A Bibliography of Publications on Cryptography:
2000–2009

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

01 October 2019
Version 3.326

Title word cross-reference

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

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p_k)
[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LZL+01, YCH04, CLT07]. (tn)
[PW05, SC05a]. + [Abe01]. {0, 1}
[LBGZ01, LBGZ02]. 1 [Wu02]. $125
[And04]. 128 [AIK+01, PCG01]. 13
[HSL+02]. $15.00 [Imr03]. 2
[Bih00, BGN05, CY02, CKL+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 ± 10
[Mau01]. 2^{28} [Bih02]. 2^k [MFFT05]. 2^m
[KLY02, KKY02]. 3 [BP04, Ben00, ChLY09, CT09, Lav09, OMT02, WH09, ZTP05]. $35.00 [Top02]. $49.99 [Gum04]. $5
[SCF01]. 5 [Pat04]. $51.48 [Pap05]. 512
[CDL+00]. 7 [Gri01, Pat03a]. (2, 128) [WB02].
0 [AIK04]. ABC [PS04b]. d [BD00b]. E_0
[FL01a]. f_8 [KSH01]. g^{13} [Shp02]. g_c(x, 1)
[SZP02]. GF(2) [CP03]. GF(2^m)
[OTT01, RMP08]. GF(p^m) [BGK+03]. GF(p^t) [PZ01]. H_2A [CBB05]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. l
[QPV05]. M + 1 [AS01a]. F_p [CY02]. Z_n
[Gro05]. GF(2) [GS03, KTT07]. GF(2^m)
[BBGM08, KTT07, KWP06, RMH03a, RS04]. GF(2^m) [KKH03]. SL_2(F_{2^d}) [SGB00]. μ
[LN04]. n
[CT08b, Gon06, HKS00, LKJ01, TM01]. N^{0.292} [BD00b]. NC^0 [AIK06]. p [FL06].
\[ p^q \] [LKYL00]. \( p^s \) [CHH01]. \( Q \) [Yas08]. \( r \) [JY01]. \( w \) [DwWMW05, OT03b]. \( x^u \) [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, GHK02, CKL03]. -Source [KLR09]. -st [AS01a]. -Steiner [WL02].

-Threshold [CLT07, Kog02]. -way [LKJL01].

.NET [For04, TG04].

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

0 [And04, BC04a, Gum04, Imr03, Puz04, WYY05d]. 0-07-222742-7 [Gum04]. 0-13-100551-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, IEEE09a].

1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05c, WYY05d, Was08a].

1-Connected [BJLS02]. 1-out-of-n [AOS02]. 1.82Gbits [KV01]. 1.82Gbits/sec [KV01]. 101 [Sei00a]. 10118-3 [ISO04]. 106 [Uni00c, Uni00d, Uni00g]. 106-1 [Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a]. 109-bit [Pri00]. 10th [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. 11-15 [AUW01]. 11th [CCMR05, HYZ05b, HH04, HH05, RM04, Roy05, USE02b]. 12 [TPS01].

128 [JJO2, WFLY04]. 128-Bit [SM03b]. 12th [GH05, MS05b, PT06]. 13-15 [ACM05b]. 130 [LM08]. 14th [AMW07, AAC+01, Bir07]. 155 [LMP+01].

15th [MJ04, BC01]. 160 [KSF00]. 16th [BS03]. 17th [IEE05b]. 186 [Nat00]. 186-2 [Nat00]. 18th [KM07]. 19005-1 [ISO05].


1999 [Lee03b, Uni00a, Uni00f, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Uni01]. 19th [BCDHN09]. 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, WP03]. 2004 [ACM04b, ZC04].

2005 [ACM05a, ACM05b, ACM05c, ANS05, HYZ05b, ISO05, Roy05, Ter08, Ytr06]. 2006 [ACM06]. 2007 [ACM07, An06b, SMO7b].

2008 [ACM08, Dew08, YRS+09]. 2009 [ACM09, May09]. 20th [Bel00]. 21 [AJ01b].

21264 [WB00]. 21st [Jof08, Ki01a]. 21th [IEE09a]. 22 [McK04, TTZ01]. 22nd [Yun02a]. 23rd [Bon03]. 24th [Cra05a, Fra04]. 256-bit [Luc00]. 25th [Sh05a]. 26 [DB04]. 26th [EBC+00]. 27th [Men07]. 29. [Eke02]. 29th [FLA+03].

3 [Duw03, Irw03]. 3-515-07640-9 [Eag05]. 3-540-66778-4 [Duw03]. 3-Key [Kel05].

3.0 [Fiu02b, Hei01, SQ01]. 305 [ECM00a]. 306 [ECM00b]. 30th [Co02a]. 314pp [Duw03]. 3278 [BWWB02]. 33rd [ACM01a].

36th [ACM04b]. 37th [ACM05c]. 39th [ACM07]. 3D [LZP+04]. 3GPP [KSHY01, SM02]. 3rd [ACM05a, USE00a].
3

4 [Duw03]. 4-round [DLP+09]. 40th [ACM08]. 41st [IEE00a]. 42nd [IEE01a]. 43rd [IEE02]. 44th [IEE03]. 45th [IEE04]. 46th [IEE05a]. 47th [IEE06]. 48th [IEE07]. 49th [IEE08]. 4th [BCKK05, BC05c, DWML05, DRS05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, KN03, MS05a, NP02a].

5 [BCJ+06, Wac05]. 50th [IEE09b]. 512 [AD07, GLG+02]. 5th [CV04, KJR05, LL03, LLT+04, Li05, NP02a, Syv02, WKP03].

64 [LKH+08, WWCW00]. 6th [Bla03, Des02, HA00, JQ04, LL04c, MMV06, Oka00].

7 [And04, Gun04]. 7-round [Pha04]. 7.2 [TvdKB+01]. 7th [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].

800 [BFR04]. 8.11 [Coc02a]. 802.11I [Hir09]. 802 [Kwo03b]. 8th [Chr01, Hon01, Jue04, Mat02, SMP+09, VY01, Vau05a, WK06, Zhe02b].

9 [CGP+02, Gan08]. 9/11 [Ark05, Mah04]. 90 [BG07a, Hir09]. 9796 [GM00b]. 9796-1 [GM00b]. '98 [Wil99]. '99 [DN00b].

9th [CCMR02, CSY09, DR02c, DKU05, Lai03, NH03, Pat03b, PY05, YDK06].

= [KOMM01].

A-1 [ISO05]. A.2.4 [Kel05]. A5 [BD00a, BS01, PS01c]. A5/1 [BD00a, BS01, PS01c]. AAFG1 [Hug02].

AAIs [LOP04]. Aarhus [Cra05a]. Abadi [MW04]. Abelian [CF02, PHK+01, RS02].

Abstention [JLL02]. Abstract [CM00,Cou04,DIRR05,HLvA02,HJW01, JLO0,MSJ02,MP02,Mas04,Wag02,BJN00, BCDM00,CD00a,CC00c,FKS+00,GHJ00, GT04,HT04,HP01,Iwa08,IK00,Jun08, KKS00a,KM00,LMO0,Mes00,Pei09,Yas08].

Abstracting [Bla01a, Mon03]. abstraction [BLP06]. abstractions [BG07b]. Abstracts [SCH00b]. Accelerating [ESG+05].

acceleration [EHKH04]. Accelerator [CGBS01,RS04,TS00,XB01,DK+02].

Acceptance [CFRR02]. Access [ARNS01,Ano02e,BNPW03,CGMM02, DS06,HC08,MS03b,Ri02,Sma03a,Sun00a, ZGLX05,AW05,AW08,AFB05,BA06, BNP08,Cho08b,DFM04,Hos06b,HW03c, HY03,JW06,KNS05,LFZ+04,EF07, MSP+08,PS02a,ST07,WT05,WC01b].

access-control [BNP08]. accessible [Pau02a]. accountability [WABL+08].

Accounting [Lai08]. Accumulator [GTH02]. Accumulators [CL02a].

accurate [ZY08]. Achieve [CFS01].

Achievement [Coc01a]. Achievements [VDKP05]. achieving [PS04c]. ACISP [YG01c].

ACM [ACM01a,ACM03a,ACM03b,ACM05a,ACM05b,ACM05c, ACM06,ACM07,ACM08,ACM09,ACM10, MS05b,Bar00b,FMA02,Raj06].

ACNS [GKS05,IKY05,JY04,ZHY03]. acoustic [ZTZ05].

Acquiring [SETB08]. across [Dav07, ZBLvB05]. Act [Kha05,Uni00a, Uni00c,Uni00d,Uni00g,Uni00h].

Actel [DV08]. Action [SE01]. Active [BC05a,BACS02, BP02, JLO0, MA00a, MA00b, Tad02, BP08].

Active-Content [MA00a,MA00b]. activities [AJ08,SN07].

actually [Hau06]. Ad [BS02, KH05, WT02, Cha05b, DHMR07, KVD07, LHC08, LFZ+04,PCSM07, SLP07, TW07, ZC09, MAA04].

'ad-Durayhim's [MAA04]. Ad-hoc [BS02,WT02, DHMR07, ZC09].

Adaptation [ISSZ08]. Adapting [MJ01].

Adaptive [CM00,CBB05,CTL04,CL08,Coc02a,CS02, CS03b,DSS01,EFY+05,FMY01,JMV02,
Adaptively
[AF04b, CHK05, FMY02, JL00].
Adaptively-Secure [CHK05]. Added
[Ano02b, St.00]. Adding [FBWC02].
Addison [Puc03]. Addition
[KT00, LPZ06, PP06a]. Additive
[FMY01, MF01]. Additive-Sharing
[FMY01]. Address
[IIT03, Nik02a, Nik02b, FXAM04, RW07].
Address-Bit [IIT03]. Addressing
[HTW07]. Adi [Coc03]. Adic [GHK+06].
adjacent [JT01b]. Adjustment [BSNO00].
Adlan [MAaTxx]. Adleman [BB79, Coc03, SP79].
Administration [USE00c, USE00a, Ris06, WL04a].
administrative [Cra05b]. Admitting
[HSZI00]. Advance [CZB+01]. Advanced
[CF07, DFPS06, Lan00a, Lnt02, MM01c, Mor05, Sch06a, BBK+03b, DFCW00, ISTE08, Sve08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Coc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NJS00, Pha04, SB00, Sye00, WBRF00, Wri01, YW06]. Advances
[Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS07, ELv01, Ki01a, Oka00, Pi01, Pre00, TIS07, Yun02a, Kat01, Bih03, CC04a, Cra05a, Fra04, Knu02, Lai03, Lee04b, LLT+04, Li05, LST+05, Men07, Roy05, Sho05a, Zhe02b]. Advantage [SZ01]. advantages [CDS07]. adventures [Hroach].
Adversarial [CLR09, GSS08, MNS08].
Adversarial-knowledge [CLR09].
Adversaries [CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05]. Adversary
[Aba00, Gor06, RW02]. AES
[CGH+00b, DRS05, FIP01a, Her09a, Pha04, AG01, Ano00a, AL00b, BDK+09, CG03, Coc02b, DR00b, DR02a, DR02b, DLP+09, DPR01, Dan01, Dra00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, IKM00, IK00, IK01, Joh00, KS09a, Kel05, KS00, KV01, LP02a, Len01, MHH+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTV07, PQ03b, RRY00, SKS00, SM03b, Sch00b, SKW+00, SW00a, SL00, WW00, WB00, WOL01, WWGP00, WWC00].
AES-CBC [Fer06]. AES-like [DLP+09].
AES-related [Sch00b]. Affine
[Ben00, CT09, Fel06, HH09].
Affine-Transformation-Invariant [CT09].
AFIS [Zir07]. African [WD01b]. after
[Ber03, McL06]. again [Fox00]. Against
[CS05b, DM07b, FKS00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Bau05, BPR00, BP02, BBB+09, BBB+02, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egh00, EBS01, FP01, Fry00, Geb04, HNZI02, HLL+01, HG07, Hsu05b, HLC08, Ino05, ISW03, IIT03, JKS02, JJS00, JT01a, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, Mit00, Mól02, MG08, NRR00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC+02, PSP+08, PS01b, PQ03b, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sh00b, SKU+00, SK01, SLL+00, Tad02, TV03, VHP01, XH05, YJ00, YKL02a, YKL02b, YKL03, ZCW04, ZSJN07]. Age
[Mar08b, Lev01]. Agency
[AJ08, Bam02, Kov01]. Agent
[HQ05, CK02, PZDH09, RS01, RC01, Rot01, ZYM05, KXD00, SSM+08, SH00].
Agent-Based [HQ05, SSM+08]. Agents
[WHI01, Ha06, LSA+07]. Ages
[Eag05, Kin01]. Aggregate
[BGLS03, WK05]. Aggregated [ZSN05].
Aggregation [Her06, CCMT09, MS09b].
Aggressive [Wyl05]. AGM
[Gau02]. Agreement
[AAFG01, CT08a, GW00, HR05, HS07, RW03a, SK00, Tan07b, ABB+04, AKNR04, CY05, CYH05, Che04a, CY05, CJ04, CJL05, HWWM03, Jua04, KPT04, KRY05, KHKL05, LKKY03a, LKKY03b, LL04a, LLL04, LLL05a, LKY05b,
agricultural [Lov01]. Aided [NS01b, HLL+02]. aim [Pau02a]. Aimed [SFDF06]. Airport [Sas07]. Airwaves [Dav07]. Ajtai [GK05]. AKS [Che03]. Al [MAaTxx, Hwa05, Irw03, KJY05, MAaT05, MAaT07, PKH05, XY04, YRY05c, ZAX05, MAaT03, MAaTxx]. al-fusul [MAaT05]. al-Ka [MAaT07]. Al-Kindi [MAaT03, MAaTxx]. al-mutargima [MAaT05]. Alan [Pet08]. Alcatraz [LSVS09]. Alchemy [Pag03]. alert [AJ08]. alerts [NCRX04]. Alexandria [MS05b]. Algebra [Cou01, CD01a, Lan04a, CKY07, Fau09, HW03a, HWR09, Shi05b]. Algebraic [AK03, Bar09, Can06b, CMR06, CM03, Cou03, CFS05, FJ03, FSW01, GV05, GPS06, HR04a, HM02b, Hug02, Mas04, MN01, MR02a, MR02b, PDMS09, Bu09, CKN06, CDL06, Iwa08, May09]. algebraically [RBF08]. algebras [BDFP02]. Algorithm [ANS05, AEMR09, Bar00a, Bar00c, Bi09, BSC01a, ChLYL09, CU01, CJ03a, CJS01, CTL01, CG03, CC06, CH07c, CKM00, CT03, CP03, DR01, DG00, Dhe03, EYCP00, FBW01, FMS01, GMM01, HTS02, HM02c, HZLS05, JKK+01, KBD03, KMM+06, KY02c, KLB+02a, KTT07, KV01, LPZ06, MM01b, MM01c, MS02e, NMS01, OS01, PZL09, PB107, Ram01, RS01, SS01a, SPQ06, WHL05, Wes01,Wie00, AJ08, App05, BF06a, Bla00, C009a, CH01, CKY05, CYH+07, CHH01, FP09, Fer06, FSG08, GPX08, Jon08, K01, Kw02, Kwa03b, LCP04, LLLZ06a, LLLZ06b, MN14, OS07, SC505a, SM08, SzP02, TM01, WL02, WN05, Wuo09, YRY05c, And03, SA02]. Algorithmic [Hro09, J09, Has01b]. Algorithms [AD07, Ano09b, Ab09, BKLS02, III00, BWBL02, CPhX04, CLR01, Dan07, DWN01, FW09, Gau02, GL06b, Har06, Har00, Int00, JP03, Kel05, Lee03b, LR07, LP02b, PBB02, Pre02a, Pre02b, SL00, TLY04, TV03, WBRF00, WWGP00, AHK03b, Ano01j, Ah05, CKL+09, CCM01, GHP05, GHC08, HW03a, HWR09, HHG06, Hro05, JK01a, MCHN05, Pre07, Rhi03, TC05, XLMS06, ZLS07, Zir07, dH08]. Alien [Wil01b]. All-or-Nothing [Des00c, SR00]. Alley [DR01, Wei00]. Allied [Han03, Han06]. Allocation [CCM05, LZ09]. Allowing [JLL02]. Almost [AP09, BS00a, Ju01, Mar02b]. Alpha [WB00, Wu02]. Alphal [KHD01]. Alternating [Wer02, HKPR05]. Alternative [Bad07, Gar03a, Han00, BM02b]. always [BB79]. am [Eke02, SU07]. Anamal [BC05c, CP03]. Amenability [WW00]. America [DB04]. American [GL05, Kat05b, Alv00, Naf05]. Americans [WD01b]. among [BN00a, CT00, SKU+00, Win05c]. Amongst [Pem01b]. Amplification [CHS05, LTW05, RK05, SV08b]. Amplified [KKS00a, KKS01, KML+02]. Amplifier [Pl01]. Amsterdam [Kmu02]. Analyses [BPR05, Des00a, Pau01]. Analysing [BL02]. Analysis [ARJ08, ABR01, A05, Ano01c, AIK+01, ARC+01, Ava03, BN00a, BdhK09, BRS02, BF05, Bor01, BSL02, Cry00, CK02a, CS03b, DPV01, Dra00, FL01a, FGM00a, Gir06, G001c, GH05, GLG+02, GPR06, HSZ01, HK01, HS04, Hey03, HM02c, IT03, JK10a, JQY01, JT01a, JQY01, hKL00, KMS02, LCK03, LKHL09, LY05, LW00, LH07, M006, Mar02b, Mas04, MS01, M0M09, M0a01, Mes00, Mes01, MAaTxx, MG08, N02b, NSS02, OS06, OOP03, Puc03, Q01, SSST06, Sh01c, Sma03b, SDMN06, SQ01, SWT07, YSS+01, ZC00, ZGLX05, AvdH00, AW05, AW08, Ab01, AHK03b, As04b, BDS08, BBK+03b, Bjo05, BG07a, BR05,
BCJ+06, CKL+09, CW07, CS05a, DS09, DKS08, GW08, GM04, GTZ04, Has01b, Hir09, Hro05, Hut01, JEZ04, JPL04, JSW05, KS00, Kor09, LKH+08, LMW05]. analysis [LW05a, LKHL01, Ls07, Mea04, MT07, MRST06, OS00, P09+09, PS08b, SK01b, WL09a, WP05, XH05, XMST07, YCW+08, YC08, ZWWL01, ZL04c, ZDW06].

Analytic [LW05a, LKJL01, Lu07, Mea04, MT07, MRST06, OS00, PSG09, PS08b, SK01b, WL09a, WP05, XH05, XMST07, YCW+08, YC08, ZWWL01, ZL04c, ZDW06].

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

anatomy [Bam02].

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, ELv01a, Fra04, IEE00a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE08, IEE09b, Ki01a, MZ04, Men07, S005a, USE01b, USE01a, USE02c, VY01, Yun02a, ACM00, Bel00, HA00, Jef08, NH03, ST01d].

anomaly [RCG+05].

Anonymous [ABC+05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL+08, SOOO2, Wan04a, YT09, Z09, BP03a, Chio08b, Chi08d, EY00, LH08, Sace02, Sha03c, WC05, YTWY05, ZC09].

ANSI [H00, Kel05, Oiw09].

ANSI-C [Oiw09].

Answers [PT08].

Anthony [Pag03].

Anti [Kha05, A005c].

Anti-Circumvention [Kha05].

anti-virus [A005c].

anticipation [Goo00].

Any [Fis01b, HNO09, A005b, CDM00, DFM04, DMS00, H07, P000].

Anyone [Ros07].

Anywhere [DJL01].

Apache [Had00].

API [W01, Mor03].

APIs [BM01c].

Appendix [Kel05].

Applet [ZFK04].

applets [Bis03a].

Applicability [Wya02, TM01].

Application [ADI09, ACS02, Bai01b, Boy01, CL02a, CKQ03, Dam07, Dhe03, GHK+06, HF00, IKP+07, JX05, Jou04, Lai03, Lee04b, LLS05b, LXM+05, NP07, Oka00, Pf01, PQ03b, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TW08, TEM+01, UHA+09, WG05, YS01, Zhs02b, BG09, CMKT00, CP07, DM08, FP00, HCBLETRG06, JRS09, Lav09, MT07, MPH06, MK05a, NZS05, RSS04, SSST06, T00].

Application-Aware [IKP+07].

Applications [AF04b, AC02, AGT01, And04, BLST01, BH05, Bar06b, BI05a, BKG+03, BS00a, Bih03, BGOY08, BSS02, BL08, CC04a, CD00a, CV02, CGHG01, CZ05, CHSS02, CS09, Cra05a, CD05, DJ01, DK02, DK07, DA03, DFPS06, FR02, GSS08, GKK+09, GJKR03, Gen04a, GRW06, Gol01a, Gol04, HRS02, HN06, Has01a, HSS04, HR05, HJW05, JTO1b, JYO1, KMM+06, KGL04, KMO01, KBB09, KKKM01, KM02, MA007, MM07b, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Syl03, SXY01, SPQ06, Vae02, Wao02, XYL09, Z00, Zee00, Zho02, ÁCTZ05, At04, 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, Lao00, Lee04a].

applications [LJ05a, LPW06, LB05, MY01, MA006, MC04, MSV04, Nie04, PW08, PB07, PC00, Q000, Ros06b, SSS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPHH06, WW08, WA06, WV00, YS04, ZBP05].

Applied [HW03a, HW09, SL07, GV09, GNP05, IKY05, JY04, ZY03].

Applying [Elb09, Ko02, Lan00d, LMSV07, S001, SM002, TN09+09, vDKST06].

Appointed [CL01a].

Apprehension [AJ08].

Approach [BKM07, CGFSH09, CDR01, CW09, Ch08a, CB01, DJL01, Kra03,
Lai07, LL05c, Lut03, OMT02, PBD00, Pau02a, Pre02a, SKG09, VH09, VVS01, Vir03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLMM05, GGH+08, Har05a, JJ01, JW01, KVD07, LG09, LYC02, Ma05b, M09, Mos06, NN03, SLP07, SK03, SN04, SW00b, ZLX99, ZSZ01, ZL04b, ZL04a. Approaches [CGMM02, AvdH00, DG05, Fri07, Has01b, KXD00]. Approval [Wan04b]. Approximation [CLZ02, Kuk01, WL02]. Approximations [BDQ04]. Apress [Ter08]. April [Ano00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH+00b, DFPS06, Joy03b, Knu02, Mat02, NIS00, Nac01, Sch01d, SMP+09, YDKM06]. APSS [ZSV05]. Arabic [MAaTxx]. Arbitrarily [RW03b]. Arbitrary [AR01, BR00b, BR01, CKN00, CHJ+01b, CF02, Tee06]. Arbitrary-Length [AR01, BR00b, CKN00, CHJ+01b]. Architectural [ASK07, AB00, BMA00a, BMA00b, BMA00c, CW02, Gro03, KV01, LTM+00, ZYL05, Ano05c]. Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LKM+05, LZ04, LXM+05, Lut02, MFS+09, Rot02a, SMTM01, SM03b, SLG+05, Uzn04, Che00, CC05c, DHL06, Ino05, LHL03b, MPPM09, SKW+07, SHL07, SH05, Tan01, WWA01]. Architectures [BGK+03, KLY02, RM02, SM02, Con04, DP04, GKS05, NdM04, RH00, WH02b]. Archival [SGMV09]. Archives [RC01]. Archiving [DMSW09]. Area [BP03a, Cal00c]. Areas [HH04, MZ04, PT06, VY01, AMW07, Buc00a, HH05, HA00, NH03, ST01d]. Aren’t [Bau01a, Bau01b]. Arguments [HNO+09]. ARITH [BS03, BC01, IE05b]. ARITH-15 [BC01]. ARITH-16 [BS03]. ARITH-17 [IE05b]. Arithmetic [BS03, BIP05, BGK+03, BCDH09, BC01, CT03, Gro03, IE05b, KM07, Kir03, PPV96, RDJ+01, SR06, GPS05, PS04a, SOIG07]. arithmetics [Lam91]. ARM7 [DV08, XBO1]. Armies [Ano03b]. Army [Boy03]. Arne [Bec02]. array [DZL01]. Arrays [ABM08, BS00a, GC01a, HWW05, P06a]. Arrived [Law05]. arsenal [Blu09]. Art [And07, Bis03b, Col03, Ma05a, MZ02, CS07a, DMS07, Eri03, Eri08, MES02a]. Article [Che08b]. Artifacts [EHK+03]. Artificial [Cop04b, MMHY02]. Arun [For04]. ASCI [MJD01]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DN00b, KI01a]. ASIP [SKW+07]. asks [Ano08a]. ASM [MK05a]. Aspect [Kos01a]. Aspects [BLMS00, CM06, Pe06, AN03, DLP+09, Rup09]. Aspiration [Ash03]. assembly [Gou09]. assessing [CDD+05]. assessment [CC05e, DMS07]. assets [KH03, NRR00]. Assignment [BRTM09, HC08, CHC04, CJ03c, DFM04, HW03c, Hwa00, Lin01a, TP07, WC01b, hY08]. assignments [SWR05]. Assisted [ECC+07, XS03, Art04, BB05, LHL04a]. ASSL [VH09]. associated [XLMS06]. associativity [HR08]. Assumption [CS00, DN00a, FOPS01, KZ03, ZD05]. Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT+00, Nao03, SB02, Mic02a]. Assurance [LXM+05, AL04, BJ02, FOP06, Gha07, Jen09]. Assurances [Bar06b]. Astrology [Pag03]. Astronomy [MYC01]. Asymmetric [CH07b, Man01, SY01a, SBZ02, WH01, YG01a, GJ04, Lee01, OP01b]. Asymptotically [vDW04]. Asynchronous [CKPS01, FLM+03, KSR02, SKR02, ZSV05]. at-targama [MAaT05]. Atlanta [IEE09b]. ATM [Pat02a, Pat02b, Zee00]. Atomic [CNV06]. Attached [RCBL00]. Attachments [Ric07]. Attack [Ahm08, CKQ03, CS05b, CS03b, Des00b].
Fil00, FV03, GHJV00, GHJV01, HQ01, Hug02, HW01, J00b, KCP01, KSO0a, KML+02, KM01c, LY07, LNL+08, LV04, LMV05, Luc02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, P03b, RMS05, SGM09, Sch01b, Sho00b, Sma03b, VHP01, YKLM02a, ZC04, ASK05, DKL+00a, Duj08, Duj09, GM00a, HAU04, Hes04b, HG07, Iwa08, JJ02, KS09a, KM04a, LM08, Law09b, LS05b, Mir05, OS00, SIR04, XY05, ZCW04.

Attack-Resistant [LNL+08]. attacker [BDSV08]. Attackers [JMV02]. Attacking [FMP03, KPR03, TMMM05, BF06a].

Attacking-Based [TMMM05]. Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, BM00, BBB+02, BK+09, BU02, BM03b, BCP02b, BM01c, Can06b, CS07b, CZ03, CT08a, CJ01, CKM00, CJNP00, CM03, Con03, CWR09, CD01b, DPO04, DJ06, DS08, DM07b, FKS00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GK02, HSH+08a, HNZ02, HR04a, HSH+01, HLC08, ISW03, JK02, J00d, KKS00a, KS00b, KKS01, KCJ+01, KI01a, Law09a, LLS05a, LW05, LJ05b, MOP06, MP06, MF01, McK04, Mes00, Mes01, M0102, MG08, OT03a, OT03b, OOP03, OST05, Ove06, PKBD01, PDS09, RS01, SK01q, Sen00, SWT07, Tad02, VV07, WYY05a, WYY05d, WLZ05, YYD001, YY01, YG01b, vW01, BP08, Bau05, BC08, BZ03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05a, HL05b, Ino05, IM06, JDJ01, KS05a].

attacks [KTC03, LPV+09, LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RG05, Sch00c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07a, WL04b, Yun07, YS02, ZSNJ07].

Attitudes [FDIR00, CF05]. attractors [HHYW07]. Attribute [LY05, RSA00e, IY05]. Attributes [SS01b].

Auction [AS01a, Ano01a]. auctioning [RCG+05]. Auctions [Bra01b]. Audio [Arn01, CS05c, DRL09, MH05, WNY09, WWL+02, XE01, WQ08, BS01b, KJ05, KN03]. Audio- [KJ05]. Audio-and [BS01b, KN03]. Augmented [CS07c, Y01]. Augmenting [AL04].

August [AMW07, Be00, B+02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KKP02, Kl01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch04b, Sch05a, Sh05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Y02a]. Australia [Boy01, IZ00]. Austria [DKU05, Pi01, Jef08]. Authentic [DGMS03, D001b]. Authenticate [Ban03a, Bau03b].

Authenticated [AGT01, BN00a, BPR00, BU02, BC04b, BM01, BCP01, CPP04, Ch08e, DG03, DA03, EP02, GKK007, GL03, GTTC03, HOY01, KY03, Kra01, Lee01, LHT09, MPS00, Mac01, MSJ02, MN+04, NA07, Nam02, Ng05, P01, SK00, Vau05b, WC01a, YPPK09, Y04, ZW02, BKN04, BCP07, CY05, CY05, CHE04a, CL08, CJ04, CJL05, DG06, GL06a, GM005, HT08, HWW02, HWW03, Hsu05a, Hwa05, HL05c, JL05d, J04, KOY09, KRY05, LKK03a, LKK03b, LL04a, LL05b, LKY05c, LKY05d, LHC08, LLL02, LL06, LWW05a, Mi08b, PQQ03a, PQ06, RB03, Sei05, SW05, SC05b, TL05, TJ01a, Tse07, WL06, WH02a, XY04, YW05, YC09a, YS02, YSH03, YRY05b, YPK08, ZC04, ZAX05, ZWW05b, ZL05].

Authenticating [AIP01, Ch08a, CGV09, Fur05, JW05, PM08, RCBL00, YSS+01, Lin01b].

Authentication [AAK09, AP09, ANR01, An01b, An01c, An01e, An02d, AHK02, ANL01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, B K00, BCC01, BCC02, BC05b, BDBK09, BR02, BDFP05, BDF01b, BM03c, BL02, BL09, BWE+00, CV03, CG08, CS07b, CC01b, CL01a, CL01b, CC05b, CC09, CJ02, CJ03d, CW05, CT09, Cim02, CIR01, CFR02, CK+02,
CF05, CJK+04, Cou01, CMB+05, Dav07, DP00, Dw03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, FDIR00, Gan01a, Gar03a, GMW05, GSV06, GD02, GT02, Gut04c, Had00, HSZI01, HSHI02, HSHI06, HKW06, HY01, Hs01b, HP00, HL07, ISSZ08, Jab01, JP02a, JP07, JP02b, KJR05, KC09b, KH05, KVD07, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LTL+04, LB04, LL05c, LSH03a, LM00, LOP04, LHL+08, Lys07, MW06, MM01a, Mal02]. Authentication [MJ04, MD04, MR03, MGC02, MNT06, Nao02, Nik02a, Nik02b, OKE02, PK01, Qu01, RKZD02, Ric07, Ril02, SNWX01, SR01, Sch04c, Sch05b, Sei00b, SY01b, SB02, Sm00, Sm01c, Sm01d, SE09, SK06, Str01b, SJ05, SYLC05, SC01, TK03, TZZ09a, TZT09b, Tsa01, VN04, WLLL09, WC09, Way01, Way02a, Wsa06, WK08, WT02, WS03, WL07b, WL05b, XYL09, YJ01, YEP+06, YSR01, YLLL02, YKW01, Zaf00, ZBL05, AvdH00, AF04a, AI00, An00k, An00l, AO05b, Art04, AAKD09, Asl04a, Asl04b, AL04, Ayo06, Bel04, BGP02, BSSM+07, BFG04, BFG05, BS01b, BBJ+02, BDFP02, BM07, Cer04a, CB05, CC01a, CCK04a, CL04d, CC04b, CCK04b, CC05c, CZ03, CY05, CCS08, CWJT01, CHT01, CJ03b, CH07a, Chi08b, Chi08c]. Authentication [Ch08d, CL09, CF07, Coc01a, CmDV06, Dal01, DSGP06, DY09a, DGK+04, DG05, DW05, FLZ02, FC05, FGM02, Gar08, GGC+04, GY08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Her09b, Hsu05b, HLJT09, HY03, HLL04, HL05b, sHP09, JPL04, KLY03, KJ05, KN03, KTC03, KCL03, Ku04, KC05, KCC05, LC03, LH02, LL03a, LF03, LKY04, LW04, LHL04a, LKY05a, LLY06, LLS+09, LFHT07, Li05, LST+05, LCX08, LW05a, LL06, LF04, LHL03b, LH03, LT04, LC04a, Lin07, LN04, LL08a, LLW08b, LC05a, LC05b, Lk01, MS09c, MABI06, 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, Sh05c, SLH03, SSM+08, SW06, Shi05, SL05a, St00, Ste05a, SW02]. Authentication [SCS05b, SC05c, SCS05c, SCS06, SY06, TM06, TB02, TOEO00, TIS07, TW07, Tsa08, TW05, UBE09, VM03, VK08, Voi05, Wac05, WL05, Wac04a, WL05a, WDLN09, WDC09, WC03b, WL04b, WHHT08, Xw08, YW04b, YW04a, YWC05, YW05, YTW05, YC09a, YC09b, YS04, YRY04, YRY05a, YRY05c, YRY05d, YY05b, YbJf04, ZK05, ZSN05, Zha06, ZD06, ZSJN07, dB07, CS08b, ECM00a, ECM00b, LSH03a]. Authenticator [CK07, jLJ07]. Authenticity [AB01, Bla02a, CBD+05, GJ03, GOR02b, HG03, RW03b, Sch01a, Mit02]. AUTHMAC_DH [Asl04b]. Author [An00b, An01d]. authorisation [SN07]. Authorities [CHSS02, HWW04, WH02b]. Authority [Con00, JLL02, CCH05, KB09]. Authorization [BACS02, CJK+04, LSZ05, RKZD02, YT09, GJJ05, JE204, Ln07, LOP04, SR01, WL04a, WZB05, YbJf04]. Authorship [Top02], auto [YY00]. auto-recoverable [YY00]. Automata [LZ04, MGC02, Wue09, Bao4, CC05d, KK03, La00, LQ08, Mon03, SBZ04, SHH07, TC00, dRMS05]. Automatize [Bur02]. Automated [CD01, LL05, LL09, HJW05, IY05, LS05b]. Automatic [BD04a, GJJ05, GL00, ST01c, XNK+05, RG05]. automorphism [Pae03]. automotive [LPW06]. Autonomic [VH09, Che05b]. autopsie [Car00]. auxiliary [Dan00, DK09]. availability [CBD+05]. Available [DJLT01]. AVBPA [BS01b, KJR05, KN03]. Average
average-case [Mic02b]. 
Award [RSA03a, Bar00b, Coc03]. 
Awarded [Coc02b]. 
Aware [IKP07, OHB08a, CBSU06, OHB08b, Zea00]. 
Away [Coc03, Ols00, Tee06]. 
Awareness [HLM03, BK05]. 
Away [Tyn05]. 
Avoided [CNPQ03]. 
Avoid [Mic02b]. 
Away [COC02b]. 
Aware [IKP07, OHB08a, CBSU06, OHB08b, Zea00]. 
Awareness [HLM03, BK05]. 
Away [Tyn05]. 
Avoided [CNPQ03]. 
Avoid [Mic02b]. 
Away [COC02b]. 
Aware [IKP07, OHB08a, CBSU06, OHB08b, Zea00]. 
Awareness [HLM03, BK05]. 
Away [Tyn05]. 
Avoided [CNPQ03]. 
Avoid [Mic02b]. 
Away [COC02b]. 
Aware [IKP07, OHB08a, CBSU06, OHB08b, Zea00]. 
Awareness [HLM03, BK05]. 
Away [Tyn05].
LLW08a, LLW08b, LCC05, LSA+07, LCZ05c, LCZ05a, LCC06a, LCC06b, MW06, MS09c, Mic01, MR09, MI09, Mit00, MB08. based [MC04, MPPM09, MV03b, NZCG05, NC09, NSNK05, OS09, PCSM07, PW05, PBBM01, PFG+09, PS08a, Pel06, PSP+08, PC00, Pha06, PLJ05a, PLJ05b, QCB05a, Reg03, Reg04, RG09, RCG+05, Sae02, SG07, Sco04, Sei05, SFG02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SLH03, SCS05a, mSgFL05, SSM+08, SW05, SH00, SK01b, SCL05, SLC05, Sun02, SCS05c, SY06, TNG04, TWNA08, Tsa08, Tsa05, UHA+09, UBEP09, VS01, VKS09, WAF00, WLT03, WLG07a, WLP07, WNQ08, WLHH05, Whi09, WVO0, WH02b, WY05, WC05, XMST07, YY04a, YCW+08, YIW08, YC09b, YS04, hY08, YJ00, YPSZ01, YRY05c, YPK09, YY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRMS05, NZS05].

Basics [AAC+01, ADDS06, BKP09, BV+02, ČvTMH01, EBC+00, FJ03, FLA+03, CCT08, Fau09, ZT03]. Basic [Gol01b, Gol01a, Gol04, Kat05b, Puc03, Ste02, Bon00]. Basics [Leh06, Lut02].

Basing [BPR+08, CHL02, AGGM06, AGGM10]. Basis [RMH03b, Vav03, vW01, GPS05, LS05b, RMH03a]. Batch [Ara02, HLT01, PBD07, Sha01d, BLH06, HLH00].

Batching [SB01]. Battery [CBSU06]. Battle [Bud00a, Bud02, SM00c, SM05, SM07a]. Bay [Cal00c]. Bayes [Goo00]. BB84 [Iau02a]. BC [IEE02]. BCH [MLC01].

BDD [KLN+06, Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01]. Beach [IEE00a]. beat [Lee01]. because [AJ08]. Become [Ont00]. Been [Nic01].

BeepBeep [Dri02]. before [Uini0a, Uini0b, Uini0f, Uini0e, Uini0h, YJ00]. Beginning [Dew08, Hoo05]. Beginnings [Bud00b]. Begins [MP00]. Behavior [Vav03].

BEHEMOTH [Bar00c]. behind [Hen06b]. Beijing [FLY06, LST+05]. Being [ASW+01, ES00a]. beleid [dl00]. Belgium [DR02c, Pre00, QS00]. Belief [BPST02]. believing [Buh06]. Bell [BZ02, Eke02].

Benchmark [Asc02, TLYL04, LDH06, YLT06]. Bendy [Sas07]. Benefit [YKL02a]. benefits [CH00]. Benford [NM09]. Bergen [Ytr06].

Berkley [IEE06]. Berlin [FLA+03]. Bermuda [Bl03]. Bernard [DNR03]. Berners [Coc02b]. Berners-Lee [Coc02b].

Best [Bau01a, Bau01b, MFS+09, Gol08, Ste02]. BestCrypt [Bau02b]. Bethesda [ACM09].

Better [FV03, PM00, RR02, SKQ01, HLLL03, Pau03]. BetterBASIC [ASW+01].

Between [DKMR05, Ket06, Ngu05, NN06, Fau09, GKM+00, GC05, MSV04, Pau01, RW03a, Sch02, Sch04d, SK06].

Beurling [Bec02]. Beyond [Gar06, Hei03, LMW05, Mar08a, Sch03, Sec04, Sty04].

BGP [ZSN05, vOWK07]. Bi [Con04, PJK01].

Bi-directional [PJK01]. Bi-linear [Con04].

Bias [CL02c, Se100]. Biased [BS00a, LSKC05]. BiBa [RR02].

Bibliography [Bee05]. Bidiagonal [BR09].

Bidiagonal-Singular [BR09]. big [RR03a].

BigNum [SR06]. Bilateral [CT08a].

Bilinear [BGLS03, BMS03, CL04a, HMO5, KK02, DSGP06, LC05b, VK08]. Bill [Gen00a]. billing [SSM+08].

Binarization [LSK05]. Binary [AD09, HHM01].

LSK05, OSSST04, SKG09, WCJ09, ACTZ05, BG08, BG09, FSGV01, GB09].

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

Binding [DN02b]. BioAW [MJ04].

Biometric [AHKM02, Dal01, EM03, HWH01, KJR05].

LLT+04, PMRZ00, PK01, SR01, Sas07, Way01, Way02a, Wea06, BS01b, KN03, Li05, LST+05, MR00, RFR07a, RFR07b, RFR07c, Smi00, MJ04, TBJ02, ZJ04].

Biometric-Based [PMRZ00]. Biometrics [Ash03, Bjo05, MR03, RLi02, Str01a].
BSSM+07, BCP+03, Buh06].

Biometrics-Based [Ril02]. Biomolecular
[Bi09]. Birds [MLM03], birth
[Bud06, SE01]. Birthday [Wag02].

Bisimulation [BJP02]. Bit
[AIK+01, BK06a, BL08, CSHG01, CDL+00,
DMS00, GS07a, ITO03, KZ07, LNS02,
MS08d, PCC01, RMM03b, SM03b, SXY01,
VKS09, ATSVY00, Barb0a, BK07, GPX08,
KZ03, KKL09, Luc00, Pri00, RMPI08,
SWR05, UHA+09, WW08, ZFK04].

Bit-Fixing [KZ07, KZ03]. bit-substitution
[GPX08]. BitLocker [Kor09]. Bits
[BS01d, SZ01, HN04, Shp02]. Bitslice
[DPV01]. Black [An01i, CF02, CNS05,
DI05, DRR05, DS08, KY01d]. Black-Box
[An01i, BR02, CF02, CNS05, DI05,
DRR05, KY01d]. Blackmailing [PS01b].

Bletchley [Sal00b, Cop05, Op06, HS01a,
Sal05a, SE01, Sm01b, Wei06, Win00]. Blind
[AO00, BNPS02, BB00a, BSC01b, CL01b,
GSK09, JKK+01, LY07, Na05, Pan02b,
SPK08, ZTP05, ZK02, Fan03, HC04a,
JL01, JL04, LH05, LCZ05b, MS09a,
SV08a, SHT05, WH05, ZC05]. blindness
[AvdH00]. Blink [Sas07]. Block
[AIK+01, BBC+09, BKR00, BR02, BR02,
BSC01a, CvTMH01, Can01b, CL01b,
CP02, CM+05, Cr01, DR00a, Dwe03,
EYC00, Flu02a, HSH+01, JKK+01, KCP01,
KYHC01, KKG03, LLR07, LRW02, MV00,
MS02e, NPV01, OMSK01, Pat01, PS06,
Pit01, RMS05, SM03b, SY+02, SKU+00,
SK01, WC09, XH03, YG01a, Bai01,
BF06a, DY01, Dun06, Egh00, GPX08,
Hey03, JK01b, Jun05, Kat05a, KJ01, LDH06,
LC04, LKH+08, MM05, PSS+08, RBB03,
SHR04, SHT07, WF02, XH05, Y00].

Block-Based [LLR07, BBC+09].
Block-Cipher [BR02, RB03].
Block-Cipher-Based [BR02].
Block-DCT [BS01]. Blockcipher
[GM02c, OS07]. blockciphers [Fur01].

Blocks [Jou02]. Blockwise [JM02].
Blockwise-Adaptive [JM02]. Bluetooth
[GB02, LV04, LMV05]. Blunders [Bur01].
Blur [VHP01]. Blur/Deblur [VHP01].
Blurring [LS05, SK06]. Board
[CGB01]. boat [DB04]. Body
[Bam02, TG07]. BOEL [Fin02]. Boethius
[Eag05b]. bolstered [An01i]. bombe
[Wil01a, Tur04]. Bombes [An01i, LBA00].

doms [Lov01]. Bonds [CAC03]. Boneh
[ASK05, Hes04a]. Bonn [DRS05]. Book
[And04, Duw03, Eac05, Fai07, For04, Gas01,
Gun04, Im03, Jan08a, Lee03a,
Lee03b, Mar05a, MP01b, Nie02a, Nie04,
Pag03, Pap05, Rec01, Rot07, Sal03b, Sea04,
Shp04a, Sin02, Spr03, Sty04, Ter08, Top02,
Uzu04, Wal00, Was08a, Kat05b, Lam07,
Lun09, MA05, Sin09, Sin00, AAG+00].

Books [Dr.00c, Rec01]. Bookshelf
[Lut02, Lut03, Wil01b]. Bookworm
[Sal03]. Boolean
[Car02, CT03, CS09, MS02b, QPV05,
SM00a, SM00b, SM03a, WV00].

Boomerang [KKS00a, KKS01, KML+02].

Boot [HSH+08a, HSH+08b, HSH+09].
Border [MJJ07]. Borders [PCT07].

Boston [USE01b, USE01a]. bot [An08b].

Botschaften [Sch09]. bottleneck [WL02].

bottlenecks [HT07]. Bound [CY08,
DGN03, KMT01, HLL03, y08, GW00].

Boundaries [PCT07]. Bounded
[Che04b, DFS08, DIS02, Din01, Din05,
Lu02, MPS05, MTS04, Vag03, DFS05].

Bounded-Quantum-Storage [DFS08].

Bounding [DM07b]. Bounds [BDF01b,
BP03b, DRR05, Di01, GGTK05, RW03a,
SNWX01, SM00b, Shp03, Wal01, WW05,
GT00, GGT03, JZ09, KS05b, PS02a, Shp99].

Bouwmeester [Dwu03]. Box
[An01i, BR02, CF02, CNS05, DI05,
DRR05, DS08, FM02b, KY01d, Kil01b,
SMTM01, JmBDX01]. Boxes
[Bi00, BCDM00, ZC00]. BP
[Wei00, Wei05]. Braid
[AAFG01, CJ03a, GM02a, Hug02, KLC+00].
LLH01, LP03, MSU05, Cho08b, Hen06a.
Braille [Pau02b]. Branch [AKS06].
Branches [Fel06]. Break [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breakers [CD00b]. Breaking [BKN04, DKFX05, GO03, GK02, Kov01,
KR03, Küh08, Sal00a, Wri05, Fie09, Gar01, SE01, Smi01b, SL07, Swe08]. breaks [OS05].
Breakthrough [Coc02a, LR01, Pau02a].
Brief [Bon07, Cos03, Kir01a, Boo05, Gra01].
Briefs [MP00, PM00, Pau02a, Pau02b,
Pau03, Pau09]. Bright [Ano01i, LNP02].
Bristol [DFCW00]. British [ACM08, Fie09, Fra01, Syv02, Bud00b].
Broadband [MP00, SHL07, MJF+08].
Broadcast [AFI06, BGW05, CKPS01,
CNV06, DS03, FWW04, GSW00, GKK07,
GRW06, HS02a, HLL05, LNP02, SNW01,
Woo00, ASW00, KSW06, Kre05, Mar05b,
NLD08, RG09, WDLN09, LN04].
broadcasting [TJ01b, WH02b].
Broke [Urb01, KS04]. Broken [Ahn08]. Brooks [Bar00b].
BRSIM [BPS08]. BRSIM/UC [BPS08].
BRSIM/UC-soundness [BPS08].
Bruce [Hei03, Sty04, See04]. Bruges [Pre00].
Brunley [ASK05]. Brute [Cur05, SGA07]. Brutus [CJM00]. BSD [Lin02, ASW03+01, Lin02].
BSDCon [USE02a]. Bubble [Ber03]. Buchmann [Lee03a].
Buffer [FOBH05, Fry00, Ino05].
Bug [BCS08, Bor00]. bugs [GJL06].
Building [Jou02, Kin07, Mar02a, And08,
Bra01a, FB01, LS05b, McG06, MPH06,
PQ06, DB04]. buitenlands [dL00].
Bulletin [Cer04b]. Bulletproof [Cha05b].
bundles [GT02]. Burrows [ABM08].
Burying [Arn01]. Bush [Ris06]. business [HHSS01, Pohl01]. Buy [PLW07]. Buyer [MM01a].
buys [Zaf00]. Buzzes [Coc02b].
Bytecode [Coo02, Ler02]. Byzantine [CNV06, HGR07, LLR02, LLR06, Pl06].
Byzantine-Resistant [CNV06].

C [Ter08, Zol01, III00, Oiw09, RMPJ08,
Sea05, Sea09, VM03, WK01, Wel05]. C# [MJ03]. C-testable [RMPJ08]. C2C [HTJ08].
CA [ACM03b, Joy03b, KKP02, Men05, Men07, Nac01, Oka04, Poi06, Pre02c,
USE02a, USE02b]. CAA [MGC02]. Cache [BTTF02, Kie07, OST05, OST06, TSS+03,
Ino05, WL07a]. cache-based [WL07a].
Caches [GSVC02, LLK05]. Caernarvon [TKP+08]. Caesar [Cha02, You06].
CAIDA [Pri00]. Cairo [EBC+00]. CaLC [Sil01]. calculus [MRST06].
Calcutta [Roy00a]. Calibrating [SDM06]. Calif [ACM03c]. California [ACM03a, ACM07,
Bel00, Bon03, Fra04, IEE00a, Kii01a, Sch01c,
Sch04a, Sch05a, Sho05a, USE00b, USE02c,
Wii09, Yum02a, IEE06]. Call [Ano04a, Ano07b, Ano07a, MD04].
Calls [WG05, Ano08c, WCJ05]. Cambridge [ACM10, Chr00, Chr01, CCMR02, CCMR05,
IEE03, JQ04, Kat05b, Kii05, Nao04, Pag03,
Puc03, Rot07]. Camellia [AIK+01, HQ01,
KMO2, LHL+02, SM03b, SK101, XH05].
Camera [CGK+02]. Camera-Based [CGK+02]. Can [BB02, CZB+01, Dav01c, Lai08, Ros07,
Ver06b, CNP03, CG05, SBB05, Zir07].
Canada [ACM02, ACM08, AMW07, HH04,
HH05, HA00, IEE02, MS05a, MZ04, NH03,
PT06, YTO1d, YVO1]. Candidate [HI00, EYCP00, NIS00, SKW+00, SL00].
Candidates [AL00b, DPR01, Dra00, GC01a, SB00,
SGB01, WW00, GC00a, WB00]. Cannes [AJ01a, AJ01b]. cannot [Gav08]. canonical
to [TP07]. CANS [DWML05]. Canterbury [CZ05].
Cantor [WPP05]. Capabilities [BDTW01, AL04, AB01].
Capability [MH05]. capable [ETMP05]. Capacity [ChY09, Sug01, M08a, Wan05].
Cape [EE05b]. capture [AMB06]. Card [BCST00, CMG+01, CL07, CJT02, DF01,
DFPS06, RE03, RS01, SR01, Ano00k,
Ano00l, Ano05b, AJ01b, Bor00, BGL+03,
Bur00, Cal00c, Car01, CCCY01, Cha05a,
Cla00b, Con00, CH00, DFCW00, GMG00, HM01a, Has02, Hen01, Hus01, Jac00, LSA+07, LC05a, Lu07, QSO0, RE00, SP02, Smii00, VK08, Zaf00, Che00, FGL02, Pau02b, SKKS00, TV03, card-based [LSA+07], CARDIS [DFPS06]. CARDIS'98 [QS00].

Card-based [LSA+07]. CARDIS [DFPS06]. CARDIS'98 [QS00].

