Title word cross-reference

#1
[Ble98a, Kal98b, KS98a, RSA93f, RSA93a].

#10 [Kal98c].

#11 [Ano95j, Ano96k].

#12 [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]. $\mathbf{1}$ [Gar97b]. 1 [JV98b].

$\mathbf{1}$-Million [GC97]. 16 [BS93a, GC94]. 2 [JV98b, KG95, Kob91b, MVZ98, SBVG99].

$\mathbf{2}$-95 [Hat96]. 2n [QG90]. 2R [YLD99]. 3

[Ben99, BALS99, CK95, KSW97b, Nas94, TK99, Wor96, YY99a]. 511 [CC98]. 64

[MMI97], 8 [Miy90], < [Zhe97b]. 2 [TZ94].


[JS95b]. mod2^82 [Ber93]. c [WD99b]. \chi^2

[HG97b]. d [BD99b]. \ell [BR91]. f [DJL93].

F_2^m [MVZ93]. F_2^n [SS98a, Ler97]. F_p

[Miy93a]. G\nD(2^n) [Ara93]. G\nF(2) [She95c].

G\nF(208) [Ros98a]. G\nF(2^n) [FBT96]. G\nF(p)

[Gor93b, HNM98]. \gg [GQW+91]. k

[Car97c, DJL93, HKS97b, KR99b, KS97b, WD99b]. l [HL93a, KS97b]. L_2

[Vau99a]. \lambda [RS99c]. L \geq 2 [SVxW91]. \ll

[GQW+91]. m [Bla94a, FR94]. N

[BS91e, BS91d, HKS97a, HKS97b, KSW99b, KSW99c, KK98, Per93, QG90, Tak97].

N = p^l q [BDHG99a, BDHG99b]. N^{0.292}

[BD99b]. P [BS90b]. p^k q [Tak98a, Tak98b].

r [BDHG99a, BDHG99b, FJR96]. s

[YT95a, YT95b]. s^2 [Knu93b]. Step_k,m

[MMI97], 8 [Miy90], < [Zhe97b]. 2 [TZ94].


[JS95b]. mod2^82 [Ber93]. c [WD99b]. \chi^2

[HG97b]. d [BD99b]. \ell [BR91]. f [DJL93].

F_2^m [MVZ93]. F_2^n [SS98a, Ler97]. F_p

[Miy93a]. G\nD(2^n) [Ara93]. G\nF(2) [She95c].

G\nF(208) [Ros98a]. G\nF(2^n) [FBT96]. G\nF(p)

[Gor93b, HNM98]. \gg [GQW+91]. k

[Car97c, DJL93, HKS97a, HKS97b, KR99b, KS97b, WD99b]. l [HL93a, KS97b]. L_2

[Vau99a]. \lambda [RS99c]. L \geq 2 [SVxW91]. \ll

[GQW+91]. m [Bla94a, FR94]. N

[BS91e, BS91d, HKS97a, HKS97b, KSW99b, KSW99c, KK98, Per93, QG90, Tak97].

N = p^l q [BDHG99a, BDHG99b]. N^{0.292}

[BD99b]. P [BS90b]. p^k q [Tak98a, Tak98b].

r [BDHG99a, BDHG99b, FJR96]. s

[YT95a, YT95b]. s^2 [Knu93b]. Step_k,m
[GC90].  $t$ [KOO95b, KOO95a].  $T_3$ $P$
[GPSV98].  $y^2 + axy = x^3$ (mod $n$) [Koy95].
$z$ [MSS93].  $Z/nZ$ [CLL99, MM96b].  $Z_n$
[ML98].  $Z_n$
[KMOV91, OFF93, VZ97, KK98, SE96].
-Adic [KG95, Tak97].  -Bit [GQ90, MM97].
-boxes [YT95a, YT95b].  -calculus [RS99c].
-Cascades [GC90].  -Cheater
[KOO95b, KOO95a].  -Codes
[JS95b, MSS93].  -D [CK95, TK99].
-Decorrelation [Vau99a].  -Dependent
[DJL93].  -DES [Kum93b].  -Dimensional
[Per93].  -divisibility [FR94].  -Fields
[BMT96].  -fold [BR91].  -formulae
[WD99b].  -Hash [BS91c, BS91d].  -means
[SBV999].  -Round [BS93a, GC94].
-sequences [Bla99a].  -Span [HL93a].
-Tuples [FJR99].  -WAY [KSW97b].
-wheel [Car97c].

