Title word cross-reference

#1 [Man01, RSA02]. #10 [RSA00b]. #11 [RSA01, Chu03]. #13 [RSA03b]. #15 [RSA00d, RSA00c]. #9 [RSA00e].

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p_k)
[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LYL2001, YCH04, CLT07]. (tn)
[PW05, SC05a]. + [Abe01]. {0, 1}
[LBGZ01, LBGZ02]. 1 [Wu02]. $\text{\$125}$
[And04]. 128 [AKI+01, PCG01]. 13
[HSLT02]. $\text{\$15.00}$ [Imr03]. 2
[Bih00, BGN05, CY02, CLK+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 [Eva09].
2000 ± 10 [Mau01]. $2^{28}$ [Bih02]. $2^k$
[MFFT05]. $2^n$ [KLY02, KKY02]. 3
[BP04, Ben00, ChLYL09, CT09, DVP09, Lav09, OMT02, WH09, ZTP05]. $\text{\$35.00}$
[Top02]. $\text{\$49.99}$ [Gum04]. $\text{\$5}$ [SCF01]. 5
[Pat04]. $\text{\$51.48}$ [Pap05]. 512 [CDL+00]. 7
[Gri01, Pat03a]. (2,128) [WB02]. 0 [AIK04].
[ABC] [PS04b]. a [BD00b]. E_0 [FL01a]. f_8
[KSHY01]. g^{x^2} [Shp02]. g_c(x, 1) [SZP02].
GF(2) [CP03]. GF(2^n) [OTT01, RMPJ08].
GF(p^n) [BGK+03]. GF(p^t) [PZ01]. H_2A
[CB05]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. 1 [QPV05]. M + 1
[AS01a]. F_q [CY02]. Z^n [Gro05]. GF(2)
[GS03, KTT07]. GF(2^n)
[BBGM08, KTT07, KWP06, RMH03a, RS04].
GF(2^n) [KKH03]. SL_2(F_{2^n}) [SGGB00]. μ
[LN04]. n
[CT08b, Gon06, HKS00, LKLJ01, TM01].
n = pq \ [KOMM01]. N^{0.292} \ [BD00b]. NC^0
\ [AIK06]. \ p \ [FL06]. \ p^q \ [LYL00]. \ p^x
\ [CHH01]. \ Q \ [Yas08]. \ r \ [JY01]. \ w
\ [DwWmW05, OT03b]. \ x^v \ [Gon06]. \ y \ [OS01].
Z_n \ [LWL09].

-Adic \ [GHK^+06]. -Bit
\ [AIK^+01, CDL^++00, PCG01]. -Connected
\ [BJLS02]. -Coordinate \ [OS01]. -coverings
\ [SC02b]. -D \ [DVP09]. -decompositions
\ [vDKST06]. -DNF \ [BGN05]. -Metric
\ [LBGZ01, LBGZ02]. -NNAF \ [DwWmW05].
-out-of- \ [CT08b]. -Polynomials
\ [FL06, CHH01]. -Round
\ [BP04, Bih00, GIKR02, CKL^+03]. -Source
\ [KLR09]. -st \ [AS01a]. -Steiner \ [WL02].
-Threshold \ [CLT07, Kog02]. -way
\ [LKJL01]. -Year-Old \ [Eva09].

.NET \ [For04, TG04].

/dev/random \ [BH05]. /evolution
\ [Pat02a]. /MOM \ [DJI01].

0 \ [And04, BC04a, Gum04, Imr03, Puz04, WYY05d]. \ 0-07-222742-7 \ [Gum04].
0-13-100851-X \ [For04]. \ 0-226-74410-8
\ [Top02]. \ 0-262-14075-6 \ [Pag03].
0-321-20217-1 \ [Puz04]. \ 0-385-49532-3
\ [Imr03]. \ 0-470-84402-7 \ [And04]. \ 024-Bit
\ [GS07a]. \ '05 \ [ACM05c, MS05b, ZC09]. \ '07
\ [ACM07]. \ '08 \ [ACM08]. \ '09
\ [AC09, IEE99a].

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].
10118-3 \ [ISO04]. \ 106
\ [Uni00c, Uni00d, Uni00g]. \ 106-1
\ [Uni00c, Uni00d, Uni00g]. \ 108-bit \ [Bar00a].
109-bit \ [Pru00]. \ 10th \ [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. \ 11-15
\ [AUW01]. \ 11th \ [CCMR05, HYZ05b, HH04, HH05, RM04, Roy05, USE02b]. \ 12 \ [TPS01].
128 \ [JJ02, WFLY04]. 128-Bit \ [SM03b].
12th \ [GH05, MS05b, PT06]. \ 13-15
\ [ACM05b]. \ 130 \ [LM08]. \ 14th
\ [AMW07, AAC^+01, Bir07]. 150-Kilometer
\ [Das08]. \ 155 \ [LMP^+01]. \ 15th \ [MJ04, BC01].
160 \ [KSF00]. 16th \ [BS03]. \ 17th \ [IEE05b].
186 \ [Nat00]. 186-2 \ [Nat00]. \ 18th \ [KM07].
19005-1 \ [ISO05]. 192-bit \ [Luc00]. \ 1930s
\ [Bur02]. \ 1945 \ [Ban08]. \ 1960s \ [Bur02], 1962
\ [AJ08]. \ 1887 \ [Kha05]. \ 1993 \ [PPV96].
1999 \ [Lee03b, Uni00a, Uni00b, Uni00f, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Uni01].
19th \ [BCDH09]. \ 1V \ [CGB05].

2 \ [Nat00, SK05a]. \ 2.0 \ [Cor00a]. \ 2000
\ [CGH^+00b, Eke02, Irw03, KH08, KI01a, Sch00b, Wit01, YG01c]. \ 2001
\ [ACM01a, BC01, GJS01, Lee03a, Pen01b].
2002 \ [B^++02, IEE02, RSA03a, Yun02a]. \ 2003
\ [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA^+03, WKP03]. \ 2004 \ [ACM04b, ZC04].
2005 \ [ACM05a, ACM05b, ACM05c, ANS05, HYZ05b, ISO05, Roy05, Ter08, Ytr06]. \ 2006
\ [ACM06]. \ 2007 \ [ACM07, Ano06b, SM07b].
2008 \ [ACM08, Dew08, YRS^+09]. \ 2009
\ [ACM09, May09]. \ 20th \ [Bel00]. \ 21 \ [AJ01b].
21264 \ [WB00]. \ 21st \ [Jef08, KI01a]. \ 21th
\ [IEE09a]. \ 22 \ [McK04, TTZ01]. \ 22nd
\ [Yun02a]. \ 23rd \ [Bon03]. \ 24th
\ [Cra05a, Fra04]. \ 256-bit \ [Luc00]. \ 25th
\ [Sho05a]. \ 26 \ [DB04]. \ 26th \ [EBC^+00]. \ 27th
\ [Men07]. \ 29, \ [Eke02]. \ 29th \ [FLA^+03].

3 \ [Duw03, Imr03]. \ 3-515-07640-9 \ [Eag05].
3-540-66778-4 \ [Duw03]. \ 3-Key
\ [Kel05a, Kel05b]. \ 3.0 \ [Flu02b, Hei01, SQ01].
305 \ [ECM00a]. \ 306 \ [ECM00b]. \ 30th
\ [Coc02a]. \ 314pp \ [Duw03]. \ 3278 \ [BWBL02].
33rd \ [ACM01a]. \ 36th \ [ACM04b]. \ 37th
\ [ACM05c]. \ 39th \ [ACM07]. \ 3D \ [LZP^+04].
3GPP [KSHY01, SM02]. 3rd
[ACM05a, USE00a].

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, KKKP02, 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 [Blao3,
Des02, HA00, JQ04, LL04d, MMV06, Oka00].

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

8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800
[BG07a, Hir09]. 800-90 [BG07a, Hir09].
802.11b [SIRO4]. 802.11g [Coc02a].
802.11i [HSD+05]. 802.15.4 [Mis08]. 82
[Kwo03b]. 8th [Chr01, Hon01, Jae04, Mat02,
MP02, Vau05a, WK06, Zhe02b].

9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04].
90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1
[GM00b]. '98 [Wi99]. '99 [DN00b]. 9th
[CCMR02, CSY09, DR02c, DKO05, Lai03,
NH03, Pat03b, PY05, YDKM06].

A-1 [ISO05]. A.2.4 [Keo5a, Keo5b]. A5
[BD00a, BSW01, PS01c]. A5/1
[BD00a, BSW01, PS01c]. AAFG1 [Hug02].
AAs [LOP04]. Aarhus [Cra05a]. Abadi
[MW04]. Abelian [CF02, PHK+01, RS02].
Abstention [JLL02]. Abstract
[CM00, Cou04, DR05, HLvA02, HJW01,
JL00, MSJ02, MP02, Mas04, Wag02, BJN00,
BCD00, CD00a, CC04c, FKS+00, GHJV00,
GTV04, HT04, Iwa08, IK00, Jon08,
KKS00a, KM00, LM08, Mes00, Pe09, Yas08].
Abstracting [Blao1, Mon03]. abstraction
[BLP06]. abstractions [BG07b]. Abstracts
[Sch00b]. Accelerated [Elb08].
Accelerating [ESH+05]. acceleration
[EHKH04]. Accelerator
[CGBS01, RS04, TS00, XB01, DPT+02].
Acceptance [CFRR02]. Access
[ANRS01, An02e, BNPW03, CGMM02,
DS06, HC08, MS03b, Sm03a, Sm03a, Sun00a,
ZGLX05, AW05, AW08, AFB05, BA06,
BN08, Che08b, DFM04, H006b, H003c,
HY03, JY06, JY06, KNS05, LKZ+04, MF07,
MSP+08, PS02a, ST07, W01, WC01b,
You04]. access-control [BN08].
accessible [Pau02a]. accountability
[WABL+08]. Accounting [Lai08].
Accumulator [GTH02]. Accumulators
[CL02a, accurate [Z08]. Achieve
[CFS01]. Achievement [Coc01a].
Achievements [VK05]. achieving
[PS04c]. ACISP [YG01c]. ACM
[ACM01a, ACM03a, ACM03b, ACM03c, ACM05b,
ACM05c, ACM06, ACM07, ACM08, ACM09,
ACM10, MS05b, Ba06, MBA02, RA06].
ACNS [GKS05, IY05, JY04, ZY03].
acoustic [ZLT05]. Acquiring [SET08].
across [Dav07, ZBLvB05]. Act [Kha05,
Uni00a, Uni00c, Uni00d, Uni00g, Uni00h].
Actel [DV08]. Action [SE01]. Active
[BC05a, BAC05, BP02, L05, MA00a,
MA00b, T02, BPS08]. Active-Content
[MA00a, MA00b]. activities [AJ08, SN07].
actually [Hau06]. Ad
[BSS02, KH05, W02, Cha05b, DHMR07,
KVD07, LHC08, LKZ+04, PSM07, SLP07,
TW07, ZC09, MA04]. 'ad-Durayhim’s
[MA04]. Ad-hoc
[BSS02, W02, DHMR07, ZC09].
Adaptation [SSZ08]. Adapting [MD01].
Adaptive
Adaptively [AF04b, CHK05, FMY02, JL00].
Adaptively-Secure [CHK05]. Added [Ano02b, St.00]. Adding [FBWC02].
Addison [Puc03]. Addition [KT00, LPZ06, PP06a]. Additive [FMY01, MF01].
Additive-Sharing [FMY01]. Address [IIT03, Nik02a, Nik02b, FXAM04, RW07].
Address-Bit [IIT03]. Addressing [HTW07]. Adi [Coc03]. Adic [GHK+06].
adjacent [JT01b]. Adjustment [BSNO00]. Adlan [MAaTxx]. Adleman [BB79, Coc03, SP79].
Administration [USE00c, USE00a, Ris06, WL04a]. administrative [Cra05b]. Admitting [HSZI00].
Advance [CZB+01]. Advanced [CF07, DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Swe08, Tan01, Ase02, Bar03c, III00, Bur03, CM06, Coc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sve00, WBRF00, Wri01, YW06]. Advances [Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS07, ELvS01, Kl01a, Oka00, Pfi01, Pre00, TIS07, Yun02a, Kat01, Bih03, CCC04a, Cra05a, Fra04, Kru02, Lee04b, LTT+04, L05, 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, EYCP00, Elb08, Fer06, FM02b, GC00a, HW03b, IBM00, IK00, IK01, Jh00, KS09a, KEl05a, Ker05b, KFSS00, KV01, LP02a, Len01, MMH+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03b, RRY00, SKKS00, SM03b, Sch00b, SKW+00, SW00a, SL00, WW00, WB00, WLO01, WWGP00, WWCW00]. AES-CBC [Fer06]. AES-like [DLP+09]. AES-related [Sch00b]. Affine [Ben00, CT09, Fel06, HH09].
Affine-Transformation-Invariant [CT09]. AFIS [Zir07]. African [WD01b]. after [Ber03, McL06], again [Fox00]. Against [CS05b, DM07b, FKW00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, Av03, Bau05, BPR00, BP02, BB09, BB09, BGM09, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egh00, EBS01, FP01, Fry00, Geb04, HNIZ02, HLL+01, HG07, Hau05b, HLC08, In05, IWS03, IIT03, JK02, JJ00b, JT01a, Kan01, KM02, KLM+02, LM08, LPV+09, Lu02, Mri00, Mlo02, MG08, NRR00, NDS06, OS06, OT03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PQ03b, RS01, SKQ01, Sch01b, Sch01f, SDF00, SDF01, Sen00, Sho00b, SKU+00, SK01, SLL+00, Tad02, TV03, VHP01, XH05, Y00, YKLM02a, YKLM02b, YKLM03, ZCW04, ZSJN07]. Age [Mar08b, Lev01]. Agency [AJ08, Bam02, Kov01]. Agent [HQ05, KC02, PZ09, RS01, RC01, Rot01, ZMV05, KX00, SS0+08, SH00]. Agent-Based [HQ05, SS0+08]. Agents [WH01, Haut06, LSA+07]. Ages [Eag05, Kin01]. Aggregate [BGLS03, WK05]. Aggregated [ZSN05]. Aggregation [Her06, CCM07, MS09b]. Aggressive [Wyl05]. AGM [Gau02]. Agreement [AAG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB+04, AKNR04, CYY05, CYH05, etc.].
agricultural [Lov01]. Aided [NS01b, HLL +02]. Aim [Pau02a]. Aimed [SFDF06]. Airport [Sas07]. Airwaves [Dav07]. Ajtai [GK05]. Al [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx]. al-fusul [MAaT05]. al-Ka [MAaT07]. Al-Kindi [MAaTxx, MAaT03, MAaTxx]. al-mutargima [MAaT05]. Alan [Pet08]. Alcatraz [LSVS09]. Alchemy [Pag03]. alert [AJ08]. alerts [NCRX04]. Alexandria [MS05b]. Algebra [Cou01, CD01a, Lan04a, CKY07, Fau09, HW03a, HWR09, Sho05b]. Algebraic [AK03, Bar09, Can06b, CMR06, CM03, Cou03, CFS05, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mas04, MNP01, MR02a, MR02b, PDMS09, Bul09, CKN06, CDL06, Iwa08, May09]. algebraically [RBF08]. algebras [BDFP02]. Algorithm [ANS05, AEMR09, Bar00a, Bar00c, BSC01a, ChLYL09, CU01, CJ03a, CJS01, CTLLO1, CG03, CC06, CH07e, CKM00, CT03, CP03, DR01, DGO0, Dhe03, EYCP00, FWB01, FMS01, GMM01, HTS02, HM02c, HZSL05, JK*K01, KB03, KMM*K06, KY02c, KLT02a, KTT07, KV01, LPZ06, MM01b, MM01c, MS02e, NMSK01, OS01, PZLO9, PBTW07, RAM01, RS01, SS01a, SPGQ06, WHLH05, Wes01, Wie00, AJ08, App05, BF06a, Bla00, CO09a, CH01, CKY05, CYH+07, CHH01, FP09, Fer06, FSGV01, GPX08, Jon08, KJ01, Kwo02, Kwo03b, LCP04, LLLZ06a, LLLZ06b, MN14, OS07, SH11, SCS05a, SM08, SZP02, TM01, WL02, WN95, Wue09, YRY05c, And03, SA02]. Algorithmic [Hro09, Jou09, Has01b]. Algorithms [Hro03]. Algorithm [AD07, Ano09d, AB09, BKLS02, III00, BWBL02, CPhX04, CLR01, Dam07, DWN01, FW09, Gau02, GL06b, Har06, Har00, Int00, JP03, Kel05a, Kel05b, Lee03b, LR07, LP02b, PBB02, Pre02a, Pre02b, SL00, TLYL04, TV03, WBRF00, WWGP00, AHK03b, Ano01n, AH05, CKL*K09, CCM01, GHPT05, GPC08, HW03a, HWR09, HH06, Hro05, JK01a, MCHN05, Pre07, Rh03, TC05, XLM06, ZLZS07, Ziu07, dH08]. Alien [Wil01b]. All-or-Nothing [Des00c, SR00]. Alley [DR01, Wi00]. Alliance [An004e]. Allied [Hau03, Hau06]. Allocation [CCM05, LZ09]. Allowing [JLL02]. Almost [AP09, BS00a, Jut01, Mar02b]. Alpha [WB00, Wu02]. Alphai [KHD01]. Alternating [Wer02, HKPR05]. Alternative [Bad07, Gar03a, Han00, BMW02b]. always [BB79]. am [Eke02, SU07]. Amalfi [BC05c, CGP03]. Amenability [WW00]. America [DB04]. American [GL05, Kat05b, Al00, Na05]. Americans [WD01b]. among [BN00a, KT00, SKU +00, Win05c]. Amongst [Pen01b]. Amplification [CHS05, LTW05, RK05, SV08b]. Amplified [KKS00a, KKS01, KML+02]. Amplifier [Pl01]. Amsterdam [Knu02].
Asymptotically [vDW04]. Asynchronous [CKPS01, FML+03, KSR02, SKR02, ZSV05].
at-targama [MAaT05]. Atlanta [IEE09b].
ATM [Pat02a, Pat02b, Zaa00]. Atomic [CNV06]. Attached [RCBL00].
Attachments [Ric07]. Attack [Ahm08, CKQ03, CS05b, Des06b, Fil00, FV03, GHJ0v0, GHJV01, HQ01, Hug02, HW01, J00b, KCP01, KS00a, KML+02, KM01c, LY07, LNL+08, LV04, LMV05, L02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, PQ03b, RMS05, SG09, Sho0b, Sho0b, Sma03b, VHP01, YKLM02a, ZC04, ASK05, Ade09, An009c, DKL+00a, Duj08, Duj09, GM00a, HAu04, He04b, 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, BBB+02, BDK+09, Bu02, BM03b, BGM09, BCP02b, BM01c, Can06b, CS07b, CZ03, CT08a, CJ01, CKM00, CJNP00, CM03, Cou03, CWR09, CD01b, DVP01, DFS04, DJ06, DS08, DM07b, FKSW00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GKO2, HSH+08a, HNZI02, HR04a, HSH+01, HLC08, ISW03, JKS02, J00d, KS00a, KS00b, KKS01, KCI+01, KI01a, Law09a, LLS05a, LWS05, L05b, MOP06, MP06, MF01, Mc04, Mes00, Mes01, M02, MG08, OT03a, OT03b, ÖOP03, OST05, Ove06, PKBD01, PDM09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZZ05, YD001, YY01, YG01b, vW01, BPS08, Bau05, BCS08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05b, HL05b, In005, IM06, JD01]. attacks [KS05a, KTC03, LPV+09, LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RG05, Sch00c, Sch01f, Sbi05, SL06, SK05b, SW00b, WL07a, WL04b, Yan07, YS02, ZSJ07].
Attitudes [FDI00, CF05]. attractors [HIY07]. Attribute [LY05, RSA00e, YI05]. Attributes [SS01b].
Auction [AS01a, An001a]. auctioning [RCG+05]. Auctions [Bra01b]. Audio [Arn01, CS05c, DRL09, MH05, WNY09, WVL+02, XZ01, WNQ08, BS01b, KJR05, KN03]. Audio- [KJR05]. Audio-and [BS01b, KN03]. Augmented [CS07c, You01]. Augmenting [AL04].
August [AMW07, Be+00, B+02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KKP02, Kil01a, KP01, MZ04, Men07, NH03, PO06, RS05, Sch00a, Sch04b, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a].
Australia [B01, IZ00]. Austria [DKU05, Pf01, Jef08]. Authentic [DGMS03, Dur01, SS01b]. Authenticate [Ban03a, Bau03b]. Authenticated [AGT01, BN00a, BPR00, Bu02, BC04b, BM01, BMM00, BCP01, CPP04, Ch08e, DG03, DA03, EP02, GKK07, GL03, GTTC03, HS07, K01, KY03, K03, Lee01, LHT09, M00, Mac01, MSJ02, MND+04, NA07, Nam02, Ng05, P01, SK00, Vau05b, WC01a, YPPK09, YI04, ZWW02, BKN04, BCP07, CY05, CYH05, Che04a, CL08, CJ04, CJL05, DG06, GL06a, GM05, HT08, HWW02, HWW03, Hsu05a, Hwa05, HL05c, HL05d, J00a, KO09, KRY05, LLM07, LKK03a, LKK03b, LL04a, LL05a, LKY05c, LKY05d, LH08, LSR02, LL06, LWK05a, Mis08, PQ03a, PQ06, RBB03, Se05, SW05a, SC05b, TLH05, TJ01a, Tse07, WHL06, WH02a, XY04, YW05, YC09a, YS02, YSH03, YRY05b, YPKL08, ZC04, ZAX05, ZW05b, ZL05].
Authenticating [AIP01, Chi08a, CGV09, Fur05, JW05, PM08, RCBL00, YSS+01, Lin01b].
Authentication [AAK09, AP09, ANRS01, An01b, An01c, An01f, An02d, AHKM02,
ANL01, BH06, BACS02, BCL^+05b, BCG^+02, BM03a, BH00a, BKR00, BCC01, BCC02, BC05b, Ber04, BDhKB09, BR02, BDFP05, BDF01b, BL03, BLDT09, BWE^+00, CV03, CGP08, CS07b, CC01b, CLK01a, CLK01b, CC05b, CC09, CJT02, CJ03d, CWY05, CT09, Cin02, Cin01, CFR02, CGK^+02, CF05, CJK^+04, Cou01, CMB^+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, FDIR00, Gan01a, Gar03a, GMW05, GSV02, GD02, GT02, Gut04c, Had00, Hsz01, HSH01, HSH06, HKW06, HY01, Hoe01, HSO1b, HP00, HL07, ISSZ08, Jab01, JP02a, JP07, JP02b, KJ05, K09b, KH05, KVD07, Km01, K02, KZ09, KS06b, Law05, Li01, LLT^+04, LL04b, LSH03b, LM00, LOP04, LHL^+08, Lys07, MW06, MM01a.

**Authentication** [Mal02, MJ04, MD04, MR03, MGC02, MNT06, Nao02, Nik02a, Nik02b, OKE02, OHB08a, PBD00, Par04, PMRZ00, PBC05, PK01, Qu01, RKZD02, Ric07, Ri02, SNWX01, SR01, Sch04c, Sch05b, Sei00b, SY01b, SBB02, Smi00, Smi01c, Smi02, SE09, Sk06, Str01b, SJ05, SYL05, SC01, TK03, TZT09a, TZT09b, Tsa01, VN04, WLL09, WC09, Way01, Way02a, Wea06, WB08, WT02, WS03, WL07b, WLT05b, WHL05, XYL09, YI01, YEP^+06, YSR01, YLLL02, YKW01, Za00, ZJ04, ZBL0b05, AvdH00, AF04a, Ali06, Ano00k, Ano00l, Ano05b, Art04, AAKD09, Asl04a, Asl04b, AL04, Ay06, Bado07, Bel04, BGP02, BSSM^+07, BFG04, BF05b, BS01b, BBG^+02, BDFP02, BF07, Cer04a, CBB05, CC01a, CCK04a, CL04d, CC04b, CCK04b, CC05c, CZ03, CY05, CCS08, CWJT01, CJ01, CJ03b, CH07a, Chi08b.]

**authentication** [Chi08c, Chi08d, CL09, CF07, Coc01a, CMD06, Da01, DSGP06, DY09a, DGK^+04, DG05, DW05, FLZ02, FC05, FGM03, Gan08, GLC^+04, GTY08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Her09b, Hsu05b, HLT09, HYS03, HLL04, HL05b, shCP09, JP06, JPL04, KJ05, KJY05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LH02, LHL03a, LF03, LKY04, LW04, LHL04a, LKY05a, LLY06, LLS^+09, LFHT07, Li05, LST^+05, LCX08, LW05a, LL06, LW04, LHL03b, LH03, LT04, LC04a, Lin07, LN04, LLW08a, LLW08b, LC05a, LC05b, Luk01, MS09c, MAB06, MCo04, Mit00, MR00, ME08b, MP07, NC09, NLD08, OHB08b, PY08, PCS03, PCC03, PI06, Pei04, Pha06, Pot03, Pot07, RFR07a, RFR07b, RFR07c, RG06, Sae00, SNW01, SG07, SN07, Sch05c, Sco04, Sei05, SBS09, Sha05c, SLH03, SSM^+08, SW06, Shi05, SL05a, St.00].

**authentication** [Ste05a, SW02, SCS05b, SC05c, SCS05c, ZS05, SY06, TM06, TBJ02, TOEO00, TIS07, TW07, Tsa08, TWL05, UBE09, VM03, VK08, Voi05, Wac05, WL03, Wan04a, WLT05a, WDL09, WDC09, WC03b, WL04b, WHHT08, XwWL08, YW04b, YW04a, YWC05, YWL05, YTWW05, YCYW07, YWWD08, YC09c, YC09b, YS04, YRY04, YRY05a, YRY05c, YRY05d, YY05b, YbJf04, ZL04a, ZK05, ZSN05, Za06, ZDW06, ZSN07, dB07, CS08b, ECM00a, ECM00b, LSH03a.]

**authenticator** [CKY07, jLC07].

**Authenticity** [AB01, Bla02a, CBD^+05, G03, GOR02b, HG03, RW03b, Sch01a, DVP09, Mit02a].

**AUTHMAC_DH** [Asl04b].

**Author** [Ano00b, Ano01d].

**authorisation** [SN07].

**Authorities** [CHSS02, HW04, WH02b].

**Authority** [Con00, JLL02, CCH05, KB09].

**Authorization** [BACS02, CJK^+04, LSW05, RKZD02, YT09, GJJ05, JE04, Lin07, LOP04, SR01, WL04a, WZB05, YbJf04].

**Authorship** [Top02].

**auto** [YY00].

**auto-recoverable** [YY00].

**Automata** [LZ04, MGC02, Wue09, Bao04, CC05d, K03, La00, LQ08, Mon03, SBZ04, SHH07, TC00, dRMS05].

**automate** [Bur02].

**Automated** [CDR01, LLW05, LLW09].
HJW05, IY05, LS05b]. Automatic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05].

Automating [Gue09]. automorphism [Pae03]. automotive [LPW06]. Autonomic [VH09, Che05c]. autopsie [Car00].

auxiliary [Dam00, DKL09]. availability [CBD+05]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03].

Average [CBD+05]. Average-case [Mic02b]. Award [RSA03a, Bar00b, Coc03]. Awarded [Coc02b]. Aware [IKP+07, OHB08a, CBSU06, OHB08b, Zea00]. Awareness [HLM03, BK05].

Away [Coc03, Ols00, Tee06]. Awkward [TvdKB+01]. Axiomatization [dH08].

B [SPK08, YG01a]. B-Spline [SPK08]. B2B [Zho02]. Babbage [Bar00a].

Back [CZB+01, KCD07, SF07, Ano00g, Dea06]. Back-End [KCD07]. Backdoors [CS07c].

Backup [Str02]. backward [HCD08a, HCD08b]. backward-and-forward [HCD08a, HCD08b]. Bacon [GG05a]. bad [BBN+09]. bail [Ano01h]. Bait [Luc02a].

Balancing [Hö01, Lut02]. Ballot [Cha04]. Baltimore [ACM05b, ACM05c, GL05].

Banach [AUW01]. Bandwidth [CG+02, YY01, SLP07].

bandwidth-efficient [SLP07]. Bandwidth-Optimal [YY01]. Bangalore [MMV06]. Banking [HKW06].

Barbara [Bel00, Bon03, Fra04, Kıl01a, Men07, Sho05a, Yun02a]. Barcode [Che08b]. Bare [DPV04].

Barren [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, XSWC10, IR02].

Based [An001c, ANR01, AF03, AJ08, BDG+01, BKLS02, BNPS02, BN02, Ben00, BR02, BF01b, BF03, BO04, Bon07, BCHK07, BGH07, BPR+08, BD03, BMN01, Boy03, BQR01, BM01c, BSN00, BRTM09, CGFSGH09, CvTMH01, CK02a, CGM02, CF01b, CC02a, CV03, CPP04, CCD07, CS07b, CC01b, CLT07, CHSS02, CHM+02, CZZK05, CM05a, CTH08, CGK+02, Coc01b, Cou01, CFS01, CS00, DN00a, DKMR05, DT03, EHK+03, EM03, FL06, FM02a, FMY01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, Hq05, HC08, HH09, Igl02, Jam00, KBD03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05a, Kel05b, KY01c, KY02b, KCO09, KK02, KCO2, KCO07, KPR03, KM05, Kra02a, Ku02, KWP06, KT00, LLL02, LP03]. Based [LKL05, LHT09, LZ01, LZ04, LL05c, LPZ06, LY07, LH07, LLRW07, LWK00, LSC03, LHS05, LS05b, LCD07, MPS00, Mar08a, Mar08b, MNP01, Miy01, MGC02, Mi001a, MSU05, NM005, Nam01, Na02, NB01, NSS02, Nov01, NMSK01, PV06a, PV06b, PV06c, PZL09, PMRZ00, Ri02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sal05b, Sch01a, SSFC09, Sha02, Sha01e, SOO02, SXY01, Sma03a, SBEW01, SGB01, TMM05, TL02, TT09a, TZT09b, VMSV05, Vau05b, Ver06a, VHP01, VK07, WR02, WY02, WZ05, WG05, WC09, WH09, WBD01, WC04, XYL09, YKMY01, YT09, YPDO01, YSS+01, YKW01, YLH05, ZK02, ZGL05, ZP05, ZJ09, ZS05, ZWCY02, vDW04, AAP07, AA08, An002b, An005b, App05, AAKD09, BGB09, BBC+09, BR04, BFG08, BS01b, Bla01b, BW05, BL06, BGL+03, BSN09b, Bu06, CG06, CG06, CL02b].

based [CO09a, CL04d, CFY+10, CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CJL06, CLK04, CJL05, Cho08b, CYH+07, CFVZ06].

CCD+04, CTT07, CHT02, CC04c, Cra05b, DS09, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EHKK04, FLZ02, FXAM04, FW08, GM08, GW08, GS09, GL06a, GHGSS00, GS01, GPS05, GGS+09, GB09, HM00, HLL+02, HCD08a, HCD08b, HRL09.
Has00, Her07, Her09b, HN07, HPS01, HG05a, Hsu05a, HLwW09, Hüh00, HP01, HLL03, HL05d, shCP09, IM06, JK01a, JK01b, JMv09, JW06, JPL04, JZC05w, JLL01, KG09, hKLS00, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KLC03, Ku04, KCC05, Kwo03a, KHKL05, LH03a, LF03, LL04b, LKY05a, LKY05b, LHY05, jLC07, LG09, LD01, LPM05, LW05a, LWZH05, LYGL07, LW08a, LW08b, LCC05, LSA+07, LCZ05c, LCZ05a, LLC06a, LLC06b, MW06, MS09c. based [Mic01, MR09, MI09, Mit00, MB08, MC04, MPPM09, MV03b, NZCG05, NC09, NSNK05, OS09, PCSM07, PW05, PBMB01, PSG+09, PS08a, Pel06, PSP+08, PC00, Pha06, PLJ05a, PLJ05b, QCB05a, Reg03, Reg04, RG09, RCG+05, Sae02, SG07, Sco04, Sei05, SH11, SM11, SPG02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SLH03, SCS05a, mSGFl05, SM+08, SW05a, SH00, SK01b, SCL05, SLC05, Sun02, SC05c, SY06, TNG04, TSWNA08, Tsa08, Tsa05, UHA+09, UBE09, V061, VKS09, WAF00, WLT03, WL07a, WP07, WNP08, WLIH05, Wh09, WW00, WH02b, WY05, WC05, XMST07, YW04a, YCW+08, YWWD08, YC09b, YS04, hY08, YJ00, YPSZ01, YRY05c, YPKL08, YY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRM05, NZ05]. Bases [AAC+01, ADDS06, BKP09, B+02*, CtVTM01, EBC+00, FJ03, FLA+03, CCT08, Fau09, ZT03]. Basic [Gol01b, Gol01a, Gol04, Kat05b, Puc03, Ste02, Bon00]. Basics [Leh06, Lut02]. Basing [BPR+08, CHL02, AGGM06, AGGM10]. Basis [RMH03b, Vav03, vW01, GPs05, LS05b, RMH03a]. Batch [Ara02, HLT01, PBD07, Sha01d, BLH06, HLH00]. Batching [SB01]. Battery [CBSU06]. Battle [Bud00a, Bud02, SM00c, SM05, SM07a]. battles [Cal00d]. Bay [Cal00c]. Bayes [Goo00]. BB84 [Iao02a]. BC [IEE02]. BCH [MLC01]. BDD [KLN+06, Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01]. Beach [IEE00a]. beat [Lev01]. because [AJ08]. Become [ORT00, WAI04]. Been [Nic01]. BeepBeep [Dri02]. before [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YJ00]. Beginning [Dew08, Hoo05]. Beginnings [Bud00b]. Begins [MP00]. Behavior [Vav03]. BEHEMOTH [Bar00c]. behind [Hen06b]. Beijing [FLY06, LST+05]. Being [ASW+01, ES00a]. beleid [dL00]. Belgium [DR02c, Pre00, QS00]. Belief [BPST02]. believing [Buh06]. Bell [BZ02, Eke02]. Benchmark [As02, TLYL04, LDH06, YLT06]. Bendy [Sas07]. Benefit [YKLM02a]. benefits [CHO0]. Benford [NM09]. Bennett [BGM09]. Bergen [Ytr06]. Berkeley [IEE06]. Berlin [FLA+03]. Bermuda [Bl03]. Bernard [DNR03]. Berners-Lee [Coc02b]. Best [Bau01a, Bau01b, MFS+09, Gol08, Ste02]. BestCrypt [Bau02b]. Bethesda [ACM09]. Better [FV03, PM00, RR02, SKQ01, HLL03, Pau03, Rei00]. BetterBASIC [ASW+01]. Between [DKMR05, Ket06, Ngu05, NN06, Fan09, GKM+00, GC05, MSV04, Pau01, RW03a, Sch02, Sch04d, SK06]. Beurling [Bec02]. Beyond [Gor06, Hei03, LMW05, Mar08a, Sch03, See04, Sty04]. BGP [ZSN05, vOWK07]. Bi [Cou04, PJK01]. Bi-directional [PK01]. Bi-linear [Cou04]. Bias [CL02c, Sel00]. Biased [BS00a, LSKC05]. Biva [RR02]. Bibliography [Bee05]. Bidiagonal [BR09]. Bidiagonal-Singular [BR09]. big [RR03a]. BigNum [SR06]. Bilateral [CT08a]. Bilinear [BGLS03, BMS03, CL04a, HSM04, KK02, DSGP06, LC05b, VK08]. Bill [Gen00a]. billing [SM+08]. Binarization [LSK05]. Binary [AD09, HHM01, LSK05, OSSST04, SKG09, WCJ09].
ACTZ05, BG08, BG09, FSGV01, GB09.

Binary-Ternary [AD09], BIND [Kle07].

Binding [DN02b], BioAW [MJ04].

Biometric [AHKM02, Da03, EM03, HWH01, KJR05, MR00, RR07a, RR07b, RR07c, SMi00, MJ04, TB00, ZJ04]. Biometric-Based [PMRZ00].

Biometric-Based [PMRZ00]. Biometrics [Ano04a, Ash03, Bjo05, MR03, Ril02, Str01a, BSSM07, BCP03, Buh06]. Biometrics-Based [Ril02].

Biomolecular [Bi09]. Birds [MLM03]. birth [Bud06, SE01]. Birthday [Wag02].

Bisimulation [BJP02]. Bit [AK+01, BK06a, BO8, CGH01, CDL+00, DMS00, GS07a, IT03, KZ07, LNS02, MS09d, PCC01, RMH03b, SM03b, SX01, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, PLs01, Pri00, RMP08, SWR05, UHA+09, WW08, ZFK04].

Bit-Fixing [KZ07, KZ03]. bit-substitution [GPX08]. BitLocker [Kor09]. Bits [BS01d, SZ01, SN04, Slp02]. Bitslice [DP01].

Black [An01j, CF02, CFS05, D05, DRR05, DS08, KY01d]. Black-Box [An01j, BRS02, CF02, CFS05, D05, DRR05, KY01d]. Blackmaling [PS01b].

Bletchley

[Kid07, Sal00b, Cop05, Cop06, Cop10, HS01a, Sal05a, SE01, Smi01b, Wei06, Win00]. Blind [AO00, BNPS02, BB00a, BSC01b, CL01b, GSK09, JK01, KY01, NA05, Pau02b, SPK08, ZTP05, ZK02, Fru03, HCO4a, JLL01, JLY05, LC05b, MS09a, SV08a, SHT05, WSH05, ZC05]. blindness [AvdH00]. Blink [Sas07]. Block

[AIK+01, BK06, BR00, BRS02, BR02, BSC01a, CVTM01, Can01, CLLL00, CP02, CMB+05, Cro01, DR00a, Dw003, EYCP00, Fhu02a, Hlu04, HSY01, JKK+01, KC01, KYHC01, KKG03, LRR07, LR02, MV00, MS02e, NP01, OMSK01, Pat01, PS06, Phi01, RMS05, SM03b, SYY+02, SUV+00, SK01, WC09, XH03, YG01b, BA08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kato0a, KJ01, LDH06, LCP04, LKH+08, MJ05, PSH+08, RBB03, SHJR04, SHH07, WF02, XH05, Y100]. Block-Based [LLRW07, BBC+09].

Block-Cipher [BR02, RBB03]. Block-Cipher-Based [BR02].

Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. blockciphers [Fur01]. Blocks [Jon02]. Blockwise [JM02]. Blockwise-Adaptive [JM02].

Bluetooth [GBM02, LV04, LMV05]. Blunders [Bur01]. Blur [VHP01]. Blur/Deblur [VHP01].

Blurring [LSKC05, SK06]. Board [CGBS01]. boat [DB04]. Body [Bam02, TG07]. BOEL [Fin02].

Book [And04, Duw03, Eg05, Eva09, Fal07, For04, Gas01, Gum04, Inr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pap03, Pap05, Rec01, Rot07, Sal03b, See04, Slp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wal00, Was08a, Kat05b, Lam07, Lun09, MAA05, Ros00b, Sin99, Sin00, AAG+00].

Books [Che00b, Dr.00c, Ros00b, Rec01]. Bookshelf [Lut00, Lut03, Wil01b]. Bookworm [Sal03b].

Boolean [Car02, CT03, CS09, MS02b, MFD04, QPV05, SM00a, SM00b, SM03a, VW00].

Boom [An04a]. Boomerang [KKS00a, KKS01, KML+02]. Boot [HSH+08a, HSH+08b, HSH+09]. Border [MFT07]. Borders [PGT07]. Boston

[USE01b, USE01a]. bot [An08b]. both [Sae00]. Botschaften [Sch09]. bottleneck [W02]. bottlenecks [HT07]. Bound [CY01, DGN03, KMT01, HLL03, hY08, GW00]. Boundaries [PGT07]. Bounded
[Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vad03, DFSS05].

Bounded-Quantum-Storage [DFSS08].

Bounding [DM07b].

Bounds [BDF01b, BP03b, DIRR05, Di01, GGK05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKS03, JZ09, KS05b, PS02a, Shp99].

Bouwmeester [Duw03].

Boxes [Ano01j, BRS02, CF02, CFS05, DI05, DIRR05, DS08, FM02b, KY01d, Kil01b, SMTM01, JmBdXm05].

BP [Wei00, Wei05].

Braid [AAFG01, CJ03a, GM02a, Hug02, KLC00, LLH01, LP03, MSU05, Cho08b, Hen06a].

Brief [Bon07, Cos03, Kir01a, Boo05, Gra01].

Briefs [MP00, PM02a, Pau02b, Pau03, Pau09].

Bright [Ano04e].

Break [Ano09a, BKN04, Das08, DKF05, G003, GKS02, Kov01, KR03, Kli08, SM00b, Shp03, Wal01, WW05, GT00, GKS03, JZ09, KS05b, PS02a, Shp99].

Breaking [Ano09a, BKN04, Das08, DKF05, G003, GKS02, Kov01, KR03, Kli08, SM00b, Shp03, Wal01, WW05, GT00, GKS03, JZ09, KS05b, PS02a, Shp99].

breaks [OS00].

Breakthrough [Coc02a, LR01, Pau02a].

Brief [Bon07, Cos03, Kir01a, Boo05, Gra01].

Briefs [MP00, PM02a, Pau02b, Pau03, Pau09].

Bright [Ano04e].

brings [Ano04e].

Britain [Gui06].

Bristol [DFCW00].

BSLCon [USE02a].

Bubble [Ber03].

Buchmann [Lee03a].

Buffer [FOBH05, Fr00, Ino05].

Bug [BCS08, Bor00].

Building [Jen02, Kuo07, Mar02a, And08b, Bra01a, FB01, LS05b, McG06, MPH06, PQQ06, DB04].

Bouwmeester [Duw03].

Bounded-Quantum-Storage [DFSS08].

Bounding [DM07b].

Bounds [BDF01b, BP03b, DIRR05, Di01, GGK05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKS03, JZ09, KS05b, PS02a, Shp99].

Bouwmeester [Duw03].

Boxes [Ano01j, BRS02, CF02, CFS05, DI05, DIRR05, DS08, FM02b, KY01d, Kil01b, SMTM01, JmBdXm05].

BP [Wei00, Wei05].

Braid [AAFG01, CJ03a, GM02a, Hug02, KLC00, LLH01, LP03, MSU05, Cho08b, Hen06a].

Brief [Bon07, Cos03, Kir01a, Boo05, Gra01].

Briefs [MP00, PM02a, Pau02b, Pau03, Pau09].

Bright [Ano04e].

brings [Ano04e].

Britain [Gui06].

Bristol [DFCW00].

BSLCon [USE02a].

Bubble [Ber03].

Buchmann [Lee03a].

Buffer [FOBH05, Fr00, Ino05].

Bug [BCS08, Bor00].

Building [Jen02, Kuo07, Mar02a, And08b, Bra01a, FB01, LS05b, McG06, MPH06, PQQ06, DB04].
HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. **Candidate** [II00, EYCP00, NIS00, SKW8+0, SL00]. **Candidates** [AL00b, DPR01, Dra00, GC01a, SB00, SGB01, WW00, GC0a0a, WB00]. Cannes [AJ01a, AJ01b]. *cannot* [Gav08]. **Canonical** [TP07]. **Canceled** [DWML05]. Canterbury [CZ05]. Cantor [WPP05]. **Capabilities** [BDTW01, AL04, ABDS01]. Capability [MH05]. capable [ETMP05]. **Capacity** [ChLYL09, Sug01, ME08a, Wan05]. Cape [IEE05b]. capital [SW05b]. capture [AMB06]. Card [BCST00, CMG8+01, CL07, CJT02, DF01, DFPS06, RE03, RS01, SR01, Ano00k, Ano00l, Ano05b, AJ01b, Bor00, BGL8+03, Bur00, Cal00c, Car01, CCCY01, Cha05a, Cla00b, Con00, CH00, DFCW00, GMG00, HM01a, Has02, Hen01, Hus01, Jac00, LSA8+07, LC05a, Lu07, QS00, RE00, SP02, Smi00, VK08, Zaf00, Cho00a, FGL02, Pau02b, SKK00, TV03]. card-based [LSA8+07]. **CARDIS** [DFPS06].

**CARDIS'98** [QS00]. **Cards** [An04, AJ01b, Be01, CK06, DJL01, HBdJL01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NFQ03, QS01, Sak01, Sha01c, TDBDL01, VPG01, YKM01, Ano04c, Ano04f, AJ01a, BPR01, BCHJ05, Bur00, DFH01, DFPS07, FCZ05, Fin03, GGU01, Gui06, HHS01, Hsu05b, Jua04, KLY03, LKY05a, Ler02, LCS09, MY01, Pha06, Poh01, PB01, Pre07, SVDF07, SLH03, TIS07, WC03b, YYW04b, YWWD08, Ano03a, BJvdB02, CL04d, CCK04b, Che00a, Gro03, HL05b, Kuo4, KC05, LHY02, Sco04, SCF01, YW04a]. Card**4** [GN01]. **Care** [Mad00a, RC06, Ano03a]. carefully [Cl00b]. **Carlo** [Bi09, Sug03]. carrying [Art04]. cars [LPW06]. **Cartilage** [MYC01]. Cartography [SGM09, SWR05]. **Cascade** [DGH8+04]. **Cascaded** [Jou04]. Case [ABK00, Ano05a, BBGM08, BU02, BCP01, CNS02, GS07a, Nie02b, OST05, Vau01, BKN04, BF06a, BK05, CSK8+08, HRS08, KWDB06, Mic02a, Mic02b, OST06, Pei09, STY07, SKW8+07, SPPH06, Sul05, ZWWL01]. case/average [Mic02b]. cases [ABHS09]. Cash [PS01b]. **Cathedral** [USE02a]. **Cats** [Pem01b]. Caught [Wei00]. cause [SB00]. Causes [M01]. **Cautionary** [GMP01a]. **Cayley** [Lam91]. **Cayman** [Syv02]. CBC [BBKN01, BPR05, BR00b, DGH8+04, Fer06, JM02, KI03, Vau01, Vau02]. CBIDs [MC04]. CCA [KOMM01, M¨ul01b]. **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, MG02, PZL09, Ric00, SBZ04, Bao04, ETMP05, KK03, SHH07, Wan04a, dRMS05, Wue09, SSM8+08]. Censoring [An01e]. Center [AUW01, CH01a, CYH04, LPM05]. Centered [BKM07, CMB8+05]. Central [CHL02]. Centralized [Wac05]. Centre [PPV96]. Centric [Mit02b]. Century [Eva09, Kob00, Lan00c, PRS04, Gan01b, Lan00a]. Century-Long [Eva09]. CERT [Sea09]. **certicom** [LM08]. Certificate [BLM01, Gen03, GMR08]. Certificate-Based [Gen03, GMR08]. Certificateless [HLC08, HRL09]. Certificates [BDTW01, CMG8+01, RdS01, Bra01a, LCK04, ZSM05]. Certification [An01o, CHM8+02, RSA00b, BGB09, BD04b, KB09]. Certified [AN01, CSV07, LH07, NZCG05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LWK05a, NZS05, Sha04b, Sha05b, TLH05, Tsa05, TJC03, W303]. **Cerven** [Sal03b]. **CFS** [Ito01]. **ChaCha** [Ber08]. Chain [YT09, YZ00, Wue09]. chain-rules [Wue09]. Chained [BCC01, BC05b]. Chaining [BKR00, CB005, PCC03].
challenge [LM08, LW05a, PRS04, Smi08].
challenge/response [LW05a]. Challenges [Cla00a, GV09, Nao03, Sta03, SVEG09].
Chang [CWJT01, ZC05]. change [CYH05].
Changed [CWJT01, ZC05].
Changing [BST03]. Channel [BU02, CHVV03, Law09a, LCK03, Mölo2, NMO05, OT03a, OT03b, Sch06a, SYLC05, ARR03, BP03a, BG07b, Buh06, CNPQ03, KSWH00, LCZ05b, MS09c, PSP+08, WL07a, YTWW05]. Channels [AIP01, CK02b, Nam02, Vau05b, LH04].
Chaos [JK01b, SK01b, JCM+03, McN03, PSG+09].
Chaos-Based [WZW05, SK01b, JCM+03, McN03, PSG+09].
Chaotic [BCH11, LLL+01, Mul06, SXY01, US02, Vav03, AMRP00, AMRP04, GHGS+00, GB09, HHYW07, HLWZ09, JK01b, LMC+03, LYGL07, MA02, PBB01, PS01a, PZ09, SP02, SL09, UHA+09, VKS09, WG02, WW08, kWPwW01, WLW04, YZEE09]. Chapman [Kat05b, Was08a].
Chapters [MAaT05, Tat05]. Characteristic [Gau02, GPS06, KT00, Ver02, GPS05].
characteristics [RFR07a, RFR07b, RFR07c].
Characterization [AJ008, Nam02, XH03, BM04, KY00, QPV05, XLSM06].
Characterizations [Pas05].
Characterizing [BTW05, BTW08].
Charging [BACS02, RH02]. Chatter [Kee05].
Chau [BNPS02, KLM+06, WHH05]. Chaumian [Mölo3a].
Cheating [CCL09, OVS06, PZ01, PZ02b, PZ02a, ZP01].
check [Kirt01b]. Checkable [BPST02].
Checking [BL02, JP07, KLM+06, YJ00, GHG+08, RG05].
checklists [Sha01a].
Checks [FM02a].
Checksums [St01, SGPH08].
Chemical [EIG01].
Chen [BL05c].
Chen [EIG01].
Chemical [EIG01].
Chen [BL05c].
Chennai [CV04, RD01, Roy05].
Chernobyl [Rie03].
CHES [JQ04, KKP02, KP01, KNP01, RS05, WK03].
CHESS [LKHL09].
CHESS-64 [LKHL09].
Cheswick [Che05b].
Chicago [ACM04b, Top02, Cou00].
Chien [YRY05b].
Children [Pau02a, Sye00].
China [B+02, DWML05, FLY06, JYZ04, LTL+04, Li05, LST+05, ZJ04, ZYH03, Ano00c, TTZ01].
Chinese [LTL+04, Li05, Sch01b, CAC06, YKL03].
Chip [Ade09, BPW03, DVO8, MM01b, MM01c, MP00, Mit02b, Fox00, ISTE08, Ano04c].
Chip-Secured [BPW03].
Chipkarten [Ano04c]. Chips [Ano00d, GP00, Pau02b].
Choice [Jam00].
Choquet [SH11, SM11].
Chosen [BCHK07, CN03, CHJ+01a, CHJ+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JK02, J00b, KS00a, KY01a, KJC+01, KMZ+03, KM01c, KI01a, Man01, Nov01, PV06b, Poi00, Sho00b, BW05, CHH+09, KG09, ZCW04].

