Title word cross-reference

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

(k, n) + 1 [LCZ05c]. (λ, ω) [vDKST06]. (p^k)
[BINP03]. (t, n) [CHY05a, HL05c, Kog02, LYL+01, YCH02, CLT07]. (tn)
[PW05, SC05a]. + [Abe01]. \{0, 1\}
[LBGZ01, LBGZ02]. 1 [Wu02]. $125
[And04]. 128 [AIK+01, PCG01]. 13
[HSL+02]. $15.00 [Imr03]. 2
[Bih00, BGN05, CY02, CKL+03, DNP07, Gau02, GHK+06, GIKR02, HKA+05, KLR09, SC02b, Ver02, Wen03]. 2000 ± 10
[Man01]. 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]. \(\mathbb{A}\mathbb{B}\mathbb{C}\) [PS04]. \(d\) [BD00b]. \(E_0\)
[FL01a]. \(f_k\) [KSHY01]. \(g^{x^2}\) [Shp02]. \(g_e(x, 1)\)
[SZP02]. \(\mathbb{G}\mathbb{F}(2)\) [CP03]. \(\mathbb{G}(\mathbb{F}^{2^m})\)
[OTIT01, RMP10]. \(\mathbb{G}(\mathbb{F}^{p})\) [BGK+03]. \(\mathbb{G}(\mathbb{F}^{p})\) [PZ01]. \(k\) [BJLS02, CT08b, GFC08, HKS00, QPV05, WL02]. \(l\) [QPV05]. \(M + 1\)
[AS01a]. \(\mathbb{F}_q\) [CY02]. \(\mathbb{Z}_n\) [Gro05]. \(\mathbb{G}(2)\)
[GS03, KTT07]. \(\mathbb{G}(2^m)\)
[BBG08, KTT07, KWP06, RMH03a, RS04]. \(\mathbb{G}(\mathbb{F}^*)\) [KKH03]. \(\mathbb{S}\mathbb{L}_2(\mathbb{F}_{2^m})\) [SGGB00]. \(\mu\)
[LN04]. \(n\)
[CT08b, Gor06, HKS00, LKJL01, TM01]. \(N^{0.292}\) [BD00b]. \(NC^0\) [AIK06]. \(p\) [FL06].
$p^rq^s \text{ [LKYL00]. } p^r \text{ [CHH01]. } Q \text{ [Yas08]. } r \text{ [JY01]. } w \text{ [DwWmW05, OT03b]. } x^v \text{ [Gon06]. } y \text{ [OS01]. }

-Adic [GHK+06]. -Bit [AIK+01, CDL+00, PCG01]. -Connected [BJLS02]. -Coordinate [OS01]. -coverings [SC02b]. -decompositions [vDKST06].

-DNF [BGN05]. -Metric [AIK+01, CDL+00, PCG01]. -Connected [BJLS02]. -Coordinate [OS01]. -coverings [SC02b]. -decompositions [vDKST06].

-out-of- [CT08b]. -Polynomials [FL06, CHH01]. -Round [BP04, Bih00, GIKR02, CKL+03]. -Source [KL09]. -st [AS01a]. -Steiner [WL02]. -Threshold [CLT07, Kog02]. -way [LKJL01].

.NET [For04, TG04].

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

0 [And04, BCOa4, Gm04, 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 [G07a]. '05 [ACM05c, MS05b, ZC09]. '07 [ACM07]. '08 [ACM08]. '09 [ACM09, IEE09a].

1 [BD00a, BSW01, FOP06, GM00b, GLG+02, HKR01, MP06, PS01c, Puz04, Uni00c, Uni00d, Uni00g, WYY05b, WYY05c, Was08a]. 1-58488-518-1 [Was08a]. 1-Connected [BJLS02]. 1-out-of-n [AOS02]. 1.82Gbits/sec [KV01]. 1.82Gbits/sec [KV01]. 101 [Sei00a].

10118-3 [ISO04]. 106 [Uni00c, Uni00d, Uni00g]. 106-1 [Uni00c, Uni00d, Uni00g]. 108-bit [Bar00a]. 109-bit [Pri00]. 10th [Coc02a, Joh03, Lee04b, MZ04, Sma05, dCdVSG05]. 11-15 [AUW01]. 11th [CCMR05, HZY05b, HH04, HH05, RM04, Roy05, USE02b]. 12 [TPS01]. 128 [JJ02a, WFLY04]. 128-Bit [SM03b].

12th [GH05, MS05b, PTP06]. 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 [Sei00a]. 196 [Sei00a]. 1962 [AJ08]. 1987 [Kha05]. 1993 [PPV96]. 1999 [Lee03b, Uni00a, Uni00b, Uni00c, Uni00e, Uni00d, Uni00g, Uni00h, Uni01].

19th [BCD09]. 1V [CGBS01].

2 [Nat00, SK05a]. 2.0 [Cor00a]. 2000 [CGH+00b, Eke02, Irw03, KH08, KI01a, Sch00b, Wit01, YG01c]. 2001 [AOC01a, BC01, GJSS01, Lee03a, Pem01b]. 2002 [B+02, EIE02, RSA03a, YUN02a]. 2003 [ACM03a, ACM03b, ACM03c, BS03, Bon03, FLA+03, WKP03. 2004 [ACM04b, ZC04]. 2005 [ACM05a, ACM05b, ACM05c, ANS05, HZY05b, ISO05, Roy05, Ter08, Ytr06]. 2006 [ACM06]. 2007 [ACM07, Ano06b, SM07b]. 2008 [ACM08, Dw08, YRS+09]. 2009 [ACM09, May09]. 2010 [Bel00]. 21 [AJ01b].

218 [WB00]. 21st [Jef00, Kil01a]. 21th [IEE09a]. 22 [TTZ01]. 22nd [Yun02a]. 23rd [Bon03]. 24th [Cra05a, Fra04]. 256-bit [Luc00]. 25th [Sh05a]. 26 [DB04]. 26th [EBC+00]. 27th [Men07]. 29. [Eke02]. 29th [FLA+03].

3 [DUW03, Imr03]. 3-15-07640-9 [Eag05]. 3-540-66778-4 [Dw03]. 3-Key [Kel05]. 3.0 [Flu02b, Hei01, SQ01]. 305 [ECM00a]. 306 [ECM00b]. 30th [Coc02a]. 314pp [Dw03]. 3278 [BWBL02]. 33rd [ACM01a]. 36th [ACM04b]. 37th [ACM05c]. 39th [ACM07]. 3D [LZP+04]. 3GPP [KSHY01, SM02]. 3rd [ACM05a, USE00a].
4 [Duw03]. 4-round [DLP\textsuperscript{+}09]. \textbf{40th}
[ACM08]. 41st [IEE00a]. \textbf{42nd} [IEE01a].
43rd [IEE02]. \textbf{44th} [IEE03]. 45th [IEE04].
46th [IEE05a]. 47th [IEE06]. 48th [IEE07].
49th [IEE08]. 4th
[BCKK05, BC05b, DWML05, DR05, Fra01, Gum04, JM03, KKP02, Kim01, Kim02, KN03, MS05a, NP02a].
5 [BCJ\textsuperscript{+}06, Bac05]. \textbf{50th}
[IEE09b]. \textbf{512}
[AD07, GLGW\textsuperscript{+}02]. 5th
[CV04, KJR05, LL03, LLT\textsuperscript{+}04, Li05, NP02a, Syv02, WKP03].
64 [LKH\textsuperscript{+}08, WWCW00]. 6th
[Bl03, Des02, HA00, JQ04, LL04c, MMV06, Oka00].
7 [And04, Gum04]. \textbf{7-round} [Pha04]. \textbf{7.2}
[TvdKB\textsuperscript{+}01]. \textbf{77}
[AL04]. 7th
[BDZ04, Boy01, Chr00, DFPS06, PC05a, RS05, Sch01d, ST01d, Wri03].
8-Round [BF00a]. \textbf{8.8/11.2} [DFPS06]. \textbf{800}
[BG07a, Hir09]. \textbf{80-90} [BG07a, Hir09].
\textbf{802.11b} [SIR04]. \textbf{802.11g} [Coc02a].
\textbf{802.11i} [HSD\textsuperscript{+}05]. \textbf{802.15.4} [Mi08]. \textbf{82}
[Kwo03b]. 8th
[Chr01, Hon01, Jue04, Mat02, SMP\textsuperscript{+}09, VY01, Vau05a, WK06, Zhe02b].
9 [CGP\textsuperscript{+}02, Gan08]. 9/11 [Ark05, Mah04].
\textbf{90} [BG07a, Hir09]. \textbf{9796} [GM00b]. \textbf{9796-1}
[GM00b]. \textbf{98} [Wil99]. \textbf{99} [DN00b]. 9th
[CCMR02, CS09, DR02c, DKU05, Lai03, NH03, Pat03b, PY05, YDKM06].
= [KOMM01].
A-1 [ISO05]. \textbf{A.2.4} [Kel05]. \textbf{A5}
[BD00a, BS01, PS01c]. \textbf{A5/1}
[BD00a, BS01, PS01c]. \textbf{AAFG1} [Hag02].
\textbf{Abadis} [CF02, PHK\textsuperscript{+}01, RS02]. \textbf{Abstention}
[JJL02]. \textbf{Abstract}
[CM00, Cou04, DTHR05, HLVA02, HJW01, JL00, MS02, MP02, Mas04, Wag02, BJN00, BCDM00, CD00a, CC04c, FKS\textsuperscript{+}00, GHJ00, GTZ04, HT04, HP01, Iwa08, IK00, Jon08, KKS00a, KM00, LM08, Mes00, Pei09, Yas08].
\textbf{Abstracting} [Bl01a, Mon03]. \textbf{abstraction}
[BLP06]. \textbf{abstractions} [BG07b]. \textbf{Abstracts}
[Sch00b]. \textbf{Accelerating} [ESG\textsuperscript{+}05]. \textbf{acceleration} [EHK04]. \textbf{Accelerator}
[CGBS01, RS04, TSO00, XB01, DPT\textsuperscript{+}02].
\textbf{Access}
[ANRS01, An02e, BNP03, CGM02, DS06, HC08, MS03b, Ril02, Sma03a, Sun00a, ZGLX05, AW05, AW08, AFB05, BA06, BNP08, Che08b, DFM04, Hos06b, HY03, IV06, JW06, KNS05, LKZ\textsuperscript{+}04, MF07, MSP\textsuperscript{+}08, PS02a, ST07, WL05, WC01b].
\textbf{access-control} [BNP08]. \textbf{accessible}
[Pau02a]. \textbf{accountability} [WAB\textsuperscript{+}08].
\textbf{Accounting} [Lai08]. \textbf{Accumulator}
[GTH02]. \textbf{Accumulators} [CL02a].
\textbf{accurate} [ZY08]. \textbf{Achieve} [CF02].
\textbf{Achievement} [Coc01a]. \textbf{Achievements}
[VDP05]. \textbf{achieving} [PS04c]. \textbf{ACISP}
[YG01c]. \textbf{ACM}
[ACM01a, ACM03a, ACM03b, ACM03c, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, MS05b, Bar00b, FMA02, Raj06]. \textbf{ACNS}
[GKS05, IKY05, JYZ04, ZYH03]. \textbf{acoustic}
[ZT05]. \textbf{Acquiring} [SETB08]. \textbf{across}
[Dav07, ZBL05]. \textbf{Act}
[Kha05, Uni00a, Uni00b]. \textbf{Actel}
[DV08]. \textbf{Action} [SE01]. \textbf{Active}
[BC05a, BACS02, BP02, LJJ05, MA00a, MA00b, Tad02, BPS08]. \textbf{Active-Content}
[MA00a, MA00b]. \textbf{activities} [AJ08, SN07].
\textbf{actually} [Hau06]. \textbf{Ad}
[BSS02, KH05, WT02, Cha05b, DMR07, LHC08, LKZ\textsuperscript{+}04, PCSM07, SLP07, TW07, ZC09, MAaT04].
\textbf{’ad-Durayhim’s} [MAaT04]. \textbf{Ad-hoc}
[BSS02, WT02, DMR07, ZC09].
\textbf{Adaptation} [ISSZ08]. \textbf{Adapting} [MJD01].
\textbf{Adaptive}
[CM00, CTL04, CL08, Coc02a, CS02, CS03b, DSS01, EFY\textsuperscript{+}05, FMY01, JMV02, KCM\textsuperscript{+}01, KLL01, LP01, MP05, Nov01, Pie05, ZWC02, AAP07, Che07].
Adaptively-Secure [CHK05]. Added [Ano02b, St.00]. Adding [FBWC02].

Adaptive [AF04b, CHK05, FMY02, JL00].

Adaptive [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 [GHK06].

Adjacent [JT01b]. Adjustment [BSNO00]. Adjustment [BSNO00].

Adjacency [JTG00, McL06]. Again [Fox00]. Against [CS05b, DM07b, FKSW00, KS00a, KKS00a, KKS01, Mes00, Mes01, MPSW05, MH04, PV06b, Pro01, RK05, AG01, ABR05, BPR00, BP02, BBN+09, BBB+02, BCP02b, CM00, CS03b, DB04, DJ06, Des00b, Des00c, Egd00, EBS01, FP01, FY00, Geb04, HNZI02, HLL+01, Hsu05b, HLC08, Ino05, ISW03, IIT03, JK02, JAO06, JT01a, Kan01, KM02, KML+02, LM08, LPV+09, Lu02, Mit00, MoI02, MG08, NRR00, NLD08, OKS06, OS00, OT03a, OT03b, PKBD01, PSC+02, PSp+08, PS01h, PQ03b, RS01, SKQ01, Sch01b, Sch01f, SDFH00, SDF01, Sem00, Sho00b, SKU+00, SK01, SLL+00, Tad02, TV30, VHP01, XH05, YJ00, YKLM02a, YKLM02b, YKLM03, ZSJN07].

Age [Mar08b, Lev01]. Age [Mar08b, Lev01].

Adversary-Based [HQ05, SSM+08]. Agents [WHI01, Hau06, LSA+07]. Agents [WHI01, Hau06, LSA+07].

Adversarial [CLR09, GSS08, MNS08]. Adversarial [CLR09, GSS08, MNS08]. Adversarial Knowledge [CLR09].

Adversary [CM00, JQ01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05]. Adversary [CM00, JQ01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05].

Adversaries [CM00, JQ01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05]. Adversary [CM00, JQ01, KSR02, Lu02, RK05, SKR02, GXT+08, ZD05].
al-fusul [MAaT05].

al-Ka [MAaT07].

Al-Kindi [MAaT03, MAaTxx].

al-mutargima [MAaT05].

Alan [Pet08].

Alcatraz [LSVS09].

Alchemy [Pag03].

alert [AJ08].

alerts [NCRX04].

Alexandria [MS05b].

Algebra [Cou01, CD01a, Lan04a, CKY07, Fau09, HW03a, HWR09, Sho05b].

Algebraic [AK03, Bar09, Can06b, CM03, Cou03, CFS05, FJ03, FSW01, GPS06, HR04a, HM02b, Hug02, Mas04, MN01, MR02a, MR02b, Pau01, Pau02a, Pre02b, Pre02b, SL00, TLYL04, TV03, WBRF00, WWGP00, AHK03b, Ano01j, AH05, CKA+09, CCM01, GHP00, GPC08, HW03a, HWR09, HHG06, Hro05, JK01a, MCHN05, Pre07, Rhi03, TC05, XLS06, ZLZS07, Zir07, dH08].

Alien [Wil01b].

All-or-Nothing [Des00c, SR00].

Alley [DR01, Wie00].

Allied [Hau03, Hau06].

Allocation [CCM05, LZ09].

Allowing [JLL02].

Almost [AP09, BS00a, Jut01, Mar02b].

Alpha [WB00, Wu02].

Alphai [KBD01].

Altera [A02e].

Alternating [Wer02, HKP05].

Alternative [Bad07, Gar03a, BMW02b].

always [BB79].

An [Eke02, SU07].

Amalfi [BC05b, CGP03].

Amenability [WW00].

America [DB04].

American [GL05, Kat05b, Alv00, Naf05].

Americans [WD01b].

among [BN00a, KT00, SKU+00, Win05c].

Amongst [Pem01b].

Amplification [CHS05, LTW05, RK05, SV08b].

Amplified [KKS00a, KKS01, KML+02].

Amplifier [Pri01].

Amsterdam [Knu02].

Analyses [BPR05, Des00a, Pau01].

Analysing [BL02].

Analysis [ARJ08, ABR01, AKS06, AD07, Ano01c, AIK+01, ARC+01, Ava03, BN00a, BDhKB09, BRS02, BF05, Bor01, BSL02, Cry00, CK02a, CS03b, DPV01, Dra00, FL01a, FGM00a, Gir06, GHPT05, GLG+02, GPR06, HSS01, HK01, HSS04, Hey03, HM02c, IIT03, JK01a, JQYY01, JT01a, JQY01, hKLS00, KMS02, LCK03, LKH09, LY05, LWK00, LH07, MOP06, Mar02b, Mas04, MS01, MMMT09, Mea01, Mes00, Mes01, MAaTxx, MG08, NP02b, NSS02, OS06, ÒP03, Puc03, Q501, SSS06, Sha01c, Sma03b, SDM06, SQ01, SWT07, YSS+01, ZZ00, ZGLX05, AvdH00, AW05, AW08, Abd01, AHK03b, BDDV08, BBK+03b, Bjo05, B07a, BR05, BCJ+06, CKL+09, CW07, C05a, DKS08, GW08, GM04, GTR04, Has01b, Hir09, Hro05, Hut01, JEZ04, JSW05, KSF00, Kor09, LKH+08, LMW05, LW05a, LKJL01, Lu07].

analysis
Analyzing [MS01, Shi02, CP07, DFG00, HM02a, ME08b, NCRX04].

anatomy

Analytic [Shp03, Nie04].

Anchor [Ree01].

Ancient [Imr03, Sin00, Mol05, Pin06].

Andrei [Puz04].

Andrew [Puz04].

Anguilla [Fra01].

Anniversary [Sal01b, Coc02a].

annotated [Pet08].

annoying [Tyn05].

Annual [ACM01a, ACM02, ACM04b, ACM05c, ACM06, ACM07, ACM08, Bon03, Cra05a, ELvS01, Fra04, IEE00a, IEE02, IEE03, IEE04, IEE05a, IEE06, IEE07, IEE08, IEE09b, Kil01a, MZ04, Men07, Sho05a, USE01b, USE01a, USE02c, VY01, Yun02a, ACM00, Be100, HA00, Je008, NH03, ST01d].

anomaly

Anonymity [GM03, IKOS06, MP02, SS01b, EY09, NH03, ST01d].

Anonymization [FXAM04, RW07].

Anonymous [ABC05, CL02a, CL04a, HSHI02, HSHI06, KT01, LHL08, SOOI02, Wan04a, YT09, ZJ09, BP03a, EY09, LHC08, Sae02, Sha03c, WCJ05, YTWY05, ZC09].

ANSI [III00, Kel05, Oiw09].

ANSI-C [Oiw09].

Answers [PT08].

Ant [Kha05, Ano05b].

Anti-Circumvention [Kha05].

anti-virus [Ano05b].

anticipation [Goo00].

Any [Fis01b, HNO09, CD00, DFM04, DMS00, HR07, Po00].

Anyone [Ros07].

Anytime [DJL01].

Apache [Had00].

API [MWM01, Mor03].

APIs

BM01c. Appendix [Kel05].

Applet [ZFK04].

applets [Bis03a].

Applicability [Wya02, TM01].

Application [AD109, ACS02, Bai01b, Boy01, CL02a, CKQ03, Dam07, Dhe03, GHK+06, HF00, IKP07, JX05, Jou04, Lai03, Lee04b, LLS05b, LXM08, NP07, Oka00, PF01, PQ03b, PS01c, Pre00, RC01, Roy05, RK06, Sch01a, SFDF06, TWNA08, TEM+01, UHA+09, WG05, YSR01, Zhe02b, BG09, CMKT00, CP07, DIM08, FP00, JRS09, Lav09, MT07, MPH00, MK05a, NZ05, RSS04, SSST06, TC00].

Application-Aware [IKP07].

Applications [AF04b, AC02, AGT01, Amd04, BLST01, BH05, Bar06b, BL05a, BGK+03, BS00a, Bi03, BGOY08, BSS02, BL08, CC04a, CD00a, CV02, CGH01, CZ05, CHSS02, CS09, Cra05a, CD01, DJ01, DK02, DK07, DA03, DFPS06, FR02, GSS08, GKK09, GJ0K03, Gen04a, GRW06, G0l01a, G0l04, HR02, H06N, Hau06, Has01a, HSS04, HER05, HJ05, JT01b, JY01, KMM06, KGL04, KMO01, KKM01, Knu02, MAA07, MM07b, Nie02c, Nie02d, PS02b, RSN01, Sch06b, Shp03, SXY01, SPQ06, Vau02, Wya02, XYL09, YZ00, Zao00, Zao02, ACTZ05, Ate04, AH05, AFH06, BG08, BGL03, CCC01, CM05b, CS09, CSK08, DY09a, DFCW00, DJL01, FP09, Fin03, Fis01a, Gal02, GVC08, GKK07, GB09, HHSS01, Has02, Hen01, HKPR05, Jac00, KVN09, KNS05, Lao00, Lee04a].

applications

[LJ05a, LPW06, LB05, MY01, Mal06, MC04, MSV04, Nie04, PW08, PBD07, PC00, QS00, Ros06b, SSS06, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SPH06, WW08, WA06, WV00, YS04, ZBP05].

Applied [HW03a, HWR09, SL07, GV09, GNP05, IKY05, JY04, ZHY03].

Applying

[Elb09, KC02, Lao00d, LMS07, SQ01, SML02, TND09, vDST06].

Appointed [CL01a].

Apprehension [AJ08].

Approach

[BKM07, CFS09, CDR01, CW09, Chi08a, CB01, DJL01, Kra03, Lai07, LL05c, Lut03, OMT02, PBD00, pau02a, Pre02a, SKG09, VH09, VVS01, Vir03, XYL09, YKMB08, AA08, CGL08a, CGL08b, CGL08c, CJT01, DMM05, GGH08, Har05a, JJ01, JW01, LYM02, MT09, Mar05b,
MI09, Mos06, NN03, SLP07, SN04, SW00b, ZLX99, ZSZ01, ZL04b, ZL04a. Approaches [CGMM02, AvdH00, DG05, Fri07, Has01b, KXD00]. approach [Wan04b].

Approximations [CLZ02, Kuk01, WL02]. Approaches [BDQ04]. Apress [Ter08]. April [Ano00d, Buc00a, Chr00, Chr01, CCMR02, CCMR05, CGH∗06b, DFP06, Joy03b, Km02, Mat02, NIS00, Nac01, Sch01d, SMP∗09, YDKM06]. APSS [ZSV05].

Arabic [MAaTxx]. Arbitrarily [RW03b]. Arbitrary [AR01, BR00b, BR01, CKN00, CHJ∗01b]. Arbitrary-Length [AR01, BR00b]. Architectural [ASK07, ABM08, BS00a, GC01a, HWW05, PP06a]. Architectures [BGK∗03, KLY02, RM02, SM02, Con04, DP04, GKS05, NdM04, RH00, WH02b].

archival [SGMV09]. Archives [RC01]. archiving [DMSW09]. area [BP03a, Cal00c]. Areas [HH04, MZ04, PT06, VY01, AMW07, Buc00a, HH05, HA00, NH03, ST01d].

Aren't [Bau01a, Bau01b]. Arguments [HNO∗09]. ARITH [BS03, BC01, IEE05b]. ARITH-15 [BC01]. ARITH-16 [BS03]. ARITH-17 [IEE05b]. Arithmetic [BS03, BIP05, BGK∗03, BCDH09, BC01, CT03, Gro03, IEE05b, KM07, Kir03, PPV96, RDJ∗01, SR06, GPS05, PS04a, SOIG07].

arithmetics [Lan91]. ARM7 [DV08, XB01]. armies [Ano03b]. Army [Boy03]. Arne [Bec02]. array [DZL01]. Arrays [ABM08, BS00a, GC01a, HWW05, PP06a].

Arrived [Law05]. arsenal [Blu09]. Art [And07, Bis03b, Col03, Mar05a, MZ02, CS07a, DMS07, Eri03, Eri08, MS02d].

Article [Che08b]. Artifacts [EHK∗03]. Artificial [Cop04b, MMH02]. Arun [For04]. ASCI [MJD01]. ASIACRYPT [Lai03, Lee04b, Roy05, Zhe02, Boy01, Oka00, DN00b, KL01a]. ASIC [WOL01].

ASIP [SKW∗07]. asks [Ano08a]. ASM [MK05a]. Aspect [Kos01a]. Aspects [BLMS00, CMR06, Pel06, DLP∗09, Rup09]. Aspiration [Ash03]. assembly [Gon09].

assessing [CDD∗05]. assessment [CC05e, DMS07]. assets [KH03, NRR00]. Assignment [BRTM09, HC08, CHC04, DFM04, Hwa00, TP07, WC01b, hY08].

assignments [SWR05]. Assisted [ECG∗07, XS03, BB05, LHL04]. 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 [LX∗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 [IE09b]. ATM [Pat02a, Pat02b, Zan09]. Atomic [CNV06]. Attached [RCB00].

Attachments [Ric07]. Attack [Alm08, CKQ03, CS05b, CS03b, Des00b, Fi00, VF03, GHJ0V0, GHJ0V01, HQ01, Hug02, HW01, J00b, KCP01, K500a, 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, Duj08].
Duj09, GM00a, HAURO4, Hes04b, HG07, Iwa08, JJ02a, KS09, KM04a, LM08, Law09b, LS05b, Mir05, OS00, SIR04, XH05.

**Attack-Resistant** [LNL+08], **attacker** [BDSV08]. **Attacker** [JMV02]. **Attacking** [FMP03, KPR03, Luc00, TMMM05, BF06a].

**Attack-Based** [TMMM05]. **Attacks** [ARR03, AK03, BCP00, BP02, BM00, BCK02, BBK02, BCK02b, BM10c, Can06b, CS07b, CT08a, CS10, CKM00, CM03, Cou03, CWR09, CD01b, DP01, DFS04, DJ06, DS08, DM07b, FKSW00, FOBH05, FP01, Fry00, Fur02b, Gen04a, Gir06, GK02, HSH08a, HNZI02, HR04a, HSH08b, HLC08, ISW03, JK00d, KKS00a, KS00b, KKS01, KCJ*01, KI01a, Law09a, LLS05a, LWS05, LJ05b, MOP06, MP06, MF01, Mes00, Mes01, Mê02, MG08, OT03a, OT03b, OOP03, OST05, Ove06, PKB01, PDM09, RS01, SKQ01, Sem00, SWT07, Tad02, VV07, WY05a, WY05d, WLZ05, YYDO01, YY01, YG01b, vW01, BFS08, Bau05, BCS08, BZ03, CKL09, CS05a, DK08, Geb04, HSH08b, HSH09, Has01b, Hsu05b, HL05d, In005, IM06, JDJ01, KS05a, KTC03, LPV09].

**attacks** [LSH00, MMJ05, NS05a, NLD08, OST06, PQ03a, RG05, Sch00c, Sch01f, SL06, SK05b, SW00b, WL07a, WL04a, Yan07, YS02, ZSJN07].

**attractors** [HHYW07]. **Attribute** [LY05, RSA00e, IY05]. **Attributes** [SS01b]. **Auction** [AS01a, Ano01a]. **auctioning** [RCG+05].

**Auctions** [Bra01b]. **Audio** [Arn01, CS05c, DRL09, MH05, WNY09, WWL02, XFX01, WQ06, BS01b, KJ05, KN03]. **Audio-** [KJR05]. **Audio-and** [BS01b, KN03]. **Augmented** [CS07e, You01]. **Augmenting** [AL04].

**August** [AMW07, Bel00, B02, Bon03, Fra04, HH04, HH05, HA00, JQ04, KK02, Kil01a, KP01, MZ04, Men07, NH03, PT06, RS05, Sch00a, Sch04a, Sch04b, Sch05a, Sho05a, ST01d, USE00a, USE00d, USE01c, USE02b, VY01, Yun02a]. **Australia** [Boy01, IZ00]. **Austria** [DKU05, Pf01, Jef08]. **Authentic** [DGMS03, Dur01, SS01b]. **Authenticate** [Bau03a, Bau03b]. **Authenticated** [AGT01, BN00a, BPR00, BU02, BC04b, BM01, BMP00, BCP01, CPP04, Chio08b, DG03, DA03, EP02, GKK07, GL03, GTTC03, HS07, KOY01, KY03, Kra03, Lee01, LH09, MPS00, Mac01, MSJ02, MND04, NA07, Nam02, Ngu05, Pol01, SK00, Vau05b, WC01a, YPPK09, Yi04, ZWC02, BK04, BCP07, CY05, CYH05, Che04a, CLC08, CJ04, CJO4, GL06a, GMR05, HTJ08, HWW02, HWW03, Hsu05a, Hwa05, HL05c, HL05d, KOY09, KRY05, LKK03a, LKK03b, LL04a, LL04b, LL05a, LKY05c, LKY05d, LHC08, LLR02, LLR06, LWK05a, Mi08, PQ03a, PQ06, RBB03, Sei05, SW05, SC05b, TLH05, TJ01a, Tse07, WH02a, XY04, YW05, YC09a, YS02, YSH03, YRY05b, YPKL08, ZC04, ZAX05, ZW05b, ZL05].

**Authenticating** [AIP01, Chi08a, CGV09, Fur05, JW05, PM08, RCBL00, YSS01, Lin01a]. **Authentication** [AAK09, AP09, ANRS01, Ano01b, Ano01c, Ano01e, Ano02d, AHKM02, ANL01, BH06, BACS02, BCL05b, BCG02, BM03a, BH00a, BCC01, BDKB00, BR02, BDFP05, BDF01b, BM03c, BL02, BLDT09, BWE00, CV03, CGP08, CS07b, CLK01a, CLK01b, CC05b, CC09, CJS03, CWY05, CT09, Cim02, Cir01, CGK02, CJK04, Cou01, CMB05, Dav07, DP00, Dwo03, ETZ00, EM03, FIP02a, FGM00b, Fre03, FSSF01, Gan01a, Gab03a, GMW05, GSV02, GD02, GTO2, Gut04c, Had00, HSZI01, HSHI02, HSHI06, HKW06, HY01, Hoe01, HS01b, HP00, HL07, ISSZ08, Jab01, JP02a, JP07, JP02b, KJ05, KC09b, KH05, Kra01, Kut02, KZ09, KS06b, Law05, Li01, LIT04, LB04, LL05c, LSH03b, LM00, LLH08, Lys07, MM01a, Mal02, MJ04, MD04, JR03, MGC02, MNT06,
Nao02, Nik02a, Nik02b, OKE02, OHB08].

**Authentication** [PBD00, Par04, PBC05, PK01, Qu01, RKZD02, Ric07, Ril02, SNWX01, SR01, Sch04c, Sch05b, Sei00b, SY01b, SBG02, Smi00, Smi01c, Smi02, SE09, SK06, Str01b, SJ05, SYLC05, SC01, TK03, TZZ09a, TZZ09b, Tsa01, VN04, WLLL09, WC09, Way01, Way02a, Wea06, WKB08, WT02, WS03, WL07b, WL075, WHL05, XYL09, YL01, YEP+06, YSR01, YLLL02, YK01, Za00, Z04, ZBLvB05, AvdH00, AF04a, All06, Ano00k, Ano00l, AAKD09, AL04, Bad07, Bel04, BGP02, BSSM07, BFG04, BFG05, BS01b, BB02, BDFP02, BFM07, Cer04a, CC01, CCK04a, CL04d, CC04b, CKB4b, CC05c, CY05, CCS08, CWJT01, CJ01, CJ03b, CH07a, CL09, Coc01a, CMdV06, Da01, DY09a, DG+04, DG05, DW05, FGM03, Gan08, GLC04, GT08, GS09, GUQ01, GTZ04, HM02a, Hen06b, Hsn05b, HYS03, HLL04, HL05b].

**authenticator** [CKY07].

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

**Author** [An00b, An01d].

**authorisation** [SN07].

**Authorities** [CHSS02, HW04, WH02b].

**Authority** [Con00, JLL02, CCH05, KB09].

**Authorization** [BACS02, CJ+04, LS05, RKZ02, YT09, GJ05, JE04, Lin07, SR01, WL04a, WZ05, YJ04].

**Authorship** [Top02].

**auto** [YY00].

**auto-recoverable** [YY00].

**Automata** [LZ04, MG02, Wue09, Bao04, CC05d, K03, Lf00, LQ08, Mon03, SBZ04, SHH07, TC00, dRMS05].

**automate** [Bur02].

**Automated** [CD01, LL05, LL09].

**Automatic** [BD04a, GJ05, GL00, ST01c, XN+05, RG05].

**automorphism** [Pae03].

**automotive** [LPW06].

**Autonomic** [VH09, Che05b].

**autopsie** [Car00].

**auxiliary** [Dam00, DKL09].

**availability** [CBD+05].

**Available** [DJLT01].

**AVBPA** [BS01b, KJR05, KN03].

**Average** [KMT01, CGHG06].

**average-case** [Mic02b].

**avoid** [Tyn05].

**avoided** [CNPQ03].

**Award** [RSA03a, Bar00b, Coc03].

**Awarded** [Coc02b].

**Aware** [IKP07, OHB08, CBSU06, Zea00].

**Awareness** [HLM03, BK05].

**Away** [Coc03, Ols00, Tee06].

**Awkward** [TvdKB+01].

**Axiomatization** [dH08].

**B** [SPK08, YG01a].

**B-Spline** [SPK08].

**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** [H0f01, Lu02].

**Ballot** [Cha04].

**Baltimore** [AC05b, ACM05c, GL05].

**Banach** [AW01].

**Bandwidth** [CGJ+02, YY01, SLP07].

**bandwidth-efficient** [SLP07].
Bandwidth-Optimal [YY01]. Bangalore [MMV06]. Banking [HKW06]. Barbara [Bel00, Fra04, Kil01a, Men07, Sho05a, Yun02a]. Barcode [Che08b]. Bare [DPV04]. Barken [Sty04]. Barret [Gro01]. barriers [Kov01]. base [DIM08, IR02].

Based [Ano01c, ANR01, AF03, AJO08, BDG+01, BKLS02, BMS02, BMS02, BEN02, BFR01b, BF03, BB04, Bon07, BCHK07, BG07, BPR+08, BD03, BM01, Bo03, BQR01, BM01c, BSN00, BRTM09, CGFSHG09, ČvTM01, CK02a, CGMM02, CF01b, CC02a, CPP04, CDD07, CS07b, CLT07, CHSM02, CHM+02, CZK05, CM05a, CTH08, CGK+02, Coo01b, Cou01, CFS01, CS00, DDM00a, DMM05, DTM03, EH03, EM03, FL06, FM02a, FM01, FGL02, GMP01a, GMP01b, Gar03a, Gen00b, GM02a, GL03, GS02b, Gen03, GST04, GSP06, Gro01, Gro03, GW01, Her06, HM02b, HS00, HL02, HQ05, HC08, HH09, Ig02, Jam00, KBD03, KLM02, KEP03, KK01, KKG03, KY02a, KL05, Kel05, KY01c, KY02b, KC09b, KK02, KC02, KCD07, KP03, Kra02a, Ku02, KWP06, KT00, LLL02, LP03, LKLK05, LHT09, LZ01].

Based [LZ04, LL05c, LPZ06, LY07, LLRW07, LWK00, LSC03, LHS05, LS02, LSS05, LCD07, MP00, Mar08, Mar08b, MN01, Miy01, MG02, Mii01a, MSU05, NMO05, Nak01, Nam02, NB01, NSS02, Nov01, NSK01, PV06a, PV06b, PP06a, PZL09, Ri02, RE02, RH02, RS00, RS03, RS08, RMC01, Sal05b, Sch01a, SFC09, Sha02, Sha01e, SO02, SY01, Sm03a, SBE01, SGB01, TM05, TYL02, TZT09a, TZT09b, VMS05, Vau05b, Ver06a, VHP01, VK07, WVR02, WY02, WZ05, W05, WC01, WH09, WBD01, WC04, XYL09, YKMY01, YT09, YV0001, YSS01, YKW01, YLH05, ZK02, ZGLX05, ZP05, ZJ09, ZS05, ZW01, vDW04, AAP07, AA08, An02b, App05, AAK09, BGB09, BR04, BFG08, BS01b, Bia01b, BMW05, BLP06, BGL03, BDS09b, Buh06, CG06, CL02b, CL04d, CL00, CH04, CY05, Che05a, CCS08, CGL03a].

Bases [AAG+01, ADDS06, BKP09, B+02, ČvTM01, EBC+00, FJ03, FLA+03, CCT08, Fan09, ZT03]. Basic [Gol01b, Gol01a, Gol04, Kat05b, Puc03, Ste02, Bon00]. Basics [Leh06, Lu02].

Basing [BPR07, CHL02, AGGM06, AGGM10]. Basis [RMH03b, Vav03, vW01, GPS05,
LS05b, RMH03a. Batch [Ara02, HLT01, PBD07, Sha01d, BLH06, HLH00]. Batching [SB01]. Battery [CBSU06]. Battle [Bud00a, Bud02, SM00c, SM05, SM07a]. Bay [Cal00c]. Bayes [Goo00]. BB84 [Ina02a]. BC [IEE02]. BCH [MLC01]. BDD [KLN+06, Kra02a]. BDD-Based [Kra02a]. Be [Bar00a, Pau02a, CNPQ03, YJ00, vT01]. Beach [IEE00a]. beat [Lev01]. 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, QS00]. Belief [BPST02]. believing [Buh06]. Bell [BZ02, Eke02]. Benchmark [Ase02, TLYL04, LDH06, YLT06]. Bendy [Sas07]. Benefit [YKLM02a]. benefits [CH00]. Benford [NM09]. Bergen [Ytr06]. Berkeley [IEE06]. Berlin [FLA+03]. Bermuda [Bla03]. Bernard [DNRS03]. Berners [Coc02b]. Berners-Lee [Coc02b]. Best [Bau01a, Bau01b, MFS+09, Go08, Ste02]. BestCrypt [Bau02b]. Bethesda [ACM09]. Better [FV03, PM00, RR02, SK01, HLLL03, Pau03]. BetterBASIC [ASW+01]. Between [DKMR05, Ket06, Ngu05, NN06, Fau09, GKM+00, GC05, MSV04, Pau01, RW03a, SK06]. Beurling [Bec02]. Beyond [Gor06, LMW05, Mar08a, Sch03, See04, Sty04]. BGP [ZSN05, vOWK07]. Bi [Cou04, PJK01]. Bi-directional [PJK01]. Bi-linear [Cou04]. Bias [CL02c, Sei00]. Biased [BS00a, LSKC05]. BiBa [RR02]. Bibliography [Bee05]. Bidiagonal [BR09]. Bidiagonal-Singular [BR09]. big [RR03a]. BigNum [SR06]. Bilateral [CTO8a]. Bilinear [BGLS03, BMS03, CL04a, HMS04, KK02, LC05b, VK08]. Bill [Gau00a]. billing [SSM+08]. Binarization [LSKC05]. Binary [AD09, HHH01, LSKC05, OSSST04, SKG09, WCJ09, ACTZ05, BG08, BG09, FSGV01, GB09]. Binary-Ternary [AD09]. BIND [Kle07]. Binding [DN02b]. BioAW [MJ04]. Biometric [AHK02, Dal01, EM03, HWH01, KJR05, LTT+04, PK01, SR01, Sas07, Way01, Way02a, Wea06, BS01b, KN03, Li05, LST+05, MR00, Smi00, MJ04, TBJ02, ZJ04]. Biometrics [Ash03, Bjo05, JR03, Rii02, Str01a, BSSM+07, BCP+03, Buh06]. Biometrics-Based [Rii02]. Biomolecular [Bii90]. Birds [MLM03]. birth [Bud06, SE01]. Birthday [Wag02]. Bismulation [BJP02]. Bit [AIK+01, BK06a, BL08, CGH01, CDL+00, DMS00, GS07a, IIT03, KZ07, LNS02, MS09d, PCC01, RMH03b, SM03b, SXY01, VKS09, ATSVY00, Bar00a, BK07, GPX08, KZ03, KKL09, Luc00, Pri00, RMP08, SW05, UHA+09, WW08, ZFK04]. Bit-Fixing [KZ07, KZ03]. bit-substitution [GPX08]. BitLinker [Kor09]. Bits [BS01d, SZ01, HN04, Slp02]. Bitslice [DPV01]. Black [Ano01i, CF02, CFS05, DI05, DIRR05, DS08, KY01d]. Black-Box [Ano01i, BRS02, CF02, CFS05, DI05, DIRR05, KY01d]. Blackmailing [PS01b]. Bletchley [Sal00b, Cop05, Cop06, HS01a, Sal05a, SE01, Sni01b, Wei06, Win00]. Blind [AO00, BNPS02, BB00a, BSC01b, CL01b, JKK+01, LY07, Na05, Pau02b, SPK08, ZTP05, ZK02, Fan03, HC04a, JLL01, JL04, LHY05, LCZ05b, MS09a, SV08a, SHT05, WHH05, ZC05]. blindness [AvdH00]. Blink [Sas07]. Block [AIK+01, BRS02, BR02, BSC01a, CVT001, Can01b, CLL00, CP02, CMB+05, CR01, DR00a, Dwo03, EYP00, Flt02a, HSH+01, JKK+01, KCP01, KYHC01, KKG03, LLR07, LRW02, MV00, MS02a, NP01, OMS01, Pat01, PS06, Pli01, RMS05, ...
SM03b, SYY+02, SKU+00, SKI01, WCJ09, XH03, YG01b, Bai08, BF06a, DY01, Dun06, Egh00, GPX08, Hey03, JK01b, Jun05, Kat05a, KJ01, LDH06, LCP04, LKH+08, MMJ05, PSP+08, RBB03, SIJ10, SHH07, WF02, XH05, YG01b.

Block-Based [LLRW07]. Block-Cipher [BR02, RBB03]. Block-Cipher-Based [BRS02]. Block-DCT [BSC01a]. Blockcipher [GM02c, OS07]. blockciphers [Fur01]. Blocks [Jou02]. Blockwise [JMV02]. Blockwise-Adaptive [JMV02]. Bluetooth [GBM02, LV04, LMV05]. Blunders [Bur01]. Blur [VHP01]. Blur/Deblur [VHP01]. Blurring [LSKC05, SK06]. Board [CGS01]. Body [Bam02, TG07]. BOEL [Fin02]. Boethius [Eag05]. bolstered [Ano01h]. bombe [Wil01a, Tur04]. Bombs [Canc03]. Boneh [ASK05, Hess04a]. Bonn [DRS05]. Book [And04, Duw03, Eac05, Fal07, For04, Gas01, Gun04, Imr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, MP01b, Nie02a, Nie04, Pap03, Pap05, Rec01, Rot07, Sal03b, See04, Shp04a, Sin02, Spr03, Sty04, Ter08, Top02, Uzu04, Wal00, Was08a, Kat05b, Lam07, Lmn09, MaaT05, Sin99, Sin00, AAG+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+02]. Boot [HSH+08a, HSH+08b, HSH+09]. Border [MJF07]. Borders [PCT07]. Boston [USE01b, USE01a]. bot [Ano08b]. Bottschaften [Sche09]. bottleneck [WL02]. bottlenecks [HTW07]. Bound [CY08, DGN03, KMT01, HLL03, hY08, GW00]. Boundaries [PCT07]. Bounded [Che04b, DFSS08, DIS02, Din01, Din05, Lu02, MPSW05, MSTS04, Vado03, DFSS05]. Bounded-Quantum-Storage [DFSS08].

Bounding [DM07b]. Bounds [BDF01b, BP03b, DI01, GGKT05, RW03a, SNWX01, SM00b, Shp03, Wal01, WW05, GT00, GGK03, JZ09, PS02a, Shp99]. Bouwmeester [Duw03]. Box [Ano01i, BRS02, CF02, CFS05, DI05, DIRR05, DS08, FM02b, KY01d, Kii01b, SMTM01, JmBxGxMn05]. Boxes [Bih00, BCDM00, ZC00]. BP [Wei00, Wei05]. Braid [AAFG01, CJO3a, GM02a, Hug02, KLC+00, LLH01, LP03, MSU05, Cho08b, Hen06a]. Braille [Pau02b]. Branch [AKS06]. Branches [Fe06]. Break [BP06, Sin02, HM04, WA06]. Breaker [Rey01]. Breakers [CD00b]. Breaking [BKN04, DKFX05, GO03, GK20, Kov01, KR03, Kii08, Sal00a, Wri05, Fie09, Gar01, SE01, Smi01b, SL07, Swe08]. breaks [OS00]. Breakthrough [Coc02a, LR01, Pau02a]. Brief [Bon07, Cos03, Kir01a, Boo05, Gra01]. Briefs [MP00, PM00, Pau02a, Pau02b, Pau03, Pau99]. Bright [Ano01i, LNP02]. Bristol [DFCW00]. British [ACM08, Fie09, Fra01, Syv02, Bud00b]. Broadband [MP00, SLO7, MJF+08]. Broadcast [AF106, BGW05, CKPS01, CNV06, DS03, FFW04, GSW00, GKK007, GRW06, HS02a, HLL05, LP02, SNW01, Woo00, ASW00, KSW06, Kru05, Mar05b, NLD08, RG09, WDLN09, LNO4].

broadcasting [TI01b, WH02b]. Broke [Urb01, KS04]. Broken [Ahn08]. Brooks [Bar00b]. BRSIM [BPS08]. BRSIM/UC [BPS08]. BRSIM/UC-soundness [BPS08]. Bruce [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, Bor00]. bugs [GJL06]. Building [Jou02, Kn07, Mar02a, And08, Bra01a, FB01, LS05b, McG06, MPH06].
[BBKN01, BPR05, BR00b, DGH+04, Fer06, JMv02, KI03, Vau01, Vau02]. **CBIDs** [MC04]. **CCA** [KOMM01, Mü01b]. **CCA2** [BST02, Lin03, RG09]. **CCA2-Secure** [Lin03]. **CCGrid** [TL06]. **CCM** [Dwo03]. **CCS** [Mar02b, MS05b]. **CDH** [CM05a]. **CDH-Based** [CM04]. **Cell** [Fox00, MYC01, SHL07]. **Cell-phone-free** [Fox00]. **Cellular** [Laf00, LZ04, MGC02, PZL09, SB04, Bao04, ETM05, KK03, SHH07, Wan04a, dRMS05, Wue09, SS0+08]. **Center** [AUW01, CH01a, CYH04, LPM05]. **Centered** [BKM07, CM05]. **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, CM01, RdS01, Bra01a, LCK04, ZSM05]. **Certification** [AN01k, CM01, RSA00b, BGB09, BD04b, KB09]. **Certified** [AN01, CSV07, NZCG05, BCL05a, BCW05, CWH00, CCH05, C05, HW04, HW05, HL04, LL06, LWK05a, NZS05, Sha04b, Sha05b, TLH05, Tsa05, TJC03, WH03]. **Cerven** [Sal03b]. **CFS** [Ito01]. **ChaCha** [Ber08]. **Chain** [YT09, YZ00, Wue09]. **chain-rules** [Wue09]. **Chained** [BCC01]. **chaining** [PCC03]. **challenge** [LM08, LW05a, PRS04]. **challenge/response** [LW05a]. **Challenges** [Cla00a, GV09, Nao03, Sta03, SVE09]. **Chang** [CWJT01, ZC05]. **Chang-Wu** [CWJT01]. **change** [CYH05]. **Changes** [Murt01]. **Changing** [BST03]. **Channel** [BU02, CHV03, Law09a, LCK03, Mö02, NMO05, OT03a, OT03b, Sch06a, SYL05, ARR03, BP03a, BG07b, Buh06, CNPQ03, KSWH00, LCZ05b, MS09c, PSP+08, WL07a, YTWY05]. **Channels** [AIP01, CK02b, Nam02, Vau05b, LH04]. **Chaos** [JK01b, SK01b, WZW05, JK01a, LMC+03, McN03, PGS+09]. **Chaos-Based** [WW05, SK01b, JK01a, PGS+09]. **Chaotic** [LLL+01, SXY01, US02, Vav03, AMR00, AMR04, GhGSS00, GB09, HHYW07, HLwWZ09, JK01b, LMC+03, LYGL07, MA02, PBM01, PS01a, PZL09, SPG02, SL09, UHA+09, VSK09, WG02, WW08, kWPwW01, WL04, YZEE09]. **Chapman** [Kat05b, Was08a]. **chapters** [MAaT05, Tat05]. **Characteristic** [Gau02, GPS06, KT00, Ver02, GPS05]. **Characterization** [AJ08, Nam02, XH03, BGM04, KY00, QVP05, XLS06]. **Characterizations** [Pas05]. **Characterizing** [BTW05, BTW08]. **Charging** [BACS02, RH02]. **Chatter** [Kee05]. **Chau** [BNPS02, KLN+06, WH05]. **Chaumian** [Mö03a]. **Chaining** [CCL09, OKS06, PZ01, PZ02b, PZ02a, ZP01]. **check** [Kir01b]. **Checkable** [BPST02]. **Checking** [BL02, JP07, KLN+06, YJ00, GG+08, RG05]. **checklists** [Sha01a]. **Checks** [FM02a]. **Checksums** [Sto01, SGPH98]. **Cheju** [Kim01]. **Chemical** [EIG01]. **Chen** [LW05c]. **Chennai** [CV04, RD01, Roy05]. **CHES** [JQ04, KKP02, KP01, KN01, RS05, WKP03]. **CHESS** [LKHL09]. **CHESS-64** [LKHL09]. **Chicago** [ACM04b, Top02, Con00]. **Chien** [YR05]. **Children** [Pau02a, Sey00]. **China** [B+02, DWML05, FLY06, JY04, L1+04, Li05, LST+05, ZJ04, ZYH03, An00c, TZZ01]. **Chinese** [LLT+04, Li05, Sch01b, CAC06, YKL03]. **Chip** [BNPW03, DV08, MM01b, MM01c, MP00, Fox00, ISTE08, An00b]. **Chip-Secured** [BNPW03]. **Chipkarten** [An00b]. **Chips** [An00d, Pau02b]. **Choice** [Jam00]. **Chosen** [BCHK07, CKN03, CHJ+01a, CHJ+01b, CS02, CS03b, DN02a, Des00b, DK05, FP01, IM06, JKS02, JJ00b, KS00a, KY01a, KCJ+01, KMM03, KM01c,
Codebook-linked [YWWS09].

