISC

REFERENCES


Park:2005:NDS


Patarin:2001:QBL


Patarin:2003:ESA

REFERENCES


Pemble:2001:CEW

Pemble:2001:SPA

Perrine:2003:ECP

Perlman:2005:EMD

Petullo:2003:IEH

Petullo:2005:EYR

Petzold:2008:ATG
REFERENCES


REFERENCES


[PJH01] Ji Hwan Park, Sook Ee
REFERENCES


Park:2001:RFW


Poh:2001:HBP


Petitcolas:2003:DWF


Park:2001:CSC

[PKBD01] DongGook Park, JungJoon Kim, Colin Boyd, and


Shun-Fu Pon, Erl-Huei Lu, and Albert B. Jeng. One private-key for all DL-based cryptosystems. *Applied Mathematics and Com-

**Pfleeger:2007:IBC**


**Paulson:2000:NBU**


**Piper:2002:CVS**


**Pang:2008:AQR**


**Peyravian:2000:MBB**


**Pohlmann:2001:SCA**


**Pointcheval:2000:CCS**

[David Pointcheval. Chosen-ciphertext security for any


REFERENCES


REFERENCES

**Paar:2009:UCT**


**Pellikaan:1996:AGC**


**Pereira:2003:SAU**


**Piret:2003:DFA**


**Pereira:2006:IBS**


**Picard:2001:NNF**

REFERENCES


Pass:2005:NIC


Pass:2008:NIC


Preneel:2000:ACE


Preneel:2001:NES


Preneel:2002:NEA


REFERENCES


[Paun:2004:CTT]
Padro:2002:LBI


Pomerance:2002:SOC


Page:2004:PCA


Park:2004:UUC


Prabhakaran:2004:NNS


Prabhakaran:2005:RES

REFERENCES


Phan:2006:FDB


Park:2008:SRB


Pavlou:2008:FAD


Park:2002:SRL


Pareschi:2009:PAC


Petit:2008:BCB

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

Computer and Communications Security (ASIACCS),

Preneel:2006:SAC


Pang:2008:VCR


Pfleeger:2007:GEI


Pucella:2003:JRB


Pucella:2006:SCC


Pucella:2007:Ib

Riccardo Pucella. Introduction. ACM SIGACT News,
REFERENCES

Puzmanova:2004:RWF

Page:2006:FAP

Paillier:2006:TOW

Phillips:2001:GRI

Pang:2005:NMS

Peikert:2008:LTF
Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In ACM [ACM08], pages 187–196. ISBN 1-60558-047-

**Pelzl:2003:HCC**


**Paterson:2006:LTT**


**Palanivel:2008:MPA**


**Pieprzyk:2001:CPS**

REFERENCES

Pieprzyk:2002:CPL


Pieprzyk:2002:CCI


Pecho:2009:APW


Peng:2009:DIE


Qian:2005:CLT


Qian:2005:SPL

Haifeng Qian, Zhenfu Cao, and Haiyong Bao. Security
of Pon–Lu–Jeng’s Meta-He
digital signature schemes.
*Applied Mathematics and
Computation*, 170(1):724–
730, November 1, 2005. CO-
DEN AMHCBQ. ISSN
0096-3003 (print), 1873-
5649 (electronic).

**Quisquater:2005:SCC**

[QPV05] Michaël Quisquater, Bart
Preneel, and Joos Vande-
walle. Spectral charac-
terization of cryptographic
Boolean functions satisfying
the (extended) propagation
criterion of degree $l$ and
order $k$. *Information Pro-
cessing Letters*, 93(1):25–28,
January 16, 2005. CODEN
IFPLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

**Quisquater:2000:SCR**

[QS00] J.-J. Quisquater and Bruce
Schneier, editors. *Smart
card research and applica-
tions: third international
conference, CARDIS’98,
Louvain-la-Neuve, Belgium,
September 1998: proceed-
ings*, volume 1820 of *Lec-
ture Notes in Computer
Science*. Springer-Verlag,
Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2000.
ISBN 3-540-67923-5. LCCN

**Quisquater:2001:EAE**

[QS01] Jean-Jacques Quisquater
and David Samyde. Electro-
magnetic analysis (EMA):
Measures and counter-
measures for smart cards.
*Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
com/link/service/series/
0558/bibs/2140/21400200.
htm; http://link.springer-
ny.com/link/service/series/
0558/papers/2140/21400200.
pdf.