##### Additional Entries

Chosen-Ciphertext [BCHK07, CN03, CHJ+01a, CHJ+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, JK02, J00b, KC+01, KMZ+03, Nov01, PV06b, Poi00, CHH+09, KG09].

Chosen-Plaintext [DN02a, KM01c, KI01a].

CHW [CHC04].

CIA [Mah04, Ris06].

Cincinnati [BD08].

Cinematic [CAC03].

Cipher [AIK+01, BKR00, BRS02, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DP05, DF07, Dwo03, EYP00, FF01a, Flu02a, GG05a, GBM02, HJC02, HQ01, HI04, KY01, KH01, LKH09, MS07, NP01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY+02, SYX01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BVP+04, GPX08, HanR04, 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, CHJ02, CP02, CM03, Con03, DP01, Eag05, Fil00, FF01a, Fil02, Gol01d, Gol01e, HR00, HR04a, HSH+01, Jam00, Jan06, Kan01, KCP01, KKG03, LRW02, MV00].
Oni01, PP06a, Pli01, RMS05, Sar02, SM03b, SKU +00, Wa100, Wri05, ??02, YG01b, ZC00, Bai08, Bar06a, Be07a, Ber07, Bod99, DLP +09, DY01, DS09, Dun06, DK08, Egh00, GPG06, HW03a, HWR09, Hey03, JK01b, Jun05, Kat05a, KSWH00, Kin01, LMSV07, LDH06, Lun09, Max06, M09, MRT10, MWM01, Pin06, SIJR04, SK03, Smi01b, SL07, SB05, TT00, Wag03, YI00, You06, Kat05b.

Ciphertext [BBK03a, BCHK07, CKN03, CF01b, CS07c, CHJ +01a, CHJ +01b, CS02, CS03b, Des00b, DK05, FP01, JKS02, J006, KS00a, KY01a, KCI +01, KM09, Kur01, Man01, Nov01, PV06b, Sho00b, BMW05, CHH +09, IM06, KG09, Poe00].

Ciphertext-Only [BBK03a].

Ciphertexts [AFI06, BGW05, BGN05, Gen04b, J006].

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].

Citizen [Mit02b], citizens [An03a].

Clam [DS00], clamping [An03a].

Clandestine [Wri05].

Class [Car02, KM01a, KKH03, NN06, OP01a, Pli01, SBZ02, XXXXYX11, DKL00b, Fox00, HM00, Uni01].

Classes [CY02, RSA00c].

Classical [BYJK08, Gav08, GW00, LW05b, NA07, BYJK04, J009].

Classification [HMS04, PB00, Uni01].

Clauses [SV08a].

Cle [RSA09a].

Cleaner [TR09a, TR09b].

Cleaning [L006].

Client [AN01, An001f, AN01, FSS01, PS05, WK08, Bad07, HT08, LF03, YS04].

Client-Server [AN01, PS05].

Client-to-client [HT08].

Clients [JRF01, RKZD02, WH06].

Clint0n [Gen00a].

Clip [FG02].

Cliques [PQ06].

Cliques-type [PQ06].

Clock [DM07b].

Close [An004e].

Closing [Lau08b, PWGP03].

Cloud [CKS09].

Clouds [GS01, VS01].

Cluster [H01, KCD07, SEF +06, TLC06, W07].

Cluster-Based [KCD07].

Clusters [MFS +09].

CMS [BWBL02, KU05].

Co [Bud00b, Nd05, ACM01b].

Co-Design [Nd05].

Co-operation [Bud00b].

Coalition [ACJT00].

Coalition-Resistant [ACJT00].

Coarse [Ri03].

Coast [Boy01].

Cod [IEE05b].

Code [Ark05, BKR00, BR04, CD00b, CV03, Cer04b, FIP02a, FF01b, HSZI01, Imr03, KY01e, Lai08, OS09, Rey01, Sal00a, Sin02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MMJ05, Mul02, Ros00b, RSA09a, SM00c, SM05, SM07a, Sin09, Sm00, Swe08, AAG +00, SE01].

Code-based [BR04, OS09, BGB09].

Codebook [CTH08, YWWS09, WJP07].

Codebook-linked [YWWS09].

Codebreaker [Hau03, Pin06].

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

Codebreaking [Bud00a, Bud00b, Kid07, Sin01b, Alv00, Bud02, Cop05, Cop06, Cop10].

Codebuster [An04d].

Decode [Che08a].

Decodes [LLR07].

Coded [MLC01].

Code [Bec05, BP06, Big08, Bod09, BQR01, CC09, Chu02, CDG +05, GMW05, J006, KY02b, Mol05, NN06, SNWX01, Sin01b, Sm01b, Urb01, Wri05, ??02, YYDO01, Yek07, Bel07a, aSM01, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HWR09, Kov01, Lam07, Lun09, Min03, NS01a, PCS03, Pin06, Rev05, Reg09, Sav04, Sun02].

Codeword [AJ08].

Coding [Buc00a, CS05c, HHL +00, Joy00, LLL +01, MZ02, Pat03b, RK06, Sal05c, Sm05, TW02, TW06b, Ytr06, Che07a, DW05, Gar04, Hon01, PPV96, Scho0a, Scho1c, S +03, Scho4a, Scho4b, Scho5a, Sea05, Sea09, TW05, Irw03].

Coefficients [CH01b, KT00].

Coffin [Rie03].

Cohen [Was08a].

Coherent [TPPM07].
RMH03a, Rot02b, Rot03, Shp99, SPHH06, TW06a, SV08a, Fal07, Rot07.

Complexity-Theoretic [CB01].

Compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BL02, TEM01].

Complexity-Theoretic [CB01].

Compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BL02, TEM01].

Component [BSL02, Hei01, TEM01]. Composability [PS04c]. Composable [AF04b, BOHL05, BLDT09, CF01a, CKO2b, DN02a, DN03, NMO05, RK05, Can01a, CLOS02].

Complexity-Theoretic [CB01].

Compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BL02, Hei01, TEM01].

Component [BSL02, Hei01, TEM01]. Composability [PS04c]. Composable [AF04b, BOHL05, BLDT09, CF01a, CKO2b, DN02a, DN03, NMO05, RK05, Can01a, CLOS02].

Composite [CQS01, GMP01a, RDJ01, Zhe01].

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

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

Computation [ACS02, Bai01b, BCL+05b, BI05a, BIM00, BJLS02, CC00, CDM00, CDN01, CDG+05, CDI05, DN03, DI05, DMM00b, FS02, FGM001, FWW04, GIKR02, HCK09, Has01a, HM01b, IH04, Jef08, KO04, KLM05, KSR02, Lin01c, PS05, WW05, Ano02g, AB09, BEZ00, BZ02, CLOS02, CLC08, CDD00, DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WLHH05, WY05, SM07b, Duw03].

Computation-efficient [CLC08].

Computational [CCL09, DLP+09, GH02, HG03, KLR09, KK06, Rup09, SM07b, Wvd02, AUW01, IKOS08, Lam01, Lau08a, Nie02a, Sho05b, SHJR04].

Computational [MPSW05].

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

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

Computer [BS03, Bis03b, Bro05a, BCDH09, BC01, CSW+08, CZK05, CGK+02, Coc02a, Coc03, Eva09, HYZ05b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Ifr00, IH04, JBR05, KM07, Leh06, Lu02, MYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Tyn05, Cas02, Che05b, DFGH04, Fan09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Shu06, SL06, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coc03].

computerized [LM+03, Pau02b].

Computers [Coc03, Ett02, TSS+03, Cop05, Cop06, Cop10, Heg09, RH00, Kid07].

Computing [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBDK00, CGH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Lut03, May04, PFM03, Sch06b, SKG09, SFC01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Wri00, Yan00, YKMB08, Cha07, Che05c, CHT02, DHL06, HV09, HKPR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sei05, WLH06, W199, YLR05, Lut03].

Compuation [Ano02d].

conceal [BB79], Concealing [DS00].

Conceal [DA03].

Concept [ARC+01, Ano09c].

Concepts [MFD04, AB09, Kra07, SWR05, MC04].

concerning [HW03b]. Concerns [MP00].

concrete [KNS05].

Concurrency [JL00].

Current [BP02, DPDV04, Gen04a, KKG03, Ros00a, Ros06a, Dam00].

Conditional [LMV05, WN02].

Conditions [IK05].

Conference [ACH05, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bih03].

Computation [CL00].

Compression [ABC00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBDK00, CGH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Lut03, May04, PFM03, Sch06b, SKG09, SFC01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Wri00, Yan00, YKMB08, Cha07, Che05c, CHT02, DHL06, HV09, HKPR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sei05, WLH06, W199, YLR05, Lut03].

Compuation [Ano02d].

Conceal [BB79], Concealing [DS00].

Concealment [DA03].

Concept [ARC+01, Ano09c].

Concepts [MFD04, AB09, Kra07, SWR05, MC04].

concerning [HW03b]. Concerns [MP00].

concrete [KNS05].

Concurrency [JL00].

Current [BP02, DPDV04, Gen04a, KKG03, Ros00a, Ros06a, Dam00].

Conditional [LMV05, WN02].

Conditions [IK05].

Conference [ACH05, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bih03].
Bla03, Bon03, Boy01, Buc00a, CC04a, CV04, 
CGP03, CGH+00b, Cra05a, DKU05, 
DFCW00, DFPS06, EBC+00, ELvS01, 
FLY06, Fra01, FMA02, Fra04, FLA+03, 
HR06, HYD05b, IEE09a, IKY05, JYD04, 
JM03, Jov03b, Jue04, KJR05, Kil01a, 
Kim02, KN03, Knu02, Lai03, Le04b, 
LTT+04, LL04d, MMV06, MS05b, MS02c, 
Men05, Men07, NIS00, Nac01, Nao04, Oka00, 
Oka04, Pat03b, Pen01b, Pfi01, Poi06, Pre00, 
Pre02c, RD01, Roy00a, Roy05, Sho05a, Si01, 
SM07b, Sma05, Syv02, USE00c, USE00a, 
USE01b, USE01a, USE02c, Wil09, Won01, 
Wri03, Yun02a, YDKM06, ZD04, Zhe02b, 
ZYH03, AUW01, BC05c, DV05, DWML05, 
DRS05, Hon01, Kil05, Lit05, PC05a, PY05, 
PPV96, QS00, Son00, WK06].

Confidences [Gan01a].
Confidentiality [Dwo03, Pem01a, YC08].
configurable [MBS04].
Configuration [Sha02, Mos06].
Confirmation [SK00].
Confirmer [CM00, GM03].
Confiscation [DBS01].
Conformance [LBR00, RSA00c].
conflated [Bel07a].
confusion [She01].
congestion [SBB05].
Congress [Uni00a, Uni00b, Uni00f, Uni00h].
congruences [Ste08].
Congruential [CS05b, LS05a, SB05].
conic [LWL09, LCC05, LCZ05a].
Conjecture [CU01].
Conjugacy [CJ03a].
Conjugate [Igl02].
Connected [BJL05, H0601].
Connection [HR00, Jam00, Goo00, Mic02b].
Connection-Polynomials [Jam00].
Connections [WRW02].
Conquer [SKQ01].
conscious [DMSW09].
Consensus [CNV06].
conservation [Che05b].
Considerations [DBS+06, Hei07, Rub01, Sch07, SVEG09].
Considering [WA07].
Consistency [ABC+05, JEZ04].
consistent [RG06].
Constant [App07, BI05a, CS07c, CD01a, DPV04, 
DN02b, DI05, Lin01c, Smu00a, IKOS08].
Constant-Depth [BI05a].
Constant-Round [DPV04, DI05, Lin01c].
Constrained [BCH+00, DBS+06, HS01b, 
MRL+02, Nit09, Zhe02a, Has00, RAL07].
constraints [CC05d, LPM05, SN04].
Construct [CDMP05, Go01d].
constructed [Tsa05].
Constructible [NNT05].
Constructing [Des00b, Fis01b, LL04b, Vad03, Wen03, 
JZCW05, NS01a, ZL05].
Construction [BBKN01, BB00b, Car02, CMKT00, Lin03, 
Nie02c, SM00a, TNM00, YWD08, DW05, 
SC02c].
Constructions [BS00a, BR00b, BRS02, GMW05, GGT05, 
GM02c, J04, P08, PZ02b, SNX01, 
SM00b, GT00, GPV08, IK03, IK06, NR04, 
PR05, Reg03, Reg04, vDST06].
constructive [GGH+08].
consumption [Mis08].
Contact [YKMY01, Car00].
Contact-Less [YKMY01].
Contactless [And04, KS02, Cla00b, Fin03].
Contemporary [Ahm07, SVEG09].
Content [AAK09, CGJ+02, HHJS04, 
MA00a, MA00b, Re02, XMST07, YK01, 
ATS04, DY09a, GSK09, SG07].
Content-adaptive [XMST07].
Content-Based [RE02, YK01, SG07].
Content-triggered [HHJS04].
Contest [Bar00b].
Context [DJL01, FPS01, SN04].
continue [Lov01].
continued [Dan02].
Contra [Mah04].
contract [WK05].
Contrast [BDDS03, HKS00, HT06, KS03, CDFM05].
Contrast-optimal [HKS00].
Contrast-Sensitive [HT06].
Control [ABEL05, ANRS01, BW07, CGMM02, HC08, 
LY05, Sma03a, ZGLX05, BNP08, DFS04, 
DPT+02, HW03c, JW06, KNS05, LKZ+04, 
MD04, MSP+08, PS04b, STY07, WC01b].
Control-flow [ABEL05].
Controlled [GVC+08, IMM01, AW05, AW08, LAPS08].
Controlling [HY03, MS03b, MS02d, WL05].
Controls [Har01a, Har01b, Ge03].
convenience [WDC09].
conventional [CJ04, YW05, YRY05b].
Convergence
Converging [Pot07].
Conversation [GK04]. conversations [VAVY09]. Conversion [CDI05, Ket06].
Conversions [Kl01b]. Convertible
[Chi08e, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b]. Convolution [PG05].
cookbook [VM03]. cookies [Cha05a]. Cool [Ano00d]. Coordinate [OS01].
COPACOBANA [GKN +08]. Copenhagen [TB02]. Copley
[USE01b, USE01a]. coprocessing [ML05].
Coprocessor [Gut00, Ito00, LS01b, OTIT01, AV04].
Coprocessors [Smi02]. Copy
[BF00a, Dim07, DV08, HMS04, TPS01].
Copy [MV01, Top02, MB08]. Creator [Coc01a]. Credentials
[CL02a, CL04a, LLW05, LLW09]. Credit
[CNB +02]. Crete [ACM01a]. crime
[Cas02, KB00, Lau08b, Mad00c]. criminal
[Men03]. criminals [Win05c]. crisis
[Gui06, Wal04]. Criteria [Can01b, IBM00].
criterion [QP05]. Critical
[LKM +05, SE09, CS07a, Gor05, Her09b].
cron [Oue05]. Cropping [SDFH00]. Cross
[Bau02b, SM08, LCX08, SLP07].
cross-authentication [LCX08].
Cross-disciplinary [SM08]. cross-layer
[SLP07]. Cross-Platform [Bau02b]. crowd
[Fox00]. CRT [FMP03, Kuh02a, May02].
CRT-Exponent [May02]. crypt [Per03].
Cryptanalyses [HW03c, Kan01, SKU +00]. Cryptanalysis
[ASK07, AMRP00, And03, Ano07b, BDG +01, Bao04, BLH06, BP03a, BBK03a,
Bar06a, BP01a, BD00a, Bih00, BM02]. BDK02a, BDK02b, BSW01, BDD03, BD00b,
BCC01, CGFSHG09, CV02, CC01a,
CC01b, CL01b, CYY05, CKY05, CKK\(^{+}\)02, CWJT01, CJT03, Cho06, Cho08b, CHJ02, CP02, Cou04, CGJ\(^{+}\)02, DG00, DGP07a, DGP07b, DGP09, DN00b, FJ03, FKS\(^{+}\)00, FKL\(^{+}\)01b, FKL\(^{+}\)01a, Fin06, Fhu02a, Fhu02b, Fur01, Fur02a, Fur02b, GS07a, GM02a, GS02c, GM02b, GM00b, GBM02, GC00b, Gra02a, GS09, GKN\(^{+}\)08, HPC02, HQR01, HAuR04, Hen06a, HLL\(^{+}\)01, HSM\(^{+}\)02, HHK\(^{+}\)04, Hsu05a, HLH00, Hwa00, JK02a, JJ00c, JJ01, JMBD0X05, Jou09, Joy03a, KM02, KW03, KRY05, KW02, KRS\(^{+}\)02, KKS00b, Kra02a, KC05, K"uh01, K"uh02b, KHKL05, LC03, LHL\(^{+}\)02, LP03, Lee03c, LKY04, LL05a, LR07, LG0Z01, LG0Z02. Cryptanalysis [LLH04, LL05c, LLCL08, LW05c, MS03a, May02, MG01, MHL\(^{+}\)02, Mor05, NPV01, Nit09, PSC\(^{+}\)02, PKN05, Pei04, Pel06, Pha06, PS06, PS01c, QCB05a, Sch06a, Sco04, Sha03c, Sha05a, STK02, SG08, SK01, SH07, TGD01, TM06, TLI05, TJ01b, TSS\(^{+}\)03, Wag00, Wag03, WLT03, WL05, WBD01, WB02, Wu02, XwWL08, XY04, YSD02, YW04b, YW05, YKLM02a, YKLM02b, YR05a, YY05a, You1, YG01a, YG01c, ZR01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, AMP04, BF01a, Baf08, Bar09, BS01c, Buh06, Bu09, Bur02, CV05, CKN06, CKL\(^{+}\)03, Dum06, Eg00, EBS01, Eke09, Fie09, GPG06, Goo00, Jun05, KSWH00, Kuk01, LMSV07, Max06, MAu03, MAu04, MAu05, MAu06, MAu07, Ny01, Pha04, RSQ03, Rup09, SK01a, Sel00, Sin09, SL07, SLS05b, SLL\(^{+}\)00, Swe08, TC00, TM01, WLW04, WF02, YI00]. Cryptanalysis [YJ00, YKLM03, Kat05b]. Cryptanalyst [Wil06]. Cryptanalytic [BS00b, KS09b, Kus02, Law09a, LN08, LS05a, LJKL01, MS02a, MOP06, Mea01, MNP01, MRL\(^{+}\)02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Nao03, Ndu05, Ngu05, Nie04, OIT01, OP01a, PKBD01, PR08, PZ09]. Cryptographer [Joy03b, Nac01, Oka04, Poi06, Pre02c, Men05]. Cryptographers [Coc03, Heg09, KL0706, Tsa07, Beh07a, Hau03]. Cryptographic [AC02, AADK05, AL00a, Ano09d, ADH\(^{+}\)07, Ase02, BLST01, BDF01a, Bar00a, BGK\(^{+}\)03, Bli03, Bla01a, Bon01, BDP02, Bra01b, BM01c, BL08, Bur06, CC04a, Can01b, Car02, CDP01, CH02, CK07, CB01, Cra05a, CS09, CO09b, DD02, DHR00, DVO8, DFG01, FIP01b, FS00, Fis01a, FG00a, Fri01, GMP01a, Gar05, GSS08, GGGT05, GOL01d, GKO2, GTOH02, Gor02a, GL00, GU01, Gut00, Gut02b, Gut04a, HTO07, HNO6, Har06, Has01a, HI04, HL05a, HC08, Ig02, JYO0, Jem01, JMO1, JTO05, KMO01, KY01b, KY02b, KI01b, KS06a, KS09b, Kus02, Law09a, LN08, LS05a, LJKL01, MS02a, MOP06, Mea01, MNP01, MRL\(^{+}\)02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Nao03, Ndu05, Ngu05, Nie04, OIT01, OP01a, PKBD01, PR08, PZ09]. Cryptographic [Pem01b, Pi01, Pin02, Pin03, PS02b, Pot06, Pre00, Pre02a, Pre02b, SAA04d, RSA01, RR00, RRS06, Rot01, RSN\(^{+}\)01, SM00a, SS01a, SGM09, Sha02, Shp03, Shy02, SDF06, SVW00, SR06, SL09, TLY04, TW08, TBD01, UZ04, WKP03, WN02, WBL01, WY01b, You1, Zha08, AMRP04, BAY05, BF01a, Bar00a, FSG00a, Fri01, GMP01a, Gar05, GSS08, GGGT05, GOL01d, GKO2, GTOH02, Gor02a, GL00, GU01, Gut00, Gut02b, Gut04a, HTO07, HNO6, Har06, Has01a, HI04, HL05a, HC08, Ig02, JYO0, Jem01, JMO1, JTO05, KMO01, KY01b, KY02b, KI01b, KS06a, KS09b, Kus02, Law09a, LN08, LS05a, LJKL01, MS02a, MOP06, Mea01, MNP01, MRL\(^{+}\)02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Nao03, Ndu05, Ngu05, Nie04, OIT01, OP01a, PKBD01, PR08, PZ09].
Cryptography [Reg04, Ren09, RMH04, RB08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, TNG04, kWpLwW01, WLW04, XLMS06, YLT06, ZLX99, ZW0L01, ZL04b, dH08, BW0L02, JQ04, KKP02, KP01, KN01, RS05]. Cryptographically [ADD09, AHS08, BJF02, BCGH11, BFCZ08, BB00b, FR08, MS02b, PLSvdLE10, RGX06, Aam03, AW05, AW08, Lau08a, SM03a]. Cryptographically-masked [AHS08]. CryptoGraphics [CK06]. cryptography [RSA09a]. Cryptography [AN05, AF04b, ADI09, AA04b, An00e, A01j, Ano02b, An02f, Ano02h, Ano04b, Ano05a, Ano07b, Ano07a, AAFG01, AIK04, AIK06, App07, AEAQ07, ABM00, Bai01a, Bai01b, BIN03, BD02, BOV03, BOV07, BBGM08, BM01a, BR00a, BY03, Ber03, Big08, BW0L02, Bla04, BBDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, BK006, BM07, Bc00b, BD08, BP01b, BRTM09, CPS07, Cer04b, CCL09, CWS08, CQ01, CDP06, Cob04, CFA06, Cop00, Cor06, Dr.00c, Dam07, DFS08, DFS05, Das08, DD00, DF04H04, DK02, DK07, Des02, DT03, DY09b, DSS01, DNN00, DNN03, Dre00, DP08, EPP07, EP05, EK09, EJ04, ECG07, Ett02, FS03b, Gal01, Gal02, GHK06, GKK09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, GRI01, Gro05, HR06, HH04]. Cryptography [HHM01, HMV04, HSS01, HPS08, Hon01, IEE00b, IYK05, Irw03, IH04, IK05, IOS08, JY04, JL00, JT01b, JT01a, Jue04, Kak06, KLR09, KZ07, KGS07, Kat05b, KK06, KBM09, KPMF02, KWDB06, KY01c, Kir01a, KMS02, KM05, KS02, KS03, KWP06, Lam01, LCS01, LSY01, Lee03b, LLL01, Lie05, LDM04, LW05b, LP02b, Lut03, Lys08, MNT00, MP02, Mao01, Mao04, MS10, MZ04, Mau01, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pe06, PM02, PBB02, Poi02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Shaoib, She01, SXY01, Sma03a, Sta02a, SGK08, Sti95, Sti01, Sti02, Sti04c, SJ05, Syv02, TS00, TW06a, TG04, TMM01, TW02, TW06b, Tro08, TR09a]. Cryptography [TR09b, Uni01, US02, VY01, VMC02, WP01, W04, WK01, We05, Wei00, WvD02, Wri00, YWC08, Ytr06, YC01, YDK06, ZH03, vDW04, Imr03, AMW07, AEP17, AN03, AUW01, An02a, An02g, ABD01, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BEZ00, BEZ01, BGM04, BEM07, Buc00a, Buc01, Buc04, BR05, BMA00, BMA00b, BMA00c, CCT08, CIO08, CDF05, CDD07, Cos00, Cre00, DD04, Di01, DIM08, DwW05, DOP04, DKL09, DW09, Duw03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK07, Geb04, GRT02, Gol09, GG05b, GHP05, GPS05, GNP05, HH05, HHL00, He03, HK05, HA00, Hig08, HSK00, Hoo05, HG05b, HLW09, IZ00, IM06, J01b, Jan08b, JMV09, Joy00, KZ03, KL08, Kat01, Kil05, Kim01, Kob00, Kra07]. cryptography [La00c, Le04a, Lin01a, Lop06, Mau04, May01, MCA08, MBS04, MM07a, Mol07, NP02a, Nis03a, NH03, Opp05, OP09, PP09, PY05, PC09, PC00, Pin06, Pip03, Reg05, Reg09, Rot02b, Rot03,
Roy00b, Rup09, STY07, Sch02, Sch04d, SBZ04, Ser06, SH05, Shp99, Sil05, Sin99, Sin00, Smo04, ST01d, Sti11, SK01b, TW05, UHÀ+09, Van03, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wri03, YC09a, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Ree01, Wa00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08, Ros00b].
cryptography-based [FXAM04].
Cryptologic [BS00a]. Cryptological [Lew00]. Cryptologie [dL00]. Cryptologists [WD01b]. Cryptology [Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Lai03, LL04d, Lut02, MMV06, MF04, Neu04, NS01c, Ngu01, Oka04, Po06, Rot05, RSA03, Sha03b, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bih03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam91, LL03, Lee04b, Men05, Men07, Nac01, Oka00, PC05a, Pre00, Pre02c, ZC09].
cryptovirology [YY04]. CRYPTREC [IY00]. CSCW [ZP05]. CSP [SBS09]. CT [Joy03b, Men05, Oka04, Poi06, Pre02c, ZC09]. CRYPTO [Ano03g]. CTS [Con00]. Cuban [AJ08].
Cure [DS08, PDMS09]. Cure-Type [PDMS09]. culture [Gil07]. Cumulative [LG04, WP03]. cure [RD09]. cure-all [RD09].
Current [Ano03b, DFH01, PRS04, LPW06].
curriculum [FOP06].
Curve [ANS05, ADI09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BMM00, BWBL02, BS01d, BMN01, CQS01, CFA+06, GPP08, HYZ05a, HHM01, HMV04, HM02c, JH01b, JT01a, KBB09, KPMF02, KSZ02, KW06, LW02, Mî02, Kir03, OTT01, OS01, PWG03, Pe06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YYZ01, ZLK02, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFV06, DIM08, DWwW05, EKK04, GBK01, Has01b, Hsu05a, HL05d, JMV09, JW06, LL04c, LWL09, Mis06, OS00, ST03a, SSST06, SH05, Sma01, SC05, SL05, TC05, Van03, Ver01, Wu04, WPP05, YC09a, YC09b, ZS01, ZLK05, vT01].
Curve-Based [KW06, P01].
Curves [AHR08, B00b, B01b, C02, Ga01, GLV01, Gra02, GHK+06, Kid02, PWG03, Ver02, CMKT00, Hus04, LWZH05, MP01b, SVD04, Sil05, Sim02, SC02b, Was08b, Wen03, Yas08].

customer [Lin01].

CVS [DFG01].

Cyber [FNRC05, WW04, Mad00c, Mao05].

cyber-crime [Mad00c].

cyberinsurance
Cybersecurity [PLW07], cyberspace [Mit02a], cycles [ABHS09, BPS08]. Cyclic [PG05, Mic02a].
Czech [MJ04].

D [Duw03, Ben00, ChLYL09, CT09, DNP07, DVP09, Lav09, OMT02, WH09, ZTP05].

D.R [Irw03]. Dad [Che05b].

Damgård [CDMP05]. Dark [Blu09]. Darkening [CDD07]. DARPA [Coc01a].

Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BS00b, BNWP03, Bro05b, Che01a, CTLLO1, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTT03, HLL+02, Ken02a, Ken02b, Lau00b, LLRWO7, LP00, LHS05, LS08, Lut03, MND+04, MS03b, MFS+09, NNAM10, NM09, OS05, Per05a, RKZD02, RK06, Sal03a, Sal07, Sin01a, SK03, SDMN06, TZD05, TPPM07, VDKP05, WS05, WY02, kY01, kV01, AMBO6, AG09, Ade09, AHK03b, AKSX04, Ano02c, Arn01, Bl00a, BNPO8, CCMT09, Cer04a, CO09a, CLR09, CFG+04, DZL01, DGMS03, DVP09, FS04, HILM02, LLK05, MJ03, Mal06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGP98, SETB08, WMDR08, YLC+09, YC08, ZSJN07, Zir07, AEH17, Cur05, DK08, Lin02, Pap05].

Data-Hiding [VDKP05]. Data-Oriented [NNAM10]. Data/image [Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, BI05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Mau04, PS08b, PBVB01].

Database-service-provider [HILM02]. Databases [AK02b, CDM+05, DN04, AKH03a, CDD+05, CKY07, GA03, MSP09, MNT06, NS05b, ÜG08, YPPK09].

Datamining [DN04].

Datenverschlüsselung [Lin02]. David [Gas01, Pap05, Bar05, Eag05]. Days [SE01, CSW05, Win05c]. DC [USE01c].

[BSC01a, BSC01b, CH01b, KT00, LY07, LSC03]. DCT-Based [LY07, LSC03]. DDH [Lys02]. DDO [LKH+08]. DDO-64 [LKH+08]. Dead [Gut02a]. deaf [Pau02b].

Dealer [DK01, Snn00a]. Dealing [BH00a, BC05b]. death [For09]. Debate [Jol01, Mad00a]. Debian [YRS+09, Ahm08].

Deblur [VHP01]. Debugger [Ano02d]. Debugging [Ano02d]. Dec [IEE09a].

decades [Lov01]. decades-old [Lov01].

December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, Lau04, Lee04b, LLT+04, L05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b].

Decentralized [MSP+08]. deception [CS07a, MAh04, MS02d]. Decidability [Kus02].

Deciding [Bau05]. Decimal [BJvd02].

Decimisation [BZ03]. Decimation [Fl00]. decipherable [AS0M, Sav04].

Deciphering [Eri02, KB07, Ark05, Bau08, Lov01, NS01a].

Decision [DJ06, GR04, KMO4a].

Decisional [CU01].

Decisions [Coc02a, Sch07]. Decodable [Yek07].

Decoding [KY02b, LGZ01, LGZ02, Rai00, AGKS07, Bul09, Eva09].

decomposing [FP09]. Decomposition [BR09, CL04c, SC02c]. decompositions [vDKST06].

Decorrelation [CLLL00, Vau01]. decrypt [Bih02].

Decrypted [Ban00, Ban02a, Bau07, MB01].

Decryption [Bar00b, BST02, CS03a, CDD07, FPS01, HGNP+03, Int00, KCJ+01, Ano08a, Che01e, DZL01, GH08, Mil03, OS07, Shp04b, SWH+09, Wh09].

 Decryptor [TPS01, Zol01].

DeCSS [Coc02a]. Dedicated [ISO04]. Deep [CMS08].

Defeating [CSK+08]. Defective [BTTF02, Dav01b, Dav01c, KLR09].

Defending [NRR00, Pro01].

Defense [GK02, HW01, Mir05, Wy05, Bo102].

defenses [SL06]. defined [Yas08].
**Definition** [YWD08, SNI00]. Definitions [Uni01, AH05]. **Definitive** [BS01a, BSB05, Gar03b]. defying [HRS08]. **Degenerate** [Ber09a]. Degradation [BSC01a]. **Degrees** [Sat06]. Déejá [DP00]. DeKaRT [Gol03]. Dekker [Irw03]. Delacorte [Imr03]. Delay [WRW02, NS01a]. Delayed [JM07]. delegated [CL04c]. Delegation [WN02, ZP05, MW06]. Delhi [JM03, RM04]. Delivers [Ano02e]. Delivery [NZCG05, RMCG01, DY09a, NZS05]. Delphi [TEM +01, Hei01]. Demand [BD03, CMB +05, SEF +06]. Demilitarized [Kum07]. Democracies [CZB +01]. **Democracy** [CTBA +01]. Demography [Coc03]. Demons [Mos06]. demonstrably [HL06]. demystifying [RR04]. **Deniability** [Pas03]. Deniable [Nao02, CCK04a]. CSK +08, DG05, LC05b, YRY +05c, Zha06].

**Denial** [Mah04, Nik02a, Nik02b, PKBD01, Ril02, Mir05]. Denial-of-Service [Nik02a, PKBD01]. Denmark [Cra05a, TBJ02]. Denver [ACM01b, Scho04b, USE00d]. Department [Bol02, Eri01]. Dependable [NAB03, And08b]. Dependent [Gol03, WOS5, BPS05, SK03]. deployed [BDET00]. Deploying [BH00b, GSB +04]. Deployment [CL07, KDO01, Mur01, Sin01a, App05, JRR09]. Dept [Uni01]. **Depth** [BI05a]. Derandomization [BOV03, BOV07]. Derivation [DGH +04]. Deriving [BJP02, CUS05]. DES-encrypted [Bih02]. DES-like [Egh00, EBS01]. **Desch** [LBA00]. Describing [PS06]. Description [Lav06, MH05]. **Descriptors** [DN07, SP04]. Design [Abd01, AADK05, Ano02e, ADD09, AIK +01, ARC +01, Bar00b, Can01b, CCDP01, Cim02, CB01, CS03b, CM +05, CLZ02, DR02a, DR02b, DS09, DF07, EHK +03, FF01a, FZH05, GSS08, Geb04, Gut02b, Gut04a, HRL09, Hro05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04c, LB05, MKP09, MP00, Nd05, NSS02, Rhi03, SJT09, SPG02, SQRL03, Uzu04, WZW05, WW08, WLLL09, ARJ08, Ade09, CMS08, GG05b, Gut04c, HC04a, Hut01, KSF00, MI09, MWM01, SVE09, YCW +08, YC08]. **Design/CPN** [AADK05]. designated [LV07]. Designing [HBC +08, MRT10, TCR03, C +02, CG05, Lan00c]. Designs [Bee05, CC02a, Bli08, Des00a, HN07, WL07a]. Desktop [Mun08, BDET00]. Desmedt [CHH +09]. Desynchronization [CDTT05]. Detached [Sha01c]. Detailed [Lut03]. Details [Scr01]. Detect [FOBH05]. Detecting [CMS09, FG01, JQYY01, Har07a, LHL04a]. Detection [AS01b, AD07, BB00a, BKM07, CH01b, CZK05, JT05, KK03, SKQ01, SY01a, SLT01, ST01c, TZD05, TMM05, WG05, YI01, Zan01, Bej06, BBK +03b, HLL +02, Men03, NN02, WMS08, YW06, ZGTM05]. Detection/Correction [SKQ01]. Detector [BSC01b, DN07]. Determined [KKH03]. Determining [KS03, LQ08, OS07]. Deterministic [BK06a, Her06, KZ03, KZ07, May04, BK07]. dev [BH05]. Developers [An006c, Dew08, MK05b, Nis03a]. Developing [MV03b, Cra05b, Gal02, HL06]. Development [An02b, CN +02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a]. Developments [An03b, Pre07, Sha04a]. develops [Pau02b]. Deviates [Rad55, Rau01]. Device [Ric07, TO03b, WPS01]. Devices [BCH +00, CFRR02, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KHD01, MV01, MRL +02, SCF01, WC01a, An06a, CMS08, CF07, DMT07, sHCP09, Tse07, YC09b, ZYW07]. Devil [Bla01c]. DFT [Che08a]. DH [Lys02]. DHIIES [ABR01]. DHP [MSV04]. **Diablerets** [Vau05a]. **Diagnosis** [An04b, BK06b, XNK +05]. Diagnostics
Diagonal [PJH01, PJK01].
Dickson [SZP02]. Dictionaries [AGT01].
Dictionary [BPR00, BCP02b, CS07b, DJ06, Pho01, NS05a]. did [MH09].
Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b].
Dies [Bar00a, Coc01a, Mat05].
difference [PBMB01, dW02].
Differencing [LS08, WWTH08].
Different [CGMM02, Sma01].
Differential [Ava03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eke09, Fur02a, Gra02a, HLL+01, HSM+02, HHK+04, IIT03, JT01a, Kan01, KM02, KCP01, LHL+02, MP06, MM00, MM06, MG08, PSC+02, PQ03b, SK01a, SKU+00, SK101, YSD02, vW01, BF01a, CUS08, Che08a, DLP+09, Egh00, EBS01, Pha04, SLL+00, TM01].
Differential-Linear [BDK02a].
Differentials [BF00b].
Difficult [Bud00b, MT02].
Difficult-to-pass [MT02].
Diffie [Jan08a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKRT08, FS01b, GR04, Kl01b, KK02, KMK04a, Kra03, Kra05, Mis08, Tsa06, YRY05c].
diffuse [Wal04].
diffuser [Fer06].
diffusing [She01].
digest [MSP09].
Digit [KWP06, Tan07a, BG09, HKP05, Kir01b].
Digital [ANS05, AvH00, AR00, AS08, Ano01g, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00b, CCH05, CC09, Che01b, CSF01, CMB02, CBM+08, CZB+01, CGJ+02, DSP01, EIG01, Eng00, EHK+03, HSZ00, HZS01, Han00, HS01b, HHPG+03, HW01, HL01, JRB05, KZ01, Kao01, KCC02, Kuh00, Kwo02, Kwo03b, LZX+01, LLL+01, Lin01b, LWL09, LL01, Lut03, Mad00a, MM01a, MM02, MSH10, Meh01, PL01, PJH01, PGC01, PZL09, PBM+07, Ram01, RdS01, RS01, Sam09, Sch00d, Sch06b, Scr01, Sha01e, SC02a, Shi08, SLT01, Sug01, TM001, TJC03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03a, WC04, Wya02, XFZ01, XYL09, YWWS09, YYDO01, YYZ01, ZWC02, Zho02, ZCW04, AAP07, A08, Ano00i, Ano01p, Ate04, BLH06, Bra01a, Cal00a, CS07a, CWH00, CL00, CJ05, Cho07a, Che00b, Die00, DVP09].
digital [FB01, GGK03, Gil07, HRJ09, HLC07, HHL00, HH05, KP00, LG04, LG09, Lev01, LL06b, MKY08, NRR00, PC05b, PLJ05a, PV08, QC05b, Ree03, Sae00, Sha01d, Sha04b, Sha05d, SCL05, TCD02, TND+09, UP05, WQ08, WHLH03, WC05, XC05, XMST07, Ano09b, Ano13, BCKK05, CDS07, CLK05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].
Digital-Audio [WNY09].
Digital-Signature [Eng00].
Digits [Che04b, Ran55, Ran01].
Dimension [DDG+06, TZT09a, TZT09b].
Dimensions [CLR09].
Dining [KLN+06].
diplomacy [Alv00].
Direct [BMW05, KG09].
directional [PJH01].
Directions [Sha01b, DFH01].
directly [JZCW05].
Director [Mad04].
directories [C+02, Pet03].
directory [C+02].
disadvantage [CDS07].
Disappear [Per05a].
Disappearing [Way02b, Way09].
disappointed [Ste00].
Disaster [WC05].
disciplinary [SM08].
disclosure [JM07, Swi05].
Discover [Eva09].
Discovery [Bi09, HLL+02, SG07, SGA07].
discredits [Ano09c].
Discrete [CS03a, CNS02, Che04b, CCM02, Gen00b, GV05, GPP08, KC09b, LW02, LJ05, VK07, HN04, HW03a, HWR09, Hsu05a, HL05d, JLO3, JLL01, LHL03a, LLO4b, LHY05, LTH05, PLJ05a, QCB05a, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SCL05, SCS05c, Yas08].
discretized [MA02].
Discruption [Har07b].
discursive [Mit02a].
Discussion [Ano01a, Ano01b, Ano01c, Ano01j, Ano01n, Ano01f, Ano01o, KLB+02a, Mal02, Nik02b].
dish [Ano01].
dishonest [GKK07].
disjoint [Gut04c]. Disk
[Cro01, Har07b, Siv06, CS08a, Fer06].
dismantles [Hil06], dispatches [Kee05].
displayed [CGV09]. Displays [Kuh02a].
Disputed [CAC06]. Distance
[CGFSHG09, CPlX04, DM07b, DW01].
distinguished [HWW04, WH02b].
Distinguishers [HI04]. Distinguishing
[HSR+01]. Distortion [BG10, CS05c].
Distortion-Free [BG10]. Distortions
[HH09, SDF01]. Distributed
[BCS02, BT02, CLK01a, CS08b, CD01a,
DS03, EP05, FM02a, FS01a, GJKR03,
GSCV02, GTH02, LLYO, SCFO1, WT02,
And08b, AFGH06, BDET00, CO09b,
FM02, KKL09, LN04, MTP08, PA09,
PM08, PS08a, RAj06, WZB05, YbJf04].
Distribution [BDF+01a, BOHL+05,
BBB+02, BGM09, BSN00, FS01a, Ina02a,
Ina02b, Ku02, LLL02, NA07, Sch01a, YI01,
ATS04, Asl04b, Bad07, CYH04, CDD06,
GL06b, MP08, SLP07, Shp01, Shp04b, SY06,
WHHT08, YS04, ZGL01]. Distributions
[CY08]. Diversity [Kun01]. Divide
[SKQ01]. Division
[HZSL05, KKY02, Tan07a, Che08b, MN14].
Divisor [KM01a]. DL
[HRL09, PLJ05b, Sc01f, Sc01e, WMDR08].
DL-based [HRL09, PLJ05b].
DL-encryption [Sc01f]. DL-keys [Sc01e].
DL-STD [WMDR08]. DLP [MSV04].
DM [Eag05]. DNA [AEH17, GPX08]. DNF
[BN05]. DNS [Her09b, Kle07].
DNS-based [Her09b]. DNSSEC [Gue09].
Do [Bur06, HSR+01, HR04b, Win01, BB79].
Dobb's [Dr.00c]. Document
[ISO05, PJK01, AW05, AW08,
DGK+04, GA03, ÚGO8]. Dodging [Phil06].
Does [AB01, Pie05, Con09, WA04]. Doing
[BM01a]. Dolev [BPS08, BDNN02, ZD05].
Domain [AS08, Bar00c, BSC01a, BSC01b,
BSL02, CJK+04, Cor00b, Cor02, DOP05,
DNP07, GW01, ISSZ08, Kuh02a, Lan00d,
LZ01, MM01a, OMT02, PBC05, SOHS01,
SDFH00, ZLK02, BR06, CS05a, DSP01,
EKRMA01, Zir07]. Domains
[BR01, CLK01a, CLK01b, VAT01].
Domingo [CKN06]. Dominic [Rot07].
Dominica [PY05], domino
[LLLZ06a, LLLZ06b]. Don't [Win05c].
Don'ts [FSSF01]. DONUT [CLLL00].
Door [SF07]. Doors [Eri02].
DOS-Resistant [Ano01f, ANL01]. Double
[ADD06, CY08, CMJ03, Coo02a, DIM08,
GH08, GB09, Hau06, JSW05], double-base
[DM08]. Double-Gate [Cco02a].
Double-Size [CMJ03], double-trapdoor
[JSW05]. Doubling [FV03]. Douglas
[Sp03]. Down [BBPV00, Coo02b, Ano00g,
Ano03d, Ano03a, Po03, PBS01, GST05c].
Downwards [FV03]. DPA [SGB01, TV03].
DPA-Based [SGB01]. Dr [Ano03g].
[Dr.00c]. Draft [Mad00b, Ste00, Dwo03].
drastic [Sug03]. drawn [vOT08]. DRBG
[Hir09]. Dress [Ahm08]. drinks [Ano03d].
Drive [NP07, Kor09]. DSA
[MR01a, SA02, Sha01d, TvdKB+01].
DSA-type [Sha01d]. DSEA
[LLLZ06a, LLLZ06b]. DSP
[Geb04, WWGP00]. DSP-embedded
[Geb04]. DSPs [WWGP00]. DSS
[Ano09b, Ano13, FIP00, Nat00]. DTD
[PK02]. Dual [HLC07, KHY04, LKL05,
SFO7, WCJ09, ST03a], dual-field
[ST03a]. Dual-Pair [WCJ09]. Dual-Tree
[LKL05]. Dual-wrapped [HLC07]. Dublin
[Phil01]. Dummies [Cob04]. Dumb [KCJ+01].
Dunaynir [MAa05]. d'une [Car00].
Duraheim [MAaTxx]. Durayhim's
[MAaT04]. during [AJ08, Bec02, WA07].
Dust [KGS07]. Dutch [dL00]. Duty
[ZGLX05]. DVD [Ge03, Per05b]. Dwork
[DNRS03, GK05, Zha06]. DWT
[LHS05, PBC05]. DWT-Based [LHS05].
Dynamic [AFB05, BNP08, BCP01,
BFC02a, BF07, CL02a, CW09, CCD+04,
CTT07, GTH02, HQ05, Pat01, Sug03, TT01,
BBG\textsuperscript{+02}, GL06b, HW03c, LCP04, LLY06, LCK04, LCC05, RG05, Yi04].  
\textbf{dynamic-key}  
[LC04].  
\textbf{dynamics}  
[BGP02, sHCP09, jLC07, MR00].  
\textbf{dynamics-based}  
[sHCP09, jLC07].  

\textbf{E-business} [Poh01, HHSS01].  
\textbf{E-Commerce} [Kir01a, TM01, BM03a, Gra01, SN07, Sta00, MY01].  
\textbf{E-Goods} [NZCG05].  
\textbf{e-Government} [RM02].  
\textbf{E-learning} [CAC06].  
\textbf{e-mail} [Che01f, LL04c, NZS05, Smi03, All06, ANR01, KS00a, Law05].  
\textbf{e-mails} [LG09].  
\textbf{e-payment} [Has02].  
\textbf{E-Security} [NDJB01].  
\textbf{E-smart} [AJ01b].  
\textbf{E-Vote} [Che07b].  
\textbf{e-voting} [CJT03, Cha04].  
\textbf{E-Wallet} [ETZ00].  
\textbf{Early} [ASW01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Cal00d, Smo04, ZGTG05].  
\textbf{Easier} [Pau09].  
\textbf{Easy} [GR04, Hos06b].  
\textbf{Eavesdropping} [Kuh02a, Kee05].  
\textbf{ebanking} [WDCJ09].  
\textbf{Ebook} [Ano02d, WWL02].  
\textbf{EC} [SF07].  
\textbf{ECC} [BWBL02, CL09, Mis08, Tsa05].  
\textbf{ECC-based} [CL09, Tsa05].  
\textbf{ECC2K} [LM08].  
\textbf{ECC2K-130} [LM08].  
\textbf{ECCV} [MJ04, TB01].  
\textbf{ECDSA} [ANS05].  
\textbf{Eclipse} [Coc02b].  
\textbf{ECMA-305} [ECM00a].  
\textbf{ECMA-306} [ECM00b].  
\textbf{Economics} [Ble07].  
\textbf{ECPP} [Che03].  
\textbf{Ed} [Gum04, Nis03a].  
\textbf{Edg} [Sta05].  
\textbf{Edinburgh} [RS05, Pem01b].  
\textbf{Edit} [CGFSG09].  
\textbf{Editing} [MAaTxx].  
\textbf{Edition} [Cho08a, Irv03, Spr03].  
\textbf{Editor} [MFS+09, Sak01, KP03, SK06].  
\textbf{Editorial} [Eri01, Eri02, FOP06].  
\textbf{Editors} [BK06b, PTP07, SJ09, SG08].  
\textbf{EDK} [Ano02e].  
\textbf{Edu} [Dw03, Pag03].  
\textbf{Education} [Puz04, RC06, CAC03].  
\textbf{Effect} [AEV07].  
\textbf{Effective} [CDR01, PD07, Sen03, SL06].  
\textbf{Effects} [BBGM08, Har00, GJ04, SN07].  
\textbf{Efficiency} [III00, GGKT05, SLG05, GT00, GGK03, KT06, YTH04].  
\textbf{Efficient} [ACS02, ABRW01, AEM09, BCGH11, Bai01b, BINP03, BKLS02, BR00a, BGHP02, BDSV08, BGK03, BS00a, BF01c, BGH07, BB00b, BCDM00, CKPS01, CL02a, CCMT09, CCD07, CL01b, CPhX04, CM05a, CJ02, Chi08a, CJ05, CT08b, CKK03, Cou01, Dam00, DN03, Dhe03, FF00, Fis05, FS01c, GL01, GC01b, GTH02, GST04, GBKP01, HCJ02, HSZ01, Has01a, HI04, HS00, HW04, HZSL05, HL07, Hüh00, HS07, Jua04, KOY01, KOY09, KLY02, KO03, KHD01, KKH03, LS01, LCK01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, MN14, Nd05, NSK05, OS01, PCS03, PBD05, Ram01, RSQ03, RDJ01, SM01, SM03a, SW06, SRQ03, SSNG00, Tsa08, TC05, WHL05, WYY05d, WH10, WC01a, XB01, XS03, YWD08, YL05, Zan01, Zho06, ACT05, AFB05, Bla01b, CC04b, CC05c, CY05, CH05, CLC08, DS09].  
\textbf{efficient} [Dew08, DwWmW05, FP09, FSM01, HHG06, HC04a, JW06, KHYM08, LPV09, LS09, LCK04, LHH04, LYC02, Mic02a, MSP09, NR04, PCC03, RG05, RBB03, SLP07, SKW07, Sha05b, SC05a, WK05, XC05, Yan02, YTW05, YC09a, ZSN05, ZYW07].  
\textbf{Efficiently} [IKNP03, NNT05, AGK07].  
\textbf{effort} [Weh00].  
\textbf{Efforts} [Pau02a].  
\textbf{Eggs} [Wei06, Wei05].  
\textbf{EGPGV} [MFS+09].  
\textbf{Egypt} [EBC00, Imr03, Sin00].  
\textbf{Eighth} [ACM06, B02, ELvS01, IEE01b].  
\textbf{Einstein} [HR13, MNT00].  
\textbf{EJB} [TEM01].  
\textbf{Ekert} [Duw03].  
\textbf{El-Gamal} [EKRMA01].  
\textbf{Election} [JLL02, Cal00b].  
\textbf{Elections} [Cha04, PvS01].  
\textbf{Electrical} [Wal04].  
\textbf{Electromagnetic} [SFM09, QS01].  
\textbf{Electronic} [Bl07, CLK01b, CM02, Dur01, Höö01, ISO05, IY00, KMO01, KS02, Lan04b, LLL02, Mad00a, MNG02, Rub01, RMCG01, Str01a, YKM01, ZYM05, AvdH00, AAKD09, Cal00a, Cas03, EY09, FBO1, HJW05].  
\textbf{element} [MS02d].  
\textbf{Elementary} [Sin09, Ste08, Tat05].  
\textbf{Elephant} [Fer06].  
\textbf{Eleven} [All03].  
\textbf{ElGamal} [BJN00, CL02b, CWH00, HL04, LTH09, SJ00].
ElGamal-like [CWH00, HL04]. Elizabeth [Bud06]. Elliptic
[AD09, AN05a, BAI01a, BNP03, Bar00a, BBGM08, BMM00, BS01d, BMN01, BB00b, CQS01, CFA06, GLV01, Gan02, GP08, HYZ05a, HMM01, HMV04, HM02c, Hus04, JT01b, JT01a, KMB09, KPMF02, Kid02, KSZ02, LW02, MP01b, Mös02, Kir03, OTT01, OS01, OT03b, PW03, RSA03b, RS04, RS01, Sat06, Sil05, Was08a, Was08b, WP01, X01, YZ01, vT01, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DWW05, EKH04, GCK01, Hsu05a, HL05d, JMV09, JW06, LL04c, LWZH05, Mis06, MS04, ST03a, SS06, SH05, Sma01, SC02b, SCL05, SL05, TC05, Van03, Ver01, YC09a, YC09b, YZ05a, ZSZ01, ZL05, ANS05, BW02].

