Title word cross-reference

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

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (pk)

{[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LKL01, YCH04, CLT07]. (tn)

[PPW05, SC05a]. + [Abe01]. {0, 1}

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

[And04]. 128 [AIK01, PCG01]. 13

[HSL02]. $15.00 [Imr03]. 2

[Bih00, BGN05, CY02, CKL03, DNP07, Gau02, GHK06, GIKR02, HKA05, KLR09, SC02b, Ver02, Wen03]. 2000 [Eva09]. 2000 ± 10 [Mau01]. 2^{28} [Bih02]. 2^e

[MFFT05]. 2^m [KLY02, KKY02]. 3

[BP04, Ben00, ChLYL09, CT09, Lav09, OMT02, WH09, ZTP05]. $35.00 [Top02].

$49.99 [Gumb04]. $5 [SCF01]. 5 [Pat04].

$51.48 [Pap05]. 512 [CDL00]. 7

[Griv01, Pat03a]. (2, 128) [WB02]. 0 [AIK04].

[ABC] [PS04b]. d [BD00b]. E_0 [FL01a]. f 8

[KSHY01]. g^{2^e} [Sht02]. g(x, 1) [SZP02].

GF(2) [CP03]. GF(2^m) [OTIT01, RMPJ08].

GF(p^m) [BGK03]. GF(p^t) [Z01]. H_2 A

[CBJLS05]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WLL02]. l [QP02]. M + 1

[AS01a]. F_q [CY02]. Z^n [Gro05]. GF(2)

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

[BBGM08, KTT07, KWP06, RMH03a, RS04].

GF(2^m) [KKH03]. SL_2(F_{2^m}) [SGBB00]. μ

[LCN04]. n

[CT08b, Gon06, HKS00, LKJL01, TM01].
N^0.292 [BD00b]. NC^0 [AIK06]. p [FL06]. p^q^s^t [LKY00]. p^s^t [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]. -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 [DJLT01].

0 [And04, BC04a, Gum04, Imr03, Puz04, WYY05d]. 0-07-222742-7 [Gum04]. 0-13-100851-X [For04]. 0-226-74410-8 [Top02]. 0-262-14075-6 [Pag03]. 0-321-20217-1 [Puz04]. 0-385-49532-3 [Imr03]. 0-470-84402-7 [And04]. 024-Bit [GS07a]. '05 [ACM05c, MS05b, ZC09]. '07 [ACM07]. '08 [ACM08]. '09 [ACM09, IEE09a].

1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05b, WYY05c, Was08a]. 1-58488-518-1 [Was08a]. 1-Connected [BJLS02]. 1-out-of-n [AOS02]. 1.82Gbits [KV01]. 1.82Gbits/sec [KV01]. 101 [Sei00a]. 10118-3 [ISO04]. 106 [Uni00c, Uni00d, Uni00g]. 106-1 [Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a]. 109-bit [Pri00]. 10th [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. 11-15 [AUW01]. 11th [CCMR05, HYZ05b, HH04, HH05, 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].

19005-1 [ISO05]. 192-bit [Luc00]. 1930s [AUW01]. 19th [BCDH09]. 1V [CGBS01]. 2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH+00b, Eke02, Irw03, KH08, KI01a, Sch00b, Wit01, YG01c]. 2001 [ACM01a, BC01, GJSS01, Lee03a, Pem01b]. 2002 [B+02, IEE02, RSA03a, Yun02a]. 2003 [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, 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, Kii01a]. 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, Irw03]. 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 [Dwu03], 4-round [DLP+09], 40th [ACM08], 41st [IEEE00a], 42nd [IEEE01a]. 43rd [IEEE02], 44th [IEEE03], 45th [IEEE04]. 46th [IEEE05a], 47th [IEEE06], 48th [IEEE07]. 49th [IEEE08], 4th [BCKK05, BC05c, DWML05, DRS05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, KN03, MS05a, NP02a]. 5 [Duw03, Wac05]. 50th [IEEE09b]. 512 [AD07, GLG+02]. 5th [CV04, KJR05, LL03, LLT+04, Li05, NP02a, Syv02, WKP03].

64 [LKH+08, WWCW00]. 6th [Bla03, Des02, HA00, 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 [SIR04]. 802.11i [HSD+05]. 802.15.4 [Mis08]. 82 [Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02, SMP+09, Vy01, Vau05a, WK06, Zhe02b].

9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04]. 90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1 [GM00b]. 98 [Wil99]. 99 [DN00b]. 9th [CCMR02, CSY09, DR02c, DKU05, Lai03, NH03, Pat03b, PY05, YDKM06].

= [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05a, Kel05b]. A5 [BD00a, BSW01, PS01c]. A5/1 [BD00a, BSW01, PS01c]. AA1 [AML04]. Aarhus [Cra05a]. Abadi [MW04]. Abelian [CF02, PHK+01, RS02]. Abstention [JLL02]. Abstract [CM00, Cou04, DRR05, HLYA02, HJW01, JL00, MSJ02, MP02, Mas04, Wag02, BJN00, BCDM00, CD00a, CC04c, FKS+00, GHJ00, GT04, HT04, HP01, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Pei09, Yas08]. Abstracting [Bla01a, Mon03]. abstraction [BLP06]. abstractions [BG07b]. Abstracts [Sch00b]. Accelerated [Elb08]. Accelerating [ESG+05]. acceleration [EHKH04]. Accelerator [CBG01, RS04, TS00, X01, DPT+02]. Acceptance [CFRR02]. Access [ANRS01, Ano02e, BNPW03, CGMM02, DS06, HC08, MS03b, Ri02, Sma03a, Sun00a, ZGLX05, AW05, AW08, AFB05, BA06, BNP08, Che08b, DFM04, Hos08b, HW03c, HY03, IY06, JW06, KNS05, LKZ+04, MF07, MSP+08, PS02a, ST07, WL05, WC01b, You04]. access-control [BNP08]. accessible [Pau02a]. accountability [WABL+08]. Accounting [Lai08]. Accumulator [GTH02]. Accumulators [CL02a]. accurate [ZY08]. Achieve [CFRS01]. Achievement [Coc01a]. Achievements [VDKP05]. achieving [PS04c]. ACISP [YG01c]. ACM [ACM01a, ACM03a, ACM03b, ACM03c, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, MS05b, Bar00b, FMA02, Rai06]. ACNS [GBK05, IY05, J04, ZY03]. acoustic [ZZT05]. Acquiring [SETB08]. across [Dav07, ZBLV05]. Act [Kha05, Uni00a, Uni00e, Uni00d, Uni00g, Uni00h]. Actel [DV08]. Action [SE01]. Active [BC05a, BACS02, BP02, LTL05, MA00a, MA00b, Tad02, BPS08]. Active-Content [MA00a, MA00b]. activities [AJ08, SN07]. actually [Hau06]. Ad [BSS02, KH05, WT02, Cha05b, DHMR07, KVD07, LHC08, LKZ+04, PSM07, SLP07, T07, ZC09, MA004]. 'ad-Durayhim's [MAA04]. Ad-hoc [BSS02, WT02, DHMR07, ZC09]. Adaptation [ISSZ08]. Adapting [MJD01].
Adaptive
[CM00, CBB05, CTL04, CL08, Coc02a, CS02, CS03b, DSS01, EFY+05, FMY01, JMV02, KCJ+01, KLL01, LP01, MP05, Nov01, Pie05, ZWC02, AAP07, Che07a, DP04, MB08, SH11, WNQ08, XMST07, YZDW07, ZCW04].
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
[CF07, DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Sve08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DR05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sve00, WFR00, Wri01, YW06].
Advances
[AKi09, Bel00, BSS04, BS05, Bon03, Boy01, Cla00a, DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Sve08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DR05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sve00, WFR00, Wri01, YW06].
Advantages
[AKi09, Bel00, BSS04, BS05, Bon03, Boy01, Cla00a, DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Sve08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DR05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sve00, WFR00, Wri01, YW06].
Adversarial
[CLR09, GSS08, MNS08].
Adversarial-knowledge
[CLR09].
Adversaries
[CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05].
Adversary
[Aba00, Gor06, RW02].
AES
[CGH+00b, DR05, FIP01a, Her09a, Pha04, AG01, Ano00a, AL00b, BDK+09, CG03, Coc02b, DR00b, DR02a, DR02b, DLP+09, DPR01, Dan01, Dra00, EYCP00, Eib08, Fer06, FM02b, GC00a, HW03b, IBM00, IKM00, IK00, Jol00, KS09a, Kel05a, Kel05b, KFSS00, KV01, LP02a, Len01, MMH+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03b, RRY00, SKKS00, SM03b, Sch00b, SWK+00, SW00a, SL00, WW00, WB00, WOL01, 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, FKS00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Bau05, DPR00, BPR02, BNN+09, BBN+02, BGM09, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egh00, EBS01, FPP01, Fry00, Geb04, HNZI02, HLL+01, HG07, Hsu05b, HLC08, Ino05, ISW03, IIT03, JKS02, J00b, JT01a, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, M100, M0102, MG08, NRR00, NLD08, OKS06, O00T03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PQ03b, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sho00b, SKU+00, SK01, SLL+00, Tad02, TV03, VHP01, XH05, YJ00, YKLM02a, YKLM02b, YKLM03, ZCW04, ZSJN07].
Age
[Mar08b, Lev01].
Agency
[AJ08, Ban02, K0v01].
Agent
[HAQ05, KC02, PZD09, R0501, RC01, Rot01, ZYM05, KX0D00, SSM+08, SH00].
Agent-Based
[HAQ05, SSM+08].
Agents
[WHII01, Hau06, LAS+07].
Ages
[Eag05, Kin01].
Aggregate
[BGLS03, WK05].
Aggregated
[ZN05].
Aggregation
[Her06, CCMT09, MS09b].
Aggressive
[Wy05].
AGM
[Gau02].
Agreement
[AAGF01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b].
ABB\textsuperscript{+}04, AKNRT04, CYY05, CYH05, Che04a, CY05, CJ04, CJa05, HWWM03, Jua04, KPT04, KRY05, KHKL05, LKKY03a, LKKY03b, LL04a, LLL04, LL05a, LKY05b, LKY05c, LKY05d, LLY06, LLS\textsuperscript{+}09, LLR02, PQ03a, PQ06, Sh05, SW05a, SC05b, Tsa06, Tse07, VK08, YW05, YC09b, YS02, YSH03, Yi04, YRFY05b, ZC04, LLR06\textsuperscript{+}.

agricultural [Lov01].

Aided [NS01b, HLL\textsuperscript{+}02].

Aimed [Pau02a].

Aimed [SFDF06].

Airport [Sas07].

airwaves [Dav07].

Ajtai [GK05].

AKS [Che03].

Al [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx].

al-fusul [MAaT05].

al-Ka [MAaT07].

Al-Kindi [MAaT03, MAaTxx].

al-mutargima [MAaT05].

Alan [Pet08].

Alcatraz [LSVS09].

Alchemy [Pag03].

alert [AJ08].

alerts [NCRX04].

Alexandria [MS05b].

Algebra [Cou01, CD01a, Lan04a, CK07, Fau09, HW03a, HWR09, SH09b].

algebraic [AK03, Bar09, Can06b, CMR06, CM03, Cout03, 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, Bi09, BSC01a, CLY09, CU01, CJS03a, CTL01, CG03, CC06, CH07c, CM00, CT03, CP03, DR01, DG00, Dhe03, EYCP00, FBW01, FMS01, GMM01, HTS02, HM02c, HZLS05, JK01, KBD03, KMM\textsuperscript{+}06, KY02c, KTB07, KV01, LPZ06, MM01b, MM01c, MS02e, NMSK01, OS01, PZLO9, PBLO7, Ram01, RS01, SS01a, SPGQ06, WHL05, Wes01, Wie00, AJ08, App05, BF06a, Bia00, CO09a, CHC01, CKY05, CYH05, CHH01, CP09, Fe06, FSGV01, GPX08, Jon08, KJ01, Kwo02, Kwo03b, LCP04, LLZ06a, LLZ06b, MN14, OS07, SH11, SCS05a, SM08, SZF02, TM01, WL02, WN95, Wue09, YRFY05c, And03, SA02].

Algorithmic [Hro09, Jou09, Has01b].

Algorithms [Hro03].

Algorithms [AD07, An09d, AB09, BKLS02, II00, BWBL02, CPhX04, CLR01, Dam07, DWN01, FW09, Gan02, GL06a, Har06, Har00, Int00, JP03, Kel05a, Kel05b, Lee03b, LR07, LP02b, PBB02, Pre02a, Pre02b, SL00, TLY04, TV03, WBF00, WWGP00, AHK03b, An01n, AH05, CKL\textsuperscript{+}09, CCM01, GHPT05, GPC08, HW03a, HWR09, HHG06, Hro05, JK01a, MCHN05, Pre07, Rhi03, TC05, XLSM06, ZZLS07, Zir07, dH08].

Alien [Wil01b].

All-or-Nothing [Des00c, SR00].

Allied [DR01, Wie00].

Alliance [CCM05, LQ09].

Allowing [JLL02].

Almost [AP09, BS00a, Jut01, Mar02b].

Alpha [WB00, Wu02].

Alpha1 [KHD01].

Altera [An02e].

Alternating [WB00, HKPR05].

Alternative [Bad07, Gar03a, Han00, BMW02b].

always [BB79].

am [Eke02, SU07].

Amalfi [BC05c, CGP03].

Amenability [WW00].

America [DB04].

American [GL05, Kat05b, Alv00, Na05].

Americans [WD01b].

among [BN00a, KT00, SKU\textsuperscript{+}00, Win05c].

Amenity [Pen01b].

Amplification [BPR05, Des00a, Pau01].

Amplify [Ch01].

Amsterdam [Knt02].

Analyses [BPR05, Des00a, Pau01].

Analysing [BL02].

Analysis [AR08, ABR01, AKS06, AD07, An01c, AIK\textsuperscript{+}01, ARC\textsuperscript{+}01, Ava03, BN00a, BDhKB09, BRS02, BF05, Bo01, BSL02, Cry00, CK02a, CS03b, DPV01, Dra00, FL01a, FGM00a, Gir06, Gol01c, GHPT05, GLG\textsuperscript{+}02, GPR06, HSZ10, HKR01, HSS04, Hey03, HM02c, IIT03, JK01a, JQY01, JT01a, JQY01, hKLS00, KMS02, LCK03, LKLH09, LY05, LWK00, LH07, MOP06, Mar02b, Mas04, MS01, MM01b, Mea01].
Mes00, Mes01, MAaTxx, MG08, NP02b, NSS02, OS06, ÖÖP03, Puc03, QS01, SSST06, Sha01c, Sm03b, SDMN06, SQ01, SWT07, YSS+01, ZCO0, ZGLX05, AvdH00, AW05, AW08, Ab01, AHK09, Aso04b, BDSV08, BBK+03b, Bjo05, BG07a, BR05, BCJ+06, CKL+09, CW07, CS05a, DS09, DKS08, GW08, GM04, GTZ04, Has01b, Hir09, Hro05, Hut01, JEZ04, JPL04, JSW05, KSF00, Kor09, LKH+08, LMW05]. analysis [LW05a, LKJL01, Lu07, Mea04, MT07, MRST06, OS00, PS08b, SK01b, WLT05a, WPP05, XH05, XMST07, YCW+01, YC08, ZWWL01, ZL04c, ZDW06].

Analytic [Shp03, Nie04]. Analyzing [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04]. anatomy [Ban02].

Anchor [Ree01]. Ancient [Imr03, Sin00, Mol05, Pin06]. Andrei [Puz04]. Andrew [Puz04]. Anguilla [Fra01]. Anniversary [Sal01b, Coc02a]. annotated [Pet08]. annoyances [Tyn05].

annoying [Tyn05]. Annual [ACM01a, ACM02, ACM04b, ACM05c, ACM06, ACM07, ACM08, Bon03, Cra05a, ELvS01, Fra04, IE00a, IE02, IE03, IE04, IE05a, IE06, IE07, IE08, IE09b, Kii01a, Men07, Sho05a, USE01b, USE01a, USE02c, VY01, Yun02a, ACM00, Bel00, Han00, Jef08, NH03, ST01d].

anomaly [RCG+05]. Anonymity [GM03, IKOS06, MP02, SS01b, EY09, LV07, Par04].

anonymization [FXAM04, RW07].

Anonymous [ABC+05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL+08, SOO002, Wan04a, YT09, ZGI0, BP03a, Ch08b, Chi08c, Chi08d, EY09, LHC08, Sac02, Sha03c, WCJ05, YTYW05, ZCO9]. ANSI [II00, Kel05a, Kel05b, Oiw09]. ANSIC-C [Oiw09]. answer [Ano01e]. Answers [PT08]. Anthony [Pag03]. Anti [Kha05, Ano05c]. Anti-Circumvention [Kha05] anti-virus [Ano05c]. anticipation [Goo00]. Antikythera [Eva09].

Any [Fis01b, HNO+09, Ano05b, CDM00, DFM04, DMS00, HR07, PO00]. Anyone [Ros07]. Anytime [DJLT01]. Anywhere [DJLT01]. Apache [Had00]. API [MWM01, Mor03]. APIs [BM01c]. Appendix [Kel05a, Kel05b]. Applet [ZFK04]. applets [Bis03a].

Applicability [Wya02, TM01]. Application [ADI09, ACS02, BAI01b, Boy01, CL02a, CKQ+03, Dam07, Dhe03, GHH+06, HF00, HI04, IKP+07, JX05, JOu04, Lai03, Lee04b, LLS05b, LXM+05, NP07, Oka00, Pi01, PQ03b, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SDFD06, TWNA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG09, CMKT00, CP07, DM08, FP00, HCLETRG06, JRS09, JMV09, LGKY10, Lav09, MT07, MPGD06, MK05a, NZS05, RSS04, SSST06, TC00]. Application-Aware [IKP+07].

Applications [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, BI05a, BGK03, BS00a, Bili03, BGOY08, BSS02, BLO8, CC04a, CD00a, CV02, CGH01, CZ05, CHSS02, CSY09, Cra05a, CD01, DJ01, DK02, DK07, DA03, DFPS06, FR02, GSS08, GK+09, GJKR03, Gen04a, GRW06, Gol01a, Gol04, HRS02, HNO6, Han06, Has01a, HSS04, HR05, HJW05, HI04, JT01b, JY01, KM+06, KGL04, KMO09, KKM01, Kn02, MA00, MMT07, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Shi03, SY01, SPGQ06, Vau02, Wau02, XL09, YZ00, Zie00, Zho02, ÁCTZ05, Ate04, AH05, AFHG06, BG08, BGL+03, CCCY01, CM05b, CS09, CSK+08, DY09a, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gal02, GVC+08, GKK+07, GB09, HHS01, Has02, Hen01, HPK05, Jac00, KV+09, KNS05]. applications [Laf00, Lee04a, LJO0a, LPW06, LB05, MY01, Mal06, MC04, MS04, Nie04, PW08, PBD07, PC00, Q500, Ros06b, SS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPHH06, WW08, WA06, WV00, YS04, ZBP05].
Applied [HW03a, HWR09, SL07, GV09, GNP05, IKY05, JYZ04, ZYH03]. Applying [Elb09, KC02, Lan00d, LMS07, SQ01, SPMLS02, TND+09, vDKST06].

Appointed [CL01a]. apprehension [AJ08].

Approach [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJJT01, Kra03, Lai07, LL05c, Lut03, OMTO2, PBD00, Pau02a, Pre02a, SKG09, VH09, VVS01, Vir03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLMM05, GG08+0, Har05a, JJ01, JW01, KVD07, LG09, LHC02, MT09, Mar05b, Mos06, NN03, SLP07, SK03, SN04, SW00b, ZL99, ZSZ01, ZL04b, ZL04a]. Approaches [CGMM02, AvdH00, DG05, Fri07, Has01b, KXD00].

approval [Wan04b].

Approximation [CLZ02, Hro03, Kuk01, WL02]. Approximations [BDQ04].

Apress [Ter08].

April [AN00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH+06, DFP06, Joy03b, Kuo02, Mat02, NIS00, Nac01, Sch01d, SMP+09, YDKM06]. APSS [ZSV05]. Arabic [MAaTx]. Arbitrarily [RW03b]. Arbitrary [AR01, BR00b, Br01, CJK00, CHJ+01b, CF02, Tee06].

Arbitrary-Length [AR01, BR00b, CJK00, CHJ+01b].

Architectural [ASK07, ABM00, BMA00a, BMA00b, CAM00e, CW02, Gro03, KV01, LTM+00, ZZLG05, Ano05c]. Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KYY2c, KDE01, LKM+05, LZ04, LXM+05, Lu02, MP01c, MFS+09, Rot02a, SMTM01, SM03b, SLG+05, Uz04, Che00a, CC05e, DHL06, Ino05, LHH03b, MPPM09, SKW+07, SLL7, SH05, Tau01, WWA01].

Architectures [BH05, GC01b, RM02, Con04, DP04, GKS05, NdM04, RH00, WH02b].

archival [SGMV09]. Archives [RC01]. archiving [DMSW09]. area [BP03a, Cal00c].

Area [HH04, MZ04, PT06, VV01, AMW07, Buc00a, HH05, HA00, NH03, ST01d].

Aren’t [Bau01a, Bau01b]. Arguments [HNO+09]. ARITH [BS03, BC01, IE05b]. ARITH-15 [BC01]. ARITH-16 [IE05b]. Arithmetic [BS03, BIP05, BGK+03, BCDH09, BC01, CT03, Gro03, IE05b, KM07, Kir03, PPV96, RDJ+01, SR06, GPS05, PS04a, SO1G07].

arithmetics [Lam91]. ARM7 [DV08, XBO1]. armies [Ano03c]. Army [Boy03]. Arne [Bec02]. array [DZL01].

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

Article [Che08b]. Artifacts [EE+03]. Artificial [Cop04b, MMH02]. Arun [For04]. ASCI [MJD01]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DN00b, RJ01a]. ASC [WOL01].

ASIP [SKW+07]. asks [Ano08a]. ASM [MK05a]. Aspect [Kos01a]. Aspects [BLMS00, CMMR06, FEL06, AN03, DLP+09, Rup09]. Aspiration [Ash03]. assembly [Gou09]. assessing [CDD+05]. assessment [CC05e, DMS07]. assets [KH03, NRR00].

Assignment [BRTM09, HC08, CHC04, CJ03c, DFCM04, HW03c, Hw00, Lin01a, TP07, WC01b, hY08]. assignments [SW05].

Assisted [ECG+07, XS03, Art04, BB05, LHL04a].

ASSL [VH09]. associated [XLMS06]. associativity [HRS08]. Assumption [CS00, DN00a, FPSO01, KMZ03, ZD05].

Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT+00, Nao03, SB02, Mic02a].

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

Astrology [Pag03]. Astronomy [MYC01].

Asymmetric [CH07b, M01, SY01a, SB02, WH01,
Asymptotically [vDW04]. Asynchronous [CKPS01, FML+03, KSR02, SKR02, ZSV05].

At-targama [MAaT05]. Atlanta [IEE09b].

ATM [Pat02a, Pat02b, Zea00]. Atomic [CNV06]. Attached [RCBL00].

Attachments [Ric07]. Attack [Ahm08, CKQ03, CS05b, Des00b, Fil00, FV03, GHJV00, GHJV01, HQ01, Hug02, HW01, JJ00b, KCP01, KS00a, KML+02, KM01c, LY07, LNL+08, LV04, LMV05, Luc02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, PQ03b, RMS05, SG09, Sch01b, Sho00b, Sma03b, VHP01, YKLM02a, ZC04, ASK05, Ade09, Ano09c, DKL+00a, Duj08, Duj09, GM00a, HabR04, Hes04b, HG07, Iwa08, JI02, 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, BM00b, BBB+02, BDK+09, BU02, BM03b, BGM09, BCM02b, BM01c, Can06b, CS07b, C203, CT08a, CS01, CKM00, CJNP00, CM03, Cou03, CWR09, CD01b, DPV01, DFS04, DJ06, DS08, DM07b, FKSW00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GK02, HSH+08a, HNZ02, HR04a, HSH+01, HLC08, ISW03, JKS02, JJ00d, KS00a, KS00b, KKS01, KCJ+01, KI01a, Law09a, LSS05a, LW05, LJ05b, MOP06, MP06, MF01, Mck04, Mes00, Mes01, Møl02, MG08, OT03a, OT03b, ÖOP03, OST05, Ove06, PKE01, PMS09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLY05, YDD001, YY01, YG01b, vW01, BPS08, Bau05, BCS08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05b, HL05b, Io05, IM06, JDJ01]. attacks [KS05a, KTC03, LPV+09, LS00, MMJ05, NS05a, NL08, OST06, PQ03a, RG05, Sch00c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07a, WL04b, Yan07, YS02, ZS070].

Attitudes [FDIR00, CF05]. attractors [HHY07]. Attribute [LY05, RSA00e, IV05]. Attributes [SS01b].

Auction [AS01a, Ano01a]. auctioning [RGC+05]. Auctions [Bra01b]. Audio [Arn01, CS05c, DRL09, MH05, WNY09, WWL+02, XFN01, WNQ08, BS01b, KJR05, KN03]. Audio-and [BS01b, KN03]. Augmented [CS07c, You01]. Augmenting [AL04].

August [AMW07, Be00, B+02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KKP02, KI01a, KP01, MZ04, Men07, NY03, PT06, RS05, Sch00a, Sch04a, Sch05a, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a]. Australia [Boy01, IZ00]. Austria [DKU05, P601, Jef08]. Authentic [DGMS03, Dur01, SS01b]. Authenticate [Bau03a, Bau03b]. Authenticated [AGT01, BN00a, BPR00, BU02, BC04b, BM01, BMP00, BCP01, CPP04, Chi08e, DG03, DA03, EP02, GKK007, GL03, GTTC03, HS07, KOY01, KY03, Kras03, Lee01, LHT09, MPS00, Mac01, MSJ02, MND+04, NA07, Nan02, Ng02, SK00, Vau05b, WC01a, YPPK09, Yi04, ZWCY02, BKN04, BCP07, CYY05, CYH05, Che04a, CLC08, CJ04, CJI05, DG06, GL06a, GM05, HTJ08, HWW02, HWW03, Hsu05a, Hwa05, HL05c, HL05d, Jua04, KOY09, KRY05, LLM07, LKKY03a, LKKY03b, LL04a, LLL04, LLL05a, LKY05c, LKY05d, LHC08, LRR02, LRR06, LWK05a, Mi08, PQ03a, PQ06, RBB03, Sei05, SW05a, SC05b, TLH05, TJ01a, Tse07, WH06, WH02a, XY04, YW05, YCO9a, YS02, YSH03, YRY05b, YPKL08, ZC04, ZAX05, ZW05a, ZL05].

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

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

Automating [Gue09]. automorphism [Pae03]. automotive [LPW06]. Autonomic [VH09, Che05c]. auxordsies [Car00]. auxiliary [Dam00, DKL09]. available [CBD+05]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average [KMT01, CGHG06]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average [KMT01, CGHG06]. Average-case [Mic02b].

Avoid [Tyn05]. Avoided [CNP03]. 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 [CS03c]. Backup [Str02]. backward [HCD08a, HCD08b]. backward-and-forward [HCD08a, HCD08b]. Bacon [GG05a]. bad [BBN+09]. bail [Ano01h]. Bait [Luc02a].

Balancing [Hööf01, Lut02]. Ballot [Cha04]. Baltimore [ACM05b, ACM05c, GL05]. Bandwidth [AUW01]. Bandwidth [CGJ+02, YY01, SLP07]. bandwidth-efficient [SLP07]. Bandwidth-Optimal [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Bel00, Bon03, Fra04, Kii01a, Men07, Sh00a, Yun02a]. Barcode [Che08b]. Bare [DPV04].

Barken [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, XSWC10, IR02]. Based [Ano01c, ANR01, AF03, AJ008, BDG+01, BKLS02, BNPS02, BN02, Ben00, BRS02, BFO1b, BF03, BB04, Bon07, BCHK07, BGH07, BPR+08, BD03, BMN01, Boy03, BQR01, BM01c, BSN000, BRTM09, CGFSHG09, CvTMH01, CK02a, CGMM02, CF01b, CC02a, CV03, CPP04, CCD07, CS07b, CC01b, CLT07, CHSS02, CHM+02, CZK05, 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, HMO2b, HS00, HL02, HQ05, HCO8, HH09, Igl02, Jam00, KBO03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05a, Kel05b, KY01c, KY02b, KCO0b, KKO2, KCO2, KCD07, KPR03, KM05, Kri02a, Ku02, KWP06, KT00, LLL02, LP03]. Based [LKLK05, LHT09, LZ01, LZ04, LL05c, LPZ06, LY07, LXH07, LLRW07, LK000, LSC03, LHS05, LSZ05, LL05b, LCD07, MPS00, Mar08a, Mar08b, MN005, Nak01, Nam02, NBD01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP06a, PZ09, PMZ00, Rij02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sal05b, Sch01a, SSFC09, Sha02, Sha01e, SOO102, SXY01, Sma03a, SBEW01, SGB01, TMM05, TLYL02, TZT09a, TZT09b, VMS05, Vau05b, Ver06a, VHP01, VK07, WRW02, WY02, WZ05, WGO5, WCO09, WOH09, WBD01, WCO4, XLY09, YKMY01, YT09, YVD001, YSS+01, YKW01, YLH05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWCV02, vDW04, AAP07, AA08, Ano02b, Ano05b, App05, AAKD09, BGB09, BBC+09, BR04, BFG08, BS01b, Bla01b, BMW05, BLP06, BGL+03, BDS09b, Buh06, CGHG06, CG06, CL02b]. based [CO09a, CL04d, CFY+10, CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CJL06, CLK04, CLJ05, Cho08b, CYH+07, CFVZ06, CCD+04, CTT07, CHT02, CC04c. Cra05b, DS09, DPT+02, DHL06, DLR09, DV08, DW01, Dug04, EHKH04, FLZ02, FXAM04, FWL08, GM08, GW08, GSK09, GL06a, GHdGSS00, GS01, GPS05, GGS+09, GB09,
LSKC05, OSSST04, SKG09, WCJ09, ÁCTZ05, BG08, BG09, FSGV01, GB09.

Binary-Ternary [ADI09, BIND [Kle07].

Binding [DN02b]. BioAW [MJ04].

Biometric [AHKM02, Da01, EM03, HWH01, KJR05, LTL+04, PMRZ00, PK01, SR01, Sas07, Way01, Way02a, Wea06, BS01b, Gui06, JP06, KZ03, Li05, LST+05, MR00, RF07a, RF07b, RF07c, Smi00, MJ04, TB02, ZJ04]. Biometric-Based [PMRZ00].

Biometrics [Ano04a, Ash03, Bjo05, MR03, Ril02, Str01a, BSSM+07, BCP+03, Buh06]. Biometrics-Based [Ril02].

Biomolecular [Bi09].

BIRDS [MLM03].

Birthday [Wag02].

Bisimulation [BJP02].

Bit [AIK+01, BK06a, BL08, CGH01, CDL+00, DMS00, GS07a, ITO03, KZ07, LST05, MS09d, PCC01, RMH03b, SBBM+07, BKR00, BRS02, BR02, BSC01a, ČvTMH01, Can01b, CLLL00, CP02, CMB+05, Čro01, DRO0a, Dwo03, EYCP00, Fhu02a, HI04, HSH+01, JKK+01, KCP01, KYH01, KKG03, LLLR07, LRO02, MV00, MS02c, NPY01, OMS01, Pat01, PS06, Pli01, RMS05, SM03b, SYY+02, SKU+00, SKI01, WCJ09, XH03, YG01b, Bao08, BF06a, DY01, Dum06, Egh00, GPX08, Hey03, JKH01b, Jun05, Kat05a, KJ01, LDH06, LCO04, LKH+08, MML05, PSP+08, RBB03, SHJR04, SHH07, WFO2, XH05, YI00].

Block-Based [LLR07, BBC+09].

Block-Cipher [BR02, RBB03].

Block-Cipher-Based [BRS02].

Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. blockciphers [Fur01].

Blocks [Jon02]. Blockwise [JM02].

Blockwise-Adaptive [JM02]. Bluetooth [GBM02, LVD04, LM05]. Blunders [Bur01].

Blurr [VHP01]. Blur/Deblur [VHP01].

Blurring [LSKC05, SK06]. Board [CB01].

boats [DB04]. Body [Bam02, TG07].

Boethius [Eag05]. bolstered [Ano01]. bombe [Wil01a, Tur04]. Bombes [Ano02i, LBA00].

bombs [Lov01]. Bonds [CAC03].

Bonné [AS05, Hes04a].

Bonn [DRS05].

Book [And04, Duw03, Eas05, Eva09, Fal07, For04, Gas01, Gun04, Imr03, Irw03, Jun08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Ree01, Rot07, Sal03b, See04, Sph04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wa00, Was08a, Kat05b, Lan07, Lun09, MAaT05, Ros00b, Sin99, Sin00, AAG+00].

Books [Che00b, Dr.00c, Ros00b, Ree01].

Bookshelf [Lut02, Lut03, Wil01b].

Bookworm [Sal03b].

Boolean [Car02, CT03, CS09, MS02b, MFD04, QPV05, SM00a, SM00b, SM03a, WV00].

Boom [Ano04a].

Boomerang [KKS00a, KKM01, KML+02]. Boot [HSH+08a, HSH+0b, HSH+09].

Border [MJ07].

Borders [PGT07].

Boston USE01b, USE01a].

bot [Ano08b].

Botschaften [Sch09]. bottleneck [WL02].

bottlenecks [HTW07]. Bound [CY08, DGO03, KMT01, HLLL03, yY08, GW00].
Boundaries [PGT07]. Bounded [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vad03, DFSS05].

Bounded-Quantum-Storage [DFSS08]. Bounding [DM07b]. Bounds [BDF01b, BP03b, DIRR05, Di 01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKK03, JZ09, KS05b, PS02a, Shp99]. Bouwmeester [Duw03]. Box [Ano01j, BRS02, CF02, CFS05, DI05, DIRR05, DS08, FM02b, KY01d, Kil01b, SMTM01, JmBdXgXm05]. Boxes [Bih00, BCDM00, ZC00]. BP [Wei00, Wei05]. Braid [AAFG01, CJ03a, GM02a, Hug02, KLC00, LLH01, LP03, MSU05, Cho08b, Hen06a].

Branches [Fel06]. Brassard [BGM09]. Branch [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breakers [CD00b].

Breaking [Ano09a, BKN04, Das08, DKFX05, GO03, GK02, Kov01, KR03, Kil08, Sal00a, Wri05, Fie09, Gar01, SE01, Sm01b, SL07, Swe08]. breaks [OS00]. Breakthrough [Coc02a, LR01, Pal02, Pau02a]. Brief [Bon07, Cos03, Kir01a, Boo05, Gra01]. Briefs [MP00, PM00, Pau02a, Pau02b, Pau03, Pau09]. Bright [Ano01j, LN00]. brings [Ano04e]. Bristol [DFCW00].

Britain [Gui06]. British [ACM08, Fie09, Fra01, Syv02, Bud00b]. Broadband [MP00, SHL07, MJF'08]. Broadcast [AF106, BGW05, CKP01, CVN06, DS03, FWW04, GSW00, GKK007, GRW06, HS02a, HLL05, LN02, SNWX01, Wooo, ASW00, KSW06, Kre05, Mar05b, NLD08, RG09, WDL09, LN04]. broadcasting [TJ01b, WH02b]. Broke [Urb01, KS04]. Broken [Ahm08]. Brooks [Bar00b]. BRSIM [BPS08]. BRSIM/UC [BPS08]. BRSIM/UC-soundness [BPS08]. Bruce [Hei03, Sty04, See04]. Bruges [Pre00]. Brunley [ASK05]. Brute [Cur05, SGA07]. Brutus [CJM00]. BSD [Lin02, ASW+01, Lin02]. BSDCon [USE02a]. Bubble [Ber03]. Buchmann [Lec03a]. Buffer [FOB105, Fry00, Ino05]. Bug [BCS08, Bor00]. bugs [GJL06]. Building [Jou02, Knu01, Mar02a, And08b, Bra01a, FB01, LS05b, MCG06, MPHD06, PQ06, DB04]. buitenlands [dL00]. Bulletin [Cer04b]. Bulletproof [Cha05b]. bundles [GT02]. Burrows [ABM08]. Burning [Arn01]. Bush [Rik06]. business [HHSS01, Poh01]. Buy [PLW07]. Buyer [MM01a]. buys [Zaf00]. Buzzes [Coc02b]. Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGR07, LLR02, LLR06, P106]. Byzantine-Resistant [CNV06].

C [Ter08, Zol01, III00, Oiw09, RMPJ08, Sea05, Sea09, VM03, WK01, Wel05]. C# [MJ03]. C-testable [RMPJ08]. C2C [HTJ08]. CA [ACM03b, Joy03b, KKP02, Men05, Men07, Nac01, Oka04, Pio06, Pre02c, USE02a, USE02b]. CAA [MGC02]. Cache [BBT02, Kle07, OST05, OST06, TSS+03, Ino05, WL07a]. cache-based [WL07a]. Caches [GSVC02, LLK05]. Caernarvon [TKP+08]. Caesar [Chat02, You06]. CAIDA [Pri00]. Cairo [EBC+00]. CalLC [Sil01]. calculus [MRST06]. Calcutta [Roy00a]. Calibrating [SDM06]. Calif [ACM03c]. California [ACM03a, ACM07, Bel00, Bon03, Fra04, IEE00a, Kim01a, Sch01c, Sch04a, Sch05a, Sh05a, USE00b, USE02c, Wll99, Yum02a, IEE06]. Call [Ano04b, Ano07b, Ano07a, MD04]. Calls [WG05, Ano08c, WCJ05]. Cambridge [ACM10, Chr00, Chr01, CCMM02, CCMMR05, IEE03, JQ04, Kat05b, Kil05, Nao04, Pag03, Puc03, Rot07]. Camellia [AIK+01, HQ01, KM02, LHL+02, SM03b, SK01, XH05]. Camera [CGK+02, Ge03]. Camera-Based [CGK+02]. Can [BB02, CZB+01, Dav01c, Lai08, Ros07, Ver06b, CNP03, CG05, SBB05, Zir07].
Canada [ACM02, ACM08, AMW07, HH04, HH05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01]. Candidate [II00, EYCP00, NIS00, SKW00].
Candids [AL00b, DPR01, Dra00, GC00a, SB00, SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b]. cannot [Gav08]. canonical [TP07]. CANS [DWML05]. Canterbury [CZ05]. Cantor [WPP05]. Capabilities [BDTW01, AL04, ABDS01]. Capability [MH05]. capable [ETMP05]. Capacity [ChLYL09, Sug01, ME08a, Wan05]. Cape [IEE05b]. capital [SW05b]. capture [AMB06]. Card [BCST00, CMG+01, CL07, CJT02, DF01, DFPS06, RE03, RS01, SR01, Ano00k, Ano01l, Ano50b, AJ01b, Bor00, BGL+03, Bur00, Cal00c, Car01, CCCY01, Cha05a, Cla00b, Con00, CH00, DFCW00, GMG00, HM01a, Has02, Hen01, Hsu05b, Jua04, Jac00, LSA+07, LC05a, Lu07, Q500, RE00, SP02, Sni00, VK08, Zaf00, Che00a, FGL02, Pau02b, SKK050, TV03]. card-based [LSA+07]. CARDIS [DFPS06].
CARDIS’98 [Q500]. Cards [An004, AJ01b, Be01, CK06, DJLT01, HBDJL01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NQF03, Q500, Sak01, S501]. Caught [Wei00]. cause [SBB05]. Causes [Mur01]. Cautionary [GMP01a]. Cayley [Lam91].
Cayman [Syv02]. CBC [BBKN01, BPR05, BR00b, DGH+04, Fer06, JM02, KI03, Var01, Vau02]. CBIDs [MC04]. CCA [KOMM01, Mii01b]. CCA2 [BST02, Lin03, RG09]. CCA2-Secure [Lin03]. CCGrid [LCL06]. CCM [Dwo03]. CCS [Mar02b, MS05b]. CDH [CM05a]. CDH-Based [CM05a]. Cell [Fox00, MYC01, SHL07]. Cell-phone-free [Fox00]. Cellular [Laf00, LZ04, MGC02, PZL09, Rie00, SBZ04, Ba04, ETMP05, KK03, SHH07, Wan04a, dRMS05, Wue09, SS05+08]. Censoring [An01e]. Center [AUW01, CH01a, CYH04, LPM05].
Centered [BK070, CMB+05]. Central [CHL02]. Centralized [Wac05]. Centre [PPV96]. Centric [Mit02b]. Century [Eva09, Kob00, Lan00c, PLS04, GS01, Lan00a]. Century-Long [Eva09]. CERT [Sea09]. certicom [LM08]. Certificate [BLM01, Gen03, GMR08]. Certificate-Based [Gen03, GMR08]. Certificateless [HLC08, HRL09]. Certificates [BDTW01, CMG+01, RdS01, Bra01a, LCK04, ZSM05]. Certification [An01o, CHM+02, RSA00b, BG08, BD04b, KB09]. Certified [ANR01, CSV07, LCH07, NZC05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LWW05a, NZS05, Shao4b, Shao5b, TLH05, Tsa05, TJ03, WH03]. Cerven [Siu03b]. CFS [Ito01]. ChaCha [Ber08]. Chain [YT09, YZ00, Wue09]. chain-rules [Wue09]. Chained [BCC01, BC05b].
Chaining [BKR00, CBB05, PCC03].

challenge [LM08, LW05a, PRS04, Smi08].

challenge/response [LW05a].

Challenges [Cla00a, GV09, Nao03, Sta03, SVEG09].

Chang [CWJT01, ZC05].

change [CYH05].

Changed [McE04].

Changes [Mur01].

Changing [BST03].

Channel [BU02, CHVV03, Law09a, M¨ol02, NMO05, OT03a, OT03b, Sch06a, SYLC05, ARR03, BP03a, BG07b, Buh06, CNPQ03, KSWH00, LCZ05b, MS09c, PSP +08, WL07a, YTWY05].

Channels [AIP01, CK02b, Nam02, Vau05b, LH04].

Chaos [JK01b, SK01b, WZW05, M¨ol01a, LMC+03, McN03, PSG+09].

Chaos-Based [WZW05, SK01b, JK01a, PSG+09].

