Title word cross-reference

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

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

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

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

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

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

[HSL+02]. $15.00 [Imm03]. 2

[Bih00, BGN05, CY02, CKL+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 [Eva09]. 2000 ± 10 [Man01]. 2^{28} [Bih02]. 2^x

[MFFT05]. 2^n [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

[Gr01, Pat03a]. (2, 128) [WB02]. 0 [AIK04].

ABC [PS04b]. d [BD00b]. E_0 [FL01a]. f_8

[KSHY01]. g^{2^x} [Shp02]. g_1(x, 1) [SZ02].

[WF02]. (2) [CP03]. GF(2^m) [OTIT01, RMPJ08].

[TF01]. GF(p^n) [BGK+03]. GF(q^m) [PZ01]. H_2 A

[CBB05]. k [BJL02, CT08b, GPC08, HKS00, QV05, W02]. l [QV05]. M + 1

[AS01a]. F_q [CY02]. Z_n [Gro05]. GF(2) [GS03, KTT07]. GF(2^n)

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

GF(2^n) [KKH03]. SL_2(F_{2^m}) [SGGB00]. μ

[LN04]. n

[CT08b, G06, HKS00, LKL01, TM01].
\[ N^{0.292} \text{ [BD00b]. } N_{C0}^{0} \text{ [AIK06]. } p \text{ [FL06]. } p^{q^*} \text{ [LKY00]. } p^* \text{ [CHH01]. } Q \text{ [Yas08]. } r \text{ [JY01], } w \text{ [DwWmW05, OT03b]. } x^n \text{ [Gon06]. } y \text{ [OS01]. } Z_n \text{ [LWL09]. }

-Adic [GHK06]. -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]. -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]. 1.82Gbit/sec [KV01]. 1.82Gbit/sec [KV01]. 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, RM04, Roy05, USE02b]. 12 [TPS01]. 128 [JY02, WFLY04]. 128-Bit [SM03b]. 12th [GH05, MS05b, PT06]. 13-15 [ACM05b]. 130 [LM08]. 14th [AMW07, AAC*01, Bir07]. 150-Kilometer [Das08]. 155 [LMP*01]. 15th [MJ04, BC01]. 160 [KSF00]. 16th [BS03]. 17th [IEE05b]. 186 [Nat00]. 186-2 [Nat00]. 18th [KM07]. 19005-1 [ISO04]. 192-bit [Luc00]. 1930s [Sei00a]. 1960s [Bur02]. 1962 [AJ08]. 1987 [Kha05]. 1993 [PPV96]. 1999 [Lee03b, Uni00a, Uni00b, Uni00f, Uni00c, Uni00e, Uni00d, Uni00g, Uni01]. 19th [BCDH09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH*00b, Eke02, Irw03, KO08, 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, RRS*09]. 2009 [ACM09, May09]. 20th [Bel00]. 21 [AJ01b]. 21264 [WB00]. 21st [Jef08, Ki01a]. 21th [IEE09a]. 22 [McC04, 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 [Ke05a, Ke05b]. 3.0 [Fl02b, Hei01, SQ01]. 305 [ECM00a]. 306 [ECM00b]. 30th [Coc02a]. 314pp [Duw03]. 3278 [BWBL02]. 33rd [ACM01a]. 36th [ACM04b]. 37th [ACM05c]. 39th [ACM07]. 3D [LZP*04]. 3GPP [KSY01, SM02]. 3rd
4 [Duw03]. 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 [BCJ+06, Wac05]. 5th [CV04, KJR05, LL03, LLT+04, Li05, NP02a, Syv02, WKP03].

64 [LKH+08, WWCW00]. 6th [Bla00, Des02, HA00, LL04d, MMV06, Oka00].

7 [And04, Gum04]. 7-round [PHA04].

8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800 [BG07a, Hir09]. 800-90 [BG07a, Hir09].

802.11b [SIR04]. 802.11b [SIR04].

802.11i [HSD+05]. 802.15.4 [Miš08].

9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04]. 90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1 [GM00b]. '98 [Wli99]. '99 [DN00b]. 9th [CCMR02, CSY09, DR02c, DKU05, Lai03, NH03, Patt03b, PY05, YDKM06].

= [KOMMO1].

A-1 [ISO05]. A.2.4 [Ko05a, Ko05b]. A5 [BD00a, BSW01, PS01c]. A5/1 [BD00a, BSW01, PS01c]. AAFG1 [Hug02]. AAIs [LOP04]. Aarhus [Cra05a]. Abadi [MW04]. Abelian [CF02, PHK+01, RS02]. Abstention [JLL02]. Abstract [CM00, Cou04, DIRR05, HLvA02, HJW10, JLO00, JS02, MP02, Mas04, Wag02, BN00, BCDM00, CD00a, CC04c, FKS+00, GHJV00, GT04, HT04, HP01, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Pei09, Yas08]. Abstracting [Bla01a, Mon03]. abstraction [BL06]. abstractions [BG07b]. Abstracts [Sch00b]. Accelerated [Elb08]. Accelerating [ESG+05]. acceleration [EHKH04]. Accelerator [CGBS01, RS04, TSO00, XB01, DPT+02]. Acceptance [CFRR02]. Access [ANRS01, An02a, BNPW03, CM02, DS06, HC08, MS03b, Ril02, Sma03a, Sun00a, ZGLX05, AW05, AW08, AFB05, BA06, BNP08, Che08b, DFMO4, Hos06b, HW03c, HY03, IY06, JW06, KNS05, LKZ+04, MF07, MSP+08, PY05, ST01d, WKP03].

Ad [BSS02, KH05, WT02, Cha05b, DHMR07, KVD07, LHC08, LKZ+04, PCSM07, SLP07, TV07, ZC09, MAaTA04]. 'ad-Durayhim’s [MAA04]. Ad-hoc [BSS02, WT02, DHMR07, ZC09]. Adaptation [ISSZ08]. Adaptations [ISSZ08].
Adaptive
CM00, CBB05, CTL04, CL08, Coc02a, CS02, CS03b, DSS01, EFY+05, FM01, 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, Sze08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DR05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sze06, WBRF00, Wri01, YW06.

Advances
Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS06, Lan00a, Lut02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Sze08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DR05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sze06, WBRF00, Wri01, YW06.

Agreement
AAFG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b.
agricultural [Lov01].

Aided [NS01b, HLL02].

Aimed [Pau02a].

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, CKY07, Fau09, HW03a, HWR09, Sho05b].

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, ChLYL09, CU01, CJ03a, CJ01, CTL01, CG03, CC06, CH07c, CM00, CT03, CP03, DR01, DG00, Dhe03, EYCP00, FW01, FMS01, GM01, HTS02, HM02c, HZSL05, JKK01, KBD03, KMM06, KY02c, KLB02, KTT07, KV01, LPZ06, MM01b, MM01c, MS02e, NMSK01, OS01, PZL09, PTB07, Ram01, RS01, SS01a, SPQ06, WHL05, Wes01, Wie00, AJ08, App05, BF06a, Bi09, CO09a, CH01, CKY05, CYH07, CHH01, FFP09, Fer06, FSGV01, GPX08, Jon08, KJ01, Kwo02, Kwo03b, LCP04, LLLZ06a, LLLZ06b, MN14, OS07, SH11, SCS05a, SM08, SZP02, TM01, WL02, WN95, Wue09, YRY05c, And03, SA02].

Algorithmic [Hro09, Jou09, Has01b].

Algorithms [Hro03].

Algorithms [AD07, Ano09d, AB09, BKLS02, II00, BWBL02, CPhX04, CLR01, Dan07, DWN01, FW09, Gau02, GL06b, Har06, Har00, Int00, JP03, Kel05a, Kel05b, Lee03b, LR07, LP02b, PB02, Pre02a, Pre02b, SL00, TLY04, TV03, WBRF00, WWP00, AKH03b, Ano01n, AH05, CKL09, CCM01, GHPT05, GPC08, HW03a, HWR09, HXG06, Hro05, JK01a, MCHN05, Pre07, Rhi03, TC05, XLMS06, ZLZ07, Zir07, dHO8].

Alien [Wil01b].

All-or-Nothing [Des00c, SR00].

Alley [DR01, Wie00].

Alliance [Ano04e].

Allied [Hau03, Hau06].

Allocation [CCM05, L309].

Allowing [JLL02].

Almost [AP09, BS00a, Jut01, Mar02b].

Alpha [WB00, Wu02].

Alpha1 [KHD01].

Altera [Ano02e].

Alternating [Wer02, HKPR05].

Alternative [Bad07, Gar03a, Han00, BMW02b].

always [BB79].

am [Eke02, SU07].

Amaifi [BC05c, CGP03].

Amenability [WW00].

America [DB04].

American [GL05, Kat05b, Alv00, Naf05].

Americans [WD01b].

among [BN00a, KT00, SKU00, Win05c].

Amongst [Pen01b].

Amplification [CHS05, LTW05, RK05, SV08b].

Amplified [KKS00a, KKS01, KML02].

Amplifier [Pli01].

Amsterdam [Knt02].

Analyses [BPR05, Des00a, Pau01].

Analysing [BL02].

Analysis [ARJ08, ABR01, AKS06, AD07, Ano01c, AIK01, ARC01, Ava03, BN00a, BDeKB09, BRS02, BF05, Bor01, BSL02, Cry00, CK02a, CS03b, DV01, Dra00, FL01a, FGM00a, Gir06, Gol01c, GHPT05, GLG02, GPR06, HS01, HK01, HSS04, Hey03, HM02c, IIT03, JK01a, JQY01, JT01a, JQY01, hKLS00, KMS02, LCK03, LKHAL9, Ly05, LW00, LH07, MOP06, Mar02b, Mas04, MS01, MM09, Mea01].
Mes00, Mes01, MAaTxx, MG08, NP02b, NSS02, OS06, ÒOP03, Puc03, QS01, SSST06, Sha01c, Sm03b, SDMN06, SQ01, SWT07, YSS+01, ZCO0, ZGLX05, AvdH00, AW05, AW08, Ab01, AH03b, As04b, BDSV08, BBK+03b, Bjo05, BG07a, BR05, BCJ+06, CKL+09, CW07, CS05a, DS09, DKS08, GW08, GM04, GTZ04, Has01b, Hir09, Hro05, Hut01, JE04, JPL04, JSW05, KSF00, Kor09, LKH+08, LMW05, LKJ01, Lu07, Mea04, MT07, MRST06, OS00, PSG+09, PS08b, SK01b, WLT05a, WPP05, XMST07, YCV+08, YC08, ZWWL01, ZL04c, ZDW06.

Analytic [LW05a, LKJL01, Lu07, Mea04, MT07, MRST06, OS00, PSG+09, PS08b, SK01b, WLT05a, WPP05, XMST07, YCV+08, YC08, ZWWL01, ZL04c, ZDW06].

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

Anchor [Ree01].

Ancient [Imr03, Sin00, Mol05, Pin06].

Andrei [Puz04].

Andrew [Puz04].

Anguilla [Fra01].

Anniversary [Sal01b, Coc02a].

annotated [Pet08].

annoyances [Tyn05].

anoymy [GM03].

Applability [Wya02, TM01].

Application

Application-Aware [IKP+07].

Applications [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, Bi05a, BG04a, CD00a, CV02, CGH01, CZ05, CHSS02, CSY09, Cra05a, CD00a, CI05, DJ01, DK02, DK07, DA03, DFPS06, FR02, GSS08, GKH+09, GJKR03, Gen04a, GRW06, Gol01a, Gol04, HRS02, HN06, Has01a, HSS04, HR05, HJW05, JT01b, KY01, KMM+06, KGL04, KMO01, KBM09, KKIM01, Km02, MAA07, MM07b, Noc02, Noc04, PS02b, RSN+01, Sch06b, Shp03, SXY01, SPG06, Vau02, Wya02, XYL09, YZ00, Zsc00, Zho02, ÁCTZ05, Ate04, AH05, AFGH06, BG08, BGL+03, CCCI01, CM05b, CS09, CSG+08, DY09a, DFCE00, DJL01, FP09, Fin03, Fis01a, Gal02, GVC+08, GKK+07, GB09, HHS01, Has02, Hen01, HKPR05, Jac00, KVN+09, KNS05, Lai00, Lee04a].

applications [LJ05a, LPW06, LB05, MY01, Mal06, MC04, MSV04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SSS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPHH06, WW08.
Asymptotically \cite{vDW04}. Asynchronous \cite{CKPS01, FML+03, KSR02, SKR02, ZSV05}.

at-targama \cite{MAt05}. Atlanta \cite{IEEE09b}.

ATM \cite{Pat02a, Pat02b, Zea00}. Atomic \cite{CV06}. Attached \cite{RCBL00}.

Attacks \cite{Ric07}. Attack-Resistant \cite{LNL+08}.

Attackers \cite{JMV02}. Attacking \cite{FMP03, KPR03, Luc00, TMMM05, BF06a}.

Attacking-Based \cite{TMMM05}. Attacks \cite{ARR03, AG01, AK03, BC05a, BPR00, BP02, BMM00, BBB+02, BDK+09, BU02, BM03b, BGM09, BCP02b, BM01c, Can06b, CS07b, CZ03, CT08a, CS01, CKM00, CJNP00, CM03, Cou03, CWR09, CD01b, DPV01, DFS04, DJ06, DS08, DM07b, FKSW00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GKI02, HSH+08a, HNZ02, HR04a, HSH+01, HLC08, ISW03, JKS02, JG00d, KKS00a, KS00b, KKS01, KCI+01, KL01a, Law09a, LLS05a, LWS05, LJ05b, MOP06, MP06, MF01, MeK04, Mes00, Mes01, M03b, MG09, OT03a, OT03b, OOP03, OST05, OVE06, PKBD01, PDMS09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZ05, YYD001, YY01, YG01b, vW01, BPS08, Bau05, BCS08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05b, HL05b, Ino05, IM06, JDJ01]. attacks \cite{KS05a, KTC03, LPV+09, LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RG05, Scho0c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07a, WL04b, Yau07, YS02, ZSJN07}.

Attributes \cite{FD00, CF05}. attractors \cite{HHYW07}.

Attribute \cite{LY05, RSA00e, IY05}. Attributes \cite{SS01b}.

Audience \cite{AS01a, Ano01a}. auctioning \cite{RCG+05}.

Auctions \cite{Bra01b}.

Audio \cite{Arn01, CS05c, DRL09, MH05, WNY09, WWL+02, XFZ01, WQ08, BS01b, KJR05, KN03}.

Audio- \cite{KJR05}.

Audio-and \cite{BS01b, KN03}.

Augmented \cite{CS07c, Yau01}. Augmenting \cite{AL04}.

August \cite{AMW07, Be100, B+02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KKP02, Ki01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch05a, Sch05b, ST01d, USE00a, USE00b, USE01c, USE02b, VV01, Yun02a}. Australia \cite{Boy01, IZ00}.

Austria \cite{DKU05, P601, Jef08}.

Authenticate \cite{Bau03a, Bau03b}, Authentic \cite{Bau03a, Bau03b}.

Authenticated \cite{AGT01, Chi08a, CGV09, Fur05, JW05, PM08, RCBL00, YS+01, Lin01b}.
Authentication
[AAK09, AP09, ANRS01, Ano01b, Ano01c, Ano01f, Ano02d, AHKM02, ANL01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, BKR00, BCC01, BCC02, BC05b, BDKB09, BR02, BDFP05, BDF01b, BM03c, BL02, BLDT09, BWE+00, CV03, CGP08, CS07b, CC01b, CLK01a, CLK01b, CC05b, CC09, CJT02, CJF04, CW05, CT09, Cim02, Cir01, CFRR02, CGK+02, CF05, CJK+04, Cen01, CMF+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, FDR00, Gan01a, Gar03a, GMW05, GSV02, GD02, GT02, Gutt04c, Had00, HZI01, HSHI02, HSHI06, HKW06, HY01, Hae01, HS01b, HP00, Hl07, ISSZ08, Jab01, JI02a, JI07, JI02b, KJ05, KC09b, KH05, KVD07, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LLT+04, LB04, LL05c, LSH03b, LM00, LOP04, LHL+08, Lys07, MW06, MM01a, Mal02].

authorisation
[MI04, MD04, MR03, MGC02, MNT06, Nao02, Nik02a, Nik02b, OKE02, OHS08a, PBD00, Par04, PMR00, PBC05, PK01, Qu01, RKK02, Ric07, Ril02, SNWX01, SR01, Sch04c, Sch05b, Sei00b, SY01b, SBG02, Smi00, Smi01c, Smi02, SE09, SK06, Str01b, SJ05, SYL05c, SC01, TK03, TGT09a, TGT09b, Tsa01, VN04, WLL09, WCJ09, Way01, Way02a, Wao06, WKB08, WT02, WS03, WL07b, WLT05b, WHL05, XYL09, Y101, YEP+06, YSR01, YLL02, YKW01, ZaF00, ZJ04, ZBLv05, AvdH00, AF04a, All06, Ano00k, Ano00l, Ano05b, Art04, AAK09, Asl04a, Asl04b, AL04, Ayo06, Bado07, Bel04, BGP02, BSSM+07, BFG04, BF05, BS01b, BBG+02, BDFP02, BM07, Cer04a, CBB05, CC01a, CCK04a, CL04d, CC04b, CCK05c, C203, CY05, C5S08, CWJT01, CJF01, CJ30b, CH07a, Ch08b, Ch08c].

Automaticity
[AB01, Bla02a, CBD+05, GJ03, GOR02b, HG03, RW03b, Sch01a, Mit02a].

AUTHMAC_DH
[Asl04b].

Auto-recoverable
[YY00].

AUTHORSHIP [Top02].

Auto-recoverable [YY00].

Automata
[LZ04, MGC02, Wue09, Bao04, CC05d, KK03, La00, LQ08, Mon03, SBZ04, SHH07, GLC+04, GTY08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Her09b, Hsu05b, HL0709, HYS03, HLL04, HLL05b, shC09, JF06, JPL04, KLY03, KJ05, KN03, KT03, KCL03, Ku04, KC05, KCCC05, LC03, LHY02, LLL03a, LF03, LKY04, LW04, LHL04a, LKY05a, LL06, LLL+09, LFT07, L05, LST+05, LC08, LWH05, LW06, LFW04, LHL03b, LH03, LT04, LC04a, Lin07, LN04, LLL08a, LLL08b, LC05a, LC05b, LK01, MS09c, MAI06, McK04, Mit00, MR00, ME08b, MP07, N09, NLD08, OHB08b, PY08, PCS03, PCC03, PI06, Pei04, Pha06, Pot03, Pot07, RF07a, RF07b, RF07c, RG06, SN01, SG07, SN07, Scho05c, Scho04, Sei05, SBS09, Sha05c, SLH03, SSM+08, SW06, Shi05, SL05a, St.00, Ste05a, SW02].

AUTHentication [SCS05b, SC05c, SCS05c, SCS05c, SCS05c, SCS05e, SCS05f, SY06, TM06, TB02, TE000, TIS07, TW07, Ts08, TW10, UBE09, VM03, Vok05, Wac05, WLT03, Wan04a, WLT05a, WL0N09, WDC09, WC03b, WL04b, WH0708, XwWL08, YW04b, YW04a, YW05, YW05, YTWY05, YCYW07, YWWD08, YC09c, YC09b, YS04, YR04, YRY05a, YRY05c, YRY05d, YYY05b, YbJf04, ZL04a, ZK05, ZSN05, Zha06, ZDW06, ZSN07, dB07, CS08b, ECM00a, ECM00b, LSH03a].

AUTHMAC_DH
[Asl04b].

Author
[An00b, An01d].

authuerisation
[SN07].

Authorizes
[CHS02, HWW04, WH02b].

Authority
[Con00, JLL02, CCH05, KB09].

Authentication
[BACS02, CJK+04, LSZ05, RKK02, YT09, GJJ05, JEL04, Lin07, LOP04, SR01, WL04a, WZB05, YBJ04].

Authorship
[Top02].

auto [YY00].

auto-recoverable
[YY00].

authenticator
[CKY07, jLC07].

Authenticity
[AB01, Bla02a, CBD+05, GJ03, GOR02b, HG03, RW03b, Sch01a, Mit02a].

Auto-recoverable
[YY00].
TC00, dRMS05. automate [Bur02].
Automated [CDR01, LLW05, LLW09, HJW05, IY05, LS05b]. Automatic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05].
Automating [Gue09]. automorphism [Pae03]. automotive [LPW06]. Autonomic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05].
Average [KMT01, CGHG06]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average-case [Mic02b].
Avoid [Tyn05]. Avoided [CNPQ03]. Award [RSA03a, Bar00b, Coc03]. Awarded [Coc02b]. Aware [IKP+07, OHB08a, CBSU06, OHB08b, Zea00]. Awareness [HLM03, BK05]. Away [Coc03, Ols00, Tee06]. Awkward [TvdKB+01].
Banach [AUV01]. Bandwidth [CGJ+02, YY01a, SLP07]. bandwidth-efficient [SLP07].
Bandwidth-Optimal [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Bel00, Bon03, Fra04, Kil01a, Men07, Sho05a, Yun02a]. Barcode [Che08b]. Bare [DPV04].
Barpen [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, XSWC10, IR02].
Based [Ano01c, ANR01, AF03, AJO08, BDG+01, BKLS02, BNPS02, BN02, Ben00, BR02, BF01b, BF03, BB04, Bon07, BCHK07, BGH07, BPR+08, BD03, BMN01, Boy03, BQR01, BM01c, BSNO00, BRTM09, CGFSHG09, ČvTMH01, CK02a, CGMM02, CF01b, CC02a, CV03, CPP04, CCD07, CS07b, CC01b, CLT07, CHSS02, CHM+02, CKZ05, CM05a, CTH08, CGK+02, Coc01b, Cou01, CFS01, CS00, DN00a, DMR+05, DT03, EHK+03, EM03, FL06, FM02a, FMY01, FGL02, GMP01a, GMP01b, Gar03a, Gen06b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HLO2, HQ05, HCO8, HH09, Ig02, Jam00, KBD03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05a, Kel05b, KY01c, KY02b, KC09b, KJ02, KC02, KCD07, KPR03, KM05, Kra02a, Ku02, KWP06, KT00, LLO2, LP03].
Based [LKLK05, LHT09, LZ01, LZ04, LL05c, LP06, LY07, LXH07, LRRW07, LWK00, LSC03, LHS05, LS05b, LCD07, MPS00, Mar08a, Mar08b, MN01, Mi01, MGC02, Mi01a, MSU05, NM05, Nak01, Nam02, NB01, NS02, Nov01, NMS01, PV06a, PV06b, PV06a, PZL09, PMRZ00, Ri02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sa05b, Sch01a, SSFC09, Sha02, Sha01c, SO01a, SX01, Sma03a, BSEW01, SGB01, TMM05, TYL02, TGT09a, TZT09b, VMSV05, Vau05b, Ver06a, VHP01, VK07, WR02, WY02, WZ05, WG05, WC09, WH09, WB01, WC04, XYL09, YKMY01, YT09, YDY00, YSS+01, YK01, YL05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWC02, vD04, AAPP07, AA08, Ano02b, Ano05b, App05, AAKD09, BGB09, BBC+09, BR04, BFG08, BS01b, Bla01b, BM05, BLP06, BLS09b, Buh06, CGHG06, CG06, CL02b].
Based [CO09a, CL04d, CFY+10, CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CI06, CLK04, CJL05, Cho08b, CYH+07, CFVZ06, CCD+04, CTT07, CHT02, CC04c, Cra05b, DS09, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EHK04, FL02, FXAM04, FW08, GMR08, GW08, GSK09, GL06a,
GHdGSS00, GS01, GPS05, GGS+09, GB09, HM00, HLL+02, HCD08a, HCD08b, HRL09, Has00, Her07, Her09b, HPS01, HG05a, Hsu05a, HlwWZ09, Hüh02, HP01, HLL03, HL05d, sHCP09, IM06, JK01a, JK01b, JMV09, JW06, JPL04, JZCW05, JZ01, KG09, hLSS00, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KCL03, KtU04, KK05, Kwo03a, KHKL05, LHL03a, LF03, LL04b, LKY05a, LKY05b, LHY05, jLC07, LG09, LD01, LTH05, LPM05, LlW05a, LWH05, LYGL07, LLW08a, LLW08b, LCC05, LSA+07, LCZ05c, LCZ05a, LLC06a, LLC06b, MW06, MS09c, Mic01].

Based [MR09, MI09, Mit00, MB08, MC04, MPPM09, MV03b, NZCG05, NC09, NSNK05, OS09, PCSM07, PW05, PBMB01, PSG+09, PS08a, Pe06, PSP+08, PC00, Pha06, PLJ05a, PLJ05b, QC05, Reg03, Reg04, RG09, RG+05, Sae02, SG07, SCo04, Si05, SH11, SM11, SCo04, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SLH03, SCS05a, mSgtL05, SSM+08, SW05a, SH00, SK01b, SCL05, SLC05, Sun02, SC05c, SY06, TNG04, TWNA08, Ts08a, Ts08b, UHA+09, UEP09, VS01, VKS09, WAF00, WLT03, WLO7a, WIP07, WNQ08, WlHH05, Wh109, Wv00, WH02b, WY05, W05c, XMST07, YW04a, YCW+08, YWWD08, YC09b, YS04, hY08, YJ00, YPS01, YRY05c, YPKL08, YY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRMS05, N005]. 

Bases [AAC+01, ADDS06, BKP09, B+02, CvTMH01, EBC+00, FJ03, Fla+03, CCT08, Fau09, ZT03]. 

Basic [Go01b, Go01a, Go04, Kat05b, Puc03, Ste02, Bon00]. 

Basics [Leh06, Lut02]. 

Basing [BPR+08, CHL02, AGG06, AGGM10]. 

Basis [RMH03b, Vav03, vW01, GPS05, LS05b, RMH03a]. 

Batch [Ara02, HLHT01, PBD07, Sha01d, BLH06, HLH00]. 

Batching [SB01]. 

Battery [CBSU06]. 

Battle [Bud00a, Bud02, SM00c, SM05, SM07a]. 

battles [Cal00d]. 

Bay [Cal00c]. 

Bayes [Goo00]. 

BB84 [Ina02a]. 

BC [IEE02]. 

BCH [MLC01]. 

BDD [KLN+06, Kra02a]. 

BDD-Based [Kra02a]. 

Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01]. 

Beach [IEE00a]. 

because [AJ08]. 

Become [Ort00, Wal04]. 

 Been [Nic01]. 

Belief [ASW+01]. 

Belief [BPST02]. 

believing [Buh06]. 

Bell [BZ02, Eke02]. 

Benchmark [Ase02, TLY04, LDH06, YLT06]. 

Bendy [Sas07]. 

Benefit [YKL+02a]. 

benefits [CH00]. 

Benford [NM09]. 

Bennett [BGM09]. 

Bergen [Ytr06]. 

Bermuda [Bla03]. 

Bernard [DNRS03]. 

Berners [Coc02b]. 

Berners-Lee [Coc02b]. 

Best [Bau01a, Bau01b, MFS+09, Go08, Ste02]. 

Better [NV03, PM00, RR02, SK01, HLL03, Pau03, Rie00]. 

BetterBASIC [ASW+01]. 

Between [DKMR05, Ket06, Ngu05, NN06, Fau09, GKM+00, GC05, MSV04, Pau01, RWV03a, Sch02, Sch04d, SK06]. 

Beurling [Bec02]. 

Beyond [Gor06, Hei03, LMW05, Mar08a, Sch03, See04, Sty04]. 

BGP [ZSN05, vOWK07]. 

Bay [Con04, PJK01]. 

Bi-directional [PJ01]. 

Bi-linear [Con04]. 

Bias [CL02c, Sel00]. 

Biased [BS00a, LSK05]. 

BiBa [RR03a]. 

Bibliography [Bes05]. 

Bidiagonal [BR09]. 

Bidiagonal-Singular [BR09]. 

big [RR03a]. 

BigNum [SR06]. 

Bilateral [CT08a]. 

Bilinear [BGLS03, BW03, CR04, HMG04, KK02, DSGP06, LC05b, VK08]. 

Bill [Gen00a]. 

billing [SSM+08]. 

Binarization
Binary [ADI09, HHM01, LSKC05, OSSST04, SKG09, WCJ09, ÁCTZ05, BG08, BG09, FSGV01, GB09].
Binary-Ternary [ADI09].
BIND [Kle07].
Binding [DN02b].
BioAW [MJ04].
Biometric [AHKM02, Dal01, EM03, HWH01, KJR05, Li05, LST+04, PMRZ00, PK01, BS01b, Gu06, JP06, KN03, Li05, LST+05, MR00, RFR07a, RFR07b, RFR07c, Smi00, MJ04, TB02, Z04].
Biometric-Based [PMRZ00].
Biometrics [Ano04a, Ash03, Bjo05, MR03, Ril02, Str01a, BSSM+07, BCP+03, Buh06].
Biometrics-Based [Ril02].
Biomolecular [Bi09].
Birds [MLM03].
birth [Bud06, SE01].
Birthday [Wag02].
Bisimulation [BJP02].
Bit [AIK+01, BK06a, BL08, CGHG01, CDL+00, DMS00, GS07a, IIT03, KZ07, LNS02, MS09d, PCG01, RM03, Ril02, SM03b, SX01, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, PLs01, Pri00, RMP08, SWR05, UHA+09, WW08, ZFK04].
Bit-Fixing [KZ07, KZ03].
bit-substitution [GPX08].
BitLocker [Kor09].
Bits [BS01d, SZ01, HN04, Slp02].
Bitslice [DPV01].
Black [Ano01j, CF02, CFS05, DI05, DIRR05, DS08, KY01d].
Black-Box [Ano01j, CRS02, CF02, CFS05, DI05, DIRR05, KY01d].
Blackmailing [GPX08].
Bletchley
[Sal00b, Cop05, Cop06, Cop10, HS01a, Sal05a, SE01, Smi01b, Wei06, We00].
Blind [AO00, BNPS02, BB00a, BSC01a, CL01b, GS09, JKK+01, KY01d, Naf05, Pa02, SPK08, ZTP05, ZK02, Fan03, H04a, JLL01, JL04, LHY05, L005, MS09a, SV08a, SHT05, WH05, ZC05].
blindness [AvdH00].
Blink [Sas07].
Block [AIK+01, BBC+09, BK00, BRS02, BR02, BSC01a, CVTH01, Can01b, CLLL00, CP02, CMB+05, Cro01, DR00a, Dwo03, EYCP00, Fhu02a, HSH+01, JKK+01, KCP01, KYHC01, KKG03, LLRW07, LRW02, MV00, MS02e, NPV01, OMS01, Pat01, PS06, Pi01, RMS05, SM03b, SY+02, SKU+00, SK01, WCJ09, XH03, YG01b, Bai08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kat05a, KJ01, LDH06, LCP04, LSH+08, MMJ05, PAB+08, RBB03, SHJR04, SHH07, WF02, XH05, YI00].
Block-Based [LLRW07, BBC+09].
Block-Cipher [BR02, RBB03].
Block-Cipher-Based [Ril02].
Block-DCT [BSC01a].
Blockcipher [GM02c, OS07].
blockciphers [Fur01].
Blocks [Joo02].
Blockwise [JMV02].
Blockwise-Adaptive [JMV02].
Bluetooth [GBM02, LV04, LMV05].
Blunders [Bur01].
Blurr [VHP01].
Blurring [LSKC05, SK06].
Board [CGBS01].
boat [DB04].
Body [Bam02, TG07].
BOEL [Fin02].
Boethius [Eag05].
bombe [Wil01a, Tur04].
Bombes [Ano01j, LBA00].
bombs [L0v01].
Bonds [CAG03].
Boney [AKS05, Hes04a].
Boon [DRS05].
Book [And04, Duw03, E0g05, E0a09, F0u07, F0or4, Gas01, Gum01, Imr03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Re01, Rot07, Sal03b, See04, Slp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wal00, Was08a, Kat05b, Lam07, Lun09, MAaT05, Ros00b, Sin99, Sin00, AAG+00].
Books [Che00b, Dr.00c, Ros00b, Ree01].
Bookshelf [Lut02, Lut03, Wil01b].
Bookworm [Sal03a].
Boolean [Car02, CT03, CS09, MS02b, QPV05, SM00a, SM00b, SM03a, WV00].
Boom [Ano04a].
Boomerang [KKS00a, KKS01, KML+02].
Boot [HSH+08a, HSH+08b, HSH+09].
Border [MJF07].
Borders [PGT07].
Boston [USE01b].
bot [Ano08b].
Botschaften [Sch09].
bottleneck [WL02].
bottlenecks [HTW07].
Bound [CY08, DGN03, KMT01, HLLL03, HY08, GW00].
Boundaries [PGT07]. Bounded [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vado3, DFSS05]. Bounded-Quantum-Storage [DFSS08]. Bounding [DM07b]. Bounds [BDF01b, BP03b, DIRR05, Di01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKK03, JZ09, KS05b, PSS02a, 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]. Branch [BDF01b, BP03b, DIRR05, Di01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GKK03, JZ09, KS05b, PSS02a, Shp99]. Branches [Fel06]. Brassard [BGM09]. Break [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breaker [CD00b]. Breaking [Ano09a, BKN04, Das08, DKFX05, GO03, Gk02, Kev01, KR03, Kt0h08, Sl00a, Wro05, Fie09, Gar01, Sfm01b, SL07, Swo08]. Breaks [OS00]. Breakthrough [Coc02a, LR01, Pa02, Pau02a]. Brief [Bon07, Cos03, Kir01a, Boo05, Gra01]. Briefs [MP00, PM00a, Pa02, Pa02b, Pau03, Pau09a]. Bright [Ano01j, LN05]. brings [Ano04e]. Bristol [DFCW00]. Britain [Gu06]. British [ACM08, Fie09, Foa01, Svy02, Bud00b]. Broadband [MP00, SLL07, MJF08]. Broadcast [AF106, BGW05, CKPS01, CNV06, Ds03, FWW04, GSW00, GKK07, GRW06, HS02a, HLL05, LN02, SNWX01, Woo00, ASW00, KSW06, Kre05, Mar05b, NLD08, RGG0, WDLN09, LN04]. Broadcasting [TJ01b, WH02b]. Broke [Urb01, KS04]. Broken [Ahn08]. Brooks [Bar00b]. BRSIM [BPS08]. BRSIM/UC [BPS08]. BRSIM/UC-soundness [BPS08]. Bruce [Helt03, Sty04, See04]. Bruges [Pre00]. Brunley [ASK05]. Brute [Cur05, SGA07]. Brutus [CJM00]. BSD [Lin02, ASW0+01, Lin02]. BSDCon [USE02a]. Bubble [Ber03, Buchmann [Lee03a]]. Buffer [FOBH05, Fry00, Ino05]. Bug [BCS08, Bor00]. bugs [GJL06]. Building [Jou02, Knu07, Mar02a, And08b, Bra01a, FB01, LS05b, MC06, MPPD06, PQ06, DB04]. buitenlands [DL00]. Bulletin [Cer04b]. Bulletproof [Cha05b]. bundles [GT02]. Burros [ABM08]. Burying [Arn01]. Bush [Ris06]. business [HHS01, Poh01]. Buy [PLW07]. Buyer [MM01a]. buys [Zaf00]. Buzzes [Coc02b]. Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGR07, LLR02, LLR06, PL06]. Byzantine-Resistant [CNV06].
Chaining [BKR00, CBB05, PCC03].
challenge [LM08, LW05a, PRS04, Smi08].
challenge/response [LW05a]. Challenges [LM08, LW05a, PRS04, Smi08].
Change [CWJT01, ZC05]. changes [CYH05].
Changes [Mur01]. Changing [BST03].
Channel [BU02, CHVV03, Law09a, LCK03, Moli02, NM005, OT03a, OT03b, Sch06a, SYL05, ARG03, BG07b, Buhl06, CNPQ03, KSHW00, LCZ05b, MS09c, PSP+08, WL07a, YTW05]. Channels [AIP01, CWJT01, ZC05].
Chaos [JK01b, SK01b, LMC+03, McN03, PSG+09]. Chaos-Based [WZW05, SK01b, LMC+03, McN03, PSG+09]. Chaotic [BCGH11, LLL+01, Mul06, SXY01, US002, Vav03, AMRP00, AMRP04, GHdGSS00, GB09, HHY07, HLwWZ09, JKK01b, LMC+03, LYGL07, MA02, PBM100, PS01a, PZL09, SPG02, SL09, UHA+09, VKS09, WG02, WW08, kWPgLW01, WLW04, YZEE09].
Character [KA05, Was08a]. characteristics [RFR07a, RFR07b, RFR07c]. Characterization [AJ008, Nam02, XH03, BGM04, KY00, PV005, XLM05].
Characterizations [Pas05]. Characterizing [BTW05, BTW08]. Changing [BAC02, RH02]. Chatter [Kee05].
Chaum [BN005, KLN+06, WH005]. Chaumian [Mlo03a]. 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, SGPH05]. Cheju [Kim01].
Chemical [EIG01]. Chen [LW05c].
Chennai [CV04, RD01, Roy05]. Chernobyl [Rie03]. CHES [JQ04, KKP02, KP01, KNP01, RS05, WKP03]. CHESS [LKH09].
CHESS-64 [LKH09]. Cheswick [Che05b].
Chicago [ACM04b, Top02, Con00]. Chien [YRY05b]. Children [Pau02a, Sye00].
China [B+02, DWML05, FLY06, JYZ04, LYT+04, LYT+05, ZY04, ZYH03, Ano00c, TZZT01].
Chinese [LYT+04, LYT+05, Sch01b, CAC06, YKLM03].
Chip [Ade09, BNPW03, DV08, MM01b, MM01c, MP00, Mt02b, Fox00, IST08, Ano04c]. Chip-Secured [BNPW03]. Chipkarten [Ano04c]. Chips [Ano00d, GP00, Pau02b].
Choice [JZ00]. Choquet [SH11, SM11].
Chosen [BCK07, CKN03, CHJ+01].
Chosen-Ciphertext [BCHK07, CKN03, CHJ+01a, CHJ+01b, CS02, CS03b, DNO02a, Des00b, Dk05, FP01, IM06, JK02, JNO03, KS00a, KY01a, KCJ+01, KMD03, KM01c, KL01a, Man01, Nov01, PV06b, Poo00, Sho00b, BMU05, CHH+09, KG09, ZCW04].
Chosen-Plaintext [BCHK07, CKN03, CHJ+01a, CHJ+01b, CS02, CS03b, DNO02a, Des00b, Dk05, FP01, JK02, JNO03, KCJ+01, KMD03, Nov01, PV06b, Poo00, CHH+09, KG09].

15
Oni01, PP06a, Pl01, RMS05, Sar02, SM03b, SKU++00, Wal00, Wri05, ??02, YG01b, ZC00, Baj08, Bar06a, Bel07a, Ber07, Bod99, DLP++09, DY01, D09, Dun06, DK08, Egh00, GPG06, HW03a, HWR09, Hey03, JK01b, Jun05, Kat05a, KSWH00, Kin01, LMSV07, LDH06, Lun09, Max06, M09, MRT10, MWM01, Pin06, SJJR04, SK03, Smi01b, SL07, SB05, TT00, Wag03, YI00, You06, Kat05b.

Ciphertext [BBK03a, BCHK07, K03, CS02, CS03b, Des00b, DK05, FP01, JKS02, J00b, KS00a, KY01a, K01, KMZ03, Kur01, Man01, Nov01, PV06b, Sho00b,BMW05, CHH++09, IM06, KG09, Poi00].

Ciphertext-Only [BBK03a, BCHK07, K03, CS02, CS03b, Des00b, DK05, FP01, JKS02, J00b, KS00a, KY01a, K01, KMZ03, Kur01, Man01, Nov01, PV06b, Sho00b,BMW05, CHH++09, IM06, KG09, Poi00].

Ciphertexts [AFI06, BGW05, BGN05, Gen04b, JJ00a].

Circuit [EHK++03, GSS08, HR05, MG08, KS05b].

Circuits [BI05a, FML++03, Gol03, ISW03, MD05, PBTW07, You01, GLC++04].

Circumvention [Kha05].

Cirencester [Hon01, Pat03b, Sma05].

CIRM [PPV96].

CISC [FLY06].

Citizen [Mit02b].

citizens [Ano03a].

claims [DS00].

clamping [Ano03a].

Clandestine [Wri05].

Class [Car02, KM01a, KKH03, NN06, OP01a, Pl01, SB02, XXYX11, DLK00b, Fox00, HM00, Uni01].

Classes [CY02, RSA00c].

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

Classification [HMS04, PBD00, Uni01].

Clauses [SV08a].

cle [RSA09a].

Cleaner [TR09a, TR09b].

Cleaning [Lut03].

cleanup [Lau08b, PWGP03].

clo [RSA09a].

Clouds [GS01, VS01].

Cluster [Hö01, KCD07, SEF++06, TLC06, TW07].

Cluster-Based [KCD07].

Clusters [MFS++09].

CM [CMKT00, GHK++06].

CMS [BWBL02, DUK05].

Co [Bud00b, Nd05, ACM01b].

Co-Design [Nd05].

Co-operation [Bud00b].

Coalition [ACJT00].

Coalition-Resistant [ACJT00].

coarse [Rhi03].

Coast [Boy01].

Cod [IEE05b].

Code [Ark05, BKR00, BR04, CD00b, CV03, Cer04b, FIP02a, FF01b, HSZI01, Imr03, KY01e, Lai08, OS09, Ree01, Rey01, Sal00a, Sin02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MMJ05, Msp02, Ros00b, RSA09a, SM00c, SM05, SM07a, Sn09, Sn00, Swe08, AAG++00, SE01].

Code-based [BR04, OS09, BGB09].

Codebook [CTH08, YWWS09, WJP07].

Codebook-linked [YWWS09].

Codebreaker [Hau03, Pin06].

Codebreakers [Bec02, Gan01b, Gas01, HS01a, Kahl75, Kahl76, Kahl77, Kahl96].

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

Codebuster [Ano04d].

codec [Che08a].

Codes [LLR07].

Coded [MLC01].

Codes [Bec05, BP06, Big08, Bod99, BQR01, CC09, Chu02, CDG++05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ??02, YD001, Yek07, Bel07a, aSM01, Bul09, DB04, DLK00b, DW05, DW01, Gar01, HW03a, HWR09, Kov01, Lam07, Lun09, Min03, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02].

codeword [AJ08].

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

Coefficients [CH01b, KT00].

coffin [Rie03].

Cohen [Was08a].

Coherent [TPPM07].
Coin [Lin01c]. Coin-Tossing [Lin01c]. Coins [HR04b]. Cold [SH08a, AJ08, SH08b, SH09]. Cold-boot [SH08b, SH09]. collaboration [ED03, PCSM07, SBG05, SBG07]. collaborative [LLY06]. collapse [ED03, PCSM07, SBG05, SBG07]. collapse [LLY06]. Collapse [GMM08, Bro05a]. Collaborations [Kuh00]. Collective [BBB02, BGM09]. Collision [DG02, IK005, MS09c, WYY05a, WYY05d, GM00a, Sem00]. Collision-Resistant [IK005]. Collisions [BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c]. Collisional [IK005]. Collusion [BGW05, HNZI02, Zan01]. Cologne [WKP03]. Color [CTL04, Che07a, Che08a, CTY09, FGD01, AEEdR05, CO09a, CDD07, Yan02, YCL07]. Colorado [BC01, Sch04b, USE00d]. Colored [CDD07]. Colossus [Cop04a, Cop05, Cop06, Cop10, Lav06, Sal00b, Sal00a, Sal05a, Salxx]. Colour [RS00]. Coloured [AADK05]. Commonwealth [PY05]. Comment [SCS05b, WY05, WLW04]. Comments [AS01c, CGH00b, JW01, MNFG02, SKW00, CTT04]. Comment [AS01c, CGH00b, JW01, MNFG02, SKW00, CTT04]. Commentary [DN00a, Nie02b]. commodity [CGL08a, CGL08b, CGL08c]. Common [Pas03, TG07]. Commonwealth [PY05]. communicating [Hut01]. Communication [AK02a, ANRS01, BYJK08, BK03a, BIW08, Big08, Coll03, Fis05, GKK09, LLS09, Mar07, NA07, PL01, Sch06b, SKR02, Wri05, vDW04, BYJK04, BC05c, CC05c, CGP03, EY09, GKK07, GGG05b, GC05, HYS03, JZ09, JRS09, KPS02, LPM05, Lin02, MP08, Mul06, PBMB01, Par04, RH03, SNW01, UP05, WWA01]. Communication-Efficient [Fis05, LLS09]. Communications [BCC02, GN06, HJ07, Igl02, Kra01, Lin00a, Lan04b, LCK01, LL01, MS05b, Sal01b, Vau05b, VM02b, BP03a, CY04, HWW02, LC04a, Sal05c, Ser06, SL05a, Wil99, WGL00, YT05, DNU05]. Community [SK06]. commutativity [MRS00]. commuting [CKRT08]. Compact [CG03, JT01b, SMTM01, YT09, ZKL02, JAW00, Mic02a]. companies [Ros04, Ste00]. Company [ASW01, Zaf00]. Comparative [DPR01, GLG02, Kat05b, LFF07, LOP04]. Comparing [HU05, KLN06]. Comparison [GC00a, GC01a, Gau02, JRB06, MS02e, SW00a, WW00, FGM03, JL03, Sma01, WB00]. Compendium [Lut02]. Compensated [AAK09]. competition [Clao0b]. compiler [DFG00, Oiw09]. Compilers [Lut02]. complement [YC09c]. Complementary [AS01c]. Complete [Bar00a, Bee05, Bud00a, FGM001, GCKL08, HMSN04, KY00, MS09d, Sal07, TWM09, Bud02]. Completeness [HG03, MW04, ABHS09, PT08]. Complex [JKK01, LKL05]. Complexity [BYJK08, BLM01, BDK09, CKRT08, CB01, DN00a, FW01, GKO07, GKK09, HR04a, Lut02, Nie02b, RMH03b, Ros00a, Rot05, Shp03, BYJK04, CDD00, GKK07, 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]. Composite [CQS01, GMP01a, RDJ+01, Zhe01]. Composition [BJP02, BN00a, CR03, CV02, Pie05, Sho00a, Can06a, LLR02, LLR06, Puc06].