Codebreaker [Han03, Pin06].

Codebreakers [Bec02, Gan01b, Gas01, HS01a, Kah67a, Kah67b, Kah74, Kah96].

Codebreaking [Bud00a, Bud00b, Sin01b, Alv00, Bud02, Cop05, Cop06]. codec [Che08a]. Codes [MLC01].

codes [MLC01].

codeword [AJ08]. Coding [Buc00a, CS05c, HHL +00, Joy00, LLL +01, MZ02, Pat03b, RK06, Sal05c, Sma05, 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 [Lin01b]. Coin-Tossing [Lin01b]. Coins [HR04b]. Cold [HSH+08a, AJ08, HSH+08b, HSH+09].

cold-boot [HSH+08a, HSH+08b, HSH+09].

collaboration [ED03, PCSM07, SBG05, SBG07]. collaborative [LLY06]. collapse [SBB05].

Collection [GMM08, Bro05a]. Collections [Kuh00]. Collective [BBB+02]. collide [GPN05]. Collision [DG02, IK05, MS09c, WYY05a, WYY05d, GM00a, Sem00].

Collision-Resistant [IK05]. Collisions [BC04a, GIS05, HR04b, WFLY04, WYY05b, WYY05c].

Collusion [BGW05, HNZJ02, Zan01].

Cologne [WK03]. Color [CTL04, Che07, Che08a, CTY09, FGD01, AEEdR05, CDD07, Yan02, 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, Gan02, GHPT05, GB09].

Combinatorial [GMW05, SLTB+06, Hen06a].

Combinatorics [Lee03b]. Combined [LLS05a]. Combiner [Sar02, LL06].

Combiners [AK03]. Combining [Abe04].

Comes [Mar08b, An03e]. Coming [Dan01]. Commemoration [BZ02].

Comment [SCS05b, WY05, WLW04].

Comments [AS01c, CGH+00b, JW01, MNFG02, SKW+00, CJT04]. Commerce [CLK01b, GS02a, Kir01a, Sta00, Uni01, ZYM05, BM30a, FB01, Gra01, MY01, SN07, YC09a].

commercial [CC05, YLR05]. Commitment [DN02b, DMS00, FF00, CAC06, HR07, KKL09]. Commitments [BN00b, CF01a, DFS04, FM02a, Gen04a, HNO+09]. Committee [Uni00a, Uni00b].

committing [DN00a, Nie02b]. commodity [CGL+08a, CGL+08b, CGL+08c]. Common [Pas03, TG07]. Commonweal [PY05].

communicating [Hut01]. Communication [AK02a, ANRS01, BYJK08, BBK03a, BIW08, Big08, Col03, Fis05, GKK+09, LLS+09, Mar07, NA07, PL01, Sch06b, SKR02, Wri05, vDW04, BYJK04, BC05b, 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 [GN06, HJ07, Igl02, Kra01, Lan00a, Lan04b, LCK01, LL01, MS05b, Sal01b, Van05b, VMC02, BP03a, CY04, HW02, LC04a, Sal05c, Ser06, SJ05a, Wil09, WGL00, YTW05, DKU05].

Community [SK06]. commutativity [HRS08]. commuting [CKRT08]. Compact [CG03, JT01b, SMTM01, YT09, ZLK02, JAW+00, Mic02a].

companies [Ste00].
Company [ASW01, Za00]. Comparative [DPR01, GLG+02, Kat05b]. Comparing [HU05, KLN+06]. Comparison [GC00a, GC01a, Gau02, JR+06, MS02c, SW00a, WW00, FGM03, JL03, Sma01, WB00].

Compendium [Lut02]. Compensated [AAK09]. Comparisons [DPR01, GLG+02, Kat05b]. Comparing [HU05, KLN+06]. Comparison [GC00a, GC01a, Gau02, JRB+06, MS02c, SW00a, WW00, FGM03, JL03, Sma01, WB00].

Compilers [Lut02]. compile [DFG00, Oiw09]. Compilers [Lut02]. compile [DFG00, Oiw09].

Compliance [LMW05]. Compliant [CGBS01, RVS09]. Component [BSL02, Hei01, TEM+01]. composability [PS04c]. Composable [AF04b, BOHL+05, BLD09, CF01a, CK02b, DN02b, DN03, NMO05, RK05, Can01a, CLOS02].

Composite [CQ01, GM01a, RDJ+01, Zhe01]. Composition [BJP02, BN00a, CR03, CV02, Pie05, Sh00a, Can06a, LL02, LL06, Puc06].


Compressibility [HN06]. Compression [ABM08, BD03, CC06, HSCK01, Kei02, LHS05, RS08, Sal07, SDFH00, WWL+02, WC03, FS08, Gar04, La00, LJ05a, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, TTZ01, Zir07].

Compression-Encryption-Hiding [BD03]. Compromise [Ahm08, Lai08]. Compromised [ZYN08]. Computer [ACM00, ACM01a, ACM01b, ACM02, ACM03b, ACM04a, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10, ASW+01, BBDD00, CGH00a, CLK01a, Cop04b, EP02, JP03, LBA00, LKHL09].
19

continued [Dan02]. Contra [Mah04]. contract [WK05]. Contrast [BDDS03, HKS00, HT06, KS03, CDFM05]. Contrast-optimal [HKS00]. Contrast-Sensitive [HT06]. Control [ABEL05, ANRS01, BW07, CGMM02, HC08, LY05, Sma03a, ZGLX05, BN08, DFM04, DPT’02, JW06, KNS05, LKZ’04, MD04, MSP’08, PS04b, STY07, WC01b]. Control-flow [ABEL05]. Controlled [GVC’08, IMM01, AW05, AW08, LAPS08]. Controlling [HY03, MS03b, MS02d, WL05]. Controls [Har01a, Har01b]. conventional [CJ04, YW05, YRY05b]. Converging [Pot07]. Conversation [GK04]. conversations [VAVY’09]. Conversion [CDI05, Ket06]. Conversions [K101b]. Convertible [Chi08b, LH04, LHT09, WH02a, CL04b, LWK05a, ZW05b]. Convolution [PG05]. cookbook [VM03]. cookies [Cha05a]. Cool [Ano00d]. Coordinate [OS01]. COPACOBANA [GKN’08]. Copenhagen [TBJ02]. Copley [USE01b, USE01a]. coprocessing [ML05]. Coprocessor [Gut00, Ito00, LS01b, OTIT01, AV04]. Coprocessors [Smii02]. Copy [LTM’00]. copying [SV08a]. Copyright [Kha05, LLL02, PBB02, XF01, ZTP05, Gil07, Kw03a]. CORBA [TEM’01]. Core [BF00a, Din07, DV08, HMS04, TPS01]. Corfu [SM07b]. Corner [Mar08a, TR09a, TR09b]. corners [Blu09]. Corporate [HW01, KH03]. Correcting [M202, NN06, YYDO01, ZYR01]. Correction [BQR01, CTBA’01, Din05, LN08, LW05b, MPSW05, SKQ01, TEM’01, Gar04]. Correctness [PBB05, Bel07b, HSD’05, dH08]. Correlated [FWW04]. Correlation [BSC01b, CJS01, Gol01c, JJO0d, LV04, LMV05, MH04, Nyb01, SY01a, WRW02, ZC00, GG05b, JJ02a]. Correlations [KM00, KM01b]. corruption [XNK’05]. COS [FF01a, WB02]. Cost [CDF01, FBW01, PD07, Sta05, YEP’06, CL09, SHJR04, YLR05]. Cost-Effective [PD07]. cost-ineffectiveness [YLR05]. could [Cla00b, Pau02b]. Counter [DI02, QS01, SLG’05, SL60, MMJ05]. Counter-Measures [QS01]. Countering [PP06b, SK05b]. Countermeasure [IIT03, MMT09, OT03a, PKBD01, YKLM02a]. Countermeasures [Av03, Fry00, GM00b, MOP06, OST05, Has01b, JDJ01, Man08, OST06]. Counters [KMO01]. counterterrorism [Na05]. Counting [Gau02, Kuh00, Hig08]. Couple [SXY01]. coupled [LF03]. course [AA04b, GV09, GL05]. courses [Gha07]. Cover [GA05, Gut02a, LNP02, NN03, RS00]. coverage [DS00]. coverings [SC02b]. Covert [Col03]. Cozens [Sal03b]. CPCMS [Sha02]. CPI [ECG’07]. CPN [AADK05]. CPOL [BZP05]. CPUs [ESG’05]. Crack [Sin02, Ano08b]. Crackberries [Sta05]. Cracked [AAG’00, Nic01, Pri00]. Crackers [Ols00, SEK01, SEK02, NRR00]. cracking [DZL01, BZ03, Cur05]. Crackproof [Sal03b]. Cracks [Bar00a, Ste05c]. Cramer [Luc02b, VMSV05]. CRC [Kat05b, Spr03, Was08a, SGPH98]. Creation [MV01, Top02, MB08]. Creator [Coc01a]. Credentials [CL02a, CL04a, LLW05, LLW09]. Credit [CNB’02]. Crete [ACM01a]. crime [Cas02, KB00, Lau08b]. criminal [Men03]. criminals [Win05c]. Criteria [Can01b, IBM00]. criterion [QPV05]. Critical [LKM’05, SE09, CS07a, Gor05]. cron [Oue05]. Cropping [DFH00]. Cross [Ban02b, SM08, LCX08, SL07]. cross-authentication [LCX08]. Cross-disciplinary [SM08]. cross-layer [SL07]. Cross-Platform [Ban02b]. crowd [Fox00]. CRT [FMP03, Kuh02a, May02]. CRT-Exponent [May02]. crypt [Per03].
Cryptanalyses [Kan01, SKU+00].

Cryptanalysis
[ASK07, AMRP00, And03, Ano07b, Ano07a, BDG+01, Bao04, BLH06, BP03a, BBK03a, Bar06a, BP01a, BD00a, Bih00, BMFR02, BDK02a, BDK02b, BSW01, BDD03, BD00b, BCC01, CGFSH09, CV02, CC01, CL01b, CY05, CKY05, CKK+02, CWJT01, CJT03, Cho06, Cho08b, CHJ02, CP02, Cout, CGJ+02, DG00, DGP07a, DGP07b, DGP09, DN00b, FJ03, FKS+00, FKL+01b, FKL+01a, Fin06, Fru02a, Flu02b, Fur01, Fur02a, Fur02b, GSO7a, GM02a, GJSS01, GS02c, GM02b, GM00b, GMB02, GC00b, Gra02a, GS09, GKN+08, HPC02, HQR01, HAU04, Hen06a, HLL+01, HSM+02, HHK+04, Hsu05a, HLH00, Hwu00, JK02a, J000c, J01, JnBdXgXm05, Jou09, J03a, KM02, KW03, KS00b, KRY05, KW02, KRS+02, KKS00b, Kra02a, KC05, Kuh01, Kuh02b, KHKL05, L03C, LHL+02, LP03, L00e, LL05a, LR07, LBGZ01, LBGZ02, LLH04].

Cryptanalyst
[Wil06].

Cryptanalytic [BS00b, KFSS00, Oec03, QSR+02, Yan07, Wil01a].

Cryptic
[Wri05].

CRYPTIM
[Ust01b].

CRYPTO
[Al00, Men07, Sho05a, Ahm08, Ano01j, Ano03e, Bau01a, Bau01b, Bur01, CCM01, CNB+02, Lev01, Lev02, Mar08a, Mar02b, MC04, Mem01b, SYLC05, TR09a, TR09b, Yun02b, Bec02, BK05, HGNS03, Web02, Bel00, Bon03, Kili01a, Yun02a, Se100a].

Crypto-algorithms
[Ano01j, CCM01].

Crypto-based
[MC04].

Crypto-CCS
[Mar02b].

Crypto-integrity
[Yun02b].

Crypto-systems
[Ano01j, CCM01].

Cryptoanalysis
[HSIR02, LD01].

CryptoAPI
[Bon00].

Cryptoclub
[BP06].

Cryptocomplexity
[Rot05, Fal07].

Cryptocoprocessor
[HV04].

Cryptographer
[Joy03b, Nac01, Oka04, Po06, Pre02c, Men05].

Cryptographers
[Coc03, KLN+06, Tsa07, Bel07a, Han03].

Cryptography
[AC02, AADK05, AL00a, ADH+07, Ase02, BLST01, BDF+01a, Bar00a, BGK+03, Bih03, Bla01a, Bor01, BDP00, Bia01b, BM01c, BL08, Bur06, CC04a, Can01b, Car02, CCD01, CHL02, CKY07, CB01, Cra05a, CS09, CO09, DD02, DHR07, DFM04, DS00, DWN01, DHR00, DV08, DFG01, FIP01b, FS00, Fox01a, GMM00a, Fri01, GMP01a, Gar05, GSS08, GGT05, G02, GTH02, Gor02a, GL00, GU01, Gut00, Gut02b, Gut04a, HTS02, H06, Har06, Has01a, HL05a, Hlu04, Ig02, IY00, Ito01, IMM01, JT05, KMO01, KY01b, KY02b, Kili01b, KS06a, Knu02, Kis02, Law09a, LN08, LS05a, LKJL01, MS02a, MOP06, Mea01, MNP01, MRL+02, MMH02, Mor03, MK05b, MSU05, NIS01a, NIS01b, Na03, Nd05, Ngu05, Nie04, OTI01, OP01a, PKBD01, PR08, PJ0H09, Pem01b, P601, Pin02, Pin03, Po02b].

Cryptographic
[Pot06, Pre00, Pre02a, Pre02b, RSA00d, RSA01, RR00, RSS06, Rot01, RSN+01, SM00a, SS01a, SGM09, Sha02, Ship03, Shy02, SDFD06, SR06, SL09, TLY04, TWNA08,
TBDL01, Uzu04, WKP03, WN02, WBL01, WC01b, You01, Zha08, AMRP04, ÁCTZ05, ALV02, AV04, BGB09, BDSV08, Bla01b, BP05, BG08, BG09, BDNN02, BD04a, BGL+03, BMV06, BR05, Can01a, Can06a, CHC04, Cih03, CC05d, CDL06, DP04, Dug04, DFC00, FS03a, FSGV01, GT00, GPV08, GJ04, GM04, GB09, HY03, IYK03, IYK02, JW01, KAM08, KS00, KP03, LMTV05, Lau05, LLW05, LLW09, ML05, Mea04, MT07, Mic02b, MRST06, Mon03, NN03, NdM04, NdM06, PS04a, PS09, PH05, Pri07, Puc06, QPV05, Reg03, Ren09, RHM04, RBF08, RAL07, RSS04, ST03a, SOIG07, SW00b.

cryptographic
[kWpLwW01, WLW04, XLMS06, YLT06, ZLK99, ZWWL01, ZL04b, dH08, BWBL02, JQ04, KKP02, KP01, KNP01, RS05].

Cryptographically
[ADD09, AHS08, BJF02, BFCZ08, BB00b, FR08, MS02b, RGX06, Aam03, AW05, AW08, Lau08a, SM03a].

Cryptographically-masked [AHS08].

Cryptography [RSA09a].

Cryptography [ANS05, AF04b, ADI09, AA04b, An00c, An01i, An02b, An02f, An04a, An05a, An07b, An07a, AAFG01, AIK04, AIK06, App07, AEQ05, ABMO0, BAI01a, BAI01b, BINP03, BD204, BOV03, BOV07, BBG08, BM01a, BR00a, BY03, Ber00, Ber03, Big08, BWBL02, Bha02b, BDS03, Bon00, Bon07, BPR01, Boy03, BLMS00, BK06b, BKM07, Buc00b, BD08, BP01b, BRT090, CPS07, Cer04b, CCL09, CSW+08, CQS01, CDP06, Cob04, CFA+06, Cop00, Cor06, Dr.00c, Dam07, DFS05, DFSS05, DDD, DFGH04, DK02, DK07, Des02, DT03, DYO9b, DSS01, DDN00, DDN03, Dre00, DP08, EPP+07, EP05, Ell09, Ell04, ECG+07, Ett02, FS03b, Gal01, Gal02, GHK+06, GKK+09, Gen06, GS02b, GH02, Gol01b, Gol01a, Gol04, GC01b, Gra01, GPS06, GN06, Gri01, Gro05, HR06, HH04, HM01].

Cryptography
[HMV04, HSS01, HPS08, Hon01, IEE00b, IKY05, Irw03, IKOS06, IKOS08, JYZ04, JL00, JT01b, JT01a, Jue04, Kako06, KLR09, KZ07, KGS07, Kat05b, KK06, KBF09, KPMF02, KWD06, KY01c, Kir01a, KMS02, KSZ02, KS03, KWP06, Lam01, LGS01, LSY01, Lee03b, LLL+01, Lie05, LSD04, LW05b, LP02b, Lut03, Lys08, MNT+00, MP02, Mao01, Mao04, Muz01, MAA07, MBR09, MS03b, Mol01, Mol03b, Mol04, Nie02a, Nie02d, NH02, PV06a, PY06, Pe06, PM02, PBB02, Poi02, PT06, Puc03, RSA00a, RSA02, RSA03b, RS04, Rot07, RS03, RS08, Rug04, Sat06, SP05, Sch06b, Sha01b, She01, SXY01, Sma03a, Sta02a, SGK08, Sti05, Sti01, Sti02, ST05, Syv02, TSO00, TW06a, TG04, TW02, TW06b, Tro08, TR09a, TR09b, Uni01, USS02, VY01, VMC02].

Cryptography
[WPS01, Wei04, WK01, Wel05, Wz00, WvD02, Wi00, YWC08, Ytr06, YC01, YDYM06, ZHY03, vD04, Imr03, AMW07, AUW01, An02a, An02g, ABD01, Ber09b, BBD09, Biso3a, BSS04, BSS05, Bla03, BDN00, BCD06, BEZ00, BEZ01, BG04, BEM+07, Buc00a, Buc01, Buc04, BLRS09, BMA00a, BMA00b, BMA00c, CTT08, CDFM05, CDD07, Cos00, Cre00, DDD04, Dif01, DIM08, DwWmW05, DOPS04, DKL09, DW09, Dw03, Eke02, FXAM04, FP09, Fra01, FP00, GV09, GL05, GGK+07, Geb04, GRTZ02, Gol00, GG05b, GHT05, GPS05, GNP05, HH05, HHL+00, HK05, HAA0, Hig08, HKS00, Hol05, HG05b, HLwWZ09, IZ00, IM06, JK01b, Jan08b, Joy00, KZ03, KL08, Kat01, KI05, Kim01, K00b, Kra07, Lan00c, Lee04a, Lop06, Mau04, May01, Me08, MBS04, MM07a, Mol07, NP02a].

Cryptography
[Nis03a, NH03, Opp05, OS09, PP09, PY05, PC09, PC00, Pi06, Reg05, Reg09, Rot02b,
Rot03, Roy00b, Rup09, STY07, SBZ04, Ser06, SH05, Shp09, Si05, Sin99, Sin00, Sma04, ST01d, SK01b, TW05, UHA+09, Van05a, VM03, WW08, Was08b, Way02b, Way09, Wen03, Whi09, Wro03, YC09a, YY04, YC07, vT05, For04, HC02, Kat05b, Pat03b, Sil01, Sma05, Bee05, Lee03a, Ree01, Wal00, Was08a, MP01b, Shp04a, Kat05b, Spr03, Ter08.
cryptography-based [FXAM04].
Cryptologic [BS00a].
Cryptological [Lew00].
Cryptologie [dL00].
Cryptologists [WD01b].
Cryptology [Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Lai03, LL04c, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka04, Poi06, Rot05, RS02, Sha03b, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bih03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam01, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, PC05a, Pfi01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sbo05a, Sou00, Won01, WK06, Yun02a, vT00, DWML05].
CryptoManiac [WWA01].
Crypton [CKK +02, MG01].
Cryptop [CKK +02, MG01].
Cryptologist [WD01b].
Cryptology [Bar02, Bon03, CGM07, CC04a, Fal07, FLY06, Fra04, JM03, Knu02, Lai03, LL04c, Lut02, MMV06, Neu04, NS01c, Ngu01, Oka04, Poi06, Rot05, RS02, Sha03b, Zhe02b, dL00, Bau00, Bau02a, Bau07, Bel00, Bih03, Boo05, Boy01, CV04, Cra05a, DV05, Fau09, Gar01, Joy03b, Kil01a, Kim02, Lam01, LL03, Lee04b, MS02c, Men05, Men07, Nac01, Oka00, PC05a, Pfi01, Pre00, Pre02c, RD01, Roy00a, Roy05, Sbo05a, Sou00, Won01, WK06, Yun02a, vT00, DWML05].
Cryptosystems [Aki09, Av03, BDG +01, BKLS02, BP000, BM00, CHSS02, CCW02, DG +06, DKXY02, ESG +05, FJ03, Fel06, FP01, HJW01, IZ00, Jou02, JQYY01, KY02a, Kim01, KLY02, KLY02, Kil01b, KM04b, Kos01b, LZ04, LP01, MA02, NP02a, NSS02, OTU00, OS01, PWGP03, ST01a, SKQ01, SKG09, Ste01, Vadi03, Wya02, XB01, ZLK02, Ban05, BF06a, BB79, CHC01, CMKT00, EBS01, EHKH04, GH08, GKBKP01, HM00, Has00, Has01b, Huh00, HP01, KW00, Kos01c, LD01, Luk01, Mic01, Mis06, OS00, Pei09, PLJ05b, SSS06, Sha05c, Sma01, TO01, TC05, Tsa05, Ver01, Why05, Wol04, WPP05, WV00, YY00, ZSS01, vT01].
cryptovirology [YY04].
CRYPTREC [IY00].
CSCW [ZP05].
CT [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09].
CT-RSA [Joy03b, Men05, Nac01, Oka04, Poi06, Pre02c, ZC09].
CTO [An003c].
CTS [Con00].
Cuban [AJ08].
Cube [DS08, PDMS09].
Cube-Type [PDMS09].
culture [Gil07].
Cumulative [WP03].
cure [RD09].
cure-all [RD09].
Current [DFH01, PRS04, LPW06].
curriculum [FOP06].
Curve [ANS05, ADI09, An05a, Ava03, BINP03, Bar00a, BBGM08, BM00, BWBL02, BS01d, BM01, CSQ01, CFA +06, GP08, HYZ05a, HHM01, HMV04, HM02c, JT01b, JT01a, KMB09, KPMF02, KSZ02, KW06, LW02, Mö02, Kir03, OTIT01, OS01, PWGP03, Pel06, RSA03b, RS04, RS01, Sat06, Was08a, WPS01, XB01, YY01, ZLK02, BS04, BSS05, BGM04, BG07a, CCH04, Che05a, CFV06, DIM08, DwWmW05, EHKH04, GKBKP01, Has01b, Huh05a, HL05d, JW06, LL04b, Mis06, OS01, SSS06, SH05, Sma01, SCL05, SL05, TC05, Ver01, Wol04, WPP05, YC09a, ZSS01, ZLK05, vT01].
Curve-Based [KW06, Pel06].
Curves [AHRH08, Bai01a, BB00b, CB02, Gal01, GLV01, Gau02, GHK +06, Kid02, PWGP03, Ver02, CMKT00, Hiro04, LWH05, MP01b, MS04, Sito0, SC02b, Was08b, Wen03, Yas08].
customer [Lin01a].
CVS [DFG01].
Cyber [FNRC05, WW04, Mau05].
Cyberinsurance [BP07].
Cybersecurity [PLW07].
cyberspace [Mit02].
cycles [ABHS09, BP08].
Cyclic [PG05, Mic02a].
Czech [MJ04].
D [Duv03, Ben00, ChLYL09, CT09, DNP07, Lav09, OMT02, WH09, ZTP05]. D.R [Irw03]. daemons [Mos06]. Damgård [CDMP05]. dark [Blu09], darkening [CDD07], DARPA [Coc01a]. Data [ACM03a, ACM04a, ABM08, Ano02a, AAC+01, BGHP02, B+02, BS00b, BNW03, Bro05b, Che01a, CTLL01, DBS01, EBC+00, Elb09, FMA02, FLA'+03, GA05, GMM08, GTTC03, HLL+02, Ken02a, Ken02b, Kius02, Lan00b, LLRW07, LHS05, LS08, Lut03, MND'+04, MS03b, MFS+09, NM09, OS05, Per05, RKZD02, RK06, Sal03a, Sal07, Sin01a, SDMN06, TZD025, TPPM07, VDK05, WS05, WY02, WN02, kc01, vW01, AG09, AH03b, AKSX04, Ano02c, Arn01, Bla00, BN08, CCMT09, Cer04a, CLR09, CPG'+04, DL01, DGM03, FS04, HILM02, LLK05, MJ03, Men03, MI09, PY05, Pin02, Pin03, Sal05c, Sch00a, Sch01c, S'+03, Sch04a, Sch04b, Sch05a, SGPH08, SET08, WMDR08, YLC'+09, YC08, ZSJN07, Zir07, Curr05, DK08, Lin02, Pap05]. Data-Hiding [VDKP05]. data/image [Sch00a, Sch01c, S'+03, Sch04a, Sch04b, Sch05a]. Database [ACM03c, ACM05b, Bf05a, BBPV00, KS02, SVEG09, Gal02, HILM02, Mau04, PS08b, PBVB01]. database-service-provider [HILM02]. Databases [AK02b, CDM'+05, DN04, AHK03a, CDD'+05, CKY07, GA03, MSP09, MNT06, NS05b, ÜG08, YPPK09]. Datamining [DN04]. Datenverschlüsselung [Lin02]. David [Gas01, Pap05, Bar05, Eaga05]. Day [SE01, CSW05, Win05c]. Days [Adl03, Riv03, Sm04]. DC [USE01c]. DCT [BSC01a, BSC01b, CH01b, KT00, LY07, LSC03]. DCT-Based [LY07, LSC03]. DDH [Lys02]. DDO [LK'+08]. DDO-64 [LKH'+08]. Dead [Gut02a]. deaf [Pau02b]. Dealer [DK01, Sun00a]. Dealing [BH00a]. Debate [Jol01, Mad00]. Debian [YRS+09, Akm08]. Deblur [VHP01]. Debugger [Ano02d]. Debugging [Ano02d]. Dec [IEE09a]. decades [Lov01]. decades-old [Lov01]. December [ACM05a, Boy01, CV04, DWML05, FLY06, Hon01, JM03, Kim02, Lai03, Lee04b, LLT'+04, Li05, MMV06, MS02c, Oka00, PC05a, Pat03b, RD01, Roy00a, Roy05, Sma05, Son00, USE00c, Uni01, Won01, WK06, Zhe02b]. Decentralized [MSP+08]. Decryption [CS07a, Mah04, MS02d]. Decidability [Kius02]. Deciding [YPPK09]. Decimation [DCT]. Decipherable [aSM01, Sav04]. Deciphering [Eri02, KB07, Ark05, Lov01, NS01a]. Decision [DJ06, GR04, KM04a]. Decisional [CU01]. Decisions [Coc02a, Sch07]. Decodable [Yek07]. Decoding [KY02b, LBZ01, LBZ02, Ral00, AGKS07, Bul09]. Decomposing [FP09]. Decomposition [BR09, CL04c, SC02c]. Dedications [IS04]. Deep [CMS08]. Defeating [CSK+08]. Defective [BTTF02, Dav01b, Dav01c]. Decoding [NRR00, Pro01]. Defense [GK02, HW01, Mir05, Wy05, Bol02]. defenses [SL06]. defined [Yas08]. Definition [YWD08, SN00]. Definitions [Uni01, AH05]. Definitive [BS01a, BSB05, Gar03b]. defying [HRS08]. Degenerate [Ber09a]. Degradation [BSC01a]. Degree [CV02, QP05]. Degrees [Sat06]. Déjà [DP00]. DeKaRT [Go03]. Dekker [Irw03]. Delacorte [Irm03]. Delay [WRW02, NS01a]. Delayed [JM07]. delegated [CL04c]. Delegation
Delhi [JM03, RM04].
Delivers [Ano02c]. Delivery
[NZCG05, RMCG01, DY09a, NZS05].
Delphi [TEM+01, Hei01]. Demand
[BD03, CMB+05, SEF+06]. Democracies
[CZB+01]. Democracy [CTBA+01].
Demography [Coc03].

Demonstrably [HL06]. demystifying
[RR04]. Deniability [Pas03]. Deniable
[Nao02, CCK04a, CSK+08, DG05, LC05b, 
YRY05c, Za10]. Denial [Mah04, Nik02a, 
Nik02b, PKB01, Ril02, Mir05].

Denial-of-Service [Nik02a, PKBD01].
Denmark [Cra05a, TBJ02].
Denver [ACM01b, Sch04b, USE00d].

Dependable [NABG03, And08].
Dependent [Gol03, WS05, BPS08].

deployed [BDET00]. Deploying
[BH00b, GSB+04]. Deployment
[CL07, KD001, Mur01, Sin01a, App05, 
JRR09]. Dept [Uni01].

Deployment [CL07, KDO01, Mur01, Sin01a, 
App05, JRR09]. Dept [Uni01].

Derandomization [BOV03, BOV07].
Derivation [DGH+04]. Deriving
[BJP02, CSW05]. DES-encrypted [Bih02].

DES-like [Egh00, EBS01]. Desch [LBA00].
Descing [PS06]. Description
[Lav06, MH05]. Descriptors
[DN07, SP04]. Design [Abd01, AADK05, 
Ano02a, ADD09, AIK+01, ARC+01, Bar00b, 
Can01b, CDP01, Cim02, CB01, CS03b, 
CBM+05, CL020, DR02a, DR02b, DF07, 
EHK+03, FF01a, FZ05, GS08, Geb04, 
Gut02b, Gut04a, HRL99, Hro05, Ken02b, 
KB09, KDO01, Lan04a, LCP04, LL04b, 
LB05, MKP09, MP00, Nd05, NSS02, Rhi03, 
SJT09, SP02, SRQ03, Uzo04, WZ05, 
WW08, WLL09, ARJ08, CMS08, GG05b, 
Gut04c, HCO04a, Hut01, KSF00, MI09, 
MM01, SVM09, YCW+08, YCO8].

Design/CPN [AADK05]. designated
[LV07]. Designing
[HBC+08, TCR03, C+02, CG05, Lan00c].

Designs
[Be05, CC02a, Bai08, Des00a, WL07a].

Desktop [Mun08, BDET00]. Desmedt
[CHH+09]. Desynchronization [CDTT05].
Detached [Sha01c]. Detailed [Lut03].
Details [Scr01]. Detect [FOBH05].

Detecting
[CMS09, FGD01, JQYY01, Har07a, LHL04].
Detection
[AS01b, AD07, BB00a, BKM07, CH01b, 
CZK05, JX01, KKG01, SY01a, 
SLT01, ST01c, TZZ05, TM05, WG05, 
Y101, Zan01, Bej06, BBK+03a, HLL+02, 
Men03, NNO2, WMS08, YYW06, ZGTG05].

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

Determining
[KS03, LQ08, OS07]. Deterministic
[BP06a, Her06, KZ03, KZ07, May04, BK07].

dev [BH05]. Developers
[An06c, Dew08, MK05b, Nis03a].

Developing
[BP06a, Her06, KZ03, KZ07, May04, BK07].

Development
[An03e, Pre07, Sha04a].

Develops [Pau02b]. Deviates
[Ran55, Ran01]. Device

[RIC07, ST03b, WPS01]. Devices
[BCH00, DAM07, EP02, GST04, Hei07, 
JP02a, JW05, Kha05, KHD01, MV01, 
MRL+02, SC01, WCO01, Ano06a, CMS08, 
DMT07, Tse07, ZYW07]. Devill [Bla01c].

DFT [Che08a]. DH [Lys02]. DHIES
[ABR01]. DHP [MSV04]. Diablerets
[Vau05a]. Diagnosis
[An04a, BK06b, XNK+05]. Diagnostics
[NM09]. Diagonal [PJJ01, PJK01].

dickson [SZP02]. Dictionaries [AGT01].
Dictionary [BP00, BCP02b, CS07b, DJ06, 
Pho01, NS05a]. did [MH09]. Diego
[ACM03a, ACM03b, ACM03c, ACM07, 
Sch00a, Sch01c, Sch04a, Sch05a, USE00b].

Dies [Bar00a, Coc01a]. difference
[PBMB01, dW02]. Differenting
[LS08, WWTH08]. Different
[CGMM02, Sma01]. Differential [Ava03,
BMM00, BF00a, BFM02, BDK02a, Cry00, CV02, CKK+02, CKL+03, Eke09, Furt02a, Gra02a, HLL+01, HSM+02, HHK+04, IIT03, JTO1a, Kan01, KM02, KCP01, LHL+02, MP06, MMT09, MHL+02, MG08, PSC+02, PQ03b, SK01a, SKU+00, SK01, YSD02, vW01, BF01a, CUS08, Che08a, DLP+09, Egh00, EBS01, Pha04, SLL+00, TM01].

Differential-Linear [BDK02a].

differential [BF00b].

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

dier [Jan08a, ABR01, ASW+01, BS01d, BMP00, BCP01, BCP02a, BCP02b, BCP07, CY08, CU01, CJ03a, CKRT08, FS01b, GR04, Kil01b, KK02, KM04a, Kra03, Kra05, Mis08, Tsa06, YRY05c].

diuser [Fer06].

diusing [She01].

digest [MSP09].

digit [KWP06, Tan07a, BG09, HKPR05, Kiu01b].

digital [ANS05, AvdH00, AR00, AS08, Ano01f, Ano02d, ABRW01, Bar00a, Bar06b, BL08, BDS09b, Cal00b, CCH05, CC09, Che01b, CFS01, CM02, CM08, CBZ+01, CGJ+02, DSP01, EIG01, Eng00, EHK+03, HSZI00, HSZI01, HSGP+03, HW01, HT01, JBR05, KAL01, KCU02, Kuh00, Kwo02, Kwo03b, LZZ+01, LLL+01, Lin01a, LL01, Lut03, Mad00, MM01a, MM02, Mee01, PL01, PJH01, PCG01, FJZ09, PBM+07, Ram01, Rd01, RS01, Sam09, Scho0d, Sch06b, Scr01, Sha01e, Sc02a, Sh08, SLT01, Sug01, TJ03, US02, VSP01, VK07, WNY09, Win05a, WBD01, Wu01, WV01, WC03, WC04, Wny02, XZ01, YX09, YWWS09, YY001, YYZ01, ZWC02, Zho02, AAP07, AA08, Ano00i, Ate04, BLH06, Bra01a, Cal00a, CS08a, CWH00, CL00, CJ05, Che07, Die00, FB01, GKG03, Gil07, HRL09, HHL00, HK00, Lev01].

digital [LCL06b, MKY08, NR00, PC05b, PLJ05a, PBV08, QC05b, Sha01d, Sha04b, Sha05d, SCL05, TCC02, TND+05, U05, WNQ08, WHLH03, X05, XMST07, Ano09, Ano13, BCKK05, CDS07, CKL05, FIP00, Fox00, Gen00a, KCR04, Nat00, PK03, SA02].

Digital-Audio [WNY09].

Digital-Signature [Eng00].

Digits [Che04b, Ran55, Ran01].

Dimension [DDG+06, TZ09a, TZ09b].

Dimensionality [SBG02].

Dimensions [CLR09].

Dining [KLN+06].

diplomacy [Alv00].

Direct [BMW05, KG09].

directional [PK01].

Directions [Sha01b, DFH01].

directly [JZCW05].

Director [Mad04].

directories [C+02].

dirk [Pet03].

directory [C+02], disabled [Pau02a].

Disadvantage [Pau02a].

disadvantage [CD07].

Disappear [Per05].

Disappearing [Way02b, Way09], disappointed [St00].

Disaster [WCH05].

discursive [SM08].

disclosure [JMW07, SW05].

Discovery [Bi09, HLL+02, SGB07, SGA07].

Discr [CS03a, CSG02, Che04b, CWW02, Gen00b, GV05, GPP08, KC09b, LW02, LL05, VN04, HW03a, HW09, Hsu05a, HL05d, JL03, JLL01, LHL03a, LH05, LTH05, PL05a, QC05b, Sha01e, Sha05c, Sha05d, SWT05, SLC05, SLC05, SCS05c, Yas08].

discretized [MA02].

Discription [Har07b].

discursive [Mit02].

Discussion [Ano01a, Ano01b, Ano01c, Ano01d, Ano01e, Ano01f, Ano01g, Ano01h, Ano01i, KLB+02a, Mal02, Nik02b].

Dishonest [GGK007].

dijoint [Gut04c].

Disk [CRO01, Har07b, SIV06, CS08a, Fer06].

disman [Hil06].

dispatches [Ke05].

displayed [CGV09].

Displays [Kuh02a].

Disputed [CAC06].

Distance [CGFSG09, CPHX04, DM07b, DW01].

distinguished [HWW04, WH02].

Distinguishing [HSR+01].

Distortion [BG08, CS05c].

Distortion-Free [BG08].

Distortions [HH09, SDF01].

Distorted [BCS02, BT02, CLK01a, CS08b, CD01a, DS03, EP05, FM02a, FS01a, GJKR03, GSV02, GTH02, LLY06, SCF01, WT02, And08, AFG06, BDE06, CO09, FMY02, KKL09, LNO4, LLW08a, MSP+08, PS08a, Raj06, WZB05, YBJ04].

Distribution [BDF+01a, BOHL+05, BBT+02, BSN00,
FS01b, Ina02a, Ina02b, Ku02, LLL02, NA07, Sch01a, Yi01, ATS04, Bad07, CYH04, GL06b, MP08, SLP07, Shp01, Shp04b, WHHT08, YS04, ZLG01. Distributions [CY08]. Diversity [Kun01]. Divide [SKQ01]. Division [HZSL05, KK02, Tan07a, Che08b, MN14]. Divisor [KM01a]. DL [HRL09, PLJ05b, Sch01f, Sch01e, WMDR08]. DL-based [HRL09, PLJ05b]. DL-encryption [Sch01f]. DL-keys [Sch01e]. DL-STDM [WMDR08]. DLP [MSV04]. DM [Eag05]. DNA [GPX08]. DNF [BGN05]. DNS [Kle07]. Do [Bur06, HSR01, HR04b, Win01, BB79]. Dobb's [Dr.00c]. Document [ISO05, PJH01, ST01c, VHP01, CDS07, CL04c]. Documents [PJK01, AW05, AW08, DGK04, GA03, UG08]. Does [AB01, Pie05, Con09]. Dolev [BP08, BDNN02, ZD05]. Domain [AS08, Bar00c, BSC01a, BSC01b, BSL02, CJK04, Cor00b, Cor02, DOP05, DNP07, GW01, ISSZ08, Kuh02a, Lan00d, LZ01, MM01a, OMT02, PBC05, SOHS01, SDFH00, ZLK02, BR06, CS05a, DSP01, EKRMA01, Zir07]. Domains [BR01, CLK01a, CLK01b, Vau01]. Domingo [CKN06]. Dominic [Rot07]. Dominica [PY05]. domino [LLLZ06a, LLLZ06b]. don't [Win05c]. Don’ts [FSSF01]. DONUT [CLL00]. Door [SF07]. Doors [Eri02]. DOS-Resistant [Ano00e, ANL01]. Double [ADDS06, CY08, CMJ03, Coc02a, DIM08, GH08, GB09, Hau06, JSW05]. double-base [DIM08]. Double-Gate [Coc02a]. Double-Size [CMJ03]. double-trapdoor [JSW05]. Doubling [FV03]. Douglas [Spr03]. Down [BBPV00, Coc02b, Ano00g, Ano03c, Ano03a, Pot03, PBVB01, Ste05c]. Downwards [FV03]. DPA [GBK01, TV03]. DPA-Based [GBK01]. Dr [Ano03e]. Dr. [Dr.00c]. draft [Ste00, Dwo03]. drastic [Sug03]. drawn [vOT08]. DRBG [Hir09]. Dress [Ahm08]. drinks [Ano03c]. Drive [NP07, Kor09]. DSA [MR01a, SA02, Sha01d, TvdKB01]. DSA-type [Sha01d]. DSEA [LLLZ06a, LLLZ06b]. DSP [GB04, WWGP00]. DSP-embedded [GB04]. DSPs [WWGP00]. DSS [Ano09, Ano13, FIP00, Nat00]. DTD [PCK02]. Dual [KHY04, LKK05, SF07, WCJ09, ST03a]. dual-field [ST03a]. Dual-Pair [WCJ09]. Dual-Tree [LKK05]. Dumb [Eri01]. Dummies [Cob04]. Dump [KCJ01]. Dunaynir [MaaT05]. d'une [Car06]. Durahim [MaaTxx]. Durayhim’s [MaaT04], during [AJ08, Bec02, WA07]. Dust [KGS07]. Dutch [dl00]. Duty [ZGLX05]. Dwork [DRN03, GK05, Zha06]. DWT [LHS05, PBC05]. DWT-Based [LHS05]. Dynamic [AFB05, BNP08, BCP01, BCP02a, BM07, CL02a, CW09, CCD04, CTT07, GTH02, HQ05, Pat01, Sug03, TT01, BBG02, GL06b, LCP04, LLY06, LCK04, LCC05, RG05, Yi04]. dynamic-key [LCP04]. dynamics [BGP02, MR00].

E-business [Poh01, HHSS01]. E-Commerce [Kir01a, BM03a, Gra01, SN07, Sta00, MY01]. E-Goods [NZCG05]. e-Government [RM02]. E-Learning [CAC06]. e-mail [LL04b, NZS05, All06, ANR01, KSO00, Law05]. e-payment [Has02]. E-Security [NDJB01]. E-smart [AJ01b]. e-voting [CJT03, Cha04]. E-Wallet [ETZ00]. E0 [LV04]. E2 [SKU00]. Early [ASW01, Nik02a, Nik02b, Pag03, Riv03, Bur02, Sma04, ZGTG05]. Easier [Pau09]. Easy [GR04, Hos06b]. Eavesdropping [Kuh02a, Kee05]. eBook [Ano02d, WWL02]. EC [SF07]. ECC [BWBL02, CL09, Mis08, Ts05]. ECC-based [CL09, Ts05]. ECC2K
Embrace [CNB+02]. Embracing [Ano03c]. EMD [BR06]. Emperor [Smi01b]. Empirical [HW03b, Goo00]. Emptiness [DIS02]. Emulex [CZB+01, CTBA+01]. Enabled [For06, CCCY01, DY09a]. Enabling [Web02]. encapsulation [CHH+09, KG09]. Encipher [BR00a]. Enciphering [HR03, KT01]. Encode [BR06, BKN04, Ano08c]. Encode-Then-Encipher [BR00a]. Encode-then-Encrypt-and-MAC [BKN04]. encoded [WMS08]. Encoding [JT01b, RS00, Lin02]. encounter [Win05c]. Encrypt [BKN04, BTTF02, Dav01c, Pet05, Dav01b]. Encrypted [BBK03a, BGH02, BGLS03, CD01b, Hug04, Lan04a, LH07, RMCC01, Sta02b, Vau01, WRW02, Whi09, Woo00, Ano06a, Bih02, BNP08, CMT09, CDD+05, CSK+08, FJ04, HILM02, Hes04a, LSH00, MW04, Pet03, ÜG08]. Encrypting [Pro00, RC01, Zho06]. Encryption [ABC+05, Abe01, AS01a, Abe04, AP09, AB01, ADR02, Ano03, Ano01f, Ano01g, Ano01h, Ase02, ANR01, AF06, AF03, Bar00c, III00, Baut02b, BNO0a, BR00a, BMM0, BBDP01, BU02, BF01b, BF03, BB04, BGW05, BCHK07, BGH07, BPR+08, BB03, BNW03, BD03, BKY02, Bur03, CD00a, CS03a, CHK03, CHK05, CGHG01, Che01a, CTLL01, Chi08b, Cho08a, CMRO6, Cla00a, Coc02b, Coc01b, CJNP00, CHJ+01b, CD01n, CS02, CS03b, Cro01, Cur05, DS03, DR01, DR02b, DR02c, DN00a, DN03, Dan01, DJ06, Des00a, Des00b, Des00c, DL98, DR02d, DA03, DKF+03, DK05, DS05b, Drifi02, FIP01a, FLO1a, GCO1a, GSW00, Gen03, GRW06, GH05, GD02, GMN01, Gutxx, HSH+08a, HS02a, HYZ05a, HSH02, HSH06, HKR01, HWW05, Har07b, Har00, Hei07, Her09, HS00, HR05, HG03, HL02, HGNP+03, HLL05]. Encryption [HLC08, ISSZ08, Joh03, Jol01, JK02b, JJ02b, JMV02, JKR01, Jut01, KBD03, KSHY01, KS00a, KY01a, Kha05, KKK+07, Kos01a, Kra01, Kur01, KD04, Lai07, Lan00a, Lan00b, LP03, LHT09, LY07, LLRW07, Lin03, LNP02, LM05, LCD07, Man01, Mar07, Mar08a, Mar08b, MF01, MM01c, MP01a, MP00, MP05, Mö03a, Mor05, Mü01a, MS09d, NIS00, Nam02, NZCG05, NZS05, NP02b, Nie02b, PV06b, PM00, Pan09, Pen01a, PZL09, PDM09, Pha04, P00, Pre01, RM04, RK06, RDJ+01, Sam01, Sch00b, SJ00, Siv06, SB00, CAC06, SRQL03, SPGQ06, SBZ02, Sye00, TV03, Uni00a, Uni00c, Uni00d, Uni00g, Uni00h, Ust01b, VMS05, WZW05, WBRF00, Wri01, YEF+06, YW06, ASW00, Abd01, ABHS09, AKSX04, AMRP00, ABW09, Ano00e, Ano00c, Ano00f, Ano00g, Ano00h, Ano00j, Ano02a, Ano03c]. encryption [Ano06d, App05, Ato04, AcM05, AFGH06, BPS08, BKN04, BR04, BR0+09, Ber09a, BK+03b, Bir07, Bna0, BJ00, Bro05b, CG06, CS08a, CBSU06, CHC01, CKRT08, D2ZL01, DL07, DRS05, DW01, Fer06, FB01, Fox00, FMS05, GM08, GGG03, Gen09a, Gen09b, GKM+00, Gou09, Gua05, Gut04c, HSH+08b, HSH+09, HS02b, HYHW07, HCD08a, HCD08b, HAU04, HWW02, Hsuo05, Hwa05, HLO5c, HLO5d, IM06, JK01a, JK01b, JXW05, JSW05, JZCW05, KY00, Kj01, KSW06, KHL09, Kor09, KW00, Kre05, Kü08, La00, LV07, Lee01, LCP04, LJO5a, LMC+03, LLZ06a, LLZ06b, LLCL08, LB05, Lu02, Lud05, LK01, LWK05a, Mad04, Mar05b, Mat02, Mü01b, Mun08, NK06, OS07, PBMB01, PS01a, Pau02a, Pau03, RG09, Rh03, RBB03, RSP05, SN00, SKW+07, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, Sch01d].
YC07, ZLG01, ZL04a, ZAX05, ZW05b, ZL05, ZFK04, ZD05, CHKO08, CHJ+01a, RR04, Unio0f, Wue09, Jan08a.

encryption/cipher [HAuR04], encryption/decryption [OS07].

Encrypted [LMP+01, TPS01, Ano00a]. Encryptor [TPS01].

Encyclopedia [Bid03, vT05]. End [KCD07, Per03, SKKS00, WWGP00, YSR01, SU07].

End to End [YSR01]. End [Kus02].

Endomorphisms [GLV01]. Endpoint [Kad07].

Enemies [DM07b]. Energy [GC01b, Ino05, LPV+09, SLP07, Mis08].

Energy-efficient [LPV+09]. Energy-security [Ino05].

Enforcement [GN06]. Enforces [BP05].

Enforcing [GMM08, HRS08]. Enrich [Fri01, MMH02, DP04, SHL07].

Engineer [Pau02b, SN04]. Engineering [CNB+02, TPS01].

Engineers [Pri00]. engines [PM08]. Enhance [ZWC02]. Enhanced [JKRW01, ZGLX05, OP01b, TWL05, WHH05, ZSM05].

enhanced-security [OP01b].

