Title word cross-reference

<table>
<thead>
<tr>
<th>#1</th>
<th>[Man01, RSA02]. #10 RSA00b.</th>
<th>#11 RSA01, Clu03.</th>
<th>#13 RSA03b.</th>
<th>#15 RSA00d, RSA00e.</th>
<th>#9 RSA00e.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p_k) [BINP03]. (t, n) [CHY05a, HL05c, Kog02, LKL+01, YCH04, CLT07]. (tn) [PW05, SC05a]. + [Abe01]. {0, 1} [LBGZ01, LBGZ02]. 1 [Wu02]. $125 [And04]. 128 [AIK+01, PCG01]. 13 [HSL+02]. $15.00 [Inmr03]. 2 [Bih00, BGN05, CY02, CLT+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, ChLYL09, 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]. \text{ABC} [PS04b]. d [BD00b]. E_{0} [FL01a]. f_{8} [KSHY01]. g^{2} [Shp02]. g_{e}(x,1) [SZP02]. GF(2) [CP03]. GF(2^{m}) [OTIT01, RMPJ08]. GF(p^{n}) [BGK^{+}03]. GF(pt) [PZ01]. H_{2}A [CBB05]. k [BJLS02, CT08b, GPC08, HKS00, QPV05, WL02]. l [QPV05]. M + 1 [AS01a]. F_{q} [CY02]. Z_{n} [Gro05]. GF(2) [GS03, KTT07]. GF(2^{m}) [BBGM08, KTT07, KWP06, RMH03a, RS04]. GF(2^{n}) [KKH03]. SL_{2}(F_{2^{n}}) [SGGB00]. N^{0.292} [BD00b]. NC^{0} [AIK06]. p [FL06].</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
$p^r q^s$ [LKYL00]. $p^s$ [CHH01]. $Q$ [Yas08]. $r$
[JY01]. $w$ [DwWmW05, OT03b]. $x^w$ [Gon06].
y [OS01]. $Z_n$ [LWL09].

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

.NET [For04, TG04].

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

0 [And04, BC04a, Gum04, Imr03, Puz04, WYY05d]. 0-07-222742-7 [Gum04].
0-13-100851-X [For04]. 0-226-74410-8
[Top02]. 0-262-14075-6 [Pag03].
0-321-20217-1 [Puz04]. 0-385-49532-3
[Imr03]. 0-470-84402-7 [And04]. 024-Bit
[GS07a]. '05 [ACM05b, MS05b, ZC09]. '07
[ACM07]. '08 [ACM08]. '09
[ACM09, IEE09a].

1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05c, WYY05d, Was08a].
1-58488-518-1 [Was08a].
1-Connected [BJLS02]. 1-out-of-n
[AOS02]. 1.82GBits [KV01].
1.82GBits/sec [KV01]. 101 [Sci00a].
10118-3 [ISO04]. 106
[Uni00c, Uni00d, Uni00g]. 106-1
[Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a].
109-bit [Pri00]. 10th [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. 11-15
[AUW01]. 11th [CCMR05, HYZ05b, HH04, HH05, Roy05, USE02b]. 12 [TPS01].
128 [JY02, 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].
192-bit [Luc00]. 1930s [Bur02]. 1960s
[PPV96]. 1999
[Lee03b, Uni00a, Uni00f, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Uni01].
19th [BCDH09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000
[CGH+00b, Eke02, Irw03, KH08, KI01a, Sch00b, Wit01, YG01c]. 2001
[ACM01a, BC01, GJSS01, Lee03a, Pem01b]. 2002
[B+02, IEE02, RSA03a, Yun02a]. 2003
[ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, WK03]. 2004 [ACM04b, ZC04].
2005 [ACM05a, ACM05b, ACM05c, ANS05, HYZ05b, ISO05, Roy05, Ter08, Ytr06]. 2006
[ACM06]. 2007 [ACM07, Ano06b, SM07b].
2008 [ACM08, Dew08, YRS+09]. 2009
[ACM09, May09]. 20th [Bel00]. 21 [AJ01b].
21264 [WB00]. 21st [Jef08, Kii01a]. 21th
[IEE09a]. 22 [McK04, TZZ01]. 22nd
[Yun02a]. 23rd [Bon03]. 24th
[Cra05a, Fra04]. 256-bit [Luc00]. 25th
[Sho05a]. 26 [DB04]. 26th [EBC+00]. 27th
[Men07]. 29 [Eke02]. 29th [FLA+03].

3 [Duw03, Imr03]. 3-515-07640-9 [Eag05].
3-540-66778-4 [Duw03]. 3-Key [Kel05].
3.0 [Flu02a, Hei01, SQ01]. 305 [ECM00a].
306 [ECM00b]. 30th [Coc02a]. 314pp
[Duw03]. 3278 [BWBL02]. 33rd [ACM01a].
36th [ACM04b]. 37th [ACM05c]. 39th
[ACM07]. 3D [LZP+04]. 3GPP
[KSH01, SM02]. 3rd [ACM05a, USE00a].
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].
Adrian [MaaTxx]. Adleman [BB79, Coc03, SP79].
Administration
[USE00c, USE00a, Ris06, WL04a].
administrative [Cra05b]. Admitting
[HSZI00]. Advance [CZB+01]. Advanced
[CF07, DFPS06, Lan00a, Lut02, MM01c, Mor05, Scho0a, BBK+03b, DFCW00, ISTE08, Swe08, Tan01, Ase02, Bar00c, III00, Bur03, CMR06, Cuc02b, DR01, DR02b, Dan01, DRS05, FIP01a, GC01a, Har00, Her09a, Lan04a, MP01a, Mor05, NIS00, Pha04, SB00, Sye00, WBRF00, WFR01, YW06]. Advances
[Aki09, Bel00, BSS04, BSS05, Bon03, Boy01, Cla00a, DFPS07, ELv01, Kili01, Oka00, Pl01a, Pre00, TIS07, Yun02a, Kat01, Bib03, CC04a, Cra05a, Fra04, Knu02, Lai03, Lee04b, LLT+04, Li05, LST+05, Men07, Roy05, Sho05a, Zhe02b]. Advantage [SZ01].
advantages [CDS07]. adventures [Hro09].
Adversarial [CLR09, GSS08, MNS08].
Adversarial-knowledge [CLR09].
Adversaries [CM00, JQY01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05]. Adversary
[Aba00, Gor06, RW02]. AES
[CGH+00b, DRS05, FIP01a, Her09a, Pha04, AG01, Ano00a, AL00b, BDK+09, CG03, Coc02b, DR00b, DR02a, DR02b, DLP+09, DPR01, Dan01, Dra00, EYCP00, Fer06, FM02b, GC00a, HW03b, IBM00, IKM00, IK00, IK01, Joh00, KS09a, Kel05, KS00a, KV01, LP02a, Len01, MHM+02, Mes00, Mes01, MR02a, MR02b, OST05, OST06, PBTW07, PQ03b, RRY00, SKKS00, SM03b, Sch00b, SKW+00, SW00a, SL00, WW00, WB00, WOL01, WWGP00, WWCW00].
AES-CBC [Fer06]. AES-like [DLP+09].
AES-related [Sch00b]. Affine
[Ben00, CT09, Fel06, HH09].
Affine-Transformation-Invariant [CT09].
AFIS [Zir07]. African [WD01b]. after
[Ber03, McL06]. again [Fox00]. Against
[CS05b, DM07b, FKS000, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, Ava03, Bau05, BPR00, BP02, BBN+09, BB+02, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egh00, EBS01, FP01, Fry00, Geb04, HNZI02, HLL+01, HG07, Hsu05b, HLC08, Inv05, ISW03, IIT03, JKS02, J00b, J01a, Kan01, KM02, KML+02, LM08, LP+09, Lu02, Mit00, Mıl02, MG08, NRR00, NLD08, OKS06, OSS00, OT03a, OT03b, PKBD01, PSC+02, PSS+08, PS01b, PQ03b, RS01, SKQ01, Sc01b, Sc01f, SDFH00, SDF01, Sem00, Sho00b, SKU+00, SKI01, SLL+00, Tad02, TV03, VHP01, X05, Y00, YKL02b, YKL03b, YKL04, ZCW04, ZSJN07]. Age [Mar08b, Lev01]. Agency
[AJ08, Bm02, Kov01]. Agent
[HQ05, KV02, PDZD09, RS01, RC01, Rot01, ZYM05, KXD00, SSM+08, SH00].
Agent-Based [HQ05, SSM+08]. Agents
[WHI01, Hau06, LSA+07]. Ages
[Eag05, Kin01]. Aggregate
[BGLS03, WK05]. Aggregated [ZSN05].
Aggregation [Her06, CCM09, MS09b].
Aggressive [Wy05]. AGM [Gau02].
Agreement [AAAG01, CT08a, GW00, HR05, HS07, RSW03a, SK00, Tan07b, ABB+04, AKNT04, CYY05, CYH05, Che04a, CY05, CJ04, CJL05, HWWM03, Jua04, KPT04, KRY05, KKH05, LKKY03a, LKYY03b, LL04a, LLL04, LL05a, LKY05b, LKY05b,
LKY05c, LKY05d, LLY06, LLS+09, LLR02, 
PQ03a, PQ06, SW06, Shi05, SW05, SC05b, 
Tsa06, Tse07, VK08, YW05, YC09b, YS02, 
YS03, Yi04, YRY05b, ZC04, LLR06].

Agricultural [Lov01]. Aided 
[NS01b, HLL+02]. aim [Pau02a]. Aimed 
[SFDF06]. Airport [Sas07]. airwaves 
[Dav07]. Ajtai [GK05]. AKS [Che03]. A1 
[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 
[NCRX04]. alerts [AN01c]. alert [AJ08].

alerts [NCHR04]. Alexandria [MS05b].

Algebra [Cou01, CD01a, Lan04a, CKY07, 
Fau09, HW03a, HWR09, Sh005b].

Algebraic [AK05, Bar09, Can06b, CM06, 
CM03, Cou03, CFS05, FJ03, FSW01, GV05, 
GPS06, HR04a, HMO2b, Hug02, Mas04, 
MNP01, MR02a, MR02b, PDMS09, Bul09, 
CKN06, CDL06, Iwa08, May09].

algebraically [RBF08]. algebras 
[BDFP02]. Algorithm [ANS05, AEMR09, 
Bar00a, Bar00c, Bi09, BSC01a, ClhLYL09, 
CU01, CJS0a, CJ03a, CTLT01, CG03, 
COC06, CH07c, CKM00, CT03, CP03, DR01, 
DG00, Dhe03, EYCP00, FBW01, FMS01, 
GMM01, HTS02, HMO2c, HZLS05, JJK+01, 
KBD03, KMM+06, KY02c, KLb+02a, KTT07, 
KV01, LPZ06, MM01b, MM01c, MS02e, 
NMSK01, OS01, PZL09, PBWT07, Ram01, 
RS01, SS01a, SPQ06, WHLH05, Wes01, 
Wie00, AJ080, App05, BF06a, Bla00, C009a, 
CHC01, CKY05, CYH+07, CHH01, FP09, 
Fer06, FSGV01, GPX08, Jon08, KJ01, 
Kw002, Kw003b, LCP04, LLLZ06a, LLLZ06b, 
MN14, OS07, SC05a, SM08, SPZ02, TM01, 
WL02, WN05, Wue09, YRY05c, And03, SA02].

Algorithmic [Hro09, Jou09, Has01b].

Algorithms [AD07, AN01c, 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, WWG00, 
AHK03b, Ano01j, AH05, CKL+09, CCM01, 
GHP05, GPC08, HW03a, HWR09, HSH06, 
Hro05, JK01a, MCHN05, Pre07, Rhi03, 
TC05, XLMS06, ZLZ07, Zir07, diH08].

Alien [Wil01b]. All-or-Nothing 
[Des00c, SR00]. Ally [DR01, We00].

Allied [Hau03, Hau06]. Allocation 
[CCM05, LZ09]. Allowing [JLL02]. Almost 
[AP09, BS00a, Jut01, Mar02b]. Alpha 
[WB00, Wu02]. Alphal [KHD01]. Alter 
[AN02e]. Alternating [Wer02, HKPR05].

Alternative 
[Bad07, Gar03a, Han00, BMW02b]. always 
[BB79]. am [Eke02, SU07]. Analys 
[BCS05c, CG03]. Amenability [WW00].

America [DB04]. American 
[GL05, Kat05b, Alv00, Naf05]. Americans 
[WDO1b]. among 
[BN00a, KT00, SKU+00, Win05c].

Amongst [Pen01b]. Amplification 
[CHS05, LTW05, RK05, SV08b]. Amplified 
[KK05a, KKS01, KML+02]. Amplifier 
[Pli01]. Amsterdam [Kru02]. Analyses 
[BPR05, Des00a, Pau01]. Analysing [BLO2].

Analysis [ARJ08, ABR01, AKS06, AD07, 
An01c, AII+01, ARC+01, Ava03, BN00a, 
BBdKB09, BRS02, BF05, Bor01, BSL02, 
Cry00, CK02a, CS03b, DPV01, Dra00, 
FL01a, FGM00a, Gir06, Gol01c, GHP05, 
GLG+02, GPR06, HSH01, HK01, HSS04, 
Hey03, HMO2c, IT03, JK01a, JQY01, 
JT01a, JQY01, hKL00, KMS02, LCK03, 
LKL09, LY05, LWK00, LH07, MOP06, 
Mar02b, Mas04, M01, MMT09, Mea01, 
Mes00, Mes01, MAaTxx, MG08, NPO2b, 
NSS02, OS06, ÔOP03, Puc03, QSO1, 
SSST06, Sha01c, Sma03b, SDM06, SQ01, 
SWT07, YSS01, ZC00, ZGLX05, AvdH00, 
AW05, AW08, Abd01, AKH03b, Asl04b, 
BDS08, BBK+03b, Bjo05, BG07a, BR05,
BCJ+06, CKL+09, CW07, CS05a, DS09, DKS08, GW08, GM04, GTZ04, Has01b, Hir09, Hro05, Hut01, JEZ04, JPL04, JSW05, KSF00, Kor09, LKH+08, LMW05]. analysis [LW05a, LKJ01, Lu07, Mea04, MT07, MRST06, OS00, PSG+09, PS08b, SK01b, WLT09a, WP05, XH05, XMST07, YCW+08, YC08, ZWWL01, ZL04c, ZDW06].

Analytic [LW05a, LKJ01, Lu07, Mea04, MT07, MRST06, OS00, PSG+09, PS08b, SK01b, WLT09a, 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, ELv001, Fra04, IEE00a, IEE02, IEE03, IEE04, IEE05a, IEE06, IE08, IEE09b, Ki01a, MZ04, Mno07, Sh00a, USE01a, USE02a, YY01, Yun02a, ACM00, Bel00, HA00, Jef08, NH03, ST01d]. anomaly [RCG+05]. Anonymity [GM03, IKOS06, MP02, SS01b, EY09, LV07, Par04]. anonymization [FXAM04, RW07]. Anonymous [ABC+05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL+08, SOO02, Wan04a, YT09, Z009, B030a, Chi08b, Chi08d, EY09, LHC08, Sac02, Sha03c, WC05, YT05, ZC09]. ANSI [III00, Kel05, Oiw09]. ANSI-C [Oiw09]. Answers [PT08]. Anthony [Pag03]. Anti [Kha05, Ano05c]. Anti-Circumvention [Kha05]. anti-virus [Ano05c]. anticipation [Goo00]. Any [Fis01b, HNO+09, Ano05b, CDM00, DFM04, DMS00, HR07, Poi00]. Anyone [Ros07]. Anytime [DJLT01]. Anywhere [DJLT01]. Apache [Had00]. API [WM01, Mor03]. APIs [BM01c]. Appendix [Kel05]. Applet [ZFK04]. applets [Bis03a]. Applicability [Wya02, TM01]. Application [ADI09, ACS02, Bai01b, Boy01, CL02a, CKB03, Dam07, Dhe03, GKH+06, HF00, IKP+07, JX05, Jou04, Lai03, Lee04b, LLS05b, LSL05+05, N07, Ok00, Pi01, PQ03b, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TWNA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG08, CMKT00, CP07, DMY08, FP00, HCBLET06, JRS09, Lav09, MT07, MPH06, MK05a, N0505, RSS04, SS06, TC00]. Application-Aware [IKP+07]. Applications [AF04b, AC02, AGT01, Amd04, BLST01, BH05, Bar06b, BI05a, BGK+03, BS00a, Bih03, BGOY08, BS02, BL08, CC04a, CD00a, CV02, CGH01, CZ05, CHS02, CS09, Cra05a, CD05, DJ01, DK02, DK07, DA03, DFPS06, FR02, GSS08, GKK+09, GJKT03, Gen04a, GRW06, Go01a, Go04, HRS02, HN06, Has01a, HSS04, HR05, HJ05, JT01b, JY01, KMM+06, KGL04, KMT01, KSM00, KKK01, Knu02, MA07, MM07b, Nie02c, Nie02d, PS02b, RSN+01, Sch06b, Slp03, SX01, SPP06, Van02, Wya02, ZY09, Z00a, Zho02, ÁCTZ05, Ate04, AH05, AFGH06, BG08, BGL+03, CCCC01, CM05b, CS09, CSK+08, DY09a, DFCW00, DJLT01, FP09, Fin03, Fis01a, Gal02, GHC+08, GKK+07, GB09, HSS01, Has02, Hen01, HKPR05, Jac00, KVN+09, KNS05, La04a]. applications [LJ05a, LPW06, LB05, MY01, Mal06, MC04, MS04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SP0H06, WW08, WA06, WV00, YS04, ZBP05]. Applied [HW03a, HW09, SL07, GV09, GP05, IKY05, JY04, ZY03]. Applying [Elb09, KC02, Lan04d, LMS07, SQ01, SPML02, TND+09, vDST06]. Appointed [CL01a]. apprehension [AJ08]. Approach [BKM07, CGFSH09, CDR01, CW09, Chi08a, CB01, DJLT01, Kra03].
Lai07, LL05c, Lut03, OMT02, PBD00, Pau02a, Pre02a, SKG09, VH09, VVS01, Vir03, XYL09, YKMB08, AA08, CGL+08a, CGL+08b, CGL+08c, CJT01, DLM05, GGH+08, Har05a, JJ01, JW01, KVD07, LG09, LYC02, MT09, Mar05b, Mi09, 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].

Aprile [Ano00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH+00b, DFPS06, Joy03b, Kn02, 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, ABM00, BMA00a, BMA00b, BMA00c, CW02, Gro03, KV01, LTM+00, ZYL05, An05c].

Architecture [BH05, GC01b, Gut02b, Gut04a, KKY02, KY02c, KDO01, LKM+05, LZ04, LXM+05, Lut02, MP01c, MFS+09, Rot02a, SMT01, SM03b, SLG+05, Uzn04, Che00, CC05c, DHL06, In05, LHL03b, MPM09, 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].

Are'nt [Bau01a, Bau01b]. Arguments [HNO+09].

ARRITH [BS03, BC01, IEE05b].

ARRITH-15 [BC01].

ARRITH-16 [BS03].

ARRITH-17 [IEE05b].

Arithmetic [BS03, BIP05, BGK+03, BCDH09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDJ+01, SR06, GPS05, PS04a, SOIG07].

Arithmetics [Lam91].

ARM7 [DV08, XBO1].

Arms [An03b].

Army [Boy03].

Arne [Bau02]. array [DZL01].

Arrays [ABM08, BS00a, GC01a, HW05, PP06a].

Arrived [Law05]. arsenal [Blu09].

Art [And07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Eri03, Eri08, MS02d].

Article [Che08b].

Artifacts [EHK+03].

Artificial [Cop04b, MMYH02].

Arun [For04].

ASCI [MJD01].

ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02b, Boy01, Oka00, DN00b, KI01a].

ASIC [WOL01].

ASIP [SKW+07]. asks [An08a].

ASM [MK05a].

Aspect [Kos01a].

Aspects [BLMS00, CMR06, Pe06, AN03, DLP+09, Rup09].

Aspiration [Ash03]. assembly [Gou09].

Assessing [CDD05]. assessment [CC05e, DMS07].

assets [KH03, NRR00].

Assignment [BRTM09, HC08, CHC04, CJ03c, DFM04, HW03c, Hwa00, Lin01a, TP07, WC01b, hY08].

Assignments [SWR05].

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

ASSL [VH09]. associated [XLMS06].

associativity [HRS08].

Assumption [CS00, DN00a, FOPS01, KMZ03, ZD05].

Assumptions [ABR01, BP04, BCP02a, FS01a, KLR09, Lin03, MNT+00, Nao03, SBZ02, 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, FML+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, JJo00, KCP01, KS00a, KML+02, KM01c, LY07, LNL+08, LV04, LMV05, Luc02a, Man01, MH04, MSU05, Nov01, OM09, PV06a, PQ03b, RMS05, SGM09, Sch01b, Sho00b, Sma03b, VHP01, YKL02a, ZC04, ASK05, DKL+00a, Dujo8, Dujo9, GM00a, HAr04, He04b, HG07, Iwa08, JJo2, KS09a, KM04a, LM08, Law09b, LS05b, Mir05, OS00, SIR04, XH05, ZCW04.

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

Attacking-Based [TMMM05]. Attacks [ARR03, AG01, AK03, BC05a, BPR00, BP02, BM000, BBB+02, BDK+09, BU02, BM03b, BCP02b, BM01c, Can06b, CS07b, CZ03, CT08a, CJS01, CKE00, CN00b, CM03, Cpa03, CWR09, CD01b, DFS04, DJ06, DS08, DM07b, FKS00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GKM02, HSH+08a, HNZ02, HR04a, HSH+01, HLC08, IS03, JKS02, JJo04d, KKS00a, KS00b, KKS01, KsJ+01, Kt01a, Law09a, LLS05a, LMS05, LJ05b, MOP06, MP06, MF01, Mck04, Mes00, Mes01, MÖ02, MG08, OT03a, OT03b, OOP03, OST05, Ove06, PKBD01, PDS09, RSO1, SQ01, Sem00, SWT07, Tad02, VV07, WYY05a, WYY05b, WL07a, WY00b, vW00b, vW01, BPS08, Bau05, BC080, Bzo03, CKL+09, CS05a, DK08, Geb04, HSH+08b, HSH+09, Has01b, Hsu05b, HL05b, Ino05, IM06, JDJ01, KS05a]. attacks [KTC03, LPV+09, LMS00, MML05, NS05a, NLD08, OST06, PQ03a, RG05, Sch00c, Sch01f, Shi05, SL06, SK05b, SW00b, WL07a, WL04b, Yan07, YS02, ZSJ07].

Attitudes [FDI00, CF05]. attractors [HHYV07]. Attribute [LY05, RSA00e, IY05]. Attributes [SS01b].

Auction [AS01a, An001a]. auctioning [RGC+05]. Auctions [Bra01b]. Audio [Arn01, CS05c, DRL09, MH05, WNY09, WL+02, XZ01, WQ08, BS01b, KJR05, KN03]. Audio- [KJR05]. Audio-and [BS01b, KN03]. Augmented [CS07c, You01]. Augmenting [AL04].

August [AMW07, Bho00, B+02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KCP02, Kil01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a]. Australia [Boy01, IZ00]. Austria [DKU05, Pf01, Jef08]. Authentic [DGMS03, Dur01, SS01b]. Authenticate [Ban03a, Bau03b]. Authenticated [AGT01, BN00a, BPR00, BU02, BC04b, BM01, BMP00, BCP01, CPP04, Chi08e, DG03, DA03, EP02, GKK007, GL03, GTCC03, HS07, KOY01, KY03, Kra01, Lee01, LHT09, MPS00, Mac01, MSJ02, MN+04, NA07, Nam02, Ng05, Poh01, SK00, Vau05b, WC01a, YPPK09, YI04, ZWC02, BKN04, BC07, CYY05, CYH05, Che04a, CLC08, CJ04, CJL05, DG06, GL06a, GM05, HT08, HWW02, HWW03, Hsu05a, Hwa05, HL05c, HL05d, Jua04, KOY09, KRY05, LKK03a, LKK03b, LL04a, LL05a, LKY05c, LKY05d, LHC08, LLR02, LRR06, LWK05a, Mis08, PQ03a, PQ06, RBB03, Sei05, SW05, SC05b, TLH05, TJ01a, Tse07, WLH06, WH02a, XY04, YW05, YCO9a, YSO2, YSH03, YRY05b, YPKL08, ZC04, ZAX05, ZW05b, ZL05].

Authenticating [API01, Chi08a, CGV09, Fur05, JQ05, PM08, RCBL00, YSS+01, Lin01b].

Authentication [AAK09, AP09, ANRS01, An001b, An001c, An001e, An002d, AHKM02, ANL01, BH06, BACS02, BCL+05b, BCG+02, BM03a, BH00a, BR00, BCC01, BCC02, BC05b, BB0KB09, BR02, BDFP05, BDF01b, BM03c, BL02, BLD09, BWE+00, CV03, CG08, CS07b, CC01b, CLK01a, CLK01b, CC05b, CC09, CJT02, CJO3d, CWY05, CT09, Cim02, CIR01, CFR02, CGK+02,
CF05, CJK+04, Cou01, CMB+05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, FDIR00, Gan01a, Gar03a, GMW05, GSVC02, GD02, GT02, Gut04c, Had00, HSZI01, HSHI02, HSHI06, HKW06, HY01, Hoe01, HS01b, HP00, HL07, ISSZ08, Jab01, JP02a, JP07, JP02b, KJR05, KC09b, KH05, KVD07, Kra01, Ku02, KZ09, KS06b, Law05, Li01, LYT+04, LB04, LL05c, LSH03b, LM00, LOP04, LHL+08, Lys07, MW06, MM01a, Mal02].

**Authentication**

[MJ04, MD04, MR03, MGC02, MNT06, Nao02, Nik02a, Nik02b, OKE02, PK01, Qu01, RKZD02, Ric07, Ril02, SNWX01, SR02, Sch04c, Sch05b, Sei00b, SY01b, SBG02, Sni00, Smi01c, Smi02, SE09, SK06, Str01b, SJ05, SYLC05, SC01, TK03, TSZ09a, TSZT99b, Tsa01, VN04, WLLL09, WC090, Way01, Way02a, Wae06, WKB08, WT02, WS03, WLT04b, WHL05, XYL09, YI01, YEP+06, YSR01, YLL02, YKW01, Zaf00, ZBHvB05, AvdH00, AF04a, AII06, AII09b, Ano01d, Art04, AAKD09, Asl04a, Asl04b, AL04, Ayo06, Bel04, BGP02, BSSM+07, BF04, BFG05, BS01b, BBG+02, BDFP02, BF07, Cer04a, CBB05, CC01a, CCK04a, CL04d, CC04b, CCK04b, CC05c, CZ03, CY05, CCS08, CWJ01, CQ03b, CH07a, Chi08b, Chi08c].

**authentication**

[Chi08d, CL09, CF07, Coc01a, CMDV06, Dal01, DSGP06, DY09a, DGK+04, DG05, DW05, FLZ02, FCZ05, FGM03, Gan08, GLC+04, GTY08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Her09b, Hsu05b, HST09, HY050, HLL05b, sHCP09, JPL04, KLY03, JK05, KN03, KTC03, KLC03, Ku04, KC05, KCC05, LC03, LHY02, LL02, LHL03a, LF03, LKY04, LW04, LHL04a, LKY05a, LLY06, LLS+09, LFHT07, Li05, LST+05, LCX08, LW05a, LH06, LF04, LHL03b, LH03, LT04, LC04a, Lin07, LN04, LL08a, LLW08b, LC05a, LC05b, Luk01, MS09c, MAB06, MCK04, Mit00, MR00, ME08b, MP07, NC09, NLD08, OHB08b, PY08, PCS03, PCC03, PI06, Pei04, Pha06, Pot03, Pot07, RFR07a, RFR07b, RFR07c, RG06, SNW01, SG07, SN07, Sch05c, Sco04, Sei05, SBS09, Sha05c, SLH03, SSM+08, SW06, Shi05, SL05a, St.00, Ste05a, SW02].

**authentication**

[SCS05b, SC05c, SCS05c, SZS05, SY06, TM06, TB02, TOEO00, TIS07, TW07, Tsa08, TWL05, UBP09, VM03, VK08, Voi05, Wac05, WL03, Wan04a, WLT05a, WDNL09, WDC09, WC03b, WL04b, WHH08, YW04b, YW04a, YWC05, YWL05, YTW05, YCY07, YWWD08, YC09c, YC09b, YS04, YRY04, YRY05a, YRY05c, YRY05d, YY05b, YbJf04, ZK05, ZSN05, Zha06, ZD06, ZSJ07, dO07, CS08b, ECM00a, ECM00b, LSH03a].

**authenticator**

[CKY07, jLC07].

**Authorization**

[AB01, Bla02a, CBD+05, GJ03, GOR02b, HG03, RW03b, Sch01a, Mit02].

**AUTHMAC_DH**

[Asl04b].

**Author**

[Ano00b, Ano00d].

**authorisation**

[SN07].

**Authorities**

[CHSS02, HWW04, WH02b].

**Authority**

[Con00, JLL02, CCH05, KB09].

**Authorization**

[BACS02, CJK+04, LSZ05, RKZD02, YT09, GJJ05, JE204, Lin07, LOP04, SR01, WL04a, WZB05, YbJf04].

**Authorship**

[Top02].

**auto**

[YY00].

**auto-recoverable**

[YY00].

**Automata**

[LZ04, MGC02, Wue09, Bao04, CC05d, KK03, La00, LQ08, Mon03, SBZ04, SHH07, TC00, dRMS05].

**automate**

[Bur02].

**Automated**

[CDR01, LLW05, LLW09, HJW05, IY05, LS05b].

**Automatic**

[BD04a, GJJ05, GL00, ST01c, XNK+05, RG05].

**automorphism**

[Pae03].

**automotive**

[LPW06].

**Autonomic**

[DH09, Cha05b].

**autopsie**

[Car00].

**auxiliary**

[Dan00, DK09].

**availability**

[BD+05].

**Available**

[DJLT01].

**AVBPA**

[BS01b, KJR05, KN03].

**Average**
average-case [Mic02b]. Avoid [Tyn05]. Avoided [CNPQ03]. Award [RSA03a, Bar00b, Coc03]. Awarded [Coc02b]. Aware [IKP+07, OHB08a, CBSU06, OHB08b, Zea00]. Awareness [HLM03, BK05]. Away [Coc03, Ols00, Tee06]. Awkward [TvdKB+01]. Axiomatization [dH08]. B [SPK08, YG01a]. B-Spline [SPK08]. B2B [Zho02]. Babbage [Bar00a]. Back [CZB+01, KCD07, SF07, Ano00g]. Back-End [KCD07]. Backdoors [CS03c]. Backup [Str02]. backward [HCD08a, HCD08b]. backward-and-forward [HCD08a, HCD08b]. Bacon [GG05a]. bad [BBN+09]. bail [Ano01g]. Bait [Luc02a]. Balancing [Höf01, Lut02]. Ballot [Cha04]. Baltimore [ACM05b, ACM05c, GL05]. Banach [AUW01]. Bandwidth [CGI+02, YY01, SLP07]. Bandwidth-Optimal [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Bel00, Bon03, Fra04, Kili01a, Men07, Sho05a, Yun02a]. Barcode [Che08b]. Bare [DPV04]. Barken [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, IR02]. Based [Ano01c, ANR01, AF03, AN00, AJO08, BDG+01, BKLS02, BNS02, BN02, Ben00, BRS02, BF01b, BF03, BB04, Bon07, BCHK07, BGG07, BPR+08, BD03, BM01, Boy03, BQR01, BM01c, BSN00, BRT09, CGFSGH09, CVTMH01, CK02a, CGMM02, CF01b, CC02a, CV03, CPP04, CDD07, CS07b, CC01b, CLTM02, CHSS02, CHM+02, CZK05, CM05a, CTH08, CGK+02, Coc01b, Cou01, CFS01, CS00, DN00a, DKMR05, DT03, EHK+03, EM03, FL06, FM02a, FMY01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GPS06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HC08, HH09, Igl02, Jam00, KBD03, KLN+06, KJR05, KKG03, KY02a, KL05, Kel05, KY01c, KY02b, KC09b, KK02, KC02, KCD07, KPR03, KM05, Kra02a, Ku02, KWP06, KT00,LLL02, LP03, LKLK05]. Based [LHT09, LZ01, LZ04, LL05c, LPZ06, LY07, LLRW07, LWK00, LSC03, LHS05, LSZ05, LLS05b, LCD07, MPS00, Mar08a, Mar08b, MNP01, Miiy01, MGC02, Müll01a, MSU05, NMO05, Nond01, Nam02, NBD01, NSS02, Nov01, NMSK01, PV06a, PV06b, PP06a, PZL09, PMR02, Rii02, RE02, RH02, RS00, RS03, RS08, RMCG01, Sal05b, Sch01a, SSFC09, Sha02, Sha01e, SOO02, SXY01, Sma03a, SB01, TMM05, TYLL02, TZZ09a, TZZ09b, VMS05, Vau05b, Ver06a, VH01, VK07, WRR02, WY02, WZM05, W05, WC09, WH09, WBD01, WCD04, YKL09, YKMY01, YL09, YYY00, YSS+01, YKW01, YLH05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZWC02, vDW04, AAPP07, A08, Ano02b, Ano05b, App05, AAK09, BGB09, BCG+09, BR04, BFG08, BS01b, Bla01b, BMW05, BLP06, BBG+03, BDS09b, Buh06, CGH06, CG06, CL02b, CO09a, CL04d]. based [CL00, CCH04, CY05, Che05a, CCS08, CGL+08a, CGL+08b, CGL+08c, CJT01, CL09, CJL06, CIA05, Cho05b, CYH+07, CVFZ06. CCD+04, CTT07, CTH02, CCC04c, Cra05b, DS09, DPT+02, DHL06, DRL09, DV08, DW01, Dug04, EH04, FLZ02, FXAM04, FWL08, GM08, GW08, GSK09, GL06a, GH02c, GS01, GP05, GGS+09, GB09, HM00, HLL+02, HCD08a, HCD08b, HRL09, Has00, Her07, Her09b, HPS01, H05a, Hsu05a, HLWZ09, Hül00, HP01, HLL03, HL05d, shCP09, IM06, JK01a, JK01b, JW06, JPL04, JZCW05, JLL01, KG09, hKLS00, KLY03, KPT04, KN03, KHL09, KW00, KNS05, KLC03, Ku04, KCC05, Kwo03a, KHKL05, LHL03a, LF03, LKY05a, LKY05b, LH05, jLC07, LG09, LD01, LTH05, LPM05, LW05a, LWH05, LYGL07,
11

LLW08a, LLW08b, LCC05, LSA+07, LCZ05c, LCZ05a, LCC06a, LCC06b, MW06, MS09c, Mic01, MR09, MI09, Mit00, MB08].

based [MC04, MPM09, MV03b, NZCG05, NC09, NSNK05, OS09, PCSM07, PW05, PBMB01, PFG+09, PS08a, Pel06, PSP+08, PC00, Pha06, PLJ05a, PLJ05b, QCB05a, Reg03, Reg04, RG09, RCG+05, Sae02, SG07, Sco04, Sei05, SPM02, Sha03c, Sha03d, SC05a, Sha05c, Sha05d, SLH03, SCS05a, mSFTL05, SSM+08, SW05, SH00, SK01b, SCL05, SLC05, Sun02, SCS05c, SY06, TNG04, TWIN08, Tsa08, Tsa05, UHE+09, WLT03, WL07a, WJP07, WNQ08, WLHH05, Whi09, WV00, WH02b, WY05, WC05, XMST07, YW04a, YCW+08, YWW08, YC09b, YS04, hY08, YJ00, YPS01, YRY05c, YPK08, YY00, ZC04, ZC09, ZDW06, ZCL05, ZYW07, dRMS05, NZS05].

Bases [AAC+01, ADDS06, BKP09, B+02, ČvTMH01, EBC+00, FJ03, FLA+03, CCT08, Fau09, ZTW01].

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 [Ca00c].

Bayes [Goo00].

BB84 [Iau02a].

BC [IEE02].

BCH [MLC01].

BDD [KLN+06, Kra02a].

BDD-Based [Kra02a].

Be [Bar00a, Pan02a, CNPQ03, YJ00, vT01].

Beach [IEE00a].

because [AJ08].

Become [Ort00].

Been [Nic01].

BeepBeep [Dri02].

before [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YJ00].

Beginning [Dew08, Hoo05].

Beginnings [Bud00b].

Begins [MP00].

Behavior [Vav03].

BEHEMOTH [Bar00c].

behind [Hen06b].

Beijing [FLY06, LST+05].

Being [ASW+01, ES00a].

beleid [dL00].

Belgium [DR02c, Pre00, Q00].

Belief [BPST02].

believing [Buh06].

Bell [BZ02, Eke02].

Benchmark [Asc02, TLYL04, LDH06, YLT06].

Bendy [Sas07].

Benefit [YKM02a].

benefits [CH00].

Benford [NM09].

Berge [Ytr06].

Berkeley [IEE06].

Berlin [FLA+03].

Bermuda [Bia03].

Bernard [DNRS03].

Berners [Coc02b].

Berners-Lee [Coc02b].

Best [Bau01a, Bau01b, MFS+09, Gol08, Ste02].

BestCrypt [Bau02b].

Bethesda [ACM09].

Better [FV03, PM00, RR02, SKQ01, HLL03, Pau03].

BetterBASIC [ASW+01].

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

Beurling [Bec02].

Beyond [Gor06, Hei03, LMW05, Mar08a, Sch03, Sev04, Sty04].

BGP [ZN05, vOWK07].

Bi [Cou04, PK01].

Bi-directional [PK01].

Bibliography [Bee05].

Bidiagonal [BR09].

Bidiagonal-Singular [BR09].

Big [Gen00a].

billing [SSM+08].

Binarization [LSKC05].

Binary [ADI09, HHM01, LSK05, OSSST04, SKG09, WCJ09, ACTZ05, BG08, BG09, FSG01, GB09].

Binary-Ternary [ADI09].

BIND [Kle07].

Binding [DN02b].

BioAW [MJ04].

Biometric

[AHKM02, Dal01, EM03, HHW01, 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, Rit02, Str01a,
BSSM\textsuperscript{+}07, BCP\textsuperscript{+}03, Buh06].
Biometrics-Based [Ril02]. Biomolecular [Bil09].
Birds [MLM03]. birth
[Bud06, SE01]. Birthday [Wag02].
Bisimulation [BJP02]. Bit
[AIK\textsuperscript{+}01, BK06a, BLO8, CGH01, CGL\textsuperscript{+}00,
DMS00, GS07a, ITO3, KZ07, LNS02,
MS08d, PCCG01, RMH03b, SM03b, SXY01,
VKS09, ATSVY00, Bar06a, BK07, GPX08,
KZ03, KKL09, Lu00, Pri00, RMJ08,
SBR05, UHA\textsuperscript{+}99, WW08, ZFK04].
Bit-Fixing [KZ07, KZ03]. Bit-substitution
[GPX08]. BitLocker [Kor09].
Bits [BS01d, SZ01, HN04, Shp02].
Bitslice [DPV01]. Black
[Ano01i, CF02, CFS05, DI05, DRR05, DS08, KY01d].
Black-Box [Ano01i, BR02, CF02, CFS05, DI05,
DRR05, KY01d]. Blackmailing
[PS01b]. Bletchley [Sal00b, Cop05, Cop06, HS01a,
Sal05a, SE01, Sm01b, Wei06, Win00]. Blind
[A000, BNPS02, BB00a, BSC01b, CL01b,
GSK09, JKK\textsuperscript{+}01, LY07, Na05, Pan02b,
SPK08, ZTP05, ZK02, Fan03, HCO4a,
JLL01, JJ04, LHY05, LCZ05b, MS09a,
SV08a, SHT05, WH05, ZC05]. blindness
[AvdH00]. Blink [Sas07]. Block
[AIK\textsuperscript{+}01, BCC\textsuperscript{+}09, BKR00, BR02, BR02,
BSC01a, CVTMH01, Can01b, PCCG01,
CP02, CM05, CR01, DR00a, Dwe03,
EY00, Fl02a, HSH\textsuperscript{+}01, JKK\textsuperscript{+}01, KCP01,
KYH01, KGG03, LHR07, LRL02, MV00,
MS02e, NPD01, OMSK01, Pat01, P06,
Pi01, RMS05, SM03b, SYY\textsuperscript{+}02, SK1\textsuperscript{+}00,
SK10, WC09, XH03, YG01b, Bai08,
BF06a, DY01, Dun06, Eg00, GPX08,
Hey03, JK01b, June05, K05a, KJ01, LDH06,
LCP04, LKH\textsuperscript{+}08, MMJ05, PS08b, RRB03,
SHJR04, SH07, WF02, XH05, Y00].
Block-Based [LRL07, BBC\textsuperscript{+}09].
Block-Cipher [BR02, RB03].
Block-Cipher-Based [BR02].
Block-DCT [BSC01a]. Blockcipher
[GM02c, O807]. blockciphers [Fur01].
Blocks [Jou02]. Blockwise [JMV02].
Blockwise-Adaptive [JMV02]. Bluetooth
[GBM02, LV04, LM05]. Blunders [Bur01].
Blur [VHP01]. Blur/Deblur [VHP01].
Blurring [LSKC05, SM06]. Board
[GBS01]. boat [DB04]. Body
[Bam02, TG07]. BOEL [Fin02]. Boethius
[Eag05]. bolstered [Ano01h]. bombe
[Wil01a, Tur04]. Bombes [Ano02i, LBA00].
Bombs [Lov01]. Bonds [CA03]. Boneh
[ASK05, Hes04a]. Bonn [DRS05].
Book [And04, Duw03, Eas05, Fell07, For04,
Gas01, Gun04, Imr03, Jan08a, Lee03a,
Lee03b, Mar05a, MP01b, Nie02a, Nie04,
Pag03, Pap05, Rce01, Rot07, Sal03b, See04,
Shp04a, Sin02, Spr03, Sty04, Ter08, Top02,
Uzu04, Wal00, Was08a, Kat05b, Lam07,
Lun09, MA05, Sin09, Sm00, AAG\textsuperscript{+}00].
Books [Dr.00c, Rec01]. Bookshelf
[Lut02, Lut03, Wil01b]. Bookworm
[Sal03b]. Boolean
[Car02, CT03, CS09, MS02b, QPV05,
SM00a, SM00b, SM03a, WV00].
Boomerang [KKS00a, KKS01, KML\textsuperscript{+}02].
Boostr [HSH\textsuperscript{+}08a, HSH\textsuperscript{+}08b, HSH\textsuperscript{+}09].
Border [MJ07]. Borders [PT07].
Boston [USE01b, USE01a]. bot [Ano08b].
Botschaften [Sch09]. bottleneck [WL02].
Bottlenecks [HT07]. Bound [CY08,
DGN03, KMT01, HLL03, y08, GW00].
Boundaries [PT07]. Bounded
[Che04b, DFS08, DJS02, Din01, Din05,
Lu02, MPS05, MTS04, Vao03, DFS05].
Bounded-Quantum-Storage [DFS08].
Bounding [DM07b]. Bounds [BD01b,
BP03b, DRR05, Di01, GGT05, RW03a,
SNWX01, SM00b, Shp03, Wal01, WW05,
GT00, GGT03, JZ09, KS05b, PS02a, Shp99].
Bowmeester [Duw03].
Box [Ano01i, BR02, CF02, CSS05, DI05,
DRR05, DS08, FM02b, KY01d, Kil01b,
SMTM01, JmBdXm05]. Boxes
[Be00, BCDM00, ZC00]. BP
[Wei00, Wei05]. Braid
[AAFG01, CJ03a, GM02a, Hug02, KLC\textsuperscript{+}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, Køv01, Küh08, Sal00a, Wri05, Fie09, Gar01, SE01, Sni01b, SL07, Swe08]. breaks [OS00].