Elmau [IEE01b]. Else [FL01b]. elude [Che01f]. EMA [QS01]. Email [ES00b, Gar03a, Her09b, Luc06]. Email-Based [Gar03a]. emanations [ZZT05]. Embedded
[An01c, An02d, An02e, BBGM08, Dri02, DV08, GSS08, JT05, JQ04, KKP02, LPW06, Nd04, RS05, SPGQ06, WKP03, YSS01, ARJ08, BGM04, Fox00, Geb04, KVN09, KP01, KNP01, KP03, MB04, Nis03a, TKP08, XQ07, Fin02]. Embedding
[AAK09, JX05, JG07, LSC03, Sal03b, WW02, WC04, CO09a, KC09a, Wan05]. Embrace [CNB02]. Embracing [An03d]. EMD [BR06]. Emperor [Smi01b]. Empirical [HW03b, Goo00]. empirically [SS03].

employee [You04]. Emptiness [DIS02]. Emulex [CZB01, CTBA01]. Enabled
[Por06, CCCY01, DY09a]. Enabling
[Web02]. encapsulation [CH09, KG09]. Encipher [BR00a]. Enciphering
[HR03, KT01]. Encode
[BR00a, BKN04, AN08c]. 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, BB01b, GLS03, CD01b, Hug04, Lan04a, LH07, MMZ00, NNAM10, RMCG01, Sta02b, Wat01, WRW02, Whi09, Woo00, AMB06, An06a, Bib02, BN08, CCM09, CDD05, CSK06, FJ04, HLM02, He04a, LHL04b, LSH00, MW04, Pet03, UG08].

Encryption [Pro00, RC01, Zho06]. Encryption
[ABC05, Abe01, AS01a, Abe04, AEH17, AP09, AB01, AD02, An03, An01g, An01h, An01i, Ave02, ANR01, AF106, AF03, Bar00c, II00, Bau02b, BN00a, BR00a, BBMM00, BB01d, BU02, BF01b, BF03, BB04, BG05, BCHK07, BG07, BPR08, BB03, BNP03, BD03, BKY02, Bur03, Cal00d, Cal00e, CD00a, CS03a, CHK03, CHK05, CGHG01, Che01a, CCTL01, Chi08e, Cho08a, CMRD06, Cla00a, Coc02b, Coc01b, CJNP00, CH01b, CD01n, CS02, CS03b, Cro01, Curt05, DS03, DR01, DR02b, DR02e, DN05a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DFK03, DK05, DS05b, Dri02, FIP01a, FL01a, GC01a, GS00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HSH08a, HS02a, HYZ05a, HSH02, HSH06, HK01, HW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03].

Encryption [HL02, HGP04, HLM05, HLC08, ISSZ08, Jol03, Jol01, JK02b, JK02c, JM02, JKR01, Jut01, KBD03, KSY01, KS00a, KY01a, KKA05, KKJ07, Kos01a, Kral01, Kur01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LLL07, Lin03, LNP02, LM05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, MÖ03a, Mor05, Mö01a, MS09a, NIS00, Nam02, NZCG05, NZ05, NP02b, NIE02b, PV06b, PM00, Pau09, Pem01a, PZL09, PDMS09, Pha04, Por01, PS00, Pre01, RM04, RK06, RDJ01, Sam01,}
Scho06b, SJ00, Siv06, SB00, CAC06, SRQL03, SPGQ06, SBZ02, Sye00, TV03, Uni00a, Uni00c, Uni00d, Uni00g, Uni00h, Ust01b, VMS05, WZW05, WBRF00, Wri01, YEP+06, YW06, ASW00, Abd01, ABHS09, AMRP00, ABW09, Ano00e, Ano00c, Ano00f, Ano00g, Ano00h].

encryption
[Ano00j, Ano02a, Ano03g, Ano06d, App05, Ate04, ACDm05, AFGH06, BPS08, BKN04, BR04, BBN+09, Ber09a, BBK+03b, BIR07, Bla00, BJ00, Bro05b, CG06, CS08a, CBSU06, CHC01, CKRT08, DZL01, DL07, DRS05, DFW01, Fer06, FB01, Fox00, FMS05, GMR08, GGK03, Gen09a, Gen09b, GKM+00, Gou09, Gua05, Gut04c, HSHG08b, HSHG09, HS02b, HHYW07, HCD08a, HCD08b, HAU04, HWW02, Hsu05a, Hwa05, HL05c, HL05d, IM06, JK01a, JK01b, JXW05, JSW05, JZCW05, KY00, KJ01, KS06, KHL09, Kor09, KW00, Kre05, K+08, Lau00, LV07, Lee01, LCP04, LJ05a, LMC+03, LLLZ06a, LLLZ06b, LLCL08, LB05, Lu02, Lu05, LK01, LWK05a, Mad04, Mar05b, Mat02, Mi01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pau03, RG09, Rhi03, RBB03, RSP05, SN00, SKW+07, Scho0a, Sch01c, S+03, Scho0a].

cryption [Sch04b, Sch05a, Sch01d, Sch01f, SH11, SM11, SR00, SVEG09, Sph04b, SK03, Ste00, SP03, SW+09, Tan01, TTZ01, TOEO00, TM01, TLH05, Uni00b, UP05, VKS09, WQ02, Weh00, WN95, Wol03, WHO2a, XY04, XSWC10, YG05, YZEE09, YCO7, ZLG01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CHKO08, CJH+01a, RR04, Uni00f, Wue09, Jan08a].

cryption/cipher [Hau04].

cryption/decryption [OS07].

Encryptor [LMP+01, TPS01, Ano00a].

Encryptor/Decryptor [TPS01].

Encyclopedia [Bid03, vT05]. End [KCD07, Per03, SKKS00, WWGP00, YSR01, AMB06, SU07]. End-to-End [YSR01, AMB06].

End [K+02].

Endomorphisms [GLV01]. Endpoint [Kad07].

Enemies [DM07b]. Energy [GC01b, Ino05, LPV+09, SLP07, Mis08].

Energy-efficient [LPV+09].

Energy-security [Ino05]. enforce [SN04].

Enforcement [GN06]. enforces [BP05].

Enforcing [GMM08, HRS08].

Engine [Fri01, MMH02, DP04, SLH07].

engineer [Pau02b, SN04].

Engineering [CNB+02, MNT+00, MYC01, Pem01b, Roy00b, SM07b, TR09a, TR09b, VH09, And08b, EC05, Jen09, Man08, Wal04].

engineers [Pau00]. engines [PM08].

Enhance [ZWC02].

Enhanced [JMRW01, LHL04b, ZGLX05, CZ03, McK04, OP01b, TWL05, WLT03, WHH05, ZSM05].

enhanced-security [OP01b].

Enhancement [CJ05, FLZ02, LSH03a, LSH03b, SLH03, YW04a]. 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, Th03, W101a, Win05b, Win00].

Enigma [Kap05].

Enough [CNB+02, Pat03a, Ano03c, YJ00].

Enrolment [HWH01].

Entangled [Bar00c, LB04].

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

Entropic [DS05b].

Entropy [DS05b, EHS00, LH07, JRS09].

Entzifferung [Bau08].

Environment [BST03, DeL07, Hs01b, LSVS09, IM06, KKL09, KB00, Rhf03, Whi09, ZBP05].

Environmental [PS05].

Environments [CJ04, LKHL09, BGM04, MS05, SBG05, SBG07, SN04, YCS09, YbJ04].

ephemeral [Mis08].

Ephemizer [Per05a].

EPOC [JQY01].

ePOST [MPHD06].

EPR [Ina02b].

Equation [FJ03]. Equations [CP02, DDG+06, GS03, PBMB01].

Equipping [DMT07].

Equitability
SZ01, CKY05, Duj08, GD05, Shp04b.

Exponential [BYJK04, BYJK08, CY08, GKK+07, GKK+09, Shp05].

Exponentiation [KKH03, SK07, CKRT08, HGNS03].

Exponents [FS02, FS01b, BS02].

Export [Mad00b, Ano00h, Mad00c].

Exposed [Gum04, MSK03, SSS06].

exposing [YY04].

Expositive [MAaT05].

Exposure [BM03b, DSS01, KZ07, CDD+05, KZ03].

Exposure-Resilient [DSS01, KZ07, KZ03].

expressions [MW04].

Extended [ABDS01, BPS00, CM00, Cou04, DIRR05, HlvA02, HJW01, JL00, MSJ02, MP02, OST05, Wag02, BJN00, CD00a, HT04, Mis06, Pei09, QPV05, LKJL01].

Extending [ADDS06, IKNP03, Ove06, Sal03b, SS01a].

Extension [Bai01a, YWD08, BR06, CMdV06].

Extensions [ABC+05, BBGM08, CS07c, HM02b, Rot02a, Wei04, Elb08].

Extracting [Cer04a, HN07].

Extraction [DGH+04, RW03a, MB08, PBV08].

Extractors [Fist05, KLR09, KZ07, Lu02, Vad03, DW09, KZ03, Sha04a].

Extraordinary [Top02].

Extreme [Ree03, Ano02d].

Extrusion [Bej06].

Eye [Sas07, CAC03].

Eye-Opening [CAC03].

F5 [Wes01].

Face [KZ09, NH02, PK01, SBG02, TZT09b, PY08].

FaceHashing [TNG04].

Faces [NS01c, Ngu01].

facets [Rot02b, Rot03].

fact [Ano03g].

Factor [DN02b, Sas07, BSSM+07, Hen06b, Sch05c, St.00, Ste05a, YWWD08, dB07].

Factoring [BN02, KY02a, KLB+02a, KOMM01, May04, PV06b, ST03b, LTH05, LC05c, Mi101b, PLJ05a, QC05a, Sha03d, Sha05d, ZCL05].

Factoring-Based [PV06b].

factorisation [GG08].

Factorization [CDL+00, Lam91].

Facts [GO03].

Fade [CAC03].

Fail [JQYY01, SSNGS00].

Fail-stop [SSNGS00].

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, Flit02b, NPV01, SK05a, You01, Ber07, FNRC05, GBKP01, 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, HGG07, HR04a, JJK04, KKIM01, KK03, KKJ+07, LSY01, LS05b, MN07, Kiz03, SS05a, NSS02, OKE02, OT03b, PG05, RR02, Tsa06, UHA+09, Yan05, ABB+04, BMA00a, BMA00b, BMA00c, JAW+00, JJK02, Lud05, PBMB01, WW01, Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d].

Faster [Bar00c, CMJ03, GLV01, KZ09a, IV04, Oec03, Ban05, Why05].

faszinierende [Sch09].

Fat [MYC01, TvdKB+01].

Fault [Ano04b, BMM00, BK06b, BKM07, DS03, Gir06, PV06a, PQ03b, WL07b, YKLM02b, HGR07, Lin07, Pl06, RM04, YJ00, YKLM03, ZL04a].

Fault-Tolerant [WL07b, HGR07, Lin07, RM04].

Faults [GSS08, VS08].

Favour [Gen01].

Favre [MFS+09].

FBI [Mad04].

FC [Bl0a, 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, Kil05, Kim01, Men05, NP02a, Nao04, Ola04, PY05, Po06, Pre02c, RM04, Syv02, USE02a, Wi99].

Federated [DeL07, Ano04e, GT08, SMI08, SU05].

Feedback [CGFSHG09, CM03, Cou03, Ig02, Hey03, SPG02].

FeedForward [BP01a].

Feel [PM00].

Feeling [Buh06].

Feistel
Feldman [AF04b], Ferrer [CKN06], Fetal [MYC01].
fetch [HTW07], Fi [Sty04, Bar03], Fiction [Ano03g].
FIDES [ISTE08], Field [FJ03, GC01a, RDJ01, CKY07, GMG00, Has00, JL03, ST03a].
Fields [Bai01a, BT02, CU01, Che04b, CQS01, CFS05, HCK09, HHM01, KKH03, Lov01, MNP01, MM07b, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sim02, Sma01].
Fifth [ACM03b, SM07b].
Fighting [DGN03, SZ03].
File [CCDP01, GIS05, Ito01, LK01, BDET00, CSK08, HTW07, Hos06b, ISO05, MKKW00, MSP08].
Files [Tot00, Che02, Lov01].
Filesystem [Bau02b, Pet05].
Filesystems [WBL01].
Filter [LBGZ01, LBGZ02, MSN07, Sar02, CMS08].
Filter-Combiner [Sar02].
Filtered [MH04].
Filtering [SDFH00].
Final [DPR01, Dra00, GC01a].
Finalist [SB00].
Finalists [EYCP01, GKS00, IK00, IK01, Mes00, Mes01, SKKS00, SW00a, WWCC00].
Finally [Coc02b].
Financial [ANS05, Gri01, Pem01b, Wri03, Bla03, Fra01, Jue04, PY05, Syn02].
Finding [Hi04, HR04b, MP06, WYY05b, WYY05c, ZT03, SW00b].
FINDsomeone.com [Gra98].
Fine [SS01b].
Fine-Grained [SS01b].
Fingerprint [Ano02d, HHYW07, HBF09, KHY04, MMHY02, CL04d, MMJP03, UBE09].
finger-print-based [CL04d].
Fingerprinting [KT01, CT07].
Fingerprints [TK03, KLY03, Sco04].
Fingers [MMHY02].
Fine [BLST01, BR01, CU01, Che04b, CQS01, HCK09, HW005, 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, NNT05, ÖÖP03, PK03, QSR+02, Roy00a, USE00b, Wil99, ZJ04, ZHY03, AJ01a, Cla00b, Coc02a, DV05, LBA00, RH00, Uni00a, Uni00b, Uni00f, Uni00e, Uni00b, Lan00a].
First-order [Coh03, KS06b].
Fish [Fic09, Wei06, Wei00, Wei05].
Fit [CCM05].
Five [SW00a, MS02b, Rot02b, Rot03].
five-lecture [Rot02b, Rot03].
Fix [TEM+01].
Fixed [AR01, BCCN01, CKN00, LS01a, Shp04b, SP79].
Fixed-Length [AR01, CKN00].
Fixed-Pattern [BCCN01, LS01a].
Fixing [KZ07, KZ03].
FL [Des02, Jue04].
Flat [SV08a].
Flaws [Gra02a, SPMLS02, Van02, SL05a].
Flexibility [LP02a].
Flexible [CMG+01, CL01b, DGK+04, OT03a, Tsa01, BA06, KC05, LHY02, WWA01].
Floating [Ber04, NS05c].
Floating-Point [Ber04, NS05c].
Flow [BDNN02, ABEL05, FR08, ME08a, TW+09].
Flows [ECM00a, AHS08, Cer04a, Van08a].
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, CMK00, LS01a, SL01, HSW09].
Forgotten [Eag05, Kin01, OC03].
Form [AD10, CH07c, OS01, LKYL00, Mic01].
Formal [BGB09, Bel07b, BCHJ05, BCJ+06, CL05, DK508, GOR02b, HG03, Lan00d, Mea01, YWD08, ABHS09, JW01, Mea04, Pau01, SW02, ZLX09, ZL04b].
Formalizing [HM01a].
Formally [BP02].
format [ISO05, RG05].
format-string [RG05].
Formation [RW03a, Luk01]. Formats [GIS05]. Former [Mad04]. Forms [JT01b, LLL04]. Formula [Kog02]. Formulæ [CH07b, WPP05]. Formulas [BGN05]. Formulations [AHRH08]. Fort [Smi03]. Forums [HiI06]. Forwards [AR00, AFI06, CHK03, IR01, HCD08a, HCD08b, SY06, ZYW07]. Forward-Secure [AR00, AFI06, CHK03, IR01]. Forward-Security [BY03]. Forwarding [KCD07, Kra02b]. FOSS [Bol02]. Foundation [Bar00a]. Foundations [DKK07, Gol01b, Gol01a, Gol04, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Nie02d, Sal05d, Kat05b, Puc03]. Founder [Bar00a, Ano03g]. Four [LXM+05]. Four-Layer [LXM+05]. Fourier [Cho07a, DSP01, DNP07, KC09b, LPZ06, SP04]. Fourteenth [USE00c]. Fourth [ACM02, ACM05b, DFCW00]. FPGA [Ano02e, CC02a, GBS01, CG03, CNPQ03, EYCP00, EHKK04, KMM+06, KY09, KBM09, KRS+02, LP02a, MM01b, MM01c, OTT01, OOP03, Pat01, PBTW07, QSR+02, TYLL02, TPS01, USS02, WW00]. FPGAs [AD07, DPF01, MMT09, RSQL03, SGM09, SK05a]. Fractal [AA04a, JLM030, WC03a]. Fraction [Wal03]. fractional [DSP01, SSST06]. fractions [Dan02]. Fragile [CC09, CH01b, CTO9, Nak01, PKJ01, LYGL07, SY01b]. Frame [LHS05]. Frames [HW05]. Framework [ANRS01, GL03, GOR02b, Hum05, NMO05, NP07, PS06, RS00, SHY02, ZYN08, AHK03b, AYO06, CCCIY01, CP07, CC04c, DMSW09, GJJ05, GL06a, GM04, JEZ04, KNS05, MS09b, MBS04, YCW+08, HF00]. France [ACM04a, ACM05a, AJ01a, AJ01b, GH05, KNP01, NP02a, PPV96, KM07]. Francisco [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b]. FranzSteiner [Eag05]. fraud [Ano03a]. Fred [Bar00b]. Free [AP09, Ano02e, Bao01a, Bao01b, BGI08, Coc01a, CNV06, DG02, HS00, HM01b, JP03, Jut01, Fox00, KS06b, SBG05, Bo02]. FreeBSD [Coc01a, Mur02, Siv06]. Freedom [Uni00a, Uni00c, Uni00d, Uni00g, Uni00h, Mil03]. FREENIX [USE01b, USE02c]. French [Wri03]. Frequencies [DD02]. Frequency [OMT02, Sak01, SOHS01, CS05a]. Frequency-Domain [OMT02]. Frey [Was08a]. Friar [GG05a]. Friendly [CTY09, CRSP09, Hsu05b, HL05b, SZZ05, WLT05a, WC03b, YY04b]. fries [Ano01k]. FrontPage [WWL+02]. FSE [Bir07, DR02c, GH05, JH03, Mat02, RM04, Sch00b, Sch02d]. FTC [Ste05c]. fuels [Mad04]. Full [Cor00b, DOP05, LKH09, WYY05b, WYY05c, BI04, CS08a, HS02b, LKH+08, Ow09]. full-encryption [HS02b]. Full-Round [LKH09, LKH+08]. Fully [BL08, FS01a, Gen09b, KPMF02, RG09, Gen09a]. Function [BRSS02, CDMP05, Fiss01b, Flu02b, GIS05, HNO+09, HPC02, JH03, Kan01, Kil01b, Nie02c, RB01, Yan05, CHY05b, CJ04, HR07, LW04, LPM05, Tsao8, WWTH08, YW05, YRY05b]. Functionalities [PS05]. functionality [ETMP05]. Fundamentals
Funds [Coc01a]. Further [JS05, JPL04, LL04a, LL05c, Ano09c, MP07, YRY05a]. Fusion [KZ09, TZDZ05, ZS05, BG09]. fusul [MAaT05]. Future
[ASW+01, Ano02f, Joh00, LNP02, NFQ03, Sch00e, Ano05b, HP00, LPW06, SK03]. Fuzzing [SGA07]. Fuzzy [SH11, HS02b, NC09, SM11]. fuzzy-based [NC09].

G [Coc03, For04, Was08a]. Gaitherburg [SMP+09]. Gamal [EKRMA01]. Game [DHR00, LM02, CAC06, BR04, Gou09, HCBLETRG06]. game-like [Gou09]. game-playing [BR04]. Gamers [MP00]. Games [KN08, HCBLETRG06]. Ganesh [For04]. Ganz{´u}a [GPG06]. Gap [OP01a, PWGP03, RW03a, Sch02, Sch04d].

Gap-Problems [OP01a]. Gate [Coc02a, GC01a]. gates [TWM+09]. Gauging [PvS01]. Gauss [KKH03]. Gaussian [EKRMA01, JL03]. Gbps [TPS01]. GCD [JP03]. GCD-Free [JP03].

GCM [KS09a]. geeks [McN03]. Geheimschreiber [Joy00, UW00]. GEM [CHJ+01a, JMV02]. gems [Six05]. General [AB09, CDM00, DN00a, ESG+, GMP01b, Kog02, Lin03, MND+, Sal01a, YC01, HCBLETRG06, IY06, JL03, LJ05a].

General-Purpose [ESG+05]. Generalisation [DJ01]. Generalization [YYZ01, HWW02]. Generalizations [LD04, LS08]. Generalized

[KSR02, Mic02a, TC01, T01a, Wag02, WHLH05, Elb03, LKYL00, LWL09, Shi05]. Generate [HSR+01, Wer02, FSGV01]. Generated

[ADD09, MRL+, XXYX11, RBF08]. Generating

[BMK00, BCDM00, GG01, MFK+, SS03]. Generation [ACS02, BCCH11, BH05, BK06a, CS03c, ESG+, GJKR03, GL01, GW01, MR01a, Ram01, TL07, TV03, WP03, WHLH05, Web08, WS02, Ano04f, BK07, BG08, BF01c, ISTE08, LS05b, TNG04, Van03]. Generator

[ADD09, BP01a, DI05, Die03, DGP07a, DGP07b, DV08, EHK+, Gen00b, GM02a, Gol01c, GPR06, Int03, Kel05a, Kel05b, LMHCETR06, LV04, NNAM10, SY01, SDFD06, TWNA08, TZE09a, TZE09b, ZKL01, Aam03, ACTZ05, Bel08, BG08, BG09, BG07a, CFY+, DGP09, GB09, HG05a, HLwWZ09, JAW+, KH08, KSF00, LGKY10, MRT10, Pan07, PSG+, PLSvdLE10, PSP+, PC00, RGX06, SH11, SM11, SR07, SB05, UHA+, VW08, XSWC10, VKS09]. Generators

[BST03, BK06a, BL08, CF01b, CS05b, Fin06, Kral02a, LGZ01, LGZ02, LS05a, MH04, RSN+, Vav03, BK07, BPGS05, CO90b, Sti11, SK01b, Tsa06, YZE09]. generators-part [SK01b]. Generic

[BN00a, DOP05, GGK05, HLL05, Mar02b, M01, GT00, M08, Sch01f, Sch01e, XLMS06, CHJ+01a]. Genetic [HSIR02, LMHCETR06, CV05, SCS05a, WJP07].

Gennaro [Miy01]. Gennaro-Krawczyk-Rabin [Miy01]. gentle [RR03a]. Gentry [Hes04a]. Genuine [HR13]. Genus [CY02, GHK+, Wen03]. Geometric [GTTC03, HH09, LLS05a, LL05c, LJ05b, SDFD01, CJT01].

Geometrical [LWS05]. geometry [PPV96, WW06]. George [Gum04]. Georgia [IEE09b]. German

[Sch09, Ano04c, Baut08, Lin02, Mor05, Sal00b, Sal00a, Win05b]. Germany [DRA05, Duw03, FLA+, WK03, IEE01b]. Geschichte [Sch09]. Get

[Coc01a, WD01a, Cia00b]. gets [Bor00]. Getting [Kar02, PM00]. GF

[BINP03, KPMF02, KLY02, KKY02]. GH [GHW01]. GHS [Hes04b]. giant [Lam07]. Gibson [Ove06]. Giesbrecht [CHH01]. Gigabit [CGBS01]. Gigabits [HTS02]. Give [CNB+, Given [Wal03]. Giving
[Tee06, Wu01]. Global [Ahm08, LWS05, Por06, Ano00b, BK00, Kee05, KB00].

Globus [MJD01]. GN [SC05b].

GN-authenticated [SC05b]. Guana [For04]. GNU [Coc01a]. GnuPG [JKS02, Sti06].

GNY [Tee06]. Go [Bur06, CZB01, HCBLETRG06]. Goals [PHM03, Phi06].

Gold [Boy01, For04, Tse07]. Goldreich [Kat05b, Lee03b, Puc03, AC02].

Gong [GG01]. Good [CB01, Kid02, MP06, GG05b, vT01]. Goodness [CMB05]. Goods [NZCG05].

Google [Con09, Law09b]. Googling [Con09]. GOST [SK01a].

GOT [SC05]. Government [IY00, RM02, Lev01, LCS09]. Governments [Ano00g].

GPG [Bau01a, Bau01b, Luc06]. GPS [CKQ03].

GPT [Ove06]. GPU [BCGH11]. GQ [BP02].

graduate [GV09]. Grafton [Pag03]. grain [Rhi03]. Grained [SS01b]. Grand [Syv02].

granted [Ano00h]. Graph [CGFSHG09, GTTC03, HM02b, VVS01, YKW01, CTT07].

Graph-Based [CGFSHG09, HM02b, CTT07]. graphical [vOT08]. Graphics [CK06, DNP07, MFS09].

Graphs [NNT05, Ust01b, JMV09, WGL00]. Gravrilenko [Puz04]. Gray [FGD01, Har05b].

Gray-Scale [FGD01]. grayscale [YL07]. greatest [Bel07a].

Greece [ACM01a, KGL04, SM07b]. greedy [HKPR05]. Green [TR09a, TR09b].

GREMLIN [Hs01]. Grenoble [ACM05a]. grey [BDN00, SCS05a]. GRH [JMV09].

Grid [ACM05a, MJD01, SEF06]. TLC06, ZBP05, Cha07, CJK04]. GridOne [YC09c].

Grids [CTY09, MPPM09]. grip [Buh06]. Gröbner [CCT08, FJ03, Fau09].

Group [ANRS01, AAFG01, ACJT00, BBS04, BCP01, BCP02a, BCP02b, CD00a, CvTMH01, CH01a, HSHI02, HSHI06, HWW04, Hug02, JP02b, KY03, Kin02, LNZ01, MSU05, SOO02, SWH05, Ste01, Tan07b, VMSV05, Wer02, AKNR04, BCP07, CL04b, CYH04, CH05, CWJT01, CJT04, CLK04, Cho08b, ED03, He02, Hen06a, HWW02, KS05a, KPT04, KKKL09, LL06, LLH04, LJP05, LJK05b, NS05b, PQ03a, PQ06, RH03, SNW01, Sha05a, TJ01a, Tse07, WGL00, WHHT08, YLC09, YY05a, ZC04, ZK04, group-by [YL07].

Group-Oriented [LZL01, HWW04, CH05, CWJT01, LL06, TJ01a, WHHT08]. Groups [BSS02, CV03, CF02, Drc00, GM02a, GST04, KM01a, KLC00, LLH01, LP03, Luc02b, MN01, PHK01, GR04, HM00, LLY06, Pae03, Yi04].

GSM [An09a, BK03a, BD00a, Cha05b, Cim02].

Guadeloupe [Wri03]. Guanajuato [Buc00a].

Guessing [AGKS07, BSS02, CV03, CF02, Drc00, GM02a, GST04, KM01a, KLC00, LLH01, LP03, Luc02b, MN01, PHK01, GR04, HM00, LLY06, Pae03, Yi04].

Guessbook [SEK01, SEK02].

Gui [Z08, Pet08]. Guidelines [MMZ00, Die00].

Guildford [KN03]. Gummy [MYH02].

Guo [LLLZ06a, LLLZ06b]. Gutmann [Uzu04].
Hall [Bar00c, For04, Kat05b, Was08a, MAaT05]. Hall/CRC [Kat05b, Was08a]. Halmstad [BS01b]. Hamming [GK02]. hamper [Lov01]. Handbook [WBL01]. Hand [Bar00c, For04, Kat05b, Was08a, MAaT05]. Handheld [BMK00, Ano06a]. Handhelds [MP00]. Handle [RC06]. Handling [KL05, Lut03]. Handoff [OKE02]. Hands [KLB+02b, Shu06]. Hands-on [KLB+02b, Shu06]. Handshake [SB01]. Handshakes [Ver06a]. Handwriting [Ano02d]. Hankerson [Irw03]. Haptic [PBM+07]. Haptics [Pau02a]. Hard [Har07b, HMS04, Hro03, Lai07, CGHG06, GPV08]. Hard-Core [HMS04]. Hard-Disk [Har07b]. Hard-Line [Lai07]. hard-on-average [CGHG06]. hardcore [Sch01e]. Harle [RFR07a, RFR07b, RFR07c]. Harley [WPP05]. Harn [GG01]. Hash [Ano08d, Ano12, AEMR09, BBKN01, BRS02, BDS09b, Bur06, CBB05, Cor00b, Cor02, CDMP05, CS02, DOP05, FIP02b, Fil02, GIS05, GLG+02, HPC02, HR04b, ISO04, Jou04, KMM+06, MD05, RRS06, RR08, RB01, SS01a, Sho00a, Sho00b, SK05a, WFLY04, Yan05, YZ00, BR06, DS09, KCL03, Ku04, KCC05, LLH02, LKY04, LW04, MS09c, Mic02b, Tsa08, Wag00, YRY04, FIP02a, ZW05a]. Hash-based [BDS09b, KCL03, Ku04, KCC05]. Hash-CBC [BBK01]. Hash-chaining [CBB05]. Hash-Function [BR02]. Hash-functions [ISO04]. Hashes [Sch01a, GNP05]. Hashing [IK005, SGGB00, WS03]. HAVAL [WFLY04]. HAVEL-128 [WFLY04]. HAVEGE [SS03]. HB [MP07]. HB-family [MP07]. HB-MP [MP07]. HCI [YKMB08]. head [RFR07a, RFR07b, RFR07c]. headlines [Hen06b]. Health [Mad00a, Ano03a, CCCY01]. health-care [Ano03a]. Healthcare [TBTF02]. Heart [Uni00c, Uni00g, Uni00b, Uni00f, Uni00h]. heartbreak [Uni00b]. heart [Mur06]. heavens [Eva09]. Hedge [Sho00b]. Hedged [BGN09]. Heimdal [WD01a]. held [Buc00a, PPV96, Uni00b]. Hellman [KM04a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKRT08, FS01b, GR04, Kil01b, KK02, Kra03, Kra05, Mi08, Tsa06, YRY05c]. help [Ano08a]. Helped [Gan01b]. Help [DF01, Pri00]. Helsinki [Bur00]. Hensel [CSS02]. Here [Bud06]. Here [Bur06, Law05]. Hermite [Mic01]. heroes [OC03]. Herriot [Coc03]. Hersonissos [ACM01a]. Hessenberg [SSFC09]. heterogeneous [BCS02, Hof01, KHYM08, ZL0vB05]. heuristic [SS03]. Heuristics [Hro03]. HFE [FJ03, CHH01, FJ06]. HFE-Cryptosystems [FJ06]. HIBE [CS07c]. Hidden [HGN03, KW03, LNS02, Six05, GMR05, Lun09, Shp05, FJ03, Sch09]. Hide [CC06, PH03, Shp05]. hide-and-seek [Shp05]. Hiding
Hierarchies

Hierarchical

Hierarchies

Hierarcy

Hierocrypt

Hieroglyphs

High-assurance

High-Bandwidth

High-Dynamic-Range

High-End

High-Performance

High-Speed

High-technology-crime

High-Throughput

Hijacking

Hilton

History

Historical

History-based

HMAC

HMQV

HPC

Hold

Holier

Homage

Home

Homegrown

Homeland

homogeneous

Homomorphic

Homomorphism

Honeynets

Honor

Hook

Hop

Horizon

Huttenhain

Hwang

Hwang-Rao

Hwall

Hybrid

Hyperelliptic

Hyperencryption

Hyperchaotic

Hyper-Encryption

HyperOS

Hypeline

Hypervisor

Hyperorthogonal

HyperText

Hypertext Markup Language
[Che01d]. hyperlinking [Che01e]. hypotheses [KW00].

I-tracings [RE02]. i.e. [NP02a, Wil99]. IA [WWCW00]. IA-64 [WWCW00]. IACBC [JMV02]. IBE [ABC+05]. IBM [Ano04e, AV04, ADH+07, CGH+06b, Web08, Weh00]. Ibn [MAaT04, MAaT05, MAaTxx, MAaT07]. Ibn-Adlan [MAaTxx]. Ibn-Al-Durahim [MAaTxx]. iButton [HWH01]. IC [BGL+03, PC00]. ICBA [ZJ04]. ICCMSE [SM07b]. ICISC [Kino, LL03, LL04d, PC05a, Won01, WK06]. ICISC’99 [Son00]. ICM [IEE09a, IEE09a]. ICs [Bar00c]. ID [Gui06, ZJ09, BRTM09, CCD07, CL07, CS07c, CL00, GS02b, GTY08, HC08, KLY03, KHL09, Ku02, LCS09, Sco04, SW05a, SCL05, WBD01, WH02b, YC09b, YLH05, ZK02, ZC04, ZC09]. Id-Based [ZJ09, CCD07, GS02b, HC08, Ku02, WBD01, YLH05, ZK02, CL00, KLY03, KHL09, Sco04, SW05a, SCL05, WH02b, YC09b, ZC04, ZC09]. IDE [Ano02d]. Idea [Cos03, RR03a, CTL01]. Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b]. Ideas [Gha07, Eri01].

Identification
[BP02, BLDT09, Gar03a, GLC+04, KK02, Kirt01b, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZC09]. ideBased [AN02d]. Idea [Cos03, RR03a, CTL01]. Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b]. Ideas [Gha07, Eri01].

Identifiers [MC04]. Identifying [HBF09, LL05b, ZHY08, DMS07]. identities [Kwo02, Kwo03b]. Identity [App05, BF01b, BF03, BB04, BCHK07, BGH07, BPR+08, Boy03, BRTM09, CL01a, CHM+02, Coc01b, Dea06, DT03, GKO4, Her06, Her07, HY01, HL02, KC02, LCO7, Mar08a, Mar08b, Mit02b, Neu06, PCS07, Phi06, SPM+09, Ano011, Ano004e, BMW05, CG06, CJ05, GG08, Gni06, KG09, LL04b, LWZH05, RG09, Sa02, Sha03c, Sma06, Smi08, Sul05, Wal04, Wan04b, Win05a, Woo05, YCW+08, You04, ZYW07].

Identity-Based
[BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, LCO7, Mar08a, Mar08b, App05, Her07, PCS07, BMW05, CG06, CJ05, KG09, LL04b, LWZH05, Sa02, Sha03c, YCW+08, ZYW07]. IIDSFM [TZDZ05]. IDtrust2009 [SMP+09]. IEC [ISO04]. IEEE [BS03, BCDH09, BC01, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, KM07, HSD+05, Hug04, Mi08, PHM03, ZDW06]. IEM [RC05]. IFIP [DKU05, DFPS06, DFCW00, ELvS01]. II [Ban05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Han03, Kav01, MO03, Res01a, Res01b, Sal00a, ZTO3, McE04]. III [Sch00a, Ano00d, Bau03b]. IKE [CK02a, Kra03]. I’ll [PLW07]. illegal [Che01e]. Illinois [ACM04b]. Illusions [Koc02]. illustrated [Lun09]. Im [BG1+01, DOPS04, RR05]. IMA [Pat03b, Sma05, Hon01]. Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, CLT07, CC09, CC06, GW01, KBD03, KC09b, LL05a, LZ01, LWS05, LY07, LJO5b, LSC03, LSKC05, PZL09, RS00, SDFH00, SDF01, SSFC09, SH11, SM11, SYLC05, TTZ01, TH01, TC01, UP05, VKS09, VKO7, WY02, WLT05b, YZEE09, AAP07, AA08, CC02b, CHC01, Che07a, Che08a, GSK09, HLC07, KC09a, LLCL08, Lin00a, LT04, LYGL07, LCO6b, MS09a, MB08, PBV08, Sch09a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, mSgfLt05, TL02, Wan05, WMS08, WC05, XSWC10, YCYW07, YCL07, ZLZS07]. Image-Feature [GW01]. image-identification [PBV08]. Images [CTL04, CC08, CW09, DP00, FGD01, LS08, PZH01, PBC05, REC02, WCI09, WC04, YWWS09, APP07, AEEdR05, BN00, FWTC05, HHYW07, TCC02, TND+09]. Imaginary [HJW01, HM00, Hüh00]. Imai [DDG+06, YG01a]. Imbalanced [ZWCY02].
Immersion [Coc01a]. Immune
[CZK05, PZ02b, YKLM02b, ZP01, YKLM03].
Immunization [HR05]. Impact
[Ber03, HGNP+03, JKRW01, MMYH02, Wri00, CS08a]. Imperfect
[CPS07, DOPS04]. Impersonation
[BP02, Hsu05b]. implant [Fox00]. Implement
[HQ05]. Implementation
[AD07, AG01, Ase02, Ash03, ARC+01, BBD+02, CDDP01, CG08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK+03, FW09, FB01, GD01, GC01a, Gir06, HTS02, HMM01, JKR02, KMM+06, KMS01, KTT+07, KV01, LP02a, MMZ00, MKP09, MM01c, MNP01, MP01c, Mur02, Nov01, NMS01, Otw09, OTIT01, Pat01, PBTW07, QSR+02, RDJ+01, SM01, Sha01e, SK05a, SRQL03, USS02, Vir03, WZW05, WW00, WLO1, XBO1, Zea00, BI04, BBK+03b, C+02, CNPQ03, DS09, DKL+00a, GHGSS00, GBKP01, Hiih00, HP01, Hut01, KY09, LL04c, LCX08, LB05, Rhi03, SM03a, SVDF07, Wlo04, YW06, ZFK04].
Implementations
[AL00b, BJ002, III00, CTLL01, CGBS01, EPP+07, GLG+02, MM01b, MP01a, RS01, WW00, ASK05, BFCZ08, BFTG08, BG07b, Elb08, FR08, RAL07, RSQ03].
Implemented [TSS+03]. Implementing
[Dwi04, Kor09, LM08, LD04, MWS08, NDJ01, Pet03, Smi01a, SR06, Wou05, C+02, CW02]. Implications
[Kun01, LJ05a, MP01, Ayo06, Bjo05, Fri07]. Implies [KY01e]. Imply [Pie05]. Importance [Ane02b, KCJ+01, TID01]. Important [SM00a]. imposed [XLS06]. Impossibilities [CHL02]. Impossibility
[APV05, BPR+08, Fis01b, PQ06]. Impossible
[BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SK01]. impostor [LC07]. improve
[Pan02a, CA06]. Improve-ment [CA06]. Improved
[AFGH06, BPR05, BB05, BF00b, CL01b, CKK+02, CJ04, DN00a, DG02, Fan03, FKS+00, FKL+01b, FKL+01a, GMR08, Gen00b, HCK09, HKA+05, JQY01, Kin00, KT06, Ku02, Kiih02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02c, PR08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QC05a, YW05, YRY05a, ZW05a].
Improvement
[AS01c, AJ008, Che04a, CZK05, CCW02, Di01, HWM03, HW003, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Sa04b, Sha05b, WHL03, YRY05b, YRY05c, ZMY05, ZAX05, BL06, CCK04a, CL04c, CH05a, Hsu05a, JSW05, JmBdXm05, KJY05, LL04a, LW05c, SZZ05, TO01, WLT05a, YW04a, YWC05, YRY05a, YRY05d, ZC09]. Improving
[ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SK01, SB01, Sun02, XQ07, YEP+06, YGZ05]. incentives [Swi05]. Incident
[JBR05, Tom06]. Including
[SR01]. Incomputable [Ver06b]. inconsistencies [MS09a]. Incorporating
[MFS+09]. incorrectness [CHC04]. Increase
[NNAM10, PBTW07]. Increasing
[AEM17, CS05c]. Incremental
[BKY02, LKLK05]. IND-CCA
[Mli01b]. IND-CCA2 [BST02]. Independence
[BPO03b]. Independent
[BS00a, BSL02, Kin02, GSK09]. Index
[An00b, An01d]. indexing [YPPK09]. India
[CV04, JM03, MVE06, MS02c, RD01, Roy00a, RM04, Roy05, An03d]. Indices
[Fra01, Sy02, Wri03]. Individual
[BCC02, TW07]. INDCRYPT
[CV04, JM03, MVM06, MS02c, RD01, Roy00a]. Induced
[Vau02]. Industrial
[USE00b]. Industry
[ANS05, Mad00a, Ort00]. ineffectiveness [YL05]. Infeasibility
[FS08]. Inference
[Mar02b, DDD05]. Infinite
[TZT09a, TZT09b, Vau01]. infinity
[Hil05]. Influencing
[Bla01c]. Inform
Kil01a, Kim01, Kim02, KN03, Kn02, KP01, KNP01, Lair01, LL03, Lee04b, LST+05, LL04d, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, Pk03, P010, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Sch014, Sho05a, Sil01, SM07b, Syv02, TBJ02, TLC06, U000a, VY01, Van05a, WKP03, Wili99, Won01, Wri03. International [Yun02a, YDKM06, ZJ04, Zhe02b, ZYH03, AMW07, AUW01, Ano00e, AJ01a, BCKK05, Che05b, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, Pv01, Pho01, PM00, Rub01, SBB05, SE01, SEK02, Sto01, Tsa01, TWL05, Uri01, WC05, Wri05, ZGTG05, kc01]. Internet [SMP+09, ABB+04, Ben01a, Ben02, Cal00a, Che05b, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, P01, Pho01, PM00, Rub01, SBB05, SE01, SEK02, Sto01, Tsa01, TWL05, Uri01, WC05, Wri05, ZGTG05, kc01]. Internet-wide [SBB05]. Interoperability [Hil00, TEM+01, BHM03]. interoperable [BFGT08]. Interpolation [LW02, YG01b, FWTC05, KT06]. Interpolations [Sat06]. Interpretation [Mas04, CC04c]. interpretation-based [CC04c]. Intersections [KS06a, KS09b]. Interstate [RM02]. intranet [Jan00]. Intrinsic [ZWC02]. introduced [Ano00a]. Introducing [JL00]. Introduction [Ben02, Ber09b, Bis03a, BK06b, Buc00b, Buc01, Buc04, CLR01, DK02, DK07, Fal07, Hay06, HPS08, Hro03, HC02, IH04, K08, MA07, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGS08, TW02, TW05, TW06, Big08, CS07a, CM05b, Gar01, HW98, Hro05, K03, Mol07, RR03a, RP00, Sho05b, TW06a, K0t05b, Rot07, Lee03a]. Intrusion [CZK05, DFK+03, DP07, JT05, TZZD05, TMMM05, WG05, HLL+02, MAC+03, NCRX04, NN02, YB J04, IR02]. Intrusion-Resilient [DFK+03, DP07, IR02]. intrusion-tolerant [Yb04]. intrusions [Bej06]. intrusive [AMB06, RFR07a, RFR07b, RFR07c]. invalid [CJT04]. Invariant [Bnu00, CT09, HH09, ZLZS07]. Invariants [WH09]. Invasion [ASW+01], invasions [Tyn05]. Invention [Bra06, frr00, Sav05a]. Inventions [Sav05b]. Inventors [Bar00c]. Inversion [BNPS02, KKY02, KTT07, SPG02]. Inversion/Division [KKY02], invasive [SB05]. Investigating [AMB06, BW07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08, WD01b, WC04]. Invitation [Bar02]. Invited [F0GM0, Jan00d, Drs05]. involutional [S0H07]. ions [Min03]. IP [Ano00a, CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSEC [Vau02, CGBS01, Dav01a, KMM+06, SKW+07, FS00, FS03a, XLMS06]. IPSec-Compliant [CGBS01]. IPTables [GC05]. IPV6 [Nik02a, Nik02b]. Iran [Mah04]. IRe [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFSH09]. Irreversibility [ZWC02]. ISBN [And04, Duw03, Eaq05, For04, Gun04, Imr03, Pag03, Puz04, Top02]. Island [CSY09, KGL04, Kim01, Lee04b, IEE07]. ISO [GM00b]. ISO/IEC [ISO04]. ISSAC [Jef08]. issue [FOP06, FOP06]. Issues [BDF+01a, BHO0a, H0l0, KR01, Maa01, PBM+07, SERF+06, MKY08, Pat02b]. Italy [AAC+01, AL06, BCKK05, BC05c, CGP03, dCDVSG05, IEE04].
Libraries [Fin02, MK05b, Sae00], Library [KSZ02, Lau05, Law09b], Libre [Ken09], license [Ano00h], Lies [Gan01b, Sch00d, Swa01, Che00b, Ste05c], Life [Cop04b, GSB + 04], lifecycle [HL06], Lifetime [Coc01a, CPG + 04], Lifting [CNS02], Light [WT02], Light-Weight [WT02], Lights [EPP + 07, Mal02, CH07a, CL09, MP07], Like [Coc02a, PSC + 02, VMSV05, BCDM00, CWH00, DLP + 09, Egh00, EBS01, Gou09, HSL + 02, HL04, SKU + 00, SLL + 00], LILI [JJ02], LILI-128 [JJ02], Limit [Das08], Limitations [Gua05, Fis01a, LG09], Limited [AK02a, LCD07, Buh06, Tse07], limiting [CC02b, CHY05a, KTC03, YY05b], Linear [BDK02a, BDK02b, BDQ04, CGFSHG09, CS05b, CH02, Cou01, CM03, Cou03, CDM00, CD01a, CDG + 05, FM02a, FM02b, GS03, GBM02, HLL + 01, Hug02, JJo0d, Kan01, KMT01, Kn02, KM01c, KR + 02, KY01e, LLL + 01, LS05a, NVP01, PSC + 02, PG05, PZ02a, SNWX01, STK02, WF02, YSD02, BD04a, Bu09, CLK + 03, Cou04, GHPT05, Luk01, LLL04, Reg05, Reg09, RSL03, Se00, SLL + 00, TM01, XSWC10], Linearization [DG + 06], Linearly [ADD09], Lines [SP04], Linguistic [CDR01], link [LPV + 09], link-layer [LPV + 09], linkages [ZAX05], linked [YWWS09], Linking [GW00], Linux [Lin02, ASW + 01, FR02, Fin02, Fri01, GJJ05, Gan08, GPR06, JZ04, Lin02, Mor03, Pri00, Shu06, Sta02b, Sta05], LISA [USE00c], list [AGKS07], Listening [Cas03], little [Che01d, Lam07, Sch05c], Live [Lov01], Lived [GSW00], lives [FNRC05], living [BCB + 05], LLL [CKY05, NS05c], Load [CC08, Hó01], Loads [GH02], Loan [SOI02], Loaning [Blal0c], Local [NABG03, Lav09], Locality [MFS + 09], Localization [WLT05b, CKL + 09], Locally [Vad03, Yek07], Location [HY01, KZ01, LNL + 08, Buh06, SG07], Locations [Kra02b], Log [Gen00b, HN04], Logarithm [CNS02, Che04b, CCW05, GPP08, L02, Hsu05a, HLM05d, JLL01, LLM04, LHY05, Sch01e, SCL05, SL05, Yas08], Logarithmic [EGK08], Logarithms [CS03a, JL03, LHL03a, LTY05, PLJ05a, QCB05a, Sha05c, Sha05d, SCS05c], Logging [Fox00, MT09], Logic [BPST02, Cop04b, KBD03, KS06b, Li01, Nie02d, SQ01, SC01, Tee06, TV03, BDNN02, BD04a, DZL01, SW02, WZB05, dH08], Logic-Based [KBD03], Logical [As04b, Kra07, SP03, CLK04, Zha08], Logics [IK03, IK06], Login [LL05c, CCK04b, CJT01], Logistic [KJ01], Logo [LZ09], London [Pag03, Top02], Long [ABRW01, DVP09, Dur01, Eva09, GSW00, Gro03, PGP01, Zho06, BMV06, ISO05, LG04, SGMV09], Long-Lived [GSW00], Long-Term [ABRW01, Dur01, DVP09, BMV06, ISO05, LG04, SGMV09], Look [Bon07, Has00, Lut03, Sve00, Hen06b], Look-up [Has00], Looking [ASW + 01, An01j, Cla00b], looks [Nis03a], Lookup [MFFT05], loop [KVN + 09], loop-level [KVN + 09], Loopholes [Ste01], Lorenz [GHdGSS00, Sal00a], Lorenz-based [GHdGSS00], Losing [Sta05], LosLobos [Pri00], Loss [LHS05, BC05b, Mit00], Lossy [AIP01, HSKC01, PW08, As04a], Lost [PY06, Rob02, Rob09], Lösung [An04c], lot [Cla00b], Lotteries [FPS01], Louisiana [USE00c], Louvain [QSO0], Louvain-la-Neuve [QSO0], Low [An00d, BM01b, CH07a, GST04, HNZI02, HGR07, JP02a, KBBM09, RM03b, RMH03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09b, Fan03, HLM03, LGKY10, LCO4a, SK03, WLH05, WLH06, WY05, ZYW07].
low-computation [Fan03, LC04a].
low-cost [CL09]. Low-end [SU07].