Enhancement [CNB+02, Pat03a, YJ00].

Environments [CJK+04, LKHL09, BGM04, MNS08, SBG05, SBG07, SN04, YC09a, YbJF04]. ephemeral [Mi08]. Ephemerizer [Per05].

EPOC [JQY01], ePOST [MPHD06], EPR [Ina02b]. Equation [FJ03]. Equations [CP02, DDG+06, GS03, PBMB01].

Equipping [DMT07]. Equitability [DBS01]. equivalence

Erratum [AGGM10, Kwo03b, LLLZ06a]. Erroneous [CH01b, MNT+00]. Error

Error-Correcting [NN06, ZYR01]. Error-Prone [MLC01]. Errors [AD07, AL07, Reg05, Reg09].

escape [Blu09, Fur05]. Escrow [AK02a, Ano01a, CL01a, DBS01, LCK01, ATSVY00, CL02b, LCC05].

Escrowed [PS01b], eServer [AV04]. ESORICS [dCdVSG05]. espionage [Bud06]. essays

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

[CPH04, CMJP03, CLZ02, WL02]. EULA [WWL+02]. EUR [Eag05]. EUROCRYPT [Bih03, CC04a, Cra05a, Knu02, Phi01, Pre00, GJS001]. Eurographics [MFS+09].

Europe [Pag03]. European

[AL06, CZ05, KGL04, Pre01, dCdVSG05, Ano00f, Che08b, Die09, Pre02a].

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

Evaluate [Pre02a]. Evaluating

[BGN05, NTW07]. Evaluation


[BSC01a, EYCP00, FS00, FML+03, IKM00, IY00, JJ00a, Kan01, Kir03, SKSS00, BZP05, FXAM04, FS03a, LCP04, MCHN05, RC05, RN00a, RN00b]. Evaluations [LM02]. Evangelizing [Co01a]. evasion [Blu09]. even [Bih02, OS00, Win05c]. EventGuard [SL05b]. ever [Fur05]. Everlasting [DR02d]. Every [TH01, DKK07, Win05c]. Everything [CTBA+01]. Everywhere [Ber00]. Evidence [Ver01, Bro05a, HW03b]. Evolution [DF01, Ree01, Pat02a, SP02, Sin99, Sin00]. evolutionary [LMSV07]. Evolved [LMHCETR06]. Exact [Cor00b]. examines [Nis03a]. example [Bla00, GC05, Zir07]. Exchange [BH06, BPR00, BMN01, BMP00, BCP01, BCP02a, BCP02b, CK02a, CK02b, DG03, DLY08, GL03, JL08, KOY01, KY03, MSP00, Mac01, MSJ02, Ng05, VPG01, WC01a, WV01, ZWCY02, BBG+02, BCP07, CL08, CWJ01, GL06a, GM05, HT08, KS05a, KOY09, LW04, LHC08, LSH00, MS03a, Mis08, 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, BCHK05]. Experiences [MPH06, USE00b]. Experimental [BG09, CGBS01, ÖOP03, WS02, RSQ03, Sm04a]. Experimentation [Hun05]. Experimenting [LSV09]. experiments [Bru06]. expert [Ano01b]. Expiration [MP00, Sch05b]. Explicit [CY08, GRW06, WPP05]. Exploit [BR00a, FOBH05]. exploitation [Eri03, Eri08, KVN+09]. Exploiting [CK06, ETMP05, HR00, HM04, ZWC02].

Exploits [MJF07, CSW05]. exploration [SKW+07]. Exploratory [Lut03]. Exponent [BP04, BM01b, DN00b, May02, ZS01, CKY05, Duj08, GD05, Shp04b]. Exponential [BYJK04, BYJK08, CY08, GKK+07, GKK+09, Shp05].

Exponentiation [KKH03, SK07, CKRT08, HGNS03]. Exponents [FS02, FS01b]. export [An00h]. Exposed [Gum04, MSK03, SS06]. exposing [YY04]. Expositive [MAaT05]. Exposure [BM03b, DSS01, KZ07, CDD+05, KZ03]. Exposure-Resilient [DSS01, KZ07, KZ03]. expressions [MW04]. Extended [ABDS01, BPS00, CM00, Con04, DIRR05, HLvA02, HJW01, JL00, MS02, MP02, OST05, Wag02, BJN00, CD00a, HT04, HP01, Mis06, Pei09, QPV05, LKJ01]. Extending [ADD06, IKNP03, Ove06, Sal03b, SS01a].

Extension [Bai01a, YWD08, BR06, CMD06]. Extensions [ABC+05, BBGM08, CS07c, HM02a, Rot02a, Wei04]. Extracting [Cer04a]. Extraction [DGH+04, RW03a, MB08, PBV08]. Extractors [Fis05, KLR09, KZ07, Lu02, V Adam03, DWO9, KZ03, Sha04a].

Extraordinary [Top02]. Extreme [An02d]. Extrusion [Bo06]. Eye [Sas07, CAC03]. Eye-Opening [CAC03].

F5 [Wes01]. Face [KZ09, NH02, PK01, SBG02, TZN09b, PY08].

Faces [NS01c, Ng01]. facets [Rot02b, Rot03]. fact [An03c]. Factor [DN02b, Sas07, BSS07, Hen06b, Sch05c, St00, Ste05a, dB07]. Factoring [BN02, KY02a, KLM+02a, KOMM01, May04, PV06b, ST03b, LTH05, LCZ05c, MIH01b, PL05a, QCB05a, Sha03d, Sha05d, ZCL05].

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

Facts [GO03]. Fade [CAC03]. Fail
First-order [Coh03, KS06b].

Fish [Fie09, Wei06, Wei00, Wei05].

Fit [CCM05].

Five [SW00a, MS02b, Rot02b, Rot03].

Fixed-lecture [Rot02b, Rot03].

Fixed-Length [AR01, BCCN00, LS01a, Shp04b, SP79].

Fixed-Length [AR01, CKN00].

Fixed-Length Pattern [BCCN01, LS01a].

Fixing [KZ07, KZ03].

FL [Des02, Jue04].

Flash [ST06, SGB01].

Flat [SV08a].

Flexibility [LP02a].

Flexible [CMG01, CLK01b, DGK04, OT03a, Tsa01, BA06, KC05, LHY02, WWA01].

Floating [NS05c].

Floating-Point [NS05c].

Flow [BDNN02, ABE05, FR08, ME08a, TWM09].

Foam [SGB01].

Foraging [WF01].

Forensic [PS08b, Cas02, Kor09].

forensically [ME08b].

Forensics [JBR05, CS04, CS08a, CDS07, MS09a, MKY08, MAC03].

Forest [FBW01].

Forgery [CH01a, CMM00, LS01a, SLT01, HSW09].

Forgotten [Eng05, Kin01, OC03].

Form [AD109, CH07c, OS01, LKYL00, Mic01].

Format [BGB09, B07b, BCH05, BCJ06, CL05, DKS08, GOR02b, HG03, Lan00d, Mea01, YWD08, ABHS09, JW01, Mea04, Pau01, SW02, ZLX99, ZL04b].

Formalizing [HM01a].

Formally [BJP02].

format [ISO05, RG05].

formats [RG05].

data types [ISO05, RG05].
FranzSteiner [Eag05]. fraud [Ano03a]. Fred [Bar00b]. Free [AP09, Ano02e, Bau01a, Bau01b, BGI08, Coc01a, CNV06, DG02, HS00, HM01b, JP03, Jut01, Fox00, Ks06b, SBG05, Bol02]. FreeBSD [Coc01a, Mu02, Siv06]. Freedom [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, Mil03]. FreeBSD [Coc01a, Mur02, Siv06]. Freedom [Uni00a, Uni00e, Uni00d, Uni00g, Uni00h, Mil03]. Freenix [USE01b, USE02c]. French [Wri03]. Frequencies [DD02]. Frequency [OMT02, Sak01, SOHS01, CS05a]. Frequency-Domain [OMT02]. Frey [Was08a]. Friar [GG05a]. Friendly [CTY09, CRSP09, Hsu05b, HL05b, SZS05, WLT05a]. FrontPage [WWL+02]. FSE [Bir07, DR02e, GH05, Joh03, Mat02, RM04, Sch00b, Sch01d]. FTC [Stef05c]. 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, KPFM02, RG09, Gen09a]. Function [BR08, CDM05, Fis01b, Flu02b, Gis05, HNO+09, HPC02, JI00a, Kan01, Kid01b, Nie02c, RB01, Yam05, CHY05b, CJ04, HR07, LW04, LPM05, WWTH08, YW05, YR05b]. Functional [ECM00a, WA06]. Functionalities [PS05]. functionality [ETMP05]. Functions [AEM09, BBDDK00, Bon01, Can01b, CV02, Car02, Cle01c, DN02a, DGN03, DR03, Fil02, FIPR05, GLG+02, HMD04, HR04b, Jut04, KI01b, LTV05, Lys02, PR01, RR08, SM00a, SM00b, SS01a, Sh00a, Sh00b, Ver02, WP03, WFLY04, Wer02, AGGM06, AGGM10, ALV02, CS09, GVC+08, HR05b, IS004, KK07, LLH02, LKY04, MS02b, MS09c, Mic02a, Mic02b, NR04, PW08, QPV05, SM03a, Wh09, YR04, ZW05a, RRS06]. Fundamentals [And04, PHS03, Shi08, Way01, vT00, Fin03]. Funds [Coc01a]. Further [JS05, LL04a, LL05c, MP07, YRY05a]. Fusion [KZ09, TZDD05, ZS05, BG09]. fusul [MAa05]. Future [ASW+01, Ano02e, Joh00, LNP02, NFQ03, Sch00e, HP00, LPW06]. Fuzzing [SGA07]. fuzzy [HS02b, NC09]. fuzzy-based [NC09].

G [Coc03, For04, Was08a]. Gaitherburg [SMP+09]. Gamal [EKRM01]. Game [DHR00, LM02, CAC06, BR04, Gou09]. game-like [Gou09]. game-playing [BR04]. Gamers [MP00]. Games [KN08]. Ganesh [For04]. Ganzúa [GPG06]. Gap [OP01a, PWGP03, RW03a]. Gap-Problems [OP01a]. Gate [Coc02a, GCO01a]. gates [TWM+09]. Gauging [PvS01]. Gauss [KKH03]. Gaussian [EKRM01, JL03]. Gbps [TPS01]. GCD [JP03]. GCD-Free [JP03]. GCM [KS09]. geeks [McN03]. Geheimsschreiber [Joy00, UW00]. GEM [CHJ+01a, JM02]. General [AB09, CDM00, DN00a, ESG+05, GMP01b, Kog02, Lin05, MND+04, Sal01a, VC01, Y06, JL03, L05a]. General-Purpose [ESG+05]. Generalisation [DJ01]. Generalization [YYZ01, HWW02]. Generalizations [LD04, LS08]. Generalized [KSR02, Mic02a, TC01, T01a, Wag02, WHLH05, LKYL00, Shi05]. Generate [HSR+01]. Wer02. FSGV01]. Generated [ADD09, MRL+02, RBF08]. Generating [BMK00, BCD00, G01, MFK+06, SS03]. Generation [ACS02, BH05, BK06a, CS03c, ESG+05, GJRK03, GL01, GW01, JG01, MR01a, Ram01, TL07, TV03, WP03, WHLH05, Web08, WS02, Ano04e, BK07, BG08, BF01c, ISTE08, LS05b]. Generator [ADD09, BP01a, DI05, Die03, DGP07a, DGP07b, DV08, EHK+03, Gen00b, GM02a, Gol01c, GPR06, Int03, Ke05, LMHCETR06, LV04, SXY01, SFDF06, TWNA08, TZ09a, T09b, ZKL01, Aam03, ACTZ05, Be08, BG08, BG07a, DGP09, GB09, HG05a, HLwWZ09, JAW+00, KH08, KSF00, Pan07, PSS+09, PSP+08, PC00, RGX06, SR07.
held [Buc00a, PPV96, Uni00b]. Hellman
[KM04a, ABK01, ASW+01, BS01d, BMP00,
BGP01, BCP02a, BCP02b, BCP07, CY08,
CU01, CJ03a, CRK08, FS01b, GR04,
Kil01b, KKK03, Kra05, Mis08, Tsa06,
YRY05c]. help [Ano08a]. Helped [Gan01b]. Helps
[DF01, Pri00]. Helsinki [Buc00a].
Hensel [CNS02]. Her
[Bur06, Law05]. Here
[Bur06, Law05]. Hermite [Mic01].
heroes [OC03]. Herriot
[Coc03]. Hersonissos
[ACM01a]. Hessenberg
[SSFC09]. Heterogeneous
[BCS02, KHYM08, ZBLvB05].
Heterogenous [Hof01]. heuristic
[SS03]. HFE
[FJ03, CHH01, Fel06]. HFE-Cryptosystems
[Fei06]. HIBE
[CS07c]. Hidden
[HGN03, KW03, LNS02, GMR05, LK09, Shp05, FJ03, Sch09]. Hide
[CC06, PH03, Shp05]. hide-and-seek
[Shp05]. Hiding
[BD03, CLT07, Col03, DN02, GA05,
HNO+09, LHS05, LS08, MH05, MM00,
VDP05, WC03, HR07, JD01, KP00,
RSP05, Way02b, Way09, YCL07]. Hierarchy
[HC08]. Hierarchical
[GS02b, HNZ02, HL02, MN01, YLH05, BD04b, Che07, JW06,
KAM08, WX01b, hY08]. hierarchies
[AFL05, Cer04a, HY03, WL05]. hierarchy
[CMD06, Hwa00, JA02]. Hierocrypt
[OMS01]. Hieroglyphs
[Wir05]. High
[ACM01b, Ano00d, Ano02d, ClLYL09,
CW09, CJL06, CGJ+02, DS05b, FZH05,
Gro01, HNZ02, HV04, Int00, JKRW01,
KMK+06, Ken02b, KB00, Kra05, KT01,
MM01b, NFQ03, SW07, SKKS00, SOTD00,
SM02, SGM09, SLG+05, TL07, Uni00c,
Wie00, WWP00, YKMY01, Zhe01,
BVP+04, BZP05, BGL+03, Jen09, KC09a,
Uni00f, WWTH08, Zir07]. high-assurance
[Jen09]. High-Bandwidth
[CGJ+02]. High-Dynamic-Range
[CW09]. High-End
[SKKS00, WWP00]. High-Performance
[Kra05, NFQ03, BZP05]. High-Speed
[Ano00d, Ano02d, Gro01, JKRW01,
KMK+06, SOTD00, SM02, Wie00,
YKMY01, RW07, BGL+03].
High-technology-crime
[KB00]. High-Throughput
[HV04]. Higher
[CW02, KCP01, BF01a]. Highly
[CW02]. hijacking
[Ste05c]. Hill
[Gum04, USE02a]. Hilton
[KJR05]. HIPAA
[AEV+07]. historic
[Pet08]. Historical
[RE02, MWM01]. History
[BP03b, Pag03, Sal01a, Sin01b,
CAC06, Top02, AJ08, Boo05, HSW09,
Jan08b, KNS05, Naf05, Nis07, Pin06, Ris06,
RH00, RG06, Wi01a, dLB07].
history-based
[KNS05]. hit
[Bjo05]. HMAC
[FIP02a, DGH+04, Hir09, RR08].
HMKV
[Kra05]. Hoare
[Bel08]. Hoax
[CBZ+01, CTBA+01]. hoc
[BS01, Cha05b, DHMR07, KH05, LHC08,
LKZ+04, PCSM07, SL07, TW07, WT02, ZC09]. Hold
[PM00]. Holier
[MCC01]. Holistic
[RM02]. Homage
[JP02b]. Home
[IEE00b, SEK01, SEK02, CAC03, Pet03].
Homegrown
[Str02]. Homeland
[Man02, Man05, RR03]. homogeneous
[MF07, PS02a]. Homomorphic
[AS01a, Aki09, CDN01, DN03, HS00, Cho06,
Gen09a, Gen09b]. homomorphism
[CKN06]. homophonic
[Sav04]. Honeynets
[Dim07]. Hong
[B+02, ZJ04, Cla00b]. honor
[OC03]. hook
[JEZ04]. hooks
[GGJ05]. hop
[NC09, ZSJN07]. hop-by-hop
[ZSJN07]. Horizon
[Coc02b]. host
[Shu06]. hostile
[ABB+04]. Hosts
[H0801, SZ08]. Hot
[IEE01b]. Hotel
[USE01b, USE01a, USE02a]. HotOS
[IEE01b]. HotOS-VIII
[IEE01b]. hours
[Fox00]. House
[UN00a, Uni00b, Uni00f, Uni00e, Uni00h].
Hsu
[BCW05, HUL05c]. HTML
[CNB+02]. HTTP
[Zha00]. Huang
[ZC05]. Huge
[MSNH07, NNT05]. Hull
[KMT01]. Human
[Dre00, GL01, JW05, KOY01, Man08,
MS02d]. Human-Memorable
[KOY01].
Hundred
[Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].

Hung [GJL06].

Hwang [SCS05b, ZK05, HL05d, KTC03, KCL03, LW05c, QCB05a, WL05, ZYR01].

Hwang-Rao [ZYR01].

HWWM [LKY05c].

HWWM-authenticated [LKY05c].

Hybrid [ADI09, KD04, LZ04, PK01, CJ03b, HG07, LPM05, TM06].

Hyderabad [MS02c].

Hype [Way02a].

Hyper [DR02d, Lu02, PZL09].

Hyper-chaotic [PZL09].

Hyper-Encryption [DR02d, Lu02].

Hyperelliptic [Ava03, CY02, CFA + 06, HSS01, PWGP03, Ver02, Was08a, ZLK02, CMKT00, Wen03, Wol04, WPP05].

hypotheses [KW00].

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].

ICCA [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, GTH08, HCO8, KLY03, KHL09, Kn02, LCS09, Sco04, SW05, SCL05, WBD01, WH02b, YLH05, ZK02, ZC04, ZC09].

Id-Based [ZJ09, BRTM09, CCD07, CL07, CS07c, CL00, GS02b, GTH08, HCO8, KLY03, KHL09, Kn02, LCS09, Sco04, SW05, SCL05, WBD01, WH02b, YLH05, ZK02, ZC04, ZC09].

IDE [Ano02d]. Idea [Cos03, RR03a, CTLL01, HTS02]. Ideal [BTW05, BTW08, CDFM05, Lan00d, Gen09b]. Ideas [Gha07, Eri01].

Identification [BP02, BLDT09, Gar03a, GLC + 04, KK02, Kir01b, Lys07, Sak01, SK06, Zhe01, And04, Dal01, Fin03, PBV08, YCW + 08, ZC09].

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

identities [Kwo02, Kwo03b]. Identity [App05, BF01b, BF03, BB04, BCHK07, BGH07, BPR’08, Boy03, BRTM09, CL01a, CHM + 02, Coc01b, DT03, GK04, Her06, Her07, HY01, HL02, KC02, LCD07, Mar08a, Mar08b, PCSM07, SM + 09, BMW05, CG06, CJ05, GG08, KG09, LWZH05, RG09, Sa02, Sha03c, Wan04b, Win05a, YCW + 08, ZYW07]. Identification-Based [BF01b, BF03, BCHK07, Boy03, BRTM09, DT03, Her06, HL02, KC02, LCD07, Mar08a, Mar08b, App05, Her07, PCSM07, BMW05, CG06, CJ05, KG09, LWZH05, Sa02, Sha03c, YCW + 08, ZYW07].

IDSFAM [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, PH03, ZDW06]. 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, Ano00d, Bau03b]. IKE [CK02a, Kra03]. I’ll [PLW07]. Illinois [ACM04b]. Illusions [Koc02]. illustrated [Lun09]. Im [BGI’01, DOPS04, RR05].

IMA [Pat03b, Sma05, Hon01]. Image [AS01c, BSC01a, BSC01b, BQR01, CYH01, CL07, CC09, CC06, GW01, KB03, KC09b, LLS05a, LZ01, LWS05, LY07, LJ05b, LSC03, LSK05, PZL09, RS00, SDFH00, SDF01, SSFC09, SYLC05, TTZ01, TH01, TC01, UP05, VKS09, VK07, WY02, WL05b, YZEE09, AAP07, AA08, CC02b, CHC01, Che07, Che08a, KCO9a, LLCL08, Lin00a, LT04, LYGL07, LLC06b, MS09a, MB08, PBV08, Sch00a, Sch01c, S’03, Sch04a,
Sch04b, Sch05a, mSgFtL05, TL02, Wan05, WMS08, YCYW07, YCL07, ZLZS07.

Image-Feature [GW01].

image-identification [PBV08]. Images [CTL04, CC08, CW09, DP00, FGD01, LS08, PJH01, PBC05, RE02, WCJ09, WC04, YWWS09, AAPP07, AEEdR05, BDN00, FWT05, HHYW07, TCC02, TND+09].

Imaginary [HJW01, HM00, Huh00]. Imai [DDG+06, YG01a]. Imbalanced [ZWCY02]. Immerse [Coc01a]. Immune [CZK05, PZ02b, YKLM02b, ZP01, YKLM03]. Immunization [HR05]. Impact [Ber03, HGNP+03, JKRW01, MMYH02, Wri00, CS08a]. Imperfect [CPS07, DOPS04]. Impersonation [BP02, Hsu05b]. Implement [HQ05]. Implementation [AD07, AG01, Ast02, Ash03, Arc+01, BBD+02, CCDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK+03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HHM01, JKS02, KMM+06, KMS01, KTT07, KR+02, KV01, LP02a, MKP09, MM01c, MN01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBTW07, QSR+02, RDJ+01, SM01, Sha01e, SK05a, SRQ03, USS02, Vir03, WZW05, WW00, WOL01, XB01, Zea00, BI04, BBK+03b, C+02, CNPQ03, DKL+00a, GHdGS00, GBKP01, Hii00, HP01, Hutt01, KYY09, LL04b, LCX08, LB05, Rhi03, SM03a, SVDF07, Wol04, YW00, ZFK04].

Implement [HQ05]. Implementation [AD07, AG01, Ast02, Ash03, Arc+01, BBD+02, CCDP01, CGP08, CG03, CQS01, CS05a, Cor00a, EYCP00, EHK+03, FW09, FBW01, FD01, GC01a, Gir06, HTS02, HHM01, JKS02, KMM+06, KMS01, KTT07, KR+02, KV01, LP02a, MKP09, MM01c, MN01, MP01c, Mur02, Nov01, NMSK01, Oiw09, OTIT01, Pat01, PBTW07, QSR+02, RDJ+01, SM01, Sha01e, SK05a, SRQ03, USS02, Vir03, WZW05, WW00, WOL01, XB01, Zea00, BI04, BBK+03b, C+02, CNPQ03, DKL+00a, GHdGS00, GBKP01, Hii00, HP01, Hutt01, KYY09, LL04b, LCX08, LB05, Rhi03, SM03a, SVDF07, Wol04, YW00, ZFK04].

Implement [TSS+03]. Implementing [Dwi04, Kor09, LM08, LDM04, MWS08, NDJB01, Pet03, Smi01a, SR06, C+02, CW02].

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

Implies [KY01e]. Imply [Pie05].

Importance [Ano02b, KJC+01, TIGD01].

Important [SM00a]. imposed [XLMS06].

Possibilities [CHL02]. Impossibility [APV05, BPR+08, Fis01b, PQ06].

Impossible [BF00a, BF00b, CKK+02, HSM+02, MHL+02, Pha04, SKU+00, SKI01].

improve [Pau02a, CAC06]. Improve-ment [CAC06]. Improved [AS01c, AJO08, Che04a, CZZ05, CCW02, Di01, HWWM03, HWW03, Hwa05, LKY05c, LKY05d, LTH05, MNT+00, NP07, Sha04b, Sha05b, WHLH03, YRY05b, YRY05c, ZYM05, ZAX05, BLH06, CCK04a, CL04c, CHY05a, Hsu05a, JHW05, JmBDxGxM05, KJY05, LL04a, LW05c, SZS05, TO01, WLT05a, YW04, YW05, YRY05a, ZC09].

Improvements [BBM00, HWW02, JL03, NP02b, YCYW07, CH07a, SRQ03].

Improving [ASK05, Dim07, EBS01, KMT01, LHC08, LS01b, Mic01, SK01, 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, LKL05].

IND-CCA [Mi01b]. IND-CCA2 [BST02].

Independence [BP03b]. Independent [BS00a, BSL02, Kin02]. Index [Ano00b, Ano01d]. indexing [YPPK09].

India [CV04, JM03, MMV06, MS02c, RD01, Roy00a, RM04, Roy05, Ano03c]. Indices [Fra01, Syv02, Wri03]. individual [TW07].
INDOCRYPT [CV04, JM03, MMV06, MS02c, RD01, Roy00a]. Induced [Vau02].
Industries [USE00b, Industry [ANS05, Mad00, Ort00]. ineffectiveness [YL05]. Infeasibility [FS08]. Inference [Mu02b, CDD +05]. Infinite
[TT09a, TTT09b, Vau01]. Influencing [Bla01c]. Inform [Kwo03b, San05]. Information [AP09, BW07, BM00, BZ02, Big08, BB03, BJ02, Boy01, CGM07, CC06, DM00b, ECM00a, ELs01, Hay06, HQ05, HW01, ISO04, JDJ01, JG07, KP00, Ke02, KLB +02b, KO00, Lai03, Lee04b, LW05b, LL01, MH05, Oka00, PP06b, RSA00d, RS01, Roy05, Sch06b, Son00, Sta06, Ste02, TG07, VDK05, WABL +08, Yek07, Zhe02b, ZS05, vW01, ABHS09, ABW09, Ar01, Bii03, BK00, BEZ00, BE01, Bro05b, Dau03, FR08, FOP06, Gar04, Gha07, IV05, KN08, KB00, Kov03, MS09b, ME08a, PS02a, Sun02, TWM +09, Way02b, Way09, dLB07, CSY09, FLY06, GW00, Kim02, LL03, LL04c, PC05a, Won01, WK06]. information-flow [FR08]. Information-Theoretic [VDK05, vW01]. Information-Theoretically [DM00b]. Infrastructure [AHKM02, AL06, BC04b, BWE +00, CL07, ES00a, FL01b, KGL04, Sin01a, BM03, BS09a, Ben01a, C05, FB01, Gor05, LC04, MWS08, Ben02]. Infrastructures [HCD002, Lin00b, PTH03, WB001, Bra01a, LAPS08, SN07]. INIDP04 [LDM04]. initial [DK08]. Initiative [Coc01a, Cal00b]. initiatives [Mau05]. injection [MMJ05, ZSJN07]. Injective
[CMDv06, Kos01c]. Innovation [Sam09]. innovations [Web02]. Innovative [MM07a]. Innsbruck [Pi01]. Input
[CAC06, TC00, DKL09, VM03]. Input-trees [TC00]. Insecure
[Vau05b, Wal01, BJN00]. Insecurity [Bla02b, DOP05, Lai08, Man02, NS01b]. insertion [MB08]. insertion-extraction [MB08]. Insider
[CMS09, Tad02, KS05a, Mau04]. Insights [Kun01]. Inspired [CC09]. Installation
[USE00a]. instance [FS08]. Instances
[GG01, HN06]. Instant [BBK03a, RR05]. Instantiated [RR08]. Instantiation
[BF05]. Instruction [BBCG08, EP05, KTT07, Brr06, HTW07, MMJ05]. Instruction-Level [EP05]. Instruction-Set [BBG08]. Instructions
[LSY01]. instrumentation [MPM09]. insubvertible [ACdM05]. Insulated
[DKXY02]. Integer [Gro03, Jo03, MN14]. Integers
[CH07c, GM01a, KKM01, ERM00a]. Integral [KW02, WR09]. Integrated
[EC00a, ECM00b, GMG00, Lut03, GLC +04, LK01, SSM +08, SN04]. Integrating [Wit01]. Integration
[Ito00, CJL06, Sog03]. Integrity
[Ana02e, C08b, Jut01, MA00a, MA00b, Pre01, Sch01a, ABEL05, AL04, MD04, MNT06, SHJR04, Yun02b]. Intel
[Coe02a, MP00]. Intellectual
[Qu01, WY02]. Intelligence
[Cop04b, AJ08]. Intelligent [Co03]. Inter
[WRW02, ECM00b]. Inter-Exchange
[EC00b]. Inter-Packet [WRW02]. interaction [Gav08]. Interactions [Fau09]. Interactive
[DG00, MS09c, CHK05, DDO +01, Fis01b, Fis05, HNZI02, HJW01, KKL09, KKL09, MTS06, PAS05, vT00, MS09c]. Intercourse
[CHVV03]. interdomain
[MAB06, vWK07]. interesting [SWR05]. Interface
[RSA01]. Interference
[FGM00a, FGM00b, GA05, BR05]. Interlaken [CC04a]. Interleaved
[ZSJN07, NC09]. intermediaries [JA02]. Internal
[Haro07b, Be06]. International
[ACM03a, ACM04a, ACM05a, ACM09, ACM10, Ans00d, AAC +01, AJ01b, BDZ04, Bel00, B +02, BB09, BS01b, Bii03, Bla03, Bon03, Boy01, Buc00a, BD08, CC04a, CV04, CTL01, Chr00, Chr01, CCMR02, CCMR05, CS09, CGP03, Cra05a, DR02c, Des02,
DKU05, DFPS06, EBC+00, Fra01, FMA02, Fra04, FLA+03, GH05, HYZ05b, IEE09a, IZ00, IKY05, JYZ04, Jef08, Joh03, JM03, JQ04, Jue04, KKP02, KCR04, KJR05, Ki01a, Kim01, KN03, Kim02, KN03, Knu02, KP01, KNP01, Lai03, LL03, Lee04b, LST05, LL04c, MMV06, MJ04, MS05a, Mat02, MZ04, MS02c, Men07, NP02a, NH03, Oka00, Pat03b, PK03, Pf01, Pre00, PT06, RD01, RS05, Roy00a, RM04, Roy05, Scho1d, Sho05a, Si01, SM07b, Syv02, TB02, TLC06, Uni00a, VY01, Vau05a, WKP03, Wil99, Won01, Wri03, Yun02a.

International [YDKM06, ZJ04, Zhe02b, ZYH03, AMW07, AUW01, Ano00e, AJ01a, BCKK05, Bir07, BC05b, CKL05, DV05, DWML05, DRS05, GKS05, HH04, HH05, HA00, Hon01, May09, PC05a, PY05, PPV96, QS00, Sma05, Son00, ST01d, WK06, Ytr06].

Internet [SMP09, ABB04, Ben01a, Ben02, Cal00a, Chu02, Cla00a, Coc03, DP04, DGMS03, EM03, Gal02, GSS03, HKW06, IFH01, Jan00, MF01, McN03, MA00a, Mir05, PM00, PLW07, Ps01, Ph01, PHM03, Rub01, SBB05, SEK01, SEK02, Sto01, Tsa01, TWL05, Uri01, WC05, Wri05, ZG05, ky01]. Internet-wide [SBB05].

Interoperability [Hil00, TEM01, BHM03].

Interoperable [BFGT08]. Interpolation [LW02, YG01b, FWTC05, KT06].

Interpolations [Sat06]. Interpretation [Mas04, CC04c]. interpretation-based [CC04c]. Intersections [KS06a]. Interstate [RM02]. intranet [Jan00]. Intrinsic [ZWC02]. introduced [Ano00a].

Introducing [JL00]. Introduction [Ben02, Ber09b, Bis03a, BK06b, Buc00b, Buc01, Buc04, DK02, DK07, Fai07, Hay06, HPS08, HC02, KL08, MAA07, Mol01, Neu04, PTP07, PM02, PH03, Puc07, Res01a, Res01b, Rot05, Sak01, SJ09, SG08, TW02, TW05, TW06b, Big08, CS07a, CM05b, Gar01, HW98, Hro05, KP03, Mol07, RR03a, RP00, Sho05b, TW06a, Kat05b, Rot07, Lee03a].

Intrusion [CZK05, DFK+03, DP07, JT05, TZ05, TMM05, WG05, HLL+02, MAC+03, NCRX04, NN02, YbJ04, IR02].

Intrusion-Resilient [DFK+03, DP07, IR02]. intrusion-tolerant [YbJ04]. intrusions [Bej06]. invalid [CTJ04]. Invariant [Ben00, CT09, HH09, ZLZ07]. Invariants [WH09]. Invasion [ASW+01]. invasions [Yn05]. Invention [If00]. Inventors [Bar00c]. Inverse [Har06, OS07]. Inverses [CGH00a, Has01a, JP03, MFFT05].

Inversion [BNPS02, KKY02, KTT07, SPG02].

Inversion/Division [KKY02]. invasive [SB05]. Investigating [BW07]. investigation [Cas02]. Investigative [Men03]. investigator [KB00]. Invisibility [GM03]. Invisible [MB08, WD01b, WC04].

Invitation [Bar02]. Invited [FGM00a, Lan00d, DRS05]. involutional [SH07]. IP [Ano00a, CD01b, FXAM04, HL07, Lin07, MV03b, RW07]. IP-based [MV03b]. IPAKE [CPP04]. IPSec [Vau02, CGBS01, Dav01a, KMM+06, SKW+07, FS00, FS03a, XLS06]. IPSec-Compliant [CGBS01]. IPTables [GC05]. IPv6 [Nik02a, Nik02b]. Iran [Mah04]. Ire [Cos03]. Iris [CJL06]. Irregular [MH04]. Irregularly [CGFHS09]. Irreversibility [ZWC02].

ISBN [And04, Duw03, Eags05, For04, Gum04, Im03, Pag03, Puz04, Top02].

Island [CSY09, KGL04, Kim01, Lee04b, IEE07].


ISSAC [Jef08]. issue [FOP06, FOP06]. Issues [BDF+01a, BH00a, Hl00, KRV01, Mea01, PM+07, SEF+06, MKY08, Pat02b].

ISW97 [You01]. IT-Architectures [RM02]. Italy [AAC+01, AL06, BCKK05].
J2EE [BTTF02]. Jack [Coc03], James [Top02]. jamming [LPV+09]. Jan [YRY05b]. January [Des02, GL05, IZ00, Vau05a, Wri05]. Japan [Ano00d, Mat02, Oka00, Coc02b, Smi01b]. Japanese [IY00]. Java [Ano04b, Mar05a, WBL01, Ano02e, Ano03a, Ano04b, Ano04c, AJ01a, BCS02, Bis03a, BJvdB02, CMG+01, Che00, CCM05, Coo02, DPT+02, DJLT01, Dra00, EM03, Gal02, GW08, GN01, HM01a, Has02, Hoo05, Hum05, Lai08, LBR00, Ler02, LDM04, Mar02a, MWM01, Nis03a, RC01, Rot02a, SA02, SL00, Str01b, SJ05, Vir03, Wei04, Win01, Zea00, ZKF04]. Java-Based [EM03, DPT+02, GW08]. Java-Lösung [Ano04b]. JAVA-Ring [WBL01]. JavaCard [AJ01a]. JavaCards [Cim02]. JavaScript [TEM+01]. javax.crypto [Win01]. JBitsTM [MP01a]. JCCM [CMG+01]. Jean [MFS+09]. Jeju [CSY09, Lee04b]. Jeng [QCB05b]. Jenness [Sal03b]. JICC [HYZ05b]. Jin [Coc01a]. Job [MYC01]. jobs [Oue05]. Joel [Gum04]. Johannes [Lee03a]. John [And04, BZ02, NH03, Rot07, Coc03]. Joins [Bar00c, Con00]. Joint [ADI09, ADR02, CR03, HYZ05b, HYZ05a, Puc03, MI09]. Jörg [Fal07]. Jose [Poi06, Pre02c]. Joseph [LBA00]. Journal [LLLZ06a]. Journey [FF01b]. Jr [Kat05b]. Judiciary [Unio00h]. Julius [Chu02]. July [ACM01a, CZ05, Jef08, KJR05, May09, PPV96, Roy00b, Sch01c, S+03, Uni00a, Uni00b, Unio0e, Unio0d, ZJ04]. Jump [MP00]. June [ACM03a, ACM03b, ACM03c, ACM04b, ACM04a, ACM05b, ACM07, ACM09, ACM10, AL06, BS03, BS01b, BCDH09, BC01, CZ05, FMA02, IEE05b, IKY05, JYZ04, KGL04, KN03, KM07, PPV96, TB02, USE01b, USE01a, USE02c]. Just [ABB+04, Ano06a, Gut02a, Car01]. Kahn [Gas01]. Kaikan [Ano00d]. Kaspersky [Ano08a]. KASUMI [KYH01, KSHY01, SM02]. Katholieke [BB00]. Katz [Bar00a]. Keccak [BDPV09]. Keep [DM07b, Lys08, FS04]. Keeping [SEK01, SEK02]. KEM [NMO05]. Kerberos [BC+06, Coc01a, Gar03b, Hii00, It00, LLW08a, MJ01, MPPM00, Rub00, Smi01a, Wac05, WD01a, Wit01]. Kerchoffs [KMZ03]. Kernel [Int00, Mor03, BK05, HB06]. Key [ANS05, ASW00, AK02a, Ano01j, AAFG01, AEAQ05, AL06, AF03, ABM00, BC05a, BPS08, BH06, BD+01, BDZ04, Bar00a, BPS00, BPR00, BBDM01, BY03, BOHL+05, Ben02, BLMO1, Bib00, BBB+02, BDK+09, BR00b, BM03b, BDTW01, BMN01, BM03c, BMO01, BCP01, BCP02a, BCP02b, BM01c, BST02, CK02a, CK02b, CH03, CHK05, CPP04, Che01a, CT08a, CHK008, CCM02, CCM01, CM00, CS02, CS03b, CS03c, DPV04, DJ01, DPOS, Des00c, DBS01, Des02, DG03, DY09b, DKXY02, DFK+03, DGH+04, DBS+06, ESG+05, EP05, ES00a, FL06, FKS00, FMS01, FL01b, GL03, GJKR03, GW00, GL01, Gl03, GH01, GC01b, GSB+04, Gut04b, HNZ02, HCD02, HLM03, Hoe01, HR05, HG03, HC08, HJW01, HS07, HLC08, IEE00b, Ina02a, Ina02b, JL08, Jou02, JG01, Jue04, KGL04, KOY01, KY03, Kat05b]. Key [Kel05, Kel00, KKKI01, KM01a, KLY02, KKY02, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KU02, KOMM01, KY01e, Kur01, KI03, LCK01, LLL02, LP03, LV00, Len01, Lin03, Lin00b, MPS00, Mac01, MS02, MHM+02, May04, MR01b, MR01c, Mö03a, Mol03b, Mü01a, MUR00, NIS03b, NA07, Ngu05, NBD01, NSS02, OTU00.
Ort00, PHK+01, PR01, Poi02, PHM03, RSA00a, RR00, RW03a, RW02, ST01a, ST02, Sha01c, Sin01a, SK00, Ste01, ST01c, TS000, Tan07b, TT01, VV07, Wai03, WZW05, WH01, WC01a, Woo00, WBD01, Wya02, YKMY01, YI01, YG01c, YDKM06, Zhe02a, ZWCY02, ABHS09, AJ08, AUW01, AKLRT04, AF05, BH03, Bad07, BBN+09, Ben01a, BB79, BG08, BBG02, BD00b, Bra01a, BCP07, BMA00a, BMA00b, BMA00c, BD04b, CCT08, CL02b, CZ05, CY05, CYH05, Che04a, CHC04, CY05].

key [CLC08, CKRT08, CWJT01, CJ04, Cho06, CHH+09, CJL05, Cre00, DFM04, DMT07, DW09, EKRMA01, ED03, EHKK04, FMY02, FP00, GMLS02, Gal02, GH08, GL06a, GM00, GKM+00, GS01, GL06b, GMW01, HCD08a, HCD08b, HAU04, HHG06, HLLL03, HTJ08, HG05b, HWWM03, HMvdLM07, Hwa00, HLLL04, IZ00, Iwa08, IM06, Jan08b, JRR09, JW06, JXW05, JZCW05, KY00, KS05a, KRY05, KPT04, KRY05, Ko000, KW00, Kos01c, KHKL05, LHL03a, LF03, LKKY03a, LKKY03b, LCP04, LL04a, LW04, LLLL03, LL05a, LKY05b, LKY05c, LKY05d, LLY06, LLS+09, LCK04, LPM05, LHC08, LKJL01, LSH00, LS01c, LCC05, Lop06, MWS08, MKKW00, MP08, Mis08, Mii01b, NP02a, PS08a, PI06, Pei09, Pei04, PQ03a, PQ06, PC09, PSP+08, PLJ05b, Poi06, Pri00, RHO3, SNI00, SLP07, SRJ01, SBZ04, Sha05c, Shi05].

key [SL05a, SW05, Sh04a, SC05b, SIR04, SLC05, Sun00b, Sun02, SZP02, SCS05b, SC05c, SCS05c, TP07, TO01, Tsa06, Tsa05, Tse07, VS01, Vau05a, VK08, WDL09, War00, WGL00, WV00, WC01b, Wu01, WL04b, WHHT08, XH05, YW05, YC09a, YS02, YS03, YS04, hY08, Yi04, YR05a, YY05b, YPKL08, ZL01, ZC04, ZK05, ZSM05, ZYW07, ABB+04, GL05].

Key-Based [Sha01c, Key-Dependent [Gol03, BPS08]. Key-Exchange [BH06, CK02a, KS05a]. Key-Insulated [DKXY02]. Key-management [JW06]. Key-Privacy [BBDP01]. Key-Recycling [DPS05]. Key-Share [CT08a]. Key-Sharing [HNZI02, WBD01]. Keyboard [ZZT05]. Keyczar [Law09b]. keyed [Küh08, SR00, FIP02a]. Keyed-Hash [FIP02a]. keying [ABB+04, Che08a, EGG08]. Keyless [Qu01]. Keys [AOS02, APV05, AF06, BT02, BMK00, BGW05, CHM+02, EHMS00, Fer00, HSH+08a, Luc00, MN01, MRL+02, Oni01, PS00, Sni01c, Str02, TvdKB+01, BCL05a, BC05, Ber09a, BF01c, CWH00, CCH05, CJ05, HSH+08b, HSH+09, HW04, HY03, HL04, KAM08, LLW08b, LS01c, LWK05a, ML05, NN03, Sch01e, Sha04b, Sha05b, SB05, TLH05, TJ03, WH03, YRS+09].

Keystream [AMRP04, Kra02a, LV04, MH04, WIW04, PS01a]. Keystroke [MR00, BGP02]. Keystrokes [SWT07].

Keyword [FIP05], KG [LC08], KG [ZYW07], KH [Q03b], KI [May09]. Kid [CAC06]. Kikai [Ana00d]. Kikai-Shinko-Kaikan [Ana00d]. kill [Lov01]. Killing [Lov01]. kind [DW01].

Kindi [MaT03, MAxTxx]. King [Eag05]. Kingdom [DCF00]. Kingston [HA00, PT06]. Kit [Ana02e]. Klaus [Ana04]. Kleptographic [YY01]. knapsack [Kos01c, SLC05]. knapsacks [Mic02a].

Knife [Boy03]. Know [CMB+05, Ros07, Con09, DKK07, Win05c].

Knowing [CH01a]. Knowledge [Abe01, Abe04, AS01b, APV05, BP04, Con01, DPV04, DFS04, DDO+01, Eri02, Fis05, Gen04a, GK05, HNO+09, KS06b, LMS05, LH+08, MR01b, MV03a, Pas05, Ros00, Ros06a, TG07, BSV08, CLR09, Dam00, Hro09, IKOS07, JRR09, PBD07, KIK07].

Knowledge-of-Exponent [BP04]. Known [CKN06, CMB+05, DNM2a, Fur02b, HSH+01, Bao04, YTH04]. Known-IV [HSH+01]. Known-Plaintext
[DN02a, Fur02b, CKN06]. knows [Fox00].
Koblitz [AHRH08, Has01b]. Kolmogorov [Sch01a]. Kommunikation [Lin02].
Kong [B+02, ZJ04, Cla00b]. Konstantin [Puz04].
Korea [CSY09, CKL05, KCR04, Kim01, Kim02, Lee04b, LL04c, May09, PC05a, PK03, Son00, Won01, WK06].
Korner [Mor03]. Kosciuszko [OC03].
Krawczyk [Miy01]. Kryptoanalyse [Mor05].
Kuala [DV05]. Kunming [ZYH03].
Kurosawa [CHH09]. Kurtz [Gum04]. Kyoto [Oka00].