Cards [And04, AJ01b, Bel01, CK06, DJLT01, HbdJL01, JSJK01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NQF03, QS01, Sak01, Sha01c, TBLD01, VPG01, YKMY01, Ano04b, Ano04c, AJ01a, BPR01, BCI05, Bur00, DFIH01, DFPS07, FCC05, Fin03, GUQ01, HSDS01, HSU05b, Jua04, KLY03, LKY05a, Ler02, LCS09, MY01, Pha06, Poh01, PB01, PRE07, SVDF07, SLH03, TIS07, WO04b, YW04b, YWWD08, Ano03a, BjvdB02, CL04d, CCK04b, Che00, Gro03, HLO5b, Ku04, KCO5, LHY02, SCF01, YW04a].

CardS4 [GN01]. Care [Mad00, RC06, Ano03a].

carefully [Cla00b].

Carlo [BI09, Sug03]. carrying [Art04]. cars [LPW06].

Cartilage [MYC01]. Cartography [SGM09, SWR05].

Cascade [DGH+04]. Cascaded [Jou04]. Case [ABK00, ANI05a, BBGM08, BU02, BCP01, CNS02, GS07a, Nie02b, OST05, Vau01, BKN04, BF06a, BK05, CSK+08, HRS08, KWD06, Mic02a, Mic02b, OST06, Pe09, STY07, SW+07, SPH06, ZWLO1].

case/average [Mic02b]. cases [ABHS09].

Cash [PS01b]. Cathedral [USE02a]. Cats [Pem01b].

Caught [Wei00]. cause [SBB05].

Causes [Mur01]. Cautionary [GMP01a].

Cayley [Lam91].

Cayman [SY02].

CBC [BBKN01, BPR05, BR00b, DGH+04, Fer06, JM02, KI03, Vau01, Vau02]. CBIDs [MC04].

CCA [KOMM01, Mi01b].

CCA2 [BTS02, Lin03, RGO9]. CCA2-Secure [Lin03].

CCGrid [TL06].

CCM [Dwo03].

CCS [Mar02b, MS05b].

CDH [CM05a].

CDH-Based [CM05a]. Cell [Fox00, MYC01, SHL07]. Cell-phone-free [Fox00].

Cellular [La00, LZ04, MG02, PZ09, SBZ04, BAO0, ETMP05, KK03, SHH07, WAN04a, dRMS05, Wue09, SS+08].

Center [AU01, CH01a, CYH04, LPM05].

Centered [BKM07, CMB+05].

Cert [CH02]. Centralized [Wac05]. Centre [PPV96].

Certification [Ano01k, CHM+02, RSA00b, BGB09, BD04b, KB09]. Certified [ANR01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LMK05a, NSA05, Sha04b, Sha05b, TLM05, Tsa05, TJC03, WH03].

Cerven [Sal03b].

CFS [ITA01]. ChaCha [Ber08].

Chain [YT09, YZ00, Wue09]. Chained [BCC01, BC05b].

Chaining [KBR00, CBB05, PCC03].

challenge [LM08, LW05a, PRS04].

challenge/response [LW05a].

Challenges [Cla00a, GV09, Nao03, STA03, SVEG09].

Chang [CWJ01, ZC05]. change [CYH05].

Changes [Mur01]. Changing [BST03].

Channel [BU02, CHV03, Law09a, LKM03, MÖL02, NMO05, OT03a, OT03b, Sch06a, SYL05, ARR03, BPO03, BOG07b, Buh06, CNPQ03, KSW00, LCZ05b, MS09c, PS09, WO07a, YTW05].

Channels [AIP01, CK02b, NAM02, Vau05b, LH04].

Chaos [JK01b, SK01b, WZ005, JK01a, LMC+03, MC03, PEF+09].

Chaos-Based [WZ005, SK01b, JK01a, PEF+09]. Chaotic [LLL+01, SXY01, URR02, Vau03, AMR00, ĜHG00, GB09, HYW07, HLW09, JK01b, LMC+03, YLGL07, MA02, PBMB01, PS01a, PZO09, PG02, SL09, UHA+09, VKS09, WW08, kWP08, WO07a, WZ005].

Chapman [Kat05b, WO18a]. chapters
[MAaT05, Tat05]. Characteristic [Gau02, GPS06, KT00, Ver02, GPS05]. characteristics [RFR07a, RFR07b, RFR07c]. Characterization [AJO08, Nam02, XH03, BGM04, KY00, QPV05, XLM06]. Characterizations [Pas05]. Characterizing [BTW05, BTW08]. Charging [BACS02, RH02]. Chatter [Kee05]. Chaum [BNPS02, KLN+06, WHH05]. Chaumian [Möl03a]. Cheating [CCL09, OKS06, PZ01, PZ02b, PZ02a, ZP01]. check [Kir01b]. Checkable [BPST02]. Checking [BL02, JP07, KLN+06, YJ00, GGH+08, RG05]. checklists [Sha01a]. Checks [FM02a]. Checksums [Sto01, SGPH98]. Cheju [Kim01]. Chemical [EIG01]. Chen [LW05c]. Chennai [CV04, RD01, Roy05]. CHES [JQ04, KKP02, KP01, KN01, RS05, WK03]. CHESS [LKHL09]. CHESS-64 [LKHL09]. Chicago [ACM04b, Top02, Con00]. Chien [YRY05b]. Children [Pau02a, Sye00]. China [B+02, DWML05, FLY06, JYZ04, LLT+04, Li05, LST+05, ZJ04, ZYH03, Ano00c, TTZ01]. Chinese [LLT+04, Li05, Sch01b, CAC06, YKL03]. Chip [BNPW03, DV08, MM01b, MM01c, MP00, Fo00, ITE08, Ano04b]. Chip-Secured [BNPW03]. Chipkarten [Ano04b]. Chips [Ano06a, Pau02b]. Choice [Jam00]. Chosen [BCHK07, CK03, CHJ+01a, CHJ+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JKS02, JKS00b, KS00a, KY01a, KCJ+01, KMZ03, KM01c, KI01a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH+09, KG09, ZCW04]. Chosen-Ciphertext [BCHK07, CK03, CHJ+01a, CHJ+01b, Des00b, DK05, FP01, JKS02, JJS00b, KCJ+01, KMZ03, Nov01, PV06b, Poi00, CHH+09, KG09]. Chosen-Plaintext [DN02a, KM01c, KI01a]. CHW [CHC04]. CIA [Mah04, Ris06]. Cincinnati [BD08]. Cinematic [CAC03]. Cipher [AIK+01, BKR00, BS00b, BR02, Cer04b, CLLL00, Cro01, CL02c, DR00a, DG00, DPs05, DF07, Dwo03, EYCP00, FF01a, Fl02a, GG05a, GBS02, HCJ02, HQ01, KYHC01, KHD01, LKHL09, MS07, NV01, OMSK01, Pat01, PS06, Sal00a, SM01, SM02, SY+02, SXY01, SBEW01, SK01, WB02, Wu02, XH03, ZCC01, BPG09, BD00a, BP04, GP08, HA04, Hey03, KH08, Kid00, LKH+08, Mac00, MSP+08, RBB03, Sal00b, SHH07, WW08, Win05b, WF02, XH05]. Ciphers [AAG+00, BBKN01, BS00b, BR01, BK07, CVTM01, Can01b, CN06b, CJS01, Chu02, CHJ02, CP02, CM03, Cou03, DPV01, Eag05, Fil00, FF01a, Fil02, G001d, G001e, HR00, HR04a, HSH+01, Jam00, Jam06, Kan01, KCP01, KRG03, L020, MV00, On01, P06a, Pl01, RMS05, Sar02, SM03b, SKU+00, Wal00, Wri05, ??02, YG01b, ZC00, Bai08, Bar06a, Bel07a, Ber07, Bod99, DLP+09, DY01, DS09, Dun06, DK08, Egh00, GPG06, HW03a, HWR09, Hey03, JK01b, Jun05, Kat05a, KSWH00, Kin01, LMS07, LD06, Lun09, Max06, M09, MMW01, Pin06, SH09, SK03, Sm01b, SL07, SB05, TT00, Wag03, Y006, You06, Kat05b]. Ciphertext [BB03a, BCHK07, CK03, CF01b, CS07c, CHJ+01a, CHJ+01b, CS02, CS03b, Des00b, DK05, FP01, JKS02, JJS00b, KS00a, KY01a, KCJ+01, KMZ03, KI01a, Man01, Nov01, PV06b, Poi00, Sho00b, BMW05, CHH+09, IM06, KG09, Poi00]. Ciphertext-Only [BB03a]. Ciphertexts [AF06, BGW05, BGN04b, J00a]. Circuit [EHK+03, GS08, HR05, MG08, KS05b]. Circuits [BI05a, FM+03, Go03, ISW03, MD05, PBTW07, You01, GL+04]. Circumvention [Kha05]. Cirencester [Hon01, Pat03b, Sma05]. CIRM [PP96]. CISC [FLY06]. citizens [Ano03a]. claims
Combinatorial
[GMW05, SLTB+06, Hen06a].
Combinatorics [Lee03b]. Combined [LLS05a]. Combiner [Sar02, LL06].
Combiners [AK03]. Combining [Abe04]. Comes [Mar08b, An03e]. Coming [Dan01]. Commemoration [BZ02]. Comment [SCS05b, WY05, WLW04]. Comments [AS01c, CGH+00b, JW01, MNFG02, SKW+04, CJT04]. Commerce [CLK01b, GS02a, Kir01a, Sta00, Uni01, ZYM05, BM03a, FB01, Gra01, MY01, SN07, TMM01, YC09a].
commercial [LCC05, YLR05]. Commitment [DN02b, DMS00, FF00, CAC06, HR07, KKL09]. Commitments [BN00b, CF01a, DFS04, FM02a, Gen04a, HNO+09]. Committee [Uni00a, Uni00b]. communicating [Hut01]. Communication [AK02a, ANRS01, BYJK08, BBK03a, BIW08, Big08, Col03, Fis05, GKK+09, LLS+09, Mar07, NA07, PL01, Sch06b, SKR02, Wri05, vDW04, BYJK04, BC05c, CC05c, CGP03, EY09, GKK+07, GG05b, GC05, HYS03, JZ09, JRS09, KPS02, LPM05, Lin02, MP08, PBMB01, Par04, RH03, SN01, UP05, WVA01]. Communication-Efficient [Fis05, LLS+09]. Communications [BCC02, GN06, HJ07, Igl02, Kra01, Lan00a, Lan04b, LCK01, LL02, LL01, MS05b, Sal01b, Vau05b, VM02, BP03a, KPM04, HW02, LC04a, Sal05c, Ser06, SL05a, Wii99, WGL00, YTW05, DKO05]. Community [SK06]. commutativity [HRS08]. commuting [CKR08]. Compact [CG03, JT01b, SMTM01, YT09, ZLK02, JAW+00, Mic02a]. companies [Ste00]. Company [ASCW+01, Zaf00]. Comparative [DPR01, GLG+02, Kat05b, LFHT07, LOP04]. Comparing [HU05, KLN+06]. Comparison [GC00a, GC01a, Gau02, JRB+06, MS02e, SW00a, WW00, FGM03, JL03, Sma01, WB00]. Compendium [Lut02]. Compensated [AAK09]. competition [Cla00b]. compiler [DFG00, Oiw09]. Compilers [Lut02]. complement [YCO9c]. Complementary [AS01c]. Complete [Bar00a, Bee05, Bud00a, FGM001, GCKL08, HSM04, KY00, MS09d, Sal07, TWM+09, Bud02]. Completeness [HG03, MW04, ABHS09, PT08]. Complex [JKK+01, LKL05]. Complexity [BYJK08, BLM01, BDK+09, CR01, CB01, DN00a, FBW01, GKK007, GKK+09, HR04a, Lut02, Niz02b, RMH03b, Ros00, Rot05, Shp03, BYJK04, CDD00, GKK+07, GI001, Gor05, JZ09, Mic02a, MP08, RMH03a, Rot02b, Rot03, Shp99, SPHH06, TW06a, SV08a, Fal07, Rot07]. Complexity-Theoretic [CB01]. compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BSL02, Hei01]. TEM+01. composability [PS04c]. Composable [AF04b, BOHL+05, BLDT09, CF01a, CK02b, DN02b, DN03, NMO05, RK05, Can01a, CLOS02]. Composite [CQ501, GMP01a, RDI+01, Zhe01]. Composition [BJP02, BN00a, CR03, CV02, Pie05, Sho00a, Can06a, LLR02, LLR06, Puc06]. compositional [GM04]. Compostela [BS03]. Compound [SB05]. comprehensive [dLB07]. Compress [Gen04b]. Compressed [ISSZ08, SB04]. Compressed-Domain [ISSZ08]. Compressibility [HN06]. Compression [ABM08, BD03, CC06, HS001, Ke02, LHS05, RS08, Sal07, SDF00, WTW+02, WC03a, FS08, Gar04, Lai00, L050a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TTZ01, Zir07]. Compression-Encryption-Hiding [BD03]. Compromise [Ahm08, Lai08].
Compromised [ZYNO8]. Comput [McK04]. computability [Pet08].

Computable [Vad03]. Computation
[ACS02, Baj01b, BCL+05b, BI05a, BIM00, BJLS02, CC00, CDMO00, CDN01, CDG+05, CDI05, DN03, DI05, DM00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, Je08, KO04, KCLL05, KRZ02, Lin01c, PS05, WW05, Ano02g, AB09, BEZ00, BEZ01, CLOS02, CLCO08, CDD00, DwWmW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WLH05, WY05, SM07b, Duw03].

computational-efficient [CLC08].

Computational [CCL09, DLP+09, GH02, HG03, KLR09, KK06, Rup09, SM07b, WvD02, AUW01, IEO08, Lam01, Lau08a, Nie02a, Sh005b, SHJR04].

Computationally [MPSW05].

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

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

Computer
[BS03, Bis03b, Bro05a, BCDH09, BC01, CSW+08, CZK05, CGK+02, Coc02a, Coc03, HY05b, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, frr00, JBR05, KM07, Leh06, Lu02, MYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Tyn05, Cas02, DFH04, Fan09, FOP06, GKS05, Lov01, Mal06, PRS04, PHS03, Sal05c, Sal05d, Sh006, SL06, SE01, dCdVSG05, GKS05, dCdVSG05].

Computer-Science [Coc03].

computerized [LMC+03, Pau02b].

Computers [Coc03, Ett02, TSS+03, Cop05, Cop06, RH00]. Computing
[AC00, AC01a, AC01b, AC02, AC03b, AC04b, AC05a, AC05c, AC06, AC07, AC08, ACM09, ACM10, ASW+01, BBDK00, CGH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09, Lu03, May04, PHM03, Sch06b, SKG09, SCF01, Sim02, SEF+06, Sta03, TL06, VH09, Ver02, WC01a, Wi00, Yan00, YKM08, Cha07, Che05b, CHT02, DHL06, HV09, HKP05, LMC+03, MI09, PP03, PP07, Raj06, RP00, Sei05, WLH06, Wnl99, YLR05, Lut03], Compupware [Ano02d].

conceal [BB79]. Concealing [DMS00].

Concealment [DA03]. Concept [ARC+01].

concepts [AB09, Krr07, SWR05, MO04].

concerning [HW03b]. Concerns [MP00].

concrete [KNS05]. Concurrency [JL00].

Concurrent [BP02, DPHV04, Gen04a, KKG03, Ros00, Ros06a, Dam00].

Conditional [LM05, WN02]. Conditions
[IK05]. Conference
[AC03a, ACM04a, Ano06b, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bli03, Bla03, Bon03, Boy01, Buc00a, CCO04a, CV04, CGP03, CGH+06b, Cra05a, DKU05, DFCW00, DFPS06, EBC+00, ELvS01, FLY06, Fra01, FMA02, Fra04, FLA+03, HR06, HY05b, IEE09a, IY05, JYZ04, JM03, Joy03b, Jue04, KJR05, Ki01a, Kim02, KN03, Knu02, Lai03, LL03, Lee04b, LLT+04, LL04c, MMV06, MS05b, MS02c, Men05, Men07, NIS00, Nac01, Nan04, Oka00, Oka04, Pat03b, Pem01b, Pfm01, Poi06, Pre00, Pre02c, RD01, Roy00a, Roy05, Sh05a, Sil01, SM07b, Sma05, Syv02, USE00c, USE00a, USE01b, USE01a, USE02c, Wi99, Won01, Wri03, Yun02a, YDKM06, ZJ04, Zhe02b, ZHY03, AUW01, BC05c, DV05, DWML05, DRS05, Hon01, Ki05, Li05, PC05a, PY05, PPV96, Q500, Son00, WK06].

Confidences [Gan01a]. Confidentiality
[Dwo03, Pem01a, YC08]. configurable
[MBS04]. Configuration [Sha02, Mos06].

Confirmation [SK00]. Confirmer
[CM00, GM03]. Confiscation [Sha02].

Conformance [LB00, RSA00c].

confounded [Bel07a]. confusion [She01].

congestion [SB05]. Congress
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].

congruences [Ste08]. Congrualent
[CS05b, LS05a, SB05].

conic
[LWL09, LCC05, LCZ05a]. Conjecture [CU01]. Conjugacy [CJ03a]. Conjugate [Igl02]. Connected [BJLS02, Höf01].
Connection [HR00, Jam00, Goo00, Mic02b]. Connection-Polynomials [Jam00].
Connections [WRW02]. Conquer [SKQ01].
conscious [DMSW09]. Consensus [CNV06]. Considerations [DBS06, Hei07, Rub01, Sch07, SVEG09].
Considering [WA07]. Consistency [ABC05, JEZ04].
constant [App07, BI05a, CS07c, CD01a, DPV04, DN02b, Di05, Lin01c, Sm00a, IK08].
Constant-Depth [BI05a].
Constant-Round [DPV04, Di05, Lin01c]. Constrained [BCH00, DBS06, HS01b, MRL02, Zhe02a, Has00, RAL07].
constraints [CC05d, LPM05, SN04]. Construct [CDMP05, Gol01d].
constructed [Tsa05]. Constructible [NNT05].
Constructing [Des06b, Fis01b, Vad03, Wen03, JZCW05, NS01a, ZL05].
Construction [BBK01, BB00b, Car02, CMKT00, Lin03, Nie02e, Sm00a, TNM00, YWD08, DW05, SC02c].
Constructions [BS00a, BR00b, BRS02, GMW05, GGKT05, GM02c, Jou04, PR08, PZ02b, SNWX01, Sm00b, GT00, GPV08, IK03, IK06, NR04, PR05, Reg03, Reg04, vDKST06].
constructive [GGH08]. consumption [Mis08]. Contact [YKMY01, Car00]. Contact-Less [YKMY01]. Contactless [And04, KS02, Cha00b, Fin03].
Contemporary [Ahm07, Opp05, SVEG09]. Content [AAK09, CGJ02, HHJS04, MA00a, MA00b, RE02, XMST07, YKW01, ATS04, DY09a, GSK09, SG07].
Content-adaptive [XMST07].
Content-Based [RE02, YKW01, SG07]. Content-triggered [HHJS04]. Contest [Bar00b]. Context [DJLT01, FPS01, SN04].
continue [Lov01]. continued [Dan02].
Contra [Mah04]. contract [WK05].

Contrast [BDDS03, HKS00, HT06, KS03, CDFM05].
Contrast-optimal [HKS00].
Contrast-Sensitive [HT06]. Control [ABEL05, ANRS01, BW07, CGMB02, HC08, LY05, Sma03a, ZGLX05, BNP08, DFM04, DPT02, HW03c, JW06, KNS05, LKZ04, MD04, MSP08, PS04b, ST07, WC01b].
Control-flow [ABEL05]. Controlled [GVC08, IMM01, AW05, AW08, LAPS08].
Controlling [HY03, MS03b, MS02d, WL05].
Controls [Har01a, Har01b]. convenience [WDCJ09].
conventional [CJ04, YW05, YRY05b]. Converging [Pot07]. Conversation [GK04]. conversations [AVY09]. Conversion [CD05, Ket06]. Conversions [Kl01b]. Convertible [Chi08e, LH04, LHT09, WH02a, CL04b, LW05a, ZW05b].
Convolution [PG05]. cookbook [VM03]. cookies [Cha05a]. Cool [An00d].
Coordinate [OS01]. COPACOBANA [GKN08]. Copenhagen [TBJ02]. Copley [USE01b, USE01a].
coprocessing [ML05].
Coprocessor [Gut00, Ito00, LS01b, OTIT01, AV04].
Coprocessors [Sm02]. Copy [LTM00].
copying [SV08a]. Copyright [Kha05, LLL02, PBB02, XFZ01, ZTP05, Gil07, HLC07, KA09, Kwo03a].
CORBA [TEM01]. Core [BF00a, Dim07, DV08, HMS04, TPS01].
Corfu [SM07b]. Corner [Mar08a, TR09a, TR09b]. corners [Blu09].
Corporate [HW01, KH03]. Correcting [MIZ02, NN06, YY00, ZYR01].
Correction [BQR01, CTBA01, Dim05, LN08, LW05b, MP05, SKQ01, TEM01, Gar04].
Correctness [PBD05, Bel07b, HSD05, DH08].
Correlated [FWW04].
Correlation [BSC01b, CS01, Go01c, JI00d, LV04, LM05, MH04, Ny01, SY01a, WRW02].
Cryptanalysis [YKL03, Kat05b]. Cryptanalyst [Wil06]. Cryptanalytic [BS00b, KFSS00, Occ03, QSR02, Yan07, Wil01a]. Cryptic [Wri05]. CryptIM [Ust01b]. CRYPTO [Fra04, Men07, Sh005a, Ahm08, Ano01j, Ano03c, Bau01a, Bau01b, Bur01, CCM01, CNB02, Lev01, Lev02, Mar08a, Mar02b, MC04, Pem01b, SYLC05, TR09a, TR09b, Yun02b, Bec02, BK05, HGNS03, Web02, Bel00, Bon03, Kil01a, Yun02a, Sei00a]. Crypto-algorithms [Ano01j, CCM01]. Crypto-based [MC04]. Crypto-CCS [Mar02b]. Crypto-integrity [Yun02b]. Crypto-systems [An001j, CCM01]. Cryptoanalysis [HSIR02, LD01]. CryptoAPI [Bon00]. Cryptoclub [BP06]. Cryptocomplexity [Rot05, Fal07]. Cryptocryptographer [Joy03b, Nac01, Oka04, Poi06, Pre02c, Men05]. Cryptographers [Coc03, KLN06, Tsa07, Bel07a, Haut03]. Cryptologic [AC02, AADK05, AL00a, Ano09b, ADH07, Ase02, BLST01, BDF01a, Bar00a, BGK03, Bib03, Bla01a, Bor01, BDP02, Bra01b, BM01c, BL08, Bur06, CCO04a, Can01b, Car02, CCD01, CL02, CK07, CB01, Cra05a, CS09, CO09b, D002, DHMR07, DF04, DS00, DNV01, DHR00, DV08, DFG01, FIP01b, FS00, Fis01a, FGM00a, Fr01, GMP01a, Gar05, GSS08, GGKT05, Gol01d, GKO2, GTH02, Gor02a, GL00, GUQ01, Gut00, Gut02b, Gut04a, HT02, HN06, Har06, Has01a, HL05a, HCO8, Igl02, IY00, Ito01, IMM01, J05, KMO01, KY01b, KY02b, Ki010, KS00a, KS00b, Knu02, Kus02, Law09a, LN08, LS05a, LKJL01, MS02a, MOP06, Mea01, MNP01, MRL02, MHH02, Mor03, MK05b, MS05, NIS01a, NIS01b, Nao03, Nd05, Ngu05, Nie04, OTT01, OP01a, PKBD01, PR08, PZH09, Pem01b, Pfi01]. Cryptographic [Pin02, Pin03, PS02b, Pot06, Pre00, Pre02a, Pre02b, RSA00d, RSA01, RR00, RRS06, Rot01, RSN01, SM00a, SS01a, SGM09, Sha02, Sh02, Shy02, SD0F06, SV00, SR06, SL09, TLY04, TWNA08, TDBL01, Uzu04, WK03, WN02, WBL01, WCO10, You01, Zha08, AMR04, ACT05, ALV02, AV04, BGB09, BDSV08, Bla01b, BP05, BG08, BG09, BDN02, BD04a, BGL03, BM06, BR05, Can01a, Can06a, CH040, Coh03, CC05d, CDL06, DP04, Dug04, DFG00, FS03a, FGV01, GT00, GP08, GJ04, GM04, GB09, HU03c, HY03, IK03, IK06, IY02, IYK03, JW01, KAM08, KS00, KS05b, KP03, LMT05, Lau05, LL05, LL09, ML05, Mea04, MT07, Mic02b, MRST06, Mon03, NN03, N040, ND06, PS04a, PSG09, PR05, Pre07, Pri00, Puc06, PV05, Reg03, Reg04, Ren09, RM04]. Cryptographic [R08, RAL07, RS04, ST03a, SV08a, S070, SW00b, TNG04, kWpLw01, WL04, XLM06, YTL06, ZL09, ZW0L01, ZL04b, dHO8, B0W02, J004, KK02, KP01, KN01, RS05]. Cryptographically [ADD09, AHS08, BJ02, BFC08, BB00b, FR08, MS02b, RGX06, A030, AW05, AW08, Lau08a, SM03a]. Cryptographically-masked [AHS08]. CryptoGraphics [CK06]. cryptographie [RSA09a]. Cryptography [ANS05, AF04b, AD09, AA04b, An000c, An01i, An02b, An02f, An002b, An04a, An05a, An07b, An07a, AAFG01, AIK04, AIK06, App07, EA0Q05, ABM00, Bai01a, Bai01b, BNP03, BD04, BOV03, BOV07, BGM08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BW02, Bla02b, BDDS03, Bon00, Bon07, BPR01, Boy03, BLS00, BK06b, BKM07, B0C08b, BD08, BP01b, BRTM09, CPS07, Cer04b, CCL09, CS0W08, CSV01, CPD06, CO040, CFA06, Cop00, Cor06, Dr00c, Dam07, DFS08, DFS05, DD00, DFG04, DK02, DK07, Des02, DT03,
DY09b, DSS01, DDN00, DDN03, Dre00, DP08, EPP+07, EP05, Elb09, Eli04, ECG+07, Ett02, FS03b, Gal01, Gal02, GHK+06, GKK+09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Grib01, Gro05, HR06, HH04, HHM01.

**Cryptography**

[HMV04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irw03, IKOS06, IKOS08, JYZ04, JL00, JT01b, JT01a, Jue04, Kak06, KLR09, KZ07, KGS07, Kat05b, KK06, KPMF02, KWDB06, KY01c, Kri01a, KMS02, KM05, KSZ02, KS03, KWP06, Lam01, LGS01, LSY01, Lee03b, LL+01, Lie05, LDM04, LW05b, LP02b, Lut03, Lys08, MNT+00, MP02, Mao01, Mao04, MZ04, Mao01a, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pel06, PM02, PBB02, Poi02, PT06, Puc03, RASA00a, RSA02, RSA03b, RS04, Rto07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SX01, Sma03a, Sta02a, SGK08, Sti95, Sti01, Sti02, Sti06c, SJ05, Syv02, TSO00, TW06a, TG04, TMM01, TW02, TW06b, Tro08, TR09a, TR09b, Uni01, USS02].

**Cryptography**

[VY01, VM02, WPS01, Wei04, WK01, Wei05, Wie00, WvD02, Wri00, YWC08, Yr06, YC01, YDK06, ZY03, vDW04, Imr03, AMW07, AN03, AUW01, An002a, An002g, ABD01, Ber09b, BBD09, Bis03a, BSS04, BSS05, Bla03, BDN00, BCD06, BEZ00, BE01, BM04, BEH+07, Buc00a, Buc01, Buc04, BLS09B, BMA00a, BMA00b, BMA00c, CCT08, CJ03c, CDF05, CCD07, Cos00, Cre00, DD04, Di01, DIM08, DwWmW05, DOPS04, DKL09, DW09, Duw03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK+07, Geb04, GRTZ02, Gol09, GG05b, GHP05, GPS05, GN05, HH05, HHL+00, He03, HKPR05, HA00, Hig08, HKS00, Hoo05, HG05b, HLwWZ09, IZ00, I006,JK01b, Jan08b, Joy00, KZ03, KL08, Kat01, Kii05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Lin01a, Lop06, Mau04, May01].

**Cryptography**

[McA08, MBS04, MM07a, Mol07, NP02a, Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00, Pin06, Pip03, Reg05, Reg09, Rot02b, Rot03, Roy00b, Rup09, ST07, SCH02, SCH04d, SBZ04, Ser06, SH05, Slp99, Si05, Sin99, Sin00, Sna04, ST01d, SK01b, TW05, UHA+09, Van03, Van05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wri03, YC09a, YC07, vT05, For04, HC02, Kat05b, Pat03b, Si01, Sma05, Bee05, Lee03a, Rec01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08].

**Cryptography-based**

[FXAM04].

**Cryptologic**

[BS00a].

**Cryptologic**

[Lew00].

**Cryptologic**

[dL00].

**Cryptologists**

[WD01b].

**Cryptography**

[Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Kn02, L03c, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka04, Poi06, Rot05, RS02, Sha03a, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bil03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kii01a, Kim02, Lam91, LL03, Lee04b, MS02c, Men05, Men07, Nao01, Oka00, PC05a, Pf01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sh05a, Son00, Won01, WK06, Yun02a, vT00, DWML05].

**CryptoManiac**

[WWA01].

**Cryptography**

[KK+02, MG01].

**Cryptography**

[BT02, FL06, GG01, GK05, GH01, Hug02, KM01a, KY02c, KLC+00, LHT09, dVP06, Luc02b, NSNK05, NBD01, Ove06, PHK+01, YG01a, YG01c, Zhe02a, Zhe06, Bao04, CL02b, CCH04, Che05a, Cho06, CFVZ06, CHH01, Dan02, DHL06, ERKMA01, GHdGSS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, LL04b, LL06, LKYL00, Loi00, LS01c, OP01b, Pae03, Poi00, SP02, SCS05a, SP79, SL05, Sun00b, Sun02, SZP02, T01b, T01a, VSO1, War00, YC09b, hY08].

**Cryp**
cryptovirology [YY04]. CRYPTREC [IY00]. CSCW [ZP05]. CSP [SBS09]. CT [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09]. CT-RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09]. CTO [Ano03e]. CTS [Con00]. Cuban [AJ08].

Cube [DS08, PDMS09]. Cube-Type [PDMS09]. culture [Gil07]. Cumulative [LG04, WP03]. cure [RD09]. cure-all [RD09]. Current [DFH01, PRS04, LPW06]. curriculum [FOP06]. Curve [ANS05, ADI09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BMM00, BWBL02, BS01d, BMN01, CQS01, CFA+06, GPP08, HYZ05a, HMM01, HMV04, HM02c, JTO1b, JTO1a, KBM09, KPMF02, KSS02, KWP06, LW02, MLO2, Kir03, OTP01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YBY01, ZLK02, BSS04, BSS05, BG04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHWH04, GBKP01, Has01b, Hsu05a, HLO5d, JWD01, LWL09, Mis06, OS01, ST03a, SSST06, SH05, Sma01, SCL05, SLC05, TCO5, Van03, Ver01, Wlo04, WPP05, YC09a, YC09b, ZSZ01, ZLK02, WL09, VTL01].

Cure-Based [KWP06, Pel06]. Curves [AHRH08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK+06, Kid02, PWGP03, Ver02, CMKT00, Hsu04, LWZ05, MP01b, MSV04, Sil05, Sim02, SC02b, Was08b, Wen03, Yas08]. customer [Lin01b]. CVS [DFG01]. Cyber [FNN05, WW04, Mao05]. Cyberinsurance [BP07]. Cybersecurity [PLW07]. cyberspace [Mit02]. cycles [ABH09, BPS08]. Cyclic [FG05, Mic02a]. Czech [MJ04].

D [Duw03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WW09, ZTP05]. D.R [Irw03]. daemons [Mos06]. Damgård [CDP05]. dark [Blu09]. darkening [CDD07]. DARPA [Coc01a]. Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BS00b, BNWP03, Bro05b, Che01a, CTL01, DBS01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTC03, HLL+02, Ken02a, Ken02b, Kus02, Lan00b, LLRW07, LP00, LHS05, LTO0, MND+04, MS03b, MFS+09, NM09, OSA0, Per05, RKZ02, RK06, Sal03a, Sal07, Sin01a, SK03, SMD06, TZZD05, TPN07, VDKP05, WS05, WW02, WN02, x01, vW01, AMB06, AG09, AK03b, AKS04, Ano02c, Arn01, Bla00, BNWP03, CCMM09, Cer04a, CO09a, CLR09, CPG+04, DZL01, DGM03, FS04, HLM02, LK05, MJ03, MA06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGPH08, SETB08, WMD08, YLC+09, YC08, ZS070, Zir07, Cur05, DK08, Lin02, Pap05]. Data-Hiding [VDP05]. data/image [Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, BI05a, BBP00, KS02, SVEG09, Gal02, HLM02, Mao04, PS08b, PBV01]. database-service-provider [HILM02]. Databases [AK02b, CDM+05, DN04, AHK03a, CDD+05, CKY07, GA03, MS09, MNT06, NS05b, ÚG08, YPPK09]. Datamining [DN04]. Datenvenschlüsselung [Lin02]. David [Gas01, Pap05, Bar05, Eag05]. Day
[SE01, CSW05, Win05c]. Days
[Adl03, Riv03, Smo04]. DC [USE01c]. DCT
[BSC01a, BSC01b, CH01b, KT00, LY07, LSC03]. DCT-Based [LY07, LSC03]. DDH
[Lys02]. DDO [LKH*08]. DDO-64 [LKH*08]. Dead [Gut02a]. deaf [Pau02b]. Dealer [DK01, Sun00a]. Dealing [BH00a, BC05b]. Debate [Jol01, Mad00]. Debian [YRS*09, Ahm08]. Deblur [VHP01]. Debugger [Ano02d]. Debugging [Ano02d]. Dec [IIE09a]. decades [Lov01]. decades-old [Lov01]. December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, Lai03, Lee04b, LYT*04, Li05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b]. Decentralized [CS07a, Mah04, MS02d]. Decidability [K¨us02]. Deciding [Bau05]. Decimal [BJvdB02]. Decimalisation [BZ03]. Decimation [Fil00]. decipherable [aSM01, Sav04]. Deciphering [Eri02, KB07, Ark05, Lov01, NS01a]. Decision [DJ06, GR04, KM04a]. Decisional [CU01]. Decisions [Coc02a, Sch07]. Decodable [Yek07]. Decoding [KY02b, LGZ01, LGZ02, Rai00, AGKS07, Bul09]. decomposing [FP09]. Decomposition [BR09, CL04c, SC02c]. decompositions [vDKST06]. Decorrelation [CLL00, Vau01]. decrypt [Bih02]. Decrypt [Bau00, Bau02a, Bau07, MB01]. Decryption [Bar00b, BST02, CS03a, CCD07, FPS01, HGNP*03, Int00, KCJ*01, Ano08a, DZL01, GH08, Mil03, OS07, Slop04b, SWH*09, Wh09]. Decryptor [TPS01, Zol01]. Decrypt [Coc02a]. Dedicated [ISO04]. Deep [CMS08]. Defeating [CSK*08]. Defensive [BTTF02, Dav01b, Dav01c, KLR09]. Defending [NRR00, Pro01]. Defense [GK02, HW01, Mir05, Wy05, Bol02]. defenses [SL06]. defined [Yas08]. Definition [YWD08, SNI00]. Definitions [Uni01, AH05]. Definitive [BS01a, BSB05, Gar03b]. defying [HRS08]. Degenerate [Ber09a]. Degradation [BSC01a]. Degree [CV02, QPV05]. Degrees [Sat06]. Déjà [DP00]. DeKaRT [Go03]. Dekker [Irw03]. Delacorte [Imr03]. Delay [WRW02, NS01a]. Delayed [JM07]. delegated [CL04c]. Delegation [WN02, ZP05, MW06]. Delhi [JM03, RM04]. Delivers [Ano02c]. Delivery [NZCG05, RCMG01, DY09a, NLS05]. Delphi [TEM*01, Hei01]. Demand [BD03, CMB*05, SEF*06]. Democracies [CZB*01]. Democracy [CTBA*01]. Demography [Coc03]. Demons [Mos06]. demonstrably [HL06]. demystifying [RR04]. Deniability [Pas03]. Deniable [Nao02, CCK04a, CSK*08, DG05, LC05b, YRY05c, Zha06]. Denial [Mal04, Nik02a, Nik02b, PKBD01, Ri02, Mir05]. Denial-of-Service [Nik02a, PKBD01]. Denmark [Cra05a, TB02]. Denver [ACM01b, Sch04b, USE00d]. Department [Bol02, Er01]. Dependent [NAG03, And08]. Dependent [Go03, WS05, BPS05, SK03]. deployed [BDET00]. Deploying [BH00b, GS*04]. Deployment [CL07, KDO01, Mur01, Sin01a, App05, JRR09]. Dept [Uni01]. Depth [BF05a]. Derandomization [BOV03, BOV07]. Derivation [DGH*04]. Deriving [BJP02, CSW05]. DES-encrypted [Bih02]. DES-like [Egh00, EBS01]. Desch [LBA00]. Describing [PS06]. Description [Lav06, MH05]. Descriptors [DNP07, SP04]. Design [Abd01, AADK05, Ano02e, ADD09, AIK*01, ARC*01, Bar00b, Can01b, CCD01, Cim02, CB01, CS03b, CMB*05, CLZ02, DR02a, DR02b, DS09, DF07, EHK*03, FF01a, FZ05, GSS08, Geb04, Gut02b, Gut04a, HRL09, Hro05].
Design/CPN [AADK05]. Designing [HBC+08, TCR03, C+02, CG05, Lan00c]. Designs [Bee05, CC02a, Bai08, Des00a, WL07a]. Desktop [Mun08, BDET00]. Desmedt [CHH+09]. Desynchronization [CDTT05]. Detached [Sha01c]. Detailed [Lut03]. Details [Scr01]. Detect [FOBH05]. Detecting [CMS09, FGD01, JQYY01, Har07a, LHL04a]. Detection [AS01b, AD07, BB00a, BKM07, CH01b, CZK05, JT05, KKG03, SKQ01, SY01a, SLT01, ST01c, TZZD05, TMM05, WGO5, YI01, Zau01, Bej06, BBK+03b, HLL+02, Men03, NN02, WMS08, YW06, ZGTG05]. Detection/Correction [SKQ01]. Detector [BSC01b, DNP07]. Determined [KKH03]. Determining [KS03, LQ08, OS07]. Deterministic [BK06a, Her06, KZ03, KZ07, May04, BK07].
developers [Ano06c, Dew08, MK05b, Nis03a]. Developing [MV03b, Cra05b, Gal02, HL06]. Development [Ano02e, CNB+02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a]. developments [Ano03c, Pre07, Sha04a]. develops [Pan02b]. Deviates [Ran55, 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 [Bha01c]. DFT [Che08a]. DH [Lys02]. DHIES [ABR01]. DHP [MSV04]. Diablerets [Vau05a]. Diagnosis [Ano04a, BK06b, XNK+05]. Diagnostics [NM09]. Diagonal [PHJ01, 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]. difference [PBMB01, dW02]. Differenting [LS08, WWTH08]. Different [CGMM02, Sna01]. Differential [Ava03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eko09, Fur02a, Gra02a, HLL+01, HMK+02, HMK+04, HY01, JT01a, Kan01, KM02, KCP01, LHL+02, MP06, MM09, MHL+02, MG08, PSC+02, PQ03b, SK01a, SK+00, SKI01, YSD02, vW01, BF01a, CUS08, Che08a, DL+09, Egh00, EBS01, Pha04, SLL+00, TM01]. Differential-Linear [BDK02a]. Differentials [BF00b]. Difficult [Bud00b, MT02]. Difficult-to-pass [MT02]. Diffie [Jan08a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, C01, C03a, CKRT08, FSO1b, GR04, Ki01b, KK02, KM04a, Kra03, Kra05, Mi08, Tsa06, RY05c]. diffuser [Fe06]. diffusing [She01]. digest [MS09]. Digit [KWP06, Tan07a, BGO9, HKPR05, Kir01b]. Digital [ANS05, AvdH00, AR00, AS08, Ano01f, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDO9b, Cal00b, CCH05, CC09, Che01b, CFS01, CMB02, CMB+08, CZB+01, CGJ+02, DSP01, EIG01, Eng00, EME03, HSI00, HIS01, Han00, HSO1b, HSGP+03, HW01, HLT01, JBR05, KZ01, Kal01, KC02, Kuh00, Kwo02, Kwo03b, LZL+01, PLL+01, Lin01b, LW09, LL01, Lut03, Mad00, MM01a, MM02, Mhe01, PL01, PHJ01, PCG01, PZL09, PBM+07, Ram01, Rs01, RSO1, Sam09, Sch00d, Sch06b, Scr01, Sha01e, SC02a, Sh08, SLT01, Sug01, TM01, TJ03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03a,
WC04, Wya02, XZF01, XYL09, YWWS09, YYDO01, YYZ01, ZWC02, Zho02, ZCW04, AAP07, AA08, Ano00i, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CJ05, Che07, Die90, FB01, GGK03, Gii07, HRL09.

digital [HLC07, HLH00, HHC05, KP03b, LG04, LG09, Lev01, LLC06b, MKY08, NRR00, PC05b, PLJ05a, PBV08, QCB05b, Sha01d, Sha04b, Sha05d, SCL05, TCC02, TND+09, UP05, WNQ08, WHLH03, WC05, X05, XMST07, Ano09a, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].

digital-Audio [WNY09].
digital-Signature [Eng00].
Digits [Che04b, Ran55, Ran01].
Dimension [DDG+06, TZT09a, TZT09b].
Dimensionality [SBG02].
dimensions [CLR09].
Dining [KLN+06].
diplomacy [Alv00].
Direct [BMW05, KG09].
directional [PJK01].
directions [Sha01b, DFH01].
directly [JZCW05].
Director [Mad04].
directories [C+02, Pet03].
directory [C+02].
disabled [Pau20a].
Disappear [Per05].
Disappearing [Way02b, Way09].
disappointed [Ste00].
Disaster [WCZ05].
disciplinary [SM08].
disclosure [JM07, Swi05].
Discovery [Bi09, HLL+02, SBG07, SGA07].
Discrete [CS03a, CNS02, Che04b, CCW02, Gen00b, GV05, GPP08, KC09b, LW02, LJL05, VK07, HN04, HW03a, HW09, Hsu05a, HL05d, JL03, JLL01, LHL03a, LHY05, LTH05, PLJ05a, QCB05a, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SLC05, SCS05c, Yas08].
discretized [MA02].
discrionry [Har07b].
discursive [Mit02].
Discussion [Ano01a, Ano01b, Ano01c, Ano01i, Ano01j, Ano01e, Ano01k, KLB+02a, Mal02, Nik02b].

Disheonest [GKK007].
disjoint [Gutt04c].
Disk [Cro01, Har07b, Siv06, CS08a, Fer06].
dismantles [Hil06].
dispatches [Kee05].
displayed [CGV09].
Displays [Kuh02a].

Disputed [CAC06].
Distance [CGFSH09, CPhX04, DM07b, DW01].
distinguished [HWW04, WH02b].
Distinguishing [HSL+01].
Distortion [BGI08, CS05c].
Distortion-Free [BGI08].
Distortions [HH09, SDF01].
Distributed [BCS02, BT02, CLK01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJKR03, GSV02, GTH02, LLY06, SCF01, WT02, An08, AFGH06, BDET00, CO09b, FM02, KKL09, LN04, LLW08a, MSP+08, PS08a, Raj06, WZB05, YbJ04].

Distribution [BDF+01a, BOHL+05, BBB+02a, BSNO00, FS01b, Ina02a, Ina02b, Ku02, LLL02, NA07, Sch01a, YI01, ATS04, As04b, Bad07, CYH04, GL06b, MP08, SL07, Sph01, Sph04b, SY06, WHHT08, YS04, ZLG01].

Distributions [CY08].

Diversity [Kum01].
Divide [SKQ01].
Division [HLY05, KKY02, Tan07a, Che08b, MN14].

Divisor [KM01a].

DL [HRL09, PLJ05b, Sch01f, Sch01e, WMDR08].
DL-based [HRL09, PLJ05b].

DL-encryption [Sch01f].
DL-keys [Sch01e].

DL-STD-M [WMDR08].

DNF [BGN05].

DNS-based [Her09b].

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

Dobb’s [Dr.00c].

Document [ISO05, PJH01, ST01c, VHP01, CDS07, CL04c].

Documents [PJK01, AW05, AW08, DGK+04, GA03, ÜG08].

Do [AB01, Pie05, Con09].

Doing [BM01a].

Dolev [BPS08, BDNN02, ZD05].

Domain [AS08, Bar00c, BSC01a, BSC01b, BSL02, CJK+04, Cor00b, Cor02, DOP05, DNP07, GW01, ISSZ08, Kuh02a, Lan00d, LZ01, MM01a, OMT02, PBC05, SOHS01, SDFH00, ZLK02, BR06, CS05a, DSP01, EKRMA01, Zir07].

Domains [BR01, CLK01a, CLK01b, Vau01].

Domingo [CKN06].

Dominic [Rot07].

Domina [PY05].

Domino [LLLZ06a, LLLZ06b].
don’t [Win05c]. Don’ts [FSS01].
DONUT [CLL00]. Door [SF07]. Doors [Eri02]. DOS-Resistant [Ano01c, ANL01].
Double [ADDS06, CY08, CMJP03, Coc02a, DIM08, GH08, GB09, Hau06, JSW05].
double-base [DIM05]. Double-Gate [Coc02a]. Double-Size [CMJP03].
double-trapdoor [JW05]. Doubling [FV03].
Douglas [Spr03]. Down [BBPV00, Coc02b, Ano00g, Ano03c, Ano03a, Pot03, PBVB01, Ste05c].
Downwards [FV03]. DPA [SGB01, TV03]. DPA-Based [SGB01].
Dr. [Dr.00c]. Draft [Ste00, Dwo03]. Drastic [Sug03].
Drawn [vOT08]. DRBG [Hir09]. Dress [Ahm08].
drinks [Ano03c]. Drive [NP07, Kor09].
DSA [MR01a, SA02, Sha01d, TvdKB01].
DSA-type [Sha01d]. DSEA [LLZ06, LLLZ06b]. DSP [Geb04, WWGP00]. DSP-embedded [Geb04].
DSPs [WWGP00]. DSS [Ano09a, Ano13, FIP00, Nat00]. DTD [PCK02].
Dual-Pair [WC09]. Dual-Tree [LK05].
Dual-wrapped [HLC07]. Dumb [Eri01].
Dummies [Cob04]. Dump [KCI*01].
Dunaynir [MAaT05]. d’une [Car00].
Durahim’s [MAaT04]. during [AJ08, Bec02, WA07].
Dust [KG07]. Dutch [dL00]. Duty [ZGLX05].
Dwork [DNRS03, GK05, Zha06].
DWT [LHS05, PBC05]. DWT-Based [LHS05]. Dynamic
[AFB05, BN08, BPC01, BCP02a, BFM07, CL02a, CW09, CCD04, CTT07, GTH02, H05, Pat01, Sup03, TTT01, BB05, GL06b, HW03c, LCP04, LLY06, LCK04, LCO05, RG05, Y04]. dynamic-key [LCP04].
dynamics [BGP02, shCP09, JLC07, MR00]. dynamics-based [shCP09, JLC07].

E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-Goods [NCG05]. e-Government [RM02].
E-Learning [CAC06]. e-mail [LL04b, NS05, All06, ANR01, KS00a, Law05].
e-mails [LG09]. e-payment [Has02].
E-Security [NDJB01]. E-smart [AJ01b].
e-voting [CJT03, Cha04]. E-Wallet [ETZ00].
E-Business [Poh01, HHSS01].
KKH03, LSY01, LCK01, LKY05a, LKY05b, LC05a, Mac01, MV03a, MP01c, MN14, Nd05, NSNK05, OS01, PCS03, PBD05, Ram01, RSQ03, RDJ+01, SM01, SM03a, SW06, SRQL03, SSNGS00, Tsa08, TC05, WHLH05, WY05d, WH01, WC01a, XB01, XS03, YWD08, YLH05, Zan01, Zho06, ACTZ05, AFB05, Bla01b, CC04b, CC05c, CY05, CHC05, CLC08, DS09, Dew08, DwWmW05, FP09, efficient
[FSGV01, HHG06, HC04a, JW06, KHYM08, LPV+09, LLS+09, LCK04, LLH04, LKY05a, MAC01, MV03a, MP01c, MN14, Nd05, NSNK05, OS01, PCS03, PBD05, Ram01, RSQ03, RDJ+01, SM01, SM03a, SW06, SRQL03, SSNGS00, Tsa08, TC05, WHLH05, WY05d, WH01, WC01a, XB01, XS03, YWD08, YLH05, Zan01, Zho06, ACTZ05, AFB05, Bla01b, CC04b, CC05c, CY05, CHC05, CLC08, DS09, Dew08, DwWmW05, FP09].

Efficiently
[INP03, NNT05, AGKS07].

Effort
[Weh00].

Efforts
[Pau02a].

Eggs
[Wei06, Wei05].

EGPV
[MFS+09].

Egypt
[EBC+00, Imr03, Sin00].

Eighth
[ACM06, B+02, ELS01, IEE01b].

Einstein
[MNT+00].

EJB
[TEM+01].

Ekert
[Duw03].

El-Gamal
[EKRMA01].

Election
[JLL02, Cal00b].

Electronic
[Ble07, CLK01b, CM02, Dur01, Høi01, ISO05, IY00, KMO01, KS02, Lan04b, LLL02, Mad00, MNFG02, Rub01, RMC01, Str01a, YKMY01, ZYM05, AvdH00, AAKD09, Cal00a, EY09, FB01, HJW05].

Element
[MS02d].

Elementary
[Sin09, Ste08, Tat05].

Elephant
[FER06].

Eleven
[All03].

ElGamal
[BJN00, CL02b, CW00, HLO4, LHT09, SJ00].

ElGamal-like
[CWH00, HL04].

Elizabeth
[Bud06].

Elliptic
[ADI09, An05a, Bai01a, BNP03, Bar00a, BG09, BMM00, BS01d, BM01, BB06b, CQS01, CFA+06, GLV01, Gan02, GP08, HY05a, HMM01, HMV04, HMO2c, Hus04, JT01b, JT01a, KBM09, KMF02, Kid02, KSZ02, LW02, MP01b, Mü02, Kir03, OTT01, OS01, OT03b, WP03, RSA03b, RS04, RS01, Sat06, Sil05, Was08a, Was08b, WPS01, XBO1, YYZ01, vT01, BSS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFVZ06, DIM08, DwWmW05, EHK04, GBKP01, Hsu05a, HL05d, JW06, LL04b, LWZH05, Mis06, MSV04, OS00, ST03a, SSS06, SH05, Sim02, Sma01, SC02b, SCL05, SLC05, TC05, Van03, Ver01, YC09a, YC09b, Ya08, ZSZ01, ZL05, ANS05, BWBL02].

Ellina
[IIE01b].

Else
[FL01b].

EMA
[Qso1].

Email
[ES00b, Gar03a, Hero09b, Luc06].

Email-based
[Gar03].

Emanations
[ZZT05].

Embedded
[Ano01c, An02d, An02e, BBGM08, Dri02, DV08, GSS08, JT05, JQ04, KKP02, LPW06, NdM04, RS05, SPQ06, WKP03, YSS+01, ARJ08, BGM04, Fox00, Geb04, KVN+09, KP01, KNP01, KP03, MBS04, NS03a, TKP+08, XQ07, Fin02].