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

1 [Ano93k, CCN95, Nat95].  1.0.1 [Sun91b].
1.2 [DDJ98e, DDJ98f, Zuk98a].  10
[CMM93].  101 [Hon98].  1040 [Lin88a].
105-1
[Uni98a, Uni98b, Uni98c, Uni98d, Uni98e].  105-263 [Uni98f].
105-415 [Uni98g].  105th [Ano98f].  10th
[Ano93d, CMM93, IEE94c, USE96a].  1113
[Lin89a].  1186 [Riv90a].  11th [SI93].  120
[DLM994].  128-Bit
[SKW+98b, DKR97b, Kun98c, Lin98, Luc98a, Luc99a, Luc99b, SKW+98c].  12th
[Bri92, Bri93, KG96].  130 [Ano96b].  1320
[Riv92a].  1321 [Riv92b].  1334 [LS92].  1395
[Uni94a].  13th
[IEE97b, IEE97c, Sti93b, Sti94].  1409
[Bor93a].  1411 [Bor93b].  1412 [AIA93b].
1416 [Bor93c].  1421 [Lin93a].  1446
[GM93a].  14th [Des94b, KK99b].  15
[UU97b].  1507 [Kan93].  1510 [KN93].  1511
[Lin93c].  1544 [Ros93].  15th
[Cop95b, Cop95d, NSS92].  16 [HB99].  16-18
[Q+98].  16-bit [Bro97].  160
[BDP97, DBP96, BBP97].  16th
[Kob96, MSDS90].  1704 [HA94a].  1731
[Mye94a].  1734 [Mye94b].  17th
[Hei96a, Kal97c].  180 [Nat95].  180-1
[Ano95i, Nat95].  1810 [Tou95].  1824
[Dan95].  1826 [Atk95a].  1827 [Atk95b].
1828 [MS95c].  1829 [KMS95a].  1847
[GMCF95].  1851 [KMS95b].  1852
[MS95d, MS95e].  1864 [MR95b].  18th
[Kra98, Yua92].  1915 [Kaz96].  1929 [Lee96].
194 [Uni94a].  1940 [CWM91].  1961
1993 [ACM93b].  1994
[Ano94e, Sim96b, Uni95a].  1995
[Ame95, Dan95].  1995/4 [Dan95].  1996
[Ano95f, UU97b].  1997
[ACM97a, ANS97, Acc97, MZ98, Uni98a, Uni98c, Uni98d, Uni98e, Uni98f, Uni98g].
19th [Ano96a, Tv92, Wie99].  1B [Lea99].
1st [ACM93a].

2 [BA97, DS97c, DFKN93, HG97e, HG97d].
2-6 [IEE95c].  2-adic [GK95a].  2-key
[HP99a, HP99b].  2-Proof [DFK93].
2.2gn [Ano97r].  2015 [Elk96].  2040
[BR96a].  2058 [RRSW97a].  2069
[FHBH+97].  2082 [BA97].  2085 [OG97].
20n [DBV96].  20th [CWM91].  21-25
[BS95].  21-January [USE91].  2104
[KBC97].  2138 [RRSW97b].  2144 [Ada97b].
2154 [MBW97].  219 [ECM96].  21st
[KG96, Sch96b].  2222 [Mye97].  2268
[Riv98a].  2284 [BV98b].  22nd [IEEE97].
2313 [Kal98b].  2314 [Kal98c].  2315
[Kal98f, Kal98d].  23rd [IEE98f].
2402 [KA98a].  2403 [MG98a].  2404 [MG98b].
2405 [MD98].  2406 [KA98b].  2410 [GK98].
2419 [SM98b].  2420 [Kum98].  2437
Almost [AMP99, Bra95d, CCD99, Mau90]. Along [BDC+95]. Alpha [Zim96a, Zim96b].


Analysis [AO96, AMP94, BKS99, BR97a, BP98e, BS97a, BPR9F9, Bro94, CM97b, CJRR99a, CRRY99, CH99b, DD99, Dra98, FM98a, FY95b, GS97, Gue98b, Gne96, Kea99, KSF99, Kmu94b, KJJ99, L197a, Lei99b, LvD98, MM99a, MT95, MDS99, MO99, NA95, Pai99a, PB99a, Pre93a, PJ99, Sch99k, Sha99b, She99a, SVB96, SW93, VN94, WS96a, WS96b, WS97, WB92, YMWP99, Y196, AA99, Abr97, Bar91, BCK98, BM95, Cha94b, Dan97, Don98, LM96, LLG10, Nas94, Pau99, PS98h, RS93, RS99b, Tha91, vT94].


Anguilla [Fra99, Hir97, Hir98]. Animated [HE98]. animation [HEG98]. Ann [Dob95b]. Anniversary [CFK+91]. annotating [DSSZ99]. Announcement [Ano99b, Nat92b]. Announcements [Ano95f, Ano95d, Ano95e, Ano97e, Ano97f, Ano97g, Ano98a, Ano94e]. Announces [Got99, Ano97u]. Announcing [Ano97h, Nat97b]. Annual [ACM94a, ACM97b, Ano95l, Bri92, Bri93, CH96, Cop95b, Cop95d, IE99b, EIE93c, IE94b, IE94c, IE94f, IE96a, IE97b, IE97f, IE98a, IE98f, IE99a, Kra98, Spi95, St93b, St94, USE99d, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, IE99d, IE99e, IE99f, Kal97c, Kob96, TM99, USE99e, USE99f, USE99c, Wie99]. anomalous [GLV99]. Anonymity [BD99a, DFTY97, FJ98, JMP99, STS99b].

Anonymous [DF98, DF99, FT99b, GGMM97, Jae96, Jae99, MS99a, OKST97, PW97a, RSG98, STS99a, SPP99, SGR97, Phi95].

Anonymously [Coh96]. ANSI [Ano94b, Ano96c, Bak92, Bas98, BK98a, BK98b, Jbh99, SS97]. Answer [WD99a, Ude98]. answers [Di 97a, Fre94, Ano92a]. Ant [BP95a]. Anti [Ano93a]. Anti-counterfeit [Ano93a].