L [Sem00]. L-collision [Sem00].
Laboratory [Bru06, LBA00]. Lagrange [FWTC05].
Laid [Wei06, Wei05]. Lam [Wag00].
Lamar [LMHCETR06]. Lamp [McN03].
LAN [Bar03, Pau03, SZ08, Sty04].
Lanczos [BF06a]. Landau [Jan08a].
Landscape [Ahm07]. Language [ARC01, DD02, Gou99, Jen09, MW04, WAF00].
language-based [WAF00]. languages [Lun09, Rob02, Rob09].
Languages [Lun09]. Laplace [Bau03a, Bau03b, BH00b]. Lead [Tsa07].
Leak [RST01]. Leakage [CKN01, DP08, Kel02, RS01, ABHS09, CNK04, IY05].
 Leakage-Resilient [DP08]. Learned [GSB04]. Learning [KS06a, LY07, CAC06, BKW03, Mal06, Reg05, Reg09, SM08, Whi09]. Least [SZ01].
lecture [Rot02b, Rot03, Adl03, RSA03a, Riv03, Sha03b]. Lee [Sty04, Coo02b, KRY05, KLC03, KHK05, LKY05d, SCS05b, ZK05].
Left [Dhe03, HKPR05]. left-to-right [HKPR05]. Legal [Coo02a]. Legislation [Eng00]. legislative [AvdH00]. legitimate [Lin01a].
Leighton [Rub00]. Leighton-Micali [Rub00]. Length [AR01, BR00b, CKN00, CHJ01b, Mol03a, RK06].
Length-Preserving [MGL03a]. Leonard [Coc03]. Less [YKMY01, BD00b]. Lessons [GSB04, KFS00]. Lest [HSH08a, HSH08b, HSH09]. Lets [Pan02a]. Lett [Kwo03b]. Letters [ASW01, BTTF02, MNT00, TEM01, TvdKB01, WWL02].
Leuven [BBD09, DR02c]. Level [EP05, MV00, TV03, BDN00, DHL06, KVN09, SS03].
levels [CUS08, Voi05]. Leveraging [BRTM09]. LEVIATHAN [CL02c]. Levin [AC02]. LFSR [Jan00, JZC05].
LFSR-Based [Jan00]. LHL [Pei04, YRY05a]. LHL-key [Pei04, YRY05a]. Li [JW01, KLC03, SZS05, QCB05a, SCS05b, ZK05]. Liaw [TJ01b].
Liberty [Lan04b, An000e]. librarian [PBV08]. Libraries [Fin02, MK05b].
Library [KSZ02, Lau05, Law09b]. Libre [Jen09]. license [An000h]. Lies [Gan01b, Sch00d, Swa01]. Ste05c]. Life [Coo04b, GSB04]. lifecycle [HL06].
Lifetime [Coc01a, CPG04]. Lifting [CNS02]. Light [WT02]. Lightweight [WT02]. Lightweight [EPP07, Mal02, CH07a, CL09, MP07].
Like [Coc02a, PSC02, VMSV05, BCDM00, CWH00, DLP09, Egh00, EBS01, Egh00,
M [DNRS03]. M8 [TM01]. MA [ACM10, JQ04, Ki05, KP01, Nao04, Pag03]. MAC [BKN04, CKM00, Ki03, LPV+09, Vau01, Krs03]. MacDES [CKM00]. Machine [LBA00, Mal06, Pro00, Cas06, Kid00, Pau02b, SWR05, WNQ08, Win05b, HM01a, Pet08]. Macraigor [Ano02d]. MACs [BPR05, BR00b, BM01c, Sem00]. Made [Ste05b]. Madison [FMA02]. Maelstrom [MYC01]. Magic [DNRS03, Bur02, Hro09]. Magyarik [dVP06]. Mail [ANR01, Cos03, KS00a, Law05, LL04b, NZS05, All06]. Mainframe [Web08]. mainstream [Bjo05]. 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 [LH07, SZ03]. Man [Gen04a, Urb01]. Man-in-the-Middle [Gen04a]. Management [ACM03a, ACM04a, Ano02d, Ano02e, BP07, BW07, ELVS01, FMA02, GKK04, Gut04b, KB06, Lin00b, Scr01, Sha02, Wud00, Wya02, ASW00, AJS08, AFB05, CG06, Cha05a, GTY08, ISO05, Jan00, JW06, KHYM08, KAM08, LMW05, LPM05, LR01, LK01, MKK00, Pot06, RH03, SRJ01, Sen03, UP05]. manager [KH03, Sha01a]. Managing [MA00a, MA00b, NDJB01, Oue05, PTP07, PBB02, Tot00, BJ02, Kov03, KH03]. Mandrake [TvdKB+01]. MANETs [STY07, DF07]. manipulation [SWR05]. Manuscript [GG05a, Ruc04]. manuscripts [MAaTxx]. Many [BB02, Di 01, MP03, Di 03, SVDF07]. Many-Round [MP03]. many-to-one [SVDF07]. map [KJ01, Lee04a, PC05b, SL09]. Maple [Cos00, TT00]. mapping [Tan01]. Maps [BGLS03, BMS03, CL04a, LLL+01, WP03, JK01b, MA02]. Maqasid [MAaT05]. Marcel [Irw03]. March [BDZ04, Bire07, Bla03, HR06, PY05, Sii01, Uni00g, Uni00h, Ytr06]. Marian [Kap05]. Marjan [BCB+05]. Markers [FBW01]. Market [Bar00a, Ano001, Swi05]. Marketplace [PLW07, VN04]. Markov [KW03]. Marks [Ano01c, YSS+01]. Markup [Uni00a, Uni00d, Uni00e]. Marrakech [IEE09a]. Marriott [USE01b, USE01a]. MARS [BF00a, BCDM00, Fer00, IBM00, IK00, KS00a, KS00b, KS01, SOTD00]. MARS-like [BCDM00]. Mary [Ree01, Sin99]. Maryland [ACM05b, ACM05c, ACM09, SMP+09, GL05]. masked [AH08, Land08]. Masking [CH02, CT03, GK02, Lav09]. Massachusetts [IEE05b, USE01b, USE01a, IEE03]. masses [Pot06]. massively [FP00]. massively-parallel [FP00]. Match [JJ00a, WC04, LL06a]. Matching [ABM08, Len01, UEBP09, Vo05]. materialized [MP09]. Materials [SLT01]. Math [SR06, 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 [RSA99b, PPV99]. Matrices [TL07, CFVZ06, LMTV05]. Matrix [CV03, BF06a, OS07]. Matroids [CDG+05]. Matsumoto [DG+06, YG01a]. Mature [Tro08], Max [Di 01]. maximal [Huh00, HJW01]. maxims [Bau00, Bau02a, Bau07]. Maximum [KMT01, ZC00, DW01]. May [ACM00, ACM02, ACM05c, ACM06, ACM08, ACM09, Bie03, CC04a, Cra05a].
DRS05, IEE01b, Kau02, KNP01, MJ04, MS05a, PM00, Pi01, Pre00, TLC06, Unio06, Uni00c, YKLM02a, Pa02a, YJ00]. Mbps [LMP01]. McClure [Gum04]. McEliece [CFS01, Ki01a, Ki01b, Loi00, L01c, Sun00b]. McEliece-Based [CFS01]. McFarland [Car02]. McEliece [Gum04]. MD4 [DG02, WFLY04]. MD5 [Eke09, WFLY04]. Mean [Bar00c, KLML05, Ver06b]. Means [LMHCETR06, Nis03a]. measurement [Lav09]. Measurement [Ano02e, c01, CO09, FXAM04, RW07]. measurement-based [FXAM04]. Measures [CB01, Q501]. Measuring [Siv06]. Mechanism [Bel01]. Mechanisms [BACS02, CJK04, Lin00a, MD04, Mir05]. mechanized [dH08]. Media [Hei07, Ano02d]. Median [Cap01]. Mediated [DT03, CG06]. mediator [SBG05]. mediator-free [SBG05]. medical [AL07]. Medicine [MYC01]. Meet [Cha00a, HG07]. meeting [Je08]. Meets [Way02a]. Melbourne [IZ00]. Member [CTH08]. Membership [NBD01, Fis01a]. Memoir [Bar05]. Memorable [KOY01]. Memoriam [DNR03]. Memory [AK03, AJ08, BS00b, CCM05, DK08, DGN03, HNZ02, HBdJL01, KCJ01, Oec03, OT03b, QSR02, RSP05, YEP06, CC05d, Has00, Oiw09, Pa02a, ST06, XNK05, YGZ05]. Memory-Bound [DGN03]. memory-safe [Oiw09]. Memoryless [Sar02]. MEMS [EGG07]. MEMS-Assisted [EGG07]. ment [CAC06]. menu [Mea04]. Mercy [Fut02a, Cro01]. Merkle [CDMP05, JLMS03]. Mersenne [Aro03d]. Mesh [LPZ06, ZTP05, KB09, LZP04, YPSZ01]. Meshes [BG08, Lav09]. Message [BR02, BWBL02, BDF01b, CV03, Co02b, FIP02a, FGM00b, GTZ04, Jut01, OM09, SNR04, WS03, Zol01, BPS08, CCH05, CJ05, Gav08, HW05, MD04, MS09c, Sha04b, TJ03, Wu01, ZF05, ZAX05]. Messages [Ara02, AR01, Br00b, CHJ01b, DSO5b, Sch09, Wri05, Zho06, Alv00, Ano00c, BCG02, Bih02, BB79, Lim09, SP79]. messaging [Opp01, RR05]. meta [SM08, PLJ05a, QCBO05b, Sha05d]. meta-learning [SM08]. metadata [CDS07, FJ04]. metanomorphic [CSW05]. Metaphor [CNB02]. Metering [BCO4b]. Method [BDTW01, GHK06, GL00, Gro01, HRS02, HQ05, JKK01, M002, OKE02, OT03a, OT03b, SOH01, TIG01, TSO00, WH09, WNY09, ZL05, AMR04, DwWmW05, Gut04c, JL03, MSP09, MFK06, WG02, WWTH08, kWpLwW01, WLL04, YC09b, YC09b, YC09b]. Methodologies [SPMLS02, NDM04]. Methodology [VMS05, HM02a]. Methods [BCDM00, FD01, Kin00, Lan00d, Mea01, Neu04, Sal05b, Sch06a, SM07b, TNM00, Vir03, Bau00, Bau02a, Bau07, BGM04, BHC05, CM05b, GKS05, JZCW05, LMSV07, Mal06, SSST06, SHp99, YW06]. Metric [LBGZ01, LBGZ02]. Metrics [LZ01, NP07]. Mexico [Buc00a]. MGC05 [ACM05a]. Miami [Des02]. Micali [Rub00]. Michael [Ter08]. Micro [ASK07, Eng00, Ste05c]. Micro-Architectural [ASK07]. microcontrollers [GBK01]. Microelectronics [IEE09a]. Microprocessor [Web08]. Microprocessors [LMI05]. Microscopic [MYC01]. Microsoft [Bon00, Scr01, Ste05b, Wth00]. Middle [Eag05, Gen04a, HG07, Kin01]. Middleware [ACM05a, KRV01, LG01, MB04]. Migration [Pat02a]. Mikhailovsky [Puz04]. Milan [dCdVSG05]. military [Ark05]. Million [Ran55, Ran01, Ano03a].
MIME [Dav01b, Dav01c, Opp01]. Min [MR01b]. Min-round [MR01b]. mind [Lau08b]. Mine [For04]. Minimal [FBW01, FGM01, JY01, SC02b]. Minimalist [Tro08]. Minimizing [LPM05]. Mining [LP00, Lut03, HLL+02, Mal06, Men03, Pin02, Pin03, ZY08]. MiniPASS [HS01b]. Minos [CC05e]. MinRank [Cou01]. Minutiae [UBEP09]. Minutiae-based [UBEP09]. Misbehaving [JQY01, SBB05]. Misinformation [CZB+01]. Missed [TvdKB+01]. MIST [Wal03]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Mistakes [LPM05]. Missed [Xue01]. Modelling [HLL+02]. Mobile-commerce [YC09a]. Modular [BI00, BK00, CM00, CH00, D00, F00, G00, H00, H00, J00, K00, L00, M00, N00, O00, P00, Q00, R00, S00, T00, U00, V00, W00, X00, Y00, Z00]. Monoalphabetic [GPG06]. monolithic [GHdGSS00]. Monotones [WW05]. Motion [EFY+05, hKLS00, WMDR08]. Mountain [JYZ04]. mouse [HLwWZ09]. move [Jac00]. movement [HLwWZ09]. MP
[MP07]. MP3 [DRL09]. MPEG
[LS05, MLC01, SQ07, YZD07]. MPEG-4 [SG07]. MRF [Che01a]. MRM
[TIGD01]. MSP430x33x [GBKP01]. MSXML [TEM+01, Hei01]. Mu [CJT03].
much [Con09]. Multi
[ARR03, BBM00, BR06, CCD07, CJK+04, CD06, CDG+05, DLY08, DJL01,
FGMO01, FWW08, Gen04a, HM01b, HS07, JLL02, Kur01, LV07, LLL04, Tsao01, ZJ09,
BSSM+07, CLO02, CC05a, CHY05a, CHY05b, DZL01, FWTC05, GML02,
HHY07, HWH05, HC04b, HL04, LHL03b, LC025b, LW05c, NC09, PW05, SC05a,
TWL05, TYH04, YCH04]. Multi-applications [DJL01].
Multi-Authority [JLL02]. Multi-channel [ARR03]. Multi-designated [LV07].
Multi-Domain [CJK+04]. multi-factor [BSSM+07].
multi-hop [NC09]. multi-linear [LL04]. Multi-party [CD00, CDG+05, FGMO01, FWW04,
HM01b, LLL04, CLO02]. Multi-property-preserving [BR06].
Multi-Proxy [ZJ09, HC04b, LW05c, TYH04].
Multi-Receiver [CCD07]. Multi-recipient [Kur01]. multi-scroll [HYW07].
multi-secret [CC05a, CHY05a, FWTC05, PW05, SC05a, YCH04]. Multi-server
[Tsao01, LHL03b, TWL05]. Multi-Servers [HS07]. multi-signature [HHY05, HC04b,
HL04, LC025b, LW05c, TYH04].
multi-stage [CHY05b]. Multi-trapdoor
[Gen04a]. Multi-user [BBM00, DLY08, GML02]. multi-valued [DZL01]. Multiagent [ZS05].
Multiagent-Based [ZS05]. multibit
[TND+09]. Multicast
[AP01, BPS00, BDF01b, ASW00, GIKR01, GL06b, JAO2, KB09, MP08, PCS03, YC08].
Multicollisions [Jou04]. Multilevel
[LN04]. Multimedia [AAK09, FMS05, GA05, HL07, LLR07, Sun05, WLLL09,
DY09a, DKU05, Laf00, Ren09, SG07, YC08]. Multimodal [PY08]. Multiparty
[BGOY08, CDN01, DN03, DIO5, GI02, OZL08, CDD00, HTO4, IK0507]. multipath
[SK05b]. Multiple [Aik+01, Ara02, BDQ04, CK01a, CK01b, CHSS02, Che08b, DI05,
Har00, HZSL05, HL01, Jab01, STK02, SR06, TIGD01, BLH06, Che04a, CIO4,
DM07a, HL00, KC09a, MN14, Sha01d, SW05, TC002, YW05, YSH03, YRY05b].
multiple-key [Che04a, CJ04, SW05, YW05, YSH03, YRY05b]. Multiple-Precision
[HZSL05, MN14]. Multiple-watermarking
[Che08b]. Multiples [HR00]. Multiplication
[AREG08, ADDS06, BKP09, CMJ03, CH07c, Dhe03, GLV01,
HM02c, KKIM01, Mio02, NMSK01, O01, Tan07a, Wa01, BIN03, Dw0W05, FP00,
GD05, Ha00, Mis06]. Multiplications [Har06, OT08b]. Multiplicative
[Has01a, KO03, MFT05]. Multiplier
[HA+05]. Multipliers
[CMJ03, KWP06, RMH03b, WS05, HGN03, RMP08, RMH03a]. Multiply
[KT07]. multiprocessor [ISTE08]. Multipurpose [Boy03]. Multireceiver
[HSZ01]. Multiresolution
[LL0500, YPSZ01]. Multiset [aSM01]. Multisignature
[Tao02, CWH00, CL04c, CCH04, He02, LC04b, LW05b, Wa01, Y05a, Z04].
multisignatures [CL00, WH02b]. Multithreaded [Zha00]. Multivariable
[DS05a]. Multivariate
[DI050b, BP09, FP09]. Municipal
[MILF+08]. Music [MNS01, XMST07].
mutargima [MA05]. Mutation [Lut02]. Mutual
[JP02a, KH05, CSS08, VK08].
Mutually [WC01a]. MYCRYPT
[DV05]. mysterious [Bel07a]. Mystery
[GG05a, Rug04]. Myths [G03, kc01].
N [Mar05a, AOS02, K01]. NAF
[OT03b]. Names
[Coc01a, Sha02, Ark05, CGV09]. Naming
[Ano01b, BH00b]. Nanotechnology
[RR03a, RR03b]. Naor [Zha06]. Napoleon
[Urb01]. narrowing [MT07]. NASA
[Ano02c, Wil99]. Nation [Lan04a]. National
[BWE + 00, Jol01, LCS09, AJ08, Bam02]. National-Scale
[BWE + 00]. Natural
[ARC + 01, Top02, WMS08]. Nature [Pag03].
NaPi0 [Goo00]. Nazi
[Hau06, KS04]. NC [AIK04]. nCipher
[Ano03e]. NCP [SQ01]. NCR [LBA00].
Near [BC04a, DPS05]. Near-Collisions
[BC04a]. Necessary [LCK03, MN01].
Necessity [SBZ02]. Nederländen [dL00]. Need
[Coc01a, HR04b, Sty04]. Needs
[CZB + 01, DKK07]. Negotiation
[DBS + 06, HHJS04, IY05, LLW05, LLW09].
Nema [Kid00]. NIESSE [Pre01, Mac00,
Pre02a, Pre02b, SGB01, DPV00]. nested
[LCK04]. Net [CACA03, Ano08b, LKJL01].
Netherlands [Kna02]. Nets [AADK05].
Netspionage [BK00]. Network [An020d,
An03b, Bar03, BGOY08, Con04, CLZ02,
Dim07, FBWC02, Gm04, Har05a, IKY05,
JYZ04, KKG03, KPS02, Ken02b, LMP + 01,
Lu07, Mal02, NN02, PJDH09, PZL09, Poo03,
RCBL00, RC05, Sty04, TLYL04, VMC02,
YC01, ZYH03, ZS05, Br06, CJ03b, CMS08,
Coc01a, DWML05, GKS05, HLL + 02, LC03,
LPV + 09, ME08a, MSK03, Mi08, Pri00,
RAL07, Sch00c, Sta02a, TIS07, Vac06,
Wyl05, YLT06, ECM00a, ECM00b].
Network-Attached [RCBL00].
network-based [HLL + 02]. Networked
[Sch00d, LB05]. Networking
[ACM01b, Ros07, VM03]. Networks
[AE05, BJLS02, CGM07, DBS + 06, Fin06,
GPC08, Gor05, JKRW01, KZ01, Ken02a,
KH05, LNL + 08, NAB03, PR01, RKKZD02,
Sin01a, WT02, Zea00, ZYN08, ZWY02,
AJS08, BBG + 02, BC05b, CCM09, CG03,
CBD + 05, DHMR07, ETMP05, HJ07,
HMvdlM07, JRR09, KXTZ09, KHYM08,
KB09, LDH06, LHC08, LW05a, Lin07, LN04,
Lop06, LKZ + 04, MWS08, MJF + 08, MS09b,
NC09, NLD08, PCSM07, PS08a, Pat02b,
SLP07, SSM + 08, TP07, TM06, TCR03,
TW07, WDLN09, YC07, ZSJN07, ZBLvB05,
Ano02d, CS08b]. Neural
[KMS02, PZL09, PR01, YC01, YC07].
Nuclear [KMS02, PZL09, PR01, YC01, YC07].

Neural-Network [YC01]. Neveu [QS00].
Nevada [ELvS01, IEE01a]. Never
[Wei00, Hau06]. Newfoundland [NH03].
Newman [Pag03]. Newmanry [Sal01a].
News [An03c, Bar00a, Bar00b, Bar00c,
Cla00a, Coc01a, Coc02a, Coc02b, Coc03,
Eng00, Fox00, MC01, MP00, PM00,
Pau02a, Pau02b, Pau03, Pau09, Pri00,
CAC03, CAC06, Sta05, Raj06]. Newton
[KT06]. Next [ESG + 05, Mc06, TV03,
Web08, BD04b, ISTE08, RR03a].
Next-Generation [ESG + 05, Web08]. NFA
[DIS02]. NFS [Sta02b]. Nice [DS06, JJ00c].
Nicko [An03e]. Nimbus [Fur02a, Mac00].
nine [Tat05]. Ninth [USE00d]. NIST
[BG07a, Dra00, H0r09, 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
[DPV00]. Noise [BK03, GA05,
MPSW05, SM00a, SM00a, PC00].
noise-based [PC00]. Noise-tolerant
[BK03]. noisv [HGSN03]. Nominative
[PL01]. Non
[BR05, CHK05, CBZ + 01, DN00a, DDO + 01,
DW09, FF00, Fin01b, Fin05, FGM00a,
FGR05b, HNZI02, HJW01, IY02, IYK03,
JT01b, Kos01c, KO00, MSTS04, Nie02b,
PHK + 01, Pas05, PK08, WBL01, DOM7a,
DS02, HHH00, HLL04, IM06, KKL09,
KH09, LSA + 07, PR05, RP00, SC05c].
Non-adjacent [JT01b]. Non-committing
[DN00a, Nie02b]. Non-Cryptographic
[WBL01, IYK02, IYK03]. Non-injective
Non-interactive [CHK05, DDO+01, Fis01b, Fis05, HNZI02, HJW01, MSTS04, Pas05, KKL09, KHL09].
Non-interference [BR05]. Non-malleable [DW09, FF00, PR05]. Non-maximal [HJW01, Hüh00]. Non-OOD [CZB+01].
Non-deviation [BR05]. Non-malleable [DW09, FF00, PR05]. Non-maximal [HJW01, Huh00]. Non-OOSD [CZB+01].
Non-perfect [DM07a]. Non-physicists [RP00]. Non-quantum [IM06]. Non-trivial [KO00]. Non-Uniform [SPK08].
Nonce [CY05, LKY05a]. Nonces [BR00a]. Noncontact [Sak01]. Noninterference [DFG00].
Non-invertibility [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]. Notarized [GTY08]. Notation [Eag05, Kin01]. Notes [KSF00]. Notion [Des00c, SR00].
Notions [BPS00, BN00a, CK02b, DKMR05, HU05, Kos01a, Des00a, KY00, PS04c]. Novel [CC02a, CYH01, CDTD05, CW09, HC08, MP01c, WCJ09, AJ08, BG08, CCS08, GB09, HG05a, SPG02, SCs05a, mSGfLt05].
November [ACM0b, ACM0a, BZ02, CKL05, Eko02, IEEE00a, IEEE02, Lai03, LL03, LL04c, MS05b, PK03].
Notion [Dew08, Gou09]. Novo [Bi09]. NP [AGGMe6, FS08, HN06, AGGM10].
NP-hardness [AGGMe6, AgGM10]. NPCryptBench [YLTO6]. NSA [RC05].
NSS [GJS01, HPS01]. NT [Str01b, USE00a]. NT/2000 [USE00a].
NTRU [GJS01, GSO2c, HPS01, HHP+03, HGPN+03, HG07, JJO06, NPO2b].
NTRUEncrypt [HGH06, KY09]. NTRUSign [HHG06, HHG06, HW108, ZJ09].
NTRUSign-Based [ZJ09]. Number [BIP05, BST03, BK06a, Che08b, Cos00, CD01a, CFS05, Dic03, DGP07a, DGP07b, DV08, Ego05, EHK+03, Fin06, Gon06, GPR06, Hig08, Int03, Kat05b, Kel05, Ket06, KM01b, LMHCETR06, LNS02, MNP01, NR04, RSN+01, SP05, Shp09, Shp03, SFDF06, TWNA08, TL07, TTT09a, TTT09b, Vav03, Wal00, Yan00, YKLMB02b, Aam03, AUW01, BK07, Bel08, BPGS05, BG08, Bg09, Bg07a, BILL+03, CNPQ03, CO09, DIM08, DGP09, FP00, HGO5a, HGN0s, HLaWZ09, HP01, JAWt00, JL03, KH08, KSF00, Kin01, Lam01, Mit00, Nie02a, Nie04, Pan07, PSG+09, PSP+08, PC00, RGX06, Shp05b, Shp05, Sim02, Ste08, SR07, SK01b, Tat05, Wag03, Was0b, ZYEE09].
Number-Notation [Eag05, Kin01]. Number-theoretic [NR04]. Numbers [HSR+01, HFB09, ffr00, 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, Sh01].
Obfuscated [NS05b]. Obfuscating [BG+01]. obfuscation [CT02]. Object [RSA00e, DHL06, MWM01, ST06].
object-oriented [DHL06, MWM01]. Objects [CCM05, ZTP05, PB01, Whi09]. Oblivious [CT08b, Din01, FIPR05, IKNP03, SDF01, GKM+00, KKL09]. obscurity [MN03]. Observability [JQYY01].
observers [JL04]. Obstacles [KM04a].
Obtaining [Bar06b, BP03b]. OCB
[RBB03]. occur [Web02]. Ocean [MYC01].
October
[AJO8, BD08, CKL05, IE01a, IE03, IE04,
IE05a, IE06, IE07, IE08, IE09b, 
KCR04, LST+05, TTZ01, USE00b, ZYH03].
Octopus [Cla00b]. Oded [Lee03b].
Odyssey [Gol08]. Oedipus [Lav06].
O [AJO8, Coc02b, Oec03, Shi05, YLLL02, 
Bau05]. O-Line [YLLL02, Shi05, Bau05].
Oering [YC08]. Oce [Uni01].
ocer [Kov03]. Ocial [BP01b, Coc02b].
Oine [DJ06, ST01b, WV01]. Os [PS01c].
O-Line [SEF+06]. 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, KIO1a, KO03, 
KO00, LTW05, LDM04, MLM03, PV06b, 
P05, PLJ05b, RR02, Sh00a, Uni00a, 
Uni00b, Uni00f, Uni00c, Uni00h, YZ00, 
YKL02a, AGGM06, AGGM10, BYJK04, 
CCK04b, CHY05b, CJ04, CC05d, Di 03, 
DS02, GKK+07, HR07, HRS08, JZ09, KK07, 
KKK05, KK03, LW04, LPM05, LQ08, 
LC04a, Mic02a, Po00, SVDF07, SV08a, 
SW05, YW05, YRY05b, ZW05a].
One-Time [HM02b, LDM04, RR02, CCK04b, DS02, 
LC04a]. one-variable [SV08a]. One-Way
[BYJK08, CHL02, DMS00, Fis01b, GKK+09, 
HNO+09, HR05, KO03, KO00, LTW05, 
Sh00a, YZ00, AK02a, AGGM06, AGGM10, 
BYJK04, CH05b, CJ04, GKK+07, HR07, 
HRS08, JZ09, KK07, KKK05, KK03, 
LW04, LPM05, LQ08, Mic02a, Po00, 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, VY01]. OOSCD [CZB+01].
OOSD [CZB+01]. Open
[Bar00c, Bol02, Can06b, EP02, Gut00, Joh05, 
Kus02, Lin02, Mei01, PM00, VDKP05, 
An03c, ETMP05, McA08, Bar00b, Lin02].
Open-Ended [Kus02]. Open-Secret
[Joh05]. Open-Source
[Bol02, Gut00, McA08]. OpenCard [HF00].
Opening [CAC03]. OpenSSL
[Bau01c, Sta02b, TvdKB+01, Hos06a, Mos06].
OpenSSL [Fri01, Res01a, Res01b, Sti06a, 
VCM02, YRS+09, Bel08]. Operating
[BCST00, DGP07a, DGP07b, IE01b, SR01, 
CGL+08a, CGL+08b, CGL+08c, DGP09, 
KWDB06, MHPD06, SETB08, TKP+08].
Operation [BR02, BK07, Dwo03, EP02, 
Goli01, HSH+01, JKR01, KD01a, Bud00b, 
RBB03, Win00]. Operation-Centered
[BKM07]. Operational [WA07, GMG00].
Operations [BIP05, IMM01, KDO01, 
KS05b, LS01b, Ark05, Dug04]. operator
[Wan05]. Operators [CH00]. opinion
[BHM03, GS07b, Lan00c]. Opponent
[Cos03]. Opportunities [CWR09]. Optical
[Kuh02a, Pau02b]. Optimal [Bai01a, 
BDDS03, CH01b, CDF01, CF02, DPS05, 
DNP07, GMW05, IR01, KO04, KS03, LZ09, 
Man01, MPSW05, MP08, SNR04, YY01, 
vDW04, BCD06, HK00, LSH03a, LSH03b].
optimality [NK06]. Optimised [TL07].
Optimistic [CC00, DLY08]. Optimization
[Ken02a, Kre05, KV01, SMTM01, TLY04, 
WPP05]. optimized [LC03]. optimizing
[Dwi04]. Optimun [KWP06, OKS06].
options [Fri07, Pot03]. Oracle
[ABR01, Abe01, Abe04, BF05, Chi08b, 
Gra02b, Nie02b, Pas03, An02e]. Oracles
[BNP02, BB04, KG09, RG09]. Order
[AKS04, Bai01a, CV02, KCP01, KJC+01, 
Kra01, Luc02b, NNT05, NM09, Sty04].
52

Tad02, Zhe01, BF01a, Coh03, JZCW05, KS06b, QPV05. Order-Specified [Tad02]. ordered [HY03, WL05]. Ordering [Mea04]. Orders [HJW01, PS02b, HM00, Huh00]. Ore [CHH01]. Oregon [ACM00, BCDH09]. Organization [JG07, MP00, C02]. Organizational [FTP07, BJ02]. organized [AUW01]. Original [JQY01]. Originators [Cop04a]. Origins [Cop04a]. Orleans [USE00c]. Our [Sta05]. ourselves [Fur05]. Outbound [Smi02]. Output [Dic03, YJ00]. Outsource [HL05a]. outsourced [MSP09, MNT06, YPPK09, YLC09]. overcoming [CHC04]. Overdefined [CP02]. Overflow [FOBH05, Fry00, Ino05]. overhead [HGR07, IKOS08, RSP05]. overheads [XLSM06]. overlay [SL05b, YC08]. overlays [SK05b]. Overshadow [CGL08a, CGL08b, CGL08c]. overview [SVEG09]. Ownership [AS01b, Nik02a, Nik02b, CL08, Lin01a].

P [Puc03, AKS02, KR03]. P1363 [IEE00b]. P2P [BRTM09, STY07, WN02, YLR05]. P2Ps [LHL08]. PA [Cor00a, WWCW00]. PA-RISC [Cor00a, WWCW00]. Package [Win01]. Packed [HL07]. Packet [BR09, WRW02, WLZZ05, CMS08]. Pad [LD04, DS02]. Padding [AR01, BCCN01, CKN00, CJNI02, KO03, LS01a, Man01, Vau02]. Padding [NP02b]. PadLock [Lud05]. PadLock-wicked [Lud05]. Page [IEE00b]. PageRank [GPC08]. pages [Fal07, Rot07]. paging [SZ08]. Paillier [CGHG01, DJ01, NSNK05, ST02]. Pair [WCJ09]. Pairing [BKLS02, BF01b, BF03, CHSS02, GPS06, HCD08a, HCD08b, Kri03, PV06a, SKG09, Sma03a, GPS05, Lce04a, PC05b, VAVY09]. Pairing-Based [BKLS02, GPS06, PV06a, HCD08a, HCD08b, GPS05]. Pairings [Bon07, BGH07, Jou02, SB04, ZK02, CJL05, LWZH05, LC05b, SW05, VK08]. pairs [LYGL07, Shp01]. Pairwise [CLL00, FM02a, AMvIL07]. PAKE [HTJ08]. Palm [BDhKB09, WPS01, Wil99, Ano02d]. Palmprint [KZ09]. PAM [FR02, Sei00b]. Panama [BDPV09]. Panel [FL01b]. Panopticyn [YN01]. Paper [CC09, MFS09, Pet08]. Papers [Ano04a, Ano07b, Ano07a, Sch00b, Ytt06, Wil09, Bla03, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GH05, Joh03, Jue04, KKP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PK03, PT06, RM04, Sil01, AMW07, AJ01a, Bir07, BC05b, CZ05, CKL05, DR05, HH04, HH05, PC05a, PY05, WK06, Wri03]. Paradigm [BN00a, CS02, Go03, KDO4, YC01, BKN04, Can01a]. Paradigms [Des00b, Swa01, Hro05]. Paradise [USE00b]. Paradox [Che01b]. Parallel [AHRH08, App07, AEMR09, CPhX04, CTLL01, CNFP03, CNB02, Dam07, DM00b, JL08, KY02c, Lin01b, MFS09, PS04a, RMH03b, SS01a, BF06a, FP00, OS07, RMP08]. parallelism [KVN09]. Parallelizable [BR02, MG02]. parallelizing [Fis01a]. Parallelizable [LKKY03a, LKKY03b]. parameter [Wue09]. Parameterizable [KPM02]. parameterization [LZP04]. Parameters [ZLK02]. Parametric [Vir03]. Paranoian [Bau01a, Bau01b, Bau01c, Bau02b, Bau03a, Bau03b, Gua05, Oue05, Ste05a, Luc06].
Parascript [Ano02d]. Parasitic [ETZ00].
Parents [Pau02a]. Parents-to-Be [Pau02a].
Paris [ACM04a, GH05, KNP01, NP02a].
Parity [DRL09, KKG03, Yon01, BKW03].
Parity-Based [KKG03, DRL09]. Park
[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
[AO00, MSP00, Bao04, Fan03, HC04a, HY03,
HLL03, WL05, WLHH05, WY05, ZC05].
Participatory [CTBA01]. parties
[LKY05b]. Partition
[CTH08, WJP07]. Partitioned
[DN04]. partitioning
[BFO06a, Cle07]. partitions [Sav04]. Party
[KO04, Lin01b, MR01a, WW05, WV01,
CLOS02, CLC08, CDM00, CDG04,
FGM001, FWW04, GCKL08, HM01b, JW01,
LLL04, LLS09, LSH00, YCO09a, ZLX99].
Pass [SK00, MT02]. passe [Car00]. Passes
[Coc03]. Passing [Vin03]. Passive
[Sha01c, VV07, RW07]. Passive-Only
[VV07]. Password
[BMN01, BMP00, CHVV03, CPP04, CS07b,
DG03, GL03, GMR05, Har01a, Har01b,
Jab01, KOY01, LSH03a, LSH03b, MPS00,
Mac01, MSJ02, Ngu05, SBEW01, WHL05,
YS04, ZWCY02, CC01, CC04b, CCK04b,
CYH05, Fur05, GL06a, HTJ08, JM07, KLY03,
KJJ05, KTC03, KCL03, Ku04, KCC05,
KHKL05, LFW04, LCO04a, Sco04, Shi05,
YW04, YWC05, YSO2, YPKL08, ZDW06].
Password-Authenticated
[BMP00, DG03, KOY01, MPS00, Mac01,
MSJ02, Ngu05, HTJ08]. Password-Based
[CPP04, CS07b, GL03, SBEW01, YS04,
GL06a, KHKL05, ZDW06].
password-guessing [Shi05]. Passwords
[GL01, KOY01, Per03, Smi01c, Ano03c,
FZ06, KOY09, NS05a, RD09, vOT08].
Patarin [Bih00]. Patent [MP00]. Path
[GXT+08, CCD+04, Dew08, ZSN05].
path-based [CCD+04]. Path-quality
[GXT+08]. Pattern
[ABM08, BDiKB09, BLPO6, BCCN01,
LM01a, TIGD01, Buh06, LYGL07].
Pattern-based [BLP06]. Patterns
[DD02, MP06, WCJ09]. Pavol [Sal03b]. pay
[Joy03a]. pays-as-you-watch [Joy03a].
payload [KC09a]. Payment [MV01,
RMCG01, YKMY01, Has02, HP00, SH00].
PC [BSW01, Ste05c]. PCIXCC [AV04].
PCKS#7 [Dav01c]. PCPs [FS08]. PCs
[BDET06]. PDA [GW08]. PDF
[ISO05, CNB02]. PDF/A [ISO05].
PDF/A-1 [ISO05]. Pearson [Puz04].
Pebbling [DNW05]. Pedersen [GJKR03].
Peer [HR02, RH02, ATS04, LLY06,
MPHD06, PI06, WCJ05, YI04].
Peer-to-Peer [HR02, RH02, ATS04,
MPHD06, PI06, WCJ05]. PeerAccess
[WZB05]. Peinado [YNY05a]. PEM
[Dav01b]. Penguin
[Sha01b, Bau01a, Bau01c, Bau02b, Bau03a,
Bau03b, Gua05, Oue05, Ste05a].
Pennsylvania [IE05a, IE08]. People
[ASW+01, CG05, Lov01]. Perceptual
[PBM07]. Perceptually [EFY05].
Perfect [AJ08, CLO00, DO2b, DSS01,
Sun00a, DMO7a, SC02c, ZD05]. Perfectly
[DMS00, KSR02, SNR04]. Perform [Kin00].
Performance [ACM01b, BH00a, DPR01,
Dra00, EYCP00, FZH05, Int00, Ken02a,
Ken02b, Kra05, LWK00, MM01b, NFN03,
PWGP03, PBTW07, SSKS00, SW00a, SB01,
Sv06, SL00, SGPH98, WBRF00, WWCW00,
WS02, XH03, YEP06, ZEA00, AKNRT04,
BVP+04, BZP05, KCL+09, CRSP09, GC00a,
HM02a, JRB06, LWO05, NTW07, YGZ05].
performance-friendly [CRSP09]. periodic
[XQ07]. Periods [KKH03]. Perl [Sal03b].
Permutation [DMS00, HS0+01, IYK02,
KKG03, KO03, LSY01, DP02, IYK03].
Permutations [BPR+08, CHL02, KO00,
Persistent [AGT01, ST06]. Person [KJR05, LLT+04, PK01, BS01b, KN03, Li05, LST+05, PY08].

Personal [Bar05, EHMS00, SEK01, SEK02, Tyu05, UP05], personalized [GPC08].

Perspective [LL01]. Perspectives [BMV06, SM08]. Perturbation [HWH08, ZY08]. Pervasive [BDhKB09, JW05, LKHL09, Lut03, Lut03].

PET [MS05a]. Peter [For04, Uzu04]. Petersburg [GKS05]. petitions [Cal00b].

Petri [LKJL01, AADK05], PGP [McL06, Ano00h, BCH+00, Dav01b, Dav01c, JKS02, Luc06, Opp01]. PGPV [BRS02].

pharaohs [Pin06]. Phase [CDF01, Ig02, KLB+02a, Che07, Che08a].

Phase-Conjugate [Ig02], phase-shift [Che08a]. Phil [Bar00a]. Philadelphia [IEE08].

Phil [McL06]. Philosophy [Cop04b], phrasing [Be04]. Phone [CAC03, Fox00].

Photonic [TWNA08]. Photonic-based [TWNA08]. Photons [Bar00c].

Physical [CGMM02, LR07, YKL02a, GVC+08, UHA+09]. Physicist [BZ02], physici[RP00]. Physics [MYC01, Sch06b, BEZ00, BEZ01, Duw03].

Pi [OS08]. PIC [Fin02], pick [Cla00b].

Picks [PM00]. PicoDBMS [PBVB01].

PicoDMBS [BBPV00]. Picturing [Pau03].

Piecwise [LLL+01], Pigeon [Pem01b].

piling [Kuk01]. piling-up [Kuk01]. PIN [BZ03]. Pioneer [Coc03]. PIPE [CBD+05].

Pipe[MD05, Mis06]. PIR [BIM00].

Pirates [KY01d]. PISN [ECM00a, ECM00b]. Pittsburgh [IEE05a].

Pixel [LS08, WCJ09, BCD06, LYGL07, WWTH08].

pixel-pairs [LYGL07]. Pixel-Value [LS08, WWTH08]. PKC [BDZ04, Des02, Kim01, NP02a, Vau05a, IZ00, KI01a, KI01b, ZC04]. PKC98 [HPC02]. PKCS [Cha03, Man01, RSA00c, RSA00b, RSA00d, RSA00e, RSA01, RSA02, RSA03b].

PKCS#1 [CJNP00]. PKCS#11 [DKS08].

PKCS#7 [DAv01b]. PKI [AL06, CZ05, KGL04, Ahm08, ES00b, ES00a, Gar03a, Gut02a, Hoo05, NDJB01, Ort00, St.00].

PKIX [FL01b]. PKP [JJ01]. PKWare [Bar00a]. Place [USE01b, USE01a, GS07b, IEE09a].

placement [GJJ05, JEZ04]. Plain [Col03].

Plaintext [DN02a, Furt02b, GK05, HLM03, Jol01, Ke02, KM01c, KI01a, MF01, CKN06].

Plaintexts [BR00a]. Plan [CAC06, CGP+02, Gan08]. plane [WL02].

Planning [WCZ05]. plans [Ark05].

Platform [Bau02b, MMH02, PJDH09, ARJ08, ISTE08].

Platforms [AIK+01]. Play [WD01a].

Playing [Shp05, BR04]. Please [Per03].

Pluggable [Sei00b]. plus [Cop04b]. PODS [ACM03c, ACM05b]. poetry [MAaT06].

pogromca [Kap05]. Point [GLV01, M302, NS05c, USE00b, WW06].

point-sampled [WW06]. Points [BG08].

Poi[O02, Gau02, Cla00b]. poised [CH00].

Poisoning [Kle07]. Poland [AUV01, Bih03]. Polarization [HR05].

Poles [KS04]. Policies [AEV+07, ZP05, BNP08, LJS04, RN00a, RN00b]. Policy [Bla01c, HQ05, An000e, BFG08, BZP05, DFM04, Gor05, RVS09, Uni00b, RR04].

policy-based [BFG08]. policy-compliant [RVS09]. Polish [Kap05]. Politics [Ch08a, DL98, Jan08a, DL07].

polyalphabetic [GPG06]. Polygon [Ben00, BB00a, BGI08, SP04].

polymorphic [CSW05]. Polynomial [AF03, BIP05, BDG+01, Bul09, CU01, CJO3a, CH07c, CLZ02, DS05a, GOn06, HR00, KL05, KYY01c, KTT07, LW02, May04, Pl01, RMH03b, Sat06, LFV04, MRST06, SZP02].

Polynomial-Time [CLZ02, KLO5, Pl01, MRST06].

Polynomials [BLST01, DS08, FL06, Jam00, JJ00d, Lan04a, CHH01, FP09, GS09]. Pon [QCB05b]. Pool [BTTF02]. Popular
Port [Kra02b]. Portable [Hei07, Wan04a]. Portfolio [Ano02c].
Portland [ACM00, BCDH09]. Possessing [CC08]. Possession [Tee06]. Possibility [SF07, BGI01, DOPS04]. Possible [Mur01]. Post [BBDO9, BLRS09, Ber09b, HHG06, BBD09, BD08]. Post-Quantum [BBDO9, BLRS09, Ber09b, HHG06, BD08, BBD09]. Postage [Tee07]. Poster [TSO00, RN00b]. Potential [Kid02]. Potentially [Wal01]. POTSHARDS [SGMV09]. Power [AKS06, Ano00d, Ava03, BI05b, BNPS02, Cry00, DPV01, DBSt06, Gir06, Has01b, HM02c, HBF09, IIT03, JP02a, JQY01, KBBM09, KLY02, MOP06, Mas04, MS01, MMNT09, Mes00, Mes01, MG08, OS00, OS06, ÖOP03, PGS+09, Sha01c, Sma03b, WS05, WC01a, vW01, CBSU06, CO09, Geb04, Mit02, OS08, XH05, ZYW07]. Power-Analysis [ÖOP03]. power-attacks [Geb04]. power-aware [CBSU06]. Power-Sum [KLY02]. Power-Up [HBF09]. Pp [Eag05, Pag03, Top02]. PPC [ASW01]. PPK [YDKM06]. pq [KOMM01]. PQCrypto [BD08]. Practical [Ano01c, AR01, Ash03, ACJT00, BDK+09, BF05, BLMS00, CS03a, Cap01, CDR01, Chi08a, CS03b, DK01, Dr00, FS03b, GSS03, GIS05, GH02, HQR01, HJW01, Ina02a, Ina02b, IIT03, Kan01, LMV05, LCD07, Luit3, LWK05a, MM02, MS05, OM09, PBD00, Pel06, Poi02, Poo03, Roy00b, Sug01, Wei04, YSS+01, Bro05b, DKL+00a, Har05a, KSW06, Luc06, Mos06, MSV04, Sha01b]. Practice [AL06, BDZ04, Des02, IZ00, Kim01, Mao04, NP02a, PY06, SB07, Vau05a, YDKM06, KXTZ09, Sta02a, Sta06, Sti05, Sti02, Sti06c, Luit3, Spr03]. practices [Ste02]. practitioners [PP09]. pragmatic [BMW02b]. Prague [MJ04]. Pre [Adl03, AA08]. pre-processing [AA08]. Precise [Wal01]. Precision [HZSL05, SR06, LMC+03, MN14]. Precomputation [SLG+05]. predecryption [RSP05]. Predict [Dic03]. predictable [Bel08]. Predicting [AG09, BGPGS05]. Prediction [AKS06, SLG+05]. predictive [vOT08], predeletion [HMvdLM07, JRR09, TP07]. Preface [CGM07]. Prefix [FXAM04, RW07]. Prefix-preserving [FXAM04, RW07]. Prehistory [FHR00]. Preliminary [KS00b, KKS00b]. Prentice [For04]. Prentice-Hall [For04]. Preparations [FJ04]. Prepared [ASW+01]. Preprocessing [BIM00, CKK03]. presence [BIW08, GXT+08, Mi08, VS08]. Preservation [Che01b, Dur01, Bro05a, ISO05]. Preserving [HNT05]. Preservation [DN04, KS05b, LP00, Mö03a, YWD08, AKS04, BR06, BSSM+07, BA06, FXAM04, GA03, HJW05, LCK04, Pin02, Pin03, RW07, HJ07]. President [Gen00a]. Press [Imr03, Kat05b, Pag03, Puc03, Rot07, Top02, Spr03]. Pressure [HWH01]. pretty [vOWK07]. Prevent [FOBH05]. Preventing [CS07b, CCL09, HSW09, IY05, RG05, DMS07]. Prevention [JT05, PZ01, PZ02a]. Price [AS01a, BRA01b]. Primality [BT02, Che03]. Prime [ACS02, BAI01a, Har07a, Pan02a, WS03, JL03, dW02]. Prime-detecting [Har07a]. Primer [KLB+02b, Lad06]. Primes [Ano03d, SZ01, HLLL03, Ste08, AKS02]. Primitive [CFS05, IY02, IMM01, ST01a, ST02, IYK03]. Primitives [BDFP02, CHL02, FGMO01, Ngu05, RR00, BDFP05, Gar05, JZCW05, RAL07]. principal [ZL04b]. Principle [CZK05]. Principles [ACM03c, ACM05b, DK02, DK07, KLO8, MAA07, SB07, Sta02a, Sta06]. Print [Kra02b]. Printed [SLT01]. Printer [Bar00a]. Priority [WWL+02]. Privacy [An00i, AEV+07, BBDO1, BSSM+07, CDM+05, Cho08a, DL98, DL07, DFKX05, DN04, GSO2a, GMM08, HY01, KS05b].
Knu07, LP00, Pap05, PBD05, PP06b, Por06, PGT07, RW03b, RK05, Ros07, Sal03a, SE09, Tom06, YWD08, Bel04, Bjo05, BA06, Bra01a, CLR09, CKN06, HJW05, JRS09, KXTZ09, LL05b, Lev01, LCS09, NS05b, Pin02, Pin03, Ros06b, SIR04, Tyn05, WK05, ZYLG05, ZSM05, MS05a, Jan08a].

Privacy-Enabled [Por06].

privacy-enhanced [ZSM05].

Privacy-Enhancing [SE09].

Privacy-Preserving [DN04, KS05b, YWD08, BA06, HJW05, Pin02, Pin03].

Private [AF04a, AFI06, BDF01a, BIM00, BY03, BSW09, BJLS02, BGW05, ISW03, KO00, OS05, SDMN06, ST01c, Wal03, Yek07, BD00b, Cal00b, HLLL03, KY00, KPS02, PLJ05b, Sun02, YRS*09, ZY08, ECM00a, ECM00b].

Private-Key [BY03, KY00, PLJ05b, Sun02].

prize [Fox00, Coc02b, MNT00].

PRNG [HSS04, Mur02, SF07].

Proactive [DBS01, FMY01, JS05, ZSV05].

Probabilistic [CCW02, CPD06, DJ01, DJ06, Kuh00, Lee03b, CP07, DLMM05, Go99, JZCW05, KY00, MRST06, PBMB01, dh08, Neu04].

Probability [KMT01, MNT00, DLP09].

Probing [ISW03].

Problem [AL00a, AF03, Cap01, CU01, Che04b, CJ03a, CGK+02, Cou01, CLZ02, DIS02, DHR00, FLO6, Gen03, GV05, GPP08, KK02, LNS02, NBD01, Wag02, BKW03, CGHG06, CJT04, DLMM05, HGN03, Hua05a, LHY05, LD01, Luk01, Pei09, Shp05, SCL05, WL02, Whi09, Yas08, KM04a]. problem-solving [Whi09]. Problems [B105a, Can06b, MV03a, OP01a, TvdKB+01, VDKP05, HL05d, KX00, LMTV05, LMC+03, RSS04].

Procedure [LY07]. Procedures [DJ06, BBK+03b]. Procedings [AC00, ACO02, ACM04a, ACM05a, AAC+01, Bon03, EBC+00, FMA02, FLA+03, SM07b, USE00c, USE00b, USE00a, USE00d, USE01b, USE01c, USE01a, USE02a, USE02c, USE02b, WK03, Yun02a, ACM05c, ACM07, ACM08, ACM09, AUV01, AJ01b, BS03, Be00, B+02, Boy01, Bu00a, BC01, HA00, Hon01, IEE00a, IEE01a, IZ00, Kil01a, MS05b, Oka00, PPV96, P601, Pre00, Q500, RD01, Roy00a, SMP+09, ST01d, VY01, ACM01a, ACM03a, ACM03b, ACM03c, ACM04b, ACM05b, ACM06, ACM10, AL06, BZ04, BS01b, Bih03, BCD09, BD08, CC04a, CV04, Ch00, Des02, DFPS06, FLY06, Fra01, Fra04, HR06, HYZ05b, IEE02, IEE03, IEE04, IEE05b, IEE07, IEE08, IEE09b, JY04, Jef08, JM03, Joy03b, JQ04, KJ05, KGL04, Kim01, Kim02, KN03, Knu02, KP01, KN01, KM07, Lai03, Lee04b, LLT+04, MM06, MJ04, May09, MS02c].

Proceedings [Men05, Nac01, NP02a, Nao04, Oka04, Pat03b, Pre02c, RS05, Sch01d, Sma05, Syv02, TB02, Vau05a, Won01, YDKM06, ZJ04, Zhe02b, ZY03, BCK05, Cra05a, DV05, DWML05, DKU05, GKS05, IK05, Kil05, Li05, LST+05, Men07, Poi06, Sho05a, Sun00, dCdVSG05]. Process [Kwo03b, MNT+00, BDFP02, HL06, MRST06, VKS09]. Processes [BDP02, ALV02, BDNN02, WH09].

Processing [ISSZ08, KLB+02b, PCK02, AA08, AA04a, YPS01]. Processor [Ane02e, BBGM08, EP05, FBW02, FZH05, GC01b, Int00, KBD03, KPMF02, TYLL02, ST03a, SHL07].

Processors [TLYL04, CW02, CRSP09, Geb04, LJO5a, YGZ05, YLT06, ZYLG05]. Procurement [Lad06].

produce [Zir07]. producing [SO1G70]. product [KSW00, Sun02].

Products [AC02, Ane02d, Ane02e, Knu07, Ane00c]. professional [Dew08, vT00]. proficiency [Dew08].

Profile [PJK01, RGA00]. Profiles [MV01, PJK01]. Program [Hö01, Bec02, GG0+08, Kok03, KHO3, CS08b].

Programmable [Dam07, GC01a, HV04, SMI02].

Programmer
Programmers [Coc01a, We04, Gou09]. Programming [ASW+01, An02d, Coc03, LMHCETR06, 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, MWM01, Sha01a, Coc01a, Coc02b, IY00, Pre02b].

projects [Gha07].

Prolog [Bla01a, Bla01b].

Promise [An02f]. promises [Pau02a].

promote [WK05]. Promotes [Bar00b].

Prone [MLC01].

Proof [Abe01, Abe04, AS01b, ARC+01, BDP02, Cor02, GKI05, SOIG07, SPML02, Tee06, BR05, GM04, HSD+05, LMW05, PBD07].

proof-of-compliance [LMW05].

Proof-of-Concept [ARC+01].

Proofing [CT02].

Proofs [BBM00, BP02, CS02, DFS04, DNW05, Fis05, Gen04a, KL05, Lee03b, MV03a, Nie02b, BGB09, BR04, GoI99, HG05b, SV08b, dH08].

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

Property [LPZ06, Qu01, Uni00b, 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, DKF05, ECG+07, FBWC02, MV01, MG08, PP06b, Rot01, SS01b, VHP01, WY02, XFZ01, ZTP05, CL08, CGL+08a, CGL+08b, CGL+08c, CT02, Gor05, K03, KH03, Kwo03a, LL05b].

