A Bibliography of Publications on Cryptography:
1990–1999

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/
13 March 2015
Version 1.88

Title word cross-reference

#1
[Ble98a, Kal98b, KS98a, RSA93f, RSA93a].
#10 [Kal98c].
#11 [Ano95j, Ano96k].
#12 [RSA99a].
#14 [BG98].
#15 [Nys99].
#3 [RSA93b].
#5 [RSA99b].
#6 [RSA93c].
#7 [Kal98f, Kal98d, RSA93d].
#8 [RSA93e].

((2^n)^m) [PSR97]. (2^n ± 1) [Zim99]. (k, n)
[KOO95b, KOO95a]. (t, n) [LWC96]. +
[Zhe97b]. $1$ [Gar97b]. 1 [JW98b].
$1$-Million [GC97]. 16 [BS93a, GC94]. 2
[JW98b, KG95, Kob91b, MVZ98, SBV99].
$29.95$ [Hatt96]. 2n [QG90]. 2R [YLD99]. 3
[Ben99, BALS99, CK95, KSW97b, Nas94,
TK99, Wors96, YY99a]. 511 [CC98]. 64

[MIM97]. 8 [Miy90]. << [Zhe97b]. 2 [TZ94].
x [Hol91]. A [BMT96]. $A + BN$ [Bak92]. $A^2$
[JS95b]. mod2^a2 [Ber93]. c [WD99b]. $\chi^2$
[HG97b]. d [BD99b]. $\ell$ [BR91]. f [DJL93].
$F_2^n$ [MVZ93]. $F_2$ [SS98a, Ler97]. $F_p$
[Miy93a]. $GD(2^n)$ [Ara93]. GF(2) [She95c].
GF(208) [Ros98a]. GF($2^m$) [FBT96]. GF(p)
[Gor93b, HNM98]. $\gg$ [GQW+91].
[Car97c, DJL93, HKS97a, HKS97b, KRR99b,
KRS97b, WDR99b]. l [HL93a, KS97b]. L2
[Vau99a]. $\lambda$ [RS99c]. L $\geq$ 2 [SvW91]. $\ll$
[GQW+91]. m [Bla94a, FR94]. N
[BS91c, BS91d, HKS97a, HKS97b, KSW99b,
KSW99c, KK98, Per93, QG90, Tak97].
$N = p^r q$ [BDHG99a, BDHG99b]. N.0.292
[BD99b]. P [BS90b]. p^q [Tak98b]. r
[BDHG99a, BDHG99b, FJRS96]. s
[YT95a, YT95b]. $s^2$ [Knu93b]. Step_k,m

1
[GC90]. \( t [\text{KOO95b, KOO95a}]. T^3 P \)
[GPSV98]. \( y^2 + axy = x^3 \pmod n \) [Koy95].
[z [MS93], \( Z/nZ [\text{CLL99, MM96b}] \), \( Z^*_n \) [ML98], \( Z_n \),
[KMOV91, OFF93, VZ97, KK98, SE96].

- [JV98b]. -Adic [KG95, Tak97]. -Bit
[QG90, MM97]. -boxes [YT95a, YT95b].
-calculation [RS99c]. -Cascades [GC90].
-Cheater [KOO95b, KOO95a]. -Codes
[JS99b, MS93]. -D [CK95, TK99].
-Decorrelation [Vau99a]. -Dependent
[DJL93]. -DES [Knu93b]. -Dimensional
[Per93]. -divisibility [FR94]. -Fields
[BMT96]. -fold [BR91]. -formulæ
[WD99b]. -Hash [BS91c, BS91d]. -means
[SBVG99]. -Round [BS93a, GC94].
-sequences [Ba94a]. -Span [HL93a].
-Tuples [FJ98]. -WAY [KSW97b].
-wheel [Car97c].

/ [Ano96k, IEE92b, IEE94c, IEE96c, IEE97i, TV94]. / [Acc97, Cla98a].

0 [CJ98]. 0-387-94441-9 [Hat96].

1 [Ano93k, CCN95, Nat95]. 1.0.1 [Sun91b].
1.2 [DD98e, DD98f, Zuk98a]. 10
[CMM93]. 101 [Hon98]. 1040 [Lin98a].

105-1
[Un98a, Un98b, Un98g, Un98j, Un98i].
105-263 [Un98i]. 105-322 [Un98g].
105-415 [Un98]. 105th [Ano98f]. 10th
[Ano93d, CMM93, IEE94c, USE96a]. 1113
[Lin98a]. 1186 [Riv90a]. 11th [SJD93]. 120
DML94]. 128-Bit
[SKW98b, DKR97b, Knm98c, Lim98,
Luc98a, Luc99a, Luc99b, SKW98c]. 12th
[Bri92, Bri93, KG96]. 130 [Ano96b]. 1320
[Riv92a]. 1321 [Riv92b]. 1334 [LS92]. 1395
[Un94a]. 13th
[IE97b, IEE97c, Sti93b, Sti94]. 1409
Bor93a]. 1411 [Bor93b]. 1412 [Ala93b].

1416 [Bor93c]. 1421 [Lin93a]. 1446
[GM93a]. 14th [Des94b, KK99]. 15
[UU97b]. 1507 [Kau93]. 1510 [KN93]. 1511
[Un93c]. 1544 [Ros93]. 15th
Cop95b, Cop95d, NIS92]. 16 [HB99]. 16-18
Q+98]. 16-bit [Bro97]. 160
[BDP97, DBP96, PBD97]. 16th
Kob96, MSD90]. 1704 [HA94a]. 1731
[Mye94a]. 1734 [Mye94b]. 17th
[He96a, Kal97c]. 180 [Nat95]. 180-1
[An95i, Nat95]. 1810 [Ton95]. 1824
[Dan95]. 1826 [At95a]. 1827 [At95b].
1828 [MS95c]. 1829 [KMS95a]. 1847
[GMCF95]. 1851 [KMS95b]. 1852
[MS95d, MS95e]. 1864 [MR95b]. 18th
[Kra98, Yua92]. 1915 [Kas96]. 1929 [Lee96].
194 [Un94a]. 1940 [CWM91]. 1961
1993 [ACM93b]. 1994
[An94e, Sim96b, Un95a]. 1995
[Ame95, Dan95]. 1995/4 [Dan95]. 1996
[An95f, UU97b]. 1997
[ACM97a, AN97, Acc97, MZ98, Un98a,
Un98c, Un98b, Un98d, Un98e, Un97b,
Un98f, Un98g, Un98i]. 1998
[ANS98b, ODP98, RD99a]. 1999 [I99a].
19th [An96a, Tv92, Wie99]. 1B [Lea99].
1st [ACM93a].

2 [BA97, DS97c, DFKN93, HG97c, HG97d].
2-6 [IEE95c]. 2-adic [GK95a]. 2-key
[HP99a, HP99b]. 2-Prover [DFK93].
2.2gn [An97f]. 2015 [Elk96]. 2040
[BR96a]. 2058 [RRS97a]. 2069
[FHHB97]. 2082 [BA97]. 2085 [OG97].
20n [DB96d]. 20th [CWM91]. 21-25
[BS95c]. 21-January [USE91]. 2104
[KBC97]. 2138 [RRS97b]. 2144 [Ada97b].
2154 [MB97]. 219 [EMC96]. 21st
[KG96, Sch96b]. 2222 [Mye97]. 2268
[Riv98a]. 2284 [BV98b]. 22nd [IEE97].
2313 [Kal98b]. 2314 [Kal98c]. 2315
[Kal98f, Kal98d]. 23rd [IEE98f]. 2402
HY98b, HY98a, JG95, KSW99b, KR96b, KOT95a, KOT95b, LL94a, LvD98, NY90, OK96b, RS93, SG98, WK97, Win93, YL97b.

Age [Bar94, SB97, Uni98, Wal95, BS97b, Car97a, Joh98, Mar95b, Uni97c, Duh90].

Agencies [MKS99]. Agency [Gar97a].


Agile [KLZL99, THP98]. Agnes [Luj98].

agnostic [JY96]. Agree [Gar97a, Ano97-27]. Agreement [BWM99a, Bor95, Bor96, Cae96b, Gar94, Gar97c, JV96, LM94b, LP99, Mau93a, MW98d, MDP94, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. Aids [Cra92]. AIR [Ano97r, DIF94, SVA+98].

AIR-BAG [Ano97r]. Airborne [CKN99].


Albuquerque [IEE91]. aléatoire [Bou94].


algorithmic-geometric [JM96a]. ALGOL [RS99c]. Algorithm [ANS97, Ada97b, IBM93, Ano96c, Ano96e, ADEDS99, COP+95a, CD91, DK97b, DNRS97, Dra98, GX99, GK98, GT94, GN95c, HG97a, HG97b, HW98, Kali91, KY95a, KR96a, KY98, MK99b, Kob98c, Kra93, Kwa97, MD98, MW94, Mas94, Mat97, MS90b, Mom99, Nat97b, PBGV90, PRB98b, Riv92a, Riv92b, Riv95c, Riv95b, Riv98a, RC94a, RC94b, RH99, Sch93d, Sch94f, Sch95a, Sch95b, SW98e, Sch98g, SW98h, SHK99a, SW99e, SW99f, She94b, SB98, SW93, Sta99b, Swa94, TK99, THP98, VK98, Whe94, Yin97, ZY98a, BF94, BS95a, Bow93, CC98, CG94, ISO97, KN98b, JMW94, KY95b, KY97, KYxx, Kir95, LR93, LZ91a, LL93b, Lon91, LC97b, MSS93, MPL99, Mol98, Pai96, Riv90a, Riv91b, Riv95d, Sch91a, Sch94i, Tay94, Vad95, VN95, VL93, YL95b, ZW99, ZPS93].Algorithm [AA95, Acc97, LL98, Moe97, OA94, Sch93b, Sch94e, See97, Sim93, Sta94b, WSK97a, WSK97b].

Algorithm-Agile [THP98]. Algorithms [ACM97b, ANS97, Ano95a, Ano95b, Ano96b, Ano97c, AMP99, Ata99, BS99a, BP98a, BR96a, Bas98, BGM97a, BGM97b, BL96b, BL96a, Buc91a, DGV92, FCD98, GL98, Gl99a, HEQL98, KM98a, KAK96, KB92, LC99, Lei99b, LD99, MT99b, PSR97, PA98a, PA98b, S93b, For98, Pre97a, PRB98b, PRB98a, QR69, RS99a, Sch94f, Sch94j, Sch94e, Sch96a, SW97a, SW97b, Sch94h, Sot98, SB99, Sp95, Ste96, VCF90, AA95, Ano90, CPP98, CMM93, CJL92, Cad96, DG, DN95b, FR95a, GP97, HJ99, HP94, Imp92, KKL99, MS99c, OS91, OS92, PV96, Q98a, Sch91b, Sm93a, Tab94, TY92, Tay90, TV94]. Alive [BK90]. All-Or-Nothing [Riv97c, Ste98b, BMM99a, BM99b, Boy99, SRY99].

 Alleged [Gol97d]. Alley [KR96a, PR98b, Sch94f, Sch95a, Sch95b, Swa94]. Alliance
GPT91a, GPT91b, Gog99, GQ95, HN99S9, HHY93, Hat97, He94, Hof99, IRM93, IR99, JDK+91, KMP99, KP99a, Ki96, KK95, LOX99, LC99, Mar98a, Man96b, Mr91a, Mun91b, NC97, PSN95b, QV90, QG95, Rog95, Rue93, SSS98, Sch96i, Sz93, SK98c, SK98b, SKIT99, VDDR99, Ara93, BY93c, BY93b, CC98, DDD95a, DDD95b, DF97, GZ91, HP94, LL97b, MW94, Nyb98, Pet91, PK97, SI93b, SRR98, SIu99, Ste99b, SW98, SW99a, TY92, Woo90].

Applications [Aga92, BGR98a, BFW99, CJR98a, CGB+93, COZ99, Cr90, Dan96, DY91a, DFGH99, Duf98, DN94, Do97, Ebe93, FMM99, Far93, Fis98, IE95a, IEE97a, IEE92b, IE94c, IEE97b, JMS96, KSHW97, KSHW98, KSW99b, KSW99c, KM96a, Knu94b, KTG91, Lan97, MS95f, OiD98, OOO90, PS96b, SY96a, TN96a, TN96b, VV98, VP96, ZYR91, vW94, vW95, ACM99c, Ad91, An98b, BM90, Ber93, BMP+97b, BY97, Boy98, BP97b, Com96, CFG96, DiD96, Dom96, Eng99, FO98, GvP98, Gre94, GS94b, HMP95, JV98a, Ka95, KW92, KG93, LC93, LN94, Lub96, Mei92, Mic97, MT98, KNC94, Ped91a, PC98, Rob95, Sch90c, Sch97c, Sha95a, SSM94, Sin95, Sta97c, SSG99, T+98, USE96e, Way98, YL93, ZY90]. Applied [BHJM99, HH98, MR95a, Sch99a, Schl94, Sch96a, Sch94b, Sha99a, FWF99, FMR99, MV97, PR98, CMM93, Dav94].


Arithmetic [BM93, BCC99, CJR98a, CJR98b, CO98a, CGB+93, COZ99, Cre90, Dan96, DY91a, DFGH99, Du98, DN94, Dwo97, Ebe93, FMM99, Far93, Fis98, IE95a, IEE97a, IEE92b, IE95c, IE97b, JMS96, KSHW97, KSHW98, KSW99b, KSW99c, KM96a, Knu94b, KTG91, Lan97, MS95f, OiD98, OOO90, PS96b, SY96a, TN96a, TN96b, VV98, VP96, ZYR91, vW94, vW95, ACM99c, Ad91, An98b, BM90, Ber93, BMP+97b, BY97, Boy98, BP97b, Com96, CFG96, DiD96, Dom96, Eng99, FO98, GvP98, Gre94, GS94b, HMP95, JV98a, Kal95, KW92, KG93, LC93, LN94, Lub96, Mei92, Mic97, MT98, KNC94, Ped91a, PC98, Rob95, Sch90c, Sch97c, Sha95a, SSM94, Sin95, Sta97c, SSG99, T+98, USE96e, Way98, YL93, ZY90]. Applied [BHJM99, HH98, MR95a, Sch99a, Schl94, Sch96a, Sch94b, Sha99a, FWF99, FMR99, MV97, PR98, CMM93, Dav94]. apply [Cl97, UU97b]. Applying [CO98a, HO96, Jan99, KMP99, MW98a, War98, ARR99].

Arresting [Mad92]. arsenal [Me98]. Art [Eri99, Lan98, NM96a, Pre98c, She92e, BFS92a, BFS92b, Beu94, B+96b, PG93d, PR98]. article [Bur98]. Artificial [An96l, SBTV99]. Arts [Tv92]. Asia [Uni98c]. ASIACRYPT
[IRM93, KM96a, PSN95b, PSN95a].
Asiacrypt'98 [OiD98]. ASIACRYPT'99
[LOX99]. Asian [GO96c]. ASICS [DN95a].
Asimov [CFK+91]. asking [MILY93].
Aspect [LL99]. Aspects [Des98c, Sch98b, Ved93, ZTR99, Kob98b, Lid90, Pos98].
Aspray [CFK+91]. Assessing [AFB95, KAK96].
Assessment [EN98, ENK99, FL93]. asset [Oko97].
assign [LL93b]. Assignment [Hwa97, RH99, GPSN97].
Assistance [IS91, HY93a, Wu92]. Assumption [Sak96, Sal98].
Assumptions [AB99a, AB99b, BD91, KRS99, NOV93, Oka93a, Sim98c].
Assurance [IEE94b, IEE96d, KYG92]. Assuring [Car95].
ASTRAL [Dan97]. Asymmetric
[BWM98, FO99b, Jak99c, JM96b, Pat96, PG97a, PG97b, PS96a, PW97b, Thu95, BR94b, BR95a, MI90].
Asymptotic [SOB98]. Asynchronous [AMP99, TY94].
AT&T [SSM94]. Athena [DS90b]. Athens [Kat97].
Atlanta [ACM99b]. Atlantic [Bra94b]. ATM
[PS98c, PS98d, PS98e, PS98f, PS99a, PS99c, PS99b, PS99e, THP+98, VSH97]. atomic
[BBS98b]. Attack [BP98b, Ber97c, dBB91, BDF98, CG99, CS91, CML99, Cop94b, CS98b, DBC+99, Dod96b, EH96, GC91, GC94, HK90, JK97, KSW98a, KSW98b, LA98, LD98, M199, Mis97, MS98, OM94, PBGV90, RS91, SMK98a, SK98c, SK98b, TOU94, Wag99a, BP98c, BB95b, BK95a, BQ97, HA94b, Hor98, JG95, Kuh98, KO95a, KOT95b, LG90, Lon91, Low95, MRS99, MY93a, Men95b, Miy90, RS98f, SNT93, SG98, SGS99, dB91, vOW91].
Attack-Resistant [LA98]. Attacking
[ESST99, LUC98c, SH95a, SH95b, IEE97c].
Attacks
[BQ95b, BQ95a, BBS99b, BK98d, BW99, BWM99b, BLE98a, Bon99, BKR97, CT994, CJR99a, CSV94, CNS99b, CMY98, Dae99, Dan91b, DY91f, FY95b, FG98, GGO99, GQW91, GS99b, HGS98, HK98, Hwa92a, HC98a, Jas96, JS95b, JJJ99a, JJJ99b, Jut98, KSW98d, Koc96b, Kwa93, KS97c, LR96, LL94a, Luc98b, MDS99, MSK99b, PV97, PK95a, PK95b, Pen96, PAK98, PW93a, SVx91, TJ99, Wa90, WK97, WZ98, Wol98, YY97b, ZS93, Bih94a, CP94, Cop94a, GO95, HY98b, HY98a, HLL+95, JS95a, KL95b, KM96b, Koc95, LM93c, NY90, OY91, SNT95, Tze99, TH99, YL97b, dV98, vT93].
Attaining [LL94a, ZS93, CP94]. Attempt
[MS99b]. Attitudes [CF99, Jun99, MI99].
Attorney [Mer97]. attract [MB99a].
attractions [BDC+99]. Attract [MB99a].
attribute [EC96, Ho99].
Attribute-Efficient [Hof99]. attributed
[Lea90]. Auction [PUF99]. Auctions
[Nur94, SS99a, SS99f, MB99a]. Audio
[An98f, BTH96, DH98a, NH98, NI98, BP98d, CKLS96c, SNT98, BCS97]. Audio-
[BCS97]. Audiovisual [PMP99]. Audit
[SK99, Yaa99a, Yaa99b, Ana93d, SS96].
Auditability [VNM95]. Auditable
[ST99a]. Auditing [SK97c].
auditorialization [HW91]. Auditorium
[IEE99b]. Aufenthaltsorts [FT95].
Augmented [BD98, KT98]. August
[B+96b, Bri92, Bri93, BS95e, Cop95b, Cop95d, Des94b, IE98b, Kal97c, Kob96, KP99b, Kra98, MSD90, Nat98, RD99a, St93b, ST94, TM99, USE90, USE98a, USE98b, USE99a, Wie99, Yaa92].
AUSCRYPT [SP90, ZS93].
Austin
[An94d, IEE98c]. Australasian [VPM97].
Australia [DG96, GN95b, KG93, KK99b, MSD90, PSN95b, SP90, ZS93, VPM97].
Australian
[CFK+91, GN95b, Cae96a, Orl96]. Austria
[BS95e]. Authenticated
[BF97a, BWM98, BWM99a, BZ97, CH97, Dan95, HC96a, JN96, LG97, Mau97a, RH93, CKWH96, BSNP96a, BSNP96b, BF99b, BR97b, Dv92, HY98b, HY98a, Yaa99].
Authenticating [ADS99, He98a, KS99a,
Mit92a, SK96a, LC94a. Authentication [ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94j, AS96, Atr95a, AR98, AC97, BA97, Bakh99, Bal99, Bec99, BR97a, BG90, BR94a, BCK96d, BCK96c, BM91a, BGS98, BR91, BBDF97, BH11a, Bis91, BHK11a, BGH91, Bis91, BHK99, BWM98, Ble98b, BV98b, Bor96, Bor93a, Bor93c, Boy92, Bru98, BAN90, CV93, CGM97b, COZ99, DLF97, DVPL92, DVW90, DY91f, DvW92, Dra99, DMFB97, BM91a, BGS98, BR91, BBDF97, BGH91, Bis91, BHK99, BWM98, Ble98b, BV98b, Bor96, Bor93a, Bor93c, Boy92, Bru98, BAN90, CV93, CGM97b, COZ99, DLF97, DVPL92, DVW90, DY91f, DvW92, Dra99, DMFB97, DS97d, Dwo95, ECM96, EPR99b, EPR99a, FGS96, fFl990, FHHB97, FL96, GHY90, GLZ99, GL96, Geh94, Geh95, GM90, Go90a, GBL94, Gue98b, Gui97, HK97, HA94a, HS94, HL92, Hill97, HP98b, Ins95, IH98, JS92a, Joe94, Koh95, KH94, KNS93, KCC94a, KCC94b, Kra95, KBC96, KBC97, Kuru94, KY92, KY92, KS97c, LABW91, LABW92, Lee96a. Authentication [LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Man96a, MAM95, McM96, Mee98, MS95c, MS95d, MW99, TMT92, Mor97, Mye94a, Mye97, NP97, OG97, OK91, OM94, Opp96, PKOT94, PS98c, PLWSN99, P991, PGV93c, Pre98a, Pre98c, MS95e, RS99b, RRSW97a, RRSW97b, Rsg95, SNT93, S939, ST94, SNT95, SNW98a, SNW98b, SSH93, SS96, SP99, SA95, SC96a, SC96, Sch94, Sch93, Sga90, Sga91b, She97, She95a, She96, Sim96b, SVxW91, SW94c, SKAM99, Sti91b, SL99, TAB90, Tay95, TN99, Tum99, Ude98, Van93, Van93, Wai93, WKG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wn96, Wn94a, Wn94b, ZG96, AG95, ABC+98, Ano97d, Atr93, BSNP97, BGR95, BCK98, BCX9c, BCX9d, BH+95a, B99a, Car94, CW97, CGM96, D990, D993, DH96b, Gu90, HS96b, Hor95, HC95b. authentication [HLL+91, HW98c, JC98, JC90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin89a, Low95, MSN97, MF97, Men91, MC96, Nac93, NT94, PS98c, PS98f, PS98h, RS98a, RS98f, Sg91a, Sga93, SY96b, Sta99b, Sti91a, Sun98b, Syv93, Tsu92b, Tsu92a, TH99, Ver98b, WL94, X98, Xie98, YL97a, YL97b, You97, Zuk98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a. Authentications [OO90, KSL92]. Authenticator [Zuk98a]. Authenticators [DF91a, SN96]. Authenticity [BK90, Lud97, MI90, Way91]. Authentication [Fly97]. author [Lea90]. Authorisation [COZ99]. authorities [Ame95, Ame96a]. authority [CFSY96, CGS97, JMO95a]. Authorization [BAPS95c, Cas95, FL96, W80a]. Auto [YY98, YY99]. auto-certifiable [YY98c]. Auto-Recoverable [YY99b, YY98c]. Automata [BI95, BG98, GOL92, HH99, KPR99, KV94, MC92, NC97, vWN99, Bao94, B949, BMP97b, BK98f, DYL98, NKC94, Sin99, CKF91]. Automated [Dan97, FIP93a, FSN93, FK99, GSN94, GDS91, She96a, SPGV98, VDDR99, WG99, CD98a]. Automatic [CWM91, MM99a, Na97, SK97b, SK97a, Sch99k, WKHG97, DF98, OA99]. Automating [Bur99, Sm93a]. Automation [Des99a]. Automaton [DD93, Gys96, DW96, MIZ98, Tao94, TCC97, TC99b]. automorphisms [VP96]. Autonomous [CKN90, RZ99]. autoscritcher [Dea98a, CF92, Cra92]. aux [Bec90]. Available [DD98c]. Avalanche [Cus96, CS96c, HT95, O’C94, ZZ95, SZZ94a, SZZ95b, YT96]. avant [Blo98a]. AVBPA [BC97]. Average [DLP93, Kob99]. average-case [AD99]. Avoided [NMR95]. avoiding [ZW99]. Award [Pin98]. Awarded [DD98b]. Awards [Eri97a]. Aware [BCC99]. Away [DD99]. Axis [AK99]. AXYTRANS [GBC93]. azo [SBTV99].

b [Cli97, UU97b, Ano99e, HS90, Lam99].
B-Trees [HS90]. ba [IPdNbbprm91].
Babbage [Fra93]. Back
[GC97, GO96c, WSFC99, IEE97e, WG97].
Backup [Mah96]. backwards
[BKR98a, BKR98b]. Bacon [Lea90]. Badge
[WHFG92]. BAG [Ano97r]. Baker [PS96b].
Bal [IPdNbbprm91]. Balance [RG99].
balanced [MCD98b, YT95a, YT95b].
Balatonfured [Rue93]. Ballot [CFSY96, BT94]. Ballots [Sal91].
Baltimore [ACM90, Ano96a, NIS92, USE92b]. Ban
[Gar97a, BP98f, XZZ97]. BAN-like
[XZZ97]. Bandwidth
[Bla96a, Bla96b, JMP98, MM92b, Sim98b]. Bandwidth-Efficient
[JMP98]. Banking
[Chi92]. Barbara [Bri92, Bri93, Cop95b, Des92, RCM99]. Based
[Des92, ADES99, BDPS95, BG90, BJY97, BS99b, BS99c, Ben99, BLM94, BBT94, BMT96, Bie98, BPR99, BMS94, BM96b, BM96c, Bie98a, BP99f, Bol98a, Bol98b, Bra95b, BP97c, CC99b, CS91, Cre97, DGV93, Dae95, Dan95, DNM98, DSSB95, DS96, DPP90, DMP98, DDM97, DQ94, Dem94, DF99, EKLM99, EN98, EN99, FCH99, FBS97, FK99, FMY98, FJM96, FBS98, FR95d, GKR97, GJKGR99, GRB99, GN95c, Gys96, Hes97, HPS98, HJPT98b, JO97, Jia99, JSZ94, J99a, KKS97, Kal98e, KR98, Kim93, KG95, KP96a, K97, KM99b, KA99, KMOV91, Kra94b, KH98b, LM93a, LM93b, LHY93, LL97a, Len99a, LW91, Liu98, MNSV97, MD99, MR95a, Mau93a, MM96a, MM99b, MM99b, MG91, MM99b, Mue99, MM99b, Miu99, NMR95, NM99, NOVY93, NS98a, Nec96]. Based
[NS97b, NM98, OM98, OO93, OFF93, vO91a, Pau99d, Pen96, PL94, PR299, Poi99, PB99a, PV98, PK99, Pre97a, PMP99, RSA99b, Ros98a, SSN98a, SCT99, SC96a, SPS97, SE96, SJS98, She92e, Sho96, SM91, ST91, SSN99, SKIT99, SZT98a, Var99b, WCS95, WD99b, WS99, YKB94, YY97b, ZL99, vO91h, Ala93a, AW95, Ale98, AAPS92, BSN96a, BSN96b, BSN97, BDHIJ97, BBC98, BSB97, BCD98a, Bea97a, BBI90, BCB97, BMP97a, BBL95, BFKL94, BCCG99, CC99a, CPS95, Cha95a, CW97, CS97c, CCH98, CLL99, CD95, Cus95, DD95, FSS94, FGY96b, FGY96a, GM91, GH99, G95a, HZ93, HY93b, Hae99, HSW96, He92, HI97, HLMW93, HM94, HMP95, HW98a, HJPT98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JJ95, J95, J90, JY98, KM99a, KSL92, KM99d, Kuy95, Ku92, KH97]. based
[KK96, LRW93, LvdLB96, LS98a, LHW99, LZ90, L9CL95, MRS99, MS98a, MLA91, Mau91b, Mch92, MZ98, MM95, MTN97, Mu92, MVZ98, NS97c, NR95, OFH99, OU98b, Ole95, Pat91b, Pat91a, PS97, PC98, PGCSN96, PBBC97, Por93, PGV91, PGV93b, PGV94, RP95b, SV94, SV95a, Sha94, SRR98, Sim89c, SM90, SS95b, SS95c, SM98b, Son99, SK94, Ste95, SS98b, SZT98b, Tan90, TA97, TAP90, TC91, VNM99, Ven92, Wan92a, WKH97, Wil93a, WWH95, XA98, YWC97, YK99, Dhe98, Por93, TY98b, TY98a]. Bases
[BCE94, MSDS90, Yua92]. Basic
[CF99, Des98a, vdL98, OK98, YHK99, Zie97, van98, BDH197, Rac90, dVdV98, He98b]. Basics
[BGR98a, By93c, By93b, BFP99, Fia90, Fia97, BGR98b, YL95a]. Battle
[Ban93, Gar97a, Gar97b, Gar98b, SB97, Fro96]. battleships [Jar97]. Bayesian
[BBDF97, Jen99]. BCH [CC98, FC94]. Be
[BF99a, BV98c, Cha93, CD98b, DY91f, EvH91, GSV99, NMR95, Way93c, Ano90, Ano95c, Ano98h, CP91, Cs95, Ev92, EvH93, LF97, NMV95a, NMV95b, NOVY93, Pel97, Pel98, Pel99, Pel99b, Pel99c].
Ros98c, Sch91b, Sim98c, van97a. Beach [IEE97f]. Beacon [JSZ94]. Beans [NK98b]. Bear [AB96a]. Beaufort [Fra93].

Beach [IEE97f]. Beacon [JSZ94]. Beans [NK98b]. Bear [AB96a]. Beaufort [Fra93]. Been [MLLG95]. Before [Ano96d, CFK91, Blo98a, Blo98b, Blo98c, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98b, Uni97c, Uni95a, Uni98k].

Begin [Ano93a]. Begins [Gar98b]. Beguin [NS98b, NS98c]. Beguin-Quisquater [NS98c].

Behavior [FM98a, SCT99]. Behavioral [Moc97, Ale97]. Behaviour [HJTW99, HN94]. behind [Car97b].


Best [FJM96, Rit99, Bax97]. Better [BF99a, Cha93, DQ93]. Between [BFS96, Mar98b, MW99, RCM99, SZZ95c, BS99b, BS99c, BMS96, CV95, Gal99, HT99, IKM99, Kem99, KM99c, LC97a, Mat95, Pes97, SF93a, ZM91].

Beyond [BGK99, FKM98, Fuc99, Gar98a, GK99a, Opp97].

Bi [FOO91]. Bi-Proof [FOO91]. Biased [BN6, TS98, Ueh95]. bibliography [LIE93, SAB94]. Bicentenary [CFK91]. bid [Ano94b]. bidirectional [Mit92a]. Big [Hat96, Wai95, Hof95, Kal93b, Des96a].


Billions [WSFC99]. Binary [BLLV98, Gar97b, Gol96b, KT93, GLV99, SK94d].


bis [SM98b]. Bisimulation [AG98a, AG98b].

Bit [Bur99, CWM+91, DF92, IOS94, MSN99, PF94, QG90, Sa98, SKW+98b, S99].

ZYWR91, Bro97, DKR97b, HNM98, ISO97, Knu98c, Lim98, Luc98a, Luc99a, Luc99b, MMI97, MLLG95, PC98, Sch94b, SKW+98c].

Bit-level [DF92]. Bit-Sliced [PF94]. Bits [BV96, BDF98, FS97b, VVD90, CDE+96, HN98, CH94b]. bitstream [HC97e]. Black [BL96b, BL96a, SV94, SV95a, Yar90, YY96, YY98d, YY98b, BD98b]. Black-Box [BL96b, BL96a, YY96, YY98d, YY98b].

Blacklisting [KRS99]. Blackmailing [Jak95].

BlackNet [MLL95]. Bletchley [Ano97-28, Cla98b, HS93, Smi98b]. Blind [CPS95, Eri97b, JLO97, LK99, LR98, NMV98, NMV99, Oht98, PS96c, RGV97, SY96a, SYM98, HMP95, Tra97, XA98].

blindfolded [JY96]. Blinding [Bra95c, Kra99, FY95c].

Block [AB96a, ABK98b, ABK98c, BKR94, BAK98, CDN98, Cle91, CJM95, DGV94a, DKR97b, DKR97a, DR99a, DDNM98, De 99, DW94, JK97, Jak98, KR94a, KV99, Knu94b, KP96a, Knu98b, Knu98c, Knu99b, Knu99c, Knu99d, Kob99, LM93a, LM93b, LM91b, Lim98, Luc98a, Luc99a, Luc99b, MNSV97, Mat94, Mat96a, Mat97, MT99a, MSK99b, Pat99, Pre97a, QG90, RRS98, Rob95a, SZ96, Sch94b, SK96c, SK96d, SKW+98b, SKW+98c, SKW+98e, SKW+8f, Sch99d, Vau98b, Y96, YL98, YL97c].

Block-Ciphering [Mas94].
[MB99a]. Byte [Mas94, PV98, YLCY98a, YLCY98b, CFK+91]. Byte-Oriented [Mas94, YLCY98a, YLCY98b]. Bytes [Yuv97]. Byzantine [Bea92, Bor95].


California [ACM93b, ACM98a, And96c, CFK+91, Chr99b, Go96d, Lom97, RBCE99, Sch94].
came [Fro96]. Camera [Fri93, SKWH96].

Campbell [CFK+91]. Campbell-Kelly [CFK+91]. Campus [WN94]. Can [Ano93c, BF99a, CP91, Cha93, CD98b, CMYY97, DY91f, EvH91, GS99, NMR95a, NMR95b, NMR95, Riv98b, Sim98c, Ste95, BGV97a, CG05, Ev92, EvH93, LF97, NOVY93, Sch91b, Ude98, Way95].

Canada [ACM94c, CFG96, GS94b, IEE94f, IEE96d, TM99, Yua92, Rob98b, Tsa98].


Cards [Ano96b, Ano99d, BDB92, Cha99a, CM99c, Con98, Con99a, Con98, CH99a, DJ98d, DJ98d, DJ98b, DJ98, De97, De98, Fan96, FW91, FGPL96a, FGPL96b, FOM91, GL96, Gut98a, HKQ99, JT97a, Koe99, KCCT94a, KCCT94b, MSN99, Mye96, NM96b, PV98, Roh99, SKW*98d, SS99a, Sch90b, SR96, Smi98a, Taa99, VV98, ABKL91, ABKL93, Ale97, Ano98h, BGV97a, Bro97, CJRR99b, DS98a, Dhe98, DT98b, DF97, Gau97, T997, AG99, Bak99, BF99a, Gir99, GST96, LW99, NFQ99].

deT0AP [SGPV98]. Carmichael [Pin97]. carrier [SVWM95, SOB98, VSB95]. Carry [SM91, DF92]. carry-save [DF92].

Cartesian [DVW90]. cascade [BCK96b, BCK96c, YL93]. Cascades [GC90, Men95b]. Case [ABDV98, BY93a, BGG94, BR95b, BGM97a, BGM97b, BPR99, DSSB95, Duh90, FL99b, FR95d, GR99, GM99a, LBHM99, Mad92, MD90, MR95a, Mar98a, PK99, Riv98c, Var99b, AD97, AD99, BHR99, DFL93, LMS97].

Case-Based [DSSB95, FR95d, GR999, MD90, MR95a, PK99, Var99b].

case/average [AD99].

case/average [AD97].

Cases [BMC95, Blo99]. Cash [BFP99, Bra95b, Cha93, DFT97, DT98a, EN98, EN99, FO97, Jak99b, LR98, NMV98, O90, STS99a, STS99b, Tra99].
Yac99a, Yac99b, AMS96, VNM99]. CASL
[Mos99]. CAST [Ada97a, Ada97b, Ada98, KSW97a, KSW97b, MSK98]. CAST-128
[Ada97b]. CAST-256 [Ada98]. casting
[Pit96a]. cataloguing [DSSZ99]. catch
[Way93b]. catching [WS96c]. Caught
[Mei98]. Causal
[RG95]. Cautionary
[KM92, Roh99, CJRR99b, RS98f]. Cautious
[Gla99b]. CBC
[BR96a, KMS95a, MD98, PA98a]. CBC-Mode
[PA98a]. CBCM
[BK98a, BK98b]. CBR
[GAO94, FCS97, Ev92, Kuk99]. CFR
[UU97b, Cli97]. Chaffing
[Riv98d]. chain [JVF98a]. Chaining
[BKR94, CMJ95, Jas96]. Chains
[YY98a, dR95]. Challenge
[Ano97c, Ano97w, BCE+C94, DDJ98c, DDJ98f, Sim96b, WD98, Wir98, BT97, Ano97e]. Challenges
[Ano98c, BS97b, GB98, McC96, Cer97, FM98b]. Challenging
[CM99d]. Chamber
[Yar90]. Chameleon [AM97]. chan
[XtTm94]. Chance [GB98]. Chang
[Bur94a, Bur94b, HLC96]. Chang-Wu-Chen
[Bur94a, Bur94b]. Change
[FY99, Wal99b, MW98a]. changeable
[HYLT99]. changing
[MW98a]. Channel
[AO96, AIP96, ADE96, B99, Bro94, KSW98a, KSW98b, KSW98c, MM92a, MM92b, OKST97, WB92, BM95, FC94, PS97, Pf95]. Channels
[BDI+W96, Cre97, Des96a, vD97, KI97, Lip94, MM96a, MK94, MM94, PN92, SI94, Sch94c, Sim93, Sim96a, Sim97, VN95, WD99a, Des96b, Gr98, Mau91c, SI93b, Sch93b, Sim94c, Sim98a, Sim98b, Tod97, YL97a]. Chaocipher
[Joh98]. Chaos
[BGR94, BLM94, Ano96b]. Chaotic
[Bih91, GKS97, HNS91]. Chaotic-Map
[Bih91]. CHAP
[Sim96b]. Chapter
[Kal97b]. chapters
[Tat98, Tat99]. Character
[BH99, Sab94]. Characterisation
[KMH99, Kob91b, MVZ98, SS98a]. Characteristics
[Fer98, Kuu93b, ZZZ95c, She95a, ZZZ95]. Characterization
[BSS99b, BS99c, CDD99, DFP99, Ito91, PLWSN99]. Characterizations
[FY97, St91a]. Characterizing
[LPN95, Pro91]. Charles
[LP98]. Charlesworth
[WZ95]. Charon
[Atk93]. Chasing
[GAR97b]. chausses
[Sch98c]. chausses-trappes
[Sch98c]. Cheap
[LT98]. cheaper
[Sch98c]. Cheaply
[Ano93j, Str93a, Str93b]. Check
[KDO95b, KDO95a, LSH9b, HLC96, HLC96]. Cheating
[GP99, Rab94, OK96b]. Check
Checkers [Fis97, KA91]. Checking [BGR98a, Bol98a, Bol98b, BDL97, FL99b, FGY96a, GMV98, PV98, BCR98, FGY96b, MHPS96, MW94]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93]. Chen [Ala97, Bur94a, Bur94b]. CHES [KP99b]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93]. Chen [Ala97, Bur94a, Bur94b]. CHES [KP99b]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93].
[BK98f]. Computable [DSV99].
Computation [BM99a, BM99b, CH98, Cra99, FH98, FH94, GM93b, HHT93, HHT97, HCY96a, KR94c, LO91a, LYH93, LL95a, Mon93, Mor98, PK95a, PK95b, SSN98a, Wat91, ARRW99, Ata99, BHKR95, BM94c, CL97a, GM95b, Hor98, LY93, MILY93, PW93a, Shp99a, Xie92].
Computational [CH96, HKL94, Kos97, KRS99, PG90, Sab94, TGKI99, BC95a, Ger99b, McC90b, Pom90a, SS95a].
Computationally [WP90].
Computations [Cha90, CDD+99, Mas91].
computed [Ev92, EvH93].
Computer [ACM93a, ACM94a, ACM97a, Ano93d, Ano97-29, Ano98b, Bac95, BK90, Ber96b, Bre99, CWM+91, CO98, De 98a, De 93b, De 98c, DQ93, Des92, DEQ92, FJM+96, GMV98, HM91, HM92, Hig97a, Hig97b, Hor94, IEE92a, IEE92b, IEE92c, IEE93b, IEE93c, IEE94b, IEE94d, IEE94f, IEE96a, IEE96c, IEE97b, IEE97d, IEE98a, IEE99a, KK99b, LBMC94, LC95, MDP94, NIS92, Nac97, Neu92, OD99, PGV93d, Q+98, Sal91, SSS98, SK96a, SK99, Ste91, SL93, VGP93, Ver98a, VG99, Wh90, AFB95, Ano93k, AC97, Bur98a, Car97c, Car98, CW91a, Coh94, GBL94, Gru98, HLLC96, IEE92d, IEE95c, Joc98, LS98a, LFSY94, LC96b, LC96c, NT94, Nis91, PR98, Riv98c, Shp99a, UFC94, Wil93a, Woe97, Wuo90].
Computer-Related [De 93b, De 98c].
Computerized [Ive91].
Computers [???97, BF99a, CWM+91, HM96, Kan96, Sch98c, CFK+91].
Computing [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98a, ACM98b, ACM99b, Bak92, BDDG99, BV96, Bra94a, CFK+91, DJD98d, DJD98b, DDJ99, Dwo95, FP99, GC98, GN95b, IEE94e, IEE95b, Kon95, Law98, MMM+98, Mau94, MW99, NS98a, PEN96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b, BGT96, CWM+91, DiDPS96, FM91, FJV97, HK99b, HC95a, KG93, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK+91, PH91].
COMSEC [Mye98]. concatenated [LYG94].
concealed [Ano97i, CZ90, Lea90].
Concealing [CD97, Ben94, Juh97b].
Concept [Lin98, GM91, HLC99, YKY99].
ConConcept-Based [YKY99]. Conception [NS98a].
Concerning [Cle91, Hub91, FR94, Fri96, GHS93, Gro94, Sim98b].
Conciliation [BBDF97].
Concrete [OO98, BCK96c, BDJ97].
Concurrency [SG99b, IEE94b].
Concurrent [BMT98, DO99, DS98b, RS99c, Zwi98, ARK99].
condition [Sta96b].
Conditional [DOR99, GKG99a, KS97a, KG99].
conditionally [Des90b].
Conditions [GS99a, Rus93b, Gua99].
Conducts [Law98].
Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95l, Ano96i, Ano96a, ???97, Ano97f, Ano97g, Ano97a, Ano98a, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BS95e, CH96, Cha91, Cop95d, DDJ98a, Dan96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, Hir97, Hir98, IEE95a, IEE97a, IEE99b, IEE93c, IEE94b, IEE94c, IEE94e, IEE94f, IEE96b, IEE97b, IEE97c, IEE97d, IEE97g, IEE97i, IEE97k, IEE98c, IEE98f, IEE98e, IERM93, KG96, Kat97, KM96a, Kra98, LO99, LP99, Mau96b, MSD90, NS92, Nat98, Nat99b, Nyb98, OW95, OiDP98, PSN95b, QG95, RD99a, RD99b, Sch94m, SJ97, SIK93, Sti93b, Sti94, T+98, USE91, USE92a, USE94, USE95a, USE96a, USE99b, USE99d, Wal99a, Yu92, ACM99c, Ano93d, Boy95b, BD95b, Cop95b, Dar97, DC96, Des94b, HQ97, HI97, IEE92d, IEE95c, IEE96f].
conference [IEE98b, Kal97c, KG93, Kob96, LM98a, SP90, Ste99b, USE96f, USE98c, USE98d, VPM97, Wie99, Ano95f].
Conferences [BDHK93, MZ98, Sch95f].
Conferencing
confidence [Chi99a, Chi99b, Graxx].

Confident [Jan95]. Confidential
[Bet95b, Bet95a, vD97]. Confidentiality
[Ano98j, Jac96, Riv98d, ZG96, FT95, MI90]. Configurable [VMS97b, VMS97a].

configuration [Hi97]. Confirmer
[Oka94, Cha95b, MS98b]. conflict [All97].

Conflicts [ACM94b]. Confounder [BTD98].

confrontation [Za97]. Confusion [GC97].
Cong [Mye98]. Congressional
[Smi97a, UU97a]. congruence [Sch91a].
Congruent [Kra90]. Conic
[Cao99, Mra95]. Conjecture
[Jia99, GHS93, Ili94]. Conjectures [KP95].
Connect [Lic94]. Connection
[Kas96, CV99]. Connections
[RSG98, SGR97, Yu94a, Yu94b].

Connectivity [Pit96b]. Consequences
[KP95, Sim94a]. Conservation [Bro94].

Considerations [Cra96, Hub91, Mos98],
Bas95, Bou94, SY92, YSS99, Bou94].

Considered [LT91]. Considering [HH94].
Considers [Ano95]. consistency [ZYR90].

Conspiracy [WK97, Scu92]. Constitutional
[Bas95]. Constrained
[Gol96b, Has99]. Constraint
[S95, WS99, GMLH94].

Constraint-Based [WS99]. Constraints
[DS98b, Ou99, Koz96]. construct
[Lon92, Sun91a, ZH98]. Constructed
[Rus93a]. Constructing
[Ada97a, AB99a, AB99b, DT93, Gal99],
KTM9a, Koh91b, XL98, ZZ96].

Construction [BCK96c, BR99a, BR99b],
CNST98, vD95a, DS999, EM93, GPSNW98,
Joh94, Kim93, KYDB98, NR98, SXW91,
ZMI90, BCK96a, BCK96b, BCK96c, B93,
MPL99, OS91, OS92, Pet91, vD95b].

Constructions [AVH98, ABDS96, KRS99],
SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE99c]. contactless
[DS98a]. contain [Lea90]. Contemporary
[Kma99b, Sim92]. Content

[Ano99e, KBRS97, WW98a, Lam99].
Confidence [Chi99a, Chi99b, Graxx].

Confident [Jan95]. Confidential
[Bet95b, Bet95a, vD97]. Confidentiality
[Ano98j, Jac96, Riv98d, ZG96, FT95, MI90]. Configurable [VMS97b, VMS97a].

configuration [Hi97]. Confirmer
[Oka94, Cha95b, MS98b]. conflict [All97].

Conflicts [ACM94b]. Confounder [BTD98].

confrontation [Za97]. Confusion [GC97].
Cong [Mye98]. Congressional
[Smi97a, UU97a]. congruence [Sch91a].
Congruent [Kra90]. Conic
[Cao99, Mra95]. Conjecture
[Jia99, GHS93, Ili94]. Conjectures [KP95].
Connect [Lic94]. Connection
[Kas96, CV99]. Connections
[RSG98, SGR97, Yu94a, Yu94b].

Connectivity [Pit96b]. Consequences
[KP95, Sim94a]. Conservation [Bro94].

Considerations [Cra96, Hub91, Mos98],
Bas95, Bou94, SY92, YSS99, Bou94].

Considered [LT91]. Considering [HH94].
Considers [Ano95]. consistency [ZYR90].

Conspiracy [WK97, Scu92]. Constitutional
[Bas95]. Constrained
[Gol96b, Has99]. Constraint
[S95, WS99, GMLH94].

Constraint-Based [WS99]. Constraints
[DS98b, Ou99, Koz96]. construct
[Lon92, Sun91a, ZH98]. Constructed
[Rus93a]. Constructing
[Ada97a, AB99a, AB99b, DT93, Gal99],
KTM9a, Koh91b, XL98, ZZ96].

Construction [BCK96c, BR99a, BR99b],
CNST98, vD95a, DS999, EM93, GPSNW98,
Joh94, Kim93, KYDB98, NR98, SXW91,
ZMI90, BCK96a, BCK96b, BCK96c, B93,
MPL99, OS91, OS92, Pet91, vD95b].

Constructions [AVH98, ABDS96, KRS99],
SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE99c]. contactless
[DS98a]. contain [Lea90]. Contemporary
[Kma99b, Sim92]. Content

[Ack98, JPLJ99, KR98, MW98b, MR95b],
PMP99, Ros93, SC96a, Way93a, SNT95].

Content-Addressable [Way93a].

Content-Based [PMP99]. Content-MD5
[MR95b, Ros93]. Contents [vHH97].

Context [COZ99, MM96a, Des90b, Des90a, Ili94].

Context-Based [MM96a]. context-free
[Ili94]. Continue [Ano96k]. Continued
[KE97]. Continues
[An97y, An97z, An98h, DDJ98d, An96i].
Continuous [BP95a, NHB98, She95a].

Contours [LFC99]. Contract
[GJM99a, GJM99b, KHB99]. Contractor
[KHB99]. Contracts [Ped99]. Contrast
[HKS97a, HKS97b]. Contrast-Optimal
[HKS97a, HKS97b]. Contribution
[Lud97, SS97, AK98, Blo98b].

carbohydrates [Hil94]. Control
[ABL93, Ban93, BDPSNG97, DFTY97],
FY99, FL96, Hwa97, JPLJ99, Kas96, KA99,
KKW99, Lin98, Mey96, NW98, NAA99,
NS98a, FRAM98, Per99, STS99b, She93a,
She93b, Sim90b, Sim91, ZH98, ACC99,
Ano93d, BG96, CWM91, CS96b, CS97b,
CW94, LL93b, LM93c, Mat91, MLA91,
RO96, RT93, SS96, Uni97d, WW91].

Controllable [CTT94]. Controlled
[GPR98, GO96b, Gol94, Jak99c, SKB9x,
GM91, GO95, Men95b]. Controller
[CIBM99, FCH99]. Controls
[Ame96b, Ban94, Cil97, UU97b].

Controversy [Law98]. Convention
[An94d, An96a, An98f, IEE96f, NIS92].

Conventional [PRB98a]. Convergence
[GC97, Mos98]. Conversation [Woe97].

Conversational [LTE99]. conversion
[Sab94]. Convert [Pet98]. Convertible
[BCDP91, DP96]. Convolutional
[Cha99c, JJ99b, TY94]. Cool [An99c].

Cooperative [Oh99]. Coordinating
[Lee99b]. Coordination [COZ99, FL99a].
Cope [WI99, HJKY95]. Coprocessor
WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Wic90, Wie90b, Wie90a, WBDY98, YLD99, YLH98, ZYR91, Ada92, Alv98b, BSN95, BB94, Ber93, BS90a, BS91e, BS91f, Bih92, Bih95b, Bih98b, BK98e, Bir99, BD95a, Bowxx, Bur98a, CV95, CD98a, Cra92, DYL98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, GoI95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kal98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos7, Kuk99, Lan95, LS98a, Lew92, Mat93, Mih96, Mil92, Moh92, Mor92, NS97c.

cryptanalysis
[OC95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZYR90, ZH90].
cryptanalyst
[Rey96, Rey97, Rey99].
Cryptanalytic
[Gla99b, KSWH98d, MG91, vW99, Bih94a].
cryptic
[Wri98].
CRYPTO
[Fei91, ACM94b, Ame96b, And96a, Bar93a, Bar93b, BE90, HP98a, HMV94, Koo97, LKB+94, Mah96, MPPS95, Neu97, Sch98c, Way95, Way96b, Neu95, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol90b, Kal97c, Kob96, Kra98, MZ98, MV91, StI93b, StI94, Wie99, BC98, Bra98, Bri98, CP91, CRS98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, StI93b, Wil98].