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

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

Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSKC01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL+02, WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Compression-Encryption-Hiding [BD03].

Compromise [Ahm08, Lai08].

Compromised [ZYN08]. Comput [Mck04]. computability [Pet08].

Computable [Vad03].

Computation [ACS02, Bhai01b, BCL+05b, BI05a, BIM00, BJLS02, CC00, CDM00, CDN01, CDG+05, CDI05, DN03, DI05, DM00b, FS02, FGMO01, FWW04, GI02, HCK09, Has01a, HM01b, Jef08, K004, KLML05, KSR02, Lin01c, PS05, WW05, An002g, AB09, BEZ00, BEZ01, CLOS02, CLC08, CDD00, DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WHH05, WY05, SM07b, Duw03].

computation-efficient [CLC08].

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

Computationally [MPSW05].

Computations [HL05a, ML05, RMH04, SBZ04, TC05]. Compute [MFS+09]. Computed [FBW01].

Computer [BS03, Bis03b, Bro05a, BCDH09, BC01, CSW+08, CZK05, CGK+02, Coc02a, Coc03, Eva09, HYZ05b, IEE00a, IEE01a, IE02, IEE03, IEE05a, IEE05b, IEE06, IE07, IE08, IEE09b, If00, JBR05, KM07, Le06, Lu02, MYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Ty05, Cas02, Che05b, DFGH04, Faul09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Shu06, SL06, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coc03].

computerized [LMC+03, Pau02b].

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

Computing [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBDDK00, CGHH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Lu03, May04, PHM03, Sch06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TIC06, V09, Ver02, W01a, Wri00, Yan00, YKMB08, Cha07, Che05c, CHT02, DHL06, HV09, HKPR05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sei05, WH06, Wil99, YLR05, Lu03]. Compuware [Ana02a].

conceal [BB79].

Concealing [DMS00].

Concealment [DA03].

Concept [ARC+01, Ana09c]. concepts [AB09, Kra07, SWR05, MCO4]. concerning [HW03b]. Concerns [MP00]. concrete [KNS05].

Concurrency [JL00].

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

Conditional [LMV05, WN02].

Conditional [IK05]. Conference [ACM03a, ACM04a, An006b, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bih03, Bla03, Bon03, Boy01, Buc00a, CC04a, CV04,
Confidences [Gan01a]. Confidentiality [Dwo03, Pem01a, YC08]. configurable [MBS04]. Configuration [Sha02, Mos06]. Confirmation [SK00]. Conﬁrmer [CM00, GM03]. Confiscation [DBS01]. Conformance [LBR00, RSA00c]. confounded [Bel07a]. confusion [She01]. congestion [SBB05]. Congress [Uni00a, Uni00b, Uni00f, Uni00h]. congruences [Ste08]. Congruential [CS05b, LS05a, SB05]. conic [LWL09, LCC05, LCZ05a]. Conjecture [CU01]. Conjugacy [CJ03a]. Conjugate [Ig02]. Connected [BJLS02, H001]. Connection [HR00, Jam00, Goo00, Mic02b]. Connection-Polynomials [Jam00]. Connections [WRW02]. Conquer [SKQ01]. conscious [DMSW09]. Consensus [CNV06]. conservation [Che01]. Considerations [DBS+06, Hei07, Rub01, Sch07, SVEG09]. Considering [WA07]. Consistency [ABC+05, JEZ04]. consistent [RG06]. Constant [App07, BI05a, CS07c, CD01a, DPV04, DN02b, DI05, Lin01c, Sun00a, IKOS08]. Constant-Depth [BI05a]. Constant-Round [DPV04, DI05, Lin01c]. Constrained [BCH+00, DBS+06, HS01b, MRL+02, Nit09, Zhe02a, Has00, RAL07]. constraints [CC05d, LPM05, SN04]. Construct [CDMP05, Goi01d]. constructed [Tsa05]. Constructible [NNT05]. Constructing [Des00b, Fis01b, LL04b, Vad03, Wen03, JZCW05, NS01a, ZL05]. Construction [BBKN01, BB00b, Car02, CMKT00, Lin03, Nie02c, SM00a, TNM00, YWD08, DW05, SC02c]. Constructions [BS00a, BR00b, BRS02, GMW05, GGKT05, GM02c, Jon04, PR08, PZ02b, SNWX01, SM00b, GT00, GPV08, IK03, IK06, NR04, PR05, Reg03, Reg04, vDKST06]. constructive [GGH+08]. consumption [Mis08]. Contact [YKMY01, Car00]. Contact-Less [YKMY01]. Contactless [And04, KS02, Cla00b, Fin03]. Contemporary [Ahm07, Opp05, SVEG09]. Content [AAK99, CGJ+02, HHJS04, MA00a, MA00b, RE02, XMST07, YKWO1, ATS04, DY09a, GSK09, SG07]. Content-adaptive [XMST07]. Content-Based [RE02, YKWO1, SG07]. Content-triggered [HHJS04]. Contest [Bar00b]. Context [DJLT01, FPS01, SN04]. continue [Lov01]. continued [Dan02]. Contra [Mah04]. contract [WK05]. Contrast [BBDS03, HSK00, HT06, KS03, CDFM05]. Contrast-optimal [HKS00]. Contrast-Sensitive [HT06]. Control [ABE05, ANRS01, BW07, CGMM02, HC08, LY05, Sma03a, ZGLX05, BNP08, DFV04, DPT+02, HW03c, JW06, KNS05, LKZ+04, MD04, MSP+08, PS04b, STY07, WC01b]. Control-flow [ABE05]. Controlled [GVC+08, IMM01, AW05, AW08, LAPS08]. Controlling [HY03, MS03b, MS02d, WL05]. Controls [Har01a, Har01b, Gei03]. convenience [WDCJ09]. conventional [CJ04, YW05, YRY05b]. convergence [An04e]. Converging [Pot07].
Conversation [GK04]. conversations [VAVY09]. Conversion [CDI05, Ket06].
Conversions [K01b]. Convertible [Chi08c, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b]. Convolution [PG05].
cookbook [VM03]. cookies [Cha05a]. Cool [Ano00d]. Coordinate [OS01].
COPACOBANA [GKN08]. Copenhagen [TBJ02]. Copley [USE01b, USE01a]. coprocessing [ML05].
Coprocessor [Gut00, Ito00, LS01b, OTIT01, AV04]. Coprocessors [Smi02]. Copy [LTM00, Per05b]. copying [Gei03, SV08a].
Copyright [Kha05, LLL02, PBB02, XFZ01, ZTP05, Ano01p, Gil07, HLC07, KA09].
Correcting [MZ02, NN06, YYDO01, ZYR01]. Correctness [PBB05, Bel07b, HSD05, dH08].
Correlated [FWW04]. Correlation [BC01b, CL01c, JJ04d, LV04, LMV05, MH04, N01b, SY01a, WR02, ZC00, GG05b, JJ02].
Correlations [KM00, KM01b]. corruption [XNK05].
COS [FF01a, WB02]. Cost [CDF01, FW01, PD07, Sta05, YEP05, CL09, SHJR04, SK03, YLR05].
Cost-Effective [PD07]. cost-ineffectiveness [YL05]. Could [Min03, Cla00b, Pau02b]. Count [Che07b].
Counter [DIS02, QS01, SLG05, SL06, MJM05]. Counter-Measures [QS01]. Countering [PP06b, SK05b]. Countermeasure [IT03, MMT09, OT03a, PKB01, YKLM02a].
Countermeasures [Ava03, Fry00, GM00b, MOP06, OST05, Has01b, JD01, Man08, OST06]. Counters [KMO01]. counterterrorism [Na05].
Counting [Gau02, Kuh00, Hig08]. Couple [SXY01]. coupled [LF03]. course [AA04b, GV09, GL05]. courses [Gha07].
Cover [GA05, Gutt02a, LP02, NN03, RS00]. coverage [DS00]. coverings [SC02b].
Covert [Col03]. Cozens [Sal03b]. CPCMS [Sha02]. CPI [ECG07]. CPN [AADK05].
CPOL [BZ05]. CPUs [ESG05]. Crack [Sin02, Ano08b, Min03]. Crackberries [Sta05].
Cracked [AA00, Nic01, Pri00]. Crackers [ols00, SEK01, SEK02, NRR00].
Cracking [DZL01, BZ03, Cur05]. Crackproof [Sal03b]. Cracks [Bar00a, Ste05c]. Cramer [Liu02b, VMV05].
Creation [MV01, Top02, MB08]. Creator [Coc01a]. Credentials [CL02a, CL04a, LLW05, LW09]. Credit [CNB02].
Crete [ACM01a]. crime [Cas02, KB00, Lau08b, Mad00c]. criminal [Men03]. criminals [Win05c]. crisis [Gu06, Wal04].
Criticism [PAV05]. Critical [LKM05, SE09, CS07a, Gor05, Her09b].
Cron [Oue05]. Cropping [SDFH00]. Cross [Ban02b, SM08, LCX08, SL07].
cross-authentication [LCX08]. Cross-disciplinary [SM08]. cross-layer [SL07]. Cross-Platform [Ban02b]. crowd [Fox00].
CPT [FMP03, Kuh02a, May02]. CRT-Exponent [May02]. crypt [Per03].
Cryptanalyses [HW03c, Kan01, SKU00]. Cryptanalysis [ASK07, AMRP00, An03, An07b, An07a, BDG01, Bao04, BLH06, BP03a, BBK03a, Bar06a, BP01a, BD00a, Bih00, BFM02, BDK02a, BD02b, BS01, BDD03, BD06b, BCCN01, CGFSG09, CV02, CC01a, CC01b, CL01b, CY05, CKY05, CKK05, CWJT01, CJT03, Cho06, Cho08b, CHJ02].

CP02, Cou04, CGJ+02, DG00, DGP07a, DGP07b, DG09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Fin06, Flu02a, Flu02b, Fur01, Fur02a, Fur02b, GS07a, GM02a, GJSS01, GS02c, GM02b, GM00b, GBM02, GC00b, Gra02a, GS09, GKN+08, HPG02, HQR01, HAuR04, Hen06a, HLL+01, HS0+02, HHH+04, Hsu05a, HLH00, Hwa00, JK02a, J00c, J01, JmBdXu05, Jou09, Joy03a, KM02, KWO3, KS00b, KRY05, KW02, KRS+02, KKK00b, Kaa02a, KC05, Küh01, Küh02b, KKL05, LC03, LHL+02, LP03, Lee03c, LKY04, LL05a, LR07, LBGZ01, LBGZ02, Cryptanalysis [LLH04, LL05c, LLCL08, LW05c, MS03a, May02, MG01, MHL+02, Mor05, NP01, Nit09, PSC+02, PKH05, Pei04, Pei06, Pha06, PS06, PS01c, QCB05a, Sch06a, Sco04, Sha03c, Sha05a, STK02, SG08, SK01, SHH07, TID01, TM06, TLH05, TJ01b, TSS+03, Wag00, Wag03, WLT03, WL05, WBD01, WBO2, Wu02, XwWLI08, XY04, YSD02, YW04b, YW05, YKL02a, YKL02b, YRY05a, YY05a, You01, YG01a, YG01c, ZYR01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, AMRP04, BF01a, Bui08, Bar09, BS01c, Buh06, Bul09, Bur02, CV05, CKN06, KCL+03, Dun06, Egh00, EBS01, Eko09, Fie09, GPG06, Goo00, Jun05, KWH00, Kuk01, LMSV07, Max06, MAaT03, MAaT04, MAaT05, MAaT06, MAaT07, Nby01, Pha04, RSQ03, Rup09, SK01a, Sel00, Sin09, SL07, SCS05b, SL0+00, Swe08, TC00, TM01, WLW04, WF02, YI00].
cryptanalysis [YJ00, YKL03, Kat05b].
cryptanalyst [Wil06].
Cryptanalytic [BS00b, KFSS00, Oec03, QSR+02, Yan07, Wil01a].
Cryptic [Wri05, An03b].
CRYPTIM [Ust01b].
CRYPTO [Fra04, Men07, Sho05a, Ahm08, An001a, An003g, Bao01a, Ban01b, Bar01, CCM01, CNB+02, Gen01, HII05, Lev01, Lev02, Mad00b, Mar08a, Mar02b, MC04, Mur06, Pa02, Pem01b, SYLC05, TR09a, TR09b, Yun02b, An001e, An001k, An001m, Bec02, BK05, HGNS03, Mad00c, Mat05, Pot05, Web02, Bel00, Bon03, KII01a, Yun02a, Sei00a].
Cryptological [An001n, CCM01].
Crypto-based [MC04].
Crypto-CCS [Mar02b].
Crypto-integrity [Yun02b].
Crypto-systems [An001n, CCM01].
Cryptoanalysis [HSR02, LD01].
CryptoAPI [Bon00].
Cryptoclub [BP06].
Cryptocomplexity [Rot05, Fal07].
Cryptocompressor [HV04].
Cryptographer [Joy03b, Nac04, Poi06, Pre02c, Men05].
Cryptographers [Coc03, Hes09, KLN+06, Tsa07, Bel07a, Hau03].
Cryptographic [AC02, AADK05, AL00a, An009d, ADH+07, Ase02, BLST01, BSD+01a, Bar00a, BGK+03, Bih03, Bla01a, Bor01, BDP02, Bra01b, BM01c, BL80, Bur06, CC04a, Can01b, Car02, CDP01, CHL02, CKY07, CB01, Cra05a, CS09, CO99b, DD02, DM07, DF04, DS00, DH01, DHR00, DV08, DF01, FS00, Fis01a, FGM00a, Fri01, GMP01a, Gar05, GSS08, GGKT05, Gol01d, GKO2, GTH02, Gor02a, GL00, GUQ01, Gut00, Gut02b, Gut04a, HTO02, HN06, Har06, Has01a, HL05a, HC08, Ig02, IY00, Ito01, IMM01, J05, KMM01, KY01b, KY02b, KII01b, KSI06a, KSO9b, Km02, Kii02, Law09a, LN08, LS05a, LKJL01, MS02a, MOP06, MEO1, MN01, MRL+02, MHH02, Mor03, MK05b, MSU05, NISO1a, NISO1b, Nao03, Ndd05, Ngu05, Nie04, OT010, OP01a, PKBD01, RO8, PZDH09, Pem01b, Pfi01].
Cryptographic [Pin02, Pin03, PS02b, Pot06, Pre00, Pre02a, Pre02b, RSA00d, RSA01, RR00, RRS06, Rot01, RSN+01, MM00a, SS01a, SGM09, Sha02, Shp03, Shy02, SEFD06, SVW00, SR06, SL09, TLYL04, TWA08, TBDL01, Uzu04, WKP03, WN02, WBL01, WC01b, You01, Zha08, AMRP04, ACTZ05, ALV02, AV04, BGB09, BDSV08, BII01b, BP05, BG08, BG09, BDNN02, BD04a, BGL+03].
BMV06, BR05, Can01a, Can06a, CHC04, Coh03, CC05d, CDL06, DP04, Dug04, DFG00, FS03a, FSGV01, GT00, GPV08, GJ04, GM04, GB09, HW03c, HY03, IK03, IK06, IYK02, IYK03, JW01, KAM08, KS05b, KP03, LGKY10, LMTV05, Lau05, LLW05, LLW09, ML05, Mea04, MT07, Mic02b, MRST06, Mon03, NN03, NdM04, NdM06, PS04a, Psg09, Pre05, Pri00, Puc06, QPV05, Reg03, Reg04, Ren09, Cryptographic [RMH04, RBF08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, TNG04, kWpLwW01, LWL04, XLM06, VLT06, ZL99, ZWWL01, ZL04b, dH08, BWBL02, JQ04, KKP02, KP01, KN01, RS05]. Cryptographically [ADD09, AHS08, BCP02, Bcheng11, BFCZ08, BB00b, FR08, MS02b, PLSvdLE10, RGX06, Aam03, AW05, AW08, Lau08a, SM03a]. Cryptographically-masked [AHS08]. CryptoGraphics [CK06]. Cryptographie [RSA09a]. Cryptography [ANS05, AF04b, ADI09, AA04b, Ano00e, Ano01], Ano02b, Ano02f, Ano02g, Ano04b, Ano05a, Ano07b, AAAG01, AIK04, AIK06, App07, AAEAQ05, ABM00, Bai01a, Bai01b, BIP03, BD04, BOV03, BOV07, BBGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BWBL02, Bla02b, DD00, Bon00, Bon07, BPR01, Boy03, BLMS00, BK06b, BM07, Buc00a, BD08, BP01b, BRTM09, CPS07, Cer04b, CCL09, CSW08, CQ01, CP06, Cob04, CFA06, COP00, Cor06, Dr00c, Dam07, DFS08, DFS05, Das08, D00, DF04, DK02, DK07, Des02, DT03, D09b, DSS01, DD00, DND03, Dre00, DP08, EPP07, EP05, Elb09, El04, ECG07, Ett02, F03b, Gal01, Gal02, GKH06, GKK09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Gri01, Gro05, HR06, HH04]. Cryptography [HMM01, HM04, HSS01, HPS08, Hon01, IEE00b, IYK05, Irw03, IK08, JY04, JH00, JT01b, JT01a, Jue04, Kak06, KLR09, KZ07, KSG07, Kat05, KK06, KMB09, KPMF02, KWD06, KY01c, Khr01a, KMS02, KM05, KZ02, KZ03, KW06, Lam01, LSG01, LSY01, Lee03b, LLL01, Lie05, LDM04, LW05b, LP02, Lut03, Lys08, MNT00, MP02, Mao01, Mao04, MS010, MZ04, Mau01, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nic02a, Nic02d, NH02, PV06a, PV06b, Pe06, PM02, PBB02, Po02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGK08, Sti95, Sti01, Sti02, Sti06c, SJ05, Syv02, TSO00, TW06a, TG04, TMM01, TW02, TW06b, Tro08, TR09a, TR09b]. Cryptography [Unio01, USS02, VY01, VMC02, RP05, W04, WK01, Wei05, We06, WvD02, Wri00, YWC08, Ytr06, YC01, YDKM06, ZY03, vDW04, Und03, AM07, AEO17, AN03, AUW01, Ano02a, Ano02g, AB001, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bsl03, BDN00, BCD06, BEZ00, BEZ01, BGM04, BEM07, Buc00a, Buc01, Buc04, BLSR09, BMA00a, BMA00b, BMA00c, CCT08, CJ03c, CDFM05, CD07, Cos00, Cre00, DD04, Dif01, DIM08, Dw05, DOP04, DK09, DW09, Du03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK07, Geb04, GRTZ02, Gol99, GG05b, GHPT05, GPS05, GNP05, HH05, HHL00, He03, HKP05, HA00, Hig08, HKS01, H05b, HG05b, HLwWZ09, L00, IM06, JK01b, Jan08b, JM09, Joy00, KZ03, KL08, Kat01, Kilt05, Kim01, Kob00, Kra07, Lam00c, Lee04a]. Cryptography [Lin01a, Lop06, Mau04, May01, Ma08, MBS04, M07a, Mol07, NP02a, Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00, Pin06, Pip03, Reg05, Reg09, Rot02b, Rot03, Roy00b, Ru09, STY07, Sch02, Sch04a, SZB04, Ser06, SH05, Shp09, Sil05, Sin99, Sin00, Sm04, ST01d,
Sti11, SK01b, TW05, UHA°09, Van03, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wei03, YC09a, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Si01a, Sma05, Bee05, Lee03a, Ree01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08, Ros00b.
cryptography-based [FXAM04]. Cryptologic [BS00a]. Cryptological [Lew00]. Cryptologie [dL00]. Cryptologists [WD01b]. Cryptology [Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Lai03, LL04d, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka04, Poi06, Rot05, RS02, Sma05, Bee05, Lee03a, Ree01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08, Ros00b].

cryptoManiac [WWA01]. Crypton [CKK°02, MG01]. Cryptosystem [BST02, FL06, GG01, GK05, GH01, Bug02, KM01a, KY02c, KLC°00, LHT09, dVP06, Luc02b, NSNK05, NBD01, Ove06, PHK°01, YG01a, YG01c, Zhe02a, Zhe06, Bao04, CL02b, CCH04, Che05a, Cho06, CFVZ06, CH01, Dan02, DHL06, EKRM01, GHGSS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04c, LL06, LKYL00, Lo00, LS01e, OP01b, Pae03, Po00, SPG02, SCS05a, SP79, SLC05, Sun00b, Sun02, SYP02, TJ01b, TJ01a, VS01, War00, YC09b, hY08].

Cryptosystems [Aki09, Ava03, BDG°01, BKLS02, BPS00, BM00, CHSS02, CCW02, DDG°06, DKKY02, ESG°05, FJ03, FC06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KKY02, KL01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vao03, Wya02, XB01, ZLK02, Ban05, BF06a, BB79, CHC01, CMKT00, EBS01, EHKH04, G08, GKP01, HM00, Has00, Has01b, Hiu00, HP01, KW00, Kos01c, LL04b, LD01, Luk01, Mic01, Mis06, OS00, Pei09, PLJ05b, SSST06, Sha05c, Sma01, TO01, TC05, Tsa05, Ver01, Wuo04, WPP05, VW00, YH00, ZSZ01, vT01].
cryptovirology [YY04]. CRYPTREC [YY00]. CSCW [ZP05]. CSP [SB09]. 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, PM09]. Cube-Type [PDMS09]. culture [GI07]. Cumulative [LG04, WP03]. cure [RD09]. cure-all [RD09]. Current [An03b, DFH01, PRS04, LPW06].
curriculum [FOP06]. Curve [ANS05, AD09, An05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BM01, CQS01, CFA°06, GPP08, HY05a, H01, HM04, HM02c, JT01b, JT01a, KMB09, KPMF02, KSZ02, KWP06, LW02, M0l02, Kir03, OTIT01, OS01, PWGP03, Pei06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YYY01, ZLK02, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, Dim08, DwWmW05, EHKH04, GKP01, Has01b, Hsu05a, HL05d, MJ09, JW06, LL04c, LWL09, Mis06, OS00, ST03a, SSSST06, SH05, Sma01, SCL05, SLC05, TC05, Van03, Ver01, Wlu04, WPP05, YC09a, YC09b, ZSZ01, ZL05, vT01].

curves [KWP06, Pei06]. Curves [AHR08, Bai01a, BB00b, CY02, Gal01, G1V01, Gau02, GHK°06, Kid02, PWGP03, Ver02, CMKT00, Hus04, LWZH05, MP01b, MVS04, Sil05, Sim02, SC02b, Was08b, Wen03, Yas08].
customer [Lin01b]. CVS [DFG01]. Cyber [FNRC05, WW04, M00c, Mau05].

cyber-crime [Mad00c]. Cyberinsurance [BP07]. Cybersecurity [PLW07].
cyberspace [MIT02a]. cycles
Cyclic [PG05, Mic02a]. Czech [MJ04].

D [Duw03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05]. D.R [Irw03]. dad [Che05b]. dæmons [Mos06]. Damgård [CDMP05]. dark [Blu09]. darkening [CDD07]. DARPA [Coc01a]. Data [ACM03a, ACM04a, ABM08, Ano02a, AAC01, BGHP02, B+02, BS00b, BNWP03, Bro05b, Cle01a, CTL01, DBS01, EBC+04, Elh09, FMA02, FLA+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, Küüs02, Lan00b, LLRR07, LP00, LHS05, LS08, Lut03, MND+04, MS03b, MFS+09, NNAM10, NM09, OS05, Per05a, RKKD02, RK06, Sal03a, Sal07, Sin01a, SK03, SDMN06, TZZD05, TPPM07, VDKP05, WS05, WY02, WN02, kc01, vW01, AMB06, AG09, Ade09, AHK03b, AKS040, Am01, Bla00, BP08, CCMT09, Cer04a, CO03a, CLR09, CPG+04, DZL01, DGMS03, FS04, HILM02, LLK05, MJ03, Mal06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sche04a, Sch04b, Sch05a, SGP09, SETB08, WMDR08, YLC+09, YC08, ZSJN07, Zir07, AEH17, Cur05, DK08, LIn02, Pap05].

Data-Hiding [VDKP05]. Data-Oriented [NNAM10]. data/image [Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, BI05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Mau04, PS08b, PBVB01]. database-service-provider [HILM02]. Databases [AK02b, CDM+05, DN04, AHK03a, CDD+05, CKY07, GA03, MSP09, MNT06, NS05b, ÚG08, YPP09]. Datamining [DN04]. Datenverschlüsselung [Lin02]. David [Gas01, Pap05, Bar05, EAg05]. Day [SE01, CSW05, Win05c]. Days [Adl03, Riv03, Smo04]. DC [USE01c]. DCT [BC01a, BC01b, CH01b, KT00, LY07, LSC03]. DCT-Based [LY07, LSC03]. DDH [Lys02]. DDO [LKH+08]. DDO-64 [LKH+08]. Dead [Gut02a]. deaf [Pau02b]. Dealer [DK01, Sm00a]. Dealing [BH00a, BC05b]. death [For09]. Debate [Jol01, Mad00a]. Debian [YRS+09, Ahm08]. Deblur [VHP01]. Debugger [Ano02d]. Debugging [Ano02d]. Dec [IEE09a]. decades [Lov01]. decades-old [Lov01].

December [ACM05a, Boy01, CV04, DVWM05, FLY06, Hon01, JM03, Kim02, Lai03, Lee04b, LTT+04, Li05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sm05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b]. Decentralized [MSP+08]. deception [CS07a, Mal04, MS02d]. Decidability [Küüs02]. Deciding [Bau05]. Decimal [BJvdB02]. Decentralisation [BZ03]. Decimation [Fil00]. decipherable [aSM01, Sav04]. Deciphering [Eri02, KB07, Ark05, Lov01, NS01a]. Decision [DJ06, GR04, KM04a]. Decisions [CU01]. Decisions [Coc02a, Sch07]. Decodable [Yek07].

Decoding [KY02b, LBGZ01, LBGZ02, Rai00, AGK07, Bul09, Eva09]. decomposing [FP09]. Decomposition [BR09, CL04c, SC02c]. decompositions [vDKST06]. Decorrelation [CLLL00, Vau01]. decrypt [Bih02]. Decrypter [Ban00, Bau02a, Bau07, MB01]. Decryption [Bar00b, BST02, CS03a, CCD07, FPS01, HGNP+03, Int00, KCJ+01, Ano08a, Che01e, DZL01, GH08, Mil03, OS07, Shp04b, WH+09, Wh09]. Decryptor [TPS01, Zol01]. DeCSS [Coc02a]. Dedicated [ISO04]. Deep [CMS08]. Defeating [CSK+08]. Defective [BTTF02, Dav01b, Dav01c]. Defending [NRR00, Pro01]. Defense [GK02, HW01, Mir05, Wy05, Bol02]. defenses [SL06]. defined [Yas08].

Definition [YWD08, SN100]. Definitions [Uni01, AH05]. Definitive [BS01a, BS05, Gar03b]. defying [HRS08].
Degenerate [Ber09a]. Degradation [BSC01a]. Degree [CV02, QPV05]. Degrees [Sat06]. Déjà [DP00]. DeKaRT [Gol03]. Dekker [Irw03]. Delacorte [Imr03]. Delay [WRW02, NS01a]. Delayed [JM07]. delegated [CL04c]. Delegation [WN02, ZP05, MW06]. Delhi [JM03, RM04]. Delivers [Ano02e]. Delivery [NZCG05, RMCC01, DY09a, NZS05]. Delphi [TEM+01, Hei01]. Demand [BD03, CMB+05, SEF+06]. Demilitarized [Kum07]. Democracies [CZB+01]. Democracy [CTBA+01]. Demography [Coc03]. Demons [Mos06]. demonstrably [HL06]. demystifying [RR04]. Deniability [Pas03]. Deniable [Nao02, CCK04a, CSK+08, DG05, LC05b, SY05c, Zha06]. Denial [Mah04, Nik02a, Nik02b, PKBD01, Riley05]. Denial-of-Service [Nik02a, PKBD01]. Denmark [Cra05b, TBJ02]. Denver [ACM01b, Sch04b, USE00d]. Department [Bol02, Eri01]. Dependable [NABG03, And08b]. Dependent [Gol03, WS05, BS08, SK03]. deployed [BDE00]. Deploying [BH00b, GSB+04]. Deployment [CL07, KDO01, Mur01, Sin01a, App05, JR09]. Dept [Uni01]. Depth [BI05a]. Derandomization [BOV03, BOV07]. Derivation [DGH+04]. Deriving [BJP02, CSW05]. DES-encrypted [Bih02]. DES-like [Egh03, EBS01]. Desch [LBA00]. Describing [PS06]. Description [Lav06, MH05]. Descriptors [PS07, SP04]. Design [Abd01, AADK05, Ano02e, ADD09, AIK+01, ARC+01, Bar00b, Can01b, CDP01, Cim02, CB01, CS02b, CMB+05, CL02, DR02a, DR02b, DS09, DF07, EH0+03, FF01a, FZH05, GSS08, Geb04, Gut02b, Gut04a, HRL09, Hor05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04c, LB05, MKP09, MP00, Nd05, NSS02, Rhi03, SJT09, SPG02, SRQL03, Uzu04, WZW05, WYO9, WLL09, ARJ08, Ade09, CMS08, GG05b, Gut04c, HC04a, Hut01, KSF00, MI09, MMM01, SME09, YCW0+08, YC08]. Design/CPN [AADK05]. designated [LV07]. Designing [HBC+08, MRT10, TCR03, C+02, CG05, Lan00c]. Designs [Bec05, CC02a, Bai08, Des00a, WL07a]. Desktop [Mun08, BDE00]. Desmedt [CHH+09]. Desynchronization [CDT05]. Detached [Sha01c]. Detailed [Lut03]. Details [Scr01]. Detect [FOBH05]. Detecting [CMS09, FGD01, JQYY01, Har07a, LHL04a]. Detection [AS01b, AD07, BB00a, BKM07, CH01b, CZEK05, JT05, KKG03, SKQ01, SY01a, SLT01, ST01c, TZZD05, TMM05, WG05, YI01, Zan01, Bej06, BBK+03b, HLL0+02, Men03, NNO2, WMS08, YW06, ZGTM05]. Detection/Correction [SKQ01]. Detector [BSC01b, DNP07]. Determined [KKH03]. Determining [KS03, LQ08, OS07]. Deterministic [BK06a, Her06, KZ03, KZ07, May04, BK07]. dev [BH05]. Developers [Ano06c, Dew08, MK05b, Nis03a]. Developing [MV03b, Cra05b, Gal02, HL06]. Development [Ano02e, CMB+02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a]. Developments [Ano03g, Pre07, Sha04a]. develops [Pau02b]. Deviates [Rau55, Ran01]. Device [Ric07, ST03b, WFS01]. Devices [BCH+00, CFRR02, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KHD01, MV01, MRL+02, SCF01, WC01a, Ano06a, CMS08, CF07, DMT07, sHCP09, Tse07, YCO0b, ZYW07]. Devil [Bla01c]. DFT [Che08a]. DH [Lys02]. DHIES [ABR01]. DHP [MSV04]. Diablerets [Van05a]. Diagnosis [Ano04b, BK06b, XNK+05]. Diagnostics [NM09]. Diagonal [PJJ01, PKJ01]. Dickson [SZP02]. Dictionaries [AGT01].
Dictionary [BPR00, BCP02b, CS07b, DJ06, Pho01, NS05a]. did [MH09]. Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b].

Dies [Bar00a, Coc01a, Mat05]. difference [PBMB01, dW02]. Differentiating [LS08, WWTH08]. Different [CGMM02, Sma01]. Differential [Av03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eke09, Fur02a, Gra02a, HLL+01, HSM+02, IIT03, JT01a, Kan01, KM02, KCP01, LHL+02, MP06, MMT09, MHL+02, MG08, PSC+02, SK01a, SKU+00, SKU01, YSD02, vW01, BF01a, CUS08, Che08a, DLP+09, Egh00, EBS01, Pha04, SLL+00, TM01].

Differential-Linear [BDK02a]. Differentials [BF00b]. Difficult [Bud00b, MT02]. Difficult-to-pass [MT02]. Diffie [Jan08a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CR08, FS01b, GR04, Kil01b, KK02, KM04a, Kra03, Kra05, Mis08, Ts06, YRY05c].

diffuse [Wal04].

Diffuser [Fer06]. diffusing [She01]. digest [MSP09]. Digit [KWP06, Tan07a, BG09, HKPR05, KIr01b].

Digital [ANS05, Atd00, AR00, AS08, Ano01g, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00b, CCH05, CC09, Che01b, CFS01, CM02b, CM08, CZB+01, CGJ+02, DSP01, EIG01, Eng00, EH9+03, HSZ00, Hs01a, Hs01b, HHGP+03, HW01, HLT01, JBR05, KZ01, Ka01, KC02, Kuh00, Kwo02, Kwo3b, LLL+01, Lin01b, LW09, LL01, Lut03, Mad00a, MM01a, MMT02, MSI01, Meh01, PL01, PZH01, PCG01, PZL09, PBM+07, Ram01, Rds01, RS01, Sam09, Sch00d, Sch06b, Sc01, Sha01e, SC02a, Shi08, SL01, Sag01, TMM01, TJC03, US02, VHP01, VK07, WNO9, Win05a, WBD01, Wu01, WV01, WC03a, WC04, Wy02, XZ01, XYL09, YWWS09, YYDO01, YZ01, ZWC02, ZNO02, ZC04, AAP07, AA08, Ano00i, Ano01p, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CNO, Che07a, Che00b, Die00, FB01].

digital [GKK03, Gl07, HRL09, HLC07, HHL00, HHC05, K00, LG04, LG09, Lev01, LLL06b, MKY08, NRR00, PC05a, PLJ05a, PBV08, QCB05b, Re03, Sha01d, Sha04b, Sha05d, SCL05, TCC02, TND+09, U05, WNO08, WHL03, WC05, XC05, XMST07, Ano09b, Ano13, BCK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].

Digital-Audio [WNY09]. Digital-Signature [Eng00]. Digits [Che04b, Ran55, Ran01]. Dimension [DDG+06, TST09a, TST09b]. Dimensional [XYXYX11]. Dimensionality [SBG02]. dimensions [CLR09]. Dining [KLN+06]. diplomacy [Alv00]. Direct [BMW05, K09]. direct [PJK01]. Directions [Sha01b, DF01]. directly [JZC05]. Director [Mad04]. directories [C+02, Pet03]. directory [C+02]. disabled [Pau02a]. disadvantage [CDS07]. Disappear [Per05a]. Disappearing [Way02b, Way09]. disappointed [Ste00]. Disaster [WC05]. disciplinary [SM08]. disclosure [JM07, Swi05]. Discover [Eva09].

Discovery [Bi09, HLL+02, SBG07, SG07]. discrimatsby [Ano09c]. Discrete [CS03a, CNS02, Che04b, CWC02, Gen00b, GV05, GPP08, KC09b, LW02, L05, VK07, HN04, HW03a, HWR09, Hsu05a, HLL05d, JL03, JLL01, LHL03a, LL04b, LHY05, LTH05, PLJ05a, QC05a, Sch01e, Sha05c, Sha05d, SW05, SCL05, SLC05, SCS05c, Y05]. discretized [MA02].

Discription [Har07b]. discursive [Mit02a]. Discussion [Ano01a, Ano01b, Ano01c, Ano01j, Ano01n, Ano01f, Ano01o, KLB+02a, Mal02, Nik02b].
dish [Ano01]. Dishonest [GKK007].

disjoint [Gut04c]. Disk [CRO01, Har07b, Siv06, CS08a, Fer06].
dynamics-based [sHCP09, jLC07].

E-business [Poh01, HHSS01].
E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-Goods [NZCG05].
e-Government [RM02].
E-Learning [CAC06].
e-mail [Che01f, LL04c, NZS05, Smi03, All06, ANR01, KS00, Law05].
e-mails [LG09].
e-payment [Has02].
E-payment [Has02].
E-smart [AJ01b].
E-Vote [Che07b].
e-voting [CJT03, Cha04].
E-Wallet [ETZ00].
Easier [Pau09].
Easy [GR04, Hos06b].
Eavesdropping [Kuh02a, Kee05].
ebanking [WDCJ09].
eBook [Ano02d, WWL02].
EC [SF07].
ECC [BWBL02, CL09, Miˇs08, Tsa05].
ECC-based [CL09, Tsa05].
ECC2K [LM08].
ECC2K-130 [LM08].
ECCV [MJ04, TBJ02].
ECDSA [ANS05].
Eclipse [Coc02b].
ECMA-305 [ECM00a].
ECMA-306 [ECM00b].
economics [Ble07].
ECPP [Che03].
ed [Gum04, Nis03a].
Edge [STA05].
Edinburgh [RS05, Pen01b].
edit [CGFSH09].
editing [MAaTxx].
Edition [Cho08a, Irw03, Spr03].
Editor [MFS09].
Editors [ACM06, B+02, ELvS01, IEE01b].
Einstein [HR13, MNT00].
EJB [TEM01].
Ekert [Duw04].
El-Gamal [EKRMA01].
Election [JLL02, Cal00b].
elections [Cha04, PvS01].
electrical [Wal04].
Electromagnetic [SGM09, QSO1].
Electronic [Ble07, CL001b, CM02, Dur01, Höf01].
ISO65, IF00, KMO01, KS02, Lan04b, LLL02, Mad00a, MNFG02, Rub01, RMCG01, Str01a, YKMY01, ZYM05, AvdH00, AAKD09, Cal00a, Cas03, EY09, FB01, HJW05].
element [MSO2d].
elementary [Sin09, Ste08, Tat05].
Elephant [Fer06].
Eleven [All03].
ElGamal [Bijn00, CL02b, CW00, HL04, LHT09, SJ00].
ElGamal-like [CW00, HL04].
Elizabeth [Bud06].
Elliptic [AD01, Ano05a, Bai01a, BINP03, Bar00a, BBGM08, BMM00, BS01d, BMN01, BB00b,
CQS01, CFA+06, GLV01, Gau02, GPP08, HYZ05a, HHM01, HMV04, HM02c, Hus04, JTO1b, JTO1a, KBM09, KPM02, Kid02, KSS02, LW02, MP01b, Möl02, Kir03, OTIT01, OS01, OT03b, PWGP03, RSA03b, RS04, RS01, Sat06, Sil05, Was08a, Was08b, WP01, XB01, YYZ01, vTO1, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHKH04, GBKP01, Hsu05a, HL05d, JMV09, JW06, LL04c, LWZH05, Mis06, MSV04, OS00, ST03a, SSST06, SH05, Sim02, Sma01, SC02b, SCL05, SLC05, TC05, Van03, Ver01, YC09a, YC09b, Was08, ZSZ01, ZL05, ANS05, BWBL02].

Ellis [Coc01a].

Elmau [IEE01b].

Elude [Che01f].

EMA [QS01].

Email [ES00b, Gar03a, Her09b, Luc06].

Email-Based [Gar03a].

emanations [ZZT05].

Embedded [Ano01c, Ano02d, Ano02e, BBGM08, Dri02, DV08, GSS08, JTO5, JQ04, KKP02, LPW06, NdM04, RS05, SPGQ06, WK03, YSS+01, ARJ08, BGM04, Fox00, Geb04, KV+09, KP01, KNP01, KP03, MB04, Nis03a, TKP+08, XQ07, Fin02].

Embedding [Aak09, JX05, JG07, LSC03, Sal03b, WY02, WC04, CO09a, KC09a, Wan05].

Embrace [CNB+02].

Embracing [Ano03d].

EMD [BR06].

Emperor [Smi01b].

Empirical [HW03b, Goo00].

empirically [SS03].

employee [You04].

Emptiness [DIS02].

Emulex [CZB+01, CTB+01].

Enabled [Por06, CNCY01, DY09a].

Enabling [Web02].

encapsulation [CHH+09, KG09].

Encipher [BR00a].

Enciphering [HR03, KT01].

Encode [BR00a, BKN04, Ano08c].

Encode-Then-Encipher [BR00a].

Encode-then-Encrypt-and-MAC [BKN04].

encoded [WMS08].

Encoding [JT01b, RS00, Lin02].

encounter [Win05c].

Encountering [Wol03].

Encrypt [BKN04, BTTF02, Dav01c, Pet05, Dav01b].

Encrypted [BBK03a, BGHP02, BGLS03, CD101b, Hug04, Lan04a, LH07, MMZ00, NAM10, RMCG01, Sta02b, Vau01, WRW02, Whi09, Woo00, AMB06, Ano06a, Bib02, BN08, CCMT09, CDD+05, CSK+08, FJ04, HLM02, Hes04a, LHL04b, LSH00, MW04, Pet03, ÜG08].

Encrypting [Pro00, RC01, Zho06].

Encryption [ABC+05, Abe01, AS01a, Abe04, AEH17, AP09, AB01, ADR02, And03, Ano01g, Ano01h, Ano01i, Ase02, ANR01, AFI06, AF03, Bar00c, III00, Ban02b, BN00a, BR00a, BBM00, BBPD01, BU02, BF01b, BF03, BBO4, BWW05, BCHK07, BGH07, BPR+08, BB03, BN03, BD03, BKY02, Bur03, Cal00d, Cal00e, CD00a, CS03a, CHK03, CHK05, CGHG01, Che01a, CTL01, Chi08e, Cho08a, CMR06, Cla00a, C02b, Cob01b, CINP00, CHJ+01b, CDN01, CS02, CS03b, Cro01, Curt05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DFK+03, DK05, DS05b, Dri02, FJP01a, FL01a, GC01a, GSW00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HS00a, HS02a, HY05a, HSHI02, HSHI06, HKR01, HWW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03].

Encryption [HL02, HGNP+03, HLL05, HLC08, ISSZ08, Jol03, Jol01, JK02b, JK02c, JMV02, JKR01, Jut01, KSD03, KSH01, KS00a, KY01a, Kha05, KJK+07, Kos01a, Kra01, Kur01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LRRW07, Lin03, LNP02, LM05, LCO07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, Möl03a, Mor05, Mi01a, MS09d, NIS00, Nam02, NZCG05, NZS05, NP02b, Nie02b, PV06b, PM00, Pau09, Pema01a, PZL09, PDM09, Phao4, Por01, P00, Pre01, RM04, RK06, RJD+01, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQ03, SPQ06, SBZ02, Syeo0, TV03, Un00a, Un00c, Un00e, Un00d, Un00g, Un00h, Ust01b, VMS05, WZW05, WBRF00,
Wri01, YEP+06, YW06, ASW00, Abd01, ABHS09, AKSX04, AMRP00, ABW09, Ano00e, Ano00c, Ano00f, Ano00g, Ano00h].

**encryption**

[Ano00j, Ano02a, Ano03g, Ano06d, App05, Ate04, AcDM05, AFGH06, BPS08, BKN04, BR04, BBN+09, Ber09a, BBK+03b, Bir07, Bla00, BJN00, Bro05b, CG06, CS08a, CBSU06, CHC01, CKRT08, DZL01, DL07, DRS05, DW01, Fer06, FB01, FMS05, GM08, GGK03, Gen09a, Gen09b, GKM+00, Gou09, Gua05, Gut04c, HSH+08b, HSH+09, HS02b, HCD08a, HCD08b, HAURO4, HWW02, Hua05, Hwa05, Hua05, HL05c, HL05d, IM06, JK01a, JK01b, JWX05, JSW05, JZCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Kik08, La0f0, LV07, Lee01, LCP04, LJ05a, LMC+03, LLZ06a, LLZ06b, LLZ08, LB05, Lu02, Luc05, LK01, LW05a, Mad04, Mar05b, Mat02, Miu01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pan03, RG09, Rhi03, RBB03, RSP05, SN11, SKW+07, Sch00a, Sch01c, S+03, Sch04a].

**encryption/cipher**

[HAURO4, HWW02, Hua05, Hwa05, Hua05, HL05c, HL05d, IM06, JK01a, JK01b, JWX05, JSW05, JZCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Kik08, La0f0, LV07, Lee01, LCP04, LJ05a, LMC+03, LLZ06a, LLZ06b, LLZ08, LB05, Lu02, Luc05, LK01, LW05a, Mad04, Mar05b, Mat02, Miu01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pan03, RG09, Rhi03, RBB03, RSP05, SN11, SKW+07, Sch00a, Sch01c, S+03, Sch04a].

**encryption/decryption**

[SN04].

**Encryptor**

[LMP+01, TPS01, Ano00a].