Protections [JT01a]. Protocol

[An01a, Bel01, BPST02, BL02, CK02a, CJ03c, CWY05, Cim02, ECM00b, Fre03, GJKR03, GL00, HS07, J02b, JRFH01, JT05, KLN+06, Kak06, Kra05, Ku02, LCK01, Mea01, MS05, NS01b, Rub00, RMCG01, SK00, Tan07b, TZT09a, TZT09b, WHL05, YSR01, BP03a, Bla01b, BDFF05, BK05, CS04, CCK04a, C04b, CY05, CC05c, CYH05, Che04a, CL08, CJ03b, CJ04, CL09, CJL05, DP04, GM04, GTZ04, HT08, HWW03, HHC05, KH08, KKL09, KTC03, LC03, LF03, LKK03a, LKK03b, LW04, LHL04, LKY05b, LKY05c, LHC08, LHS03a, LC05b, Luk01, MS03a, Par04, Pau01, RG06, Shi05, SW05, SIR04, TM06, Ts06, Tse07, WK05, WLT05a, WHHT08, YW05, YTYY05, YC09a, YS02, YS03, YRY05b, YRY05c, YPKL08, ZW01L, ZL04c, ZDW06, ZYW07, LSH03b].

Protocols [AADK05, AL00a, AAFG01, BP04, Bla01a, Bla02a, Bor01, BM01N, BM03c, Bra01b, BLDT09, CKPS01, CT08a, CCMR02, CCMR05, C01, CNV06, DJ06, DFG01, Fis01b, FGM00a, GMP01a, GMV01, Gor02a, JP07, JW05, KS00a, KY03, KL08, Kra03, Ki02, MS02a, MNP01, PBD00, PR08, PJDH09, Rot01, Shy02, SC01, Tee06, AA04b, AKR04T04, Bar06a, Ban05, Bell07b, BDSV08, BFGT08, BP05, BL06, BD04a, BR05, Can01a, Can06a, CP07, CKRT08, CWJ01T01, CH07a, Cho08b, Chr00, Chr01, C00M0, Coh03, CC05d, CDL06, DFG00, GJ03, GJ04, GU0Q01, Gut04c, HM02a, JW01, KS05a, LPV+09, LL04, LL06, LLS+09, Mea04, MT07, MRST06, Mon03, MP07, PR05, PQ03a, PQ06, Puc06, SY08a, SL05a, SR00, SW00b, YS04, ZLX09, ZL04b, PDM09, Puc03].

ProtoMon [JT05].

Provability [GOR02]. Provable [HM02b, HLL+01, HSL+02, KSH01, PBD05, SLL+00, BGP09].

Provably [AO00, ACJT00, BPM00, BCP01, BCP07, CHKO08, DG03, HLAV02, HVAL09, HL07, HS07, JM02V, M013a, NS0K05, NSS02].
VMSV05, XS03, ZCL05, BKN04, CCMT09.
provenance [HSW09]. Provers [MV03a].
Provide [AB01, Sch01a]. Providence [IE07, Si01]. Provider [LDM04, HILM02].
providers [MV03b]. Provides [OT03b].
Providing [BACS02, BDS+09a, DeL07, Lin07, Par04].
Proving [Che03, FS01c, GNO1, Tce06].
Provision [ Khan05]. Proxy
[AH05, BCL05, DFKX05, LCK03, LCZ05b, PL01, RdS01, Sha03d, ZJ09, AF06, AFG06, CCH04, DYO9a, HW03, HW04, HW05, HW05, HC04b, KHL09, LL05b, LH05, LCZ05c, LW05c, PKH05, Sha05b, SHT05, TYH04, YTH04, ZCL05].
proxy-enabled [DY09a].
proxy-protected [PKH05, ZCL05]. psBGP [vOWK07].
Pseudo [BH05, FFW04, Gen00b, LLL+01, LHL+08, MP03, SYX01, TZ09a, TZ09b, WP03, BG09, GB09, MKF+06, NR04, PSP+08, RX06, SL09, WW08, YZEE09].
Pseudo-Random
[LLL+01, MP03, WP03, Gen00b, SYX01, MKF+06, NR04, RGX06, SL09, WW08].
Pseudo-Ransom [BH05].
Pseudo-signatures [FFW04].
pseudo-noise [HG05a]. pseudonym [CG06].
pseudoprimes [ZT03]. Pseudorandom
[CD05, DN02a, DI05, DP02, Fin06, Fh02b, FIPR05, GM02a, IYK02, LMHCE06, Nie02c, RSN+01, Aam03, BGPG05, IYK03, KS00].
Pseudorandomness
[GM02c, IK00, IK01, KYHC01, LL01, Lee03b, MV00, Shp03, Go99].
Psychology [MYC01]. PUB [Nat0]. Public [ANS05, AUW01, APV05, An01j, EA05, AF03, BC05a, BDC+01, BDZ04, Bar0c, BPS00, BBM00, BBPD01, BLM01, Bhi00, BDTW01, BST02, CHK03, CHK05, CDM+05, CHM+02, CHK008, Chi08a, CCW02, CT09, CCM01, CS02, CS03b, DPV04, DJ01, Des02, DYO9b, DFKX02, DF+03, ESG+05, ES00a, ED03, FL06, FL01b, GML02, GH01, GC01b, GSB+04, Gut04b, HCOD02, HR05, HG05b, HR04b, HJ01, HLC08, IEE00b, IZ00, Jou02, Kat05b, KKM01, KM01a, Kim01, KLY02, KKY02, KYS02, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KOM01, KY01, Kur01, LLL02, LP03, LV00, Len01, LPZ06, Lin03, Lin00b, MR01b, MR01c, Ml03a, Mol03b, Ml01a, NP02a, NBD01, NSS02, OT00, PHK+01, Pei09, P01, PHM03, Qu01, RSA00a, RKKD02, ST01a, ST02, Sin01a, Sin01c, Ste01, TSO00, TT01, Vau05a, WZ05].
Public [WH01, WV00, Wy02, WKMA01, YGO1c, YDKM06, Zhe02a, AG09, BMH03, BCL05a, BCW05, BBN+09, Ben01a, BB01, Bra01a, BD04b, Ca00b, CCT08, CL02b, CWH00, CCH05, CJ05, CKRT08, Cho06, Cre00, DMT07, EKRMA01, EKHK04, FMY02, FP00, Ga02, G08, GKM+00, GS01, Gor05, GM01, HCD08a, HCD08b, HH06, HW04, HL04, Iwa08, IM06, Jan08b, JXW05, JZCM05, KPS02, Kon00, KW00, Kos01c, LF03, LKY05b, LC04, LL00b, LS01c, Lop06, LW05a, MWS08, M01b, PI06, PC09, SN01, SRJ01, Sha04b, Sha05b, Shp04a, SLC05, Sun00b, SZP02, SC05c, TO01, TLH05, Tsa05, TJC03, VS01, WDL09, W00, Wu01, WH03, WL04b, hY08, YRS+09, ZSM05, AL06, BDZ04, Ben02, C05, D02, GL05, KGL04, Kim01, NP02a, Vau05a, YDKM06]. Public-Key
[A001j, EA05, BC09a, BMM00, BBPD01, BLM01, BST02, CHK03, CHK05, CCCM01, CS02, CS03b, DPV04, DJ01, DF+03, ESG+05, ES00a, FL06, GH01, GC01b, HR05, IEE00b, Kat05b, KK01, KM01a, KLY02, KKY02c, KLC+00, KI01b, KM04b, Kos01a, Kos01b, KY01, Kur01, L03, Lin03, Lin00b, MR01b, MR01a, Ml03a, Mol03b, NSS02, OT00, P01, RSA00a, ST01a, ST02, Sin01a, TS00, TT01, WH01, YDKM06, AUW01, ED03, HG05b, Pei09, BMH03, BBN+09, BD04b, Cho06, FMY02, FP00, GMW01, HCD08a, HCD08b, HH06, Iwa08, Jan08b,
Public-Key-Based [YKMY01].
Publication [Top02, DGMS03].
Publications [Bee05].
Publish [SL05b].
publish-subscribe [SL05b].
Published [MS03b].
Publishing [Ano02d].
puce [Car00].
PUFs [MKP09].
Purpose [Ano07b, Ano07a, ESG +05, GS07a, GPP08, SGK08, LJ05a].
Purposes [LS05a, FSGV01, PBV08].
Push [Pau03].
puzzle [LF03].
Puzzles [ANL01, CHS05].
Q [BFMR02, CH01b].
Q&A [Str01b, Win01].
QCQC [Wil99].
QCQS [Wil99].
QDSL [CUS08].
QNX [Ano02d].
QoS [JKRW01, Zea00].
QoS-aware [Zea00].
QSIG [ECM00b].
QSIG-WTMAU [ECM00b].
Q'tron [YC07].
QUAD [BG09].
Quadratic [BT02, Coc01b, HJW01, SP05, CCS08, HM00, Hiih00, HP01, LD01].
Quality [BW07, TL07, DMSW09, GXT +08, KC09a, WWTH08].
quality-conscious [DMSW09].
Quantifier [KS06b].
Quantifier-free [KS06b].
Quantitative [Bai08, ME08a].
Quantization [DRL09, WC04].
Quantum [AC02, ATSVY00, An002f, An002g, An002h, BYJK08, BOHL +05, BBD09, BZ02, BBB +02, BB03, BLMS00, BEM +07, Coc03, DFS04, DPS05, DFSS08, DMS00, Elij04, Ett02, GKK +09, GH02, GW00, GRTZ02, HV09, Hay06, Imr03, Ina02a, Ina02b, Kak06, KK06, KLB +02b, LB04, LW05b, NA07, OTU00, PC09, Rec01, RK05, Ser06, SR07, TO01, Wil99, Wri00, YI01, YI01, ZL02, ABW09, An003e, An006d, BYJK04, BCG +02, Ber09b, BEZ00, BEZ01, BLRS09, DFSS05, Duw03, Eke02, GKK +07, Gav08, HHC06, IM06, JZ09, JRS09, JAW +00, Joy00, KK07, KH08, KKKP05, LQ08, May01, NK06, Pin06, RP00, Sin99, Sin00, Sm004, UHA +09, BZ02, BD08, BBD09].
quantum-storage [DFSS05].
quarter [Ko00].
quarter-century [Ko00].
quarters [CLA00b].
QUARTZ [PCG01].
Quasi [MD05].
Quasi-Pipelined [MD05].
Quasigroup [MSNH07].
Québec [ACM02].
Queen [Rec01, Sin99].
Queens [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].
radar [GG05b].
Radiations [SGM09].
radical [Web02].
Radio [Sak01].
RadioGatún [BDPV09].
Radix [HKA +05, JY01].
Radix- [HKA +05, JY01].
rails [Fox00].
Rainbow [DS05a].
Raises [MP00].
Raising [Cos03].
ramp [IY06].
Ramping [Coc02b].
Random [Abe01, Abe04, BST03, BK06a, BF05, BB04, BL08, CHTY09, Chi08b, Dic03, DGP07a, DGP07b, DVO8, EHK +03, Gra02b, GPR06, HSR +01, HBF09, Int03, JRR09, Kel05, LLL +01, LM02, Lys02, MP03, Mir02, NNT05, Nie02b, Pas03, Pat04, Ran55, Ran01, RSN +01, SFDF06, TWNA08, TL07, Tip27, TYZT09a, TYZT09b, Vav03, VKS09, WP03, BK07, Bel08, BG08, BG09, BG07a, BGL +03, CJL06, CO09, DG09, Fis01a, GVC +08, Gen00b, GB09, HG05a, HLWZ09, HMvdLM07, JAW +00, KH08, KB39, KG09, MI09, MKF +06, NR04, Pan07, PIS +09, PSP +08, PC00, Reg05, Reg09, RG09, RGX06, SS03, SYX01, SR07, SK01b, Sug03, SL09, UHA +09, WW08, YZEE09, BH05].
Random-Error [LM02].
random-self-reductions [Fis01a].
Randomats [Sam01].
randomization
randomization-enhanced
Randomness
[DD00, DD04, DGH04, FWW04, Gen06, HSS04, JG01, KLR09, Kos01a, Kos01b, MT02, SB00, Sun00a, BBN09, DOPS04, Kat05a, KW00, RSS04, SU07, Sut03].
Range [CW09].
Rao [ZYR01].
Rapid [OP01b].
Rate [KT01, LZ09, PS02a, Sun02].
Rates [GH02].
Ratio [Di01].
Rational [HT04].
Ratios [Zir07].
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].
Red [BSW01, Dri02, GSB05, JBR05, SP05, Sta05, YKMB08, GM04, HP01, Li05, SL07, SGPH98, YZDW07].
Real-Time [Dri02, GM04, YZDW07].
Reality [Coc01a].
Really [CZB01, Wei00, Dav01c].
reap [CH00].
reason [Lau08b].
reasoning [IK03].
Rebalanced [SWH09].
Rebalanced-RSA [SWH09].
rebels [Lev01].
Rebuild [Salxx].
Rebuilding [Sal05a].
Receipt [HS00].
Receipt-Free [HS00].
Receipts [Cha04].
Receive [Coc03].
Receiver [CCD07].
Recovers [NNL01, SBB05].
recency [SW02].
recently [JK01a].
Recipies [VM03].
Recipient [ANR01, Kur01].
Recipients [Coc01a].
recoding [SSST06].
Recognition [Ano02d, LLT04, LST05, TZT09b, HS02b, Li05, MMJP03].
Recommendation [Bar06b, BK03a, BK07, Dwo03, NIS03b].
Recommended [Keo05].
Reconciling [BNPW03, PGT07].
Reconfigurable
FD01, FZH05, GC01b, KBD03, LZ04, MKP09, MMH02, SJT09, SKG09, SRQL03, CMS08, DHL06, GC00a, HBC08, Rhi03].
Reconfiguration [PBTW07].
Reconsidered [Sho01].
Reconstructing [CDF01, FL06, PS01a].
Reconstruction [AF03, CF01b, CDF01, JJ00d, KY01c].
Records [Dur01].
Recoverable
[NZCG05, NZS05, SGMV09, YY00].
Recovery [BDK02b, CM05, CS05c, FKSW00, HQ01, HSR01, KSS00a, KSS00b, KSS01, KML02, KM01b, KSS00b, MHL02, NP01, STK02, SK01, YSD02, CV05, Kuh01, SK01a].
Reduced-Round [FKSW00, KSS00a, KSS00b, KSS01, KML02, NP01, YSD02, CV05, Kuh01].
Reducibility [DM00b].
Reducing
[AL07, BIM00, SPHH06].
Reduction [CM05, CH07, Dhe03, Gro01, HG07, Kid02, PG05, AL02, HG07, SUN03].
reductions [Fis01a].
Redundancy [AB01, BR00a, FM02b, YLR05].
Redundant [MF01, Tan07a, PS04a].
Redwood [KKP02].
Reed [KY02b].
Reference
[BR09, CPS07, Pas03, RS00, Sal07, vT00].
Reference-Watermarking [BR09].
Refined [Sma03b].
Regarding [GMP01a].
Regexp [BTTF02].
Region [BSNO00, Bur00].
Region-Based [BSNO00].
register [HTW07].
Registers [CGFSH09].
Registration [HLM03].
regression [mSGFL05].
regulations [Ano00g, Cha00b].
Rehearsal [Ahm08].
reinforce [SWR05].
Rejewski
[BCB05, Kap05].
Related
[BD06a, Can06b, CY08, FKSW00, Kil01b].
KLML05, Sat06, Buc00a, Gutxx, HAU04, Hen06a, Sch00b. Related-Key [FKSW00].
Relation [ABC05, NN06]. Relational
[AK02b, AHK03a, AHK03b, CKY07, GA03, PT08]. Relations [BN00a, Pan01, Uni00a, Uni00f, Uni00e, SP03, Zha08]. Relationship
[Ngu05, GKM00]. Relationships [AK02b, AHK03a, AHK03b, CKY07, GA03, PT08]. Relative [JRS09, Mul01b]. Relaxing
[CKN03, PS05]. Relaxing [DKMR05, SKU00].
Relay [DM07b, Zha00]. Release [CHKO08, Mao01, HGNS03]. Released [Bar00c, Ano01g]. Releases [Bar00c, AJ08]. Reliability
[IKP07, WK05]. Reliable [JR03, MPH06]. reloaded [SL06].
Remainder [Sch01b, YKL03]. Remarks [BCW05, CL04d, SC05c]. remedy [FZ00]. Remember [HSH08a, HSH08b, HSH09].
Remote [CWR09, Kra02b, LL05c, Rub01, TK03, WKB08, CC01, CL04d, GT01, Hsu05b, HL05b, KC05, LHY02, LLH02,
LKY05a, LHL03b, LC05a, SZS05, WLT05a]. remotely [Küh08, SL06]. Removal [LL05a]. Removing [JL00]. rencontres [PP96]. Renewable [TOE00].
Repairing [DKFX05, GMM0b, HL04, ZJ09, BKN04]. replace [Gav08]. Replacing [FZ06, KAM08]. replication [BIW08].
Reply [WLW04]. Report [DFG01, Pen01b, Pre01, Sal01a, Sha03b, BCH05].
Repository [Bar00b]. Representation [BJvdB02, FS01, JLM03, JY01, RN00a, RN00b, ZL0K2, BDS08, BA06, PS04a, SWR05]. Representations [OSSST04]. Representative [CTBA01].
Representatives [Uni00a, Uni00b, Uni00f, Uni00e, Uni00h]. Republican [MJ04, dL00]. Republiek [dL00]. repudiation [HLL04, LSA07, SC05c]. reputation [KNS05, RCG05]. reputation-systems [KNS05]. Request [RSA00b]. require [SV00b]. Required [Sun00a, Lov01, Wan05]. Requirements [FIP01b, HWH01, Kin02, NIS01b, Mea04].
Rescue [ASW01]. Research
[AJ01b, CZ5, CZK05, DFP06, KGL04, LXM05, RC06, Sch00e, TAMM05].
DFC00, JXW05, MH09, QSO00, dCdV005]. Researchers [Ano08b, Ano08c, Pan02b].
Resettable [DFV04, MR01b]. Residue
[TIG001, YKL02b, CNP03, FP00, LD01]. Residues [Coc01b, Zhe01, CCS08].
Resiliency [JH00]. Resilient [Che01c, DSS01, DFK03, DP07, DP08, GSS08, KZ07, SM00a, KZ03, IR02]. Resist
[HM02c]. Resistance
[HNZ02, M61, EBS01]. Resistant
[Ano01c, ACJT00, ANL01, BGW05, CDT05, CN06, Gir06, IK05, Lrr05a, LWS05, LT00, LNL08, KS09, PC09,
WL04b, YS02, MS09c]. Resolution
[SAM09]. resolving [Lin01a]. Resort
[USE00b]. Resource [MR01]. Resource-Constrained [MR01]. resource-limited [Tse07]. Resources
[Gutxx, FOP06]. Response
[JBR05, LW05a, XNK05].
Responsibilities [Vix02]. Resting
[GTT02a]. restricted [ASW00]. Restriction
[CTH08]. Restudy
[FZL08]. Results
[APV05, GM02c, OOP03, RR08, Way02a, YRS09, CV05, MK08, DM07a, GM00, PM08]. Rethinking
[Bra01b, KZ03]. Retreat [FKSW00]. Retrieval
[BIM00, KO00, RE02, Yek07]. Retroactive
[DBS01]. retrofitting
[CGL08a, CGL08b, CGL08c]. reunion
[LAB00]. Revealed [Gal03]. Reversal
[Cap01, DIS02]. Reversal-Bounded
[DIS02]. Reversals
[MS02e]. Reversal
[Coo02, EC05, Wue09]. Reversed
[Ina02b]. reversibility
[KC09a]. Reversible
[Gal03]. Reversing
[EC05, YWC08, YN01, CDF05]. Review
[And04, Ano02b, Du03, Eag05, Fal07, Gas01, Gum04, Inr03, Irw03, Jan08a, Lee03a, Lee03b, Mar05a, Pag03, Pap05].
Puz04, Ree01, Rot07, See04, Spr03, Ter08, TvdKB+01, Top02, Uzu04, Was08a, Kat05b, Lu07, MP01b, Nie02a, Nie04, Puc03, Shp04a, Wal00. **Reviews** [For04, Kid00, Sal03b, Sty04]. **Revised** [Bla03, BC05b, Chr01, CCMR02, CCMR05, CSY09, CGP03, DR02c, GS02e, GH05, HH04, HH05, Jhe09, KPP02, KCR04, LL03, LL04c, MS05a, Mat02, MZ04, NH03, PC05a, PK03, PT06, RM04, Si01, Ytr06, AMW07, AJ01a, BK07, Bir07, C505, CKL05, DRS05, Irw03, PY05, WK06, Wri03]. **Revisited** [ABC+05, Ano02h, BM01b, CDMP05, Knu00b, NS05c, OSSST04, Hes04b, ZZT05]. **Revisiting** [AEAQ05, Har01a, Har01b, JMV02]. **Revocation** [Bor00, Con00]. **Revolution** [CMB+05]. **Rewriting** [Cir01, HR04a]. **RFC** [BWBL02]. **RFID** [And04, AL07, ACdM05, BLDT09, CCS08, CH07a, CL09, FW09, FM03, KKJ+07, OS06, Ros06b, SE09, TZT09a, TZT09b]. **Rhee** [Kuh08]. **Rhode** [IEE07]. **RI** [Sil01]. **Right** [Dhe03, GS07b, HkPR05]. **rightful** [CL08, Lin01a]. **Rights** [Bar00a, BNPW03, Dre06, Scro01, Wya02, BA06, UP05]. **Rijndael** [BB02, MP01a, SKU+00, Wer02, CCK+02, CGBS01, DR00a, DR00b, DR01, DR02b, FKS+00, FKL+01b, FKL+01a, FSW01, FD01, GM00a, JmBdXm05, KY01b, KMT01, KV01, Luc00, MM01b, MMH02, PSC+02, RDJ+01, SMTM01, SRQLO3]. **Rijndael-Like** [PSC+02]. **Ring** [BSS02, Na02, WBL01, ZK02, Her07]. **Rings** [BLST01]. **RIPEMD** [DG02, WFLY04]. **RISC** [Cor00a, Gro03, WWCW00]. **RISC-Based** [Gro03]. **Risk** [WA07, Vo05]. **Risks** [ES00a, Kuh02a, Ros07, Bel04, BJ02, ES00b, Jan00, MN03, Pvs01, Sch00c]. **Rivest** [BB79, Coc03, Sp79]. **RMI** [JRB+06, Mar02a]. **RNS** [BI04, BKP09, NMSK01]. **Road** [BDP09, HR04b, PB01]. **Roadmap** [Coc02b]. **Roaming** [Coc03]. **RFID** [And04, AL07, ACdM05, BLDT09, CCS08, CH07a, CL09, FW09, Fin03, KKK+07, OS06, Ros06b, SK01a]. **Rijndael-Like** [PSC+02]. **Ring** [BSS02, Na02, WBL01, ZK02, Her07]. **Risks** [Bar00a, BNPW03, Dre06, Scro01, Wya02, BA06, UP05]. **Rivest** [BB79, Coc03, Sp79]. **RMI** [JRB+06, Mar02a]. **RNS** [BI04, BKP09, NMSK01]. **Road** [BDP09, HR04b, PB01]. **Roadmap** [Coc02b]. **Roaming** [Coc03]. **RFID** [And04, AL07, ACdM05, BLDT09, CCS08, CH07a, CL09, FW09, Fin03, KKK+07, OS06, Ros06b, SK01a]. **Rijndael-Like** [PSC+02]. **Ring** [BSS02, Na02, WBL01, ZK02, Her07]. **Risks** [Bar00a, BNPW03, Dre06, Scro01, Wya02, BA06, UP05].
CFS05, CDG^+05, CDI05, Di 01, DKL00b, DS06, DN00b, DP07, EHMS00, FM02a, FS02, Fis01b, Gal03, Gas01, Hoe01, HR05, HR04b, Jun06, Jo05, JLL02, Kah67a, Kah67b, Kah69, Kar01, Kin02, Kog02, KS03, LD04, LT04, LM02, May04, MN01, NABG03, NN06, OKS06, PZ01, PZ02b, PZ02a, RW03a, RW03b, RST01, Sin01b, Sin00a, TL02, Top02, TC01, UW00, Ver06a, Wri05, ZYR01, ZP01, vW01, AEEdR05, Ano02c, Ano08c, Bam02, BCB^+05, Cal01, CDD00, DD04, DB04, DM00a, Di 03, DW01, Duj08, FNRC05, FZ06, Gal02, GIKR01, HT04, HJ07]. secret [HKS00, IY06, Kee05, KB09, Lam07, Lun09, MF07, Mi09, Naf05, PS02a, PW05, Ris06, Sch01e, SBZ04, SC05a, Smi01b, SC02c, Wan05, Win00, YCH04, ZSV05, dRMS05, vDKST06, Hil06]. Secret-Ballot [Cha04]. secret-code [DW01]. Secret-Key [HR05, RW03a]. Secretly [CC08]. Secrets [BH06, BBD^+02, CMS09, CP07, Cop04b, Di 01, Gum01b, Gum04, KMS05, LKM^+05, Lys08, Pag03, Puz04, Sch00d, Swa01, Tee06, TEM^+01, VGM04, AGKS07, Ano03b, Ano08b, Bam02, Bau00, Bau02a, Bau07, Cop05, Cop06, DM07a, Di 03, DW09, EC05, FS04, GD05, MKS03, Pan01, Ste08, TCC02, DLMM05]. Section [An004a, Ano07a, BK06b, SGK08, TL02, KP03]. Sector [Cro01, MV01]. Secure [AR00, AO00, AF04b, AG01, AP09, Ano01k, ACJT00, AFI06, BDF^+01a, BST03, BCL^+05b, Bar03, BI05a, BPR00, BMS03, BB04, BMP00, Bra01b, BCP02b, BG07b, CC00, CKPS01, CM00, CG06, CK02b, CHK03, CHK05, CG08, CW07, CG01, CHJ^+01a, CHJ^+1b, CDM00, CD01a, CS02, CS03b, CDG^+05, CDI05, Des00b, DG03, DM00b, ES00b, FGMO01, FB01, FP01, FOPSO1, GPC08, GIKR02, GJ03, Gen04a, GD05, HSZI00, HSZI01, HSIII02, HSH06, HRS02, Har07b, HKW06, HLV02, Hvl09, HR04b, HL07, Hut01, HLC08, IR01, It000, IFH01, JH00a, JH00, JVM02, KMM^+06, KY01a, KO04, KLML05, KC02, KH05, KKL09, K01b, Kos01a, Kos01b, Kra01, Kra05, KSR02, LCK01, LLL02, LCK03, LWK00, Lin01b, Lin03, Lin02, MKP09, Mar02a, MAR07, MV01, MLO03a, MJD01, NMO05, Nan02, Nd05, NSNK05]. Secure [NSS02, OKS06, OKE02, OT03b, Opp01, PS08a, RV09, R0101, ST01a, Sea05, SVD07, SBG05, Smi02, SKR02, SNR04, SBEW01, Sty04, Tad02, VMS05, Vau05b, VM02, VM03, WLL09, WBL01, WL00, WHL05, X03, ZYM05, Zho06, Aam03, Ab01, AEEdR05, AL07, AFGH06, BDS^+09a, BDFP05, BC07, CLOS02, CCMT09, CC04b, CCR04b, CRSP09, CHH^+09, CG05, Dw04, FM02, Geb04, GIKR01, GCKL08, HSW09, HL03, HL06, HJW05, HBC^+08, In05, ISTE08, IKOS07, IV06, KOY09, KG09, LL04b, LL04h, LHC08, LC04a, LCZ05b, MT09, ML05, Mu01b, OS00, PCSM07, PBMB01, PQ06, PSP^+08, RH03, RG09, RGX06, Sea09, SBG07, SGMV09, TKP^+08, TCR03, Tse07, Ver01, VK08, WWA01, YGZ05, YT050, hy08, YRY04, ZBP05, ZCL05, vW0K07, An008d, An02, BS01a, BS05, CHK008, FIP02b]. Secured [BNPW03, It001, UP05]. Securely [HL05a, LLK05]. Securing [Abe01, Cal00a, CYH01, Dav01a, FR02, HHS01, Her02, Hos06a, ISW03, LAP08, LLS05b, Mes00, Mes01, RR04, SL05b, TV03, Kwo02, Kwo03b, LPW06]. Security [AW05, AW08, Ahn07, A08, ADR02, And07, An008d, An006c, AHIKM02, BP07, BW07, Bau02, BPM00, BBM00, BP02, BNPS02, BY03, BPR05, BHO^+05, BNN^+02, Bis03b, Bla02a, BF06b, BDWT01, BCHK07, Boy01, BLS000, CG07, CK02a, CK03, Can06a, CCHG01, Cer04b, CK02b, CSW^+08, Che05b, CM05a, CH07a, CS09, Chu03, Coc01a, CK06, Cor00b, Cor02, CGP^+02,
Security-related [Gutxx].

security-sensitive [SPHH06]. seed [TP07, KKJ+07]. Seeing [Wal03]. Seek [Coc01a, PH03, Shp05].

Seeks [CAC06]. Seems [Coc02a]. Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, YV01, Ytr06, AMW07, Bir07, BC05b, CZO5, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bur03, dB07]. Selection [IBM00, JKK+01, RS00, SM08].

Selective [CS07c, LS01a, LM02]. Selective-ID [CS07c]. Selectively [Chi08b]. Self [GMM08, WH05, KY01d, PS01b, PBC05, Sch06b, WHLH05, WLT05b, ZKLO1, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, AMW07, Bir07, BC05b, CZO5, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06].

Seems [CAC06]. Seems [Coc02a]. Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, YV01, Ytr06, AMW07, Bir07, BC05b, CZO5, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bur03, dB07]. Selection [IBM00, JKK+01, RS00, SM08].

Selective [CS07c, LS01a, LM02]. Selective-ID [CS07c]. Selectively [Chi08b]. Self [GMM08, WH05, KY01d, PS01b, PBC05, Sch06b, WHLH05, WLT05b, ZKLO1, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, AMW07, Bir07, BC05b, CZO5, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06].

Seems [CAC06]. Seems [Coc02a]. Selected [BKP09, Bar00c, CCMR05, CSY09, GH05, HA00, MS05a, Neu04, PT06, RSA00e, ST01d, YV01, Ytr06, AMW07, Bir07, BC05b, CZO5, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06]. Selecting [Bur03, dB07]. Selection [IBM00, JKK+01, RS00, SM08].

Selective [CS07c, LS01a, LM02]. Selective-ID [CS07c]. Selectively [Chi08b]. Self [GMM08, WH05, KY01d, PS01b, PBC05, Sch06b, WHLH05, WLT05b, ZKLO1, BCL05a, BCW05, CSV07, CWH00, CCH05, CJ05, Fis01a, HW04, AMW07, Bir07, BC05b, CZO5, CKL05, DRS05, HH04, HH05, PC05a, Wil99, WK06, AMW07, HH04, HH05, MZ04, NH03, PT06].
TLH05, Tsa05, TJC03, WH03, Wy05].

Self-certified
[HW05, BCL05a, BCW05, CWH00, CCH05, CJC03, HW04, HL04, LL06, LWK05a, Sha04b, Sha05b, TLH05, Tsa05, TJC03, WH03].

Self-defense [Wyl05]. Self-Enforcing [GMM08]. Self-Escrowed [PS01b].

Self-Localization [WLT05b].

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

Self-Shrinking [WHLH05, ZKL01].

Self-Similarity [Sch06b]. Selling [Bla01c].

Semantic [PBV08, SN100, Sch00c, Coc01a]. Semantically [KI01b, ST01a].

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

Self-Equivalent [Fer00]. Semi-Equivalent [Fer00].

Semi-Fragile [YCW01]. Seminal [Cop04b].

Sensibility [Sch04c]. Sensibly [See04, Sty04, Sch03].

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

Sensor [AAq05, CS08b, DBS+06, Fin06, GPČS08, LNL+08, NABG03, PJDH09, ZYN08, AJ05, CCM09, HMDVL07, JRR09, KXZT09, KHY08, LD04, Lop06, MWS08, MS09b, NC09, NLD08, PS08a, RAL07, TP07, WDLN09, ZSN07]. Seoul [CL05, KCR04, Kim02, LL03, LL04c, May09, PC05a, PK03, Son00, Won01, WK06].

Separable [CD00a]. Separating [MKK00, Nie02b]. Separation [BYJK08, GKK+09, Ke00, Lys02, Mur00, ZGLX05, BYJK04]. separations [GKK+07].

September [AUW01, AAC′+01, AJ01a, BCKK05, BC05b, CS09, CGP03, DVI05, DKU05, DFCW00, EBC′+00, ELVS01, FLA′+03, GKS05, QS00, RS05, SM07b, WK03, dCdvS05, AJ08].

September19 [AJ01b]. September19-21 [AJ01b]. Sequence [HWH01, MS02c, WHLH05, ÁCTZ05, GB09, SL09, WG02, YZZE09]. Sequences [ADD09, BI09, FSGV01, HG05a, JZCW05].

Sequential
[GSS08, SNW00, RMLH03a, WH02b]. Serial [CTLL01, KWP06, Uni00g, Mit00]. Serpent [BDK02b, ABK00, IK00, IK01, KKS00a, KKS01, KKS00b, Os00, Pat01]. Server [ANRS01, BMK00, Dew08, KO00, LWK00, NS01b, PS05, TMM05, X03, Zha00, B05, LHL04, LKY05b, LHL03b, NTW07, T01, TWL05, Y04]. Server-Aided [NS01b]. Server-Assisted [X03].

serverless [BDET00]. Servers [BIM00, HS07, Jab01, KCD07, Mar02a, TEM′+01, LS05b, PT08]. Service [BACS02, BH00a, CLK01a, DeL07, KZ01, Lan04a, LDM04, Nik02a, Nik02b, PKBD01, CUS08, HILM02, KWD06, LB05, M05, MV03b, SRJ01, SSM′+08, ÜG08, Coc02b, Hii06].

Services [ANS05, BCS02, DJ01, ECM00a, ECM00b, K007, Tsa01, Uni00b, W07b, BDS′09a, BFG04, BFG05, BFG08, CCCC01, HM05, JRB′+06, MPPM09, MV03b, RR04, SBG07, SL05b, TWL05, WA06, BH00b]. serving [LL05]. Session [GL01, OHB08, CS04, RN00b, Uni00a, Uni00b, Uni00f, Uni00e, Uni00h].

Session-Aware [OHBO8]. Session-Key [GL01]. Sessions [KPR03]. Set [BBGM08, GRW06, JRFH01, KS05b, WG05, aSM01, BDET00, Che07, CC05d, DM00a, Mar05b, Sta00]. Setback [MYC01]. Sets [CF05, EIG01, TW07]. Setting [BBM05, DLY08, LP01, PG07, GML02]. settings [Lee01]. setup [PS04c]. Seven [Luc00]. seventh [AAC′+01]. Several [KS00a, LD04, Tsa05, ZT03]. SFLASH [GM02b, SG01]. SGI [Bar00c]. SGID [Tot00]. SHA [AD07, BC04a, GLG′02, HKR01, MP06, SK05a, TYYL02, WYY05d, WYY05b, WYY05c]. SHA-0 [BC04a, WYY05d]. SHA-1 [GLG′02,
Signature-Based [CK02a].
Signature-Embedded [Ano01c, YSS+01].
Signature-Tree [TNM00].
signature/multisignature [Wu01].
Signatures [AO00, AOS02, ABRW01, BN02, BGLS03, BBS04, BSS02, BCCN01, CD00a, CL01b, CNV06, CZB+01, DK01, GMP01b, GM03, Gen04b, Gra02b, HSZI01, Her06, HM02b, HS01b, HHGP+03, HLT01, IR01, IR02, JS05, KZO1, Kal01, LCK03, LS01a, Lys02, MR01a, Mad00, MM02, MNFG02, PCG01, Ram01, RR02, RdS01, WV01, Xs03, Zhu02, An00i, Ate04, AH05, BLH06, BB05, BW02b, BMW02b, BLRS09, Cal00a, CKK03, Die00, DMT07, Fan03, FWW04, FB01, GMLS02, HRL09, Her07, HLH00, JLL01, JL04, KKKL09, LV07, LS05b, MM05, PLJ05a, PBV08, Sch01f, Sha01d, ZNs05].
Signcryption [Boy03, MLM03, Zhe01].
Signed [FL01b, OSSST04, Sch01a, SJ00].
Signer [DKFX05, CJT04, LL05b, WK05, IR02].
Signer-Base [IR02]. signer-verified [CJT04].
Signers [LZL+01, Sae02, Sha03c, YTH04].
Significant [SZ01, MS02b, Shp02]. Signing [An00j, IR01, RR02, HWW4, WK05, WH02b]. signs [Gen00a, Lun09]. SIM [AAKD09]. SIM-based [AAKD09]. similar [Che08b]. Similarity [Sch06b]. Simon [Im03, Ree01].
Simple [AKS06, CYH05, CJS01, CJ03c, CWY05, CC06, CS03c, DT03, FS01, Gir06, HM02c, HLT01, MS01, Nam02, PBD05, RK06, YS02, YW06, Dan02, GM04, KTC03, LKKY03a, LKKY03b, LFW04, XH05]. Simpler [Lin03].
Simplicity [MS01]. Simplification [DJ01].
Simplifications [JS05]. Simplified [Bon01].
Simplifying [Gut04b]. Simply [Oni01].
Simply-Iterated [Oni01]. Simulatability [HU05]. simulatable [Lau05]. Simulation [DKMR05, KL05, CPG+04]. Simulation-Based [DKMR05, KL05].
Simulations [WBRF00]. simultaneously [Wu01]. Singapore [BDZ04, TLC06]. Singh [Im03, Ree01]. Single [GIS05, KO00, MM01b, MM01c, WLZZ05, SV08a].
Single-Chip [MM01b, MM01c]. Single-Packet [WLZZ05]. Single-Server [KO00]. Singular [AS08, Bai01b, BR09].
SINOBOMETRICS [LTT+04, Li05]. SIP [NTW07, PM00, Szo08]. Sir [Bud06]. Site [AEV+07, Coc02a]. Sites [Ros07]. situation [AJ08]. six [Bel07a]. Sixth [Uni00a, Uni00b, Uni00e, Uni00h, TLC06]. Size [CS07c, CM05, HNZ02]. Skein [AEMR09]. Sketching [MNS08, SLTB+06].
Skipjack [Gra02a, HSL+02, SLL+00]. Skipjack-like [HSL+02, SLL+00]. SKLOIS [FLY06]. Sky [MYC01]. SLAAC [CGBS01].
SLAAC-1V [CGBS01]. Slide [Fur02b]. Small [CCM05, ELvS01, Fin02, GPS06, MNT+00, May02, OT03b, RK06, SM02, Sch01e, SPGQ06, Wal03, YLC+09, Du08, dW02].
Small-Project [MNT+00]. Smaller [Bar00c]. Smart [And04, An00a, AJ01b, Bel01, BCST00, Car01, CL07, DF01, DFCW00, DJLT01, HBDJ01, Hen01, HQ05, Jac00, JSJK01, JY01, Lan00d, LSA+07, MOP06, MV01, MG08, NSFQ03, Poh01, Q500, QS01, RE00, RE03, RS01, Sak01, SR01, Sha01c, SP02, TBDL01, VPG01, YKMY01, An00k, An00l, An00c, AJ01a, Bor00, BPR01, BCHJ05, BGL+03, Bur00, Cal00c, CCCI01, Cha05a, Cla00b, Con00, CH00, DMT07, DFH01, DFSP07, Fin03, GMG00, GUQ01, HHSS01, Hsu05b, Hus01, KLY03, LKY05a, Ler02, LC05a, Lu07, MY01, PB01, Pre07, SVDF07, Sm01, TIS07, VK08, Zaf00, BJvdB02, CL04d, CCK04b, Che00, DFPS06, FGL02, Gro03, HL05b, Kt04, KC05, LHY02, Pau02b, SKSS00, Sco04, SCF01, TV03, YW04].
smart-card [GMG00]. Smartcard [HWH01, KRV01, RMCG01, Uri01, PBVB01, BBPV00, CGMM02, DM07b, HRS02, Ito01, KS02]. Smartcard-Based [RMCG01, CGMM02].

Smartcards [CMG01, GN01, IFH01, MS01, Str01a, UST01a, KSW06, Ano04b, RM02]. smarter [Car01, Cla00b]. Smartly [MS01]. Smooth [PS02b, GMR05].

SMS [Coc02b, ETMP05, LLS05b]. SMS-capable [ETMP05]. SMV [ZWWL01]. snake [RD09]. snake-oil [RD09]. Sni [Ano02e]. Snort [GC05]. SOAP [DJLT01]. Social [Ros07, Man08, AG09]. Society [GL05, Kat05b, EY09, LWZH05, Sae02, Sha03c].

Socket [ZL04c]. Soft [DV08]. Soft-Core [DV08]. Software [Ahm07, And07, Ano02e, Bar00b, BC04b, Coc01a, CS05a, DR02c, DF01, GH05, HCJ02, HMM01, Heo01, Jia03, Knu07, KSW02, Lad06, Law09a, LSY01, LLLZ06a, LSVS09, LTM+00, MNT+00, MSNH07, McG06, Nd05, PM00, PS01c, RM04, Sch01a, Sch00b, Ste00, USE00b, VH09, VVS01, WHLH05, Wo04, ZCC01, ARJ08, Ano00h, Ano00i, Bir07, CT02, CCD+04, CTT07, CC04c, DMS07, GPS05, HM04, HL06, Jen09, Mat02, Mca08, MCHN05, Pan03, Sch01d, SS03, WLT07a, WA06, Sal03b, Bol02].

Software-Efficient [HCJ02]. Software-Hardware [PS01c].

Software-Only [Hoe01]. Software-Oriented [ZCC01].

Software/Software [Nd05]. SOI [Ano02e, NFQ03]. SOISIC [Ano02e]. Solaris [Ano06c, BH00b]. Solomon [KY02b]. Solution [Cap01, DHR00, LLS05b, Poh01, Str02, TvdKB+01, LSH00].

Solutions [Ano04a, MV01, Jan00, MSK03, MV03b, St.00, Gum04]. Solve [CU01, GS03].

Solving [CJT04, GPP08, Wil01a, Bul09, Whi09]. Some [AG01, BDF+01a, DJ01, DFG01, GM02c, HSS04, JMV02, KY01b, MT02, Max06, PQ03a, Rot01, Rot02b, Rot03, Wal01, Fur01, HAnR04, He02, JK01a, RSS04, SHT05, ZF05].

Somen [Ano03c]. Something [FL01b]. sometimes [FNRC05]. Sons [And04]. Sorry [San05]. sorts [Ano03e]. Soul [Bla01c]. Sound [BJP02, FR08]. Soundness [ABHS09, DPV04, MR01c, BPS08, Lau08a].

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

Sources [KZ07, WLZZ05, KZ03]. Southampton [Bla03]. Soviet [AJ08]. SP [BG07a, Hir09]. SP800 [SF07]. SP800-90 [SF07]. SPA [FMP03, Nov01]. SPA-Based [Nov01].

Space [BGH07, Lu02, MSNH07, NS05a].

Space-Bounded [Lu02]. Space-Efficient [BGH07]. Spain [BS03, DFP06]. Spam [CMB+05, DGN03, Vix02]. Spamming [Bel04]. SPARX [Jen09]. Sparse [BLST01, BDG+01b, FS01b, GS03, BF06a].

Spatial [MM01a, SGM09, SDFH00, Lin00a, SL09, YPPK09]. Spatial-Domain [SDFH00]. Spatio [CDTT05].

Spatio-Temporal [CDTT05]. speakables [BZ02]. Speaker [LM00]. Speaks [VN04].

Spec [Bar00c]. Special [Ano04a, Ano07b, Ano07a, BK06b, GIS05, GS07a, GPP08, SGK08, KP03, FOP06]. Special-Purpose [Ano07b, Ano07a, GS07a, GPP08, SGK08]. specialized [Wan04b]. Specific [HCK09, Zir07]. Specification [BCST00, ECM00a, LKJL01, RSA00c, Mea04].

Specifications [IEE00b, BDFP05, BD04a]. Specified [Tad02, He02, LWK05b, YY05a, ZX04].

Specifying [BJvdB02, Cir01]. Speck [KGS07]. Spectr [GMM01]. Spectr-H64 [GMM01]. spectra [MS02b]. Spectral [QPV05, SK07]. Spectrum [BQR01, LY07, PM00]. Speech
Speech-Generated [MRL\textsuperscript{+02}]. SpeechStudio [Ano02e]. Speed [Ano00d, Ano02a, Gro01, JKRW01, KMM\textsuperscript{+06}, Lut02, SOTD00, SM02, Wie00, YKMY01, BGL\textsuperscript{-03}, RW07, RMC01].

Speeding [Osv00, SWH\textsuperscript{-09}, TC05]. Speedup [YKLM02b, YKLM03]. Speedy [Cre00]. spherical [LZP\textsuperscript{+04}]. Spider [Tur04]. Spies [Gan01b, Win05c, Hau06, NRR00]. SPIHT [Che08a]. SPIN [MS02a]. Spline [SPK08]. Splitting [GMW05, LLK05]. SPN [HLL\textsuperscript{+01}, Kan01, PQ03b]. SPNs [CKL\textsuperscript{+03}]. spot [Naf05]. Spread [BQR01]. Spring [Pap05]. Spring-Verlag [Pap05]. Springer [Fal07, Lee03a, Lee03b, Pho01]. Springers [Wil09]. spying [FNRC05]. spymaster [Bud06]. spyware [Ste05c]. SQL [Dew08, HILM02]. Squadron [OC03].

Square [HCK09, HQ01]. Squaring [CH07b, NS02]. SRAM [HBFO9]. SSC2 [HQR01, ZCC01]. SSH [All03, BS01a, BS05, BKN04, Dwi04, H-io1, Hos06b, Kra02b, Naz02, One05, SWT07, Str02].

SSH-Connected [H-f01]. SSHFS [Hos06b]. SSL [ASK05, BPST02, CHVV03, JRB\textsuperscript{+06}, KCD07, KPR03, Kra01, LLK05, LW00, Net04, OHBO8, SB01, SQ01, Van02, ZFK04].

SSL/TLS [BPST02, CHVV03, KPR03, OHBO8], SST [Gau02]. St [GKS05, NH03, AS01a]. Stack [Pot03]. Stage [Kak06, CHY05b]. stamp [CL00]. stamping [HHC05]. Stamps [KZ01]. Stand [CAC03]. Standard [Ano08d, Ano09, Ano12, Bar13, Bar00a, BCP02a, FIP00, FIP01a, FS01a, Her09, Hug04, HLC08, IEE00b, MM01c, MP01a, Nat00, PM00, Pha04, RSA00b, RSA00d, RSA01, RSA02, RSA03b, SM02, SK05a, BBK\textsuperscript{-03b}, DRS05, GM08, Sea09, Tan01, Ase02, Bar00c, HI00, Bur03, CM00, Coc02a, Coc02b, Cur05, DR01, DR02b, Dan01, FIP02b, GC01a, Har00, Lan00a, Lan00b, Lan04a, Mor05, NIS00, SB00, Sta00, Sye00, WBRF00, Wri01, YW06].

Standardized [Man01]. Standards [Ano01f, Bur06, CL07, Cuc02b, Hsu01, RSA00a, Tsa06]. 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\textsuperscript{+09}, Jun05, KK07, LZ01, LLL\textsuperscript{+01}, MV03a, Neu04, Pro01, RSN\textsuperscript{+01}, BKV03, Hey03].

Statistically [Fis01b, HR07, HNO\textsuperscript{+09}]. Statistically-hiding [HR07].

Statistically-Secret [Fis01b]. Statistics [CKN01, CN04, KLMM05]. Status [Pre01, Sha03b]. statute [Cal00b]. STDM [WMDR08]. Stealing [Gan01b]. Stefan [AUW01]. Steganalysis [Pro01, Sal05b, WW04]. Steganografie [Sch09]. Steganographic [CTL04, HR02, MJF07, RH02, RS00, Wes01, KC09a, LYC02, WW08, YCL07].