Applicability [KCT94a, KCT94b, HM95]. Application [IBM93, BS99a, BSN95, Bar99, BGG95, BL96b, BL96a, Dam90a, Dam91a, Dav91, De 95, ECM96, FJRS96, Fun97, GPT91a, GPT91b, Gog99, QQ95, HNS999, HHY93, Hat97, He94, Ho99, IRR93, IR99].
Applications [Aga92, BGR98a, BFW99, CG98, CJR98a, CJR98b, CGB + 93, COZ99, Cré90, Dan96, DY91a, DFGH99, Duf98, DN94, Dwo97, Ebe93, FMM99, Far93, Fis98, IE95a, IEE97a, IEE97b, IEE97c, JMSI96, KSHW97, KSHW98, KSW99b, KSW99c, KM96a, Km94b, KT91b, Lan97, MS95f, OiDP98, OO90, PS96b, SY96a, DY91c, TN96a, TN96b, VV98, VP96, ZYR91, vW94, vW99, ACM99c, Ad91, An98b, BM90, Ber93, BM9+97b, BV97, Boy98, BP97b, CNG96, DI-DPS96, Dix94, Dom96, Eng99, FO98, GvP98, Gre94, GS94b, HMP95, JV98a, Kal95, KW92, KG93, LY93, LN94, Lub96, Me9f2, Mic97, MT98, NKC94, Ped91a, PC98, Rh95, Sch90c, Sch97c, Sha95a, SS94, Sin95, Sta97c, SS99, T+98, USE96e, Way98, YL93, ZYR90]. Applied [BJHJM99, HH98, MR95a, Sch94g, Schw9a, Sch94h, Sha99a, FFW99, FMR99, MV97, PR98, CMM93, Dav94]. April [ACM97a, Ano95c, Ano99c, Auc98, Chr98, Chr99b, Dar91, IEE95c, IEE97d, IEE98d, KK99b, Lon97, QV90]. Aquarelle [ADF98]. Arab [AK98, Arbiter]. Arbitrated [DY91f, HW98c]. Arbitration [Joh94, Kur94, PLWSN99, DS93, KOS95]. arcane [Beu94]. Archaeological [Ano97t]. Architectural [BS95c, PN92]. Architecture [IBM93, BCCD99, CJR98a, CJR98b, Con99a, Fei93, Fei96, Gut99, JDK + 91, MM99b, Muf93, NH90, NK98b, Oh99, PF94, RBvR94, Rus90, SS90, She92a, She93c, Tref99, Tua99, VGG93, YS99, Kar96, LS98a, Con98, JD91, LMJW93, SV99, SY92]. Architectures/390 [SY92]. Areas [Fum93, LE99, Van95b]. aren’t [Cha99a]. Arguments [BJY97, BD91, NOVY93]. Arias [DHMR96]. arising [APDS93]. Arithmetic [BP98a, Bre99, BP97c, Bus97, CD98b, DBVD96, KK99b, LL99, LD99, Mih94, NM96a, PR97, SSS98, SLJ93, CPPK98, ISO97, JS93a, Kal92, Kal93b, KM99a, Pos93]. Arbitrarily [De 98d]. Arizona [IEE99b]. Army [Mee98, Mee98, Dav98a, DR99b, Ros99]. Arnoldi [HRV99]. Array [MT95, DF92]. Arrays [BGS94, BGS96, BKK98, MT95, TT99, JM93]. Arresting [Mad92]. arsenal [Mc98]. Art [Eri99, Lan98, NM96a, Pre98c, She92e, BFS99a, BFS99b, Beu94, B+96b, PGV93d, PR98]. article [Bur98b]. Artificial [Ano97b, SBT99]. Arts [Tv92]. Asia [Uni98c]. ASIACRYPT [IRM93, KM96a, PSN95b, PSN95a].
Abbreviations

[ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94j, AS96, Atk95a, AR98, AC97, BA97, Bak99, Bal99, Bec99, BR97a, BG90, BR99, BCK96d, BCK96e, BM91a, BGS98, BR91, BBDF97, BGL99, Bis91, BHK99, BWM98, Ble98b, BV98b, Bor96, Bor93a, Bor93c, Boy92, Bru98, BAN90, CV93, CGM97b, COZ99, DLF97, DVPL92, DVW90, DY91f, DvW92, DH90, Dra99, DMFB97, Dwo95, ECM96, EPR99b, EPR99a, FGS96, FHBH97, FL96, GHY90, GLZ99, GL96, Geh94, Geh95, GN94, GM90, Gol90a, GBL94, Gue98b, Gui97, HK97, HA94a, HS94, HL92, Hi97, HJP97, HP98b, In95, IH98, JSZ94, Joe98, Jol94, KR95b, Kau93, KA98a, Koh90, KN93, KCCT94a, KCCT94b, Kra94b, Kra95, KBC96, KBC97, Kur94, KK95, KY92, KY92, KS97c, LABW91, LABW92].

Authentication

[Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Mau96a, MAM95, McM96, Mee98, MS95c, MS95d, MWW94, MTVZ92, Mor97, Mye94a, Mye97, NP97, OG97, OOK91, OM94, Opp96, Pkot94, PS98c, PLWS99, PSN91, PGV93c, Pre98a, Pre98c, MS95e, RS99b, RRSS97a, RRSS97b, Rog95, SNT93, SN93, ST94, SNT95, SN98a, SN98b, SSH93, SS96, SP99, SA95, SC96a, SCxx, Sch94d, Sch99k, Sga90, Sga91b, She97, Shi95a, Sho96, Sim96b, SVW91, SW94c, SKAM99, Sti91b, SL99, Tap90, Tay95, TSN93, Tun99, Ude98, Van95b, Van93, Wal95, WKHG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC+98, Ano97d, Atk93, BSP97, BGR95, BCK98, BCKx, BC97, BGL99, BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gu90, HS96b, Hor95].

authentications

[HC95b, HLL+95, HW98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin89a, LOW95, MS97, MF97, Men91, MC96, Nac93, NT94, PS98c, PS98f, PS98h, RS98a, RS98f, Sch99j, Sga91a, Sga93, SY96b, Sta99b, Stub91a, Sun98b, Syv93, Ts92b, Ts92a, TH99, Ver98b, WL94, XA98, Xie98, YL97a, YL97b, You97, ZK98b, ZH93, v93, Mye94b, Ala93b, Bor93b, WL92a].