Chaotic [BCGH11, LLL+01, Mul06, SXY01, USS02, Vav03, AMRP00, AMRP04, GHdGS00, GB0, HHY07, HLwWZ09, JK01b, LMC+03, LYGL07, MA02, PMB01, PS01a, PZL09, SPG02, SL09, UHA+09, VKS09, WG02, WW08, kWpLwW01, WLW04, YZEE09].

Chapman [Kat05b, Was08a].

Chapters [MAaT05, Tat05].

Characteristic [Gau02, GPS06, KT00, Ver02, GPS05].

characteristics [RFR07a, RFR07b, RFR07c].

Characterization [AJ080, Nam02, XH03, BGM04, KY00, QPV05, XLMS06].

Characterizations [Pas05].

Characterizing [BTW05, BTW08].

Charging [BACS02, RH02].

Chatter [Kee05].

Chau [BNPS02, KL+06, WH05].

Chauvinism [M¨ol03a].

Cheating [CCL09, OKS06, PZ01, PZ02b, PZ02a, ZP01].

check [Kir01b].

Checkable [BPST02].

Checking [BL02, JP07, KLN+06, YJ00, GGH+08, RG05].

checklists [Sha01a].

Checks [FM02a].

Checksums [Sto01, SGPH98].

Check [Kim01a].

Chemical [EIG01].

Chen [LW05c].

Chennai [CV04, RD01, Roy05].

Chernobyl [Rie03].

CHES [JQ04, KKP02, KP01, KNP01, RS05, WKP03].

CHES-64 [LKHL09].

CHESS [LKHL09].

Chip [Ade09, BPST02, D08, MM01b, MM01c, MP00, Mit02b, Fox00, STE08, Ano04c].

Chip-Secured [BPST02].

Cho [Ano04c].

Chips [Ano00d, GP00, Pau02b].

Choice [Jam00].

Choquet [SH11, SM11].

Chosen [BCHK07, CKN03, CHJ+01a, CHJ+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JKS02, J00b, KS00a, KY01a, KUC01, KM01c, KI01a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH+09, KG09, ZCW04].

Chosen-Ciphertext [BCHK07, CKN03, CHJ+01a, CHJ+01b, Des00b, DK05, FP01, JKS02, J00b, KUC01, KM01c, Nov01, PV06b, Poi00, CHH+09, KG09].

Chosen-Plaintext [DN02a, KM01c, KI01a].

CHW [CHC04].

CIA [Mah04, Ris06].

Cincinnati [BD08].

Cinematic [CAC03].

Cipher [AIK+01, BKR00, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DPS05, DF07, Dwo03, EYC00, FF01a, Flt02a, GG05a, GBM02, HJC02, HQ01, HI04, KY01c, KUC01, LKMH09, MSN07, NP01, OM01, O MK01, Pat01, PS06, SA01, SM01, SM02, SY03, SXY01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BV04, GPX08, HAn04, Hey03, KH08, Kid00, LKH+08, Mak00, PSS+08, RBB03, SA01, S06, S07, WV08, Win05b, WF02, XH05].

Ciphers [AAG+00, BBKN01, BS00b, BR01, BM07, CVMH01, Can01b, CF01b, Can06b, CJS01, Ch02, CHJ02, CP02, CM03, COu03, DP01, Eaa05, Fil00, FF01a, Fil02, Gol01d, Gol01e, HR00, HR04a, HSH+01, Jam00, Jan06, YKLM03].
Cohen [Was08a]. Coherent [TPPM07].
Coin [Lin01c]. Coin-Tossing [Lin01c].
Coins [HR04b]. Cold [HSH +08a, AJ08, HSH +08b, HSH +09].
cold-boot [HSH +08b, HSH +09].
collaboration [ED03, PCSM07, SBG05, SBG07].
collaborative [LLY06].
collaboration [ED03, PCSM07, SBG05, SBG07].
collaborative [LLY06].
collapse [SBB05].
collection [GMM08, Bro05a]. Collections [Kuh00].
collective [BBB +02, BGM09].
collide [GNP05].
collision [DG02, IKO05, MS09c, WYY05a, WYY05d, GM00a, Sem00].
collision-resistant [IKO05].
collisions [BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c].
collusion [BGW05, HNZI02, Zan01].
college [WKP03].
colored [CDD07].
colour [RS00].
coloured [AADK05].
columbia [ACM08].
column [Raj06].
combination [CF01b, Gau02, GHPT05, GB09].
combinatorial [GMW05, Hro03, SLTB +06, Hen06a].
combinatorics [Lee03b]. combined [LLS05a]. combiner [Sar02, LL06].
combiners [AK03]. combining [Abe04].
comes [Mar08b, Ano03g]. coming [Dan01].
commemoration [BZ02].
comment [SCS05b, WY05, WLW04].
comments [AS01c, CGH +00b, JW01, MNGF02, SKW +00, CJT04].
commerce [CLK01b, GSS02, Kir01a, St00, Uni01, ZYM05, BM03a, FB01, Gra01, MY01, SN07, TMM01, YCO09a].
commercial [LCC05, YLR05]. commercializing [Moo07].
commitment [DN02b, DMS00, FF00, CAC06, HR07, KKL09].
commitments [BN00b, CF01a, DFS04, FM02a, Gau04a, HNO +09]. committee [Un00a, Un00b]. committing [DN00a, Nie02b].
commodity [CGL +08a, CGL +08b, CGL +08c]. common [Pas03, TG07].
commonwealth [PY05].
communicating [Hut01]. communication [AK02a, ANRS01, BYJK08, BBK03a, BIW08, Big08, Col03, Fis05, GKK +09, LLS +09, Mar07, NA07, PL01, Sch06b, SKR02, Wri05, vDW04, BYJK04, BC05c, CC05c, CP03, EY09, GKK +07, GG05b, GC05, HYS03, JZ09, JRS09, KPS02, LPM05, Lin02, MP08, Mul06, PBMB01, Par04, RH03, SNW01, UP05, WWA01].
communication-efficient [Fis05, LLS +09].
communications [BCC02, GN06, HJ07, Ig02, Kra01, Lan00a, Lan04b, LCK01, LL02, LL01, MS05b, Sal01b, Vau05b, VM02, BP03a, CYH04, HW02, LC04a, Sal05c, Ser06, SL05a, Wil09, WGL00, YT05, DKU05]. community [SK06].
commutativity [HRS08].
commuting [CKRT08].
compact [CG03, JT01b, SMTM01, YT09, ZLK02, JAW +00, Mic02a].
companies [Ros04, Ste00]. company [ASW +01, Za00].
comparative [DPR01, GLG +02, Kat05b, LFHT07, LOP04].
comparing [HU05, KLN +06].
comparison [GC00a, GC01a, Gau02, JRB +06, MS02e, SW00a, WW00, FGM03, JL03, Sna01, WB00].
compendium [Lut02].
compensated [AAK09].
competition [Ch00b]. compiler [DFG00, Oiw09]. compilers [Lut02].
complement [YC09c]. complementary [AS01c].
complete [Bar00a, Bee05, Bud00a, FGM001, GC00L, HS04, KY00, MS09d, Sal07, TWM +09, Bud02].
completeness [HG03, MW04, ABHS09, PT08].
complex [JKK +01, LKL05].
complexity [BYJK08, BLM01, BDK +09, CKRT08, CB01, DN00a, FBW01, GKK07, GKK +09, HR04a, Lut02, Nie02b, RMH03b, Ros00a, Rot05, Shp03, BYJK04, CDD00, GKK +07, HR04a, Gau04a, HNO +09].
committee [Un00a, Un00b]. committing.
GIKR01, Gor05, JZ09, Mic02a, MP08, RMH03a, Rot02b, Rot03, Shp99, SPHH06, TW06a, SV08a, Fal07, Rot07.

Complexity-Theoretic [CB01].

compliance [LMW05].

Compliant [CGBS01, RVS09].

Component [BSL02, Hei01, TEM+01].

Composability [PS04c].

Composable [AF04b, BOHL+05, BLDT09, CF01a, CK02b, DN02b, DN03, NMO05, RK05, Can01a, CLOS02].

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

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

compositional [GM04].

Compositional [HN06].

Compostela [BS03].

comprehensive [dLB07].

Compress [Gen04b].

Compressed [ISSZ08, SB04].

Compressed-Domain [ISSZ08].

Compressed-Encryption-Hiding [BD03].

Compromise [Ahm08, Lai08].

Compromised [ZYN08].

Computability [Pet08].

Computable [Vad03].

Computation [ACS02, Bai01b, BCL+05b, BI05a, BIM00, BJLS02, CC00, CDM00, CDN01, CDG+05, CDI05, DN03, DI05, DMO00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, IH04, Je08, KO04, KLML05, KSR02, Lin01c, PS05, WW05, Ano02g, AB09, BEZ00, BEZ01, CLOS02, CLC08, CDD00, DwWnW05, 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, Laut08a, Nie02a, Sho05b, SHJR04].

Computationally [MPSW05].

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

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, Lut02, MYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Tyn05, Cas02, Che05b, DFGH04, Fan09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Sim06, 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, EP03, JP03, LBA00, LKHL09, Lut03, May04, PHM03, Sch06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Wri00, Yan00, YKMB08, Cha07, Che05c, CHT02, DL06, HV09, HKPR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sci05, WLH06, Wli99, YLR05, Lu03].

Compurware [Ano02c].

conceal [BB79].

Concealing [DMS00].

concealment [DA03].

Concept [ARC+01, Ano09c].

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

concerning [HW03b].

Concerns [MP00].

Concrete [KNS05].

Concurrency [JL00].

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

Conditional [LM05, WN02].

Conditions [IK05].

Conference [ACM03a, ACM04a, Ano06b, AAC+01].
AJ01b, Bel00, B+02, BZ02, BS01b, Bih03, Bla03, Bon03, Boy01, Buc00a, CC04a, CV04, CGP03, CGH+00b, Cra05a, D-KU05, DWC00, DFPS06, EBC+00, ELv01, FLY06, Fra01, FMA02, FRu04, FLA+03, HR06, HYZ05b, IEE09a, IKY05, JY04, JM03, Joy03b, Jue04, KJR05, Kilo1a, Kim02, KN03, Knu02, Lai03, Lee04b, LLT+04, LL04d, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Naco1, Nao04, Okao0, Ok04, Pat03b, Pem01b, Pfe01, Pfe06, Pre00, Pre02c, RD01, Roy00a, Roy05, Shi05a, Sii01, SM07b, Sma05, Syv02, USE00c, USE00a, USE01b, USE01a, USE02c, Wi09, Won01, Wri03, Yun02a, YDKM06, ZJ04, Zhe02b, ZY03, AUW01, BC05c, DV05, DWML05, DR05, Hon01, Kil05, Li05, PC05a, PY05, PPV96, QSO0, Son00, WK06].

Confidences [Gan01a].
Confidentiality [Dwo03, Pem01a, YC08].
Configurable [MBS04].
Configuration [Sha02, Mos06].
Confirmation [SK00].
Confirmer [CM00, GM03].
Confiscation [DBS+06, Hei07, Rub01, Sch07, SVEG09].

Conformance [LBR00, RSA00].
confounded [Bel07a].
confusion [She01].

congestion [Un00a, Uni00b, Uni00f, Uni00e, Uni00h].
congruences [Ste08].
Congruential [CS05b, LS05a, SB05].
conic [LW09, LCC05, LC205a].

Conjecture [CU01].
Conjugacy [CG03a].
Conjugate [Igl02].
Connected [BJL02, Hé01].

Connection [HR00, Jam00, Goo00, Mic02b].
Connection-Polynomials [Jam00].
Connections [WRW02].
Conquer [SKQ01].

conscious [DM09].
Consensus [CNV06].
conservation [Che05b].

Considerations [DVS+06, Hei07, Rub01, Sch07, SVEG09].
Considering [WA07].
Consistency [ABC+05, JEZ04].
consistent [RG06].

Constant [App07, BI05a, CS07c, CD01a, DPV04, DN02b, DI05, Lin01c, Sun00a, IK05].
Convergence [CJ04, YW05, YRY05b]. Converging [Ano04e]. 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 [TBJ02]. Copley [USE01b, USE01a]. coprocessing [ML05]. Coprocessor [Gut00, Ito00, LS01b, OTIT01, AV04]. Coprocessors [Smi02]. Copy [LTM+00, Per05b]. copying [Gei03, SV08a]. Copyright [Kha05, LLL02, PBB02, XFZ01, ZTP05, Ano10p, Gil07, HLC07, KA09, Kwo03a, Rec03]. CORBA [TEM+01]. Core [BF00a, Dim07, DV08, HMS04, TPS01]. Corfu [SM07b]. Corner [Mar08a, TR09a, TR09b]. corners [Bh09]. Corporate [HW01, KH03]. Correcting [MZ02, NN06, YYDO01, ZYR01]. Correction [BQR01, CTBA+01, Din05, LN08, LW05b, MPSW05, SKQ01, TEM+01, Gar04]. Correctness [PBB05, Bel07b, HSD+05, dH08]. Correlated [FWW04]. Correlation [BSC01b, CJS01, Gol01c, JJ00d, LV04, LMV05, MH04, Ny01b, SY01a, WRW02, ZC00, GG05b, J02]. Correlations [KM00, KM01b]. corruption [XNK+05]. COS [FF01a, WB02]. Cost [CDF01, FBW01, PD07, Sta05, YEP+06, CL09, SHJR04, SK03, YLR05]. Cost-Effective [PD07]. cost-ineffectiveness [YLR05]. Could [Min03, Cla00b, Pau02b]. Count [Che07b]. Counter [DIS02, QS01, SLG+05, SL06, MMJ05]. Counter-Measures [QS01]. Countering [PP06b, SK05b]. Countermeasure [IIT03, MMMT09, OT03a, PKBD01, YKLM02a]. Countermesures [Ava03, Fry00, GM00b, MOP06, OST05, Has01b, JD01, Man08, OST06]. Counters [KMO01]. counterterrorism [Na05]. Counting [Gau02, Kuh00, Hig08]. Couple [SXY01]. coupled [LF03]. Course [Mc04, AA04b, GV09, GL05]. courses [Gha07]. Cover [GA04, Gut02a, LNP02, NN03, RS00]. coverage [DS00]. coverings [SC02b]. Covert [Col03]. Cozens [Sal03b]. CPCMS [Sha02]. CPI [ECG+07]. CPN [AADK05]. CPOL [BZP05]. CPUs [ESG+05]. Crack [Sin02, Ano08b, Min03]. Crackberries [Sta05]. Cracked [AAD+00, Nic01, Pri00]. Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZL01, BZ03, Cur05]. Crackproof [Sal03b]. Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZL01, BZ03, Cur05]. cracks [Bar00a, Ste05c]. Cramer [Luc02b, VMSV05]. CRC [Kat05a, Spr03, Was08a, SGPH98]. Creation [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 [One05]. Cropping [SFH00]. 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, Ano07a, BDG+01, Bao04, BLH06, BP03a, BBK03a, Bar06a, BP01a, BD00a, Bih00, BFM02, BD02a, BDK02b, BSW01, BDD03, BD00b,
WBL01, WC01b, You01, Zha08, ÁM04, ÁCTZ05, ALV02, AV04, BGB09, BDSV08, Bla01b, BP05, BG08, BG09, BDNN02, BD04a, BGL+03, BMV06, BR05, Can01a, Can06a, CHC04, Coh03, CC05d, CDL06, DP04, Dug04, DFG00, FS03a, FSGV01, GT00, GPV08, GJ04, GM04, GO09, HW03c, HY03, IK03, IK06, IYK02, IYK03, JW01, KAM08, KS05b, KP03, LGK010, LA05, LLW05, LLW09, ML05, Mea04, MT07, MS02b, MRST06, Mon03, NN03, NdM04, NdM06, PS04a, PSG+09, PR05, Pre07, Pri00, Puc06, QPV05, Reg03, encryptographic [Reg04, Ren09, RMH04, RBF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, TNG04, kWpLwW01, WLW04, XLM06, YLT06, ZL09, ZWWL01, ZL04b, dH08, BWBL02, JQ04, KKP02, KP01, KN01, RS05].

Cryptographically [ADD09, AHS08, BCGH11, BFCZ08, BB06b, FR08, MS02b, PLsLvLE10, RGX06, Aam03, AW05, AW08, Lau05, SM02a, SM03a].

Cryptographically-masked [AHS08].

Cryptographic [RSA09a].

Cryptographically [RSA09a].

CryptoGraphics [CK06].

Cryptography [ANS05, AF04b, ADI09, AA04b, An00e, An001], An002b, An002f, An002h, An005a, An007b, An007a, AAFG01, AIK04, AIK06, App07, AEAQ05, ABM00, Bai01a, Bai01b, BINP03, BD02, BOV03, BOV07, BBGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BWBL02, Bla02b, BDDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, BK006, BKM07, Buc00b, BD08, BP01b, BRTM09, CPS07, Cer04b, CCL09, CSW+08, CSQ01, CP06, Cob04, CFA+06, Cop00, Cor06, Dr.00c, Dam07, DFS08, DFS05, Das08, D000, DFG04, DK02, DK07, Des02, DT03, DY09b, DSS01, DD00, DDDN03, DDD03, Dre00, DP08, EPP+07, EP05, Elb09, ElI04, ECG+07, Ett02, FS03a, Gal01, Gal02, GHK+06, GKK+09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Grot01, Gro05, HR06, HH04].

Cryptography [HHM01, HMV04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irw03, IH04, IKOS06, IKOS08, JYZ04, JL00, JTT01b, JTO1a, Jue04, Kak06, KLR09, KZ07, KG07, Kat05b, KK06, KBM09, KPMF02, KD08, KIS02, KWP06, Lam01, LGS01, LSY01, Lee03b, LL+01, Lie05, LDM04, LW05b, LP02b, Lut03, LYS08, MNT+00, MP02, Ma01, Mao04, MS01, MZ04, Mat01, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02c, NH02, PV06a, PY06, Pe06, PM02, PBB02, Poi02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGK08, Sti95, Sti01, Sti02, Sti06c, SJ05, Sy02, TSO00, TW06a, TG04, TMM01, TW02, TW06b, Tro08, TR09a].

Cryptography [TR09b, Uni01, USS02, VY01, VMC02, WPS01, Wei04, WK01, Wei05, Wie00, WdV02, Wri00, YWC08, Yrt06, YC01, YDKM06, ZH03, vDW04, Imm03, AM07, AHC17, AN03, AU001, An02a, An02g, ABD01, Ber09b, BBD09, Bis03a, BSS04, Bla03, BD00, BCD06, BEZ00, BEZ01, BGM04, BEM+07, Buc00a, Buc01, Buc04, BLR09, BMA00a, BMA00b, BMA00c, CCT08, CJ03c, CDFM05, CDD07, Cos00, Cre00, DDR04, Dif01, DIM08, DwWMW05, DOPS04, DLK09, DW09, Duw03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK+07, Geb04, GRTZ02, Gol09, GGM05b, GHPT05, GNP05, GNP05, HH05, HHM+00, He03, HKPR05, HA00, Hig08, HK500, Hoo05, HG05b, HLwWZ09, IZ00, IM06, JKO01b, Jan08b, JMV09, Joy00, KZ03, KL08, Kat01, Kil05, Kim01, Kob00, Kra07].

cryptography [Lan00c, Lee04a, Lin01a, Lop06, Mau04, May01, Me08, MBS04, MM07a, Mol07, N02a, Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00,
Pin06, Pip03, Reg05, Reg09, Rot02b, Rot03, Roy00b, Rup09, STY07, Sch02, Sch04d, SBZ04, Ser06, SH05, Shp99, Sil05, Sin00, Sno04, ST01d, Sti11, SK01b, TW05, UHA +09, Van03, Van05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wri03, YC09a, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Reo01, Wa00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08, Ros00b.
cryptography-based [FXAM04].
Cryptologic [BS00a].
Cryptological [Lew00].
Cryptologie [dL00].
Cryptologis [WD01b].
Cryptology [Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Kun02, Lu03, LL04d, Lut02, MMV06, MFD04, Neu04, NS01c, Ngu01, Oka04, Po05, Rot05, RS02, Sha03b, Zhe02b, Dl00, Bau00, Bau07, Bel00, Bih03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kii01a, Kim02, Lam91, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, PC05a, Pi01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sho05a, Son00, Won01, WK06, Yun02a, vT00, DWML05].
CryptoManiac [WWA01].
Crypton [CKK +02, MG01].
Cryptosystem [BST02, FL06, GG01, Gk05, GH01, Hug02, KM01a, KY02c, KLC +00, LHT09, dVP06, Luc02b, NSKN05, NBD01, Ove06, PHK +01, YG01a, YG01c, Zhe02a, Zho06, Bau04, CL02b, CCH04, Che05a, Cho06, CFVZ06, CHH01, Dan02, DHL06, EKRMA01, GhdGSS00, GS01, GC00b, GMW01, Henc06a, Iwa08, JW06, KY09, LL04c, LL06, LKYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SP02, SCS05a, SP79, SLC05, Sun00a, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, YC09b, yH08].
Cryptosystems [Aki09, Ava03, BDG +01, BKL02, BPS00, BMM00, CHS02, CCW02, DDG +06, DKXY02, ESG +05, FJ03, Fel06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KKY02, KII01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vad03, Wya02, XB01, ZLK02, Ban05, BF06a, BB79, CHC01, CMKT00, EBS01, EHHK04, GH08, GBKP01, HM00, Has00, Has01b, Hii00, HP01, KWW00, Kos01c, LL04b, LD01, Luk01, Mic01, Mis06, OS00, Pe09, PLJ05b, SST06, Sh05c, Sma01, TO01, TC05, Ts05, Ver01, Why05, Wol04, WPP05, WW00, YY00, ZS01, yT01].
cryptovirology [YY04].
CRYPTREC [IY00].
CSCW [ZP05].
CSP [SBS09].
CT [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09].
CT-RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09].
CTO [An03g].
CTS [Con00].
Cuban [AJ08].
Cube [DS08, PDMS09].
Cube-Type [PDMS09].
culture [Gil07].
Cumulative [LG04, WP03].
cure [RD09].
cure-all [RD09].
Current [An03b, DFH01, PRS04, LPW06].
icumulieren [FOP06].
Curve [ANS05, ADI09, An00a, Ava03, BINP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BMN01, CQS01, CFA +06, GPP08, HYZ05a, HHM01, HM04, HRC02, JI01a, JI01b, KMM09, KMP02, KSP02, KWP06, LW02, Ml02, Kur03, OTT01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YYY01, ZLK02, BS04, BS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHKH04, GBKP01, Has01b, Hsu05a, HL05d, JMV09, JW06, LL04c, LWL09, Mis06, OS00, ST03a, SST06, SH05, Sma01, SCL05, SL05, TC05, Van03, Ver01, Wol04, WPP05, YC09a, YC09b, ZS01, ZL05, yT01].
Curve-Based [KW06, Pel06].
Curves [AHRH08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK +06, Kid02, PWGP03, Ver02, CMKT00, Hus04, LWZ05, MP01b, MSV04, Sil05, Sim02, SC02b, Was08b, Wen03, Yaso8].
customer [Lin01b].
CVS [DFG01].
Cyber [FNRC05, WW04, Mad00c, Man05].
Definitions [YWD08, SNI00]. Definitions [Uni01, AH05]. Definitive [BS01a, BSB05, Gar03b]. Defying [HRS08]. Degenerate [Ber09a]. Degradation [BSC01a]. Degree [CV02, QPV05]. Degrees [Sat06]. Déjà [DP00]. DeKaRT [Gol03]. Dekker [Irw03]. Delacorte [Inr03]. 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]. Demand [KL07]. Degenerate [Ber09a]. Degradation [BSC01a]. Degree [CV02, QPV05]. Degrees [Sat06]. Déjà [DP00]. DeKaRT [Gol03]. Dekker [Irw03]. Delacorte [Inr03]. 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]. Demand [KL07].
[Ano04b, BK06b, XNK+05]. **Diagnostics**
[NM09]. **Diagonal** [PJH01, PJK01].
**Dickson** [SZP02]. **Dictionaries** [AGT01].
**Dictionary** [BPR00, BCP02b, CS07b, DJ06, Pho01, NS05a], **did** [MH09].
**Diego** [ACM03a, ACM03b, ACM03c, ACM07, Schö0a, Schö1c, Schö4a, Schö5a, 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, Eke90, Fur02a, Graft0a, HLL+01, HSM+02, HHK+04, IIT03, JT01a, Kan01, KM02, KCP01, LHL+02, MP06, MMT09, MHL+02, MG08, PSC+02, PQ03b, SK01a, SKU+00, SK101, YSD02, vW01, BFS01, CUS08, Che08a, DLP+09, Egh00, EIG01, Eng00, EHK+03, HSZI00, HSZI01, Han00, HS01b, HEHK+03, HW01, HLT01, JBR05, KZ01, Ka01, KC02, Kuhl00, Kwo02, Kwo03b, LTL+01, LLL+01, Lin01b, LWL09, LL01, Lu03, Mad00a, MM01a, MM02, MS01, Me01, PL01, PJH01, PGC01, PZL09, PBM+07, Ram01, RdS01, RS01, Sam09, Schö0d, Schö0b, Sch01, Sha01e, SC02a, Shi08, SLT01, Sug01, TMM01, TJC03, US02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03a, WC04, Wya02, XFZ01, XYL09, YWWS09, YYDS01, YYZ01, ZWC02, Zho02, ZCW04, AAPP07, AA08, Ano00i, Ano01p, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CJ05, Che07a, Che00b, Die00, FB01].
**digital** [GGK03, Gil07, HRL09, HLC07, HLH00, HHC05, KP00, LG04, LG09, Lev01, LL06b, MKY08, NR00, PC05b, PLJ05a, PBV08, QCB05b, Re03, Sh01d, Sh04b, Sha05d, SCL05, TCC02, TND+09, UP05, WNQ08, W HLH03, WC05, X505, XMST07, Ano09b, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].
**Digital-Audio** [WNY09].
**Digital-Signature** [Eng00].
**Digits** [Che04b, Ran55, Ran01].
**Dimension** [DDG+06, TZT09a, TZT09b].
**Dimensionality** [SBG02].
**dimensions** [CLR09].
**Dining** [KL+06].
**diplomacy** [Alv00].
**Direct** [BMW05, KG09].
**directional** [PJK01].
**Directions** [Sh01b, DHF01].
**directly** [JZW05].
**Director** [Mad04].
**directories** [C+02, Pet03].
**directory** [C+02].
**disabled** [Pau02a].
**disadvantage** [CDS07].
**Disappear** [Per05a].
**Disappearing** [Way02b, Way09].
**disappointed** [Ste00].
**Disaster** [WCZ05].
**disciplinary** [SM08].
**disclosure** [JM07, Swi05].
**Discover** [Eva09].
**Discovery** [Bi09, HLL+02, SBG07, SGA07].
**discredits** [Ano09c].
**Discrete** [CS03a, CNS02, Che04b, CCW02, Gen00b, GV05, GPP08, KC09b, LW02, LJL05, VK07, HNO4, HW03a, HWR09, Hue05a, HH05d, JL03, JLL01, LHL03a, LL04b, LH05, LTH05, PLJ05a, QCB05a, Sch01e, Sha05c, Sh05d, SWR05, SCL05, SLC05, SCS05c, Ysa08].
**discretized** [MA02].
**Disruption** [Har07b].
**discursive** [Mit02a].
**Discussion** [Ano01a, Ano01b, Ano01c, Ano01j, Ano01n, Ano01l, Ano01o, KB+02a, Mal02, Nik02b].
dish [Ano01]. Dishonest [GKK007].
disjoint [Gut04c]. Disk
[Cro01, Har07b, Siv06, CS08a, Fer06].
dismantles [Hi06]. dispatches [Kee05].
displayed [CGV09]. Displays [Kuh02a].
Disputed [CAC06]. Distance
[CGFSHG09, CPhX04, DM07b, DW01].
distinguished [HWW04, WH02b].
Distinguishers [HI04]. Distinguishing
[HSR+01]. Distortion [BGI08, CS05c].
Distortion-Free [BGI08]. Distortions
[HH09, SF01]. Distributed
[BCS02, BT02, CLK01a, CS08b, CD01a,
DS03, EP05, FM02a, FS01a, GJKR03,
GSVC02, GTH02, LLY06, SFC01, WTO2,
And08b, AFGH06, BDET00, CO09b,
FM02, KKL09, LN04, LLLW08a, MSP+08,
PS08a, RaJ06, WZB05, YJH04].
Distribution [BDF+01a, BOH04a,
BBB+02, BGM09, BNS00, FS01b, Ina02a,
Ina02b, Kr02, LLL02, NA07, Sch01a, YI01,
ATS04, Asl04b, Bad07, CYH04, CDD06,
GL06b, MP08, SLP07, Shp01, Shp04b, SY06,
WHHT08, YS04, ZLG01].
Distributions [Cy08]. Diversity [Kun01].
Divide
[SKQ01]. Division
[HZSL05, KKY02, Tan07a, Che08b, MN14].
Divisor [KM01a]. DL
[HRL09, PLJ05b, Sch01f, Sch01e, WMDR08].
DL-based [HRL09, PLJ05b].
DL-encryption [Sch01f]. DL-keys [Sch01e].
DL-STD-M [WMDR08]. DLP [MSV04].
DM [Eag05]. DNA [AEH17, GPX08]. DNF
[BGN05]. DNS [Her09b, Kle07].
DNS-based [Her09b]. DNSSEC [Gue09].
Do [Bur06, HSR+01, HR04b, Win01, BB79].
Dobb’s [Dr.00c]. Document [ISO05,
PJR01, ST01c, VHP01, CDS07, CL04c].
Documents [PJ01, AW05, AW08,
DKG+04, GA03, ÜG08].
dodging [Phi06].
Does [AB01, Pie05, COn09, Wal04].
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,
EKRA01, Zir07]. Domains
[BR01, CLK01a, CLK01b, Vau01].
Dominic [CKN06]. Dominic [Rot07].
Dominica [PY05]. domino
[LLLZ06, LLLZ06b]. don’t [Win05c].
Don’ts [FSSF01]. DONUT [CLL00].
Door [SF07]. Doors [Eri02].
DOS-Resistant [Ano01f, ANL01]. Double
[ADDS06, CY08, CMJ03, Coo02a, DIM08,
GH08, GB09, Hau06, JSW05]. double-base
[DM08]. Double-Gate [Coo02a].
Double-Size [CMJ03]. double-trapdoor
[JSW05]. Dubbling [FV03]. Douglas
[Spr03]. Down [BBPV00, Coo02b, Ano00g,
Ano03d, Ano03a, Pot03, PBV01, Ste05c].
Downwards [FV03]. DPA [SGB01, TV03].
DPA-Based [SGB01].Dr [Ano03g]. Dr.
[Dr.00c]. Draft [Mad00b, Ste00, Dwo03].
drastic [Sug03]. drawn [vOT08]. DRBG
[Hir09]. Dress [Alm08]. drinks [Ano03d].
Drive [NP07, Kor09]. DSA
[MR01a, SA02, Sha01d, TvdK+01].
DSA-type [Sha01d]. DSEA
[LLLZ06a, LLLZ06b]. DSP
[Geb04, WWGP00]. DSP-embedded
[Geb04]. DSPs [WWGP00]. DSS
[Ano00b, Ano13, FIP00, Nat00]. DTD
[PCK02]. Dual [HLC07, KHY04, LKLK05,
SF07, WCJ09, ST03a]. dual-field [ST03a].
Dual-Pair [WCJ09]. Dual-Tree [LKLK05].
Dual-wrapped [HCJ07]. Dumb [Eri01].
Dummies [Cob04]. Dump [KCJ+01].
Dunaynir [MAaT05]. d’une [Caf00].
Durahim [MAt0x]. Durahim’s
[MAaT04].
during [AJ08, Bec02, WA07].
Dust [KGS07]. Dutch [dL00]. Duty
[ZGLX05]. DVD [Ge03, Per05b]. Dwork
[DNRS03, GKL05, Zha06]. DWT
[LHS05, PBC05]. DWT-Based [LHS05].
Dynamic [AFB05, BNP08, BCP01,
BCP02a, BFM07, CL02a, CW09, CCD+04,
dynamic-key

E-business [Poh01, HHSS01].
E-Commerce [Kir01a, TM01, BM03a, Gra01, SN07, Sta00, MY01]. E-Goods [NZCG05].
E-Learning [CAC06]. e-mail [Che01f, LL04c, NZS05, Smi03, All06, ANR01, KSS00, Law05].
e-payment [Has02]. E-Security [NDJB01].
E-smart [AJ01b]. E-Vote [Che07b]. e-voting [CJT03, Cha04]. E-Wallet [ETZ00].
E2 [SKU +00]. Early [ASW +01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Cal00d, Smo04, ZGT05].
Easier [Pau09]. Easy [GR04, Hos06b].
Eavesdropping [Kuh02a, Kee05].
ebanking [WDCJ09]. eBank [Ano02d, WWL +02]. EC [SF07]. ECC [BWBL02, CL09, Mis08, Tsao05].
Eclipse [Coc02b]. ECMA-305 [ECM00a].
ECMA-306 [ECM00b]. economics [Bl07].
ECPP [Che03]. ed [Gum04, Nis03a]. Edge [Sta05].
Edinburgh [RS05, Pem01b]. Edit [CGFSHG09]. editing [MAaTxx]. Edition [Cho08a, Iro03, Spr03].
Editor [Eri01, Eri02, FOP06]. Editors [BK06b, PTP07, SJT09, SKG08]. EDK [An002e].
Eds [Du03, Pag03]. Education [Puz04, RC06, CAC03]. Effect [AEV +07].
Effective [CDR01, PD07, Sen03, SL06]. Effects [BBGM08, Har00, GJ04, SN07].
Efficiency [HI00, GGK05, SLG +05, GT00, GGK03, KT06, YTH04]. Efficient [ACS02, ABRW01, AEMR09, BCGH11, Bai01b, BINP03, BKLS02, BR00a, BGHP02, BSV08, BGK +03, BS00a, BF01c, BGH07, BB00b, BCDM00, CKP01, CL02a, CCMT09, CCD07, CL01b, CPF04, CM05a, CJT02, Chi08a, CJL05, CT08b, CCK03, Cou01, Dam00, DN03, Dhe03, FF00, Fis05, FS01c, GLV01, GC01b, GTH02, GST04, GKP01, HCJ02, HSZ01, Has01a, Hl04, HS00, HW04, HZLS05, HL07, Hü00, HS07, Jua04, K0Y01, K0Y09, KLY02, KO03, KHD01, KKH03, LSY01, LCK01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, MN14, Nd05, NSN05, OS01, PCS03, PB005, Ram01, RSQL03, RDJ +01, SM01, SM03a, SW06, SRQL03, SSNGS00, Tsao08, TC05, WHL05, WY05d, WH01, WC01a, XB01, XS03, YWD08, YL05, Zan01, Zho06, ACTZ05, AFB05, Bla01b, CC04b, CC05e, CY05, CHC05, CLC08, D09].
efficient [Dew08, DwWmW05, FP09, FSV01, HH06, HC04a, JW06, KHYM08, LPV +09, LLS +09, LCK04, LHC04, LYL02, Mic02a, MSP09, NR04, PCC03, RG05, RBB03, SLP07, SKW +07, Sha05b, SC05a, WK05, XC05, Yau02, YTW05, YC09a, ZNS05, ZY07].
Efficiently [IKPN03, NNT05, AGKS07]. effort [Weh00].
efforts [Pau02a]. Eggs [Wei06, Wei05].
EGPGV [MFS +09]. Egypt [EBC +00, Im03, Sin00]. Eighth [ACM06, B +02, ELs01, EIE01b]. Einstein [HR13, MNT +00].
EBJ [TE01]. Ekert [Du03]. ElGamal [EKMA01]. Election [JLL02, Cal00b].
Elections [Cha04, PVS01]. Electrical [Wal04]. Electromagnetic [GSM09, Q301].
Electronic [Ble07, CLK01b, CM02, Dor01, H001]. ISO05, JY00, K0M01, KS02, Lan04b, LLL02, Mad00a, MNFG02, Rub01, RMCG01, Str01a, YKMY01, ZYM05, AvH00, AAKD09, Cal00a, Cas03, EY09, FB01, HJW05].
element [MS02d]. Elementary [Sin09, Ste08, Tat05].
Elephant [Fer06].
Eleven [All03]. ElGamal [BJN00, CL02b,
CWH00, HL04, LHT09, SJ00]. ElGamal-like [CWH00, HL04]. Elizabeth [Bud06]. Elliptic [AD09, Ano05a, Bai01a, BINF03, Bar00a, BBGM08, BMBM00, BS01d, BMN01, M"ol02, Kir03, OT1T01, OS01, OT03b, PWG03, RSA03b, RS04, RS01, Sat06, Sil05, Was08a, Was08b, WPS01, XBO1, YYZ01, vT01, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, Dlm08, DwWinW05, EHH04, GKP01, Hsu05a, HL05d, JMV09, JW06, LL04c, LWZH05, Mis06, MS00, ST03a, SSS06, SH05, Sim02, Sma01, SC02b, SLC05, SLC05, TC05, Van03, Ver01, YC09a, YC09b, YC09b, Yas08, ZSS01, ZLO5, ANS05, BWBl02].

Ellis [Coc01a]. Elmau [IEE01b]. Else [FL01b]. elude [Che01f]. EMA [QS01]. Email [ES00b, Gar03a, Her09b, Luc06]. Email-Based [Gar03a]. emanations [ZZT05]. Embedded [An001c, An002d, An002e, BBGM08, Dri02, DV08, GSS08, JT05, JQ04, KKP02, LPW06, NdM04, RS05, SPQ06, WK03, YSS+01, ARJ08, BGM04, Fox00, Geb04, KV0+9, KP01, KNP01, KPO3, MS04, Nis03a, TKP0+8, QEM07, Fin02]. Embedding [Akk09, JX05, JG07, LSC03, Sal03b, WY02, WC04, CO09a, KC09a, Wan05]. Embrace [CNB+02]. Embracing [An003d]. EMD [B006]. Emperor [Smi01b]. Empirical [HW03b, Goo00]. empirically [SS03]. employee [You04]. Emptiness [DIS02]. Emulex [CZH01, CTBA+01]. Enabled [Por06, CCCY01, DY09a]. Enabling [Web02]. encapsulation [CHH+09, KG09]. Encipher [BR00a]. Enciphering [HR03, KT01]. Encode [BR00a, BK04, An008c].

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, BBGP02, BGLS03, CD01b, Hug04, Lan04a, LH07, MMZ00, NNAM10, RMCG01, Sta02b, Vau01, WRW02, Whi09, Woo00, AMB06, Ano06a, Bih02, BNP08, CCMT09, CDD+05, CSK+08, FJ04, HLM02, Hes04a, LHL04b, LSH0, MW04, Pet03, UG08].

Encrypting [Pr00, RC01, Zho06]. Encryption [ABC+05, Abe01, AS01a, Abe04, AEH17, AP09, AB01, ADR02, And03, An001g, An01b, An01i, Ase02, ANR01, AF06, AF03, Bar00c, II00, Bau02b, BN00a, BR00a, BMM00, BB01, BU02, BF01b, BF03, BB04, BGS05, BHH07, BHR0+8, BB03, BNP03, BD03, BK02, Bur03, Cal004, Cal00e, CDD00a, CS03a, CH03, CHK05, CGPH01, Che01a, CTLL01, Ch08e, Cho08a, CM06, Cla00a, Cob02b, Coo01b, CUN00, CHJ+01b, CDD00a, CS03b, CDD00a, CTLL01, Ch08e, Cho08a, CM06, Cla00a, Cob02b, Coo01b, CUN00, CHJ+01b, CDD00a, CS03b, Cro01, Crr05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL08, DR02a, DA03, DFK+03, DK05, DS05, Dri02, FIP01a, FL01a, GC01a, GS00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HSH+08a, HS02a, HY05a, HSH02, HSH06, HK01, HWW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03].

Encryption [HL02, HG05+03, HLM05, HLC00, IS00, IS00, J00, J01, J02b, JK02c, JMV02, JPK01, Jut01, KB03, KSH01, KS00a, KY01a, Xha05, KK01+07, Kos01a, Kra01, Kur01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LRW07, Lin03]. LNP02, LMV05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, Møl03a, Mor05, Mi01a, MS09d, NIS00, Nam02, NCC05, NZ05, NP02b, Nie02b, PV06b, PM00, Pau09, Pem01a, PZL09, PDMS09, Pha04, Por01,
encryption [Ano00j, Ano02a, Ano03g, Ano06d, App05, Ate04, ACdM05, AFGH06, BP08, BKN04, BR04, BBN09, Ber09a, BBK+03b, Bir07, Bla00, BJN00, Bro05b, CG06, CS08a, CBSU06, CHC01, CKRT08, DZL01, DL07, DRS05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GGK03, Gen09a, Gen09b, GKM+00, Gou09, Gua05, Gut04c, HSH+08b, HSH+09, HS02b, HHYW07, HCD08a, HCD08b, HauR04, HWW02, Hsu05a, Hwa05, HLO5c, HLO5d, IM06, JK01a, JK01b, JXW05, JSCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Küh08, Lafo00, LV07, Lee01, LCP04, LJO5a, LMC+03, LLZZ06a, LLZZ06b, LLC08, LB05, Lu02, Lu05, LK01, LWK05a, Mad04, Man05b, Mat02, Mülo01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pau03, RG09, Rhi03, RB03, RSP05, SN00, SKW+07, Sch00a, Sch01c, S+03, Sch04a].

encryption [Sch04b, Sch05a, Sch01d, Sch01f, SH11, SM11, SR00, SVEG09, Shp04b, SK03, Ste00, SP03, SWH+09, Tan01, TTZ01, TOEO00, TM01, TLH05, Unio00b, UP05, VKS09, WG02, Weho00, WN95, Wlo03, WH02a, XY04, XWSC10, Yan02, YGZ05, YZEE09, YC07, ZLG01, ZLO4a, ZAX05, ZW05b, ZLO5, ZFK04, ZD05, CHK008, CHJ+01a, RR04, Unio00f, Wue09, Jan08a].

encryption/cipher [HAnR04].

encryption/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]. Ended [Küs02].

Endomorphisms [GLV01]. Endpoint [Kad07]. Enemies [DM07b]. Energy [GC01b, Ino05, LPV+09, SL07, MS08].

Energy-efficient [LPV+09]. Energy-security [Ino05]. enforce [SN04]. Enforcement [GN06]. enforces [BP05].