Steganography [BC05a, BGI08, CYH01, ChLYL09, CDR01, CW09, CTH08, Col03, CMB\textsuperscript{-08}, CS05c, DIRR05, DRL09, FGD01, Fri07, Gal03, HLvA02, HvAL09, Hn05, HSK01, LS08, PH03, Sal05b, Sch09, Sha01e, Shi08, SWR05, Wan05, WW06, CDS07, Che07, Che08a, GGS\textsuperscript{-09}, JD01, KPO0, LT04, WW04, WMS08, Way02b, Way09, YCW07]. 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 [SSNG00, Win05c]. Storage [DFSS08, Din01, Din05, HR02, Har07b, Hug04, MSTS04, RCBL00, Ric07, RH02, Vad03, AFGH06, DFSS05, HGR07, LPM05, SGMV09]. Store [CTBA+01]. Storing [ST06]. Story [Ben01b, Ben04, Bud00a, Gas01, Kah67a, Kah67b, Kar01, Sch09, Bud02, DB04, Hau06, Hig08, HS01a, Win00]. strategic [AJ08]. Strategies [Cir01, KL05, SKQ01, Dwi04]. Strategy [DR02a, TPPM07, KC00a]. Stream [BCC01, BSW09, BS00b, BL02, CF01b, Cant06b, CJ301, CHJ02, CM03, Cout03, CL02c, DF07, Fi00, FO1a, Go10d, GM020, HCJ02, HR00, HR04a, Jam00, KHD01, MSNH07, PP06a, SM01, Sar02, SY01, WB02, Wu02, ZC00, ZC01, BGP09, Ber07, BD00a, BG08, BV04+0, DK08, KH08, Max06, MI09, PCS03, PCC03, SB05, WW08]. Stream-Cipher [SXY01, WW08]. Streaming [OS05]. Streams [AIP01, YLC+09]. Strength [CB01, JX05, Oui01, CLK+99]. Strengthening [Loi00, MHH+02]. String [CP07, DFS04, Pas03, Dam00, RG05]. Strings [Vau05b]. Strong [ADD09, BB00b, CS00, DKFX05, KCJ+01, KW00, LH03a, LH03b, Lu02, Pau09, SBZ02, WHL05, CCO4b, HRS08, KTC03, Ku04, LL05b, SS03, ZT03, ZFK04]. Strong-Password [LH03a, LSH03b, WHL05, CCO4b, KTC03, Ku04]. Strongly [Y06]. Structural [BS01c, LBR00]. Structure [DNP07, EIG01, H010, HLL+01, MR02a, MR02b, GT02, HSL+02, MF07, PS02a, SG07, SSL+00, XMST07]. Structured [BRTM09, CKK03]. Structures [An002e, DS06, GTT03, HCD002, KCP01, Kus02, MND+04, MFT05, PSC+02, PQ03b, Sun00a, XH03, Hen06a, IY06, SWR05]. struggle [Bur02]. Stuart [Gum04]. students [AA04b, PP09]. Studies [Pag03, SPH06]. Study [BBGM08, Car02, DPR01, DP00, KKK+07, WCZ05, BKN04, BF06a, DY09a, KW06, SKW+07, ZW01]. Stuttgart [Eag05]. style [BPS08, dH08]. Subcommittee [Uni00f, Uni00h]. Subdivision [LDD07]. Subgroup [NBD01, KM04a]. Subgroups [Gro05, GMR05]. subsampling [LCO6b]. subscribe [SL05b]. subsets [Sch01e]. substitute [Bih02]. Substitution [KKG03, GPX08, RBF08, WL04b]. Substitution-Permutation [KKG03]. Subsystem [HL07, MBS04]. Subleties [Lai08]. subverting [HB06]. Success [An006d]. successful [KH03]. Succinct [BA06, FS08]. Sued [Nic01]. Sufficient [IKO05, Kos01b, KNO0, MN01]. Suffix [ABM08]. SUID [Tot00]. SUID/SID [Tot00]. Suitable [AIK+01, CQS01, KTT07, LKH09, SP05, Wenn]. Suite [RSN+01, SBE01, YLT06]. Suited [WWGP00]. Sum [Che04b, KLY02]. Sum-of-Digits [Che04b]. Sums [CY08, Shp05]. Sunspots [CP07]. Super [Lam07, CAC06, Hos06b]. supercluster [Pri00]. Supercomputer [Coc01a]. Supersingular [Gal01, RS02, Ver01]. Supplemental [BBDL01]. Supplementary [ECM00a, ECM00b]. Supplies [Sh01c]. Support [ABM00, Gro03, LTM+00, PJDH09, SB02, An005b, BMA00a, BMA00b, BM00c, ED03, MGFt05, SSM+08, WNQ08, ZYL05]. Supporting [CLK01a, SW02]. Suppression [GA05]. Sure [Tom06]. surface [Iwa08, LDD07]. Surfaces [SPK08]. surveillance [LCS09]. Survey [EPP+07, KM04b, HDH06, ATS04, Kao00e]. BEM+07, CDL06, EY09, Mea04, Miel01b, OZ08, PC09, Pre07, RH03, RAL07, Sch01f.
ÜG08, ZLZS07. Survivable [CLZ02].
Susan [Jan08a]. SVD [CYH+07, FWL08].
SVD-based [CYH+07, FWL08]. SVGGrid [ZBP05]. Sweden [BS01b, Joh03]. Swedish [Bec02].
Swiss [Boy03, Kid00]. Switching [CT03]. Switzerland [CC04a, Vau05a].
Symbiosis [DF01]. Symbol [SVDF07]. Symbolic [Bor01, Jef08, Mar02b, May09,
MT07, MP05, ALV02]. symbols [Lun09]. Symmetric [Ano01j, ABM00, CCM01,
EP05, RR00, BMA00a, BMA00b, BMA00c, DW09, Lee01, PBMB01]. Symmetric-Key [Ano01j, ABM00, CCM01,
EP05, RR00, BMA00a, BMA00b]. symmetry [RBF08]. Symposium [ACM00, ACM01a, ACM02, ACM03b,
ACM03c, ACM04b, ACM05b, ACM05c, ACM06, ACM07, ACM08, ACM09, ACM10,
Ano00d, BS03, BCDH09, BC01, CGM07, IEE00a, IEE01a, IEE02, IEE03, IEE04,
IEE05a, IEE05b, IEE06, IEE07, IEE08, IEE09b, Jef08, KM07, MFS+09, SMP+09,
TC06, USE00d, USE01c, USE02b, May09, dCdsnVSG05]. synchronisation [CMdV06].
Synchronization [GPCS08, SW02]. synchronize [Pau02b]. Synchronous [CH01b, Sar02]. synoposes [YLC+09].
Syntax [BWBLO2, RSA00b, RSA00d]. Synthesis [XFZ01, SOIG07, UBEP09].
sysslogs [ME08b]. System [Ano02d, Ano02e, ANR01, BIP05, BCST00, Bhi00, CCDP01, CHM+02, CSW+08,
CGJ+02, DJS01, DGP07a, DGP07b, DV08, EM03, FL01a, Ito01, Joh05, KC02, KHY04,
LV00, LSZ05, LLS05b, LXM+05, MA00a, MA00b, Miy01, MFK+06, MFS+09, RH02,
SR01, Sha02, SO00, Ste05b, TK03, TZZT09b, USE00a, WG05, WA07, YKMY01,
YKL02b, ZYM05, AHK03a, AMRP00, Ano00j, ADH+07, AAKD09, Bhi00,
BDE00, Bu09, CC02b, CCH05, CIL06, CPG+04, Cocc01a, Cre00, CO09, DZL01,
DPT+02, DIM08, DGP09, FP00, GG08, GMG00, Gou09, HLL+02, Joy03a, KWDB06,
KX00, Kwo03a, LL04b, LKJL01, Lin00a, Lk01, MKKW00, RCG+05, Sa00b, SCS05a,
SGMV09, SETB08, TKA+08, Wan04a, dB07]. systematic [DW05, ZL04a]. Systemic [KB06]. Systems
[ACM03c, ACM05b, ANRS01, Ano02e, BCS02, BRTM09, CP02, ELvS01, Fel06,
GS03, GRW06, IEE01b, JQ04, KKP02, Ket06, Len01, LST+05, LLLZ06a, LJ05b,
Lut03, Mar02b, MYHM02, NAGB03, RS05, Ri02, SM01, SRS07, SXY01, USE00c,
USE00b, Vav03, VHP01, WKP03, ARJ08, Ano08, Ano01j, Bid03, Ble07, CUS08,
CC05c, CCA05, CBL+08a, CL+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, NAM06, Nis03a, PBMB01,
Par04, PI06, RI07, SRS07, TOEO00, WA00, QX07, ZSV05, Ano02d, Lut03].
Systolic [KLY02, KKY02, MP01c].
Table [Ano03d, MFFT05, XFZ01, BZ03,
CC05b, Has00]. table-based [Has00].
Tables [AJO08, KB39, RBF08]. Tag
[KKJ+07]. tagging [BP05]. Tags
[OS06, ACdM05]. Taipei [Lai03]. Taiwan
[Lai03, Ano03a]. Takagi [LKYL00].
Takagi-cryptosystem [LKLY00]. Takaragi
[WHHL03]. Taking [CDS07, Lai07, PM00].
Telbot [Ros07]. Talk [FGM00a, Lau00d].
tamer [Kap05]. Taming [Aba00, Lov01].
Tamper [LTM+00, CT02].
tamper-proofing [CT02]. tampering
[PS08b]. tandem [DPT+02]. tank [Pau03].
tar [Str02]. targama [MA00, T05]. target
[BD04b]. Targets [MV01, Pau03].
Tarragona [DFPS06]. tasks [XQ07]. Tate
[Jou02, SKG09]. TATSU [TS00]. tattling
[CSK+08]. TC [DKU05]. TC-11 [DKU05].
TC-6 [DKU05]. TC11 [ELvS01]. TC8
[DFCW00]. TC8/WG8.8 [DFCW00]. TCB
Three-Key [BR00b]. Three-party [LSH00, CLC08, LLS+09, YC09a].  

Three-Principal [ZL04b]. Three-Stage [Kak06]. Threshold [AF04b, AIP01, BTW05, BTW08, BDDS03, BSS02, CCD07, CLT07, CDN01, DK01, DN03, DG03, FS01a, FP01, JL00, KY02a, Kin00, Kin02, Kog02, LSL+01, LSC03, LCL05a, LP01, MSJ02, Nie02c, STY07, WQWZ01, Wan04b, WH03, XSL03, BCW05, BMW02a, CL02b, CC05a, CYH04, CHY05a, Che05a, HW02, HW03, HW05, JLL01, JL04, LCC05, LCL05c, SCL05, TLY04, WHLH03, XCO5, YTH04]. Throughput [HV04, LS01b]. thwarting [WL07a]. TI [GBK01]. tib [MAaT07]. Tickets [FGL02, KS02]. Tie [SZS05]. tier [TW07]. 

Tight [CM05a, Di 01]. Time [AK02a, App07, AJ008, BPST02, BS00b, BSW01, CU01, CJ03a, CNV06, CLZ02, Dri02, GP02S08, HM02b, Ina02b, KL05, Kuh02a, LP02a, LSL06, LSL05, LLM04, May04, Occ03, Plk01, QSR+02, RR02, CAC03, CCK04b, CL00, DS02, GSO7b, GM04, HHC05, LCO4a, MRST06, NS05a, YZD07, hY08, DK08]. time-bound [hY08]. Time-Domain [Kuh02a]. 

Time-Free [CNV06]. Time-Limited [AK02a]. Time-Memory [AJ008, Oec03, QSR+02]. 

Time-Memory-Data [DK08]. Time-Reversed [Ina02b]. time-space [NS05a]. 

Time/Memory/Data [BS00b]. Timed [BN00b, CHK008, JP07, LSL01, Mao01, HGN03, Zha06]. Timed-Release [CHK008, Mao01, HG03]. times [AJ08, CCK04b, Mol05]. timestamp [YW04]. timestamp-based [YW04]. 

Timestamping [MS05]. Timing [CKQ03, CWR09, Law09b, Sch01b, SWT07, ASK05, DKL+00a, KS09, OS00]. timing-attack [KS09]. Tiny [Bar00b, WN95, And03]. Tipsy [TvdKB+01]. Tissue [MYC01]. Title [ZYH03]. TLS [BPST02, CHVV03, HSL+05, JK02b, JJ02b, KPR03, OH08, SBE01, BFCZ08]. 

TMAC [K03]. TMS20C6x [WWGP00]. today [Li05, Nis03a]. Together [WD01a]. 

Token [Fri01, RSA00d, RSA01, CS04]. Tokyo [An00d]. Told [ES00a]. Tolerance [An04a, Bank06b]. Tolerance [DS03, HSC01, WL07b, BKW03, HGR07, Lin07, P06, RMH04, YHJ04]. Tolerating [KSR02, SKR02]. too [Sch05c, vT01]. took [IEE09a]. Tool [An02d, An02e, Kil01b, GPG06]. Toolkit [Nis01a, Sha01a]. Tools [An02d, An02e, Bar00b, G01b, Ken02b, Ust01b, Bai08, Cas02, CT02, GC05, NCRX04, SETB08, Kat05b, Puc03]. toolset [Jen09]. 

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

Top-Level [MV00]. Topics [HSS01, IEE01b, Joy03b, Men05, Nac01, Neu04, Oka04, Po06, Pre02c]. topology [HJ07]. 

Tori [GV05, GPS06]. Toronto [MS05a, VY01]. torsion [KM04a]. torsion-subgroup [KM04a]. Torus [RS03, RS08, vD04]. Torus-Based [RS03, RS08, vD04]. Tossing [Lin01b]. 

totality [HRS08]. Touch [Pau02a]. tour [Pet08]. Town [KJR05]. Trace [B01, LNS02, NN03]. trace-and-revoke [NN03]. Traceability [HLL03, HW05, WLH05, WY05]. 

Traceable [LZL+01, CLH04]. traceback [CS04]. Tracing [KY01d, KY01e, LLL02, SNW00, T01, WRW02, WLZ05, WH01]. 

Tracings [RE02]. Track [Fox00, Joy03b, Nac01, Oka04, Po06, PHM03, Pre02c, USE01b, USE02c, Men05, CAC03, CAC06]. Tracking [WCJ05, FNRC05, SZ08, TWM+09]. Trade [BR00b, Kak06, LSH00, MAaT06, AJ08, CLC08, FGM03, G05, LKY05b, LLS+09, MF07, MAaTxx, SPH06, YC09a, ZL04b].
[AJO08, CMS09, Oec03, PS01c, Uni00f]. Trade-Off [AJO08, Oec03]. Trade-Offs [PS01c]. Tradeoff [LP02a, QSR+02, CW02, Ino05, NS05a, DK08]. Tradeoffs [BS00b, CTLL01, SRQL03, SU07]. Trading [PV06b, SWH+09]. Traffic [FGL02, Mii08, Fie09]. Trail [DR02a]. train [Pri00]. Training [Coc02a]. Traitor [KY01d, KY01e, LLL02, SNW00, TT01, WH101]. Transacted [HBdJL01]. Transaction [RH02, AAKD09]. Transactional [RH02]. Transactional [ST06]. transactions [Cal00b, Cal00a]. Transcript [Ano01a, Ano01b, Ano01c, Ano01i, Ano01j, Ano01c, Ano01k, Mal02, Nik02b]. Transfer [CT08b, Din01, GKM+00, KKL09]. Transferability [HSZI00]. Transfers [IKNP03]. Transform [ABM08, BR09, CPX04, BR09, BR09, KLLK05, Nak01, SSFC09, VK07, BR06, Che07, OP01b, SR00, LPZ06]. Transformation [CT09, HLL05, DSP01]. Transformations [Fel06, KYHC01, LMTV05, Pag03]. transforms [La00]. Transient [Ric07, VS08]. Transistor [Coc02a]. Transistors [Bar00b]. Transit [Con00, Cal00c]. Transition [Ase02, TL07]. Transitive [BN02]. Translation [GGT+06]. Translation-based [GGT+09]. TransLink [Cal00c]. Transmission [MLC01, SNR04, SVDF07]. Transparent [CCDP01, For01, Lin00a]. transport [Bor00]. Trapdoor [BPR+08, Fis01h, KO03, KO00, Gen04a, JSW05, PW08]. Trapdoors [GPV08]. Travel [Bur00]. Traversal [JLMS03]. Trawling [Km00a, Km00b]. treatise [Bla00, MAaT03, MAaT04, MAaT07]. treatises [MAaT06, MAaT07]. Treatment [CL05, DK08]. Tree [CC05d, GST04, JLMS03, KPT04, LLLK05, LM02, TNM00, Mon03, PCC03, WL02]. Tree-Based [GST04, KPT04]. trees [Che02, Che07, TC00]. Trends [Ahm08, KB07, Or00, NaM06, PRS04]. tricks [All03]. triggered [HHJS04]. tripartite [SW05]. Triple [HS+01, BR04, CBGB01, Cor00a, FZH05, Ke05, LMP+01]. Triple-DES [Cor00a, LMP+01]. Triples [FSL01b]. Tripwire [TvKB+01]. trival [KO00]. troubleshooting [HJW05]. True [BST03, Chau04, DV08, EHK+03, HBF09, Pan07, SFDF06, BG08, BG09, GB09, Hau06, HWZ09, Ste05c, vT01, VKS09]. Truecrypt [CSK+08]. truly [BGL+03]. Truncated [CS05b, KM02, LHL+02, SKU+00, SK10, GS09]. Trust [CHSS02, HCCD02, Lin00b, LHL+08, Mit02, SMP+09, Dav01c, HHJS04, IY05, LCK04, LLW05, LMW05, LLW09]. Trusted [DK01, WH101, WV01, ARJ08, PS04c, ZLYG05]. Trusting [CKS09]. trustworthy [CCH05]. Truth [MNT+00]. Tseng [Hwa05, XY04, ZAX05]. TTM [GC00b]. Tuesday [Uni00a, Uni00f, Uni00c]. tunable [LB05]. Tunny [Sal01a]. Turin [AL06]. Turing [Bar00b, RSA03a, Adl03, Coc03, Cop04b, Goo00, Pet08, Riv03, Sha03b]. Turkey [Bar00]. Turkish [DD02]. Turn [Tsa07]. Turning [DJL01]. tutorial [Can06a, Puc06, Rot02b, Rot03, vT00]. Tweakable [DS08, HR03, LRW02]. Twentieth [Ban01b]. Twenty [AC03c, ACM05b, AAC+01, B+02, Lan00a]. Twenty-Eighth [B+02]. Twenty-first [Lan00a]. Twenty-Fourth [AC05b]. Twenty-Second [AC03c]. Twenty-seventh [AAC+01]. Twin [Ram01]. TWIRL [ST03b]. Two [Ahm08, BG+01, DIS02, FD01, Hen06b, HSIR02, HSS01, HU05, HLT01, HLM05, JZCW05, KCP01, KO04, KTC03, K103, Lin01h, MR01a, MLM03, MAaT07, NS01c, Ngu01, Pau02a, Sch05c, SK00, St00, Ste05a, Ste01, TW07, WW05, XS03, YDD01, CLOS02, DHL06, GCKL08, JW01, LMTV05, MS09c, McN03, MCHN05, Pau01, ZLX99, dB07].
Two-Block [KCP01], two-channel [MS09c], Two-factor [Hen06b, Sch05c, St00, Ste05a, dB07], Two-Key [KJ03], two-level [DHL06], Two-Party [K04, Lin01b, MR01a, WW05, CLOS02, GCKL08, JW01, ZLX99], Two-Pass [SK00], Two-tier [TW07], Two-Way [DIS02], TWOBLOCK [Yan05], Two-Shadow [BF00b, FKSW00, IK00, Kel00, Knu00a, Knu00b, Luc02a, Mur00, SKW+00], Type [CKQ03, Dug04, Hf001, KYHC01, PDM09, 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, Chr01, CCMR02, CCMR05, KN03, Pat03b, RS05, Sma05, Hon01], Ultimate [Di001], ultra [Bam02, CH07a, DB04, Cal01, Win00], ultra-lightweight [CH07a], ultra-secret [Bam02], Ultrafast [FF01a], UltraSONIC [MM002], UMTS [Ch05b, HL07], Unauthorized [Ano02e], Unbalanced [FMP03, May02, HLL03], Unbelievable [Len01], Unborn [Pau02a], Unbounded [RW02, WvD02], Unbreakable [Ver06b], Uncertain [See04, Sty04, Sch03], UNCITRAL [MNFG02], uncompletatable [NS01a], Unconditional [HM01b, May01, Pas05, RW03b, WW05], Unconditionally [HSZI00, HSZI01, HSHI02, HSHI06], Uncovering [MNT+00], Uncrackable [Ano02e], undeciphered [Rob02, Rob09], Undeniable [GMP01b, GM03, JSJK01, Miy01, WQWZ01, CH05, LH04, LCZ05a, SSM+08], undergraduate [AA04b, Gha07], undergraduates [DFG04], Understanding [CPG+04, Cra05b, Elb09, Gor06, PP09, Sun05, Lum09], undetachable [BMW02b], Unexpectedly [Bar00a], Unforgeable [BK02, KY01a], Unicode [MJF07], Unified [CZB+01, HKA+05, MFS+09, SM03b], Uniform [SPK08, TL07, SU07], uniformity [Shp01, Shp04b], Unimodular [CV03], Unique [Lam91, Lys02, TH01], United [DFC00, Jo01], Universal [BOHL+05, CR03, CJNP02, CS02, Irf00, KKKP05, KO03, Phi01, Sho00a, SP79, Cal00c, PS04c], universality [DS02], Universally [AF04b, BLD09, CF01a, Can01a, CK02b, CLOS02, DN02b, DN03, NMO05, RK05], Universally-Composable [AF04b], Universiteit [BBD09], University [Kat05b, Pur03, Rot07, Top02], UNIX [CCDP01, Har01a, Har01b, Hf001, Wit01, GSS03], UNIX-Type [Hf001], Unknown [CT08a, Luc02b, CSW05, HJ07], Unknowns [CMB+05], unleash [McN03], Unleashing [Lop06], unlinkability [WHH05], Unpredictability [BS01d], unprotected [ASK05], Unravelling [Ano03e], Unsolved [GG05a, Bel07a], untold [DB04], untraceability [CL09, LH05, Par04], Untraceable [AcM05], Untrusted [BMK00, CGK+02, LS09, LLK05, ZBP05], Unusual [GG05a], Unveiled [Bar00a], Update [TEM+01], Updated [Cho08a], upgrade [Pau02a, Pau02b], Upgrades [Ano02e], upon [DFG01, PQ03a], UPPAAL [BB+02], Upper [BP03b, DIR05, KMT01], Upwards [FV03], URSA [LKZ+04], US$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, Poi06, Pre02c, Sch01d, Sho05a, Si01, YDKM06, ACM10, Bel00, Bon03, BCDH09, ELvS01, FMA02, IEE01a, IEE05a, IEE05b, IEE08, IEE09b, Kil01a, MS05b, NIS00, Sch00a, Sch01c, S+03, Sch04a, Sch04b, Sch05a, SMP+09, USE00c, USE00b, USE00a, USE01b, USE01c, USE01a, USE02c, Wi99, Yui02a]. **usability** [CG05]. **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, Had00, HY01, KZ09, LSZ05, JR03, OHB08, PS010, Poh01, Sas07, SM+08, Str01a, Ts01, BBM00, CLR04d, DLY08, GML02, Hsu05b, HL05b, KCS05, LAPS08, LHY02, LHL02, LKY04, LKY05a, LHL03b, LCO05a, LK01, Par04, SS03, SZS05, TWW05, WLT05a, YS04, YRY04, ZYL05, vOT08]. **User-Centered** [CMB+05]. **user-controlled** [LAPS08]. **user-drawn** [vOT08]. **user-friendly** [SS03]. **Users** [LS05b]. **Uses** [Bau01c, RSQL03]. **ushers** [Bur00]. **V** [Kat05b, Puz04, S+03]. **V1.1** [RSA00d]. **V1.5** [CJNP00]. **v1.7** [RSA00b]. **V1.9** [Man01, RSA00e]. **V2.1** [RSA02]. **V2.11** [RSA01]. **V5** [It00]. **V5.1a** [CSK+08]. **Vail** [BC01]. **valid** [Wan04b]. **valid-signature** [Wan04b]. **Validation** [ABRW01, BLM01, KCJ+01, BBG09, ME08b, VM03]. **Validity** [Zho02]. **Valuable** [PM00]. **Value** [BR09, GIPS05, LS08, BWMW02a, DK08, WWTH08]. **valued** [TL07, MS05a, ZFW05]. **Vancouver** [IEE02]. **Varadharajan** [CJT03]. **Varadharajan** [MS03a]. **various** [SV08a]. **Variables** [HR04a]. **Variant** [Luc02b, NSNK05, Ber08, Dju08, Dju09]. **Variants** [BDK+09, DG02, KS00b, CJ05, Sha04b, TJC03]. **Varieties** [RSA02]. **Variety** [AOS02]. **Vascular** [BDD09]. **vault** [SHL07]. **Vector** [AS08, Che01c, DNP07, SBG02, WC04, Pe09, mSgFl05, WNQ08]. **vectors** [LHL04]. **Vegas** [ELvS01, IEE01a]. **Vein** [BDD09]. **Vendors** [Pau03, MV03b]. **Venona** [Ben01b, Ben04]. **Verenigde** [dL00]. **Veridicom** [Ano02d].
Verifiable [ANR01, Ate04, CD00a, CS03a, CHS05, Cha04, JLL02, JG01, Lys02, NZC05, NZS05, NSNK05, NN06, CHY05a, CDD00, GIKR01, KKL09, SC05a].

Verifiably [BGLS03, Hes04a].

verifiably-encrypted [Hes04a].

Verification [AADK05, Ara02, BPST02, BP05, GMV01, GL00, Gut02b, Gut04a, HWH01, Hoe01, Str01a, BD04a, CC05b, CJL06, Coh03, DS00, HL05c, JW01, Ler02, MD04, MT07, MSP09, PBD07, TYH04, Wan04b, Wu01, YLC+09, ZLX99, ZL04b, CS08b, Uzu04].

Verifed [BJP02, BFGT08, BFCZ08, CJT04].

verifier [Bla01b, LKY05b].

verifier-based [LKY05b].

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

Verify [MS02a].

Verifying [BFG08, BJvdB02, CJM00, HLT01, IR01, PT08, RR02, BLH06, BLP06, HLH00, SV08a, Shat04].

Verlag [Eag05, Lee03a, Lee03b, Pap05].

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

Versions [HSR+01, NPV01, An006, CV05].

Versteckte [Sch09].

Versus [Mad00, Rub00, WWL+02, ASW+01, BJLS02, DBS01, WPP05].

Vertically [DN04].

Very [AAC+01, B+02, CG03, EBC+00, FLA+03, Hf01, PM02, PBMB01, Zir07].

Vestiges [Top02].

VI [Sch04a, via AGKS07, An006, ACdM05, BDPV09, Car02, Ch03, CPG+04, FBWC02, Fox00, HHYW07, HLM03, J00a, KT06, ML05, PG05, RG05, SB01, SLG+05, ZL001, Lud05].

Victoria [ACM08, IZ00].

Victorian [Top02].

victory [Ha03].

Vid [CAC06].

Video [BDF+01a, BD03, CDTT05, E+F+05, ISS08, KBD03, KJR05, KLL01, LHS05, MLC01, SC02a, BS01b, JA02, KN03, UP05].

Video-Based [KJR05, BS01b, KN03].

videos [YZDW07].

Vienna [BZ02].

Vietnam [Lov01].

View [Bar00a, Mah04, Sin09].

Views [Bar00a, Bar00b, Bar00c, Cocc01a, Cocc02a, Cocc02b, Cocc03].

Vigenère [DG00].

VII [Sch04b].

VIII [IEE01b, Sch05a].

Virginia [MS05b].

Virtual [An001c, HM01a, Pro00, YSS+01, BDS+09a, ML05, ZBP05].

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

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

Virtues [Tro08].

Virus [G06, An005b].

Visible [HT06].

Visual [BDF01, BDF02, BD04a, CDD07, DD04, HKS00, Lav09, PY08, Yan02, YC07, Bon00, Zol01].

Visualization [XYL09, MFS+09].

Viterbi [LBGZ01, LBGZ02].

Vladimirov [Puz04].

VLDB [EBC+00, FLA+03].

VLDSP [B+02].

VLSI [KV01].

VMSS [SC05a].

Voice [An001, PK01, VN04].

VolIP [An006, SZ08, VAY09, WCJ05].

vol [Kat05b, Lee03b].

volatile [SETB08].

Volume [Gol04].

Vortrag [Eke02].

Voter [Cha04].

Voter-Verifiable [Cha04].

Voting [Cha04, FPS01, Hs00, Joh05, JLL02, KMO01, Rub01, CJT03, HJW05].

Voylich [Rug04].

VPN [KMM+06].

VPNs [Dav01a].

VQ [WJP07].

VQ-based [WJP07].

Vs [CTBA+01, Di 01, Di 03, SU07, WW04].

VSS [AF04b, CDF01, FM02a].

Vu [DP00].

vulnerabilities [CS05, DMS05, Swi05, XNK+05].

vulnerability [KHL09, SGA07, YRS+09].

WA [ACM06].

WACs [Kov01].

Wagner [DVP06].

Wagstaff [Kat05b].

Wahab [MAaT07].

Walking [Fox00].

Wallet [ETZ00, JL04].

Walsh [MS02b].

Walsingham [Bud06].

WAN [H06].

WAN-Cluster [H06].

Wang [S05].

WAP [JRFH01].

War [Bec02, Bud00a, Bud02, Hau03, K01, MH09, OC03, AJ08, DB04, Ris06, Lov01].
Wave [HW01, WW04]. warrior [PC04].
Wars [RR03b]. Warsaw [AUW01, Bih03].
Washington [S’03, USE00a, USE01c].
wasn’t [Bur02]. WaSP [Coc02b]. WASSA [Ano05b].
Watch [MA00a, Joy03a].
Waterloo [HH04, HH05, ST01d].
Watermark [AS01b, GMV01, JX05, KHY04, Kwo03a, Meh01, PBB02, Re02, SY01a, CAC03, TH01, WY02, Zan01, AA08, CL08, LYGL07, LLC06a].
Watermark-based [Kwo03a].
Watermark-Fingerprint [KHY04].
Watermarked [ST01c]. Watermarking [AS08, AK02b, AHK03b, AS01c, Arn01, ARC+01, BR09, BSC01a, BSC01b, BSL02, BQR01, BSN000, CC02a, CH01b, CDTT05, CT09, CT02, CM02, CMB+08, DWN01, DNP07, EFY+05, EIG01, GW01, HT06, HH09, JKK+01, KCR04, KL00, Kun01, KT00, LZ09, LLS05a, LKL05, LZ01, LZF04, LWS05, LPZ06, LJ05b, LSC03, LL01, LSKC05, MM01a, MNS01, Nak01, OMT02, PJH01, PJK01, PR01, PBM+07, Qu01, Sam09, SOHS01, SDFH00, SDF01, SSFC09, SC02a, SY01b, Shi08, SP04, SLT01, SPK08, VVS01, VHP01, VK07, WCJ09, WH09, WY09, WWL+02, WLT05b, XFZ01, YWWS09, ZTP05, ZWC02, AK03a, AAPP07, BCKK05, CC02b, Che08b, CYH+07, CCD+04, CS05a, CC04c, CMB02, CKL05, DSP01, FWL08, FMS05, GA03, IHCC05, JDJ01, JA02, KP00, LDD07, Lin00a, Lin01a, LLC06a, LLC06b, MB08, MCHN05, PK03, Ren09, mSgFl05].
watermarking [WJP07, WNPQ08, Way02b, Way09, WMDR08, XMST07, YZDW07, YPSZ01, ZLZS07]. Watermarks [Ben00, BB00a, MLC01, Sug01, WC03, 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, K003, KO00, LTW05, Sh000a, YZ00, AK02a, AGGM06, AGGM10, BYJK04, CHY05b, CJ04, Cla00b, GKK+07, HR07, HRS08, JZ09, KK07, KKKP05, KK03, LW04, LPM05, LQ08, LKL01, Mc02a, Po00, 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]. Weakness [SW05, SZS05, YPKL08]. Weaknesses [FMS01, He02, KCL03, KCC05, SGGB00].
Weapons [RR03b]. Weather [WWL+02].
Web [Mar05a, BFG05, BFG08, Hii06, An01c, An02e, An03c, AEV+07, BFG04, BC04b, CCCY01, Coc01a, Coc02a, Coc02b, CZZ+01, De07, DMSW09, FSSF01, GS02a, GSVC02, HM05, JRB+06, KCD07, LWK00, LLS05b, LXM+05, MMPM09, PM00, RR04, Sam09, SSS06, Sch01a, SBG07, TMMM05, WA06, YSS+01]. Web-Based [An01c, Sch01a, YSS+01]. Web-enabled [CCCY01].
webcam [McN03].
webrelay [Zha00]. Weight [CH07c, GKO2, WT02].
Weighted [BTW05, BTW08, SC02c, YZ00].
Weil [BF01b, BF03, Jou02, Kir03].
Well [WWPG00]. Welschenbach [Ter08]. Welsh [Rot07].went [AJ08]. WEP [SIR04]. were [Han06]. Wesley [Puc03].
West [Fra01, Jue04, Syv02, Wri03]. Westbridge [An02e]. Western [CZB+01]. Wet [CC09].
Weyl [Sug03]. WG [DFPS06]. WG11.1 [ELvS01]. WG11.1/WG11.2 [ELvS01]. WG11.2 [ELvS01]. WG8.8 [DFCW00].
Wheelers [ARB08, Bar05]. Where [Bur06, Pen01a]. Where [Tee06]. WHIM [JA02]. WHIRLPOOL [RB01]. Whisper [NABG03]. Whitening [Oni01]. Whitfield
Who [CZB+01, Urb01, Hau06]. whole [CPG+04]. Wi [Puz04, Sty04, VG04, FMA02, Bar03]. Wi-Fi [Sty04, Bar03]. Wi-Foo [Puz04, VG04]. wicked [Lud05]. Wi-Fi [Sty04, Bar03]. Wi-Foo [Puz04, VG04]. wicked [Lud05]. Wide [DR02a, SBB05]. Width [OT03b]. Width-OT03b]. Wiener [Du08, Du09]. WIESS [USE00b]. Wiley [And04, Gra01, Kir01a]. Will [Ort00, Cla00b, Fur05]. William [Pag03]. Williams [Mul01a]. Window [OT03a, SSST06]. Windows [USE00a, DGP07a, DGP07b, DGP09, HB06, WD01a, Wit01]. Wins [Bar00b]. Wired [Gil07, Pot07]. Wireless [AEAQ05, Bar03, BCH+00]. ECM00b, Fin06. KH05. HD101, L1N+08, Pan03, PJDH09. Pot03, Puz04. Sin01a, Sty04, SYL05. VGM04. YSR01, ZYN08, ZWCY02, Bad07, BB03a, BGB+02, CCMT09, Cha05b, GW08, GG05b, JRR09, KKTZ09, KB09, LDH06, LPV+09, LW05a, Lin07, Lop06, MJF+08, NC09, NLD08, PCSV07, Par04, Pat02a, Pot02b, Pot07, SLP07, SZ08, TP07, Vac06, Wan04a, YTW05, CS08b, ECM00a, PDS009]. Wiretapping [Cho08a, DL98, Jan08a, DL07]. WISA [CSY09]. Within [MR02a, CHM+02, MR02b]. Without [BCL+05b, Bha01c, BB04, BG07, Har06, NA07, Ano03b, Cho1a, CCK04b, CYH04, CCH05, CTH08, CJO4, CDD07, CNV06, DK01, KG09, Ku04, LV07, LW04, LKY05b, LL06, LCFZ05b, Lys07, MP02, Mar07, FSO4c, RG09, WH01, YW05, YRY05b, ZW05a]. Withstanding [DFS04]. Wits [Bud00a, Bud02]. WLAN [SSM+08]. WLAN/cellular [SSM+08]. Woes [BTT02]. Women [FF01b]. won [Hau03]. Worcester [KP01]. Word [HR00, SKU+00]. Word-Oriented [HR00, SKU+00]. Wordlengths [PG05]. words [GS01, Max06, NS01a, VS01]. Work [DFG01, DWN05, Fox00]. Working [DFCW00, ELvS01, KB00]. workload [BGM04]. Works [Net04]. Workshop [ACM05a, Ano05b, AL06, BDZ04, BBD09, BD08, C005, Chr00, Chr01, CCMR02, CCMR05, CS09, DR02c, Des02, GH05, IEE01b, J00, J004, KKP02, KCR04, KGL04, Kin01, KP01, KNP01, LST+05, MJ04, MS05a, Mat02, MZ04, NP02a, NH03, PK03, PT06, RS05, RRS06, RM04, Sch00b, Sch01d, TB02, USE00b, Y001, Vau05a, WK03, Ytr06, AM07, AJ01a, BCK05, Bir07, CKL05, GKS05, HH04, HH05, HA00, ST01d]. World [Ber03, G05a, HW01, Nik02a, Nik02b, Sch004, Sty04, YKMB08, Ano03b, Ark05, Bel07a, HHC06, Hus01, KPS02, Kee05, Lie05, Lun09, Rob02, Rob09, Sch03, SL07, Bec02, Bud00a, Bud02, Hau03, Kov01, MH09, OC03, Sty04, Sec04]. Worlds [Wil01b]. Worm [LJL05, CSW05]. Worms [ZGT05]. Worst [CCM05, HRS08, Mic02a, Mic02b, Pei09]. worst-case [HRS08, Mic02a, Mic02b, Pei09]. worst-case/average-case [Mic02b]. Woz [Bar00c]. WPA [OM09]. Wrapper [Ol00]. Write [BB02]. Writers [G006]. Writing [HL03, Jan06, Kah67a, Kah67b, Kah96, Gas01]. Writings [Cop04b]. WS [JRB+06, RR04]. WS-Policy [RR04]. WS-Security [JRB+06, RR04]. WSDL [Bar00c]. WTLS [Vau02]. WTMAU [ECM00a, ECM00b]. WTMAU-SD [ECM00a]. Wu [BCW05, CHY05a, CWJT01, HL05c, MS03a, YY05b]. Wu-Lin [YY05b]. Wuhan [TTZ01]. WW [Sal00a]. WWII [WD01b].
RR04, ÜG08, Uri01, UST01a]. XMT [SG07].
XrML [Bar00a]. XTEA
[CV05, HHK+04, MHL+02]. XTR
[LW02, LV00, LNS02, Ver01].

Yahalom [Pau01]. Yang
[KJY05, WL05, YWC05]. Yang-Shieh
[YWC05]. Yao [BPS08, BDNN02, ZD05].

Z-parameter [Wue09]. z10
[Web08]. Z [ADH+07]. Zealand [Zhe02b].
Zeilinger [Duw03]. Zero [AS01b, APV05,
BP04, Con01, DPV04, DFS04, DDO+01,
HNO+09, IKOS07, LMS05, LHL+08, MR01b,
MV03a, Pas05, Ros00, Ros06a, CSW05,
Dam00, PBD07, KK07]. zero-day [CSW05].

Agreste:2008:NAP
Santa Agreste and Guido Andaloro. A new
approach to pre-processing
digital image for wavelet-
based watermark. Journal
of Computational and
Applied Mathematics, 221(2):
REFERENCES


REFERENCES


REFERENCES


[Abe04] Masayuki Abe. Combin-


[ABR01] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The oracle Diffie–Hellman


Ambainis:2009:NEQ


Ateniese:2000:PPS

Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Bellare [Bel00], pages 255–??
REFERENCES


[ACM03c] ACM, editor. Proceedings of the Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium on
References


[ACM07] ACM, editor. STOC ’07: proceedings of the 39th Annual ACM Symposium on
REFERENCES


ACM:2008:SPA


ACM:2009:SPA


ACM:2010:PAI


Algesheimer:2002:ECM


Alvarez:2005:EBS


Ahmad:2007:ADE

Imtiaz Ahmad and A. Shoba Das. Analysis and detection of errors in implementation of SHA-512 algorithms on FPGAs. The
REFERENCES


Anyanwu:2009:DCS


Avanzi:2006:ESM


Arnold:2007:CSE


Adikari:2009:HBT


Adleman:2003:TLP


An:2002:SJS

Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature

**Arazi:2005:RPK**


**Alvarez:2005:SSS**


**Atighehchi:2009:EPA**


**Anton:2007:HEW**


**Augot:2003:PKE**


**Abadi:2004:PA**

Martín Abadi and Cédric Fournet. Private authentication. *Theoretical Comput-
REFERENCES


Abe:2004:ASF
Masayuki Abe and Serge Fehr. Adaptively secure Feldman VSS and applications to universally-composable threshold cryptography.

Atallah:2005:DEK

Ateniese:2006:IPR
Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage.

Acquisti:2009:PSS
Alessandro Acquisti and


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

Agrawal:2003:WRD


Armington:2002:BAI


Ahmad:2007:CSS


Ahmad:2008:ATT


Ahmadi:2008:PFS


Askarov:2008:CMF


Aoki:2001:CBB

Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda,
REFERENCES


REFERENCES


Attali:2001:SCP


Aid:2008:NSA


Avoine:2008:CIT


Al-Jarrah:2008:NKM


Abe:2002:KES

REFERENCES

CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL [Aki09]

Agrawal:2002:WRD

Armknecht:2003:AAC

Akinwande:2009:AHC

Amir:2004:PGK

Agrawal:2002:PP

Acicimez:2006:PSB
Omer Acicimez, Cetin Kaya Koç, and Jean-Pierre Seifert. On the power of simple branch prediction analysis. Technical report, School
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Anon:2000:AIIH
Anonymous. AES IP hardware encryptor introduced. [Ano00a]

Anon:2000:AIah

Anon:2000:CRR
Anonymous. China relaxes rules on encryption products. [Ano00c]

Anon:2000:CCI

Anon:2000:CLII

Anon:2000:EES
Anonymous. European encryption still safer than US versions. [Ano00f]

Anon:2000:GBE
Anonymous. Governments back down on encryption regulations. [Ano00g]

Anon:2000:PESa
Anonymous. PGP encryption software granted global export license. [Ano00h]
*Network Security*, 2000(1):1,
Anonymous:2000:PTD


Anonymous:2000:SES


Anonymous:2000:UAS


Anonymous:2000:VAS


Anonymous:2001:AAPb


Anonymous:2001:ANT

REFERENCES


[Ano01i] Anonymous. Looking on the bright side of black-box cryptography (transcript of discussion). Lec-
REFERENCES


Anonymous:2001:PKC


Anonymous:2001:SCS


Anonymous:2001:DEC


Anonymous:2002:IHB


Anonymous:2002:NSD


Anonymous:2002:PPD

Anonymous. Products: Palm Digital Media’s eBook publishing tools; Veridicom’s fingerprint authentication module; high-speed de-

Anonymous:2002:PSS


Anonymous:2002:PFQ


Anonymous:2002:QCQ


Anonymous:2002:QCR


Anonymous:2002:RUB

Anonymous. Review of US bombes. IEEE An-
REFERENCES


Anonymous: 2003: TMC

Anonymous: 2003: NAW

Anonymous: 2003: NUP

Anonymous: 2003: TMP
<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>unknown</td>
<td>Anon</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>unknown</td>
<td>Anon</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>unknown</td>
<td>Anon</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>1461</td>
<td>Anonymous</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>1588</td>
<td>P. A. Cataldi</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>1883</td>
<td>I. M. Pervushin</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>1911</td>
<td>R. E. Powers</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>1913</td>
<td>E. Fauquembergue</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>1876</td>
<td>E. Lucas</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>1750</td>
<td>L. Euler</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1913</td>
<td>E. Fauquembergue</td>
</tr>
<tr>
<td>15</td>
<td>127</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>Anon</td>
</tr>
<tr>
<td>18</td>
<td>3217</td>
<td>1957</td>
<td>H. Riesel</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1961</td>
<td>A. Hurwitz</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>1963</td>
<td>D. B. Gillies</td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>1971</td>
<td>B. Tuckerman</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>L. C. Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>H. Nelson &amp; D. Slowinski</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1982</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>1988</td>
<td>W. N. Colquitt &amp; L. Kurosky</td>
</tr>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td>Anonymous</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>D. Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>756839</td>
<td>1992</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski &amp; Gage</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Armengaud et al. (GIMPS)</td>
</tr>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Anonymous</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence et al. (GIMPS)</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, Wolfman &amp; Nowak (GIMPS)</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala et al. (GIMPS)</td>
</tr>
<tr>
<td>39</td>
<td>13466917</td>
<td>2001</td>
<td>M. Cameron (GIMPS)</td>
</tr>
<tr>
<td>40</td>
<td>20996011</td>
<td>2003</td>
<td>M. Shafer (GIMPS)</td>
</tr>
<tr>
<td>41</td>
<td>24036583</td>
<td>2004</td>
<td>Josh Findley (GIMPS)</td>
</tr>
<tr>
<td>42</td>
<td>25964951</td>
<td>2005</td>
<td>Martin Nowak (GIMPS)</td>
</tr>
<tr>
<td>43</td>
<td>30402457</td>
<td>2005</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
</tr>
<tr>
<td>44</td>
<td>32582657</td>
<td>2006</td>
<td>Curtis Cooper &amp; Steven Boone (GIMPS)</td>
</tr>
<tr>
<td>45</td>
<td>37156667</td>
<td>2008</td>
<td>Hans-Michael Elvenich, George Woltman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>46</td>
<td>42643801</td>
<td>2009</td>
<td>Odd Magnar Strindmo (GIMPS)</td>
</tr>
<tr>
<td>47</td>
<td>43112609</td>
<td>2008</td>
<td>Edson Smith, George Woltman, Scott Kurowski (GIMPS)</td>
</tr>
<tr>
<td>48</td>
<td>57858161</td>
<td>2013</td>
<td>Curtis Cooper, George Woltman, Scott Kurowski, and others</td>
</tr>
<tr>
<td>49</td>
<td>72407281</td>
<td>2016</td>
<td>Curtis Cooper (GIMPS)</td>
</tr>
<tr>
<td>50</td>
<td>77232917</td>
<td>2018</td>
<td>Jon Pace (GIMPS)</td>
</tr>
</tbody>
</table>


Anonymous. New generation Java smart cards. *Card Technology Today*, 16(3):10–11,
Anon

Anonymous:2005:CEC

Anonymous:2005:WAS

Anonymous:2006:JHD

Anonymous:2006:SSD

Anonymous:2006:SQE

Anonymous:2007:CPSh

Anonymous:2007:CPSf
REFERENCES

Anonymous:2008:KAD

Anonymous:2008:RCB

Anonymous:2008:RES

Anonymous:2008:SHS

Anonymous:2009:DSS

Anonymous:2012:SHS
REFERENCES


Ateniese:2001:SRC


Amir:2001:FAC


ANSI:2005:AXP


Abe:2000:PSP

REFERENCES


REFERENCES


Arnold:2001:AWB


Agrawal:2003:MCA


Abe:2001:SPA


Adelsbach:2001:ZKW


Agung:2001:ICI

[AS01c] I. Wiset Agung and Peter Sweeney. Improvement and comments on image wa-

[Ash03] Julian Ashburn. *Practical Biometrics: From As-
piration to Implementation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 1-

[Asenjo:2002:AES] Juan C. Asenjo. The Advanced Encryption Stan-
dard — implementation and transition to a new crypto-

[Aciicmez:2005:IBB] Onur Aciciçmez, Werner Schindler, and Çetin K. Koç. Improving Brumley and Boneh timing attack on unprotected SSL imple-

DEN ???. ISSN 1540-7993 (print), 1558-4046 (electronic).


REFERENCES

Arnold:2004:IPN


Avanzi:2003:CAD


Aalberts:2000:DSB


Abadi:2005:SAC


Abadi:2008:SAC


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, China,*
REFERENCES


**Blanton:2006:SRF**


**Bagnulo:2002:PAA**


**Badra:2007:AWC**


**Baier:2001:ECP**


**Baier:2001:ECS**

Baigneres:2008:QSB


Bao:2004:CPK


Baran:2000:NVB


[Bar00b] Nicholas Baran. News and views: More on tiny transistors; Open Source repository launched; design contest promotes new software tools; and then there’s a decryption contest; Fred Brooks wins ACM Turing Award. *Dr. Dobb's Journal of Software Tools*, 25(3):18, March 2000. CODEN DDJOEB. ISSN 1044-789X. URL http://sourceforge.net/.

Bamford:2002:BSA


Baran:2000:NVM

Baran:2000:NVR

[Bar00c] Nicholas Baran. News and views: RSA algorithm in the public domain; Woz joins the Inventors Hall of Fame; entangled photons mean faster, smaller ICs; BEHEMOTH mothballed; Advanced Encryption Standard selected; SGI releases SDK as open source; WSDL spec released. Dr. Dobb’s Journal of Software Tools, 25(12):18, December 2000. CODEN DDJOEB. ISSN 1044-789X.

Barr:2002:IC


Barkan:2006:CCP


Barker:2006:RO


Bard:2009:AC

Bauer:2000:DSM


Bauer:2001:PPGa


Bauer:2001:PPGb


Bauer:2001:PPUb


Bauer:2002:DSM


Bauer:2002:PPB


Bauer:2003:PPAa


Bauer:2003:PPAb

REFERENCES

Baudet:2005:DSP

Bauer:2007:DSM

Blakley:1979:RSA

Benedens:2000:TBD

Buchmann:2000:ECC

Barkan:2002:HMW


REFERENCES

Bernstein:2009:PQC


Beimel:2000:CFS


Bellare:2001:KPP


Bartolini:2008:EIS


Barkan:2003:ICO

Elad Barkan, Eli Biham, and Nathan Keller. In-

[Bertoni:2003:EAD]


[Bellare:2001:OCH]


[Bellare:2009:HPK]

REFERENCES

delberg, Germany / London, UK / etc., 2009. ISBN ????. LCCN ???. URL ???.


Backes:2005:PKS


Blundo:2005:SCN


Bergadano:2001:CSA


Brier:2001:CRS

Eric Brier, Christophe Clavier, Jean-Sébastien Coron, and David Naccache. Cryptanalysis of RSA signatures with
fixed-pattern padding. In Kilian [Kil01a], pages 433–??. ISBN 3-540-42456-3 (paper-
back). LCCN QA76.9.A25
no.2139. UK £47.00. URL
com/link/service/series/
0558/bibs/2139/21390433.
htm; http://link.springer-
ny.com/link/service/series/
0558/papers/2139/21390433.
pdf.

Carlo Blundo, Stelvio Cimato, and
Alfredo De Santis. Visual
cryptography schemes
with optimal pixel expan-
sion. *Theoretical Com-
CODEN TCSCDI. ISSN
0304-3975 (print), 1879-2294
(electronic).