Crypto-Chip
[HMV94].
Crypto-Coprocessors
[HP98a].
Crypto-Engine
[BE90].

Crypto'91
[DBGV93].

CryptoAPI
[Boy98].

CryptoBytes
[Cry95, Riv95c].
cryptochip
[PP96].
cryptograms
[Har94, Web93].

Cryptographers
[WP90].

Cryptographic
[AG98a, AG98b, IBM93, Ano96f, AB97, BDPNSNG95, BDPNSNG97, BH93, BY93a, BGM97a, BGM97b, BBT94, BM97e, BFKL94, Bol98a, Bol98b, BDL97, BDP97, Bra95a, Bra96, BD91, CS96a, CJR98a, CJR98b, CPOR97, CF95, CD99, Cop94b, Cre97, DGV92, DC98a, Dam90a, Dam91a, Dan95, DIF94, DY90, DY91a, DY91d, DY91b, De 95, DS97a, DF91c, DK91, ECD+99, Eil98, FGR92, Fir98, FGY96a, Fum97, GI99, GS94a, GKF99a, Gol96c, GKF97, GQ95, Gut99, HHT93, HHT97, Hel94, Hwa97, II96, I ve91, JDK+91, JD91, KM98a, Kal98f, Kal98d, KV94, KSF99, Kha93, KP99b, KT91b, KT98, KS97b, LM99j, LL97a, LHB96, LM96, Mac94, MM99a, Mau96b, Mau97b, MS90a, Mil96b, Mo93, Mos98, Mun91a, Mun91b, NM96b, Ng99, NS99b, NR94, NK98b, Nur94, Nys99, OP9+99].

Cryptography
[Oka93a, OS98, PS99d, PV97, PS96b, PBBG90, Pre93a, PGV93a, Pre93b, Pre94a, PBD97, PRB98b, Pre98c, PRB98a, Pre99, Pre94b, QV90, QG95, RSA93d, RS93, Ritxx, Rue93, SI94, SZ96, Sak96, DY91c, Sch95f, SK96a, Sch98d, SK98a, Sch91c, Sch93f, SPS97, SZ93, SZZ95c, Sha99a, She92d, SV99, Sm90, SY92, SM91, Ste96, T+99, Tou91, Tou93, TY96, VCF+90, VIG98, Wai95, YSS99, YY97c, YY98a, ZZ95, ZMI91, AN94, AG97b, AG97c, AG97a, BD92, Boli97, BV97, Com94c, CDG95, Cli99, DD95, Dan7, Dhe98, Di 99, DFHR91, Don98, FGY96b, Fro96, FL93, Gol96a, Har91, Hof95, IS99, Jenxx, JW01, JP96, Kob91a, LR93, Lia95, Lea90, Lev91, LL93b, Lub96, Mun91c, Mea95, Mol98, Mu92, IP9d, bbbpr91, NT93, Nhy98, Pan98, PKM97, Ros97c].
cryptographic
[Sch93g, SZZ94a, SZZ95b, Ste99b, Way98, WN94, XZZ97, XZZ98, YS91, ZZZ97, ZLX99].

Cryptographic-Token
[Nys99].

Cryptographical
[AN94, Ano99h, AA93, ABDS96, AE93, AVG94, AVG95, AVG96, AVG97a, AVG97b, AVG97c, AVG97d, AVG98a, AVG98b, AVG98c, AVG98d, AVG99a, AVG99b, AVG99c, AVG99d, AVG99e, AVG99f, AVG99g, AVG99h, AVG99i, AVG99j, AVG99k, AVG99l, AVG99m, AVG99n, AVG99o, AVG99p, AVG99q, AVG99r, AVG99s, AVG99t, AVG99u, AVG99v, AVG99w, AVG99x, AVG99y, AVG99z, AVG99aa].

Cryptography
[ANS97, ANS98b, Ano99h, AA93, ABDS96, Avo98, BCE+94, BGG94, BGG95, BGR98a,
SG99a, Sam98, ST91, Sun98a, Tak98a, Tak98b, Van98a, Vau98c, Wal99c, Wan92a, WY93, Yam99, AMV93, AD97, AD99, Ala97, AAPS92, ACBR90, Bao94, BI94, BS97, Boy97, BCCG99, CC99a, CS98a, CC98, CW91a, CW97, CS97c, CCH98, Cle96, CS97d, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a, CW97, CW91a,
D [Ben99, BALS99, CK95, Nas94, TK99, Wor96, YY99a]. **D.E.S.** [Cle91]. **D.S.A.** [NMVR95a, NMVR95b]. **Dabbling** [Ritxx]. **DAEs** [JV98b]. **Dallas** [ACM98b, USE91]. **Dangård** [DG93]. **Dangård’s** [Gib90]. **dan** [PNdbbbprm91]. **Dark** [YY96]. **DASS** [Kau93]. **Data** [All97, Ano92c, Nat93b, Ano95f, Ano96c, Ano97e, Ano97f, Ano97g, Ano97a, Ano97w, Ano97x, Ano98a, Ano99e, Ano99a, AWV99, BGML96, BRS99, Ber98, BS95b, BS98, BY92, BW98, BZ98, Cle96, Con99b, CH99b, DC98c, DFGH99, EKLM99, Gai90, Gre90, Gui97, HS96a, Int91b, JMLW94, Kop97, KH98b, LvdLB96, LT98, MPPS95, MSHP99, Moc97, Nat93c, Nat93a, NH989, OA94, Sch99b, Sch94m, See97, Sme97, Sto90, SZT96a, TYD99, Tay90, TLS99, Way91, WSFC99, Wei95, Whe94, YY91, ZTR99, Ano93k, Ano95c, CCN95, Cha94b, Cli99, CS99, Cra96, Dam99b, DF97, Gil97, GTGW94, Gut96, Hel93, KAK96, Lam99, Los97, MSDS90, Mic97, Nor95b, PD99a, Rev91, Ros94, Rot97, Sch92a, Sch98b, Su98, Th91, Tv92, Uni96a, V93c, Way95, Wn900, Yua92, ARR99]. **Data** [Ano97v, Bar91, BS93b, Bir95, Con94a, Cop94a, Den90, HK98, HK99d, Joh90, Kap98, KM97, Mat94a, Nat94b, Nat99a, Pa96, Per91, RP94, She95b, She92g, Sim95, SB92, Wi99a, Ano94h]. **Data-Dependent** [Con99b]. **data/image** [Sch98b]. **Data/Image** [Sch99b]. **Database** [AKF94, BPDSNG95, KT96, LCL92, Ou99, SJ97, Wat99, HY95, IS97, Lee95]. **Databases** [BDPSNG97, CP93, GM99b, KB92, Len99b, PF94, RZ99, SG99b, Har90, Wad93, Ano95k]. **datagram** [PSB97]. **Datamation** [CWM+91]. **Date** [GN95c]. **David** [Ers99, Bar95]. **Davies** [BB95b]. **Dawson** [Roe99]. **DC** [USE99a]. **DCE** [Cas95, GH95, Kon95]. **DCI** [Pin98]. **DCT** [BBCP98b, BBC98, HW98a, PBBC97, TA97]. **DCT-based** [BBC98, HW98a, PBBC97, TA97]. **DCT-domain** [BBCP98b]. **DDJ** [Con99a]. **Deal** [FW91, Knu98c, Luc98a, Luc99a, Luc99b, Out98]. **Dealer** [Rab94, BGS95]. **Dealing** [Bec99, MSN99]. **deals** [Joh97f]. **Death** [CFK+91]. **Deavours** [Ers99, CFK+91]. **Debate** [Ano96f, Dum94, Un98], We91a, We91b, Fre94, Hof95, Neu95, RDK94, The96, Un98k, Hat96, Wai95]. **Debating** [Ano92b]. **Debugging** [Wot99]. **Debut** [Gar98b]. **December** [And94a, Boy95a, Boy95b, Bra93a, CW94, Con99a, Dar97, Far93, IE92b, IEE93c, IE94c, IE97b, KG93, Org98a, PSN95b, Pre95a, SZ93, Tv92, Wal99a, WN98b, Zim96b]. **Decentralized** [Md94]. **Decidable** [BRS99]. **Deciding** [Bra95a, Bra96]. **decipherability** [CGV94]. **Deciphering** [CJ99, Duh90, Has95, TG94, Bru91]. **Decision** [AA93, Bon98b, Bon98a, CKN99, DTDJ99, HTY99]. **Decision-Making** [CK99]. **Decisions** [Bar96a]. **Declarations** [SHK99b]. **Declarative** [Sch99c]. **decode** [Har94]. **Decoding** [CS96a, SY96a, SYMI98, HG97d, HK99c, SKD94]. **Decoherence** [OD99]. **Decomposition** [All98, AMP94, HK98a, SC97]. **Decompositions** [PS9, BDSV93]. **Decorrelated** [KR99a, Van98]. **Decoration** [Vau98b, Van99a]. **Decrypt** [Bau97, DSB99]. **Decrypting** [Bar92b]. **Decryption** [GOH97a, HJ98b, Oht98, CB96, GBL94, HJ98a, MS99c, MVN99]. **Decrypts** [Pea97]. **DEDICA** [RCM99]. **Dedicated** [ISO97, DV96, NM96b]. **Deduction** [GPPV98]. **Deductive** [PS99f]. **DEFACTO** [BDDC99]. **Defeat** [Luc98b]. **Defects** [Dav96]. **Defense** [RS93, Bax97]. **Definability** [GM99b]. **defined** [Ler97]. **Defining** [BG93, BMR98]. **Definitions** [Blo99, Uni96c]. **Deformation** [DFL99].
[AKF94, BV98a, BK95c, BM94b, CH99b, DL99, DMVC99, Ger99a, Gor93a, HJ99, JS93a, Kem99, PM99a, PD99b, Sch94c, SW97a, SW97b, SZZ94b, Ste94a, SAS99b, TLS99, Zhe90, CG05, Hor99, HLC99].

Designs [DJHP98, FY95b, Jun96, KK95, Mou99, RB99, Wot99, Ton96]. DESIRE [JKVP99].


Dickson [Pie93]. DICTA [KG93]. DICTA-93 [KG93]. Dictionary [Jas96, Luc98b, BCR98]. Dictyostelium [Ram92]. Diego [ACM93b, IEE97b, Sch98b, USE96f].

Difference [LP94]. Different [KBR97, Sch99h, RT93]. Differential [BB94, Ber93, BS90a, BS91c, BS91e, BS91d, BS91f, Bih92, BS93b, BS93a, BS97a, BK98d, BKPS93, CJ98, Con99b, Dae95, Din94, Fer98, Haw98b, Haw98a, KTM+99, Kau96, KM98b, Kob99, KJ99, Kwa93, LMM91, LH94, Lan95, Mat96a, Miy93c, MSK98, NK93, OMR4, Pai99a, Sch96c, SMK98a, VR98, Wag98a, YLH98, Ada92, CV95, KY95b, KYx, KM96b, OC95, OG95, RP95b, TN97, Way95, YT95a, YT95b].

Differential-Linear [Haw98b, LH94, Haw98a, Lan95].

Differentially [Ny94]. Differentials [BBS99a, Fer99a, KR99, BBS98a]. Difficulty [KP96b, Riv93a, ZZ96, Hor99, Riv95a]. Diffie [BY93c, BY93b, BBR99, BMW99a, BV96, Bon98b, Bon98a, CS97, CS97d, HY98b, HY98a, Kalg97a, Koc95, Koc96b, Lut98, Man94, MW96c, MW96b, MW99, RSA93b, Van95a, WV96, WM93, vOW96].

Diffusion [Mas99b]. Digest [FHBH97, GT94, Kalg91, Riv92a, Riv92b, Riv90a, Riv91b]. Digit [TK99].

Digit-Recurrence [TK99]. Digital [Ame95, Am96a, ANS98b, Ack98, ALO98, AW94, AR97, Int91a, NS94, Ano96c, Ano97-29, AS98, Aur96, BG90, BM99a, BM99b, Bm94, Ber97b, BM94a, BM96a, BM96b, BM96c, BS95b, BS98, BTH96, Boy97, Boy98, Brea93a, Bf99, Bf99, Car95, CR91, CPO+98, CHO+98, DDM98, DDM96, EL99, EGM90, EGM96, FCF99, FKM99, FBS98, Fri93, Fro97, FOM91, Gar97c, Gar98b, GR97, GDD+97, GB98, GO96c, GQW+91, HKS95, HG96, HG97e, HEG98, HA96, HW97, IEE97c, IEE98d, JLO97, Jue99, KKS97, Kob97, Kob98c, Kra93, KH98a, LQ99, LW96, LR98, LR98, MSO96, Man98, MAM98, MB99a, MW98b, Mer90b, Mer97, MTN97, Mo98, MBW97, Nat91, Nat94a, NH98, NM98, NIS93a, O093, O196, OFF93, Ok96, Per97, Pet98, Pf96c, PW93b, PG93c, RDK98].

Digital [dR94b, Rot95b, SC96a, SCxx, Sch93c, Sch94d, SK97b, SK97a,

E-Cash [DFTY97, Yac99a, Yac99b]. e-commerce [VM96, DDJ98d, Jak99b, Lut98, Gar97b]. E-mail [LF97, Ril96, Bac95, Sta94a, Ano93j, Got99, RS98b, Sch95c, Sch95d, SH97, Ano95c, Gar97b, Str93a, Str93b]. E.I.S.S [BFS92a, BFS92b]. E.I.S.S. [Dan95]. E.I.S.S.-Report [Dan95]. E2 [KMA +98, Kobs99, MT99a]. EAP [BV98b]. early [Alv98c, Mar96]. Earth [YHKI99]. Earthcam.com [Ano98]. Ease [HJL99]. Easier [GMDS98, BBR99, Sch98c, Way95]. East [Str95]. Easy [Sim94d, Ken95].
embeddings [CT99b]. Embraces [Ts'97].
EMEF [Org98a]. Emergent [Jun99].
Emerging [Kal99, Org98a]. Empirical
[WW98b]. Employing [BWM98]. emulator
[Obe99]. EMV [Gu97]. enable [Sch93e].
enabled [Cha99b]. Enabling [DS97b].
Encapsulating [Atk95b, KA98b].
enciphered [Lea90, Per91]. enciphering
[Beu94]. Encipherment
[HS90, OA94, Lin88a, Lin89a]. encoded
[DS97b, HG97d, QN98b]. Encoding
[Til98, HG97d]. encodings [CGV94].
Encrypt
[Ber98, JSY99, Ril96, WT99, Rot97].
Encrypted
[AW99, Bla98, GLZ99, Gil98, Jas96, YY91, BTD98, DF97, STW95, Kip97].
Encrypting
[Ano97r, Bla94b, Lom94, Luc98b, LW99, SS99c, Ben94, KAK96]. Encryption
[ASW99, AAB+97, Ada97b, Ada98, A099b, And98, ABK98a, Nat93b, Ano94c, Ano96c, Ano96l, Ano97b, Ano97v, Ano97x, Ano99e, Bac95, Bal97, Ban93, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b, BDPR98, BS99b, BS99c, BRW99, BS93b, Bir95, BB95c, Bla96a, Bla96b, BFN98b, Ble98a, BC95c, BFS96, BY92, Com94a, Com94b, CDNO99, CMN99, COP+95a, CH98, CMKK98, CT99a, Cop94a, Cou93, DD98e, DD98c, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DS97c, Ele98, FIP94, FN94, FY95b, FY97, FH94, FO99a, FO99b, GSY99, Gai90, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, GK98, Got99, HG97a, HG97b, Hat96, HK98, HK99d, Hub98, Jol90, JM96b, Kal93a, KY95a, KR96a, Kal98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kum98]. Encryption
[KBR97, KH98b, KYD98, Kwa93, Kwa97, RSA93f, Law98, Lea99, LT91, LW91, LM91b, Lin93a, LS98b, Luc97, Luc98c, Luc99c, LW99, MGL+98, Mat94a, Mat97, Mer91, Mey96, Mil95, Moc97, Mue99, Mil99, Nat93a, Nat94b, Nat94d, Nat97b, Nat98, Nat99a, Nat99c, Natxx, NBD+99, NH90, Ohi99, Oka94, Ori96, Pai96, Par98a, Par98c, Per91, PRZ99, Pin97, RSA93a, RSA94, RP94, Riv95c, Riv95b, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SVA+98, SKN98a, SKN98b, Sch99a, Sch99b, Sch93d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SE96, See97, She95b, She92g, SB98, Sim95, SM96, SM98b, SB92, Sm93b, Sm97a, SB99, Sta97c, SW99b, Sto90, TPH+98, Univ97a, Univ98a, Univ98c, Univ98b, Univ98d, Univ98e, Univ96b, UU97a]. Encryption
[Univ97b, Uni98f, Uni98h, Uni98i, Uni97c, Univ98j, Uni98i, VB96, VKR98, WSK97a, WSK97b, War98, Way93b, Way93c, WSFC99, Wei91a, Wei91b, Whe94, Wir98, Yin97, YY97c, Yuv97, Zhe97b, Zol93, Aus96, Abr97, Ala93a, All97, And94a, Ano90, Ano92b, Ano94c, Ano95c, Ano95k, Ano96d, Ano96m, Ano97a, Ata94, AM99, Ban94, BTD98, Bax97, Bea96, BR94b, BR95a, BDJR97, BR97b, BHI90, Bet95c, Bih97c, BFN98a, BC96a, BMS96, BFS96, Bow93, Bro96, Bus96, Com97, CCN95, Cha94b, CLW98, Cle96, Cli97, Cli99, CJM96, Cra96, DH96a, DOR99, Dia91, DL98, Ele99, Ell97, FC94, FB97, Gil97, Gol99b, Gol96d, GBL94, Goo96, GKS97, Har90, HK90, Hat97, Hel93, Hel98b, HT95, HP94, HY95, HCY96b, HCC98, Int91b, Jac90a, Jac90b,Jak99c, JT96, JT97b, KY95b]. encryption
[KY97, KYxx, Ken95, Kir95, Knu99c, Kop97, Ku92, Kuh98, Ku90, LM91a, Lam99, Lee95, LC97a, Los98, MRS99, Mar95b, MM95, MI97, Mol98, Mra95, Nat93c, Nor95c, Oel97, Pos92, Pos93, Pre95a, QN98a, Rev91, Ril96, Riv95d, RKD94, Rot95a, Sab94, Sch98b, Sch94i, Sch98c, Sch99j, She96a, Sme97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts90, Univ96a, Univ95a, Univ98k, Univ94a, Univ94b, Univ97d, UNU94,
UU97b, Vad95, Vau98e, Ven90, Vu95, Wad98, Wel95, WN95, Whi93, Wil93a, Wil93b, Woo90, Yeu99, You97, Zaj97, Zan90, Zer96a, vOV91, vT93, Ano98j, Ano93j, Hon98.

encryption/authentication [Sch99j].

Encryption/MAC [Yuv97].

encryption/decryption [Hat97, Vu95].

Encryption/MAC [Yuv97].

encryption/multisignature [HCC98].

Encryptions [Mv93].

encrypts [Ano93k].

Encyclopedia [CFK+91, New97, UFC94].

End [Bra94a, DDJ98c, Gar98a, NH90, WSFC99].

End-to-End [NH90].

endlicher [Wal98].

ends [McC90b].

Endured [Che92].

Energy [DFL99].

Enforce [BDS98].

Enforcement [Cae99a, Cli99].

enforcers [Way93c].

Enforcing [Ano97n].

Engine [BE90, CM98, She92d].

Engineering [Ano98j, DFGH99, DSB99, EKLM99, IEE96d, LBHM99, SSSW98, Smi98a, AN94, IEE97k].

Engines [T+99, Way93a].

Enhance [FO99a].

Enhanced [Ano95c, AR98, Ken93, LK96, Zan90, Zeg93].

Enhancement [HW99, Lin93a, Lin88a, Lin89a].

Enhancements [JM96b].

enhancing [HY95].

Enigma [CWM+91, Har96b, Kip97, Kip99b, Obe99, Kah91, Blo98a, Blo98b, Blo98c, Cra92, Kah98a, Kip97, Kru98, Mil96b, Tur99, Wel97].

Enjoyable [CM99d].

Enough [CFK+91, Dea98b].

Enscheide [Hei96a].

Ensuring [Com97, Rot95b, ZG96, Way91].

Enter [Wor96].

Enterprise [ECD+99, FY99, Mar95b, Wad93, SY92].

enterprise-wide [Wad93], enters [Joh98].

Entities [KM99c].

Entity [BR94a, BW98].

Entrepreneur [Pin98].

Entropy [Bro94, EHMS99, KSHW97, KSHW98].

entwufen [Hor99].

envelope [SOB98].

Environment [BKS99, BDDG99, CM98, DL99, FMM99, GRB99, HVH98, Kon95, Per97, PK99, RH93, SS99b, HK99b, HC95a, lbb97, Joh90].

Environmental [RS98c, RS98d].

Environments [GSTY96, SKAM99, DNS98].

EPIC [Rot95a].

EPS [Ano96i].

equally [Ito91].

Equation [Cop95c, LG97].

Equations [Por98, RZ99, BMF97a, Cus95, GK95b, LCL95, Lon92, Sun91a].

Equilibria [Ett98].

equipment [Int91b].

Equitable [BDS98].

Equivalent [BV98c, De 98d, Gib91, GO93, HTY99, MM96b, Miy96, Oka94, Pai99c].

Era [DDJ98c].

Ergonomic [DDJ98c].

Erika [Mat99].

Errata [Con99a].

Erratum [Ano91a].

Error [AW94, AR98, BGS96, Cha99c, DLR97, KKS97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, DLP93, JV98b, Ste95, Wan92a, YL97a, vT94, CW94].

Error-Correcting [AW94, BGS96, DLR97, KKS97, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, Ste95, Wan92a, YL97a, vT94].

Error-Correction [MG91].

Errors [GGH97a, SHK99b].

ESA [Spi95, YS91].

ESA/390 [YS91].

ESAT [PGV93d].

Escrow [ABB+97, Bla96c, BDS98, Cae99a, CGM97a, DDJ98d, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, LY95, MA96, Mar97, MS95f, MKS99, Nec96, HYMI98, Sun98, SM95a, VvT97, VBD99, YY99b, Ano94e, BDHJ97, BR96b, DH96a, Des95, Fre94, KL94, Ma90, UH95a].

Escrowed [Bas95, Con94b, FIP94, Nat94d].

ESIGN [FOM91].

ESORICS [DEQ92, Q+98].

ESP [KA98b, ATK95b, KMS95a, KMS95b, MD98, MG98a, MG98b, PA98a].

Espionage [HK99c].

Espoo [Ny98].

Essential [SSv+98, SSM+97, SMD+99].

Essentially [BR91].

Establishing [Des96a].

Esterel [RB99].

Estimate [Miy93c, UU97a].

estimates [DL093].

estimating [Al 96].
[Bih91, Dan90a, Dam91a, Dav91, De 95, Fum97, QG95, He94, Mao96b, MZ98, Nyb98, QV90, QG95, Rue93, Ste99b, Ano98e, Bet98, BCI98, CP98, Dam98, Dav98b, De 98b, Fun98a, Gue98a, GQ98, He98c, Ing98, Mao98, Pat95, QV98, Rue98, Pie98].

Eurographics [Kui91, PH91]. Europe [And96a, Koo97]. European [Dan96, DEQ92, Q+98, Spi95, T+98, Com97, Gar97c, VCF+90]. Eusipco [T+98]. Eusipco-98 [T+98]. evaluated [LMS97].

Evaluating [Pai99a]. Evaluation [AGS97, Ano97b, BK99, BP95b, CJR98a, CJRR99b, HW98, KR97, PDG99, RIP95b, RIP95a, Rob93, Roh99, WT99, CJRR99b, KM97, PS99a, Sim95, VCF+90].


Examining [RC95]. example [Kay95, Nee94]. Excellence [Eri97a]. Exchange [ASW98, ASZ96, BCG90, BM94b, Dan94b, Dan95, fifi90, FW91, Hhy93, Jas96, Luc98b, MSN98, RSA99a, SSN98a, SOOS95, Van93, BSN96a, BSNP96b, BTD98, BCK89, BM95, Dan94a, LL95b, MS98a, SKB97, STW95]. exchanges [DvW92]. Executable [JPL199]. Executing [AW99]. Executive [Zer96a]. Exhausting [CR97]. Exhaustive [CR97, QD91, KR96b]. Existence [FDB93a, HT98, RV99, FDB93b].

Existentially [DN94]. Existing [SS99d, BB95a, NM96b]. Expansion [BO96b, Tak97]. Experience [ADB99, Gla99a, Ros96b, SVB99, Moy98, CWM+91].

Experiences [FC99, Lun90, GH96, MAM95]. Experiment [AB97, DL95]. Experimental [BB+91, Mat94a, SGB99].


Expiration [BDS98].


Exploring [JJ98b, JJ98a]. explosive [DL95].

Exploit [An95a, CFPR96b, CNS99b, CFPR96a, FR95b, KOT95a, KOT95b].

Exportability [Wei91a, Wei91b]. Exports [Bar96a, Sta97c]. Exposed [MSK99a].

Exporting [Sil99]. Expressive [MTES99].

Extend [Ts97]. Extended [ASW98, FBN98b, BV98c, BD90, BS91g, BD91, CvHP91, CK90, DPD90, DY91d, DPP99, D99, DY91f, DF91a, Dob95a, EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, vHP993, BCA97a, BCK89, BT94, CV93, Des90b, Des90a, Has99, LLG10, Oke95, Pai96].


Extensible [BV98b, WBDF97]. Extension [BP98a, CTT94, FHBH+97, MS90b].
[LMJW93, STW95]. **Extensions**
[C901, DT98a, Law98, NW97, Atk93, GH99, GK95a, JD91]. **Extensive** [Ano97y, Sim95].
**Externalization** [OA99]. **Extracting** [Nis96]. **Extraction** [SD99]. **Extraordinary** [Jam98].
**Extremely** [Ano90]. **Eyewitnesses** [Ano97t].

**FA** [Bao94]. **Fabrication** [DDJ99]. **Face** [DDJ98d, DMFB97]. **Faces** [GB98].
**Fachtagung** [BGH95b]. **Facial** [LMP99, HEG98]. **Facilitation** [Cli99].
**Facility** [AKF94, Bis90, She96a, YS91, JMLW94, SY92], **facing** [KG96].
**faktor** [Pri94]. **Factor** [KM98b, SVB95]. **Factored** [Ano96b].
**Factoring** [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pa99c, Ponn90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, MK99, Mei96b, Riv95a].
**Factoring-Based** [Kal98e]. **Factorisation** [DHW95a, Jon90, DHW95b].
**Factorization** [Ale92, DDEM94, MM98a, MM98b, Od95, vO91a, vO91b, LLMP93, Mao98, Whi93, vO92].
**Factorizations** [BMS94, NS97b, NS97c]. **Facts** [Ano91b].
**Faded** [Alv98a]. **fading** [Tod97]. **Fail** [BP97a, PP97, SSN99, vHP93, And94b, Pf96c].
**Fail-Stop** [BP97a, PP97, SSN99, vHP93, Pf96c].
**Failed** [BCE+94]. **fails** [DH96b]. **Failsafe** [KL94].
**Failure** [Ano95a, Ber97c, Gar98a, TYD99, FR95b].
**Failures** [CH98, JQ97, Moo92, Sim94b].
**Fair** [AS98, CFGS99, DT98a, KL95a, LL95, Mi93a, Mi93b, MKS99, SS99e, SS99f, Tra97].
**Fairfax** [ACM93a, ACM94a]. **Fairly** [HD96a]. **fall** [Od90, Rob98b]. **False** [LKD98, She92b].
**Families** [Kal98e, Per99]. **Family** [KT98, Miy91, RP97a, ABC+98, BGH+95a, FSS94, Ito91, Kob90, SRR98].
**FAPKC** [DYL98]. **FAPKC3** [TCC97]. **FAPKC4** [TC99a]. **Far** [Str95].
**Fast** [AGS97, AMV90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bih97b, Bih97c, BHK+99, BD94, BQ95d, BV96, C991, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBV96, DNR97, EPR99b, EPR99a, Gar97b, Gol96a, HJPT98b, HP94, HC96a, J99a, JJ99b, KR94a, KTM+99, KP99a, KP97, KR99a, KM99c, KMKH99, KA91, Kov95, Man90, Mer91, Mih94, MM95, NS99a, NKP99, P997a, P997b, SOOS95, SV93, SB98, Sho96, Si97b, Tak97, Tak98a, Tak98b, T+99, Vau98d, Vau98e, AMV93, AB96b, Ano98j, CGV94, DKR97b, DV96, HJPT98a, Jemxx, LRW93, LC98, MZ98, P995, RRS98, She92c, SN94, SH99, SAM97, SGSD99, YL93, Gol96d, OA94].
**Faster** [Luc96a, Luc96b, WZ99, YY99b, Bosxx, Mih96, Sch98c].
**Father** [CFK+91, DDJ99].
**Fault** [BS97a, DHSS95, GX99, OKST97, P99a, RBvR94, IEE94b, T+91].
**Fault-Tolerant** [DHSS95, RBvR94].
**Fauvel** [CFK+91].
**Fax** [DHL95a, Jon90, DHW95b].
**FaxModem** [Ano93k].
**FC** [Fra99, Hir97, Hir98]. **FCC** [Gar97b].
**FCD** [ISO97]. **FDR** [Low96]. **FEAL** [GC91, KR95a, MY93a, Miy90, Miy91, TN97, BS91e, BS91d].
**FEAL-8** [GC91]. **FEAL-N** [TN97].
**Feasibility** [DN95a, NFQ99].
**Feasible** [Lip94]. **Feature** [Sar99, SD99].
**Features** [ADEDS99, Zav99]. **February** [ACM98a, Fra99, FJ97, Gol96d, Hir97, Hir98, IZ98, RP97b, SJ97, Wol93a, Wol93b, van96, Ano94c].
**Federal** [Ano97h, Ano97x, Lee99a, RP94].
**Federated** [S99b].
**Feedback** [CJM95, GKH95a, Ros98a].
**Feistel** [Jut98, Kmu94a, SN93, SK96c, SK96d, Vau99a].
**Fermat** [LLMP93, MC99].
**Few** [HJPT98b]. **FFT** [DBG93, MS90b, Sch93c, Sch93g, SVB96, Vau93].
FFT-Hash [DBGV93, Sch93g, Sch93f].

Fifteen [Den90]. Fifteenth [CFK+91]. Fifth [SJ97, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni98g, Uni97c, Uni98k, ACM93b, USE95b].

FIGHT [De93b, De98c]. FIL [AB99a, AB99b]. FIL-MACs [AB99a, AB99b]. File [ANS98, AW99, Ano97a, Bia94b, Gill98, Mau97b, RC95, HSK97, MKKW99, SK97d].


Final [RIP95b, RIP95a, BFS92a, BFS92b, BP95b]. Financial [AA95, ANS98b, BFS92b, Fra99, HSW97, Lan97, Riv97b].

Finding [BMRW98, Cop95c, Ler97, Riv91a, Sim98c, YY98a, CC98, Car97c, Sta94a]. Fingerprint [DDJ98g, DJ98b, HWJ98].

Fingerprinting [Ano99h, BS95b, BS98, DF99, He96b, PS96a, PW97a, PW97b, Sas99a, YST99a, YST99b, DF98].


Finite-Impulse-Response [She92e]. Finite-Size-Particle [BVFD99]. Finland [Nyb98]. FIPS [Nat93b, Ano93f, Ano95i, Nat93a, NIS93b, Nat94a, Nat95, Nat99a].

Fire [Way93b]. Firewalls [GLZ99, Opp97]. Firms [GC97]. Firmware [MNS97].

Firmware-Oriented [MNS97]. First [BCB97, GPSV98, Hr97, KP99b, KW99, Law98, Mat94a, Nat98, Nat99c, RD99b, ACM99b, And96c, Dob98, HOQ97, IZ98, NBD’99, Uni97a, Uni98c, Uni98d, Uni98f, Uni97b, Uni98f, Uni97c, Uni98k, USE95c, RD99a].

First-Order [KW99]. Fish [BD94]. Fishermen [Ano96b].

Fissures [DDJ98e, DDJ98f]. five [KAK96]. fix [Ano98j]. Fixed [FK93b, Mae98, HP94].

Fixed-parameter [FK93b]. Fixed-parameter [FK93b]. Fixing [Low96].


Flexibility [Wed99]. Flexible [JPL99, LL94b, AG95, BP97b, Ts90].

Floating [Gar97b]. Floating-Point [Gar97b]. Floradora [Fil95]. Florence [EE92d].

Florida [IE93c, IEE94c, IEE96f, IEE97f]. Flow [STS99b]. Flows [Pin98].

fly [PS98b]. Focus [GO96c].

focusing [Com96, USE96e]. Foil [MB94a]. Foiling [Kle90, Bis92]. fold [BR91].

Folger [Mor92]. forgotten [MPS94]. Football [ARB99].


Form [Cha93, STP93]. Formal [BR97a, FBN99b, Bol98a, Bol98b, Boy92, GFB93, Gue98b, Mea95, PD99b, SM95b, Tou93, WK96, AHdJF97, APS92, Ata94, BFN98a, JW01, ZLX99]. Formality [ACD94]. Format [CDFT98, Nys99].

Formats [AS96]. Formed [Gar97c]. forms
[Mok97]. Formulae [KV94, WD99b]. Forty [CWM+91]. Forum [IEE98a, MB99a, Org98a, Ano97c, GO96c, KSS+92]. Forward [BM99a, BM99b, CadHSV96]. Forward-Secure [BM99a, BM99b].

Foundation [Ada91, BDFM99, Gol97a, Gol97b, IEE92a, IEE96a, IEEE96c, IEE97f, IEE98a, IEE99a, JR96]. Founder [Pin98].

Fourth [HKQ99, Koe99, Riv91a, DL95]. Fourier [MS94, NA95]. fourteenth [IEE95c]. Fourth [OW95, Uni96b, Far93, IEE93a].


France [Chr98, DEQ92, FR95a, GQ95, QG95, Vau98c]. Francis [Lea90]. Francisco [Ano97a, Ano98f, USE92a]. Franconia [IEE92a]. Franklin [WD99a]. Fraud [Neu92, VGP93, VvT97].

Fraud-Detectable [VvT97]. Free [BP97a, BHT98, BDI+96, CD98b, Dob97, Eri97b, GJM99a, GJM99b, HBKL99, Rus93b, SK95, All97, BT94, Des90b, Des96b, Dob95a, Ili94, Vau93]. Free-Space [HBKL99]. Freedom [Cae96b, Uni97a, Uni98c, Uni98b, Uni98e, Uni96b, UU97a, Uni97b, Uni98f, HM96].

FreeNIX [USE98c]. French [Blo98b, Bout94]. Frencelk [CFK+91].

Frequency [BP98c, MSHP99, Ano90, Tod97]. Freshness [KYG92]. FRG [Olt96]. Friedman [Uni92]. friendly [Bus96].

Friends [DD98e, DJ98f, Sch92b]. Frobenius [CPP98, Graxx, KMKH99]. FROG [WFS99, Wagg99b, GLC98, WFS98].

Front [Hed97]. Frontier [Bar93a, Bar93b, HM91, HM92, HM95].


fulfilled [Mar96]. Full [BS93a, f0rR90, SK98c, SK98b, Pos93].

Fuller [CFK+91]. Fully [BCDV94, BCDV96, HE98]. Function [BJY97, BDP97, BP97c, CP91, DBGV93, DGV93, Dae95, DC98a, DDP90, Dob97, FGY96a, HLL99, HL99, MCD99, NSS99, PB97, Sch91c, TOU94, AB96b, DK94, DFFY94, DI99, FGY96b, KSB96b, KSB97, LTT95, MZI98, MVZ98, PK97, Sch91a, SRR98, SSS95b, SSS95c, YL97c, ZPY96, d94]. Functional [Yam99]. Functions [AHV98, Ano95a, BDP99, BCK96d, BCK96e, BHS98a, BHS98a, BG99, BS94, BSG96, BM94a, BL95, BHT98, CDD99, Car93, DGV93, D90, DY91d, DY91b, DFL99, ECM96, EPR99b, EPR99a, FBS98, GJKR96b, JQ97, KTM99, Kim93, KP96a, Kra95, KS97b, LM93a, LM93b, MS99b, MS90a, Mer90a, Mer91, MS95f, Mi96a, Mon93, NR98, OS98, PW93b, PG92, Pre93a, PG93a, PGV93c, Pre97a, Pre99, Pre94b, QQ90, Roe94, Sch91b, SZ99c, SRY99, ZZ95, Zhe90, vW94, BS99a, BS99b, BD92, BGR95, BCK96b, BCK96c, BHR99, BK98f, CC98, CD95, Cus96, CS96c, Dam90b, Gol96a, Gou95, GHS93, HSK97, HLMW93, HXMW94, HYLT99, ISO97, JQ95, KL95b, Lai95, MCD98b, O'C94, PG91, PGV93b, Pre94a, PG94, Pov95, RP95b, Roe95, Rom90b, SZZ94a, SZZ95b, Sim98c, Tsu92b, Tsu92a].

Fundamental [IEE97e]. Funds [BGC93].

[KKW99].


general-purpose [Sch91b]. Generalised [GS99b]. Generalization [Jab90, HKM95, MSS93, TC99a].

Generalized [BBCM95, BFS98, CT97, HL93a, Jut98, LH93a, LH93b, Mau96a, PS96b, Bad99, BBR99, BCC99, Kn92, Por93, Son99].

generate [Wer93a, Wer93b]. Generated [SVB93].

Generating [Ble96, De98d, FMM99, Len96, Len98, MS95f, WY99, CH97b, SH99].

Generation [ARV99a, ARV99b, BG98, BGM97a, BGM97b, Bir98, BF97b, BD93, Cc97, CD96, DF91a, GJKR99, Gil99, Gut98b, HL99, Kal97b, KS98c, MWB99, Mat96b, Mau90, Mih94, PS98g, ROT94, RS98c, RS98d, SN96, SI97b, W99, Bou94, FMY98, GTS90, LLH96, MS99c, PS97, PS98h, SH94, Bou94].

Generator [FIP93a, HILL99, JK99, KS99, KW99, MS95b, PS98b, Dad93, Jenxx, MS95a, Mih96, PC98, Rev91, Sin99, TS98, Wal90].

Generators [HL99, KSW98d, Kra90, ZYWR91, CS96b, CS97b, Imp92, Kos99, Lag90, Pat91b, Por93, SGSD99].

Generic [Bel92, CM99a, MS98b, Tua99, ZK98]. Genetic [BS99a, LC99].

Genius [Ano99t]. Genomic [MUSM98].

Geodesic [Blo99, LFCK99]. Geometric [OMA98, SIM91, JM93, JM96a, Mra95].


Geometry-Based [Ben99]. George [Pm98, WG97]. Georgia [ACM99b].

Gerdes [CFK+91]. German [Wei99, Cra92, Dav98a, FT95, Ger97, Hor99, Jar97, Kah91, KK97, Kip97, Kru98, Wal98].

Germany [BFS92a, BFS92b, Fum97, IEE97d, LM98a, Wat91, Rat96].

Geschichten [CWM+91]. Get [Ano96j, Cae96b, DDJ98a, Sch98c, Ude98].

Geting [WG97]. Gets [Gar98b, GO96c, Los97, Sch98c]. Getting [Kwa93, Way95].

GI-Fachtagung [BGH95b].

GI [BGH95b].

GF [PSR97, DBVD96, LD99]. GI [BGH95b].

GF [PSR97, DBVD96, LD99].

Global [JL+94].

GMD [SBGK99].

Goldreich [Ngo99a, Ngo99b].


Goppa [Gib91].

GOST [KSW96, Sch95b].

Goverment [RKD94, SG96a].

Gow [Ano94h, AWV99, Elk96, Gar95, GM95a, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, KOB91a, Ler97, Mei96a, SX90, Zim96a, Zim98b, Pin98].

Goppa [Gib91].

Gow [Ano94h, AWV99, Elk96, Gar95, GM95a, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, KOB91a, Ler97, Mei96a, SX90, Zim96a, Zim98b, Pin98].

Goppa [Gib91].

Grace [GC97].

Gradient [Jen99].

Gral [Sal99].

Grand [FBS97].

Graph

**H** [Sru92, Lea99]. **H-1B** [Lea99]. **H** [WG97]. **H.R** [Un98c, Uni96b, UU97a, Uni97b]. **H.R.** [Un97a, Uni98b, Uni98c, Uni98f]. **hacker** [Mei98]. **Hackers** [GC97, HM91, HM92, HM95, Mei98]. **Hacking** [MSK99a]. **Hades** [Bie98]. **Hagelin** [Hag98]. **Haifa** [Bil97c]. **Halevi** [Nga99a, Nga99b]. **Halkidiki** [Pit95]. **Halske** [Dav98c, Sel98b]. **Hamburg** [LM98a]. **Hamming** [She95c]. **Hampshire** [IEE92a]. **Hand** [BF99a]. **Hand-Held** [BF99a]. **Handbook** [Bac95, MV97, Sha99a, Ata99, Rey96, Rey97, Rey99]. **Handles** [Sat99]. **Handling** [BM99a, Dae98, HC95a, Mat91]. **hands** [Riv98c]. **Handshake** [Sim96b]. **Harari** [Ver95]. **Harbor** [Kah98b, Par98b]. **Hard** [MGL98+]. **Harder** [Sch97b]. **Hardness** [BV96, NS99b, DI99, Kha93]. hardness-amplification [D99]. **Hardware** [ACD94, Bir98, BP99b, Bri90b, BS91h, Cla98a, DGV92, GN95c, Ko96a, OSA91, Wir93a, Wot99, YK98, BB95a, DN95b, Gai90, KP99b, LMS97, MZ98, Nor95a, Nor95b, Nor95c, NO96, See97, SN94, TY92, Way95, Zhe95b, Kui91]. **Harmonic** [RG99]. **Hash** [ANS97, AV98, An93f, An95a, An95i, BDPNSN97, BCK96d, BCK96e, BS91c, BS91d, BD97, BHT98, CP91, DBGV93, DGV93, Daw95, D90, DY91d, DY91b, EPR99b, EPR99a, FIP93b, GHR99, GS94a, ISO97, KP96a, Kra95, LM93a, LM93b, Mer90a, Nat92b, NS93b, Nat95, PRZ99, PW93b, PV92, Pre93a, PV93a, PV93b, PV93c, PV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sch91c, Sch93f, SV94, SRY99, Sta94b, Van93, Zhe90, vW94, AB96b, BSN96a, BSN96b, BD92, Dan90b, DK94, G90, HLM93, HXMW94, HYLT99, JG95, KL95b, MI98, PV91, Pre94a, PQ95, RP95b, Roe95, SV95a, SRRL98, Sim98c, Tst192b, Tsu92a, YL97c, DBGV93, Sch93g, ERP99b]. **Hash-and-Sign** [GHR99]. **Hash-Based** [PRZ99]. **Hash-Functions** [QG90, ISO97]. **Hash-Values** [GS94a]. **Hashing** [AS96, BGG94, DC98b, FNSS92, KP97, Kra94b, KBC97, PS93b, Rog95, Rus93b, Sch91c, Sch93f, Sho96, St391b, TZ94, BG96, Bosxx, Gil90, PJBM90, Sab94, ...
Hasn’t [Gar97a].

HotOS-VII [IEE99b]. House
[Cli97, DDJ99, BHHR99]. Houthalen
[QV90]. HP [GC97, Hed97]. Hsu
[XtTmW94]. HTTP [FHBH+97, Ude98].
Huang [PBGV90]. Huffman [Moh92].
Huge [HE98]. Hui [XtTmW94]. Human
[DDGM97, GB98, K196, RP97b, OA99].
Hundred [Uni97a, Uni98c, Uni98d, Uni98e, Uni99b, Uni99f, Uni99h, Uni97c, Uni95a, Uni98k]. Hungary [Rue93].
Hungary [Rue93]. Hunger [WSFC99]. Hurt [Gar97a].
Hut [Wel97]. Hwang [Ala97]. Hybrid
[DD99, JLM+94, KA99, MD99, NT99, Var99a, BP97b, GML994, RO96].
Hyperchaotic [BCCG99]. Hypercubes
[DHW95a, DHW95b]. Hyperelliptic
[Sma99, BK98g, OS91, OS92, SS98a, SS198].
Hypermedia [Kl99]. HyperText [RS96a].
Hypotheses [ZMI90, Kuk99]. Hypothesis
[MSU98]. I/O [Got99]. IBM [Cm90, Gar98b, Zun98].
IC [DDJ98g, DDJ98h, JT97a, PC98].
ICALP'99 [vWN99]. ICARUS [Var99b].
ICE [Kwa97, VKR98]. ICICS [HOQ97].
ICIP [Ano94, IEE96e]. ICIP-94 [Ano94d].
ICL [CFK+91]. ICSA [Nic99]. ID [CS97c, Hwa92a, Hwa92b, Hwa92c, I999, JY98, LH99, MS98a, Mu92, TC91, WS99].
ID-based [CS97e, Hwa92a, Hwa92b, Hwa92c, JY98, LH99, MS98a, Mu92, TC91]. Idea [OA99, BBS99b, BKR97, DGV94c, HO96, H98b, H99a, KSW96, Lip99, Me94, Sch93d].
Ideal [ABDV98, BC93a, BD90, Bri90a, BP97c, Pa98a, Pa98b]. Idealised [RS99c].
Idealized [MTES99, MM92b]. Ideals
[GPT91a, GPT91b]. Ideas
[GH989, RS99d, TCH+91]. Identical
[BCCG99]. Identifiable
[KOO95b, KOO95a]. Identification
[BCCG93, BLMO94, BDB92, Cha94b, GS94a, KM99b, K196, LMO95, LML98, NP97, OO98, Oka93b, Sak96, Sch90b, Ste94a, Ver95, BBC98, BM95, BM91b, DF91b, DF98, HLC99, IS99, K997, Mu92, SS98b, Sch90a]. Identities [MS99a, Sar99].
Identity [AL909, Dan95, DQ94, FKMY98, HJB97, JG90, KP98, Len99a, SS98a, Gua99, OU98b, Tan90]. Identity-Based
[Dan95, DQ94, SS98a, OU98b, Tan90].
IEC [Int91a]. IEEE [Ano95a, CH96, Ano96k, Ano97-28, Ano98i, IEE95b, IEE96d, Ka97a, KK99b, LW96, Pit95].
IEEE-IMS [IEE94a]. IETF [Ano97c]. If
[GPR98]. IFIP [Kat97, LM98a]. IFIP/GI
[LM98a]. II [Sch99b, AK99, Ano97w, Ano98c, Ano99c, BS91f, CF96, CK95, CW91b, Dar98a, Don98, Eri97b, Mit92b, Mon96, Pin98, Rat96, Rey97, RP97b, Sch93f, Sch93g, USE90, Van93]. III [Fri92b, Gan93, GN95c, Nor95a, Ree98, Rey99, USE92b].
iKP [HS96]. illicit [SG96b]. Illinois
[USE99c]. IMA
[Boy95b, Dar97, Furr93, Wal99a]. Image
[BKZ98, BNP99, DS96, DP99,Fri93, HPA99, HPG98, HWJ98, IEE95a, IEE97a, IEE96e, IEE97h, IEE97j, KZ95, KM92, LMP99, Mae98, Man98, Pit95, PZ98, PNK95, SC96a, SCxx, SJ97, SD97, SZT96b, TOH98, VP99, Wal95, YKY99, BCP98b, BCD98a, CCH98, JT96, JTB97, KS99c, KG93, KH97, NP98b, OP97, OP98, Ok96, PBC97, Sch99b, Sc99a, SH98, TK98, VP96, VP99, Xie98, YM98, CFK+91]. Image-Adaptive
[PZ98]. Imagery [WD97]. Images
[BLO95, BO96b, B99, Car95, JJ98c, KR98, KPR99, LvdVL97, Lv98, LS95, MFG95, NNE97, Per97, SC96b, SZT96a, WD96, ZK95, BP98b, BP98c, BCP97, BCP98a, BCV97, BOD95, CKLS96c, HW98b, Ibb97, Irw98, Nas94, Nat97a, ODB96, ÓPH+99, Pit96a, RR97, RK96, TA97, XBA97, ZL97]. Imaginary
[HHJ98b, HHJT98a, ZPY96]. Imagination
[Sh99a, Ros97c]. Imaging
[AA97, RP97b, Yeu97]. Imai [Pat95].
Imake [Hus94]. IMP4 [Mye94a].
Immunology [SZ96], immunity [Ada92].
Immunize [FY95a]. Impact
[Mar96, Ven90]. Impending [Bra95e].
imperceptible [CKLS96b], imperfect
[MY98]. Imperfectly [BMC95].
impersonation [SNT93], Implementation
[Auc96, Bih97b, Bra96, BS91h, Dae99,
DG97b, DRR95, DBVD96, Ebe93, Fei93,
Fe96, FOM91, Gla99a, HKQ99, HRVV99,
IM93b, KP99a, Kob98c, Koç94, Koç96a,
Lan97, LCN99, NM99, OAS91, PL94, PP90,
Ros96b, SJ98, Sho95b, Tot92, Var99a,
YKY99, You97, Zim99, BR96b, BC90,
CKM99, Dia91, HNM98, IM93a, LS98a,
Men91, MV90, MZ198, MPL99, Nor95a,
Pat96, Per91, SS98a, See97, SAM97, Vad95,
XL95b, Koe99]. Implementations
[Bas98, Bri90b, Gou98, HK98, HK99d,
Koc96b, Mos98, SV93, Wal99c, Web98,
WS98, Gai90, KSK96, Zhou94].
Implementing [SAS99b, Van95a, Lee99a].
Implications [Bas93, CMY98, NS99b,
PN92, Van95a, Wel95]. Implicit
[Jam98, MIL93]. Implicitly [HRVV99].
implies [LHL95b, LHL95a]. Importance
[BDL97, Sch99h, CM97d]. important
[Sta94a, Wec97]. Impossibility [MP91].
Impossible
[BBS99a, Fer99a, BBS98a, OK96a].
Imprimitve [Pat99] Improv [Far92].
Improved [Ano96e, BK98e, Bow90, BS91g,
CRR99, CJL+92, JM99, JJ99b, KM96b,
LD99, RP95b, SH97, SAM97, WS98, YL95b,
YL95a, ZYR91, Cao99, He92, NM95a,
NMV95b, SH95a, SH95b]. improvement
[BB95b, Bir95]. Improvements
[HLJ99, Kle90, IKN98]. Improving
[BHS93, BKPS93, GLV99, SP97, SZZ94a,
SMK98a, Sun98a, HM97b]. Impulse
[She92e]. IMS [IEE94a], In-memory
[Ven90]. in/for [SH98]. Inaccuracies
[OD99]. inadequacy [Kah98b]. Including
[DGV93, DW94, JS95b, JS95a, KL95b,
UU97a]. incorporation [Ano95c].
Jac90b, Ken95, KS98c, KW92, Mar95b, Mau93b, NIS92, Ped91b, Ped91e, Rot95a, Sch90c, Sch97c, SG96b, Sim92, Tas98.