**Quisquater:2002:CTM**

[QSR+02] Jean-Jacques Quisquater,
François-Xavier Standaert,
Gael Rouvroy, Jean-Pierre
David, and Jean-Didier
Legat. A cryptanalytic
time-memory tradeoff: First
FPGA implementation.
*Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
com/link/service/series/
0558/bibs/2438/24380780.
htm; http://link.springer-
ny.com/link/service/series/
0558/papers/2438/24380780.
pdf.

**Qu:2001:KPW**

[Qu01] Gang Qu. Keyless pub-
lic watermarking for intel-
lectual property authenti-
cation. *Lecture Notes in
Computer Science*, 2137:
REFERENCES


Raikhel:2000:DF


Rajsbaum:2006:ASNb


Roman:2007:SCP


Ramesh:2001:TAE


Rand:1955:MRD


Rand:2001:MRD


Rijmen:2001:WHF

Vincent Rijmen and Paulo S. L. M. Barreto. The


REFERENCES

CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic). URL [RD09]

Rubin:2005:ARS

Rangan:2001:PCI

Renaud:2009:VPC

Rudra:2001:ERE

Romao:2001:SMA


REFERENCES

Regev:2005:LLE


Regev:2009:LLE


Ren:2009:CWT


Rescorla:2001:IOPa


Rescorla:2001:IOPb


Reynard:2001:SCB


Rodwell:2007:NIBa


Rodwell:2007:NIBb


REFERENCES

Roscoe:2002:TBC


Rafaeli:2003:SKM


Rhinelander:2003:DIE


Rich:2007:ATS


Riezenman:2000:CSB


Riebeck:2003:SCC


Rila:2002:DAB


Risen:2006:SWS

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


REFERENCES

Roy:2004:FSE

Reyhani-Masoleh:2003:LCS

Reyhani-Masoleh:2003:LCB

Ruiz:2001:SPS
REFERENCES


REFERENCES


Roth:2002:JSA


Roth:2002:SFC


Roth:2003:SFC


Rothe:2005:CTC


Rothe:2007:BRB


Roy:2000:PCI

REFERENCES

Roychowdhury:2000:PCJ


Roy:2005:ACA


Rieffel:2000:IQC


Ramzan:2000:RSS


Reyzin:2002:BTB

Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. Lecture Notes in
REFERENCES

Ratner:2003:NGI


Ratner:2003:NHS

[RR03a]

Rosenberg:2004:SWS


Rittinghouse:2005:IIM


Rechberger:2008:NRN


Rechberger:2006:NCW

REFERENCES

pdf;  http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=334811
15888277;  http://www.csrc.nist.gov/pki/HashWorkshop/

Rivest:2000:RA


Rosenbaum:2000:SFR


Romer:2001:ILA


Rubin:2002:SAV

REFERENCES

Rubin:2003:TBC


Riley:2004:HAE


Rao:2005:CHE


Rubin:2008:CFF


RSA:2000:PKC


RSA:2000:PVCa

REFERENCES

RSA:2000:PCP

RSA:2000:PVCb

RSA:2000:PVS

RSA:2001:PVC

RSA:2002:PVR

Rivest:2003:TAL

RSA:2003:PEC
REFERENCES

pkcs/pkcs-13/index.html
Still under development.