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 [Ahm08].

Brooks [Bar00b].

BRSIM [BPS08]. BRSIM/UC [BPS08]. BRSIM/UC-soundness [BPS08].

Bruce [Hei03, Sty04, See04]. Bruges [Pre00].

Brunley [ASK05]. Brute [Cur05, SGA07].

Brutus [CJM00]. BSD [Lin02, ASW+01, Lin02]. BSDCon [USE02a].

Bubble [Ber03]. Buchmann [Lee03a]. Buffer [FOBH05, Fry00, Ino05].

Bug [BCS08, Bar00]. bugs [GJL06].

Building [Jou02, Kin07, Mar02a, And08, Bra01a, FB01, LS05b, McGo06, MPH06, PQ06, DB04].

buitenlands [dL00].

Bulletin [Cer04b].

Bulletproof [Cha05b].

bundles [GT02]. Burrows [ABM08].

Burying [Arn01]. Bush [Ris06].

business [HHSS01, Pol01]. Buy [PLW07]. Buyer [MM01a].

buys [Zaf00].

Buzzes [Coc02b], Bytecode [Coo02, Ler02], Byzantine [CNV06, HGR07, LRR02, LRR06, P106]. Byzantine-Resistant [CNV06].

C [Ter08, Zol01, III00, Oiw09, RMP08, Sea05, Sea09, VM03, WK01, Wel05]. C# [MJ03]. C-testable [RMP08]. C2C [HTJ08]. CA [ACM03b, Joy03b, KKP02, Men05, Men07, Nac01, Ok04, Poi06, Pre02c, USE02a, USE02b]. CAA [MGC02]. Cache [BTTF02, KL07, OST05, OST06, TSS+03, Ino05, WL07a]. cache-based [WL07a].

Caches [GSC02, LLK05].

Caernarvon [TPK+08].

Causa [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, Wil09, Yun02a, IEE06].

Call [Ano04a, Ano07b, Ano07a, MD04].

Calls [WG05, Ano08c, WC05].

Cambridge [ACM10, Chr00, Chr01, CCMR02, CCMR05, IEE03, JQ04, Kat05b, Kii05, Nao04, Pag03, Puc03, Rot07].

Camellia [AKI+01, HOQ1, KMO2, LHL+02, SM03b, SK101, XH05].

Camera [CGK+02]. Camera-Based [CGK+02].

Can [BB02, CZB+01, Dav01c, Lai08, Ros07, Ver06b, CNPQ03, CG05, SBB05, Zir07].

Canada [ACM02, ACM08, AMW07, H04, H05, HA00, IEE02, MS05a, MZ04, NH03, PT06, ST01d, VY01].

Candidate [III00, EYCP00, NIS00, SKW+00, SL00].

Candidates [AL00b, DPR01, Dra00, GC01a, SBB01, WW00, GC00a, WB00].

Cannes [AJ01a, AJ01b].

cannot [Gav08].

canonical [TP07].

CANS [DWML05].

Canterbury [CZ05].

Cantor [WPP05].

Capabilities [BDT01, AL04, ABD01].

Capability [MH05].

capable [ETMP05].

Capacity [ChLYL09, Sug01, ME08a, Wan05].

Cape [IEE05b].

capture [AMB06].

Card [BCST00, CMG+01, CL07, CMT02, DF01, DFPS06, RE03, RS01, SR01, Ano00k, Ano001, Ano05b, AJ01b, Bur00, BGL+03, Bur00, Cal00c, Car01, CCCY01, Cha05a,
Cla00b, Con00, CH00, DFCW00, GMG00, HM01a, Has02, Hen01, Hus01, Jac00, LSA+07, LC05a, Lu07, QS00, RE00, SP02, Smi00, VK08, Zaf00, Che00, FGL02, Pau02b, SKKS00, TV03. card-based [LSA+07], CARDIS [DFPS06]. CARDIS’98 [QS00].

CARDIS [DFPS06]. CARDIS’98 [QS00].

Cards [And04, AJ01b, Bel01, CK06, DJLT01, HBl01, JSJ01, JY01, Lan00d, MOP06, MV01, MN01, MG08, NQ03, Q01, Sak01, Sha01c, TBDL01, VPG01, YKY01, Ano04a, Ano04b, Ano04c, AJ01a, BPR01, BCIJ05, Bur00, DFH01, DFPST07, FCZ05, Fin03, GUQ01, HHSS01, Hsu05b, Jua04, KLY03, LKY05a, Ler02, LCS09, MY01, Pha06, Poh01, PB01, Pre07, SVDF07, SL03, TIS07, WC03b, YW04b, YWWD08, Ano03a, BJvdB02, CL04d, CCK04b, Che00, Gro03, HL05b, Ku04, KC05, LHY02, Sco04, 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, Ano05a, BBGM08, BU02, BCP01, CNS02, GS07a, Nio02b, OST05, Vau01, BKN04, BF06a, BK05, CSK+08, HRS08, KWD06, Mic02a, Mic02b, OST06, Pei09, STY07, SKW+07, SPH06, ZZWL01].

case/average [Mic02b]. cases [ABHS09]. Cash [PS01b]. Cathedral [USE02a]. Cats [Pem01b]. Caught [Wei00]. cause [SBB05]. Causes [Mur01]. Cautionary [GMP01a].

Cayley [Lam91]. Cayman [Svy02]. CBC [BBKN01, BPR05, BR00b, DGH+04, Fer06, JMVD02, KI03, Vau01, Vau02]. CBIDs [MC04]. CCA [KOMM01, M¨ul01b]. CCA2 [BST02, Lin03, RG09]. CCA2-Secure [Lin03]. CCGrid [TL06]. CCM [Dwo03].

CCS [Mar02b, MS05b]. CDH [CM05a]. CDH-Based [CM05a]. Cell [Fox00, MYC01, SHL07]. Cell-phone-free [Fox00]. Cellular [Laf00, LZ04, MGC02, PZL09, SBZ04, Bao04, ETMP05, KK03, SHH07, Wan04a, dRMS05, Wue09, SSM+08].

Center [AUW01, CH01a, CY04, LPM05]. Centered [BK04, CMB+05]. Central [CHL02]. Centralized [Wac05]. Centre [PPV96]. century [Kob00, Lan00c, PRS04, Gan01b, Lan00a]. CERT [Sea09]. certicom [LM08].

Certificate [BLM01, Gen03, GMR08]. Certificate-Based [Gen03, GMR08]. Certificateless [HLC08, HRL09]. Certificates [BDTW01, CMG+01, RdS01, Bra01a, LCK04, ZSM05]. Certification [Ano11k, CHM+02, RSA00b, BGB09, BD04b, KB09]. Certified [ANR01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HW05, HL04, LL06, LWK05a, NZS05, Sha04b, Sha05b, TLH05, Tsa05, TJC03, WH03].

Cerven [Sal03a]. CFS [It00]. ChaCha [Ber08].

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

Chaining [BKR00, CBB05, PCC03]. challenge [LM08, LW05a, PRS04].

challenge/response [LW05a]. Challenges [Cla00a, GV09, Nao03, Sta03, SVEG09].

Chang [CWJT01, ZC05]. change [CYH05]. Changes [Mur01]. Changing [BST03].

Channel [BU02, CHV03, Law09a, LCK03, M¨ol02, MMO05, OT03a, OT03b, Sch06a, SYLC05, ARR03, BP03a, BG07b, Buh06, CNP03, KSWH00, LCZ05b, MS09c, PSP+08, WL07a, YTW05].

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

Chaos [JKD01b, SK01b, WZW05, JK01a, LMC+03, MCN03, PSG+09]. Chaos-Based [WZW05, SK01b, JK01a, PSG+09]. Chaotic [LLL+01, SXY01, USS02, Vao03, AMRP00, AMRP04, GDGSS00, GB09, HHYW07, HLWZ09, JK01b, LMC+03, LYGL07, MA02, PBMB01, Pso01a, PLZ09, SP02, SL09, UHA+09, VKS09, WG02, WW08, kWPW01, LW04, YZEE09].

Chapman [Kat05b, Was08a]. chapters
Clamping [Ano03a]. Clandestine [Wri05].

Classes [CY02, RSA00c].

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

Classification [HMS04, PBD00, Uni01].

Clauses [SV08a].

Cle [RSA09a].

Cleaner [TR09a, TR09b].

Cleaning [Lut03].

Cleanup [Lov01].

Client [ANRS01, Ano01e, ANL01, FSSF01, PS05, WKB08, Bud07, HTJ08, LF03, YS04].

Client-Server [ANRS01, PS05].

Client-to-client [HTJ08].

Clients [JRFH01, RKZD02, WLH06].

Clinton [Gen00a].

Clip [FGL02].

Cliques [PQ06].

Cliques-type [PQ06].

Clocked [CGFSHG09, MH04].

Close [DM07b].

Closing [Lau08b, PWGP03].

Cloud [CKS09].

Clouds [GS01, VS01].

Cluster [Höf01, KCD07, SEF +06, TLC06, TW07].

Cluster-Based [KCD07].

Clusters [MFS +09].

CM [CMKT00, GHK +06].

CMS [BWBL02, DUK05].

Co [Bud00b, Nd05, ACM01b].

Co-Design [Nd05].

Co-operation [Bud00b].

Coalition [ACJT00].

Coalition-Resistant [ACJT00].

Coarse [Rhi03].

Coast [Boy01].

Cod [EIE05b].

Code [Ark05, BKR00, BR04, CD00b, CV03, Cer04b, FIP02a, FF01b, HSZI01, Imr03, KY01e, Lai08, OS09, Ree01, Rey01, Sal00a, Sm02, SZ03, ZYR01, BGB09, CSV07, Che08b, DW01, HM04, HL03, KS04, Lev01, MMJ05, RSA09a, SM00c, SM05, SM07a, Sin09, Sin00, Swe08, AAG +00, SE01].

Code-based [BR04, OS09, BGB09].

Codebook [CH08, YYWS09, WJP07].

Codebook-linked [YYWS09].

Codebreaker [Hau03, Pin06].

Codebreakers [Bec02, Gau01b, Gas01, HS01a, Kah67a, Kah67b, Kah74, Kah96].

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

Codec [Che08a].

Codecs [LLRW07].

Coded [MLC01].

Codes [Bec05, BP06, Big08, Bod09, BQR01, CC09, Chu02, CDG +05, GMW05, Jan06, KY02b, Mol05, NN06, SNWX01, Sin01b, Smi01b, Urb01, Wri05, ?, YD001, Yek07, Bel07a, aSM01, Bul09, DB04, DKL00b, DW05, DW01, Gar01, HW03a, HWR09, Kov01, Lam07, Lun09, NS01a, PCS03, Pin06, Reg05, Reg09, Sav04, Sun02].

Codeword [AJ08].

Coding [Buc00a, CS05c, HHL +00, Joy00, LLL +01, MZ02, Pat03b, RK06, Sal05c, Smo05, TW02, TW06b, Ytr06, Che07, DW05, Gar04, Hon01, PPV96, Sch00a, Sch01c, S +03, Sch04a, Sch04b, Sch05a, Sea05, Sea09, TW05, Irw03].

Coefficients [CH01b, KT00].

Cohen [Was08a].

Coherent [TPPM07].

Coin [Lin01c].

Coin-Tossing [Lin01c].

Coins [HR04b].

Cold [HSH +08a, AJ08, HSH +08b, HSH +09].

Cold-boot [HSH +08b, HSH +09].

Collaboration [ED03, PCSM07, SBG05, SBG07].

Collaborative [LLY06].

Collapse [SBB05].

Collection [GMM08, Bro05a].

Collections [Kuh00].

Collective [BBB +02].

Collide [GNP05].

Collision [DG02, IK05, MS09c, WYY05a, WYY05d, GM00a, GM05, GM00a, Sem00].

Collision-Resistant [IK05].

Collisions [BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c].

Collusion [BGW05, HNZI02, Zan01].

Cologne [WKP03].

Color [CTL04, Che07, Che08a, CTY09, FGD01, AEEEd05, CO09a, CDDL07, Yau02, YCL07].

Colorado [BC01, Sch04b, USE00d].

Colored [CDD07].

Colossus [COP04a, Cop05, Cop06, Lav06, Sal00b, Sal00a, Sal05a, Salxx].

Colour [RS00].

Coloured [AADK05].

Columbia [ACM08].

Column [Raj06].

Combination [CF01b, Gau02, GHPT05, GB09].
Combinatorial
[GMW05, SLTB+06, Hen06a].
Combinatorics
[Lee03b]. Combined
[LLS05a]. Combiner
[Sar02, LL06].
Combiners
[AK03]. Combining
[Abe04]. Comes
[Mar08b, Ano03e]. Coming
[Dan01]. Commemoration
[BZ02]. Comment
[SCS05b, WY05, WLW04]. Comments
[AS01c, CGH+00b, JW01, MNFG02, SKW+00, 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
[Unio0a, Uni00b]. committing
[DN00a, Nie02b]. commodity
[CGL+08a, CGL+08b, CGL+08c]. Common
[Pas03, TG07]. Commonwealth
[PY05].
communicating
[Hut01]. Communication
[AK02a, ANRS01, BYJK08, BBK03a, BIW08, Big08, Col03, Fis05, GKK+09, LLS+09, Mar07, NA07, PL01, Sch06b, SKR02, Wri05, vDW04, BYJK04, BC05c, CC05c, CGP03, EY09, GKK+07, GG05b, GC05, HYS03, JZ09, JRS09, KPS02, LPM05, Lin02, MP08, PBMB01, Par04, RH03, SNW01, UP05, WWA01]. Communication-Efficient
[Fis05, LLS+09]. Communications
[BCC02, GN06, HJ07, Ig02, Kra01, Lan00a, Lan04b, LCK01, LL02, LL01, MS05b, Sal01b, Vau05b, VMC02, BP03a, CYH04, HWW02, LC04a, Sal05c, Ser06, SL05a, Wili99, WGL00, YTW05, DKU05].
Community
[SK06]. commutativity
[HRS08]. committing
[CKRT08]. Compact
[CG03, JT01b, SMTM01, YT09, ZLK02, JAW+00, Mic02a]. companies
[Ste00].
Company
[ASW+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
[YC09c]. Complementary
[AS01c]. Complete
[Bar00a, Bee05, Bud00a, FGM001, GCK08, HMS04, KY00, MS09d, Sal07, TWM+09, Bud02]. Completeness
[HG03, MW04, ABHS09, PT08]. Complex
[JKK+01, LKLK05]. Complexity
[BYJK08, BL01, BKD+09, CR01, CB01, DN00a, FBW01, GKK07, GKK+09, HR04a, Lut02, Nie02b, RMH03b, Ros00, Rot05, Shp03, BYJK04, CDD00, GKK+07, GIKR01, Gor05, JZ09, Mic02a, MP08, RMH03a, Rot02b, Rot03, Shp99, SPHH06, TW06a, SU08a, Fal07, Rot07]. Complexity-Theoretic
[CBO1]. compliance
[LMW05]. Compliant
[CGBS01, RVS09]. Component
[BSL02, Hei01, TEM+01]. composability
[PS04c]. Composable
[AF04b, BOHL+05, BLDT09, CF01a, CK02b, DN02b, DN03, NOM05, RK05, Can01a, CLOS02]. Composite
[CQS01, GMP01a, RDJ+01, Zhe01]. Composition
[BJ02, BNO0a, CR03, CV02, Pie05, Sh00a, Can06a, LRR02, LRR06, Puc06]. compositional
[GM04]. Compostela
[BS03]. Compound
[SB05]. comprehensive
[dLB07]. Compress
[Gen04b]. Compressed
[ISSZ08, SB04]. Compressed-Domain
[ISSZ08]. Compressibility
[HN06]. Compression
[ABM08, BD03, CC06, HS01, Ke02, LHS05, RS08, Sal07, SDFH00, WVL+02, WC03a, FS08, Gar04, Lai00, Lj05a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TZH01, Zir07]. Compression-Encryption-Hiding
[BD03]. Compromise
[Ahm08, Lai08].
Compromised [ZYN08]. Comput [McK04]. computability [Pet08].
Computable [Vad03]. Computation [ACS02, Bai01b, BCL+05b, BI05a, BIM00, BJLS02, CC00, CDM00, CDN01, CDG+05, CDI05, DI05, DM00b, FS02, FGMO01, FWW04, GIKR02, HCK09, Has01a, HM01b, Je08, Ko04, KCL05, KS02, Lin01c, PS05, WW05, An02g, AB09, BEZ00, BEZ01, CLOS02, CLO08, CDD00, DwWiW05, Fan03, GCKL08, HT04, HLL03, IKOS07, LMSV07, LC04a, May09, Mis06, SH05, WHH05, WY05, SM07b, Duw03].
Computer [BS03, Bro05a, BCDH09, BC01, CSM+08, CZK05, CGK+02, Coo2a, Coo3, HY05b, IE00a, IE01a, IE02, IE03, IE04, IE05a, IE05b, IE06, IE07, IE08, IE09b, Fr00, JBR05, KM07, Luh06, Lu02, MLYC01, MS05b, MAC+03, Nie02d, RC06, SB07, Tyn05, Cas02, DFGH04, Fan09, FOP06, GKS05, Lo01, M06, PRS04, PHS03, Sal05c, Sal05d, Sh06, SL06, SE01, dCdvS05, GKS05, dCdvS05].

Computer-Science [Coc03].
computerized [LMC+03, Pau02b].
Computers [Coc03, Ett02, TSS+03, Cop05, Cop06, RH00]. Computing [AC00, ACM01a, ACM01b, ACM02, ACM03b, ACM04b, ACM05a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBK00, CGH00a, CL01a, Cop04b, EP02, JP03, LBA00, LKH09, Lu03, May04, PHM03, Sch06b, SK09, SCF01, Sim02, SEF+06, Sta03, TLC06, VH09, Ver02, WC01a, Wri00, Yan00, YKMB08, Cha07, Che05b, CHT02, DHL06, HV09, HKP05, LMC+03, M09, PP03, PP07, Raj06, RP00, Sei05, WHH06, Wji99, YLR05, Lu03]. Compoware [An02d]. conceal [BB79]. Concealing [DMS00].
Concealment [DA03]. Concept [ARC+01]. concepts [AB09, Kra07, SWR05, MC04].
concerning [HW03b]. Concerns [MP00].
concrete [KNS05]. Concurrency [JL00].
Current [BP02, DPV04, Gen04a, KK03, Ros00, Ros06a, Dam00].
Conditional [LMV05, WN02]. Conditions [IKO05]. Conference [ACM03a, ACM04a, An06b, AAC+01, AJ01b, Bel00, B+02, BZ02, BS01b, Bli03, Bla03, Bon03, Boy01, Buc00a, C04a, CV04, CGP03, CGH06b, Cra05a, DKU05, DFCW00, DFPS06, EBC+00, ELvS01, FLY06, Fr01, FAM02, Fru04, FLA+03, H06, HY05b, IE09a, IY05, JY04, JM03, Joy03b, Jue04, K05, K06, K01a, Ki02, Kn03, Knu02, Lai03, LL03, L04b, LLT+04, LL04c, MM06, MS05b, MS02e, Men05, Men07, NIS00, Nao01, Nao04, Oka00, Oka04, Pat03b, Pem01b, Pfi01, P06, Pre00, Pre02c, RD01, Roy00a, Roy05, Sho05a, Sil01, SM07b, Sm05a, S02, USE00c, USE00a, USE01b, USE01a, USE02c, Wji99, Won01, Wri03, Yun02a, YDKM06, ZJ04, Zhe02b, ZY03, AU01, B05c, DV05, DWM05, DRS05, Ho01, Ki05, Li05, PC05a, PP05, PPV96, Q00, Son00, WK06]. Confidences [Gan01a]. Confidentiality [Gan01b, YC08].
Configurable [MBS04]. Configuration [Sha02, Mos06].
Confirmation [SK00]. Confirming [CM00, GM03]. Confiscation [Sha02].
Conformance [LBR00, RSA00].
confounded [Bel07a]. confusion [She01].
congestion [SB05]. Congress [Un00a, Un00b, Un00f, Un00e, Un00h].
congruences [Ste08]. Congruential [CS05b, LS05a, SB05]. conic
Conjecture [CU01]. Conjugacy [CJ03a]. Conjugate [Igl02]. Connected [BJLS02, Höf01]. Connection [HR00, Jam00, Goo00, Mic02b]. Connection-Polynomials [Jam00].

conscious [DMSW09]. Consensus [CNV06]. Considerations [DBS +06, Hei07, Rub01, Sch07, SVEG09]. Considering [WA07]. Consistency [ABC +05, JEZ04]. consistent [RG06].

Constant [App07, BI05a, CS07c, CD01a, DPV04, DN02b, DI05, Lin01c, Sun00a, IKOS08]. Constant-Depth [BI05a]. Constant-Round [DPV04, DI05, Lin01c].

Constrained [BCH +00, DBS +06, HS01b, MRL +02, Zhe02a, Has00, RAL07]. constraints [CC05d, LPM05, SN04]. Construct [CDMP05, Gol01d]. constructed [Tsa05]. Constructible [NNT05]. Constructing [Des00b, Fis01b, Vad03, Wen03, JZCW05, NS01a, ZL05].

Construction [BBK01, BBo00b, Car02, CMKT00, Lin03, Nie02c, 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 [GGH +08]. consumption [Miš08]. Contact [YKMY01, Car00]. Contact-Less [YKMY01]. Contactless [And04, KS02, Cha00b, Fin03].

Contemporary [Ahm07, Opp05, SVEG09]. Content [AAK09, CGJ +02, HHJS04, MA00a, MA00b, RE02, XMST07, YKW01, ATS04, DY00a, 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].
Cryptanalysis [YKL03, Kat05b]. Cryptanalyst [Wil06].
Cryptanalytic [BS00b,KFSS00,Oec03, QSR +02,Yau07,Wil01a]. Cryptic [Wri05].
Cryptographic [AC02, AADK05, AL00a,Ano09b,ADH+07, Ase02, BLST01, BDF+01a,Bar00a, BGK+03, Bilh3,Bla01a,Bor01,BDP02, Bra01b,BMo1c,BLo8,Bur06,CC04a, Can01b,Car02,CCPD01,CHL02,CKY07, CB01,Cra05a,CS09,CO09b,DD02, DHMR07,DFM04,DS00,DVN01, DHR00,DV08,DFG01,FIP01b,FSo0,Fis01a, FGM00a,Fri01,GMP01a, Gar05,GSS08, GGKT05,Go01d,GK02,GTH02,Gor02a, GL00, GUQ01,Gut00,Gut02b,Gut04a, HTS02,HNe6,Har06,Has01a,HLo5a,HCo8, Ig02,iYo0,Ito01,IM01,JT05, KM001, KY01b,KY02b,Kl01b,KSo0a,KSo0b, Knu02,Kiis02,Law09a,LD00,LS05a, LKJL01,MS02a,MP06,Me01, MN01, MRL+02,MHH02,Mor03, MK05b, MSU05, NIS01a,NIS01b,Nao03,Nd05,Ngr05,Nie04, OTT01,OP01a,PKBD01,PR08,PZDH09, Pem01b,Pi01]. Cryptographic [Pin02, Pin03,PS02b,Pot06,Pre00,Pre02a, Pre02b,RA00d,SA01,RR00,RRS06, Rot01,RSN+01,SM00a,SR00a,SGM09, Sha02,Shp02,SYDF06,SVW00, SR06,SL09,TLYL04,TWN08,TBDL01, Uzu04,WKP03,WN02,WBL01,WC01b, You01,Zha08,AMRP04,ÁCT05,ALV02, AV04,BGB09,BDSV08,Bla01b,BP05, BG08,BG09,BDNN02,BD04a,BGL+03, BMV06, BR05, Can01a, Can06a, CHC04, Coh03,CC05d,CL06,DP04,Dug04, DFG00,FS03a,FSGV01,GT00,GPV08, GJ04,GM04,GB09,HV03c,HY03,IK03, IK06,IVK02,IVK03,JW01,KAM08,KSF00, KS05b,KP03,LMTV05,Lau05,LLW05, LLW09,ML05,Mea04,MT07,Mic02b, MRST06,Mon03,NN03,NdM04,NdM06, PS04a,PSG+09,PR05,Pre07,Pri00,Puc06, PV05,Reg03,Reg04,Re09,RM04].
Cryptographic [RBF08,RAL07,RS04, ST03a,SV08a,SO107,SW00b,TNG04, kWpLw01,WLW04, XLMS06,YLT06, ZLX99,ZW+W01,ZL04b,dH08,BWBL02, JQ04,KK02,KP01,KNP01,RS05].
Cryptographically-masked [AHS08].
Cryptographic [CK06]. cryptographic [RSA09a]. Cryptography
[ANS05,AF04b,AD09,AA04b,An00e, An01i,An02b,An02f,An02h,An04a, An05a,An07a,AAFG01,AK04, AIK06,App07,AA007,AB05,Bai01a, Bai01b,BIN03,BD04,BOV03,BOV07, BBGM08,BM01a,BR00a,BY03,Ber00, Ber03,Big08,BWBL02,Bla02b,BDDS03, Bon00,Bon07,BP01,BY03,BLMS00, BK06b,BKM07,Buc06b,BD08,BP01b, BRTM09,CP07,Cer04b,CCL09,CSW+08, CSQ01,CPD06,Cob04,CFA+06,Cop00, Cor06,Dr.00c,Dam07,DFSS08,DFSS05, DD00,DFGH04,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, Gri01, Gro05, HR06, HH04, HHM01].

Cryptography

[HMV04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irw03, IKOS08, JLY04, JL00, JT01b, JT01a, Jae04, Kak06, KLR09, KZ07, KGS07, Kat05b, KK06, KBB09, KPMF02, KWDB06, KY01c, Kir01a, KMS02, KM05, KS03, KWP06, Lam01, LG01, LSY01, Lee03b, LLL+01, Lie05, LDM04, LW05b, LP02b, Lut03, Lys08, MNT+00, MP02, Mao01, Mao04, MZ04, Mao1, MAA07, MB01, MR09, MS03b, Mol01, Mol03b, Mur01, Nao04, Nie02a, Nie02d, NH02, PV06a, PY06, Pel06, PM02, PBB02, Poi02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGK08, Sth05, St01, St02, St06c, SJ05, Syv02, TSO00, TW06a, TG04, TMM01, TW02, TW06b, Tro08, TR09a, TR09b, Uni01, USS02].

Cryptography

[VY01, VM02, WPS01, Wei04, WK01, Wei05, Wie00, WvD02, Wri00, YWC08, Yru06, YC01, YDKM06, ZY03, vDW04, Irn03, AMW07, AN03, AUW01, Ano02a, Ano02g, ABD01, Ber09b, BBD09, Bis03a, BSS04, BS05, Bla03, BDN00, BCD06, BE00, BE01, BM04, BEM+07, Buc00a, Buc01, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CCT08, CJ03c, CDF05, CDD07, Cos00, Cre00, DD04, Di01, DIM08, DwWM05, DOPS04, DKL09, DW09, Duw03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GKK+07, Geb04, GRTZ02, Gol09, GG05b, GHP05, GPS05, GP05, HH05, HHL+00, He03, HKPR05, HA00, Hig08, HS00, Hoo05, HG05b, HWZ09, IZ00, IM06, JK01b, Jan08b, Joy00, KZ03, KL08, Kat01, Kii05, Kim01, Kob00, Kra07, Lan00c, Lee04a, Lin01a, Lop06, Mans, May01].

cryptography

[McAO9, MBS04, MM07a, Mol07, NP02a, Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00, Pin06, Pip03, Reg05, Reg09, Rot02b, Rot03, Roy00b, Roy09, ST07, Sch02, Sch04d, SB04, Ser06, SH05, Slp09, Sio05, Sin99, Sin00, Sm04, ST01d, SK01b, TW05, UHA+09, Van03, Van05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Wh09, Wri03, YC09a, YC07, yT05, For04, HC02, Kat05b, Pat03b, Sio01, Sma05, Bee05, Lee03a, Rec01, Wal00, Was08a, MP01b, Sbp04a, Kat05b, Spr03, Ter08].

cryptography-based [FXAM04].

Cryptologic [BS00a].

Cryptological [Lew00].

Cryptography [dL00].

Cryptologists [WD01b].

Cryptography

[Bar02, Bon03, CM07, CC04a, Fal07, FLY06, Fra04, JMO3, Kn02, Ll03, Lut02, MMV06, Ne04, N01c, Ng01, Oka04, Poi06, Rot05, RS02, Sha03b, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bi03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kii01a, Kim02, Lam01, LL03, Lee04b, MS02c, Men05, Men07, Naco01, Oka00, PC05a, Pfi01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sh05a, Son00, Won01, WK06, Yun02a, vT00, DWM05].

CryptoManiac [WWA01].

Cryptography

[CKK+02, MG01].

Cryptosystem

[BST02, FL06, GG01, G05, GH01, Hug02, KM01a, KY02c, KCL+00, LHT09, dVP06, Lc02b, NSNK05, NB01, Ori06, PHK+01, YG01a, YG01c, Zhe02a, Zho06, Bao04, CL02b, CCH04, Che05a, Cho06, CFZ06, CHH01, Dan02, DHL06, EKMA01, GHdGS00, GS01, GC00b, GMW01, Hen06a, Iwa08, JW06, KY09, Ll04b, Ll06, LKYL00, L000, LS01c, OP01b, Pa03, Po00, SPG02, SC05a, SP79, LCO5, Sun00b, Sun02, SPZ02, TJ01b, TJ01a, VSO1, War00, YC09b, yH08].

Cryptosystems
[Aki09, Ava03, BDG+01, BKLS02, BPS00, BM00, CHSS02, CCW02, DDG+06, DKXY02, ESG+05, FJo03, Fe06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KI01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, VAD03, WXY02, XB01, ZLK02, Ban05, BFO6a, BB79, CHC01, CMKT00, EBS01, EHKK04, GH08, GBKP01, HM00, Has00, Has01b, Hüb00, HP01, KW00, Kos01c, LD01, Mc01, Mis06, OS00, Pei09, PLJ05b, SSST06, Sha05c, Sma01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WV00, YY00, ZS09, vT01].

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].

CUB [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, ADJ09, Ano05a, Ava03, BINP03, Bar00a, BBGM08, BMM00, BWBL02, BS01d, BMN01, CQS01, CFA+06, GPP08, HYZ05a, HM01, HM02c, JTS01b, JT01a, KB09, KPMF02, KSW02, KWP06, LW02, MÖ02, Kir03, OTT01, OS01, PWGP03, Pei06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YSY09, ZLK02, BSS04, BSS05, BGM04, BGO7a, CCH04, Che05a, CFVZ06, DM08, DwWM05, EHK04, GBKP01, Has01b, Hsu05a, HIL05d, JD04b, LW09, Mis06, OS00, ST03a, SSST06, SH05, Sma01, SCL05, SLC05, TCO5, VAD03, Ver01, Wol04, WPP05, YC09a, YC09b, ZSZ01, ZLK05, vT01].

Curve-Based [KWP06, Pei06].

Curves [AHRH08, Bai01a, BB00b, CY02, Gal01, GLV01, Gau02, GHK+06, Kid02, PWGP03, Ver02, CMKT00, Hus04, LWZH05, MP01b, MSV04, Sim05, Sim02, SC02b, Was08b, Wen03, YS08].

customer [Liu01b].

CVS [DFG01].

Cyber [FNRC05, WW04, MA05].

Cyberinsurance [BP07].

Cybersecurity [PLW07].

cyberspace [Mit02].

cycles [ABHS09, BPS08].

Cyclic [PF05, Mic02a].

Czech [MJ04].

D [Duw03, Ben00, ChL01, CT09, DNP07, Lav09, OMT02, W09, ZTP05].

D.R [Irw03].

daemons [Mos06].

Daugerd [CDMP05].

dark [Blu09].

darkening [CDD07].

DARPA [Coc01a].

Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BS00b, BNPW03, Bro05b, Che01a, CTLL01, DSB01, EBC+00, Elb09, FMA02, FLA+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, Kus02, Lan00b, LLRW07, LP00, LHS05, LS08, Lut03, MND+04, MS03b, MSF+09, NM09, OS05, Per05, RKZ02, RO6, Sal03a, Sal07, Sin01a, SK03, SDMN06, TZZ05, TCPP07, VDKP05, WS05, WY02, WN02, fc01, vW01, AMB06, AG09, AK03b, AKS04, Ano02e, Arn01, Bla00, BN08, CSTM09, Cer04a, CO09a, CLR09, CPG+04, DZL01, DGM03, FS04, HIL02, LLK05, MJ03, Mal06, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SGPH08, SETB08, WM0R08, YLC+09, YC08, ZJSN07, Zir07, Cur05, DK08, Lin02, Pap05].

Data-Hiding [VDK05].

data/image [Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a].

Database [ACM03c, ACM05b, Bl05a, BBPV00, KS02, SVEG09, Gal02, HIL02, MA04, PS08b, PBV01].

database-service-provider [Hilm02].

Databases [AK02b, CDM+05, DN04, AHK03a, CDD+05, CKY07, GA03, MSG09, MNT06, NS05b, ÚG08, YPP09].

Datamining [DN04].

Datenverschlüsselung [Lin02].

David [Gas01, Pap05, Bar05, Eag05].

Day
Ken02b, KB09, KDO01, Lan04a, LCP04, LL04b, LB05, MKP09, MP00, Nd05, NSS02, Rhi03, Sjt09, SPG02, SRQL03, Uzu04, WZW05, WW08, WLLL09, ARJ08, CMS08, GG05b, Gut04c, HC04a, Hut01, KSF00, MI09, MWM01, SVEG09, YC08.

Design/CPN [AADK05].

Designated [LV07]. Designing [HBC08, TCR03, CG05, Lan00c].

Designs [Bee05, CC02a, Bai08, Des00a, WL07a].

Desktop [Mun08, BDET00].

Desmedt [CHH09].

Desynchronization [CDTT05].

Detached [Sha01c]. Detailed [Lut03].

Details [Scr01]. Detect [FOBH05].

Detecting [CMS09, FG010, JQYY01, Har07a, LHL04a]. Detection [AS01b, AD07, BB00a, BKM07, CH01b, CZK05, JT05, KKG03, SKQ01, SY01a, SLT01, ST01c, TZZ05, TMM05, WGM05, YI01, Zan01, Bej06, BBK03b, HLL02, Men03, NNO2, WMS08, YW06, ZGT05].

Detection/Correction [SKQ01]. Detector [BSC01b, DNP07]. Determined [KKH03].

Determining [KS03, LQ08, OS07].

Deterministic [BK06a, Her06, KZ03, KZ07, May04, BK07].

dev [BH05]. Developers [An006c, Dew08, MK05b, Nis03a].

Developing [MV03b, Cra05b, Gal02, HL06].

Development [An002e, CNB02, Dam07, HF00, WA07, HL06, Lov01, Sha01a, Mar05a].

Developments [An003c, Pre07, Sha04a].

develops [Pau02b]. Deviates [Ran55, Ran01]. Device [Ric07, ST03b, WPS01].

Devices [BCH00, CFR02, Dam07, EP02, GST04, Hei07, JP02a, JW05, Kha05, KHD01, MV01, MRL02, SCPF01, WC01a, An006a, CMS08, CF07, DMT07, sHCP09, Tse07, YC09b, ZYW07].

Devil [Bha01c]. DFT [Che08a].

DH [Lys02]. DHIES [ABR01]. DHP [MSV04].

Diablerets [Vau05a]. Diagnosis [An04a, BK06b, XNK05]. Diagnostics [NM09]. Diagonal [PJH01, PJK01].

Dickson [SZP02]. Dictionaries [AGT01].

Dictionary [BRP00, BCP02b, CS07b, DJ06, Pho01, NS05a]. did [MH09].

Diego [ACM03a, ACM03b, ACM03c, ACM07, Sch00a, Sch01c, Sch04a, Sch05a, USE00b].

Dies [Bar00a, Cco01a].

difference [PBMB01, dW02].

Differencing [LS08, WWTH08].

Different [CGMM02, Sna01].

Differential [Ava03, BMM00, BF00a, BFMR02, BDK02a, Cry00, CV02, CKK02, CKL03, Ek09, Fur02a, Gra02a, HLL02, HHK04, IIT03, JT01a, Kan01, KM02, KCP01, LHL02, MP06, MMT09, MHL02, MG08, PSC02, PQ03b, SK01a, SKU00, SK01, YSD02, vW01, BF01a, CUS08, Che08a, DL009, Egl00, EBS01, Pha04, SLL00, TM01].

Differential-Linear [BDK02a].

Differentials [BF00b].

Difficult [Bud00b, MT02]. Difficult-to-pass [MT02].

Diffie [Jan08a, ABR01, ASW01, BS01d, BMP00, BCP01, BCP02a, BCP07, CY08, C01, C03a, CKRT08, F01b, GR04, KI01b, KK02, KM04a, Kra03, Kra05, Mi08, Tsa06, YRY05c].

diffuser [Fer06].

diffusing [She01].

digest [MS09].

Digit [KWP06, Tan07a, BG09, HKPR05, Kir01b].

