Title word cross-reference

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

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

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

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

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

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

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

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

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (pk)
\( N^{0.292} \) [BD00b]. \( N_{C}^{0} \) [AIK06]. \( p \) [FL06].
\( p^{r}q^{*} \) [LKY00]. \( p^{*} \) [CHH01]. \( Q \) [Yas08]. \( r \) [JY01], \( w \) [DwWmW05, OT03b]. \( x^{\infty} \) [Gon06].
\( y \) [OS01]. \( Z_{n} \) [LWL09].

-Adic [GHK+06], -Bit [AIK+01, CDL+00, PCG01]. -Connected [BJLS02]. -Coordinate [OS01]. -Coverings [SC02b]. -Decompositions [vDKST06].
-DNF [BGN05]. -Metric [LBGZ01, LBGZ02]. -NNAF [DwWmW05]. -Out-of [CT08b]. -Polynomials [FL06, CHH01]. -Round [BP04, Bih00, GIKR02, CKL+03]. -Source [KLR09]. -Steiner [WL02]. -Threshold [CLT07, Kog02]. -Way [LKJL01]. -Year-Old [Eva09].

.NET [For04, TG04].

/dev/random [BH05]. /evolution [Pat02a]. /MOM [DJLT01].

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

1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05b, WYY05c, Was08a]. 1-58488-518-1 [Was08a].
1-Connected [BJLS02]. 1-out-of-n [AOS02]. 1.82Gbits [KV01].
1.82Gbits/sec [KV01]. 101 [Sei00a].
10118-3 [ISO04]. 106 [Uni00c, Uni00d, Uni00g]. 106-1 [Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a].
109-bit [Pri00]. 10th [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. 11-15 [AUW01]. 11th [CCMR05, HY05b, HH04, HH05, RM04, Roy05, USE02b]. 12 [TPS01].
128 [JJ02, WFLY04]. 128-Bit [SM03b]. 12th [GH05, MS05b, PT06]. 13-15 [ACM05b]. 130 [LM08]. 14th [AMW07, AAC+01, Bir07]. 150-Kilometer [Das08]. 155 [LMP+01]. 15th [MJ04, BC01].
160 [KF00]. 16th [BS03]. 17th [IEE05b]. 176 [Nat00]. 18-2 [Nat00]. 18th [KM07].
19005-1 [ISO05]. 192-bit [Luc00]. 1993 [PPV96]. 1999 [Lee03b, Uni00a, Uni00b, Uni00c, Uni00d, Uni00g, Uni00h, Uni01].
19th [BCDH09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH+00b, Eke02, Irw03, KH08, KI01a, Sch00b, Wit01, YG01c]. 2001 [ACM01a, BC01, GJSS01, Lee03a, Pem01b].
2002 [B+02, IEE02, RSA03a, Yun02a]. 2003 [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, WKP03]. 2004 [ACM04b, ZC04].
2005 [ACM+05a, ACM05b, ACM05c, ANS05, HY05b, ISO05, Roy05, Ter08, Ytr06]. 2006 [ACM06]. 2007 [ACM07, Ano06b, SM07b].
2008 [ACM08, Dew08, YRS+09]. 2009 [ACM09, May09]. 20th [Bel00]. 21 [AJ01b].
21264 [WB00]. 21st [Jef08, KI01a]. 21th [IEE09a]. 22 [McK04, TTZ01]. 22nd [Yun02a]. 23rd [Bon03].
24th [Cra05a, Fra04]. 256-bit [Luc00]. 25th [Yun02a]. 26 [DB04]. 26th [EBC+00]. 27th [Men07]. 29. [Eke02]. 29th [FLA+03].

3 [Duw03, Imr03]. 3-515-07640-9 [Eag05].
3-540-66778-4 [Duw03]. 3-Key [Ko05a, Ko05b]. 3.0 [Flu02b, Hei01, SQ01].
305 [ECM00a]. 306 [ECM00b]. 30th [Coc02a]. 314pp [Duw03]. 3278 [BWBL02].
33rd [ACM01a]. 36th [ACM04b]. 37th [ACM05c]. 39th [ACM07]. 3D [LZP+04].
3GPP [KSHY01, SM02]. 3rd
3

[ACM05a, USE00a].

4 [Duw03]. 4-round [DLP+09]. 40th [ACM08]. 41st [IEE00a]. 42nd [IEE01a]. 43rd [IEE02]. 44th [IEE03]. 45th [IEE04]. 46th [IEE05a]. 47th [IEE06]. 48th [IEE07]. 49th [IEE08]. 4th [BCKK05, BC05c, DWML05, DRS05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, KN03, MS05a, NP02a]. 5 [BCJ+06, Wac05]. 50th [IEE09b]. 512 [AD07, GLG+02]. 5th [CV04, KJR05, LL03, LLT+04, Li05, NP02a, Syv02, WKP03]. 64 [LKH+08, WWCW00]. 6th [Bla03, Des02, HA00, JQ04, LL04d, MMV06, Oka00]. 7 [And04, Gum04]. 7-round [Pha04]. 7.2 [TvdKB+01]. 77 [AL04]. 7th [BDZ04, Boy01, Chr00, DFPS06, PC05a, RS05, Sch01d, ST01d, Wri03].

8-Round [BF00a]. 8.8/11.2 [DFPS06]. 800 [BG07a, Hir09]. 800-90 [BG07a, Hir09]. 802.11b [BG07a, Hir09]. 802.11g [Coc02a]. 802.15.4 [Miˇs08]. 82 [Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02, SMP+09, VY01, Vau05a, WK06, Zhe02b].

9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04]. 90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1 [GM00b]. '98 [Wi99]. '99 [DN00b]. 9th [CCMR02, CSY09, DR02c, DKU05, Lai03, NH03, Pat03b, PY05, YDKM06].

= [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05a, Kel05b]. A5 [BD00a, BSW01, PS01c]. A5/1 [BD00a, BSW01, PS01c]. AA FG1 [Hug02]. AAIs [LOP04]. Aarhus [Cra05a]. Abadi [MW04]. Abelian [CF02, PHK+01, RS02]. Abstention [JLL02]. Abstract [CM00, Cou04, DIRR05, HLvA02, HJV01, JL00, MSJ02, MP02, Mas04, Wag02, BJN00, BCDM00, CD00a, CC04c, FKS+00, GHJ00, GT04, HT04, HP01, Iwa08, IK00, Jon08, KKS00a, KM00, LMO, Mes00, Pei09, Yas08]. Abstracting [Bla01a, Mon03]. abstraction [BLP06]. abstractions [BG07b]. Abstracts [Sch00b]. Accelerated [Elb08]. Accelerating [ES+05]. acceleration [EHK04]. Accelerator [CGBS01, RS04, TS00, XB01, DPT+02]. Acceptance [CFRR02]. Access [ANRS01, Ano02e, BNPW03, CGMM02, DS06, HC08, MS03b, Riq02, Sma03a, Sun00a, ZGLX05, AW05, AW08, AFB05, BA06, BNP08, Che08b, DFM04, Hos06b, HW03c, HY03, JY06, JW06, KNS05, LKZ+04, MF07, MSP+08, PS02a, STY07, WL05, WCO1b, You04]. access-control [BNP08]. accessible [Pau02a]. accountability [WAB01]. Accounting [Lai08].

Accumulator [GTH02]. Accumulators [CL02a]. accurate [ZT05]. Achieve [CFS01]. Achievement [Coc01a]. Achievements [VDK05]. achieving [PS04c]. ACISP [YG01c]. ACM [ACM01a, ACM03a, ACM03b, ACM03c, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, MS05b, Bar00b, FMA02, Ra06].

ACNS [GKS05, IY05, JY04, ZT05]. acoustic [ZT05]. Acquiring [SETB08]. across [Dav07, ZBLvB05]. Act [Kha05, Uni00a, Uni00e, Uni00d, Uni00g, Uni00h]. Actel [DV08]. Action [SE01]. Active [BC05a, BACS02, BP02, LJL05, MA00a, MA00b, Tad02, BPS08]. Active-Content [MA00a, MA00b]. activities [AJ08, SN07]. actually [Hau06]. Ad [BS02, KH05, WT02, Cha05b, DHM07, KVD07, LHC08, LKZ+04, PCSM07, SLP07, TW07, ZC09, MAa04]. 'ad-Durayhim’s [Ma04]. Ad-hoc [BS02, WT02, DHM07, ZC09].

Adaptation [ISSZ08]. Adapting [MJD01].
Adaptive
\[\text{CM00, CBB05, CTL04, CL08, Coc02a, CS02,}
\text{CS03b, DSS01, EFY}^+05, \text{FMY01, JM02,}
\text{KCJ}^+01, \text{KL01, LP01, MP05, Nov01, Pie05,}
\text{ZWC02, AAPP07, Che07a, DP04, MB08,}
\text{SH11, WNQ08, XMST07, YZDW07, ZCW04].}

Adaptively
\[\text{AF04b, CHK05, FMY02, JL00}.\]

Adaptively-Secure
\[\text{CHK05}.\]

Added
\[\text{Ano02b, St.00}.\]

Adding
\[\text{FBWC02}.\]

Addison
\[\text{Puc03}.\]

Addition
\[\text{KT00, LPZ06, PP06a}.\]

Additive
\[\text{FMY01, MF01}.\]

Additive-Sharing
\[\text{FMY01}.\]

Address
\[\text{IIT03, Nik02a, Nik02b, FXAM04, RW07}.\]

Address-Bit
\[\text{IIT03}.\]

Addressing
\[\text{HTW07}.\]

Adi
\[\text{Coc03}.\]

Adic
\[\text{GHK}^+06.\]

adjacent
\[\text{JT01b}.\]

Adjustment
\[\text{BSNO00}.\]

Adlan
\[\text{MAaTxx}.\]

Adleman
\[\text{BB79, Coc03, SP79}.\]

Administration
\[\text{USE00c, USE00a, Ris06, WL04a}.\]

administrative
\[\text{Cra05b}.\]

Admitting
\[\text{HSZI00}.\]

Advance
\[\text{CF07, DFFS06, Lan00a, Lut02b, MM01c,}
\text{Mor05, Sch06a, BBK}^+03b, \text{DFCW00, ISTE08,}
\text{Swe08, Tan01, Ase02, Bar00c, III00, Bur03,}
\text{CMR06, Coc02b, DR01, DR02b, Dan01,}
\text{DRS05, FIP01a, GC01a, Har00, Her09a,}
\text{Lan04a, MP01a, Mor05, NIS00, Pha04, SB00,}
\text{Sey00, WBRF00, Wri01, YW06}.\]

Advances
\[\text{AI09, Bel00, BSS04, BSS05, Bon03, Boy01,}
\text{Cla00a, DFPST07, ELv01, Kil01a, Oka00,}
\text{Ph01, Pre00, TIS07, Yum02a, Kat01, Bih03,}
\text{CC04a, Cra05a, Fra04, Knu02, Lai03,}
\text{Lee04b, LIT}^+04, \text{Li05, LST}^+05, \text{Men07,}
\text{Roy05, Sho05a, Zhe02b}.\]

Advantages
\[\text{CDS07}.\]

Adventures
\[\text{Hro09}.\]

Adversarial
\[\text{CLR09, GSS08, MNS08}.\]

Adversarial-knowledge
\[\text{CLR09}.\]

Adversaries
\[\text{CM00, JQY01, KSR02, Lu02,}
\text{RK05, SKR02, GXT}^+08, \text{ZD05}.\]

Adversary
\[\text{Aba00, Gor06, RW02}.\]

AES
\[\text{CGH}^+00b, \text{DRS05, FIP01a, Her09a, Pha04,}
\text{AG01, Ano00a, AL00b, BDK}^+09, \text{CG03,}
\text{Coc02b, DR00b, DR02a, DR02b, DLP}^+09,}
\text{DPR01, Dan01, Dra00, EYCP00, Elb08,}
\text{Fer06, FM02b, GC00a, HW03b, IBM00,}
\text{IK00, IK01, Jok00, KS09a, Kel05a,}
\text{Kel05b, KFSS00, KV01, LP02a, Len01,}
\text{MMH}^+02, \text{Mes00, Mes01, MR02a, MR02b,}
\text{OST05, OST06, PBFW07, PQ03b, RRY00,}
\text{SKKS00, SM03b, Sch00b, SKW}^+00, \text{SW00a,}
\text{SL00, WW00, WB00, WOL01, WWGP00,}
\text{WWCW00}.\]

AES-CBC
\[\text{Fer06}.\]

AES-like
\[\text{DLP}^+09.\]

AES-related
\[\text{Sch00b}.\]

Affine
\[\text{Ben00, CT09, Fel06, HH09}.\]

Affine-Transformation-Invariant
\[\text{CT09}.\]

AFIS
\[\text{Zip07}.\]

Agency
\[\text{Ber03, McL06}.\]

After
\[\text{UC05b, DM07b, FKS00, KS00a, KKS00a,}
\text{KSS01, Mes00, Mes01, MPS05, MH04,}
\text{P010b, Pro01, RK05, AG01, Ava03, Bau05,}
\text{BPR00, BP02, BNN}^+09, \text{BBB}^+02, \text{BGM09,}
\text{BCP02b, CM00, CS03b, DB04, DJ06,}
\text{Des00b, Des00c, Eg0h0, EBS01, FP01, Fry00,}
\text{Geb04, HNZT02, HLL}^+01, \text{PG07, Hau05b,}
\text{HLC08, In05, ISW03, IIT03, JKS02, JJ00b,}
\text{JT01a, Kan01, KM02, KML}^+02, \text{LM08,}
\text{LPV}^+09, \text{Lu02, Mi00, M02, MG08,}
\text{NRR00, NLD08, OKS05, OS00, OTO0b,}
\text{OTO3b, PKBD01, PSC}^+02, \text{PSP}^+08, \text{PS01b,}
\text{PQ03b, RS01, SKQ01, Sch01b, Sch01f,}
\text{SDF00, SDF01, Sem00, Sho00b, SKU}^+00,}
\text{SK01, SLL}^+00, \text{Tad02, TV03, VHP01,}
\text{XH05, YJ00, YKLM02a, YKLM02b,}
\text{YKLM03, ZCW04, ZSJN07}.\]

Age
\[\text{Mar08b, Lev01}.\]

Age
\[\text{AAFG01, CT08a, MS09b}.\]

Aggressive
\[\text{Wy05}.\]

Agreement
\[\text{AAFG01, CT08a, GW00,}
\text{HR05, HS07, RW03a, SK00, Tan07b.}
Mes00, Mes01, MAaTxx, MG08, NP02b, NSS02, OS06, ŒOP03, Puc03, QS01, SSST06, Sha01c, Sma03b, SDMN06, SQ01, SWT07, YSS+01, ZCO0, ZGLX05, AvdH00, AW05, AW08, Ab01, AHK03b, As04b, BDSV08, BKK+03b, Bjo05, BG07a, BR05, BCJ+06, CKL+09, CW07, CS05a, DS09, DKS08, GW08, GM04, GTZ04, Has01b, Hir09, Hro05, Hutt01, JEO04, JPL04, JSW05, KS00, Koc09, LKH+08, LMW05]. Analysis [LW05a, LKJL01, Lu07, Mea04, MT07, MRST06, OS00, PSG+09, PS08b, SK01b, WLT05a, WPP05, XH05, XMST07, YCW+01, YC08, ZWWL01, ZL04c, ZDW06]. Analytic [Shp03, Nie04]. Analyzing [MS01, Shy02, CP07, DFG00, HM02a, ME08b, NCRX04]. Anatomy [Ban02]. Anchor [Ree01]. Ancient [Imr03, Sin00, Mol05, Pin06]. Andrei [Puz04]. Andrew [Puz04]. Anguilla [Fra01]. Anniversary [Sal01b, Coc02a]. Annotated [Pet08]. Annoyances [Tyn05]. Annoying [Tyn05]. Annual [ACM01a, ACM02, ACM04b, ACM05c, ACM06, ACM07, ACM08, Bon03, Cra05a, ELvS01, Fra04, IEE00a, IEE02, IEE03, IE04, IE05a, IE06, IE07, IE08, IE09b, Kiel01a, Men07, Sho05a, USE01b, USE01a, USE02c, VY01, Yun02a, ACM00, Be100, HA00, Jef08, NW03, ST01d]. Anomaly [RCG+05]. Anonymity [GM03, IKOS06, MP02, SS01b, EY09, LV07, Par04]. Anonymization [FXAM04, RW07]. Anonymouse [ABC+05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL+08, SOO02, Wan04a, YTO09, ZBO0, BPO3a, Chi08b, Chi08c, Chi08d, EY09, LHC08, Sac02, Sha03c, WCJ05, YTW02, ZCO0]. ANSI [III00, Kel05a, Kel05b, Oiw09, ANSI-C [Oiw09]. Answer [Ano01e]. Answers [PT08]. Anthony [Pag03]. Anti [Kha05, Ano05c]. Anti-Circumvention [Kha05]. Anti-virus [Ano05c]. Anticipation [Goo00]. Antikythera [Eva09]. Any [Fis01b, HNO+09, Ano05b, CDM00, DFM04, DMS00, HR07, Poi00]. Anyone [Ros07]. Anytime [DJLT01]. Anywhere [DJLT01]. Apache [Had00]. API [MW01, Mor03]. APIs [BM01c]. Appendix [Kel05a, Kel05b]. Applet [ZFK04]. Applets [Bis03a]. Applicability [Wya02, TM01]. Application [AD09, ACS02, Bai01b, Boy01, CL02a, CK03, Dam07, Dhe03, GHK+06, HF00, IKP+07, JX05, Jou04, Lai03, Lee04b, LS05b, LXM+05, NP07, Oka00, Pf01, PQ03b, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TWA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG09, CMK07, CP07, DIME, FP00, HCBELTR06, JRS09, JMV09, LGKY10, Lav09, MT07, MPH06, MK05a, NZS05, RSS04, SSST06, TC00]. Application-Aware [IKP+07]. Applications [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, BI05a, BGK+03, BS00a, Bih03, BG04, BS02, BLO8, CC04a, CD00a, CV02, CG01, CZ05, CHSS02, CSY09, Cra05a, CDI05, DJ01, DK02, DK07, DA03, DF06, FR02, GSS08, GKK+09, GJKR03, Gen04a, GR06, Gol01a, Gol04, HRS02, HNO0, Har06, Has01a, HSS04, HR05, HJW05, JT01b, JY01, KMM+06, KGL04, KMO01, KM09, KK10, KM02, MA00, MM07b, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Shp03, SX01, SPG06, Vau02, Wya02, XYL09, YZ00, Zes00, Zh02, ACTZ05, Ate04, AH05, AFGH06, BG08, BGL+03, CCCY01, CM05b, CS09, CSK+08, DY09a, DFCW00, DJL01, FP09, Fin03, Fis01a, Gal02, GVC+08, GKK+07, GB09, HHSS01, Has02, Hen01, HKPR05, Jac00, KVN+09, KNS05, LA00, Lee04a]. Applications [LJO5a, LPW06, LB05, MY01, Mal06, MC04, MSV04, Nie04, PW08, PBD07, PC00, Q500, Ros06b, SSS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPH06, WW08.
WA06, WV00, YS04, ZBP05]. **Applied** [HW03a, HWR09, SL07, GV09, GNP05, IKY05, JYZ04, ZYH03]. **Applying** [Elb09, KC02, Lan00d, LMSV07, SQ01, SPMLS02, TND+09, vDKST06]. **Appointed** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08]. **Approach** [BKM07, CGFSHG09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03, Lai07, LL05c, Lu03, OMT02, SQ01, SPMLS02, TND+09, vDKST06]. **Approaches** [CL01a]. **apprehension** [AJ08].
Asymptotically \cite{dvo04}. Asynchronous \cite{ckps01, fml04, ksr02, skr02, zsv05}.

at-targama \cite{maat05}. Atlanta \cite{iee09b}. ATM \cite{pat02a, pat02b, zea00}. Atomic \cite{cn06}. Attached \cite{rcbl00}. Attachments \cite{ric07}. Attack \cite{ahm08, ckq03, cs05b, des06b, fil00, fv03, ghjv00, ghjv01, hq01, hug02, hw01, jj00b, kcp01, kso0a, km01c, ly07, lnl08, lv04, lmv05, luc02a, man01, mho04, mus05, nov01, om09, pv06a, pq03b, rms05, sg00, sch01b, sho00b, sma03b, vhp01, yklm02a, zc04, ask05, ade09, ano09c, dkl00a, duy08, duy09, gm00a, han04, hes04b, hg07, iwa08, jj02, kso09a, km04a, lm08, law09b, ls05b, mir05, os00, sir04, xh05, zcw04]. Attack-Resistant \cite{lnl08}. attacker \cite{bdsv08}. Attackers \cite{jmv02}. Attacking \cite{fmp03, kpr03, luc00, tmmm05, bfs06a]. Attacking-Based \cite{tmmm05}. Attacks \cite{arr03, ag01, ak03, bc05a, bpr00, bp02, bmm00, bbd02, bdk09, bu02, bm03b, bmg09, bcp02b, bm01c, can06b, cs07b, cz03, ct08a, cs01, ckm00, cjp00, cm03, cou03, cwr09, cd01b, dpv01, dfs04, dj06, ds08, dm07b, fksw00, fobh05, fp01, fry00, fur02b, gen04a, gk02, hsh08a, hnz02, hr04a, hsh01, hlc08, isw03, jks02, jj00d, kks00a, kss00b, kks01, kcj01, ki01a, law09a, lls05a, lws05, lj05b, m06, mp06, mf01, mk04, mes00, mes01, mel02, mg08, ot03a, ot03b, oop03, ost05, ove06, pkbd01, pdms09, rs01, skq01, sem00, swt07, tad02, vv07, wyy05a, wyy05d, wylz05, ydo01, yy01, yg01b, vwo1, bps08, bau05, bcs08, bzo3, ckl09, cs05a, dko8, geb04, hsh08b, hsh09, has01b, hsu05b, hl05b, ino05, im06, jd01]. attacks \cite{ks05a, ktc03, lvp09, lsh00, mmj05, ns05a, nd08, ots06, pq03a, rg05, scho0c, scho1f, shi05, sl06, sk05b, sw00b, w107a, w104b, yau07, yso2, zsjn07]. Attitudes \cite{fdi00, cf05}. attractors \cite{hyw07}. Attribute \cite{ly05, rsa00e, iy05}. Attributes \cite{ss01b}. Auction \cite{asa01a, ana01a}. auctioning \cite{rcg05}. Auctions \cite{bra01b}. Audio \cite{arn01, cs05c, drl09, mh05, wny09, wwl02, xfz01, wq08, bs01b, kjr05, kn03]. Audio- \cite{kjr05}. Audio-and \cite{bs01b, kn03]. Augmented \cite{cs07c, you01]. Augmenting \cite{al04}. August \cite{amw07, bel00, b02, bon03, fra04, hh04, hh05, ha00, jq04, kkp02, kll01a, kp01, mz04, men07, nh03, pt06, rs05, sch00a, sch04a, sch05a, sho05a, st01d, use00a, use00d, use01c, use02b, vy01, yu02a]. Australia \cite{boy01, iz00]. Austria \cite{duk05, p01, jef08]. Authentic \cite{dgm03, dur01, ss01b]. Authenticate \cite{bau03a, bau03b}. Authenticated \cite{agt01, bno0a, bpr00, bu02, bc04b, bmn01, bmp00, bcp01, cpp04, ch08e, dg03, da03, ep02, gko07, gl03, gttc03, hso7, kyo01, kyo03, kra03, lee01, lht09, mps00, mac01, ms02, mnd04, na07, nam02, p01, sk00, vau05b, wc01a, yppk09, yio4, zwc02, bkn04, bcp07, cyy05, cyh05, cle04a, clc08, cj04, cjl05, dg06, gl06a, gmr05, hjt08, hww02, hww03, hs05a, hwa05, hl05c, hl05d, jua04, koy09, kry05, lky03a, lky03b, ll04a, ll04, ll05a, lky05c, lky05d, lhc08, llr02, llr06, lwk05a, mis08, pq03a, pq06, rbb03, sei05, sw05a, sc05b, tlh05, t01a, tse07, wh06, wh02a, xyo4, yw05, yc09a, yso2, ysh03, yr05b, ypl08, zc04, zax05, zwo05b, zl05]. Authenticating \cite{aip01, ch08a, cv09, fur05, jw05, pm08, rcbl00, yso01, lin01b].
Authentication
[AAK09, AP09, ANRS01, Ano01b, Ano01c, Ano01f, Ano02d, AHKM02, ANL01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, BKR00, BCC01, BCC03, BC05b, BDKKB09, BR02, BDF05, BDF01b, BM03c, BL02, BLDT09, BWE+00, CV03, CGP08, CS07b, CC01b, CKL01a, CKL01b, CC05b, CC09, CJT02, CJ03d, CWY05, CT09, Cim02, Cir01, CFRR02, CGK+02, CF05, CJK+04, Cou01, CMB+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, FDIR00, Gan01a, Gar03a, GMW05, GSVC02, GD02, GT02, Gut04c, Had00, HSHI01, HSHI02, HSHI06, HKW06, HY01, Hae01, HS01b, HP00, HL07, ISSZ08, Jab01, JP02a, JP07, JP02b, JK05, KC09b, KH05, KVD07, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LTL+04, LB04, LL05c, LSH03b, LM00, LOP04, LHL+08, Lys07, MW06, MMO1a, Mal02]. Authentication
[MJ04, MD04, MR03, MGC02, MNT06, Nao02, Nik02a, Nik02b, OKE02, OH08a, PBD00, Par04, PMRZ00, PBC05, PK01, Qu01, RKZD02, Ric07, Ril02, SNWX01, SR01, Sch04c, sch05b, Sei00b, SY01b, SGB02, Sm00, Sm01c, Sm02, SE09, SK06, Str01b, SJ05, SYLC05, SC01, TK03, T TZ09a, TZT09b, Tsao01, VN04, WLL09, WCJ09, Way01, Way02a, Wea06, WKB08, WT02, WS03, WL07b, WLT05b, WH05, XYL09, Y101, YEP+06, YSR01, YLLL02, YKW01, Za00, ZJ04, ZBlv05, AhdH00, AF04a, Al06, Ano00k, Ano00l, Ano05b, Art04, AAKD09, Asl04a, Asl04b, AL04, Ayo06, Bad07, Bel04, BGP02, BSSM+07, BFG04, BFG05, BS01b, BBG+02, BDFP02, BF07, Cer04a, CBB05, CC01a, CCK04a, CL04c, CC04b, CC05c, C203, CY05, CCS08, CWJ01, CJT01, CJ03b, CH07a, Ch08b, Ch08c]. authentication [Chi08d, CL09, CF07, Coc01a, CmDv06, Dal01, DSGP06, DY09a, DGK+04, DG05, DW05, FLZ02, FCZ05, FGM03, Gan08, GLC+04, GTY08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Her09b, Hsu05b, HLTJ09, HYS03, HLL04, HL05b, sHCP09, JP06, JPL04, KLY05, KJ05Y, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LHY02, LH02, LH03a, LF03, LKY04, LW04, LH04a, LKY05a, LLY06, LLS+09, LFHT07, Li05, LST+05, LC08, IW05a, LH06, LWF04, LHL03b, LH03, LT04, LC04a, Lin07, LN04, LL08a, LL08b, LC05a, LC05b, Luk01, MS09c, MAB106, McK04, Mit00, MR00, ME08b, MP07, NC09, NLD08, OH08b, PY08, PCS03, PCC03, PI06, Pei04, Pha06, Pot03, Pot07, RFR07a, RFR07b, RFR07c, RG06, SNW01, SG07, SN07, Sch05c, Sco04, Sei05, SBS09, Sha05c, SL03, SSM+08, SW06, Shi05, SL05a, St.00, Ste05a, SW02]. authentication [SCS05b, SC05c, SCS05b, SZ05, SY06, TM06, TB02, TOEO00, TIS07, TW07, Tsa08, TWL05, UBE09, VM03, VK08, Voi05, Wac05, WLT03, Wan04a, WLT05a, WDLN09, WDCJ09, WC03b, WL04b, WHH08, XwWL08, YW04b, YW04a, YW05, YT09, YTWY05, YCYW07, YWWD08, YC09c, YCO9b, YS04, YRY04, YRY05a, YRY05c, YRY05d, YYY05, YbJf04, ZL04a, ZK05, ZSN05, Zha06, ZD06, ZSJ07, dB07, CS08b, ECM00a, ECM00b, LSH03a]. authenticator [CKY07, jLC07]. Authenticity
[AB01, Bla02a, CBD+05, GJ03, GOR02b, HG03, RW03b, Sch01a, MIt02a]. AUTHMAC_DH [Asl04b]. Author
[An005, An01d]. Authorisation [BM03a, CJK+04, LSZ05, RKZD02, YT09, GJJ05, JEZ04, Lin07, LOP04, SRJ01, WL04a, WZ05b, YbJf04]. Authorship [Top02]. auto [YY00]. auto-recoverable [YY00]. Automata
[LZ04, MGC02, Wue09, Bao04, CC05d, KKO3, Lf00, LQ08, Mon03, SBZ04, SHH07,
TC00, dRMS05. automate [Bur02].
Automated [CDR01, LLW05, LLW09, HIJW05, IY05, LS05b]. Automatic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05].
Automating [Gue03]. automorphism [Pae03]. automotive [LPW06]. Autonomic [VR02, LLW05, LLW09, HJW05, IY05, LS05b]. Automatic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05].
Auxiliary [Dam00, DKL09]. availability [CBD+05]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average [KMT01, CGHG06]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average [KMT01, CGHG06]. Average-case [Mic02b]. Avoid [Tyn05]. avoided [CNPQ03]. Award [RSA03a, Bar00b, Coc03]. Awarded [Coc02b]. Aware [IKP+07, OHB08a, CBSU06, OHB08b, Zea00]. Awareness [HL03, BK05]. Away [Coc03, Ols00, Tee06]. Awkward [TvdKB+01]. Axiomatization [dH08]. B [SPK08, YG01a]. B-Spline [SPK08]. B2B [Zho02]. Babbage [Bar00a]. Back [CZB+01, KCD07, SF07, Ano00g, Dea06]. Back-End [KCD07]. Backdoors [CS03c]. Backup [Str02]. backward [HCD08a, HCD08b]. backward-and-forward [HCD08a, HCD08b]. Bacon [GG05a]. bad [BBN+09]. bail [Ano01h]. Bait [Luc02a]. Balancing [Höf01, Lut02]. Ballot [Cha04]. Baltimore [ACM05b, ACM05c, GL05]. Banach [AUW01]. Bandwidth [CGJ+02, YY01a, SLP07]. Bandwidth-efficient [SLP07]. Bandwidth-Optimal [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Be00, Bon03, Fra04, Kl01a, Men07, Sh05a, Yun02a]. Barcode [Che08b]. Bare [DPV04]. Barken [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, XSWC10, IR02]. Based [Ano01c, ANR01, AF03, AJ08, BDG+01, BKLS02, BNS02, BN02, Ben00, BRS02, BF01b, BF03, BB04, Bon07, BCH07, BGH07, BPR+08, BD03, BM01, Boy03, BQR01, BM01c, BSN00, BRTM09, CGFSHG09, ČvTMH01, CK02a, CGMM02, CF01b, CC02a, CV03, CPP04, CCD07, CS07b, Cl01b, CLT07, CHSS02, CHM+02, CZK05, CM05a, CTH08, CGK+02, Coc01b, Con01, CFS01, CS00, DN00a, DKMR05, DT03, EHK+03, EM03, FL06, FM02a, FMY01, FGL02, GMF01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HCO8, HH09, Ig02, Jam00, KBD03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05a, Kel05b, KY01c, KY02b, KC09b, KK02, KC02, KCD07, KPR03, KM05, Kra02a, Ku02, KWP06, KT00, LL02, LP03]. Based [LKL05, LHT09, LZ01, LZ04, LL05c, LP06, LY07, LXH07, LLWR07, LWK00, LSC03, LHS05, LS05, LL05b, LCO7, MPS00, Mar08a, Mar08b, MNP01, Miy01, MGC02, Mul01a, MSU05, NM05, N001, N02, NBD01, N002, Nov01, NMS01, PV06a, PV06b, PP06a, PL09, PMRZ00, Ri02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sal05b, Sch01a, SSFC09, Sha02, Sha01c, SO012, SXY01, Sma03a, SBEW01, SGB01, TMM05, TYL02, TMT09a, TMT09b, VMS05, Vau05b, Ver06a, VHP01, VK07, WR02, WY02, WZ05, WG05, WCJ09, WCJ09, WBD01, WC04, XYL09, YKMY01, YT09, YYD00, YSS+01, YK01, YL05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWC02, vDW04, AAPP07, AA08, Ano02b, Ano05b, App05, AAKD09, BGB09, BBC+09, BR04, BFG08, BS01b, Bla01b, BW05, BLP06, BGL+03, BDS09b, Buh06, CGHG06, CG06, CL02b]. based [CO09a, CL04d, CYF+10, CL00, CCH04, CY05, Che05a, CSS08, CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CL06, CLK04, CLJ05, Cho08b, CYH+07, CFY+06, CCD+04, CTT07, CHT02, CC04c, Cra05b, DS09, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EHKK04, FL02, FXAM04, FW08, GMR08, GW08, GSK09, GL06a,
Binary [ADI09, HHM01, LSKC05, OSSST04, SKG09, WCJ09, ÁCTZ05, BG08, BG09, FSGV01, GB09].

Binary-Ternary [ADI09, KLE07].

Binding [DN02b, BioAW [MJ04].

Biometric [AHKM02, Dal01, EM03, HWH01, KJR05, LSt+05, MR00, RFR07a, RFR07b, RFR07c, Smi00, MJ04, TBJ02, ZJ04].

Biometric-Based [PMRZ00].

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

Biometrics-Based [Ril02].

Biomolecular [Bi09].

Birds [MLM03].

Birthday [Wag02].

Bisimulation [BJP02].

Bit [AIK+01, BK06a, BL08, CGHG01, CDL+00, DMS00, GS07a, IIT03, KZ07, LNS02, MS09a, PCD01, RMH03b, SM03b, SX01, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, PLsVdLE10, Pri00, RMP08, SWR05, UHA+09, WW08, ZFK04].

Bit-Fixing [KZ07, KZ03].

Bit-substitution [GPX08].

Bit-Locker [Kor09].

Bits [BS01d, SZ01, HN04, Shp02].

Bitslice [DPV01].

Black [Ano01j, CF02, CFS05, DI05, DRR05, DS08, KI01d].

Black-Box [Ano01j, BRS02, CF02, CF05, DI05, DRR05, KY01d].

Blackmailing [PS01b].

Bletchley

[Sal00b, Cop05, Cop06, Cop10, HS01a, Sal05a, SE01, Smi01b, Wei06, Win00].

Blind [AO00, BNPS02, BB00a, BSC01b, CL01b, GSK09, JKK+01, LY07, Na05, Pau02b, SPK08, ZP05, ZK02, Fan03, HC04a, JLL01, JLI04, LHY05, LC05b, MS09a, SV08a, SHT05, WHH05, ZC05].

blindness [AvdH00].

Blink [Sas07].

Block [AIK+01, BBC+09, BK06, BRS02, BR02, BSC01a, CvTMH01, Can01b, CLL00, CP02, CMB+05, Cro01, DR00a, Dwo03, EYCP00, Fhu02a, HSH+01, JKK+01, KCP01, KYHC01, KKG03, LLRW07, LRW02, MV00, MS02e, NPV01, OMSK01, Pat01, PS06, Pli01, RMS05, SM03b, SYY+02, SKU+00, SK10, WCJ09, XH03, YG01b, Bai08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kat05a, KJ01, LDH06, LCP04, LKH+08, MMJ05, PSP+08, RBB03, SHJR04, SHH07, WF02, XH05, YI00].

Block-Based [LLRW07, BBC+09].

Block-Cipher [BR02, RBB03].

Block-Cipher-Based [BRS02].

Block-DCT [BSC01a].

Blockcipher [GM02c, OS07].

blocks [Fur01].

Blocks [Joo02].

Blockwise [JM02].

Blockwise-Adaptive [JM02].

Bluetooth [GBM02, LV04, LMV05].

Blunders [Bur01].

Blur [VHP01].

Blurring [LSKC05, SK06].

Board [CBGS01].

body [DB04].

Body [Bam02, TG07].

BOEL [Fin02].

Boethius [Eag05].

bolstered [Ano01i].

bombe [Wil01a, Tur04].

Bombes [Ano01i].

Bonds [CAC03].

Boneh [ASK05, Hes04a].

Bonn [DRS05].

Book [And04, Duw03, Eag05, Eva09, Ful07, For04, Gas01, Gum04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pag03, Pap05, Ril02, Sal03b, Se04, 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 [Sal03b].

Boolean [Car02, CT03, CS09, MS02b, PQV05, SM00a, SM00b, SM03a, WV00].

Boomerang [KKS00a, KKS01, KML+02].

Boot [HSH+08a, HSH+08b, HSH+09].

Border [MJ07].

Borders [PGT07].

Boston [USE01b, USE01a].

bot [Ano08b].

Botschaften [Sch09].

bottleneck [WL02].

bottlenecks [HTW07].

Bound [CY08, DGN03, KMT01, HLLL03, hY08, GW00].
Chaining [BKR00, CBB05, PCC03].

challenge [LM08, LW05a, PRS04, Smi08].

challenge/response [LW05a].

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

Chang [CWJT01, ZC05].

change [CYH05].

Changes [Mur01].

Changing [BST03].

Channel [BU02, CHVV03, Law09a, LCK03, Mö02, NM005, OT03a, OT03b, Sch06a, SYLC05, ARR03, BP03a, BG07b, Buh06, CNPQ03, KSWH00, LCZ05b, MS09c, PSP +08, WL07a, YTWW05]. Channels [AIP01, CK02b, Nam02, Vau05b, LH04].

Chaos [JK01b, SK01b, WW05, KCJ +01a, LMC +03, McN03, PSG +09].

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

Chaotic [BCGH11, LLL +01, Mul06, SXY01, US02a, Vav03, AMRP00, AMRP04, GHdGSS00, GB09, HHYW07, HLwWZ09, JK01b, LMC +03, LYGL07, MAO2, PBMB01, PS01a, PZL09, SPG02, SL09, UHA +09, VKS09, WG02, WW08, kWPILW01, WLW04, YZEE09]. Chapman [Kat05b, Was08a].

Character [Gau02, Gauss06, KTO0, Ver02, GPS05].

Characteristics [RFR07a, RFR07b, RFR07c].

Characterization [AJO08, Nam02, XH03, BGM04, KY00, QVF05, XLM06].

Characterizations [Pas05].

Characterizing [BTW05, BTW08].

Charging [BAC02, RH02].

Chatter [Kee05].

Chauvin [BNPS02, KLN +06, WHH05].

Chauvinian [Mö03a].

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

check [Kir01b].

Checkable [BPST02].

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

checklists [Sha01a].

Checks [FM02a].

Checksums [Sto01, SGPH08].

Cheju [Kim01].

Chemical [EIG01].

Chen [LW05c].

Chennai [CV04, RD01, Roy05].

Chernobyl [Rie03].

CHES [Q04, KKP02, KP01, KNP01, RS05, WKP03].

CHESS [LKHL09].

CHESS-64 [LKHL09].

Cheswick [Che05b].

Chicago [ACM04b, Top02, Con00].

Chien [YRY05b].

Children [Pau02a, Sye00].

China [B +02, DWML05, FLY06, JYZ04, LTL +04, Li05, LST +05, ZJ04, ZYH03, Ano00c, TTZ01].

Chinese [LTL +04, Li05, Sch01b, CAC06, YKL03].

Chip [Ade09, BNPW03, DV08, MM01b, MM01c, MP00, Mit02b, Fox00, ISTE08, Ano04c].

Chip-Secured [BNPW03].

Chipkarten [Ano04c].

Chips [Ano00d, GP00, Pau02b].

Choice [Jam00].

Choquet [SH11, SM11].

Chosen [BCHK07, CKN03, CHJ +01a, CHJ +01b, CS02, CS03, DN02a, Des00b, DK05, FP01, IM06, JKS02, JJO0b, KS00a, KY01a, KJC +01, KMC03, KM01c, KL0a, Man01, Nov01, PV06b, Poi00, Sho00b, BW05, CHH +09, KG09, ZCW04].

Chosen-Ciphertext [BCHK07, CKN03, CHJ +01a, CHJ +01b, Des00b, DK05, FP01, JKS02, JJO0b, KCJ +01, KMC03, Nov01, PV06b, Poi00, CHH +09, KG09].

Chosen-Plaintext [DN02a, KM01c, KL01a].

CHW [CHC04].

CIA [Mah04, Ris06].

Cincinnati [BD08].

Cinematic [CAC03].

Cipher [AIK +01, BKR00, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DONS05, DF07, Dwo03, EYC00, FF01a, Fluo2a, GG05a, GBM02, HCJ02, H01, KYHC01, KHD01, LKH09, MSN07, NPC01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY +02, SYX01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BVP +04, GPX08, HAnR04, Hey03, KH08, Kid00, LKH +08, Mac00, PSP +08, RBB03, Sal00b, SHH07, WW08, Win05b, WF02, XH05].