[RSA09a]

[RSA09b]

[RSP05]

[Rouvrroy:2003:EUF]
G. Rouvroy, F.-X. Staundraert, J.-J. Quisquater, and J.-D. Legat. Efficient uses of FPGAs for implementations
REFERENCES

Bayes:2004:CAP

[Bay04]


Rivest:2001:HLS

[Riv01]


Rubin:2000:KVL


Rubin:2001:SCR


Rugg:2004:CMV


Rupp:2009:CAC


Mark S. Schmalz et al., editors. *Mathematics of*
REFERENCES


Saini:2002:JMD


Saeednia:2002:IBS


Sakamura:2001:GEI


Sale:2000:CGL


Sale:2000:CBP


Sale:2001:GRT

Tony Sale. General report on Tunny: The Newnary
REFERENCES


Salus:2001:CA [Sal01b]

Salomon:2003:DPS [Sal03a]

Salus:2003:BRBb [Sal03b]

Salomon:2005:CDC [Sal05c]

Sale:2005:R [Sale05a]

Sallee:2005:MBM [Sal05b]

Salomon:2005:F [Sal05d]
David Salomon. Foundations of computer security. Springer-Verlag,


\[\text{Sarkar:2002:FCM}\] Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung \[\text{Yun02a}\],
Sasse:2007:REB


Satoh:2006:DPI


Savelli:2004:NDC


Savage:2005:IPW


Savage:2005:IPWh


Soto:2000:RT


Shacham:2001:ISH

REFERENCES


Scott:2004:CP


Stoklosa:2005:CIC


Stallings:2007:CSP


Sherwood:2005:MTR


Steiner:2001:SPB

[SBG02] Fabrizio Smeraldi, Josef Bigun, and Wulfram Gerstner. Support vector features and the role of dimensionality in face authentication. Lecture

Shehab:2005:SCM


Shehab:2007:WSD


Shaikh:2009:SAU


Steinfeld:2002:ASA


Seredynski:2004:CA


Syverson:2001:LAP

Paul Syverson and Iliano Cervesato. The logic of au-
REFERENCES


REFERENCES


[Sch00d] Bruce Schneier. Secrets and Lies: Digital Security in a
Schneier:2000:SRF


Scharinger:2001:ASK


Schindler:2001:ATA


Schmalz:2001:MDI


Schneier:2001:FSE

Schnorr:2001:SGH [Sch01e]


Schnorr:2001:SDE [Sch01f]


Schultz:2002:GBC [Sch02]


Schneier:2003:BFT [Sch03]


Schmalz:2004:MDIa [Sch04a]


Schmalz:2004:MDIb [Sch04b]

Mark S. Schmalz, editor. Mathematics of data/

Schneier:2004:SA [Sch04c]

Schultz:2004:GBC [Sch04d]

Schmalz:2005:MDI [Sch05a]

Schneier:2005:AE [Sch05b]

Schneier:2005:TFA [Sch05c]

Schramm:2006:AMS [Sch06a]
Kai Schramm. Advanced
REFERENCES


Schroeder:2006:NTS


Schneier:2007:NCS


Schneier:2008:SS


Schmeh:2009:VBF


Su:2005:IBT


Schmeh:2009:VBF

Scott:2004:CIB


REFERENCES


References


REFERENCES


Sennewald:2003:ESM

Sergienko:2006:QCC

Sutherland:2008:AVO

Shumow:2007:PBD

Simka:2006:MTR

Sakr:2007:RCB
Ziad Sakr and Nicolas D.

**Sutton:2007:FBF**


**Steinwandt:2000:WHS**


**Steinwandt:2008:GEI**


**Sauvage:2009:ERF**

Laurent Sauvage, Sylvain Guilley, and Yves Mathieu. Electromagnetic radiations of FPGAs: High

[Storer:2009:PSR]


[Stone:1998:PCC]


[Shailer:2001:PMT]


[Shirase:2005:AEC]


[Shamir:2001:NDC]

REFERENCES

0558/papers/2162/21620159.pdf.