Enforcing [GMM08, HRS08]. Engine [Fri01, MMH02, DP04, SHL07]. engineer [Pau02b, SN04]. Engineering [CNB+02, MNT+00, MYC01, Pem01b, Roy00b, SM07b, TR09a, TR09b, VH09, And08b, EC05, Jen09, Man08, Wa04]. engineers [Pri00]. engines [PM08].

Enhance [ZWC02]. Enhanced [JKRW01, LHL04b, ZGLX05, CZ03, MK04, 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, Chm02, Cop04b, DB04, GO03, Goo00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Thi03, Wil01a, Win05b, Win00]. Enigmy [Kap05]. Enough [CNB+02, Pat03a, Ana03e, YJ00].

Enrolment [HWH01]. Entangled [Bar00c, LB04]. Enterprise [BH00b, C+02, HM05, MJF07, App05, TCR03]. Entropic [DS05b]. Entropy [DS05b, EHMS00, LH07, JRS09].

Entzifferung [Bau08]. Environment [BST03, DeL07, HS01b, LSVS09, IM06, KKL09, KB00, Rhi03, Whi09, ZBP05].

Environmental [PS05]. Environments [CJ04+04, LKHL09, BGM04, MNS08, SBG05, SBG07, SN04, YC09a, YbJ04].

ephemeral [MS08]. Ephemerizer [Per05a]. EPOC [JQY01]. ePOST [MPHD06]. EPR [Ina02b]. Equation [FJ03]. Equations [CP02, DDG+06, GS03, PBMB01].
Equipping [DMT07]. Equitability [DBS01].
Equivalence [Fis01a, LQ08, MSV04]. Equivalent [Fer00, KOMM01, May04, SIR04]. Era [MP00, Unio00c, Bur00, Unio00f]. erasure [PCS03]. Erasure [JL00]. Erich [Bau08].
ERP [LSZ05]. Erratum [AGGM10, Kwo03b, LLLZ06a, McK04]. Erroneous [CH01b, MNT +00]. Error [BBK +03b, BQR01, Din05, KKG03, LW05b, LM02, MLC01, MPSW05, MZ02, NN06, SKQ01, YI01, YYDO01, ZYR01, Zo01, Gar04, LHL04a, YW06]. Error-Correcting [NN06, ZYR01]. Error-Prone [MLC01].
Errors [AD07, AL07, Reg05, Reg09]. escape [Blu09, Fur05]. Escrow [AK02a, Ano01a, CL01a, DBS01, LCK01, ATSVY00, CL02b, LCC05]. Escrowed [PS01b]. eServer [AV04]. ESORICS [dCdVSG05]. espionage [Bud06]. essays [MAaT07]. Essential [Cop04b, Dr.00c, MR02a, MR02b]. essentials [HHL +00, Irw03]. establishing [Kov03, KH03]. Establishment [BM03c, NIS03b, HMvdL07, LF03, SL05a].
Estimation [EFY +05, JX05, KLB +02a, LNL +08, Se00]. ethical [Har05b, Woo05]. Euclidean [CPhX04, CMJP03, CLZ02, WL02]. EULA [WWL +02]. EUR [Eag05]. EUROCRYPT [Bih03, CC04a, Cra05a, Knu02, P601, Pre00, GJSS01]. Eurographics [MFS +09].
Europe [Pag03]. European [AL06, CZ05, KGL04, Pre01, dCdVSG05, Ano00f, Che05b, Die00, Pre02a]. EUROPKI [AL06, CZ05, KGL04]. EV [HTJ08]. EV-C2C-PAKE [HTJ08]. Evaluate [Pre02a]. Evaluating [BGN05, NTW07]. Evaluation [BSC01a, EYCPO0, FS00, FML +03, IKM00, IY00, JJO0a, Kan01, Kir03, SKKS00, BZP05, FXAM04, FS03a, LCP04, MCHN05, RC05, RN00a, RN00b]. Evaluations [LM02].
Evangelizing [Coc01a]. evasion [Blu09]. even [Bih02, OS00, Win05c]. EventGuard [SL05b]. events [BS09]. ever [Fur05].
Everlasting [DR02d]. Every [Che07b, TH01, DKK07, Win05c]. Everyone [Han00]. Everything [CTBA +01]. Everywhere [Ber00]. Evidence [Ver01, Bro05a, HW03b].
Evolution [DF01, Re01, Pa02a, Ro00b, SP02, Sin99, Sin00]. Evolutionary [HI04, MFD04, LMSV07]. Evolved [LMHCETR06]. Exact [Cor00b]. examines [Nis03a]. example [Bla00, GC05, Zir07]. Exchange [BH06, BPR00, BM01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JL08, KOY01, KY03, MPS00, Mac01, MSJ02, Ngu05, VPG01, WC01a, WV01, ZWCY02, BBU +02, BCP07, CLC08, CJWT01, DG06, GL06a, GMR05, HTJ08, KS05a, KOY09, LLM07, LHL04b, LW04, LFHT07, LHC08, LSH00, MS03a, Mis08, WLH06, YC09a, YPKL08, ZYW07, CPP04, CP07, ECM00b]. exchanging [KN08]. Exclusive [GRW06]. Executing [HLML02, LJ05a].
Execution [Coo02]. Exhaustive [Des00c]. Existing [MV01, BDET00]. Expanded [Cho08a, Irw03]. Expander [JMV09]. Expanding [DN02a]. expansible [LLW08a]. Expansion [DN02b, BCD06, HKP05]. expansions [HKP05]. Expected [KL05, RK06, DLP +09]. Experience [Sas07, BCHJ05]. Experiences [MPHD06, USE00b]. Experimental [BG09, CGBS01, OP03, WS02, RSQL03, Snu04].
Experimentation [Hum05]. Experimenting [LSVS09]. experiments [Bru06]. expert [Ano01h, Che05b].
Expiration [MP00, Sch05b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOH05]. exploitation [Eri03, Eri08, KVN +09]. Exploiting [CK06, ETM05, HR00, HM04, ZWC02]. Exploits [MJF07, CSM05]. exploration [SKW +07]. Exploratory [Lut03].
Feel [PM00]. Feeling [Buh06]. Feistel [MYC01]. fetch [HTW07]. Fi
Sty04, Bar03]. Fiat [VS08]. fiction [Ano03g]. FIDES [ISTE08]. Field
FJ03, GC01a, RDJ+01, CKY07, GMG00, Has00, JL03, ST03a]. Fields
[Bai01a, BT02, CU01, Che04b, CQS01, CFS05, HCK09, HMM01, KKH03, Lov01,
MNP01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sim02, Sma01].
Fifth [ACM03b, SM07b]. Fighting
[DGN03, SZ03]. File [CCDP01, GIS05,
Ito01, LK01, BDET00, CSK+08, HTW07,
Hos06b, ISO05, MKK00, MSP+08]. Files
[Tot00, Che02, Lov01]. Filesystem
[Bau02b, Pet05]. Filesystems [WBL01]. Filter
[LBGZ01, LBGZ02, MSNH07, Sar02, CMS08].
Filter-Combiner [Sar02]. Filtered [MH04].
Filtering [SDFH00]. Final
[DPR01, Dra00, GC01a]. Finalist [SB00].
Finally [Coc02b]. Financial
[ANS05, Gri01, Pen01b, Wri03, Bla03,
Fra01, Jue04, PY05, Syv02]. Find [LH07]. Finding
[HI04, HR04b, MP06, WYY05b, WYY05c, ZT03, SW00b].
FINDsomeone.com [Gra98]. Fine [SS01b].
Fine-Grained [SS01b]. Fingerprint
[Ano02d, HHY07, HBF09, KHY04, MMY02, CL04d, MJM03, UEBP09].
fingerprint-based [CL04d].
Fingerprinting [KT01, CTT07].
Fingerprints [TK03, KLY03, Sco04].
Fingers [MMY02]. Finite
[BLST01, BR01, CU01, Che04b, CQS01, HCK09, HWW05, 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, OOP03, PK03, QSR+02, Roy00a, USE00b, Wu99, ZJ04, ZYH03, AJ01a, Cla00b, Coc02a, DV05, LBA00, RH00, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, Lan00a].
First-order [Coh03, KS06b]. Fish
[Fle09, Wei06, Wei00, Wei05]. Fit [CCM05].
Five [SW00a, MS02b, Rot02b, Rot03].
five-lecture [Rot02b, Rot03]. Fix
[TEM+01]. Fixed [AR01, BCCN01, CKN00,
LS01a, Shp04b, SP79]. Fixed-Length
[AR01, CKN00]. Fixed-Pattern
[BCCN01, LS01a]. Fixing [KZ07, KZ03].
FL [Des02, Jue04]. flash [ST06, SGB01].
Flat [SV08a]. Flaws
[Gra02a, SPMLS02, Van02, SL05a].
Flexibility [LP02a]. Flexible
[CMG+01, CLK01b, DGK+04, OT03a,
Tsa01, BA06, KC05, LHY02, WWA01].
Floating [NS05c]. Floating-Point [NS05c].
Flow [BDNN02, ABEL05, FR08, ME08a,
TWM+09]. Flows
[ECM00a, AHS04, Cer04a, Lao08a]. 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, CKM00, LS01a, SLT01, HSW09].
Forgotten [Eag05, Kin01, OC03]. Form
[ADI09, CH07c, OS01, LKY00, Mic01].
Formal [BGB09, Bel07b, BCHJ05, BCJ+06,
CL05, DKS08, GOR02b, HG03, Lan00d,
Mea01, YWD08, ABHS09, JW01, Mea04,
Pau01, SW02, ZLX99, ZL04b]. Formalizing
[HM01a]. Formally [JB02]. format
Fundamentals
[And04, PHS03, Shi08, Way01, vT00, Fin03].
Funds [Coc01a]. Further [JS05, JPL04,
LL04a, LL05c, Ano09c, MP07, YRY05a].
Fusion [KZ09, TZDZ05, ZS05, BG09]. fusul
[MAaT05].
Fusion [KZ09, TZDZ05, ZS05, BG09].
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,
HCBELETRG06]. game-like [Gou09].
Game-playing [BR04]. Gamers [TMW+09].
Games [KN08, HCBELETRG06]. Ganesh
[For04]. Ganzúa [GPG06].
Gap [OP01a, PWGP03, RW03a, Sch02, Sch04d].
Gap-Problems [OP01a]. Gate
[Coc02a, GC01a]. gates [TWm+09].
Gauging [PvS01]. Gauss [KHH03].
Gaussian [EKRMa01, JLM03]. Gbps
[TP05]. GCD [JP03]. GCD-Free [JP03].
GCM [KSe09a]. geeks [McN03].
Geheimsschreiber [Joy00, UW00]. GEM
[CHJ+01a, JMV02]. gens [Six05]. General
[AB09, CD00, DNO0a, ESG+05, GMP01b,
Kog02, Lin03, MND+04, Sal01a, YCO1,
HCBELETRG06, IY06, JLM03, LJ05a].
General-Purpose [ESG+05].
Generalisation [DJO1]. Generalization
[YY01, HWW02]. Generalizations
[LD04, LS08]. Generalized
[KRS02, Mic02a, TC01, TJ01a, Wag02,
WHLH05, Elh08, LKYL00, LWW09, Shi05].
Generate [HSH+01, Wer02, FSGV01].
Generated
[ADD09, MRL+02, XXYYX11, RBF08].
Generating
[BMK00, BCDM00, GGO1, MFK+06, SS03].
Generation [ACS02, BCGH11, BH05,
BK06a, CS03c, ESG+05, GJKR03, GL01,
GW01, JG01, MR01a, Ram01, TL07, TV03,
WP03, WHLH05, Web08, WS02, Ano04f,
BK07, BG08, BF01c, ISTE08, LS05b,
TNG04, Van03]. Generator
[ADD09, BP01a, DI05, Dix03, DGP07a,
DGP07b, DV08, EHK+03, Gen00b, GM02a,
Gol01c, GPR06, Int03, Kel05a, Kel05b,
LMHCETR06, LV04, NNAM010, SXY01,
SDF06, TWNA08, TZT09a, TZT09b,
ZKL01, Aam03, ACMT05, Bel08, BG08,
BG09, BG07a, CFY+10, DGP09, GB09,
HG05a, HLwWZ09, JAW+00, KH08, KSF00,
LGKY10, MRT10, Pan07, PSS+09,
PLSvdLE10, PSP+08, PC00, RGX06, SH11,
SM11, SR07, SB05, UHA+09, WW08,
XSWC10, VKS09]. Generators
[BST03, BK06a, BL08, CF01b, CSM05,
Fin06, Kra02a, LBGG01, LBGG02, LS05a,
MH04, RSN+01, Vav03, BK07, BPGPS05,
CO09b, Sti11, SK01b, Ts06, YZEE09].
generators-part [SK01b]. Generic
[BN00a, DOP05, GGTK05, HLH05, Mar02b,
MV01, GT00, MP08, Sch01f, Sch01e,
XLMS06, CHJ+01a]. Genetic [SHIR02,
LMHCETR06, CV05, SCS05a, WIP07].
Gennaro [Miy01].
Gennaro-Krawczyk-Rabin [Miy01].
gentle [RR03a]. Gentry [Hes04a]. Genuine
[HR13]. Genus [CY02, GHK+06, Wen03].
Geometric [GTTC03, HH09, LLS05a,
LL05c, LJ05b, SDF06, CJT01].
Geometrical [LWS05]. geometry
[PPV96, WW06]. George [Gum04].
Georgia [IEE09b]. German
[Sch09, Ano04c, Baut08, Lin02, Mor05,
Sal00b, Sal00a, Win05b]. Germany
[DRS05, Duw03, FLA+03, WKP03, IEE01b].
Gesichte [Sch09]. Get
[Coc01a, WD01a, Cla00b]. gets [Bor00].
Getting [Kar02, PM00]. GF
[BINP03, KP002, KLY02, KKK02]. GH
[GHW01]. GHS [Hes04b]. giant [Lam07].
Gibson [Ove06]. Giesbrecht [CHH01].
Gigabit [CBGS01]. Gigabits [HTS02].
Give [CNB'02]. Given [Wal03]. Giving [Tee06, Wu01]. Global [Ahn08, LWS05, Por06, Ano00h, BK00, Kee05, KB00].

Globus [MJ01]. GN [SC05b]. GN-authenticated [SC05b]. Gnana [For04]. GNU [Coc01a, GnuPG [JKS02, Sti06b]. GNY [Tee06].

Goals [AH08, LWS05, Por06, Ano00h, BK00, Kee05, KB00]. GLOBUS [MJD01]. GN [SC05b]. GN-authenticated [SC05b]. Gnana [For04]. GNU [Coc01a, GnuPG][JKS02, Sti06b]. GNY [Tee06].

Goals [PHM03, Phi06].

Gold [Boy01, For04, Tsa07]. Goldreich [Kat05b, Lee03b, Puc03, AC02]. Gong [GG01].

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

Goodness [CMB'05]. Goods [NZCG05].

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

GOST [SK01a].

got [Car01].

Goubin [Sma03b].

Governance [TPPM07].

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

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

GPT [Ove06].

GUI [LG09].

Guide [Ano06c, BS01a, BSB05, BCP03, BP01b, HMV04, Poo03, Vac06, Wei04, And08b, Bon00, Bro05b, C+02, Che00a, Gar03b, Kov03, Lun09, Mol05, SL06].

Guidebook [SEK01, SEK02].

Guided [ZY08, Pet08].

Guidelines [MMZ00, Die00].

Guildford [KN03].

Gummy [MMYH02].

Guo [LLLZ06a, LLLZ06b].

Gutmann [Uzu04].

H [Was08a].

H.R [Unio0d, Unio0h]. H.R. [Unio0a, Unio0c].

H64 [GMM01].

Hack [MYC01, Sin02, SL06]. hacked [Ano02c].

hacker [Go08, Har05b, Woo05].

HACKERS [SEK01, SEK02, Ano01i, BD04b, NRR00, Win05c]. Hacking [Eri03, Eri08, Gum04, Man08, MSK03, SSS06, VGM04, Puz04, Har05b].

hacks [Sti06b, Sti06a].

Hadamard [HHW05].

Hagenberg [Jef08].

Half [HS02b].
Half-encryption [HS02b]. Halfspaces [KS06a, KS09b]. Hall [Bar00c, For04, Kat05b, Was08a, MAaT05]. Hall/CRC [Kat05b, Was08a]. Hallmstad [BS01b]. Hamming [GK02]. hamper [Lov01]. Hand [WBL01]. Hall-and-CRC [Kat05b, Was08a]. 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, Lai07, CGHG06, GPV08]. Hard-Core [HMS04]. Hard-Disk [Har07b]. Hard-Line [Lai07]. hard-on-average [CGHG06]. hardcore [Sch01c]. hardcover [Eag05, Pag03, Top02, Pap05]. hardening [Mos06]. Hardness [CHS05, CNS02, KY02b, KS06a, LFW05, SV08b, AGGM06, KS09b, SU07, AGGM10]. Hardware [Ano02b, Ano07b, Ano07a, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG+02, Gro01, GP08, IKM00, ISW03, JQ04, KPK02, N05, P01c, RS05, RS04, SOTD00, SMT01, SM02, SM03b, SRQL03, SGK08, TSO00, TBL01, WKP03, WBRF00, X03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK+03b, DS09, EHKK04, GC00a, HBC+08, KP01, KNP01, KP03, NDM04, RAL07, SOIG07, VS08, W0104, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07]. hardware/software [ARJ08]. Harley [WPP05]. Harn [GG01]. Hash [Ano08d, Ano12, AEMR09, BBKN01, BRS02, BKS09b, 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, LKH02, LKY04, LW04, MS09c, Mic02b, Tsa08, Wag08, YR04, FIP02a, ZW05a]. Hash-based [BDS09b, KCL03, Ku04, KCC05]. Hash-CBC [BBKN01]. Hash-chaining [CBR05]. 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-SP [MP07]. HCI [YKMB08]. head [RFR07a, RFR07b, RFR07c]. headlines [H06b]. Health [Mad00a, Ano03a, CYY01]. health-care [Ano03a]. Healthcare [BTTF02]. heap [ST06]. Hearing [Uni00c, Uni00g, Uni00b, Uni00f, Uni00h]. hearings [Uni00b]. heart [Mur06]. Heavens [Eva09]. Hedges [Sho06b]. Hedged [BBN+01]. Heimdal [WD01a]. held [Buc00a, PPV96, Uni00b]. Hellman [K04a, AB01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKR05, FS01b, GR04, Kil01b, KK02, Kra03, Kra05, Mis08, Tsa06, YR05c]. help [Ano08a]. Helped [Gan01b]. Helps [DF01, Pri00]. Helsinki [Bur00]. Hensel [CNS02]. Her [Bud06]. Here [Bur06, Law05]. Hermite [Mic01]. heroes [OC03]. Herriot [Coc03]. Hersonissos [ACMO1a]. Hessenberg [SSFC09]. Heterogeneous [BCS02, H010, KHY08, ZBL05]. heuristic [SS03]. Heuristics [HR03]. HFE [FJ03, CHH01, Fel06]. HFE-Cryptosystems [Fel06]. HIBE [CS07c]. Hidden [HGN03, KW03, LNS02, Six05, GMR05, Lue09, Shp05, FJ03, Sch09]. Hide [CC06]. PH03, Shp05]. hide-and-seek
Hiding [BD03, CLT07, Col03, DN02b, GA05, HNO+09, LH05, LS08, MH05, MMT09, VDKP05, WC03a, HR07, JDJ01, KP00, RSP05, Way02b, Way09, YCL07]. Hierarchical [HC08]. Hierarchical [GS02b, HNZI02, HL02, Lin01a, MN01, YLH05, BD04b, Che07a, CJ03c, JW06, KAM08, WC01b, hY08]. Hierarchies [AFB05, Cer04a, HY03, WL05]. hierarchy [CLK04, CMdV06, HW03c, Hwa00, JA02]. Hierocrypt [OMSK01]. Hieroglyphs [Wri05]. High [ACM01b, Ano00d, Ano02d, ChLYL09, CW09, CJL06, CGJ+02, DS05b, FZH05, Gro01, HNZI02, HV04, Int00, JKRW01, KMM+06, Ken02b, KM05, KB00, Kra05, KT01, MM01b, NFQ03, RW07, SKKS00, SOTD00, SM02, Wie00, WWGP00, YKMY01, Zhe01, BVP+04, BZP05, BGL+03, Jen09, KC09a, SK03, Uni00f, WWTH08, YKMY01, RW07, BGL+03]. high-assurance [Jen09]. High-Bandwidth [CGJ+02]. High-Dynamic-Range [CW09]. High-End [SKKS00, WWGP00]. High-Performance [Kra05, NFQ03, BZP05]. High-Speed [Ano00d, Ano02d, Gro01, JKRW01, KMM+06, SOTD00, SM02, Wie00, YKMY01, RW07, BGL+03]. High-technology-crime [KB00]. High-Throughput [HV04]. Higher [CV02, KCP01, BF01a]. Highly [CV02]. hijacking [Ste05c]. Hill [Gum04, USE02a]. Hilton [KJR05]. HIPAA [AEV+07]. histograms [CO09a]. historic [Pet08]. Historical [RE02, MWM01]. History [BP03b, Ifr00, Pag03, Sal01a, Sin01b, CAC06, Top02, dLB07, AJO8, Boo05, HSW09, Jan08b, KNS05, Na05, Nis03a, Pin06, RIs06, RH00, RO06, Wil01a]. history-based [KNS05]. hit [Bjo05a]. HMAC [FP02a, DGH+04, Hir09, RR08]. HMQV [Kra05]. Hoare [dH08]. Hoax [CZB+01, CTBA+01]. hoc [BSS02, Cha05b, DHMR07, KH05, KVD07, LHC08, LKZ+04, PCSM07, SLPG07, TW07, WQ02, ZC09]. Hold [PM00]. Holier [MYC01]. Holistic [RM02]. Homage [JP02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03]. Homegrown [Str02]. Homeland [Man02, Mau05, RR03b]. homogeneous [MF07, PS02a]. Homomorphic [AS01a, Aki09, CDN01, DN03, HS00, Cho06, Gen09a, Gen09b]. homomorphism [CKN06]. homophonic [Sav04]. Honeynets [Dim07]. Hong [B+02, ZJ04, Cla00b]. honor [OC03]. hook [JEZ04]. hooks [GJJ05]. hop [NC09, ZSJM07]. hop-by-hop [ZSJM07]. Horizon [Coc02b]. host [Sla06]. hostile [ABB+04]. Hosts [H601, SZ08]. Hot [IEE01b]. Hotel [USE01b, USE01a, USE02a]. HotOS [IEE01b]. HotOS-VIII [IEE01b]. hours [Fox00]. House [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hsu [BCW05, HL05c]. HTML [CNB+02]. HTTP [Zha00]. Huang [ZC05]. Hube [MSNH07, NNT05]. Hull [KMT01]. Human [Dre00, GL01, JW05, KY01, You04, Man08, MS02d, RFR07a, RFR07b, RFR07c]. Human-Memorable [KOY01]. Hundred [Unio0a, Unio0b, Uni00f, Uni00e, Uni00h]. Huntington [GJL06, Hüttchenhain [Bau08, Bau08]. Hwang [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KCL03, LW05c, QC05a, WL05, YRY05d, ZYR01]. Hwang-Rao [ZYR01]. HWWM [LKY05c]. HWWM-authenticated [LKY05c]. Hybrid [AD109, CBB05, KD04, LZ04, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a, Che01d]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02]. Hyperelliptic [Ava03, CY02, CFA+06, HSS01, PWGP03, Ver02, Was08a, ZLK02, CMKT00, Wen03].
Wol04, WPP05]. Hyperencryption
[Che01d], hyperlinking [Che01e].

hypotheses [KW00].

I-tracings [RE02], i.e [NP02a, Wi99]. IA
[WWCW00]. IA-64 [WWCW00]. IACBC
[JM02]. IBE [ABC+05]. IBM [Ano04e, AV04, ADH+07, CGH+00b, Web08, Web00].

Ibn
[MAaT04, MAaT05, MAaTxx, MAaT07].

Ibn-Adlan [MAaTxx].

Ibn-Al-Durahim [MAaTxx].

iButton [HWH01].

IC [BGL+03, PC00]. ICBA [ZJ04]. ICCMSE
[SM07b].

ICISC
[Kim02, LL03, LL04d, PC05a, Won01, WK06].

ICISC’99 [Sau00]. ICM [IEE09a, IEE09a].

ICs [Bar00c]. ID [Gui06, ZJ09, BRTM09, CDD07, CL07, CS07c, CL00, GS02b, GTY08, HC08, KLY03, KHL09, Ku02, LCS09, Sco04, SW05a, SCL05, WBD01, WH02b, YC09b, YLH05, ZK02, ZC04, ZC09].

Id-Based
[ZJ09, CDD07, GS02b, HC08, Ku02, WBD01, YLH05, ZK02, CL00, KLY03, KHL09, Sco04, SW05a, SCL05, WH02b, YC09b, ZC04, ZC09].

Identity-Based
[ZJ09, CDD07, GS02b, HC08, Ku02, WBD01, YLH05, ZK02, CL00, KLY03, KHL09, Sco04, SW05a, SCL05, WH02b, YC09b, ZC04, ZC09].

Identification
[BP02, BL0709, Gar03a, GLC+04, KK02, Kir01b, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YC09+08, ZC09].

identifiers [MC04]. Identifying
[HBF09, LLS05b, ZYN08, DMS07].

identities [Kwo02, Kwo03b]. Identity
[App05, BF01b, BF03, BB04, BCHK07, BG07, BPR+08, Boy03, BRTM09, CL01a, CHM+02, Coo01b, Dea06, DTK04, GKO4, Her06, Her07, HY01, HL02, KC02, LDD07, Mar08a, Mar08b, Mit02b, Neu06, PCSTM07, Phi06, SMP+09, Ano01l, Ano04e, BMW05, CG06, CJL05, GGO8, Gvu06, KG09, LL04b, LWZH05, RG09, Sae02, Sha03c, Sm06, Smi08, Sul05, Wal04, Wan04b, Win05a, Wo05, YCW+08, Yout04, ZYW07].

Identity-Based
[BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, LDD07, Mar08a, Mar08b, App05, Her07, PCSTM07, BM05, CG06, CJL05, KG09, LL04b, LWZH05, Sae02, Sha03c, YCW+08, ZYW07].

IDSFM
[TZDZ05]. IDtrust2009 [SMP+09]. IEC
[ISO04]. IEEE
[BS03, BCD09, BC01, EIE01a, EIE02, EIE03, EIE05a, EIE05b, EIE06, EIE07, EIE08, EIE09b, KM07, HSD+05, Hug04, Mis08, PHM03, ZDW06]. IEM
[RC05]. IFIP
[DKU05, DFFP06, DFCW00, ELvS01]. II
[Bau05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Hau03, Kov01, MH09, OC03, Res01a, Res01b, Sal00a, ZT03, McE04]. III
[Sch00a, Ano00d, Bau03b]. IKE
[CK02a, Kra03]. I’ll [PLW07]. illegal
[Che01e]. Illinois [ACM04b]. Illusions
[Koc02]. illustrated [Lun09]. Im
[BGI+01, DOPS04, RR05]. IMA
[Pat03b, Sma05, Hon01]. Image
[AS01c, BSC01a, BSC01b, BQR01, CYH01, CLT07, CC09, CC06, GW01, KBD03, KC09b, LSS05a, LZ01, LWS05, LY07, LJ05b, LSC03, LSKC05, PZL09, RS00, SDFH00, SDF01, SSFC09, SH11, SM11, SYLC05, TTZ01, TH01, TC01, UP05, VKS09, VK07, WY02, WL05b, YZ009, AAP07, AA08, CC02b, CH01, Che07a, Che08a, GSK09, HLC07, KC09a, LLCL08, Lin00a, LTQ4, LYG07, LLLC06b, MS09a, MB08, PBV08, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, mSgFt05, TL02, Wan05, WMS08, WC05, XSW010, YCYW07, YCL07, ZLZS07].

Image-Feature
[GW01].

image-identification [PBV08]. Images
[CLT04, CC08, CW09, DP00, FG01, TL08, Pj01, PBC05, RE02, WCJ09, WC04, YWWS09, AAP07, AEDR05, BDN00, FWTC05, HYYW07, TCC02, TND+09].

Imaginary
[HJW01, HM00, HüH00]. Imai
Imbalanced [ZWCY02].
Immersive [Coc01a]. Immune
[CZK05, PZ02b, YKLM02b, ZP01, YKLM03].
Immunization [HR05]. Impact
[Ber03, HGNP +03, JKRW01, MMYH02, Wri00, CS08a]. Imperfection
[CP07, DOPS04]. Improvement
[BP02, Hsu05b]. implant [Fox00].
Implement [HQ05]. Implementation
[AD07, AG01, Ase02, Ash03, Arc+01, BBD +02, CCDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK +03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HHM01, JKS02, KMM +06, KMS01, KTT07, KRS +02, KV01, Lp02a, MMZ00, MK01c, MNP01, MP01c, Mur02, Nov01, NMSK01, Oi09, OTIT01, Pat01, PBTW07, QR+03, SM01, Sha01c, SK05a, SRQL03, USS02, Vir03, WZW05, WW00, WOL01, XB01, Ze00, BI04, BBK +03b, C +02, CNPQ03, DS09, DKL +00a, GHIG00, GBPK01, Hui00, HP01, Hut01, KY09, LL04c, LCX08, LB05, Rhi03, SM03a, SVDF07, Wli04, YY06, ZFK04].
Implementations
[AL00b, BP02, I000, CTLL01, CGBS01, EPP +07, GLG +02, MM01b, MP01a, RS01, WWCW00, ASK05, BFZC08, BFGT08, BG07b, Elb08, FR08, RAL07, RSQ03].
Implemented
[TSS +03]. Implementing
[Dwi04, Kor09, LM08, LD04, MWS08, NDJB01, Pet03, Smi01a, SR06, Woo05, C +02, CW02].
Implications
[Kun01, LJ05a, MF01, Ayo06, Bjo05, Fri07].
Implies
[KY01c]. Imply
[Pie05].
Importance
[Ano02b, KJC+01, TIGD01]. Important
[SM00a]. imposed [XLMS06].
Impossibilities
[CHL02]. Impossibility
[APV05, BPR+08, Fis01b, PQ06].
Impossible
[BFO00a, BF00b, CKK +02, HSM +02, MHL +02, Pha04, SKU +00, SKT01]. impostor
[jLC07]. improve
[Pau02a, CAC06]. Improvement
[CAC06]. 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, Kuo02, Kui02b, LW04, LL06, Mio2b, Miy01, MH04, Kir03, MS02e, PR08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].
Improvement
[AS01c, AJO08, Che04a, CZK05, CCM02, Di01, HWWM03, HW003, Hwa05, LKY05c, LKY05d, LTH05, MNT +00, NP07, Sha04b, Sha05b, WHL03, YR05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JSW05, JnBrXgXm05, KJY05, LL04a, LW05c, SZS05, TO01, WLT05a, YW04a, YWC05, YRY05a, YRY05d, ZC09]. Improvements
[BBM00, HW02, JL03, NP02b, YCYW07, CH07a, HW03c, SRQL03]. Improving
[SK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SKQ01, 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
[AEH17, CS05c]. Incremental
[BKY02, LKLK05]. IND-CCA
[Mii01b].
IND-CCA2
[BST02]. Independence
[BP03b]. Independent
[BS00a, BSL02, Kin02, GSK09]. Index
[An00b, An01d]. indexing
[YPPK09]. India
[CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, An03d]. Indices
[Fra01, Syv02, Wri03]. Individual
[BCC02, TW07]. INDCRYPT
[CV04, JM03, MMV06, MS02c, RD01, Roy00a]. Induced
[Vau02]. Industrial
[USE00b]. Industry
[ANS05, Mad00a, Or00]. ineffectiveness
[YLR05]. Infeasibility
[FS08]. Inference
[Mar02b, CDD+05]. Infinite
[TZT09a, TZT09b, Vau01]. infinity
informing [Bla01c]. Information [Kwo03b, San05]. Information-flow [FR08]. Information-Theoretic [VDKP05, vW01]. Information-Theoretically [DM00b]. Infrastructure [AHKM02, AL06, BC04b, BWE+00, CL07, ES00a, FL01b, KGL04, Sin01a, BHM03, BDS+09a, Ben01a, CZ05, FB01, Gor05, LCK04, MWS08, Ben02]. Infrastructures [HCDO02, Lin00b, PHM03, WBD01, Bra01a, LAPS08, LOP04, SN07]. INIDP04 [LDM04]. initial [DK08]. initiative [YWL05]. Initiative [Coc01a, Cal00b]. initiatives [Man05]. injection [MMJ05, ZSJN07]. Injective [Cmdv06, Kos01c]. Innovation [Sam09, SW05b]. innovations [Web02]. Innovative [MM07a]. Innsbruck [F01]. Input [CAC06, TC00, DKL09, VM03]. Input-trees [TC00]. Insurenc [Vau05b, Wal01, BJN00, LLH06, XwWL08]. Insecurity [Bl02b, DOP05, Lai08, Man02, SN01b]. insertion [MB08]. insertion-extraction [MB08]. Insider [CMS09, Tad02, KS05a, Mah04]. Insights [Kun01]. Inspired [CC09]. Installation [USE00a]. instance [FS08]. Instances [GG01, HN06]. Instant [BBK03a, RR05]. Instantiated [RR08]. Instantiation [BF05]. Instruction [BBGM08, EP05, KTT07, Bru06, Elb08, HTW07, MMJ05]. Instruction-Level [EP05]. Instruction-Set [BBGM08]. Instructions [LSY01]. instrumentation [MPPM09]. insubvertible [ACdM05]. Insulated [DKYX02]. Integer [Gro03, JL03, MN14]. Integers [CH07c, GMP01a, KKIM01, EKRMA01]. Integral [KW02, WH09, SM11, SH11]. Integrated [ECM00a, ECM00b, GMG00, Lut03, GLC+04, LK01, SSM+08, SN04]. Integrating [Wit01, AEH17]. Integration [Ito00, CJL06, Sug03]. Integrity [An02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel [Coc02a, MP00]. Intellectual [Qu01, WY02]. Intelligence [Cp04b, AJ08]. Intelligent [Cos03]. Inter [WRW02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WRW02]. interaction [Gav08]. Interactions [Fau09]. Interactive [BC05b, DG00, MS09c, CHK05, DDO+01, Fis01b, Fis05, HNZI02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00, MS09c]. Interception [CHVV03]. interdomain [MABJ06, vOWK07]. interesting [SWR05]. Interface [RSA01]. Interference [FGM00a, FGM00b, GA05, BR05]. Interlaken [CC04a]. Interleaved [ZSJN07, NC09]. intermediaries [JA02]. Internal [Har07b, Bej06]. International [ACM03a, ACM04a, ACM05a, ACM09, ACM10, AN03, An00d, AAC+01, AJ01b, BDZ04, Be00, B+02, BBD09, BS01b, Bii03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CC02, CCMR05, CSY09, CGP03, Cra05a, DR02c, Des02, DKL05, DFPS06, EBC700, Fra01, FMA02, Fra04, FLA+03, GH05, HY05b, IEE09a, IZ00, IKY05, JYZ04, Jef08, Joh03,
International [Yun02a, YDKM06, ZJ04, Zhe02b, ZYH03, AMW07, AUW01, Ano00e, AJ01a, BCKK05, Bir07, BC05c, CKL05, DV05, DWML05, DRS05, GKS05, HH04, HH05, HA00, Hon01, May09, PC05a, PY05, PPV96, Q500, Sma05, Son00, ST01d, WK06, Ytr06]. Internet [SMP09, ABB04, Ben01a, Ben02, Cal00a, Che05b, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, Pv01, Pho01, PHM03, Rub01, SBB05, SEK01, SEK02, Sto01, Tsao01, TWL05, Uri01, WCJ05, Wri05, ZGTG05, kc01]. Internet-wide [SBB05]. Interoperability [Hil00, TEM01, BHM03]. interoperable [BFGT08]. Interpolation [LW02, YG01b, FWT05, 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, KLO8, MA00a, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGK08, TW02, TW05, TW06b, Big08, CS07a, CM05b, Gar01, HW98, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06a, Kat05b, Rot07, Lee03a]. Intrusion [CZK05, DFK03, DP07, JT05, TZD05, TMMM05, WG05, HLL02, MAC03, NCRX04, NN02, YbJ04, IR02]. Intrusion-Resilient [DFK03, DP07, IR02]. intrusion-tolerant [YbJ04]. intrusions [Bej06]. intrusive [AMB06, RFR07a, RFR07b, RFR07c]. invalid [CJT04]. Invariant [Ben00, CT09, HH09, ZLZS07]. Invariants [WH09]. Invasion [ASW01]. invasions [Tyn05]. Invention [Bra06, Ifr00, Sav05a]. Inventions [Sav05b]. Inventors [Bar00c]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, MFFT05]. Inversion [BNPS02, KKY02, KT07, SPG02]. Inversion/Division [KKY02]. inversive [SB05]. Investigating [AMB06, BW07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08, WD01b, WC04]. Invitation [Bar02]. Invited [FGM00a, Lan00d, DRS05]. involutional [SHH07]. ions [Min03]. IP [Ano00a, CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSEC [Vau02, CGBS01, Dav01a, KMM06, SKW07, FS00, FS03a, XLMS06]. IPSec-Compliant [CGBS01]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFSG09]. Irreversibility [ZWC02]. ISBN [And04, Duw03, Eag05, For04, Gum04, Imr03, Pag03, Puz04, Top02]. Island [CSY09, KGL04, Kim01, Lee04b, IEE07]. ISO [GM00b]. ISO/IEC [ISO04]. ISO9979 [TM01]. ISO9979-20 [TM01]. Isolated [LSVS09, MMDT09]. Isomorphism [CY02]. Isomorphisms [CPP04]. Israel [Jol01]. ISSAC [Jef08]. issue [FOP06, FOP06]. Issues [BDF01a, BH00a, Hil00, KRV01, Mea01, PBM07, SEF06, MKY08, Pat02b]. ISW97 [You01]. IT-Architectures [RM02]. Italy [AAC01, AL06, BCKK05].
NA07, Ngu05, NBD01, NSS02, OTU00, Ort00, PHK+01, Pr01, Poi02, PHM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sha01e, Sin01a, SVW00, SK00, Ste01, ST01c, TS00, Tan07b, TT01, VV07, Wa03, WZW05, WH01, WC01a, Woo00, WBD01, Wya02, YKMY01, Yi01, YG01c, YDKM06, Zhe02a, ZWCY02, ABHS09, AJS08, AUW01, AKNRT04, Asl04b, AFB05, BHM03, Bad07, BBN09, Bra01a, BCP07, BMA00a, BMA00b, BD04b, CCT08, key[CL02b, CZ05, CYY05, CYH05, Che04a, CHC04, CY05, CLC08, CRRT08, CWJT01, CJ04, CLK04, Cho06, CHH+09, CJL05, CCD06, Cre00, DFM04, DG06, DMT07, DW09, EKRM01, ED03, EHKO04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GM05, GKM+00, GS01, GL06b, GMW01, Gue09, HCD08a, HCD08b, Hwa00, HLL04, IZ00, Iwa08, IM06, Jau08b, JRR09, JW06, JXW05, JZCW05, Jua04, KY00, KS05a, KOY09, KHYM08, KAM08, KG09, Kim01, KPT04, KRY05, Kob00, KW00, Kos01c, KHH05, LLM07, LHL03a, LF03, LKKY03a, LKKY03b, LCP04, LH04b, LL04a, LW04, LLL04, LLL05a, LKY05b, LKY05c, LKY05d, LLY06, LLS+09, LFHT07, LCK04, LPM05, LH08, LJKL01, LSH00, Lin01a, LS01c, LCC05, Lop06, MW08, MKKW00, MP08, Mi08, MRT10, Mi01b, NP02a, key[PS08a, PI06, Pe09, Pe04, PQ03a, PQ06, PC09, PSP+08, PLJ05b, Pot06, Pri00, RH03, SN00, SLP07, SRJ01, SBZ04, SK05c, SW06, Shi05, SL05a, SW05a, Shp04a, SC05b, SR04, SLC05, Sun00b, Sun02, SP02, SC05b, SC05c, SY06, TP07, TO01, TNG04, Tsa06, Tsa05, Tse07, VS01, Vau05a, VK08, WDLN09, War00, WL06, WGL00, WV00, WC01b, Wai01, WL04b, WHHT08, XH05, YY05b, YC09a, YC09b, YS02, YS03, YS04, hY08, Yi04, YRY05a, YRY05b, YY05b, YPKL08, ZLG01, ZC04, ZK05, ZSM05, ZYW07, ABB+04, GL05]. Key-Based [Sha01e]. Key-Dependent [Gol03, BPS08]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKXY02], key-management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DP05]. Key-Share [CT08a]. Key-Submission [HHZ02, WBD01]. Keyboard [ZT05]. Keyczar [Law09b]. keyed [Küh08, SR00, FIP02a]. Keyed-Hash [FIP02a]. Keying [ABB+04, Che08a, EGK08]. Keyless [Qu01]. Keys [AOS02, AP05, AV00, BR06, BT02, BMK00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, LXX07, Lue00, MN01, MRL+02, Moo07, Nit09, On01, PS00, St01c, Str02, Tvdb09, An01k, BCL05a, BCW05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH+08b, HSH+09, HW04, HY03, HL04, KAM08, LH04b, LL08b, LS01c, LW05a, ML05, NN03, Sch01e, Sha04b, Sha05b, SB05, TL05, TJC03, WH03, YRS+09]. Keystream [AMRP04, Kru02a, LV04, MH04, WLW04, PS01a, SM11]. Keystroke [ACS09, MR00, BGP02, JL07]. Keystrokes [SWT07]. Keyword [FIP05]. KGC [HLC08]. KG [ZYW07]. KHAZAD [PQ03b]. KIAS [May09]. Kid [CAC06]. Kikai [An00d]. Kikai-Shinko-Kaikan [An00d]. kill [Lov01]. Killing [Lov01]. Kilometer [Das08]. kind [DW01]. Kindi [MAaT03, MAaTx]. King [Eag05]. Kingdom [DFCW00]. Kingston [HA00, PT06]. Kit [An02e]. Klaus [And04]. Kleptographic [YY01]. knapsack [Kos01c, SL05c]. knapsacks [Mic02a]. Knife [Boy03]. Know [CMB+05, Ros07, Con09, DKK07, Win05c]. Knowing [CH01a]. Knowledge [Abe01, Abe04, AS01b, AP05, BP04, Con01, DPV04, DFS04, DDO+01, Er02, Fis05, Gen04a, GK05, HNO+09, KS06b, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00a,
Knowledge-of-Exponent [BP04]. Known [CKN06, CMB+05, DN02a, Fur02b, HSH+01, Bao04, YTH04]. Known-IV [HSH+01].