Ciphers [AAG +00, BBKN01, BS00b, BR01, BK07, ČtvTM01, Can01b, CF01b, Can06b, CJ01, Chu02, CHJ02, CP02, CM03, Con03, DPV01, EAg05, Fil00, FF01a, Fil02, Gol01d, Gol01e, HR00, HR04a, HSH +01, Jam00, Jan06, Kan01, KCP01, KKG03, LRW02, MV00, 

D00a, DONS05, DF07, Dwo03, EYC00, FF01a, Fluo2a, GG05a, GBM02, HCJ02, H01, KYHC01, KHD01, LKH09, MSN07, NPC01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SYY +02, SYX01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BGP09, BD00a, BVP +04, GPX08, HAnR04, Hey03, KH08, Kid00, LKH +08, Mac00, PSP +08, RBB03, Sal00b, SHH07, WW08, Win05b, WF02, XH05].
Ciphertext [BBK03a, BCHK07, CKN03, CF01b, CHJ01a, CHJ01b, CS02, CS03b, Des00b, DK05, FP01, JKS02, JJ00b, KS00a, KY01c, LA01, LK01, LK01b, LK01c, LK01d, LK01e, LK01f, LK01g, LK01h, LK01i, LK01j, LK01k, LK01l, LK01m, LK01n, LK01o, LK01p, LK01q, LK01r, LK01s, LK01t, LK01u, LK01v, LK01w, LK01x, LK01y, LK01z, LK01aa, LK01ab, LK01ac, LK01ad, LK01ae, LK01af, LK01ag, LK01ah, LK01ai, LK01aj, LK01ak, LK01al, LK01am, LK01an, LK01ao, LK01ap, LK01aq, LK01ar, LK01as, LK01at, LK01au, LK01av, LK01aw, LK01ax, LK01ay, LK01az, LK01ba, LK01bb, LK01bc, LK01bd, LK01be, LK01bf, LK01bg, LK01bh, LK01bi, LK01bj, LK01bk, LK01bl, LK01bm, LK01bn, LK01bo, LK01bp, LK01bq, LK01br, LK01bs, LK01bt, LK01bu, LK01bv, LK01bw, LK01bx, LK01by, LK01bz, LK01ca, LK01cb, LK01cc, LK01cd, LK01ce, LK01cf, LK01cg, LK01ch, LK01ci, LK01cj, LK01ck, LK01cl, LK01cm, LK01cn, LK01co, LK01cp, LK01cq, LK01cr, LK01cs, LK01ct, LK01cu, LK01cv, LK01cw, LK01cx, LK01cy, LK01cz, LK01da, LK01db, LK01dc, LK01dd, LK01de, LK01df, LK01dg, LK01dh, LK01di, LK01dj, LK01dk, LK01dl, LK01dm, LK01dn, LK01do, LK01dp, LK01dq, LK01dr, LK01ds, LK01dt, LK01du, LK01dv, LK01dw, LK01dx, LK01dy, LK01dz, LK01ea, LK01eb, LK01ec, LK01ed, LK01ee, LK01ef, LK01eg, LK01eh, LK01ei, LK01ej, LK01ek, LK01el, LK01em, LK01en, LK01eo, LK01ep, LK01eq, LK01er, LK01es, LK01et, LK01eu, LK01ev, LK01ew, LK01ex, LK01ey, LK01ez, LK01fa, LK01fb, LK01fc, LK01fd, LK01fe, LK01ff, LK01fg, LK01fh, LK01fi, LK01fj, LK01fk, LK01fl, LK01fm, LK01fn, LK01fo, LK01fp, LK01fq, LK01fr, LK01fs, LK01ft, LK01fu, LK01fv, LK01fw, LK01fx, LK01fy, LK01fz, LK01ga, LK01gb, LK01gc, LK01gd, LK01ge, LK01gf, LK01gg, LK01gh, LK01gi, LK01gj, LK01gk, LK01gl, LK01gm, LK01gn, LK01go, LK01gp, LK01gq, LK01gr, LK01gs, LK01gt, LK01gu, LK01gv, LK01gw, LK01gx, LK01gy, LK01gz, LK01ha, LK01hb, LK01hc, LK01hd, LK01he, LK01hf, LK01gg, LK01gh, LK01gi, LK01gj, LK01gk, LK01gl, LK01gm, LK01gn, LK01go, LK01gp, LK01gq, LK01gr, LK01gs, LK01gt, LK01gu, LK01gv, LK01gw, LK01gx, LK01gy, LK01gz, LK01ha, LK01hb, LK01hc, LK01hd, LK01he, LK01hf, LK01gg, LK01gh, LK01gi, LK01gj, LK01gk, LK01gl, LK01gm, LK01gn, LK01go, LK01gp, LK01gq, LK01gr, LK01gs, LK01gt, LK01gu, LK01gv, LK01gw, LK01gx, LK01gy, LK01gz], Ciphertexts [AFI06, BGW05, BGN05, Gen04b, JG00a].
Complexity-Theoretic [CB01].

compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BSL02, Hei01, TEM⁴⁰⁰¹]. composability [PS04c]. Composable [AF04b, BOHL⁺⁰⁵, BLDT09, CF01a, CK02b, DN02b, DN03, NMO05, RK05, Can01a, CLOS02].


Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Computational [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Computational [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Computational [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Computational [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Computational [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kel02, LHS05, RS08, Sal07, SDFH00, WWL⁺⁰², WC03a, FS08, Gar04, La00, Lj05a, Sch00a, Sch01c, S⁺⁰³, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].
CGP03, CGH+00b, Cra05a, DUK05, DFCW00, DFP06, EBC+00, ELv01, FLY06, Fra01, FMA02, Fra04, FLA+03, HRO6, HYZ05b, IEE09a, IKY05, JYJ04, JM03, Joy03b, Jue04, KJR05, Kil01a, Kin02, KN03, Kn02, Lai03, Lee04b, LTT+04, LL04d, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Nac01, Nao04, Oka00, Oka04, Pat03b, Pem01b, Pfi01, Poi06, Pre00, Pre02c, RD01, Roy00a, Roy05, Sho05a, Sil01, SM07b, Sma05, Syv02, USE00c, USE00a, USE01b, USE01a, USE02c, Wil09, Won01, Wri03, Yun02a, YDKM06, ZJ04, Zhe02b, ZHY03, AUW01, BC05c, DV05, DWML05, DRS05, Hon01, Kil05, Li05, PC05a, PY05, PPV96, Q500, Son00, WK06].

Confidences [Gan01a]. Confidentiality [Dwo03, Pem01a, YC08]. configurable [MBS04]. Configuration [Sha02, Mos06]. Confirmation [SK00]. Conformer [CM00, GM03]. Coniscation [DBS01]. Conformance [LBR00, RSA00c]. confounded [Bel07a]. confusion [She01]. congestion [SBB05]. Congress [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. congruences [Ste08]. Congruential [CS05b, LS05a, SB05]. conic [LWL09, LCC05, LCZ05a]. Conjecture [CU01]. Conjugacy [CJ03a]. Conjugate [Ig02]. Connected [BJLS02, H601]. Connection [HR00, Jam00, Goo00, Mic02b]. Connection-Polynomials [Jan00].

Connections [WRW02]. Conquer [SKQ01]. conscious [DS09]. Consensus [CNV06]. conservation [Che05b]. Considerations [DBS+06, Hei07, Rub01, Sch07, SVE09]. Considering [WA07]. Consistency [ABC+05, JEZ04]. consistent [RG06].

Constant [App07, Bl05a, CS07c, CD01a, DP04, DN02b, DI05, Lin01c, Sun00a, IK080]. Constant-Depth [Bl05a]. Constant-Round [DP04, DI05, Lin01c]. Constrained [BCH+00, DBS+06, HS01b, MRL+02, Nit09, Zhe02a, Has00, RAL07]. constraints [CC05d, LPM05, SN04]. Construct [CDMP05, G01id]. 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, BR02, GMW05, GGT05, GM02c, Jun04, PR08, PZ02b, SNWX01, SM00b, GT00, GP08, IK03, IK06, NR04, PR05, Reg03, Reg04, vDST06]. constructive [GH+08]. consumption [Mis08]. Contact [YKMY01, Car00]. Contact-Less [YKMY01]. Contactless [And04, KS02, Cl00a, Fin03]. Contemporary [Ahm07, Opp05, SVE09]. Content [AAK09, CGJ02, HHJS04, MA00a, MA00b, RE02, XMST07, YK01, ATS04, DY09a, GSK09, SG07]. Content-adaptive [XMST07]. Content-Based [RE02, YK01, SG07]. Content-triggered [HHJS04]. Contest [Bar06b]. Context [DJLT01, FPS01, SN04]. continue [Lov01]. continued [Dan02]. Contra [Mah04]. contract [WK05]. Contrast [BDDS03, HS00, HT06, KS03, CDFM05]. Contrast-optimal [HS00]. Contrast-Sensitive [HT06]. Control [ABEL05, ANRS01, BW07, CGMM02, HC08, LY05, Sma03a, ZGLX05, BNP08, DFM04, DPT+02, HW03c, JW06, KNS05, LKZ+04, MD04, MSP+08, PS04b, STY07, WC01b]. Control-flow [ABEL05]. Controlled [GVC+08, IMM01, AW05, AW08, LAP08]. Controlling [HY03, MS03b, MS02d, WL05]. Controls [Har01a, Har01b, Ge03].

convenience [WDCJ09]. conventional [CJ04, YW05, YRY05b]. convergence [An04]. Converging [Pot07].
Conversation [GK04]. conversations [VAVY09]. Conversion [CDI05, Ket06].
Conversions [KIO1b]. Convertible [Chi08e, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b]. Convolution [PG05].
cookbook [VM03]. cookies [Cha05a]. Cool [An00d]. Coordinate [OS01].
COPACOBANA [GKN+08]. 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, XZ01, ZTP05, An01p, GI07, HLC07, KA09, Kwo03a, Ree03]. Core [BF00a, Dim07, DV08, HMS04, TPS01].
Corfu [SM07b]. Corner [Mar08a, TR09a, TR09b]. corners [Bhu09]. Corporate [HW01, KH03]. Correcting [MZ02, NN06, YYDO01, ZYR01].
Correction [BQR01, CTBA01, Din05, LN08, LW05b, MPSW05, SKQ01, TEM01, Gar04].
Correctness [PBD05, Bel07b, HSD05, dH08]. Correlated [FWW04]. Correlation [BSC01b, CS01c, JJD04, LV04, LMV05, MH04, Nyb01, SY01a, WRW02, ZC00, GG05b, JJ02].
Correlations [KM00, KM01b]. corruption [XNK05].
COS [FF01a, WB02]. Cost [CDF01, FBW01, PD07, Sta05, YEP06, CL09, SHJR04, SK03, YLR05].
Cost-Effective [PD07]. cost-ineffectiveness [YL05]. Could [Min03, Cla00b, Pau02b]. Count [Che07b].
Counter [DIS02, QS01, SLG05, SL06, MMJ05]. Counter-Measures [QS01]. Countering [PP06b, SK05b]. Countermeasure [IT03, MMT09, OT03a, PKBD01, YKLM02a].
Countermeasures [Ava03, Fry00, GM00b, MOP06, OST05, Has01b, JDJ01, Man08, OST06]. Counters [KMO01]. counterterrorism [Nac05].
Counting [Gau02, Kuh00, Hig08]. Couple [SXY01], coupled [LF03]. course [AA04b, GV09, GL05]. courses [Gha07].
Cover [GA05, Gut02a, LNP02, NN03, RS00].
coverage [DS00]. coverings [SC02b].
Covert [Col03]. Cozens [Sal03b]. CPCMS [Sha02]. CPI [ECG07]. CPN [AADK05].
CPOL [BZP05]. CPUs [ESG05]. Crack [Sin02, Ayo08b, Min03]. Crackberries [Sta05]. Cracked [AAG00, Nic01, Pri00].
Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZ01, BZ03, Cur05]. Crackproof [Sal03b].
Crack [Sin02, An08b, Min03]. Crackberries [Sta05]. Cracked [AAG00, Nic01, Pri00].
Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZ01, BZ03, Cur05]. Crackproof [Sal03b].
Crack [Sin02, An08b, Min03]. Crackberries [Sta05]. Cracked [AAG00, Nic01, Pri00].
Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZ01, BZ03, Cur05]. Crackproof [Sal03b].
Crack [Sin02, An08b, Min03]. Crackberries [Sta05]. Cracked [AAG00, Nic01, Pri00].
Crackers [Ols00, SEK01, SEK02, NRR00]. Cracking [DZ01, BZ03, Cur05]. Crackproof [Sal03b].
CP02, Cou04, CGJ+02, DG00, DGP07a, DGP07b, DGP09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Fin06, Fhu02a, Fhu02b, Fur01, Fur02a, Fur02b, G07a, GM02a, GJSS01, GS02c, GM02b, GM00b, GBM02, GC00b, Gra02a, GS09, GKN+08, HPC02, HQR01, HAuR04, Hen06a, HLL+01, HSM+02, HHK+04, Hsu05a, HLL00, Hwa00, JK02a, JJo0c, JJo1, JmBDxGxMn05, Jou09, Joy03a, KM02, KW03, KS00b, KRY05, KW02, KRS+02, KKS00b, Kra02a, KC05, Kuh01, Kuh02b, KKL05, LC03, LHL+02, LP03, Lee03c, LKY04, LL05a, LR07, LBGZ01, LBGZ02. Cryptanalysis [LLH04, LL05c, LLCL08, LW05c, MS03a, May02, MG01, MHL+02, Mor05, NPV01, Nit09, PSC+02, PKH05, Pei04, Pei06, Pha06, PS06, PS01c, QCB05a, Sch06a, Sco04, Sha03c, Sha05a, STK02, SG01, SK01, STH07, TIGD01, TM06, TLH05, TJ01b, TSS+03, Wag00, Wag03, WLT03, WL05, WBD01, WBO2, Wu02, XwWL08, XY04, YSD02, YW04b, YW05, YKLM02a, YKL01, YRY05a, YY05a, You01, YG01a, YG01c, ZYR01, ZKL01, ZC05, ZK05, ZF05, ZC09, dW02, AMRP04, BF01a, Bao8, Bar09, BS01c, Buh06, Buo9, Bur02, CV05, CKN06, CLK+03, Dun06, Egh00, EBS01, Eke09, Fie09, GPG06, Goo00, Jun05, KewH00, Kuk01, LMSV07, Max06, MAaT03, MAaT04, MAaT05, MAaT06, MAaT07, Nyb01, Pha04, RSQ03, Rup09, SK01a, Se100, Sin09, SL07, SCS05b, SSL+00, Swe08, TC00, TM01, WLW04, WF02, YI00]. Cryptanalyst [YJ00, YKL03, Kat05b].

cryptanalysis [YJ00, YKL03, Kat05b].
cryptanalyst [Wil06]. Cryptanalytic [BS00b, KFSS00, Oec03, QSR+02, Yan07, Wil01a]. Cryptic [Wri05, Ano03b].

CRYPTIM [Us10b]. CRYPTO [Fra04, Men07, Sho05a, Alm08, Ano01a, Ano03b, Bau01a, Bau01b, Bur01, CCM01, CNB+02, Gen01, Hil05, Lev01, Lev02, Mad00b, Mar08a, Mar02b, MC04, Mur06, Pal02, Pem01b, SYLC05, TR09a, TR09b, Ymu02b, Ano01e, Ano01k, Ano01m, Bec02, BK05, HGNS03, Mad00c, Mat05, Pot05, Web02, Bel00, Bon03, Kii01a, Ymu02a, Sei00a].

Crypto-algorithms [An001n, CCM01]. Crypto-based [MC04, Crypto-CCS] [Mar02b]. Crypto-integrity [Yun02b]. Crypto-systems [Ano01n, CCM01].

Cryptoanalysis [HSIR02, LD01]. Cryptography [Jon03, Nac04, Poi06, Pre02c, Men05]. Cryptographers [Coc03, Heg09, KLN+06, Tsa07, Bel07a, Hau03].

Cryptographic [AC02, AADK05, AL00a, Ano09d, ADH+07, Ase02, BLST01, BDF+01a, Bar00a, BGK+03, Bih03, Bla01a, Bor01, BDP02, Bra01b, BM01c, BL08, Bur06, CC04a, Can01b, Car02, CCD01, CHL02, CKY07, CB01, Cral05a, CS09, CO09b, DD02, DHR07, DM04, DS00, DWN01, DHR00, DV08, DFG01, FJ00a, FSS00, Fis01a, FGM00a, Fri01, GMP01a, Gar05, GSS08, GGKT05, Gol01d, GK02, GTH02, Gor02a, GL00, GUQ01, Gut00, Gut02b, Gut04a, HTS02, HN06, Har06, Has01a, HL05a, HC08, Igl02, IY00, Ito01, IMM01, J05, K001, KY01b, KY02b, Kii01b, KS06a, KSC09b, Kmo02, Kus02, Lau09a, LN08, LS05a, LKJ01, MS02a, MOP06, Mea01, MN01, MRL+02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Nao03, N0d05, Ngu05, Nie04, OTIT01, OP01a, PKB01, PR08, PZ09, Pem01b, Pfi01].

Cryptographic [Pin02, Pin03, PS02b, Pot06, Pre00, Pre02a, Pre02b, RSA00d, RSA01, RR00, RRS06, Rot01, RSN+01, SM00a, SS01a, SG09, Sha02, Shp03, Shy02, SDF06, SVW00, SR06, SL09, TLY04, TWA08, TBD01, Uzu04, WKP03, WN02, WBL01, WC01b, You01, Zha08, AMRP04, ACTZ05, ALV02, AV04, GB09, BDSV08, Bla01b, BP05, BG08, BG09, 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, KSF00, KS05b, KP03, LGKY10, LMTV05, Lau05, LLW05, LLW09, ML05, Mea04, MT07, Mic02b, MRS06, MN03, ND04, ND06, PS04a, PSH05, PR05, Pre07, Pri00, Puc06, QPV05, Reg03, Reg04, Ren09].

Cryptographic
[RMH04, RB08, RAL07, RSS04, ST03a, SV08a, SOIG07, SW00b, TNG04, kWpLwW01, LW04, XLM06, VT06, ZL99, ZWWL01, ZL04b, dH08, BWBL02, JQ04, KKV02, KP01, KP40, KN01, RS05].

Cryptographically
[ADD09, AHS08, BJ02, BCGH11, BFCZ08, BB00b, FR08, MS02b, PLVdLE10, RGX06, Aam03, AW05, AW08, Lau08a, SM03a].

Cryptographically-masked
[AHS08].

CryptoGraphics [CK06], cryptographic
[RSA09a, Cryptography
[ANS05, AF04b, AL09, AA04b, A00c, A001], Ano02b, Ano02f, Ano02h, Ano04b, Ano05a, Ano07b, AAFG01, AI04, AI06, App07, AE05, AB00, BA10a, 10b, BIN03, BD04, BOV03, BOV07, BBGM08, BM01a, BR00a, BY03, Ber00, Ber03, Bi08, BWBL02, Bla02, BDD03, Bon00, Bon07, BPR01, Boy03, BLM00, BK06b, BK07, Bu00c, BD08, BO01b, BRT09, CPS07, C04b, CL09, CSW^08, C01, CPD06, Cob04, CFA^06, Cop00, Cor06, Dc00c, Dam07, DFS08, DFS05, Das08, DD00, DFGH04, DK02, DK07, Des02, DT03, DY09b, DSO0, DND00, DND03, Dme00, DP08, EPP^07, EP05, Elb09, Elh04, ECG^07, Ett02, FS03b, Gal01, Gal02, GHK^06, GKK^09, Gen06, GS02b, GH02, G01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Gri01, Gro05, HR06, HH04].

Cryptography
[HHM01, HM04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irw03, IK05, IK06, IYK02, IYK03, JW01, KAM08, KSF00, KS05b, KP03, LGKY10, LMTV05, Lau05, LLW05, LLW09, ML05, Mea04, MT07, Mic02b, MRS06, MN03, ND04, ND06, PS04a, PSH05, PR05, Pre07, Pri00, Puc06, QPV05, Reg03, Reg04, Ren09].
Sti11, SK01b, TW05, UHA+09, Van03, Vau05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wei03, YC09a, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Ree01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08, Ros06b.
cryptography-based [FXAM04].
Cryptologic [Lew00]. 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, Sma01, SCL05, SUN02, SZP02, Taj01b, Tj01a, V001, Was08b, Wen03, YC09b, YC09a, YC09b, YZ01, vT01].
cryptovirology [YY04]. CRYPTREC [IY00]. CSCW [ZP05]. CSP [SB09]. CT [Joy03b, Men05, Oka04, Poi06, Pre02c, ZC09]. CT-RSA [Joy03b, Men05, Oka04, Poi06, Pre02c, ZC09]. CTO [Ano03g]. CTS [Con00]. Cuban [AJ08]. Cube [DS08, PDMS09]. Cube-Type [PDMS09]. culture [Gil07]. Cumulative [LG04, WP03]. cure [RD09]. cure-all [RD09]. Current [Ano03b, DFH01, PRS04, LPW06]. curriculum [FOP06]. Curve [ANS05, AD09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BBWL02, BS01d, BM01, CQ01, CFA+06, GPP08, HY05a, HBM00, HM02c, JT01b, JT01a, KBM09, KPMF02, KSZ02, KWP06, LW02, Möl02, Kir03, OTIT01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YZ01, ZLK02, BSS04, BSS05, BGM04, BG07a, CCH04, Che06, CFV06, CH01, Dan02, DHL06, EKRMA01, GHG00, GS01, G00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04c, LL06, LKYL00, Lo01, LS01c, OP01b, Pae03, Poi00, SPG02, SCS05a, SP79, SLC05, Sun00b, Sun02, SZP02, TJ01b, TJ01a, VS01, War00, YC09b, yH08].
Cryptosystems [Aki09, Ava03, BDG+01, BKLS02, BPS00, BM00, CHSS02, CCW02, DDG+06, DKK802, ESG+05, FJ03, Fe06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KKY02, KI01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vad03, Wya02, XB01, ZLK02, Ban05, BF06a, BB79, CHC01, CMKT00, EBS01, EH01H04, GH08, GBK01, HM00, Has00, Has01b, Hül00, HP01, KW00, Kos01c, LL04b, LD01, Luk01, Mic01, Mis06, OS00, Pei09, PLJ05b, SSST06, Sha05c, Sma01, T001, TC05, Ts05, Ver01, Why05, Wol04, WPP05, WV00, Y001, ZSZ01, vT01].
cryptography [Yang04]. CRYPTREC [FY00]. CSCW [ZH05]. CSP [SB09]. CT [Joy03b, Men05, Oka04, Poi06, Pre02c, ZC09]. CT-RSA [Joy03b, Men05, Oka04, Poi06, Pre02c, ZC09]. CTO [Ano03g]. CTS [Con00]. Cuban [AJ08]. Cube [DS08, PDMS09]. Cube-Type [PDMS09]. culture [Gil07]. Cumulative [LG04, WP03]. cure [RD09]. cure-all [RD09]. Current [Ano03b, DFH01, PRS04, LPW06]. curriculum [FOP06]. Curve [ANS05, AD09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BBWL02, BS01d, BM01, CQ01, CFA+06, GPP08, HY05a, HBM00, HM02c, JT01b, JT01a, KBM09, KPMF02, KSZ02, KWP06, LW02, Möl02, Kir03, OTIT01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YZ01, ZLK02, BSS04, BSS05, BGM04, BG07a, CCH04, Che06, CFV06, DIM08, DwWmW05, EHK04, GBK01, Has01b, Has05a, HL05d, JM09, JW06, LL04c, LWL09, Mis06, OS00, ST03a, SSST06, SH05, Sma01, SCL05, SLC05, TC05, Van03, Ver01, Wol04, WPP05, Y009a, YC09b, ZSZ01, Z05, vT01].
Curve-Based [KWP06, Pel06]. Curves [AHR08, Bao01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK+06, Kid02, PWGP03, Ver02, CMKT00, Hul04, LWZH05, MP01b, MS04, Sil05, Sim02, SC02b, Was08a, Wen03, Yas08].
customer [Lin01b]. CVS [DFG01]. Cyber [FNRC05, WW04, Mad00c, Mau05].
cyber-crime [Mad00c]. Cyberinsurance [BP07]. Cybersecurity [PLW07].
cyberspace [Mit02a]. cycles
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, DGO5, LC05b, YRY05c, Zha06]. Denial [Mah04, Nik02a, Nik02b, PKBD01, Ril02, Mir05]. Denial-of-Service [Nik02a, PKBD01]. Denmark [Cra05a, TBJ02]. Denver [ACM01b, Sch04b, USE00d]. Department [Bol02, Eri01]. Dependable [NABG03, And08b]. Dependent [Gol03, WS05, BP08, 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 [Egh00, EBS01]. Desch [LBA00]. Describing [PS06]. Description [Lav06, MH05]. Descriptors [DN07, SP04]. Design [Abd01, AADK05, Ano02e, ADD09, AIK+01, ARC+01, Bar00b, Can01b, CDP01, Cim02, CB01, CSS02, CMB+05, CL02, DR02a, DR02b, DS09, DFO7, EHEK+03, FF01a, FZH05, GSS04, Geb04, Gut02b, Gut04a, HRL09, Hro05, Ken02b, KB09, KDO01, Lan04a, LCP04, LL04c, LB05, MKP09, MP00, Nd05, NSS02, Rho03, SJT09, SPG02, SRQL03, Uzu04, WZW05, WW08, WLLL09, ARJ08, Ade09, CMS08, GGO5b, Gut04c, HC04a, Hut01, KSF00, MI09, MWM01, SVEG09, YCW+08, YC08]. Design/CPN [AADK05]. designated [LV07]. Designing [HBC+08, MRT10, TCR03, C+02, CG05, Lan00c]. Designs [Bec05, CC02a, Bli08, Des00a, WL07a]. Desktop [Mon08, BDE00]. Desmedt [CHH+09]. Desynchronization [CDT05]. Detached [Sha01c]. Detailed [Lut03]. Details [Scr01]. Detect [FOBH05]. Detecting [CMS09, FGD01, JQYY01, Har07a, LHL04a]. Detection [AS01b, AD07, BB00a, BM07, CH01b, CZK05, JT05, KKG03, SKQ01, SY01a, SL01, ST01c, TZZD05, TMM05, WG05, YL01, Zan01, Bej06, BBK+03b, HLL+02, Men03, NN02, WMS08, YW06, ZG05]. 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, Cra05a, 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, WPS01]. Devices [BCH+00, CFR02, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KHD01, MV01, MRL+02, SCF01, WC01a, Ano06a, CMS08, CF07, DMT07, sHCP09, Tse07, YC09b, ZYW07]. Devil [Bla01c]. DFT [Che08a]. DH [Lys02]. DHIES [ABRO1]. DHP [MSV04]. Diablerets [Vau05a]. Diagnosis [Ano04b, BK06b, XNK+05]. Diagnostics [NM09]. Diagonal [PJH01, PJK01]. Dickson [SZP02]. Dictionaries [AGT01].
Dictionary [BPR00, BCP02b, CS07b, DJ06, Pho01, NS05a, did [MH09]. Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b]. Dies [Bar00a, Coc01a, Mat05], difference [PBMB01, dW02]. Different [LS08, WWTH08]. Different [CGMM02, Sma01]. Differential [Ava03, BMM00, BF00a, BFM02, 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, MKY08, NRR00, PC05b, PLJ05a, PBV08, QCB05b, Reet03, Sha01b, Sha04b, Sha05d, SCL05, TCC02, TND+09, UP05, WNQ08, WHL03, WC05, XC05, XMST07, Ano09b, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02]. Digital-Audio [WNY09]. Digital-Signature [Eng00]. Digits [Che04b, Ran55, Ran01]. Dimension [DDG+06, TTT09a, TTT09b]. Dimensionality [SBG02]. dimensions [CLR09]. Dining [KLN+06]. diplomacy [Alv00]. Direct [BMW05, KG09]. directly [PJK01]. Directions [Sha01b, DFH01]. 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, SGA07]. discretizes [An009c]. Discrete [CS03a, CNS02, Che04b, CCA02, Gen00b, GV05, GPP08, KC09b, LW02, JLJ05, VK07, HN04, HW03a, HWR09, Hsu05a, HLL+05, JL03, JLL01, LH03a, LL4b, LH05, PLJ05a, QCB05a, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SLH05, SCS05c, YAS08]. discretized [MA02]. Discretion [Har07b]. discursive [Mit02a]. Discussion [An01a, An01b, An01c, An01j, An01n, An01f, An01o, KLB+02a, Mal02, Nik02b]. dish [An01]. Dishonest [GKK007]. disjoint [Gut04c]. Disk [Cro01, Har07b, Siv06, CS08a, Fer06].
dismantles [Hil06]. dispatches [Kee05]. displayed [CGV09]. Displays [Kuh02a]. Disputed [CAC06]. Distance [CGFSFH09, CPXH04, DM07b, DW01]. distinguished [HHW04, WH02b]. Distinguishing [HSR+01]. Distortion [BG08, CS05c]. Distortion-Free [BG08]. Distortions [HH09, SF01]. Distributed [BC502, BT02, CLK01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJKR03, GSCV02, GTH02, LLY06, SCF01, WT02, And08b, AFGH06, BDET00, CO09b, FMY02, KKL09, LN04, LLW08a, MSP08a, Ra06, WZB05, YbJ04]. Distribution [BDF+01a, BOHL+05, BBB+02, BGM09, BSNO00, FS01b, Ina02a, Ina02b, Ku02, LLL02, NA07, Sch01a, YI01, ATS04, As08b, Bad07, CYH04, CCD06, GL06b, MP08, SLP01, Sh01b, Sh04b, SY06, WHHT08, YS04, ZL01]. Distributions [CY08]. Diversity [Kun01]. Divide [SK01]. Division [HZLS05, KKY02, Tan07a, Che08b, MN14]. Divisor [KM01a]. DL [HRL09, PL05b, Sch01f, Sch01e, WMDR08]. DL-encryption [HRL09, PL05b]. DL-keys [Sch01e]. DL-STD [WMDR08]. DLP [MS04]. DM [Eag05]. DNA [AEH17, GXP08]. DNF [BG05]. DNS [Her09b, Kl07]. DNS-based [Her09b]. DNSSEC [Gue09]. Do [Bar06, HSR+01, HR04b, Win01, BB79]. Dobb’s [Dr.00c]. Document [ISO05, PWH01, VHP01, CDS07, CL04c]. Documents [PJK01, AW05, AW08, DGK+04, GA03, ÜG08]. dodging [Phil06]. Does [AB01, Pie05, Con09, Wal04]. Doing [BM01a]. Dolev [BPS08, BDNN02, ZD05]. Domain [AS08, Bar00b, BSC01a, BSC01b, BSL02, CJK+04, Cor00b, Cor02, DOP05, DNP07, GW01, ISSZ08, Kuh02a, Lan00d, Lz01, MM01a, OMT02, PBC05, SOHS01, SFH00, ZLK02, BR06, CS05a, DSP01, EKRMA01, Zir07]. Domains [BR01, CLK01a, CLK01b, Vau01]. Domingo [CKN06]. Dominic [Rot07]. Dominica [PY05]. domino [LLLZ06a, LLLZ06b]. don’t [Win05c]. Don’ts [FSS01]. DONUT [CLL00]. Door [SF07]. Doors [Eri02]. DOS-Resistant [An01f, AN01]. Double [ADD06, CY08, CMJP03, Cood2a, DIM08, GH08, GB09, Hau06, JSW05]. double-base [DIM08]. Double-Gate [Cood2a]. Double-Size [CMJP03]. double-trapdoor [JSW05]. Doubling [FV03]. Douglas [Spr03]. Down [BBPV00, Coc02b, An00g, An03d, An03a, Pot03, PVB01, Ste05c]. Downwards [FV03]. DPA [SGB01, TV03]. DPA-Based [SGB01]. Dr [An03g]. Dr. [Dr.00c]. Draft [Mad00b, Ste00, Dwo03]. drastic [Sug03]. drawn [vOT08]. DRBG [Hir09]. Dress [Ahm08]. drinks [An03d]. Drive [NP07, Kor09]. DSA [MR01a, SA02, Sha01d, TvdKB+01]. DSA-type [Sha01d]. DSEA [LLLZ06a, LLLZ06b]. DSP [Geb04, WWGP00]. DSP-embedded [Geb04]. DSPs [WWGP00]. DDS [An09b, An013, FIP00, Nat00]. DTD [PCK02]. Dual [HLC07, KHY04, LKK05, SF07, WC09, ST03a]. dual-field [ST03a]. Dual-Pair [WC09]. Dual-Tree [LKK05]. Dual-wrapped [HLC07]. Dumb [Eri01]. Dummies [Cob04]. Dump [KCJ+01]. Dunaynir [MAA05]. d'une [Car00]. Durahim [MAA04]. Durahim’s [MAA04]. during [A08, Bec02, WA07]. Dust [KGS07]. Dutch [dl00]. Duty [ZGLX05]. DVD [Ge03, Per05b]. Dwork [DNRS03, GK05, Zha06]. DWT [LHS05, PBC05]. DWT-Based [LHS05]. Dynamic [AFB05, BNP08, BCP01]. BCP02a, BFM07, CL02a, CW09, CCD+04, CTT07, GTH02, HQ05, Pat01, Sug03, TT01, BBG+02, GL06b, HW03c, LCP04, LLY06, LCK04, LCC05, RG05, Yi04]. dynamic-key [LCP04]. dynamics
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, KS00a, Law05]. e-mails [LG09]. e-payment [Has02]. E-Security [NDJB01]. E-smart [AJ01b]. E-Vote [Che07b].
e-voting [CJT03, Cha04]. E-Wallet [ETZ00]. E0 [LV04]. E2 [SKU00].

Early [ASW01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Cal00d, Smo04, ZGTG05].

Easier [Pau09]. Easy [GR04, Hos06b].

Eavesdropping [Kuh02a, Kee05].

ebanking [WDCJ09].

Economics [Ble07].

ECP [Che03]. ed [Gum04, Nis03a]. Edge [Sta05].

Edinburgh [R505, Pen01b]. Edit [CGFSHG09]. editing [MAaTxx]. Edition [Cho08a, Irw03, Spr03]. Editor [MFS+09, Sak01, KP03, SK06].

Editorial [Eri01, Eri02, FOP06]. Editors [BK06b, PTP07, SJT09, SGK08].

EDK [Ano02e]. Eds [Dwu03, Pag03]. Education [Puz04, RC06, CAC03]. Effect [AEV+07].

Effective [CDR01, PD07, Sen03, SL06].

Effects [BBGM08, Har00, GJ04, SN07].

Efficiency [IIH00, GGKT05, SLG+05, GT00, GGK03, KT06, YTH04]. Efficient [ACS02, ABRW01, AEW00, BCGH11, Bai01b, BNP03, BKLS02, BR00a, BGHP02, BDSV08, BGK+03, BS00a, BF01c, BGH07, BB00b, BCDM00, CKPS01, CL02a, CCMT09, CCD07, CL01b, CPhX04, CM05a, CJT02, Chi08a, CJK05, CT08b, CKK03, Cou01, Dam00, DN03, Dhe03, FF00, Fis05, FS01c, GLV01, GC01b, GT02, GF04, GBK01, HCK02, HSSZ01, HAS01a, HS00, HW04, HZSL05, HL07, Hii00, HS07, Jua04, KOY01, KLY02, KO03, KH01, KKH03, LSY01, LCK01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, MN14, Nd05, NSKN05, OS01, PCS03, PBD05, Ram01, RSQ03, RDC+01, SM01, SM03a, SW06, SRL03, SSNS00, Tsa08, TC05, WH05, WYY05d, WHI01, WC01a, X03, YWD08, YLD05, Zan01, Zho06, ACTZ05, AFB05, Bla01b, CC04b, CC05c, CY05, CHC05, CL08, DS09, Dew08, DwWm05].

Efficient [FP09, FSGV01, HHG06, HC04a, JW06, KHYM08, LPV+09, LLS+09, LCK04, LLH04, LYY02, Mic02a, MSP09, NR04, PCC03, RG05, RBB03, SLP07, SKW+07, Sha05b, SC05a, W05, X05, Yan02, YT05, YC09a, ZSN05, ZYW07].

Efficiently [IKNP03, NNT05, AGK07].

effort [Wei06, Wei05].

EGPGV [MFS+09].

Egypt [EBC+00, Imr03, Sin00].

Eighth [ACM06, B+02, ELvS01, IEE01b].

Einstein [HR13, MNT+00].

EJB [TEM+01].

Ekert [Duw03].

El-Gamal [EKRMA01].

Election [JLL02, Cal00b].

Elections [Cha04, PvS01].

electrical [Wal04].

Electromagnetic [SGM09, QS01].

Electronic [Ble07, CLK01b, CM02, Dur01, H0f01].

ISO05, IY00, KMO01, KS02, LLL02, Mad00a, MNFG02, Rub01, RMCG01, Str01a, YKMY01, ZYM05, AvdH00, AAK09, Cal00a, Cas03, EY09, FB01, HJW05].

element [MS02d].

Elementary [Sin09, Ste08, Tat05].

Elephant [Fer06].

Eleven [All03].

ElGamal [BJN00, CL02b, CWH00, HL04, LHT09, SJ00].

ElGamal-like [CWH00, HL04].

Elizabeth [Bud06].

Elliptic [AD09, Ano05a, Bai01a, BNP03, Bar00a, BBGM08, BM00, BS01d, BMN01, BB00b,
CQS01, CFA+06, GLV01, Gau02, GPP08, HYZ05a, HHM01, HMV04, HM02c, Hus04, JT01b, JT01a, KBM09, KPM02, Kid02, KSS02, LW02, MP01b, Möl02, Kir03, OTIT01, OS01, OT03b, PWGP03, RSA03b, RS04, RS01, Sat06, Sil05, Was08a, Was08b, WP01, XB01, YYZ01, vT01, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHKH04, GBKP01, Hsu05a, HL05d, JMV09, JW06, LL04c, LWZH05, Mis06, MS00, ST03a, SSST06, SH05, Sim02, Sma01, SC02b, SCL05, SLC05, TC05, Van03, Ver01, YC09a, YC09b, Was08, ZSZ01, ZL05, ANS05, BWBL02].

Ellis [Coc01a]. Elmau [IEE01b]. Else [FL01b]. elude [Che01f]. EMA [QS01]. Email [ES00b, Gar03a, Her09b, Luc06]. Email-Based [Gar03a]. emanations [ZZT05].

Embedded [Ano01c, Ano02d, Ano02e, BBGM08, Dri02, DV08, GSS08, JT05, JQ04, KKP02, LPW06, NdM04, RS05, SPGQ06, WKP03, YSS+01, ARJ08, BGM04, Fox00, Geb04, KV+09, KP01, KN01, KP03, MB04, Nis03a, TKP+08, XQ07, Fin02]. Embedding [AAK09, JX05, JG07, LSC03, Sal03b, WY05, WC04, CO09a, KC09a, Wan05]. Embrace [CJ02]. Embracing [Ano03d]. EMD [BR06]. Emperor [Sn00]. Empirical [HW03b, Goo00]. empirically [SS03].

employee [You04]. Emptiness [DIS02]. Emulex [CZB+01, CTBA+01]. Enabled [Por06, CACY01, DY09a]. Enabling [Web02]. encapsulation [CH+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, CD01b, Hug04, Lan04a, LH07, MMZ00, NNAS01, RMCG01, St02b, Vau01, WRW02, Whi09, Woo00, AMB06, Ano06a, Bib02, BN08, CCMT09, CDD+05, CSK+08, FJ04, HLM02, Hes04a, LHL04b, LSH00, MW04, Pet03, ÜG08].

Encryption [Pro00, RC01, Zho06].

Encryption

[ABC+05, Abe01, AS01a, Abe04, AEH17, AP09, AB01, ADR02, And03, Ano01g, Ano01h, Ano01i, Ase02, AN01, AFI06, AF03, Bar00c, III00, Ban02b, BN00a, BR00a, BBM00, BBD01, BU02, BF01b, BF03, BB04, BGW05, BCK07, BGF07, BPR+08, BB03, BNP03, BD03, BKY02, Bur03, Cal00d, Cal00e, CD00a, CS03a, CHK03, CHK05, CGHG01, Che01a, CTL01, Ch08e, Cho08a, CM06, CLo0a, Coo0b, Coo1b, CJNP00, CHJ+01b, CD01, CS02, CS03b, Cor01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL08, DR02d, DA03, DK03, DK05, DS05b, Dri02, FIP01a, FL01a, GC01a, GSW00, Gen03, GRW06, GH05, GD02, GMM01, Gutxx, HS08a, HS02a, HY05a, HSHI02, HSHI06, HRR01, HWW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03].

Encryption [HL02, HGN+03, HLL05, HLC08, ISSZ08, Jol03, Jol01, JK02b, JK02c, JMV02, JKRW01, Jut01, KBD03, KSHY01, KS00a, KY01a, Kha05, KK+07, Kos01a, Kra01, Kur01, KD04, Lai07, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LLRW07, Lim03, LNP02, LM05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, Möl03a, Mor05, Mü01a, MS09d, NIS00, Nam02, NZC05, NZS05, NP02b, Nie02b, PV06b, PM00, Pau09, Pena01a, PZL09, PDM09, Pho04, Por01, PS00, Pre01, RM04, RK06, RDJ+01, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQ03, SPQ06, SB02, Sye00, TV03, U00a, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Ust01b, VMS05, WZW05, WBRF00,
Wri01, YEP⁺06, YW06, ASW00, Abd01, ABHS09, AJSX04, AMRP00, ABW09, Ano00e, Ano00c, Ano00f, Ano00g, Ano00h] Encryption [Ano00j, Ano02a, Ano03g, Ano06d, App05, Ade04, AcdM05, AFGH06, BPS08, BKN04, BR04, BBN⁺09, Ber09a, BBK⁺03b, Bir07, Bla00, BJN00, Bro05b, CG06, CS08a, CBU06, CHC01, CKRT08, DL07, DRS05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GGK03, Gen09a, Gen09b, GKM⁺00, Gou09, Gua05, Gut04c, HSH⁺08b, HSH⁺09, HHYW07, HCD08a, HCD08b, HAU04, HWW02, Hsu05a, Hwa05, HL05c, HLU05d, IM06, JK01a, JK01b, JW05, JSW05, JZC05, KY00, Kl01, KSW06, KHL09, Kor09, KW00, Kre05, Kühr08, Laa00, LB04, LCP04, LJ05a, LMC⁺03, LLZ00a, LLZ00b, LLZ08, LB05, Lu02, Lu05, LK01, LWK05a, Mad04, Mar05b, Mat02, Mü01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pan03, RG09, Rhi03, RBB03, RSP05, SN100, SKW⁺07, Sch00a, Sch01c, S⁺03, Sch04a]. 