Embedding
[AAK09, JX05, JG07, LSC03, Sal03b, WY02, WC04, CO09a, KC09a, Wan05].

Embrace
[CNB+02].

Embracing
[An00c].

EMD
[BR06].

Emperor
[SM01b].

Empirical
[HW03b, Goo00].

Empirically
[SS03].

Emptiness
[DIS02].

Emulex
[CZB+01, CTBA+01].

Enabled
[Por06, CCCY01, DY09a].

Enabling
[Web02].

Encapsulation
[CHH+09, KG09].

Encipher
[BR00a].

Enciphering
[KH03, KT01].

Encode
[BR00a, BKN04, An08e].

Encode-Then-Encrypt
[BR00a].

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

Encoded
[WMS08].

Encoding
[JT01b, RS00, Lin02].

Encounter
[Win05c].

Encountering
[Hol03].

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

Encrypted
[BBK03a, BGHP02, BGLS03, CD01b, Hug04, Lan04a, LH07, MMZ00, RMC01, Sta02b, Van01, WRW02, Whi09, Woo00, AMB06, An06a, Bih02, BNP08, CCMT09, CDD+05, CSK+08, FJ04, HLM02, Hes04a, LHL04b, LSH00, MW04, Pet03, UG08].
Encrypting [Pro00, RC01, Zho06].

Encryption [ABC+05, Abe01, AS01a, Abe04, AP09, AB01, ADR02, And03, Ano01f, Ano01g, Ano01h, Ase02, ANR01, AFI06, AF03, Bar00c, III00, Ban02b, BN00a, BR00a, BMB00, BBDP01, BU02, BF01f, BF03, BB04, BGW05, BCHK07, BGH07, BPR+08, BB03, BNPW03, BD03, BKY02, Bur03, CD00a, CS03a, CHK03, CHK05, CGHG01, Che01a, CTL001, Chi08e, Cho08a, CMR06, Cla00a, Coc02b, Coc01b, CJN00, CD00a, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL08, DR02d, DA03, DFK+03, DK05, DS05b, Dr02, FIP01a, FL01a, GC01a, GSW00, Gen03, GRW06, GH05, GD02, GMM01, Gut0x, HSH*08a, HS02a, HYZ05a, HS02b, HSHI02, HW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03, HL02, HGNP*03, HLO05]. Encryption [HLC+08, ISSZ08, Joh03, Jo01, JK02b, JK02c, JM02, JKRW01, Jut01, KBD03, KSHY01, KS00a, KY01a, Kha05, KKJ+07, Kos01a, Kra01, Kur01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LLRW07, Lin03, LNP02, LM05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, M003a, Mor05, M001a, MS00, N00, NAM02, NZCG05, NZ05, NPO02b, Nie02b, PV06b, PM00, Pau09, Pem01a, PZL09, PDMS09, Pha04, Por01, PS00, Pre01, RM04, RK06, RDJ+01, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQ06, SPG06, SBZ02, SZe00, TV03, Un00a, Uni00c, Uni00e, Uni00d, Uni00g, Un01b, UST01b, VMM05, WZW05, WBFR00, Wri01, YEP+06, YW06, ASW00, Abd01, ABHS09, AKS0X4, AMRP00, ABW09, An000e, An000c, An000f, An000g, An000h, An000j, An002a, An003e].

encryption [An006d, App05, At04, AC0005, AFC006, BPS08, BKN04, BR04, BBN+09, Ber09a, BBK+03b, Bir07, Bla00, BJN00, Bro05b, CG06, CS08a, CSB06, CHC01, CKRT08, DDL01, DL07, DRS05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GKK03, Gen09a, Gen09b, GKM+00, Gou09, Gua05, Gut04c, HSH+08b, HSH+09, HS02b, HSH07, HCD08a, HCD08b, HAU04, HW02, Hsu05a, Hau05, HL05c, HL05d, Im06, JK01a, JK01b, JXW05, JSW05, JZCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Kuh08, La00, LV07, Lee01, LCP04, LJ05a, LMC+03, LLL06a, LLL06b, LLCL08, LB05, Lu02, Lu05, LK01, LW05a, Mad04, Mar05b, Mat02, Mull01b, Mun08, NK06, OS07, PB00, PS01a, Pau02a, Pau03, RG09, Ru03, RBB03, RSP05, SN00, SKW+07, Sch00, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sch01d]. encryption/cipher [HAu04].

encryption/decryption [OS07].

Encryptor [LMP+01, TPS01, An000a].

Encryptor/Decryptor [TPS01].

Encyclopedia [Bid03, vT05]. End [KCD07, Per03, SKK00, WWGP00, YSR01, AMB06, SU07]. End-to-End [YSR01, AMB06]. Ended [Kus02].

Endomorphisms [GLV01]. Endpoint [Kad07]. Enemies [DM07b].

Energy [GC01b, In05, LPV+09, SLP07, Mis08].

Energy-efficient [LPV+09].

Energy-security [In05].

enforce [SN04].

Enforcement [GN06].

enforces [BP05].

Enforcing [GMM08, HRS08].

Engine [Fri01, MMH02, DP04, SHL07].

engineer [Pau02b, SN04].

Engineering [CNB+02, MNT+00, MYC01, Pem01b, Roy00b, SM07b, TR09a, TR09b, VH09].
And08, EC05, Jen09, Man08]. engineers [Pri00]. engines [PM08]. Enhance [ZWC02]. Enhanced [JKRW01, LHL04b, ZGLX05, CZ03, McK04, OP01b, TWL05, WLT03, WHH05, ZSM05]. enhanced-security [OP01b]. Enhancement [CJ05, FLZ02, LSH03a, LSH03b, SLH03, YY04a]. enhancements [ADH+07]. Enhancing [BDK02a, MS05a, SE09, Sun00b, DY01]. enigma [Rob02, Rob09, BCB+07, Cas06, Chuh02, Cop04b, DB04, GO03, Gro00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Wil01a, Win05b, Win00]. Enigma [Kap05]. Enough [CNB+02, Pat03a, YJ00]. Enrolment [HWH01]. Entangled [Bar00c, LB04]. Enterprise [BH00b, C+02, HM05, MJF07, App05, TCR03]. Entropic [DS05b]. Entropy [DS05b, EHMS00, LH07, JRS09]. Environment [BST03, DeL07, HS01b, LSV09, IM06, KKL09, KB00, Rhi03, Whi09, ZBP05]. Environmental [PS05]. Environments [CJ05, LKH09, BG04, MNS08, SBG05, SG07, SN04, YC09a, YbJf04]. ephemeral [Mis08]. Ephemerizer [Per05]. EPOC [JQY01]. ePOST [MPHD06]. EPR [Ina02b]. Equation [FJ03]. Equations [CP02, DDDG+06, GS03, PBMB01]. Equipping [DMM07]. Equitability [DB01]. equivalence [Fis01a, LQ08, MSV04]. Equivalent [Fer00, KOM01, May04, SIR04]. Era [MP00, Uni00c, Bur00, Uni00f]. erase [PCS03]. Erasures [JL00]. ERP [LS05]. Equipment [DMT07]. Equitability [DB01]. Equivalence [Fis01a, LQ08, MSV04]. Equivalent [Fer00, KOM01, May04, SIR04]. Era [MP00, Uni00c, Bur00, Uni00f]. erase [PCS03]. Erasures [JL00]. ERP [LS05]. Erratum [AGGM10, Kwo03b, LLLZ06a, McK04]. Erroneous [CH01b, MNT+00]. Error [BBK+03b, BQR01, Din05, KGG03, JW05b, LM02, MLC01, MPSW05, MZ02, NN06, SKQ01, YI01, YYYD01, ZYR01, Zo01, Gar04, LHL04a, YY06]. Error-Correcting [NN06, ZYR01]. Error-Prone [MLC01]. Errors [AD07, AL07, Reg05, Reg09]. escape [Bhu09, Fur05]. Escrow [AK02a, Ano01a, CL01a, DBS01, LCK01, ATSVY00, CL02b, LCC05]. Escrowed [PS01b]. eServer [AV04]. ESORICS [dCdVSG05]. espionage [Bud06]. essays [MAaT07]. Essential [Cop04b, Dr.00c, MRO2a, MR02b]. essentials [HHL+00, Irw03]. establishing [Kov03, KH03]. Establishment [BM03c, NIS03b, HMDLM07, LF03, SL05a]. Estimation [EFY+05, JX05, KLB+02a, LNL+08, Sel00]. ethical [Har05b]. Euclidean [CPH04, CMJP03, CLZ02, WL02]. EULA [WWL+02]. EUR [Eag05]. EUROCRYPT [Bih03, CC04a, Cra05a, Knu02, Pri01, Pre00, GJSS01]. Eurographics [MFS+09]. Europe [Pag03]. European [AL06, CZ05, KGL04, Pre01, dCdVSG05, Ano00f, Che08b, Die00, Pre02a]. EUROPKI [AL06, CZ05, KGL04]. EV [HTJ08]. EV-C2C-PAKE [HTJ08]. Evaluate [Pre02a]. Evaluating [BGN05, NTW07]. Evaluation [BSC01a, EYCP00, FS00, FML+03, IKM00, IY00, JI00a, Kan01, Kir03, SKK00, BZP05, FXAM04, FS03a, LCP04, MCHN05, RC05, RN00a, RN00b]. Evaluations [LM02]. Evangelizing [Coc01a]. evasion [Bhu09]. even [Bih02, OS00, Win05c]. EventGuard [SL05b]. events [SBS09]. ever [Fur05]. Everlasting [DR02d]. Every [TH01, DKK07, Win05c]. Everyone [Han00]. Everything [CTBA+01]. Everywhere [Ber00]. Evidence [Ver01, Bro05a, HW03b]. Evolution [DF01, Ree01, Pat02a, SP02, Sin99, Sin00]. evolutionary [LMSV07]. Evolved [LMHCETR06]. Exact [Cor00b]. examines [Nis03a]. example [Bla00, GC05, Zir07]. Exchange [BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JI08, KOY01, KY03,
MPS00, Mac01, MSJ02, Ngu05, VPG01, 
WC01a, WV01, ZWCY02, BBG+02, BCP07, 
CLC08, CWJT01, DG06, GL06a, GMR05, 
HTJ08, KS05a, KOY09, LHL04b, LW04, 
LFHT07, LHC08, LSH00, MS03a, Miš08, 
WLH06, YC09a, YPKL08, ZYW07, CPP04, 
CP07, ECM00b. exchanging [KN08].

Exclusive [GRW06]. Executing
[HILM02, LJ05a]. Executing [Coo02].
Execution [HILM02, LJ05a].

Exhaustive [Des00c]. Existing
[MV01, BDET00]. Expanded
[Cho08a, Irw03]. Expanding [DN02a].

Expansible [LLW08a]. Expansion
[DN02a, BCD06, HKPR05]. expansions
[HKPR05]. Expected
[KL05, RK06, DLP+09]. Experience
[Sas07, BCHJ05]. Experiences
[MPHD06, USE00b]. Experimental [BG09, 
CGBS01, ÖOP03, WS02, RSQL03, Smo04].

Experimentation [Hun05]. Experimenting
[LSVS09]. experiments [Bru06]. expert [Ano01g]. Expiration
[MP00, Sch05b]. Explicit
[CY08, GRW06, WPP05]. Exploit
[BR00a, FOBR05]. exploitation
[Eri03, Eri08, KV+09]. Exploiting
[CK06, ETMP05, HR00, HM04, ZWC02].

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

Exponentiation [BP04, BM01b, DN00b, May02, 
SZ01, CKY05, Duj08, GD05, Shp04b].

Exponential [KKH03, SK07, CKRT08, HGNS03].
Exponents [FS02, FS01b]. export [Ano00h].
Exposed
[Gum04, MSK03, SSS06]. exposing [YY04].

Expositive [MAaT05]. Exposure
[BM03b, DSS01, KZ07, CDD+05, KZ03].
Exposure-Resilient [DSS01, KZ07, KZ03].

expressions [MW04]. Extended
[ABDS01, BPS00, CM00, Cou04, DIRR05, 
HLvA02, HJW01, JL00, MSJ02, MP02, 
OST05, Wag02, BJN00, CD00a, HT04, HP01, 
Mls06, Pei09, QPV05, LklJl01]. Extending
[ADD06, IKNP03, Ove06, Sal03b, SS01a].

Extension [Bai01a, YWD08, BR06, Cmmd06].

Extensions [ABC+05, BBGM08, CS07c, 
HM02b, Rot02a, Wei04]. Extracting
[Cer04a]. Extraction
[DG+04, RV03a, MB08, PV08].

Extractors [Fis05, KLR09, KZ07, Lut02, 
Vad03, DW09, KZ03, Sha04a].

Extraordinary [Top02]. Extreme
[Ano02d]. Extrusion [Bej06]. Eye
[Sas07, CAC03]. Eye-Opening [CAC03].

F5 [Wes01]. Face
[KZ09, NH02, PK01, SBG02, Tzt09b, PY08].

FaceHashing [Tng04]. Faces
[NS01c, Ngu01]. facets [Rot02b, Rot03].

fact [Ano03e]. Factor
[DN02b, Sas07, BSSM07, Hen06b, Sch05c, 
St.00, St05a, YWWD08, db07]. Factoring
[BN02, KY02a, KLB+02a, KOMM01, May04, 
PV06b, ST03b, LTH05, LCEO5c, Mü01b, 
PLJ05a, QCBO5a, Sh03d, Sh05d, ZCL05].

Factoring-Based [PV06b]. factorisation
[GG08]. Factorization [CDL+00, Lam91].

Facts [GO03]. Fade [CAC03]. Fail
[QYY01, SSG00]. Fail-stop [SSG00].

Failures [DFG01, HGNP+03]. Fail
[CC00, DLY08, GC01a, JLL01, JL04, LMS05, 
PS00, VPG01, Wv01, LSA+07, MS03a].

Fair-Zero [LMS05]. fairness [GCKL08].
faithfulness [GTZ04]. false [ZJSN07].

Falsification [OM09]. Fame [Bar00c].
Family [CQ01, Fh02b, NPV01, SK05a, 
You1, Ber07, FRNC05, GBKP01, MP07].

Fan [YR05c]. fare [GM00]. Fascinating
[Sch09]. FASME [RM02]. Fast
[AL00b, ABM00, BDTW01, BST02, CJS01, 
CC06, CQ01, Cor00a, Cou03, Cro01, FS02, 
GC01a, GD02, GMM01, GPC08, HGG07, 
HR04a, JJo0d, KKM01, KK03, KJ+07, 
LSY01, LS05b, MSNH07, Kix03, NS05a,
NSS02, OKE02, OT03b, PG05, RR02, Tsa06, UHA+09, Yan05, ABB+04, BMA00a, BMA00b, BMA00c, JAW+00, J02, Lud05, PBM01, WWA01, Bir07, DR02c, GH05, Job03, Mat02, RM04, Sch00b, Sch01d.

Faster [Bar00c, CMJP03, GLV01, KS09a, LV04, Oec03, Ban05, Why05]. faszinierende [Sch09]. Faster [Bar00c, CMJP03, GLV01, KS09a, LV04, Oec03, Ban05, Why05]. faszinierende [Sch09].

Fault [Ano04a, BMM00, BK06b, BKM07, DS03, Gir06, PV06a, PQ03b, WL07b, YKLM02b, HGR07, Lin07, PI06, RMH04, YJ00, YKLM03, ZL04a]. fault-based [YJ00].

Fault-Tolerant [WL07b, HGR07, Lin07, RMH04]. Faults [GSS08, VS08]. Favour [MFS+09]. FB1 [Mad04]. FC [Bl03, Fra01, Jue04, PY05, Syv02, Wri03].

Feasibility [APV05, BDET00]. feasible [LM08]. Feature [GW01, Gut02a, HH09, LN02, LL06a, NN03]. Features [PK01, SBC02]. February [DR02c, Fra01, GH05, Job03, Jue04, Ki05, Kim01, Men05, NP02a, Nao04, Ok04, PY05, Poi06, Pre02c, RM04, Syv02, USE02a, Wil99].

Federated [DeL07, GTY08]. Feedback [CGFSHG09, CM03, Con03, Ig02, Hey03, SPG02]. FeedForward [BP01a]. Feel [PM00]. Feeling [Buh06]. Feistel [Con04, Kan01, LMSV07, On01, Pat04].

Feldman [AF04b]. Ferrer [CNK06]. Fetal [MYC01]. fetch [HT07]. Fi [Sty04, Bar03]. Fiat [VS08]. fiction [An003e]. FIDES [ISTE08]. Field [FJ03, GC01a, RDJ+01, CKY07, GM00, Has00, JL03, ST03a]. Fields [Bai01a, BT02, CU01, Che04b, CQ01, CFS05, HCK09, HHM01, KKH03, Lov01, MNP01, MM07b, RS08, SP05, SKG09, Ver02, Gar04, HP01, JL03, RM04, Sim02, Sm01].

Fifth [ACM03b, SM07b]. Fighting [DGN03, SZ03]. File [CCDP01, GIS05, Ito01, LK01, BDET00, CSK+08, HTW07, Hos06b, ISO05, MKKW00, MSP+08]. Files [Tot00, Che02, Lov01]. Filesystem [Bau02b, Pet05]. Filesystems [WBL01].

Filter [LBGZ01, LBGZ02, MSHN07, Sar02, CMS08]. Filter-Combiner [Sar02]. Filtered [MH04]. Filtering [SDH00]. Final [DPR01, Dra00, GC01a]. Finalist [SB00].

Finalists [EYCP00, IKM00, IK00, IK01, Mes00, Mes01, SKKS00, SW00a, WWCW00]. Finally [Coc02b]. Financial [An05, Gri01, Pem01b, Wri03, Bla03, Fra01, Jue04, PY05, Syv02]. Find [LH07]. Finding [HR04b, MP06, WYY05b, WYY05c, ZT03, SW00b]. FINDsomeone.com [Gra98]. Fine [SS01b]. Fine-Grained [SS01b]. Fingerprint [An02d, HHY07, HBF09, KHY04, MMH02, CL04d, MMJP03, UBEP09]. fingerprint-based [CL04d].

Fingerprinting [KT01, CTT07]. Fingerprints [TK03, KLY03, S04]. Fingers [MMH02]. Finite [BLST01, BR01, CU01, Che04b, CQ01, HCK09, HW05, KKH03, MM07b, PHK+01, RS08, Ver02, Gar04, Has00, LMC+03, LQ08, NS01a, RMH04, Sma01, SLTB+06, TC00].

Finkenzeller [And04]. FIPS [Nat00]. firewall [LJ04]. firm [Zaf00]. First [Bar00a, BBD09, Coh03, CM02, CMB+05, FLY06, KGL04, KS06b, MPN01, Nao04, NNT05, OP03, PK03, QSR+02, Roy00a, USE00b, Wi99, ZJ04, ZHY03, AJ01a, Cla00b, Coc02a, DV05, LBA00, RH00, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, Lan00a].

First-order [Coh03, KS06b]. Fish [Fie09, Wei06, Wei00, Wei05]. Fit [CCM05]. Five [SW00a, MS20b, Rot02b, Rot03]. five-lecture [Rot02b, Rot03]. Fix [TEM+01]. Fixed [AR01, BCCN01, CKN00, LS01a, Shp04b, SP79]. Fixed-Length [AR01, CKN00]. Fixed-Size [BCCN01, LS01a]. Fixing [KZ07, KZ03]. FL [Des02, Jue04]. flash [ST06, SGB01]. Flat [SV08a]. Flaws
[Gra02a, SPMLS02, Vau02, SL05a].  
**Flexibility** [LP02a].  
Flexible [CMG01, CLK01b, DGK00, OT03a, Tsa01, BA06, KOC05, LHY02, WWA01].  
**Floating** [NS05c].  
Floating-Point [NS05c].  
Flow [BDNN02, ABEL05, FR08, ME08a, TWM05].  
**Flows** [ECM00a, AHS08, Cer04a, Lau08a].  
**Flying** [Fox00].  
FOCS [IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07].  
**FOKSTRAUT** [BH00a].  
**Foo** [Puz04, VGM04].  
**Food** [MNT00].  
**Fool** [RW02].  
**Footsteps** [Lav06].  
**force** [Cur05, SGA07].  
**forces** [AJ08].  
**Ford** [Mar05a].  
**Forecast** [Rai00].  
**Forecasting** [WWL02].  
**Forensic** [PS08b, Cas02, Kor09].  
**forensically** [ME08b].  
**Forensics** [JBR05, CS04, CS08a, CDS07, MS09a, MKY08, MAC03].  
**Forest** [FBW01].  
**Forgery** [CH01a, CKM00, LS01a, SLT01, HSW09].  
**Forgotten** [Eag05, Kin01, OC03].  
**Form** [ADI09, CH07c, OS01, LKYL00, Mic01].  
**Formal** [BGB09, Bel07b, BCHJ05, BCJ06, CL05, DKS08, GOR02b, HG03, Lan00d, Mea01, YWD08, ABHS09, JW01, Mea04, Pau01, SW02, ZLX99, ZL04b].  
**Formalizing** [HM01a].  
**format** [ISO05, RG05].  
**format-string** [RG05].  
**Formation** [RW03a, Luk01].  
**Formats** [GIS05].  
**Former** [Mad04].  
**Forms** [JT01b, LLL04].  
**Formula** [Kog02].  
**Formulas** [CH07b, WPP05].  
**Forum** [CH06a].  
**Formulations** [AHRH08].  
**Forum** [CBZ01, CTBA01, CNB02, CMB05].  
**forums** [Hil06].  
**Forward** [AR00, AF106, BY03, CH03, IR01, HCD08a, HCD08b, SY06, ZYW07].  
**Forward-Secure** [AR00, AF106, CH03, IR01].  
**Forward-Security** [BY03].  
**Forwading** [KCD07, Kra02b].  
**FOSS** [Bo102].  
**Found** [Bar00a].  
**Foundation** [Lut03].  
**Foundations** [DKK07, Gol01b, Gol01a, Gol04, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Nie02d, Sal05d, Kat05b, Puc03].  
**Founder** [Bar00a, Ano03c].  
**Four** [LXM05].  
**Four-Layer** [LXM05].  
**Fourier** [Che07, DSP01, DNP07, KOC09b, LPZ06, SP04].  
**Fourteenth** [USE00c].  
**Fourth** [ACM02, ACM05b, DFCW00].  
**FPGA** [Ano02e, CC02a, CGBS01, CG03, CNPQ03, EYCP00, EHKH04, KMM06, KY09, KBM09, KRS02, LP02a, MM01b, MM01c, OTIT01, OOP03, Pat01, PBTW07, QSR02, TYLL02, TPS01, US02, WW00].  
**FPGAs** [AD07, DPR01, MMT09, RSQ03, SGM09, SK05a].  
**Fractal** [AA04a, JLM03, WC03a].  
**Fraction** [Wal03].  
**fractional** [DSP01, SSST06].  
**fractions** [Dan02].  
**Fragile** [CC09, CH01b, CT09, Nac01, OK04, USE02a, USE02b].  
**Frame** [LHS05].  
**Frames** [HWW05].  
**Framework** [ANRS01, GL03, GOR02b, Hun05, NMO05, NP07, PS06, R002, ZYN08, AHK03b, Ayo06, CCCY01, CP07, CC04c, DMSW09, GJJ05, GL06a, GM04, JEZ04, KNS05, MS09b, MBS04, YC08, HF00].  
**France** [ACM04a, ACM05a, AJ01a, AJ01b, GH05, KN01, NP02a, PPV06, KM07].  
**Francis** [Cal00c, Joy03b, Men05, Nac01, Oka04, USE02a, USE02b].  
**FranzSteiner** [Eag05].  
**fraud** [Ano03a].  
**Fred** [Bar00b].  
**Free** [AP09, Ano02e, Bau01a, Bau01b, BGI08, Coc01a, CNC06, DG02, HS00, HM01b, JP03, Jut01, Fox00, KSO06, SBG05, Bol02].  
**FreeBSD** [Coc01a, Mur02, Siv06].  
**Freedom** [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, Mil03].  
**FREENIX** [USE01b, USE02c].  
**French** [Wri03].  
**Frequencies** [DD02].  
**Frequency** [OMT02, Sak01, SOHS01, CS05a].  
**Frequency-Domain** [OMT02].  
**Frey** [Was08a].  
**Friar** [GG05a].  
**Friendly** [CTY09, CRSP09, Hau05b, HL05b, S050, WLT05, WC03b, YW04b].  
**FrontPage** [WWL02].  
**FSE** [Bi07, DR02c, GH05].
Joh03, Mat02, RM04, Sch00b, Sch01d]. FTC [Ste05c]. fuels [Mad04]. Full [Cor00b, DOP05, LKHL09, WYY05b, WYY05c, BLO4, CS08a, HS02b, LKH+08, Oiw09].

full-encryption [HS02b]. Full-Round [LKHL09, LKH+08]. Fully [BL08, FS01a, Gen09b, KPMF02, RG09, Gen09a].

Function [BR02, CDMP05, Fis01b, Flu02b, GIS05, HNO+09, HMS04, HR04b, Jou04, Kil01b, LTW05, Lys02, PR01, RR08, SM00a, SM00b, SS01a, Sho00a, Sho00b, Ver02, WP03, WFLY04, Wer02, AGGM06, AGGM10, ALV02, CS09, DS09, GVC+08, HRS08, ISO04, KK07, KS05b, LLH02, LKY04, MS02b, MS00c, Mic02a, Mic02b, NR04, PW08, QPV05, SM03a, Whi09, YRY04, ZW05a, RRS06].

Fundamentals [And04, PHS03, Shi08, Way01, vT00, Fin03].

Funds [Coc01a]. Further [JS05, JPL04, LL04a, LL05c, MP07, YRY05a].

Fusion [KZ09, TZDZ05, ZS05, BG09]. fusul [MaaT05].

Future [ASW+01, Ano02f, Joh00, LNP02, TF05, YRY05a].

Fuzzing [SGA07]. fuzzy [HS02b, NC09].

fuzzy-based [NC09].

G [Coc03, For04, Was08a]. Gaitherburg [SMP+09]. Gamal [EKRAM01]. Game [DHR00, LM02, CAC06, BR04, Jou09, HCBLETRG06]. game-like [Gou09].

game-playing [BR04]. Gamers [MP00]. Games [KN08, HCBLETRG06]. Ganesh [For04].

Ganzua [GP06]. Gap [OP01a, PWGP03, RW03a, Sch02, Sch04d].

Gap-Problems [OP01a]. Gate [Coc02a, GC01a]. gates [TW+09].

Gauging [PvS01]. Gauss [KKH03].

Gaussian [EKRAM01, JL03]. Gbps [TPS01]. GCD [JP03]. GCD-Free [JP03].

GCM [KS09a]. geeks [McN03].

Geheimschreiber [Joy00, UW00]. GEM [CHJ+01a, JM02].

General [AB09, CDM00, DN00a, ESG+05, GMP01b, Kog02, Lin03, MND+04, Sal01a, YC01, HCBLETRG06, IY06, JL03, LJ05a].

General-Purpose [ESG+05].

Generalisation [DJ01]. Generalizations [YYZ01, HWW02].

Generalized [LD04, LS08].

Generating [BMK00, BCDM00, GG01, MFK+06, SS03].

Generation [ACS02, BH05, BK06a, CS03c, ESG+05, GJKR03, GL01, GW01, JG01, MR01a, Ram01, TL07, TV03, WP03, WLY05, Web08, WS02, Ano04c, BK07, BG08, BF01c, ISTE08, LS05b, TNG04, Van03].

Generator [ADD09, MRL+02, RF08].

Generators [BST03, BK06a, BL08, C01b, CS05b, Fin06, Kra02a, LGZ01, LGZ02, LS05a, MH04, RSN+01, Vav03, BK07, BGPG05, C090b, SK01b, Tsa06, YZ09].

generators-part [SK01b].

Generic [BN00a, DOP05, GG05T05, HLL05, Mar02b, MV01, GT00, MP08, Sch01f, Sch01e, XLMS06, CHJ+01a].

Genetic [HSIR02, LHCETR06, CV05, SC05a, WJP07].
Gennaro [Miy01].
Gennaro-Krawczyk-Rabin [Miy01].
gentle [RR03a]. Gentry [Hes04a]. Genus [CY02, GHK+06, Wen03]. Geometric [GTTC03, HH09, LLS05a, LL05c, LJ05b, SDF01, CJT01]. Geometrical [LWS05].
genometry [PFV96, WW06]. George [Gum04]. Georgia [IEE09b].
German [Sch09, Ano04b, Lin02, Mor05, Sal00b, Sal00a, Win05b].
Germany [DRS05, Duw03, FLA+03, WKP03, IEE01b].
Geschichte [Sch09].
get [Coc01a, WD01a, Cla00b].
gets [Bor00].
GF [BINP03, KPMF02, KLY02, KKY02].
GHS [GHW01].
GHS-authenticated [SC05b].
Gnana [For04].
GNU [Coc01a].
GnuPG [JKS02, KPMF02, KLY02, KKY02].
GNY [Tee06].
Go [Bur06, CZB+01, HCBLETRG06].
Goals [PHM03].
Gold [Boy01, For04, Tsa07].
Goldreich [Kat05b, Lee03b, Puc03, AC02].
Gong [GG01].
Good [CB01, Kid02, MP06, GG05b, vT01].
Goodness [CMB+05].
Goods [NZCG05].
Google [Con09, Law09b].
Googling [Con09].
GOST [SK01a].
Goubin [Sma03b].
Governance [TPPM07].
Government [IY00, RM02, Lev01, LICS09].
Governments [Ano00g].
Grad [Bau01a, Bau01b, Luc06].
GPS [CKQ03].
GPT [Ove06].
GQ [BP02].
graduate [GV09].
Grafton [Pag03].
grain [Rhi03].
Grained [SS01b].
Grand [Svy02].
granted [Ano00b].
Graph [CGFSHG09, GTTC03, HM02b, VVS01, YKW01, CTT07].
Graph-Based [CGFSHG09, HM02b, CTT07].
Graphical [vOT08].
Graphics [CK06, DNP07, MFS+09].
Graphs [NNT05, Ust01b, WGL00].
Gravrilenko [Puz04].
Gray [FG01, Har05b].
Gray-Scale [FG01].
grayscale [YCL07].
greatest [Bel07a].
Greece [ACM01a, KGL04, SM07b].
greedy [HKPR05].
Green [TR09a, TR09b].
GREMLIN [Hes01].
Grenoble [ACM05a].
grey [BDN00, SCS05a].
Grid [ACM05a, MJ02, SEF+06, TLC06, ZBP05, Cha07, CJK+04].
GridOne [YC09c].
Grinds [CTY09, MPPM09].
grip [Buh06].
Gröbner [CCT08, FJ03, Fau09].
Group [ANRS01, AAFG01, ACJT00, BSS04, BCP01, BCP02a, BCP02b, CD00a, CvTMH01, CH01a, HSH02, HSH06, HWW04, Hug02, JPDF02, KY01, Kin02, LZL+01, MSU05, SOO10, SWH05, Ste01, Tan07b, VMS05, Wer02, AKNR04, BCP07, CL04b, CYN04, CHC05, CWJ01, CTO04, Cho08b, ED03, He02, Hen06a, HWW02, KS05a, KPT04, KKL09, LL06, LHK04, LWK05b, NS05b, PQ03a, PQ06, RH03, SNW01, Shao05a, TJ01a, Tse07, WGL00, WHHT08, YLC+09].
Group-by [YLC+09].
Group-Oriented [LZL+01, HWW04].
CHC05, CWJ01, LLD06, TJ01a, WHHT08].
Groups [BSS02, CV03, CF02, Dru00, GM02a, GST04, KM01a, KLC+00, LL01, LP03, Luc02b, MN01, PHK+01, GR04, HM00, LLY06, Pac03, Yi04].
GSM [BBK03a, BD00a, Cha05b, Cim02].
Guadeloupe [Wri03].
Guana [Buc00a].
Guangzhou [LLT+04, Li05].
Guessing [AGKS07, Bau05, Shi05, YS02, DLMM05].
Guest [KP03, Sak01, BK06b, MFS+09, PTP07, SJT09, SGK08].
GUI [LGO9].
Guide [Ano06c, BS01a, BSB05, BCP+03, BCP01b, HM04, Poo03, Vac06, Wei04, And08, Bon00, Bro05b, C+02, CHe00, Gar03b, Kov03, Lun09, Mol05, SL06].
Guidebook [SEK01, SEK02]. Guided [ZY08, Pet08]. Guidelines [MMZ00, Die00].

Guildford [KN03]. Gummy [MMYH02].

Guo [LLLZ06a, LLLZ06b]. Gutmann [Uzu04].

H [Was08a]. H.R [Uni00d, Uni00h]. H.R. [Uni00a, Uni00e]. H64 [GMM01].

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

hacker [Gol08, Har05b]. Hackers [SEK01, SEK02, Ano01h, BD04b, NRR00, Win05c].

Hacking [Eri03, Eri08, Gum04, Man08, MSK03, SSS06, VGM04, Puz04, Har05b].

hacks [Sti06b, Sti06a]. Hadamard [HWW05]. Hagenberg [Jef08]. Half [HS02b]. Half-encryption [HS02b].

Halfspaces [KS06a, KS09b]. Hall [Bar00c, For04, Kat05b, Was08a, MAA05].

Hall/CRC [Kat05b, Was08a]. Halmstad [BS01b]. Hamming [DK02]. halper [Lov01].

Hand [WBL01]. Handbook [And04, Cas02, CFA +06, Jan06, MMJP03, RE03, AB09, Fin03, Har05b, KB00, KH03, MJ03, RE00, dLB07, Was08a].

Handheld [BMK00, Ano06a]. Handhelds [MP00].

Handle [RC06]. Handling [KL05, Lut03].

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

Handshakes [Ver06a]. Handwriting [Ano02d]. Hankerson [Irw03]. Haptic [PBM *07].

Haptics [Pau02a]. Hard [Har07b, HMM04, 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, DIC03, FW09, FD01, Fri01, GS03, GS07a, GKO2, GPS05, GLG+02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, Nd05, PS01c, RS05, RS04, SOTD00, SMTM01, SM02, SM03a, SRQL03, SGK08, TSO00, TBLD01, WK03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK+03b, DS09, EHHK04, GC00a, HBC+08, KP01, KNP01, KP03, N0M04, RAL07, SOI07, VS08, Wol04, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07]. hardware/software [ARJ08].

Harley [WPP05]. Harn [GG01]. Hash [Ano08d, Ano12, AEMR01, BBK01, BRS02, BDS09b, Bu06, CBB05, Cor00b, Cor02, CDMP05, CS02, DOP05, FIP02b, Fil02, GIS05, GLG+02, HPC02, HR04b, ISO04, Jou04, KMM+06, MD05, RRS06, RR08, RB01, SS01a, Sho00a, Sho00b, SK05a, WFLY04, Yan05, YZ00, BR06, DS09, KCL03, Ku04, RCC05, LLH02, LKY04, LW04, MS09c, Mic02b, Tsa08, Wag00, YR04, FIP02a, ZW05a]. Hash-based [BDS09b, KCL03, Ku04, KCC05].

Hash-CBC [BBK01]. Hash-chaining [CBB05]. Hash-Function [BRS02].

Hash-functions [ISO04]. Hashes [Sch01a, GN05]. Hashing [IK005, SGG00, WS03]. HAVAL [WFLY04]. HAVALE-128 [WFLY04].

HAVEGE [SS03]. HB [MP07]. HB-family [MP07]. HB-MP [MP07]. HCI [YKMB08].

crack [RFR07a, RFR07b, RFR07c]. crack [RFR07a, RFR07b, RFR07c]. headlines [Hen06b]. Health [Mad00, Ano03a, CCC01]. health-care [Ano03a].

Healthcare [BTTF02]. heap [ST06].

Hearing [Uni00c, Uni00g, Uni00b, Uni00f, Uni00h].

hearings [Uni00b]. Hodge [Sho00b].

Hedged [BBN+09]. Heimdal [WD01a].

held [Buc00a, PPV96, Uni00b]. Help [Pau02a].

help [Buc00a, PPV96, Uni00b]. Hellman [KM04a, ABR01, ASW+01, BS01d, BNP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKR97, FS01b, GR04, K1001b, KK02, Kra03, Kra05, Mi08, Tsa06, YRW05]. 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, KHYM08, ZBLvB05]. Heterogenous [H¨of01]. heuristic [SS03]. HFE [FJ03, CHH01, Fel06]. HFE-Cryptosystems [Fel06]. HIBE [CS07c]. Hidden [HGNs03, KW03, LNS02, GMR05, Lun09, Shp05, FJ03, Sch09]. Hide [CC06, PH03, Shp05]. hide-and-seek [Shp05].
Hiding [BD03, CLT07, Col03, DN02b, GA05, HNO*09, LHS05, LS08, MH05, MMT09, VDKP05, WC03a, HR07, JD01, KP00, RSP05, Way02b, Way09, YCL07]. Hierachy [HC08]. Hierarchical [GS02b, HNZI02, HL02, Lin01a, MN01, YLH05, BD04b, Che07, C303c, JW06, KAM08, WC01b, hY08]. hierarchies [AFB05, Cer04a, HY03, WL05]. hierarchy [CMD06, HW03c, Hwa00, JA02].
Hierocrypt [OMSK01]. Hieroglyphs [Wri05]. High [ACM01b, An00d, An002d, ChLYL09, CW09, CJL06, CGJ*02, DS05b, FZH05, Gro01, HNZI02, HV04, Int00, JKRW01, KMM*06, Ken02b, KM05, KB00, Kra05, K05, MM01b, NF03, RW07, SKKS00, SOTD00, SM02, SGM09, SLG*05, TL07, Uni00e, Wie00, WWGP00, YKMY01, Zhe01, BVP*04, BZP05, BGL*03, Jen09, KCC09a, SK03, TH00W08, Zir07].
high-assurance [Jen09]. High-Bandwidth [CGJ*02]. High-Dynamic-Range [CW09]. High-End [SKKS00, WWGP00].
High-Performance [Kra05, NF03, BZP05]. High-Speed [An000d, An002d, Gro01, JKRW01, KMM*06, SOTD00, SM02, Wie00, YKMY01, RW07, BGL*03].
High-technology-crime [KB00].
High-Throughput [HV04]. Higher [CV02, KCP01, BF01a]. Highly [CV02].
hijacking [Ste05c]. Hill [Gun04, USE02a].
Hilton [KJR05]. HIPAA [AEV*07].
histograms [CO09a]. historic [Pet08].
Historical [RE02, MMM01]. History [BP03b, ffr00, Pag03, Sal01a, Sin01b, CAC06, Top02, AJ08, Boo05, HSW09, Jan08b, KNS05, Na050, Nis03a, Pin06, Ris06, RH00, RG06, Wi01a, dLB07].
history-based [KNS05]. hit [Bjo05].
HMAC [FIP02a, DGH*04, Hir09, RR08].
HMQV [Kra05]. Hoare [dH08].
Hoax [CZB*01, CTBA*01]. loc [BSS02, Cha05b, DHMR07, KH05, KVD07, LH08, LKZ*04, PCS07, SLP07, TW07, WT02, ZC09].
Hold [PM00]. Holier [MYC01]. Holistic [RM02].
Homage [JPR02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03].
Homegrown [Str02]. Homeland [Man02, Man05, RR03b]. homogeneous [MF07, PS02a]. Homomorphic [AS01a, Aki09, CDN01, DN03, HS00, Cho06, Gen09a, Gen09b].
homomorphism [CKN06]. homophonically [Sav04].
Honeynets [DMD07]. Hong [B+02, ZJ04, Cla00b]. honor [OC03]. hook [JEZ04].
hooks [GJJ05]. hop [NC09, ZS07].
hop-by-hop [ZS07].
Horizon [Coc02b]. host [Shu06]. hostile [ABB*04].
Hosts [HFC01, SZ08]. Hot [IEE01b].
Hotel [USE01b, USE01a, USE02a]. HotOS [IEE01b]. HotOS-VIII [IEE01b].
hours [Fox00]. House [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Hsu [BCW05, HL05c]. HTML [CNB*02].
HTTP [Zha00]. Huang [ZC05].
Huge [MSNH07, NNT05]. Hull [KMT01]. Human [Dre00, GL01, JW05, KOY01, Man08, MS02d, RFR07a, RFR07b, RFR07c].
Human-Memorable [KOY01]. Hundred [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].
Hunting [GJL06]. Hwang [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KCL03, LW05c].
QCB05a, WL05, YRY05d, ZYR01.

Hwang-Rao [ZYR01]. HWWM [LKY05c].

HWWM-authenticated [LKY05c].

Hybrid

[ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJO3b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02].

Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05,TM06]. Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05, TM06].

Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02].

Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02].

Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02].

Hybrid [ADI09, CBB05, KD04, LZO4, PK01, Asl04a, CJ03b, HG07, LPM05, TM06]. Hyderabad [MS02c]. Hype [Way02a]. Hyper [DR02d, Lu02, PZL09]. Hyper-chaotic [PZL09]. Hyper-Encryption [DR02d, Lu02].
Image-Feature [GW01].
image-identification [PBV08]. Images [CTL04, CC09, CW09, DP00, FG01, LS08, PJ01, PBC05, RE02, WC09, WC04, YWWS09, AAP07, AEE05, BDN00, FWTC05, HHYW07, TCC02, TN09].
Imaginary [HJW01, HM00, H¨uh00]. Imaginary [HJW01, HM00, H¨uh00].
Imbalance [ZWCY02]. Imbalance [ZWCY02].
Immersive [Coc01a]. Immune [DDG06, YG01a]. Imbalanced [ZWCY02].
Immunization [HR05]. Impact [Ber03, HGNP03, JKRW01, MMYH02, Wri00, CS08a].
Imperfect [CPS07, DOPS04]. Impersonation [BP02, Hsu05b]. implant [Fox00]. Implement [HQ05]. Implementation [AD07, Ase02, Ash03, ARC01, BBD02, CCDP01, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, JKS02, KMM06, KV01, LP02a, MMZ00, MKP09, MM01c, MN01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBTW07, QR07, RDI01, SM01, Sha01e, SK05a, SR0L03, USS02, Vir03, WZW05, WW00, WOL01, XB01, Zea00, BI04, BB03b, C+02, CNPQ03, DS09, DKL00a, GH0400, GKB01, Huh00, HP01, Hut01, KY09, LR04b, LCX08, LB05, Rhi03, SM03a, SVD07, W01, YW06, ZKF04].
Implementations [AL00b, BJ02, IIO0, CLT0L0, CG05b, EPP07, GLG02, MM01b, MP01a, RS01, WW0W00, ASK05, BCFZ08, BF0708, BG07b, FR08, RAL03, RS0L03].
Implemented [TSS03]. Implementing [Dw04, Ko08, LM08, MDO4, MWS08, NDJB01, PET03, Sm01a, SR06, C+02, CW02].
Implications [Kun01, LJO5a, MF01, AYO06, BJ05, Fr07]. Implies [KY01e]. Imply [Pie05].
Importance [ANO2b, KJC01, TIGD01]. Important [SM00a]. imposed [XLMS06].
Impossibilities [CHL02]. Impossibility [APV05, BPR08, FIS01b, P06].
Impossible [BF00a, BF00b, CKA+02, HSQ02, MHL02, Pha04, SKU00, SKI01].
imposter [LC07]. improve [Pau02a, CAC06]. Improve-ment [CAC06]. Improved [AFGH06, BPR05, BB05, BF00b, CL01b, CKA+02, CJO4, DN00a, DG02, Fun03, FKS00, FKL01b, FKL01a, GMR08, Gen00b, HCK09, HKA05, JQY01, Kin00, KT06, Ku02, Kiuh02b, LW04, LL06, Mic02b, Miy01, MH04, Kirk03, MS02e, PR08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, JHT08, Iwa08, PR05, QC05a, YW05, YRY05a, ZW05a].
Improvement [AS01c, AOJ08, Che04a, C2505, CCW02, Di01, HWW03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT00, NP07, Sha04b, Sha05b, WHL03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, C2CO4c, CL04c, CHY05a, Hsu05a, JSW05, JnBdXm05, KJ05, LL04a, LA05, SZS05, TO01, WLT05a, YW04a, YWC05, YRY05a, YRY05d, ZC09].
Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, HW03c, SRQL03]. Improving [ASK05, Dim07, EB01, KMT01, LHC08, LS01b, Mic01, SK01, SB01, Sun02, XQ07, YEP06, YG05]. incentives [Swi05].
Incident [JBR05, Tom06]. Including [SR01]. Incomputable [Vor06b].
inconsistencies [MS09a]. Incorporating [MFS09]. incorrectness [CHC04].
Increase [PBTW07]. Increasing [CS05c]. Incremental [BKY02, LKLK05].
IND-CCA [Mii01]. IND-CCA2 [BST02].
Independence [BP03b]. Independent [BS00a, BS01, Kin02, GSK09]. Index [An000b, An001d]. indexing [YPPK09].
India [CV04, JM03, MM06, MS02c, RD01, Roy00a, RM04, Roy05, An003c]. Indies [Fra01, Syv02, Wri03]. Individual [BCC02, TW07]. INDOCYPRT [CV04,
Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTLL01, Chr00, Chl01, CCMR02, CCMR05, CSY09, CGP03, Cra05a, DR02c, Des02, DKU05, DFPS06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JYZ04, Jef08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, Kil01a, Kim01, Kim02, KN03, Knu02, KP01, KNP01, Lai03, LL03, Lee04b, LST+05, LL04c, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pli01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Sch01d, Sho05a, Sil01, SM07b, Syv02, TB02, TLC06, Unio0a, VY01, Vau05a, WKP03, Wil99, Won01, Wri03. 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, QQ00, SMA05, Son00, ST01d, WK06, Ytr06]. Internet [SMP+09, ABB+04, Ben01a, Ben02, Cal00a, Chuo02, Cla00a, Coc03, DP04, DG05, EM03, Gal02, GSS03, HKW06, IF01, Jan00, Mf01, Mc03, MA00a, Mir05, PM00, PLW07, Psv01, Pho01, PHS03, Rub01, SB05, SE01, SE02, Sot01, Tsa01, TW05, Uio01, WJC05, Wri05, ZG05, Zk01]. Internet-wide [SBB05]. Interoperability [Hl00, TEM+01, BM03]. interoperable [BFGT08]. Interpolation [LW02, YG01b, FT05, KT06]. Interpolations [Sat06]. Interpretation [Mas04, CC04c]. interpretation-based [CC04c]. Intersections [KS06a, KS09b]. Interstate [RM02]. intranet [Jan00]. Intrinsic [ZW02]. introduced [Ano00a]. Introducing [JL00]. Introduction [Ben02, Ber09b, Bis03a, BK06b, Buc00b, Buc01, Buc04, CLR01, DK02, DK07, Fal07, Hay06, HPS08, HC02, KL08, MA07, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJ09, SG08, TW02, TW05, TW06b, Big08, CS07a, CM05b, Gar01, HW08, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06a, Kat05b, Rot07, Lee03a]. Intrusion [CZ05, DFK+03, DP07, JT05, TQZ05, TMM05, WG05, HLL+02, MAC+03, NCRX04, NN02, YbJ04, IR02]. Intrusion-Resilient [DFK+03, DP07, IR02]. intrusion-tolerant [YbJ04]. intrusions [Be06]. intrusive [AMB06, RFR07a, RFR07b, RFR07c]. invalid [CJ04]. Invariant [Ben00, CT09, HH09, ZLZ07]. Invariants [WH09]. Invasion [ASW+01]. invasions [Tyn05]. Invention [If00]. Inventors [Bar00c]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, MFT05]. Inversion [BNPS02, KKY02, KT07, SPG02]. Inversion/Division [KKY02]. inversive [SB05]. Investigating [AMB06, BW07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08, WD01b, WC04]. Invitation [Bar02]. Invited [FGM00a, Lan00d, DR05]. involutional [SH07]. IP [Ano00a, CD01b, FX04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSec [Vau02, CGBS01, Dav01a, KMM+06, SKW+07, FS00, FS03a, XLM06]. IPSec-Compliant [CGBS01]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFSHG09]. Irreversibility [ZWC02]. ISBN [And04, Duv03, Eao05, For04, Gum04, Imr03, Pag03, Puz04, Top02]. Island [CSY09, KGL04, Kim01, Lee04b, IEE07]. ISO [GM00b]. ISO/IEC [ISO04]. ISO9979 [TM01]. ISO9979-20 [TM01]. Isolated [LSVS09, MMT09]. Isomorphism [CY02]. Isomorphisms [CPP04]. Israel [Jol01]. ISSAC [Jef08]. issue [FOP06, FOP06].
Issues [BDF⁺01a, BH00a, Hil00, KRV01, Mea01, PBM⁺07, SEF⁺06, MKY08, Pat02b].
ISW’97 [You01]. IT-Architectures [RM02]. Italy [AAC⁺01, AL06, BCKK05, BC05c, CP03, dCdVSG05, IEE04].
Itanium [CHT02, Int00]. Itanium-based [CHT02]. Iterated [Jou04, Oni01]. Iteration [Che03]. IV [Sch01c, HSH⁺01].
IWBRS [LST⁺05]. IWDW [BCKK05, CKL05, KCR04, PK03].
J2EE [BTTF02]. Jack [Coc03]. James [Top02]. jamming [LPV⁺09]. Jan [VRY05b].
Japanese [YI00]. Java [Ano04b, Mar05a, WBL01, Ano02e, Ano03a, Ano04b, Ano04c, AJ01a, BC05b, BJvdB02, CMG⁺01, Che00, CCM05, Coo02, DPT⁺02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hum05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Vir03, Wei04, Win01, Zia00, ZFK04]. Java-Based [EM03, DPT⁺02, GW08]. Java-Lösung [Ano04b].
Job [MYC01]. jobs [Oue05]. Joel [Gum04].
Johannes [Lee03a]. John [And04, BZ02, NH03, Rot07, Coc03]. Joins [Bar00c, Con00]. Joint [AD09, ADR02, CR03, HYZ05b, HYZ05a, Puc03, M09].
Julius [Chu02]. July [ACM01a, 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, BS03, BS01b, BCDH09, BC01, Cz05, FMA02, IEE05b, IKY05, JYZ04, KGL04, KN03, KM07, PPV96, TBJ02, USE01b, USE01a, USE02c]. Just [ABB⁺04, Ano06a, Gut02a, Car01].
Kahn [Gas01]. Kaikan [Ano00d]. Kaspersky [Ano08a]. KASUMI [KYHC01, KSHY01, SM02]. Katholieke [BB09]. Katz [Bar00a]. Keccak [BDPV09]. Keep [DM07b, Ly008, FS04]. Keeping [SEK01, SEK02]. KEM [NMO05]. Kerberos [BCJ⁺06, Coc01a, Gar03b, Hil00, It00, LLW08a, MJ01, MP009, Ru00, Sm01a, Wac05, WD01a, Wit01]. Kerchhoff [KM03]. Kernel [Int00, Mor03, BK05, HB06]. Key [ANS05, ASW00, AK02a, Ano01j, Ano09b, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BPS08, BH06, BDG⁺01, BDZ04, Bar00a, BPS00, BPR00, BM00, BBDP01, BY03, BOHL⁺05, Ben02, BLM01, Bih00, BBB⁺02, BDK09, BB05b, BM03b, BDTW01, BM01, BM03c, BMP00, BCP01, BCP02a, BC02b, BM01c, MST02, CK02a, CK02b, CH03, CK05, CPP04, Che01a, CT08a, CH008, CJ03c, CCW02, CCM01, CKM00, CS02, CS03b, CS03c, DP04, DJ01, DPS05, Des00c, DB01, Des02, DG03, DIO9b, DKXY02, DFK⁺03, DGH⁺04, DBS⁺06, ESG⁺05, EP05, ES00a, FL06, FKS00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Gol03, GWH01, GC01b, GS⁺04, Gut04b, HNZ02, HCD02, HLM03, Hve01, HR05, HG03, HC08, HJV01, HS07, HLC08, IEE00b, Ina02a, Ina02b, JL08, Jou02, JG01, Jue04, Kal03]. Key [KGL04, KOY01, KY03, Kat05b, Kel05, Kel00, KK01, KM01a, KLY02, KY02, KY02c, KLC⁺00, Kl01b, KM04b, Kos01a, Kos01b, Ku02, KOM01, KY01e, Kur01]
KI03, LCK01, LLL02, LP03, LV00, Len01, Lin03, Lin00b, MPS00, Mac01, MSJ02, MHH+02, May04, MR01b, MR01c, Mü03a, Mol03b, Mü01a, Mur00, NIS03b, NA07, Ngu05, NBD01, NSS02, OTO00, Ort00, PHK+01, PR01, Poi02, PHM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sha01e, Sin01a, SVW00, SK00, Stol01, ST01c, TSO00, Tan07b, TT01, VV07, Wal03, WZW05, WH01, WC01a, Waa00, WBD01, Way02, YKMY01, Yi01, YG01c, YDKM06, Zhe02a, ZWCY02, ABHS09, AJS08, AUW01, AKNRT04, Asl04b, AFB05, BHM03, Bad07, BBN+09, Ben01a, BB79, BG08, BCG+02, BD00b, Bra01a, BCP07, BMA00a, BMA00b, BMA00c, BD04b, CCT08, CL02b].

key [CZ05, CYY05, CYH05, Che04a, CHC04, CY05, CLC08, CKRT08, CWJT01, CJ04, Cho06, CHF+09, CJL05, Cre03, DFM04, DG06, DMRT07, DW09, EKRM01, ED03, EHKH04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GMR05, GKM+00, GS01, GL06b, GMW01, HCD08a, HCD08b, Hau004, HHG06, HLLL03, HTJ08, HG05b, HW03c, HWW03, HMDLM07, HLT09, Hwa00, HLL04, IZ00, Iwa08, IM06, Jan08b, JRR09, JW06, JXW05, JZCW05, Jua04, KY00, KS05a, KOKY01, KHYM08, KM08, KG09, Kim01, KPT04, KRY05, Kob00, KWO0, Kos01c, HXKO05, HL03a, LF03, LKSY03a, LKKY03b, LCP04, LH04b, LL04a, LW04, LLL04, LL05a, LKY05b, LKY05c, LKY05d, LL06, LLS+09, LFHT07, LCK04, LPM05, LHC08, LKJL01, LSH00, Lin01a, LS01c, LCC05, Lop06, MWS08, MKKW00, MP08, Mis08, Mi01b, PS08a, PL06, Pe09, Po04, PQ06a, PQ06].

key [PC09, PSP+08, PLJ05b, Pot06, Pri00, RH03, SN000, SLP07, SRJ01, SBZ04, Sha05c, SW06, Shi05, SL05a, SW05, Shp04a, SC05b, SIR04, SLC05, Sun00b, Sun02, SZP02, SC05b, SC05c, SC05c, SY06, TP07, TO01, TNG04, Tsa06, Tsa05, Tse07, VS01, Vau05a, VK08, WDLN09, War00, WL06, WGL00, WV00, WC01b, Wa01, WL04b, WHHT08, XH05, YW05, YC09a, YC09b, YS02, YSH03, YS04, hY08, Yi04, YRY05a, YRY05b, YY05b, YPKL08, ZLG01, ZC04, ZK05, ZSM05, ZYW07, ABB+04, GL05].