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

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

Korea [CSY09, CKL05, KCR04, Kim01, Kim02, Kun07, LLO3, Lee04b, LLO4d, May09, PC05a, PK03, Son00, Won01, WK06].

Korner [Mor03]. Kościuszko [OC03].

Krawczyk [Miy01]. Kryptoaanalyse [Mor05]. Kuala [DV05]. Kumon [YH03].

Kurosawa [CHH+09]. Kurtz [Gun04]. Kyoto [Oka00].

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

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

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

Lamar [LMHCETR06]. lamp [McN03].

LAN [Bar03, LFHT07, Pau03, SZ08, Sty04].

Lanczos [BF06a].

Landau [Jan08a].

Language [ARC+01, DD02, Gou09, Jen09, MWH04, WAF00].

language-based [WAFO0].

languages [Lun09, Rob02, Rob09].

Lantern [Ano10k].

Laos [Lov01].

Laptop [PGT07].

Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, G001, Kuh00, PG05, SM01, ST03b, USE00a, BP03a, CK05, CJ03b, Has00, HMvdLM07, HY03, PS08a, SM03a, TM06, WL05].

Large-Scale [CD01a, BH00a, B+02, HMvdLM07, PS08a].

Larger [Car02].

LARPBS [CPhX04].

Lasers [Igl02, UHA+09].

late [Sch05c].

latency [RSP05].

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

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

lattice-reduction [HG07].

Lattices [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Shp05, Sil01].

Launched [Bar02b, Ano00j].

Launches [Ano02d].

lava [McN03].

Law [GN06, MNFG02, Ste05c, NM09].

lawsuits [Ree03].

Layer [LXM+05, LPV+09, SLP07, ZL04c].

layered [KVD07].

Layers [Gri01].

Laying [Lut03].

Lazy [CCM05].

LDAP [Ban03a, Ban03b, BH00b].

Lead [Tsa07].

Leak [RST01].

Leakage [CKN01, DP08, Kel02, RS01, ABHS09, CNK04, YI05].

Leakage-Resilient [DP08].

leaked [Mad00b].

Learned [GBS+04].

Learning [KSD06a, LY07, CAC06, BKW03, KSN09, Mal06, Reg05, Reg09, SM08, Whi09].

Least [SZ01].

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

Lee [Sty04, YRY05d, Coc02b, KRY05, KCL03, KKL05, LKY05, SCS05b, ZK05].

Left [Dhe03, HKPR05].

left-to-right [HKPR05].

Legal [Coc02a, AN03].

Legislation [Eng00].

legislative [AviH00].

legitimate [Lin01b].

Leighton [Rub00].

Leighton-Micali [Rub00].

Length [AR01, BR00b, CKN00, CHJ+01b, Mål03a, RK06].

Length-Preserving [Mål03a].

Leonard [Coc03].

Less [YKM01, BD00b].

Lessons [GBS+04, KS00].

Lest [HS+08a, HSH+08b, HSH+09].

Lets [Pau02a].

Lett [Kwo03b].

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

Leuven [BBD09, DR02c].

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

Levels [KM05, CUS08, Voi05].

Leveraging [BRTM09].

LEVIATHAN [CL02c].

Levin [AC02].

LFSR [DS09, Jam00, JZCW05, MRT10].

LFSR-Based [Jam00].

LHL [Pei04, YRY05a].

LHL-key [Pei04, YRY05a].

Li [JW01, KCL03, SZS05, QCBO5a, SCS05b].
[AHS08, Lau08a]. **Masking**
[CHJ02, CT03, GK02, Lav09].

**Massachusetts**
[IEE05b, USE01b, USE01a, IEE03]. **masses**
[Pot06]. **Massive** [Ano01]. **massively** [FP00]. **massively-parallel** [FP00]. **Match**
[JJ00a, WC04, LLCo06a]. **Matching**
[ABM08, Len01, UBEF09, 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, S+03, Sch04a, Sch04b].

**Math´ematiques** [RSA09b, PPV96].

**Matrices** [TL07, CFVZ06, LMTV05].

**Matrix** [CV03, BF06a, OS07]. **Matroids**
[CDG+05]. **Matsumoto** [DDG+06, YG01].

**Mature** [Tro08]. **Max** [Di01]. **maximal** [H¨uh00, HJW01]. **maximizing** [GSK09].

**maxims** [Bau00, Bau02a, Bau07].

**Maximum** [KMT01, ZC00, DW01]. **May**
[ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bi03, CC04a, Cra05a, DRS05, IEE01b, Knu02, KNP01, MJ04, MS05a, PM00, Pi01, Pre00, TLC06, Uni00f, Uni00e, YKL02a, Pau02a, YJ00].

**Mbps** [LMP+01]. **McClure** [Gum04].

**McEliece** [CFS01]. **McEliece-Based** [CF01, KI01a, KI01b, Lio00, LS01c, Sun00b].

**McEliece-Based** [CF01]. **McFarland** [Car02]. **McGraw** [Gum04].

**McGraw-Hill** [Gum04]. **MD4** [DG00, WFLY04]. **MD5**
[An00, Eke09, For90, WFLY04]. **Me**
[CAC03, CNB+02]. **Mean**
[Bar00c, KLML05, Ver06b]. **Means**
[LMHCETR06, Nis03a]. **measure** [Lav09].

**Measurement**
[An00e, ko1, CO09b, FXAM04, RW07]. **measurement-based** [FXAM04].

**Measures** [CB01, Q501, GSK09].

**Measuring** [Siv06]. **Mechanising** [Bel01].

**Mechanism** [Eva09, LXM+05, WYY02, CL08, CL04, GH08, LCP04, ME08b, RFR07a, RFR07b, RFR07c, WAF00]. **Mechanisms**
[BACS02, CJK04, Her09b, Lin00a, MD04, Mir05, Pip03]. **mechanized** [di08]. **Media**
[And08a, Hei07, CBB05, An002d].

**media-streaming** [CBB05]. **Median**
[Cap01]. **Mediated** [DT03, CG06].

**mediator** [SBG05]. **mediator-free** [SBG05]. **medial** [AL07]. **Medicine**
[MYC01, Moo01]. **Meet** [Cla00a, GH07].

**meet-in-the-middle** [HG07]. **meeting** [Jef08].

**Meets** [Way02a]. **Melbourne**
[IZ00]. **Member** [CTH08]. **Membership**
[NBD01, Fis01a]. **Memoir** [Bar05].

**Memorable** [KOY01]. **Memoriam**
[DNRS03]. **Memory** [AK03, AJO08, BS00b, CC05, DK08, DGN03, HNZI02, HbAJL01, KCJ+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05]. **Memory-Bound**
[DGN03]. **memory-safe** [Oiw09].

**Memoryless** [Sar02]. **MEMS** [ECG+07]. **MEMS-Assisted** [ECG+07]. **ment**
[CAC06]. **menu** [Mea04]. **Mercy**
[Flu02a, Cro01]. **Merkle**
[CDMP05, JLS03]. **Mersenne** [An03f].

**Mesh**
[LP06, ZTP05, KB09, LZP+04, YPSZ01].

**Meshes** [BGI08, Lav09]. **Message**
[BKR00, BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SNR04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, Kar02, MD04, MS09c, Sha04b, TJC03, Wu01, ZF05, ZAX05, ZCW04]. **Messages**
[Ara02, AR01, BB00b, CJK+01b, DS05b, Sch09, Wri05, Zho06, Ala0v, An008c, BCG+02, Bi02, BB79, Lmi09, SP79].

**messaging** [Opp01, RR05]. **meta**
[SM08, PL05a, QC05b, Sha05d].

**Meta-He** [PLJ05a, QC05b, Sha05d]. **meta-learning** [SM08]. **metadata**
[CD07, FJ04]. **metamorphic** [CSW05].

**Metaphor** [CNB+02]. **Metering** [BC04b].

**Method** [BDTW01, GHK+06, GL00, Gro01,
Methodologies [SPMLS02, NdM04].
Methodology [VMSV05, HM02a, HCBLETRG06].
Methods [BCDM00, CFRR02, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Bau00, Bau02a, Bau07, BGM04, BCHJ05, CM05b, GKS05, LFHT07, Mal06, SSST06, Shp99, YW06].
Metric [LBGZ01, LBGZ02].
Metrics [LZ01, NP07].
Mexico [Buc00a].
MGC'05 [ACM05a].
Miami [Des02].
Micali [Rub00].
Michael [Ter08].
Micro [ASK07, Eng00, Ste05c].
Micro-Architectural [ASK07].
microcontrollers [GBKP01].
Microelectronics [IEE09a].
Microprocessor [Web08, GP00].
Microprocessors [LKM+05].
Microscopic [MYC01].
Microsoft
Bon00, Scr01, Ste05b, Weh00].
Middle
Eag05, Gen04a, HG07, Kin01].
Middleware
ACM05a, KRV01, LGS01, MBS04].
Migration
[Pat02a].
Mikhailovsky
Puz04].
Milan [dCdVSG05, military
Ark05].
Million [Ran55, Ran01, An03a].
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, Lut03, HLL+02, Mal06, Men03, Pin02, Pin03, ZY08].
MiniPASS
HS01b].
Minos [CC05e].
MinRank
[Con01].
Minutiae
UBEP09].
Minutiae-based [UBEP09].
Misbehaving
JQY01, SBB05].
Misinformation
CZB+01].
Missed [TvdKB+01].
MIST
Wal03].
Mistakes [Ste05b].
MISTY [KYHC01, Küh01].
MISTY-Type
[KYHC01].
MISTY1 [BF01a, Küh02b].

Mithra
Fre03].
Mitigating [NL08].
Mix
JJ00a].
Mixed [SKR02].
Mixes [Mö03a].
Miyazaki [WHL03].
MMM [GKS05].
MMM-ACNS [GKS05].
Mnemosyne
RH02, HR02].
Mobile
Cha05a, CFR02, Dim07, GN06, JP02a, KZ01, KB07, KC02, KHD01, LCK01, Mal02, MM02, PL01, RKZ02, RdS01, RC01, Rot01, SH00, ZYM05, CC05c, CJ03b, CF05, CF07, DHMR07, HP00, HYS03, sHCP09, ISTE08, KVD07, KXXD00, LC03, LC04a, Lin07, LKZ+04, Par04, Pan02a, SMS+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, RBB03, ZL04c].
Model
Abe01, Abe04, BH05, BPST02, BL02, CLK01a, CS07c, CPhX04, Chio8e, CT09, DPV04, DFSS08, Din01, Din05, ECM00a, Gra02b, HLC08, KLN+06, KW03, LJJ05, MND+04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SFDF06, TZZD05, Vag03, WCZ05, WT02, WvD02, ZGXL05, ZP05, ZS05, WK03, CUS08, CCD06, DQ00a, DFSS05, GMR08, HILM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SRJ01, TP07, DY09a].
Model-Based [Sal05b].
Modeling
[ADK05, CDD+05, HMvLM07, KS05a, ZP05, La00, SS04].
modelled [BG08].
Modelling
[HCDO02, JP07, Puc03].
Models
Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01b, SC02b, vOT08].
Modern
[Go09, Mao04, Pag03, SM07b, Sw08, Bud06, Fur01, IM06, KL08, Mo05, SE01, Lut03, Lee03b].
Modes
DGH+04, Dwo03, GD02, Go01c, HSH+01, JMV02, JKRW01, Jut01, KY01a].
Modified
[CHC04, HPC02, JY01, KI01a, ST02,
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, KKIM01, M¨ol02, NMSK01, OS01, Tan07a, Wal01, BINP03, DwWmW05, FP00, GD05, Has00, 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** [HSZ1].

**Multiresolution** [hKLS00, YPSZ01].

**Multiset** [aSM01].

**Multisignature** [Tad02, CWH00, CL04c, CCH04, Heo2, LWL09, LC04b, LWK05b, Wu01, YY05a, ZX04].

**multisignatures** [CL00, WH02b].

**Multithreaded** [Zha00].

**Multivariable** [DS05a].

**Multivariate** [DY09b, BGP09, FP09].

**Municipal** [HR04b, Sty04].

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

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

**Nema** [Kid00].

**NESSIE** [Pre01, Mac00, Pre02a, Pre02b, SGB01, DPVR00], **nested** [LCK04].

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

**Network-Attached** [RCBL00].

**network-based** [RCBL00].

**network-based** [RCBL00].

**network-based** [RCBL00].

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

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

**Networks** [AEAQ05, BJLS02, CGM07, DBS +06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, Bru06, CJ03b, CMS08, Cos01a, DWML05, GKS05, HLL +02, LC03, LPV +09, MW06, ME08a, MS03, Mio08, Pri00, RAL07, SCh00, Sta02a, TIS07, Vac06, Wy05, YLT06, ECM00a, ECM00b].

**Network-Attached** [RCBL00].

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

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

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

**Networks** [AEAQ05, BJLS02, CGM07, DBS +06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL +08, NAG03, PR01, RKKZ02, Sin01a, WT02, Zea00, ZYN08, ZWCY02, AJS08, Asl04a, BBG +02, BC05c, CCMT09, CGP03, CBD +05, DHRM07, ETMP05, HJ07, HMLD07, JRR09, KXST09, KHYM08, KB09, KVD07, LDH06, LHC08, LW05a, LLH06, Lin07, LN04, Lop06, LKZ +04, MWS08, MJF +08, MS09b, NC09, NLD08, PCSM07, PS08a, Pat02b, SLP07, ...
SSM+08, TP07, TM06, TCR03, TW07, WDLN09, XwWL08, YC07, ZJSN07, ZBLvB05, Ano02d, CS08b]. Neural [KMS02, PZL09, PR01, YC01, YC07]. Neural-Network [YC01]. Neuve [KMS02, PZL09, PR01, YC01, YC07]. Never [Ano02d, CS08b]. Neural-Network [YC01]. Nevue [QS00]. Nevada [ELvS01, IEE01a]. Never [Wei00, Hau06]. Newfoundland [NH03]. Newman [Pag03]. Newmanry [Sal01a]. News [Ano03d, Bar00a, Bar00b, Bar00c, Cla00a, Coc01a, Coc02a, Coc02b, Coc03, Eng00, Fox00, MYC01, MP00, PAU02a, PAU02b, PAU03, PAU09, Pri00, CAC03, CAC06, Sta05, Raj06]. Newton [KT06]. Next [ESG+05, McL06, TV03, Van03, Web08, BD04b, IST08, RR03a, Ros04]. Next-Generation [ESG+05, Web08]. NFA [DIS02]. NFS [Sta02b]. Nice [DS06, JH00c]. Nicko [Ano03g]. Nimbus [Fur02a, Mac00]. Ninth [USE00d]. NIST [BG07a, Dra00, Hir09, Kel05a, Kel05b, RRS06, SF07]. NFA/HMAC [RR08]. NMAC [Ran55, GPS05, Mic01, RMH03]. Normal [PL01]. Non [KM05, CHK05, CB+01, DNN00, DDO+01, DD09, FF00, Fis01b, Fis05, FSG00a, FGM00b, HNJ02, HJW01, IYK02, IYK03, JT01b, Kos01c, KO00, MST04, Nie02b, PHK+01, Pas05, SPK08, WBL01, DM07a, DSW02, HUt00, HLL04, IM06, KKL09, KHL09, LSA+07, PR05, RP00, RFR07a, RFR07b, RFR07c, SC05c, XWSC10]. Non-adjacent [JT01b]. Non-committing [DN00a, Nie02b]. Non-Cryptographic [WBL01, IYK02, IYK03]. Non-interactive [Kos01c]. Non-interactive [CHK05, DDO+01, Fis01b, Fis05, HNJ02, HJW01, MST04, Pas05, KKL09, KHL09]. Non-interference [BR05]. Non-intrusive [RFR07a, RFR07b, RFR07c]. Non-linear [XWSC10]. Non-malleable [DWe09, FF00, PR05]. Non-maximal [HJW01, HUt00]. Non-OOSD [CZB+01]. non-perfect [DM07a]. Non-physicists [BP01a, BL05b, CV02, Che01c, LGZ01, LGZ02, SM00a, ZC00, BGPG05, CFVZ06, KH08]. Non-linearity [SM00b]. Non-malleable [ABW09, DNN00, DNN03, PR08]. nonrepudiable [TYH04, YTH04]. nonrepudiation [HW05, OZL08]. Nondeterministic [Sch07]. Nonuniform [CU01]. Normal [Ran55, Ran01, GPS05, Mic01, RMH03a]. Normalization [VK07]. Norway [YtR06]. Nose [Fox00]. notation [LG04]. Notarized [GTY08]. Noun [Eag05, Kon01]. Note [CWY05, FS02, GMP01a, GIS05, KCP01, Ros00a, MF07, PC05b, Yan02, Zha06]. Notes [KF00]. Nothing [Des00c, SR00]. Notes [KF00]. Nothing [Des00c, SR00]. Notions [BPS00, BN00a, CK02b, DKMR05, HU05, Kos01a, Des00a, KY00, PS04c]. Novel [BBB+C09, CC02a, CYH01, CDTT05, CW09, HC08, MP01c, WJC09, AJ08]. BG08, CCS08, DSGP06, GB09, HG05a, MRT10, SPG02, SCS05a, mSGFL05, 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, HGNP+03, HG07, JJ00b, NP02b].
NTRUEncrypt [HHG06, KY09].
NTRUSIGN [HHGP+03, HHG06, HWH08, ZJ09].
NTRUSign-Based [ZJ09].
Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CF05, Dic03, DGP07a, DGP07b, DV08, EAG05, EH05, Fon06, GPR06, Hig08, Int03, Kat05b, Ke06, KM01b, LMHCETR06, LN02, MNP01, NR04, NNM10, RSN+01, SP05, Sch06b, Slp09, Slp03, SFDF06, TWNA08, TL07, TTT09a, TTT09b, Vav03, Wal00, Yan00, YKLM02b, AAM03, AUW01, BS02, BK07, Be08, BGPS05, BG08, BG09, BG07a, BGL+03, CFY+10, CNP3Q03, CO09b, DIM08, DGP09, FP00, HG05a, HGNS03, HlwWZ09, HP01, JAW+00, JL03, KH08, KSF00, Kin01, Lam01, LGKY10, MTT00, MRT10, Nie02a, Nie04, Pan07, PGG+09, PSS+08, PCC00, RGX06, SH11, Sho05b, Slp05, Sim02, Ste08, SR07, Sti11, Sk01b, Tat05, Wag03, Was08b, XSWC10, YZE09].
Number-Notation [EAG05, Kin01].
Number-theoretic [NR04].
Numbers [BCGH11, GH04, HR5+01, HBF09, Ifr00, MN01, ST05b, AG09, HW98, KB39, Kin01b, MFK+06, SS03, Slp05, Tip27]. numeric [AKS04].
Numerical [WWL+02].
numerically [Sav04].
Numerous [CC08].
NURBS [Ben00].
NUSH [WF02].
NY [HR06, IKY05, KJ05, Sch01d, YDGM06, An001, NISO0].
Nyberg [Ara02].

O [Kat05b, Puc03].
OAEP [Man01, BF05, BF06b, Bon01, FOPS01, Shi01].
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, KGM+00, KKL09]. obscurity [MN03]. Observability [JQY01].

observers [JL04].
Obstacles [KM04a].
Obtaining [Bar06b, BP03b].

OCB [RRB03].
occur [Web02].
Ocean [MYC01].

October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KR04, LST+05, TT09, USE00b, ZHY03].
Octopus [Cl00b].

Oded [Lee03b].

Odyssey [CT02].

October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KR04, LST+05, TT09, USE00b, ZHY03].

one-variable [SV08a].

On-Demand [SEF+06].
On-Line [Lu02, BCS02, L001].

One [AK02a, BYJ08, CHL02, Che03, DII02, Di 01, DW01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, KI01a, KO03, KO00, LTW05, LDM04, ML03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00e, XXYYX11, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJO4, CC05d, Di 03, DS02, GKK+07, HR07, HRS08, HLTJ09, JZ09, KK07, KKPK05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05a, Tsa08, YW05, YRY+05a, ZW05a].
One-Dimensional [XYXYX11].

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

one-variable [SV08a].

One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJO4, GKK+07, HR07, HRS08, JZ09, KK07, KKPK05, KK03,
LW04, LPM05, LQ08, Mic02a, Poi00, Tsa08, YW05, YRY05b, ZW05a. One-Wayness [KI01a, PV06b]. Ongoing [Sam09]. Onion [CL05]. Online [BDF+01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAVY09, Voi05, FNRC05, Fox00, Pan07, Tyn05, PT08].

Online/Offline [ST01b]. Only [BBK03a, CF01b, GL01, Hoe01, VV07, BCDM00, FKS+00, GHJV00, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Yas08]. Ontario [HA00, ST01d, VY01]. OOSCD [CZB+01].

OOSD [CZB+01]. Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Ki00, Lin02, Mea01, PM00, VDKP05, Ano03d, ETMP05, McA08, Bar00b, Lin02]. Open-Ended [Ki00]. Open-Secret [Joh05]. Open-Source [Bar00c, Bol02, Gut00, McA08]. OpenCard [HF00].

Opening [CAC03]. OpenSSH [Bar00c, Sta02b, TvdKB+01, Hos06a, Mos06]. OpenSSL [Fri01, Res01a, Res01b, Sti06a, VMC02, YRS+09, Bel08]. Operating [BCST00, DGP07a, DG07b, IEE01b, SR01, CGL+08a, CGL+08b, CGL+08c, DG09, KWD06, MPH06, SETB08, TKP+08].

Operation [BR02, BBK07, Dwo03, EP02, Go01e, HSH+01, JKRW01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BBK07]. Operational [WA07, GMG00]. Operations [BIP05, IMM01, KDO01, KS05c, LS01b, Ark05, Dug04].

operator [Wan05]. Operators [CH00], opinion [BHM03, G507b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Pau02b]. Optimal [Bai01a, BDDS03, CHJ+01b, CDF01, CF02, DPN07, GMW05, IR01, KO04, KS03, LZ09, Man01, MPSW05, MP08, SNN04, YY01, vDW04, BCD06, HKS00, LSH03a, LSH03b]. optimality [NK06]. Optimised [TL07]. Optimistic [CC00, DLY08]. Optimization [Hro03, Ken02a, Kre05, KV01, SMTM01, TLY04, WPP05]. optimized [LC03].

optimizing [Dw04]. Optimum [KWP06, O05]. option [Mat05]. options [Fri07, Pot03]. Opt [Han00]. Oracle [ABR01, Abe01, Abe04, BF05, Chi08e, Gra02b, Nie02b, Pas03, Ano02c]. Oracles [BNPS02, BB04, KG09, RG09]. Order [AKS04, Bai01a, CV02, KCP01, KJ+01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Coh03, JZCW05, KS06b, QPV05]. Order-Specified [Tad02]. ordered [HY03, WL05]. Ordering [Mea04]. Orders [HJ01, PS02b, HM00, Huh00].

Ore [CHH01]. Oregon [ACM00, BCDH09]. Organization [JG07, MMZ00, MP00, C±02]. Organizational [PTP07, BJ02]. organized [AUW01]. Oriented [HR00, LNZ+01, NNAM10, SKU+00, ZCC01, CH05, CWJT01, DL06, HW04, LL06, LWZH05, MWM01, Sae02, Sha03c, TJ01a, WHHT08].

Origin [MABI06, MD04]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Orsay [DPT02]. OS- [CRSP09]. oscillator [BGL+03, GB09]. oscillator-based [BGL+03]. oscillators [SPG02]. OSNP [HLTJ09]. Other [BF05, Ngu05, Wri05, Cla00b]. Otherworldly [MYC01]. Ottawa [AM07, MZ04]. our [Sta05]. ourselves [Fur05]. Outbound [Smi02]. Output [Dic03, YJ00]. Outsource [HL05a].

outsourced [MSP09, MNT06, YPPK09, YLC+09]. overcoming [CHC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, Ino05]. overheat [HGR07, IK08, RSP05]. overheads [XLMS06]. overlay [SL05b, YC08]. overlays [SK05b].

Overshadow [CGL+08a, CGL+08b, CGL+08c]. overview [SVEG09]. own [Phi06]. own-goals [Phi06]. Ownership [AS01b, Nik02a, Nik02b, CL08, Lin01b].
Page 55

P [Puc03, AKS02, KR03]. P1363 [IEE00b]. P2P [BRTM09, STY07, WN02, YLR05]. P2Ps [LHL+08]. PA [Cor00a, WWCW00]. P2Ps [LHL+08]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07].
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, WLT03, XwWL08, YW04a, YWC05, YS02, YPKL08, ZDW06.

Password-Authenticated [BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HTJ08].

Password-Based [CPP04, CS07b, GL03, SBEW01, SY06, 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, Dev08, ZSN05].

path-based [CCD+04].

Path-quality [GXT+08].

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].

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, SKKS00, SW00a, SB01, Siv06, SL00, SGPH98, WRBF00, WWCW00, WS02, XH03, YEP+06, Zea00, AKNRT04, BVP+04, BZP05, CKL+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTW07, SK03, YGZ05].

performance-friendly [CRSP09].

periodic [XQ07].

Periods [KKH03].

Perf [Sal03b].

Permutation [DMS00, HSR+01, IYK02, KKG03, KO03, LSY01, DP02, IYK03].

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

Persistent [AGT01, ST06].

Person [KJR05, LI+04, KN03, Li05, LST+05, PY08].

Personal [Bar05, EHMS00, SEK01, SEK02, TY05, UP05, Wal09].

Personalised [TNG04].

Perspective [LL01].

Perspectives [BMV06, SM08].

Perturbation [HWH08, ZY08].

Pervasive [BDhKB09, JW05, KHCL09, Lut03, Lut03].

PET [MS05a].

Peter [For04, Uzu04].

Petersburg [GKS05].

petitions [Cal00b].

Petri [KJL01, AADK05].

PGP [McL06, Ano00a, BCR+00, Dav01b, Dav01c, JKS02, Luc06, Opp01].

PGV [BR902].

pharaohs [Pio06].

Phase [CDF01, Iglg02, KLB+02a, Che07a, Che08a].

Phase-Conjugate [Igl02].

Phase-shift [Che08a].

Phil [Bar00a].

Philadelphia [EIE08].

Philip [McL06].

Philosophy [Cop04b].

Phone [CAC03, Fox00].

Photonic [TWNA08].

Photonic-based [TWNA08].

Photons [Bar00c].

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

Physicist [BZ02].

physics [RP00].

Physics [RP00].
Pp [Eag05, Pag03, Top02]. PPC [ASW01]. PPK [YDKM06]. pq [KOM01]. PQCrypto [BD08]. Practical [An01c, AR01, Ash03, ACJT00, BDK09, BF05, BL00, BS03a, Cap01, CD01, CT02, Chi08a, Chi08b, Chi08c, Chi08d, CS03b, DK01, Drei00, FS03b, G003, G005, GH02, HQR01, HJ01, Ina02a, Ina02b, IIT03, Kan01, LCD07, Lut03, LW05a, MM02, MU05, OM09, PB00, P06, Poo03, Roy00b, Sug01, Wei04, YSS01, Bro05b, DKL00a, Har05a, KSW06, L06, M06, MS04, Sha01a].

Practice [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXT09, Sta02a, Sta06, St05, Sti02, St06c, Lut03, Spr03].

practices [CF05, Ste02]. practitioners [PP09]. pragmatic [BMW02b]. Prague [MJ04].

Pre [Adl03, AA08]. preprocessing [AA08]. Precise [Wal01]. Precision [HZ05, SR06, LMC03, MN14].

Precomputation [SLG05]. predecryption [RSP05]. Predict [Dic03]. predictable [Be08]. Predicting [AG09, BGPG05]. Prediction [AKS06, SLG05]. predictable [vOT08].

predistribution [HMvLM07, JRR09, TP07]. Preface [CGM07]. Prefix [FXAM04, RW07].

Prefix-preserving [FXAM04, RW07]. Prehistory [Iz00]. Preliminary [KS00b, KKS00b]. Prentice [For04]. Prentice-Hall [For04]. Preparations [FJ04]. Prepared [ASW01].

Preprocessing [BIM00, CCKK03]. presence [BIW08, GXT+08, Mis08, VS08].

Preservation [Che01b, Dur01, Bro05a, ISO05, LG04]. Preserve [NNT05]. Preserving [DN04, KS05c, LP00, M003a, YW08, AKS04, BR06, BS03b, BA06, FXAM04, GA03, HJ05, L05, Pin02, Pin03, RW07, HJ07].

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

Pressure [HW01]. pretty [vOV07]. Prevent [FOBH05]. Preventing [CS07b, CCL09, HSW09, IY05, RG05, DMS07].

Prevention [JT05, PZ01, PZ02a, G003, Smi03]. Price [AS01a, Bra01b]. Primality [BT02, Che03].

Prime [ACJ02, Bai01a, Har07a, Pau02a, WS03, JL03, Dw02]. Prime-detecting [Har07a]. Primer [KLB02, Lad06].

Primes [An03f, Z01, HLL03, Ste08, AKS02]. Primitive [CFS05, IY02, IM01, ST01a, ST02, IY03]. Primitives [BD02, CHL02, FGM001, Gol01, G005, RR00, BF05, Gar05, JZCW05, RA07].

Princeton [Gen01]. Principal [ZL04b].

Principle [CZ05]. Principles [ACM03c, ACM05b, DK02, DK07, KL08, MAA07, SB07, Sta02a, Sta06]. Print [Kra02b]. Printed [SLT01]. Printer [Bar00a]. Priority [WWL02]. Privacy [An00i, AEV07, BB01, BSSM07, CDM05, Cho08a, DL08, DL07, DKF05, DN04, G002a, G008, HY01, KS05c, Knu07, LP00, MP00, Pap05, PB05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YW08, Be04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KXT09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZLYG05, ZSM05, MS05a, Jan08a].

Privacy-Enabled [Por06]. privacy-enhanced [ZS05].

Privacy-Enhancing [SE09].

Privacy-Preserving [DN04, KS05c, YW08, BA06, HJW05, Pin02, Pin03].

Private [AF04a, AF06, BDF+01a, B000, BY03, BS09, BJLS02, BGW05, ISW03, K000, OS05, SD06, ST01e, Wal03, Yek07, BD00b, Ca00b, HLL03, KY00, KPS02, PLJ05b, Sun02, YRS+09, ZY08, ECM00a, ECM00b].

Private-Key [BY03, KY00, PLJ05b, Sun02]. prize
proof-of-compliance [LMW05].

Proof-of-Concept [ARC01]. proofing [CT02].

Proofs [BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BG09, BR04, Gol99, HG05b, SV08b, dH08].

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

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

Proposal [DPVR00, Mac00]. Proposed [Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06].

Protect [ETZ00, BBN09, WK05].

Protecting [Des00c, EHMS00, KL05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYL05].

Protection [CGJ07, DKFX05, ECG07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL08a, CGL08b, CGL08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].

Propose [Coc02a, HPC02, KI01a, You01, YG01c, JK01a, ZDW06].

Proposing [CT02, Gor05, HLC07, KA09, KL05, Lee03b, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL08a, CGL08b, CGL08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].

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

Proposing [CT02, Gor05, HLC07, KA09, KL05, Lee03b, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL08a, CGL08b, CGL08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].

Protocols [AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Bor01, BM00a, BMA0c, Bra01b, BL05, CKPS01, CT08a, CCM02, CCM05, Cir01, CNV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, G07, JW05, KS00a, KY03, KL08, Kra03, Kus02, MS02a, MN01, PB00, PR08, PZDH09, Rot01, Shy02, SC01, Tee06, AA04b, AKNRT04, Bar06a, Ban05, Bel07b, BDSV08, BFTG07, BP05, BL05, BD04a, BR05, Can01a, Can06a, CP07, CKR08, CWJT01, CH06a, Cho08b, Chr00, Chr01, C08, Col03, CC05d, CDL06, DFG00, GJ03, G04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV09, LLL04, LLY06, LLS09, Mea04, MT07, MR06, Mon03, MP07, PR05, PQ03a, PQ06, PV08a, SL05a, SR00, SW00b, SY06, WL06, YS04, ZLX09, ZL04b, PDMS09, Puc03].

ProtoMon [JT05]. Provability [GOR02b].

Provable [HM02b, HLL01, HSL02, KSH01, PB05, SLL00, B09].

Provably [A00, ACJ00, B00, BC01, BC07, CHKO08, DG03, DG06, HL02, HvAL09, HL07, HS07, JM02, Mi03a, NS05, SS02, VMS05, WL06, XS03, ZL05, BKN04, CC07].

Provenance [HSW09].

Provers [MV03a].

Provide [AB01, S01].

Provider [LDM04, HILM02].

Providers [MV03b].

Providing [AT03b].

prove [AH05, BCL05a, DKFX05, LCK03, LCZ05b, PL01, Rd01, Sha03d, Z09, AF06, CCH04, DY09a, HWW03, HW04, HW05, HW05, HC04b, KL09, LL05b, LH05, LCZ05c, LW05c, PK05, Sh05b, SHT05, TY04, YTH04, ZL05].

proxy-enabled [DY09a].

proxy-protected
psBGP [vOWK07].

Pseudo
[PKH05, ZCL05]. psBGP [vOWK07].

Pseudo-Random
[PLL+01, LH+08, MP03, SX01, TZZ09a, TZZ09b, WP03, XYYYYX11, BG09, CFY+10, GB09, MFK+06, NR04, PLsVdE10, PSP+08, RGX06, SH11, SM11, SL09, WW08, XSWC10, YZEE09].

Pseudo-Ransom [BH05].

Pseudo-Randomness
[BPW04].

Pseudo-signatures
[FWW04].

Pseudonoise
[HG05a].

Pseudonym
[CG06].

Pseudoprimes
[ZT03].

Pseudorandom
[BCGH11, CDI05, DN02a, DI05, DP02, Fin06, Flu02b, FIPR05, GM02a, IYK02, LMHCETR06, Nie03, MP03, WP03, XYXYX11, Gen00b, SXY01, CFY+10, MFK+06, NR04, PLsVdE10, RGX06, SH11, SM11, SL09, WW08, XSWC10].

Pseudo-Ransom [BH05].

Pseudo-randomness
[GM02c, IK00, IYK02, LMHCETR06, Nie03, MP03, WP03, XYXYX11, Gen00b, SXY01, CFY+10, MFK+06, NR04, PLsVdE10, RGX06, SH11, SM11, SL09, WW08, XSWC10].

Pseudorandomness
[BPW04].

Public-Key
[Ano02d].

Public-Key-Based
[YKMY01].

Publication
[Top02, DGMS03].
GPP08, SGK08, LJ05a. Purposes [LS05a, FSGV01, PBV08]. Push [Pau03].
puzzle [LF03]. Puzzles [Ano01f, ANL01, CHS05].

Q [BFMR02, CH01b]. Q&A [Str01b, Win01]. QCQC [Wil99]. QCQS [Wil99]. QNX [Ano02d].
QoS [JKRW01, Zea00]. QoS-aware [Zea00].
QSIG [ECM00b]. QSIG-WTMAU [ECM00b]. Q'tron [YC07]. QUAD [BG09]. Quotient [KS06b].
Quantifier-free [KS06b]. Quantitative [Bai08, ME08a]. Quantization [DRL09, WC04, WC05].
Quantum [AC02, ATSVY00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL+05, BBD09].

Radix [HKA+05, JY01]. Radix-quadrant [PCG01]. Quasi [MD05]. Quasi-Pipelined [MD05].
Quasigroup [MSNH07]. Québec [ACM02]. Queen [Ree01, Ros00b, Sin99].
Queenstown [Zhe02b]. queries [CKK03, Fis01a,GPC08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC+09].
Query-preserving [GA03]. querying [FJ04, UG08]. question [OC03]. Questions [Ett02, Joh00, Jac00]. Queues [WWL+02].
queuing [CUS08]. quick [Dew08].
Kos01a, Kos01b, MT02, MSI10, SB00, Sun00a, BBN+09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03. Range [CW09].

Rank [Sun00a, DW01, Sim02]. Ransom [BH05]. Rao [Zyr01]. rapid [OP01b]. Rate [KT01, Lz09, PS02a, Sun02]. Rates [CW09].

Range [CW09]. Rank [Sun00a, DW01, Sim02]. Ransom [BH05]. Rao [Zyr01]. rapid [OP01b]. Rate [KT01, Lz09, PS02a, Sun02]. Rates [CW09].
KLML05, Sat06, Buc00a, Gutxx, HAU04, Hen06a, Sch00b. Related-Key [FKSW00].
Relation [ABC05, NN06]. Relational
[AK02b, AHK03a, AKH03b, CKY07, GA03, PT08]. Relations [BN00a, Pau01, Uni00a, 
Uni00f, Uni00e, SP03, Zha08]. Relationship
[Ng05, GKI01]. Relationships
[AK02b, AHK03a, AKH03b, CKY07, GA03, 
PT08]. Relation [ABC05, NN06].
Related-Key [FKSW00].
Relaxing [CKN03, PS05]. Relaxing
[CKN03, PS05]. Relaxing [PS05].
Reliability [IKP07, WK05]. Reliable
[MR03, MPHD06]. reload [SL06].
Remainders [Che01f]. Remainder
[Sch01b, YKLM03]. Remarks
[BCW05, CL04d, SCS05c]. remedy [FZ06].
Remember
[HS01a, HSH01b, HSH01c, HSH01d]. Remote
[CJ07, CWR09, Kra02b, LL05c, Rub01, 
TK03, WKB08, CCK01a, CL04d, CTJ01, 
DSCP06, FCZ05, Hsu05b, HL05b, KC05, 
LHY02, LLM02, LKY05a, LHL03b, LC05a, 
MW06, SW06, SZ05, WLT05a, WC03b, 
YW04b, YR05d]. remotely
[Küh08, SR00]. Removal
[LS05a]. Removing
[JL00]. rencontre [PPV96].
Renewable
[TOE000]. Repairing
[DFX05, GM00b, HL04, Z09, BKN04]. replace
[Gav08]. Replacing
[FZ06, KAM08]. replication
[BIW08]. Reply
[WLW04]. Report
[DFG01, Pem01b, Pre01, Sal01a, Sha03b, BCR05].
Repository
[Bar00b]. Representation
[BJvR02, FSW01, JLM03, JY01, R00a, 
R00b, ZL02, BDS08, BA06, PS04a, 
SAR05]. Representations
[OSST04]. Representative
[CTBA01].
Representatives
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Republic
[ML04, DL00]. Republik
[DL00]. repudiating
[HLL04, LSA07, SC05c]. reputation
[KNS05, RCG05]. reputation-systems
[KNS05]. Request
[SA00b]. require
[SV08b]. Required
[Sun00a, L001, Wan05]. Requirements
[FIP01b, HWWO, Kin02, NIS01b, Mea04].
Research
[ASW01]. Research
[DK01b, CZ05, CZK05, DFP06, 
KLG04, LX05, RC06, Sch00e, TM05, 
DPC00, JXW05, M09, Q500, dCDG05].
Researchers
[Ano08a, Ano08c, Pau02b].
Resettability
[DFV04, MR01b]. Residue
[TIGD01, YKLM02, CNPQ03, FP00, LD01].
Residues
[Co01b, Zhe01, C008].
Resilience
[J00]. Resilient
[HNZ02, Mö02, EBS01]. Resistant
[Ano01f, ACJ00, ANL01, BGW05, 
CDT05, CVN06, G06, IO05, LLS05a, 
LVS05, LT05, NL07, KS09a, PC09, 
YR04b, YS02, MS09c]. Resilience
[SNM09]. resolving
[L01]. Resort
[USE00b]. Resource
[MRL02, T07]. Resource-Constrained
[MRL02]. resource-limited
[Tse07]. Resources
[Gutxx, You04, FOP06]. Response
[JBR05, LV05a, X05]. Responsibilities
[Vix02]. Resting
[Gut02a]. restricted
[AS00b]. Restriction
[CTH08]. Restudy
[FWM08]. Results
[APV05, GM02c, OOP03, RR08, Way02a,
YRS09, CV05, CKR05, DM07a, G00, 
PM08]. Rethinking
[Bra01a, K03]. Retraining
[LC07]. Retreat
[FKS00]. Retrieval
[BIM00, K00, RE02, Y07]. Retroactive
[DSB01]. retrofitting
[CGL08a, CGL08b, CGL08c]. reunion
[LBA00]. Revealed
[Gal03]. Reversal
[Cap01, DIS02]. Reversal-Bounded
[DIS02]. Reversals
[MS02]. Reversal
[Coo02, EC05, Wue09]. Reversed
[Ina02b]. reversibility
[K09a]. Reversible
[Go02]. Reversing
[EC05, YWC08, YN01, CDFM05]. Review
[And04, Ano02i, Duw03, Eag05, Eva09,
Fal07, Gas01, Gum04, Imr03, Irw03, Jan08a,
Lee03a, Lee03b, Mar05a, Pag03, Pap05,
Puz04, Ree01, Rot07, Sec04, Spr03, Ter08,
TvdKB*01, Top02, Uzu04, Was08a, Her09b,
Kat05b, Kid07, Ln07, McE04, MP01b,
Nie02a, Nie04, Puc03, Shp04a, Wal00].

Reviews [For04, Kid00, Sal03, Sty04].

Revised [Bla03, BC05c, Chr01, CCMR02, CCMR05,
CSY09, CGP03, DR02c, GS02c, GH05,
HH04, HH05, Joh03, Jue04, KKP02, KCR04,
LL03, LL04d, Mad00b, MS05a, Mat02, MZ04,
NH03, PC05a, PK03, PT06, RM04, Sil01,
Ytr06, AMW07, AJ01a, BK07, Bir07, CKL05,
Drs05, Ige03, FY05, WK06, Wli03].

Revisited [ABC05, Ano02b, BM01b,
CDMP05, Knu00b, NS05c, OSSST04,
Hes04b, OHI08b, ZTT05].
Revisiting [AAEQ05, Har01a, Har01b, JMV02].

Revocation [BDTW01, CL02a, Gen03,
GST04, NN01, TTO1, ZSM05, KTO6,
KSW06, LHH05, SW02].
revoke [NN03].