Information
[Uni97c, WSFC99, van97a, GS94b).

Information-Theoretic
[Cac98, MW96a, Mau99a, Mau99b, MO99, Ped91d, SV99a, JH91].

Information-Theoretically
[Mau97a].

Informational
[Sga90].

Infrared
[DDJ98b].

Infrastructure
[HFPS99, Orl96, SS99d, VSH97, Ame95, Ame96a, FB97, GH96, HMT+98].

Infrastructures
[Ano99f, BPK99, BFK99, RCM99].

Inherent
[She94c, KSB96b, KSB97].

Initial
[Bih98b, BBD99, SV99a, JH91].

Initialization
[YY99b].

Ink
[BD99a, JM99].

Inkar
[AHMS99].

Inmarsat
[Lam99].

Inmarsat-B
[Lam99].

Inn
[IEE92a, IEE94a, IEE97e].

Inner
[SV98a, KSB97].

Innocuous
[CD97].

Innovative
[PJ99].

Innovative
[BP95, Ou99, RIP95b, RIP95a, VCF+90, Sim92, Tay94].

Intel[Gar97b, GC97, GO96c, JK99, SW97a, SW97b, Wor96].

Inteligenz
[CWM+91].

Intelligent
[BS95e, CFGS99, LQR+98, Ate98].

Intelligence
[AK99, Hrn93, Rat96, SW94b].

Intellectual
[BP95b, MB97b, TH99].

Inter-domain
[KMP99].

Inter-functional
[TH99].

Inter-functional
[BB99b].

Interconnection
[BW98, Por91].

Interconnect
[IBM93, Gog99, HVH98, LTEH99, JDM+91].

Interconnections
[DMVC99].

Interferometric
[Hru96].

Interleaving
[TH99].

Internals
[Zim95b].

International
[AR97, Ano99c, AA97, Auc98, BCB97, Bih97c, Bir92, Bir93, Cha91, Chr99b, CMM93, Cop95d, ES98, Fra99, Fum97, Gol96d, GQ95, Hed97, Hir97, Hir98, IE95a, IE95b, IE96a, IE96b, IE97c, IE97h, IE97g, IE97d, IE97g, IE98c, IE98d, IRM93, IZ98, KC96, KM96a, Knu99c, KP99b, Kra98, LOX99, Mad92, Mar97, Mat96b, MDS90, MK99a, MP94, Nyb98, OW95, OiDP98, PSN95b, QG95, Sti93b, Sti94, TM99, Ved99b, Wat91, Yua92, And96c, Chr98, Cop95b, DG96, Des94b, Ele99, FR95a, HO97, Kail97c, Kob96, LM98a, Lom97, Pre95a, SP90, Sta97c, Ste99b, TV94, Vou98e, Wad98, Wie99, vWN99, Int91a, Moc97, See97].

Internet
[Cha99a, SS99d, Ano97z, Ano98b, Atk97, Bel98, BO96a, B99a, Bet95b, Bet95a, Bhi96, BDC+95, FFW99, FT99b, Fum98b, Gar97a, Gar97b, Gar97c, GC97, Gar96b, GO96c,
HA94a, HFPS99, HC95b, II96, Ken93, Lin88a, Lin89a, Lin93a, Los97, McC96, Mit92a, Opp97, Pau99, Rit99, Ros97c, Sar97, Sch99b, Sme97, Smi97b, SL99, TAP90, VJ98, VM96, Way98, Wri98, Zim98, dVdVI98, Sha99a.

Internetworks [Sta96d].

Interoperability [BPR99, RCM99, UNU94].

Interpersonal [Ano97p].

Interpolating [CW91a, LC96b, LC96c].

Interpolation [JK97, MSK99b].

Interpretation [Bie98, KO95a, Mor92].

Interrupt [HC95a].

Interview [Di 97a].

Intra [DVPL92].

Intra-Domain [DVPL92].

Intracerebral [BALS99].

Intractability [HT99, Luc95].


Intrusion [Hur98].

Invariant [BS95d, GO93, KA99, OP97, OP98].

Invariants [DR94c, Mra95].

Invented [Got99].

Invected [DDJ98d].

Inversion [Len96].

invertible [DKR98a, BKR98b, NO98].

Investigating [W935].

Investigation [JR96, Ano97q, Xie93].

Investigations [MDS99].

Investing [MS99a].

invincible [Me98].

Invisibility [Aur96].

Invisible [CMY98, YYH98, YM98, CMY97, ZL97].

Invited

[BE90, Bra90a, Bri90b, Di90, Duh90, FK93a, Fuc99, HMT98, Koh90, Le90b, Sim90b, SB93, Sim90, Wat99, BS91c, Gol99c, Sim91].

Involving [FMM99, Bea92, Pos98].

IP [An95b, Atk95a, Atk95b, KA98a, KA98b, MB99a, MS95c, MS95d, OG97, MS95e].

IPSEC [Wa96, GK98].

Ireland [IEE97a, IEE96b].

Irish [Got99].

irreducible [Ito91, Kob91c].

IRREGULAR [FR95a].

irregularly [FR95a].

Irrelevant [BD99a].

Irreversible [ANS97, AA95].

ISAAC [Jenxx].

ISAKMP [CH97a].

ISBN [Hat96].

ISC [Ano93g].

ISO [Int91a, Gar98b, GQW91, VGV93].

ISO-OSI [VGV93].

ISO/IEC [Int91a].

ISO/IEC [GQW91].

IsocRob [AVLPF99].

isogenies [Gal99].

Isolation [GX99].

Israel [Bih97c].

ISSAC [Wat91].

issuance [FL99b].

Issue [DF91c, Eri97b, Ano97e, FT99b, MDP94].

Issued [Gar97c].

Issues [Ac98b, Don98].

items [Uni97d].

Iterated

[ABDV98, Pat99, BCKxx, Bih92, Har96a, HLMW93, HXMW94, Ort95b, Ort95a].

iterating [HNSM91].

Iterative [CDN98, Knu93b, MG91, LYG94].

itself [Ri96].

IV [IEE93a, BP98c, Far93, MD98, USE93].

I’ve [Bra95d].

IX [T99].

J [Ers99, Hat96, Sha99a, Wai95].

Jack [Pin98].

Jacks [Bec99].

Jacobi [BK98g, Kob91c].

Jacobian [Kob90].

James [Scu92, Sha99a].

Jammers [SV95b].

Jan [WL92a].

JANET [You97].

January [ACM97b, ACM99a, Ano97a, Bih97c, SP90, USE91, USE92a, USE92a, USE96f, USE98d].

Japan [Ano93g, Ano99c, IEE96b, IR93, IZ99, IZ99, Win93].

Japanese [DK99b, Mea98, Wei99, Win93].

Java [ACM98a, Dra98, GA98, Ale98, AW99, Ano97u, Ano97v, Ano97-7, Bann97, Bar99, Ber97a, Ber97, Bro97, DDJ98e, DDJ98f, DDJ98a, DDJ99, Di 97b, DT98b, DE99, Hol99, Gar97a, Gar97b, GC97, Gar98b, Gar96c, Gau97, GPO98a, GPO98b, Gon98, GS98, HN99, HH98, KHB99, Knu98a, Law98, MGL98, MF97, NK98b, PV98, TJ97, Taa98, Tre99, WBDF97, Way98].
You96, Zuk98b, Zuk98a]. **Java-based**
[Ale98]. **Java*/Smart [Bro97].
**JDesignerPro** [Ano97s]. **Jedi** [MPS94].
**Jenayah** [Ano97-29]. **Jeopardy** [Gar97c].
**Jobs** [RH93]. **Johnny** [WT99].
**Joining** [ARH95]. **Joins** [Law98].
**Joint** [Ano93g, Cla98a, FH94, IEE94f, IEE95c, Kat97, IEE92d, vT93].
**Jose** [Com96, FJV97, RP97b, Sj97, USE96e, USE96g, van96].
**Jour** [Lut98].
**Journal** [Eri97a, Zol93, OW95].
**journyx** [Ano97s].
**JSafe** [Way98].
**JTC** [Gar97a]. **Juan** [CMM93].
**Judge** [GC97].
**Judiciary** [Uni96b, Uni97c].
**July** [AR97, AA97, BFS92a, BFS92b, Com96, DG96, IEE94b, IEE94f, IEE96b, USE96e, USE96g, vPN99, Uni98i].
**Jump** [DRR95].
**Jumps** [Gar97b].
**Junction** [CIBM99].
**June** [ACM95, An96c, AA97, GS94b, IEE92a, IEE94b, IEE94f, IEE96b, IEE96c, IEE96f, IEE97g, USE96e, USE98c, USE98e, USE98x, USE99d].
**Junk** [DN93].
**JW** [Ano93g].
**JW-ISC** [Ano93g].

**K-64** [Mas94]. **Kahn** [Ers99]. **Kamakura** [IZ99].
**Kansas** [Sin98]. **Kapera** [CWM+91].
**Kasmira** [PNdhhbbprn91]. **Kawasaki** [DP99]. **kazdeho** [Gar98c]. **Keep** [BK90, Riv98c, Sch95d, Way95].
**Keeping** [Oko97]. **Kelly** [CFK+91]. **Kenmare** [IEE96c].
**KERBEROS**
[Hor94, ARH95, An90e, Atk93, BR97a, BP98e, BP98f, BM91a, Bor93b, Br98, DW98, DS90b, Dav95, DG95, DT96, De93a, HRT96, HI99b, Kay95, Koh90, KN93, KNT94, Le99a, Lin96b, Lun90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts97, Tu99, Yu94a, Yu94b].
**Kernel** [BCCG93, WB92]. **Kerry** [IEE96c]. **KEY**
[YY98d, ANS97, ANS98b, AKP96, AAB+97, AN95, IBM93, An90a, An90c, An90e, An90m, An97e, An90f, An90h, AA93, BP98a, Bi95, BDH98, BDG98, BCE’94, Bar96a, BCG90, BR94a, BR95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BS97a, Bir98, BMS94, BW98, BW99a, BW99b, Bla94b, BDR96, Bla96c, BPK99, BFK99, Ble97, BDH93, BS96, BDF98, BD99b, BF99c, Boy90, BM94b, Bra95c, BS94, Bur94b, BMT98, Cae96a, CC99b, CG99, CDN98, CJS91, CM97a, CS98b, Cra98, Cs97, DDJ95, DDJ98b, Da98, Dam91b, DK96, Dan95, DD90, Dav96, De93c, DP98c, DB96, Di90, ECM96, iFiR90, FW91, FDB93a, FY95a, FY98a, FYM99, FKS98, FO99a, Fum98c, Fum93, GY90, Gao96, Gan96a, GJK99, Gip91, Giv96, Giv99, GM90, GGH97b, Gys96, HK99a, HGS98, HP98a].
**Key**
[HS90, HMT98, HMV93, Hj98b, HD96b, HJJ+xx, Hes97, HPS98, HPS99, HM98, HR90, Hwa97, Iss90, Jab90, Jas96, JV96, Kal99, KP99a, KSW96, KSW99a, Ke99, KS99b, KP96b, KM90c, KT91a, KMOV91, KKOT91, KP93, RSA93f, Lan99, LM94b, LW95, LMS97, LA98, LP99, Low96, Luc98b, Mah96, Mar97, Mat91, MY91, Mau93a, MW96a, Mau97a, MP91, Mv93, Men93, MM96b, Mic93a, Mic93b, MS95f, MM99c, MS99c, MS99d, MS99e, MS99f, MTS92, MAO96, MM98a, MM98b, NMR95, NS97a, Nec96, Neu97, NS99a, Oka94, OU98a, Oka98a, Oka98b, Oum90, vO91a, PSR97, Pa99d, PKOT94, Pat95, Pio97, Pot99, PB99a, RAS93b, RAS93e, RSA94, ROT94, RS98c, RS98d, Ros96a, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c, RCM99, SSN98a, SYM98, Sam98, DPD91, SGS99a, Sch94b, SKW+98a, SKWW97].
**Key**
[SOOS95, SM95a, SE96, Sha99b, She94d, SiK93, SR96, Sh98, Sta99b, ST91, SW99b, SH94, Sun98a, Sut99, TAP90, Uni98i, Van95a, Van93, VSH97, VVT97, VBD99, WM93, dWQ91b, WLEB96, WW98b,
WKS+99, Wie96, Wie98a, Wie98b, Wol98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vOW96, A995, Acc97, Lip98, AD97, AD99, AI 96, Ano90, Ano96m, BSNP96a, BSNP96b, Bao94, BI94, BDHJ97, BD98a, BTD98, BSB97, BR96b, BCK98, BY93c, BY93b, BS91a, BFG95a, BMP97a, BF96, Ble96, BMS96, BFS98, BM95, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Cra97, Cus95, DKR97b, DW96, DS90a, DH96a, Des95, DVQ96, Dhe98, DvW92, DN95b, ES97, FGB97a, FMY98, Fre94, Fro96, FGLP96a, FGLP96b, FL93, Gar96b, GH96, Gib95, GL94, GLH99, GTS90]; key
[HNSM91, HP99a, HP99b, HY93b, Haw98a, He92, HW96, HJJ+97, HI97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IZ98, IZ99, JM96a, Jar96, JLM+94, Jon90, JY98, KASH90, KM99a, KSW97a, KSW97b, KL94, KR96b, Kir95, Ko997, KM99d, Kum97, LG97, Las92, LJM97, Lee95, LC96a, LM94a, LZ90, LZ91a, LD94, LL95b, LCL95, Lon91, Lon92, Low95, MS98a, Mao97, MLA91, Mau91b, MY93b, MKKW99, Mu92, MLLG95, NM96a, NY90, Nab97a, Nec91, Odl94b, Ole95, PS98e, PS98f, Pet91, PP92b, RT93, Roe99, Sal90, Sal96, SW95a, Sch92c, Sh99a, Sh99b, Sh99c, SK97y, SY96b, SM90, SM93b, SS95b, SS95c, ST95w, Sun91a, SS98b, Swv93, SM95b, Tab94, Tao94, TCC97, TC99b, TC99a, Te90, TC91, Tze99, TH99, Uni97c, Uni95a, V96, Ven92, Van92b, Wie94, Wil93b, Xie92]; key
[Xie93, XLP99, XW97, Yam98a, YL97b, Yu92, Zha91, Zhe95a, Zhe95b, ZPY96, vOW91, vO92, vT90, MC96, BFS92b]; Key-Agreement [RSA93b]; key-clustering [RSA93b]; Key-dependency [MAO96]; Key-Dependent [FS99]; Key-Escrow [VvT97]; Key-Exchange [Dan95]; key-management [ML91]; Key-Recovery [Oka98a, Oka98b]; Key-Schedule [KSW96]; Key-Search [KP99]; Key-Share [BWM99b]; Key-signing [Ros96a, Ros96b, Ros96c]; Key-specific [LMS97]; key-vowel [Lip98]; Keyboard [GO96c, She95a, Ale97]; Keyboards [CFK+91]; Keyed [Ano95a, BN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pre99b, MS95e, BN98a, Gon95, KBC96]; Keyed-Hashing [KBC97]; Keyed-MD5 [KBC96]; Keying [BCK96d, BCKxx]; KeyNote [BFK99]; Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Dae98, EHM99, Gir91, KSH97, KSH98, KM99c, Lum98b, MP91, PS98g, SV99a, SV99b, Ste94a, Van96, Way96b, Bih94a, CH97, Cl99, DGV94c, JP96, KC95, Kn95, LL93, M99b, MF97, Mok97, SS97a, SS97b, SV98, SH99, Sta95a]; Keystroke [CD98c]; keystream [CS96b, CS97b]; keystroke [CG97]; Kid [FK93a]; kids [WS96c]; Kimba [KW99]; Kind [AM97, SX90]; Kingdom [D*98, Lom97]; Kingston [TM99]; Kiosk [BO96a, Gar96b]; Kit [Ano97u, Sun91b]; Kleptographic [YY97b]; Kleptography [YY97a]; KMOV [Ble97]; KN [SMK98a]; Knapsack [CP91, JS93b, ACR90, C90, He92, JG95, LC97b, Odl90, Yan92, Yu92, Zha91]; knapsack-based [He92]; Knapsacks [CJS91, Ort95b, Ort95a]; Know [DD99, Fly97, Hill97, Kir95, Mil95]; knowing [Ble96]; Knowledge [ADB99, BMT98, BG90, BG93, BJY97, Bie98, BD91, BDB92, COM99, Coc97, CDS94, CD98b, Dam99a, DDP94a, DDP99, DO99, DKF93, DS98b, GM91, GK96, GSV99, G093, HT98, JKVP99, NOV93, NM99, O090, RS91, SI93a, SY99, Stu99, Tou91, BOGG+90, BBP95a, BBP95b, CDP95, DDP94b, DF93, DP94, DF91b, SA99, Sak97]; Knowledge-Based [Bie98].

Key-Search [KSW96].
SHG98, DSSZ99. **Library**
[Ano97v, CFK +91, DK91, KHB99, Dhe98, RRP97, Man98]. **License** [AG99]. **Licenses** [Ano97v, Tj97]. **Licensing** [Par98a]. **Life** [CJ99, DDJ98e, DDJ98f, DQ94, GAGCDAFC99, Ros95a, CWM +91]. **Life-Span** [DQ94]. **Lift** [Gar97a]. **Liftings** [CNST98]. **Light** [Gar97b, HPG98, YYH98, BGH +95a]. **light-weight** [BGH +95a]. **Like** [JQ97, BS90a, BS91c, CCZ98, Kob99, MS95f, MT99c, Nac93, WSFC99, XZZ97, Kim93, KP93, Way93a]. **Likely** [Bar96a]. **Limit** [Lea99, Way93c]. **Limitations** [BM91a, CMYY98, Fis98, KV94]. **Limited** [AR99, BDS98, DQV96, VBD99]. **Limiting** [KI96]. **Limits** [And96b, AP98, EKK99, Swi97, BH98, SOB98]. **Line** [Bra95b, Cac95a, Cac95b, CDFI95, DT98a, Ell99, EGM90, EGM96, LMOB95, PUF99, SS99e, SS99f, Tra99, DL98, Gau97, Mao98, Nal97, VN99]. **Line/Off** [EGM90, EGM96]. **Linear** [Ano95a, AMP99, BGS96, BK94a, BL95, BPV99, CFSY96, Dae95, DD99, Des98a, vD95a, DLR97, Gol95b, H096, Haw98b, KR94b, KR95a, KT949, KR99b, LO91b, LH94, MS94, Mat93, Mat94b, MB96a, Nyb95, OA94, Ros98a, SZ96, SF97, Sch96c, Sch991, Sf98a, SK98c, SK98b, TN97, TSM95, YMWP99, ZYR91, Ala93a, AW95, BS95, Bao94, BI93, Bnh95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, HKM95, Haw98a, Jak98, KY95b, Kyyx, KR96c, Kuk99, Lai95, LLB98, Lan95, MM90a, MAO96, MK92, OG95, SKD94, Tz99, YT95a, YT95b, ZYR90, ZH90, vD95b, vT94, Duh90]. **Linear-Time** [KR99b]. **linearity** [SB95]. **Linguistic** [CH99a]. **linkage** [HCY96b, LC97a]. **Linked** [BRS99]. **Linking** [BLLV98, CM95, RP94, SM99]. **Links** [BIO99, CV95, DDM98, JC93]. **L’inuktitut** [Ano99g]. **Linux** [Cor98, DDJ98a, Eri97b, Mor97]. **Lion** [AB96a]. **Lippman** [vdWS97, vS97]. **LISA** [USE99b]. **LISA’96** [USE96a]. **List** [LC97b, Uni97d]. **Lists** [FGR92, Riv98b]. **literate** [Sab94]. **little** [Ano91b]. **little-known** [Ano91b]. **Lives** [DDJ98d]. **LL** [FY95a]. **LLL** [Mis97]. **Local** [Fum93, IEE97d, IEE98f, MM95]. **Localization** [PF99]. **Locating** [KP93]. **Location** [FJP96, Jac96, KFJP96, KRJ98, WHFG92, FT95]. **locking** [CS96b, CS97b]. **Locks** [Way95, CC95]. **Locomotive** [Var99b]. **Loen** [LW96]. **Lofthus** [Hel94]. **Log** [Bal95, GJKR99, Gor93a, PS98b, WD98, YY97b, Kob90, SS95a, SK97d]. **logarithm** [CPS95, CS97d, FR94, FMR99, HY93b, HI97, HMP95, McC90a, MVZ98, NR95]. **Logarithms** [BBT94, CH98, GM93b, LO91a, Man94, MW99, vO91a, Tes98, vO91b, VW94, Gor93b, HZ93, Odl94a, SS95b, SS95c, vO92]. **LOGCFL** [LMSV99]. **Logic** [AHMS99, BRS99, BAN90, CIBM99, CO98, DRR95, Gue96b, SG95, SM95a, SHK99b, CS99, Pos98]. **Logical** [PS99f, Wad93]. **Logics** [ADD99, GAGCDAFC99, KW99, Len99b, WK96, Bad99, XZZ97]. **Login** [ARH95, DQ93, HI97]. **Logout** [Poo95]. **Logs** [SK98a, SK99]. **LOKI** [BS91f, BKPS93, Kn92, Knu93c, Kn95, TSM95]. **LOKI91** [Kn93d, Kn93a, SF97]. **LOKI97** [BPS98, RK98, Rij99]. **London** [Ano93d, Ano97p]. **Lone** [Ano97r]. **LONE-TAR** [Ano97r]. **Long** [CHN97, Len96, RH93, SS95, Pos93]. **Long-term** [CHN97]. **Longevity** [Rot95b]. **Look** [Coh96, Has99, Pf95, Zha97, GTGW94, Way91]. **Look-up** [Has99]. **Looks** [Sch97b, vWS97, vS97]. **Loops** [SvA +98, SHK99b]. **Lorenz** [Car97b, Dav98d]. **Lose** [GPR98, Way96b]. **Losses** [Law98]. **Loss** [PW97c]. **Lossy** [CI96]. **Lottery** [Riv97a]. **Lotto** [QD91]. **Lotus** [Dwo95]. **Louis** [Ers99]. **Louisiana**
Many-to-One [BHSV98b, BHSV98a].
Many-Valued [KW99]. Map
[Bih91, KMKH99, CPPPK98, HNSM91,
LYG94, TOU94]. Maple [Yan95]. Mapper
[BPR99]. mapping [FO90]. mappings
[LFSY94, Nyb94]. March [ACM98a, Ano95l,
BC97, IEE99b, IZ99, Knu99c, Nat99b,
Uni97b, Uni98b, Vau98e, Uni98g]. Market
[Wor96, Org98a, Sta97c]. Marketplace
[GC97]. Markets [And96a]. Marking
[BLMO94, LMBO95, LM98b, PAK98,
PA98b]. Markov
[AA93, HSW94, LMM91, MFG95, OG95].
Marks [LT98, BBC98a]. Markup
[Uni98b, Uni98c, Uni98e]. Marling
[CFK+91]. Marmaras [Pit95]. MARS
[BCD+98b, Con99b, Zun98]. Marvelous
Maryland [ACM90, Ano96a]. MAS [CF99].
Maschine [CWM+91]. Masked [Web93].
Masking
[CJM95, JMLW94, SZTB98, Ti98].
Masonic [Mor92]. Mass [USE98b, ZTR99].
Massachusetts
[ACM96a, IEE95c, IEE98f, USE94].
MASSC [Tua99]. Massey
[HWB93, LLG10]. Massive [Pos98].
Massively [GM93b]. Master
[BF96, CWM+91]. Master-key [BF96].
match [CGM96, GOL97c]. Matching
[HTY99, WD99b, Sch91b]. Math [Gar97b].
Mathematical
[BDFM99, PBVP99, Car98, Lid90].
Mathematics
[Far93, Mil96b, Con99, Duf98, Sch98b, Sch99b]. Mathematic
[SPS97]. Matrix
[CD91, CZ90, Whi93, Gar97d]. Matroids
[KOS+94]. Matsui [Bih95b, HKM95].
Matsumoto [Pat95]. Mattheyses
[CKM99]. Maximal
[Br91, Man90, HJPT98a, HJPT98b].
Maximus [DSB99, Bau97]. Maximum
[DJL93, Kob99]. May
[ACM90, ACM91, ACM93b, ACM94c,
ACM95, ACM96b, ACM97c, ACM98b,
ACM99b, And96c, Ano97p, BV98c, CH96,
CFG96, CMM93, Dam90a, Dam91a, Dan96,
De 95, FIP93b, Fum97, GQ95, GS94b,
Hei96a, Hel94, IEE92c, IEE93b, IEE94d,
IEE94e, IEE95b, IEE97i, KG96, Man96b,
Nyb98, PGV93d, QG95, Rue93, Ste99b,
Uni98d, Uni95a, USE99c, Uni98a].
McCurley’s [WD98]. McEliece
[Ber97c, CS98a, CC98, Gib91, Gib95, JM96a,
KT91a, LDW94, Sun98a, vT90]. McCaffin
[RP95a]. McNeil [CFK+91]. MCS [Jia99].
MD [IEE94b, NIS92, PV95, USE92b].
MD-x [PV95]. MD4 [Ano95a, DB91,
Dob95a, Dob96a, Dob98, Dobxx, Kal91,
Riv90a, Riv91b, Riv92a, Vau95, DB91].
MD5 [MG98a, Ano95b, BAK97, BCKxx,
Ber93, Dob96b, GTG94, KR95b, KBC96,
MS95c, MR95b, OG97, Par98a, Pre95b,
Riv92b, Ros93, Tow95, DB94]. MDx
[SRRL98]. MDx-family [SRRL98]. me
[ZKOY99]. means [WD99b].
Measurement [RK99, SCG99].
Measurements [VNW94]. Mechanical
[SY99]. Mechanics [PT95, Ros97a].
Mechanising [BP98]. Mechanism
[BDPSNC95, Bis91, Lin96b, New98].
Mechanisms
[HJ99, Mye94a, CGM96, HC95a, ZH93].
mechanization [Bo97]. Mechanized
[SM95a]. Medals [JJ98b]. Media
[DDJ98d, GB98, Hat96, MW98b, Ros94].
median [KR99b]. Mediated [FJ98].
Mediator [Kem99]. medical [Cha99b].
Meet [FY99, Van95b]. meeting
[Sh99a, Zim96b]. Mellen [Ers99].
Members [Par98c]. Membership
[FG92, Fis98, OOK91, SPP99, AK95,
MW94, Sak97]. Memoir [Bar05]. memoirs
[Sed94]. Memorial [IEE98b]. Memory
[ARV99a, ARV99b, CM97a, DHRM96, Fis97,
Got99, KS99a, Lei99b, MS91, Sha95a, Gut96,
Has99, Ven90]. Memory-Bounded
[CM97a]. Menezes [Sha99a, Kie98].
Mental [CF99, Jun99, KKOT91]. Merced
[GC97]. Merging [DVQ96]. Merkle
[NS97c, NS97b]. mesh [PHF99]. Message
[AGS97, AB99a, AB99b, Int91a, ASZ96,
Bax97, BG90, BCK96d, BCK96c, Ber97c,
Bie98, BHK+99, CDFT98, EPR99b,
EPR99a, FH94, GLZ99, GTG94, GQW+91,
HK97, Kal91, KR95b, Kal98f, Kal98d, K97,
Kra95, KBC96, KBC97, HK99, Lin88a,
Lin89a, Lin89b, Lin89b, Lin89d, Pre98a,
RSA93d, Riv92a, Riv92b, Rog95, Sho96,
Ts92b, Ts92a, WSK97a, WSK97b,
BSNP97, BGR95, BJQ97, CLH98, Cli99,
HMP95, HC97a, Lin99a, Riv90a,
Riv91b, Sta99b, Tze99, Yeu99].
Message-Digest [GTG94, Riv92a, Riv92b].
Message-Efficient [FH94]. Message-Resend
[Ber97c]. Messages
[CFPR96b, vD97, SS99c, SKAM99,
CFPR96a, Joh97b, Kip97, Mit92a, Par98b,
Sch95d, Way93b, Wri98]. Messaging
[DDJ98c, AC97, DMW94]. Meta
[EKLM99, FBS97, HMP95, PS99f].
meta-blind [HMP95]. Meta-Logical
[PS99f]. Meta-message [HMP95].
Meta-Object [EKLM99]. Meta-Protocols
[FB97]. MetaML [MTES99]. Metaphor
[BP95a, Fuc99]. Metaphors [BJH99].
Metaproof [DY91a, DY91c]. Meteor
[Sch93a, UN94]. Metering
[SK96b, SK96e, Ros94]. Method
[AG98a, AG98b, ADD99, BP98f, ESST99,
GDD+97, HRV99, KI97, KT93, LL94a,
Mat94b, McM96, MS95f, Miy93c, SF97,
SKBxx, Tes98, VN94, CP94, CM97c,
GTS90, JTD93, JTH97b, Joh98, KN98b, KAK96,
KH97, LC98, Mat93, MY93a, McK99, Pit96a,
RT93, SH99, Su98, Vu95, YEA+98, ZH90].
méthodes [Bec90]. Methodology [CH99b,
DD95, FM98a, NMR95, PNFK95, SSSW98].
Methods [Bas93, Bir99, CL98, DSB99,
GSY99, IM93b, KBR97, LvdLL97, LM98b,
MCD99, Per99, SW94a, AHdJ97, Ale92,
Ata94, Baur97, BGR95, Car97c, HLC99,
IM93a, vdl98, QN98b, RT93, Rh95,
Shp99b, TG94, Wh93, XL98, van98].
Metric [Joe98, RS99b]. Metrics [LA98].
Metropolis [DP99]. Mexico [IEE91].
Meyer [Lu98, QJ98b]. Meyer-Müller
[QJ98b]. Mi [XTmW94]. Miami [IEE97f].
Micali [Zhe95a]. Micro
[Ano99, HS96, Pri94]. Micro-payments
[HSW96]. microcomputer [HNM98].
microcontroller [Kh98].
Microcontrollers [KKW99]. MicroMint
[RS96b, RS96c]. Micropayment
[JO97, RS96c, RS96b]. Micropayments
[Riv97a]. Microprocessor
[DDJ98d, Mar96]. microprocessors
[NM96b]. Microsoft
[Boy98, Fly97, Gar98a, SM98a, Ts97].
Middle [BB99]. Middleware [BCCD99].
Might [DDJ98c, DDJ98f]. Military
[Ano96n, Fri92a, Fri92b, LU95]. Millicent
[Man95]. Million [Ran01, Riv91a]. Millions
[Wal99b]. MIMD [DH99a, DH99b].
MIMD-factorisation [DH99a, DH99b].
MIME
[Ano95c, Ano95n, Ano97b, El99, GM95].
Minefield [Han94]. Mini [Jakt99b].
Mini-Cash [Jakt99b]. Minimal
[BDR+96, GM90]. Minimalistic [Jak99b].
minimally [CGM97b]. Minimax [All98].
Minimization [LE99, SB99]. Minimizing
[BR97b, SSN98a]. Minimum
[Ano95m, Ano97b, DK96, FO99a, CC98].
minimum-weight [CC98]. Mining
[DC98c]. Minneapolis [IEE97].
Minnesota [IEE97]. Minorities [Cha90].
Minsky [GTGW94]. MIPS [Si99].
Miss [BBS99b]. Missed [LKD98]. Mistrust
[Bla93]. Mistrusting [CGM97a, Mar97].
MISTY [Mat97]. MITRE [Go90a]. Mix
[Abe98a, FJ98, SK95]. Mix-Mediated
[BP96]. Mix-net [Abe98a]. Mix-servers
[Abe98a]. Mix-Type [SK95]. Mixed
[DDJ98d]. Mixes [JFP96, PP90].
mixing [VP98]. My2a [IKM99]. MMH
Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].

Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode
[BK98a, BK98b, MT95, BP98c, CJM96, PNRB94, PA98a]. Model
[AR99, BMT98, BPRF99, Bol98b, CJM96, PNRB94, PA98a].
multi-carrier [SVWMB95, SOB98, VSB95].
Multi-disciplinary [DFGH99].
multi-exponentiation [CL97a].
Multi-function [KSB97, KSB96b].
Multi-Receiver [SNW98b]. Multi-Secret [BM99c, BDD+94]. multi-senders [HW98c].
Multi-Service [HS94]. Multi-tiered [CC99c]. Multi-user [SJS98].
Multi-variable [TN96a, TN96b]. Multiapplication [Gir99, Tua99].
Multidrawing [BMRW98]. Multifeature [Bet95c]. Multifunction [She94c].
Multigroups [OOK91]. Multilevel [CGB+93, GPSN98, KT96, DN95a, ZH93].
Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D+98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBRS97, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, EIE97k, Kat97, LS98a, Oko97, PSB97].
Multitaplication [GMC95]. Multiparty [GMC95].
Multitaplication/Encrypted [GMC95]. Multi-Service [IJRH94].
Multitaplication [HS94]. Multi-tiered [CC99c]. Multi-user [SJS98].
Multiple [AS96, Bih98a, Boy90, DK96, GO96b, Han94, Kal92, KR94b, KR96a, SS99e, SHK99b, Wag98b, Bih95a, GK91a, KSL92, Or95b, Or95a, SSM94].
multiple-iterated [Or95b, Or95a].
Multiple-length [Han94].
Multiple-precision [Kal92]. multiplexer [SGSD99]. Multiplication [Abe99, KAK96, Kor93, MS93, Zim99, FBT96, Ias99, LC98, TY92].
Multiplications [MNSV97]. Multiplicative [BBBDW96, DDB95a, DDB95b, Mis97].
Multiplier [HMvT94, HWB93].
Multiprocessor [BPS96]. Multiprocessors [Lei99b, HJ99].
Multi-receiver [SNW98a]. Multi-resolution [BCV97, HW98b, SZT98a, SZT98b, XBA97, KH98a]. Multiround [Geh94, Geh95].
Multisecret [DLR97, JMO94, WAMO94].
Multisecret-Sharing [DLR97].
Multiversion [KT96]. Munich [IEE97d]. munitions [Uni97d]. Muscle [Cor98].
Musicians [MB99a]. Musings [Ins95]. must [Csi95].
Mutual [Bak99, ARK99, BO99, CS96b, CS97b].
Mutually [CGM97a, IS91, Mar97, HY93a, JMO95a, Wus92]. My [Cur98]. mystery [Fra93]. Mythical [Sil99].

National [Acc97, Ano96a, DDJ98e, Dan96, IEE94b, NIS92, Uni98a, Wei91a, Wei91b, Rat96, Uni98d, VB96]. Nations [Sch98a]. Natural [Din94, KKL99]. Nature [BMM99a, BMM99b]. Naval [Wei99, SW94b, Win93]. navies [Don98].
Navigating [HE98]. Navigation [YKB94].
NBS [Gau90]. NC [Blu97]. NDRAM [Gar97b].
necessity [KK97]. Need [DS98b, Fly97, RS98e, V995]. Needed [RSxx]. Needham [Low95, Low96].
MY93b, Sah99. Non-invertible
[NO98, BKR98a, BKR98b]. Non-linear
[FCD98, Jak98, KR96c, LLB98].
non-linearity [SB95]. Non-Malleable
[DDN91a, BS99b, BS99c, DDN91b, Sah99]. Non-maximal
[HJPT98b, HJPT98a].
non-Oracle [Ano95k]. Non-perfect
[Pa98a, Pa98b]. Non-Reachability
[DR94c]. Non-repudiation [GP99].
non-secret [Ell97]. non-secure [Sin95].
Non-Synchronized [Yah94]. Non-uniform
[AWV99]. Noncryptographic
[Fei99]. Nondeterministic
[Mol98]. nonequivalence
[Mol98]. nongroup
[SBB99]. Noninteractive
[GSV99, Ped91c]. Noninterference
[MC92]. Nonlinear
[GYS96, KT91b, MS99b, Pit95, Go99c, RD96b].
Nonlinearity
[MS90a, SZZ95c, SZZ95a]. Nonlinearly
[MS94]. Nonmonotonic
[COM99]. Nonoblivious
[FNSS92]. Nonperfection
[KOS+94, OKT93, OK98, OK95].
Nonrecursive [Ruo94]. Nonreproducible
[LHW98]. nonrigid [Nas94]. Nonsecret
[DD98g, DDJ98h]. Nonsense
[BS91a, MS93]. Norm
[TK99]. Normal
[Bra90a, Ran01, Mok97].
Normalisation
[ZTR99]. Norway
[Hel94, LW96]. Norwegian
[PP96, Sel94, Sel98b]. Not-So
[Ano99a, CM99c, Chr99a]. Notable [Bar94].
Notarization
[SK97b, SK97a]. Notation
[Sch99c]. Note
[Ano95g, Ano95h, Ano96g, Ano96h, Ano97k, Ano97l, Ano98d, Ano99a, Bib99c, BPK99, EKK99, KM92,
Roh99, Blu95, CJR99b, ES97, GH99, LM93c, MS98a, TX92, YL97a, Yu92].
Notebook
[Ano99a]. Notes
[GB98, KSF99, WN94, Dwo95]. Nothing
[BMM99a, BMM99b, Boy99, GMW91,
Riv97c, SRY99, Ste98b]. Nothingness
[Way96a]. Notions
[BDPR98, BS99b, BS99c]. Notwendigkeit
[KK97]. Novel [Ger99a]. November
[ACM93a, ACM94a, ACM96a, ????0,
Ano94d, Cli97, DEQ92, GN95b, HOQ97,
HF97, IEE91, IEE92b, IEE97i, IEE98a,
IRM93, KM96a, LOX99, PSN95b, USE96d,
USE96b, USE99b, UU97b, XiTmW94].
Nox
[Ts’90]. NP [BD91, DDP99, DFKN93,
GMW91, NOVY93, Sch94k].
NP-completeness [Sch94k]. NRC [Wor96].
NSK [PP96]. NSN [Un94a, Un94b]. NSW
[GN95b, KG93, VPM97]. NT
[BD98, Hille97, HIl98, USE98a]. NTRU
[HPS98]. Nuclear [HRV99]. NULL
[GB98]. Number
[Ac98a, Ag99a, ARV99a, ARV99b, BG98,
BGM97a, BGM97b, Bir98, Bor95, Buc91a,
BP97c, De98d, JK99, KSW98d, KSF99,
Koh94, LLM90, LLL93, Loz90, Mat96b,
Miy93c, PG90, ROT94, Sch90c, Sch97c,
Shp99b, WI99, BMxx, Bou94, CS97c, CB96,
Cor99, CDE+96, Cus96, CS96c, Gor93b,
Jenxx, Ka93b, Kos99, KK98, Lag90,
LLMP93, McC90b, Me92, O’C94, Pom90a,
Pom94, PP92a, PP92b, PP95b, PP95a,
PNR99, Rev91, Shp99a, S999, SBB99,
Tat98, Tat99, TSY98, YT96]. Numbers
[Cha93, Ell98, Gut98b, Kra99, Mac94,
MSN99, Pin97, ST91, GK95a, PGCS96,
Yan95]. Numerical [She92e]. Nuts [Net98].
Nyberg [NMV98]. Nyberg-Rueppel
[NMV98].
Oakland [IEE92c, IEE93b, IEE94d, IEE95b,
IEE97i, USE96d, USE96b]. Oakley [CH97a].
OB [Lut98]. OBDD [GS99a]. Oberwolfach
[BFS92a, BFS92b]. Object
[AK94, BDPS95, BDPS97, BHJM99,
CIO98, DSB99, EKL99, KM98a, ON99,
PD99a, STSW99, SG99b, vDS97, Wat99,
vS97, BB96, GVG97a, LS98a, TCH+91].
Object-Instance-Based [BDPS95].
Object-Oriented
[AKF94, BDPSNG95, BDPSNG97, DSB99, Ou99, PD99a, SG99b, BG97a]. **Objects** [CK95, GS98, HHW99, Kem99, YY99a].

**Oblivious** [Bla96c, DF99, HHY93, Mic97, NP99, Bea93, BM90, BR96b, DOR99, GO96a, JY96] .

**Observation** [MM99c, Mur99, Bih98b]. **Observations** [BBDR99, WKS99]. **Observers** [CP93, DT98a, NT99].

**Obstacle** [ZW99]. **Obstacle-avoiding** [ZW99].

Obtained [EvH93]. **Obtaining** [CLHL98].

**Occam** [GN95b]. **Ochrono** [Sch95e].

**October** [Ano93d, Ano93g, Ano96a, Cha91, FM91, IEE93a, IEE94a, IEE96a, IEE96d, IEE97f, IEE97h, IEE97j, IEE98f, IEE99a, NIS92, Oht96, OdP98, TV94, USE93, USE96a, Ame95]. **Odds** [McC90b].

**ODEs** [Ruo94].

**ODMG** [Wat99]. **OECD** [Org98a].

**Off** [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AG95, Ano94h, Ano96l, Mao98, Riv98c, VNM99].

**Off-Line** [Bra95b, DT98a, Tra99, Mao98, VNM99]. **Offer** [Mar96]. **Offers** [Gar97a, GC97].

**Office** [Fuc99, U997a, Uni96c]. **Official** [Zim95a].

**offs** [BFS96, BMS96, NMVR95a, NMVR95b]. **Oil** [KS98d, KPG99]. **OK** [Gar98b]. **Okamoto** [Hwa92a, MS98a].

**Okamoto-Tanaka** [MS98a]. Old [IEE94a, Mar96]. **Olympiad** [DDJ98b]. **Olympic** [Myc96].

**Omnidirectional** [PJ99, SKIT99]. **Omura** [HWB93]. **On-Line** [Cac95a, Cac95b, CDF95, E199, EGM90, EGM96, PUF99, SS99e, SS99f, Na97].

**On-Line/Off-Line** [EGM90, EGM96]. **One** [BJ97, BHS98b, BHS98a, BD94, BHH99, BM94a, BM96a, BM96b, BM96c, BKK98, BP97c, DGV93, DDP90, Fii95, Gys96, HILL99, HT99, HYL79, Mero9a, MSN99, New98, Riv98c, Roe94, Rom90b, Sch91b, Sch95a, TOU94, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k, Zhe90, Ano97d, BD95a, BK98f, CB96, DI99, Dob98, Hwa92a, IEE92d, MB94b, MZI98, Roe95, Sim98c, Ste95, Sze98, Tao94, Tsu92b, Tsu92a, Wer93a, Wer93b, ZPS93, MAM95]. **One-Bit** [MS99]. **one-hot** [CB96].

**One-Key** [Gys96, Tao94]. **one-round** [Wer93a, Wer93b]. **One-Step** [Ano97d].

**One-Time** [BM96a, Fl95, BM96b, BM96c, MAM95]. **One-Time-Password** [New98]. **One-Way** [BJ97, BMDM94, BM94a, BKK98, DGV93, DDP90, Roe94, Sch91b, TOU94, Zhe90, BHH99, HILL99, HYL79, Rom90b, BK98f, DI99, Dob98, Hwa92a, MZI98, Sim98c, Sze98, Tsu92b, Tsu92a, ZPS93].

**One-Wayness** [HT99]. **Onion** [RSG98, SG97]. **Online** [FL99b, Jam98, MGL+98, MB99a]. Only [BK98d, TOU94, MRS99]. **Ontario** [GS94b, IEE96d, IJL93, TM99].

**Ontology** [CHLT99]. **Ontology-Driven** [CHLT99]. **Ontology** [ADBB99, Gua99, Mec99].

**Oorschot** [Sha99a]. **Op** [MGL+98]. **Op-Ed** [MGL-98]. **Open** [AT99, BCE+94, Con99a, DMVC99, GS97, HWH98, Luc98b, Muf93, Hor94, SY96b, Sta96b, Con98, Dra99].

**OpenBSD** [dRHG+99]. **OpenCard** [DT98b, HH99]. **OpenGL** [DDJ98e, DDJ98f]. **Opening** [Bur94c].

**OpenPGP** [CDFT98]. **Operand** [SS98h].

**Operating** [CH94b, IEE93a, IEE99b, Mar98a, WABL94, AHdJ97, FM98b, SG96b, WABL93].

**Operation** [Ano96c, Bih94b, Bih98a, Bih99b, HP99a, HP99b, Wag98b, Bih95a, Glaa98b, Mon96, Pos92]. **Operational** [Car97b, RZ99]. **Operations** [DBVD96, Zie97, Win93]. **Operator** [Uni94a, BP98c]. **operators** [BP98b].

**Ophthalmical** [FCD98]. **OPIE** [MAM95]. **Opolizing** [YY98d].

**Opportunistic** [BRW99]. **Opportunities** [MBB98].

**Optical** [DH98a, FVEA99, HLMP96, Tow98, van96, van97b]. **Optimal** [BP98a, BR94b, BR95a, BJY97, BM96b,
BM96c, Car94, FGMY97a, HKS97a, HKS97b, LC99, PRS99, PLWSN99, ST94, SW97a, SW97b, Tay95, BJQ97, DP94, LL93b.

Optimality [Mas99b]. optimally [CGS97].

Optimisation [CD98a, FCD98]. Optimised [RC94a, RC94b]. Optimising [DN95b].

Optimistic [ASW98, GJM99a, GJM99b].

Optimization [ARK99, DDNM98, RP98]. Optimized [EPR99b, EPR99a, SL99]. Optimizing [Cla97, MS99b].

Optimum [OK96b].

Option [Dra99, Bor93c]. options [Ros94, Sta97c].

Oracle [Ano95k, GHR99, Ano95k, Got99, MSO96].

Oracle [HTY99, MW96c, MW96b, BR97b, Bra90d].

Orange [IEE96f].

Order [CH98, KW99, KS97b, Mil96a, MSK98, SMK98a, SVxW91, Boy97, Gol96a, GK95b, Jak99a, ML98, Mat95, She95c, VZ97].

ordering [Sab94]. Orders [BBT94, HJPT98b, KS97a, GvP98, HJPT98a].

Ordinary [Miy93b].

Oregon [Auc98, USE90]. Organizational [FY99]. organized [Far93]. Organizing [OMV98].

P [YT96, MS90b]. P-1 [MS90b]. P. [IEE97c]. P0k [Tak98a]. P1363 [Ano96k, Ana97y, Ana97z, Ana98i, Kal97a].

PA [AR97]. Pacific [Unf98e, Win93].

Pacifio [I298]. Package [BMS99, Riv97c, Sta94a]. packet [TY94].


PalmPilot [DB99].

Palo [ACM98a, IEE98a, IEE98b].

Panama [DC98a, DC98b]. Panel.

Panel [ADKN90, CFGS99, CPOR97, EQ98].

Paper [BKF99, Cha93, CM99c, Fuc99, Mer90b, YST99a, Gol99c]. Papers

SB97, Ana95l, Cha91, CFG96, RRP97, CW94].


Parallelisation [FCD98].

Parallelism [BS91h, Cla99, PP92b, Pos93, Pos98].

Parallelization [BFVD99, RG99].

SKW^+99b, She92c, Sma99, Sut99, Tou95, VNW94, Wie98b, Nor95b, NO96, SS98.

**Performer** [KS98b]. **Period** [RH99].

**Periodic** [Mun91a, Mun91b, Abe98b].

**periods** [GvP98].

**Perl** [DDJ98a].

**Permit** [Joh94].

**Permits** [Gar97b].

**Permutation** [BM92, BS90b, CT99a, EM93, HMvT94, Pat99c, Pat99, CSV94, HT95, O'C95, Pat91b, Por93, Zan90].

**Permutations** [BY93a, DW94, FJRS96, SPS97, CCZ98, Pat91a, Pie93, Sha94, SMK98b].

**Permuted** [BCCG93, KM99b].

**perpetual** [HJKY95].

**Persistence** [DL99].

**Person** [BBDF97, Ble98b, DLF97, DMFB97, WKHG97, BCB97].

**Personal** [Ano97s, BE90, Bar05, Cae96b, EHMS99, Gar97b, Hamxx, Los97, Los98, RSA99a, Rivxx, Cra96, Mil95, Wil93a].

**Personalized** [GGMM97].

**Perspective** [Bre99, Cae96a, CM99b, Orl96, Swi97, UFC94].

**Perspectives** [GO96c, Des98a, DR98b, Ano95c].

**pertaining** [Cha94b]. **Perugia** [De 95].

**pessimistic** [Kru98]. **Petard** [WG97].

**Peter** [vdWS97, vS97]. **Petho** [La92].

**Petre** [CFK91]. **Petri** [DR98b, KA99, LL97a, NT93, YK98]. **PGM** [HMvT94, MMT90, MM90a, MM90b].

**PGP** [Ano97s, ASZ96, Elk96, End97, Gar95, GM95a, Gar98c, Joh96, Kar96, Ken95, MR98, MLLG95, Ros95a, Ros95b, Ros96a, Ros96b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, SA95, Sta94a, Sta95a, Sta95b, WCS95, WT99, Zim95a, Zim95b].

**PGPmail** [Pre97b, Pre97c]. **Phantomic** [Lip93].

**Phase** [BGV93, Chi92, ODB96, HY95].

**Phases** [Tou92]. **Phil** [Ros95a, Ros96c, Ros97a].

**Philadelphia** [ACM96b, AR97, CH96]. **Philosophical** [Mos98].

**Phone** [Gar97a]. **Phones** [MB99a].

**Photographic** [Fri93].

**Physical** [GBC93, Oka93a, Sal98]. **Physically** [Wal90].

**physics** [Sch90c, Sch97c].

**Picard** [BSB97].

**Picking** [Way95].

**Picture** [GDD97, MT94, DDM98, YEA98].

**pictures** [ONT98]. **Piecewise** [YMWP99].

**PIL** [Sch99k]. **PIL/SETHEO** [Sch99k].

**piling** [HKM95]. **piling-up** [HKM95].

**Piloting** [KW92]. **Pinyin** [OSH91].

**Pioneer** [Pin98]. **Pioneers** [Unixxb, Riv98c].

**Pipelined** [Pos93]. **Pirates** [Wal94].

**Pkg** [Sch99a, Ano96f, Kal97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, Nys99, RSA93d, RSA93b, RSA93c, RSA93e, RSA93a, RSA99b, RSA99a].