Key-Based [Sha01e]. Key-Dependent [Go03, BPS08]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKXY02]. Key-Management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DKXY02]. Key-Share [CT08a]. Key-Sharing [HNZI02, WBD01]. Keyboard [ZZT05]. Keyczar [Law09b]. key [KüH08, SR00, FP02a].

Keyed-Hash [FP02a]. keying [ABB+04, Che08a, EGK08]. Keyless [Qu01]. Keys [AOS02, APV05, AFI06, BT02, BMD00, BGM05, CHM02, EM00, Fer00, HSH08a, Luc00, MN01, MRL+02, Oni01, PS00, Sm01c, Str02, TvdKB+01, BCL05a, BCW05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH08b, HSH09, HW04, HY03, HL04, KAM08, LHL04b, LL08b, LS01c, LWK05a, ML05, NN03, Sch01e, Sha04b, Sha05b, SB05, TLH05, TJS03, WH03, YRS+09]. Keystream [AMRP04, Koa02a, LV04, MH04, WLW04, PS01a]. Keystrokes [SWT07]. Keyword [FIPR05]. KC [HLC08]. KG [ZYW07]. KHAZAD [PQ03b]. KIAS [May09]. Kid [CAC06].

Kikai [An00d]. Kikai-Shinko-Kaikan [An00d]. kill [Lov01]. Killing [Lov01]. Kind [DW01]. Kind [MAaT03, MAaTXX]. King [Eag05]. Kingdom [DFCW00]. Kingston [HA00, PT06]. Kit [An02e]. Klaus [An04]. Kleptographic [YY01]. knapsack [Kos01c, SL05]. 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].
Library [KSZ02, Lau05, Law09b]. Libre [Jen09]. License [Ano00h]. Lies [Gan01b, Sch00d, Swa01, Ste05c]. Life [Cop04b, GSB+04]. Lifecycle [HL06]. Lifetime [Coc01a, CPG+04]. Lifting [CNS02]. Light [WT02]. Light-Weight [WT02]. Lightweight [EPP+07, Mal02, CHO7a, CL09, MP07]. Like [Coc02a, PSC+02, VMSV05, BCDM00, CWH00, DLP+09, Egh00, EBS01, Gou09, HSL+02, HL04, SKU+00, SLL+00]. LILI [JJ02]. LILI-128 [JJ02]. 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, Baut05, BCS02, DL07, Luk01, Shi05]. Linear [BDK02a, BDK02b, BDQ04, CGFSHG09, CS03b, CHJ02, Cou01, CM03, Cou03, CDM00, CD01a, CDG+05, FM02a, FM02b, GS03, GBM02, HLL+01, Hug02, J000d, Kan01, KMT01, Kin02, KM01c, KRS+02, KY01e, LLL+01, LS05a, NPV01, PSC+02, PG05, PZ02a, SNWX01, STK02, WF02, YSD02, BD04a, Bu09, CKL+03, Cou04, GHPT05, Kuk01, LLL04, Reg05, Reg09, RSQL03, Se00, SLL+00, TM01]. Linearization [DDG+06]. Linearly [ADD09]. Lines [SP04]. Linguistic link [LPV+09]. link-layer [LPV+09]. linkages [ZAX05]. linked [YWW09]. Linking [GW00]. Linux [Lin02, ASW+01, FR02, Fin02, Fri01, GJJ05, Gan08, GPR06, JEZ04, Lin02, Mor03, Pri00, Shu06, Sta02b, Sta05]. LISA [USE00c]. list [AGK07]. little [Lam07, Sch05c]. Live [Lov01]. Lived [GW00]. lives [FRN05]. living [BCB+05]. LLL [CKY05, NS05c]. Load [CC08, Hfof01]. Loads [GH02]. Loan [SOO02]. Loaning [Bla01c]. Local [NAGB03, Lav09]. Locality [MFS+09]. Localization [WLT05b, CKL+09]. Locally [Vad03, Yek07]. Location [HY01, KZ01, LNL+08, Buh06, SG07]. Locations [Kra02b]. Log [Gen00b, HN04]. Logarithm [CNS02, Che04b, CCW02, GV05, GPP08, LW02, Hsu05a, HL05d, JLL01, LHY05, Sch01e, SCL05, SLC05, Yas08]. Logarithmic [EGK08]. Logarithms [CS03a, JL03, LHL03a, LTH05, PLJ05a, QCB05a, Sha05c, Sha05d, SCS05c]. Logging [Fox00, MT09]. Logic [BPST02, Cop04b, KB03, KS06b, Li01, Nie02d, SQ01, SC01, Tec06, TV03, BDNN02, BD04a, DZL01, SW02, WZ05, dH08]. Logic-Based [KBD03]. Logical [Asl04b, Kra07, SP03, Zha08]. Logics [IK03, IK06]. Login [LL05c, CCK04b, CJT01]. Logistic [JJ02]. Look-up [Has00]. Looking [ASW+01, Ano01i, Cla00b]. looks [Nis03a]. Lookup [MFFT05]. loop [KVN+09]. loop-level [KVN+09]. Loopholes [Ste01]. Lorenz [GHdGSS00]. Lorenz-based [GHdGSS00]. Losing [Ano04b]. LosLobos [Pri00]. Loss [LHS05, BC05b, Mit00]. Lossy [AIP01, HSKC01, PW08, Asl04a]. Lost [PY06, Rob02, Rob09]. Lösung [Ano04b]. lot [Cla00b]. Lotteries [FPS01]. Louisiana [USE00c]. Louvain [QS00]. Louvain-la-Neuve [QS00]. Low [Ano00d, BM01b, CH07c, GST04, HNZI02, HGR07, JP02a, KKM09, RMH03b, RMH03a, SU07, SHJR04, SZ01, WC01a, CL09, CO09b, Fan03, HL03, LC04a, SK03, WHH05, WLH06, WY05, ZYW07]. low-computation [Fan03, LC04a]. low-cost [CL09]. Low-end [SU07]. Low-Exponent [SZ01]. Low-overhead
[HGR07]. Low-Power
[Ano00d, JP02a, KBM09, CO09b, ZYW07]. Low-State [GST04]. Low-Weight [CH07c].
Lower [BDF01b, BP03b, DIRR05, GT00, GKG03, PS02a, Shp03, WW05, KS05b, Shp99]. LSB [CS05c, FGD01, WMS08]. LSB-encoded [WMS08]. LSD [HGS02a]. Lu [QCB05b].
Luby [MP03, Pat03a]. LUC [LNS02].
M [DNRS03]. M8 [TM01]. MA [ACM10, JQ04, Kil05, KP01, Nao04, Pau03]. MAC [BKN04, CKM00, Ki03, LPV09, Vau01, Kra03]. MacDES [CKM00].
Machine [LBA00, Mal06, Pro00, Cas06, Kid00, Pau02b, SWR05, WNQ08, Win05b, HM01a, Pet08]. Macraigor [Ano02d]. MACs [BPR05, BR00b, BM01c, Sen00]. Made [Ste05b]. Madison [FMA02]. Maelstrom [MYC01]. Magic [DNRS03, Bur02, Hrs09].
Magyavik [dVP06]. Mail [ANR01, Cos03, KS00a, Law05, LL04b, Ns05, Alf06]. mails [LG09]. Mainframe [Web08]. mainstream [Bj05]. Maintaining [MJF07, Zho02]. Maintenance [NABG03]. Maiorana [Car02]. Majesty [Budu06]. Majority [GK007, SV08b]. Make [BP06, Ber03, Sin02]. Makes [Pau09].
Making [CSP09, Gar01, Lut03, Mit00, Oec03, Per05, Wri05]. Malaysian [Kha05]. Malicious [HLC08, SZ03, YYY04, Tsa06]. malleable [DW09, FF00, PR05]. Malware [DH07, SZ03]. Man [Gen04a]. Urb01].
Man-in-the-Middle [Gen04a]. Management [ACM03a, ACM04a, Ano02d, Ano02e, BP07, BW07, ELv01, FMA02, Gk04, Gut04b, KB06, Lin00b, Scr01, Sha02, TMM01, W000, Wya02, AW00, AIS08, AFB05, CG06, Cha05a, GTY08, ISO05, Jan00, JW06, KHY08, KM00, LMW05, LPM05, LR01, LK01, MK00, Pot06, RH03, SR01, Sen03, UP05]. manager [KH03, Sha01a]. Managing [MA00a, MA00b, NDJB01, Oue05, PTP07, PBB02, To00, BJ02, K0v03, KH03]. Mandrake [TvdKB01]. MANETs [STY07, DF07]. manipulation [SWR05]. Manuscript [GG05a, Rug04]. manuscripts [MAaTxx]. Many [BB02, Di01, MP03, Di03, SVDF07]. Many-Round [MP03]. many-to-one [SVDF07]. map [KJ01, Lee04a, PC05b, SL09]. Maple [Cos00, TT00]. mapping [Tan01]. Maps [BGLS03, BMS03, CL04a, LLL01, WP03, JK01b, MA02]. Maqasid [MAaT05]. Marcel [Ir03]. March [BDZ04, Bir07, Bla03, HR06, PY05, Sil01, Uni00g, Uni00h, Ytr06]. Marian [Kap05]. Marjan [BCC05]. Markers [FBW01]. Market [Bar00a, An01h, Swi05].
Marketplace [PLV07, VN04]. Markov [KW03]. Marks [An01c, YSS01]. Markup [Uni00a, Uni00d, Uni00e].
Marrakech [EE09a]. Marriott [USE01b, USE01a]. MARS [BFO0a, BCDM00, Fer00, IBM00, KKS00a, KKS00b, KKS01, SOTD00].
MARS-like [BCDM00]. Mary [Ree01, Sin09]. Maryland [ACM05b, ACM05c, ACM09, SMP09, GL05]. masked [AHS08, Lato08a]. Masking [CH02, CT03, GKO2, LA09].
Massachusetts [IEE05b, USE01b, USE01a, IE03]. masses [Pot06]. massively [FP00]. massively-parallel [FP00]. Match [JJ00a, WC04, LLC06]. Matching [ABM08, Len01, UBEP09, Voi05].
materialized [MSP09]. Materials [SLT01]. Math [SR06, McN03]. Mathematical [AUW01, Cas06, FF00b, GL05, HPS08].
Kat05b, You06, GKS05, Sin09].

Mathematics
[BP06, Lew00, Nie20d, Sch05a, 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
[Hüh00, HJW01].

maximizing
[GSK09].

maxims
[Bau00, Bau02a, Bau07].

Maximum
[KMT01, ZC00, DW01].

May
[ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bib03, CCOa4a, Cra05a, DRS05, IEE01b, Kau02, KNP01, MJ04, MS05a, PM00, Pf01, Pre00, TLC06, Uni005, Uni00c, YKL02a, Pau02a, YJ00].

Mbps
[LMP+01].

McClure
[Gum04].

McEliece
[CFS01, KI01a, KI01b, Loi00, LS01c, Sun00b].

McEliece-Based
[CFS01].

McEliece
[CDMP05, JLMS03].

Me
[CAC06].

mechanized
[dH08].

Media
[Hei07, CBB05, Ano02d].

media-streaming
[CBB05].

Median
[Cap01].

mediator
[SBG05], mediator-free
[SBG05].

medical
[AL07].

Medicine
[MYC01].

meet-in-the-middle
[HG07].

meeting
[Jef08].

Meets
[Way02a].

Melbourne
[IZ00].

Member
[CTH08].

Membership
[NBD01, Fis01a].

Memoir
[Bart05].

Memorable
[KOY01].

Memorandum
[DNRS03].

Memory
[AK03, AJ08, BS00b, CCM05, DK08, GN03, HNZ02, HB+JL01, KCI+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNY+05, YGZ05].

Memory-Bound
[GN03].

memory-safe
[Oiw09].

Memoryless
[Bar02].

MEMS
[ECG+07].

MEMS-Assisted
[ECG+07].

Meat
[CAC06].

Merkle
[CDMP05, JLM03].

Mersenne
[An03d].

Mesh
[LPZ06, ZTP05, KB09, LZP+04, YPSZ01].

Messages
[BG08, LB09].

Message
[BKR00, BR02, BWBL02, BDF01b, CV03, Coo2b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SN04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, MD04, MS09c, Sha04b, TJC03, Wu01, ZF05, ZAX05, ZCW04].

Messages
[Ara02, AR01, BR00b, CHJ+01b, DS05b, Sch09, Wri05, Zho06, Alv00, Ano08c, BCG02, Bib02, BB79, Lum09, MP79].

messaging
[Opp01, RR05].

meta
[SM08, PLJ05a, QCB05b, Sha05d].

Meta-He
[PLJ05a, QCB05b, Sha05d].

meta-learning
[SM08].

metadata
[CDS07, FJ04].

metamorphic
[CSW05].

Metaphor
[CBN+02].

Metering
[BCN04].

Method
[BDTW01, GHK+06, GL00, Gro01, HRS02, HQ05, JKK+01, LL02, MÖ02, OKE02, OT03a, OT03b, SOHS01, TIGD01, TSO00, WH09, WNY09, ZL05, AMRP04, DwWni05, Gut04c, JL03, MSP09, MKF06, WG02, WWT08, kWPwW01, WLI04, YC09c, YC107, CHJ01a].

Methodologies
[SM08, NdM04].

Methodology
[VMSV05, HM02a, HCBLETRG06].

Methods
[BCDM00, CFR02, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Bau00, Bau02a, Bau07, BGM04, BCHJ05, CM05b,
Modulus-Based [WY02]. Mollin [Kat05b].
MOM [DJLT01]. MONA [KMS01].
Mondriaan [BF06a]. Money [Ano01a, YKMY01].
Monitor [MK05a].
Monitored [PS05]. Monitoring [AK02a, BCS02, Por06, Bej06, GXT+08, ZGTG05].
Monitors [JT05]. Monks [Eag05, Kin01].
monoalphabetic [GPG06]. monolithic [GHdGSS00]. Monotones [WW05]. Monte [Bi09, Sug03].
Montgomery [CH07c, HKA+05, NMSK01, OS01, PS04a, TSO00, Wal01, WS03].
Montgomery-Form [OS01]. Montpellier [KM07]. Montréal [ACM02].
Morocco [IEE09a]. MorphoSys [Tan01]. MOSS [Dav01b]. Most [GG05a, Shp02, Tyn05].
Motheballed [Bar00c]. Motif [Bi09].
Motion [EFY+05, hKLS00, WMDR08]. Mountain [JYZ04]. mouse [HLwWZ09].
move [Jac00]. movement [HLwWZ09].
MP [MP07]. MP3 [DRL09]. MPEG [LHS05, MLC01, SG07, YZW07].
MPEG-4 [SG07]. MRF [Che01a]. MRM [TIGD01].
MSP430x33x [GBKP01]. MSXML [TEM+01, Hei01]. Mu [CJT03].
much [Con09]. Multi [ARR03, BBM00, BR06, CCD07, CJK+04, CDM00, CDG+05, DLY08, DJLT01, FGM001, FW004, Gen04a, HM01b, HS07, JLL02, Kur01, LVO7, LLOL4, Tsa01, ZJ09, BSSM+07, CLOS02, CC05a, CHY05a, CHY05b, DZL01, FWTC05, GMLS02, HHY07, HWH05, HC04b, HL04, LHL03b, LCZ05b, LVO5c, NC09, PW05, SC05a, Tsa08, TWL05, TYH04, YCH04].
Multi-applications [DJLT01].
Multi-Authority [JLL02]. Multi-channel [ARR03]. Multi-designated [LV07].
Multi-Domain [CJK+04]. multi-factor [BSSM+07]. multi-hop [NC09].
multi-linear [LLOL4]. Multi-party [CDM00, CDG+05, FGM001, FW004, HM01b, LLOL4, CLOS02].
Multi-property-preserving [BR06]. Multi-Proxy [ZJ09, HC04b, LVO5c, TYH04].
Multi-Receiver [CCD07]. Multi-recipient [Kur01]. multi-scroll [HHY07]. multi-secret [CC05a, CHY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server [Tsa01, LHL03b, Tsa08, TWL05].
Multi-Servers [HS07]. multi-signature [HWH05, HC04b, HL04, LCZ05b, LVO5c, TYH04].
multi-stage [CHY05b]. Multi-trapdoor [Gen04a]. Multi-user [BBM00, DLY08, GMLS02]. multi-valued [DZL01].
Multiagent [ZS05]. Multiagent-Based [ZS05]. multibit [TND+09]. Multicast [AIP01, BPS00, BDF01b, ASW00, Asl04a, CBB05, GIKR01, GL06b, JA02, KB09, MP08, PCS03, YC08, ZCW04].
Multicollisions [Jou04]. Multilevel [LN04]. Multimedia [AAK09, FMS05, GA05, HL07, LLOW07, Sun05, WLLL09, DY09a, DKU05, La00, Ren09, SG07, YC08].
Multimodal [PY08]. Multiparty [BCC02, BGOY08, CDN01, DN03, DI05, GIKR02, OZL08, PMRZ00, CDD00, HT04, IKOS07].
multipath [SK05b]. Multiple [AIK+01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, CK05, Har00, HZLS05, HL01, Jab01, STK02, SR06, TIGD01, BL06, Che04a, CJ04, DM07a, HLH00, KC09a, MN14, Sha01d, SW05, TCC02, YW05, YSH03, YRY05b]. multiple-key [Che04a, CJ04, SW05, YW05, YSH03, YRY05b].
Multiplication [BDQ04, CLK01a, CLK01b, CHSS02, Che08b, CK05, Har00, HZLS05, HL01, Jab01, STK02, SR06, TIGD01, BL06, Che04a, CJ04, DM07a, HLH00, KC09a, MN14, Sha01d, SW05, TCC02, YW05, YSH03, YRY05b].
Multiplicative [AIK+01, Ara02, BDQ04, CLK01a, CLK01b, CHSS02, Che08b, CK05, Har00, HZLS05, HL01, Jab01, STK02, SR06, TIGD01, BL06, Che04a, CJ04, DM07a, HLH00, KC09a, MN14, Sha01d, SW05, TCC02, YW05, YSH03, YRY05b].
Multiple-Precision [HZLS05, MN14].
Multiple-watermarking [Che08b]. Multiples [HR00].
Multiplication [AIK+01, ARD06, BDK01, CMJ03, CH07c, Dhe03, GLV01, HM02c, KKM01, M02, NMSK01, OS01, Tan07a, Wal01, BIP03, DwWmW05, FP00, GD05, Has00, Mis06]. Multiplications [Har06, OT03b]. Multiplicative [Has01a, KO03, MFF05]. Multiplier [HKA+05]. Multipliers
[CMJP03, KWP06, RMH03b, WS05, HGNS03, RMPJ08, RMR03a]. Multiply
[KT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver
[HSZI01]. Multiresolution [hKLS01, YTSL01]. Multiset [aSM01]. Multisignature
[Ta02, WH02b]. Multithreaded [Zha01]. Multivariable [DS05a]. Multivariate
[DY09b, BGP09, FP09]. Municipal [MJF08]. Music [MNS01, XMST07]. mutargima
[MAaT05]. Mutation [Lut02]. Mutual [JP02a, KH05, CCS08, SW06, VK01, YWW02b]. Mutually
[WC01a]. MYCRYPT [DV05]. mysterious [Bel07a]. Mystery [GG05a, Rug5]. Myths [GO03, kc01].

N [Mar05a, AOS02, KOMM01]. NAF [OT03b]. Names [Coc01a, Sho01, Ark05, CGV09]. Naming
[Ano01b, BH00b]. Nanotechnology [RR03a, RR03b]. Naor [Zha06]. Napoleon
[Urb01]. narrowed [Sch04d]. narrowing [MT07]. NASA [Ano02c, W199]. Nation
[Ano04a]. National
[BWE07, J01, LCS09, AJ08, Bau02]. National-Scale [BWE07]. Natural
[ARC+01, Top02, WMS08]. Nature [Pag03]. Naval [LBA00, Goo00]. Nazi
[Hau06, KS04]. NC [AIK04]. nCipher
[Ano03e]. NCP [SG01]. NCR [LBA00]. Near [BC04a, DS05]. Near-Collisions
[BC04a]. Necessary [LKC03, MN01]. Necessity [SBZ02]. Nederlanden [dLO0]. Need
[Coc01a, HR04b, StO4]. Needs
[CZB+01, DDK07]. Negotiation
[DBS06, HHS04, IY05, LLW05, LLW09]. Nema [Kid00]. NESSIE [Pre01, Mac00, Pre02a, Pre02b, SGB01, DPVR00]. nested
[LCK04]. Net [CAC03, Ano08b, LKJL01]. Netherlands [Koo02]. NetHost [AMB06].

NetHost-Sensor [AMB06]. Nets
[AADK05]. Netspionage [BK00]. Network
[Ano02d, Ano03b, Bar03, BGOY08, Con04, CL02, Din07, FBWC02, Gum04, Har05a, IY05, JY04, KSG03, KPS02, Ken02b, LMP+01, Lu07, Mal02, NN02, PZDH09, PZL09, Poo03, RCBL00, RC05, Sty04, TLYL04, VMC02, YC01, ZYH03, ZS05, Bru06, CJ03b, CMS08, Coc01a, DWML05, GKS05, HLL+02, LC03, LP+09, MW06, ME08a, MS03, MS08, Pri00, RAL07, Sch02c, Sta02a, TIS07, Vac06, Wy05, YLT06, ECOM0a, ECOM0b].

Network-Attached [RCBL00]. network-based [HLL+02]. Networked
[Sch00d, LB05]. Networking
[ACM01b, Ros07, VM03]. Networks
[AEAQ05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKR01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RZKD02, Sin01a, WT02, Zea00, ZYH03, ZWC02, AJ08, Asl04a, BBG+02, BC05c, CMT09, CGP03, CBD+05, DHMR07, ETM05, HJ07, HMDL07, JRR09, KTT09, KHY05, KB09, KVD07, LDH06, LHC08, LW05a, LLH06, Lin07, LN04, Lop06, LKZ+04, MWS08, MJF+08, MS09b, NC09, NLD08, PC07, PS08a, Pat02b, SL07, SSM+08, TP07, TM06, TCR03, TW07, WDL09, XWWL08, YCO7, ZJSN07, ZBLvB05, Ano02d, CS08b].

Neural [KMS02, PZL09, PR01, YC01, YC07].
Neural-Network [YC01]. Neuve [Q500].
Nevada [ELvS01, IEE01a]. Never
[Wei00, Hau06]. Newfoundland [NH03]. Newman [Pag03]. Newmanry [Sal01a].
News [Ano03c, 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, ML06, TV03, Van03, Web08, BD04b, ISTE08, R03a].
Next-Generation [ESG+05, Web08]. NFA
BG08, BG09, BG07a, BGL, CNPQ03, CO09b, DIM08, DGP09, FP00, HG05a, HGNS03, HLwWZ09, HP01, JAW00, JL03, KH08, KSF00, Lam01, Mit00, Nie02a, Nie04, Pan07, PSG09, PSP08, PC00, RGX06, Sho05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Wagn03, Was08b, YZEE09.

Number-Notation [Eag05, Kin01].

Number-theoretic [NR04]. Numbers [HSR01, HBF09, Ifr00, MN01, ST03b, AG09, HW08, KB39, Kir01b, MFK06, SS03, Shp05, Tip27]. numeric [AKSX04].

Numerical [WWL02]. numerically [Sav04]. Numerous [CC08]. NURBS [Ben00].

NUSH [WF02]. NY [HR06, IKY05, KJR05, Sch01d, YDKM06, NIS00]. Nyberg [Ara02].

O [Kat05b, Puc03]. OAEP [Man01, BF05, BF06b, Bon01, FOPS01, Sho01].

Obfuscated [NS05b]. Obfuscating [BGI01]. obfuscation [CT02]. Object [RSA00e, DHL06, MWM01, ST06]. object-oriented [DHL06, MWM01].

Objects [CCM05, ZTP05, PBO1, Whi09].

Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GKM00, KKL09]. obscurity [MN03]. Observability [JQY01].

observers [JL04]. Obstacles [KM04a]. Obtaining [Bar06b, BP03b]. OCB [RB03]. occur [Web02]. Ocean [MYC01].

October [AJ08, BD08, CKL05, IE00a, IE00e, IE00f, IE00g, IE02, IE07, IE02, IE07, IE09b, KCR04, LST05, TTZ01, USE00b, ZHY03].

Octopus [Clc00b]. Oded [Lee03b]. odyssey [Gold98].

Oedipus [Lav06]. Off [AJ08, Coc02b, Oco03, Shi05, YLL02, Bau05].

Off-Line [YLL02, Shi05, Bau05]. Offering [YC08]. Office [Uni01]. officer [Kov03].

Official [BP01b, Coc02b]. Offline [DJ06, ST01b, WV01]. Offs [PS01c]. OH [BD08]. oil [RD09]. old [Lav01].

On-Demand [SEF06]. On-Line [Lu02, BCS02, Luk01]. One [AK02a, BYJK08, CHL02, Che03, DIS02, Di01, DW01, DMS00, Fis01b, GKK09, HNO09, HM02b, HR05, KIO1a, KO03, KO00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, DI03, DS02, GKK07, HR07, HRS08, HLT09, JZ09, KK07, KKK05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, Tsa08, YW05, YRY05b, ZW05a].

One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLT09, LC04a]. one-variable [SV08a].

One-Way [BYJK08, CHL02, DMS00, Fis01b, GKK09, HNO09, HR05, KO03, KO00, LTW05, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, DI03, DS02, GKK07, HR07, HRS08, JZ09, KK07, KKK05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, Tsa08, YW05, YRY05b, ZW05a].

One-Wayness [KI01a, PV06b]. Ongoing [Sami09]. Onion [CL05]. Online [BDF01a, BBKN01, Fis05, LSC09, ort00, Rey01, ST01b, VAVY09, Voit05, FNRC05, Fox00, Pan07, Tyn05, PT08].

Online/Offline [ST01b]. Only [BBK03a, CF01b, GL01, Hoe01, VV07, BCDM00, FKS00, GHJ0V0, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Vas08].

Ontario [HA00, ST01d, YV01]. OOSCD [CZB01].

OOSD [CZB01]. Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Kius02, Lin02, Mea01, PM00, VDFP05, An03c, ETM05, MAC08, Bar00b, Lin02].

Open-Ended [Kius02]. Open-Secret [Joh05]. Open-Source [Bol02, Gut00, MAC08].

OpenCard [HF00].

Opening [CAC03]. OpenSSH [Bau01c, Sta02b, TvdKB01, Hos06a, Mos06].

OpenSSL [Fri01, Res01a, Res01b, Sti06a].
VMC02, YRS+09, Bel08. Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL+08a, CGL+08b, CGL+08c, DGP09. KWD06, MPH06, SET08, TKP+08]. Operation [BR02, BKM07, Dwo03, EP02, Gol01e, HSH+01, JKR01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BK07]. Operational [BR02, BKM07, Dwo03, EP02, Gol01e, HSH+01, JKR01, KY01a, Bud00b, RBB03, Win00]. Operations [BIP05, IMM01, KDO01, KS05c, LS01b, Ark05, Dug04]. Operator [Wan05]. Operators [CH00]. Opinion [BHM03, GS07b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Pau02b]. Optimized [LC03]. Optimising [Dw04]. Optimistic [CC00, DLY08]. Optimization [Ken02a, Kre05, KV01, SMTM01, TLY04, WPP05]. Optimised [TL07]. Optimisation [CC00, DLY08]. Optimisation [Ken02a, Kre05, KV01, SMTM01, TLY04, WPP05]. Optimised [LC03]. Optimizing [Dw04]. Optimum [KWP06, OKS06]. Options [Fri07, Pot03]. Options [Han00]. Oracle [ABR01, Abe01, Abe04, BF05, Chi08e, Gra02b, Nie02b, Pas03, Ano02c]. Oracles [BNPS02, BB04, KG09, RG09]. Order [AKS04, Bai01a, CV02, KCP01, KJ+01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Col03]. Order-Specified [Tad02]. Ordered [HY03, WL05]. Ordering [Mea04]. Orders [HJW01, PS02b, HM00, Hüh00]. Ore [CHH01]. Oregon [ACM00, BCDH09]. Organization [JG07, MMZ00, MP00, C+02]. Organizational [PTP07, BJ02]. organized [AUW01]. Oriented [HR00, LZZ+01, SKU+00, ZCC01, CHC05, CWJT01, DHL06, HWW04, LL06, LWZH05, MWM01, Sae02, Sha03c, TJO01a, WHHT08]. Origin [MABI06, MD04]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Orsay [DPT+02]. OS- [CRSP09]. oscillator [BGL+03, GB09]. oscillator-based [BGL+03]. oscillators [SPG02]. OSNP [HLTJ09]. Other [BF05, Ngu05, Wri05, Cla00b]. Otherworldly [MYC01]. Ottawa [AMW07, MZ04]. our [Sta05]. ourselves [Fur05]. Output [Dic03, YJ00]. Outsource [HL05a]. outsourced [MNT06, YPPK09, YLC+09]. overcomes [HC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, Ino05]. overhead [HR07, IKOS08, RSP05]. overheads [XLMS06]. Overlay [SL05b, YC08]. overlays [SK05b]. Overshadow [CGL+08a, CGL+08b, CGL+08c]. overview [SVEG09]. Ownership [AS01b, Nik02a, Nik02b, CL08, Lin01b]. P [Puc03, AKS02, KR03]. P1363 [IEE00b]. P2P [BRMT09, ST07, WN02, YLR05]. P2Ps [LHL+08]. PA [Cor00a, WW00]. PA-RISC [Cor00a, WW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. Pad [LDM04, DS02]. Padding [AR01, BCCN01, CKN00, CJNP02, KO03, LS01a, Man01, Van02]. Paddings [NP02b]. PadLock [Lud05]. PadLock-wicked [Lud05]. Page [IEE00b]. PageRank [GPC08]. pages [Fal07, Rot07]. paging [SZ08]. Paillier [CGHG01, DJ01, NSNK05, ST02]. Pair [WC09]. Pairing [BKLS02, BF01b, BF03, CHSS02, GPS06, HCD08a, HCD08b, KM05, Kir03, PV06a, SKG09, Sm03a, GPS05, Lee04a, PC05b, VAY09]. Pairing-Based [BKLS02, GPS06, KM05, PV06a, HCD08a, HCD08b, GPS05]. Pairings [Bon07, BG07, Jot02, SB04, ZK02, CJL05, DSGP06, LWZH05, LC05b, SW05, VK08].
pairs [LYGL07, Slp01]. Pairwise [CLLL00, FM02a, HMvdLM07]. PAKE [HTJ08]. Palm [BDhKB09, WPS01, Wil99, Ano02d]. Palmprint [KZ09]. PAM [FR02, Sei00b]. Panama [BDPV09]. Panel [FL01b]. Panopticon [YN01]. Paper [CC09, MFS+09, Pet08]. Papers [Ano04a, Ano07b, Ano07a, Sch00b, Ytr06, Wil99, Bla03, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PK03, PT06, RM04, Sio01, AJo01a, Bir07, BC05c, CJ05, CKL05, DAM07, DM00b, JL08, KY02c, MFS+09, PS04a, RMH03, SS01a, BF06a, FP00, OS07, RMPJ08]. parallelism [KVN+09]. Parallelizable [BR02, Mio02]. parallelizing [Fis01a]. Paradigm [BN00a, CS02, GO03, KD04, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Paradox [Che01b]. Paradoxes [Des00b, Swa01, Hro05]. parallelism [KVN+09]. Parallelizable [BR02, Mio02]. parallelizing [Fis01a]. Paradigm [BN00a, CS02, GO03, KD04, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Paradox [Che01b]. Paradigms [Des00b, Swa01, Hro05]. parallelism [KVN+09]. Parallelizable [BR02, Mio02]. parallelizing [Fis01a]. Paradigm [BN00a, CS02, GO03, KD04, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Parallel-Based [CPhX04, CTLL01, CNP03, CNPQ03, MS05a, PS04a, RMH03, SS01a, BF06a, FP00, OS07, RMPJ08]. parameterization [LZP+04]. Parameters [ZL02]. Parametric [Vir03]. Paradox [ETZ00]. Parents [Pau02a]. Parents-to-Be [Pau02a]. Paris [ACM04a, GH05, KNP01, NP02a]. Parity [DR09, KKG03, YO11, BKW03]. Parity-Based [KKG03, DR09]. Park [COp05, COp06, HS01a, Sal00b, Sal05a, SE01, Smi01b, WE06, Win00]. Part [Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bao01a, Bao01b, Bao01c, Bao03b, Res01a, Res01b, Wac05]. Partial [BM03b, Cor02, Her06, ABHS09, CP07]. Partial-Domain [Cor02]. Partially [AO00, MS09, Bao04, Fan03, HCO04, HY03, HLL03, WL05, WLLH05, WY05, ZC05]. Participatory [CTBA+01]. parties [LKY05b]. Partition [CTH08, WJP07]. Partitioned [DN04]. partitioning [BF06a, Che07]. partitions [Sav04]. Party [KO04, Lin01c, MR01a, WW05, WV01, CLOS02, CLC08, CDM00, CDG+05, FGMO01, FW04, GCKL08, HM01b, JW01, LHL04b, LL04, LLS+09, LSH00, YC09a, ZLX99]. Pass [SK00, MT02]. passe [Car00]. Passes [Coc03]. Passing [Vir03]. Passive [Sha01c, VV07, RW07]. Passive-Only [VV07]. Password [BMN01, BMP00, CHVV03, CPP04, CS07b, CC01b, DG03, GL03, GMR05, Har01a, Har01b, Jak01, KOY01, LSH03a, LSH03b, MS00, Mac01, MS02, Ngu05, SBEW01, SY06, WHL05, YS04, ZWCY02, CC01a, CC04b, CCK04b, CHY05, DG06, FLZ02, F06, GL06a, HTJ08, JM07, JPL04, Jua04, KLY03, KJY05, KTC03, KLC03, Ku04, KCO05, KHKL05, LLH06, LFW04, LHO3, LC04a, Pha06, Sco04, SLH03, Shin05, WLT03, XW0L08, YW04a, YW05, YS02, YPKL08, ZDW06]. Password-Authenticated [BMP00, DG03, KOY01, MPS00, Mac01, MS02, Ngu05, DG06, HTJ08]. Password-Based [CPP04, CS07b, GL03, SBEW01, SY06, YS04, GL06a, KHKL05, Pha06, ZDW06]. password-guessing [Shi05]. Passwords [GL01, KOY01, Per03, Smi01c, Ano03c, FZ06, KOY09, NS05a, RD09, YWW08, vOT08]. Patarin [Bih00]. Patent [MP00]. Path [GXT+08, CCD+04, Dew08, ZSN05]. path-based [CCD+04]. Path-quality [GXT+08]. Pattern [ABM08, DHK09, BLP06, BCC01, LS01a, TIGD01, Buh06, LYGL07]. Pattern-based [BLP06]. Patterns [DD02, MP06, WC09, JLC07]. Pavol [Sal03b]. pay [Joy03a]. pay-as-you-watch
placement [GJ05, JEZ04]. Plain [Col03].
Plaintext [DN02a, Fur02b, GK05, HLM03, Jol01, Ke02, KM01c, Ki01a, MF01, CK06].
Plaintexts [BR00a, Plan [CAC06, CP02, Gan08]. plane [WL02].
Planning [WCZ05]. plans [Ark05].
Platform [Bau02b, MM02, PZDH09, AR08, ISTE08].
Platforms [AIK01]. Play [WD01a].
Playing [Sho05, BR04]. Please [Per03].
Pluggable [Sei00b]. plus [Cop04b]. PODS [ACM03c, ACM05b]. poetry [MA06].
pogromca [Kap05]. Point [GL01, M60, NS05c, USE00b, WW06].
point-sampled [WW06]. Points [BG08, Ga02, Cha00b]. poised [CH00].
Poisoning [Kle07]. Poland [AUW01, Bih03]. Polarization [HR05].
Poles [KS04]. Policies [AEV07, ZP05, BN08, LJY04, RN00a, RN00b]. Policy [Bla01c, HQ05, AN00e, BFG08, BZP05, DFM04, Gor05, RV09, Uni00b, RR04].
policy-based [BFG08]. policy-compliant [RV09]. Polish [Kap05]. Politics [Cho08a, DL98, Jan08a, DL07].
polyalphabetic [GP06]. Polygonal [Ben00, BB00a, BGI08, SP04].
polyomorphic [CSW05]. Polynomial [AF03, BIP05, BDG+01, Bul09, CU01, CJ03a, CH07e, CLZ02, DS05a, Gon06, HR00, KL05, KY01c, KTT07, LW02, May04, Pli01, RM03b, Sat06, LFW04, MRST06, SZP02].
Polynomial-Time [CLZ02, KL05, Pli01, MRST06].
Polynomials [BLST01, DS08, FL06, Jan00, JD00, Lan04a, CHH01, FP09, GS09]. Pon [QCB05b]. Pool [BTTF02]. Popular [RR08, CAC06]. Port [Kra02b]. Portable [Hei07, Wan04a]. Portfolio [An02e].
Portland [ACM00, BCD09]. Possessing [CC08]. Possession [Te06]. Possibility [SF07, BGI01, DOPS04]. Possible [Mor01]. Post [BB09, BLRS09, Ber09b, HHG06, BB09, BD08]. Post-Quantum [BB09, BLRS09, Ber09b, HHG06, BD08, BB09].
postage [Ble07]. Poster [Tso00, RN00b]. Potential [Kid02]. Potentially [Wai01].
POTSHARDS [SGVM09]. Power [AKS06, An00d, Ava03, BI05b, BNPS02, Cary00, DP01, DBS06, Gir06, Has01b, HM02c, HBF09, IIT03, JP02a, JQ01, KBF09, KLY02, MOP06, Mas04, MS01, MMST09, Mes00, Mes01, MG08, OS00, OS06, OOP03, PS0+09, Sha01c, Sma03b, WS05, WC01a, vW01, CBSU06, CO09b, Geb04, Mit02, OS08, WH06, XH05, ZY07].
Power-Analysis [OOP03]. power-attacks [Geb04]. power-aware [CBSU06].
Power-Sum [KL02]. Power-Up [HB09]. Pr [Eag05, Pag03, Top02]. PPC [ASW+01].
PPK [YDKM06]. pq [KOMM01].
PQCrypto [BD08]. Practical [An01c, AR01, Ash03, ACJT00, BD+09, BF05, BLMS00, CS03a, Cap01, CDR01, CJT02, Chi08a, Chi08b, Ch08c, Chi08d, CS03b, DK01, Dre00, FS03b, GSS03, GIS05, GH02, HR01, JH01, Ina02a, Ina02b, IIT03, Kan01, LM05, LCD07, Lut03, LW05a, MM02, MS05, OM09, PBB00, Pel06, Poo03, Roy00b, Sug01, Wei04, YSS01, Bro05b, DKL00a, Har05a, KSW06, Luc06, Mos06, MV04, Sha01a].
Practice [AL06, BDZ04, Des02, IZ00, Kim01, Ma04, 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 [HLS05, SR06, LMC+03, MN14].
Precomputation [SLG+05].
predecryption [RSP05]. Predict [Dic03].
predictable [Bel08]. Predicting [AG09, BGP05]. Prediction [AK06, SLG+05]. predictable [vOT08].
predistribution
LCK01, Mea01, MSU05, NS01b, Rub00, RMCG01, SK00, Tan07b, TZT09a, TZT09b, WHL05, YSR01, Asl04b, BP03a, BC05b, Bla01b, BDFP05, BK05, CS04, CCK04a, CC04b, CYY05, CC05c, CYH05, Che04a, CLC08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, GTZ04, HTJ08, HWWM03, HLTJ09, HHC05, KH08, KKL09, KTC03, LC03, LF03, LKKY03a, LKKY03b, LW04, LHL04a, LKY05b, LKY05c, LHC08, LSH03a, LC05b, Luk01, MS03a, Par04, Pau01, RG06, Shi05, SW05, SIR04, TM06, Tsa06, Tse07, WK05, WLT05a, WHHT08, YW05, YWL05, YTWY05, YC09a, YS02, YSH03, YRY05b, YRY05c, YPKL08, ZWWL01, ZL04c, ZDW06, ZYW07, LSH03b].

Protocols [AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Bor01, BMN01, BM03c, Bra01b, BLDT09, CKPS01, CT08a, CCMR02, CCMR05, Cir01, CNV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, JP07, JW05, KS00a, KY03, KL08, Kra03, Kius02, MS02a, MNP01, PBD00, PR08, PZDH09, Rot01, Shy02, SC01, Tee06, AA04b, AKNRT04, Bar06a, Ban05, Bel07b, BSV08, BFGT08, BP05, BL06, BD04a, BR05, Can01a, Can06a, CP07, CKRT08, CWJT01, CH07a, Cho08b, Chr00, Chr01, CMM00, CC05d, CDL06, DFG00, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV+09, LLL04, LLY06, LLS+09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SL05a, SR00, SW00b, SY06, YS04, ZLX99, ZL04b, PDMS09, Puc03].

ProtoMon [JT05]. Provability [GOR02b]. Provably [AO00, ACM02, BMP00, BC01, BC07, CHK08, DG03, DG06, HL:AV02, Hval09, HL07, HS07, JMV02, Ml03a, NS005, NS002, VMV05, WHL06, X030, ZCL05, BKN04, CCM09]. provenance [HSW09]. Provers [MV03a]. Provide [MN01, Sch01a]. Providence [IEE07, Sil01]. Provider [LDM04, HIL02]. providers [MV03b]. Provides [DT03b]. Providing [BACS02, BS+09a, Del07, Lin07, Par04]. Proving [Che03, FS01c, GN01, Tee06]. Provision [Kha05]. Proxy [AH05, BCL05a, DKFX05, LCK03, LC05b, PL01, Rs001, Sh03d, ZJ09, AFH06, CCH04, DYY09a, HWW03, HW04, HWW05, HW05, HC04b, KHL09, LL05b, LH05, LC05c, LW05c, PKH05, Sha05b, SHT05, TYH04, YTH04, ZCL05]. proxy-enabled [DY09a]. proxy-protected [PKH05, ZCL05]. psBGP [vOWK07].

Pseudo [BH05, FWW04, Gen00b, LLL*01, LHL+08, MP03, SXY01, TST09a, TST09b, WP03, BG09, GB09, MFK+06, NR04, PSP+08, RGX06, SL09, WW08, YZEE09].

Pseudo-Random [LLL+01, MP03, WP03, Gen00b, SXY01, MFK+06, NR04, RGX06, SL09, WW08].

Pseudo-Ransom [BH05].

Pseudo-signatures [FWW04]. pseudonoise [HG05a]. pseudonym [CG06]. pseudoprimes [ZT03]. Pseudorandom [CD05, DN02a, DI05, FP02, Fin06, Fhu02b, FP05, GM02a, IYK02, LMHCETR06, Nie02c, RSN+01, Aam03, BGPG05, IYK03, KSF00].

Pseudorandomness [GM02c, IK00, IK01, KYHC01, LHL01, Lee03b, MV00, Sh03p, G099]. Psychology [MYC01]. PUB [Nat00]. Public [ANS05, AUW01, APV05, Ano01j, AEAQ05, AF03, BC05a, BDG+01, BDZ04, Bar00c, BPS00, BM00, BB01, BL01, Bih00, BDTW01, BST02, CHK03, CHK05, CD0+05, CHM+02, CHK08, CJ03c, Chi08a, CCW02, CT09, CCM01, CS02, CS03b, DPV04, DJ01, Des02, DY09b, DKXY02, DF+03, ESG+05, ES00a, ED03, FL06, FLP01b, GMLS02, GH01, GC01b, GSB+04, Gut04b, HCD002, HR05, HG05b, HHR04b, HJW01, HLC08, IEE00b, IZ00, Jou02, Kat05b, KKM01, KM01a, Kim01, KLY02, KKY02,
KY02c, KLC+00, Kl01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Möl03a, Mol03b, Müi01a, NP02a, NBDO1, NSS02, OTU00, PHK+00, Pei09, PR01, PHM03, Qu01, RSA0a, RKZD02, ST01a, ST02, Sini01a, Sini01c, Ste01, TSO00, TT01, Vau05a].

Public
[WZW05, WHI01, WV00, Wya02, YKMY01, YG01c, YDKM06, Zhe02a, AG09, BHM03, BCL05a, BCW05, BBN+09, Ben01a, BB79, Bra01a, BD04b, Cal00b, CCT08, CL02b, CWH00, CCH05, CJ05, CKRT08, Cho06, Cre00, DMT07, EKRMA01, EHKH04, FMY02, FP00, Gal02, GH08, GKM+00, GS01, Gor05, GMW01, HCD08a, HCD08b, HHG06, HW04, HL04, Iwa08, IM06, Jan08b, JXW05, JZCW05, Kos01c, LF03, Lin01a, LS01c, Lop06, LWK05a, MWS08, Müi01b, PI06, PC09, SN100, SRJ01, Sha04b, Sha05b, Shp04a, SLC05, Sm00b, SZP02, SC05c, TOO1, TLH05, Tsa05, TJC03, VS01, WDLN09, War00, Wu01, WH03, WL04b, Hy08, YRS+09, ZM05, AL06, BDZ04, Ben02, CZ05, Des02, GL05, KGL04, Kim01, NP02a, Van05a, YDKM06].

Public-Key
[Ano01j, AEAQ05, BC05a, BBM00, BBPD01, BLMO1, BST02, CH03, CHK05, CCM01, CS02, CS03b, DPV04, DJ01, DFK+03, ESG+05, ES00a, FL06, GH01, GC01b, HR05, IEE00b, Kat05b, KK01a, KLY02, KKY02, KLC+00, Kl01b, KMO4b, Kos01a, Kos01b, KY01e, Kur01, LP03, Lin03, Lin00b, MR01b, MR01c, Möl03a, Mol03b, Müi01a, NP02a, NBDO1, NSS02, OTU00, Po02, RASA0a, ST01a, ST02, SN100, TSO00, TT01, WHI01, YDKM06, AUW01, ED03, HG05b, Pei09, BM03, BN+09, BD04b, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HHG06, Iwa08, Jan08b, JXW05, JZCW05, Kos01c, LF03, Lin01a, LS01c, Lop06, MWS08, Müi01b, SN100, Shp04a, SLC05, Sm00b, TO01, ZSM05, GL05].

Public-Key-Based [YKMY01].
Publication [Top02, DGMS03].
Publications [Bee05].
Public-Key [Ano01j, AEAQ05, BC05a, BBM00, BBDP01, BLM01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DPV04, DJ01, DFK+03, ESG+05, ES00a, FL06, GH01, GC01b, HR05, IEE00b, Kat05b, KK01a, KLY02, KKY02, KLC+00, Kl01b, KMO4b, Kos01a, Kos01b, KY01e, Kur01, LP03, Lin03, Lin00b, MR01b, MR01c, Möl03a, Mol03b, Müi01a, NP02a, NBDO1, NSS02, OTU00, Po02, RASA0a, ST01a, ST02, SN100, TSO00, TT01, WHI01, YDKM06, AUW01, ED03, HG05b, Pei09, BM03, BN+09, BD04b, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HHG06, Iwa08, Jan08b, JXW05, JZCW05, Kos01c, LF03, Lin01a, LS01c, Lop06, MWS08, Müi01b, SN100, Shp04a, SLC05, Sm00b, TO01, ZSM05, GL05].

Public-Key-Based [YKMY01].
Publication [Top02, DGMS03].
Publications [Bee05].
publique [RSA09a].
publish [SL05b].
publish-subscribe [SL05b].
Published [LS05a, FSGV01, PBV08].
Push [Pau03].
puzzle [LF03].