Robustness [CS05c, HM01b, Rot01, AEH17, CKL*09].

Rogaway [MW04].
Roger [GG05a].
Role [SBG02, YT09, ZGLX05, Cer04a, Cra05b,
Gor05, Mau04, You04].
Role-Based [YT09, ZGLX05, Cra05b].

Rome [IEE04].
Ronald [Coc03].

Rolle [SBG02, YT09, ZGLX05, Cer04a, Cra05b,
Gor05, Mau04, You04].
Role-Based [YT09, ZGLX05, Cra05b].

Rootkits [HB06].
Roots [Gon06, HCK09, CAC06].

Rosen [HR13].
Rotation [RF08], rotations [SK03].
Roth [Fal07].

Round [NB00, GBW03, Dreu01, Scr01, TMM01, Wya02, BA06, UP05].

Rijndael [BB02, MP01a, SKU*00, Wer02, CKK*02,
CGB01, DR00a, DR00b, DR01, DR02b,
FKS*00, FKΛ*01b, FKΛ*01a, FSW01,
FD01, GM00a, JmbdXm05, KY01b,
KMT01, KV01, Luc00, MM01b, MMH02,
PSC*02, RDJ*01, SMT01, SRQL03].

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

Rings [BLST01].

RIPEMD [DG02, WFLY04].
RISC [Cor00a, Gro03, WW00].
RISC-Based [Gro03].
Risk [WA07, Voi05].
Risks [ES00a, Kuh02b, Ros07, Bjo04, Bjo02, ES00b,
Jan00, MN03, Pvs01, Sch00c].
Rivest [BB79, Coc03, SP79].

RM [JRB*06, Mar02a].
RNS [BI04, BP03, NMSK01].
Road [BDPV09, HR04b, PB01].
Roadmap [Coc02b].
Roaming [Cac03, YWD08, SSM*08].
Robotic [Kum07].
Robots [Coc01a].
Robust [BB00a, BR09, CJ03d, CYY05, DDO*01,
FC05, HO09, hKLS00, Lin00a, LHS05,
LL06b, PJ01, SO07, SDFH00, SDF01, VK07,
WNN09, Wl04b, WMDR08, YPSZ01, ZTP05,
KA09, LCZ05c, LKZ*04, Mit00, MB08, TND*09, YY05b].

Robustness [CS05c, HM01b, Rot01, AEH17, CKL*09].

Rogaway [MW04].
Roger [GG05a].
Role [SBG02, YT09, ZGLX05, Cer04a, Cra05b,
Gor05, Mau04, You04].
Role-Based [YT09, ZGLX05, Cra05b].

Rome [IEE04].
Ronald [Coc03].

Rolle [SBG02, YT09, ZGLX05, Cer04a, Cra05b,
Gor05, Mau04, You04].
Role-Based [YT09, ZGLX05, Cra05b].

Rootkits [HB06].
Roots [Gon06, HCK09, CAC06].

Rosen [HR13].
Rotation [RF08], rotations [SK03].
Roth [Fal07].

Round [NB00, GBW03, Dreu01, Scr01, TMM01, Wya02, BA06, UP05].

Rijndael [BB02, MP01a, SKU*00, Wer02, CKK*02,
CGB01, DR00a, DR00b, DR01, DR02b,
FKS*00, FKΛ*01b, FKΛ*01a, FSW01,
FD01, GM00a, JmbdXm05, KY01b,
KMT01, KV01, Luc00, MM01b, MMH02,
PSC*02, RDJ*01, SMT01, SRQL03].

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

Rings [BLST01].

RIPEMD [DG02, WFLY04].
RISC [Cor00a, Gro03, WW00].
RISC-Based [Gro03].
Risk [WA07, Voi05].
Risks [ES00a, Kuh02b, Ros07, Bjo04, Bjo02, ES00b,
Jan00, MN03, Pvs01, Sch00c].
Rivest [BB79, Coc03, SP79].

RM [JRB*06, Mar02a].
RNS [BI04, BP03, NMSK01].
Road [BDPV09, HR04b, PB01].
Roadmap [Coc02b].
Roaming [Cac03, YWD08, SSM*08].
Robotic [Kum07].
Robots [Coc01a].
Robust [BB00a, BR09, CJ03d, CYY05, DDO*01,
FC05, HO09, hKLS00, Lin00a, LHS05,
LL06b, PJ01, SO07, SDFH00, SDF01, VK07,
WNN09, Wl04b, WMDR08, YPSZ01, ZTP05,
KA09, LCZ05c, LKZ*04, Mit00, MB08, TND*09, YY05b].

Robustness [CS05c, HM01b, Rot01, AEH17, CKL*09].

Rogaway [MW04].
Roger [GG05a].
Role [SBG02, YT09, ZGLX05, Cer04a, Cra05b,
Gor05, Mau04, You04].
Role-Based [YT09, ZGLX05, Cra05b].

Rome [IEE04].
Ronald [Coc03].

Rolle [SBG02, YT09, ZGLX05, Cer04a, Cra05b,
Gor05, Mau04, You04].
Role-Based [YT09, ZGLX05, Cra05b].

Rootkits [HB06].
Roots [Gon06, HCK09, CAC06].

Rosen [HR13].
Rotation [RF08], rotations [SK03].
Roth [Fal07].

Round [NB00, GBW03, Dreu01, Scr01, TMM01, Wya02, BA06, UP05].
Pat03a, Pat04, GM00a, SK01a. **Routing** [BGOY08, CL05, Ken02a, KB09, LAPS08, LHC08, MAB106, PS08a, RVS09, vOWK07]. **RSA** [Joy03b, Men05, Oka04, Poi06, Pre02c, Shp04a, Wal00, Adl03, Ano01o, Ano02e, AR01, BI04, BS02, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD06b, BMK00, BJN00, BF01c, Bon01, BCCN01, BP01b, CNS02, CDL+00, CW02, Che01a, CKY05, CNPQ03, CKN00, CJNP02, CS00, CS03c, CD01b, DK01, Duj08, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gro01, HN04, Her07, HLLL03, HLH00, HLL03, Int00, Jan08b, JS05, Jon08, JK02b, JK02c, JG01, Kal01, Kal03, Kat05b, Kat01, KKL09, Kh00, KPR03, LS01a, MPS00, MLM03, Man01, May02, May04, Miy01, Mol03b, MP01c, NZCG05, NZS05, NS01b, Nit09, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Shp03a, Shp01]. **RSA-based** [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLLL03, NZCG05, Sei05, WHL05, WY05, YPKL08, YY00]. **RSA-Encrypted** [CD01b]. **RSA-Primitive** [ST01a]. **RSA(R)** [Ano06b]. **RSES** [LLCL08]. **RST** [ZLZS07]. **Rueppel** [Ara02]. **Rules** [Bla01a, Ano06c, Bla01b, GM04, Ste06, Wei09]. **Running** [ZL04c]. **Running-mode** [ZL04c]. **Runtime** [PBTW07, Russia] [GKS05]. **Ryan** [Puc03]. **Rye** [KJR05]. **Ryan** [KCC05]. **S** [BZ02, Kat05b, Puc03, Bih00, BCDM00, Dav01b, Dav01c, FM02b, JmBdXgXn05, LG09, Opp01, SMTM01, ZC00]. **S-Box** [FM02b, SMTM01, JmBdXgXn05]. **S-boxes** [BCDM00, ZC00]. **S/MIME** [Dav01b, Dav01c, LG09, Opp01]. **SAC** [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR+01, HSS04, ST01d, VY01]. **SAC’99** [HA00]. **SAFE** [Uni00a, Uni00b, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Oiw09]. **Safe-Prime** [ACS02]. **Safeguard** [LXM+05]. **Safeguarding** [Sty04, Bar03]. safer [Ano00f, NPV01, BDD03]. safety [HM01a]. **SAF KASI** [WAF00]. **Sage** [Eva09]. **Salomon** [Pap05]. **Salsa20** [Ber07, Ber08]. Salt [PKBD01]. **Salzburg** [DKU05]. **Samba** [BH00a]. **SAML** [RR04]. **Samos** [KGL04]. **sampled** [WW06]. **sampling** [KB39, Sug03, Tip27]. **San** [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Oka04, Poi06, Pre02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c]. **sanity** [Sk03a]. **sans** [Car00]. **Santa** [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a]. **Santiago** [BS03]. **Sanxin** [LSZ05]. **SAR** [B+02]. **SASAS** [BS01c]. **SAT** [KLN+06]. **Satan** [Men04]. satellite [CC05c, HYS03]. **Satisfy** [PHM03]. satisfying [QP05]. **Saturation** [Luc02a]. saving [Lev01]. **Savings** [CAC03]. **SAX2** [TEM+01, Hei01]. **Say** [Sta05]. says [Ano01e, Mad04]. **SBLH** [JK02a]. **SBboxes** [WOL01]. **SC-CFS** [It01a]. **SC2000** [SYY+02, YSD02]. **SC2001** [ACM01b]. **Scalable** [CPhX04, HKA+05, HLY05, KY03, KYH08, SPQ06, LLW08b, ST03a]. **Scalar** [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. **Scale** [BWE+00, CDR01, FG01, BP03a, BH00a, HMvdlM07, PS08a]. **Scaling** [BBP00, Coc02b, SDFH00, SDF01, PBV01]. **Scambray** [Gum04]. **Scan** [MYC01, BD03, KB03]. **SCAN-Based** [BD03]. **Scaring** [Ols00]. **Scenarios** [BF05]. scene [SG07]. **Sceptical** [Pen01b]. **Schedule** [MMH+02, XH05]. **Scheduling** [FMS01, XQ07]. **Scheme** [AR00, AK02a, ACJT00, AF03, BBC+09].
BNPS02, BR09, BS01d, BMS03, CL01a, CHK03, CGH01, CC01b, CYPH01, CTL04, CG09, CH01b, CM05a, Coc01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJSS01, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LXH07, LCD07, MyI01, MuI01a, OK06, PL01, RK06, Scr01, SOO102, SWH05, SGLB00, SYLC05, SSNGS00, Tad02, TC01, Tsa01, TT01, WQWZ01, WZW05, WBD01, YWWS09, YG01a, YLH05, ZJ09, AEEdR05, Asl04a, BCL05a, BCW05, BKN04, BBG\[FWL08, FWTC05, Gen09a, GS09, Hes04a, HWW03, HWW04, Hsu05a, HWH05, HL05c, HL05d, HL05b, JW06, JSW05, KC09a, KLY03, KRY05, KSW06, KHL09, KCL03, Ku04, KC05, KCC05, KHKL05, LHY02, LH02, LHL03a, LKY04, LL04a, LJY04, LL04a, LKY05a, LKY05d, LL05b, LMC+03, LHL04, LTH05, LLCL08, LH02, LHL03b, LH02, LCC05, LC05a, LCC05b, LC05b, LCZ05a, LCZ05b, LCZ05c, LCZ05a, LWKL05b, MS09, NC09, PW05, PBMB01, PCC03, PC05b, PS01a, PeI04, Sae02, Scc04, SM11, Sha03c, Sha03a, SC05a, Sha02c, Sha02b, SLH03, mSfTL05, SCS05b, SCS05c, SCS05c, SCS05c, SLH03, TSL05, Tla08, TCC05, TLD05, TYYH04, VKL08, VS08, WILT03, Wan04b, WL05, WKL05, JW05, WJP07, WDLN09, WHKL05, WC01b, WH02a, WHEL03, WH03, WC03b, WL04b, WC05, XwWL08, XC05, YW04b, YTH04, YW04a, YCH04, YWL05, YCO09b, Yh08, YRY04, YRY05a, YY05a]. scheme [YRY05d, YY05b, YbJ04, ZC04, ZK05, ZK05, ZW05a, ZAX05, ZC09, ZL05, dRMS05]. Schemes [AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CDP06, CKNO0, Cor02, CJNP02, Cou04, CS00, CS03b, CDG+05, CL02, DN00a, DN02b, Des00b, DS06, DN00b, FF00, HSZI00, HWW05, HM02b, HLL05, Hin02, K01a, KS03, KOMM01, L407+01, LP01, MV00, NIS03b, Nam02, NNN01, NN06, OP01a, Pat04, Pre01, ST01b, SB02, SPML02, Sm00a, VM050V, WCJ09, XS03, YWC08, YYDO01, Yek07, YYZ01, ZTP05, ZYR01, Abd01, AFH06, BCD06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DFMO4, Des00a, GGO03, HCD08a, HCD08b, Hau040, He02, HK000, HWO3c, HW04, HW05, HC04b, HL04, IY06, JPL04, JXW05, KJ05, Kir01b, KT06, Kee05, Küh08, LWZH05, LWK05a, LW05c, MF07, MüI01b, NK06, P02a, PKH05, PhA06, QC05b, QC05b, SJ001, Sha03d, Sha05b]. schemes [SCL05, SC02c, SHT05, Tsa05, Wu01, XY04, YWC05, YCW+08, ZF05, ZCL05, vDKST06]. Schloss [IEE01b]. Schneider [Puc03]. Schneier [Ano01e, Hei03, See04, Sty04]. Schnorr [BP02]. School [Coc02a]. Schools [PM00]. Science [Bis03b, Ccc03, IE00a, IE01a, IE02, IE03, IE04, IE05a, IE06, IE07, IE08, IE09b, Im03, McE04, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04, Pot05, Six05]. Scientific [CHT02, MH09, Lao08b]. Scientists [Coc01a, MH09]. SCN [BC05c, CGP03]. Scots [Rec01, Ros00b, Sin99]. Scream [HCJ02]. Scribner [Gas01]. Scripts [Urr01, Oue05, Rob02, Rob09]. scroll [GB09, HHCW07]. SD [ECM00a]. SDK [Ano02d, Bar00c]. SDL [HL06]. SEA [SPQ06]. SEAL [Flu02b]. Seamless [OKE02]. Search [B105a, Des00c, Eva09, FIPR05, KB07, LM02, MFD04, TIGD01, TIGD01].
WYY05a, WYY05d, FZ06, PM08].

**Searchable** [ABC+05, AFI06]. **Searches** [PGT07]. **Searching** [BSW09, GTTC03, OS05]. **Seattle** [ACM06, S+03, USE00a]. **sec** [KV01].

**Second** [ACM03c, Bra01b, BD08, CZ05, GW01, HTS02, JY04, KCR04, Ki05, KP01, NM09, RD01, ACM00, Irw03, Swa01, Tec06, TEM+01, VGM04, AGKS07, Ano03c, Ano08b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, Cop10, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DLMM05, Eva09]. **Section** [Ano04b, Ano07a, BK09, SGK08, TL02, KP03]. **Sector** [Cro01, MV01]. **Secur** [McK04].

**Secret** [ACS02, Alv00, Ano03c, BBDK00, BTW05, BI05b, BTW08, BP06, BM01b, CGH06, CGH00a, CH01a, CLT07, Cha04, CTY09, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG+05, CDI05, Di01, DKL00b, DNO09b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah67b, Kah96, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, Me04, MN01, NABG03, NN06, OKS06, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sm00a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, AJ08, AEEEd05, Ano02c, Ano08c, Bamb02, BCB+05, Ca01, CC05a, CH05a, CH05b, CJLO6, CN04, CDD00, DD04, DB04, DM00a, Di 03, DW01, Duj08, FRNC05, FWTC05, FZ06, Gal02, GIKR01]. **secret** [HT04, HJ07, HSK05, IY06, Kee05, KB09, Lam07, Lun09, MF07, MI09, Na01, PS02a, PW05, Ris06, Sch01e, SBZ04, SC05a, Sm01b, SC02c, Wan05, Win00, YCH04, ZSV05, dRMS05, vDKST06, HIl06].

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

**Secret-Sharing** [BI05b, CD000, CDI05, DKL00b]. **Secretly** [CC08]. **Secrets** [BH06, BBD+02, CMS09, CP07, Che00b, Cop04b, Di 01, G001b, Gun04, Kid07, KMS01, LKM+05, Lys08, Pag03, Pr04, Sch00d, Swa01, Tec06, TEM+01, VGM04, AGKS07, Ano03c, Ano08b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, Cop10, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DLMM05, Eva09].

**Secure** [Nid05, NNSK05, NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RV009, Rd01, ST01a, Sea05, SVDF07, SBG05, Sm02, SKR02, SNR04, SBEW01, Sty04, Tad02, VMS05, Van05b, VM02, VM03, WLL09, WBL01, WGL00, WH05, XS03, YWL05, ZYM05, Zho06, Aam03, Abd01, AEEEd05, AL07, AFGH06, BSD+09a, BDFP05, BCP07, CLOS02, CCMT09, CC04b, CCK04b, CRS09, CHH+09, CCD06, CG05, DG06, Dw04, FMY02, Geb04, GIKR01, GCKL08, HS09, HL03, HL06, HJW05, HBC+08,
Secure

[Ano12, BS01a, BSB05, CHKO08, FIP02b].

Secured

[BNPW03, Ito01, UP05].

Securely

[HL05a, LLK05].

Securing

[Abe01, Ca00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03a, LPW06].

Security

[AW05, AW08, Ahm07, AJ08, ADR02, And07, And08b, Ano02b, Ano03b, Ano06c, AHKM02, Ayo06, BP07, BW07, Bam02, BPS00, BBM00, BKR00, BP02, BNPS02, BY03, BP05, BOHL+05, BBR+02, Bis03b, Bla02a, BF06b, BDTW01, BCHK07, Boy01, BGM09, BLMS00, CG07, CK02a, CKN03, Can06a, CGHG01, Cer04b, CC02b, CSW+08, Che05c, CM05a, CH07a, CSY09, Chu03, Coc01a, CK06, Cor00b, Cor02, CGP+02, CG05, Dr.00c, Dal01, DN02a, DKMR05, DeL07, DJ06, Des00c, Dim07, DR02d, DSS01, DK05, DS05b, DBS+06, Elb09, Elv09, Elv02, FIP01b, FBW02, FW09, FLY06, For04, FML+03, FMY01, GS02a, GSS03, Gum04, Gut02b, Gut04a, Gutxx, HM00, HSZ01, Hei07, HM02b, Hir09, HLL+01, HGPN+03, HQ05, HL05c, HL05d, ISO04, Ina02a, Ina02b, Int00, IKY05, IH04, IKP+07, JY04, JP07, JP02b].

Security

[JSW05, JG07, Jol01, JBR05, JK02b, JK02c, JM02, JQY02, Kan01, KM02, KSHY01, KL05, Ken02a, KB06, KMZ03, KDO01, KM05, Koc02, KHL09, Kos01a, Kov01, KXD00, Lad06, Lai03, Lan00a, Lan04b, LGS01, Lee04b, LKH+08, LKH09, Leh06, Len01, LNS02, LL04d, LSH03a, LSH03b, Lin02, LXM+05, LWK05b, LP01, MJF07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Mil01a, NIS01b, NJD01, NNAM10, NP07, Oka00, OP01a, Ort00, PV06b, PSC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PT07, PP07, Pho01, Pie05, Plt01, Poi02, PHM03, Poo03, PF03, PS05, Puc06, QCB05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sal03a, SJT09, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch01f, See04, Sha05d, SLH03, SLG+05, SL05a, Shp02].

Security

[Sko03, SEF+06, SEK01, SEK02, SK06, Sta03, SB07, Ste05b, SBZ02, Sty04, SKI01, Sum05, Swi05, Tan07b, TG07, TG04, TPPP07, Uni00a, USE00d, USE01c, USE02b, Uni00c, Uni00d, Uni00g, Uz04, Vau02, VMC02, WLT05a, WBL01, WWL+02, WA07, YEP+06, YWD08, Zan01, ZWC02, ZDW06, Zhe02b, ZYH03, ZS05, blL07, AA04a, Ano05c, AJ01a, AJ01b, BPS08, Bai08, Baut05, Bej06, Bel07b, BR04, BGP09, BFGT08, BFG08, Bjo05, Blt07, BJ02, BMW05, BG07a, Br06, BMV06, Can01a, C+02, Cha07, Cha05b, CKL+09, Che00b, Che05b, CKRT08, Chi08b, Chi08c, Chi08d, CIL06, CJM00, Con09, Con04, CC05e, DP04, DKK07, DY01, DFGH04, Des00a, DWML05, DKU05, DMS07, Egh00, FXAM04, FR08, FOP06, GH08, GJ06, GJJO5, Gha07, GJ03, Gor05, GKS05, GMW01, GC05, Gut04c].

security

[HN04, HCD08a, HCD08b, Har05a, Hei03, Hen01, Hes04a, HM05, HSL+02, HL06, HG05b, Ino05, JEZ04, Jan00, Kad07, KY00, KPS02, Kim02, KVD07, Kov03, KH03, Kwo03a, LLM07, LC03, LL03, LLY04, LL05b, LPW06, LM+03, LMB05, LLL06a, LLL06b, LHC08, MJ03, Mal06, Man08, Mau05, Man04, May01, MKKW00, MSK03, MG06, Men03, MS02a, MK05a, MPPM09, OP01b, Pae03, PSC+09, PC05a, Pat02a, PY05, PP06a, Pau03, PHS03, PIP03, Poi00, PS04c, Rie00, RC05, Ros06b, RN00a, RN00b, SNI00, Sal05d, Sch03, Sch02, Sch04d, Sen03,
SHL07, Shu06, SPHH06, Son00, SH00, Sta02a, Sta06, Ste02, Sun00b, SHT05, SLL+00, 
Tsa05, Uni00f, Vac06, Van03, Voi05, VS08, 
WAF00, WDCJ09, WA06, Won01, WK06, 
Woo05, XQ07, YW04a, YY05b, ZSZ01, 
ZW05b, ZSN05, dCdVSG05, vOWK07].

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

Security-related [Gutxx].

security-sensitive [SPHH06].

seeing [Wal03].

Seek [Coc01a, PH03, SH00, Uni00b, Won01, WK06].

Seeking [Mos06].

Seeks [CAC06].

Selected [BKP09, Bar00c, CCMR05, CSY09, 
CH05, HA00, MS05a, Neu04, PT06, R000e, 
ST01d, VY01, YR06, AMW07, Bir07, BC05c, 
CZ05, CKL05, DR05, HH04, HH05, PC05a, 
Win09, WK06, AMW07, HH04, HH05, MZ04, 
NH03, PT06].

Selecting [Bur03, dB07].

Selection [IBM00, KK+07].

Selective-ID [CS07c].

Selectively [Chi08e].

Self [GMM08, HW05, KY01d, LXH07, 
PS01b, PBC05, Sch00b, W0L05, WLT05b, 
ZKL01, BCL05a, BCW05, CSV07, CWH00, 
CCH05, CJ05, Fis01a, HW04, H0L04, Lee04a, 
LL06, LS05b, LWK05a, PC05b, SH11, 
Sha04b, Sha05b, TLH05, Tsa05, TJ03, 
W0H03, Wy05].

Self-Adapting [SH11].

Self-Certified [LXH07, HW05, BCL05a, 
BCW05, CCH00, CCH05, CJ05, HW04, 
HL04, LL06, LWK05a, Sha04b, Sha05b, 
THL05, Tsa05, TJ03C, W0H03, Wy05].

Self-Defence [Wy05].

Self-Enforcing [GMM08].

Self-Escrowed [PS01b].

Self-Localization [WLT05b].

Self-Modifying [CSV07].

Self-Pairing [Lee04a, PC05b].

Self-Protecting [LS05b].

Self-Shrinking [WHL05, ZKL01].

Self-Similarity [Sch06b].

Selling [Bla01c].

Semantic [PBV08, SN100, Sch00c, Coc01a].

Semantically [KI01b, ST01a].

Semantics [Li01, Mar02b, BFG04, BFG05, SW02].

Semi [Fer00, Nak01, SY01b].

Semi-Equivalent [Fer00].

Semi-Fragile [SY01b].

Semiconductor [Coc02h, Igi02, UHA+09].

Sensational [Cop04b].

Sensibly [See04, Syl03, Sch03].

Sensitive [HT06, Bro05b, SPHH06].

Sensitivity [SDMN06, GSK09].

Sender [AAEQ05, CS08b, DBS+06, Fin06, GPCS08, 
LNL+08, NAB03, NNAM10, PZDH09, 
ZYN08, AJ03, CCM09, HMM0LM07, 
JJR09, KXTZ09, KHYM08, LDH06, 
LPV+09, LN04, LOP06, MWS08, MS09b, 
NC09, NLD08, PS08a, RAL07, TP07, 
WDLN09, ZSN07, AMB06].

Sentry [Kum07].

Seoul [CKL05, KCR04, Kim02, LL03, LL04d, 
May09, PC05a, PK03, Son00, Won01, WK06].

Separable [CD00a].

Separating [MKK00, Nie02b].

September [AUW01, AAC+01, AJ01a, BCKK05, BC05c, 
CS09, CGP03, DV05, D0KU05, DFCW00, 
EBC+00, ELV01, FLA+03, GKS05, QS00, 
RS05, SM07b, WK03, dCdVSG05, AJ08].

September19 [AJ01b].

September19-21 [AJ01b].

Sequence [HWH01, MS02e, WHL05, ACTZ05, GB09, 
SL09, W0G2, YZEE09].

Sequences [ADD09, Bi09, XYXX+11, FSGV01, HG05a, 
JZCW05].

Sequential [GSS08, SNW00, RHH03a, WH02b].

Serial [CTLL01, KWP06, Uni00g, Mit00].

Server [ANRS01, BMK00, Dew08, KO00, LK00, 
NS01b, PS05, TMM05, XS03, Zha00, 
BB05, LHL04b, LHL04a, LKY05b, LHL03b, 
NTO07, Tsa08, Tsa01, TWL05, YS04].
Server-Aided [NS01b]. Server-Assisted [XS03] serverless [BDET00]. Servers [BIM00, HS07, Jab01, KCD07, Mar02a, TEM+01, LS05b, PT08]. Service [BACS02, BH00a, CLK01a, DeL07, KZ01, Lan04a, LDM04, Nik02a, Nik02b, PKBD01, CUS08, HILM02, KWDB06, LB05, Mir05, MV03b, SR JM01, SSM+08, UG08, Cac02b, Hila06].

Services [ANSO5, BCS02, DJLT01, ECM00a, ECM00b, Knu07, Tsa01, Uni00b, WL07b, BDS+09a, BFG04, BFG05, BFG08, CCCY01, HM05, JRB+06, MW06, MPPM09, MV03b, RR04, SBG07, SL05b, TWL05, WA06, BH00b].

Serving [LLK05]. Session [GL01, OHB08a, CS04, OHB08b, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YW05]. Session-Aware [OHB08a, OHB08b]. Session-Key [GL01]. Sessions [KPR03]. Set [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDET00, Che07a, CC05d, DM00a, Ehl08, Mar05b, Sta00].

Setback [MYC01]. Sets [CFS05, EIG01, TW07]. Setting [BBM00, DLY08, LP01, PGT07, GMLS02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC+01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SGB01]. SGI [Bar00c]. SGID [Tot00]. SHA [AD07, BC04a, GLG+02, HK01, MP06, SK05a, TYLL02, WYY05d, WYY05b, WYY05c].

SHA-0 [BC04a, WYY05d]. SHA-1 [GLG+02, HK01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TYLL02]. SHA-512 [AD07, GLG+02]. SHA1 [WYY05a]. SHACAL [KML+02]. Shacham [Hes04a].

Shamir [BB79, SP79, Coc03, PW05, VS08]. Shamir’s [LD04]. Shape [Gan01b, Gil07]. Shapes [OMT02]. SHARC [DMSW09]. Share [CT08a, CDI05, FS04, AEEdR05].

Shared [ACSO2, BH06, BBDK00, BT02, CGH00a, TEM+01, PW03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01]. Sharing [BTW05, Bl05b, BTW08, BGP02, CD00a, CLT07, CC08, CTY09, CDM00, CF02, CFS05, CDG+05, CDI05, Di 01, Di 03, DS06, DP07, FM02a, FPS01, FMY01, HN02, KI02, KOS03, LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, SZ01, Sun00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CDD00, DD04, DM07a, DKL00b, FWTC05, GIKR01, HT04, HK05, HY06, LTO4, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YH04, YCY07, ZSV05, dRMS05, vDKST06].

She [Gu05]. Sheets [MNS01]. shell [Dw04, Gu05, BS01a, BSB05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [McK04, CZ03, YWC05]. Shift [CGFSH09, Che08a]. shifting [Cal00e]. shifts [Neu06]. Shin [Kuh08, Kuhn08]. Shines [Coc02b]. Shinko [An00d]. Ships [An02e]. Shops [An01c, YSS+01]. Shor [KLB+02a]. Shores [KKP02]. Short [An01o, 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, WHL05, ZK01].

SHS [An008d, An012]. Shuffle [FS01c, NSK05, Sas07]. Shuffles [Mir02]. Shuffling [PBD05]. shut [Gil07]. SiBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [An01j, BU02, KSWH00, Law09a, LL01, M02, OT03a, OT03b, S06a, WC04, CNPQ03, PSP+08, WL07a]. Side-Channel [BU02, Law09a, M02, CNPQ03, PSP+08].

Side-Match [WC04]. Siena [BCKK05]. sieve [CM05b, JL03]. sieves [Har07a]. SIGABA [Lee03c]. SIGACT [ACM03c, ACM05b, RA06]. SIGART [ACM03c, ACM05b]. Sight [Col03].


SIGMA [Kra03]. SIGMOD [ACM03a, ACM03c, ACM05b, ACM04a, FMA02]. SIGMOD-SIGACT-SIGART [ACM03c, ACM05b]. Sign [BSC01b, BTTF02, Dav01c, Kra03, Dav01b]. Sign-and-Encrypt [BTTF02, Dav01c]. Sign-and-MAC [Kra03]. Signal [BSC01b, BTTF02, Dav01c, Kra03]. Signalling [ECM00b]. signals [Ren09]. Signature [ANS05, AAK09, AR00, ADR02, Ano01c, Ano01g, Ano09b, Ano13, Ara02, AR01, ACJT00, Bar06b, BNPS02, BGOY08, BMS03, BDS09b, CM00, CD00a, CL04a, CK02a, CGP08, CM05a, CK02a, CWH00, CL04b, CYH04, CS03c, DT03, FSW01, Gir06, HM02c, HLT01, MS01, Nam02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKKY03a, LKKY03b, LFW04, XH05, YRY05d]. Signatures [AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCCN01, CD00a, CL01b, CNV06, CZB+01, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZI01, Her06, HM02b, HS01b, HHGP+03, HLTO1, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00a, MM02, MNFG02, PCG01, Ram01, RR02, Rdo01, WV01, X509, Zhou02, Ano00i, Ate04, AH05, BLH06, BB05, BMW02b, BMW02a, BLRS09, Cal00a, CKK03, Die00, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HLH00, JLL01, JLL04, KKKL09, LV07, LG04, LG09, LS05b, MJM05, PLJ05a, PBV08, Sch01f, Sha01d, NZS05]. Signcryption [Boy03, LXH07, MLM03, Zhe01]. Signed [FL01b, OSSST04, Sch01a, SJ00]. Signer [DKFX05, CJT04, LL05b, WK05, IR02]. Signer-Base [IR02]. signer-verified [CJT04]. Signers [LZL+01, Sae02, Sha03c, YTH04]. Significant [SZ01, MS02b, Shp02]. Signing [An000i, IR01, RR02, HW004, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imr03, Ree01]. Simple [AKS06, CYH05, CJS01, CJ03d, CWY05, CC06, CS03c, DT03, FSW01, Gir06, HM02c, HLTO1, MS01, Nam02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKKY03a, LKKY03b, LFW04, XH05, YRY05d]. Simpler [Lin03]. Simplicity [MS01]. Simplification [DJ01]. Simplifications [JS05]. Simplified [Bon01]. simplify [Sma06]. Simplifying [Gut04b]. Simply [Oni01]. Simply-Iterated [Oni01]. Simulatability [HU05]. simulatable [Lau05]. Simulation [DKMR05, KL05, CPG+04]. Simulation-Based [DKMR05, KL05]. Simulations [WBRF00]. simultaneously [Wu01]. Singapore [BDZ04, TLC06]. Singh [Imr03, Ree01]. Single [GIS05, KO00].
MM01b, MM01c, WLZZ05, SV08a].

**Single-Chip** [MM01b, MM01c].

**Single-Packet** [WLZZ05]. **Single-Server** [KO00]. **Singular** [AS08, Bai01b, BR09].

**SINOBIOMETRICS** [LLT+04, Li05]. **SIP** [NTW07, PM00, SZ08]. **Sir** [Bud06]. **Site** [AEV+07, Coc02a]. **Sites** [Che01d, Ros07]. **situation** [AJ08]. **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]. **SLAAC** [CGBS01]. **SLAAC-1V** [CGBS01].

**slide** [Fur02b]. **Small** [CCM05, ELvS01, Fin02, GPS06, MNT+00, May02, OTO3b, RKO6, SCH01e, SPOGQ06, WAL03, YLC+09, DJ08, 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, QS00, QS01, RE00, RE03, RS01, Sak01, SR01, Sha01c, SP02, TBDLO1, VPG01, YKM01, An00k, An001, An04f, AJ01a, Bar03, BPR01, BCHJ05, BGL+03, Bur00, Cal00c, CCCY01, Cha05a, Cla00b, Con00, CH00, DMT07, DFH01, DFST07, FCZ05, Fin03, GMG00, GUQ01, HHS01, Hus05b, Hus01, Jua04, KLY03, LKY05a, Lcr02, LC05a, Lu07, MY01, Pha06, PB01, Pre07, SVDF07, SLH03, Sm00, TIS07, VK08, WC03b, YW04b, YWWD08, Za00, BJVdB02, CL04d, CCK04b, Che00a, DFPS06, FGLO2, Gro03, HLO5b, Ku04, KC05, LHY02, Pau02b, SKKS00, Sco04, SCFO1, TV03, YW04a]. **smart-card** [GMG00]. **Smartcard** [HW04, KRV01, RMCG01, Uri01, PBVB01, BBPV00, CGMM02, DM07b, HRS02, Ito01, KS02]. **Smartcard-Based** [RMCG01, CGMM02]. **Smartcards** [CMG+01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, An004c, RM02]. **smarter** [Car01, Cla00b]. **Smartly** [MS01]. **SMS** [R09]. **SNAKE** [R09]. **Sneak** [Ade09]. **Sniff** [An02c]. **Snort** [GC05]. **SOAP** [DJLT01]. **Social** [Ros07, Man08, AG09]. **Society** [GL05, Kat05b, EY09, LWZH05, Sae02, Sha03c]. **Socket** [ZL04c]. **Soft** [DV08]. **Software** [Ahm07, And07, An02c, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HHH01, Hoe01, Joh03, Knu07, KSW06, Lal06, Law09a, LSY01, LLLZ06, LSVS09, LTM+00, MNT+00, MSNB07, MKY08, MG06, Nd05, PM00, PS01a, Sch01a, Sch00b, Sto00, USE00b, VH09, VVS01, WHL05, W014, ZCC01, ARJ08, An003b, Bir07, Che01e, CT02, CCD+04, CT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, KA09, Mat02, M008, MN00, MSNH07, An04h, An00j, Bir07, Che01e, CT02, CCD+04, CT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, KA09, Mat02, M008, MN00, MSNH07, An04h, An00j, Bir07, Che01e, CT02, CCD+04, CT07, CC04c]. **Software-Only** [Hoe01]. **Software-Oriented** [ZCC01]. **Software/Hardware** [Nd05]. **SOI** [An02c, NFQ03]. **SOISIC** [An02e]. **Solaris** [An06c, BH00b]. **SOLomon** [KY02b]. **Solution** [Cap01, CJT02, DHR00, LLS05b, Poh01, Str02, TvdKB+01, LSH00]. **Solutions** [An04c, MV01, Jan00, MSK03, MV03b, St.00, Gum04]. **Solve** [CU01, GS03]. **Solving** [CJT04, GPP08, Wil01a, Bul09, Whi09]. **Some** [AG01, BDF+01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, Han04, He02, JK01a, RSS04, SHT05, ZF05].
Someren [Ano03g]. Something [FL01b].

sometimes [FNRC05]. Sons [And04].

Sorry [San05]. sorts [Ano03g]. Soul [Bla01c]. Sound [BJP02, FR08]. Soundness [ABHS09, MR01c, BPS09, Lau08a].

Source [Bar00c, Bol02, Gut00, HBF09, KLR09, PM00, RK06, TEM+01, Ano03d, BGL+03, CBB05, Mea08, RVS09, SB05, Bar00b, Lin02]. Sources [KZ07, WLZZ05, KZ03]. Southampton [Bla03]. Soviet [AJ08]. SP [BG07a, Hir09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPA-Based [Nov01].

Space [BGH07, Lu02, MSNH07, NS05a]. Space-Bounded [Lu02]. Space-Efficient [BGH07]. Spain [BS03, DFPS06]. Spam [CMB+05, DGN03, Vix02]. Spamming [Bel04]. SPARK [Jen09]. Sparse [BLST01, BG+01, FS01b, G03, BS02, BF06a].

Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09]. Spatial-Domain [SDFH00]. Spatio [CDTT05]. Spatio-Temporal [CDTT05]. speakables [BZ02]. Speaker [LM00]. Speaks [VN04].

Spec [Bar00c]. Special [Ano04b, Ano07b, Ano07a, B+06b, GIS05, GS07a, GPP08, SGK08, KP03, FOP06]. Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08]. specialized [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00a, LKLJ01, RSA00c, Mea04].

Specifications [IEE00b, BDFP05, BD04a]. specificity [GSK09]. Specified [Tad02, He02, LKW05b, YY05a, ZX04]. Specifying [BJvdB02, Cir01, SBS09].

Speer [KGS07]. Spectr [GMM01]. Spectr-H64 [GMM01]. spectra [MS02b]. Spectral [QP05, SK07]. Spectrum [BQR01, LLY07, PM00]. Speech [MRL+02, AA04a, PY08].

Speech-Generated [MRL+02]. SpeechStudio [Ano02e]. Speed [Ano00d, Ano02d, Gro01, JKRW01, KMM+06, Lut02, SOTD00, SM02, Wie00, YKMY01, BGL+03, RW07, RMCG01].

Speeding [Osv00, SWH+09, TC05]. Speedup [YKLM02b, YKLM03]. Speedy [Cre00]. spherical [LZP+04]. Spider [Tur04]. Spies [Gan01b, Win05c, Hau06, NRR00]. SPIHT [Che08a]. SPIN [MS02a]. Spline [SPK08].

Splitting [GMW05, LLK05]. SPN [HLL+01, Kan01, PQ03b]. SPNs [CL+03]. spot [Naf05]. Spread [BQR01]. Spring [Pap05]. Spring-Verlag [Pap05]. Springer [Fal07, Lee03a, Lee03b, Pho01]. Sprinngs [Wil09]. spying [Cas03, FNRC05].

spymaster [Bud06]. spyware [Ste05c]. SQL [Dew08, HILM02]. Squadron [OC03].

square [HCK09, HQ01]. Squaring [CH07b, NSS02]. SRAM [HBF09]. SSC2 [HQR01, ZCC01]. SSH [All03, BS01a, BSB05, KBN04, Dwi04, Hsf01, Hos06b, Kra02b, Naz02, Oue05, SWT07, Str02].

SSH-Connected [Hsf01]. SSHFS [Hos06b]. SSL [ASK05, BPT02, CHVV03, JRB+06, KCD07, KPR03, Kra01, LLK05, LKW00, Net04, OHB08b, OHB08a, SB01, SQ01, Vau02, ZFK04].

SSL/TLS [BPT02, CHVV03, KPR03, OHB08b, OHB08a]. SST [Gau02]. St [GKS05, NH03, AS01a]. Stack [Pot03]. Stage [Kak06, CY05b]. stamp [CL00]. stamping [HHC05]. Stamps [KZ01]. Stand [CAC03].

Standard [Ano08d, Ano96, Ano12, Ano13, Bar00a, BCP02a, FIP00, FIP01a, FS01a, Her09a, Hug04, HLC08, IEE00b, MM01c, MP01a, Nat00, PM00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, Ano04e, BBK+03b, DR05, GMR08, Sea09, Tan01, AHE17, Ase02, Bar00c, III00, Bur03, CMR06, C02a, C02b, C05, DR01, D02b, Dan01, FIP02b, GC01a, Har00, Lan00a, Lan00b, Lan04a, Mor05, NIS00, SB00, Sta00, Sye00, WBRF00, Wr01, YW06].

Standardized [Man01]. Standards [Ano01g, Bur06, CL07, C02b, Hus01].
RSA00a, Tsao06. Standing [Lan00b]. Star [Pot05].

State [And07, CR03, GST04, HBF09, Kar01, MSNH07, Ris06, TL07, Mit00].

State-transition [TL07]. statecraft [dL00]. Stateless [ANR01, NNL01, SK05b]. Stateless-Recipient [ANR01]. States [LB04, Jol01]. Static [CW07]. Statistical [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, L01, LLL+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]. statute [Cal00b]. STDM [WMDR08]. Stealing [Gan01b]. Steering [HR13]. Stefan [AUW01]. Steganalysis [Pro01, Sol05b, GSK09, WW04]. Steganografi [Sch09]. Steganographic [CTL04, HR02, MJF07, RH02, RS00, Wes01, KC09a, LYT02, WWTH08, YCL07].

Steganography [BC05a, BG108, CYH01, ChLYL09, CRD01, CW09, CTH08, Col03, CMB+08, CS05c, DIRR05, DRL09, FGD01, Fri07, GAL03, HCBLETRG06, HVAM02, HVAM09, Hun05, HSC01, LS08, PH03, Sal05b, Sch09, Sha01e, Sh08, 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, Ano04c, MP07, SL06]. step-by-step [SL06]. Step-out [KKKL09]. Stepping [WRW02]. steps [Bih02].

Sterotypes [GO03]. Stern [CPG08, CS05b]. sticker [GXP08]. Sticks [Sam01]. still [Ano00f, Rie00]. Stinson [Spr03]. STL [Zol01]. STOC [ACM05c, ACM07, ACM08, ACM09]. Stochastic [MG01]. Stock [Bar00a]. Stone [MLM03]. Stones [WRW02]. stop [SSNGS00, Win05c]. Storage [DFSS08, Din01, Din05, HR02, Har07, Hug04, MTS04, RCB00, Ric07, RH02, Vados, AFGH06, DFSS05, 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, TCPPM07, KC09a]. Stream [BCC01, BC05b, BSW09, BS00b, BL02, CF01b, Can06b, CJ01, CJ02, CM03, Cou03, CL02c, DF07, Fil00, FF01a, Gol01d, Gol01e, GBM02, HJC02, HR00, HR04a, Jam00, KHD01, MSNH07, PP06a, SM01, Sar02, SXY01, WB02, Wu02, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, BV+04, DS09, DK08, KH08, Max06, M09, MRT10, PCS03, SCC03, SB05, WW08].