**PKC** [IZ98]. **PKC'99** [IZ99].

**PKCS** [Ano95j, Ano96k, Ano97y, Ano98i, Ble98a, Kal97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, Nys99, RSA93d, RSA93b, RSA93c, RSA93e, RSA93a, RSA99b, RSA99a].

**PKCY** [XW97]. **PKZIP** [BK95a].

**Place** [DR94c, Des98a, DR98b, Ano95c].

**Placement** [Des98a, DR98b].

**Planar** [LE99].

**plane** [ZW99]. **Planet** [Sta97c, Fro96].

**planning** [Mas97]. **Plants** [PRAM98].

**Plasma** [BVFD99]. **plastic** [Gau97].

**platform** [Ale98, LS98a, Way98].

**platforms** [Ril96].

**Play** [Bea97b, DDJ98d, IKM99].

**Players** [IKM99].

**Playing** [Sv98, SV99a, SV99b].

**Plays** [Lea90].

**Pleasures** [Kör96].

**Plug** [Bea97b].

**Pluggable** [IH98, Mor97].

**plugs** [GTGW94].

**Plus** [Dav95]. **plutonium** [Ano96m].

**PMLP** [BPBV99]. **Pocono** [IE97e].

**Poe** [Sha99a, Ros97c].

**poems** [Lea90].

**Point** [FF99, Gar97b, Lau98, STP93, Ken95, Shp99a, SM98a].

**point-&-click** [Ken95].

**Point-to-Point** [SM98a].

**points** [KK98, MVZ93].

**Poker** [KKOT91].

**polities** [HK99b].

**Policy** [ACM94b, And96a, Ano96f, Bar93a, Bar93b, CPOR97, Ell99, Gir99, Hat96, Wai95, Aus96, Akr97, Ban94, Bro96, Dum96, DG96, Ele99, HAHH94, Hof95, LKB+94, Rot95a, Tas98, Wad98, Zaj97].

**Polish** [Blo98b, Blo98c].

**Politics**
IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, Ken93, KFJP96, Lin88a, Lin89a, Lin93a, Lut98, MW97, Mjo93, NKP99, Par98c, SY96a, SYMI98, SB97, SG96a, Sta94a, Tho96, Tra99, Uni98a, Uni98i, Ban94, Bro96, CM95, Car94, Cha92a, CK93, Cli99, Dom96, HM96, JMLW94, Mar95b, Mei96a, Mil95, Rot95a, Smi94a, Sta95b, Uni97c, VPM97, Zim96a, Zim96b, Gar98c, Ros97a, SS97a, SS97b, Sta94a, Sta95a, Zeg93.

Privacy-Protection [Tra99].

Private [BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, Me93, RSA93c, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts'90, Wil93b, ZG96].

Private-Key [HR90, Mv93, RSA93e, DS90a, SS98b].

Privilege [ECM96].

Prize [GC97, Pin98].

PRO [Ano97r, Gar98c].

Proactive [CHN97, FGM97b, HJKY95, HJJ+xx, IBMxx, Jar96, Rab98, BCR98, FGMY97a].

Probabilistic [Jak98, JO97, SF97, Sch91b, Tou93, Goli99a, GO95, HK90, Imp92, Lon91, TX89].

probabilities [Lew92].

Probability [BDG99, Gol96b, Koh99, TY94, A196, MHHMW98, MA96b, WM93].

Probable [BD93, NK93, DLP93, Graxx].

Problem [Bon98b, Bon98a, BN96, CS98a, Cha90, DDD99, DJL93, GO96c, HM98, KM99b, KR99b, MT99b, NS99b, OMV98, Per99, RS99b, CP995, HY93b, HI97, HM97b, HMP95, LC97b, Mas97, McC90a, NR95, OA99, MS96].

Problem-Solving [Per99].

Problems [AA93, BD95a, Bra90a, GGH97b, KRS99, MC92, Po99, Smi90, AP993, Bea92, BFKLO4, FR95a, HC95a, IEE97e, Lew92].

Procedure [Ada97a].

Procedures [Hig97b, Lin93a, Lee95, Lin88a, Lin93a].

Proceeding [BPR99].

Proceedings [ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, Ano95l, Ano98f, Bri92, Bri93, Com96, GN95b, IEE95a, IEE91, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96d, IEE97a, IEE97j, IEE97k, IEE97l, IEE97m, MO98, Nat99b, OW95, PSN95a, Pat95, Shi93b, SL93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96c, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94d, BHH97c, B+96b, BGGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fum97, Gol90b, HOQ97, Hir97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, KG93, Kni99c, KP99b, KK99b, Kra98, LOX99, LM98a, LW96, Lom97].

proceedings [MV91, Nyb98, ODP98, Pre95a, QV90, QG95, Q+98, Rue93, S93, Sp95, Ste99b, TM99, TV94, T+98, TV92, USE90, USE98d, VPM97, Vau98e, Wat91, Wie99, Wol93b, Yuan92, vWN99, ACM93b, CH96, Ckr99b, IEE94e, Sti94, Wal99a, ECB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fei91, Gol96d, GQ95, GS94b, He94, IRM93, Kal97a, Kol96, Mau96b, PSN95b, SP90].

Process [AMP94, Kn99a, Rob98a, RS99c, YT96, CWM+91].

Processes [Gar98b, Bea92].

Processing [Ano97h, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97d, IEE97j, IEE97k, IN99, KV99, LMP99, LW96, Pin98, Pit95, Ano92a, DO99, DF97, Man98, Sab94, T+98, Whi90].

Processor [Gar98a, RB99, SW97a, SW97b, She92e, Sut99, VVDJ90, Von92a, Von92b, DQ96, She92c].

Processor-efficient [Von92a, Von92b].

Processors [Cla97, KK99a, She92e, BS95c, MHPS96, NM96a].

Proctoring [SKW96].

Prodigy [CFK+91].

produced [SSI97a, SS97b].

Product [GO96c, KSW98a, KSW98b, KSH98c, GN95a, SS98b, Ano94h].

Products [Ano97r, Ano97s, Cha94b, Cli97, Los97, U97b].
Professor [Swi97]. Profile
[HFPS99, MM90a, MK92]. Program
[BDFM99, FGY96a, LBMC94, FGY96b, LS98a, Pre97b, Pre97c, Uni95a]. Programmable
[Bre99, DDJ98a, Jol95, Ste94b, vdWS97, vS97]. Programmers
[Gar97c, Joh97a, Joh97b]. Programming
[IBM93, BGS96, CO98, Eri97a, JDK+91, Ste90a, Ste90b, ACM99a, Gre94, GA98, LS98a, OA99, Sab94, vWN99]. Programs
[BK95c, DRR95, SG95, SHK99b, WB95, Zwi98, B+96b, DFHR91]. Progress
[Ano96k, Ano97z, BDI+96, KSB96b, Wol93b, Wol93a]. Progressions
[MP99]. Project
[BPBV99, IBMxx, GH96, Man98, DS90b, RC99]. PROMIS [SSCP99]. Promise
[Law98, Los97, Mar96]. promises [Way93b]. Promotes [GO96c]. PROMS
[IEE98e]. PROMS-MmNet [IEE98e]. Proof
[Bol98a, Bol98b, CD99, CDS94, FO091, GMW91, GK96, NMV99, RS91, Zhe95b]. Proof-Based
[Bol98a, Bol98b]. Proofs
[BG90, BG93, BD91, CD98b, DFKN93, FS97b, GMW91, GO93, JMS196, CDP95, DP94, Gol99a, PS96d, Sak97]. Propagation
[GPR98, SG99b, SZZ95c]. Properties
[Boy99, Con99b, KA99, MM90b, MS91, OK98, OS98, Tou93, VW98, WW98b, Zie97, BHHRR99, CDG95, FSS94, KSB96a, Kob91a, PS93a, XZZ97]. Property [CFGS99, DL99, LQR98, SY99, Uni97b, Ale98, BS95c]. Proposal
[ABK98b, ABK98c, ABK98a, BAK98, D98a, KR94a, LM91b, Cli99, LM91a, RHAl92, RSS98, Ban94]. Proposals
[DAe99, VvT97]. Propose
[Gar98b]. Proposed
[CP91, Lea99, LL98, Nat92a, Riv93c, SB93, Wag98b, CJM96, Gua90]. Proposes
[SVB99]. Protect
[Sch94i, Sta95b, Cli99, KR96b, Way93b]. Protected [CH94b, DY91f]. Protecting
[BO96a, Ble98b, Des90a, EHMS99, GMDS98, KRJ98, Lut98, Mar95b, MW98b, PT95, SYMI98, Tra99, VP99]. Protection
[BGG95, CHN97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LQRS98, LvdLB96, LvdLL97, LML98, Per97, Smi90, Uni97a, Uni98i, ZK95, ZK96, Ale98, BBCP97, BBCP98a, BOD95, CPO+98, CHO+98, Cli99, DFHR91, GO96a, Ibb97, OP+99, RP94, RKDB96, SY96a, Sta94a, Tv92, TSN93, Uni97c, YE+A+98, FT95]. protections [HPA99]. protest [Ano97-30]. Protocol
[ATAV98, Ano95a, BWM99b, BV98b, Bra95a, Bra96, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JMP+98, JC97, Kas96, KS98a, KS98b, Kra99, Kum98, Low96, Man94, MW99, Mey96, Moe92, NS98b, NS98c, OM93, RS96a, RS98b, SN98a, SH97, SM98a, SM95a, Sim96b, SM96, SM98b, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CTSS, Des96b, Ev993, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS89f, SK97, Sim94b, TH99, WS97, WL94, Zhe95a, GM93a, Sar97]. Protocols
[AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BGH+91, BWM98, BWM99a, BCM93b, Ble98a, Bol98a, Bol98b, BDL97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dan99a, DGT96, DQ93, DS97d, Fei93, Fei96, FBS97, Fum98b, GM93a, Geh95, GS97, GMV98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IEE98e, KKOT91, KY92, KS97c, LYH93, LL97a, LH96, LL95a, LS92, LM96, MB94a, MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, SI93a, Sch94g, Sch96a, Sch94h, Sch99k, SSP90, Tou91, Tou93, AN94, AG97b, AG97c, AG97a, Aa99, ABC+98, BDHJ97, BH93, BCK98, BGH+95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, CJ95, Dan97, Fei99, Hor98, HLL+95, JW01, LY93, LHW99, LL95b,
Lom97, Man95, Mas97, MILY93, Mea95, MW98c, NT93, PS98c, PS98e, PS98f.

protocols [Pau98, PW93a, PKM97, SSG99, Syv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].

Prototypes [Pau98, PW93a, PKM97, SSG99, Syv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].

Prototyping [AKP99].

Provable [Bel99, CT99a, Mat96a, Mih94, SZ96, Vau98b, BOGG+90, Mo98].

Provably [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, Man91d, Oka93b, PS96c, Sh96, ZMI90, BH93, Dam94a, FO98, Go90c, NY90, PSW95].

Provable-Secure [DY90, DY91d, DY91b, Mau91d].

prove [Zha96].

proven [DS93, Lea90].

Prover [DY91a, GPSV98, HB99, DY91c, DFKN93].

provers [JY96, Ped91a].

Provide [BDR+96, SA95].

Provider [Tre99].

provides [MHMW98].

proving [Bos90, DR94c, DE99, FK99, DF91b].

provisions [CL97, UU97b].

proxies [LC94].

Proxy [GP99, Jak99c, LHW98, Zha98, BBS98b].

PRPs [HWKS98a, HWKS98b].

Prudent [AN94].

Pruning [AP94].

Pseudo [BG98, BGM97a, BGM97b, Imp92, MS95f, NR98, PS98b, Bou94, TSY98].

pseudo-aléatoire [Bou94].

Pseudo-Random [BG98, BGM97a, BGM97b, MS95f, NR98, Imp92].

Pseudonymous [GGK+99].

Pseudonyms [KRJ98, Mjo93].

Pseudorandom [ARV99a, ARV99b, BCK96b, BCK96c, BGK99, EM93, HILL99, KSW98d, KS99, Lag90, Mac94, Pat91a, Siu99, ZYWR91, BGR95, Kos99, Pat91b, Rev91].

Pseudorandomness [Kob99, Lub96, LLG10, BCK9x, GOL99a, MM95].

psychoacoustic [Til98].

Psychovisual [DM98].

PTY [LT98].

PTY-Marks [LT98].

PUB [Nat95, Nat99a, FIP93b, NIS93b].

Public [ANS97, ANS98b, Acc97, AKP96, AN95, IBM93, Ano96m, Ano99f, Ano99h, AA93, BP98a, BI95, BDHJ98, BDG98, BCE94, Bec99, BC95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BFK99, Ble97, BF99c, BS94, CC99b, CG99, CJS91, CL97b, CS98b, CRA98, Cus97, DDJ98b, Dam91b, Dav96, De93c, DP98e, Dif90, Eil99, FY95a, FY98a, FYM99, FGLP96a, FGLP96b, FO99a, GHT90, Gal96, Gar96b, Gib91, Gib96, Git91, GGH97b, GH99, HK99a, HGS98, HP99a, HY93b, HMY93, HL93b, HJJ+xx, Hes97, HPS98, HFP99, IZ98, IZ99, Ise90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKOT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Man93a, Mat97a, Men93, MM96b, Mic93a, Mic93b, MM98a, MM98b, NS97a, NY90, Nec91, Nec96, NS99a].

Public [Od94b, Oka94, OU98a, Ox91a, PSR97, Pale99d, Pat95, Pin97, Poi99, RSA94, RCM99, Rud91, Sal90, Sal96, DP91, Sas99a, SE96, She94d, Smi93b, ST91, Sun98a, Sut99, TAP90, VSH97, wQ91b, We98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zim96b, dW91a, vO91b, AA95, AD97, AD99, Ano90, ASD99, Bao94, BI94, BD98a, BS97, BS91a, Ben94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cus95, DW92, Dam96, Den90, DQV96, Dhe98, DN95b, ES97, FGM97a, GH96, Gih95, He92, HFW96, HJJ+97, JM96a, Jar96, Jon90, KASH90, KM99a, Kir95, KM99d, Kos99, LG97, Las92, LM93, Lee95, LC96a, LM94a, LZ90, LZ91a, LD94, LCL95, Lon91, Lon92, Low95, MI90, Man91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rae90, Roe99, SW95a, Sch92c, Sha95a, She96a].

Public [She92c, SM90, SS95b, SS95c, Sta94a, Sta95a, Sun91a, Tab94, TCC97, TC99b, TC99a, Tb99, Ven90, Wan92b, Wil93b, Xie92, Xie93, XLP99, XW97, Yu92, Zha91, vO92, vT90, BFS92b, HML+98].

Public-Key [AKP96, Ano99f, Ano99h, AA93, BP98a, BHSV98b, BHSV98a, BDPR98, Ber97c,
BMS94, BPK99, BFK99, CC99b, CJ91, Cra98, Cus97, DP98c, Dif90, FY99, FO99a, GHY90, GGH97b, HK99a, HGS98, HP98a, HMY93, Hes97, Iss90, Kal99, KM99c, KT91a, KMOV91, LM94b, Low96, MY91, Mic93a, Mic93b, NS97a, Oka94, OU98a, vO91a, PSR97, Pai99d, DP91, Sas99a, ST91, Sun98a, Wie98b, Yam98b, YST99a, YST99b, Ano96m, BFS92a, FGLP96a, FGLP96b, GH99, HY93b, NY90, Nec91, Sal90, Sal96, Smi93b, Yam98a, AD97, AD99, BKP97a, CC99a, Cle96, Cra97, DV96, Dhe98, DN95b, ES97, FGMY97a, KASH90, KM99a, KM99d, LM94a, LZ91a, LDW94, LCI95, Lou92, Low95, Man91b, MY93b, NM96a, Ole95, SW95a, Sch92c, Sha95a, SS95b, T99b, Tze99, Ven92, Wan92b, XLP99, Yu92, v990. Public-key [BFS92b]. Public-Key-Based [Nec96, TAP90]. Public-Randomness [DP91]. Publication [Nat93b, HV98, Nat92b, Nat93a, Nat94a]. Publicly [Mao97, Sch99i, Sta96a, VBD99, FO98]. Published [Ano97c, Ano97z]. Publish [Ano95j]. Pudding [KS97a]. Purchaser [RS99a]. Purple [Cur98]. Purpose [KP93, Sut99, Sch91b, Vu95]. purposes [Cli99]. pursuant [Cli97, U97b]. Push [Eri97b]. Pushes [Bar97]. Putting [DDJ98c]. puzzle [Bar92b, Gre90, WSFC99]. PVM [BSN95]. PVS [DS97d].


KR94c, Nis96, DP91, Sot98, SB99, BGS95.


Rapid [KM93, GTS90]. Rate [BDGV93, BS91g, LD98, St93a, Bla94a, BDGV96, KL95b, MHW98]. Rates [HK97, HR90]. Rational [KG95, Koz96, ST91]. raw [HG96].

Ray [Aga92, BALS99]. RBF [WKHG97]. RC2 [Ano97c, KSW97a, KSW97b, KRR98, Riv98a]. RC4 [MT99c]. RC4-like [MT99c].

RC5 [Ano97z, BR96a, BK98e, BPV99, GPO98a, GPO98b, KY95b, KY95a, KY97, KY98, KYYx, KM96b, MAO96, Riv95c, Riv95b, Riv95d, Sel98a, Yin97]. RC5-CBC [BR96a]. RC5-CBC-Pad [BR96a].

RC5-CTS [BR96a]. RC5P [KSW99b, KSW99c].

Re [FL99b, Yak99c, AGY95a, Bur98b, HG97d]. re-encoding [HG97d]. Re-encryption [Yak99c]. Re-issuance [FL99b]. re-sharing [AG99a]. Reachability [DR94c].

Reached [Lea99]. Reaches [MB99a].

Reaching [Gar94, HH94]. React [Par98c].

Reaction [HGS98]. Reactive [MKL99].

Reactor [HRVV99]. Read [Sta97b, Cohl96, LF97]. Reading [Eri97b].


Real-Quadratic [BBT94, BMT96].


Really [Ano93c, DDJ98a, Ritt99, Sim90a]. Realms [ARH95]. Reapplication [Sch99c].

Reasoner [MD99]. Reasoning [AG97a, BMC95, DSB95, KM99c, MR95a, PK99, Var99b, Ger99b]. reasons [Ril96].

Reassessing [Neu95]. Reassure [MB99a].


Rechnergestützte [MPS94]. Recipes [FBS97]. Recipient [WP90, Wal90, WK97].

Recognition [HCD99, HA96, WD99b]. Recognizer [WB94]. Recognizes [Pin98]. Recommendations [Ano95m, Kal98g].

Reconciliation [BS94, CM95].

Reconfigurable [BP99b, PJB90].

Reconstruct [HD96a]. Reconstruction [BC95b, BD98e, LH95]. Record [Har90, LCL92, Cha99b, CDEH+96, IEE96f, IEE98b, JLM+94]. Record-Oriented [LCL92]. Recoverable [YY99b, YY98c].

recovering [HCC98]. Recently [Wag98b]. Recently-Proposed [Wag98b].


Redistribution [MSNW99]. redistributors [DF98]. REDOC [Nor95a, BS91f, CW91b, GN95c].

REDOC-II [BS91f]. Reduce [Hig97b, SVWM95]. Reduced [BBS99a, BKR97, MT99a, BBS98a, PNR94].

Reducing [DS98b, JQ98b]. Reduction [CTT94, GGH97b, BK98g, PP92a, PP95b, PP95a, SH95a, SH95b, SOB98]. Reductions [Fis98, HSSI99, OU98b]. Redundancy [GM97, Mis97]. redundant [SOB98, TY92].

Redux [DDJ98c]. Reengineering [AMP94].

Reference [Bar96b, CDF95, KMKH99, Pre97c].

refined [HWF96]. Refinement
Reflective [BCCD99, DL99, KHB99].

Regional [ADEDS99].

Regional [BCCD99, DL99, KHB99].

Refunds [Hir93].

Regarding [Roh99, CJRR99b].

Regenerating [Jan95].

Register [CS96b, CS97b, GN95a, GM91].

Registers [GO96b, Gol94, GO95, GK95a].

Registration [Bal97, TOH98].

Registry [PKA+98].

Reglementierung [MPS94].

Regulated [Way93].

Regulating [Riv98c].

regulation [Koo97, Ram92].

regulations [Cha94b, Cli97, UU97b].

Reinventing [Yuv97].

Rejected [Eri97b].

Rejects [Gar97a, GC97].

Related-key [KSW97a, KSW97b].

Related-Message [Ber97c].

relating [Aus96].

Relation [BHSV98b, BHSV98a, SK98c, SK98b].

Relations [BDPR98, Jak98, NMV99, Uni98c, Tze99].

Relationship [GSO99, HT99, MW99, Oka93a, SSZ95c].

Relationships [Kem99, Len99b, RG95, SS95a, SG99b, SSZ95a, GK95a].

Release [Dam94b, Dam94a, DOR99, Sun91b, Zim96b].

Released [JJ99a].

Releases [Got99, Wor96].

Relevance [SS99d, Tra99].

relevant [HI94].

reliability [BHS93, HS96b, IEE94b].

Reliable [BF97a, BF99b, KM93, FD92].

Relinearization [KS99a].

Relying [ZM90, Sak97, Sch99e].

remainder [DiDP99, WW99].

Remark [CMTNY94, LHL94, FR94].

Remarks [BY92, GPSN97, Gro94, Gui97, Oht98, BBL95, LA98].

Remote [BLM94, FMM99, HS97, Hel98a, LC95, RRSW97a, RRSW97b, SK97c].

Remotely [BFN98b, Luc97, Luc99c, LW99, BFN98a].

Removing [LB98, RCM99].

repair [Zhe95a].

repeated [Syv93].

Replacement [Cap94, SN94].

Replay [OG97, YL97b].

Replicate [RB94].

Replicated [KB92].

Replicating [HS96b].

Replication [BLM94, Pit96b].

Reply [NC97, BMP+97b].

Report [Bra93a, BDI96, Dra98, EMMN98, Kru91, Nat99c, Par98c, PH91, RIP95a, RD99a, Tou95, Vau99d, Wor96, BFS92a, BP95b, Bur98a, KSB96b, NBD+99, Org98a, RIP95b, UU97a, Zer96a, Dan95, BFS92b].

Reports [Ano97a].

Repositories [CHLT99].

repository [HSK97].

Represent [MI99].

Representation [CK95, Ger99b, JKV99, LE99, NA95, PNFK95, TY92].

Representations [CF99].

Representatives [Chi97, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f, UU97b].

Representing [HL99].

Republic [Ste99b, vWN99, Hru98].

Repudiation [GP99].

Required [BGS95].

Requirement [Sill97a].

Requirements [Ano97b, BD92, Bel92, BC95c, FR95d, HJTW99, HH94, VW98, Com94c, MW98a, SM95b, UNU94].

Research [Ano99a, DDJ98c, Dam96, Des92, Des98c, DEQ92, Ele98, IEE92e, IEE93b, IEE94d, IEE98d, Jan99, Q+98, Rhe93, Wol93b, Ano97-30, Wol93a].

researching [Uni96a].

Resend [Ber97c].

Reserve [Ano97x].

Resharing [AGY95b].

Residue [KKOT91, PP92b, CB96, PP92a, PP95b, PP95a].

Residuosity [Pai99d, DDP94b].

resilience [FGMY97a].

Resilient [BGS94, BGS96, MS99b, RS98a, GHS93].

Resistance [BKPS93, Dae99, SY98, YT95a, YT95b, CL97b].

Resistant [Ano96, BDHJ98, EKK99, KK99a, KS97a, LA98, PGV91].

Resolution [ADD99, BLM99, CH97a].

Resolvable [KK95].

resolve [CMY97a].

Resolving [CMY97b, QN98b, ZL97].

resorting [PBBC97].

Resource [BCCD99].

Resource-Aware [BCCD99].

Resources [GI99, LBHM99, KS95].

Response [She92e, SB93].

Responses [RHAL92].
DL96, Dam96, Gua99, Mau93b, Sin98.
Role-based [JJ95]. Role-Centered [VC99].
ROLLING [PWU99]. ROM [Ano96i, GTGW94, Ros94, UFC94, Yuv97].
Roman [Has95]. Rome [Knu99c, Nat99b, Wol93a, Wol93b, DDJ98b].
ROMs [GTGW94, UFC94]. Ron [Riv93a, Riv95a, vdWS97, Woe97, vS97].
Roosevelt [Kah98c]. Root [Cop95c, JJ91].
Rooted [PB99a]. Rooted-Tree [PB99a].
Roots [Kob97]. Rosemont [IEE97g].
Rosenheim [Sha99a]. Rosser [Ole95].
Rotation [OP97, OP98]. Routers [DMVC99].
Routing [GRS96, RSG98, SGR97, CadHSV96]. rover [Bis90]. Royal [Far93, Tv92, Don98]. RPC [SSH93]. RSA [Ano94b, Ano95f, AA99, And93, Ano95d, Ano95e, Ano95a, Ano95j, Ano95m, Ano96b, Ano97e, Ano97f, Ano97g, Ano97u, Ano97v, Ano97a, Ano97w, Ano98a, Ano99a, BTD08, BQ95b, BQ95a, BR96c, BJ97, Ble98a, BF97b, BDF98, BV98c, BD99b, Bon99, Bra95e, Bri90b, BM94c, Cao99, CH97b, CH98, CB96, CLE99, CMNY94, CD91, Cle96, Cof97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, Cus97, Dav95, Dem94, DDLM94, DN95a, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FM97b, FM97b, FY98b, FR95b, GJKR96b, GKR97, GGOQ98, Gil99, GM97, GTS90, Gro94, GS99b, HN98, HWF96, Hor98, Hub91, HP94, IMI93a, IMI93b, JQ97, JQBD07, JQ98a, KR95c, Ka97a, Kahlb, KS98a, Kir95, Koc94, Koc96a, Koc95, Koc96b, Koy95, KOT95a, KOT95b, KKL96]. RSA [Len98, LHL94, LL95a, Lon91, MBB09, MLY93, Mau90, MWW98d, MWW98c, MSS98, Mis97, Mis98, MS99c, Mue99, Miul99, NS98b, NS98c, Oka98a, Oka98b, OSA91, PPKW97, PP90, PW93a, Poi99, PS98g, Rab98, RS98e, RSxx, SSI97a, SSI97b, Sam98, SKNO98a, SKNO98b, SS98, SCH94m, Sha95b, SV93, SH99, Sil97b, Sil97a, Smi93b, TY92, Tak97, Tak98a, Tak98b, T+99, TT99, VVDJ90, VNM99, Ven92, Ve97, Wal99c, Way98, Wie90b, Wie90a, Wir98, XL99, YW99, Zer96b, Zho94]. RSA-120 [DDLM94]. RSA-130 [Ano96b]. RSA-Based [CD96, GKK97, VNM99]. RSA-cryptosystem [Gro94]. RSA-implementation [PP90]. RSA-key [FMY98]. RSA-keys [SSI97a, SSI97b]. RSA-Like [JJ97]. RSA-Moduli [Mau90]. RSA-signatures [Ev92]. RSA-type [BI97, JQBD97, Tak97, Q98a, Koy95, KKL96]. RSAb [MPPS95]. RSAEuro [Bar96b]. RTD [KW92]. RTR [KV99]. Ruby [JS93a]. Ruepe [NM98]. Rule [PL94]. Rule-Based [PL94]. Ruling [Eri97b]. Run [DF91c]. Run-Time [DF91c]. Running [RH93]. Runtime [WF94]. Runtime-Tunable [WF94]. Russia [CW94].
Safeguarding [Beu94]. Safer [Hir93, BM97, CMKK98, KSW96, KSW99a, Kel99, Mas94, Mas99b, Van95]. Safety [Ane94c, DDJ99, Clh99, IEE94b]. Safford [Bur98b, Kru98]. Safer [Hir93, BM97, CMKK98, KSW96, KSW99a, Kel99, Mas94, Mas99b, Van95]. Safety [Ane94c, DDJ99, Clh99, IEE94b]. Safford [Bur98b, Kru98]. Saint [GQ95, QG95]. Saint-Malo [GQ95, QG95]. Sales [Gar97a]. Salient [CKLS96b]. Salt [Ude98]. Samos [OMV98]. Salesman [OMV98]. Salt [USE95b]. Samba [Bla98]. Same [Ude98]. Samplers [MV98]. Same [Ude98]. Santorini [IEE97c]. Saragossa [Mau96b]. Sardinas [MSS93]. SASL [Mye97, New98]. SAT [McH92]. Satellite [Ane99c, Gar97a, Gar98a, Lam99]. Satisfying [Kim93, Ces96, CS96c, O’C94, YT96]. Save [DF92]. Saving [Ame96b]. Says [Riv98c]. Scalable [Hei96b, IEE94e, Kh98b, L98, RG99, SL99, Goo96]. Scale [SA95, SS90, She92a, FO93, OP97, OP98]. Scaling [SA95]. SCALPS [DVG96]. Scanners [Mei98]. Scanning [CO98]. Scenario [Amp94]. Scene [SZT98a, SZT98b]. Scene-Based [SZT98a, SZT98b]. Scenes [BDC+95, MCD98a]. SCFS [IHR99]. Schedule [KSW96, KSW99a, Kel99, MM99c, Mur99, SKW98a, SKW99, WKS+99]. Scheduler [KT96]. Schedules [CDN98]. Scheduling [KP93, Por98, SJS98, Sha99b]. Schema [Pit96b]. Schemas [Wed99]. Scheme [Int91a, ADF98, BCG93, BM99a, BM99b, BF99c, Boy90, BY92, CT97, CK95, Cop94b, DQ94, DKK98, DN94, GHY90, GQW+91, HL93a, Hwa93, Hwa97, Iye91, IM93b, KKS97, KS98d, KMK99b, KR99b, LK96, LW91, LH94, LH93b, MS98, Mjy96, Mue99, Mi99, MV98, OOK91, O90, OFF93, Pat95, Pet98, PM99b, RGV97, Sch99i, Smi90, Ver95, ZL99, AW95, BD98a, CW97, CL98, CC95, CL98, CM98, CMT94, CGS97, FO093, FO98, GML94, GPS97, Guar, Har91, HZ93, HK90, HY95, HC96, HW98c, HCC98, IS99, IM89a, Jc98, JLM+94, Kuc92, LWC96, LLG90, MRS99, MS98a, MLA91, Mau91b, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SS98b, SVW95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WW95, vF93]. Schemes [AW94, BP97a, BC93a, BDPR98, BBDW96, BK94a, BK95b, BM96b, BM96c, BDG93, BDD+94, BFS96, BM99c, BV96, BD90, Bir90a, BS91g, BLLL98, BDB92, CS97a, CM99a, CD95, Dar99a, DWW90, DMPW98, D91e, vD95a, DFK99, DLR97, FDB93a, FY97, FO091, FO99b, GPS98, GP99, GS94a, HKS97a, HKS97b, IS91, JMO94, KPG99, Ki96, KMOV91, KOS+94, KOO95b, KOO95a, LHW98, MH96, Mis98, MWWW94, OK98, Oka93b, Pal93a, Pal98b, PM98, PS96c, PB99a, RS96e, dR94b, SK95, Sak96, SE96, Si93, Sim90b, Sim91, Sim94a, Ste94a, Sti93a, Sti98b, SW99b, SN99, YLD99, Zha98, AR99, BC95a, BR97b, BI93, BSDV93, BC95b, BCS96, BCDV96, BDG93, BMS96, BD97, BFS98, BD98a, BD98b, BDG99, Bur96, BM94c, CDGV91, CP95, CS94, CV94, DP96]. Schemes [DF93, DDB95a, DDB95b, Des99b, FDB93b, HY93a, HMP95, HCY96b, J93, Koy5, K95a, KO96, K97, LS98a, LC97a, LH95b, LHL95a, MS98b, MPS99, MTS97, Mu92, NR95, OK96a, OK97, OK95, Pad98, PS98a, PPKW97, Pf96c, PS96d, RD96a, RS96b, SI93b, Sha94, Sha95a, She92g, SW98, SW99a, SS94, SC97, TJ99, Tze99, VNM99, WAM904, ZHS94, ZI98, dR94a, vD95b]. Schernes [BBC93a]. Schnorr
[DBGV93, dR94b, dR94a]. Schoof
IKNY98]. school [Duf98]. Schools
DDJ98e, DDJ98f]. Schroeder
Low95, Low96]. Schussel [Pin98]. Schutz
FT95]. Schwierigkeit [Hor99].

Science [Ano93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97f, IEE98a, IEE99a, Ste91, Beu94, Sch90c, Sch97c, Shp99a, Sim92, WS96c]. Sciences [Ano95l, Tv92].

Scientific

Scientist [CHLT99, PH91, GTGW94, HW91].

Scots [Sin99]. Scott [Sha99a]. Scramble

Scraping [CN99]. ScriptEase [Ano97s]. Scripting

SDK [Ano97s]. SDNS [NH90]. SDSC

Secret [Bur96, CDGV91, Dam94a, Dwo91, Eil97, FO093, FO98, GM95b, GPSN97, Gre90, HNSM91, He93, HJKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, Jar96, JY98, Kahl96b, KO95a, KO96, KO97, LY93, LH95, Mei92, MPSV99, OK96a, OKT93, OK96b, OK95, Pad9b, Ped91b, Ped91e, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, Ve97, Wie90a, WS96c, Win99, Wir98, ZHS94, vD95b, van97a]. Secret-Ballot

Secret-Key [CFSY96, BT94].

secret-sharing [RD96a]. secret-sleuthing [WS96c]. Secretly [MT94]. Secrets

Section [Alv98c]. Secure

Secure [AHV98, AB96a, Ano93c, Ano93f, Ano95i, Ano99e, Ano99f, ATK97, AR99, Bal99. BQ95b, BQ95a, BMM99a, BMM99b, BR95b, BM99a, BM99b, BR91, BHK*99, BDHK93, BFS96, BS95b, BS98, BM94b, CG99, Car99, CG98, Cha90, CvhP91, CR91, CCR95, CKLS96b, CKLS96a, CKLS96c, CKLS97, CD95, CD96, CS98b, CDD+99, Cra99. Dam91b, Dam94b, DY90, DY91d, DY91f, FIP93b, FIRM90, FB97, FYM99, FH94, FO99b, GGMM97, GXY90, Gal96, Geh95, GJKR99, GHR99, Gut96, IOS94, Jac90a, Jac90b, JT97a, KRR95c, KM93, Kar96, KT96,
KSHW97, KSHW98, KS99a, Knu94a, KP97, Kon95, KBS97, KYDB98, LY93, Mar98a, Mau90, Mau91d, Mau97a, MW97, Mos98, NIS93b, Nat95, NS98b, NS98c, Oka93b, OU98a, Ped91d, PS96c, PB99a, PGV92, RR97, RS96a, RIP95a, SHH03, SSI98, SK94a.

Secure [SSSW98, Sas99a, Sch94a, SK98a, SK99, SM95a, S99, SM94, SH96, Smi93b, Str93a, Str93b, Tay95, WP90, WD99a, WK7, Web98, Yah94, YST99a, YST99b, ZM90, Zhe90, ZL99, Zol93, vHH97, BH93, Bea93, Bea96, BMS96, BP95b, Bow93, BM95, BD95b, CNST98, CGS97, CG05, Dam94a, Des90b, DS93, Des95, DVQ96, FO98, GGK99, GM95b, Gol90c, GBL94, HY98b, HY98a, HCG9a, Hwa93, HW98c, IS97, IKNY98, KC95, KSB96a, Lam99, Los97, MS98b, NY90, OK96b, Opp96, Ped91b, Ped91e, PWS95, Rh94, RRS98, Rom90b, Sar97, Sch92c, SKB97, Sim98c, Sin95, Sta97c, Ven92, YL97b, ANS97, Ano93j, Nat92b, Sta94b, Bou94a. secured [Way98]. Securely [RB94, DDFY94]. SecureNet [Ano97r]. Securing [Bhi96, Des95, Lin96a, RG95, SG98, VJ98, Ano95k, DL96]. sécurité [Sch98e]. Security [ACM93a, ACM94a, ACM97a, AKP96, ADDS91, ARH95, ABDV98, Ala97, And94a, Ano91a, Int91a, Ano92c, Ano93g, Ano95f, Ano95b, Ano96i, Ano96a, ??97?, Ano97e, Ano97f, Ano97g, Ano97a, Ano97w, Ano97x, Ano98a, Ano98b, Ano98h, Ano99a, Atk95b, AR98, Bal99, BCCG93, KSB96a, KAM94, BDP98, Bel99, BGK99, Bel92, Ber96b, BDR99, Ble97, BPRF99, Bov98a, Bov98b, Boy99, Bra90a, BK94b, BNP99, Com96, Com94c, CM97a, CH94a, CHN97, CGJ99, CS96a, CM97b, CT99a, Chr98, CGB+93, CNS99a, Cor99, CN99, CG05, DMW94, Dan95, DS98a, Dav95, DG95, De 93a, De 98a, DDK98, Des92, Di 99, DI99, Dwo95, ECM96, ElK96, EH96, FGS96, FS97b, FO99a, Fum93, Fum98b, GM93a, GMCF95, Gan96b, Gar97c, Gar96c, Gib96, Gir99, GH95, Gon98, GA98, Gut99, HHT93].

Security [HHT97, HP99a, HP99b, HSK97, HH94, HLMW93, HXMW94, Hur98, IBM9x, IE92a, IE92b, IE92c, IE93b, IE93c, IE94c, IE94d, IE95b, IE96c, IE97b, IE97i, ISO97, IH99a, JD91, JLO97, KY95a, KR96a, KY98, KTM+99, Kau93, KA98b, KM96a, Kle90, KRR98, KS97c, LOX99, LBMC94, LL94a, LL95a, Lom97, Luc97, Luc98a, Luc99a, Luc99b, MMST98, Mat96a, MSK99a, MW98d, MSS98, MM98a, Mue99, Muf93, MM98b, MiL99, Mye97, NIS92, Ng99, NK93, ODP98, OO98, OU98b, Opp97, PS98d, PS99c, Pff97, PS96d, PS98h, Rei92, RBr94, Rob93, Rob98a, Rog96, Rus90, Sch94m, Sch95c, Sch95d, SH97, Sch97a, SSv+98, Sch98f, SS99a, Sch98h, She97, SSP90, SS90, She92a, She92f, She93c, She93d, She94c, She96b, SK97d, Sun98a, Uni97a, Uni98a, Uni98e, Uni96b, UB97a, Uni98f, Uni98j, USE90]. Security [USE92b, USE93, USE95b, USE96c, USE96g, USE98d, USE99a, Van95a, VSH97, Van98b, Van99b, Van99c, Ved93, Ved98a, Ved98b, VVG93, Ver98a, WSC95, Wol98, Wol99, ZS93, ZFKP98, ZFK+98, vT94, Aba99, AFB95, Ano93d, Bec97, BR96c, BCK96c, BDJ97, BKR98a, BKR98b, BB99, B3+96a, Bet95c, BHH99, Boy98, Bro96, Com97, Cha95a, CP94, Cha99a, Cha99b, CJ95, CI99, CTXs9, Dam99b, DS90a, Den99, DEQ92, D98+, FF99, FM98b, Fra92, Gon92, Gru98, HH98, HK99b, HOQ97, HS96b, Hor94, HC95a, HC95b, HY95, HLLC96, IE94b, JT96, JT97b, JJ95, KY97, KG96, Kat97, KSB96b, KSB97, KW92, Kuh98, La92, LTT95, Lee95, LHW99, Len93, LCH95, MW94, Mar95b, MSN97, Mas97, Man91c, MKKW99, MF97, Me94, MW98c, Nor95b, PS99d, PS99a, PS99b, PS99e, PV93d, PV906].

security [PR98, Q98, Riv98c, Ros94, SSN98b, Sah99, Sch92a, SSM+97, SMD+99, She92c, Sta94a,
Sta99a, Sun98b, Tay90, Tho96, TY98b, TY98a, Tsu92c, Uni98d, Uni98k, VB96, VPM97, Ven90, WBDF97, Woe97, Xie92, XLP99, XZZ98, dVdVI98, van96, van97b, Chr99b, Far92, Uni98c, Uni98b, Uni97b.

Security-analysis [vT94].

Security-preserving [DI99]. See [Web98].

Seeing [JJ98b, JJ98a, Lut98].

Seek [Gar97b, SV99a, SV99b, SvS98]. Seeks [Gar97b, SV99a].


selectable [Gon95]. Selected [CW94, TM99, Cha91, CFG96]. Selecting [Bax97, CDF195].

Selection [Hub91, Len99a, PNFK95, BM94c, Fei99, UFC94]. Selections [DKK+98, Ers99]. Selective [GM97, HVH98, IS97]. selectively [WY93].

Self-Certified [Gir91, SG99a]. self-confident [Jan95].


Self-Reductions [Fis98]. Self-shrinking [MS95b, MS95a, Mih96]. Self-similarity [BCD98a, Sch90c, Sch97c]. Self-Study [Sch99d]. Self-synchronised [KI97].

Self-Synchronizing [Mau91a]. Semantic [BPR99, Mee99].

Semantics [DJH98, DE99, FL99a, RZ99, RS99c, SG99b, WK96, Ts’90].

Semiconductor [Gar97c]. Seminar [Ers95d].

Semiotics [Gog99]. Senate [Uni98g, Uni98i]. send [Way91].

Sender [WP90, Wai90]. senders [HW98c]. sendmail [BRW99]. Sense [Ame96b, CC98]. Sensitivity [LyD98].

Sensors [Fuc99]. Seoul [Ano93g].


Separating [MKKW99, Tou92].

September [Ano98f, D’98, ES98, FR95a, IEE96e, IEE97e, IEE97k, Kat97, LW96, Q’98, Spi95, TV94, T’98, Uni97a, Uni96b, Uni98j, Uni98k, USE92b, USE96a, USE98b, Gar98a].

seq [Cl97, UU97b]. Sequence [LYH93, GM91, LY93, MHMW98].

Sequences [DSV99, JQ97, MS94, Mun91a, Mun91b, PMP99, SB94, Bla94a, GN95a, Gol99c, KS96a, MK92]. sequential [LHW99]. ser [IPNdbbp991]. Serial [Si93a, SS99, Yor96].

Series [Ano95d, HEQ98, CJR98a, CJR98b]. Series-Parallel [HEQ98]. Serpent [ABK98c, ABK98b, ABK98a, BAK98].

servant [CWM+91]. serve [Sch93e]. Server [Ano97r, Ano97s, BQ95b, BQ95a, DL99, ECD’99, HS94, HCY96a, LYH93, LL95a, MW98d, NS98b, NS98c, Oh99, SvA’98, Wat99, Ano97d, BM94c, HS96b, Hor98, LY93, MW98c, PW93a, Sin95, Ts’90].

Server-Aided [BQ95b, BQ95a, HCY96a, LYH93, LL95a, MW98d, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a].

Server-Side [SV99a]. servers [Abe98a, AG95, CGM97b, GGK’99, Lee95, Ude98].

Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau93, MB99a, RRSW97a, RRSW97b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, Zha96, Ber96a, KN93].

Service-Level [MB99a]. Serviceability [WP90]. Services [ANS98b, Cas95, HVH98, RB94, VSH97, Ved98a, AA95, AC97, D89ob, Don98, KW92, PS99b, You7, Zer96a, AA95, Acc97]. ses [Bou94].

Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f, Uni98b, Uni97c, Uni95a, Uni98k].

Session-Layer [BB95c]. Sessioneer [AG95].

Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB98, Kra99]. sets [MT98].

settings [Car97c]. Settled [En97b].

Seventh [IEE99b, USE98d, ACM95].
Several [HGS98, LL95b, MH96, SiK93]. Severely [Gib95]. SG [Gue98b]. SHA [ANS97, MG98b, BGV97b, CJ98, MS95d, MS95e, Sta94b]. SHA-0 [CJ98]. SHA-1 [ANS97]. Shakespeare [Lea90]. Shallow [ACD94, WF94]. Shamir [She92g, Ada92, GGO98, Nac93, OOK91, OO93, The95]. Shamir-like [Nac93]. Shannon [Sga91a]. Shannon-theoretic [Sga91a]. Shape [HHD99]. shapes [Ger99b]. Share [BWM99b, Csi95, DDFY94, Sim90a]. Shared [BF97b, DHMR96, DF91a, iFiR90, HD96a, IS91, Lei90b, Mwb99, PS08g, Rz99, SN96, Sim90b, Sim91, Sim94a, WI99, Yl97b]. Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [BSN99, BDG99, CDGV91, OK95, ZHS94]. Sharing [AGY95b, BC93a, BC95b, Bbdw96, BK94a, BK95b, BDGV93, Bdd94, BM90c, BD90, Bri90a, BS91g, Cac95a, Cac95b, CG98, CT97, CK90, DDF94a, Dkk98, vDF95a, DLR97, FDB93a, Fgy96a, GJK96b, Gpsn98, Gpsn99, Hl93a, Hks97a, Hks97b, K96, Kras94a, KOS94, KoO95b, KoO95a, Lp99, Lcl92, Lh93b, Mei92, Msi95f, Ms99n, NW98, Ok98, Pai98a, Pai98b, Ped91d, Rab94, Rto94, Sch92b, Sch91, Sti93a, Agy95a, BC95a, Bl93, Bdv93, Bdv93, Bdv93, Bdv94, Bg95, Bdv96, Bg96, Bdh97, Bdv98, Bgd99, Bur96, CDGV91, Cmp97, Cmgw97, Df93, Ddb95a, Ddb95b, Dwo91, Fdb93b, Fgy96b, Fr95c, Ffo98, Gm95b, Gpsn97, Hjk95, Hwa92d, Hc96, Hlc99, Jm93, Jmo95a, Jmo95b, Jar96, Koa95a, Ko96, Koa97, Mao98, Mpsv99, Ok96a, Okt93, Ok96b, Ok95, Pad98, Ps98a, Pad91b, Ped91e, Rd96a]. sharing [Rd96b, Sta96a, Sc97, Tc91, Zhs94, Vd95b, Van97a, Kol95]. Shark [Rdp96, Wg97]. Shawn [Sha99a]. Shedding [HPG98, Yyh98]. Shelf [Hat96, Ag95]. Shell [Car99, Sch99a]. Shift [Go96b, Gol94, G95a, G91, Go95, Ps97]. shift-register [G95a]. Shifting [Lmb905]. Ship [NS98a, Rp98]. Ship-Board [NS98a]. Shipping [Ano95k]. Shooting [Aga92]. Shop [Ano97r]. Short [Kra94a, Ste94a, Wie90b, Ow96, Bc95a, Coh94, Har94, Joh99, Vw96, Vw97, Wie90a]. Shortage [Dj98a]. Should [Way93c, Yy96, Ano95c, Riv98c]. shrinking [Ms95a, Ms95b, Mi96]. Sis [NIS93b, Nat92b]. shu [Xt9W94]. SIAM [ ACM97b]. sicher [Ano97-29]. sicher [Hor99]. Side [Ksw98a, Ksw98b, KSW98c, Sva99b, Yy96]. sides [M99b]. Siege [Eh96]. Siegenthaler [Ms99b]. Siemens [Ano97-27, Bro97, Dav98c, Mac98, Se98b, Tj97]. Sieve [Llmp90, L993a, Per93, Cde96, Gor93b, Pm94]. sifrovani [Gar98c]. SIGACT [ACM99a]. SIGGRAPH [ACM99c, B96b]. Sight [Phi98]. SIGINT [My98]. Sign [M92, Gr97, Gr99, Web98, Br96c]. Signal [Iee97c, Iee97d, Iee97k, LW96, Pit95, She92e, T98]. Signalling [Lin98]. Signals [Ak99, Bth96, Dd98m, Mhw98]. Signature [Aa95, Acc97, Aw94, Int91a, Nis94, Ano96e, Ano97-29, Bp97a, Bm99a, Bm99b, Bm96b, Bm96c, Bra93a, Cs97a, Cm99a, Cg98, Ch98, Ck95, Cdf95, Cd95, Dmpw98, Dq94, D9y1e, Dn94, Fl99a, Fk98y98, Fom91, Foo91, Gp99, Gqw91, Hj97xx, Kks97, Ks98d, Kpg99, Kob98c, Kras, Lk96, Lhw98, Lk99, Lh94, Ll98, M94, M99a, Mer90b, Mer97, Mh96, Mss98, Ms98, Miy96, Mon93, Nat91, Nat92a, Nat94c, Nat94a, Nm959b, Na97, Nm98, Nm99, Nis93a, Off93, Ok93b, Pf94, P98, Ps96c, Pj99, Rgy97, Rdk98, Rv93c, Dr94b, Sc96a, Sch93b, Sch94e, Sk97a, Se96, Sim93, Sin98, Sb93, Snp99, Zha98, Zhe97b, Ztr99, Am95, Ame96a, Ark99, Al93a, Aw95, Ale97, Bd98a, Bis90, Boy97, Bur96.
Smart-Card [Roh99, ABKL91, ABKL93, CJRR99b].

Smartcard [Ano98h, Ano99b, USE99c, Ano97, Ara93, Bam97, Ano98g, CH94b, IH99b, KK99a].

Smartcards [Bla96a, Bla96b, Sch90a, DR99a, IH99a, IHR99, MDS99].

SmartLink [Ano93k].

smooth [Odl94a, VZ97].

SNAKE [MSK99b].

Snefru [BS91f].

SNMP [Sta96a, IH99a, IHR99, MDS99].

SNMP-CORBA [VDDR99].

SNMPv2 [GM93a].

snoop [Ano94h].

Soar [Gar97b].

SOBER [BP99a].

Soccer [BL99, CM99d, INDI99, PWU99].

Societal [Sta97b].

Societies [IEE92d, IEE94f, IEE95c].

Society [Ano98f, IEE92c, IEE93b, IEE94d, Mar96, DL96, KG96, Tas98].

Socio [SM99].

Socio-technical [SM99].

Sockets [ZG96].

SOCKS [Lee96, McM96].

Soft [NS98a].