Digital [ANS05, AvdH00, AR00, AS08, An01f, An02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00b, CCH05, CC09, Che01b, CNS01, CMB02, CMB03, CGJ02, DSP01, EIG01, Eng00, EHK03, HSZ00, HSZI01, Han00, HS01b, HHGP03, HW01, HLT01, JBR05, KZ01, Kal01, KC02, Kuh00, Kwo02, Kwo03b, LZL01, LLL01, Lin01b, LWL09, LL01, Lu03, Mad00, MM01a, MM02, Mhe01, PL01, PJH01, PSC01, PZL09, PBM03, Ram01, Rd01, RS01, Sam09, Sch00d, Sch06b, Scr01, Sha01e, SC02a, Shi08, SLT01, Sug01, TMM01, TJC03, USS02, VHP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03a,
WC04, Wya02, XZF01, XYL09, YWWS09, YYDO01, YYZ01, ZWC02, Zho02, ZCW04, AAPP07, AA08, Ano00i, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CJ05, Che07, Die90, FB01, GGK03, Gil07, HRL09.
digital [HLC07, HLH00, HHC05, KP00, LG04, LG09, Lev01, LLC06b, MKY08, NRR00, PC05b, PLJ05a, PBV08, QCB05b, Sha01d, Sha04b, Sha05d, SCL05, TND+09, UP05, WNQ08, WHLH03, WC05, XC05, XMIST07, 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, SAG07].
Discrete [CS03a, Cne04b, CCW02, Gen00b, GV05, GFP08, KC09b, LW02, LJL05, VK07, HN04, HW03a, HWR09, Hsu05a, HL05d, JL03, JLL01, LHL03a, LHY05, LTH05, PLJ05a, QCBO5a, Sch01e, Sha05c, Sha05d, SWR05, SCL05, SLC05, SCS05c, Yas08].
discretized [MA02].
discryption [Har07b].
discursive [Mit02].
Discussion [An001a, An001b, An001c, An001i, An001j, Ano01e, Ano01i, KL+02a, Mal02, Nik02b].
Dishonest [GKK007].
disjoint [Gut04c].
Disk [Cro01, Har07b, Siv06, CS08a, Fer06].
dismantles [Hi06].
dispatches [Kee05].
displayed [CGV09].
Displays [Kuh02a].
Disputed [CAC06].
Distance [CFHSG09, CPhX04, DM07b, DW01].
distinguished [HWW04, WH02b].
Distinguishing [HRS+01].
Distortion [BG08, CS05c].
Distortion-Free [BG08].
Distortions [HH09, SDF01].
Distributed [BSCS02, BT02, CLK01a, CS08b, CD01a, DL03, EP05, FM02a, FS01a, GJKR03, GSV02, GTH02, LLY06, SCF01, WT02, And08, AFGH06, BDET00, CO09b, FMY02, KKL09, LN04, LLW08a, MSP+08, PS08a, Raj06, WZB05, Ybf04]. Distribution [BDF+01a, BOHL+05, BBB+02, BSNO00, FSO1a, Ina02a, Ina02b, Kuo2, LL02, NA07, Sch01a, Yf01, ATS04, Asl04b, Bad07, CYH04, GL06b, MP08, SL07, Sph01, Sph04b, SY06, WHHT08, YS04, ZLG01].
Distributions [CY08].
Diversity [Kun01].
Divide [SKQ01].
Division [HZS05, KKY02, Tan07a, Che08b, MN14].
Divisor [KM01a].
DL [HRL09, PLJ05b, Sch01f, Sch01e, WM0808].
DL-based [HRL09, PLJ05b].
DL-encryption [Sch01f].
DL-keys [Sch01e].
DL-STD-M [WMR08].
DLP [MSV04].
DM [Eag05].
DNA [GPX08].
DNF [BG05].
DNS [Her09b, Kie07].
DNS-based [Her09b].
Do [Bur06, HSR+01, HR04b, Win01, BB79].
Dobb's [Dr00c].
Document [ISO05, PJH01, ST01c, VHP01, CD07, CL04c].
Documents [PKJ01, AW05, AW08, DGK+04, GA03, UG08].
Does [AB01, Pie05, Con09].
Doing [BM01a].
Dolev [BP08, BN02, ZD05].
Domain [AS08, Bar00c, BSC01a, BSC01b, BS02, CJK+04, Cor00b, Cor02, DOP05, DNP07, GW01, ISSZ08, Kuh02a, Lan00d, L01, MM01a, OMT02, PBC05, SOHS01, SDFH00, ZL02, BR06, CS05a, DSP01, EKRMA01, Zir07].
Domains [BR01, CLK01a, CLK01b, Van01].
Dominic [Rot07].
Dominica [PY05].
domino [LLLZ06a, LLLZ06b].
don’t [Win05c]. Don’ts [FSS01].
DONUT [CLL00]. Door [SF07]. Doors [Eri02]. DOS-Resistant [Ano01e, ANL01].
Double [ADD06, CY08, CMJP03, Coc02a, DIM08, GH08, GB09, Hau06, JSW05].
double-base [DIM08]. Double-Gate [Coc02a]. Double-Size [CMJP03].
double-trapdoor [JSSW05].
Door [SF07]. Doors [Eri02]. DOS-Resistant [Ano01e, ANL01].
Double [ADD06, CY08, CMJP03, Coc02a, DIM08, GH08, GB09, Hau06, JSW05].
double-base [DIM08]. Double-Gate [Coc02a]. Double-Size [CMJP03].
double-trapdoor [JSSW05].
Doubling [FV03].
Douglas [Spr03].
Down [BBPV00, Coc02b, Ano00g, Ano03c, Ano03a, Pot03, PBVB01, Ste05c].
Downwards [SJ-03].
DPA [SGB01, TV03]. DPA-Based [SGB01].
Dr [Ano03e]. Dr. [Dr.00c].
drastic [Sug03].
drawn [vOT08].
DRBG [Hir09].
Dress [Ahm08].
drinks [Ano03c]. Drive [NP07, Kor09].
DSA [MR01a, SA02, Sha01d, TvdKB+01].
DSA-type [Sha01d]. DSEA [LLLZ06a, LLLZ06b]. DSP [Geb04, WWGP00]. DSP-embedded [Geb04].
DSPs [WWGP00]. DSS [Ano03a, Ano03c, Ano03a, Pot03, PBVB01, Ste05c].
DTP [PCK02]. Dual [HLC07, KHY04, LKLK05, SF07, WCJ09, ST03a].
dual-field [ST03a].
Dual-Pair [WCJ09]. Dual-Tree [LKLK05].
Dual-wrapped [HLC07]. Dumb [Eri01].
Dummies [Cob04]. Dump [KCH+01].
Dunaynir [MAaT05]. d’une [Car00].
Durahim [MAaTxx]. Durahim’s [MAaT04]. during [AJ08, Bec02, WA07].
Dust [KS07]. Dutch [dL00]. Duty [ZGLX05].
Dwork [DNRS03, GK05, Zha06].
DWT [LSH05, PBC05]. DWT-Based [LSH05].
Dynamic [AF05, BN08, BCP01, BCP02a, BFM07, CL02a, CW09, CCD+04, CT707, GTH02, HQ05, Pat01, Sus03, TTO1, BBG+02, GL06b, HW03c, LCP04, LLY06, LCK04, LCC05, RG05, Y04].
dynamic-key [LCP04].
dynamics [BG02, sHCP09, JLC07, MR00].
dynamics-based [sHCP09, JLC07].
EO [Ano05c]. E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-Goods [NCCG05]. e-Government [RM02].
E-Learning [CAC06]. e-mail [LL04b, ZZ05, All06, ANR01, KS00a, Law05].
e-mails [LG09]. e-payment [Has02].
E-Commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
E-commerce [Kir01a, TMM01, BM03a, Gra01, SN07, Sta00, MY01].
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, WYY05d, WH01, WC01a, XB01, XS03, YWD08, YLH05, Zan01, Zho06, ÁCTZ05, AFB05, Bla01b, CC04b, CC05c, CY05, CHC05, CLC08, DS09, Dew08, DWMW05, FP09]. Efficient [FSGV01, HHG06, HC04a, JW06, KHYM08, LPV+09, LLS+09, LCK04, LLH04, LYC02, Mic02a, MSP09, NR04, PCC03, RG05, RBB03, SLPO7, SKW+07, Shao15, SC05a, WK05, XCO5, Yan02, YTWH05, YCO9a, ZSN05, ZYW07]. Efficiently [IKNP03, NNT05, AGKS07]. effort [Weh00]. efforts [Pau02a]. Eggs [Wei06, Wei05]. EGPGV [MFS+09]. Egypt [EBC+00, Imr03, Sin00]. Eighth [ACM06, B+02, ELvS01, IEE01b]. Einstein [MNT+00]. EJB [TEM+01]. Ekert [Duw03]. El-Gamal [EKRA01]. Election [JLL02, Cal00b]. Elections [Cha04, PVS01]. Electromagnetic [SGM09, QS01]. Electronic [Ble07, CLK01b, CM02, Dur01, Ho01, ISO05, IY00, KMO01, KS02, Lan04b, LLL02, Mad00, MNFG02, Rub01, RMC01, Str01a, YKMY01, ZYM05, AvdH00, AAKD09, Cal00a, EY09, FB01, HWJ05]. element [MS02d]. Elementary [Sin09, Ste08, Tat05]. Elephant [Fer06]. Eleven [All03]. ElGamal [BJN00, CL02b, CWH00, HL04, LHT09, SJ00]. ElGamal-like [CWH00, HL04]. Elizabeth [Bud06]. Elliptic [AD09, An005a, Bai01a, BINP03, Bar00a, BBGM08, BM00, BS01d, BM01, BB00b, CQS01, CFA+06, GLV01, Guo02, GPP08, HY05a, HM01, HM04, HM02c, Hus04, JT101, JT01a, KBM09, KMF02, Kid02, KSSZ02, LW02, MP01b, Moi02, Kiri03, OTIT01, OS01, OT03b, PWGP03, RSA03b, RS04, RS01, Sat06, SI05, Was08a, Was08b, WPS01, XB01, YYZ01, vT01, BSS04, BSS05, BGM04, BGo07a, CCH04, Che06a, CFVZ06, DIM08, DWMW05, EHHK04, GKP01, Hsu05a, HL05d, JW06, LL04b, LWZH05, Mis06, MSV04, OS00, ST03a, SSST06, SH05, Sim02, Sma01, SC02b, SCL05, SLC05, TC05, Van03, Ver01, YC09a, YC09b, Yas08, ZSZ01, ZL05, ANS05, BWBL02]. Ellis [Coc01a]. Elmna [IEE01b]. Else [FL01b]. EMA [QS01]. Email [ES00b, Gar03a, Her09b, Luc06]. Email-Based [Gar03a]. Emanations [ZT05]. Embedded [An001c, An002d, An002e, BBGM08, Dr02, DV08, GS00, JT05, JQ04, KKP02, LPW06, NdM04, RS05, SPQ06, WK03, YS+01, AR08, BGM04, Fox00, GB04, KVN+09, KP01, KNP01, KP03, MBS04, Nis03a, TKP+08, XQ07, Fin02]. Embedding [AAD09, JX05, JQ07, LSC03, Sal03b, WY02, WC04, CO09a, KO09a, Wan05]. Embrace [CNB+02]. Embracing [An003c]. EMD [BR06]. Emperor [Smi01b]. Empirical [HW03b, Goo00]. empirically [SS03]. Emptiness [DIS02]. Emulex [CZB+01, CTBA+01]. Enabled [Por06, CCG01, DY09a]. Enabling [Web02]. encapsulation [CHB+09, KG09]. Encipher [BR00a]. Enciphering [HR03, KT01]. Encode [BR00a, BKN04, AN008c]. Encode-Then-Encipher [BR00a]. Encode-then-Encrypt-and-MAC [BKN04]. encoded [WMS08]. Encoding [JT01b, RS00, Lin02]. encounter [Win05c]. Encountering [Wo03]. Encrypt [BKN04, BTTF02, Dav01c, Pet05, Dav01b]. Encrypted [BBK03a, BGHP02, BGLS03, CD01b, Hugo04, Lan04a, LH07, MMZ00, RMC01, Sta02b, Van01, WRW02, Wl09, Woo00, AMB06, An006a, Bih02, BN08, CCMT09, CDD+05, CSK+08, FJ04, HLM02, Hes04a, LHL04b, LSH00, MW04, Pet03, UG08].
Encryption [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, BBM00, BBDP01, BU02, BF01, BF03, BB04, BGW05, BCHK07, BGH07, BPR^+08, BB03, BNPW03, BD03, BKY02, Bur03, CD00a, CS03a, CHK03, CHK05, CGHG01, Che01a, CTL00, Chi09e, Cho08a, CMR06, Cla00a, Coc02b, Coc01b, CNP00, CHJ^+01b, CDN01, CS02, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DFK^+03, DK05, DS05b, Dri02, FIP01a, FL00a, GC01a, GSW00, Gen03, GRW06, GD02, GMM01, Gutxx, HSH^+08a, HS02a, HY05a, HSHI02, HSHI06, HKR01, HW05, Har07b, Har00, Hei07, Her09a, HS00, HR05, HG03, HL02, HGNP^+03, HLL05]. Encryption [HLC08, ISSZ08, Joh03, Jol01, JK02b, JK02c, JM02, JKRW01, Jut01, KBD03, KSHY01, KS00a, KY01a, Kha05, KJK^+07, Kos01a, Kraf01, Kraf01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LLRR07, Loc03, LNP02, LM05, LCD07, Man01, Mar07, Mar09e, Mar09b, MF01, MM01c, MP01a, MP00, MP05, Mîîî03a, Mor06, Müîî01a, MS09e, NIS00, Nam02, NZCG05, NZS05, NP02b, Nie02b, PV06b, PM00, Pan09, Penn01a, PZ09, PDMS09, Pha04, Por01, PS00, Pre01, RM04, RK06, RDJ^+01, Sam01, Sch00b, SJO0, Siv06, SB00, CAC06, SRQL03, SPQ06, SBZ02, Sye00, TV03, Uni00a, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Ust01b, VMSV05, WZW05, WBF00, Wri01, YEP^+06, YW06, ASW00, Abd01, ABHS09, AKSX04, AMRP00, ABW09, Ano00c, Ano00c, Ano00f, Ano00g, Ano00h, Ano00j, Ano02a, Ano03e].

encryption [An006d, App05, Ate04, ACD05, AFGH06, BPS08, BKN04, BR04, BBN^+09, Ber09a, BBK^+03b, Bir07, Bii00a, BJN00, Bro05b, CG06, CS08a, CBSU06, CHC01, CKRT08, DZL01, DL07, DRS05, DW01, Fer06, FB01, Fox00, FMS05, GMR08, GG03, Gen09a, Gen09b, GKM^+00, Gou09, Gua05, Gut04c, HSH^+08b, HSI^+09, HS02b, HYW07, HCD08a, HCD08b, HAU04, HWW02, Hsu05a, Hwa05, HL05c, HL05d, IM06, JK01a, JK01b, JW05, JSW05, JCW05, KY00, KJ01, KSW06, KHL09, Kor09, KW00, Kre05, Küh08, Laf00, LV07, Lee01, LCP04, LJ05a, LMC^+03, LLLZ06a, LLLZ06b, LLCL08, LB05, Lu02, Lu05, LK01, LWK05a, M04, Mar05b, Mat02, Miiî01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pan03, RG09, Rhu03, RBB03, RSP05, SM00, SKW^+07, Sch00a, Sch01c, S^+03, Sch04a, Sch04b, Sch05a, Sch01d].

cipher [HAuR04].

cipher/decryption [OS07].

encryption [Sch01f, SR00, SVEG09, Shp04b, SK03, Ste00, SP03, SWH^+09, Tan01, TTZ01, TOEO00, TM01, TLH05, Un00b, UP05, VKS09, W02, W09, W03, WH02a, XY04, Yan02, YG05, YZ09, Y07, ZLG01, Z04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CHK08, CHJ^+01a, RR04, Un00f, Wu09, J008a].

Encyclopedia [Bid03, vT05]. End [KCD07, Per03, SKKS00, WWGP00, YSR01, AMB06, SU07]. End-to-End [YSR01, AMB06]. Ended [Kus02].

Endomorphisms [GLV01]. Endpoint [Kad07]. Enemies [DM07c]. Energy [GC01b, Ino05, LPV^+09, SLP07, M08]. Energy-efficient [LPV^+09].

Energy-security [Ino05]. enforce [SN04]. Enforcement [GN06]. enforces [BP05].

Enforcing [GMM08, HRS08]. Engine [Fri01, MMH02, DP04, SHL07]. engineer [Pau02b, SN04]. Engineering [CNB^+02, MNT^+00, MYC01, Pau01b, 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, YW04a]. enhancements [ADH+07]. Enhancing [BDK02a, MS05a, SE09, Sun00b, DY01]. enigma [Rob02, Rob09, BCB+05, Cas06, Chu02, Cop04b, DB04, GO03, Goo00, Joy00, Kap05, KS04, SM00c, SM05, SM07a, SE01, Wil01a, Win05b, Win00]. Enigmy [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, LSVS09, IM06, KKL09, KB00, Rhi03, Whi09, ZBP05]. Environmental [PS05]. Environments [CJK+04, LKHL09, BGM04, MNS08, SBG05, SBG07, SN04, YC09a, YbJf04]. ephemeral [Miˇs08]. Ephemerizer [Per05]. EPOC [JQY01]. ePOST [MPHD06]. EPR [Ina02b]. Equation [FJ03]. Equations [CP02, DDG+06, GS03, PBMB01]. Equipping [DMT07]. Equitability [DS01]. equivalence [Fis01a, LQ08, MSV04]. Equivalent [Fer00, KOMM01, May04, SIR04]. Era [MP00, Uni00c, Bur00, Uni00f]. erasure [PC03]. Erasures [JL00]. ERP [LSZ05]. Erratum [AGGM10, Kwo03b, LLLZ06a, McK04]. Erroneous [CH01b, MNT+00]. Error [BBK+03b, BQR01, Din05, KGG03, IW05b, LM02, MLC01, MPSW05, MZ02, NN06, SKQ01, YI01, YYDO01, ZYR01, Zol01, Gar04, LHL04a, YW06]. 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, MR02a, MR02b]. essentials [HHL+00, Irw03]. establishing [Kov03, KH03]. Establishment [BM03c, NIS03b, HMvdLM07, LF03, SL05a]. Estimation [EFY+05, JX05, KLB+02a, LNL+08, Sel00]. ethical [Har05b]. Euclidean [CPhiX04, CMJP03, CLZ02, WL02]. EULA [WWL+02]. EUR [Eag05]. EUROCRYPT [Bih03, CC04a, Cra05a, Kun02, 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, CS00, FML+03, IKM00, YI00, JJ00a, Kan01, Kir03, SKKS00, BZP05, FXAM04, FS03a, LPC04, 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 [LMHCTR06]. Exact [Cor00b]. examines [Nis03a]. example [Bla00, GC05, Zir07]. Exchange [BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JL08, KOY01, KY03,
MPS00, Mac01, MSJ02, Ngu05, VPG01, WC01a, WV01, ZWcy02, BBG+02, BCP07, CLC08, CWJT01, DG06, GL06a, GMR05, HTJ08, KS05a, KOY09, LHH04b, LW04, LFHT07, LHC08, LSH00, MS03a, Mis08, WLH06, YC09a, YPKL08, ZYW07, CPP04, CP07, ECM00b. exchanging [KN08].

Exclusive [GRW06]. Executing [HILM02, LJ05a]. Execution [Coo02]. Exhaustive [Des00c]. Existing [MV01, BDET00]. Expanded [Cho08a, Irw03]. Expanding [DN02a]. expansible [LLW08a]. Expansion [DN02b, BCD06, HKPR05]. expansions [HKPR05]. Expected [KL05, RK06, DLP+09]. Experience [Sas07, BChJ05]. Experiences [MPHD06, USE00b]. Experimental [BG09, CGBS01, OOP03, WS02, RSQL03, Smo04]. Experimentation [Hum05]. Experiencing [LSVS09]. experiments [Bru06]. expert [Ano01g]. Expiration [MP00, Sch05b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOBR05]. exploitation [Eri03, Eri08, KVN+09]. Exploiting [CK06, ETMP05, HR00, HM04, ZWC02]. Exploits [MJF07, CSW05]. exploration [SKW+07]. Exploratory [Lut03].

Exponentiation [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 [ADDs06, IKNP03, Ove06, Sal03b, SS01a]. Extending [Bai01a, YWD08, BR06, CmvdV06]. Extensions [ABC+05, BBGM08, CS07c, HM02b, Rot02a, Wei04]. Extracting [Cer04a]. Extraction [DGH+04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lnt02, 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, BSSM+07, Hen06b, Sch05c, St.00, Ste05a, YWW08, dB07]. Factoring [BN02, KOY02a, KLB+02a, KOMM01, May04, PV06b, ST03b, LTH05, LCZ05c, Mü01b, PLJ05a, QCBO5a, Sha03d, Sha05d, ZCL05]. Factoring-Based [PV06b]. factorisation [GG08]. Factorization [CDL+00, Lam91].

Facts [GO03]. Fade [CAC03]. Fail [JQY01, SSNGS00]. Fail-stop [SSNGS00]. Failures [DFG01, HGNP+03]. Fair [CC00, DLY08, GC01a, JLL01, JL04, LMS05, PS00, VPG01, WV01, LSA+07, MS03a]. Fair-Zero [LMS05]. fairness [GCKL08]. faithfulness [GTZ04]. false [ZSJN07]. Falsification [OM09]. Fame [Bar00c]. Family [CQS01, Fhu02b, NPV01, S05a, You1, Ber07, FNR05, GKP01, MP07]. Fan [YRW05c]. fare [GMG00]. Fascinating [Sch09]. FASME [RM02]. Fast [AL00b, ABM00, BDTW01, BST02, CJS01, CC06, CQS01, Cor00a, Cou03, Cro01, FS02, GC01a, GD02, GMM01, GPC08, HGG07, HR04a, JJo0d, KKIM01, KK03, KKS+07, LSY01, LS05b, MSNH07, Kir03, N05a,
Flexible [LP02a]. Flexible [CMG+01, CLK01b, DGK+04, OT03a, Tsa01, BA06, KOC05, LHY02, WWA01]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM+09]. Flows [ECM00a, AHS08, Cer04a, Lau08a]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM+09]. Flows [ECM00a, AHS08, Cer04a, Lau08a]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM+09]. Flows [ECM00a, AHS08, Cer04a, Lau08a]. Floating [NS05c]. Floating-Point [NS05c]. Flow [BDNN02, ABEL05, FR08, ME08a, TWM+09]. Flows [ECM00a, AHS08, Cer04a, Lau08a].
Joh03, Mat02, RM04, Sch00b, Sch01d. FTC [Ste05c]. fuels [Mad04]. Full [Cor00b, DOP05, LKHL09, WYY05b, WYY05c, BI04, CS08a, HS02b, LKH+08, Oiw09].

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

Function [BR02, CDMP05, Fis01b, Flu02b, GIS05, HNO+09, HPC02, JJ00a, Kan01, Kil01b, Nef02c, RB01, Yan05, CHY05b, CJ04, HR07, LW04, LPM05, Tsao08, WWTH08, YW05, YRY05b]. Functional [Bl08, FS01a, Gen09b, KPMF02, RG09, Gen09a]. Functionality [ETMP05]. Functions [AEMR09, BBDK00, Bon01, Can01b, CV02, Car02, Che01c, DNO2a, DGN03, DNRS03, Fil02, FIPR05, GLG+02, 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, KKI07, KSO5b, LLH02, LKY04, MS02b, MS00c, Mic02a, Mic02b, NR04, PW03, 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, NFQ03, Sch00e, Ano05b, HP00, LPW06, SK03].

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

G [Coc03, For04, Was08a]. Gaitherburg [SMP+09]. Gamal [EKRA01]. Game [DHR00, LM02, AC06, BR04, Gon09, HCBLETGR06]. game-like [Gou09].

game-playing [BR04]. Gamers [MP00]. Games [KN08, HCBLETGR06]. Ganesh [For04]. 

Ganzía [GP06]. Gap [OP01a, PWGP03, RW03a, Sch02, Sch04d]. Gap-Problems [OP01a]. Gate [Coc02a, GC01a]. gates [TWM+09].


GCM [KS09a]. geeks [McN03]. Geheimschreiber [Joy00, UW00]. GEM [CHJ+01a, JM02]. General [AB09, CDM00, DN00a, ESG+05, GMP01b, Kog02, Lin03, MND+04, Sal01a, YC01, HCBLETGR06, HY06, JL03, LJO5a].

General-Purpose [ESG+05]. Generalisation [DJ01]. Generalizations [YYZ01, HWW02]. Generalizations [LD04, LS08]. Generalized [KSR02, Mic02a, TC01, TJ01a, Wag02, WHLH05, LKYL00, LWL09, SHi05].

Generate [HSR+01, Wer02, FSGV01]. Generated [ADD09, MRL+02, RBF08]. Generating [BMK00, BCDM00, GG01, MFK+06, SS03].

Generation [ACS02, BH05, BK06a, CS03c, ESG+05, GJKR03, GL01, GW01, JG01, MR01a, Raml01, TL07, TV03, WP03, WHLH05, Web08, WS02, Ano04c, BK07, BG08, BF01c, ISTE08, LS05b, TNG04, Van03]. Generator [ADD09, BP01a, Di05, Diec03, DGP07a, DGP07b, DV08, EHK+03, Gen00b, GM02a, Gol01c, GPR06, Int03, Kel05, LMCETR06, LV04, SY01, SFD06, TWNA08, TZT09a, TZT09b, ZKL01, Aam03, ACTZ05, BeI08, BG08, BG09, BG07a, DGP09, BG09, HG05a, HlwWZ09, JAW+00, KH08, KS00, Pan07, PSG+09, PSP+08, PC00, RGX06, SR07, SB05, UHA+09, WW08, VKS09].

Generators [BST03, BK06a, BL08, CF01b, CS05b, Fin06, Kra02a, LBZ01, LBZ02, LS05a, MH04, RSN+01, Vav03, BK07, BPGS05, CO09b, SK01b, Tsao06, YZEE09].

generators-part [SK01b]. Generic [BN00a, DOP05, GGKT05, HLL05, Mar02b, MV01, GT00, MP08, Sch01f, Sch01e, XLMS06, CHJ+01a]. Genetic [HSIR02, LMHCETR06, CV05, SC05a, WJP07].
Gennaro [Miy01].
Gennaro-Krawczyk-Rabin [Miy01].
ge [RR03a]. Gentry [Hes04a]. Genus [CY02, GHK +06, Wen03].
Geometric [GTTC03, HH09, LL05a, LJ05b, SDF01, CJT01]. Geometrical [LWS05].
geometry [PFV96, WW06].
George [Gum04].
Georgia [IEE09b].
German [Sch09, Ano04b, Mer05, Sal00b, Sal00a, Win05b].
Germany [DR05, Duw03, FLA +03, WKP03, IEE01b].
Geschichte [Sch09].
Get [Coc01a, W01a, Cla00b].
gets [Bor00].
Getting [PM00]. GF
[BINP03, KPMF02, KLY02, KKY02].
GH [GHW01].
GHS [Hes04b]. giant [Lam07].
Gibson [Ove06]. Giesbrecht [CHH01].
Gigabit [CGS01]. Gigabits [HTS02].
Gibson [Ove06]. Goes [Pan07].
Golds [Boy01, For04, Tsa07].
Goldreich [Kat05b, Lee03b, Puc03, AC02].
Gong [GG01].
Good [CB01, Kid02, MP06, G05b, vTO01].
Goodness [CMB+05].
Goods [NZCG05].
Google [Con09, Law09b].
Gooing [Con09].
GOST [SK01a].
Goubin [Sma03b].
Governance [TPM07].
Government [IY00, RM02, Lev01, LCS09].
Governments [Ano00g].
GPB [Bau01a, Bau01b, Luc06].
GPS [CKQ03].
GPT [Ove06]. GQ [BP02].
Graduate [GV09].
Grafton [Pag03].
Gran [Rhi03].
Grained [SS01b].
Grand [Svy02].
Grand [Ano00h].
Graph [CGFSG09, GTTC03, HM02b, VVS01, YKW01, CTT07].
Graph-Based [CGFSG09, HM02b, CTT07].
Graphical [vOT08].
Graphics [CK06, DNP07, MFS+09].
Graphs [NNT05, Ust01b, WGL00].
Gavrilenko [Puz04].
Gray [FGD01, Har05b].
Gray-Scale [FGD01].
grayscale [YCL07].
greatest [Bel07a].
Greece [ACM01a, KGL04, SM07b].
Green [HKP05].
GREMLIN [H01].
Grenoble [AMC05a].
grey [BDF00, SC05a].
Grid [AMC05a, MJ01, SEF+06, WKP03, IEE01b].
GridOne [YC09c].
Grids [CTY09, MPPM09].
Grip [Buh06].
Gröbner [CCT08, FJ03, Fau09].
Group [ANR01, AAFG01, ACJT00, BBS04, BCP01, BCP02a, BCP02b, CD00a, CvTMH01, CH01a].
HSH02, HSH06, HW04, Hug02, JP02b, KY03, Kin02, LZZ+01, MS05, SOO02, SWH05, Ste01, Tan07b, VMS05, Wer02, AKNRT04, BCP07, CLO4b, CYH04, CH05, CWJ01, CJT04, Cho08b, ED03, HC02, Hen06a, HW02, KS05a, KPT04, KKK09, LL06, LLH04, LPM05, LJK05b, NS05b, PQ03a, PQ06, RH03, SN01, Sha05a, TJ01a, Tse07, WGL00, WH08, YLC+09, Y05a, ZC04, ZX04].
group-by [YLC+09].
Group-Oriented [LZZ+01, HW04].
CHC05, CWJ01, LL06, TJ01a, WHHT08].
Groups [BSS02, CV03, CF02, Dri00, GM02a, G01, K01, KPP04, KKK09, LL06, TJ01a, WHHT08].
Group-Oriented [LZZ+01, HW04].
CHC05, CWJ01, LL06, TJ01a, WHHT08].
Groups [BSS02, CV03, CF02, Dri00, GM02a, G01, K01, KPP04, KKK09, LL06, TJ01a, WHHT08].
Guanajuato [Buc00a].
Guangzhou [LL+04, Li05].
Guessing [AGK07, Bau05, Shi05, YS02, DLMM05].
Guest [K03, Sak01, BK06b, MFS+09, PTP07, SJT09, SK08].
GUI [LG09].
Guide [Ano06c, BS01a, BSB05, BCP+03, B01b, HM04, Poo03, Vac06, Wei04, And08, Bon00, Bro05b, C+02, Che00, Gar03b, Kov03, Luna09, Mol05, SL06].
Guidebook [SEK01, SEK02]. Guided [ZY08, Pet08]. Guidelines [MMZ00, Die00].
Guidford [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, MAaT05]. Hall/CRC [Kat05b, Was08a]. Halfmad [BS01b]. Halfspaces [KS09b]. Hall [Bar00c, For04, Kat05b, Was08a, MAaT05]. Hall/CRC [Kat05b, Was08a]. Halfmad [BS01b]. Hamming [GK02]. hamper [Lov01]. Hand [WBL01]. Handbook [And04, Cas02, CFA +06, Jan06, MMJP03, RE03, AB09, Fin03, Har05b, KB00, KH03, MJ03, RE00, dLB07, Was08a]. Handheld [BMK00, Ano06a]. Handbooks [MP00]. Handle [RC06]. Handling [KL05, Lut03]. Handoff [OKE02]. Hands [KLB +02b, Shu06]. Hands-on [KLB +02b, Shu06]. Handshake [SB01]. Handshakes [Ver06a]. Handwriting [Ano02d]. Hankerson [Irw03]. Haptic [PBM +07]. Haptics [Pau02a]. Hard [Har07b, HMS04, Lai07, CGH06, GPV08]. Hard-Core [HMS04]. Hard-Disk [Har07b]. Hard-Line [Lai07]. hard-on-average [CHG06]. hardcore [Sch01e]. hardcover [Eag05, Pag03, Top02, Pap05]. Harddisk [Por01]. hardness [Mos06]. Hardness [CHS05, CNS02, KY02b, KS06a, LTW05, SV08b, AGGM06, KS09b, SU07, AGGM10].
Hardware [Ano02b, Ano07b, Ano07a, BM01a, DF01, Dic03, FW09, FD01, Fri01, GS03, GS07a, GK02, GPS05, GLG +02, Gro01, GPP08, IKM00, ISW03, JQ04, KKP02, Nd05, PS01c, RS05, RS04, SOTD00, SMTM01, SM02, SM03b, SRQL03, SGK08, TSO00, TBLD01, WK03, WBRF00, XH03, XB01, YKLM02b, Zhe02a, ARJ08, Ano00a, BBK +03b, DS09, EHKH04, GC00a, HBC +08, KP01, KNP01, KP03, NiM04, RAL07, SOIG07, VS08, WOL04, YKLM03, YW06]. Hardware-based [Ano02b]. hardware-constrained [RAL07]. hardware/software [ARJ08]. Harley [WPP05]. Harn [GG01]. Hash [Ano08d, Ano12, AERM09, BBKN01, BR02, BDS09b, Bur06, CBB05, Cor00b, Cor02, CDMP05, CS02, DOP05, FIP02b, Fil02, GIS05, GLG +02, HPC02, HR04b, ISO04, Jou04, KMM +06, MD05, RRS06, RR08, RB01, SS01a, Sho00a, Sho00b, SK05a, WFLY04, Yan05, YZ00, BR06, DS09, KCL03, KLu04, KCC05, LLH02, LK04, LW04, MS09c, Mic02b, Ts008, Wag00, YRY04, FIP02a, ZW05a]. Hash-based [BD09b, KCL03, KLu04, KCC05]. Hash-CBC [BBKN01]. Hash-chaining [CBB05]. Hash-Function [BR02]. Hash-functions [ISO04]. Hashes [Sch01a, GNP05]. Hashing [IKO05, SGGB00, WS03]. HAVALEH [WFLY04]. HAVALEH-128 [WFLY04]. HAVEGE [SS03]. HB [MP07]. HB-family [MP07]. HB-MP [MP07]. HCI [YKMB08]. head [RFR07a, RFR07b, RFR07c]. headlines [Hen06b]. Health [Mad00, Ano03a, CCCY01]. health-care [Ano03a]. Healthcare [BTTF02, heap]. Help [Buc00a, PPV96, Uni00b]. Held [Buc00a, PPV96, Uni00b]. Hellman [KM04a, ABR01, ASW +01, BS01d, BMP00, BCM01, BC02a, BC02b, BC07, CY08, CU01, CJ03a, CKR08, FS01b, GR04, Ki01b, KK02, Kra03, Kra05, Misi08, Ts006, YRY05]. 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, Höf01, KYHM08, ZBLvB05]. heuristic [SS03]. HFE [FJ03, ChH01, Fel06]. HFE-Cryptosystems [Fel06]. HIBE [CS07c]. Hidden [HGN03, KV03, LNS02, GMR05, Lun09, Shp05, FJ03, Sch09]. Hide [CC06, PH03, Shp05]. hide-and-seek [Shp05]. Hiding [BD03, CLT07, Col03, DN02b, GA05, HNO09, LHS05, LS08, MH05, MMT09, VDKP05, WC03a, HR07, JD01, KP00, RSP05, Way02b, Way09, YCL07]. Hierarchy [HC08]. Hierarchical [GS02b, HNZI02, HL02, Lin01a, MN01, YHL05, BD04b, Che07, C303c, JW06, KAM08, WC01b, yY08]. hierarchies [AFB05, Cer04a, HY03, WL05]. hierarchy [CMD06, HW03c, Hwa00, JA02]. Hierocrypt [OMSK01]. Hieroglyphs [Wri05]. High [ACM01b, A000c, A002d, ChL019, CW09, CLJ06, CGJ02, DS05b, FZH05, Gro01, HNZI02, HV04, Int00, JKRW01, KMM06, Ken02b, KM05, KB00, Kra05, KT01, MM01b, NFQ03, RW07, SKKS00, SOTD00, SM02, SG09, SLG05, TL07, Uni00c, Wie00, WWG00, YKMY01, Zhe01, BVP04, BZP05, BGL03, Jen09, KC09a, SK03, WWTH08, Zir07]. high-assurance [Jen09]. High-Bandwidth [CGJ02]. High-Dynamic-Range [CW09]. High-End [SKKS00, WWG00]. High-Performance [Kra05, NFQ03, BZP05]. High-Speed [A000d, A002d, Gro01, JKRW01, KMM06, SOTD00, SM02, Wie00, YKMY01, RW07, BGL03]. High-technology-crime [KB00]. High-Throughput [HV04]. Higher [CV02, KCP01, BF01a]. Highly [CV02]. hijacking [Ste05c]. Hill [Gun04, USE02a]. Hilton [KJR05]. HIPAA [AEV07]. histograms [CO09a]. historic [Pet08]. Historical [RE02, MMO01]. History [BP03, ffr00, Pag03, Sal01a, Sin01b, CAB06, Top02, AJ08, Boo05, HSW09, Jan08b, KNS05, Naf05, Nis03a, Pin06, Ris06, RH00, RG06, Wi01a, dLB07]. history-based [KNS05]. hit [Bjo05]. HMAC [FIP02a, DGH04, Hir09, RR08]. HMQV [Kra05]. Hoare [dH08]. Hoax [CZB01, CTBA01]. hoc [BSS02, Cha05b, DHMR07, K05, KVD07, LH08, LZK04, PCRM07, SLP07, TW07, WT02, ZC09]. Hold [PM00]. Holier [MYC01]. Holistic [RM02]. Homage [JP02b]. Home [IEE00b, SEK01, SEK02, CAC03, Pet03]. Homegrown [Str02]. Homeland [Man02, Mant05, RR03]. homogeneous [MF07, PS02a]. Homomorphic [AS01a, Aki09, CDN01, DN03, HS00, Cho06, Gen09a, Gen09b]. homomorphism [CKN06]. homophonic [Sav04]. Honeyd [Dim07]. Hong [B02, ZJ04, Cla00b]. honor [OC03]. hook [JEZ04]. hooks [GJG05]. hop [NC09, ZSJN07]. hop-by-hop [ZSJN07]. Horizon [Coc02b]. host [Shu06]. hostile [ABB04]. Hosts [Hs01, ZS08]. Hot [IEE01b]. Hotel [USE01b, USE01a, USE02a]. HotOS [IEE01b]. HotOS-VIII [IEE01b]. hours [Fox00]. House [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hsu [BCW05, HL05c]. HTML [CNB02]. HTTP [Zha00]. Huang [ZC05]. Huge [HN07, NNT05]. Hull [KMT01]. Human [Dre00, GL01, JW05, K01, Man08, MS02d, RFR07a, RFR07b, RFR07c]. Human-Memorable [K01]. Hundred [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Hunting [GL06]. Hung [SCS05b, ZK05, Hsu05a, HL05d, KTC03, KCL03, LW05c].
I-tracings [RE02], i.e [NP02a, Wil99]. IA [WWCW00]. IA-64 [WWCW00]. IACBC [JMV02]. IBE [ABC+05]. IBM [AV04, ADH+07, CGH+00b, Web08, Weh00]. Ibn [MAaT04, MAaT05, MAaTxx, MAaT07]. Ibn-Adlan [MAaTxx]. Ibn-Al-Durahim [MAaTxx]. iButton [HWH01]. IC [BGI+01, DOPS04, RR05]. ICBA [ZJ04]. ICCMSE [SM07b]. ICISC [Kim02, LL03, LL04c, PC05a, Won01, WK06]. ICISC’99 [Son00]. ICM [IEE09a, IEE09a].

ICs [Bar00c]. Id [ZJ09, BRTM09, CCD07, CL07, CS07c, CL00, GS02b, GTY08, HCO8, KLY03, KHL09, Ku02, LCS09, Sco04, SW05, SCL05, WBD01, WHO2b, YCO9b, YLH05, ZKO2, ZCO4, ZCO9].

Id-Based [ZJ09, CCD07, GS02b, HCO8, Ku02, WBD01, YLH05, ZKO2, CL00, KHL09, Sco04, SW05, SCL05, WHO2b, YCO9b, ZCO4, ZCO9].

IDE [An02d]. Idea [Cos03, RR03a, CTLL01, HTS02]. Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b]. Ideas [Gha07, Eri01].

Identification [BP02, BLDT09, Gar03a, GL+04, KK02, Kir01b, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW+08, ZCO9].

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

identities [Kwo02, Kwo03b]. Identity [App05, BF01b, BF03, BB04, BCHK07, BGH07, BPR+08, Boy03, BRTM09, CL01a, CHM+02, Coo11b, D03, GKO4, Her06, Her07, HY01, HL02, KC02, LCD07, Mar08a, Mar08b, PCSM07, SMP+09, BMW05, CG06, CJL05, GG08, KG09, LWZ05, RG09, Sage02, Shao03c, Wao04b, Win05a, YCW+08, ZYW07]. Identity-Based [BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, LCD07, Mar08a, Mar08b, App05, Her07, PCSM07, BMW05, CG06, CJL05, KG09, LWZ05, Sage02, Shao03c, YCW+08, ZYW07].

IDSFM [TZDZ05]. IDtrust2009 [SMP+09]. IEC [ISO04]. IEEE [BS03, BCDH09, BC01, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, KM07, HSD+05, Hug04, Mis08, PHM03, ZWD06]. IEM [RC05]. IFIP [DKU05, DFPS06, DFCW00, ELvS01]. II [Ban05, Bau01a, Bau01b, Bau01c, Bec02, Bud00a, Bud02, Bau03, Kov01, MH09, OC03, Res01a, Res01b, Sal00a, ZT03]. III [Sch00a, An00d, Bau03b]. IKE [CK02a, Kra03]. I'll [PLW07]. Illinois [ACM04b]. Illusions [Koc02]. illustrated [Lun09]. In [BGI+01, DOPS04, RR05].

IMA [Pat03b, Sma05, Hon01]. Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, CL07, CC09, CC06, GW01, KBD03, KC09b, LLS05a, LZ01, IWS05, LY07, LJ05b, LSC03, LSKC05, PZL09, RSO0, SDFH00, SDF01, SSFC09, SYLC05, TTT01, TH01, TC01, UP05, VS09, VK07, WY02, WLT05b, YZEE09, AAP07, AA08, CC02b, CHC01, Che07, Che08a, GSK09, HLC07, KC09a, LLCL08, Lin00a, LT04, LYCL07, LLCL06b, MS09a, MB08, PBV08, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, mSgFl05, TL02, Wan05, WMS08, WC05, YCYW07, YCL07, ZLZ07].
Image-Feature [GW01].
Image-Identification [PBV08].
Images [CTL04, CC08, CW09, DP00, FGD01, LS08, PJH01, PBC05, RE02, WCJ09, WC04, YWWS09, AAPp07, AEEdR05, BDN00, FWTC05, HHYV07, TCC02, TND+09].
Imaginary [HJW01, HM00, HHYW07, TCC02, TND+09].
Imai [DDG06, YG01a].
Imbalanced [ZWCY02].
Immersive [Coc01a].
Immune [CZK05, PZ02b, YKLM02b, ZP01, YKLM03].
Immunization [HR05].
Impact [Ber03, HGNP03, JKRW01, MMYH02, Wri00, CS08a].
Imperfect [CPS07, DOPS04].
Impersonation [BP02, Hsu05b].
Implant [Fox00].
Implement [HQ05].
Implementation [AD07, Ase02, Ash03, ARC+01, BBD+02, CCDP01, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HHM01, JKS02, KMM+06, KV01, LDP02a, MMZ00, MKP09, MM01c, MNP01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBTW07, QSR+02, RDJ+01, SM01, Sha01e, SK05a, SRQL03, USS02, Vir03, WZW05, WW00, WOL01, XBO01, Zee00, BI04, BBK+03b, C+02, CNPQ03, DS09, DKL+00a, GHGGS00, GBKP01, Hiih00, HP01, Hut01, KY09, LL04b, LCX08, LB05, Rhi03, SM03a, SVDF07, Wol04, YW06, ZFK04].
Implementations [AL00b, BJP02, III00, CTL01, CGBS01, EPP+07, GLG+02, MM01b, MP01a, RS01, WWCW00, ASK05, BFCZ08, BFGT08, BG07b, FR08, RAL07, RSQ03].
Implemented [TSS+03].
Implementing [Dwi04, Ko08, LM08, MDO4, MWS08, NDJB01, Pet03, Smi01a, SR06, C+02, CW02].
Implications [Kun01, LJO5a, MF01, Ayo06, BJO05, Fri07].
Implies [KY01e].
Imply [Pie05].
Importance [ANO2b, KCJ+01, TIGD01].
Important [SM00a].
Impossibilities [CHL02].
Impossibility [APV05, BPR+08, Fis01b, PQ06].
Impossible [BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SKI01].
impostor [LC07].
improve [Pau02a, CAC06].
Improvement [CAC06].
Improved [ABF06, BPR05, BB05, BF00b, CL01b, CKK+02, CJ04, DN00a, DG02, Fun03, FKS+00, FKL+01b, FKL+01a, GMR08, Gen00b, HCK09, HKA+05, JQYY01, Kin00, KT06, Ku02, Kiih02b, LW04, LL06, Mic02b, Miy01, MH04, Kir03, MS02e, PR08, ST01b, SWH05, SC05c, TNM00, YSH03, ZKL01, vDKST06, CYY05, HTJ08, Iwa08, PR05, QCBO5a, YW05, YRY05a, ZW05a].
Improvement [AS01c, AJO08, Che04a, CCK05, CWW02, Di01, HWWM03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Sha04b, Sha05b, WHLH03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JSW05, JnBdXn05, KJY05, LL04a, LW05c, SZS05, TO01, WLT05a, YW04a, YWC05, YRY05a, YRY05d, ZC09].
Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, HW03c, SRQL03].
Improving [AS01c, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SKQ01, SB01, Sun02, XQ07, YEP+06, YGZ05].
incentives [Swi05].
Incident [JBR05, Tom06].
Including [SR01].
Incomputable [Ver06b].
inconsistencies [MS09a].
Incorporating [MFS+09].
incorrectness [CHC04].
Increase [PBTW07].
Increasing [CS05c].
Incremental [BKY02, LKLK05].
IND-CCA [Miil01b].
IND-CCA2 [BST02].
Independence [BP03b].
Independent [BS00a, BSL02, Kin02, GSK09].
Index [An000b, An001d].
indexing [YPPK09].
India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, An003c].
Indies [Fra01, Syv02, Wri03].
Individual [BCC02, TW07].
INDOCRYPT [CV04,
KI03, LCK01, LLL02, LP03, LV00, Len01, Lin03, Lin00b, MPS00, Mac01, MSJ02, MHM+02, May04, MR01b, MR01c, Moli03a, Mol03b, Mii01a, Mur00, NIS03b, NA07, Ngu05, NBD01, NSS02, OTU00, Ort00, PHK+01, PR01, Poi02, PHM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sha01e, Sin01a, SVW00, SK00, Ste01, ST01c, TS000, Tan07b, TT01, VV07, Wal03, WZW05, WH01, WC01a, Wo00, WBD01, Wya02, 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-Based [Sha01e]. Key-Dependent [Gol03, BPS08]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKXY02]. Key-management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DKS05]. Key-Share [CT08a]. Key-Sharing [HNZI02, WBD01]. Keyboard [ZTW05]. Keyczar [Law09b].

Keyed [Küh08, SR00, FIP02a]. Keyed-Hash [FIP02a]. Keying [ABB+04, Che08a, EGK08]. Keyless [Qu01].