Stream-Cipher [SXY01, WW08]. Streaming [OS05, CBB05]. Streams [AIP01, CO09a, YLC+09, ZCW04]. Street [Mec04]. Strength [CB01, JX05, On01, CL+09]. Strengthening [Lo00]. String [CPS07, DFSS04, Pas03, Dam00, RG05]. Strings [Vau05b]. Strong [ADD09, BB00b, CS00, DKFX05, KJC+01, KW00, LHS03a, LHS03b, Lu02, Pau09, SBZ02, WHL05, Ano01m, CC04b, HRS08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04]. Strong-Password [LHS03a, LHS03b, WHL05, CC04b, KTC03, Ku04]. Stronger [LLM07]. Strongly [IY06]. Structural [BS01c, LBR00]. Structure [DNS07, EIG01, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SLL+00, XMST07]. Structured [BRTM09, CKK03]. Structures [Ano02e, DS06, GTC03, HCD002, KCP01, Kus02, MND+04, MFT05, PSC+02, PQ03b, Sun00a, XH03, Hen06a, IY06, SWR05].
struggle [Bur02]. Stuart [Gum04].
students [AA04b, PP09]. Studies [Pag03, LFHT07, SPHH06]. Study [BBGM08, Car02, DPR01, DP00, KKK+07, WCZ05, BKN04, BF06a, DY09a, KWDB06, SKW+07, ZWWL01]. Sturgeon [Wei05, Wei00, Wei06].

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]. Substructure [MRT10]. Subsystem [HL07, MB04]. Subtleties [Lai08]. Subverting [HB06]. Success [Ano06d].

Successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Sufficient [IKO05, Kos01b, KO00, MN01]. Suffix [ABM08]. SUID [Tot00]. SUID/SGID [Tot00]. Suitable [AIK+01, CQS01, KTT07, LKH09, SP05, Wen03]. Suite [RSN+01, SBWE01, YLT06]. Suited [WWGP00]. Sun [Che04b, KLY02].

Sum of-Digits [Che04b]. Sum [CY08, Shp05]. Sunspots [CPS07]. Super [Lam07, CAC06, Hos06b]. Supercluster [Pri00]. Supercomputer [Coc01a, Wa109]. Supersingular [Gal01, RS02, Ver01].

Supervision [FDIR00]. Supplementary [TBDL01]. Supplementary [ECM00a, ECM00b]. Supplies [Sha01c]. Support [ABM00, Gro03]. LTM+00. PZDH09, SBG02, Ano04e, Ano05c, BMA00a, BMA00b, BMA00c. ED03. mSgfLt05. SSM+08. WNQ08. ZYL05]. Supporting [CLK01a, SW02]. Suppression [GA05]. Sure [Tom06]. surface [Iwa08, LDD07].

Surfaces [SPK08]. surveillance [Che01f, LCS09]. Survey [EPP+07, FDIR00, KM04b, LDH06, MS10, ATS04, Ano00e, BEM+07, CF05, CDL06, EY09, LOP04, Mea04, Müü01b, 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 [Bor01, Jef09, May09, MT07, MP05, ALV02]. symbols [Lun09]. Symmetric [Ano01a, ABM00, BU02, BKM07]. ČvTMH01, CCM01, Des00b, EP05, FW09, Fil02, RR00, Ust01b, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01].

Symmetric-Key [Ano01a, ABM00, CCM01, EP05, RR00, BMA00a, BMA00b, BMA00c]. Symmetry [RF08]. Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, Ano00d, BS03, BCDH09, BC01, CGM07, IEEE00a, IEE00b, IEEE02, IEEE03, IEEE04, IEEE05a, IEEE05b, IEEE06, IEEE07, IEEE08, IEEE09b, Jef08, KM07, MFS+09, SMP+09, TCL06, USE00d, USE01c, USE02b, May09, dCdVSG05]. synchronisation [CmV06]. Synchronization [GPCS08, SW02]. synchronize [Pau02b]. Synchronous [CH01b, Sar02]. synopses [YLC+09]. Syntax [BWBL02, RSA00b, RSA00d]. Synthesis [XFZ01, SOIG07, UBE09]. syslog [ME08b]. System [Ano02d, Ano02e, ANR01, BIP05, BCST00, Bih00, CDP01, CHM+02, CSW+08, CGJ+02, DJ01, DGP07a, DGP07b, DV08, EM03, FL01a, Ito01, Joh05, KC02, KHY04, LV00, LSS05b, LXM+05, MA00a, MA00b, My01, MFK+06, MFS+09, RH02, SR01, Sha02, SOII02, Ste05b, TK03, TZT09b, USE00a, WG05, WA07, YKMY01].
YKLM02b, ZYM05, AHK03a, AMRP00, Ano00j, ADH+07, AAKD09, Bn09, BDET00, Bu09, Cco2b, CCH05, CJL06, CPG+04, Coc01a, Cre00, CO09b, DZL01, DPT+02, DIM08, DG09, GG08, GSK09, GGMG00, Gou09, HLL+02, Joy03a, KWDB06, KXD00, Kwo03a, L04c, LKJL01, Lin00a, LK01, MKKW00, RCG05, Sal00b, SCS05a, SGMV09, SETB08, Wan04a, dB07].

dimensional [DW05, ZL04a].

Systemic [KB06].

Systems [ACM03c, ACM05b, ANRS01, Ano02e, BCS02, BRTM09, CP02, ELvS01, Fel06, Gr03, GRW06, IEE01b, JQ04, Ket06, Mar02b, MMY02, NABG03, RS05, Ri02, SM01, Sas07, SJT09, SXY01, USE00c, USE00b, Vav03, VHP01, WKP03, ARJ08, Ando08b, Ano01n, Bid03, Ble07, CGL08a, CGL08b, CGL08c, CCM01, CNPQ03, CHT02, CG05, CSG05c, CO05b, Has00, Tsa08].

table-based [Has00].

Tables [AJO08, KB39, RBF08].

tactics [Cal00c]. Tag [KKJ+07, NAM10].
tagging [BP05]. Tags [OS06, ACM05b, PLsveL010].

Taipei [Lai03].

Takagi [LKYL00].

Takagi-cryptosystem [LKYL00].

Takaragi [WHHL03].

take [Heg09, Per05b].

Taking [CDS07, Lai07, PM00].

Talk [FGM00a, Lan00d].

Talking [Ano01p]. tamer [Kap05].

Taming [Aba00, Lov01].

Tamper [LTM+00, CT02].

tamper-proofing [CT02].

tampering [PS08b].

tandem [DPT+02].

Tang [YRY50].

tank [Pau03].

tar [Str02].

targama [MAA02].

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].

TC8 [DFC00].

TC8/WG8.8 [DFC00].

TCB [SPH06].

TCC [HR06, KI05, Nao04].

TCP [CD01b, OS00, SBB05].

TEA [CV05, HS101, HS01, HHK04, MHL02, WN95].

Teaching [Mc08, Shu06, GV09, Jan08].

Tech [Ko01a, TvdKB01, Uni00c, Gra01, Ros04, Uni00f].

Technical [BHM03, GS07b, Lan00c, Scr01, TL02, USE01b, USE01a, USE02c].

Technique [CC02a, Pau09, P03b, SC02a, WC03a, vW01, CL00, Che08b, Pau03, Ren09, WC05].

Techniques [AIP01, BSW09, Bib03, BBP00, BDP02, CR04a, CR05a, DBS+06, D06, Gal03, KLN+06, Ken02b, Kn02, KO03, MKP09, NCR04, PJK01, P01, Pre01, Shi08, YKW01, AB09, BMW05, BR05, Che08a, DY01, DMH07, DY09a, Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08].

Technologie [RSA09b].

Technologies [MS05a, PP06b, Sam09, SE00, VH09, Way01, Way02a, ZW02, A904, PB01, TTZ01].

Technology [CZK05, Cla00a, GS00, GS04b+06, MP03, P03b, TF03, AL07, Ble07, Car01, Cas02, Che00a, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b, Six05].

Tektronix [Ano01c, TecCorroo, LM00].

telegram [Tu66].

Telelogic [Ano01c].

Telephone [KZ01].

telephones [CF05].

Telephony [Ano02c, CFRR02, PM00, CG09].

teleportation [BEZ00, BEZ10, Duw03].

Telling [Gan01b].

template [LLC06a, UEP09].

Temporal [CDTT05, KXTZ09].

Ten [ES00a].

Tenth
Term [ABRW01, Dur01, BMV06, ISO05, LG04, SGMV09, WDLN09]. Terminal [ECM00a, ECM00b]. Terminals [Chi08a, ISTE08]. termination [BP05]. terms [LMTV05]. Ternary [AD01, DKL01]. Terrorism [PP06b].

terrorists [Mad04, Win05c]. TESLA [LN04]. Test [BT02, HSS04, Lan00b, LN08, RSN+01, Way02a, DS00, GMG00, Kat05a, KKKP05, RSS04]. testable [RMPJ08]. Testing [III00, CGBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03].

Tests [MT02, NM09, GT02, Gut04c, JPL04]. Testable [RMPJ08]. Testing [III00, CGBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03]. Tests [MT02, NM09, GT02, Gut04c, JPL04]. Text [Lut02, PJH01, PM08]. textbook [BJN00, PP09]. Thank [CMB+05]. Theft [CMS09, Ana011, Phi06]. Their [AGT01, CD00a, Gen04a, JKRW01, LLL+01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, Sti11, TO01, WV00]. Them [WD01a, Tco06]. Theorem [AC02, Eke02, GN01, Sho00a, Sch01b, YKL03]. theorems [MW04, Nyb01]. Theoretic [CB01, DHR00, Kat05b, Nie02b, VVS01, VDKP05, vW01, Mar05b, NR04, Shp99, Wag03]. Theoretical [SGB01, PRS04]. Theoretically [AP09, DM00b]. Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bib03, Boy01, CC04a, Cra05a, Des02, Fal07, HR06, Hay06, IZ00, Irw03, Kim01, Kmo02, Lai03, Lee04b, Liu03, MNT+00, Mao04, NP02a, Nao04, Oka00, PY06, Phi01, Pre00, Rot05, Roy05, Sch06b, Shp03, Spr03, TW02, TWW06b, Vau05a, Wa00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cas06, Cos00, DW05, Gar04, HHL+00].

HW98, Joy00, Kii05, Lif00, Lam01, PPV06, Rot02b, Rot03, SCS05a, Sho05b, Ste08, Sti95, Ste02, Sti06c, Tat05, TW02, Was08b, HR06, KXTZ09, Kii05, Nao04, Nie02b, Nie04]. THERE [Bar00b, GW00, Ne06]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Hei03, Sch03, Sma06].

Third [AL06, BS01b, CGP03, HR06, IKY05, KN01, MS02c, NIS00, Won01, WV01, CKL05, GS05, Z00, JZCW05, QS00, CGH+00b]. third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM00]. Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thirty-Fourth [ACM02]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT+00]. Thoughts [Joh00]. Threat [Por06, SS04, BK00, Geb04]. threatened [Ano00]. threats [CNPQ03]. Three [BR00b, Kak06, LSH00, MAA06, AJ08, CLC08, FGM03, GPS05, LHL04b, LKY05b, LLS+09, MF07, MANTxx, SPHH06, YCO09, ZL04b]. Three-Key [BR00b]. Three-party [LSH00, CLC08, LHL04b, LLS+09, YCO09]. three-principal [ZL04b]. Three-Stage [Kak06]. Threshold [AF04b, AIP01, BTW05, BTW08, BDDS03, BSS02, CDD07, CLT07, CDN01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, KS05b, In00, In02, Kog02, LZL+01, LCS03, LCZ05a, LP01, MSJ02, Nie02c, STY07, WQW01, Wan04b, WH03, XS03, BCW05, BMV02a, CL02b, CC05a, CYH04, CHY05a, Che05a, DG06, HW02, HW03, HW05, JLL01, JLO4, LCC05, LCZ05c, SCL05, TYH04, WHL03, XCV05, YTH04].

Throughput [HV04, LSO1b]. thwarting [WL07a]. thwarted [ADE09, SW05b]. TI [GBK01]. tib [MAA07]. Tickets [FGL02, KS02]. Tie [SZ05]. tier [TW07]. Tight [CM05a, DI01]. Time [AK02a, App07, AJO08, BPST02, BS00b, BSW01, C01, CJ03a, CNOV06, CL02, Dri02, GPCS08, HM02b, IN02b, KL05, Kuh02a, LP02a, Lan00b, LLD05, LDM04, May04, Oec03, Phi01, QSR+02, RR02, CAC03, CCK04b, CL00, DS02, GSO7b, GM04, HLTJ09, HHC05, LC04a, MRST06, NS05a, YZDW07, hYK08, DK08]. time-bound [hYK08]. Time-Domain [Kuh02]. Time-Free [CV06].
Time-Limited [AK02a]. Time-Memory
[AK02a, Oec03, QSR+02].
Time-Memory-Data [DK08].
Time-Reversed [Ina02b]. time-space
[NS05a]. time-stamping [HHC05].
Time/Memory/Data [BS00b]. Timed
[BS00b, CHK06, JP07, LKJL01, Mao01,
HGN03, Zha06]. Timed-Release
[AG08, CCK04b, Mol05]. Timestamp
[AJ08, CCK04b, Mol05]. Timestamping
[MSTS04]. Timing
[CKQ03, CWR09, Law09b, SCH01,
SWT07, ASK05, DKL+00a, KS09a, Oso00].
timing-attack [KS09a]. Tiny
[Bar00b, Min03, WN95, And03]. Tipsy
[TvdKB+01]. Title
[ZYH03]. TLS [BPST02, CHVV03, HSD+
05, JK02b, WRW02, WHI01]. tracings
[RE02]. Track [Fox00, Joy03b, Nac01,
Oka04, Poi06, PHM03, Pre02, USE02b,
USE02c, Men05, CAC03, CAC06]. Tracking
[WCJ05, FNRC05, Szo08, TML+09]. Trade
[AK08, CMS09, Oec03, PS01c, Un00f].
Trade-Off [AK08, Oec03]. Trade-Offs
[PS01c]. Tradeoff [LP02a, QSR+02, CW02,
Ino05, NS05a, DK08]. Tradeoffs
[BS00b, CAC03, CAC06]. Trading
[PV06b, SWH+09]. Traffic
[FG02, Mi08, Fe09]. Trail [DR02a]. train
[Pri00]. Training [Coc02a]. Traitor
[KY01d, KY01e, LLL02, SNW00, TT01,
WHI01]. Transacted [HBdJL01].
Transaction [RH02, AAKD09].
Transaction-Based [RH02]. transactional
[ST06]. transactions [Cal00b, Cal00a].
Transcript
[An01a, An01b, An01c, An01j, An01n,
An01f, Mal02, NK02b]. Transfer
[CT08b, Din01, GKM+00, KKL09].
Transferability [HSZI00]. Transfers
[IKNP03]. Transform
[ABM08, BCC+09, BR99, CPH04, KC09b,
LKL05, Nak01, SFSC09, V07, BR06,
Che07a, OP01b, SR00, LPZ06].
Transformation [CT09, HLL05, DSP01].
Transformations
[Fe06, KYHC01, LMV05, Pag03].
transforms [La00]. Transient
[Ric07, VS08]. Transistor [Coc02a].
Transistors [Bar00b]. Transit
[RS03, RS08, vDW04]. Torus-Based
[RS03, RS08, vDW04]. Toshiba [Pal02].
Tossing [Lin01c]. totality [HRS08]. Touch
[PAU02a, JP06]. toughest [Min03]. tour
[Pet08]. Town [KJR05]. Trace
[Bo01, LNS02, NN03]. trace-and-revoke
[NN03]. Traceability
[HLL03, HW05, WLLH05, WY05].
Transition [Ase02, TL07]. Transitioning [Ano09d]. Transitive [BN02]. Translation [GGS+09, PY06]. Translation-based [GGS+09, TransLink [Cal00c], Transmeta [GP00]].

Transmission [MLC01, SNR04, SVDF07, Smi03]. Transparent [CCDP01, Por01, Lin00a]. transport [Bor00]. Trapdoor [BPR+08, Fis01b, KO03, KO00, Gen04a, JSW05, PW08]. Trapdoors [GPV08]. trapping [Min03]. Travel [Bur00].Traversal [JLMS03]. Trawling [Knu00a, Knu00b]. treatise [Bla00, MAaT03, MAaT04, MAaT07]. treatises [MAaT06, MAaT07].

treatment [CL05, DK08]. Tree [CC05d, GST04, JLM03, KPT04, LKL05, LMK00, Mon03, PCC03, WL02].

trees [Che02, Che07a, TC00]. trek [Pot05]. Trends [Ahm08, KB07, Ort00, NdM06, PRS04]. tricks [Mit02b, All03]. triggered [HHJS04]. tripartite [SV05a].

Trips [CL05, DK08]. Tree [CC05d, GST04, JLM03, KPT04, LKL05, LMK00, Mon03, PCC03, WL02].

Tree-Based [GST04, KPT04]. trees [Che02, Che07a, TC00].

tree [Pot05].

Trends [Ahm08, KB07, Ort00, NdM06, PRS04]. tricks [Mit02b, All03]. triggered [HHJS04]. tripartite [SV05a].

Trips [CC05d, GST04, JLM03, KPT04, LKL05, LMK00, Mon03, PCC03, WL02].

tree [Pot05].
[SM03]. Usenet [Coc01]. USENIX [Coc01].

[Ano00k, BGP02, CL01b, CMB+05, DP00, FDI00, Had00, HY01, KZ09, LSZ05, MR03, OHB08a, PS01b, Poh01, Sas07, SSM+08, Str01a, Tsa01, WDCJ09, BBM00, CL04d, Chi08b, Chi08c, Chi08d, CF07, DSGP06, Dea06, DLY08, GMLS02, HW03c, Hsu05b, HL05b, KC05, LAPS08, LHY02, LLH02, LKY4, LKY05a, LHL03b, LC05a, LK01, OHB08b, Par04, SS03, SZS05, TWL05, WL05a, WC03b, YW04b, YS04, YRY04, YRY05d, ZYL05, vOT08]. 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, BJP02, BH06, BK06a, BBC+09, Bau01a, Bau01b, BP06, BPT02, BR09, BT02, BMK00, BMP00, BL02, Che01a, CL000, CGBS01, CCW02, CCM01, CC06, CH07c, Cin01, DI05, DPR01, DP00, DWN01, DGH+04, EFY+05, FJ03, FMP03, Fri01, GC01a, GL01, GSB+04, HHGP+03, HQ05, HJW01, Jab01, JKK+01, JSJK01, KEL05a, Ke05b, KM01a, KL+00, KTT07, Kra02b, KZ09, Lan04a, Len01, LB04, LS05a, LHX07, LM02, LH07, MS02a, MS09a, ML03, MS03b, MMJ05, NNAM10, NZCG05, NM09, OT03a, PHK+01, PJK01, PCK02, PK01, Sho00b, SK05a, Sma03a, SW00, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VPG01, WY02, W01, WC03a, XF01, YKMY01, YLL02, YSS+01, ZWWL05, Zhe01, AS00, AL07, BCL05a, BCW05].

using [BK07, CG06, CDS07, CWH00, CL04d, CCK04b, CCH05, CHY05b, CKY05, C05, Che07a, CKY07, Che08a, Che08b, CK04, CCK03, Cos00, DZL01, Dan02, DSGP06, DS09, DFG00, FWTC05, GC00a, GMR05, Gen09b, GS09, HHSS01, HW05, HAuR04, HTW07, Hir09, HW04, HLT09, HY03, HL04, JRR09, Jua04, K09a, KLY03, KB09, KKL09, KJ+07, KSW06, KR03, Ku04, KC05, LHY02, LLH02, LKY04, LCP04, LL04c, LW04, LKY05a, LW05, LWW09, LF0W04, LC05a, LCC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, Ptha06, RC05, SC04, SBS09, Sha04b, Sha05b, SL03, SH07, Tan07a, TL05, Ts0a, TJC03, V08, Wan04b, WK05, Wan05, WGL0, WH03, YW04a, YW05, YC09a, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. utilising [RFR07a, RFR07b, RFR07c]. utility [Gua05]. Utilizing [Str02].

V [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00e]. v2.1 [RSA02]. v2.11 [RSA01]. V5 [Ito00]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BLM01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [FM00]. Value [BR09, G05, LS08, BM02a, DK08, WTH08]. valued [DL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadharajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSNK05, Ber08, Duj08, Duj09].

Variants [BDK+09, DG02, KS00b, CJ05, Sha04b, TJ03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDhKB09]. vast [Wal04]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SB02, WC04, Pei09, mSgtL05, WNQ08, WC05]. vectors [LHL04a]. Vegas [ELvS01, IEE01a]. Vein [BDhKB09]. Vendors [Pau03, MV03b]. Venona [Ben01b, Ben04]. venture [SW05b]. Verenigde [dl00]. Veridicom [Ano02d]. Verifiable [AN01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Lys02, NZCG05, NZS05, NSNK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a].
Verifiably [BGLS03, Hos04a].

verifiably-encrypted [Hos04a].

Verification
[AAKD05, Ara02, BPST02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJL06, Coh03, DS00, HL05c, JW01, Ler02, MD04, MT07, MS09, PBD07, Tsa08, TYH04, Wun04b, Wu01, YLC+09, ZLX99, ZL04b, CS08b, Uzu04].

Verified
[BJP02, BFGT08, BFCZ08, CJT04].

verifier [Bla01b, LKY05b].

verifier-based [LKY05b].

Verifiers
[CL01a, He02, LV07, LWK05b, YY05a, ZX04].

Verify
[MS02a].

Verifying
[BFG08, BJvdB02, CJM00, HLT01, IR01, PT08, RR02, BLH06, BLP06, HL00, SV08a, Shal01d].

Verlag
[Eag05, Lee03a, Lee03b, Pap05].

Version
[Bol02, HPC02, OST05, SKI01, Mis06].

Versions
[HSR+01, NPV01, Ano00f, CV05].

Versteckte
[Sch09].

Versus
[Mad00a, Rub00, WWL+02, ASW+01, BJLS02, DBS01, WPP05].

Vertically
[DN04].

Very
[AAC+01, B+02, CG03, EBC+00, FLA+03, Høi01, PM02, PBMB01, Zir07].

Vestiges
[Top02].

VI
[Sch04a].

via [AGKS07, Ano00k, ACDm05, BDPV09, Car02, Che03, CPG+04, Elb08, FBWC02, Fox00, HHYW07, HLM03, JIO00a, KTO06, ML05, PG05, RG05, SB01, SLG+05, ZLG01, Lud05].

Victoria
[ACm08, IZ00].

Victorian
[Top02].

victory
[Hau03].

Vid [CAC06].

Video
[BDF+01a, BD03, CDTT05, EFY+05, ISS08, KBD03, KJR05, KLL01, LHS05, ML05, SC02a, BS01b, CO09a, JA02, KNO3, UP05].

Video-Based
[KJR05, BS01b, KN03].

videos
[ZDW07].

Vienna
[BZ02].

Vietnam
[Lov01].

View
[Bar00a, Mah04, Sin09, Woo05].

Views
[Bar00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03].

Vigenère
[DG00].

VII
[Sch04b].

VIII
[IEE01b, Sch05a].

Virtual
[Ano01c, HM01a, Pro00, YSS+01, BDS+09a, ML05, ZBP05].

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

virtualization-based
[CGL+08a, CGL+08b, CGL+08c].

Virtues
[Tr08].

Virus
[Ge06, Ano05c].

Visible
[HT06].

Visual
[BDN00, BDDS03, BCD06, CCL09, CTY09, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, ZF05, ABDS01, CDFM05, CDD07, DD04, HKS00, LAV09, PY08, Yan02, YC07, Bon00, Zo01].

Visualization
[XYL09, MFS+09].

vital
[Wal04, You04].

Viterbi
[LBGZ01, LBGZ02].

Vladimirov
[Puz04].

VLDB
[EBC+00, FLA+03].

VLDP
[B+02].

VLSI
[KV01].

VMSS
[SC05a].

Voice
[An00l, PK01, VN04].

VoIP
[An00c, ZS08, VAVY09, WJC05].

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, HJW05].

Voyrich
[Rug04].

VPN
[KM+06].

VPNs
[Dav01a].

VQ
[WJP07].

VQ-based
[WJP07].

Vs
[CTBA+01, DI01, DI03, SU07, WW04].

VSS
[AF04b, CDF01, FM02a].

Vu
[DP00].

vulnerabilities
[CSW05, DMS07, Swi05, XNK+05].

vulnerability
[KHL09, SGA07, YRS+09].

WA
[ACM06].

WACs
[Kov01].

Wagner
[dVP06].

Wagstaff
[Kat05b].

Wahhab
[MAaT07].

Walking
[Fox00].

Wall
[McE04].

Wallet
[ETZ00, JL04].

Walsh
[MS02b].

Walsingham
[Bud06].

WAN
[H601].

WAN-Cluster
[H601].

Wang
[SZS05].

Wants
[Hau00].

WAP
[JRF01].

War
[Bec02, Bud00a, Bud02, Han03, Kov01, MH09, MC04, OC03, AJ08, DB04, Ris06, Lvo01].

Warfare
[HW01, WW04].

warrior
[PC04].

Wars
[R03b, Cal00d, Cal00e].
Warsaw [AUW01, Bih03], washer [Ano01l].
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, 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, BSNO00, CC02a, CH01b, CDT05, CT09, CT02, CM02, CMB+08, DWN01, DNP07, EFY+05, EIG01, GW01, HT06, HH09, JKK+01, KCR04, hKLS00, KLL01, Kun01, KT00, LZ09, LLS05a, LKLK05, LZ01, LZP+04, LWS05, LPZ06, LJo05b, LSC03, LL01, LSKC05, MM01a, MNS01, Nak01, OMTO, PJK01, PR01, PBM+07, Qu01, Sam09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SPK08, VVS01, VHP01, VK07, WC09, WH09, WNY09, WWL+02, WL05b, XF01, YWW09, ZTP05, ZWC02, AIK03a, AAP07, BCKK05, CC02b, Che08b, CYH+07, CCD+04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, HLC07, HH05, JDJ01, JA02, KA09, KP00, LDD07, Lin00a, Lin01b, LLC06a, LLC06b, MB08, MCHN05].
watermarking
[PK03, Ren09, mSFl05, WP07, WNQ08, Way02b, Way09, WC05, WMDR08, XMST07, YZDW07, YPSZ01, ZLZS07].
Watermarks
[Ben00, BB00a, MLC01, Sug01, WC03a, WC04, YLL02, MB08, TND+09].
Watershed
[FBW01]. Watershed-from-Markers [FBW01].
WAV [XFZ01]. WAV-Table [XFZ01].
Wavelet [BR09, GW01, LKLK05, LZ01, Nak01, VD97, AAP07, AA08].
wavelet-based [AAP07, AA08].
Wavelet-Domain [LZ01]. WAVES
[LBA00]. Way [BYJK08, BM01a, CHL02, DIS02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTV05, Shi00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJo4, Cla00b, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LKLJ01, Mcl02a, Poi00, Tsa08, YW05, YRY05b, ZW05a].
Wayness [KI01a, PV06b]. Ways [BB02].
WCC [Ytr06]. WDDL [MMMT09]. Weak
[HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00]. Weakening [ZD05].
Weakly [BS00a, CHS05]. Weaknesses
[SW05a, SZS05, YPKL08]. Weakness
[FMS01, He02, KCL03, KCC05, SGGB00].
Weapons [RR03b]. Weather [WVL+02].
Web [Che01d, Mar05a, BFG05, BFG08, HIl06, Ano01c, Ano02e, Ano03d, AEV+07, BFG04, BC04b, CCCY01, Ccoc01a, Ccoc02a, Ccoc02b, CCB+01, DeL07, DMSW09, FSSF01, GSS02a, GSV02, HM05, JRB+06, KCD07, LWK00, LS05b, LMX+05, MPPM09, PM00, RRR4, Sam09, SSS06, Sch01a, SBG07, TMM05, WA06, YSS+01].
Web-Based [Ano01c, Sch01a, YSS+01].
Web-enabled [CCCY01]. webcam
[McN03]. WebFountain [Ano03d].
Webrelay [Zha00]. Weight
[CH07c, GK02, WT02]. Weighted
[BTW05, BTW08, SC02c, YZ00]. Weil
[BFO1b, BFO3, Jou02, Kir03]. Well
[WWGP00]. Welschenbach [Ter08]. Welsh
[Rot07]. went [AJ08]. WEP [SIR04]. were
[Han06]. Wesley [Puc03]. West
[Fra01, Jue04, Syv02, Wri03]. Westbridge
[Ano02e]. Western [CZB+01]. Wet [CC09].
Weyl [Sug03]. WG [DFPS06]. WG11.1
[ELvS01]. WG11.1/WG11.2 [ELvS01].
WG11.2 [ELvS01]. WG8.8 [DFCW00].
Wheeler [ABM08, Bar05]. Where
REFERENCES

[Ste05b]. XCBC [GD02]. XECB [GD02]. Xia [CJT04, Sha05a]. Xiamen [DWML05]. Xiao [JW01, YY05a]. Xilinx [Ano02c]. XIV [USE00c]. Xix [Top02]. XL [CP03]. XML

[Hai01, 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, LV00, LNS02, Ver01].

Yahalom [Pau01]. Yang [McK04, CZ03, KJY05, WL05, YWC05].

[Yang-Shieh] [YWC05]. Yao [BPS08, BDNN02, ZD05]. Yarrow [BO00].

[AA04a] Al-Akaidi:2004:FSP


You:2004:BSP

Agreste:2008:NAP


Apers:2001:PTS


Al-Azzoni:2005:MVC


Anshel:2001:NKA


Almgren:2000:HWC


Ababneh:2009:CSE

ASHRAF:2009:SBE


AAMODT:2003:CSP


AGRESTE:2007:IAW


AN:2001:DER


ATALLAH:2009:ATC

Abadi:2000:TA


Aiello:2004:JFK


Abdalla:2005:SER


Abdalla:2001:DAS


Ateniese:2001:ECV


Abe:2001:SEP

Masayuki Abe. Securing “Encryption + Proof

Adao:2009:SCF


Anderson:2000:CS


Austin:2000:ASF


Abe:2004:CEP


Abadi:2005:CFI


Abadi:2000:CFI


ABEL05

REFERENCES


Ambainis:2009:NEQ

REFERENCES


ACM:2003:PTF


ACM:2003:PTS


ACM:2004:PAS


ACM:2004:PAA


ACM:2005:SPA


ACM:2005:PTF


ACM:2005:MP1

ACM, editor. STOC ’05: proceedings of the 37th Annual ACM Symposium on
Algesheimer:2002:ECM

REFERENCES

Alvarez:2005:EBS

Ahmad:2007:ADE

Anyanwu:2009:DCS

Avanzi:2006:ESM

Adee:2009:CDT
Arnold:2007:CSE


Adikari:2009:HBT


Adleman:2003:TLP


An:2002:SJS


Arazi:2005:RPK


Alvarez:2005:SSS

Ahmed:2017:IRD


Atighehchi:2009:EPA


Anton:2007:HEW


Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF

Atallah:2005:DEK


Ateniese:2006:IPR


Attrapadung:2006:FSS


Akkar:2001:IAS


Acquisti:2009:PSS


Akavia:2006:BOW

References

citation.cfm?id=1132516
See erratum [AGGM10].

Akavia:2010:EBO

Alon:2007:GSE

Anagnostopoulos:2001:PAD

Ateniese:2005:PRS

Agrawal:2003:SWR

Agrawal:2003:WRD

Armington:2002:BAI
Ahmad:2007:CSS


Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB


Applebaum:2004:CNS

[AIK04] B. Applebaum, Y. Ishai, and E. Kushilevitz. Cryptography in NC0. In
REFERENCES


Applebaum:2006:C


Al-Ibrahim:2001:AMS


Attali:2001:JSC


Attali:2001:SCP

REFERENCES


REFERENCES

Armknecht:2003:AAC

Akinwande:2009:AHC

Amir:2004:PGK

Agrawal:2002:PP

Acicimez:2006:PSB

Agrawal:2004:OPE
Amadio:2000:RPC


Aoki:2000:FIA


Atallah:2004:ALA


Atzeni:2006:PKI


Anshel:2007:RME

REFERENCES


REFERENCES


REFERENCES


Anonymous: 2000: GBE

Anonymous: 2000: PESa

Anonymous: 2000: PTD

Anonymous: 2000: SES

Anonymous: 2000: AAPb
Anonymous: 2001: ANT


Anonymous: 2001: AWB


Anonymous: 2001: CCA


Anonymous: 2001: RAC

REFERENCES


Anonymous:2001:PKC


Anonymous:2001:SCS


Anonymous:2001:TAD


Anonymous:2001:DEC


Anonymous:2002:IHB


Anonymous:2002:NSD


Anonymous:2002:PPD

Anonymous. Products: Palm Digital Media’s eBook publishing tools; Veridicom’s fingerprint authentication module; high-speed debugging tool for Macraigor Systems; QNX

**Anonymous:2002:PSS**


**Anonymous:2002:PFQ**


**Anonymous:2002:QCQ**


**Anonymous:2002:QCR**


**Anonymous:2002:RUB**

Anonymous. Review of US bombes. *IEEE An-
REFERENCES

Anonymous:2003:TMC

Anonymous:2003:YCS

Anonymous:2003:NAW

Anonymous:2003:SEY

Anonymous:2003:TMP
Mersenne primes are primes of the form $M(n) = 2^p - 1$. The known members of this set in order of increasing $p$ (not of discovery), year of discovery, and discoverer, are:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>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>1750</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1750</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1752</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1752</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1752</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1957</td>
<td>H. Riesel</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson &amp; D. Slowinski</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>1988</td>
<td>W. N. Colquitt &amp; G. L. Caldwell</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; G. L. Caldwell</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski &amp; G. L. Caldwell</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski &amp; G. L. Caldwell</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, Woltermann &amp; puff</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; G. L. Caldwell</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; G. L. Caldwell</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elkenburg</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, Gene Newsom</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, G. L. Caldwell</td>
</tr>
<tr>
<td>49</td>
<td>74207281</td>
<td>2016</td>
<td>Curtis Cooper &amp; G. L. Caldwell</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. Woltman</td>
</tr>
</tbody>
</table>
Anonymous:2003:UCD
[Ano03g]

Anonymous:2004:BB
[Ano04a]

Anonymous:2004:CPS
[Ano04b]

Anonymous:2004:CJL
[Ano04c]

Anonymous:2004:Cf
[Ano04d]

Anonymous:2004:ISL
[Ano04e]

Anonymous:2004:NGJ
[Ano04f]

Anonymous:2005:CEC
[Ano05a]
Anonymous:2005:SCB

Anonymous:2005:WAS

Anonymous:2006:JHD

Anonymous:2006:RC

Anonymous:2006:SSD

Anonymous:2006:SQE

Anonymous:2007:CPSh

Anonymous:2007:CPSf
Anonymous:2008:KAD


Anonymous:2008:RCB


Anonymous:2008:RES


Anonymous:2008:SHS


Anonymous:2009:BG


Anonymous:2009:DSS


Anonymous:2009:PCA

REFERENCES

Anonymous:2009:TCA


Anonymous:2012:SHS


Anonymous:2013:DSS


Ateniese:2001:SRC


Amir:2001:FAA

ANSI:2005:AXP


Abe:2000:PSP


Abe:2002:SVK


Alomair:2009:ITS


Appenzeller:2005:IBE


Applebaum:2007:CCP

the ACM 2007 Doctoral Dissertation Award.


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


REFERENCES


REFERENCES


Avanzi:2003:CAD


Abadi:2005:SAC

Abadi:2008:SAC

Ayoade:2006:SIR

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


Blanton:2006:SRF


Bagnulo:2002:PAA


Badra:2007:AWC


Baier:2001:ECP


Baier:2001:ECS

Baignères:2008:QSB


Bao:2004:CPK


Baran:2000:NVB

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

Baran:2000:NVM

Nicholas Baran. News and views: More on tiny transistors; Open Source repository launched; design contest promotes new software tools; and then there’s a decryption contest; Fred

Banks:2005:TFC

William D. Banks. Towards faster cryptosystems, II. In Garrett and Lie-

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

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

**Bauer:2003:PPAb**


**Baudet:2005:DSP**


**Bauer:2007:DSM**


**Bau03b**

**Bau05**

**Bau07**

**Bau08**

**Blakley:1979:RSA**


**Benedens:2000:TBD**

Oliver Benedens and ChristopBuchmann:2000:ECC


**Buchmann:2000:ECC**

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

**Barkan:2002:HMW**


**Bicakci:2005:ISA**


**Biham:2002:SQK**

Basso:2009:NBB

Behrmann:2002:UIS

Bernstein:2009:PQC

Beimel:2000:CFS

Bellare:2001:KPP
REFERENCES


[BBK03a] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. In Boneh [Bon03], pages 600–616.


REFERENCES

UK£47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390292.htm;

Bellare:2000:PKE


Bellare:2009:HPK


Bobineau:2000:PSD


Boneh:2004:SGS


Burgess:2001:ISC

Biham:2004:NCS


Blundo:2004:SIA


Backes:2005:PKS


Bergadano:2005:DPL


Blundo:2005:SCN

Brzeziński:2005:MRL


Bergadano:2001:CSA


Bergadano:2002:IAM


Brier:2001:CRS

REFERENCES

Blundo:2006:VCS

Bruguera:2009:PIS

Burnett:2000:EMG

Barnum:2002:AQM

Bahi:2011:ECS
Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom num-
bers on GPU. arxiv.org, ?? (??),??, December 22, 2011.
URL http://arxiv.org/
abs/1112.5239.

Brown:2000:PCW


Breunesse:2005:FMS


Boneh:2007:CCS


Butler:2006:FAK


Barni:2005:DWI


Bao:2005:PSS

REFERENCES


REFERENCES


REFERENCES

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


Bourbakis:2003:SBC


Bozzano:2004:AVS


Burmester:2004:HPK


Buchmann:2008:PQC


Biryukov:2003:CS

REFERENCES


[179x634] BDD03


[179x610] Boneh:2001:LBM


[179x598] Bao:2001:SPD


[179x515] Bolosky:2000:FSD

REFERENCES


REFERENCES


Feng Bao, Robert Deng, and Jianying Zhou, editors. Public Key Cryptography—PKC 2004: 7th International Workshop on Practice and Theory in Public Key Cryptography, Singapore, March 1–4, 2004:
Beckman:2002:CAB


Beebe:2005:CBPd


Bejtlich:2006:EDS


Bellare:2000:ACC


Bella:2001:MPS

REFERENCES


REFERENCES

Benson:2001:VS

Benantar:2002:IPK

Benson:2004:VS

Berson:2000:CE

Berson:2003:CAB

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

[Bernstein:2008:CVS]

[Bergmann:2009:DKR]

[Bernstein:2009:IPQ]

[Bouwmeester:2000:PQI]

[Bouwmeester:2001:PQI]

[Biham:2000:IDR]
REFERENCES


REFERENCES


Bisseling:2006:MSM


Boldyreva:2006:SO


Bhargavan:2008:VPB


Bhargavan:2004:SWS


Bhargavan:2005:SWS


Bhargavan:2008:CVI

REFERENCES

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

Bhargavan:2008:VII


Bugliesi:2007:DTA


Biham:2002:DCQ


Brown:2007:SAN


Bugliesi:2007:SIT


Blaszczyk:2008:NMT

REFERENCES

[Blaszczyk:2009:EVT]
&arnumber=4753211.

[Barthe:2009:FCC]

[Bennett:2002:ESE]

[Barak:2001:IPO]
REFERENCES


[BG02] Boneh:2005:EDF


[BGN05] Boldyreva:2008:NMS


[BGOY08] Bergadano:2002:UAT


[BGP02] Bergbain:2009:QMS


[BGP09] Blackburn:2005:PNP


**Boneh:2005:CRB**


**Beck:2000:FSD**


**Bialaski:2000:SLN**


**Barak:2005:MAP**


**Badra:2006:KEA**

Backhouse:2003:TOT


Bajard:2004:FRI


Barkol:2005:SCC


Beimel:2005:PNS


Bi:2009:MCE


Bidgoli:2003:EIS


Biggs:2008:CII

Norman Biggs. *Codes: An introduction to Information Communication and
REFERENCES


REFERENCES

0558/papers/1880/18800055.pdf.