**Encryptor/Decryptor**

[TPS01].

**Encyclopedia**

[Bid03, vT05].

**End**

[KCD07, Per03, SKKS00, WWP00, YSR01, AMB06, SU07].

**End-to-End**

[YSR01, AMB06].

**Ended**

[Kü02].

**Endomorphisms**

[GLV01].

**Endpoint**

[Kad07].

**Enemies**

[DM07b].

**Energy**

[GC01b, Ino05, LPV+09, SLP07, Mis08].

**Energy-efficient**

[LPV+09].

**Energy-security**

[Ino05].

**enforce**

[SN04].

**Enforcement**

[GN06].

**enforces**

[BP05].

**Enforcing**

[GMM08, HRS08].

**Engine**

[Fri01, MMH02, DP04, SLH07].

**engineer**

[Pau02b, SN04].

**Engineering**

[CNB+02, MNT+00, MYC01, Pem01b, Roy00b, SM07b, TR09a, TR09b, VH09, Ano09b, EC05, Jen09, Man08, Wal04].

**engineers**

[Pri00].

**engines**

[PM08].

**Enhance**

[ZWC02].

**Enhanced**

[JKRW01, LHL04b, ZGLX05, CZ03, McK04, OP01b, TWL05, WLT03, WHH05, ZSM05].

**enhanced-security**

[OP01b].

**Enhancement**

[CJ05, FLZ02, LSH03a, LSH03b, SLH03, YW04a].

**enhancements**

[ADH+07].

**Enhancing**

[BDK02a, MS05a, SE09, Sun00b, DY01].

**enigma**

[Rob02, Rob09, BCB+05, Cas06, Chuo02, Cop04b, DB04, GO03, Goo00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Th03, Wil01a, Win05b, Win00].

**Enigmy**

[Kap05].

**Enough**

[CNC+02, Pat03a, Ano03c, YJ00].

**Enrolment**

[HWH01].

**Entangled**

[Bar00c, LB04].

**Enterprise**

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

**Entropic**

[DS05b].

**Entropy**

[DS05b, EHS00, LH07, JRS09].

**Environment**

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

**Environmental**

[PS05].

**Environments**

[CJF+04, LKLH09, BGM04, MNS08, SBG05, SBG07, SN04, YC09a, YhJ04].

**ephemeral**

[Miš08].

**Ephemizer**

[Per05a].

**EPOC**

[JQY01].

**ePOST**

[MPHD06].

**EPR**

[Ina02b].

**Equation**

[FJ03].

**Equations**

[CP02, DDG+06, GS03, PBMB01].

**Equipping**

[DMT07].

**Equitability**

[DBS01].

**equivalence**

[Fis01a, LQ08, MS04].

**Equivalent**

[Fer00, KOMM01, May04, SIR04].

**Era**

[MP00, Uni00c, Bur00, Uni00f].

**erasure**
[PCS03]. Erasures [JL00]. ERP [LSZ05].

Erratum
[AGGM10, Kwo03b, LLLZ06a, McK04].

Erroneous [CH01b, MNT +00].

Error
[BBY +03b, BQR01, Din05, KKG03, LW05b, LM02, ML03, MPWS05, MZ02, NN06, SKQ01, YI01, YYDO01, ZYR01, Zol01, Gar04, LHL04a, YW06]. Error-Correcting
[BBK +03b, BQR01, Din05, KKG03, LW05b, LM02, ML03, MPWS05, MZ02, NN06, SKQ01, YI01, YYDO01, ZYR01, Zol01, Gar04, LHL04a, YW06]. 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].

establishing
[Kov03, KH03]. Establishment
[BM03c, NIS03b, HMvdLM07, LF03, SL05a].

Estimation
[EFY +05, JX05, KLB +02a, LNL +08, Sel00]. Ethical
[Har05b, Woc05]. Euclidean
[CPhX04, CMJP03, CLZ02, WI02]. EULA
[WWL +02]. EUR [Eag05]. EUROCRYPT
[Bih03, CC04a, Cra05a, Knut02, Pi01, Pre00, GJSS01]. Eurographics
[MFS +09].

Europe [Pag03]. European
[AL06, CZ05, KGL04, Pre01, dCdVSG05, Ano00f, Che08b, Die00, Pre02a].

EUROPKI
[AL06, CZ05, KGL04]. EV
[HTJ08]. EV-C2C-PAKE
[HTJ08].

Evaluate
[Pre02a]. Evaluating
[BN05, NTW07]. Evaluation
[BSC01a, EYCP00, FS00, FML +03, IKM00, IY00, JX00a, Knat01, Kir03, SKKS00, BZP05, FXAM04, FS03a, LCP04, MCHN05, RC05, RN00a, RN00b]. Evaluations
[LM02].

Evangelizing
[Coc01a]. evasion
[Blu09].

even [Bih02, OS00, Win05c]. EventGuard
[SL05b]. events
[SBS09]. ever
[Fur05].

Everlasting
[DR02d]. Every
[Che07b, TH01, DKK07, Win05c].

Everyone
[Han00]. Everything
[CTBA +01]. Everywhere
[Ber00].

Evidence
[Ver01, Bro05a, HW03b].

Evolution
[DF01, Rec01, Pat02a, Ros00b, SP02, Sin99, Sin00]. evolutionary
[LMSS07]. Evolved
[LMHCETR06]. Exact
[Cox00b]. examines
[Nis03a]. example
[Bla00, GC05, Zir07]. Exchange
[BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JX08, KOT01, KY03, MPS00, Mac01, MSJ02, Ngu05, VPG01, WC01a, WV01, ZWCY02, BBG +02, BCP07, CLC08, CWJT01, DG06, GL06a, GM05, HTJ08, KS05a, KOY09, LHL04b, LW04, LFHT07, LHC08, LSH00, MS03a, Mi08, WLH06, YC09a, YPKL08, ZYW07, CPP04, CP07, ECM00b]. exchanging
[KN08]. Exclusive
[GRW06]. Executing
[HILM02, LJJ05a].

Execution
[Coo02]. Exhaustive
[Des00c].

Existing
[MV01, BDE00]. Expanded
[Ch08a, Irw03]. Expander
[JMV09].

Expanding
[DN02a]. expansible
[LLW08a].

Expansion
[DN02b, BCD06, HKPR05]. expansions
[HKPR05]. Expected
[KL05, RK06, DL +09]. Experience
[Sas07, BCHJ05]. Experiences
[MPHD06, USE00b]. Experimental
[BG09, CGBS01, OOP03, WS02, RSQL03, Sm04].

Experimentation
[Hum05].

Experimenting
[LSVS09]. experiments
[Bru06], expert
[Ano01h, Che05b].

Expiration
[MP00, SCH05]. Explicit
[CY08, GRW06, WPP05]. Exploit
[BR00a, FOBH05]. exploitation
[Eri03, Eri08, KV +09]. Exploiting
[CK06, ETMP05, HR00, HM04, ZWC02].

Exploits
[MJF07, CSW05]. exploration
[SKW +07]. Exploratory
[Lut03].

Exponent
[BP04, BM01b, DN00b, May02, SZ01, CKY05, Duj08, GD05, SH04b].

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

Exponentiation
[KKH03, SK07, CKRT08, HGNS03].
Exponents [FS02, FS01b, BS02]. Export [Mad00b, Ano00h, Mad00c]. Exposed [Gum04, MSK03, SSS06]. exposing [YY04]. Expositive [MAaT05]. Exposure [BM03b, DSS01, KZ07, CDD05, KZ03]. Exposure-Resilient [DSS01, KZ07, KZ03]. expressions [MW04]. Extended [ABDS01, BPS00, CM00, Cou04, DIRR05, HLvA02, HW01, JL00, MSJ02, MP02, OST05, Wag02, BJN00, CD00a, HT04, HP01, Mis06, Pci09, QPV05, KLJ01]. Extending [ADDS06, IKNP03, Ove06, Sal03b, SS01a]. Extension [Bai01a, YWD08, BR06, CMdV06]. Extensions [ABC05, BBGM08, CS07c, HM02b, Rot02a, Wei04, Elb08]. Extracting [Cer04a]. Extraction [DGH04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lu02, Vad03, DW09, KZ03, Sha04a]. Extraordinary [Top02]. Extreme [Ree03, Ano02d]. Extrusion [Bej06]. Eye [Sas07, CAC03]. Eye-Opening [CAC03].

F5 [Wes01]. Face [KZ09, NH02, PK01, SBG02, TZT09b, PY08]. FaceHashing [TNG04]. Faces [NS01c, Ngt01]. facets [Rot02b, Rot03]. fact [Ano03g]. Factor [DN02b, Sas07, BSSM07, Hend06b, Sch05c, St.00, Ste05a, YWW00, DB07]. Factoring [BN02, KY02a, KLB02a, KMM01, May04, PV06b, ST03b, LTH05, LCZ05c, Mil01b, PL05a, QC05a, Sha03d, Sha05d, ZCL05]. Factoring-Based [PV06b]. factorisation [GG08]. Factorization [CDL00, Lam91]. Facts [GO03]. Fade [CAC03]. Fail [JQYY01, SSS00]. Fail-stop [SSS00]. Failures [DFG01, HGPN03]. Fair [CC00, DLY08, GC01a, JL01, JL04, LMS05, PS00, VPG01, WV01, LSA07, MS3a]. Fair-Zero [LMS05]. fairness [GCKL08]. faithfulness [GTZ04]. false [ZSJN07]. Falsification [OM09]. Fame [Bar00c]. Family [CQS01, Flu02b, NPV01, SK05a, You01, Ber07, FNR05, GBKP01, MP07]. Fan [YRY05c]. fare [GMG06]. Fascinating [Sch09]. FASME [RM02]. Fast [AL00b, ABM00, BTW03, BST02, CJS01, CC06, CQS01, Cor00a, Cou03, Cro01, FS02, GC01a, GD02, GMM01, GP08, HGO07, HR04a, JF00d, KKIM01, KK03, KKJ07, LSY01, LS05b, MSNH07, Kir03, NS05a, NSS02, OEo02, OT03b, PG05, RR02, Ts06, UHA09, Yan05, AB07, BAMA00a, BAMA00b, BMAA00c, JAW00, JJ02, Lud05, PBMB01, WWA01, BR07, DR02c, GH05, Jol03, Mat02, RM04, Sch00b, Sch01d]. Faster [Bar00c, CMJ03, GLV01, KS09a, LV04, Oec03, Ban05, Why05]. faszinierende [Sch09]. Fat [MYC01, TvdKB01]. Fault [Ano04b, BM00, BK06b, BK07, DS03, Gir06, PV06a, PQ06b, WL07b, YKLM02b, HGR07, Lin07, PI06, RMH04, YJ00, YKL03, ZL04a]. fault-based [YJ00]. Fault-Tolerant [WL07b, HGR07, Lin07, RMH04]. Faults [GS08, VS08]. Favour [Gen01]. Favre [MFS09]. FBI [Mad04]. FC [Bl03a, Fra01, Jue04, PY05, Syv02, Wri03]. Fear [Hei03, See04, Sty04, Sch03]. Feasibility [APV05, BD00]. feasible [LM08]. Feature [GW01, Gut02a, HH09, LNP02, LLC06a, NN03]. Features [PK01, SBG02]. February [DR02c, Fra01, GH05, Jol03, Jue04, Kli05, Kim01, Men05, NP02a, Nao04, Oka04, PY05, Poi06, Pre02c, RM04, Syv02, USE02a, Wi99]. Federated [De07, Ano04c, GT08, Sm08, Sul05]. Feedback [CGFSHG09, CM03, Cou03, Igl02, Hey03, SPG02]. FeedForward [BP01a]. Feel [PM00]. Feeling [Buh06]. Feistel [Cou04, Kan01, LMSV07, Omi01, Pat04]. Feldman [AF04b]. Ferrer [CKN06]. Fetal [MYC01]. fetch [HTW07]. Fi [Sty04, Bar03]. Fiat [VS08]. fiction [An03g]. FIDES [ISTE08]. Field
Fields [FJ03, GC01a, RDJ+01, CKY07, GMG00, Has00, JL03, ST03a]. Fighting [Bai01a, BT02, CU01, Che04b, CQS01, CF505, HCK09, HHM01, KKH03, Lov01, MN01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RMH04, Sim02, Sma01].

Fifth [ACM03b, SM07b]. Fighting [DGN03, SZ03]. File [CCDP01, GIS05, Ito01, LK01, BDET00, CSK08, HTW07, Hos06b, ISO05, MKK00, MSP08]. Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pet05]. Filesystems [WBL01]. Filter [LBGZ01, LBGZ02, MSN07, Sar02, CMS08]. Filter-Combiner [Sar02]. Filtered [MH04]. Filtering [SDFH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00]. Finalists [EYCP00, IKM00, IK00, IK01, Mes00, Mes01, SKS00, SW00a, WW00]. Finally [Coc02b]. Financial [ANS05, Gri01, Pem01b, Wri03, Bla03, Fra01, Jue04, PY05, Syv02]. Finding [HR04b, MP06, WYY05b, WYY05c, ZT03, SW00].

FINDsomeone.com [Gra98]. Fine [SS01b]. Fine-Grained [SS01b]. Fingerprint [An002d, HHY07, HBF09, KHY04, MMH02, CL04d, MJ100, UBE09]. fingerprint-based [CL04d]. Fingerprinting [KT01, CT07]. Fingerprints [TK03, KLY03, Sco04]. Fingers [MMH02]. Finite [BLST01, BR01, CU01, Che04b, CQS01, HCK09, HW05, KKH03, MM07b, PH01, RS08, Ver02, Gar04, Has00, LMC03, LQ08, NS01a, RMH04, Sma01, SLT06, TC00]. Finkenzeller [And04]. FIPS [Nat00].

firewall [LJY04]. firn [Zaf00]. First [Bar00a, BB09, Coh03, CM02, CMB+05, FLY06, KGL04, KS06b, MN01, Nao04, NNT05, ÒP03, PK03, QSR+02, Roy00a, USE00b, Wil99, ZJ04, ZHY03, AJ01a, Cla00b, Coc02a, DV05, LBA00, RH00, Un00a, Un00b, Uni00f, Uni00e, Uni00h, Lan00a, Lan00b]. First-order [Coh03, KS06b]. Fish [Fie09, Wei06, Wei00, Wei05]. Fit [CCM05].

Five [SW00a, MS02b, Rot02b, Rot03]. five-lecture [Rot02b, Rot03]. Fix [TEM+01]. Fixed [AR01, BCCN01, CKN00, LS01a, Shp04b, SP07]. 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, CLK10b, DGK+04, OT03a, Tsa01, BA06, KC05, LHY02, WWA01]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM+09]. Flows [ECM00a, AHS08, Cer04a, Lao08a]. Flying [Fox00]. FOCS [IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07]. foes [Ric00]. 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 [BCC05, CS04, CS08a, CDS07, MS09a, MKY08, MAC+03]. Forest [FBW01]. Forgery [CH01a, CKN00, LS01a, SLT01, HSW09]. Forgotten [Eag05, Kin01, OC03]. Form [AD09, CH07c, OS01, LKY00, Mic01]. Formal [BGB09, Bel07b, BCHJ05, BCJ+06, CL05, DKS08, GOR02b, HG03, Lan00d, Mea01, YWD08, ABH09, JW01, Mea04, Pau01, SW02, ZLYX99, ZLY6b]. Formalizing [HM01a]. Formally [BJP02]. format [ISO06, RG05]. format-string [RG05].

Formation [RW03, Luk01]. Formats [GSM05]. Former [MADO4]. Forms [JT01, LLL04]. Formula [Kog02]. Formulas [CH07b, WPP05]. Formulas [BGN05]. Formulations [AHK08]. Fort
Forums
[CZB+01, CTBA+01, CNB+02, CMB+05].

Forward
[AR00, AFI06, BY03, CHK03, IR01,
HCD08a, HCD08b, SY06, ZYW07].

Forward-Secure
[AR00, AFI06, CHK03, IR01,
HCD08a, HCD08b, SY06, ZYW07].

Forwarding
[KCD07, Kra02b].

FOSS
[Bol02].

Founder
[Bar00a].

Four
[LXM+05].

Four-Layer
[LXM+05].

Fourier
[Che07a, DSP01, DNP07, KC09b, LPZ06,
SP04].

Fourteenth
[UJE00c].

Fourth
[ACM02, ACM05b, DFCW00].

FPGA
[Ano02e, CC02a, CGBS01, CG03, CNPQ03,
EYCP00, EHKK04, KMM+06, KY09,
KBM09, KRS+02, LP02a, MM01b, MM01c,
OTIT01, ÖOP03, Pat01, PBTW07, QSR+02,
TYLL02, DPS01, USS02, WW00].

FPGAs
[AD07, DPR01, MM0709, RSQLO3, SGM09,
SK05a].

Fractal
[AA04a, JLS03, WC03a].

Fraction
[DSP01, SSST06].

fractions
[Dan02].

Fragile
[CC09, CH01b, CT09, Nak01,
PJK01, LYGLO7, SY01b].

Frame
[LHS05].

Frames
[HW005].

Framework
[ANRS01, GL03, GOR02b, Hun05, NMO05,
NP07, PS06, RS00, Shy02, ZYN08, AHH03b,
Ayo06, CCCY01, CP07, CC04c, DMSW09,
GJ05, GL06a, GM04, JEZ04, KNS05,
MS09b, MBS04, YCW+08, HF00].

Francais
[ACMO4a, ACMO5a, AJ01a, AJ01b, GH05,
KN01, NP02a, PPV07].

Francisco
[Cal00c, Joy03b, Men05,
Nac01, Oka04, USE02a, USE02b].

FranzSteiner
[EE03].

Fred
[Bar00b].

Free
[AP09, Ano02e, Bau01a, Bau01b, BGI08,
Coc01a, CNV06, DG02, HS00, HM01b, JP03,
Jut01, Fox00, KS06b, SG05, B002].

FreeBSD
[Coc01a, Mur02, Siv06].

Freedom
[UNI00a, UNI00c, UNI00d, UNI00g,
UNI00h, MII03].

FREENIX
[USE01b, USE02c].

French
[Wri03].

Frequencies
[DD02].

Frequency
[OMT02, Sak01, SOHS01, CS05a].

Frequency-Domain
[OMT02].

Frey
[Was08a].

Friar
[GG05a].

FRIEND
[CTY09, CRSP09, Hsu05b, HL05b, SZS05,
WLT05a, WC03b, YW04b].

Fried
[An01k].

FrontPage
[WWL+02].

FSE
[Bi07, DR02c, GH05, Joh03, Mat02, RM04,
Sch00b, Sch01d].

FTC
[Ste05c].

fuels
[Mad04].

Full
[Cor00b, DOP05, LKHL09,
WYY05b, WYY05c, BI04, CS08a, HS02b,
LKH+08, Oiw09].

full-encryption
[HS02b].

Full-Round
[LKHL09, LKH+08].

Fully
[BL08, FS01a, Gen09b, KPMF02, RG09,
Gen09a].

Function
[BR02, CDMP05,
Fis01b, Flh02b, GIS05, HNO+09, HPC02,
JJ00a, Kan01, Kil01b, Niel02c, RB01, Yan05,
CH05b, CJ04, HR07, LW04, LPM05,
Tsa08, WWT08, YW05, YRY05b].

Functional
[ECM00a, WA06].

Functionality
[PS05].

Fundamentals
[TTMP05].

Fundamental
[ETMP05].

Functions
[AEMR09, BBDK00, Bon01, Can01b, CV02,
Car02, Che01c, DNO2a, DGN03, DNR03,
Fie02, FIPR05, GL+02, HSM04, HR04b,
Jou04, Kil01b, LW05, Lyso2, PB01, RR08,
SM00a, SM00b, SS01a, Sh00a, Sh00b,
Ver02, WP03, WFLV04, Wer02, AGGM06,
AGGM10, ALV02, CS09, DS09, GVC+08,
HR08, ISO04, KK07, KS05b, LHL02,
LKY04, MS02b, MS09c, Mie02a, Mic02b,
NR04, PW08, QPV05, SM03a, Whi09,
YRY04, ZW05a, RRS06].

Fundamentals
[And04, PHS03, Shi08, Way01, vTO04, Fin03].

Funds
[CC01a].

Further
[JS05, JPL04,
LL04a, LL05c, Ano09c, MP07, YRY05a].

Fusion
[KZ09, TZZD05, ZS05, BG09].

fusul
[MAAT05].

Future
[ASW+01, Ano02f, Joh00, LNP02, NFQ03,
Handheld [BMK00, Ano06a]. Handhelds [MP00]. Handle [RC06]. Handling [KL05, Lut03].

Handoff [OKE02]. Hands [KLB+02b, Shu06]. Hands-on [KLB+02b, Shu06]. Handshake [SB01].

Handshakes [Ver06a]. Haptic [PBM+07]. Haptics [Pau02a]. Hard [Har07b, HMS04, Hro03, Lai07, CGHG06, GPV08]. Hard-Core [HMS04]. Hard-Disk [Har07b]. Hard-Line [Lai07]. hard-on-average [CGHG06]. hardcore [Sch01e].

Hashed [Ano02d]. Hankerson [Irw03]. Haptic [PBM+07]. Haptics [Pau02a]. Hard [Har07b, HMS04, Hro03, Lai07, CGHG06, GPV08]. Hard-Core [HMS04]. Hard-Disk [Har07b]. Hard-Line [Lai07].

hardware [Ano07b, Ano07a, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG+02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, Nd05, PS01c, Rs05, RS04, SOTD00, SMTM01, SM02, SM03b, SRQL03, SGK08, TSO00, TBLD01, WKP03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK+03b, DS09, EHKK04, GC00a, HBC+08, KP01, KNP01, KP03, Nd04, RA07, SOIG07, V08, W0104, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07].

Hardware [Ano07b, Ano07a, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG+02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, Nd05, PS01c, Rs05, RS04, SOTD00, SMTM01, SM02, SM03b, SRQL03, SGK08, TSO00, TBLD01, WKP03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK+03b, DS09, EHKK04, GC00a, HBC+08, KP01, KNP01, KP03, Nd04, RA07, SOIG07, V08, W0104, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07]. hardware/software [ARJ08].

Hardware [Ano07b, Ano07a, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG+02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, Nd05, PS01c, Rs05, RS04, SOTD00, SMTM01, SM02, SM03b, SRQL03, SGK08, TSO00, TBLD01, WKP03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK+03b, DS09, EHKK04, GC00a, HBC+08, KP01, KNP01, KP03, Nd04, RA07, SOIG07, V08, W0104, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07].
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, CJ06, CJG’02, DS05b, FZH05, Gro01, HNZ02, HV04, Int00, JKRW01, KMM’06, Ken02b, KM05, KB00, Kra05, KTO1, MM01b, NFQ03, RW07, SKKS00, SOTD00, SM02, SGM09, SLG+05, TL07, Uni00c, Wie00, WWGP00, YKMY01, Zhe01, BVP+04, BZP05, BGL+03, Jen09, KC09a, SK03, Uni00f, WWTH08, Zir07]. 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, Zhe01, BVP+04, BZP05, BGL+03, Jen09, KC09a, SK03, Uni00f, WWTH08, Zir07]. Hijack [Ste05c]. Hill [Gum04, USE02a]. Hilton [KJR05]. HIPAA [AEV+07]. histograms [CO09a]. historic [Pet08]. Historical [RE02, MWM01]. History [BP03b, Ifr00, Pag03, Sal01a, Sin01b, CAC06, Top02, AJO8, Boo05, HSW09, Jan08b, KNS05, Na05, Nis03a, Pin06, Ris06, RH00, RG06, Wil01a, dLB07]. history-based [KNS05]. hit [Bjo05]. HMAC [FIP02a, DGH+04, Hir09, RR08]. HMQV [Kra05]. Hoare [dH08]. Hoax [CZH+01, CTBA+01]. hoc [BSS02, Cha05b, DHMR07, KH05, KVD07, LHC08, LKZ+04, PSC07, SL07, TW07, WT02, ZC09]. Hold [PM00]. Holier [MYC01]. Holistic [RM02]. Homage [JP02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03]. Homegrown [Str02]. Homeland [Man02, Man05, RR03b]. homogeneous [MF07, PS02a]. Homomorphic [AS01a, Aki09, CNI01, DN03, HS00, Cho06, Gen09a, Gen09b]. homomorphism [CKN06]. homophonic [Sav04]. Honeynets [Dim07]. Hong [B+02, ZJ04, Cl00b]. honor [OC03]. hook [JEZ04]. hooks [GJ05]. hop [NC09, ZSJN07]. hop-by-hop [ZSJN07]. Horizon [Coc02b]. host [Shu06]. hostile [ABB+04]. Hosts [H6f01, SZ08]. Hot [IEE01b]. Hotel [USE01b, USE01a, USE02a]. HotOS [IEE01b]. HotOS-VIII [IEE01b]. hours [Fox00]. House [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hsu [BC05, HL05c]. HTML [CNB+02]. HTTP [Zha00]. Huang [ZC05]. Huge [MSNH07, NNT05]. Hull [KMT01]. Human [Dre00, GL01, JW05, KY01, Yon04, Man08, MS02d, RFR07a, RFR07b, RFR07c]. Human-Memorable [KOY01]. Hundred [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hunting [GJL06]. Hwang [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KLC03, LW05c, QCB05a, WL05, YRY05d, ZYR01]. Hwang-Rao [ZYR01]. HWMM [LKY05c]. HWMM-authenticated [LKY05c]. Hybrid [AD09, CBB05, KD04, LZ04, PK01, AS04a, CJ03b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a, Che01d]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02]. Hyperelliptic [Av03, CY02, CAF+06, HSS01, PWGP03, Ver02, Was08a, ZLK02, CMKT00, Wen03, Wol04, WPP05]. Hyperencryption [Che01d]. hyperlinking [Che01e]. hypotheses [KW00].
Ibn
[MAAT04, MAAT05, MAATxx, MAAT07].

Ibn-Adlan [MAATxx]. Ibn-Al-Durahim [MAATxx]. iButton [HWH01]. IC [BGL+03, PC00]. ICBA [ZJ04]. ICCMSE [SM07b]. ICISC [Kim02, LL04d, PC05a, Won01, WK06]. ICISC’99 [Sau00]. ICM [IEE09a, IEE09a]. ICs [Bar06c]. ID [Gui06, ZJ09, ZJ09, CCD07, CL00, GS02b, GTY08, HC08, KLY03, KHL09, Ku02, LSC09, Sco04, SW05a, SCL05, WBD01, WH02b, YC09b, YLH05, ZK02, ZC04, ZC09]. Id-Based [ZJ09, CCD07, GS02b, HC08, Ku02, WBD01, YLH05, ZK02, CL00, KLY03, KHL09, Sco04, SW05a, SCL05, WH02b, YC09b, ZC04, ZC09]. IDE [Ano02d]. Idea [Cos03, RR03a, CTL10, Hts02]. Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b]. Ideas [Cha07, Eri01].

Identification
[BP02, BLDT09, Gar03a, GLC+04, KK02, Kiri01b, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZC09]. identifiers [MC04]. Identifying [HBF09, LLS05b, ZYN08, DMS07]. identities [Kwo02, Kwo03b]. Identity [App05, BF01b, BF03, BB04, BCHK07, BGH07, BPR+08, Boy03, BRTM09, CL01a, CHM+02, Coo01b, Dea06, DT03, GKO4, Her06, Her07, HY01, HL02, KC02, LCO7, Mar08a, Mar08b, Mit02b, Neu06, PSCM07, Phi06, SMV+09, Ano01l, Ano04e, BMW05, CG06, CJO5, GGu06, Gui06, KG09, LL04b, LWZH05, RGO9, Sae02, Sha03c, Sma06, Smi08, Sul04, Wal04, WDN04b, WO05a, YC09b, YC09, ZC09].

Immersive [Coc01a]. Immune [CZK05, PZ02b, YKLM02b, YKLM03]. Immunization [HR05]. Impact [Ber03, HGNP+03, JKRW01, MMHYH02, Wri00, CS08a]. Implant [Fox00].
Implement [HQ05]. Implementation [AD07, AG01, Ase02, Ash03, ARC+01, BBD+02, CDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK+03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HMM01, JKS02, KMM+06, KMS01, KTT07, KRŠ+02, KV01, LP02a, MMZ00, MKP09, MM01c, MNP01, MP01c, Mur02, Nov01, NMSK01, Ow09, OTIT01, Pat01, PBTW07, QSR+02, RDM01, Sm01, Sha04b, Sh05b, WHLH03, YRF05b, YRF05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JSW05, JnBdXgXm05, KJY05, LL04a, LW05c, SGS05, TO01, WLT05a, YW04a, YWC05, YRF05a, YRF05d, ZC09]. Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, HW03c, SRQL03]. Improving [ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SKQ01, SB01, Sun02, XQ07, YEP+06, YGZ05]. incentives [Svi05]. Incident [JBR05, Tom06]. Including [SR01]. Incomputable [Ver06b]. inconsistencies [MS09a]. Incorporating [MFS+09]. incorrectness [CHC04]. Increase [NNAM10, PBTW07]. Increasing [AEH17, CS05c]. Incremental [BKPY02, LKLK05]. IND-CCA [Mühl01b]. IND-CCA2 [BST02]. Independence [BP03b]. Independent [BS00a, BSI02, Kin02, GSK09]. Index [Ano00b, Ano01d]. indexing [YPKP09]. India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03d]. Indies [Fra01, Syy02, Wri03]. Individual [BCC02, TW07]. INDCRYPT [CV04, JM03, MMV06, MS02c, RD01, Roy00a]. Induced [Vau02]. Industrial [USE00b]. Industry [ANS05, Mad00a, Ort00]. ineffectiveness [YLR05]. Infeasibility [FS08]. Inference [Mar02b, CDD+05]. Infinite [TZZT09a, TZZT09b, Vau01]. infinity [Hii05]. Influencing [Bla01c]. Inform [Kwo03b, San05]. Information [AP09, BW07, BIM00, BZ02, Big08, BB03, BJ02, Boy01, CGM07, CC06, DM00b, ECM00a, ELvS01, Hax06, HQ05, HW01, ISO04, JDDJ01, JG07, KP00, Ke02, KLB+02b, KO00, Lat03, Lee04b, LW05b, LL01, MH05, MMZ00, Oka00, PP06b, RSA00d, RS01]
Roy05, Sch06b, SVW00, Son00, Sta06, Ste02, TG07, VDKP05, WABL+08, Yek07, Zhe02b, ZS05, vW01, ABH509, ABW09, Arn01, Bid03, BK00, BEZ00, BEZ01, Bro05b, Duw03, FR08, FOP06, Gar04, Gha07, IY05, KN08, KB00, Kov03, MS09b, ME08a, PS02a, Sch02, Sch04d, Sun02, TWM+09, Way02b, Way09, dLB07, CSY09, FLY06, GW00, Kim02, LL03, LL04d, PC05a, Won01, WK06. 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, Bra01, LAPS08, LOP04, SN07]. INIDP04 [LDM04]. initial [DK08]. initiation [YWL05]. Initiative [Coc01a, Cal00b]. initiatives [Man05]. injection [MMJ05, ZSJN07]. Injectable [CMdV06, Kos01c]. Innovation [Sam09, SW05b]. innovations [Web02]. Innovative [MM07a]. Innsbruck [Fpi01]. Input [CAC06, TC00, DKL09, VM03]. Input-trees [TC00]. Insecure [Vau05b, Wal01, BJN00, LLH06, XwWL08]. Insecurity [Bla02b, DOP05, Lai08, Man02, NS01b]. insertion [MB08]. insertion-extraction [MB08]. Insider [CMS09, Tad02, KS05a, Mah04]. Insights [Kun01]. Inspired [CC09]. Installation [USE00a]. instance [FS08]. Instances [GG01, HN06]. Instant [BBK03a, RR05]. Instantiated [RR08]. Instantiation [BF05]. Instruction [BBGM08, EP05, KTT07, Bru06, Elb08, HTW07, MMJ05]. Instruction-Level [EP05]. Instruction-Set [BBGM08]. Instructions [LSY01]. instrumentation [MPPM09]. insubvertible [ACdM05]. Insulated [DKXY02]. Integer [Gro03, JL03, MN14]. Integers [CH07c, GMP01a, KKIM01, EKRMA01]. Integral [KW02, WH09, SM11, SH11]. Integrated [ECM00a, ECM00b, GMG00, Lutt03, GLC+04, LK01, SSM+08, SN04]. Integrating [Wit01, AEH17]. Integration [Ito00, CJL06, Sug03]. Integrity [Ano02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel [Coc02a, MP00]. Intellectual [Qu01, WY02]. Intelligence [Cop04a, AJ08]. Intelligent [Cos03]. Inter [WR02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WR02]. interaction [Gav08]. Interactions [Fau09]. Interactive [BC05b, DG00, MS09c, CHK05, DDO+01, Fis01b, Fis05, HN02, JHW01, KKL09, KHL09, MTS04, Pas05, vT00, MS09c]. Interception [CHV03]. interdomain [MABI06, vOWK07]. interesting [SWR05]. Interface [RSA01]. Interference [FGM00a, FGM00b, GA05, BR05]. Interlaken [CC04a]. Interleaved [ZSJN07, NC09]. intermediaries [JA02]. Internal [Har07b, Bej06]. International [ACM03a, ACM04a, ACM05a, ACM09, ACM10, AN03, Ano00d, AAC+01, AJ01b, BDZ04, Be010, B+02, BB09, BS01b, Bhi03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCMR02, CCMR05, CSY09, CGP03, Cra05a, DR02c, Des02, DUK05, DFP06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JY04, Jef08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, Kil01a, Kiu01, Kin02, KN03, Knu02, KP01, KNP01, Lai03, LL03, Lee04b, LST+05, LL04d, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, Pk03, Pfi01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Sch01d, Sh05a, Sl01, SM07b, Syv02, TJ02,
Japanese [IY00]. Java [Ano04e, Mar05a, WBL01, Ano02e, Ano03a, Ano04c, Ano04f, AJ01a, BCS02, Bis03a, BJvdB02, CMG+01, Che00a, CCM05, Coo02, DPT+02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hun05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Vir03, Wei04, Win01, Zea00, ZFK04]. Java-Based [EM03, DPT+02, GW08]. Java-L¨osung [Ano04c]. JAVA-Ring [WBL01]. JavaCard [AJ01a]. Javacards [Cim02]. JavaScript [TEM+01]. javax.crypto [Win01]. JBits™ [MP01a]. JCCM [CMG+01]. Jean [MFS+09]. Jeju [CSY09, Lee04b]. Jeng [QCB05b]. Jenness [Sal03b]. Jessop [Ano03b]. JICC [HYZ05b]. Jim [Coc01a]. Job [MYC01]. jobs [Oue05]. Joel [Gum04]. Johannes [Lee03a]. John [And04, BZ02, NH03, Rot07, Ano03b, Coo03]. Joins [Bar00c, Con00]. Joint [ADI09, ADR02, CR03, HYZ05b, HYZ05a, Puc03, MI09]. J¨org [Fal07]. Jose [Poi06, Pre02c]. Joseph [LAB00]. Journal [LLLZ06a]. Journey [FF01b]. Jr [Kat05b]. Judiciary [Uni00h]. Julius [Chu02]. July [ACM01a, CZ05, Je08, KJR05, May09, PPV96, Roy00b, Sch01c, S+03, Uni00a, Uni00b, Uni00e, Uni00d, ZJ04]. Jump [MP00]. June [ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BSO1b, BC01, BC05, FMA02, IEE05b, IK05, JY04, KLG04, KN03, KM07, PPV96, TBJ02, USE01b, USE01a, USE01c]. Just [ABB+04, Ano06a, Gut02a, Car01]. Kahn [Gas01]. Kaikan [Ano00d]. Kaspersky [Ano05a]. Kasumi [KYHC01, KSHY01, SM02]. Katholieke [BBD09]. Katz [Bar00a]. Keccak [BDPV09]. Keep [DM07b, Lys08, FS04]. Keeping [SEK01, SEK02]. KEM [NMO05]. Kerberos [BCJ+06, Coc01a, Gar03b, Ili00, Ito00, LLW08a, MJ01, MPPM09, Rub00, Smi01a, Wac05, WD01a, Wit01]. Kerckhoffs [KMZ03]. Kernel [Int00, Mor03, BK05, HB06]. Key [ANS05, ASW00, AK02a, Ano01n, Ano09d, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BPS08, BH06, BDG+01, BDZ04, Bar00a, BPS00, BPR00, BBM00, BBDP01, BY03, BOHL+05, Ben02, BLM01, Bib00, BBB+02, BDK+09, BR00b, BM03b, BDTW01, BNM01, BM03c, BGM09, BMP00, BCP01, BCP02a, BCP02b, BM01c, BST02, CK02a, CK02b, CHK03, CK05, CPP04, Che01a, CT08a, CHK008, CJO3c, CCW02, CCM01, CKM00, CS02, CS03b, CS03c, DPV04, DJ01, DPS05, Des00c, DBS01, Des02, DG03, DY09b, DKK+02, DFK+03, DGH+04, DBS+06, ESC+05, EP05, ES00a, FL06, FKS00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Gol03, GHW01, GC01b, GSB+04, Gut04b, HNZI02, HCD002, HLM03, Hoe01, HR05, HG03, HC08, HJW01, HS07, HLC08, IEE00b, Ina02a, Ina02b, JL08, Jot02, JG01, Jue04, Ka03]. Key [KGL04, KQY01, KY03, Kat05b, Kel05a, Kel05b, Kel00, KKIM01, KM01a, KLV02, KKY02, KY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, Ku02, KOMM01, KY01e, Kuri01, KI03, LCK01, LLL2, LP03, LV00, Len01, Lin03, Lin00b, MPS00, Mac01, MSJ02, MHM+02, May04, MR01b, MR01c, Mol03a, Mol03b, Mül01a, Muro00, NIS03b, NA07, Ngu05, NB01, NSS02, OTU00, Ort00, PHK+01, PR01, Poi02, PHM03, RAS00a, RR00, RW03a, RW02, ST01a, ST02, Sha01e, Sin01a, SVW00, SK00, Ste01, ST01c, TSO00, Tan07b, TT01, TV07, Wal03, WZW05, WHI01, WC01a, Woo00, WBD01, Wya02, YKMY01, YI01, YG01c, YDKM06, Zhe02a, ZWY02, ABHS09, AJS08, AUW01,
AKNRT04, Asl04b, AFB05, BHM03, Bad07, BBN+09, Ben01a, BB79, BG08, BBG+02, BD00b, Bra01a, BCP07, BMA00a, BMA00b, BMA00c, BD04b, CCT08]. key

[CL02b, CZ05, CYY05, CYH05, Che04a, CHC04, CY05, CLC08, CKRT08, CWJT01, CJ04, CLK04, Cho06, CHH+09, CJL05, CCD06, Cre00, DFM04, DG06, DM07, DW09, EKRAM01, ED03, EHKH04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GMR05, GKM+00, GS01, GL06b, GMW01, Gue09, HCD08a, HCD08b, HAuR04, HHG06, HTJ08, HG05b, HW04, KAM08, LHK04b, LKY05a, LL04a, LW04, LLL04, LKJL01, LSH00, Lin01a, LS01a, LCC05, Lop06, MWS08, MKW00, Mi08, MRT10, Mü01b, NP02a, PS08a]. key

[PI06, Pei09, Pei04, PQ03a, PQ06, PC09, PSP+08, PLJ05b, Pot06, Pri00, RH03, SN100, SL07, SR01, SBZ04, Sha05c, SW06, Shi05, SL05a, SW05a, Shp04a, SC05b, SIR04, SLC05, Sun00b, Sun02, SZP02, SCS05b, SC05c, SCS05c, SY06, TP07, T001, TNG04, Tsa06, Tsa05, Tso07, VS01, Vau05a, VK08, WDLN09, War00, WHL06, WGL00, WV00, WCI0b, Wu01, WL04b, WHHT08, XH05, YW05, YC09a, YC09b, YS02, YSH03, YS04, hY08, Y04, YRY05a, YRY05b, YY05b, YPKL08, ZLG01, ZC04, ZK05, ZSM05, ZYW07, A00b, GL05]. Key-Based [Sha01e]. Key-Dependent [Gol03, BPS08]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKXY02]. key-management [JW06]. Key-Privacy [BB04a]. Key-Recycling [PS05]. Key-Share [CT08a].

Key-Sharing [HNZ02, WBD01].

Keyboard [ZCW05]. Keyczar [Law09b].

Keyed [Küh08, SR00, FIP02a].

Keyed-Hash [FIP02a]. keying [ABB+04, Che08a, EGK08].

Keyless [Qu01].

Keys [AOS02, APV05, AFI06, BT02, BNM00, BWA05, CHM+02, EHMS00, Fer00, HSH+08a, LKH07, Luc00, MN01, MRL+02, M007, Nit09, Oni01, PS00, Sm01c, Str02, TvdKB+01, An01k, BCL05a, BCP07, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH+08b, HSH+09, HW04, HY03, HL04, KAM08, LHL04b, LL05a, LW05a, LL05b, LS01c, LWK05a, ML05, NN03, Sch01e, Sh09b, Sh05b, SB05, TL05, TJ03, WH03, YRS+09].

Keystream [AM04p, Kra02a, LV04, MH04, WLV04, PS01a, SM11]. Keystroke [SCHP09, MR00, BGP02, JLC07].

Keystrokes [SWT07]. Keyword [FIP05].

KGC [HL08]. KGS [ZY07]. KHAZAD [PQ03b]. KIA [May09]. Kid [CAC06].

Kikai [An00d]. Kikai-Shinko-Kaikan [An00d].

Kilometer [Das08]. kind [DW01]. Kindi [MAAT03, MAAT0x].

Kilometer [Das08], kind [DW01]. Kindi [MAAT03, MAAT0x].

Knowledge [Abe01, Abe04, AS01b, APV05, BP04, Cou01, DP04, DFS04, Doo+01, Era02, Fis05, Gen04a, GK05, HNO+09, KS06b, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00a, Ros06a, TG07, BDS08, CLR09, Dau00, Hro09, IK050, JRR09, PB07, KK07].

Knowledge-of-Exponent [BP04]. Known [CN06, CM05, DN02a, Fur02b, HSH+01, Bao04, YTH04]. Known-IV [HSH+01].

Known-Plaintext [DN02a, Fur02b, CN06]. knows [Fox00].

Koblitz [AHRH08, Has01b]. Kolmogorov
Kommunikation [Lin02], Kong [B+02, ZJ04, Cla00b], Konstantin [Puz04], Korea [CSY09, CKL04, Kim01, Kim02, Kum07, Lee04a, LL04d, May09, PC05a, PK03, Son00, Won01, WK06], Korner [Mor02], Ko´sciuszko [OC03], Krawczyk [Miy01], Kryptoanalyse [Mor05], Kuala [DV05], Kunming [ZYH03], Kurosawa [CHH+09], Kurtz [Gum04], Kyoto [Oka00].