Low-Exponent [SZ01]. Low-overhead [HGR07].

Low-Power [Ano00d, JP02a, KRM09, CO09b, ZYW07].

Low-State [GST04]. Low-Weight [CH07c].
Lower [BDF01b, BP03b, DIRR05, GT00, GGK03, PS02a, Shp99].

LSB [CS05c, FGD01, WMS08].

LSD [HS02a]. Lu [QCBO5b].

Luby [MP03, Pat03a].

Luminy [PPV96].
Lumpur [DV05].
Lund [Joh03].

Lurk [Rie00].

LUT [CC02a, TL07].

Luxembourg [Bir07].

Lyndon [GS01, VS01].

Lynn [Hes04a].

LZ [AL04].

M [DNR03].

MAC [ACP10, JQ04, K105, KP01, Nao04, Pag03].

MACs [BPR05, BR00b, BM01c, Sem00].

Made [Ste05b].

Maelstrom [MYC01].

Magic [DNR03, GH04, Bur02, GP00, Hro09, Ano01k].

Magyarik [dVP06].

Mail [ANR01, Cos03, KS00a, Law05, Che01f, LL04c, NZS05, Sni03, All06].

mails [LG09].

Maintain [Web08].

Mainstream [Bj05].

Maintaining [MJF07, Zho02].

Maintenance [NABG03].

Majorana [Car02].

Majesty [Bud06].

Majority [GKKO07, SV08b].

Make [BP06, Ber03, Sin02].

Makes [Pan09, Pal02].

Making [Che07b, CRSP09, Gar01, Lut03, Mit00, Mul02, Oec03, Per05a, WR05].

Malaysia [DV05].

Malaysian [Kha05].

Malicious [LHC08, Sz03, YY04, Tsa06].

malleable [DW09, FF00, PR05].

Malware [LH07, SZ03].

Man [Gen04a, Urb01].

Man-in-the-Middle [Gen04a].

Management [ACM03a, ACM04a, Ano02d, Ano02e, BP07, BW07, ELs01, FMA02, GK04, Gut04b, KB06, Lin00b, Mit02b, Scr01, Sha04, TMM01, Woo00, Wya02, ASW00, AJ508, AFB05, CG06, Cha05a, Dea06, GTY08, ISO05, Jan00, JW06, KYM08, KAM08, LMW05, LPM05, LR01, LK01, MKK00, Neu06, Pot06, RH03, SRJ01, Sen03, Sna06, Smi08, UP05, Woo05, You04].

manager [KH03, Sha01a].

Managing [MA00a, MA00b, NDJB01, Oue05, PTP07, PBB02, Tot00, BJ02, K0v03, KH03].

Mandrake [TvdKB+01].

MANETs [STY07, DF07].

manipulation [SWR05].

Manuscript [GG05a, Rug04].

manuscripts [MAaTxx].

Many [BB02, Di01, MP03, Di03, SVDF07].

Many-to-one [SVDF07].

Map [XXXYX11, JK10, Lee04a, PC05b, SL09].

Maple [Cos00, TT00].

mapping [Tan01].

Mappings [HI04].

Maps [BGLS03, BMS03, CL04a, LLL01, WP03, JK01b, MA02].

Maqasid [MAaT05].

March [BDZ04, Bir07, Bla03, HR06, PY05, Sil01, Uni00g, Uni00a, Ytr06].

Marion [Kap05].

Marjan [BCB+05].

Markers [FBW01].

Market [Bar00a, Ana01i, Neu06, Swi05].

Marketplace [PLW07, VN04].

Markov [KW03].

Marks [Ano01c, YSS+01].

Markup [Un00a, Un00d, Un00c].

Marrakech [IEE09a].

Mariott [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].

Mash [And08a].

masked [AHS08, Laut08a].

Masking [CHJ02, CT03, GK02, Lav09].
Massachusetts [IEE05b, USE01b, USE01a, IEE03]. masses [Pot06]. Massive [Ano01l]. massively [FP00]. massively-parallel [FP00]. Match [JJ00a, WC04, LLC06a]. Matching [ABM08, Len01, UEBEP09, Voi05].

materialized [MSP09]. Materials [SLT01]. Math [SR06, McN03]. Mathematical [AUW01, Cas06, FF01b, GL05, HPS08, Kat05b, You06, GKS05, Hil05, Sin09]. Mathematics [BP06, Lew00, Nie02d, Sch05a, Wal00, Gar04, Sch03, Sch+03, Sch04a, Sch04b]. Math´ematiques [RSA09b, PPV96]. Matrices [TL07, CFVZ06, LMTV05]. Matrix [CV03, BF06a, OS07]. Matroids [CDG+05]. Matsumoto [DDG+06, YG01a].

Mature [Tro08]. Max [Di 01]. maximal [H¨uh00, HJW01]. maximizing [GSK09]. maxims [Bau00, Bau02a, Bau07]. Maximum [KMT01, ZC00, DW01]. May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bih03, CC04a, Cra05a, DRS05, IEE01b, Knu01, MJ04, MS05a, PM00, Pii01, Pre00, TLC06, Uni00f, Uni00c, YKLM02a, Pau02a, YJ00]. Mbps [LMP+01]. McClure [Gum04]. McEliece [CFS01, KI01a, KI01b, Lio00, LS01c, Sun00b]. McEliece-Based [CFS01]. McFarland [Car02]. McGraw [Gum04]. McGraw-Hill [Gum04]. MD4 [DG02, WFLY04]. MD5 [Ano09c, Eke09, For09, WFLY04]. Me [CAC03, CNB+02]. Mean [Bar00c, KLML05, Ver06b]. Means [LMHCETR06, Nis03a]. measure [Lav09]. Measurement [Ano02e, kc01, CO09b, FXAM04, RW07]. measurement-based [FXAM04]. Measures [CB01, QS01, GSK09]. Measuring [Siv06]. Mechanising [Bel01]. Mechanism [Eva09, LXM+05, WY02, CL08, CLK04, GH08, LCP04, ME08b, RFR07a, RFR07b, RFR07c, WAF00]. Mechanisms [BACS02, CJK+04, Her09b, Lin00a, MD04, Mir05, Pip03]. mechanized [dBH08]. Media [And08a, Hei07, CBB05, Ano02a].

media-streaming [CBB05]. Median [Cap01]. Mediated [DT03, CG06]. mediator [SBG05]. mediator-free [SBG05]. medical [AL07]. Medicine [MYC01, Moo01]. Meet [Cla00a, HG07]. meet-in-the-middle [HG07]. meeting [Jef08]. Meets [Way02a]. Melbourne [IZ00]. Member [CTH08]. Membership [NBD01, Fis01a]. Memoir [Bar05]. Memorable [KOY01]. Memoriam [DNRS03]. Memory [AK03, AJ00, BS00b, CCM05, DK08, DGN03, HNZI02, HBAJ01, KCI+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05]. Memory-Bound [DGN03]. memory-safe [Oiw09]. Memoryless [SBG05]. MEMS [ECG+07]. MEMS-Assisted [ECG+07]. ment [CAC06]. menu [Mea04]. Mercy [Flu02a, Cro01]. Merkle [CDMP05, JLM03]. Mersenne [Ano03f].

Mesh [LPZ06, ZTP05, KB09, LZP+04, YPSZ01]. Meshes [BG08, Lew09]. Message [BKR00, Ber04, BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SN04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, Kar02, MD04, MS09c, Sha04b, TJC03, W01, ZF05, ZAX05, ZC04]. Messages [Ara02, AR01, BR00b, CH3+01b, DS05b, Sch09, Wir05, Zho06, Alv00, An00e, BCG+02, Bib02, BB79, Lui09, SP79]. messaging [Opp01, RR05]. meta [SM08, PLJ05a, QCB05b, Sha05d]. Meta-He [PLJ05a, QCB05b, Sha05d]. meta-learning [SM08]. metadata [CDS07, FJ04]. metamorphic [CSW05]. Metaphor [CNB+02]. Metering [BC04b]. Method [BDTW01, GHK+06, GL00, Gno01, HRS02, HQ05, JKK+01, LL02, Moi02, OKE02, OT03a, OT03b, SOHS01, TIGD01,
Methodologies [SPMLS02, NdM04].
Methodology [VMSV05, HM02a, HCBLETRG06].
Methods [BCDM00, CFRR02, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Bau00, Bau02a, Bau07, BGM04, BCHJ05, CM05b, GKS05, JZCW05, LFHT07, Mal06, SSST06, Slp99, YV06].
Metric [LBGZ01, LBGZ02].
Metrics [LZ01, NP07].
Mexico [Buc00a].
MGC’05 [ACM05a].
Miami [Des02].
Micali [Rub00].
Michael [Ter08].
Micro [ASK07, Eng00, Ste05c].
Micro-Architectural [ASK07].
microcontrollers [GBK01].
Microelectronics [IEE09a].
Microprocessor [Web08, GP00].
Microprocessors [LKM+05].
Microscopic [MYC01].
Microsoft [Bon00, Scr01, Ste05b, Wei00].
Middle [Eag05, Gen04a, HG07, Kin01].
Middleware [ACM05a, KRV01, LGS01, MBS04].
Migration [Pat02a].
Mikhailovsky [Puz04].
Milan [dCdVSG05].
military [Ark05].
Million [Ran55, Ran01, Ano03a].
MIME [Dav01b, Dav01c, LG09, Opp01].
Min [MR01b].
Min-round [MR01b].
mind [Lau08b].
Mine [For04].
Minimal [FBW01, FGMO01, JY01, SC02b].
Minimalist [Tro08].
Minimizing [LPM05].
Mining [LP00, Luo03, HLL*02, Mal06, Men03, Pin02, Pin03, ZY08].
MiniPASS [HS01b].
Minos [CC05e].
MinRank [Cou01].
Minutiae [UBE09].
Minutiae-based [UBE09].
Misbehaving [JQY01, SBB05].
Misinformation [CZB+01].
Misssed [TvdKB+01].
MIST [Wal03].
Mistakes [Ste05b].
MISTY [KYHC01, Küh01].
MISTY-Type [KYHC01].
MISTY1 [BF01a, Küh02b].
Mithra [Fre03].
Mitigating [NLD08].
Mix [JJ00a].
Mixed [SKR02].
Mixes [Mó03a].
Miyazaki [WHLH03].
MMM [GKS05].
MMM-ACNS [GKS05].
Mnemosyne [RH02, HR02].
Mobile [Cha05a, CFRR02, Dim07, GN06, JP02a, KZ01, KB07, KC02, KH01, LK01, Mal02, MM02, PL01, RKZD02, Rü01, Ros01, SH00, ZYM05, CC05e, CJ03b, CF05, CF07, DMR07, HP00, HY03, SHC09, ISTE08, KVD07, KX03, LC04, Lin07, LKZ+04, Par04, Pan02a, SM+08, SL05a, TM06, TW07, Tse07, Wan04a, YC09a, YC09b].
mobile-commerce [YC09a].
mod [TM01].
Modal [GN01].
Mode [BR02, Dwo03, HR03, HKR01, KSHY01, SLG+05, WB02, Hey03, RB03, ZL04c].
Model [Abe01, Abe04, BH05, BPS02, BL02, CL01a, CS07c, CPhX04, Lio08e, CT09, DPV04, DFSS08, Din01, Din05, ECM00a, Gra02b, HLC08, KLN+06, KW03, LJJ05, MN+04, MNFG02, MR01b, MR01c, MISTS04, Pas03, SA02, SL05a, SAR02, SFDF06, TZZD05, Vad03, WC05, WT02, WvD02, ZGLX05, ZP05, BK03, CUS08, CDD06, Dan00, DFSS05, GMR08, HLM02, LCX08, LL08a, LL08b, MS09b, PS04b, SR01, TP07, DY09a].
Model-Based [Sa05b].
Modeling [AADK05, CDD+05, HMvdLM07, KS05a, ZP05, Lf00, SS04].
modelled [BG08].
Modelling [HCD002, JP07, Puc03].
Models [Ben00, BB00a, LR07, Lio00b, WH09, Cra05b, GKS05, Lio01b, SC02b, vOT08].
Modern [Gol99, Mao04, Pag03, SM07b, Swo08, Bud06, Fur01, IM06, KL08, Mol05, SE01, Lut03, Lec03b].
Modes [DGH+04, Dwo03, GD02, Gol01e, HSH+01, JMV02, JKR01, Jut01, KY01a].
Modified [CHC04, HPC02, JY01, Kfl01, ST02, Che08a, CTT01, HWW03, LL04a, LL05a, kWPWL01].
modifying [CSV07].
Modular [BKP09, CMJP03, CH07c, Dhe03, FP00, Gro01, Har06, HGG07, JP03, NIS01b, PG05, SK07, Ste01, Tan07a, Wal01, WAL04a, HSD+05]. Modulation [AS01c, Che07a]. Module [Ano02d, LM00, SGM09, ARJ08, BG09, Jan08b]. Modules [FIP01b, NIS01b, GJJ05, JEZ04, Sei00b]. Moduli [Bai01b, GMP01b, Wal01]. Modulo [ACS02, Gon06, Gro03, MFFT05, Zhe01, Wan05]. Modulus [Ano01o, CGH00a, CDL+00, SZ01, WY02, WS02, LKYL00, WWTH08]. Modulus-Based [WY02]. Mollin [Kat05b]. MOM [DJLT01]. MONA [KMS01]. Mondriaan [BF06a]. Money [Ano01a, YKMY01, JP06]. monitor [MK05a]. Monitored [PS05]. Monitoring [AK02a, BCS02, Por06, Bej06, GXT+08, ZGTG05]. Monitors [JT05]. Monks [Eag05, Kin01]. Monotones [WW05]. Monsters [And08a]. Monte [Bi09, Sug03]. Monterey [USE02c]. Montgomery [CH07c, HKA+05, NMSK01, SO01, PS04a, TSO00, Wal01, WS03]. Montgomery-Form [OS01]. Montpellier [KM07]. Montréal [ACM02]. Morocco [IEE09a]. MorphoSys [Tan01]. MOSS [Dav01b]. Most [GG05a, Shp02, Tyn05]. Mothballed [Bar00c]. Motif [Bi09]. Motion [EFY+05, hKL00, WMDR08]. Mountain [JYZ04]. mouse [HLwWZ09]. move [Jac00]. movement [HLwWZ09]. MP [MP07]. MP3 [DRL09]. MPEG [LHS05, MLC01, SG07, YZDW07]. MPEG-4 [SG07]. MRF [Che01a]. MRM [TIGD01]. MSP430x33x [GBKP01]. MSXML [TEM+01, Hei01]. Mu [CJT03]. Much [Che01d, Con09]. Multi [ARR03, BBM00, BR06, CCD07, CJK+04, CDM00, CDG+05, DLY08, DJLT01, FGMO01, FWW04, Gen04a, HM01b, HS07, JLL02, Kur01, LV07, LLL04, Tsa01, ZJ09, BSSM+07, CLOS02, CC05a, CHY05a, CHY05b, DZL01, FWTC05, GMLS02, HHYW07, HH05, HC04b, HL04, LHL03b, LCZ05b, LW05c, NC09, PW05, SC05a, Tsa08, TWL05, TYH04, YCH04]. Multi-applications [DJLT01]. Multi-Authority [JLL02]. Multi-channel [ARR03]. Multi-designated [LV07]. Multi-Domain [CJ07]. Multi-factor [BSSM+07]. multi-hop [NC09]. multi-linear [LLL04]. Multi-party [CDMO, CDG+05, FGMO01, FWW04, HM01b, LLL04, CLOS02]. Multi-property-preserving [BR06]. Multi-Proxy [ZJ09, HC04b, LW05c, TYH04]. Multi-Receiver [CCD07]. Multi-recipient [Kur01]. multi-scroll [HHYW07]. multi-secret [CC05a, CHY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server [Tsa01, LHL03b, Tsa08, TWL05]. Multi-Servers [SH07]. multi-signature [HH05, HC04b, HL04, LCZ05b, LW05c, TYH04]. multi-stage [CHY05b]. Multicollisions [Jou04]. Multilevel [LN04]. Multimedia [AAK09, FMS05, GA05, HL07, LLRW07, Sun05, WLLG09, DY09a, DKL05, FZL08, PMRZ00, CDD00, HTO4, IKOS07]. Multiway [SK05b]. Multiple [AIK+01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, DK05, Har00, HZSL05, HLT01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJ04, DM07a, HLH00, KC09a, MN14, Sha01d].
SW05a, TCC02, YW05, YSH03, YRY05b].

**multiple-key** [Che04a, CJ04, SW05a, YW05, YSH03, YRY05b].

**Multiple-Precision** [HZSL05, MN14].

**Multiple-watermarking** [Che08b].

**Multiples** [HR00].

**Multiplication** [AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02c, KKM01, Mö02, NMSK01, Tan07a, Wal01, BNP03, DwWmW05, FP00, GD05, Has05, Mis06].

**Multiplications** [Har06, OT03b].

**Multiplicative** [Has01a, KO03, MFFT05].

**Multiplier** [HKA+05].

**Multipliers** [CMJP03, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a].

**Multiply** [KTT07].

**Multiprocessor** [ISTE08].

**Multipurpose** [Boy03].

**Multireceiver** [HSZI01].

**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** [MJF+08].

**Music** [MNS01, XMST07].

**mutargima** [MAaT05].

**Mutation** [Lut02].

**Mutual** [JP02a, KH05, CC08, SW06, VK08, YWWD08, YC09b].

**Mutually** [WC01a].

**MYCRYPT** [DV05].

**mysterious** [Bel07a].

**Mystery** [GG05a, Rug04].

**Myths** [GO03, kc01].

**N** [Mar05a, AOS02].

**NAF** [OT03b].

**Names** [Coc01a, Sha02, Ark05, CVG09].

**Naming** [An01b, BH00b].

**Nanotechnology** [RR03a, RR03b].

**Naor** [Zha06].

**Napoleon** [Urb01].

**narrowed** [Sch04d].

**Narrowing** [MT07].

**NASA** [An02c, Wil09].

**National** [Lan04a].

**National-Scale** [BWE+00].

**Natural** [ARC+01, Top02, WMS08].

**Nature** [Pag03].

**Naval** [LBA00, Goo00].

**Nazi** [Han06, KS04].

**NC** [AIK04].

**nCipher** [An03g].

**NCR** [LBA00].

**Near** [BC04a, DPS05].

**Near-Collisions** [BC04a].

**Necessity** [SBZ02].

**Need** [Coc01a, HR04b, Sty04].

**Needs** [CZB+01, DKK07].

**Negotiation** [DBS+06, HHJS04, IY05, LLW05, LLW09].

**Nema** [Kid00].

**NESSIE** [Pre01, Mac00, Pre02a, Pre02b, SGB01, DPPR00].

**nested** [LCK04].

**Net** [CAC03, An08b, LKJL01].

**Netherlands** [Knu02, An01m].

**NetHost** [AMB06].

**NetHost-Sensor** [AMB06].

**Nets** [AADK05].

**Netspionage** [BK00].

**Network** [An02d, An03c, Bar03, BGOY08, Con04, CLZ02, Dim07, FBWC02, Gum04, Has05, IKY05, JYZ04, KKG03, KPS02, Kru02b, LMP+01, Lu07, Mal02, NAM01, NN02, PZDH09, PZL09, Pou03, RCBL00, RC05, Sty04, TLYL04, VMC02, YC01, ZY03, ZS05, Brui06, CJ03b, CM00, Coc01a, DWML05, GSH05, HLL+02, LC03, LPV+09, MW06, ME08a, MS03, Miš08, Pri00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wyl05, YL06, ECM01a, ECM00b].

**Network-Attached** [RCBL00].

**Network-based** [HLL+02].

**Networked** [Sch00d, Che00b, LB05].

**Networking** [ACM01b, Ros07, Moo01, VM03].

**Networks** [AAEQ05, BJLS02, CGM07, DBS+06, Fin06, GPC08, Gor05, JKR01, KZ01, Ken02a, KH05, NL+08, NAB03, PR01, RZK02, Sin01a, WT02, Zee00, ZYN08, ZWCY02, AJ08, As04a, BBG+02, BC05c, CCMT09, CGP03, CBD+05, DHRM07, ETM05, HJ07, HMvdLM07, JRR09, KXTZ09, KHY08, KB09, KVD07, LDH06, LHC08, LWO5a, LLH06, Lin07, LN04, Lop06, LKZ+04, MWS08, MJF+08, MS09b, NC09, NLD08, PCLS07, PS08a, Pat02b, SLP07, SSM+08, TP07, TM06, TCR03, TW07, WDLN09, XwWL08, YC07, ZS07, ZB05, An02d, CS08b].

**Neural**
Neural-Network [YC01].

Neuve [QS00].

Nevada [ELvS01, IEE01a].

Never [Wei00, Hau06].

Newfoundland [NH03].

Newman [Pag03].

Newmanry [Sal01a].

News [Ano03d, Bar00a, Bar00b, Bar00c, Cla00a, Coc00a, Coc02a, Coc02b, Coc03, Eng00, Fox00, MYC01, MP00, PM00, Pau02a, Pau02b, Pau03, Pau09, Pri00, CAC03, CAC06, Sta05, Raj06]. Newton [KT06]. Next [ESG+05, McL06, TV03, Van03, Web08, BD04b, ISTE08, RR03a, Ros04].

Next-Generation [ESG+05, Web08]. NFA [DIS02]. NFS [Sta02b]. Nice [DS06, JJ00c]. Nicko [Ano03g]. Nimbus [Fur02a, Mac00]. Nine [Tat05]. Ninth [USE00d]. NIST [BG07a, Dra00, Hir09, Kel05a, Kel05b, RRS06, SF07]. NIST-Recommended [Kel05a, Kel05b]. NMAC [RR08]. NMAC/HMAC [RR08]. NNAF [DwWmW05]. No [Sta05, Sty04, Uni00g, Wei06, Wei05, CC05b]. Nobel [MNT+00]. Node [BRTM09, Fox00]. Nodes [ZYN08, RAL07]. NOEKEON [DPVR00]. Noise [BKW03, GA05, MPSW05, SDMN06, MS09a, PC00]. noise-based [PC00]. Noise-tolerant [BKW03], noisy [HGS03]. Nominative [PL01]. Non [Br05, CHK05, CZB+01, DN00a, DDO+01, DW09, FF00, Fis01b, Fis05, FG00a, FG00b, HNZ102, HJW01, IYK02, IYK03, JT01b, Kos01c, KO00, MSTS04, Nie02b, PHK+01, Pas05, SPK08, WBL01, DM07a, DS02, Hüh00, HLL04, IM06, KKL09, KHL09, LSA+07, PR05, RP00, RFR07a, RFR07b, RFR07c, SC05c, XSWC10]. Non-adjacent [JT01b]. Non-committing [DN00a, Nie02b]. Non-Cryptographic [WBL01, IYK02, IYK03]. Non-injective [Kos01c]. Non-interactive [CHK05, DDO+01, Fis01b, Fis05, HNZ102, HJW01, MSTS04, Pas05, KKL09, KHL09]. Non-interference [BR05]. non-intrusive [RFR07a, RFR07b, RFR07c]. non-linear [XSWC10]. Non-malleable [DW09, FF00, PR05]. Non-maximal [HJW01, Hüh00]. Non-OOSD [CZB+01]. non-perfect [DM07a]. non-physicists [RP00]. non-quantum [IM06]. non-repudiation [HLLO4, LSA+07, SC05c]. Non-trivial [KO00]. Non-Uniform [SPK08]. Non-contact [Sak01]. nonsecurity [Sch07]. Nonuniform [CU01]. Normal [Ran55, Ran01, GPS05, Mic01, RMH03a]. Normalization [VK07]. Norway [Ytr06]. Nose [Fox00]. notarization [LG04]. Notarized [GTY08]. Notation [Eag05, Kin01]. Note [CWY05, FS02, GMP01a, GIS05, KCP01, Ros00a, MF07, PC05b, Yan02, Zha06]. Notes [KSF00]. Nothing [Des00c, SR00]. Notions [BPS00, BN00a, CK02b, DKKM05, HU05, Kos01a, Des00a, KY00, PS04c]. Novel [BBB+09, CC02a, CYH01, CDTT05, CW09, HC08, MP01c, WCJ09, AJ08, BG08, CCS05, DSGP06, GB09, HG05a, MRT10, SPG02, SCS05a, mSgFtL05, WC05]. November [ACM01b, ACM05a, BZ02, CKL05, Eke02, IEE00a, IEE02, Lai03, LL03, LL04d, 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, HG09, HJJ07, NP02b].
NTRUEncrypt [HHG06, KY09].
NTRUSIGN [HHGP +03, HHG06, HWH08, ZJ09].
NTRUSign-Based [ZJ09].
Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Dic03, DGP07a, DGP07b, DVO8, Eag05, EHHP +03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05a, Kel05b, Ket06, KM01b, LMHCETR06, LNS02, MNP01, NR04, NNAM10, RN +01, SP05, Sch06b, Shp99, Shp03, SFDF06, TWNA08, TL07, TZZ09a, TZZ09b, Vav03, Wbl00, Yan00, YKLM02b, Aam03, AUW01, BS02, BK07, Be08, BGPG05, BG08, BG09, BG07a, BGL +03, CFY +10, CNPQ03, CO09b, DIM08, DGP09, FP00, HG05a, HGNS03, HlwWZ09, HP01, JAW +00, JL03, KH08, KSF00, Kin01, Lam01, LGKY10, Mt00, MRT10, Nie02a, Nie04, Pan07, PSG +09, PSP +08, PC00, RGX06, SH11, Sho05b, Shp05, Sim02, Ste08, SR07, Sti11, SK01b, Tat05, Wag03, Was08b, XSWC10, YZEE09].
Number-Notation [Eag05, Kin01].
Number-theoretic [NR04].
Numbers [BCGH11, GH04, HSR +01, HBF09, Ifr00, MN01, ST03b, AG09, HW08, KB39, Kir01b, MFK +06, SS03, Shp05, Tiy27].
numeric [AKSX04]. Numerical [WW +02]. numerically [Sav04]. Numerous [CC08].
NURBS [Ben00]. NUSH [WF02].
NY [HR06, IKY05, KJRR05, Sch01d, YDKM06, An0011, NS00].
Nyberg [Ara02].
O [Kat05b, Puc03]. OAEP [Man01, BF05, BF06b, Bon01, FOPS01, Sh01].
Obfuscated [NS05b]. Obfuscating [BG1 +01]. obfuscation [CT02]. Object [RSA00e, DHL06, MWM01, ST06]. object-oriented [DHL06, MWM01].
Objects [CCM05, ZTP05, PB01, WH09].
Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GKM +00, KKL09]. obscurity [MN03]. Observability [JQYY01]. observers [JL04]. Obstacles [KM04a].
Obtaining [Bar06b, BP03b]. OCB [RBB03], occur [Web02]. Ocean [MYC01].
October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST +05, TTTZ01, USE00b, ZYH03].
Octopus [Cla00b]. Oded [Lee03b].
Oedipus [Lav06].
Off [AJO08, CCO02b, Oec03, Shi05, YLLL02, Bau05].
Off-Line [YLLL02, Shi05, Bau05]. Offering [YC08]. Office [Uni01]. officer [Kov03].
Official [BP01b, CCR02b]. Offline [DJ06, ST01b, WV01]. Offs [PS01c]. OH [BD08]. oil [RD09]. Old [Eva09, Lov01].
On-Demand [SEF +06]. On-Line [Lu02, BCS02, Luk01].
One [AK02a, BYJK08, CHL02, Che03, DIS02, Di 01, DW01, DMS00, Fis01b, GKK +09, HNO +09, HM02b, HR05, KI01a, KO03, KO00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sh000a, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, XYXYX11, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CH05b, CJ04, CO05d, Di 03, DS02, GKK +07, HR07, HRS08, HLT09, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05a, Tsa08, YW05, YR05b, ZW05a].
One-Dimensional [XYXYX11]. One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLT09, LC04a].
one-variable [SV08a]. One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK +09, HNO +09, HR05, KO03, KO00, LTW05, Sh000a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, GKK +07, HR07, HRS08, JZ09, KK07, KKK05, KK03, LW04, LPM05, LQ08, Mic02a, Poi00, Tsa08, YW05, YR05b, ZW05a]. One-Wayness [KAS01].
Online [CL05].

[CL05]. Online
[BDF+01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAVY09, Voi05, FNRC05, Fox00, Pan07, Tyn05, PT08].

Online/Offline [ST01b]. Only
[BBK03a, CF01b, GL01, Hes01, VV07, BCDM00, FKS+00, GHJV00, Iwa08, IK00, Jon08, KSS00a, KM00, LM08, Mes00, Wan04b, Yst08].

Ontario [HA00, ST01d, VY01].

OOSCD [CZB+01].

Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Kus02, Lin02, Mea01, PM00, VDKP05, Ano03d, ETMP05, McA08, Bar00b, Lin02].

Open-Ended [Kus02].

Open-Secret [Joh05].

Open-Source [Bol02, Gut00, McA08].

OpenCard [HF00].

Opening [CAC03].

OpenSSH [Bau01c, Sta02b, TvdKB+01, Hos06a, Mos06].

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

Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL+08a, CGL+08b, CGL+08c, DGP09, KWDB06, MPH06, SETB08, TKP+08].

Operation [BR02, BKM07, Dwo03, EP02, Gol01e, HSH+01, JKR01, KY01a, Bud00b, RBB03, Win00].

Operation-Centered [BKM07].

Operational [WA07, GMG00].

Operations [BIP05, IMM01, KDO01, KS05e, LS01b, Ar05, Bug04].

operators [Han00].

Oracle [ABR01, Abe01, Abe04, BF05, Ch03, Gra02b, Nie02b, Pas03, An002c].

Oracle [BNPS02, BB04, KG09, RG09].

Order [AKS04, Bai01a, CV02, KCP01, KCJ+01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Coh03, JZCW05, KS06b, QPV05].

Order-Specified [Tad02].

ordered [HY03, WL05].

Ordering [Mea04].

Orders [HIW01, PS02b, HM00, Huh00].

Ohio [CHH01].

Oklahoma [ACM00, BCDH09].

Organisation [JG07, MMZ00, MP00, C02].

Organizational [PTP07, BJ02].

organize [AUW01].

Organized [HR00, LZL+01, NNAM10, SKU+00, ZCC01, CHC05, CWJT01, DHL06, HWL04, LL06, LWZH05, WM01, Sae02, Shahc03, TJ01a, WHHT08].

Origin [MABI06, MD04].

Original [JQY01].

Origners [Cop04a], Origins [Cop04a].

Outbound [Smi02].

Output [Dic03, YJ00].

Outsource [HL05a].

outsourced [MSP09, MNT06, YPPK09, YL09].

overcoming [CHC04].

Overdefined [CP02].

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

overview [SVE69].

ownership [AS01b, Nik02a, Nik02b].

P [Puc03, AKS02, KR03].

P1363 [IEE00b].
P2Ps [LHL+08]. **PA** [Cor00a, WWCW00].
**PA-RISC** [Cor00a, WWCW00]. **PACA** [Art04]. **Package** [Win01]. **Packed** [LH07].
**Packet** [BR09, WRW02, WLZZ05, BC05b, CMS08].
**Pad** [LDM04, DS02]. **Padding** [AR01, BCCN01, CJNIPO2, KO03, LS01a, Man01, Van02]. **Paddings** [NP02b].
**PadLock** [Lud05]. **PadLock-wicked** [Lud05].
**Page** [IEE00b]. **PageRank** [GPC08]. **pages** [Fal07, Rot07].
**paging** [SZ08]. **Paillier** [CGHG01, DJ01, NSNK05, ST02].
**Pair** [WCJ09]. **Pairing** [BKLS02, BF01b, BF03, CHSS02, GPS06, HCD08a, KM05, LXH07, Kir03, PV06a, SKG09, Sma03a, GPS05, Lee04a, PC05b, VAVY09].
**Pairing-Based** [BKLS02, GPS06, KM05, LXH07, PV06a, HCD08a, HCD08b, GPS05].
**Pairings** [Bon07, BHG07, Jou02, SB04, ZK02, CJI05, DSGP06, LWZH05, LC05b, SW05a, VK08].
**pairs** [LYGL07, Shp01]. **Pairwise** [CLL00, FM02a, HMLvLM07]. **PAKE** [HT08]. **Palace** [McE04]. **Palm** [BDhKB09, WPS01, Wil99, Ano02d].
**Palmprint** [KZ09]. **PAM** [FR02, Sei00b].
**Panama** [BDP09]. **Panel** [FL01b].
**Panopticon** [YN01]. **Paper** [CC09, MFS+09, HN07, Pet08].
**paper-based** [HN07]. **Papers** [An04b, Ano07b, Ano07a, Sch09, Ytrt06, Wil99, Bia03, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GH05, Jol03, Jue04, KKP02, KCR04, LL03, LL04d, MS05a, Mat02, MZ04, NH03, PK03, PT06, RM04, SI01, AMW07, AJ01a, Bir07, BC05c, CZ05, CKL05, DR05, HH04, HH05, PC05a, PY05, WK06, Wri03]. **Paradigm** [BN00a, CS02, G03, K04, YC01, BK04, Can01a]. **Paradigms** [Des00b, Swa01, Hro05].
**Paradise** [USE00b]. **Paradox** [Che01b].
**Parallel** [AHRH08, App07, AEMR09, CPhX04, CTL01, CNP03, CNB+02, Dam07, DM00b, JL08, KY02c, Lin01c, MFS+09, PS04a, RM03b, SS01a, BF06a, FP00, MRT10, OS07, RMPJ08]. **parallelism** [KVN+09]. **Parallelizable** [BR02, Mio02]. **parallelizing** [Fis01a]. **Parallelizable** [LPK03a, LKYY03b]. **parameter** [Wue09]. **Parameterizable** [KPMF02].
**parameterization** [LZP+04]. **Parameters** [ZL02]. **Parametric** [Vir03]. **Parity** [DR09, KKG03, Y01, BK03].
**Parity-Based** [KKG03, DRL09]. **Park** [Kid07, McE04, Cop05, Cop10, HS01a, Sal00b, Sal05a, SE01, Sm01b, 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** [AO00, MSP09, Bao04, Bau03, HC04a, HY03, HLL03, WL05, W05, ZC05].
**Participatory** [CTBA+01]. **parties** [LKY05b]. **Partition** [CTH08, WJP07].
**Partitioned** [DN04]. **partitioning** [BF06a, Che07a]. **partitions** [Sav04]. **Party** [KO04, Lin01c, MR01a, WW05, WV01, CLOS02, CLC08, CMD00, CDG+05, FGM001, FWW04, GCKL08, HM01b, JW01, LH04b, LLL04, LLS+09, LSH00, YC09a, ZLX99]. **Pass** [SK00, MT02]. **passe** [Car00]. **Passes** [Coc03]. **Passing** [Vir03]. **Passive** [Sha01c, VV07, RW07].
**Passive-Only** [V07]. **Password** [BMN01, BMP00, CHV03, CPP04, CSP07b, CC01b, DG03, GL03, GMR05, Har01a, Har01b, J01, KOL01, LSH03a, LSH03b, MPS00, Mac01, MS02, Ngu05, SBEW01, SY06, WH05, YS04, ZW02, CC01a, CC04b, CCK04b, CYH05, DG06, FLZ02,
Fur05, GL06a, HTJ08, JM07, JPL04, Jua04, KLY03, KJY05, KTC03, KCL03, Ku04, KCC05, KHKL05, LLH06, LFW04, LH03, LC04a, Pha06, Sco04, SLH03, Shi05, WL03, XwWL08, YW04a, YWC05, YS02, YPKL08, ZDW06]. **Password-Authenticated** [BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HT08].

**Password-Based** [CPP04, CS07b, GL03, SBEW01, SY06, YS04, GL06a, KHKL05, Pha06, ZDW06].

**password-guessing** [Shi05].

**Passwords** [GL01, KOY01, Per03, Smi01c, Ano03d, FZ06, KOY09, NS05a, RD09, YWWD08, vOT08].

**Patarin** [Bih00].

**Patent** [MP00, Sav05a, Sav05b].

**Path** [GXT+08, CCD+04, Dew08, ZSN05].

**path-based** [CCD+04].

**Path-quality** [GXT+08].

**Pattern** [ABM08, BDhKB09, BLP06, BCCN01, LS01a, TIGD01, Buh06, LYGL07].

**Pattern-based** [BLP06].

**Patterns** [DD02, MP06, WCJ09, JLC07].

**Pavol** [Sal03b].

**pay** [Joy03a].

**pay-as-you-watch** [Joy03a].

**payload** [KC09a].

**Payment** [MV01, RMCG01, YKMY01, Has02, HP00, SH00].

**PC** [BSW01, Ste05c].

**PCIXCC** [AV04].

**PCs** [BDET00].

**PDA** [GW08].

**PDF** [ISO05, CNB+02, ISO05].

**PDF/A-1** [ISO05].

**Pearson** [Puz04].

**Pebbling** [DNW05].

**Pedersen** [GJKR03].

**Peer** [Art04, HR02, RH02, ATSO4, LLY06, MPH06, PI06, WCJ05, YI04].

**Peer-assisted** [Art04].

**Peer-to-Peer** [HR02, RH02, ATSO4, MPH06, PI06, WCJ05].

**PeerAccess** [WZB05].

**Peinado** [YRY05a].

**PEM** [Dav01b].

**Penguin** [Bau01a].

**Phonetic** [Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a].

**Pennsylvania** [IEE05a, IEE08].

**People** [ASW+01, CG05, Lov01].

**perceptions** [WDCJ09].

**Perceptual** [PBM+07].

**Perceptually** [EFY+05].

**Perfect** [AJO08, CLLL00, DN02b, DSS01, Sun00a, DM07a, SC02c, SY06, ZD05].

**Perfectly** [DMS00, KSR02, SNR04].

**Perform** [Kin00].

**Performance** [ACM01b, BH00a, DPR01, Dra00, EYCP00, FZH05, Int00, Ken02a, Ken02b, Kra05, LWK00, MM01b, NFQ03, PWGP03, PBTW07, SSKS00, SW00a, SB01, Siv06, SL00, SGPH98, WBRF00, WWCW00, WS02, XH03, YEP+06, Zea00, AKNRT04, BVP+04, BZP05, CKL+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTW07, SK03, YZ05].

**performance-friendly** [CRSP09].

**periodic** [XQ07].

**Periods** [KKH03].

**Perl** [Sal03b].

**Permutation** [DMS00, HSR+01, IYK02, KKK03, KO03, LSY01, DP02, IYK03].

**Permutations** [BPR+08, CHL02, KO00, MP03, KKKP05, WV00].

**Persistent** [AGT01, ST06].

**Person** [KJR05, LLT+04, PK01, BS01b, KN03, Li05, LST+05, PY08].

**Personal** [Bar05, EHMS00, SEK01, SEK02, Tyn05, UP05, Wal09].

**Personalised** [TNG04].

**personalized** [GPC08].

**Perspective** [LL01].

**Perspectives** [BMV06, SM08].

**Perturbation** [HWH08, ZY08].

**Pervasive** [BDhKB09, JW05, LKHL09, Lut03, Lut03].

**PET** [MS05a].

**Peter** [For04, Uzu04].

**Petersburg** [GK05].

**petitions** [Cal00b].

**Petri** [LKJL01, AADK05].

**PGP** [McL06, An00a, BCH+00, Dav01b, Dav01c, JKS02, Luc06, Opp01].

**PGV** [BRS02].

**pharaohs** [Pin06].

**Phase** [CDF01, Ig02, KLB+02a, Che07a, Che08a].

**Phase-Conjugate** [Ig02].

**phase-shift** [Che08a].

**Phil** [Bar00a].

**Philadelphia** [IE08].

**Phil** [McL06].

**Philosophy** [Cop04b].

**phishing** [Bel04].

**Phone** [CAC03, Fox00].

**Photonic** [TWNA08].

**Photonic-based** [TWNA08].

**Photons** [Bar00c].

**Physical** [CGMM02, LR07, YKLM02a, GVC+08, UHA+09].

**Physicist** [BZ02].

**physicists** [RP00].

**Physics** [MYC01, Sch06b, BEZ00, BEZ01, Dwu03].
physiological [RFR07a, RFR07b, RFR07c].
Pi [OS08]. PIC [Fin02]. pick [Clau00b].
Picks [PM00]. PicoDBMS [PBVB01].
PicoDMBS [BBPV00]. Picturing [Paut03].
Piecewise [LLL+01]. Pigeon [Pem01b].
piling [Kuk01]. piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03].
FAPE [CBD+05]. Pipelined [MD05, Mis06]. PIR [BIM00].
Viro [BBPV00]. Picturing [Pau03].
Piecewise [LLL+01]. Pigeon [Pem01b].
piling [Kuk01]. piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03].
FAPE [CBD+05]. Pipelined [MD05, Mis06]. PIR [BIM00].
Viro [BBPV00]. Picturing [Pau03].
Piecewise [LLL+01]. Pigeon [Pem01b].
piling [Kuk01]. piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03].
FAPE [CBD+05]. Pipelined [MD05, Mis06]. PIR [BIM00].
Viro [BBPV00]. Picturing [Pau03].
Piecewise [LLL+01]. Pigeon [Pem01b].
piling [Kuk01]. piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03].
FAPE [CBD+05]. Pipelined [MD05, Mis06]. PIR [BIM00].
Viro [BBPV00]. Picturing [Pau03].
PPK [YDKM06]. PQCrypto [BD08].
Practical [Ano01c, AR01, Ash03, ACJT00, BDK+09, BF05, BLMS00, CS03a, Cap01, CDR01, CJT02, Chi08a, Chi08b, Chi08c, Chi08d, CS03b, DK01, Dre00, FS03b, GSS03, GIS05, GH02, HQR01, HJW01, Ina02a, Ina02b, IIT03, Kan01, LMV05, LCD07, Lat03, LWK05a, MM02, MSU05, OM09, PBD00, Pel06, Poo03, Roy00b, Sug01, Wei04, YSS+01, Bro05b, DKL+00a, Har05a, KSW06, Luc06, Mos06, MSV04, Sha01a].
Practice [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti95, Sti02, Sti06c, Lat03, Spr03].
Practices [CF05, Ste02].
practitioners [PP09].
Pragmatic [BMW02b].
Prague [MJ04].
Pre [Adl03, AA08]. pre-processing [AA08].
Precise [Wal01].
Pre-computation [SLG+05].
predecryption [RSP05]. Predict [Die03].
predictable [Bel08]. Predicting [AG09, BGPGS05]. Prediction [AKS06, SLG+05]. predictive [vOT08].
predistribution [HMvdLM07, JRR09, TP07]. Preface [CGM07]. Prefix [FXAM04, RW07].
Prefix-preserving [FXAM04, RW07].
Prehistory [Ir00]. Preliminary [KS00b, KKS00b]. Prentice [For04].
Prentice-Hall [For04]. Preparations [FJ04]. Prepared [ASW+01].
Preprocessing [BMI00, CKK03]. presence [BIW08, GXT+08, Mis08, VS08].
Preservation [Che01b, Dur01, Bro05a, DVP09, IS05, LG04]. Preserve [NNT05].
Preserving [DN04, KS05c, LP00, M603a, YW08, AKSX04, BR06, BSSM+07, BA06, DVP09, 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, DM07]. Prevention [JT05, PZ01, PZ02a, Gei03, Smi03]. Price [AS01a, Bra01b]. Primality [BT02, Che03].
Prime [ACS02, Bai01a, Har07a, Pau02a, WS03, JL03, dW02]. Prime-detecting [Har07a]. Primer [KLB+02b, Lod06].
Primes [Ano03f, SZ01, HLLL03, Ste08, AKS02].
Primitives [CF05, IYK02, MM01, ST01a, ST02, IYK03].
Privacy [AN00i, AEV+07, BBPD01, BSSM+07, CDM+05, Ch08a, DL98, DL07, DKFX05, DN04, GS02a, GMM08, HY01, KS05c, Knu07, LP00, MP00, Pap05, PBD05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YW08, Bel04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, Sae00, SI04, Ty05, WK05, ZYL05, ZSM05, MS05a, Jan08a].
Privacy-Enabled [Por06].
privacy-enhanced [ZSM05].
Privacy-Enhancing [SE09].
Privacy-Preserving [DN04, KS05c, YW08, BA06, HJW05, Pin02, Pin03].
Private [AF04a, AF106, BDF+01a, BIM00, BY03, BSW09, BJLS02, BGW05, ISW03, 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, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLMM05, Gol99, JZCW05, KY00, MRST06, PBMB01, dH08, Neu04].

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

Probing [ISW03].

Problem [AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK+02, Cou01, CLZ02, DIS02, FL06, Gen03, GPP08, KK02, LNS02, NBD01, Wag02, BKY03, CGH06, CJT04, DLMM05, HGS03, Hsu05a, HYS05, LD01, Luk01, Pei09, Shp05, SCL05, WL02, Whi09, Yas08, KM04a].

Problem-solving [Whi09].

Problems [BI05a, Can06b, Hro03, MV03a, OP01a, TvdKB+01, VDKP05, HL05d, KX00, LMTV05, LMC+03, RSS04].

Procedure [LY07]. Procedures [DJ06, BBK+03b].

Proceedings [ACM00, ACM02, ACM04a, ACM05a, AAC+01, Bon03, EBC+00, FMA02, FLA+03, SM07b, USE00b, USE00a, USE00d, USE01b, USE01c, USE01a, USE02a, USE02c, USE02b, WKP03, Yun02a, ACM05c, ACM07, ACM08, ACM09, AUW01, AJ01b, BS03, Bel00, B+02, Boy01, Buc00a, BC01, HA00, Hon01, IEE00a, IEE01a, IZ00, Kil01a, MS05b, Oka00, PPV96, Pri01, Pre00, Q500, RD01, Roy00a, SMP+09, ST03d, YY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BDZ04, BS01b, Bih03, BCDH09, BD08, CC04a, CV04, Chr00, Des02, DFPS06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE05b, IEE07, IEE08, IEE09b, JYZ04, JF08, JM03, Joy03b, JQ04, KJR05, KLG04, Kim01, Kim02, KN03, Knu02, KP01, KNP01, KM07, Lai03, Lee04b, LL+04, MM06, MJ04, May09, MS02c].

Proceedings [Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sma05, Syv02, TBJ02, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZYH03, BCKK05, Cra05a, DV05, DWML05, DUK05, GKS05, IKY05, Kil05, Li05, LST+05, Men07, Poi06, Sho05a, Son00, dCdVSG05].

Process [Kwo03b, MNT+00, BDFP02, HL06, MRST06, VKS09]. Processes [BDP02, ALV02, BDN02, Whi09].

Processing [ISSZ08, KLB+02b, PCK02, AA08, AA04a, Ayo06, YPSZ01].

Processor [An02e, BBGM08, EP05, FBWC02, FZ05, GC01b, Int00, KBD03, KPMF02, TLYL02, ST03a, SHL07].

Processors [TLYL04, CW02, CRSP09, Geb04, LJ05a, YG05, YLT06, ZYL05].

Procurement [Lad06].

produce [Zir07]. producing [SOIG07]. product [KSWH00, Sun02].

Products [ACS02, An02d, An02e, Knu07, An00c].

profession [Wal04].

professional [Dew08, V00].

proficiency [Dew08].

Profile [PJC01].

Profiles [MV01, PJK01].

Program [H00, Bec02, GGH+08, Kov03, KH03, CS08b].

Programmable [Dam07, GC01a, HV04, Sni02].

Programmer [Wil01b, Bon00, Che00a, DKK07].

Programmers [Coc01a, Wei04, Gou09].

Programming [AS+01, An02d, Coc03, LHME06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03].

Programs [BGI+05, Ark05, SLTB+06].

Progress [KK06, KSS00, RD01, Roy00a, CV04, DV05, JM03, MM06, MS02c].

Project [Fri01, IY00, MNT+00, Pau02a, Sal0x, Gou09, LR01, Lvo01, MW01, Sha01a, Coc01a, Coc02b, IY00, Pre02b].

projects [Gha07].

Prolog [Bla01a, Bla01b].

Promise [An02f].

promises [Pau02a].

promote [WK05].

Promotes [Bar02b].

Prone [MLC01].

Proof [Abe01, Abe04, AS01b, An09c, ARC+01, BDP02, Cor02, GK05, SOIG07, SPMLS02, Tec06, BR05, Chi08b, Chi08c, Chi08d, GM04, HSD+05, LM05, PBD07].

proof-of-compliance [LMW05].

Proof-of-Concept [ARC+01].
Proofs
[BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, GOL99, HG05b, SV08b, dH08].

Propagation
[LJL05, QPV05].

Properties
[ABC+05, BM01c, KY01b, LLL+01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].

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

Proposal
[DPVR00, Mac00].