Encryption [Sch04b, Sch05a, Sch01d, Sch01f, SH11, SM11, SR00, SVEG09, Shp04b, SK03, Ste00, SP03, SWH⁺09, Tan01, TTZ01, TOEO00, TM01, TLI05, Un00b, UP05, VK05, WGO2, Wei00, WN95, Wol03, WHO2a, XY04, XSWC10, Yan02, YGO2, YZE09, YC07, ZLG01, Zuo04, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CKKO08, CHJ⁺01a, RR04, Un00f, Wue09, Jan08a]. 

Encryption/cipher [HAU04]. 

Encryption/decryption [OS07]. 

Encryptor [LMP⁺01, TPS01, Ano00a]. 

Encryptor/Decryptor [TPS01]. 

Encyclopedia [Bid03, vT05]. 

End [KCD07, Per03, SKK00, WWGP00, YSR01, AMB06, SU07]. 

End-to-End [YSR01, AMB06]. 

End [Küs02]. 

Endomorphisms [GLV01]. 

Endpoint [Kad07]. 

Energy [GCO1b, Ino05, LPV⁺09, SL07, Mis08]. 

Energy-efficient [LPV⁺09]. 

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

Enforcement [GN06], enforces [BP05]. 

Enforcing [GMM08, HRS08]. 

Engine [Fri01, MHH02, DP04, SL07]. 

Engineering [CBN⁺02, MNT⁺00, MYC01, Pem01b, Roy00b, SM07b, TR09a, VR09b, VH09, Ano08b, EC05, Jun09, Man08, Wal04]. 

engineers [Pri00]. 

engine [PM08]. 

Enhance [ZWC02]. 

Enhanced [JRW01, LHL04b, ZGLX05, CZ03,McK04, OP01b, TW05, WLT03, WNN05, ZSM05]. 

enhanced-security [OP01b]. 

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

Enhancements [ADH⁺07]. 

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

enigma [Rob02, Rob09, BC05, Cas06, Chu02, Cop04b, DB04, GO03, Goo00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Th03, Wil01a, Win05b, Win00]. 

Enigma [Kap05]. 

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

Enrolment [HHW01]. 

Entangled [Bar00c, LB04]. 

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

Entropic [DS05b]. 

Entropy [DS05b, EHS00, LH07, JS09]. 

Entzifferung [Bau08]. 

Environment [BST03, Del07, HS01b, LSVS09, IM06, KKL09, KB00, Rhi03, W09, ZBP05]. 

Environmental [PS05]. 

Environments [CJ⁺04, LKHL09, BGM04, MNS08, SBG05, SBG07, SN04, YC09a, YbJ04]. 

ephemeral [Mis08]. 

Ephemeralizer [Per05a]. 

EPOC [JQY01]. 

ePOST [MPH06]. 

EPR [Ina02b]. 

EPR [JF03]. 

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

Equipping [DM70]. 

Equitability [DB01]. 

equivalence [Fis01a, LQ08, MSV04]. 

Equivalent [Fer00, KOMM01, May04, SIR04]. 

Era [MP00, UN00c, Bur00, UN00f]. 

erase
Exponents [FS02, FS01b, BS02]. Export [Mad00b, Ano00h, Mad00c]. Exposed [Gum04, MSK03, SSS06]. exposing [YY04]. Expositive [MAaT05]. Exposure [Mad00b, Ano00h, Mad00c]. Exposing [Gum04, MSK03, SSS06]. Exposition [MAaT05]. Exposure-Resilient [DSS01, KZ07, KZ03].

expressions [MW04]. Extended [ABDS01, BPS00, CM00, Cou04, DIRR05, HLvA02, HJW01, JL00, MSJ02, MP02, OST05, Wag02, BJN00, CD00a, HT04, HP01, Mis06, Pei09, QVP05, KJL01]. Extending [ADDS06, IKNP03, Ove06, Sal03b, SS01a].

Extension [Bai01a, YWD08, BR06, CMdV06]. Extensions [ABC05, BBGM08, CS07c, HM02b, Rot02b, Wei04, Elb08]. Extracting [Cer04a]. Extraction [DGH04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lu02, Vao03, 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 [Ano02b]. Factor [DN02b, Sas07, BSSM07, Hen06b, Sch05c, St.00, Ste05a, YWW008, dB07]. Factoring [BN02, KY02a, KLB02a, KOM01, May04, PV06b, ST02b, LTH05, LCZ05c, Mill01b, PLJ05a, QC05a, Sha03d, Sha05d, ZCL05].

Factoring-Based [PV06b]. factorisation [GG08]. Factorization [CDL04b, Lam04]. Facts [GO03]. Fade [CAC03]. Fail [JQY01, SSNS00]. Fail-stop [SSNS00]. Failures [DFG01, HGNN03]. Fair [CC00, DLY08, GC01a, JL01, JU04, LMS05, PS00, VP01, VW01, LSA07, MS03a].

Fair-Zero [MS05]. fairness [GCKL08]. faithfulness [GTZ04]. false [ZSJN07]. Falsification [OM09]. Fame [Bar00c]. Family [CQS01, Fnu02a, NP01, SK05a, You01, Ber07, FNRC05, GBKP01, MP07].

Fan [YY05c]. fare [MG00]. Fascinating [Sch09]. FASME [RM02]. Fast [AL00b, ABM00, BDTW01, BST02, CJ01, CC06, CQS01, Cor00a, Cou03, Cro01, FS02, GC01a, GD02, GMM01, GPC08, HGG07, HR04a, JJ00d, KKM01, KK03, KK07, LSY01, LS05b, MSN07, Kir03, NS05a, NSS02, OKE02, OT03b, PG05, RR02, Tsa06, UHA09, Yan05, ABB04, BMA00a, BMA00b, BMA00c, JAW00, JJ02, Lub05, PBMB01, WWA01, Bir07, DR02c, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d].

Faster [Bar00c, CMJP03, GLV01, KS09a, LV04, Oec03, Ban05, Why05]. faszinierende [Sch09]. Fat [MY01, TdK02]. Fault [Ano01b, BM00, BK06b, BK07, DS03, Gir06, PV06a, PQ03b, WL07b, YKL02, HGR07, Lin07, PJ06, RM04, YJ00, YKL03, ZL04a]. fault-based [YJ00].

Fault-Tolerant [WL07b, HGR07, Lin07, RM04]. Faults [GS08, VS08]. Favour [Gen01]. Favre [MFS09]. FBI [Mad04]. FC [Bl03, Fra01, Jue04, PY05, Syv02, Wri03].

Fear [Hei03, See04, Sty04, Sch03]. Feasibility [APV05, BDET04]. feasible [LM08]. Feature [GW01, Gut02a, HH09, LNP02, LLC06a, NN03]. Features [PK01, SBG02].

February [DR02c, Fra01, GH05, Joh03, Jue04, Kil05, Kim01, Men05, NF02a, Nao04, Oka04, PY05, Po06, Pre02c, RM04, Syv02, USE02, Wli09].

Federated [DeL07, Ano04e, GY08, Smi08, Sul05]. Feedback [CGFSH09, CM03, Cou03, Ig02, Hey03, SPC02]. FeedForward [BP01a].

Feel [PM00]. Feeling [Buh06]. Feistel [Cou04, Kan01, LMS07, On01, Pat04].

Feldman [AF04b]. Ferrer [CK06]. Fetal [MY01]. fetch [HTW07]. Fi [Sty04, Bar03]. Fiat [VS08]. fiction [An03g]. FIDES [ISTE08]. Field
First-order [Coh03, KS06b]. Fish [Fie09, Wei06, Wei00, Wei05]. Fit [CCM05].
Five [SW00a, MS02b, Rot02b, Rot03].
Five-lecture [Rot02b, Rot03]. Fix [TEM+01].
First [ACM03b, SM07b]. Fighting [DGN03, SZ03].
File [CCDP01, GIS05, Ito01, LK01, BDET00, CSK08, HTW07, Hos06b, ISO05, MKKW00, MSP08].
Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pet05].
Filter [LBGZ01, LBGZ02, MSNH07, Sar02, CMS08].
Filter-Combiner [Sar02]. Filtered [MH04].
Filtering [SDFH00]. Final [DPR01, Dra00, GC01a].
Finalist [SB00]. Finalists [EYCP00, IKM00, IK00, IK01, Mes00, Mes01, SKKS00, SW00a, WWCW00].
Finally [Coc02b]. Financial [ANS05, Gri01, Pem01b, Wri03, Bla03, Fra01, Jue04, PY05, Syv02].
Finding [HR04b, MP06, WYY05b, WYY05c, ZT03, SW00b].
FINDsomeone.com [Gra98]. Fine [SS01b].
Fine-Grained [SS01b]. Fingerprint [An002d, HHYW07, HBF09, KHY04, MMYH02, CL04d, MMJP03, UBEP09].
fingerprint-based [CL04d].
Fingerprinting [KT01, CTT07].
Fingerprints [TK03, KLY03, Sco04].
Fingers [MMYH02]. Finite [BLST01, BR01, CU01, Che04b, CQS01, HCK09, HW05, KKK03, MM07b, PHK+01, RS08, Ver02, Gar04, Has00, LMC+03, LQ08, NS01a, RMH04, Sma01, SLTB06, TC00].
Finkenzeller [And04]. FIPS [Nat00].
firewall [LJY04]. firm [Za00]. First [Bar00a, BBD09, Coh03, CM02, CMB+05, FLY06, KGL04, KS06b, MNP01, Nao04, NNT05, ÖOP03, PK03, QSR+02, Roy00a, USE00b, Wil99, ZJ04, ZHY03, AJ01a, Cl00b, Coc02a, DV05, LBA00, RH00, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, Lan00a].
Scho0e, Ano05b, HP00, LPW06, SK03. Fuzzing [SGA07]. Fuzzy
[SH11, HS02b, NC09, SM11]. fuzzy-based [NC09].

G [Coc03, For04, Was08a]. Gaithburg
[SMP+09]. Gamal [EKRMA01]. Game
[DHMR00, LM02, CAC06, BR04, Gou09, HCBLETRG06]. game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
game-playing [BR04]. Gamers [MP00]. Games
[KN08, HCBLETRG06]. Game-like [Gou09].
RE03, dLB07, AB09, Fin03, Har05b, KB00, KI03, MJ03, RE00, Was08a. **Handheld** [BMK00, Ano06a]. **Handhelds** [MP00]. **Handle** [RC06]. **Handling** [KL05, Lut03]. **Handoff** [OKE02]. **Hands** [KLB07, Shu06]. **Hands-on** [KLB07, Shu06]. **Handshake** [SB01]. **Handshakes** [Ver06a]. **Handwriting** [Ano02d]. **Haptic** [PBM07]. **Haptics** [Pau02a]. **Hard** [Har07b, HMS04, Hro03, Lai07, CGHG06, GPV08]. **Hard-Core** [HMS04]. **Hard-Disk** [Har07b]. **Hard-Line** [Lai07]. **hard-on-average** [CGHG06]. **hardcore** [Sch01e]. **hardcover** [Eag05, Pag03, Top02, Pap05]. **Harddisk** [Por01]. **hardening** [Mos06]. **Hardness** [CHS05, CNS02, KY02b, KS06a, LTW05, SV08b, AGGM06, KS09b, SU07, AGGM10]. **Hardware** [Ano02b, Ano07b, Ano07a, BM01a, DF01, Di03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, Nd05, PS01c, RS05, RS04, SOTD00, SMTM01, SM02, SM03b, SRQL03, SGK08, TSO00, TBLD01, WK03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK03, DS09, EHKH04, GC00a, HBC08, KP01, KNP01, KP03, Nd04, RA07, SOIG07, VS08, Wo04, YKLM03, YW06]. **Hardware-based** [Ano02b]. **hardware-constrained** [RAL07]. **hardware/software** [ARJ08]. **Harley** [WW05]. **Harn** [GG01]. **Hash** [Ano08d, Ano12, AEMR09, BBKN01, BR02, BDRS09b, Bur06, CBB05, Cor06b, Cor02, CMDP05, CS02, DOP05, FIP02b, Fil02, GIS05, GLG02, HPC02, HR04b, ISO04, Jou04, KMM06, MD05, RRS06, RR08, RB01, SS01a, Sho00a, Sho00b, SK05a, WFLY04, Yan05, YZ00, BR06, DS09, KCL03, Ku04, KCC05, LLHO2, LKY04, LW04, MS09c, Mic02b, Tsa08, Wag00, YRY04, FIP02a, ZW05a]. **Hash-based** [BDS09b, KCL03, Ku04, KCC05]. **Hash-CBC** [BBKN01]. **Hash-chaining** [CBB05]. **Hash-Function** [BRS02]. **Hash-functions** [IS004]. **Hashes** [Sch01a, GNP05]. **Hashing** [IK05, SGGB00, WS03]. **HAVAL** [WFLY04]. **HAVAL-128** [WFLY04]. **HAVEGE** [SS03]. **HB** [MP07]. **HB-family** [MP07]. **HCl** [YKMB08]. **head** [RFR07a, RFR07b, RFR07c]. **headlines** [Hen06b]. **Health** [Mad00a, Ano03a, CCCY01]. **health-care** [Ano03a]. **Healthcare** [BTTF02]. **Heap** [ST06]. **Heating** [UNo00c, UNi00g, UNi00b, UNi00f, UNi00h]. **hearings** [UNi00b]. **heart** [Mur06]. **Heavens** [Eva09]. **Hedge** [Sho00b]. **Hedged** [BBN09]. **Heimdal** [WD01a]. **held** [Buc00a, PPV96, UNi00b]. **Hellman** [KM04a, ABR01, ASW01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKRT08, FS01b, GR04, Ki01b, KK02, Kra03, Kro05, Mi08, Tsa06, YRY05c]. **help** [Ano08a]. **Helped** [Gan01b]. **Helps** [DF01, Pri00]. **Helsinki** [Bur00]. **Hensel** [CNS02]. **Her** [Bud06]. **Here** [Bur06, Law05]. **Hermite** [Mic01]. **heroes** [OC03]. **Herriot** [Coc03]. **Hersonissos** [ACM01a]. **Hessenberg** [SSFC09]. **Heterogeneous** [BCS02, Hf01, KHYM08, ZBLV05]. **heuristic** [SS03]. **Heuristics** [Hro03]. **HFE** [FJ03, CHH01, Fel06]. **HFE-Cryptosystems** [Fel06]. **HIBE** [CS07e]. **Hidden** [HGN03, KW03, LNS02, Six05, GMR05, Lun00, Shp05, FJ03, Sch09]. **Hide** [CC06, PH03, Shp05]. **hide-and-seek** [Shp05]. **Hiding** [BD03, CLT07, Co03, DN02b, GA05, HNO09, LHS05, LS08, MH05, MMT09, VDKP05, WC03a, HR07, JDJ01, KP00, RFLP05, Way02b, Way09, YCL07]. **Hierarchy** [HC08]. **Hierarchical** [GS02b, HNZZ02, HL02, Lin01a, MN01,
38

YLH05, BD04b, Che07a, CJ03c, JW06, KAM08, WC01b, hY08]. hierarchies
[AFB05, Cer04a, HY03, WL05]. hierarchy
[CLK04, CMdV06, HW03c, Hwa00, JA02]. Hierocrypt [OMSK01]. Hieroglyphs
[Wri05]. High [ACM01b, Ano00d, Ano02d, ChLYL09, CW09, CJL06, CGJ+02, DS05b, FZH05, Gro01, HNZI02, HV04, Int00, JKRW01, KMM+06, Ken02b, KM05, KB00, Kra05, KT01, MM01b, NFQ03, RW07, SKKS00, SOTD00, SM02, SGM09, SLG+05, TL07, Uni00c, Wie00, WWGP00, YKMY01, Zhe01, BVP+B04, BZP05, BGL+03, Jun09, 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, RW07, BGL+03]. High-technology-crime [KB00]. High-Throughput [HV04]. Higher [CV02, KCP01, BFO1a]. Highly [CV02]. hijacking [Ste05c]. Hill [Gum04, USE02a]. Hilton [KJR05]. HIPAA [AEV+07]. histograms [C009a, historic [Pet08]]. Historical [RE02, MWM01]. History [BP03b, Irf00, Pag03, Sal01a, Sin01b, CAC06, Top02, dLB07, AJ08, Boo05, HSW09, Jan08b, KNS05, Na05, Nis03a, Pin06, Ris06, RH00, RG06, Wil01a]. history-based [KNS05]. hit [Bjo05]. HMAC [FIP02a, DGH+04, Hir09, RR08]. HMQV [Kra05]. Hoare [dH08]. Hoax [CZB+01, CTBA+01]. hoc [BSS02, Cha05a, DHMR07, KH05, KVD07, LHC08, LKZ+04, PSM07, SLP07, TW07, WT02, ZC09]. Hold [PM00]. Holier [MYC01]. Holistic [RM02]. Homage [JP02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03]. Homegrown [Str02]. Homeland [Man02, Man03, RR03b]. homogeneous [MF07, PS02a]. Homomorphic [AS01a, Aki09, CDN01, DN03, HS00, Cho06, Gen09a, Gen09b]. homomorphism [CKN06]. homophonic [Sav04]. Honeynets [Dim07]. Honk [B+02, ZJ04, Cla00b]. honor [OC03]. hook [JEZ04]. hooks [GJJ05]. hop [NC09, ZSJN]. hop-by-hop [ZSJN]. Horizon [Coc02b]. host [Shu06]. hostile [ABB+04]. Hosts [Hef01, 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, KOY01, Yon04, Man08, MS02d, RFR07a, RFR07b, RFR07c]. Human-Memorable [KOY01]. Hundred [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hunting [GJL06]. Hütttenhain [Bau08, Bau08]. Hv [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KCL03, LW05c, QC05a, WL05, YR05d, ZYR01]. Hwang-Rao [ZYR01]. HWMM [LKY05]. HWMM-authenticated [LKY05c]. Hybrid [AD109, 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, CFA+06, HSS01, PWGP03, Ver02, Was08a, ZLK02, CMKT00, Wen03, Wol04, WPP05]. Hyperencryption [Che01d]. hyperlinking [Che01e]. hypotheses [KW00].

I-tracings [RE02]. i.e [NP02a, Wil99]. IA [WWCW00]. IA-64 [WWCW00]. IACBC [JM02]. IBE [ABC+05]. IBM [An04e,
AV04, ADH+07, CGH+00b, Web08, Web00].

Ibn
[MAAT04, MAAT05, MAATxx, MAAT07].

Ibn-Adlan [MAATxx]. Ibn-Al-Durahim [MAATxx].

iButton [HWH01]. IC [BGL+03, PC00]. ICBA [ZJ04]. ICCMSE [SM07b]. ICISC [Kini02, LL04d, PC05a, Won01, WK06].

ICISC'99 [Son00]. ICCM [IEE09a, IEE09a]. ICs [Bar00c]. ID [Gui06, ZJ09, BRTM09, CCD07, CL07, CS07c, CL00, GS02b, GTY08, HC08, KLY03, KHL09, Ku02, LCS09, Sco04, SW05a, SCL05, WBD01, WH02b, YC09b, YLH05, ZK02, ZC04, ZC09].

Id-Based [ZJ09, CCD07, KS02b, HC08, Ku02, WBD01, YLH05, ZK02, CL00, KLY03, KHL09, Sco04, SW05a, SCL05, WBD01, WH02b, YC09b, YLH05, ZK02, ZC04, 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, GK04, Her06, Her07, HY01, HL02, KC02, LCD07, Mar08a, Mar08b, Mit02b, Net06, PCSM07, Phi06, SMP+09, An001, An004e, BM05, CG06, CJL05, GG08, Gu06, KG09, L04b, LWZH05, RG09, Sau02, Shao3c, Sma06, Sm08, Su05, Wal04, Wan04b, Win05a, Wou05, YCW+08, Yout04, ZYW07].

Identity-Based [BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, LCD07, Mar08a, Mar08b, App05, Her07, PCSM07, BM05, CG06, CJL05, KG09, LL04b, LWZH05, Sae02, Shao3c, YCW+08, ZYW07].

IDSFM [TZDZ05]. IDtrust2009 [SMP+09]. IEC [ISO04]. IEEE [BS03, BCDH09, BC01, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KM07, HSD+05, Hug04, Mi08, PHM03, ZD06]. IEM [RC05]. IFIP [DK05, DFPS06, DFCW00, ELvS01]. I

II [Ban05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Hait03, K09, OC03, Res01a, Res01b, Sal00a, ZT03].

III [Sch00a, An00d, Bau03b]. IKE [CK02a, Kra03]. I'll [PLW07]. illegal [Che01e]. Illinois [ACM04b]. Illusions [Koc02]. illustrated [Lun09]. Im [Box03b, Sma05, Hon01].

Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, CLT07, CC09, CC06, GW01, KBD03, K09b, L05a, LZ01, L05b, LSC03, LSCI05, PZL09, R00, SDFH00, SGD01, SSFC09, SH11, SM11, SYLC05, T01, TH01, TC01, UP05, V09, VK07, W02, WLT05b, YZEE09, AAPP07, A08, CC02b, CHC01, Che07a, Che08a, GSK09, HLC07, K09a, L05a, L05b, L04, LYG07, L006b, MS09a, MB08, PBV08, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, mSfL05, TL02, Wan05, WMS08, WC05, XSWC10, YCY07, YLC07, ZLZ07].

Image-Feature [GW01]. image-identification [PBV08]. Images [CTL04, CC08, CW09, DP00, FGD01, LS08, PJH01, PBC05, RE02, W09, WC04, YWWS09, AAPP07, AEEd05, BD00, FWT05, H07, T02, T03†].

Imaginary [HJW01, HM00, Hau00]. Imai [DDG+06, YG01a]. Imbalanced [ZWC02].

Immu [Coo1a]. Immune [CZK05, PZ02b, YKLM02b, ZP01, YKLM03].

Immunization [HR05]. Impact [Ber03, HGNP+03, JKR01, MMY02, Wri00, CS08a]. Imperfect [CPS07, DOPS04].
[BP02, Hsu05b]. implant [Fox00].

**Implement** [HQ05]. **Implementation**

[AD07, AG01, Ase02, Ash03, ARC+01, BBD+02, CCDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EH+03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HHM01, JKS02, KMM+06, KMS01, KTT07, KRS+02, KV01, LP02a, MMZ00, MKP09, MM01c, MNP01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBTV07, QSR+02, RDJ+01, SMO1, Sha01e, SK05a, SRLQ03, USS02, Vir03, WZW05, WW00, WOL01, XBO1, Zea06, BI04, BBK+03b, C+02, CPNQ03, DS09, DKL+00a, GHDGSS00, GBKP01, Hüh00, HP01, Hut01, KY09, LLO4c, LCX08, LB05, Rhi03, SM03a, SVDF07, WoI04, YW06, ZFK04].

**Implementations** [AL00b, BJP02, III00, CTLL01, CGBS01, EPP+07, GLG+02, MM01b, MP01a, RS01, WWCW00, ASK05, BFCZ08, BG07b, Elb08, FR08, RAL07, RSQLO3].

**Implemented** [TSS+03].

**Implementing** [Dwi04, Kor09, LM08, LDM04, MW008, NDJb01, Pet03, Sni01a, SR06, WoO05, C+02, CW02].

**Implications** [Kun01, LJ05a, MF01, Ayo06, Bjo05, Fri07].

**Implies** [KY01e].

**Importance** [Ano02b, KCJ+01, TIGD01].

**Important** [SM00a], imposed [XLS06].

**Impossibilities** [CHL02].

**Impossiiblity** [APV05, BPR+08, Fis01b, PQ06].

**Impossible** [BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SK101].

**impostor** [jLC07].

**Improve** [Pau02a, CAC06].

**Improvement** [CAC06].

**Improved**

[AFGH06, BPR05, BB05, BF00b, CL01b, CKK+02, CJ04, DN00a, DG02, Fun03, FKS+00, FKL+01b, FKL+01a, GM008, Gen00b, HCK09, HKA+05, JQY01, Kin00, KT06, Ku02, Küh02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02e, PR08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCB05a, YW05, YRY05a, ZW05a].

**Improvement** [AS01c, AJ008, Che04a, CZK05, CCW02, Di01, HWWM03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Sha04b, Sha05b, WHL03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04e, CHY05a, HS05a, JSW05, JmBdXxm05, KJY05, LL04a, LW05c, SZS05, TO01, WL05a, YW04a, YWC05, YRY05a, YRY05d, ZC09].

**Improvements** [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, HW03c, SRLQ03].

**Improving** [ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SKQ01, SB01, Sun02, XQ07, YEP+06, YGZ05].

**incentives** [Swi05].

**Incident** [JBR05, Tom06].

**Including** [SR01].

**incomputable** [Ver06b].

**inconsistencies** [MS09a].

**Incorporating** [MFS+09].

**incorrectness** [CHC04].

**Increase** [NNAM10, PBTW07].

**Increasing** [AEH17, CS05c].

**Incremental** [BK02, LKL05].

**IND-CCA** [Mühl01b].

**IND-CCA2** [BST02].

**Independence** [BP03b].

**Independent** [BS00a, BSL02, Kin02, GSK09].

**Index** [Ano00b, Ano01d].

**indexing** [YPPK09].

**India** [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03d].

**Indies** [Fra01, Syv02, Wri03].

**Individual** [BCC02, TW07].

**INDOCRYPT** [CV04, JM03, MMV06, MS02c, RD01, Roy00a].

**Induced** [Vau02].

**Industrial** [USE00b].

**Industry** [ANS05, Mad00a, Ort00].

**ineffectiveness** [YLR05].

**Infeasibility** [FS08].

**Inference** [Mar02b, CDD+05].

**Infinite** [TZZ09a, TZZ09b, Vau01].

**infinity** [Hül05].

**Influencing** [Bla01c].

**Inform** [Kwo03b, San05].

**Information** [AP09, BW07, BM00, BZ02, Big08, BB03, B02, Boy01, CGM07, CC06, DM00b, ECM00a, ELvS01, Hay06, HQ05, HW01, ISO04, JDJ01, JG07, KP00, Ke02, KLB+02b, KO00, Lai03, Lee04b, LW05b, LL01, MH05,
MMZ00, Oka00, PP06b, RSA00d, RS01, Roy05, Sch06b, SVW00, Son00, Sta06, Ste02, TG07, VDKP05, WABL+08, Yek07, Zhe02b, ZS05, dLB07, vW01, ABHS09, 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, CSY09, FLY06, Kim02, LL03, LL04d, PCT05a, 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, C05, FB01, Gor05, LCK04, MWS08, Ben02]. Infrastructures [HCDO02, Lin00b, PHM03, WBD01, Bra01a, LAPS08, LOP04, SN07]. INIDP04 [LDM04]. initial [DK08].

initiation [YW05]. Initiative [Coc01a, Cal00b]. initiatives [Man05]. injection [MMJ05, ZSJN07]. Injectable [Cmdv06, Kos01c]. Innovation [Sam09, SW05b]. innovations [Web02].

Innovative [MM07a]. Innsbruck [Pfi01]. Input [CAC06, TC00, DKL09, VM03]. Input-trees [TC00]. Insecure [Vau05b, Wal01, BJN00, LLH06, XwWL08].

Insecurity [Bl02b, 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, EKRM01]. Integral [KW02, WH09, SM11, SH11].

Integrated [ECM00a, ECM00b, GMG00, Lut03, GLC+04, LK01, SSM+08, SN04]. Integrating [Wei01, AEH17]. Integration [Ito00, CJL06, Sug03]. Integrity [An02e, CS08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel [Coc02a, MP00]. Intellectual [Qu01, WY02]. Intelligence [Cop04b, AJ08]. Intelligent [Cos03]. Inter [WRW02, ECM00b]. Inter-Exchange [ECM00b]. Inter-Packet [WRW02]. interaction [Gav08]. Interactions [Fau09].

Interactive [BC05b, DG00, MS09c, CHK05, DDO+01, Fis01b, Fis05, HNJ02, HJW01, KKL09, KHL09, MSTS04, Pas05, vT00, MS09c].

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

Interlaken [CC04a]. Interleaved [ZSJN07, NC09]. intermediaries [JA02].

Internal [Har07b, Bej06]. International [ACM03a, ACM04a, ACM05a, ACM09, ACM10, AN03, An00d, AAC+01, AJ01b, BDZ04, Bel00, R+02, BBD09, BS01b, Bih03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCMR02, CCMR05, CSY09, CDP03, Cra05a, DR02c, Des02, DUK05, DFS06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JYZ04, Jef08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, KIm01, Kim02, 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,
Sho05a, Sil01, SM07b, Syv02, TB02, TLC06, Uni00a, VY01, Vau05a, WKP03, Wil99, Won01, Wri03. \textit{International} [Yun02a, YDKM06, ZJ04, Zhe02b, ZYH03, AMW07, AUW01, Ano00e, AJ01a, BCKK05, Bir07, BC05c, CKL05, DV05, DWML05, DRS05, GKS05, HH04, HH05, HA00, Hon01, May09, PC05a, PY05, PPV96, QS00, Sma05, Son00, ST01d, WK06, Ytr06]. \textit{Internet} [SMP09, ABB04, Ben01a, Ben02, Cal00a, Che05b, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, PvS01, Pho01, PHL03, Rub01, SBB05, SEK01, SEK02, Sto01, Tsa01, TVL05, Uri01, WC05, Wri05, ZGTG05, kc01]. \textit{Internet-wide} [SBB05]. \textit{Interoperability} [Hil00, TEM01, BHM03]. \textit{Interoperable} [BFGT08]. \textit{Interpolation} [LW02, YG01b, FWTC05, KT06]. \textit{Interpolations} [Sat06]. \textit{Interpretation} [Mas04, CC04c]. \textit{Interpretation-based} [CC04c]. \textit{Intersections} [KS06a, KS09b]. \textit{Interstate} [RM02]. \textit{Intranet} [Jan00]. \textit{Intrinsic} [ZWC02]. \textit{Introduction} [ANo00a]. \textit{Introducing} [JL00]. \textit{Introduction} [Ben02, Ben09b, Bis03a, BK06b, Buc04, CLR01, DK02, DK07, Fal07, Hay06, HPS08, Hro03, HC02, KL08, MA00a, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJT09, SGK08, TW02, TW05, TW06b, Big08, CS07a, CM05b, Gar01, HW98, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06a, Kat05b, Rot07, Lee03a]. \textit{Intrusion} [CZK05, DFK+03, DP07, JT05, TZZ05, TMMM05, WF05, HLL+02, MAC+03, NCRM0, NN02, YbJf04, IR02]. \textit{Intrusion-Resilient} [DFK+03, DP07, IR02]. \textit{Intrusion-tolerant} [YbJf04]. \textit{Intrusions} [Bej06]. \textit{Intrusive} [AMB06, RFR07a, RFR07b, RFR07c]. \textit{Invalid} [CJT04]. \textit{Invariant} [Ben00, CT09, HH09, ZLZS07]. \textit{Invariants} [WH09]. \textit{Invasion} [ASW+01]. \textit{invasions} [Tyn05]. \textit{Invention} [Bra06, Fv00, Sav05a]. \textit{Inventions} [Sav05b]. \textit{Inventors} [Bar00c]. \textit{Inverse} [Har06, OS07]. \textit{Inverses} [CGH00a, Has01a, JP03, MFT05]. \textit{Inversion} [BNPS02, KKY02, KTT07, SPG02]. \textit{Inversion/Division} [KKY02]. \textit{Inversive} [SB05]. \textit{Investigating} [AMB06, BW07]. \textit{investigation} [Cas02]. \textit{Investigative} [Men03]. \textit{investigator} [KB00]. \textit{Invisibility} [GM03]. \textit{Invisible} [MB08, WD01b, WC04]. \textit{Invitation} [Bar02]. \textit{Invited} [FGM00a, Lan00d, DRS05]. \textit{involutional} [SHH07]. \textit{ions} [Min03]. \textit{IP} [Ano00a, CD01b, FXM04, HL07, Lin07, MV03b, RW07]. \textit{IP-based} [MV03b]. \textit{IPAKE} [CPP04]. \textit{IPSEC} [Vau02, CGBS01, Dav01a, KMM+06, SKW+07, FS00, FS03a, XLM06]. \textit{IPSec-Compliant} [CGBS01]. \textit{IPTables} [GC05]. \textit{IPv6} [Nik02a, Nik02b]. \textit{Iran} [Mah04]. \textit{Ire} [Cos03]. \textit{Iris} [CJL06]. \textit{Irregular} [MH04]. \textit{Irregularly} [CGFS09]. \textit{Irreversibility} [ZWC02]. \textit{ISBN} [And04, Duw03, Eeg05, For04, Gun04, Imr03, Pag03, Puz04, Top02]. \textit{Island} [CSY09, KGL04, Kim01, Lee04b, IEE07]. \textit{ISO} [GM00b]. \textit{ISO/IEC} [ISO04]. \textit{ISO9979} [TM01]. \textit{ISO9979-20} [TM01]. \textit{Isolated} [LSVS09, MMT09]. \textit{Isomorphism} [CY02]. \textit{Isomorphisms} [CPP04]. \textit{Israel} [Jol01]. \textit{ISSAC} [Jef08]. \textit{Isaac} [FOP06, FOP06]. \textit{Issues} [BDF+01a, BH00a, Hii00, KR01, Mea01, PBM+07, SEF+06, MK08, Pat02b]. \textit{ISW'97} [You01]. \textit{IT-Architectures} [RM02]. \textit{Italy} [AAC+01, AL06, BCKK05, BC05c, CGP03, dCDV05, IEE04]. \textit{Itanium} [CHT02, Int00]. \textit{Itanium-based} [CHT02]. \textit{Iterated} [Jon04, Oni01]. \textit{Iteration} [Che03]. \textit{IV} [Scho01c, HSH+01]. \textit{IWBRS} [LST+05]. \textit{IWDW} [BCKK05, CKL05, KCR04, PK03].
J2EE [BTTF02]. Jack [Coc03]. James [Top02]. jamming [LPV+09]. Jan [YRY05b]. January
[Des02, GL05, IZ00, Vau05a, Wri03]. Japan [Ano00d, Mat02, Coc02b, Smi01b].
Japanese [IY00]. Java [Ano04c, Mar05a, WBL01, Ano02e, Ano03a, Ano04c, Ano04f, AJ01a, CS020, Bis03a, BJVdB02, CMG+01, Che00a, CCM05, Coo02, DPT+02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Mun05, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Vir03, Weи04, Win01, Zee00, ZFK04].
Judiciary [Uni00h]. Julius [Chu02]. July [AC01a, CZ05, Jef08, KJR05, May09, PPV96, Roy00b, Sch01c, S+03, Uni00a, Uni00b, Uni00c, Uni00d, ZJ04]. Jump [MP00]. June [ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BSO3, BSO1b, BCD09, BC01, CZ05, FMA02, IEE05b, IKY05, JY04, KGL04, KN03, KM07, PPV96, TBJ02, USE01b, USE01a, USE02c]. Just [ABB+04, Ano06a, Gut02a, Car01].

Kahn [Gas01]. Kaikan [An00d].
Kaspersky [Ano08a]. KASUMI

KYHC01, KSHY01, SM02]. Katholieke [BD09]. Katz [Bar00a]. Keccak [BDPV09]. Keep [DM07b, Lys08, FS04]. Keeping [SEK01, SEK02]. KEM [NMO05]. Kerberos [BCJ+06, Coc01a, Gar03b, Hil00, Ito00, LLW08a, MJ01, MPPM09, Rub00, Smi01a, Wac05, WD01a, Wit01].
Kerckhoffs [KMZ03]. Kernel [Int00, Mor03, BK05, H00]. Key [ANS05, ASW00, AK02a, An01n, Ano09d, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BPS08, BH06, BDG+01, BDZ04, Bar00a, BPS04, BPR00, BM00, BBDP01, BY03, BOHL+05, Ben02, BL01, Bih00, BBB+02, BDK+09, BR00b, BM03b, BDTW01, BM01, BMO3c, BGM09, BMP00, BCP01, BCP02a, BCP02b, BM01c, BST02, CK02a, CK02b, CH03, CHK05, CPP04, CHe01a, CT08a, CHK08, CJ03c, CCW02, CCM01, CMO0, CS020, CS03c, DPV04, DJ01, DPS05, Des00c, DSB01, Des02, DG03, DY09b, DXY02, DFK+03, DGH+04, DBS+06, ESG+05, EP05, ES00a, FL06, FKSW00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Go03, GH01, GC01b, GS+04, Gut04b, HNZ02, HCD002, HLM03, Hoe01, HR05, H03, HC08, HJ01, HS07, HLC08, EEE00b, Ina02a, Ina02b, JL08, J01, J01, J04a, Ka01]. Key [KGL04, KOY01, KY03, Kat05b, Kel05a, Kel05b, Kel00, KKIM01, KM01a, KLY02, KKY02, KY02c, KLC+00, KJ01b, KM04b, Kos01a, Kos01b, KU02, KOM01, KY01e, Kur01, Ki03, LCK01, LLL02, LP03, LV00, Len01, Lin03, Lin00b, MPS00, Mac01, MSJ02, MHH+02, May04, MR01b, MR01c, M013a, Mol03b, Mö10a, Mur00, NIS03b, NA07, Ngu05, NBD01, NSS02, OTU00, Ort00, PHK+01, PR01, Poi02, PHM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sha01e, Sin01a, SVW00, SK00, ST01, ST01c, TSO00, Tan07b, TTO1, VV07, Wal03, WZ05, WH01, WC01a, Woo00, WBD01, Wya02, YKMY01, YI01, YG01c, YDKM06,
Zhe02a, ZWCY02, 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, CY05, Che04a, CHC04, CY05, CLC08, CKRT08, CWJT01, CJ04, CLK04, Che06, CHH+09, CJL05, CCD06, Cre00, DFM04, DG06, DMT07, DW09, EKRM01, ED03, EHKH04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GMR05, GKM+00, GS01, GL06b, GMW01, Gue09, HCD08a, HCD08b, Cao01, HLLL03, HTJ08, HG05b, HWWM03, HMvdLM07, HLTJ09, Hwa00, HLLL04, IZ00, Iwa08, IM06, Jun08b, JRR09, JW06, JXW05, JZCW05, Jua04, KY00, KS05a, KOY09, KY08, KAM08, KG09, Kim01, KPT04, KRY05, Kob00, KW00, Kos01c, KHKL05, LH03a, LF03, LKKY03a, LKKY03b, LCP04, LHL04b, LL04a, LW04, LLL04, LL05a, LKY05b, LKY05c, LKY05d, LLY06, LL05a, LL05b, LL05c, LL05d, LLL06, LL06b, LFHT07, LCK04, LPM05, LH08, LKL01, LS00, L01a, LS01c, LCC05, Lop06, MWS08, MKW00, MP08, MS08, MRT10, Mut01b, NP02a, PS08a]. key [PI06, Pei09, Pei04, PQ03a, PQ06, PC09, PSP+08, PL05b, Pot06, Pri00, RH03, SN01, SLP07, SR01, SBZ04, Sha05c, SW06, Shi05, SL05a, SW05a, Shp04a, SC05b, SIR04, SL05c, Sun00b, Sun02, SZP02, SCS05b, SC05c, SCS05c, SY06, TP07, TO01, TN04, Ts06, Ts05, Ts07, VS01, Vau05a, VK08, WDLN09, War00, WLH06, W010, WVC01b, Wu04, WL04b, WHHT08, XH05, YW05, YC09a, YC09b, YS02, YSH03, YS04, hY08, Yi04, YR05a, YR05b, YY05b, YPKL08, ZGL01, ZC04, ZK05, ZSM05, ZYW07, Abb+04, GL05]. Key-Based [Sha01e]. Key-Dependent [Gol03, BPS08]. Key-Exchange [BH06, CK02a, K05a]. Key-Insulated [DKXY02]. key-management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DPS05]. Key-Share [CT08a]. Key-Sharing [HNZI02, WBD01]. Keypad board [ZZ05, EGK08]. Keyless [Qu01]. Keys [AOS02, APV05, AFL06, BTO2, BM00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, LXX07, Luc00, MN01, MRL+02, Moo07, Nit09, On01, P00, Sni01c, Str02, TvdK+01, Ano01k, BCL05a, BCW05, B09a, BF01c, CWH00, CCH05, C05, HSH+08b, HSH+09, HW04, HY03, HLL04, K08, LL04b, LLL04b, LS01c, LWK05a, ML05, N03, Sch01c, Sha04b, Sha05b, SB05, TLH05, TJ03, WH03, WH03, YRS+09]. Keystream [AMR04, K02a, LV04, MH04, LVW04, P01a, SM11]. Keystrokes [SWT07]. Keyword [FIPR05]. KGC [HLC08]. KG [ZY07]. KHADZ [PS03b]. KIAS [May09]. Kid [CAC06]. Kikai [An00d]. Kikai-Shinko-Kaikan [An00d]. kill [Lov01]. Killing [Lov01]. Kilometer [Das08]. kind [DW01]. Kindi [MAaT03, MAaTxx]. King [Eag05]. Kingdom [DCW00]. Kingston [HA00, PT06]. Kit [An02a]. Klaus [And04]. Kleptographic [YY01]. knapsack [Cos01c, SLC05]. knapsacks [Mic02a]. Knife [Boy03]. Know [CMB+05, Ros07, Con09, DKK07, Win05c]. Knowing [CH01a]. Knowledge [Abe01, Abe04, AS01b, APV05, BP04, Con01, DPV04, DFS04, DDO+01, Eri02, Fis05, Gen04a, GK05, HNO+09, KS06b, LMS05, LHL+08, MR01b, MV03a, Pas05, Ros00a, Ros06a, TG07, BSV08, CLR09, Dam00, Hro09, IKOS07, JRR09, PBD07, KKT07]. Knowledge-of-Exponent [BP04]. Known [C06, CMB+05, DN02a, Fur02b, HSH+01, Bao04, YTH04]. Known-IV [HSH+01]. Known-Plaintext [DN02a, Fur02b, CKN06]. knows [Fox00].
Koblitz [AHRH08, Has01b]. Kolmogorov [Sch01a]. Kommunikation [Lin02]. Kong [B+02, ZJ04, Cla00b]. Konstantin [Puz04]. Korea [CSV09, CKL05, KCR04, Kim01, Kim02, Kum07, LL03, Lee04b, LL04d, May09, PC05a, PK03, Son00, Won01, WK06]. Korner [Mor03]. Ko´sciuszko [OC03]. Krawczyk [Miy01]. Kryptoanalyse [Mor05]. Kuala [DV05]. Kunming [ZYH03]. Kurosawa [CHH+09]. Kurtz [Gum04]. Kyoto [Oka00].