[Sha03b] Adi Shamir. Turing Lecture on cryptology: a status report. World-Wide Web slide presentation, video, and audio,


REFERENCES

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

Shao:2005:SMD


Hwang:2009:KDB


Shepherd:2001:CDC


Sung:2007:CIB


Shim:2005:LPG


Shih:2008:DWS

Sierra:2004:LCC

Shimizu:2007:CBE

Shoup:2000:CTU

Shoup:2000:UHF

Shoup:2001:OR

Shoup:2005:ACC

Shoup:2005:CIN


Shparlinski:2001:UDR


Shparlinski:2002:SMS


Shparlinski:2003:CAA

Igor E. Shparlinski. Crypt-


REFERENCES

Shyamasundar:2002:ACP


Silverman:2001:CLI


Silverman:2005:ECC


Simon:2002:CRE


Singh:1999:CBE


Singh:2000:CBE

[Sin00] Simon Singh. The code book: the evolution of secrecy from Ancient Egypt to quantum cryptography. An-

**Singh:2001:DPK**


**Singh:2000:SSS**


**Singh:2002:CBH**


**Sinkov:2009:ECM**


**Stubblefield:2004:KRA**


**Sivonen:2006:MPF**

Six:2005:HGS


Schnorr:2000:SSE


Sucurovic:2005:JCX


Schaumont:2009:GEI


Song:2000:TPA


Seki:2001:DCR

Stojanovski:2001:CBRa

Sklavos:2003:DDR

Stavrou:2005:CAS

Stabell-Kulo:2006:ESC

Saldamli:2007:SME

Shu:2009:RCA
REFERENCES


K. Srinathan, M. V. N. Ashwin Kumar, and C. Pandu

Sugita:2000:RAD


Scharwaechter:2007:AAE

REFERENCES


REFERENCES

**Su:2005:KPK**


**Sung:2000:PSS**


**Shi:2005:HEC**


**Salido:2007:EBE**


**Shen:2003:SET**


**Song:2001:DWF**


[SM00b] Palash Sarkar and Subhamoy Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In Bellare [Bel00],
REFERENCES


REFERENCES


Smith-Miles:2008:CDP


Smart:2001:CDF


Smart:2003:ACU

Nigel P. Smart. Access control using pairing based cryptography. In Joye [Joy03b], pages 111-

Smart:2003:AGR


Smart:2005:CCI


REFERENCES

Seamons:2009:IPS

Satoh:2001:CRH

Strembeck:2004:IAE

Schlager:2007:EAA

Sakai:2000:NDS

Srinathan:2004:OPS
K. Srinathan, Arvind Narayanan, and C. Pandu Rangan. Optimal perfectly secure


Shelfer:2002:SCE


Sumii:2003:LRE


Solachidis:2004:WPL


Schielzeth:2005:RQN


Shahruz:2002:DNC


Standaert:2006:SSE


Singaravelu:2006:RTC

[SPHH06] Lenin Singaravelu, Calton Pu, Hermann Härting, and
REFERENCES


Sun:2008:BWN


Stern:2002:FAP


Song:2001:ANL


Shin:2000:ANT


Springer:2003:BRB


Sanchez-Reillo:2001:IBA

Raul Sanchez-Reillo. In-


Stubblebine:2001:AAF

Seznec:2003:HUL

Swiderski:2004:TM

Seddik:2009:IWB

Shi:2008:UAU

Susilo:2000:NEF
Willy Susilo, Rei Safavi-Naini, Marc Gysin, and Jennifer Seberry. A new and efficient fail-stop signature scheme. The Com-
REFERENCES


[Scambry:2006:HEW]

[Scambry:2006:HEW]

[StPierre:2000:TFA]


Mark Stamp. *Information security: principles and practice*. Wiley-Interscience, New York, NY,
REFERENCES


Sterlicchi:2000:SCD [Ste00]


Steinwandt:2001:LTP [Ste01]


Stefanek:2002:ISB [Ste02]


Steele:2005:PPT [Ste05a]


Steil:2005:MMM [Ste05b]


Stern:2005:MLF [Ste05c]

REFERENCES

htm; http://csdl.computer.org/dl/mags/mi/2005/01/m1006.pdf.