Authentications [0090, KSL92].

Authenticator [Zuk98a].

Authentications [DF91a, SN96].

Authenticity [BK90, Lud97, M90, Way91].

Authentcode [Fly97].

author [Lea90].

Authorisation [COZ99].

authorities [Ame95, Ame96a].

authority [CFSY96, CGS97, JMO95a].

Authorization [BDPSNG95, Cas95, FL96, W990].

Auto [YY98c, YY99b].

auto-certifiable [YY98c].

Auto-Recoverable [YY99b, YY98c].


Automated [Dan97, FIP93a, FS93, FK99, GSN94, GDS91, She96a, SG95V9, VDDR99, W999, CD98a].

Automatic [CWM91, MM99a, Na97, SK97b, SK97a, Sch99k, WKHG97, DF98, OA99].

Automating [Bur99, Sm93a].

Automaton [Des99a].

Automata [DGV93, Gys96, DW96, MZ98, Tao94, TCC97, TC99b].

Automorphisms [VP96].

Autonomous [CK99, RZ99].

Autoscritcher [Dea98a, CF92, Cra92].

aux [Bec90].

Available [DDJ98c].

Avalanche [Cas96, CS96c, IT95, OC94, ZZ95, SZZ94a, SZZ95b, YT96].

avant [Blo98a].

AVBPA [BC97].

Average [DLP93, Koh99].

average-case [AD97, AD99].

Avoided [NMR95].

avoiding [ZW99].

Award [Pin98].

Awarded [DDJ98b].

Awards [Eri97a].

Aware [BCCD99].

Away [DDJ99].

Axis [AK99].