L [Sem00]. L-collision [Sem00]. Laboratory [Brut06, LBA00]. Lagrange [FWTC05]. Laid [Wei06, Wei05]. Lam [Wag00]. Lamar [LMHCETR06]. Lamp [McN03]. LAN [Bar03, LFHT07, Pau03, SZ08, Sty04]. Lanchester [BFR06a]. Landau [Jan08a]. Landscape [Ahm07]. Language [ARC+01, DDO2, Gou09, Jen09, MW04, WAF00]. language-based [WAF00]. languages [Lun09, Rob02, Rob09]. Lantern [Ano01k]. Laos [Lav01]. Laptop [PGT07]. Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, G01, Kuhl00, PG05, SM01, ST03b, USE00a, BP03a, CKY05, CJ03b, Has00, HMvdLM07, HY03, PS08a, SM03a, TM06, WL05]. Large-Scale [CD01b, BH00a, BP03a, HMvdLM07, PS08a]. Larger [Car02]. LARPBS [CPH04]. Lasers [Igl02, UHA+09]. late [Sch05c]. latency [RSP05]. Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HPS01, HG07, IM06, Mic01, Reg03, Reg04]. Lattice-based [MR09, HPS01, IM06, Reg04]. lattice-reduction [HG07]. Lattices [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Shp05, Sil01]. Launched [Bar00b, Ano00j]. Launches [Ano02d]. lava [McN03]. Law [GN06, MNFG02, Ste05c, NM09]. lawsuits [Ree03]. Layer [LXM+05, LPV+09, SLP07, ZL04c]. layered [KVD07]. Layers [Gri01]. Laying [Lut03]. Lazy [CCM05]. LDAP [Bau03a, Bau03b, BH00b]. Lead [Tsa07]. Leak [RST01]. Leakage [CKN01, DP08, Kel02, RS01, ABHS09, CNK04, HY05]. 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, C02b, 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, C00, CHJ+01b, Mål03a, RK06]. Length-Preserving [Mål03a]. Leonard [Coc03]. Less [YKMY01, BD00b]. Lessons [GSB+04, KS00]. Lest [SH+08a, HSH+08b, HSH+09]. Lets [Pau02a]. Lett [Kwo03]. 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, CS08, Vo05]. Leveraging [BRTM09]. LEVIATHAN [CL02c]. Levin [AC02]. LFSR [DS09, Jam00, JZCW05, MRT10]. LFSR-Based [Jam00]. LHL [Pe04, YRY05a]. LHL-key [Pe04, YRY05]. Li [JW01, KCL03, S205, QCB05a, SCS05b, ZK05]. Liaw [TJ01b]. Liberty [Lan04b, Ano00e, Ano04e]. librarian [PBV08]. Libraries [Fin02, MK05b]. Library [KSZ02, Lau05, Law09b]. Libre [Jen09]. license [An00h]. Lies [Gan01b, Sch00d, Swa01, Che00b, Ste05c]. Life [Cop04b, GSB+04]. lifecycle [HL06].
Lifetime [Coc01a, CPG+04]. Lifting [CNS02]. Light [WT02]. Light-Weight [WT02]. Lights [Gei03]. Lightweight [EPP+07, Mal02, CH07a, MP07]. Like [Coc02a, PSC+02, VMS05, BCD00, CW00, DLP+09, Egh00, EBS01, Gou09, HSL+02, HL04, SKU+00, SLL+00]. LILI [JJ02]. LILI-128 [JJ02]. Limit [Das08]. Limitations [Gua05, Fis01a, LG09]. Limited [AK02a, LCD07, Buh06, Tse07]. limiting [CCK04b]. Limits [CWR09]. Lin [CC02b, CHY05a, KTC03, YY05b]. Line [Cho08a, DL98, Jan08a, Lai07, Lu02, SK06, YLLL02, Bau05, BCS02, DL07, Luk01, Shi05]. Linear [BDK02a, BDK02b, BDQ04, CGFSHG09, CS05b, CHJ02, Cou01, CM03, Cou03, CDM00, CD01a, CDG+05, FM02a, FM02b, GS03, GBM02, HLL+01, Hug02, JJ00d, Kan01, KMT01, Kin02, KM01c, KRS+02, KY01e, LLL+01, LS05a, NP01, PSC+02, PG05, PZ02a, SNWX01, STK02, WF02, YSD02, BD04a, Bul09, CCK04b, CJT01, CK04, GHPT05, Kuk01, LLL04, Reg05, Reg09, RSQ01, Sel00, SLL+00, TM01, XWSC10]. 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, Fin02, Fri01, GJ05, Gan08, GPR06, JZ04, Lin02, Mor03, Pri00, Shn06, Sta02b, Sta05]. LISA [USE00c]. list [AGKS07]. Listening [Cas03]. little [Che01d, Lam07, Sch05c]. Live [Lov01]. Live [Lov01]. Lives [FPS01]. living [BCB+05]. LLL [CKY05, NS05c]. Load [CC08, Hõõ01]. Loads [GH02]. Loan [SOO10]. Loaing [Bl01c]. Local [NABG03, Lav09]. Locality [MFS+09]. Localization [WLT05b, CKL+09]. Locally [Vad03, Yek07]. Location [HY01, KZ01, LNL+08, Buh06, SG07]. Locations [Kra02b]. Log [Gen00b, HR04]. Logarithm [CNS02, Che04b, CCW02, GV05, GPP08, LW02, Hsu05a, HL05d, JLL01, LL04b, LHY05, Sch01e, SCL05, SL05c, YSC05]. Logarithmic [EGK08]. Logarithms [CS03a, J03, LLL03a, LTH05, PLJ05a, QCB05a, Sh05c, Sha05d, SCS05c]. Logging [Fox00, MT09]. Logic [BPST02, Cop04b, KBD03, KS06b, Li01, Nie02d, SQ01, SC01, Tee06, TV03, BDDN02, BD04a, DZL01, SW02, WZB05, dH08]. Logic-Based [KBD03]. Logical [Asl04b, Kra07, SP03, CL04, Zha08]. Logs [IK03, I06]. Login [LL05c, CCK04b, CJT01]. Logist [KJ01]. Logo [LAH09]. London [Pag03, Top02]. Long [ABRW01, O01, Eva09, GSW00, Gro03, PC01, Zhu06, BM06, ISO05, LG04, SGMV09]. Long-Lived [GWS00]. Long-Term [ABRW01, O01, BM06, ISO05, LG04, SGMV09]. Look [Bon07, Has00, Lu03, Sye00, H06b]. Look-up [Has00]. Looking [ASW+01, An01j, Cla00b]. looks [Nis03a]. Lookup [MFT05]. loop [KVN+09]. loop-level [KVN+09]. Loopholes [S01]. Lorenz [G00, Sal00a]. Lorenz-based [G00]. Losing [Sta05]. LosLobos [Pri00]. Loss [H05, BC05b, Mit00]. Lossy [AIP01, HSKC01, PW08, As04a]. Lost [PY06, Rob02, Rob09]. Lösung [An04c]. lot [Cla00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [Q50]. Louvain-la-Neuve [Q50]. Low [An00d, BM01b, CH07c, GST04, HNZ02, HGR07, J02a, KMB09, RH03b, RMH03a, SU07, SHJ04, SZ01, WC01a, CL09, CO09b, Fan03, HLL03, LG04, SL05c, SK03, WLH05, W06, WY05, ZYW07]. low-computation [Fan03, LC04a]. low-cost [CL09]. Low-end [SU07]. Low-Exponent [SZ01]. Low-overhead [HGR07]. Low-Power [An00d, JP02a, KMB09, CO09b, ZYW07].
Low-State [GST04]. Low-Weight [CH07c].
Lower
[BDF01b, BP03b, DIRR05, GT00, GKK03, PS02a, Shp03, WW05, KS05b, Shp99]. LSB
[CS05c, FGD01, WMS08]. LSB-encoded [WMS08]. LSD [HS02a]. Lu [QCBO5b].
Luby [MP03, Pat03a]. LUC [LNS02]. Lu [QCB05b].
Luminy [PPV96]. Lumpur [DV05]. Lund
[Joh03]. lurk [Rie00]. LUT [CC02a, TL07].
Lund [Joh03]. lurk [Rie00]. LUT [CC02a, TL07].
LZ [AL04]. LZ-77 [AL04]. LZSS [CFY+10].
LZ-77 [AL04]. LZSS [CFY+10].

M [DNR03]. M8 [TM01]. MA
[ACM10, JQ04, Kil05, KP01, Nao04, Pag03]. MAC
[BKN04, CM00, Ki03, LPV+09, Vau01, Kra03]. MacDES [CM00].
Machine
[LBA00, Mal06, Pro00, Cas06, Kid00, Pau02b, SWR05, WQ08, Win05b, HM01a, Pet08].
Macraigor [An002d]. MACs
[BPR05, BR00b, BM01c, Sen00]. Made
[Ste05b]. Madison [FMA02]. Maelstrom
[MYC01]. Magic [DNR03, GHL04, Bur02, GP00, Hro09, An001k]. Magyarik [jVNP06].
Mail
[ANR01, Cos03, KS00a, Law05, Che01f, LL04c, NZS05, Smi03, All06]. mails
[LG09]. Mainframe [Web08]. mainstream
Maintenance [NABG03]. Maiora
[Car02]. Majesty [Bud06]. Majority
[GKK07, SV08b]. Make
[BP06, Ber03, Sin02]. Makes [Pau09, Pal02]. Making
[Che07b, CRSP09, Gar01, Lut03, Mit00, Mul02, Oec03, Per05a, Wri05].
Malaysia [DV05]. Malaysian [Kha05].
Malicious
[HLC08, SZ03, YY04, Tsao06]. malleable [DW09, FF00, PR05]. Malware
[HL07, SZ03]. Man [Gen04a, Urb01].
Man-in-the-Middle [Gen04a]. Management
[ACM03a, ACM04a, Ano02d, Ano02c, BP07, BW07, ELvS01, FMA02, GKO4, Gut04b, KB06, Linn0b, Mit02b, Scro1, Sha02,
TMM01, Woa00, Wya02, ASW00, AJ08, AFB05, CG06, Cha05a, Dea06, GTY08,
ISO05, Jan00, JW06, KHYM08, KAM08, LMW05, LPM05, LR01, LK01, MKKW00,
Neu06, Pot06, RH03, SJR01, Sen03, Sina06, Smi08, UP05, Woa05, You04]. manager
[KH03, Sha01a]. Managing
[MA00a, MA00b, NDJB01, Oue05, PTP07,
PB02, Tot00, BJ02, Kov03, KH03].
Mandrake [TvKB+01]. MANETs
[STY07, DF07]. manipulation [SFR05]. Manuscript [GG05a, Rug04]. manuscripts
[MAA10]. Many
[BB02, Di 01, MP03, Di 03, SVD07]. Many-Round [MP03]. many-to-one
[SVD07]. Map
[XYYYY11, KJ01, Lee04a, PC05b, SL09].
Maple [Cos03, TT00]. mapping [Tan01].
Maps
[BGLS03, BMS03, CL04a, LLL+01, WP03, JK01b, MA02]. Maqasid [MjA05].
Marcell [Ir03]. March
[BDZ04, Bir07, Bla06, HR06, PY05, S101,
Uni00g, Uni00h, Ytr06]. Marian [Kap05].
Marjan [BCB+05]. Markers [FBW01].
Market
[Bar00a, An001i, Neu06, Swi05].
Marketplace
[PLW07, VN04]. Markov
[KW03]. Marks [An001c, YSS+01].
Markup
[Uni00a, Uni00d, Uni00e].
Marrakech [EE09a]. Marriott
[USE01b, USE01a]. MARS
[BF00a, BCD00, Fer00, IBM00, IK00,
KK00a, KS00b, KKS01, SOD00].
MARS-like [BCD00]. Maryland
[REN01, Ros00b, Sin99]. Maryland
[ACM05b, ACM05c, ACM09, SMP+09,
GL05]. Mash [An08a]. masked
[AHS08, Lao08a]. Masking
[CHJ02, CT03, GK02, Lav09].
Massachusetts
[EE05b, USE01b, USE01a, IE03]. masses
[Pot06]. Massive [An011]. massively
[FP00]. massively-parallel [FP00]. Match
[JH00a, WC04, LL06a]. Matching
[ABM08, Len01, UBE09, Voi05].
materialized [MSP09]. Materials [SLT01].
Math [SR06, McNo3]. Mathematical [AUW01, Cas06, FF01b, GL05, HPS08, Kat05b, You06, GKS05, Hi05, Sin09].
Mathematics [BP06, Lew00, Nie02d, Wal00, Gar04, Sch00a, Sch01c, S+03, Sch04a, Sch04b].
Mathématiques [RSA09b, PPV96].
Matrices [TL07, CFVZ06, LMTV05].
Matrix [CV03, BF06a, OS07].
Matroids [CDG+05].
Matsumoto [DDG+06, YG01a].
Mature [Tro08].
Max [Di 01].
maximal [H¨uh00, HJW01].
maximizing [GSK09].
maxims [Bau00, Bau02a, Bau07].
Maximum [KMT01, ZC00, DW01].
May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bi03, CC04a, Cra05a, DRS05, IEE01b, Knut2, KN01, MJ04, MS05a, PM00, Pfe01, Pre00, TLC06, Unio00f, Unio00c, YKL02a, Pan02a, Y00].
Mbp [LMP+01].
McClure [Gum04].
McEliece [CFS01, KI01a, KI01b, Loi00, LS01c, Sun00b].
McEliece-Based [CFS01].
McEliece [Car02].
McGraw [Gum04].
McGraw-Hill [Gum04].
MD4 [DG02, WFLY04].
MD5 [Ano09c, Eke09, For09, WFLY04].
Means [LMHCTR06, Nis03a].
measure [Lav09].
Measurement [Ano02e, k01, C009b, FXAM04, RW07].
measurement-based [FXAM04].
Measures [CB01, Q01, GSK09].
Measuring [Si06].
Mechanisation [Bel01].
Mechanism [Eva09, LXM+05, WY02, CL08, CL04, GH08, LCP04, ME08b, RFR07a, RFR07b, RFR07c, WA00].
Mechanisms [BACS02, CJK+04, Her09b, Lin00a, MD04, Mir05, Pip03].
mechanized [dH08].
Media [And08a, Hei07, CBB05, Ano02d].
media-streaming [CBB05].
Median [Cap01].
Mediated [DT03, CG06].
mediator [SBG05].
mediator-free [SBG05].
medical [AL07].
Medicine [MYC01, Moo01].
Meet [Cla00a, HG07].
meet-in-the-middle [HG07]. meeting [Jef08].
Meets [Way02a].
Melbourne [IZ00].
Member [CTH08].
Membership [NBD01, Fis01a].
Memoir [Bar05].
Memorable [KOY01].
Memoriam [DNRS03].
Memory [AK03, AJ08, BS00b, CC05, DK08, DGN03, HN01, KCJ+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YG05].
Memory-Bound [DGN03].
memory-safe [Oiw09].
Memoryless [Sar02].
MEMS [ECG+07].
MEMS-Assisted [ECG+07]. ment [CAC06].
menu [Mea04].
Mercy [Flu02a, Cro01].
Merkle [CDMP05, JLS03].
Mersenne [Ano03f].
Mesh [LP06, ZT05, KB09, LZ+04, YPS01].
Meshes [BGI08, Lav09].
Message [BK00, BR02, BWL02, BDF01b, CV03, Cocc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SN04, Z03, Z01, BPS08, CCH05, CJ05, Gav08, HW05, Kar02, MD04, MS09c, Sha04b, TJC03, Wu01, ZF05, ZAX05, ZCW04].
Messages [Ara02, AR01, BR00b, CHJ+01b, DS05b, Sch09, Wri05, Zho06, Al00, An008c, BCG+02, Bi02, BB79, L09, SP79].
messaging [Opp01, RR05].
meta [SM08, PL05a, QCB05b, Sha05d].
Meta-He [PL05a, QCB05b, Sha05d].
meta-learning [SM08].
metadata [CD07, FJ04].
metamorphic [CST05].
Metaphor [CNB+02].
Metering [BC04b].
Method [BDTW01, GHK+06, GL00, Gro01, HRS02, HQ05, JKK+01, LL02, Mi02, OKE02, OT03a, OT03b, SOHS01, TIGD01, TSO00, WH09, WNY09, ZL05, ÅR04, DwWmW05, Gutt04c, JL03, SM09, MFK+06, W02, WHT08, kWPLW01, WLI04, YC09c, YCL07, CHJ+01a].
Methodologies [SPMS02, 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 [CdVSG05]. military [Ark05]. Million [Ran55, Ran01, Ano03a]. MIME [Dav01b, Dav01c, LG09, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [FBW01, FGM001, 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, SBB05]. Misinformation [CZB+01]. Missed [TvdKB+01]. MIST [Wal03]. Mistakes [Ste05b]. MISTY [KYHC01, Küh01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Küh02b]. Mithra [Fre03]. Mitigating [LND08]. Mix [JJ00a]. Mixed [SKR02]. Mixes [Möl03a]. Miyazaki [WHLH03]. MMM [GKS05]. MMM-ACNS [GKS05]. Mnemosyne [RH02, HR02]. Mobile [Cha05a, CFRR02, Dim07, GN06, JP02a, KZ01, KB07, KC02, KHD01, LCK01, Mal02, MM02, PL01, RKZD02, RsS01, RC01, Rot01, SH00, ZYM05, CC05c, CJ03b, CF05, CF07, DHMR07, HP00, HYS03, sHCP09, ISTE08, KVD07, KXD00, 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, CLK01a, CS07c, CPhX04, Cli08e, CT09, DPV04, DFSS08, Din01, Din05, ECM00a, Gra02b, HLC08, KLN+06, KW03, LJL05, MND+04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SFDF06, TZDZ05, Vad03, WC05, WT02, WvD02, ZGLX05, ZP05, ZS05, Bkw03, CUS08, CDD06, Dan00, DFSS05, GMR08, HILM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SRJ01, TP07, DY09a]. Model-Based [Sal05b]. Modeling [AADK05, CDD+05, HmvdmLM07, KS05a, ZP05, Lf00, SS04]. modelled [BG08]. Modelling [HCDO02, JP07, Puc03]. Models [Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01b, SC02b, vOT08]. Modern [Gol09, Mao04, Pag03, SM07b, Swe08, Bud06, Fur01, IM06, KLO8, Mol05, SE01, Lut03, Lec03b]. Modes [DGH*04, Dwo03, GD02, Gol01e, HSH+01, JMV02, JKRW01, Jun01, KY01a]. Modified [CHC04, HPC02, JY01, K101a, ST02, Che08a, CJT01, HWWM03, LL04a, LL05a, kwpLwW01]. modifying [CSV07]. Modular [BIP05, BKP09, CMJP03, CH07c, Dhe03, FP00, Gro01, Haa06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wal01, WL04a, HSD+05]. Modulation [AS01c, Che07a]. Module [Ano02d, LM00, SGM09, ARJ08, BG09, Jan08b]. Modules
[FIP01b, NIS01b, GJJ05, JEZ04, Sei00b].
Moduli [Bai01b, GMP01b, Wal01]. Modulo [ACS02, Gon06, Gro03, MFFT05, Zhe01, Wan05].
Modulus [Ano01o, CGH00a, CDL00,00, SZ01, WY02, WS02, LKYL00, WTH08].
Modulus-Based [WY02]. Mollin [Kat05b].
MOM [DJLT01]. MONA [KMS01].
Mondriaan [BF06a]. Money [Ano01a, YKMY01, JP06]. monitor [MK05a]. Monitoring [AK02a, BCS02, Por06, Bej06, GXT08, ZGTG05]. Monitors [JT05].
Monks [Eag05, Kin01]. monoalphabetic [GPG06]. monolithic [GHdGSS00]. Monotones [WW05]. Monsters [And08a]. Monte [Bi09, 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, Tya05].
Mothballed [Bar00c]. Motif [Bi09]. Motion [EFY05, hKLS00, WMDR08]. Mountain [JYZ04]. mouse [HLwWZ09]. move [Jac00]. movement [HLwWZ09]. MP [MP07]. MPG [DRL09]. MPEG [LH05, MLC01, SG07, YZDW07].
MPEG-4 [SG07]. MRF [Che01a]. MRN [TID01]. MSP430x33x [GBK01]. MSXML [TEM01, Hei01]. Mu [CJT03].
Much [Che01d, Con09]. Multi [ARR03, Multi-designated [LV07]. Multi-Domain [CJK04]. multi-factor [BSSM07]. multi-hop [NC09]. multi-linear [LLL04]. Multi-party
[CMM00, CDG05, FGM001, FW04, HMM01, LLL04, CLOS02]. Multi-property-preserving [BR06].
Multi-Proxy [ZJ09, HCO4b, LW05c, TY04]. Multi-Receiver [CCD07]. Multi-recipient [Kur01]. multi-scroll [HHYW07].
multi-secret [CC05a, CY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server
[Tsa01, LHL03b, Tsa08, TWL05]. Multi-Servers [HS07]. multi-signature
[HWH05, HC04b, HL04, LCZ05b, LW05c, TY04]. multi-stage [CY05b].
Multi-trapdoor [Gen04a]. Multi-user [BBM00, DY09a, GMS02]. multi-valued
[DZL01]. Multiagent [ZS05]. Multiagent-Based [ZS05]. multibit
[TND09]. Multicast [AIP01, BPS00, BDF01b, ASW00, Asl04a, CBB05, GIKR01, GL06b, JA02, KB09,
MP08, PCS03, YC08, ZCW04].
Multicollisions [Jou04]. Multilevel
[LN04]. Multimedia [AAK09, FMS05, GA05, HL07, LLRW07, SM05, WLL09,
DY09a, DKU05, Lf00, Ren09, SG07, YC08].
Multimodal [PY08]. Multipartite [HR03].
Multiparty [BC02, BGOY08, CDF01, DNO3, D05, GIKR02, OZL08, PMRZ00,
CDD00, HT04, IKOS07]. multipath
[S05]. Multiple [A01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, DK05,
Har00, HZSL05, HLT01, Bab01, STK02,
SR06, TID01, BLH06, Che04a, CJ04,
DM07a, HL00, KCO9a, M14, Sha01d,
SW05a, TCC02, YW05, YSH03, YRY05b].
multiple-key [Che04a, CJ04, SW05a,
YW05, YSH03, YRY05b].
Multiple-Precision [HZSL05, MN14].
Multiple-watermarking [Che08b].
Multiples [HR00]. Multiplication
[AHRH08, ADDS06, BKP09, CMJP03, CH07c, Dhe03, GLV01, HM02c, KKIM01, Mol02, NMSK01, OS01, Tan07a, Wal01, BINP03, DwWmW05, FP00, GD05, Has00, Mis06]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KO03, MFFT05]. Multiplier [HKA+05]. Multipliers [CMJP03, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMH03a]. Multiply [KTT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver [HSZI01]. Multiresolution [hKLS00, YPSZ01]. Multiset [aSM01]. Multisignature [Tad02, CWH00, CL04c, CCH04, He02, LWL09, VMC02, YC01, ZHY03]. Multisignatures [CL00, WH02b]. Multithreaded [Zha00]. Multivariable [DS05a]. Multivariate [DY09b, BGP09, FP09]. Municipal [MJF+08]. museums [Six05]. Music [MNS01, XMST07]. mutargima [MAaT05]. Mutation [Lut02]. Mutual [JP02a, KH05, CCS08, SW06, VK08, YWWDO8, YCO09b]. Mutually [WC01a]. My [Che05b]. MYCRYPT [DV05]. mysterious [Bel07a]. Mystery [GG05a, Rug04]. Myths [GO03, kc01].

N [Mar05a, AOS02, KOMM01]. NAF [OT03b]. Names [Coo01a, Sha02, Ark05, CGV09]. Naming [Ano02b, BH00b]. Nanotechnology [RR03a, RR03b]. Naor [Zha06]. Napoleon [Urb01]. narrowed [Sch04d]. narrowing [MT07]. NASA [Ano02c, Wil99]. Nation [Lan04a]. National [BWE07b, Jo01, LCS09, AJ08, Bam02]. National-Scale [BWE07b]. Natural [ARC+01, Top02, WMS08]. Nature [Pag03]. Naval [LBA00, Goo00]. Nazi [Han06, KS04]. NC [AIK04]. nCipher [Ano03g]. NCP [SQ01]. NCR [LBA00]. Near [BC04a, DPS05]. 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, CAC03, CAC06, Sta05, Raj06]. Newton [KT06]. Next [ESG+05, McL06, TV03, Van03, Web08, BD04b, ISTE08, RR03a, Ros04].

Next-Generation [ESG+05, Web08]. NFA [DIS02]. NFS [Sta02b]. Nice [DS06, JJ00c]. Nimbus [Fur02a, Mac00]. Nice [DS06, JJ00c].尼克 [Ano03g]. Nimbus [Fur02a, Mac00]. Nice [DS06, JJ00c].尼克 [Ano03g]. Nimbus [Fur02a, Mac00]. Nice [DS06, JJ00c].尼克 [Ano03g]. Nimbus [Fur02a, Mac00]. Nice [DS06, JJ00c].
NTRUSIGN
[HHGP+03, HHG06, HWH08, ZJ09].
NTRUSign-Based [ZJ09].
Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Die03, DGP07a, DGP07b, DV08, Ego05, EHk+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05a, Kel05b, Ket06, KM01b, LMHCETR06, LNS02, MNP01, NR04, NNAM10, RSN01, SP05, Sch06b, Shp99, Shp03, SFDF06, TWNA08, TL07, TZT09a, TZT09b, Vav03, Wal00, Yan00, YKLM02b, Aam03, AUW01, BS02, BK07, Bel08, BGPGS05, BG08, BG09, BG07a, BGL+03, CFY+10, CNPQ03, DIM08, DGP09, FP00, HG05a, HGNS03, HLwWZ09, HP01, JAW+00, JL03, KH08, KSF00, Kin01, Lam01, LGKY10, MFK+06, SS03, Shp05, Tip27].
Number-Notation [Eag05, Kin01].
Number-theoretic [NR04].
Numbers [BCGH11, GH04, HSR+01, HBF09, Ifr00, MN01, ST03b, AG09, CW08, KB39, Kir01b, MKF+06, SS03, Shp05, Tip27]. numeric [AKSX04]. Numerical [WWL+02]. numerically [Sav04]. Numerous [CC08].
NURBS [Ben00]. NUSH [WF02]. NY [HR06, IKY05, KJI05, Sch01d, YDKM06, Ano011, NIS00]. Nyberg [Ara02].
O [Kat05b, Puc03]. OAES [Man01, BF05, BF06b, Bon01, FOPS01, Sho01].
Obfuscated [NS05b]. Obfuscating [BGI+01]. obfuscation [CT02]. Object [RSA00e, DHL06, MMW01, ST06]. object-oriented [DHL06, MMW01]. Objects [CCM05, ZTP05, PB01, WHI09]. Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GKM+00, KKL09]. obscurity [MN03]. Observability [JQYY01]. observers [JL04]. Obstacles [KM04a]. Obtaining [Bar06b, BP03b]. OCB [RBB03], occur [Web02]. Ocean [MYC01].
October [AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, KCR04, LST+05, TTZ01, USE00b, ZYH03]. Octopus [Cl00b]. Oded [Lee03b]. odyssey [Gol08]. 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, VW01]. Offs [PS01c]. OH [BD08], oil [RD09]. Old [Eva09, Lov01].
On-Demand [SEF+06]. On-Line [Lu02, BCS02, Luk01]. One [AK02a, BYJK08, CHL02, Che03, DIS02, Di 01, DW01, DMS00, Fis01b, GKK+09, HNO+09, HM02b, HR05, KO1a, KO03, KO00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00e, Uni00b, XYXYX11, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, Di 03, DS02, GKK+07, HR07, HRS08, HLT09, JZ09, KK07, KKKP05, KKK, LW04, LPM05, LQ08, LC04a, Mf02a, Poi00, SVDF07, SV08a, SW05a, Tsa08, YW05, YRY05b, ZW05a]. One-Dimensional [XYXYX11]. One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLT09, LC04a]. one-variable [SV08a]. One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KKK, LW04, LPM05, LQ08, Mf02a, Poi00, Tsa08, YW05, YRY05b, ZW05a]. One-Wayness [KO1a, PV06b]. On-going [Sam09]. Onion [CL05].
Online [BDF+01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAY09, Voit05, FNRC05, Fox00, Pan07, Tyn05, PT08].
Online/Offline [ST01b]. Only
Pad [LDM04, DS02]. Padding [AR01, BCCN01, CKN00, CJNP02, KO03, LS01a, Man01, Vau02]. PadLock [Lud05]. PadLock-wicked [Lud05]. Page [IEE00b]. PageRank [GPC08]. pages [Fal07, Rot07]. paging [SZ08]. Paillier [CGHG01, DJ01, NSNK05, ST02]. Pair [WCJ09]. Pairing-Based [BKLS02, GPS06, KM05, LXH07, PV05a, Sma03a, GPS05, Lee04a, PC05b, VAVY09]. Pairings [Bon07, BH07, Bon07, BGH07, Jou02, SB04, ZK02, CJL05, DSGP06, LWZH05, LC05b, SW05a, VK08]. pairs [LYGL07, Slhp01]. Pairwise [CLL00, FM02a, HMvdLM07]. PAKE [HTJ08]. Palm [BDhKB09, WPS01, Wil99, Ano02d]. Palmprint [KZ09]. PAM [FR02, Sei00b]. Panama [BDPV09]. Panel [FL01b]. Panopticon [YN01]. Paper [CC09, MFS88, 09, Pet08]. Papers [Ano04b, Ano07b, Ano07a, Sch00b, Ytr06, Wil99, Bla03, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GH05, Joh03, Jue04, KKP02, KCR04, LL03, LLD04, MS05a, Mat02, MZ04, NH03, PK03, PT06, RM04, Sil01, AMW07, Al01a, Bir07, BC05c, Czo05, CKL05, DR05, HH04, HH05, PC05a, PY05, WK06, Wri03]. Paradigm [BN00a, CS02, Go03, KD04, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Paradise [USE00b]. Paradox [Che01b]. Parallel [ARHRO8, App07, AEMR09, CPHX04, CTL01, CNPQ03, CNB602, Dam07, DM00b, JL08, KY02c, Lin01c, MFS809, PS04a, RMH03b, SS01a, BF06a, FP00, MRT10, OS07, RMPJ08]. parallelism [KVN99]. Parallelizable [BR02, Mol02]. parallelizing [Fis01a]. Parallelizable [LKK03a, LKK03b]. parameter [Wue09]. Parameterizable [KPMF02]. parameterization [LZP+04]. Parameters [ZLK02]. Parametric [Vir03]. Paranoid [Bau01a, Bau01b, Bau02b, Bau03a, Bau03b, Gu05, Oue05, Sto05a, Luc06]. Parascript [Ano02a]. Parasitic [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Paris [ACM04a, GH05, KN01, NV02a]. Parity [DRL09, KKG03, You01, BKW03]. Parity-Based [KKG03, DRL09]. Park [Cop05, Cop06, Cop10, HS01a, Sal00b, Sal05a, SE01, Sm01b, Wei06, Win00]. Part [Har01a, Har01b, ISO04, ISO05, Puc06, Tr009b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05]. Partial [BMO3b, Cor02, Her06, ABHS09, CP07]. Partial-Domain [Cor02]. Partially [AO00, MSP09, Bau04, Bau03, HC04a, HY03, HLL03, WL05, WHH05, WY05, ZC05]. Participatory [CTBA01]. parties [LKY05b]. Partition [CTH08, WJP07]. Partitioned [DN04]. partitioning [BF06a, Che07a, partitions [Sav04]. Party [KO04, Lin01c, MR01a, WW05, WV01, CLOS02, CLC08, CDG05, FGMO01, FWW04, GCKL08, HM01b, JW01, LHL04b, LLD04, LLS99, LSH00, YC09a, ZLX99]. Pass [SK00, MT02]. passe [Car00]. Passes [Coc03]. Passing [Vir03]. Passive [Sha01c, VW07, RW07]. Passive-Only [VW07]. Password [BMN01, BMP00, CHVV03, CPP04, CS07b, CC01b, DG03, GL03, GMR05, Har01a, Har01b, Jab01, KOY01, LSH03a, LSH03b, MPS00, Mac01, MSJ02, Ngu05, SBW01, SY06, WHL05, YS04, ZWCY02, CC01a, CC04b, CCK04b, CYH05, DG06, FLZ02, Fur05, GL06a, HTJ08, JPL04, Jua04, KLY03, KJY05, KTC03, KCL03, Ku04, KCC05, KHKL05, LL06, LW04, LH03, LC04a, Pha06, Sco04, SLH03, Shi05, WLT03, XWWL08, YY04a, YWC05, YS02, YPKL08, ZDW06]. Password-Authenticated
[BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HTJ08].

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

password-guessing [Shi05].

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

Patarin [Bih00].

Patent [MP00, Sav05a, Sav05b].

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

path-based [CCD+04].

Path-quality [GXT+08].

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

Pattern-based [BLP06].

Patterns [DD02, MP06, WCJ09, JLC07].

Pavol [Sal03b].

pay [Joy03a].

pay-as-you-watch [Joy03a].

payload [KC09a].

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

PC [BSW01, Ste05c].

PCIXCC [AV04].

PCKS#7 [Dav01c].

PCPs [FS08].

PCs [BDET00].

PDA [GW08].

PDF [ISO05, CNB+02, ISO05].

PDF/A [ISO05].

PDF/A-1 [ISO05].

Pearson [Puz04].

Pebbling [DNW05].

Pedersen [GJKR03].

Peer [Art04, HR02, RH02, ATS04, LLY06, MPH06, P106, WCJ05, Y104].

Peer-assisted [Art04].

Peer-to-Peer [HR02, RH02, ATS04, MPH06, P106, WCJ05].

PeerAccess [WZB05].

Pezina [YRY05a].

PEM [Dave01b].

Penguin [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Ou05, Ste05a].

Pennsylvania [IEE05a, IEE08].

People [ASW+01, CG05, Lov01].

perceptions [WDCJ09].

Perceptual [PBM+07].

Perceptually [EFY+05].

Perfect [AJO08, CLLL00, DN02b, DSS01, Sun00a, DM07a, SC02c, SY06, Z05].

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, CKL+09, CRSP09, GC00a, HM02a, JRB+06, LW05a, NTV07, SK03, YGZ05].

performance-friendly [CRSP09].

periodic [XQ07].

Periods [KKH03].

Perl [Sal03b].

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

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

Persistent [AGT01, ST06].

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

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

Personalised [TNG04].

Perspective [LL01].

Perspectives [BMV06, SM08].

Perturbation [HWH08, ZY05].

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

PET [MS05a].

Peter [For04, Uzu04].

Petersburg [GKS05].

petitions [Cal00b].

Petri [LKJL01, AADK05].

PGP [McL06, Ano00h, BCH+00, Dav01b, Dav01c, JKS02, Luc06, Opp01].

PGV [BR02].

pharaohs [Pin06].

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

Phase-Conjugate [Ig02].

phase-shift [Che08a].

Phil [Bar00a].

Philadelphia [IEE08].

Philip [McL06].

Philosophy [Cop04b].

phishing [Bel04].

Phone [CAC03, Fox00].

Photonic [TWNA08].

Photonic-based [TWNA08].

Photons [Bar00c].

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

Physicist [BZ02].

physicists [RP00].

Physics [MYC01, Sch06b, BEZ00, BEZ01, Dzw03].

physiological [RFR07a, RFR07b, RFR07c].

Pi [OS08].

PIC [Fin02].

pick [Cl100b].

Picks [PM00].

PicoDBMS [PBVB01].

PicoDMBS [BBPV00].

Picturing [Pau03].

Piecewise [LL+01].

Pigeon [Pem01b].

piling [Kuk01].

piling-up [Kuk01].

PIN
GH02, HQR01, HJW01, Ina02a, Ina02b, IIT03, Kan01, LMV05, LCD07, Lut03, LWK05a, 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, Lut03, 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].

pre-decryption [RSP05].

Predict [Dic03].

predictable [Bel08].

Predicting [AG09, BGPGS05].

Prediction [AKS06, SLG+05].

predictive [vOT08].

Prehistory [Ir00].

Prehistory [Ir00].

Prentice-Hall [For04].

Preparations [FJ04].

Preprocessing [BIW08, GXT+08, Mis08, VS08].

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

Preserve [NNT05].

Preserving [DN04, KS05c, LP00, M603a, YWD08, AXX04, Bro06, BSSM+07, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07].

President [Gen00a].

Preventing [Innr03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03].

Pressure [HWH01].

Pretty [vOWK07].

Prevent [FOBH05].

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

Prevention [JT05, PZ01, PZ02a, Gei03, Smi03].

Price [AS01a, Bra01b].

Primality [BT02, Che03].

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

Prime-detecting [Har07a].

Primer [KLB+02b, Lad06].

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

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

Primitives [BDFP02, CHL02, FGMO01, Golo01d, Ngu05, RR00, BDFP05, Gar05, JZCW05, RA07].

Princeton [Gen01].

Principal [ZL04b].

Principle [CZK05].

Principles [ACM03c, ACM05b, DK02, DK07, KLU05, MAA07, SB07, Sta02a, Sta06].

Print [Kra02b].

Printed [SLT01].

Printer [Bar00a].

Priority [WWL+02].

Privacy [An000i, AEV+07, BDFP01, BSSM+07, CDM+05, Cho08a, DL98, DL07, DKFX05, DN04, GS02a, GMM08, HY01, KS05c, Knu07, LP00, M005, Pap05, PB05, PB06b, Por06, PG07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YW08, Bel04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZYL05, ZSM05, MS05a, Jan08a].

Privacy-Enabled [Por06].

privacy-enhanced [ZSM05].

Privacy-Enhancing [SE09].

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

Private [AF04a, AFI06, BD00a, BMM00, BY03, BSW09, BJLS02, BGW05, ISW03, KO00, OS05, SDM06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PLJ05b, Sm02, YRS+09, ZY08, ECM00a, ECM00b].

Private-Key [BY03, KY00, PLJ05b, Sm02].

prize [Fox00, Coc02b, MNT+00].

PRNG [HSS04, Mur02, SF07].

Proactive [DS01, FM01, JS05, ZSV05].