Stein:2008:ENT

Stinson:1995:CTP

[Sti95]

[Sti06a]

[Sti06b]

Stinson:2001:C

[Sti01]

Stinson:2002:CTP

Stieber:2006:OH

Stieber:2006:GH

Stinson:2006:CTP

Shimoyama:2002:MLC
Takeshi Shimoyama, Masahiko Takenaka, and Takeshi

[Str01b]

Stone:2001:CI


[Sto01]

Struif:2001:UBU


[Str01a]

Strunk:2001:JQJ


[Str01]

Stytz:2004:BR


[Sty04]
REFERENCES


REFERENCES

**Sun:2005:UMS**


**Seidl:2008:FOV**


**Shaltiel:2008:HAP**


**Sebe:2007:SMO**


**Shmueli:2009:DEO**


**Smith:2000:CIR**


**Schneier:2000:PCF**

REFERENCES


REFERENCES


Shujun:2001:PRB


Seo:2001:CDA


Shi:2001:NSF


Sun:2006:PBA


Syed:2000:CLA

REFERENCES

Sun:2005:CSS


Syverson:2002:FCI


Steinfeld:2001:ALE


Skoudis:2003:MFM


Shimoyama:2002:BCS

REFERENCES


REFERENCES

/Tattersall:2005:ENT


/Trichina:2001:SCH


/Tistarelli:2002:BAI


/Tao:2000:ITF


/Tsai:2001:GSI

Tsaur:2005:EAS


Tsai:2002:SMS


Trudel:2003:DSE


Teepe:2006:PPA


Todd:2001:LSS


Terai:2008:BRB

REFERENCES

//doi.acm.org/10.1145/1360443.1360446. See [WK01, Wel05].

Thorsteinson:2004:NSC


Theoharidou:2007:CBK


Tirkel:2001:UWE


Tabatabaian:2001:NSP


Tippett:1927:RSN


Torres:2007:ANS

Joaquin Torres, Antonio Izquierdo, and Jose Maria Sierra. Advances in network smart cards authentication. Computer Networks (Amsterdam, Netherlands: 1999), 51(9):2249–2261, June 20, 2007. CODEN ????? ISSN
References

Tseng:2001:GGO


Tseng:2001:CLB


Tseng:2003:DSM


Tico:2003:RAS


Toll:2008:CSE


Thien:2002:TSS


Thomas:2007:HQU


Turner:2006:SIS


Tsai:2005:CAE


Tang:2006:CHA


Torrubia:2001:CRC

Tian:2005:RWS


Tsolis:2009:ARM


Teoh:2004:PCK


Tousidou:2000:IMS


Tanaka:2001:QPK


Tochikubo:2000:RAE


Tsai:2008:EMS


Tseng:2007:SAG


Takano:2000:PTH

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

Tsunoo:2003:CIC


Tahir:2000:RCM


Tzeng:2001:PKT

Tian:2001:ICE

Tuchman:1966:ZT

Turing:2004:BS

Tiri:2003:SEA

Toft:2001:LTT
George Toft, Hugo van der Kooij, Mick Bauer, Chris Hendrickson, Stephanie Black, Adrian Ho, Markus Hogger, Ian Abbott, and Robin Rowes. Letters: Tech tipsy; awkward solution; Mandrake 7.2 review;


Mohit Tiwari, Hassan M. G. Wassel, Bita Mazloom, Shashidhar Mysore, Frederick T. Chong, and Timothy

**Thamrin:2008:PBR**


**Tzeng:2004:NTM**


**Ting:2002:FBS**


**Tynan:2005:CPA**


**Tian:2005:NDF**

REFERENCES


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

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

[Uni00b] United States Congress.House
Committee on Armed Ser-
vice.
U.S. encryption policy: hearing before the
Committee on Armed Ser-
vices, House of Repre-
sentatives, One Hundred
Sixth Congress, first ses-
tion: hearings held July 1,
13, 1999. Washington, DC,
H.A.S.C. no. 106-16.