Software [Abr97, Ano93j, Auc96, AG99, Bal97, Bih97b, BD94, CD97, Cla98a, CT99b, DBVD96, DF91c, DS89a, Gar97a, GO96a, Gut98b, HK92, JH98, KP96b, LU95, Lacs93, Lec99, Lut94, Mat96b, Mer91, MI97, RAS94, RC94a, RC94b, SW94a, Sch99c, SK96a, SK96b, SK96c, SW95a, SW97b, SK97c, She95b, You96, And94a, Ano95k, Bih97c, BP97b, DH96a, Des95, Goll96d, Knu99c, Pre95a, SS98a, SAM97, Str93a, Str93b, Vau98e, Woo90].

Software-Optimised [RC94a, RC94b].

software [MM95].

SOI [NF99].

Solaris [Sun91b].

SOLID [Ano97r, CK95, Gut96].

solid-state [Gut96].

Solution [GO96c, Law98, LR98, WD98].

Solutions [HM98, MSK99a].

solve [WSFC99].

Solved [Ano97c, Ano98c, Rec98].

Solving [LO91b, Lew92, MS96, OMV98, Per99].

SOM [BBN96].

Some [Abe98b, AT99, BBL95, Bri90a, BS91g, CD95, CRRY99, CL98, Des98c, EvH91, FDB93a, Gi99, Gui97, HGH98, Hub91, HCY96a, Kn99a, KP95, KLY98, La92, LP94, Li90, MSS98, OK98, Sim97, TCH91, Wag98b, Cao99, Cha95a, FDB93b, Goll97c, Lan96, RD96a, SM98b, TH99, Koo97].

Someone [MB99a].

Something [Sva98].

Son [CFK91].

soon [Pri94].

sophisticated [Mei98].

Sought [Ano97z].

Sound [CJRR99a, MGL98, Ano96l].

Soundness [DE99].

sounds [BDC95].

Source [Sch94g, Sch96a, Sch94h, Zim95b, Zim96a, Zim96b].

sourcebook [Ban94, Rot95a].

Sources [ADDB99, Cor99, Un94c].

Southcon [IEE96f].

Southcon/96 [IEE96f].

Soviet [COP95a, HK99a].

SP [STP93].

Space [AR99, BC95c, FP99, Gar97c, HBK99, KV99, KI96, SCG99, BB90, Mra95, Pad98, Sze98].

space-filling [BB90].

spaced [It90].

spaceflight [CWM91].

Spaces [BP95a, DFB93a, FDB93b, Koz96, Son99].

Spain [Mau96b].

Spoke [CFK91].

Span [BDS98, DQ94, HL93a, VBD99].

Spanning [Aga92].

SPARC [Sun91b].

Sparse [LO91b].

Spass [WABC99].

Spatial [BP95a, FDB93a, FDB93b, Koz96, Son99].

Speakeasy [LU95].

speaking [LC95].

spearhead [Ano98h].

SPEC [DDJ98a].

Special [vD97, FT99b, MP94, SS99e, SS99f].

Specific [ADDB99, EvH93, Kha93, LMS97].

Specification [GB93, HJTW99, LL97a, Otu99, SW94a, Tou92].

Specifications [KS98a, Nat92b].

Specified [Gui97, HCC98].

Specifying [SW94a].

Specs [Got99].

Spectral [WF94].

Spectrum [CKLS97, She94c, CKLS96b, CKLS96c, Dix94, KSB96b, KSB97, LL98, OP98].

Speech [DMFB97, Eri97b, GDS91, IEE97d, IEE97e, Lud97, SW95b, All97, CW94].
Speeches [Bar94]. Speed
[ARV99a, ARV99b, Ano99c, Ano99e, DP98a,
DP98b, Ebe93, FVEA99, IMI93b, Koc94,
LS97, MPPS95, SKNO98a, SKNO98b,
SW97a, SW97b, She92d, She95b, IMI93a,
Kap98, KAK96, Lam99, Nor95a, HKSW98,
HKRS99, Zhe97a]. Speeding
[ADEDS99, KT93, McK99, Tes98]. spi
[AG97b, AG97c, AG97a]. Spiculated
[ZTR99]. Spin [RK99]. Spite [Wai90]. SPJ
[TL99]. SPLICE [HC95b]. SPLICE/AS
[HC95b]. Split [Cool97]. Splittting
[Coc97]. Splitting [Sga91b].
SPM [CV93]. SPN [Kob99].
SPN-Structures [Kob99]. Spoofing
[SVxW91]. SPRC [Wol93b]. Spread
[CKLS97, Dix94, She94c, CKLS96b,
CKLS96c, KSB96b, KSB97, LLB98, OP98].
Spreading [SB94, KSB96a]. Spring
[DG99d]. Springer [Hat96].
Springer-Verlag [Hat96]. Spurs [Lea99].
SPX [Ara93b]. Spy [WS96c, Win91].
spy-catching [WS96c]. Spymasters
[Cha90]. SQL [CM98]. SQL*Net [Ano95k].
Square [DKR97b, DKK97a, EPR99b,
EPR99a, Gar98a]. squares [BSNP97].
squeamish [AGLL95]. SRA [SSH93]. SSH
[Sar97]. SSL
[Ano97r, FKK96, WS96a, WS96b, WS97].
ssmail [BRW09]. Stabbing [Aga92].
Stability [Wed99, DX99]. Stabilization
[YMW99]. Stabilizer [BS99a]. Stage
[Ano97d]. staircase [MK92]. Stakes
[GO96c]. stamp [HS91]. Stamping
[BL998, BS99]. Stamps [HS95].
Standard [AA95, Acc97, Int91a, Nat93b,
Ano93f, NIS94, Ano95i, Ano95j, Ble98a,
Com94a, Com94b, FIP99b, FIP94, Gar98a,
Gar98b, Kal97a, RAS93f, Law98, Len96,
LM91b, Nat91, Nat93a, NIS93b, Nat94a,
Nat95, Nat97b, Nat98, Nat99a, Natxx,
NIS93a, Nys99, RAS93d, RAS95c, RAS93e,
RAS93a, RSA99b, RP94, RD99a, RD99b,
SB93, Ano90, Ano95c, CCN95, LM91a,
Nat93c, NMVR95a, Pri94, Rev91, Tha91,
Un196a, Ada98, ARW99, ABK98a, Ano94b,
Ano95n, Ano97h, Ano97b, Ano97x, Bar91,
Bas98, Bas95, BS93b, Bir95, CMKK98,
Cop94a, DD98a, Den90, Gai90, Gar98b,
HK98, HK99d, Hub98, Joh90, Kap98, KIM97,
Mat94a, Nat92a, Nat92b, Nat94b, Nat94c,
Nat94d, Nat99c, NMVR95b, NBD+99, Pai96,
Per91, RSA93b, RP94, Riv93c, She95b,
She92g, Sim95, SB92, SB99, Wil93a, Ano95c].
Standardisation [Ved98].
Standardization [Ano96k, Pre93b].
Standardized [Ano95n]. Standards
[Ano90, Ano95n, Ano96k, Ano97x, Ano97y,
Ano97z, Ano98i, DD99d, Spi99, Gar98a,
Gar98b, Got99, GO96c, IEE94b, Kal93a, Kal99,
MBB98, PP96, Ano92b]. Standards-Based
[BS97]. Stanford [IEE98b]. Stanica
[YT96]. Stanley [vdWS97, vS97]. Star
[Ano97r, HI97]. starts [Ano96l]. State
[FGS96, Lan98, LF99, Mjo93, NM96a, Pre98c,
PR98, Pre99, She92e, Wol93a, Wol93b, Zaj97,
BFS92a, BFS92b, Gut96, PGV93d, Ri996].
State-industry [Zaj97]. State-of-the-Art
[She92e]. Stateless [BG99].
STATEMATE [JH98]. Statement
[II96]. States
[Chis97, Chis99, Lev91, Mil95, UU97b]. Station
[BMM99b, SMI98b]. Station-to-Station
[BMM99b]. Statistical
[De99, GC91, GSV99, GUS96, PNFK95,
NO98, Tha91, GKS97]. Statistics
[BBDF97, IEE94a, FO90]. Status
[Dob96b, FL99b, Nat99c, NBD+99, Ros95b].
Stay [MK94]. Staying [Rit99]. Steady
[MHP99]. Steal [Wai99b]. Steganalysis
[East98, JI98c]. Steganographia [Reed98].
Steganographic [ANS98a, CM97c, NHB98,
ZFQP98, ZFK98]. Steganographic
[MPS94]. Steganography [All98, And96b,
AP98, Cac98, Cra98, CI96, DS96, FJM+96,
Joh97a, Joh97b, JJ98b, JJ98a, JJ98e,
Kah96a, MT94, Mau97c, NNEK97, Phi98,
Rho95, WW98a, Cai96, Cra97]. Steiner
[ZW99]. step [Ano97d]. Steps [GO96b].
Stern [Cus97]. Still [BI99, Mei98, BBCP97].

Stockholders [MS99a]. Stop [BP97a, PP97, SSNP99, vHPP93, Pif96c].


store-and-forward [CadHSV96]. Stored [SV99a, SV99b, Lee95, SvS98].

Story [DDJ98g, DDJ98h, Pra96, Ritxx, Ell97, Hag98, HS93, Kah96b, Wel97]. STRATA [PMP99].

Strategies [AWV99, CO98, Dae95, KFJP96]. Strategy [Gar97a, KTM+99, OMV98].

Stream [AM97, BD94, Cha94a, CS91, Cla97, Cla98a, DC98b, Din94, DNRS97, Gol97d, Gol99b, JJ99b, LS97, Mau91a, MS91, PK95a, PK95b, Pen96, Rob95b, Ros98a, SK97b, SK97a, She94a, She94d, War98, ZYW91, ZG96, BK95a, DGV94b, DX91, Gol95b, Gol99b, JV98a, LRW93, Tay94]. Stream-Cipher [ZYWR91].

Streams [GR97, PSB97].

Street [KS98b, Sim98c, HRT96, Law98].

Strength [HK98, HK99d, Cop94a, KM97, Mat95]. strengthen [BB95a]. Strengthened [MB94a].

Strengthening [MB94a]. Stretch [Pa99b]. Stretching [And96b]. strict [SZZ94a, YT96, Cus96, CS96c, O'C94].

string [Ole95]. string-rewriting [Ole95].

Strings [Gol96b]. Strong [CvHP91, Gar97b, Gut98b, GS99b, PW97c, RS98e, RSxx, Sil97b, Sil97a, WD99b, Woi98, ZZ96, DLP93, DT93, MCD98b, SZZ95b, Sze98, Ver98b, YWY99]. Stronger [FS97b, MAM95, SVAA+98]. Stronghold [Ano97]. Strongly [Mau91d].

Strongly-Randomized [Mau91d].


Studies [WD97, DN95a, Ger99b]. Study [BPP99, Dae99, LBHM99, LL98, Sch99d, Gua90, LMS97, Sta97a, Zhou94]. subband [TKS98].

Subcommittee [Un98d, Un97b, Un95a]. Subcommittees [Un98e]. subgroup [Boy97]. subgroups [ML98]. Subjective [Joe98]. Subliminal [BDI+96, Gru98, KI97, SI93b, SI94, Sch93b, Sch94e, Sim93, Sim94d, Sim94c, Sim96a, Sim97, Des96b, Sim98a, Sim98b, YL97a]. Subliminal-Free [BDI+96]. Sublists [Rus93a]. submanifolds [Mra95].

Submission [Ada98, CMKK98, BT97, Zun98]. Submissions [SKW+99a, SKW+99b].

Submit [Law98]. Subquadratic [BBP95a, BBP95b]. Subscribers [GC97].

subscribe [Mau91b]. Subsegments [KPR99]. Subset [NS99b, CJL+92].

Substitution [CT99a, HS90, PRAM98, SZZ94b, ZZ96, Ata94, FS93, Frid92b, HT95, O'C95, Zan90]. Substitution-Permutation [CT99a, HT95, O'C95, Zan90]. Subtitle [Mer90b]. success [Blo98c, TY94].

successful [HA94b]. successfully [AI 96].

Successor [Ano97z]. Sufficient [MSN99, Rus93b, Rom90b]. Suggested [Bih91]. Suggestions [Mat96b].

suitable [CCZ98, Kob90, MZI98, Miy93a, Nac93, NM94, XL98, YL96a]. Sum [NS99b, CJL+92, JV98a].

Summary [CFG99, DY91d, Uni96a]. summation [Daw93]. Summer [USE94, Mye96].

Summit [CFK+91]. sums [BK98g, CFS97, Kob91c]. Sun [Bro97, Gar98b, Got99, Law98]. SunOS [Ste92, Sun91b]. Super [Sut99].

Supercomputer [DS95, She92e, Bam97]. Supercomputing [IEE91]. superhighway [BDC+95]. Superimposing [YY91].

supersafe [PP96]. Superscalar [Cla97].
superscritcher [Cra92, CF92].

Supersingular [BS91b]. Supervisory [KA99].
Supersingular [BS91b]. Supervisory [KA99].

Supporting [PK99, MI90]. Surmounting [CI96].
Surrounding [GA98]. Surveillance [CKN99, SB97].

Surveys [Ell99]. Susceptibility [AW94]. suspected [LHL95b, LHL95a]. swapping [TN97].

Swedish [LF97]. Swindles [Dob95b].
Switches [Bec99]. Switching [MOM91].

Switzerland [ACM97a, BCB97, IEE96c].
Swiss [Den95]. Sydney [KG93, SP90, VPM97]. Sylvester [Por98].

Symbolic [Wat91, AM99, BHKR97].
Symbols [Pes97, CS99]. Symmetric [Ada97a, Bir98, BDR+96, BFN08a, FO99b, Gus96, QG90, Roe94, YY98d, YY98b, BDJR97, Cra96, GHS93, H1099, Hwa93].

Symmetry [BS95d, PS97]. Symposium [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97b, ACM97c, ACM98b, ACM99b, Ano99c, Com96, CMM93, DEQ92, Hei96a, IE93c, IE93e, IE94d, IE95b, IE96a, IE97f, IE97i, IE98a, IE99a, KK99b, Q+98, Sp95, SL93, USE93b, USE95b, USE96c, USE96g, USE98a, USE98d, USE99a, Wat91, Wol93a, Wol93b, Tv92]. synchronised [KI97]. Synchronization [DHS95, BCCG99].

Sync [Yah94, Gon92]. Synchronizing [Mau91a].
Synchronous [AMP99, NT99, DGV94b].
Syndrome [CS96a, ZYR91, ZH90]. Syntax [Kal98f, Kal98c, Kal98d, RSA93d, RSA93c, RSA93e, RSA99a]. Synthesis [HL99, Sab94]. synthetic [PGV93b, PGV94]. System [ANS98a, Ano97r, ADF98, AHMS99, BS99a, BLM99, BKS99, Bal97, BR97a, BM91a, Bie98, Bla94b, BHJM99, BG99, Bur94b, CIBM99, CD97, CM99b, Ch92, CC99c, CH94b, CM99d, DPD90, DT98a, DTDJ99, Far92, FK99, FO97, FR95d, Gan96b, Gar97a, GRB99, Go90a, GPSV98, GS99a, HJTW99, HCD99, HJL99, HE98, IND99, JO97, Jia99, KI99, KW99, LMP99, LW95, LC99, ML94a, MKL99, MR95a, Mar98a, Mau97b, MTV92, Mon93, NM99, NS98a, Nec96, PR99, PS99f, PK99, Rei92, Rus90, RH99, SYMI98, SSSW98, Sam98, STSW99, SCT99, SK96b, SK96c, Sch98b, SSP90, SM99, SKIT99, Tro93, Tun99, Var99b, WHFG92, WABC99, WW98a, WBBL99, WABM94, ZK96, ACC99, BBCP98b, Bax97, BMP97a, Bur94a, BD95b, Car94, CB96, Cus95, DSS99, Des95, DH96b, FM98b, HN94].
system [HI97, Hwa92a, HC95b, KM98b, Kwn97, LC96a, LCL95, MY93b, MKK99, MM95, Oel97, PS99e, PSW95, Sch99j, SY96b, SS95b, SS95c, TCH+91, TC91, Ven90, WSCF99, WABL93, ADDS91, Ano91a, Bax97, Bel92, Dan95, JD91, RC95, YK99, ZHJ98].
Systematic [BGH+91, Zav99, Men95b].
Systematising [MKL99]. Systeme [BGH95b]. Systems [ABLP93, AKP96, AKF94, Ako99, Ano94j, Ano95i, Ano96a, ADEDS99, AA97, AMP99, BDPSN95, Bar99, Bas93, BR91, BBD97, BF98a, CF95, DDJ98a, Dam91b, DFTY97, DY91a, DD99, DB96, ENK99, FJP96, FY95a, FY95b, FY99b, FOO91, GL96, GFB93, Gil98, GM90, GMW91, GK96, GS97, GM98, HGD98, HJ+xx, HH94, HP98b, IE93a, IE96b, IE96d, IE98e, IE99b, IH99a, KT96, Koc96b, KA99, KY92, LO91b, LQRS98, LABW92, Lan99, Lee99b, Mar99, Mes99a, MS95f, MDP94, Mu93, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PSN91, Pin97, Pit96b, PM99a, PD99b, RBV94, RG95, RIP95a, ST94, SN96, STS99b, DY91c,
SOOS95, SS90, She92a, SY92, Sta99, Tra99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a. **Systems** [WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFKP98, ZFK+98, ARK99, AHJF97, AMS96, AM99, AC97, BY93c, BGT96, BP95b, CG05, DMW94, Dix94, Frn92b, Goo96, GKS97, Gru98, HJJ+97, IE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Oht96, Ole95, Op96, PAK98, PA98b, PP92a, PP92b, PP95b, PP95a, RO96, SK97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DVQ96]. **Systolic** [SSS98, DF92, PJBM90]. **SZ42** [Dav98d]. **SZK** [GSV99]. **T** [YT96, PDGI99]. **T-Team** [PDGI99]. **T52** [Dav98c]. **T52e** [Sel98b]. **Table** [KMKH99, Has99, Hor95]. **Tableaux** [Mas99a]. **Tableaux-99** [Mas99a]. **Tables** [DRR95, JC98, lPNdbbbprm91]. **Tactical** [IKM99]. **Tagging** [Lud97]. **Tailoring** [CGM96]. **Talent** [DDJ98e, DDJ98f]. **Talk** [Deu97, Lei99b, Wat99, BS91c, Sim91]. **Talking** [HH99]. **Tamper** [Auc96, BDHJ98, KK99a, Zhe95b]. **tamper-free** [Zhe95b]. **Tamper-Resistant** [Auc96, KK99a]. **Tamper-proof** [Zhe95b]. **Technological** [UFC94]. **Technologies** [Dan96, DDS98, Aus96, BGV97a, BK94b, BS95e, Oht96, Uni96a]. **Technology** [Int91a, Ano96l, Ano98j, AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, II96, IEE94b, IEE98d, Lic94, Lin93c, NFQ99, Riv98c, USE99c, AnoS99a, DS97b, Gil97, ISO97, Ril96, Ros94, Smi97a, VB96, CFK+91, Ers99, Ano99b]. **Telecollaboration** [Fuc99]. **Telecommunications** [IEE97e, UN94, Mac98]. **Telemedicine** [Ano97-29]. **Teleperubatan** [Ano97-29]. **Telephone** [Gar97a]. **Telephony** [Ban94, Gar97b, MB99a, Mar95b]. **teletype** [Mac98]. **TELNET** [SSH93, Ala93b, Bor93a, Bor93b, Bor93c]. **Temporal** [KV99]. **Temporary** [KRJ98]. **Tennessee** [IEE94e]. **TeraSpell** [Ano97s]. **Term** [EO95b, CHN97, EO95a]. **Terminal** [Con98, Con99a]. **Terminals** [Ano99e, ADSW99, Lam99]. **Terminology** [Pf96a]. **Ternary** [PKA+98]. **Terrorists** [Uni98j, Uni98k]. **Terschelling** [TV94]. **Tesla** [Ano97t]. **TESS** [Dan95]. **Test** [DS97a, Law98, MOM91, SS91, DLP93, Graxx, Gre90, ZYR90]. **Testing**

Tetherless [Law98]. Texas [ACM97c, ACM98b, Ano94d, IEE92b, USE98d]. Text [Bar93a, Bar93b, Cai96, CD97, LM98b, PF94, PBGV90, CFK’91, Sga94, SHG98].

Textual [JKVP99]. Teyjus [NM99]. Theft [Gur97]. Their [BK95c, BL96b, BL96a, Con99b, GPT91a, GMW91, JMSI96, K96, Len99b, OO90, SY96a, SG99b, Tra99, VDDR99, AA99, BHSV98b, BHSV98a, BV93c, BV93b, Car98, DDB95a, DDB95b, Don98, Eng99, HMP95, KT91b, LN94, LM96, NM96b, SS99, SI93b, TY92, ‘YY98a].

Theme [Way95]. Theorem [AA93, FK99, GQ95, HEQL98, H94a, DiDPS96, Sga91a, WWH95]. Theoretic [Buc91a, Cac98, Cle91, MW96a, Mau99a, Mau99b, MO99, Ped91d, PB99a, STP93, W98, APDS93, Kos97, Ped91b, Ped91c, Sga91a, Sga93, Shp99b].

theoretical [Sak97, van97a]. Theoretically [AR99, Mau97a]. Theories [T’98]. Theory [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, Ber96b, BMP’97b, Car97b, CFK+91, Dam90a, Dam91a, Dav91, De 95, DS99, Fum97, GQ95, He94, IEE94a, IRR93, IZ98, IZ99, KM96a, KR99a, K9b, LOX99, LABW92, LW91, Mau96b, Mau96a, MDP94, NK94, NC97, OiDP98, PSN95b, PG90, Q90, Q95, R93e, SG98b, Hil94, Lag90, LABW91, Lox90, MW98a, Mau99b, MeC90b, Mei92, Ny98b, Pom90a, Rac90, Sch93a, Sch90c, Sch97c, Sga91a, Shp99a, Ste99b, Si95, Tat98, Tat99].

There [RL96, Zha97, Way93b]. Therefore [FJM+96]. these [Ano98h]. They’re [Wri94]. Third [AAB+97, Fra99, MKS99, RS98b, Spi95, Uni95a, ACM91, G96d, G94b, GK95b].

Third-Party [AAB+97]. Thirteenth [IEE94f, USE99b]. thirtieth [ACM98b].

Three [Ano95a, BR95b, HEQL98, KS97b, Ng99, OMA98, SN96, FR95b, OMA97, XZZ98]. Three-Dimensional [OMA98, OMA97].

Three-Party [Ng99, XZZ98]. Threshold [BBC93b, BBC93a, CGJ’99, DF90, Des93, Des94a, Des98a, OF98, Gem97, HHT93, HHT97, J90, KOO95b, KOO95a, LH93a, LH94, LH95b, LH95a, MKS99, NP98a, Oka98a, Oka98b, PM98, Ra98, Sti98b, SS99, Zha98, CG99, Bh95, CMTN94, DDB95a, DDB95b, F92, GJKR96a, Lan95, Lan96, LL97b, M99, Ped91c, SG98, SS94, TJ99, W94a, X99].


Tiger [AB96b]. Tighter [Hur98]. tickets [Gar96a, Gar97d]. Till [Mar95a]. Time [BM96a, BL98, BDS98, BF99, CM98, CGB’93, DDJ99, DJHP98, DF91c, F95, GFB93, H95s, IR99, J99c, KR99a, MGL’98, Mar99, MSH99, NA95, New98, RH99, Sch99i, Tro93, VBD99, Yac99a, Yac99b, ACC99, B98d, BHS93, BM96b, BM96c, BK98f, G95s, HS91, IEE94b, M99].

Time-stamp [HS91].

Time-Stamping [BL98, BHS93].


Timeliness [Yah94]. Timely [KYP92].

Timestamp [W99]. Timetabling [CC99c].

Timing [DS98b, EH96, HK98, HK99d].
[BFS96, Cha90, CvHP91, CR91, DY91f, Tay95, BMS96, Des90b, HW98c].

unreadable [PBBC97]. Unencrypted [Pfi95]. Undang [Ano97t-29].

Undang-undang [Ano97-29]. Undeniable [CvHP91, DY91f, FOO91, GKR97, SY96a, BCDP91, DP96, HY93a, Jak95, LWC96, Ped91a].


Unified [FBS97, Mau96a, OG95]. uniform [AWV99, Nyb94]. Union [Gar97c]. Unique [Fil95, CGV94]. Uniqueness [WW98b].

Unit [Un94b]. United [Cl97, Cli99, D98, Lam97, Un98h, Un97c, Cli95a, Cli98k, UU97b, Cli99, Lev91, Mil95, Sch98a].

Univariate [Cop95c]. Universal [AW94, AS96, BB97, CHSV96, EPR99b, EPR99a, KP99a, Sho96, Sti91b].

Universality [SS91]. Universally [Abe98a, BC93a]. Universe [Ros95a].

University [CFK+91, IEE98b, KG93, RBCE99, SKIT99, PDG99]. UNIX [Ano93c, Gar97c, IHR99, JF91, LT91, USE90, USE92b, USE93, USE95b, WB92, Car99, De93a, ZG96, Ano92a].

Unknown [BM999b, Pa99a]. Unlinkable [SSG99].


Uncatchable [WP90, Wa90].

Untraceable [OO90]. Untrusted [SK98a].

Untruths [For99]. Unveil [GC97, Gar98a].

Unveiling [Jam98].

update [Ano94i, Ano95a, Ano95b, Ano95n, Ano96b, Ano96k, Ano97c, Ano97y, Ano97z, Ano98i, MGL+98, Pin98, Ros95b, Ros96d, Ros97b, Ste99c, Wie97, Wie98a]. updated [Ano97t].

upon [BMP97a, CCH98, LCL95]. Upper [Fe98, A96, O94]. Urge [BG98].

Urgent [Pra96]. URL [Zuk98b]. USA [???90, Ano98f, AA97, Au98, Bri92, Bri93, Cop95d, Des94b, HF97, IEE97g, IEE97e, IEE98c, IE98e, Ke97e, Kob96, KP99b, Kra98, SJ97, Sti93b, Sti94, USE91, USE93, USE94, USE95b, USE95c, USE95a, USE95f, USE99a, USE99b, USE99c, USE99d, Wie99].

Usability [WT99, CG05]. USACM [Ano97t-30]. Usage [End97]. Use [ADBB99, BCE+94, Bra90a, CFGS99, Con99b, Gan96a, Gar97a, Gar97b, GC97, GK98, HLL99, Iss90, KR95c, Koh90, Lan99, MG98a, MG98b, Por91, Rud91, SB94, Zuk98a, BDHJ97, BR97b, Cha94b, Cli99, CG05, Gil97, Joh90, Sti93c, Zer96a].

Used [GS94a, S96, Car97c, Car98, Gau97, Kuk99, Sch91b, SX90, van97a].

USERNET [Bis91]. Usenix [USE99d, Com96, Ros96a, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c].

User [AKF94, BE90, Bus96, Dra99, Gog99, Go90a, GN95b, IS99, KCT94a, KCT94b, PMP99, RRSW97a, RRSW97b, SYM98, SCT99, Zim95a, DF91b, MC96, Mu92, RSA94, RT93, SJS98, Sta95b].


Users [Hel98a, WK97, Sta94a].

Uses [Swi97, DKB97b, Sc99g].

using [CGM97b, CPPK98, CB96, Cle96, Dan97, GK99b, GBL94, Gor93b, Hor95, ISO97, Jak95, JM96a, KR95a, KC95, Kar96, Kay95, Koc95, KH97, KH98a, LC96b, LC96c, MHP95, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SSM94, SD97, Su98, SZT98b, SZTB98, Tak97, Til98, VZ97, VP98, Whi93, Wil93a, Yam98a, Zho94, dR95].

Utah [USE95b].

Utility [Zol93, Vu95].

Utilization [GRB99].

Utilize [MSO96].

utilizing [SW95a].

V [IEE92a].

V1.0 [Lim99, RSA99a].

v2.0 [Ano97r, RSA99b].

V32bis [Ano93k].

V5 [IEE96a].

Validating [Gai90].

Validation [DDNM98, GS99a, RB99, Ste96].

Validity [GMW91, Kuk99].

Value [Ack98, Oko97, Tay94].

Values [GS94a, Tho96].

Vancouver [Yua92].

Vanstone [Kie98, NS97c, NS97b, Sha99a].

Vaporware [DDJ98e, DDJ98f].

Variable [BR99a, BR99b, DW94, GK95b, Sch94b, Su98, TN96a, TN96b, ZPS93].

Variable-Input-Length [BR99a, BR99b].

Variable-Length [Sch94b, Su98].

Variance [Kas96].

Variants [CRRY99, MSS98, RS99a, Sha95a].

variation [CCN95].

variations [Zho94].

varieties [Fir92b].

Various [GQW+91].

Vasculature [BAL99].

Vatican [Alv98a].

Vector [ADEDS99, TK99, TYD99, CCH98, MTN97, Pad98, dR95].

vectors [LM93c, Mat91, MLA91].

Vegas [ACM95, AA97].

Vehicle [CKN99].

Vendors [Gar97a, Gar97b, Gar98a, GB98].

Venona [HK99c, Pea97].

Ventura [Nat98, RD99a].

VerCheck [MGL+98].

Verdict [Wri94].

Veri [SY99].

Veri-KoMoD [SY99].

Verifiable [Abe98a, AGY95b, CG98, Cre90, FR95c, GM95b, Ped91d, Sch99i, VBD99, AGY95a, BD98a, Bur96, FO98, Mao97, MILY93, Ped91b, Ped91e, Sta96a].

Verification [Abe98a, AB97, BGR98a, Bol98a, Bol98b, CDF915, DS97a, GFB93, GS99a, HL92, MM99a, Na97, OM93, PM98, PV98, SM95a, SY99, Tou93, WW98b, YY99a, BGR98b, Bol97, BS95c, Des90a, Dwo91, JC98, JW01, Mea95, YL95a, YM98, ZL99].

Verifications [GMV98].

Verifier [JMS96].

Verifiers [PM98].

Verify [DS97d, Chi99a, Chi99b].

Verifying [LHB96, Sa91, DN95b, Pau98].

Verlag [Hat96].

Verl¨assliche [BGH95b].

Vermont [IEE96a].

Verschl¨usselungssysteme [Wal98].

Verschl¨usselungsverfahren [Ger97].

Version [An97r, An98r, BC93a, BP98e, DB96, FKK96, Gar97b, Kal98b, Kal98d, Kal98e, KS98a, RSA93f, Lim99, MT99a, McM96, RSA93a, RSA94, DY91c, SS99b, SM98b, WABC99, CLW98, GM93a, Gib95, Bor93b, Lin96b].

Versus [MGL+98].

Vertraulichkeit [FT95].

Very [HMV93, MS90, PF94, Yua92, SN94].

Veto [OK96a].

VHDL [Oel97].

via [BR96b, BCKxx, BM95, BS95d, DS90a, DN95a, DN93, EPR99b, EPR99a, Fuc99, HS94, JJ99b, NW98, UFC94].

Vibration [Nas94, NA95].

VICS [Uni96a].

VICTOR [OSA91].

Victorian [Abe98b].

Video [An99e, BF99, DLF97, DS97c, DS98, HG97c, KBR97, KH98b, LT98, MT94, SJ97, SB98, SZT98a, WK97, WW98a, ZL99, BB90, BCB97, CPO+98, CHO+98, CKLS96c, DS97b, HG96, HG97e, HG97d, HG98, HW97, HW98a, Lam99, Oht96,
Video-based [WKHG97, BCB97].
Video-Steganography [MT94]. Vienna
View [CK95, Lan98, MUSM98, MM96a, STP93, Ste91, ZL99, Ano97i, Pri94, UU97a, Wad93].
Viewpoint [Ste91].
Views [DDJ98e, DDJ98c, DDJ98f, DDJ98a, DDJ98d, DDJ98b, DDJ98g, DDJ98h, DDJ99, Eri97b, TLS99].
VII [IEE99b].
VIL [AB99a, AB99b].
VIL-MACs [AB99a, AB99b]. Village [Ber97b].
Vinegar [KS98d, KPG99].
VINO [DW94].
Virginia [ACM93a, ACM94a, IEE94a].
Virtual [DFGH99, GB98, HL99, CCH98, LS98a].
VirtuFlex [Ano97s].
Virus [BGG95, Hig97b, Nac97, LFSY94, OY91].
Viruses [Hig97a, Whi90, Coh94].
VIS [BGH95b]. Visa [Lea99, Gau97].
Visibility [LE99].
Vision [CKN99, HCDC99, PJ99, SW95b, SKT99, CS99, RP97b].
Vision-Based [SKIT99].
visit [JQ98a].
Visited [FY95b].
Visual [ABDS96, B996, BD98b, DDM97, Dro96, HKS97a, HKS97b, JKVP99, KI96, NS95, NP97, PKA+98, PZ98, PNFK95, Sha98, St98b, BW97, Ger99b].
Visualisation [MM99b].
Visualization [Jan99, PH91, GTW94].
Visualize [BW98].
VLDB [Yua92].
VLIW [Cla97].
VLSI
[CK99, Mas91, Pai96, Pos98, Vad95, Zim99].
VoD [GMDS98]. Voice
[CM97b, MB99a, Cha94b, Int91b]. vol.
[Ano97-28].
volume [Kat97]. Voting
[Boy90, JT97a, Mr93, NR94, SK94, SK95, Sch99, FO093].
vowel [Lip98].
Voyager [AHMS99].
Vries [GK95b].
VRML
[Gar97b, Gar98a].
vs
[DP99, GA98, Tho96, Uni98a, Uni98d].
VSP
[YEA+98].
Vulnerabilities [Sch98d].
Vulnerability [Gar97c, AFB95].
W [YT96].
WA [USE99b]. Wafers
[Gar97a].
waggery [Beu94]. Waldmeister
[HJL99]. Wall [HRT96, Law98].
Wallet [CP93].
Wallets [DT98a].
Walsh [SBS97].
Wang [vT93].
Want [Rot97, Way93c].
Wanted [Bra95d, Hii97, PKA+98].
War
[Alv98b, AK99, Dav98a, Don98, Law98, Mon96, Rat96, Wei99, Mar98b, Hin93, Joh95].
Warden [Cra98, Cra97].
Warranty
[EKLM99, TLS99].
Warhousing
[BMNL99].
warfare [Den99, Rot95a].
WARM
[MPL99].
WARM-UP [MPL99].
Warning [Gar97c].
Warrant [LWY95].
Warranty-Based
[FKMY98].
Wars [GC97].
warum [MPS94].
Was [CFK+91, Dea98b, Kru98, Mon96].
Washington
[HF97, USE98a, USE99a, DDJ98c, DDJ98f].
WASS
[PS99b, PS99c].
Watch
[Cha99a, Rit99, Sch99h].
watchdog
[MHPS96].
Water
[WF94].
Watermark
[Ano97o, CKLS96a, ONT98, SY98, TRS+93, WD96, vTO94, And98, Ano93a, CKLS96b, CMYY97, PBB97, TOH98, XBA97, YEA+98].
watermarked
[BP98b, BP98c, RRP97].
Watermarking
[Ack98, ADF98, Ben99, Ber97b, BOD95, BO96b, BFW99, Car97a, CKLS97, CMYY98, DDM98, DDGM97, DSS98, EQ98, Eil99, FBS98, GDD97, GB98, GO96c, HG97c, HG97d, HG98, KR98, Koh97, LQRS98, MB98, Mos98, NH98, OMA97, OMA98, PZ98, QN98b, RKDB96, SCxx, SZT96b, SZT98a, WK97, WD97, Xie98, YY99a, ZK96, BBPC97, BBPC98b, BBC98, BCD98a, BP98d, BVC97, BO96a, CPO+98, CHO+98, CT99b, CKLS96c, CM97d, DDM98, DDM99, DNN98, DNS98, HG96, HG97c, HEG98, HPA99, HW97, HW98a, HW98b, Irw98, KH97, KH98a, MTr97, Nat97a, NO98, NP98b, ODB96, OP97, OP98, OP98, OP98, OKO96, PHF99, SD97, SHG98, SZT98b, SZTB98, TA97, TKS98, VP96, VP98, VNP98, Yeu97, Yeu98, YMY98.]
84

ZK98, ZKOY99. **Watermarks** [Ano97n, BTH96, BI99, CL98, EKK99, HPG98, LvD98, LKD98, Mae98, MMST98, YYY98, CL97b, LLB98, Min97, MBY97, ZL97, Zha96]. **Watson** [CFK+91]. **Wave** [GO96c]. **Waveguides** [FVEA99]. **Wavelet** [LSVV95, KH97, KH98a, NO98, XA98]. **wavelet-based** [KH97]. **Wavelets** [Lut98]. **Way** [BJY97, BdM94, BM94a, BKK98, BP97c, DGV93, DDP90, GMD98, Mer90a, Roe94, Sch91b, TOU94, ZKB98, BK98f, DI99, Dob98, HILL99, HYLT99, Hwa92a, MZ98, Rom90b, Sim98c, Sta94a, Sz98, Tso92b, Tso92a, ZPS93, KSW97a, KSW97b]. **Wayner** [vdWS97, vS97]. **Wayness** [HT99]. **ways** [Den95]. **WDAG** [TV94]. **Weak** [DGV94c, DYL98, Haw98b, Pit98b, Sze98, Vau96, FY95c, Haw98a, Knu95, SSI97a, SSI97b, YL97b]. **Weakened** [AB99a, AB99b]. **Weakly** [MP91]. **Weakness** [Cop99, KSW99a, Kie98]. **Weaknesses** [BMS94, Dyon91, Kel99, KP93, Lan96, PA98b, RK98, Rj99, SJ96, DGV94b, She96b, XZZ97]. **weapon** [Ano97]. **weapons** [Mei98]. **Web** [Ano97r, MR98, OW95, SA95, Sta95a, Ver98b, Ale98, Ano97d, Bn99, BMN199, Cha99b, Dav95, DDK98, FL96, GMM97, GO96c, Law95, She96b, Ude98, WCSS95, You96, ZL99]. **Web-Based** [ZL99]. **Web-enabled** [Cha99b]. **WebTime** [Ano97]. **Weighing** [KR96a]. **Weight** [PK95a, PK95b, Pen96, She95c, BGH+95a, CC98]. **Weighted** [MP99]. **Welcome** [Riv95c]. **wen** [XTrmW94]. **West** [DDJ98c, Fra99, Hir97, Hir98]. **wheel** [Car97c]. **Wheeler** [Bar05]. **Where** [DDJ98c, DDJ98d, LH95b, LHF95a, Van95b]. **wherein** [Lea90]. **Which** [Che92, EvH91, EvH92, EvH93, Gir99]. **while** [vdWS97, vS97]. **Who** [BCE+94, DDJ98d, Mar95a, Mon96]. **whom** [LC95]. **Whose** [Ano94j]. **Wide** [Ale98, Dav95, OW95, She96b, CDEH+96, Wad93, HC95b]. **widespread** [C199]. **Width** [GM99b]. **Wie** [MP99]. **Will** [DDJ98d, Gar97b, GC97, Gar98a, Wor96, Ano98b, Gau97, Mii95, Sch93e, ZKOY99]. **William** [Lea90, Uni92, vdWS97, vS97]. **Williams** [JQ98b]. **Window** [Bel92, KT93, PAK+98]. **Windows** [USE98a, Boy98, Br98, IH98, Ken95, RC95, ZG96]. **Windsor** [SL93]. **Winkel** [Ers99]. **Winnowing** [Riv98d]. **Winter** [USE91, USE92a, USE96c]. **WIPO** [Gar97c]. **Wire** [Wal94]. **Wireless** [Gar98a, PS98d, She93d, Goo96, IEE97k, PS98e, PS99a, PS99b, PS99c, WSFC99, PS98e, PS98f]. **Wiretap** [Ele98]. **wiring** [DL98, RK94, Rot95a]. **wisdom** [JC98]. **Wise** [Ano96j]. **Within** [BGV93, BGM97a, BMN97b, FL93, HJT99, KW92, MG98a, MG98b]. **Without** [BP97a, BMNV98, GHR99, Hus99, Len96, Luc98b, SG99a, Abe99, Ano98, Ben94, Ble96, HY93a, HG97d, Hor95, IS91, JMO95a, JC98, KRS99, LM94a, LM94b, LW96, Ped91c, PBBC97, Riv98d, Sak97, Sim98b, SS99e, SS99f, Wu92]. **withstand** [OY91]. **Withstanding** [SVX91]. **Witness** [CD94, FGY96b, FGY96a, RGV97]. **Witness-based** [FGY96b, FGY96a]. **witnesses** [She92b]. **Woes** [DDJ98g, DDJ98h]. **Wollongong** [PS95b]. **won't** [AK95, ZKOY99]. **Woolongong** [GN95b]. **Worcester** [KP99b]. **Word** [LMBO95]. **Words** [HKL94, Ata94, AG95, CC98, SM90, Sta96b]. **Work** [Abe98a, Ano97y, BK95c, CFSY96, Gar98b, MGL+98, Blo98b, KM98b]. **workfactor** [Jas96, Kau96]. **Working** [DDJ99, Kat97, LM98a, MB99b]. **Works** [Ano96k, FJM+96]. **Workshop** [ACM98a, Ano94a, ???90, Ano93g, Ano99b, Auc98, Bih97c, Bra93a, CW94, Chr99b, Dam90a, Dam91a, Dav91, De 95, FM91,
REFERENCES


Y2K
Ano98j, DDJ98b, Eri97b, Law98, MGL+98.

Yaksha [Gan96b]. Yarrow [KSF99]. Year [Sch95a, Sil99, Roe95]. Years [Bon99, Yin97, BC96b, CWM+91, Den90, Gol97c, Mar96]. yi [IPNdbbbrm91]. Yield [GMW91]. Yokohama [Iz98]. York [IEE99a, USE95c]. Yu [BY92]. YY [Nat92b].


References

Anonymous:1990:IWH

???90

IT Workshop, Hawaii, USA, November 27–30. ???, ????, 1990.

Anonymous:1997:ACC

REFERENCES


**Almgren:2000:HWC**


**Anderson:1996:TPP**


**Anderson:1996:TFN**


**Ayadi:1997:VCP**


REFERENCES

89

of the number of mix-

servers. In Nyberg [Nyb98],

pages 437–447. ISBN 3-540-

64518-7 (paperback). ISSN

0302-9743 (print), 1611-

3349 (electronic). LCCN

QA267.A1 L43 no.1403.


ac.uk/~fapp2/steganography/
bibliography/072403.html

Abeles:1998:SVP

Stanley H. Lipson Francine

Abeles. Some Victorian

periodic polyalphabetic ci-

phers. In Deavours et al.

[DKK+98], pages 309–

315. ISBN 0-89006-862-


US$78.20. URL http://

www.opengroup.com/open/

cbooks/089/0890068623.

shtml. Third volume of se-

lected papers from issues of

Cryptologia.

Abe:1999:RDM

M. Abe. Robust distributed

multiplication without in-

teraction. In Wiener

[Wie99], pages 130–147.

ISBN 3-540-66347-9. LCCN


Anderson:1998:SPA

R. Anderson, E. Biham, and

L. Knudsen. Serpent: a pro-

posal for the Advanced En-

cryption Standard. NIST

AES proposal, National In-

stitute for Standards and

Technology, Gaithersburg,

MD 20899-8900, USA, June


Anderson:1998:SNBa

Ross Anderson, Eli Biham,

and Lars Knudsen. Serpent:

a new block cipher pro-

posal. In National Institute

of Standards and Technol-

ogy [Nat98], page ?? ISBN

???? LCCN ???. URL

http://www.cl.cam.ac.

uk/~rja14/serpent.html.

No slides for the conference

talk are available.

Anderson:1998:SNBb

Ross Anderson, Eli Biham,

and Lars Knudsen. Serpent:

a new block cipher proposal.

In Vaudenay [Vau98e],

pages 222–238. CODEN

LNCSD9. ISBN 3-540-

64265-X (paperback). ISSN

0302-9743 (print), 1611-

3349 (electronic). LCCN


Abadi:1991:ADS

M. Abadi, M. Burrows,

C. Kaufman, and B. Lamp-

son. Authentication and
delegation with smart-

cards. Lecture Notes in

Computer Science, 526:

326–??, 1991. CODEN

LNCSD9. ISBN 3-540-

64265-X (paperback). ISSN

0302-9743 (print), 1611-

3349 (electronic).

Abadi:1993:ADS

M. Abadi, M. Burrows,

C. Kaufman, and B. Lamp-

son. Authentication and


REFERENCES


REFERENCES

2. LCCN QA76.A15 1990. ACM order no. 508900.

[ACM:1991:PTT]


[ACM91]

[ACM:1993:FAC]


[ACM93a]

[ACM:1993:PTF]


[ACM93b]

[ACM:1994:AAC]


[ACM94a]

[ACM:1994:CKC]


[ACM94b]

[ACM:1994:PTS]


[ACM94c]

[ACM:1995:PTS]

ACM:1996:PAM

ACM:1996:PTE

ACM:1997:ACC

ACM:1997:PEA

ACM:1997:PTN

ACM:1998:AWJ

ACM:1998:PTA
REFERENCES

1998. ACM order number 508980.

**ACM:1999:PPA**


**ACM:1999:PTF**


**ACM:1999:SPCd**


**ACM:1999:SPCd**


**Ajtai:1997:PKC**


**Ajtai:1999:PKC**

Adamek:1991:FCT


Adams:1992:IAB


Adams:1997:CSC


Adams:1997:RCE


Adams:1998:CSA


Achour:1999:UUK


Areces:1999:PRR

Abraham:1991:TSS


See erratum [Ano91a].

Appas:1999:SVS


Augot:1998:DSM


URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073404.html

Alagappan:1990:PDA


Adleman:1979:SAD


Adleman:1983:BGK


Adleman:1987:PRD


Asokan:1999:APT

N. Asokan, Hervé Débar, Michael Steiner, and Michael Waidner. Authenticating public ter-
REFERENCES

Alves-Foss:1995:ACS

Apostolico:1984:PM

Apostolico:1985:CA

Anderson:1995:SFS

Abadi:1997:RAC

Abadi:1997:CCPa
Abadi:1997:CCPb


Abadi:1998:BMCa


Abadi:1998:BMCb


Aura:1999:SLM


Agarwal:1992:RSO


Atkins:1995:MWS


Agnew:1987:RSC

[Agn87] G. B. Agnew. Random sources for cryptographic systems. In Chaum and


Aiello:1998:NCS

Al-Kadi:1998:OCA

Akritas:1983:CEA

Alvarez:1999:AAS

Aberer:1994:DUO

Akoka:1999:CDP
REFERENCES


Abdelguerfi:1996:GEI


Anlauff:1999:TSL


Aljabri:1996:UDU


Alabbadi:1993:IEC


Alagappan:1993:RTA


Alabbadi:1997:SCH


Alexander:1945:CHG

REFERENCES

**Alexandris:1992:FMC**


**Alexandre:1997:BSC**


**Alexandre:1998:JBP**


**Allen:1997:DEC**


**Allen:1998:SUM**


**Ahituv:1987:PED**


**Aiello:1998:FDI**


**Alvarez:1998:FLV**

David Alvarez. Faded lustre: Vatican cryptography, 1815–1920. In Deavours...

**Alvarez:1998:IDC**


**Alvarez:1998:PCS**


**Akl:1985:FPR**


**Adams:1988:SRC**


**Adams:1989:SRC**

Anderson:1997:CNK


Atanasiu:1999:ASE


ACE:1981:RPC


ANSI:1983:ANS


ABAECITC:1995:DSG


ABAECITDISC:1996:DSG


Ames:1996:SDM

M. Ames. Saving dollars makes sense of crypto export controls. Lecture Notes in Computer Science, 1029:90–??, 1996. CODEN LNCSD9. ISSN 0302-9743
REFERENCES


REFERENCES


[Anderson:1995:RPP]


[Andree:1952:C]


[Andelman:1979:MLE]


[Andelman:1980:MLE]

[Andelman:1980:MLE]


[Andrew:1986:CSI]


[Anderson:1993:PRT]


[Anderson:1994:FSE]

REFERENCES

Anderson:1994:WCF


Anderson:1996:CEM


Anderson:1996:SLS


Anderson:1996:IHF


Anderson:1998:EWF


Anonymous:1922:PUS


Anonymous:1939:ITM

Anonymous. Introductory talk to members of the William and Mary College cryptanalysis class. Technical report, William and Mary College, Williamsburg, VA, USA, 1939. 7 pp.

Anonymous:1960:CNH

Anonymous. *Cryptanalysis, a new horizon*, by Dr. Cryp-
REFERENCES

Anonymous: 1960: CCA
10 + 1 + 27 pp.

Anonymous: 1966: CCA

Anonymous: 1976: CCA

Anonymous: 1978: CSD

Anonymous: 1980: ACS

Anonymous: 1981: CHP

Anonymous: 1981: GIU

Anonymous: 1981: ODA
Anonymous:1982:CC


Anonymous:1982:ESS

Anonymous. Encryption scrambling the satellite signal for security, 1982. 1 sound cassette (75 min.).

Anonymous:1982:NNPa


Anonymous:1984:ESC


Anonymous:1985:BM


Anonymous:1985:DEA


Anonymous:1987:EVE


Anonymous:1988:EVE

Anonymous, editor. *Enigma
REFERENCES


Anonymous: 1988: ERH

Anonymous: 1989: SZS

Anonymous: 1990: SEL

Anonymous: 1991: ESS

Anonymous: 1991: FFL

Anonymous: 1992: AUd
Anonymous. Answers to UNIX. UNIX/World, 9(9): 121–??, September 1992. ISSN 0739-5922. [Ano92c]

Anonymous: 1992: DES
Anonymous: 1993: ACT


Anonymous: 1993: BRd


Anonymous: 1993: CKR


Anonymous: 1993: CSA


Anonymous: 1993: SMC

1993. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1993:WND
Anonymous. What’s new: The DTR-1 is a notebook or a pen computer, the SmartLink V32bis FaxModem encrypts your data, LapCAD 5 for the Mac gives you finite modeling, and more.BYTE Magazine, 18 (6):57–??, May 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1994:CNC

Anonymous:1994:DAX

Anonymous:1994:HSK

Anonymous:1994:ICI

Anonymous:1994:KEE

Anonymous:1994:LBA

Anonymous:1994:PPR
Anonymous. Product review: Pretty Good Privacy is a privacy advocate’s plan to head off the government’s bid to snoop on data. Open
Anonymous:1994:Uc

Anonymous:1994:WAS

Anonymous:1994:EES
Anonymous. An E-mail encryption standard should be in place by April, providing for the incorporation of Privacy Enhanced Mail into the MIME standard. Open Systems Today, 168:26–??, February 1995. ISSN 1061-0839.