AXYTRANS [GBC93].
Babbage [Fra93]. Back [GC97, GO96c, WSFC99, IEE97e, WG97].
Bal [PNdbbbprm91]. Balance [RG99]. balanced [MCD98b, YT99a, YT95b].
Balatonfured [Rue93]. Ballot [CFSY96, BT94]. Ballots [Sal91].
Baltimore [ACM90, Ano96a, NIS92, USE92b]. Ban [Gar97a, BP98f, XZZ97]. BAN-like [XZZ97].
Banking [Chi92]. Barbara [Bri92, Bri93, Cop95b, Cop95d, Cre97, DGV93, Dae95, IEE97].
Barriers [Des92, RCM99]. Based [AW94, ADEDS99, BDPSNG95, BG90, BJY97, BS99b, BS99c, Ben99, BLM94, BBT94, BMT96, Bie98, BPR99, BMS94, BM96b, BM96c, Ble98a, BPRF99, Boli98b, Bol98b, Bra95b, BP97c, CC99b, CNS91, Cre97, DG93, Dau95, DNM98, DSSB95, DS96, DDP00, DMPW98, DDGM97, DQ94, Dem94, DF99, DKo97, EN98, EKL99, ENK99, FCH99, FBS97, FK99, FKM98, FJM96, FKS98, FR95c, GKR97, GJK99, GRB99, GN95c, Gys96, Hes97, HPS98, HJPT98b, JO97, Jia99, JSS94, JZ99a, KKS97, KG95, KP96a, KP97, KMM99, KA99, KMOV91, Kra94b, KHM98, LM93a, LM93b, LY93, LL97a, LM99a, LW91, Lin98, MNS97, MD99, MR95a, Mau93a, MM96a, MM99b, MM99c, MG91, MG98a, Mue99, MM98b, Mui99, NMR95, NM99, NOV93, NS98a, Nec96]. Based [NS97b, NMR98, OM98, OO93, OFF93, vO91a, Pai94d, Pen96, PL94, PRZ99, Poi99, PB99a, PV98, PK99, Pre97a, PMP99, RSA99b, Ros98a, SSN98a, SCT99, SC96a, SPS97, SE96, SJS98, She92e, Sh96, SM91, ST91, SSN99, SKIT99, SHT98a, Var99b, WCs95, WD99b, WS99, YKB94, YY97b, ZL99, vO91b, Ala93a, AW95, Ale98, AAPS92, BS96a, BS98b, BS97, BDH97, BBC98, BSB97, BCD98, Be97a, BB91, BCB97, BMM99a, BBL95, BFK94, BCC99, CC99a, CPS9, Cha95a, CW97, CS97c, CCH98, CLL99, CD95, Cus95, DD95, FSS94, FY96b, FY96a, GM91, GH99. GK95a, HZ93, HY93b, Has99, HSW96, He92, HI97, HLM93, HX94, HMP95, HW98a, HJPT98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JJ95, JG95, JG90, JY98, KM99a, KSL92, KM99d, Koy95, Ku92, KH97].
Based [NS97b, NMR98, NM99, NIS92, USE92b]. Ban [Gar97a, BP98f, XZZ97]. BAN-like [XZZ97].
Banking [Chi92]. Barbara [Bri92, Bri93, Cop95b, Cop95d, Cre97, DG93, Dae95, Dau95, DNM98, DSSB95, DS96, DDP00, DMPW98, DDGM97, DQ94, Dem94, DF99, EKL99, EN98, EKL99, FCH99, FBS97, FK99, FKM98, FJM96, FKS98, FR95c, GKR97, GJK99, GRB99, GN95c, Gys96, Hes97, HPS98, HJPT98b, JO97, Jia99, JSS94, JZ99a, KKS97, KG95, KP96a, KP97, KMM99, KA99, KMOV91, Kra94b, KHM98, LM93a, LM93b, LY93, LL97a, Len99a, LW91, Lin98, MNS97, MD99, MR95a, Mau93a, MM96a, MM99b, MM99c, MG91, MG98a, Mue99, MM98b, Mui99, NMR95, NM99, NOV93, NS98a, Nec96]. Based [NS97b, NMR98, OM98, OO93, OFF93, vO91a, Pai94d, Pen96, PL94, PRZ99, Poi99, PB99a, PV98, PK99, Pre97a, PMP99, RSA99b, Ros98a, SSN98a, SCT99, SC96a, SPS97, SE96, SJS98, She92e, Sh96, SM91, ST91, SSN99, SKIT99, SHT98a, Var99b, WCs95, WD99b, WS99, YKB94, YY97b, ZL99, vO91b, Ala93a, AW95, Ale98, AAPS92, BS96a, BS98b, BS97, BDH97, BBC98, BSB97, BCD98, Be97a, BB91, BCB97, BMM99a, BBL95, BFK94, BCC99, CC99a, CPS9, Cha95a, CW97, CS97c, CCH98, CLL99, CD95, Cus95, DD95, FSS94, FY96b, FY96a, GM91, GH99. GK95a, HZ93, HY93b, Has99, HSW96, He92, HI97, HLM93, HX94, HMP95, HW98a, HJPT98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JJ95, JG95, JG90, JY98, KM99a, KSL92, KM99d, Koy95, Ku92, KH97].
Based [KK96, LRW93, LvdLB96, LS98a, LW99, LZ90, LCL95, MRS99, MS98a, MLA91, Mau91b, Mch92, MZ98, MM95, MT97, Mu92, MVZ98, NS97c, NR95, OP99, OU98b, Ole95, Pat91b, Pat91a, PS97, PC98, PGCSN96, PPBC97, Por93, PGV91, PGV93b, PV94, RP95b, SV95a, Sha94, SRR98, Sim98c, SM90, SS95b, SS95c, SMK98b, Son99, SK94, Ste95, SS98b, SZ98b, Tan90, TA97, TAP90, TC91, VNM99, Ven92, Wan92a, WK97, Wil93a, WW95, X98, YWC97, YL97c, Zhe95b, ZPY96, vO92, vT94, CD96, KY99, Dhe98, Por93, TY98b, TY98a]. Bases [BCE94, MSDS90, Yua92]. Basic [CF99, Des98a, vdL98, OK98, YHK99, Zie97, van98, BDH97, Rac90, dVdI98, Hel98b].
Basics [Bal99, IEE97]. Basis [FBS98, LL99, The95, Wal98, BK98g, Car98, FBT96].
Batch [BGR98a, BY93c, BY93b, BFP99, Fia90, Fia97, BGR98b, YL95a].
Batch [Ban93, Gar97a, Gar97b, Gar98b, SB97, Fro96]. battleships [Jar97]. Bayesian [BBDF97, Jen99]. BCH [CC98, FC94]. Be [BF99a, BV98c, Cha93, CD98b, DY91f, Ev91, GSV99, NMR95, Way93c, Ano90, Ano95c, Ano98b, CP91, CS95, Ev92, Ev93, LF97, NMR95a, NMR95b, NOY93, Ros98c, Sch91b, Sim98c, van97a]. Beach
Byte-Oriented [Mas94, YLCY98a, YLCY98b]. Bytes [Yu97]. Byzantine [Bea92, Bor95].

C [Sha99a, vdWS97, vS97, Bak92, Bas98, BMS99, DS99, Gar98b, Hei98b, Kal92, MGL+98, Sch94g, Sch94a, Sch94h, Sed92, Ste90a, Ste90b]. CYNTIA [WBBL99].

C2 [Ste92]. CA
[RD99a, C99b, IE93a, IEE93c, SJ97, USE93, USE96b, USE96g, W99]. Caching [STSW99]. Cactus [Ano97p]. CADE [HB99]. CADE-16 [HB99]. cAESar [Koe99].


Calculating [CFK+91]. California [ACM93b, ACM98a, Ano97a, Bri92, Bri93, Com96, Cop95d, Des94b, FJV97, IEE92c, IEE93b, IEE94d, IEE95b, IEE97b, IEE97h, IEE97t, IE98a, IE98b, IE98d, Kal97c, Kob96, Kra98, Nat98, RP97b, Spi93b, Spi94, USE92a, USE96c, USE96d, USE96f, USE99d, WE99, van96, Sch98b].

Camel [VCF+90, Zav99, Miy90]. Call-Coverage [Zav99]. called [Way95]. Cambridge [And94a, And96c, CFK+91, Chr99b, GoI96d, Lom97, RBCE99, Sch94a].

came [Fro96]. Camera [Fro96, SKWH96].