Proposed
[Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06].

Protect
[ETZ00, BBN+09, WK05].

protected
[CYH05, PKH05, ZCL05].

Protecting
[Des00c, EHMS00, KY01d, Kra01, LKM+05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYL05].

Protection
[CJ+02, DKFX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XZF01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].

Protections
[JT01a].

Protocol
[Ano01a, Bel01, BPST02, BGM09, BL02, CK02a, CJ03d, CWY05, Cim02, ECM00b, Fre03, GJKR03, GL00, HS07, JP02b, JRFH01, JT05, KLN+06, Kak06, Kra05, Ku02, LCK01, Mea01, MS05, NS01b, Rub00, RMC01, SK00, Tan07b, TZT09a, TZT09b, WHL05, YSR01, Asl04b, BP03a, BC05b, Bla01b, BDFP05, BK05, CS04, CCK04a, CC04b, CYY05, CC05c, CYH05, Che04a, CLC08, CJO3b, CJ04, CL09, CJL05, DP04, GM04, GTO4, HT08, HHWM03, HLTJ09, HHC05, KO08, KKL09, KTO3, LC03, LFO3, LKKY03a, LKY03b, LW04, LHL04a, LKY05b, LKY05c, LHO8, LSH03a, LCO5b, Lk01, MS03a, Par04, Pan01, RG06, Shi05, SW05a, SIR04, TM06, Tsa06, Tse07, WK05, WLT05a, WHHT08, YW05, YWL05, YTW05, YC09a, YS02, YSH03, YR05b, YRY05c, YPKL08, ZW0L01, ZL04c, ZDW06, ZYW07, LSH03b].

Protocols
[AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, BM01, BM03c, Bra01b, BLD09, CKPS01, CT08a, CCMR02, CCMR05, Cir01, CV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, JP07, JW05, KS00a, KY03, KL08, Kra03, Kiis02, MS02a, MN01, PB00, PR08, PZD09, Rot01, Shy02, SC01, Tee06, AA04b, AKMR04, Bar06a, Bau05, Bel07b, BDS08, BFGT08, BP05, BL06, BD04a, BR05, Can01a, Can06a, CP07, CKR08, CWJT01, CH07a, Cho08b, Chr00, Chr01, CJM00, Coh03, CC05d, CDL06, DFG00, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV+09, LLL04, LLY06, LLS+09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SL05a, SR00, SW06b, SY06, WLMH06, YS04, ZLX99, ZL04b, PDM09, Puc03].

ProtoMon
[JT05].

Provability
[GOR02b].

Provable
[HM02b, HLL+01, HSL+02, KSH01, PB05, SL+00, BGP09].

Provably
[A000, ACJT00, BMP00, BCP01, BCP07, CHK00, DG03, DG06, HL09, HL07, HS07, JMV02, MS03a, NS05, NSS02, VMS05, WLMH06, XS03, ZCL05, BKN04, CC09].

provenance
[HWS09].

Provers
[MV03a].

Provide
[AB01, Sch01a].

Providence
[IEE07, Sil01].

Provider
[LDM04, HILM02].

providers
[MV03b].

Provides
[OT03b].

Providing
[BAC02, BDS+09a, DeL07, Lin07, Par04].

Proving
[Che03, FS01c, GN01, Tee06].

Provision
[Kha05].

Proxy
[AH05, BCL05a, DKFX05, LCK03, LC05b, PL01, Rds01, Sha03d, ZJ09, AFGH06, CCH04, DY09a, HW03, HW04, HWH05, HW05, HC04b, KHL09, LL05b, LHH05, LC05c, LW05c, PK05, Sha05b, SHT05, TYH04, YTH04, ZL05].

proxy-enabled
[DY09a].

proxy-protected
[PK05, ZCL05].

psBGP
[vOWK07].

Pseudo
[BH05, FWW04, Gen00b, LLL+01, HLL+08,
MP03, SXY01, TZT09a, TZT09b, WP03, XYYXY11, BG09, CFY+10, GB09, MFK+06, NR04, PLsvdLE10, PSP+08, RGX06, SH11, SM11, SL09, WW08, XSWC10, YZEE09.

Pseudo-Random [LLL+01, MP03, WP03, XYYXY11, Gen00b, SXY01, CFY+10, MFK+06, NR04, PLsvdLE10, RGX06, SH11, SM11, SL09, WW08, XSWC10].

Pseudo-Ransom [BH05].

Pseudo-signatures [FWW04].

dpseudonoise [HG05a].
dpseudonym [CG06].
dpseudoprimes [ZT03].

dPseudorandom [BCGH11, CDI05, DN02a, DI05, DP02, Fin06, Flu02b, FIPR05, GM02a, IYK02, LMHCETR06, Nie02c, RSN+01, Aam03, BGPGS05, IYK03, KSF00].

dPseudorandomness [GM02c, IK00, IK01, KYHC01, LLH01, Lee03b, MV00, Shp03, Gol99].

Psychology [MYC01].

PUB [Nat00].

Public [ANS05, AUW01, APV05, Ano01n, AEQA05, AF03, BC05a, BDG+01, BDZ04, Bar00c, BPS00, BBPD01, BLM01, Bih00, BDTW01, BST02, CHK03, CHK05, CDM+05, CHM+02, CHK008, CI03c, Chi08a, CCW02, CT09, CCM01, CS02, CS03b, DPK+04, DZ01, Des02, DY09b, DKXY02, DPK+03, ESG+05, ES00a, FL06, GHW01, GC01b, GB+04, Gut04b, HCD002, HR05, HGM05b, HR04b, HJ01, HC08, IEE00b, IZ00, Jou02, Kat05b, KKM01, KM01a, Kim01, KLY02, KYY02c, KLC+00, K101b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, LXH07, Lin03, Lin00b, MR01b, MR01c, Mö03a, Mö03b, Mö01a, NPD02, NBD01, NSF02, OTU00, PHK+01, Pei09, PR01, Poi02, PHM03, Qui01, RSA00a, RKF02, ST01a, ST02, Sin01a, Sm01c, Ste01, TSO00, TT01].

Public [Van05a, WZW05, WHI01, WW00, Wya02, YKMY01, YG01c, YDKM06, Zhe02a, AG09, BHM03, BCD05a, BCW05, BBN+09, Ben01a, BB79, Bra01a, BD04b, Cal00b, CCT08, CL02b, CWH00, CHT05, CJ05, CKRT08, Ch06, Cre00, DMT07, EKRMA01, EHK04, FMY02, FP00, Ga02, GH08, GKM+00, GS01, Gor05, GWM01, HCD08a, HCD08b, HHG06, HW04, HL04, Iwa08, IM06, Jan08b, JXW05, JZCW05, KPS02, Kob00, KW00, Kos01c, LF03, LHL04b, LK05b, LCK04, Lin01a, LLW08b, LS01c, Lp06, LWK05a, MWS08, Mü01b, PI06, PC09, SN00, SJ01, Sha04b, Sha05b, Shp04a, SLC05, Sun00b, SZP02, SC05c, TO01, THL05, Ts05, TJ03, VS01, WDL090, War00, Wu01, WH03, WLO4b, hY08, YRS+09, ZSM05, AL06, BDZ04, Ben02, CZ05, Des02, GL05, KGL04, Kim01, NP02a, Van05a, YDKM06].

Public-Key [Ano01n, AEQA05, BC05a, BBM00, BBPD01, BLM01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DPV04, DZ01, DPK+03, ESG+05, ES00a, FL06, GHW01, GC01b, HR05, IE00b, Kat05b, KKM01, KM01a, KLY02, KYY02c, KLC+00, K101b, KM04b, Kos01a, Kos01b, KY01e, Kur01, LP03, Lin03, Lin00b, MR01b, MR01c, Mö03a, Mö03b, NSS02, OTU00, Poi02, RSA00a, ST01a, ST02, Sin01a, TSO00, TT01, WHI01, YDKM06, AUW01, ED03, FG05b, Pei09, BHM03, BBN+09, BD04b, Cho06, FMY02, FP00, GM01, HCD08a, HCD08b, HHG06, Iwa08, Jan08b, JXW05, JZCW05, Kos01c, LF03, Lin01a, LS01c, Lp06, MWS08, Mü01b, SN00, Shp04a, SLC05, Sun00b, TO01, ZSM05, GL05].

Public-Key-Based [YKMY01].

Publication [Top02, DGMS03].

Publications [Bee05].

publique [RSA09a].

publish [SL05b].

publish-subscribe [SL05b].

Published [MS03b].

Publishing [Ano02d].

puc [Car00].

PUFs [MKP09].

Purpose [Ano07b, Ano07a, ESG+05, GS07a, GPP08, SGK08, L05a].

Purposes [LS05a, FSGV01, PBV08].

Push [Pau03].

puzzle [LF03].

Puzzles
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 [BG09]. Quadratic [BT02, Coc01b, HJW01, SP05, CCS08, HM00, Hii00, HP01, LD01]. Quality [BW07, TL07, DMSW09, GXT’08, KC09a, WWTH08]. quality-conscious [DMSW09]. Quantifier [KS06b]. Quantifier-free [KS06b]. Quantitative [Bai08, ME08a]. Quantization [DRL09, WC04, WC05]. Quantum [AC02, ATSVY00, Ano02f, Ano02g, Ano02h, BYJK04, BOHL’05, B9D02, BB’02, BG09, BLM00, BEM’07, Coc03, DFS04, EK02, DFS05, DFS05, DMS00, Eil04, Ett02, GKK’09, GH02, GW00, GRTZ02, HV09, Hay06, Imr03, Ina02a, Ina02b, Kak06, KK06, KL’02b, LB04, LW’05b, Moc01, NA07, OTU00, Pal02, PC09, Pr05, Ree01, RK05, Ser06, SR07, Sti11, TO01, W09, Wri00, Y100, Y101, ZLG01, ABW09, Ano03g, Ano06d, BYJK04, BCG’02, Ber09b, BEZ00, BEZ01, BLS09, DFS05, Duw03, EK02, GKK’07, Gav08, Heg09, HH06, IM06, JZ00, JRS09, JS00, JO01, KO07, KH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Ros00b, Sn09, Sin00, Smo04, UHA’09, BZ02, BD08, BB09]. quantum-storage [DFS05]. quarter [Kob00]. quarter-century [Kob00]. quarters [Cla00b]. QUARTZ [PCG01]. Quasi [MD05]. Quasi-Pipelined [MD05]. Quasigroup [MNH07]. Québec [ACM02]. Queen [Rec01, Ros00b, Sin99]. Queenstown [Zhe02b]. queries [CKK03, Fis01a, GP08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC’09]. Query-preserving [GA03]. querying [FJ04, ÜG08]. question [OC03]. Questions [Ett02, Joh00, Jac00]. Queues [WBL’02]. queuing [CUS08]. quick [Dew08].

R [Che05b, Kat05b, Pag03, Spr03, Bib00]. R&D [Mau05]. Rabbit [BVP’04]. Rabin [Bon01, Gen04b, Miy01]. race [Hil05]. Rackoff [MP03, Pat03a]. radar [GG05b]. Radiations [SGM09]. radical [Web02]. Radio [Sak01]. RadioGatún [BDP09]. Radix [HKA’05, JY01]. Radix-rails [Fox00]. Rainbow [DS05a]. Raises [MP00]. Raising [Cos03]. ramp [IV06]. Rampaging [Coc02b]. Random [Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CTY09, Chi08e, Die03, DGP07a, DGP07b, DV08, EHH’03, Gra02b, GPR06, HSR’01, HBF09, Int03, JRR09, Kel05a, Kel05b, LLL’01, LM02, Lys02, MP03, Mtr02, NNT05, NAM10, Nie02b, Pas03, Pat04, Ran55, Ran01, RSN’01, SDF06, TWNA08, TL07, Tip27, TZT09a, TZT09b, Vav03, VKS09, WP03, XYX11, BK07, B08, B09, BG07a, BGL’03, CFY’10, CJL06, CO09b, DGP09, Fis01a, GVC’08, Gen00b, GB09, HG05a, HLwWZ09, HAM07, JAW’00, KH08, KB39, KG09, LGKY10, MI09, MRT10, MFK’06, NR04, Pan07, PSC’09, PLsvdLE10, P’08, PC00, Reg05, Reg09, RG09, RGX06, SN11, SM11, SS03, SXY01, SR07, Sti11, SK01b, Sug03, SL09, UHA’09, WW08, XSWC10, YZEE09, BH05].

Random-Error [LM02]. random-self-reductions [Fis01a].

Randomats [Sam01]. Randomization [Hro03, WHH05]. randomization-enhanced [WHH05]. Randomized [Sem00, Hro05].

Randomness [DD00, DD04, DGH’04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, MS10, SB00, Sn00a, BBN’09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03]. Range [CW09].
Rank [Sun00a, DW01, Sim02]. Ransom [BH05]. Rao [Zyr01]. 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 [GHJV00, GHJV01, IK00, IK01, KM00, KM01b, Rry00, STK02]. RCES [LLCL08]. RCES/RSES [LLCL08]. re [AH05, AFGH06, KHL09, Sma06]. re-encryption [AFGH06, KHL09]. re-signatures [AH05]. re-thinking [Sma06]. Reachability [AL00a, MT07]. REACT [OP01b]. Reactive [Shy02]. Real [BSW01, Dri02, GSB + 04, JBR05, SP05, Sta05, YKB08, GM04, HP01, Lie05, Pot05, SL07, SGPH98, YZDW07]. Real-Time [Dri02, GM04, YZDW07]. Reality [Coc01a]. Really [CZB + 01, Wei00, Dav01c]. reason [Lau08b]. reasoning [IK03, IK06]. Rebalanced [SWH + 09]. Rebalanced-RSA [SWH + 09]. rebels [Lev01]. Rebuild [Salxx]. Rebuilding [Sal05a]. Receipt [HS00]. Receipt-Free [HS00]. Receipts [Cha04]. Receive [Coc03]. Receiver [CCD07]. Receivers [Nnl01, Sbb05]. recency [SW02]. recently [JK01a]. Reception [Top02]. Recipes [VM03]. Recipient [ANR01, Kur01]. Recipients [Coc01a]. recoding [SSST06]. Recognition [Ano02d, Llt + 04, Lst + 05, Ttz09b, Hs02b, Li05, MMJP03]. Recommendation [Bar06a, BK06a, BK07, Dwo03, NIs03b]. Recommended [Kel05a, Kel05b]. Reconfiguring [BNPW03, Pgt07]. Reconfigurable [FD01, FZ05, GC01b, KB03, Lz04, MKP09, Mmh02, SJ09, KG09, SR0L03, CMS08, DHL06, GC00a, Hbc + 08, rhs03]. Reconfiguration [PBTW07]. Reconsidered [Sho01]. Reconstructing [CDF01, FL06, PS01a]. Reconstruction [AF03, CF01b, CDF01, Jj00d, KY01c]. Records [Dur01]. Recoverable [Nzcg05, Nz05, SGMV09, Yy00]. Recovery [BDK + 09, BM01c, Ckm00, MMZ00, OS01, PBC05, SVW00, TC01, Vv07, WC05, WL01b, CCh05, CJ05, CL04, HW05, LKJL01, PSp + 08, Shao4b, SIR04, TJC03, Wu01, ZF05]. Recursive [WHHT08]. Recycling [DPS05, TR01a, TR01b]. Red [Sas07]. Red-Eye [Sas07]. redistribution [KB09]. Redondo [IEE00a]. Reduced [BDK02b, CC08, CS05c, FKS00, HQ01, HSR + 01, KKS00a, KS00b, KKS01, KML + 02, KM01b, KKS00b, MHL + 02, NP01, STK02, SK01, YSD02, CV05, Küh01, SK01a, Thi03]. Reduced-Round [FKS00, KKS00a, KS00b, KKS01, KML + 02, KS00b, NP01, YSD02, CV05, Küh01]. Reducibility [DM00c]. Reducing [AL07, BIM00, SPH06]. Reduction [CM05a, CH07c, Dhe03, Gr01, HGG07, Kid02, PG05, ALV02, HG07, Sug03]. reductions [Fis01a]. Redundancy [Ab01, BR00a, FM02c, YL005]. Redundant [MF01, Tan07a, PS04a]. Redwood [KKP02]. Reed [KY02b]. Reference [BR09, CPS07, Pas03, RS00, Sal07, vT00]. Reference-Watermarking [BR09]. Refined [Sma03b]. Regarding [Gmp01a]. Regex [BTTF02]. Region [Bsn00, Bur00]. Region-Based [Bsn00]. register [HTW07]. Registrars [CGFSH09]. Registration [HLM03]. regression [mSgFl05]. regulation [Mat05]. Regulations [Gen01, Mad00b, TMM01, Ano00g, Cler00b]. Rehearsal [Ahm08]. reinforce [SWR05]. Rejewski [BCB + 05, Kap05]. Related [BDK + 01a, Can06b, CY08, FKS00, KI01b, KLML05, S01a, Buc00a, Gutxx, Haur04, Hen06a, Sch00b]. Related-Key [FKS00]. Relation [ABC + 05, NN06]. Relational
Puz04, Ree01, Rot07, See04, Spr03, Ter08, TvKB*01, Top02, Uzu04, Was08a, Her09b, Kat05b, Kid07, Lu07, McE04, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wal00. Reviews [For04, Kid00, Sal03b, Sty04]. Revised [Bla03, BC05c, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR00a, G02c, GH05, HH04, HH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04d, Mad00b, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PT06, RM04, Sil01, Ytr06, AMW07, AJO1a, BK07, Bir07, CZ05, CKL05, DR05, Irw03, PY05, WK06, Wri03]. Revisited [ABC+05, Ano02h, BM01b, CDMP05, Knu00b, NS05c, OSSST04, Hes04b, OH08b, ZZT05]. Revisiting [AEAQ05, Har01a, Har01b, JMV02]. Revocation [BDTW01, CL02a, Gen03, GST04, NNL01, TT01, ZSM01, KSW06, LH05, SW02]. revoke [NN03]. revolution [Bor00, Con00]. Revolutionary [CMB+05]. Rewriting [Cir01, HR04a]. RFC [BWBL02]. RFID [And04, AL07, ACDM05, Ayo06, BLDT09, CSS08, CH07a, CL09, FW09, Fin03, KKJ+07, OS06, PL04LE10, Ros06a, SE09, TZT09a, TZT09b]. Rhee [Küh08]. Rhode [IE07]. RI [Sil01]. Right [Dhe03, GS07b, HKPR05]. rightful [CL08, Lin01a]. Rights [Bar00a, BNPW03, Dref00, Scr01, TMM01, Wya02, BA06, UP05]. Rijndael [BB02, MP01a, SKU+00, Wer02, CKK+02, CB03, DR00a, DR00b, DR01, DR02b, FKS+00, FKL+01b, FKL+01a, FSW01, FD01, GM00a, JmdXgXm05, KY01b, KMT01, KV01, Luc00, MM01b, MMH02, PSC+02, RDJ+01, SMTM01, SR0Q3]. Rijndael-Like [PS+02]. Ring [BSS02, Nao02, WBL01, ZK02, Her07]. Rings [BLST01]. RIPEMD [DG02, WFLY04]. RISC [Cor00a, Gro03, WW00]. RISC-Based [Gro03]. Risk [WA07, Voi05]. Risks [ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, Psv01, Sch00c]. Rivest [BB79, Coc03, SP79]. RMI [JRB+06, Mar02a]. RNS [BL04, BKP09, NMSK01]. Road [BDPV09, HR04b, PB01]. Roadmap [Coc02b]. Roaming [CAC03, YWD08, SSM+08]. Robotic [Kum07]. Robots [Coc01a]. Robust [BB00a, BR09, CJ03d, CW05, DDO+01, FCZ05, HH09, hKLS00, Lin00a, LHS05, LL06b, PJK01, SG07, SOHS01, SDF00, SDF01, VK07, WNY09, WL04b, WMD08, YPSZ01, ZTP05, KA09, LCZ05c, LKZ+04, Mit00, MB08, TND+09, YY05b]. Robustness [CS05c, HM01b, Rot01, AEI17, CKL+09]. Rogaway [MW04]. Roger [GG05a]. Role [SBG02, YT09, ZGLX05, C04a, Cra05b, Gor05, Man04, You04]. Role-Based [YT09, ZGLX05, Cra05b]. Roles [LLL+03, Vix02]. rollover [Gue09]. Roma [AAC+01]. Rome [IE04]. Ronald [Coc03]. root [Pet05]. rootkit [Bh09]. Rootkits [HB06]. Roots [G06, HCK09, CAC06]. Roseau [PY05]. Rosen [HR13]. Rotation [RBF08]. rotations [SK03]. Rothe [Fal07]. Rough [Nao02, WG05]. roughness [Lav09]. Round [III00, BP04, Bi00, BF00a, BDK02b, Che03, DPV04, DI05, Dra00, FKSW00, GKK07, GI-K02, HSR+01, Kan01, KO04, KKS00a, KKS0b, KKS01, KML+02, KKS00b, LKVL09, Lin01e, MP03, MHL+02, NV01, RR00, Ros00a, STK02, WBRF00, Wer02, YSD02, CV05, CLC08, CKL+03, DLP+09, GI-K01, HSL+02, Küh01, LKH+08, MR01b, Pha04, SW05a]. round- [CL08]. Round-Complexity [Ros00a]. Round-Optimal [KO04]. Rounds [BDK+09, CD01a, HSI02, KM01b, Luc00, Pat03a, Pat04, G00a, SK01a]. Routing [BG0Y08, CL05, Ken02a, KB09, LAPS08, LHC08, MABI06, PS08a, RVS09, vOWK07].
RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, Shp04a, Wal00, Adl03, Ano01a, Ano02e, AR01, BI04, BS02, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BJN00, BF01c, Bon01, BCCN01, BP01b, CNS02, CDL00, CW02, Che01a, CKY05, CNPQ03, CK00, CJNP02, CS00, CS03c, CD01b, DK01, DT03, Du08, Du09b, DN00b, FS02, FS01a, FM03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gro01, HN04, Her07, HLL00, HLH00, HLL03, Int00, Jan08b, JS05, Jon08, JK02b, JK02c, JG01, Kal01, Kal03, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, May04, Mj03b, MP01e, NZ05, NS01b, Nit09, Nov01, NMS01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Sha03a, Shp01].

RSA-based [NZ05, BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZ05, Sei05, WL05, WY05, YPK08, Y00]. RSA-Encrypted [CD01b]. RSA-Primitive [ST01a].

RSA(R) [Ano06b]. RSES [LL08]. RST [ZL08]. Rueppel [Ara02]. Rules [Bla01a, Ano00c, Bla01b, GM04, Ste02, Wie09].

Running [ZL04c]. Running-mode [ZL04c]. Runtime [PBTW07].

Ryan [Puc03]. Ry [CJR05]. Ryu [KCC05].

S [BZ02, Kat05b, Puc03, Bih00, BCMM00, Dav01b, Dav01c, FM02b, JmDx05, LG09, Opp01, SMTM01, ZC00]. S-Box [FM02b, SMTM01, JmDx05]. S-boxes [BCMM00, ZC00]. S/MIME [Dav01b, Dav01c, LG09, Opp01]. SAC [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR01, HSS04, ST01d, VY01]. SAC’99 [HA00]. SAFE [Un00a, U00e, Un00d, U00g, U00h, ACS02, LBR00, Lys08, Oiw09]. Safe-Prime [ACS02]. Safeguard [LX05].

Safeguarding [Sty04, Bar03]. safer [An000f, NV01, BDD03]. safety [HM01a].

SAFASI [WAF00, Saga [Eva09]. Salomon [Pap05]. Salsa20 [Ber07, Ber08].

Salt [PKBD01]. Salzburg [DKU05].

Samba [BH00a]. SAML [RR04]. Samos [KGP04]. sampled [WW06]. sampling [KB39, 809, Tip27].

San [ACM03a, ACM03b, ACM03c, ACM07]. SASA [NZ05, BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZ05, Sei05, WL05, WY05, YPK08, Y00].

SASAS [BS01c]. SAT [KLN06]. Satan [Mea04]. satellite [CC05c, HY03]. Satisfy [PHM03]. satisfying [BPV05]. Saturation [Luz02a]. saving [Lev01]. Savings [CAC03].

SAX2 [TEM01, Hei01]. Say [Sta05]. says [An0001, 04]. SBLH [JK02a]. SBoxes [WOL01]. SC-CFS [It01]. SC2000 [SYY02, YSD02].

Scalable [CPhX04, HKA05, KY03, KH05, SPQ06, LLW08b, ST03a].

Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwW05, 05]. Scale [BWE00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a].

Scalable [CPhX04, HKA05, LLW05, KY03, KH05, SPQ06, LLW08b, ST03a].

Saying [Lev01]. Savings [CAC03].

SAR [B02]. SASA [BS01c]. SAT [KLN06]. Satan [Mea04]. satellite [CC05c, HY03]. Satisfy [PHM03]. satisfying [BPV05]. Saturation [Luz02a]. saving [Lev01]. Savings [CAC03].

SAX2 [TEM01, Hei01]. Say [Sta05]. says [An0001, 04]. SBLH [JK02a]. SBoxes [WOL01]. SC-CFS [It01]. SC2000 [SYY02, YSD02].

Scalable [CPhX04, HKA05, KY03, KH05, SPQ06, LLW08b, ST03a].

Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwW05, 05]. Scale [BWE00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a].

Scalable [CPhX04, HKA05, LLW05, KY03, KH05, SPQ06, LLW08b, ST03a].

Saying [Lev01]. Savings [CAC03].

SAR [B02]. SASA [BS01c]. SAT [KLN06]. Satan [Mea04]. satellite [CC05c, HY03]. Satisfy [PHM03]. satisfying [BPV05]. Saturation [Luz02a]. saving [Lev01]. Savings [CAC03].
CDM00, DS05a, DKFX05, FS01c, GJSS01, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL06c, LXH07, LCD07, Miy01, Mü01a, OKS06, PL01, RK06, Scr01, SOO02, SWH05, SGB00, SYLC05, SSNGS00, Tad02, TC01, Tsa01, TT01, WQWZ01, WZW05, WBD01, YWWS09, YG01a, YLH05, ZJ09, AEEr05, As04a, BCL05a, BCW05, BKN04, BBG, CL02b, CBB05, CC01a, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CHY05a, CHY05b, CL00, CHC04, CCHO4, CY05, CHC05, Che05a, Che07a, Che08a, Che08b, CCS08, CKN06, CJT01, Chi08b, Chi08c, Chi08d, DSGP06, DW01, FLZ02, FXAM04, FCZ05.

\textbf{scheme} [FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HW03, HWW04, Hsu05a, HWW05, Hsu05b, HLC07, HC04a, Hwa00, HYS03, HLL04, Hwa05, HLO5c, HLO5d, HLO5b, JW06, JSW05, KC09a, KLY03, KRY05, KSW06, KHL09, KCL03, Kuo4, KC05, KCC05, KHKL05, LHY02, LHL02, LHL03a, LKY04, LL04a, LL05a, LKY05a, LKY05d, LLO5b, LMC+03, LLO5h, LLCL08, LLH06, LHL03b, LH03, LCO4a, LYG07, LCC05, LC04b, LC05a, LH05h, LCZ05b, LCOZ05c, LCOZ05a, LWK05b, MSP09, NC09, PW05, PBMB01, PCC03, PC05b, PS01a, Pe04, Sae02, Sco04, SM11, Sha03c, Sha05a, SC05a, Sha05c, Sha05d, SLH03, mSFL05, SC05b, SC05c, SC05c, SZZ05, TLH05, Ts08, TWL05, TYH04, VK08, VS08, WLT03, Wan04b, WL05, WK05, WJP07, WDLN09, WHH05, WC01b, WHO2a, WHL03, WHO3, WC03b, WL04b, WC05, XWLO8, XC05, YW04b, YTH04, YW04a, YCH04, YWL05, YCO9b, hY08, YRY04, YRY05a, YRY05a. \textbf{scheme} [YRY05d, YY05b, YbJ04, ZC04, ZX04, ZC05, ZK05, ZW05a, ZAX05, ZC09, ZL05, dRMS05]. \textbf{Schemes} [AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CPD06, CKN00, Cor02, CJNP02, Cou04, CS00, CS03b, CDG+05, CL02, DN00a, DN02b, Des00b, DS06, DN00b, FF00, HSZI00, HW05, HM02b, HLL05, Kin02, Kos01a, KS03, KOMM01, LZL+01, LP01, MV00, NIS03b, Nam02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SBZ02, SPMLS02, Sun00a, VMSV05, WC09, XS03, YWC08, YY0101, Yek07, YYZ01, ZTP05, ZY01, Abd01, AFGH06, BCD06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DF04, Des00a, GGK03, HCD08a, HCD08b, HU04, HWW03c, HW04, HW05, HCO4b, HL04, IY06, JPL04, JXW05, KJY05, Kir01b, KT06, Kren05, Kühr08, LWH05, LWK05a, LW05c, MF07, Mü01b, NK06, PS02a, PKH05, Ph06, QC05b, QC05b, SNI00, Sha03d, Sha05b.

\textbf{Schemes} [SCL05, SC02c, SHT05, Ts05, Wu01, XY04, YWC05, YCW+08, ZF05, ZCL05, vDKST06].

\textbf{Schloss} [IEE01b]. \textbf{Schneider} [Puc03].

\textbf{Schneier} [Ano01e, Hei03, See04, Sty04].

\textbf{Schnorr} [BP02]. \textbf{School} [Coc02a]. \textbf{Schools} [PM00]. \textbf{Science} [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Im03, McE04, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04, Pot05, Sin05].

\textbf{Scientific} [CHT02, MH09, Lau08b]. \textbf{Scientists} [Coc01a, MH09]. \textbf{SCN} [BC05c, CGP03]. \textbf{Scots} [Ree01, Ros00b, Sin99]. \textbf{Scream} [HCJ02].

\textbf{Scribner} [Gas01]. \textbf{Scripts} [Uro01, Oue05, Rob02, Rob09]. \textbf{scroll} [GB09, HHYW07]. \textbf{SD} [ECM00a]. \textbf{SDK} [An002d, Bar00c]. \textbf{SDL} [HL06]. \textbf{SEA} [SPQQ06]. \textbf{SEAL} [Flu02b]. \textbf{Seamless} [OKE02]. \textbf{Search} [BI05a, Des00c, Eva09, FIPR05, KB07, LM02, MFD04, TIGD01, WYY05a, WYY05d, Z06, FM08].

\textbf{Searchable} [ABC+05, AFI06]. \textbf{Searches} [PGT07]. \textbf{Searching} [...].
Seattle [ACM06, S*03, USE00a]. sec [KV01].

Second [ACM03c, Bra01b, BD08, CZ05, GW01, HTS02, JYZ04, KCR04, Ki05, KP01, NM09, RD01, ACM00, Irw03, Rie03, Son00, Spr03].

Second-Order [NM09]. Second-Price [Bra01b]. Second [Top02]. Secrecy [Bla02a, GH02, Imr03, Lau05, Ree01, RW03a, Sin01b, BDNN02, BLP06, BD04a, Mol05, Ros00b, Sin99, Sin00, SY06, ZYW07].

Secret [ACS02, Alv00, Ano03e, BBDK00, BTW05, BI05b, BWT08, BP06, BM01b, CGHG06, CGH00a, CH01a, CLT07, Cha04, CTY09, CC06, CS05b, CK01, CDM00, CDF01, CF02, CFS05, CDG+05, CDI05, Di 01, DKL00b, D506, DNN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah67b, Kah96, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, McE04, MN01, NABG03, NN06, OKS06, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sun00a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, AJ08, AEEEdR05, Ano02c, Ano08c, Bam02, BCB, Cal01, C05a, CH05a, CH05b, CJL06, CNK04, CDD00, DD04, DB04, DM00a, Di 03, DW01, Duj08, FNRC05, FWT05, FZ06, Gal02, GIKR01].

secret [HT04, HJ07, HS00, IY06, Kee05, KB09, Lam07, Lun09, MF07, M909, Na05, PS02a, PW05, Ris06, Sch01e, SBZ04, SC05a, Smi01b, SC02c, Wau05, Win00, YCH04, ZSV05, dRMS05, vDKST06, Hii06].

Secret-Ballot [Cha04]. secret-code [DW01]. Secret-Key [HR05, RW03a].

Secret-Sharing [BI05b, CDM00, CDI05, DKL00b]. Secretly [CC08]. Secrets [BH06, BBD+02, CMS09, CP07, Che00b, Cop04b, Di 01, Gu01b, Gum04, Kid07, KMS01, LKM+05, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM+01, VGM04, AGKS07, Ano03c, Ano08b, Ban02, Bau00, Bau02a, Bau07, Cop05, Cop06, Cop10, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DM005, Eva09]. Section [Ano4b, An07a, BK06b, SGK08, TL02, KP03]. Sector [Cro01, MV01]. Secur [McK04]. Secure [AR00, AO00, AF04b, AG01, AP09, Ano01o, ACJT00, AF06, BCCH11, BDF+01a, BST03, BCL+05b, Bar03, BI05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CHK03, CHK05, CGP08, CW07, CQS01, CHJ+01a, CHJ+01b, CDM00, CD01a, CS02, CS03b, CDG+05, CDI05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, FP01, FOPS01, GPC08, GIKR02, GJ06, Gen04a, GD05, HZS00, HZS01, HSH01, HSH02, HSH06, HRS02, Har07b, HKW06, HV02a, Hv0AL09, HR04b, HL07, HLT09, Hul01, HLC08, IR01, Ito00, IFH01, JJ00a, JL00, JMV02, KMM+06, KY01a, KO04, KLML05, K02, KH05, KKL09, K101b, Kos01a, Kos01b, Kra01, Kra05, KSR02, LC01, LLL02, LCK03, LWK00, Lin01c, Lin03, Lin02, LL02, MKP09, Mar02a, Mar07, MV01, M0l03a, MJ01, NM005, Nam02].

Secure [Nd05, NSNK05, NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RVS09, Ro01a, So05, SVDF07, SBG05, Smi02, SKR01, SN04, SBEW01, Sty04, Tad02, VMS05, Vau05b, VMC02, VM03, WLLL09, WBL01, WGL00, WHL05, XS03, YWWL05, ZYM05, Zho06, Aan03, Abd01, AEEEdR05, AL07, AFGH06, BDS+09a, BDFP05, BCP07, CLOS02, CCMT09, C04b, CCK04b, CRSP09, CHH+09, CDDL, CCG05, DG06, Dwi04, FMY02, Geb04, GIKR01, GCKL08, HSW09, H03, HL06, HJW05, HBC+08, Ino05, ISTE08, IKOS07, IV06, KO09, KG00, LLL04, LLH04, LHC08, LH03, LC04a, LCZ05b, MT09, ML05, M0101b, OS00,
PCSM07, PBMB01, PQ06, PLSvLE10, PSP+08, RH03, RG09, RGX06, Sea09, SBG07, SGMV09, TKP+08, TCR03, Tse07, Ver01, VK08, WLH06, YGA01, YGZ05, YTWW05, hY08, YRY04, ZBP05, ZCL05, ZCW04, vOWK07, Ano03b, Ano08d]

Secure
[Ano12, BS01a, BS05, CHKO08, FIP02b]

Secured
[BNPW03, Ito01, UP05]

Securely
[HL05a, LLK05]

Securing
[Abe01, Cal00a, CHKO08, FIP02b, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPV06]

Security
[AW05, AW08, Ahm07, AJ08, ADR02, Amb07, Amb08b, Ano02b, Ano03b, Ano06c, AHKM02, Ay06, BP07, BW07, Ban02, BPS00, BBN00, BKR00, BP02, BNP02, BY03, BPR05, BOHL+05, BBB+02, Bis03b, Bla02a, BF06b, BDTW01, BCHK07, Boy01, BGM09, BLMS00, CM05a, CK07, CK02a, CKN03, Can06a, CGGH01, Cer04b, CC02b, CSW+08, Che05c, CM05a, CH07a, CSY09, Chu03, Coc01a, CK06, Cor06b, Cor02, CGP+02, CG05, Dr00c, Dal01, DN02a, DKMR05, Del07, DJ06, Des00c, Dim07, DR02d, DSS01, DK05, DS05b, DBS+06, Elb09, ELvS01, FIP01b, FBWC02, FW09, FLY06, For04, FML+03, FMV01, GSO2a, GSS03, Gum04, Gut02b, Gut04a, Gutxx, HM00, HS01, He07, HM02b, Hir09, HLL+01, HGNP+03, HQ05, HL05c, HL05d, ISO04, Ina02a, Ina02b, Int00, IK05, IH04, IKP+07, JY024, JP07, JP02b]

Security
[JSW05, JG07, Jol01, JBR05, JK02b, JK02c, JM02, JQY01, Kan01, KM02, KSHY01, KL05, Ken02a, KB06, KM03, KDO01, KM05, Koc02, KHL09, Kos01a, Kvo01, KXXD0, Lad06, Lai03, Lan00a, Lan04b, LGS01, Lee04b, LKH+08, LKLH09, LKh06, Len01, LNS02, LL04d, LSH03a, LSH03b, Lin02, LXM+05, LWK05b, LP01, MJF07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Müö10a, NIS01b, NDJB01, NNAM10, NP07, Oka00, OP01a, Ort00, PV06b, PSC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PTP07, PP07, Ph01, Pie05, Plö01, Po02, PHM03, Pool03, PF03, PS05, Puc03, Puc06, QCB05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sal03a, SJT09, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch01f, See04, Sch05d, SLH03, SLG+05, SL05a, Sph02]

Security
[Sko03, SEF+06, SEK01, SEK02, SK06, Sta03, SB07, Ste05b, SBZ02, Sty04, SK01, Sm05, Swi05, Tan07b, TG07, TG04, TPPM07, Uni00a, USE00d, USE01c, USE02b, Uni00c, Uni00d, Uni00g, Uzu04, Vau02, VMC02, WLT05a, WBL01, WWL+02, WA07, YEP+06, YWD08, Zan01, ZWC02, ZDW06, Zhe02b, ZHY03, ZS05, dLB07, AA04b, Ano05c, Aj01a, Aj01b, BPS08, Bai08, Baut05, Bej06, BeI07, BR04, BGP09, BFGT08, BF08, Bjo05, Ble07, BJ02, BM05, BG07a, Br06, BM06, Can01a, C+02, Cha07, Chat05b, CL+09, Che00b, Che05b, CKRT08, Chi08b, Chi08c, Chi08d, CJL06, CJM00, Con09, Con04, CC05e, DP04, DKK07, DY01, DFGH04, Des00a, DWML05, DKU05, DMS07, Eg00, FXAM04, FR08, FOP06, GH08, GJL06, GJ05, Gha07, GJ03, Gor05, GKS05, GMW01, GC05, Gut04c]

security
[HN04, HCD08a, HCD08b, Har05a, Hei03, Hen01, Hes04a, HM05, HSL+02, HL06, HG05b, Ino05, JEQ04, Jan00, Kad07, KY00, KPS02, Kim02, KVD07, Kov03, KH03, Kwo03a, LLM07, LC03, LL03, LL04, LL05b, LPW06, LMIC+03, LMW05, LLLZ06a, LLLZ06b, LH08, M03, Mal06, Man08, Man05, Man04, May01, MKK00, MK03, McG06, Men03, MS02d, MK05a, MPPM09, OP01b, Pae03, PSM+09, PC05a, Pat02a, PY05, PP06a, Pau03, PHS03, Pip03, Po00, PS04c, Rie00, RC05, Ros06b, RN00a, RN00b, SN00, Sal05d, Sch03, Sch02, Sch04d, Sen03, SHL07, Shu06, SH06, SH06, Son00, SH00, Sta02a, Sta06, Ste02, Sun00b, SHT05, SLL+00, Tsa05, Uni00f, Vac06, Van03, Voi05, VS08]
security
[vT05, AG09, Auo02c, BC05c, BP01b, Chr00, Chr01, CCMR02, CCMR05, CGP03, JRB+06, Lin02, RR04, Uni00h, ZL04c, Pap05].

Security-related [vT05, AG09, Ano02e, BC05c, BP01b, Chr00, Chr01, CCMR02, CCMR05, CGP03, JRB+06, Lin02, RR04, Uni00h, ZL04c, Pap05].

Security-sensitive [SPHH06].

Seed [TP07, KKJ+07].

Seeing [Wal03].

Seek [Coc01a, PH03, Shp05].

Seeking [Mos06].

Seeks [CAC06].

Seems [Coc02a].

Segmenting [HN07].

Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, VY01, Ytr06, AMW07, Bir07, BC05c, CZ05, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06].

Selecting [Bur03, dB07].

Selection [IBM00, JKK+01, RS00, SM08].

Selective [CS07c, LS01a, LM02].

Selective-ID [CS07e].

Selectively [Chi08e].

Self [GMM08, HW05, KY01d, LXH07, PS01b, PBC05, Scho06b, WHLH05, WLT05b, ZKL01, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, HL04, Lee04a, LL06, LS05b, LWK05a, PC05b, SH11, Sha04b, Sha05b, TLH05, Tsao05, TJC03, WH03, Wy05].

Self-Adaptive [SH11].

Self-Certified [LXH07, HW05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HL04, LL06, LWK05a, Sha04b, Sha05b, TLH05, Tsao05, TJC03, WH03].

Self-Defense [Wy05].

Self-Enforcing [Wy05].

Self-Escrowed [PS01b].

Self-Localization [WT05b].

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 [SY01b].

Semiconductor [Coc02b, IgI02, UHA+09].

Seminal [Cop04b].

SemiPublic [YC07].

Sender [CBM+05, Her09b, TJo1a].

Sensation [Top02].

Sensible [Sch04c].

Sensibly [See04, Hei03, Sch03].

Sensitive [HT06, Bro05b, SPHH06].

Sensitivity [SDMN06, GSK09].

Sensor [AEAQ05, CS08b, DBS+06, Fin06, GPČS08, LNL+08, NABG03, NNAM10, PZDH09, ZYN08, AJJS08, CMT09, HMvdLM07, JRR09, KXTZ09, KHYM08, LDMH06, LPV+09, LNO04, MWS08, MS09b, NC09, NDL08, PS08a, RAL07, TP07, WDLN09, ZJSN07, AMBO06].

Sentry [Kum07].

Seoul [CKL05, CR04, Kim02, LL03, LL04d, May09, PC05a, PK03, Son00, Won01, WK06].

Separable [CD00a].

Separating [MKKW00, Nie02b].

Separation [BYJK08, GKK+09, Ke000, Lys02, Mur00, ZGLX05, BYJK04].

Separations [GKK+07].

September [AUW01, AAC+01, AJ01a, BCKK05, BC05c, CS09, CGP03, DV05, DU05, DFCW00, EBC+00, ELvS01, FLA+03, GKS05, QSO0, RS05, SM07b, WP03, dCdVSG05, AJ08].

September19 [AJ01b].

September19-21 [AJ01b].

Sequence [HWH01, MS02e, WHLH05, ACTZ05, GB09, SL09, WG02, YZEE09].

Sequences [ADD09, BI09, XYXYX11, FG01, HG05a, JZCW05].

Sequential [GSS08, SNWO0, RMH03a, WH02b].

Serial [CTL01, KWP06, Uni00g, Mit00].

Server [BDK02b, ABK00, IK00, IK01, KKS00a, KKS01, KKS00b, OSv00, Pat01].

Server [ANRS01, BMK00, Dew08, KO00, LW00, NS01b, PS05, TMM05, XS03, Zha00, BB05, LHL04b, LHL04a, LKY05b, LHL03b, NTW07, Tsao08, Tsao10, TWL05, YSO4].

Server-Aided [NS01b].

Server-Assisted [XS03].

serverless [BDET00].

Servers
[BIM00, HS07, Jab01, KCD07, Mar02a, TEM+01, LS05b, PT08]. **Service** [BACS02, BH00a, CLK01a, DeL07, KZ01, Lan04a, LDM04, Nik02a, Nik02b, PKBD01, CUS08, HILM02, KWD06, LB05, Mir05, MV03b, SRJ01, SSM+08, Ug08, Coc02b, Hil06].

**Services** [ANS05, BCS02, DJLT01, ECM00a, ECM00b, Kn07, Tsa01, Uni00b, WL07b, BDS+09a, BFG04, BFG05, BFG08, CCCY01, HM05, JRB+06, MW06, MPPM09, MV03b, RR04, SBG07, SL05b, TWL05, WA06, BH00b].

**Session** [GL01, OHB08a, CS04, OHB08b, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00n, YWL05].

**Session-Aware** [OHB08a, OHB08b].

**Session-Key** [GL01].

**Sessions** [KPR03].

**Set** [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDET00, Che07a, CC05d, DM00a, El05b, Mar05b, Sta00].

**Setback** [MYC01].

**Sets** [CFS05, EIG01].

**Setting** [BBM00, DLY08, LP01, PGT07, GMLS02].

**settings** [Lee01].

**setup** [PS04c].

**Seven** [Luc00].

**seventh** [AAC+01].

**Several** [KS00a, LD04, Tsa05, ZT03].

**SFLASH** [GM02b, SGB01].

**SGI** [Bar00c].

**SGID** [Tot00].

**SHA** [AD07, BC04a, GLG+02, HKR01, MP06, SK05a, TYYL02, WYY05d, WYY05b, WYY05c].

**SHA-0** [BC04a, WYY05d].

**SHA-1** [GLG+02, HKR01, MP06, WYY05b, WYY05c].

**SHA-2** [SK05a].

**SHA-256** [TYYL02].

**SHA-512** [AD07, GLG+02].

**SHACAL** [KML+02].

**Shacham** [Hes04a].

**Shamir** [BB79, SP79, Coc03, PW05, VS08].

**Shamir’s** [LD04].

**Shape** [Gan01b, Gil07].

**Shapes** [OMT02].

**SHARC** [DMSW09].

**Share** [CT08a, CD05, FS04, AEE05].

**Shared** [ACS02, BH06, BBK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04].

**Shares** [TT01].

**Sharing** [BTW05, BI05b, BTW08, BGHP02, CD00a, CLT07, CC08, CTY09, CDM00, CF02, CFS05, CDG+05, CDI05, Di 01, Di 03, DS06, DP07, FM02a, FSW01, FMY01, HNZI02, Kin02, Kog02, KS03, LD04, MN01, NN00, OHS06, PZ01, PZ02b, PZ02a, SZ01, Sun00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CDD00, DD04, DM07a, DKL00b, FWTC05, GIKR01, HT04, HKS00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDKST06].