Keys [AOS02, APV05, AFI06, BT02, BMK00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, Luc00, MN01, MRL+02, Oni01, PS00, Smi01c, Str02, TvdKB+01, BCL05a, BCW05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH+08b, HSH+09, HW04, HY03, HL04, KAM08, LHL04b, LLW08b, LS01c, LWK05a, ML05, NN03, Sch01e, Sh04b, Sh05b, SB05, TLH05, TJC03, WH03, YRS+09]. Keystream [AMRP04, Kra02a, HW04, HY03, KY04, JUC08, LLW08b, PS01a]. Keystroke [sHC09, MR00, BGP02, LJC07].

Keystrokes [SWT07]. Keyword [FIP05]. KGC [HLC08]. KGS [ZYW07]. KHAZAD [PQ03b]. KIAS [May09]. Kid [CAC06].

Kikai [An00d]. Kikai-Shinko-Kaikan [An00d]. kill [Lov01]. Killing [Lov01].

kind [DW01]. King [Eag05]. Kingdom [DFCW00]. Kingston [HA00, PT06]. Kit [An02c].

Klaus [An04d]. Kleptographic [YY01]. knapsack [Kos01c, SLC05]. knapsacks [Mic02a]. Knife [Boy03].

Know [CMB+05, Ros07, Con09, DKK07, Win05c]. Knowing [CH01a]. Knowledge [Abe01, Abe04, AS01b, APV05, BP04, Cou01, DPV04, DFS04, DDO+01, Er102, Fis05, Gen04a, GKO5, HNO+09, KS06b, LMS05,
Knowledge-of-Exponent [BP04]. Known [CKN06, CMB+05, DN02a, Fur02b, HSH+01, Bao04, YTH04]. Known-IV [HSH+01].

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

Koblitz [AHRH08, Has01b]. Kolmogorov [Sch01a]. Kommunikation [Lin02].
Kong [Bh+02, ZJ04, Csa00b]. Konstantin [Puz04].
Korea [CSY09, CKL05, KCR04, Kim01, Kim02, LL03, Lee04b, LL04c, May09, PC05a, PK03, Son00, Won01, WK06]. Korner [Mor03]. Ko´sciuszko [OC03]. Krawczyk [Miy01].
Kryptoanalyse [Mor05]. Kuala [DV05]. Kunming [ZYH03]. Kurtz [Gao04]. Kyoto [Oka00].

L [Sem00]. L-collision [Sem00].
Laboratory [Bru06, LBA00]. Lagrange [FWTC05].
Laid [Wei06, Wei05]. Lam [Wag00]. Lamar [LMHCETR06]. lamp [Me03].
LAN [Bar03, LFHT07, Pau03, SZ08, Sty04].
Lanczos [BF06a]. Landau [Jan08a].
Language [ARC+01, DD02, Gou99, Jen09, MW04, WAF00].
language-based [WAF00]. languages [Lun09, Rob02, Rob09].

Laptop [PGT07]. Large [AAC+01, BH00a, B+02, CDR01, Cro01, EBC+00, FLA+03, GG01, Kuh00, PG05, SM01, ST03b, USE00a, BP03a, CKY05, CJ03b, Has00, HmvLM07, HY03, PS08a, SM03a, TM06, WL05].
Large-Size [CDR01, BH00a, BP03a, HmvLM07, PS08a].
Larger [Car02]. LARPBS [CPH+04].
Lasers [Ig02, UHA+09]. late [Sch05c].
latency [RSP05]. Lattice [CD01b, HHGP+03, MV03a, MR09, BLRS09, HPS01, HG07, IM06, Mic01, Reg03, Reg04].
Lattice-based [MR09, HPS01, IM06, Reg04].

Lattice-reduction [HG07]. Lattices [NS01c, Ngu01, GPV08, Gen09b, Mic02a, Reg05, Reg09, Shp05, Sif01]. Launched [Bar00b, Ano00]. Launches [Ano02d]. lava [Mc03].

Law [GN06, MNFG02, Ste05c, NM09]. Layer [LXM+05, LPV+09, SL07, ZL04c].
layered [KVD07]. Layers [Gri01]. Laying [Lut03].

Lazy [CCM05]. LDAP [Bau03a, Bau03b, BH00b]. Lead [Tsa07].
Leak [RST01]. Leakage [CKN01, DP08, Ke02, RS01, ABHS09, CNK04, IY05].
Leakage-Resilient [DP08]. Learned [GSP+04]. Learning [SK06a, LY07, CAC06, BKW03, KS09b]. Mal06, Reg05, Reg09, SM08, Wh09]. Least [SZ01]. lecture [Rot02b, Rot03, Adl03, RSA03a, Riv03, Sha03b]. Lee [Sty04, YRY05d, Coc02b, KRY05, KHL05, LKY05d, SC05b, ZK05]. Left [Dhe03, HK05]. left-to-right [HK05].

Legal [Coc02a, AN03]. Legislation [Eng00]. legislative [AvdH00]. legitimate [Lin01b].
Leighton [Rub00]. Leighton-Micali [Rub00].
Length [AR01, BR00b, CKN00, CHJ+01b, M003a, RK06].
Length-Preserving [M003a]. Leonard [Coc03]. Less [YKM01, BD00b]. Lessons [GSP+04, KFSS00]. Lest [HS+08a, HSH+08b, HSH+09].
Lets [Pau02a]. Lett [Kwo03b]. Letters [ASW+01, BTTF02, MNT+00, TEM+01, TvdKB+01, WYL+02].
Leuven [BB00, DR02c]. Level [EP05, MV00].
TV03, BDN00, DHL06, KYN+09, SSO3].
Levels [KM05, CUS08, Voi05]. Leveraging [BRT01]. LEVIA THAN [CL02c]. Levin [AC02].
LFSR [DS09, Jam00, JZC05].

LFSR-Based [Jam00]. LHL [Pei04, YRY05a]. LHL-key [Pei04, YRY05a].
Li [JW01, KCL03, SZ05, QCB05a, SC05b, ZK05]. Light [T01b].
Liberty [Lan04b, An00e]. Librarian [PBV08]. Libraries [Fin02, MK05b].
[HGR07]. Low-Power
[Ano00d, JP02a, KBM09, CO09b, ZYW07].

Low-State [GST04]. Low-Weight [CH07c].

Lower
[BD07b, BP03b, DIRR05, GT00, GKK03, PS02a, Shp03, WW05, KS05b, Shp99]. LSB
[CS05c, FGD01, WMS08]. LSB-encoded
[WMS08]. LSD [HPS02a]. Lu [QC05b].

Luby
[MP03, Pat03a]. LUC [LNS02].

Luminy
[PPV96]. Lumpur
[DV05]. Lund
[Joh03]. LUT [CC02a, TL07]. Luxembourg
[Bir07]. Lyndon
[GS01, VS01]. Lynn
[Hes04a]. LZ [AL04]. LZ-77 [AL04].

M [DNRS03]. M8 [TM01]. MA
[ACM10, JQ04, Kil05, KP01, Nao04, Pag03]. MAC
[BKN04, CMM00, Kil03, LPV*09, Vau01, Kra03]. MacDES [CKM00].

Machine
[LBA00, Mul06, Pro00, Cas06, Kid00, Pau02b, SWR05, WNQ08, Win05b, HMO1a, Pet08].

Macraigor
[Ano02d]. MACs
[BPR05, BR00b, BM01c, Sem00]. Made
[Ste05b]. Madison
[FMA02]. Maelstrom
[MYC01]. Magic
[DNRS03, Bur02, Hrs09].

Magyarik
[dVP06]. Mail
[ANR01, Cos03, KS00a, Law05, LL04b, NZS05, All06]. mails
[LG09]. Mainframe
[Wes08]. mainstream
[Bj05]. Maintaining
[MJF07, Zho02].

Maintenance
[NABG03]. Maiorana
[Car02]. Majesty
[Bud06]. Majority
[GKK07, SV08b]. Make
[BP06, Ber03, Sin02]. Makes
[Pau09].

Making
[CRSP09, Gar01, Lut03, Mit00, Oec03, Per05, Wri05].

Malaysia
[DV05].

Malaysian
[Kha05]. Malicious
[HLC08, SZ03, YY04, Tsa06]. malleable
[DW09, FF00, PR05]. Malware
[LO07, SZ03]. Man
[Gen04a, Urb01].

Man-in-the-Middle
[Gen04a]. Management
[ACM03a, ACM04a, Ano02d, Ano02e, BP07, BW07, ELvS01, FMA02, GKO4, Gut04b, KB06, Lin00, Sc01, Sha02, TM01, Woo00, Wya02, ASW00, AJS08, AFB05, CG06, Cha05a, GTY08, ISO05, Jan00, JW06, HYM08, KAM08, LMW05, LPM05, LR01, LK01, MKK00, P0t06, RH03, SRJ01, Sen03, UP05]. manager
[KH03, Sha01a]. Managing
[MA00a, MA00b, NDJ01, Oue05, PTP07, PBB02, T0t00, BJ02, Kov03, KH03].

Mandrake
[TvdK*01]. MANETs
[STY07, DF07]. manipulation
[SWR05].

Manuscript
[GG05a, Rug04]. manuscripts
[MA00a]. Many
[BB02, Di 01, MP03, Di 03, SV07].

Many-Round
[MP03]. many-to-one
[SV07]. map
[KJ01, Lee04a, PC05b, SL09]. Maple
[Cos00, TT00]. mapping
[Tan01]. Maps
[BGL03, BMS03, CL04a, LLL*01, WP03, JK01b, MA02]. Maqasid
[MA00a].

Marcel
[Irw03]. March
[BD04, Bir07, Bla03, HR06, PY05, SIL01, Uni00g, Uni00h, Ytr06]. Marian
[Kap05].

Marjan
[BCB*05]. Markers
[FBW01]. Market
[Bar00a, Ano01h, Swi05].

Marketplace
[PLV07, VN04]. Markov
[KW03]. Marks
[Ano01c, YSS*01].

Markup
[Unio0a, Unio0d, Unio0e].

Marrakech
[EE09a]. Marriott
[USE01b, USE01a]. MARS
[BF00a, BC000, Fer00, IBM00, IK00, KS00a, KS00b, KS01, SOTD00].

MARS-like
[BC000]. Mary
[Rec01, Sin09]. Maryland
[ACM05a, ACM05c, ACM09, SIM*09, GL05]. masked
[AHS08, L0u08a]. Masking
[CH02, CT03, GKO2, Lav09].

Massachusetts
[IEE05b, USE01b, USE01a, IEE03]. masses
[Pot06]. massively
[FP00].

massively-parallel
[FP00]. Match
[J00a, WC04, LL06a]. Matching
[ABM08, Len01, UBE09, Voi05].

materialized
[MP09]. Materials
[SLT01]. Math
[SRO6, McN03]. Mathematical
[AUW01, Cas06, FF01b, GL05, HPS08].
Kat05b, You06, GKS05, Sin09].

Mathematics
[BP06, Lew00, Nie02d, Sch05a, Wal00, Gar04, Sch00a, Sch01c, S+03, Sch04a, Sch04b].

Mathématiques [RSA09b, PPV96].

Matrix
[CV03, BF06a, OS07].

Matrices [TL07, CFVZ06, LMTV05].

Matroids
[CDG+05].

Matsumoto [DDG+06, YG01a].

Maximum
[Tro08].

max
[Di01].

maximal
[Huh00, HJW01].

maximizing
[GSK09].

maxims
[Bau00, Bau02a, Bau07].

Maximum
[KMT01, ZC00, DW01].

May
[ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bib03, CC04a, Cra05a, DRS05, IEE01b, Kau02, KN01, MJ04, MS05a, PM00, Pfi01, Pre00, TLC06, Uni00f, Uni00c, YKL02a, Pau02a, YJ00].

Mbps
[LMP+01].

McClure
[Gum04].

McEliece
[CFS01, KI01a, KI01b, LOI00, LS01c, SUN00b].

McEliece-Based
[CFS01].

McFarland
[Car02].

McGraw
[Gum04].

McGraw-Hill
[Gum04].

MD4
[DG02, WFLY04].

MD5
[Eke09, WFLY04].

Me
[ACM03, CB01, LS05, Ver06b].

Mean
[Bar00c, KLML05, Ver06b].

Means
[LMHCETR06, Nis03a].

Measurement
[Ano00a, kio1, CO09b, FXAM04, RW07].

measurement-based
[FXAM04].

Measures
[CB01, Q01, GSK09].

Measuring
[Siv06].

Mechanise
[Bel01].

Mechanism
[LXM+05, WY02, CL08, GH08, LCP04, ME08b, RFR07a, RFR07b, RFR07c, WAF00].

Mechanisms
[ACS02, CJK+04, Her09b, Lin00a, MD04, Mir05, Pip03].

Mechanized
[DH08].

Media
[Hei07, CBB05, Ano02d].

media-streaming
[CBB05].

Median
[Cap01].

Mediated
[DT03, CG06].

mediator
[SBG05].

medical
[AL07].

Medicine
[MYC01].

Meet
[Cia00a, HG07].

meet-in-the-middle
[HG07].

meeting
[Jef08].

Meets
[Way02a].

Melbourne
[IZ00].

Member
[CTH08].

Membership
[NBD01, Fis01a].

Memoir
[Bart05].

Memorable
[KYO01].

Memorandum
[DNRS03].

Memory
[AK03, AJ08, BS00b, CCM05, DK08, DGN03, HNZ02, HBdJL01, KCI+01, Oec03, OT03b, QSR+02, RSP05, YEP+06, CC05d, Has00, Oiw09, Pau02a, ST06, XNK+05, YGZ05].

Memory-Bound
[DGN03].

memory-safe
[Oiw09].

Memoryless
[Sar02].

MEMS
[ECG+07].

MEMS-Assisted
[ECG+07].

Ment
[CAC06].

menu
[Mea04].

Mercy
[Flu02a, Cro01].

Merkle
[CDMP05, JLS03].

Mersenne
[Ano03d].

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

Meshes
[BG08, Lav09].

Message
[BKR00, BR02, BWBL02, BDF01b, CV03, Coc02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SNR04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, MD04, MS09c, Sha04b, TJ03, Wu01, ZF05, ZAX05, ZCW04].

Messages
[Ara02, AR01, BR00b, CJH+01b, DS05b, Sch09, Wri05, Zho06, Alv00, Ano08c, BCG+02, Bib02, BB79, L09, SP79].

messaging
[Opp01, RR05].

meta
[SM08, PLJ05a, QCB05b, Sha05d].

Meta-He
[PLJ05a, QCB05b, Sha05d].

meta-learning
[SM08].

metadata
[CDS07, FJ04].

metamorphic
[CSW05].

Metaphor
[CNB+02].

Metering
[BC04b].

Method
[BTDW01, GHK+06, GL00, Gro01, HRS02, HQ05, JKK+01, LL02, M602, OKE02, OT03a, OT03b, SOHS01, TIGD01, TSO00, WH09, WNY09, ZL05, AMP04, DwWin05, Gt04c, JL03, MSP09, MFK+06, WG02, WWT08, kwpLwW01, WIW04, YC09c, YCL07, CHJ+01a].

Methodologies
[SPMLS02, NdM04].

Methodology
[VMSV05, HM02a, HCBLETRG06].

Methods
[BCDM00, CFFR02, FD01, Kin00, L00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TN00, Vir03, B00, Bau02a, Bau07, G04, BC05b, CM05b, CM06].
GKS05, JZCW05, LMSV07, LFHT07, Mal06, SSST06, Slap99, YV06. Metric [LBGZ01, LBGZ02]. Metrics [LZ01, NP07]. Mexico [Buc00a]. MGC’05 [ACM05a]. Miami [Des02]. Micali [Rub02]. Michael [Ter08]. Micro [ASK07, Eng00, Ste05c]. Micro-Architectural [ASK07]. Microcontrollers [GBK01]. Microelectronics [IEE09a]. Microprocessor [Web08]. Microprocessors [LKM05]. Microscopic [Myc01]. Microsoft [Bon00, Scr01, Ste05b, Weh00]. Middle [Eag05, Gen04a, HG07, Kin01]. Middleware [ACM05a, KRV01, LGS01, MBS04]. Migration [Pat02a]. Mikhailovsky [Puz04]. Million [Ran01]. Mine [For04]. Minimal [FBW01, FGM01, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LPM05]. Mining [LP00, Lut03, HLL02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [CC05e]. MinRank [Cou01]. Minutiae [UBE09]. Minutiae-based [UBE09]. Misbehaving [JQY01, SBB05]. Misinformation [CZB01]. Missed [TvdKB01]. MIST [Wal03]. Mistakes [Ste05b]. MISTY [KYHC01, Küh01]. MISTY-Type [KYHC01]. MISTY1 [BF01a, Küh02b]. Mithra [Fre03]. Mitigating [NLD08]. Mix [JJ00a]. Mixed [SKR02]. Mixes [M03a]. Miyazaki [WHLH03]. MMM [GKS05]. MMM-ACNS [GKS05]. Mnemosyne [RH02, HR02]. Mobile [Cha05a, CFRR02, Dim07, GN06, JP02a, KZ01, KB07, KC02, KHD01, LCK01, Mal02, MM02, PL01, RKZD02, RsS01, RC01, Rot01, SH00, ZY05, CC05c, CJ03b, CF05, CF07, DHMR07, HP00, HY03, shCP09, ISTE08, KVD07, KXD00, LC03, LC04a, Lin07, LKZ04, Par04, Pau02a, SSM08, SL05a, TM06, TW07, Tse07, Wan04a, YC09a, YC09b]. mobile-commerce [YC09a]. mod [TM01]. Modal [GN01]. Mode [BR02, Dwo03, HR03, HKR01, KSHY01, SLG05, WB02, Hey03, RBB03, ZL04c]. Model [Abe01, Abe04, BH05, BPST02, BL02, CLK01a, CS07c, CPhX04, Chi08e, CT09, DPV04, DFSS08, Din01, Din05, ECM00a, Gra02b, HLC08, KLN06, KW03, LJL05, MND04, MNFG02, MR01b, MR01c, MSTS04, Pas03, SA02, Sal05b, Sar02, SFDF06, TZZD05, Vd03, WCZ05, WT02, WvD02, ZGLX05, ZP05, ZS05, BKW03, CUS08, Dar00, DFSS05, GMR08, HLM02, LCX08, LLW08a, LLW08b, MS09b, PS04b, SR01, TP07, DY09a]. Model-Based [Sal05b]. Modeling [AADK05, CDD05, HMvdLM07, KS05a, ZP05, La00, SS04]. modelled [BG08]. Modelling [HCD002, JP07, Puc03]. Models [Ben00, BB00a, LR07, Lin00b, WH09, Cra05b, GKS05, Lin01b, SC02b, vOT08]. Modern [Gol09, Mao04, Pag03, SM07b, Swe08, Bud06, Fur01, IM06, KL08, Mol05, SE01, Lut03, Lee03b]. Modes [DGH04, Dwo03, GD02, Gol01e, HSH01, JMV02, JKRW01, Jun01, KY01a]. Modified [CH04, HPC02, JY01, KI01a, ST02, Che08a, CJT01, HWWM03, LL04a, LL05a, kWPW01]. modifying [CSV07]. Modular [BBP05, BKP09, CMJ03, CH07c, Dhe03, FP00, Gro01, Har06, HGG07, JP03, NSS02, PP06a, PG05, SK07, Ste01, Tan07a, Wal01, WL04a, HSD05]. Modulation [AS01c, Che07]. Module [Ane02d, LM00, SGM09, ARJ08, BG09, Jan08b]. Modules [FIP01b, NIS01b, GJJ05, JEZ04, SE00b]. Moduli [Ba01b, GMP01b, WJ01]. Modulo [AC02, Gou06, Gro03, MFFT05, Zhe01, Wan05]. Modulus [An01k, CGH00a, CD00, SZ01, W02, WS02, KLYL00, WWTH08].
[CMJP03, KWP06, RMH03b, WS05, HGNS03, RMP08, RMH03a]. Multiply [KTT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver [HSZI01]. Multiresolution [hKLS01, YPSZ01]. Multiset [aSM01]. Multisignature [Tad02, CWH00, CL04c, CLZ02, Dim07, FBWC02, Gum04, Har05a, IKY05, JYZ04, KKG03, KPS02, Ken02b, LMP+01, Lu07, Mal02, NN02, PZDH09, PZL09, Po03, RCBL00, RC05, Sty04, TLYL04, VMC02, YC01, ZYH03, ZS05, Bru06, CJ03b, CMS08, Coc01a, DWML05, GKS05, HLL+02, LC03, LPV+09, MW06, ME08a, MSK03, Mi08, Pri00, RAL07, Sch00c, Sta02a, TIS07, Vac06, Wy05, YLT06, ECM00a, ECM00b].

Network-Attached [RCBL00]. network-based [HLL+02]. Networked [Sch00d, LB05]. Networking [ACM01b, Ros07, VM03]. Networks [AEAQ05, BJLS02, CGM07, DBS+06, Fin06, GPCS08, Gor05, JKRW01, KZ01, Ken02a, KH05, LNL+08, NABG03, PR01, RKZW02, Sin01a, WT02, Zea00, ZYN08, ZWCY02, AJS08, Asl04a, BBG+02, BC05c, CCMT09, CGP03, CBD+05, DHRM07, ETMP05, HJ07, HMvdLM07, JRR09, KXTZ09, KHYM08, KB09, KVD07, LDH06, LHC08, LW05a, LLH06, Lin07, LN04, Lop06, LKZ+04, MWS08, MJF+08, MS09b, NC09, NLD08, PCSM07, PS08a, Pat02b, SLP07, SS+08, TP07, TM06, TCR03, TW07, WDLN09, XwWL08, YC07, ZSJN07, ZBLvB05, Ano03d, 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, Panu02a, Panu02b, Panu03, Panu09, Pri00, CAC03, CAC06, Sta05, Raj06]. Newton [KT06]. Next [ESG+05, McL06, TV03, Van03, Web08, BD04b, ISTE08, RR03a]. Next-Generation [ESG+05, Web08]. NFA
NFS [Sta02b]. Nice [DS06, JJ00c]. Nicko [Ant03c]. Nimbus [Fur02a, Mac00]. nine [Tat05]. Ninth [USE00d]. NIST [BG07a, Dra00, Hir09, Kel05, RRS06, SF07]. NIST-Recommended [Kel05]. NMAC [RR08]. NMAC/HMAC [RR08]. NNAF [DwWmW05]. No [Sta05, Sty04, Uni00g, Wei06, Wei05, CC05b]. Nobel [MNT+00]. Node [BRTM09, Fox00]. Nodes [ZYN08, RAL07]. NOEKEON [DPVR00]. Noise [BKW03, GA05, MPSW05, SDMN06, MS09a, PC00]. noise-based [PC00]. Noise-tolerant [BKW03]. noisy [HGNS03]. Nominative [PL01]. Non [BR05, CHK05, CZB+01, DN00a, DDO+01, DW09, FF00, Fis01b, Fis05, FGM00a, FGM00b, HNZI02, HJW01, IYK02, IYK03, JT01b, Kos01c, KO00, MSTS04, Nie02b, PHK+01, Pas05, SPK08, WBL01, DM07a, DS02, Huh00, HLL04, IM06, KKL09, KHL09, LSA+07, PR05, RP00, RFR07a, RFR07b, RFR07c, SC05c]. Non-adjacent [JT01b]. Non-committing [DN00a, Nie02b]. Non-Cryptographic [WBL01, IYK02, IYK03]. Non-injective [Kos01c]. Non-interactive [CHK05, DDO+01, Fis01b, Fis05, HNZI02, HJW01, MSTS04, Pas05, KKL09, KHL09]. Non-interference [BR05]. non-intrusive [RFR07a, RFR07b, RFR07c]. Non-malleable [DW09, FF00, PR05]. Non-maximal [HJW01, Huh00]. Non-OOSD [CZB+01]. non-perfect [DM07a]. non-physicists [RP00]. non-quantum [IM06]. non-repudiation [HLL04, LSA+07, SC05c]. Non-trivial [KO00]. Non-Uniform [SPK08]. nonce [CY05, LKY05a]. nonce-based [CY05, LKY05a]. Nonces [BR00a]. Noncontact [Sak01]. noninterference [DFG00]. noninvertibility [HRS08]. Nonlinear [BP01a, BI05b, CV02, Che01c, LBGZ01, LBGZ02, SM00a, ZC00, BGPGS05, CFVZ06, KH08]. Nonlinearity [SM00b]. Nonmalleable [ABW09, DDN00, DDN03, PR08]. nonrepudiable [TYH04, YTH04]. nonrepudiation [HW05, OZL08]. Nonsecurity [Sch07]. Nonuniform [CU01]. Normal [Ran55, Ran01, GPS05, Mic01, RMH03a]. Normalization [VK07]. Norway [Ytr06]. Nose [Fox00]. notarization [LG04]. Notarized [GT05]. Notation [Eag05, Kin01]. Note [CWY05, FS02, GMP01a, GIS05, KCP01, Ros00, MF07, PC05b, Yan02, Zha06]. Notes [KSF00]. Nothing [Des00c, SR00]. Notions [BPS00, BN00a, CK02b, DKMR05, HU05, Kos01a, Des00a, KY00, PS04c]. Novel [BBC+09, CC02a, CYH01, CDTT05, CW09, HC08, MP01c, WC09, AJ08, BG08, CCS08, DSGP06, GB09, HG05a, SPG02, SCS05a, mSgFtL05, WC05]. November [ACM01b, ACM05a, BZ02, CKL05, Eke02, IEE00a, IEE02, Lai03, LL03, LL04c, MS05b, PK03]. novice [Dew08, Gou09]. Novo [B109]. NP [AGGM06, FS08, HN06, AGGM10]. NP-hardness [AGGM06, AGGM10]. NPCryptBench [YLT06]. NSA [RC05]. NSF [Han00]. NSS [GJSS01, HPS01]. NT [Str01b, USE00a]. NT/2000 [USE00a]. NTRU [GJSS01, GS02c, HPS01, HHGP+03, HGNP+03, HG07, JJ00b, NP02b]. NTRUEncrypt [HG06, KY09]. NTRUSIGN [HHGP+03, HH06, WH08, ZJ09]. NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Dic03, DGP07a, DGP07b, DV08, Eag05, EHK+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05, Ke06, KM01b, LMHCETR06, LNS02, MN01, NR04, RSN+01, SP05, Sch06b, Shp99, Shp03, SFDF06, TNWA08, TL07, TTT09a, TTT09b, Vav03, Wal00, Yan00, YKLM02b, Aam03, AUW01, BK07, Bel08, BGPGS05, ...
BG08, BG09, BG07a, BGL +03, CNPQ03, CO09b, DIM08, DGP09, FP00, HG05a, HGNS03, HlwWZ09, HP01, JAW +00, J03, KH08, KS00, Kin01, Lam01, Mit00, Nie02a, Nie04, Pan07, PSG +09, PSP +08, PC00, RGX06, Sho05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Wag03, Was08b, YZEE09].

Number-Notation [Eag05, Kin01].
Number-theoretic [NR04].
Numbers [HSR +01, HBF09, Ifr00, MN01, ST03b, AG09, HW98, KB39, Kir01b, MFK +06, SS03, Shp05, Tip27].
numeric [AKSX04].
Numerical [WWL +02].
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 [BG1 +01].
Obfuscatiion [CT02].
Object [RSA00e, DHL06, MWM01, ST06].
object-oriented [DHL06, MWM01].
Objects [CCM05, ZTP05, P301, Whi09].
Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GKM +00, KKL09].
ordinance [MN03].
Observability [JQY001].
observers [JL04].
Obstacles [KM04a].
Obtaining [Bar06b, BP03b].
OCB [RBB03].
occur [Web02].
Ocean [MYC01].

October
[AJ08, BD08, CKL05, IEE01a, IEE03, IEE04, IEE05a, IEE06, IE07, IEE08, IE09b, KCR04, LST +05, TT01, USE00b, ZHY03].

Octopus [Cla00b].
Oded [Lee03b].
Odyssey [Gol08].
Oedipus [Lav06].
Offering [AJ08, Coc02b, Oec03, Shi05, YLL02, Bau05].
Off-Line [YLL02, Shi05, Bau05].
Offering [YC08].
Office [Uni01], office [Kov03].
Official [BP01b, Coc02b].
Offline [DJ06, ST01b, VW01].
Ofs [PS01c].
OH [BD08].
oil [RD09], old [Lov01].
On-Demand [SEF +06].
On-Line [Lu02, BCS02, Luk01].
One [AK02a, BYJK08, CHL02, Che03, DIS02, Di 01, DW01, DMS00, Fis01b, GKK +09, HNO +09, HM02b, HR05, KI01a, KO03, KO00, LTW05, LDM04, MLM03, PV06b, PG05, PLJ05b, RR02, Sho00a, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YZ00, YKLM02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, DI 03, DS02, GKK +07, HR07, HRS08, HLTJ09, JZ09, KKK05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, Tsa08, YW05, YRY05b, ZW05a].
One-Time [HM02b, LDM04, RR02, CCK04b, DS02, HLTJ09, LC04a].
one-variable [SV08a].

One-Way
[BYJK08, CHL02, DMS00, Fis01b, GKK +09, HNO +09, HR05, KKK05, LDM04, Sho00a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CCK04b, CHY05b, CJ04, CC05d, DI 03, DS02, GKK +07, HR07, HRS08, JZ09, KKK05, KK03, LW04, LPM05, LQ08, LC04a, Mic02a, Poi00, SVDF07, SV08a, SW05, Tsa08, YW05, YRY05b, ZW05a].
One-Wayness [KI01a, PV06b].
Ongoing [Sam09].
Onion [CL05].

Online
[BDF +01a, BBKN01, Fis05, LCS09, Ort00, Rey01, ST01b, VAVY09, Vo05, FNRC05, Fox00, Pan07, Tyn05, PT08].
Online/Offline [ST01b].
 Only [BBK03a, CF01b, GL01, Hoe01, VV07, BCDM00, FKS +00, GHJV00, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Wan04b, Yas08].
Ontario [HA00, ST01d, YY01].
OOSCD [CB0 +01].
OOSD [CB0 +01].
Open [Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, Kuis02, Lin02, Mea01, PM00, VDKP05, An03c, ETMP05, McA08, Bar00b, Lin02].
Open-Ended [Kuis02].
Open-Secret [Joh05].
Open-Source [Bau02, Gut00, McA08].
OpenCard [HF00].
Opening [CAC03].
OpenSSH [Bau01c, Sta02b, TvdKB +01, Hos06a, Mos06].
OpenSSL [Fri01, Res01a, Res01b, Sti06a,
VMC02, YRS+09, Bel08. Operating [BCST00, DGP07a, DGP07b, IEE01b, SR01, CGL+08b, CGL+08c, DGP09, KWD06, MPH06, TKP+08].

Operation [BR02, BKMO, Dwo03, EP02, Gol01e, HSH+01, JKRW01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BKMO]. Operational [BR02, BKM07, Dwo03, EP02, Gol01e, HSH+01, JKRW01, KY01a, Bud00b, RBB03, Win00]. Operation-Centered [BKMO].

Operators [CH00]. Opinion [BHM03, GS07b, Lan00c]. Opponent [Cos03]. Opportunities [CWR09]. Optical [Kuh02a, Pau02b]. Optimistic [CC00, DLY08]. Optimization [Ken02a, Kre05, KY01, SMTM01, TLY04]. Optimized [LC03]. Optimising [Dwi04]. Optimality [NK06]. Optimised [TL07]. Optimistic [CC00, DLY08]. Optimization [Ken02a, Kre05, KY01, SMTM01, TLY04]. Optimized [LC03]. Optimising [Dwi04]. Optimality [NK06]. Optimised [TL07].

Order [AKSX04, Bai01a, CV02, KCP01, Kra01, Luc02b, NNT05, NM09, Sty04, Tad02, Zhe01, BF01a, Cole03]. Order-Specified [Tad04]. ordered [HY03, WL05]. Ordering [Mea04]. Orders [HJW01, PS02b, HM00, Huh00]. Oregon [CHH01]. Oregon [ACM00, BCDH09].

Organization [JG07, MMZ00, MP00, C+02]. Organizational [PPT07, BJ02]. organized [AUW01]. Oriented [HR00, LYL+01, SKU+00, ZCC01, CHC05, CJWT01, DHL06, HWW04, LL06, LWZH05, MWM01, Sae02, Sha03c, TJO1a, 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 [HTLJ09]. Other [BF05, Ngu05, Wri05, Cla00b].

Otherworldly [MYC01]. Ottawa [AMW07, MZ04]. our [Sta05]. ourselves [Fur05]. Output [Dic03, YJO0]. Outsource [HL05a]. outsourced [MSP09, MNT06, YPPK09, YLCT+09]. overcoming [CHC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, Ino05]. overhead [HGR07, 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 [BRTM09, STY07, WN02, YLR05]. P2Ps [LHL+08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. PACA [Art04]. Package [Win01]. Packed [LH07]. Packet [BR09, WRW02, WLZZ05, BC05b, CMS08]. Pad [LDM04, DS02]. Padding [AR01, BCCN01, CKN00, CJNP02, KO03, LS01a, Man01, Vau02]. Paddings [NP02b]. PadLock [Lud05]. PadLock-wicked [Lud05]. Page [IEE00b]. PageRank [GPC08]. pages [Fal07, Rot07]. paging [SZ08]. Paillier [CGHG01, DJ01, NSNK05, ST02]. Pair [WCJ09]. Pairing [BKL02, BF01b, BF03, CHSS02, GSP06, HCD08a, HCD08b, KM05, Kir03, PV06a, SKG09, Sma03a, GPS05, Lee04a, PC05b, VAY09]. Pairing-Based [BKL02, GSP06, KM05, PV06a, HCD08a, HCD08b, GPS05]. Pairings [Bon07, BGH07, Jou02, SB04, ZK02, CJL05, DSGP06, LWZH05, LC05b, SW05, VK08].
pairs [LYGL07, Slp01]. Pairwise
[CLL00, 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, SI01, AMW07, A.J01a, Bir07, BC05c, C05, CKL05, DR05, HH04, HH05, PC05a, PW05, WK06, Wir03]. Paradigm [BN00a, CS02, Go03, KD04, YC01, BKN04, Can01a]. Paradigms
[Des00b, Swa01, Hro05]. Paradox
[Che01b]. Paradise
[USE00b]. Parallel
[APR08, App07, AERM09, CPH04, CTL01, CNPQ03, CNB+02, Dan07, DM00b, JL08, KY02c, Lin01c, MFS+09, PS04a, RMH03b, SS01a, BF06a, FP00, OS07, RMP08]. Parallelism
[KVN+09]. Parallelizable
[BR02, Mio02]. parallelizing
[LKKY03a, LKKY03b]. parameter
[Wue09]. Parameterizable
[KPMF02]. parameterization
[LZP+04]. Parameters
[ZL02]. Parametric
[Vir03]. Paranoïd
[Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Lu06]. Parascript
[Ano02d]. Parasitic
[ETZ00]. Parents
[Pau02a]. Parents-to-Be
[Pau02a]. Paris
[ACM04a, GH05, KNP01, NP02a]. Parity
[DR09, KKG03, Y01, BKW03]. Parity-Based
[KKG03, DR09]. Paper
[Cop05, Cop06, HS01a, Sal00b, Sal05a, SE01, Smi01b, Wei06, Win00]. Part
[Har01a, Har01b, ISO04, ISO05, Puc06, TR09b, Can06a, SK01b, Bau01a, Bau01b, Bau01c, Bau03b, Res01a, Res01b, Wac05]. Partial
[BM03b, Cor02, Her06, ABHS09, CP07]. Partial-Domain
[Cor02]. Partially
[A000, MSP09, Bao04, Bau03, HC04a, HY03, HLL03, WL05, WLHH05, WY05, ZC05]. Participatory
[CTA+01]. parties
[LKY05b]. Partition
[CH08, WJP07]. Partitioned
[DN04]. partitioning
[BF06a, Che07]. partitions
[Sav04]. Party
[K004, Lin01c, MR01a, WW05, WV01, CLOS02, CLC08, CDM00, CDG+05, FGM01, FWW04, 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, Jab01, KOY01, LSH03a, LSH03b, MP00, Mac01, MSJ02, Ngu05, SBEW01, SY06, WHL05, YS04, ZWCY02, CC01a, CC04b, CCK04b, CYH05, DG06, FLZ02, Fur05, GL06a, HTJ08, JM07, JPL04, Jua04, KLY03, KJY05, KTC03, KLC03, Ku04, KCC05, KHKL05, LL06, LFW04, LH03, LC04a, Pha06, Sco04, SLH03, Sh05, WLT03, XWL08, YW04a, YC05, YS02, YPKL08, ZDW06]. Password-Authenticated
[BMP00, DG03, KOY01, MPS00, Mac01, MSJ02, Ngu05, DG06, HTJ08]. Password-Based
[CPP04, CS07b, GL03, SBEW01, SY06, YS04, GL06a, KHKL05, Pha06, ZDW06]. password-guessing
[Shi05]. Passwords
[GL01, KOY01, Per03, Smi01c, An003c, FZ06, KOY09, NS05a, RD09, YWWD08, VOT08]. Patarin
[Bih00]. Patent
[MP00]. Path
[GXT+08, CCD+04, Dew08, ZSN05]. path-based
[CCD+04]. Path-quality
[GXT+08]. Pattern
[ABM08, BDhKB09, BLP06, BCCN01, LS01a, TIGD01, Buh06, LYGL07]. Pattern-based
[BLP06]. Patterns
[DD02, MP06, WCJ09, jLC07]. Pavol
[Sala03b]. pay
[Joy03a]. pay-as-you-watch
[Joy03a]. payload [KC09a]. Payment
[MV01, RMCG01, YKMY01, Has02, HP00, SH00]. PC [BSW01, Ste05c]. PCIXCC
[AV04]. PCKS#7 [Dav01c]. PCPs [FS08].
PCs [BDET00]. PDA [GWO0]. PDF
[ISO05, CNB+02, ISO05]. PDF/A [ISO05].
PDF/A-1 [ISO05]. Pearson [Puz04].
Pecking [DNW05]. Pedersen [GJKR03].
Peer [Art04, HR02, RH02, AT04, LLY06, MHPD06, PI06, WCJ05, YI04].
Peer-assisted [Art04]. Peer-to-Peer
[HR02, RH02, AT04, MH06D, PI06, WCJ05]. PeerAccess [WZB05]. Peinado
[YRY05a]. PEM [Dav01b]. Penguin
[Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Guo05, Ou05, Ste05a].
Pennsylvania [IEE05a, IEE08]. People
[ASW*01, CGO5, Lov01]. perceptions
[VJC09]. Perceptual [BM07].
Perceptually [EFY*05]. Perfect
[AJO08, CL00, DNB02b, DSS01, Sun00a, DM07a, SC02c, SY06, ZD05]. Perfectly
[DMS00, KSR02, SN04]. Perform [Kin00].
Performance
[ACM01b, BH00a, DPA01, Dra00, EYC000, FZH05, Int00, Ken02a, Ken02b, Kra05, LMK00, MM01b, NFQ03, PWG03, PBTW07, SKSS00, SW00a, SB01, Siv06, SL00, SGPH98, WBRF00, WWC00, WS02, XH03, YEP*06, Zaa00, AKNR04, BVP*04, BZP05, CKL*09, CRSP09, GC00a, HM02a, JRB*06, LW05a, NWT07, SK03, YGZ05]. performance-friendly [CRSP09]. periodic
[XQ07]. Periods [KKH03]. Perl [Sal03b].
Permutation
[DMS00, HSR*01, IYK02, KKG03, K003, LS01, DP02, IYK03].
Permutations [BPR*08, CHL02, KO00, MP03, KKKP05, WV00]. Persistent
[AGT01, ST06]. Person [KJR05, LLT*04, PK01, BS01b, KN03, LI05, LST*05, PY08].
Personal [Bar05, EHMS00, SEK01, SEK02, Tyn05, UP05]. Personalised
[TNG04]. personalized [GPC08]. Perspective
[LL01]. Perspectives [BMV06, SM08].
Perturbation [HWH08, ZY08]. Pervasive
[BDKB09, JW05, LKHL09, Lu03, Lu03].
PET [MS05a]. Peter [Fou04, Uze04].
Petersburg [GK05]. petitions [Cal00b].
Petri [LKJL01, AADK05]. PGP
[MCL06, A00h, B00h, D01b, D01c, JKS02, Luc06, Op01]. PGV [BRS02].
Pharaohs [Pin06]. Phase
[CDF01, Ig02, KL*02a, Che07, Che08a].
Phase-Conjugate [Ig02]. phase-shift
[Che08a]. Phil [Bar00a]. Philadelphia
[IEE08]. Philip [McL06]. Philosophy
[Cop04b]. phising [Bai04]. Phone
[CAC03, Fox00]. Photonic [TW08].
Photonic-based [TW08]. Phots
[Bar00c]. Physical [CGMM02, LR07, YKLM02a, GVC*08, UHA*09]. Physicist
[BZ02]. physicists [RP00]. Physics
[MYC01, Sch06b, B00, B01, DU03].
physiological [RFR07a, RFR07b, RFR07c].
Pi [OS08]. PIC [Fou02]. pick [Cla00b].
Picks [PM00]. PicoDBMS [BPVB01].
PicoDMBS [BBPB00]. Picturing [Pau03].
Piecewise [LL*01]. Pigeon [Pen01b].
piling [Kuk01]. piling-up [Kuk01]. PIN
[BZ03]. Pioneer [Coc03]. PIPE [CBD*05].
Pipelined [MD05, Mis06]. PIR [BIM00].
Pirates [KY01d]. PISN
[EC00a, ECM00b]. Pittsburgh [IEE05a].
Pixel
[LS08, WCJ09, BCD06, YL07, WW08]. pixel-pairs [YL07]. Pixel-Value
[LS08, WW08]. PKC
[BDZ04, Des02, Kim01, NP02a, Vau05a, IZ00, KO1a, KO1b, ZC04]. PKC'98
[HPC02]. PKCS
[Chu03, Man01, RSA00c, RSA00b, RSA00d, RSA00e, RSA01, RSA02, RSA03b].
PKCS#1 [CNP00]. PKCS#11 [DK08].
PKCS#7 [Dav01b]. PKI
[AL06, CZ05, KGL04, Ahm08, ES00b, ES00a, Gar03a, Gut02a, Han00, Hoo05, ND01, Ort00, St.00]. PKIX [FL01b].
PKP [JL01]. PKWare [Bar00a]. Place
RD01, Roy00a, SMP +09, ST01d, VY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BDZ04, BS01b, Bih03, BCDH09, BD08, CC04a, CV04, Clhr00, Des02, DFP06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE04, IEE05b, IEE07, IEE08, IEE09b, JY040, Jf08, JM03, Joy03b, JQ04, KJR05, KLG04, Kim01, Kim02, KN03, Kn02, KP01, KNP01, KM07, Lai03, Lee04b, LTT +04, MMV06, MJ04, May09, MS02c.

Proceedings [Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sma05, Syv02, TB03, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZYH03, BCKK05, Cra05a, DV05, DWML05, DUK05, GKS05, IKY05, Kitti05, Li05, LST +05, Men07, Po06, Sho05a, Son00, dCdVSG05].

Process [Kwo03b, MNT +00, BDFP02, HL06, MRST06, VKS09].