Probabilistic [CCW02, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLMM05, Gao99, JZCW05, KY00, MRST06, PBMB01, dH08, Neu04].
Probability [KMT01, MNT⁰⁰, DLP⁰⁹].
Probing [ISW⁰³]. Problem
[AL₀₀ᵃ, AF₀₃, Cap₀₁, CU₀¹, Che₀₄ᵇ, CJ₀₃ᵃ, CGK⁰⁺₀₂, Cou₀₁, CL₀₂, DIS₀⁰, DH₀₀, FL₀₆, Gen₀₃, GV₀₅, GPP₀₈, KK₀₂, LNS₀², NB₀₀, Wāɡ₀₂, BKW₀³, CGH₀₆, CJＴ₀₄, DLMM₀⁵, HGN₀₃, Hsuo₅ᵃ, LHY₀₅, LD₀₁, Luk₀₁, Pe₀₉, Shp₀₅, SCL₀₅, WL₀₂, Wh₀₉, Yas₀₈, KM₀₄ᵃ]. problem-solving [Whi₀⁹].
Probing [ISW₀₃]. Problem
[AL₀₀ᵃ, AF₀₃, Cap₀₁, CU₀¹, Che₀₄ᵇ, CJ₀₃ᵃ, CGK⁰⁺₀₂, Cou₀₁, CL₀₂, DIS₀⁰, DH₀₀, FL₀₆, Gen₀₃, GV₀₅, GPP₀₈, KK₀₂, LNS₀², NB₀₀, Wāɡ₀₂, BKW₀³, CGH₀₆, CJＴ₀₄, DLMM₀⁵, HGN₀₃, Hsuo₅ᵃ, LHY₀₅, LD₀₁, Luk₀₁, Pe₀₉, Shp₀₅, SCL₀₅, WL₀₂, Wh₀₉, Yas₀₈, KM₀₄ᵃ].
Procedure [LY₀⁷]. Procedures
[DJ₀₆, BBK⁰⁺₀₃].
Proceedings
[ACM₀₀, ACM₀₂, ACM₀⁴ᵃ, ACM₀⁵ᵃ, AAC⁺₀¹, Bon₀₃, EBC⁺₀₀, FMA₀₂, FLA⁺₀₃, SM₀₇ᵇ, USE₀₀ᶜ, USE₀₀ᵇ, USE₀₀ᵃ, USE₀₀ᵈ, USE₀₁ᵇ, USE₀₁ᶜ, USE₀₁ᵃ, USE₀₂ᵃ, USE₀₂ᶜ, USE₀₂ᵇ, WK₀₃, Yum₀₂ᵃ, ACM₀⁵ᶜ, ACM₀⁷, ACM₀₈, ACM₀₉, AUW₀₁, AJ₀₁ᵇ, BS₀₃, Bel₀₀, B⁺₀₂, Boy₀₁, Buc₀₀ᵃ, BＣ₀₁, HA₀₀, Hon₀₁, IEE₀₀ᵃ, IEE₀₁ᵃ, IZ₀₀, Kili₀ᵃ, MS₀₅ᵇ, Oka₀₀, PPV⁰₆, Pφ₀₁, Pre₀₀, QSO₀, RD₀₁, Roy₀₀ᵃ, SMP⁺₀⁹, ST₀₁ᵈ, VＹ₀₁, ACM₀¹ᵃ, ACM₀³ᵃ, ACM₀₅ᵇ, ACM₀₃ᶜ, ACM₀⁴ᵇ, ACM₀⁵ᵇ, ACM₀₆, ACM₁₀, AL₀₆, BD₀₂⁴, BS₀₁ᵇ, Bih₀₃, BCDH₀⁹, BD₀₈, CC₀₄ᵃ, CV₀₄, Chr₀₀, Des₀₂, DFＰ₀⁶, FLY₀₆, Fra₀₁, Fra₀⁴, HR₀₆, HYZ₀₅ᵇ, IEE₀₂, IEE₀₃, IEE₀⁴ᵇ, IEE₀₅ᵇ, IEE₀⁷, IEE₀₈, IEE₀⁹ᵇ, JIＺ₀⁴, JＦ₀₈, JM₀₃, Joy₀₃ᵇ, JQ₀₄, KJR₀₅, KGL₀₄, Kim₀₁, Kim₀₂, KN₀₃, Knu₀₂, KP₀₁, KNP₀₁, KM₀⁷, Lai₀₃, Lee₀⁴ᵇ, LLT⁺₀⁴, MMV₀₆, MＪ₀⁹, MS₀²ᶜ].
Proceedings
[Men₀⁵, Nac₀₁, NP₀₂ᵃ, Nao₀⁴, Oka₀⁴, Pat₀₃ᵇ, Pr₀₂ᶜ, RS₀₅, Sch₀₁ᵈ, Sm₀₅, Syv₀₂, TBＪ₀₂, Vau₀₅ᵃ, Won₀₁, YDKM₀⁶, ZJ₀₄, Zhe₀₂ᵇ, ZHY₀₃, BCKK₀⁵, Cra₀₅ᵃ, DV₀₅, DWLM₀⁵, DKU₀₅, GKS₀⁵, IKY₀₅, Kili₀, Li₀₅, LST⁺₀⁵, Men₀⁷, Poi₀₆, Sha₀₅ᵃ, Son₀₀, dCdvSG₀₅]. Process
[Kwo₀₃ᵇ, MNT⁺₀⁰, BDFP₀², HL₀₆, MRST₀⁶, VK₀₉⁹]. Processes
[BDP₀², ALV₀₂, BDNN₀², Whi₀⁹].
Processing
[ISSZ₀⁸, KLB⁺₀²ᵇ, PCK₀₂, AA₀₈, AA₀⁴ᵃ, Ayo₀⁶, YPSZ₀¹]. Processor
[Ano₀²ᵈ, BBGM₀⁸, EP₀₅, FBWC₀², FZH₀⁵, GC₀₁ᵇ, Int₀₀, KBD₀₃, KPMF₀², TYLL₀², ST₀₃ᵃ, SHL₀⁷]. Processors
[TLYL₀⁴, CW₀₂, CRSP₀⁹, Geb₀₄, LJ₀₅ᵃ, YGZ₀₅, YLT₀⁶, ZYLG₀⁵]. Procurement
[Lad₀⁶]. produce [Zir₀⁷]. producing [SOIG₀⁷].
Process [AL₀⁶, DMO₀³]. processing [ISSZ₀⁸, KLB⁺₀²ᵇ, PCK₀₂, AA₀₈, AA₀⁴ᵃ, Ayo₀⁶, YPSZ₀¹]. Processor
[Ano₀²ᵈ, BBGM₀⁸, EP₀₅, FBWC₀², FZH₀⁵, GC₀₁ᵇ, Int₀₀, KBD₀₃, KPMF₀², TYLL₀², ST₀₃ᵃ, SHL₀⁷]. Processors
[TLYL₀⁴, CW₀₂, CRSP₀⁹, Geb₀₄, LJ₀₅ᵃ, YGZ₀₅, YLT₀⁶, ZYLG₀⁵]. Procurement
[Lad₀⁶]. produce [Zir₀⁷]. producing [SOIG₀⁷].
Products
Profile [JH₀¹, RAS₀⁰ᶜ]. Profiles
[MV₀¹, PJK₀¹]. Program [Hφ₀¹, Bec₀², GGH⁺⁰⁸, Kov₀₃, KH₀₃, CS₀⁸ᵇ]. Programmable
[Dam₀⁷, GC₀₁ᵃ, HV₀₄, Smi₀²]. Programmer
[Wil₀¹ᵇ, Bon₀⁰, Che₀⁰ᵃ, DKK₀⁷]. Programmers
[Coc₀¹ᵃ, Wei₀⁴, Gon₀⁹]. Programming
[ASW⁺₀¹, Ano₀²ᵈ, Coc₀³, LMHCETR₀⁶, Res₀¹ᵃ, Res₀¹ᵇ, Swa₀¹, Uri₀₁, AJ₀₁ᵃ, AJ₀₁ᵇ, CW₀₇, Nis₀³ᵃ, VM₀³]. Programs
[BGI⁺₀¹, Ark₀⁵, SLT⁺⁰⁶].
Progress
[KK₀⁶, KFS₀⁰, RD₀¹, Roy₀⁰ᵃ, CV₀⁴, DV₀⁵, JM₀₃, MMV₀⁶, MS₀²ᶜ]. Project
[Fri₀¹, IY₀₀, MNT⁺₀⁰, Pau₀²ᵃ, Salxx, Gon₀⁹, LR₀₁, Lov₀₁, MWM₀¹, Sha₀¹ᵃ, Coc₀¹ᵃ, Coc₀²ᵇ, IY₀₀, Pre₀²ᵇ]. projects
[Gha₀⁷]. Prolog
[Bla₀¹ᵃ, Bla₀¹ᵇ]. Promise
[Ano₀²ᶠ]. promises [Pau₀²ᵃ]. promote
[WK₀⁵]. Promotes
[Bar₀⁰ᵇ]. Prone
[MLC₀¹]. Proof
[Ab₀¹ᵉ, Abe₀⁴, AS₀¹ᵇ, Ano₀⁹ᶜ, ARC⁺₀¹, BDP₀², Cor₀², GK₀⁵, SOIG₀⁷, SPMLS₀², Tee₀⁶, BR₀⁵, Ch₀⁸ᵇ, Ch₀⁸ᵈ, GM₀⁴, HSD⁺⁰⁵, LMW₀⁵, PBD₀⁷]. proof-of-compliance [LMW₀⁵]. Proof-of-Concept [ARC⁺₀¹].
proofing [CT0₂].
Proofs
[BBM₀⁰, BP₀², CS₀², DFS₀⁴, DNW₀⁵, Fis₀⁵, Gen₀⁴ᵃ, KL₀⁵, Lee₀³ᵇ, MV₀₃ᵃ, Niel₀²ᵇ, BGB⁰⁹, BR₀⁴, Göl₉⁹, HG₀⁵ᵇ, SV₀⁸ᵇ, dH₀⁸].
Propagation \[LJL05, QPV05\]. Properties \[ABC+05, BM01c, KY01b, LLL+01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03\].

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

Proposal \[DPVR00, Mac00\]. Proposed \[Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06\]. Protect \[ETZ00, BBN+09, WK05\]. protected \[CYH05, PKH05, ZCL05\]. Protecting \[Des00c, EHMS00, WK05\].

Protection \[CGJ+02, DKFX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VP01, WY02, XFS01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, CT02, Gor05, HLC07, KA09, Kov03, Kwo03a, LL05b, ML05, NN03, Sha01c, vW01, Bro05b, LIJ04, LS05b, ZYL05\].

Proposition \[LPZ06, Qu01, Uni00h, WY02, BR06, JRS09\].

Proposal \[DPVR00, Mac00\]. Proposed \[Coc02a, GM00b, HPC02, KI01a, You01, YG01c, JK01a, ZDW06\]. Protect \[ETZ00, BBN+09, WK05\]. protected \[CYH05, PKH05, ZCL05\]. Protecting \[Des00c, EHMS00, WK05\].

Protection \[CGJ+02, DKFX05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VP01, WY02, XFS01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, CT02, Gor05, HLC07, KA09, Kov03, Kwo03a, LL05b, ML05, NN03, Sha01c, vW01, Bro05b, LIJ04, LS05b, ZYL05\].

Protocols \[AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Bor01, BM01a, BM03c, Bra01b, BL04b, CKPS01, CT08a, CCMR02, CCMR05, Chr01, CNV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, JP07, JW05, KS00a, KY03, KL08, Kra03, Kus02, MS02a, MNP01, PB00, PR08, PZHD09, Rot01, Shy02, SC01, Tee06, AA04b, AKNRT04, Bar06a, Bau05, Bel07b, BDS08, BFG08, BP05, BL06, BD04a, BR05, Can01a, Can06a, CP07, CKRT08, CWJT01, CH07a, Cho08b, Chr00, Chr01, CJM00, Coh03, CC05d, CDL06, DFG00, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV+09, LL04, LLY06, LS+09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SL05a, SR00, SW00b, SY06, WLH06, YS04, ZLX99, ZL04b, PDMS09, Puc03\].

ProtoMon \[JT05\]. Provability \[GOR02b\].

Provable \[HM02b, HLL+01, HSL+02, KSHY01, PB05, SLL+00, BG09\].

Provably \[AO00, ACJT00, BMP00, BC01, BC07, CHKO08, DG03, DG06, HLV02, HvAL09, HL07, HS07, JMV02, MS03a, NSNK05, NSS02, VMS05, WLH06, XG03, ZCL05, BKN04, CCMT09\].

provenance \[HSW09\]. Provers \[MV03a\]. Provide \[AB01, Sch01a\]. Providence \[IEE07, Si01\].

Provider \[LDM04, HILM02\]. providers \[MV03b\]. Provides \[OT03b\]. Providing \[BACS02, BCS+09a, Del07, Lin07, Par04\].

Proving \[Che03, FS01c, GN01, Tee06\].

Provision \[Kha05\]. Proxy \[AH05, BCL05a, DKFX05, LC03, LCZ05b, PL01, RD01, Sha03d, ZJ09, AFGH06, CCH04, DY09b, HW03, HW04, HW05, HC04b, KHL09, LL05b, LH05, LC05c, LW05c, PKH05, SH05, SY04, YTH04, ZCL05\].

proxy-enabled \[DY09a\]. proxy-protected \[PKH05, ZCL05\]. psBGP \[vOWK07\].

Pseudo \[BH05, FFW04, Gen00b, LL+01, LH+08, MP03, SXY01, TST09a, TST09b, WP03, XYXYX11, BG09, CFY+10, GB09, FK+06, NR04, PLsved10, PSP+08, RGX06, SH11, SM11, SL09, WW08, XSWC10, YZEE09\].
Pseudo-Random [LLL+01, MP03, WP03, XYYXYX11, Gen00b, SYX01, CFY+10, MFK+06, NR04, PLSvLE10, RGX06, SH11, SM11, SL09, WW08, XSWC10].

Pseudo-Ransom [BH05].

Pseudo-signatures [FWW04].

pseudonoise [HG05a].

pseudonym [CG06].

pseudoprimes [ZT03].

Pseudorandom [BCGH11, CDI05, DN02a, DI05, DP02, Fin06, Fhu02b, FIPR05, GM02a, IYK02, LMHCETR06, Nie02c, RSN01, Aam03, BGPGS05, IYK03, KSF00].

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

Psychology [MYC01].

PUB [Nat00].

Public [ANS05, AUW01, APV05, Ano01n, AEAQ05, AF03, BC05a, BDG01, BDZ04, Bar00c, BPS00, BBDP01, BLM01, Bih00, BDTW01, BST02, CHK03, CHK05, CDM+05, CHM+02, CHKO08, CJ03c, Chi08a, CCW02, CT09, CMC01, CS02, CS03b, DP04, DJ01, Des02, DY09b, DKKY02, DFK+03, ESG+05, ES00a, ED03, FL06, FL01b, GMLS02, GH01, GC01b, GSB+04, Gutt04b, HCD002, HR05, HG05b, HR04b, HJW01, HLC08, IEE00b, IZ00, Jou02, Kat05b, KIKIM01, KM01a, Kim01, KLY02, KKY02, KYY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, LH07, Lin03, Lin00b, MR01b, MR01c, Moi03a, Mol03b, Mu01a, NP02a, NBD01, NSS02, OTU00, PHK+01, Pei09, PR01, Poi02, PHM03, Qu01, RSA00a, RKZD02, ST01a, ST02, Sin01a, Sm01c, Ste01, TSO00, TT01].

Public [Vau05a, WZW05, WHI01, WV00, Wya02, YKMY01, YG01c, YDKM06, Zhe02a, AG09, BH03, BCL05a, BCW05, BBN+09, Ben01a, BB79, Bra01a, BD04b, Cal00b, CCT08, CL02b, CWH00, CCH05, CJ05, CTR08, Cho06, Cre00, DMT07, EKRMA01, EKKH04, FMY02, FP00, G02, GH08, GKM+00, GS01, Gor05, GMW01, HCD08a, HCD08b, HH06, HW04, HL04, Iwa08, IM06, Jan08b, JXW05, JZCW05, KPS02, Kob00, KW00, Kos01c, LF03, LHL04b, LKY05b, LCK04, Lin01a, LLW08b, LS01c, Lop06, LWK05a, MS08, Mü01b, PI06, PC09, SNI00, SRJ01, Sha04b, Sha05b, Shp04a, SLC05, Sun00b, SZP02, SC05c, TO01, TLM05, Tsa05, TJC03, VS01, WDLN09, War00, Wu01, WH03, WL04b, hY08, YRJ+09, ZSM05, AL06, BDZ04, Ben02, CZ05, Des02, GL05, KGL04, Kim01, NP02a, Vau05a, YDKM06].

Public-Key [Ano01n, AEAQ05, BC05a, BBM00, BBDP01, BLM01, BST02, CHK03, CHK05, CMC01, CS02, CS03b, DP04, DJ01, Des02, DY09b, DFK+03, ESG+05, ES00a, FL06, GH01, GC01b, HR05, IE00b, Kat05b, KIKIM01, KM01a, KLY02, KKY02, KYY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, LH07, Lin03, Lin00b, MR01b, MR01c, Mü03a, Mol03b, Mü01a, NP02a, NBD01, NSS02, OTU00, PHK+01, Pei09, PR01, Poi02, PHM03, Qu01, RSA00a, RKZD02, ST01a, ST02, Sin01a, Sm01c, 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 [MKP09].

Purpose [Ano07b, Ano07a, ESG+05, GS07a, GPP08, SGK08, LJ05a].

Purposes [LS05a, FSVG01, PBV08].

Push [Pau03].

puzzle [LF03].

Puzzles [Ano01f, ANL01, CHS05].

Q [BFMR02, CH01b].

Q&A [Str01b, Win01].

QCQC [Wil99].

QCQS
[Wil99]. QDSL [CUS08]. QNX [Ano02d]. QoS [JKRW01, Zea00]. QoS-aware [Zea00]. QSIG [ECM00b]. QSIG-WTMAU [ECM00b]. Q'tron [YC07]. QUAD [BG09]. Quadratic [BT02, Cooc11, CJS05, CCS08, HM00, Hi00, HP01, LD01]. Quality [BW07, TL07, DMSW09, GXT'08, KC09a, WWTH08]. quality-conscious [DMSW09]. Quantifier [KS06b]. Quantifier-free [KS06b]. Quantitative [Bai08, ME08a]. Quantization [DRL09, WC04, WC05]. Quantum [AC02, ATSVY00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL+05, BBD09, BZ02, BBB+02, BB03, BGM09, BLMS00, BEM+07, C03, DFS04, DPs05, DFS08, Das08, DMS00, E104, Ett02, GKK+09, GH02, GW00, GRTZ02, HV09, Hay06, Imr03, Inao2a, Inao2b, Kak06, KKL+02b, LB04, LW05b, Moot07, NA07, OTU00, Pal02, PC09, Pot05, Rec01, RK05, Ser06, SR07, Sti11, T001, Wi99, Wrio00, YI00, YI01, ZLG01, ABW09, Ano03g, Ano06d, BYJK04, BCG+02, Ber09b, BEZ00, BEZ01, BLRS09, DFS05, Duw03, Eke02, GKK+07, Gav08, Heg09, HG06, IM06, JZ09, JRS09, JAW+00, Joy00, KKH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Ros00b, Sin99, Sin00, Sm06, UHA+09, BZ02, BD08, BBD09]. quantum-storage [DFS05]. quarter [Kob00]. quarter-century [Kob00]. quarters [Cla00b]. QUARTZ [PCG01]. Quasi [MD05]. Quasi-Pipelined [MD05]. Quasigroup [MSNH07]. Québec [ACM02]. Queen [Rec01, Ros00b, Sin99]. Queenstown [Zhe02b]. queries [CKK03, F01a, GCC08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC+09]. Query-preserving [GA03]. querying [FJ04, UG08]. question [OC03]. Questions [Ett02, J00, J00]. Queues [WWL+02]. queuing [CUS08]. quick [Dew08]. R [Che05b, Kat05b, Pag03, Spr03, Bih00]. R&D [Mau05]. Rabbit [BVP+04]. Rabin [Bon01, Gen04b, Miy01]. race [Hi05]. Rackoff [MP03, Pat03a]. radar [GG05b]. Radiations [S09]. radical [Web02]. Radio [Sak01]. RadioGatún [BDPV09]. Radix [HKA+05, JY01]. Radix- [HKA+05, JY01]. rails [Fox00]. Rainbow [DS05a]. Raises [MP00]. Raising [Cos03]. ramp [IY06]. Rampaging [Coocb]. Random [Abe01, Abe04, BTO3, BK06a, BF05, BB04, BL08, CTO90, Choi08e, Die03, DGP07a, DGP07b, DV08, EHK+03, Gra02b, GPR06, HSR+01, HBF09, Int03, JRR09, Kel05a, Kel05b, LLL+01, LM02, Lys02, MP03, Mir02, NT005, NNN10, Nie02b, Pas03, Pat04, Ron05, Ran01, RSN+01, SFDF06, Tyna08, TL07, Tip27, TZZ09a, TZZ09b, Vav03, VKS09, WP03, XYZYX11, BK07, Bel08, BG08, BG07a, BGL+03, CFY+10, CJO06, CO09b, DGP09, Fis01a, GVC+08, Gen00b, GB09, HC05a, Hlws09, HmdLM07, JAW+00, KH08, KB39, KG09, LGK010, MI09, MRT10, MFK+06, NR04, Pap07, PSC+09, PLs06, PSLM07, PSP08, PC00, Reg05, Reg09, RG09, RGV06, SH11, SN11, SS03, SXY01, SR07, Sti11, SK01b, Sug03, SLO9, UHA+09, WW08, XSWC10, YZEE09, BH05]. Random-Error [LM02]. random-self-reductions [Fis01a]. Randomized [Sem00]. Randomization [Hro03, WH05]. randomization-enhanced [WH05]. Randomized [Sem00, Hro05]. Randomness [DD00, DD04, DGH+04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, MS10, SB00, Sun00a, BNN+09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03]. Range [CW09]. Rank [Sun00a, DW01, Sin02]. Ransom [BH05]. Rao [ZYR01]. rapid [OP01b]. Rate [KT01, L0Z9, PS02a, Sun02]. Rates [GH02]. Ratio [Di01]. Rational [HT04].
Relaxed [Ano00c].
Relaxing [CKN03, PS05].
Relay [DM07b, Zha00].
Released [CHK08, Mao01, HGNS03].
Reliability [IKP+07, WK05].
Remainder [Sch01b, YKLM03].
Remarks [BCW05, CL04d, SCS05c].
Remedies [FZ06].
Remote [CJT02, CWR09, Kra02b, LL05c, Rub01, TK03, WKB08, CC01a, CL04d, CJT01, DSGP06, FCZ05, Hsu05b, CV05, CKRT08, DM07a, GMG00, PM08].
Removal [LLS05a].
Removing [JL00].
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, JLY01, RN00a, RN00b, ZLK02, BDSV08, BA06, PS04a, SWR05].
Representations [OSSST04].
Representative [CTBA+01].
Representatives [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Republic [MJ04, dL00].
Republicik [dL00].
reputation [HL04, LSA+07, SC05c].
reputation [KNS05, RCG+05].
reputation-systems [KNS05].
Request [RSA00b], require [SV08b], Required [Sun00a, Lov01, Wan05].
Requirements [FIP01b, HWH01, Kin02, NIS01b, Mea04].
Rescue [ASW+01].
Research [Pip03].
Research [AJ01b, CZ05, CZK05, DFPS06, KGL04, LXM+05, RC06, Sch00e, TMMM05, DFCW00, JXW05, MH09, QS00, DCdVSG05].
Researchers [Ano08b, Ano08c, Pau02b].
Resettable [DV04, MR01b].
Residues [Coc01b, Zhe01, CCS08].
Resiliency [Joh00].
Resource [MRL+02, Tse07].
Resource-Constrained [MRL+02].
resource-limited [Tse07].
Resources [Gutxx, You04, FOP06].
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, KMZ03].
Retraining [dLC07].
Retreat [FKSW00].
Retrieval [BIM00, KO00, RE02, Yek07].
Retroactive [DBS01].
retrofitting [CGL+08a, CGL+08b, CGL+08c].
reunion [LBA00].
Revealed [Gal03].
Reversals [Cap01, DIS02].
Reversal-Bounded [DIS02].
Reversals [MS02e].
Reverse [Coo02, EC05, Wue09].
reversibility [SK09a].
Reversible [Gal03].
Reversing [EC05, YWC08, YN01, CDFM05].
Review [And04, Ano02i, Duw03, Ead05, 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, CJNI02, CS00, CS03c, CD01b, DK01, DT03, Dujo08, Dujo09, 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, MPCS00, MLM03, Man01, May02, May04, Miy01, MP01c, NZCG05, NZS05, NS01b, Ols00, 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, XCO5, Yan07, hY08, YKLM02b, YKLM03, YPKL08, YY00, You6, ZCO9, Zhe01, ZWCOY02, dW02]. RSA-based [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLLL03, NZCG05, Sei05, WLHH05, WY05, YPKL08, YY00]. RSA-Encrypted [CD01b]. RSA-Primitive [ST01a].

S [BZ02, Kat05b, Puc03, Bih00, BCDM00, Dav01b, Dav01c, FM02b, JmDxGxm05, LG09, Opp01, SMTM01, ZCO0]. S-Box [FM02b, SMTM01, JmDxGxm05]. S-boxes [BCDM00, ZCO0]. S/MIME [Dav01b, Dav01c, LG09, Opp01]. SAC [AMW07, HHI04, HHI05, MZ04, NH03, PT06, HSR+01, HSS04, ST01d, VY01]. SAC'99 [HA00]. SAFE [Un00a, Uni00c, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Oiw09]. Safe-Prime [ACS02]. Safeguard [LXM+05]. Safeguarding [Sty04, Bar03]. safer [Ano00f, NPV01, BDD03]. safety [HM01a]. SAFKASI [WAF00]. Saga [Eva09]. Salomon [Pap05]. Salsa20 [Ber07, Ber08]. Salt [PKBD01]. Salzburg [DKU05].

Samba [BH00a]. SAML [RR04]. Sanss [KGL04]. sampling [WW06]. sampling [KB39, Sug03, Tip27]. San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Oka04, Pol06, Pre02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c, sanity [Sko03]. sans [Car06]. Santa [Bel00, Bon03, Fra04, Kilo01a, Men07, Sho05a, Yun02a]. Santiago [BS03]. Sanxin [LSZ05]. SAR [B02]. SASAS [BS01c]. SAT [KLN+06]. Satan [Mea04]. satellite [CC05c, HYS03]. Satisfy [PHM03]. satisfying [QPV05]. Saturation [Luc02a]. saving [Lev01]. Savings [CAC03]. SAX2 [TEM+01, Hei01]. Sax [Ano01c, Mad04]. SBLH [JK02a]. SBoxes [WOL01]. SC-CF [It01]. SC2000 [SY+02, YS02]. SC2001 [ACM01b].

Scalable [CPH04, HKA+05, HLL05, KY03, KHYM08, SPGQ06, LLW08b, ST03a]. Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. Scale [BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a]. Scaling [BBP00, Coc02b, SDHF00, SDF01, PBVB01].

Scambay [Gun04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Ols00]. Scenarios [BF05]. scene [SG07]. Skeptical [Pen01b]. Schedule [MHH+02, XH05]. Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BBC+09, BNPS02, BR09, BS01d, BMS03, CLO1a, CHK03, CGHG01, CC01b, CYH01, CTL04, CC09, CH01b, CM05a, C0c01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJSS01, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LXH07, LCD07, Miy01, Mi01a, Mi01b].

SAFES [WAF00]. Saga [Eva09]. Salomon [Pap05]. Salsa20 [Ber07, Ber08]. Salt [PKBD01]. Salzburg [DKU05].

Samba [BH00a]. SAML [RR04]. Sanss [KGL04]. sampling [WW06]. sampling [KB39, Sug03, Tip27]. San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Oka04, Pol06, Pre02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c, sanity [Sko03]. sans [Car06]. Santa [Bel00, Bon03, Fra04, Kilo01a, Men07, Sho05a, Yun02a]. Santiago [BS03]. Sanxin [LSZ05]. SAR [B02]. SASAS [BS01c]. SAT [KLN+06]. Satan [Mea04]. satellite [CC05c, HYS03]. Satisfy [PHM03]. satisfying [QPV05]. Saturation [Luc02a]. saving [Lev01]. Savings [CAC03]. SAX2 [TEM+01, Hei01]. Sax [Ano01c, Mad04]. SBLH [JK02a]. SBoxes [WOL01]. SC-CF [It01]. SC2000 [SY+02, YS02]. SC2001 [ACM01b].

Scalable [CPH04, HKA+05, HLL05, KY03, KHYM08, SPGQ06, LLW08b, ST03a]. Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. Scale [BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PS08a]. Scaling [BBP00, Coc02b, SDHF00, SDF01, PBVB01].

Scambay [Gun04]. Scan [MYC01, BD03, KBD03]. SCAN-Based [BD03]. Scaring [Ols00]. Scenarios [BF05]. scene [SG07]. Skeptical [Pen01b]. Schedule [MHH+02, XH05]. Scheduling [FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BBC+09, BNPS02, BR09, BS01d, BMS03, CLO1a, CHK03, CGHG01, CC01b, CYH01, CTL04, CC09, CH01b, CM05a, C0c01b, CFS01, CDM00, DS05a, DKFX05, FS01c, GJSS01, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJK01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KD04, LD04, LHT09, LL05c, LXH07, LCD07, Miy01, Mi01a, Mi01b].
Second-Order [NM09]. Second-Price [Bra01b]. Second-Price Secrecy [Top02]. Secrecy [Bla02a, GH02, Imr03, Lau05, Rec01, RW03a, Sin01b, BDNN02, BLP06, BD04a, Mol05, Ros00b, Sin99, Sin00, SY06, ZYW07].

Secret [ACS02, Alv00, Ano03e, BBDK00, BTW05, BI05b, BTV08, BP06, BM01b, CGHG06, CGH00a, CH01a, CLT07, Cha04, CTV09, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG+05, CDI05, 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, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sin00a, TL02, Top02, RC01, U000, Ver06a, Wri05, ZYR01, ZP01, vW01, A, AEEdR05, Ano02c, Ano08c, Bao02, BCB05+05, Ca01, CC05a, CHY05a, CHY05b, CJL06, CNK04, CDD00, DD04, DB04, DM00a, Di 03, DW01, Du08, FNRC05, FWTC05, FZ06, Gal02, GIKR01, HT04].

d[Cha04]. secret-code [DW01]. Secret-Key [HR05, RW03a]. Secret-Sharing [Bi05b, CDM00, CDI05, DKL05b]. Secretly [CC08]. Secrets [BH06, BBD+02, CMS09, CP07, Che00b, Cop04b, Di 01, Gan01b, Gun04, KMS01, LKM+05, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM+01, VG04, AGKS07, Ano03c, Ano08b, Bao02, Bao00, Bao02a, Bau07, Cop05, Cop06, Cop10, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Ste08, TCC02, DLM05, Eva09]. Section [Ano04b, Ano07a, BK06b, SGK08, TL02, KP03]. Sector [Cro01, MV01]. Secure [McK04]. Secure [AR00, AO00, AF04b, AG01, AP09, Ano01o, ACJT00, AF06, BGCH11, BDF+01a, BST03, BCL+05b, Bar03, BI05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CHK03, CHK05, CGP08, CW07, CSQS01, CHJ+01b, CHJ+01b, CD00, CD01a, CS02, CS03b, CDG+05, CDI05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, FP01, FOPS01, GPC08, GIKR02, GJKR03, Gen04a, GD05, HSZI00, HSZI01, HSHI02, HS06, HRS02, Har07b, HKW06, HLvA02, HvAL09, HR04b, HL07, HLTJ09, Hut01, HLC08, IR01, Ito00, IFH01, J00a, J00, JM02, KL0+06, KY01a, KO04, KLML05, K02, K05, KKK09, KI01b, Kos01a, Kos01b, Kral05, KSR02, L01, LLL02, LCK03, LW00, Lin01c, Lin03, Lin02, LL02, MKP09, Mar02a, Mar07, MV01, M03a, MJD01, NMO05, Nam02]. Secure [Nd05, NSN05, NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RVS09, Rdl01, ST01a, Sea05, SVDF07, SBB05, Sm02, SKR02, SNR04, SBEW01, Sty04, Tad02, VM05, Vau05b, VM02, VM03, WLL09, WBL01, WGL00, X03, Y0LW05, ZY05, Z006, A03a, Ab01, AEE0R05, AL07, AF06, BDS+09a, BDF05, BCP07, CLOS02, CMT09, C04b, CCK04b, CRSP09, CHH+09, CDD06, CG05, DG06, Dwi04, FMV02, Geb04, GIKR01, GCL08, HSW09, HL03, HL06, HJW05, HBC+08, In05, ISTE08, IK0S07, IY06, KOY09, KG09, LL2c, LH04, LH08, LH03, LC04a, LC05b, MT09, ML05, Mi01b, OS00, PCSV07, PBMB01, PQ06, PLSy0E10, PSP+08, RH03, RG09, RGX06, Sea09, SB07, SGMV09, TKP+08, TCR03, Tse07, Ver01, VK08, WH06, WWA01, YGZ05, YTY05, hY08, YRY04, ZBP05, ZCL05, ZCW04, vW07, Ano03b, Ano08d]. Secure
[Ano12, BS01a, BSB05, CHKO08, FIP02b].

**Secured** [BNPW03, Ito01, UP05]. **Securely** [HL05a, LLK05].

Abe01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. **Security**

[Ao01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. **Security**

[Ao01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. **Security**

[Ao01, Cal00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. **Security**

[Ano02e, BC05c, BP01b, Chr00, Chr01, CCMR02, CCMR05, CG04, JRB+06,}
[Lin02, RR04, Uni00h, ZL04c, Pap05]. Security-related [Gutxx].

security-sensitive [SPHH06]. seed [TP07, KKJ +07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06]. Seeks [CAC06]. Seems [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05]. seeking [Mos06].
[ANS05, BCS02, DJLT01, ECM00a, ECM00b, Knu07, Tsa01, Uni00b, WL07b, BSD+09a, BFG04, BFG05, BFG08, CCCY01, HM05, JRB+06, MW06, MPPM09, MV03b, RR04, SBR07, SL05b, TWL05, WA06, BH00b]. serving [LLK05]. Session [GL01, OHB08a, CS04, OHB08b, RN00b, Uni00a, Uni00b, Uni00e, 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, HKR01, MP06, SK05a, TTYL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG+02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [AD07, GLG+02]. SHA1 [WYY05a]. SHACAL [KML+02]. Shacham [Hes04a]. Shamir [BB79, SP79, Coc03, PW05, VS08]. Shamir’s [LD04]. Shape [Gan01b, Gil07]. Shapes [OMT02]. SHARC [DMSW09]. Share [CT08a, CD05, FS04, AEEdR05]. Shared [AC02, BH06, BBDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYY04]. Shares [TT01]. Sharing [BTW05, BI05b, BTW08, BGHP02, CD00a, CLT07, CC08, CTY09, CDM00, CF02, CFS05, CDG+05, CDI05, Di 01, Di 03, DS06, DP07, FM02a, FPS01, FMY01, HNZI02, Kin02, Kog02, KS03, LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, SZ01, Sm00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CDD00, DD04, DM07a, DKL00b, FWTC05, GIKR01, HT04, HKS00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCYW07, ZSV05, dRMS05, vDKST06]. shc [Gua05]. Sheets [MNS01]. shell [Dwi04, Gua05, BSN01, BSB05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [McK04, CZ03, YWC05]. Shift [CGFSHG09, Che08a]. shifting [Cal00e]. shifts [Neu06]. Shin [Küh08, Küh08]. Shines [Coc02b]. Shinko [Ano00d]. Ships [Ano02e]. Shops [Ano01c, YSS+01]. Shor [KLB+02a]. Shores [KKP02]. Short [Ano01a, AF06, BBS04, BWG05, DN00b, Gra02b, LS01b, PM02, RR02, RW02, Vau05b, GL05, WDLN09, Coo02b, Sch01c]. short-term [WDLN09]. Shortcuts [Sha03a]. Shortened [Kur01]. shortest [Pei09]. ShortPK [WDLN09]. Shoup [Luc02b, VMSV05]. show [GP00, Sm03]. Shows [Gen01, AJ08]. Shrinking [Go01c, WHLH05, ZKL01]. SHS [Ano08d, Ano12]. Shuffle [FS01c, NSNK05, Sas07]. Shuffles [Mir02]. Shuffling [PBD05]. shut [Gil07]. SiBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [An01j, BU02, KSWH00, Law09a, LL01, Möl02, OT03a, OT03b, Sch06a, WC04, CNPQ03, PSP+08, WDL07a]. Side-Channel [BU02, Law09a, Möl02, CNPQ03, PSP+08]. Side-Match [WC04]. Siena [BCKK05]. sieve [CM05b, JL03]. sieves [Har07a]. SIGABA [Lee03c]. SIGACT [AC03c, ACM05b, Ra006]. SIGART [AC03c, ACM05b]. Sight [Col03]. SIGMA [Kra03]. SIGMOD [AC03a, ACM03c, ACM05b, ACM04a, FMA02]. SIGMOD-SIGACT-SIGART [AC03c, ACM05b]. Sign [BSC01b, BTTF02, Dav01c, Kra03, Dav01b]. Sign-and-Encrypt [BTTF02, Dav01c]. SIGn-and-MAc [Kra03]. Signal [Ano02e, GG05b, Sha01e, CLK+09, LLLZ06a, 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, CD00a, CL04a, CK02a, CGP08, CH01a, Che02, CM05a, Cor02, CFS01, CS00, D505a, DKFX05, Eng00, FIP00, Gen00a, GJSS01, GS02c, HYZ05a, HSZI00, Han00, HM02b, JSJK01, KC02, Kuh00, LZL01, LYL09, LG04, LG09, LS05b, MMJ05, PL05a, PBV08, Sch01f, Sha01d, NZS05].