Bajard:2003:EMG


Bajard:2005:AOP


Biryukov:2007:FSE


Bishop:2003:ICJ


Bishop:2003:CSA


Barkol:2008:CPR


Boyce:2002:IAM

REFERENCES


REFERENCES


Boni:2000:NGT


Burnside:2005:CCP


Barker:2006:RRN


Breveglieri:2006:GEI


Barker:2007:RRN


Barreto:2002:EAP

Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In
REFERENCES


Breveglieri:2007:OCA


Bellare:2004:BPR


Bajard:2009:SRB


Bellare:2000:SCB


Blum:2003:NTL


Buonanno:2002:IUE

Enrico Buonanno, Jonathan Katz, and Moti Yung. Incremental unforgeable en-


REFERENCES


Ble07  Gerrit Bleumer. Electronic postage systems: technol-

[Bao:2006:CIB]


[BLM01]

[Brassard:2000:SAP]

[Bozga:2006:PBA]
Buchmann:2009:PQC


Banks:2001:CAS


Blomer:2001:LSE


Blunden:2009:RAE


Batina:2001:AWD


Blincat:2001:KRA

[BM01c] Karl Brincat and Chris J. Mitchell. Key recovery


[BM00a] Jerome Burke, John McDonald, and Todd Austin. Architectural support for fast symmetric-key cryptography. Operating Systems
Burke:2000:ASFc

Boneh:2000:GRK

Boyko:2000:PSP
REFERENCES


Bellare:2000:AER

Buchmann:2006:PCL


Boyen:2005:DCC

Borselius:2002:PAU


Borselius:2002:VTS


Buchmann:2006:PCL

Boneh:2000:TC


Bellare:2002:TSB


Bellare:2002:PRI


Bouganim:2003:CSD

[BNPW03] Luc Bouganim, François Dang Ngoc, Philippe Pucheral, and Lilan Wu. Chip-secured data access: Reconciling access rights with...
REFERENCES


REFERENCES


Barak:2007:DC


Boy01


Boyen:2003:MIB


Bedi:2001:CNF


Burnett:2001:RSO

REFERENCES


[BP05] Bruno Blanchet and Andreas Podelski. Verification of cryptographic protocols: tagging enforces ter-
REFERENCES

Beissinger:2006:CUM

Baer:2007:CIS

Bellare:2000:AKE

Borst:2001:CSC

Bellare:2005:ISA

Boneh:2008:IBI
D. Boneh, P. Papakonstanti-

Baudron:2000:ENS


Backes:2008:KDM


Benerecetti:2002:VST


Brandao:2001:UEC

M. Bellare and P. Rogaway. Code-based game-playing proofs and the se-
REFERENCES


Barrett:2001:SSS


Bigun:2001:AVB


Biryukov:2001:SCS


Boneh:2001:UBE

REFERENCES


REFERENCES


REFERENCES


Black:2002:SCA


Buchmann:2000:CTC


Buchmann:2000:IC


Buchmann:2001:IC


Buchmann:2004:IC


Budiansky:2000:BWC


Budiansky:2000:DBU

[Bud00b] Stephen Budiansky. The difficult beginnings of US–British codebreaking cooperation. Intelligence and...
REFERENCES


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


REFERENCES


Burr:2003:SAE


Burr:2006:CHS


Boesgaard:2004:RNH


Baker:2007:ISU


Blake-Wilson:2002:RUE


Butler:2000:NSA

REFERENCES

Bellare:2003:FSP


Bar-Yossef:2004:ESQ


Bar-Yossef:2008:ESQ


Bertlmann:2002:QUB


Bond:2003:DTA


Borders:2005:CHP


Carrington:2002:EDS

[C+02] Charles Carrington et al., editors. Enterprise directory and security implementation guide: designing and

[Staf03] NTC

CACM Staff. News track: Cinematic watermark; eye-opening education; roaming time; stand by me; savings bonds fade to net; phone home. Communications of the Association for Computing Machinery, 46(7):9–10, July 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). [Cal00c]

[Staf06] NTS

CACM Staff. News track: Super game plan: E-learning roots disputed; Chinese history; U.K. seeks popular science input; encryption commitment; Improve-ment news; vid kid. Communications of the Association for Computing Machinery, 49(11):9–10, November 2006. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). [Cal00d]

[Cal00a]


[Cal00b]


[CAMTC:2000:TSC]


[Caloyannides:2000:EWE]


[Caloyannides:2000:EWS]

REFERENCES


REFERENCES

Carter:2001:SCT


Carlet:2002:LCC


Casey:2002:HCC


Cass:2003:LES


Casselman:2006:MTE


Cobas:2001:CTA

REFERENCES

Cachin:2000:OFS

Challal:2005:HHC

Cooper:2005:AAP

Chandramouli:2006:BPA

Chan:2001:CRP

Chan:2001:CTB

Carline:2002:NWT
Dylan Carline and Paul

[CC00]

[CC01a]

[CC01b]

[CC02a]
REFERENCES


Chao-Wen Chan and Chin-Chen Chang. A scheme for...


**Chan:2001:WEF**


**Collberg:2004:DPB**


**Cimato:2006:UMU**


**Chai:2007:EIB**


**Cattaneo:2001:DIT**


**Chen:2004:TPM**

Tzer-Shyong Chen, Yu-Fang Chung, and Kuo-

Chang:2005:DSM


Chang:2004:IDA


Chang:2004:SOT


Chang:2009:PCC


Christianson:2001:PKC


Choi:2005:JMA

Hyung-Kyu Choi, Yoo C. Chang, and Soo-Mook Moon. Java memory allocation with lazy worst fit for small objects. *The Com-


Cramer:2005:CMS

Cramer:2005:SCP

Cavallar:2000:FBR

Cortier:2006:SAP
Ronald Cramer, Ivan Damgård, and Ueli Maurer. General

Chawla:2005:TPP


Coron:2005:MDR


Cramer:2001:MCT


Chapman:2001:PEA

Mark Chapman, George I. Davida, and Marc Rennhard. A practical and effective approach to large-scale automated linguistic steganography. Lecture Notes in Computer Science, 2200: 156–??, 2001. CODEN
REFERENCES


Castiglione:2007:TAD

Chen:2005:NVW

Ceravolo:2004:ERH

Certicom:2004:CCC

Canetti:2001:UCC

Canteault:2001:COR
REFERENCES

Cramer:2002:OBB

Clarke:2005:AUM

Clarke:2007:AUA

Cohen:2006:HEH

Clarke:2002:ASA
REFERENCES

Courtois:2001:HAM

Cramer:2005:BBS

Climent:2006:NEC

Chang:2010:PRN

Chodowiec:2003:VCF
REFERENCES

Cranor:2005:SUD


Candebat:2006:SPM


Chodowiec:2001:ETG


Caballero-Gil:2009:GBA


Catalano:2000:CIS

REFERENCES

[Coppersmith:2000:ICT]

[Catalano:2001:BSP]

[Caballero-Gil:2006:SSB]

[Crosby:2002:CHB]
REFERENCES


REFERENCES


Canovas:2002:DSB


Cox:2002:SP9


Cimato:2003:SCN


Cayrel:2008:SIS

REFERENCES

Chow:2009:ADN

Crotch-Harvey:2000:OPR

Chang:2001:TFG

Chien:2007:SUL

Chung:2007:ASF

Chung:2007:MRA
[CH07c] Jaewook Chung and M. Anwar Hasan. Montgomery reduction algorithm for modular multiplication using low-

Chen:2001:SFW

Chaum:2004:VSB


Chaun:2005:MCM


Chandra:2005:BWS


Chakrabarti:2007:GCS


Chang:2001:NEA


Chen:2004:MCK

[CHC04] Tzer-Shyong Chen, Kuo-Hsuan Huang, and Yu-Fang Chung. Modified cryptographic key assignment scheme for overcoming the incorrectness of the CHW scheme. Applied Mathematics and Computation, 159


[Che01d] S. M. Cherry. Hyperencryp-
tion: Much hype about little
that is new [web sites]. *IEEE
Spectrum*, 38(4):87, April
2001. CODEN IEESAM.
ISSN 0018-9235 (print),
1939-9340 (electronic).

[Che01e] S. M. Cherry. Is hyperlink-
ing to decryption software
illegal? *IEEE Spectrum*,
CODEN IEESAM. ISSN
0018-9235 (print), 1939-
9340 (electronic).

[Che01f] S. M. Cherry. Remailer
elude e-mail surveillance.
*IEEE Spectrum*, 38(11):69,
November 2001. CODEN
IEESAM. ISSN 0018-9235
(print), 1939-9340 (electronic).

[Che02] Yangjun Chen. Signature
files and signature trees.
*Information Processing Let-
ters*, 82(4):213–221, May
31, 2002. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

[Che03] Qi Cheng. Primality
proving via one round in
ECPP and one iteration in
AKS. In Boneh [Bon03],
pages 338–348. CODEN
LCNSD9. ISBN 3-540-
40674-3. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
tocs/t2729.htm; http://
issn=0302-9743&volume=2729;

[Che04a] Bi-Hui Chen. Improvement
of authenticated multiple-
key agreement protocol.
*Operating Systems Review*, 38
(3):35–41, July 2004. CO-
DEN OSRED8. ISSN 0163-
5980 (print), 1943-586X
(electronic).

[Che04b] Qi Cheng. On the bounded
sum-of-digits discrete log-
arithm problem in finite
fields. In Franklin [Fra04],
pages 201–225. CODEN
LNCSD9. ISBN 3-540-
22668-0. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN 10.1007/b99099
issue&issn=0302-9743&volume=
3152; http://www.springerlink.com/openurl.asp?genre=
volume&id=doi:10.1007/b99099.
Chen:2005:TSS


Cherry:2005:MDC


Chess:2005:SAC


Chen:2007:MEV


Chen:2008:CIS


Chen:2008:MWS


Coulter:2001:GAH

[CHH01] Robert S. Coulter, George Havas, and Marie Henderson. Giesbrecht’s al-

Choi:2009:KDK

Chien:2008:EPA

Chien:2008:PAUa

Chien:2008:PAUb

Chien:2008:PAUb

Chien:2008:SCA
REFERENCES

Coron:2001:GMC


Coron:2001:OCC


Coppersmith:2002:CSC


Canetti:2003:FSP

Canetti:2005:ASN


Cheon:2008:PST


Chao:2009:HCS


Chen:2002:CPK


Choi:2006:CHP

Su-Jeong Choi. Cryp-
REFERENCES


CHS05 Ran Canetti, Shai Halevi, and Michael Steiner. Hardness amplification of weakly
REFERENCES


Chen:2002:AMT


Cornea:2002:SCI


Churchhouse:2002:CCJ


Canvel:2003:PIS


Chang:2005:ILW

Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang


REFERENCES

issn=1570-7873&volume=2&issue=4&spage=301.

[Choie:2005:EIB]


[Chin:2006:HSI]


[Clarke:2000:VSP]


[Coron:2000:NAP]


[Coron:2002:UPS]


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


Canetti:2002:UCN


Cook:2006:CEG


Cheon:2002:IID


Chung:2003:EPX


Chun:2003:DLC

Kilsoo Chun, Seungjoo Kim, Sangjin Lee, Soo Hak Sung, and Seonhee Yoon. Differential and linear cryptanaly-

\textbf{Cox:2005:DWT} \hfill \textbf{[CKL05]}


\textbf{Chen:2009:SRP} \hfill \textbf{[CKL+09]}


\textbf{Coppersmith:2000:KRF} \hfill \textbf{[CKM00]}


\textbf{Coron:2000:FLA} \hfill \textbf{[CKN00]}

Coron:2001:SSL


Canetti:2003:RCC


Cheon:2006:KPC


Cachin:2001:SEA


Cathalo:2003:NTT


**Chang:2001:CIU**


**Camenisch:2002:DAA**


**Cao:2002:TKE**


**Crowley:2002:BLS**


**Camenisch:2004:SSA**

Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Franklin [Fra04], pages 56–?? CODEN LNCS90. ISBN 3-540-22668-0. ISSN 0302-9743.
Chang:2004:CGS


Chang:2004:IDM


Chang:2004:RFB


Chang:2004:AWM


Chien:2009:EBL

Hung-Yu Chien and Chi-


Julie Clark. Looking for new contactless points: Hong Kong’s Octopus smart card could get a lot smarter, but it will have to pick its way carefully through regulations and competition from other quarters first. *ITS international*, 6(2):77–78, March/April 2000.


REFERENCES

Cho:2004:GKR

Cheon:2000:NBC

Canetti:2002:UCT

Cormen:2001:IA

Chen:2009:AKD

Chang:2007:SIH

Clulow:2003:SP
| [Clu03] Jolyon Clulow. On the security of PKCS #11. In Wal-
REFERENCES


[CLZ02]


[CM00]


[CM05a]

Benoit Chevallier-Mames. An efficient CDH-based


[CMB+05] Diane Crawford, Marius Matioc, Steven M. Bellovin, Richard Hubert, Andrew D. Wolfe, Jr., David Foulser, and Andrew R. Kilner. Forum: To block spam, demand sender authentication; not revolutionary (thank goodness); how to know the known from the unknowns; user first in user-centered design. Communications of the Association for Computing Machinery, 48(3):11–13, March 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


[CMdV06] C. J. F. Cremers, S. Mauw,


Cho:2008:DNP


Caputo:2009:DIT


Crawford:2002:FEE


Coron:2004:SSL


Ciet:2003:PFI


Catalano:2002:HHL

Correia:2006:CAB


Cetin:2009:NSA


Czernik:2009:CRN


Cobb:2004:CD


Cochran:2001:NVS

Shannon Cochran. News and views: Scientists seek immersive reality; USENIX names lifetime achievement recipients [the GNU Project and the Kerberos network authentication system]; robots need program-

**Cocks:2001:IBE**


**Cochran:2002:NVSb**


**Cochran:2002:NVW**


**Cochran:2003:NVC**


**Cohen:2003:FOV**

Ernie Cohen. First-order

**Cole:2003:HPS**


**Constantinou:2000:CSC**


**Convery:2004:NSA**


**Conti:2009:GSH**


**Cook:2002:REJ**


**Coppersmith:2000:C**


**Copeland:2004:COO**

puting, 26(4):38–45, October/December 2004. CO-
DEN IAHEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL http://
csdl.computer.org/dl/mags/an/2004/04/a4038.
htm; http://csdl.computer.org/dl/mags/an/2004/04/
a4038.pdf.

Copeland:2004:ETS

B. Jack Copeland, editor. The Essential Turing: Sem-
inal Writings in Computing, Logic, Philosophy, Ar-
tificial Intelligence, and Artificial Life, plus The Se-
crets of Enigma. Oxford University Press, Walton
825079-7 (hardcover), 0-19-825080-0 (paperback). viii + 613 pp. LCCN QA29.T8
E77 2004. URL ftp://
uiarchive.cso.uiuc.edu/

Copeland:2005:CSB

B. Jack Copeland, editor. Colossus: the secrets of
Bletchley Park’s codebreaking computers. Oxford University Press, Walton Street,
C66 2006.

[Cor00a]
Francisco Corella. A fast implementa-
tion of DES and Triple-DES on PA-
RISC 2.0. In USENIX [USE00b], page ?? ISBN

Coron:2000:ESF

Jean-Sébastien Coron. On the exact security of full
domain hash. In Bellare [Bel00], pages 229–??
REFERENCES


REFERENCES


Cimato:2006:PVC


Chow:2004:UDL


Chen:2004:SEP


Catalano:2004:IPP


Canetti:2007:CSH

REFERENCES


REFERENCES


[CS03a] Jan Camenisch and Victor Shoup. Practical ver-


REFERENCES

Cvejic:2005:IRL

Capaldi:2007:ADI

Chakrabarti:2007:PBA

Chatterjee:2007:CSC

Casey:2008:IFD

Chang:2008:DAP
Cusick:2009:CBF


Czeskis:2008:DED


Cai:2007:CSM


Crandall:2005:DUV


Chen:2008:CCS


Chung:2009:ISA

REFERENCES


URL http://www.springerlink.com/content/978-3-642-00305-2.

Collberg:2002:WTP


Coron:2003:NAS


Chen:2008:BUK


Chu:2008:EOT


Chou:2009:ATI

Crawford:2001:FPV


Cheung:2001:TPS


Chiang:2008:CPB


Chang:2004:ASS


Collberg:2007:DGB


Chen:2009:FCV

REFERENCES


[CU01] [CV02] [CV03] [CUS08]
REFERENCES


[CW07] Brian Chess and Jacob West. Secure program-
Cheng:2009:NAS


Chang:2000:ELD


Chien:2005:NRS

REFERENCES

Choie:2002:ICH


Chen:2005:ENB


Chang:2008:EBD


Chang:2001:NSS


Chang:2004:TSSb


Chang:2005:SAK

Ting-Yi Chang, Wei-Pang Yang, and Min-Shiang Hwang. Simple authenticated key agreement and protected password change protocol. *Computers and
REFERENCES

Chung:2007:SBW


Chang:2005:CIA


Chen:2003:AEY


See erratum [McK04].

Chadwick:2005:PKI


Crawford:2001:FHC

Diane Crawford, Mick Zraly, Hal Berghel, Ken Pugh, Mat H. West, Conrad Weisert, Terry Steyaert, and Richard Johnson. Forum: How can the Web advance Western democracies? who needs digital signatures; misinformation and the Emulex hoax; OOSCD not really so unified; go back to non-

Crawford:2001:OOSD

See [Sch00c].

Cheng:2005:RIC


CZK05

Dodis:2003:CAA


DA03

Dale:2001:BSA

Richard Dale. Biometric security: It’s all about identification and authentication.

Dal01

See [Dan01].


Dodis:2003:CAA


Damgaard:2000:ECZ

Damaj:2007:PAD


Danielyan:2001:AAE

Edgar Danielyan. AES: Advanced Encryption Standard is coming. *USENIX Association newsletter*, 26(1):??,
REFERENCES


Danas:2002:CUS

George Danas. On a cryp-
tosystem using simple con-
ISSN 1537-5978.

Das:2008:BQC

S. R. Das. Breaking quan-
tum cryptography’s 150-
kilometer limit [update]. IEEE Spectrum, 45(9):15, September 2008. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (elec-
tronic).

Davis:2001:ISV

Carlton R. Davis. IPSec: Securing VPNs. Mc-
212757-0. xix + 404 pp. LCCN TK5105.567 D38
200. US$49.99.

Davis:2001:DSA

Don Davis. Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML. In USENIX [USE01a], page ??.

Davis:2001:DSE

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

Davis:2007:AAA

Adrian Davis. Authentication

DeBrosse:2004:SBU

Jim DeBrosse and Colin B.
Burke. The secret in Building 26: the untold story of
America’s ultra war against
the U-boat Enigma codes.
Random House, New York,
NY, USA, 2004. ISBN 0-
375-50807-4, 1-58836-353-8,
0-375-75995-6. xxix + 272
pp. LCCN D810.C88 D43
loc.gov/catdir/samples/
random045/2003058494.html.
http://www.randomhouse.
com/catalog/display.pperl?
isbn=9781588363534.

deBorde:2007:STF

Duncan de Borde. Selecting a two-factor au-

[Desmedt:2001:ERD] Yvo Desmedt, Mike Burmester, and Jennifer Seberry. Equi-

[DBS01] Barry Doyle, Stuart Bell, Alan F. Smeaton, Kealan McCusker, and Noel E. O’Connor. Security consider-
ations and key negotiation techniques for power con-

REFERENCES


REFERENCES


Antonio Durante, Riccardo Focardi, and Roberto Gorrieri. A compiler for analyzing cryptographic protocols using noninterfer-
Durante:2001:CWR


DePalma:2004:CCS


Domingo-Ferrer:2001:CDS


Dodis:2003:IRP


DeSantis:2004:CKA

Alfredo De Santis, Anna Lisa


REFERENCES

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


[DG04] Yevgeniy Dodis, Rosario Gennaro, Johan Håstad,

Devanbu:2004:FAX


Devanbu:2003:ADP


Dwork:2003:MBF


Dorrendorf:2007:CRNa


Dorrendorf:2007:CRNb

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


REFERENCES

[**Dodis:2000:CSG**]

[**DiCrescenzo:2001:SOS**]

[**DiCrescenzo:2003:SOS**]

[**Damgaard:2005:CRM**]

[**Dichtl:2003:HPO**]
REFERENCES


REFERENCES

[Din05] Yan Zong Ding. Error correction in the bounded storage model. In Kilian [Kil05], pages 578–?? CODEN LNCSD9.


[DJ06] Stéphanie Delaune and Florent Jacquemard. Decision procedures for the security of protocols with probabilistic encryption against offline dictionary attacks. Jour-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

0558/papers/2332/23320065.pdf.


REFERENCES


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

Dowd:2007:ASS


Denev:2009:SFQ


Ding:2007:ESD


Damgaard:2000:INC


Durfee:2000:CRS

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Damgaard:2005:QCN

DPS05

Delbourg:2002:JBC

[DPVR00]

Daemen:2000:NPN

[DPV04]

Crescenzo:2004:CRR

[DPV01]


[Dr.00c] Dr. Dobb’s Journal. Dr. Dobb’s essential books on cryptography and security. CD-ROM containing PDF files., 2000. URL http://www.ddj.com/cdrom/;


Daemen:2002:FSE


[DR02c]

Ding:2002:HEE


[DR02d]

Dreyfus:2000:PUC

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

[Dray]
REFERENCES


REFERENCES


Ding:2002:NUO


Ding:2005:RNM


Dodi:2005:ESE


Ding:2006:SSS


Dawson:2005:PCM


Drutarovsky:2008:CSC


Levy-dit-Vehel:2006:WC


Du:2001:OKS


deWeger:2002:CRS


Ding:2005:CTC


Dodis:2009:NME

Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key


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


Dawu:2001:TES


Deng:2009:SCA


Ding:2009:MPK


Dai:2001:CDE


Eagleton:2005:BRD


ElAbbadi:2000:VPI

REFERENCES


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


[EHMS00] Carl Ellison, Chris Hall, Randy Milbert, and Bruce Schneier. Protecting secret...


Ekeraa:2009:DCM


El:2001:GPK


Ek:2004:QC

Chip Elliott. Quantum cryptography. *IEEE Se-
REFERENCES


Eisenbarth:2007:SLC Thomas Eisenbarth, Christof Paar, Axel Poschmann,


Hans Eberle, Sheueling...

Enck:2005:EOF


Evans:2009:BRS


Edman:2009:AES


Elbirt:2000:FIP

ISBN ???? LCCN ????

Faliszewski:2007:BRB

Fan:2003:ILC

Faugere:2009:IBC

Ford:2001:SEC

Felkel:2001:ICW

Feghali:2002:SAP
Wajdi Feghali, Brad Burres, Gilbert Wolrich, and Douglas Carrigan. Security: Adding protection to
REFERENCES


Fan:2005:RRA


Fischer:2001:TMR


Furnell:2000:ASS


Felke:2006:ATH


Ferguson:2000:SEK


Ferguson:2006:ACE

Fischlin:2000:ENM


Filiol:2001:NUS


Flannery:2001:CYW


Fridrich:2001:DLS


Frenkiel:2002:CCS


Focardi:2000:ITN

Riccardo Focardi, Roberto Gorrieri, and Fabio Martinelli. Invited talk: Non interference for the analysis of cryptographic protocols. Lecture Notes in
REFERENCES


Focardi:2000:MAT


Focardi:2003:CTA


Fitzi:2001:MCP


Field:2009:BCB


Filiol:2000:DAS

REFERENCES


REFERENCES

FIPS:2001:SRC


FIPS:2002:KHM


FIPS:2002:SHS


Freedman:2005:KSO


Fischlin:2001:CLP

Marc Fischlin. Cryptographic limitations on parallelizing membership and


REFERENCES

Fox:2001:PPK

Faure:2006:NPK

Freytag:2003:VPI

Fluhrer:2002:CMB

Fluhrer:2002:CSP
Feng:2006:ISC

Fan:2002:ETB

Fehr:2002:LVD

Fuller:2002:LRA

Franklin:2002:PAS

Fournier:2003:SEA
Jacques J. A. Fournier, Simon Moore, Huiyun

Fouque:2003:AUR


Furht:2005:MEW

REFERENCES

387-24425-5; 0-387-26090-0.  
[102x681]?? pp. LCCN QA76.575 F885 2005.

[FMY01] Yair Frankel, Philip D. MacKenzie, and Moti Yung. [FOBH05]


REFERENCES

link/service/series/0558/bibs/2139/21390260.htm;

Forbes:2004:BRN


Forte:2009:DM


FP00


FP01


Fox:2000:NTFb


Fouque:2001:TCS


Franklin:2004:ACC

Fremberg:2003:MAP

Friberg:2001:UCH

Frith:2007:SAO

Frykholm:2000:CAB

Ferguson:2000:CEI


REFERENCES


[FZH05] Yongzhi Fu, Xuejie Zhang, and Lin Hao. Design of
REFERENCES

high performance recon-
figurable Triple DES pro-
cessor. In Han et al. [HYZ05b], pages 110–??
ISBN 981-270-153-2. LCCN ?????
URL http:// [Gal02]
eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

**Gross-Amblard:2003:QPW**


**Gang:2005:CNI**


**Galbraith:2001:SCC**


**Galbraith:2001:CID**


**Gallo:2003:SST**


**Ganger:2001:AC**


**Gannon:2001:SST**

James Gannon. Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century. Brassey's,


REFERENCES

32(2):5–6, June 2001. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [Kah67a, Kah67b, Kah74, Kah96].

Gaudry:2002:CCS


Gavinsky:2008:CIC


Guajardo:2001:EIE


Golic:2002:LCB


REFERENCES


REFERENCES


Rosario Gennaro. An improved pseudo-random generator based on discrete log. In Bellare [Bel00],
REFERENCES


Gengler:2001:PPS


Gentry:2003:CBE


Gennaro:2004:MTC


Gentry:2004:HCR


Gennaro:2006:RC


[GG05a] Lawrence Goldstone and Nancy Bazelon Goldstone.


Goldwasser:2008:CAP

Gennaro:2003:LBE

Gennaro:2005:BEG

Grothoff:2009:TBS

Gilbert:2002:SCL

Gross:2004:MNh

Gilbert:2005:FSE

Galindo:2008:SPK

Ghafarian:2007:IPU

Gonzales:2000:LBC

Gilbert:2000:SAR

Gilbert:2001:SAR
REFERENCES


Gaudry:2006:ACM


[GHK+06]

[GIKR01]

[GIKR02]

[GHPT05]


Gong:2001:GPK


[GHW01]


Gennaro:2001:RCV


Gennaro:2002:RSM


REFERENCES

com/openurl.asp?genre=
issue&issn=0302-9743&volume=
2442.

Gillespie:2007:WSC

Tarleton Gillespie. Wired
shut: copyright and the
shape of digital culture.
MIT Press, Cambridge,
MA, USA, 2007. ISBN
0-262-07282-3. 420 (est.)
pp. LCCN K1447.15
www.loc.gov/catdir/toc/
ecip0620/2006030129.html

Giraud:2006:RIR

C. Giraud. An RSA imple-
mentation resistant to fault
attacks and to simple power
analysis. IEEE Transac-
tions on Computers, 55(9):
CODEN ITCOB4. ISSN
0018-9340 (print), 1557-
9956 (electronic). URL
org/stamp/stamp.jsp?tp=
&arnumber=1668039.

Gebhardt:2005:NPV

M. Gebhardt, G. Illies, and
W. Schindler. A note on
the practical value of sin-
gle hash function collisions
for special file formats. In
NIST Cryptographic Hash
Workshop 2005, page ??
???, ???, 2005. ISBN [GJKR03]
???, LCCN ???.
gov/pki/HashWorkshop/2005/
Oct31_Presentations/Illies.

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

Gordon:2003:ATS

Andrew D. Gordon and
Alan Jeffrey. Authenticity
by typing for security
protocols. Journal of
Computer Security, 11
CODEN JCSIET. ISSN
0926-227X (print), 1875-
8924 (electronic).

Gordon:2004:TEA

Andrew D. Gordon and
Alan Jeffrey. Types and ef-
facts for asymmetric cryp-
tographic protocols. Journal
of Computer Security,
CODEN JCSIET. ISSN
0926-227X (print), 1875-
8924 (electronic).

Ganapathy:2005:APA

Vinod Ganapathy, Trent
Jaeger, and Somesh Jha.
Automatic placement of au-
thorization hooks in the
Linux security modules
framework. In Meadows and
Syverson [MS05b], pages
330–339. ISBN 1-59593-
ACM order number 459050.

Gennaro:2003:SAP

Rosario Gennaro, Stanis-
law Jarecki, Hugo Kraw-
czyk, and Tal Rabin. Secure
applications of Pedersen’s
distributed key generation

**Gallagher:2006:HSB**


**Gentry:2001:CNS**


**Gomulkiewicz:2002:HWA**


**Goldsmith:2004:CAI**


**Goldwasser:2005:PPK**

Shafi Goldwasser and Dmitriy Kharchenko. Proof of plaintext knowledge for the Ajtai–Dwork cryptosystem. In Kilian [Kil05], pages 529–?? CODEN LNCSD9. ISBN 3-540-24573-1 (soft-
Gavinsky:2007:ESO


Gavinsky:2009:ESO


Garay:2007:RCA


Gertner:2000:RBP


Guneysu:2008:CC

REFERENCES


REFERENCES


REFERENCES

Galbraith:2003:IAU

Galbraith:2002:PKS

Gorrieri:2004:SFR

Golle:2008:DCS
Philippe Golle, Frank McSherry, and Ilya Mironov.
REFERENCES


**Galbraith:2001:CNR**


**Galbraith:2001:RBU**


**Gentry:2005:PAK**


**Galindo:2008:ICB**


**Gopalakrishnan:2001:PWV**


**Grosek:2001:SPK**

Otokar Grošek, Spyros S. Magliveras, and Wandi Wei. On the security of a public-key cryptosystem. In *Public-key cryptography and com-


Goldreich:2001:FCBb


Goldreich:2001:FCBa


Golic:2001:CAS


Golic:2001:HCC


Golic:2001:MOS


Golic:2001:CAS

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


REFERENCES

ISBN 1-60558-085-6. LCCN ????

Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT


Guneysu:2008:SPH


Guterman:2006:ALR


Granger:2005:HSN


Granger:2006:SCA


Gentry:2008:THL

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for


REFERENCES

4031329. IEEE Computer Society Order Number P2720. [GS02b]

**Geppert:2000:T**


**GonzalezVasco:2001:CPK**


**Garfinkel:2002:WSP**


**Gentry:2002:HIB**


**Gentry:2002:CRN**


**Geiselmann:2003:HSS**

Willi Geiselmann and Rainer Steinwandt. Hardware to solve sparse systems of linear equations over GF(2). In Walter et al. [WKP03], pages 51–61. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743
REFERENCES


REFERENCES


Gennaro:2000:LBE


Guttman:2002:ATS


Goodrich:2002:EDD


Guttman:2004:FAP

Joshua D. Guttman, F. Javier Thayer, and Lenore D. Zuck. The faithfulness...
REFERENCES


**Guar:2005:PPL**


**Guette:2009:ATK**


**Guizzo:2006:BIC**


**Gumz:2004:BRH**


**Guillou:2001:CAP**


**Gutmann:2000:OSC**


**Gutmann:2002:CFP**

REFERENCES

Gutmann:2002:DVC


Published in book form [Gut04a].

Gutmann:2004:CSA


Gutmann:2004:SPK


Gutmann:2004:ATD


Gutmann:20xx:ESR


Granger:2005:DLP

R. Granger and F. Vercauteren. On the discrete logarithm problem on algebraic tori. In Shoup [Sho05a], pages
REFERENCES


Goldberg:2008:PQM


Heys:2000:SAC


REFERENCES


Haddad:2000:AUA


Hancock:2000:EWP


Harvey:2000:EMA


Hare:2001:RUPa


Hare:2001:RUPb


Harrington:2005:NSP

REFERENCES

Harris:2005:GHE


Hars:2006:MIA


Harman:2007:PDS


Hasan:2000:LTB


Hasan:2001:ECM


Hasan:2001:PAA

[Has01b] M. A. Hasan. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz


Hassler:2002:JCP


Haufler:2003:CVH


Haufler:2006:SWN


Hayat:2004:CSE

Khawaja Amer Hayat, Umar Waqar Anis, and S. Tauseef ur Rehman. Cryptanalysis of some encryption/cipher schemes using related key attack. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 36(4):85–87, December 2004. CODEN SIGSD3. ISSN 0018-9340 (print), 1557-9956 (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


Hui-Feng Huang and Chin-Chen Chang. A novel cryptographic key assignment


[Han:2009:ICS]

[Hei03]

[Hei07]

[Hen01]
REFERENCES


[Hes04a] F. Hess. On the security of the verifiably-encrypted signature scheme of Boneh,


Nick Howgrave-Graham. Public-key cryptography and proofs of security. In Garrett and Lieman [GL05], pages 73–89. ISBN 0-821-
Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2003:HNP


Howgrave-Graham:2003:IDF

Hendricks:2007:LOB


Handschuh:2004:SAC


Handschuh:2005:SAC


Hung:2009:FBA

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

Hwang:2005:TSP


REFERENCES

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


Hamann:2001:SBA


Han:2007:FIE


Hernandez:2004:FED


Higgins:2008:NSC


Hill:2000:KII


Hilley:2005:CRM

Sarah Hilley. Crypto race for mathematical infinity.
REFERENCES


Hilley:2006:SSD

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

Hirose:2009:SAD

Hinkelmann:2007:CUN

Huhnlein:2001:TPN

Huang:2005:ASE
Qiang Huang, David Jao, and Helen J. Wang. Applications of secure electronic voting to automated privacy-preserving


Hiltgen:2006:SIB

Horwitz:2002:THI

Howard:2003:WSC

Hwang:2004:REL

Hohenberger:2005:HSO

Hwang:2005:TAU
Hwang:2005:SHW

Hwang:2005:STH

Howard:2006:SDL

Huang:2007:EPS

Hu:2007:DWD

Hwang:2008:CPK


REFERENCES


Hong:2003:BBP

Herzog:2003:PAK

Hwang:2001:TSB

Huang:2009:OSW

Hopper:2002:PSS
REFERENCES

Hu:2009:TRN

Hamdy:2000:SCB

Hartel:2001:FSJ

Hirt:2001:RFU

Harbitter:2002:MAP

Hevia:2002:PSG
Alejandro Hevia and Daniele Micciancio. The provable security of graph-based one-time signatures and extensions to algebraic signature schemes. Lecture Notes in Computer Science, 2501:379–??, 2002. CODEN
REFERENCES


REFERENCES

Huang:2007:MPK


Haitner:2009:SHC


Haastad:2004:SAR


Hanaoka:2002:HNI


Harnik:2006:CNI


Hoepman:2001:SKA

REFERENCES

Hofinger:2001:LBE

Honary:2001:CCI

Hook:2005:BCP

Hoskins:2006:SO

Hoskins:2006:SSE

Horn:2000:APF
Günter Horn and Bart Preneel. Authentication and payment in future mobile

**Huhnlein:2001:ICB**


**Han:2002:CMV**


**Hoffstein:2008:IMC**


**He:2001:SAR**

Hu:2005:USA


Hawkes:2001:PCS


Hand:2002:MPP


Halevi:2003:TEM


Haitner:2007:SHC


He:2013:GME


Harn:2009:DDB


Hromkovic:2003:AHP


Hromkovic:2005:DAR


Hromkovic:2009:AAH

REFERENCES

Haneberg:2002:MSS

Hemaspaandra:2008:EDA

Hirt:2000:ERF

Hinsley:2001:CIS

Hoffstein:2001:MAD
REFERENCES 372


Halevy:2002:LBE


Han:2002:HEF


Hwang:2007:PEA


Hong:2001:KIA

[HS+08a] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William

Halderman:2008:LWRb


Halderman:2009:LWR


Hanaoka:2002:USA


Hanaoka:2006:USA

REFERENCES

[Hernandez:2002:GCT]

[Hwang:2001:LCT]

[Hong:2002:PSR]

[Hong:2002:IDC]

[Hernandez:2001:DTR]
REFERENCES


Hanaoka:2001:EUS


Halpern:2004:RSS


Huang:2006:CSV


Hongfeng:2008:ECP


Hamalainen:2002:GPS


Hines:2007:AIF

[HTW07] Stephen Roderick Hines, Gary Tyson, and David
REFERENCES


REFERENCES


[Hsu:2005:SCT] Chien-Lung Hsu and Tzong-Sun Wu. Self-certified threshold proxy signature schemes with message recovery, nonrepudiation, and
REFERENCES


[Hwang:2003:CAL]

[Hwang:2003:ASM]

[Hye:2008:STB]

[Han:2005:PJIb]

[Huang:2005:EMP]
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:2001:IPH


IEEE:2001:ISF


REFERENCES


IEEE:2005:PIS


IEEE:2006:AIS


IEEE:2007:PAI


IEEE:2008:PAI


IEEE:2009:ISI

[IEE09a] IEEE, editor. ICM ’09: 21th [sic] International Conference on Microelectronics (ICM 2009): took place from Dec 19, 2009 to Dec 22, 2009 in Marrakech, Morocco. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA,
IEEE:2009:PAI  

Itoi:2001:SIS  

Ifrah:2000:UHN  

Iglesias:2002:NSB  

Isasi:2004:IAE  

Bassham:2000:ETA  
Lawrence E. Bassham III.
Efficiency testing of ANSI C implementations of round 2 candidate algorithms for the Advanced Encryption Standard. In NIST [NIS00], pages 136–148. [IK00] ISBN ????. LCCN ???.

Itoh:2003:PCA


Iwata:2000:PAF

Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of AES finalists — RC6, Serpent, MARS and Twofish (abstract only). In NIST [NIS00], page 9. ISBN ????. LCCN ???.

Iwata:2001:PAF

impagliazzo:2003:lra


impagliazzo:2006:lra


ichikawa:2000:hea


ishai:2003:eot


REFERENCES


Robert J. Irwin. Book review: Coding Theory and Cryptography: the Essentials, second edition, re-

**ISO:2004:IIIb**


**ISO:2005:IDM**


**Iqbal:2008:CDV**


**Inoue:2008:FAC**


**Ishai:2003:PCS**


[**Itoi:2000:SCI**]


[**Itoi:2001:SCS**]


[**Iwami:2008:AIA**]


[**Imai:2000:CPC**]


[**Irwin:2005:PAI**]


[**Iwamoto:2006:SSR**]


[**Iwata:2002:NCP**]

Tetsu Iwata, Tomonobu Yoshino, and Kaoru Kurosawa. Non-cryptographic primitive for pseudorandom permutation. Lecture
Iwata:2003:NCP


Imai:2000:PKC


Judge:2002:WWM


Jablon:2001:PAU


Jackson:2000:SCQ

REFERENCES

Jambunathan:2000:CCP


Janczewski:2000:IIS


Janczko:2006:TSH


Jankowski:2008:BRBb

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

Jankvist:2008:TMH

Jennewein:2000:FCQ

Jones:2005:RDF

Johnson:2001:IHS

Jeffrey:2008:PAM

Jennings:2009:SLL
Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC

Johansson:2000:FCA

Jaulmes:2001:CPN

Jonsson:2002:FCA

Jakimoski:2001:ASR

Jakimoski:2001:CCB

Jakimovski:2002:CS
Jonsson:2002:SRE


Jonsson:2002:SRT


Jang:2001:BWA


Jung:2001:EMO


Jallad:2002:ICC

Kahil Jallad, Jonathan
REFERENCES


**Jarecki:2000:AST**


**Joux:2003:IGN**


**Juang:2004:FBT**

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

Jeong:2008:PKE


Lee:2007:RKD


Juang:2001:FBT


Juang:2002:VMA


Jakobsson:2003:FMT


Johansson:2003:PCI

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


Jakobsson:2007:DPD


Jing-mei:2005:CRB


Joux:2002:BAA


Jao:2009:EGB

Johansson:2000:AFR


Johansson:2003:FSE


Johnson:2005:OSV


Jolish:2001:EDP

REFERENCES


REFERENCES


REFERENCES


REFERENCES

January 28, 2005. CODEN ???? ISSN 0948-6968.

Juang:2004:EPA


Juels:2004:FCI


Junod:2005:SCB

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

Jutla:2001:EMA


Ji:2001:CAF

Dongyao Ji and Yuming Wang. Comments on “An approach to the formal verification of the two-party cryptographic protocols” by
REFERENCES


**Juels:2005:APD**


**Jeng:2006:EKM**


**Jin:2005:EAW**


**Jiang:2005:RNP**


**Joye:2001:NMM**


**Jakobsson:2004:ACN**

REFERENCES

Jain:2009:NBC

Jiang:2005:TMD

Kamal:2009:RSW

Kadrich:2007:ES

Kahn:1967:CSSa

Kahn:1967:CSSb
David Kahn. *The Codebreakers: the Story of Se-
<table>
<thead>
<tr>
<th>Reference</th>
<th>Citation</th>
<th>Description</th>
</tr>
</thead>
</table>
Kapera:2005:MRP

Karski:2001:SSS

Kariya:2002:GM

Katzenbeisser:2001:RAR

Katos:2005:RTB

Katz:2005:CBR

Kendall:1939:TRS
Maurice G. (Maurice George) Kendall and Bernard Babington Smith. Tables of random sampling numbers, volume

**Kovacich:2000:HTC**


**Kiely:2006:SSM**


**Kamvar:2007:DTM**


**Kim:2009:DCA**


**Kachris:2003:RLB**


**Keller:2009:ECC**

DEN ????, ISSN 1936-7406 (print), 1936-7414 (electronic).

[[kc01] claffy:2001:IMM


[[KC09b] Kieu:2009:IAB

[[KCC05] Ku:2005:WYR
REFERENCES


REFERENCES


Kurosawa:2004:NPH


Keefe:2005:CDS


Kelsey:2000:KST


Kelsey:2002:CIL


King:2001:SAD

Kellar:2005:NRR


Keller:2005:NRR


Kenyon:2002:HPD


Kettani:2006:CBN


Kelsey:2000:CPL


Kiltz:2009:DCC

REFERENCES

Katsikas:2004:PKI


Kaps:2007:CSD


Kovacich:2003:MHC


Kim:2005:SMA


Kato:2008:QSC

REFERENCES

aip.org/link/?PSI/7092/70920H/1. Quantum Communications and Quantum Imaging VI.