Anonymous:1995:AUC

Anonymous:1995:AUM

Anonymous:1995:ARD

Anonymous:1995:ENa
Anonymous. Editor’s note. CryptoBytes, 1(2):
REFERENCES

Anonymous:1995:ENb

Anonymous:1995:FSH

Anonymous:1995:NIX

Anonymous:1995:OIN

Anonymous:1995:PTN

Anonymous:1995:RLM

Anonymous:1995:SUE

Anonymous:1996:NIS
REFERENCES

Anonymous:1996:RF


[Ano96f]


Anonymous:1996:ADX

[Ano96g]


Anonymous:1996:BCU

[Ano96h]


Anonymous:1996:CID

[Ano96i]


Anonymous:1996:CPD

&arnumber=508326. See [YL95b].

Anonymous:1996:ENa

[Ano96j]


Anonymous:1996:ENb


Anonymous:1996:ECC


Anonymous:1996:SCG


Anonymous:1996:SCG

REFERENCES


Anonymous:1996:SUS


Anonymous:1996:TBAa


Anonymous:1996:TBSa


Anonymous:1997:RDSa


Anonymous:1997:AES


Anonymous:1997:AUC

REFERENCES


REFERENCES


Anonymous:1997:ENc

Anonymous:1997:EW

Anonymous:1997:HEW

Anonymous:1997:INI

Anonymous:1997:MNL

Anonymous:1997:NPA
Anonymous. New products: AcceleratedX Server Version 3.1; CDE Business Desktop; DNEWS News Server 4.0; SecureNet PRO v2.0; Dynamic Modules; Stronghold Encrypting SSL Web Server; SOLID Desktop; Lone Star LONE-TAR 2.2gn Shop; Cactus System Crash AIR-BAG 3.4.1.1. Linux Journal, 39(??), July 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Anonymous:1997:NPNb
Anonymous. New products: NetTracker 3.0; ScriptEase: Integration SDK; JDesignerPro 2.1; VirtuFlex 2.0; PGP Version 5.0 for Personal Privacy; TeraSpell 97; FileDrive File Transfer Server; journyx WebTime. Linux Journal, 43(??), November 1997. CODEN LIJOFX. ISSN 1075-3583
Anonymous:1997:RCU


Anonymous:1997:RAJ


Anonymous:1997:RDL


Anonymous:1997:RDSb


Anonymous:1997:SFR


Anonymous:1997:SUE


Anonymous:1997:SUR


Anonymous:1997:SSA


Anonymous:1997:CBP

Anonymous. The Colossus of Bletchley Park, IEEE Rev., vol. 41, no. 2,
REFERENCES


Anonymous:1997:UUS


Anonymous:1997:UPP


Anonymous:1998:ARD


Anonymous:1998:CSIb


Anonymous:1998:EN


Anonymous:1998:Ea

Anonymous:1998:PCA


Anonymous:1998:SIb


Anonymous:1998:SIC

Anonymous. Smartcard invasion continues — security applications will be the spearhead for these “credit cards with brains.” BYTE Magazine, 23(4):112C–??, April 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Anonymous:1998:SUP


Anonymous:1998:TBF


Anonymous:1999:RDS


Anonymous:1999:AWS


Anonymous:1999:CCI

Anonymous, editor. Cool Chips II: An International Symposium on Low-Power and High-Speed Chips: Kyoto Research Park. Ky-
Anonymous:1999:DSC


Anonymous:1999:DSV


Anonymous:1999:KNT


Anonymous:1999:L

Anonymous. L'inuktitut. World-Wide Web document., 1999. URL http://colourlab.com/arctic/inuktitut.htm; http://www.culture.fr/edm/fr/index.html. Follow the navigation panel link “Les écritures” to inuktitut. The author observes that the syllabary used for the Inuit language, Inuktitut, was created at the end of the 19th Century by James Evans, a Wesleyan missionary, inspired by stenography. Originally intended for transcription of the Ojibway language, it was later used for Cree and Inuktitut; only these three languages have been written in this syllabary. Examples of the syllabary are shown in links that can be followed from this page; another alphabet table is shown in the colourlab.com URL.

Anonymous:1999:SFU


ANSI:1997:AXP

Anderson:1998:SFS

ANSI:1998:AXD

Anderson:1996:CCA

Abbott:1993:INT

Abreu:1994:DAI

Anderson:1998:LS
Andrasiu:1993:LTP


Aruliah:1985:PIE


Allen:1997:PSA


Aumann:1999:ITS


Arazi:1993:AEC

B. Arazi. Architectures for exponentiation over GD(2^n) adopted for smartcard application. *IEEE Transactions on Computers*, 42
Arensberg:1921:CD


Arensberg:1922:CSP


Adamson:1995:JSR


Adleman:1999:AMC


Adleman:1999:OMS


Adleman:1983:CCS


REFERENCES

Asokan:1998:OFE


Abdalla:1999:TMB


Atkins:1996:RPM


Akl:1983:CSP


Ateniese:1999:SOI


Atallah:1999:ATC


Atanasiu:1993:AEU


REFERENCES


REFERENCES


Aspray:1988:RCD
REFERENCES


**AufderHeide:1999:PGP**


**Ayoub:1968:EKR**


**Ayoub:1968:EEK**


**Ayoub:1981:EKR**


**Bernstein:1996:ISB**


**Blau:1996:VPA**

REFERENCES


[Bal99] Jimmy Ball. Web security basics with Apache:
REFERENCES


[Ban94] David Banisar. 1994 cryptography and privacy sourcebook: primary documents on U.S. encryption
REFERENCES


Barker:1984:CSG

Barker:1992:CSC

Barlow:1992:DPP

Barlow:1993:EFA
Barlow:1993:EFP


Barlow:1994:NSI


Barker:1995:CDT


Barlas:1996:NKD


Barron:1996:RTR


Barias:1997:NBP


Barnes:1999:ESJ

REFERENCES

138

Barron:2005:DWP


Baskerville:1993:ISS


Bastian:1995:CCE


Bassham:1998:ETA


Bauer:1997:DSM


Baxter:1997:SBE

Bowers:1960:PC

Bowers:1967:PC

Blakley:1979:RSA

Bennett:1985:UQC

Bennett:1989:EQC

Ben-Aroya:1994:DCL
Ishai Ben-Aroya and Eli Bi-


REFERENCES


[BBS85] E. Biham, A. Biryukov, Niels Ferguson, Lars R. Knudsen, Bruce Schneier, and Adi Shamir. Crypt-


REFERENCES


REFERENCES


[BC90] Andreas Bender and Guy Castagnoli. On the imple-
Beimel:1995:SSP


Blundo:1995:SRB


Blundo:1996:BES


Brassard:1996:YQC


Blakley:1998:C


Barker:1988:ECT


Bigun:1997:AVB

REFERENCES


Blair:1999:DRA


Baritaud:1993:SPK


Brucoli:1999:DHC


Bas:1998:SSB


Burwick:1998:MCC


Boyar:1991:CUS

J. Boyar, D. Chaum,
REFERENCES


[BCI85] Thomas Beth, N. Cot, and I. Ingemarsson, editors. *Advances in cryptology: proceedings of EUROCRYPT 84, a Workshop*
REFERENCES


with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Bellare:1996:MAU


Bellare:1998:MAD


Bellare:19xx:KMM


Bromley:1983:RFM


Bergadano:1998:HDC

Francesco Bergadano, Bruno

**Berbecel:1997:MTW**


**Birnbaum:1986:VPS**


**Borucki:1974:MNN**


**Brickell:1990:CIS**


**Burmester:1991:ALN**

REFERENCES

Bauspiess:1992:RCH

Brandt:1993:GPP

Bloecher:1994:FFS

Buerndt:1995:SEC

Blundo:1997:LBR

Bao:1998:SSS
REFERENCES


REFERENCES


Bondalapati:1999:DDE


Boneh:1998:ARG


BenAyed:1999:MFP


Blundo:1999:PSS


Bao:1998:MFA


Blundo:1993:IRS

C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the inform-

[Blundo:1996:IRS]


[Boneh:1999:FL]


[Boneh:1999:FPL]


[Bao:1997:DAT]


[Bao:1998:BPK]


[Blundo:1993:PSK]


[Burmester:1996:PRS]

M. Burmester, Y. G. Desmedt, T. Itoh, K. Saku-

Bellare:1997:CST


Boneh:1997:ICC


Benaloh:1994:OWA


Bosselaers:1997:RCH


Bellare:1998:RAN

REFERENCES


REFERENCES

Blundo:1998:SSS

Bright:1979:QRN

Barrett:1990:SDU

Beauquier:1992:TDP

Beaver:1993:HBS

Beaver:1996:ASE

Beaver:1997:CBC

Beaver:1997:PPE


Becker:1982:EDE


Beckett:1988:IC


Beckett:1997:ICP


Beck:1999:DPE


Beesly:1981:CIW


REFERENCES


REFERENCES


Berson:1997:FMP


Berg:1998:JQHd


Bergmann:2009:DKR


Beth:1983:CPW


Beth:1995:CCIb


Beth:1995:CCIa

Thomas Beth. Confidential communication on the Internet. Scientific American,
REFERENCES


Beth:1995:MST


Blaze:1996:MKC


Beimel:1997:RCP


Boneh:1997:EGS

REFERENCES

Balfanz:1999:HHC


Beimel:1999:RCP


Boneh:1999:EPK


Boneh:19xx:


Blaze:1999:KTM


Blum:1994:CPB

Blum:1988:NIZ


Blaze:1998:PSS


Blaze:1998:FTR


Boyd:1999:EEC


Beth:1992:PCS


Beth:1992:PKC

Thomas Beth, M. Frisch, and Gustavus J. Simmons, editors. Publ...

**Blundo:1996:TBC**


**Blundo:1998:GBC**


**Busch:1999:DWC**


**Blum:1985:EPP**

REFERENCES

Bellare:1990:NPD

Bellare:1993:DPK

Baldwin:1998:PPR

Boyapati:1999:KSD

Bellare:1994:ICC
REFERENCES


REFERENCES


Bellare:1997:PNG


Bellare:1997:PRN


Bender:1996:TDH


1996. CODEN IBMSA7. ISSN 0018-8670. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054106.html

Balkin:1994:CEC


Bellare:1995:XMN

REFERENCES

Bellare:1998:BVA


Bellare:1998:FBV


Bierbrauer:1996:OAR


Bierbrauer:1994:BRF


Benantar:1996:ACS


Bosselaers:1993:CWP


[BGV97a]

Bosselaers:1996:FHP


[BGV97b]
Beaver:1993:CPP


Baker:1998:LTC


Beygelzimer:1999:OWF


Bhimani:1996:SCI


Boeleoni:1999:SBM


Black:1999:UFS

J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway. UMAC: Fast and secure message au-
REFERENCES

Bar. URL http://link.
springer-ny.com/link/


Bubeck:1995:DSC
Bubeck:1995:DSC

[T. Bubeck, M. Hiller, W. Kuchlin, and W. Rosen-
[102x352]stiel. Distributed sym-
[181x340]bolic computation with
DTS. In Ferreira and Rolim
[FR95a], pages 231–248.
ISBN 3-540-60321-2. LCCN

Bayer:1993:IER

[102x168]D. Bayer, S. Haber, and W. S. Stornetta. Improving
the efficiency and reliability of digital time-stamping.
In R. M. Capocelli, A. De
Santis, and U. Vaccaro, edi-
tors, Sequences II: Methods in Communication, Secu-
[181x292]rity, and Computer Science,
[102x304]pages 329–334. Springer-
Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993.

Bellare:1998:MTF

[102x304]M. Bellare, S. Halevi, A. Sa-
[181x328]hai, and S. Vadhan. Many-
to-one trapdoor functions
[102x156]and their relation to public-
key cryptosystems. Lecture
Notes in Computer Science,
1462:283–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-

Bertilsson:1993:CPS

M. Bertilsson and I. Ingemarsson. A construc-

[181x256]tion of practical secret shar-
REFERENCES


Bao:1994:RAF

Bao:1995:BFA

Breitbach:1999:CCM

Bar-Ilan:1989:NFC


Biermann:1998:HKB

Biham:1991:CCC


Biham:1992:DCI

Eli Biham. *Differential cryptanalysis of iterated cryptosystems*. Dis-


E. Biham, editor. Fast software encryption: 4th International Workshop, FSE ’97, Haifa, Israel, January 20–22, 1997: proceedings, volume 1267 of
Biham:1998:CMM


Biham:1998:IOS


Biham:1999:CM


Biham:1999:NCA

REFERENCES

http://www.nist.gov/aes. No slides for the conference talk are available. [Bis88a]


Mark Birman. Accelerating cryptography in hardware: Public key, random number generation, symmetric key. In IEEE [IEE98b], page ?? ISBN ???. LCCN ???.


RIACS memorandum 88.3, NASA contractor report NASA CR-185397. [BQJ97]


Matt Bishop. Administrator’s guide to the digital signature facility “rover”. Technical report PCS-TR 90-153, Department of Mathematics and Computer Science, Dartmouth College, Hanover, NH, USA, 1990. [Bis90]

Matt Bishop. An authentication mechanism for USENET. In USENIX Association [USE91], pages 281–288. LCCN QA 76.76 O63 U84 1992. [Bis91]


REFERENCES

org/stamp/stamp.jsp?tp=&arnumber=1675571.


REFERENCES

[Buydos:1997:C]

[Biham:1998:CAXa]

[Biham:1998:CAXb]

[Biham:1998:TA]

[Biryukov:1998:DCC]

[Biryukov:1998:ICR]


[Buhler:1998:LBR]
Joe Buhler and Neal Kobliitz. Lattice basis

**Buchholz:1998:OGO**


**Brown:1993:IRD**


**Bellare:1994:SCB**


**Bellare:1998:LRB**


REFERENCES

stanford.edu/~dabo/papers/bbf.ps.gz.

Binsted:1999:CDS


Blatman:1975:MMC


Blakley:1979:SCK


Blahut:1983:TPE


Blakley:1985:ITF


Blanchard:1989:CSS


Blaze:1993:TMS

REFERENCES

Blackburn:1994:IRO

Blaze:1994:KME

Bleichenbacher:1996:GES

Blais:1998:SEP

Bleichenbacher:1997:SKP
REFERENCES


REFERENCES

0558/papers/0839/08390318.pdf.


REFERENCES


REFERENCES


**Boyer:1984:PCR**


**Blakley:1985:SRS**


**Beale:1989:EUR**


**Bellare:1990:NIO**


**Bellovin:1991:LKA**

REFERENCES

bell-labs.com/dist/kerblimit.
usenix.ps.Z; local --
- kerblimit.usenix.
ps.FTP - research.att.com:/dist/kerblimit.usenix.ps;
local - kerblimit.usenix.ps.

Brickell:1991:IID


Bellare:1992:HSG


Bleichenbacher:1994:DAG


Boyd:1994:DSK


Burns:1994:PSS

&arnumber=262121.

Boyd:1995:DAK

REFERENCES


[BMxx] Simon R. Blackburn and Sean Murphy. The num-
REFERENCES

ber of partitions in Pollard rho. Private communication., 19xx.


**Blackburn:1994:WPK**


**Bubak:1999:DHP**


**Biehl:1996:CPB**


**Barker:1998:TKL**

REFERENCES


CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


Book:1985:SNP


Book:1985:SNS


Book:1985:VTA

REFERENCES

Book:1985:CRE


Brickell:1988:CSR


Brickell:1992:CSR


Bo:1999:NMA


Ben-Or:1983:CSS

Michael Ben-Or, Benny Chor, and Adi Shamir. On

Boland:1995:WDI


Boland:1995:WDI

Ben-Or:1988:EPP


Ben-Or:1988:EPP

Bolignano:1997:TMC


Bolignano:1997:TMC

Bolignano:1998:IPB


Bolignano:1998:IPB

Bolignano:1998:IPM

D. Bolignano. Integrating proof-based and model-checking techniques for the formal verification of cryptographic protocols. Lecture
REFERENCES

Notes in Computer Science, 1427:77–??, 1998. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bond:1947:FSC [Bon47]

Boneh:1998:DDP [Bon98a]

Boneh:1998:DDH [Bon98b]

Booth:1981:ASU [Boo81]

Borman:1993:RTAa [Bor93a]
REFERENCES

//www.math.utah.edu/pub/rfc/rfc1416.txt. Obso-

Borman:1993:RTAb

D. Borman. RFC 1411: Tel-
net Authentication: Ker-
beros Version 4, Jan-
uary 1993. URL ftp://
ftp.internic.net/rfc/
rfc1411.txt; http://
www.math.utah.edu/pub/
rfc/rfc1411.txt. Status:
EXPERIMENTAL.

Borman:1993:RTAc

D. Borman. RFC 1416: Tel-
ftp.internic.net/rfc/
rfc1409.txt; ftp://
ftp.internic.net/rfc/
rfc1416.txt; http://
www.math.utah.edu/pub/
rfc/rfc1409.txt; http://
www.math.utah.edu/pub/
rfc/rfc1416.txt. Ob-
soletes RFC1409 [Bor93a]. Status: EXPERIMENTAL.

Borcherding:1995:NAR

M. Borcherding. Levels of authentication in distributed agreement. Lecture
Notes in Computer Science, 1151:40–??, 1996. CODEN
LNCS9D. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Borcherding:1996:LAD

M. Borcherding. Levels of authentication in distributed agreement. Lecture
Notes in Computer Science, 1151:40–??, 1996. CODEN
LNCS9D. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Bosworth:1982:CCC

Bruce Bosworth. Codes, ci-
phers, and computers: an
introduction to information
security. Hayden Book Co.,
Rochelle Park, NJ, USA,
259 pp. LCCN Z103.B58
1982.

Bosma:1990:PPC

W. Bosma. Primality Prov-
ing with Cyclotomy. Doc-
toral dissertation, Univer-
sity of Amsterdam, Am-
sterdam, The Netherlands,

Bosselaers:19xx:EFH

A. Bosselaers. Even faster
hashing on the Pentium.
In ????, page ?? ????,
????, 19xx. ISBN ????
LCCN ????. URL ftp://
ftp.esat.kuleuven.ac.
be/pub/COSIC/bosselaes/
pentiumplus.ps.gz. Pre-
sented at the rump session
of Eurocrypt'97, Konstanz,
Germany, May 12-15, 1997,
and updated on November
REFERENCES


REFERENCES

USA, 19xx. 21 + 18 + 61 + 57 pp.


REFERENCES

Boyd:1995:CCI


Boyd:1997:DSP


Boyko:1999:SPO


Beker:1982:CSP


Beker:1985:SSC

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Borst:1999:LCR


Beguin:1995:FSR


Beguin:1995:FSA


Bellare:1994:EAK


Blakley:1988:CBA


Beutelspacher:1991:EFS

REFERENCES

Bellare:1994:OAEa


Bellare:1995:OAE


Bellare:1995:PSS


Baldwin:1996:RRR


Bellare:1996:TCA


Bellare:1996:ESD

Bella:1997:FAK


Bellare:1997:MUR


Bellare:1999:CVC


Bracha:1987:ERR


Brassard:1988:MCT

Gilles Brassard. Introduction to modern cryptology. Publication 606, Université de Montréal, Département d’Informatique et de Recherche Opérationnelle, Montréal, Québec, Canada, 1987. 56 pp.
Brassard:1989:CCb


Brassard:1989:CCa


Brand:1990:PNU


Brassard:1990:ACC


Brassard:1990:CCH

REFERENCES

Branstad:1993:RNW

Brassard:1993:CM

Brassard:1994:CCQ

Bray:1994:UA

Brackin:1995:DCP

Brands:1995:LEC

Brands:1995:RBS


REFERENCES


REFERENCES


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB


Brundrett:1998:KAW


Bentley:1999:SOE


Bryan:1967:CA


Brillhart:1967:SFR


Brickell:1983:SRK

Benois:1986:CSE  

Biham:1990:DCD  

Brown:1990:DPT  

Beth:1991:NSE  

Biham:1991:DCD  
Biham:1991:DCFb


Biham:1991:DCFa


Biham:1991:DCS


Brickell:1991:SIB


Broscius:1991:EPH


Biham:1993:DCF


Biham:1993:DCD

[BS93b] Eli Biham and Adi Shamir. Differential Cryptanalysis
REFERENCES


Brassard:1994:SKR


Blaze:1995:MBC


Boneh:1995:CSF


Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy.

Bose:1995:ATV


Bruckstein:1995:SSD

REFERENCES


Barreiro:1997:PKC


Bakhtiari:1995:APL


Bakhtiari:1996:PAK


Bakhtiari:1997:MAC


Blake:1999:ECC


Bateman:1989:NMC

P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff,

The authors state: **NEW MERSENNE CONJECTURE.** If two of the following statements about an odd positive integer \( p \) are true, then the third one is also true. (a) \( p = 2^k + 1 \) or \( p = 4^k \pm 3 \). (b) \( M_p = 2^p - 1 \) is prime. (c) \( (2^p + 1)/3 \) is prime.

**Benaloh:1994:RFS**


**Boney:1996:DWA**


**Buchmann:1991:NTA**


REFERENCES

Barros:1998:DWS

Blunk:1998:RPE

Boneh:1998:BRM

Briguglio:1999:PGF

Beker:1985:KMS


REFERENCES

sored by the International Association for Cryptologic Research.

[Biehl:1997:TVC]

[Brandes:1998:UGL]

[Biryukov:1999:SA]


[Blake-Wilson:1999:UKS]

[Buchholz:1988:CQDc]
Boyd:1992:RDE


Bellare:1993:CCT


Beller:1993:BDK


Beller:1993:BDH


CBEMA:1981:ANS


CBEMA:1983:ANSb

REFERENCES

CBEMA:1983:ANSa


Cachin:1995:LSS


Cachin:1995:OSS


Cachin:1998:ITM


Cypher:1996:UAS


Caelli:1996:CKE


Caelli:1996:CPF

[Cae96b] W. Caelli. Cryptography: Personal freedom and law enforcement — is it possible to get agreement? Lecture
Cain:1996:TS
Adam Douglas Cain. Text steganography. Thesis (M.S.), University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, USA, 1996. vii + 90 pp.

Calvocoressi:1980:TSU

Callimahos:1989:TAZ

Campagne:1971:REC

Campbell:1987:MBC

Cammack:1988:MDE

Cao:1999:CAR

Capecchi:1994:TGR
REFERENCES

Carr:1997:WDA

Carter:1997:BLC

Carter:1997:CCC

Carr:1997:WDA

Carter:1997:BLC

Carter:1997:CCC

Carlsen:1994:OPA

Caronni:1995:AOR

Carson:1997:WDA

Carter:1997:BLC

Carter:1997:CCC

Carter:1998:CCC

Carlet:1993:PBF

Carlsen:1994:OPA

Caronni:1995:AOR

Carter:1997:WDA

Carter:1997:BLC

Carter:1997:CCC

Carter:1998:CCC

Carlet:1993:PBF
Carasik:1999:USS

Caswell:1995:EDA

Chren:1996:RDU

Clark:1981:ECC

Chen:1995:SIB

Canteaut:1998:NAF

Cai:1999:LBPa
Cai:1999:LBPb


Chun:1999:DMT


Chaum:1988:MUS


Canteaut:1999:NCA


Chen:1998:VIC


Carter:1995:DVD


Carlet:1998:CBF


Coppersmith:1985:AF

REFERENCES

Chuang:1991:MER

Cramer:1995:SSS

Cramer:1996:NGS

Chapman:1997:HHS

Clark:1998:OHA

Cramer:1998:ZPF
R. Cramer and I. Damgaard. Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free? Lecture Notes in Computer Science, 1462:
Curtin:1998:BFS

Compton:1999:PTC

Cramer:1999:EMC

Cowie:1996:WWN

Congedo:1995:SRS

Callas:1998:ROM
REFERENCES

rfc/rfc2440.txt. Status: PROPOSED STANDARD.

Chang:1995:SCP


Capocelli:1991:SSS


Carter:1998:KSI


Canetti:1997:DE


Chen:1995:PDP


Cramer:1994:PPK

REFERENCES


REFERENCES

[Coe:1995:DDC]

[CF95]

[CFGS99]

[CF99]

[CFG96]

[CFG*91]
REFERENCES


**Chor:1994:TT**


**Coppersmith:1996:LRR**


**Coppersmith:1996:LER**


**Canetti:1997:CES**


**Cramer:1996:MAS**

REFERENCES


Coppersmith:1975:GCA


Chor:1985:RRL


Cover:1987:OPC


Chor:1988:UBS


Catalano:1998:NES

Canetti:1999:ETP


Canetti:1999:AST


Chen:1996:TAP

REFERENCES


Clark:1994:BSP

Cai:1996:PEA

Carrel:1997:RIO

Chang:1997:SAG

Chen:1998:PFR
Corcoran:1999:SCB


Cordon:1999:AMD


Chaum:1979:UEM


Chaum:1981:UEM


Chandler:1983:IMC


Chaum:1983:ACP


Chaum:1985:HKS

[Cha85a] David Chaum. How to keep a secret alive extensible partial key, key safeguarding, and threshold systems. In Blakley and
REFERENCES


**Chaum:1985:SIT**


**Chang:1986:DKL**


**Chapman:1986:NFS**

Chaum:1990:SDA


Chaum:1991:SCS


Chaum:1992:AEPb


Chaum:1992:AEPa


Chaum:1993:NCB


Chambers:1994:TSC


Chandler:1994:IAF

REFERENCES

Chabaud:1995:SSC


Chaum:1995:DCS


Chaum:1998:Cb


Chadwick:1999:IWS


Chan:1999:WES


Chau:1999:QCE


Chesson:1973:CC


Cheswick:1992:EBW

Bill Cheswick. An evening with Berferd in which a cracker is lured, endured, and studied. In USENIX [USE92a], pages 163–174.
REFERENCES

Canetti:1997:MAC


Chiopris:1992:SBE


Chin:1999:HCD


Chin:1999:HDS


Christophides:1999:ODI


Canetti:1997:PSL


Chor:1986:TIP


**Chung:1998:DWCb**


**Christianson:1998:SPI**


**Christianson:1999:DSCb**


**Christianson:1999:SPI**


**Chuang:1989:NES**

Ta-Fu Chuang. Non-homomorphic encryption schemes and properties of Chinese remainder theorem. Thesis (Ph.D. in engineering), University of Wisconsin-Milwaukee, Mil-
REFERENCES


[CJM95] Don Coppersmith, Don B. Johnson, and Stephen M.

Coppersmith:1996:PMT


Charlwood:1998:EXA


Charlwood:1998:EXS


Chari:1999:TSA


Chari:1999:CNR


Chee:1991:CNP

Yeow Meng Chee, Antoine Joux, and Jacques Stern. The cryptanalysis of a new public-key cryptosystem based on modular knapsacks. *Lecture Notes in Computer Science,*
REFERENCES


Chor:1990:SSI


Chor:1993:CPT


Cole:1995:MDR


Chor:1998:PIR


Cox:1996:SRW

REFERENCES


[Chang:1997:PCM] Chin-Chen Chang and Der-Chyuan Lou. Parallel computation of the multi-exponentiation for cryp-


[Cla97] Three volumes. IEEE order plan catalog number 97CB36144.


REFERENCES


[Cli97] Bill Clinton. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part
Bill Clinton. *A legislative proposal: message from the President of the United States transmitting a legislative proposal to protect the privacy, security and safety of the people of the United States through support for the widespread use of encryption, protection of the security of cryptographic keys, and facilitation of access to the plaintext of data for legitimate law enforcement purposes*. United States Government Printing Office, Washington, DC, USA, September 21, 1999. 40 pp. Referred to the Committee on the Judiciary and Government Reform. Shipping list no.: 2000-0018-P.


REFERENCES


REFERENCES

uk/~fapp2/steganography/
bibliography/1045.html.

Chen:1998:DRT

[CM98] D. Chen and A. K. Mok. Design of a real-time SQL
engine in the distributed environment. Lecture Notes
in Computer Science, 1553:27–38, 1998. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Camenisch:1999:SEG

for generic group signature schemes. In Wiener
Wie99], pages 413–430. ISBN 3-540-66347-9. LCCN

Charlton:1999:DPM

[CM99b] P. Charlton and E. Mandani. A developer’s perspective on multi-agent sys-
tem design. Lecture Notes in Computer Science, 1647:

Christianson:1999:DSCa

[CM99c] Bruce Christianson and James A. Malcolm. Delegation and not-so smart cards
(position paper). Lecture Notes in Computer Science,
1550:154–157, 1999. CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/1550/15500154.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1550/15500154.p
df.

Coradeschi:1999:HMC

S. Coradeschi and D. Malec. How to make a challenging AI course enjoyable using
the RoboCup soccer simulation system. Lecture Notes in Computer Science,
1604:120–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1998:SCC

[CMKK98] Lily Chen, James L. Massey, Gurgen H. Khachatryan, and Melsik K. Kuregian. SAFER+:
Cylink Corporation’s submission for the Advanced Encryption
Standard. In National Institute of Standards and Technology [Nat98],
page 20. ISBN ??? LCCN ??? URL
http://csrc.nist.gov/
encryption/aes/round1/
conf1/saferp1s-slides.
pdf. Only the slides for the conference talk are available.

Cohen:1993:AAA

G. Cohen, Teo Mora, and Oscar Moreno, editors. Applied algebra,


S. Craver, N. Memon, B. L. Yeo, and M. M. Yen...
http://www.cl.cam.ac.uk/~fapp2/steganography/
bibliography/063115.html.

[CMYY98] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Re-
solving rightful ownership with invisible watermark-
ing techniques: Limitations, attacks and implications. [CNS99a]
IEEE Journal on Selected Areas in Communications,
16(4):573–586, May 1998. CODEN ISACEM. ISSN
0733-8716 (print), 1558-0008 (electronic). URL
http://www.cl.cam.ac.uk/~fapp2/steganography/
bibliography/072114.html.

[Crilly:1987:BPB] Tony Crilly and Shekhar Nandy. The birthday prob-
lem for boys and girls. The Mathematical Gazette,
71 (455):19–22, March 1987. CODEN MAGAAS. ISSN

[Coron:1999:SRSb] Jean-Sébastien Coron and David Naccache. On the
security of RSA screening. Lecture Notes in Computer Science, 1560:
197–203, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
bibs/1560/15600197.htm; http://link.springer-
ny.com/link/service/series/0558/papers/1560/15600197.

[Corrine:1999:ELA] Christophe Coupé, Phong Nguyen, and Jacques Stern. The
effectiveness of lattice attacks against low-exponent RSA. Lecture
Notes in Computer Science, 1560:204–218, 1999. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). URL http:


Cominsky:1987:CAP


Comba:1990:ECI


CSL:1994:DES


CSL:1994:EES


CSL:1994:SRC


CERT:1996:PSA


CEC:1997:EST

REFERENCES


REFERENCES

Coppersmith:1984:FEL


Coppersmith:1987:C


Coppersmith:1989:AID


Coppersmith:1994:DES


Coppersmith:1994:ACS


Coppersmith:1994:ACS


Charnes:1995:CSE

REFERENCES


REFERENCES


[CP88] David Chaum and Wyn L. Price, editors. Advances
REFERENCES


Camion:1991:KHF


Chaum:1993:WDO


Chung:1998:DWCa

REFERENCES

CODEN DTPEEL. ISBN ????. ISSN 0747-668X.
LCCN ????. IEEE catalog number 98CH36160.

Charney:1997:PSC


Cheon:1998:TEA


Camenisch:1995:BSB


Chor:1988:KTP


Carroll:1988:CC


Chor:1988b


Chaum:1991:USD

David Chaum and Sandra Roijakkers. Uncondi-
REFERENCES


CREPEAU:1990:VDS


CREPEAU:1997:ECP


CONTINI:1999:IAS


CHAUM:1998:Ca


CRYPTO:1981:ACP


CRYPTOBYTES:1995:C


REFERENCES

CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic).

Chen:1997:NIC


Coppersmith:1997:PAP


Canteaut:1998:COM


Cramer:1998:PPK


Coradeschi:1999:ASV


Chaum:1989:SCF


Csirmaz:1995:SSM

[Csi95] L. Csirmaz. The size of a share must be large. *Lecture

Coppersmith:1994:ABP


Chang:1997:GSS


Chen:1999:TPS


Collberg:1999:SWM


Cox:19xx:NST


Chao:1994:DEC

Currier:1998:MPT


Cusick:1995:CPK


Cusick:1996:BNFa


Cusick:1997:CRN


Calvelli:1993:ARS


Chabaud:1995:LBD


Cohn:1999:MC


Chaum:1991:CSU

David Chaum, Eugène van Heijst, and Birgit Pfitzmann. Cryptographically strong undeniable signatures, unconditionally se-


Chin-Chen Chang and Tzong-Chen Wu. A smart card oriented password authentication scheme based


[CZ90] Zhen Fu Cao and Bao Dong Zheng. A discussion on knapsack cryptosystems


concealed by a matrix cover. 


**DeMillo:1983:ACC**


**Dittmann:1998:MSW**


**Daemen:1995:HFC**


**Daemen:1998:MSK**


**Daemen:1999:RAI**

REFERENCES

http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm;
http://www.nist.gov/aes. No slides for the conference talk are available.

Damgaard:1990:ACE


Damgaard:1991:DPP


Damgaard:1991:ACE


Damgaard:1991:TPP


REFERENCES


REFERENCES

QA267.A1 L43 no.196.
article&issn=???&volume=0&issue=0&page=393.CRYPTO84: a Workshop on the
Theory and Application of Cryptographic Techniques,
held at the University of California, Santa Barbara,
August 19–22, 1984, sponsored by the International
Association for Cryptologic Research.

Davies:1991:ACE
Donal Watts Davies, editor. Advances in cryptology — EUROCRYPT ’91:
Workshop on the Theory and Application of Cryptography
Techniques, Brighton, UK, April 8–11, 1991: proceedings,
volume 547 of Lecture Notes in Computer Science.
Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
3-540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic).
LCCN QA76.9.A25 E964 1991. Rev. and expanded papers from the
meeting which was sponsored by the International Association for
Cryptology Research (IACR) and others.

Davies:1995:KPR
Don Davis. Kerberos plus RSA for world wide Web security.
In USENIX Association [USE95c], pages 185–188. ISBN 1-880446-74-
usenix.org/publications/library/proceedings/ec95/davis.html.

Davis:1996:CDP
Don Davis. Compliance defects in public key cryptography.
In USENIX Association [USE96g], pages 171–178. URL http://www.
usenix.org/publications/library/proceedings/sec96/davis.html.

David:1998:WWI
Charles David. A World War II German army field
cipher and how we broke it. In Deavours et al.
shml. Third volume of selected papers from issues of
Cryptologia.

Dav91
Dav95
Dav96
Dav98a
Dav94
Davies:1998:E


Davies:1998:NIH


Davies:1998:LCM


Dawson:1993:CSG


Dawson:1996:CSR


Denning:1981:SRR


denBoer:1988:CF

REFERENCES

Denning:1989:EET


Denning:1996:TKE


DenBoer:1991:ALT


DenBoer:1994:CCF


Daswani:1999:EEC


Boer:1991:ALT

[dBB91] Bert den Boer and Antoon Bosselaers. An at-


DHalluin:1999:ASR


DeWin:1996:FSI


DeJonge:1986:ASR


Desmedt:1995:MNA


Desmedt:1995:MNS


Desantis:1994:HSF


Davio:1985:EHS


DDJStaff:1998:NVS

DDJ Staff. News and views: a Standard Linux? cryptography contest; drives get smaller and smaller; Perl conference; really embedded systems; programmer

[DDJ98b] DDJ Staff. News and views: Computing olympiad; the public’s right to know; smart cards; more Y2K; why Rome burns; bio-computing; new infrared standards; national medals awarded. Dr. Dobb’s Journal of Software Tools, 23(3):18, March 1998. CODEN DDJOEB. ISSN 1044-789X.

[DDJ98c] DDJ Staff. News and views: Going west; end of an era; electronic messaging available; putting your money where your mouth is; Amiga redux; un-scrambling encryption; ergonomic research; PPTP bug. Dr. Dobb’s Journal of Software Tools, 23(8):16, August 1998. CODEN DDJOEB. ISSN 1044-789X.

[DDJ98d] DDJ Staff. News and views: In your face; who invented the microprocessor?; mixed media; but where will they go for spring break?; quantum computing lives; E-commerce continues to grow...; ...but will smart cards play a role? Dr. Dobb’s Journal of Software Tools, 23(12):18, December 1998. CODEN DDJOEB. ISSN 1044-789X. URL http://www.microcomputerhistory.com/.


DDJStaff:1998:NVc
[DDJ98g]  DDJ Staff. News and views: The secret story of nonsecret encryption; Netscape news; key escrow woes; fingerprint IC. *Dr. Dobb's Journal of Software Tools*, 23(4):18, April 1998. CODEN DDJOEB. ISSN 1044-789X. Discusses a claim by the British GHCQ agency to have invented public-key cryptography in unpublished classified work prior to the RSA and Diffie–Hellman publications.

DDJStaff:1998:NVd

DDJstaff:1999:NVR

DePaoli:1998:WBS

Denny:1994:FR

Delaigle:1996:DW
REFERENCES


REFERENCES


DeSantis:1994:SSP


DeSantis:1994:KCQ


DeSantis:1999:NIZ


Darmstaedter:1998:LCS


DeVries:1953:SMC

DeAlvare:1990:HCC


DeDecker:1993:USK


DeSchutter:1993:TFA


DeSoete:1993:PKC


DeSantis:1995:ACE


DeDecker:1998:ICS


DeSantis:1998:E


DeSchutter:1998:TFA

REFERENCES


[Dem88] A. Caner Demirdogen. Flaw detection methods based on

Demytko:1994:NEC


Denning:1979:SPC


Denning:1979:EOS


Denning:1984:DSR


Denning:1984:FEA


Denniston:1986:GCC

REFERENCES


[Den95] Dorothy Elizabeth Robling Denning. Encryption is a sword that cuts two ways, 1995. 1 videocassette (42 min.).


[Des90b] Yvo G. Desmedt. Making conditionally secure cryp-


Desmedt:1996:EBB


Desmedt:1996:SPF


Desel:1998:BLA


Desmedt:1998:C


Desmedt:1998:SRR


Desfray:1999:ADP


Desmedt:1999:ES


Deugo:1997:CTS


[Dawid:1992:BSC] H. Dawid and G. Fet-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Daemen:1994:WKI

Diffie:1976:NDC

Diffie:1977:ECN

Davis:1985:NRI

Davis:1985:UFS

Dawson:1996:AAS
REFERENCES


REFERENCES


Damm:1995:MH


DiGiorgio:1997:ISC


DiGiorgio:1997:JDJ


DiCrescenzo:1999:SAC


DiCrescenzo:1999:SPH


DiazdeLeon:1991:PIE


Ding:1996:CRT

[C. (Cunsheng) Ding, Ting i (Dingyi) P’ei, and Arto


Ding:1994:DCD


Dixon:1994:SSS


Damm:1998:CRT


Dessmark:1993:MDD


Deavours:1985:MCM


Deavours:1989:CMH


Dusse:1991:CLM

REFERENCES


of Software Tools, 22(10): 54, 56-57, October 1997. CODEN DDJOEB. ISSN 1044-789X.


[DeMillo:1982:CP] Richard A. DeMillo, Nancy A. Lynch, and Michael J. Mer-
Dammgard:1993:ACE


Ding:1997:LMS


DeMillo:1983:PDS


Duc:1997:PAF


DeWin:1998:PSS


Denning:1981:MMK


Dongarra:1995:TSS

J. J. Dongarra, H. W. Meuer, and E. Strohmaier. TOP500 supercomputer

**Denazis:1999:DIO**


**DAngelo:1994:SEM**


**Dwork:1993:PPC**


**Dwork:1994:EEU**


**Dossis:1995:FSR**


**Dossis:1995:OVH**

REFERENCES


[Ding:1997:TFS]


[DO99]


[Dittmann:1998:IWE]


[Dobbertin:1995:EMC]


[Dobbertin:1995:ASA]


[Desmedt:1986:CTA]

REFERENCES


[Santis:1991:PRP]


[Davida:1998:HC]


[Davida:1998:HSC]


[DeWin:1998:ECP]

Descombes:1999:MVK

DeWaleffe:1993:BLP

Delos:1994:IBS

Desmedt:1985:DOI

deRooij:1994:SPD
Peter de Rooij. On Schnorr’s preprocessing for digital signature schemes.
REFERENCES

CODEN LNCS-9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650435.htm;

Rooij:1994:SPD

Peter de Rooij. On Schnorr’s preprocessing for digital signature schemes.
CODEN LNCS-9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer-ny.com/link/service/series/0558/bibs/0765/07650435.htm;

Rooij:1995:EEU

Peter de Rooij. Efficient exponentiation using precomputation and vector addition chains.
CODEN LNCS-9. ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/link/service/series/0558/bibs/0950/09500389.htm;

Daemen:1998:APR

J. Daemen and V. Rijmen. AES proposal: Rijndael.

Desel:1998:PTP

J. Desel and W. Reisig.
Place/transition Petri nets.
CODEN LNCS-9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Daemen:1999:EBC

In USENIX [USE99c], page ??
Drea:1999:NEB

Dray:1998:RNJ

Drach:1999:RDO

Dreher:1979:PSC

deRaadt:1999:COO

Dror:1989:SCG

Droste:1996:NRV


REFERENCES

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

Dittmann:1997:ETT


Dittmann:1997:TAT


Dutertre:1997:UPE


David:1998:SIC


Dwork:1998:CZR


Durham:1999:BOO

Dittmann:1998:RMV


Dave:1995:CBS


Desai:1999:CSC


Durand:1999:DCC


Detombe:1993:CLC


DeSolages:1998:EFO


DiGiorgio:1998:JDS

DuBoulay:1999:DDT


DuCarlet:1644:CCV


Dufner:1998:ACH


Duhoux:1990:DBA


Dumey:1994:CQD


DeVivo:1998:ISA


DeDecker:1992:HID

REFERENCES


REFERENCES


Ding:1991:STS


DeSantis:1990:DPS


DeSantis:1991:CAN


DeSantis:1991:DPSa

 REFERENCES

link/service/series/0558/bibs/0473/04730412.htm;

[Desmedt:1991:WUS]

[Desmedt:1991:AUS]

[Dai:1998:WIF]

[Eberle:1993:HSI]

[Easter:1999:PES]

[Ecker:1982:MGE]
A. Ecker. Über die mathematischen Grundlagen einiger Chiffrierverfahren. (German) [On the mathematical foundations of some cryptosystems]. Computing, 29(4):277–287,
REFERENCES


**Ecker:1983:FSR**


**Ecker:1985:STS**


**ECMA:1996:EAP**


**Ellis:1975:PKC**


**Edwards:1915:CCT**


**Epstein:1956:FBC**


**El-Gamal:1985:PCS**

T. El-Gamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Informa-
REFERENCES


Ellison:1999:PSK


Ergun:1999:NLC


Estrella:1999:DED


Eigenthaler:1984:CGA


Evans:1974:UAS


EFF:1998:CSE

www.eff.org/descracker/


[Ell98] C. Ellison. Cryptographic random numbers. Techni-
REFERENCES


**Ellis:1999:PPN**


**Elvin:1987:CWW**


**Even:1993:CCS**


**Eades:1998:GDC**


**Ehrsam:1978:CKM**


**Ezawa:1998:ATS**


**Endler:1997:PSU**


**Eng:1999:ECT**


Jonathan Erickson. Dr. Dobb’s news and views: Linux trademark issue settled; Inslaw ruling rejected; push over?; reading signs for the blind; free speech I; free speech II; Y2K insurance. *Dr. Dobb’s Journal of Software Tools*, 22 (11):16, November 1997. CODEN DDJOEB. ISSN 1044-789X. URL http://www.iplawyers.com/text/linux.htm. A patent and trademark claim dispute on the name Linux has been resolved in favor of Linus Torvalds and the Linux community. A U.S. District Court Judge has ruled that source code is protected speech under the First Amendment to the U.S. Constitution, and that the U.S. Commerce Department acted illegally in requiring academics to obtain a government license before discussing cryptographic research with scholars on the Internet.

Erskine:1999:CDD

Emerald:1997:NPC

Effelsberg:1998:SAI

Escott:1999:AEC

Estell:1980:BW

Ettinger:1998:SGE

Evertse:1992:WNR
Jan-Hendrik Evertse and Eugène van Heyst. Which new RSA-signatures can be computed from certain given RSA-signatures? Journal of Cryptology, 5(1):
REFERENCES


Even:1985:CSW


Evertse:1991:WNR


Evertse:1993:WNR


Falk:1988:DST


Fancher:1996:SCa


Farago:1967:BSS


Farago:1969:BSS

Ladislas Farago. The broken seal: the story of Op-
REFERENCES


REFERENCES

**Ferland:1994:PBC**


**Firoiu:1999:LER**


**FontdecabaBaig:1998:PNL**


**Fan:1999:DFS**


**Frankel:1992:PRT**


**Frankel:1993:NEH**


**Frankel:1993:NHG**

REFERENCES

Feak:1983:SIS


Feiestel:1973:CCP


Feigenbaum:1991:ACC


Feit:1993:TIA


Feit:1996:TIA


Feigenbaum:1998:C

[Fei98] J. Feigenbaum. Crypto ’91. Lecture Notes in
REFERENCES


Friedman:1957:SCE


Feghhi:1999:DCA


Fung:1998:PAE


Fuchsberger:1996:PKC


Fuchsberger:1996:PCS


Frankel:1997:ORP


Frankel:1997:PR

[FGMY97b] Yair Frankel, Peter Gemmell, Philip D. MacKenzie, and Moti Yung. Proactive RSA. In Kaliski [Kal97c], pages 440–?? CODEN
REFERENCES

335


REFERENCES

Franks:1997:REH


Frederickson:1984:PRT


Frieze:1988:RTI


Fiat:1990:BR


Fiat:1994:TT

REFERENCES

ac.uk/~fapp2/steganography/

Fiat:1997:BR


Filby:1995:FUB


FIPS:1993:APG


FIPS:1993:SHS


FIPS:1994:EES


Fischlin:1997:ICM


Fischlin:1998:CLP

Franz:1998:MMA


Franz:1996:CBS


Friedman:1996:AFR


Freeman:1997:MCN


Fellows:1993:KKI

REFERENCES


[FLL96] Benjamin Fried and Andrew Lowry. BigDog: Hi-


[FM85] Steven Fortune and Michael Merritt. Poker protocols. In Blakley and
REFERENCES


CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Feigenbaum:1991:DCC


[FM91]


Feustel:1998:DU1


Fairfield:1985:LRN


CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of

Faihe:1998:ADR

California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

**Fagundes:1999:EGA**


**Frey:1999:TPD**


**Fairfield:1985:LDE**


**Frankel:1998:RED**


**Fiat:1994:BE**

REFERENCES


REFERENCES


[Fol99]

[FOM91]

[Fujioka:1991:IBS]

[Fujioka:1993:PSV]

[Forte:1999:BUT]

[Foster:1982:CM]
REFERENCES


REFERENCES


[ Fra99] Matthew Franklin, editor. Financial cryptogra-
REFERENCES


[Fri99]


[Fre94]

William F. (William Frederick) Friedman. The cryptanalyst accepts a challenge. War Department, Office of the Chief Signal Officer, Washington, DC, USA, 1939. 24–36 pp. LCCN ????

[Fri39a]


[Fri39b]


[Fri41]


[Fri42]

William F. (William Frederick) Friedman. Codes
and ciphers (cryptology). Encyclopaedia Britannica, Chicago, IL, USA, 1956. 8 pp.

**Friedman:1963:SLC**


**Friedman:1966:AMC**


**Friedman:1976:EC**


**Friedman:1976:EMC**


**Friedman:1976:CCA**


**Friedman:1987:ICA**


**Friedman:1992:MC**


**Friedman:1992:MCP**


N. Ferguson and B. Schneier. Cryptanalysis of Akelarre. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419, Au-
REFERENCES


REFERENCES


REFERENCES

**Funny:1993:KM**


**Futrelle:1973:BTM**


**Feldman:1999:HSH**


**Fischer:1991:MSK**


**Frankel:1995:CIL**


**Frankel:1995:EES**

Franklin:1995:BWS


Frankel:1997:CEE


Frankel:1998:DPK


Frankel:1998:RMU


Frankel:1999:CRA


Frankel:1999:ASD


Gritzalis:1998:SIS

REFERENCES

Gabriel:1982:VPI


Gaddy:1998:CC


Gomez-Albarran:1999:MCL


Gaines:1939:ECS


Gaines:1940:ECS


Gaines:1943:ECS


Gaines:1944:CSC


Gaines:1956:CSC


[Gal45a] Joseph Stanislaus Galland. An historical and analytical bibliography of the literature of cryptology. Northwestern University studies in the humanities no. 10. Northwestern University, Evanston,
REFERENCES


Ganesan:1996:HUK

Ganesan:1996:YSS

Gardner:1977:MG

Garlinski:1979:IEW

Garlinski:1980:EW

Garay:1994:RMA
REFERENCES


[Gar97b] Lee Garber. News briefs: Binary version could bring VRML into the mainstream. FCC jumps into Internet fray. Java and floating-point math. Intel to design NDRAM. battle over net telephony. vendors seek fast modems. US permits export of strong en-


REFERENCES


Gaudin:1997:VBJ


Gilmour-Bryson:1982:CDT

[GB82] A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino [CM82], pages 451–467. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.I4 I58. From Computing Reviews: “The article reports on the progress of an historical study using a computer for statistical analysis. The subject of the study is a mass of trial depositions of the Knights Templar. The purpose of the project is to find statistical regularities in the large amount of testimony and to create a model for similar studies. The Order of the Knights Templar, founded around 1100, was the first Christian military order. After the Crusades, in the early fourteenth century, 127 articles of accusation were brought against the order, including charges of idolatry, sacrilege, and sodomy. The data being studied are the responses of 900 men to each of 127 accusations. The article details the accusations and the way in which the responses are being coded. The statistical package SAS (Statistical Analysis System) will be used. Examples of the results to be sought are: tallies of guilty/innocent responses, tallies of offenses committed versus seen versus heard about, and correlations between, for example, age and other responses. Depositions that differ markedly from the average response will be identified.”.

Golshani:1998:NDW


Geoffroy:1993:APF

[GBC93] M. Geoffroy, R. Bjones, and


Lee Garber and David Clark. News briefs: Judge rejects US restrictions on export of encryption; Intel, HP unveil Merced chip; Java wars heat up; AOL acquires CompuServe subscribers; confusion in the DVD marketplace; 'amazing grace' heads to sea; PC firms back down on convergence; business use will drive Internet growth; company offers $1-million prize for hackers.