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

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

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

United States Congress.House
Committee on International
Relations. Subcommittee on
International Economic Pol-
icy and Trade. Encryption


[Uri01] Pascal Urien. Programming Internet smartcard with XML scripts. Lecture
REFERENCES


USENIX:2000:PLI


USENIX:2000:PFW


USENIX:2000:PFSa


USENIX:2000:PNU


USENIX:2001:PUA


USENIX:2001:PFT

[USE01b] USENIX, editor. Proceedings of the...


REFERENCES


[UUW00] Lars Ulfving and Frode Weierud. The Geheimschreiber secret. In Joyner


Vadhan:2003:CLC

Vanstone:2003:NGS

Vaudenay:2005:PKC

Vaudenay:2002:SFI

Vaudenay:2001:DID
REFERENCES


vanDijk:2004:AOC


Verheul:2001:EXM


Vercauteren:2002:CFZ


Vergnaud:2006:RBS


Vernitski:2006:CUM


Vladimirov:2004:WFS


Vo:2008:SMA


Volos:2009:IEP


Viega:2002:NSO


Viega:2003:SPC


Vasco:2005:NCS

REFERENCES


Voyiatzis:2008:SFS


vanTilborg:2000:FCP


vanTilborg:2001:ECC


vanTilborg:2005:ECS


Vaudenay:2007:POK


Venkatesan:2001:GTA

REFERENCES


REFERENCES

[Wang:2004:TVS]


[Wardlaw:2000:RPK]

[Washington:2008:BRB]

[Washington:2008:ECN]

[Wayman:2001:FBA]

[Wayman:2002:BAT]

[Wayner:2002:DCI]
Peter Wayner. *Disappearing cryptography: informa-
REFERENCES

Wayner:2009:DCI

Wayner:2009:DCI

Wu:2002:CSCa

Wu:2001:CDS
REFERENCES


REFERENCES


REFERENCES


[WD01b] Williams:2001:ICA


[Wea06] Weaver:2006:BA


REFERENCES


[WG00] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam.

**Wu:2002:CAE**


**Wu:2002:IBM**


**Wu:2003:TSS**


**Wang:2009:NWM**


**Wen:2005:URE**


**Wu:2008:RPG**

 REFERENCES

Watanabe:2001:EAP

White:2009:EOD

Wu:2003:IMT

Wang:2005:EAS

Whyte:2005:TFC
REFERENCES

Wiener:2000:AAH


Williams:1999:QCQ


Wilco:2001:SEH


Wilson:2001:PBA


Williams:2006:C


Winterbotham:2000:USI


Wincelberg:2001:JQH

REFERENCES

Windley:2005:DI


Winkel:2005:GEC


Winkler:2005:SAU


Withers:2001:IWU


Wang:2005:VBW


Welschenbach:2001:CCC


Wang:2005:ECSb

[WK05] Chih-Hung Wang and Yan-Sheng Kuo. An efficient contract signing protocol using the aggregate signature scheme to protect signers' privacy and promote reliability. Operating Systems
References


Won:2006:ISC

Weigold:2008:RCA

Walter:2003:CHE

Wang:2002:AAB
REFERENCES


REFERENCES

Wang:2009:DSM

[WLZ05]

Wong:2004:RCK

Wang:2005:TSP

Wu:2005:IAW
Wu:2008:RWM


Watters:2008:VDL


Wheeler:1995:TTE


Watanabe:2002:CCD


Wang:2008:NAD


Wang:2009:RD


Wolkerstorfer:2001:AIA

Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger. An

**Wolfe:2003:EE**


**Wollinger:2004:SHI**


**Won:2001:ISC**


**Wool:2000:KME**


**Wang:2003:SGP**

REFERENCES


Wollinger:2005:CVH


Weimerskirch:2001:ECC


Wang:2001:TUR


Wright:2000:IQC


Wright:2001:AES

Wright:2003:FCI


Wrixon:2005:CCO


Wang:2002:IPD


Wright:2002:EPS


Whiting:2003:MPH

REFERENCES

Walter:2005:DDP [Wu02]


Weimerskirch:2002:DLW [WT02]


Wuensche:2009:CAE [Wue09]


Wu:2000:PKC [WV00]