Signcryption [Boy03, LXH07, MLM03, Zhe01]. Signed [FL01b, OSSST04, Sch01a, SJ00]. Signer [DKFX05, CJT04, LW05b, WK05, IR02]. Signer-Base [IR02]. signer-verified [CJT04]. Signers [LZL01, Sae02, Sha03c, YTH04]. Significant [SZ01, MS02b, Shp02]. Signification [Ano00j, IR01, RR02, HWW04, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAM09]. SIM-based [AAK09]. similar [Che08b]. Similarity [Sch06b]. Simon [Imr03, Rec01]. Simple [AKS06, CYH05, CJS01, CJ03d, CYW05, CC06, CS03c, DT03, FSW01, Gir06, HM02c, HL01, MS01, Nam02, PB05d, RK06, YS02, YW06, Den02, GM04, KTC03, LKKY03a, LKKY03b, LFW04, XH05, YRY05d]. Simpler [Lin03]. Simplicity [MS01]. Simplification [DJ01]. Simplifications [JS05]. Simplified [Bon01]. simplify [Sma06]. Simplifying [Gut04b]. Simply [Oni01]. Simply-Iterated [Oni01]. Simulatability [HU05]. simulatable [Lau05]. Simulation [DKMR05, KL05, CPG04]. Simulation-Based [DKMR05, KL05]. Simulations [WBRF00]. simultaneously [Wu01]. Singapore [BDZ04, TCC06]. Singh [Imr03, Rec01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a]. Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09]. SINOBIOLOGIC [LL04, Lit05]. SIP [NTW07, PM00, SZ08]. Sir [Bud06]. Site [AEV07, Coc02a]. Sites [Che01d, Ros07]. situation [AJ08]. six [Bel07a]. Sixth [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
TLC06. Size [CS07c, CMJP03, HNZI02, Kal03]. Sizes [Ano09d]. Skein [AEMR09]. Sketching [MNS08, SLTB + 06]. Skipjack [Gra02a, HSL + 02, Skipjack-like [HSL + 02, SLL + 00]. SKLOIS [FLY06]. Sky [MYC01]. SLAAC [CGBS01]. SLAAC-1V [CGBS01]. Slide [Fur02b]. Small [CCM05, ELvS01, Fin02, GPS06, MNT + 00, May02, OT03b, RK06, SM02, Sch01c, SPGQ06, Wal03, YLC + 09, Duj08, dW02]. Small-Project [MNT + 00]. Smaller [Bar00c]. Smart [And04, Ano03a, Ano05b, AJ01b, Bel01, BCST00, Car01, CL07, CJT02, DF01, DFCW00, DJLT01, HBdJL01, Joh01, HQ05, Jac00, JSJK01, JY01, Lan00d, LSA + 07, MOP06, MV01, MG08, NFQ03, Poh01, Q500, Q501, RE00, RE03, Sak01, SR01, Sha01c, SP02, TBDL01, VP01, YKM01, Ano00k, Ano00l, Ano04f, AJ01a, Bar00, BPR01, BCH05, BGL + 03, BU00, Cal00c, CCCY01, Cha05a, Cla00b, Con00, CH00, DMT07, DFH01, DFPS07, FCZ05, Fin03, GM00, GUQ01, HHSS01, Hus05b, Hus01, Jua04, KLY03, LKY05a, Ler02, LC05a, Lu07, MY01, Pha06, PB01, Pre07, SVDF07, SLH03, Smi00, TIS07, VK08, V003b, YW04b, YYW08, Za00, BJVdB02, CL04d, CCK04b, Che00a, DFP06, FGL02, Gro03, H050, Ku04, KC05, LKY02, Pau02b, SKKS00, Sco04, SCF01, TV03, YW04a]. smart-card [GMG00]. Smartcard [HWH01, KRV01, RMCG01, Uro01, PBV01, BBPV00, CGM02, DM07b, HRS02, Ito01, KS02]. Smartcard-Based [RMCG01, CGM02]. Smartcards [CMG + 01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, Ano04c, RM02]. smarter [Car01, Cla00b]. Smartly [MS01]. Smooth [PS02b, XYXYX11, GMR05]. SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. sneak [Ade09]. Sniff [Ano02c]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Saw02, Sha03c]. Socket [ZL04c]. Software [Ano07, Ano08, Ano02c, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HHM01, J010, K010, K011, K012, Lad06, Law09a, LSY01, LLLZ06a, LSV09, LTM + 00, MNT + 00, MSNH07, MKY08, McG06, Nd05, PM00, PS01c, Sch01a, Sch00b, Ste00, USE00b, VH09, VW01, WLV05, W014, ZCC01, ARJ08, Ano00b, Ano00j, Bir07, Che01e, CT02, CDT + 04, CTT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, KA09, Mat02, MCA08, MCHN05, Pau03, Sch01d, SS03, WL07a, WA06, Sal03b, Ano03b, Bol02]. Software-Efficient [HCJ02]. Software-Hardware [PS01c]. Software-Only [H010]. Software-Oriented [ZCC01]. Software/Hardware [Nd05]. SOI [Ano02c, NFQ03]. SOISIC [Ano02c]. Solaris [Ano06c, BH00b]. Solomon [KY02b]. Solution [Cap01, CJT02, DHR00, LS05b, Poh01, Str02, TvdKB + 01, LSH00]. Solutions [Ano04c, MV01, Jan00, MSK03, MV03b, St.00, Gum04]. Solve [CU01, GS03]. Solving [CJT04, GPP08, W01a, Bui09, Whi09]. Some [AG01, BDF + 01, DJ01, DFG01, GM02c, HSS04, JM02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HANR04, He02, JK01a, RSS04, SHT05, ZF05]. Seromen [Ano03g]. Something [FL01b]. sometimes [FNRC05]. Sons [And04]. Sorry [San05]. sorts [Ano03g]. Soul [Bla01c]. Sound [BHP02, FR08]. Soundness [ABHS09, DPV04, MR01c, BPS08, Lan08a]. Source [Bar00c, Bui02, Gut00, HBF09, KLR09, PM00, RK06, TEM + 01, Ano03d, BGL + 03, CBB05, MCA08, RVS09, SB05, Bar00b, Lin02]. Sources
Statistically [Fis01b, HR07, HNO +09].
Statistically-hiding [HR07].
Statistically-Secret [Fis01b].
Statistics [CKN01, CNK04, KLML05].
Status [Pre01, Sha03b].
status [Cal00b].
STD-M [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, HVa02, HvAL09, Hun05, HS08, HVa03, Sal05b, Sch09, Sha01e, Shi08, SWR05, Wan05, WW06, CDS07, CO09a, Che07a, Che08a, GGS +09, JD01, KP00, LT04, WW04, WMS08, Way02b, Way09, YCYW07].
Stegeo [KC09a].
Stego-image [KC09a].
Steiner [WL02].
Step [DRL09, KKKL09, Ano04c, MP07, SL06].
step-by-step [SL06].
Step-out [KKKL09].
Stepping [WRW02].
steps [Bih02].
Stereotypes [GO03].
Stern [CGP08, CS05b].
stick [GPX08].
Sticks [Sam01].
still [Ano00f, Rie00].
Stinson [Spr03].
STL [Zol01].
STOC [ACM05c, ACM07, ACM08, ACM09].
Stochastic [MG01].
Stock [Bar00a].
Stone [MLM03].
Stones [WRW02].
stop [SSNGS00, Win05c].
Storage [DFSS08, Din01, Din05, HR02, Har07b, Hug04, MSTS04, RCBLO0, Ric07, RH02, Vao03, AGFH06, 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, TTPM07, KC09a].
Stream [BCC01, BC05b, BSW09, BS00b, BL02, CF01b, Can06b, CJ01, CH02, CM03, Cou03, CL02c, DF07, Fil00, FF01a, Go01d, Go01e, GBM02, HCJ02, HR00, HR04a, Jan00, KHD01, MSN07, PP06a, SM01, Sar02, SXY01, WB02, Wu02, ZC00, ZZC01, BGP09, Ber07, BD00a, BG08, BVP +04, DS09, DK08, KHO8, Max06, MI09, MRT10, PCS03, PCC03, SB05, WW08].
Stream-Cipher [SXY01, WW08].
Streaming [OS05, CBB05].
Streams [AIP01, CO09a, YLC +09, ZC04].
Strength [CB01, JX05, On01, CKL +09].
Strengthening [Loi00, MHM +02].
String [CP07, DFS04, Pas03, Dan00, RG05].
Strings [Vau05b].
Strong [ADD09, BB00b, CS00, DKFX05, KCJ +01, KW00, LSH03a, LSH03b, Lu02, Pau09, SB02, WHL05, An01m, CC04b, HR08, KTOC03, Ku04, LL05b, SS03, ZT03, ZFK04].
Strong-Password [LSH03a, LSH03b, WHL05, CC04b, KTOC03, Ku04].
Strongly [IY06].
Structural [BS01c, LBR00].
Structure [DNP07, EIG01, H01, HLL +01, MR02a, MR02b, GT02, HSL +02, MF07, PS02a, SG07, SSL +00, XMST07].
Structured [BRTM09, CKK03].
Structures [An02e, DS06, GTTC03, HCD002, KCP01, Kus02, MND +04, MFT05, PSC +02, PQ03b, Sun00a, XH03, Hen06a, IY06, SWR05].
struggle [Bur02].
Stuart [Gum04].
students [AA04b, PP09].
Studies [Pag03, LFHT07, SPH06].
Study [BBGM08, Car02, DPR01, DP00, KKL +07, WC05, BKN04, BF06a, DY09a, KD00, SKW +07, ZWW01].
Sturgeon [Wei05, Wei00, Wei06].
Stuttgart [Eag05].
style [BPS08, dH08].
Subcommittee [Un00f, Un00h].
Subdivision [LDD07].
Subgroup [NBD01, KM04a].
Subgroups
subliminal [LH04].

subsampling [LLC06b]. subscribe [SL05b].

Subscriber [CFRR02]. subscription [MW06]. subscription-based [MW06].

subsets [Sch01e]. substitute [Bih02].

Subscriber [CFRR02]. subscription [MW06]. subscription-based [MW06].

subsets [Sch01e]. substitute [Bih02].

subscription [MW06]. subscription-based [MW06].

survey [Che01f, LCS09]. surveillance [Che01f, LCS09].

Survey [EPP+07, FDIR00, KMO4b, LDH06, MSI10, ATSO4, AN00a, BEM+07, CF50, CDL06, EY09, LOP04, MEO4, Mi001b, OZL08, PC09, Pre07, RH03, RAL07, Sch01f, ÜG08, ZLZ07].

Survivable [CLZ02]. Susan [Jan08a]. SVD [BBC+09, CYH+07, FWL08].

SVD-based [CYH+07, FWL08]. SVG [ZBP05].

Switzerland [CC04a, Vau05a].

Symbolic [DF01]. symbol [SVDF07].

Symbolic [Ver01]. symbol [SVDF07].

Symmetric [An01n, ABM00, CCM01, EP05, ROK05, SL05b]. symmetrical [An01n, ABM00, CCM01, EP05, ROK05, SL05b].

Symmetrical [An01n, ABM00, CCM01, EP05, ROK05, SL05b]. symmetrical [An01n, ABM00, CCM01, EP05, ROK05, SL05b].

Syndrome [SH08]. Systemic [SH08]. Systemic [SH08].

Systematic [SH08]. Systematic [SH08].

Systems [BEM09]. Systems [BEM09].

Systems [BEM09]. Systems [BEM09].
77

[KB06]. Systems
[ACM03c, ACM05b, ANRS01, Ano02e, BCS02, BRTM09, CP02, ELvS01, Fel06, GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST+05, LLLZ06a, LJ05b, Lut03, Mar02b, MMY02, NABG03, RS05, Ril02, SM01, Sas07, SJT09, SXZ01, USE00c, USE00b, Vav03, VHP01, WK03, ARJ08, And08b, Ano01n, Bid03, Ble07, CUS08, CCS08, CGL08c, CCM01, CNPQ03, CHT02, CG05, CSK+08, DY09a, EY09, FM02, FP00, HP00, HBC+08, Hut01, HYS03, JP06, KAM08, KP01, KN03, KRP03, KNS05, MBS04, MSP+08, ND06, Nis03a, PBMB01, Pa04, Pl06, RW07, Sha01a, SK03, TOEO00, WAF00, XQ07, ZSV05, Ano02d, Lut03].
systems/ciphers [SK03]. Systolic
[KLY02, KYY02, MP01c].

Table [Ano03f, MFFT05, XFZ01, BZ03, CC05b, Has00, Tsa08]. table-based [Has00].
Tables [AJO08, KB39, RBF08]. tactics
[Cal00c]. Tag [KKJ+07, NNAM10]. tagging [BP05]. Tags [OS06, ACDM05, PLSvLE10].
Taipei [Lai03]. Taiwan [Lai03, Ano03a].
Takagi [LKYL00]. Takagi-cryptosystem
[LKYL00]. Takaragi [WHOL03]. take
[Heg09, Per05b]. Taking
[CDS07, Lai07, PM00]. Talbot [Rot07].
Talk [FGM00a, Lan00d]. Talking [Ano01p].
tamer [Kap05]. Taming [Aba00, Lov01].
Tamper [LTM+00, CT02].
tamper-proofing [CT02]. tampering
[PS08b]. tandem [DPT+02]. Tang
[YRY05d]. tank [Pau03]. tar [Str02].
targama [MA05]. 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]. TCB
[SPHH06]. TCC [HR06, Kil05, Nao04].
TCP [CD01b, Ols00, SBB05]. TEA
[CV05, HS01, HSIR02, HHH+04, MHL+02, WN95]. Teaching
[McA08, Shu06, GV09, Jan08b].
Tech [Kir01a, TvdKB+01, Uni00c, Gra01, Ros04, Uni00f].
Technical
[BHM03, GS07b, Lan00c, Sc01, TL02, USE01b, USE01a, USE02c].
Techniques [AIP01, BSW09, Bi03, BBP00, BDP02, CC04a, Cra05a, DBS+06, Dun06, Ga03, KLL+06, Ken02b, Kn02, KO03, MKP09, NCRX04, PJ01, P01, Pre00, Shi08, YKW01, AB09, BM05, BR05, Che08a, DY09, DMR07, DY09a, Ga02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08]. Technologie
[RSA09b]. Technologies
[MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZWC02, ATS04, PB01, T02].
Technology [CKZ05, Cla00a, GS00, GSB+04, MP00, NFQ03, Pag03, TV03, AL07, Ble07, Car01, Cas02, Che00a, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b, Six05].
Tektronix [Ano02c]. TelCorreo [LM00].
telegram [Tuc66]. Telelogic [Ano02c].
Telephone [KZ01]. telephones [CF05].
Telephony
[Ano02e, CFRR02, PM00, CGV09].
teleportation [BEZ00, BEZ01, Duw03].
Telling [Gan01b]. template
[LLC06a, UBE09]. Temporal
[CDTT05, KXTZ09]. Ten [ES00a].
Tenth [USE01c]. Term [ABRW01, Dur01, BM06, ISO05, LG04, SGMV09, WDLN09].
Terminal [ECM00a, ECM00b]. Terminals
[Cha08a, ISTE08]. termination [BP05].
terms [LMTV05]. Ternary
[ADI09, DKL00b]. Terrorism [PP06b].
terrorists [Mad04, Win05c]. TESLA
[LN04]. Test [BT02, HSS04, Lan00b, LN08, RSN+01, Way02a, DS00, GMG00, Kat05a, KKKP05, RSS04]. testable [RMPJ08].

TCP
Testing [III00, CGBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03]. Tests [MT02, NM09, GT02, Gut04c, JPL04]. Text [Lut02, PJJH01, PM08]. textbook [BJN00, PP09]. Thank [CMB05, CGBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03]. Their [AGT01, CD00a, Gen04a, JKRW01, LLL+01, 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, Shp99, Wag03]. Theoretical [SGB01, PRS04]. Theoretically [AP09, DM00b]. Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, AL06, BDZ04, Bih03, Boy01, CC04a, Cra05a, Des02, Fal07, HR06, Hay06, IZ00, Irw03, Kim01, Kin02, Lai03, Lee04b, Lut03, MNT+00, Mao04, NP02a, Nao04, Oka00, PY06, Pfi01, Pre00, Rot05, Roy05, Sch06b, Shp03, Spr03, TW02, TW06b, Vau05a, Wai00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cas06, Cos00, DW05, Gar04, HHL+00, HW98, Joy00, Kil05, La00, Lam01, PMV96, Rot02b, Rot03, SC05a, Sho05b, Ste08, Sti95, Sti02, Sti06c, 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, CGH+00b]. third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM00]. Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thirty-Fourth [ACM02]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT+00]. Thoughts [Joh00]. Threat [Por06, SS04, BK00, Geb04]. threatened [An00]. Threats [CNPQ03]. Three [BR00b, Kak06, LSH00, MAA06, AJ08, CL00C, FG03, GPS05, LHL04b, LKY05b, LLS+09, MAA06, SPH06, YC09a, ZL04b]. Three-Key [BR00b]. Three-party [LSH00, CL00C, LHL04b, LLS+09, YC09a]. three-principal [ZL04b]. Three-Stage [Kak06]. Threshold [AF04b, AIP01, BTW05, BTW08, BDD03, BSS02, CDD07, CLT07, CD01, D01, D03, DG03, FS01a, FP01, JLO0, KY02a, KS05b, Kin00, Kin02, Kob02, LHZ+10, LSC03, LCZ05a, LP01, MS02, Nie02c, ST07, WQZ01, Wan04b, WH03, XS03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, DG06, HW02, HW03, HW05, JLL01, JLO0, LCC05, LCZ05c, SCL05, TYH04, WHL03, XC05, YTH04]. Throughput [HV04, LS01b]. thwarting [WL07a]. thwarts [Ade09, SW05b]. TI [GBKP01]. ticket [MAA07]. Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01]. Time [AK02a, App07, AJO08, BPST02, BS00b, BSW01, CU01, CJ03a, CNV06, CLZ02, Dri02, GP08, HM02b, I202b, KL05, Kuh02a, LP02a, Lam00, LLO05, LDO04, May04, Oec03, Pl01, QSR+02, RR02, CAC03, CCK04b, CL00, DS02, GS07b, GM04, HLT09, HHC05, LC04a, MRST06, NS05a, YZDW07, hY08, DK08]. time-bound [hY08]. Time-Domain [Kuh02a]. Time-Free [CNV06]. Time-Limited [AK02a]. Time-Memory [AJ008, Oec03, QSR+02]. Time-Memory-Data [DK08]. Time-Reversed [I202b]. time-space [NS05a]. time-stamping [HHC05]. Time/Memory/Data [BS00b]. Timed [BN00b, CHKO08, JP07, LKLJ01, Mao01, HGNS03, Zha06]. Timed-Release [CHKO08, Mao01, HGNS03]. times [AJ08, CCK04b, Mol05]. Timestamp
JSW05, PW08. Trapdoors [GPV08].

trapping [Min03]. Travel [Bur00].

Traversal [JLMS03]. Trawling [Knu00a, Knu00b].

trattise [MAaT06, MAaT07]. Treatment [CL05, DK08].

Tree [CC05d, GST04, JLMS03, KPT04, LKLK05, LM02, TNM00, Mon03, PCC03, WL02].

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

trek [Pot05].

Trends [Ahm08, KB07, Ort00, NdM06, PRS04].

Tricks [Mit02b, All03]. triggered [HHJS04].

tripartite [SW05a]. Triple

[HSH+01, BR04, CGBS01, Cor00a, FZH05, Kel05a, Kel05b, LMP+01].

Triple-DES [Cor00a, LMP+01]. Tripples [FS01b].

tripwire [TvdKB+01].

trivial [KO00].

troubleshooting [HJW05]. True

[BST03, Cha04, DVD08, EHK+03, HBF09, Pan07, SFD06, BG08, BG09, GB09, Han06, HLwWZ09, Ste05c, vT01, VKS09].

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

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

[CHSS02, HCOD02, Lin00b, LHL+08, Mit02a, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, LLW09]. Trusted

[DK01, WH01, VW01, ARJ08, Gue09, PS04c, ZYL05]. Trusting [CSK09].

trustworthy [CCH05, SK03]. Truth

[MNT+06]. Tseng [Hwa05, XY04, ZAX05].

TTM [GC00b]. Tuesday

[Uni00a, Uni00f, Uni00e]. tunable [LB05].

Tunny [Sal01a]. Turin [AL06]. Tuning

[Bar00b, RSA03a, Ad03, Coc03, Cop04b, Goo00, Pet08, Riv03, Sha03b]. Turkey

[Bor00]. Turkish [DD02]. Turn [Tsa07].

Turing [DJLT01]. tutorial

[Can00a, Puc06, Rot02a, Rot03, vT00]. TV

[Smi03]. Tweakable [DS08, HR03, LRW02]. Twentieth [Gan01b]. Twenty

[ACM03c, ACM05b, AAC+01, B+02, Lan00a]. Twenty-Eighth [B+02]. Twenty-first [Lan00a]. Twenty-Fourth [ACM05b].

Twenty-Second [ACM03c].

Twenty-seventh [AAC+01]. Twin

[Ran01]. TWIRL [Kal03, ST03b]. Two

[Ahm08, BDG+01, DIS02, FD01, Hen06b, HSI02, HSS01, HU05, HLT01, HL05b, JZCW05, KCP01, KO04, KTC03, KI03, Lin01c, MR01a, MLM03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, St00, Ste05a, Ste01, TW07, WW05, XS03, YWWD08, YYDO01, CLOS02, DHL06, GCKL08, HW03c, JW01, LMTV05, MS09e, McN03, MCHN05, Pan01, Pha06, ZLX99, dB07].

Two-Block [KCP01]. two-channel

[MS09c]. Two-factor [Hen06b, Sch05c, St00, Ste05a, YWWD08, dB07]. Two-Key

[KI03]. two-level [DHL06]. Two-Party

[KO04, Lin01c, MR01a, WW05, CLOS02, GCKL08, JW01, ZLX99]. Two-Pass [SK00].

Two-tier [TW07]. Two-Way [DIS02].

TWOBLOCK [Yan05]. Twofish

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

[CKQ03, Dug04, Hoh01, KYHC01, PDMS09, RMS05, Vir03, GO08, FQ06, Sh01d].

Type-based [Dug04]. Type-Passing

[Vir03]. typed [BG07b, FR08]. Types

[Gor02a, GJ04, RSA00c, BFM07, Lan05].

Typical [BSC01a]. typing [GJ03]. Tzeng

[QCB05a, Hsu05a, HL05d].

U [DB04]. U-boat [DB04]. U.K. [CAC06].

U.S [Uni01]. U.S. [Bal02, PM00, Uni00b].

Ubiquitous [Sta03, LKZ+04].

UC-soundness [BPS08]. UCON

[LY05, PS04b]. UK

[CZ05, Chr00, Chr01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01, Mat05].

Ultimate [Dif01]. ultra

[Bam02, CH07a, DB04, Cal01, Win00]. ultra-lightweight [CH07a]. ultra-secret

[Bam02]. Ultrafast [FP01a]. UltraSONIC

[MMH02]. Ultrawideband [Bra06]. UMTS
YRY05d, ZYLG05, vOT08]. **User-Centered** [CMB+05]. **user-controlled** [LAPS08]. **user-drawn** [vOT08]. **user-friendly** [SZS05, WLT05a]. **users** [LLS05b, CF05]. **Uses** [Bau01c, RSQL03]. **ushers** [Bur00]. **Using** [AS01a, AS01c, AADK05, AIP01, Ano01a, Ano01c, Ano01n, ADDS06, BJF02, BH06, BK06a, BBC+09, Bau01a, Bau01b, BP06, BPS02, BR09, BTO2, BMK00, BMP00, BL02, Che01a, CLLL00, CGBS01, CCW02, CCM01, CC06, CH07c, Cir01, DI05, DPR01, DP00, DWN01, DGH+04, EFI+05, FJ03, FMP03, Fri01, GC01a, GL01, GSB+04, HHGP+03, HQ05, HJW01, Jab01, JKK+01, JSJK01, KOY01, Kel05a, Kel05b, KM01a, KLC+00, KTT07, Kra02b, KZ09, Lan04a, Len01, LB04, LS05a, LXH07, LM02, LH07, MS02a, MS09a, ML03, MS03b, MMJ05, NNM10, NZCG05, NM09, OT03a, PKH+01, PJH01, PJK01, PCK02, PK01, Sho00b, SK05a, Sma03a, SVW00, SP04, Ste01, ST01c, TSO00, TL07, TK03, TT01, VPG01, WY02, Wit01, WC03a, XFZ01, YKM01, YLLL02, YSS+01, ZWWL01, Zhe01, AS00, AL07, BCL05a, BCW05]. **using** [BK07, CG06, CDS07, CWH00, CL04d, CCK04b, CCH05, CHY05b, CXY05, CJ05, Che07a, CKY07, Che08a, Che08b, CJ04, CK03, Cos003a, DZL01, Dan02, DSGP06, DS09, DFG00, FWT05, GC00a, GMR05, Gen09b, GS09, HH05, HW05, Hau04, HTW07, Hira09, HW04, HL07, HY03, HL04, JRR09, Jua04, KOY09, KC09a, KY04, KB09, KKL09, KJK07, KSW06, KR03, Ku04, KC05, LHY02, LLH02, LKY04, LFC04, LL04c, LW04, LKY05a, LKW09, LFW04, LCO5a, LCC06a, LKW05a, MT07, Mic01, N050a, Pae00, PS04a, PY08, PCS03, PCC03, PC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SHH07, Tan07a, TLH05, Tsao05, TJ03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04a, YW05, YC09a, YRY04, YRY05b, YZEE09, YC07, ZW05a, ZFK04]. utilising [RFR07a, RFR07b, RFR07c]. utility [Gua05]. Utilizing [Str02].

V [Kat05b, Puz04, S+03]. v1.1 [RSA00d]. v1.5 [CJNP00]. v1.7 [RSA00b]. v2.0 [Man01, RSA00c]. v2.1 [RSA02]. v2.11 [RSA01]. V5 [It00]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BL01, KCl+01, BG09, ME08b, VM03]. Validity [Zh02]. Valuable [PM00]. Value [BR09, GS05, LS08, BM02a, DK08, WWTH08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadharajan [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSN05, Ber08, DJ08, DJ09]. Variants [BDK+09, DG02, KS00b, CM05, Sha04b, TJ03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDKB09]. vast [Wa04]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pei09, mSgFl05, WNQ08, WC05]. vectors [LHL04a]. Vegas [Elv01, 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, GIKR01, KKL09, SC05a]. Verifiably [BGLS03, Hes04a]. verifiably-encrypted [Hes04a]. Verification [AADK05, Ara02, BPS02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJL06, Col03, DS00, HL05c, JW01, Ler02, MD04, MT07, MS09b, PB07, Tsao08, TYH04, Wan04b, Wu01, YLC+09, ZLX99, ZL04b, CS08b, Uzu04]. Verified [BJP02, BFG08, CF08, CJ04]. verifier [Bla01b, LKY05b]. verifier-based
[LKY05b]. Verifiers
[CL01a, He02, LV07, LWK05b, YY05a, ZX04]. Verify [MS02a]. Verifying
[BFG08, BJvdB02, CJM00, HLT01, IR01, PT08, RR02, BLH06, BLF06, HLH00, SV08a, Sha01d]. Verlag
[Eag05, Lee03a, Lee03b, Pap05]. Version
[Bol02, HPC02, OST05, SKI01, Mis06]. Versions
[HSR+01, NPV01, Ano00f, CV05]. Versteckte
[Sch09]. Versus
[Mad00a, Rub00, WWL+02, ASW+01, BJLS02, DBS01, WPP05]. Vertically
[DN04]. Very
[AAC+01, B+02, CG03, EBC+00, FLA+03, Hoh01, PM02, PBMB01, Zir07]. Vestiges
[Top02]. VI [Sch04a]. via [AGKS07, Ano00k, AcDiM05, BDPV09, Car02, Che03, CPG+04, Elb08, FBWC02, Fox00, HHYW07, HLM03, JJo0a, KT06, ML05, PG05, RG05, SB01, SLG+05, ZLG01, Lud05]. Victoria
[ACM08, IZ00]. Victorian [Top02]. victory
[Hau03]. Vid [CAC06]. Video [BDF+01a, BD03, CDTT05, EFY+05, ISSN08, KB03, KJR05, KLL01, LHS05, MLC01, 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, Coo01a, Coo02a, Coo02b, Coo03]. Vignére [DG00].
VII [Sch04b]. VIII [IEE01b, Sch05a]. Virginia
[MS05b]. Virtual [Ano01c, HM01a, Pro00, YSS+01, BDS+09a, ML05, ZBP05]. virtualization
[CGL+08a, CGL+08b, CGL+08c]. virtualization-based
[CGL+08a, CGL+08b, CGL+08c]. Virtues
[Tro08]. Virus [Gor06, Ano05c]. Visible
[HT06]. Vista [Fer06]. Visual
[BDN00, BDSS03, BCD06, CCL09, CTY09, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, ZP05, ABDS01, CDFM05, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Zol01]. Visualization
[XYL09, MFS+09]. Vital [Wal04, You04].
Viterbi [LBGZ01, LBGZ02]. Vladimirov
[Puz04]. VLDB [EBC+00, FLA+03].
VLDP [B+02]. VLSI [KV01]. VMSS
[SC05a]. Voice [Ano001, PK01, VN04].
VolP [Ano08c, SZ08, VAVY09, WCJ05]. vol
[Kat05b, Lee03b]. volatile [SETB08].
Volume [Gol04]. Vortrag [Eke02]. Vote
[Che07b]. Voter [Cha04]. Voter-Verifiable
[Cha04]. Voting
[Cha04, FPS01, HS00, Joh05, JLL02, KMO01, Rub01, CJT03, HJJW05]. Voynich
[Rug04]. VPN [KMM+06]. VPNS [Dav01a].
VQ [WJP07]. VQ-based [WJP07]. Vs
[CTBA+01, DI 01, DI 03, SU07, WW04].
VSS [AF04b, CDF01, FM02a]. Vu [DP00]. vulnerabilities
[CSW05, DMS07, Swi05, XNK+05]. vulnerability
[KHL09, SGA07, YRS+09].
WA [ACM06]. WACs [Kov01]. Wagner
[dVP06]. Wagstaff [Kat05b]. Wahab
[MAaT07]. Walking [Fox00]. Wallet
[ETZ00, JLL04]. Walsh [MS02b].
Walsingham [Bud00]. WAN [Hoh01].
WAN-Cluster [Hoh01]. Wang [SZS05].
Wants [Han00]. WAP [JRHF01]. War
[Bec02, Bud00a, Bud02, Han03, Kov01, MH09, OC03, AJO8, DB04, Ris06, Lov01].
Warfare [HW01, WW04]. warrior [PC04].
Wars [RR03b, Cal00d, Cal00e]. Warsaw
[AUW01, Bih03]. washer [Ano01].
Washington [S+03, USE00a, USE01c].
wasn’t [Bur02]. WaSP [Coc02b]. WASSA
[Ano05c]. Watch
[MA00a, Sav05a, Sav05b, Ano01m, Joy03a].
Waterloo [HH04, HH05, ST01d].
Watermark [AS01b, GMV01, JX05, KHY04, Kwo03a, Meh01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zan01, AA08, CL08, LYGL07, LCC06a].
Watermark-based [Kwo03a].
Watermark-Fingerprint [KHY04].
Watermarked [ST01c]. Watermarking
[AS08, AK02b, AHK03b, AS01c, Arn01, ARC+01, BBC+09, BR09, BSC01a, BSC01b, BS02, BQR01, BSN00, CC02a, CH01b, CD05t, CT09, CT02, CM02, CMB+08, DNW01, DNP07, EFY+05, EIG01, GW01, HT06, HH09, JKK+01, KCR04, hKLS00, KLL01, Kun01, KT00, LZ01, LLS05a, LKLK05, LZ01, LZF04, LZW05, LJP06, L05b, LSC03, LL01, LSK05, MM01a, MNS01, Nak01, OMT02, PJJ01, PJK01, PR01, PBM+07, Qu01, So09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Sh08, SP04, SLT01, SPK08, VVS01, VK07, WC09, WH09, WY09, WW+02, WLT05b, XZF01, YYWS09, ZTP05, ZWC02, AK03a, AAPP07, BCKK05, CC02b, Che08b, CYH+07, CCD+04, CS05a, CC04e, CMB02, CKL05, DSP01, FW08, FMS05, GA03, HLC07, HH05, JD01, JA02, KA09, KP00, LDD07, Lin00a, Lin01b, LLL06a, LL05b, MB08, MCHN05].

Watermarking
[PK03, Ren09, mSgLt05, WJP07, WNQ08, Way02b, Way09, WC05, WMDR08, XMST07, YZDW07, YPSZ01, ZLZS07].

Watermarks
[Ben00, BB00a, MLC01, Sug01, WC04, YLL02, MB08, TND+09].

Watershed
[FBW01].

Watershed-from-Markers [FBW01].

Wavelet
[BR09, GW01, LKLK05, LZ01, Nak01, VK07, AAPP07, AA08].

wavelet-based [AAPP07, AA08].

Wavelet-Domain [LZ01].

WAVES
[LBA00]. Way [BYJK08, BM01a, CHL02, DIS02, DSM00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sh00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LKLJ01, Mic02a, Poi00, Tsa08, YW05, YRY05b, ZW05a].

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

WCC [Ytr06]. WDDL [MMMT09]. Weak [HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00].

Weakening [ZD05].

Weakly
[BS00a, CHS05].

Weaknesses
[FR03, Ren09, mSgFtL05, WJP07, WNQ08, Way02b, Way09, WC05, WMDR08, XMST07, YZDW07, YPSZ01, ZLZS07].

Weakly
[BS00a, CHS05].

Weakness
[SWS05a, SDF01].

Wavelet
[BR09, GW01, LKLK05, LZ01, Nak01, VK07, AAPP07, AA08].

Wavelet-Domain
[LZ01].

WAVES
[LBA00].

Way
[BYJK08, BM01a, CHL02, DIS02, DSM00, Fis01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sh00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LKLJ01, Mic02a, Poi00, Tsa08, YW05, YRY05b, ZW05a].
Will [Ort00, Cla00b, Fur05]. William [Che05b, Pag03]. Williams [Mul01a]. Window [OT03a, SSST06]. Windows [USE00a, DGP07a, DGP09, DGP07b, DGP09, Fer06, HB06, WD01a, Win01]. Wins [Bar00b]. Wired [Gil07, Pot07, SIR04]. Wireless [AAEQ05, Bar03, BCH*00, ECM00b, Fin06, KH05, KHD01, LNL*08, NNAM10, Pan03, PZDH09, Pot03, Puz04, Sin01a, Sty04, SYLC05, VGM04, YSR01, ZYN08, ZWCY02, Badd07, BP03a, BBC*02, CCMT09, Cha05b, GW08, GG05b, HLTJ09, JRR09, KXTZ09, KB09, LDH06, LPV*09, LHTHT07, LW05a, Lin07, Lop06, MJF*08, Moo01, NC09, NLD08, PCSM07, Par04, Pat02a, Pat02b, Pot07, SL07, S206, TP07, Vac06, Van03, Wan04a, YTWY05, CS08b, ECOM00a, PDMS09].

Wiretapping [Cho08a, DL98, Jan08a, DL07]. WISA [CSY09]. Within [MR02a, CHM*02, MR02b, You04]. Without [BCL*05b, Bla01c, BB04, BH07, Har06, NA07, Ano03c, CH01a, CCK04b, CYH04, CCH05, CTH08, CJC03, CJ04, CDD07, CNV06, DKO1, KG09, Ku04, LV07, LHL04b, LW04, LKY05b, LL06, Lin01a, LCZ05b, Lys07, MP02, Mar07, PSS04c, RG09, Ts08, WH01, YW05, YRY05b, ZW05a].

Withstanding [DFS04]. Wits [Bud00a, Bud02]. WLAN [SSM*08]. WLAN/cellular [SSM*08]. Woes [BTTF02]. Women [FF01b]. won [Hau03]. Worcester [KP01]. Word [HR00, SKU*00]. Word-Oriented [HR00, SKU*00].

Wordlengths [PG05]. works [GS01, Max06, NS01a, VS01]. Work [DFG01, DNW05, Fox00]. Working [DFCW00, ELvS01, KB00]. workload [BGM04]. Works [Net04]. Workshop [ACM05a, Ano05c, AL06, BDZ04, BD09, BD08, CZ05, Chr00, Chr01, CCMR02, CCMR05, CS09, DR02c, Des02, GH05, IE01b, IZ00, Joh03, JQ04, KKP02, KCR04, KGL04, Kim01, KP01, KNP01, LST*05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RRR06, RM04, Sch06b, Sch01d, TB02, USE00b, VY01, Vau05a, WK03, Ytr06, AMW07, A01a, BCKK05, Bir07, CKL05, GKS05, HH04, HH05, HA00, ST01d].

World [Ber03, GG05a, HW01, Nik02a, Nik02b, Sch00e, Sty04, YKMB08, Ano03c, Ark05, Bel07a, Che00b, Hei03, HHG06, Hus01, KPS02, Kee05, Lie05, Lun09, Rob02, Rob09, Sch03, SL07, Bec02, Bud00a, Bud02, Hau03, K01, MHO9, OC03, Sty04, See04]. Worlds [Wil01b]. Worm [LJL05, CSW05]. Worms [ZGTG05]. Worst [CCM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case [HRS08, Mic02a, Mic02b, Pei09]. worst-case/average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. wrapped [HLC07]. Wrapper [Ols00]. Write [BB02]. Writers [Gor06]. Writing [HL03, Jan06, Kah67a, Kah67b, Kah69, Gas01]. Writings [Cop04b].

WS [JRB*06, RR04]. WS-Policy [RR04]. WS-Security [JRB*06, RR04]. WSDL [Bar00c]. WTLS [Vau02]. WTMAU [ECM00a, ECM00b]. WTMAU-SD [ECM00a]. Wu [BCW05, CHY05a, CWJT01, HL05c, MS03a, YY05b]. Wu-Lin [YY05b]. Wuhan [TTZ01]. WW [Sal00a]. WWII [WD01b].

X [For04]. X.509 [SJ05]. X.9.31 [Kel05a, Kel05b]. X.9.62 [ANS05]. Xbox [Ste05b]. XCBC [GD02]. XECB [GD02]. Xia [CJT04, Shao05a]. Xiamen [DWML05]. Xiao [JW01, YY05a]. Xilinx [Ano02e]. XIV [USE00c]. xix [Top02]. XL [CP03]. XML [Hei01, TEM*01, AW05, AW08, Ano02e, BNP08, CKK03, Dau01b, Dau01c, DGK*04, FJ04, FL01b, GA03, Her02, LC04b, PCK02, RR04, ÜG08, Uri01, UST01a]. XMT [SG07]. XrML [Bar00a]. XTEA [CV05, HHK*04, MH*02]. XTR [LW02, LV00, LNS02, Ver01].
REFERENCES

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

Yang-Shieh [YWC05]. Yao [McK04, CZ03, KJY05, WL05, YWC05].

Yao-style [BPS08]. Yarrow [KSF00, Mur02].

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

YCH [SC05a]. YCN [Hwa00]. Year [Eva09, Naz02, Bur00].

Years [Ahm08, CM02, Ros04]. Yellow [JY04].

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]. Zealander [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].

Zeta [Ver02]. Zhang [JW01, YY05a]. Zhou [PKH05]. Zimmermann [McL06, Tuc06].

ZK [PBD05]. Zodiac [HSM+02]. Zone [Kum07].

References


[AA08] Agreste:2008:NAP


REFERENCES


REFERENCES


Aamodt:2003:CSP


Agreste:2007:IAW


An:2001:DER


Atallah:2009:ATC


Abadi:2000:TA

REFERENCES

Aiello:2004:JFK

Abdalla:2001:DAS

Abdalla:2005:SER

Ateniese:2001:ECV

Abe:2001:SEP
REFERENCES

Abe:2004:CEP

Abadi:2005:CFI

Adao:2009:SCF

Anderson:2000:CS

Austin:2000:ASF

Adjeroh:2008:BWT


[ACJT00] 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

ACM:2007:SPA


ACM:2008:SPA


Algesheimer:2002:ECM


Alvarez:2005:EBS

REFERENCES


Adikari:2009:HBT


Adleman:2003:TLP


An:2002:SJS


Arazi:2005:RPK


Alvarez:2005:SSS


Ahmed:2017:IRD


Atighehchi:2009:EPA

[AEH17] Kévin Atighehchi, Adriana Enache, Traian Muntean,

Anton:2007:HEW


Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR

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


[Ahm07] 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:SCP**


**Attali:2001:JSC**


**Aid:2008:NSA**

Matthew M. Aid and Thomas R. Johnson. *National Security Agency releases history of cold war intelligence activities: Soviet strategic forces went on alert three times during September–October 1962 be-


REFERENCES


REFERENCES

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


REFERENCES

Aljifri:2003:ILA


Andem:2003:CTE


Anderson:2004:BRR


Aura:2001:RAC

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

REFERENCES

Anonymous: 2001: AWB


Anonymous: 2001: AIGb


Anonymous: 2001: CCA


Anonymous: 2001: RAC


Anonymous: 2001: EDS


Anonymous: 2001: EER


REFERENCES

Anonymous:2001:SCS


Anonymous:2001:TAD


Anonymous:2002:DEC


Anonymous:2002:IHB


Anonymous:2002:NSD


Anonymous:2002:PPD


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 $M(n) = 2^p - 1$. The known members of this set in order of increasing $p$ (not of discovery), year of discovery, and discoverer, are:
<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1913</td>
<td>E. 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>1750</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>E. Lucas</td>
</tr>
<tr>
<td>19</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>9689</td>
<td>1961</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>21</td>
<td>9941</td>
<td>1961</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>22</td>
<td>11213</td>
<td>1961</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; E. 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>317636</td>
<td>1992</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>859433</td>
<td>1992</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>33</td>
<td>1257787</td>
<td>1996</td>
<td>Hans-Michael Elvenich, George Wolman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>34</td>
<td>1398269</td>
<td>1996</td>
<td>Hans-Michael Elvenich, George Wolman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>35</td>
<td>199997</td>
<td>2001</td>
<td>Hans-Michael Elvenich, George Wolman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, Wolman, Kurowski, and Slowinski (GIMPS)</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala et al. (GIMPS)</td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>2001</td>
<td>M. Cameron (GIMPS) (German)</td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>M. Shafer (GIMPS)</td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2004</td>
<td>Josh Findley (GIMPS)</td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2005</td>
<td>Martin Nowak (GIMPS)</td>
</tr>
<tr>
<td>43</td>
<td>30402457</td>
<td>2005</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich, George Wolman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo (GIMPS)</td>
</tr>
<tr>
<td>47</td>
<td>43121609</td>
<td>2008</td>
<td>Edson Smith, George Wolman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, George Wolman, Scott Kurowski, and others</td>
</tr>
<tr>
<td>49</td>
<td>74207281</td>
<td>2016</td>
<td>Curtis Cooper (GIMPS)</td>
</tr>
<tr>
<td>50</td>
<td>77232917</td>
<td>2017</td>
<td>Jon Pace (GIMPS)</td>
</tr>
<tr>
<td>51</td>
<td>(??)</td>
<td>82589933</td>
<td>2018</td>
</tr>
</tbody>
</table>
REFERENCES

Anonymous:2004:Cf

Anonymous:2004:ISL

Anonymous:2004:NGJ

Anonymous:2004:CEC

Anonymous:2005:SCB

Anonymous:2005:WAS

Anonymous:2006:JHD

Anonymous:2006:RC
Anonymous:2006:SSD


Anonymous:2006:SQE


Anonymous:2007:CPSH


Anonymous:2007:CPSf


Anonymous:2008:KAD


Anonymous:2008:RCB


Anonymous:2008:RES


Anonymous:2008:SHS


Anonymous:2009:BG


Anonymous:2009:DSS


Anonymous:2009:PCA


Anonymous:2009:TCA


Anonymous:2012:SHS


Anonymous:2013:DSS

References

Ateniese:2001:SRC

Amir:2001:FAA

ANSI:2005:AXP

Abe:2000:PSP

Abe:2002:SVK
REFERENCES


**Ara02**


**ARJ08**


**Ark05**

REFERENCES

Arnold:2001:AWB


Agrawal:2003:MCA


Artail:2004:PAC


Abe:2001:SPA


Adelsbach:2001:ZKW


Agung:2001:ICI

[AS01c] I. Wiseto Agung and Peter
REFERENCES


Aslan:2004:LAA


Blanchet-Sadri:2001:MSD


Abdalla:2000:KMR


Ateniese:2004:VED


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**


**Blanton:2006:SRF**


**Bagnulo:2002:PAA**


**Badra:2007:AWC**

[Mohamad Badra. Alterna-


Baigneres:2008:QSB


Bamford:2002:BSA


Banks:2005:TFC

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


[Bar00a] Nicholas Baran. News and views: 108-bit elliptic curve cryptographic key found; new algorithm cracks the stock market; first complete Babbage printer unveiled; XrML view to be digital rights standard; PKWare founder [phil katz] dies unexpectedly. Dr. Dobb’s Journal of Software Tools, 25(3):18, March 2000. CODEN DDJOEB. ISSN 1044-789X.


REFERENCES


REFERENCES

Bauer:2001:PPUb

Bauer:2002:PPB

Bauer:2002:PPAa

Bauer:2002:DSM

Bauer:2003:PPAb

Bauer:2003:PPAa

Bau02a

Bau02b

Bau03a

Bau03b

Baudet:2005:DSP

Bauer:2007:DSM

Bauer:2008:EHE
Friedrich L. Bauer. Erich Hüttenhain: Entzifferung 1939–1945. (German)
REFERENCES


REFERENCES


[BBD+09] Daniel J. (Daniel Julius) Bernstein, Johannes Buchmann, and Erik Dahmén,
Beimel:2000:CFS


Bellare:2001:KPP


Blumenthal:2002:SAD


Bartolini:2008:EIS


Barkan:2003:ICO

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


REFERENCES

2009. ISBN ???? LCCN ???? URL ????.


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Butler:2006:FAK


Barni:2005:DWI


Bao:2005:PSS


Barak:2005:SCA


Bresson:2001:PAG


Bresson:2002:DGD

[BCP02a] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Dynamic group Diffie–
REFERENCES


REFERENCES

Heidelberg, Germany / London, UK / etc., 2008.