P. Geffe. How to protect data with ciphers that are really hard to break. Electronics, 46(1):99–101, 1973. ISSN 0883-4989. This cipher was later broken by [Sie85].
REFERENCES


REFERENCES

Gero:1999:NME

Gero:1999:RRA

Ghezzi:1993:RSS

Goldreich:1997:EDE

Goldreich:1997:PKC

Gabber:1999:SPC

Goldreich:1985:CAR
[GGM85] Oded Goldreich, Shafi Goldwasser, and Silvio Mi-

CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Goldreich:1986:HCR


Gabber:1997:HMP


Gilbert:1998:ASR


Gittler:1995:DSS

Frederic Gittler and Anne C. Hopkins. The DCE secu-
rity service. *Hewlett-Packard Journal: technical in-
formation from the laboratories of Hewlett-Pack-
HPJOAX. ISSN 0018-1153. URL http://www.hp.com/
hpj/95dec/dec95_41.pdf; http://www.hp.com/hpj/
toc-12-95.html.

Michael Gehrke and Thomas Hetschold. Management of a public key 
certification infrastructure — Experiences from the DeTeBerkom project BM-
1, 1996. CODEN CNISE9. ISSN 0169-7552 (print), 1879-2324 (elec-
elsevier.com/cas/tree/
store/comnet/sub/1996/
28/14/1647.pdf.

Guang Gong and Lein Harn. Public-key cryp-
tosystems based on cubic fi-
nite field extensions. *IEEE 
Transactions on Information Theory*, 45(7):2601–
2605, 1999. CODEN IET-
TAW. ISSN 0018-9448 (print), 1557-9654 (elec-
tronic).

R. Gennaro, S. Halevi, and T. Rabin. Secure hash-
and-sign signatures without 
the random oracle. *Lecture 
Notes in Computer Science*, 
1592:123–??, 1999. CODEN 
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).

K. Gopalakrishnan, D. G. Hoffman, and D. R. Stinson. 
A note on a conjecture concerning symmetric resilient 
functions. *Information Pro-
cessing Letters*, 47(3):139–
143, September 14, 1993. 
CODEN IFPLAT. ISSN 
0020-0190 (print), 1872-
6119 (electronic).

Zvi Galil, Stuart Haber, and Moti Yung. A se-
cure public-key authenti-
cation scheme. *Lecture 
Notes in Computer Science*, 
434:3–??, 1990. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/0434/04340003.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340003.
pdf.

N. Gilboa and Y. Ishai. Compressing cryptographic 
resources. In Wiener

Gibson:1990:SCD


Gibson:1991:EGC


Gibson:1995:SDG


Gibson:1996:SGP


Gifford:1981:CSI


Gilder:1997:APD


Giles:1998:EFS

REFERENCES

Gilboa:1999:TPR


Girard:1999:WSP


Givierge:1925:CC


Givierge:1932:CC


Givierge:1978:CC


Garey:1979:CIG

Michael R. Garey and David S. Johnson. Computers and Intractability: a
REFERENCES


Gifford:1982:CSI


Gennaro:1996:RES


URL http://link.springer-ny.com/link/service/series/0558/bibs/1109/11090157.htm; http://link.springer-ny.com/link/service/series/0558/papers/1109/11090157.pdf. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Gennaro:1996:RTD


URL http://link.springer-ny.com/link/service/series/0558/tocs/t1070.htm; [GJKR99]
http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Gennaro:1999:SDK

REFERENCES

Garay:1999:AFO


Goldreich:1996:CZP


Garay:1999:AOC


Goresky:1995:FRB


Glenn:1998:RNE


Goldschlag:1999:BCC


Gurses:1995:VCT


Goldwasser:1999:PTU


REFERENCES

encryption/aes/round1/conf2/agenda-final.pdf; http://www.nist.gov/aes. No slides for the conference talk are available. [Gle57]

Gladwin:1999:CCS


Gruhl:1996:EH


URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054134.html

Georgoudis:1998:TPF


Only the slides for the conference talk are available. [Gle87]

Gleason:1957:ECP


Gleason:1986:ECP


Gleason:1987:PIC


Gonzalez:1999:RMT

REFERENCES

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

**Gallant:1999:IPP**


**Gamage:1999:EMA**


**Goldwasser:1982:PEH**


**Goldwasser:1984:PE**


**Goodman:1985:NTK**


**Godlewski:1990:KMA**

REFERENCES

Golic:1991:NCC


Galvin:1993:RSP


Gordon:1993:MPC


Garfinkel:1995:PPGb


Gennaro:1995:VSS


Girault:1997:SFR


GomezdeSilvaGarza:1999:EAC


Goldwasser:1985:PSS


Goldwasser:1988:DSS

REFERENCES

SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.


[Goldreich:1991:PYN] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the Association for Computing Machinery*, 38(3):691–729, July 1991. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/116852.html. They show that for a language $L$ in $NP$ and a string $w$ in $L$, there exists a probabilistic interactive proof that efficiently demonstrates membership of $x$ in $L$ without conveying additional information. Previously, zero-knowledge proofs were known only for some problems that were in both $NP$ and $co-NP$. A preliminary version of this paper appeared in *Proc. 27th Ann. IEEE Symp. on Foundations of Computer Science*, 1986, under the title “Proofs that yield nothing but their validity and a methodology of cryptographic protocol design.”.
REFERENCES

Gemmell:1994:CIA

Goettfert:1995:GLB

Gray:1995:PCT

Guerrero:1995:CHB

Goldwasser:1993:ISN

Golic:1995:EPC

Goldreich:1996:SPS
Oded Goldreich and Rafail Ostrovsky. Software protection and simulation on

**Golic:1996:CCC**


**Grosky:1996:NAH**


Goldberg:1990:MUA


Goldwasser:1990:ACC


Goldwasser:1990:SPS


Gollmann:1992:ATC


Gollmann:1994:CCC


Goldreich:1995:FCF


Golic:1995:LCS

REFERENCES

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


Goldreich:1997:FMCa


Goldreich:1997:FMCb

Goldwasser:1997:NDC


Golic:1997:CAA


Goldwasser:1998:C


Golic:1998:RAS


Goldreich:1999:MCP


Golic:1999:SCe


Golomb:1999:CNS

REFERENCES


University of Paris, Sorbonne.

**Gordon:1993:DDT**


**Guajardo:1997:EAE**


**Ghodosi:1999:RCN**


**Ghodosi:1996:CHG**


**Gladychev:1998:CRJa**


**Goth:1999:NBG**


**Ghodosi:1999:RCN**


REFERENCES


REFERENCES

Guillou:1991:PTA

Goeker:1999:DUC

Gennaro:1997:HSD

Grantham:19xx:FPP

Greenfield:1994:DPP
REFERENCES


REFERENCES


[Girault:1994:LCH]

[Gulliver:1994:ITA]

[Gritzalis:1997:CPO]


QA76.9.A25 C79 1999
Bar. URL http://link.
springer-ny.com/link/
1666/16660372.htm; http://
link.springer-ny.com/
papers/1666/16660372.
pdf.

[GTG94] P. Gramata, P. Trebat-


Maria Victoria Guarin. A study of information authentication and a proposed digital signature scheme. Thesis (M.S. in Engin.), University of Texas at Austin, Austin, TX, USA, 1990. viii + 135 pp.

REFERENCES


REFERENCES

[392]

Gurnsey:1997:CT


Gustafson:1996:SAS


Gutmann:1996:SDD


Guthery:1998:SC


Gutmann:1998:SGP


Gutmann:1999:DCS


Guy:1976:HFN

R. K. Guy. How to factor a number. In Hartnell and Williams [HW70], pages 49–89.
REFERENCES


cryptanalysis of “cryptograph type C-36,” provided with six key wheels, 27 slide bars, the latter having moveable projections, single or multiple. A. B. Teknik co., Stockholm, Sweden, 1938. 10 pp.

Gysin:1996:OKC

Garzon:1991:CGG

Haller:1994:RIA

Hendessi:1994:SAA

Hollaar:1996:LRD

Haddon:1984:BRS

Hagelin:1998:SHC
REFERENCES


[Har91] S. Harari. A correlation cryptographic scheme. Lec-
REFERENCES


Hart:1994:DSC


Harpes:1996:CIB


Harris:1996:E


Haskett:1984:PAU


Haastad:1987:OWP


Haastad:1988:SSM


Haselberger:1995:DRB


Hasan:1999:LTB

M. A. Hasan. Look-up table based large finite field multiplication in memory constrained cryptosystems
REFERENCES

Hawkes:1998:DLW


Hutter:1999:DCI


Hughes:1999:PFS


Hu:1995:YCE

Ping Hu and Bruce Christianson. Is your computing...

**Hwang:1995:SSA**


**Hwang:1996:DSS**


**Hwang:1998:EMS**


**Hernandez:1999:DAV**


**Hwang:1996:SAA**


**Hwang:1996:AES**


**He:1996:HFR**

J. He and E. Dawson. How to fairly reconstruct

**He:1996:NKE**


**He:1992:IKB**


**Huang:1998:FAI**


**Hedberg:1997:FIC**


**Hartung:1998:DWM**


**Heidel:1676:JTP**

Wolfgang Ernesto Heidel. *Johannis Trithemii primo Spanheimensis deinde Divi Jacobi Penopolitani abbatis Steganographia: quae hucusque a nemo intellecta sed passim ut supposititia, perniciosa, magica & necromantica rejecta, elusa, damnata & sententiam inquisitionis passa, nunc tandem vindicata, reserata et illustrata ubi post vindicias Trithemii clarissime explicantur conjurationes spirituum ex Arabicis, Hebraicis, Chaldaicis & Graecis spirituum nominibus juxta quosdam conglobatae, aut secundum alios ex barbaris & nihil significantibus verbis concinnatae: deinde solvuntur & exhibentur artificia nova
steganographica a Trithemio in literis ad Arnoldum Bostium & Polygraphia promissa, in hunc diem a nemine capta, sed pro paradoxis & impossibilibus habita & summe desiderata. Wormatiense, Moguntiae. Sumptibus Joannis Petri Zubrodt, 1676. 8 + 394 (or 396) + 4 pp. LCCN Z103 .T84 1676. Includes Heidel's life of Trithemius and his vindication of the Steganographia.


**Heintze:1996:SDF**


**Hellman:1979:MPK**


**Hellman:1981:ACA**


**Held:1993:TSD**


**Helleseth:1994:ACE**

Held:1998:ARU  

Held:1998:LET  

Helleseth:1998:E  

Henry:1981:BJB  

Hong:1998:DAS  

Herlestam:1978:CRS  

Hershey:1981:DLP  
J. E. (John E.) Hershey. The discrete logarithm pub-
lic cryptographic system. NTIA report 81-81, PB82-
130097, U.S. Dept. of Com-
merce, National Telecom-
munications and Information Administration, Wash-
ington, DC, USA (??), September 1981. iv + 40
pp.

Jeffrey Stuart Hersch. Digital signature analysis of radar reflections for the as-
seSSment of concrete bridge deck deterioration. Thesis (M.S.), Massachusetts Insti-

E. Hess. Public-key cryptosystems based on elliptic curves — an evolution-
ary approach. Lecture Notes in Computer Science, 1355:
118–??, 1997. CODEN LNCS9D. ISSN 0302-9743
(print), 1611-3349 (electronic).

James D. Hollan and James D. Foley, editors. ACM Multimedia '97: pro-
cedings: November 9-13, 1997, Seattle, Washington,
USA. ACM Press, New York, NY 10036, USA,


[HGD85] Frank Hoornaert, Jo Goubert, and Yvo Desmedt. Efficient hardware implementation of the DES. In Blakley and Chaum
REFERENCES


CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


[HUSE99] Dirk Husemann and Reto Hermann. OpenCard:


REFERENCES


[Hil31] Lester S. Hill. Concerning certain linear transformat-
REFERENCES


and M. Yung. Proactive public key and signature systems. In ????, [???97], page ??.

**Herzberg:19xx:PPK**


**Herzberg:1995:PSS**


**Hillenbrand:1999:SDW**


**Hong:1997:IAU**


**Huehnlein:1998:CBN**


**Huehnlein:1998:CBN**

Detlef Hünnlein, Michael J. Jacobson, Jr., Sachar Paulus, and Tsuyoshi Takagi. A cryptosystem based on non-maximal imaginary

**Herlea:1999:SBR**


**Harn:1999:EPE**


**Halevi:1997:MSM**


**Hevia:1998:STD**


**Halevi:1999:PKC**

REFERENCES


Halfmann:1999:ESP


Haynes:1999:VDS


Hevia:1999:STD


Hromkovic:1994:CDC


Harpes:1995:GLC


Hachez:1999:IFA


Hall:1999:CS

C. Hall, J. Kelsey, V. Rijmen, and B. Schneier. [HKRS99]
REFERENCES


Haber:1995:HDD


Hofmeister:1997:CKS


Hofmeister:1997:COS


Hall:1998:CS


He:1988:SDK


Hauser:1992:VMA


Harn:1993:SGS

HERZBERG:1993:PRC


HAN:1999:VFG


HWANG:1999:CDC


HWANG:1995:TAN


HWANG:1996:SCW


HUGHES:1996:QCU


HOHL:1993:SIH

W. Hohl, X. Lai, T. Meier, and C. Waldvogel. Security of iterated hash func-
REFERENCES


Hunter:1983:ERA


Hule:1988:RCW


Hafner:1991:COH


Hafner:1995:COH


Hedlund:1996:CFP

Patric Hedlund and Gary Meyer. Computers, freedom, and privacy, 1996. 13 videocassettes (930 min.).

Harpes:1997:PC

REFERENCES

Hoogeboom:1997:CPT


Hoyle:1998:SKE


Horster:1995:MRM


Harkavy:1998:IPP


Harper:1993:PKC


Horvath:1994:PPM

[HMvT94] Tamás Horváth, Spyros S. Magliveras, and Tran van
REFERENCES


[HO96] P. Hawkes and L. O’Connor. On applying linear cryptanalysis to IDEA. Lecture
REFERENCES


REFERENCES

Horng:1995:PAU


Horng:1998:AAP


Horster:1999:SSK


Herzberg:1987:PPS


Hung:1994:FRD


Handschuh:1998:SCC


Horn:1998:APF


Handschuh:1999:SDK


**Handschuh:1999:SDT**


**Heileman:1999:IWC**


**Hernandez:1998:SML**


**Hoffstein:1998:NRB**


**Holland:1982:GSA**


**Hwang:1990:PKA**

Hollander:1996:KWS


Harrison:1976:POS


Hruby:1995:QDQ


Hruby:1995:QQC


Hruby:1996:SCI


Hruby:1998:TQC


Hruby:1999:SUD

P. Hruby. Structuring UML design deliverables. Lecture Notes in Computer Science, 1618:278–??, 1999. CODEN LNCSD9. ISSN 0302-9743
REFERENCES

Hernandez:1999:CLM


Haastad:1985:CST


Hammer:1987:EUH


Hardjono:1989:TCB


Hardjono:1990:SKS


Haber:1991:HTD


Hinsley:1993:CIS

REFERENCES


G. Hornauer, W. Stephan, and R. Wernsdorf. Markov ciphers and alternating groups. Lecture Notes
REFERENCES

423


Hauser:1996:MBI


Hinsley:1979:BISA


Heys:1995:ACS


Hada:1998:EZP


Hada:1999:RBO


Handschuh:1999:DOE


Huang:1988:APE


Huber:1991:SCC

Klaus Huber. Some considerations concerning the se-


REFERENCES

Husain:1994:EI

Husemann:1999:SCD

Hulaas:1998:MLI

Hardy:1975:ITN

Hartnell:1976:PFM

Hardy:1979:ITN

Huthnance:1988:UPP

Hotchkiss:1991:ASI
R. S. Hotchkiss and C. L. Wampler. The auditori-

ization of scientific information. In IEEE [IEE91],
Hsu:1997:DWV


Hsu:1998:DBW


Hsu:1998:MWD


Hwang:1998:AUS


Hwang:1991:CGO


Hwang:1992:AOT


Hwang:1992:EIB

Hwang:1992:EIK


Hwang:1992:PGO


Hwang:1993:SSD


Hwang:1997:CKA


Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE

Hall:1998:BPPa


Hall:1998:BPPb


Hohl:1994:SIH


Harn:1993:GUS


Harn:1993:PKC


Hwang:1995:TPE


Hirose:1998:ADK

Hirose:1998:ADH


Hsieh:1998:H


Hsieh:1999:OWH


Hardjono:1993:PDM


Ibbotson:1997:CPI


Anonymous:1993:CCA


IBM:19xx:PSP


IEEE:1974:ASS

IEEE, editor. *15th Annual Symposium on Switching and Automata The-
REFERENCES

IEEE, October 14–16, 1974, the University of New Orleans. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1974.

IEEE:1979:ASF


IEEE:1980:PSS


IEEE:1981:CLC


IEEE:1982:ASF


IEEE:1982:CFP


IEEE:1983:PSS


REFERENCES

Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. Three volumes. IEEE catalog no. 87CH2520-5.


REFERENCES


IEEE, editor. Proceedings: IEEE Infocom ’92, the conference on computer communications, one world through communications, eleventh annual joint conference of the IEEE Computer and Communications Societies, Florence, Italy. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. Three volumes. IEEE Computer Society order number 2860. IEEE catalog number 92CH3133-6. [IEE92c]


[IEEE:1996:ASF]


[IEEE:1996:AIC]


[IEEE:1996:IIC]


[IEEE:1996:PICb]


[IEEE:1996:PICa]

REFERENCES


IEEE:1996:SCR


IEEE:1997:SIC


IEEE:1997:ACS


IEEE:1997:ICD


IEEE:1997:IICb

[IEE97d] IEEE, editor. 1997 IEEE International Conference
REFERENCES


REFERENCES

7, 0-8186-8184-5 (case).
Three volumes. IEEE Computer Society order number
PR08183. IEEE order plan
catalog number 97CB36144.

[IEE97i] IEEE, editor. Proceedings
/ 1997 IEEE Symposium
on Security and Privacy,
May 4–7, 1997, Oakland,
California. IEEE Computer
Society Press, 1109 Spring
Street, Suite 300, Silver
Spring, MD 20910, USA,
1997. ISBN 0-8186-7828-
3 (softbound), 0-7803-4159-
7 (casebound), 0-8186-7830-
5 (microfiche). LCCN QA
76.9 A25 I43 1997.

[IEE97j] IEEE, editor. Proceedings,
International Conference on Image Processing:
October 26–29, 1997, Santa
Barbara, California. IEEE
Computer Society Press, 1109 Spring
Street, Suite 300, Silver
Spring, MD 20910, USA,
0-8186-8184-5 (casebound),
0-8186-8185-3 (microfiche).
Three volumes. IEEE order
plan catalog number 97CB36144.

[IEE97k] IEEE, editor. Proceedings
of 1997 International
Conference on Information,
Communications, and
Signal Processing, 9–12
September 1997, Singapore:
theme: Trends in information systems engineering and wireless multimedia communications. IEEE Computer Society Press,
1109 Spring Street, Suite
300, Silver Spring, MD 20910,
0-7803-3677-1 (microfiche).
Three volumes. IEEE catalog
number: 97TH8237.

Technical Committee on
Computer Communications,
editor. Proceedings, 22nd annual Conference on Local Computer Networks: LCN '97: November 2–5,
1997, Minneapolis, Min-
nesota. IEEE Computer So-
ciety Press, 1109 Spring
Street, Suite 300, Silver
Spring, MD 20910, USA,
1997. ISBN 0-8186-8141-1,
0-8186-8142-X (casebound),
0-8186-8143-8 (microfiche).
ISSN 0742-1303. LCCN
TK5105.5 .C82 1997. IEEE
Computer Society Press
order number PR08141.
IEEE Order Plan number
97TB100179.

[IEE98a] IEEE, editor. 39th Annual
Symposium on Foundations
IEEE:1998:HCC


IEEE:1998:IIC


IEEE Computer Society Order Number PR08557.

IEEE:1998:LPA

IEEE Computer Society.
REFERENCES


usenix.org/publications/library/proceedings/usenixnt98/itoi_slides. [I96]

Itoi:1999:PSS


Itoi:1999:SIK


Itoi:1999:SUF


IAB:1996:RII


Igarashi:1999:ITP


Izu:1998:PSE


Israel:1983:AOS

[J. E. Israel and T. A. Linden. Authentication in office system internetworks.
REFERENCES


[Imp92] Russell Graham Impagliazzo. Pseudo-random generators for probabilistic algorithms and for cryptography. Thesis (Ph.D. in mathematics), Department of Mathematics, University of California, Berkeley, Berke-


**Impagliazzo:1989:ECS**

**Ito:1999:DPS**

**Ingemarsson:1998:E**

**Instenes:1995:MAA**
Norwalk, CT 06855, USA, February 1987. vii + 197 pp.


REFERENCES


Irwin:1998:RWD


Ingemarsson:1991:PSS


Ikram:1997:CSE


Ikram:1999:UIN


Ito:1987:SSS


ISO:1997:ITS


Isselhorst:1990:UFP


Itoh:1991:CFI


Iversen:1991:CSC


Ingemarsson:1981:UAS


Imai:1998:PKC

REFERENCES


[Jac87] T. H. Jackson. From number theory to secret codes.


Jac96

REFERENCES


[Jan99] P. Janecek. Applying visualization research towards design. *Lecture Notes in
REFERENCES


Jarecki:1996:PSS

Jarvis:1997:GB

Jaspan:1996:DWE

Jaeger:1993:LCC

Jan:1998:PWP

Johnson:1991:TSS

Johnson:1991:CCA

Jeffery:1986:GCC
Keith Jeffery. The Government Code and Cypher
REFERENCES


**Jensen:1999:GDT**


**Jenkins:19xx:IFC**

Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Website, 19xx. URL http://burtleburtle.net/bob/rand/isaacafa.html. ISAAC (Indirection, Shift, Accumulate, Add, and Count) is based on cryptographic principles, and generates 32-bit random numbers. ISAAC-64 is similar, but requires 64-bit arithmetic, and generates 64-bit results.

**Jevons:1874:PS**


**Joyce:1990:IAB**


**Joux:1995:PAA**


**Jian:1999:SDM**


**Jolitz:1991:PUI**

Jolitz:1995:RNS


Johnson:1998:ESS


Johnson:1998:CPE


Johnson:1998:SIC


Johansson:1999:FCA


Johansson:1999:IFC


Jakobsen:1997:IAB

REFERENCES

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

Jun:1999:IRN

Jonker:1999:VTK

Jones:1975:ESP

Johnson:1994:HKD

Juels:1997:SBD

Jurgensen:1984:SRI

Jackson:1993:CAG
REFERENCES

Janwa:1996:MPK

Johnson:1996:AEE

Jurisic:1997:ECC

Jakobsson:1999:IMI

Johnson:1994:CDM

Jackson:1994:MTS

Jackson:1995:ESS
REFERENCES

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

**Jackson:1995:SMS**


**Jerichow:1998:RTM**


**Jarecki:1997:EMS**


**Joesang:1998:SMA**


**Johns:1984:RAS**


**Jakobsson:1996:DVP**

rfc/rfc912.txt; ftp://ftp.math.utah.edu/pub/rfc/rfc931.txt. Obso-
leted by RFC0931 [St.85]. Status: UNKNOWN.

Johnston:1989:BDC


Johnson:1990:EDE


Johns:1993:RIP

POSED STANDARD.

Johansson:1994:CPA


Johnson:1995:ACD

REFERENCES


[Johnson:1996:LP]

[Johnson:1997:SP]

[Johnson:1997:SPS]

[Johnson:1999:LES]

[Jolitz:1995:PB]

[Jones:1978:WWB]

Jones:1978:MSW


Jones:1986:DEB


Jones:1990:PKC


Josse:1885:CSA


JCryptology:1988:JCJ


Juels:1996:HCC


Jaeger:1999:FCD


Joye:1997:PFR


[Joye:1998:CRT]


[JQBD97]


[JS93a]


[Jourgensen:1996:TFC]


[Joux:1993:CAK]


[Johansson:1995:AIA]

REFERENCES


Jan:1997:SEV

Jan:1997:SIE

Juenemann:1981:DES

Juels:1999:TTS
REFERENCES


Ji:2001:CAF


Jakobsson:1996:OAB


Joye:1998:IBS


Kompella:1991:FCC


Kent:1998:RIA


Kent:1998:RIE

Kahn:1967:CSSa

Kahn:1967:CSSb

Kahn:1974:C

Kahn:1983:KCS
Kahn:1984:COS


Kahn:1991:SER


Kahn:1996:HS


Kahn:1996:CSS


Kahn:1998:EC


Kahn:1998:PHI


Kahn:1998:RMU

volume of selected papers from issues of Cryptologia.

**Kak:1983:EMP**


**Kak:1984:MPK**


**Kak:1985:EEC**


**Koc:1996:ACM**

Çetin Kaya Koç, Tolga Acar, and Burton S. Kaliski, Jr. Analyzing and comparing Montgomery multiplication algorithms — assessing five algorithms that speed up modular exponentiation, the most popular method of encrypting and signing digital data. *IEEE Micro*, 16(3):26–33, June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

**Kaliski:1984:AWA**


**Kaliski:1985:WAE**

REFERENCES

Kaliski:1991:MMD


Kaliski:1992:MAC


Kaliski:1993:SES


Kaliski:1993:ZBA


Kaliski:1995:MIA


Kaliski:1997:IPS


Kaliski:1997:PNG


Kaliski:1997:ACC

[B] Burton S. Kaliski, editor. Advances in Cryptology, CRYPTO ’97: 17th annual international cryptol-
REFERENCES


Kaliski:1998:RPCa


Kaliski:1998:RPCb


Kaliski:1998:RPCc


Kaliski:1998:EDF

rfc/rfc2315.txt. Status: INFORMATIONAL.

Kaliski:1998:REC


Kaliski:1999:ESP


Kaneshige:1996:ITC


Kaps:1998:HSF


Karger:1985:ADA


Karger:1987:LDP


Kari:1989:CBP

REFERENCES


Kaufman:1996:DWC


Kawai:1987:LAI


Kay:1995:CTE


Krishnakumar:1992:HTE


Krawczyk:1996:HKM


Krawczyk:1997:RHK


Klein:1989:STR


Karp:1988:SDN

[KBN88] Bennett C. Karp, L. Kirk Barker, and Larry D. Nel-


REFERENCES


Kravitz:1999:CAC


Kundur:1997:RDI


Kundur:1998:DWU


Kunkelmann:1998:VEB


Kharitonov:1993:CHD


Karaorman:1999:CRJ

Kobara:1996:LVS


Kobara:1997:SSM


Katsumoto:1999:DPL


Kilian:1988:FCO


Kim:1993:CLB


Kippenhahn:1997:VBG

REFERENCES

Kippenhahn:1999:CBH


Kippenhahn:1999:VBG


Kirby:1995:RPK


Kak:1977:SEU


Kocher:1999:DPA


Kurosawa:1995:NBA


Kuwakado:1996:NRT


Kelm:1997:NK

[KK97] S. Kelm and K. P. Kos sakowski. Zur Notwendigkeit der Kryptographie (German) [on the necessity of cryptography]. *Datenschutz*
REFERENCES


Kabatianskii:1997:DSS


Kramer:1999:FCD


Kothari:1984:CMW


Kilian:1994:FKE


Kilian:1995:FCR


Knudsen:1995:NAA


Klein:1990:FCS

Kannan:1988:PFN


Klupsch:1999:ARR


Kurosawa:1988:CSP


Kurak:1992:CNI


Kang:1993:PRR


Kim:1996:ACA

REFERENCES

Knudsen:1996:IDA

Knudsen:1999:CIS

Kosuda:1997:SED

Kosuda:1998:OMC

Kaufman:1998:DWF

Kasahara:1999:NPK

Knudsen:1999:RAP

Koscielny:1999:QBP


Kanda:1998:ECC


Kobayashi:1999:FEC


Konheim:1980:ICP


Koyama:1991:NPK

REFERENCES

Kande:1999:AUD


Karn:1995:REC


Karn:1995:RET


Kohl:1994:EKA


Knut:1969:SNM

REFERENCES


References


[Kob97] M. Kobayashi. Digital
watermarking: Historical roots. IBM Research Report RT0199, IBM Japan, Tokyo, Japan (??), April 1997. ??–?? pp. URL
http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073142.html


Kocher:1995:CDR


Koc:1996:RHI


Kocher:1996:TAI


Kocher:1999:B


Koeune:1999:CRI

aes. No slides for the conference talk are available.

**Kohl:1990:UEK**


**Koland:1995:SSH**


**Konheim:1981:CP**


**Konheim:1985:CAE**


**Konheim:1989:RMC**


**Kong:1995:DES**

REFERENCES


Koopman:1986:OES

Kurosawa:1995:TIK

Kurosawa:1995:CIT

Koops:1997:CRE

Kopooshian:1997:DCE

Kornerup:1993:HRM
0-8186-3861-3 (microfiche).
ISSN 0018-9340 (print),
1557-9956 (electronic). LCCN
QA 76.9 C62 S95 1993.
URL http://www.acsel-
lab.com/arithmetic/arith11/
papers/ARITH11_Kornerup.
pdf. IEEE Transactions on

Korner:1996:PC

T. W. (Thomas Will-
liam) Körner. The Plea-
sures of Counting. Cam-
bridge University Press,
Cambridge, UK, 1996.
ISBN 0-521-56823-4 (pa-
paperback), 0-521-56087-X
(hardback), x + 534 pp.
URL http://www.loc.
gov/catdir/description/
camo29/97108334.html;
http://www.loc.gov/catdir/ toc/camo29/97108334.html

Koscielny:1983:PRD

Czesław Koscielny. Pro-
gramowa realizacja działań
w ciałach skończonych
do zastosowań w technice
ekodowania korekcyjnego i
kryptografii, volume 61.
11 of Prace naukowe In-
stytutu Cybernetyki Tech-
nicznej Politechniki Wro-
cławskiej; Seria Mono-
grafie. Wydawn. Politech-
niki Wrocławskiej, Wro-
cław, Poland, 1983. ISBN
???? ISSN 0324-9786. 115
pp. LCCN QA76.9.A251 K6
1983. zl93.00. Title on p.

Kurosawa:1994:NSS
Kaoru Kurosawa, Koji
Okada, Keiichi Sakano,
Wakaha Ogata, and Shi-
geo Tsujii. Nonperfect se-
cret sharing schemes and
matroids. Lecture Notes
in Computer Science, 765:
126–??, 1994. CODEN
LNCS9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/0765/07650126.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0765/07650126.
pdf.

Koshiba:1997:CLT
T. Koshiba. Computational
learning theoretic crypt-
analysis of language theo-
retic cryptosystems. Lecture
Notes in Computer Science,
1334:28–??, 1997. CODEN
LNCS9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Koshiba:1999:UPN
Takeshi Koshiba. Un-


REFERENCES

Koyama:1995:FRT


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kozen:1996:RSS


Kim:1989:PRP


Kwan:1993:GPT

REFERENCES


REFERENCES


REFERENCES

Kaliski:1995:LCU

Kaliski:1995:MAM

Kaliski:1995:SUR

Kaliski:1996:MEW


Kilian:1996:HPA

Knudsen:1996:NAL

Kankanahalli:1998:CBW


Knudsen:1999:DFC


Kolliopoulos:1999:NLT


Kolliopoulos:1999:NLT


Kranakis:1986:PC


Krawczyk:1990:HPC


Kraitz:1993:DSA


REFERENCES


Knudsen:1998:DSR


Kumar:1999:CCB


Kruh:1998:WWS


Knudsen:1999:TDS


Kordes:1989:UMC


Kelsey:1997:CPO


Kurosawa:1997:DSP

REFERENCES


REFERENCES

501

Kelsey:1999:AST


Kipnis:1999:CHP


Kemp:1996:CPC


Kemp:1999:NDA

J. Kelsey, B. Schneier, and N. Ferguson. Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In Sixth Annual Workshop on Selected Ar-


REFERENCES

//www.counterpane.com/key_schedule.html.


REFERENCES


Kucera:1992:GES


Kuhn:1998:CIS


Kuijk:1991:RSE


Kukorelly:1999:VCH


Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC

REFERENCES


REFERENCES


Kaul:1999:IBP


Kirstein:1992:PAS


Konrad:1999:SDK


Kwan:1993:SAD


Kwan:1997:DIE


Kaliski:1995:SRE

Kaliski:1995:DLC


Kaliski:1997:SRE


Kaliski:1998:SRE


Kaliski:19xx:DLC

[B. S. Kaliski, Jr. and Y. L. Yin. On differential and linear cryptanalysis of the RC5 encryption algorithm. Accepted to Crypto ’95., 19xx.]

Kwok-Yan:1992:TAD


Kurosawa:1998:SBC


Kwok-Yan:1992:FAA

Kasami:1982:KMS


Koch:1995:TRH


Levien:1998:ART


Lampson:1991:ADS


Lampson:1992:ADS


Lacy:1993:CCS


Laffin:1964:CCS

Lagarias:1984:KPK

Lagarias:1984:PAS

Lagarias:1990:PNG

Lai:1995:ALS

Lakshmivarahan:1983:APK

Lai:1992:DSB
[Lai92] Xuejia Lai. On the design and security of block ciphers. Hartung-Gorre Verlag, Konstanz, Switzerland, 1992. ISBN 3-89191-573-X. xii + 108 pp. LCCN QA76.9.A25L335 1992. This is the author’s Ph.D. dissertation, “Secret-key block ciphers are the subject of this work. The design and security of block ciphers, together with their application in hashing techniques, are considered. In particular, iterated block ciphers that are based on iterating a weak round function several times are considered. Four basic constructions for the round function of an iterated cipher are studied.”.
REFERENCES


REFERENCES

Langford:1996:WST


Lange:1997:SCI


Landrock:1998:TOC


Landrock:1999:PTU


Lassek:1985:CCA

[Las85] Teresa A. Lassek. Cryptology and the computer age. Thesis (Honors), University of Nebraska at Omaha, Omaha, NE, USA, 1985. 58 pp.

Lassak:1992:SRP


Lauer:1981:CSC


Lawton:1998:NBS

[Law98] George Lawton. News briefs: Sun joins tetherless network fray; private doorbells: Solution to encryption controversy; Web extensions promise distributed computing; Wall


Mark Lomas and Bruce Christianson. Remote booting in a hostile world: to whom am I speaking?

**Lee:1996:IAP**


**Lin:1996:BCC**


**Lin:1996:CBC**


**Lee:1997:AES**


**Lou:1997:PTL**


**Lou:1998:FMM**


**Lacan:1999:SOE**

REFERENCES


[Leary:1987:CSM] Penn Leary. *The Cryptographic Shakespeare: a monograph wherein the poems and plays attributed to William Shakespeare are proven to contain the en


REFERENCES


[Lev61a] Jack Levine. Some applications of high-speed computers to the case $n = 2$ of alge-


Fredrik Laurin and Calle Froste. Secret Swedish e-mail can be read by the U.S.A. Web site, November 1997. URL http://catless.ncl.ac.uk/Risks/19.52.html.


REFERENCES


Landwehr:1984:SMM

Lee:1998:ZNP

Lee:1999:STI

Lichtenthal:1994:CBT

Lidl:1985:CBP

Lidl:1990:SMA

Lieberherr:1981:UCD
REFERENCES

Liebl:1993:ADS

Lim:1998:CNB

Lim:1999:RVC

RFC0989

RFC1040

[Lin87]
[Lin88a]
[Lin88b]
[Lin98]
[Lin99]
REFERENCES


soletes RFC1113 [Lin89a]. Status: PROPOSED STANDARD.

RFC1421


Linn:1993:RCA


Linn:1996:IRC


Linn:1996:RKV


Linnartz:1998:TCC


Lippit:1993:PIC


Lipton:1994:CNF


IEEE Catalog No. 94TH8100.
REFERENCES

Abeles:1998:KVC


Lipmaa:1999:ICM


Litant:1987:BRC


Lindsay:1997:BC

[LJWH97] Charles Lindsay, Derek Jacobi, Hugh Whitemore, and Andrew Hodges. Breaking the code, 1997. ISBN 1-56442-662-9. Based on the play of the same title by Hugh Whitemore, and on the book, “Alan Turing: the enigma”, by Andrew Hodges. Originally broadcast as an episode of the PBS television series, Mobil masterpiece theatre Credits: Director of photography, Robin Vidgeon; editor, Laurence Mery-Clark; introduced by Russell Baker Performers: Derek Jacobi, Alun Armstrong, Richard Johnson, Harold Pinter, Amanda Root, Prunella Scales The story of Alan Turing, British mathematical genius and designer of the computer that broke the German Enigma code during World War II, whose admission to homosexuality at a time when it was illegal presented problems for him, for his family, for his colleagues, and for the State’s preoccupation with national security Close-captioned.

Laih:1996:CEE


Lee:1999:MRF


**Lindau:1994:CPP**


**Linnartz:1998:MFA**


**Lenstra:1993:DNF**


**Liaw:1993:OAA**


**Lim:1994:AMA**

Chae Hoon Lim and Pil Joong Lee. Another method for attaining security against adaptively chosen ciphertext attacks. *Lecture Notes in Computer Science*, 773:
REFERENCES

Lim:1994:MFE


Lim:1995:SPS


Lim:1995:SPP


Lee:1997:PNB


Lim:1997:DSA

REFERENCES

Lim:1998:SPK

Lee:1999:NAD

Langelaar:1998:RSS

Luo:2010:PAE

Laih:1989:NTS

Lam:1996:EGE

Lenstra:1990:NFS
REFERENCES


Lai:1991:MCD


Lee:1999:DPP


Longo:1990:GCC


Leonard:1997:CSP


Lautemann:1999:DCA


Lidl:1994:IFF

REFERENCES


REFERENCES

Lomas:1994:ENT


Lomas:1997:SPI


Long:1991:PAA


Long:1992:UDE


Loshin:1997:CGP

[Los97] Pete Loshin. Cryptography gets personal — six products that promise to secure your data, both over the Internet and on your desktop. BYTE Magazine, 22(11):121–??, November 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Loshin:1998:PEC


Lowe:1995:ANS


Lowe:1996:BFN


REFERENCES


Lacy:1998:IPP

Luby:1986:PRP

Luby:1988:HCP

Leverrier:1989:TDF

Lagarias:1988:UEP
REFERENCES

Lai:1996:AHH


Lysyanskaya:1998:GBD


Lai:1993:FCC


Lange:1981:TC


Lu:1989:SCI


Lloyd:1992:RPA


Lin:1997:LNU

Lasker:1998:ACC


Luby:1998:CBB


Lamport:1982:BGP

[LSP82] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4 (3):382–401, July 1982. CODEN ATPSDD. ISSN 0164-0925 (print), 1558-4593 (electronic). They proved that Byzantine agreement cannot be reached unless fewer than one-third of the processes are faulty. This result assumes that authentication, i.e., the crypting of messages to make them unforgeable, is not used. With unforgeable messages, they show that the problem is solvable for any \( n > t > 0 \), where \( n \) is the total number of processes and \( t \) is the number of faulty processes.

Livens:1995:CCI

REFERENCES

Leung:1985:SCT


Leong:1991:UPE


Linnartz:1998:MPM


Langley:1999:ACI


Laih:1995:SLF


Lioen:1988:OMA


Lu:1979:EGC

Shyue Ching Lu. The existence of good cryptosys-

Lu:1980:AEG


Lackey:1995:SMS


Lubi:1996:PCA


Lucks:1995:HEI


Lucks:1996:FLC


Lucks:1996:FLR


Lucks:1997:SRK

REFERENCES


REFERENCES


Lujan:1998:AMD


Lunt:1990:EK


Lutz:1998:NBM


Linnartz:1998:ASA


Langelaar:1996:CPM


Langelaar:1997:RLM

REFERENCES

uk/~fapp2/steganography/bibliography/063145.html

Long:1988:DLH


Li:1991:JAE


Lervik:1996:IDS


Lucks:1999:RKE


Lin:1996:GTU


Lenstra:1995:KES


MacPherson:1987:CUN


MacLaren:1994:CPN


Mache:1998:SCT


Madsen:1992:GCD

Jørgen Bo Madsen. The greatest cracker-case in Denmark: The detecting, tracing, and arresting of two international crackers. In *USENIX* [USE92b], pages 17–40. ISBN 1-880446-46-4. LCCN ?????

Maes:1998:TPH


Maher:1996:CBK


McDonald:1995:OTP

Daniel L. McDonald, Randall J. Atkinson, and Craig Metz. One-Time Passwords in Everything (OPIE): Experiences with building and
Mandelbrot:1960:BRJa


Manasse:1995:MPE


Manjunath:1998:IPA


Moriai:1996:KLP


Mao:1997:PVP


Mao:1998:GCS


Marsh:1970:CSS

Marsh:1970:MEC


Marion:1976:ANB


Marion:1995:WGT


Marks:1995:PEI


Markoff:1996:MIS


Martin:1997:IEI


Markantonakis:1998:CSM


Marks:1998:BSC

Martyna:1999:NNA


Massey:1983:LFC


Mastrovito:1989:VDM


Mastrovito:1991:VAC

Massey:1994:SKB


Massey:1994:SKB


Massacci:1997:BSP


Massacci:1999:DRT

Massey:1999:OSD


Matyas:1979:DSO


Matyas:1991:KHC


Matsui:1993:LCM


Matsui:1994:FEC


Matsui:1994:LCM


Matsui:1995:CBO

[Mat95] M. Matsui. On correlation between the order of

**Matsui:1996:NSB**


**Matsui:1997:NBE**


**Matsumura:1999:DTE**


**Maurer:1990:FGS**


**Maurer:1991:NAD**


REFERENCES

Maurer:1996:UGT


Maurer:1996:ACE


Maurer:1997:ITS


Mauriello:1997:TTC

REFERENCES


REFERENCES


Moskowitz:1992:CAA


Mitchell:1996:CKU


McCarty:1975:AFP


REFERENCES

McCurley:1996:CIL


McCane:1998:ICS


McHugh:1992:EBD


McIvor:1985:SC


McKee:1999:SFF


Millan:1998:HDC


Millan:1999:BFD

McMahon:1996:RGA


Madson:1998:REC


Main:1999:HCB


Moreno-Diaz:1994:SIE


Messerges:1999:IPA


Meador:1920:KCE


Meadows:1995:FVC

REFERENCES

**Mead:1998:BJA**


**Meek:1998:AAM**


**Meersman:1999:SOT**


**Meijer:1981:NCM**


**Meijer:1983:CCC**

Henk Meijer. Cryptology computational complexity and applications. Thesis (Ph.D.), Queen’s University, Ottawa, ON, Canada, 1983. 2 microfiches (179 fr.).

**Meijer:1985:MEN**


**Meijer:1992:SSA**


**Meier:1994:SIB**

REFERENCES


communications and Information Theory.

**Menezes:1995:ECC**


**Menicocci:1995:SAC**


**Mersenne:1644:CPM**

[Mer44] Marin Mersenne. *Cogitata Physica-Mathematica ... Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theorica, practica. Et Mechanica phaenomena. Ballistica et acontismologia*. Antonii Bertier, Paris, France, April 1, 1644. [30], 40 [24], 41–370, [16], 96, [8], 138, [34] + 40 pp. URL http://www.mersenne.org/prime.htm; http://www.mersenne.org/status.htm. Three volumes. This is the book that introduced the conjecture that numbers of the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

**Merkle:1978:SCI**

Ralph C. Merkle. Secure communications over insecure channels. *Communications of the Association for Computing Machinery*, 21(4):294–299, April 1978. CODEN CACM-A2. ISSN 0001-0782 (print), 1557-
REFERENCES


REFERENCES


REFERENCES


Madson:1998:RUHb


Mackenzie:1998:LPS


Merkle:1978:HIS


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

Merkle:1981:SME


Michels:1996:RDS


McPherson:1998:CRH


REFERENCES


[Mil76] G. L. Miller. Reimann’s hypothesis and tests for pri-
REFERENCES


**Miller:1985:PES**


**Miller:1986:UEC**


**Millen:1987:CCC**


**Mills:1987:RDP**


**Millikin:1992:ECC**


**Miller:1995:HWK**

Millan:1996:LOA


Miller:1996:CME


Matsumoto:1993:VIA


Mintzer:1997:EIDa


Misarsky:1997:MAU


Misarsky:1998:HDR


Mitchell:1976:EAD

James Melvin Mitchell. Encryption algorithm for data security based on a polyalphabetic substitution scheme and a pseudorandom number generator. Thesis (M.S.), University of Tennessee, Knoxville,

Mitchell:1989:MDS

Mitchell:1992:AMI

Mitchell:1992:CCI

Miyaguchi:1990:FCC

Miyaguchi:1991:FCF

Miyaji:1993:ECS
REFERENCES

Miyaji:1993:OEC


Miyano:1993:MEN


Miyaji:1996:MRS


Miyaji:1999:ECC


Mjolsnes:1993:PCP


Morii:1992:PSP


Moskowitz:1994:CCH


Mazières:1999:SKM

David Mazières, Michael Kaminsky, M. Frans

Maibaum:1999:SRS


Miyazaki:1999:TFI


Monge:1967:NMC


Maulucci:1987:HAC


Mao:1998:CPO


Matyas:1991:KSB

REFERENCES

Muffett:1995:BPK
A. Muffett, P. Leyland, A. Lenstra, and J. Gillogly. The BlackNet 384-bit PGP key has been BROKEN. Message posted to sci.crypt and other newsgroups on June 26, 1995.

Matyas:1978:GDI

Meyer:1982:CND

Moler:1983:SVA

Magliveras:1990:LCP

Magliveras:1990:PCP

Moskovitz:1992:CCC

Moskovitz:1992:IDI
REFERENCES

Moskowitz:1994:STC

Moldovyan:1995:FSE

Meadows:1996:CCC

Meyer:1996:PKC

Mueller:1998:SPK

Muller:1998:SPK
Siguna Müller and Winfried B. Müller. The security of public key cryptosystems based on integer factorization. Lecture Notes in Computer Science, 1438:9–23, 1998. CO-
Marchignoli:1999:AVC


Meddes:1999:ABV


Mirza:1999:OKS


Moldovyan:1997:SEN


MattosBrasil:1998:CCC


Matheson:1998:RSD


Magliveras:1990:CTC


**Muller:1986:CDS**

**MN86**


**MRaihi:1997:XFO**

**MNSV97**


**MOI82**


**Mock:1997:BDS**


**Mohtashemi:1992:CHC**


**Matsumoto:1982:DTL**


**Mok:1997:KNF**

Wai Yin Mok. On keys and normal forms. *Informa-
REFERENCES


Morrice:1692:EB


Morrison:1983:SEA


Morain:1988:IGP


Mora:1989:AAA


Morris:1992:FMC


Morgan:1997:PAM


MorenoDiaz:1998:NCC

[Mor98] R. Moreno Diaz. Neurocybernetics, codes and computation. Lecture Notes

Moskowitz:1998:C

Mosses:1999:CGT

Moura:1999:PAP

Mullin:1988:ONB

Moynihan:1998:SAE

Mevis:1986:SCP

McInnes:1991:IPK
REFERENCES

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


REFERENCES

/\www.math.utah.edu/pub/rfc/rfc1864.txt. Obso-
letes RFC1544 [Ros93]. Status: DRAFT STANDARD.

McLeod:1998:TMP


Micali:1987:NSP


Maitra:1999:COA


Mitchell:1989:RHF


Macalister:1976:SLI

Robert Alexander Stewart Macalister and John Sampson. The secret languages of Ireland: Ogham, Hisperic, Bearlagair na Saer, Bog-Latin, and cryptography, with special reference to the origin and nature of the Shelta language;

McEliece:1981:SSR

Muller-Schloer:1983:MBC

Meier:1990:NCC

Montgomery:1990:FEP

Meier:1991:CPC

Meier:1993:EMC
W. Meier and O. Staffel-

**Massey:1994:FTA**


**Metzger:1995:RIAa**


**Metzger:1995:RIAb**


**RFC1852**

Micali:1995:SMG


Mambo:1998:NCB


Michels:1998:GCS


MacKenzie:1999:AIH


Maitra:1999:HNR


Miyazaki:1999:KGD


McLeod:1990:VLD

Dennis McLeod, Ron Sacks-Davis, and H.-J Schek, editors. *Very large data bases: 16th International Conference on Very Large Data Bases: August 13–16, 1990,*
REFERENCES


Miksch:1999:ASQ

S. Miksch, A. Seyfang, W. Horn, and C. Popow. Abstracting steady qualitative descriptions over time from noisy, high-frequency data. Lecture Notes in Computer Science, 1620:281–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

MSHP99


Martin:1997:MAS


Moriai:1998:HOD


Mizuki:1998:ESK


McClure:1999:HEN


Mizuki:1999:DNS

Martin:1999:BTE


Mambo:1996:HUT


Madonia:1993:GSP


Michels:1998:SSV


Mullender:1986:DCD

REFERENCES


REFERENCES

Marayati:1987:AWA


Moggi:1999:IMS


Mackinnon:1985:OAA


Moriya:1997:DWS


Molva:1992:KAK


Mu:1992:ICS

REFERENCES

Mueller:1999:SRB

Muftic:1988:SMC

Muftic:1993:SAO

Mulherin:1981:FDE

Mulligan:1989:UMA

Mullin:1989:LEN

Muller:1999:SRB
REFERENCES

Mund:1991:ZCP

Mund:1991:ZLC

Muraszko:1987:CVR

Murphy:1996:CC

Murphy:1999:OST

Maruyama:1998:TGH

Menezes:1990:IEC
REFERENCES

Menezes:1991:ACC

Meijers:1993:EMV

Menezes:1998:C

Mu:1999:DD

Menezes:1997:HAC

Menezes:1993:CPE
Muller:1998:DLB


Manber:1994:AAM


Maurer:1996:TCW


Maurer:1996:DO


Maurer:1996:DO


Maurer:1997:PAS


MacNish:1998:BRD

Reference: C. K. MacNish and M.-A. [MW98a]


Mitchell:1994:CPA


Maurer:1991:NIP


Mayers:1998:QCI


Matsui:1993:NMK


Maurer:1993:RNI


Myers:1994:RIA

REFERENCES


REFERENCES


V. S. Nalwa. Automatic online signature verification. Lecture Notes in Computer Science, 1351:1–??, 1997. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic).