Javier D. Bruguera, Marius
Cornea, Debjit Das-
Sarma, and John Harri-
son, editors. *Proceedings of
the 19th IEEE Symposium
on Computer Arithmetic,
June 8–10, 2009, Portland,
Oregon, USA*. IEEE Com-
puter Society Press, 1109
Spring Street, Suite 300,
Silver Spring, MD 20910,
USA, 2009. ISBN 0-7695-
3670-0. ISSN 1063-6889.
URL http://www.ac.usc.
es/arith19/.

H. Barnum, C. Crepeau,
D. Gottesman, A. Smith,
and A. Tapp. Authentic-
tion of quantum mes-
sages. In IEEE [IEE02],
pages 449–458. CODEN
ASFPDV. ISBN 0-7695-
1822-2. ISSN 0272-5428.
LCCN QA267. URL http:
//ieeexplore.ieee.org/
iel5/8411/26517/01181969.
pdf?isnumber=26517&prod= CNF&arnumber=1181969&arSt=
+449&ared=+458&arAuthor=
Barnum%2C+H.%2B+Crepeau%2C+
2C%2B+Gottesman%2C+D.%2B+Smith%2C+A.%2B+Tapp%2C

REFERENCES


Brown:2000:PCW


Breunesse:2005:FMS


Boneh:2007:CCS


Butler:2006:FAK


Barni:2005:DWI


Bao:2005:PSS

REFERENCES

Barak:2005:SCA


Bresson:2001:PAG


Bresson:2002:DGD


Bresson:2002:GDH


Bolle:2003:GB

pp. LCCN TK7882.B56 G85
2003. US$49.95.

Bresson:2007:PSA

Emmanuel Bresson, Olivier Chevassut, and David Pointcheval.

Bellavista:2002:JLD


Bao:2005:R


Biham:2000:CA

REFERENCES

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

**Boneh:2000:CRP**


**Bourbakis:2003:SBC**


**Bozzano:2004:AVS**


**Burmester:2004:HPK**


**Buchmann:2008:PQC**


**Biryukov:2003:CS**

REFERENCES


Blundo:2003:COT


Bolosky:2000:FSD


Bao:2001:SPD


Boneh:2001:LBM


Bodei:2002:PAP

Chiara Bodei, Pierpaolo Degano, Riccardo Focardi, and Corrado Priami. Primitives for authentication in

**Bodei:2005:APS**


**Bao:2001:CTS**


**Bhattacharyya:2009:VPA**


**Biham:2002:EDL**


**Biham:2002:LCR**

REFERENCES

Biryukov:2009:KRA


Blundo:2000:VCG


Boreale:2002:PTC


Bertoni:2009:RPK

REFERENCES


REFERENCES


REFERENCES

Bellovin:2004:IRS

Belfield:2007:SUC

Bella:2007:FCS

Bello:2008:OPR

Bruss:2007:QCS

Benedens:2000:AIW

Benantar:2001:IPK
REFERENCES


**Benson:2001:VS**


**Benantar:2002:IPK**


**Benson:2004:VS**


**Berson:2003:CAB**


**Bernstein:2007:SFS**

REFERENCES


Biham:2000:IID


Babbage:2001:MHO


Boneh:2001:IBE


Boneh:2001:EGS


Boneh:2003:IBE


Boldyreva:2005:ARO


December 2008. CODEN ATPSDT. ISSN 0164-0925 (print), 1558-4593 (electronic).


REFERENCES


Bertoni:2003:EAA


Bucci:2003:HSO


Branovic:2004:WCE


Boneh:2005:EDF

REFERENCES


[Boneh:2005:CRB] Dan Boneh, Craig Gentry, and Brent Waters. Collision resistant broadcast encryption with short ciphertexts and private keys. In Shoup [Sho05a], pages 258–?? ISBN 3-540-28114-2. ISSN 0302-9743 (print), 1611-3349 (elec-
REFERENCES


REFERENCES


Biham:2002:HDE

[Bih02] Eli Biham. How to de- 
crypt or even substitute 
DES-encrypted messages in 
$2^{28}$ steps. Information Pro-
cessing Letters, 84(3):117– 
124, November 15, 2002. 
CODEN IFPLAT. ISSN 
0020-0190 (print), 1872-6119 
(electronic).

Biham:2003:ACE

[Bih03] Eli Biham, editor. Ad-
vances in cryptology — 
EUROCRYPT 2003: In-
ternational Conference on 
the Theory and Applica-
tions of Cryptographic Tech-
niques, Warsaw, Poland, 
May 4–8, 2003: Proceed-
ings, volume 2656 of Lecture 
Notes in Computer Science. 
Springer-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc., 
ISBN 3-540-14039-5 (paper-
back). ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25 
E964 2003. URL http://
link.springer-ny.com/
link/service/series/0558/
0558/papers/2656/2656.

Beimel:2000:RSC

[BIM00] Amos Beimel, Yuval Ishai, 
and Tal Malkin. Reduc-
ing the servers computation 
in private information re-
trieval: PIR with prepro-
cessing. In Bellare [Bel00], 
pages 55–?? ISBN 3-540-
67907-3. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25 
C79 2000 Bar. URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1880/18800055.htm; 
http://link.springer-
ny.com/link/service/series/ 
0558/papers/1880/18800055.
pdf.

Bajard:2003:EMG

[BINP03] J.-C. Bajard, L. Imbert, 
C. Negre, and T. Plan-
tard. Efficient multiplication 
in $\text{GF}(p_k)$ for elliptic curve 
cryptography. In Bajard and 
Schulte [BS03], pages 181–
ISSN 1063-6889. LCCN ???
URL http://www.dec.usc.
es/arith16/. IEEE order 
no. PRO1894.

Bajard:2005:AOP

[BIP05] Jean-Claude Bajard, Lau-
rent Imbert, and Thomas 
Plantard. Arithmetic op-
erations in the polynomial 
modular number system. In 
IEEE [IEE05b], page ?? 
ISBN ?? LCCN ???. URL 
http://arith17.polito.
it/final/paper-168.pdf.

Biryukov:2007:FSE

[Bir07] Alex Biryukov, editor. Fast 
software encryption: 14th in-

REFERENCES


REFERENCES

Bjorn:2005:BHM


Backes:2002:DCS


Boni:2000:NGT


Burnside:2005:CCP


Barker:2006:RRN

Elaine Barker and John Kelsey. Recommendation
**REFERENCES**


**Breveglieri:2006:GEI**


**Barker:2007:RRN**


**Barreto:2002:EAP**


**Breveglieri:2007:OCA**


**Bellare:2004:BPR**

Mihir Bellare, Tadayoshi Kohno, and Chanathip Namprempre. Breaking and provably repairing the SSH authenticated encryption scheme: a case study of the encode-then-encrypt-
REFERENCES


[BL00] Michael Andrew Black. A treatise on data encryption and an example of the
REFERENCES

black algorithm. Thesis (M.A.), University of California, Santa Barbara, Santa Barbara, CA, USA, 2000.

[Bla02a]

Blanchet:2001:ACP


[Bla01a]

Blanchet:2001:ECP


[Bla01b]

Blaze:2001:LYS


[Bla01c]

Blanche:2002:SAS


[Bla02b]

Blaze:2003:FCI

REFERENCES


Burmester:2009:UCR


Bleumer:2007:EPS


Bao:2006:CIB


Berbecaru:2001:CPK


Brassard:2000:SAP

Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Security aspects of practical quantum cryptography. *Lec-
REFERENCES

ture Notes in Computer Science, 1807:289–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:\[BLST01\]
link.springer-ny.com/link/service/series/0558/bibs/1807/18070289.htm;

<table>
<thead>
<tr>
<th>Bozga:2006:PBA</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Blunden:2009:RAE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Banks:2001:CAS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Blunden:2009:RAE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Blunden:2009:RAE</th>
</tr>
</thead>
</table>
REFERENCES


REFERENCES


REFERENCES

Boyko:2000:PSP


Borselius:2002:VTS


Borselius:2002:PAU


Bucmann:2006:PCL


Boneh:2003:SSS

REFERENCES


[BNS02] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The power of RSA inversion oracles and the security of chaum’s RSA-based blind


REFERENCES

C79 2001; QA267.A1 L43
no.2139. UK£47.00. URL
com/link/service/series/|
0558/bibs/2139/21390275.|
htm; http://link.springer-
ny.com/link/service/series/|
0558/papers/2139/21390275.|
pdf.

[Bon03] Dan Boneh, editor. Advances
in Cryptology—CRYPTO
2003: 23rd Annual Inter-
national Cryptology Confer-
ence Santa Barbara, Cal-
ifornia, USA, August 17–
21, 2003 Proceedings, vol-
ume 2729 of Lecture Notes in
Computer Science. Springer-
Verlag, Berlin, Germany /
Heidelberg, Germany / Lon-
don, UK / etc., 2003. CO-
DEN LNCSD9. ISBN 3-540-
40674-3. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2003. URL http://
link.springer-ny.com/
link/service/series/0558/|
tocs/t2729.htm; http://
www.springerlink.com/
openurl.asp?genre=issue&|
issn=0302-9743&volume=
2729; http://www.springerlink.|com/openurl.asp?genre=
volume&id=doi:10.1007/|
b11817.

pairings based crypto-
graphy. In IEEE [IEE07],
pages 19–26. ISBN 0-7695-
3010-9. ISSN 0272-5428.
URL http://ieeexplore.
ieee.org/servlet/opac?
punumber=4389466. IEEE
Computer Society order
number P3010.

[Boo05] J. V. Boone. A brief history
of cryptography. Naval Institute
Press, Annapolis, MD, USA,
+ 192 pp. LCCN TK5102.85
www.loc.gov/catdir/toc/
ecip055/2005000009.html.

[Bor00] Kevin Borras. A trans-
port revolution: Turkey gets
the smart card bug. Toll-
trans, pages 36–38, Septem-
ber 2000.

[Bor01] Michele Boreale. Sym-
bolic trace analysis of cryp-
tographic protocols. Lecture
Notes in Computer Sci-
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/|
bibs/2076/20760667.htm;
http://link.springer-
ny.com/link/service/series/|
0558/papers/2076/20760667.|pdf.
REFERENCES


REFERENCES


REFERENCES

Blanchet:2005:VCP

Beissinger:2006:CUM

Baer:2007:CIS

Bellare:2000:AKE

Borst:2001:CSC

Bellare:2005:ISA
Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. In Shoup [Sho05a], pages
REFERENCES


REFERENCES

Bellare:2000:ETE


[BR00a]

Black:2000:CMA


[BR01]

Black:2002:BCM

REFERENCES


Bellare:2004:CBG


Bugliesi:2005:NIP


Bellare:2006:MPP


Bhatnagar:2009:RRW


 Brands:2001:RPK


Brandt:2001:CPS


Brown:2005:CEC

REFERENCES


[Browne:2005:DEP]


[Brustoloni:2006:LEN]


[Bierbrauer:2000:AIW]

[BS00b] Alex Biryukov and Adi Shamir. Cryptanalytic time/memory/data tradeoffs for stream ciphers. Lecture
Barrett:2001:SSS


Bigun:2001:AVB


Biryukov:2001:SCS


Boneh:2001:UBE

REFERENCES

171


Bajard:2003:ISC


Bo:2001:EID

Bo:2001:SCD

Bounklong:2002:ICA

Stéphane Bounkong, David Saad, and David Lowe. Independent component anal-

Barrett:2005:SSS


Barrett:2005:SSS


Bo:2001:SCD


Bounklong:2002:ICA


Bounklong:2002:ICA

Brisbane:2000:RBW


Bresson:2002:TRS


Blake:2004:AEC


Blake:2005:AEC

REFERENCES

number-theory/advances-elliptic-curve-cryptography

Bhargav-Spantzzel:2007:PPM


Buchmann:2002:ICP


Barak:2003:TRN


Biryukov:2001:RTC


Bethencourt:2009:NTP

REFERENCES

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

**Biehl:2002:NDP**

**Beimel:2005:CIW**
Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In Kilian [Kil05], pages 600–??. CODEN LNCSD9.

**Beimel:2008:CIW**

**Blak:2002:SCA**

**Buchmann:2000:CTC**
Johannes Buchmann, editor. *Coding theory, cryptography, and related areas: proceedings of an International Conference on*


REFERENCES


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


Boesgaard:2004:RNH


Baker:2007:ISU


Blake-Wilson:2002:RUE


Bar-Yossef:2004:ESQ

Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In ACM [ACM04b],

Blair:2000:BD

Butler:2000:NSA


Bellare:2003:FSP


[BY03]


[BYJK04]

Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In ACM [ACM04b],

[ACM04b]

[ACM04b]
REFERENCES

Bar-Yossef:2008:ESQ


Bertlmann:2002:QUB


Bond:2003:DTA


Borders:2005:CHP


Carrington:2002:EDS


Sta:2003:NTC

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

Sta:2006:NTS

CACM Sta. News track: Super game plan; E-learning roots disputed; Chinese history; U.K. seeks popular science input; encryption


REFERENCES

(180)

180


Caprara:2001:PSR


Carriere:2000:PSC


Carter:2001:SCT


Carlet:2002:LCC


Casey:2002:HCC


Casselman:2006:MTE

REFERENCES

181

php/C/30. The front cover of this issue displays eight pages of Alan Turing’s description of the Enigma machine. The issue is a special tribute to Kurt Gödel for the centenary of his birth.

Cobas:2001:CTA


Cachin:2000:OFS


Cooper:2005:AAP


Chan:2001:CRP


Carline:2002:NWT

Dylan Carline and Paul Coulton. A novel watermarking technique for LUT based FPGA designs. *Lec-
REFERENCES

Chan:2002:SLI [CC02b]

Cachin:2004:ACE [CC04a]

Chang:2004:SES [CC04b]

Cousot:2004:AIB [CC04c]

Chan:2005:STM [CC05a]
REFERENCES

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


REFERENCES


REFERENCES

Chang:2004:IDA

Chang:2004:SOT

Chang:2009:PCC

Christianson:2001:PKC

Christianson:2002:SPI

Choi:2005:JMA
REFERENCES


REFERENCES


Ceselli:2005:MAI


Cimato:2005:ICV


Cramer:2001:CRS


Cimato:2007:CVC


Cramer:2005:CMS


Cramer:2005:SCP

[CDI05] Ronald Cramer, Ivan Damgård, and Yuval Ishai. Share conversion, pseudorandom
REFERENCES


Cavallar:2000:FBR


Cortier:2006:SAP


Cramer:2000:GSM


Chawla:2005:TPP

REFERENCES

Coron:2005:MDR

Cramer:2001:MCT

Chapman:2001:PEA

Castiglione:2007:TAD

Chen:2005:NVW
Zhenyong Chen, Junhui Deng, Long Tang, and Zesh-


Cohen:2006:HEH

Courtois:2001:HAM

Cramer:2005:BBS

Climent:2006:NEC

Chodowiec:2003:VCF
Cranor:2005:SUD


Candebat:2006:SPM


Chodowiec:2001:ETG


Caballero-Gil:2009:GBA


Catalano:2000:CIS

REFERENCES


REFERENCES

aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=APCPCS000963000002000935000001&
amp;idtype=cvips.

Canovas:2002:DSB


Cox:2002:SP9


Cimato:2003:SCN

[CGP03] Stelvio Cimato, Clemente Galdi, and Guiseppe Persiano, editors. Security in communication net-


Cayrel:2008:SIS


Chow:2009:ADN

REFERENCES

1089-7089 (print), 1538-7305 (electronic).

Crotch-Harvey:2000:OPR


Chang:2001:TFG


Chien:2007:SUL


Chung:2007:ASF


Chung:2007:MRA


Chaum:2004:VSB

David Chaum. E-voting: Secret-ballot receipts: True
REFERENCES


REFERENCES


Chen:2008:MWS


Coulter:2001:GAH


Chien:2008:EP


Chien:2008:SCA


Choi:2009:KDK


Coron:2001:GGC

Coron:2001:OCC


Coppersmith:2002:CSC


Canetti:2003:FSP


Canetti:2005:ASN


Cheon:2008:PST

Jung Hee Cheon, Nicholas Hopper, Yongdae Kim, and

Chang:2002:IBO


Chao:2009:HCS


Chen:2002:CPK


Choi:2006:CHP


Choo:2008:PLP

Chowdhury:2008:CBG


Christianson:2000:SPI


Christianson:2001:SPI


Canetti:2005:HA


Chen:2002:AMT

Cornea:2002:SCI

Churchhouse:2002:CCJ

Canvel:2003:PIS
Brice Canvel, Alain Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a SSL/TLS channel. In Boneh

Chang:2005:IL

Chang:2005:NMS

Cimato:2002:DAP
Stelvio Cimato. Design
REFERENCES


Chen:2005:EDS


Cornwall:2004:AAM


Choie:2005:EIB


Chin:2006:HSI


Clarke:2000:VSP

REFERENCES

Coron:2000:NAP

Coron:2002:UPS

Chien:2001:MRL

Chien:2003:CMV
Hung-Yu Chien, Jinn-Ke...

Chien:2004:SIS

Canetti:2002:UCN

Cook:2006:CEG

Cheon:2002:IID
REFERENCES


REFERENCES

Coron:2000:FLA


Coron:2001:SSL


Canetti:2003:RCC


Cheon:2006:KPC


Cachin:2001:SEA

Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup. Secure and ef-
References

[102x681] REFERENCES

[102x681]212

Cathalo:2003:NTT


Chevalier:2008:CRS


Chen:2005:CLR


Chen:2007:CRA


[CL02c] Paul Crowley and Stefan Lucks. Bias in the LEVIATHAN stream cipher.
REFERENCES


[CL07] Ramaswamy Chandramouli and Philip Lee. Infrastructure standards for smart

Chang:2008:AWM


Chien:2009:EBL


Chang:2001:ASM

REFERENCES


REFERENCES


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

REFERENCES


REFERENCES


[Miguel Correia, Nuno Ferreira Neves, and Paulo Veríssimo. From consensus to atomic broadcast: Time-free Byzantine-resistant protocols without signatures.]


Cochran:2002:NVSb


Cochran:2002:NVW


Cochran:2003:NVC


Cohen:2003:FOV


Cole:2003:HPS


Constantinou:2000:CSC


Convery:2004:NSA

REFERENCES


Con:2009:GSH


Cook:2002:REJ


Cop:2000:C


Copeland:2004:COO


Copeland:2004:ETS


REFERENCES


[Cou02] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. Lecture Notes in
REFERENCES 226


Courtois:2003:AXA


Chatzikokolakis:2007:FAP


Cimato:2006:PVC


Chow:2004:UDL


Chen:2004:SEP

Ling Chen, Yi Pan, and Xia hua Xu. Scalable and efficient parallel algorithms for Euclidean distance transform on the LARPBS model. IEEE Transactions on Parallel and Distributed Systems, 15(11):
Catalano:2004:IIP


Canetti:2003:UCJ


Canetti:2007:CSH


REFERENCES


REFERENCES


Casey:2008:IFD


Chang:2008:DAP


Cusick:2009:CBF


Czeskis:2008:DED


Cai:2007:CSM


Crandall:2005:DUV


Chen:2008:CCS

L. Chen, W. Susilo, H. Wang, D. S. Wong, E. Daw-
REFERENCES

Chung:2009:ISA


Coron:2003:NAS


Chen:2008:BUK

REFERENCES

www.jucs.org/jucs_14_3/
bilateral_unknown_key_share.

Chu:2008:EOT

Chou:2009:ATI

Crawford:2001:FPV

Chiang:2008:CPB

Chang:2004:ASS

Cheung:2001:TPS
Collberg:2007:DGB


Chen:2009:FCV


Cheng:2001:NPT


Curtin:2005:BFC


Chaitanya:2008:QQM


Canteaut:2002:DCH

REFERENCES

CODEN LNCS09. ISSN
0300-9784 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/2332/23320518.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2332/23320518.
pdf.

[Cary:2003:MAC] Matthew Cary and Rama-
ratnam Venkatesan. A
message authentication code
based on unimodular ma-
trix groups. In Boneh
[Bon03], pages 500–512. CO-
DEN LNCS09. ISBN 3-540-
40664-3. ISSN 0300-9784
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2003. URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/2332/23320518.htm;
http://link.springer-ny.com/
link/service/series/0558/
papers/2332/23320518.
pdf.

[CvTMH01] Valer Canda, Tran van
Trung, Spyros Magliveras,
and Tamás Horváth. Sym-
metric block ciphers based
on group bases. Lecture
Notes in Computer Sci-

[Canteaut:2004:PCI] Anne Canteaut and Ka-
paleeswaran Viswanathan,
editors. Progress in crypt-
tology: INDOCRYPT 2004:
[ČVTMH01] 5th International Confer-
ence on Cryptology in In-
dia, Chennai, India, De-
cember 20–22, 2004: Pro-
ceedings, volume 3348 of
Lecture Notes in Com-
puter Science. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2004. CO-
DEN LNCS09. ISBN 3-540-
24103-2. ISSN 0300-9784
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
I5535 2004. URL http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0300-9784&volume=
2729; http://www.springerlink.
com/openurl.asp?genre=issue&
issn=0300-9784&volume=
2729; http://www.springerlink.
com/openurl.asp?genre=
volume&id=doi:10.1007/
b104579.

[Castro:2005:NRG] Julio César Hernández Cas-
tro and Pedro Isasi Viñuela.
New results on the ge-
etic cryptanalysis of TEA
and reduced-round versions
of XTEA. New Gener-
ation Computing, 23(3):
233–243, 2005. CODEN
NGCOE5. ISSN 0288-
3635 (print), 1882-7055
(electronic). URL http://
www.springerlink.com/
content/e018uh040400kh87/

[Canda:2001:SBC] Valéry Canda, Tran van
Trung, Spyros Magliveras,
and Tamás Horváth. Sym-
metric block ciphers based
on group bases. Lecture
Notes in Computer Sci-
REFERENCES


Chien:2005:NRS


Chen:2005:ENB


Chang:2008:EBD


Chang:2001:NSS

REFERENCES


Cheng:2005:RIC


DA03


Dal01


Damgaard:2000:ECZ


Damaj:2007:PAD

Danielyan:2001:AAE


Danas:2002:CUS


Davis:2001:ISV


Davis:2001:DSA


Davis:2001:DSE


Davis:2007:AAA


DeBrosse:2004:SBU


deBorde:2007:STF

REFERENCES


**Desmedt:** 2001: ERD


**[DBS01]**

**Doyle:** 2006: SCK


**[DBS+06]**


**diVimercati:** 2005: CSE


**[dCdVSG05]**

**DeBonis:** 2000: RV


**[DD00]**

**Dalkilic:** 2002: CPF

Mehmet Emin Dalkiliç and Gökhan Dalkiliç. On the


DeBonis:2004:RSS


Dolev:2003:NC


DeLooze:2007:PWS

Lori DeLooze. Providing Web service security in a federated environment. *IEEE*


[Dew08] Robin Dewson. Beginning SQL Server 2008 for developers: from novice to professional; [the quick and efficient path to proficiency in SQL Server 2008]. The expert’s voice in SQL Server.
REFERENCES


[DF01]


[DF07]


[Durante:2000:CA]


REFERENCES


DePalma:2004:CCS


Domingo-Ferrer:2001:CDS


Dodis:2003:IRP


DeSantis:2004:CKA


Domingo-Ferrer:2006:SCR

Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors. Smart Card Research and Advanced Applications: 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19–21, 2006. Proceedings, volume 3928 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Ger-


Debaert:2002:RRI


DiRaimondo:2003:PST


DiRaimondo:2005:NAD


DiRaimondo:2003:ADP


DoDis:2004:REK


Devanbu:2003:ADP


Devanbu:2004:FAX

REFERENCES

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

Dwork:2003:MBF


Dorrendorf:2007:CRNa


Dorrendorf:2009:CRN


Dorrendorf:2007:CRNb


denHartog:2008:TMC


Dhem:2003:EMR

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

[DHL06] Yan-Xiang Deng, Chao-Jang Hwang, and Jiang-Lung Liu. An object-oriented cryp-
tosystem based on two-level recon-
figurable computing ar-

[DHMR07] Vanesa Daza, Javier Her-
ranz, Paz Morillo, and Carla Ráfols. Cryptographic tech-

[DHR00] Yevgeniy Dodis, Shai Halevi, and Tal Rabin. A crypto-
tographic solution to a game theoretic problem. In Bellare [Bel00], pages 112–?? ISBN 3-540-67907-3. ISSN 0302-9743 (print), 1611-3349 (elec-


REFERENCES


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*

REFERENCES


Damgaard:2001:GSS


Delaune:2006:DPS


Donsez:2001:TMA


Damgaard:2001:PTR

REFERENCES

Delfs:2002:ICP


Dodos:2005:CCS


Delfs:2007:ICP


Dunkelman:2008:TIV


Du:2005:BRS


Daswani:2007:FSW

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

**Dhem:2000:PIT**


**Ding:2000:SSC**


**Dodis:2009:CAI**


**Datta:2005:RBN**


**Delaune:2008:FAP**


[DKL09]
[DKL00a]
[DKMR05]
[DKL00b]
[DKS08]
[DKL+00a]
[ACM09]
REFERENCES

[Dittmann:2005:CMS]

[Dodis:2002:KIP]

[Diffie:1998:PLP]

[deLeeuw:2000:CSD]

[Diffie:2007:PLP]

[deLeeuw:2007:HIS]
Karl de Leeuw and J. A. Bergstra, editors. *The history of information security: *


DeSan
tis:2007:NRN


Drimer:2007:KYE


Dumais:2000:PCQ


Dowd:2007:ASS


Denev:2009:SFQ


Ding:2007:ESD


REFERENCES


REFERENCES


REFERENCES


Crescenzo:2004:CRR


Daemen:2000:NPN


Daemen:2000:RA


Daemen:2000:BCR


Daemen:2001:AAR

REFERENCES


Daemen:2002:AWT


Daemen:2002:DRA


Daemen:2002:FSE


Ding:2002:HEE

REFERENCES


REFERENCES


Yevgeniy Dodis and Adam Smith. Entropic security and the encryption of high entropy messages. In

Ding:2006:SSS


Dinur:2008:CAT


Dodis:2001:PAS


Djurovic:2001:DWF

Igor Djurovic, Srdjan Stankovic, and Ioannis Pitas. Digital watermarking in the fractional Fourier transform-


Ed Dawson and Serge Vaudenay, editors. *Progress in cryptography — MYCRYPT 2005: first international conference on cryptography in Malaysia, Kuala Lumpur, Malaysia, September 28–30,


REFERENCES


Desmedt:2005:CNS


Dittmann:2001:UCW


Dworkin:2003:DRB


Ding:2005:NME

REFERENCES


[EBS01] Tareq Eghlidos, Albrecht Beutelspacher, and Babak Sadeghiyan. Improving

**Eilam:2005:RSR**


**English:2007:MAC**


**ECMA:2000:EPIa**


**ECMA:2000:EPIb**


**Ellison:2003:PKS**


**Echizen:2005:PAV**

Isao Echizen, Yasuhiro Fujii, Takaaki Yamada,

**Eghlidos:2000:SLB**


**Eghlidos:2000:SLB**


**Elmallah:2008:LK**


**Epstein:2003:DIT**


**Ernst:2004:FBH**


**Ellison:2000:PSK**


**Eggers:2001:DWC**

Joachim J. Eggers, Wolf-


REFERENCES


REFERENCES


[Ericson:2003:HAE]

[Ericson:2008:HAE]

[Ellison:2000:TRP]

[Ellison:2000:IRRa]

[Eberle:2005:ANG]

[Enck:2005:EOF]

[Ettinger:2002:QQC]
Mark Ettinger. 20 questions, quantum computers, and

**Ebringer:2000:PAP**


**Edman:2009: AES**


**Elbirt:2000:FIP**


**Faliszewski:2007:BRB**


**Fan:2003:ILC**

REFERENCES

Faugere:2009:IBC


Ford:2001:SEC


Felkel:2001:ICW


Feghali:2002:SAP


Fischer:2001:TMR


Felke:2006:ATH


Ferguson:2000:SEK

N. Ferguson. Semi-equivalent keys in MARS. In ???? ed- itor, Third AES Candidate Conference, page ?? ????.
REFERENCES


REFERENCES


[Fil00] Eric Filiol. Decimation
REFERENCES


[FIP01a] FIPS. Advanced Encryption Standard (AES). National Institute for Standards and
REFERENCES


FIPS:2001:SRC


REFERENCES

2004. CODEN CSSEEI. ISSN 0267-6192.


REFERENCES

Fox:2001:PPK

Faure:2006:NPK

Freytag:2003:VPI

Fluhrer:2002:CMB

Fluhrer:2002:CSP
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Fernandes:2002:SAL]

[Fournet:2008:CSI]

[Frankel:2001:FCI]

[Franklin:2004:ACC]

[Fremberg:2003:MAP]
Daniel Fremberg. The
REFERENCES

Mithra authentication protocol. Dr. Dobb’s Journal of Software Tools, 28
(5):44, 46–48, May 2003. CODEN DDJOEB. ISSN
1044-789X. URL http://
www.ddj.com/documents/
s=7927/ddj0305d/.

Friberg:2001:UCH

Paul Friberg. Using a cryptographic hardware token with Linux: The
OpenSSL project’s new engine. Linux Journal, 89:
??, September 2001. CO-
DEN LIJOFX. ISSN 1075-
3583 (print), 1938-3827
(electronic). URL http://
www.linuxjournal.com/
articles/style/0006.html
Web only.

Frith:2007:SAO

David Frith. Steganography
approaches, options, and im-
itations. Network Security,
CODEN NTSCF5. ISSN
1353-4858 (print), 1872-9371
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485807700715.

Frykholm:2000:CAB

N. Ferguson and B. Schneier.
A cryptographic evaluation of
IPsec. Technical re-
port, Counterpane Internet
Security, 3031 Tisch Way,
Suite 100PE, San Jose, CA
95128, USA, 2000. URL
http://www.counterpane.
com/ipsec.html; http:
//www.counterpane.com/
ipsec.pdf.

Fouque:2001:FDT

Pierre-Alain Fouque and
Jacques Stern. Fully dis-
tributed threshold RSA un-
der standard assumptions.
Lecture Notes in Computer
CODEN LNCS9. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
//link.springer-ny.com/
link/service/series/0558/
bibs/2248/22480310.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2248/22480310.
pdf.

Friedlander:2001:DDH

John B. Friedlander and
Igor E. Shparlinski. On
the distribution of Diffie–
Hellman triples with sparse
exponents. SIAM Jour-
nal on Discrete Mathematics,
REFERENCES


REFERENCES


signatures, broadcast, and multi-party computation from correlated randomness. [FZH05]


Fan:2004:PPI

Jinliang Fan, Jun Xu, Mostafa H. Ammar, and Sue B. Moon. Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme. [GA05]


Furnell:2006:RPS

Steven Furnell and Leith Zekri. Replacing passwords: in search of the secret remedy. [Gal01]


Fu:2005:DHP


Gross-Amblard:2003:QPW


Gang:2005:CNI


Galbraith:2001:SCC

bibs/2248/22480495.htm; http://link.springer-  
ny.com/link/service/series/  
0558/papers/2248/22480495.pdf.

Galbreath:2002:CID

Gallo:2003:SST

Ganger:2001:AC

Garrett:2001:MBC

Garfinkel:2003:EBI
REFERENCES

computer.org/dl/mags/sp/2003/06/j6020.pdf.

Garman:2003:KDG


Garrett:2004:MCT


Garrett:2005:CP


Gasarch:2001:BRBa


Gaudry:2002:CCS


Gavinsky:2008:CIC


Guinee:2009:NTR

R. A. Guinee and M. Blaszczyk. A novel true random binary sequence generator based on a chaotic double scroll oscillator combination with a pseudo random generator for cryptographic applications.
REFERENCES


**Goodman:2001:EER**


**Guerrero:2005:ECB**


**Gordon:2008:CFS**


**Gligor:2002:FEA**


**Gennaro:2005:SMS**

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

**Gebotys:2004:DSC**


**Gengler:2000:UPC**


**Gennaro:2000:IPR**


**Gentry:2004:IPR**

Craig Gentry. How to compress Rabin ciphertexts and signatures (and more). In Franklin [Fra04], pages 179–?. CODEN LNCS9D.
REFERENCES

300


[Gennaro:2006:RC]

[Gentry:2009:FHEa]

[Gentry:2009:FHEb]

[Giuliani:2001:GLI]

[Goldstone:2005:FCR]

[Golomb:2005:SDG]
Solomon W. (Solomon Wolf) Golomb and Guang Gong. *Signal design for good correlation for wireless commu-
REFERENCES

Gambino:2008:ITW

Goldwasser:2008:CAP

Gennaro:2005:BEG

Grothoff:2009:TBS

Gilbert:2002:SCL
REFERENCES


REFERENCES

Gilbert:2001:SAR

Gaudry:2006:ACM

Grabner:2005:ALC

Gong:2001:GPK

Gennaro:2001:RCV

Gennaro:2002:RSM
Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. On 2-round secure multiparty computation. In Yung [Yun02a],


REFERENCES


[GK05] Shaﬁ Goldwasser and Dmitriy Kharchenko. Proof of plain-

Garay:2007:RCA

Gertner:2000:RBP

Guneysu:2008:CC


REFERENCES


[Gallant:2001:FPM]


Girault:2000:CCP


Girault:2002:CS


Girault:2002:NRP

REFERENCES


REFERENCES

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


REFERENCES


Goldreich:2001:FCBb


Goldreich:2001:FCBa


Golic:2001:CAS


Golic:2003:DNP

REFERENCES

Goldreich:2004:FCV


Goldstein:2008:BHO


Gonda:2006:NMR


Good:2000:TAE


Gordon:2002:TCP


Gurgens:2002:APF

REFERENCES

Gorman:2005:NSC


Gordon:2006:UA


Goulding:2009:ESA


Gupta:2008:FAT


Ganeriwal:2008:STS


Garcia-Pasquel:2006:GCT


Gunesyu:2008:SPH

Tim Güneysu, Christof Paar, and Jan Pelzl. Special-purpose hardware for solving the elliptic curve discrete logarithm problem. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 1(2):8:1–
REFERENCES

---

Gutterman:2006:ALR


Granger:2005:HSN


Granger:2006:SCA


Gentry:2008:THL


Geng:2008:DSA


Galbraith:2004:EDD


Grasser:1998:FC


Graff:2001:CCW

Jon Graff. *Cryptography and e-commerce: a Wiley tech

Granboulan:2002:FDC


Granboulan:2002:SSR


Grigg:2001:FCL


Grossschadl:2003:ASL

REFERENCES


[Gent06] Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. Lecture Notes in Computer Sci-
REFERENCES

Gentry:2002:CRN


[GS03]


Geiselmann:2003:HSS


Goodell:2007:TOR


Grassl:2009:CAS

REFERENCES

**Guida:2004:DUP**


**Garfinkel:2003:PUI**


**Gaubatz:2008:SCD**


**Goodrich:2004:ETB**


**Giles:2002:ADW**


Goodrich:2008:NFI


Guttman:2004:FAP


Guar:2005:PPL


Gumz:2004:BRH


Guillou:2001:CAP


Gutmann:2000:OSC


Gutmann:2002:CFP


**Gutmann:2002:DVC**


**Gutmann:2004:CSA**


**Gutmann:2004:SPK**


**Gutmann:2004:ATD**


**Gutmann:20xx:ESR**


**Granger:2005:DLP**

REFERENCES

[Sujata Garera and Jorge Vasconcelos. Challenges in teaching a graduate course in applied cryptography. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 41(2):103–107, June 2009. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).]


[Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford. Path-quality monitor-]
REFERENCES

Haddad:2000:AUA


Harvey:2000:EMA


Hare:2001:RUPa


Hare:2001:RUPb


Harvington:2005:NSP


Harris:2005:GHE


Hars:2006:MIA


Haufler:2006:SWN


Hayat:2004:CSE

[HAuR04] 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.

Hoglund:2006:RSW


Huffmire:2008:DSS


Hartel:2001:TMS

REFERENCES

link/service/series/0558/|-
|bib/2021/20210478.htm;
|http://link.springer-
|com/link/service/series/
|0558/papers/2021/20210478.
|pdf.

Holcomb:2009:PSS

Humphries:2002:IC

Huang:2004:NDE

Hwang:2004:NMP

Huang:2008:NCK

Han:2008:PBPa

Han:2008:PBPb
Song Han, Elizabeth Chang, and Tharam Dillon. Pairing-based public-key encryption schemes with backward-and-forward security. *International Journal of Computer

[HCCDO02]

[HCCJ02]

[HCK09]

[HCCDO02]

[HCCJ02]

[HCCJ02]
REFERENCES

July/August 2007. CODEN ??? ISSN 1540-7993 (print), 1558-4046 (electronic).


Hess:2004:SVE

[Hes04a]

Hess:2004:GAR


Heys:2003:ASC


Hassler:2000:OFA


Horvitz:2003:WKA


Horan:2005:NRN


Howgrave-Graham:2005:PKC

[HG05b] Nick Howgrave-Graham. Public-key cryptography and proofs of security. In Garrett and Lieman [GL05],
REFERENCES


Howgrave-Graham:2003:HNP
REFERENCES

Hendricks:2007:LOB


Handschuh:2004:SAC


Handschuh:2005:SAC


Hung:2009:FBA


Hwang:2005:TSP

REFERENCES

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


REFERENCES


Hamann:2001:SBA


Han:2007:FIE


Higgins:2008:NSC


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],
REFERENCES

pages 216–227. ISBN ????
LCCN ???? ACM order number 475020.

[Hir09]

[HJ07]

[HJW05]

[HJW01]

[Kim2000:RMW]


**REFERENCES**

Howard:2003:WSC


Hwang:2004:REL


Hohenberger:2005:HSO


Hwang:2005:TAU


Hwang:2005:SHW


Hwang:2005:STH


Howard:2006:SDL

Michael Howard and Steve Lipner. *The security develop-


REFERENCES

Hwang:2003:TRB


Hwang:2004:KAS


Hwang:2005:GTS


Hong:2003:BBP


Herzog:2003:PAK


Hwang:2001:TSB

REFERENCES


Hopper:2002:PSS

Hu:2009:TRN

Hamdy:2000:SCB

Hartel:2001:FSJ

Hirt:2001:RFU
REFERENCES


REFERENCES

Hankerson:2004:GEC

Huang:2007:MPK

Haastad:2004:SAR

Harnik:2006:CNI

Haitner:2009:SHC

Hanaoka:2002:HNI
Hoepman:2001:SKA


Hofinger:2001:LBE


Honary:2001:CCI


Hook:2005:BCP


Hoskins:2006:SO

Hoskins:2006:SSE


Horn:2000:APF


Huhnlein:2001:ICB


Han:2002:CMV


Hoffstein:2001:NNL


Hoffstein:2008:IMC


He:2001:SAR

Yeping He and Sihan Qing. Square attack on reduced


REFERENCES

Hawkes:2004:RVC

Holenstein:2005:OWS

Halevi:2006:TCT
REFERENCES


REFERENCES

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


[Hs07] Ren-Junn Hwang and Sheng-Hua Shiau. Provably efficient authenticated key agreement protocol for multiservers. The Computer Journal, 50(5):602–615, Septem-
He:2005:MCP


Hong:2001:KIA


Halderman:2008:LWRa


Halderman:2008:LWRb


Halderman:2009:LWR

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. Communications of the Associa-
REFERENCES


Seokhie Hong, Jaechul Sung, Sangjin Lee, Jongin Lim, and Jongsu Kim. Provably secure for 13 round Skipjack-like structure. In-
REFERENCES

Hong:2002:IDC

Deukjo Hong, Jaechul Sung, Shiho Moriai, Sangjin Lee, and Jongin Lim. Impos-

sible differential cryptanalysis of Zodiac. Lecture Notes in Computer Sci-

cence, 2355:300–??, 2002. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349
bibs/2355/23550300.htm; http://link.springer-ny.com/link/service/series/
0558/papers/2355/23550300.pdf.

Hess:2001:TTH

Florian Hess, Gadiel Seroussi, and Nigel P. Smart. Two

topics in hyperelliptic cryptography. Lecture Notes in Computer Science, 2259:

181–??, 2001. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349
bibs/2259/22590181.htm; http://link.springer-ny.com/link/service/series/
0558/papers/2259/22590181.pdf.

Hernandez:2004:STN

Julio César Hernández, José María Sierra, and Andre Seznec.
The SAC test: a new randomness test, with some applications to PRNG analysis.
CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349
(electronic). URL http://www.springerlink.com/content/an44921nl5aa5bf0g/.

Hsu:2005:CIT

Chien-Lung Hsu. Cryptanalysis and improvement of the


[Huang06] Biao-Bing Huang and Shao-

Hongfeng:2008:ECP


Hamalainen:2002:GPS


Hines:2007:AIF


Hofheinz:2005:CTN


Hughes:2002:LAA

Hughes:2004:ISE


Huhnlein:2000:EIC


Hunt:2005:JFE


Husemann:2001:SSC


Husemoller:2004:EC


Huth:2001:SCS


Hodjat:2004:HTP

[Alireza Hodjat and Ingrid Verbauwhede. *High-...

**Hallgren:2009:QC**


**Hopper:2009:PSS**


**Hutchinson:2001:IWC**


**Hardy:2003:AAC**


**Hellekalek:2003:EEC**

REFERENCES


[Hsu:2004:EPS]


[Hsu:2005:SCT]


[Hwang:2000:CYK]


[Hwang:2005:ITA]


[Henderson:2001:IEV]


[Hsu:2005:NPM]


[Hu:2008:NNP]
Hardy:2009:AAC


Hsu:2002:IGT


Hsu:2003:ITP


Hsu:2004:GOS


Harkins:2005:ESU


Hsu:2003:IMA


Huang:2005:EMP


IBM-MARS-Team:2000:MAS


security/final-comments.ps.

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, editor. *Proceedings: 46th Annual IEEE Symposium on Foun-


REFERENCES


IEEE:2009:PAI


IEEE:2009:PAI

Itoi:2001:SIS


Ifrah:2000:UHN


Iglesias:2002:NSB


Bassham:2000:ET

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 [IK00]???
LCCN ???


LCCN ???

REFERENCES

Impagliazzo:2003:LRA


Ichikawa:2000:HEA


Ishai:2003:EOT


Ishai:2005:SCC

Ishai:2006:CA


Ishai:2007:ZKS


Ishai:2008:CCC


Iyer:2007:TAA


Ioannidis:2005:ACN


Izmerly:2006:CCA

Oleg Izmerly and Tal Mor. Chosen ciphertext attacks on lattice-based public key encryption and modern (non-quantum) cryptography in
REFERENCES


Inamori:2002:SPB

Inamori:2002:SPT

Inoue:2005:EST
Intel:2000:IIP


Intel:2003:IRN


IR01


IR02


Irwin:2003:BRBb


ISO:2004:IIIb

REFERENCES

ISO:2005:IDM


Iqbal:2008:CDV


Inoue:2008:FAC


Ishai:2003:PCS


Itoi:2000:SCI


Itoi:2001:SCS

REFERENCES

Iwami:2008:AIA

Imai:2000:CPC

Irwin:2005:PAI

Iwamoto:2006:SSR

Iwata:2002:NCP

Iwata:2003:NCP
REFERENCES

Imai:2000:PKC

Judge:2002:WWM

Jablon:2001:PAU

Jackson:2000:SCQ

Jambunathan:2000:CCP

Janczewski:2000:IIS
REFERENCES


Janeczko:2006:TSH


Jankowski:2008:BRBb


Jankvist:2008:TMH


Jennewein:2000:FCQ

Thomas Jennewein, Ulrich Achleitner, Gregor Weihl, Harald Weinfurter, and Anton Zeilinger. A

Jones:2005:RDF


[JBR05]

Johnson:2001:IHS


Jaeger:2004:CAA


[JEZ04]

Juels:2001:RKG

REFERENCES


Jaulmes:2001:CPN


Jonsson:2002:FCA


Jonsson:2002:SRE


Jakimoski:2001:ASR


Jakimoski:2001:CCB


Jakimovski:2002:CS


Jonsson:2002:SRT

Jakob Jonsson and Burton S. Kaliski Jr. On the security
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://
//link.springer.de/link/
service/series/0558/bibs/
2442/24420127.htm; http://
//link.springer.de/link/
service/series/0558/papers/
2442/24420127.pdf.

Jang:2001:BWA

Yongwon Jang, Intaek Kim, Hwan Il Kang, Kab Il Kim, and Seung-Soo Han. Blind
watermarking algorithm using complex block selection method. Lecture Notes in
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://
//link.springer-ny.com/
link/service/series/0558/bibs/
2195/21950996.htm; http://link.springer-ny.com/link/service/series/
0558/papers/2195/21950996.pdf.

Jung:2001:EMO

Oliver Jung, Sven Kuhn, Christoph Ruland, and Kai Wollenweber. Enhanced
modes of operation for the encryption in high-speed networks and their impact on
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://
//link.springer-ny.com/

Jallad:2002:ICC

Kahil Jallad, Jonathan Katz, and Bruce Schneier. Implementation of chosen-
ciphertext attacks against PGP and GnuPG. In Lynn Batten and Jennifer Seberry,
editors, Information security and privacy: 7th Australasian conference, ACISP
Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,
//link.springer-ny.com/
REFERENCES

Jarecki:2000:AST

Joux:2003:IGN

Juang:2004:FBT

Jeong:2008:PKE

Juang:2001:FBT
REFERENCES

Juang:2002:VMA


Jakobsson:2003:FMT


Jakobsson:2007:DPD


Johansson:2003:PCI

[JM03] Thomas Johansson and Subhamoy Maitra, editors. Progress in Cryptology—


Jing-mei:2005:CRB


**Joux:2002:BAA**

**Johnson:2000:AFR**

**Johansson:2003:FSE**

**Johnson:2005:OSV**
REFERENCES

Jolish:2001:EDP

Jon08

Joux:2002:WTP
Antoine Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. Lecture Notes in Computer Science, 2369:20-??, 2002. CODEN LNCS-D9. ISSN [Joy00]

Joux:2004:MIH

Joux:2009:AC

Joyner:2000:CTC
David Joyner, editor. Cod-
REFERENCES

ing theory and cryptography: from Enigma and Geheim-
schreiber to quantum the-
ory. Springer-Verlag, Berlin,
Germany / Heidelberg, Ger-
munity / London, UK / etc.,
2000. ISBN 3-540-66336-
3 (softcover), 3-642-59663-
0 (e-book). LCCN QA268
.C67 1999. UK £44.50. URL
http://frode.home.cern.
ch/frode/pubs/cryptoday.pdf. Proceedings of the
Conference on Coding The-
yory, Cryptography and Num-
ber Theory held at the U.S.
Naval Academy during Oc-

[Marc Joye:2003:CPY]
Marc Joye. Cryptanaly-
sis of a pay-as-you-watch
system. Information Pro-
cessing Letters, 88(3):119–
120, November 15, 2003.
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-6119
(electronic).

[Marc Joye:2003:TCC]
Marc Joye, editor. Topics in
cryptology, CT-RSA 2003: the
Cryptographers’ Track at the RSA Conference 2003, San Francisco, CA, USA, April 13–17, 2003: Proceedings, volume 2612 of Lecture Notes in Computer Science. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 2003. CO-
DEN LNCS9D. ISBN 3-540-
00847-0. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
CS22 2003. URL http:
//link.springer-ny.com/
link/service/series/0558/t-
tocs/t2612.htm; http://
www.springerlink.com/
openuurl.asp?genre=issue&
issn=0302-9743&volume=
2612.

[Markus Jakobsson:2002:MAL]
Markus Jakobsson and David
Pointcheval. Mutual au-
thentication for low-power
mobile devices. Lecture
Notes in Computer Sci-
CODEN LNCS9D. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/b-
bibs/2339/23390178.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/2339/23390178.
pdf.

[Éliane Jaulmes:2002:SHG]
Éliane Jaulmes and Guil-
laume Poupard. On the se-
curity of homage group au-
thentication protocol. Lecture
Notes in Computer Sci-
CODEN LNCS9D. ISSN
0302-9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/b-
bibs/2339/2339016.htm;
REFERENCES


Joye:2003:GFA


Jakubowska:2007:MCT


Joye:2004:CHE


Joye:2001:PMA


REFERENCES

JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Jarecki:2005:FSP


Jiang:2005:SAI


Joye:2001:PAD


Joye:2001:CEN


Jongkook:2001:NUS


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

**Juels:2005:APD**


**Jeng:2006:EKM**


**Jin:2005:EAW**


**Juels:2005:APD**


**Jeng:2006:EKM**


**Jin:2005:EAW**


**Joye:2001:NMM**


**Jakobsson:2004:ACN**

REFERENCES


Jain:2009:NBC


Jiang:2005:TMD


Kadrich:2007:ES


Kahn:1967:CSSa


Kahn:1967:CSSb


Kahn:1974:C

REFERENCES


[Katzenbeisser:2001:RAR] Stefan Katzenbeisser. Recent advances in RSA cryptography, volume 3 of Advances in information se-
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


Keller:2009:ECC

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

Kieu:2009:HSI

Kieu:2009:IAB

Ku:2005:WLY


Wei-Chi Ku, Chien-Ming Chen, and Hui-Lung Lee. Weaknesses of Lee–Li–Hwang’s...