REFERENCES

Burmester:2004:HPK


Buchmann:2008:PQC


Biryukov:2003:CS


Blundo:2003:COT


Bolosky:2000:FSD

REFERENCES


REFERENCES


REFERENCES

math.utah.edu/pub/tex/bib/index-table-d.html#designscodescryptogr.

Bejtlich:2006:EDS


Bellare:2000:ACC


Belfield:2007:SUC


Bella:2007:FCS


Bellovin:2004:IRS

REFERENCES


Bello:2008:OPR


Bruss:2007:QCS


Benedens:2000:AIW


Benantar:2002:IPK


Benson:2001:VS


Benoar:2001:IPK


Benson:2004:VS

coldwar/assets/files/venona_story.pdf.

[Beron:2000:CE]

[Beron:2003:CAB]

[Ber07]

[Bernstein:2008:CVS]

[Bergmann:2009:DKR]

[Bernstein:2009:IPQ]
REFERENCES

[Bouwmeester:2000:PQI]

[Bouwmeester:2001:PQI]

[Biham:2000:IID]

[Babbage:2001:MHO]

[Boneh:2001:IBE]
Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pair-
REFERENCES


**Boneh:2001:EGS**


**Boneh:2003:IBE**


**Boldyreva:2005:ARO**


**Bisseling:2006:MSM**


**Boldyreva:2006:SO**


**Bhargavan:2008:CVI**

Karthikeyan Bhargavan, Cédric Fournet, Ricardo Corin, and Eugen Zalinescu.


REFERENCES

ny.com/link/service/series/0558/papers/2355/23550174.pdf.


REFERENCES


[BGL+03] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo. A high-speed oscillator-based truly random number source for

**Boneh:2003:AVE**


**Branovic:2004:WCE**


**Boyer:2009:SBB**


**Boneh:2005:EDF**


**Boldyreva:2008:NMS**

REFERENCES


[BH00a] Robert Beck and Steve Holstead. FOKSTRAUT and Samba — dealing with authentication and performance issues on a large-scale Samba service. In USENIX [USE00c], page ?? ISBN 1-880446-13-8. LCCN ????
REFERENCES


**Bialaski:2000:SLN**


**Barak:2005:MAP**


**Badra:2006:KEA**


**Backhouse:2003:TOT**


**Bajard:2004:FR1**


**Barkol:2005:SCC**

Beimel:2005:PNS


Bi:2009:MCE


Bidgoli:2003:EIS


Biggs:2008:CII


Biham:2002:HDE


Biham:2003:ACE

Eli Biham, editor. *Advances in Cryptology — EU
REFERENCES


Beimel:2000:RSC


Bajard:2003:EMG


Bajard:2005:AOP


Biryukov:2007:FSE

REFERENCES


[BJLS02]


[BJLS02]


[BJW08]


[BJ02]


[BJ02]

REFERENCES


REFERENCES


Bajard:2009:SRB


Bellare:2000:SCB


Blum:2003:NTL


Buonanno:2002:IUE


Broadfoot:2002:ASA


Bucci:2008:FDR

REFERENCES

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

Blanchet:2001:ACP

Blanchet:2001:ECP

Blaze:2001:LYS

Blanchet:2002:SAS

Blaze:2002:C1
REFERENCES


Brassard:2000:SAP

Bozga:2006:PBA

Buchmann:2009:PQC

Banks:2001:CAS

Blunden:2009:RAE
Bill Blunden. *The rootkit arsenal: escape and evasion in the dark corners of the system*. Wordware Publishing, Plano, TX, USA,
Batina:2001:AWD


Blomer:2001:LSE


Blomer:2003:NPK


Basu:2003:AC


Brincat:2001:KRA

Karl Brincat and Chris J. Mitchell. Key recovery
REFERENCES


[BMM00] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential fault attacks on elliptic curve cryptosystems. In Bellare [Bel00], pages
REFERENCES


**Boyd:2001:ECB**


**Boyko:2000:PSP**


**Boneh:2003:SSS**


**Buchmann:2006:PCL**


**Borselius:2002:VTS**

Niklas Borselius, Chris J. Mitchell, and Aaron Wil-
REFERENCES


**Borselius:2002:PAU**


**Boyen:2005:DCC**


**Bellare:2000:AER**


**Boneh:2000:TC**


**Bellare:2002:TSB**


[Bouganim:2008:DAC]

[Bellare:2002:PRI]

[Bouganim:2003:CSD]

[Bodycombe:1999:CC]

[Ben-Or:2005:UCS]

[Bollinger:2002:UFO]
REFERENCES


REFERENCES


[Boy03] Xavier Boyen. Multipurpose identity-based signcryption: a Swiss Army knife for

**Bedi:2001:CNF**


**Barbancho:2003:CAC**


**Buchbinder:2003:LUB**

Niv Buchbinder and Erez Petrank. Lower and
REFERENCES

Bellare:2004:KEA


Blanchet:2005:VCP


Beissinger:2006:CUM


Baer:2007:CIS


Bellare:2000:AKE

REFERENCES

Borst:2001:CSC


Bellare:2005:ISA


Boneh:2008:IBI


Baudron:2000:ENS


Backes:2008:KDM

REFERENCES

Benerecetti:2002:VST

Brandao:2001:UEC

Bellare:2000:ETE

Black:2000:CMA
Black:2001:CAF


Black:2002:BCM


Bellare:2004:CBG


Bugliesi:2005:NIP


Bellare:2006:MPP


Bhatnagar:2009:RRW

Brands:2001:RPK


Brandt:2001:CPS


Brackenridge:2006:IUU


Brown:2005:CEC


Browne:2005:DEP


Black:2002:BBA


Butler:2009:LIB

[KRBT09] Kevin R. B. Butler, Sunam Ryu, Patrick Traynor, and
REFERENCES


Josef Bigun and Fabrizio Smeraldi, editors. *Audio- and video-based biometric person authentication: Third International Conference, AVBPA 2001, Halm-
REFERENCES


Biryukov:2001:SCS


Boneh:2001:UBE


Banks:2002:NSR


Bajard:2003:ISC


Barrett:2005:SSS

Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes. SSH: The Secure Shell: The Defini-
REFERENCES

[181]


REFERENCES

182

Bresson:2002:TRS


Bresson:2004:AEC


Bhargav-Spantzel:2007:PPM


Buchmann:2002:ICP

Johannes Buchmann, Kouichi Sakurai, and Tsuyoshi Takagi. An IND-CCA2 public-key cryptosystem with fast decryption. Lecture Notes
Barak:2003:TRN

Biryukov:2001:RTC

Bethencourt:2009:NTP

Biehl:2002:NDP

Boyer:2002:LDS
John Boyer, Andrew D.

Beimel:2005:CIW


Beimel:2008:CIW


Black:2002:SCA


Buchmann:2000:CTC


Buchmann:2000:IC

REFERENCES

185


Buchmann:2001:IC


Buchmann:2004:IC


Budiansky:2002:BWC


Budiansky:2006:HMS


Buhans:2006:FBL

[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.

Bulygin:2009:PSS

[Bul09] Stanislav Bulygin. Polynomial system solving for decoding linear codes and algebraic cryptanalysis. Ph.D.
REFERENCES

thesis (??), Technische Universität Kaiserslautern, Kaiserslautern, Germany, 2009.


REFERENCES


REFERENCES


Staff:2003:NTC


Staff:2006:NTS


CALACIT:2000:SID
in California. Sacramento, CA, August 4, 2000. various pp. [Cal01]

CADOJ:2000:DSE


CAMTC:2000:TSC


Caloyannides:2000:EWE


Caloyannides:2000:EWS


Calvoressi:2001:TSU


Canetti:2001:UCL


Canteaut:2001:CFD


Canetti:2006:SCC

REFERENCES


REFERENCES

Casselman:2006:MTE


Cobas:2001:CTA


Challal:2005:HHC


Cooper:2005:AAP


Chandramouli:2006:BPA

Cachin:2000:OFS


Chan:2001:CRP


Chan:2001:CTB


Carline:2002:NWT


Cachin:2004:ACE

REFERENCES


Chang:2004:SES


Cousot:2004:AIB


Chan:2005:STM


Chang:2005:ASN


Chang:2005:EAP


Comon:2005:TAO

REFERENCES


REFERENCES

Cimato:2006:UMU


Chai:2007:EIB


Cattaneo:2001:DIT


Chen:2004:TPM


Chang:2005:DSM


Chang:2004:IDA


Chang:2004:SOT

REFERENCES


[CCMR05] Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors. *Security Protocols: 11th International...
REFERENCES


REFERENCES


Cramer:2001:MCT


Chapman:2001:PEA


Castiglione:2007:TAD


Chen:2005:NVW


Ceravolo:2004:ERH

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


Certicom:2004:CCC


Canetti:2001:UCC


Canteaut:2001:COR


Cramer:2002:OBB


Clarke:2005:AUM

REFERENCES


[CFVZ06] Joan-Josep Climent, Francisco Ferrández, José-Francisco Vicent, and Antonio Zamora.
REFERENCES


Chang:2010:PRN


Chodowiec:2003:VCF


Cranor:2005:SUD


Candebat:2006:SPM


Chodowiec:2001:ETG

Paweł Chodowiec, Kris Gaj, Peter Bellows, and Brian Schott. Experimental testing of the Gigabit IPsec-compliant implementations of Rijndael and Triple DES

**Caballero-Gil:2009:GBA**


**Catalano:2001:BSP**

Dario Catalano, Rosario Gennaro, and Nick Howgrave-Graham. The bit security of Paillier’s encryption scheme and its applications. In *Advances in Cryptology—EUROCRYPT* 2001 (Innsbruck), volume
REFERENCES


publications/library/proceedings/sec02/cox.html.


Chow:2009:ADN


Crotch-Harvey:2000:OPR


Chang:2001:TFG


Chen:2001:SFW

Minghua Chen and Yun He. A synchronous fragile watermarking scheme for


REFERENCES


Chakrabarti:2007:GCS


Chang:2001:NEA


Chen:2004:MCK


Chen:2005:EUG


Chen:2000:JCT


Cherry:2000:SLD


Chen:2001:DEU

Chaur-Chin Chen. Data encryption using MRF with an RSA key. Lecture Notes in Computer Science,
REFERENCES


Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. In Boneh [Bon03],


REFERENCES


Hung-Yu Chien. Practical anonymous user authen-


REFERENCES

Coppersmith:2002:CSC


Canetti:2003:FSP


Canetti:2003:PST


Chang:2002:IBO

REFERENCES

Chao:2009:HCS


Chen:2002:CPK


Chowdhury:2008:CBG


Christianson:2000:SPI


Churchhouse:2002:CCJ

Canvel:2003:PIS

Chang:2005:ILW

Chang:2005:NMS

Cimato:2002:DAP

Cirstea:2001:SAP
Horatiu Cirstea. Specifying authentication protocols using rewriting and

**Cheon:2003:PTA**


**Chien:2003:HAP**


**Chien:2003:NHA**


**Chien:2003:RSA**


**Chien:2004:IAM**

Chen:2005:EDS


Cornwall:2004:AAM


Choi:2005:EIB


Chin:2006:HSI


Clarke:2000:VSP

REFERENCES

Coron:2000:NAP


Coron:2002:UPS


Chepyzhov:2001:SAF


Chien:2001:MRL


Chien:2002:EPS

Hung-Yu Chien, Jimn-Ke Jan, and Yuh-Min Tseng.

**Chien:2003:CMV**


**Chien:2004:SIS**


**Canetti:2002:SAI**


**Canetti:2002:UCN**


**Cook:2006:CEG**

REFERENCES

Cheon:2002:IID


Chung:2003:EPX


Chun:2003:DLC


Chen:2009:SRP

REFERENCES

CODEN ???? ISSN 1550-4859 (print), 1550-4867 (electronic).

Coppersmith:2000:KRF [CKM00]

Coron:2000:FLA [CKN00]

Coron:2001:SSL [CKN01]

Canetti:2003:RCC [CKN03]

Cheon:2006:KPC [KN06]
Jung Hee Cheon, Woohwan Kim, and Hyun Soo


Chen:2007:CRA

Chen:2000:IBD

Chen:2001:IES

Chang:2001:CIU

Camenisch:2002:DAA


REFERENCES


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

REFERENCES


Chang:2001:ASM


Chang:2001:FAM


Cho:2004:GKR


Cheon:2000:NBC


Canetti:2002:UCT

REFERENCES


REFERENCES

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


Chevallier-Mames:2003:FDS

Benoît Chevallier-Mames, Marc Joye, and Pascal Paillier. Inst. Faster double-size modular multiplication from Euclidean multipliers. In Walter et al. [WKP03], pages 214–227. CODEN LCNSD9. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
REFERENCES


Chao:2000:CHC

Cid:2006:AAA

Caputo:2009:DIT

Crawford:2002:FEE
Coron:2004:SSL


Ciet:2003:PFI


Catalano:2002:HHL


Correia:2006:CAB


Cetin:2009:NSA


Czernik:2009:CRN

[CO09b] Pawel Czernik and Jakub


---


---

Cochran:2002:NVW


Cochran:2003:NVC


Cohen:2003:FOV


Cole:2003:HPS


Constantinou:2000:CSC


Convery:2004:NSA


Conti:2009:GSH

Greg Conti. Googling security: how much does Google know about you? Addison-Wesley, Reading, MA,
REFERENCES


REFERENCES


Copeland:2010:CSB


Corella:2000:FIT


Coron:2006:WC


Coron:2000:ESF

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

Coron:2002:SPP


Coron:2010:CSB

Cosgrave:2000:NTC


Costlow:2003:BIM


Courtois:2003:FAA


Courtois:2004:FSB


Courtois:2002:CBC

Nicolas T. Courtois and Josef Pieprzyk. Cryptanal-

Courtois:2003:AXA


Chatzikokolakis:2007:FAP


Cimato:2006:PVC


Chow:2004:UDL


Chen:2004:SEP

Ling Chen, Yi Pan, and Xiaohua Xu. Scalable and efficient parallel algorithms for Euclidean distance transform on the

Catalano:2004:IIP


Canetti:2003:UCJ

Cramer:2005:ACE

Crampton:2005:UDR

Crenshaw:2000:SPK

Crowley:2001:MFL

Chhabra:2009:MSP
REFERENCES


REFERENCES


[CS05b] Scott Contini and Igor E. Shparlinski. On Stern’s attack against secret truncated linear congruential generators. Lecture Notes in Computer Science, 3574:


REFERENCES


Jedidiah R. Crandall, Zhen-dong Su, and S. Felix

Chen:2008:CCS


Chung:2009:ISA


Collberg:2002:WTP


Coron:2003:NAS


REFERENCES


[CUS08] Shiva Chaitanya, Bhuvan Urgaonkar, and Anand Sivasubramaniam. QDSL: a queuing model for systems with differential service levels. *ACM SIGMETRICS*
REFERENCES


Julio César Hernández Castro and Pedro Isasi Viñuela. New results on the genetic cryptanalysis of TEA and reduced-round versions of XTEA. New Genera-
REFERENCES

Canda:2001:SBC

Cheng:2009:NAS

Chien:2001:CCW

Crosby:2009:OLR


Chien:2005:NRS


Chen:2005:ENB


Chang:2008:EBD

REFERENCES

Chang:2001:NSS


Chang:2004:TSSb


Chang:2005:SAK


Chung:2007:SBW


Chang:2005:CIA


Chen:2003:AEY

REFERENCES


(CZB+01) Diane Crawford, Mick Zraly, Hal Berghel, Ken Pugh, Mat H. West, Conrad Weisert, Terry Steyaert, and Richard Johnson. Forum: How can the Web advance Western democracies? who needs digital signatures; misinformation and the Emulex hoax; OOSCD not really so unified; go back to non-


(Dal01) Richard Dale. Biometric security: It’s all about identification and authentication.
REFERENCES


REFERENCES


REFERENCES


Desai:2000:SAN


Dewson:2008:BSS


Dhem:2001:HSS


Dhem:2001:HSS

Delgado:2007:SCD


Domingo-Ferrer:2000:SCR


Durante:2001:CWR


DePalma:2004:CCS

Paul De Palma, Charles Frank, Suzanne Gladfelter, and Joshua Holden. Cryptography and computer security for undergraduates. SIGCSE Bulletin (ACM Special Interest Group on Computer Science Educa-

REFERENCES

Domingo-Ferrer:2001:CDS

Domingo-Ferrer:2006:SCR

Domingo-Ferrer:2007:ASC
REFERENCES

DEN???? ISSN 1389-1286 (print), 1872-7069 (electronic).

[Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstand-]


REFERENCES

DiRaimondo:2003:PST


DiRaimondo:2005:NAD


DiRaimondo:2006:PST


Dodis:2004:REK


Devanbu:2004:FAX


Devanbu:2003:ADP

Dwork:2003:MBF


Dorrendorf:2007:CRNa


Dorrendorf:2007:CRNb


Dorrendorf:2009:CRN


Dhem:2003:EMR

Jean-François Dhem. Efficient modular reduction algorithm in and its application to “left to right” modular multiplication in. In Walter et al. [WKP03],
REFERENCES


[Di 03] Giovanni Di Crescenzo. Sharing one secret vs. sharing many secrets. Theoretical Computer Science,


Vassil Dimitrov, Laurent Imbert, and Pradeep K.


Zhe Dang, Oscar H. Ibarra,


REFERENCES

Delfs:2002:ICP

Dunkelman:2008:TIV

Du:2005:BRS
REFERENCES

Daswani:2007:FSW


Dhem:2000:PIT


Ding:2000:SSC


Dodis:2009:CAI


Datta:2005:RBN


Delaune:2008:FAP

REFERENCES

Symposium, pages 331–344. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN ???. LCCN ???. URL ?.

[Dittmann:2005:CMS]

[DKU05]

[Dodis:2002:KIP]

[DL98]

[DKXY02]

[deLeeuw:2000:CSD]

[DL00]

[Diffie:2007:PLP]


Equipping smart devices with public key signatures. 
CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).  

**Damgaard:2000:INC**


**Damgaard:2002:EPF**


**Durfee:2000:CRS**


Dwork:2003:MFM

Dwork:2005:PPW
REFERENCES


[DP04] Andreas Dandalis and Viktor K. Prasanna. An adaptive cryptographic engine for Internet protocol security architectures. ACM
REFERENCES


Dziembowski:2007:IRS

Dziembowski:2008:LRC

Dandalis:2001:CSP

Damgaard:2005:QCN

Delbourgo:2002:JBC

Daemen:2001:BCP
Joan Daemen, Michael Peeters, and Gilles Van
REFERENCES

//link.springer-ny.com/link/service/series/0558/bibs/1978/19780134.htm;

Crescenzo:2004:CRR [DR00]

Daemen:2000:BCR [DR00a]

Daemen:2000:RA [DR00b]

DDJ:2000:DDE [Dr.00c]
REFERENCES


Daemen:2001:AAR

[DR01]

Daemen:2002:AWT

[DR02a]

Daemen:2002:DRA

[DR02b]

Daemen:2002:FSE

[DR02c]

Ding:2002:HEE
Yan Zong Ding and Michael O. Rabin. Hyper-


REFERENCES


Dobbertin:2005:AES


Devanbu:2000:CVT


Dodis:2002:NUO


DArco:2003:FTD

REFERENCES


Djurovic:2001:DWF


Dodis:2001:PAS


Duggan:2004:TBC


Dujella:2008:VWA


Dujella:2009:VWA

REFERENCES

Dunkelman:2006:TCB


Dawson:2005:PCM


Durani:2001:LTP


Duwell:2003:BRB


Drutarovsky:2008:CSC


Levy-dit-Vehel:2006:WC

Françoise Levy dit Vehel and Ludovic Perret. On the Wagner–Magyarik
cryptosystem. In Ytrehus [Ytr06], pages 316–329.

[Du:2001:OKS]

Wei Zhang Du and Xin Mei Wang. One kind of secret-
code encryption scheme based on maximum rank
distance codes. *Chinese Journal of Computers = Chi-
CODEN JIXUDE. ISSN 0254-4164.

[DW01]

Benne de Weger. Crypt-
analysis of RSA with small
prime difference. *Applicable
algebra in engineering, com-
munication and computing*,
CODEN AAECEW. ISSN 0938-1279
(print), 1432-0622 (elec-
tronic).

[dW02]

Cunsheng Ding and Xuesong
Wang. A coding theory
construction of new system-
atic authentication codes.
*Theoretical Computer
Science*, 330(1):81–99,
CODEN TCSCDI. ISSN 0304-3975
(print), 1879-2294 (elec-
tronic).

[DW05]

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

[DW09]

Himanshu Dwivedi. *Im-
plementing SSH: strategies
for optimizing the secure
shell*. John Wiley and Sons,
Inc., New York, NY, USA,
2004. ISBN 0-471-45880-
5. xxvi + 376 pp.
CODEN QA76.76.O63
UK£24.50. URL ftp://
uiarchive.cso.uiuc.edu/
pub/etext/gutenberg/;
http://www.loc.gov/catdir/
bios/wiley046/2004297174.
html; http://www.loc.
gov/catdir/description/
wiley041/2004297174.html;
http://www.loc.gov/catdir/toc/
wiley041/2004297174.html.

[DML05]

Yvo G. Desmedt, Huaxiong
Wang, Yi Mu, and Yongqing
Li, editors. *Cryptology and
network security: 4th inter-
national conference, CANS
2005, Xiamen, China, De-
Cember 14–16, 2005: pro-
cceedings*, volume 3810 of
*Lecture Notes in Computer
Science*. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2005.
CODEN LNCSD9. ISBN 3-540-
30849-0. ISSN 0302-9743
(print), 1611-3349 (elec-
REFERENCES

Dittmann:2001:UCW

Dworkin:2003:DRB

Ding:2005:NME

Dawu:2001:TES

Deng:2009:SCA

Ding:2009:MPK
Jintai Ding and Bo-Yin Yang. Multivariate public key cryptography. In Bernstein et al. [BBD09],
REFERENCES

Dai:2001:CDE


Eagleton:2005:BRD


ElAbbadi:2000:VPI


Eghlidos:2001:IRL


Eilam:2005:RSR


English:2007:MAC

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


Echizen:2005:PAV


Ellison:2003:PKS

REFERENCES

Epstein:2003:DIT


Ernst:2004:FBH


Ellison:2000:PSK


Ekert:2002:BTQ


Ekeraa:2009:DCM

REFERENCES


El-Kassar:2001:GPK


Elbirt:2008:AAI


Elbirt:2009:UAC


Elliott:2004:QC


Eloff:2001:AIS


Everitt:2003:JBI

English:2000:MNDb


England:2002:AOO


Elbirt:2005:ILD


Eisenbarth:2007:SLC


Erickson:2001:EDD


Erickson:2002:EDD


Erickson:2003:HAE

REFERENCES

Erickson:2008:HAE

Ellison:2000:TRP

Ellison:2000:IRRa

Ellison:2000:TRP

Ellison:2000:IRRa

Enck:2005:EOF

Ettinger:2002:QQC

Ebringer:2000:PAP
REFERENCES


Evans:2009:BRS

Edman:2009:AES

Elbirt:2000:FIP

Faliszewski:2007:BRB

Fan:2003:ILC
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


FIPS:2000:DSS


FIPS:2001:AES


FIPS:2001:SRC


FIPS:2002:KHM


REFERENCES


[FKJ00] Niels Ferguson, John Kelsey, Bruce Schneier, Mike Stay, David Wagner, and Doug

Ferguson:2000:TRR


Fluhrer:2001:AES


Fox:2001:PPK


Faure:2006:NPK


Freytag:2003:VP1

Johann Christoph Freytag, Peter C. Lockemann, Serge Abiteboul, Michael J. Carey, Patricia G. Selinger, and Andreas Heuer, edi-
FLY06
Fluhrer:2002:CMB

FLZ02
Fluhrer:2002:CSP

FLY06

FLZ02

FM02a
Serge Fehr and Ueli Maurer. Linear VSS and distributed commitments based on secret sharing.


REFERENCES


Foster:2005:BOA


Frincke:2006:ESI


Fujisaki:2001:ROS


Forbes:2004:BRN


Forte:2009:DM


Fox:2000:NTFb

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

Freking:2000:MMR


Fouque:2001:SDC


Fernandes:2002:SAL

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


REFERENCES

Fischer:2002:NFC

Ferguson:2003:CEI

Ferguson:2003:PC

Fundulaki:2004:SYD

Fortnow:2008:IIC

Fuster-Sabater:2001:EAG
REFERENCES


[Fur05] Steven Furnell. Authentic-


REFERENCES


Galbreath:2002:CID


Gallo:2003:SST


Ganger:2001:AC


Gannon:2001:SST


Ganti:2008:PAL


Garrett:2001:MBC


Garfinkel:2003:EBI

Garman:2003:KDG

Garrett:2004:MCT

Garrett:2005:CP

Gasarch:2001:BRBa

Gaudry:2002:CCS

Gavinsky:2008:CIC

Guinee:2009:NTR


REFERENCES

Gordon:2008:CFS

Gligor:2002:FEA

Gennaro:2005:SMS

Goodman:2001:EER

Guerrero:2005:ECB
0020-0190 (print), 1872-6119 (electronic).

**Gebotys:2004:DSC**


**Geier:2003:LCC**


**Gengler:2000:UPC**


**Gennaro:2000:IPR**


**Gengler:2001:PPS**


**Gentry:2003:CBE**


**Gennaro:2004:MTC**

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


Lawrence Goldstone and Nancy Bazelon Goldstone.

Golomb:2005:SDG


Gambino:2008:ITW


Goldwasser:2008:CAP


Gennaro:2003:LBE


Gennaro:2005:BEG


Grothoff:2009:TBS


[GHdGSS00] Octavio A. Gonzales, Gum-

**Gilbert:2000:SAR**


**Grabner:2005:ALC**


**Gong:2001:GPK**

[GHW01] Guang Gong, Lein Harn,


REFERENCES

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

Gordon:2003:ATS

Gordon:2004:TEA

Ganapathy:2005:APA

Gentry:2001:CNS

Gallagher:2006:HSB

Gennaro:2003:SAP
REFERENCES

0558/papers/2248/22480001.pdf.

**Gomulkiewicz:2002:HWA**


**Goldsmith:2004:CAI**


**Goldwasser:2005:PPK**


**Gavinsky:2007:ESO**


**Gavinsky:2009:ESO**


**Garay:2007:RCA**

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

**Gertner:2000:RBP**


**Guneysu:2008:CC**


**Goubault-Larrecq:2000:MAC**


**Goldreich:2001:SKG**

Oded Goldreich and Yehuda


Giuliano:2000:ISC


Galbraith:2002:PKS


Goots:2001:FEA


Golle:2008:DCS


Galbraith:2001:CNR


Galbraith:2001:RBU


Gentry:2005:PAK

[Craig Gentry, Philip Mackenzie]


[GN06] Vanessa Gratzer and David Naccache. Cryptography, law enforcement, and mobile communications. *IEEE
REFERENCES


**Gutmann:2005:WHC**


**Gaj:2003:FME**


**Goldreich:1999:MCP**


**Goldreich:2001:FCBb**


**Goldreich:2001:FCBa**


**Golic:2001:CAS**

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

See also volume 1 [Gol01b].

REFERENCES


[Gor06] Sarah Gordon. Understanding the adversary: Virus writers and beyond. IEEE
REFERENCES

Goulding:2009:ESA


Geppert:2000:TMS


Gupta:2008:FAT

[Manish Gupta, Amit Pathak, and Soumen Chakrabarti. Fast algorithms for top-


Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT


Güneysu:2008:SPH

Gutterman:2006:ALR

Granger:2005:HSN

Granger:2006:SCA

Gentry:2008:THL

Geng:2008:DSA

Galbraith:2004:EDD

Grasser:1998:FC

Graff:2001:CCW
Granboulan:2002:FDC


Granboulan:2002:SSR


Grigg:2001:FCL


Grossschädl:2001:HSR


Grossschädl:2003:ASL


Groth:2005:CS

Jens Groth. Cryptography in subgroups of $\mathbb{Z}_n$. In
Kilian [Kil05], pages 50–??  
CODEN LNCSD9.

Gisin:2002:QC [GRTZ02]

Gentry:2006:EES [GRW06]

Geppert:2000:T [GS00]

GonzalezVasco:2001:CPK [GS01]

Garfinkel:2002:WSP [GS02a]
REFERENCES


REFERENCES


REFERENCES


Giles:2002:ADW

Gennaro:2000:LBE

Guttman:2002:ATS

Goodrich:2002:EDD


**Guillou:2001:CAP**


**Gutmann:2002:DVC**


**Gutmann:2002:CFP**


**Gutmann:2004:CSA**


[GW00] Nicolas Gisin and Stefan Wolf. Linking classical and

Guoxiang:2001:IFB


Gebotys:2008:EAW


Goldberg:2008:PQM


Heys:2000:SAC

REFERENCES


Haddad:2000:AUA


Hancock:2000:EWP


Harvey:2000:EMA

Hare:2001:RUPa


Hare:2001:RUPb


Harrington:2005:NSP


Harris:2005:GHE


Hars:2006:MIA


Harman:2007:PDS

REFERENCES

<table>
<thead>
<tr>
<th>Hars:2007:DIH</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hassan:2000:LTB</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hasan:2001:ECM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hassan:2001:PAA</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hassler:2002:JCP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Haufler:2003:CVH</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Haufler:2006:SVN</th>
</tr>
</thead>
</table>

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

**Hayashi:2006:QIT**


**Hoglund:2006:RSW**


**Huffmire:2008:DSS**


**Hartel:2001:TMS**


**Holcomb:2009:PSS**

REFERENCES


Humphries:2002:IC

Huang:2004:NDE

Hwang:2004:NMP

Huang:2008:NCK

Hernandez-Castro:2006:SGG

Han:2008:PBPa

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


REFERENCES


Herranz:2007:IBR

Heron:2009:AES

Herzberg:2009:DBE

Hess:2004:SVE

Hess:2004:GAR

Heys:2003:ASC

Hassler:2000:OFA
REFERENCES

Horvitz:2003:WKA


Horan:2005:NRN


Howgrave-Graham:2003:IDF


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2005:PKC

Nick Howgrave-Graham. Public-key cryptography and proofs of security. In Garrett and Lieman [GL05], pages 73–89. ISBN 0-8218-
REFERENCES


Howgrave-Graham:2003:HNP


_Hendricks:2007:LOB_


_Handschuh:2004:SAC_


_Handschuh:2005:SAC_

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


[HJJS04] Adam Hess, Jason Holt, Jared Jacobson, and Kent E. Seamos. Content-triggered...

**Hong:2004:DCT**


**Hankerson:2000:CTC**


**Hamann:2001:SBA**


**Han:2007:FIE**

REFERENCES

Higgins:2008:NSC


Hill:2000:KII


Hilley:2005:CRM


Hilley:2006:SSD


Hacigumus:2002:ESE

Hakan Hacigümcü, 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


Hofmeister:2000:COS


Hiltgen:2006:SIB


Horwitz:2002:THI


Howard:2003:WSC


Hwang:2004:REL


Hohenberger:2005:HSO

Susan Hohenberger and Anna Lysyanskaya. How to
securely outsource cryptographic computations. In
Kilian [Kil05], pages 264–?? CODEN LNCSD9.
ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
T44 2005. URL http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
3378; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b106171.

[Hl05b] Kuo-Feng Hwang and I-
En Liao. Two attacks
on a user friendly remote
authentication scheme with
Smart Cards. Operating
Systems Review, 39(2):94–
96, April 2005. CODEN
OSRED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic).

[Hl05c] Shin-Jia Hwang and Hao-
Chih Liao. Security of
Hsu–Wu’s authenticated en-
cryption scheme with (t,n)
shared verification. Applied
Mathematics and Computation,
167(1):281–285, August
5, 2005. CODEN
AMHCBA. ISSN 0096-3003
(print), 1873-5649 (elec-
tronic).

[Hl05d] Shin-Jia Hwang and Hao-
Chih Liao. Security of
Tzeng–Hwang’s authenti-
cated encryption scheme
based on elliptic curve dis-
crete logarithm problems.
Applied Mathematics and
Computation, 168(1):717–
721, September 1, 2005.
CODEN AMHCBA. ISSN
0096-3003 (print), 1873-
5649 (electronic).

[HL06] Michael Howard and Steve
Lipner. The security de-
velopment lifecycle: SDL,
a process for developing
demonstrably more secure
software. Secure soft-
ware development series.
Microsoft Press, Redmond,
WA, USA, 2006. ISBN 0-
7356-2214-0. xxii + 320
pp. LCCN QA76.76.D47
H74 2006.

[Hl07] Chung-Ming Huang and
Jian-Wei Li. Efficient and
provably secure IP multi-
media subsystem authentica-
tion for UMTS. The Com-
puter Journal, 50(6):739–
757, November 2007. CO-
DEN CMPJA6. ISSN 0010-
4620 (print), 1460-2067
(electronic). URL http://
comjnl.oxfordjournals.
org/cgi/content/abstract/1
50/6/739; http://comjnl.
oxfordjournals.org/cgi/
content/full/50/6/739;
org/cgi/reprint/50/6/739
REFERENCES


Huang:2009:OSW


Hopper:2002:PSS


Hu:2009:TRN


Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU

REFERENCES


**Harbitter:2002:MAP**


**Hevia:2002:PSG**


**Hoglund:2004:ESH**


**Hollar:2005:EWS**


**Holenstein:2004:CCB**

Hankerson:2004:GEC


Huang:2007:MPK


Haastad:2004:SAR


Haitner:2009:SHC


Hanaoka:2002:HNI

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

Harnik:2006:CNI


**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-
REFERENCES

He:2001:SAR

Hu:2005:USA

Hawkes:2001:PCS

Hand:2002:MPP


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

[HS01b] Deukjo Hong, Jaechul Sung, Seokhie Hong, Wonil Lee,

Halderman:2008:LWRa


Halderman:2009:LWR


Hanaoka:2002:USA


Hernandez:2001:DTR


Hernandez:2004:STN


Hess:2001:TTH


Hsu:2005:CIT


Hsu:2005:UFR

REFERENCES


REFERENCES

Hamalainen:2002:GPS


Hines:2007:AIF


Hofheinz:2005:CTN


Hughes:2002:LAA


Hughes:2004:ISE


Huhnlein:2000:EIC

[Hüh00] Detlef Hühnlein. Efficient implementation of cryp-
REFERENCES


Sean Hallgren and Ulrich Vollmer. Quantum


REFERENCES


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


Hirose:2001:UAS


Hwang:2003:CAL


Yeh:2008:STB

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.


REFERENCES


Impagliazzo:2003:LRA


Impagliazzo:2006:LRA


Ichikawa:2000:HEA


Ishai:2003:EOT


REFERENCES


Inoue:2005:EST


Intel:2000:IIP


Intel:2003:IRN


Itkis:2001:FSS


Itkis:2002:SSB


Irwin:2003:BRBb


ISO:2004:IIIb

ISO:2005:IDM

Inoue:2008:FAC

Iqbal:2008:CDV

Ishai:2003:PCS
REFERENCES


[Itoi:2000:SCI]

[Itoi:2001:SCS]

[Iwami:2008:AIA]

[Iwata:2002:NCP]

[Irwin:2005:PAI]

[Iwamoto:2006:SSR]

[Iwata:2002:NCP]
Tetsu Iwata, Tomonobu Yoshino, and Kaoru Kurosawa. Non-cryptographic primitive for pseudorandom permutation. Lecture
Iwata:2003:NCP


Imai:2000:PKC


Judge:2002:WWM


Jablon:2001:PAU


Jackson:2000:SCQ

Jambunathan:2000:CCP


Janczewski:2000:IIS


Janeczko:2006:TSH


Jankowski:2008:BRBb

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


Jankvist:2008:TMH


Jennewein:2000:FCQ


Jones:2005:RDF


Johnson:2001:IHS


Jeffrey:2008:PAM


Jennings:2009:SLL

Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC

REFERENCES

Johansson:2000:FCA

Jaulmes:2001:CPN

Jonsson:2002:FCA

Jakimoski:2001:ASR

Jakimoski:2001:CCB

Jakimovski:2002:CS
REFERENCES

Jonsson:2002:SRE


Jonsson:2002:SRT


Jang:2001:BWA


Jung:2001:EMO


Jallad:2002:ICC

Kahil Jallad, Jonathan

Jarecki:2000:AST


Joux:2003:IGN


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:2002:VMA


Juang:2001:FBT


Jakobsson:2003:FMT


Johansson:2003:PCI

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


REFERENCES

[Jon08]

[Jou02]

[Joy00]

[Joy03a]
PLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Joye:2003:TCC

Jaulmes:2002:SHG

Joye:2003:GFA


REFERENCES


REFERENCES


Juels:2005:APD


Jeng:2006:EKM


Jin:2005:EAW


Jiang:2005:HNP


Joye:2001:NMM


Jakobsson:2004:ACN

REFERENCES


Jain:2009:NBC


Jiang:2005:TMD


Kamel:2009:RSW


Kadrich:2007:ES


Kahn:1967:CSSa


Kahn:1967:CSSb

David Kahn. The Codebreakers: the Story of Se-
REFERENCES


REFERENCES


REFERENCES


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]


[Kc01]


[Kieu:2009:HIS]


[Kieu:2009:ISI]

REFERENCES

Kim:2007:SBE


Kim:2001:SAC


Ku:2003:WLL


Kang:2001:NHO


Kalker:2004:DWS

REFERENCES

Kurosawa:2004:NPH


King:2001:SAD


Keefe:2005:CDS


Kelsey:2000:KST


Kelsey:2002:CIL

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
REFERENCES

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


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
REFERENCES


Kiltz:2001:TBC


[Kim01]


Kim:2002:ISC


King:2000:IMP


King:2001:CMF


King:2002:RG1


Kirkby:2001:CCW

REFERENCES


Montgomery:2003:FEC


Kocarev:2001:LMB


Kanade:2005:AVB


Kim:2005:IYA


Kim:2002:NIS

Myungsun Kim and Kwangjo Kim. A new identification

**Klein:2003:FOW**


**Kawachi:2006:PQC**


**Kashefi:2007:SZK**


**Karri:2003:PBC**


**Kwon:2003:EEC**

REFERENCES


Khachatrian:2001:FMI [KKIM01]


Ko:2007:SRT [KKJ+07]


Klonowski:2009:SGS


Kawachi:2005:UTQ


Kim:2009:SVN

Soongohn Kim, Seoksoo Kim, and Geuk Lee. Secure verifiable non-interactive oblivious transfer protocol
CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

**[KKP02]**

**[KKS00a]**

**[Kohno:2000:PCR]**
 pdf.

Kelsey:2001:ABA


Kim:2002:IDS


Katz:2005:HEP


Katz:2008:IMC


Knill:2002:FPE

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


Knill:2002:QIP


Ko:2000:NPK


Kiltz:2005:SCM

REFERENCES


**Kacprzak:2006: CBS**


**Kalai:2009: SEU**


**Kim:2002:EPS**


**Knudsen:2000: CRA**

Kim:2001:NPK


Knudsen:2001:CPL


Kanda:2002:SCA


Koblitz:2004:OTS

Neal Koblitz and Alfred J. Menezes. Obstacles to

Koblitz:2004:SPK


Koblitz:2004:SPK

Koblitz:2005:PBC


Kornerup:2007:PIS


Kim:2002:ABA

Kakarountas:2006:HSF


Katz:2001:CCA


Klarlund:2001:MIS


Klimov:2002:ANC


Keliher:2001:IUB

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:
REFERENCES


Kim:2003:RCC


Kol:2008:GEI


Koc:2001:CHEb


REFERENCES


Krukow:2005:FCR

Knudsen:2000:TT

Knudsen:2000:TTR

Knudsen:2002:ACE

Knutson:2007:BPS

Kushilevitz:2000:OWT
Eyal Kushilevitz and Rafail Ostrovsky. One-way trapdoor permutations are sufficient for non-trivial single-server private information retrieval. Lecture Notes in Computer Science, 1807:104–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349


REFERENCES

Koc:2003:GEI

Kerins:2002:FPE

Klima:2003:ARB

Kaufman:2002:NSP

Kim:2004:TBG
Yongdae Kim, Adrian Perrig, and Gene Tsudik. Tree-based group key agreement.

Krishna:2003:BUP


Krawczyk:2001:OEA


Krause:2002:BBC


Krause:2002:USP


Krawczy:2003:SSM

Krawczyk:2005:HHP


Kramer:2007:LCC


Kreitz:2005:OBE


Koeune:2002:FIL


Kehr:2001:ISM


Kim:2005:CLL

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


REFERENCES


REFERENCES


secret sharing scheme with combinatorial structures / Douglas R. Stinson and R. Wei — Protecting a mobile agent’s route against collusions / Dirk Westhoff ... [et al.] — Photuris: design criteria / William Allen Simpson.


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-


Kukorelly:2001:PAL

Kumagai:2007:RSK

Kundur:2001:WDI

Kurosawa:2001:MRP

Kusters:2002:DCP

Kuo:2001:AOS
H. Kuo and I. Verbauwhede. Architectural optimization for a 1.82gbits/sec VLSI implementation of the AES Rijndael algorithm. Lecture Notes in Computer Science, 2162:51–??, 2001. CO-
REFERENCES


Komninos:2007:ALS


Kejariwal:2009:ELL


Koshiba:2000:SEP


Knudsen:2002:IC


Karolof:2003:HMM


ACM order number 508000.