Khaw:2005:EDA


Komninos:2001:ESC


Kwon:2005:CLK


Koo:2009:SVN


Kirovski:2004:DWF


Kausar:2008:SEK


**Kidwell:2000:SNC**


**Kidwell:2007:CSB**

Peggy Aldrich Kidwell. *Colossus: The Secrets of
REFERENCES


REFERENCES

Kim:2002:ISC


King:2000:IMP


King:2001:CMF


King:2002:RGI

REFERENCES


**Kim:2002:NIS**


**Klein:2003:FOW**


**Kawachi:2006:PQC**


**Kashefi:2007:SZK**


**Karri:2003:PBC**

REFERENCES


[KKKP05] Akinori Kawachi, Hirota Ko, Toshihiro Takeishi

**Kim:2009:SVN**


**Kaliski:2002:CHE**


**Kelsey:2000:ABA**


**Kohno:2000:PCR**

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


Kelsey:2001:ABA

Katz:2005:HEP

Katz:2008:IMC
Knill:2002:FPE


Knill:2002:QIP


Ko:2000:NPK


Klein:2007:BDC


Kong:2001:AVW


REFERENCES

Knudsen:2000:CRA


Knudsen:2001:CRR


Knudsen:2001:CPL


Kanda:2002:SCA

Masayuki Kanda and Tsutomu Matsumoto. Security of Camellia against truncated differential cryptanalysis. Lecture Notes in Computer Science, 2355:
Koblitz:2004:OTS

Koblitz:2004:SPK

Koblitz:2005:PBC

Kornerup:2007:PIS
REFERENCES


REFERENCES

Keliher:2001:IUB

Kim:2003:RCC

Kol:2008:GEI

Koc:2001:CHEb
Çetin K. Koç, David Naccache, and Christof Paar, editors. Cryptographic hard


references


Kushilevitz:2000:OWT


Komano:2003:EUP


Katz:2004:ROS


Koblitz:2000:TQC


Kocher:2002:IS

Paul Kocher. Illusions of security, 2002. URL
Koga:2002:GFR


Kurosawa:2001:ICP


Koshiba:2001:NAS


Koshiba:2001:SRS


Kornblum:2009:IBD


Ko:2002:GFR

Koskinen:2001:NIK


Kovach:2001:BCB


Kovacich:2003:ISS


Katz:2001:EPA


Katz:2009:ESA


Katzenbeisser:2000:IHT

Koc:2001:CHEa


Koc:2003:GEI


Kerins:2002:FPE


Klima:2003:ARB

REFERENCES

Kaufman:2002:NSP


Kim:2004:TBG


Krishna:2003:BUP


Krawczyk:2001:OEA


Krause:2002:BBC


Krause:2002:USP

Krawczy:2003:SSM  

Krawczyk:2005:HHP  

Kramer:2007:LCC  

Kreitz:2005:OBE  

Koeune:2002:Fil  
Kehr:2001:ISM


Kim:2005:CLL


Katz:2000:CCA


Kelsey:2000:MAP


Kuramitsu:2002:ETC

Krause:2003:DOC


Kozaczuk:2004:EHP


Katz:2005:MIA


Kiltz:2005:TCL


Kissner:2005:PPS


Klivans:2006:CHL

REFERENCES

4031329. IEEE Computer Society Order Number P2720.

Kurkowski:2006:QFF


Kasper:2009:FTA


Klivans:2009:CHL


Kelsey:2000:YND

REFERENCES


Kang:2001:PSK

Kumar:2002:APS

Kogan:2006:PRS
REFERENCES

Kelsey:2000:SCC


Kuribayashi:2000:WSB


Kuribayashi:2001:NAF


Kogan:2006:IER


Ku:2003:TSA

Wei-Chi Ku, Hao-Chuan

Kobayashi:2007:AIG


Kuhn:2000:PCL


Kuhn:2001:CRR


Kuhn:2002:OTD


Ku:2002:IIB


Ku:2004:HBS


**Kuhn:2002:ICM**


**Kuhn:2008:BSS**


**Kukorelly:2001:PAL**


**Kumagai:2001:MRP**


**Kundur:2001:WDI**


**Kurosawa:2001:MRP**

Kusters:2002:DCP


Kuo:2001:AOS


Komninos:2007:ALS


Kejariwal:2009:ELL


Koshiba:2000:SEP


Knudsen:2002:IC

Lars Knudsen and David
REFERENCES


Karlof:2003:HMM


Keromytis:2006:COS


Kwon:2002:DSA


Kwok:2003:WBC


Kwon:2003:EDS


Kumar:2006:ODS

Sandeep Kumar, T. Wollinger, and C. Paar. Optimum

Wong:2001:MCC


Kun:2000:SMA


Kamat:2009:TPW


Katz:2000:CCS


Katz:2001:UEC

REFERENCES

Kavut:2001:SCP


Kiayias:2001:PRB


Kiayias:2001:SPP


Kurosawa:2001:LCI


Katz:2002:TCB

Kiayias:2002:CHB


Kim:2002:PAA


Katz:2003:SPA


Kamal:2009:FIN


Kang:2001:PMT

Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. Lecture Notes in Computer Science, 2119:60–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:
Kabatnik:2001:LSD


Kamp:2003:DEB


Kumar:2009:UAU


Ladd:2006:SPS


Lafe:2000:CAT

Olu Lafe. *Cellular automata transforms: theory*


REFERENCES

[Lambert:2007:SLG]

[Lan00a]

[Lan00b]

[Lan00c]

[Lanet:2000:ITS]

[Lan04a]
REFERENCES

http://www.rsasecurity.com/rsalabs/faq3-1.html


Lawton:2005:MAH


Lawson:2009:SCA


Lawson:2009:TAG


Li:2004:QAU


Lindskog:2005:DIT


Lee:2000:UBN


Leveiller:2001:CNF

REFERENCES


[LC05a] Rongxing Lu and Zhenfu Cao. Efficient remote user authentication scheme using

[Lu:2005:NDA]

[Lu:2007:NPL]

[Lee:2001:SEK]

[Lee:2003:APS]

[Levi:2004:UNC]
Albert Levi, M. Ufuk Caglayan, and Cetin K. Koc. Use of nested certifi-

Lee:2004:DEB


Lim:2009:OPG


Li:2008:CAM


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

**Lai:2004:SGS**


**Lavoue:2007:SSW**


**Law:2006:SBB**


**Lindquist:2004:JCS**


**Lee:2001:AES**


**Lee:2003:BRBa**


**Lee:2003:BRBb**


REFERENCES


Lekkas:2004:CNL


Levi:2009:ULM


Lan:2010:RNG


Lang:2001:CMS


Lin:2003:PAS


Lee:2004:CUS

Narn-Yih Lee and Pei-Hsiu Ho. Convertible undeni-


REFERENCES


REFERENCES

Li:2001:NSA


Li:2005:ABPa


Lieman:2005:CRW


Lin:2000:RTI


Linn:2000:TMM


REFERENCES

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


REFERENCES


Lee:2005:ENB

Lee:2005:EVB

Lee:2005:IHA

Lee:2005:ILL

Lim:2000:GTC

Luo:2004:UUR

Lu:2001:DWC
Chun-Shien Lu and Hong-Yuan Mark Liao. Digital


Lim:2004:ISC


Lee:2005:CMA


Lee:2005:SSP


Li:2005:FCR

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


Lee:2006:ISC

REFERENCES


Lesniewski-Laas:2005:SSS


Li:2001:SPD


Lee:2002:SEC


Lee:2004:MPA


Li:2006:ESY


[HYZ05a] Hongjun Liu, Ping Luo, and Daoshun Wang. A scalable authentication model based on public keys. *Journal...
REFERENCES


REFERENCES


REFERENCES


[LPL96] Pierre Loidreau.

[LOI00] Pierre Loidreau.

[Lov01] Daniel Lovering.


[Lop00] Javier Lopez.


REFERENCES


**Lindell:2000:PPD**


**Lysyanskaya:2001:AST**


**Labbe:2002:AIF**


**Luccio:2002:AC**


**Lee:2003:CPK**

Eonkyung Lee and Je Hong Park. Cryptanalysis of the public-key encryption based on braid groups. Lecture Notes in Computer Science, 2656:477–490, 2003. CODEN
REFERENCES


Li:2005:MCK


Li:2006:PMW


Li:2008:DEO


Lientz:2001:BTP

REFERENCES


REFERENCES


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

Lu:2005:BIW


Li:2005:ABPb


Liang:2009:AIE


Lee:2001:EP1


Liu:2005:RBU

Lin:2004:SIS


Li:2005:ISS


Lie:2000:ASC


Lin:2005:HAO


Lu:2002:HEA


Lu:2007:NSC

REFERENCES

Lucks:2000:ASR
Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys. In NIST [NIS00], pages 215–229. ISBN ???. LCCN ???. URL [Luc00]

Lucks:2000:SAB
Stefan Lucks. The saturation attack — A bait for Twofish. Lecture Notes in Computer Science, 2355:1–??, 2002. CODEN [Luc02b]

Lucks:2002:VCS

Lucas:2006:PGE

Ludvig:2005:PWF

Lukyanov:2001:PFA
Dmitro O. Luk’yanov. On the problem of the forma-

Lunde:2009:BCU


Lutz:2002:BBS [LVo0]


Lutz:2003:BLF [LV04]


Lenstra:2000:XPK


Lu:2004:FCA

Yi Lu and Serge Vaudenay. Faster corre-
tion attack on Bluetooth keystream generator E0. In Franklin [Fra04], pages 407–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN [LW04]
0302-9743 (print), 1611-3349 (electronic). LCCN 10.1007/b99099. URL
volume&id=doi:10.1007/b99099.

Laguillaumie:2007:MDV


Lange:2002:PIE

link/service/series/0558/1
bibs/2387/23870137.htm; http://link.springer-n
ny.com/link/service/series/1

Lyuu:2005:CIH

Yuh-Dauh Lyuu and Ming-Luen Wu. Cryptanalysis of


REFERENCES


Li:2007:PBS


Lixin:2005:FLA


Li:2007:NBA


Lou:2002:ESA


Liu:2007:IFW

REFERENCES

Lysyanskaya:2002:USV


Lysyanskaya:2007:AI


Lysyanskaya:2008:CHK


Leung:2001:WDI


Li:2004:CAB


Lao:2009:ORA


Li:2001:GOT

Zi-Chen Li, Jun-Mei Zhang, Jun Luo, William Song,

Li:2004:WMS


Michener:2000:MSA


Masuda:2002:CDC


Maurer:2007:ICP


Mrayati:2003:AKT

REFERENCES


MacKenzie:2001:MEP


Mohay:2003:CIF


Madsen:2000:HCI


Madsen:2000:RDU


Madsen:2000:WUN


Madsen:2004:FFD


Mahle:2004:DDI

Melissa Boyle Mahle. Denial and deception: an insider's view of the CIA from Iran–Contra to 9/11. Nation Books, New York, NY,


[Mar04]


[Mar02a]


[Mar02b]


[Mars05a]


[Mar05b]


[Mart07]


[Mart08a]

REFERENCES


Mohanty:2008:IWB


McAndrew:2008:TCO


McKinnon:2004:CCS


Montenegro:2004:CBI


McGraw:2006:SSB


Myles:2005:ETS

Ginger Myles, Christian

**McKenna:2004:EAE**


**McLaughlin:2006:PZW**


**McNichol:2003:HTM**


**Martin:2004:AMC**


**Macchetti:2005:QPH**


**McCaman:2008:QIF**

Monteiro:2008:AVM


Meadows:2001:OIF


Meadows:2004:OSM


Mehrabi:2001:DW


Mena:2003:IDM


Menezes:2005:TCC

REFERENCES

Menezes:2007:ACC

Messerges:2000:SAF

Messerges:2001:SAF

McGrew:2001:AAE

Marti-Farre:2007:NSS


Millan:2004:NCE


Matula:2005:TLS


Mueller:2006:SMG


Muller:2009:BPE


Minier:2001:SCC

REFERENCES

Muresan:2008:PCA


Mukherjee:2002:CAB


Maas:2009:SRW

Moon:2002:IDC


May:2002:SKS


Mihaljevic:2009:ASC


Micciancio:2001:ILB


Micciancio:2002:GCK

REFERENCES

Micciancio:2002:ICH


Millen:2003:FD


Minkel:2003:CTT


Mironov:2002:RSO


Mirkovic:2005:IDS


Mishra:2006:PCS


Misic:2008:TEC

Jelena Mišić. Traffic and
energy consumption of an IEEE 802.15.4 network in
the presence of authenticated, ECC Diffie-Hellman
ephemeral key exchange. [Miy01]

Computer Networks (Amsterdam, Netherlands: 1999),
52(11):2227–2236, August 8, 2008. CODEN ???? ISSN
1389-1286 (print), 1872-7069 (electronic).

Mitchell:2000:MSN

Chris J. Mitchell. Making serial number based au-
thentication robust against loss of state. Operating
OSRED8. ISSN 0163-5980 (print), 1943-586X (elec-
tronic).

Mitra:2002:TAD

Ananda Mitra. Trust, authenticity, and discursive
power in cyberspace. Communications of the Associa-
tion for Computing Machinery, 45(3):27–29, March
2002. CODEN CACMA2. ISSN 0001-0782 (print),
1557-7317 (electronic).

Mitrakas:2002:CCI

Andreas Mitrakas. Citizen centric identity manage-
July 1, 2002. CODEN NTSCF5. ISSN 1353-4858
(print), 1872-9371 (electronic). URL http://

www.sciencedirect.com/science/article/pii/S1353485802070101

Miyazaki:2001:ISG

Takeru Miyazaki. An improved scheme of the
Gennaro-Krawczyk-Rabin undeniable signature sys-
tem based on RSA. Lecture Notes in Computer Science,
2015:135–??, 2001. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic). URL http://
http://link.springer-ny.com/link/service/series/0558/1
bibs/2015/20150135.htm; http://link.springer-
y.com/link/service/series/0558/papers/2015/20150135.
pdf.

MacDonald:2003:CDS

Matthew MacDonald and Erik Johansson. C# data
security handbook. W r o x
(paperback). vii + 356 pp. LCCN ????

Maltoni:2004:BAE

Davide Maltoni and Anil K. Jain, editors. Biome-
tric Authentication: ECCV 2004 International Work-
shop, BioAW 2004, Prague, Czech Republic, May 15th,
2004: Proceedings, volume 3087 of Lecture Notes in
Computer Science. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
REFERENCES

Moore:2001:AGK


Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS


Moyle:2005:CLD


Mazieres:2000:SKM

REFERENCES

Majzoobi:2009:TDI


McDonald:2008:SID


McGregor:2005:PCK


Malone-Lee:2003:TBO


Maitra:2001:SDD

S. Maitra and D. P. Mukherjee. Spatial domain digital watermarking with buyer


[MM07b] Gary L. Mullen and Carl
REFERENCES


Moreira:2002:RCE


Milenkovic:2005: UIB


Maltoni:2003:HFR


McEvoy:2009:IWH


Maitra:2006:PCI

REFERENCES


Matsumoto:2002:IAG


Maclean:2000:OIG


Mizuki:2001:NSN


Mercuri:2003:IRS


Mukhopadhyay:2014:EMP

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

**Martel:2004:GMA**

Charles Martel, Glen Nuckolls, Premkumar Devanbu, Michael Gertz, April Kwong and Stuart G. Stubblebine.

A general model for authenticated data structures.


**Mansonri:2001:WMS**

M. Monisgnori, P. Nesi, and M. B. Spinu.


**Mironov:2008:SAE**

Ilya Mironov, Moni Naor, and Gil Segev.

Sketching in

MacAndrew:2000:LPT


Mykletun:2006:AIO


Mollin:2001:IC


Moller:2002:PEC


Moller:2003:PSP

### References

**Mollin:2003:RPK**


**Mollin:2005:CGS**


**Mollin:2007:IC**


**Monniaux:2003:ACP**

David Monniaux. Abstracting cryptographic protocols with tree automata.

**Moo01**


**Mool03b**


**Moo07**


**MOP06**

REFERENCES

Morris:2003:KKL


Moritz:2005:KAE


Moses:2006:DSD


Merton:2000:NBG


McMillan:2001:JIA


Mihailescu:2001:BRE

REFERENCES


Moshopoulos:2001:NSA


Malkhi:2002:ACE


Maurer:2003:SMR


Micciancio:2005:ASS


Matusiewicz:2006:FGD

Krystian Matusiewicz and Josef Pieprzyk. Finding

Munilla:2007:HMF


Micciancio:2008:OCC


Mislove:2006:EBO


Moralis:2009:KSA


Micali:2005:OEC

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

522


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


Murphy:2002:EASb


Matyas:2003:TRU


Micciancio:2009:LBC


Monrose:2002:TSG


Mitchell:2006:PPT


Moghadam:2010:DRN

I. Zarei Moghadam, A. S. Rostami, and M. R. Tahatalab. Designing a random number generator with

Mayer-Sommer:2001:SAS


Maggi:2002:USV


Maitra:2002:CSB


Menezes:2002:PCI


[Meadows:2005:CPA]

[Mahdian:2009:UNI]

[Myers:2009:BEC]

[Shen:2005:NW]

[Marton:2010:RDC]
Kinga Marton, Alin Suciuc, and Iosif Ignat. Ran-

MacKenzie:2002:TPA


Matsumoto:2007:FSC


Miltchev:2008:DAC


Mouratidis:2009:PMD

Kyriakos Mouratidis, Dimitris Sacharidis, and Hweehwa Pang. Partially mate-


Muller:2001:SWB


Mullins:2002:MUC


Mullins:2006:CC


Munro:2008:DE


Murphy:2000:KST

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

Murray:2001:CDC


Murray:2002:IYP


Murton:2006:CGH


Moriai:2000:PTL


Meister:2001:PPG


Micciancio:2003:SZK

REFERENCES


REFERENCES


REFERENCES

/N ds online.computer.org/ 0309/f/gaep.htm.


/Nakai:2001:SFW


[Nao:2002:DRA]
REFERENCES


Niederreiter:2002:BRC


Nielsen:2002:SRO


Nievergelt:2002:FLM

[Niederreiter:2004:BRC]

[Nikander:2002:DSAb]

[NIST:2000:TAE]
REFERENCES

NIST:2001:CT

NIST:2001:SRC

Nitaj:2009:CRCo

Nisley:2003:ELH

NIST:2003:RKE

Nisley:2003:ELH

NIST:2003:RKE

Ning:2008:MAA
REFERENCES

[NM09] Mark J. Nigrini and Steven J. Miller. Data diagnostics using second-order tests of Benford’s Law. *Audit-


[NN06] Ventzislav Nikov and Svetla...

Navin:2010:ETU


Naor:2001:RTS


Naor:2005:ECH


Novak:2001:SBA

REFERENCES


REFERENCES

Nichols:2000:DYD


Neraud:2001:CFD


Nguyen:2001:TFLa


Narayanan:2005:FDA


Narayanan:2005:ODG

Arvind Narayanan and Vitaly Shmatikov. Obfuscated databases and group


REFERENCES


REFERENCES


Ohigashi:2009:PMF

Ohkuma:2001:BCH

Ohbuchi:2002:FDA

Onions:2001:SSI

Ors:2003:PAA


REFERENCES


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

Okeya:2004:SBR


Osvik:2005:CAC


Osvik:2006:CAC


Osvik:2000:SS

Dag Arne Osvik. Speeding up Serpent. In NIST [NIS00], pages 317–329. ISBN ???. LCCN ???. URL ???.

Okeya:2003:MFC


REFERENCES


[OZL08]

[Pal02]

[Pae03]

[Pap05]
REFERENCES


REFERENCES


Patarin:2003:LRR

Paterson:2003:CCI

Patarin:2004:SRF

Paulson:2001:RBS

Paulson:2002:NBPb
Linda Dailey Paulson. News briefs: Project promises accessible technology for the

**Paulson:2002:NBR**


**Paulson:2003:NBV**


**Paulson:2009:NBT**


**Praca:2001:SCS**


**Piva:2002:MCW**

Alessandro Piva, Franco Bartolini, and Mauro Barni. Managing copyright: Wa-

Piva:2005:SRA


Park:2000:CAP


Peng:2005:SES


Peng:2007:BZK


Prattichizzo:2007:PIH


Papadimitriou:2001:PSE

S. Papadimitriou, T. Bountis, S. Mavroudi, and
REFERENCES


REFERENCES


Park:2005:ISC


Park:2005:NDS


Perlnert:2009:QRP


Park:2003:ESA


Patarin:2001:QBL

REFERENCES


Pelzl:2006:PAC


Pemble:2001:CEW


Pemble:2001:SPA


Perrine:2003:ECP


Perlman:2005:EMD


Perry:2005:DCP


Petullo:2003:IEH


Petullo:2005:EYR

REFERENCES

2005. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Petzold:2008:ATG


Potter:2003:S


Pfitzmann:2001:ACE


Phatak:2005:FMR


Power:2007:SBB


Provos:2003:HSI

[PH03] Niels Provos and Peter Honeyman. Hide and

PHAN:2004:IDC


PHAN:2006:CTP


PHILPOTT:2006:ITD


PAENG:2001:NPK


POLK:2003:IIC

REFERENCES


[Pin06] Stephen Pincock. Codebreaker: the history of codes
and ciphers, from the ancient pharaohs to quantum cryptography. Walker, [PJK01]
2006. URL http://www.loc.gov/catdir/enhancements/fy0730/2007310362-b.html;
http://www.loc.gov/catdir/enhancements/fy0730/2007310362-d.html.

[Pip03]

[PJH01]

[Poh:2001:HBP]

[Petitcolas:2003:DWF]
Fabien A. P. Petitcolas and Hyoung Joong Kim, editors. Digital watermark-
REFERENCES


REFERENCES


REFERENCES


Bruce Potter. Converging wired and wireless authentication. *Network Se-


REFERENCES


[PQ06] Olivier Pereira and Jean-Jacques Quisquater. On the impossibility of building secure Cliques-type authenticated group key agree-

Preneel:2000:ACE


Preneel:2001:NES


Preneel:2002:NEA


Preneel:2002:NPT


Preneel:2002:TCC

REFERENCES


**Preneel:2007:SRD**


**Price:2000:NCH**


**Provos:2000:EVM**


**Provos:2001:DAS**


**Paun:2004:CTT**


**Poupard:2000:FER**

Guillaume Poupard and Jacques Stern. Fair encryption of RSA keys. *Lecture Notes in Computer Science,*
REFERENCES


Parker:2001:RKC


Pfitzmann:2001:SEC


Pornin:2001:SHT


Padro:2002:LBI


Pomerance:2002:SOC

REFERENCES

bibs/2369/23690338.htm;


Prabhakaran:2005:RES

Phan:2006:FDB

Prabhakaran:2004:NNS

Park:2008:SRB
REFERENCES

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

[Pavlou:2008:FAD]


[Park:2002:SRL]


[Pareschi:2009:PAC]


[Preneel:2006:SAC]

REFERENCES

Pang:2008:VCR

Pfleeger:2007:GEI

Pucella:2003:JRB

Pucella:2006:SCC

Pucella:2007:Jb

Puzmanova:2004:RWF

Page:2006:FAP
D. Page and F. Vercauteren. A fault attack on pairing-


REFERENCES


Pieprzyk:2002:CCI


Pecho:2009:APW


Peng:2009:DIE


Qian:2005:CLT


Qian:2005:SPL


Quisquater:2005:SCC

REFERENCES


[Raj06] Sergio Rajsbaum. ACM


[Raj06] Sergio Rajsbaum. ACM


Rijmen:2008:RSA


Roth:2001:EJA


Rogers:2005:NSE


Rubin:2006:CSE


Reed:2000:ANA


Rubin:2005:ARS

REFERENCES


[RE02] K. Jonathan Riley and John P. Eakins. Content-based retrieval of histori-
References


REFERENCES

Ren:2009:CWT


Rescorla:2001:IOPa


Rescorla:2001:IOPb


Reynard:2001:SCB


Rodwell:2007:NIBa


Rodwell:2007:NIBb


Rodwell:2007:NIBc

Ringenburg:2005:PFS

Rotondi:2006:CHA

Ren:2009:FCS

Rose:2006:CSP

Rojas:2000:FCH

Roscoe:2002:TBC

Rafaeli:2003:SKM
Sandro Rafaeli and David Hutchison. A survey of key management for secure group communication. ACM Computing Surveys, 35(3):
REFERENCES

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


Ruan:2006:NSC


Reddy:2002:AAM


Riedl:2002:FSH


Roy:2004:FSE

REFERENCES

Ruiz:2001:SPS


Reyhani-Masoleh:2003:LCS


Reyhani-Masoleh:2003:LCB


Reyhani-Masoleh:2004:TFT


Rahaman:2008:CTB

REFERENCES


REFERENCES

2000. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).


Rothe:2002:SFC


Rothe:2003:SFC


Rothe:2005:CTC


Rothe:2007:BRB


Roy:2000:PCI


Roychowdhury:2000:PCJ


Roy:2005:ACA

Bimal Roy, editor. *Advances in cryptology: ASI-
REFERENCES


**REFERENCES**

**Ratner:2003:NHS**


**Rosenberg:2004:SWS**


**Rittinghouse:2005:IIM**


**Rechberger:2008:NRN**


**Ricthberger:2006:NCW**


**Rivest:2000:RA**

REFERENCES

[RS00]

[Rubin:2002:SAV]

[Rubin:2003:TBC]

[Ros01]
REFERENCES


[RSA00c] RSA Laboratories. PKCS #15 v1.1: Cryptographic Token Information Syntax Standard. RSA Data Security, Inc., Redwood City, CA, USA, June 6,
REFERENCES


Rukhin:2001:STS

Rogers:2005:MPH

Rouvroy:2003:EUF

Ryabko:2004:NTR


S. P. Saini and F. Ahmad. Java model of DSA (Dig-
Saeednia:2002:IBS


Sakamura:2001:GEI


Sale:2000:CGL


Sale:2000:CBP


Sale:2001:GRT


Salus:2001:CA


Salomon:2003:DPS

David Salomon. *Data Privacy and Security*. Springer-

Salus:2003:BRBb


Sale:2005:RCB


Sallee:2005:MBM


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

Salomon:2005:CDC


Salomon:2005:FCS

Salomon:2007:DCC


Sale:20xx:CRP


Samid:2001:ESR


Santini:2005:WSI


Sarkar:2002:FCM


Sasse:2007:REB


Stoklosa:2005:CIC

Stallings:2007:CSP

Sherwood:2005:MTR

Steiner:2001:SPB

Smeraldi:2002:SVF

Shehab:2005:SCM


Stoll:2002:MMC

Sun:2002:WDC

Shao:2005:NEV

Stephanides:2005:GAK

Sun:2005:IPK

Siegelin:2001:SCD

[SC02b]

[SC02c]

[SC05a]

[SC05b]

[SC05c]
Schmalz:2000:MAD


Schneier:2000:AAR


Schneier:2000:SLD


Schneier:2000:SRF


Scharinger:2001:ASK

Josef Scharinger. Application of signed Kolmogorov hashes to provide integrity and authenticity in Web-based software distribution. Lecture Notes in Computer Science,
REFERENCES


Schindler:2001:TAA


Schmalz:2001:MDI


Schneier:2001:FSE


Schnorr:2001:SGH

Schnorr:2001:SDE


Schultz:2002:GBC


Schneier:2003:BFT


Schmalz:2004:MDIa


Schmalz:2004:MDIb


Schneier:2004:SA

REFERENCES


<table>
<thead>
<tr>
<th>References</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SCS05b] Sun:2005:CCL</td>
<td>Da-Zhi Sun, Zhen-Fu Cao, and Yu Sun. Comment: cryptanalysis of Lee-</td>
</tr>
</tbody>
</table>
REFERENCES


REFERENCES

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

Seifert:2005:ACR


Speed:2002:PIS


Selçuk:2000:BEL


Semanko:2000:CAA


Sennewald:2003:ESM


Sergienko:2006:QCC


Sonntag:2000:MAS

Shirase:2005:AEC

Seyedzadeh:2011:IEA

Shailer:2001:PMT

Shamir:2001:NDC

Shamir:2001:PSC
Adi Shamir. Protecting smart cards from passive power analysis with detached power supplies. Lecture Notes in Computer Science, 1965:71–??, 2001. CODEN LNCSD9. ISSN 0302-
Shao:2001:BVM

Sharp:2001:IKB

Shapiro:2002:CCM

Shamir:2003:RS

Shamir:2003:TLC

Shao:2003:CIB


REFERENCES

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

Hwang:2009:KDB


Shepherd:2001:CDC


Sung:2007:CIB


Shih:2008:DWS


Sierra:2004:LCC


**Shoup:2005:CIN**


**Shparlinski:1999:NTM**


**Shparlinski:2001:UDR**


**Shparlinski:2002:SMS**


**Shparlinski:2003:CAA**


Shparlinski:2005:PHS


REFERENCES


Silverman:2001:CLI

Silverman:2005:ECC

Simon:2002:CRE

Singh:1999:CBE

Singh:2000:CBE

Singh:2001:DPK
REFERENCES


REFERENCES


**REFERENCES**


REFERENCES


REFERENCES

Shim:2005:SFA


Srivatsa:2005:SPS


Skoudis:2006:CHR


Stamp:2007:ACB


Sun:2009:CPR


Su:2005:KPK

REFERENCES

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

Shi:2005:HEC


Shen:2003:SET


Sung:2000:PSS


Salido:2007:EBE


Song:2001:DWF


Solar-Lezama:2006:CSF

Armando Solar-Lezama, Liviu Tancau, Rastislav Bodik, Sanjit Seshia, and Vijay Saraswat. Combinato-

**Sarkar:2000:CNB**


**Sarkar:2000:NBC**


**Sebag-Montefiore:2000:EBC**


**Sarkar:2001:EIL**


**Satoh:2002:SHS**

Akashi Satoh and Sumio Morioka. Small and high-speed hardware architectures for the 3GPP standard cipher KASUMI. *Lee-
Sarkar:2003:EIC


Satoh:2003:UHA


Sebag-Montefiore:2005:EBC


Sebag-Montefiore:2007:EBC


Simos:2007:CMS

REFERENCES

Smith-Miles:2008:CDP

Seyedzadeh:2011:IES

Smart:2001:CDF

Smart:2003:ACU

Smart:2003:AGR
REFERENCES

Smart:2005:CCI

Small:2006:USR

Smith:2000:ABS

Smith:2001:IK

Smith:2001:ECB

Smith:2001:APP

Smith:2002:OAP
REFERENCES


Mark Strembeck and Gustaf Neumann. An integrated approach to engineer and enforce context constraints in RBAC environments.
REFERENCES


REFERENCES


REFERENCES


REFERENCES

5827 (electronic). See [Sti95, Sti02, Sti06c].


REFERENCES

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


REFERENCES

Seddik:2009:IWB

Shi:2008:UAU

Susilo:2000:NEF

Scambray:2006:HEW

Schmidt-Samoa:2006:AFW

StPierre:2000:TFA
Sakurai:2001:NSS


Shamir:2001:IOO


Stern:2001:ADW


Stinson:2001:SAC


Sakurai:2002:SMP

Kouichi Sakurai and Tsuyoshi Takagi. On the security of a modified Paillier public-key primitive. *Lecture Notes in Computer Science,*
REFERENCES


REFERENCES


REFERENCES


Steele:2005:PPT

Stiel:2005:MMM

Stern:2005:MLF

Stein:2008:ENT

Stinson:1995:CTP

Stinson:2001:C

Stinson:2002:CTP

**Stieber:2006:OH**

**Stieber:2006:GH**

**Stinson:2006:CTP**

**Stipcevic:2011:QRN**

**Shimoyama:2002:MLC**

**Stone:2001:C1**

**Struif:2001:UBU**
Bruno Struif. Use of biometrics for user verification in electronic signature smartcards. *Lecture...
REFERENCES


Strunk:2001:JQJ


Strubinger:2002:HBS


Stytz:2004:BRW


Saxena:2007:TCP


Shaltiel:2007:LEU


Sugihara:2001:PCD

Sugita:2003:DRW


Sun:2000:ESM


Sun:2002:IIR


Sun:2005:UMS


Seidl:2008:FOV

Helmut Seidl and Kumar Neeraj Verma. Flat and one-variable clauses: Complexity of verifying cryptographic protocols with single blind copying. *ACM
Shaltiel:2008:HAP


Sebe:2007:SMO


Shmueli:2009:DEO


Smith:2000:CIR


Schneier:2000:PCF


Sun:2000:AFA

Yongxing Sun and Xinmei Wang. An approach to finding the attacks on the cryptographic protocols. Operat-
Stubblebine:2002:ALF


Shim:2005:WIB


Stuck:2005:HVC


Shieh:2006:ERM


Swaine:2001:PPSa


Swenson:2008:MCT

REFERENCES

**Song:2005:ISG**


**Song:2007:TAK**


**Swire:2005:SMI**


**Stevenson:2005:SCI**

Daniel E. Stevenson, Michael R. Wick, and Steven J. Ratering. Steganography and cartography: interesting assignments that reinforce machine representa-

**Sun:2009:TDS**


**Shujun:2001:PRB**

REFERENCES

Seo:2001:CDA


Shi:2001:NSF


Syed:2000:CLA


Sun:2005:CSS


Syverson:2002:FCI

REFERENCES


Shimoyama:2002:BCS


Steinfeld:2001:ALE


Skoudis:2003:MFM


Sarikaya:2008:SPT


Sun:2002:NAD

Qi Sun, Qi Fan Zhang, and Guo Hua Peng. A new algorithm for the Dickson polynomial $g_{e}(x; 1)$ public key cryptosystem. Sichuan Daxue Xuebao, 39(1):18–23,
REFERENCES

2002. CODEN SCTHAO. ISSN 0490-6756.


[TBDL01] Trichina:2001:SCH Elena Trichina, Marco Bucci, Domenico De Seta,


Trudel:2003:DSE


Teepe:2006:PPA


Todd:2001:LSS


Terai:2008:BRB


Thorsteinson:2004:NSC


Theoharidou:2007:CBK

REFERENCES


REFERENCES

Tseng:2001:CLB


Tseng:2003:DSM


Tico:2003:RAS


Toll:2008:CSE


Thien:2002:TSS


Thomas:2007:HQU


Turner:2006:SIS


Tsai:2005:CAE


Tan:2004:OBC


Torrubia:2001:CRC


Tian:2005:RWS

Tsolis:2009:ARM


Teoh:2004:PCK


Tousidou:2000:IMS


Tanaka:2001:QPK


Tochikubo:2000:RAE


Tomaszewski:2006:YSY


www.sciencedirect.com/science/article/pii/S0167404808000084


REFERENCES


REFERENCES


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


[Tyn05] Tzeng:2004:NTM


[TYH04] Ting:2002:FBS


[TZT09b] Tong:2009:RAPa

Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number generator. In 2009. CSO 2009. International Joint Conference on Computational Sci-
REFERENCES

Tong:2009:RAPb

&arnumber=5193698.

TZT09b

Uz:2009:MBT


UBEP09

Unay:2008:SQE


UHA+09

Uchida:2009:FPR

&arnumber=5162237.

Uni00a

USC:2000:HRS

United States Congress. H.R. 850, the Security and Freedom through Encryption (SAFE) Act: Markup before


USENIX, editor. Proceed-
REFERENCES


USENIX:2001:PTU


USENIX:2002:PBF


USENIX:2002:PUS


USENIX:2002:PFT


Utami:2002:FID


Urien:2001:XS


Salil P. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. In Boneh [Bon03], pages 61--77. CODEN LNCSD9. ISBN 3-540-40674-3. ISSN 0302-9743
REFERENCES


Verheul:2001:EXM


Vercauteren:2002:CFZ


Vergnaud:2006:RBS


Vernitski:2006:CUM


Vladimirov:2004:WFS


Vassev:2009:STA

REFERENCES

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

Voloshynovskiy:2001:BDA


Viroli:2003:TPA


Vixie:2002:SRR


Vural:2007:IND


Vo:2008:SMA

REFERENCES

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


REFERENCES

csd1.computer.org/dl/mags/co/2004/03/r3013.

[Voice:2005:OAM]


[Vogt:2001:USC]

Holger Vogt, Henning Pag- nia, and Felix C. Gärtner. Using smart cards for fair exchange. Lecture Notes in Computer Science, 2232:
link.springer-ny.com/link/service/series/0558/bibs/2232/22320101.htm;

[Vaso:2001:CPK]

elsevier.com/gej-ng/10/23/20/84/36/30/abstract.html.

[vOWK07]


[vOT08]


[vOorschot:2008:PMU]

P. C. van Oorschot, Tao Wan, and Evangelos Kranakis. On interdomain routing security and pretty secure BGP (psBGP). ACM Transactions on Information and System Security,
scheme in the presence of transient hardware faults. 


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

vanTilborg:2000:FCP


vanTilborg:2001:ECC


vanTilborg:2005:ECS


Vaudenay:2007:POK


Venkatesan:2001:GTA

vonWillich:2001:TIT


Vaudenay:2001:SAC


Whittaker:2006:HBW


Woody:2007:COS


Weitzner:2008:IA


Wachsmann:2005:CAK

REFERENCES

Wallach:2000:SSM


Wagner:2000:CYL


Wagner:2002:GBP


Wagstaff:2003:CNT


Walsh:2000:BRM

References

Walter:2001:PBM


Walter:2003:STM


Wallich:2004:EEI


Wallich:2009:SGP


Wang:2004:AWA


Wang:2004:TVS

Shiuh-Jeng Wang. Threshold verification scheme to a valid-signature using identity only on specialized ap-

Wang:2005:SCR


Wardlaw:2000:RPK


Washington:2008:BRB


Washington:2008:ECN


Wayman:2001:FBA


Wayman:2002:BAT


Wayner:2002:DCI

REFERENCES

Wayner:2009:DCI


Way:2000:AC


Wu:2002:CSCa


Wu:2001:CDS


Weis:2001:SYH

Rüdiger Weis, Bastiaan Bakker, and Stefan Lucks. Security on your hand: Secure filesystems with a

**Weeks:2000:HPS**


**Wong:2001:EMA**


**Wu:2001:CKA**


**Wu:2003:HDW**


**Wu:2003:UFR**


Shyi-Tsong Wu and Bin-Chang Chieu. A user friendly remote authentication scheme with smart

**Wu:2004:EIW**


**Wu:2005:NDI**


**Wang:2005:SDR**


**Westerlund:2001:HWK**

REFERENCES


Weierud:2000:SFB


Weierud:2005:BSF


Weierud:2005:BPS

Frode Weierud. Bletchley Park’s Sturgeon, the fish that laid no eggs. Rutherford Journal, 1(??):??, ???. 2005–2006. CODEN ???. ISSN 1177-

Weiss:2004:JCE


Weierud:2000:SFB


Weng:2003:CHC


REFERENCES


Michael J. Wiener. Algorithm alley: High-speed cryptography with the RSA

**Williams:1999:QCQ**


**Wilcox:2001:SEH**


**Wilson:2001:PBA**


**Williams:2006:C**


**Winterbotham:2000:USI**


**Wincelberg:2001:JQH**


**Windley:2005:DI**

REFERENCES


REFERENCES


Wu:2004:RKA


Wang:2005:CHY


Wang:2007:NCD


Williams:2007:FTA


Wen:2006:PSA


Wen:2005:TRB

REFERENCES


[Wang:2003:CET]

[Wang:2005:SAI]

[Wu:2005:IAW]

[Wong:2004:RCK]

[WLZZ05]

[WMDR08]
Xiaomao Wu, Lizhuang Ma, Zhuoqun Dong, and Lionel Revéret. Robust watermarking motion data with DL-STDMD. *Computers
Watters:2008:VDL


Wheeler:1995:TTE


Watanabe:2002:CCD


Wang:2008:NAD


Wang:2009:RDA


Wolkerstorfer:2001:AIA


[WP03] Huaxiong Wang and Josef Pieprzyk. Shared generation of pseudo-random


REFERENCES


Walter:2005:DDP


Weimerskirch:2002:DLW


Wu:2001:DSM


Wu:2002:CSCb


Wuensche:2009:CAE


Wu:2000:PKC

Chuan-Kun Wu and Vijay Varadharajan. Public


[WW05] Stefan Wolf and J"{u}rg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In Shoup


[Wollinger:2000:HWH] Thomas J. Wollinger, Min Wang, Jorge Guajardo, and Christof Paar. How well are high-end DSPs...

**Wincelberg:2002:LIE**


**Wang:2008:HQS**


**Wang:2002:WEM**


**Wu:2005:CTR**


**Wyant:2002:APK**

Jeremy Wyant. Applicabil-

Wyler:2005:ANS


Wang:2005:CSA


Wang:2005:FCFa


Wang:2005:FCFb

Wang:2005:ECSa

Winslett:2005:PLD

Wang:2005:DIC

Xu:2001:EIE

Xu:2005:ETR

Xu:2001:CPW

Xiao:2003:HPC
REFERENCES


REFERENCES

Yang:2002:NEC


Yang:2005:TFN


Yan:2007:CAR


Yasuda:2008:DLP


Yuan-bo:2004:ITA


Yue:2001:GNN


Yue:2007:SEV


Yang:2008:NFD


Yang:2007:IIS


Yang:2006:PKC


Yekhanin:2007:LDC


Yan:2006:ICP


Youssef:2001:CIM

A. Youssef and G. Gong. Cryptanalysis of Imai and Matsumoto scheme B asymmetric cryptosystem. *Lecture Notes in Computer Sci-


Yi:2004:AKA


Yen:2000:CBO


Yen:2002:RSR


Yen:2003:RSC

REFERENCES

Yardi:2008:HAC


Yamamoto:2001:PKB


Yu:2001:TCB


Yi:2009:SSG


Yoo:2005:EHI


Yoo:2002:LAU

REFERENCES

Yourkewych:2005:CIR


Yue:2006:NCB


Young:2001:RP


Young:2001:CIR


Young:2004:HRV


Young:2006:MCC


REFERENCES

Yeh:2003:IAM


Yang:2001:EEA


Yoshiura:2001:AWB


Yao:2009:CAR


Yang:2004:ENT


Ytrehus:2006:CCI

[Ytr06] Øyvind Ytrehus, editor.
REFERENCES

Yang:2005:SEA

Yung:2002:ACC

Yang:2002:CI

Yang:2004:ISE
REFERENCES

Yang:2004:CUF


Yang:2005:CIA


Yang:2005:IYS


Yang:2006:SED


Yang:2008:VCS


Yang:2008:FSD


Yoon:2005: CZX


Yoon:2005: SWL


You:2001: GEC


Yen:2000: WOW


Ye:2001: ATD


Zhao:2005:SSV
Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. In ACM [ACM05a], pages 1–6. ISBN 1-59593-269-0. LCCN ????

Zhang:2000:MCA

Zhang:2004:AIB

Zhang:2005:CHC

Zhang:2009:CII

Zhang:2001:SOS

Zhou:2005:PSP
Yuan Zhou, ZhenFu Cao,

**REFERENCES**

Zhu:2004:DSM


Zunino:2005:WPE


Zhao:2006:SAP


Zeadally:2000:IPQ


Zhang:2005:CSS


Zhen:2004:IBS

Z. Zhen, B. Fei, and L. Kejun. The implementation of 128 bit strong encryption for SSL by using Java applet. Journal — Huazhong Uni-


Zhao:2006:NDN


Zheng:2001:ISS

Zheng:2002:NPK


Zheng:2002:ACA


Zhong:2006:ESC


Zirkind:2007:ADC


Erik Zenner, Matthias Krause, and Stefan Lucks.

Zhang:2004:SAE


Zhang:2004:AFV


Zhang:2004:RMA


Zhao:2005:MCE


Zhang:2001:QKD


Zhang:2002:CRD


REFERENCES


Zafeiriou:2005:BRW


Zhang:2005:ISS


Zhang:2005:SCA


Zhao:2002:EII


Zhu:2002:PAK


**[ZX04]**


**[Zhong:2008:GPT]**


**[Zhou:2003:ACN]**


**[Zhang:2005:ASP]**


**[Zhang:2005:ISM]**

Zhang:2008:FIC


Zeng:2001:CHR


Zhuang:2005:KAE


Zhu:2007:EIB