Nanovic:1936:SWI


Nanovic:1974:SWI


Nastar:1994:VMN


NBS:1977:DES


NBS:1980:MO


NCSOTS:1984:ISR


NIST:1985:FPSa


NIST:1985:FPSb

[Nat85b] National Institute of Standards and Technology. FIPS PUB 113: Standard
REFERENCES


REFERENCES


REFERENCES


Nechvatal:1999:SRF


Nilsson:1978:OST


Nandi:1997:RCT


Nechvatal:1991:PC


Nechvatal:1996:PKB


Newman:1997:EC


Newman:1998:ROT


Neve:1999:FSC


Ng:1999:CST


Nguyen:1999:CGC


Nguyen:1999:CGG


Nelson:1990:SAE

REFERENCES

ny.com/link/service/series/0558/papers/0435/04350356.pdf. [Nic98b]

Neubauer:1998:DWI


Neubauer:1998:CSD


Nichols:1998:CCCa


Nichols:1998:CCCb


Nichols:1999:IGC


Niederreiter:1986:KTC


Niederreiter:1988:SNC


NIST:1985:FPC

NIST. FIPS PUB 113: Computer Data Authentication. National Institute of


NIST. Digital Signature Standard. Gaithersburg, MD 20899-8900, USA, February 1, 1993. ?? pp. FIPS PUB 186.


REFERENCES


[NM96b] David Naccache and David M’Raïhi. Cryptographic
smart cards — comparing the existing cryptography-
dedicated microprocessors
and describing possible di-
rections for their evolution. IEEE Micro, 16(3):14, 16–
24, June 1996. CODEN IEMIDZ. ISSN 0272-1732
(print), 1937-4143 (electronic).

G. Nadathur and D. J. Mitchell. System description: Teyjus — a compiler
and abstract machine based
implementation of lambd-
daProlog. Lecture Notes
in Computer Science, 1632:
287–??, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

David Naccache, David M’Raïhi, and Dan Raphaeli. Can Montgomery parasites
be avoided? A design meth-
ood based on key and cryptosystem modifi-
cations. Designs, Codes,
and Cryptography, 5(1):73–
80, January 1995. CODEN
DCCREC. ISSN 0925-1022
(print), 1573-7586 (elec-
tronic). URL http://
www.wkap.nl/oasis.htm/
77820; http://link.
springer.com/article/
10.1007/BF01388505.
REFERENCES


Nozaki:1997:LCS


Noras:1996:CHH


Nicchiotti:1998:NIS


Four volumes.

Nobauer:1984:CRS


Nobauer:1985:CRS


Nobauer:1988:CPK


Norman:1973:SWB

Bruce Norman. Secret warfare: the battle of codes and ciphers. David and
REFERENCES


REFERENCES

ISSN 0165-1684. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073158.html


REFERENCES


Norris-Saucedo:1989:DAD


Naor:1995:VC


Naccache:1997:NPK


Nguyen:1997:MRC


Nguyen:1997:MHR


Nechaev:1998:DSB

REFERENCES

Nguyen:1998:BQS


Nguyen:1998:BSR


Nguyen:1998:CAC


Nguyen:1998:CAD


Nguyen:1999:CFP


Nguyen:1999:HHS


Naccache:1999:HCF


Nieh:1993:MAC


M. Naor and M. Yung. Universal one-way hash functions and their crypto-

[Naor:1989:UOH]


[Naor:1990:PKC]


[Nyb98]


[Nyberg:1995:LAB]


[Nyb94]


[Nystrom:1999:PCT]

REFERENCES

proceedings/smartcard99/
ystrom.html.

[OA94]


[OA99]

[OA99]


[Oak78]

[OA99]

[Oakley:1978:RPC]

[Ohsuga:1999:EH1]

[O’Connor:1994:UBN]


[O’Connor:1995:DCT]

[Ohsuga:1999:EHI]

[Oakley:1978:RPC]

[Ohsuga:1999:EHI]

[O’Connor:1994:UBN]


[Oberzalek:1999:GEE]


[O’Connor:1995:DCT]

[Oakley:1978:RPC]
REFERENCES


REFERENCES

att.com/~amo/doc/arch/factoring.logs.troff.

Odlyzko:1987:ACC


Odlyzko:1990:RFK


Odlyzko:1994:DLS


Odlyzko:1994:PKC

Odlyzko:1995:FIF


Odlyzko:1998:C


Oelke:1997:VDE


Okamoto:1993:EDS


OConnor:1995:UMA


Oehler:1997:RHM


Oh:1999:DCT

Ohira:1999:EDD


Ohta:1996:DCT


Ohta:1998:RBD


Ohta:1998:ACA


Okada:1995:LBS


Obana:1996:VIS

REFERENCES

Ogata:1996:OSS


Ogata:1998:SBP


Okamoto:1988:DMS


Okamoto:1993:RAC

[Oka93a] T. Okamoto. On the relationship among cryptographic physical assump-


Okamoto:1993:PSP


Okamoto:1994:DCS


Okamoto:1998:TKR

[Oka98a] T. Okamoto. Threshold key-recovery systems for RSA. *Lecture Notes in
REFERENCES


Okamoto:1998:TKS


Okon:1996:DWN


Okon:1997:KMA


Ogata:1993:NSS


Oleschuk:1995:PKC


Ohta:1994:DAM

REFERENCES


Okamoto:1990:DZK

Ohta:1991:MAH

Ohta:1993:DMS

Ohta:1998:CST

ORuanaidh:1997:RST

ORuanaidh:1998:RST


REFERENCES

of Experts on Cryptography Policy Guidelines.


[OS92] Tatsuaki Okamoto and Kouichi Sakurai. Efficient algorithms for the construc-


Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as

**Okamoto:1998:SIB**


**Ou:1999:UUC**


**Outerbridge:1998:ACD**


**Ozarow:1984:WTC**

Lawrence H. Ozarow and Aaron D. Wyner. Wiretap channel II. *ATT Bell Lab. tech. j.*, 63(10 part 1):2135–2157, 1984. CODEN ABLJER. ISSN 0748-612X.
The World Wide Web Journal is a quarterly publication that provides timely, in-depth coverage of the issues, techniques, and research developments in the World Wide Web. The December issue contains the Conference Proceeding papers that were chosen for the 4th International World Wide Web conference in Boston, MA.

Ostrovsky:1991:HWM


Pereira:1998:REC


Petitcolas:1998:WCM


Paabo:1993:AD


Padro:1998:RVS


Pai:1996:VIE


Paillier:1998:INP

Paillier:1998:INS


Paillier:1999:EDF


Paillier:1999:LCD


Paillier:1999:TPE


Paillier:1999:PKC


Petitcolas:1998:ACM


Parthasarathy:1985:DSG


Parent:1998:ALM

Michael Parent. ActiveX licensing with MD5 encryp-
REFERENCES

Parker:1998:UMP

Parrish:1998:RMM

Patterson:1987:MCC

Patarin:1991:PPB

Patarin:1991:NRP

Patarin:1995:CMI

Patarin:1996:ACH
J. Patarin. Asymmetric cryptography with a hidden monomial. Lecture
REFERENCES

Notes in Computer Science, 1109:45–??, 1996. CODEN LNCSDA9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Paterson:1999:IPG


Paulson:1998:IAV


Paulson:1999:IAI


Poovendran:1999:ITA


Proctor:1999:PC


Piva:1997:DBW


Preneel:1997:CHF


[PC98]


[Preneel:1990:CTA]

[PD99a]


[PD99b]

[PD99a]

[PC98]


[PD99a]

[PD99b]


[PD99b]

[PD99a]

REFERENCES


Rev. and expanded papers from the meeting which was sponsored by the International Association for Cryptology Research (IACR) and others.


Rene Caupolican Peralta. Three results in number theory and cryptography: a new algorithm to compute square roots modulo a prime number; On the bit complexity of the discrete logarithm; A framework for the study of cryptoprotocols. Thesis (Ph.D.), Department of
Computer Science, University of California, Berkeley, Berkeley, CA, USA, December 1985. 52 pp.

Perry:1991:EIT


Peralta:1993:QSD


Perrig:1997:CPE


Perkuhn:1999:DSC


Pesic:1997:SSS


Petho:1991:PTA


Petersen:1998:HCD


Panagopoulos:1994:BSS

G. Panagopoulos and C. Faloutos. Bit-sliced signature files for very large text databases
REFERENCES


Pfitzmann:1995:BEA


Pfitzmann:1996:IHT


Pfitzmann:1996:TTT


Pfitzmann:1995:BEA

Pfleeger:1989:SC


Pfleeger:1995:ULC


Pfleeger:1989:SC

Pfleeger:1995:ULC
REFERENCES


References


[PHF99] Emil Praun, Hugues Hoppe,

Phillips:1998:SHI


Pichler:1998:E


Pierce:1977:SSP


Pieper:1993:CRD


Pinch:1997:UCN


REFERENCES

Popek:1979:ESC


Penzhorn:1995:CLP


Penzhorn:1995:CLW


Praehofer:1999:SRS


Pamplona:1998:LVC


Postma:1997:DCF


Park:1994:KDA

REFERENCES


REFERENCES


REFERENCES

Proctor:1992:AIC


Pudil:1995:ASM


Preneel:1994:CCM


Pointcheval:1999:NPK

[Poi99] David Pointcheval. New public key cryptosystems based on the dependent —

Pollard:1974:TFP


Pollard:1978:MCM


Pomerance:1988:ACC


'CRYPT0'87, a Conference on the Theory and Applications of Cryptographic Techniques, held at the University of California, Santa Barbara... August 16–20, 1987.


Gary Andrew Poole. Logout. Open Computing, 12
REFERENCES


REFERENCES


Posch:1989:AEA


Pfitzmann:1990:HBD


Posch:1992:MRR


Posch:1992:RNS


Posch:1995:MRRa


Posch:1995:MRRb

Pakstas:1996:SNN


Pedersen:1997:FSS


Park:1997:TER


Peleg:1979:BSC


Preneel:1998:SAA


Pratt:1939:SUS


Pratt:1996:SUS

Parra:1998:MPS


Preneel:1998:RDD


Preneel:1998:AAP


Preneel:1993:ADC


Preneel:1993:SCT


Preneel:1994:CHF


Preneel:1994:CHF


Preneel:1995:FSE

REFERENCES


REFERENCES


C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&page=174. CRYPTO
84: a Workshop on the
Theory and Application of
Cryptographic Techniques,
held at the University of
California, Santa Barbara,
August 19–22, 1984, spon-
sored by the International
Association for Cryptologic
Research.

Patel:1999:TML

[PRS99] S. Patel, Z. Ramzan, and
G. S. Sundaram. To-
wards making Luby-Rackoff
ciphers optimal and practi-
cal. In Knudsen [Knu99c],
pages 171–185. ISBN 3-540-
66226-X (softcover). LCCN

Peyravian:1999:HBE

[PRZ99] M. Peyravian, A. Roginsky,
and N. Zunic. Hash-based
cipher system. Computers
and Security, 18(4):
345–350, 1999. CODEN
CPSEDU. ISSN 0167-4048.

Paun:1993:CPS

[PS93a] Gheorghe Păun and Arto
Salomaa. Closure properties
of slender languages. The-
etorical Computer Science,
120(2):293–301, November
22, 1993. CODEN TCS-
CDI. ISSN 0304-3975
(print), 1879-2294 (elec-
tronic). URL http://
www.elsevier.com/cgi-
bin/cas/tree/store/tcs/
cas_sub/browse/browse.
cgi?year=1993&volume=
120&issue=2&aid=1406.

Pieprzyk:1993:DHA

Josef Pieprzyk and Babak
Sadeghiyan. Design of
Hashing Algorithms, vol-
ume 756 of Lecture Notes in
Computer Science. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
(New York), 3-540-57500-
6 (Berlin). xiii + 194
pp. LCCN QA76.9.H36 P53
1993.

Pfitzmann:1996:AF

B. Pfitzmann and M. Schunter.
Asymmetric fingerprinting.
In Maurer [Mau96b], pages
84–95. CODEN LNCSD9.
ISBN 3-540-61186-X. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
ac.uk/~fapp2/steganography/
bibliography/053630.html
Sponsored by the Interna-
tional Association for Cryp-
tologic Research (IACR), in
cooperation with the Univer-
sity of Saragossa.

Pichler:1996:FDG

F. Pichler and J. Scharinger.
Finite dimensional gener-
alized Baker dynamical sys-
tems for cryptographic ap-
REFERENCES

Pointcheval:1996:PSB


Pointcheval:1996:SPS


Parker:1997:GFA


Patel:1998:EDL


Patiyoot:1998:APW


Patiyoot:1998:SIW


REFERENCES

655


References

Pieprzyk:1995:ACA


Pomerance:1988:PAF


Pomerance:1980:P


Paar:1997:FAA


Pfitzmann:1995:HBA

REFERENCES

Phoenix:1995:QCP


Parkes:1999:ACC


Purdy:1974:HSL


Puteanus:1627:EPC


Preparata:1990:PCD


Peinado:1997:HPC


Posegga:1998:BCV


Preneel:1995:MMB

REFERENCES

URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm;

Preneel:1996:STM


Pfitzmann:1986:NUO


Pfitzmann:1987:NUO


Pfitzmann:1993:APS

REFERENCES

Piper:1993:DSH

Pfitzmann:1997:AF

Pfitzmann:1997:AFL

Pfitzmann:1997:SLT

Piccardi:1999:CLD

Polani:1999:DAR

Podilchuk:1998:IAW
Christine I. Podilchuk and Wenjun Zeng. Image-adaptive watermarking using visual models. _IEEE Journal on Selected Areas
REFERENCES


Quisquater:1998:CSE


Quisquater:1991:CLE


Quisquater:1989:BHF


Quisquater:1990:BHF


Quisquater:1995:ACE

REFERENCES


REFERENCES

Quisquater:1998:E


Rabin:1977:DS


Rabin:1981:HES


Rabin:1989:EDI


Rabin:1994:RSS


Rabin:1998:SAT


Rackoff:1990:BTP

Charles Rackoff. A basic theory of public and private cryptosystems. Lecture
Radlo:1997:LIC


Ramagopal:1992:DRB


Randell:1982:ODC


Rand:2001:MRD


Rao:1984:JEE


Ratcliff:1996:DIN

Rebecca Ann Ratcliff. *Delusions of intelligence: na-
tional cultures of cryptology, secrecy and bureaucracy in Germany and Britain during World War II. Thesis (Ph.D. in rhetoric), Department of Rhetoric, University of California, Berkeley, Berkeley, CA, USA, December 1996. xix + 303 pp.

Rhodes-Burke:1982:RSA


Reiter:1994:HSR


Ramesh:1999:VPP


Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF

Rogaway:1994:SEA


Rogaway:1994:SOE


Russinovich:1995:EWL


Rubia:1999:RIB


Renvall:1996:ASS


Renvall:1996:NSS


Roback:1999:CRF


Roback:1999:FAE


Rebel:1998:ADS


Rijmen:1996:CS


Reeds:1979:CMC


Reeds:1998:SCB


Reischuk:1985:NSB


Robert Reynard. *Secret
REFERENCES


REFERENCES

Rivest:1992:RNP


Rhee:1993:RAC


Rhee:1994:CSC


Richards:1974:SWP

[Ric74] Sheila R. Richards. Secret writing in the public records: Henry VIII–George II. London, 1974. x + 173 + 4 plates pp. UK£4.50. Contains one hundred documents, all but one of which are written wholly or partially in cipher and are now deciphered and printed in full for the first time. Includes letters in French or Italian, with a summary in English.

Rihaczek:1987:T


Rijmen:1999:WL


Riley:1996:LET

[Ril96] W. D. Riley. LANDSCAPE — encrypt this!! — there
are a thousand reasons to use encryption. Unfortunately, the current state of technology does not lend itself to e-mail platforms. *Datamation*, 42(9):27–??, ???? 1996. CODEN DTM-NAT. ISSN 0011-6963.

**REFERENCES**

**670**


**RIPE:1995:IPS**


**RIPE:1995:RIP**


**Ritter:1999:IWC**

[Dennis M. Ritchie. Dabbling in the cryptographic world — a story. This undated note describes the interesting history behind the non-publication of a paper [RRM78] on the Hagelin cypher machine (M-209), submitted to the journal Cryptologia, because of shadowy suggestions of a “retired gentleman from Virginia”., 19xx. URL http://www.cs.bell-labs.com/~dmr/crypt.html.**

**Ritchie:19xx:DCW**


**Rivest:1974:HCA**


**Rivest:1979:CRC**


**Rivest:1980:DSC**


**Rivest:1985:RCP**


**Rivest:1987:EDR**


**Rivest:1990:RMM**


**Rivest:1990:C**

REFERENCES


REFERENCES


[Riv95e] Ronald L. Rivest. Welcome to CryptoBytes. Crypto-


REFERENCES


Rosenson:1994:GWE


Ruanaidh:1996:WDI


Reeds:1985:NPR


issn=?????&volume=0&issue=0&page=377. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Rao:1987:PKA


Rao:1989:PKA


Raisch:1996:ACH

REFERENCES

Roberts:1993:ECI


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Roe:1994:PSC


Roe:1995:PBC


Roelse:1999:CWD


Rogaway:1995:BHA

[Rog95] Phillip Rogaway. Bucket hashing and its application to fast message au-
REFERENCES

authentication. *Lecture Notes in Computer Science*, 963:


Rosen:1994:EMT


Rose:1995:PPZ


Rose:1995:SUP


Rose:1996:IUP


Rose:1996:PMI


Rose:1996:PPZH


Rose:1996:UC1


Rose:1996:UPKaf

REFERENCES

Lognem. ISSN 1044-6397.


REFERENCES

JMOPEW. ISSN 0950-0340 (print), 1362-3044 (electronic). URL http://www.tandfonline.com/doi/abs/10.1080/09500349414552281


[Roy:1986:CBI] Marc Paul Roy. A CMOS bit-slice implementation of the RSA public key encryption algorithm. Thesis (M.Sc.(Eng.)), Queen’s University, Ottawa, ON, Canada, 1986. 3 microfiches (210 fr.).


REFERENCES


REFERENCES


Rackoff:1993:CDA


Rescorla:1996:SHT


Rivest:1996:PMTa


Rivest:1996:PMTb


Reiter:1998:RAU


Riordan:1998:CMF


Riordan:1998:EKGa

J. Riordan and B. Schneier.

[RS98d]


[Riordan:1998:EKBg]


[Rivest:1998:SPN]


[Ryan:1998:ARA]


[Ravi:1999:AAT]


[Reiter:1999:AMA]

C. Roeckl and D. Sangiorgi. A $\lambda$-calculus process semantics of concurrent idealised
REFERENCES


Rozenberg:1999:DCN


Rivest:1993:PRE


Rivest:1982:MOD


RSA:1993:PDH


[RSA94] 


[RSA99a] 


[RSA99b] 


REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072144.html


REFERENCES


[Ruskey:1993:SCG] F. Ruskey. Simple combinatorial gray codes con-

Russell:1993:NSC


Roychowdhury:1999:ENQ


S:1873:COD


Robshaw:1997:ECC

M. J. B. Robshaw and Yiqun Lisa Yin. Elliptic curve cryptosystems.


Rytter:1986:SCU


Ras:1999:DES

REFERENCES

Schiller:1995:SWT


Sabourin:1994:CCP


Sacco:1977:MC


Sahai:1999:NMN


Saks:1989:RNP


Sakurai:1996:HCA


Sakurai:1997:PPK

Kouichi Sakurai. Practical proofs of knowledge without relying on theoretical proofs of membership on languages. Theoretical
REFERENCES


Saltzer:1978:DS


Saltzer:1978:DS

Salomaa:1985:PKC


Salomaa:1990:PC


Salomaa:1991:VRS


Salomaa:1996:PC


Salvail:1998:QBC


Salvail:1999:SHG


Shimoyama:1997:IFS

T. Shimoyama, S. Amada, and S. Moriai. Improved


REFERENCES

[102x681] link/service/series/0558/ bibs/1550/15500090.htm;

[SAS99b]

[Sat89]

[Sau89]

[Saw55]

[SB82]

[SB92]

[SB93]
Shepherd:1994:UBS


Shepherd:1995:CNL


Schneier:1997:EPP


Shi:1998:FMV


Soto:1999:RTA


Serpell:1985:PES


REFERENCES

Chen:1985:RGE


Schneider:1996:RCB


Smith:1996:MIH


Sun:1997:DCP


Schneider:19xx:DWI


Scacchitti:1986:CT

Fred A. Scacchitti. The cryptographer’s toolbox.
REFERENCES

Dr. Dobb’s Journal of Software Tools, 11(5):58–??, May 1986. CODEN DDJOEB. ISSN 1044-789X.


REFERENCES

**Schroeder:1984:NTS**


**Schroeder:1986:NTS**


**Schnorr:1990:EISa**


**Schnorr:1990:EISb**

REFERENCES


Schmitt:1991:EAA


Schneier:1991:OHF

Bruce Schneier. One-way hash functions: Probabilistic algorithms can be used for general-purpose pattern matching. Dr. Dobb’s Journal of Software Tools, 16 (9):148–151, September 1, 1991. CODEN DDJOEB. ISSN 1044-789X.

Schnorr:1991:FHE


Schifreen:1992:PPD


Schneier:1992:SSA


Schneier:1992:UPC


Schilling:1993:MBC

REFERENCES

Schneier:1993:SCD

Schneier:1993:DS

Schneier:1993:IEA

Schneier:1993:UHD

Schnorr:1993:FHI

Schnorr:1993:FIE

Schiller:1994:SDC

Schneier:1994:DNV
REFERENCES

//www.counterpane.com/bfsverlag.html. [Sch94g]

**Schneier:1994:DEA**


**Schneier:1994:PAD**


**Schneier:1994:SCD**


**Schneier:1994:AAAd**


**Schneier:1994:AC94**


**Schneier:1994:BEA**


**Schneier:1994:CAW**


**Schneier:1994:NC**

REFERENCES

1994. CODEN DDJOEB. ISSN 1044-789X.

Schneier:1994:PYM

Schneier:1994:RDS

Schneier:1995:MS

Schneier:1995:MSH

Schneier:1995:OPE

Schneier:1995:PCC
REFERENCES

CODEN ????. ISSN 1079-8595.

Schneier:1996:ACP

Schneier:1996:CC

Schneier:1996:DLC

Schneier:1997:IRC

Schneier:1997:WCH

Schroeder:1997:NTS

Schweighofer:1997:DIF
E. Schweighofer. Downloading, information filtering and copyright. Information & Communications Technology Law, 6(2):??, June 1997. ISSN 1360-0834. URL
REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064383.html

Schlesinger:1998:CPC


Schmalz:1998:MDI


Schneier:1998:CBT


Schneier:1998:CDV


Schneier:1998:CTS


Schneier:1998:SPC

REFERENCES


Mark S. Schmalz, editor. Mathematics of Data/Image Coding, Compres-
REFERENCES


Schouten:1999:FEU


Sicherman:1983:AQR


Smillie:1986:RWA


Schwenk:1996:PKE


Sears:1986:SWK

Floor. US$9.95. Discusses secret writing, ciphers, and
the processes of creating and deciphering secret or
difficult languages. Includes thinking and writing exercises.

Seachrist:1995:DIM

D. Seachrist. Document image managers. BYTE Magazine,
ISSN 0360-5280 (print), 1082-7838 (electronic).

Sedlak:1988:RCP

H. Sedlak. The RSA cryptographic processor: The first high speed one-
URL http://link.springer-
ny.com/link/service/series/
0558/tocs/t0293.htm;
http://www.springerlink.
com/openurl.asp?genre=
issue&issn=0302-9743&
volume=293. CRYPTO '87,
a Conference on the Theory
and Applications of Crypto-
graphic Techniques, held at
the University of California,
Santa Barbara ... August

Seeley:1989:PCG

Donn Seeley. Password cracking: a game of wits. Communications of the
Association for Computing Machinery, 32(6):700–703, June 1989. CODEN
CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http:
//www.acm.org/pubs/toc/
Abstracts/0001-0782/63529.
html.

Seethamraju:1997:HII

Srisai Rao Seethamraju. A hardware implementation of the International Data En-
cryption Algorithm. Thesis (M.S.), North Carolina State University, Raleigh,

Segal:1992:NTC

Alida Segal. New trends in cryptology. Thesis (M.S. [C.Sc.]), School of Engineering. Department of Computer Sciences, City College of New York, New York,
NY, USA, 1992. 3 + 34 pp.

Selmer:1994:MNC

E. Selmer. From the memoirs of a Norwegian crypto-
tologist. Lecture Notes in Computer Science, 765: 142–??, 1994. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
REFERENCES

Selcuk:1998:NRL


Selmer:1998:NMS


Serpell:1985:CES


Seshadri:1981:KPP


Sakurai:1997:ILC


Saglam:1995:ACL


Shearer:1996:GCR


bibs/0473/04730283.htm;
http://link.springer-


**Schneier:1997:IMS**


**Shi:1999:FGM**


**Shannon:1945:MTC**


Claude Shannon. A mathematical theory of communication. The Bell System Technical Journal, 27 (3):379–423, July 1948. CODEN BSTJAN. ISSN 0005-8580. From the first page: “If the base 2 is used the resulting units may be called binary digits, or more briefly, bits, a word suggested by J. W. Tukey.”. This is the first known printed instance of the word ‘bit’ with the meaning of binary digit.

**Shannon:1948:MTCa**


**Shannon:1949:CTS**

REFERENCES


Shamir:1979:HSS

Shamir:1982:PTA

Shamir:1983:ECC

Shamir:1983:ECT

Shamir:1983:GCS

Shamir:1984:PTA

Shamir:1985:IBC
tographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


Sherman:1986:CVT


Sherman:1987:CVT


Sherman:1992:CVT


Shepherd:1992:FFW

Shepherd:1992:HSC  

Shepherd:1992:NPS  

Shepherd:1992:SIR  

Shepherd:1992:DES  

Shepherd:1993:ACCa  

Shepherd:1993:ACCb  

Shepherd:1993:EOS  

Shepherd:1993:WNS  


S. J. Shepherd. Primitive polynomials over GF(2) of Hamming weight 3 and 5 up to high order. Report
573, Electronic and Electrical Engineering Department, University of Bradford, Bradford, Yorkshire, UK, March 1995.


Victor Shoup. On fast and provably secure message authentication based on universal hashing. Lecture


occultism, and historians of science.

Sakurai:1993:DBS


Sakurai:1993:SCS


Sakurai:1994:SCT


Sidhu:1981:APG


Sieminski:1983:SBB


Siegenthaler:1984:CIN


Siegenthaler:1985:DCS

REFERENCES

9340 (print), 1557-9956 (electronic). This paper breaks the cipher of [Gef73].

Swartzlander:1993:SCA


Shimbo:1993:CSC

Shimbo:1993:CSC


Silverman:1987:MPQ


Silverman:1997:FGR


Silverman:1999:EMM


Silverman:1983:RVS


Silverman:1987:MPQ

Silverman:1997:FGR

Silverman:1999:EMM
Simmons:1979:HID


Simmons:1979:CCA


Simmons:1979:SAE

Simmons:1982:SCA


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID

REFERENCES

[Sim85a]

[Sim85b]


[Sim90a]

[Sim90b]

Simmons:1991:GSS


Simmons:1992:CCS


Simmons:1993:SCU


Simmons:1994:CTS


Simmons:1994:CPF


Simmons:1994:SCP

Simmons:1994:SCE


Simovits:1995:EDE


Simmons:1996:HSC


Simmons:1997:SCS


Simmons:1998:HSC


[Sin95] Bappaditya Sinha. Kerberos for non-secure client-


REFERENCES


REFERENCES


[SK98b] T. Shimoyama and T. Kaneko. Quadratic relation of S-box and its application to the linear attack of full round

**Shimoyama:1998:QRB**


**Shepherd:1997:EKE**


**Schell:19xx:CMC**


**Sorokine:1994:TBD**

REFERENCES

Suzuki:1999:AVB


Satoh:1998:HSR


Satoh:1998:HSS


Schneier:1996:DP


Schneier:1998:TKSa


Schneier:1998:TBBa

REFERENCES


REFERENCES

of Standards and Technology [Nat99b], page ?? ISBN ?? LCCN ???. URL http://csrc.nist.gov/encryption/aes/round1/conf2/Schneier.pdf. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.


Sufatrio:1999:IMS


Slutsky:1998:KDQ


Schobi:1983:FAT


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


REFERENCES


[SN98b]
REFERENCES


REFERENCES

Schroeppel:1995:FKE


Sorkis:1980:USM


Soto:1998:RTA


Smith:1979:UFM


Seberry:1989:CIC


Seberry:1990:ACA

Schechter:1999:AAM


Spirakis:1995:AET


Shoup:1996:SKD


Saltzer:1984:EEA

Shin:1998:NHF


Shin:1999:HFM


Shamir:1984:CCV


Siromoney:1986:PKC


Shepherd:1989:CSS


Shepherd:1990:DSA


Schrift:1991:UNB

REFERENCES


REFERENCES


REFERENCES

**Subramanian:1987:DTP**


**Siromoney:1988:CPL**


**Saito:1999:DPC**


**Stubblebine:1999:UST**


**Safford:1993:SRA**


**Sakai:1997:WRK**

Sakai:1997:WRP


Sakai:1998:SHC


Subramanian:1992:LT


Sherman:1994:SNA


Schneier:1997:DDE


Saeednia:1998:NLI


Saeednia:1998:SGI


Susilo:1999:FST


REFERENCES


Shawe-Taylor:1989:BRB


Stern:1991:CPK


Safavi-Naini:1994:OAS


Stark:1970:INT


Stark:1978:INT

Stallings:1994:PGP

[Sta94a] William Stallings. Pretty Good Privacy: Privacy and security are important issues to commercial users of public E-mail systems. PGP, an E-mail security package, is finding acceptance as the way to achieve protection. *BYTE Magazine*, 19(7):193–??, July 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Stallings:1994:SSH


Stallings:1995:PWT


Stallings:1995:PYP


Stadler:1996:PVS


Staiger:1996:CSW


Stallings:1996:PCS


Stallings:1996:PCI

REFERENCES

Staddon:1997:CSC


Stallman:1997:SDR


Stark:1997:ESP


Stallings:1999:CNS


Stallings:1999:HAK


Stevenson:1976:MC1


Stern:1987:SLC

REFERENCES


Stevens:1988:CPR


[Ste88]

Stephenson:1989:PPM


[Ste89]

Stevens:1990:CPi


[Ste90a]

Stevens:1990:CPk


[Ste90b]

Steinberg:1991:VSV


[Ste91]

Stern:1994:DIS


[Ste94a]

Stevens:1994:PBa


[Ste94b]

Stewart:1992:SCK


[Ste92]

Stern:1995:COD

J. Stern. Can one design a signature scheme based on error-correcting codes? Lecture Notes in Computer
REFERENCES

Stern:1996:VCA

Stern:1998:LCO

Stern:1998:NEA

Stephenson:1999:C

Stern:1999:ACE

Stern:1999:DU

Stinson:1991:CCA
Douglas R. Stinson. Combinatorial characterizations of
REFERENCES

authentication codes. Lecture Notes in Computer Science, 576:62–73, 1991. CO- 
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http: 
//link.springer-ny.com/ 
link/service/series/0558/ 
bibs/0576/0576062.htm; 
http://link.springer- 
ny.com/link/service/series/ 
0558/papers/0576/0576062. 

Stinson:1991:UHA

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http: 
//link.springer-ny.com/ 
link/service/series/0558/ 
bibs/0576/0576074.htm; 
http://link.springer- 
ny.com/link/service/series/ 
0558/papers/0576/0576074. 

Stinson:1993:NGL

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

Stinson:1993:ACC

Douglas R. Stinson, editor. Advances in Cryptology, CRYPTO ’93: 13th Annual International Cryptology Conference, Santa Bar- 

Stinson:1994:ACC

Douglas R. Stinson, editor. Advances in Cryptol- 
yogy, CRYPTO ’93: 13th Annual International Cryp-
tology Conference, Santa Barbara, California, USA, August 22–26, 1993: Proceedings, volume 773 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, UK / etc., 1994. CO- 
DEN LNCSD9. ISBN 0-387-57766-1 (New York), 3- 
540-57766-1 (Berlin). ISSN 0302-9743 (print), 1611- 
ny.com/link/service/series/ 
0558/tocs/t0773.htm; 
http://www.springerlink. 
com/openurl.asp?genre=
REFERENCES

issue&issn=0302-9743&
volume=773.


REFERENCES

Su:1998:DEM

Summers:1984:OCS

Sun:1991:UDE

Sun:1991:RSE

Sun:1998:ISM

Sundsted:1998:SDI

SuperMacSoftware:1988:SDE

Sutoh:1999:HPP
Hiroki Sutoh. A high-performance public key cryptography co-processor for super multi-purpose smart card. In Anonymous [Ano99c], page ??

Shand:1993:FIR

Schnorr:1994:BBC


Schnorr:1995:BBC


Shepherd:1995:GJ


Stern:1998:CC


Shamir:1999:PHS


Shamir:1999:PSS


Samuels:1998:LSA

Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling PC’s; server-side scripting; stronger encryption; inner loops; Einstein kudos. Dr. Dobb’s Journal of Software Tools, 23(3):8, 12, March 1998. CODEN DDJOEB. ISSN 1044-789X.

Sivakumar:1999:PPN

R. Sivakumar, N. Venkitaraman, and V. Bhargha-

**Shepherd:1996:SAD**


**Shamir:1998:PHS**


**Shepherd:1995:SCS**


**Smeets:1991:CAC**


**Shulman:1961:GC**


**Smith:1983:HCR**

Silverman:1993:PAE


Saeki:1994:SSS


Safford:1994:UNC


Snow:1994:SA


Scheidler:1995:PKC


Stansfield:1995:CCS


Schneier:1997:FSEa

Schneier:1997:FS Eb


Stinson:1998:ARS


Stinson:1999:ARS


Stinson:1999:KPT


Swan:1994:AA b


Swire:1997:UL F


Salzer:1981:RHH

REFERENCES

762

.computer.org/an/books

**Sun:1989:TKE**


**Sun:1990:KGE**


**Salomaa:1986:PKC**


**Smith:1992:ICF**


**Sakurai:1996:BDB**

ac.uk/~fapp2/steganography/bibliography/054625.html

[SY96b] Shieh:1996:AKD


Sakurai:1996:CWR


Szepietowski:1998:WSO


Swanson:1996:TRI


Three volumes. IEEE catalog number 96CH35919.

Swanson:1998:MSB


Swanson:1998:MSV

REFERENCES

[765]

0733-8716 (print), 1558-0008 (electronic).

**Swanson:1998:RAW**


**Seberry:1994:ISA**


**Seberry:1994:PDS**


**Seberry:1995:RAN**


**Seberry:1995:SCF**


**Seberry:1995:RBP**

REFERENCES

Theodoridis:1998:NES


Takano:1999:CAC


Tang:1997:DBC


Taaffe:1998:NBL


Tabatabaian:1994:CAP


Takagi:1997:FRT


Takagi:1998:FRC


Takagi:1998:FRT

Tao:1994:FAO


Tardo:1990:PKB


TFEC:1998:CPF


Tattersall:1998:ENT


Tattersall:1999:ENT

Taylor:1990:DSI

Taylor:1994:ICV

Taylor:1995:NOU

Tao:1985:FAP

Tao:1986:TVF

Tsuji:1991:NIB

Tao:1999:GPK

Tao:1999:FAP


**REFERENCES**


[Tex84] Texas Instruments Inc. TMS7500 TMS75C00 user’s guide, data encryption device: 8-bit microcomputer family. Texas Instruments, Dallas, TX, USA, 1984. various pp.

REFERENCES

Tanaka:1999:PCD


Tzeng:1999:IP1


Thao:1991:SAD


Theobald:1995:HBS


Thomas:1974:RPS


Thompson:1984:RTT


Thompson:1986:SDE


Thompson:1987:RTT

Thomas:1996:PVS

Tarman:1998:AAE

Tsujii:1988:PKC

Tilki:1998:EHD

Tippett:1927:RSN

Taaffe:1997:NSL

Tseng:1999:ATS
REFERENCES

Takagi:1999:DRA


Tzovaras:1998:RIW


Theodoratos:1999:DGD


Tavares:1999:SAC


Takagi:1996:MMP


Takagi:1996:MVM

REFERENCES

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

Terada:1997:LDC
[Routo Terada and Jorge Nakahara. Linear and differential cryptanalysis of FEAL-N with swapping. Relatorio tecnico RT-MAC-9709, Universidade de Sao Paulo, Instituto de Matematica e Estatistica, Sao Paulo, Brasil, September 1997. 10 pp.]

Todorovic:1997:CAS

Tirkel:1998:IWR

Tonchev:1996:CDG

Toussaint:1991:DCK

Toussaint:1992:SSI
Toussaint:1993:FVP


Tsunoo:1994:COA


Touch:1995:RRM


Townsend:1998:QCO


Thompson:1963:SDE


Traore:1997:MUF


Traore:1999:GST

REFERENCES


REFERENCES


[Tri21c] Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*. Balthasaris Aulaeandri, Darmstadt, Germany, 1621. 8 + 152 + 2 pp. LCCN Z103 .T84 1621. Authore ... Ioanne Trithemio ... ; praefixa est huic operi sua clavis, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Darmstadtij. Ex officina typographica Balthasaris Aulaeandri, sumptibus vero Ioannis Berneri, bibliop. Francof., anno 1621.


scribes this book as “re-count[ing] the political effects of the most important cryptogram solution in history”.


REFERENCES


Tel:1994:DAI


Tan:1992:NPE


Takagi:1992:MMH


Trabelsi:1994:PPS


Tsiounis:1998:SEE

REFERENCES


[Tze99]

Tax:1999:PFD


[TZ94]

[Tzeng:1999:CMC]


[Ude98]

[Udell:1998:HAW]


[Ueh95]

[Uehara:1995:ESB]


[UFC94]

[Udell:1994:BCRb]


[102x681]

**REFERENCES**


**USASC:1923:EC**

[UG23]


**USASC:1923:EC**

[Uni42]


**USWARDEPT:1942:ACC**

[Uni70]


**USWARDEPT:1924:EC**

[Uni24a]


**USWARDEPT:1924:EC**

[Uni77]


**USDOS:1970:BC**

REFERENCES


[Uni82c] United States. General Services Administration. Telecommunications: general security requirements for equipment using the Data Encryption Standard. General Services Administration, Washington, DC,


REFERENCES


[Uni95a]


[USDOA:1994:OMT]

[Uni94a]


[USDOA:1994:UDS]

[Uni94b]


[USNSACS:1994:SC]

[Uni94c]


[UCC:1996:SRP]


[USNSGC:1995:NDN]

REFERENCES


REFERENCES


[UNU85]


[USE88a]


[USE88b]


REFERENCES


[USENIX:1995:PUT]


[USENIX:1995:PUT]


[USENIX:1995:PFUa]


[USENIX:1996:PFUa]


[USENIX:1996:PFUa]


[USENIX:1996:PFUa]


[USENIX:1995:PFUb]

USA, July 22–25, 1996.


REFERENCES

USENIX:1999:PEU


USENIX:1999:PTSa


USENIX:1999:PUWa


USENIX:1999:UAT


USWD:1980:EC


USWD:1983:EC


USDOA:1989:BC

[UU89] United States. Dept. of the Army and United States

**USCHCJ:1997:SFT**


**USPBC:1997:AEC**


**Vadhr:1995:VID**

Kumar S. Vadhr. VLSI implementation of the data encryption algorithm. Thesis (M.S.), Department of Electrical Engineering, University of Hawaii at Manoa, Manoa, HI, USA, 1995. x + 89 pp.

**Valerio:1892:C**


**Vamos:1985:BRB**


**VanTassel:1969:ACT**

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


vanDijk:1997:MIT


vanRenesse:1997:ODS


vanderLubbe:1998:BMC


Varaiya:1999:IDD


Varma:1999:IDD


Vaudenay:1993:FHI


Vaudenay:1995:NMC


Vaudenay:1996:WKB

REFERENCES


REFERENCES


[vdws97] Ron van der Wal and William Stallings. Programmer’s bookshelf — Ron examines Stanley Lippman’s Inside the C++ Object Model, while William looks at Peter Wayner’s Disap-


VonzurGathen:1999:MCA


Vandewalle:1993:TAT


Vallee:1988:HBO


Vallee:1989:HGR


Verschuren:1993:IOS


vanFaber:1997:SDD

vanHeijst:1993:NCF


Vigna:1998:CTM


Vincent:1971:PAG


Vincent:1972:CPA


Vandenauwera:1998:SIE


Voydock:1983:SMH


Voydock:1984:SMT

REFERENCES


Voyatzis:1999:PDI


Varadharajan:1997:ISP


Vassiliadis:1988:PEA


Volts:1941:BC


vanderWal:1997:PBR


VanEetvelt:1995:DPF

[VSB95] P. W. J. Van Eetvelt, S. J. Shepherd, and S. K. Bar-
REFERENCES

809


Vu:1995:CPM


[Vu95]

Vazirani:1985:ESP


[VV85]

Verheul:1997:CLS


[Vv97]

Vandemeulebroecke:1990:SCB

Verheul:1997:BEF


vanOorschot:1994:PCS


Vedder:1998:SCR


vanOorschot:1999:PCS


vanEmdeBoas:1999:ALP

REFERENCES


REFERENCES


Wagner:1983:F


Wagner:1998:DCK


Wagner:1998:CSR


Wagner:1999:BA


Wagner:1999:CFb

David Wagner. Cryptanalysis of FROG. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ?? LCCN ?? URL ??

Waidner:1990:USR

steganography/bibliography/1024.html.


[Walther:1998:VBE]
REFERENCES


Wallich:1999:HSM


Walter:1999:MTI


Wen-Ai:1994:MTS


Wang:1986:UEA


Wang:1992:CDS


Wang:1992:DKT


Warren:1982:BTC

Alexander Z. Warren. *Basicplus through cryptanalysis; an introduction to structured programming*. ????,
REFERENCES


Wayner:1995:PCL

Peter Wayner. Picking the crypto locks — with today’s hardware and a new technique called differential cryptanalysis, it’s getting easier for data burglars to crack your safe. What can you do to keep them out? *BYTE Magazine*, 20(10):77–??, October 1995. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1996:DCB


Wayner:1996:DLY


Wayner:1998:MJD


Willcox:1992:TCS


Wagner:1994:PPR


Wolf:1995:ICR

Thomas Wolf and Andreas Brand. Investigating DES with CRACK and related programs. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 29(2S (special issue)): 
Whittle:1999:SDC


Wallach:1997:ESA


Wu:1998:CRP


Weeks:1995:CBW


Wynn:1997:CTS


Wegman:1981:NHF

Wolfgang:1996:WDI


Wolfgang:1997:WTD


Weber:1998:SMD


Wang:1999:SCB


Wendling:1999:PRS


Weber:1979:USD


Webb:1988:NPK


Weber:1993:MDC

REFERENCES


Weber:1998:SWY

Wedemeijer:1999:DFM

Weiss:1988:BOP

computer.org/an/books/an1988/pdf/a4348.pdf; 

Weissman:1991:IRA

Weissman:1991:IRN

Weierud:1994:SPB
REFERENCES

Weierud:1998:C

Weierud:1999:TJG

Wells:1980:ADB

Welchman:1982:HSS

Wells:1982:USE

Welchman:1986:PBB

Wells:1988:NAI

Welsh:1988:CC

Welsh:1989:CC
REFERENCES


Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.
REFERENCES


Wiener:1990:CSRb

Wiener:1990:CSRa

Wiener:1994:EKS

Wiener:1996:EKS

Wiener:1997:EKS

Wiener:1998:EKS

Wiener:1998:PCP
cryptobytes/crypto4n1.pdf.

**Wiener:1999:ACC**


**Wilkins:1641:MSS**


**Wilkes:1968:TSCa**


**Wilkes:1968:TSCb**


**Wilkes:1972:TSC**


**Wilkes:1975:TSC**


**Williams:1980:MRP**


**Williams:1982:CHP**

Hugh C. Williams. Computationally “hard” problems as a source for cryptosystems. In Secure communications and asymmetric...
REFERENCES


Willett:1983:TKS


Williams:1983:PAP


Williams:1983:SPK


Williams:1986:PKE


Williams:1986:ACC


Winterbotham:1978:NC


Winterbotham:1991:US


Winternitz:1983:POW


Winternitz:1984:SOH


Winton:1993:UPH


Winterbotham:1989:US


Wired:1998:REC


Woo:1994:LAP


Wong:1999:DSF


Walker:1996:CKR


Wagner:1985:PKC


Waldvogel:1993:PDD

REFERENCES

Wheeler:1994:TCN


Wheeler:1995:TTE


Wheeler:1998:CX


Wright:1998:NTD


Woehr:1997:CRR


Wolfe:1943:FCCa


Wolfe:1943:FCCb


Wolfe:1943:FCCc

REFERENCES

Wolfe:1970:SWC


Wolfe:1983:FCC


Wolfowicz:1993:SPR


Wolfowicz:1993:SPS


Wolf:1998:SSAb


Wolf:1999:USC


Woolsey:1990:DDE


Worth:1975:CMA


Wortmann:1987:BRB

[Wor87] J. C. Wortmann. Book review: Mr. Babbage’s secret:
REFERENCES


REFERENCES


Minnehaha Parkway, Minneapolis, MN 55419, December 2, 1998. ????

**White:1999:CBA**


**Wagner:1998:CO**


**Wagner:1999:CO**


**Weatherford:1999:NGA**


**Wagner:1997:CCMa**


**Wagner:1997:CCMb**

David Wagner, Bruce Schneier, and John Kelsey. Cryptanalysis of the Cellular Message Encryption Algorithm. *Lecture Notes in
REFERENCES


REFERENCES

[Xie:1998:WDI]

[XL98]

[XL99]

[Xiong:1999:LPK]

[Xiao:1994:MMH]

[Xu:1997:BPK]

[Xu:1999:STP]
REFERENCES


Yacobi:1999:RMC


Yacobi:1999:RME


Yahalom:COMPSYS-7-4-451


Yamamura:1998:PCU


Yamamura:1998:PKC


Yamamura:1999:FCU


Yan:1995:PTL


Yao:1982:PSC

A. Yao. Protocols for secure computation. In IEEE [IEE82a], pages 160–164. CODEN ASFPDV.
REFERENCES

Yao:1982:TAT

Yao:1986:HGE

Yardley:1983:CBC

Yardley:1990:ABC

Yoshiura:1998:VDW
Yeung:1997:DWH

Yeung:1998:DW

Yeun:1999:DSM

Yokokawa:1999:BDE

Yi:1996:DAN

Yin:1997:REA

Yakovlev:1998:PND
REFERENCES

Yahalom:1994:TBN


Yang:1999:DIC


Yen:1993:FCE


Yen:1995:IDSa


Yen:1997:N EC


Yen:1995:IDSb


Yen:1997: SAT

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


REFERENCES


REFERENCES

Youssef:1995:RBS

Youssef:1996:CBN

Yu:1992:VLD

Yung:1985:CSP
Mordechai Yung. Cryptoprotocols: Subscription to a public key, the secret blocking and the multi-player mental poker game (extended abstract). In Blakley and Chaum [BC85], pages 439–453. CODEN LNCSRD9.
REFERENCES

848


CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Yung:1985:SUK


Yun85b

Yuval:1997:RTE


YWC97


Yuv97


YWY97


YY99

REFERENCES

48–54, February 1991. CO-
DEN CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http:
//www.acm.org/pubs/toc/
Abstracts/0001-0782/102800.
html. See [BY92].

[BY92] A. Young and M. Yung. The
dark side of black-box cryp-
tography, or: Should we
trust Capstone? *Lecture
Notes in Computer Science*,
1109:89–??, 1996. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[YY96] A. Young and M. Yung. The
dark side of black-box cryp-
tography, or: Should we
trust Capstone? *Lecture
Notes in Computer Science*,
1109:89–??, 1996. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[YY97a] Adam Young and Moti
Yung. Kleptography: Using
cryptography against cryp-
tography. *Lecture Notes in
Computer Science*, 1233:
62–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/1233/12330062.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1233/12330062.
pdf.

[YY97b] Adam Young and Moti
Yung. The prevalence
of kleptographic attacks
on discrete-log based cryp-
tosystems. *Lecture Notes
in Computer Science*, 1294:
264–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/1294/12940264.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1294/12940264.
pdf.

[YY97c] Adam Young and Moti
Yung. Sliding encryption:
a cryptographic tool for
mobile agents. *Lecture
Notes in Computer Science*,
1267:230–??, 1997. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/1267/12670230.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1267/12670230.
pdf.

Finding length-3 positive
Cunningham chains and
their cryptographic signif-
cance. *Lecture Notes in
Computer Science*, 1423:
289–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
Young:1998:MBS


Young:1998:ARA


Young:1998:MBB


Yeo:1999:WOV


Young:1999:ARC


Yeung:1998:DWS

 REFERENCES

Zajacz:1997:SCE


Zang:1990:ESE


Zave:1999:SDC


Zegwaart:1993:PEM


Zeidler:1979:DDE


Zergo:1996:UER


Zerovnik:1996:RC


Zollner:1998:MSS

J. Zölner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke,

Zoellner:1998:MSS


Zuquete:1996:TAC


Zeng:1990:LSM


Zviran:1993:CPT


Zhao:1991:BNK


Zhao:1996:WSE

REFERENCES


[Zha97]

[Zhao:1997:LT]


[Zha98]

[Zhang:1998:TPS]


[Zhe90]

[Zheng:1990:PDS]


[Zhe95a]


[Zhe95b]


[ZHJ98]
REFERENCES

Zhou:1994:SDS
Fang Zhou. A survey of digital signature variations and a study of implemen-

Zheng:1994:RSS

Zheng:1998:HCE

Zieschang:1997:CPB

Zimmermann:1995:OPU

Zimmermann:1995:PSC
REFERENCES

Zimmermann:1996:PGPa


Zimmermann:1996:PGPb


Zimmermann:1998:CI


Zhao:1995:ERL


Zhao:1996:DWS

Jian Zhao and Eckhard Koch. A digital watermarking system for mul-

REFERENCES


Zhao:1998:GDW


Zhao:1998:BTT


Zhao:1999:DWW


Zeng:1997:RRO


Zhou:1999:SPP


Zhang:1999:AFV

Yuqing Zhang, Jihong Li, and Guozhen Xiao. An approach to the formal verification of the two-party cryptographic proto-
REFERENCES


Zwiggelaar:1999:DCM


Zukowski:1998:JTUb


Zukowski:1998:JTUa


Zunic:1998:MCI

[ZYR90] Nevenko Zunic. The MARS cipher — IBM submission to AES. In National Institute of Standards and Technology [Nat98], page ??.

Zwiers:1998:CTD


Zeng:1990:LCT