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


[KY02c] Hyun-Sung Kim and Kee-


REFERENCES


[KZ09] Ajay Kumar and David Zhang. User authentica-

tion using fusion of face and palmprint. Interna-
tional Journal of Image and Graphics (IJIG), 9(2):251–
270, April 2009. CODEN ????? ISSN 0219-4678.


REFERENCES


Laird:2007:THL


Lai:2008:JIA


Lamont:1991:UFC


Lam:2001:CCN


Lambert:2007:SLG


Landau:2000:CST

REFERENCES

[Landau:2000:STT]
Susan Landau. Standing
the test of time: The Data
Encryption Standard. Not-
tices of the American Math-
etical Society, 47(3):341–
349, March 2000. CODEN
AMNOAN. ISSN 0002-9920
(print), 1088-9477 (elec-
tronic). http://www.ams.org/notices/200003/fe-
landau.pdf.

[Landau:2000:TOD]
Susan Landau. Technical
opinion: designing cryp-
tography for the new cen-
tury. Communications of
the Association for Com-
puting Machinery, 43(5):
115, May 2000. CODEN
CACMA2. ISSN 0001-0782
(print), 1557-7317 (elec-
acm.org/pubs/citations/
journals/cacm/2000-43-
5/p115-landau/.

[Landau:2004:PNS]
Susan Landau. Polynomi-
als in the nation’s service:
Using algebra to design the
Advanced Encrypted Stan-
dard. American Mathemat-
ical Monthly, 111(2):89–117,
February 2004. CODEN
AMMYAE. ISSN 0002-9890
(print), 1930-0972 (elec-
tronic). URL http://re-
search.sun.com/people/
slandau/maa1.pdf; http:
//www.esat.kuleuven.ac.
be/~rijmen/rijndael;
http://www.rsasecurity.
com/rsalabs/faq3-1.html.

[Landau:2004:SLE]
Susan Landau. Security,
liberty, and electronic
communications. In Frankli
[Fra04], pages 355–
?? CODEN LNCSD9.
ISBN 3-540-22668-0. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
10.1007/b99099. URL
http://www.springerlink.
com/openurl.asp?genre=
issue&issn=0302-9743&volume=
3152; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b99099.

[Lakshminarayanan:2008:SUC]
Karthik Lakshminarayanan,
Daniel Adkins, Adrian Per-
rig, and Ion Stoica. Secur-
ing user-controlled routing

**Laud:2005:STS**


**Laud:2008:CSC**


**Laud:2008:CSC**


**Lavington:2006:FCD**


**Lavoue:2009:LRM**


**Lawton:2005:MAH**


**Lawson:2009:SCA**


**Lawson:2009:TAG**

REFERENCES

05/28/timing-attack-in-google-keyczar-library.

Li:2004:QAU

Lindskog:2005:DIT

Lee:2000:UBN

Leveiller:2001:CNF

Leveiller:2002:CNF
REFERENCES

Laufer:2000:SSC


Laih:2003:COP


Lin:2004:SOT


Lu:2004:XMS


Lu:2005:ERU


Lu:2005:NDA


Long:2005:DTC

Lu:2007:NPL


Lee:2001:SEK


Lee:2003:APS


Levi:2004:UNC


Lee:2004:DEB


Lim:2009:OPG

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


REFERENCES

Lee:2004:ACA


Lenstra:2001:USM


Leroy:2002:BVJ


Levy:2001:CHC


Lehtinen:2006:CSB

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
REFERENCES


Lu:2005:NPS


Lee:2004:SAA


REFERENCES


Lindell:2001:PCT


Lingmann:2002:DSK


Lindell:2003:SCC


Lin:2007:PFT


Lee:2005:IEC


Licks:2005:GAI

Vinicius Licks and Ramiro Jordan. Geometric attacks on image watermarking systems. IEEE MultiMedia, 12
Li:2005:AWP


Lee:2004:SSP


Ludwig:2001:FSE


Lee:2008:SAF


Lee:2009:SAF


Lim:2001:SAW


Lee:2003:PSAa

Sung-Woon Lee, Woo-Hun Lee:2003:PSAa


Lee:2003:ISC


Lee:2004:DIS


Lee:2004:CIB


Lee:2004:FIM


Lim:2004:ISC


Lee:2006:ISC

Lu:2006:FBW

Lu:2006:RDI
Li:2008:CRR


Lee:2001:PBG


Lee:2002:RUA


Li:2001:SPD

[LLL*01] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou,

**Lee:2002:SEC**


**Lee:2004:MPA**


**Li:2006:ESY**


**Li:2006:SYG**


**Lindell:2002:CAB**

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

Lindell:2006:CAB


Lian:2007:MDE


Lee:2005:IWR


Liu:2005:SWA


Lee:2009:CET


Li:2004:ABP


References

Li:2005:ATN


Liu:2008:DEA


Li:2009:ATN


Lee:2006:DCK


Linares:2000:SAM

Leandro Rodríguez Liñares and Carmen García Ma-
REFERENCES


[Leitold:2001:MTN] Herbert Leitold, Wolfgang Mayerwieser, Udo Payer,
REFERENCES


Lepinski:2005:FZK


Laskari:2005:TTC


Lu:2005:CCA


Laskari:2007:AEC


REFERENCES


[LNS02]
REFERENCES

issn=0302-9743&volume=2442.

[Loidreau:2000:SMC]


[Lopez:2004:AAI]


[Lopez:2006:UPK]


[Lovering:2001:TKF]


[Lindell:2000:PPD]


[Lysyanskaya:2001:AST]

REFERENCES


Labbe:2002:AIF


Luccio:2002:AC


Lee:2003:CPK


Li:2005:MCK


Law:2009:EEL

REFERENCES


REFERENCES


Liang:2009:AIE

Lee:2001:EPI

Liu:2005:RBU

Lin:2004:SIS

Li:2005:ISS


HongQian Karen Lu. Network smart card review and analysis. Computer Net-
REFERENCES

ny.com/link/service/series/0558/papers/2355/23550001.pdf. [Luk01]

Lucks:2002:VCS


Lucas:2006:PGE


Ludvig:2005:PWF


Lukyanov:2001:PFA


Lunde:2009:BCU


Lutz:2002:BBS

REFERENCES


REFERENCES

Lee:2004:IAK


Liang:2005:PAC


Loepp:2005:PIC


Lyuu:2005:CIH


Lin:2000:PAS


Lv:2005:PCA

REFERENCES

Lv:2005:SMS

[LWK05b]

Lin:2009:DMG

[LWL09]

Li:2005:IWR

[LWS05]

Lin:2005:NIB

[LWXZH05]

Li:2007:PBS

[LXH07]

Lixin:2005:FLA
REFERENCES


REFERENCES

computer.org/co/books/co2000/pdf/r7108.pdf.

Michener:2000:MSA


Masuda:2002:CDC


Maurer:2007:ICP


Mrayati:2003:AKT


Mrayati:2004:IAD


Mrayati:2005:IDB


Mrayati:2006:TTC

Mrayati:2007:TTC


Mrayati:20xx:AET


McDaniel:2006:OAI


Machado:2000:NCP


MacKenzie:2001:MEP


Mohay:2003:CIF


Madsen:2000:HCl


James Manger. A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1

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


Matsui:2002:FSE


Mastroeni:2004:APA


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.

May:2004:CRS

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
volume&id=doi:10.1007/b99099.

May:2009:PIS

John P. May, editor. Pro-
cedings of the 2009 interna-
tional symposium on Sym-
boic 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 ????

Mel:2001:CD

H. X. Mel and Doris M.
Baker. Cryptography De-
rypted. Addison-Wesley,
352 pp. LCCN QA76.9.A25
M44 2001. US $29.95; CDN
$44.95; UK £22.99.

Mohanty:2008:IWB

Saraju P. Mohanty and
Bharat K. Bhargava. In-
visible watermarking based
on creation and robust
insertion-extraction of im-
ge adaptive watermarks.
ACM Transactions on Multi-
tmedia Computing, Com-
munications, and Applica-
tions, 5(2):12:1–12:??, Novem-
ber 2008. CODEN ?? ??
ISSN 1551-6857 (print), 1551-6865 (elec-
tronic).

McKinnon:2004:CCS

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 (elec-
tronic).

Montenegro:2004:CBI

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.
REFERENCES

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

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:OI F


Meadows:2004:OSM


Mehrabi:2001:DW

Hamid Reza Mehrabi. Digital watermark. Lecture Notes in Computer Science, 2163:49–??, 2001. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349
REFERENCES


Mena:2003:IDM


Menezes:2005:TCC


Menezes:2007:ACC


Messerges:2000:SAF

REFERENCES


[MFS+09] Christoph Müller, Steffen Frey, Magnus Strengert, Carsten Dachsacher, and Thomas Ertl. Best paper


REFERENCES


Maas:2009:SRW


Moon:2002:IDC


Mihaljevic:2009:ASC

REFERENCES


REFERENCES


MacDonald:2003:CDS


Maltoni:2004:BAE


Moore:2001:AGK


Mabry:2007:USE


Mandviwalla:2008:MBW


Moffie:2005:AAS

REFERENCES

Moyle:2005:CLD

Mazieres:2000:SKM

Majzoobi:2009:TDI

McDonald:2008:SID

Malone-Lee:2003:TBO

Miaou:2001:BCW

Maitra:2001:SDD


McLoone:2001:HPS


McLoone:2001:SCF


Mana:2002:PMD

REFERENCES


[MN03] Rebecca T. Mercuri and Pe-
Mukhopadhyay:2014:EMP


Martel:2004:GMA


Martinez-Nadal:2002:CUM


Meyer:2001:FIC

REFERENCES


REFERENCES

[MOP06] Stephan Mangard, Elisa-
beth Oswald, and Tho-
mas Popp. Power Anal-
ysis Attacks and Counter-
measures for Crypto-
graphic Smart Cards, volume 450
of Advances in Information
Security. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2006. ISBN 0-
387-30857-1. 250 (est) pp.
LCCN ???? URL http://
deposit.ddb.de/cgi-bin/
dokserv?id=2739575&prov=
M&dok_var=1&dok_ext=htm

[Mor03] James Morris. Kernel ko-
rner: The Linux kernel
cryptographic API. Linux
CODEN LIJOFX. ISSN
1075-3583 (print), 1938-
3827 (electronic).

[Mor05] Hannes Moritz. Krypto-
analyse des Advanced En-
cryption Standard. (Ger-
man) [cryptanalysis of the
Advanced Encryption Stan-
dard]. Diplom-Arbeit, Tech-
nische Universität Wien,
Wien, Austria, 2005. iii +
116 pp.

[Mos06] Phil Moses. Demons
seeking demons—a prac-
tical approach to harden-
ing your openSSH config-
uration. Linux Journal,
CODEN LIJOFX. ISSN
1075-3583 (print), 1938-
3827 (electronic).

[Mert00] Orren Merton and Linda Dai-
ley Paulson. News briefs:
Gamers jump into broad-
band technology; Intel has
new chip design for hand-
helds; patent expiration be-
gins new encryption era;
privacy organization raises
privacy concerns. Com-
puter, 33(11):16–19, No-
vember 2000. CODEN CP-
TRB4. ISSN 0018-9162
(print), 1558-0814 (elec-
computer.org/co/books/

[MP01a] Scott McMillan and Cameron
Patterson. JBitsTM im-
plementations of the Ad-
vanced Encryption Stan-
dard (Rijndael). Lecture
Notes in Computer Science,
2147:162–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/2147/21470162.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2147/21470162.pdf.
REFERENCES

**Mihailescu:2001:BRE**


**Moshopoulos:2001:NSA**


**Malkhi:2002:ACE**


**Maurer:2003:SMR**


**Micciancio:2005:ASS**

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

Matusiewicz:2006:FGD


Munilla:2007:HMF


Micciancio:2008:OCC


Moralis:2009:KSA


REFERENCES


REFERENCES


Matyas:2003:TRU


Micciancio:2009:LBC


Monrose:2002:TSG


REFERENCES


[MS03b] Gerome Miklau and Dan Suciu. Controlling access to published data using cryptography. In
Freytag et al. [FLA+03], pages 898–909. ISBN 0-12-722442-4. LCCN ????.
URL http://www.vldb.org/dblp/db/indices/a-tree/m/Miklau:Gerome.html


[MS09d] S. Myers and A. Shelat. Bit encryption is complete. In


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


REFERENCES

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.

Meseguer:2007:SRA

Ma:2009:NAS

Muller:2001:SIC

Mullins:2002:MUC

Mullins:2006:CC


REFERENCES

Micciancio:2003:SZK

[MV03a]

Morrow:2003:DIB

[MV03b]

Micciancio:2004:CTA

[MW06]

Ma:2006:ADS

[MW04]

Morelli:2001:JAH

[MWS08]

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

**MRaihi:2001:CAS**


**McCook:2001:NSS**


**Morelos-Zaragoza:2002:AEC**


**Matsui:2004:SAC**

REFERENCES

Nagy:2007:AQK


Naik:2003:DSW


Naccache:2001:TCC


Naftali:2005:BSS


Nakai:2001:SFW


Namprempre:2002:SCB

[Nam02] Chanathip Namprempre. Secure channels based on
authenticated encryption
schemes: a simple charac-
terization. Lecture Notes in
Computer Science. 2501: 515–?, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). URL http://
link.springer.de/link/
service/series/0558/bibs/
2501/25010515.htm; http:
//link.springer.de/link/
service/series/0558/papers/
2501/25010515.pdf.

Naor:2002:DRA

Moni Naor. Deniable
ring authentication. In
Yung [Yun02a], pages 481–
498. CODEN LNCSD9. ISBN 3-540-44050-X (pa-
perback). ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2002. URL http://
link.springer.de/link/
service/series/0558/bibs/
2442/24420210.htm; http:
//link.springer.de/link/
service/series/0558/papers/
2442/24420481.pdf.

Naor:2003:CAC

Moni Naor. On crypto-
graphic assumptions and
challenges. In Boneh
[Bon03], pages 96–109. CO-
DEN LNCSD9. ISBN 3-540-
40674-3. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2003. URL http:
//link.springer-ny.com/
link/service/series/0558/
tocs/t2729.htm; http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2729; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b11817.

Naor:2004:TCF

Moni Naor, editor. Theory
of Cryptography: First The-
ory of Cryptography Con-
ference, TCC 2004, Cam-
bridge, MA, USA, Febru-
ary 19–21, 2004: Proceed-
ings, volume 2951 of Lec-
ture Notes in Computer
Science. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2004. CO-
DEN LNCSD9. ISBN 3-540-
21000-8. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C6676 2004. URL http:
//link.springer-ny.com/
link/service/series/0558/
tocs/t2951.htm; http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2951; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b95566.


REFERENCES


REFERENCES


REFERENCES

Niederreiter:2002:BRC


Nielsen:2002:SRO


Nielsen:2002:TPF


Nicholson:2001:YBC

REFERENCES


Nievergelt:2002:FLM


Niederreiter:2004:BRC


Nikander:2002:DSAa


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


Naor:2004:NTC


Nichols:2000:DYD


Neraud:2001:CFD


Nguyen:2001:ISA


Nguyen:2001:TFLa

REFERENCES

Narayanan:2005:FDA


Narayanan:2005:ODG


Nguyen:2005:FPL


Nguyen:2005:PSE


Nishioka:2002:DAF


Nahum:2007:ESS


Nyberg:2001:CTC

Kaisa Nyberg. Correlation theorems in cryptanalysis. Discrete Applied Mathematics,
REFERENCES


REFERENCES


[Oiwa:2009:IMS]


REFERENCES

Ogata:2006:OSS


Olson:2000:SCT


Ohigashi:2009:PMF


Ohkuma:2001:BCH


Ohbuchi:2002:FDA


Onions:2001:SSI


}


REFERENCES

Ortiz:2000:ITW


Okeya:2000:PAB


Okeya:2001:EEC


Ostrovsky:2005:PSS


Oren:2006:PAR


Obimbo:2007:PAD

REFERENCES


[OST05]

Oury:2008:PP


[OS08]

Overbeck:2009:CBC


[OS09]

Okeya:2004:SBR


[OST06]

Osvik:2005:CAC


[OST05]

Osvik:2006:CAC


[OST06]

Osvik:2000:SS


Ouellette:2005:PPM


Overbeck:2006:EGA


Onieva:2008:MNS


Paeng:2003:SCU


Page:2003:BRW


Palmer:2002:TMQ


Panditaratne:2007:TRN

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


Patiyoot:2002:MSE


Patiyoot:2002:SIW


Patarin:2003:LRR


Patarin:2004:SRF

REFERENCES

Paulson:2001:RBS

Paulson:2002:NBPb

Paulson:2003:NBV

Paulson:2009:NBT


**Papadimitriou:2001:PSE**


**Pucheral:2001:PSD**


**Poulos:2008:TSE**


**Prattichizzo:2007:PIH**


**Perez:2007:URR**

REFERENCES

Petrie:2000:NBI


Peikari:2004:SW


Park:2005:NDS


Perlner:2009:QRP


Park:2003:ESA

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


Peinado:2004:CLK


Peikert:2009:PKC


Pelzl:2006:PAC


Pemble:2001:SPA


Perrine:2003:ECP


Perlman:2005:EMD

REFERENCES

560

techrep/2005/sml1-tr02005-140.pdf.

Perry:2005:DCP


Petullo:2003:IEH


Petullo:2005:EYR


Petzold:2008:ATG


Potter:2003:S


Pfitzmann:2001:ACE


Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park. New public key cryptosystem using finite non Abelian groups. In Kilian [Kil01a], pages 470–?? ISBN 3-540-42456-3 (paperback). LCCN ???.
REFERENCES

Polk:2003:IIC

Phoha:2001:SDI

Pieprzyk:2003:FCS

Pathak:2006:BFT

Pietrzak:2005:CDI

Pinkas:2002:CTP
REFERENCES


**Pinkas:2003:CTP**

**Pincock:2006:CHC**

**Piper:2003:RCS**

**Park:2001:NDW**

**Park:2001:RFW**
REFERENCES

Poh:2001:HBP

Petitcolas:2003:DWF

Park:2001:DNP
Hee-Un Park and Im-Yeong Lee. A digital nominative proxy signature

**Pliam:2001:PTU**


**Pon:2005:MDS**


**Pon:2005:OPK**


**Peris-Lopez:2010:CSP**


**Pfleeger:2007:IBC**


REFERENCES


Pointcheval:2006:TCC


Poole:2003:NSP


Pornin:2001:THE


Porras:2006:PEG


Potter:2003:WAO


[Pass:2005:NIC]


[Pass:2008:NIC]


[Pre00]


Preneel:2002:NPT


Preneel:2002:TCC


Preneel:2007:SRD


Price:2000:NCH


Provos:2000:EVM


Provos:2001:DAS


[Paun:2004:CTT]  

[PRS04]  

[Pfitzmann:2001:SEC]  

[Pornin:2001:SHT]  


Pomarance:2002:2002:SOC


Prabhakaran:2004:NNS


Prabhakaran:2005:RES

REFERENCES

Phan:2006:FDB


Park:2008:SRB


Pavlou:2008:FAD


Park:2002:SRL


Pareschi:2009:PAC


Petit:2008:BCB

C. Petit, F. Standaert, O. Pereira, T. Malkin, and M. Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In ???, editor, ASIAN ACM Symposium on Information,
References


Riccardo Pucella. Introduction. ACM SIGACT News,
REFERENCES


Puzmanova:2004:RWF


Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI


Pang:2005:NMS


Peikert:2008:LTF

Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In ACM [ACM08], pages 187–196. ISBN 1-60558-047-

[PELZ2003: HCC]


[PY2006: LTT]


[PY2008: MPA]


[PZ2001: CPS]

REFERENCES

//link.springer-ny.com/
link/service/series/0558/1
bibs/2247/22470079.htm;
http://link.springer-

Pieprzyk:2002:CPL


Pieprzyk:2002:CCI


Pecho:2009:APW


Peng:2009:DIE


Qian:2005:CLT


Qian:2005:SPL

Haifeng Qian, Zhenfu Cao, and Haiyong Bao. Security

Qian:2005:SPL
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]
Michaël Quisquater, Bart
Preneel, and Joos Vande-
walle. Spectral charac-
terization of cryptographic
Boolean functions satisfying
the (extended) propagation
criterion of degree l and
order k. *Information Pro-
cessing Letters*, 93(1):25–28,
January 16, 2005. CODEN IFPLAT. ISSN 0020-0190
(print), 1872-6119 (electronic).

[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: proceed-
ings*, volume 1820 of *Lec-
ture Notes in Computer Sci-
cence*. Springer-Verlag,
Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2000.
ISBN 3-540-67923-5. LCCN

[Quisquater:2001:EAE]
Jean-Jacques Quisquater
and David Samyde. Electro-
Magnetic analysis (EMA):
Measures and counter-
measures for smart cards.
*Lecture Notes in Computer
CODEN LNCSDE. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
pdf.

[Quisquater:2002:CTM]
Jean-Jacques Quisquater,
François-Xavier Staedt,
Gael Rouvroy, Jean-Pierre
David, and Jean-Didier
Legat. A cryptanalytic
time-memory tradeoff: First
FPGA implementation. *Lec-
ture Notes in Computer Sci-
CODEN LNCSDE. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
pdf.

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


Raikhel:2000:DF


Rajsbaum:2006:ASNb


Roman:2007:SCP


Ramesh:2001:TAE


Rand:1955:MRD


Rand:2001:MRD


Rijmen:2001:WHF

Vincent Rijmen and Paulo S. L. M. Barreto. The
REFERENCES


Rubin:2005:ARS


Rangan:2001:PCI


Renaud:2009:VPC


Rudra:2001:ERE


Romao:2001:SMA


Regev:2005:LLE


Regev:2009:LLE


Ren:2009:CWT


Rescorla:2001:IOPa


Rescorla:2001:IOPb


Reynard:2001:SCB


Rodwell:2007:NIBa


Rodwell:2007:NIBb


**Rodwell:2007:NIBc**


**Ringenburg:2005:PFS**


**Rotondi:2006:CHA**


**Ren:2009:FCS**


**Rose:2006:CSP**


**Rojas:2000:FCH**

REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


Roychowdhury:2000:PCJ


Roy:2005:ACA


Rieffel:2000:IQC


Ramzan:2000:RSS


Reyzin:2002:BTB

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


REFERENCES


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


Rousseau:2009:MT


Rukhin:2001:STS


Rogers:2005:MPH


Rouvroy:2003:EUF

REFERENCES


REFERENCES

LCCN ????


[Sch03] Mark S. Schmalz et al., editors. Mathematics of


**Salus:2001:CA**


**Salomon:2003:DPS**


**Salus:2003:BRBb**


**Sale:2005:RCB**


**Sallee:2005:MBM**


**Salomon:2005:CDC**


**Salomon:2005:FCS**

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


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

[SB04]

Stoklosa:2005:CIC

[SB05]

Stallings:2007:CSP

[SB07]

Sherwood:2005:MTR

[MS05b]

Steiner:2001:SPB

[SB01]

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


Shaiikh:2009:SAU


Steinfeld:2002:NSA


Seredynski:2004:CAC


Syverson:2001:LAP

Paul Syverson and Iliano Cervesato. The logic of au-
REFERENCES

Shen:2002:NDW


Sun:2002:WDC


Shao:2005:NEV


Stephanides:2005:GAK

REFERENCES


[Sch00d] Bruce Schneier. Secrets and Lies: Digital Security in a
Schneier:2000:SRF


Scharinger:2001:ASK


Schmalz:2001:MDI


Schneier:2001:FSE

REFERENCES


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


Schneier:2004:SA


Schmalz:2005:MDI


Schneier:2005:AE


Schneier:2005:AE


Schneier:2005:TFA

Kai Schramm. Advanced
REFERENCES


Schmeh:2009:VBF


Su:2005:IBT


Scott:2004:CIB

Screamer:2001:MDR


Shen:2005:NCB


Sun:2005:CCL


Sun:2005:RNK


Sebe:2001:OIW


Sebe:2000:SDI

REFERENCES


REFERENCES

Smith:2006:SID

Seifried:2000:C

Seifried:2000:PPA

Seifert:2005:ACR

Speed:2001:PIS

Speed:2002:PIS

Selcuk:2000:BEL

Semanko:2000:CAA
[Sem00] Michael Semanko. L-collision attacks against randomized MACs. In Bellare [Bel00], pages 216–?? ISBN 3-540-67907-3. ISSN
REFERENCES


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


**[SGM09]** Laurent Sauvage, Sylvain Guilley, and Yves Mathieu. Electromagnetic radiations of FPGAs: High
REFERENCES

spatial resolution cartography and attack on a cryp
tographic module. ACM Transactions on Reconfig-
urable Technology and Systems (TRETS), 2(1):4:1–
4:??, March 2009. CODEN ????? ISSN 1936-7406
(print), 1936-7414 (electronic).

Storer:2009:PSR

[SGMV09] Mark W. Storer, Kevin M. Greenan, Ethan L. Miller, and Kaladhar Voruganti. POTSHARDS — a se-
cure, recoverable, long-
term archival storage sys-
tem. ACM Transactions on Storage, 5(2):5:1–5:??, June
2009. CODEN ????? ISSN 1553-3077 (print), 1553-
3093 (electronic).

Stone:1998:PCC

[SGPH98] Jonathan Stone, Michael Greenwald, Craig Par-
tridge, and James Hughes. Performance of checksums
and CRC’s over real data. IEEE/ACM Transactions on Networking, 6(5):529–543, October 1998. CODEN
IEANEP. ISSN 1063-6692 (print), 1558-2566 (elec-
acm.org/pubs/citations/
journals/ton/1998-6-5/
p529-stone/.

Sonntag:2000:MAS

[SH00] Michael Sonntag and Rudolf Hörmanseder. Mobile agent
security based on payment. Operating Systems Review,
0163-5980 (print), 1943-586X (electronic).

Shirase:2005:AEC

Masaaki Shirase and Yasushi Hibino. An archi-
tecture for elliptic curve cryptography computation.
124–133, March 2005. CODEN CANED2. ISSN
0163-5964 (print), 1943-
5851 (electronic).

Seyedzadeh:2011:IEA

Seyed Mohammad Seyedzadeh and Yasaman Hashemi. Image encryption algo-

rithm based on Choquet Fuzzy Integral with self-
adaptive pseudo-random number generator. In 2011
11th International Conference on Intelligent Systems Design and Applications
(ISDA), pages 642–647.
IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD
20910, USA, 2011. URL
org/stamp/stamp.jsp?tp=
&arnumber=6121728.

Shailer:2001:PMT

David M. Shailer. The project manager’s toolkit: prac-

tical checklists for sys-

Shamir:2001:NDC


Shamir:2001:PSC


Shao:2001:BVM


Sharp:2001:IKB


Shapiro:2002:CCM


Shamir:2003:RS

Adi Shamir. RSA short-


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).

Shih:2008:DWS


Sierra:2004:LCC


Shimizu:2007:CBE


Shoup:2000:CTU


Shoup:2000:UHF


Shoup:2001:OR

Victor Shoup. OAEP reconsidered. In Kilian [Kil01a],
UKE47.00. URL http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390239.htm; [Shp99]

Shoup:2005:ACC

Shoup:2005:CIN

Shparlinski:1999:NTM

Shparlinski:2001:UDR
Shparlinski:2002:SMS


Shparlinski:2003:CAA


Shparlinski:2004:BRR


Shparlinski:2004:UDD


Shparlinski:2005:PHS


Sun:2005:SSP

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

Ho:2006:THL


Shyamasundar:2002:ACP


Silverman:2005:ECC


Simon:2002:CRE


Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. A Key Recovery Attack on the 802.11b Wired

Sivonen:2006:MPF

Six:2005:HGS

Schnorr:2000:SSE

Song:2000:TPA
Boyeon Song and Kwangjo Kim. Two-pass authenticated key agreement protocol with key confirmation. Lecture Notes in Computer Science, 1977:237–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
References

Seki:2001:DCR

Stojanovski:2001:CBRa

Sklavos:2003:DDR

Sklavos:2005:ISH

Stavrou:2005:CAS

Stabell-Kulo:2006:ESC
REFERENCES


Werner Schindler, François Koeune, and Jean-Jacques Quisquater. Improving

**Srinathan:2002:ASC**


**Sugita:2000:RAD**


**Schneier:2000:CTA**

REFERENCES

Scharwaechter:2007:AAE

Sterbenz:2000:PAC

Shim:2005:SFA

Srivatsa:2005:SPS

Skoudis:2006:CHR
REFERENCES


**Song:2001:DWF**


**Solar-Lezama:2006:CSF**


**Sarkar:2000:CNB**


**Sarkar:2000:NBC**


**Sebag-Montefiore:2000:EBC**


Hugh Sebag-Montefiore. Enigma: the battle for the code. John Wiley and Sons, Inc., New York, NY, USA,
REFERENCES


Sebag-Montefiore:2007:EBC


Simos:2007:CMS


Smith-Miles:2008:CDP


Seyedzadeh:2011:IES


Smart:2001:CDF


Smart:2003:ACU

REFERENCES

Smart:2003:AGR

Smart:2005:CCI

Small:2006:USR

Smith:2000:ABS

Smith:2001:IK

Smith:2001:ECB
Michael Smith. The Emperor’s Codes: Bletchley
REFERENCES


Smith:2001:APP


Smith:2002:OAP


Smith:2003:FTT


Smith:2008:CFI


Smolin:2004:EDE


Seamons:2009:IPS


Safavi-Naini:2001:BAG


Safavi-Naini:2001:LAC


Sanchez:2001:RNM


Slind:2007:PPS


Song:2000:ISC

[Joo00] JooSeok Song, editor. *Information security and cryptography — ICISC’99: second international confer-
Shigetomi:2002:ALS


Satoh:2000:HSM


Smith:1979:UFM


Shelfer:2002:SCE


Sumii:2003:LRE

REFERENCES


REFERENCES


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


Stipcevic:2007:QRN


Samarati:2001:AMP


Standaert:2003:EIR


Sarkar:2001:PAE


Stubblebine:2001:AAF

REFERENCES

Seznec:2003:HUL

Swiderski:2004:TM

Seddik:2009:IWB

Shi:2008:UAU

Susilo:2000:NEF

Scambray:2006:HEW
REFERENCES


REFERENCES


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


[STK02] Takeshi Shimoyama, Masahiko Takenaka, and Takeshi


[Sti06a]


Saxena:2007:TCP


Shaltiel:2007:LEU


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


Sebe:2007:SMO


Shmueli:2009:DEO


Smith:2000:CIR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Skoudis:2003:MFM]

[Sarikaya:2008:SPT]

[Sun:2002:NAD]

[Sun:2005:WIW]

[Tada:2002:OSM]

[Tan:2001:AES]

[Tan:2007:MMU]
Tang:2007:SGK

Tattersall:2005:ENT

Trichina:2001:SCH

Tistarelli:2002:BAI

Tao:2000:ITF

Tsai:2001:GSI
Chwei-Shyong Tsai and


REFERENCES

[Tippett:1927:RSN]

[Torres:2007:ANS]

[Tseng:2001:GGO]

[Tseng:2001:CLB]

[Tseng:2003:DSM]

[Tico:2003:RAS]

[Toll:2008:CSE]

[Thien:2002:TSS]
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

Tang:2006:CHA


Torrubia:2001:CRC


Tian:2005:RWS


Tsolis:2009:ARM


Teoh:2004:PCK


Tousidou:2000:IMS


REFERENCES

Trimberger:2001:GED


Troutman:2009:CCGa


Tsaur:2001:FUA


Troutman:2009:CCGb


Troutman:2008:VMM


Tsaur:2005:SSS

Tsaban:2006:FGD


Tsang:2007:WCT


Tsai:2008:EMS


Tseng:2007:SAG


Takano:2000:PTH

[TSO00] Kohji Takano, Akashi Satoh, and Nobuyuki Ohba. Poster 5: TATSU — hardware accelerator for public-key cryptography using Montgomery method. In Anonymous [Ano00d], page ??

Tsunoo:2003:CIC

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 LNCS9D. ISBN 3-540-40833-9. ISSN 0302-9743 (print), 1611-
REFERENCES


Toft:2001:LTT


Trappe:2002:ICC


Trappe:2005:ICC


Talbot:2006:CCI


Talbot:2006:CCI


Tsai:2007:TTA

REFERENCES


Tsaur:2005:EUA


Tiwari:2009:CIF


Thamrin:2008:PBR


Tzeng:2004:NTM


Ting:2002:FBS

Tynan:2005:CPA


Tian:2005:NDF


Tong:2009:RAPb


Tong:2009:RAPa


Uz:2009:MBT


Unay:2008:SQE

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


REFERENCES


[UP05] Andreas Uhl and Andreas Pommer. Image and video encryption: from digital


USENIX, editor. Proceedings of the Ninth USENIX Security Symposium, August 14–17, 2000, Denver,
REFERENCES


USENIX:2001:PUA


USENIX:2001:PFT


USENIX:2001:PTU


USENIX:2002:PBF


USENIX:2002:PUS


USENIX:2002:PFT

REFERENCES

URL http://www.usenix.org/publications/library/proceedings/usenix02/

[USS02]

[UST01a]

[Uw00]

[Uzu04]
REFERENCES


REFERENCES


[Voloshynovskiy:2005:ITD] Sviatoslav Voloshynovskiy,

vanDijk:2006:ICS


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.

[VK07]

[Vo:2008:SMA]

[VKS09]

[Viega:2003:SPC]

[Viega:2002:NSO]


REFERENCES


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


Wallich:2004:EEI

Wallich:2009:SGP


Wang:2004:AWA


Wang:2004:TVS


Wang:2005:SCR


Wardlaw:2000:RPK


Washington:2008:BRB


Washington:2008:ECN

REFERENCES


Wayman:2001:FBA

Wayman:2002:BAT

Wayner:2002:DCI

Wu:2002:CSCa

Wayner:2009:DCI


References

Wu:2001:CDS

Weis:2001:SYH

Weeks:2000:HPS
Wu:2001:CKA  

Wu:2003:HDW  

Wu:2003:UFR  

Wu:2004:EIW  

Wang:2005:TAP  

Wang:2009:NWA  


**Weber:2008:IZN**


**Weierud:2000:SFB**


**Weierud:2005:BSF**


**Weierud:2005:BPS**


**Welschenbach:2005:CCC**


**Weiss:2004:JCE**

REFERENCES

Weng:2003:CHC


Wernsdorf:2002:RFR


Westfeld:2001:FSA


Wu:2002:LCN


Wang:2004:CHF


Wang:2002:CSE

[ WG02 ] Xiang Sheng Wang and Juan Ren Gan. A chaotic se-


Wu:2008:RPG


REFERENCES


REFERENCES

**Winterbotham:2000:USI**


**Wincelberg:2001:JQH**


**Windley:2005:DI**


**Winkel:2005:GEC**


**Winkler:2005:SAU**


**Withers:2001:IWU**


**Wang:2007:VBW**


REFERENCES


[WLH06] Hsiang-An Wen, Chun-Li Lin, and Tzonelih Hwang.
REFERENCES


Wang:2005:TSP


Wu:2008:RWM


Watters:2008:VDL


Wheeler:1995:TTE


Watanabe:2002:CCD


Wang:2008:NAD

Wang:2009:RDA


Wolkerstorfer:2001:AIA


Won:2001:ISC

REFERENCES

Wool:2000:KME


Wood:2005:IIM


Wang:2003:SGP


Wollinger:2005:CVH


Weimerskirch:2001:ECC


Wang:2001:TUR

REFERENCES

Wright:2000:IQC

Wright:2001:AES

Wright:2003:FCI

Wrixon:2005:CCO

Wang:2002:IPD
REFERENCES

Wright:2002:EPS

Whiting:2003:MPH

Walter:2005:DDP

Weimerskirch:2002:DLW

Wu:2001:DSM

Wu:2002:CSCb
Hongjun Wu. Cryptanalysis of stream cipher Alphal. *Lecture Notes in Computer Science*, 2384:
REFERENCES

Wuensche:2009:CAE

Wu:2000:PKC

Wu:2001:FED

WvD02

WW00


[W00] John Worley, Bill Worley, Tom Christian, and

Wollinger:2000:HWH


Wollinger:2000:HWH


Wincelberg:2002:LIE


Wang:2008:HQS


Wang:2002:WEM

Wu:2005:CTR

Wyant:2002:APK

Wang:2005:CSA

Wang:2005:FCFb
REFERENCES

Wang:2005:ECSa

Winslett:2005:PLD

Wang:2005:DIC

Xu:2005:ETR

Xu:2001:CPW
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


REFERENCES


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


Yan:2006:ICP


Youssef:2001:CIM


Youssef:2001:IAB


Yang:2005:IME

### REFERENCES

<table>
<thead>
<tr>
<th>Year</th>
<th>Name</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Pages</th>
<th>Electronic Details</th>
</tr>
</thead>
</table>

**Note:** The URLs are placeholders and may not be accessible.
Yen:2003:RSC


Yardi:2008:HAC


Yamamoto:2001:PKB


Yu:2001:TCB


Yi:2009:SSG

REFERENCES

Yu:2005:EHI


Yoo:2002:LAU


Yukewych:2005:CIR


Yue:2006:NCB


Young:2001:RP


Youssef:2001:CAF

REFERENCES

[Young:2004:HRV]

[Young:2006:MCC]

[Youn:2008:WRB]

[Yin:2001:RMW]

[Yilek:2009:WPK]

[Yoon:2004:SUA]

**[Yoon:2005:CFI]**


**[Yoon:2005:IHL]**


**[Yeh:2002:SAK]**


**[Yeh:2004:PBU]**

REFERENCES


**Yanami:2002:DLC**


**Yeh:2003:IAM**


**Yang:2001:EEA**


**Yoshiura:2001:AWB**


**Yao:2009:CAR**

Danfeng Yao and Roberto Tamassia. Compact and

Yang:2004:ENT


Ytrehus:2006:CCI


Yang:2005:SEA


Yung:2002:ACC


Yung:2002:C1

Moti Yung. Cryptointegrity. Lecture Notes in Computer Science, 2501:
Yang:2004:ISE


Yang:2004:CUF


Yang:2005:YWC


Yang:2008:YWC

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

[PHY:2008]
a-Phy schemes with revers-
ing. *The Computer Jour-
nal*, 51(6):710–722, No-
ember 2008. CODEN CM-
PJAA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
comjnl.oxfordjournals.
org/cgi/content/abstract/51/6/710;
org/cgi/content/full/51/6/710;
org/cgi/reprint/51/6/710.

[YANG:2008:FSD]
G. Yang, D. S. Wong, and
X. Deng. Formal security
definition and efficient con-
struction for roaming with
a privacy-preserving exten-
sion. *J.UCS: Journal of
Universal Computer Sci-
cence*, 14(3):441–462, ????
2008. CODEN ????. ISSN
0948-6968. URL http://
www.jucs.org/jucs_14_3/
formal_security_definition,
and.

[YEW:2005:SAS]
Chou-Chen Yang, Ren-
Chiu Ho, Shih-Chuan Yang,
and Wei-Ting Liu. Secure authent-
cation scheme for session ini-
tiation protocol. *Comput-
396, August 2005. CODEN
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167404804002640.

[YY:2000:RBA]
Adam Young and Moti
Yung. RSA-based auto-
recoverable cryptosystems.
*Lecture Notes in Com-
puter Science*, 1751:326–
341, 2000. CODEN
LNCS9D. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[YY:2001:BOK]
A. Young and M. Yung.
Bandwidth-optimal klepto-

**Young:2004:MCE**


**Yoon:2005:SWL**


**Ye:2001:ATD**


**You:2001:GEC**

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.

Zivkovic:2005:AAH


Zhao:2005:SSV

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

Zhang:2000:MCA


Zhang:2004:AIB


Zhang:2005:CHC


Zhang:2009:CII


REFERENCES


REFERENCES

Zheng:2001:ISS


Zheng:2002:NPK


Zheng:2002:ACA

[Zhe02b] Yuliang Zheng, editor. Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and In-

Zhong:2006:ESC

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

Zhou:2002:MVD


Zhou:2002:MVD

**Zirkind:2007:ADC**


**Zirkind:2007:ADC**


**Zhang:2008:IBF**


**Zhang:2002:IBB**

Zhang:2005:CLH


Zenner:2001:ICS


Zhang:2004:AFV


Zhao:2005:MCE


Zhang:2001:QKD

Yong-Sheng Zhang, Chun-Feng Li, and Guang-Can
REFERENCES


[ZP05] Zhiyong Zhang and Jiexin Pu. Delegation model for CSCW based on RBAC policies and visual modeling. In Han et al.
REFERENCES


Zhou:2005:MBI


Zhu:2007:IHH


Zhang:2005:RPE


Zhao:2005:APA


Zhou:2005:APS


Zhang:2001:ASE


Zhang:2003:FSP

Zhenxiang Zhang and Min Tang. Finding strong pseudoprimes to several bases. II. Mathematics of Computation, 72(244):2085–2097, October 2003. CODEN MCMPAF. ISSN 0025-5718 (paper), 1088-6842
REFERENCES


[ZWCY02] Feng Zhu, Duncan S. Wong, Agnes H. Chan, and Robbie Ye. Password authenticated key exchange based on RSA for imbalanced wireless networks. Lecture
REFERENCES


Zhang2001:USC

Zhang2004:NMS

Zhang2008:GPT

Zhou2003:ACN

Zhou2005:ASP
Zhang:2005:ISM


Zhang:2008:FIC


Zhuang:2005:KAE