Processes [BDP02, ALV02, BDNN02, Wh01].

Processing [ISSZ08, KLB +02b, PCK02, AA08, AA04a, Aye06, YPSZ01].

Processor [An02a, BBGM08, EP05, FFWC02, FZH05, GC01b, Int00, KBD03, KPMF02, TYLL02, ST03a, SHL07].

Processors [TLYL04, CW02, CRSP09, Geb04, L05a, YGZ05, YLTI06, ZYLG05].

Procurement [Lad06]. produce [Zir07]. producing [SOIG07].

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

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

Profile [PJJ00, R00a].

Program [H050, Bec02, GGH +08, Kov03, KH03, CS08b].

Programmable [Dam07, GC01a, HV04, S002].

Programmer [Wil01b, Bon00, Che00, DKK07].

Programmers [Coc01a, Wei04, Gou09].

Programming [ASW +01, An02d, Coc03, LMHCTR06, Res01a, Res01b, Swa01, Uri01, AJ01a, AJ01b, CW07, Nis03a, VM03].

Programs [BGI +01, Ark05, SLTB +06].

Progress [KK06, KFSS00, RD01, Roy00a, CV04, DV05, JM03, MMV06, MS02c].

Project [Fri01, IY00, MNT +00, Pau02a, Salxx, Gou09, LR01, Lov01, MMW01, Sha01a, Coc01a, Coc02b, IY00, Pre02b].

projects [Gha07].

Promises [An02f].

Promote [WK05].

Promotes [Bar00b].

Prone [MLC01].

proof-of-compliance [LMW05].

Proof-of-Concept [ARC +01].

proofing [CT02].

Proofs [BBM00, BP02, CS02, DFS04, DNV05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nic02b, BGB09, BR04, Go099, HG05b, SV08b, dH08].

Propagation [LJL05, QPV05]. Properties [ABC +05, BM01c, KY01b, LLL +01, MS02a, NNT05, SM00a, BD04a, CDL06, FGM03].

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

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

Protect [ETZ00, BBN +09, WK05].

protected [CYH05, PKH05, ZCL05].

Protecting [Des00c, EHMS00, KY01d, Kra01, LKM +05, LW05b, ML05, NN03, Sha01c, vW01, Bro05b, LJY04, LS05b, ZYLG05].

Protection [CGJ +02, DKFX05, ECG +07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL +08a, CGL +08b, CGL +08c, CRT02, Gor05, HLC07, KA09, KVO3, KH03, Kwo03a, LL05b].

Protection [JT01a].

Program [An01a, Bel01, BPS02, BL02, CK02a, C030d, CW05, Cin02, ECM06b, Fre03, GJKR03, GL00, HS07, JP02b, JRF01, JT05, KKL +06, Kak06, Kra05, Ku02].
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, CL08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, GTZ04, HTJ08, HWWM03, HLJT09, HHC05, HK08, 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, BDS08, BFGT08, BP05, BLP06, BD04a, BR05, Can01a, Can06a, CP07, CKRT08, CWJT01, CH07a, Cho08b, Chr00, Chr01, CJ00, Coh03, CC05d, CDL06, DFG01, GJ03, GJ04, GUQ01, Gut04c, HM02a, JW01, KS05a, LPV09, LLL04, LL06, LLS09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SV08a, SL05a, SR00, SW00b, SY06, WHL06, YS04, ZLX99, ZL04b, PDS09, Puc03].

ProtoMon [JT05]. Provability [GOR02b].

Provable [AI00, ACJT00, BMP00, BC01P, BCP07, CHKO08, DG03, DG06, HL:AV02, HvAL09, HL07, HS07, JMV02, Mi03a, NSN05, NSS02, VMSV05, WHL06, XS03, ZCL05, BKN04, CCMT09]. provenance [HSW09]. Provers [MV03a]. Provide

[AB01, Sch01a]. Providence [IEE07, Sil01].

Provider [LDM04, HLM02]. providers [MV03b]. Provides [OT03b]. Providing [BACS02, BDS09a, DeL07, Lin07, Par04].

Proving [Che03, FS01c, GN01, Tee06].

Provision [Kha05]. Proxy [AH05, BCL05a, DKFX05, LCK03, LCZ05b, PL01, RdS01, Sha03d, ZJ09, AFGH06, CCH04, DY09a, HWW03, HW04, HWW05, HW05, HC04b, KHL09, LL05b, LL05b, LCZ05c, LW05c, PKH05, Sha05b, SHT05, TYH04, YTH04, ZCL05]. proxy-enabled [DY09a]. proxy-protected [PKH05, ZCL05].

PsBGp [vOWK07]. Pseudo [BH05, FWW04, Gen00b, LLL01, LHL08, MP03, SX01, TZT09a, TZT09b, WP03, BG09, GB09, MKF06, NR04, PSP08, RGX06, SL09, WW08, YZEE09].

Pseudo-Random [LLL01, MP03, WP03, Gen00b, SX01, MKF06, NR04, RGX06, SL09, WW08].

Pseudo-Ransom [BH05].

Pseudo-signatures [FWW04].

pseudonoise [HG05a]. pseudonym [CG06]. pseudoprimes [ZT03].

Pseudorandomness [CD01, DN02a, DJ05, DP02, Fin06, Flu02b, FIPR05, GM02a, IYK03, KSF00].

pseudorandomness [GM02c, IK00, KY00, LH01, Lee03b, MV00, Shp03, Go09]. Psychology [MYC01].

PUB [Nat00]. Public [ANS05, AW001, APV05, Ano01j, AEAQ05, AF03, BC05a, BG0401, BDZ04, Bar00c, BPS00, BMM0, BBDP01, BLM01, Bih00, BDTW01, BST02, CHK03, CHK05, CD05, CHM02, CHK08, CJ03c, Choi08a, CCW02, CT09, CCM01, CS02, CS03b, DP04, DJ01, Des02, DY09b, DKXY02, DF03, ES05, ES00a, ED03, FL01b, GMLS02, GH01, GC01b, GSB04, Gut04b, HCDO02, HR05, HG05b, HR04b, HJ01, HLC08, IEE00b, IZ00, Jou02, Kat05b, KKIM01, KM01a, Kim01, KLY02, KXY02,
KY02c, KLC+00, Kl01b, KM04b, Kos01a, Kos01b, KOMM01, KY01e, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Mö03a, Mol03b, Mü01a, NP02a, NBD01, NSS02, OTU00, PHK01, Pei09, PR01, PHM03, Qu01, RSA00a, RKZD02, ST01a, ST02, Sin01a, Sni01c, Ste01, TS000, TT01, Vau05a. **Public**

[WZW05, WHI01, WV00, Wya02, YKMY01, YG01c, YDKM06, Zhe02a, AG09, BHM03, BCL05a, BCW05, BBN09, Ben01a, BB79, Bra01a, BD04b, Cal00b, CCT08, CL02b, CWH00, CCH05, CJ05, CKRT08, Cho06, Cre00, DMT07, EKRM01, 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, LKY05b, LCK04, Lin01a, LLW08b, LS01c, Lop06, LWK05a, MWS08, Mü01b, PI06, PC09, SN00, SRJ01, Sha04b, Sha05b, Shp04a, SLC05, Sun00b, SZP02, SC05c, TO01, TLH05, Tsa05, TJC03, VS01, WDL09, War00, Wu01, WH03, WL04b, hY08, YRS+09, ZM05, AL06, BDZ04, Ben02, CZO5, Des02, GL05, KLG04, Kim01, NP02a, Vau05a, YDKM06.]

**Public-Key**

[Ano01j, AEAQ05, BC05a, BNM00, BBPD01, BL01, BST02, CHK03, CHK05, CCM01, CS02, CS03b, DPV04, DJ01, DFK+03, ESG+05, ES00a, FL06, GHW01, GC01b, HR05, IE00b, Kat05b, KK01, KM01a, KLY02, KLY02c, KLC+00, Kl01b, KM04b, Kos01a, Kos01b, KY01e, Kur01, LP03, Lin03, Lin00b, MR01b, MR01c, Mö03a, Mol03b, Mü01a, NP02a, NSS02, OTU00, POI02, RSA00a, ST01a, ST02, SIN01a, TS000, TT01, WHI01, YDKM06, AUW01, ED03, HG05b, Pei09, BH03, BBM03, BBN+09, BD04b, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HHG06, Iwa08, Jan08b, JXW05, JZCW05, Kos01c, LF03, Lin01a, LS01c, Lop06, MWS08, Mü01b, SN00, Shp04a, SLC05, Sun00b, TO01, ZSM05, GL05.]

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

**Publication** [Top02, DGMS03].

**Publications** [Bee05].

**Publish** [SL05b].

**Published** [RSA09a].

**Publish-subscribe** [SL05b].

**Q** [BFMR02, CH01b].

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

**QCQC** [Wil99].

**QCQS** [Wil99].

**QDSL** [CUS08].

**QNX** [Ano02d].

**QoS** [JKRW01, ZEA00].

**QoS-aware** [ZEA00].

**QSIG** [ECM00b].

**QSIG-WTMAU** [ECM00b].

**Q'tron** [YC07].

**QUAD** [BGP09].

**Quadratic** [BT02, Coc01b, HJW01, SP05, CCS08, HM00, Hieh00, HP01, LD01].

**Quality** [BW07, TL07, DMSW09, GT+08, KC09a, WWII08].

**quality-conscious** [DMSW09].

**Quantifier** [KS06b].

**Quantifier-free** [KS06b].

**Quantitative** [Bai08, ME08a].

**Quantization** [DRL09, WC04, WC05].

**Quantum** [AC02, ATSVM00, Ano02f, Ano02g, Ano02h, BYJK08, BOHL+05, BB09, BB02, BBB+02, BL03, BM00, BM+07, Coc03, DFS04, DPO5, DFSS08, DMS00, ELL04, Ett02, GKK+09, GH01, GW00, GRTZ02, HG09, Hay06, Im03, Ina02a, Ina02b, Kak06, KK06, KLB+02b, LB04, LW50b, NA07, OTU00, PC09, R01, RK05, Ser06, SR07, TO01, Witt99, Wii00, Yi00, Yi01, ZL01, ABW09, Ano03e, Ano06d, BYJK04, BCG+02, Ber09b, BEZ00, BEZ01, BLRS09, DFSS05, Duw03, Eke02, GKK+07, Gav08, HHH06, IM06, JZ09, JRS09, JAW+00, Joy00, KK07, KH08, KKKP05, LQ08, May01, NK06, P06, RP00, Sin99, Sin00, Smo04, UHA+09, BB02, BD08, BB09].
quantum-storage [DFSS05]. quarter [Kob00]. quarter-century [Kob00].
quarters [Cla00b]. QUARTZ [PCG01]. Quasi [MD05]. Quasi-Pipelined [MD05].
Quasigroup [MSNH07]. Québec [ACM02]. Queen [Ree01, Sin99]. Queenstown [Zhe02b].
queries [CKK03, Fis01a, GPC08]. Query [GA03, PT08, PCK02, BKW03, PM08, YLC+09].
Query-preserving [GA03]. querying [FJ04, ¨UG08]. question [OC03]. Questions [Ett02, Joh00, Jac00].
Queues [WWL+02]. queuing [CUS08]. quick [Dew08]. R [Kat05b, Pag03, Spr03, Bih00].
R&D [Mau05]. Rabbit [BVP+04]. Rabin [Bon01, Gen04b, Miy01]. Rackoff [MP03, Pat03a].
Radiations [SGM09]. radical [Web02]. Radio [Sak01]. RadioGatún [BDPV09].
Radix [HKA+05, JY01]. Radix- [HKA+05, JY01]. rails [Fox00]. Rainbow [DS05a].
Raises [MP00]. Raising [Cos03]. ramp [Y06]. Rampaging [Coc02b]. Random
[Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CTY09, Chio8c, Dico3, DGP07a, DGP07b, DV08, EHK+03, Gra02b, GPR06, HSR+01, HB09, Int03, JRR09, Kel05, LLL+01, LM02, Lys02, MP03, Mir02, NNT05, Nob02b, Pas03, Pat04, Ran55, Ran01, RSN+01, SFDF06, TWNA08, TL07, Tip27, TTT09a, TTT09b, Vav03, VKS09, WP03, BK07, Bel08, BG08, BG09, EG07a, BGL+03, CJL06, CO09b, DGP09, Fis01a, GVC+08, Gen00b, GB09, HG05a, HLWZ09, HMvLM07, JAW+00, KH08, KB39, KG09, MI09, MFK+06, NR04, Pan07, PSM+09, PSS+08, PC00, Reg05, Reg09, RG09, RGX06, SS03, SXY01, SR07, SK01b, Sug03, SL09, UHA+09, WW08, YZEE09, BH05].
Random-Error [LM02].
random-self-reductions [Fis01a].
Randomats [Sam01]. randomization [WHH05]. randomization-enhanced [WHH05]. Randomized [Sem00, Hro05].
Randomness
[DD00, DD04, DGH+04, FWW04, Gen06, HSS04, JG01, KL09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN+09, DOPS04, Kat05a, KW00, RSS04, SU07, Sug03].
Range [CW09]. Rank [Sun00a, DW01, Sim02]. Ransom [BH05].
Rao [Zyr01]. rapid [OP01b]. Rate [KT01, Lz09, PS02a, Sun02]. Rates [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+04, JBR05, SP05, Sta05, YKMB08, GM04, HP01, Lie05, SL07, SGP08, YZDW07]. Real-Time
[Dri02, GM04, YZDW07]. Reality [Coc01a]. Really [CZB+01, Wei00, Dav01c]. reap [Ch00]. reason [Lau08b]. reasoning [IK03, IK06]. Rebalanced [SWH+09].
Rebalanced-RSA [SWH+09]. rebels [Lev01]. Rebuild [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, LTT+04, LST+05, TTT09b, HS02b, L05, MMJP03].
Recommendation
[Bar06b, BK06a, BK07, Dwo03, NIS03b]. Recommended [Kel05]. Reconciling [BNPW03, PGT07]. Reconfigurable
[FD01, FZH05, GC01b, KBD03, LZ04].
MKP09, MMH02, SJT09, SKG09, SRQL03, CMS08, DHL06, GC00a, HBC+08, Rhi03].

Reconfiguration [PBTW07].

Reconsidered [Sho01]. Reconstructing [CDF01, FL06, PS01a]. Reconstruction [AF03, CF01b, CDF01, JJ00d, KY01c].

Records [Dur01]. Recoverable [NZCG05, NZS05, SGMV09, YY00].

Recovery [BDK+09, BM01c, CKM00, MMZ00, OS01, PBC05, SVW00, TC01, VV07, WCZ05, WLT05b, CCH05, CJ05, HW05, LKJL01, PSh04b, SIR04, TJC03, Wu01, ZF05].

Recursive [WHHT08].

Recycling [DPS05, TR09a, TR09b]. Red [Sas07].

Red-Eye [Sas07]. redistribution [KB09].

Redondo [IEE00a]. Reduced [BDK02b, CC08, CS05c, FKSW00, HQ01, HSR+01, KKS00a, KS00b, KKS01, KML+02, KM01b, KKS00b, MHL+02, NPV01, STK02, SK10, YSD02, CV05, Küh01, SK01a].

Reduced-Round [FKSW00, KS00b, KKS01, KML+02, KKS00b, NPV01, YSD02, CV05, Küh01]. Reducibility [DM00b]. Reducing [AL07, BIM00, SPHH06].

Reduction [CM05a, CH07c, Dhe03, Gro01, HGG07, Kid02, PG05, ALV02, HG07, Sug03].

reductions [Fis01a]. Redundancy [AB01, BR00a, FM02b, YLR05].

Redundant [MF01, Tad07a, PS04a].

Redwood [KKP02]. Reed [KY02b].

Reference [BR09, CPS07, Pas03, RS00, Sal07, vT00].

Reference-Watermarking [BR09].

Refined [Sma03b]. Regarding [GMP01a].

Regexp [BTTF02]. Region [BSN000, Bur00]. Region-Based [BSN000]. register [HTW07]. Registers [CGFSHG09]. Registration [HLM03].

regression [mSgFtL05]. Regulations [TMM01, Ano00g, Cha00b]. Rehearsal [Ahm08]. reinforce [SWR05]. Rejewski [BCB+05, Kap05]. Related [BDF+01a, Can06b, CY08, FKSW00, Kil01b, KLM05, Sat06, Buc00a, Gutxx, HAuR04, Hen06a, Sch00b]. Related-Key [FKSW00].

Relation [ABC+05, NN06]. Relational [AK02b, AHK03a, AHK03b, CCK07, GA03, PT08]. Relations [BN00a, Pau01, Uni00a, Uni00f, Uni00e, SP03, Zha08]. Relationship [Ngu05, GM+00]. Relationships [DKMR05, SKU+00]. relative [JRS09, Mii01b]. relaxes [Ano00c].

Relaxing [CKN03, PS05]. Relay [DM07b, Zha00]. Release [CHKO08, Mao01, HGSN03]. Released [Bar00c, Ano01g]. Releases [Bar00, AJ08].

Reliability [IKP+07, WK05]. Reliable [MR03, MPHD06]. reloadeded [SL06].

Remainder [Sch01b, YKLM03]. Remarks [BCW05, CL04d, SCS05c]. remedy [FZ06].

Remember [HSN+08a, HSN+08b, HSN+09]. Remote [CJT02, CWVR09, Kra02b, LL05c, Rub01, TK03, WKB08, CC01a, CL04d, CJT01, DSGP06, FCZ05, Hsu05b, LL05b, KC05, LHY02, LLH02, LKY05a, LHL03b, LC05a, MW06, SW06, SZS05, WLT05a, WC03b, YW04b, YC09b, YR05d]. remotely [Küh08, SR00]. Removal [LLS05a].

Removing [JL00]. rencontres [PPV96].

Renewable [TOEO00]. Repairing [DKFX05, GM00b, HL04, ZJ09, BKN04].

replace [Gav08]. Replacing [FZ06, KAM08]. replication [BIW08].

Reply [WLW04]. Report [DFG01, Pem01b, Pre01, Sal01a, Shao01b, BCHJ05].

Repository [Bar00b]. Representation [BvdB02, FSW01, JLM03, JY01, RN00a, RN00b, ZLK02, BDSV08, BA06, PS04a, SWR05]. Representations [OSSST04].

Representative [CTBA+01].

Representatives [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].

Republic [MJ04, dL00]. Republic [dL00].

repudiation [HLL04, LSA+07, SC05c].

reputation [KNS05, RCG+05].
reputation-systems [KNS05]. Request [RSA00b]. require [SV08b]. Required [Sun00a, Lov01, Wan05]. Requirements [FIP01b, HWH01, Kin02, NIS01b, Mei04a]. Rescue [ASW+01]. Researcher [Pip03]. Research [AJ01b, CZ05, CZK05, DFPS06, KGL04, LXM+05, RC06, Sch00e, TMMM05, DFCW00, JXXW05, 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, Mo02, EBS01]. Resistant [Ano01a, ACJT00, ANL01, BGW05, CDT05, CN06, Gir06, IK05, LLS05a, LWS05, LTM+00, LNL+08, KS09a, PC09, WL04b, YS02, MS09c]. Resolution [SGM09]. resolving [Lin01b]. Resort [USE00b]. Resource-Constrained [MRL+02]. resource-limited [Tse07]. Resources [Gutxx, FOP06]. Response [JBR05, LW05a, XNK+05]. Responsibilities [Vix02]. Restrict [ASW00]. restricted [ASW00]. Restriction [CTH08]. Restrudy [FWL08]. Results [APV05, GM02a, OOP03, RR08, War02a, YRS+09, CV05, CKRT08, DM07a, GMG00, PM08]. Retraining [Bra01a, KMZ03]. Retraining [JLC07]. Retreat [FKSW00]. Retractable [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, Ano02a, Duw03, Eau05, Fal07, Gas01, Gum04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, Pag03, Pap05, Puz04, Ree01, Rot07, See04, Spr03, Ter08, TvdKB+01, Top02, Uzu04, Was08a, Her09b, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wal00]. Reviews [For04, Kid00, Sal03b, Sty04]. Revised [Bl03, BC05c, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02, GS02c, GH05, HH04, HH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PT06, RM04, Sio1, Ytr06, AMW07, AJO1a, BK07, Bir07, CZ05, CKL05, DRS05, Irw03, PY05, WK06, Wri03]. Revisited [ABC+05, Ano02h, BM01b, CDP05, Kmu00, NS05c, OSSST04, Hes04b, OHH08b, ZTT05]. Revisiting [AEAO05, Har01a, Har01b, JMVO2]. Revocation [BDTW01, CL02a, Gen03, GST04, NNL01, TT01, SZM05, KT06, KSW06, LHH05, SW02]. revoke [NN03]. revolution [Bor00, Con00]. Revolutionary [CMB+05]. Rewriting [Cir01, HR04a]. RFC [BWBL02]. RFID [And04, AL07, ACDM05, Ayo06, BLDT09, CCS08, CH07a, CL09, FW09, FIt03, KKK+07, OS06, Ros06b, SE09, TZZT09a, TZZT09b]. Rhee [Küh08]. Rhode [IEE07]. RI [Siu01]. Right [Dhe03, GSO7b, HKP05]. rightful [CL08, Lin01b]. Rights [Bar00a, BNPW03, Dre00, Scr01, TMM01, Wya02, BA06, UP05]. Rijndael [BB02, MP01a, SKK+00, Wer02, CKK+02, CGBS01, DR00a, DR00b, DR01, DR02b, FKS+00, FKL+01b, FKL+01a, FSW01, FD01, GM00a, JMBdXGM05, KY01b, KMT01, KV01, Luc00, MM01b, MMH02, PSC+02, RDJ+01, SMTM01, SRQL03]. Rijndael-Like [PSC+02]. Ring [BSS02, Nao02, WBL01, ZK02, Her07]. Rings [BLST01]. RIPEMD [DG02, WFLY04]. RISC [CMB+05]. RISC-Based
Risk [WA07, Voi05]. Risks [ES00a, Kuhl02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, Ps01, Sch00c]. Rivest [BB79, Coc03, SP79]. RMI [JR8+06, Mar02a]. RNS [BJ04, BKP90, NMSK01]. Road [BDPV09, HR04b, PB01]. Roadmap [Coc02b]. Roaming [CAC03, YWD08, SSM+08]. Robots [Coc01a]. Robust [BB00a, BR09, CJ03d, CW05, DDO+01, FCZ05, HH09, hKLS00, LHS05, LLC06b, PJK01, SG07, SOHS01, SDFH00, SDF01, VK07, WNY09, WL04b, WMD08, YPSZ05, ZTP05, KA09, LCZ05c, LKH07, 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 [Blu09]. Rootkits [HB06]. Roots [Gon06, HCK09, CAC06]. Roseau [PY05]. Rotation [RBF08]. rotations [SK03]. Rothe [Fal07]. Rough [Nas02, WG05]. roughness [Lav09]. Round [JI00, BP04, Bih00, BF00a, BD02b, Che03, DPV04, DI05, Dra00, FKS00, GKK07, GIK02, HSR+01, Kan01, KO04, KKS00a, KS00b, KKS01, KML+02, KKS00b, LKH09, Lin01c, MP03, MHL+02, NP01, RR00, Ros00, STK02, WBRF00, Wer02, YSD02, CV05, CLC08, CKL+03, DLP+09, GIKR01, HSL+02, Kih01, LKH+08, MR01b, Pha04, SW05]. round- [CLC08].

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, Pre02c, Shp04a, Wal00, Adl03, Ano01k, Ano02e, AR01, BI04, BLH06, Bar00c, BM01a, BNPS02, BN02, Ber09a, BT02, BM10b, BM03b, BD00b, BMK00, BJN00, BF01c, Bon01, BCCN01, BP01b, CNS02, CDR+00, CW02, Che01a, CKY05, CNPQ03, CKN00, CNJP02, CS00, CS03c, CD01b, DK01, DT03, Duj08, Duj09, DN06b, FS02, FS01a, FOMP03, FMY01, FOPS01, GMP01b, GS07a, Gi06, Gon06, Gro01, HN04, Her07, HLL03, HL00, HLL03, Int00, Jan08b, JS05, Jon08, JK02b, JK02c, JG01, Kal01, Kal03, Kat05b, Kat01, KKL09, Kin00, KPR03, LS01a, MPS00, MLM03, Man01, May02, May04, Miy01, Mol03b, MP01c, NZCG05, NZ05, N01b, Nov01, NMSK01, PS00, Riv03, RSA09a, ST01a, Sch01b, Sei05, Sha03a, Shp01, Shp04b, ZS01]. RSA [Str02, SWH+09, TIGD01, TT00, Ver06a, Wal01, Wal03, WQWZ01, War00, WLH05, Wie00, WS02, WY05, XC05, Yan07, hY08, YKL02b, YKL03, YPKL08, YY00, You06, ZC09, Zhe01, ZW02, dW02]. RSA-based [NZS05, BNPS02, GMP01b, KPR03, Ver06a, HLL03, NZCG05, Sei05, WLH05, WY05, YPKL08, YY00]. RSA-Encrypted [CD01b]. RSA-Primitive [ST01a]. RSA(R) [Ano06b]. RSES [LLCL08]. RST [ZLZ07]. Rueppel [Ara02]. Rules [Bla01a, Ano00c, Bla01b, GN04, Ste02, Wue09]. Running [ZL04c]. Running-mode [ZL04c]. Runtime [PBTW07]. Russia [GKS05]. Ryan [Puc03]. Rye [KJR05]. Ryu [KCC05].

S [BZ02, Kat05b, Puc03, Bih00, BCD00, Dav01b, Dav01c, FM02b, JmbDxg05, LG09, Opp01, SMTM01, ZC00]. S-Box [FM02b, SMTM01, JmbDxg05]. S-boxes [BCD00, 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 [LXm+05].
Safeguarding [Sty04, Bar03]. safer
[Aho00f, NPV01, BDD03]. safety [HM01a].
SAFKASI [WAF00]. Salomon [Pap05].
Salsa20 [Ber07, Ber08]. Salt [PKBD01].
Salzburg [DKU05]. Samba [BH00a].
SAML [RR04]. Samos [KGL04]. sampled
[WW06]. sampling [KB39, Sug03, Tip27].
San [ACM03a, ACM03b, ACM03c, ACM07, Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, Sch00a, Sch01c, Sch04a, Sch05a, USE00b, USE02a, USE02b, Cal00c]. sans
[Car00]. Santa [Bel00, Bon03, Fra04, Kii01a, Men07, Sho05a, Yun02a].
Sanxin [LSZ05]. 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 [It00]. SC2000
[SY+02, YSD02]. SC2001 [ACM01b].
Scalable [CPhX04, HKA+05, HLL05, KY03, KHYM08, SPGQ06, LLW08b, ST03a].
Scalar [AHRH08, ADDS06, HM02c, OS01, OT03b, DwWmW05, Mis06]. Scale
[BWE+00, CDR01, FGD01, BP03a, BH00a, HMvdLM07, PIS08a]. Scaling [BBPV00, Coc02b, SDH00, SDFO1, PBVB01].
Scambry [Gun04]. Scan
[MYC01, BD03, KBD03]. SCAN-Based
[BD03]. Scaring [Ols00]. Scenarios [BF05].
scene [SG07]. Sceptical [Pen01b].
Schedule [MHM+02, XH05]. Scheduling
[FMS01, XQ07]. Scheme [AR00, AK02a, ACJT00, AF03, BBC+09, BPNS02, BR09, BS01d, BMS03, CL01a, CHK03, CGH01, CC01b, CY01, CTL04, CC09, CH01b, CM05a, Cof01b, CFS01, CD000, DS05a, DKFX05, FS01c, GJS01, GS02c, HS02a, HNZI02, HY01, HT06, HC08, Ig02, JSJ01, KK02, KC02, KCD07, Kog02, KLL01, KT00, KT01, KKD04, LD04, LHT09, LL05c, LCD07, Miy01, Mil01a, OKS06, PL01, RK06, Scr01, SOO02, SWH05, SGG00, SYL05, SSNG00, Tad02, TC01, Tsa01, TT01, WQW01, WZW01, WBD01, YWWS09, YG01a, YHL05, Z09, AE0R05, As04a, BCL05a, BCW05, BKN04, BBG+02, CL02b, CBB05, CC01a, CC05a, CL04b, CL04c, CL04d, CCK04b, CHY05a, CHY05b, CL00, CHC04, CCH04, CY05, CHC05, Che05a, Che07, Che08a, Che08b, CCS08, CKN06, CHT01, Ch08b, Ch08c, Ch08d, DSG06, DW01, FZ02, FXAM04, FCZ05]. scheme
[FWL08, FWCT05, Gen09a, GS09, Hes04a, HPS01, HW03, HWW04, Hsu05a, HWW05, Hsu05b, HL07, HCO4a, Hwa00, HY03, HLL04, Hwa05, HL05c, HL05d, HL05b, JW06, JSW05, KCO9a, KLY03, KRY05, KSW06, KKL09, KCO10, KCO1, KCO5, KCC05, KHK05, LHY02, LLH02, LHL03a, LKY04, LL04a, LJY04, LL05a, LKY05a, LKY05d, LLM05b, LMC03s, LLH04, LTH05, LCL08, LLH06, LHL03b, LH03, LCO4a, LG070, LCC05, LCO4b, LC05a, LHH05, LC05b, LC05c, LC05a, LWK05b, MS09, NC09, PW05, PBMB01, PCC03, PC05b, PS01a, Pei04, Sae02, Sco04a, Sha03a, Sha05a, Sha05c, Sha05d, SLH03, sMGfL05, SCS05b, SCS05c, SCS05c, SZS05, TLH05, Tsa08, TWL05, TYH04, VK08, VS08, WLT03, Wan04b, WLO5, WK05, WP07, WDLN09, WHH05, WC01b, WH02a, WHLH03, WH03, WC03b, WL04b, WC05, XW08L, XCO5, YW04b, YTH04, YW04a, YCH04, YWL05, YCO9b, hY08, YRY04, YRY05a, YYY05a, YYY05d].
schemes
[YY05b, YbJ04, ZC04, ZC05, ZK05, ZK05, ZW05a, ZAX05, ZC09, ZL05, dRMS05].
Schemes
[AR01, BP02, BU02, BDDS03, BF05, BGOY08, BDS09b, CM00, CD00a, CL04a, CGP08, CT08b, CPDP06, CKN00, Cor02, 65]
CJNP02, Cou04, CS00, CS03b, CDG+05, CLZ02, DN00a, DN02b, Des00b, DS06, DN00b, FF00, HSZI00, HWW05, HM02b, HLL05, Kin02, Kos01a, KS03, KOM01, LZL+01, LP01, MV00, NIS03b, Nam02, NNL01, NN06, OP01a, Pat04, Pre01, ST01b, SBZ02, SPMLS02, Sun00a, VMSV05, WCJ09, X503, YWCO8, YYD001, Yek07, YYZ01, ZTP05, ZYR01, Ab01d, AFHG06, BCD06, CWH00, CC05b, CJT03, CDFM05, DD04, DM00a, DFM04, Des00a, GGK03, HCD08a, HCD08b, HAU04, He02, HKS00, HW03c, HW04, HW05, HC04b, HL04, IY06, JPL04, JXW05, KJY05, Kir01b, KT06, Kre05, Küh08, LWZH05, LWK05a, LW05c, MF07, Mi01b, NK06, PS02a, PKH05, Ph06, QC05a, QC05b, SN010, Sha03d, Sha05b].

schemes
[SCL05, SC02c, SHT05, Ts05, Wu01, XY04, YWC05, YCW+08, ZF05, ZCL05, vDKST06].

Schloss [IEE01b].

Schneider [Puc03].

Schneier [Hei03, See04, Sty04].

Schnorr [BP02].

School [Coc02a].

Schools [PM00].

Science [Bis03b, Coc03, IEE00a, IEE01a, IYE02, IYE03, IYE04, IYE05a, IYE06, IYE07, IYE08, IYE09b, Im03, Nie02d, Pag03, Sch06b, SM07b, Sin01b, CAC06, PRS04].

Scientific [CHT02, MH09, Lau08b].

Scientists [Coc01a, MH09].

SCN [BC05c, CGP03].

Scots [Ree01, Sin99].

Scream [HCJ02].

Scribner [Gos01].

Scripts [Uri01, Oue05, R02b, R02b].

scroll [GB09, HHYW07].

SD [ECM00a].

SDK [An02d, Bar00c].

SDL [H006].

SEA [SPQ06].

SEAL [Flu02b].

Seamless [OKE02].

Search
[Bi05a, Des00c, FFR05, KB07, LM02, TIGD01, WYY05a, WYY05d, FZ06, PM08].

Searchable [ABC+05, AFI06].

Searches [PGT07].

Searching
[BW09, GTTC03, OS05].

Seattle
[ACM06, S*03, USE00a].

sec [KV01].

Second [ACM03c, Bra01b, BD08, CZ05, GW01, HTS02, JYZ04, KRC04, Ki05, KP01, NM09, RD01, ACM00, Irw03, Son00, Spr03].

Second-Order [NM09].

Second-Price
[Bra01b].

Secord [Top02].

Secrecy
[Bla02a, GH02, Im03, Lan05, Rec01, RW03a, Sin01b, BDNN02, BLP06, BD04a, Mol05, Sin99, Sin00, SY06, ZY07].

Secret
[ACS02, Alv00, BBK00, BTW05, BI05b, BTW08, BM01b, CGHG06, CH00a, CH01a, CLT07, Cha04, CTY90, CC06, CS05b, CKN01, CDM00, CDF01, CF02, CFS05, CDG+05, CI05, Di 01, DKL00b, DS06, DN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jan06, Joh05, JLL02, Kab07a, Kab07b, Kab09, Kar01, Kin02, Kog02, 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, AEEd05, An02c, An08c, Bam02, BC07+05, Cal01, CC05a, CHY05a, CHY05b, CILJ06, CNK04, CDD00, DD04, D004, D004a, Di 03, DW01, Duj08, FNRC05, FWTC05, FZ06, Gal02, GIKR01, HT04, H07].

secret
[HKS00, IY06, Kee05, KB09, Lam07, Lun09, MF07, Mi09, Na05, PS02a, PW05, Ris06, Sch01e, SZ04, SC05a, Sin01b, SC02c, Wan05, Win00, YCH04, ZSV05, dRE05, vDKST06, HI06].

Secret-Ballot [Cha04].

secret-code [D001].

Secret-Key
[HR05, RW03a].

Secret-Sharing
[BI05b, CDM00, CI05, DKL00b].

Secretly [CC08].

Secrets [BH06, BBD+02, CMS09, CP07, Cop04b, Di 01, Gan01b, Gum04, KMS01, LKM+05, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM+01, VGM04, AGKS07, An03a, An05b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, DM07a, Di 03, DW09, EC05, FS04, GD05, MSK03, Pau01, Se08, T002, DLM05].

Section
[An04a, An04b, BK06b, S080, TL02, KP03].

Sector [Cro01, MV01].

Secure
[McK04].
Selected [BKPO9, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, VY01, Ytro06, AMW07, Bir07, BC05c, CZ05, CKL05, DR05, HH04, HH05, PC05a, Wli09, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06].

Selecting [Bar03, dBo7]. Selection [IBM00, JK00, RS00, SM08]. Selective [CS07c, LS01a, LM02]. Selective-ID [CS07c]. Selectively [Ch10s]. Self [GMM08, HW05, KY01d, PS01b, PBC05, Sch06b, WHL05, WLT05b, ZKL01, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, HL04, Lee04a, LL06, LS05b, LKW05a, PC05b, Sha04b, Sha05b, TLH05, Tsa05, TJ03, WH03, Wyl05].

Self-certified [HW05, BCL05a, BCW05, CWH00, CCH05, CJ05, HW04, HL04, LL06, LWK05a, PC05b, Sha04b, Sha05b, TLH05, Tsa05, TJ03, WH03, Wyl05].

Self-Enforcing [GMM08]. Self-Escrow [PS01b].

Self-Localization [WLT05b].

self-modifying [CSV07]. self-pairing [Lee04a, PC05b]. self-protecting [LS05b].

Self-Shrinking [WHL05, ZKL01].

Self-Similarity [Sch06b]. Selling [Bl10c]. semantic [PBV08, SN00, Sch00c, Coc01a]. Semantically [Kh01b, ST01a]. Semantics [Li01, Mar02b, BFG04, BFG05, SW02].

Semi [Fer00, Nak01, SY01b].

Semi-Equivalent [Fer00]. Semi-fragile [SY01b]. Semiconductor [Coc02b, Ig102, UHA+09]. Seminal [Cop04b]. semipublic [YC07]. Sender [CMB+05, Her09b, TJ01a]. Sensation [Top02]. Sensible [Sch04c]. Sensibly [See04, Sty04, Hei03, Sch03]. Sensitive [HT06, Bro05b, SPH06]. Sensitivity [SDMN06, GSK09]. Sensor [AEAOQ05, CS08b, DB+06, Fin06, GPC+08, LNL+08, NABG03, PZH09, ZYN08, AJ08, CCMT09, HMvdLM07, JRR09, KXZ09, KHY08, LDH06, LPV+09, LN04, Lop06].

Security [CGP03, JRB+06, Lin02, RR04, Uni06b, ZL04c, Pap05]. Security-related [Gutxx]. security-sensitive [SPH06].

seed [TP07, KKJ+07]. Seeing [Wal03].

Seek [Coc01a, PH03, Shp05]. seeking [Mos06]. Seeks [CAC06]. Seems [Coc02a].
MWS08, MS09b, NC09, NLD08, PS08a, RAL07, TP07, WDLN09, ZSJN07, AMB06.

Seoul
[CKL05, KCR04, Kim02, LL03, LL04c, May09, PC05a, PK03, Son00, Won01, WK06].

Separable [CD00a]. Separating [MKKW00, Nie02b]. Separation [BYJK08, GKK07+09, Kel00, Lys02, Mur00, ZGLX05, BYJK04].

September
[AUW01, AAC01, AJ01a, BCKK05, BC05c, CSY09, CGP03, DV05, DKU05, DFCW00, EBC00, ELvS01, FLA03, GKS05, QS00, RS05, SL09, WG02, YZEE09].

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

Sequence [HWH01, MS02e, WHLH05, AC19Z05, GB09, SL09, WG02, YZEE09]. Sequences [ADD09, Bi09, FSGV01, HG05a, JZCW05]. Sequential [GSS08, Bi09, FSGV01, HG05a, JZCW05]. Serial [CTLL01, KWP06, Uni00g, Mit00].

Serial [HWH01, MS02e, WHLH05, ÁCTZ05, GB09, SL09, WG02, YZEE09]. Sequences [ADD09, Bi09, FSGV01, HG05a, JZCW05]. Sequential [GSS08, SNW00, RMH03a, WH02b]. Serial [CTLL01, KWP06, Uni00g, Mit00]. Serpent [BDK02b, ABK00, IK00, IK01, KKS00a, KKS01, KKS00b, OSv00, Pat01]. Server [ANRS01, BA00, 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 [BS00, BM00, HS07, Jab01, KCD07, Mar02a, TEM+01, LS05b, PT08]. Service [BACS02, BH00a, CLK01a, De007, KZ01, Lan04a, LD04, Nik02a, Nik02b, PKBD01, CUS08, HILM02, KWD06a, LB05, Mir05, MV03b, SRJ01, SSM+08, ÚG08, Coo02b, Hil06].

Services
[ANS05, BC02, DJLT01, ECM00a, ECM00b, Kn07, Tsa01, Uni00b, WL07, BDF09a, BFG04, BFG07, BFG08, CCCY01, HM05, JRB+06, MW06, MPPM09, MV03b, RR04, SGB07, SL05b, TWL05, WA06, BH00b].

serving [LK05]. Session [GL01, OHB08a, CS04, OHB08b, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h, YWL05].

Session-Aware [OHB08a, OHB08b]. Session-Key [GL01]. Sessions [KPR03].

Set [BBGM08, GRW06, JRFH01, KS05c, WG05, aSM01, BDE00, Che07, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01].

Sets [CF05, EIG01, TW07]. Setting [BBM00, DLY08, LP01, PGT07, GMLS02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SGB01]. SGI [Bar00c]. SGID [Tot00]. SHA [AD07, BC04a, GLG02, HKR01, MP06, SK05a, TYYL02, WYY05d, WYY05b, WYY05c].

SHA-0 [BC04a, WYY05d]. SHA-1 [GLG02, HKR01, MP06, WYY05b, WYY05c]. SHA-2 [SK05a]. SHA-256 [TYYL02]. SHA-512 [AD07, GLG02]. SHA1 [WYY05a].

SHACAL [KML02]. Shacham [Hes04a]. Shamir [BB79, SP79, Co03, PW05, VS08]. Shamir's [LD04]. Shape [Gan01b, Gil07].

Shapes [OMT02]. SHARC [DMS09].

Share [CT08a, CD01, FS04, AEEd05]. Shared [ACS02, BH06, BDK00, BT02, CGH00a, TEM+01, WP03, WS02, BF01c, CYH04, GD05, HL05c, Tyl04]. Shares [TT01]. Sharing [BTW05, Bi05b, BTW08, BGHP02, CD00a, CLT07, CC08, CTY09, CDM00, CF02, CS05, CDG05, CD05, Di 01, Di 03, DS06, DP07, FM02a, FPS01, FMY01, HNZ02, Kin02, Kog02, KS03, LD04, MN01, NN06, OHS06, PZ01, PZ02b, PZ02a, S01, Sn00a, TC01, TCC02, WN02, WBD01, ZP01, CGH06, CC05a, CHY05a, CHY05b, CDD00, DD04, DM07a, DL00b, FWTC05, GIKR01, HTO4, HK00, IY06, LT04, MF07, PS02a, PW05, PS08a, SC05a, SC02c, TL02, YCH04, YCV07, ZSV05, dRMS05, vDKST06].

Sheets [MNS01]. shell [Dwi04, Gua05, BS01a, BS05]. Sheltering [MYC01]. Shen [KTC03]. Shieh [McK04, CZ03, YWC05]. Shift
Signer-Base [IR02]. signer-verified [CJT04]. Signers [LZL+01, Sae02, Sha03c, YTH04].

Significant [SZ01, MS02b, Shp02]. Signing [Ano00j, IR01, RR02, HWW04, WK05, WH02b].

Signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b].

SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b].

Significant [SZ01, MS02b, Shp02]. Signing [Ano00j, IR01, RR02, HWW04, WK05, WH02b].

signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b].

Significant [SZ01, MS02b, Shp02]. Signing [Ano00j, IR01, RR02, HWW04, WK05, WH02b].

signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b].

Significant [SZ01, MS02b, Shp02]. Signing [Ano00j, IR01, RR02, HWW04, WK05, WH02b].

signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b].
Sch00b, Ste00, USE00b, VH09, VVS01, WHLH05, W010, ZCC01, ARJ08, Ano00h, Ano00j, Bir07, CT02, CCD+04, CTT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, KA09, Mat02, MC08, MCHN05, Pau03, Sch01d, SS03, WL07a, WA06, Sal03b, Bol02].