**Shepherd** [Gu05].

**Sheets** [MNS01].

**shc** [Gua05].

**Sheets** [MNS01].

**Shell** [Dwi04, Gua05, BS01a, BSB05].

**Sheltering** [MYC01].

**Shen** [KTC03].

**Shieh** [McK04, CZ03, YWC05].

**Shift** [CGFSHG09, Che08a].

**shifting** [Cal00e].

**shifts** [Neu06].

**Shines** [Coc02b].

**Shinko** [Ano00d].

**Ships** [Ano02e].

**Short** [Ano01o, AFI06, BBS04, BGW05, DN00b, Gra02b, LS01b, PM02, RR02, RW02, Vau05b, GL05, WDLN09, Coc02b, Sch01e].

**short-term** [WDLN09].

**Shortcuts** [Sha03a].

**Shortened** [Kur01].

**shortest** [Pei09].

**ShortPK** [WDLN09].

**Shoup** [Luc02b, VMSV05].

**show** [GP00, Smi03].

**Shows** [Gen01, AJ08].

**Shrinking** [Gol01c, WHLH05, ZKL01].

**SHS** [Ano08d, Ano12].

**Shuffle** [FS01c, NSNK05, Sas07].

**Shuffles** [Mir02].

**Shuffling** [PBD05].

**shut** [Gil07].

**SiBIR** [IR02].

**sic** [IEEE09a].

**sichere** [Lin02].

**Side** [Ano01].

**Side-Channel** [BU02, Law09a, MÖ02, MÖ02, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP+08, WLY07].

**Shuffle** [FS01c, NSNK05, Sas07].

**Shuffles** [Mir02].

**Shuffling** [PBD05].

**shut** [Gil07].

**SiBIR** [IR02].

**sic** [IEEE09a].

**sichere** [Lin02].

**Side** [Ano01], BU02, KSW00, Law09a, LL01, MÖ02, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP+08, WLY07].

**Side-Channel** [BU02, Law09a, MÖ02, CNPQ03, PSP+08].

**Shading** [WC04].

**Siena** [BCKK05].

**sieve** [CM05b, JL03].

**SIGABA** [Lee03c].

**SIGACT** [ACM03c, ACM05b, Raj06].

**SIGART** [ACM03c, ACM05b].

**Sight** [Col03].

**SIGMA** [Kra03].

**SIGMOD** [ACM03a, ACM03c, ACM05b, ACM04a].
Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09].

SINOBIOMETRICS [LLT+04, Li05]. SIP [NTW07, PM00, SZ08]. Sir [Bud06]. Site [AEV+07, Coc02a]. Sites [Che01d, Ros07]. situation [AJ08]. Six [Bel07a]. Sixth [Uni00a, Uni00b, Uni00e, Uni00h, TLC06]. Size [CS07c, CMJP03, HNZI02, Kal03]. Sizes [Ano09d]. Skein [AEMR09]. Sketching [MNS08, SLTB+06]. Skipjack [Gra02a, HSL+02, SLL+00]. Skipjack-like [HSL+02, SLL+00]. SKLOIS [FLY06]. Sky [MYC01]. SLAG [CGBS01]. SLAAC-1V [CGBS01]. Slide [Fur02b]. Small [CCM05, ELvS01, GPS06, MNT+00, May02, OT03b, RK06, SM02, Sch01c, SPGQ06, Wal03, YLC+09, Duj08, dW02]. Small-Project [MNT+00]. Smaller [Bar00c]. 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, Q500, Q501, RE00, RE03, RS01, Suk01, SR01, Sha01c, SP02, TBLD01, VPG01, YKMY01, Ano00k, Ano01l, Ano04f, AJ01a, Bor00, BPR01, BHCJ05, BGL+03, Bur00, Cal00c, CCCY01, Cha05a, Clao0b, Con00, CH00, DMT07, DFH01, DFPST07, FCZ05, Fin03, GMG00, GUQ01, HHSS01, Hsu05b, Hus01, Jna04, KLY03, KLY05a, Ler02, LC05a, Lu07, MY01, Pha06, PB01, Pre07, SVD07, SLH03, Sm00, TIS07, VK08, WC03b, YW04b, YWWD08, Za0f, BvJdV02, CL04d, CCK04b, Che00a, DFPS06, FGL02, Gro03d, HLO5b, Ku04, KC05, LHY02, Pau02b, SKKS00, Sco04, SCF01, TV03, YW04a].

smart-card [GMG00]. Smartcard [HWH01, KRV01, RMCG01, URI01, PBVB01, BBVPV00, CGMM02, DM07b, HRS02, Ito01, KS02]. Smartcard-Based [RMCG01, CGMM02]. Smartcards [CMG+01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, Ano04c, RM02]. smarter [Car01, Cla00b]. Smartly [MS01]. Smooth [PS02b, XYXYX11, GMR05]. SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. sneak [Ade09]. Sniff [Ano02e]. Snort [UC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sa02, Sha03c]. Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Ahn07, And07, Ano02c, Bar00b, BC04b, Coo10a, CS05a, DR02c, DF01, GH05, HC02, HMM01, Hoe01, Jha03, Knu07, KSZ02, LAD06, Law09a, LS01, LLLZ06a, LSV09, LT+00, MNT+00, MSHN07, MKY08, Mc06, ND05, PM00, PS01c, Sch01a, Sch00b, Ste00, USE00b, VH09, VVS01, WHLM05, Wh04, ZCC01, AJ08, Ano00h, Ano00j, Bir07, Che01e, CT02, CCD+04, COTT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, KA09, Mat02, MCA08, MCR05, Pau03, Sch01d, S03, WL07a, WA06, Sal03b, Ano03b, Bo02]. Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [Hoe01]. Software-Oriented [ZCC01]. Software/Hardware [N05]. SOI [Ano02e, NFQ03]. SOISIC [Ano02e]. Solaris [Ano06c, BH00b]. Solomon [KY02b]. Solution [Cap01, CJT02, DHR00, LLS05b, Pol01, Str02, TvdKB+01, LSH00]. Solutions [Ano04c, MV01, Jan00, MSK03, MV03b, St00, Gum04]. Solve [CU01, GS03]. Solving [CJT04, GPP08, W101a, Bull09, Whi09]. Some [AG01, BDF+01a, D101, DFG01, GM02c, HSS04, JM02, KLY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HANR04, He02, JK01a, RSS04, SHT05, ZF05]. Someren [Ano03g]. Something [FL01b]. sometimes [FNRC05]. Sons [And04].
Sorry [San05]. sorts [Ano03g]. Soul [Bla01c]. Sound [BJP02, FR08]. Soundness [ABHS09, DPV04, MR01c, BPS08, Lau08a]. Source [Bar00c, Bo102, Gut00, HBF09, KLR09, PM00, RK06, TEM’01, Ano03d, BGL’03, CB09, McA08, RVS09, SB05, Bar00b, Lin02]. Sources [KZ07, WLZZ05, KZ03]. Southampton [Bla03]. Soviet [AJ08]. SP [BG07a, Hir09]. SP800 [SF07]. SP800-90 [SF07]. SPA. SPA-Based [Nov01]. Space [BGH07, Lu02, MSNH07, NS05a]. Space-Bounded [Lu02]. Space-Efficient [BGH07]. Spain [BS03, DFPS06]. Spam [CMB’05, DGN03, Vix02]. Spamming [Bel04]. SPARK [Jun09]. Sparse [BLST01, BG07b, GS03, Bo02, BF06a]. Spatial [MM01a, SG09, SDFH00, Lin00a, SL09, YPPK09]. Spatial-Domain [SDFH00]. Spatio [CDTT05]. Spatio-Temporal [CDTT05]. speakables [BZ02]. Speaker [LM00]. Speaks [VN04]. Spec [Bar00c]. Special [Ano04b, Ano07b, Ano07a, BK06b, GIS05, GS07a, GPP08, SGK08, KP03, FOP06]. Special-Purpose [Ano07b, Ano07a, GPP08, SGK08]. specialized [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00a, LKJL01, RSA00c, Mea04]. Specifications [IJE00b, BDFP05, BD04a]. 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]. Speed [Ano00d, Ano02d, Gro01, JKR01, KMM’06, Lut02, SOTD00, SM02, Wei00, YKMY01, BGL’03, RW07, RMCG01]. Speeding [Osv00, SWH’09, TC05]. Speedup [YLKM02b, YLKM03]. Speedy [Cre00]. spherical [LZP’04]. Spider [Tur04]. Spies [Gan01b, Win05c, Han06, NRR00]. SPIHT [Che08a]. SPIN [MS02a]. Spline [SPK08]. Splitting [GMW05, LKL05]. SPN [HLL’01, Kan01, PQ03b]. SPNs [CKL’03]. spot [Nat05]. Spread [BQR01]. Spring [Pap05]. Spring-Verlag [Pap05]. Springer [Fal07, Lee03a, Lee03b, Pho01]. Springs [Wil99]. spying [Cas03, FNRC05]. spymaster [Bud06]. spypware [Ste05c]. SQL [Dew08, HILM02]. Squadron [OC03]. Square [HCK09, HQ01]. Squaring [CH07b, NSS02]. SRAM [HBF09]. SSC2 [HQR01, ZCC01]. SSH [All03, BS01a, BSB05, BKN04, BLS04, H¨Ofer01, LA02, Naz02, Ou05, SWT07, Str02]. SSH-Connected [H601]. SSHFS [Hos06b]. SSL [ASK05, BPST02, CHV03, JRB’06, KCD07, KPR03, Kra01, LKL05, LWK00, Net04, OHB08b, OHB08a, SB01, SQ01, Vau02, ZFK04]. SSL/TLS [BPST02, CHV03, KPR03, OHB08b, OHB08a]. SST [Gau02]. St [GKS05, NH03, AS01a]. Stack [Pot03]. Stage [Kak06, CHY05b]. stamp [CL00]. stamping [HHC05]. Stamps [KZ01]. Stand [CAC03]. Standard [Ano08d, Ano09b, Ano12, Ano13, Bar00a, BCP02a, FIP00, FIP01a, FS01a, Herz09a, Hug04, HLC08, IE00b, MM01c, MP01a, Nat00, PM00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, Ano04e, BBK’03b, DR05, GMR08, Sea09, Tan01, AEH17, Ase02, Bar00c, III00, Bur03, CMR06, C02a, C02b, Cur05, DR01, DR02b, Dan01, FIP02b, G01a, Har00, Lan00a, Lan00b, Lan04a, Mor05, NIS00, SB00, Sta00, Sye00, WRBF00, Wri01, YW06]. Standardized [Man01]. Standards [Ano01g, Bur06, CL07, C02b, Hus01, RSA00a, Tsa06]. Standing [Lan00b]. Star [Pot05]. State
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, LLI+01, MV03a, Neu04, Pro01, RSN+01, BKW03, GSK09, Hey03].
Statistically [Fis01b, HR07, HNO+09].
Statistically-hiding [HR07].
Statistically-Secret [Fis01b].
Statistics [CKN01, CNK04, KLML05].
Status [Pre01, Sha03b].
STDM [WMDR08].
Stealing [Gan01b].
Steering [HR13].
Stefan [AUW01].
Steganalysis [Pro01, Sal05b, GSK09, WW04].
Steganografie [Sch09].
Steganographic [CTL04, HR02, LJM07, RH02, RS00, Wes01, KC09a, LYC02, WWTH08, YCL07].
Steganography [BC05a, BGI08, CVH01, ChYL09, CDR01, CW09, CTH08, Col03, CMB+08, CS05c, DIRR05, DRL09, FGD01, Fr07, Gal03, HCBLETRG06, HLvA02, HvAL09, Hun05, HSKC01, LS08, PH03, Sal05b, Sha09, Sha01e, Shi08, SWR05, Wan05, WW06, CDS07, CO09a, Che07a, Che08a, GGS+09, JDJ01, KP00, LT04, WW04, WMS08, Way02b, Way09, YCYW07], stego [KC09a].
Stego-image [KC09a].
Steiner [WL02].
Step [DRL09, KKKL09, An004e, MP07, SL06].
step-by-step [SL06].
Stepping [WRW02].
step [Bih02].
Stereotypes [GO03].
Stem [CGP08, CS05b].
stickers [GPX08].
Sticks [Sam01].
still [An000f, Riv00].
Stinson [Spr03].
STL [Zo01].
STOC [ACM05c, ACM07, ACM08, ACM09].
Stochastic [MG01].
Stock [Bar00a].
Stone [MLM03].
Stones [WRW02].
Stop [SSNS00, Win05c].
Storage [DFSS08, Din01, Din05, HR02, Har07b, Hug04, MSTS04, RCBL00, Ric07, RH02, Vad03, AFGH06, DFS05, HGR07, LPM05, SGMV09].
Store [CTBA+01].
Storing [ST06].
Story [Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, HS01a, Win00].
Strategic [AJ08].
Strategies [Cir01, KL05, SKQ01, Dw04].
Strategy [DR02a, TPPM07, KC09a].
Stream [BCC01, BC05b, BSW09, BS00b, BL02, CF01b, Can06b, CJS01, CHJ02, CM03, Cou03, CL02c, DF07, Fil00, FF01a, Gol01d, Gol01e, GBM02, JC02, HR00, HR04a, Jam00, KHD01, MSNH07, PP06a, SM01, Sar02, SXJ01, WB02, Wu02, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, BVP+04, DS09, DK08, KH08, Max06, MI09, MRT10, PCS03, PC030, SB05, WW08].
Stream-Cipher [SXY01, WW08].
Streaming [OS05, CB05b].
Streams [AIP01, CO09a, YLC+09, ZCW04].
Street [McE04].
Strength [CB01, JX05, Oni01, CKL+09].
Strengthening [Loi00, MHS+02].
String [CP0707, DFS04, Pas03, Dam00, RG05].
Strings [Vau05b].
Strong [ADD09, BB00b, CS00, DKF05, KJ+01, KW00, LSH03a, LSH03b, Lu02, Pau09, SBZ02, WHL05, An01m, CC04b, HRS08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04].
Strong-Password [LSH03a, LSH03b, WHL05, CC04b, KTC03, Ku04].
Stronger [LLM07].
Strongly [YI06].
Structural [BS01c, LBR00].
Structure [DNP07, EIG01, H601, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SSL+00, XMST07].
Structured [BRTM09, CKK03].
Structures [An02e, DS06, GTCC03, HCD002, KCP01, Kus02, MND+04, MFFT05, PSC+02, PQ03b, Sun00a, XH03, HN06a, YI06, SWR05].
struggle [Bur02].
Stuart [Gum04].
students [AA04b, PP09].
Studies
Study [BBGM08, Car02, DPR01, DP00, KJK+07, WCZ05, BKN04, BF06a, DY09a, KWDB06, SKW+07, ZWWL01]. Sturgeon [Wei07, Wei00, Wei06]. Stuttgart [Eag05]. style [BPS08, dH08]. Subcommittee [Uni00f, Uni00h]. Subdivision [LDD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro05, GMR05]. subliminal [LH04]. subsampling [LLC06b]. subscribe [SL05b]. Subscriber [CFRR02]. subscription [MW06]. subscription-based [MW06]. subsets [Sch01e]. substitute [Bih02]. Substitution [KKG03, GPX08, RBF08, WL04b]. Substitution-Permutation [KKG03]. structure [MRT10]. Subsystem [HL07, MBS04]. Subtleties [Lai08]. subverting [HB06]. Success [Ano06d]. successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Suitable [AIK+01, CQS01, KTT07, LKH09, SP05, Wen03]. Suite [RSN+01, SBEW01, YLT06]. Sunspots [CPS07]. Super [Lam07, CAT06, Hos06b]. supercluster [Pri00]. Supercomputer [Coc01a, Wal09]. Supersingular [Gal01, RS02, Ver01]. Supervision [FDIR00]. Supplemental [TBDD01]. Supplementary [ECM00a, ECM00b]. Supplies [Sha01c]. Support [ABM00, Gro03, LTM+00, PZDH09, SGB02, Ano04e, Ano05c, BMA00a, BMA00b, BMA00c, ED03, mSgFtL05, SSM+08, WNQ08, ZYL05]. Supporting [CLK01a, SW02]. Synchronized [GA05]. Sure [Tom06]. surface [Iwa08, LDD07]. Surfaces [SPK08]. surveillance [Che01f, LCS09]. Survey [EPP+07, FDIR00, KM04b, LDH06, MSI10, ATS04, Ano00e, BEM+07, CF05, CDL06, EY09, LOP04, Mea04, Mül01b, OZL08, PC09, Pre07, RH03, RAL07, Sch01f, ÜG08, ZLZ07]. Survivable [CLZ02]. Susan [Jan08a]. SVD [BBC+09, CYH+07, FWL08]. SVD-based [CYH+07, FWL08]. SVGrid [ZBP05]. Sweden [BS01b, Joh03]. Swedish [Bec02]. Swiss [Boy03, Kid00]. Switching [CT03]. Switzerland [CC04a, Vau05a]. Symbiosis [DF01]. symbol [SDF07]. Symbolic [Bo01, Jef08, Mar02b, May09, MT07, MP05, ALV02]. symbols [Lun09]. Symmetric [Ano01n, ABM00, BU02, BM07]. ČvTMH01, CCM01, Des00b, EP05, FW09, Fil02, RR00, Ust01b, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01]. Symmetric-Key [Ano01n, ABM00, CCM01, EP05, RR00, BMA00a, BMA00b, BMA00c]. 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]. synchronization [CMdV06]. Synchronization [GP08, SW02]. synchronize [Pau02b]. Synchronous [CH01b, Sar02]. synopses [YLC+09]. Syntax [BWBL02, RAS00b, RSA00d]. Synthesis [RFZ01, SOIG07, UEPE09]. syslogs [ME08b]. System [Ano02d, Ano02e, ANR01, BIP05, BCST00, Bih00, CCDP01, CHM+02, CSW+08, CGJ+02, D01, DGP07a, DGP07b, D08, EM03, FL01a, Ito01, J08, K02, KHY04, LV00, LSS05, LSL05b, LXM+05, MA00a, MA00b, Miy01, MFK+06, MFS+09, RH02, SR01, Sha02, SOO0I2, Ste05b, TK03, TZT09b, USE00a, WG05, WA07, YKMY01, YKLM02b, ZYM05, AHK03a, AMRP00, Ano00j, ADH+07, AAKD09, Bltu09].
BDET00, Bul09, CC02b, CCH05, CIL06, CPG +04, Coc01a, Cre00, CO09b, DZL01, DPT +02, DIM08, DPG09, FP00, GG08, GSK09, GMG00, Gou09, HN07, Joy03a, KWDB06, KX00, Kwo03a, LL04c, LKJL01, Lin00a, LK01, M KK00, RCG +04, Sal00b, SCS05a, SGMV09, SETB08, TKP +08, Wan04a, dB07. **Systematic** [DW05, ZL04a]. **Systemic** [KB06]. **Systems** [ACM03c, ACM05b, ANRS01, Ano02e, BCS02, BRTM09, CP02, ELvS01, Fel06, GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST +05, LLLZ06a, LJ05b, Lut03, Mar02b, MMYH02, NABG03, RS05, Rii02, SM01, Sas07, SJT09, SXY01, USE00c, USE00b, Vav03, VHP01, WK03, ARJ08, And08b, Ano01n, Bld03, Ble07, CUS08, CC05c, CCS08, CGL +08a, CGL +08b, CCL03, CCM01, CNPQ03, CHT02, CG05, CSK +08, DYO09a, EYO09, FMY02, FP00, HP00, HBC +08, Hut01, HY03, JPO06, KAM08, KP01, KN01, KP03, Kvo03, KRS03, KNS05, MBS04, MSP +08, NdM06, Nis03a, PBMB01, Par04, Pl06, RW07, Sha01a, SK03, TOEO00, WAP00, XQ07, ZSV05, Ano02d, Lut03]. **systems/ciphers** [SK03]. **Systolic** [KLY02, KKY02, MP01c].

**Table** [Ano03f, MFFT05, XFZ01, BZ03, CC05b, Has00, Tsa08]. **table-based** [Has00]. **Tables** [AJO08, KB09, RB08]. **tactics** [Cal00e]. **Tag** [KKJ +07, NNAM10]. **tagging** [BP05]. **Tags** [OS06, ACD05, PLSvdLE10]. **Taipei** [Lai03]. **Taiwan** [Lai03, Ano03a]. **Takagi** [LKL00]. **Takagi-cryptosystem** [LKL00]. **Takaragi** [WHHL03]. **take** [Heg09, Per05b]. **Taking** [CDS07, Lai07, PM00]. **Talbot** [Rot07]. **Talk** [FGM00a, Lan00d]. **Talking** [An01p]. **tamer** [Kap05]. **Taming** [Ada00, Lov01]. **Tamper** [LTM +00, CT02]. **tamper-proofing** [CT02]. **tampering** [PS05b]. **tandem** [DPT +02]. **Tang** [YRY05d]. **tank** [Pau03]. **tar** [Str02]. **targama** [MAaT05]. **target** [BD04b]. **Targets** [MV01, Pau03]. **Tarragona** [DFPS06]. **tasks** [XQ07]. **Tate** [Jou02, SKG09]. **TATSU** [TS00]. **tattling** [CSK +08]. **TC** [DKU05]. **TC-11** [DKU05]. **TC-6** [DKU05]. **TC11** [ELvS01]. **TC8** [DFCW00]. **TC8/WG8.8** [DFCW00]. **TCB** [SPHH06]. **TEA** [HR06, Kili05, Nao04]. **TCP** [CD01b, Os00, SBB05]. **TECH** [CV05, HSR +01, HSI02, HHI04, HHL +02, WN95]. **Teaching** [McA08, Shu06, GV09, Jan08b]. **Tech** [Kir01a, TvdKB +01, Uni00c, Gra01, Ros04, Uni00f]. **Technical** [BHM03, GS07b, Lan00c, Scr01, TL02, USE01b, USE01a, USE02c]. **Technique** [CC02a, Pau09, PQ03b, SC02a, WC03a, vW01, CL00, Che08b, Pau03, Ren09, WC05]. **Techniques** [AIP01, BSW09, Bih03, BBPV00, BDP02, CC04a, Cra05a, DBS +06, Dun06, Gal03, KLN +06, Ken02b, Knu02, KO03, MKP09, NCRX04, PJ01, P601, Pre00, Shi08, YKW01, AB09, BMW05, BR05, Che08a, DY01, DHMR07, DY09a, Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08]. **Technologie** [RSA09b]. **Technologies** [MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZWC02, ATS04, PB01, TTZ01]. **Technology** [CZK05, Cla00a, GS00, GSB +04, MP00, NFQ03, Pau06, TV03, AL07, Ble07, Car01, Cas02, Che00a, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b, Six05]. **Tektronix** [Ano02c]. **TelCorreos** [LM00]. **telegram** [Tuc66]. **Telelogic** [Ano02c]. **Telephone** [KZ01]. **telephones** [CF05]. **Telephony** [Ano02c, CFR02, PM00, GV09]. **teleportation** [BEZ00, BEZ01, Dutm03]. **Telling** [Gan01b]. **template** [LLT06a, UBE09]. **Temporal** [CDTT05, KXTZ09]. **Ten** [ES00a]. **Tenth** [USE01c]. **Term** [ABRW01, Dur01, BM06, DVP09, ISO05, LG04, SGMV09, WDLN09].
Terminal [ECM00a, ECM00b]. Terminals [Chi08a, ISTE08]. termination [BP05].

terms [LMTV05]. Ternary [AD09, DKL00b]. Terrorism [PP06b].

terrorists [Mad04, Win05c]. TESLA [LN04]. Test [BT02, HSS04, Lan00b, LN08, RSN01, Way02a, DS00, GMG00, Kat05a, KKKP05, RSS05]. testable [RMPJ08]. Testing [III00, CGBS01, Fil02, Lan00b, LN08, RSN+01, Way02a, DS00, GMG00, Kat05a, KKKP05, RSS05].

text [Lut02, PJH01, PM08]. textbook [BJN00, PP09]. Thank [CMB05]. Theft [CMS09, Ano01l, Phi06]. Their [AGT01, CD00a, Gen04a, JKRW01, LLL01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, Sti01, TO01, WY02].

them [WD01a, Tee06]. Theorem [AC02, Eke02, GN01, Scho0a, YKL03]. theorems [MW04, Nyb01]. Theoretic [CB01, DHR00, Fil02, Lut02, Lut03, SB00, WA06, Lut03].

Tests [MT02, NM09, GT02, Gut04c, JPL04]. Testing [III00, CGBS01, Fil02, Lut03, SB00, WA06, Lut03]. Text [MT02, NM09, GT02, Gut04c, JPL04].

Textbook [BJN00, PP09]. Thank [CMB05]. Theft [CD00a, Gen04a, JKRW01, LLL01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, Sti01, TO01, WY02].

There [Bar00b, GW00, Neu06]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Hei03, Sch03, Sma06].

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].

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

There [Bar00b, GW00, Neu06]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Hei03, Sch03, Sma06].

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].

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

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

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

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

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

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

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

Thirty-Fifth [ACM03b]. Thirty-Eighth [ACM06]. Thiry [ACM02].
Time-Memory-Data [DK08].

Time-Reversed [lna02b]. time-space [NS05a]. time-stamping [HHC05].

Time/Memory/Data [BS00b]. Timed [BN00b, CHK008, JP07, LKJL01, Mao01, HGNS03, Zha06]. Timed-Release [CHK008, Mao01, HGNS03].

times [NS05a].

Timestamp [HHC05].

Timed-Release [CHK008, Mao01, HGNS03].

Timing-Attack [KS09a]. Tiny [Bar00b, Min03, WN95, And03]. Tipsy [TvdKB01]. Tissue [MYC01].

Title [ZYH03]. TLS [BPST02, CHVV03, HSD05, JK02b, JK02c, Mao01, HGNS03].

TLS-Off [AJ08, CCK04b, Mol05].

Timestamp-Based [CC01b, FLZ02, SLH03, LIT03, YW04a].

Timestamping [MSTS04].

Timing [CKQ03, CWR09, Law09b, Sch01b, SWT07, ASK05, DKL00a, KSL00, OS00].

timing-attack [KS09a]. Tossing [Lin01c].

totality [HRS08]. Tough [Pau02a, JP06]. toughest [Min03], tour [Pet08].

Tour [KJR05]. Trace [Bor01, LNS02, NN03]. trace-and-revoke [NN03].

Traceability [HLL03, HW05, WLHH05, WY05].

Traceable [LZL01, CCH04]. traceback [CS04]. Trading [KY01d, KY01e, LLL02, NN01, SN00, TT01, WRW02, WLZZ05, WH01].

tracings [RE02]. Track [Fox00, Joy03b, Nac01, Oka04, Poi06, PHM03, Pre02c, USE01b, USE02c, Men05, CAC03, CAC06].

Tracking [WCJ05, FNC05, S08, TW09]. Trade [AJ008, CMS09, Oec03, PS01c, Uni00f].

Trade-Off [AJ008, Oec03]. Trade-Offs [PS01c]. Tradeoff [LP02a, QR02, CW02, Ina05, NS05a, DK08].

Tradeoffs [BS00b, CTLL01, SRQ03, SU07]. Trading [PV06b, SW09]. Traffic [FGL02, MiS08, Fe09]. Trail [DR02a]. train [Pri00].

Training [Coc02a, CAC06].

Traitor [KY01d, KY01e, LLL02, NN01, TT01, WH01]. Transacted [HBl01].

Transaction [RH02, AAKD09]. Transaction-Based [RH02]. transactional [ST06]. transactions [Cal00b, Cal00a].

Transcript [An01a, An01b, An01c, An01j, An01n, An01f, An01o, Mal02, Nik02b].

Transfer [CT08b, Din01, GKM00, KKL09].

Transferability [HSZI00]. Transfers [IKNP03].

Transform [ABM08, BCB09, BR09, CPh04, KC09b, LKL05, Nak01, SFC09, VK07, BR06, Che07a, OP01b, SR00, LPZ06].

Transformation [CT09, HLL05, DSP01]. Transformations [Fe06, KYHC01, LMT05, Pa03]. transforms [La00].pare

Transitive
[BN02]. Translation [GGS+09, PY06]. Translation-based [GGS+09]. TransLink [Cal00c]. Transmeta [GP00].

Transmission

[MLC01, SNR04, SVD07, Smi03].

Transparent

[CCDP01, Por01, Lin00a].

transport

[Bor00]. Trapdoor

[BPR+08, Fis01b, KO03, KO00, Gen04a, JW05, PW08]. Trapoors [GPV08].

trapping

[Min03] Travel [Bor00].

Traversal

[JLMS03].

Trawling

[Knu00a, Knu00b].

treatise

[Bla00, MAaT03, MAaT04, MAaT07].

treatises

[MAaT06, MAaT07].

Treatment

[CL05, DK08].

Tree

[CC05d, GST04, JLMS03, KPT04, LKLK05, LM02, TMM00, Mon03, PCC03, WL02].

Tree-Based

[GST04, KPT04].

trees

[Che02, Che07a, TC00].

trek

[Pot05].

Trends

[Ahm08, KB07, Ord00, Ndm06, PRS04].

Tricks

[Mit02b, All03].

triggered

[HHJS04].

triptartite

[SW05a].

Triples

[FS01b].

Tripwire

[TvdKB+01].

trivial

[KO00].

troubleshooting

[HJW05].

True

[BST03, Cha04, DV08, EHK+03, HBF09, Pan07, SFD06, BG08, BG09, GB09, Han06, HLW05, Ste05c, vT01, VOS09].

Truecrypt

[CSK+08].

truly

[BGL+03].

Truncated

[CS05b, KM02, LHL+02, SKU+00, SKI01, GSN09].

Trust

[CHSS02, HCD02, Lin00b, LHL+08, Mit02a, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, LMV05, LLW09].

Trusted

[DK01, WHI01, WVI01, ARJ08, Gue09, PS04c, ZYL05].

Trusting

[CS05b, KM02, LHL+02, SKU+00, SKI01, GSN09].

trustworthy

[CCH05, SK03].

Truth

[MNT+00].

Tseng

[Hwa05, XY04, ZAX05].

TTM

[GC00b].

Tuesday

[Uni00a, Uni00f, Uni00e].

tunable

[LB05].

Tunny

[Sal01a].

Turin

[AL06].

Turing

[Bar00b, RSA03a, Adl03, Cec03, Cop04b, Goo00, Pet08, Riv03, Sha03b].

Turkey

[Bor00].

Turkish

[DD02].

Turn

[Tsa07].

Turning

[DLT01].

tutorial

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

Tuxedo

[McE04].

TV

[Smi03].

Tweakable

[DS08, HR03, LRW02].

Twentieth

[Gan01b].

Twenty

[ACM03c, ACM05b, AAC+01, B+02, LAM06a].

Twenty-Eighth

[B+02].

Twenty-first

[ACM03c].

Twenty-seventh

[ACM03c].

Twin

[Ran01].

TWIRL

[Kal03, ST03b].

Two

[Ahm08, BDG+01, DIS02, FD01, Hen06b, HSIR02, HSS01, Hu05, HLT01, HLT05, JZCW05, KCP01, KO04, KTC03, KI03, Lin01c, MR01a, MLM03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, St.00, Ste05a, Ste01, TW07, WW05, XS03, YWW08, YYY001, CLO02, DHL06, GCKL08, HW03c, JW01, LMTV05, MS09c, MCN03, MCHN05, Pau01, Pha06, ZLX99, bD07].

Two-Block

[KCP01].

two-channel

[MS09c].

Two-factor

[Hen06b, Sch05c, St.00, Ste05a, YWW08, dB07].

Two-Key

[KI03].

two-level

[DLH06].

Two-Party

[KO04, Lin01c, MR01a, WW05, CLO02, GCKL08, JW01, ZLX99].

Two-Pass

[SK00].

Two-tier

[TW07].

Two-Way

[DIS02].

TWOBLOCK

[Van05].

Twofish

[BF00b, FKW00, IK00, Kel00, Knu00a, Knu00b, Luc02a, Mur00, SKW+00].

Tycoon

[McE04].

Type

[CKQ03, Dug04, H¨of01, KIYHC01, PDMS09, RMS05, Vir03, GSSP08, PQ06, Sh01d].

Type-based

[Dug04].

Type-Passing

[Vir03].

typed

[BG07b, FR08].

Types

[Cor02a, GJ04, RSA00e, BFM07, LAM06a].

Typical

[BSC01a].

typing

[GJ03].

Tzeng

[QCB05a, Hsu05a, HL05d].

U

[DB04].

U-boat

[DB04].

U.K.

[CAC06].

U.S

[Uni01].

USA

[Bol02, PM00, Uni00b].
Ubiquitous [Sta03, LKZ+04].
UC-soundness [BPS08]. UCON [LY05, PS04b]. UK [CZ05, Chr00, Chr01, CCMR02, CCMR05, KN03, Pato03b, RS05, Sma05, Hon01, Mat05].
Ultimate [Dii01]. ultra [Bam02, CH07a, DB04, Cal01, Win00]. ultra-lightweight [CH07a]. ultra-secret [Bam02]. UltraSONIC [MMH02]. Ultrafast [FF01a]. UltraSONIC [MMH02]. Ultrawideband [Bra06]. UMTS [Cha05b, HL07]. Unauthorized [Ano02e].
Unbalanced [FMP03, May02, HLLL03]. Unbelievable [Len01]. Unborn [Pau02a]. Unbounded [RW02, WvD02]. Unbreakable [Ver06b, Mav02].
Uncertain [See04, Sty04, Hei03, Sch03]. UNCITRAL [MNFG02]. uncompletable [NS01a]. Unconditional [HM01b, May05, Pas05, RW03b, WW05].
Unconditionally [HSZI00, HSZI01, HSHI02, HSHI06, CCD06]. Uncovering [MNT+00]. Uncrackable [Ano03d]. undeciphered [Rob02, Rob09].
Undeniable [GMP01b, GM03, JSJK01, Miy01, WQWZ01, CHC05, LH04, LCZ05a, SS02]. Undergraduate [AA04b, Gha07].
undergraduates [DFGH04]. Understanding [AN03, CPGC+04, Cra05b, Elb09, Gor06, LG09, PP09, Sun05, Lun09]. Uncoverable [BMW02b]. Unexpectedly [Bar00a]. Unforgeable [BKY02, KY01a].
Unhooking [Moo01]. Unicode [MJF07]. Unified [CZB+01, HKA+05, MFS+09, SM03b, CCD06]. Uniform [SPK08, TL07, SU07]. uniformity [Shp01, Shp04b]. Unify [Sma06].
Unimodular [CV03]. Unique [Lam91, Lys02, TH01]. United [DFC00, Jol01]. Universal [BOHL+05, CR03, CJNP02, CS02, If00, KKKP05, KO03, Pli01, Sho00a, SP79, Cal00c, PS04c]. universality [DS02]. Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DN02b, DN03, NMO05, RK05]. Universally-Composable [AF04b].
Universiteit [BBDO9]. University [Kat05b, Puc03, Rot07, Top02]. UNIX [CCDP01, Har01a, Har01b, H601, Wi01, GSS03]. UNIX-Type [H501]. Unknown [CT08a, Luc02b, CSW05, HJ07]. Unknown [CMB*05]. unleash [Mc03]. Unleashing [Lop06]. unlinkability [WHH05]. Unpredictability [BS01d]. unprotected [ASK05]. Unravelling [Ano03g].
unrecongnizably [Wal04]. Unveiled [Bar00a]. unveils [Mad00c]. Update [Das08, TEM*01, Heo09]. Updated [Cho08a]. upgrading [HL03]. upgrade [Pau02a, Pau02b]. Upgrades [Ano02a].
upon [DFG01, PQ03a]. UPPAAL [BBDO9]. Upper [BP03b, DRR05, KMT01]. Upset [Bar06]. Upwards [FV03]. USR [LKZ+04].
US$54 [Duw03]. USA [ACM03, ACM04, ACM05a, ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KKP02, KJR05, Kili05, KP01, Men05, Men07, Nac01, Nao04, Oka04, Poo06, Pre02c, Sch01d, Sho05a, Sill01, YDM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FAM02, IEEE1a, IEEE05a, IEEE05b, IEEE08, IEEE09b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S*03, Sch04a, Sch05a, SMP+09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, W109, Yun02a]. usability [CG05, DVP09, WDC09]. Usage [LY05, PS04b]. Use [Bai01a, BWBL02, BDP02, BQR01, CPS07, Dru00, ISO05, Kra03, LCK04, Pau09, PHPW07, Str01a, WS05, Win01, CG05, OS07, St11].
used [CDL06, MSV04]. useful [SM03a]. Usenet [Coc01a]. USENIX [Coc01a]. User
[Ano00k, BGP02, CL01b, CMB+05, DP00, FDIR00, Had00, HY01, KZ09, LSZ05, MR03, OHB08a, P501b, Poh01, Sas07, SSM+08, Str01a, Tsao1, WDCJ09, BBM00, CL04d, Chi08b, Chi08c, Chi08d, CF07, DSGP06, Dea06, DLY08, GMLS02, HW03c, Hsu05b, HL05b, KC05, LAPS08, LHY02, LLH02, LKY04, LCP04, LL04c, LW04, LKY05a, LLW05, LLW09, LW04, LC05a, LLC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SHH07, Tan07a, TLH05, Tsao1, TJC03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04a, YW05, YC09a, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. User-Centered [CMB+05, user-controlled [LAPS08], user-drawn [vOT08], user-friendly [SZS05, WLT05a]. Users [LLS05b, CF05]. Uses [Bau01c, RSQL03]. ushers [Bur00]. Using [AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01c, Ano01n, ADDS06, BJ02, BH06, BK06a, BBC+09, B01a11b, B01b, BP06, BPS02, BR09, BT02, BM00, BPM00, BL01, Che01a, CLLL00, CGBS01, CCW02, CCM01, CC06, CC07c, C01a, DI05, DFR01, DP00, DW01, DGH+04, EFY+05, FJ03, FMP03, Fri01, GC01a, GL01, GSB+04, HHC+03, HQ05, HJW01, Jab01, JKK+01, JS01, KOY01, Kel05a, Kel05b, KM01a, KLC+00, KTT07, Kral2b, KZ09, L04a, Len01, LB04, LS05a, LXH07, LM02, LH07, MS02a, MS09a, MLM03, MS03b, MMJ05, NNAM10, NZC05, NM09, OT03a, PHK+01, PJH01, PJK01, PCK02, PK01, Sho00b, SK05a, Sma03a, SVW00, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VP01, WY02, W01, WC03a, XZ01, YK01, YLLL02, YSS+01, ZW01, Zhe01, ASW00, AL07, BCL05a, BCW05]. using [BK07, CG06, CDS07, CWH00, CL04d, CCK04b, CCHH05, CHY05b, CKY05, C01a, Che07a, CKY05, Che08a, Che08b, C04, CK03, Cos00, DZL01, Dan02, DSGP06, DS09, DFG00, FWTC05, GC00a, GMR05, Gen09b, GS09, HHS01, HW05, HA0R04, HT06, Hir09, HW04, HLT09, HY03, H0R04, JRR09, Jua04, KOY09, K09a, KLY03, KB09, KKL09, KKK+07, KSW06, KR03, Ku04, KO5, LHY02, LLH02, LKY04, LCP04, LL04c, LW04, LKY05a, LLW05, LLW09, LW04, LC05a, LLC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SHH07, Tan07a, TLH05, Tsao1, TJC03, 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. [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00c]. v2.1 [RSA02]. v2.11 [RSA01]. v2.1 [RSA01]. v5 [It00]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BL01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [PM00]. Value [BR09, G05, LS08, BM02a, DK08, WWTH08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadhrajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSN05, Ber08, Duj08, Duj09]. Variants [BDK+09, DG02, KS00b, CJ05, Sha04b, TJC03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDkKB09]. vast [Wa04]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pe09, mSgFtL05, WN04, WC05]. vectors [LHL04a]. Vegas [ELvS01, IEE01a]. Vein [BDkKB09]. Vendors [Pau03, MV03b]. Venona [Ben01b, Ben04]. venture [SW05b]. Verenigde [dL00]. Veridicom [Ano02d]. Verifiable [ARN01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Lyn02, NZC05, NSN05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a]. verifiably [BGLS03, Hes04a]. verifiably-encrypted [Hes04a].
YLC
HL05c, JW01, Ler02, MT07, MSP09,
PBD07, Tsa08, TYH04, Wan04b, Wn01,
YLC+09, ZLX99, ZL04b, CS08b, Uzu04.
Verified
BJP02, BFGT08, BFCZ08, CJT04, verifier
Bl01b, LKY05b, verifier-based
LKY05b.
Verifiers
CL01a, He02, IY07, LWK05b, YY05a, ZX04.
Verify [MS02a]. Verifying
BFG08, BJvB02, CJM00, HL01, IR01,
PT08, RR02, BLH06, BLP06, HLH00,
SV08a, Sh01d. Verlag
Eag05, Lee03a, Lee03b, Papp05. Version
Bol02, HPC02, OST05, SKI01, Mis06.
Versions [HRS+01, NPV01, An00f, CV05].
Verstecke [Sch09]. Versus
Mad00a, Rub00, WWL+01, ASW+01,
BJLS02, DBS01, WPP05. Vertically
[DN04]. Very
AAC+01, B+02, CG03, EBC+00, FLA+03,
Höf01, PM02, PBMB01, Zir07. Vestigies
[Top02]. VI [Sch04a]. via [AGKS07,
Ano00k, ACDM05, BDPV09, Car02, Che03,
CP+04, Eil08, FBWC02, Fox00, HHYW07,
HLM03, JJo00a, KT06, ML05, PG05, RG05,
SB01, SLG+05, ZLG01, Lod05. Victoria
ACM08, ZK00]. Victorian [Top02],
victory [Han03]. Vid [CAC06]. Video [BDF+01a,
BD03, CDTT05, EFY+05, ISSZ08, KBD03,
KJR05, KLL01, LHS05, ML01, S02a,
BS01b, CO09a, JAO2, KNO3, UP05].
Video-Based [KJR05, BS01b, KNO3].
videos [YZDW07]. Vienna [BZ02].
Vietnam [Lov01]. View
Bar00a, Mah04, Sin09, Woo05. Views
Bar00a, Bar00b, Bar00c, Coo01a, Coo02a,
Coo02b, Coo03. Vigenère [DG00]. VII
[Sch04b]. VIII [EEE01b, Sch05a]. Virginia
MS05b. Virtual [An00c, HM01a, Pro00,
YSS+01, BDS+09a, ML05, ZBP05].
Virtualization
CGL+08a, CGL+08b, CGL+08c.
Virtualization-based
CGL+08a, CGL+08b, CGL+08c. Virtues
[Tro08]. Virus [Gor06, An00c]. Visible
[HT06]. Vista [Fer06]. Visual
BDN00, BDDS03, BCD06, CCL09, CTY09,
CPD06, DD00, Kog02, KS03, RD09, WMS08,
YWC08, YC01, ZP05, ABDS01, CDFM05,
CDD07, DD04, HKS00, Lav09, PY08, Yan02,
YC07, Bon00, Zol01. Visualization
[XYL09, MS+09]. Vital [Wal04, Yon04].
Viterbi [LBGZ01, LGZ02]. Vladimirov
Puz04. VLDB [EBC+00, FLA+03].
VLDP [B+02]. VLSI [KV01]. VMSS
SC05a. Voice [An00f, PK01, VN04].
VoIP [An00c, SZ08, VAVY09, WC05]. Vol
Kat05b, Lee03b. volatile [SETB08].
Volume [Gol04]. Vortrag [Eke02]. Vote
Che07b. Voter [Cha04]. Voter-Verifiable
Cha04. Voting
Cha04, FPS01, HS00, Joh05, JLL02,
KMO01, Rub01, CJT03, HIW05. Voyovich
Rug04. VPN [KMM+06]. VPNS [Dav01a].
VQ [WJP07]. VQ-based [WJP07]. Vs
CTBA+01, Di 01, Di 03, SU07, WW04.
VSS [AF04b, CF01, FM02a]. Vu [DP00].
Vulnerabilities
CSW05, DMS07, Swi05, XNK+05.
Vulnerability [KHL09, SGA07, YRS+09].
WA [AC06]. WACs [Kov01]. Wagner
dVP06]. Wagstaff [Kat05b]. Wahab
MAaT07. Walking [Fox00]. Wall [Mc04].
Wallet [ETZ00, JL04]. Walsh [MS02b].
Walsingham [Bu06]. WAN [Höf01].
WAN-Cluster [Höf01]. Wang [SZ05].
Wants [Han00]. WAP [JRF01]. War
Bec02, Bud00a, Bud02, Han03, Kov01,
MH09, MC04, OC03, AJ08, DB04, Ris06,
Lov01]. Warfare [HW01, WW04]. Warrior
[PC04]. Wars [RR03b, Ca00d, Ca00e].
Warsaw [AUW01, Bih03]. washer [An00f].
Washington [S+03, USE00a, USE01c].
wasn’t [Bur02]. **WaSP** [Coc02b]. **WASSA** [Ano05c]. **Watch** [MA00a, Sav05a, Sav05b, Ano01m, Joy03a]. **Waterloo** [HH04, HH05, ST01d]. **Watermark** [AS01b, GMV01, JX05, KHY04, Kwo03a, Meh01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zan01, AA08, CL08, HN07, LYGL07, LLC06a]. **Watermark-based** [Kwo03a]. **Watermark-Fingerprint** [KHY04]. **Watermarked** [ST01c]. **Watermarking** [AS08, AK02b, AHK03b, AS01c, Arn01, ARC+01, BBC+09, BR09, BSC01a, BSC01b, BSL02, BQR01, BSN00, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB+08, DWN01, DNP07, EFY+05, EIG01, GW01, HTO6, HH09, JKK+01, KCR04, hKLS00, KLL01, Kun01, KTO0, LZ09, LLS05a, LKKL05, LZ01, LZP+04, LWS05, LPZ06, LJ05b, LSC03, LL01, LSKC05, MM01a, MNN00, OM01, OMM02, PJJH01, PJK01, PR01, PBM+07, Qu01, Sam09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Sh08, SP04, SLT01, SPK08, VVS01, VHP01, VK07, WC09, WH09, WNY09, WWL+02, WLT05b, XFZ01, YWWS09, ZTP05, ZWC02, AHK03a, AAPP07, BCKK05, CC02b, Che08b, CYH+07, CCD+04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, HLC07, HHC05, JDJ01, JA02, KA09, KP00, LDD07, Lin00a, Lin01b, LLC06a, LLC06b, MB08, MCH05].

**watermarking** [PK03, Ren09, mSGFL05, WJP07, WNQ08, Way02b, Way09, WC05, MRD08, XMST07, YZD07, YPSZ01, ZLZS07]. **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, LKKL05, LZ01, Nak01, VK07, AAPP07, AA08]. **wavelet-based** [AAPP07, AA08]. **Wavelet-Domain** [LZ01]. **WAVES** [LBA00]. **Way** [BYJK08, BM01a, CHL02, DIS02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, KKK7, KKKP05, KK03, LW04, LPM05, LQ08, LJKL01, Mic02a, Po00, Tsa08, YW05, YRY05b, ZW05a]. **Wayness** [KI01a, PV06b]. **Ways** [BB02]. **WCC** [Yr06]. **WDDL** [MMMT09]. **Weak** [HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00]. **Weakening** [ZD05]. **Weakly** [HGW01, LS01c, RW03b, DW09, GG08, KOY09, KW00]. **Weakness** [SW05a, CH05]. **Weaknesses** [FMS01, He02, KCL03, KCC05, SGGB00]. **Weapons** [RR03b]. **Weather** [WWL+02]. **Web** [Che01d, Mag05a, BFG05, BFG08, HIl06, An01c, An02e, An03d, AEV+07, BFG04, BC04b, CCCY01, Coc01a, Coc02a, Coc02b, CZB+01, De07, DMS09, FSS01, GS02a, GSVCO2, HM05, JMB+06, KCD07, JW00, LLS05b, LXM+05, MPPM09, PM00, RR04, Sam09, SS05, Sch01a, SBG07, TMMM05, WA06, YSS+01]. **Web-Based** [An01c, Sch01a, YSS+01]. **Web-enabled** [CCCY01]. **webcam** [McN03]. **WebFountain** [An03d]. **Webrelay** [Zha00]. **Weight** [CH07c, GK02, WT02]. **Weighted** [BT05, BT08, SC02c, YZ00]. **Weil** [BF01b, BF03, Jou02, Kir03]. **Well** [WWGP00]. **Welschenbach** [Ter08]. **Welsh** [Rot07]. **went** [AJ08]. **WEST** [SIR04]. **were** [Hau06]. **Wesley** [Puc03]. **West** [Fao01, Jue04, Syv02, Wri03]. **Westbridge** [An02e]. **Western** [CZB+01]. **West** [CC09]. **Weyl** [Sug03]. **WG** [DFPS06]. **WG11.1** [ELvS01]. **WG11.1/WG11.2** [ELvS01]. **WG11.2** [ELvS01]. **WG8.8** [DFCW00]. **Wheeler** [ABM08, Bar05]. **Where** [Bur06, Pen01a]. **While** [Tee06]. **WHIM** [JA02]. **WHIRLPOOL** [RB01]. **Whisper**
[NABG03]. Whitehouse [Mad00c]. Whitening [Oni01]. Whitfield [Jan08a]. Who [CZB+01, Urb01, Han06, Neu06]. whole [CPG+04]. Wi
[Puz04, Sty04, VGM04, FMA02, Bar03]. Wi-Fi [Sty04, Bar03]. Wi-Fo
[Puz04, VGM04]. wicked [Lud05]. Wi-Fi [Sty04, Bar03]. Wi-Foo
[Puz04, VGM04]. wicked [Lud05]. Wide [DR02a, SBB05]. Width [OT03b]. Width
[OT03b]. Wiener [Duj08, Duj09]. WIESS
[USE00b]. Wiley [And04, Gra01, Kir01a]. Will
[Ort00, Cla00b, Fur05]. William [Che05b, Pag03]. Williams [M¨ul01a]. Window
[OT03a, SSST06]. Windows
[USE00a, DGP07a, DGP07b, DGP09, Fer06, HB06, WD06, WD01a, Wit01]. Wins
[Bar00b]. Wired [Gil07, Pot07, SIR04]. Wireless
[AEAQ05, Bar03, BCH+00, ECM00b, Fin06, KH05, KHD01, LNL+08, NNAM10, Pau03, PZH09, Pot03, Puz04, Sin01a, Sty04, SYLC05, VGM04, YSR01, ZYN08, ZWCY02, Bad07, BP03a, BBG+02, CCM09, Cha05b, GW08, GG05b, HLT09, JRR09, KXTZ09, KB09, LDH06, LPV+09, LFHT07, LW05a, Lin07, Lop06, MJF+08, Mo01, NC09, NLD08, PCSV07, Par04, Pat02a, Pat02b, Pot07, SLP07, SVO8, TPO7, Vac06, Van03, Wan04a, YTWY05, CS08b, ECM00a, PDM09]. Wiretapping
[Cho08a, DL98, Jan08a, DL07]. WISA
[CS09]. Within
[MR02a, CHM+02, MR02b, You04]. Without
[BCL+05b, Bla01c, BB04, BGH07, Har06, NA07, Ano03c, CHO01a, CCK04b, CYH04, CCH05, CT08, CJO3c, CJ04, CDD07, CV06, DK01, KG09, Ku04, LV07, LHL04b, LW04, LKY05b, LL06, Lin01a, LCZ05b, Lys07, MP02, Mar07, PS04c, RG09, Ts08, WIFI0, WV05, YRY05b, ZW05a]. Withstanding
[DFS04]. Wits
[Bud00a, Bud02]. WLAN
[SSM+08]. WLAN/cellular
[SSM+08]. Woes
[BTTF02]. Women [FF01b]. won [Han03]. Worcester
[KP01]. Word
[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, BD08, CZ05, Chr00, Chr01, CCMR02, CCMR05, CSY09, DR02c, Des02, GH05, IEEO1b, IO00, JQ04, KPK02, KCR04, KGL04, Kim01, KP01, KN01, LST+05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RSS06, RM04, Sch00b, Sch01d, TB02, USE00b, VY01, Vau05a, WKP03, Ytr06, AMW07, AJ01a, BCKK05, Bir07, CL05, GKS05, HH04, HH05, HA00, ST01d]. World
[Bar03, GG05a, HW01, McE04, Nik02a, Nik02b, Sch00d, Sty04, YKMB08, Ano03c, Ark05, Bel07a, Che00b, Hei03, HH06, Hus01, KPS02, Kee05, Lie05, Lun09, Rob02, Rob09, Sch03, SL07, Bec02, Bud00a, Bud02, Han03, Kov01, MH09, OC03, Sty04, See04]. Worlds
[Wil01b]. Worm
[HL05a, CSW05]. Worms
[ZCTG05]. Worst
[CCM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case
[HR08, Mic02a, Mic02b, Pei09]. worst-case/average-case
[Mic02b]. Woz
[Bar00c]. WPA
[OM09]. wrapped
[HLC07]. Wrapper
[OS00]. Write
[BB02]. Writers
[Got06]. Writing
[HL03, Jan06, Kah67a, Kah67b, Kah69, Gas01]. Writings
[Cop04b]. WS
[JR06, RR04]. WS-Policy
[RR04]. WS-Security
[JR06, RR04]. WS-DL
[Bar00c]. WTLS
[Vau02]. WTMAU
[ECM00a, ECM00b]. WTMAU-SD
[ECM00a]. Wu
[BC05, CHY05a, CW01, CS03a, YY05b]. Wu-Lin
[YY05b]. Wuhan
[TTZ01]. WW
[Sal00a]. WWII
[WD01b]. X
[For04]. X.509
[SO05]. X.9.31
[Ke05a, Ke05b]. X.9.62
[ANS05]. Xbox
[Ste05b]. XCBC
[GD02]. XECB
[GD02]. Xia
[CJT04, Sha05a]. Xiamen
[DWML05].
REFERENCES

References

Xiao [JW01, YY05a]. Xilinx [Ano02e]. XIV [USE00c]. XIX [Top02]. XL [CP03]. XML [Hei01, TEM+01, AW05, AW08, Ano02e, BNP08, 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, LN00, LNS02, Ver01]. XML [Hei01, TEM+01, AW05, AW08, Ano02e, BNP08, 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, LN00, LNS02, Ver01].