Q [BFMR02, CH01b].
Q&A [Str01b, Win01].
QCQC [Wils99].

QCQS [Wils99].

QDSL [CUS08].
QNX [Ano02d].
QoS [JRW01, Zea00].
QoS-aware [Zea00].

QSIG [ECM00b].
QSIG-WTMAU [ECM00b].

Q'tron [YC07].
QUAD [BGP09].

Quadratic
[BT02, Coc01b, HJW01, SP05, CCS08, HM00, Hüh00, HP01, LD01].
Quality
[BW07, TL07, DMS09, GXT+08, KCO9a, WWTH08].
quality-conscious [DMS09].

Quantifier [KS06b].
Quantifier-free [KS06b].

Quantitative [Bai08, ME08a].
Quantization [DRL09, WC04, WC05].

Quantum
[AC02, ATSV00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL+05, BBD09, BZ02, BBB+02, BBM00, BEM+07, Coc03, DFS04, DPP05, DFS08, DMS00, Ell04, Ett02, GKK+09, GH02, GW00, GRTZ02, HV09, Hay06, Imr03, Ina02a, Ina02b, Kak06, KK06, KLB+02, LB04, LW05b, NA07, OTU00, PC09, Rec01, RK05, Ser06, SR07, TOO1, Wil99, Wri00, YI00, YI01, ZLG01, ABW09, Ano03c, Ano06d, BYJK04, BCG+02, Ber09b, BEZ00, BEZ01, BLRS09, DFS05, Duw03, Eke02, GKK+07, Gay08, HHG06, IM06, JZ09, JRS09, JAW+00, Joy00, KK07, KH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Sin99, Sin00, Sm04, UHA+09, BZ02, BD08, BBD09].
quantum-storage [DFSS05]. quarter [Kob00]. quarter-century [Kob00]. quarters [Cla00b]. QUARTZ [PCG01]. Quasi [MD05]. Quasi-Pipelined [MD05]. Quasigroup [MSNH07]. Québec [ACM02]. Queen [Rec01, Sin99]. Queenstown [Zhe02b]. queries [CKK03, Fis01a, GPC08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC\textsuperscript{+}09]. Query-preserving [GA03]. querying [FJ04, ÚG08]. question [OC03]. Questions [Ett02, Joh00, Jac00]. Queues [WWL\textsuperscript{+}02]. queuing [CUS08]. quick [Dew08]. R [Kat05b, Pag03, Spr03, Bih00]. R&D [Mau05]. Rabbit [BVP\textsuperscript{+}04]. Rabin [Bon01, Gen04b, Miy01]. Rackoff [MP03, Pat03a]. radar [GG05b]. Radiations [SGM09]. radical [Web02]. Radio [Sak01]. RadioGatún [BDPV09]. Radix [HKA\textsuperscript{+}05, JY01]. Radix- [HKA\textsuperscript{+}05, JY01]. rails [Fox00]. Rainbow [DS05a]. Raises [MP00]. Raising [Cos03]. ramp [Y06]. Rampaging [Coc02b]. Random [Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CTY09, Chi08e, Dio03, DGP07a, DGP07b, DV08, EHK\textsuperscript{+}03, Gra02b, GPR06, HSR\textsuperscript{+}01, HB09, Int03, JRR09, Ke05, LLL\textsuperscript{+}01, LM02, Lys02, MP03, Mir02, NNT05, Nie02b, Pas03, Pat04, Ran55, Ran01, RSN\textsuperscript{+}01, SDFD06, TWNA08, TL07, Tip27, TZT09a, TZT09b, Vav03, VKS09, WP03, BK07, Bel08, BG08, BG09, BG07a, BGL\textsuperscript{+}03, CJL06, CO09b, DGP09, Fis01a, GVC\textsuperscript{+}08, Gen00b, GB09, HG05a, HLwWZ09, HMvdLM07, JAW\textsuperscript{+}00, KH08, KB39, KG09, MI09, MKF\textsuperscript{+}06, NR04, Pan07, PSS\textsuperscript{+}09, PSP\textsuperscript{+}08, PC00, Reg05, Reg09, RG09, RGX06, SS03, SXY01, SR07, SK01b, Sug03, SL09, UHA\textsuperscript{+}09, WW08, YZEE09, BH05]. Random-Error [LM02]. random-self-reductions [Fis01a]. Randomats [Sam01]. randomization [WHH05]. randomization-enhanced [WHH05]. Randomized [Sem00, Hro05]. Randomness [DD00, DDO4, DGH\textsuperscript{+}04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN\textsuperscript{+}09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03]. Range [CW09]. Rank [Sun00a, DW01, Sim02]. Ransom [BH05]. Rao [ZHR01]. rapid [OP01b]. Rate [KT01, LZ09, PS02a, Sun02]. Rates [GH02]. Ratio [Di 01]. Rational [HT04]. ratios [Zir07]. raw [CO09a]. RBAC [LSZ05, SN04, ZP05]. RBAC-Based [LSZ05]. RC4 [FMS01, Mir02, VV07]. RC6 [GHJV00, GHJV01, IK00, IK01, KM00, KM01b, RRY00, STK02]. RCES [LLCL08]. RCES/RSES [LLCL08]. re [AH05, AFGH06, KHL09]. re-encryption [AFGH06, KHL09]. re-signatures [AH05]. Reachability [AL00a, MT07]. REACT [OP01b]. Reactive [Shy02]. Real [BSW01, Dri02, GSB\textsuperscript{+}04, JBR05, SP05, Sta05, YKMB08, GM04, HP01, Lie05, SL07, SGPH98, YZDW07]. Real-Time [Dri02, GM04, YZDW07]. Reality [Coc01a]. Really [CZB\textsuperscript{+}01, Wei00, Dav01c]. reap [CH00]. reason [Lau08b]. reasoning [IK03, IK06]. Rebalanced [SWH\textsuperscript{+}09]. Rebalanced-RSA [SWH\textsuperscript{+}09]. rebels [Lev01]. Rebuild [Salxx]. Rebuilding [Sal05a]. Receipt [HS00]. Receipt-Free [HS00]. Receipts [Cha04]. Receive [Coc03]. Receiver [CCD07]. Receivers [NNL01, SBB05]. recency [SW02]. recently [JK01a]. Reception [Top02]. Recipes [VM03]. Recipient [ANR01, Kur01]. Recipients [Coc01a]. recoding [SSST06]. Recognition [Ano02d, LLT\textsuperscript{+}04, LST\textsuperscript{+}05, TZT09b, HS02b, LI05, MMJP03]. Recommendation [Bar06b, BK06a, BK07, Dwo03, NIS03b]. Recommended [Kel05]. Reconciling [BNPW03, PG07]. Reconfigurable [FD01, FZH05, GC01b, KBD03, LZ04].
reputation-systems [KNS05]. Request [RSA00b]. require [SV08b]. Required [Sun00a, Lov01, Wan05]. Requirements [FIP01b, HWH01, Kin02, NIS01b, Mea04].

Rescue [ASW001]. Research [Pip03]. Research [AJ01b, CZ05, CZK05, DFPS06, KGL04, LXM+05, RC06, Sch00e, TMMM05, DFCW00, JXW05, MH09, QS00, dCdVSG05].

Researchers [Ano08b, Ano08c, Pau02b]. Resettable [DPV04, MR01b]. Residue [TIGD01, YKLM02b, CNPQ03, FP00, LD01]. Residues [Coc01b, Zhe01, CCS08]. Resiliency [Joh00]. Resilient [Che01c, DSS01, DFK+03, DP07, DP08, GSS08, KZ07, SM00b, KZ03, IR02]. Resist [HM02c]. Resistance [HNZI02, Möl02, EBS01]. Resistant [Ano01e, ACJT00, ANL01, BGW05, CDXT05, CNV06, Gir06, KKO05, LLS05, LTM+00, LNL+08, KS09a, PC09, PC05a, PK03, PT06, RM04, SI00, Ytr06, AMW07, Aju01a, BK07, Bir07, C505, CK105, DR505, Irw03, PY05, WK06, Wri03].

Revisited [ABC+05, Ano02h, BM01b, CDMP05, Knu00b, OSSST04, Res04b, OOB08b, ZTZ05]. Revisiting [AEAQ05, Har01a, Har01b, JM020].

Revocation [Vix02]. Retraining [jLC07]. Retreat [FJSW00]. Resource-Constrained [MRL+02]. resource-limited [Tse07]. Resources [Gutxx, FOP06]. Response [JBR05, LW05a, XK+05]. Responsibilities [Vis02]. Resting [Gut02a]. restricted [ASW00]. Restriction [CHT08]. Restudy [FWL08]. Results [APV05, GM02c, OOP03, RR08, Way02a, YRS+09, CV05, CKRT08, DM07a, GMG00, PM08]. Rethinking [Bra01a, KMZ03].

Refactoring [JLC07]. Retrieve [BIM00, KO00, RE02, Yek07]. Retroactive [DBS01]. retrofitting [CGL+08a, CGL+08b, CGL+08c]. reunion [LBA00]. Revealed [Gal03]. Reversal [Cap01, DIS02]. Reversal-Bounded [DIS02]. Reversals [MS02e]. Reverse [Coo02, EC05, Wue09]. Reversed [Ina02b]. reversibility [KC09a]. Reversible [Gal03]. Reversing [EC05, YWC08, YN01, CDFM05]. Review [And04, Ano02i, Duw03, Eaf05, Fal07, Gas01, Gum04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, Pag03, Pap05, Puz04, Re01, Rot07, See04, Spr03, Ter08, TvdKB+01, Top02, Uzu04, Was08a, Her09b, Kat05b, Lu07, MP01b, Nic02a, Nie04, Puc03, Sip04a, Wal00].

Reviews [For04, Kid00, Sal03b, Sty04]. Revised [Bl03, BC05c, Chr01, CCMR02, CCMR05, CS09, CPF03, DR02c, GS02c, GH05, HH04, HH05, Joh03, Jue04, KKO02, CR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PT06, RM04, SI00, Ytr06, AMW07, Aju01a, BK07, Bir07, C505, CK105, DR505, Irw03, PY05, WK06, Wri03].

Revisited [ABC+05, Ano02h, BM01b, CDMP05, Knu00b, OSSST04, Res04b, OOB08b, ZTZ05]. Revisiting [AEAQ05, Har01a, Har01b, JM020].
Risk [WA07, Voi05]. Risks [ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, PsV01, Sch00c]. Rivest [BB79, Coc03, SP79]. RMI [JR8+06, Mar02a]. RNS [BI04, BKP09, NMSK01]. Road [BDPV09, HR04b, PB01]. Roadmap [Coc02b]. Roaming [CAC03, YWD08, SSM+08]. Robots [Coc01a]. Robust [BB00a, BR09, CJ03d, CW05, DDO+01, FC05, HH09, hKLS00, LHS05, LLC06b, PJK01, SG07, SOHS01, SDFH00, SDF01, VK07, WNY09, WL04b, WMDR08, YPSZ01, ZTP05, KA09, LCZ05c, LKZ+04, Mit00, MB08, TND+09, YY05b].

Robustness [CS05c, HM01b, Rot01, CKL+09]. Rogaway [MW04]. Roger [GG05a]. Role [SBG02, YT09, ZGLX05, Cra05b, Gor05, Mau04]. Role-Based [YT09, ZGLX05, Cra05b]. Roles [LLL+01, Vix02]. Roma [AAC+01]. Rome [IEE04]. Ronald [Coc03]. root [Pet05]. rootkit [Bln09]. Rootkits [HB06]. Roots [Gon06, HCK09, CAC06]. Roseau [PY05].

Rotation [RF08]. rotations [SK03]. Rothe [Fal07]. Rough [Nas02, WG05].

roundness [Lav09]. Round [II00, BP04, Bih00, BF00a, BD02b, Che03, DP04, DI05, Dara00, FKS00, GKK07, GI02, HSR+01, Kan01, KO04, KKS00a, Ks00b, KKS01, KML+02, KKS06b, LKHL09, Lin01c, MP03, MHL+02, NPV01, RR00, Ros00, STK02, WBRF00, Wer02, YSD02, CV05, CL08, CLK+03, DLP+09, GI01, HSL+02, Khi01, LKH+06, MR01b, Pha04, SW05]. round- [CL08].

Round-Complexity [Ros00].

Round-Optimal [K004]. Rounds [BDK+09, CD01a, HSIR02, KM01b, Luc00, Pat03a, Pat04, GM00a, SK01a]. Routing [BGOY08, CL05, Ken02a, KB09, LAPS08, LHC08, MAB106, PS08a, RVS09, vOWK07].

RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, Shp04a, Wal00, Ad03, An01k, An02e, AR01, BI04, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM01b, BM03b, BD00b, BMK00, BJN00, BF01c, Bon01, BCC01, BP01b, CNS02, CDL+00, CW02, Che01a, CKY05, CNP03, CKN00, CNP02, CS00, CS03c, CD01b, DK01, DT03, Duj08, Duj09, DN00b, FS02, FS01a, FMP03, FMY01, FOPS01, GMP01b, GS07a, Git06, Gon06, Gro01, HN04, Her07, HLL03, HL00, HLL03, Int00, Jan08b, JS05, Jon08, JK02b, JK02c, JG01, Ka01, Kal03, Kat05b, Kai01, KKL09, Kin00, KPR03, LS01a, MPS00, NLM03, Man01, May02, May04, Miy01, Mol03b, MP01c, NZCG05, NZS05, NS01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Sha03a, Shp01, Slp04b, SZ01].

RSA [Str02, SWH+09, TID01, TT00, Ver06a, Wal01, Wal03, WQWZ01, War00, WHH05, Wic00, WS02, WY05, XC05, Yan07, hY08, YKL02b, YKL03, YPKL08, YY00, You06, ZC09, Zhe01, ZC09, WC02, dW02].

RSA-based [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZCG05, Sei05, WHHH05, WY05, YPKL08, YY00].

RSA-Encrypted [CD01b].

RSA-Primitive [ST01a]. RSA(R) [An006]. RSES [LLC08]. RST [ZLZ07].

Rueppel [Ara02]. Rules [Bla01a, An00c, Bla01b, GM04, Ste02, Wue09]. Running [ZL04c]. Running-mode [ZL04c].

Runtime [PTB07]. Russia [GKS05].

Ryan [Puc03]. Rye [KJ05]. Ryu [KCC05].

S [BZ02, Kat05b, Puc03, Bih00, BCD00, Dav01b, Dav01c, FM02b, JmBdXgXm05, LG09, Opp01, SMTM01, ZC00]. S-Box [FM02b, SMTM01, JmBdXgXm05]. S-boxes [BCDM00, ZC00]. S/MIME [Dav01b, Dav01c, LG09, Opp01]. SAC [AMW07, HH04, HH05, MZ04, NH03, PT06, HSR+01, HSS04, ST01d, YY01]. SAC'99
SAFE
[Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, ACS02, LBR00, Lys08, Ow09]. Safe-Prime
[ACS02]. Safeguard
[ACS02]. Safeguarding
[Sty04, Bar03]. safer
[Ano00f, NPv01, BDD03]. safety
[HMO1a]. SAFKASI
[WAF00]. Salomon
[Pap05]. Salsa20
[Ber07, Ber08]. Salt
[PKBD01]. Salzburg
[DKU05]. Samba
[BH00a]. SAR
[B+02]. SASAS
[BS01c]. SAT
[KLN+06]. Satan
[Mea04]. Satellite
[CC05c, HYS03]. Satisfy
[PHM03]. satisfying
[QPV05]. Saturation
[Luc02a]. saving
[Lev01]. Savings
[CAC03]. SAX2
[TEM+01, Hei01]. Say
[Sta05]. says
[Mad04]. SBLH
[JK02a]. SBoxes
[WOL01]. SC-CFS
[Ito00]. SC2001
[ACM01b]. Scalable
[ChX04, HKA+05, HLL05, KY03, KHYM08, SPQG06, LLL008, ST03a]. scalable
[ARH08, ADDS06, HM02c, OS01, OTo03b, DwWmW05, Mis06]. Scale
[BWE+02, CDR01, FGD01, BP03a, BH00a, HMvdlM07, PS08a]. Scaling
[BBPV00, Cocolb, SDFH00, SDF01, PBV01]. Scambray
[Gun04]. Scan
[MYC01, BD03, KBD03]. SCAN-Based
[BD03]. Scaring
[Ols00]. Scenarios
[BF05]. scene
[G07]. Sceptical
[Pen01b]. Schedule
[MHM+02, XH05]. Scheduling
[FMS01, XQ07]. Scheme
[AR00, AK02a, ACJ00, AF03, BDD03, BNPS02, BR09, BS01d, BMS03, CL01a, CHK03, CGH01, CC01b, CYP01, CC09, CH01b, CM05a, Cocolb, 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, LCD07, Miy01, Mü01a, OKS06, PL01, RK06, Scr01, SO0102, SWH05, SGGB00, SYL05, SNSG00, Tad02, TC01, Tso01, TT01, WQWZ01, WZW05, WBD01, YWWS09, YG01a, YLH05, Z09, AEEd05, As04a, BCL05a, BCW05, BKN04, BBG+02, CL02b, CBB05, CC01a, CC05a, CL04b, CL04c, CL04d, CCK04b, CYH04, CHY05a, CHY05b, CL00, CHC04, CCH04, CY05, CHC05, Che05a, Che07, Che08a, Che08b, CCS08, CKN06, CJT01, Chi08b, Chi08c, Chi08d, DSGP06, DW01, FLZ02, FXAM04, FZC05]. scheme
[FWL08, FWTC05, Gen09a, GS09, Hes04a, HPS01, HW03, HW04, Hsu05a, HWH05, Hsu05b, HLC07, HC04a, Hwa00, HY03, HLL04, Hwa05, HL05c, HL05d, HL05b, JW06, JSW05, KCO9a, KLY03, KRY05, KSW06, KHL09, KCL03, KU04, KCO5, KCC05, KHKL05, LHY02, LHL03a, LKY04, LL04a, LJY04, LL05a, LKY05a, LKY05d, LL05b, LMC+03, LH04, LTL05, LHL08, LHL06, LH03b, LH03, LC04a, LYGL07, LCC05, LC04b, LC05a, LHH05, LCZ05b, LCZ05c, LCZ05a, LWK05b, MSP09, NC09, PW05, PBMB01, PCC03, PCC05, Ps01a, Pei04, Sae02, Scc04, Shao3c, Sha05a, SC05a, Sha05c, Sha05d, SLH03, mSgFtL05, SCS05b, SC05c, SCS05c, SZS05, TLH05, Tsao08, TWL05, TYH04, VK08, VS08, WL03, Wan04b, WL05, WK05, WJP07, WDLN09, WH05, WC01b, WH02a, WHLH03, WH03, WC03b, WL04b, WC05, XWWL08, XC05, YW04b, YTH04, YW04a, YCH04, YWL05, YC09b, y08, YRY04, YRY05a, YY05a, YY05d]. schemes
[YY05b, YbJf04, ZCO4, ZC04, ZC05, ZK05, ZW05a, ZAX05, ZCO9, ZL05, dRMS05]. Schemes
[AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CPD06, CKN00, Cor02].
CJNP02, Cou04, CS00, CS03b, CDG05, CLZ02, DN00a, DN02b, Des00b, DS06, DN00b, FF00, HSZI00, HWW05, HM02b, HLL05, Kin02, Kos01a, KS03, KOM01, LZL05, LP01, MV00, NIS03b, Nam02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SBZ02, SPMLS02, Sun00a, VMSV05, WCJ09, XSO3, YWCO8, YYDO01, Yek07, YYZ01, ZTP05, ZYR01, Abd01, AFHG06, BCD06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGG03, HCD08a, HCD08b, Han04, Heo2, HKS00, HW03c, HW04, HW05, HC04b, HL04, IY06, JPL04, JXW05, KJY05, Kir01b, KT06, Kre05, Küh08, LWZH05, LWK05a, LW05c, MF07, Miü01b, NK06, PS02a, PKH05, Pha06, QCBO5a, QCBO5b, SN100, Shao03d, Shao05b.

schemes [SCL05, SC02c, SHT05, Wu01, XY04, YWCO8, YCW05, ZF05, ZCL05, vDKST06].

Schloss [IEE01b]. Schneider [Puc03]. Schneier [Hei03, See04, Sty04]. Schnorr [BP02]. School [Coc02a]. Schools [PM00]. Science [Bis03b, Coc03, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IE09b, Imm03, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04]. Scientific [CHT02, MH09, Lau08b]. Scientists [Coc01a, MH09]. SCN [BC05c, CP03]. Scots [Rec01, Sin99]. Screan [HCJ02]. Scribner [Gas01]. Scripts [Uri01, Une05, Rob02, Rob09]. scroll [GB09, HYYW07]. SD [ECM00a]. SDK [ANO02, Bar00c]. SDL [HL06]. SEA [SPQ06]. SEAl [Flu02b]. Seamless [OKE02]. Search [BI05a, Des00c, FIR05, KB07, LM02, TIGD01, WYY05a, WYY05d, ZF06, PM08]. Searchable [ABC05, AFI06]. Searches [PGT07]. Searching [BSW09, GTTC03, OS05]. Seattle [ACM06, S03, USE00a]. sec [KV01]. Second [ACM03c, Bra01b, BD08, CZ05, GW01, HTS02, JYZ04, KCR04, K105, KP01, NM09, RD01, ACM00, Irw03, Son00, Spr03].

Second-Order [NM09]. Second-Price [Bra01b]. Secord [Top02]. Secrecy [Bl02a, GH02, Imm03, Lan05, Rec01, RW03a, Sin01b, BDNN02, BLP06, BD04a, Mol05, Sin09, Sin00, SY06, ZY07]. Secret [ACS02, Alv00, BBDD00, BTW05, BI05, BTW08, BP06, BM01b, CGHG06, CGHG00a, CH01a, CLT07, Cha04, CTY09, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG05, CDI05, Di01, DKL00b, DS06, DN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kab07a, Kab06, Kar01, Kin02, Kon02, KS03, LD04, LT04, LM02, May04, MN01, NABG03, NN06, OKS06, PZ01, PZ02b, PZ02a, RW03a, RW03b, Rey01, RST01, Sin01b, Sun00a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, A08, AED05, Ano02c, Ano08c, Bam02, BCB05, Cal10, CC05a, CHY05a, CHY05b, CIL06, CNK04, CDD00, DD04, DB00a, Di03, DW01, Duj08, FNRC05, FWTC05, FZ06, Gal02, GI0R01, HT04, HJ07]. secret [HKS00, IY06, Kee05, KB09, Lam07, Lun09, MF07, MI09, NA05, PS02a, PW05, R06, Sch01e, SBZ04, SC05a, Sni01b, SC02c, Wan05, Win00, YCH04, ZS05, dRS05, vDKST06, Hii06]. Secret-Ballot [Cha04].

secret-code [DW01]. Secret-Key [HR05, RW03a]. Secret-Sharing [BI05b, CD00, CD05, DKL00]. Secretly [CC08]. Secrets [BH06, BBD02, CMS09, CP07, Cop04b, Di01, Gan01b, Gum04, KMS01, LKM05, Lys08, Pag03, Puz04, Sch02d, Swa01, Tee06, TEM01, VGM04, AGKS07, Ano03b, Ano08b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, DM07a, Di03, DW09, EC05, FS04, GD05, MSDK03, Pau01, Ste08, TCC02, DLM05]. Section [An04a, An07a, BK06b, SGK08, TL02, KP03]. Sector [Cro01, MV01]. Secure [McK04].
Secure [BNPW03, It001, UP05]. Securely
[HL05a, LLK05]. Securing

[AR00, AO00, AF04b, AG01, AP09, Ano01k, ACJT00, AFI06, BDF+01a, BST03, BCL+05b, Bar03, Bi05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02h, CHK03, CHK05, CGP08, CW07, CQS01, CHJ+01a, CHJ+01b, CDM00, CD01a, CS02, CS03b, CDG+05, CDI05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, FP01, FOPS01, GPˇCS08, GIKR02, GJKR03, Gen04a, GD05, HSHI00, HSHI01, HSHI02, HSI06, HR02, Har07b, HKW06, HLvA02, Hy0401, HR40b, HL07, HLTJ09, Hut01, HLO8, IR01, It000, IFH01, JI00a, JL00, JM02, KMM+06, KY01a, KO04, KLM05, KC02, KH05, KKL09, Kli01b, Kos01a, Kra01, Kra05, KSR02, LCK02, LLL02, LCK03, LW00, Lin01c, Lin03, Lin02, LL02, MKP09, Mar02a, Mar07, MV01, Mö03a, MJ01, NM05, Na02b, Nd05].

Secure [NSNK05, NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RVS09, Rsl01, ST01a, Sea05, SVDF07, SBG05, Smi02, SKR02, SNR04, SBEW01, St04, Tad02, VMSV05, Vau05b, VM02, VM03, WLLL09, WBL01, WGL00, WHL05, X03, YWL05, ZYM05, Zha06, Aam03, Ab01, AEE05, AL07, AFGH06, BBS09a, BDFP05, BC07, CLOS02, CCMT09, CC04b, CCK04b, CRSP09, CH+09, CG05, DG06, Dwi04, FMY02, Geb04, GIKR01, GCKL08, HSW09, HL03, HL06, HJW05, HBC+08, Ino05, ISTE08, IKOS07, IY06, KOY09, KG09, LL04b, LLH04, LHC08, LH03, LC04a, LCZ05b, MT09, ML05, Mili01b, SO00, PCMS07, PPB01, PQ06, PSp+08, RH03, RG09, RGX06, Sea09, SBBG07, SGMV09, TKP+08, TCR03, Tse07, Ver01, VK08, WH06, WWA01, YGZ05, YTW05, y08, YRY04, ZBP05, ZCL05, ZCW04, vOWK07, Ano08d, Ano12, BS01a, BSB05, CHKO08].

Secure [FIP02b]. Secured
[BNPW03, It001, UP05]. Securely
[HL05a, LLK05]. Securing

[Abe01, CAL00a, CYH01, Dav01a, FR02, HHSS01, Her02, Hos06a, ISW03, LAPS05, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. Security

[AW05, AW08, Ah07, Aj08, ARD02, An07, An08, An02b, An06c, AHIKM02, Ay06, BP07, BW07, Bam02, BP00, BB00, BKR00, BP02, BNP02, BY03, BPR05, BOHL+05, BBS09b, Bsl03b, Bla02a, BF06b, BDTW01, BCK07, Boy01, BLM00, CGM07, CK02a, CKN03, Can06a, CGH01, Ccr04b, CCG02, CSW+08, Che05b, CM05a, CH07a, CS09, Chu03, Cco01a, CK06, Cor00b, Cor02, CCG02, CG05, Dr00c, Dal01, DNO2a, DKMR05, DeL07, DJ06, Des00c, Din07, DR02d, DSS01, DK05, DS05b, DBS+06, Elb09, ELV01, FIP01b, FBWC02, FW90, FLY06, For04, FML+03, FMY01, GSO2a, GSO3, Gum04, Gut02b, Gut04a, Gutxx, HM00, HSHI01, Hei07, HM02b, Hir09, HLL+01, HGNP+03, HQ05, HL05c, HL05d, IS04, Ina02a, Ina02b, Int00, IK05, IKP+07, JYZ04, JP07, JP02b, JSW05, JG07, Jol01]. Security

[JBR05, JK02b, JK02c, JM02, JQY01, Kan01, KM02, KSHY01, KL05, Ken02a, KB06, KMZ03, KDO01, KM05, Koc02, KHL09, Kos01a, Kov01, KXX00, Lad06, Lai03, Lan00a, Lan04b, LG01, Lee04b, LK+08, LKHL09, Le06, Len01, LN02, LL04c, LSH03a, LSH03b, Lin02, LXM+05, LW005b, LP01, MJ07, MS02a, MS09b, MP03, MF01, MS05b, MV01, MN03, MP05, Mü01a, NIS01b, ND01b, NP07, Oka00, OP01a, Orto00, PBC+02, Pat03a, Pat04, Pat02b, PD07, PC04, PP03, PTP07, PP07, Ph01, Pie05, Pl01, Poi02, PH03, Poo03, PF03, PS05, Puc02, Puc06, QCB05b, RR00, RR03b, RR05, RC01, Rot02a, Roy05, Rub01, RC06, ST02, Sal03a, SJ09, Sch00d, Sch00e, Sch07, Sch08, SJ00, Sch01f, See04, Sha05d, SL03, SLG+05, SL05a, Shp02, SEF+06, SEK01, SEK02, SK06]. Security

[STA03, SB07, Ste05b, SBZ02, St04, SK01,
Sun05, Swi05, Tan07b, TG07, TG04, TPPM07, Uni00a, USE00d, USE01c, USE02b, Uni00c, Uni00d, Uni00g, Uzu04, Vau02, VMC02, WLT05a, WBL01, WWL07+02, WA07, YEP07+06, YWD08, Zan01, ZWC02, ZDW06, Zhe02b, ZYH03, ZS05, AA04b, Ano05c, AJ01a, AJ01b, BPS08, Bai08, Bau05, Bej06, Bel07b, BR04, BGP09, BFGT08, BF08, Bjo05, Ble07, BJ02, BMV05, BG07a, Bru06, BM06, Can01a, C+02, Cha07, Cha05b, CKL09, CKRT08, Chi08b, Chi08c, CJK06, CMJ00, Con09, Con04, CC05e, DP04, DKK07, DY01, DFGH04, Des00a, DWML05, DK05, DMS07, Egh00, FXAM04, FR08, F06, GH08, GJJ05, Gha07, GJ03, Gor05, GKL05, GMW01, GC05, Gut04c, HN04, HCD08a, HCD08b, Har05a, Hei03, Hen01, Hes04a, HM05, security
[HSL02, HL06, HG05b, Ino05, JEZ04, Jan00, Kad07, KY00, KPS02, Kim02, KVD07, Kov03, KH03, Kwo03a, LC03, LL03, LJY04, LL05b, LPW06, LC03, LM05, LLLZ06a, LLLZ06b, LHC08, MJ03, Mal06, Man08, Man05, Mau04, May01, MKK00, MK05, MG06, MN03, MS02d, MK05a, MPPM09, OP01b, Pae03, PSU07, PC05a, Pat02a, PP05, PP06a, Pan04, PHS03, Pip03, Poi01, PS04c, RC05, Ros06b, RN00a, RN00b, SN00, Sal05d, Sch03, Sch02, Sch04d, Sen03, SHL07, Shu06, SPH06, Son00, SH00, Sta02a, Sta06, Ste02, Sun00b, SHT05, SLL*00, Tsa05, Uni00f, Vac06, Van03, Voi05, VS08, WA00, WDC09, WA06, Won01, WK06, XQ07, YY05a, ZS01, ZW05b, ZS05, dLB07, dCD05, vOV07, vTO5, AG09, Ano02c, BC05c, BP01b, Chr00, Chr01, CMJ00, CMR05, Security [CG03, JRB06, Lin02, RR04, Uni00b, ZL04c, Pap05]. Security-related [Gutxx]. security-sensitive [SPH06]. seed [TP07, KJK07]. Seeing [Wal03]. Seek [Coc01a, PH03, Slp05], seeking [Mos06]. Seeks [CAC06]. Seems [Coc02a].
Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, VY01, Ytr06, AMW07, Bir07, BC05c, CZ05, CKL05, DRS05, HH04, HH05, PC05a, Wi09, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bar03, dB07]. Selection [IBM00, JKK09, RS00, SM08]. Selective [CS07c, LS01a, LM02]. Selective-ID [CS07c]. Selectively [Chi08e]. Self [GGM08, HW05, KY01d, PS01b, PBC05, Sch06b, WHL05, WL05b, ZKL01, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, HL04, Lee04a, LL06, LS05b, LWK05a, PC05b, Sha04b, Sha05b, TL05, Tsa05, TJ03, WH03, Wy05]. Self-certified [HW05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, LL06, LWK05a, PC05b, Sha04b, Sha05b, TL05, Tsa05, TJ03, WH03, Wy05]. Self-Enforcing [GMM08]. Self-Escrowed [PS01b]. Self-Localization [WL05b]. self-modifying [CSV07]. self-pairing [Lee04a, PC05b], self-protecting [LS05b]. Self-Shrinking [WHL05, ZKL01]. Self-Similarity [Sch06b]. Selling [Bla01c]. semantic [PBV08, SN00, Sch00, Coc01a]. Semantically [KI01b, ST01a]. Semantics [Li01, Mar02b, BFG04, BFG05, SW02]. Semi [Fer00, Nak01, SY01b]. Semi-Equivalent [Fer00]. Semi-fragile [SY01b]. Semiconductor [CC02b, Ig02, UHA09]. Seminal [Cop04b]. semipublic [YC07]. Sender [CMB05, Her09b, TJ01a]. Sensation [Top02]. Sensible [Sch04e]. Sensibly [See04, Sty04, Hei03, Sch03]. Sensitive [HT06, Bro05b, SPH06]. Sensitivity [SDM06, GSK09]. Sensor [AEAQ05, CS08b, DBS06, Fin06, GPDS08, LNL08, NAB03, PZDH09, ZYN08, AJ08, CCMT09, HMvLM07, JRR09, KXT09, KHY08, LDH06, LPV09, LN04, Lop06,
Separable [CD00a]. Separating [MKKW00, Nie02b]. Separation [BYJK08, GKK07+09, Kel00, Lys02, Mur00, ZGLX05, BYJK04]. separations [GKK07+09].

September [AUW01, AAC01+01, AJ01a, BCKK05, BC05c, CSY09, CGP03, DV05, DKU05, DFCW00, EBC00+00, ELvS01, FLA03+03, GKS05, QS00, RS05, SMA07, WKP03, dCdVSG05, AJ08]. September 19 [AJ01b]. September 19-21 [AJ01b].

Sequence [HWH01, MS02e, WHLH05, ACTZ05, GB09, SL09, WG02, YZEE09]. Sequences [ADD09, Bi09, FSGV01, HG05a, JZCW05]. Sequential [GSS08, SNW00, RMH03a, WH02b]. Serial [CTLL01, KW06, Uni00g, Mit00]. Serpent [BDK02b, ABK00, IK00, IK01, KKS00a, KKS01, KKS00b, Os00, Pat01]. Server [ANRS01, BMK00, Dew08, KO00, LWK00, NS01b, PS05, TMM05, XS03, Zha00, BB05, LHL04b, LHL04a, LKY05b, LHL03b, NTV07, Tsa08, Tsa01, TWL05, YS04].

Server-Aided [NS01b]. Server-Assisted [XS03]. serverless [BDET00]. Servers [BIM00, HS07, Jab01, KC07, Mar02, TEM0+01, LS05b, PT08]. Service [BACS02, BH00a, CLK01a, DeL07, KZ01, Lan04a, LDM04, Nik02a, Nik02b, PKBD01, CUS08, HILM02, KWDB06, LB05, Mir05, MV03b, SRJ01, SSM0+08, UG08, Coc02b, Hilo06].

Services [ANS05, BC02, DJLT01, ECM00a, ECM00b, Knu07, Tsa01, Uni00b, WL07b, BDS0+09a, BFG04, BFG05, BFG08, CCCY01, HM05, JRB0+06, MW06, MMPM09, MV03b, RR04, SBG07, SL05b, TWL05, WA06, BH00b]. serving [LLK05]. Session [GL01, OHBO8a, CS04, OHBO8b, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YWL05].

Session-Aware [OHBO8a, OHBO8b]. Session-Key [GL01]. Sessions [KPR03]. Set [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDET00, CHe07, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01]. Sets [CF05, EIG01, TW07]. Setting [BBM00, DL08, LP01, PG107, GMLS02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC0+01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SGB01]. SGI [Bar00c]. SGID [Tot00]. SHA [AD07, BC04a, GLG0+02, HKR01, MP06, SK05a, TYYL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG0+02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TYYL02]. SHA-512 [AD07, GLG0+02]. SHA1 [WYY05a]. SHACAL [KML0+02]. Shamash [Hes04a]. Shamir [BB79, SP79, Co03, PW05, VS08]. Sha-1 [BD07, GLG0+02]. SHA1 [WYY05a]. SHAAC [OMT02]. SHARC [DMSW09]. Share [CT08a, CDF05, FS04, AEEdR05]. Shared [AC02, BH06, BBDK00, BT02, CGH00a, TEM0+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, TYH04]. Shares [TT01]. Sharing [BTW05, BI05b, BTW08, BGHP02, CD00a, CLT07, CC08, CTY09, CD00m, CF02, CS05f, CDG0+05, CD05, Di01, Di03, DS06, DP07, FM02a, FPS01, FMY01, HNZ02, Kin02, Kog02, KS03]. LD04, MN01, NN06, OKS06, PZ01, PZ02b, PZ02a, S01, S00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CDD00, DD04, DM07a, DKL00b, FWTC05, GIKR01, HTO4, HKS00, IYO6, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YC04, YCY07, ZSV05, dRMS05, vDKST06]. shc [Gua05]. Sheets [MNS01]. shell [Dwi04, Gua05, BS01a, BS05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [McK04, C03, YWC05]. Shift
[CGFSHG09, Che08a]. Shin [Küh08, Küh08]. Shines [Coc02b]. Shinko [Küh08, Küh08]. Shines [Coc02b]. Shinko [Ano00d]. Ships [Ano02e]. Shops [Ano01c, YSS+01]. Shor [KLB+02a]. Shores [KKP02]. Short [Ano01k, AFI06, BBS04, BGW05, DN00b, Gra02b, LS01b, PM02, RR02, RW02, Vau05b, GL05, WDLN09, Coc02b, Sch01c]. short-term [WDLN09]. Shortcuts [Sha03a]. Shortened [Kur01]. shortest [Pei09]. ShortPK [WDLN09]. Shoup [Luc02b, VMSV05]. shows [AJ08]. Shrinking [Gol01c, WHLH05, ZKL01]. SHS [Ano08d, Ano12]. Shuffles [Mir02]. Shuffling [PBD05]. shut [Gil07]. SiBIR [IR02]. sic [IEE09a]. sichere [Lin02]. Side [Ano01i, BU02, KSWH00, Law09a, LL01, Möld02, OT03a, OT03b, Sch06a, WC04, CFPQ03, PSP+08, WL07a]. Side-Channel [BU02, Law09a, Möld02, CFPQ03, PSP+08]. Side-Match [WC04]. Siena [BCKK05]. sieve [CM05b, JL03]. sieves [Har07a]. SIGABA [Les03c]. SIGACT [ACM03c, ACM05b, Raj06]. SIGART [ACM03c, ACM05b]. Sight [Col03]. SIGMA [Kra03]. SIGMOD [ACM03a, ACM03c, ACM05b, ACM04a, FMA02]. SIGMOD-SIGACT-SIGART [ACM03c, ACM05b]. Sign [BSC01b, BTTF02, Dav01c, Kra03, Dav01b]. Sign-and-Encrypt [BTTF02, Dav01c]. SIGn-and-MAc [Kra03]. Signal [Ano02e, GG05b, Sha01e, CKL+09, LLLZ06a, LLLZ06b, SBS09, Kov01]. Signalling [ECM00b]. signals [Ren09]. Signature [ANS05, AAK09, AR00, ADR02, Ano01c, Ano01f, Ano09a, Ano13, Ara02, AR01, ACJT00, Bar06b, BNP02, BG0Y08, BMS03, BSD09b, CM00, CDO0a, CL04a, CK02a, CGP08, CH01a, Che02, CM05a, Cor02, CF0S01, CS00, D505a, DKFX05, Eng00, FIP00, Gen00a, GJSS01, GS02c, HYZ05a, HSZI00, Han00, HM02b, JSJK01, KC02, Kuh00, LYL01, LP01, MV01, Miy01, Nat00, NZCG05, PL01, PCK02, Pre01, RS01, SA02, ST01b, SO0J02, SW05, SPMS02, Str01a, SYLC05, SSNGS00, TNM00, WQZ01, WBD01, XYL09, YYDO01, YSS+01, YYZ01, YLH05, ZK02, ZJ09, Zhe01, Avd00, BCL05a, BCW05, Cai00b, CWH00, CL04b, CYH04, CCH05, CJ05, CHC05, Cht05a, CJT04, GKK03, HLL0+02, He04a, HPS01, HW02, HW03, HW04, HW04, HW05, HW05, HC04a, HL03, HC04b, HL04, Kwo02, Kwo03b, LH04, LHY05, LL05b, LLH04, LTH05, LWZH05]. signature [LHH05, LCZ05b, LZC05c, LCZ05a, LW05c, PKH05, PC05b, QCB05a, QCB05b, Sa02, Sha03c, Sha03d, Sha04b, Sha05a, Sha05b, Sha05d, SCL05, SHT05, TJC03, TYH04, Wan04b, WK05, WLLLH05, WHH05, WTH01, WLLLH03, WTH03, WY05, XCO05, YTH04, ZCO05, ZFO05, ZW05a, ZCLO5, ZCWO4, RR04]. Signature-Based [CK02a]. Signature-Embedded [Ano01c, YSS+01]. Signature-Tree [TNM00]. signature/multisignature [Wu01]. Signatures [AO00, AOS02, ABW01, BN02, BGLS03, BBS04, BSC01, CDO0a, CL01b, CNOV06, CFB+01, DK01, GM01b, GM03, Gen04b, Gra02b, HSZI01, Her06, HM02b, HS01b, HHGP+03, HLT01, IR01, IR02, JS05, KZ01, Kal01, LCK03, LS01a, Lys02, MRO1a, Mad00, MM02, MNFG02, PCG01, Ram01, RR02, Rs01, WV01, XS03, Zhao02, Ano01i, Ate04, AH05, BLH06, BB05, BMW02a, BLS09b, Cai00a, CKK03, Die00, DMT07, Fan03, FW04, FB01, GMSL02, HRL09, Her07, HL000, JLL01, JL04, KKKL09, LV07, LG04, LG09, LS05b, MMJ05, Pj05a, PBV08, Sch01f, Sha01d, NZ505]. Signcryption [Boy03, MLM03, Zhe01]. Signed [FL01b, OSSST04, Sch01a, SJ00]. Signer [DKFX05, CJT04, LL05b, WK05, IR02].
Signer-Base [IR02]. signer-verified [CJT04]. Signers
[LZL+01, Sae02, Sha03c, YTH04].
Significant [SZ01, MS02b, Shp02]. Signing
[An00j, IR01, RR02, HWW04, WK05, WH02b]. signs [Gen00a, Lun09]. SIM
[AAK09]. SIM-based [AAK09]. similar
[Che08b]. Similarity [Sch06b]. Simon
[Imr03, Ree01]. Simple
[AKS06, CYH05, CJS03, CWY05, CC06, CS03c, DT03, FSW01, Gir06, HM02c, HLT01, MS01, Nam02, PBD05, RK06, SF02, YW06, Dan02, GM04, KTC03, LKK03a, LKK03b, LF04, KH05, YRF05d].
Simpler [Lin03]. Simplicity [MS01]. Simplification [DJ01]. Simplications
[JS05]. Simplified [Bon01]. Simplifying
[Gen04]. Simply-Iterated [Oni01]. Simulatability
[HU05]. simulatable [Lau05]. Simulation
[DKMR05, KL05]. Simulation-Based [DKMR05, KL05]. Simulations
[WBR00]. simultaneously
[Wu01]. Singapore [BDZ04, TLC06]. Singh
[Imr03, Ree01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a].
Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server
[KO00]. Singular [AS08, Bai01b, BR09].
SINOBOMETRICS [LLT+04, Li05].
Sizes
[An09b]. Skein [AEMR09]. Sketching
[MNS08, SLTB+06]. Skipjack
[Gr02a, HSL+02, SL+00]. Skipjack-like
[HL+02, SL+00]. SKLOIS [FLY06]. Sky
[MYC01]. SLAAC [CGBS01]. SLAAC-1V
[CGBS01]. Slide [Fur02b]. Small
[CCM05, ELvS01, Fin02, GPS06, MNT+00, May02, OT03b, RK06, SM02, Sch01c, SPQQ06, Wa03, YLC+09, Duj08, dW02].
Small-Project [MNT+00]. Smaller
[Bar00c]. Smart
[An04, An00a, An05b, AJ01b, Bel01, BCST00, Car01, CL07, CJT02, DF01, DFCW00, DLJL01, HBJL01, Hen01, HQ05, Jac00, JSJK01, JY01, Lam00d, LS+07, MOP06, MV01, MG08, NFQ03, Poh01, QS00, QS01, RE00, RE03, RS01, Sak01, SR01, Sha01c, SP02, TBDL01, VPG01, YKMY01, An00k, An00l, An04a, AJ01a, Bor00, BPR01, BCHJ05, BGL+03, Bur00, Ca00c, CCCY01, Cha05a, Cla00b, Con00, CH00, DMT07, DFFH01, DFPS07, FCZ05, Fin03, GMG00, GUQ01, HHSS01, Hsu05b, Hsu05a, Jua04, KLY03, LKY05a, Ler02, LC05a, Lu07, MY01, Pba06, PB01, Pr07, SDFV07, SLH03, Sm00, TIS07, VK08, WC03b, YW04b, YWWD08, Zaf00, BJvdB02, CL04d, CCK04b, Che00, DFPS06, FGL02, Gro03, HL05b, Ku04, KC05, LHY02, Pan02b, SKKS00, Sco04, SCF01, TV03, YW04a].
smart-card [GMG00]. Smartcard
[HW01, KRV01, RMCG01, Uri01].
PBVB01, BBVP00, CGMM02, DM07b, HR02, It01, KS02. Smartcard-Based
[RMCG01, CGMM02]. Smartcards
[CMS00, GN01, IFH01, MS01, Str01a, UST01a, KWS06, An04b, RM02]. smarter
[Car01, Cla00b]. Smartly
[MS01]. Smooth
[PS02b, GM05]. SMS
[Coc02b, ETM05, LSL05]. SMS-capable
[ETM05]. SMV [ZWW01]. snake
[RD09]. snake-oil [RD09]. Sniff
[An02c]. Snort
[GC05]. SOAP [DLJ01]. Social
[Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sae02, Sha03c].
Socket [ZL04c]. Soft [DV08]. Soft-Core
[DV08]. Software
[Ahm07, An07, An02c, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HJC02, HH01, Hoe01, Jov03, Knu07, KSZ02, Lai06, Law09a, LSY01, LLZ06a, LSVS09, LTM+00, MNT+00, MSNH07, MKY08, MG06, N005, PM00, PS01c, RM04, Sch01a, So00b, YW04b, Zaf00].
Software-Efficient [HCJ02].
Software-Hardware [PS01c].
Software-Only [Hoe01].
Software-Oriented [ZCC01].
Software/Hardware [Nd05].
SOI [Ano02e, NFQ03].
SOISIC [Ano02e].
Solaris [Ano06c, BH00b].
Solomon [KY02b].
Solution [Cap01, CJT02, DHR00, LLS05b, Poh01, Str02, TvKB+01, LSH00].
Solutions [Ano04b, MV01, Jan00, MSK03, MV03b, St.00, Gum04].
Solve [CU01, GS03].
Solving [CJT04, GPP08, Wil01a, Bul09, Whi09].
Some [AG01, BDF+01a, DJ01, DFG01, GM02c, HSS04, JMv02, KY02b, KY02b, KO02, MT02, Max06, P00a, Pot01, Pot02, Pot03, Wal01, Fur01, Han04, He02, JKH0a, RSS04, SHT05, ZF05].
Someren [Ano03c].
Something [FL01b].
sometimes [FNRC05].
Sons [And04].
Sorry [San05].
Sorts [Ano03e].
Sound [Bla01c].
Soundness [ABHS09, DPV04, MR01c, BPS08, Lau08a].
Source [Bar00c, Bol02, Gut00, HBF09, KLR09, PM00, RK06, TEM+01, Ano03c, BGL+03, CBB05, MC0a, RVS09, SB05, Bar00b, Lin02].
Sources [KZ07, WLZZ05, ZK03].
Southampton [Bla03].
Soviet [AJ08].
SP [BG07a, Hr09].
SP800 [SF07].
SP800-90 [SF07].
SPA [FMP03, Nov01].
Space [BGH07, Lu02, MSH07, NS05a].
Space-Bounded [Lu02].
Space-Efficient [BGH07].
Spain [BS03, DFPS06].
Spam [CMB+05, DGN03, Vix02].
Spamming [Bel04].
SPARK [Jen09].
Sparse [BLST01, BDG+01, FS01b, GS03, BF06a].
Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09].
Spatial-Domain [SDFH00].
Spatial-Temporal [CDTT05].
speakables [BZ02].
Speaker [LM00].
Speaks [VN04].
Spec [Bar00c].
Special [Ano04a, Ano07b, Ano07a, BK06b, GS05, GS07a, GPP08, SGK08, KP03, FOP06].
Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08].
specialized [Wan04b].
Specific [HCK09, Zir07].
Specification [BCT00, ECH00, LKJL01, RSA00c, Mea04].
Specifications [IEEE00b, BDFP05, BD04a].
specificity [GSK09].
Specified [Tad02, He02, LWK05b, YY05a, ZF04].
Specifying [BvdB02, C01, SBS09].
Speck [EKS07].
Spectr [GMM01].
Spectr-H64 [GMM01].
spectra [MS02b].
Spectral [QPV05, SK07].
Spectrum [BQR01, LY07, PM00].
Speech [MRL+02, AA04a, PY08].
Speed [Ano00d, Ano02d, Gro01, KJR01, KMM+06, Lut02, SOTD00, SM02, Wic00, YKMY01, BGL+03, RW07, RMCG01].
Speeding [Osv00, SWH+09, TC05].
Speedup [YKL02b, YKL03].
Spider [Cre00].
spherical [LZP+04].
Spies [Gan01b, Win05c, Hau06, NRR00].
SQUINT [Che08a].
SPIN [MS02a].
Spline [SPK08].
Splitting [GMW05, LLK05].
SPN [HLL+01, Kan01, PQ03b].
SPNs [CKL+03].
Spot [Na05].
Spread [BQR01].
Spring [Pap05].
Spring-Verlag [Pap05].
Springer [Fal07, Lee03a, Lee03b, Pho01].
Springs [Wil99].
Spying [FNRC05].
Spymaster [Bud06].
Spyware [Ste05c].
SQL [Dew08, HILM02].
Squadron [OC03].
Square [HCK09, HQO1].
Squaring [CH07b, NSS02].
SRAM [HBF09].
SCC [HQR01, ZCC01].
SSH [All03, BS01a, BS05, BKN04, Dwi04, H001, Hos06b].
Kra02b, Naz02, One05, SWT07, Str02.

**SSH-Connected** [Höf01].

**SSHFS** [Hos06b].

**SSL** [ASK05, BPST02, CHVV03, JRB+06, KCD07, KPR03, Kra01, LLK05, LWK00, Net04, OHB08a, OHB08b, SB01, SQ01, Vau02, ZFK04].

**SSL/TLS** [BPST02, CHVV03, KPR03, OHB08a, OHBO8b]. **SST** [Gau02]. **St** [GKS05, NH03, AS01a]. **Stack** [Pot03].

**State** [GK01, NH03, AS01a]. **Stamps** [Gau02]. **Stamp** [CL00]. **stamping** [HHC05]. **Stamps** [KZ01]. **Stand** [CAC03]. **Standards** [Ano01f, Bur06, CL07, Coc02b, Hus01, RSA00a, Tsa06].