Laboratory [Bru06, LBA00], Lagrange [FWTC05], Laid [Wei06, Wei05], Lam [Wag00], Lamar [LMHCETR06], lamp [McN03], LAN [Bar03, LFHT07, Pau03, SZ08, Sty04], Large-Scale [CDR01, BH00a, BP03a, HMvDL07, HY03, PS08a, SM03a, TM06, WL05], Larger [Car02], LARPBS [CPH+04], Lasers [Igl02, UHA+09], late [Sch05c], latency [RS05], Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HPS01, HG07, IM06, Mic01, Reg03, Reg04], Lattice-based [MR09, HPS01, IM06, Reg04], lattice-reduction [HG07], Latitudes [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Shp05, Sii01], Launched [Bar00b, Ano00b], 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 [Bau03a, Bau03b, BH00b], Lead [Tsa07], Leak [RST01], Leakage [CKN01, DP08, Kel02, RS01, ABHS09, CNK04, IY05], Leakage-Resilient [DP08], leaked [Mad00b], Learned [GSB+04], Learning [KS06a, LY07, CAC06, BKW03, KS09b, Mal06, Reg05, Reg09, SM08, Whi09], Least [SZ01], lecture [Rot02b, Rot03, Adl03, RSA03a, Riv03, Sha03b], Lee [Sty04, YRY05d, Coc02b, KRY05, KCL03, KHKL05, LKY05d, SCS05b, ZK05], Left [Dhe03, HKPR05], left-to-right [HKPR05], Legal [Coc02a, AN03], Legislation [Eng00], legislative [AvdH00], legitimate [Lin01b], Leighton [Rub00], Leighton-Micali [Rub00], Length [AR01, BR00b, CKN00, CHJ+01b, M ’ ; 03a, RK06], Length-Preserving [M ’ ; 03a], Leonard [Coc03], Less [YKY01, BD00b], Lessons [GSB+04, KFSS00], Lest [HSH+08a, HSH+08b, HSH+09], Lets [Pau02a], Lett [Kwo03b], Letters [ASW+01, BTTF02, MNT+00, TEM+01, TvdKB+01, WWL+02], Leuven [BB09, 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, SCS05, QCC05a, SCS05b, ZK05], Liaw [TJ01b], Liberty [Lan04b, Ano00e, Ano04e], librarian [PBV08], Libraries [Fin02, MK05b], Library [KSL02, Lau05, Law09b], Libre [Jen09], license [Ano00h], Lies [Gan01b, Sch00d, Swa01, Che00b, Ste05c], Life [Cop04b, GSB+04], lifecycle [HL06], Lifetime [Coc01a, CPG+04], Lifting
Light [WT02]. Light-Weight [WT02]. Lights [Gei03]. Lightweight [EPP+07, Mal02, CH07a, CL09, MP07].
Like [Coc02a, PSC+02, VMSV05, BCDM00, CWH00, DLP+09, Egh00, EBS01, Gou04, HSL+02, HL04, SKU+00, SLL+00].
LILI [JJ02]. LILI-128 [JJ02]. Limit [Das08].
Limitations [Gua05, Fis01a, LG09]. Limited [AK02a, LCD07, Buh06, Tse07].
limiting [CCK04b]. Limits [CWR09].
Linear [CC02b, CHY05a, KTC03, YY05b]. Line [Cho08a, DL98, Jan08a, Lai07, Lu02, SK06, YLLL02, Bau05, BCS02, DL07, Luk01, Shi05].
Linearization [DDG+06]. Linearly [ADD09]. Lines [SP04].
Linguistic [CDR01]. link [LPV+09]. link-layer [LPV+09].
linkages [ZAX05]. linked [YWWS09].
Linking [GW00]. Linux [Lin02, ASW+01, FR02, Fin01, GJ05, Gan08, GPR06, JZ04, Lin02, Mor03, Pri00, Shu06, Sta02b, Sta05].
LISA [USE00c]. list [AGKS07]. Listening [Cas03]. little [Che01d, Lam07, Sch05c]. Live [Lov01].
Lived [GSW00]. lives [FNRC05]. living [BCB+05]. LLL [CKY05, NS05c]. Load [CC08, H0501]. Loads [GH02]. Loan [SOOI02].
Loaning [Bla01c]. Local [NABG03, Lav09]. Locality [MFS+09].
Localization [WLT05b, CKL+09]. Locally [Vad03, Yek07]. Location [HY01, KZ01, LNL+08, Buh06, SG07].
Locations [Kra02b]. Log [Gen00b, HN04].
Logarithm [CNS02, Che04b, CCW02, GV05, GPP08, LW02, Hsu05a, HL05d, JLL01, LL04b, LH05, Sch01e, SCL05, SLC05, Yas08]. Logarithmic [EGK08]. Logarithms [CS03a, JL03, LHL03a, LTH05, PLJ05a, QC805a, Sha05c, Sha05d, SCS05c]. Logging [Fox00, MT09]. Log [BPST02, Cop04b, KBD03, KS06b, Li01, Nie02d, SQ01, SC01, Tee06, TV03, BDNN02, BD04a, DZL01, SW02, WLB05, dH08].
Logic-Based [KBD03]. Logical [Asl04b, Kra07, SP03, CLK04, Zha08].
Logics [IK03, IK06]. Login [LL05c, CCK04b, CJT01]. Logistic [KJ01].
Logo [LZ09]. London [Pag03, Top02].
Long [ABRW01, Dur01, Eva09, GSW00, Gro03, PCC01, Zho06, BM06, ISO05, LG04, SGMV09]. Long-Lived [GSW00].
Long-Term [ABRW01, Dur01, BM06, ISO05, LG04, SGMV09]. Look [Bon07, Has00, lut03, Sye00, Hen06b].
Look-up [Has00]. Looking [ASW+01, Ano01j, Cla00b]. looks [Nis03a].
Lookup [MFFT05]. loop [KVN+09]. loop-level [KVN+09]. Loopholes [Ste01].
Lorenz [GHdGSS00, Sal00a]. Lorenz-based [GhdGSS00]. Losing [Sta05]. LosLobos [Pri00].
Loss [LHS05, BC05b, Mit00]. Lossy [AIP01, HSKC01, WP08, Asl04a]. Lost [PY06, Rob02, Rob09]. Lösung [Ano04c].
Lot [Cla00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [QSE00].
Louvain-la-Neuve [QSE00]. Low [Ano00d, BM01b, CH07c, GST04, HNZI02, HGR07, JPB02a, KMB09, RMH03b, RMH03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09b, Fan03, HLL03, LGKY10, LCO4a, SK03, WHH05, WH06, WY05, ZY07].
low-computation [Fan03, LC04a].
low-cost [CL09]. Low-end [SU07].
Low-Exponent [SZ01]. Low-Weight [CH07c].
materialized [MSP09]. Materials [SLT01].
Math [SR06, McNo3]. Mathematical
[AUW01, Cas06, FF01b, GL05, HPS08,
Kat05b, Yon06, GKS05, Hiil05, Sin09].
Mathematics [BP06, Lew00, Nie02d, Wa00, Gar04,
Sch00a, Sch01c, S+03, Sch04a, Sch04b].
Matrices [TL07, CFVZ06, LMTV05].
Matrix [CV03, BF06a, OS07].
Matroids [CDG+05].
Matsumoto [DDG+06, YG01a].
Mature [Tro08].
Max [Di01].
maximal [H+00, HJW01].
maximizing [GSK09].
maxims [Bau00, Bau02a, Bau07].
Maximum [KMT01, ZC00, DW01].
May [ACM00, ACM02, ACM05c, ACM06,
ACM08, ACM09, Bih03, CC04a, Cra05a,
DRS05, IEE01b, Kn02, KNP01, MJ04,
MS05a, PM00, Pfi01, Pre00, TLC06, Uni00f,
Uni00c, YKL02a, Pau02a, YJ00].
Mbps [LMP+01].
McClure [Gum04].
McEliece [CFS01, KI01a, KI01b, Loi00, LS01c, Sun00b].
McEliece-Based [CFS01].
McFarland [Car02].
McGraw [Gum04].
McGraw-Hill [Gum04].
MD4 [DG02, WFLY04].
MD5 [An009c, Eke09, For09, WFLY04].
Means [LMHCETR06, Nis03a].
Measurement [An009c, cko1, C009b, FXAM04, RW07].
measurement-based [FXAM04].
Measures [CB01, QSO1, GSK09].
Measuring [Si06].
Mechanisation [Bel01].
Mechanism [Eva09, LXM+05, WY02, CL08,
CL04, GH08, LCP04, ME08b, RFR07a,
RFR07b, RFR07c, WAF00].
Mechanisms [BACS02, CJK+04, Her09b, Lin00a, MD04,
Mir05, Pip03].
mechanized [dH08].
media [And08a, Hei07, CBB05, An02d].
media-streaming [CBB05].
Mediated [DT03, CG06].
mediator [SBG05].
mediator-free [SBG05].
medical [AL07].
Medicine [MYC01, Maa01].
Meet [Cla00a, HG07].
meet-in-the-middle [HG07].
meeting [Jef08].
Meets [Way02a].
Melbourne [IZ00].
Member [CTH08].
Membership [NBD01, Fis01a].
Merkle [CDMP05, JLS03].
Mersenne [An009c].
Mesh [LPZ06, ZTP05, KB09, LZP+04, YPSZ01].
Meshes [BGI08, Lav09].
Message [BKR00, BR02, BWBL02, BDF01b, CV03,
Coc02b, FIP02a, FGM00b, GTZ04, Jul01,
OM09, SNR04, WS03, Zol01, BPS08,
CCH05, CJ05, Gav08, HW05, Kar02, MD04,
MS09c, Sha04b, TJC03, Wu01, ZF05,
ZAX05, ZCW04].
Messages [Ara02, AR01, BR00b, CHJ+01b, DS05b,
Sch09, Wri05, Zhe06, Alv00, An08c,
BG+02, Bi02, BB79, Lm09, SP79].
messaging [Opp01, RR05].
meta [SM08, PLJ05a, QCB05b, Sha05d].
Meta-He [PLJ05a, QCB05b, Sha05d].
meta-learning [SM08].
metadata [CDS07, FJ04].
metamorphic [CSW05].
Metaphor [CNB+02].
Metering [BC04b].
Method [BDTW01, GHK+06, GL00, Gro01,
HRS02, HQ05, JKK+01, LL02, Ml02,
OK02, OT03a, OT03b, SOHS01, TIGD01,
TSO00, WH09, WNY09, ZL05, AMRP04,
DwWmW05, Gut04c, JL03, MSP09,
MKF+06, WG02, WWTH08, kWPLW01,
WLW04, YCO09c, YCL07, CHJ+01a].
Methodologies [SPMLS02, NdM04].
Methodology
Methods [BCDM00, CFRR02, FD01, Kin00, Lan00d, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Bau00, Bau02a, Bau07, BGM04, BCHJ05, CM05b, GKS05, JZCW05, LMSV07, 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 [dCdVS05]. military [Ark05]. Million [Ran55, Ran01, Ano03a]. MIME [Dav01b, Dav01c, LG09, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [FBW01, FGMO01, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LPM05]. Mining [LP00, Lut03, HLL+02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [CC05e]. MinRank [Cou01]. Minutiae [UBEP09]. Minutiae-based [UBEP09]. Misbehaving [JQY01, SB05b]. Misinformation [CZB+01]. Missed [TvdKB+01]. MIST [Wal03]. Mistakes [Ste05b]. MISTY [KYHC01, Küh01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Küh02b]. Mithra [Frec03]. Mitigating [NLD08]. Mix [JJ00a]. Mixed [SKR02]. Mixes [Mi03a]. Miyazaki [WHL03]. MMM [GKS05]. MMM-ACNS [GKS05]. Mnemosyne [RH02, HR02]. Mobile [Cha05a, CFR02, Dim07, GN06, JP02a, KZ01, KB07, KC02, KHD01, LCK01, Mal02, MM02, PL01, RKZD02, Rs01, RO01, Rot01, SH00, ZYM05, CC05c, CJ03b, CF05, CF07, DHMR07, HP00, HY03, sHCP09, ISTE08, KVD07, XDD00, LC03, LC04a, Lin07, LKZ+04, Par04, Pau02a, SSM+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, CL01a, CS07c, CPhX04, Ch08e, CT09, DP04, DFSS08, Din01, Din05, ECM00a, Gra02b, HLC08, KLN+06, KW03, LJL05, MND+04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SFD06, TYZD05, Vad03, WC05, WT02, WvD02, ZGLX05, ZP05, ZS05, BKW03, CUS08, CCGD06, Dam00, DFFS05, GR08, HILM02, LC08, LL08a, LL08b, MS09b, PS04b, SR01, TP07, DY09a]. Model-Based [Sal05b]. Modeling [AADK05, CDD+05, HMvDM07, KS05a, ZP05, La00, SS04]. modelled [BG08]. Modelling [HCD00, JP07, Puc03]. Models [Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01b, SC02b, vOT08]. Modern [Gol99, Mao04, Pag03, SM07b, Swe08, Bud06, Fur01, IM06, KL08, Mol05, SE01, Lu03, Lee03b]. Modes [DGH+04, Dwo03, GD02, Gol01e, HSH+01, JMV02, KJ01, Jut01, KY01a]. Modified [CHC04, HPCD02, JY01, KI01a, ST02, Che08a, CJ01, HWMM03, LL04a, LL05a, kWP0W01]. modifying [CSV07]. Modular [BP05, BKP09, CMJ03, CH07c, Dhe03, FP00, Gro01, Har06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wal01, WL04a, HSD+05]. Modulation [AS01c, Che07a]. Module [An02d, LM00, SGM09, AR08, BG09, Jan08b] Modules
FIP01b, NIS01b, GJJ05, JEZ04, Sei00b. Moduli [Bai01b, GMP01b, Wal01]. Modulo [ACS02, Gon06, Gro03, MFFT05, Zhe01, Wan05]. Modulus [Ano01o, CGH00a, LWW00, MFFT05, Zhe01, Wan05]. Modulus-Based [YW02]. Mollin [Kat05b]. MOM [DJLT01]. MONA [KMS01]. Mondriaan [BF06a]. Money [Ano01a, YKMY01, JP06]. monitor [MK05a]. Monitoring [AK02a, BCS02, Por06, Bej06, GXT08, ZGT05]. Monitors [JT05]. Monks [Eag05, Kin01]. monoalphabetic [GPG06]. monolithic [GHdGSS00]. Monotones [WW05]. Monsters [And08a]. Money [Ano01a, YKMY01, JP06]. monitor [MK05a]. Monitoring [AK02a, BCS02, Por06, Bej06, GXT08, ZGT05]. Monitors [JT05]. Monks [Eag05, Kin01]. monoalphabetic [GPG06]. monolithic [GHdGSS00]. Monotones [WW05]. Monsters [And08a]. Monte [B09, Sug03]. Monterey [USE02c]. Montgomery [CH07c, HKA05, NMSK01, OS01, PS04a, TSO01, Wal01, WS03]. Montgomery-Form [OS01]. Montpellier [KM07]. Montréal [ACM02]. Morocco [IEE09a]. MorphoSys [Tan01]. MOSS [Dav01b]. Most [GG05a, Shp02, Yun05]. Mothballed [Bar00c]. Motif [Bi09]. Motion [EFY05, hKLS00, WMDR08]. Mountain [JYZ04, mouse [HLwWZ09]. move [Jac00]. movement [HLwWZ09]. MP [MP07]. MP3 [DRL09]. MPEG [LHS05, MLC01, SO07, ZWDW07]. MPEG-4 [SG07]. MRF [Che01a]. MRM [TIGD01]. MSXML [TEM01, Hei01]. Mu [CJT03]. Much [Che01d, Con09]. Multi [ARR03, Multi-designated [LV07]. Multi-Domain [CJK+04]. multi-factor [BSSM+07]. multi-hop [NC09]. multi-linear [LLL04]. Multi-party [CD00, CDG+05, FGM001, FWW04, HM01b, LLL04, CLOS02]. Multi-property-preserving [BR06]. Multi-Proxy [ZJ09, HC04b, LW05c, TY04]. Multi-Receiver [CCD07]. Multi-recipient [KUR01]. multi-scroll [HHYW07]. multi-secret [CC05a, CHY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server [Tsa01, LHL03b, Tsa08, TLW05]. Multi-Servers [HS07]. multi-signature [HW05, HC04b, HL04, LC05b, LW05c, TY04]. multi-stage [CHY05b]. Multi-trapdoor [Gen04a]. Multi-user [BBM00, DLY08, GMLS02]. multi-valued [DZL01]. Multiagent [ZS05]. Multiagent-Based [ZS05]. multibit [TND+09]. Multicast [AIP01, BPS00, BDF01b, ASW00, Asl04a, CBB05, GIKR01, GL06b, JA02, KB09, MP08, PCS03, YC08, ZCW04]. Multicollisions [Jou04]. Multilevel [BN04]. Multimedia [AAK09, FMS05, GA05, HL07, LRRW07, S05, WLLW09, DY09a, DU05, LA00, Ren09, SO07, YC08]. Multimodal [PY08]. Multipartite [HR13]. Multiparty [BCC02, BGOY08, CD00, D03, DI05, GIKR02, OZL08, PMRZ00, CDD00, HT04, IK07]. multipath [SK05b]. Multiple [AK+01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, DK05, Har00, HZL05, HL07, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CJ04, DM07a, HL00, KCI09a, MN14, Sha01d, SW05a, TCC02, YW05, YSH03, YRY05b]. multiple-key [Che04a, CJ04, SW05a, YW05, YSH03, YRY05b]. Multiple-Precision [HZZL05, MN14]. Multiple-watermarking [Che08b]. Multiples [HR00]. Multiplication
[AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02c, KKIM01, Möller02, NMSK01, OS01, Tan07a, Wal01, BINP03, DwWN05, FP00, GD05, Has00, Mis06]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07].

Multiplier [CMJP03, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver [HSZI01]. Multiresolution [hKLS00, YPSZ01]. Multiset [aSM01]. Multisignature [Tad02, CWH00, CL04c, CCH04, He02, LWL09, YC01, ZHY03, ZS05, Bru06, CJP03, CJS08, Coc01a, DWML05, GKS05, HLL02, LPV09, MW06, ME08a, MSC03, Mis08, Pri00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wy05, YLT06, ECM00, ECM00b]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver [HSZI01]. Multiresolution [hKLS00, YPSZ01]. Multiset [aSM01]. Multisignature [Tad02, CWH00, CL04c, CCH04, He02, LWL09, YC01, ZHY03, ZS05, Bru06, CJP03, CJS08, Coc01a, DWML05, GKS05, HLL02, LPV09, MW06, ME08a, MSC03, Mis08, Pri00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wy05, YLT06, ECM00, ECM00b].

Network-Attached [RCBL00]. network-based [HLL02]. Networked [Sch00, Sch00, LB05]. Networking [ACM01b, Ros07, M001, VM03]. Networks [AEAQ05, BJLS02, CGM07, DBS06, Fin06, GPC08, Gor05, JKR01, KZ01, Ken02a, KH05, LNL08, NAB03, PR01, RKZD02, Sin01a, WT02, Zea00, ZNY08, ZWY02, AJ08, As04a, BBG02, BC05c, CCMT09, CGP03, CBD05, DMR07, ETMP05, HJ07, HMvdLM07, JRR09, KXTZ09, KYM08, KB09, KD07, LD06, LHC08, LW05a, LLH06, Lin07, LNO4, Lop06, LKZ04, MWS08, MJF08, MS09b, NC09, NLL08, PCS07, PS08a, Pat02b, SLP07, SSM08, TP07, TM06, TCR03, TW07, WDL09, XwWL08, YC07, ZSN07, ZBLvB05, An02d, CS08b].

Neural [KMS02, PZL09, PR01, YC01, YC07]. Neural-Network [YC01]. Neuve [QS00]. Nevada [ELvS01, EEE01]. Never [Wei00, Hau06]. Newfoundland [NH03]. Newman [Pag03]. Newmanry [Sal01a].

N [Mar05a, AOS02, KOM01]. NAF [OT03b]. Names [Coc01a, Sha02, Ard05, CGV09]. Naming [An01b, BH00b]. Nanotechnology [RR03a, RR03b]. Naor [Zha06]. Napoleon [Urb00].

narrowed [Sch04d]. narrowing [MT07]. NASA [An02c, Wil99]. National [Lan00a]. National-Scale [BWE00]. Natural [ARC01, Top02, WMS08]. Nature [Pag03]. Naval [LBA00, Go00]. Nazi [Hau06, KS04]. NC [AIK04]. nCipher [An003g]. NCP [S00]. NCR [LBA00]. Near [BC04a, DPD05]. Near-Collisions [BC04a]. Necessary [LCK03, MN01].
News [Ano03d, Bar00a, Bar00b, Bar00c, Cla00a, Coc01a, Coc02a, Coc02b, Coc03, Eng00, Fox00, MYC01, MP00, PM00, Pau02a, Pau02b, Pau03, Pau09, Pri00, CAS03, CAC06, Sta05, Raj06]. Newton [KT06]. Next [ESG*05, McLO6, TV03, Van03, Web08, BD04b, ISTE08, RR03a, Ros04]. Next-Generation [ESG*05, Web08]. NFA [DIS02]. NFS [Sta02b]. Nice [DS06, JJ00c]. Nimbus [Fur02a, Mac00]. Nine [Tat05]. Ninth [USE00d]. NIST [BG07a, Dra00, Hir09, Kel05a, Kel05b, RRS06, SF07]. NIST-Recommended [Kel05a, Kel05b]. NMAC [RR08]. NMAC/HMAC [RR08]. NNAF [DwWmW05]. No [Sta05, Sty04, Uni00g, Wei06, Wei05, CC05b]. Nobel [MNT*00]. Node [BRTM09, Fox00]. Nodes [ZYN08, RAL07]. NOEKEON [DPVR00]. Noise [BKW03, GA05, MPSW05, SDMN06, MS09a, PC00]. noise-based [PC00]. Noise-Resistant [KEL05a, Kel05b]. NMAC [RR08]. NMAC/HMAC [RR08]. NNAF [DwWmW05]. Noise [BKW03, GA05, MPSW05, SDMN06, MS09a, PC00]. noise-based [PC00]. Noise-resistant [KEL05a, Kel05b]. NMAC [RR08].
NTRUSIGN
[HHGP+03, HHG06, HWH08, ZJ09].

NTRUSign-Based [ZJ09]. Number
[BIP05, BST03, BK06a, Che08b, Co09, CD01a, CFS05, Dic03, DGP07a, DGP07b, DV08, Esg05, EH06, Fin06, Gom06, GPR06, Hig08, Int03, Kat05b, Ke05a, Kel05b, Ket06, KMHCT06, LNS02, MNP01, NR04, NNAM10, RSN01, TWNA08, TL07, TZT09a, TZT09b, Vav03, Wal00, Yan00, YKLM02b, Aam03, AUW01, BS02, BK07, Bel08, BGP05, BG09, BG07a, BGL03, CFY10, CNPQ03, CO09b, DIM08, DGP09, FP00, HG05a, HGNS03, HLwWZ09, HP01, JAW00, JL03, KH08, KSF00, Kin01, Lam01, LGM06, MFK06, SHP03, Ste08, SR07, ST01b, Tat05, Wag03, Was08b, XSWC10, YZEE09].

Number-Notation [Eag05, Kin01]. Number-theoretic [NR04]. Numbers [BCGH11, HSR+01, HBF09, Ifr00, MN01, ST03b, AG09, HW98, KB39, Ki01b, MKF+06, SS03, Slp05, Tip27]. numeric [AKSX04]. Numerical [WWL+02]. numerically [Sav04]. Numerous [CC08].

NURBS [Ben00]. NUSH [WF02]. NY [HR06, IKY05, KJRI05, Sch01d, YDK06, An011, NIS00]. Nyberg [Ara02].

O [Kat05b, Puc03]. OAEP [Man01, BF05, BF06b, Bon01, FOP01, Sh01].
Obfuscated [NS05b]. Obfuscating [BGI+01]. obfuscation [CT02]. Object [RSA00e, DHL06, MM01, ST06]. object-oriented [DHL06, MM01].
Objects [CCM05, ZTP05, PB01, Wh09].
Oblivious [CT08b, Din01, FIP05, IKNP03, SDF01, GKM+00, KKL09]. obscurity [MN03]. Observability [JQYY01]. observers [JL04]. Obstacles [KM04a].
Obtaining [Bar06b, BP03b]. OCB [RBB03]. occur [Web02]. Ocean [MYC01].

October
[AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST+05, TTZ01, USE00b, ZHY03].

Octopus [Cl00b]. Oded [Lee03b]. odyssey [Go08]. Oedipus [Lav06]. Off [AJ008, Coc02b, Oec03, Shi05, YLLL02, Bau05].

Off-Line [YLLL02, Shi05, Bau05]. Offering [YC08]. Office [Uni01]. officer [Kov03].
Official [BP01b, Coc02b]. Offline [DJ06, ST01b, WV01]. Offs [PS01c]. OH [BD08]. oil [RD09]. Old [Eva09, Lov01].

On-Demand [SEF+06]. On-Line [Lu02, BCS02, Luk01]. One [AK02a, BYJK08, CHL02, Che03, DIS02, Di01, DV01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, Ko01a, Ko03, Ko00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00e, XXYX11, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CA04, CC05d, Di03, DS02, GKK+07, HR07, HRS08, HLTJ09, JZ09, Ko07, KPP05, KKK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05a, Tsa08, YW05, YRY05b, 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, Sh000a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJO4, GKK+07, HR07, HRS08, JZ09, Ko07, KPP05, KKK03, LW04, LPM05, LQ08, Mic02a, Poi00, Tsa08, YW05, YRY05b, ZW05a].

One-Wayness [KI01a, PV06b]. On-going [Sam09]. Onion [CL05]. Online [BDF+01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAVY09, Vo05, 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 [CBZ+01]. OOSD [CZB+00]. Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Ki02s, Lin02, Mea01, PM00, VDKP05, Ano03d, ETMP05, McA08, Bar00b, Lin02]. Open-Ended [Kus02]. Open-Secret [Joh05]. Open-Source [Bol02, Gut00, McA08]. OpenCard [HF00]. Opening [CAC03]. OpenSSH [Bau01c, Sta02b, TvdKB+01, Hos06a, Mos06]. OpenSSL [Fri01, Res01a, Res01b, Sti06a, VMC02, WMC02, YRS+09, B005]. Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL+08a, CGL+08b, CGL+08c, DGP09, KWDB06, MHP06, SETB08, TKP+08]. Operation [BR02, BKM07, Dw03, EP02, Gol01e, HSH+01, JKRW01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BKM07]. Operational [WA07, GMG00]. Operations [BIP05, IMM01, KDO01, KS05c, LS01b, Arko05, Dug04]. operator [Wan05]. Operators [CH00]. opinion [BHM03, GS07b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Pau02b]. Optimal [Bai01a, BDDS03, CHJ+01b, CDF01, CF02, DSP05, DNP07, GMW05, IR01, KO04, KS03, LZ09, Man01, MPSW05, MP08, SNR04, YY01, vDW04, BCD06, HKS00, LSH03a, LSH03b]. optimality [NK06]. Optimised [TL07]. Optimistic [CC00, DLY08]. Optimization [Hro03, Ken02a, Kre05, KY01, SMTM01, TLYL04, WPP05]. optimized [LC03]. optimizing [Dwi04]. Optimum [KWP06, OKS06]. option [Mat05]. options [Fri07, Pot03]. Oracle [ABR01, Abe01, Abe04, BF05, Chi08e, Gra02b, Nie02b, Pas03, Ano02e]. Oracle [BNPS02, BB04, KG09, RG09]. Order [AKSX04, Bai01a, CV02, KCP01, KCP01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, C003, JZCW05, KS06b, QPV05]. Order-Specified [Tad02]. ordered [HY03, WL05]. Ordering [Mea04]. Orders [HJW01, PS02b, HM00, Hai00]. Ore [CHH01]. Oregon [AC00, BCD09]. Organization [JG07, MMZ00, MP00, C002]. Organizational [PT07, BJ02]. organized [AUW01]. Oriented [HR00, LCL+01, NNAM10, SKU01, ZCC01, CHC05, CWR01, DHL06, HWC04, LL06, LWZH05, MWM01, Sa02, Sha03c, T01a, WHH08]. Origin [MABJ06, MD04]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Orsay [DPT+02]. OS- [CRSP09]. oscillator [BGL+03, GB09]. oscillator-based [BGL+03]. oscillators [SPG02]. OSNP [HLT09]. Other [BF05, Ngu05, Wri05, Cla00b]. Otherworldly [MYC01]. Ottawa [AMW07, MZ04]. our [Sta05]. ourselves [Fur05]. Outbound [Smi02]. Output [Dic03, JY00]. Outsourcing [HL05a]. outsourced [MSP09, MNT06, YPPK09, YLC+09]. overcontrolled [CHC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, IN05]. overhead [HR07, IKOS08, 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]. P [Puc03, AKS02, KR03]. P1363 [IEEO0b]. P2P [BRTM09, STY07, WN02, YLR05]. P2Ps [LH+08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08].
Pad [LDM04, DS02]. Padding [AR01, BCCN01, CJNP02, KO03, LS01a, Man01, Vau02]. Paddings [NP02b]. PadLock [Lud05]. PadLock-wicked [Lud05]. Page [IEE00b]. PageRank [IEE00b]. Pages [Fal07, Rot07]. paging [SZ08]. PadLock-wicked [Lud05]. PadLock [Lud05]. PadLock [Lud05]. PadLock [Lud05]. Paradox [Che01b]. Paradigm [BN00a, CS02, Gol03, KD04, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Paradise [USE00b]. Paradox [Che01b]. Parallel [AHHR08, App07, AERM09, CPHX04, CTLLO1, CPNQ03, CNB+02, Dam07, DM00b, JL08, KY02c, Lin01c, MFS+09, PS04a, RHM03b, SS01a, BF06a, FP00, MRT10, OS07, RMPJ08]. parallelism [KVN+09]. Parallelizable [BR02, M602]. parallelizing [Fis01a]. Parallizable [LKKY03a, LKKY03b]. parameter [Wue09]. Parameterizable [KPMF02]. parameterization [LZP+04]. Parameters [LZK02]. Parametric [Vir03]. Paranoid [Bau01a, Bau01b, Bau02a, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06]. Parascript [An02d]. Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Paris [ACM04a, GH05, KN01, NP02a]. Parity [DRL09, KKG03, You01, BKW03]. Parity-Based [KKG03, DRL09]. Park [Cop05, Cop06, Cop10, HS01a, Sal00b, Sal05a, SE01, Sni01b, Wei06, Win00]. Part [Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05]. Partial [BM03b, Cor02, Her06, ABHS09, CP07]. Partial-Domain [Cor02]. Partially [AO00, MSP09, Bau04, Bau03, HCO04a, HY03, HLL03, WL05, WLHH05, WY05, ZC05]. Participatory [CTBA+01]. parties [LKY05b]. Partition [CTH08, WJP07]. Partitioned [DN04], partitioning [BF06a, Che07a, partitions [Sav04]]. Party [K04, Lin01c, MR01a, WW05, WV01, CLOS02, CLC08, CDG05, FGM001, FW04, GCKL08, HM01b, JW01, LHL04b, LLL04, LLS+09, LSH00, YC09a, ZLX99]. Pass [SK00, MT02], passe [Car00]. Passes [Coc03], Passing [Vir03]. Passive [Sha01c, VV70, RW70]. Passive-Only [VY70]. Password [BMM01, BMM01, CHV03, CPP04, CS07b, CC01b, D03, GMR05, Har01a, Har01b, KTY01, LSH03a, LSH03b, MPS00, Mac01, MSJ02, Ngu05, SBEW01, SY06, WHL05, YS04, ZC05, CC04b, CCK04b, CY05, DG06, FLZ02, Fur05, GL06a, HTJ08, JM07, JPL04, Jua04, KL03, KJY05, KTC03, KCL03, Ku04, KCC05, KHL05, LLH06, LFW04, LH03, LC04a, Pha06, Sco04, SLH03, Shi05, WL03, XWL08, YW04a, YWC05, YS02, YPKL08, ZD06]. Password-Authenticated...
[BMP00, DG03, KOY01, MPS00, Mac01, MS02, 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, Dew08, ZSN05].

**path-based**

[CCD+04].

**Path-quality**

[GXT+08].

**Pattern**

[ABM08, BihKB09, BLP06, BCCN01, LS01a, TIGD01, Buh06, LYGL07].

**Pattern-based**

[BLP06].

**Patterns**

[DD02, MP06, WCJ09, JLC07].

**Pay**

[Joy03a].

**Pay-as-you-watch**

[Joy03a].

**Payload**

[KC09a].

**Payment**

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

**PC**

[BW01, Ste05c].

**PCIXCC**

[AV04].

**PCKS#7**

[Dav01c].

**PCPs**

[FS08].

**PCs**

[BDET00].

**PDA**

[GW08].

**PDF**

[ISO05, CNB+02, ISO05].

**PDF/A**

[ISO05].

**PDF/A-1**

[ISO05].

**Pearson**

[Pez04].

**Pebbling**

[DNW05].

**Pedersen**

[GJKR03].

**Peer**

[Art04, HR02, RH02, ATS04, LLY06, MPHD06, PI06, WCJ05, YI04].

**Peer-assisted**

[Art04].

**Peer-to-Peer**

[HR02, RH02, ATS04, MPHD06, PI06, WCJ05].

**PeerAccess**

[WZB05].

**Peynado**

[YRY05a].

**PEM**

[Dav01b].

**Penguin**

[Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a].

**Pennsylvania**

[IEE05a, IEE08].

**People**

[ASW+01, CG05, Lov01].

**perceptions**

[WDCJ09].

**Perceptual**

[EFY+05].

**Perfect**

[AJO08, CLLL00, DN02b, DSS01, Sun00a, DMO7a, 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, WBRF00, WWCW00, WS02, XH03, YEP+06, Zea00, AKNRT04, BVP+04, BZP05, CLK+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTW07, SK03, YGZ05].

**performance-friendly**

[CRSP09].

**periodic**

[XQ07].

**Periods**

[KKH03].

**Perl**

[Sal03b].

**Permutation**

[DM00, HR+01, YKMY01, Has02, HP00, SH00].

**Persistent**

[AGT01, ST06].

**Person**

[KJR05, LTL+04, PK01, BS01b, KN03, Li05, LST+05, PY08].

**Personal**

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

**Personalised**

[TNG04].

**Perspective**

[LL01].

**Perspectives**

[BMV06, SM08].

**Perturbation**

[HHW08, ZY08].

**Pervasive**

[BDhKB09, JW05, LKH09, Lut03, Lut03].

**PET**

[MS05a].

**Peter**

[For04, Uzu04].

**Petersburg**

[GKS05].

**petitions**

[Cal00b].

**Petri**

[LKJ01, AADK05].

**PGP**

[Mcl06, Ano00h, BCH+00, Dav01b, Dav01c, JKS02, Luc06, Opp01].

**PGV**

[BR02].

**pharaohs**

[Pin06].

**Phase**

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

**Phase-Conjugate**

[Ig02].

**phase-shift**

[Che08a].

**Phil**

[Bar00a].

**Philadelphia**

[IEE08].

**Philosophy**

[Cop04b].

**phishing**

[Bel04].

**Phone**

[CAC03, Fox00].

**Photonic**

[TWN08].

**Photonic-based**

[TWN08].

**Photons**

[Bar00c].

**Physical**

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

**Physicist**

[BZ02].

**physicists**

[RP00].

**Physics**

[MYC01, Sch06b, BEZ00, BEZ01, Duw03].

**physiological**

[RFR07a, RFR07b, RFR07c].

**Pi**

[OS08].

**PIC**

[Fin02].

**pick**

[Cl00b].

**Picks**

[PM00].

**PicoDBMS**

[PBVB01].

**PicoDMBS**

[BBPV00].

**Picturing**

[Pau03].

**Piecewise**

[LL+01].

**Pigeon**

[Pe01b].

**piling**

[Kuk01].

**piling-up**

[Kuk01].

**PIN**
GH02, HQR01, HJW01, Ina02a, Ina02b, IIT03, Kan01, LMY05, LCD07, Lu03, LKK05a, MM02, MSU05, OM09, PBD00, Pel06, Poi02, Poo03, Roy00b, Sug01, Wei04, YSS+01, Bro05b, DKL+00a, Har05a, KSW06, Luc06, Mos06, MSV04, Sha01a.

Practice [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti95, Sti02, Sti06c, Lu03, Spr03].

practices [CF05, Ste02].

practitioners [PP09].

pragmatic [BMW02b].

Prague [MJ04].

Pre [Adl03, AA08].

pre-processing [AA08].

Precise [Wal01].

Precision [HZSL05, SR06, LMC+03, MN14].

Precomputation [SLG+05].

predecryption [RSP05].

Predict [Dic03].

predictable [Bel08].

Predicting [AG09, BGPGS05].

Prediction [AKS06, SLG+05].

predictive [vOT08].

predistribution [HMvdLM07, JRR09, TP07].

Preface [CGM07].

Prefix [FXAM04, RW07].

Prefix-preserving [FXAM04, RW07].

Prehistory [Ir00].

Preliminary [KS00b, KKS00b].

Prentice [For04].

Prentice-Hall [For04].

Preparations [FJ04].

Prepared [ASW+01].

Preprocessing [BIM00, CKK03].

presence [BIW08, GXT+08, Mi08, VS08].

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

Preserve [NNT05].

Preserving [DN04, KS05c, LP00, Mio3a, YWD08, AKSX04, BR06, BSSM+07, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07].

President [Gen00a].

Press [Inr03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03].

Pressure [HWH01].

pretty [vOWK07].

Prevent [FOBH05].

Preventing [CS07b, CCL09, HSW09, IY05, RG05, DMS07].

Prevention [JT05, PZ01, PZ02a, Gei03, Sni03].

Price [AS01a, Bra01b].

Primality [BT02, Che03].

Prime [ACS02, Bai01a, Har07a, Pau02a, WS03, JL03, dW02].

Prime-detecting [Har07a].

Primer [KLB+02b, Lad06].

Primes [An003f, SZ01, HLLL03, Ste08, AKS02].

Primitive [CFS05, IYK02, IMM01, ST01a, ST02, IYK03].

Primitives [BDFP02, CHL02, FGMO01, Gol01d, Ngu05, RR00, BDFP05, Gar05, JZCW05, RAL07].

Princeton [Gen01].

Principal [CZK05].

Practical [MW02b].

Prague [MJ04].

Precise [Wal01].

Precision [HZSL05, SR06, LMC+03, MN14].

Precomputation [SLG+05].

predecryption [RSP05].

Predict [Dic03].

predictable [Bel08].

Predicting [AG09, BGPGS05].

Prediction [AKS06, SLG+05].

predictive [vOT08].

predistribution [HMvdLM07, JRR09, TP07].

Preface [CGM07].

Prefix [FXAM04, RW07].

Prefix-preserving [FXAM04, RW07].

Prehistory [Ir00].

Preliminary [KS00b, KKS00b].

Prentice [For04].

Prentice-Hall [For04].

Preparations [FJ04].

Prepared [ASW+01].

Preprocessing [BIM00, CKK03].

presence [BIW08, GXT+08, Mi08, VS08].

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

Preserve [NNT05].

Preserving [DN04, KS05c, LP00, Mio3a, YWD08, AKSX04, BR06, BSSM+07, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07].

President [Gen00a].

Press [Inr03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03].

Pressure [HWH01].

pretty [vOWK07].

Prevent [FOBH05].

Preventing [CS07b, CCL09, HSW09, IY05, RG05, DMS07].

Prevention [JT05, PZ01, PZ02a, Gei03, Sni03].

Price [AS01a, Bra01b].

Primality [BT02, Che03].

Prime [ACS02, Bai01a, Har07a, Pau02a, WS03, JL03, dW02].

Prime-detecting [Har07a].

Primer [KLB+02b, Lad06].

Primes [An003f, SZ01, HLLL03, Ste08, AKS02].

Primitive [CFS05, IYK02, IMM01, ST01a, ST02, IYK03].

Primitives [BDFP02, CHL02, FGMO01, Gol01d, Ngu05, RR00, BDFP05, Gar05, JZCW05, RAL07].

Princeton [Gen01]. principal [ZL04b].

Principle [CZK05].

Privacy-Enabled [Por06].

privacy-enhanced [ZSM05].

Privacy-Enhancing [SE09].

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

Private [AF04a, AFI06, BDF+01a, BIM00, BY03, BSW09, BJLS02, BGW05, ISW03, KO00, OS05, SDMN06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PLJ05b, Sum02, YRS+09, ZY08, ECM00a, ECM00b].

Private-Key [BY03, KY00, PLJ05b, Sum02].

prize [Fox00, Coc02b, MNT+00].

PRNG [HSS04, Mur02, SF07].

Proactive [DBS01, FMY01, JS05, ZSV05].

Probabilistic [CCW02, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLMM05, Ga099, JZCW05, KY00, MRST06, PBMB01, dH08, Neu04].
Probability [KMT01, MNT00, DLP09].

Probing [ISW03]. Problem
[AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK+02, Con01, CLZ02, DIS02, DHRO, FL06, Gen03, GV05, GPP08, KK02, LNS02, NBD01, Wag02, BKW03, CGHG06, CJT04, DLMM05, HGNS03, Hsu05a, LHY05, LD01, Luk01, Pei09, Shp05, SCL05, WL02, Whi09, Yas08, KM04a]. problem-solving [Whi09].

Problems [BI05a, Can06b, Hro03, MV03a, OP01a, KXD00, LMTV05, LMC03, RSS04].

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

Processing [ISSZ08, KLB+02b, PCK02, AA08, AA04a, Ayo06, YPSZ01]. Processor
[An02e, BBGM08, EP05, FBWC02, FZH05, GC01b, Int00, KBD03, KPMF02, TYLL02, ST03a, SHL07]. Processors
[TLYL04, CW02, CRSP09, Geb04, LJ05a, YGZ05, YLT06, ZYL05]. Procurement [Lad06]. produce [Zir07]. producing [SOIG07]. product [KSWH00, Sun02].

Products
[ACS02, An02d, An02e, Kn07, An00c].

production [Wal04]. professional [Dew08, vT00]. proficiency [Dew08].

Profiles [MV01, PJK01]. Program [H¨of01, Bec02, GGH+08, Kov03, KH03, CS08b].

Programmable
[Dam07, GC01a, HV04, Smi02].

Programmer
[Wil01b, Bon00, Che00a, DKK07].

Programmers
[Coc01a, Wei04, Gon09].

Programming
[ASW+01, An02d, Coc03, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJ01b, AJ01b, CW07, Nis03a, VM03].

Programs
[BGI+01, Aryk05, SLTB+06].

Progress
[RK06, KS00, RD01, Roy00a, VY01, AC01a, AC03a, AC03b, AC03c, AC04b, AC05b, AC06, AC10, AL06, BD04, BS01b, Bi03, BCDH09, BD08, CC04a, CV04, CH00, Des02, DF02, LOL06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE04, IEE05b, IEE06, IEE08, IEE09b, IY04b, JF08, JM03, Joy03b, JQ04, KJR05, KGL04, Kim01, Kim02, KN03, Kn02, KP01, KN01, KM07, Lai03, Lee04b, LLT+04, MMV06, MJ09, MS02c].

Proceedings
[Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sra05, Syv02, TB302, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZHY03, BCKK05, Cra05a, DV05, DWLM05, DKU05, GKS05, IKY05, Kii05, Li05, LST+05, Men07, Poi06, Sho05a, Son00, dCdVSG05].

Process
[Kwo03b, MNT+00, BDFP02, HL06, MRST06, VKS09]. Processes
[BDP02, ALV02, BDNN02, Whi09].

Processing
[ISSZ08, KL+02b, PCK02, AA08, AA04a, Ayo06, YPSZ01]. Processor
[An02e, BBGM08, EP05, FBWC02, FZH05, GC01b, Int00, KBD03, KPMF02, TYLL02, ST03a, SHL07]. Processors
[TLYL04, CW02, CRSP09, Geb04, LJ05a, YGZ05, YLT06, ZYL05]. Procurement
[Lad06]. produce [Zir07]. producing [SOIG07]. product [KSWH00, Sun02].

Products
[ACS02, An02d, An02e, Kn07, An00c].

production [Wal04]. professional [Dew08, vT00]. proficiency [Dew08].

Profiles
[MV01, PJK01]. Program [H¨of01, Bec02, GGH+08, Kov03, KH03, CS08b].

Programmable
[Dam07, GC01a, HV04, Smi02].

Programmer
[Wil01b, Bon00, Che00a, DKK07].

Programmers
[Coc01a, Wei04, Gon09].

Programming
[ASW+01, An02d, Coc03, LMHCETR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03].

Programs
[BGI+01, Aryk05, SLTB+06].

Progress
[RK06, KS00, RD01, Roy00a, VY01, AC01a, AC03a, AC03b, AC03c, AC04b, AC05b, AC06, AC10, AL06, BD04, BS01b, Bi03, BCDH09, BD08, CC04a, CV04, CH00, Des02, DF02, LOL06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE04, IEE05b, IEE06, IEE08, IEE09b, IY04b, JF08, JM03, Joy03b, JQ04, KJR05, KGL04, Kim01, Kim02, KN03, Kn02, KP01, KN01, KM07, Lai03, Lee04b, LLT+04, MMV06, MJ09, MS02c].

Proceedings
[Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sra05, Syv02, TB302, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZHY03, BCKK05, Cra05a, DV05, DWLM05, DKU05, GKS05, IKY05, Kii05, Li05, LST+05, Men07, Poi06, Sho05a, Son00, dCdVSG05].

Process
[Kwo03b, MNT+00, BDFP02, HL06, MRST06, VKS09]. Processes
[BDP02, ALV02, BDNN02, Whi09].
Propagation [LJL05, QPV05]. Properties [ABC+05, BM01c, KY01b, LLL+01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].

Property [LP2006, Qu01, Uni00h, WY02, BR06, JRS09]. Proposal [DPVR00, Mac00]. Proposed [Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06]. Protect [ETZ00, BBN+09, WK05]. protected [CYH05, PKH05, ZCL05]. Protecting [Des00c, EHMS00, KY01d, Kra01, LKM+05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LIY04, LS05b, ZYL05].

Protection [CGJ*02, DKFX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XZ01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].

Protections [CGJ*02, DKFX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XZ01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, CT02, Gor05, HLC07, KA09, Kov03, KH03, Kwo03a, LL05b, Per05b].

Provenance [HSW09]. Provers [MV03a]. Provide [AB01, Sch01a]. Providence [IEE07, Sil01]. Provider [LDM04, HILM02]. providers [MV03b]. Provides [OT03b]. Providing [BACS02, BDS+09a, DeL07, Lin07, Par04].

Proving [Che03, FSS01c, GN01, Tee06]. Provision [Kha05]. Proxy [AH05, BCL05a, DKFX05, LC03, LCZ05b, PL01, RD01, Sha03d, ZJ09, AFGH06, CCH04, DY09a, HW03, HW04, HW05, HC04b, KHL09, LLL05b, LH05, LCZ05c, LW05c, PKH05, Sha05b, SHT05, TY04, YTH04, ZCL05]. proxy-enabled [DY09a]. proxy-protected [ZLL05, ZCL05]. psBGP [vOV07].

Pseudo [BH05, FFW04, Gen00b, LLL+01, LHL+08, MP03, SXY01, T09a, T09b, WP03, XXYX11, BG09, CFY+10, GB09, MKF+06, NR04, PLsveLE10, PSP+08, RGX06, SH11, SM11, SL09, WW08, XSWC10, YZEE09].
**Pseudo-Random** [LLL+01, MP03, WP03, XYXYX11, Gen00b, SXY01, CFY+10, MFK+06, NR04, PLSvdLE10, RGX06, SH11, SM11, SL09, WW08, XSSWC10].