Yahalom [Pau01]. Yang [McK04, CZ03, KJY05, WL05, YWC05]. Yang-Shieh [YWC05]. Yao [BPS08, BDNN02, ZD05]. Yao-style [BPS08]. Yarrow [KSF00, Mur02]. Yarrow-160 [KSF00]. Yaschenko [Kat05b]. YCH [SG07]. XMT [SG07]. XrML [Bar00a]. XTEA [CV05, HHK+04, MHL+02]. XTR [LW02, LN00, LNS02, Ver01].

Z [Wue09]. Z-parameter [Wue09]. z10 [Web08]. z9 [ADH+07]. Zealand [Zhe02b]. Zeilinger [Duw03]. Zero [AS01b, APV05, BP04, Con01, DPF04, DFS04, DDO+01, HNO+09, IKOS07, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00a, Ros06a, CSW05, Dam00, PBD07, KK07]. zero-day [CSW05].

Zeta [Ver02]. Zhang [JW01, YY05a]. Zhou [PKH05]. Zimmermann [McL06, Tuc66]. ZK [PBD05]. Zodiac [HSM+02]. Zone [Kum07].


[Aba00] Martín Abadi. Taming the adversary. In Bellare [Bel00], pages 353–??.
Aiello:2004:JFK


Abdalla:2005:SER


Abe:2001:SEP

Masayuki Abe. Security + Proof of Knowledge" in the random oracle model. Lecture Notes in Computer Science, 2271:277–??, 2001. CO-


[ACdM05] Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. Untraceable RFID tags via insubvertible encryption. In Meadows and

Atieniese:2000:PPS


ACM:2000:PTS


ACM:2001:PAA


ACM:2001:SHP


ACM:2002:PTF

ACM:2003:PTF


ACM:2003:PTS


ACM:2004:PAS


ACM:2004:PAA


ACM:2005:MPI


ACM:2005:PTF


ACM:2005:SPA

REFERENCES

960–8. LCCN QA75.5.A22 2005.


Alvarez:2005:EBS


Ahmad:2007:ADE


Anyanwu:2009:DCS


Avanzi:2006:ESM


Adee:2009:CDT


Arnold:2007:CSE

REFERENCES


Atighehchi:2009:EPA


Anton:2007:HEW


Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR

Giuseppe Ateniese, Kevin
REFERENCES


**Attrapadung:2006:FSS**


**Akkar:2001:IAS**


**Acquisti:2009:PSS**


**Akavia:2006:BOW**


See erratum [AGGM10].

**Akavia:2010:EBO**

REFERENCES

Alon:2007:GSE


Anagnostopoulos:2001:PAD


Ateniese:2005:PRS


Agrawal:2003:SWR

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

Agrawal:2003:WRD


Armington:2002:BAI

Ahmad:2007:CSS


Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB


Applebaum:2004:CNS

REFERENCES


Applebaum:2006:C


Al-Ibrahim:2001:AMS


Attali:2001:JSC


Attali:2001:SCP


Aid:2008:NSA

Matthew M. Aid and Thomas R. Johnson. National Security Agency re-

Avoine:2008:CIT


Al-Jarrah:2008:NKM


Abe:2002:KES


Agrawal:2002:WRD


Armknecht:2003:AAC

Frederik Armknecht and Matthias Krause. Algebraic attacks on combiners with memory. In Boneh [Bon03], pages 162–175. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743
REFERENCES


REFERENCES


REFERENCES


[AMWP07] Carlisle Adams, Ali Miri, and Michael Wiener, editors. Selected areas in cryptography: 14th international workshop, SAC 2007, Ottawa, Canada, August 16–17, 2007; revised se-
REFERENCES


REFERENCES


Anonymous:2000:AIH


Anonymous:2000:AIah


Anonymous:2000:CRR


Anonymous:2000:CCI


Anonymous:2000:CLI


Anonymous:2000:EES


Anonymous:2000:GBE

Anonymous. Governments back down on encryption regulations. Net-
REFERENCES

Anonymous:2000:UAS

Anonymous:2000:VAS

Anonymous:2000:APb

Anonymous:2001:APb
Anonymous. Authentication and naming (trans-

**Anonymous:2001:AWB**


**Anonymous:2001:A1gb**


**Anonymous:2001:CCA**


**Anonymous:2001:RAC**


**Anonymous:2001:EDS**

REFERENCES


REFERENCES


Anonymous:2002:PSS


Anonymous:2002:PFQ


Anonymous:2002:QCQ


Anonymous:2002:QCR


Anonymous:2002:RUB

Anonymous:2003:TMC


Anonymous:2003:YCS


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:
REFERENCES

<table>
<thead>
<tr>
<th>n</th>
<th>p</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1913</td>
<td>E. Fauquemberg</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1876</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1957</td>
<td>H. Riesel</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>25</td>
<td>21701</td>
<td>1978</td>
<td>L. C. Noll &amp; L. Noll</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson &amp; D. Shall</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>1988</td>
<td>W. N. Colquitt &amp;</td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>756839</td>
<td>1992</td>
<td>Slowinski &amp; Gagliardi</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski &amp; Gagliardi</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski &amp; Gagliardi</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud et al.</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, Wolrman</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala et al.</td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>2001</td>
<td>M. Cameron (GIMPS)</td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>M. Shafer (GIMPS)</td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2004</td>
<td>Josh Findley (GIMPS)</td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2005</td>
<td>Martin Nowak (GIMPS)</td>
</tr>
<tr>
<td>43</td>
<td>30402457</td>
<td>2005</td>
<td>Curtis Cooper &amp;</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp;</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elken</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strickland</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, Gagliardi</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, Gagliardi</td>
</tr>
<tr>
<td>49</td>
<td>74207281</td>
<td>2016</td>
<td>Curtis Cooper (GIMPS)</td>
</tr>
<tr>
<td>50</td>
<td>77232917</td>
<td>2017</td>
<td>Jon Pace (GIMPS)</td>
</tr>
<tr>
<td>51</td>
<td>82589933</td>
<td>2018</td>
<td>P. Laroche, G. Wolfé</td>
</tr>
</tbody>
</table>
Anonymous:2003:UCD


Anonymous:2004:BB


Anonymous:2004:CPS


Anonymous:2004:CJL


Anonymous:2004:Cf


Anonymous:2004:ISL


Anonymous:2004:NGJ


Anonymous:2005:CEC

REFERENCES


REFERENCES

Anonymous:2008:KAD

Anonymous:2008:RCB

Anonymous:2008:RES

Anonymous:2008:SHS

Anonymous:2009:BG

Anonymous:2009:DSS

Anonymous:2009:PCA
REFERENCES

Anonymous:2009:TCA


Anonymous:2012:SHS


Anonymous:2013:DSS


the ACM 2007 Doctoral Dissertation Award.

[APV05]

[AR00]

[AR01]

[Ara02]

[ARC+01]
Mikhail J. Atallah, Victor Raskin, Michael Crogan, Christian Hempelmann, Florian Kerschbaum, Dina Mohamed, and Sanket Naik. Natural language watermarking: Design, analy-
sis, and a proof-of-concept implementation. Lecture Notes in Computer Science, 2137:185–??, 2001. CO-
link/service/series/0558/tocs/213701.htm;

Aaraj:2008:ADH
[Najwa Aaraj, Anand Raghu-
nathan, and Niraj K. Jha. Analysis and design of a hardware/software trusted platform module for embed-
ded systems. ACM Transactions on Embedded Com-
puting Systems, 8(1):8:1–8:??, December 2008. CO-
DEN ????? ISSN 1539-9087 (print), 1558-3465 (elec-
tronic).

Ark05
www.loc.gov/catdir/toc/ecip052/2004025039.html]

Agrawal:2003:MCA
[Dakshi Agrawal, Josyula R. Rao, and Pankaj Rohatgi. Multi-channel attacks. In Walter et al. [WKP03],
pages 2–16. CODEN LNCSD9. ISBN 3-540-
40833-9. ISSN 0302-9743 (print), 1611-3349 (elec-
issue&issn=0302-9743&volume=t2779;

Artail:2004:PAC
September 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (elec-
REFERENCES

Abe:2001:SPA


Adelsbach:2001:ZKW


Agung:2001:ICI


Agarwal:2008:DWS


Asenjo:2002:AES


Ashburn:2003:PBA

Julian Ashburn. *Practical Biometrics: From
REFERENCES


Acicmez:2005:IBB


Acicmez:2007:MAC


Aslan:2004:HSM


Aslan:2004:LAA


Blanchet-Sadri:2001:MSD


Abdalla:2000:KMR

REFERENCES

Allison:2001:LLE


Aharonov:2000:QBE


Atieniese:2004:VED


Arnold:2004:IPN

REFERENCES

A workstation with a 2.2 GHz processor can perform a full search in one.


Philip A. Bernstein et al., editors. VLDP 2002: pro-

Blanton:2006:SRF


Bagnulo:2002:PAA


Badra:2007:AWC


Baier:2001:ECP


Baier:2001:ECS


[Bar00b] 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
REFERENCES


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


Gregory V. Bard. *Algebraic cryptanalysis*. Springer-Verlag, Berlin, Germany / Hei-
REFERENCES


REFERENCES

Bauer:2003:PPAb


[Bau03b] [Bau03b]

Baudet:2005:DSP


[Bau05] [Bau05]

Bauer:2007:DSM


[Bau07] [Bau07]

Blakley:1979:RSA


[BB79] [BB79]

Benedens:2000:TBD


[BB00a] [BB00a]

Buchmann:2000:ECC

Johannes Buchmann and Harald Baier. Efficient construction of cryptographically strong elliptic

**Barkan:2002:HMW**


**Bouda:2003:EQI**


**Boneh:2004:SIB**


**Bicakci:2005:ISA**


**Biham:2002:SQK**

REFERENCES


REFERENCES

Blumenthal:2002:SAD


Bartolini:2008:EIS


Barkan:2003:ICO

Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. In Boneh [Bon03], pages 600–616.

Barkan:2003:ICO


Bellare:2001:OCH


133
REFERENCES


REFERENCES

135


Biham:2004:NCS


Blundo:2004:SIA


Backes:2005:PKS


Bergadano:2005:DPL


Blundo:2005:SCN

REFERENCES


Brzeziński:2005:MRL


Bergadano:2001:CSA


Bergadano:2002:IAM


Brier:2001:CRS

REFERENCES


Brown:2000:PCW


Breunesse:2005:FMS


Boneh:2007:CCS


Butler:2006:FAK


Barni:2005:DWI


Bao:2005:PSS

REFERENCES

Barak:2005:SCA


Bresson:2001:PAG


Bresson:2002:DGD


Bolle:2003:GB

REFERENCES

pp. LCCN TK7882.B56 G85
2003. US$49.95.


REFERENCES

Boneh:2000:CRP

Bourbakis:2003:SBC

Bozzano:2004:AVS

Burmester:2004:HPK

Buchmann:2008:PQC

Biryukov:2003:CS
[BDD03] Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of Safer++. In Boneh [Bon03],
Bao:2001:SPD

Boneh:2001:LBM

Bodei:2002:PAP
Chiara Bodei, Pierpaolo

Bodei:2005:APS


Bao:2001:CTS


Bhattacharyya:2009:VPA


Biham:2002:EDL


Biham:2002:LCR

REFERENCES

144

bibs/2355/23550016.htm;
http://link.springer-
ny.com/link/service/series/0558/papers/2355/23550016.pdf.

[Biryanov:2009:KRA]

[BDN00]

[Bodei:2002:FLD]

[Boreale:2002:PTC]

[Bertoni:2009:RPK]
Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The road from Panama to Keccak via RadioGatún. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, Symmetric Cryptography, number 09031 in Dagstuhl Seminar Proceedings, page ?? Schloss Dagstuhl — Leibniz-Zentrum für Informatik,
REFERENCES

Biryukov:2004:MLA

Baldwin:2009:PSS

Buchmann:2009:HBD

Bertino: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 Pub-

Beckman:2002:CAB


Bebee:2005:CBPd


Bejtlich:2006:EDS


Bellare:2000:ACC


Bella:2001:MPS

Giampaolo Bella. Mechanising a protocol for smart cards. Lecture Notes in Computer Science, 2140: 19–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
REFERENCES

Bellovin:2004:IRS

Belfield:2007:SUC

Bella:2007:FCS

Bello:2008:OPR

Bruss:2007:QCS

Benedens:2000:AIW

Benantar:2001:IPK
M. Benantar. The Internet public key infrastruc-
REFERENCES


[Ber04] Daniel J. Bernstein. Floating-point arithmetic and mes-
sage authentication, September 18, 2004. URL https://cr.yp.to/antiforgery/ hash127-20040918.pdf. To be incorporated into the author’s High-Speed Cryptography book. [As of 13 May 2024, this book seems not to have been published].


REFERENCES


[Biham:2000:IDR]

[Biham:2000:ID]

[Babble:2001:MHO]

[Boneh:2001:IBE]

[Boneh:2001:EGS]
REFERENCES


[BFG05] Karthikeyan Bhargavan, Cédric Fournet, and An

[BFMR02]

Bhargavan:2008:VPB

[BFG08]


[Bhargavan:2008:VII]

Bhargavan:2008:VII

[BFGT08]


[Bugliesi:2007:DTA]

Bugliesi:2007:DTA

[BFM07]


[BG07a]

Brown:2007:SAN

[BG07a]


[Bugliesi:2007:SIT]

Bugliesi:2007:SIT

[BFMR02]


[BIb:2008:VII]

Bhargavan:2008:VII

[BFG08]


[BG07a]

Brown:2007:SAN

[BG07a]


[BFMR02]


[BFMR02]


[BFMR02]

REFERENCES

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

Blaszczyk:2008:NMT


Blaszczyk:2009:EVT


Boneh:2007:SEI


Bennett:2002:ESE


Barthe:2009:FCC


REFERENCES


REFERENCES


Chengpeng Bi. A Monte Carlo EM algorithm for De Novo Motif discovery in biomolecular sequences. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 6(3):370–386, July 2009. CODEN ITCBCY. ISSN 1545-
REFERENCES

5963 (print), 1557-9964 (electronic).

**Bidgoli:2003:EIS**


**Biggs:2008:CII**


**Biham:2000:CPR**


**Biham:2002:HDE**


**Biham:2003:ACE**

REFERENCES

Beimel:2000:RSC


Bajard:2003:EMG


Bajard:2005:AOP


Biryukov:2007:FSE


Bishop:2003:ICJ


Bishop:2003:CSA

REFERENCES


REFERENCES


BREUNESSE:2002:SV


BONI:2000:NGT


BURNSIDE:2005:CCP


Barker:2006:RRN


Breveglieri:2006:GEI


Barker:2007:RRN

Elaine Barker and John Kelsey. *Recommendation...

**Barreto:2002:EAP**


**Breveglieri:2007:OCA**


**Bellare:2004:BPR**


**Bajard:2009:SRB**


**Bellare:2000:SCB**

REFERENCES


[BKW03] Buonanno:2002:IUE

[BKY02] Broadfoot:2002:ASA

[BK08] Bucci:2008:FDR

[BL00] Black:2000:TDE
Michael Andrew Black. A treatise on data encryption and an example of the black algorithm. Thesis (M.A.), University of California, Santa Barbara, Santa Barbara, CA, USA, 2000.

[BL01a] Blanchet:2001:ACP
Blanchet:2001:ECP


Blaze:2001:LYS


Blanchet:2002:SAS


Blaze:2002:CI


Blaze:2003:FCI


REFERENCES

 Bozga:2006:PBA


Buchmann:2009:PQC


Banks:2001:CAS


Blunden:2009:RAE


Batina:2001:AWD

REFERENCES

**Blomer:2001:LSE**


**Brincat:2001:KRA**


**Basu:2003:AC**


**Blomer:2003:NPK**


**Boyd:2003:PAK**

REFERENCES

Burke:2000:ASFa

Burke:2000:ASFb

Burke:2000:ASFc

Boneh:2000:GRK

Biehl:2000:DFA

Boyd:2001:ECB
REFERENCES

Boyko:2000:PSP


Boneh:2003:SSS


Buchmann:2006:PCL


Borselius:2002:VTS


Borselius:2002:PAU


Boyen:2005:DCC

[BMW05] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based

Bellare:2000:AER


Boneh:2000:TC


Bellare:2002:TSE


Bouganim:2008:DAC


Bellare:2002:PRI

Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The power of RSA inversion oracles and the security of chaum’s RSA-based blind signature scheme. Lecture Notes in Computer Science, 2339:319–??, 2002. CO-


REFERENCES


REFERENCES


Burnett:2001:RSO


Bellare:2002:GSI


Buchbinder:2003:LUB


Bellare:2004:KEA

Mihir Bellare and Adriana Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In Franklin [Fra04], pages 273–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743

BP01b


BP03a


BP03b


BP04

Mihir Bellare and Adriana Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In Franklin [Fra04], pages 273–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743
REFERENCES


[BP05] Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. In Shoup [Sho05a], pages
REFERENCES


REFERENCES


Bellare:2000:ETE


Black:2001:CAF


Bellare:2000:ETE


Black:2001:CAF


Black:2002:BCM

REFERENCES


Bellare:2004:CBG


Bellare:2006:MPP


Bhatnagar:2009:RRW


Brands:2001:RPK


Brandt:2001:CPS

REFERENCES


Jürgen Bierbrauer and Holger Schellwat. Almost independent and weakly biased arrays: Efficient constructions and cryptologic applications. In Bellare [Bel00], pages 533–?? ISBN 3-540-67907-3. ISSN 0302-9743
REFERENCES


REFERENCES

0302-9743 (print), 1611-3349 (electronic).

[Boneh:2001:UBE]

[Banks:2002:NSR]

[Bajard:2003:ISC]

[Barrett:2005:SSS]

[Bo:2001:EID]
REFERENCES

Bo:2001:SCD

Bounkong:2002:ICA

Brisbane:2000:RBW

Bresson:2002:TRS
REFERENCES


REFERENCES


REFERENCES


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


Burke:2002:IWA


Burr:2003:SAE


Burr:2006:CHS


Boesgaard:2004:RNH


Baker:2007:ISU


Blake-Wilson:2002:RUE

REFERENCES

Butler:2000: NSA


Bellare:2003:FSP


Bar-Yossef:2004:ESQ


Bar-Yossef:2008:ESQ


Bertlmann:2002:QUB


Bond:2003:DTA

189

Borders:2005:CHP


Carrington:2002:EDS


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).

CAMTC:2000:TSC

REFERENCES

Caloyannides:2000:EWE

Caloyannides:2000:EWS

Calvocoressi:2001:TSU

Canetti:2001:UCS

Canetti:2001:OPR

Canetti:2006:SCC

Canetti:2006:OPR

Caprara:2001:PSR
REFERENCES


Carriere:2000:PSC

Carter:2001:SCT

Carlet:2002:LCC

Casey:2002:HCC

Cass:2003:LES

Casselman:2006:MTE
REFERENCES


REFERENCES

323–326, 2001. CODEN IJCMAT. ISSN 0020-7160.


REFERENCES


REFERENCES

Cattaneo:2001:DIT


Chen:2004:TPM


Chang:2004:IDA


Chang:2004:SOT


Chang:2005:DSM


Chang:2009:PCC


Christianson:2001:PKC

Bruce Christianson, Bruno Crispo, and James A. Malcolm. Public-key cryptosystems using symmetric-key crypto-algorithms. Lec-


[CCMT09] Claude Castelluccia, Aldar C-F. Chan, Einar Mykle- tun, and Gene Tsudik. Efficient and provably secure aggregation of encrypted


REFERENCES


Crouch:2001:LAR


Cramér:2000:CVS


Ceselli:2005:MAI


Cimato:2007:CVC


Cramér:2001:CRS

REFERENCES

QA76.9.A25 C79 2001;
QA267.A1 L43 no.2139.
UK£47.00. URL http://link.springer-ny.com/
link/service/series/0558/bibs/2139/21390503.htm;

Cimato:2005:ICV


Cramer:2005:CMS


Cavallar:2000:FBR

REFERENCES


REFERENCES


Chapman:2001:PEA


Castiglione:2007:TAD


Chen:2005:NVW


Ceravolo:2004:ERH


Certicom:2004:CCC


Canetti:2001:UCC

Ran Canetti and Marc Fischlin. Universally com-
posable commitments. In Kilian [Kil01a], pages 19–
?? ISBN 3-540-42456-
3 (paperback). LCCN
QA76.9.A25 C79 2001;
QA267.A1 L43 no.2139.
UK£47.00. URL http://
//link.springer-ny.com/
link/service/series/0558/
bibs/2139/21390019.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2139/21390019.

Canteaut:2001:COR

[CF01b] Anne Canteaut and Eric Filiol. Ciphertext only re-
construction of stream ci-
phers based on combina-
tion generators. Lecture 
Notes in Computer Science,
1978:165–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
http://link.springer-ny.com/
link/service/series/0558/
bibs/1978/19780165.htm;
http://link.springer-
ny.com/link/service/series/

Cramer:2002:OBB

[CF02] Ronald Cramer and Serge Fehr. Optimal black-box
secret sharing over arbi-
trary Abelian groups. In [CFA+06]
Yung [Yun02a], pages 272–
287. CODEN LNCSD9.
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/
2442/24420272.htm; http://
//link.springer.de/link/
/service/series/0558/papers/
2442/24420272.pdf.

Clarke:2005:AUM

[CF05] N. L. Clarke and S. M. Furnell. Authentication of
users on mobile telephones — a survey of attitudes
527, October 2005. CODEN 
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167404805001446

Clarke:2007:AUA

[CF07] N. L. Clarke and S. M. Furnell. Advanced user au-
thentication for mobile
devices. Computers & Security,
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167404806001428

Cohen:2006:HEH

Henri Cohen, Gerhard Frey, Roberto Avanzi, et al., ed-
itors. Handbook of Elliptic
and Hyperelliptic Curve
Cryptography. Discrete


[Climent:2006:NEC]


P. Caballero-Gil, A. Fúster-Sabater, and C. Hernández-Goya. Graph-based ap-

REFERENCES
proach to the edit distance cryptanalysis of irregularly clocked linear feedback shift


Crosby:2002:CHB

Chen:2008:OVBa

Chen:2008:OVBb

Chen:2008:OVBc

Caballero-Gil:2007:PSC


Canovas:2002:DSB


Cox:2002:SP9


Cimato:2003:SCN

REFERENCES


[CH07a] Hung-Yu Chien and Chen-Wei Huang. Security of ultra-lightweight RFID authentication protocols and


Chin-Chen Chang, Min-Shian Hwang, and Tung-


REFERENCES


Cheon:2001:NVR


Cherry:2001:HMH


Cherry:2001:HDS


Cherry:2001:REM


Chen:2002:SFS


Cheng:2003:PPO


Chen:2004:IAM

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

Cheng:2004:BSD

Chen:2005:TSS

Cherry:2005:MDC

Chess:2005:SAC

Chen:2007:CIS

Cherry:2007:MEV

Chen:2008:CIS
REFERENCES

Chen:2008:MWS

Chien:2008:EPA

Chien:2008:PAUa

Chien:2008:PAUb
REFERENCES

Chien:2008:PAUc


Chien:2008:SCA


Coron:2001:GGC


Coron:2001:OCC


Coppersmith:2002:CSC

REFERENCES


REFERENCES


REFERENCES


[CHS05] 

[CHSS02] 

[CHT02] 

[Chu02] 

[CHVV03] 
Brice Canvel, Alain Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password


Linda A. Cornwall, Jens Jensen, David P. Kelsey, Ákos Frohner, Daniel Kouřil.
REFERENCES


0558/papers/1807/18070369.pdf.

Coron:2002:UPS


Chepyzhov:2001:SAF


Chien:2002:EPS


Chien:2003:CMV

Chien:2004:SIS


Canetti:2002:SAI


Canetti:2002:UCN


Cook:2006:CEG


Cheon:2002:IID

REFERENCES


Chung:2003:EPX

[CKK03] Yon Dohn Chung, Jong Wook Kim, and Myoung Ho Kim.
Efficient preprocessing of XML queries using structured signatures.
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chun:2003:DLC

[CKL+03] Kilsoo Chun, Seungjoo Kim, Sangjin Lee, Soo Hak Sung,
and Seonhee Yoon. Differential and linear cryptanalysis for 2-round SPNs.
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cox:2005:DWT


Chen:2009:SRP


Coppersmith:2000:KRF

REFERENCES


REFERENCES


REFERENCES


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

**Chang:2008:AWM**


**Chien:2009:EBL**


**Chang:2001:ASM**

REFERENCES


[Chen:2009:AKD] Bee-Chung Chen, Kristen Lefevre, and Raghu Ramakrishnan. Adversarial-knowledge dimensions in


REFERENCES


[Craw] 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,
REFERENCES


Cremers:2006:ISE


Campo:2001:JFC


Chevallier-Mames:2003:FDS


Chao:2000:CHC

Jinhui Chao, Kazuto Matsuo, Hiroto Kawashiro, and Shigeo Tsujii. Construction of hyperelliptic curves with CM and its application to cryptosystems. *Lecture Notes in Computer Sci-
Cid:2006:AAA

Cho:2008:DNP

Caputo:2009:DIT

Crawford:2002:FEE

Coron:2004:SSL

Ciet:2003:PFI
M. Ciet, M. Neve, E. Peeters, and J.-J. Quisquater. Parallel FPGA implementation of RSA with residue number systems — can side-channel threats be avoided? In *MWSCAS ’03. Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Sys*
REFERENCES

tems, volume 2, pages 806–810. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. CODEN ????, ISSN ????

Catalano:2002:HHL


Correia:2006:CAB


Czernik:2009:CRN


Cobb:2004:CD

Chey Cobb. Cryptography For Dummies. For dummies. John Wiley and Sons, Inc., New York, NY,


http://www.loc.gov/catdir/toc/fy053/2004275594.html


REFERENCES

colossus-computer.com/.

Corella:2000:FIT


Coron:2000:ESF


Coron:2002:SPP


Coron:2006:WC


Cosgrave:2000:NTC


Costlow:2003:BIM

REFERENCES

dsonline.computer.org/0309/d/brief.htm.

Courtois:2001:EZK


Courtois:2003:FAA


Courtois:2003:AXA


Courtois:2004:FSB


Courtois:2002:CBC


Courtois:2003:AXA

Nicholas T. Courtois and Jacques Patarin. About the XL algorithm over $GF(2)$. In Joye [Joy03b],
Chatzikokolakis:2007:FAP


Cimato:2006:PVC


Chow:2004:UDL


Chen:2004:SEP


Catalano:2004:IIP

Dario Catalano, David Pointcheval, and Thomas Pornin. IPAKE: Isomorphisms for Password-Based

Canetti:2007:CSH


Ciet:2001:SFC


Canetti:2003:UCJ


Cramer:2005:ACE

Crampton:2005:UDR


Crenshaw:2000:SPK


Crowley:2001:MFL


Chhabra:2009:MSP


CRI:2000:DPA


Cramer:2000:SSB


Cramer:2002:UHP

Ronald Cramer and Victor Shoup. Universal hash

Camenisch:2003:PVE


Cramer:2003:DAP


Cramer:2003:DAP


Carrier:2004:STP


[CS08a] Eoghan Casey and Gerasimos J. Stellatos. The impact of full disk encryption....

Chang:2008:DAP


Cusick:2009:CBF


Czeskis:2008:DED


Cai:2007:CSM


Crandall:2005:DUV


Chen:2008:CCS

REFERENCES


REFERENCES


Chou:2009:ATI


Crawford:2001:FPV


Chiang:2008:CPB


Chang:2004:ASS


Cheung:2001:TPS


Collberg:2007:DGB

Christian S. Collberg, Clark Thomborson, and Gregg M.
REFERENCES


Chen:2009:FCV


Cheng:2001:NPT


Curtin:2005:BFC


Chaitanya:2008:QQM


Canteaut:2002:DCH

http://link.springer-ny.com/link/service/series/


REFERENCES


Chang:2002:ATI


Chess:2007:SPS


Cheng:2009:NAS


Chang:2000:ELD


Chien:2001:CCW


Crosby:2009:OLR

Scott A. Crosby, Dan S. Wallach, and Rudolf H. Riedl. Opportunities and limits of remote timing attacks. ACM Transactions
REFERENCES

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

Chien:2005:NRS


Chen:2005:ENB


Chang:2008:EBD


Chang:2001:NSS

Chang:2004:TSSb


Chang:2005:CIA


Chang:2005:SAK


Chung:2007:SBW

REFERENCES

Crawford:2001:FHC


Cheng:2005:RIC


Dodis:2003:CAA


Dale:2001:BSA


Damgaard:2000:ECZ

REFERENCES


REFERENCES

[DeBrosse:2004:SBU]

[DeBorde:2007:STF]

[Doyle:2006:SCK]

[diVimercati:2005:CSE]

REFERENCES


DeBonis:2000:RVC


Dalkilic:2002:CPF


DeBonis:2004:RSS


Diene:2006:DLE


Dolev:2000:NC


Dolev:2003:NC

DeSantis:2001:RNI

Dean:2006:IMB

DeLooze:2007:PWS

Desai:2000:ESS

Desai:2000:NPC

Desai:2000:SAN
Anand Desai. The security of all-or-nothing encryption: Protecting against exhaustive key search. In Bellare [Bel00], pages 359–?? . ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25

Desmedt:2002:PKC


Dewson:2008:BSS


Dhem:2001:HSS


Delgado:2007:SCD


REFERENCES


REFERENCES

com/openurl.asp?genre=
issue&issn=0302-9743&volume=
3152; http://www.springerlink.com/
com/openurl.asp?genre=
volume&id=doi:10.1007/b99099.

[DFSS05] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded-

[DFSS08] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-


[DG03] Mario Di Raimondo and Rosario Gennaro. Provably secure threshold password-
authenticated key exchange. Lecture Notes in Computer Science, 2656:507–
523, 2003. CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (elec-
springer.com/content/pdf/ 10.1007/3-540-39200-9_ 32.pdf.

[DG05] Mario Di Raimondo and

DiRaimondo:2006:PST


Dodis:2004:REK


Devanbu:2004:FAX


Devanbu:2003:ADP


Dwork:2003:MBF

Dorrendorf:2007:CRNa

Dorrendorf:2007:CRNb

Dorrendorf:2009:CRN

denHartog:2008:TMC

Dhem:2003:EMR

Deng:2006:OOC
Yan-Xiang Deng, Chao-Jang Hwang, and Jiang-


REFERENCES

C794 2005; QA76.9; Internet. URL http://
/ww.sprin.grlink.com/
topenurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

[Dic03] Markus Dichtl. How to predict the output of a
hardware random number generator. In Walter et al. [WKP03], pages 181–
188. CODEN LNCSDO. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
3349 (electronic). LCCN TK7895.E42. URL http://
/link.springer-ny.com/
link/service/series/0558/
tocs/t2779.htm; http://
ww.sprin.grlink.com/
topenurl.asp?genre=issue&
issn=0302-9743&volume=

[Dim07] Christos K. Dimitriadis. Improving mobile core net-
work security with honeynets. IEEE Security &
Privacy, 5(4):40–47, July/
August 2007. CODEN ????
ISSN 1540-7993 (print), 1558-4046 (electronic).

[Dif01] Whitfield Diffie. Ultimate cryptography. Com-
munications of the Association for Computing
Machinery, 44(3):84–86, March 2001. CODEN
CACMA2. ISSN 0001-0782
(print), 1557-7317 (electronic). URL http://
www.acm.org/pubs/citations/
journals/cacm/2001-44-
3/p84-diffie/.

[Die00] Jürgen Dierickx. European guidelines for dig-
March 1, 2000. CODEN NTSCF5. ISSN 1353-4858
(print), 1872-9371 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485800030063

[Dif01] Whitfield Diffie. Ultimate cryptography. Com-
munications of the Association for Computing
Machinery, 44(3):84–86, March 2001. CODEN
CACMA2. ISSN 0001-0782
(print), 1557-7317 (electronic). URL http://
www.acm.org/pubs/citations/
journals/cacm/2001-44-
3/p84-diffie/.

Imbert, and Pradeep K.
Mishra. The double-
base number system and its application to elliptic
curve cryptography. Mathematics of Computation,
77(262):1075–1104, April
2008. CODEN MCM-
PAF. ISSN 0025-5718
(print), 1088-6842 (elec-
tronic). URL http://
www.ams.org/mcom/2008-
77-262/S0025-5718-07-02048-
0/home.html; http://
www.ams.org/mcom/2008-
77-262/S0025-5718-07-02048-
0/S0025-5718-07-02048-
0.dvi; http://www.ams.
org/mcom/2008-77-262/S0025-
5718-07-02048-0/S0025-
REFERENCES

267

5718-07-02048-0.pdf;
http://www.ams.org/mcom/
2008-77-262/S0025-5718-
07-02048-0/S0025-5718-
07-02048-0.ps

[DIRR05] Nenad Dedić, Gene Itkis,
Leonid Reyzin, and Scott
Russell. Upper and
lower bounds on black-
box steganography: Ex-
tended abstract. In Kil-
ian [Kil05], pages 227–
?? CODEN LNCSD9.
ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
T44 2005. URL http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3378; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b106171.

[DJS02] Zhe Dang, Oscar H. Ibarra,
and Zhi-Wei Sun. On the
emptiness problem for two-
way NFA with one reversal-
bounded counter. Lecture
Notes in Computer Science,
2518:103–??, 2002. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer.de/link/
service/series/0558/bibs/
2518/25180103.htm; http:
//link.springer.de/link/
service/series/0558/papers/
2518/25180103.pdf.

[DJ01] Ivan Damgård and Mads
Jurik. A generalisation,

[DJ06]


[DJLT01]


[DJS00]


[D02]

REFERENCES


Dhem:2000:PIT


Ding:2000:SSC


Dodis:2009:CAI


Datta:2005:RBN


Delaune:2008:FAP


Dittmann:2005:CMS

[DKU05] Jana Dittmann, Stefan Katzenbeisser, and Andreas Uhl, editors. Communications and multimedia security: 9th IFIP TC-6 TC-11 International Conference, CMS 2005, Salzburg,

Dodis:2002:KIP

dodis:2002:kip


Diffie:1998:PLP

diffie:1998:plp


delLeeuw:2000:CSD

delleeuw:2000:csd


Diffie:2007:PLP

diffie:2007:plp


delLeeuw:2007:HIS

delleeuw:2007:his


DelLungo:2005:GSP

dellungo:2005:gsp

[DLMM05] Alberto Del Lungo, Guy Louchard, Claudio Marini,


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

Drimer:2007:KYE

Dumais:2000:PCQ

Dowd:2007:ASS

Denev:2009:SFQ

Ding:2007:ESD

Damgaard:2000:INC
Ivan Damgård and Jesper Buus Nielsen. Improved non-committing encryption schemes based on a general complexity assumption. In Bellare [Bel00], pages 432–?? ISBN 3-540-67907-3. ISSN 0302-9743
REFERENCES


(DN03) Ivan Damgård and Jesper Buus Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. In Boneh [Bon03], pages 247–
REFERENCES


REFERENCES


IEEE Computer Society order number P3010.


Crescenzo:2004:CRR


Daemen:2000:NPN


Daemen:2000:RA


Daemen:2001:AAR


Daemen:2002:AWT


Daemen:2002:DRA


Daemen:2002:FSE


Ding:2002:HEE

REFERENCES

0558/papers/2285/22850001.pdf.


[DRS05] Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors. Advanced en-
REFERENCES


Devanbu:2000:CVT


Dodis:2002:NUO


DArco:2003:FTD


Ding:2005:RNM


REFERENCES

www.sciencedirect.com/science/article/pii/S1084804500901280


[Dug04] Dominic Duggan. Type-based cryptographic oper-


[Dur01] Luciana Duranti. The long-term preservation of au-
REFERENCES

2001/P625.pdf.


[DV05]


[DV08]

[DV09]

REFERENCES


REFERENCES 286


[DY09b] Jintai Ding and Bo-Yin Yang. Multivariate public key cryptography. In Bernstein et al. [BBD09],

[DwWmW05] Yong Ding, Kwok wo Wong, and Yu min Wang. A w-
REFERENCES


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


Martin Ekerå. Differential cryptanalysis of MD5.
REFERENCES


[El-Kassar:2001:GPK]

[Elbirt:2008:AAI]

[Elbirt:2009:UAC]

[Ell04]

[Ell04]

[EM03]
REFERENCES


Erickson:2008:HAE


Ellison:2000:TRP


Ellison:2000:IRRa


Ellison:2000:IRRe


Enck:2005:EOF


Ettinger:2002:QQC


Ebringer:2000:PAP

Evans:2009:BRS


Edman:2009:AES


Elbirt:2000:FIP


Fan:2003:ILC

REFERENCES

294

(print), 1873-5649 (electronic).


**Furnell:2000:ASS**


**Feltke:2006:ATH**


**Fischlin:2000:ENM**


**Filiol:2001:NUS**


**Ferguson:2000:SEK**


**Ferguson:2006:ACE**


**Flannery:2001:CYW**

REFERENCES


[Fridrich:2001:DLS]

[Frenkiel:2002:CCS]

[Focardi:2000:ITN]

[Focardi:2000:MAT]

[Focardi:2003:CTA]
REFERENCES


REFERENCEs


[Fis05] Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In Shoup [Sho05a], pages 152–?? ISBN 3-540-28114-2. ISSN 0302-9743


REFERENCES

Whiting. Improved cryptanalysis of Rijndael (abstract only). In NIST [NIS00], page 9. ISBN ???. LCCN ???.


[FSA+03] Johann Christoph Freytag, Peter C. Lockemann, Serge Abiteboul, Michael J. Carey, Patricia G. Selinger, and Andreas Heuer, edi-
Fluhrer:2002:CMB


Fluhrer:2002:CSP


Feng:2006:ISC


Fan:2002:ETB


Fehr:2002:LVD

Serge Fehr and Ueli Maurer. Linear VSS and distributed commitments based on secret sharing.

Fuller:2002:LRA


Franklin:2002:PAS


Fournier:2003:SEA


[Fox:2000:NTFb] Robert Fox. News track: Flying the rails; logging online hours at work; top prize: embedded encryption; Digital Nose knows; walking again via chip implant; cellphone-free class; another
REFERENCES


Freking:2000:MMR


[FP00]

Fouque:2001:SDC


[FPS01]

Fouque:2001:TCS


[FR02]

Fernandes:2002:SAL

Savio Fernandes and KLM Reddy. Securing applications on Linux with PAM. *Linux Journal*, 102:??, October 2002. CODEN LI-
REFS


Fournet:2008:CSI


Frankel:2001:FCI


Fremberg:2003:MAP


Friberg:2001:UCH

Paul Friberg. Using a cryptographic hardware token with Linux: The OpenSSL

**Frith:2007:SAO**


**Frykholm:2000:CAB**


**Ferguson:2000:CEI**


**Fouque:2001:FDT**


**Friedlander:2001:DDH**


**Furukawa:2001:ESP**

Jun Furukawa and Kazue Sako. An efficient scheme for proving a shuffle. In Kilian [Kil01a], pages 368–
REFERENCES


REFERENCES

Furman:2001:CSM


Furman:2002:DCN

Fu:2001:DCA


Furuya:2002:SAK


Furnell:2005:AOW
Steven Furnell. Authentication...


[FWTC05] Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger. Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In Franklin [Fra04], pages 562–?? CO-

Fan:2004:PPI


Fan:2004:PPI

Furnell:2006:RPS


Galbraith:2001:SCC


REFERENCES


REFERENCES

&arnumber=5402536.


Goodman:2001:EER

Gordon:2008:CFS

Guerrero:2005:ECB

Gligor:2002:FEA

Gennaro:2005:SMS
REFERENCES

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

Gebotys:2004:DSC


Geier:2003:LCC


Gengler:2001:PPS


Gentry:2003:CBE


Gennaro:2000:IPR


Gennaro:2000:MTC

[Gen00b] Rosario Gennaro. Multitraptop commitments and their applications to proofs
 REFERENCES

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 10.1007/b99099. URL


Lawrence Goldstone and Nancy Bazelon Goldstone.
REFERENCES


Golomb:2005:SDG


Gambino:2008:ITW


Goldwasser:2008:CAP


Gennaro:2003:LBE


Gennaro:2005:BEG


Grothoff:2009:TBS

REFERENCES

Gilbert:2002:SCL


Gross:2004:MNh


Galindo:2008:SPK


Ghafarian:2007:IPU


Gonzales:2000:LBC

Octavio A. Gonzales, Gun-

Gilbert:2000:SAR


Gilbert:2001:SAR


Gaudry:2006:ACM


Grabner:2005:ALC


Gong:2001:GPK

[GHW01] Guang Gong, Lein Harn,

Gennaro:2001:RCV


Gennaro:2002:RSM


Gillespie:2007:WSC


Giraud:2006:RIR


Gebhardt:2005:NPV

REFERENCES

Gordon:2003:ATS

Gordon:2004:TEA

Ganapathy:2005:APA

Gentry:2001:CNS

Gallagher:2006:HSB

Gennaro:2003:SAP

NIST_05.pdf. 18 slides + 15-page paper.
REFERENCES

[0558/papers/2248/22480001.pdf]

[0558/papers/2248/22480001.pdf]

Gomulkiewicz:2002:HWA


Goldsmith:2004:CAI


Goldwasser:2005:PPK


Gavinsky:2007:ESO


Gavinsky:2009:ESO


Garay:2007:RCA

J. A. Garay, J. Katz, Chu-Yuen Koo, and R. Ostrovsky. Round complexity
REFERENCES


Gertner:2000:RBP


Guneysu:2008:CC


Gorodetsky:2005:CNS


Goubault-Larrecq:2000:MAC


Goldreich:2001:SKG

Oded Goldreich and Yehuda


Grembowski:2002:CAH


Gilbert:2000:CAR


Gallant:2001:FPM


Girault:2000:CCP


REFERENCES


[GMR05] Craig Gentry, Philip Macken-


Vanessa Gratzer and David Naccache. Cryptography, law enforcement, and mobile communications. *IEEE
REFERENCES


Gutmann:2005:WHC


Gaj:2003:FME


Goldreich:1999:MCP


Goldreich:2001:FCBb


Goldreich:2001:FCBa


Golic:2001:CAS

Jovan D. Golić. Correlation analysis of the shrinking generator. In Kilian [Kil01a], pages 440–


Goulding:2009:ESA


Geppert:2000:TMS


Gupta:2008:FAT


Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT


Guneysu:2008:SPH


Granboulan:2002:FDC

Granboulan:2002:SSR

Grigg:2001:FCL

Grossschadl:2003:ASL

Groth:2005:CS
Jens Groth. Cryptography in subgroups of $\mathbb{Z}_n^*$. In


[GS09] Markus Grassl and Rainer Steinwandt. Cryptanalysis of an authentication scheme using truncated polynomials. Information Process-
REFERENCES


REFERENCES


341

REFERENCES


Goodrich:2003:ADS


Goodrich:2008:NFI


Guttman:2004:FAP


Guar:2005:PPL


Guette:2009:ATK


Guizzo:2006:BIC


Gumz:2004:BRH


**Guillou:2001:CAP**


**Gutmann:2000:OSC**


**Gutmann:2002:CFP**


**Gutmann:2002:DVC**


**Gutmann:2004:CSA**


[HA00] Heys:2000:SAC

REFERENCES


Haddad:2000:AUA

Hancock:2000:EWP

Harvey:2000:EMA
REFERENCES


REFERENCES


[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 

Huffmire:2008:DSS 

Hartel:2001:TMS 

Holcomb:2009:PSS 
REFERENCES

Humphries:2002:IC

Huang:2004:NDE

Hwang:2004:NMP

Hernandez-Castro:2006:SGG

Han:2008:PBPa

Han:2008:PBPb
Song Han, Elizabeth Chang, and Tharam Dillon. Pairing-based public-key encryption schemes with backward-

**Henderson:2002:MTS**


**Han:2009:ICS**


**He:2002:WSM**


**Heger:2009:CTQ**


**Heijl:2001:DXS**

REFERENCES

Heiser:2003:BCB

Heikkila:2007:ESC

Hendry:2001:SCS

Henderson:2006:CBG

Henry:2006:TFA

Herzberg:2002:SX

Herranz:2006:DIB
REFERENCES

Herranz:2007:IBR


Heron:2009:AES


Herzberg:2009:DBE


Hess:2004:SVE


Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA

Horvitz:2003:WKA


Horan:2005:NRN


Howgrave-Graham:2003:IDF


Howgrave-Graham:2005:PKC


Hasenplaug:2007:FMR


Howgrave-Graham:2005:PKC

Howgrave-Graham:2003:HNP


Hendricks:2007:LOB


Handscharu:2004:SAC


Handscharu:2005:SAC

Helena Handschuh and M. Anwar Hasan, editors. Selected areas in cryptog-
Hung:2009:FBA

Hwang:2005:TSP

Hoffstein:2006:NNE

Hoffstein:2003:NDS

Hess:2004:CTT
Adam Hess, Jason Holt, Jared Jacobson, and Kent E. Seamons. Content-triggered

**Hong:2004:DCT**


**Hankerson:2000:CTC**


**Hamann:2001:SBA**


**Han:2007:FIE**

REFERENCES

Hernandez:2004:FED

Higgins:2008:NSC

Hilley:2006:SSD

Hacigumus:2002:ESE
Hakan Hacigümrüt, Bala Iyer, Chen Li, and Sharad Mehrotra. Executing SQL over encrypted data in the database-service-provider model. In Franklin et al. [FMA02], pages 216-227. ISBN ????. LCCN ????. ACM order number 475020.

Hirose:2009:SAD
**REFERENCES**

content/978-3-642-00306-6.

[Hinkelmann:2007:CUN]

[Huhnlein:2001:TPN]

[Huang:2005:ASE]

[Harris:2005:IUS]

[Kim:2000:RMW]

[Heuberger:2005:AGE]
Clemens Heuberger, Rajendra Katti, Helmut Prodinger, and Xiaoyu Ruan. The alternating greedy expansion and applications to computing digit expansions...
REFERENCES


**Handschu:2001:ASE**


**Hofmeister:2000:COS**


**Hiltgen:2006:SIB**


**Horwitz:2002:THI**


**Howard:2003:WSC**


Huang:2007:EPS


Hu:2007:DWD


Hwang:2008:CPK


Hwang:2000:CBV


Hong:2001:PSA


Han:2002:DMA

Hong Han, Xian Liang Lu, Jun Lu, Chen Bo, and Ren Li Yong. Data mining aided signature discovery in network-based intrusion detection system. *Operating...*
REFERENCES


Hwang:2003:TRB


Hwang:2004:KAS


Hwang:2005:GTS


Hong:2003:BBP


Herzog:2003:PAK


Hwang:2001:TSB

Min-Shiang Hwang, Cheng-
REFERENCES


REFERENCES

Hirt:2001:RFU


Harbitter:2002:MAP


Hevia:2002:PSG


Hitchcock:2002:NEC


Hoglund:2004:ESH


Hollar:2005:EWS

Rickland Hollar and Richard...
ard Murphy. 


**Holenstein:2004:CCB**


**Hankerson:2004:GEC**


**Huang:2007:MPK**


**Haastad:2004:SAR**


**Harnik:2006:CNI**

Hiary:2007:SSE


Haitner:2009:SHC


Hanaoka:2002:HNI


Hofinger:2001:LBE

REFERENCES


REFERENCES

Hoffstein:2001:NNL

Hoffstein:2008:IMC

Hu:2005:USA

Hawkes:2001:PCS

He:2001:SAR


Chun-Yuan Hsiao and Leonid Reyzin. Finding collisions on a public road, or do secure hash functions need secret coins? In Franklin [Fra04], pages 92–??. CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-
Holenstein:2005:OWS

Halevi:2006:TCT

Haitner:2007:SHC

He:2013:GME

Harn:2009:DDB
Lein Harn, Jian Ren, and


REFERENCES


[HS07] Ren-Junn Hwang and Sheng-Hua Shiau. Provably efficient authenticated key

He:2005:MCP


Hong:2001:KIA


Halderman:2008:LWRa


Halderman:2008:LWRb


Halderman:2009:LWR

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino,


REFERENCES

### Hong:2002:PSR


### Hong:2002:IDC


### Hess:2001:TTH


### Hernandez:2004:STN

REFERENCES

Hsu:2005:CIT


Hsu:2005:UFR


Hasan:2009:PHF


Hanaoka:2000:USD


Hanaoka:2001:EUS


Halpern:2004:RSS

Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation: extended ab-
REFERENCES


James Hughes. A linear algebraic attack on the AAFG1 braid group cryptosystem. *Lecture Notes in Computer Science*, 2384:

**Hughes:2004:ISE**


**Huhnlein:2000:EIC**


**Hunt:2005:JFE**


**Husemann:2001:SSC**


**Husemoller:2004:EC**

REFERENCES


REFERENCES


[HWH01] Neil J. Henderson, Neil M. White, and Pieter H. Hartel. iButton enrolment and verification requirements for the pressure sequence smart-card biometric. Lecture Notes in Computer Science,
Hsu:2005:NPM

Hu:2008:NPN

Hardy:2009:AAC

Hsu:2002:IGT

Hsu:2003:ITP

Hsu:2004:GOS
REFERENCES

Harkins:2005:ESU

Hsu:2003:IMA

Hirose:2001:UAS

Hwang:2003:CAL

Yeh:2008:STB

Hwang:2003:ASM
REFERENCES

HAN:2005:PJIb

HAN:2005:PJI

Huang:2005:EMP
Liusheng Huang, Hong Zhong, Hong Shen, and Yonglong Luo. An efficient multiple-precision division algorithm. In Hong Shen and Koji Nakano, editors, Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005: 5-8 December 2005, Dalian, China, pages 971–974. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7695-2405-2. LCCN QA76.58.I5752 2005. The authors present an integer-division algorithm that runs three to five times faster than Knuth’s 1981 original. However, there is an error in the renormalization algorithm that is corrected in [MN14], while retaining the speedup.