**State-transition** [TL07]. **statecraft** [dL00]. **Stateless** [ANR01, NNL01, SK05b].

**Stateless-Recipient** [ANR01]. **States** [LB04, Jol01], **static** [CW07]. **Statistical** [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, LZ01, LL+01, MV03a, Net04, Pro01, RSN+01, BK03, GSK09, Hey03]. **Statistically** [Fis01b, HR07, HNO+09].

**Statistically-hiding** [HR07]. **Statistically-Secret** [Fis01b]. **Statistics** [CKN01, CNK04, KLM05]. **Status** [Pre01, Sha03b], **statute** [Cal00b]. **STD** [WMDR08]. **Stealing** [Gau01b]. **Stefan** [AUW01].

**Steganalysis** [Pro01, Sal05b, GSK09, WW04]. **Steganografie** [Sch09]. **Steganographic** [CTL04, HR02, LL02, MJF07, RH02, RS00, Wes01, KC09a, LYC02, WWTH08, YCL07].

**Steganography** [BC05a, BG08, CYH01, ChLYL09, CDR01, CW09, CTH08, Col03, CMB+08, CS05c, DIR05, DRL09, FGD01, Fr07, Gal03, HCBLETRG06, HLVa02, HvAL09, Huv05, HSK01, LS08, PH03, Sal05b, Sch09, Sha01c, Shi08, SWR05, Wan05, WW06, CDS07, CO09a, Che07, Che08a, GGS+09, JDJ01, KP00, LT04, WW04, WMS08, Way02b, Way09, YCYW07]. **stego** [KC09a].

**Stego-image** [KC09a]. **Steiner** [WL02]. **Step** [DRL09, KK01, MP07, SL06]. **step-by-step** [SL06]. **Step-out** [KKK09].

**Stepping** [WRW02]. **steps** [Bih02].

**Stereotypes** [GO03]. **Stern** [CGP08, CS05b].

**stick** [GPX08]. **Sticks** [Sam01]. **still** [Ano00f].

**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, Hun04, MSTS04, RCBL00, Ric07, RH02, Vad03, AFGH06, DFS05, HGR07, LPM05, SGMV09]. **Store** [CTBA+01]. **Storing** [ST06]. **Story**

[Ben01b, Ben04, Bu00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, HS01a, Win00].

**strategic** [AJ08].

**Strategies** [Cir01, KL05, SKQ01, Dwi04]. **Strategy** [DR02a, TP[07, KC09a].

**Stream**

[BC05b, BSW09, BS00b, BL02, CF01b, Can06b, CJS01, CH02, CM03, Con03, CL02c, DF07, Fil00, FF01a, Gol01d, Gol01e, GM02, HC02, HR00, HR04a, Jan00, KHD01, MS07, PP06a, SM01, Sar02, SX01, WB02, Wu04, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, BVP+04, DS09, DK08, KH08, Max06, MI09, PCS03, PCC03, SB05, WW08].

**Stream-Cipher** [SX01, WW08].

**Streaming**
Streams [AIP01, CO09a, YLC+09, ZCW04].
Strength [CB01, JX05, Oni01, CKL+09].
Strengthening [Loi00, MHM+02]. String [CPS07, DFS04, Pas03, Dam00, RG05].
Strings [Vau05b]. Strong [ADD09, BB00b, CS00, DKFX05, CC04a, HRS08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04].
Strong-Password [LSH03a, LSH03b, WHL05, CC04b, KTC03, Ku04].
Strongly [IY06]. Structural [BS01c, LBR00].
Structure [DNP07, EIG01, H¨of01, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PG03, Sun00a, XH03, Hen06a, IY06, SWR05].
style [BPS08, dH08]. Subcommittee [Uni00f, Uni00h].
Subdivision [LDD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro03, GMR05].
Symbolic [Bor01, Jef08, Mar02b, May09, MT07, ALV02]. Symmetric [Ano01j, ABM00, CCM01, EP05, RR00, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01].
Symmetric-Key [Ano01j, ABM00, BU02, BK07, CV01, CCM01, Des00b, EP05, FW09, Fil02, RR00, Ust01b, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01].
BCDH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Je08, KM07, MFS+09, SMP+09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05.
synchronisation [CMdV06].

Synchronisation [GPˇCS08, SW02].
synchronize [Pau02b].
Synchronous [CH01b, Sar02].
synopses [YLC+09].
Syntax [BWBL02, RSA00b, RSA00d].
Synthesis [XFZ01, SOIG07, UBEP09].
syslogs [ME08b].
System [Ano02d, Ano02e, ANR01, BIP05, BCST00, Bih00, CCDP01, CHM+02, CSW+08, CGJ+02, DJ01, DGP07a, DGP07b, DV08, EM03, FL01a, Ito01, Joh05, KC02, KHY04, LV00, LSS05, LSS05b, LXM+05, MA00a, MA00b, Miy01, MFK+06, MFS+09, RH02, SR01, Sha02, SOOI02, Ste05b, TK03, TZT09b, USE00a, WG05, WA07, YKMY01, YKLM02b, ZYM05, AHC03a, AMRP00, Ano00j, ADH+07, AAKD09, Bih09, BDET00, Bul09, CC02b, CCH05, CJI06, CPG+04, Coc01a, Cre00, CO09b, DZL01, DPT+02, DIM08, DGP09, FP00, GG08, GSK09, GMG00, Gou09, HLL+02, Joy03a, KWDB06, KXD00, Kwo03a, LL04b, LKIJ01, Lin00a, LK01, MKKW00, RCG+05, Sal00b, SCS05a, SGMV09, SETB08, TKP+08, Wan04a, db07].
systematic [DW05, ZL04a].
Systemic [KB06].

Systems [ACM03c, ACM05b, ANR01, Ano00e, BCS02, BRTM09, CP02, ELvS01, Fel06, GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST+05, LLLZ06a, LJ05b, Lat03, Mar02b, MMYH02, NABG03, RS05, Ril02, SM01, Sas07, Sjt09, Sxy01, USE00c, USE00b, Vav03, VHP01, WK03, ARJ08, And08, Ano01j, Bif03, Bl07, CUS08, CC05c, CCS08, CGL+08a, CGL+08b, CGL+08c, CCM01, CNPQ03, CHT02, CG05, CSK+08, DYO09a, EYO09, FMY02, FP00, HP00, HBC+08, Hup01, HYS03, KAM08, KP01, KNP01, KP03, Kov03, KR03, KNS05, MBS04, MSP+08, NdM06, Nis03a, PBMB01, Par04, PI06, RW07, Sha01a, SK03, TOEO00, WAF00, XQ07, ZSV05, Ano02d, Lu03].
systems/ciphers [SK03].
Systolic [KLY02, KKY02, MP01c].

Table [Ano03d, MFFT05, XFZ01, BZ03, CC05b, Has00, Tsa08].
Tables [AJO08, KB39, RBF08].
Tag [KKJ+07].
Tags [OS06, ACdM05].
Taipei [Lai03, Ano03a].
Taiwan [Lai03, Ano03a].
Takagi [LKYL00].
Takaragi [WHLH03].
Taming [Abao0, Lov01].
Tamper [LTM+00, CT02].
tamper-proofing [CT02].
tampering [PS08b].
tandem [DPT+02].
Tang [YRY05d].
tank [Pau03].
tar [Str02].
targama [MAaT05].
target [BDO4b].
Targets [MV01, Pau03].
Tarragona [DFS06].
tasks [XQ07].
Tate [Jou02, SKG09].
TATSU [TSO00].
tattling [CSK+08].
TC [DKU05].
TC-11 [DKU05].
TC-6 [DKU05].
TC8 [ElvS01].
TC8/WG8.8 [DFCW00].
TCB [SPHH06].
TC [HR06, Kil05, Nao04].
TCP [CD01b, Os00, SB05].
TEA [CV05].
HSR+01, HSIR02, HHK+04, MHL+02, WN95].

Teaching [McA08, Shu06, GV09, Jan08b].
Tech [Kir01a, TvdKB+01, Uni00c, Gra01, Uni00f].
Technical [BHM03, GS07b, Lan00c, Scr01, TL02, USE01b, USE01a, USE02c].

Technique [CC02a, Pau09, PQ03b, SC02a, WC03a, vW01, CL00, Che08b, Pau03, Ren09, WC05].

Techniques [AIP01, BSW09, Bih03, BBPV00, BD02, CC04a, Cra05a, DBS+06, Dun06, Gal03, KLN+06, Ken02b, Knu02, K003, MKP09, NCRX04, PJK01, Pfo01, Pre00, Shi08, YK01, AB09, BM05, BR05, Che08a, DY01, DHMR07, DY09a,
Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08]. Technologie
[RSA09b]. Technologies [MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZW02, ATS04, PB01, TTZ01]. Technology [CZK05, Cla00a, GSB04, MP00, NFQ03, Pbg03, TV03, AL07, Ble07, Car01, Cas02, Che00, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b]. Tektronix [Ano02e].

TelCorreo [LM00]. Telegram [Tuc66].

Tektronix [Ano02e].

Telelogic [Ano02e].

Telephone [KZ01].

Telephony [Ano02e, CFRR02, PM00, CGV09].

Teleportation [BEZ00, BEZ01, Duw03].

Telling [Gan01b].

Template [LMTV05].

Temporal [CDTT05, KXTZ09].

Ten [ES00a].

Tenth [USE01c].

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

Terminal [ECM00a, ECM00b].

Terminals [Chi08a, ISTE08].

Termination [BP05].

Tests [MT02, NM09, GT02, Gut04c, JPL04].

Testing [II00, CGBS01, Fil02, Lu02, Lu03, SB00, WA06, Lu03].

Telephone [Ano02e, CFRR02, PM00, CGV09].

Text [Lut02, PJH01, PM08].

Textbook [BJN00, PP09].

Thank [CMB+05].

Theft [CMS09].

Their [AGT01, CD00a, Gen04a, JKW01, LLL01, WLZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SS06, TO01, WV00].

Them [WD01a, Tee06].

Theorem [AC02, Eke02, GN01, Sho00a, Sch01b, YKLM03].

Theorems [MW04, Nyb01].

Theoretic [CB01, DHR00, Kat05b, Nie02b, VV01, VDK05, vW01, Mar05b, NR04, Sh09, Wag03].

Theoretical [SGB01, PRS04].

Theoretically [AP09, DM00b].

Theory [ACM00, ACM01a, ACM02, ACM03b, ACM04b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, AL06, BDZ04, Bih03, Boy01, CC04a, Cra05a, Des02, Fau07, HR06, Hay06, IZ00, Ir03, Kim01, Knu02, Lai03, Lee04b, Lut03, MNT+00, Mao04, NP02a, Nao04, Oka00, PY06, Pfi01, Pre00, Rot05, Roy05, Sch06b, Sh03, Spr03, TW02, TW06b, Vau05a, Wa00, WG05, Yan00, YDKM06, Zhe02b, AU01, AB09, Buc00a, Cas06, Cos06, DW05, Gar04, HHL+00, HW98, Joy00, Kil05, Lam01, PPV96, Rot02b, Rot03, SCS05a, Sh05b, Ste08, Sti95, Sti02, Sti06c, Tat05, TW05, Was08b, HR06, KXTZ09, Kil05, Nao04, Nie02a, Nie04].

There [Bar00b, GW00].

Thieves [NRR00].

Think [Pau03].

Thinking [See04, St07a, Hei03, Sch03].

Third [AL06, BS01b, CP03, HR06, KY05, KNP01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QS00, CGH4+00b].

third-order [JZCW05].

Thirty [ACM03b, ACM06, ACM00].

Thirty-Eighth [ACM06].

Thirty-Fifth [ACM03b].

Thiry [ACM02].

Third-Fourth [ACM03b].

Thorsteinson [For04].

Thou [MYC01].

Thought [MNT+00].

Thoughts [Joh00].

Threat [Por06, SS04, BK00, Geb04].

threatened [An001].

threats [CNPQ03].

Three [BR00b, Kak06, LSH00, Mann06, AJ08, CL08, FGM03, GPS05, LHL04b, LKY05b, LLS+09, MF07, MAA00, SP06, YC09a, ZL04b].

Three-Key [BR00b].

Three-party [LSH00, CL08, LHL04b, LLS+09, YC09a].

three-principal [ZL04b].

Three-Stage [Kak06].

Threshold [AF04b, AIP01, BTW05, BTW08, BDDS03, BSS02, CCD07, CLT07, CDN01, DK01, DN03, DG03, F01a, FP01, JL00, KY02a, KS05b, Kin00, Kin02, Kog02, LZZ+01, LSC03, LC05a, LP01, MS02, Nie02c, STY07, WQZ01, Wau04b, WH03, X03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, DG06, HW02, HW03,
Throughput [HV04, LS01b]. thwarting [WL07a]. TI [GBKp01]. tit [MAaT07].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].

Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01].
Transcript
[Ano01a, Ano01b, Ano01c, Ano01i, Ano01j, Ano01e, Ano01k, Mal02, Nik02b]. Transfer
[CT08b, Din01, GKM+00, KKL09]. Transferability [HSZI00]. Transfers [IKNP03]. Transform
[ABM08, BBC+09, BR09, CPhX04, KC09b, LKK05, Nak01, SSFC09, VK07, BR06, Che07, OP01b, SR00, LPZ06]. Transformation [CT09, HLL05]. Transforms [Laf00]. Transient [Ric07, VS08]. Transistor [Coc02a]. Transistors [Bar00b]. Transit [Con00, Cal00c]. Transition [Ase02, TL07]. Transitioning [Ano09b]. Transitive [BN02]. Translation [GGS+09, PY06]. Translation-based [GGS+09]. TransLink [Cal00c]. Transmission [MLC01, SNR04, SVD07]. Transparent [CCDP01, Por01, Lin00a]. transport [Bor00]. Trapdoor [BPR+08, Fis01b, KO03, KO00, Gen04a, JSW05, PW08]. Trapdoors [GPV08]. Travel [Bur00]. Traversal [JLMS03]. Travelling [Knu00a, Knu00b]. treatise [Bla00, MAaT03, MAaT04, MAaT07]. treatises [MAaT06, MAaT07]. treatment [CL05, DK08]. Tree [CC05d, GST04, JLMS03, KPT04, LKK05, LM02, TNM00, Mon03, PCC03, WL02]. Tree-Based [GST04, KPT04]. trees [Che02, Che07, TC00]. Trends [Ahm08, KB07, Ort00, NdM06, PRS04]. tricks [All03]. triggered [HHJS04]. tripartite [SW05]. Triple [HSH+01, BR04, CGBS01, Cor00a, FZH05, Kel05, LMP+01]. Triple-DES [Cor00a, LMP+01]. Triples [FS01b]. Tripwire [TvdKB+01]. trivial [KO00]. troubleshooting [HJW05]. True [BST03, Cha04, DV08, EH+03, HBF09, Pan07, SFDF06, BG08, BG09, GB09, Hau06, HLwWZ09, Ste05c, vT01, VKS09]. Truecrypt [CSK+08]. truly [BGL+03]. Truncated [CS05b, KM02, LHL+02, SKU+00, SKI01, GS09]. Trust [CHSS02, HCD02, Lin00b, LHL+08, Mit02, SMP+09, Dav01c, HLL04, IY05, LCK04, LLM05, LMw05, LLW09]. Trusted [DK01, WH01, WV01, ARJ08, PS04c, ZYLG05]. Trusting [CKS09]. trustworthy [CCH05, SK03]. Truth [MNT+00]. Tseng [Hwa05, XY04, ZAX05]. TTM [GC00b]. Tuesday [Uni00a, Uni00f, Uni00e]. tunable [LB05]. Tunny [Sal01a]. Turin [AL06]. Turing [Bar00b, RSA03a, Adl03, Coc03, Cop04b, Goo00, Pet08, Riv03, Sha03b]. Turkey [Bor00]. Turkish [DD02]. Turn [Tsa07]. Turning [DJLT01]. tutorial [Can06a, Puc06, Rot02b, Rot03, vT00]. Tweakeable [DS08, HR03, LW02]. Twentieth [Can01b]. 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 [Ram01]. TWIRL [Kal03, ST03b]. Two [Ahm08, BDG+01, DIS02, FD01, Hen06b, HSIR02, HSS01, HU05, HL05b, JZW05, KCP01, KO04, KTC03, KO03, Lin01c, MR01a, MLM03, MAaT07, NS01c, Ng01, Pau02a, Sch05c, SK00, St.00, Ste05a, Ste01, TW07, WV05, XS03, YWWD08, YY001, CLOS02, DHL06, GCKL08, HW03c, JW01, LMTW05, MS09c, Mc0103, MCHN05, Pau01, Pha06, ZLX99, dB07]. Two-Block [KCP01]. two-channel [MS09c]. Two-factor [Hen06b, Sch05c, St.00, Ste05a, YWWD08, dB07]. Two-Key [Kl03]. 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, FKSW00, IK00, Kel00, Knu00a, Knu00b, Luc02a, Mur00, SKW+00]. Type
[CKQ03, Dug04, Høf01, KYHC01, PDMS09, RMS05, Vir03, GG08, PQ06, Sha01d].

Type-based [Dug04]. Type-Passing [Vir03]. typed [BG07b, FR08]. Types [Gor02a, GJ04, RSA00e, BFM07, Lau05].

Typical [BSC01a]. typing [GJ03]. Tzeng [QCB05a, Hsu05a, HL05d].

U [DB04]. U-boat [DB04]. U.K. [CAC06]. U.S [Uni01]. U.S. [Bol02, PM00, Uni00b].

Ubiquitous [Sta03, LKZ +04]. UC-soundness [BPS08]. UCON [LY05, PS04b]. UK [CZ05, Chr00, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01].

Ultimate [Di01]. ultra [Bam02, CH07a, DB04, Cal01, Win00]. ultra-lightweight [CH07a]. ultra-secret [Bam02]. Ultrafast [FF01a]. UltraSONIC [MMH02].

Unauthorized [Ano03e]. Unbalanced [FMP03, May02, HLLO03]. Unbelievable [Len01]. Unborn [Pau02a]. Unbounded [RW02, WvD02]. Unbreakable [Ver06b].

Uncertain [See04, Sty04, Hei03, Sch03]. UNCITRAL [MNFG02]. uncompletable [NS01a]. Unconditional [HM01b, May01, Pas05, RW03b, WW05].

Unconditionally [HSZI00, HSZI01, HSHI02, HSHI06]. Uncovering [MNT +00]. Uncrackable [Ano03c]. undeciphered [Rob02, Rob09].

Undeniable [GMP01b, GM03, JSJK01, Miy01, WQWZ01, CH05, LH04, LCZ05a, SSM +08].

undergraduate [AA04b, Gha07]. undergraduates [DFGH04]. Understanding [AN03, CPG +04, Cra05b, Elb09, Gor06, LG09, PP09, Sun05, Lun09].

undetectable [BMW02b]. Unexpectedly [Bar00a]. Unforgeable [BKY02, KY01a].

Unicode [MJJ07]. Unified [CZB +01, HKA +05, MFS +09, SM03b].

Uniform [SPK08, TL07, SU07]. Uniformity

[Shp01, Shp04b]. Unimodular [CV03]. Unique [Lam91, Lys02, TH01]. United [DFCW00, Jol01]. Universal [BOHL +05, CR03, CJNP02, CS02, Ifr00, KKKP05, KO03, Pli01, Sho00a, SP09, Cal00c, PS04c]. universality [DS02]. Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DN02b, DN03, NMM05, RK05].

Universally-Composable [AF04b]. Universiteit [BBDD09]. University [Kat05b, Puc03, Rot07, Top02]. UNIX [CCDP01, Har01a, Har01b, Høf01, Wit01, GSS03]. UNIX-Type [Høf01]. Unknown [CT08a, Luc02b, CSSW05, HJ07]. Unknowns [CMB +05]. unleash [Mc03]. Unleashing [Lop06]. unlinkability [WHH05].

Unpredictability [BS01d]. unprotected [ASK05]. Unravelling [Ano03e]. Unsolved [GG05a, Bel07a]. untold [DB04]. untraceability [CL09, HLY05, Par04]. Untraceable [ACD05]. Untrusted [BMK00, CGK +02, LS09, LLK05, ZBP05].

Usual [GG05a]. Unveiled [Bar00a]. Update [TEM +01]. Updated [Cho08a]. updating [LH03]. upgrade [Pau02a, Pau02b]. Upgrades [Ano02e].

upon [DFG01, PQ03a]. UPPAAL [BDD +02]. Upper [BP03b, DIRR05, KMT01]. Upwards [V03]. URSA [LKZ +04]. US$54 [Dw03].

USA [ACM03b, ACM04b, ACM05c]. ACM06, ACM07, ACM09, BD08, Des02, Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KKP02, KJR05, Ki05, KP01, Men05, Men07, Nac01, Nao04, Oka04, Poi06, Pre02c, Sch01d, Sho05a, S101, YDKM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FMA02, IE01a, IE05a, IE05b, IE08, IE09b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S +03, Sch04a, Sch04b, Sch05a, SMP +09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, WI99, Yun02a]. usability [CG05, WDCJ09]. Usage [LY05, PS04b].

Use [Bai01a, BWBL02, Bol02, BQR01,
CPS07, Dre00, ISO05, Kra03, LCK04, Pau09, PBTW07, Str01a, WS05, Win01, CG05, OS07, used [CDL06, MSV04]. useful [SM03a]. UseNet [Coc01a]. USENIX [Coc01a]. User [Ano00k, BGP02, CL01b, CMB+05, DP00, FDR00, Had00, HY01, KZ09, LSZ05, MR03, OHB08a, PS01b, Poh01, Sas07, SSM+08, Str01a, Tsao1, WDCJ09, BBM00, CL04d, CCK04b, CHY05b, CKY05, CJK+01, Che07, CKY07, Che08a, Che08b, CJ04, CKK03, Cos00, DZL01, Dan02, DSGP06, DS09, DFG00, FWTC05, GC00a, GMR05, Gen09b, GS09, HHSS01, HWW05, HAU04, HTW07, Hir09, HW04, HLTJ09, HY03, HL04, JRR09, Jua04, KOY09, KCO9a, KLY03, KBO9, KKL09, KJJ+07, KSW06, KR03, Ku04, LC05a, LHY02, LLH02, LKY04, LCP04, LL04b, LW04, LKY05a, LLW05, LLW09, LFW04, LC05a, LCC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SHH07, Tan07a, TLL05, Tsa05, TJC03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04a, YW05, YCO09a, 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 [Ito00]. V5.1a [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BLM01, KCJ+01, BG09, ME08b, VM03]. Validity [Zho02]. Valuable [PM00]. Value [BR09, GIS05, LS08, BMW02a, DK08, WWT08]. valued [DZL01, MS02b]. Vancouver [IEE02]. Varadharajan [CJT03]. Varadrarajan [MS03a]. variable [SV08a].

Variables [HR04a]. Variant [Luc02b, NSK05, Ber08, Duj08, Duj09]. Variants [BDK+09, DG02, KS00b, CJK05, Sha04b, TJC03]. Varieties [RS02]. Variety [AOS02]. Vascular [BDhKB09]. vault [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pei09, mSgFl05, WNQ08, WC05]. vectors [LHL04a]. Vegas [EIvS01, IEE01a]. Vein [BDhKB09]. Vendors [Pau03, MV03b]. Venona [Ben01b, Ben04]. Verenigde [dL00]. Veridicom [Ano02d]. Verifiable [ANR01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Lys02, NZCG05, ...]
NZS05, NSNK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a. Verifiably [BGLS03, Hes04a]. verifiably-encrypted [Hes04a]. Verification [AADK05, Ara02, BPST02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJI06, Coh03, DS00, HL05c, JW01, Ler02, MD04, MT07, MSP09, PBD07, Tsa08, TYH04, Wan04b, Wu01, YLC09, ZLX99, ZL04b, CS08b, Uzu04]. Verified [BJP02, BFGT08, BFCZ08, CJT04]. verifier [Bla01b, LKY05b]. verifier-based [LKY05b]. Verifiers [CL01a, He02, LV07, LWK05b, YY05a, ZX04]. Verify [MS02a]. Verifying [BFG08, BJvdB02, CJM00, HLT01, IR01, PT08, RR02, BLH06, BLP06, HLH00, SV08a, Sha01d]. Verlag [Eag05, Lee03a, Lee03b, Pap05]. Version [Bol02, HPC02, OST05, SKI01, Mis06]. Versions [HSR+01, NPV01, Ano00f, CV05]. Versteckte [Sch09]. Versus [Mad00, Rub00, WWL+02, ASW+01, BJL050, DBS01, WPP05]. Vertically [DN04]. Very [AAC+01, B+02, CG03, EBC+00, FLA+03, Hfö01, PM02, PBMB01, Zir07]. Vestiges [Top02]. VII [Sch04a]. via [AGK07, Ano00k, ACdM05, BDPV09, Car02, Che03, CP+04, FBWC02, Fox00, HHYW07, HLM03, J000a, KT06, ML05, PG05, RG05, SB01, SLG+05, ZL01, Luh05]. Victoria [ACM08, IZ00]. Victorian [Top02]. victory [Hau03]. Vid [CAC06]. Video [BDD+01a, BD03, CDTT05, EFY+05, ISS208, KBD03, KJR05, KLI01, LHS05, MLC01, SC02a, SB01b, C009a, JA02, KN03, UP05]. Video-Based [KJR05, BS01b, KN03]. videos [YZDW07]. Vienna [BZ02]. Vietnam [Lov04]. View [Bar00a, Mah04, Sin09]. Views [Bar00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03]. Vigenère [DG00]. VII [Sch04b]. VIII [IEE01b, Sch05a]. Virginia [MS05b]. Virtual [Ano01c, HM01a, Pro00, YSS+01, BDS+09a, ML05, ZBP05]. virtualization [CGL+08a, CGL+08b, CGL+08e]. virtualization-based [CGL+08a, CGL+08b, CGL+08e]. Virtues [Tro08]. Virus [Gor06, Ano05c]. Visible [HT06]. Vista [Fer06]. Visual [BDN00, BDS03, BCD06, CCL09, CTY09, CPD06, DD00, Kog02, KS03, RD09, WMS08, YWC08, YC01, Z09, ABD01, CDFM05, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Z01]. Visualization [XYL09, MFS+09]. Viterbi [LBGZ01, LBGZ02]. Vladimirov [Puz04]. VLDB [EBC+00, FLA+03]. VLDP [B+02]. VLSI [KV01]. VMSS [SC05a]. Voice [Ano00l, PK01, VN04]. VoIP [Ano08c, SZ08, VAYV09, WCJ05]. vol [Kat05b, Lee03b]. volatile [SETB08]. Volume [Gol04]. Vortrag [Eke02]. Voter [Cha04]. Voter-Verifiable [Cha04]. Voting [Cha04, FPS01, HS00, Joh05, JLL02, KMO01, Rub01, CJT03, HJW05]. Voynich [Rug04]. VPN [KKM+06]. VPNS [Dav01a]. VQ [WJP07]. VQ-based [WJP07]. Vs [CTB+01, Di01, DI03, SU07, WW04]. VSS [AF04b, CDF01, FM02a]. Vu [DP00]. vulnerabilities [CS05, DMS07, Swi05, XNK+05]. vulnerability [KHL09, SGA07, YRS+09]. WA [ACM06]. WACs [Kov01]. Wagner [DVP06]. Wagstaff [Kat05b]. Wahab [MAaT07]. Walking [Fox00]. Wallet [ETZ00, JL04]. Walsh [MS02b]. Walsingham [Bud06]. WAN [Hf01]. WAN-Cluster [Hf01]. Wang [SZS05]. Wants [Hau00]. WAP [JRFH01]. War [Bec02, Bud00a, Bud02, Han03, Kov01, MH09, OC03, AJ08, DB04, Ris06, Lov01]. Warfare [HW01, WW04]. warrior [PC04]. Wars [RR03b]. Warsaw [AUW01, Bih03].
Washington [S+03, USE00a, USE01c]. wasn’t [Bur02]. WaSP [Coc02b]. WASSA [Ano05c]. Watch [MA00a, Joy03a].

Waterloo [HH04, HH01, ST01d].

Watermark [AS01b, GMV01, JX05, KHY04, Kwo03a, Meh01, PBB02, RE02, SY01a, CAC03, TH01, WY02, Zau01, AA08, CL08, LGY07, LCC06a].

Watermark-based [Kwo03a].

Watermark-Fingerprint [KHY04].

Watermarked [ST01c]. Watermarking [AS03, AK02b, AHK03b, AS01c, Arn01, ARCl+01, BBCl+09, BR09, BS01a, BS01b, BSL02, BQR01, BSNO00, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB+08, DWN01, DNP07, EIGl+05, EIG01, GW01, HT06, HH09, JKKl+01, KCR04, hKL08, KLL01, Kum01, KT00, LZ09, LLS05a, LKL05, LZ01, LZP+04, LWS06, LLO05b, LSC03, LL01, LSK05, MM01a, MNO01, Nak01, OMT02, PJJ01, PJK01, PR01, PBM+07, Qo01, Sam01, SOH01, SDH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLO01, SPK08, VVS01, VHP01, VK07, WC09, WH09, WNY09, WVL+02, WL0105b, XFZ01, YWWS09, ZTP05, ZWC02, AHK03a, AAPP07, BCKK05, CC02b, Che08b, CYHl+07, CCD+l04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GAO3, HLC07, HHC05, JD01, JA02, KA09, KP00, LDD07, LNO00a, LNO1b, LCC06a, LCC06b, MB08, MCH05].

watermarking [PK03, Ren09, mSgFl05, WJP07, WNO08, Way02b, Way09, WC05, WMDR08, XTM07, YZDW07, YPSZ01, ZLZ07].

Watermarks [Ben00, BB00a, MLC01, SNG01, WC03a, WC04, YLLL02, MB08, TND+09].

Watershed [FBW01]. Watershed-from-Markers [FBW01]. WAV [XFZ01]. WAV-Table [XFZ01].

Wavelet [BR09, GW01, LKL05, LZ01, Nak01, VK07, AAPP07, AA08].

wavelet-based [AAPP07, AA08]. Wavelet-Domain [LZ01]. WAVES [LBA00]. Way [BYJK08, BM01a, CHL02, DIS02, DMS00, FIS01b, GKK+09, HNO+09, HR05, KO03, KO00, LTW05, Sh000a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, KK07, KK05, KK03, LW04, LPM05, LQ08, LKJL01, Mic02a, PO00, Tsa08, YW05, YRY05b, ZW05a].

Wayness [KI01a, PV06b]. Ways [BB02]. WCC [Ytr06]. WDDL [MMT09]. Weak [HG03, LS01c, RW03b, DW09, GG08, KOY09, KW00]. Weakening [ZD05].

Weakly [BS00a, CHS05]. Weakness [SW05, SZA05, YPKL08]. Weaknesses [FMS01, Hc02, KCL03, KCC05, SGGB00].

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

Web [Mar05a, BFG05, BFG08, HI06, AN01c, AN02e, AN03c, AVE+07, BFG04, BC04b, CC01c, COC01a, COC02a, COC02b, CZB+01, DE07, DMS09, FSS01, GSO2a, GSVC02, HM05, JRB+06, KCD07, LWK00, LLS05b, LXM+05, MPM09, PM00, RR04, Sam09, SSS06, Sch01a, SB07, TMM10, WA06, YSS+01]. Web-Based [AN01c, Sch01a, YSS+01]. Web-enabled [CC01c]. webcam [Mc03].

WebFountain [AN03c]. Webrelay [Zha00]. Weight [CH07c, G02, WT02].

Weighted [BTW05, BTW08, SC02c, YZ00].

Weil [BF01b, BF03, Jou02, Kir03].

Well [WWG00]. Welschenbach [Ter08].

Welsh [Rot07]. went [AJS08]. WEP [SIR04]. were [Han06].

Wesley [Puc03].

West [FR01, JU04, SVY02, WRI03].

Westbridge [Ant02e].

Western [CZB+01]. Wet [CC09].

Weyl [NAG03]. WG [DFPS06]. WG11.1 [ELvS01]. WG11.1/WG11.2 [ELvS01].

WG11.2 [ELvS01]. WG8.8 [DFCW00].

Wheeler [ABM08, Bar05]. Where [Bur06, Pen01a].

While [Te06]. WHIM [JAN02]. WHIRLPOOL [RB01]. Whisper [NAGB03]. Whitening [Oni01].
Who [CZB+01, Urb01, Hau06]. whole [CPG+04]. Wi
[Fig04, Sty04, VGM04, FMA02, Bar03]. Wi-Fi [Sty04, Bar03]. Wi-Fi
[Fig04, VGM04]. wicked [Lud05]. Wide [DR02a, SBB05]. Width [OT03b]. Width-
[OT03b]. Wiener [Duj08, Duj09]. WIESS [USE00b]. Wiley [And04, Gra01, Kir01a]. Will
[Ort00, Cla00b, Fur05]. William [Pag03]. Williams [M¨ul01a]. Window
[OT03a, SSST06]. Windows
[USE00a, DGP07a, DGP07b, DGP09, Fer06, HB06, WD01a, Win01]. Wins
[Bar00b]. Wired [Gil07, Pot07, SIR04]. Wireless
[AEAQ05, Bar03, BCH+00, ECM00b, Fin06, KH05, KHD01, LNL+08, Pan03, PZDH09, Pot03, Puz04, Sin01a, Sty04, SYL05, VGM04, YSR01, ZYN08, ZWCY02, Bad07, BP03a, BB04, BGH07, Har06, NA07, Ano03b, CH01a, CCK04b, CYH04, CNV06, DK01, KG09, Ku04, LV07, LHL04b, LW04, LKY05b, LL06, Lin01a, LCZ05b, Lys07, MP02, Mar07, PS04c, RG09, Tsa08, WH01, YW05, YYY05b, 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]. Word-lengths [PG05]. words
[GS01, Max06, NS01a, VS01]. Work
[DFG01, DNW05, Fox00]. Working
FJ04, FL01b, GA03, Her02, LC04b, PCK02, RR04, ÜG08, U01, UST01a. XMT [SG07].
XrML [Bar00a]. XTEA [CV05, HHK +04, MHL +02]. XTR [LW02, LV00, LNS02, Ver01].

Yahalom [Pau01]. Yang [McK04, CZ03, KJY05, WL05, YWC05].
Yang-Shieh [YWC05]. Yo [BPS08, BDNN02, ZD05]. Yao-style [BPS08].
Yarrow [KF00, Mur02]. Yarrow-160 [KS00]. Yaschenko [Kat05b].
YCH [SC05a]. YCN [Hwa00]. Year [Naz02, Bur00]. Year[s] [Alz08, CM02].
Yellow [JYZ04]. Yen [LLLZ06a, LLLZ06b].
Yen-Guo [LLLZ06a]. Yesterday [Coc02a].
Yi [Wag00]. Yi-Lam [Wag00]. Yokohama [Mat02].
You [Wag00]. Young [BP04, Cou01, DDP04, DFS04, DDO +01, HNO +09, IKOS07, LMS05, LHL +08, MR01b, MV03a, Pas05, Ros00, Ros06a, CSW05, Dam00, PBD07, KV07].
You’ve [Nic01]. Yuck [Sas07]. Yuen [KH08].

Z [Wue09]. Z-parameter [Wue09]. z10 [Web08]. z9 [ADH +07]. Zealand [Zhe02b].
Zeilinger [Duw03]. Zero [AS01b, APV05, BP04, Cou01, DPV04, DFS04, DDO +01, HNO +09, IKOS07, LMS05, LHL +08, MR01b, MV03a, Pas05, Ros00, Ros06a, CSW05, Dam00, PBD07]. Zero-Knowledge [AS01b, BP04, Cou01, DFS04, HNO +09, LHL +08, MR01b, MV03a, Pas05, Ros00, Ros06a, IKOS07, Dam00, PBD07].
Zeta [Ver02]. Zhang [JW01, YY05a]. Zhou [PKH05]. Zimmermann [McL06, Tuc86]. ZK [PBD05].
Zodiac [HSM +02].

References


Apers:2001:PTS


Al-Azzoni:2005:MVC


Anshel:2001:NKA


Almgren:2000:HWC


Ababneh:2009:CSE

REFERENCES

Ashraf:2009:SBE


Aamodt:2003:CSP


Agreste:2007:IAW


An:2001:DER


Atallah:2009:ATC


Abadi:2000:TA

[Aba00] Martín Abadi. Taming the adversary. In Bellare [Bel00], pages 353–??
REFERENCES


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


Adjeroh:2008:BWT [ABM08] Donald Adjeroh, Tim Bell, and Amar Mukherjee. The Burrows–Wheeler Transform: Data Compression,
REFERENCES


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

Ateniese:2000:PPS


ACM:2000:PTS


ACM:2001:PAA


ACM:2002:PTF

REFERENCES


REFERENCES


REFERENCES


[ADI09] Jithra Adikari, Vassil Dim-


[AEV+07] Annie I. Antón, Julia B. Eart, Matthew W. Vail, Neha Jain, Carrie M. Gheen, and Jack M. Frink. HIPAA’s effect on Web site privacy policies. IEEE
Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR


Attrapadung:2006:FSS

REFERENCES


REFERENCES

Ateniese:2005:PRS

Agrawal:2003:SWR
Rakesh Agrawal, Peter J. Haas, and Jerry Kiernan. A system for watermarking relational databases. In ACM [ACM03a], page 674. ISBN 1-58113-634-X. LCCN ????.

Agrawal:2003:WRD

Armington:2002:BAI

Ahmad:2007:CSS

Ahmad:2008:ATT

Ahmadi:2008:PFS
O. Ahmadi, D. Hankerson, and F. Rodríguez-

Askarov:2008:CMF


Aoki:2001:CBB


Applebaum:2004:CNS


Applebaum:2006:C


Al-Ibrahim:2001:AMS

M. Al-Ibrahim and J. Pieprzyk. Authenticating multicast streams in lossy channels using threshold techniques. *Lecture Notes in Computer Science*, 2094:


Gildas Avoine, Pascal Junod, and Philippe Oechslin. Characterization and improvement of time-memory trade-off based on perfect tables. *ACM Transactions*
REFERENCES


Al-Jarrah:2008:NKM


Abe:2002:KES


Agrawal:2002:WRD


Armknecht:2003:AAC


Akinwande:2009:AHC

REFERENCES


Atallah:2004:ALA


Atzeni:2006:PKI


Anshel:2007:RME


Allen:2003:EST


Allman:2006:MAW


Alvarez:2000:SMC

REFERENCES


See [kWpLwW01, WLW04].


REFERENCES

Andem:2003:CTE


Anderson:2004:BRR


Anderson:2007:SSS


Anderson:2008:SEG


Aura:2001:RAC


Anonymous:2000:AIH

[Ano00a] Anonymous. Author in-

Anonymous:2000:CRR


Anonymous:2000:CCI


Anonymous:2000:CLI


Anonymous:2000:EES


Anonymous:2000:GBE


Anonymous:2000:PESa


Anonymous:2000:PTD

REFERENCES

Anonymous:2000:SES

Anonymous:2000:UAS

Anonymous:2000:VAS

Anonymous:2001:AAPb

Anonymous:2001:ANT

Anonymous:2001:AWB

Anonymous:2001:AIgb


Anonymous:2001:EER


Anonymous:2001:EMB


Anonymous:2001:LBS


Anonymous:2001:PKC

Anonymous. Public-key crypto-systems using symmetric...

Anonymous:2001:SCS


Anonymous:2002:NSD


Anonymous:2002:PPD

Anonymous. Products: Palm Digital Media’s eBook publishing tools; Veridicom’s fingerprint authentication module; high-speed debugging tool for Macraigor Systems; QNX launches IDE for embedded programming; Extreme Networks’ network management tools; Parascript’s handwriting recognition SDK; system debugger tool from Compuware. Computer, 35(8):74–??, August 2002. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).


Anonymous:2003:TMC


Anonymous:2003:NAW


Anonymous:2003:NUP


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>
<th>Anonymous:2003:UCD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>[Ano03a]</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>P. A. Cataldi</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>L. Euler</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>I. M. Pervushin</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>R. E. Powers</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1913</td>
<td>E. Fauquembergue</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1876</td>
<td>E. Lucas</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1952</td>
<td>R. M. Robinson</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>R. M. Robinson</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>R. M. Robinson</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>R. M. Robinson</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1957</td>
<td>H. Riesel</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>1963</td>
<td>D. B. Gillies</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson &amp; D. Stinson</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>1988</td>
<td>W. N. Colquitt &amp; D. Slowinski</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>B. Slowinski &amp; Gage</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>75639</td>
<td>1992</td>
<td>Slowinski &amp; Gage</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>85943</td>
<td>1994</td>
<td>Slowinski &amp; Gage</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski &amp; Gage</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud et al. (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, Woltman</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala et al. (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>2001</td>
<td>M. Cameron (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>M. Slater (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2004</td>
<td>Josh Findley (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2005</td>
<td>Martin Nowak (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>30402457</td>
<td>2005</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich, George Woltman, Scott Kurowski (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, George Woltman, Scott Kurowski (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2013</td>
<td>Curtis Cooper, George Woltman, Scott Kurowski, and others</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>74207281</td>
<td>2016</td>
<td>Curtis Cooper (GIMPS)</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>77232917</td>
<td>2018</td>
<td>Jon Pace (GIMPS)</td>
<td></td>
</tr>
</tbody>
</table>
REFERENCES


Anonymous:2005:CEC


Anonymous:2005:SCB


Anonymous:2005:WAS


Anonymous:2006:JHD


Anonymous:2006:RC


Anonymous:2006:SSD


Anonymous:2006:SQE


Anonymous:2007:CPSh

Anonymous. Call for papers for special section on special-purpose hardware


<table>
<thead>
<tr>
<th>REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymous:2013:DSS</strong></td>
</tr>
<tr>
<td><strong>Ateniese:2001:SRC</strong></td>
</tr>
<tr>
<td><strong>Amir:2001:FAA</strong></td>
</tr>
<tr>
<td><strong>ANSI:2005:AXP</strong></td>
</tr>
</tbody>
</table>

Abe:2000:PSP


Abe:2002:SVK


Alomair:2009:ITS


Appenzeller:2005:IBE


Applebaum:2007:CCP

REFERENCES

Alwen:2005:IFR


Abdalla:2000:NFS


Arboit:2001:FLM


Araki:2002:NRS


Atallah:2001:NLW

Aaraj:2008:ADH


Arkin:2005:CND


Arnold:2001:AWB


Agrawal:2003:MCA


Artail:2004:PAC

Abe:2001:SPA


Adelsbach:2001:ZKW


Agung:2001:ICI


Adelsbach:2001:ZKW


Agung:2001:ICI


Agarwal:2008:DWS


Asenjo:2002:AES


Ashburn:2003:PBA

Julian Ashburn. Practical Biometrics: From Aspiration to Implementation. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
REFERENCES


Aciicmez:2005:IBB


Aciicmez:2007:MAC


Aslan:2004:HSM


Aslan:2004:LAA


Blanchet-Sadri:2001:MSD


Abdalla:2000:KMR


Allison:2001:LLE

[Dennis Allison, Randy Schrickel, Reid Womack, Jeremy C. Reed, Ashley

**Ateniese:2004:VED**


**Androutsellis-Theotokis:2004:SPP**


**Aharonov:2000:QBE**


**Alster:2001:PKC**


**Arnold:2004:IPN**

Avanzi:2003:CAD


Aalberts:2000:DSB


Abadi:2005:SAC


Ayoade:2006:SIR


Bernstein:2002:VPT

Philip A. Bernstein et al., editors. VLDP 2002: proceedings of the Twenty-Eighth International Conference on Very Large Data Bases, Hong Kong SAR,
Blanton:2006:SRF


Bagnulo:2002:PAA


Badra:2007:AWC


Baier:2001:ECP


Baier:2001:ECS

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(7):18, July 2000. CODEN DDJOEB. ISSN 1044-789X.

[Bar00b] Nicholas Baran. News and views: More on tiny transistors; Open Source repository launched; design contest promotes new software tools; and then there’s a decryption contest; Fred Brooks wins ACM Turing Award. *Dr. Dobb’s Journal of Software Tools*, 25
REFERENCES


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

Barr:2002:IC

Barkan:2006:CCP

Barker:2006:ROA

Bard:2009:AC
Gregory V. Bard. Algebraic cryptanalysis. Springer-Verlag, Berlin, Germany / Hei-
REFERENCES

[125]
delberg, Germany / Lon-
don, UK / etc., 2009. ISBN 0-387-88757-1 (ebook), 0-
387-88756-3. xxxiii + 356 pp. LCCN Z103 .B37 [Bau01c]
2009eb. URL http://
link.library.utoronto.caeir/EIRdetail.cfm?Resources\_\_ID=896123&T=F.

[Bau00]
Friedrich Ludwig Bauer. Decrypted secrets: meth-
ods and maxims of cryptol-
ogy. Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
many / London, UK / etc.,

[Bau01a]
Mick Bauer. Paranoid pen-
noframes.linuxjournal.com/lj-issues/issue89/4828.html.

[Bau01b]
Mick Bauer. Paranoid pen-

[Bau01c]
Mick Bauer. Paranoid pen-

[Bau02a]
Friedrich Ludwig Bauer. Decrypted secrets: meth-
ods and maxims of cryptol-
ogy. Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
many / London, UK / etc.,
third edition, 2002. ISBN 3-
540-42674-4. xii + 473 pp.

[Bau02b]
Mick Bauer. Paranoid pen-
guin: BestCrypt: Cross-
platform filesystem encrypt-

[Bau03a]
Mick Bauer. Paranoid pen-
REFERENCES

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

Bauer:2003:PPAb

Baudet:2005:DSP

Bauer:2007:DSM

Blakley:1979:RSA

Benedens:2000:TBD

Buchmann:2000:ECC
REFERENCES

Barkan:2002:HMW

Bouda:2003:EQI

Boneh:2004:SIB

Bicakci:2005:ISA

Biham:2002:SQK

Basso:2009:NBB
REFERENCES


Behrmann:2002:UIS


Bernstein:2009:PQC


Beimel:2000:CFS


Bellare:2001:KPP


Blumenthal:2002:SAD

Uri Blumenthal, Milind M. Buddhikot, Juan A. Garay, Scott C. Miller, Sarvar Patel, Luca Salgarelli, and Dorothy Stanley. A scheme for authentication and dynamic key exchange in wireless networks. Bell Labs
REFERENCES

Bartolini:2008:EIS


Barkan:2003:ICO


Bertoni:2003:EAD


Bellare:2001:OCH


Bellare:2000:PKE

Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryp-
REFERENCES


Eli Biham and Rafi Chen. Near-collisions of SHA-0. In Franklin [Fra04], pages 290–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN
REFERENCES


Blundo:2004:SIA[BC04b]


Backes:2005:PKS[BC05a]


Bergadano:2005:DPL[BC05b]


Blundo:2005:SCN

Brzezinski:2005:MRL


Bergadano:2001:CSA


Blundo:2006:VCS


Bruguer:2009:PIS

Javier D. Bruguera, Marius Cornea, Debjit Das-
REFERENCES


REFERENCES

134

SCPGRD4. ISSN 0167-6423 (print), 1872-7964 (electronic).


[BCLP01] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably authenticated group Diffie–Hellman key exchange — the dynamic case. *Lecture Notes in
REFERENCES


Bresson:2002:DGD


Bresson:2002:GDH


Bolle:2003:GB


Bresson:2007:PSA


Bellavista:2002:JLD

REFERENCES


Bozzano:2004:AVS


Burmester:2004:HPK


Buchmann:2008:PQC


Biryukov:2003:CS


Blundo:2003:COT

Bolosky:2000:FSD


Bao:2001:SPD


Bodei:2002:PAP


Bodei:2005:APS


Bao:2001:CTS

REFERENCES


[BDM00] Carlo Blundo, Alfredo De Santis, and Moni Naor. Vi-

**Bodei:2002:FLD**


**Boreale:2002:PTC**


**Bertoni:2009:RPK**


**Biryukov:2004:MLA**


**Baldwin:2009:PSS**

REFERENCES


REFERENCES

Beebe:2005:CBPd

Bejtlich:2006:EDS

Bellare:2000:ACC

Bella:2001:MPS

Bellovin:2004:IRS

Belfield:2007:SUC
Richard Belfield. The six unsolved ciphers: inside the mysterious codes that have confounded the world's greatest cryptographers. Ulysses, Berkeley, CA, USA, 2007. ISBN 1-56975-628-7 (paperback). ix
REFERENCES


REFERENCES


[Ber09a] Seth D. Bergmann. Degenerate keys for RSA encryption. SIGCSE Bulletin (ACM Special Inter-
REFERENCES


REFERENCES

0167-8191 (print), 1872-7336 (electronic).


CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

**Biham:2002:DCQ**


**Brown:2007:SAN**


**Bugliesi:2007:SIT**


**Blaszczyk:2008:NMT**


**Blaszczyk:2009:EVT**


**Barthe:2009:FCC**

Gilles Barthe, Benjamin Grégoire, and Santiago Zanella.
REFERENCES


Boneh:2007:SEI


Bennett:2002:ESE


Bogomjakov:2008:PMD


Bertoni:2003:EAA


Barak:2001:IPO

REFERENCES


REFERENCES


Bialaski:2000:SLN


Barak:2005:MAP


Badra:2006:KEA


Backhouse:2003:TOT


Bajard:2004:FRI


Barkol:2005:SCC

REFERENCES


Biham:2003:ACE

[102x681]
[102x624]Biham:2003:ACE
[102x276]

References

Biham:2003:ACE


Bajard:2003:EMG


Bajard:2005:AOP


Biryukov:2007:FSE


Beimel:2000:RSC

[102x681]
[102x228]

References

Beimel:2000:RSC


Bir07

[102x276]
REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


REFERENCES

CODEN ???? ISSN
1549-8328 (print), 1558-
0806 (electronic). URL
org/stamp/stamp.jsp?tp=
&amp;arnumber=4432925.

Michael Andrew Black. A
treatise on data encryp-
tion and an example of
the black algorithm. The-
sis (M.A.), University of
California, Santa Barbara,
Santa Barbara, CA, USA,
2000.

Bruno Blanchet. Abstract-
ing cryptographic protocols
by Prolog rules. Lecture
Notes in Computer Science,
2126:433–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2126/21260433.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2126/21260433.
pdf.

Bruno Blanchet. An effi-
cient cryptographic proto-
col verifier based on prolog
rules. In ????., editor, IEEE
Computer Security Founda-
tions Workshop, page 82.
IEEE Computer Society
Press, 1109 Spring Street,
Suite 300, Silver Spring, MD
20910, USA, 2001. ISBN
???? LCCN ???? URL
????.

Matt Blaze. Loaning your
soul to the devil: Influencing
policy without selling out,
2001. Unpublished invited
talk, Tenth USENIX Secu-
ry Symposium, August 13–
17, 2001, Washington, DC,
USA.

Bruno Blanchet. From se-
crecy to authenticity in se-
curity protocols. Lecture
Notes in Computer Science,
2477:342–??, 2002. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2477/24770342.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2477/24770342.
pdf.

Matt Blaze. Cryptography
and insecurity. In USENIX
[USE02a], pages viii + 151.
ISBN 1-880446-02-2. LCCN
QA76.76.O63 B736 2002.
URL http://www.usenix.
org/publications/library/
proceedings/bsdcon02/tech.
html. Unpublished in-
vited talk, BSDCON2002:
REFERENCES

Growing the BSD Community, February 11–14, 2002, Cathedral Hill Hotel, San Francisco, CA.