**Pseudo-Ransom** [BH05].

**Pseudo-signatures** [FWW04].

**pseudonoise** [HG05a].

**pseudonym** [CG06].

**pseudoprimes** [ZT03].

**Pseudorandom** [BCGH11, CDI05, DN02a, DI05, DP02, Fin06, Fhu02b, FIPR05, GM02a, IYK02, LMCETR06, Nie02c, Aam03, BGPGS05, IYK03, KSF00].

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

**Psychology** [MYC01].

**PUB** [Nat00].

**Public** [ANS05, AUW01, APV05, Ano01n, AEAQ05, AF03, BC05a, BDG+01, BDZ04, Bar00c, BPS00, BBM00, BBDP01, BLM01, Bi00, BDTW01, BST02, CHK03, CHK05, CDM+05, CHM+02, CHKO08, CJ03c, Chi08a, CCM01, CS02, CS03b, DP04, DJ01, Des02, DY09b, DKKY02, DFK+03, ESG+05, ES00a, ED03, FL06, FL01b, GMLS02, GH01, GC01b, GSB+04, Gut04b, HCD02, HR05, HG05b, HR04b, HJW01, HLC08, IE00b, IZ00, Jou02, Kat05b, KKIM01, KM01a, Kim01, KLY02, KKY02, KY02c, KLE+00, KL01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, LXH07, Lin03, Lin00b, MR01b, MR01c, Mo03a, Mol03b, Mü01a, NP02a, NBD01, NSS02, OTU00, PHK+01, Pe09, PR01, Poi02, PHM03, Qu01, RSA00a, RZK02, ST01a, ST02, Sin01a, Smit01c, Ste01, TSO00, TT01].

**Public-Key** [Ano01n, AEAQ05, BC05a, BBM00, BBDP01, BLM01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DP04, DJ01, DFK+03, ESG+05, ES00a, FL06, GH01, GC01b, HR05, IE00b, Kat05b, KKIM01, KM01a, KLY02, KKY02, KY02c, KLE+00, KL01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, LXH07, Lin03, Lin00b, MR01b, MR01c, Mo03a, Mol03b, Mü01a, NP02a, NBD01, NSS02, OTU00, PHK+01, Pe09, PR01, Poi02, PHM03, Qu01, RSA00a, RZK02, ST01a, ST02, Sin01a, Smit01c, Ste01, TSO00, TT01].

**Public-Key-Based** [YKMY01].

**Publication** [Top02, DGMS03].

**Publications** [Bee05].

**publique** [RSA09a].

**publish** [SL05b].

**publish-subscribe** [SL05b].

**Published** [MS03b].

**Publishing** [Ano02d].

**puce** [Car00].

**PUFs** [MPK09].

**Purpose** [Ano07b, Ano07a, ESG+05, GS07a, GP08, SGK08, LJ05a].

**Purposes** [LS05a, FSGV01, PBV08].

**Push** [Pau03].

**puzzle** [LF03].

**Puzzles** [Ano01f, ANL01, CHS05].

**Q** [BFMR02, CH01b].

**Q&A** [Str01b, Win01].

**QCQC** [Wl99].

**QCQS**
[Wil99]. QDSL [CUS08]. QNX [Ano02d].
QoS [JKRW01, Zea00]. QoS-aware [Zea00].
QSIG [ECM00b]. QSIG-WTMAU [ECM00b].
Q’tron [YC07]. QUAD [BGP09].
Quadratic [BT02, TL07, DMSW09, GXT+08, KC09a, WWTH08].
Quality-conscious [DMSW09].
Quantifier [KS06b]. Quantifier-free [KS06b].
Quantitative [Bai08, ME08a].
Quantization [DRL09, WC04, WC05].
Quantum [AC02, ATSVY00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL+05, BBD09, BZ02, BBB+02, BB03, BGM09, BLMS00, BEM+07, Coo3, DFS04, DPS05, DFFS08, Das08, DMS00, EII04, Ett02, GKK+09, GH02, GW00, GRTZ02, HV09, Hay06, Imr03, Ina02a, Ina02b, Kak06, KKL+02b, LB04, LW05b, Moo07, NA07, OTU00, Pal02, PC09, Pot05, Rec01, RK05, Ser06, SR07, Sti11, TO01, Wil99, Wri00, YJ00, YI00, ZLC01, ABW09, Ano03g, Ano06d, BYJK04, BCG+02, Ber09b, BEZ00, BEZ01, BLRS09, DFFS05, Duw03, Eke02, GKK+07, Gav08, Heg09, HHG06, IM06, JZ09, JRS09, JAW+00, Joy00, KK07, KH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Ros00b, Sin09, Sin00, Sm04, UHA+09, BZ02, BDD08, BBD09].
quantum-storage [DFFS05]. quarter [Kob00]. quarter-century [Kob00].
quartermar [Cla00b]. QUARTZ [PCG01].
Quasi [MD05]. Quasi-Pipelined [MD05].
Quasigroup [MSNH07]. Québec [ACM02].
Queen [Rec01, Ros00b, Sin99].
Queenstown [Zhe02b].
query [CKK03, Fis01a, GPC08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC+09].
Query-preserving [GA03]. querying [FJ04, UG08]. question [OC03]. Questions [Ett02, Joh00, Jac00]. Queues [WWL+02]. queuing [CUS08]. quick [Dew08].
R [Che05b, Kat05b, Pag03, Spr03, Bih00].
R&D [Mau05]. Rabbit [BVP+04]. Rabin [Bon01, Gen04b, Miy01]. race [Hii05].
Rackoff [MP03, Pat03a]. radar [GG05b].
Radiations [SGM09]. radical [Web02].
Radio [Sak01]. RadioGatún [BDPV09].
Radix [HKA+05, JY01]. Radix- [HKA+05, JY01]. rails [Fox00]. Rainbow [DS05a].
Raises [MP00]. Raising [Cos03].
ramp [YJ06]. Rampung [Coc02b]. Random [Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CTY09, Ch08e, Die03, DGP07a, DGP07b, DV08, EH+03, Gra02b, GPR06, HSR+01, HBF09, Int03, JRR09, Kel05a, Kel05b, LLL+01, LM02, Lys02, MP03, Mir02, NNT05, NNM10, Nie02b, Pas03, Pat04, Run05, Ran01, RSN+01, SFDF06, TWNA08, TL07, Tip27, TST09a, TST09b, Vav03, VKS09, WP03, XXYX11, BK07, Bel08, BG08, BG09, BGL+03, CFY+10, CIJ06, CO09b, DGP09, Fis01a, GVC+08, Gen00b, GB09, HG05a, HLwW09, HMvdLM07, JAW+00, KH08, KB39, KG09, LGK10, MI09, MRT10, MFK+06, NR04, Pan07, PSC+09, PLGvdLE10, PSP+08, FCO0, Reg05, Reg09, RG09, RGX06, SH11, SM11, SS03, SXY01, SR07, Sti11, SK01b, Sug03, SL09, UHA+09, WW08, XSWC10, YZEE09, BH05].
Random-Error [LM02].
random-self-reductions [Fis01a].
Randomats [Sam01]. Randomization [Hro03, WHH05].
randomization-enhanced [WHH05].
Randomized [Sen00, Hro05].
Randomness [DD00, DD04, DGH+04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, MS10, SB00, Sun00a, BBN+09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03]. Range [CW09].
Rank [Sun00a, DW01, Sin02]. Ransom [BH05]. Rao [ZLR01]. rapid [OP01b].
Rate [KT01, LZ09, PS02a, Sun02]. Rates [GH02]. Ratio [Di 01]. Rational [HT04].
ratios [Zir07]. raw [CO09a]. RBAC
[LSZ05, SN04, ZP05]. RBAC-Based
[LSZ05]. RC4 [FMS01, Mi02, VV07]. RC6
[GHJV00, GHJV01, IK00, IK01, KM00,
KM01b, RRY00, STK02]. RCES [LLCL08].
RCES/RSES [LLCL08]. re
[AH03, AFGH06, KHL09, Sma06].
re-encryption [AFGH06, KHL09].
re-signatures [AH05]. re-thinking
[Sma06]. Reachability [AL00a, MT07].
REACT [OP01b]. Reactive [Shy02]. Real
[BSW01, Di02, GSB+04, JBR05, SP05,
Sta05, YKMB08, GM04, HP01, Lie05, Pot05,
SL07, SGPH98, YZDW07]. Real-Time
[Dri02, GM04, YZDW07]. Reality [Coc01a].
Really [CZB+01, Wei00, Dav01c].
reap [CH00]. reason [Lau08b].
reasoning [IK03, IK06]. Rebalanced
[SWH+09]. Rebalanced-RSA [SWH+09]. rebels
[Lev01]. Rebuild [Salxx]. Rebuilding
[Sal05a]. Receipt [HS00]. Receipt-Free
[HS00]. Receipts [Cha04]. Receive [Coc03].
Receiver [CCD07]. Receivers
[NNL01, SBB05]. recency [SW02]. recently
[JK01a]. Reception [Top02]. Recipes
[VMO3]. Recipient [ANR01, Kur01].
Recipients [Coc01a]. recoding [SSST06].
Recognition [Ano02d, LLT+04, LST+05,
TZT09b, HS02b, LI05, MMJP03].
Recommendation
[Bar06b, BK06a, BK07, Dwo03, NIS03b].
Recommended [Kel05a, Kel05b].
Reconciling [BNP03, PG07].
Reconfigurable
[FD01, FZH05, GC01b, KBD03, LZ04,
MKP09, MMH02, SJT09, SKG09, SRQL03,
CMS08, DHL06, GC00a, HBC+08, Rh03].
Reconfiguration [PBTW07].
Reconsidered [Sho01]. Reconstructing
[CFD01, FL06, PS01a]. Reconstruction
[AF03, CF01b, CDF01, JJO00d, KY01c].
Records [Dur01]. Recoverable
[NZCG05, NZS05, SGMV09, YY00].
Recovery [BDK+09, BM01c, CKM00,
MMZ00, OS01, PBC05, SVW00, TC01,
V07, WCZ05, WLT05b, CCH05, CJ05,
CLK04, HW05, LKKL01, PSP+08, Sha40b,
SIR04, TJC03, Wu01, ZF05]. Recursive
[WHHT08]. Recycling
[DPS05, TR09a, TR09b]. Red [Sas07].
Red-Eye [Sas07]. redistribution [KB09].
Redondo [IEE00a]. Reduced
[BDK02b, CC08, CS05c, FKS00, HQ01,
HSR+01, KKS00a, KS00b, KKS01, KML+02,
KM01b, KKS00b, MHL+02, NP01, STK02,
SK01, YSD02, CV05, K01a, SK01a, Th03].
Reduced-Round [FKS00, KKS00a,
KS00b, KKS01, KML+02, KKS00b, NP01,
YSD02, CV05, K01b]. Reducibility
[DM00b]. Reducing
[AL07, BIM00, SPH00]. Reduction
[CM05a, CH07c, Dhe03, Gro01, HGG07,
Kid02, PG05, ALV02, HG07, Sug03].
reductions [Fis01a]. Redundancy
[AB01, BR00a, FM02b, YLR05].
Redundant [MF01, Tan07a, PS04a].
Redwood [KKP02]. Reed [KY02b].
Reference
[BR09, CPS07, Pas03, RS00, Sal07, vT00].
Reference-Watermarking [BR09].
Refined [Sma03b]. Regarding [GMP01a].
Regex [BTTF02]. Region
[BSN00, Bur00]. Region-Based
[BSN00]. register [HTW07]. Registers
[CGFS00]. Registration [HLM03].
regression [mSGFL05]. regulation
[Ma05]. Regulations
[Gen01, Mad00b, TMM01, Ana00g, Cla00b].
Rehearsal [Ahm08]. reinforce [SWR05].
Rejewski [CB+05, Kap05]. Related
[BDF+01a, Can06b, CY08, FKS00, Kil01b,
KLML05, Sat06, Buc00b, Gutxx, HAU04,
Hn06a, Sch00b]. Related-Key [FKS00].
Relation [ABC+05, NN06]. Relational
[AK02b, AHK03a, AHK03b, CKY07, GA03,
PT08]. Relations [BN00a, Pau01, Uni00a,
Uni00f, Uni00e, SP03, Zha08]. Relationship
[NG05, GKM+00]. Relationships
[DKMR05, SKU+00]. relative
[JRS09, Mü01b]. relaxes [Ano00c].
Relaxing [CKN03, PS05]. Relay
[DM07b, Zha00]. Release
[CHKO08, Mao01, HGNS03]. Released
[Bar00c, Ano01b]. Releases [Bar00c, AJ08].
Reliability [IKP+07, WK05]. Reliable
[MR03, MPHD06]. released [SL06].
Remainders [Sch01b, YKLM03]. Remarks
[BCW05, CL04d, SCS05c]. remedy [FZ06].
Remember
[HS08a, HSH+08b, HSH+09]. Remote
[CJT02, CW09, Kra02b, LL05c, Rub01, TK03, WB08, CC01a, CL04d, CJT01, DSGP06, FCZ05, Hsu05b, HL05b, KC05, LHY02, LLH02, LKY05a, LHL03b, LC05a, MW06, SW06, SZS05, WLT05a, WC03b, YW04b, YC09b, YRY05d]. remotely [Küh08, SR00]. Removal [LLS05a].
Renewable [TOEO00]. Repairing
[DKFX05, GM00b, HL04, ZJ09, BKN04]. replace [Gav08]. Replacing
[FZ06, KAM08]. replication [BIW08].
Reply [WLW04]. Report [DFG01, Pem01b, Pre01, Sal01a, Sha03b, BCHJ05].
Repository [Bar00b]. Representation
[BJvdB02, FSW01, JLY03, JY01, RN00a, RN00b, ZLK02, BDSV08, BA06, PS04a, SWR05]. Representations [OSSST04].
Representative [CTBA+01].
Representatives
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Republic [MJ04, dL00]. Republik [dL00].
reputation [HLL04, LSA+07, SC05c].
reputation [KNS05, RCG+05].
reputation-systems [KNS05]. Request
[RSA00b]. require [SV08b]. Required
[Sun00a, Lov01, Wan05]. Requirements
[FIP01b, HW01, Kin02, NIS01b, Mee04].
Rescue [ASW+01]. Research [Pip03].
Research [AJ01b, CZ05, CZK05, DFKS06, KGL04, LXM+05, RC06, Sch00e, TMMM05, DFCW00, JXW05, MH09, QSO0, dCdVSG05].
Researchers [Ano08b, Ano08c, Pau02b].
Resettable [DPV04, MR01b]. Residue
[TIGD01, YKLM02b, CNPQ03, FP00, LD01].
Residues [Coc01b, Zhe01, CCS08].
Resiliency [Joh00]. Resilient
[Che01c, DDS01, DFK+03, DP07, DP08, GSS08, KZ07, SM00b, KZ03, IR02]. Resist
[HM02c]. Resistance
[HNZ02, MÖ02, EBS01]. Resistant
[Ano01f, ACJT00, ANL01, BGW05, CDTK05, CV05, GPR06, IK005, LLS05a, LWS05, LTM+00, LNL+08, KSO9a, PC09, WL04b, YS02, MS09c]. Resolution
[SGM09]. resolving [Liu01b]. Resort
[USE00b]. Resource [MRL+02, Tse07].
Resource-Constrained [MRL+02].
resource-limited [Tse07]. Resources
[Gutxx, You04, FOP06]. Response
[JBR05, LW05a, XNK+05]. Responsibilities
[Vix02]. Resting
[Gut02a]. restricted [ASW00]. Restriction
[CTH08]. Restudy [FWL08]. Results
[APV05, GM02c, OOP03, RR08, Way02a, YRS+09, CV05, CKRT08, DM07a, GMG00, PM08]. Rethinking [Bra01a, KZM03].
Retraining [JL07]. Retreat [FKSW00].
Retrieval [BIM00, KO00, RE02, Yek07].
Retroactive [DBS01]. retrofitting
[CGL+08a, CGL+08b, CGL+08c]. reunion
[LB00]. Revealed [Gal03]. Reversal
[Cap01, DIS02]. Reversal-Bounded
[DI02]. Reversals [MS02e]. Reverse
[Coo02, EC05, Wue09]. Reversed [Ina02b].
reversibility [KC09a]. Reversible [Go03].
Reversing
[EC05, YWC08, YNO1, CDFM05]. Review
[And04, Ano02i, Duh03, Eau05, Eva09, Fal07, Gas01, Gum04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, Pag03, Pap05, Puz04, Ree01, Rot07, See04, Spr03, Ter08, TVdKB+01]. Top02, Uzu04, Was08a, Her09b, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wal00]. Reviews
BF01c, Bon01, BCCN01, BP01b, CNS02, CDL+00, CW02, Che01a, CKY05, CNPQ03, CKN00, CJNP02, CS00, CS03c, CD01b, DK01, DT03, Duj08, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Gir06, Gon06, Gro01, HN04, Her07, HLLL03, HLH00, HLLL03, Int00, Jan08b, JS05, Jon08, JK02b, JK02c, JG01, Kal01, Kal03, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, May04, Miy01, Mol03b, MP01c, NZCG05, NZS05, NS01b, Nit09, Nov01, NMSK01, PS00, Riv03, RSA09a, RSA09b, Sch01b, Sei05, Sha03a, Shp01.

RSA [Shp04b, SZ01, Str02, SWH+09, TIGD01, TT00, Ver06a, Wal01, Wal03, WQWZ01, War00, WLHH05, Wie00, WS02, WY05, XC05, Yan07, hY08, YKLM02b, YKLM03, YPKL08, YY00, You6, ZC09, Zhe01, ZWCY02, dW02].

RSA-based [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZCG05, Sei05, WLHH05, WY05, YPKL08, YY00].

RSA-Encrypted [CD01b].

RSA-Primitive [ST01a].

RSA(R) [Ano06b].

RSES [LLCL08].

RST [ZLZ07].

Rueppel [Ara02].

Rules [Bla01a, Ano00c, Bla01b, GM04, Ste02, Wue09].

Running [ZL04c].

Running-mode [ZL04c].

Runtime [PBTW07].

Russia [GKS05].

Ryan [Puc03].

Rye [KJR05].

Ryu [KCC05].

S [BZ02, Kat05b, Puc03, Bih00, BCDM00, Dav01b, Dav01c, FM02b, JmBdXgXm05, LG09, Opp01, SMTM01, ZC00].

S-Box [FM02b, SMTM01, JmBdXgXm05].

S-boxes [BCDM00, ZC00].

S/MIME [Dav01b, Dav01c, LG09, Opp01].

SAC [AMW07, HH04, HH05, MZ04, NH03, POT05, HSR+01, HSS04, ST01d, VY01].

SAC’99 [HA00].

SAFE [Uni00a, Uni00c, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Oiw09].

Safe-Prime [ACS02].

Safeguard [LXM+05].

Safeguarding [Sty04, Bar03].

safer [Ano00f, NPV01, BDD03].

SafKASI [WA00].

Sailer [Eva09].

Salomon [Pap05].

Salsa20 [Ber07, Ber08].

Salt [PKBD01].

Salzburg [DKU05].

Samba [BH00a].

SAML [RR04].

Sanos [KGL04].

Sampling [WW06].

Sanity [Sko03].

SANS [Ano01e, Mad04].

SAS [VAF00].

SBoxes [WOL01].

SC-CFS [Ito01].

SC2000 [SYY+02, YSD02].

SC2001 [ACM01b].

Scalable [CPHX04, HKA+05, HLL05, KY03, KHYM08, SPGG06, LLW08b, ST03a].

Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06].

Scaled [BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a].

Scaling [BBPV00, Coc02b, SDFH00, SDFH01, PBVB01].

Scambray [Gun04].

Scan [MYC01, BD03, KBD03].

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, CGHG01, CC01b, CYH01, CTL04, CC09, CH01b, CM05a, Coc01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJS001, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LXH07, LCD07, Miy01, MiIl01a].

SafKASI [WA00].

Sailer [Eva09].

Salomon [Pap05].

Salsa20 [Ber07, Ber08].

Salt [PKBD01].

Salzburg [DKU05].

Samba [BH00a].

SAML [RR04].

Sanos [KGL04].

Sampling [WW06].

Sanity [Sko03].

SANS [Ano01e, Mad04].

SAS [VAF00].

SBoxes [WOL01].

SC-CFS [Ito01].

SC2000 [SYY+02, YSD02].

SC2001 [ACM01b].

Scalable [CPHX04, HKA+05, HLL05, KY03, KHYM08, SPGG06, LLW08b, ST03a].

Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06].

Scaled [BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a].

Scaling [BBPV00, Coc02b, SDFH00, SDFH01, PBVB01].

Scambray [Gun04].

Scan [MYC01, BD03, KBD03].

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, CGHG01, CC01b, CYH01, CTL04, CC09, CH01b, CM05a, Coc01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJS001, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LXH07, LCD07, Miy01, MiIl01a].
OKS06, PL01, RK06, Scr01, SOO102, SWH05, SGGB00, SYL05, SSNG500, Tad02, TC01, Tsa01, TT01, WQWZ01, WZW05, WBD01, YWWS09, YGO1a, YLH05, ZJ09, AEEdR05, Asi04a, BCL05a, BCW05, BKN04, BBG+02, CL02b, CBB05, CC01a, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CY05, CH05, Che05a, Che07a, Che08a, Che08b, CCS08, CKN06, CJT01, Ch08b, Ch08c, Ch08d, DSGP06, DW01, FLZ02, FXAM04, FCZ05, FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HWW03, HWW04, Hsu05a, HWOO5, Hsu05b, HLC07, HCO4a, Hwa00, HY03, HLL04, Hwa05, HL05c, HL05d, HL05b, JW06, JSW05, KC09a, KLY03, KRY05, KSW06, KHL09, KCL03, Ku04, KC05, KCC05, KHKL05, LHY02, LL02, LSL03, LKY04, LL04a, LLY04, LL05a, LKY05a, LKY05d, LL05b, LMC+03, LLH04, LTH05, LLC08, LLH06, LHL03b, LCO4a, LYG07, LCC05, LC04b, LC05a, LHH05, LC05b, LCZ05c, LCZ05a, LWKO5b, MFP09, NCO9, PW05, PBMB01, PCC03, PC05b, PS01a, Pei04, Sae02, Sch03d, Sha03c, Sha05a, Sha05c, Sha05d, SLH03, mSfFtL05, SCS05b, SC05c, SC05c, SSZ05, TLH05, Tsa08, TWL05, TYH04, VK08, VS08, WLT03, Wnd04, WL05, WK05, WJP07, WDLN09, WHH05, WC01b, WH02a, WHLH03, WH03, WC03b, WL04b, WC05, XwWL08, XC05, YW04b, YTH04, YW04a, YWH05, YC05, y08, YRY04, YRY05a, YRY05a. scheme [YRY05d, YYY05b, YyJi04, ZC04, ZK04, ZK05, ZW05a, ZAX05, ZC09, ZL05, dRMS05]. Schemes [AR01, BP02, BU02, BDD03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CPD06, CKN04, Cor02, CHP02, Con04, CS00, CS03b, CDG+05, CLZ02, DN00a, DN02b, Des00b, DS06, DN00b, FF00, HSZ100, HW05, HM02b, HLL05, Kin02, KOS03, KOS01, LZZ+01, LP01, MV00, NIS03b, NM02, NNL01, NNO6, OP01a, Pat04, Pre01, ST01b, SBZ02, SPMLS02, Sun00a, VMS05, WC009, XSW08, YYD001, Yek07, YZ01, ZTP05, ZFR01, Abd01, AFGR06, BCD06, CW009, CC05b, CJT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGK03, HCD08a, HCD08b, HAuR04, He02, HSK00, HW03c, HW04, HW05, HC04b, HL04, IY06, JPL04, JW05, KYY05, Kir01b, KT06, Kre05, Küh08, LWZH05, LWK05a, LW05c, MF07, Mül01b, NK06, PO02a, PKH05, Pha06, QCB05a, QCB05b, SN100, Sha03d, Sh05b]. schemes [SCL05, SC02c, SHT05, Tsa05, Wu01, XY04, YWC05, YCW+08, ZFR05, ZCL05, vDST06]. Schloss [IEE01b]. Schneider [Puc03]. Schneier [Ano01e, Hei03, See04, Sty04]. Schnorr [BP02]. School [Coc02a]. Schools [PM00]. Science [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Imr03, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04, Pot05, Six05]. Scientific [CHT02, MH09, Lau08b]. Scientists [Coc01a, MH09]. SCN [BC05c, CGP03]. Scots [Ree01, Ros00b, Sin99]. Scream [HCJ02]. Scribbner [Gas01]. Scripts [Uri01b, Oue05, Rob02, Rob09]. scroll [GB09, HHY07]. SD [ECM00a]. SDK [Ano02d, Bar00c]. SDL [HL06]. SEA [SPQ06]. SEAL [Flu02b]. Seamless [OKE02]. Search [BI05a, Des00c, Eva09, FIPR05, KB07, LM02, TIGD01, WY05a, WY05d, FZ00, 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, Kil05, KP01, NM09, RD01, ACM00, Irw03, Rie03, Son00, SPR03].
Second-Order [NM09]. Second-Price [Bra01b]. Secord [Top02]. Secrecy [ACS02, Alv00, Ano03e, BBDK00, BTW05, BI05b, BTD08, BP06, BM01b, CGHG06, CGH00a, CH01a, CLT07, Cha04, CTOY90, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG05, CD05, Di 01, DKL00b, DS06, DN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah67b, Kah96, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, MN01, NABG03, NN06, OKS06, FZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sin00a, TL02, Top02, TC01, UWW00, Ver06a, Wra05, ZYR01, ZP01, wV01, AJ08, AEEdR05, Ano02c, Ano08c, Ban02, BCB05, Cal01, CC05a, CHY05a, CHY05b, CJL06, CNK04, CDD00, DD04, DB04, DM00a, Di 03, DW01, Du08, FNR05, FWT05, FZ06, Gal02, GIKR01, HT04].

Secret [ACS02, Alv00, Ano03e, BBDK00, BTW05, BI05b, BTD08, BP06, BM01b, CGHG06, CGH00a, CH01a, CLT07, Cha04, CTOY90, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG05, CD05, Di 01, DKL00b, DS06, DN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kah67a, Kah67b, Kah96, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, MN01, NABG03, NN06, OKS06, FZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sin00a, TL02, Top02, TC01, UWW00, Ver06a, Wra05, ZYR01, ZP01, wV01, AJ08, AEEdR05, Ano02c, Ano08c, Ban02, BCB05, Cal01, CC05a, CHY05a, CHY05b, CJL06, CNK04, CDD00, DD04, DB04, DM00a, Di 03, DW01, Du08, FNR05, FWT05, FZ06, Gal02, GIKR01, HT04].

Secrecy-Ballot [Cha04]. secret-code [DW01]. Secret-Key [HR05, RW03a]. Secret-Sharing [BI05b, CDM00, CDI05, DKL00b]. Secretly [CC08]. Secrets [BH06, BBD02, CMS09, CP07, Che00b, Cop04b, Di 01, Gan01b, Gum04, KMS01, LKM05, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM01, VGMO4, AGKS07, Ano03c, Ano08b, Ban02, Ban00, Bau02a, Bau07, Cop05, Cop06, Cop10, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DLMM05, Eva09]. Section [Ano04b, Ano07a, BK06b, SGK08, TL02, KP03]. Sector [Cro01, MV01]. Secure [McK04]. Secure [AR00, AO00, AF04b, AG01, AP09, Ano01o, ACJT00, AFI06, BGCH11, BDF01a, BST03, BCL05b, Bar03, B05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CH03, CHK05, CGP08, CW07, CS01, CHJ01, CHJ01b, CD00, CD01a, CS02, CS03b, CDG05, CDI05, Des00b, DG03, DM00b, ES00b, FGMQ01, FB01, FP01, FOPS01, GPCS08, GIK02, GJKR03, Gen04a, GD05, HST00, HST01, HST02, HST06, HRS02, Har07b, HKW06, HLV02, Hv09, HR04b, HL07, HLSJ09, Hut01, HL08, IR01, Ito00, IFH01, JJ00a, JL00, JMV02, KMM06, KY01a, KO04, KLML05, KC02, HK05, KKL09, KI01b, Kos01a, Kos01b, Kra01, Kra05, KSR02, LCK01, LLL02, LCK03, LWK00, Lin01c, Lin03, Lin02, LL02, MKP09, Mar02a, Mar07, MV01, Mlo03a, MJ01, NMO05, Nam02].

Secure [Nd05, NSNK05, NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RVS09, RdS01, ST01a, Sea05, SVDF07, SBG05, Smi02, SKR02, SNR04, SBEW01, Sty04, Tad02, VMSV05, Vau05b, VM02, VM03, WLL09, WBL01, WGL00, WHL05, XS03, YW05, ZYM05, Zho06, Ann03, Ab01, AEEdR05, AL07, AFHG06, BDS09a, BDFP05, BCP07, CLOS02, CCM07, CCO4b, CCK04b, CSR09, CHH09, CCO6, CG05, DG06, Dwi04, FMY02, Geb04, GIKR01, GCL08, HSW09, HL03, HL06, HJW05, HBC08, In05, ISTE08, IKOS07, IY06, KOY09, KG09, LL04c, LL04, LH08, LH03, LC04a, LCZ05b, MT09, ML05, Mlo01b, OS00, PCSV07, PBMB01, PQ06, PLStL01, PSP08, RH03, RG09, RGX06, Sea09, SBG07, SGMV09, TKP08, TCR03, Tse07, Ver01, V09, WIL06, WWA01, YGZ05, YT05, Y08, YRY04, ZBP05, ZCL05, ZCW04, vOWK07, Ano03b, Ano08d].

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

Secured [BNPW03, It001, UP05]. Securely [HL05a, LLK05].

[Ano01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLSS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. Security

[AWS05, AW08, Ahm07, AJ08, ADR02, And07, And08b, Ano02b, Ano03b, Ano06c, AHKM02, Ayo06, BP07, BW07, Bam02, BPS00, BBM00, BKR00, BP02, BNPS02, Bys03b, Bla02a, BF06b, BDTW01, BCHK07, Boy01, BGM09, BLMS00, CGM07, CK02a, CK03, Can06a, CGHG01, Cer04b, CC02b, CKN03, Can06a, CGHG01, Cer04b, CC02b, CJSW08, Che05c, CM05a, CH07a, CSY09, Cla03, Cocc01a, CK06, Cor00b, Cor02, CGP02, CG05, Dr.00c, Dal01, DN02a, DKMR05, DeL07, DJ06, Des00c, Dim07, DR02d, DSS01, DK05, DS05b, DBS06, Elb09, ELvS01, FIP01b, FBWC02, FW09, FLY06, For04, FML+03, FMV01, GSW02a, GSS03, Gum04, Gut02b, Gut04a, Gutxx, HM00, HSZI01, Hei07, HM02b, Hr09, HLL+01, HGNP03, HQ05, HL05c, HL05d, ISO04, In002a, In002b, Int00, IKY05, IKP07, JY04, JP07, JP02b, JSW05]. Security

[JJ07, Jol01, JBR05, JK02b, JK02c, JM02, JY01, Kan01, KM02, KSHY01, KLO5, Ken02a, KB06, KM03, KDO1, KM05, Koc02, KHL09, Kos01a, Kov01, KXD00, Lad06, Lai03, Lan00a, Lan04b, LGS01, Lee04b, LKH+08, LKHL09, Leh06, Len01, LNS02, LL04d, LSH03a, LSH03b, Lin02, LXM+05, LWK05b, LP01, MFP07, MS02a, MS09b, MF03, MS05b, MV01, MN03, MP05, Miil01a, NIS01b, NDJ01, NNAM10, NP07, Oks00, OP01a, ORT00, PV06b, PSC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PTP07, PP07, Pho01, Pio05, Pli01, Poi02, PHM03, Poo03, PF03, PS05, Puc03, Puc06, QC0305b, RR00, RR03b, RR05, RC01, Roi02a, Roy05, Rub01, RC06, ST02, Sa103a, SHT09, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch01f, See04, Sha05d, SLH03, SLG+05, SL05a, Shp02, Sk03]. Security

[SEF+06, SEK01, SEK02, SK06, Sta03, SB07, Ste05b, SBZ02, Sty04, SK101, Sun05, Swi05, Tan07b, TG07, TG04, TPRM07, Un00a, USE00d, USE01c, USE02b, Un00c, Uni00d, Uni00g, Uzn04, Van02, VMC02, WLT05a, WBL01, WWL+02, WA07, YEP+06, YWD08, Zan01, ZWC02, ZDW06, Zhe02b, ZHY03, ZS05, AA04b, Ano05c, AJ01a, AJ01b, BPS08, Bai08, Bao05, Bjo05, Ber07b, BR04, BPG09, BFG08, Bjo05, Ble07, BJ02, BMW05, BG07a, Brun06, BMV06, Can01a, C+02, Cha07, Cha05b, CKL+09, Che00b, Che05b, CKRT08, Chi08b, Chi08c, Chi08d, CJ06, CJM00, Con09, Con04, CCO05e, DP04, DKK07, DY01, DFGH04, Des00a, DWM05, DKU05, DMS07, Egh00, FXAM04, FR08, FOP06, GH08, GJL06, GJ05, Gha07, GJ03, Gor05, GKS05, GMW01, GC05, Gut04c, HM00, HCD08a].

security

[HCD08b, Har05a, Hei03, Hen01, Hos04a, HM05, HSL+02, HL06, HG05b, In005, JEE04, Jan00, Kad07, KY00, KPS02, Kim02, KVD07, Kvo03, KH03, Kwo03a, LC03, LL03, LJ04, LL05b, LPW06, LMC+03, LMW05, LLLZ06a, LLLZ06b, LHC08, MJ03, Mal06, Man08, Man05, Man04, May01, MKWW00, MSK03, Mcg06, Men03, MS02d, MK05a, MPPM09, OP01b, Pa03, PSG+09, PC05a, Pat02a, PY05, PP06a, Pau03, PHS03, Pip03, Poi00, PS04c, Rie00, RC05, Ros06b, RN00a, RN00b, SN00, Sal05d, Sch03, Sch02, Sch04d, Sen03, SHL07, Shu06, SPHH06, Son00, SH00, Sta02a, Sta06, Ste02, Sun00b, SHT05, SL+00, Tsa05, Uni00f, Vac06, Van03, Voi05, VS08, WAF00, WDCJ09, WA06, Won01, WK06, Wuo05, XQ07, YY04a, YY05b, ZS01, ZWO5b, ZSS05, dLB07, dCDVSG05, vWOK07, vTO5, AG09]. Security

[An002e, BC05c, BP01b, Chr00, Chr01, CCMR02, CCMR05, CGP03, JRB+06,
Security-related [Gutxx].

security-sensitive [SPHH06].

Security [Wal03].

Seeking [Coc01a, PH03, Shp05]. Seeking [Mos06].

Seeks [CAC06]. Seem [TP07, KKJ +07].

Seeking [Coc01a, PH03, Shp05]. seeking [Mos06].

Seeks [CAC06]. Seem [TP07, KKJ +07].

Seem [Coc01a, PH03, Shp05]. seeing [Wal03].

Seems [Coc02a]. Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, VY01, Ytr06, AMW07, Bir07, BC05c, C205, CKL05, DRS05, HH04, HH05, PC05a, Wil09, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bur03, dB07].

Selection [IBM00, JKK +01, RS00, SM08]. Selective [CS07c, LS01a, LM02].

Selective-ID [CS07c]. Selectively [Chi08e].

Self [GMM08, HW05, KY01d, LXH07, PS01b, PBC05, Sch06b, WHHL05, WLT05b, ZKL01, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, HL04, Lee04a, LL06, LS05b, LWK05a, PC05b, SH11, Sha04b, Sha05b, TLH05, Tsa05, TJC03, WH03, Wy05], self-adaptive [SH11].

Self-Certified [LXH07, HW05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, LL06, LWK05a, PC05b, SH11, Sha04b, TLH05, Tsa05, TJC03, WH03], self-defense [Wy05], Self-Enforcing [GMM08].

Self-Escrowed [PS01b]. Self-Localization [WLT05b]. self-modifying [CSV07].

self-pairing [Lee04a, PC05b].

self-protecting [LS05b]. Self-Shrinking [WHHL05, ZKL01]. Self-Similarity [Sch06b]. Selling [Bla01c].

Semantic [PBV08, SN00, Sch00c, Coc01a].

Semantically [KI01b, ST01a]. Semantics [Li01, Mar02b, BFG04, BFG05, SW02].

Semi [Far00, Nak01, SY01b].

Semi-Equivalent [Far00]. Semi-fragile [SY01b].

Semi-fragile [SY01b].

Semi-fragile [SY01b].

Semi-fragile [SY01b].

Semiconductor [Coc02b, Ig02, UHA +09].

Seminal [Cop04b]. semipublic [YC07].

Sender [CMB +05, Her09b, Tj01a]. Sensation [Top02].

Sensible [Sch04c]. Sensibly [See04, Sty04, Hei03, Sch03].

Sensitive [HT06, Bro05b, SPHH06]. Sensitivity [SDMN06, GSK09].

Sensor [AEAQ05, CS08b, DBS +06, Fin06, GPCS08, LNL +08, NABG03, NNAM10, PZDH09, ZYN08, AJ08, CCMT09, HMvdLM07, JRR09, KXTZ09, KHYMO8, LDH06, LPV +09, LN04, Lop06, MWS08, MS09b, NC09, NL08, PS08a, RAL07, TP07, WDNL09, ZSJN07, AMB06].

Sentry [Kum07]. Seoul [CKL05, KCR04, Kim02, LL03, LL04d, May09, PC05a, PK03, Son00, Won01, WK06].

Separable [CD00a]. Separating [BYJK08, GKK +09, Ke00, Ly02, Mur00, ZGLX05, BYJK04]. separations [GKK +07].

September [AUW01, AAC +01, AJ01a, BCKK05, BC05c, CSY09, CGP03, DV05, DKU05, DFCW00, EBC +00, ELvS01, FLA +03, GKS05, QS00, RS05, SM07b, WK03, dCdVSG05, AJ08].

September 19 [AJ01b]. September 19-21 [AJ01b].

September 19 [AJ01b].

Sequence [HW01, MS02e, WHHL05, ACTZ05, GB09, SL09, WG02, YZEE09].

Sequences [ADD09, B09, XXYX11, FSGV01, HG05a, JZCW05].

Sequential [GSS08, SNW00, RMH03a, WH02b].

Serial [CTLL01, KWP06, Uni00g, Mit00].

Serpent [BDK02b, ABK00, IK00, IK01, KKS00a, KKS01, KKS00b, Os00, Pat01].

Server [ANRS01, BMK00, Dew08, KO00, LWK00, NS01b, PS05, TMM05, XS03, Zha00, BB05, LHL04b, LHL04a, LKY05b, LHL03b, NTW07, 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, SRJ01, SSM +08, ÚG08, Coc02b, HIl06].

Services
serving [LLK05]. **Session** [GL01, OHB08a, CS04, OHB08b, RN00b, Uni00a, Uni00b, Uni00c, Uni00h, YWL05]. **Session-Aware** [OHB08a, OHB08b]. **Session-Key** [GL01]. **Sessions** [KPR03]. **Set** [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDET00, Che07a, CC05d, DM00a, Elb08, 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-256** [FYLC05, GIKR01, HT04, HKS00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDKST06]. **sha** [Gu05]. **Sheets** [MNS01], **shell** [Dwi04, Gu05, BS01a, BSB05]. **Sheltering** [MYC01]. **Shen** [KTC03]. **Shieh** [Mck04, CZ05, YWC05]. **Shift** [CGFSHG09, Che07a]. **shifting** [Cal00e]. **shifts** [Neu06]. **Shin** [K¨uh08, K¨uh08]. **Shores** [KKP02]. **Short** [An01a, ALM01, BS04, BWG05, DON00b, 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** [Go01c, WHLH05, ZKL01]. **SHS** [An12]. **Shuffle** [FS01c, NSNK05, Sas07]. **Shuffles** [Mir02]. **Shuffling** [PBD05]. **shut** [Gil07]. **SiBIR** [IR02]. **sic** [IEE09a]. **sichere** [S01]. **Side** [An01a, BU02, KSW00, Law09a, LL01, M¨ol02, OT03a, OT03b, Sch06a, WC04, CNPQ03, CSP+08, W07a]. **Side-Channel** [BU02, Law09a, M¨ol02, CNPQ03, CSP+08]. **Side-Match** [WC04]. **Siena** [BCKK05]. **sieve** [CM05b, JL03]. **sieves** [Har07a]. **SIGABA** [Lee03c]. **SIGACT** [AC03c, ACM05b, RA06]. **SIGART** [AC03c, ACM05b]. **Sight** [Col03]. **SIGMA** [Kra03]. **SIGMOD** [AC03b, ACM03c, ACM04a, FMA02]. **SIGMOD-SIGACT-SIGART** [AC03c, ACM05b]. **Sign** [BSC01b, BTTF02, Da01c, Kra03, Da01b]. **Sign-and-Encrypt** [BTTF02, Da01c]. **SIGN** [An02e, GGG05, Sha01e, K01]. **LLZ06a, LLLZ06b, SBS09, Kov01].
Signalling [ECM00b]. signals [Ren09].

Signature [ANS05, AAK09, AR00, ADR02, Ano01c, Ano01g, Ano09b, Ano13, Ara02, AR01, ACJT00, Bar06b, BNPS02, BGOY08, BMS03, BDS09b, CM00, CDO0a, CL04a, CK02a, CGP08, CH01a, Che02, CM05a, Cor02, CFS01, CS00, DSO5a, DKFX05, Eng00, FIP00, Gen00a, GJSS01, GS02c, HYZ05a, Hanz00, HMO2b, JSJK01, KC02, Kuh00, LZL01, LZZ01, LP01, MV01, Miy01, Nat00, NZCG05, PL01, PCK02, Pre01, RS01, SA02, ST01b, SWH05, SPMLS02, Str01a, SYLC05, SSNGS00, TNM00, WQWZ01, WBD01, XYL09, YYDO01, YSS01, YZ01, YLH05, ZK02, ZJ09, Zhe01, AwdH00, BCL05a, BCW05, Cal00b, CWH00, CL01b, CNV06, CZB01, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZ05, Her06, HMO2b, HS01b, HHGP03, HLT01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00a, MM02, MNFG02, PGC01, Ram01, RR02, RdS01, WVO1, XSO3, Zho02, Ano01i, Ate04, AH05, BLH06, BB05, BMW02b, BMW02a, BLRS09, Cal00a, CKK03, Die00, DMT07, Fan03, FWV04, FB01, GMLS02, HRL09, Her07, HLH00, JLL01, JLL04, KKKL09, LV07, LG04, LG09, LS05b, MMJ05, PLJ05a, PBV08, Sch01f, Sha01d, NZS05].