Keefe:2005:CDS


Kellar:2005:NRR


Kelsey:2000:KST


Kelsey:2002:CIL


Kenyon:2002:DNR


Kenyon:2002:HPD


Kettani:2006:CBN

Houssain Kettani. On the conversion between number systems. *IEEE transactions on circuits and systems.* 2, Analog and digi-
REFERENCES

Kelsey:2000:CPL

Kiltz:2009:DCC

Katsikas:2004:PKI

Kovacich:2003:MHC

Kim:2005:SMA
[KH05] Byung-Gi Kim and Sang-Sun Hong. Secure mutual authentication for ad


[KY04] Darko Kirovski, Henrique, and Yacov Yacobi. A
REFERENCES

Kausar:2008:SEK


Kobara:2001:NCP


Kobara:2001:SSM


Kurosawa:2003:TTK

REFERENCES

Kidwell:2000:SNC


Kid:2002:PGR


Kilian:2001:ACC


Kiltz:2001:TBC


Kilian:2005:TCS


[King:2002:RGI] Brian King. Require-
ments for group independent linear threshold secret sharing schemes. Lecture Notes in Computer Science, 2384:89–??, 2002.


REFERENCES


REFERENCES

issn=0010-485X&volume=85&issue=1&spage=137.

Kawachi:2005:UTQ


Kim:2009:SVN


Kaliski:2002:CHE


Kelsey:2000:ABA

Kohno:2000:PCR


Kelsey:2001:ABA


Katz:2005:HEP


Katz:2008:IMC

Jonathan Katz and Yehuda Lindell. Introduction to mod-

Knill:2002:FPE


Knill:2002:QIP


Ko:2000:NPK


Klein:2007:BDC


Kong:2001:AVW

Kiltz:2005:SCM


Kacprzak:2006:CBS


Kalai:2009:SEU


Kim:2002:EPS


Kim:2003:IBP

REFERENCES

Knudsen:2000:CRA

Lars Knudsen and Willi Meier. Correlations in RC6 (abstract only). In NIST [NIS00], page 9.
ISBN ????, LCCN ???.

Knudsen:2001:CRR

L. Knudsen and W. Meier. Correlations in RC6 with a reduced number of rounds. In Schneier [Sch01d], page ??.

Knudsen:2001:CPL


Kanda:2002:SCA

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


Koblitz:2004:OTS


Kornerup:2007:PIS


Kim:2002:ABA

Kakarounas:2006:HSF


Katz:2001:CCA


Klimov:2002:ANC


Keliher:2001:IUB

Kim:2003:RCC


Kittler:2003:AVB


Kol:2008:GEI


Koc:2001:CHEb


Krukow:2005:FCR


Knudsen:2000:TT


Knudsen:2000:TTR


Knudsen:2002:ACE


Knutson:2007:BPS


Kushilevitz:2000:OWT

REFERENCES

0558/papers/1807/18070104.

Komano:2003:EUP


Koblitz:2000:TQC


Kocher:2002:IS


Koga:2002:GFR


Kurosawa:2001:ICP

Kaoru Kurosawa, Wakah Ogata, Toshihiko Matsuo, and Shuichi Matsushima. IND–CCA public


REFERENCES


**Kovacich:2003:ISS**


**Katz:2001:EPA**


**Katz:2009:ESA**


**Katzenbeisser:2000:IHT**


**Koc:2001:CHEa**

REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>
REFERENCES


Jonathan Katz and Bruce Schneier. A chosen ciphertext attack against several E-mail encryption protocols. In USENIX [USE00d], page ?? ISBN 1-880446-
REFERENCES


Kelsey:2000:MAP


Kuramitsu:2002:ETC


Krause:2003:DOC


Kozaczuk:2004:EHP


Katz:2005:MIA

7. LCCN QA76.9.A25. ACM order number 459050.


REFERENCES


Noam Kogan and Tamir

**Ku:2003:TSA**


**KTC03**


**KTT07**


**Ku:2002:IB**


**Ku:2004:HBS**


**Kuhn:2000:PCL**

Kuhn:2002:OTD


Kuhn:2002:ICM


Kuhn:2008:BSS


Kukorelly:2001:PAL


Kundur:2001:WDI


Kurosawa:2001:MRP

Kusters:2002:DCP


Kuo:2001:AOS


Kejariwal:2009:ELL


Koshiba:2000:SEP


Knudsen:2002:IC

REFERENCES

Karlof:2003:HMM


Kwok:2003:WBC


Kwok:2003:WBC


Kumar:2006:ODS


Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC

Kwok:2003:WBC
REFERENCES

Wong:2001:MCC


Kun:2000:SMA


Kamat:2009:TPW


Katz:2000:CCS


Katz:2001:UEC


Kavut:2001:SCP

REFERENCES


Kim:2002:PAA


Katz:2003:SPA


Kamal:2009:FIN


Kang:2001:PMT


Kabatnik:2001:LSD

Kamp:2003:DEB


Kamp:2007:DEB


Kumar:2009:UAU


Ladd:2006:SPS


Lafe:2000:CAT


Laih:2003:ACA


Landau:2000:STT


Landau:2000:TOD


Landau:2004:PNS


Landau:2004:SLE


Lakshminarayanan:2008:SUC

Karthik Lakshminarayanan,
REFERENCES


REFERENCES

0558/papers/2288/22880050.pdf.

Laufer:2000:SSC


Laih:2003:COP


Lin:2004:SOT


Lu:2004:XMS


Lu:2005:ER


Lu:2005:NDA


Long:2005:DTC

Yun Long, Zhenfu Cao, and Kefei Chen. A dynamic threshold commercial key escrow scheme based on

Lu:2007:NPL


Lee:2001:SEK


Lee:2004:DEB


Li:2008:CAM


Lu:2005:TUS


Lu:2005:RTP


Li:2001:CCB


Lai:2004:SGS


Lavoue:2007:SSW

REFERENCES


REFERENCES


REFERENCES


Li Lu, Jinsong Han, Yinhao Liu, Lei Hu, Jin-Peng Huai, Lionel Ni, and Jian

Liu:2005:DBV

[LHS05]

Lee:2009:NCA

[LHT09]

Lee:2002:FRU

Li:2001:NSA

[Li01]

Lee:2005:NBS

[LHY05]

Li:2005:ABPa
REFERENCES


Jung-Seuk Lee, Jun-Cheol Jeon, and Kee-Young Yoo. A security scheme for protecting security policies in


REFERENCES


[LKY05d] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo. Improvement of Lee

Lim:2000:GTC


Luo:2004:UUR


Lu:2001:DWC


Lee:2003:ISC


Lee:2004:FIM


Lee:2004:DIS


Lee:2005:CMA


Lee:2005:SSP


Li:2005:FCR
References

**Lee:2006:ISC**


**Lee:2001:PBG**


**Lu:2006:FBW**


**Lu:2006:RDI**


**Li:2008:CRR**


**Lee:2002:RUA**


**Li:2004:CES**

References

Lesniewski-Laas:2005:SSS


Li:2001:SPD


Lee:2004:MPA


Lee:2006:SYG


Li:2006:ESY


Li:2006:SYG

[LLLZ06b] Chengqing Li, Shujun Li,
REFERENCES


Lindell:2002:CAB


Lindell:2006:CAB


Lian:2007:MDE


Lee:2005:IWR


Liu:2005:SWA


Lee:2009:CET


**Linares:2000:Sam**


**Lorenz:2002:SSG**


**Lavasani:2008:IFA**


**Li:2003:SCE**


**Lamenca-Martinez:2006:LNP**

REFERENCES


[Lepinski:2005:FZK]

[LMP*01]

REFERENCES


Li:2005:BPC

Liu:2004:MBA

Levieil:2008:CTC

Liu:2008:ARL

Lotspiech:2002:CFB

Li:2002:HNP
REFERENCES


Loidreau:2000:SMC


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


Li:2006:PMW


Li:2008:DEO


Lientz:2001:BTP


Lemke-Rust:2007:MAP


1709. xiv + 232 pp. LCCN ???. EUR 24.90.

Liskov:2002:TBC


Lenstra:2001:SFR


Lindemann:2001:ICT

[LS01b] Mark Lindemann and Sean W. Smith. Improving DES coprocessor throughput for

Loidreau:2001:WKM


Li:2005:ULC


Liang:2005:FAG


Liu:2008:GPV


Lopez:2007:SCB


Lin:2003:DBI

Lin:2000:TPE


Lin:2003:SEOa


Lin:2003:SEOb


Liang:2009:AIE


Liu:2005:RBU

Li:2005:ISS


Lie:2000:ASC


Lin:2005:HAO

REFERENCES

Lu:2002:HEA

Lu:2007:NSC

Lucks:2002:SAB

Lucks:2000:ASR

Lucks:2002:VCS

REFERENCES

Lucas:2006:PGE

Ludvig:2005:PWF

Lukyanov:2001:PFA

Lunde:2009:BCU

Lutz:2002:BBS

Lutz:2003:BLF
References

Lenstra:2000:XPK

Lu:2004:FCA

Laguillaumie:2007:MDV

Lange:2002:PIE

Lee:2004:IAK

Liang:2005:PA
Wei Liang and Wenye Wang. On performance analysis of

**Loepp:2005:PIC**


**Lyuu:2005:CIH**


**Lv:2005:PCA**


**Lv:2005:SMS**


**Li:2005:IWR**

Haifeng Li, Shuxun Wang, and Weiwei Song. Image watermarking resistant to global geometrical attacks. In Han et al. *[HYZ05b]*, pages 911–?? ISBN 981-270-153-2. LCCN
REFERENCES


Lin:2005:NIB

Lixin:2005:FLA

Li:2007:NBA

Lou:2002:ESA

Liu:2007:IFW

Lysyanskaya:2002:USV
Anna Lysyanskaya. Unique signatures and verifiable random functions from the DH-DDH separation. In Yung [Yun02a], pages 597–612. CODEN LNCSD9.
REFERENCES


REFERENCES

Li:2004:WMS

Maurer:2007:ICP

Mrayati:2003:AKT

Mrayati:2004:IAD

Mrayati:2005:IDB


Mrayati:2006:TTC


Mrayati:2007:TTC


Mrayati:20xx:AET


McDaniel:2006:OAI


Machado:2000:NCP


MacKenzie:2001:MEP

REFERENCES


Mann:2002:HI

Mann:2008:HHS

Mao:2001:TRC

Mao:2004:MCT

Marques:2002:BSJ

Martinelli:2002:SSA
Mares:2005:BRA


Martin:2005:STA


Martin:2007:SCE


Martin:2008:CCI


Matsui:2002:FSE

REFERENCES

Maurer:2001:C

[Mau01]

Maurer:2004:RCD

[Mau04]

Maughan:2005:HSC

[Mau05]

Maximov:2006:SWC

[Mai06]

Mayers:2001:USQ

[May01]

May:2002:CUR

[May02]

May:2004:CRS
Alexander May. Computing

May:2009:PIS


Mel:2001:CD


Mohanty:2008:IWB


McKinnon:2004:CCS


Montenegro:2004:CBI


McAndrew:2008:TCO

SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic). Proceedings of SIGCSE 08.


Stephen McCamant and Michael D. Ernst. Quantitative information flow


Menezes:2007:ACC


Messerges:2000:SAF


Messerges:2001:SAF


McGrew:2001:AAE

David A. McGrew and Scott R. Fluhrer. Attacks on additive encryption of redundant plaintext and implications on Internet security.

**Marti-Farre:2007:NSS**


**Matula:2005:TLS**


**Mueller:2006:SMG**


**Muller:2009:BPE**


**Minier:2001:SCC**

REFERENCES

Muresan:2008:PCA


Mukherjee:2002:CAB


Molland:2004:ICA


Ma:2005:NCD


Maas:2009:SRW


Moon:2002:IDC

Dukjae Moon, Kyungdeok Hwang, Wonil Lee, Sangjin Lee, and Jongin Lim. Impossible differential cryptanalysis of reduced round
XTEA and TEA. Lecture Notes in Computer Science, 2365:49–??, 2002.

May:2002:SKS


Mihaljevic:2009:ASC


Micciancio:2001:ILB


Micciancio:2002:GCK


Micciancio:2002:ICH


Micciancio:2002:ICH

[Mic02b] Daniele Micciancio. Improved cryptographic hash
functions with worst-case/
average-case connection. In
ACM [ACM02], pages 609–
LCCN QA75.5 .A22 2002.
ACM order number 508020.

Millen:2003:FD
Jonathan Millen. On the
freedom of decryption. In-
formation Processing Let-
ters, 86(6):329–333, June
30, 2003. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

Mironov:2002:RSO
Ilya Mironov. (not so) ran-
dom shuffles of RC4. In
Yung [Yun02a], pages 304–
319. CODEN LNCSD9.
ISBN 3-540-44050-X (pa-
erback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 2002. URL http://
link.springer-ny.com/
link/service/series/0558/
tocs/t2442.htm; http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
2442.

Mirkovic:2005:IDS
Jelena Mirkovic, editor. In-
ternet denial of service: at-
tack and defense mecha-
nisms. The Radia Perl-
man series in computer net-
working and security. Prent-
tice-Hall PTR, Upper Sad-
dle River, NJ 07458, USA,
2005. ISBN 0-13-147573-
8 (paperback). xxii +
372 pp. LCCN TK5105.59
www.loc.gov/catdir/toc/
ecip0422/2004020335.html.

Mishra:2006:PCS
P. M. Mishra. Pipelined
computation of scalar mul-
tiplication in elliptic curve
cryptosystems (extended
version). IEEE Transac-
tions on Computers, 55(8):
1000–1010, August 2006.
CODEN ITCOB4. ISSN
0018-9340 (print), 1557-
9956 (electronic). URL
org/stamp/stamp.jsp?tp=
&arnumber=1650197.

Misić:2008:TEC
Jelena Mišić. Traffic and
energy consumption of an
IEEE 802.15.4 network in
the presence of authenti-
cated, ECC Diffie–Hellman
ephemeral key exchange.
Computer Networks (Ams-
tterdam, Netherlands: 1999),
52(11):2227–2236, August 8,
2008. CODEN ????. ISSN
1389-1286 (print), 1872-7069
(electronic).

Mitchell:2000:MSN
Chris J. Mitchell. Mak-
ing serial number based au-
thentication robust against
loss of state. Operating
Systems Review, 34(3):56–
59, July 2000. CODEN
OSRED8. ISSN 0163-5980 (print), 1943-586X (electronic).


REFERENCES

Mandviwalla: 2008: MBW


Moffie: 2005: AAS


Moyle: 2005: CLD


Mazieres: 2000: SKM


Majzoobi: 2009: TDI


McDonald: 2008: SID


McGregor: 2005: PCK

John P. McGregor and Ruby B. Lee.


Máire McLoone and John V. McCanny. Single-chip FPGA

**Mana:2002:PMD**


**Moldovyan:2007:IC**


**Mullen:2007:FFA**


**Moreira:2002:RCE**


**Milenkovic:2005:UIB**

Milena Milenković, Aleksandar Milenković, and Emil Jovanov. Using instruction block signatures to counter code injection attacks. *ACM SIGARCH Computer Ar-
REFERENCES


Maltoni:2003:HFR


McEvoy:2009:IWH


Maitra:2006:PCI

[MMV06] Subhamoy Maitra, C. E. Veni Madhavan, and Ramarathnam Venkatesan, editors. Progress in Cryptology — INDOCRYPT 2005: 6th International Conference on Cryptology in India, Ban-
Mercuri:2003:IRS


Mukhopadhyay:2014:EMP


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

Martel:2004:GMA


Martinez-Nadal:2002:CUM


pdf.

Meyer:2001:FIC


Monsignori:2001:WMS


Mironov:2008:SAE


MacAndrew:2000:LPT


Mykletun:2006:AIO


Mollin:2001:IC


Moller:2002:PEC

Bodo Möller. Parallelizable elliptic curve point multiplication method with resistance against side-channel attacks. Lecture Notes in
REFERENCES


Moller:2003:PSP


Moller:2003:RPK


Mollin:2005:CGS


Mollin:2007:IC


Monniaux:2003:ACP


Mangard:2006:PAA

Stephan Mangard, Elisabeth Oswald, and Thomas Popp. Power Analysis Attacks and Countermeasures for Cryptographic Smart Cards, volume 450 of Advances in Information Security. Springer-Verlag, Berlin,

Morris:2003:KKL


Moritz:2005:KAE


Moses:2006:DSD


Merton:2000:NBG


McMillan:2001:JIA


Mihaiulescu:2001:BRE

REFERENCES


REFERENCES

Matusiewicz:2006:FGD


Munilla:2007:HMF


Micciancio:2008:OCC


Mislov:2006:EBO


Moralis:2009:KSA


Micali:2005:OEC

Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error correction against computationally bounded noise.

**Monrose:2000:KDB**

**MacKenzie:2001:TPG**

**Micali:2001:SPK**

**Micali:2001:MRR**

**Murphy:2002:EASa**
S. Murphy and M. J. B. Robshaw. Essential algebraic structure within the
REFERENCES


REFERENCES


[MS02e] S. Muthukrishnan and S. Cenk Sahinalp. An improved algorithm for sequence com-
parison with block reversals. 


**Markowitch:2003:CWV**


**Miklau:2003:CAP**


**Martin:2005:PET**


**Meadows:2005:CPA**


**Mahdian:2009:UNI**

REFERENCES

Manulis:2009:SMF


Mashatan:2009:ITC


Myers:2009:BEC


Shen:2005:NIW


MacKenzie:2002:TPA


McClure:2003:HEN

REFERENCES

pp. LCCN TK5105359

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


Munro:2008:DE


Moriai:2000:PTL


Murphy:2000:KST

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

Murray:2001:CDC


Murray:2002:IYP


Meister:2001:PPG


Micciancio:2003:SZK

Daniele Micciancio and Salil P. Vadhan. Statistical zero-knowledge proofs...
REFERENCES


REFERENCES

McCook:2001:NSS


Morelos-Zaragoza:2002:AEC


Matsui:2004:SAC


Nagy:2007:AQK


Naik:2003:DSW

REFERENCES

/Nsonline.computer.org/
0309/f/aeah.htm.


REFERENCES

(80x681) [102x681]REFERENCES

503


[Na03]


[Na04]


[Na00]


[Nat00]


[Naz02]

[Na04]


Nedjah:2006:NTC


Netcape:2004:HSW


This is a tutorial of how the Secure Sockets Layer (SSL) protocol works.

Neuenschwander:2004:PSM


Neve:2003:STF


Nguyen:2001:TFLb

Nguyen:2005:RBP


[NH02]


[Nie02a]


[NH03]


Nordholt:2002:NFC

Nordholt:2002:NFC

[NH03]


Niederreiter:2002:BRC


[Nie02a]

REFERENCES


Nikander:2002:DSAa

Nikander:2002:DSAb

NIST:2001:CT

NIST:2001:SRC

REFERENCES


[NMSK01] H. Nozaki, M. Motoyama,
A. Shimbo, and S. Kawai-
mura. Implementation of
RSA algorithm based on
RNS Montgomery multipli-
cation. Lecture Notes in
Computer Science, 2162:
364–??, 2001. CODEN
LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/0558/papers/2162/21620364.pdf.

[NN02] Stephen Northcutt and Judy
Novak. Network intrusion
detection. New Riders Pub-
lishing, Carmel, IN, USA,
0-7357-1265-4. xvii + 490
pp. LCCN TK5105.59 .N475
2003.

[NN03] Dalit Naor and Moni Naor.
Cover feature: Protecting
cryptographic keys: the
trace-and-revoke ap-
proach. Computer, 36(7):
47–53, July 2003. CO-
DEN CPTRB4. ISSN
0018-9162 (print), 1558-0814 (electronic). URL http:
//csdl.computer.org/dl/mags/co/2003/07/r7047.

Nikova. On a relation be-
tween verifiable secret shar-
ing schemes and a class of
error-correcting codes. In
Ytrehus [Ytr06], pages 275–
290. ISBN 3-540-35481-
6. LCCN QA76.9.A25 I557
2005.

[Naor:2001:RTS] Dalit Naor, Moni Naor, and
Jeff Lotspiech. Revocation
and tracing schemes for
stateless receivers. In Kil-
lian [Kil01a], pages 41–??
ISBN 3-540-42456-3 (paper-
back). LCCN QA76.9.A25
C79 2001; QA267.A1 L43
no.2139. UK £47.00. URL
http://link.springer-ny.com/
link/service/series/0558/papers/2139/2139041.pdf.

[Naor:2005:ECH] Moni Naor, Asaf Nussboim,
and Eran Tromer. Efficiently
constructible huge graphs
that preserve first order
properties of random graphs.
In Kilian [Kil05], pages 66–
?? CODEN LNCSD9.
ISBN 3-540-24573-1 (soft-
cover). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
REFERENCES


Jorge Nakahara, Jr., Bart Preneel, and Joos Vand-
REFERENCES


Naor:2004:NTC


Nichols:2000:DYD


Nguyen:2001:Isa


Nguyen:2001:TFla

Phong Q. Nguyen and Jacques Stern. The two faces of lattices in cryptology. Lecture Notes in Computer Science, 2146:146–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
References

Narayanan:2005:FDA

Narayanan:2005:ODG

Nguyen:2005:FPL

Nguyen:2005:PSE

Nishioka:2002:DAF

Nahum:2007:ESS

Nyberg:2001:CTC
Kaisa Nyberg. Correlation


**Okamoto:2000:ACA**


**Okamoto:2004:TCC**


**Ohzahata:2002:FAM**


**Ogata:2006:OSS**

Olson:2000:SCT


Ohigashi:2009:PMF


Ohkuma:2001:BCH


Ohbuchi:2002:FDA


Onions:2001:SSI


Ors:2003:PAA

Okamoto:2001:GPN


Okamoto:2001:RRE


Oppliger:2005:CC


Ortiz:2000:ITW


Okeya:2000:PAB

Katsuyuki Okeya and Kouichi Sakurai. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack.


REFERENCES


[OT03a] Katsuyuki Okeya and Tsuyoshi Takagi. A more flexible countermeasure against side channel attacks using window method. In Walter

Okeya:2003:WMN


Ouellette:2005:PPM


Okamoto:2000:QPK


Oue05

Overbeck:2006:EGA


Onieva:2008:MNS


Paeng:2003:SCU


Page:2003:BRW


Panditaratne:2007:TRN


Papanikolaou:2005:BRBa


Park:2004:APP

REFERENCES

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

**Pass:2003:DCR**


**Pass:2005:UCN**


**Patterson:2001:DFI**


**Patiyoot:2002:MSE**


**Patiyoot:2002:SIW**


**Patarin:2003:LRR**

Jacques Patarin. Luby–Rackoff: 7 rounds are enough for security. In Boneh...
References


REFERENCES

(Paulson:2002:NBR)

(Paulson:2003:NBV)

(Paulson:2009:NBT)

(Praca:2001:SCS)

(Piva:2002:MCW)
Piva:2005:SRA

Park:2000:CAP

Peng:2005:SES

Peng:2007:BZK

Prattichizzo:2007:PIH

Papadimitriou:2001:PSE
CODEN IJBEE4. ISSN 0218-1274.

Perez:2007:URR


Poulos:2008:TSE


Pucheral:2001:PSD


Petrie:2000:NB1


Peikari:2004:SW


Park:2005:ISC

References

527


Park:2005:NDS


Perlner:2009:QRP


Park:2003:ESA


Patarin:2001:QBL


Park:2002:XQP

REFERENCES


Park:2003:EMS

Pan:2007:IBS

Peeters:2007:CES

Petrakos:2009:CTA

Peinado:2004:CLK

Peikert:2009:PKC

Pelzl:2006:PAC

Pemble:2001:CEW
Matthew Pemble. Confidentiality: From encryption, to

**Pemble:2001:SPA**


**Perrine:2003:ECP**


**Perlman:2005:EMD**


**Petullo:2003:IEH**


**Petullo:2005:EYR**


**Petzold:2008:ATG**


**Potter:2003:S**

Bruce Potter and Bob Fleck. *802.11 Security*. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617
REFERENCES


[PFK+01] Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik

[Phan:2004:IDC]
REFERENCES


Phoha:2001:SDI


Pieprzyk:2003:FCS


Pathak:2006:BFT


Pietrzak:2005:CDI


Pinkas:2002:CTP

Benny Pinkas. Cryptographic techniques for

**Pinkas:2003:CTP**


**Pincock:2006:CHC**


**Pech:2009:APW**


**Park:2001:ND**


**Park:2001:RFW**

REFERENCES


Poh:2001:HBP

Petitcolas:2003:DWF

Park:2005:CZA

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


REFERENCES

Piper:2002:CVS


Pang:2008:AQR


Pohlmann:2001:SCA


Pointcheval:2002:CCS


Pointcheval:2002:PSP


Pointcheval:2006:TCC


Poole:2003:NSP

REFERENCES


Porin:2001:THE


Porras:2006:PEG


Potter:2003:WAO


Potter:2006:CKM


Potter:2007:CWW


Pfleeger:2003:SC


Paul:2006:SSC

Souradyuti Paul and Bart Preneel. On the (in)security

Popp:2006:CTT


Pfeeger:2007:SC


Paar:2009:UCT


Pellikaan:1996:AGC


Pereira:2003:SAU


Piret:2003:DFA

Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In Walter et al. [WKP03], pages 77–88. CODEN LNCSD9. ISBN 3-540-40833-9. ISSN


Bart Preneel. New European Schemes for Signature,


REFERENCES

Price:2000:NCH


Provos:2000:EVM


Provos:2001:DAS


Paun:2004:CTT


Poupard:2000:FER


Parker:2001:RK


Pfitzmann:2001:SEC

[ PS01b ] Birgit Pfitzmann and Ahmad-Reza Sadeghi. Self-escrowed cash against user blackmailing. *Lecture Notes in
Pomerance:2002:SOC


Page:2004:PCA


Park:2004:UUC


Pornin:2001:SHT


Padro:2002:LBI


PS01c


PS02b


PS04a


PS04b

REFERENCES

Prabhakaran:2004:NNS


Prabhakaran:2005:RES


Pavlou:2008:FAD


Park:2002:SRL


[Puc03] Riccardo Pucella. Joint re-

**Pucella:2006:SCC**


**Pucella:2007:Ib**


**Puzmanova:2004:RWF**


**Page:2006:FAP**


**Paillier:2006:TOW**


**Phillips:2001:GRI**

Deborah M. Phillips and Hans A. von Spakovsky. Gauging the risks of Internet elections. Communications of the Association for Computing Machinery, 44(1):73, January 2001. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-
REFERENCES


Pang:2005:NMS


[PW05]

Peikert:2008:LTTF


PW08

Pelzl:2003:HCC


[PY05]

Patrick:2005:FCD


[PY06]

Paterson:2006:LTT

REFERENCES

1540-7993 (print), 1558-4046 (electronic).


[Haiqiang Tian, Zhen Fu Cao, and Haiyong Bao. Cryptanalysis of Li–Tzeng–Hwang’s improved signature schemes

**[Qian:2005:SPL]**


**[QSP01]**


**[Quisquater:2005:SCC]**


**[Quisquater:2002:CTM]**

REFERENCES


Rand Corporation. *A Million Random Digits With


REFERENCES

Reed:2000:ANA


Rubin:2005:ARS


Rangan:2001:PCI


Renaud:2009:VPC


Rudra:2001:ERE


Romao:2001:SMA

Artur Romão and Miguel Mira da Silva. Secure mobile agent digital signatures with
proxy certificates. Lecture Notes in Computer Science, 2033:206-??, 2001. [RE03]


Oded Regev. On lattices, learning with errors, random


[Ren:2009:FCS] Yanli Ren and Dawu Gu. Fully CCA2 secure identity based broadcast encryption without random ora-

Rafaeli:2003:SKM

Rhinelander:2003:DIE

Rich:2007:ATS

Rila:2002:DAB
REFERENCES


REFERENCES

Roy:2004:FSE


Reyhani-Masoleh:2003:LCS


Reyhani-Masoleh:2003:LCB


Ruiz:2001:SPS

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


REFERENCES


[Rob09] Andrew Robinson. *Lost languages: the enigma of the world’s undeciphered scripts.*
REFERENCES


[Rot02a] Volker Roth. Java security architecture and extensions. Dr. Dobb’s Journal of Software Tools, 27(4):34,
REFERENCES


REFERENCES

Roy:2005:ACA


Rieffel:2000:IQC


Razan:2000:RSS


Reyzin:2002:BTB


Ratner:2003:NGI


**Ratner:2003:NHS**


**Rosenberg:2004:SWS**


**Rittinghouse:2005:IIM**


**Rechberger:2008:NRN**


**Rechberger:2006:NCW**


**Rivest:2000:RA**
Rosenbaum:2000:SFR


Romer:2001:ILA


Rubin:2002:SAV


Rubin:2003:TBC

REFERENCES

[RS04]

[Rao:2005:CHE]

[Rubin:2008:CFF]

[RS00a]

[RS00b]

[RS00c]

[RS00d]
RSA Laboratories. *PKCS #15 v1.1: Cryptographic
REFERENCES


REFERENCES


References


[Russell] Alexander Russell and Hong Wang. How to fool an unbounded adversary with


REFERENCES

Saini:2002:JMD


Saeednia:2002:IBS


Sakamura:2001:GEI


Sale:2000:CGL


Sale:2000:CBP


Sale:2001:GRT


Salus:2001:CA


Salus:2001:CA

Salomon:2003:DPS

Salomon:2005:CDC

Salus:2003:BRBb

Sale:2005:RCB

Sallee:2005:MBM
Salomon:2007:DCC


Sale:20xx:CRP


Samid:2001:ESR


Santini:2005:WSI


Sarkar:2002:FCM


Sasse:2007:REB

1540-7993 (print), 1558-4046 (electronic).

**Satoh:2006:DP1**


**Savelli:2004:NDC**


**Soto:2000:RTA**


**Shacham:2001:ISH**


**Scott:2004:CP**


**Stoklosa:2005:CIC**

REFERENCES

Stallings:2007:CSP


Sherwood:2005:MTR


Steiner:2001:SPB


Smeraldi:2002:SVF


Shehab:2005:SCM


Shehab:2007:WSD


Steinfeld:2002:NSA

Ron Steinfeld, Joonsang Baek, and Yuliang Zheng. On the necessity of strong assumptions for the security of a class of asymmetric encryption schemes.
Seredynski:2004:CA


Syverson:2001:LAP


Stoll:2002:MMC


Sun:2002:WDC

Shao:2005:NEV

Stephanides:2005:GAK

Sun:2005:IPK

Siegelin:2001:SCD

Schmalz:2000:MAD

Schneier:2000:AAR
REFERENCES

Schneier:2000:IRS

Schneier:2000:SLD

Schneier:2000:SRF

Scharinger:2001:ASK

Schindler:2001:TAA

Schmalz:2001:MDI
REFERENCES

Schneier:2001:FSE


Schneier:2003:BFT


Schmalz:2004:MDIa


Schnorr:2001:SGH


Schnorr:2001:SDE

Schmalz:2004:MDIb


Schneier:2004:SA


Schneier:2005:AE


Schneier:2005:TFA


Schramm:2006:AMS

REFERENCES


REFERENCES


Smith:2001:ADB


Spiekermann:2009:ACR


Seacord:2005:SCC


Seetaraman:2004:BRB


Smith:2006:SID

REFERENCES

Seifried:2000:C


Seifried:2000:PPA


Seifert:2005:ACR


Speed:2001:PIS


Speed:2002:PIS


Selcuk:2000:BELL


Semanko:2000:CAA


Sennewald:2003:ESM

[Sen03] Charles A. Sennewald. Effective security management.


Michael Sutton, Adam Greene, and Pedram Amini.
REFERENCES


Steinwandt:2001:TDB

Steinwandt:2000:WHS

Sauvage:2009:ERF


Storer:2009:PSR

Mark W. Storer, Kevin M. Greenan, Ethan L. Miller, and Kaladhar Voruganti. POTSHARDS — a se-

Stone:1998:PCC


Sonnag:2000:MAS


Shirase:2005:AEC


Shailer:2001:PMT


Shamir:2001:NDC


Shamir:2001:PSC

REFERENCES


**Shao:2001:BVM**


**Sharp:2001:IKB**


**Shapiro:2002:CCM**


**Shamir:2003:RS**


**Shamir:2003:TLC**


**Shao:2003:CIB**

Shao:2003:PSS


Shaltiel:2004:RDE


Shao:2004:IDS


Shao:2005:CXY


Shao:2005:IEP


Shao:2005:NKA


Shao:2005:SMD


Shepherd:2001:CDC

Simon Shepherd. Cryptography: diffusing the confusion, volume 5 of Communications


Shparlinski:2005:PHS


Sun:2005:SSP


Shumba:2006:THL


Shyamasundar:2002:ACP


Silverman:2001:CLI


Silverman:2005:ECC

Joseph H. Silverman. Elliptic curves and cryptography. In


REFERENCES

Revised and updated by Todd Feil.

Stubblefield:2004:KRA


Sivonen:2006:MPF


Schnorr:2000:SSE


Sucurovic:2005:JCX


Schaumont:2009:GEI


Song:2000:TPA

Seki:2001:DCR

Stojanovski:2001:CBRa

Sklavos:2005:ISH

Stavrou:2005:CAS

Stabell-Kulo:2006:ESC

Saldamli:2007:SME

Shu:2009:RCA
Chang Shu, Soohak Kwon, and K. Gaj. Reconfigurable

**Sugita:2001:SRV**


**Sano:2000:PEA**


**Schindler:2001:IDC**


**Srinathan:2002:ASC**

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


Scharwaechter:2007:AAE


Sterbenz:2000:PAC

Andreas Sterbenz and Peter Lipp. Performance of the AES candidate algo-

Shim:2005:SFA


Srivatsa:2005:SPS


Skoudis:2006:CHR


Stamp:2007:ACB


Sun:2009:CPR


Su:2005:KPK

Pin-Chang Su, Erl-Huei Lu, and Henry Ker-Chang Chang. A knapsack public-key cryptosystem based on elliptic curve discrete logarithm. Applied Mathematic-


[SM00a] Palash Sarkar and Subhamoy Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. Lecture Notes in Computer Sci-
REFERENCES

Sarkar:2000:NBC


Sarkar:2001:EIL


Sebag-Montefiore:2000:EBC


Satoh:2002:SHS


Sarkar:2003:EIC

[SM03a] P. Sarkar and S. Maitra.
Efficient implementation of cryptographically useful “large” Boolean functions. [SM07a]


REFERENCES


REFERENCES


Strembeck:2004:IAE


Schlager:2007:EAA


Sakai:2000:NDS

Hideaki Sakai, Noriko Nakamura, and Yoshihide Igarashi. A new definition of semantic security for public key encryption schemes.

Safavi-Naini:2000:STT

Safavi-Naini:2001:BAG


Safavi-Naini:2001:LAC


Sanchez:2001:RNM


Slind:2007:PPS


Song:2000:ISC

Shigetomi:2002:ALS


Smith:1979:UFM


Satoh:2000:HSM


Shelfer:2002:SCE


Sumii:2003:LRE


Solachidis:2004:WPL

REFERENCES


REFERENCES


[StDenis:2006:BMI]


André Seznec and Nicolas Sendrier. HAVEGE: a user-level software heuristic for generating empirically strong random numbers. *ACM Transactions*


StPierre:2000:TFA


Sakurai:2001:NSS


Shamir:2001:IOO


Stern:2001:ADW


Stinson:2001:SAC

REFERENCES


[Sakurai:2002:SMP]

[Satoh:2003:SDF]

[Shamir:2003:FLN]

[Spivak:2006:SPT]

[Stallings:2000:SSC]

[Stallings:2002:CNS]
REFERENCES

Standboge:2002:ENO


Stajano:2003:SCU


Stanik:2005:NLO


Stamp:2006:ISP


Sterlicchi:2000:SCD


Steinwandt:2001:LTP

REFERENCES


Stefanek:2002:ISB


Steele:2005:PPT


Steil:2005:MMM


Stern:2005:MLF


Stein:2008:ENT


Stinson:1995:CTP


Stinson:2001:C

REFERENCES


Strunk:2001:JQJ


Strubinger:2002:HBS


Stytz:2004:BRW


Saxena:2007:TCP


Shaltiel:2007:LEU


Sugihara:2001:PCD

Sugita:2003:DRW


Sun:2005:UMS


Sun:2000:DRR


Sun:2000:ESM


Sun:2002:IIIR


Shaltiel:2008:HAP


Sebê:2007:SMO


Sebê:2007:SMO


Francesc Sebê, Alexandre Viejo, and Josep Domingo-Ferrer. Secure many-to-one symbol transmission for implementation on smart cards.
REFERENCES


Shmueli:2009:DEO


Schneier:2000:PCF


Sun:2000:AFA


Stubblebine:2002:ALF


Shim:2005:WIB

REFERENCES

Swaine:2001:PPSa


Swenson:2008:MCT


Song:2005:ISG


Sun:2009:TDS


Swire:2005:SMI


Stevenson:2005:SCI


Song:2007:TAK

[SWT07] Dawn Xiaodong Song, David Wagner, and Xuqing Tian. Timing analysis of keystrokes and timing attacks on SSH. Report, University of Cal-

...


REFERENCES


REFERENCES

CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Sun:2002:NAD

Sun:2005:WIW

Tada:2002:OSM

Tang:2001:AES

Tang:2007:MMU

Tang:2007:SGK

Tattersall:2005:ENT
James J. (James Joseph) Tattersall. *Elementary number theory in nine chapters*. Cambridge University Press,
REFERENCES


REFERENCES

September 15, 2005. CO-DEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

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**

Yuh-Min Tseng and Jimn-Ke Jan. Cryptanalysis of Liaw's

**Tseng:2003:DSM**


**Tico:2003:RAS**


**Toll:2008:CSE**


**Thien:2002:TSS**


**Thomas:2007:HQU**


**Turner:2006:SIS**


[TMH]


[TM]


[TNM]


[TNM]

Tousidou:2000:IMS


Tanaka:2001:QPK


Tochikubo:2000:RAE


Tomaszewski:2006:YSY


Topham:2002:BRJ


Totsch:2000:MSS


Tague:2007:CSA

Patrick Tague and Radha Poovendran. A canonical

**Trope:2007:CSD**


**TPPM07**

**Trope:2009:CCGb**


**Tropman:2001:GED**


**TPS01**


**Trimmer:2009:CCGb**


**TR09b**

**Troutman:2008:VMM**


**Tro08**

**Tsaur:2001:FUA**


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

REFERENCES


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


Toft:2001:LTT [TW06a]


Trappe:2005:ICC


Talbot:2006:CCI


Trappe:2006:ICC


Tsai:2007:TTA

Tsaur:2005:EUA


Tiwari:2009:CIF


Thamrin:2008:PBR


Tzeng:2004:NTM


Ting:2002:FBS


Tynan:2005:CPA

[Tyn05] Dan Tynan. Computer privacy annoyances: how to

Tian:2005:NDF


Tong:2009:RAPa


Tong:2009:RAPb


Uz:2009:MBT


Unay:2008:SQE


United States Congress. House Committee on International Relations. H.R. 850, the Security and Freedom through Encryption (SAFE) Act:
markup before the Committee on International Relations, House of Representatives, One Hundred Sixth Congress, first session, Tuesday, July 13, 1999. Washington, DC, USA, 2000. iii + 102 pp. Shipping list no.: 2000-0214-P.


Andreas Uhl and Andreas Pommer. Image and video encryption: from digital rights management to secured personal communication, volume 15 of Advances in information security. Springer-Verlag, Berlin, Germany / Heidelberg, Ger-
REFERENCES


[USENIX:2001:PUA]

[USENIX:2001:PFT]

[USENIX:2001:PTU]

[USENIX:2002:PBF]

[USENIX:2002:PUS]

[USENIX:2002:PFT]
Utami:2002:FID

Urien:2001:XS

Ustimenko:2001:CGT

Ulfving:2000:GS

Uzun:2004:BRC


vanDijk:2004:AOC

Verheul:2001:EXM

Vercauteren:2002:CFZ

Vergnaud:2006:RBS

Vernitski:2006:CUM

Vladimirov:2004:WFS
REFERENCES

Vassev:2009:STA

Voloshynovskiy:2001:BDA

Viroli:2003:TPA

Vixie:2002:SRR

Vural:2007:IND

Vo:2008:SMA
Duc-Liem Vo and Kwangjo

Volos:2009:IEP


Viega:2003:SPC


Viega:2002:NSO


Vasco:2005:NCS

REFERENCES

[VAH04]

[VOI05]

[VOO18]

[VOS1]


[VOG01]
REFERENCES

[Voyiatzis:2008:SFS]

[vanTilborg:2000:FCP]

[vanTilborg:2001:ECC]

[Venkatesan:2001:GTA]

[Voyniyatzi:2007:POK]
REFERENCES

von Willich: 2001: TIT

Vaudenay: 2001: SAC

Whittaker: 2006: HBW

Woo dy: 2007: COS

Weitzner: 2008: IA

Wachsmann: 2005: CAK
REFERENCES

Wallach:2000:SSM


Wagner:2000:CYL


Wagner:2002:GBP


Walsh:2000:BRM

COLIN D. WALTER


William P. Wardlaw. The RSA public key cryptosys-

[Washington:2008:BRB]
Lawrence C. Washington.

[Washington:2008:ECN]
Lawrence C. Washington.

[Way02b]

[Way09]

[Way2001:FBA]

[WB00]
Richard Weiss and Nathan Binkert. A comparison of AES candidates on the Alpha 21264. In NIST [NIS00], pages 75-81. ISBN
REFERENCES

[Wu:2002:CSCa]

[Wu:2001:CDS]

[WB02]

[WB01]
REFERENCES


REFERENCES

Wehde:2000:IME


Weierud:2000:SFB


Weierud:2000:IME

Weiss:2004:JCE


Weng:2003:CHC

REFERENCES


[Wang:2005:RST] Lijun Wang and Chao Gao. Rough set theory’s application on intrusion detection based on system calls. In Han et al. [HYZ05b], pages
REFERENCES

LCCN ???. URL http://
eproceedings.worldscinet.com/9812701532/9812701532.0031.html.

[WGL00] Chung Kei Wong, Mohamed
Gouda, and Simon S. Lam.
Secure group communications
using key graphs. IEEE/ACM
Transactions on Networking,
CODEN ILEANEP. ISSN
1063-6692 (print), 1558-2566
acm.org/pubs/citations/journals/ton/2000-8-1/
p16-wong/.

[Wu:2002:CAE] Tzong-Sun Wu and Chien-
Lung Hsu. Convertible
authenticated encryption
scheme. The Journal of
Systems and Software, 62
CODEN JSSODM. ISSN
0164-1212 (print), 1873-1228
electronic).

[Wu:2002:IBM] Tzong-Sun Wu and Chien-
Lung Hsu. ID-based multi-
signatures with distin-
guished signing authorities
for sequential and broad-
casting architectures. Ap-
plied Mathematics and Com-
pilation, 131(2–3):349–356,
September 25, 2002. CO-
DEN AMHCBQ. ISSN
0096-3003 (print), 1873-5649
(electronic).

[Wu:2003:TSS] Tzong-Sun Wu and Chien-
Lung Hsu. Threshold sign-
signature scheme using self-
certified public keys. The
Journal of Systems and Soft-
ware, 67(2):89–97, August
15, 2003. CODEN JS-
SODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic).

Hu. A new watermarking
method for 3D models
based on integral invariants.
IEEE Transactions on Visualiza-
tion and Computer Graphics,
2009. CODEN ITVGEA. ISSN
1077-2626 (print), 1941-0506
electronic), 2160-9306.

[Wen:2005:URE] Hsiang-An Wen, Sheng-
Yu Hwang, and Tzonelih
Hwang. On the unlinkability
of randomization-enhanced
Chaum’s blind signature
scheme. Applied Mathematics
and Computation, 164
CODEN AMHCBQ. ISSN
0096-3003 (print), 1873-5649
electronic).


REFERENCES


REFERENCES


Windley:2005:DI

Windley:2005:GEC

Windley:2005:SAU

Withers:2001:IWU

Wang:2007:VBW

Welschenbach:2001:CCC

Wang:2005:ECSb
Chih-Hung Wang and Yan-Sheng Kuo. An efficient

**Won:2006:ISC**


**Walter:2003:CHE**


**Wang:2002:AAB**

658


D. J. Wheeler and R. M. Needham. TEA, a tiny encryption algorithm. Lecture Notes in Computer Sci-
REFERENCES

Watanabe:2002:CCD

Wang:2008:NAD

Wang:2009:RDA

Wolkster:orfer:2001:AIA

Wollinger:2004:SHI

Won:2001:ISC
Dongho Won, editor. Information security and cryptography: ICISC 2000, Third International Conference,

Wool:2000:KME


Wang:2003:SGP


Wollinger:2005:CVH


Weimerskirch:2001:ECC


[WRW02] Xinyuan Wang, Douglas S. Reeves, and S. Felix Wu. Inter-packet delay based correlation for tracing encrypted connections through


[WRW02] Xinyuan Wang, Douglas S. Reeves, and S. Felix Wu. Inter-packet delay based correlation for tracing encrypted connections through

Wright:2002:EPS


Whiting:2003:MPH


Weimerskirch:2002:DLW


Wu:2001:DSM

REFERENCES


REFERENCES

Wang:2004:CWS


Wolf:2005:NML


Wang:2006:SPS


Wang:2008:DCP


Wu:2001:CFF

Worley:2000:AFP


Wollinger:2000:HWH

Thomas J. Wollinger, Min Wang, Jorge Guajardo, and Christof Paar. How well are high-end DSPs suited for the AES algorithms? AES algorithms on the TMS320C6x DSP. In NIST [NIS00], pages 94–105. ISBN ???? LCCN ?????

Wincelberg:2002:LIE


Wang:2008:HQS


Wang:2002:WEM

Shiuh-Jeng Wang and Kai-Sheng Yang. Watermark embedding mechanism us-
REFERENCES


Wu:2005:CTR


Wang:2005:CHA


Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743

Wang:2005:FCFb

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [Sho05a], pages 17–?? ISBN 3-540-28114-2. ISSN 0302-9743


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

**Xiao:2003:HPC**


**Xiao:2005:SPA**


**Xenakis:2006:GCO**


**Xu:2007:CAD**


**Xu:2005:ADR**


[YAN07] Song Y. Yan. *Cryptanalytic attacks on RSA*. Springer-Verlag, Berlin, Germany /
REFERENCES


Yekhanin:2007:LDC


Yan:2006:ICP


Youssef:2001:CIM


Youssef:2001:CPK


Youssef:2001:IAB


Youssef:2001:CPK

REFERENCES


REFERENCES


Yardi:2008:HAC
REFERENCES


REFERENCES


Young:2006:MCC

Youn:2008:WRB

Yang:2009:AIO

Yin:2001:RMW

Yilek:2009:WPK

Yoon:2004:SUA
REFERENCES

Yoon:2005:CFI


Yoon:2005:ICJ


Yoon:2005:IFA


Yeh:2002:SAK


Yeh:2004:PBU


Yanami:2002:DLC

REFERENCES


REFERENCES


REFERENCES

Yang:2005:CIA


Yang:2006:SED


Yang:2005:IYS


Yang:2008:VCS


Yang:2008:FSD


Yang:2009:CLW

REFERENCES

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

Young:2000:RBA


Young:2001:BOK


Young:2004:MCE


Yoon:2005:CZX


Yoon:2005:SWL


Ye:2001:ATD

REFERENCES

You:2001:GEC


[YYZ01]

Yen:2000:WOW


[YZ00]


Zafar:2000:ACB


[Zaf00]

Ye:2007:NAW


[Zan01]

Zane:2001:EWD

REFERENCES


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 ???

Zhang:2000:MCA


Zhang:2004:AIB


Zhang:2005:CHC


REFERENCES


[Zhe01] Yuliang Zheng. Identification, signature and sign-

Zheng:2002:NPK


Zheng:2002:ACA


Zhong:2006:ESC

REFERENCES

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

Zirkind:2007:ADC

Zhang:2004:BAF

Zhang:2009:IBR

Zhang:2002:IBB
Zhang:2005:CLH


Zhang:2004:SAE


Zenner:2001:ICS


Zhang:2004:AFV


Zhang:2004:RMA


Zhao:2005:MCE


Zhang:2001:QKD

Yong-Sheng Zhang, Chuan-Feng Li, and Guang-Can Guo. Quantum key distribution via quantum encryption. *Physical Review A (Atomic, Molecular,
REFERENCES


Zhang:2002:CRD


Zhang:1999:AFV


Zhang:2005:DMC


Zolman:2001:SEM


Zhang:2001:CIS


Zheng:2007:SRI

Zhou:2005:MBI


Zhu:2007:IHH


Zhang:2005:RPE


Zhao:2005:APA

Meiyuan Zhao, Sean W. Smith, and David M. Nicol. Aggregated path authentication for efficient BGP security. In Meadows and Syver.


Zhou:2005:APS


Zhang:2001:ASE


Zhang:2003:FSP

REFERENCES


REFERENCES


[ZYW05] Peng Zhang, Chengqing Ye, and Xueying Ma. Improvement of secure mobile agent system in elec-
REFERENCES

Electronic commerce. In Han et al. [HYZ05b], pages 114–?? ISBN 981-270-153-2.


[ZYW07] Robert W. Zhu, Guomin Yang, and Duncan S. Wong.