Blaze:2003:FCI

Bao:2006:CIB

Berbecaru:2001:CPK
Diana Berbecaru, Antonio Lioy, and Marius Marian. On the complexity of public-key certificate validation. Lecture Notes in Computer Science, 2200:183–??, 2001. CODEN LNCS-D9. ISSN 0302-
References

Brassard:2000:SAP


Bozga:2006:PBA


Blunden:2009:RAE

Bill Blunden. The rootkit arsenal: escape and evasion in the dark corners of
REFERENCES

Batina:2001:AWD

Blomer:2001:LSE

Brincat:2001:KRA

Basu:2003:AC

Blomer:2003:NPK
REFERENCES

Boyd:2003:PAK

Burke:2000:ASFa

Burke:2000:ASFb

Boneh:2000:GRK

Biehl:2000:DFA
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
[BWM02a] Niklas Borselius, Chris J. Mitchell, and Aaron Wil-

**Borselius:2002:PAU**


**Boyen:2005:DCC**


**Bellare:2000:AER**


**Boneh:2000:TC**


**Bellare:2002:TSB**

REFERENCES


REFERENCES


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


[BP03b] Niv Buchbinder and Erez Petrank. Lower and
REFERENCES


Bellare:2004:KEA


Bellare:2000:AKE

REFERENCES


REFERENCES

530, ???. 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Benerecetti:2002:VST


Brandao:2001:UEC


Bellare:2000:ETE


Black:2000:CMA

REFERENCES


REFERENCES


REFERENCES

175


REFERENCES


**Biryukov:2001:SCS**


**Boneh:2001:UBE**


**Bajard:2003:ISC**


**Barrett:2005:SSS**


**Bo:2001:EID**

Xiaochen Bo, Lincheng Shen, and Wensen Chang.

Bo:2001:SCD


Bounkong:2002:ICA


Brisbane:2000:RBW


Bresson:2002:TRS

REFERENCES

http://link.springer.de/link/service/series/0558/bibs/2442/24420465.htm;

Blake:2004:AEC


Blake:2005:AEC


Bhargav-Spantzel:2007:PPM


Buchmann:2002:ICP


Barak:2003:TRN

Boaz Barak, Ronen Shaltiel, and Eran Tromer. True random number generators secure in a changing environment. In Walter et al. [WKP03], pages 166–
REFERENCES


[BSW01] Alex Biryukov, Adi Shamir, and David Wagner. Real
time cryptanalysis of A5/1 on a PC. Lecture Notes
in Computer Science, 1978:1–??, 2001. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349
link/service/series/0558/tocs/t2779.htm; http://
issn=0302-9743&volume=2779; http://www.springerlink.
b13240.

Biehl:2002:NDP

[BT02] Ingrid Biehl and Tsuyoshi Takagi. A new distributed
primality test for shared RSA keys using quadratic
fields. Lecture Notes in Computer Science, 2384:
1–??, 2002. CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http://
link.springer-ny.com/link/service/series/
0558/papers/2384/23840001.pdf.

Boyer:2002:LDS

[BTTF02] John Boyer, Andrew D.
Todd, Jason Trenough, and Doug Farrell. Letters:
Defective sign-and-encrypt and healthcare woes and
J2EE cache and pool and Regex++. Dr. Dobb’s Jour-
nal of Software Tools, 27(2):10, February 2002. CO-
DEN DDJOEB. ISSN 1044-
ddj.com/.

Bethencourt:2009:NTP

[BSW09] John Bethencourt, Dawn
Song, and Brent Waters. New techniques for private
stream searching. ACM
Transactions on Information and System Security,
12(3):16:1–16:??, January
2009. CODEN ATISBQ.

Beimel:2005:CIW

[BTW05] Amos Beimel, Tamir Tassa,
and Enav Weinreb. Characterizing ideal weighted
threshold secret sharing. In Kilian [Kil05], pages 606–
?? CODEN LNCSD9.
REFERENCES


operation. Intelligence and National Security, 15(2):49–??, 2000. ISSN 0268-4527 (print), 1743-9019 (elec-
tronic).


abeth I, Sir Francis Walsing-


[Burnett:2001:CB] Steve Burnett. Crypto blun-
db.usenix.org/publications/
library/proceedings/lisa2001/
tech/. Unpublished in-
vited talk, LISA 2001:

**Burke:2002:IWA**


**Burr:2003:SAE**


**Bur06**

William E. Burr. Cryptographic hash standards:


**Boesgaard:2004:RNH**


**Baker:2007:ISU**


**Blake-Wilson:2002:RUE**


REFERENCES


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


California Metropolitan Transportation Commission. TransLink smart card: universal transit card for the San Francisco Bay Area. Tech-
REFERENCES


REFERENCES


Yacine Challal, Abdelmadjid Bouabdallah, and Hatem Bettahar. H2A: Hybrid

Cooper:2005:AAP


Chandramouli:2006:BPA


Cachin:2000:OFS


Carline:2002:NWT

REFERENCES


### REFERENCES

**Chang:2005:ASN**


**Chang:2005:EAP**


**Comon:2005:TAO**


**Chuang:2006:USF**


**Chen:2008:SNI**


**Chang:2009:FDI**

REFERENCES


REFERENCES


Christianson:2005:SPI

Castelluccia:2009:EPS

Chen:2008:NMA

Caboara:2008:GBP
Massimo Caboara, Fabrizio Caruso, and Carlo Traverso. Gröbner bases for public key cryptography. In Jeffrey [Jef08], pages 315–324. ISBN 1-59593-904-0. LCCN ?????

Choi:2002:IPP
Dug-Hwan Choi, Seungbok Choi, and Dongho Won. Improvement of probabilistic public key cryptosystems using discrete logarithm. Lecture Notes in
REFERENCES


REFERENCES


Ceselli:2005:MAI

Cimato:2005:ICV

Cramer:2005:CMS
REFERENCES

Cramer:2005:SCP


Cavallar:2000:FBR


Cortier:2006:SAP


Cramer:2000:GSM

REFERENCES


Chen:2005:NVW


Ceravolo:2004:ERH


Certicom:2004:CCC


Canetti:2001:UCC


Canteaut:2001:COR


Cramer:2002:OBB

Ronald Cramer and Serge Fehr. Optimal black-box


Cramer:2005:BBS

Climent:2006:NEC

Chodowiec:2003:VCF

Cranor:2005:SUD

Candebat:2006:SPM
Thibault Candebat and David Gray. Secure pseudonym management using mediated identity-based
REFERENCES


REFERENCES


[Chen:2008:OVBa] Xiaoxin Chen, Tal Garfinkel, E. Christopher Lewis, Pratap Subrahmanyan, Carl A.
REFERENCES


Chin-Chen Chang and Kuo-Feng Hwang. Towards the forgery of a group signature without knowing the group center’s secret. Lecture Notes in Computer Science, 2229:47–??, 2001. CO-
REFERENCES

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL [CH07b]
http://link.springer-ny.com/
link/service/series/0558/bibs/2229/22290047.htm;

link/service/series/0558/bibs/2195/21950812.htm;

http://www.lirmm.fr/arith18/.

http://www.lirmm.fr/arith18/.


[Cha05a] Alvin T. S. Chan. Mobile cookies management on a
REFERENCES

Chandra:2005:BWS

Chakrabarti:2007:GCS

Chen:2000:JCT

Chen:2004:MCK

Chen:2005:EUG

Chen:2001:NEA
Chen:2001:DEU


Chen:2001:PDP


Chen:2003:PPO


Chen:2004:IAM

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

Cheng:2004:BSD


Chen:2005:TSS


Chen:2007:CIS


Chen:2008:CIS


Chen:2008:MWS


Coulter:2001:GAH

Robert S. Coulter, George Havas, and Marie Hen-


REFERENCES

Coron:2001:GGC


Coron:2001:OCC


Coppersmith:2002:CSC


Canetti:2003:FSP

REFERENCES


Canetti:2005:ASN


Cheon:2008:PST


Chao:2009:HCS


Chen:2002:CPK


REFERENCES

Canetti:2005:HAW


Chen:2002:AMT


Cornea:2002:SCI


Churchhouse:2002:CCJ


Canvel:2003:PIS

REFERENCES

Chang:2005:ILW

Chang:2005:NMS

Cimato:2002:DAP

Cheon:2003:PTA

Chien:2003:HAP
[CJ03b] Hung-Yu Chien and Jimm-

Chien:2003:NHA


Chien:2003:RSA


Chien:2004:IAM


Chen:2005:EDS


Cornwall:2004:AAM

REFERENCES


REFERENCES


Canetti:2002:SAI


Canetti:2002:UCN


Cheon:2002:IID


Chung:2003:EPX

REFERENCES

Chun:2003:DLC


Cox:2005:DWT


Chen:2009:SRP


Coppersmith:2000:KRF


Coron:2000:FLA

REFERENCES

Coron:2001:SSL

Canetti:2003:RCC

Cheon:2006:KPC

Cachin:2001:SEA

Cathalo:2003:NTT
Julien Cathalo, François Koeune, and Jean-Jacques Quisquater. A new type of timing attack: Application to GPS. In Walter et al. [WKP03], pages
REFERENCES


[CL01a] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with appointed verifiers. In Kilian [Kil01a], pages 388–
REFERENCES


Chang:2001:CIU


Camenisch:2002:DAA


Camerich:2002:TKE


Crowley:2002:BLS


Camenisch:2004:SSA

Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Franklin [Fra04],
REFERENCES


Chang:2004:CGS


Chang:2004:IDM


Chang:2004:RFB


Camenisch:2005:FTO


Chandramouli:2007:ISS


Chang:2008:AWM

REFERENCES

Chien:2009:EBL


Clark:2000:TNE


Clark:2000:LNC

[ Cla00b] Julie Clark. Looking for new contactless points: Hong Kong’s Octopus smart card could get a lot smarter, but it will have to pick its way carefully through regulations and competition from other quarters first. *ITS international*, 6(2):77–78, March/April 2000.

Chen:2008:RCE


Chang:2001:ASM


Chang:2001:FAM

REFERENCES

Cheon:2000:NBC


Canetti:2002:UCT


Chen:2009:AKD


Chang:2007:SIH


Clulow:2003:SP

Czumaj:2002:PTA


Camenisch:2000:CSS


Cox:2002:FYE


Courtois:2003:AAS


Chevallier-Mames:2005:ECB

REFERENCES

Cojocaru:2005:ISM

Cox:2002:DW

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

Cremers:2006:ISE
REFERENCES

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


Caputo:2009:DIT


Crawford:2002:FEE


Coron:2004:SSL


Ciem:2003:PF


Catalano:2002:HHL


Correia:2006:CAB

Miguel Correia, Nuno Ferreira Neves, and Paulo

Cetin:2009: NSA

Cetin:2009: NSA


Cob04


Cob04

Cochran:2001:NVS

Cochran:2001:NVS

Shannon Cochran. News and views: Scientists seek immersive reality; USENIX names lifetime achievement recipients [the GNU Project and the Kerberos network authentication system]; robots need programmers; evangelizing the Semantic Web; get your supercomputer software free; Usenet creator Jim Ellis dies; DARPA funds FreeBSD security initiative. *Dr. Dobb’s Journal of Software Tools*, 26(9):
Cocks:2001:IBE


Cochran:2002:NVSb


Cochran:2002:NVW


Cochran:2003:NVC


Cohen:2003:FOV

REFERENCES


REFERENCES


Coron:2006:WC


Cosgrave:2000:NTC


Costlow:2003:BIM


Courtois:2001:EZK


Courtois:2003:FAA


http://comjnl.oxfordjournals.org/cgi/reprint/49/1/97

Chow:2004:UDL


Chen:2004:SEP


Catalano:2004:IIP


Canetti:2007:CSH


Ciet:2001:SFC

REFERENCES

Canetti:2003:UCJ

Crampton:2005:UDR

Crenshaw:2000:SPK

Crowley:2001:MFL
Chhabra:2009:MSP


CRI:2000:DPA


Cramer:2000:SSB


Cramer:2002:UHP


Camenisch:2003:PVE


Cramer:2003:DAP

Ronald Cramer and Victor Shoup. Design and analysis of practical public-
key encryption schemes secure against adaptive chosen ciphertext attack. [CS03c]


Brian Carrier and Clay Shields. The session token protocol for forensics and traceback. [CS04]


REFERENCES

increasing_robustness_of_lsb.


Chakrabarti:2007:PBA

Chang:2008:DAP


Cusick:2009:CBF


Czeskis:2008:DED

Alexei Czeskis, David J. St.Hilaire, Karl Koscher, Steven D. Gribble, Tadayoshi Kohno, and Bruce Schneier. Defeating encrypted and denialable file systems: Truecrypt V5.1a and the case of the tattling OS and applications. In ?????, editor, Proceedings of the 3rd Conference on Hot
Cai:2007:CSM

Crandall:2005:DUV

Chen:2008:CCS

Chung:2009:ISA

Collberg:2002:WTP
Coron:2003:NAS


Chen:2008:BUK


Chu:2008:EOT


Chou:2009:ATI


Crawford:2001:FPV


Chiang:2008:CPB

Yung-Kuei Chiang, Piyu Tsai, and Feng-Long Huang. Codebook partition based


Curtin:2005:BFC


Chaitanya:2008:QQM


Canteaut:2002:DCH


Canteaut:2004:PCI

REFERENCES


REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Authors</th>
<th>Journal/Conference</th>
</tr>
</thead>
</table>
REFERENCES

Chang:2005:CIA


Chen:2003:AEY


Chadwick:2005:PKI


Crawford:2001:FHC


Cheng:2005:RIC

[Xiaorong Cheng, Huilin Zhao, and Jitian Kou. Research and improvement on computer intrusion detection technology based on immune principle. In Han et al. [HYZ05b], pages 167–?? ISBN 981-270-153-2. LCCN ???. URL http://
e proceedings.worldscinet. com/9812701532/9812701532. 0031.html.


REFERENCES

LCCN TK5105.567 D38
200. US$49.99.


Doyle:2006:SCK


DeBonis:2000:RVC


DeBonis:2004:RSS


DeBonis:2000:RVC


DeBonis:2004:RSS


DiVimercati:2005:CSE

REFERENCES


Diene:2006:DLE


Dolev:2000:NC


Dolev:2003:NC


DeSantis:2001:RNI


DeLooze:2007:PWS


Desai:2000:ESS


Desai:2000:NPC

Anand Desai. New paradigms for constructing symmetric encryption schemes

**Desai:2000:SAN**


**Dewson:2008:BSS**


**Dhem:2001:HSS**

REFERENCES

m12001/m6014abs.htm; http://dlib.computer.org/ 
mi/books/m12001/pdf/m6014.
pdf.

In Simos and Maroulis [SM07b], pages 965–968. 
ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 
URL http://proceedings.aip.org/getpdf/servlet/GetPDFServlet? 
filetype=pdf&id=APCPCS0000963000002000965000001& 
amp;idtype=cvips.

Delgado:2007:SCD

Smart card research and advanced applications: IFIP TC8/WG8.8 Fourth Working Conference 
on Smart Card Research and Advanced Applications, September 20–22, 2000, Bristol, 
United Kingdom, volume 52 of IFIP. Kluwer Academic Publishers, Dordrecht, 

Domingo-Ferrer:2000:SCR

[DFGW00] Antonio Durante, Riccardo Focardi, and Roberto Gorrìeri. A compiler 
for analyzing cryptographic protocols using noninterference. ACM Transactions on 
CODEN ATSMER. ISSN 1049-331X (print), 1551-7392 (electronic). 
URL http://www.acm.org/pubs/articles/ 
journals/tosem/2000-9-4/p488-durante/p488-durante.pdf; 
http://www.acm.org/pubs/citations/journals/ 

Durante:2000:CAC

[DFG00] Antonio Durante, Riccardo Focardi, and Roberto Gorrìeri. CVS at work: a 
report on new failures upon some cryptographic protocols. Lecture Notes in 
ISSN 0302-9743 (print), 1611-3349 (electronic). 
URL http://link.springer-ny.com/link/service/series/0558/ 
bib/a/2052/20520287.htm; 
http://link.springer-ny.com/link/service/series/ 
0558/papers/2052/20520287.pdf.

Durante:2000:CAC

[DFGH04] Paul De Palma, Charles Frank, Suzanne Gladfelter, and Joshua Holden. Cryptography 
and computer se-

Domingo-Ferrer:2001:CDS


Dodis:2003:IRP


DeSantis:2004:CKA


Domingo-Ferrer:2006:SCR


Domingo-Ferrer:2007:ASC

[DFPST07] Josep Domingo-Ferrer, Joachim Posegga, Francesc Sebé,

**Damgaard:2004:ZKP**


**Damgaard:2005:CBQ**


**Dalkilic:2000:ICA**


**Debaert:2002:RRI**

REFERENCES

ny.com/link/service/series/0558/papers/2355/23550052.pdf.

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:2009:CRN


denHartog:2008:TMC


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],
In Walter et al. [WKP03],
ISSN 0302-9743 (print),
1611-3349 (electronic). LCCN TK7895.E42
ISSN 0302-9743 (print),
1611-3349 (electronic). LCCN TK7895.E42
URL http://link.springer
URL http://link.springer
ny.com/link/service/series/
ny.com/link/service/series/
[2779];
ny.com/link/service/series/0558/
[2779];
ny.com/openurl.asp?genre=
y.com/openurl.asp?genre=
2779;
2779;
http://www.springerlink.
http://www.springerlink.
com/openurl.asp?genre=
com/openurl.asp?genre=
volume&id=doi:10.1007/
volume&id=doi:10.1007/
b13240.

Deng:2006:OOC

[259] Yan-Xiang Deng, Chao-
Jang Hwang, and Jiang-
Lung Liu. An object-
oriented cryptosystem based
on two-level reconfigurable
computing architecture.
The Journal of Systems
and Software, 79(4):466–
479, April 2006. CODEN
JSSODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic).

Daza:2007:CTM

[260] Vanesa Daza, Javier Her-
ranz, Paz Morillo, and Carla
Rafols. Cryptographic tech-
tiques for mobile ad-hoc
networks. Computer Net-
works (Amsterdam, Nether-
lands: 1999), 51(18):4938–
CODEN ???
CODEN ???
ISSN 1389-1286 (print), 1872-
7069 (electronic).

Dodi:2000:CSG

Yevgeniy Dodis, Shai Halevi,
and Tal Rabin. A crypto-
tographic solution to a
game theoretic problem.
In Bellare [Bel00], pages
112–7. ISBN 3-540-
67907-3. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2000 Bar. URL http:
http://link.springer-ny.com/
link/service/series/0558/
bibs/1880/18800112.htm;
http://link.springer-

DiCrescenzo:2001:SOS

Giovanni Di Crescenzo.
Sharing one secret vs. shar-
ing many secrets: Tight
bounds for the max im-
provement ratio. Lecture
Notes in Computer Science,
2136:292–7. 2001. CO-
DEN LNCS9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
http://link.springer-ny.com/
link/service/series/0558/
bibs/2136/21360292.htm;
http://link.springer-

DiCrescenzo:2003:SOS

Giovanni Di Crescenzo.
Sharing one secret vs. shar-
ing many secrets. Theo-
retical Computer Science,
REFERENCES


[Damgaard:2005:CRM]

[Dichtl:2003:HPO]

[Dierickx:2000:EGD]

[Diffie:2001:UC]

[Dimitriadis:2007:IMC]

[Dimitrov:2008:DBN]
Vassil Dimitrov, Laurent Imbert, and Pradeep K. Mishra. The double-base number system and

**Ding:2001:OTB**


**Ding:2005:ECB**


**Dedic:2005:ULB**


**Dang:2002:EPT**

Zhe Dang, Oscar H. Ibarra, and Zhi-Wei Sun. On the emptiness problem for two-way NFA with one reversal-

Damgaard:2001:GSS


Damgaard:2001:PTR


Delaune:2006:DPS


Donsez:2001:TMA

REFERENCES

Delfs:2002:ICP
URL http://www.springerlink.com/content/978-3-642-87126-9.

Dels:2007:ICP
URL http://www.springerlink.com/content/978-3-642-87126-9.

Dodis:2005:CCS

Dunkelman:2008:TIV

Du:2005:BRS

[DK02]
[DK05]
[DK07]
[DK08]
[DKFX05]
REFERENCES

com/9812701532/9812701532.

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


Dodis:2002:KIP


Diffie:1998:PLP


deLeeuw:2000:CSD


Diffie:2007:PLP


**DeSantis:2007:NRN**


**Drimer:2007:KYE**


**Dumais:2000:PCQ**


**Dowd:2007:ASS**


**Denev:2009:SFQ**


**Ding:2007:ESD**

Xuhua Ding, Daniele Mazocchi, and Gene Tsudik.

**Damgaard:2000:INC**


**Damgaard:2002:EPF**


**Damgaard:2002:PHP**


Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. In Shoup [Sho05a], pages 37–?? ISBN 3-540-28114-2. ISSN 0302-9743
REFERENCES


[DP02] Andreas Dandalis and Viktor K. Prasanna. An adaptive cryptographic engine for Internet protocol security architectures. ACM
REFERENCES


Crescenzo:2004:CRR [DPV04]

Daemen:2000:NPN [DPVR00]

Daemen:2000:BCR [DR00a]

Daemen:2000:RA [DR00b]

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


[DR02d] Yan Zong Ding and Michael O. Rabin. Hyper-

**Dray:** 2000: NPA


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC


**Dreyfus:** 2000: PUC

REFERENCES


REFERENCES

Ding:2005:RNM


Dodis:2005:ESE


Ding:2006:SSS


Dinur:2008:CAT


Deepthi:2009:DIA


Das:2006:NRU

REFERENCES


REFERENCES

[Dunkelman:2006:TCB]

[Duranti:2001:LTP]

[Dowell:2003:BRB]

[Dawson:2005:PCM]

[Drutarovsky:2008:CSC]

[Levy-dit-Vehel:2006:WC]
Françoise Levy dit Vehel and Ludovic Perret. On the Wagner–Magyarik
REFERENCES


Du:2001:OKS


[DW01]


dW02


[DW05]


Dodis:2009:NME


Dwivedi:2004:ISS


Desmedt:2005:CNS
REFERENCES


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

Dai:2001:CDE


Eagleton:2005:BRD


ElAbbadi:2000:VP1


Eghlidos:2001:IRL


Eilam:2005:RSR


English:2007:MAC

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

ECMA:2000:EPIa


ECMA:2000:EPIb


Ellison:2003:PKS


Echizen:2005:PAV


Eghlidos:2000:SLB


Elmallah:2008:LK

Epstein:2003:DIT


Ernst:2004:FBH


Ellison:2000:PSK


Ekert:2002:BTQ


Ekeraa:2009:DCM


Ellison:2000:TRP


Ellison:2000:IRRa


Eberle:2005:ANG


Enck:2005:EOF


Ettinger:2002:QQC


Ebringer:2000:PAP


Edman:2009:AES

[ETMP05] Matthew Edman and Bülent Yener. On anonymity in an
REFERENCES


Elbirt:2000:FIP


Faliszewski:2007:BRB


Fan:2003:ILC


Faugere:2009:IBC


Ford:2001:SEC


Felkel:2001:ICW

Petr Felkel, Mario Bruckschwaiger and Rainer Wegenkittl. Im-
REFERENCES

Feghali:2002:SAP


Fan:2005:RRA


Fischer:2001:TMR


Furnell:2000:ASS


Felke:2006:ATH

REFERENCES

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


REFERENCES


did in the war [MH09], page ?? ISBN 0-203-88318-
7 (e-book), 0-7103-1340-3 (hardcover). LCCN Q141
www.loc.gov/catdir/toc/ecip0824/2008033118.html

Filiol:2000:DAS

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bib/a/1977/19770031.htm;
http://link.springer-
ny.com/link/service/series/
pdf.

Filiol:2002:NST

Eric Filiol. A new statistical testing for symmetric ciphers and hash functions. Technical report, ESAT — Virology and Cryptol-
ogy Lab, B.P. 18 35998 Rennes, FRANCE, July 23, 2002. 14 pp. URL http:
//eprint.iacr.org/2002/

Finley:2002:BSE

Brian Elliott Finley. BOEL: a small Embedded Linux with PIC libraries. Embedded Linux Journal, 8:

FIPS:2000:DSS

FIPS. Digital Signature Standard (DSS). National Institute for Standards and Technology, Gaithersburg,
REFERENCES

FIPS:2001:AES


FIPS:2001:SRC


FIPS:2002:KHM


FIPS:2002:SHS


Freedman:2005:KSO


**Fluhrer:2001:AES**


**Fox:2001:PPK**


**Faure:2006:NPK**


**Freytag:2003:VP1**


**Fluhrer:2002:CMB**

REFERENCES

Fluhrer:2002:CSP


Feng:2006:ISC


Fan:2002:ETB


Fehr:2002:LVD


Fuller:2002:LRA

REFERENCES


REFERENCES


[FOP06] D. Frincke, S. Oudekirk, and B. Popovsky. Editorial: Special issue on resources for the computer se-
REFERENCES


[FP01] Pierre-Alain Fouque and David Pointcheval. Threshold cryptosystems secure against chosen-ciphertext attacks. Lecture Notes in...
Faugere:2009:EAD


Fouque:2001:SDC


Fournet:2008:CSI


Frankel:2001:FCI

REFERENCES


REFERENCES

[FS00] Ferguson:2000:CEI

[FS01a] Fouque:2001:FDT

[FS01b] Friedlander:2001:DDH

[FS01c] Furukawa:2001:ESP


[FS03a] Ferguson:2003:CEI
Niels Ferguson and Bruce Schneier. A cryptographic evaluation of IPsec. Un-

Ferguson:2003:PC


Fundulaki:2004:SYD


Fortnow:2008:IIC


Fuster-Sabater:2001:EAG


Fu:2001:DCA


Ferguson:2001:SAR

Niels Ferguson, Richard Schroeppe1, and Doug Whiting. A simple algebraic representation of Rijndael. Lecture Notes in Computer Science, 2259: 103–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
REFERENCES


REFERENCES


REFERENCES


Gannon:2001:SST


Ganti:2008:P AL


Garrett:2001: MBC


Garfinkel:2003:EBI


Garfinkel:2003:KDG


Garrett:2004:MCT


Garrett:2005:CP

REFERENCES


Gaj:2000:CHP


Goubin:2000:CTC


Gaj:2001:FIF


Goodman:2001:EER

REFERENCES


[Gen00b] Rosario Gennaro. An improved pseudo-random generator based on discrete


**[Gen03]**

**[Gen06]**

**[Gen09a]**
REFERENCES


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

P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. Lecture Notes

Grabner:2005:ALC


Gong:2001:GPK


Gennaro:2001:RCV


Gennaro:2002:RSM


Gillespie:2007:WSC


Giraud:2006:RIR

C. Giraud. An RSA implementation resistant to fault attacks and to simple power


Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In ACM [ACM07], pages 516–525.
REFERENCES


REFERENCES


REFERENCES

Goshi:2006:ADM

Gassend:2004:IAI

Grembowski:2002:CAH

Gallant:2001:FPM

Gilbert:2000:CAR
REFERENCES


[GM03] Steven D. Galbraith and Wenbo Mao. Invisibility and anonymity of undeniable and confirmers signatures. In Joye [Joy03b], pages 80–97. CODEN LNCS9D. ISBN 3-540-00847-0. ISSN 0302-9743


[GN01] Rajeev Prabhakar Goré


References

324

See also volume 2 [Gol04].

Goldreich:2001:FCBa


Golic:2001:MOSS


Golic:2003:DNP


Goldreich:2004:FCV


Goldstein:2008:BHO


Gonda:2006:NMR


Good:2000:TAE


Gordon:2002:TCP


Gurgens:2002:APF

Gorman:2005:NSC


Gordon:2006:UAV


Goulding:2009:ESA


Gupta:2008:FAT


Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT


Güney:2008:SPH

Tim Güney, Christof


REFERENCES


REFERENCES


**Gentry:2002:HIB**


**Gentry:2002:CRN**


**Geiselmann:2003:HSS**


**Geiselmann:2007:SPH**


**Goodell:2007:TOR**


**Grassl:2009:CAS**

Markus Grassl and Rainer Steinwandt. Cryptanalysis
REFERENCES


Guida:2004:DUP


Geetha:2009:BIS


Garfinkel:2003:PUI


Gaubatz:2008:SCD


Goodrich:2004:ETB

Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia. Efficient tree-based revocation in groups of
REFERENCES


Goodrich:2003:ADS

Goodrich:2008:NFI

Guttman:2004:FAP

Guttman:2004:FAP

Guillou:2001:CAP
REFERENCES


**Gutmann:20xx:ESR**


**Granger:2005:DLP**


**Garera:2009:CTG**


**Gassend:2008:CPR**


**Gisin:2000:LCQ**


**Guoxiang:2001:IFB**

Song Guoxiang and Wang Weiwei. Image-feature based second generation watermarking in wavelet domain. *Lecture Notes in
REFERENCES


Gebotys:2008:EAW


Goldberg:2008:PQM


Heys:2000:SAC

References

Shiho Moriai ... [et al.] — Key-schedule cryptanalysis of DEAL / John Kelsey and Bruce Schneier — Efficient evaluation of security against generalized interpolation attack / Kazumaro Aoki — Efficient implementation of cryptosystems based on non-maximal imaginary quadratic orders / Detlef Huhnlein — Improving and extending the Lim/Lee exponentiation algorithm / Biljana Cubaleska, Andreas Rieke, and Thomas Hermann — Software optimization of decorrelation module / Fabrice Noilhan — Pseudonym systems / Anna Lysyanskaya ... [et al.] — Unconditionally secure proactive 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.

Haddad:2000:AUA

Hancock:2000:EWP

Harvey:2000:EMA

Hare:2001:RUPa
REFERENCES

Hare:2001:RUPb

Harrington:2005:NSP

Harris:2005:GHE

Hars:2006:MIA

Harm:2007:DIH

Hasan:2000:LTB
REFERENCES


[Hay04] Khawaja Amer Hayat, Umar Waqar Anis, and S. Tauseef ur Rehman. Cryptanalysis of some encryption/cipher schemes using related key attack. SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education), 36(4):85–87, December 2004. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). NOTE FROM ACM: It has been determined that the authors of this article plagiarized the contents from a previously published paper. Therefore ACM has shut off access to this paper.

[Hay06] Masahito Hayashi. Quan-


Hwang:2004:NMP


Huang:2008:NCK


Hernandez-Castro:2006:SGG


Han:2008:PBPa


Han:2008:PB Pb


Henderson:2002:MTS

REFERENCES


Halevi:2002:SSE


Han:2009:ICS


He:2002:WSM


Heijl:2001:DXS


Heiser:2003:BCB


Heikkila:2007:ESC

REFERENCES


[Her09b] Amir Herzberg. DNS-based email sender authentication mechanisms: a critical review. Computers
Hess:2004:SVE


Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA


Horvitz:2003:WKA


Horan:2005:NRN

Howgrave-Graham:2005:PKC


Howgrave-Graham:2007:HLR


Hasenplaugh:2007:FMR


Howgrave-Graham:2003:IDF


Hwang:2005:TSP


Hoffstein:2006:NNE


Hess:2004:CTT


Hong:2004:DCT


Hankerson:2000:CTC


Hankerson:2003:NDS

REFERENCES


REFERENCES

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

(Hirose:2009:SAD)

(Huang:2005:ASE)

(Harris:2005:IUS)
David Harris, Ram Krishnamurthy, Mark Anders, Sanu Mathew, and Steven Hsu. An improved unified scalable radix-2 Montgomery multiplier. In IEEE [IEE05b], page ?? ISBN ???? LCCN ???? URL

(Hinkelmann:2007:CUN)

(Huhnlein:2001:TPN)

Kim:2000:RMW


Heuberger:2005:AGE


Handschoh:2001:ASE


Hofmeister:2000:COS


Hiltgen:2006:SIB

REFERENCES


[HL05d] Shin-Jia Hwang and Hao-


REFERENCES

Herzog:2003:PAK


Hwang:2001:TSB


Huang:2009:OSW


Hopper:2002:PSS


Hu:2009:TRN

Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU


Harbitter:2002:MAP


Hevia:2002:PSG


Hitchcock:2002:NEC

Hoglund:2004:ESH


Hollar:2005:EWS


Holenstein:2004:CCB

Thomas Holenstein, Ueli Maurer, and Johan Sjödin. Complete classification of bilinear hard-core functions. [HN04] In Franklin [Fra04], pages 73–??. CODEN LNCSD9.

Hankerson:2004:GEC


Huang:2007:MPK


Haastad:2004:SAR

Johan Håstad and Mats Näslund. The security of all RSA and discrete log...

**Harnik:2006:CNI**


**Haitner:2009:SHC**


**Hoepman:2001:SKA**


**Hofinger:2001:LBE**

REFERENCES

Honary:2001:CCI

Hook:2005:BCP

Horn:2000:APF

Huhnlein:2001:ICB
References

Han:2002:CMV


Hoffstein:2001:NNL


Hoffstein:2008:IMC


He:2001:SAR


Hu:2005:USA


Hawkes:2001:PCS

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


[Hawkes:2000:EMC]


[Hand:2002:MPP]

Hand:2002:MPP


[Halevi:2003:TEM]


[Hawkes:2004:RVC]

REFERENCES

volume&id=doi:10.1007/b99099.

Hsiao:2004:FCP


Holenstein:2005:OWS


Halevi:2006:TCT


Haitner:2007:SHC


Harn:2009:DDB

REFERENCES


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


[Hoffstein:2001:MAD]


[Haeley:2002:LBE]


[Han:2002:HEF]


[Hwang:2007:PEA]


[He:2005:MCP]


[Hong:2001:KIA]

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

Halderman:2008:LWR


Halderman:2008:LWRb


Halderman:2009:LWR


Hanaoka:2002:USA

REFERENCES


[Hernandez:2001:DTR]


[Hernandez:2004:STN]


[Hess:2001:TTH]


[Hess:2005:CIT]


[Hsu:2005:UFR]


REFERENCES

Hamalainen:2002:GPS


Hines:2007:AIF


Hofheinz:2005:CTN


Hughes:2002:LAA


Hughes:2004:ISE


Huhnlein:2000:EIC

Detlef Hühnlein. Efficient implementation of cryp-


[HV09] Sean Hallgren and Ulrich Vollmer. Quantum


REFERENCES


REFERENCES

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


REFERENCES


Huang:2005:EMP


IEEE:2000:ASF


IBM-MARS-Team:2000:MAS


IEEE:2000:IPH


IEEE:2001:ISF


IEEE:2005:AIS


IEEE:2005:PIS


IEEE:2006:AIS


IEEE:2006:PAI


IEEE:2008:PAI


Bassham:2000:ETA

Itoh:2003:PCA

Iwata:2000:PAF

Iwata:2001:PAF

Iwata:2000:PAF
REFERENCES

bibs/1978/19780231.htm;

**Impagliazzo:2003:LRA**


**Ichikawa:2000:HEA**


**Ishai:2003:EOT**

REFERENCES


Izmerly:2006:CCA


Izotov:2001:COC


Izotov:2001:COC

Inamori:2002:SPB


Inamori:2002:SPT


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

ISO:2004:IIIb


ISO:2005:IDM


Iqbal:2008:CDV

[ISSZ08] Razib Iqbal, Shervin Shir-mohammadi, Abdulmotaleb El Saddik, and Jiy-
Naomaru Itoi. Secure co-
processor integration with
Kerberos V5. In USENIX
[USE00d], page ?? ISBN
1-880446-18-9. LCCN ????
URL http://www.usenix.
org/publications/library/
proceedings/sec2000/itoi.
html.

Naomaru Itoi. SC-CFS:
Smartcard secured crypto-
graphic file system. In USENIX
[USE01c], page ?? ISBN
1-880446-07-3. LCCN QA76.9.A25
www.usenix.org/publications/
library/proceedings/sec01/
itoi.html.

Maki Iwami. An attack
on improved algebraic sur-
face public-key crypto-
system (abstract only). ACM
Communications in Com-
puter Algebra, 42(1-2):71–
74, March/June 2008. CO-
DEN ????. ISSN 1932-2232
(print), 1932-2240 (elec-
tronic).

Hideki Imai and Atsuhiro
Yamagishi. CRYPTREC
Project — cryptographic
evaluation project for the
Japanese electronic govern-
ment. Lecture Notes in
Computer Science, 1976:
399–??, 2000. CODEN
LNCS09. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/1976/19760399.htm;
http://link.springer-
ny.com/link/service/series/
pdf.

Keith Irwin and Ting Yu.
Preventing attribute informa-
tion leakage in auto-
mated trust negotiation.
In Meadows and Syver-
son [MS05b], pages 36–45.
ISBN 1-59593-226-7. LCCN
QA76.9.A25. ACM order
number 459050.

Mitsugu Iwamoto and Hirosu-
ke Yamamoto. Strongly
secure ramp secret shar-
ing schemes for general ac-
cess structures. Informa-
tion Processing Letters, 97
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

Tetsu Iwata, Tomonobu
Yoshino, and Kaoru Ku-
or-sawa. Non-cryptographic
primitive for pseudoran-
dom permutation. Lecture


Jambunathan:2000:CCP


Janczewski:2000:IIS


Janczko:2006:TSH


Jankowski:2008:BRBb

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

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


[JJ00d]


[JK01a]


[JK01b]


[JJP02a]

Jonsson:2002:SRE


Jonsson:2002:SRT


Jang:2001:BWA


Jung:2001:EMO


Jallad:2002:ICC

Kahil Jallad, Jonathan


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


Jeong:2008:PKE

Lee:2007:RKD

Juang:2001:FBT

Juang:2002:VMA

Jakobsson:2003:FMT

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


Jakobsson:2007:DPD


Joux:2002:BAA


Johnson:2000:AFR


[Jou02] Antoine Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. *Lecture
REFERENCES


Joux:2004:MIH


Joux:2009:AC


Joyner:2000:CTC


Joye:2003:CPY


Joye:2003:TCC

REFERENCES


Rui Jiang, Li Pan, and Jian-Hua Li. Further analysis

**Joye:2004:CHE**


**Joye:2001:OAD**


**Juric:2006:CPW**

Matjaz B. Juric, Ivan Rozman, Bostjan Brumen, Matjaz Colinaric, and Marjan Hericko. Comparison of performance of Web ser-


**REFERENCES**

**Jiang:2005:SAI**


**Joye:2001:PAD**


**Joye:2001:CEN**


**Joglekar:2005:PEM**


**Juang:2004:EPA**


**Juels:2004:FCI**


[Fuh-Gwo Jeng and Chung-Ming Wang. An efficient

**Jin:2005:EAW**


**Jiang:2005:RNP**


**Joye:2001:NMM**


**Jakobsson:2004:ACN**


**Jain:2009:NBC**

Rahul Jain and Shengyu Zhang. New bounds on classical and quantum one-way


- **Kaliski:2001:RDS**

- **Kaliski:2003:TRK**

- **Kanda:2001:PSE**

- **Kapera:2005:MRP**

- **Karski:2001:SSS**

- **Katzenbeisser:2001:RAR**
  - Stefan Katzenbeisser. *Recent advances in RSA cryptography*, volume 3 of Ad-


REFERENCES

Kim:2009:DCA


Kachris:2003:RLB


Keller:2009:ECC


claffy:2001:IMM


Kim:2002:SMA


Ku:2005:CFR

[KC05] Wei-Chi Ku and Shuai-Min Chen. Cryptanalysis of a
REFERENCES


**Kieu:2009:HSI**


**Kieu:2009:IAB**


**Ku:2005:WYR**


**Kim:2007:SBE**


**Kim:2001:SAC**

REFERENCES

Ku:2003:WLL


Kang:2001:NHO


Kurosawa:2004:NPH


Kalker:2004:DWS


King:2001:SAD


Keefe:2005:CDS


Kelsey:2000:KST


Kelsey:2002:CIL


Kellar:2005:NRR


Kenyon:2002:DNR


Kenyon:2002:HPD

REFERENCES


Kim:2005:SMA


Kato:2008:QSC


Khaw:2005:EDA


Komninos:2001:ESC


Kwon:2005:CLK


Koo:2009:SVN

Woo Kwon Koo, Jung Yeon Hwang, and Dong Hoon Lee. Security vulnerabili-
Kobara:2001:NCP

Kobara:2001:SSM

Kurosawa:2003:TTK
Kaoru Kurosawa and Tetsu Iwata. TMAC: Two-key CBC MAC. In Joye

Kiroski:2004:DWF

Kausar:2008:SEK

Kobara:2001:NCP

Kobara:2001:SSM

Kurosawa:2003:TTK
Kaoru Kurosawa and Tetsu Iwata. TMAC: Two-key CBC MAC. In Joye

Kidwell:2000:SNC


Kid:2002:PGR


Kilian:2001:ACC


Kiltz:2001:TBC


Kilian:2005:TCS


[Kim:2000:IMP]


[Kim:2001:CMF]

David A. King. The ciphers of the monks: a for-
REFERENCES


King:2002:RGI


Kir01a


Kir01b


Montgomery:2003:FEC


Kocarev:2001:LMB

REFERENCES


REFERENCES

Karri:2003:PBC

Khachatrian:2001:FMI

Kwon:2003:EEC

[KKIM01]

Ko:2007:SRT
REFERENCES

getpdf/servlet/GetPDFServlet?filetype=pdf&id=APCPCS000963000002000571000001&
amp;idtype=cvips.

Klonowski:2009:SGS


Kawachi:2005:UTQ


Kim:2009:SVN


Kaliski:2002:CHE


Kelsey:2000:ABA

John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent (abstract only). In NIST [NIS00], page 10. ISBN???? LCCN???? URL http://csrc.nist.
REFERENCES

Kohno:2000:PCR


Kelsey:2001:ABA


Kim:2002:IDS


Katz:2005:HEP

[Jonathan Katz and Yehuda Lindell. Handling expected polynomial-time strategies in simulation-based security proofs. In Kilian [Kil05], pages 128–]
REFERENCES

?? CODEN LNCSD9.


Knill:2002:QIP


Knill:2002:FPE

Knill:2002:QIP


Ko:2000:NPK

Klein:2007:BDC


Kong:2001:AVW


Kiltz:2005:SCM


Kacprzak:2006:CBS


Kalai:2009:SEU


Kim:2002:EPS

Nam-Young Kim, Won-Ho Lee, and Kee-Young Yoo. Efficient power-sum systolic architectures for public-key cryptosystems in GF(2^m)
REFERENCES

Kim:2003:IBP


Knudsen:2000:CRA


Knudsen:2001:CRR


Knudsen:2001:NPK

REFERENCES


Kornerup:2007:PIS


Kim:2002:ABA


Karakountas:2006:HSF


Katt:2001:CCA


Klarlund:2001:MIS

Nils Klarlund, Anders Møller, and Michael I.

Klimov:2002:ANC


Keliher:2001:IUB


Kim:2003:RCC


Kittler:2003:AVB

REFERENCES


REFERENCES


Koblitz:2000:TQC


Kocher:2002:IS


Koga:2002:GFR


Kurosawa:2001:ICP


Kornblum:2009:IBD


Koshiba:2001:NAS

REFERENCES

Koshiba:2001:SRS


Koskinen:2001:NIK


Kovach:2001:BCB


Kovacich:2003:ISS


Katz:2001:EPA


REFERENCES


[Kra02b] Matthias Krause. BDD-based cryptanalysis of keystream generators. Lecture Notes in Computer Science, 2332: 222–??, 2002. CODEN LNCSD9. ISSN 0302-
REFERENCES

Krause:2002:USP


Krawczy:2003:SSM


Krawczyk:2005:HHP


Kramer:2007:LCC


Kreitz:2005:OBE

REFERENCES

Koeune:2002:FIL


Kehr:2001:ISM


Kim:2005:CLL


Katz:2000:CCA


Kelsey:2000:MAP

Kuramitsu:2002:ETC


Krause:2003:DOC


Kozaczuk:2004:EHP


Katz:2005:MIA


Kiltz:2005:TCL


Kissner:2005:PPS

REFERENCES


[KS09b]


[KS06a]


[KSF00]


[KS09a]


Kogan:2006:PRS


Kelsey:2000:SCC


Konstantinou:2002:SLE


Kuribayashi:2000:WSB


Kuribayashi:2001:NAF

REFERENCES

Kogan:2006:IER


Ku:2003:TSA


Kobayashi:2007:AIG


Kuhn:2000:PCL


Kuhn:2001:CRR

(print), 1611-3349 (electronic).

**Kuhn:2002:OTD**


**Kuhn:2002:ICM**


**Kuhn:2008:BSS**


**Kukorelly:2001:PAL**


**Kundur:2001:WDI**


**Kurosawa:2001:MRP**


\textbf{Kusters:2002:DCP}


\textbf{Kuo:2001:AOS}


\textbf{Komninos:2007:ALS}

dations of computer science: toward a paradigm for computing in the 21st century (Japanese) (Kyoto, 2000).

**Knudsen:2002:IC**


**Karlof:2003:HMM**


**Keromytis:2006:COS**


**Kwon:2002:DSA**


**Kwok:2003:WBC**


**Kwon:2003:EDS**

November 30, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [Kwo02].

Kumar:2006:ODS


Wong:2001:MCC


Kun:2000:SMA


Kamat:2009:TPW


Katz:2000:CCS


Katz:2001:UEC

Kavut:2001:SCP


Kiayias:2001:PRB


Kiayias:2001:SPP


Kurosawa:2001:LCI


Katz:2002:TCB

Jonathan Katz and Moti Yung. Threshold cryptosystems based on fac-
Kiayias:2002:CHB


Kim:2002:PAA


Katz:2003:SPA


Kamal:2009:FIN


Kang:2001:PMT

Ju-Sung Kang, Okyeon Yi,
REFERENCES


Kabatnik:2001:LSD


Kamp:2007:DEB


Kumar:2009:UAU


Ladd:2006:SPS

David Ladd. A software procurement and security primer. IEEE Secu-
REFERENCES


science and applied logic.
Birkhäuser Verlag, Basel,
Switzerland, 2001. ISBN 3-
7643-6510-2, 0-8176-6510-2.

[Lam07] David Lambert. Super lit-
ttle giant book of secret codes.
Sterling Pub. Co., New
York, NY, USA, 2007. ISBN
1-4027-3739-4 (paperback).
287 pp. LCCN Z103.3 .L36
loc.gov/catdir/enhancements/
fy0738/2007276461-d.html

[Lan00a] Susan Landau. Communications security for
the Twenty-first Century:
The Advanced Encryption Standard.
Notices of the American Mathematical Society,
47(4):450–459, April 2000. CODEN AM-
NOAN. ISSN 0002-9920
(print), 1088-9477 (elec-
am.org/notices/200004/
fea-landau.pdf.

[Lan00b] Susan Landau. Standing
the test of time: The Data
Encryption Standard. Not-
tices of the American Mathem-
tical Society, 47(3):341–349,
March 2000. CODEN AMNOAN.
ISSN 0002-9920
(print), 1088-9477 (elec-
landau.pdf.

[Lan04a] Susan Landau. Polynomi-
als in the nation’s service:
Using algebra to design the
Advanced Encrypted Standard.
American Mathematical Monthly,
AMMYAE. ISSN 0002-9890

[Lan00d] Jean-Louis Lanet. Invited
talk: Are smart cards the
ideal domain for applying
formal methods? Lecture
Notes in Computer Science,
1878:363–??, 2000. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
l ink/service/series/0558/
bibs/1878/18780363.htm;
http://link.springer-

[Lan00c] Susan Landau. Technical
opinion: designing cryptography for the new
century. Communications of
the Association for Compu-
ting Machinery, 43(5):
115, May 2000. CODEN
CACMA2. ISSN 0001-0782
(print), 1557-7317 (elec-
acm.org/pubs/citations/
journals/cacm/2000-43-
p115-landau/.

[Lan04b] Susan Landau. Poly-
nomials in the nation’s service:
Using algebra to design the
Advanced Encrypted Standard.
American Mathematical Monthly,
AMMYAE. ISSN 0002-9890
REFERENCES

Landau:2004:SLE

Laud:2005:STS

Laud:2008:CSC

Laughlin:2008:CRC

Lavoue:2009:LRM
Lawton:2005:MAH


Lawson:2009:SCA


Lawson:2009:TAG


Li:2004:QAU


Lindskog:2005:DIT


Lee:2000:UBN


Leveiller:2001:CNF

[LBGZ01] Sabine Leveiller, Joseph Boutros, Philippe Guillot, and Gilles Zémor. Cryptanalysis of nonlinear filter generators with \{0,1\}-metric Viterbi decoding. Lecture Notes in Computer Science, 2260:402–??, 2001. CODEN LNCSD9. ISSN 0302-
Leveiller:2002:CNF


Laufer:2000:SSC


Laih:2003:COP


Lin:2004:SOT


Lu:2004:XMS


REFERENCES

Levi:2004:UNC


Lee:2004:DEB


Lim:2009:OPG


Li:2008:CAM


Lu:2005:TUS


Lu:2005:PBM


Lu:2005:RTP

REFERENCES


Lee:2003:CS

Lee:2004:SPM

Lee:2004:ACA

Lehtinen:2006:CSB

Lenstra:2001:USM
References


Robert Lyda and James Hamrock. Using entropy analysis to find encrypted

**Li:2008:ISS**


**Lu:2005:NPS**


**Lee:2002:TDC**


**Lee:2003:NKA**


**Lin:2003:NRU**


**Lee:2004:SAA**


References


Li:2005:ABPa


Lin:2000:RTI


Linn:2000:TMM


Lin:2001:HKA

REFERENCES


Licks:2005:GAI


Li:2005:AWP


Lee:2004:SSP


Ludwig:2001:FSE


Lee:2008:SAF


Lee:2009:SAF


Lim:2001:SAW

Lee:2003:PSAa


Lee:2003:PSAb


Lee:2005:NIW


Lee:2004:CUA


Lee:2005:ENB


Lee:2005:APC


REFERENCES


**Lee:2005:CMA**


**Lee:2005:SSP**


**Li:2005:FCR**

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


Shujun Li, Chengqing Li, Guanrong Chen, and Kwok-

Lee:2001:PBG


Lee:2002:RUA


Li:2001:SPD


Liao:2006:PAS


Lesniewski-Laas:2005:SSS


Li:2001:SPD

[LLL+01] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudorandom coding. Lecture
REFERENCES


Lee:2002:SEC


Lee:2004:MPA


Li:2006:ESY


Li:2006:SYG


Lindell:2002:CAB

Lindell:2006:CAB

Lian:2007:MDE

Lee:2005:IWR

Liu:2005:SWA

Lee:2009:CET

Li:2004:ABP
REFERENCES


Lorenz:2002:SSG


Lavasani:2008:IFA


Li:2003:SCE


Lamenca-Martinez:2006:LNP


Leitold:2001:MTN

Lepinski:2005:FZK


Laskari:2007:AEC


Laskari:2005:TTC


Lu:2005:CCA


Li:2005:BPC

REFERENCES

5411 (print), 1557-735X (electronic).


REFERENCES

Lopez:2004:AAI

Lopez:2006:UPK

Lovering:2001:TKF

Lindell:2000:PPD

Lysyanskaya:2001:AST

Labbe:2002:AIF
Anna Labbé and Annie Pérez. AES implementation on FPGA: Time —

Luccio:2002:AC


Lee:2003:CPK


Liu:2005:MCK


Law:2009:EEL


Lemke:2006:ESC

Kerstin Lemke, Christof Paar, and Marko Wolf, editors. Embedded security in cars: securing current and future automotive IT applications. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
REFERENCES


Li:2006:PMW

Li:2008:DEO

Lientz:2001:BTP

Lemke-Rust:2007:MAP

Liskov:2002:TBC

Lenstra:2001:SFR

Lindemann:2001:ICT
Mark Lindemann and Sean W.