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].

Solutions [Ano04b, MV01, Jun00, MSK03, MV03b, St.00, Gum04].

Solve [CU01, GS03].

Solving [CJT04, GPP08, Wil01a, Bul09, Whi09].

Some [AG01, BDF+01a, DJ01, DFG01, GM02, HSS04, JMV02, KY02, MTO2, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HAuR04, He02, JK01a, RSS04, SHT05, ZF05].

Someren [Ano06c].

Something [FL01b].

Sometimes [FNRC05].

Sons [Ano04].

Sorry [San05].

Soul [Bla01c].

Source [Bar00c, Bol02, Gut00, HBF09, KLR09, PM00, RK06, TEM+01, Ano03c, BGL+03, CBB05, McA08, RVS09, SB05, Bar00b, Lin02].

Sources [KZ07, WLZZ05, KZ03].

Southampton [Bla03].

Soviet [AJ08].

SP800 [SF07].

SP800-90 [SF07].

SPA [FMP03, Nov01].

Space [BGH07, Lu02, MSNH07, NS05a].

Space-Bounded [Lu02].

Space-Efficient [BGH07].

Spain [BS03, DFPS06].

Spam [CMB+05, DGN03, Vix02].

Spanning [Bel04].

SPARK [Jen09].

Sparse [BLST01, BDF+01, FS01b, GS03, BF06a].

Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09].

Spatial-Domain [SDFH00].

Spatial-Temporal [CT0705].

Spatio [Jen09].

Spatio-Temporal [CT0705].

speakables [BZ02].

SPEAK SREP [LM00].

Speaks [VN04].

Special [Bar00c].

Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08].

specialized [Wan04b].

Specific [HCK09, Zir07].

Specification [BCHT00, ECM00a, LKJL01, RSA00c].

Specifications [IEE00b, BD04a].

specified [GSK09].

Specified [Tad02, He02, LWK05b, YY05a, ZF05].

Specifying [BJvdB02, C010, SBS09].

Spectr-H64 [GMM01].

spectra [MS02b].

Spectral [QPV05, SK07].

Spectrum [BQR01, LY07, PM00].

Speech [MRL+02, AA04a, PY08].

Speech-Generated [MRL+02].

SpeechStudio [Ano02e].

Speech [Ano00d, Ano02d, Gr01, JKRW01, KMM+06, Lut02, SOTD00, SM02, Wie00, YKMY01, BGL+03, RW07, RMCG01].

Speeding [Osv00, SWH+09, TC05].

Speedup [YKL02, YKLM03].

Speedy [Cre00].

spherical [LZP+04].

Spider [Tur04].

Spies [Gan01b, Win05c, Hau06, NRR00].

SPIHT [Che08a].

SPIN [MS02a].

Spline [SPK08].

Splitting [GMW05, LKL05].

SPN [HLL+01, Kan01, PQ03b].

SPNs [KCL+03].

Spot [Na05].

Spread [BQR01].

Spring [Pap05].

Spring-Verlag [Pap05].

Springer [FAL07, Lee03a, Lee03b, Pho01].

Springs [Wil99].

spy [FNRC05].

spyware [Ste05c].

SQL [Dew08, HILM02].

Springer [Fal07, Lee03a, Lee03b, Pho01].

Springs [Wil09].

Squaring [CH70b, NS02].

SSRAM [HBF09].

SSC2 [HQR01, ZCC01].

SSH [All03, BS01a, BSB05, BKN04, Dwi04, H0101, Hos06b].
Kra02b, Naz02, Oue05, 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, OHB08b].

**SST** [Gau02].

**St** [GKS05, NH03, AS01a].

**Stack** [Pot03].

**Stage** [Kak06, CHY05b].

**stamp** [CL00].

**stamping** [HHC05].

**Stamps** [KZ01].

**Stand** [CAC03].

**Standing** [Lan00b].

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

**State-transition** [TL07].

**statecraft** [dL00].

**Stateless** [ANR01, NNL01, SK05b].

**Stateless-Recipient** [ANR01].

**States** [LB04, Jol01].

**static** [CW07].

**Statistical** [Fil02, GHJV00, GHJV01, HNO+09, Jun05, KK07, LZ01, LL+01, MV03a, Neu04, Pro01, RSN+01, BKW03, GSK09, Hey03].

**Statistically** [Fis01b, HR07, HNO+09].

**Statistically-hiding** [HR07].

**Statistically-Secret** [Fis01b].

**Statistics** [CKN01, CNK04, KLML05].

**Status** [Pre01, Sha03b].

**statute** [Cal00b].

**STDML** [WMDR08].

**Stealing** [Gau01b].

**Stefan** [AUW01].

**Steganalysis** [Pre01, Sal05b, GSK09, WW04].

**Steganografie** [Sch09].

**Steganographic** [CTL04, HR02, LL02, MJF07, RH02, RS00, Wes01, KC09a, LYC02, WWTH08, YCL07].

**Steganography** [BC05a, BG108, CYH01, ChLYL09, CDR01, CW09, CTH08, Cal03, CMB+08, CS05c, DIRR05, DRL09, FGD01, Fr07, Gal03, HCBLETRG06, HLvA02, HvAL09, Hun05, HSKC01, LS08, PH03, Sal05b, Sch09, Sha01e, 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, KKKL09, MP07, SL06].

**step-by-step** [SL06].

**Step-out** [KKKL09].

**Stepping** [WRW02].

**steps** [Bih02].

**Stereotypes** [GO03].

**Stern** [CGP08, CS05b].

**sticker** [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, Hud04, MSTS04, RCBL00, Ric07, RH02, Vad03, AFGH06, DFSS05, HGR07, LPM05, SGMV09].

**Store** [CTBA+01].

**Storing** [ST06].

**Story** [Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kah96, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, HS01a, Win00].

**strategic** [AJ08].

**Strategies** [Cir01, KL05, SKQ01, Dwi04].

**Strategy** [DR02a, TPPM07, KC09a].

**Stream** [BCC01, BC05b, BSW09, BS00b, BL02, CF01b, Can06b, CJS01, CHJ02, CM03, Co03, CL02c, DF07, Fil00, FFR01a, Gol01d, Gol01e, GMB02, HCJ02, HR00, HR04a, Jam00, KH01, MSNH07, PP06a, SM01, Sar02, SYX01, WB02, Wu02, ZC00, ZCC01, BGP09, Ber07, BD00a, BG08, BVP+04, DS09, DK08, KH08, Max06, MI09, PCS03, PCC03, SB05, WW08].

**Stream-Cipher** [SYX01, WW08].

**Streaming**
Streams [AIP01, CO09a, YLC+09, ZCW04].
Strength [CB01, JX05, Oni01, CKL+09].
Strengthening [Loi00, MHM+02]. Strings [CPS07, DFS04, Pas03, Dam00, RG05].

Strength [CB01, JX05, Oni01, CKL+09].
Strengthening [Loi00, MHM+02]. Strings [CPS07, DFS04, Pas03, Dam00, RG05].

Success [An006d]. Subtleties [Lai08]. Subverting [HB06].
Sufficient [IKO05, Kos01b, KO00, MN01].

ABM08]. SUID [Tot00]. SUID/SUID [Tot00].

Lam07, CAC06, Hos06b].
Supersingular [Gal01, RS02, Ver01].
Survivable [CLZ02].
Sweden [BS01b, Joh03].
Symmetric [RBF08].
Symmetry [RBF08].
Symposium [ACM00, ACM01a, ACM02, ACM03b, ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, An006d, BS03,
BCH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04, IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Je08, KM07, MFS\textsuperscript{+}09, SMP\textsuperscript{+}09, TLC06, USE00d, USE01c, USE02b, May09, dCdVSG05.
synchronisation [CMdV06].
Synchronization [GPČS08, SW02].
synchronize [Pau02b].
Synchronous [CH01b, Sar02].
synopses [YLČ+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, It01, Joh05, KC02, KHY04, LV00, LSS05, LSS05b, LXM+05, MA00a, MA00b, Miy01, MFK+06, MFS\textsuperscript{+}09, RH02, SR01, Sha02, SO01b, Ste05b, TK03, TZE09b, USE00a, WG05, WA07, YKMY01, YKLM02b, ZYM05, AHIK03a, AMRP00, Ano00j, ADH+07, AAKD09, Bih09, BDET00, Bul09, CC02b, CCH05, CJL06, CPG+04, Coc01a, Cre00, CO09b, DZZL01, DPT+02, Dim08, DGP09, FP00, GG08, GSK09, GMG00, Gou09, HLL+02, Joy03a, KWDB06, KXD00, Kwo03a, LLI04b, LKJL01, Lin00a, LK1, MKKW00, RCG+05, Sal00b, SCS05a, SGMV09, SETB08, TKP+08, Wan04a, db07].
systematic [DW05, ZL04a].
Systemic [KB06].
Systems [ACM03c, ACM05b, ANRS01, Ano02e, BCS02, BRTM09, CP02, ELvS01, Fel06, GS03, GRW06, IEE01b, JQ04, KKKP02, Ket06, Len01, LST+05, LLLZ06a, LJJ05b, Lut03, Mar02b, MMY03, NABG03, RS05, Ril02, SM01, Sas07, SJJ09, SY01, USE00c, USE00b, Vav03, VHP01, WKP03, ARJ08, And08, Ano01j, Bn03, Bl07, CUS08, CC05c, CCS08, CGL+08a, CGL+08b, CGL+08c, CCM01, CNPQ03, CHT02, CG05, CSK+08, DY09a, EY09, FMY02, FP00, HP00, HBC+08, Hut01, HYS03, KAM08, KP01, KNP01, KP03, Kov03, KR03, KNS05, MBS04, MSP+08, ND06, Nis03a, PBMB01, Par04, P106, RW07, Sha01a, SK03, TOE000, WA00, XQ07, ZSV05, Ano02d, Lut03].
systems/ciphers [SK03].
Systolic [KLY02, KKY02, MP01c].
Table [Ano03d, MFFT05, XFZ01, BZ03, CC05b, Has00, Tsa08].
Table-based [Has00].
Tables [AJ008, KB39, RF08b].
Tag [KK+07].
Tagging [BP05].
Tags [OS06, ACdM05].
Taipei [Lai03].
Taiwan [Lai03, Ano03a].
Takagi [LKYL00].
Takagi-cryptosystem [LKYL00].
Takaragi [WHL03].
Taking [CDS07, Lai07, PM00].
Talbot [Rot07].
Talk [FGM00a, Lan00d].
tamer [Kap05].
Taming [Aha00, Lov01].
Tamper [LTM+00, CT02].
tamper-proofing [CT02].
tampering [PS08b].
tandem [DPT+02].
Tang [YRY05d].
tank [Pau03].
tar [Str02].
targama [MA05T05].
target [BD04b].
Targets [MV01, Pau03].
Tarragona [DFPS06].
tasks [XQ07].
Tate [Jou02, SKG09].
TATSU [TS000].
tattling [CSK+08].
TC [DKU05].
TC-11 [DKU05].
TC-6 [DKU05].
TC11 [ElvS01].
TC8 [DFCW00].
TC8/WG8.8 [DFCW00].
TCP [SBB05].
TEA [CV05].
H5R+01, HIR20, HHHK+04, MHL+02, WN95].
Teaching [McA08, Shu06, GV09, Jan08b].
Tech [Kir01a, TvdKB+01, Unío0c, Gra01, Uni00f].
Technical [BHM03, GS07b, Lan00c, Sr01, TL02, USE01b, USE01a, USE02c].
Technique [CC02a, Pan09, PQ03b, SC02a, WC03a, vW01, CL00, Che08b, Pau03, Ren09, WC05].
Techniques [AIP01, BS09, Bih03, BBPV00, BDP02, CC04a, Cra05a, DBS+06, Dun06, Gal03, KLN+06, Ken02b, Knu02, KO03, MKP09, NCRX04, PJK01, Pfi01, Pre00, Shi08, YKW01, AB09, BM05, BR05, Che08a, DY01, DHMR07, DY09a].
Gal02, ISO04, KP00, Man08, Pin02, Pin03, PBVB01, SETB08, Swe08]. Technologie [RSA09b]. Technologies [MS05a, PP06b, Sam09, SE09, VH09, Way01, Way02a, ZWC02, ATS04, PB01, TTZ01]. Technology [CZK05, Cla00a, GSB04, MP00, NFQ03, Pag03, TV03, AL07, Ble07, Car01, Cas02, Che00, ISO04, Jac00, KB00, LR01, Pau02a, Pau02b]. Tektronix [Ano02e]. TelCorreo [LM00]. telegram [Tuc66]. Telelogic [Ano02e]. Telephone [KZ01]. telephones [CF05]. Telephony [Ano02e, CFRR02, PM00, CGV09]. teleportation [BEZ00, BEZ01, Duw03]. Telling [Gan01b]. template [LLC06a, UBEP09]. Temporal [CDTT05, KXTZ09]. Ten [ES00a]. Tenth [USE01c]. Term [ABRW01, Dur01, BMV06, ISO05, LG04, SGMV09, WDLN09]. Terminal [ECM00a, ECM00b]. Terminals [Chi08a, ISTE08]. termination [BP05]. terms [LMTV05]. Ternary [AD109, DKL005]. Terrorism [PP06b]. terrorists [Mad04, Win05c]. TELSA [LNo4]. Test [BT02, HSS04, Lan00b, LN08, RSN+01, Way02a, DS00, GMG00, Kat05a, KKKP05, RSS04]. testable [RMPJ08]. Testing [III00, CGBS01, Fil02, Lut02, Lut03, SB00, WA06, Lut03]. Tests [MT02, NM09, GTO2, Gt04c, JPL04]. Text [Lut02, PJH01, PM08]. textbook [BJN00, PP09]. Thank [CMB+05]. Theft [CMS09]. Their [AGT01, CD00a, Gen04a, KJRW01, LLL+01, WLZZ05, CM05b, Has01b, Pau02a, PW08, Sav04, SSST06, TO01, WVO0]. Them [WD01a, Tce06]. Theorem [AC02, Eke02, GN01, Sh00a, Scho1b, YKLM03]. theorems [MW04, Nyb01]. Theoretic [CB01, DHR00, Kat05b, Nie02b, VVS01, VDKP05, 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, Fal07, HR06, Hay06, IZ00, Irw03, Kim01, Kun02, Lai03, Lee04b, Lu03, MNT+00, Mao04, NP02a, Nao04, Oka00, PY06, Pre01, Pre00, Rot05, Roy05, Sch06b, Smp03, Spr03, TW02, TW06b, Vau05a, Wao00, WG05, Yan00, YDKM06, Zhe02b, AUW01, AB09, Buc00a, Cas06, Cos00b, DW05, Gar04, HHL+00, HW98, Joy00, Kil05, La00, Lam01, PPV96, Rot02b, Rot03, SCS05a, Sh05b, Ste08, Sthi95, Sti02, Sti06c, Tat05, TW05, Was08b, HR06, KXTZ09, Kil05, Nao04, Nie02a, Nie04]. There [Bar00b, GW00]. thieves [NRR00]. Think [Pau03]. Thinking [See04, Sty04, CS07a, Hei03, Sch03]. Third [AL06, BS01b, CGP03, HR06, IKY05, KN01, MS02c, NIS00, Won01, WV01, CKL05, GKS05, IZ00, JZCW05, QSO0, CGH+00b]. third-order [JZCW05]. Thirty [ACM03b, ACM06, ACM08]. Thirty-Eighth [ACM06]. Thirty-Fifth [ACM03b]. Thiry [ACM02]. Thiry-Fourth [ACM03b]. Thorsteinson [For04]. Thou [MYC01]. Thought [MNT+00]. Thoughts [Joh00]. Threat [Por06, SS04, BK00, Geb04]. threatened [An00]. threats [CNPQ03]. Three [BR00b, Kak06, LSH00, MAaT06, AJ08, CL00, FGM03, GPS05, LHL04b, LK05b, MLS+09, MF07, MAaTxx, SPH06, YC09a, ZL04b]. Three-Key [BR00b]. Three-party [LH00, CL08, LHL04b, LLS+09, YC09a]. three-principal [ZL04b]. Three-Stage [Kak06]. Threshold [AF04b, AIP01, BTW05, BTH08, BDDS03, BSS02, CCD07, CLT07, CDN01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, KS05b, Kin00, Kin02, Kog02, LSL+01, LSC03, LCZ05a, LP01, MSJ02, Nie02c, STY07, WQWZ01, Wan04b, WH03, XS03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, DG06, HHW02, HHW03,
Throughput [HV04, Ls01b]. thwisting [WL07a]. TI [GBK01]. th [Maa07]. Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. Tight [CM05a, Di01]. Time [AK02a, App07, AJO08, BPST02, BSO0b, BSW01, CU01, CG03a, CNV06, CLZ02, Dri02, GPC08, HM02b, Ina02b, KL05, Kuhn02a, LP02a, Lan00b, LJJ05, LDM04, May04, Oec03, Pi01, QSR−02, RR02, CAC03, CCK04b, CL00, DS02, GS07b, GM04, HLJ09, HHC05, LC04a, MRST06, NS05a, YZDW07, LY08, DK08]. time-bound [hY08]. Time-Domain [Kuh02a]. Time-Free [CNV06]. Time-Limited [AJO08, Oec03]. Time-Memory [AJO08, Oec03, QSR+02]. Time-Memory-Data [DK08]. Time-Reversed [hY08]. time-space [NS05a]. time-stamping [HH05]. Time/Memory/Data [BS00b]. Timed [BN00b, CHK008, JP07, LKJ01, Mao01, HGNS03, Zha06]. Timed-Release [CHK008, Mao01, HGNS03]. times [AJO08, CCK04b, Mol05]. Timestamp [CC01b, FLZ02, SLH03, WLT03, YW04a]. Timestamp-Based [CC01b, FLZ02, SLH03, WLT03, YW04a]. Timestamping [MSTS04]. Timing [CKQ03, CW090, Law09b, Sch01b, SWT07, AS05, DKL+00a, KS09a, SO00]. timing-attack [KS09a]. Tiny [Bar00b, WN95, An03]. Tipsy [TvdKB+01]. Tissue [MYC01]. Title [ZH03]. TLS [BPST02, CHVV03, HSD+05, JK02b, JK02c, KPR03, OHH08a, OHH08b, SBEW01, BFCZ08]. TMAC [KJ03]. TMS320C6x [WVG00]. today [Li05, Nis03a]. Together [WD01a]. Token [Fri01, RSA00d, RSA01, CS04]. tokens [WDCJ09]. Tokyo [Ano00d]. Told [ES00a]. Tolerance [Ano04a, BK06b, ZL04a]. Tolerant [DS03, HSKC01, WLO7b, BKW03, HGR07, Lin07, PI06, RMH04, YbJ04]. Tolerating [KSR02, SKR02]. too [Sch05c, vT01]. took [IEE09a]. Tool [Ano02d, Ano02e, Ki01b, GPG06]. Toolkit [NIS01a, Sha01a]. Tools [Ano02d, Ano02e, Bar00b, Goh01b, Ken02b, Ust01b, Bai08, Cas02, CT02, GC05, NCRX04, SETB08, Kat05b, Puc03]. toolset [Jen09]. Top [Cal01, Fox00, Jan06, MV00, AJO8, GPC08]. top- [GPC08]. Top-Level [MV00]. Topics [HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oka04, Poi06, Pre02c]. topology [HJ07]. Tori [GV05, GPS06]. Toronto [MS05a, VY01]. torsion [KM04a]. torsion-subgroup [KM04a]. Torus [BS03, RS08, vD04]. Torus-Based [BS03, RS08, vD04]. Tossing [Lin01c]. totality [HRS08]. Touch [Pau02a]. tour [Pet08]. Town [KJR05]. Trace [Br01, LNS02, NN03]. trace-and-revoke [NN03]. Traceability [HLL03, HW05, WLIH05, WY05]. Traceable [LZL+01, CCH04]. traceback [CS04]. Traceing [KY01d, KY01e, LLL02, NNL01]. SNW00, TT01, WRW02, WLZZ05, WH01]. tracings [RE02]. Track [Fox00, Joy03b, Nac01, Oka04, Poi06, PM03, Pre02c, USE01b, USE02c, Men05, CAC03, CAC06]. Tracking [WC05, FNRC05, SZ08, TWM+09]. Trade [AJO08, CMS09, Oec03, PS01c, Uni00f]. Trade-Off [AJO08, Oec03]. Trade-Offs [PS01c]. Tradeoff [LP02a, QSR+02, CW02, Ina05, NS05a, DK08]. Tradeoffs [BS00b, CTLL01, SRQL03, SU07]. Trading [PV06b, SWH+09]. Traffic [FGL02, Mi08, Fel09]. Trail [DR02a]. train [Pri00]. Training [Coc02a]. Traitor [KY01d, KY01e, LLL02, SNW00, TT01, WH01]. Transacted [HBdJL01]. Transaction [RH02, AAKD09]. Transaction-Based [RH02]. transactional [ST06]. transactions [Cal00b, Cal00a].
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, LKLK05, Nak01, SSFC09, VK07, BR06, Che07, OP01b, SR00, LPZ06]. Transformation [CT09, HLL05, DSP01]. 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]. treatise [Bla00, MAaT03, MAaT04, MAaT07]. treatises [MAaT06, MAaT07]. Treatment [CL05, DK08]. Tree [CC05d, GST04, JLMS03, KPT04, LKLK05, LM02, TNM00, Mon03, PCC03, WL02]. Tree-Based [GST04, KPT04]. trees [Che02, Che07, TC00]. Trends [Ahm08, KB07, Ort00, Ndm06, PRS04]. tricks [All03]. triggered [HJHS04]. tripartite [SW05]. Triple [IHH+01, BR04, CGBS01, Cor00a, FZH05, Kel05, LMP+01]. Triple-DES [Cor00a, LMP+01]. Triples [FS01b]. Tripwire [TvdK+01]. trivial [KO00]. troubleshooting [HJW05]. True [BST03, Cha04, DV08, EEK+03, HBF09, Pan07, SFD06, BG08, BG09, GB09, Hau06, HLwWZ09, Ste05c, vT01, VKS09]. Triplecrypt [CSK+08]. truly [BGL+03]. Truncated [CS05b, KM02, LHL+02, SKU+00, SKI01, GS09]. Trust [CHSS02, HCD002, Lin00b, LHL+08, Mit02, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, 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 [Bone00]. Turkish [DD02]. Turn [Tsa07]. Turning [DJLT01]. tutorial [Can06a, Puc06, Rot02b, Rot03, vT00]. Tweakeable [DS08, HR03, LWW02]. 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, HLT01, HL05b, JZCW05, KCP01, KO04, KTC03, KI03, Lin01c, MR01a, ML03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, St.00, Ste05a, Ste01, TW07, WW05, XS03, YWWD08, YWDO01, CLOS02, DHL06, GCKL08, HW03c, JW01, LMTV05, MS09c, MCH03, MCHN05, Pau01, Pha06, ZLX99, dBT07]. Two-Block [KCP01]. Two-channel [MS09c]. Two-factor [Hen06b, Sch05c, St.00, Ste05a, YWWD08, dBT07]. Two-Key [KIO3]. 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, Mun00, SKW+00]. Type
[CKQ03, Dug04, Höf01, 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, CM02, 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 [Ano03c]. Unbalanced [FMP03, May02, HLLL03]. 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, WQW01, CHC05, LH04, LCZ05a, SSM+08].

undergraduate [AA04b, Gha07]. undergraduates [DFGH04].

Understanding [AN03, CPG+04, Cra05b, Elb09, Gor06, LG09, PP09, Sun05, Lun09].

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

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

Uniform [SPK08, TL07, SU07]. uniformity [SHP01, SHF04b]. Unimodular [CV03].

Unique [Lam91, Lys02, TH01]. United [DFCW00, Jol01]. Universal [BOHL+05, CR03, CJNP02, CS02, Ifr00, KKKP05, KO03, Pli01, Sho00a, SP79, Cal00c, PS04c].

universality [DS02]. Universally [AF04b, BLDT09, CF01a, Can01a, CK02b, CLOS02, DN02b, DN03, NOM05, RK05].

Universally-Composable [AF04b]. Universiteit [BBD09]. University [Cac02, Puc03, Rot07, Top02]. UNIX [CCDP01, Har01a, Har01b, Höf01, Witt01, GSS03]. UNIX-Type [Höf01]. Unknown [CT08a, Luc02b, CWS05, HJ07].

Unknowns [CMB+05]. unleash [McN03]. Unleashing [Lop06]. unlinkability [WHH05].

Unpredictability [BS01d]. unprotected [ASK05]. Unravelling [Ano03c]. Unsolved [GG05a, Bel07a]. untold [DB04].

untraceability [CL09, LHY05, Par04]. Untraceable [ACD05]. Untrusted [BMK00, CGK+02, LSV09, LLK05, ZBP05].

Unusual [GG05a]. Unveiled [Bar00a].

Update [TEM+01]. Updated [Cho08a]. upgrading [LH03]. upgrade [Pau02a, Pau02b]. Upgrades [Ano02c].

upon [DFF01, PQ03a]. UPPAAL [BBD+02]. Upper [BP03b, DIRR05, KMT01]. Upwards [CV03]. URSA [LKZ+04]. USB$54 [Duw03].

USA [ACM03b, ACM04b, ACM05c]. ACM06, ACM07, ACM09, BD08, Des02. Fra04, HR06, IKY05, Joy03b, JQ04, Jue04, KKP02, KJR05, Kil05, KP01, Men05. Men07, Nac01, Nao04, Oka04, Pio06, Pre02c, Sch01d, Sho05a, Si01, YDK06, ACM10, Bel00, Bon03, BCD09, ELvs01, FMA02, IEE01a, IEE05a, IEE05b, IEE08, IEE09b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SMF+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, FDIR00, Had00, HY01, KZ09, LSZ05, MR03, OHB08a, PS01b, Poh01, Sas07, SSM+08, Str01a, Tsao1, WDCJ09, BMM00, CL04d, CKY05b, CKY05c, Che07, CKY07, Che08a, Che08b, CJ04, CKK03, Cos00, DZL01, Dan02, DSGP06, DS09, DFG00, FWTC05, GC00a, GMR05, Gen09b, GS09, HHSS01, HW05, HAU04, HTW07, Hir09, HW04, HLTC09, HY03, HL04, JRR09, Jua04, KOY09, KCO0a, KLY03, KB09, KKL09, KKI+07, KSW06, KR03, Ku04, KC05, LHY02, LLH02, LKY04, LCP04, LL04b, LW04, LKY05a, LL05, LLW05, LFW04, LC05a, LLC06a, LWK05a, MT07, Mic01, NS05a, Pae03, PS04a, PY08, PCS03, PCC03, PC05b, Pha06, RC05, Sco04, SBS09, Sha04b, Sha05b, SLH03, SHH07, Tan07a, TLH05, Tsao5, TJC03, VK08, Wan04b, WK05, Wan05, WGL00, WH03, YW04a, YW05, YC09a, YPYR05a, VZE009, YC07, ZW05a, ZF04]. utilising [RFR07a, RFR07b, RFR07c]. utility [Gua05]. Utilizing [St02].

\[ \text{vOT08} \]

User-Centered [CMB+05].
user-controlled [LAPS08]. user-drawn [vOT08]. user-friendly [SZS05, WLT05a]. user-level [SS03]. Users [CMB+05, 2005].

\[ \text{v1.1} \] [RSA00d]. \[ \text{v1.5} \] [CJNP00]. \[ \text{v1.7} \] [RSA00b]. \[ \text{v2.0} \] [Man01, RSA00c]. \[ \text{v2.1} \] [RSA02]. \[ \text{v2.11} \] [RSA01]. \[ \text{v2.5} \] [Ito00]. \[ \text{v5.1a} \] [CSK+08]. Vail [BC01]. valid [Wan04b]. valid-signature [Wan04b]. Validation [ABRW01, BLM01, KCJ+01, BGO09, ME08b, VM03]. Validity [Zho02].\[ \text{Value} \] [BR09, G0505, L0505, BMW02a, CK05, WWTH08]. valued [DZL01, MS02b].\[ \text{Vancouver} \] [IEE02]. Varadaraj [CJT03].

\[ \text{Varadharajan} \] [MS03a]. variable [SV08a]. Variables [HR04a]. Variant [Luc02b, NSK05, Ber08, Duj08, Duj09]. Variants [BDK+09, DG02, KS00b, CJ05, Sha04b, TJC03]. Varieties [RS02]. Variety [AOS02].\[ \text{Vascular} \] [BDhKB09]. Vaul [SHL07]. Vector [AS08, Che01c, DNP07, SBG02, WC04, Pei09, mSGF05, W0505, VC05]. vectors [LHL04a].\[ \text{Vegas} \] [ELvS01, IEE01a].\[ \text{Vein} \] [BDhKB09]. Vendors [Pau03, MV03b].\[ \text{Venona} \] [Ben01b, Ben04].\[ \text{Verenigde} \] [dL00].\[ \text{Veridicom} \] [Anon02].\[ \text{Verifiable} \] [ANR01, Ate04, CD00a, CS03a, CH05, Cha04, JLL02, JG01, Lys02, NC05, OS07].
NZS05, NSNK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a. Verifiably [BGLS03, Hes04a], verifiably-encrypted [Hes04a]. Verification [AADK05, Ara02, BPST02, BP05, GMV01, GL00, Gut02b, Gut04a, HW01, Hoe01, Str01a, BD04a, CC05b, CJL06, 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, HL00, SV00a, Sha01d]. Verlag [Eag05, Lee03a, Lee03b, Pap05]. Version [Bol02, HPC02, OST05, SKI01, Mis06]. Versions [HSR01, NPV01, An006f, CV05]. Versteckte [Sch09]. Versus [Mad00, Rub00, WWL02, ASW01, BJL092, DBS01, WPP05]. Vertically [DN04]. Very [AAC01, B02, CG03, EBC00, FLA03, H001, PM02, PBMB01, Zir07]. Vestiges [Top02]. Vl [Sch04a]. via [AGKS07, An00ok, ACdM05, BDPV09, Car02, Che03, CPG04, FBWC02, Fox00, HHYW07, HLM03, J000a, KT06, ML05, PG05, RG05, SB01, SLG05, ZL01, Lud05]. Victoria [ACM08, IZ00]. Victorian [Top02]. Victoria [Hau03]. Vid [CAC06]. Video [BDF01a, BD03, CDTT05, EFY05, ISS08, KBD03, KJR05, KLI01, LHS05, MLC01, SC02a, BS01b, CO09a, J002, KN03, UP05]. Video-Based [KJR05, BS01b, KN03]. videos [YZD07]. Vienna [BZ02]. Vietnam [Lov01]. View [Bar00a, Mah04, Sin09]. Views [Bar00a, Bar00b, Bar00c, Coc01a, Coc02a, Coc02b, Coc03]. Vigenère [DG00]. VII [Sch04b]. VIII [IEE01b, Sch05a]. Virginia [MS05b]. Virtual [An001c, HM01a, Pro00, YSS01, BDS09a, ML05, ZBP05]. virtualization [CGL08a, CGL08b, CGL08c]. virtualization-based [CGL08a, CGL08b, CGL08c]. Virtues [Tro08]. Virus [Gor06, An005c]. Visible [HT06]. Vista [Fe06]. Visual [BDN00, BDDS03, BCD06, CCL09, CTO09, CPO06, DD00, Kog02, KS03, RD09, WMS08, WYC08, YC01, ZP05, ABD01, CDFM05, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Z010]. Visualization [XYL09, MFS09]. Viterbi [LBSG01, LBSG02]. Vladimirov [Puz04]. VLDB [EBC00, FLA03]. VLDP [B02]. VLSI [EBC00, FLA03]. Voice [An000l, PK01, VN04]. VoIP [An008c, SZ08, VAVY09, WC005]. volatile [SETB08]. Volume [Gol04]. Vortrag [Eke02]. Voter [Cha04]. Voter-Verifiable [Cha04]. Voting [Cha04, FPS01, HS00, Joh05, JLL02, KMO01, Rub01, CJT03, HJW05]. Voyich [Rug04]. VPN [KMM06]. VPNS [Dav01a]. VQ [WJP07]. VQ-based [WJP07]. Vs [CTB01, Di01, Di03, SU07, WW04]. VSS [AF01b, CDF01, FM02a]. Vu [DP00]. vulnerabilities [CSW05, DMS05, Swi05, XNK05]. vulnerability [KHL09, SGA07, YRS09]. WA [ACM06]. WACs [Kov01]. Wagner [DVP06]. Wagstaff [Kov05b]. Wahab [MAAT07]. Walking [Fox00]. Wallet [ETZ00, JL04]. Walsh [MS02b]. Walsingham [Bud06]. WAN [H601]. WAN-Cluster [H601]. Wang [SZS05]. Wants [Hau00]. WAP [JRFH01]. War [Bec02, Bud00a, Bud02, Han03, Kov01, MH09, OC03, AJ08, DB04, Ris06, Lov01]. Warfare [HW01, WW04]. warrior [P004]. 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 [AS01h, GMV01, JX05, KHY04, Kwo03a, Meh01, PBB02, RE02,
SY01a, CAC03, TH01, WY02, Zan01, AA08, CL08, LYG07, LCC06a].
Watermark-based [Kwo03a].
Watermark-Fingerprint [KHY04].
Watermarked [ST01c]. Watermarking [AS08, AK02b, AHK03b, AS01c, Arn01,
ARC+01, BBC09, BR09, BSC01a, BSC01b, BSL02, BQR01, BSNO00, CC02a, CH01b,
CT05, CT09, CT02, CM02, CM8+08, DWN01, DNP07, EFY+05, EIG01, GW01,
HT06, HH09, JK+01, KCR04, kKL00, KLL01, Knu01, KTO0, LZ09, LLS05a,
LKLK05, LZ01, LYP+04, LWS06, LJ05b, LSC03, LL01, LSKC05, MM01a,
MNS01, Nah01, OMT02, PJJ01, PKJ01, PR01, PB+07, Qn01, Sam09, SOHS01,
SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SF04, SLO01, SP08, VVS01, VHP01,
VK07, WC09, WH09, WNY09, WWL+02, WLT05b, XFO01, YWWS09, ZTP05,
ZWC02, AHK03a, AAPP07, BCKK05, CC02b, Che08b, CYY+07, CDD+04, CS05a,
CC04c, CM02b, CKL05, DSP01, FWL08, FMS05, GA03, HLC07, HHC05, JD01,
JA02, KA09, KP00, LDD07, Lin00a, Lin01b, LLC06, LLC06b, MB08, MCH05].
watermarking [PK03, Ren09, mSgFtL05, WJP07, WNQ08, Way02b, Way09, WC05, WMDM08,
XMST07, YZDW07, YPSZ01, ZLZS07].
Watermarks [Ben00, BB00a, MLC01, Sug01, WC03a, WC04, YLLL02, MB08, TND+09].
Watershed [FBW01].
Watershed-from-Markers [FBW01].
WAV [XFZ01]. WAV-Table [XFZ01].
Wavelet [BR09, GW01, LKLK05, 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, LWTW05, Sho00a, YZ00,
AK02a, AGGM06, AGGM10, BYJK04, CH05b, CJ04, Cla00b, GKK+07, HR07,
HRS08, JZ09, KKO7, KKKP05, KK03, LW04, LPM05, LQ08, LKLJ01, Mic02a,
Po00, Tsa08, YW05, YRY05b, ZW05a].
Wayness [KI01a, PV06b]. Ways [BB02].
WCC [Ytr06]. WDDL [MMMT09]. Weak [HG03, LS01c, RW03b, DW09, GG08,
KOY09, KW00]. Weakening [ZD05].
Weakly [BS00a, CHS05]. Weaknesses [SW05, SZZ05, YPKL08]. Weaknesses [FMS01, He02, KCL03, KCC05, SGGB00].
Weapons [RR03b]. Weather [WWL+02].
Web [Mar05a, BFG05, BFG08, Hil06, Ano01c, Ano02e, Ano03c, AVE+07, BFG04,
BC04b, CCCY01, Ccoc01a, Coc02a, Coc02b, CZB+01, DeL07, DMSW09, FSSF01, GS02a,
GVSC02, HM05, JRB+06, KCD07, LWK00, LLS05b, LXM+05, MMPM09, PM00, RR04,
Sam09, SS006, Sch01a, SBG07, TMM05, WA06, YSS+01]. Web-Based [An01c, Sch01a, YSS+01]. Web-enabled [CCCY01]. webcam [McN03].
WebFountain [An03c]. Webrelay [Zha00]. Weight [CH07c, GKO2, WT02].
Weighted [BTW05, BTW08, SC02c, YZ00].
Weil [BF01b, BF03, Jou02, Kir03]. Well [WWG00]. Welschenbach [Ter08]. Welsh [Rot07]. went [AJ08]. WEP [SIR04]. were [Han06]. Wesley [Puc03]. West [Fro01, Jue04, Syv02, Wri03]. Westbridge [An02e]. Western [CZB+01]. Wet [CC09].
Wey1 [Sug09]. WG [DFPS08]. WG11.1 [ELVS]. WG11.1/WG11.2 [ELVS]. WG11.2 [ELVS]. WG8.8 [DFCW].
Wheelerl [ABM08, Bar05]. Where [Bur06, Pen01a]. While [Tes06]. WHIM [JAD02]. WHIRLPOOL [RB01]. Whisper [NABG03]. Whitening [Oni01]. Whitfield
Who [CZB+01, Urb01, Hau06]. WHO [CPG+04]. Wi [Puz04, Sty04, VGM04, FMA02, Bar03]. Wi-Fi [Sty04, Bar03]. Wi-Foo [Puz04, VGM04]. wicked [Lud05]. Wide [DRO2a, SBB05]. Width [OT03b]. Width-OT03b. Wiener [Duj08, Duj09]. WIESS [USE00b]. Wiley [And04, Gra01, Kir01a]. Will [Ort00, Cla00b, Fur05]. William [Pag03]. Williams [MüL01a]. Window [OT03a, SSST06]. Windows [USE00a, DGP07a, DGP07b, DGP09, Fer06, HB06, WD01a, Wit01]. Wins [Bar00b]. Wired [Gil07, Pot07, SIR04]. Wireless [AEAQ05, Bar03, BCH’00, ECM00b, Fin06, HK05, KH01, LNL’08, Pan03, PZD09, Pot03, Puz04, Sin01a, Sty04, SYLC05, VGM04, YSR01, ZYN08, ZWY02, Bad07, BP03a, BBG’02, CCMT09, Cha05b, GW08, GG05b, HLTJ09, JRR09, KXTZ09, KB09, LDH06, LPV’09, LFHT07, LW05a, Lin07, Lop06, MJF’08, NC09, NLD08, PSCM07, Par04, Pat02a, Pat02b, Pot07, SLP07, SZ08, TP07, Vac06, Van03, Van04a, YTYW05, CS08b, ECM00a, PDM009]. Wiretapping [Cho08a, DL98, Jan08a, DL07]. WISA [CSY09]. Within [MR02a, CHM+02, MR02b]. Without [BCL+05b, Bla01c, BB04, BGH07, Har06, NA07, An003b, Ch01a, CCK04b, CYH04, CCH05, CTH08, CJ03c, CJ04, CDD07, CVN06, DK01, KG09, Ku04, LV07, LHL04b, LW04, LKY05b, LL06, Lin01a, LCZ05b, Lys07, MP02, Mar07, PS04c, RG09, Tsa08, WH01, YW05, YRY05b, ZW05a]. Withstanding [DFS04]. Wits [Bud00a, Bud02]. WLAN [SSM+08]. WLAN/cellular [SSM+08]. Woes [BTTF02]. Women [FF01b]. won [Hau03a]. Worcester [KP01]. Word [HR00, SKU+00]. Word-Oriented [HR00, SKU+00]. Word-lengths [PG05]. words [GS01, Max06, NS01a, VS01]. Work [DFG01, DNW05, Fox00]. Working [DFCW00, ELvS01, KB00]. workload [BGM04]. Works [Net04]. Workshop [ACM05a, An005c, AL06, BDZ04, BBD09, BD08, CZ05, Chr00, Chr01, CCMR02]. CCMR05, CRY09, DR02c, Des02, GH05, IEE01b, IZ00, Job03, JQ04, KKP02, KCR04, KGL04, Kiu01, KP01, KNP01, LST+05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RR05b, RM04, Sch00b, Sch01d, TB02, USE00b, YV01, Vau05a, WKP03, Ytr06, AMW07, AJO1a, BCKK05, Bir07, CKL05, GKS05, HHH04, HHH05, HAA0, ST01d]. World [Ber03, GGO05a, HW01, Nik02a, Nik02b, Sch00d, Sty04, YKM08, An03a, Ar05, Be07a, He03, HHG06, Hus01, KPS02, Kec05, Lie05, Lio09, Rob02, Rob09, Sch03, SL07, Bec02, Bud00a, Bud02, Han03, Kov01, MH09, OC03, Sty04, See04]. Worlds [Wil01b]. Worm [LJL05, CSW05]. Worms [ZGT05]. Worst [CMM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case [HRS08, Mic02a, Mic02b, Pei09]. worst-case/average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. wrapped [HLC07]. Wrapper [Ols00]. Write [BB02]. Writers [Gor06]. Writing [HL03, Jan06, Kah07a, Kah07b, Kah08, Gas01]. Writings [Cop04b]. WS [JRB+06, RR04]. WS-Policy [RR04]. WS-Security [JRB+06, RR04]. WSDL [Bar00c]. WTLS [Van02]. WTMAU [ECM00a, ECM00b]. WTMAU-SD [ECM00a]. Wu [BCW05, CHY05a, CJW01, HLL05c, MS03a, YY05b]. Wu-Lin [YY05b]. Wuhan [TTZ01]. WW [Sal00a]. WWW [WD01b].
REFERENCES

FJ04, FL01b, GA03, Her02, LC04b, PCK02, RR04, ÜG08, Uri01, UST01a. XMT [SG07].
XrML [Bar00a]. XTEA
[CV05, HK+04, MHL+02]. XTR
[LW02, LV00, LNS02, Ver01].

Yahalom [Pau01]. Yang
[McK04, CZ03, KJY05, WL05, YWC05].
Yang-Shieh [YWC05]. Yao
[BPS08, BDNN02, ZD05]. Yao-style
[BPS08]. Yarrow [KSF00, Mur02].
Yarrow-160 [KSF00]. Yaschenko [Kat05b].
YCH [SC05a]. YCN [Hwa00]. Year
[Naz02, Bur00]. Years [Ahm08, CM02].
Yellow [JYZ04]. Yen [LLLZ06a, LLLZ06b].
Yen-Guo [LLLZ06a]. Yesterday [Coc02a].
Yi [Wag00]. Yi-Lam [Wag00]. Yokohama
[Mat02]. Yoo [KCC05, KHKL05]. Yoon
[KCC05]. York
[HR06, IKY05, NIS00, Sch01d, YDKM06].
Young [FF01b]. You’re [ES00a, Nic01].
You’ve [Nic01]. Yuck [Sas07]. Yuen
[KH08].