Campbell [CFK+91]. Campbell-Kelly [CFK+91]. Campus [VN94]. Can [Ano93c, BF99a, CF91, Cha93, CD96b, CMYY97, DY91f, EvH91, GV99, NMVR95a, NMVR95b, NMVR95c, Riv98b, Sim98c, Ste95, BGV97a, CG05, Ev92, EvH93, LF97, NOV93, Sch91b, Ude98, Way95].

Canada [ACM94c, CFG96, GS94b, IEE94f, IEE96d, TM99, Yua92, Ro99b, Tas98].


Cards [Ano96j, Ano99e, BDB92, Cha99a, CM99c, Con98, Con99a, Cor98, CH99a, DDJ98d, DD98e, DDJ98b, DDJ98d, Deu97, Deu98, Fan96, F91, FGPL96a, FGPL96b, FOM91, GL96, Gut98a, HKQ99, JT97a, Koe99, KCCT94a, KCCT94b, MSN99, Mye96, NM96b, PV98, Roh99, SKW98d, SS99a, Sch90b, SR96, Smi98a, Taa99, VV98, ABKL91, ABKL93, Ale97, Ano98h, BGV97a, Bro97, CJRR99b, DS98a, Dhe98, DT98b, DF97, Gau97, T97, AG99, Ba99, BF99a, Gir99, GSTY96, LW99, NF99].

CARD T0AP [SGPV98]. Carmichael [Pin97]. carrier [SVWMB95, SOB98, VSB95]. Carry [SM91, DF92].

carry-save [DF92]. Cartesian [DVW90]. cascade [BCK96b, BCK96c, VL93].

Cascades [GC90, Men95b]. Case [ABDV98, BY93a, BGG94, BR95b, BGM97a, BGM97b, BPR99, DSSB95, Duh90, FL99b, FR95d, GRB99, GM99a, LBHM99, Mad92, MD99, MR95a, Mar98a, PK99, Riv98c, Var99b, AD97, AD99, BHRR99, DL99, LMS97].

Case-Based [DSSB95, FR95d, GRB99, MD99, MR95a, PK99, Var99b].

case/average [AD97, AD99]. Cases [BMC95, Bl99]. Cash [BFP99, Bra95b, Cha93, DFTY97, DT98a, EN98, EN99, FO97, Jak99b, LR98, NM98, OO90, 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, RS98]. Cautious
[Gla99b]. CB [Eph98]. CBC
[BR96a, KMS95a, MD98, PA98a]. CBC-Mode
[PA98a]. CBCM
[BK98a, BK98b]. CBR [GAGCDAFC99].
CCI [WCS95]. CCI-Based [WCS95]. CD
[Ano96i, GTGW94, Ros94, UFC94]. CD-ROM
[Ano96i, GTGW94, Ros94, UFC94]. CDE
[Ano97r]. CDL [HHW99]. CDMA
[KSB96b, KMS97, She94c, SKB97, TY94]. CDMF [JMLW94]. Cell [Omu90]. Cellular
[BKK98, DGV93, HHW99, NC97]. BFM^+97b, BK98f, MZ98, NKC94, PV90, Sim99, WSK97a, WSK97b]. Center
[Ano94d, Ano96a, IEE96f, NIS92, LWC96]. Centered
[MP99, VC99]. Central
[ZTR99]. Centralized [KT96]. Centre
[IE97c]. centric [BGT96]. Centroid
[LML98]. Century
[CWM+91, KC96, Alv98c, Sch96b]. Cerebellar [FCH99]. Cerebral [DHQ98b]. Certain
[CS91, MS93, MM92a, CFS97, Ev92, Kuk99]. Certicom [BT97]. certifiable [YY98c]. Certificate
[Bra93a, FL99b, HFPS99, RSA93c, Riv98b]. Certificates
[Bra95b, Bra95c, NKP99, TAP90, DS90a, FFW99]. Certification
[Kal98c, KM99c, LA98, Ame95, Ame96a, GH96]. Certified
[Gir91, Mer90b, RS98b, SG99a]. Certifying
[BY93a, LN98]. CFB [PNRB94]. CFP
[Ano96d]. CFR [UU97b, Cll97]. Chaffing
[Riv98d]. chain [JV98a]. Chaining
[BKR94, CJM95, Jas96]. Chains
[YY98a, dR95]. Challenge
[Ano97c, Ano97w, BCE^+94, DDJ98e, DDJ98f, Sim96b, WD98, WSN98, BT97, Ano97c]. Challenges
[Ano98c, BS97b, GB98, McC96, Cer97, FM98b]. Challenging
[CM99d]. Chamber
[Yar90]. Chameleon [AM97]. chan
[XtM99]. Chance [GB98]. Chang
[Bur94a, Bur94b, HLC96]. Chang-Wu-Chen [Bur94a, Bur94b]. Change
[FY99, Wal99b, MW98a]. changeable
[HYLT99]. changing [MW98a]. Channel
[AO96, AVPN96, ADESDS99, BI99, Bro94, KSWH98a, KSWH98b, KSWH98c, MM92a, MM92b, OKST97, WB92, BM95, FC94, PSB97, Pi95]. Channels
[BDI^+96, Cre97, Des96a, vD97, KI97, Lip94, MM96a, MK94, MM94, PN92, SI94, Sch94e, Sim93, Sim96a, Sim97, VW95, WD99a, Des96b, Grub98, MAU91c, SI93b, Sch93b, Sim94c, Sim98a, Sim98b, Tod97, YL97a]. Chaocipher [Joh98]. Chaos
[BGR94, BLM94, Ano96l]. Chaotic
[Bih91, GK97, HNS91]. Chaotic-Map
[Bih91]. CHAP [Sim96b]. Chapter
[Kal97b]. chapters [Tat98, Tat99]. Character
[BL99, Sab94]. Characterisation
[SB95]. Characteristic
[KMKH99, Kob91b, MV98, SS98a]. Characteristics
[Ano93j, Str93a, Str93b]. Cheap
[LT98]. cheaper [Sch98c]. Cheaply
[Ano93j, Str93a, Str93b]. Check
[Ano95b, Ano95a, LH93b, HNC96, HLC99]. Cheating
[GP99, Rad94, OK96b]. Check
[BK95c, Bl098c, Ray94]. checker [Dan97].
Checkers [Fis97, KA91]. Checking [BGR98a, Bol98a, Bol98b, BD97, FL99b, FGY96a, GMV98, PV98, BCR98, FGY96b, MHPS96, MW94]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93].