Wu:2001:DSM [Wu01]


REFERENCES


[Wang:2006:SPS]

[Wang:2008:DCP]

[Wu:2001:CFF]


[Wollinger:2000:HWH]
REFERENCES

gov/encryption/aes/round2/ | [WY02]

Wincelberg:2002:LIE


Wang:2008:HQS


Wang:2002:WEM


Wang:2002:APK

REFERENCES


Wyler:2005:ANS

Wang:2005:CSA

Wang:2005:FCFb

Wang:2005:ECSa

Winslett:2005:PLD
REFERENCES


REFERENCES

issn=0302-9743&volume=2612.


Xiang:2008:CPA


Xie:2004:CTA


Xu:2009:AVB


Yan:2000:NTC


Yang:2002:NEC


Yang:2005:TFN


Yan:2007:CAR


Yasuda:2008:DLP

Yuan-bo:2004:ITA


Yue:2001:GNN


Yue:2007:SEV


Yiu:2008:ODC


Yang:2009:ETP


Yang:2009:IBR

REFERENCES


REFERENCES


Yang:2005:IME


Yamamura:2000:QCB


Yamamura:2001:EDA


Yi:2004:AKA


Yen:2000:CBO


Yen:2002:CAO

[YKLM02b] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon. RSA speedup with residue number system immune against hardware fault cryptanalysis. Lecture Notes in Computer Science, 2288:397–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL:


REFERENCES

Yi:2009:SSG


Yu:2005:EHI


Yoo:2002:LAU


Yurkewych:2005:CIR


Yue:2006:NCB


Young:2001:RP

REFERENCES

Youssef:2001:CAF


Young:2006:MCC


Youn:2008:WRB


Yang:2009:AIO


Yin:2001:RMW


Yilek:2009:WPK

Yo:2004:SUA


Yo:2005:CFI


Yo:2005:ICJ


Yeh:2002:SAK


Yeh:2004:PBU

Her-Tyan Yeh and Hung-

Yanami:2002:DLC


Yeh:2003:IAM


Yang:2001:EEA


Yoshiura:2001:AWB

Yao:2009:CAR


Yang:2004:ENT


Ytrehus:2006:CCI


REFERENCES

Yang:2008:VCS


Yang:2008:FSD


Yang:2005:SAS


Yang:2008:TFM


Yang:2009:CLW


Young:2000:RBA

Adam Young and Moti Yung. RSA-based auto-recoverable cryptosystem. *Lecture Notes in Computer Science*, 1751:326-
REFERENCES


[YY01:GEC] Lin You, Yi Xian Yang, and


Zhang:2005:ITA


Zivkovic:2005:AH


Zhao:2005:SSV

[ZBP05] Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. In ACM [ACM05a], pages 1–6. ISBN 1-59593-269-0. LCCN ????
REFERENCES

Zhang:2009:CII


Zhang:2001:SOS


Zhu:2004:DSM


Zunino:2005:WPE


Zhao:2006:SAP


Zeadally:2000:IPQ

[S. Zeadally. Implementation and performance of...

**Zhang:2005:CSS**


**Zhang:2005:AES**


**Zou:2005:MED**


**Zhang:2000:WMH**


**Zha:2006:NDN**


Zhong:2006:ESC

Zirkind:2007:ADC

Zhang:2004:BAF

Zhang:2009:IBR
REFERENCES


REFERENCES

Zhang:2005:DMC


Zhang:2005:RPE


Zhou:2005:MBI


Zhou:2005:APS


Zhang:2003:FSP


Zafeiriou:2005:BRW


Zhang:2005:ISS


Zhang:2005:SCA


Zhao:2002:EII

REFERENCES

Zhu:2002:PAK


Zhang:2001:USC


Zhang:2004:NMS


Zhou:2003:ACN

Zhang:2005:ASP

Zhang:2005:ISM

Zhang:2008:FIC

Zeng:2001:CHR

Zhu:2007:EIB

Zhuang:2005:KAE
QA76.9.A25. ACM order number 459050.