Z [Wue09]. Z-parameter [Wue09]. z10
[Web08]. z9 [ADH+07]. Zealnd [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, KK07]. zero-day [CSW05].
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, Tuc66]. ZK [PBD05]. Zodiac
[HSM+02].

References


XX:2002:CC

Al-Akaidi:2004:FSP


Aly:2004:CSP

Alaaeldin A. Aly and Shakil Akhtar. Cryptography and security protocols course for undergraduate IT students. SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education), 36(2):44–

Agreste:2008:NAP

Santa Agreste and Guido

**Apers:2001:PTS**


**Al-Azzoni:2005:MVC**


**Anshel:2001:NKA**


**Almgren:2000:HWC**


**Ababneh:2009:CSE**


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


Aiello:2004:JFK


Abdalla:2001:DAS


Ateniese:2001:ECV


Abe:2001:SEP

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

Abe:2004:CEP [ABK00]


Abadi:2005:CFI [ABM00]


Adao:2009:SCF [ABM08]


Anderson:2000:CS


Austin:2000:ASF


Adjeroh:2008:BWT

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


ACM:2003:PTF


ACM:2003:PTS


ACM:2004:PAS


ACM:2004:PAA


ACM:2005:MPI


ACM:2005:PTF


ACM:2005:SPA

ACM:2006:PTE


ACM:2007:SPA


ACM:2008:SPA


ACM:2009:SPA


ACM:2010:PAI


Algesheimer:2002:ECM

REFERENCES


[ADI09] Jithra Adikari, Vassil Dim-
REFERENCES


[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
REFERENCES

Augot:2003:PKE


Abadi:2004:PA


Abe:2004:ASF


Atallah:2005:DEK


Ateniese:2006:IPR


Attrapadung:2006:FSS

[Nut] Nuttapong Attrapadung, Jun Furukawa, and Hi-deki Imai. Forward-secure and searchable broadcast encryption with short ciphertexts and private keys. Lecture Notes in Computer Science, 4284:161–177, 2006. CODEN LNCS9. ISSN 0302-9743...
REFERENCES


Akkar:2001:IAS

[AG01]


Acquisti:2009:PSS

[AG09]


Akavia:2010:EBO

[AGGM06]

[AGGM10]

[AGKS07]

[AGT01]

Aris Anagnostopoulos, Michael T. Goodrich, and Roberto Tamassia. Persistent authenticated dictionaries and their applications. *Lecture Notes in
REFERENCES

**Ateniese:2005:PRS**


**Armington:2002:BAI**


**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**


**Ahmad:2007:CSS**


**Ahmad:2008:ATT**


**Ahmadi:2008:PFS**

O. Ahmadi, D. Hankerson, and F. Rodríguez-

[AIK04]


[AHS08]


[AIK06]


[AIK04]


[AIK01]


REFERENCES

Al-Jarrah:2008:NKM


Abe:2002:KES


Agrawal:2002:WRD


Armknecht:2003:AAC


Akinwande:2009:AHC

REFERENCES

101

org/jucs_15_3/advances_in_homomorphic_cryptosystems]

[AKSX04]

Amir:2004:PGK


Agrawal:2002:PP


Aciicmez:2006:PSB


Agrawal:2004:OPE


Amadio:2000:RPC


Aoki:2000:FIA

REFERENCES


REFERENCES

Amadio:2002:SRP


Abimbola:2006:NSI


Alvarez:2000:CCE


Alvarez:2004:KCC


Adams:2007:SAC


Aljifri:2003:ILA

REFERENCES


REFERENCES


 REFERENCES


Anonymous. Public-key crypto-systems using symmetric-


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 (elec-


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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>Dr Nicko van Someren,</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>Anonymous. Unraveling</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>crypto developments:</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>Anonymous.</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous.</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>L. Euler</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>E. Fauquembergue</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1750</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1950</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1952</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1976</td>
<td>L. Euler</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1976</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>1976</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>1976</td>
<td>E. Fauquembergue</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>25</td>
<td>21701</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>32</td>
<td>25964951</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>1976</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>43</td>
<td>3042457</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>48</td>
<td>57885161</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>49</td>
<td>74207281</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>50</td>
<td>77232917</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
<tr>
<td>51</td>
<td>82589933</td>
<td>2003</td>
<td>R. M. Robinson</td>
</tr>
</tbody>
</table>
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
REFERENCES


Anonymous:2009:TCA


Anonymous:2012:SHS


Anonymous:2013:DSS


Ateniese:2001:SRC


Amir:2001:FAA


ANSI:2005:AXP

REFERENCES


Alomair:2009:ITS


Appenzeller:2005:IBE


Applebaum:2007:CCP

Alwen:2005:IFR


Abdalla:2000:NFS


Arboit:2001:FLM


Araki:2002:NRS


Atallah:2001:NLW

Aaraj:2008:ADH
Najwa Aaraj, Anand Raghu
DEN ????? ISSN 1539-9087 (print), 1558-3465 (elec-
tronic).

Arkin:2005:CND

Arnold:2001:AWB
Michael Arnold. Audio watermarking: Burying infor-
DEN DDJOEB. ISSN 1044-789X. URL http://www.

Agrawal:2003:MCA
40833-9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN TK7895.E42. URL http://link.springer-
y.com/link/service/series/0558/tocs/t2779.htm;
issue&issn=0302-9743&volume=t2779;
REFERENCES

[Abe:2001:SPA]

[Adelsbach:2001:ZKW]

[Agung:2001:ICI]

[Asanjo:2002:AES]

[Ashburn:2003:PBA]
Julian Ashburn. *Practical Biometrics: From Aspiration to Implementation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
REFERENCES


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


Avanzi:2003:CAD


Aalberts:2000:DSB


Abadi:2005:SAC


Abadi:2008: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,
REFERENCES

Blanton:2006:SRF


Bagnulo:2002:PAA


Badra:2007:AWS


Baier:2001:ECP


Baier:2001:ECS

REFERENCES


[Baran:2000:NVM] Nicholas Baran. News and views: More on tiny transistors; Open Source repository launched; design contest promotes new software tools; and then there’s a decryption contest; Fred Brooks wins ACM Turing Award. *Dr. Dobb’s Journal of Software Tools*, 25
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

Barken:2003:HSY
REFERENCES


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


Barkan:2002:HMW


Bouda:2003:EQI


Boneh:2004:SIB


Bicakci:2005:ISA


Biham:2002:SQK


Basso:2009:NBB


Behrmann:2002:UIS


Bernstein:2009:PQC


Bellare:2001:KPP


Blumenthal:2002:SAD

[BBG+02] 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
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

Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Ho- 
vav Shacham, and Scott Yilek. Hedged public-key encryption: How to pro-
tect against bad randomness. In ??, editor, Advances in Cryptology – ASI-
ACRYPT 2009, pages 232–249. Springer-Verlag, Berlin, Germany / Heidelberg, 
Germany / London, UK / etc., 2009. ISBN ???. LCCN ???. URL ???.

Christophe Bobineau, Luc Bouganim, Philippe Pucheral, and Patrick Valduriez. Pi-
coDMBS: Scaling down database techniques for the Smartcard. In El 

Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In 
Franklin [Fra04], pages 41– ?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-
volume&id=doi:10.1007/b99099.

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

Bellare:2009:HPK

BBN9

BC01

BPPV00

Boneh:2004:SGS

Burgess:2001:ISC

Biham:2004:NCS
REFERENCES

Blundo:2004:SIA


Backes:2005:PKS


Bergadano:2005:DPL


Blundo:2005:SCN

REFERENCES

Brzezinski:2005:MRL

Bergadano:2001:CSA

Bergadano:2002:IAM

Brier:2001:CRS

Blundo:2006:VCS

Bruguera:2009:PIS
Javier D. Bruguera, Marius Cornea, Debjit Das-


REFERENCES


[Bresson:2001:PAG] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably authenticated group Diffie–Hellman key exchange — the dynamic case. Lecture Notes in
Bresson:2002:DGD


Bresson:2002:GDH


Bolle:2003:GB


Bresson:2007:PSA


Bellavista:2002:JLD

REFERENCES


[Biham:2008:BA]

[Betarte:2000:SSC]

[Bao:2005:RWH]

[Biham:2000:CAG]

[Boneh:2000:CRP]

[Bourbakis:2003:SBC]
REFERENCES


Bozzano:2004:AVS

Burmester:2004:HPK

Buchmann:2008:PQC

Biryukov:2003:CS

Blundo:2003:COT
REFERENCES


REFERENCES


[BN00] 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


[Bel07a] 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


Benson:2004:VS


Berson:2000:CE


Berson:2003:CAB


Bernstein:2007:SFS


Bernstein:2008:CVS


Bergmann:2009:DKR

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


Babbage:2001:MHO


Boneh:2003:IBE


Boneh:2001:IBE


Boneh:2001:EGS


Boldyreva:2005:ARO


Bisseling:2006:MSM

Boldyreva:2006:SO


Bhargavan:2008:CVI


Bhargavan:2008:VPB


Bhargavan:2008:VII


Bugliesi:2007:DTA

REFERENCES

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.

Boneh:2007:SEI


Bennett:2002:ESE


Bogomjakov:2008:PMD


Bertoni:2003:EAA


Barak:2001:IPO

REFERENCES


REFERENCES


[BH00a] Robert Beck and Steve Holstead. FOKSTRAUT and Samba — dealing with
REFERENCES


Bialaski:2000:SLN


Barak:2005:MAP


Badra:2006:KEA


Backhouse:2003:TOT


Bajard:2004:FRI


Barkol:2005:SCC

REFERENCES

Beimel:2005:PNS


Bi:2009:MCE


Bidgoli:2003:EIS


Biggs:2008:CII


Biham:2000:CPR


Biham:2002:HDE

REFERENCES

Biham:2003:ACE


Bajard:2003:EMG


Beimel:2000:RSC


Biryukov:2007:FSE

REFERENCES


REFERENCES


Bjorn:2005:BHM


Backes:2002:DCS


Boni:2000:NGT


Burnside:2005:CCP


Barker:2006:RRN


REFERENCES

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


REFERENCES

[159]

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

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

[Bla00]

[Blanchet:2001:ACP]
Bruno Blanchet. Abstract-
ing cryptographic protocols
by Prolog rules. Lecture
Notes in Computer Science,
2126:433–49, 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.

[Bla01a]
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 ???.

[Bla01b]
Matt Blaze. Crypto-
graphy 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:

[Bla01c]

[Blanchet:2002:SAS]
Bruno Blanchet. From se-
crecy to authenticity in se-
curity protocols. Lecture
Notes in Computer Science,
2477:342–49, 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.

[Bla02a]

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

[Bla02b]

[Blaze:2002:CI]
REFERENCES

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

[160]

Blaze:2003:FCI


[Bla03]

Bleumer:2007:EPS


[Ble07]

Bao:2006:CIB


[BLH06]

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 LNCSD9. ISSN 0302-
Brassard:2000:SAP


Bozga:2006:PBA


Buchmann:2009:PQC


Banks:2001:CAS


Blunden:2009:RAE

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


REFERENCES

Boyd:2003:PAK


Burke:2000:ASFa


Burke:2000:ASFb


Burke:2000:ASFc


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


[Borselius:2002:VTS] Niklas Borselius, Chris J. Mitchell, and Aaron Wil-


[Bernard W. Bellovin.] 2002:PAU

[Borselius:2002:PAU]


[Boyan:2005:DCC]


[Bellare:2002:TSB]


[Boneh:2000:TC]


[Bellare:2002:TSB]

**Bouganim:2008:DAC**


**Bellare:2002:PRI**


**Bouganim:2003:CSD**


**Bodycombe:1999:CC**


**Ben-Or:2005:UCS**


**Bollinger:2002:UFO**


Borras:2000:TRT


Boreale:2001:STA


Barak:2007:DC


Boyd:2001:ACA


Boyen:2003:MIB

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


Niv Buchbinder and Erez Petrank. Lower and

Bellare:2004:KEA


Blanchet:2005:VCP


Beissinger:2006:CUM


Baer:2007:CIS


Bellare:2000:AKE

REFERENCES


**Borst:2001:CSC**


**Bellare:2005:ISA**


**Boneh:2008:IBI**


**Baudron:2000:ENS**


**Backes:2008:KDM**

REFERENCES

Benerecetti:2002:VST


Brandao:2001:UEC


Bellare:2000:ETE


Black:2000:CMA

REFERENCES


References

Brustoloni:2006:LEN

Bierbrauer:2000:AIW

Biryukov:2000:CTM

Barrett:2001:SSS

Bigun:2001:AVB
REFERENCES


Biryukov:2001:SCS


Boneh:2001:UBE


Bajard:2003:ISC


Barrett:2005:SSS


Bo:2001:EID

Xiaochen Bo, Lincheng Shen, and Wensen Chang.


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

[BST03] Boaz Barak, Ronen Shaltiel, and Eran Tromer. True random number generators secure in a changing environment. In Walter et al. [WKP03], pages 166–
REFERENCES


REFERENCES


Beimel:2008:CIW


Black:2002:SCA


Buchmann:2000:CTC


Buchmann:2000:IC


Buchmann:2001:IC


Buchmann:2004:IC


Budiansky:2000:BWC


Budiansky:2000:DBU


Budiansky:2002:BWC


Budiansky:2006:HMS


Buhan:2006:FBL

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

Bulygin:2009:PSS


Burmansson:2000:TCY


Burnett:2001:CB

REFERENCES


REFERENCES


BORDERS:2005:CHP


CARRINGTON:2002:EDS


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

CADOJ:2000:DSE

REFERENCES

185

Canetti:2006:SCC


Canetti:2006:OPR


Caprara:2001:PSR


Carriere:2000:PSC

Bruno Carriere. Le passe sans contact: autopsie d’une
 REFERENCES


Carter:2001:SCT


Carlet:2002:LCC


Casey:2002:HCC


Casselman:2006:MTE


Cobas:2001:CTA


Challal:2005:HHC

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


REFERENCES


REFERENCES


REFERENCES


Chang:2004:IDA


Chang:2004:SOT


Chang:2009:PCC


Christianson:2001:PKC


Choi:2005:JMA


Christianson:2002:SPI


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 ????

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


Ceselli:2005:MAI

Cimato:2005:ICV

Cramer:2005:CMS
REFERENCES


[Chen:2005:NVW]

Chen:2005:NVW


[Ceravolo:2004:ERH]

Ceravolo:2004:ERH


[Certicom:2004:CCC]

Certicom:2004:CCC


[Canetti:2001:UCC]

Canetti:2001:UCC


[Canteaut:2001:COR]

Canteaut:2001:COR


[Cramer:2002:OBB]

Cramer:2002:OBB

Ronald Cramer and Serge Fehr. Optimal black-box

Clarke:2005:AUM


Clarke:2007:AUA


Courtois:2001:HAM

REFERENCES

link/service/series/0558/bibs/2248/22480157.htm;


**Chodowiec:2001:ETG**


**Caballero-Gil:2009:GBA**


**Catalano:2000:CIS**


**Coppersmith:2000:ICT**

REFERENCES

[Catalano:2001:BSP]

[Caballero-Gil:2006:SSB]

[Crosby:2002:CHB]

[Clarke:2002:UCP]

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


Chen:2008:OVBB


Chen:2008:OVBC


Caballero-Gil:2007:PSC


Canovas:2002:DSB

Cox:2002:SP9


Cimato:2003:SCN


Cayrel:2008:SIS


Chow:2009:ADN


Crotch-Harvey:2000:OPR


Chang:2001:TFG

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-
REFERENCE

Chen:2001:SFW

Chung:2007:ASF

Chung:2007:MRA

Chaum:2004:VSB

Chan:2005:MCM
Alvin T. S. Chan. Mobile cookies management on a

**Chandra:2005:BWS**


**Chakrabarti:2007:GCS**


**Chen:2000:JCT**


**Chen:2004:MCK**


**Chen:2005:EUG**

Chen:2001:DEU


Chen:2001:PDP


Chen:2001:NVR


Chen:2002:SFS


Cheng:2003:PPO


Chen:2004:IAM

REFERENCES

Cheng:2004:BSD

Chen:2005:TSS

Chess:2005:SAC

Chen:2007:CIS

Chen:2008:CIS

Chen:2008:MWS

Coulter:2001:GAH
Robert S. Coulter, George Havas, and Marie Hen-
References


REFERENCES

Coron:2001:GGC

Coron:2001:OCC

Coppersmith:2002:CSC

Canetti:2003:FSP
REFERENCES


REFERENCES


REFERENCES

Canetti:2005:HAW


Chen:2002:AMT


Cornea:2002:SCI


Churchhouse:2002:CCJ


Canvel:2003:PIS

REFERENCES


[Cir01] Hung-Yu Chien and Jimmy Chien.

Chien:2003:NHA


Chien:2003:RSA


Chien:2004:IAM


Chen:2005:EDS


Cornwall:2004:AAM

REFERENCES


REFERENCES


Chepyzhov:2001:SAF


Chien:2001:MRL


Chien:2002:ECS


Chien:2003:CMV


Chien:2004:SIS

Canetti:2002:SAI


Canetti:2002:UCN


Cook:2006:CEG


Cheon:2002:IID


Chung:2003:EPX

REFERENCES

**Chun:2003:DLC**


**Cox:2005:DWT**


**Coppersmith:2000:KRF**


**Coron:2000:FLA**


**Chen:2009:SRP**


[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


[Chevalier:2008:CRS]


[Cachin:2009:TC]


[Camenisch:2001:IES]

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


[CL04a] 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


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


REFERENCES

Cheon:2000:NBC

Canetti:2002:UCT

Chen:2009:AKD

Chang:2007:SIH

Clulow:2003:SP


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).

**Campo:2001:JFC**


**Chevallier-Mames:2003:FDS**


**Chao:2000:CHC**


**Cid:2006:AAA**


**Cho:2008:DNP**


[CNV06] Miguel Correia, Nuno Ferreira Neves, and Paulo

Cetin:2009:NSA


Czernik:2009:CRN


Cobb:2004:CD


Cochran:2001:NVS

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


Cocks:2001:IBE

Cochran:2002:NVSb

Cochran:2002:NVW

Cochran:2003:NVC

Cohen:2003:FOV
REFERENCES

Cole:2003:HPS


Constantinou:2000:CSC


Convery:2004:NSA


Conti:2009:GSH


Cook:2002:REJ


Coppersmith:2000:C


Copeland:2004:COO

REFERENCES

Copeland:2004:ETS


Corella:2000:FIT


Coron:2000:ESF


Coron:2002:SPP

Coron:2006:WC


Cosgrave:2000:NTC


Costlow:2003:BIM


Courtois:2001:EZK


Courtois:2003:FAA

Courtois:2004:FSB


Courtois:2002:CBC


Chatzikokolakis:2007:FAP


Cimato:2006:PVC

REFERENCES

Chow:2004:UDL

Chen:2004:SEP

Catalano:2004:IP

Canetti:2007:CSH

Ciet:2001:SFC
REFERENCES

Canetti:2003:UCJ

Cramer:2005:ACE

Crampton:2005:UDR

Crenshaw:2000:SPK

Crowley:2001:MFL


key encryption schemes
secure against adaptive
chosen ciphertext attack. [CS03c]

Christian Collberg and
Tapas Ranjan Sahoo. Software
watermarking in the frequency
domain: Implementation, analysis, and
JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Scott Contini and Igor E.
Shiparslinski. On Stern’s attack
against secret truncated linear congruential
generators. *Lecture Notes in Computer Science*, 3574:
180–206. 2005. CODEN
LNCSD9. ISBN 3-540-
26547-3. ISSN 0302-9743
(print), 1611-3349 (electronic). Information
Security and Privacy 10th
Australasian Conference,
ACISP 2005, Brisbane, Aus-
tralia, July 4–6, 2005. Proceed-
ings.

N. Cvejic and T. Seppänen.
Increasing robustness of
LSB audio steganography
by reduced distortion LSB
coding. *J.UCS: Journal
of Universal Computer
28, 2005. CODEN ????
ISSN 0948-6968. URL http://
www.jucs.org/jucs_11_1/
increasing_robustness_of_lsb.

Capaldi:2007:ADI

Chakrabarti:2007:PBA

Chatterjee:2007:CSC

Casey:2008:IFD

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 deniable file systems: Truecrypt V5.1a and the case of the tattling OS and applications. In ????, editor, Proceedings of the 3rd Conference on Hot
REFERENCES

ISBN ??, LCCN ??, URL ??.

Certified self-modifying code.
CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits.
In Meadows and Syverson [MS05b], pages 235–248.

Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009.

[CT02] C. S. Collberg and C. Thomborson.
Watermarking, tamper-proofing, and obfuscation — tools for software protection.


[CTH08] 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


<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Year</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Pages</th>
<th>Digital Object Identifier</th>
</tr>
</thead>
</table>
REFERENCES

Chang:2005:CIA


Chen:2003:AEY


Chadwick:2005:PKI


Crawford:2001:FHC


Cheng:2005:RIC

Xiaorong Cheng, Huilan 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://
REFERENCES


REFERENCES

LCCN TK5105.567 D38
200. US$49.99.

Davis:2001:DSA

Don Davis. Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML. In USENIX [USE01a], page ??
publications/library/proceedings/usenix01/davis.html.

Davis:2001:DSE

Don Davis. Defective sign-and-encrypt: Can you really trust S/MIME, PCKS#7, PGP, and XML? Dr. Dobb’s Journal of Software Tools,
www.ddj.com/.

Davis:2007:AAA

13–19, February 2007. CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371

DeBrosse:2004:SBU

Jim DeBrosse and Colin B. Burke. The secret in Building 26: the untold story of America’s ultra war against the U-boat Enigma codes.

loc.gov/catdir/samples/random045/2003058494.html;
http://www.randomhouse.com/catalog/display.pperl?
isbn=9781588363534.

DeBorde:2007:STF

20, July 2007. CODEN NTSCF5. ISSN 1353-4858
(print), 1872-9371 (electronic). URL http://

Desmedt:2001:ERD

Yvo Desmedt, Mike Burmester, and Jennifer Seberry. Equi-
tability in retroactive data confiscation versus proac-
tive key escrow. Lecture Notes in Computer Science,
1992:277–??, 2001. CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http:
//link.springer-ny.com/link/service/series/
0558/bibs/1992/19920277.htm;
http://link.springer-ny.com/link/service/series/
REFERENCES


REFERENCES


[Des00b] Anand Desai. New paradigms for constructing symmetric encryption schemes

Desai:2000:SAN


Dewson:2008:BSS


Dhem:2001:HSS

idtype=cvips.


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


[DFM04]


[DFH01]


[DPS06]


[DFPST07]

Josep Domingo-Ferrer, Joachim Posegga, Francesc Sebè, and

![Damgaard:2004:ZKP](DFS04)


![Damgaard:2005:CBQ](DFSS05)


![Damgaard:2008:CBQ](DFSS08)


![Dalkilic:2000:ICA](DG00)


![Debaert:2002:RRI](DG02)

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**

REFERENCES

CODEN JCSIET. ISSN 0926-272X (print), 1875-8924 (electronic).


[Dhe03] Jean-François Dhem. Efficient modular reduction algorithm in and its application to “left to right”


Deng:2006:OOC


Daza:2007:CTM


Dodi:2000:CSG


DiCrescenzo:2001:SOS


DiCrescenzo:2003:SOS

Giovanni Di Crescenzo. Sharing one secret vs. sharing many secrets. Theoretical 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**


**Delaune:2006:DPS**


**Donsez:2001:TMA**


**Damgaard:2001:PTR**

REFERENCES


Delfs:2002:ICP


Dodos:2005:CCS


Dunkelman:2008:TIV


Du:2005:BRS


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**


**Durfee:2000:CRS**


**Damgaard:2002:EPF**


**Damgaard:2002:PHP**

REFERENCES

[DN03]

[DN07]

[DNP07]

[DNR03]

[DN04]

[DNR05]

[D05]
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


(DODIS:2005:GIF)


(DP04) Andreas Dandalis and Viktor K. Prasanna. An adaptive cryptographic engine for Internet protocol security architectures. ACM


REFERENCES


Crescenzo:2004:CRR

Daemen:2000:NPN

Daemen:2000:BCR

Daemen:2000:RA

DDJ:2000:DDE


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

**Daemen:2001:AAR**


**Daemen:2002:AWT**


**Daemen:2002:DRA**


**Daemen:2002:FSE**


**Ding:2002:HEE**

Yan Zong Ding and Michael O. Rabin. Hyper-
Suelette Dreyfus. The practical use of cryptography in human rights groups, 2000. URL


A. Martín del Rey, J. Pereira Mateus, and G. Rodríguez Sánchez. A secret sharing scheme based on cellular automata. Applied Mathematics and Computation,
REFERENCES


[Dobber]:2005:AES


[Dev99]


[DD02]


[DD03]

REFERENCES


[DS05a] Ding:2005:RNM


[DS08] Dinur:2008:CAT


[DSGP06] Das:2006:NRU

Djurovic:2001:DWF


Dodis:2001:PAS


Duggan:2004:TBC


Dujella:2008:VWA


Dujella:2009:VWA


[dVP06] Françoise Levy dit Vehel and Ludovic Perret. On the Wagner–Magyark


REFERENCES


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


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


England:2002:AOO


Elbirt:2005:ILD


Eisenbarth:2007:SLC


Erickson:2001:EDD


Erickson:2002:EDD


Erickson:2003:HAE


Erickson:2008:HAE

REFERENCES

Ellison:2000:TRP


Ellison:2000:IRRa


Eberle:2005:ANG


Enck:2005:EOF


Ettinger:2002:QQC


Ebringer:2000:PAP


Edman:2009:AES

Matthew Edman and Bülent Yener. On anonymity in an...

Elbirt:2000:FIP


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

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


REFERENCES

Focardi:2000:ITN


Focardi:2000:MAT


Focardi:2003:CTA


Fitzi:2001:MCP


Field:2009:BCB

REFERENCES


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


REFERENCES

ISBN 3-540-24573-1 (soft-  
cover). ISSN 0302-9743  
(print), 1611-3349 (elec-  
tronic). LCCN QA76.9.A25  
openurl.asp?genre=issue&  
issn=0302-9743&volume=3378;  
[Fis05] b106171.

SCDI. ISSN 0304-3975 (print), 1879-2294 (elec-  

Marc Fischlin. On the im-  
possibility of constructing non-interactive statistically-  
secret protocols from any trapdoor one-way function. Lecture Notes in Computer Science, 2271:  
link/service/series/0558/  
bibs/2271/22710079.htm;  

Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In Shoup [Sho05a], pages 152–?? ISBN 3-540-  
28114-2. ISSN 0302-9743 (print), 1611-3349 (elec-  
tronic). LCCN QA76.9.A25  
C79 2005; QA76.9 .A25;  
QA76.9 C79 2005; QA76.9  
C794 2005; QA76.9: Inter-  
ternet. URL http://www.springerlink.com/  
openurl.asp?genre=issue&  
issn=0302-9743&volume=3621.

40674-3. ISSN 0302-9743 (print), 1611-3349 (elec-  
tronic). LCCN QA76.9.A25  
tocs/t2729.htm; http://www.springerlink.com/
REFERENCES

openurl.asp?genre=issue&
issn=0302-9743&volume=
2729; http://www.springerlink.com/openurl.asp?genre=


**Fluhrer:2001:AES**


**Faure:2006:NPK**


**Freytag:2003:VP1**


**Fox:2001:PPK**


**Fluhrer:2002:CMB**

REFERENCES


REFERENCES

Franklin:2002:PAS

Fournier:2003:SEA

Fluhrer:2001:WKS
REFERENCES


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


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

**Faugere:2009:EAD**


**Fouque:2001:SDC**


**Fournet:2008:CSI**


**Frankel:2001:FCI**

REFERENCES


REFERENCES


[Nils Ferguson and Bruce Schneier. A cryptographic evaluation of IPsec. Un-
REFERENCES


Furman:2001:CSM

Furman:2002:DCN

Furnell:2005:AOW

Fouque:2003:DAW

Furuya:2002:SAK
Feldhofer:2009:HIS


Fan:2008:RSB


Feng:2005:NMS


Fitzi:2004:PSB


Fan:2004:PPI


Furnell:2006:RPS

REFERENCES


Gasarch:2001:BRBa


Gaudry:2002:CCS


Gavinsky:2008:CIC


Guajardo:2001:EIE


Golic:2002:LCB


Gaj:2000:CHP


Goubin:2000:CTC


Gaj:2001:FIF


Goodman:2001:EER

REFERENCES


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


Gentry:2003:CBE

Gentry:2004:HCR

Gennaro:2004:MTC

Gentry:2006:RC

Gentry:2009:FHEa
REFERENCES


Gentry:2009:FHEb


Giuliani:2001:GLI


Goldstone:2005:FCR


Golomb:2005:SDG


Gambino:2008:ITW


Goldwasser:2008:CAP

Gennaro:2003:LBE


Gennaro:2005:BEG


Grothoff:2009:TBS


Gilbert:2002:SCL


Galindo:2008:SPK


Gilbert:2005:FSE


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
REFERENCES


REFERENCES


Gebhardt:2005:NPV


Gordon:2003:ATS


Gordon:2004:TEA


Ganapathy:2005:APA


Gennaro:2003:SAP


Gallagher:2006:HSB


Goldsmith:2004:CAI Clair W. Goldsmith and Rob Kolstad. A conversa-
tion about identity manage-
m;login: the USENIX Association newsletter, 29 (5):??, October 2004. CO-
DEN LOGNEM. ISSN 1044-6397. URL http://

Goldwasser:2005:PPK Shafi Goldwasser and Dmitriy Kharchenko. Proof of plaintext knowledge for the
Ajtai–Dwork cryptosystem. In Kilian [Kil05], pages 529–?? CODEN LNCSj9. ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743 (print), 1611-3349 (elec-

Gavinsky:2007:ESO Dmitry Gavinsky, Julia Kempe, Iordanis Kereni-
dis, Ran Raz, and Ronald de Wolf. Exponential separ-
ations for one-way quantum communication complex-
ity, with applications to cryptography. In ACM [ACM07], pages 516–525.
REFERENCES

Gavinsky:2009:ESO


Garay:2007:RCA


Gertner:2000:RBP


Guneysu:2008:CC


Gorodetsky:2005:CNS

REFERENCES

Goubault-Larrecq:2000:MAC


Goldreich:2001:SKG


Gennaro:2006:FPB

REFERENCES

Goshi:2006:ADM

Gassend:2004:IAI

Grebowski:2002:CAH

Gallant:2001:FPM

Gilbert:2000:CAR
REFERENCES


**[Gennaro:2002:CPG]**


**[Gilbert:2002:NRP]**


**[Galbraith:2003:IAU]**

Steven D. Galbraith and Wenbo Mao. Invisibility and anonymity of undeniable and confirmers signatures. In Joye [Joy03b], pages 80–97. CODEN LNCSD9. ISBN 3-540-00847-0. ISSN 0302-9743
REFERENCES

Gorrieri:2004:SFR


Giuliano:2000:ISC


Galbraith:2002:PKS


Goots:2001:FEA


Golle:2008:DCS


Galbraith:2001:CNR


[GN01] Rajeev Prabhakar Goré

[GN06]


[Gutmann:2005:WHC]


[Gaj:2003:FME]


[Goldreich:1999:MCP]


[Goldreich:2001:FCBB]

REFERENCES


[Goldreich:2001:FCBa]

[Golic:2001:MOS]

[Golic:2001:HCC]

[Golic:2001:CAS]

[Golic:2001:FCBa]

[Goldreich:2001:FCBa]

[Hol03]
Goldreich:2004:FCV


Goldstein:2008:BHO


Gonda:2006:NMR

J. Gonda. The number of the modulo \( n \) roots of the polynomial \( x^v - x \) and the RSA. *J.UCS: Journal of Universal Computer Science*, 12(9):1215–1228, ???? 2006. CODEN ???? ISSN 0948-6968. URL http://www.jucs.org/jucs_12_9/the_number_of_the.

Good:2000:TAE


Gordon:2002:TCP


Gurgens:2002:APF

REFERENCES


Gupta:2008:FAT


Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT

Tim Güneysu, Christof

Güneysu:2008:SPH


REFERENCES


REFERENCES


Groth:2005:CS

Gisin:2002:QC

GonzalezVasco:2001:CPK

Garfinkel:2002:WSP
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


![Geetha:2009:BIS](Geetha:2009:BIS)


![Gaubatz:2008:SCD](Gaubatz:2008:SCD)


![Goodrich:2004:ETB](Goodrich:2004:ETB)

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

Giles:2002:ADW


Garay:2000:LLB


Gennaro:2000:LBE


Guttman:2002:ATS


Goodrich:2002:EDD

Goodrich:2003:ADS


Goodrich:2008:NFI


Gutman:2004:FAP


Guar:2005:PPL


Gumz:2004:BRH


Guillou:2001:CAP

REFERENCES


Joshua D. Guttmann. Authentication tests and disjoint encryption: A design
REFERENCES


**Gutmann:20xx:ESR**


**Granger:2005:DLP**


**Gisin:2000:LCQ**


**Guoxiang:2001:IFB**

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


REFERENCES


Haddad:2000:AUA


Hancock:2000:EWP


Harvey:2000:EMA


Hare:2001:RUPa

Hare:2001:RUPb  

Harrington:2005:NSP  

Harris:2005:GHE  

Hars:2006:MIA  

Harman:2007:PDS  

Hars:2007:DIH  

Hasan:2000:LTB  
Hasan:2001:ECM

Hasan:2001:PAA

Hassler:2002:JCP

Haufler:2006:SWN

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

Hayashi:2006:QIT
Masahito Hayashi. Quan-


REFERENCES

Halevi:2002:SSE


Han:2009:ICS


He:2002:WSM


Hei:2003:BCB

Jay G. Heiser. Beyond cryp
tography: Bruce Schneier’s beyond fear: thinking sensibly about security in an uncertain world. Computers 
science/article/pii/S0167404803000051.

Heikkila:2007:ESC

Faith M. Heikkila. En
cryption: Security considerations for portable media devices. IEEE Security 
& Privacy, 5(4):22–27, July/August 2007. CODEN ???? ISSN 1540-7993
Hendry:2001:SCS


Henderson:2006:CBG


Henry:2006:TFA


Herzberg:2002:TX


Herzberg:2009:DBE

Amir Herzberg. DNS-based email sender authentication mechanisms: a critical review. *Computers*
REFERENCES


REFERENCES


REFERENCES

Hendricks:2007:LOB

Handschuh:2004:SAC

Handschuh:2005:SAC

Hung:2009:FBA
Kuo Lung Hung and Shin-Wei He. Feature based affine invariant watermarking robust to geometric distortions. Fundamenta Informaticae, 92(1–2):131–143, January 2009. CODEN FU-MAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).
Hwang:2005:TSP


Hoffstein:2006:NNE


Hess:2004:CTT


Hong:2004:DCT


Hankerson:2000:CTC

Hankerson:2001:SIE


Hamann:2001:SBA


Han:2007:FIE


Higgins:2008:NSC


Hill:2000:KII


Hilley:2006:SSD

Hacigumus:2002:ESE

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

Hirose:2009:SAD


Huang:2005:ASE


Huhnlein:2001:TPN


Hinkelmann:2007:CUN


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
REFERENCES

Kim:2000:RMW

Heuberger:2005:AGE
Clemens Heuberger, Rajendra Katti, Helmut Prodinger, and Xiaoyu Ruan. The alternating greedy expansion and applications to computing digit expansions from left-to-right in cryptography. Theoretical Computer Science, 341(1-3):55–72, September 5, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Hofmeister:2000:COS

Handschuh:2001:ASE

Hiltgen:2006:SIB
Horwitz:2002:THI


Howard:2003:WSC


Hwang:2004:REL


Hohenberger:2005:HSO


Hwang:2005:TAU


Hwang:2005:SHW


Hwang:2005:STH

[HL05d] Shin-Jia Hwang and Hao-
REFERENCES


Seokhie Hong, Sangjin Lee, Jongin Lim, Jaehul Sung,

Han:2002:DMA


Hwang:2004:KAS


Hwang:2005:GTS


Hwang:2003:TRB


Hwang:2003:TRB

Herzog:2003:PAK

Hwang:2001:TSB

Huang:2009:OSW

Hopper:2002:PSS

Hu:2009:TRN
REFERENCES

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

Hamdy:2000:SCB


Hartel:2001:FSJ


Hirt:2001:RFU


Harbitter:2002:MAP


Hevia:2002:PSG


Hitchcock:2002:NEC

Yvonne Hitchcock and Paul Montague. A new elliptic curve scalar multiplication algorithm to resist simple power analysis. Lecture Notes in Computer Science, 2384:214–??, 2002. CO-
REFERENCES


[Haastad:2004:SAR] Johan Håstad and Mats Näslund. The security of all RSA and discrete log...

**Harnik:2006:CNI**


**Haitner:2009:SHC**


**Hanaoka:2002:HNI**


**Hoepman:2001:SKA**


**Hofinger:2001:LBE**

REFERENCES

Honary:2001:CCI


Hook:2005:BCP


Honary:2001:CCI

Honary:2001:CCI


Huhnlein:2001:ICB

Han:2002:CMV


Hoffstein:2001:NNL


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**


**Halevi:2003:TEM**


**Hawkes:2004:RVC**


REFERENCES

**Hromkovic:2005:DAR**

**Hromkovic:2009:AAH**

**Haneberg:2002:MSS**

**Hemaspaandra:2008:EDA**

**Hirt:2000:ERF**

**Hinsley:2001:CIS**
F. H. (Francis Harry) Hinsley and Alan Stripp, editors.
References


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

Halderman:2008:LWR


Hanaoka:2002:USA

REFERENCES

Hanaoka:2006:USA


Hernandez:2002:GCT


Hwang:2001:LCT


Hong:2002:PSR


Hong:2002:IDC

Hernandez:2001:DTR


Hernandez:2004:STN


Hess:2001:TTH


Hsu:2005:CIT


Hsu:2005:UFR

REFERENCES

Hasan:2009:PHF


Hanaoka:2000:USD


Hanaoka:2001:EUS


Halpern:2004:RSS


Huang:2006:CSV


Hongfeng:2008:ECP

Hamalainen:2002:GPS


Hines:2007:AIF


Hofheinz:2005:CTN


Hughes:2002:LAA


Hughes:2004:ISE


Huhnlein:2000:EIC

[Hüh00] Detlef Hühnlein. Efficient implementation of cryp-

[Hun05]

[Hus01]

[Hus04]

[Hut01]

[HV04]

[HV09]
Sean Hallgren and Ulrich Vollmer. Quantum
REFERENCES


Hopper:2009:PSS


[HW98]


[HW03a]

Hardy:1998:ITN


Hellekalek:2003:EEC


[Hwu03c]

Hsu:2003:CIT

REFERENCES


Hardy:2009:AAC


Hsu:2002:IGT


Hsu:2003:ITP


Harkins:2005:ESU

Hirose:2001:UAS


Hwang:2003:CAL


Hwang:2003:ASM


Han:2005:PJIb


Han:2005:PJI


Han:2005:PIJ
Huang:2005:EMP


IBM-MARS-Team:2000:MAS


IEEE:2000:ASF


IEEE:2000:IPH


IEEE:2001:ISF

IEEE:2001:EIW


IEEE:2002:PAI


IEEE:2003:PAI


IEEE:2004:PAI

IEEE:2005:AIS


IEEE:2005:PIS


IEEE:2006:AIS


IEEE:2007:PAI


IEEE:2008:PAI

IEEE Computer Society order number P3436.

IEEE:2009:ISI


IEEE:2009:PAI


Itoi:2001:SIS


Ifrah:2000:UHN


Iglesias:2002:NSB

REFERENCES

[Bassham:2000:ETA]
Lawrence E. Bassham III.
Efficiency testing of ANSI
C implementations of round
2 candidate algorithms
for the Advanced Encryption
Standard. In NIST
[NIS00], pages 136–148.
ISBN ???. LCCN ???
gov/encryption/aes/round2/
conf3/aes3conf.htm;
http://csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-1.pdf;
http://csrc.nist.gov/
encryption/aes/round2/
conf3/papers/AES3Proceedings-
2.pdf; http://csrc.nist.
gov/encryption/aes/round2/
conf3/papers/AES3Proceedings-
gov/encryption/aes/round2/
conf3/papers/AES3Proceedings.

[Itoh:2003:PCA]
Kouichi Itoh, Tetsuya Izu,
and Masahiko Takenaka.
A practical countermeasure
against address-bit differential
power analysis. In Walter et al. [WKP03], pages
382–396. CODEN LNCSD9.
ISBN 3-540-40833-9. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
TK7895.E42. URL http:
//link.springer-ny.com/
lk/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.

[Iwata:2000:PAF]
Tetsu Iwata and Kaoru
Kurosawa. On the pseudorandomness of AES final-
ists — RC6, Serpent, MARS
and Twofish (abstract only).
In NIST [NIS00], page 9.
ISBN ???. LCCN ???
gov/encryption/aes/round2/
conf3/aes3conf.htm;
http://csrc.nist.gov/encryption/
aes/round2/conf3/papers/
AES3Proceedings-1.pdf;
http://csrc.nist.gov/
encryption/aes/round2/
conf3/papers/AES3Proceedings-
2.pdf; http://csrc.nist.
gov/encryption/aes/round2/
conf3/papers/AES3Proceedings-
gov/encryption/aes/round2/
conf3/papers/AES3Proceedings.

[Iwata:2001:PAF]
Tetsu Iwata and Kaoru
Kurosawa. On the pseu-
dorandomness of the AES
finalists — RC6 and Ser-
pent. Lecture Notes in
Computer Science, 1978:
231-??, 2001. CODEN
LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
lk/service/series/0558/


com/openurl.asp?genre=


REFERENCES

Izmerly:2006:CCA


Izotov:2001:COC


Imrey:2003:BRC


Inamori:2002:SPB


Inamori:2002:SPT


ISO:2004:IIb


ISO:2005:IDM


Iqbal:2008:CDV


Inoue:2008:FAC


Ishai:2003:PCS

Itoi:2000:SCI


Itoi:2001:SCS


Iwami:2008:AIA


Imai:2000:CPC


Irwin:2005:PAI


Iwamoto:2006:SSR


Iwata:2002:NCP

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


Imai:2000:PKC


Judge:2002:WWM


Jablon:2001:PAU


Jackson:2000:SCQ

REFERENCES


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


Jaeger:2004:CAA


Juels:2001:RKG


Johnson:2007:EIS


Jakobsson:2000:MMS


Jaulmes:2000:CCA


Jaulmes:2000:NC

REFERENCES


**Johansson:2000:FCA**


**Jaulmes:2001:CPN**


**Jonsson:2002:FCA**


**Jakimoski:2001:ASR**


**Jakimoski:2001:CCB**


**Jakimovski:2002:CS**


[JKS02] Kahil Jallad, Jonathan

Joux:2003:IGN


Juang:2004:FBT

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


Juang:2002:VMA

Jakobsson:2003:FMT

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

![Image of a page from a document with text]


**Jakobsson:2007:DPD**


**Joux:2002:BAA**


**Johnson:2000:AFR**

REFERENCES


[Joh03]

[Joh05]

[Jol01]

[Jon08]

[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

Jakobsson:2002:MAL


Jaulmes:2002:SHG


Joye:2003:GFA


Jakubowska:2007:MCT


Jiang:2004:FAP

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


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

**Jin:2001:WCS**


**JRFH01**

**Jaworski:2009:RKP**


**JRR09**

**Jarecki:2005:FSP**


**JSJ01**


**Jongkook:2001:NUS**

Jiang:2005:SAI

Joye:2001:PAD

Joye:2001:CEN

Joglekar:2005:PEM

Juang:2004:EPA

Juels:2004:FCI
Ari Juels, editor. Financial Cryptography: 8th International Conference, FC 2004, Key West, FL, USA, February 9–12, 2004: Revised Papers, volume 3110 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Hei...