Signcryption [Boy03, LHX07, MLM03, Zhe01]. Signed [FL01b, OSSST04, Sch01a, SJ00]. Signer [DU02, CJT04, LL05b, WK05, IR02]. Signer-Base [IR02]. signer-verified [CJT04]. Signers [LZL01, Sa02, Sha03c, YTH04]. Significant [SZ01, MS02b, Shp02]. Signatures [AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCCN01, CL04a, Gen03, Gra02b, HSZ05, Her06, HMO2b, HS01b, HHGP03, HLT01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00a, MM02, MNFG02, PGC01, Ram01, RR02, RdS01, WVO1, XSO3, Zho02, Ano01i, Ate04, AH05, BLH06, BB05, BMW02b, BMW02a, BLRS09, Cal00a, CKK03, Die00, DMT07, Fan03, FWV04, FB01, GMLS02, HRL09, Her07, HLH00, JLL01, JLL04, KKKL09, LV07, LG04, LG09, LS05b, MMJ05, PLJ05a, PBV08, Sch01f, Sha01d, NZS05].
Statistically [Fis01b, HR07, HNO+09].
Statistically-hiding [HR07].
Statistically-Secret [Fis01b].
Statistics [CKN01, CNK04, KLML05].
Status [Pre01, Sha03b].
Steal [WMDR08].
Stealing [Gan01b].
Steering [HR13].
Stefan [AUW01].
Steganalysis [Pro01, Sal05b, GSK09, WW04].
Steganografie [Sch09].
Steganographic [CTL04, HR02, MJF07, RH02, RS00, Wes01, KC09a, LYC02, WWTH08, YCL07].
Steganography [BC05a, BGI08, CYH01, ChLYL09, CDR01, CW09, CTH08, Col03, CMB+08, CS05c, DIRR05, DRL09, FGDO1, Fr07, Gal03, HCBELETRG06, HLVA02, HvAL09, Hun05, HSKC01, LS08, PH03, Sal05b, Sch09, Sha01e, Shi08, SWR05, Wan05, WW06, CDS07, CO09a, Che07a, Che08a, GGS+09, JD01, KP00, LT04, WW04, WMS08, Way02b, Way09, YCYW07].
Stego [KC09a].
Stego-image [KC09a].
Steiner [WL02].
Step [DRL09, KKKKL09, An004e, MP07, SL06].
step-by-step [SL06].
Step-out [KKKL09].
Stepping [WRW02].
Steps [Bih02].
Stereotypes [GO03].
Stern [CGP08, CS05b].
stick [GPX08].
Sticks [Sam01].
still [An000f, Ree00].
Stinson [Spr03].
STL [Zol01].
STOC [ACM05c, ACM07, ACM08, ACM09].
Stochastic [MG01].
Stock [Bar00a].
Stone [MLM03].
Stones [WRW02].
stop [SSNG00, Win05c].
Storage [DFSS08, Din01, Din05, HR02, Har07b, Hug04, MSTSO4, RCLB00, Ric07, RH02, Vadv03, AFGHO6, DFS05, HGR07, LPM05, SGMV09].
Store [CTBA+01].
Storing [ST06].
Story [Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, HS01a, Win00].
strategic [AJ08].
Strategies [Cir01, KL05, SKQ01, Dwi04].
Strategy [DR02a, TPRM07, KC09a].
Stream [BCC01, BC05b, BSW09, BS00b, BL02, CF01b, Can06b, CS01, CHJ02, CM03, Cou03, CL02c, DF07, Fil00, FF01a, G01d, Gol01e, GM02, HCJ02, HR00, HR04a, Jam00, KHD01, MSNH07, PP06a, SM01, Sar02, SX01, WB02, Wu02, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, BVP+04, DS09, DK08, KH08, Max06, MI09, MRT10, PCS03, PCC03, SB05, WW08].
Stream-Cipher [SXY01, WW08].
Streaming [OS05, CBB05].
Streams [AIP01, CO09a, YLC+09, ZCW04].
Strength [CB01, JX05, Oni01, CKL+09].
Strengthening [Loi00, MHM+02].
String [CP07, DFS04, Pas03, Dam00, RG05].
Strings [Vau05b].
Strong [ADD09, BB00b, CS00, DKFX05, KCJ+01, KW00, LSH03a, LSH03b, Lu02, Pau09, SBZ02, WHL05, An010m, CC04b, HR08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04].
Strong-Password [LSH03a, LSH03b, WHL05, C04b, KTC03, Ku04].
Strongly [AY06].
Structural [BS01c, LBR00].
Structure [DN07, EIG01, HS01, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SLL+00, XMST07].
Structured [BTRM09, CKK03].
Structures [An002e, DS06, GTTC03, HCD002, KCP01, Kus02, MND+04, MFT05, PSC+02, PQ03b, Sun00a, XH03, He06a, IY06, SWR05].
struggle [Bur02].
Stuart [Gun04].
students [AA04b, PP09].
Studies [Pag03, LFHT07, SPHH06].
Study [BBMG08, Car02, DPR01, DP00, KKJ+07, WCZ05, BKN04, BF06a, DY09a, KWDB06, SKW+07, ZWWL01].
Sturgeon [Wei05, Wei00, Wei06].
Stuttgart [Eag05].
style [BPS08, dH08].
Subcommittee [Uni00f, Uni00h].
Subdivision [LDD07].
Subgroup [NBD01, KM04a].
Subgroups
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, MBS04]. Subtleties [Lai08].
subverting [HB06]. Success [Ano06d].
succesful [KH03]. Succinct [BA06, FS08].
Sued [Nic01]. Sufficient [IKO05, Kos01b, KO00, MN01].
Suffix [ABM08]. SUID [Tot00]. SUID/S gid [Tot00]. Suitable [AK+01, CQS01, KTT07, LKH09, SP05, Wen03]. Suite [RSN+01, SBEW01, YLT06].
Suited [WWGP00].
Sum [Che04b, KLY02].
Sum-of-Digits [Che04b]. Sums [CY08, Shp05].
Sunspots [CPS07]. Super [Lam07, CAC06, Hos06b]. Supercluster [Pri00].
Supercomputer [Coc01a, Wal09].
supersingular [Gal01, RS02, Ver01].
Supervision [FDIR00]. Supplemental [TBDL01].
Supplementary [ECM00a, ECM00b]. Supplies [Sha01c].
Support [ABM00, Gro03, LTM+00, PZDH09, BS03, BCDH09, BC01, CGM07, IE00, IE01a, IE02, IE03, IE04, IE05a, IE05b, IE06, IE07, IE08, IE09b, Jef08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05].
synchronisation [CmdV06].
Synchronization [GP08, SW02].
synchronize [Pau02b]. Synchronous [CH01b, Sar02].

Syndrome [TBDL01]. Syntactic [Bih00, CHM+02, CSW+08, CGJ+02, DJ01, DGP07a, DGP07b, DV08, EM03, FL01a, Ito01, Joh05, KRC06, KRC07, Lin00a, LK01, MKKW00, RCG+05, Sal00b, SCS05a, SGMV09, SETB08, TKP+08, Wan04a, dB07].
syntactic [DW05, ZL04a]. Systemic [RBF08].
Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM09, ACM10, Ano00d, BS03, BCDH09, BC01, CGM07, IE00a, IE01a, IE02, IE03, IE04, IE05a, IE05b, IE06, IE07, IE08, IE09b, Jef08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05].
Systems [ACM03c, ACM05b, ANRS01, Ano02e, BCS02, BRTM09, CP02, ELvS01, Fei06, GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST+05, LLZ06a, LJ05b, Lut03, Mar02b, MMY02, NABG03, RS05, Rill02, SM01, Sas07, SJT09, SXY01, USE00c, USE00b, Vav03, VHP01, WKp03, ARJ08, And08b, Ano01n, Bid03, Ble07, CUS08, CCS08, CGL08c, CCM01, CNQP03, CHT02, CG05, CSK+08, DY09a, EY09, FMY02, HP00, HBC08, Hut01, HYS03, JP06, KAM08, KP01, KNPO, KP03, Kov03, KNS05, MBS04, MSP+08, ND06, Nis03a, PBMB01, Par04, Plo06, RW07, Sha01a, SK03, TOEO00, WA00, XQ07, ZSV05, Ano02d, Lut03].
systems/ciphers [SK03].

Systolic [KLY02, KKY02, MP01c].

Table [Ano03f, MFFT05, XFZ01, BZ03, CC05b, Has00, Tsa08].
table-based [Has00].

Tables [Ali08, KB39, RBF08].
tactics [KAL06c].
Tag [KKJ+07, NNAM10].
tagging [BP05].
Tags [OS06, ACD06, PLSvLE10].
Taipei [Lai03].
Taiwan [Lai03, Ano03a].
Takagi [LKYL00].
Takagi-cryptosystem [LKYL00].
Takaragi [WHLH03].
take [Heg09, Per05b].
Taking [CDS07, Lai07, PM00].
Telbot [Rot07].

Talk [FGRM00a, Ran00d].
Talking [Ano01p].
tamer [Kap05].
Taming [Abao00, Lov01].

Tamper [LTM+00, CT02].
tamper-proofing [CT02].
tampering [PS08b].
tandem [DPT+02].
Tang [YRY05d].
tank [Pau03].
tar [Str02].
targana [MAaT05].
target [BD04b].

Targets [MV01, Pau03].
Tarragona [DFPS06].
tasks [XQ07].
Tate [ Jou02, SKG09].
TATSU [TS00].
tatting [CSK+08].
TC [DKU05].
TC-11 [DKU05].
TC-6 [DKU05].
TC11 [ELvS01].
TC8 [DFCW00].
TC8/WG8.8 [DFCW00].
TCC [HR06, Kil05, Nao04].

TCP [CD01b, Ols00, SBB05].
TEA [CV05, HSR+01, HSIR02, HHK+04, MHL+02, WN95].

Teaching [McA08, Shu06, GV09, Jan08b].
Tech [Kir01a, TvdKB+01, Uni00c, Gra01, Ros04, Uni00f].

Technical [BH03, GS07b, Lan00c, Scr01, TL02, USE01b, USE01a, USE02c].

Techniques [AI01, BSW09, Bi03, BBP00, BD02, CC04a, CRA05a, DBS+06, Dun06, Gal03, KL+06, Knu02, K003, MKP09, NCR04, PK01, P601, Pre00, Shi08, YKW01, AB09, BM05, BR05, Che08a, DY01, DHMR07, DY09a, Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08].

Technologie [RSA09b].

Technologies [MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZWC02, AT04, PB01, TTZ01].

Technology [CZK05, Cla00a, GS00, GSB+04, MP00, NFQ03, Pag03, TV03, AL07, Ble07, Car01, Cas02, Che00a, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b, Six05].

Tektronix [Ano02e].
TelCorrelo [LM00].

telegram [Tuc66].
Telelogic [Ano02e].
Telephone [KZO1].

Telephony [Ano02e, CFR02, PM00, CGV09].
teleportation [BEZ00, BEZ01, Dw03].

telling [Gan01b].
template [LLC06a, UBE09].

Temporal [CDTT05, KXTZ09].
Ten [ES00a].

Tenth [USE01c].

Term [ABRW01, Dur01, BMV06, ISO05, LG04, SGMV09, WDLN09].

Terminal [ECM00a, ECM00b].

Terminals [CJ08a, ISTE08].
termination [BP05].
terms [LMTV05].

Ternary [AD09, DKL00b].

Terrorism [PP06b].
terrorists [Mad04, Win05c].

TELSA [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]. Text [Lut02, PJIH01, PM08]. textbook [BIJN00, PP09]. Thank [CMB00, GBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03]. Their [AGT01, CD00a, Gen04a, JKR01, LLL01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, Sti11, TO01, WV00]. Them [WD01a, Tee06]. Theorem [AC02, Eke02, GN01, Sho00a, Sch01b, YKLM03]. theorems [MW04, Nyb01]. Theoretic [CB01, DHR00, Kat05b, Nie02b, VVS01, VDKP05, vW01, Mar05b, NR04, Sph09, Wag03]. Theoretical [SGB01, PRS04]. Theoretically [AP09, DM00b]. Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, AL06, BDT04, Bih03, Boy01, CC04a, Cra05a, Des02, Fal07, HR06, Hay06, IZ00, Irw03, Kim01, Kin02, Lam02, Lai03, Lee04b, Lut03, MNT00, Mao04, NP02a, Nao04, Oka00, PY06, Pfi01, Pre00, Rot05, Roy05, Sch06b, Sph03, Spr03, TW02, TW06b, Vau05a, Wal00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cas06, Cos00, DW05, Gar04, HHL01, HW06, Joy05, Kil01, Lai03, Lam01, PPV06, Rot02b, Rot03, SCS05a, Sho05b, Sto08, St09, Sti02, St06c, Tat05, TW05, Was08b, HR06, KXTZ09, Kil05, Nao04, Nie02a, Nie04].

There [Bar00b, GW00, Neu06]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Hei03, Sch03, Sma06]. Third [AL06, BS01b, CGP03, HR06, IKY05, KN01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QS00, CGH01].

third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM00]. Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thirty-Fourth [ACM02].

Thorsteinson [For04]. Thou [MYC01]. Thought [MNT00]. Thoughts [Joh00]. Threat [Por06, SS04, BK00, Geb04]. threatened [An00]. threats [CNPQ03]. Three [BR00b, Kak06, LSH00, MAaT06, AJ08, CLC08, FGM03, GPS05, LHL04b, LKY05b, LLS09, MAaTxx, SP00H06, YC09a, ZL04b].

Three-Key [BR00b]. Three-party [LSH00, CLC08, LHL04b, LLS09, YC09a]. three-principal [ZL04b]. Three-Stage [Kak06]. Threshold [AF04b, AIP01, BTW05, BTW08, BDDS03, BSS02, CCD07, CLT07, CD01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, KS05b, Kin00, Kog02, LNZ01, LSC03, LCZ05a, LP01, MSJ02, Nie02c, ST07, WQWZ01, Wan04b, WH03, XS03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, DG06, HWW02, HW03, HW05, JL01, LC05, LCZ05c, SCL05, TYH04, WHL03, X05, YTH04].

Three-Key [BR00b]. Three-party [LSH00, CLC08, LHL04b, LLS09, YC09a].

Three-party [LSH00, CLC08, LHL04b, LLS09, YC09a]. Three-Key [BR00b]. Three-stage [Kak06]. Threshold [AF04b, AIP01, BTW05, BTW08, BDDS03, BSS02, CCD07, CLT07, CD01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, KS05b, Kin00, Kog02, LNZ01, LSC03, LCZ05a, LP01, MSJ02, Nie02c, ST07, WQWZ01, Wan04b, WH03, XS03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, DG06, HWW02, HW03, HW05, JL01, LC05, LCZ05c, SCL05, TYH04, WHL03, X05, YTH04].

Throughput [HV04, LS01b]. thwarting [WL07a]. thwarts [Ad09, SW05b]. TI [GBKP01].

Tib [MAaT07]. Ticket [FGL02, KS02]. Tie [SZS05]. tier [TW07].

 Tight [CM05a, Di01]. Time [AK02a, App07, AJ08, BPST02, BS00b, BSW01, CU01, CJ03a, CNV06, CLZ02, Dri02, GP08, HM02b, Ina02b, KL05, Kuh02a, LP02a, Lan00b, LLL05, LDM04, May04, OEC03, Pli01, QSR02, RR02, CAC03, CCK04b, CL00, DS02, GS07b, GM04, HLT09, HH05, LC04a, MRST06, NS05a, YZW07, hY08, DK08].

time-bound [hY08]. Time-Domain [Kuh02a]. Time-Free [CNV06].

Time-Limited [AK02a]. Time-Memory [AJ08, OEC03].

Time-Memory-Data [DK08]. Time-Reversed [Ina02b].

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

Time/Space/Data [BS00b]. Timed [BN00b, CHKO08, JPD07, LKJL01, Mao01, HGNS03, Zha06]. Timed-Release [CHKO08, Mao01, HGNS03].

times [AJ08, CCK04b, Mol05].

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

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

Timestamping
[MSTS04].

Timing
[CKQ03, CWR09, Law09b, SWT07, ASK05, DKL+00a, KS09a, OS00].

timing-attack
[KS09a].

Tiny
[Bar00b, Min03, WN95, And03].

Tipsy
[TvdKB+01].

Tissue
[MYC01].

Title
[ZYH03].

TLS
[BPST02, CHVV03, HSD+05, JK02b, JK02c, KPR03, OHB08b, OHB08a, SBEW01, BFCZ08].

TMAC
[KI03].

TMS320C6x
[WWGP00].

today
[Lie05, Nis03a].

Together
[WD01a].

Token
[Fri01, RSA00d, RSA01, CS04].

tokens
[WDCJ09].

Tokyo
[Ano00d].

Told
[ES00a].

Tolerance
[Ano04b, BK06b, ZL04a].

Tolerant
[DS03, HSKC01, WL07b, BKW03, Lin07, PI06, RMH04, Ybf04].

Tolerating
[KSR02, SKR02].

too
[Sch05c, vT01].

took
[IEE09a].

Tool
[Ano02d, Ano02e, Kil01b, GPG06].

Toolkit
[NIS01a, Sha01a].

Tools
[Ano02d, Ano02e, Bar00b, Gol01b, Ken02b, Ust01b, Bai08, Cas02, CT02, GC05, NCRX04, SETB08, Kat05b, Puc03].

toolset
[Jen09].

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

top-
[GPC08].

Top-Level
[MV00].

Topics
[HSS01, EEE01, Joy03b, Men05, Nac01, Neu04, Oka04, Poi06, Pre02c].

topology
[HL07].

Tori
[GV05, GPS06].

Toronto
[MS05a, VY01].

torsion-subgroup
[KM04a].

torsion
[R03, S08, vD04].

Torus-Based
[R03, S08, vD04].

Toshiba
[Pal02].

Tossing
[Lin01c].

totality
[HRS08].

Touch
[Pau02a, JP06].

toughest
[Min03].

tour
[Pet08].

Town
[KJR05].

Trace
[Bor01, LNS02, NN03].

trace-and-revoke
[NN03].

Traceability
[HLL03, HW05, WLHH05, WY05].

Traceable
[LZL+01, CCH04].

traceback
[CS04].

Tracing
[KY01d, KY01e, LLL02, NNL01, SNW00, TT01, WRW02, WLZZ05, WH01].

tracings
[RE02].

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

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

Trade
[AJO08, CMS09, Oec03, PS01c, Uni00f].

Trade-Off
[AJO08, Oec03].

Trade-Offs
[PS01c].

Tradeoff
[KPR03].

Traffic
[BS00b, CTLL01, SRQL03, SU07].

Trading
[PV06b, SWH+09].

Trafficability
[HLL05, DSP01].

Transform
[ABM08, BBC+09, BR09, CPhX04, KC09b, LKLK05, Nak01, SSFC09, VK07, BR06, Che07a, OP01b, SR00, LPZ06].

Transmission
[HL07].

transfers
[BS00b, CTLL01, SRQL03, SU07].

Trading
[M02a, QSR+02, CW02, Ino05, NS05a, DK08].

Tradeoffs
[BS00b, CTLL01, SRQL03, SU07].

Transaction
[RH02, AAKD09].

Transaction-Based
[RH02].

transactions
[Cal00b, Cal00a].

Transcript
[Ano01a, Ano01b, Ano01c, Ano01o, Mal02, Nik02b].

Transfer
[CT08b, Din01, GKM+00, KKL09].

Transferability
[HSZI00].

Transforms
[IKNP03].

Transform
[ABM08, BBC+09, BR09, CPhX04, KC09b, LKLK05, Nak01, SSFC09, VK07, BR06, Che07a, OP01b, SR00, LPZ06].

Transformation
[CT09, HLL05, DSP01].

Transformations
[Fel06, KYHC01, LMTV05, Pag03].

transforms
[Laf00].

Transient
[ Ric07, VS08].

Transistor
[Coc02a].

Transistors
[Bar00b].

Transit
[Con00, Cal00c].

Transition
[Ano09d].

Transitive
[BN02].

Translation
[GGS+09, PY06].

Translation-based
[GGS+09].

Translations
[Cal00c].

Transmeta
[GP00].

Transmission
[MLC01, SNR04, SVDF07, Smi03].

Transparent
[CCDP01, Por01, Lin00a].

transport
[Bar00].

Trapdoor
[BPR+08, Fis01b, KO03, KO00, Gen04a].
Unauthorized [Ano02e]. Unbalanced [FMP03, May02, HLLL03]. Unbelievable [Len01]. Unborn [Pau02a]. Unbounded [RW02, Wvd02]. Unbreakable [Ver06b, Mui02]. Uncertain [See04, Sty04, Hei03, Sch03]. UNCITRAL [MNFG02]. uncompletable [NS01a]. Unconditional [HM01b, May01, Pas05, RW03b, WW05]. Unconditionally [HSZI00, HSZI01, HSHI02, HSHI06, CCD06]. Uncovering [MNT+00]. Uncrackable [Ano03d]. undeciphered [Rob02, Rob09]. undeniable [GMP01b, GM03, JSJK01, Miy01, WQQZ01, CHC05, LH04, LCZ05a, SSM+08]. underivable [AA04b, Gha07]. undergraduates [DFG01, PQ03a]. understanding [AN03, CPG+04, Cra05b, Elb09, Gor06, PG09, Pn05, Lm09]. undetachable [BMW02b]. Unexpectedly [Bar00a]. Unforgeable [BKY02, KY01a]. Unhooking [Moo01]. Unicode [MJF07]. Unified [CZB+01, HKA+05, MFS+09, SM03b, CCG06]. Uniform [SPK08, TL07, SU07]. Unimodular [CV03]. Unique [Lam91, Lm02, TH01]. United [DFGW00, Jm01]. Universal [BOHL+05, CR03, CJP02, CS02, If00, KKK05, KO03, Pi01, Sh00a, SP79, Cal00c, PS04c]. universality [DS02]. Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CL02, DN02b, DN03, NOM05, RK05]. Universally-Composable [AF04b]. Universiteit [BBDO9]. University [Kat05b, Puc03, Rot07, Top02]. UNIX [CCDP01, Har01a, Har01b, Hif01, Wi01, GSS03]. UNIX-Type [Hf01]. Unknown [CT08a, Lm02b, CS05, HJ07]. Unknowns [CMB+05]. unleash [Mcr03]. Unleashing [Lop06]. Unlinkability [WHH05]. Unpredictability [BS01d]. unprotected [ASK05]. Unravelling [Ano03g]. unrecognizably [Wal04]. Unsolvable [GG05a, Bel07a]. untold [DB04]. untraceability [CL09, LHY05, Pn04]. Untraceable [ACD05]. Untrusted [BMK00, CPG+02, LSVS09, LKL05, ZBP05]. Unusual [GG05a]. Unveiled [Bar00a]. unveils [Mao00c]. Update [Das08, TEM+01, Hm09]. Updated [Cho08a]. upgrading [LH03]. upgrade [Pn02a, Pn02b]. Upgrades [Ano02c]. upon [DFG01, PQ03a]. UPPAAAL [BB+02]. Upper [BP03b, DIRR05, KMT01]. Upset [Bra06]. Upwards [FV03]. URSA [LKZ+04]. US$54 [Dew03]. USA [ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKY05, Joy03b, JO04, Jue04, KKP02, KJR05, Kil05, KP01, Men05, Men07, Nac01, Nao04, Oka04, Oka06, Pre02c, Sch01d, Sh05a, Si01, YDKM06, ACM10, Bel00, Bom03, BCDH09, Elx01, FMA02, IEE01a, IEE01b, IEE05b, IEE08, IE00b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S030, Sch04a, Sch05a, SMP+09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, Wi09, Ym02a]. usability [CG05, WDCJ09]. Usage [LY05, PS04b]. Use [Bai01a, BWBL02, BQ01, CPS07, Drc00, ISO05, Kra03, LCK04, Pn09, PBWT07, Str01a, WS05, Win01, CG05, O07, St11]. used [CDL06, MSV04]. useful [SM03a]. Usenet [Coc01a]. USENIX [Coc01a]. User [An00k, BGP02, CL01b, CMB+05, DP00, FDIR00, Hn00, HY01, KZ09, LSZ05, MR03, OHB08a, Pn01b, Pn01, Sas07, SSM+08, Str01a, Tsa01, WDCJ09, BMM00, CL04d, Chi08b, Chi08c, Cj07, DSGP06, Dca06, DLY08, GMLS02, HW03c, Hsu05b, HL05b, KC05, LAPS08, LHY02, LL02, LKY04, LKY05a, LHL03b, L05a, LK01, OHB08b, Par04, S03, SZZ05, TML05, WLT05a, WC03b, YW04b, YS04, YR04,
YRY05d, ZYL05g, vOT08]| User-Centered [CMB05]. user-controlled [LAP08]. user-drawn [vOT08]. user-friendly [SZS05, WLT05a]. user-level [SS03]. Users [LLS05b, CF05]. Uses [Bau01c, RSQL03]. ushers [Bur00]. Using [AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01c, Ano01n, ADDS06, BJF02, BH06, BK06a, BBC+09, Bau01a, Bau01b, BP06, BPS02, BR09, BT02, BMK00, BMP00, BL02, Che01a, CLLL00, CGB01, CCW02, CCM01, CC06, CH07c, Cir01, DI05, DPR01, DP00, DWN01, DGH+04, EFY+05, FJ03, FMP03, Fri01, GC01a, GL01, GSB+04, HHGP+03, HQ05, HJW01, Jab01, JK+01, JSJK01, KOY01, Kel05a, Kel05b, KM01a, KLC+00, KTT07, Kra02b, KZ09, Lan04a, Len01, LB04, LS05a, LXH07, LM02, LH07, MS02a, MS09a, MLM03, MS03b, MMJ05, NNM10, NZCG05, NM09, OT03a, PHK+01, PJH01, PJK01, PCK02, PK01, Sho00b, SK05a, Sma03a, SVW00, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VPG01, WY02, Wit01, WC03a, XFZ01, YKMY01, YLLL02, YSS+01, ZWWL01, Zhe01, ASW00, AL07, BCL05a, BCW05].

using [BK07, CG06, CDS07, CWH00, CL04d, CCK04b, CCH05, CHY05b, CKY05, CJ05, Che07a, CKY07, Che08a, Che08b, CJ04, CK03, Cos00, DDL01, Dan02, DSG06, DS09, DFG00, FWTC05, GC00a, GMR05, Gen09b, GS09, HHSS01, HW05, HAO04, HTW07, Hir09, HW04, HL05c, HY03, HL04, JRR09, Jua04, KOY09, KC09a, KL01, KB09, KKL09, KJ07, KSW06, KR03, KU04, KC05, LHY02, LLH02, LKY04, LCP03, LL04c, LW04, LKY05a, LKY05b, LLW09, LF04, LCO05a, LCC06a, LMK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PSC03, PPC03, PSC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SH07, Tan07a, TLH05, Tsa05, TJC03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04a, YW05, YC09a, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. utilising [RFR07a, RFR07b, RFR07c]. utility [Gua05]. Utilizing [Str02].

V [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00e]. v2.1 [RSA02]. v2.11 [RSA01]. V5 [It00]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BL01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [PM00]. Value [BR09, GNS05, LS08, BM02a, DK08, WWTH08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadharajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSN05, Ber08, Duj08, Duj09].

Variants [BK+09, DG02, KS00b, Cio05, Sha04b, TJC03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDKB09]. vast [Wal04]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pei09, mSgFl05, WNQ08, WC05]. vectors [HL04a]. Vegas [ELvS01, IEE01a]. Vein [BDKB09]. Vendors [Pan03, MV03b].

Venona [Ben01b, Ben04]. venture [SW05b]. Verenigde [dL00]. Veridicom [An02d].

Verifiable [ANR01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Lys02, NZCG05, NZS05, NSN05, NN06, CHY05a, CDD00, GI001, KKL09, SC05a].

Verifiably [BDKB09], verifiably-encrypted [Hes04a].

Verification [AADK05, Ara02, BPS02, BP05, GM01, GL00, Gut02b, Gut04a, HWH01, Hoo11, Str01a, BD04a, CC05b, CJLO6, Col03, DS00, HL05c, JW01, ler02, MD04, MT07, MPP09, PBD07, Tsa08, TYH04, Wan04b, Wu01, YLC+09, ZL04, ZL04b, CS08b, Uzu04].

Verified [BJF02, BFG08, BFC08, CJT04]. verifier [Bla01b, LKY05b]. verifier-based
[LKY05b]. Verifiers
[CL01a, He02, LV07, LWK05b, YY05a, ZKX04]. Verify [MS02a]. Verifying
[BFG08, BJvdB02, CJM00, HLT01, IR01, PT08, RR02, BLH06, BLP06, HLH00, SV08a, Sha104]. Verlag
[Eag05, Lee03a, Lee03b, Pap05]. Version
[Bol02, HPC02, OSt05, SIt01, Mis06]. Versions
[HSR01, NPV01, AIt00f, CV05]. Versteckte
[Sch09]. Versus
[Mad00a, Rub00, WWL02, AIt01, BJLS02, DBS01, WPP05]. Vertically
[DN04]. Very
[AAC01, B02, CG03, EBC00, FLA03, H01, PM02, PBMB01, ZIt07]. Vestiges
[Top02]. VI [Sch04a]. via [AGKS07, An00k, ACm05, BDPV09, Car02, Che03, CPG04, Elb08, FBWC02, Fox00, HHYW07, HLM03, J00a, KT06, ML05, PG05, RG05, SB01, SLG05, ZLG01, Lud05]. Victoria
[ACM08, IZ00]. Victorian
[Top02]. victory
[Hau03]. Vid [CAC06]. Video
[BDF01a, BD03, CDTT05, EFY05, ISSZ08, KB03, KJR05, KLL01, LHS05, ML01, Sc02a, BS01b, CO09a, JA02, KN03, UP05]. Video-Based
[KJR05, BS01b, KN03]. videos
[YZDW07]. Vienna
[BZ02]. Vietnam
[Lov01]. View
[Bar00a, Mah04, Sin09, Woo05]. Views
[Bar00a, Bar00b, Bar00c, C01a, C02a, C02b, C03]. Vigenère
[DC00]. VII
[Sch04b]. VIII
[IEE01b, Sch05a]. Virginia
[MS05b]. Virtual
[An00c, HM01a, Pro00, YSS01, BDS09a, ML05, ZBP05]. virtualization
[CGL08a, CGL08b, CGL08c]. virtualization-based
[CGL08a, CGL08b, CGL08c]. Virtues
[Tro08]. Virus
[G06, An05c]. Visible
[HT06]. Vista
[Fer06]. Visual
[BDN00, BDDS03, BCD06, CCL09, CTH09, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, ZP05, ABDS01, CDFM05, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Z01]. Visualization
[XYL09, MFS09]. vital
[Wal04, Yout04]. Viterbi
[LBGZ01, LBGZ02]. Vladimirov
[Puz04]. VLDB
[EBC00, FLA03]. VLDP
[B02]. VLSI
[KV01]. VMSS
[SC05a]. Voice
[An00l, PK01, VN04]. VoIP
[An08c, SZ08, VAY09, WCJ05]. vol
[Cat05b, Lee03b]. volatile
[SETB08]. Volume
[Gol04]. Vortrag
[Eke02]. Vote
[Che07b]. Voter
[Cha04]. Voter-Verifiable
[Cha04]. Voting
[Cha04, FPS01, H00, J05, JLL02, KMO01, Rub01, CIt03, HJW05]. Voynich
[Rug04]. VPN
[KMM06]. VPNS
[Dav01a]. VQ
[WJP07]. VQ-based
[WJP07]. Vq
[CTBA01, D01, D03, SU07, WW04]. VSS
[A04b, CDF01, FM02a]. Vu
[DP00]. vulnerabilities
[CSW05, DMS07, Swi05, XNK05]. vulnerability
[KHL09, SGA07, YRS09].

WA [ACM06]. WACs
[K01]. Wagner
[dVP06]. Wagstaff
[Kat05b]. Wahab
[MA07]. Walking
[Fox00]. Wallet
[ET00, JL04]. Walsh
[MS02b]. Walsingham
[Bd00]. WAN
[H01]. WAN-Cluster
[H01]. Wang
[SZ05]. Wants
[Han00]. WAP
[JRFH01]. War
[Bc02, Bu00a, Bu02, Han03, K01, M09, OC03, A08, DB04, R06, Lov01]. Warfare
[HW01, WW04]. warrior
[PC04]. Wars
[RR03b, Cal00d, Cal00e]. Warsaw
[AU01, B03]. washer
[An01l]. Washington
[S03, USE00a, USE01c]. wasn’t
[Bu02]. WaSP
[C02b]. WASSA
[An05c]. Watch
[MA00a, Sav05a, Sav05b, An01m, Joy03a]. Waterloo
[HH04, H05, ST04d]. Watermark
[AS01b, GMV01, JX05, KHY04, K03a, M01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zau01, A08, CL08, LGL07, LCL06a]. Watermark-based
[K03a]. Watermark-Fingerprint
[KHY04].
Watermarked [ST01c]. Watermarking [AS08, AK02b, AHK03a, AS01c, Arn01, ARC+01, BBC+09, BR09, BSC01a, BSC01b, BS02, BQR01, BSN00, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB+08, DWN01, DN07, EFY+05, EIG01, GW01, HT06, HH09, JKK+01, KCR04, hKLS00, KLL01, Kun01, KT00, LZ09, LLS05a, LKLK05, LZ01, LSP05a, LPZ06, LJS05b, LSC03, L01, LLC05, MM01a, MNS01, Nak01, OMT02, PJH01, PJK01, PR01, PBM+07, QU01, Sam09, SOH01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SPK08, VVS01, VPH01, VK07, WC09, WH09, WNY09, WVL+02, WLT05b, XZF01, YWWS09, ZTP05, ZWC02, AHK03a, AAP07, BCKK05, CC02b, Che08b, CYH+07, CCD+04, CS05a, CC04c, CMB02, CKL05, DSP01, FMS05, GA03, HLC07, HHC05, JD01, JA02, KA09, KP00, LDD07, Lin00a, Lin01b, LL01a, LL06a, MB08, MCHN05].

watermarking [PK03, Ren09, mSgFtL05, WJP07, WNQ08, Way02b, Way09, WC05, WMDR08, XMST07, YZDW07, YPSZ01, ZLZS07].

Watermarks [Ben00, BB00a, MLC01, Sug01, WC04, YLLL02, MB08, TND+09].

Watershed [FBW01].

Watershed-from-Markers [FBW01].

WAV [XFZ01]. WAV-Table [XFZ01].

Wavelet [BR09, GW01, LKLK05, L01, Nak01, VK07, AAP07, AA08].

wavelet-based [AAP07, AA08].

Wavelet-Domain [LZ01]. WAVES [LBA00]. Way [BYYJ08, BM01a, CHL02, DIS02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, K00, LWT05, Sh00a, YZ00, AK02a, AGGM06, AGGM10, BYJ04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, K00, KKK05, K03, LW04, LPM05, LQ08, LKL01, Mic02a, Poi00, Tsa08, YW05, YRY05b, ZW05a].

Wayness [KI01a, PV06b]. Ways [BB02].

WCC [Ytr06]. WDDL [MMMT09]. Weak [HG03, LS01c, RW03b, DW09, G08, KOY09, KW00]. Weakening [ZD05].

Weakly [BS00a, CHS05]. Weakness [SW05a, SZS05, YPKL08]. Weaknesses [FMS01, He02, KCL03, KCC05, SGGB00].

Weapons [RR03b]. Weather [WWL+02].

Web [Che01d, Mar05a, BFG05, BFG08, Hl06, Ano01c, Ano02e, Ano03d, AEV+07, BFG04, BC04b, CCLYY01, Coc01a, Coc02a, Coc02b, CMB+01, DeL07, DMSW09, FSSF01, GS02a, GSV02, HM05, JRB+06, KCD07, LWK00, LLS05b, LXM+05, MPM09, PM00, RR04, Sam09, SSS06, Sch01a, SBS07, TMM05, WA06, YSS+01].

Web-Based [Ano01c, Sch01a, YSS+01].

Web-enabled [CCCY01].

Webcam [McN03]. WebFountain [Ano03d].

Webrelay [Zha00].

Weight [CH07c, G02, WT02]. Weighted [BTW05, BTW08, SC02c, YZ00].

Weil [BF01b, BF03, Jou02, Kir03].

Well [WWGP00]. Welschenbach [Ter08].

Welsh [Rot07]. went [AJ08]. WEP [SIR04].

were [Hau06]. Wesley [Puc03].

West [Fra01, Jue04, Syv02, Wri03].

Western [Ano02a].

[WCZ+01]. Wet [CC09].

Weyl [Sug03].

WG [DFPS06]. WG11.1 [ELvS01]. WG11.1/WG11.2 [ELvS01].

WG11.2 [ELvS01].

WGL8.8 [DFCW00].

Wheeler [ABM08, Bar05]. Where [Bur06, F01a].

While [Tee06]. WHIM [JA02].

WHIRLPOOL [RB01]. Whisper [NABG03].

Whitehouse [Mad00c].

Whitening [Oni01]. Whitfield [Jan08a].

Who [CMB+01, Urb01, Hau06, Neu06].

whole [CGP+04].

Wi [Puz04, Sty04, VGM04, FMA02, Bar03].

Wi-Fi [Sty04, Bar03].

Wi-Foo [Puz04, VGM04]. wicked [Lud05].

Wide [DR02a, SBB05].

Width [OT03b]. Width-OT03b. Wiener [Duj08, Duj09].

WIESS [USE00b].

Wiley [And04, Gra01, Kir01a].
REFERENCES

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

Yang-Shieh [YWC05].  Yao [BPS08, BDNN02, ZD05].  Yeao-style [BPS08].

Yarrow [KSF00, Mur02].  Yarrow-160 [KSF00].  Yaschenko [Kat05b].

YCH [SC05a].  YCN [Hwa00].  Year [Eva09, Naz02, Bur00].  Years [Ahm08, CM02, Ros04].

Yellow [JYZ04].  Yen [LLLZ06a, LLLZ06b].  Yen-Guo [LLLZ06a].  Yesterday [Coc02a].

Yi [Wag00].  Yi-Lam [Wag00].  Yokohama [Mat02].  Yoo [KCC05, KHKL05].  Yoon [KCC05].

York [HR06, IKY05, NIS00, Sch01d, YDKM06].  Young [FF01b].  You’re [ES00a, Nic01].

You’ve [Nic01].  Yuck [Sas07].  Yuen [KH08].

Z [Wue09].  Z-parameter [Wue09].  z10 [Web08].  z9 [ADH+07].  Zealand [Zhe02b].

Zeilinger [Duw03].  Zero [AS01b, APV05, BP04, Cou01, DPV04, DFS04, DDO+01, HNO+09, IKOS07, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00a, Ros06a, CSW05, Dam00, PBD07, KK07].  zero-day [CSW05].

Zero-Knowledge [AS01b, BP04, Cou01, DFS04, HNO+09, LHL+08, MR01b, MV03a, Pas05, Ros00a, Ros06a, IKOS07, Dam00, PBD07].  Zeta [Ver02].  Zhang [JW01, YY05a].  Zhou [PKH05].  Zimmermann [McL06, Tuc66].  ZK [PBD05].  Zodiac [HSM+02].  Zone [Kum07].

References

XXX:2002:CC

Al-Akaidi:2004:FSP

Aly:2004:CSP

Agresti:2008:NAP
REFERENCES


REFERENCES


REFERENCES

Aiello:2004:JFK


Abdalla:2005:SER

Abe:2004:CEP


Abadi:2005:CFI


Adao:2009:SCF


Anderson:2000:CS


Austin:2000:ASF


Adjeroh:2008:BWT

Abdalla:2001:ODH


Ansper:2001:ELT


Ambainis:2009:NEQ


Adcock:2002:QGL


Ateniese:2005:URT


Ateniese:2000:PPS

Giuseppe Ateniese, Jan Camenisch, Marc Joye,


ACM:2003:PTS


ACM:2004:PAS


ACM:2004:PAA


ACM:2005:MPI


ACM:2005:PTF


ACM:2005:SPA


ACM:2006:PTE

REFERENCES


Ahmad:2007:ADE


Anyanwu:2009:DCS


Avanzi:2006:ESM


Adee:2009:CDT


Arnold:2007:CSE

Adikari:2009:HBT


Adleman:2003:TLP


An:2002:SJS


Ahmed:2017:IRD


Atighehchi:2009:EPA

[KAE] Kévin Atighechhi, Adriana Enache, Traian Muntean,


[GH06] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM

**Attrapadung:2006:FSS**

**Akkar:2001:IAS**

**Acquisti:2009:PSS**

**Akavia:2006:BOW**

**Akavia:2010:EBO**
REFERENCES


[AH05] David Ahmad. The contemporary software security landscape. *IEEE Se-
Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB


Applebaum:2004:CNS


**Applebaum:2006:C**


**Al-Ibrahim:2001:AMS**


**Attali:2001:JSC**


**Attali:2001:SCP**


REFERENCES

Akinwande:2009:AHC


Amir:2004:PGK


Agrawal:2002:PP


Aciicmez:2006:PSB


Agrawal:2004:OPE


Amadio:2000:RPC

REFERENCES


REFERENCES

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


REFERENCES


REFERENCES

Anonymous:2000:AIH

Anonymous:2000:Alah

Anonymous:2000:CRR

Anonymous:2000:CLI

Anonymous:2000:EES

Anonymous:2000:GBE
Anonymous:2000:PESa


Anonymous:2000:PTD


Anonymous:2000:SES


Anonymous:2000:UAS


Anonymous:2000:VAS


Anonymous:2001:AAPb


Anonymous:2001:ANT


Anonymous:2001:AWB


Anonymous:2001:RAC


Anonymous:2001:EDS


Anonymous:2001:EER
REFERENCES

Anonymous:2001:EMB [Ano01i]

Anonymous:2001:LBS [Ano01j]

Anonymous:2001:MLF [Ano01k]

Anonymous:2001:MIT

Anonymous:2001:NWS

Anonymous:2001:PKC
Anonymous:2001:SCS


Anonymous:2001:TAD


Anonymous:2002:DEC


Anonymous:2002:PPD


Anonymous:2002:NSD


Anonymous:2002:IHB

REFERENCES

Anonymous:2002:PSS


Anonymous:2002:PFQ


Anonymous:2002:QCQ


Anonymous:2002:QCR


Anonymous:2002:RUB


Anonymous:2003:TMC

[Ano03a] Anonymous. For Taiwan’s 22 million citizens, Java

Anonymous:2003:YCS


Anonymous:2003:NAW


Anonymous:2003:NUP


Anonymous:2003:SEY


Anonymous:2003:TMP


Mersenne primes are primes of the form $2^p - 1$. 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. Fauquembergue</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1876</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>19</td>
<td>4423</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>20</td>
<td>8969</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>21</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>22</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>23</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>24</td>
<td>21701</td>
<td>1978</td>
<td>L. O. Noll &amp; L. Miller</td>
</tr>
<tr>
<td>25</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>26</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson &amp; D. Slowinski</td>
</tr>
<tr>
<td>27</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>29</td>
<td>132049</td>
<td>1983</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>30</td>
<td>216091</td>
<td>1985</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>31</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
</tr>
<tr>
<td>32</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich, George Wolrtman, Scott Kurowski (GIMP)</td>
</tr>
<tr>
<td>33</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo (GIMS)</td>
</tr>
<tr>
<td>34</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, George Wolrtman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>35</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, George Wolrtman, Scott Kurowski, and others</td>
</tr>
<tr>
<td>36</td>
<td>6972593</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>37</td>
<td>74207281</td>
<td>2016</td>
<td>Curtis Cooper (GIMPS)</td>
</tr>
<tr>
<td>38</td>
<td>77232917</td>
<td>2017</td>
<td>Jon Pace (GIMPS)</td>
</tr>
<tr>
<td>39</td>
<td>82589933</td>
<td>2018</td>
<td>P. Laroche, G. Wolrtman, A. Blosser, et al. (GIMPS)</td>
</tr>
</tbody>
</table>

REFERENCES


REFERENCES


REFERENCES


Anonymous: 2009: BG


Anonymous: 2009: DSS


Anonymous: 2009: PCA


Anonymous: 2009: TCA


Anonymous: 2012: SHS


Anonymous: 2013: DSS

REFERENCES


REFERENCES


Alomair:2009:ITS


Appenzeller:2005:IBE


Abdalla:2000:NFS


Arboit:2001:FLM

Geneviève Arboit and Jean-Marc Robert. From


Arnold:2001:AWB


Agrawal:2003:MCA


Abe:2001:SPA


Adelsbach:2001:ZKW


Artail:2004:PAC


Agung:2001:ICI

[AS01c] I. Wiseto Agung and Peter...

Agarwal:2008:DWS


Asenjo:2002:AES


Ashburn:2003:PBA


Aciicmez:2005:IBB


Aciicmez:2007:MAC


Aslan:2004:HSM

Aslan:2004:LAA


Blanchet-Sadri:2001:MSD


Abdalla:2000:KMR


Asl04b


Blanchet-Sadri:2001:MSD


Androutsellis-Theotokis:2004:SPP

Aharonov:2000:QBE


Alster:2001:PKC


Arnold:2004:IPN


Avanzi:2003:CAD


Aalberts:2000:DSB

REFERENCES


Abadi:2005:SAC

Abadi:2008:SAC

Ayoade:2006:SIR

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

Blanton:2006:SRF

Bagnulo:2002:PAA

Badra:2007:AWC
Mohamad Badra. Alterna-
References


[Bai08]


[Bai01a]

Baier:2001:ECP

[2001:ECS]


[Bai01b]

Baier:2001:ECS


[Bam02]

Bamford:2002:BSA

William D. Banks. Towards faster cryptosystems, II. In Garrett and Lie- man [GL05], pages 139–
REFERENCES


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

Barron:2005:DWP


Barkan:2006:CCP


Barker:2006:ROA


Bauer:2000:DSM


Bauer:2001:PPGa


Bauer:2001:PPGb

REFERENCES

Bauer:2001:PPUb

Bauer:2002:DSM

Bauer:2002:PPB

Bauer:2003:PPAa

Bauer:2003:PPAb

Baudet:2005:DSP

Bauer:2007:DSM

Blakley:1979:RSA
G. R. Blakley and I. Borosh. Rivest–Shamir–Adleman public key cryptosystems do not

**Benedens:2000:TBD**


**Buchmann:2000:ECC**


**Barkan:2002:HMW**


**Bouda:2003:EQI**


**Boneh:2004:SIB**

REFERENCES


Beimel:2000:CFS


Bellare:2001:KPP


Blumenthal:2002:SAD


Bartolini:2008:EIS


Barkan:2003:ICO

REFERENCES


REFERENCES

134


REFERENCES


REFERENCES


[BCG+02] H. Barnum, C. Crepeau, D. Gottesman, A. Smith,

[BCHJ05]


[BCHJ11]


[BCGH11]


[BCHK07]


[Boneh:2007:CCS]


[Brown:2000:PCW]


[Buch:2011:ECS]


[Breunesse:2005:FMS]


[Buch:2011:ECS]


[Butler:2006:FAK]


REFERENCES


REFERENCES

139

0558/papers/2332/23320321.pdf.

[BCT02] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval.

[BCTP02b] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval.

[BCP07] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval.

[BCP+B03] Ruud Bolle, Jonathan Connell, Sharatchandra Pankanti, Nalini Ratha, and Andrew Senior.

[BCT08] E. Biham, Y. Carmeli, and A. Shamir.