REFERENCES

Lin:2000:TPE

Lin:2003:SEOa

Lin:2003:SEOb

Liang:2009:AIE
REFERENCES

Lee:2001:EPI


[LTH05] Li:2005:ISS


[LTM+00] Lie:2000:ASC


[LTW05] Lin:2005:HAO

REFERENCES


[Luc00] Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys.


REFERENCES

Lunde:2009:BCU
http://www.loc.gov/catdir/enhancements/fy1002/2009281679-d.html.

Lutz:2002:BBS

Lutz:2003:BLF
Michael J. Lutz. Bookshelf: Laying the foundation for pervasive computing [Pervasive Computing]; integrated approach to data handling [Exploratory Data

Lucas:2006:PGE

Ludvig:2005:PWF

Lukyanov:2001:PFA


**Lenstra:2000:XPK**


**Lu:2004:FCA**


**Laguillaumie:2007:MDV**


**Lange:2002:PIE**


**Lee:2004:IAK**

Narn-Yih Lee and Chien-


[LZ04] Hua Li and Chang N.

Lao:2009:ORA


Li:2001:GOT


Li:2004:WMS


Michener:2000:IWM


Michener:2000:MSA


Masuda:2002:CDC


REFERENCES

???? pp. LCCN ???? Introduction by Chaker Faham.

**McDaniel:2006:OAI**


**Machado:2000:NCP**


**MacKenzie:2001:MEP**


**Mohay:2003:CIF**


**Madsen:2000:HC1**


**Madsen:2004:FFD**


**Mahle:2004:DDI**

Malcolm:2002:LAM


Maloof:2006:MLD


Manger:2001:CCA


Mann:2002:H1


Mann:2008:HHS


Mao:2001:TRC

0558/papers/2259/22590342.pdf.

Mao:2004:MCT


Marques:2002:BSJ


Martinelli:2002:SSA


Mares:2005:BRA


Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI

REFERENCES

Martin:2008:IBE


Mastroeni:2004:APA


Matsui:2002:FSE


Maurer:2001:C


Maurer:2004:RCD


Maughan:2005:HSC


Maximov:2006:SWC

[Max06] Alexander Maximov. Some words on cryptanalysis of stream ciphers. Department of Information Tech-
REFERENCES


**Mayers:2001:USQ**


**May:2002:CUR**


**May:2004:CRS**

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

**May:2009:PIS**


**Mel:2001:CD**


**Mohanty:2008:IWB**


**McKinnon:2004:CCS**


**Montenegro:2004:CBI**


**McAndrew:2008:TCO**


**McGraw:2006:SSB**


**Myles:2005:ETS**


**McKenna:2004:EAE**

REFERENCES

[McL06]

[McN03]

[MD04]

[ME05]

[ME08a]

[ME08b]

[Mea01]


Matula:2005:TLS


Mueller:2006:SMG


Muller:2009:BPE


Minier:2001:SCC


Muresan:2008:PCA


Mukherjee:2002:CAB


REFERENCES

Mihaljevic:2009:ASC

Micciancio:2001:ILB

Micciancio:2002:GCK

Micciancio:2002:ICH

Millen:2003:FD

Mironov:2002:RSO


References

MacDonald:2003:CDS

Maltoni:2004:BAE

Moore:2001:AGK

Mabry:2007:USE

Mandviwalla:2008:MBW

Moffie:2005:AAS
Micha Moffie and David

Moyle:2005:CLD


Mazieres:2000:SKM


Majzoobi:2009:TDI


McDonald:2008:SID


McGregor:2005:PCK


Miaou:2001:BCW

REFERENCES

link/service/series/0558/  
bibs/2195/21950654.htm;  
http://link.springer-  
ny.com/link/service/series/  
0558/papers/2195/21950654.  
pdf.

[MLM03] John Malone-Lee and Wenbo  
Mao. Two birds one stone: Signcryption using  
RSA. In Joye [Joy03b], pages 211–225. CODEN  
LNCSD9. ISBN 3-540-  
00847-0. ISSN 0302-9743  
(print), 1611-3349  
(electronic). LCCN QA76.9.A25  
C822 2003. URL http:  
//link.springer-ny.com/  
link/service/series/0558/  
tocs/t2612.htm; http://  
www.springerlink.com/  
openurl.asp?genre=issue&  
issn=0302-9743&volume=  
2612.

[MM01a] S. Maitra and D. P. Mukher-  
jee. Spatial domain digital  
watermarking with buyer  
authentication. Lecture  
Notes in Computer Science,  
2247:149–??, 2001. CO-  
DEN LNCSD9. ISSN 0302-  
9743 (print), 1611-3349  
(electronic). URL http:  
//link.springer-ny.com/  
link/service/series/0558/  
bibs/2247/22470149.htm;  
http://link.springer-  
ny.com/link/service/series/  
0558/papers/2247/22470149.  
pdf.

[MM01b] John Malone-Lee and Wenbo  
Mao. Two birds one stone: Signcryption using  
RSA. In Joye [Joy03b], pages 211–225. CODEN  
LNCSD9. ISBN 3-540-  
00847-0. ISSN 0302-9743  
(print), 1611-3349  
(electronic). LCCN QA76.9.A25  
C822 2003. URL http:  
//link.springer-ny.com/  
link/service/series/0558/  
bibs/2195/21950654.htm;  
http://link.springer-  
ny.com/link/service/series/  
0558/papers/2195/21950654.  
pdf.

[MM01c] M. McLoone and John V.  
McCanny. High performance single-chip FPGA  
Rijndael algorithm implementations. Lecture Notes  
in Computer Science, 2162:  
65–??, 2001. CODEN  
LNCSD9. ISSN 0302-9743  
(print), 1611-3349  
(electronic). URL http:  
//link.springer-ny.com/  
link/service/series/0558/  
bibs/2162/21620065.htm;  
http://link.springer-  
ny.com/link/service/series/  
0558/papers/2162/21620065.  
pdf.

[MM01d] M. McLoone and John V.  
McCanny. Single-chip FPGA implementation of  
the advanced encryption standard algorithm. Lecture  
Notes in Computer Science,  
2147:152–??, 2001. CO-  
DEN LNCSD9. ISSN 0302-  
9743 (print), 1611-3349  
(electronic). URL http:  
//link.springer-ny.com/  
link/service/series/0558/  
bibs/2147/21470152.htm;  
http://link.springer-  
ny.com/link/service/series/  
0558/papers/2147/21470152.  
pdf.

[MM02] Antonio Maña and So-  
nia Matamoros. Practical  
mobile digital signatures. Lecture Notes in
REFERENCES


Moldovyan:2007:IC


Mullen:2007:FFA


Moreira:2002:RCE


Milenkovic:2005:UIB


Maltoni:2003:HFR

 REFERENCES

[MMMT09] Robert P. McEvoy, Colin C. Murphy, William P. Mar-
nane, and Michael Tunstall. Isolated WDDL: a hiding countermeasure for differential power analysis on FP-
GAs. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2(1):3:1–3:??, March 2009. CODEN ????? ISSN 1936-7406 (print), 1936-
7414 (electronic).

[MMV06] Subhamoy Maitra, C. E. Veni Madhavan, and Ramarath-
nam Venkatesan, editors. Progress in Cryptology —
INDOCRYPT 2005: 6th International Conference on Cryptology in India, Bangalore, India, Decem-
ber 10–12, 2005. Proceedings, volume 3797 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, UK / etc., 2006. CODEN LNCSD9. ISBN 3-540-
30805-9 (softcover). ISSN 0302-9743 (print), 1611-
issn=0302-9743&volume=3797.

[MMYH02] T. Matsumoto, H. Mat-
sumoto, K. Yamada, and S. Hoshino. Impact of art-
ficial gummy fingers on fingerprint systems. In Pro-
Society of Photo-optical Instrumentation Engineers
(SPIE), Bellingham, WA, USA, 2002. URL http://
www.itu.int/itudoc/itucomeeting/security/ps
d5p4.pdf.

[MMZ00] Abby Maclean, Stephen M. Matyas, and Nevenko Zu-
nic. Organization implementa-
tion guidelines for recovery of encrypted informa-

[MN01] Takaaki Mizuki and Takao Nishizeki. Necessary and suf-
cient numbers of cards for sharing secret keys on hier-
erarchical groups. Lecture Notes in Computer Science, 2223:196–??, 2001. CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http://
link.springer-ny.com/
REFERENCES

Mercuri:2003:IRS


Mukhopadhyay:2014:EMP


Martel:2004:GMA


Martinez-Nadal:2002:CUM


Meyer:2001:FIC

Monsignori:2001:WMS


Mironov:2008:SAE


MacAndrew:2000:LPT


Mykletun:2006:AIO


Mollin:2001:IC


Møller:2002:PEC

[Möl02] Bodo Möller. Parallelizable elliptic curve point multiplication method with resistance against side-channel attacks. *Lecture Notes in Computer Science*, 2433:
REFERENCES

Moller:2003:PSP


Mollin:2003:RPK


Mollin:2005:CGS

Richard A. Mollin. Codes: the guide to secrecy from ancient to modern times.
REFERENCES

LCCN ???? URL http://deposit.ddb.de/cgi-bin/dokserv?id=2739575&prov=M&dok_var=1&dok_ext=htm

Morris:2003:KKL

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

Moritz:2005:KAE

Hannes Moritz. Kryptanalyse des Advanced Encryption Standard. (German) [cryptanalysis of the
Advanced Encryption Standard]. Diplom-Arbeit, Technische Universität Wien, Wien, Austria, 2005. iii +
116 pp.

Moses:2006:DSD

Phil Moses. Demons seeking demons—a practical approach to hardening your openSSH configuration.

Merton:2000:NBG

Orren Merton and Linda Dailey Paulson. News briefs: Gamers jump into broadband technology; Intel has
new chip design for handhelds; patent expiration begins new encryption era; privacy organization raises

McMillan:2001:JIA

Scott McMillan and Cameron Patterson. JBitsTM implementations of the Advanced Encryption Standard
(Rijndael). Lecture Notes in Computer Science, 2147:162–??, 2001. CODEN LNCSD9. ISSN 0302-
pdf.

Mihaiescu:2001:BRE

70(236):1755–1759, October 2001. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (elec-
REFERENCES

Moshopoulos:2001:NSA


Malkhi:2002:ACE


Maurer:2003:SMR


Micciancio:2005:ASS

REFERENCES


REFERENCES


Murphy:2002:EASa


Murphy:2002:EASb


Matyas:2003:TRU


Micciancio:2009:LBC


Monrose:2002:TSG


Mitchell:2006:PPT

REFERENCES

118–164, March 14, 2006. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).


REFERENCES


REFERENCES


Mahdian:2009:UNI


Manulis:2009:SMF


Mashatan:2009:ITC


Myers:2009:BEC


Shen:2005:NIW


MacKenzie:2002:TPA

REFERENCES


Myasnikov:2005:PAB

Muzereau:2004:EBD

Meseguer:2007:SRA

Ma:2009:NAS

Muller:2001:SWB
Siguna Müller. On the security of a Williams based public key encryption scheme. In Public key


REFERENCES


Ma:2006:ADS


Morelli:2001:JAH

Ralph Morelli, Ralph Walke, and Gregg Marcuccio. A Java API for historical ciphers: an object-oriented
Malan:2008:IPK


MRaihi:2001:CAS


McCook:2001:NSS


Morelos-Zaragoza:2002:AEC


Matsui:2004:SAC

REFERENCES

Nagy:2007:AQK


Naik:2003:DSW


Naftali:2005:BSS


Nakai:2001:SFW

Yuichi Nakai. Semi fragile watermarking based on wavelet transform. Lecture Notes in Computer Science, 2195:796–??, 2001. CODEN LNCSD9. ISSN 0302-
REFERENCES


REFERENCES


NIST:2000:FPD


Nieto:2001:PKC


Nghiem:2009:FBI


Ning:2004:TTA


Nieto:2001:PKC

Nedjah:2005:SHC


Nash:2001:PIM


Nedjah:2004:ECH


Nedjah:2006:NTC


Netscape:2004:HSW


Neuenschwander:2004:PSM

[NFQ03] Amaury Nèove, Denis Flan- 
dre, and Jean-Jacques 
Quiqueter. SOI tech-
nology for future high-


performance smart cards. IEEE Micro, 23(3):58–67, 
May/June 2003. CODEN 
IEMIDZ. ISSN 0272-1732 
(print), 1937-4143 (elec-
computer.org/comp/mags/
mi/2003/03/m3058abs.htm;
http://csdl.computer.
org/dl/mags/mi/2003/03/
m3058.pdf.

[NH02] Phong Q. Nguyen. The 
two faces of lattices in cryp-
tology. Lecture Notes in 
Computer Science, 2259: 
313–??, 2001. CODEN 
LNCS9D. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/2259/22590313.htm;
http://link.springer-
y.com/link/service/series/
0558/papers/2259/22590313.
pdf.

[NH03] Kaisa Nyberg and Howard 
Heys, editors. Selected areas 
in cryptography: 9th annual 
International Workshop, 
SAC 2002, St. John’s, New-
foundland, Canada, Au-
gust 15–16, 2002: Re-
vised Papers, volume 2595 
of Lecture Notes in Com-
puter Science. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2003. CO-
DEN LNCS9D. ISBN 3-540-

relationship between password-
authenticated key exchange 
and other cryptographic 
primitives. In Kilian [Kil05], 
pages 457–?? CODEN 
LNCS9D. ISBN 3-540-
24573-1 (softcover). ISSN 
0302-9743 (print), 1611-
3349 (electronic). LCCN 
QA76.9.A25 T44 2005. URL 
http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b97045.

[Nгу01] Minh-Huyen Nguyen. The
REFERENCES


REFERENCES


REFERENCES


Ning:2008:MAA


Nigrini:2009:DDU


Nagao:2005:UCS


Nozaki:2001:IRA


Northcutt:2002:NID


Naor:2003:CFP

REFERENCES


REFERENCES


[NP02b]

[NP07]

[Nakahara:2001:LCR]

[Naor:2004:NTC]

[Nichols:2000:DYD]
Randall K. Nichols, Daniel J. Ryan, and Julie J. C. H. Ryan. Defending your dig-


REFERENCES

Nguyen:2005:FPL


Nguyen:2005:PSE


Nishioka:2002:DAF


Nyberg:2001:CTC


Nenadic:2005:RBC


Nenadic:2005:RBV

Aleksandra Nenadić, Ning Zhang, and Qi Shi. RSA-based Verifiable and Recoverable Encryption of Signatures and its application
REFERENCES

in certified e-mail delivery. 

**Olson:2003:QHK**


**Oechslin:2003:MFC**


**Oppliger:2008:STS**


**Oppliger:2008:STSa**


**Oiwa:2009:IMS**


**Okamoto:2000:ACA**

REFERENCES

Okamoto:2004:TCC


Ohzahata:2002:FAM


Ogata:2006:OSS


Olson:2000:SCT

REFERENCES


Okamoto:2001:GPN


Okamoto:2001:RRE


Oppliger:2005:CC


Ortiz:2000:ITW


Okeya:2000:PAB

Okeya:2001:EEC


Ostrovsky:2005:PSS


Oren:2006:PAR


Obimbo:2007:PAD


Oury:2008:PP


Overbeck:2009:CBC

Raphael Overbeck and Nicolas Sendrier. Code-based cryptography. In Bernstein et al. [BBD09], pages 95–146. ISBN 3-540-88701-6 (hardcover), 3-642-
REFERENCES

Okeya:2004:SBR

Osvik:2005:CAC

Osvik:2006:CAC

Okeya:2003:MFC
Okeya:2003:WNM


[OT03b]

Okada:2001:IEC


[OTIT01]

Okamoto:2000:QPK


[OTU00]

Ouellette:2005:PPM

John Ouellette. Para


[Oue05]

Overbeck:2006:EGA

Onieva:2008:MNS

Paeng:2003:SCU

Page:2003:BRW

Panditaratne:2007:TRN

Papanikolaou:2005:BRBa

Park:2004:APP

Pass:2003:DCR
[Pas03] Rafael Pass. On deniability in the common reference


REFERENCES


Alessandro Piva, Franco Bartolini, and Roberto Caldelli. Self recovery authentication of images in


Perez:2007:URR


Poulos:2008:TSE


Pucheral:2001:PSD


Petrie:2000:NB1


Peikari:2004:SW


Park:2005:ISC


REFERENCES


Park:2003:EMS


Pan:2007:IBS


Peeters:2007:CES


Petrakos:2009:CTA


Peikert:2009:PKC


Pelzl:2006:PAC

REFERENCES

**Pemble:2001:CEW**


**Pemble:2001:SPA**


**Perrine:2003:ECP**


**Petullo:2003:IEH**


**Petullo:2005:EYR**


**Petzold:2008:ATG**


**Potter:2003:S**

Bruce Potter and Bob Fleck. *802.11 Security*. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol,
REFERENCES


Pfitzmann:2001:ACE


Phatak:2005:FMR


Power:2007:SBB


Provos:2003:HSI


Phan:2004:IDC

REFERENCES

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

**Phan:2006:CTP**


**Paeng:2001:NPK**


**Polk:2003:IIC**


**Phoha:2001:SDI**


**Pieprzyk:2003:FCS**


**Pathak:2006:BFT**

REFERENCES

1389-1286 (print), 1872-7069 (electronic).

Pietrzak:2005:CDI


Pinkas:2002:CTP


Pinkas:2003:CTP


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

Pincock:2006:CHC


Piper:2003:RCS


Park:2001:NDW

REFERENCES

(Park:2001:RFW)


(Poh:2001:HBP)


(Petitcolas:2003:DWF)


(Park:2001:CSC)


[Pfleeger:2007:IBC] Shari Lawrence Pfleeger, Martin Libicki, and Mich-


REFERENCES

Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP


Pornin:2001:THE


Porras:2006:PEG


Potter:2003:WAO

REFERENCES


Potter:2006:CKM


Potter:2007:CWW


Pfleeger:2003:SC


Paul:2006:SSC


Popp:2006:CTT


Pfleeger:2007:SC


Paar:2009:UCT

Christof Paar and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer-Verlag, Berlin, Germany /


REFERENCES

ny.com/link/service/series/0558/papers/2137/21370142.pdf.


[Bart Preneel. The NESSIE Project: Towards new cryptographic algorithms.}
REFERENCES


Preneel:2002:TCC

Preneel:2007:SRD

Price:2000:NCH

Provos:2000:EVM

Provos:2001:DAS

Paun:2004:CTT
Gheorghe P˘ aun, Grzegorz Rozenberg, and Arto Salomaa, editors. Current trends
REFERENCES


[PS00]

[PS01a]

[PS01b]

[PS01c]

[PS02a]
REFERENCES

Pomerance:2002:SOC


Page:2004:PCA


Park:2004:UUC


Prabhakaran:2004:NNS


Prabhakaran:2005:RES


Phan:2006:FDB


Pang:2008:VCR

Pfleeger:2007:GEI

Pucella:2003:JRB

Pucella:2006:SCC

Pucella:2007:Ib

Puzmanova:2004:RWF
Rita Puzmanova. Review of Wi-Foo: The Secrets
REFERENCES

564

Page:2006:FAP


Paillier:2006:TOW


Phillips:2001:GRI


Pang:2005:NMS


Peikert:2008:LTF


Pelzl:2003:HCC


Patrick:2005:FCD


[PY05]

Paterson:2006:LTT


Palanivel:2008:MPA


Pieprzyk:2001:CPS

REFERENCES

[Pieprzyk:2002:CPL]


[Pieprzyk:2002:CCI]


[Pecho:2009:APW]


[Peng:2009:DIE]


[Qian:2005:CLT]


[Qian:2005:SPL]

QUISQUATER:2005:SCC


QUISQUATER:2000:SCR


QUISQUATER:2001:EAE


QUISQUATER:2002:CTM


QUISQUATER:2001:KPW

REFERENCES

link/service/series/0558/1
bibs/2137/21370096.htm;
http://link.springer-
y.com/link/service/series/0558/papers/2137/21370096.pdf.


Rubin:2005:ARS


Rangan:2001:PCI


Renaud:2009:VPC


Rudra:2001:ERE


Romao:2001:SMA

REFERENCES


[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of


[Rescorla:2001:IOPa]

[Rescorla:2001:IOPb]

[Rescorla:2001:IOPc]

[Rescorla:2001:IOPd]

[Rescorla:2001:IOPe]

[Rescorla:2001:IOPf]

[Rescorla:2001:IOPg]

[Rescorla:2001:IOPh]

[Rescorla:2001:IOPi]

[Rescorla:2001:IOPj]

[Rescorla:2001:IOPk]

[Rescorla:2001:IOPl]

[Rescorla:2001:IOPm]

[Rescorla:2001:IOPn]

[Rescorla:2001:IOPo]

[Rescorla:2001:IOPp]

[Rescorla:2001:IOPq]

[Rescorla:2001:IOPr]

[Rescorla:2001:IOPs]

[Rescorla:2001:IOPt]

[Rescorla:2001:IOPu]

[Rescorla:2001:IOPv]

[Rescorla:2001:IOPw]

[Rescorla:2001:IOPx]

[Rescorla:2001:IOPY]

[Rescorla:2001:IOPz]

[Rescorla:2001:IOPaa]

[Rescorla:2001:IOPab]

[Rescorla:2001:IOPac]

[Rescorla:2001:IOPad]

[Rescorla:2001:IOPae]

[Rescorla:2001:IOPaf]

[Rescorla:2001:IOPag]

[Rescorla:2001:IOPah]

[Rescorla:2001:IOPai]

[Rescorla:2001:IOPaj]

[Rescorla:2001:IOPak]

[Rescorla:2001:IOPal]

[Rescorla:2001:IOPam]

[Rescorla:2001:IOPan]

[Rescorla:2001:IOPao]

[Rescorla:2001:IOPap]

[Rescorla:2001:IOPaq]

[Rescorla:2001:IOPar]

[Rescorla:2001:IOPas]

[Rescorla:2001:IOPat]

[Rescorla:2001:IOPau]

[Rescorla:2001:IOPav]

[Rescorla:2001:IOPaw]

[Rescorla:2001:IOPax]

[Rescorla:2001:IOPay]

[Rescorla:2001:IOPaz]

[Rescorla:2001:IOPba]

[Rescorla:2001:IOPbb]

[Rescorla:2001:IOPbc]

[Rescorla:2001:IOPbd]

[Rescorla:2001:IOPbe]

[Rescorla:2001:IOPbf]

[Rescorla:2001:IOPbg]

[Rescorla:2001:IOPbh]

[Rescorla:2001:IOPbi]

[Rescorla:2001:IOPbj]

[Rescorla:2001:IOPbk]

[Rescorla:2001:IOPbl]

[Rescorla:2001:IOPbm]

[Rescorla:2001:IOPbn]

[Rescorla:2001:IOPbo]

[Rescorla:2001:IOPbp]

[Rescorla:2001:IOPbq]

[Rescorla:2001:IOPbr]

[Rescorla:2001:IOPas]

[Rescorla:2001:IOPat]

[Rescorla:2001:IOPau]

[Rescorla:2001:IOPav]

[Rescorla:2001:IOPaw]

[Rescorla:2001:IOPax]

[Rescorla:2001:IOPay]

[Rescorla:2001:IOPaz]

[Rescorla:2001:IOPba]

[Rescorla:2001:IOPbb]

[Rescorla:2001:IOPbc]

[Rescorla:2001:IOPbd]

[Rescorla:2001:IOPbe]

[Rescorla:2001:IOPbf]

[Rescorla:2001:IOPbg]

[Rescorla:2001:IOPbh]

[Rescorla:2001:IOPbi]

[Rescorla:2001:IOPbj]

[Rescorla:2001:IOPbk]

[Rescorla:2001:IOPbl]

[Rescorla:2001:IOPbm]

[Rescorla:2001:IOPbn]

[Rescorla:2001:IOPbo]

[Rescorla:2001:IOPbp]

[Rescorla:2001:IOPbq]

[Rescorla:2001:IOPbr]

[Rescorla:2001:IOPas]

[Rescorla:2001:IOPat]

[Rescorla:2001:IOPau]

[Rescorla:2001:IOPav]

[Rescorla:2001:IOPaw]

[Rescorla:2001:IOPax]

[Rescorla:2001:IOPay]

[Rescorla:2001:IOPaz]


REFERENCES


Ruan:2006:NSC


Reddy:2002:AAM


Riedl:2002:FSH


Roy:2004:FSE


Ruiz:2001:SPS

Antonio Ruiz, Gregorio Martínez, Oscar Cánovas, and Antonio F. Gómez. SPEED protocol: Smartcard-based payment with encrypted electronic deliv-
REFERENCES

ery. Lecture Notes in Computer Science, 2200:
446–??, 2001. CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http:
//link.springer-ny.com/link/service/series/0558/|
bibs/2200/22000446.htm;
http://link.springer-
ny.com/link/service/series/0558/papers/2200/22000446.
pdf.

Reyhani-Masoleh:2003:LCS

[RMH03a] Arash Reyhani-Masoleh
and M. Anwar Hasan.
Low complexity sequential
normal basis multipli-
ers over GF(2^m). In Ba-
jard and Schulte [BS03],
pages 188–195. ISBN
0-7695-1894-X. ISSN
1063-6889. LCCN EV.
URL http://www.acsel-
lab.com/arithmetic/arith16/
papers/ARITH16_Reyhani-
Masoleh.pdf. IEEE order
no. PR01894.

Reyhani-Masoleh:2003:LCB

[RMH03b] Arash Reyhani-Masoleh
and M. Anwar Hasan.
On low complexity bit
parallel polynomial basis
multipliers. In Walter
et al. [WKP03], pages 189–
202. CODEN LNCSD9. [RMS05]
ISBN 3-540-40833-9. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
TK7895.E42. URL http:
//link.springer-ny.com/
link/service/series/0558/

tocs/t2779.htm; http:
//www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2779; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/|
b13240.

Reyhani-Masoleh:2004:TFT

Arash Reyhani-Masoleh
and M. Anwar Hasan. To-
wards fault-tolerant crypto-
graphic computations over
finite fields. ACM Trans-
actions on Embedded Com-
puting Systems, 3(3):593–
613, August 2004. CO-
DEN ????. ISSN 1539-9087
(print), 1558-3465 (elec-
tronic).

Rahaman:2008:CTB

H. Rahaman, J. Mathew,
D. K. Pradhan, and A. M.
Jabir. C-testable bit paral-
lel multipliers over GF(2^m).
ACM Transactions on De-
sign Automation of Elec-
tronic Systems, 13(1):5:1–
5:??, January 2008. CODEN
ATASFO. ISSN 1084-4309
(print), 1557-7309 (elec-
tronic).

Ryabko:2005:NTA

B. Y. Ryabko, V. A.
Monarev, and Y. I. Shokin.
A new type of attack on
block ciphers. Problems of
Information Transmission,
CODEN PRITA9. ISSN
REFERENCES

0032-9460 (print), 1608-3253 (electronic).


REFERENCES


Rothe:2007:BRB


Roy:2000:PCI


Roychowdhury:2000:PCJ


Roy:2005:ACA


Rieffel:2000:IQC

REFERENCES


[RSS01] Tanja Römer and Jean-Pierre Seifert. Informa-


Rubin:2008:CFF

RSA:2000:PKC

RSA:2000:PCP

RSA:2000:PVC

RSA:2000:PVS

RSA:2001:PVC

RSA:2002:PVR
RSA Laboratories. *PKCS #1 v2.1: RSA Cryptography Standard*. RSA
REFERENCES


REFERENCES


REFERENCES


[Ren03a] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy


org/mi/books/mi2001/pdf/m6004.pdf.


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


Samtani:2009:WTO

Santini:2005:WSI

Sarkar:2002:FCM

Sasse:2007:REB

Satoh:2006:DPI

Savelli:2004:NDC

Soto:2000:RTA
Juan Soto and Lawrence E. Bassham. Randomness testing of the Advanced Encryption Standard finalist candidates. NIST internal report 6483, National

**Shacham:2001:ISH**


**Scott:2004:CP**


**Stoklosa:2005:CIC**


**Stallings:2007:CSP**


**Sherwood:2005:MTR**


**Steiner:2001:SPB**

Michael Steiner, Peter Buhr-


Seredynski:2004:CAC


Syverson:2001:LAP


Shen:2002:NDW


Stoll:2002:MMC


Sun:2002:WDC


Shao:2005:NEV

Stephanides:2005:GAK


Sun:2005:IPK


Siegelin:2001:SCD


Schmalz:2000:MAD


Schneier:2000:IRS


Schneier:2000:AR

Bruce Schneier. Inside risks: semantic network attacks. Communications of the Association for Comput-
REFERENCES


Schneier:2001:FSE

Schnorr:2001:SDE

Schultz:2002:GBC

Schneier:2003:BFT

Schmalz:2004:MDIa
Mark S. Schmalz, editor. *Mathematics of data/image coding, compression, and encryption VI, with applications: 5 and 7 August*. No scheduled publication date.
REFERENCES


Schneier:2005:TFA

Schramm:2006:AMS

Schroeder:2006:NTS

Schneier:2007:NCS

Schneier:2008:SS

Schmeh:2009:VBF

Su:2005:IBT
REFERENCES

Scott:2004:CIB


Screamer:2001:MDR


Shen:2005:NCB


Sun:2005:RNK


Sebe:2001:OIW


Sebe:2000:SDI

Francesc Sebé, Josep Domingo-

Smith:2006:CNS


Smith:2001:ADB


Spiekermann:2009:ACR


Seacord:2005:SCC


Seacord:2009:CCS


Seetharaman:2004:BRB

Priya Seetharaman. Book review: Beyond Fear—Thinking Sensibly About Security in an Uncertain

Smith:2006:SID


Seifried:2000:C


Seifried:2000:PPA


Seifert:2005:ACR


Speed:2001:PIS


Speed:2002:PIS


Selcuk:2000:BEL

Ali Aydn Selçuk. On bias estimation in linear crypt-


REFERENCES


[SGB08] Rainer Steinwandt, Willi Geiselmann, and C¸etin Kaya Koç. Guest Editors’ introduction to the special section on special-purpose hardware for cryptography and cryptanalysis. *IEEE Transactions on Computers*,
REFERENCES


**Sonntag:2000:MAS**


**Shirase:2005:AEC**


**Shailer:2001:PMT**


Shamir:2003:TLC  

Shao:2004:IDS  

Shao:2005:CXY  

Shao:2005:IEP  
AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).


Hwang:2009:KDB


Shepherd:2001:CDC


Sung:2007:CIB


Shim:2005:LPG


Shih:2008:DWS

Frank Y. Shih. *Digital Watermarking and Steganography: Fundamentals and Techniques*. Taylor and


[Shp02] Igor E. Shparlinski. Security of most significant bits...
REFERENCES


**Shparlinski:2003:CAA**


**Shparlinski:2004:BRR**


**Shparlinski:2004:UDD**


**Shparlinski:2005:PHS**


**Sun:2005:SSP**

Shumba:2006:THL

Shyamasundar:2002:ACP

Silverman:2005:ECC

Simon:2002:CRE

Singh:1999:CBE
REFERENCES


REFERENCES


REFERENCES

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

Stojanovski:2001:CBRa


[SK01b]

Sklavos:2003:DDR


[SK03]

Sklavos:2005:ISH


[S KG09]

Shu:2009:RCA

Chang Shu, Soonhak Kwon, and K. Gaj. Reconfigurable

Stavrou:2005:CAS


[SK06]

Stabell-Kulo:2006:ESC


[S K07]

Saldamli:2007:SME


[SKG07]


K. Srinathan, M. V. N. Ashwin Kumar, and C. Pandu Rangan. Asynchronous secure communication tolerating mixed adversaries. *Lec-
Sugita:2000:RAD


Schneier:2000:CTA

REFERENCES

Sterbenz:2000:PAC


Shim:2005:SFA


Srivatsa:2005:SPS


Skoudis:2006:CHR


Stamp:2007:ACB


Sun:2009:CPR

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>key cryptosystem based on elliptic curve discrete logarithm. *Applied Math-</td>
</tr>
<tr>
<td></td>
<td>ematics and Computation*, 168(1): 40–46, September 1, 2005. CODEN AMHCBCQ.</td>
</tr>
<tr>
<td></td>
<td>ISSN 0096-3003 (print), 1873-5649 (electronic).</td>
</tr>
<tr>
<td>Shi:2005:HEC</td>
<td>Weidong Shi, Hsien-Hsin S. Lee, Minmoy Ghosh, Chenghuei Lu, and Alexan-</td>
</tr>
<tr>
<td></td>
<td>dra Boldyreva. High efficiency counter mode security architecture via</td>
</tr>
<tr>
<td></td>
<td>prediction and precomputation. <em>ACM SIGARCH Computer Architecture News</em>,</td>
</tr>
<tr>
<td></td>
<td>33(2):14–24, May 2005. CODEN CANED2. ISSN 0163-5964 (print), 1943-5851</td>
</tr>
<tr>
<td></td>
<td>(electronic).</td>
</tr>
<tr>
<td></td>
<td>the timestamp-based password authentication scheme using smart cards.</td>
</tr>
<tr>
<td></td>
<td>Provable security for the Skipjack-like structure against differential</td>
</tr>
<tr>
<td></td>
<td>cryptanalysis and linear cryptanalysis. *Lecture Notes in Computer Sci-</td>
</tr>
<tr>
<td></td>
<td>(electronic).</td>
</tr>
<tr>
<td>Salido:2007:EBE</td>
<td>Javier Salido, Loukas Lazos, and Radha Poovendran. Energy and bandwith-</td>
</tr>
<tr>
<td></td>
<td>efficient key distribution in wireless ad hoc networks: a cross-layer</td>
</tr>
<tr>
<td></td>
<td>December 2007. CODEN IEANEPR. ISSN 1063-6692 (print), 1558-2566</td>
</tr>
<tr>
<td></td>
<td>gery detection in printed materials. *Lecture Notes in Computer Sci-</td>
</tr>
<tr>
<td></td>
<td>ence*, 2195:403–??, 2001. CODEN LNCSDF9. ISSN 0302-9743 (print), 1611-3349</td>
</tr>
<tr>
<td></td>
<td>bibs/2195/21950403.htm;</td>
</tr>
</tbody>
</table>
REFERENCES

Solar-Lezama:2006:CSF

Sarkar:2000:CNB

Sarkar:2000:NBC

Sarkar:2001:EIL


REFERENCES


Smith-Miles:2008:CDP


Smart:2001:CDF


Smart:2003:ACU


Smart:2003:AGR


Smart:2005:CCI


[SMP+09] Kent Seamons, Neal McBurnett, Tim Polk, et al., edi-
REFERENCES


**Satoh:2001:CRH**


**Strembeck:2004:IAE**


**Schläger:2007:EAA**


**Sakai:2000:NDS**


**Srinathan:2004:OPS**


[Safavi-Naini:2000:STT]


[Safavi-Naini:2001:BAG]


[Safavi-Naini:2001:LAC]


[SOIG07]

REFERENCES


Song:2000:ISC


Shigetomi:2002:ALS


Satoh:2000:HSM


Smith:1979:UFM


Shelfer:2002:SCE


REFERENCES

Sun:2008:BWN


Stern:2002:FAP


Shin:2000:ANT


Song:2001:ANL


Springer:2003:BRB

REFERENCES

StDenis:2006:BMI

Stipcevic:2007:QRN

Samarati:2001:AMP

Standaert:2003:EIR

Sarkar:2001:PAE
REFERENCES

629

Stubblebine:2001:AAF
[SS01b]

Stuart G. Stubblebine and [SSFC09]
Paul F. Syverson.
Authentic attributes with finegrained anonymity protection.
Lecture Notes in
Computer Science, 1962:
CODEN
LNCSD9.
ISSN 03029743 (print), 1611-3349
(electronic).
URL http:
//link.springer-ny.com/
+
link/service/series/0558/ [SSM 08]
bibs/1962/19620276.htm;
http://link.springerny.com/link/service/series/
pdf.
Seznec:2003:HUL

[SS03]

André Seznec and Nicolas Sendrier. HAVEGE: a
user-level software heuristic for generating empirically strong random numbers.
ACM Transactions
on Modeling and Computer
Simulation, 13(4):334–346,
October 2003.
CODEN [SSNGS00]
ATMCEZ. ISSN 1049-3301
(print), 1558-1195 (electronic).
Swiderski:2004:TM

[SS04]


Seddik:2009:IWB
Hassen Seddik,
Mounir
Sayadi, Farhat Fnaiech, and
Mohamed Cheriet. Image
watermarking based on the
Shi:2008:UAU
Minghui Shi, Xuemin (Sherman) Shen, Jon W. Mark,
Dongmei Zhao, and Yixin
Jiang.
User authentication and undeniable billing
support for agent-based
roaming service in WLAN/
cellular integrated mobile
networks. Computer Networks (Amsterdam, Netherlands: 1999), 52(9):1693–
1702, June 26, 2008. CODEN ???? ISSN 1389-1286
(print), 1872-7069 (electronic).
Susilo:2000:NEF
Willy Susilo, Rei SafaviNaini, Marc Gysin, and
Jennifer Seberry. A new
437, ????
2000.
CODEN CMPJA6.
ISSN
0010-4620 (print), 14602067 (electronic).
URL
http://www3.oup.co.uk/
computer_journal/hdb/Volume_
43/Issue_05/430430.sgm.
abs.html;
http://www3.


Scambray:2006:HEW


Schmidt-Samoa:2006:AFW


StPierre:2000:TFA


Sakurai:2001:NSS


Shamir:2001:IOO


Stern:2001:ADW

Julien P. Stern and Jean-Pierre Tillich. Automatic detection of a watermarked document using a private key. *Lecture Notes in
REFERENCES


REFERENCES


William Stein. Elementary number theory: primes, congruences, and secrets, volume 666 of Undergrad-

Stinson:1995:CTP


Stinson:2001:C


Stinson:2002:CTP


Stieber:2006:OH


Stieber:2006:GH


Stinson:2006:CTP


[Sax07] Nitesh Saxena, Gene Tsudik, and Jeong Hyun Yi. Threshold cryptography in P2P and MANETs: The case

Shaltiel:2007:LEU


Sugihara:2001:PCD


Sugita:2003:DRW


Sun:2000:DRR


Sun:2000:ESM


Sun:2002:IIR


Sun:2005:UMS

REFERENCES


Seidl:2008:FOV

Shaltiel:2008:HAP

Sebe:2007:SMO

Shmueli:2009:DEO

Smith:2000:CIR

Schneier:2000:PCF
REFERENCES


Sun:2000:AFA


Stubblebine:2002:ALF


Shim:2005:WIB


Shieh:2006:ERM


Swaine:2001:PPSa


Swenson:2008:MCT

REFERENCES


Song:2005:ISG


[SWH05]

Sun:2009:TDS


[SWH+09]

Swire:2005:SMI


[Swi05]

Stevenson:2005:SCI


[SWR05]

Song:2007:TAK


[SWT07]

Shujun:2001:PRB

Seo:2001:CDA


Shi:2001:NSF


Syed:2000:CLA


Sun:2006:PBA


Sun:2005:CSS


Syverson:2002:FCI

Paul F. Syverson, editor. Financial Cryptography: 5th
Shimoyama:2002:BCS


Steinfeld:2001:ALE


Skoudis:2003:MFM


Sarikaya:2008:SPT

REFERENCES

[Sun:2002:NAD]

[Sun:2005:WIW]

[Tada:2002:OSM]

[Tan07a]

[Tan07b]

[Tattersall:2005:ENT]

REFERENCES

521-85014-2 (hardcover), 0-521-61524-0 (paperback), 0-511-75634-8 (e-book). xi + 430 pp. LCCN ????


REFERENCES

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

Tsai:2002:SMS


Trudel:2003:DSE


Teepe:2006:PPA


Todd:2001:LSS


Terai:2008:BRB


Thorsteinson:2004:NSC

Theoharidou:2007:CBK


Tirkel:2001:UWE


Tabatabaian:2001:NSP


Tippett:1927:RSN


Torres:2007:ANS


Tseng:2001:GGO


Tsai:2005:CAE


Tan:2004:OBC


Tokita:2001:ADC


Tang:2006:CHA


Torrubia:2001:CRC


Tian:2005:RWS

Tsolis:2009:ARM


Teoh:2004:PCK


Tousidou:2000:IMS


Tomaszewski:2006:YSY

REFERENCES

Topham:2002:BRJ


Totsch:2000:MSS


Tague:2007:CSA


Trope:2007:CSD


Trimberger:2001:GED


Troutman:2009:CCGa

Troutman:2009:CCGb


Troutman:2008:VMM


Tsaur:2001:FUA


Tsaur:2005:SSS


Tsaban:2006:FGD


Tsang:2007:WCT


Tsai:2008:EMS

REFERENCES

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


REFERENCES


[TW02] Wade Trappe and Lawrence C. Washington. Introduction to Cryptography


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


REFERENCES

Tong:2009:RAPb


Uz:2009:MBT


Unay:2008:SQE


Uchida:2009:FPR


USC:2000:HRS

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


[USE00a] USENIX, editor. Proceed-


USESIX:2001:PTU


USESIX:2002:PBF


USESIX:2002:PUS


USESIX:2002:PFT


Utami:2002:FID


Urien:2001:XS

Ustimenko:2001:CGT

Ulfving:2000:GS

Uzun:2004:BRC

Vacca:2006:GWN

Vadhan:2003:CLC
Vanstone:2003:NGS


Vaudenay:2002:SFI


Vaudenay:2005:PKC


Verheul:2001:EXM

Vercauteren:2002:CZF

Vergnaud:2006:RBS

Vernitski:2006:CUM

Vladimirov:2004:WFS

Vassev:2009:STA
REFERENCES

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


[VN04] Steven J. Vaughan-Nichols. Voice authentication speaks to the marketplace. Com-
REFERENCES


scheme in the presence of transient hardware faults.  
CODEN ?? ?? ISSN 1539-9087 (print), 1558-3465 (electronic).

**vanTilborg:2000:FCP**

Henk C. A. van Tilborg.  
*Fundamentals of cryptology: a professional reference and interactive tutorial*, volume SECS 528 of *The Kluwer international series in engineering and computer science*.  
xiv + 490 pp.  

**vanTilborg:2001:ECC**

Henk van Tilborg.  
Elliptic curve cryptosystems; too good to be true?  
ISSN 0028-9825.

**vanTilborg:2005:ECS**

Henk C. A. van Tilborg, editor.  
*Encyclopedia of cryptography and security*.  
x + 684 pp.  
US$299.00.

**Vaudenay:2007:POK**

Serge Vaudenay and Martin Vuagnoux.  
Passively only key recovery attacks on RC4.  
LCCN QA76.9 2007.  

**Venkatesan:2001:GTA**

Ramarathnam Venkatesan, Vijay Vazirani, and Saurabh Sinha.  
A graph theoretic approach to software watermarking.  
CODEN LNCSD9.  
ISSN 0302-9743 (print), 1611-3349 (electronic).  
URL http://link.springer-ny.com/link/service/series/0558/bibs/2137/21370157.htm;  
vonWillich:2001:TIT


Vaudenay:2001:SAC


Whittaker:2006:HBW


Woody:2007:COS


Weitzner:2008:IA


Wachsmann:2005:CAK

Wallach:2000:SSM


Wagner:2000:CYL


Wagner:2002:GBP


Walsh:2000:BRM

Walter:2001:PBM


Walter:2003:STM


Wang:2004:AWA


Wang:2004:TVS


Wang:2005:SCR

REFERENCES


REFERENCES


[WBRF00] Bryan Weeks, Mark Bean, Tom Rozyloowicz, and Chris
REFERENCES


Wong:2001:EMA


[WC01b]


Wu:2003:UFR


Wu:2004:EIW


Wu:2001:CKA

Hsien-Chu Wu and Chin-Chen Chang. Embedding invisible watermarks into digital images based on side-match vector quantization. Fundamenta Informaticae,
REFERENCES


Wu:2005:NDI


Wang:2005:SDR


Westerlund:2001:HWK


Williams:2001:ICA


REFERENCES


Wu:2002:IBM


Wu:2003:TSS


Wang:2009:NWM


Wen:2005:URE


Wu:2008:RPG


Watanabe:2001:EAP

REFERENCES


REFERENCES


Wilcox:2001:SEH


Wilson:2001:PBA


Williams:2006:C


Winterbotham:2000:USI


Wincelberg:2001:JQH


Windley:2005:DI


Winkel:2005:GEC

REFERENCES


REFERENCES


[WLH06] Hsiang-An Wen, Chun-Li Lin, and Tzonelih Hwang. Cryptanalysis of an enhanced timestamp-based password


Wheeler:1995:TTE


Watanabe:2002:CCD


Wang:2008:NAD


Wolkerstorfer:2001:AIA


Wolfe:2003:EE

Wollinger:2004:SHI


Won:2001:ISC


Wool:2000:KME


Wang:2003:SGP


Wollinger:2005:CVH

Weimerskirch:2001:ECC


Wang:2001:TUR


Wright:2000:IQC


Wright:2001:AES


Wright:2003:FCI


André Weimerskirch and Gilles Thonet. A distributed light-weight authentication model for ad-hoc networks. Lecture
REFERENCES


David P. Woodruff and Marten van Dijk. Cryptography in an unbounded computational model. *Lecture
REFERENCES


REFERENCES


**Wu:2001:CFF**

**Worley:2000:AFP**

**Wollinger:2000:HWH**

**Wincelberg:2002:LIE**
David Wincelberg, Sy Wong, Dan Leach, Paul Keister, and Robert Masta. Letters: Inside eBook security; numerical weather forecasting; FrontPage EULA; priority queues; audio watermark-


[Wang:2005:FCFa]


[Wang:2005:FCFb]


[Wang:2005:DIC]


[Xu:2001:EIE]

Sheng-Bo Xu and Lejla Batina. Efficient implementation of elliptic curve cryptosystems on an ARM7 with hardware accelerator. Lecture Notes in
REFERENCES


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

**Xu:2009:AVB**


**Yan:2000:NTC**


**Yang:2002:NEC**


**Yang:2005:TFN**


**Yang:2007:CAR**


**Yasuda:2008:DLP**


**Yuan-bo:2004:ITA**


**Yue:2001:GNN**


[YCH04] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang

Yu:2007:NSM

Yu:2008:NFD

Yang:2007:IIS

Yung:2006:PKC


Yekhanin:2007:LDC

Yan:2006:ICP


Youssef:2001:CIM


Youssef:2001:IAB


Yang:2005:IME


Yamamura:2000:QCB

Akihiro Yamamura and Hirokazu Ishizuka. Quantum

Yamamura:2001:EDA


Yi:2004:AKA


Yen:2002:CAO


Yen:2002:RSR

REFERENCES


[YU:2005:EHI] Jia Yu, Daxing Li, and


[You06] Anne L. Young. Mathematical ciphers: from Caesar to RSA, volume 25 of Mathematical world. American Mathematical Society,
REFERENCES

703

Providence, RI, USA, 2006.
159 pp. LCCN ???.

[YPKL08]
Taek-Young Youn, Young-
Ho Park, Changhan Kim,
and Jongin Lim. Weakness
in a RSA-based password
authenticated key exchange
protocol. Information Pro-
342, November 30, 2008.
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

[YPPK09]
Yin Yang, Stavros Pa-
padopoulos, Dimitris Pa-
padias, and George Kol-
llos. Authenticated index-
ing for outsourced spatial
databases. VLDB Jour-
nal: Very Large Data Bases,
CODEN VLDBFR. ISSN
1066-8888 (print), 0949-
877X (electronic).

[YPSZ01]
Kangkang Yin, Zhigeng
Pan, Jiaoying Shi, and
David Zhang. Robust
mesh watermarking based
on multiresolution pro-
cessing. Computers and Graph-
ics, 25(3):409–420, June
ISSN 0097-8493 (print),
1873-7684 (electronic). URL
http://www.elsevier.nl/
gej-ng/10/13/20/57/32/
32/abstract.html; http://
www.elsevier.nl/gej-
ng/10/13/20/57/32/32/article.
df.

[Yilek:2009:WPK]
Scott Yilek, Eric Rescorla,
Hovav Shacham, Brandon
Enright, and Stefan Sav-
age. When private keys
are public: Results from the
2008 Debian OpenSSL vul-
nerability. In ???, edi-
tor, ACM Internet Measure-
ment Conference, page ??
ACM Press, New York, NY
10036, USA, 2009. ISBN
???. LCCN ???. URL ??.

[Yoon:2004:SUA]
Eun-Jun Yoon, Eun-Kyung
Ryu, and Kee-Young Yoo.
A secure user authenti-
cation scheme using hash
functions. Operating Sys-
tems Review, 38(2):62–68,
April 2004. CODEN OS-
RED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic).

[Yoon:2005:CFI]
Eun-Jun Yoon, Eun-Kyung
Ryu, and Kee-Young Yoo.
Cryptanalysis and further
improvement of Peinado’s
improved LHL-key authen-
tication scheme. Applied
Mathematics and Com-
putation, 168(2):788–794,
September 15, 2005. CO-
DEN AMHCBQ. ISSN
References

Yoon:2005:ICJ


Yoon:2005:IFA


Yoon:2005:IHL


Yeh:2002:SAK


Yeh:2004:PBU


Yanami:2002:DLC

REFERENCES


REFERENCES

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


Yang:2004:CUF


Yang:2005:CIA


Yang:2008:VCS


Yang:2008:FSD

G. Yang, D. S. Wong, and X. Deng. Formal security definition and efficient construction for roaming with
REFERENCES

Yang:2005:SAS


Yang:2008:TFM


Yang:2009:CLW


Young:2000:RBA


Young:2001:BOK


Young:2004:MCE

Adam Young and Moti Yung. *Malicious cryptography: exposing cryptovirology*. John Wiley and Sons,
REFERENCES

Yoon:2005:CZX


Yoon:2005:SWL


Ye:2001:ATD


You:2001:GEC


Yen:2000:WOW

REFERENCES


REFERENCES


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 ????

Zhao:2000:MCA


Zhao:2004:AIB


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

Zhang:2000:MCA


Zhang:2004:AIB


Zhang:2005:CHC


Zhang:2009:CII


Zhang:2001:SOS

Zhou:2005:PSP


Zhu:2004:DSM


Zunino:2005:WPE


Zhao:2006:SAP


Zeadally:2000:IPQ


Zhang:2005:CSS


Zhen:2004:IBS

Z. Zhen, B. Fei, and L. Kejun. The implementation of


REFERENCES

Zheng:2002:NPK


Zheng:2002:ACA


Zhou:2002:MVD


Zhong:2006:ESC


Zirkind:2007:ADC

REFERENCES

2007. CODEN CGRADI, CPGPBZ. ISSN 0097-8930 (print), 1558-4569 (electronic).


Zhang:1999:AFV

Zhang:2001:CIS

Zhang:2005:DMC

Zhou:2005:MBI


REFERENCES

X/S0025-5718-03-01545-X.tex.


[ZWWL01] Yuqing Zhang, Chunling


Zhang:2008:FIC

Zeng:2001:CHR

Zhuang:2005:KAE

Zhu:2007:EIB