Junod:2005:SCB

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

Jutla:2001:CAF


Juels:2005:APD


Jeng:2006:EKM

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


**Jiang:2005:TMD**


**Kamel:2009:RSW**


**Kadrich:2007:ES**


**Kah67a**


**Kah67b**


**Kah74**


**Kah96**


**Kak:2006:TSQ**

Subhash Kak. A three-stage quantum cryptogra-
CODEN FPLET. ISSN 0894-9875 (print), 1572-9524 (electronic).

Kanda:2001:PSE

Kapera:2005:MRP

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

Katos:2005:RTB


Katz:2005:CBR


Kendall:1939:TRS


Kovacich:2000:HTC


Kiely:2006:SSM


Kamvar:2007:DTM

Kim:2009:DCA


Kachris:2003:RLB


Keller:2009:ECC


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


Keefe:2005:CDS


Kelsey:2000:KST


Kelsey:2002:CIL


Kellar:2005:NRR


Kenyon:2002:DNR


Kenyon:2002:HPD

REFERENCES

[409]

Kettani:2006:CBN


Kelsey:2000:CPL


Kiltiz:2009:DCC


Katsikas:2004:PKI


Kaps:2007:CSD


Kovacich:2003:MHC

Gerald L. Kovacich and Edward P. Halbozek. The manager’s handbook for corporate security: establishing and managing a successful assets protection program. Butterworth-Heinemann, Boston, MA,
REFERENCES


Kim:2005:SMA


Kato:2008:QSC


Khw:2005:EDA


Komninos:2001:ESC


Kwon:2005:CLK


Koo:2009:SVN

Woo Kwon Koo, Jung Yeon Hwang, and Dong Hoon Lee. Security vulnerabili-

**Kirovski:2004:DWF**


**Kausar:2008:SEK**


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


Kidwell:2000:SNC


Kida:2002:PGR


Kilian:2001:ACC


Kiltz:2001:TBC


Kilian:2005:TCS

Kim:2001:PKC


Kim:2002:ISC


King:2000:IMP


King:2001:CMF

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

King:2002:RGI


Kirkby:2001:CCW


Kirtland:2001:INC


Montgomery:2003:FEC


Kocarev:2001:LMB

Kanade:2005:AVB


Kim:2005:IYA


Kim:2002:NIS


Klein:2003:FOW


Kawachi:2006:PQC


Kashefi:2007:SZK

REFERENCES


REFERENCES

getpdf/servlet/GetPDFServlet?filetype=pdf&id=APCPCS009630000020005710000011&
idtype=cvips.


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


Kim:2003:IBP


Knudsen:2000:CRA


Knudsen:2001:CRR


Kim:2001:NPK

Knudsen:2001:CPL


Kanda:2002:SCA


Koblitz:2004:OTS


Koblitz:2004:SPK


Koblitz:2005:PBC

Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. Report ??, Department of Mathematics, Box 354350, Univer-
REFERENCES

Kornerup:2007:PIS


KML+02


KMM+06


KMO01


Klarlund:2001:MIS

Nils Klarlund, Anders Möller, and Michael I.
REFERENCES


Klimov:2002:ANC


Keliher:2001:IUB


Kim:2003:RCC


Kittler:2003:AVB

REFERENCES


Knutson:2007:BPS

Kushilevitz:2000:OWT

Komano:2003:EUP

Katz:2004:ROS
REFERENCES


Koblitz:2000:TQC


Kocher:2002:IS


Koga:2002:GFR


Kurosawa:2001:ICP


Kornblum:2009:IBD


Koshiba:2001:NAS

Koshiba:2001:SRS


Koskinen:2001:NIK


Kovach:2001:BCB


Kovacic:2003:ISS


Katz:2001:EPA


KOY01]


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


Kuramitsu:2002:ETC


Krause:2003:DOC


Kozaczuk:2004:EHP


Katz:2005:MIA


Kiltz:2005:TCL


Kissner:2005:PPS

Klivans:2009:CHL

Kelsey:2000:YND


Kogan:2006:IER

Ku:2003:TSA

Kobayashi:2007:AIG

Kuhn:2000:PCL

Kuhn:2001:CRR

Ku:2004:HBS
References


REFERENCES

Kusters:2002:DCP


Kuo:2001:AOS


Komninos:2007:ALS


Kejariwal:2009:ELL


Koshiba:2000:SEP

[Takeshi Koshiba and Osamu Watanabe. Strong encryption of public key cryptosystems based on weak randomness hypotheses. Sūrikaisekikenkyūsho Kōkyūroku, 1148(1148):118–123, 2000. Theoretical found-
REFERENCES


Kumar:2006:ODS


Wong:2001:MCC


See comment and reply [ÁMRP04, WLW04].

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

[KY02a] 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,

**Kabatnik:2001:LSD**


**Kamp:2003:DEB**


**Kamp:2007:DEB**


**Kumar:2009:UAU**


**Ladd:2006:SPS**

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

Lafe:2000:CAT

Laih:2003:ACA

Laird:2007:THL

Lai:2008:JIA

Lamont:1991:UFC

Lam:2001:CCN
Kwok Yan Lam. *Cryptography and computational number theory*, volume 20 of *Progress in computer*


Landau:2004:SLE

Susan Landau. Security, liberty, and electronic communications. In Franklin [Fra04], pages 355–?

Laud:2008:CSC


Laughlin:2008:CRC


Lavington:2006:FCD


Lavoué:2009:LRM

Lawton:2005:MAH


Lawson:2009:SCA


Lawson:2009:TAG


Li:2004:QAU


Lindskog:2005:DIT


Lee:2000:UBN


Leveiller:2001:CNF

Leveiller:2002:CNF


Laufer:2000:SSC


Laih:2003:COP


Lin:2004:SOT


Lu:2004:XMS

REFERENCES


REFERENCES

**Levi:2004:UNC**


**Lee:2004:DEB**


**Lim:2009:OPG**


**Li:2008:CAM**


**Lu:2005:TUS**


**Lu:2005:PBM**


**Lu:2005:RTP**

REFERENCES

Li:2001:CCB


Lai:2004:SGS


Lavoue:2007:SSW


Law:2006:SBB


Lindquist:2004:JCS


Lee:2001:AES


Lee:2003:BRBa


Lee:2003:BRBb

vol 17, by Oded Goldreich. Springer Verlag, 1999.
DEN SIGNDM. ISSN 0163-
5700 (print), 1943-5827
(electronic). See [Gol99].

Lee:2003:CS
Michael Lee. Cryptanalysis of the SIGABA. Master
of Science in Computer Science, Department of Com-
puter Science, University of California, Santa Bar-
bara, Santa Barbara, CA, USA, June 2003. viii + 49
pp. URL ucsb.curby.net/

Lee:2004:SPM
Hyang-Sook Lee. A self-pairing map and its app-
lications to cryptography. Applied Mathematics and
Computation, 151(3):671–678, April 15, 2004. CO-
DEN AMHCBQ. ISSN
0096-3003 (print), 1873-
5649 (electronic).

Lee:2004:ACA
Pil Joong Lee, editor. Advances in cryptology, ASI-
ACRYPT 2004: 10th In-
ternational Conference on
the Theory and Applica-
tion of Cryptology and In-
formation Security, Jeju Is-
land, Korea, December 5–9,
2004: Proceedings, volume
3329 of Lecture Notes in
Computer Science. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
ISBN 3-540-23975-8 (pa-
paperback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
I555 2004; QA75.5 .L48
no. 3329. URL http://
springerlink.metapress.
com/openurl.asp?genre=
issue&issn=0302-9743&volume=
3329; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b104116.

Lehtinen:2006:CSB
Rick Lehtinen. Computer
Security Basics. O’Reilly
& Associates, Inc., 103a
Morris Street, Sebastopol,
CA 95472, USA, Tel: +1
707 829 0515, and 90 Sher-
man Street, Cambridge, MA
02140, USA, Tel: +1 617
354 5800, second edition,
306 (est.) pp. LCCN ????
EUR 38.00.

Lenstra:2001:USM
Arjen K. Lenstra. Unbe-
lievable security. matching
AES security using public
key systems. Lecture
Notes in Computer Science,
2248:67–??, 2001. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
REFERENCES


[Lew00] Robert Edward Lewand. Cryptological Mathematics. [LFW04]

Lee:2003:PKB


Liaw:2004:SPA


[Lyda:2007:UEA] 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


REFERENCES


Li:2005:ABPa

Li:2005:CRW

Lin:2005:RTI

Linn:2000:TMM

Lin:2001:HKA
REFERENCES

Lin:2001:DWM


Lindell:2001:PCT


Lingmann:2002:DSK


Lindell:2003:SCC


Lin:2007:PFT


Lee:2005:IEC


REFERENCES


References


[LL05c] Ying Li and Jintao Li. Further cryptanalysis of a remote login authentication scheme based on geometric approach. In Han et al. [HYZ05b], pages 143–?


[LLCL08] Shujun Li, Chengqing Li, Guanrong Chen, and Kwok-
REFERENCES


Lee:2001:PB


Lee:2002:RUA


Li:2001:SPD

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
Lee:2002:SEC


Lee:2004:MPA


Li:2006:ESY


Li:2006:SYG


Lindell:2002:CAB

REFERENCES


REFERENCES

Li:2005:ATN

Li:2008:ATN

Liu:2008:DEA

Liu:2008:SAM

Lee:2006:DCK

Linares:2000:SAM
Lorenz:2002:SSG


Lorenz:2002:SSG

Lavasani:2008:IFA


Lavasani:2008:IFA

Li:2003:SCE


Li:2003:SCE

Lamenca-Martinez:2006:LNP


Lamenca-Martinez:2006:LNP

Leitold:2001:MTN

REFERENCES

Lepinski:2005:FZK

Laskari:2007:AEC

Laskari:2005:TTC

Lu:2005:CCA

Li:2005:BPC
REFERENCES


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 —
REFERENCES


[LW06] 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.

Loidreau:2001:WKM


Li:2005:ULC


Liang:2005:FAG


Liu:2008:GPV


Lopez:2007:SCB


Lin:2003:DBI

REFERENCES


[LSVS05] Zhenkai Liang, Weiqing Sun, V. N. Venkatakrishnan, and R. Sekar. Alcatraz: An isolated environment for experimenting with untrusted software. ACM Transactions on Informa-
REFERENCES

477

Lee:2000:ASC

Li:2005:ISS

Lin:2004:SIS

Lee:2001:EPI

Liu:2005:RBU

Liu:2005:HAO

Lee:2001:EPI


REFERENCES

Lu:2002:HEA

Lu:2007:NSC

Luc:2000:ASR
Stefan Lucks. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys.

Luc:2002:VCS
REFERENCES

Lucas:2006:PGE


Ludvig:2005:PWF


Lukyanov:2001:PFA


Lunde:2009:BCU


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

Lenstra:2000:XPK


Lu:2004:FCA


Laguillaumie:2007:MDV


Lange:2002:PIE


Lee:2004:IAK

Narn-Yih Lee and Chien-


References


D-C Lou, T-L Yin, and M-C Chang. An efficient stego-

Liu:2007:IFW


Lysyanskaya:2002:USV


Lysyanskaya:2007:AI


Lysyanskaya:2008:CHK


Leung:2001:WDI


Li:2004:CAB

Li, Hua; and N. Chang.


REFERENCES


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

Melissa Boyle Mahle. *De
dial and deception: an
insider’s view of the CIA from
REFERENCES


REFERENCES


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 LNCS9D.

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

Meadows:2004:OSM


Mehrabi:2001:DW


Mena:2003:IDM


Menezes:2005:TCC


Menezes:2007:ACC


Matula:2005:TLS


Mueller:2006:SMG


Muller:2009:BPE


Minier:2001:SCC


Muresan:2008:PCA


Mukherjee:2002:CAB

REFERENCES


REFERENCES


MacDonald:2003:CDS

Maltoni:2004:BAE

Moore:2001:AGK

Mabry:2007:USE

Mandviwalla:2008:MBW

Moffie:2005:AAS
Micha Moffie and David
REFERENCES


Moyle:2005:CLD


Mazieres:2000:SKM


Majzoobi:2009:TDI

Mehrdad Majzoobi, Farinaz Koushanfar, and Miodrag Potkonjak. Techniques for design and implementation of secure reconfigurable PUFs. ACM Transactions on Reconfigurable Technology and Sys-


McDonald:2008:SID


McGregor:2005:PCK


Miaou:2001:BCW

Malone-Lee:2003:TBO


Maitra:2001:SDD


McLoone:2001:HPS


McLoone:2001:SCF


Mana:2002:PMD

Antonio Maña and Sonia Matamoros. Practical mobile digital signatures. Lecture Notes in
REFERENCES


REFERENCES


REFERENCES

Mercuri:2003:IRS

Mukhopadhyay:2014:EMP

Martel:2004:GMA

Martinez-Nadal:2002:CUM

Meyer:2001:FIC
Monsignori:2001:WMS


[MNS01]

Mironov:2008:SAE


[MNS08]

Mykletun:2006:AIO


[MNT06]

MacAndrew:2000:LPT


[MNT+00]

Mollin:2001:IC


[Mol01]

Moller:2002:PEC

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


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

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

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


REFERENCES


Moshopoulos:2001:NSA [MP01c]

Malkhi:2002:ACE [MP02]

Maurer:2003:SMR [MP03]

Micciancio:2005:ASS [MP05]
REFERENCES

Matusiewicz:2006:FGD

Munilla:2007:HMF

Micciancio:2008:OCC

Mislove:2006:EBO

Moralis:2009:KSA

REFERENCES


REFERENCES


REFERENCES

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

Mayer-Sommer:2001:SAS


Maggi:2002:USV


Maitra:2002:CSB


Menezes:2002:PCI


Catherine Meadows and Paul Syverson, editors. CCS
REFERENCES

Mahdian:2009:UNI

Manulis:2009:SMF

Mashatan:2009:ITC

Myers:2009:BEC

Shen:2005:NIW

MacKenzie:2002:TPA

McClure:2003:HEN


Matsumoto:2007:FSC

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

Miltchev:2008:DAC


Mouratidis:2009:PMD


Moran:2004:NIT

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

Muller:2001:SIC


Munro:2008:DE


Murphy:2000:KST


Murray:2001:CDC


Munro:2008:DE


Murray:2002:IYP


Moriai:2000:PTL

REFERENCES

Meister:2001:PPG


Morrow:2003:DIB


Micciancio:2004:CTA


Ma:2006:ADS


Morelli:2001:JAH

[Ralph Morelli, Ralph Wald 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

Nagy:2007:AQK


Naik:2003:DSW


Naccache:2001:TCC

David Naccache, editor. Topics in cryptography, CT-

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


\textbf{NIST:2000:FPD}  


\textbf{Nazario:2002:RYS}  


\textbf{Nieto:2001:PKC}  


\textbf{Nghiem:2009:FBI}  


\textbf{Ning:2004:TTA}  

Nedjah:2005:SHC


Nash:2001:PIM


Nedjah:2004:ECH


Nedjah:2006:NTC


Netscape:2004:HSW


Neuenschwander:2004:PSM

REFERENCES

Neve:2003:STF

Nguyen:2001:TFLb

Nordholt:2002:NFC

Nyberg:2003:SAC
Nicholson:2001:YBC


Niederreiter:2002:BRC


Nielsen:2002:SRO


Nielsen:2002:TPF

Nievergelt:2002:FLM


Niederreiter:2004:BRC


Niederreiter:2002:DSAb

NIST:2000:TAE


NIST:2001:CT


NIST:2001:SRC


Nisley:2003:ELH


NIST:2003:RKE


Nagaj:2006:OQE

Ning:2008:MAA


Nigrini:2009:DDU


Nagao:2005:UCS


Nozaki:2001:IRA


Northcutt:2002:NID


Naor:2003:CFP


David Naccache and Pascal Pailler, editors. Public key cryptography: 4th [i.e., 5th] International Workshop on Practice and Theory in
REFERENCES


Nguyen:2002:AIN


Nichols:2007:MFD


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

ital assets: against hackers, crackers, spies and thieves.

Néraud:2001:CFD


Nguyen:2001:ISA


Nguyen:2001:TFLa


Narayanan:2005:FDA


Narayanan:2005:ODG

REFERENCES

Nguyen:2005:FPL


Nguyen:2005:PSE


Nishioka:2002:DAF


Nyberg:2001:CTC


Nenadic:2005:RBV


Nenadic:2005:RBC

[A. Nenadic, Ning Zhang, and Qi Shi. RSA-based Verifiable and Recoverable Encryption of Signatures and its application

Nahum:2007:ESS


Okamoto:2004:TCC

References

Ogata:2006:OSS

Olson:2000:SCT

Ohzahata:2002:FAM

References
Ohigashi:2009:PMF

Ohkuma:2001:BCH

Ohbuchi:2002:FDA

Onions:2001:SSI

Ors:2003:PAA
Okamoto:2001:GPN


Okamoto:2001:RRE


Oppliger:2001:SMP


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
[OS09] 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


REFERENCES

Okeya:2003:WNM  [OT03b]

Okada:2001:IEC  [OTIT01]

Okamoto:2000:QPK  [OTU00]

Ouellette:2005:PPM  [Oue05]

Overbeck:2006:EGA  [Ove06]
Onieva:2008:MNS


Paeng:2003:SCU


Page:2003:BRW


Panditaratne:2007:TRN


Papanikolaou:2005:BRBa


Park:2004:APP


Pass:2003:DCR

Rafael Pass. On deniability in the common reference
References

Pass:2005:UCN


Patyoot:2002:MSE


Patyoot:2002:SIW


Patarin:2003:LRR


Patterson:2001:DFI


REFERENCES


Jacques Patarin. Security of random Feistel schemes with 5 or more rounds. In Franklin [Fra04], pages 106–??. CODEN LNCSD9.


REFERENCES

cse.iitk.ac.in/news/primality.html.

Paulson:2002:NBR


Paulson:2003:NBV


Paulson:2009:NBT


Praca:2001:SCS


Piva:2002:MCW


Piva:2005:SRA

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


**[PBD00]**


**[PBD05]**


**[PBM+07]**

Peng:2007:BZK


**[PBM07]**

Prattichizzo:2007:PIH


**[PBMB01]**

Papadimitriou:2001:PSE


Park:2003:EMS


Pan:2007:IBS


Peeters:2007:CES


Petrakos:2009:CTA


Peikert:2009:PKC


Peinado:2004:CLK


Pelzl:2006:PAC

Pemble:2001:CEW


Pemble:2001:SPA


Per03


Perzold:2008:ATG


Potter:2003:S

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

REFERENCES

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


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

Pietrzak:2005:CDI


Pinkas:2002:CTP


Pinkas:2003:CTP


Pincock:2006:CHC


Piper:2003:RCS


Park:2001:NDW

Ji Hwan Park, Sook Ee Jeong, and Young Huh. A new digital watermarking for text document images using diagonal profile. Lecture Notes in Computer Science, 2195:748–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349...
REFERENCES


REFERENCES

Park:2005:CZA


Pon:2005:MDS


Pon:2005:OPK


Pfleeger:2007:IBC

Shari Lawrence Pfleeger, Martin Libicki, and Mich-

**Paulson:2000:NBU**


**Piper:2002:CVS**


**Pang:2008:AQR**


**Peyravian:2000:MBB**


**Pohlmann:2001:SCA**


**Pointcheval:2000:CCS**

Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poo:2003:NSP


Pornin:2001:THE


Porras:2006:PEG


Potter:2003:WAO

REFERENCES


[PP09] Christof Paar and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer-Verlag, Berlin, Germany /


REFERENCES


**Preneel:2002:TCC**


**Preneel:2007:SRD**


**Price:2000:NCH**


**Provos:2000:EVM**


**Provos:2001:DAS**


**Paun:2004:CTT**

Gheorghe Păun, Grzegorz Rozenberg, and Arto Salomaa, editors. *Current trends

Poupard:2000:FER


Parker:2001:RKC


Pfitzmann:2001:SEC


Pornin:2001:SHT


Padro:2002:LBI

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

Pomerance:2002:SOC


Page:2004:PCA


Park:2004:UUC


Prabhakaran:2004:NNS


Prabhakaran:2005:RES


Phan:2006:FDB


[Preneel:2006:SAC] Bart Preneel and Stafford Tavares, editors. Selected
References


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


Peikert:2008:LTF


REFERENCES


REFERENCES


Raikhel:2000:DF

[Eugene Raikhel. Decoding the forecast. Scientific American, 283(3s):20–??, March 2000. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).]

[Rai00]

Rajsbaum:2006:ASNb


[Raj06]

Roman:2007:SCP


[RAL07]

Ramesh:2001:TAE


[Ram01]

Rand:1955:MRD


[Ran55]

Rand:2001:MRD


[Ran01]

Rijmen:2001:WHF

Rogaway:2003:OBC

Rijmen:2008:RSA

Roth:2001:EJA

Rogers:2005:NSE

Rubin:2006:CSE

Reed:2000:ANA
REFERENCES

570


REFERENCES


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


Ren:2009:CWT


Rescorla:2001:IOPa


Rescorla:2001:IOPb


Rescorla:2001:IOPc


Rodwell:2007:NIBa


Rodwell:2007:NIBb


Rodwell:2007:NIBc

P. M. Rodwell, S. M. Furnell, and P. L. Reynolds.


[RK05] Renato Renner and Robert Köning. Universally composable privacy amplification against quantum adversaries. In Kilian [Kil05], pages 407–??

REFERENCES


[Ruiz:2001:SPS] Antonio Ruiz, Gregorio Martínez, Oscar Cánovas, and Antonio F. Gómez. SPEED protocol: Smartcard-based payment with encrypted electronic deliv-
Reyhani-Masoleh:2003:LCS


Reyhani-Masoleh:2003:LCB


Reyhani-Masoleh:2004:TFT


Rahaman:2008:CTB


Ryabko:2005:NTA

Ryutov:2000:RESa


Ryutov:2000:RESb

Robinson:2009:LLE


Robinson:2002:LLE


Rosen:2000:NRC


Rosen:2006:CZK

REFERENCES

//www.springerlink.com/content/uu1171. With Additional Background by Oded Goldreich.


REFERENCES


Rothe:2007:BRB


Roy:2000:PCI


Roychowdhury:2000:PCJ


Roy:2005:ACA


Rieffel:2000:IQC


REFERENCES


[RS01] Tanja Römer and Jean-Pierre Seifert. Informa-
REFERENCES


REFERENCES


REFERENCES


Rogers:2005:MPH


Rouvroy:2003:EUF


Rivest:2001:HLS


Rubin:2000:KVL

REFERENCES

[Rubin:2001:SCR]

[Rugg:2004:CMV]

[Rupp:2009:CAC]

[Raghavan:2009:SPC]

[Russell:2002:HFU]

[Renner:2003:NBS]

[Renner:2003:UAP]
Renato Renner and Stefan Wolf. Unconditional authenticity and privacy

Ramaswamy:2007:HSP


Saeednia:2002:IBS


Sakamura:2001:GEI


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


REFERENCES

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 Buh-


[SBG02] [SBS09] [Shehab:2007:WSD]


[Shehab:2005:SCM]

[Smeraldi:2002:SVF] [SBS09] [Shehab:2007:WSD]

[Steinfeld:2002:NSA]


Stephanides:2005:GAK


Sun:2005:IPK


Siegelin:2001:SCD


Schmalz:2000:MAD


Schneier:2000:AAR


Schneier:2000:IRS

Bruce Schneier. *Inside risks: semantic network attacks*. *Communications of the Association for Comput-
Scharinger:2001:ASK


Schindler:2001:TAA


Schmalz:2001:MDI

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*


REFERENCES


REFERENCES

599
(print), 1873-5649 (electronic).

Scott:2004:CIB

Screamer:2001:MDR

Shen:2005:NCB

Sun:2005:RNK

Sun:2005:RNK

Sebe:2001:OIW

Sebe:2000:SDI
Francesc Sebé, Josep Domingo-


Smith:2006:SID


Seifried:2000:C


Seifried:2000:PPA


Seifert:2005:ACR


Speed:2001:PIS


Speed:2002:PIS


Selçuk:2000:BEL

Ali Aydn Selçuk. On bias estimation in linear crypt-
REFERENCES


REFERENCES


[Sakr:2007:RCB]

[Sutton:2007:FBB]

[Steinwandt:2000:WHS]

[Steinwandt:2008:GEI]
Rainer Steinwandt, Willi Geiselmann, and Çetin Kaya Koç. Guest Editors’ introduction to the special section on special-purpose hardware for cryptography and cryptanalysis. IEEE Transactions on Computers,
REFERENCES


REFERENCES

**Shamir:2001:NDC**

**Shamir:2001:PSC**

**Shao:2001:BVM**

**Sharp:2001:IKB**

**Shapiro:2002:CCM**

**Shamir:2003:RS**
Adi Shamir. RSA shortcuts. In Jove [Joy03c], page 327. CODEN LNCS-D9. ISBN 3-540-00847-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN


Ronen Shaltiel. Recent developments in extractors.

Shamir:2003:TLC

Shao:2004:IDS

Shao:2005:CXY

Shao:2005:IEP

Shaltiel:2004:RDE
Shao:2005:NKA


Shao:2005:SMD


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

Sierra:2004:LCC

Shimizu:2007:CBE

Shoup:2000:CTU

Shoup:2000:UHF

Shoup:2001:OR
REFERENCES


**Shparlinski:2003:CAA**


**Shparlinski:2004:BRR**


**Shparlinski:2004:UDD**


**Shparlinski:2005:PHS**


**Sun:2005:SSP**

REFERENCES


REFERENCES

pp. LCCN Z103 .S56 1999. US$24.95. See also [AAG+09].


REFERENCES


[SKR02] K. Srinathan, M. V. N. Ashwin Kumar, and C. Pandu Rangan. Asynchronous secure communication tolerating mixed adversaries. *Lec-
REFERENCES

Sugita:2000:RAD


Schneier:2000:CTA


Scharwaechter:2007:AAE


REFERENCES

**Su:2005:KPK**


**Shi:2005:HEC**


**Shen:2003:SET**


**Sung:2000:PSS**


**Salido:2007:EBE**


**Song:2001:DWF**


REFERENCES


Smith-Miles:2008:CDP


Smart:2001:CDF


Smart:2003:ACU


Smart:2003:AGR


Smart:2005:CCI

References

Smith:2000:ABS

Smith:2001:IK

Smith:2002:ECB

Smith:2001:APP

Smith:2002:OAP

Smolin:2004:EDE

Seamons:2009:IPS
Kent Seamons, Neal McBURNett, Tim Polk, et al., edi-


Safavi-Naini:2000:STT

Safavi-Naini:2001:BAG

Safavi-Naini:2001:LAC

Sanchez:2001:RNM

Slind:2007:PPS
REFERENCES


Song:2000:ISC


Shigetomi:2002:ALS


Satoh:2000:HSM


Smith:1979:UFM


Shelfer:2002:SCE

REFERENCES


StDenis:2006:BMI


Stipcevic:2007:QRN


Samarati:2001:AMP


Standaert:2003:EIR


Sarkar:2001:PAE

Stubblebine:2001:AAF


Seznec:2003:HUL


Swiderski:2004:TM


Seddik:2009:IWB


Shi:2008:UAU


Susilo:2000:NEF

REFERENCES


REFERENCES


Sterlicchi:2000:SCD

Steinwandt:2001:LTP

Stefanek:2002:ISB

Steele:2005:PPT

Steil:2005:MMM

Stern:2005:MLF

Stein:2008:ENT
William Stein. *Elementary number theory: primes, congruences, and secrets*, volume 666 of *Undergrad-


REFERENCES


[Str01a] Bruno Struif. Use of biometrics for user verification in electronic signature smartcards. Lecture

[Str01b] Elisabeth Strunk. Java Q&A: Java & NT authentication. Dr. Dobb’s Journal of Software Tools, 26

[Str02] Ray Strubinger. A homegrown backup solution utilizing RSA keys, SSH, and tar. Sys Admin: The


[STY07] Nitesh Saxena, Gene Tsudik, and Jeong Hyun Yi. Threshold cryptography in P2P and MANETs: The case

**Shaltiel:2007:LEU** [Su00a]


**Sugihara:2001:PCD** [Su01]


**Sugita:2003:DRW** [Su03]


**Sun:2000:DRR** [Su00a]


**Sun:2000:ESM** [Su00b]


**Sun:2002:IIR** [Su02]


**Sun:2005:UMS** [Su05]

REFERENCES

Seidl:2008:FOV


Shaltiel:2008:HAP


Sebe:2007:SMO


Shmueli:2009:DEO


Smith:2000:CIR


Schneier:2000:PCF

 REFERENCES


REFERENCES

link/service/series/0558/1
bibs/2247/22470316.htm; [SY06]

Seo:2001:CDA


Shi:2001:NSF


Sun:2006:PBA


Syed:2000:CLA


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


Tang:2007:MMU


Tang:2007:SGK


Tattersall:2005:ENT

REFERENCES

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

[TBDL01] Elena Trichina, Marco
Bucci, Domenico De Seta,
and Raimondo Luzzi. Sup-
plemental cryptographic
hardware for smart cards.
*IEEE Micro*, 21(6):26–35,
CODEN IEMIDZ. ISSN
0272-1732 (print), 1937-
4143 (electronic). URL
http://dlib.computer.org/
mi/books/mi2001/m6026abs.
htm; http://dlib.computer.
org/mi/books/mi2001/pdf/
m6026.pdf.

[TBJ02] Massimo Tistarelli, Josef Bi-
gun, and Anil K. Jain, edi-
tors. *Biometric authentica-
tion: International ECCV
2002 Workshop, Copen-
hagen, Denmark, June 1,
2002: Proceedings*, volume
2359 of *Lecture Notes in
Computer Science*. Springer-
Verlag, Berlin, Germany /
Heidelberg, Germany /
CODEN LNCSD9. ISSN
3-540-43723-1 (soft-
cover), ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN TK7882.P3
link.springer-ny.com/
link/service/series/0558/
tocs/t2359.htm; http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=2359.

[Tao00] Renji Tao and Shihua Chen.
Input-trees of finite au-
tomata and application to
Sci. Tech.*, 15(4):305–325,
2000. CODEN JCTEEM.
ISSN 1000-9000.

[Tsai01] Chwei-Shyong Tsai and
Chin-Chen Chang. A gen-
eralized secret image shar-
ing and recovery scheme.
*Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
com/link/service/series/0558/
bibs/2195/21950963.htm;
com/link/service/series/0558/papers/2195/21950963.pdf.

[Tsaur05] Woei-Jiunn Tsaur and
Chih-Ho Chou. Efficient
algorithms for speeding up
the computations of el-
lipic curve cryptosystems.
*Applied Mathematics and
Computation*, 168(2):1045–
1064, September 15, 2005.
CODEN AMHCBQ. ISSN
Tsai:2002:SMS


Trudel:2003:DSE


Teepe:2006:PPA


Todd:2001:LSS


Terai:2008:BRB


Thorsteinson:2004:NSC

REFERENCES


Theoharidou:2007:CBK


Tirkel:2001:UWE


Tabatabaian:2001:NSP


Tippett:1927:RSN


Torres:2007:ANS


Tseng:2001:GGO

Tseng:2001:CLB


Tseng:2003:DSM


Tico:2003:RAS


Toll:2008:CSE


Thien:2002:TSS


Thomas:2007:HQU


Turner:2006:SIS


Tsolis:2009:ARM


Teoh:2004:PCK


Tousidou:2000:IMS


Toussaint:2009:ARM


Tochikubo:2000:RAE


Tomaszewski:2006:YSY


REFERENCES


Tseng:2007:SAG


Takano:2000:PTH

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

Tsunoo:2003:CIC


Tahir:2000:RCM


Tzeng:2001:PKT


Tian:2001:ICE

Jun Tian, Tieniu Tan, and Liangpei Zhang, editors. Image compression and encryption technologies: 22–24 October 2001, Wuhan,
Tuchman:1966:ZT


Turing:2004:BS


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

Tiri:2003:SEA


Toft:2001:LTT


Trappe:2002:ICC

Wade Trappe and Lawrence C. Washington. Introduction to Cryptography


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


REFERENCES


[Uni00a] United States Congress. H.R. 850, the Security and Freedom through Encryption (SAFE) Act: Markup before


[USE00a] USENIX, editor. Proceed-


REFERENCES

USENIX:2001:PTU


USENIX:2002:PBF


USENIX:2002:PUS


USENIX:2002:PFT


Utami:2002:FID


Urien:2001:XS

REFERENCES

[Ust01b]

[Uzu04]

[Vac06]

[Vad03]


Vaudenay:2005:SCI


Vavriv:2003:RNG


Voloshynovskiy:2005:ITD


vanDijk:2004:AOC

Marten van Dijk and David Woodruff. Asymptotically optimal communication for torus-based cryptography. In Franklin [Fra04], pages 157–?? CODEN LNCSD9. ISBN 3-540-22668-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN
REFERENCES

Verheul:2001:EXM

Vercauteren:2002:CFZ

Vergnaud:2006:RBS

Vernitski:2006:CUM

Vladimirov:2004:WFS

Vassev:2009:STA
Voloshynovskiy:2001:BDA

Viroli:2003:TPA

Vixie:2002:SRR

Vural:2007:IND

Vo:2008:SMA


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


[Voice:2005:OAM]

[vOT08]

[vanOorschot:2007:IRS]

[Vasco:2001:CPK]

[Voyiatzis:2008:SFS]
Artemios G. Voyiatzis and Dimitrios N. Serpanos. The security of the Fiat–Shamir
scheme in the presence of transient hardware faults. [V07]


REFERENCES

Wallach:2000:SSM


Wagner:2000:CYL


Wagner:2002:GBP


Wagstaff:2003:CNT


Walsh:2000:BRM

Walter:2001:PBM


Walter:2003:STM


Wang:2004:AWE


Wang:2004:TVS


Wang:2005:SCR


Weiss:2000:CAC


Wu:2002:CScA


Wu:2001:CDS


Weis:2001:SYH


Weeks:2000:HPS

Bryan Weeks, Mark Bean, Tom Rozylowicz, and Chris
REFERENCES


Wong:2001:EMA


Wong:2001:EMA

Wu:2001:CKA


Wu:2003:HDW


Wu:2003:UFR


Wu:2004:EIW

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:TAP

Wang:2009:NWA

Wang:2005:SDR

Westerlund:2001:HWK

Williams:2001:ICA
Weir:2009:UPS


Wang:2009:SST


Weaver:2006:BA


Weber:2002:ECH


Webb:2008:IZN


Wehde:2000:IME


Weierud:2000:SFB


[Weh08]
Weiss:2004:JCE


Weierud:2005:BSF


Weierud:2005:BPS


Welschenbach:2005:CCC


Weng:2003:CHC


Wernsdorf:2002:RFR

REFERENCES

Westfeld:2001:FSA

Wu:2002:LCN

Wang:2005:RST

Wong:2000:SGC

Wu:2002:CAE
Wu:2002:IBM


Wu:2003:TSS


Wang:2009:NWM


Wen:2005:URE


Wu:2008:RPG


Watanabe:2001:EAP


REFERENCES


REFERENCES

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

Weigold:2008:RCA
ISSN 1540-7993 (print), 1558-4046 (electronic).

Walter:2003:CHE

Wang:2002:AAB

Wedde:2004:MAA
ISSN 1094-9224 (print), 1557-7406 (electronic).

Wu:2004:RKA
ISSN 0096-3003 (print), 1873-5649 (electronic).
Wang:2005:CHY


Wang:2007:NCD


Williams:2007:FTA


Wen:2006:PSA


Wang:2009:DSM


Wang:2003:CET

[WL03] Bin Wang, Jian-Hua Li, and Zhi-Peng Tong. Cryptanalysis of an enhanced timestamp-based password


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

REFERENCES

Wrixon:2005:CCO

Wang:2002:IPD

Wright:2002:EPS

Whiting:2003:MPH

Walter:2005:DDP

Weimerskirch:2002:DLW
André Weimerskirch and Gilles Thonet. A distributed light-weight authentication model for ad-hoc networks. Lecture...

Wu:2001:DSM


Wu:2002:CSCb


Wuensch:2009:CAE


Wu:2000:PKC


Wu:2001:FED


Woodruff:2002:CUC

David P. Woodruff and Marten van Dijk. Cryptography in an unbounded computational model. Lecture
Weaver:2000:CAC

Wang:2004:CWS

Wolf:2005:NML

Wang:2006:SPS

Wang:2008:DCP
Xing-Yuan Wang and Xiao-Juan Wang. Design of chaotic pseudo-random bit

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:2008:HQS]

[Wang:2002:WEM]

[Wyant:2002:APK]

[Wyler:2005:ANS]


REFERENCES


Xue:2005:ETR


Xue:2001:CPW


Xiao:2003:HPC


Xiao:2005:SPA


Xenakis:2006:GCO

REFERENCES


Xu:2007:CAD


Xu:2005:ADR


Xie:2007:ISP


Xie:2004:CTA

Xiang:2008:CPA

Xu:2007:CAD

Xu:2005:ADR

Xie:2007:ISP

Xie:2004:CTA
AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Xu:2009:AVB


Yan:2000:NTC


Yang:2002:NEC


Yue:2001:GNN


Yan:2007:CAR


Yasuda:2008:DLP


Yuan-bo:2004:ITA

k/service/series/0558/bibs/2084/20840196.htm;
http://link.springer-ny.com/link/service/series/0
558/papers/2084/20840196.pdf.

[YC07] Tai-Wen Yue and Suchen Chiang. The semipublic en-
cryption for visual cryptography using Q’tron neural
networks. *Journal of Network and Computer Appli-
cations*, 30(1):24–41, January 2007. CODEN JN-
CAF3. ISSN 1084-8045 (print), 1095-8592 (elec-
science/article/pii/S1084804505000391.

[YC08] Wai-Pun Ken Yiu and Shueng-Han Gary Chan. Of-
ering data confidentiality for multimedia overlay mul-
ticast: Design and analysis. *ACM Transactions on
Multimedia Computing, Communications, and Ap-
???? ISSN 1551-6857 (print), 1551-6865 (elec-
tronic).

[YC09b] Jen-Ho Yang and Chin-Chen Chang. An ID-
based remote mutual authentication with key agree-
ment scheme for mobile devices on elliptic curve cryp-
May/June 2009. CODEN CPSEDU. ISSN 0167-4048

[YC09c] Seung S. Yang and Hong-sik Choi. A comple-
ment to the GridOne authentication method. *Network Secu-
rity*, 2009(12):12–18, December 2009. CODEN
NTSCF5. ISSN 1353-4858 (print), 1872-9371 (elec-
science/article/pii/S1353485810700076.

three-party authenticated
REFERENCES


Yu:2007:NSM


Yung:2006:PKC


Yang:2008:NFD


Yang:2007:IIS


Yekhanin:2007:LDC


[YI00] Akihiro Yamamura and Hirokazu Ishizuka. Quantum

**Yamamura:2001:EDA**


**Yi:2004:AKA**


**Yen:2000:CBO**


**Yen:2002:CAO**


**Yen:2002:RSR**

REFERENCES


[YLH05] Jia Yu, Daxing Li, and


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


Yoon:2005:ICJ


Yoon:2005:IFA


Yoon:2005:IHL


Yeh:2002:SAK


Yeh:2004:PBU


Yanami:2002:DLC

REFERENCES


Ytrehus:2006:CCI

[706]


Yang:2005:SEA

[707]


Yung:2002:ACC

[708]


Yung:2002:CI

[709]


Yang:2004:ISE

[710]

REFERENCES

Yang:2004:CUF

Yang:2005:CIA

Yang:2006:SED

Yang:2005:IYS

Yang:2008:VCS

Yang:2008:FSD
G. Yang, D. S. Wong, and X. Deng. Formal security definition and efficient construction for roaming with

**Yang:2005:SAS**


**Young:2000:RBA**


**Yang:2008:TFM**


**Yang:2009:CLW**


**Yang:2009:CLW**


**Young:2001:BOK**


**Young:2004:MCE**


REFERENCES

(paperback). xxiv + 392 pp. LCCN QA76.9.A25 Y65
http://www.loc.gov/catdir/description/wiley041/2003023863.html;

Yoon:2005:CZX


Yoon:2005:SWL


Ye:2001:ATD


You:2001:GEC


Yen:2000:WOW

Ye:2007:NAW


Youssef:2009:IEU


Zafar:2000:ACB


Zane:2001:EWD


Zhang:2005:ITA


Zivkovic:2005:AAH

Zhao:2005:SSV

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

Zhao:2000:MCA


Zhao:2004:AIB


Zhang:2005:CHC


Zhang:2009:CII


Zhang:2001:SOS

REFERENCES

[ZCL05] Zhou:2005:PSP


[ZD05] Zunino:2005:WPE


[ZDW06] Zhao:2006:SAP


[ZF05] Zhen:2004:IBS

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


[Yuliang Zheng. Identification, signature and sign-
REFERENCES

Zheng:2002:NPK

Zheng:2002:ACA

Zhou:2002:MVD

Zhong:2006:ESC

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


REFERENCES


Zheng:2005:DMI


Zhou:2005:MBl


Zolman:2001:SEM

Zhu:2007:IHH


Zhang:2005:RPE


Zhao:2005:APA


Zhou:2005:APS


Zhang:2003:FSP

Zafeiriou:2005:BRW


Zhang:2005:ISS


Zhang:2005:SCA


Zhao:2002:EII


Zhu:2002:PAK


Zhang:2001:USC

Yuqing Zhang, Chunling
REFERENCES


Zhang:2004:NMS


Zhong:2008:GPT


Zhou:2003:ACN


Zhang:2005:ASP


Zhang:2005:ISM

Peng Zhang, Chengqing Ye, and Xueying Ma. Improvement of secure mobile agent system in electronic commerce. In Han and et al. [HYZ05b], pages 114–?? ISBN 981-270-153-2. LCCN ???. URL eproceedings.worldscinet.
Zhang:2008:FIC


Zeng:2001:CHR


Zhuang:2005:KAE


Zhu:2007:EIB


ZYR01


ZYN08