Chinese [HOQ97, OiDP98, XtTmW94]. Chinesecrypt'94 [XtTmW94]. Chinese [DiDPS96, GO96c, QD91, WHW95, Yu99]. Chip [Ban94, Bro96, Ele98, Gar97c, GC97, Got99, HMvT94, Lan97, MPPS95, MHMW98, VVDJ90, Way93b, DQV96, Kan96, Moe97, Pos98, RKD94, Sm94a, Uni95a]. Chipkarte [Kip97, Kip99b]. Chips [Ano99c, GO96c, Omu90, Ano97-27, IEE98b]. Choice [Cha99a, Way98]. Choices [Hon98, Van98a, Wel95]. Chor [BFS98, SH95a, SH95b, Vau98a, Vau98c]. Chosen [Ble98a, CG99, CS98b, Dam91b, GC94, KSW98a, KSW98b, LL94a, PBGV90, RS91, ZS93, BJQ97, CP94, NY90, SNT95, Sah99, SG98, Tze99, vT93]. chosen-ciphertext [Sah99]. chosen-content [SNT95]. chosen-message [BJQ97, Tze99]. chosen-plaintext [vT93]. chronicle [UFC94]. chronology [Kah98a]. Chua [YWC97]. Chump [Wal99b]. Chung [XtTmW94]. Chung-kuo [XtTmW94]. Church [Ole95]. CINDI [DSS99]. Cipher [Alv98c, AM97, ABK98b, ABK98c, BKR94, BAK98, BD94, Boy90, BCA98, Car97b, Cla97, Cla98a, CJM95, DGV94a, Dae95, DKT97b, DRK97a, DW94, EM93, Gol97d, KR94a, KMA98, Knu98c, KR99a, Kuh98, Lim98, LS97, Lip99, Luc98a, Luc99a, Luc99b, MNSV97, MD98, Mat94b, MT99a, Mau91d, Mil96a, Miy91, MSK98, MSK99b, PA98a, QG90, RDPB96, RRSY98, Ros98a, SZ96, Sch94b, SK96c, SK96d, SKW98c, SKW98f, Sch98d, Sch98i, She94b, SMK98a, Van98d, WBDY98, Yi96, YLH98, YLC98a, YLC98b, ZYWR91, Zhe97a, Lip98, Bar92a, Bar95, BK95a, BMP97a, BS95a, CS96b, CS97b, Cra92, DAV98a, DAV98d, DAV98c, DAV98f, Fra93, Gad98, GGH98, Gol98b, Gol99b, ISO97, Kru98, Lew92, LCL95, Mac98, Mat93, MY93a, Mei94, RT93, Se98b, YL97c, Zun98, SV98, Ers99, Van99b, Van99c]. Ciphering [DNRS97, GN95c, Mas94, Nor95a, Nor95b, NO96]. Ciphers [Ada97a, ABDV98, AAG90, AB96a, BR99a, BR99b, BDR96, CNO98, Cha94a, CS91, Cle91, DR99a, De99, Din94, Fil95, Gus96, JF97, Jak98, J99b, KS98a, KS98b, KS98c, Knu94b, Knu99b, Kob99, LMM91, LM93a, LM93b, Luc96a, Luc96b, Mat96a, Mau91a, MS91, MT99c, PRS99, Pat99, PK95a, PK95b, Pen96, Pra97a, Rec98, RP97a, Rob95a, Rob95b, Roe94, She94a, She94d, SM91, Van98b, Van99a, YY98d, YY98b, ZM90, Zhe90, Abe98b, BK98a, BK98b, CD98a, Cot99, DGV94b, DX91, FSN93, Gar96a, Gar97d, GSN94, Gol95b, Har96a, HLMW93, HMXW94, HSW94, Jak99a, JV98a, Lai92, LMM92, LRW93, Nyb95, PGV93b, P94V9, Rev91, RP95b, Roe95, SB95, SAM97, Tay94, Win93, W998]. Ciphertext [BK98d, Ble98a, CG99, CD97, CS98b, Dam91b, LL94a, MRS99, Miu93c, RS91, Riv93a, TOU94, ZS93, CP94, NY90, Sah99, SG98, Vu95]. Ciphertext-Only [BK98d]. ciphertexts [Des95]. Circuits [KT91b, KT98, WG99, JS93a, LMS97, YWC97]. circulating [Ano96]. Cirencester [Boy95a, Boy95b, Dar97, Far93, Wal99a]. CISST [AA97]. City [IEE99a, USE95b]. Claim [GO96c]. Claims [DS97a]. clandestine [W998]. Clara [USE93]. Class [vD97, Ou99, Uni96c, FR94, HBJW93, KSB96a, LZ90, LZ91a, ZUK98a, vT94].
Classes [Haw98b, Pai99d, Haw98a, Sze98].
Classical [Bra94a, MC92, Nic98a, Nic98b, CD98a, Mas99a].
Classification [BD90, LSVV95, PNFK95, Uni96c].
Classifier [CIBM99].
Claw [BHT98].
Claw-Free [BHT98].
clearly [Los98].
Click [WSFC99, Ken95].
Client [DL99, Kon95, Oh99, SL99, GGK+99, Sin95].
client-relationships [GGK+99].
Client-Server [DL99, Oh99, Sin95].
Client/Server [Kon95].