IBM-MARS-Team:2000:MAS

IEEE:2000:ASF
IEEE, editor. 41st Annual Symposium on Foundations of Computer Science: proceedings: 12-14 November, 2000, Redondo Beach, California. IEEE
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Ikawa:2000:PAF

Ikawa:2001:PAF

Impagliazzo:2003:LRA

Impagliazzo:2006:LRA
Ichikawa:2000:HEA


Ishai:2003:EOT


Ishai:2005:SCC


Ishai:2006:CA

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

**Imrey:2003:BRC**


**Inamori:2002:SPB**


**Inamori:2002:SPT**


**Inoue:2005:EST**


**Intel:2000:IIP**


**Intel:2003:IRN**

Intel Corporation. The Intel random number generator. World-Wide Web doc-
Itkis:2001:FSS


Itkis:2002:SSB


Irwin:2003:BRBb


ISO:2004:IIIb


ISO:2005:IDM

Iqbal:2008:CDV


Inoue:2008:FAC


Ishai:2003:PCS


Itoi:2000:SCI


Itoi:2001:SCS


Iwami:2008:AIA

REFERENCES


REFERENCES

lag, Berlin, Germany / Hei-
delberg, Germany / Lon-


REFERENCES


REFERENCES

[397]

Jones:2005:RDF


Johnson:2001:IHS


Jeffrey:2008:PAM


Jennings:2009:SLL


Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS

M. Eric Johnson and Eric Goetz. Embedding information security into the or-
REFERENCES

Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC


Johansson:2000:FCA


Jaulmes:2001:CPN

REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Jonsson:2002:FCA**


**Jakimoski:2001:ASR**


**Jakimoski:2001:CCB**


**Jakimovski:2002:CS**


**Jonsson:2002:SRE**


**Jonsson:2002:SRT**

REFERENCES

[102x681] REFERENCES


[Jang:2001:BWA] [JKS02]

[Jung:2001:EMO] [JKRW01]


Joux:2003:IGN


Juang:2004:FBT


Jeong:2008:PKE


Lee:2007:RKD


Juang:2001:FBT

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

**Juang:2002:VMA**


**Jakobsson:2003:FMT**


**Jakobsson:2007:DPD**

REFERENCES

Jing-mei:2005:CRB

Joux:2002:BAA

Jao:2009:EGB

Johnson:2000:AFR

Johansson:2003:FSE
REFERENCES


Johnson:2005:OSV


Jolish:2001:EDP


Joux:2002:WTP


Joux:2004:MIH

REFERENCES


Markus Jakobsson and David Pointcheval. Mutual authentication for low-


REFERENCES

Joye:2004:CHE

Joye:2001:PMA

Joye:2001:OAD

Juric:2006:CPW
Jin:2001:WCS

Jaworski:2009:RKP

Jain:2009:PQR

Jarecki:2005:FSP

Jongkook:2001:NUS

Jiang:2005:SAI
Zhengtao Jiang, Xi Sun, and Yumin Wang. Security analysis and improvement of a

**Joye:2001:PAD**


**Joye:2001:CEN**


**Joglekar:2005:PEM**


**Juang:2004:EPA**


**Juels:2004:FCI**


[Jin:2005:EAW]


[Jiang:2005:RNP]


[Joye:2001:NMM]


[Jakobsson:2004:ACN]


[Jain:2009:NBC]

REFERENCES

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


REFERENCES


[Kat01] Stefan Katzenbeisser. Recent advances in RSA cryp-

Katos:2005:RTB


Katz:2005:CBR


Kendall:1939:TRS


Kovacich:2000:HTC


Kiely:2006:SSM


Kamvar:2007:DTM

Kim:2009:DCA


Kachris:2003:RLB


Keller:2009:ECC


Keller:2009:ECC


Kim:2002:SMA

REFERENCES


[KDO01] Christopher M. King, Curtis E. Dalton, and T. Ertam Osmanoglu. Security Ar-
chitecture: Design, Deployment and Operations. 


Kovacich:2003:MHC


Kim:2005:SMA


Kato:2008:QSC


Khaw:2005:EDA


Komninos:2001:ESC


Kwon:2005:CLK

Jeoung Ok Kwon, Jung Yeon Hwang, Changwook Kim, and Dong Hoon Lee. Cryptanalysis of Lee–Kim–Yoo

Koo:2009:SVN

Khirovski:2004:DWF

Kausar:2008:SEK

Kobara:2001:NCP

Kobara:2001:SSM
REFERENCES

Kurosawa:2003:TTK

Kidwell:2007:CSB

Kilian:2001:ACC

Kiltz:2001:TBC
[Kil01b] E. Kiltz. A tool box of cryptographic functions related to the Diffie–Hellman function. Lecture Notes in Computer Science, 2247:
REFERENCES


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

Kocarev:2001:LMB


Kanade:2005:AVB


Kim:2005:IYA


Kim:2002:NIS


Klein:2003:FOW

Kawachi:2006:PQC


Kashefi:2007:SZK


Karri:2003:PBC


Khachatrian:2001:FMI

Ko:2007:SRT


Kawachi:2005:UTQ


Kim:2009:SVN


Kaliski:2002:CHE


REFERENCES

Ko:2000:NPK

Klein:2007:BDC

Kong:2001:AVW

Kiltz:2005:SCM

Kacprzak:2006:CBS
Magdalena Kacprzak, Alessio Lomuscio, Artur Niewiadomski, Wojciech Penczek, Franco Raimondi, and Maciej Szreter. Comparing BDD and SAT based techniques for model checking Chaum’s dining cryp-


REFERENCES


[KMZ03] Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng. Rethinking chosen-ciphertext security under Kerckhoff’s assumption. In Joye [Joy03b], pages 227–243. CODEN LNCS:9D. ISBN 3-540-00847-0. ISSN 0302-
REFERENCES


Knudsen:2000:TT


Knudsen:2000:TTR


Knudsen:2002:ACE


Knutson:2007:BPS


Kushilevitz:2000:OWT


Komano:2003:EUP

REFERENCES

[Katz:2004:ROS]

[Koblitz:2000:TQC]

[Kocher:2002:IS]

[Koga:2002:GFR]

[Kurosawa:2001:ICP]


[Kov03] Gerald L. Kovacich. The information systems security officer’s guide: establishing and managing

Katz:2001:EPA

com/link/service/series/0558/bibs/2045/20450475.htm; http://link.springer-n
com/link/service/series/0558/papers/2045/20450475.pdf.

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


Krause:2002:BBC


Krause:2002:USP


Krawczy:2003:SSM


Krawczyk:2005:HHP

REFERENCES


Kiltz:2005:TCL


Kissner:2005:PPS


Klivans:2006:CHL


Kurkowski:2006:QFF


Kasper:2009:FTA


Klivans:2009:CHL


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

Kumar:2002:APS


Kogan:2006:PRS


Kelsey:2000:SCC


Konstantinou:2002:SLE


Kuribayashi:2000:WSB

Minoru Kuribayashi and Hatsukazu Tanaka. A watermarking scheme based on the characteristic of addition among DCT coefficients. Lecture Notes in Computer Science, 1975:1–??, 2000. CODEN
Kobayashi:2001:NAF


Kogan:2006:IER


Ku:2003:TSA


Kobayashi:2007:AIG


Ku:2002:IIB

Ku:2004:HBS


Kuhn:2000:PCL


Kuhn:2001:CRR


Kuhn:2002:OTD


Kuhn:2008:BSS


Kukorelly:2001:PAL

REFERENCES

**Kumagai:2007:RSK**


**Kundur:2001:WDI**


**Kurosawa:2001:MRP**


**Kusters:2002:DCP**


**Kuo:2001:AOS**


**Komninos:2007:ALS**

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


Kejariwal:2009:ELL


Koshiba:2000:SEP


Knudsen:2002:IC


Karlof:2003:HMM


Keromytis:2006:COS

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


Kiyias:2001:PRB


Kiyias:2001:SPP


Jonathan Katz and Moti Yung. Scalable protocols for
REFERENCES


Kamp:2007:DEB


Laih:2003:ACA


Ladd:2006:SPS


Lafe:2000:CAT

Laird:2007:THL


Lai:2008:JIA


Lamont:1991:UFC


Lam:2001:CCN


Lambert:2007:SLG


Landau:2000:CST


Landau:2000:STT


Landau:2000:TOD

Susan Landau. Technical opinion: designing cryptography for the new century. *Communications of
Lanet:2000:ITS


Lakshminarayanan:2008:SUC


Landau:2004:SLE


Landau:2004:PNS


REFERENCES

Lindskog:2005:DIT


Lee:2000:UBN


Leveiller:2001:CNF


Leveiller:2002:CNF


Laufer:2000:SSC

REFERENCES


REFERENCES


[LCS09] 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.


Lindquist:2004:JCS


Lee:2001:AES


Lee:2003:BRBa


Lee:2004:SPM


Lee:2004:ACA

REFERENCES


[Lehtinen:2006:CSB]

[Lenstra:2001:USM]

[Leroy:2002:BVJ]

[Levy:2001:CHC]

[Levy:2002:C]

[Lewand:2000:CM]


REFERENCES


Lee:2002:TDC


Lee:2003:NKA


Lin:2003:NRU


Lee:2004:SAA


Lee:2004:ETP


Lu:2008:PTZ


Liu:2005:DBV

[LHS05] Hongmei Liu, Jiwu Huang, and Yun Q. Shi. DWT-


Lieman:2005:CRW


Lin:2000:RTI


Linn:2000:TMM


Lin:2001:HKA


Lin:2001:DWM


Lindell:2001:PCT


[LKKY03b] Lee, Sung-Woon; Kim, Woo-Hun; Kim, Hyun-Sung; Yoo, Kee-Young. Parallel simple authenticated key agreement protocol. *Operating Systems Review*, 37(3):17–22, July 2003. CODEN OSRED8. ISSN 0163-
REFERENCES


[LH01] Eonkyung Lee, Sang Jin Lee, and Sang Geun Hahn. Pseudorandomness from braid groups. In Kilian [Kil01a], pages 486–
REFERENCES

Lee:2002:RUA

Li:2004:CES

Liao:2006:PAS

Lesniewski-Laas:2005:SSS

Li:2001:SPD

Lee:2002:SEC
Hyung-Woo Lee, Sung-


Lindell:2006:CAB


Lian:2007:MDE


Lee:2005:IWR


Liu:2005:SWA

Li:2005:ATN

Lee:2006:DCK

Linares:2000:SAM
Lorenz:2002:SSG


Lavasani:2008:IFA


Li:2003:SCE


Lamenca-Martinez:2006:LNP


Leitold:2001:MTN

REFERENCES


Lepinski:2005:FZK

Laskari:2005:TTC

Lu:2005:CCA

Li:2005:BPC
Ninghui Li, John C. Mitchell, and William H. Winsborough. Beyond proof-of-

Liu:2004:MBA


Levieil:2008:CTC


Liu:2008:ARL


Lotspiech:2002:CFB


Li:2002:HNP


Loidreau:2000:SMC

Pierre Loidreau. Strength-

Lopez:2004:AAI


Lopez:2006:UPK


Lovering:2001:TKF


Lindell:2000:PPD


Lysyanskaya:2001:AST

REFERENCES


[LPW06] Kerstin Lemke, Christof Paar, and Marko Wolf, editors. Embedded security in cars: securing current and


REFERENCES

[L05b]  

[L01c]  

[LS05a]  

[L08]  

[L07]  

[L03]  
S. D. Lin, S. C. Shie, and C. F. Chen. A DCT-based

**Lin:2000:TPE**


**LSH00**


**Lin:2003:SEOA**


**LSH03a**


**Lin:2003:SEOB**


**LSKC05**

Lu:2005:BIW

Liang:2009:AIE


Lee:2001:EP1


Li:2005:ISS


Li:2005:HAO


Lie:2000:ASC


Lin:2005:RBU

hardness amplification of one-way functions. In Kilian [Kil05], pages 34–?? CODEN LNCSD9.

Lu:2002:HEA


Lu:2007:NSC


Lucks:2000:ASR


Lucks:2002:SAB

REFERENCES

[Lucks:2002:VCS]

[Lucas:2006:PGE]

[Ludvig:2005:PWF]

[Lukyanov:2001:PFA]

[Lunde:2009:BCU]

[Lutz:2002:BBS]

[Lutz:2003:BLF]
Michael J. Lutz. Book-

Lenstra:2000:XPK


Lu:2004:FCA


Laguillaumie:2007:MDV


Lange:2002:PIE


[Zude:2005:AAC] Zude Li and Xiaojun Ye. Attribute analysis of usage control (UCON). In Han

Li:2007:NBA


Lou:2002:ESA


Liu:2007:IFW


Lysyanskaya:2002:USV


Lysyanskaya:2007:A1


Lysyanskaya:2008:CHK

REFERENCES


Michener:2000:MSA


Masuda:2002:CDC


Maurer:2007:ICP


Mrayati:2003:AKT


Mrayati:2004:IAD


Mrayati:2005:IDB


Mrayati:2006:TTC


Mrayati:2007:TTC

[MAaT07] M. Mrayati, Y. Meer Alam, and M. H. at Tayyan, edi-

Mrayati:20xx:AET


Mrayati:20xx:AET


McDaniel:2006:OAI


Machado:2000:NCP


MacKenzie:2001:MEP


Mohay:2003:CIF


REFERENCES

UK£47.00. URL http://link.springer-ny.com/
link/service/series/0558/bibs/2139/21390230.htm;


Mares:2005:BRA


Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI


Martin:2008:IBE


Mastroeni:2004:APA


Matsui:2002:FSE

REFERENCES

Mathieson:2005:UCR


Maurer:2001:C


Maurer:2004:RCD


Maughan:2005:HSC


Maximov:2006:SWC


Mayers:2001:USQ


May:2002:CUR

service/series/0558/papers/2442/24420242.pdf.

May:2004:CRS


May:2009:PIS


Mel:2001:CD


Mohanthy:2008:IWB


McKinnon:2004:CCS


Montenegro:2004:CBI

REFERENCES


[McN03] Tom McNichol. How two


REFERENCES


[MFT05] David Matula, Alex Fit-Florea, and Mitchell Thornton. Table lookup structures for multiplicative inverses modulo $2^k$. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL


Håvard Molland and Tor
REFERENCES


Ma:2005:NCD


Maas:2009:SRW


Moon:2002:IDC


May:2002:SKS

Mihaljevic:2009:ASC


Micciancio:2001:ILB


Micciancio:2002:GCK


Micciancio:2002:ICH


Millet:2003:FD


Minkel:2003:CTT


Mironov:2002:RSO

REFERENCES

Mirkovic:2005:IDS


Mishra:2006:PCS


Misic:2008:TEC


Mitchell:2000:MSN


Mitra:2002:TAD


Mitrakas:2002:CCI

REFERENCES


REFERENCES

[Miaou:2001:BCW]

[MLM03]

[MM01a]

[ML001c]

[MM01b]
REFERENCES

Mana:2002:PMD

Moldovyan:2007:IC

Mullen:2007:FFA

Moreira:2002:RCE

Milenkovic:2005:UIB


REFERENCES


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


REFERENCES


Meyer:2001:FIC


Monsignori:2001:WMS


Mironov:2008:SAE


MacAndrew:2000:LPT


Mykletun:2006:AIO


Mollin:2001:IC

Richard A. Mollin. An Introduction to Cryptography. The CRC Press series
REFERENCES


Moller:2002:PEC


Moller:2003:PSP


Mollin:2003:RPK


Mollin:2005:CGS


Monniaux:2003:ACP

David Monniaux. Abstracting cryptographic protocols with tree automata.

Moore:2001:UMW


Moore:2007:CQK


Mangard:2006:PAA


Morris:2003:KKL


Moritz:2005:KAE


Moses:2006:DSD


Merton:2000:NBG

Orren Merton and Linda Dailly Paulson. News briefs: Gamers jump into broadband technology; Intel has new chip design for handhelds; patent expiration begins new encryption era; privacy organization raises privacy concerns. Computer, 33(11):16–19, Novem-


REFERENCES

bibs/2339/23390117.htm;
http://link.springer-

**Maurer:2003:SMR**


**Micciancio:2005:ASS**


**Matusiewicz:2006:FGD**


**Munilla:2007:HMF**


**Micciancio:2008:OCC**


**Mislove:2006:EBO**

REFERENCES


REFERENCES

Micciancio:2009:LBC


Monrose:2002:TSG


Mitchell:2006:PPT


Moghadam:2010:DRN


Mayer-Sommer:2001:SAS


Maggi:2002:USV

REFERENCES


Maitra:2002:CSB

Menezes:2002:PCI

Mitnick:2002:ADC

Muthukrishnan:2002:IAS
REFERENCES

Markowitch:2003:CWV


Miklau:2003:CAP


Martin:2005:PET


Meadows:2005:CPA


Mahdian:2009:UNI


Manulis:2009:SMF

Mashatan:2009:ITC


Myers:2009:BEC


Shen:2005:NIW


Marton:2010:RDC


MacKenzie:2002:TPA


McClure:2003:HEN

[MSK03] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking exposed: network security secrets and solu-

1550-4859 (print), 1550-4867 (electronic).
REFERENCES

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


REFERENCES

Muzereau:2004:EBD

Marsaglia:2002:SDP

Meseguer:2007:SRA

Ma:2009:NAS

Muller:2001:SWB

Muller:2001:SIC
REFERENCES


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:TYP


Murton:2006:CGH


Moriai:2000:PTL

Meister:2001:PPG


Morrow:2003:DIB


Micciancio:2004:CTA


Ma:2006:ADS

REFERENCES


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


[NCRX04] Peng Ning, Yun Cui, Douglas S. Reeves, and Dingbang Xu. Techniques and tools for analyzing intrusion alerts. ACM Transactions on Information and
REFERENCES


**Neuenschwander:2006:IMM**


**Neve:2003:STF**


**Nguyen:2001:TFLb**


**Nguyen:2005:RBP**


**Nordholt:2002:NFC**

Nyberg:2003:SAC


Nicholson:2001:YBC


Niederreiter:2002:BRC


Nielsen:2002:SRO

REFERENCES

Niederreiter:2004:BRC


Nikander:2002:DSAa


Nievergelt:2002:FLM


Nielsen:2002:TPF


Nievergelt:2002:FLM

Nikander:2002:DSAb


REFERENCES

URL http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf. [NM09]

[Nitaj:2009:CRCo]

[Nit09]

[NK06]

[NKO05]

[NLD08]

[NLD08]

[NMSK01]
H. Nozaki, M. Motoyama, A. Shimbo, and S. Kawamura. Implementation of RSA algorithm based on RNS Montgomery multipli-

[NM09]

[NM09]

[NM09]

[NM09]

[NM09]

[NM09]
REFERENCES

Northcutt:2002:NID


Naor:2003:CFP


Nikov:2006:RBV


Navin:2010:ETU


Naor:2001:RTS


Nichols:2007:MFD


Nakahara:2001:LCR


Naor:2004:NTC


Nichols:2000:DYD


Neraud:2001:CFD


Nguyen:2001:ISA

REFERENCES


REFERENCES

Nahum:2007:ESS

Nyberg:2001:CTC

Nenadic:2005:RBV

Olson:2003:QHK

Oechslin:2003:MFC
REFERENCES


Ohzahata:2002:FAM


Ogata:2006:OSS


Olson:2000:SCT


Ohigashi:2009:PMF


Ohkuma:2001:BCH


Ohbuchi:2002:FDA

Ryutarou Ohbuchi, Akio Mukaiyama, and Shigeo Takahashi. A frequency-domain approach to water-

[Oni01]


[ÖOP03]


[OP01a]


[OP01b]


[Opp01]

REFERENCES


Oppliger:2005:CC

Rolf Oppliger. Contempo-
rary cryptography. Artech
House computer security
series. Artech House Inc.,
Norwood, MA, USA, 2005.
ISBN 1-58053-642-5. xxv +
503 pp. LCCN Z103 .O66
artechhouse.com/Detail.
asp?strIsbn=978-1-58053-
642-4. [Opp05]

Ortiz:2000:ITW

Sixto Ortiz Jr. Industry
trends: Will PKI become
a key to online security?
Computer, 33(12):
CODEN CPTRB4. ISSN 0018-
9162 (print), 1558-0814
(electronic). URL http://dlib.computer.org/co/
books/co2000/pdf/rz013.
pdf. [Ort00]

Okeya:2001:EEC

K. Okeya and K. Sakurai. Efficient elliptic curve cryp-
tosystems from a scalar mul-
tiplication algorithm with
recovery of the y-coordinate
on a Montgomery-form el-
lipic curve. Lecture Notes
in Computer Science, 2162:
126–??, 2001. CODEN
LNCSD9. ISSN 0302-
9743 (print), 1611-3349
link/service/series/0558/
bibs/2162/21620126.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2162/21620126.
pdf. [OS00]

Ostabovsky:2005:PSS

Rafail Ostrovsky and Wil-
liam E. Skeith III. Pri-
uate searching on streaming
data. In Shoup [Sho05a],
pages 223–?? 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. [OS06]

Oren:2006:PAR

Yossi Oren and Adi Shamir.

[OSSST04] Obimbo:2007:PAD

[OS07] Oury:2008:PP

[OST05] Osvik:2005:CAC

[OST06] Osvik:2006:CAC
Dag Arne Osvik, Adi Shamir, and Eran Tromer.

Osvik:2000:SS


Okeya:2003:MFC


Okeya:2003:WNM


Okada:2001:IEC

Okamoto:2000:QPK


Ouellette:2005:PPM


Page:2003:BRW


Overbeck:2006:EGA

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

Palmer:2002:TMQ


Panditaratne:2007:TRN


Papanikolaou:2005:BRBa


Pass:2005:UCN

Rafael Pass and abhi shelat. Unconditional characterizations of non-interactive zero-knowledge. In Shoup [Sho05a], pages 118–?? ISBN 3-540-
REFERENCES


Patterson:2001:DFI


Patiyoot:2002:SIW


Patiyoot:2002:MSE


Patarin:2003:LRR


Paterson:2003:CCI


Paulson:2001:RBS


Paulson:2002:NBPb


Paulson:2003:NBV


**Paulson:2009:NBT**


**Praca:2001:SCS**


**Piva:2002:MCW**


**Piva:2005:SRA**


**Park:2000:CAP**


**Peng:2005:SES**

Kun Peng, Colin Boyd, and Ed Dawson. Simple and ef-
 REFERENCES


REFERENCES

Pucheral:2001:PSD


Petrie:2000:NBI


Peikari:2004:SW


Park:2005:ISC


Park:2005:NDS

Perlnr:2009:QRP


Park:2003:ESA


Patarin:2001:QBL


Park:2002:XQP


Park:2003:EMS


Pan:2007:IBS

Peeters:2007:CES


Petrakos:2009:CTA


Peinado:2004:CLK


Peikert:2009:PKC


Pelzl:2006:PAC


Pemble:2001:CEW


Pemble:2001:SPA


Perrine:2003:ECP

Tom Perrine. The end of crypt() passwords …


Phatak:2005:FMR


Power:2007:SBB


Phan:2006:CTP


Philpott:2006:ITD

REFERENCES


[Pipe05] Krzysztof Pietrzak. Composition does not imply adaptive security. In Shoup [Sho05a], pages
REFERENCES

Pinkas:2002:CTP


Pinkas:2003:CTP


To be published in SIGKDD Explorations, Volume 4, Issue 2.

Pincock:2006:CHC


Piper:2003:RCS


Park:2001:NDW

REFERENCES

Park:2001:RFW


Poh:2001:HBP

[PK01]


REFERENCES

Pfleeger:2007:IBC

Paulson:2000:NBU

Piper:2002:CVS

Pang:2008:AQR

Peyravian:2000:MBB

Pohlmann:2001:SCA
Pointcheval:2000:CCS


Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP


Pornin:2001:THE


Porras:2006:PEG

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


Pfleeger:2007:SC


Paar:2009:UCT


Pellikaan:1996:AGC


Pereira:2003:SAU


Piret:2003:DFA


Pereira:2006:IBS

Olivier Pereira and Jean-Jacques Quisquater. On the impossibility of building secure Cliques-type authenticated group key agree-
Picard:2001:NNF


Pass:2005:NIC


Pass:2008:NIC


Preneel:2000:ACE


Preneel:2001:NES

REFERENCES

Preneel:2002:NEA


Preneel:2002:NPT


Preneel:2002:TCC


Preneel:2007:SRD


Price:2000:NCH

REFERENCES


REFERENCES


REFERENCES

Prabhakaran:2005:RES


Phan:2006:FDB


Park:2008:SRB


Pavlo:2008:FAD


Park:2002:SRL


Pareschi:2009:PAC

REFERENCES


Pucella:2006:SCC


Pucella:2007:Ib


Puzmanova:2004:RWF


Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI


Pang:2005:NMS


**Peikert:2008:LTF**


**Pelzl:2003:HCC**


**Patrick:2005:FCD**


**Paterson:2006:LTT**


**Palanivel:2008:MPA**

S. Palanivel and B. Yegnanarayana. Multimodal person authentication using speech, face and visual speech. *Computer Vi-
REFERENCES

Pieprzyk:2001:CPS


Pieprzyk:2002:CPL


Pieprzyk:2002:CCI


Pecho:2009:APW


Peng:2009:DIE


**Qu:2001:KPW**


**Raikhel:2000:DF**


**Rajsbaum:2006:ASNb**


**Roman:2007:SCP**


**Ramesh:2001:TAE**


**Rand:1955:MRD**

Rand Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Free Press, Glencoe, IL,


Rubin:2006:CSE


Reed:2000:ANA


Rubin:2005:ARS


Rangan:2001:PCI


Renaud:2009:VPC


Rudra:2001:ERE

REFERENCES


(print), 1939-9340 (electronic).


[RGX06] Gregory Gordon Rose, Alexander Gantman, and
REFERENCES


Rila:2002:DAB


Risen:2006:SWS


Rivest:2003:TLE


Renner:2005:UCP


Ruan:2006:NSC


Reddy:2002:AM

REFERENCES


Reyhani-Masoleh:2004:TFT


Rahaman:2008:CTB


Ryabko:2005:NTA


Ryutov:2000:RESa


Ryutov:2000:RESb


Robinson:2002:LLE


Rothe:2007:BRB


Roy:2000:PCI


Roychowdhury:2000:PCJ


Rieffel:2000:IQC


Ramzan:2000:RSS

[RR00] Zulfikar Ramzan and Leonid Reyzin. On the round security of symmetric-key
REFERENCES

595

cryptographic primitives.
In Bellare [Bel00], pages 376–?? ISBN 3-540-67907-3. ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
link/service/series/0558/bibs/1880/18800376.htm;
pdf.

Reyzin:2002:BTB

[RR02]
Leonid Reyzin and Natan Reyzin. Better than BiBa:
Short one-time signatures with fast signing and
verifying. Lecture Notes in Computer Science, 2834:
144–??, 2002. CODEN LNCSD9. ISSN 0302-
link/service/series/0558/bibs/2384/23840144.htm;
pdf.

Ratner:2003:NHS

[RR03b]
Daniel Ratner and Mark Ratner. Nanotechnology and
Prentice-Hall PTR, Upper Saddle River, NJ 07458,

Rosenberg:2004:SWS

[RR03a]
Jonathan B. Rosenberg and David L. Remy. Securing
Web services with WS-Security: demystifying
WS-Security, WS-Policy, SAML, XML Signature, and
XML Encryption. SAMS Publishing, Indianapolis,

Rittinghouse:2005:IIM

[RR05]
John Rittinghouse and James Ransome. IM In-
stant Messaging Security.
1-55558-338-5. 432 (est.) pp. LCCN ???? URL

Rechberger:2008:NRN

[RR03a]
C. Rechberger and V. Rijmen. New results on
NMAC/HMAC when instantiated with popular


REFERENCES


[Rubin:2008:CFF] K. Rubin and A. Silverberg. Compression in finite fields and torus-based cryp-
REFERENCES

RSA:2000:PKC


RSA:2000:PVCa


RSA:2000:PCP


RSA:2000:PVCb


RSA:2000:PVS


RSA:2001:PVC


RSA:2002:PVR


Rivest:2003:TAL

REFERENCES


**Rogers:2005:MPH**


**Rouvroy:2003:EUF**


**Rivest:2001:HLS**


**Rubin:2000:KVL**

REFERENCES

Rugg:2004:CMV


Rupp:2009:CAC


Raghavan:2009:SPC


Russell:2002:HFU


Renner:2003:NBS


Renner:2003:UAP

Ramaswamy:2007:HSP


Schmalz:2003:MDI


Saini:2002:JMD


Saeednia:2002:IBS


Sakamura:2001:GEI

org/ml/books/mi2001/pdf/m6004.pdf.

**Sale:2000:CGL**


**Sale:2000:CBP**


**Sale:2001:GRT**


**Salus:2001:CA**


**Salomon:2003:DPS**


**Salus:2003:BRBb**


**Sale:2005:RCB**

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


Samtani:2009:WTO


Santini:2005:WSI


Sar02


Sasse:2007:REB


Satoh:2006:DPI


Savelli:2004:NDC


Savage:2005:IPWa


Sherwood:2005:MTR


Steiner:2001:SPB


Smeraldi:2002:SVF


Shehab:2005:SCM


Shehab:2007:WSD


Shaikh:2009:SAU


Steinfeld:2002:ASA

Ron Steinfeld, Joonsang Baek, and Yuilang Zheng. On the necessity of strong assumptions for the security

**Seredynski:2004:CAC**


**Syverson:2001:LAP**


**Stoll:2002:MMC**


**Sun:2002:WDC**

Shao:2005:NEV


Stephanides:2005:GAK


Sun:2005:IPK


Siegelin:2001:SCD


Schmalz:2000:MAD


Schneier:2000:AAR

REFERENCES


Schneier:2000:IRS


Schneier:2000:SLD


Schneier:2000:SRF


Scharinger:2001:ASK


Schindler:2001:TAA


Schmalz:2001:MDI

Mark S. Schmalz, editor. Mathematics of data/image coding, compression, and encryption IV, with

Schnorr:2001:SGH


Schnorr:2001:SDE


Schultz:2002:GBC


Schneier:2003:BFT

REFERENCES


Schneier:2005:AE


Schneier:2005:TFA


Schramm:2006:AMS


Schroeder:2006:NTS


Schneier:2007:NCS


Schneier:2008:SS


Schmeh:2009:VBF


Sebe:2000:SDI


Smith:2001:ADB


Spiekermann:2009:ACR


Seacord:2005:SCC

REFERENCES

Seacord:2009:CCS


Seetharaman:2004:BRB


Smith:2006:SID


Seifried:2000:C


Seifried:2000:PPA


Seifert:2005:ACR


Speed:2001:PIS


[Sen03] Charles A. Sennewald. Effective security man-


Simka:2006:MTR


Sakr:2007:RCB


Sutton:2007:FBF


Steinwandt:2001:TDB


Steinwandt:2000:WHS


Seyedzadeh:2011:IEA


Shailer:2001:PMT


Shamir:2001:NDC


Shao:2001:BVM


Sharp:2001:IKB

Toby Sharp. An implementation of key-based digital signal steganography. Lect-
REFERENCES


Shapiro:2002:CCM


Shamir:2003:RS


Shamir:2003:TLC


Shao:2003:CIB


Shao:2003:PSS


Shaltiel:2004:RDE

Shao:2004:IDS


Shao:2005:CXY


Shao:2005:IEP


Shao:2005:NKA


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:CIN


Shparlinski:1999:NTM

Shparlinski:2001:UDR

Shparlinski:2002:SMS

Shparlinski:2003:CAA
Igor E. Shparlinski. *Cryp-

Shparlinski:2004:UDD
Igor E. Shparlinski. On the uniformity of distribution of the decryption exponent

**Shparlinski:2005:PHS**


**Sil01**


**Shyamasundar:2002:ACP**


**Shumba:2006:THL**

REFERENCES

openurl.asp?genre=issue&
issn=0302-9743&volume=
2146.

Silverman:2005:ECC


Simon:2002:CRE

www.lms.ac.uk/jcm/5/lms2000-006/.

Simon:1999:CBE

[AAG+00].

Simon:2000:CBE

Simon Singh. The code book: the evolution of secrecy from Ancient Egypt to quantum cryptography. Anchor

Simon: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


Sklavos:2005:ISH

REFERENCES


Skolnikoff:2003:SS


Schindler:2001:IDC


Srinathan:2002:ASC


Sugita:2000:RAD

REFERENCES


[SL05b] Mudhakar Srivatsa and Ling Liu. Securing publish-subscribe overlay services with EventGuard. In Meadows and Syverson [MS05b],
REFERENCES


REFERENCES


[Sarkar:2000:NBC] Palash Sarkar and Subhamoy Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In Bellare [Bel00],
Sebag-Montefiore:2000:EBC


Sarkar:2001:EIL


Satoh:2002:SHS


Sarkar:2003:EIC


Satoh:2003:UHA

Akashi Satoh and Sumio Morioka. Unified hardware architecture for 128-bit block ciphers AES and Camellia. In Walter

Sebag-Montefiore:2005:EBC


Sebag-Montefiore:2007:EBC


Simos:2007:CMS


Smith-Miles:2008:CDP


Seyedzadeh:2011:IES


REFERENCES

Smith:2000:ABS


Smith:2001:IK


Smith:2001:ECB


Smith:2001:APP


Smith:2002:OAP


Smith:2003:FTT


Smith:2008:CFI


Smolin:2004:EDE

[Smo04] J. A. Smolin. The early days of experimental quantum cryptography. IBM
REFERENCES


Seamons:2009:IPS


Satoh:2001:CRH


Strembeck:2004:IAE


Schlager:2007:EAA


Sakai:2000:NDS

REFERENCES


Slind:2007:PPS


Song:2000:ISC


Shigetomi:2002:ALS


Satoh:2000:HSM


Smith:1979:UFM

Donald R. Smith and James T. Palmer. Universal fixed messages and the


REFERENCES


[Sti95, Sti02, Sti06c]

**Sanchez-Reillo:2001:IBA**


**StDenis:2006:BMI**


**Stipcevic:2007:QRN**


**Samarati:2001:AMP**


**Standaert:2003:EIR**


**Sarkar:2001:PAE**

P. Sarkar and P. J. Schel-
REFERENCES


Stubblebine:2001:AAF


SSFC09

Seznec:2003:HUL


Swiderski:2004:TM


Seddik:2009:IWB


Shi:2008:UAU

REFERENCES


REFERENCES


Stern:2001:ADW

Stinson:2001:SAC
[ST01d]

Sakurai:2002:SMP

Satoh:2003:SDF

Shamir:2003:FLN
Adi Shamir and Eran Tromer. Factoring large numbers with the TWIRL device. In Boneh [Bon03],


REFERENCES


[Ste08]

[Sti05]

[Stieber:2006:OH]

[Stieber:2006:GH]

[Sti01]

[Stinson:2002:CTP]

[Stinson:1995:CTP]
Stipcevic:2011:QRN


Shimoyama:2002:MLC


Strunk:2001:JQJ


Strubinger:2002:HBS

REFERENCES

38, April 2002. CODEN SYADE7. ISSN 1061-2688.


REFERENCES


[SW05a] Kyungah Shim and Sungsik Woo. Weakness in ID-based one round authenticated tripartite multiple-key agree-


**Stuck:2005:HVC**


**Shieh:2006:ERM**


**Swaine:2001:PPSa**


**Swenson:2008:MCT**


**Song:2005:ISG**


**Sun:2009:TDS**

REFERENCES

**Swire:2005:SMI**


**Stevenson:2005:SCI**


**Song:2007:TAK**


**Shujun:2001:PRB**


**Seo:2001:CDA**


**Shi:2001:NSF**

REFERENCES


REFERENCES


Steinfeld:2001:ALE


Skoudis:2003:MFM


Sarikaya:2008:SPT


Sun:2002:NAD


Sun:2005:WIW


Tada:2002:OSM

REFERENCES


REFERENCES


[Tao:2000:ITF]

[T00]


[Tsai:2001:GSI]

[TC03]

[Tsaur:2005:EAS]

[T05]


[Trudel:2003:DSE]


[Teepe:2006:PPA]

REFERENCES


Todd:2001:LSS


Terai:2008:BRB


Thorsteinson:2004:NSC


Theoharidou:2007:CBK


Tirkel:2001:UWE


Thimbleby:2003:RE

Tabatabaian:2001:NSP


Tippett:1927:RSN


Torres:2007:ANS


Tseng:2001:GGO


Tseng:2001:CLB


Tseng:2003:DSM


Tico:2003:RAS

Marius Tico and Pauli Kusosmanen. A remote authentication system using finger-prints. *International Jour-
REFERENCES


[Toll:2008:CSE]

[Thien:2002:TSS]

[Thomas:2007:HQU]

[Turner:2006:SIS]

[Tsai:2005:CAE]

[Tan:2004:OBC]
Zhangxi Tan, Chuang Lin, Hao Yin, and Bo Li. Optimization and benchmark of cryptographic algorithms on network processors. IEEE Micro, 24(5):55–69, September/October 2004. CO-


REFERENCES


Tsaur:2005:SSS


Tsaban:2006:FGD


Tsang:2007:WCT


Tsai:2008:EMS


Tseng:2007:SAG


Takano:2000:PTH

Kohji Takano, Akashi Satoh, and Nobuyuki Oiba. Poster 5: TATSU — hardware accelerator for public-key cryptography using Mont-
REFERENCES

[Ano00d] A. Montgomery. In Anonymous [Ano00d], page ??.


Text prepared by Ralph Erskine and Philip Marks and Frode Weierud from the only two surviving copies of Turing’s typescript.

Tiri:2003:SEA


Trappe:2002:ICC


Trappe:2005:ICC


Talbot:2006:CCI


Toft:2001:LTT


REFERENCES


REFERENCES


USENIX:2000:PFSa


USENIX:2000:PNU


USENIX:2001:PUA


USENIX:2001:PFT


USENIX:2001:PTU


USENIX:2002:PBF


USENIX:2002:PUS

[USE02b] USENIX, editor. *Proceed-
REFERENCES


[Lars00] Lars Ulfving and Frode Weierud. The Geheimschreiber secret. In Joyner
REFERENCES


REFERENCES


D. D. Vavriv. Random number generators on the basis of systems with chaotic behavior. AIP
REFERENCES


REFERENCES


REFERENCES


[VM03] John Viega and Matt Messier. Secure programming cookbook for C and C++: Recipes for cryptography, authentication, networking, input validation and more. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707...
REFERENCES


vanOorschot:2007:IRS
P. C. van Oorschot, Tao Wan, and Evangelos Kranakis.
On interdomain routing security and pretty secure BGP (psBGP).
CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Vogt:2001:USC
Using smart cards for fair exchange.
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vasco:2001:CPK
María Isabel González Vasco and Rainer Steinwandt.
Clouds over a public key cryptosystem based on Lyndon words.
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).
URL http://www.elsevier.com/gej-ng/10/23/20/84/36/30/abstract.html.

Voyiatzis:2008:SFS
Artemios G. Voyiatzis and Dimitrios N. Serpanos.
The security of the Fiat–Shamir scheme in the presence of transient hardware faults.
CODEN ????. ISSN 1539-9087 (print), 1558-3465 (electronic).

vanTilborg:2000:FCP
Henk C. A. van Tilborg.
Fundamentals of cryptography: a professional reference and interactive tutorial,
volume SECS 528 of The Kluwer international series in engineering and computer science.

vanTilborg:2001:ECC
Henk van Tilborg.
Elliptic curve cryptosystems; too good to be true?
ISSN 0028-9825.
REFERENCES


REFERENCES


Wagner:2002:GBP


Wagstaff:2003:CNT


Walsh:2000:BRM


Walter:2001:PBM


Walter:2003:STM

[Wal03] Colin D. Walter. Seeing through MIST given a small fraction of an RSA pri-

Wallich:2004:EEI


Wallich:2009:SGP


Wallich:2004:AWE


Wang:2004:TVS


Wang:2005:SCR


Wardlaw:2000:RPK


Washington:2008:BRB

of Elliptic and Hyperelliptic Curve Cryptography, by
H. Cohen and G. Frey, Chapman & Hall/CRC,
22, March 2008. CODEN SIGNDM. ISSN 0163-
5700 (print), 1943-5827 (electronic). URL http:
//doi.acm.org/10.1145/1360443.1360448. See [CFA+06].

Washington:2008:ECN

Lawrence C. Washington. Elliptic curves: number the-
ory and cryptography. Discrete mathematics and its
applications. Chapman and Hall/CRC, Boca Raton, FL,
USA, second edition, 2008. ISBN 1-4200-7146-7 (hard-
cover). xviii + 513 pp. LCCN QA567.2.E44 W37
2008.

Wayman:2001:FBA

J. L. Wayman. Fundamentals of biometric authenti-
cation technologies. International Journal of Image
and Graphics (IJIG), 1(1):93–97, January 2001. CO-
DEN ????? ISSN 0219-4678.

Wayman:2002:BAT

James L. Wayman. Biometric authentication tech-
nologies: Hype meets the test results, 2002. URL
http://www.usenix.org/publications/library/proceedings/
sec02/tech.html. Unpublished.

Wayner:2002:DCI

Peter Wayner. Disappearing cryptography: informa-
tion hiding: steganography & watermarking. Morgan
Kaufmann Publishers, Los Altos, CA 94022, USA, sec-

Wayner:2009:DCI

Peter Wayner. Disappearing cryptography: informa-
tion hiding: steganography and watermarking.
Morgan Kaufmann Publishers, Los Altos, CA 94022,
USA, third edition, 2009. ISBN 0-12-374479-2, 0-08-
092270-8 (e-book). xv + 439 pp. LCCN TK5105.59
science/book/9780123744791.

Weiss:2000:CAC

Richard Weiss and Nathan Binkert. A compari-
sion of AES candidates on the Alpha 21264. In
NIST [NIS00], pages 75–81. ISBN ????. LCCN ???.
URL http://csrc.nist.gov/encryption/aes/round2/
conf3/aes3conf.htm; http://csrc.nist.gov/encryption/
aes/round2/conf3/papers/AES3Proceedings-1.pdf;
REFERENCES


[WBL01] Wu:2002:CSCa


[WBRF00] Wu:2001:CDS


Weis:2001:SYH


Weeks:2000:HPS


REFERENCES


Wang:2005:TAP


Wang:2009:NWA


Wang:2005:SDR


Westerlund:2001:HWK


Williams:2001:ICA


Weir:2009:UPS


Weaver:2006:BA


Weber:2002:ECH


Webb:2008:IZN


Wehde:2000:IME


Weierud:2000:BSF


Weiss:2004:JCE


Weierud:2005:BSF

Frode Weierud. BP’s sturgeon, the FISH that laid no eggs. In Copeland [Cop05],
REFERENCES

Weierud:2005:BPS


Welschenbach:2005:CCC


Weng:2003:CHC


**Wu:2002:LCN**


**WFLY04**


**Wang:2004:CHF**

**Wang:2002:CSE**


**Wang:2005:RST**


**Wong:2000:SGC**


**Wu:2002:CAE**


**Wu:2002:IBM**

REFERENCES


REFERENCES


I. In Garrett and Lie-
REFERENCES

[Win05a]

[Wil06]

[Win00]

[Win01]

[Win05b]

[Win05c]
REFERENCES


Withers:2001:IWU


Wang:2007:VBW


Welschenbach:2001:CCC


Wang:2005:ECSb


Won:2006:ISC


Weigold:2008:RCA

REFERENCES

Walter:2003:CHE


Wedde:2004:MAA


Wang:2002:AAB


Wu:2004:RKA


Wang:2005:CHY


Wang:2007:NCD

Zhenghong Wang and Ruby B. Lee. New cache designs for thwarting software cache-based side channel attacks.
REFERENCES


REFERENCES

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

Wu:2005:IAW

Wong:2004:RCK

Wang:2005:TSP

Wu:2008:RWM

Watters:2008:VDL

Wheeler:1995:TTE

Watanabe:2002:CCD
Yuji Watanabe and Masayuki Numao. Conditional cryptographic delegation for P2P data sharing. Lecture Notes in Computer Science,
REFERENCES

Wang:2008:NAD

Wang:2009:RDA

Wolkerstorfer:2001:AIA

Wolke:2003:EE

Wollinger:2004:SHI

Won:2001:ISC
Dongho Won, editor. Information security and cryptography: ICISC 2000, Third

Wool:2000:KME

Wool:2005:KME

Wollinger:2005:CVH

Wollinger:2005:CVH

Weimerskirch:2001:ECC
[WPS01] André Weimerskirch, Christof Paar, and Sheueling Chang Shantz. Elliptic curve cryptography on a palm OS
REFERENCES

Wang:2001:TUR

Wright:2000:IQC

Wright:2001:AES

Wright:2003:FCI

Wrixon:2005:CCO
Fred B. Wrixon. Codes, Ciphers and Other Cryptic

Wang:2002:IPD


Wright:2002:EPS


Whiting:2003:MPH


Walter:2005:DDP


Weimerskirch:2002:DLW


Wu:2001:DSM


Wu:2002:CSCb


Wuensche:2009:CAE


Wu:2000:PKC


Wu:2001:FED


Woodruff:2002:CUC

Weaver:2000:CAC

Wang:2004:CWS

Wang:2006:SPS

Wolf:2005:NML

Wang:2008:DCP
REFERENCES


[WWGP00] Thomas J. Wollinger, Min Wang, Jorge Guajardo, and Christof Paar. How well are high-end DSPs suited for the AES algorithms? AES algorithms on the TMS320C6x DSP. In NIST [NIS00], pages 94–105. ISBN ???? LCCN ???? URL


**Xu:2005:ADR**


**Xie:2007:ISP**


**Xu:2003:TEP**


**Xin:2010:IEB**


**Xiang:2008:CPA**

REFERENCES


Xie:2004:CTA


Xu:2009:AVB


Xing-Yuan:2011:PRS


Yan:2000:NTC


Yang:2002:NEC


Yang:2005:TFN


Yan:2007:CAR


Yasuda:2008:DLP

Masaya Yasuda. The discrete logarithm problem on elliptic curves defined over Q (abstract only). ACM

Yuan-bo:2004:ITA


Yue:2001:GNN


Yue:2007:SEV


Yiu:2008:ODC


Yang:2009:ETP


Yang:2009:IBR

Jen-Ho Yang and Chin-Chen Chang. An ID-based remote mutual au-
REFERENCES


Yang:2009:CGA

Yang:2004:MSS

Yang:2007:IIS

Yu:2007:NSM


Yang:2008:NFD

Yang:2007:IIS

Yung:2006:PKC
Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors. *Public Key Cryptography: PPK 2006: 9th International Conference on Theory and Practice in Public-Key Crypt-
REFERENCES


Yang:2005:IME


Yamamura:2000:QCB


Yamamura:2001:EDA


Yi:2004:AKA


Yen:2000:CBO


Yen:2002:CAO

Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon. A countermeasure against one physical cryptanalysis may benefit another attack. *Lecture
REFERENCES


[YKW01] Heather Yu, Xiangyang Kong, and Wayne Wolf.


Youssef:2001:CAF


Young:2004:HRV


Young:2006:MCC


Youn:2008:WRB


Yang:2009:AIO


Yin:2001:RMW

Yilek:2009:WPK


Yoon:2004:SUA


Yoon:2005:ICJ


Yoon:2005:IFA


Yoon:2005:CFI


Yoon:2005:IHL


REFERENCES


Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng
References


[YYDO01] Dingfeng Ye, Junhui Yang, Zongduo Dai, and Haiwen Ou. Attacks on two digital signature schemes based on

**You:2001:GEC**


**Yen:2000:WOW**


**Ye:2007:NAW**


**Youssef:2009:IEU**


**Zafar:2000:ACB**

REFERENCES


Zane:2001:EWD


Zan01

[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 ????.

Zhang:2005:ITA


ZAX05


Zivkovic:2005:AAH


ZBLvB05


Zivkovic:2005:AAH


Zhang:2004:AIB
Zhang:2005:CHC


Zhang:2009:CII


Zhang:2001:SOS


Zhou:2005:PSP


Zhu:2004:DSM


Zunino:2005:WPE


Zhao:2006:SAP

Zhu Zhao, Zhongqi Dong, and Yongge Wang. Secu-


REFERENCES

Zhao:2006:NDN


Zhao:2008:CLR


Zheng:2001:ISS


Zheng:2002:NPK


Zheng:2002:ACA

Zhou:2002:MVD


Zho02

Zhong:2006:ESC


Zho06

Zirkind:2007:ADC


Zir07

Zhang:2004:BAF


ZJ04

Zhang:2009:IBR


ZJ09


Zhang:2001:CIS


Zhang:2005:DMC


Zhou:2005:MBI


Zhu:2007:IHH


Zhang:2005:RPE


Zhao:2005:APA


Zhou:2005:APS

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

[Zhang:2001:ASE]


[Zhang:2003:FSP]


[Zafeiriou:2005:BRW]


[Zhang:2005:ISS]


Zhang:2005:ASP


Zhang:2005:ISM


Zhang:2008:FIC


Zeng:2001:CHR


Zhu:2007:EIB

Robert W. Zhu, Guomin Yang, and Duncan S. Wong. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices. Theoretical Computer Science, 378
Zhuang:2005:KAE