[BCST00] Gustavo Betarte, Cristina Cornes, Nora Szasz, and Alvaro Tasistro.
Specification of a smart card operating system. *Lecture Notes in Computer Science*, 1956:77–??, 2000. CODEN LNCSD9. ISSN 0302-
Bao:2005:RWH


Biham:2000:CAG


Boneh:2000:CRP


Bourbakis:2003:SBC


Bozzano:2004:AVS


Burmester:2004:HPK

Mike Burmester and Yvo G. Desmedt. Is hierarchical public-key certification the next target for hackers? Communications of the Association for Computing Machinery, 47(8):68–74, August 2004. CODEN CACMA2. ISSN 0001-0782
141

REFERENCES

Buchmann:2008:PQC

Biryukov:2003:CS

Bolosky:2000:FSD

Bao:2001:SPD
REFERENCES

[102x681] Bibs/2119/21190190.htm;


[Bam:2002:EDL] Eli Biham, Orr Dunkelman, and Nathan Keller. Enhanc-
REFERENCES


Biham:2002:LCR


Biryukov:2009:KRA


Blundo:2000:VCG


Bodei:2002:FLD


Boreale:2002:PTC

[BDP02] Michele Boreale, Rocco De Nicola, and Rosario

Bertoni:2009:RPK


Biryukov:2004:MLA


Buchmann:2009:HBD


Bertolotti:2008:ERA

REFERENCES

10.1007/s00165-008-0078-3.


[Bel00] Mihir Bellare, editor. Advances in cryptology —
REFERENCES


Bella:2001:MPS


Bellovin:2004:IRS


Belfield:2007:SUC


Bella:2007:FCS


Bello:2008:OPR


Bruss:2007:QCS

Benedens:2000:AIW


Benantar:2002:IPK


Benson:2001:VS


Berson:2000:CE

REFERENCES


REFERENCES

[Bouwmeester:2001:PQI]

[BF00a]

[BF00b]

[Babbage:2001:MHO]

[Boneh:2001:IBE]
REFERENCES


[BFG04] Karthikeyan Bhargavan, Cédric Fournet, and Andrew D. Gordon. A seman-

Bhargavan:2005:SWS


Bhargavan:2008:VPB


Bhargavan:2008:VII


Bugliesi:2007:DTA


Biham:2002:DCQ


Brown:2007:SAN

REFERENCES

[152]


[Bugliesi:2007:SIT]


[Blaszczyk:2008:NMT]


[BG08]


[Boneh:2007:SEI]


[BG09]

REFERENCES


Barak:2001:IPO


Bogomjakov:2008:PMD


Bertoni:2003:EAA


Bucci:2003:HSO


Boneh:2003:AVE

Dan Boneh, Craig Gentry, Ben Lynn, and Hoory Shacham. Aggregate
REFERENCES


REFERENCES

[BGP09] Berbain:2009:QMS


[BGW05] Boneh:2005:CRB

[BH00a] Beck:2000:FSD

[BH00b] Bialaski:2000:SLN
Tom Bialaski and Michael Haines. *Solaris and LDAP Naming Services: Deploying LDAP in the Enterprise*. Sun BluePrints
REFERENCES


Barak:2005:MAP


Badra:2006:KEA


Backhouse:2003:TOT


Bajard:2004:FRI


Barkol:2005:SCC


Beimel:2005:PNS


**Bi:2009:MCE**


**Bidgoli:2003:EIS**


REFERENCES

[159]


**Bishop:2003:CSA**


**Barkol:2008:CPR**


**Boyce:2002:IAM**


**Blaser:2002:PCC**


**Boneh:2000:WTE**


**Bjorn:2005:BHM**


[BK06b] L. Breveglieri and I. Koren. Guest Editors’ introduction: Special section on fault diagnosis and tolerance in cryptography. IEEE Transac-
Barker:2007:RRN

Breveglieri:2007:OCA

Bellare:2004:BPR

Bajard:2009:SRB
REFERENCES


[Bru:2008:FDR] Michael Andrew Black. A treatise on data encryption and an example of the black algorithm. Thesis (M.A.), University of California, Santa Barbara,
REFERENCES


REFERENCES

Burmester:2009:UCR

Bleumer:2007:EPS

Bao:2006:CIB

Berbecaru:2001:CPK

Brassard:2000:SAP
Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Security

**Bozga:2006:PBA**


**Buchmann:2009:PQC**


**Banks:2001:CAS**


**Blunden:2009:RAE**


**Batina:2001:AWD**

Lejla Batina and Geike Muurling. Another way of doing RSA cryptography in hardware. Lecture Notes in Computer Science, 2260:364–??, 2001. CO-
REFERENCES


REFERENCES


REFERENCES

[BMN01] Colin Boyd, Paul Mon-tague, and Khanh Nguyen. Elliptic curve based pass-
word authenticated key exchange protocols. Lecture
Notes in Computer Science, 2119:487–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electric). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2119/21190487.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2119/21190487.
pdf.

[BM00] Victor Boyko, Philip MacKen-
zie, and Sarvar Patel. Provably secure password-
authenticated key exchange using Diffie–Hellman. Lecture
Notes in Computer Science, 1807:156–??, 2000. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-
3349 (electric). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/1807/18070156.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1807/18070156.
pdf.

[BMS03] Dan Boneh, Ilya Mironov, and Victor Shoup. A se-
cure signature scheme from bilinear maps. In Joye
[Joy03b], pages 98–110. CO-
DEN LNCSD9. ISBN 3-540-
00847-0. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C822 2003. URL http:
//link.springer-ny.com/
link/service/series/0558/
tocs/t2612.htm; http://
www.springerlink.com/
openu1.asp?genre=issue&
issn=0302-9743&volume=2
612.

[BMV06] Johannes Buchmann, Alexan-
der May, and Ulrich Vollmer.
Perspectives for crypto-
graphic long-term security. Communications of the Association for Comput-
ing Machinery, 49(9):50–55,
September 2006. CODEN
CACMA2. ISSN 0001-0782
(print), 1557-7317 (elec-
tronic).

[BW02a] Niklas Borselius, Chris J.
Mitchell, and Aaron Wil-
son. On the value of threshold
signatures. Operating
Systems Review, 36(4):30–
35, October 2002. CODEN
OSRED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic).

[BW02b] Niklas Borselius, Chris J.
Mitchell, and Aaron Wil-
son. A pragmatic alter-
native to undetachable sig-
REFERENCES

[102x681] 169


**Boyen:2005:DCC**


**Bellare:2002:TSB**


**Bouganim:2008:DAC**


**Bellare:2000:AER**


**Boneh:2000:TC**

Dan Boneh and Moni Naor. Timed commitments.
REFERENCES


REFERENCES

xx + 459 pp. LCCN QA76.73.B3 B665 2000.


[Bor01] Michele Boreale. Symbolic trace analysis of cryptographic protocols. Lecture Notes in Computer Science,
REFERENCES

Barak:2003:DC

Barak:2007:DC

Boyen:2003:MIB
REFERENCES


REFERENCES

Bellare:2005:ISA


Boneh:2008:IBI


Baudron:2000:ENS


Backes:2008:KDM


Benerecetti:2002:VST

Massimo Benerecetti, Maurizio Panti, Luca Spalazzi, and Simone Tacconi. Verification of the SSL/TLS protocol using a model checkable logic of belief and time. Lecture Notes in Computer Science, 2434:
REFERENCES


REFERENCES

Black:2002:BCM

Bellare:2004:CBG

Bugliesi:2005:NIP

Bellare:2006:MPP

Bhatnagar:2009:RRW

Brands:2001:RPK

**Brackenridge:2006:IUU**


**Brown:2005:CEC**


**Browne:2005:DEP**


**Black:2002:BBA**


**Butler:2009:LIB**


**Brustoloni:2006:LEN**

José Carlos Brustoloni. Laboratory experiments for network security instruction.
REFERENCES


Bierbrauer:2000:AIW


Biryukov:2000:CTM


Barrett:2001:SSS


Bigun:2001:AVB

REFERENCES


[BSL02]

Bo:2001:EID


[BSC01a]

Bo:2001:SCD


[BSC01b]

Brisbane:2000:RBW


[BSS02]

Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold ring signatures and applications to ad-hoc
REFERENCES


Blake:2004:AEC

[BS04]


Blake:2005:AEC

[BSS05]


Bhargav-Spantzel:2007:PPM


Buchmann:2002:ICP

REFERENCES


REFERENCES


publications/library/proceedings/sec02/black.html.


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.


[Bur00] Frank Burmannsson. Travel cards in the year 2000: the Helsinki region ushers in the smart card era. *Urban public transportation systems,
REFERENCES

pages 229–238; Engineers 2000.


REFERENCES


[BZ02] Reinhold A. Bertlmann and Anton Zeilinger, editors. Quantum Un/speakables: From Bell to Quantum Information: Conference in Commemoration of the Physicist John S. Bell, 10–14 November 2000, Vienna. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,
REFERENCES


[CAC03] 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).


by the California Attorney General. Initiative #905.

**CAMTC:2000:TSC**


**Caloyannides:2000:EWE**


**Caloyannides:2000:EWS**


**Calvocoressi:2001:TSU**


**Canetti:2001:UCS**


**Canteaut:2001:CFD**


**Canetti:2006:SCC**


**Canteaut:2006:OPR**

[Can06b] Anne Canteaut. Open problems related to algebraic attacks on stream ciphers. In
The front cover of this issue displays eight pages of Alan Turing’s description of the Enigma machine. The issue is a special tribute to Kurt Gödel for the centenary of his birth.

Cobas:2001:CTA

Challal:2005:HHC

Cooper:2005:AAP

Chandramouli:2006:BPA

Cachin:2000:OFS
REFERENCES


Zhenchuan Chai, Zhenfu Cao, and Xiaolei Dong.

[Cattaneo:2001:DIT]


[Chang:2009:PCC]

Chin-Chen Chang, Tzung-Her Chen, and Li-Jen Liu. Preventing cheating in computational visual cryptography. *Fundamenta Informaticae*, 92(1–2):27–42, January 2009. CODEN FU-
REFERENCES

MAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

Christianson:2001:PKC

Choi:2005:JMA

Christianson:2002:SPI

Christianson:2005:SPI
REFERENCES

Castelluccia:2009:EPS


Chen:2008:NMA


Caboara:2008:GBP

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

Choi:2002:IPP


Camenisch:2000:VEG

REFERENCES


REFERENCES

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


[Cavallar:2000:FBR] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist,

Cortier:2006:SAP


Cramer:2000:GSM


Chawla:2005:TPP


Coron:2005:MDR

Cramer:2001:MCT

Chapman:2001:PEA

Castiglione:2007:TAD

Chen:2005:NVW

Ceravolo:2004:ERH

Certicom:2004:CCC
Code & Cipher: Certicom’s Bulletin of Security and Cryptography,
REFERENCES

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

Canetti:2001:UCC


Canteaut:2001:COR


Cramer:2002:OBB


Clarke:2005:AUM


Clarke:2007:AUA

REFERENCES

Cohen:2006:HEH
Henri Cohen, Gerhard Frey, Roberto Avanzi, et al., editors. Hand
dbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete
mathematics and its applications. Chapman and Hall/CRC, Boca

Clarke:2002:ASA
N. L. Clarke, S. M. Furnell, P. M. Rodwell, and P. L. Reynolds. Accep-
tance of subscriber authentication methods for mobile telephony
deVICES. Computers & Security, 21(3):220–228, June 1, 2002. CODEN
CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL https://

Courtois:2001:HAM
Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve
a McEliece-based digital signature scheme. Lecture Notes in

Computer Science, 2248:
157–??, 2001. CODEN
LNCS09. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/bibs/2248/22480157.

Cramer:2005:BBS
Ronald Cramer, Serge Fehr,
and Martijn Stam. Black-
box secret sharing from primitive sets in alge-
braic number fields. In Shoup [Sho05a], pages
344–?? ISBN 3-540-
28114-2. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2005; QA76.9 .A25:
QA76.9 C79 2005; QA76.9
C794 2005; QA76.9; In-
ternet. URL http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3621.

Climent:2006:NEC
Joan-Josep Climent, Francisco Ferrández, José-Francisco Vicent, and Antonio Zamora. A nonlinear elliptic curve cryptosystem based on ma-
trices. Applied Mathematics and Computation, 174
(1):150–164, March 1, 2006. CODEN AMHCBQ. ISSN
Chang:2010:PRN


Chodowiec:2003:VCF


Cranor:2005:SUD


Candebat:2006:SPM


Chodowiec:2001:ETG

REFERENCES


[CGL+08b] Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmanym, Carl A. Waldspurger, Dan Boneh, Jeffrey Dwoskin, and Dan R. K. Ports. Overshadow:
REFERENCES


**Chen:2008:OVBc**


**Canovas:2002:DSB**


**Cimato:2003:SCN**

Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors. *Security in communication net-


REFERENCES


REFERENCES

210


REFERENCES


Chen:2004:IAM


Cheng:2004:BSD


Chen:2005:TSS


Cherry:2005:MDC


Chess:2005:SAC


Chen:2007:CIS


Cherry:2007:MEV

REFERENCES

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


REFERENCES

Coppersmith:2002:CSC


Canetti:2003:FSP


Canetti:2005:ASN


Cheon:2008:PST


Chang:2002:IBO

REFERENCES


Christianson:2001:SPI

Canetti:2005:HAW

Chen:2002:AMT

Cornea:2002:SCI

Churchhouse:2002:CCJ
Robert F. Churchhouse. *Codes and Ciphers: Julius Caesar, the Enigma, and the...*
REFERENCES


Canvel:2003:PIS


Chang:2005:ILW


Chang:2005:NMS


Cimato:2002:DAP


Cirstea:2001:SAP

REFERENCES


Cheon:2003:PTA


Chien:2003:RSA


Chien:2004:IAM


Chien:2005:EDS

[CJ05] Yi-Hwa Chen and Jinn-Ke Jan. Enhancement of digital signature with mes-
REFERENCES


Cornwall:2004:AAM


[Choie:2005:EIB]

Young Ju Choie, Eunkyung Jeong, and Eunjeong Lee. Efficient identity-based authenticated key agreement protocol from pairings.

Chin:2006:HSI


Clarke:2000:VSP


Coron:2000:NAP


Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-

Chung:2003:EPX


Chung:2003:DLC


Chen:2009:SRP


Coppersmith:2000:KRF

Don Coppersmith, Lars R. Knudsen, and Chris J.
REFERENCES


Cachin:2001:SEA


Cathalo:2003:NTT


Chevalier:2008:CRS


Cachin:2009:TC


Chen:2005:CLR

Chien:2007:CRA


Chen:2000:IBD


Chen:2001:CIU


Camenisch:2001:IES


Cao:2002:TKE

Zhen Fu Cao and Ji Guo

Crowley:2002:BLS


Camenisch:2004:SSA


Chang:2004:CGS


Chang:2004:IDM


Chang:2004:RFB


Camenisch:2005:FTO

[CL05] Jan Camenisch and Anna Lysyanskaya. A formal treatment of onion routing. In Shoup [Sho05a], pages 169–?? ISBN 3-540-28114-2. ISSN 0302-9743
Chandramouli:2007:ISS


Chang:2008:AWM


Chien:2009:EBL


Clark:2000:TNE


Clark:2000:LNC

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

Chen:2008:RCE

Chang:2001:ASM


Chang:2001:FAM


Cheon:2000:NBC


Canetti:2002:UCT


Cormen:2001:IA

REFERENCES


Chen:2009:AKD


Chang:2007:SIH


Clulow:2003:SP


Czumaj:2002:PTA


Camenisch:2000:CSS

REFERENCES


[CMB05] Diane Crawford, Marius Matioc, Steven M. Bellovin, Richard Hubert, Andrew D. Wolfe, Jr., David Foulser, and Andrew R. Kilner. Forum: To block spam,
demand sender authentication; not revolutionary (thank goodness); how to know the known from the unknowns; user first in user-centered design. Communications of the Association for Computing Machinery, 48(3):11–13, March 2005. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

[Cox:2008:DWS]

[CMdV06]

[Cam:2001:JFC]

[Chevallier-Mames:2003:FDS]


Ciet:2003:PFI
M. Ciet, M. Neve, E. Peeters, and J.-J. Quisquater. Parallel FPGA implementation of RSA with residue number systems — can side-channel threats be avoided? In MWSCAS ’03. Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems, volume 2, pages 806–810. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. CODEN ???, ISSN ???.

Catalano:2002:HHL

Correia:2006:CAB

Cetin:2009:NSA

Czernik:2009:CRN


REFERENCES


REFERENCES


[Cos00] John Cosgrave. Number theory and cryptography...
REFERENCES

(239)

Costlow:2003:BIM


Courtois:2001:EZK


Courtois:2003:FAA


Courtois:2004:FSB


Courtois:2002:CBC

REFERENCES


Courtois:2003:AXA

Chatzikokolakis:2007:FAP

Cimato:2006:PVC

Chow:2004:UDL

Chen:2004:SEP
Catalano:2004:IIP


Canetti:2007:CSH


Ciet:2001:SFC


Canetti:2003:UCJ

Cramer:2005:ACE


Crampton:2005:UDR


Crenshaw:2000:SPK


CRI:2000:DPA


Crowley:2001:MFL


Chhabra:2009:MSP

REFERENCES

Cramer:2000:SSB

Cramer:2002:UHP

Camenisch:2003:PVE

Cramer:2003:DAP

Crepeau:2003:SBR


S. Chatterjee and P. Sarkar. Constant size ciphertext
REFERENCES


REFERENCES

**Chen:2008:CCS**


**Collberg:2002:WTP**


**Coron:2003:NAS**


**Chen:2008:BUK**

L. Chen and Q. Tang. Bilateral unknown key-share attacks in key agreement

**Chung:2009:ISA**


**Collberg:2002:WTP**


**Coron:2003:NAS**


**Chen:2008:BUK**

L. Chen and Q. Tang. Bilateral unknown key-share attacks in key agreement


REFERENCES


Collberg:2007:DGB


Chen:2009:FCV


Cheng:2001:NPT


Curtin:2005:BFC


Chaitanya:2008:QQM


Canteaut:2002:DCH

[CV02] Anne Canteaut and Marion Videau. Degree of com-


REFERENCES

Canda:2001:SBC


Chang:2002:ATI


Chess:2007:SPS


Cheng:2009:NAS


Chang:2000:ELD


Chien:2001:CCW

References


Chin-Chen Chang, Jyh-Chiang Yeh, and Ju-Yuan Hsiao. A novel scheme for securing image steganog-

Chang:2005:SAK


Chen:2003:AEY


Chadwick:2005:PKI

David Chadwick and Gansen Zhao, editors. *Public

Crawford:2001:FHC


Cheng:2005:RIC


Dodis:2003:CAA


Dale:2001:BSA

REFERENCES

[Dam00]

[Dam07]

[Dan01]

[Dan02]

[Das08]

[Davis01a]

[Davis01b]

[Davis01c]
Don Davis. Defective sign-and-encrypt: Can you really trust S/MIME, PKCS#7, PGP, and XML? Dr. Dobb’s
REFERENCES

Davis:2007:AAA


DeBrosse:2004:SBU


DeBorde:2007:STF


DBS01


Doyle:2006:SCK

diVimercati:2005:CSE


DeBonis:2000:RVC


Dalkilic:2002:CPF


DeBonis:2004:RSS


Diene:2006:DLE


Dolev:2000:NC

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


Roger Dean. Identity management — back to the user.

Roger Dean. Identity management — back to the user.


Desai:2000:SAN


Desmedt:2002:PKC


Dewson:2008:BSS


Dhem:2001:HSS


Delgado:2007:SCD
REFERENCES


[DFH01] Josep Domingo-Ferrer and


Durante:2001:CWR


DePalma:2004:CCS


Dodis:2003:IRP


DeSantis:2004:CKA


Domingo-Ferrer:2006:SCR


Domingo-Ferrer:2007:ASC


Damgaard:2004:ZKP

Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-

**Damgaard:2005:CBQ**


**Damgaard:2008:CBQ**


**Dalkilic:2000:ICA**


**Debaert:2002:RRI**


**DiRaimondo:2003:PST**

REFERENCES


DiRaimondo:2005:NAD


DiRaimondo:2006:PST


Dodis:2004:REK


Devanbu:2004:FAX


Devanbu:2003:ADP


Dwork:2003:MBF

REFERENCES


REFERENCES


[Iv 05] Ivan Damgård and Yu-


REFERENCES


[Din01]

[Din05]


REFERENCES

267


Donsez:2001:TMA


Damgaard:2001:PTR
Delfs:2002:ICP


Dodis:2005:CCS


Delfs:2007:ICP


Dunkelman:2008:TIV


Du:2005:BRS


Daswani:2007:FSW

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


REFERENCES

[Dittmann:2005:CMS]

[DKU05]

[DKXY02]

[DL98]

[DL00]

[DL07]

[Diffie:1998:PLP]

[deLeeuw:2000:CSD]

[dL00]

[dLB07]
Karl de Leeuw and J. A. Bergstra, editors. *The history of information security:...


DeSantis:2007:NRN


Drimer:2007:KYE


Dumais:2000:PCQ


Dowd:2007:ASS


Denev:2009:SFQ


Ding:2007:ESD

REFERENCES


Damgaard:2003:UCE


Dwork:2004:PPD


Dwork:2004:PPD


Dwork:2003:MFM


Dwork:2005:PPW

DODIS:2005:GIF

DODIS:2004:IPC

DHAMIJA:2000:DVU

DEMATTEIS:2002:PP

DANDALIS:2004:ACE
REFERENCES

Dziembowski:2007:IRS


Dziembowski:2008:LRC


Dandalis:2001:CSP


Damgaard:2005:QCN


Delbourg:2002:JBC


Daemen:2001:BCP

REFERENCES


REFERENCES

[Daemen:2001:AAR]

[Daemen:2002:AWT]

[Daemen:2002:DRA]

[Ding:2002:HEE]
REFERENCES


Dobbertin:2005:AES


Devanbu:2000:CVT


Dodis:2002:NUO


DArco:2003:FTD


Ding:2005:RNM

J. Ding and D. Schmidt. Rainbow, a new multivariate polynomial signature scheme. *Lecture Notes in Computer Science*, 3531:
REFERENCES

164–175, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dodis:2005:ESE


Ding:2006:SSS


Dinur:2008:CAT


Deepthi:2009:DIA


Das:2006:NRU


Djurovic:2001:DWF


REFERENCES

283

of Technology, Haifa, Israel, 2006. x + 204 pp.


See [BEZ01].


[DU01] Wei Zhang Du and Xin Mei Wang. One kind of secret-code encryption scheme


Dittmann:2001:UCW Jana Dittmann, Petra
REFERENCES


REFERENCES


REFERENCES


[EHK+03] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and
REFERENCES


Ernst:2004:FBH


Ellison:2000:PSK


Ekert:2002:BTQ


Ekeraa:2009:DCM

El-Kassar:2001:GPK


Elbirt:2008:AAI


Elbirt:2009:UAC


Elliott:2004:QC


Eloff:2001:AIS


Everitt:2003:JB1


English:2000:MNDb

REFERENCES

August 2000. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).


Ellison:2000:TRP


Ellison:2000:IRRa


Eberle:2005:ANG


Enck:2005:EOF


Ettinger:2002:QQC


Ebringer:2000:PAP

Evans:2009:BRS


Edman:2009:AES


Elbirt:2000:FIP


Faliszewski:2007:BRB


Fan:2003:ILC


Faugere:2009:IBC

Jean-Charles Faugère. Interactions between com-
puter algebra (Gröbner bases) and cryptology. In May [May09], pages 383–384. ISBN 1-60558-609-9. LCCN ???.

**Ford:2001:SEC**


**Felkel:2001:ICW**


**Feghali:2002:SAP**


**Fan:2005:RRA**


**Fischer:2001:TMR**

REFERENCES


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


REFERENCES


Field:2009:BCB


Field:2009:BCB

Filiol:2000:DAS


Filiol:2000:DAS

Filiol:2002:NST


Filiol:2002:NST

Finley:2002:BSE


Finley:2002:BSE

Finkenzeller:2003:RHF


REFERENCES


REFERENCES


F. Faugère:2003:ACH


F. Ferguson:2001:ICRb

F. Ferguson:2001:ICRa

F. Ferguson:2000:ICR

F. Ferguson:2000:ICRb

REFERENCES


[Freytag:2003:VP1] Johann Christoph Freytag, Peter C. Lockemann, Serge Abiteboul, Michael J. Carey, Patricia G. Selinger, and Andreas Heuer, edi-
Fluhrer:2002:CMB


Fluhrer:2002:CSP


Feng:2006:ISC


Fan:2002:ETB


Fehr:2002:LVD

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


REFERENCES


REFERENCES

Foster:2005:BOA

Frincke:2006:ESI

Fujisaki:2001:ROS


Forbes:2004:BRN

Forte:2009:DM

Fox:2000:NTFb
[Fox00] Robert Fox. News track: Flying the rails; logging online hours at work; top prize: embedded encryption; Digital Nose knows; walking again via chip implant; cellphone-free class; another

Freking:2000:MMR


Fouque:2001:TCS


Fauqere:2009:EAD


Fouque:2001:SDC


Fernandes:2002:SAL

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

Fournet:2008:CSI


Frankel:2001:FCI


Franklin:2004:ACC


Fremberg:2003:MAP


Friberg:2001:UCH

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


Fischer:2002:NFC


Ferguson:2003:CEI


Ferguson:2003:PC


Fundulaki:2004:SYD


Fortnow:2008:IIC


Fuster-Sabater:2001:EAG

REFERENCES


[Furnell:2005:AOW] [Fur05] Steven Furnell. Authentication
cating ourselves: will we ever escape the password?


[FW04] Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger. Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In Franklin [Fra04], pages 562–?? CO-

Fan:2004:PPI


Furnell:2006:RPS


Gang:2005:CNI


Galbraith:2001:SCC


**Galbreath:2002:CID**


**Gallo:2003:SST**


**Ganger:2001:AC**


**Gannon:2001:SST**


**Ganti:2008:PAL**


**Garrett:2001:MBC**


**Garfinkel:2003:EBI**

REFERENCES


REFERENCES


【GC01a】 Kris Gaj and Pawel Chodowiec. Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using field programmable gate arrays. In Topics in
REFERENCES 315


Goodman:2001:EER


Guerrero:2005:ECB


Gordon:2008:CFS


Gligor:2002:FEA


Gennaro:2005:SMS

REFERENCES


[Gen04a] Rosario Gennaro. Multitrapdoor commitments and their applications to proofs


Lawrence Goldstone and Nancy Bazelon Goldstone.
REFERENCES


Golomb:2005:SDG


Gambino:2008:ITW


Goldwasser:2008:CAP


Gennaro:2003:LBE


Gennaro:2005:BEG


Grothoff:2009:TBS

Gilbert:2002:SCL


Gilbert:2005:FSE


Galindo:2008:SPK


Ghafarian:2007:IPU


Gonzales:2000:LBC

REFERENCES

Gilbert:2000:SAR
Henri Gilbert, Helena Handschuh, Antoine Joux, and Serge Vaudenay. A statistical attack on RC6 (abstract only). In NIST [NIS00], page 10. ISBN ???. LCCN ???.

Gilbert:2001:SAR
H. Gilbert, H. Handschuh, A. Joux, and Serge Vaudenay. A statistical attack on RC6. In Schneier [Sch01d], page ??

Gaudry:2006:ACM

Grabner:2005:ALC

Gong:2001:GPK
REFERENCES


Andrew D. Gordon and Alan Jeffrey. Authenticity by typing for security protocols. Journal

Gordon:2004:TEA

Ganapathy:2005:APA

Gennaro:2003:SAP

Gallagher:2006:HSB

Gentry:2001:CNS

Gomulkiewicz:2002:HWA
Marcin Gomulkiewicz and Miroslaw Kutyłowicki. Hamming weight attacks on cryptographic hardware —


IEEE Computer Society order number P3010.


Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, and Brian Schott. Comparative analysis of the


REFERENCES

9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320001.htm; [GM03]

Gilbert:2002:CS


Gilbert:2002:NRP


Galbraith:2003:IAU


Gorrieri:2004:SFR


Giuliano:2000:ISC

Genevieve Giuliano, James E. Moore II, and Jacqueline Golob. Integrated smart-card fare system: results from field operational test. Transportation re-
Galbraith:2002:PKS


Goots:2001:FEA


Golle:2008:DCS


Gentry:2005:PAK

Craig Gentry, Philip Mackenzie, and Zulfikar Ramzan. Password authenticated key exchange using hidden smooth subgroups. In Meadows and Syverson [MS05b], pages 299–309.

Galbraith:2001:CNR


Galbraith:2001:RBU

Galindo:2008:ICB


Gopalakrishnan:2001:PWV


Grosek:2001:SPK


Ge:2005:CCO


Gore:2001:CMT


Gratzer:2006:CLE

REFERENCES


Golic:2001:HCC


Golic:2001:MOS


Golic:2003:DNP


Goldreich:2004:FCV


Goldstein:2008:BHO

enforcements/fy0833/2008018567-t.html.


REFERENCES

Goulding:2009:ESA


Geppert:2000:TMS


Gupta:2008:FAT


Ganeirival:2008:STS


Garcia-Pasquel:2006:GCT


Guneysu:2008:SPH


Gutterman:2006:ALR

and University of Haifa, Jerusalem and Haifa, Israel, March 6, 2006. 18 pp.
URL http://www.pinkas.net/PAPERS/gpr06.pdf.


Louis Granboulan. Flaws in differential cryptanaly-

**Granboulan:2002:SSR**


**Grigg:2001:FCL**


**Grossschadl:2001:HSR**


**Grossschadl:2003:ASL**


**Groth:2005:CS**

REFERENCES

Gisin:2002:QC

Gentry:2006:EES

Geppert:2000:T

GonzalezVasco:2001:CPK

Garfinkel:2002:WSP

Gentry:2002:HIB
Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. Lecture
REFERENCES


[GS02c]

[GS07a]

[GS07b]

[GS09]


References

Giles:2002:ADW

Garay:2000:LLB

Gennaro:2000:LBE

Guttman:2002:ATS

Goodrich:2002:EDD

Goodrich:2003:ADS


REFERENCES


[GXT+08] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford. Path-quality monitoring in the presence of adversaries. *ACM SIGMETRICS Performance Evaluation Re-


Haddad:2000:AUA


Hancock:2000:EWP


Harvey:2000:EMA


Hayat:2004:CSE

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

Hayashi:2006:QIT

Hoglund:2006:RSW

Huffmire:2008:DSS

Hartel:2001:TMS

Holcomb:2009:PSS

Humphries:2002:IC
Jeffrey W. Humphries and
REFERENCES


**Huang:2004:NDE**


**Hwang:2004:NMP**


**Huang:2008:NCK**


**Hernandez-Castro:2006:SGG**


**Han:2008:PBPa**


**Han:2008:PBPb**


**Henderson:2002:MTS**

Marie Henderson, Robert

[Halevi:2002:SSE]


[Heg09]


[Hei01]

Heiser:2003:BCB


Heikkila:2007:ESC


Hendry:2001:SCS


Henderson:2006:CBG


Henry:2006:TFA


Herranz:2006:DIB


Herzberg:2002:gx

Herranz:2007:IBR


Heron:2009:AES


Herzberg:2009:DBE


Hess:2004:SVE


Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA


Horvitz:2003:WKA

Omer Horvitz and Virgil Gligor. Weak key authenticity and the computational completeness of formal encryption. In Boneh [Bon03],
Horan:2005:NRN


Howgrave-Graham:2003:IDF


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2005:PKC

REFERENCES

Howgrave-Graham:2003:HNP


Hendricks:2007:LOB


Handschuh:2004:SAC


Handschuh:2005:SAC

Helena Handschuh and M. Anwar Hasan, editors. Selected areas in cryptography: 11th international workshop, SAC 2004, Waterloo, Canada, August 9–10, 2004: Revised selected papers, volume 3357 of Lecture Notes in Computer Science. Springer-Ver-
Hung:2009:FBA


Hwang:2005:TSP


Hoffstein:2006:NNE


Hess:2004:CTT

REFERENCES

Hong:2004:DCT  

Hankerson:2000:CTC  

Hankerson:2001:SIE  

Higgins:2008:NSC  
[Hig08] Peter M. Higgins. *Number story: from counting to cryptography*. Coper-
REFERENCES


Hill:2000:KII


Hilley:2005:CRM


Hilley:2006:SSD


Hacigumus:2002:ESE

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

Hirose:2009:SAD


Hinkelmann:2007:CUN


Huhnlein:2001:TPN

Detlef Hühnlein, Michael J. Jacobson, Jr., and Damian

Huang:2005:ASE


Harris:2005:IUS


Kim:2000:RMW


Heuberger:2005:AGE


Handschoh:2001:ASE


[H05a] Susan Hohenberger and Anna Lysyanskaya. How to

Hwang:2005:TAU


Hwang:2005:SHW


Hwang:2005:STH


Howard:2006:SDL


Huang:2007:EPS

Hu:2007:DWD


Hwang:2008:CPK


Hwang:2000:CBV


Hong:2001:PSA


Han:2002:DMA


Hwang:2003:TRB

REFERENCES


Huang:2009:OSW


Hopper:2002:PSS


Hu:2009:TRN


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

Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU

REFERENCES


**Harbitter:2002:MAP**


**Hevia:2002:PSG**


**Hitchcock:2002:NEC**


**Hoglund:2004:ESH**


**Hollar:2005:EWS**


**Holenstein:2004:CCB**

Hankerson:2004:GEC

Huang:2007:MPK

Hastad:2004:SAR

Harnik:2006:CNI

Haitner:2009:SHC

Hanaoka:2002:HNI


Goichiro Hanaoka, Tsuyoshi Nishioka, Yuliang Zheng, and Hideki Imai. A hierarchical non-interactive key-sharing scheme with low

Hoepman:2001:SKA


Hofinger:2001:LBE


Honary:2001:CCI


Hook:2005:BCP


[HPS08] Jeffrey Hoffstein, Jill Catherine Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*, volume 666 of *Undergraduate texts in mathemat-
He:2001:SAR


Hu:2005:USA


Hawkes:2001:PCS


Hand:2002:MPP

Halevi:2003:TEM


Hawkes:2004:RVC


Hsiao:2004:FCP


Holenstein:2005:OWS

Halevi:2006:TCT


Haitner:2007:SHC


Hromkovic:2003:AHP


He:2013:GME

REFERENCES


[HS01a] F. H. (Francis Harry) Hinsley and Alan Stripp, editors.
REFERENCES


Hoffstein:2001:MAD

Halevy:2002:LBE

Han:2002:HEF

Hwang:2007:PEA

He:2005:MCP

Hong:2001:KIA
Deukjo Hong, Jaechul Sung, Seokhie Hong, Wonil Lee,

Halderman:2008:LWRa


Halderman:2008:LWRb


Hanaoka:2002:USA


Hasan:2009:PHF


Hanaoka:2000:USD


Hanaoka:2001:EUS


Halpern:2004:RSS


Huang:2006:CSV


Hongfeng:2008:ECP

REFERENCES


[Huhnlein:2000:EIC] Detlef Hühnlein. Efficient implementation of cryp-
tosystems based on non-
maximal imaginary quadratic
orders. *Lecture Notes in
Computer Science*, 1758:
147–162, 2000. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Hun05] K. Hunt. A Java framework
for experimentation with
steganography. *SIGCSE
Bulletin (ACM Special In-
terest Group on Computer
Science Education)*, 37(1):
282–286, 2005. CODEN
SIGSD3. ISSN 0097-8418
(print), 2331-3927 (elec-
tronic).

[Hus01] Dirk Husemann. Standards
in the smart card world. *Computer Networks
16, 2001. CODEN ????
ISSN 1389-1286 (print),
1872-7069 (electronic). URL
http://www.elsevier.nl/
gej-ng/10/15/22/61/28/
32/abstract.html; http://
www.elsevier.nl/gej-
gn/10/15/22/61/28/32/article.
pdf.

[Hus04] Dale Husemoller. *Elliptic
curves*, volume 111 of *Grad-
uate texts in mathematics*.
Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
many / London, UK / etc.,
0-387-95490-2. xxi + 487
pp. LCCN QA567 .H897
loc.gov/catdir/enhancements/
fy0814/2002067016-d.html;
http://www.elsevier.nl/catdir/
enhancements/fy0814/2002067016-
t.html. With appendices
by Stefan Theisen, Otto
Forster, and Ruth Law-
rence.

communicating systems: de-
sign, analysis, and imple-
mentation*. Cambridge Uni-
versity Press, Cambridge,
UK, 2001. ISBN 0-521-
80731-X (hardcover). x +
283 pp. LCCN TK5102.85

[HV04] Alireza Hodjat and In-
grid Verbauwhede. High-
throughput programmable
cryptocoprocessor. *IEEE
Micro*, 24(3):34–45, May/
June 2004. CODEN
IEMIDZ. ISSN 0272-1732
(print), 1937-4143 (elec-
tronic). URL http://
/csd1.computer.org/dl/mags/
mi/2004/03/m3034.htm;
http://csdl.computer.
org/dl/mags/mi/2004/03/
m3034.pdf.

[HV09] Sean Hallgren and Ul-
rich Vollmer. Quantum

Hopper:2009:PSS


Hardy:1998:ITN


Hellekalek:2003:EEC


Hsu:2003:CIT

Hsu:2004:EPS


Hsu:2005:SCT


Hwang:2000:CYK


Hwang:2005:ITA


Henderson:2001:IEV


Hsu:2005:NPM


Hu:2008:NNP

REFERENCES

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

Hardy:2009:AAC


Hsu:2002:IGT


Hsu:2004:GOS


Harkins:2005:ESU


Hsu:2003:IMA

[HY01] Hirose:2001:UAS


[HY03] Hwang:2003:CAL

[hY08] Yeh:2008:STB

[HYZ05a] Han:2005:PJI

[HYZ05b] Han:2005:PIJ
Huang:2005:EMP

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

IBM-MARS-Team:2000:MAS


IEEE:2000:ASF


IEEE:2000:IPH


IEEE:2001:ISF


<table>
<thead>
<tr>
<th>IEEE:2005:AIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[IEE05a]</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE:2005:PIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[IEE05b]</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE:2006:AIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[IEE06]</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE:2007:PAI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[IEE07]</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE:2008:PAI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[IEE08]</strong></td>
</tr>
</tbody>
</table>
IEEE:2009:ISI


IEEE:2009:PAI


Itoi:2001:SIS


Ifrah:2000:UHN


Iglesias:2002:NSB

REFERENCES


REFERENCES


Impagliazzo:2003:LRA


Impagliazzo:2006:LRA


Ichikawa:2000:HEA


Ishai:2003:EOT


Izmerly:2006:CCA


Izotov:2001:COC


Imrey:2003:BRC


Inamori:2002:SPB


Inamori:2002:SPT


**Inoue:2005:EST**


**Intel:2000:IIP**


**Intel:2003:IRN**


**Itkis:2001:FSS**


**Itkis:2002:SSB**


**Irwin:2003:BRBb**


ISO:2004:IIIb


ISO:2005:IDM


Iqbal:2008:CDV

[ISSZ08] Razib Iqbal, Shervin Shir-mohammadi, Abdulmotaleb El Saddik, and Jiy-
REFERENCES


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


Jambunathan:2000:CCP


Janczewski:2000:IIS


Janeczko:2006:TSH


Jankowski:2008:BRBb

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


Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC

Johansson:2000:FCA

Jakimoski:2001:CCB

Jonsson:2002:FCA

Jaulmes:2001:CPN

Jakimovski:2002:CS
Goce Jakimovski and Ljupco Kocarev. Cryptanalysis of SBLH. Lecture Notes in Computer Science, 2355:144–??, 2002. CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:
Jonsson:2002:SRE


Jonsson:2002:SRT


Jang:2001:BWA


Jung:2001:EMO


Jallad:2002:ICC

Kahil Jallad, Jonathan

[JL03]


[Juang:2004:FBT]

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


Jeong:2008:PKE


Lee:2007:RKD


Juang:2001:FBT


Juang:2002:VMA


Jakobsson:2003:FMT


Johansson:2003:PCI

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


Jing-mei:2005:CRB


Joux:2002:BAA


Jao:2009:EGB


REFERENCES


REFERENCES

Jain:2006:TMB

Jakubowska:2007:MCT

Jiang:2004:FAP

Joye:2001:PMA

Juric:2006:CPW


Jin:2001:WCS


Juric:2006:CPW


Jain:2009:PQR


Jarecki:2005:FSP

REFERENCES


(JSJK01) Jongkook:2001:NUS


(JT01b) Joye:2001:CEN


(JT01a) Joye:2001:PAD


[JSW05] Jiang:2005:SAI

Juan:2004:EPA


Juels:2004:FCI


Junod:2005:SCB


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

Juels:2005:APD


Jeng:2006:EKM


Jin:2005:EAW


Jiang:2005:RNP


Joye:2001:NMM


Jakobsson:2004:ACN

REFERENCES


David Kahn. The Codebreakers: the Story of Sec-
Kahn:1974:C

Kahn:1996:CSS

Kak:2006:TSQ

Kaliski:2001:RDS

Kaliski:2003:TRK

Kayem:2008:RCK

Kanda:2001:PSE
REFERENCES

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

REFERENCES

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

[claffy:2001:IMM]

[Kim:2002:SMA]

[Ku:2005:WYR]

[KCl99]

[Kiu:2009:HSI]

[KC05]
Kim:2007:SBE


Kim:2001:SAC


Ku:2003:WLL


Kang:2001:NHO


Kalker:2004:DWS

REFERENCES

416


Kellar:2005:NRR


Keller:2005:NRR


Kenyon:2002:HPD


Kettani:2006:CBN


Kelsey:2000:CPL


Kiltz:2009:DCC

Katsikas:2004:PKI


Kaps:2007:CSD


Kovacich:2003:MHC


Kim:2005:SMA


Kato:2008:QSC

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**


REFERENCES

Kobara:2001:NCP


Kobara:2001:SSM


Kurosawa:2003:TTK


Kidwell:2000:SNC


Kida:2002:PGR


Kilian:2001:ACC

Joe Kilian, editor. *Advances in cryptography — CRYPTO*
Kiltz:2001:TBC


Kim:2001:PKC

REFERENCES

Kim:2002:ISC


[Kim02]

King:2000:IMP


[King01]

King:2001:CMF


[King02]

King:2002:RG1


[Kir01a]

Kirkby:2001:CCW

REFERENCES


Montgomery:2003:FEC


Kocarev:2001:LMB


Kanade:2005:AVB


Klein:2003:FOW


Kawachi:2006:PQC


Kashefi:2007:SZK


Karri:2003:PBC


Kwon:2003:EEC

REFERENCES


Kaliski:2002:CHE


Kelsey:2000:ABA


Kohno:2000:PCR

REFERENCES

pdf.

Kelsey:2001:ABA


Katz:2008:IMC


Katz:2005:HEP


Knill:2002:FPE

Emanuel Knill, Raymond Laflamme, Howard N. Barnum, Diego A. Dalvit, Jacek J. Dziarmaga, James E. Gubernatis, Leonid Gurvits,

Knill:2002:QIP


Ko:2000:NPK


Klein:2007:BDC


Kong:2001:AVW


Kiltz:2005:SCM

REFERENCES

Kacprzak:2006: CBS


Kalai:2009: SEU


Kim:2002: EPS


Knudsen:2000: CRA

Kim:2001:NPK


Knudsen:2001:CRR


Knudsen:2001:CPL


Kanda:2002:SCA


Koblitz:2004:OTS

Neal Koblitz and Alfred J. Menezes. Obstacles to


Liam Keliher, Henk Meijer, and Stafford Tavares. Improving the upper bound on the maximum average linear hull probability for Rijndael. Lecture Notes in Computer Science, 2259:


Komano:2003:EUP

Koblitz:2000:TQC

Kocher:2002:IS

Koga:2002:GFR
Kurosawa:2001:ICP


Koshiba:2001:SRS


Koskinen:2001:NIK

Kovach:2001:BCB


Kovacich:2003:ISS


Katz:2001:EPA


Katz:2009:ESA


Katzenbeisser:2000:IHT


Koc:2001:CHEa


Yongdae Kim, Adrian Perrig, and Gene Tsudik. Tree-based group key agreement.
REFERENCES


**Krishna:2003:BUP**


**Krawczyk:2001:OEA**


**Krawczy:2003:SSM**


**Krause:2002:USP**


**Krawczy:2003:SSM**

[Kra02a] Matthias Krause. BDD-based cryptanalysis of keystream generators. Lecture Notes in Computer Science, 2332:
Krawczyk:2005:HHP


Kramer:2007:LCC


Kreitz:2005:OBE


Koeune:2002:FIL


Kehr:2001:ISM


Kim:2005:CLL

Kee-Won Kim, Eun-Kyung Ryu, and Kee-Young Yoo. Cryptanalysis of Lee–Lee

**Katz:2000:CCA**

**Kelsey:2000:MAP**

**Kuramitsu:2002:ETC**

**Krause:2003:DOC**

**Kozaczuk:2004:EHP**
REFERENCES


[Klivans:2009:CHL]

[Kelsey:2000:YND]

**Kang:2001:PSK**


**KSR02**


**Kogan:2006:PRS**


**Kelsey:2000:SCC**


**Konstantinou:2002:SLE**

Kuribayashi:2000:WSB


Kuribayashi:2001:NAF


Kogan:2006:IER


Ku:2003:TSA


Kobayashi:2007:AIG


Ku:2002:IIB

Wei-Chi Ku. An improved ID-based authenti-

Kuhn:2000:PCL


Kuhn:2001:CRR


Kuhn:2008:BSS

Ulrich Kühn. Breaking the Shin–Shin–Rhee remotely


REFERENCES


Keromytis:2006:COS

Kwon:2003:EDS

Kumar:2006:ODS

Wong:2001:MCC
Kun:2000:SMA


Kamat:2009:TPW


Katz:2000:CCS


Katz:2001:UEC


Kavut:2001:SCP


Kiayias:2001:PRB

Aggelos Kiayias and Moti Yung. Polynomial reconstruction based cryptography. *Lecture Notes in Computer Science*, 2259:
REFERENCES


Kiayias:2001:SPP


Katz:2002:TCB


Kim:2002:PAA

Hyun-Sung Kim and Kee-


REFERENCES

Landau:2000:STT


Landau:2000:TOD


Landau:2000:ITS


Landau:2004:PNS


Landau:2004:SLE


Lakshminarayanan:2008:SUC

[KLS08] Karthik Lakshminarayanan, Daniel Adkins, Adrian Perrig, and Ion Stoica. Securing user-controlled routing


Li:2004:QAU


Lindskog:2005:DIT


Lee:2000:UBN

REFERENCES


Lim:2009:OPG  Sun Sun Lim, Hichang Cho, and Milagros Rivera Sanchez. Online privacy,

**Li:2008:CAM**


**Lu:2005:TUS**


**Lu:2005:PBM**


**Lu:2005:RTP**


**Li:2001:CCB**


**Lai:2004:SGS**


**Lavoué:2007:SSW**

REFERENCES

Law:2006:SBB

Lindquist:2004:JCS

Lee:2001:AES

Lee:2003:BRBb

Lee:2003:CS

Lee:2004:SPM
Lee:2004:ACA


Lenstra:2001:USM


Leroy:2002:BVJ


Levy:2001:CHC

Levy:2002:C


Lewand:2000:CM


Lee:2003:PKB


Lei:2007:CSA


Liaw:2004:SPA


Lekkas:2004:CNL


Levi:2009:ULM

Lan:2010:RNG


Lang:2001:CMS


Lin:2003:PAS


Lee:2004:CUS


Lyda:2007:UEA


Li:2008:ISS

Chua-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. Improving the security of a secure anonymous routing protocol with authenticated

[Lu:2005:NPS]


[LHH05]


[LHL*02]


[LHL04a]


[LHL03a]


[LHL04b]


[LHL03b]


[LHL03c]


[LHL04b]

REFERENCES

Lu:2008:PTZ


Liu:2005:DBV


Lee:2009:NCA


Lee:2002:FRU


Li:2001:NSA

REFERENCES


Lindell:2001:PCT


Lingmann:2002:DSK


Licks:2005:GAI

Vinicius Licks and Ramiro Jordan. Geometric attacks on image watermarking systems. IEEE MultiMedia, 12

Lee:2005:IEC


Lin:2007:PFT


Lindell:2003:SCC


[LKM+05] Ruby B. Lee, Peter C. S. Kwan, John P. McGrego-...


REFERENCES


Lee:2005:CMA


Lee:2005:SSP


Li:2005:FCR


Lee:2006:ISC


Lu:2006:FBW


Lu:2006:RDI


[LRR02] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the composition of authenti-


REFERENCES

Li:2005:ATN


Li:2009:ATN


Lee:2006:DCK


Linares:2000:SAM

Leandro Rodríguez Liñares and Carmen García Ma-

**Lorenz:2002:SSG**


**Lavasani:2008:IFA**


**Li:2003:SCE**


**Lamenca-Martinez:2006:LNP**


**Leitold:2001:MTN**

Herbert Leitold, Wolfgang Mayerwieser, Udo Payer,

Lepinski:2005:FZK


Laskari:2005:TTC


Lu:2005:CCA


REFERENCES

Labbe:2002:AIF


Luccio:2002:AC


Lee:2003:CPK


Li:2005:MCK


Law:2009:EEL

REFERENCES


REFERENCES

(Sprint), 1872-7069 (electronic).

Lin:2003:DBI


Lin:2000:TPE


Lin:2003:SEOa


Lin:2003:SEOb


Lu:2005:BIW


Li:2005:ABPb


REFERENCES


[Lu07] HongQian Karen Lu. Network smart card review and analysis. Computer Net-


REFERENCES

Lucks:2002:VCS  

Lucas:2006:PGE  

Ludvig:2005:PWF  

Lukyanov:2001:PFA  

Lunde:2009:BCU  

Lutz:2002:BBS  


REFERENCES

Lee:2004:IAK

Liang:2005:PAC

Loepp:2005:PIC

Lyuu:2005:CIH

Lin:2000:PAS

Lv:2005:PCA
Lv:2005:SMS


Lin:2009:DMG


Li:2005:IWR


Lin:2005:NIB


Li:2007:PBS


Lixin:2005:FLA

REFERENCES


REFERENCES

493

Leung:2001:WDI


Li:2004:CAB


Lao:2009:ORA


Li:2001:GOT


Li:2004:WMS


Michener:2000:IWM

Michener:2000:MSA


Masuda:2002:CDC


Maurer:2007:ICP


Mrayati:2003:AKT


Mrayati:2004:IAD


Mrayati:2005:IDB


Mrayati:2006:TTC

**REFERENCES**

**Mrayati:2007:TTC**


**Mrayati:20xx:AET**


**McDaniel:2006:OAI**


**Machado:2000:NCP**


**MacKenzie:2001:MEP**


**Mohay:2003:CIF**


**Madsen:2000:HCI**


Mann:2002:HI

Mann:2008:HHS

Mao:2001:TRC

Mao:2004:MCT

Marques:2002:BSJ

Martinelli:2002:SSA
Mares:2005:BRA


Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI


Martin:2008:IBE


Mastroeni:2004:APA


Matsui:2002:FSE


Mathieson:2005:UCR

Maurer:2001:C

Maurer:2004:RCD

Mayers:2001:USQ

May:2002:CUR
C79 2002. URL http://
/link.springer.de/link/
service/series/0558/bibs/
2442/24420242.htm; http://
/link.springer.de/link/
service/series/0558/papers/
2442/24420242.pdf.

Alexander May. Computing
the RSA secret key is de-
terministic polynomial time
equivalent to factoring. In
Franklin [Fra04], pages 213–
?? CODEN LNCSD9. ISBN
3-540-22668-0. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
10.1007/b99099. URL
issue&issn=0302-9743&volume=
3152; http://www.springerlink.com/openurl.asp?genre=
volume&id=doi:10.1007/
b99099.

John P. May, editor. Proceed-
ing of the 2009 interna-
tional symposium on Sym-
bo l ic and algebraic compu-
tation, KIAS, Seoul, Ko-
rea, July 28–31, 2009. ACM
Press, New York, NY 10036,
USA, 2009. ISBN 1-60558-
609-9. LCCN ???.

H. X. Mel and Doris M. Baker. Cryptography De-
crypted. Addison-Wesley,
ISBN 0-201-61647-5. xx +
352 pp. LCCN QA76.9.A25
M44 2001. US $29.95; CDN
$44.95; UK £22.99.

Saraju P. Mohanty and
Bharat K. Bhargava. In-
v isible watermarking based
on creation and robust
insertion-extraction of im-
age adaptive watermarks.
ACM Transactions on Mul-
timedia Computing, Com-
munications, and Applica-
tions, 5(2):12.1–12?:?,
November 2008. CODEN
???? ISSN 1551-6857
(print), 1551-6865 (elec-
tronic).

A. David McKinnon, David E.
Bakken, and John C.
Shovic. A configurable cryp-
tography subsystem in a
middleware framework for
embedded systems. Com-
puter Networks (Amster-
dam, Netherlands: 1999),
46(6):771–795, December
20, 2004. CODEN ???.
ISSN 1389-1286 (print),
1872-7069 (electronic).

Gabriel Montenegro and
Claude Castelluccia. Crypto-
based identifiers (CBIDs):
Concepts and applications.
ACM Transactions on In-
formation and System Se-
curity, 7(1):97–127, Febru-
ary 2004. CODEN ATISBQ.
McAndrew:2008:TCO


McGraw:2006:SSB


Myles:2005:ETS


McKenna:2004:EAE


McLaughlin:2006:PZW


McNichol:2003:HTM

REFERENCES

wired/archive/11.08/random.

Martin:2004:AMC


Macchetti:2005:QPH


McCamant:2008:QIF


Monteiro:2008:AVM


Meadows:2001:OIF


Meadows:2004:OSM


Mehrabi:2001:DW

REFERENCES


Mena:2003:IDM


Menezes:2005:TCC


Menezes:2007:ACC


Messerges:2000:SAF


Matula:2005:TLS


Mueller:2006:SMG


Muller:2009:BPE

Christoph Müller, Steffen Frey, Magnus Strengert, Carsten Dachsacher, and Thomas Ertl. Best paper
REFERENCES


[Ma:2005:NCD] Yiping Ma and Jiqing
Han. A new capability description for audio information hiding. In Han et al. [HYZ05b], pages 65–?? ISBN 981-270-153-2. [MHM+02]

Maas:2009:SRW


Moon:2002:IDC


Mihaljevic:2009:ASC


Micciancio:2001:ILB

Daniele Micciancio. Improving lattice based cryptosystems using the Hermite normal form. Lecture Notes
REFERENCES


Micciancio:2002:GCK


Micciancio:2002:ICH


Mirkovic:2005:IDS


MacDonald:2003:CDS


Maltoni:2004:BAE


Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS

Moyle:2005:CLD


Mazieres:2000:SKM


Majzoobi:2009:TDI


McDonald:2008:SID


McGregor:2005:PCK


Miaou:2001:BCW

REFERENCES


REFERENCES

Moldovyan:2007:IC


Mullen:2007:FFA


Moreira:2002:RCE


Milenkovic:2005:UIB


Maltoni:2003:HFR


McEvoy:2009:IWH

REFERENCES


Maitra:2006:PCI


Matsumoto:2002:IAG


Maclean:2000:OIG


Mizuki:2001:NSN


Mercuri:2003:IRS

Rebecca T. Mercuri and Pe-


REFERENCES


REFERENCES


REFERENCES

Mihaiescu:2001:BRE


Moshopoulos:2001:NSA


Malkhi:2002:ACE


Maurer:2003:SMR


Micciancio:2005:ASS

Daniele Micciancio and Saurabh Panjwani. Adaptive security of symbolic en-


REFERENCES


(MR01c) Silvio Micali and Leonid Reyzin. Soundness in the public-key model. In Kilian [Kil01a], pages 542–?? ISBN 3-540-42456-3 (paperback). LCCN
REFERENCES

UK£47.00. URL http://link.springer-ny.com/
lake/service/series/0558/
bibs/2139/21390542.htm; [MR03]
http://link.springer-ny.com/link/service/series/
0558/papers/2139/21390542.pdf.

Murphy:2002:EASa

S. Murphy and M. J. B. Robshaw. Essential
algebraic structure within the AES. Report,
Information Security Group, Royal Holloway,
University of London, Egham, Surrey, TW20
0EX, UK, 2002. 16 pp. URL http://www.isg.rhul.ac.uk/~
mrobshaw/aes-crypto.pdf.

Murphy:2002:EASb

Sean Murphy and Matthew J. B. Robshaw. Essential
algebraic structure within the AES. In Yung [Yun02a],
pages 1–16. CODEN LNCS.D9. [MRL+02]
ISBN 3-540-44050-X (paperback). ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
C79 2002. URL http://link.springer.de/link/
service/series/0558/bibs/2442/24420001.htm; http://
link.springer.de/link/service/series/0558/papers/
2442/24420001.pdf; http://

Matyas:2003:TRU

Václav Matyáš, Jr. and Zdenek Riha. Toward reliable
user authentication through biometrics. IEEE
CODEN ????? ISSN 1540-7993 (print), 1558-4046
computer.org/sp/books/sp2003/pdf/j3045.pdf;

Micciancio:2009:LBC

Daniele Micciancio and Oded Regev. Lattice-based
cryptography. In Bernstein et al. [BBD09], pages
147–192. ISBN 3-540-88701-6 (hardcover), 3-642-

Monrose:2002:TSG

Fabian Monrose, Michael Reiter, Qi Li, Daniel P.
Lopresti, and Chilin Shih. Toward speech-generated
cryptographic keys on resource-constrained devices. In
USENIX [USE02b], pages 283–296. ISBN 1-931971-
00-5. LCCN ????? URL
http://www.usenix.org/publications/library/proceedings/
sec02/monrose.html.
REFERENCES


REFERENCES


[MS03b] Gerome Miklau and Dan Suciu. Controlling access to published data using cryptography. In

REFERENCES


[MS09d] Babak Mahdian and Stanislav Saic. Using noise inco-

[MS09a] S. Myers and A. Shelat. Bit encryption is complete. In

Shen:2005:NIW


Marton:2010:RDC


MacKenzie:2002:TPA


McClure:2003:HEN


Matsumoto:2007:FSC

Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. A fast stream cipher with huge state space and quasigroup filter for software. In Adams
REFERENCES

et al. [AMW07], pages 246–263. ISBN 3-540-77360-6. LCCN ????

Miltchev:2008:DAC


Mouratidis:2009:PMD


Moran:2004:NIT


Myasnikov:2005:PAB


Muzereau:2004:EBD


Marsaglia:2002:SDP

REFERENCES

CODEN JSSOBK. ISSN ????. URL http://www.jstatsoft.org/v07/i03; http://www.jstatsoft.org/v07/i03/tuftests.c; http://www.jstatsoft.org/v07/i03/tuftests.pdf; http://www.jstatsoft.org/v07/i03/updates.


cryption. Network Security, 2008(12):4–6, De-
cember 2008. CODEN NTSCF5. ISSN 1353-4858
(print), 1872-9371 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485808701387.

[Mur00] S. Murphy. The key separa-

[Murray:2001:CDC] Eric Murray. Changes in de-
org/publications/library/proceedings/sec01/murray/
index.htm. Unpublished invited talk, Tenth USENIX
Security Symposium, August 13–17, 2001, Washing-
ton, DC, USA.

plementation of the Yarrow PRNG for FreeBSD. In
usenix.org/publications/library/proceedings/bsdcon02/
murray.html.

goes to the heart. Network Security, 2006(5):
19, May 2006. CODEN NTSCF5. ISSN 1353-4858
(print), 1872-9371 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485806703907.

Vaudenay. On the pseu-
dorandomness of top-level
schemes of block ciphers.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
com/link/service/series/
hmt; http://link.springer-
ny.com/link/service/series/
pdf.

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

Micciancio:2003:SZK

Morrow:2003:DIB

Micciancio:2004:CTA

Ma:2006:ADS

Morelli:2001:JAH

Malan:2008:IPK
David J. Malan, Matt Welsh, and Michael D. Smith. Implementing public-key infrastructure for

**[MRaihi:2001:CAS]**


**[MCook:2001:NSS]**


**[Morelos-Zaragoza:2002:AEC]**


**[Matsui:2004:SAC]**


[Nam02] Chanathip Namprempre. Secure channels based on

[Naor:2002:DRA]


[Naor:2004:TCF]


[Naor:2003:CAC]


REFERENCES

Nash:2001:PIM

Nedjah:2004:ECH

Nedjah:2006:NTC

Netscape:2004:HSW

Neuenschwander:2004:PSM

Neuenschwander:2006:IMM
REFERENCES


Neve:2003:STF


Nguyen:2001:TFLb


Nguyen:2005:RBP


Nordholt:2002:NFC


Nyberg:2003:SAC

REFERENCES


Nievergelt:2002:FLM


Nievergelt:2002:FLM

Niederreiter:2004:BRC


Niederreiter:2004:BRC

Nikander:2002:DSAa


Nikander:2002:DSAa

Nikander:2002:DSAb


Nikander:2002:DSAb

NIST:2000:TAE

NIST, editor. *The Third*
REFERENCES


Ning:2008:MAA


Nigrini:2009:DDU


Nagao:2005:UCS


Nozaki:2001:IRA


Northcutt:2002:NID

REFERENCES


REFERENCES


Naor:2004:NTC
Moni Naor and Omer Rein-  
gold. Number-theoretic  
constructions of efficient  
pseudo-random functions.  
Journal of the ACM, 51  
CODEN JACOAH. ISSN  
0004-5411 (print), 1557-  
735X (electronic).

Nichols:2000:DYD
Randall K. Nichols, Daniel J.  
Ryan, and Julie J. C. H.  
Ryan. Defending your di-  
gital assets: against hackers,  
 crackers, spies and thieves.  
McGraw-Hill, New York,  
NY, USA, 2000. ISBN 0-07-  
212285-4. xxxv + 858 pp.  
LCCN QA76.9.A25 N528  
2000. US$59.99. URL http:  
//corpitk.earthweb.com/  
reference/0072122854.html

Neraud:2001:CFD
Jean Néraud and Carla  
Selmi. On codes with  
a finite deciphering de-  
lay: constructing incom-  
pletable words. Theo-  
retical Computer Science,  
255(1-2):151–162, March  
28, 2001. CODEN TC-  
SCDI. ISSN 0304-3975  
(print), 1879-2294 (elec-  
tronic). URL http://  
//www.elsevier.nl/28/  
abstract.html; http:  
//www.elsevier.nl/gej-  
ng/10/41/16/197/21/28/  
article.pdf.

Nguyen:2000:CFD
Phong Q. Nguyen and  
Igor E. Shparlinski. On  
the insecurity of a server-  
//link.springer-ny.com/  
link/service/series/0558/  
bibs/2248/22480021.htm;  
http://link.springer- 
ny.com/link/service/series/  
0558/papers/2248/22480021. 
pdf.

Nguyen:2001:TFLa
Phong Q. Nguyen and  
Jacques Stern. The two  
faces of lattices in cryp-  
tology. Lecture Notes in  
Computer Science, 2146:  
146–??, 2001. CODEN  
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://  
//link.springer-ny.com/  
link/service/series/0558/  
bibs/2146/21460146.htm;
REFERENCES


[OHB08b] Rolf Oppliger, Ralf Hauser, and David Basin. SSL/TLS

Oiwa:2009:IMS


Okamoto:2000:ACA


Ohzahata:2002:FAM


REFERENCES

**Ortiz:2000:ITW**

**Okeya:2000:PAB**

**Okeya:2001:EEC**

**Ostrovsky:2005:PSS**

**Oren:2006:PAR**

**Obimbo:2007:PAD**

Oury:2008:PP

Overbeck:2009:CBC

Okeya:2004:SBR

Osvik:2005:CAC

Osvik:2006:CAC

Osvik:2000:SS


Vidura Panditaratne. True random number generator goes online. World-Wide Web document, July
REFERENCES


Papanikolaou:2005:BRBa


Park:2004:APP


Pass:2003:DCR


Pass:2005:UCN


Patterson:2001:DFI

Patiyoot:2002:MSE


Patiyoot:2002:SIW


Patarin:2003:LRR


Paterson:2003:CCI


Patarin:2004:SRF

REFERENCES


REFERENCES


Prattichizzo:2007:PIH


Papadimitriou:2001:PSE


Pucheral:2001:PSD


Poulos:2008:TSE


Yongsu Park, Tae-Sun Chung, and Yookun Cho. An efficient stream authentication scheme using tree

**Patarin:2001:QBL**


**Park:2002:XQP**


**Park:2003:EMS**


**Pan:2007:IBS**


**Peeters:2007:CES**


**Petrakos:2009:CTA**

REFERENCES


REFERENCES


[Per05] Perry:2005:DCP

[Petullo:2003:IEH]

[Petullo:2005:EYR]

[Pfitzmann:2001:ACE]
REFERENCES


REFERENCES

Polk:2003:IIC

Phoha:2001:SDI

Pieprzyk:2003:FCS

Pinkas:2002:CTP
REFERENCES


REFERENCES

Poh:2001:HBP


PK01

Petitcolas:2003:DWF


PK03

Park:2001:CSC


PKBD01

Park:2005:CZA


PKH05

Park:2001:DNP

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


Paulson:2000:NBU


Piper:2002:CVS


Pang:2008:AQR


Peyravian:2000:MBB


Pohlmann:2001:SCA


Pointcheval:2000:CCS


Pointcheval:2002:PSP

David Pointcheval. Practical security in public-key cryptography. *Lecture Notes in Computer Science*, 2288:1–??, 2002. CO-

Pointcheval:2006:TCC


Porras:2006:PEG


Potter:2003:WAO

REFERENCES


Paar:2009:UCT


Pellikaan:1996:AGC


Pereira:2003:SAU


Piret:2003:DFA


Pereira:2006:IBS


Picard:2001:NNF


Preneel:2002:NPT

Preneel:2002:TCC

Preneel:2007:SRD

Price:2000:NCH

Provos:2000:EVM

Provos:2001:DAS
PAWN:2004:CTT


POUPARD:2000:FER


PARKER:2001:RKC


PFITZMANN:2001:SEC


PORNIN:2001:SHT

Padro:2002:LBI


Pomerance:2002:SOC


Page:2004:PCA


Park:2004:UUC


Prabhakaran:2004:NNS


Prabhakaran:2005:RES

REFERENCES


REFERENCES


Preneel:2006:SAC

Pang:2008:VCR

Pfleeger:2007:GEI

Pucella:2003:JRB

Pucella:2006:SCC

Pucella:2007:Ib
Riccardo Pucella. Introduction. ACM SIGACT News,
References

Puzmanova:2004:RWF


Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI


Pang:2005:NMS


Peikert:2008:LTF

Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In ACM [ACM08], pages 187–196.

**Pelzl:2003:HCC**


**Patrick:2005:FCD**


**Paterson:2006:LTT**


**Palanivel:2008:MPA**


**Pieprzyk:2001:CPS**


[QCB05b] Haifeng Qian, Zhenfu Cao, and Haiyong Bao. Security
of Pon–Lu–Jeng’s Meta-He
digital signature schemes.
*Applied Mathematics and
Computation*, 170(1):724–
730, November 1, 2005. CO-
DEN AMHCBQ. ISSN
0096-3003 (print), 1873-
5649 (electronic).

**Quisquater:2005:SCC**
Michael Quisquater, Bart
Pieneel, and Joos Vande-
walle. Spectral charac-
terization of cryptographic
Boolean functions satisfy-
ing the (extended) propaga-
tion criterion of degree
\(l\) and order \(k\). *Information Pro-
cessing Letters*, 93(1):25–28,
January 16, 2005. CODEN
IFPLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

**Quisquater:2000:SCR**
J.-J. Quisquater and Bruce
Schneier, editors. *Smart
card research and applica-
tions: third international
conference, CARDIS’98,
Louvain-la-Neuve, Belgium,
September 1998: pro ceed-
ings*, volume 1820 of *Lec-
ture Notes in Computer Sci-
tence*. Springer-Verlag,
Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2000.
ISBN 3-540-67923-5. LCCN

**Qu:2001:KPW**
Gang Qu. Keyless pub-
lic watermarking for intel-
lectual property authenti-
cation. *Lecture Notes in
Computer Science*, 2137:
REFERENCES


[RB01] Vincent Rijmen and Paulo S. L. M. Barreto. The


REFERENCES

Rankl:2000:SCH


Riley:2002:CBR


Rankl:2003:SCH


Reeds:2001:BRB


Reese:2003:ELD


Regev:2003:NLB


Regev:2004:NLB


P. M. Rodwell, S. M. Furnell, and P. L. Reynolds. A non-intrusive biometric authentication mechanism

**Rodwell:2007:NIBc**


**Ringenburg:2005:PFS**


**Rotondi:2006:CHA**


**Ren:2009:FCS**


**Rose:2006:CSP**


**Rojas:2000:FCH**

REFERENCES


[Ric07] Donald Rich. Authentication in transient storage de-


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


REFERENCES


REFERENCES


**Roth:2002:JSA**

[Rot02a]

**Roth:2002:SFC**

[Rot02b]

**Roth:2003:SFC**

[Rot03]

**Rothe:2005:CTC**


**Rothe:2007:BRB**

[Rot07]

**Roy:2000:PCI**

REFERENCES


Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. Lecture Notes in
REFERENCES


REFERENCES


RSA:2000:PCP

RSA:2000:PVCb

RSA:2000:PVS

RSA:2001:PVC

RSA:2002:PVR

Rivest:2003:TAL

RSA:2003:PEC
REFERENCES

pkcs/pkcs-13/index.html

Still under development.

Rousseau:2009:CCP


URL http://d-nb.info/997902213/34; http://nbn-resolving.de/urn:nbn:de:1111-20091103138;

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

Rousseau:2009:MT


URL http://d-nb.info/997902213/34; http://nbn-resolving.de/urn:nbn:de:1111-20091103138;

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

Rukhin:2001:STS


Rouviroy:2003:EUF


CODEN CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).

Rouviroy:2003:EUF

G. Rouvroy, F.-X. Stan- daert, J.-J. Quisquater, and J.-D. Legat. Efficient uses of FPGAs for implementations
REFERENCES


[RSS04]


[Rub00]


[Rub01]


[Rup09]


[Rup09]

REFERENCES

Raghavan:2009:SPC

Russell:2002:HFU

Renner:2003:NBS

Ramaswamy:2007:HSP

Schmalz:2003:MDI
Mark S. Schmalz et al., editors. *Mathematics of

Saini:2002:JMD


Saeednia:2002:IBS


Sakamura:2001:GEI


Sale:2000:CGL


Sale:2000:CBP


Sale:2001:GRT

Tony Sale. General report on Tunny: The Newmanry
REFERENCES


David Salomon. Foundations of computer security. Springer-Verlag,
REFERENCES


[Sar02] Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung [Yun02a],


[Sa02] Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung [Yun02a],


[Sar02] Palash Sarkar. The filter-combiner model for memoryless synchronous stream ciphers. In Yung [Yun02a],
Sasse:2007:REB


Satoh:2006:DPI


Savelli:2004:NDC


Savage:2005:IPWa


Savage:2005:IPWb


Soto:2000:RTA


Shacham:2001:ISH

REFERENCES

---

Scott:2004:CP

---

Stoklosa:2005:CIC

---

Sherwood:2005:MTR

---

Steiner:2001:SPB

---

Smeraldi:2002:SVF
Fabrizio Smeraldi, Josef Bigun, and Wulfram Gerstner. Support vector features and the role of dimensionality in face authentication. Lecture
Shehab:2005:SCM


Shehab:2007:WSD


Shaikh:2009:SAU


Steinfeld:2002:NSA


Seredynski:2004:CAC


Syverson:2001:LAP

Paul Syverson and Iliano Cervenka. The logic of au-
Shen:2002:NDW


Sun:2002:WDC


Shao:2005:NEV


Stephanides:2005:GAK

References


[Sch00d] Bruce Schneier. *Secrets and Lies: Digital Security in a*
REFERENCES


Schneier:2000:SRF


Scharinger:2001:ASK


Schmalz:2001:MDI


Schneier:2001:FSE


Schnorr:2001:SGH [Sch01e]


Schnorr:2001:SDE [Sch01f]


Schultz:2002:GBC [Sch02]


Schneier:2003:BFT [Sch03]


Schmalz:2004:MDIa [Sch04a]


Schmalz:2004:MDIb [Sch04b]

Mark S. Schmalz, editor. Mathematics of data/

Schneier:2004:SA


Schultz:2004:GBC


Schmalz:2005:MDI


Schneier:2005:AE


Schneier:2005:TFA


Schramm:2006:AMS

Kai Schramm. Advanced

Schroeder:2006:NTS


Schneier:2007:NCS


Schneier:2008:SS


Schmeh:2009:VBF


Su:2005:IBT


Scott:2004:CIB


REFERENCES


REFERENCES


Michael Semanko. L-collision attacks against randomized MACs. In Bellare [Bel00], pages 216–?? ISBN 3-540-67907-3. ISSN
REFERENCES


Sakr:2007:RCB [SG07] Ziad Sakr and Nicolas D.
REFERENCES


[Sauvage:2009:ERF] Laurent Sauvage, Sylvain Guilley, and Yves Mathieu. Electromagnetic radiations of FPGAs: High...


[Sha03] Adi Shamir. RSA short-
Shamir:2003:TLC


Shao:2003:CIB


Shao:2003:PSS


Shaltiel:2004:RDE


Shao:2004:IDS


Shao:2005:CXY

Shao:2005:IEP


Shao:2005:NKA


Shao:2005:SMD


Hwang:2009:KDB


Shepherd:2001:CDC


Sung:2007:CIB


Shim:2005:LPG

REFERENCES

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


Victor Shoup. OAEP reconsidered. In Kilian [Kil01a],
REFERENCES


Hung-Min Sun, Bin-Tsan Hsieh, and Shin-Mu Tseng. On the security of some

Shumba:2006:THL


Shyamasundar:2002:ACP


Silverman:2005:ECC


Silverman:2001:CLI

REFERENCES

Singh:1999:CBE


Sin01b

Singh:2000:CBE


Singh:2001:DPK


Sinkov:2009:ECM


SIR04

Stubblefield:2004:KRA

Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. A key recovery attack on the 802.11b wired


REFERENCES

Seki:2001:DCR


Stojanovski:2001:CBRa


Sklavos:2003:DDR


Sklavos:2005:ISH


Stavrou:2005:CAS


Stabell-Kulo:2006:ESC

REFERENCES

Saldamli:2007:SME

Shu:2009:RCA

Sugita:2001:SRV

Sano:2000:PEA

Skolnikoff:2003:SS

Schindler:2001:IDC
[Werner Schindler, François Koeune, and Jean-Jacques Quisquater. Improving

Srinathan:2002:ASC


Sugita:2000:RAD


Schneier:2000:CTA

Scharwaechter:2007:AAE


Sterbenz:2000:PAC


Shim:2005:SFA


Srivatsa:2005:SPS


Skoudis:2006:CHR

REFERENCES


Song:2001:DWF


Sarkar:2000:CNB


Sarkar:2000:NBC


Sebag-Montefiore:2000:EBC

REFERENCES


Sebag-Montefiore:2007:EBC


Simos:2007:CMS


Smith-Miles:2008:CDP


Seyedzadeh:2011:IES

REFERENCES


REFERENCES


REFERENCES


[SNW00] Reihaneh Safavi-Naini and Yejing Wang. Sequential traitor tracing. In Bellare [Bel00], pages 316–??.

[Safavi-Naini:2000:STT]
REFERENCES


JooSeok Song, editor. Information security and cryptography — ICISC'99: second international confer-
 REFERENCES

Shigetomi:2002:ALS


Smith:1979:UFM


SOTD00


Sumii:2003:LRE

REFERENCES


REFERENCES


[StDenis:2006:BMI] Tom St Denis and Greg Rose. BigNum Math: Imple-


Schmidt-Samoa:2006:AFW


StPierre:2000:TFA


Sakurai:2001:NSS


Shamir:2001:IOO


Stern:2001:ADW


REFERENCES

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

**Stallings:2000:SSC**


**Stallings:2002:CNS**


**Standboge:2002:ENO**


**Stajano:2003:SCU**


**Stanik:2005:NLO**


**Stamp:2006:ISP**


**Sterlicchi:2000:SCD**

REFERENCES


REFERENCES

Stinson:1995:CTP

Stinson:2001:C

Stinson:2002:CTP

Stieber:2006:OH

Stieber:2006:GH

Stinson:2006:CTP

Stipcevic:2011:QRN

Shimoyama:2002:MLC
[STK02] Takeshi Shimoyama, Masahiko Takenaka, and Takeshi

REFERENCES


Saxena:2007:TCP


Shaltiel:2007:LEU[Su05]


Sugihara:2001:PCD


Sugita:2003:DRW


Sullivan:2005:CFI


Sun:2000:DRR


Sun:2000:ESM

[Sun00b] Hung-Min Sun. Enhancing the security of the McEliece public-key cryptosystem. Journal of Information Science and Engineering, 16
REFERENCES


Sun:2002:IIR


Sun:2005:UMS


Seidl:2008:FOV


Shaltiel:2008:HAP


Seb:2007:SMO


Shmueli:2009:DEO


Smith:2000:CIR

REFERENCES


**Schneier:**2000:**PCF**

**Sun:**2000:**AFA**

**Stubblebine:**2002:**ALF**

**Shim:**2005:**WIB**

**Stuck:**2005:**HVC**

**Shieh:**2006:**ERM**
REFERENCES


REFERENCES

Song:2007:TAK


Shujun:2001:PRB


Seo:2001:CDA


Sun:2006:PBA

REFERENCES


REFERENCES


Skoudis:2003:MFM


Sarikaya:2008:SPT


Sun:2002:NAD


Sun:2005:WIW


Tada:2002:OSM


Tang:2001:AES


Tang:2007:MMU

REFERENCES

1063-6889. LCCN ????
URL http://www.lirmm.fr/arith18/.


[TC01] Chwei-Shyong Tsai and


Andrew W. Todd, Jonathan Erickson, Nadine McKenzie, Chris Cleeland, Richard Huang, Ragae Ghaly, and The Editors. Letters: Shared source and shared secrets; JavaScript fix; CORBA interoperability; EJB application servers update; correction [“The Delphi XML SAX2 Component and MSXML 3.0”]. *Dr. Dobb’s Journal of Software Tools*, 26(10):10, 12, October 2001. CODEN DDJOEB. ISSN 1044-
REFERENCES

Terai:2008:BRB


Thorsteinson:2004:NSC


Theoharidou:2007:CBK


Tirkel:2001:UWE


Thimbleby:2003:RE


Tabatabaian:2001:NSP

Tippett:1927:RSN


Torres:2007:ANS


Tseng:2001:GGO


Tseng:2001:CLB


Tseng:2003:DSM


Tico:2003:RAS


Toll:2008:CSE


Thien:2002:TSS

[TL02] Chih-Ching Thien and Ja-Chen Lin. Technical section: Secret image shar-

**Thomas:2007:HQU**


**Turner:2006:SIS**


**Tsai:2005:CAE**


**Tan:2004:OBC**


**Tokita:2001:ADC**

REFERENCES


Tanaka:2001:QPK

Tochikubo:2000:RAE

Tomaszewski:2006:YSY

Topham:2002:BRJ

Totsch:2000:MSS

Tague:2007:CSA

Trope:2007:CSD
REFERENCES


REFERENCES


[Takano00] Kohji Takano, Akashi Satoh, and Nobuyuki Ohba. Poster 5: TATSU — hardware accelerator for public-key cryptography using Montgomery method. In Anonymous [Ano00d], page ??

REFERENCES

Tahir:2000:RCM


Tzeng:2001:PKT


Tian:2001:ICE


Tuchman:1966:ZT


Turing:2004:BS


Tiri:2003:SEA

Kris Tiri and Ingrid Verbauwhede. Securing encryption algorithms against DPA at the logic level: Next generation Smart Card technology. In Walter et al. [WKP03], pages 125–136. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
Toft:2001:LTT


Trappe:2002:ICC


Tsai:2007:TTA

REFERENCES

Tsaur:2005:EUA


Tiwari:2009:CIF


Thamrin:2008:PBR


Tzeng:2004:NTM


Ting:2002:FBS

REFERENCES


[ÜG08] Ozan Ünay and Taflan I. Gündem. A survey on querying encrypted XML documents for databases as a service. SIGMOD
REFERENCES

Uchida:2009:FPR


USC:2000:HRS


USHCAS:2000:UEP


USHCIR:2000:HES


USHCIR:2000:MHS

REFERENCES


.Urien:2001:PIS


REFERENCES


**USENIX:2001:PUA**


**USENIX:2001:PFT**


**USENIX:2001:PTU**


**USENIX:2002:PBF**


**USENIX:2002:PUS**


**USENIX:2002:PFT**

Utami:2002:FID


Urien:2001:XS


Ustimenko:2001:CGT


Ulfving:2000:GS


Uzun:2004:BRC

REFERENCES


REFERENCES


vanDijk:2004:AOC


Verheul:2001:EXM


Vercauteren:2002:CZF


Vergnaud:2006:RBS


Vernitski:2006:CUM

REFERENCES


REFERENCES

11–14, 2002, Cathedral Hill Hotel, San Francisco, CA.

[Vural:2007:IND]


[Vo:2008:SMA]


[Volos:2009:IEP]


[Viega:2003:SPC]


[Viega:2002:NSO]


Vasco:2005:NCS


Voice:2005:OAM


vanOorschot:2008:PMU


vanOorschot:2007:IRS


Vogt:2001:USC


Venkatesan:2001:GTA


vonWillich:2001:TIT


Vaudenay:2001:SAC


Whittaker:2006:HBW


Woody:2007:COS

Carol Woody and Christopher Alberts. Consid-

**Weitzner:2008:IA**


**Wachsmann:2005:CAK**


**Wallach:2000:SSM**


**Wagner:2000:CYL**


**Wagner:2002:GBP**


**Wagstaff:2003:CNT**

REFERENCES


Walsh:2000:BRM

Walter:2001:PBM

Walter:2003:STM

Wallich:2004:EEI
REFERENCES

Wallich:2009:SGP


Wang:2004:AWA


Wang:2004:TVS


Wang:2005:SCR


Wardlaw:2000:RPK


Washington:2008:BRB


Washington:2008:ECN


REFERENCES

Wu:2001:CDS


WBL01


Wong:2001:EMA


[Wu:2001:CKA]


[WC03a]


[WC03b]

[Wu:2003:UFR]


[WC04]


REFERENCES


Weng:2003:CHC


Wernsdorf:2002:RFR


Westfeld:2001:FSA


Wu:2002:LCN


Wang:2004:CHF


Wang:2002:CSE

Xiang Sheng Wang and Juan Ren Gan. A chaotic se-


Hsiang-An Wen, Sheng-Yu Hwang, and Tzonelih


REFERENCES

Wang:2005:EAS


Whyte:2005:TFC


Wiener:2000:AAH


Williams:1999:QCQ


Wilcox:2001:SEH


Wilson:2001:PBA


Williams:2006:C

Winterbotham:2000:USI

Wincelberg:2001:JQH

Windley:2005:DI

Winkler:2000:SAU

Withers:2001:IWU

Wang:2007:VBW
REFERENCES

696

Welschenbach:2001:CCC

Wang:2005:ECSb

Won:2006:ISC

Weigold:2008:RCA

Walter:2003:CHE


[H06] Hsiang-An Wen, Chun-Li Lin, and Tzonelih Hwang.

**Wen:2005:TRB**


**Wang:2009:DSM**


**Wang:2003:CET**


**Wang:2005:SAI**


**Wu:2005:IAW**


**Wong:2004:RCK**


Wang:2005:TSP


Wu:2008:RWM


Watters:2008:VDL


Wheeler:1995:TTE


Watanabe:2002:CCD


Wang:2008:NAD

REFERENCES


Won:2001:ISC

Wool:2000:KME


Wood:2005:IIM


Wang:2003:SGP


Wollinger:2005:CVH


Weimerskirch:2001:ECC


Wang:2001:TUR

[WQWZ01] Guilin Wang, Sihan Qing, Mingsheng Wang, and Zhanfei Zhou. Threshold undeniable RSA signature scheme. Lecture Notes in Computer Science, 2229:221–??, 2001. CO-
REFERENCES


Wright:2002:EPS


Whiting:2003:MPH


Weimerskirch:2002:DLW


Wu:2001:DSM


Wu:2002:CSCb

Hongjun Wu. Cryptanalysis of stream cipher Alpha1. *Lecture Notes in Computer Science*, 2384:


REFERENCES

Wang:2004:CWS

Wolf:2005:NML

Wang:2006:SPS

Wang:2008:DCP

Wu:2001:CFF

Worley:2000:AFP
[WWCW00] John Worley, Bill Worley, Tom Christian,

Wollinger:2000:HWH


Wincelberg:2002:LIE


Wang:2008:HQS


Wang:2002:WEM

Notes in Computer Science, 2455:333–??, 2002. CO-
link/service/series/0558/ bibs/2455/24550333.htm; http://link.springer-

Wu:2005:CTR


WY05

Wyant:2002:APK

Jeremy Wyant. Applicability of public key cryptosystems to digital rights management applications. Lecture Notes in Computer Science, 2339:75–??, 2002. CO-
link/service/series/0558/ bibs/2339/23390075.htm; http://link.springer-

Wxaa

Wang:2005:CSA

yiqun/shanote.pdf.

WY05a

Wang:2005:FCFa


WY05b

Wang:2005:FCFb

Wang:2005:ECSa
[XB01]

Winslett:2005:PLD
[WZB05]

Wang:2005:DIC
[WZW05]

Xu:2001:EIE
[XC05]

Xu:2001:CPW
[XFZ01]
Changsheng Xu, David Dagan Feng, and Yongwei Zhu. Copyright protection for WAV-table syn-

**Xiao:2003:HPC**


**Xiao:2005:SPA**


**Xenakis:2006:GCO**


**Xu:2007:CAD**


**Xu:2005:ADR**


REFERENCES


Xing-Yuan:2011:PRS


Yan:2000:NTC


Yang:2002:NEC


Yang:2005:TFN


Yan:2007:CAR


Yasuda:2008:DLP


Yuan-bo:2004:ITA


Yue:2001:GNN

[YC01] Tai-Wen Yue and Suchen Chiang. The general neural-network paradigm for visual cryptography. *Lecture Notes in Computer Science*,
Yue:2007:SEV


Yiu:2008:ODC


Yang:2009:ETP


Yang:2009:IBR


Yang:2009:CGA

Yang:2004:MSS


Yu:2007:NSM


Yang:2008:NFD


Yung:2006:PKC


Yekhanin:2007:LDC

Yan:2006:ICP


Youssef:2001:CIM


Youssef:2001:IAB


Yang:2005:IME


Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon. RSA speedup with residue number system immune against hardware fault cryptanalysis. *Lecture Notes in Computer Science*, 2288:
REFERENCES

716


Yu:2005:EHI


Yoo:2002:LAU

Yoo:2006:NCB

Yun:2001:RP

Youssef:2001:CAF

REFERENCES


**Yoon:2005:CFI**


**Yoon:2005:ICJ**


**Yoon:2005:IFA**


**Yoon:2005:IHL**


**Yeh:2002:SAK**


**Yeh:2004:PBU**

REFERENCES


[YT09] Danfeng Yao and Roberto Tamassia. Compact and

**Yang:2004:ENT**


**Ytrehus:2006:CCI**


**Yang:2005:SEA**


**Yung:2002:ACC**


**Yung:2002:CI**

Moti Yung. Cryptointegrity. *Lecture Notes in Computer Science*, 2501:
REFERENCES


Yang:2004:ISE


Yang:2004:CUF


Yang:2005:CIA


Yen:2006:SED


Yang:2005:IYS


Yang:2008:VCS

Ching-Nung Yang, Chung-Chun Wang, and Tse-Shih Chen. Visual cryptography...

[102x681] REFERENCES


[D] Young:2001:BOK

A. Young and M. Yung. Bandwidth-optimal klepto-

*Young:2004:MCE* [YY04]

*Yoon:2005:SWL* [YYDO01]

*Ye:2001:ATD* [YY05a]

*You:2001:GEC* [YYZ01]
**REFERENCES**

bibs/2229/22290246.htm; 

**Yen:2000:WOW**


**Ye:2007:NAW**


**Youssef:2009:IEU**


**Zafar:2000:ACB**


**Zane:2001:EWD**


**Zhang:2005:ITA**

Zhang Zhang, Shunsuke Araki, and Guozhen Xiao.
References


Zivkovic:2005:AAH


Zhao:2005:SSV

[ZBP05] Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. In ACM [ACM05a], pages 1–6. ISBN 1-59593-269-0. LCCN ????

Zhang:2000:MCA


Zhang:2004:AIB


Zhang:2005:CHC


Zhang:2009:CII

REFERENCES


REFERENCES

Zhang:2005:CSS


Zhen:2004:IBS


Zhang:2005:AES


Zou:2005:MED


Zhang:2000:WMH


Zhao:2006:NDN


Zhang:2008:CLR

REFERENCES

[Zheng:2001:ISS]

[Zheng:2002:NPK]

[Zheng:2002:ACA]
Yuliang Zheng, editor. *Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and In-


[Zhou:2002:MVD]

[Zhong:2006:ESC]
Sheng Zhong. An efficient and secure cryptosys-

**Zirkind:2007:ADC** [Zir07]


**Zhang:2004:BAF** [ZJ04]


**Zhang:2009:IBR** [ZJ09]


**Zhang:2002:IBB** [ZK02]

Zhang:2005:CLH


Zhang:2004:SAE


Zhang:2004:AFV


Zhang:2004:RMA


Zhao:2005:MCE


Zhang:2001:QKD

Yong-Sheng Zhang, Chunfen Li, and Guang-Can

Zhang:2002:CRD


Zhang:2001:CIS


Zhang:2005:DMC

Zhiyong Zhang and Jie Xin Pu. Delegation model for CSCW based on RBAC policies and visual modeling. In Han et al.
Zhou:2005:MBI

Zhou:2005:APS

Zhu:2007:IHH

Zhang:2005:RPE

Zhang:2005:APA

Zhou:2005:APS

Zhang:2001:ASE

Zhang:2003:FSP


REFERENCES


Zhang:2004:NMS


Zhong:2008:GPT


Zhang:2001:USC


Zhang:2004:NMS


Zhong:2008:GPT

REFERENCES

CANED2. ISSN 0163-5964 (print), 1943-5851 (electronic).