clients [AG95].
Climate [TGKI99].
Climbing [MCD99].
Clipper [Pri94, Fro96, Ban94, Bro96, Hof93, Kan96, MS95f, RKD94, Smi94a, Uni95a].
Clipper-like [MS95f].
Clipping [Hof93].
clicks [JP96].
Cloak [Gre90].
Clock [DHSS95, GO96b, GM91, GO95, Men95b].
Clock-Controlled [GO96b, GM91, GO95].
Clocks [DG95, DGT96, Yah94, Gon92].
closer [Coh96].
closure [MOM91, PS93a].
Clueless [RS98c, RS98d].
Clustering [DDJ98a, HE98, Kurn97].
CM [CNST98, Kob91a].
CM-curves [Kob91a].
CMOS [BS95c, ECD+99, YS99].
Code [Gla99b, LFCK99, Sut99, NM96a].
Co-dimensional [LFCK99].
Co-operation [Gla99b].
Co-Processor [Sut99].
Co-processors [NM96a].
Co. [CFK+91].
Coast [SZ93].
COBOL [Car97a].
Code [CJ99, HR90, JI99a, Kip99a, Kur94, MV93, PV98, QD91, Sch94g, Sch96a, Sch94h, Str95, Tod97, WK97, WF94, Zim95b, Ala97, Ano97i, BSNP97, CC98, CLW98, GA98, HM97b, LJWH97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG+00, Mea98].
Code-Breaking [QD91].
code-cracking [WS96c].
Codebreakers [HS93, Kah96b, Smi98b, Yu99].
Codebreaking [Car97c, Car98, Dre92, Sch98a].
coded [HG97e].
codemaker [Mar98b].
CODER [Sto90].
Codes [ACM94b, AW94, AR98, BGS96, BVFD99, CCZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, Gib91, Hof99, Joh94, JS95b, JI99b, KKS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWSN99, Pen96, Pra96, Pre98a, RV99, Rus93a, SN93, SNW98a, SNW98b, SD99, Sga90, Sga91b, SB94, SVxW91, Sta96b, Ste91b, Ton96, Van95b, Wri98, Ada91, Ala93a, AW95, BSB97, BI93, Bru91, CC98, Cha95a, CMM93, FC94, Gre90, JK96a, Kahl91a, KO95b, LY94, LMS90, MSS93, MPL99, Moh92, SNT93, SNT95, SK94, Ste95, Sti91a, Su98, SS98b, TSN93, TY94, Wann92a, Wel97, Win93, YL97a, vT94, JS95a].
codewords [PS97].
Coding [Ber96b, IEE97e, KRS99, KH98b, LW91, Lip94, Sch99b, Sch99c, SW95b, Van95b, Wal99a, Ada91, Boy95a, Boy95b, Dar97, DDP96, Far93, Gan93, KSB96b, KSB97, Kue90, Mit92b, Sab94, Sch98b, Sga91a, SVWMB95, SOB98, Shp99a, SMS99, TA97, Ger97].
coefficient [GK95b].
Coefficient [Nac97].
Coffee [Den97].
Cognitive [CF99, Ger99b, MMM+98, PUF99].
Cohen [PBGV90].
Coin [BN96, Jue99, PW97c, Ueh95].
Coins [EO95b, WSFC99, EO95a].
COIRS [YKY99].
Cold [Joh95].
Collaborating [CF99].
Collaborative [BV98a, Neuf91, LS98a].
Collaborators [Gla99b].
College [Far93, IEE97a, UFC94].
Collision [BP97a, Dob97, PG91, Rus93b, Vau93, VW94, vW99, Dob95a].
Collision-Free [BP97a, Dob97, Rus93b, Vau93, Dob95a].
Collisionful [Gon95, BSNP96a, BSNP96b].
Collisions [Ano95a, CJ98, DBGV93, dBD94, Gon95, Sim98c].
Colloquium [Ano97p, vWN99].
Collusion [BS95b, BS98, EKK99, PW97b, LM96].
Collision-Resistant [EKK99].
Collusion-Secure [BS95b, BS98].
Colonel [BP95a].
Color [ADESD99, NNEK97].
Colorado [Sch99b].
Colossus [Ano97-28, Car97b, Car97c, Car98, Pin98].
Column [Bra94a, Dwo95, Bra90b, Bra90d, Bra95d].
Computability

Computational

Concealing

Concept

Concerning

Concerning

Conference

Computer-related

Computerized

Computing

Computing

Conference
Vau98c, Vv97, Ver95, WSK97a, WSK97b, WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Wie90, Wie90b, Wie90a, WBDY98, YLD99, YLH98, ZYR91, Ada92, Alv98b, BSN95, BB94, Ber93, BS90a, BS91e, BS91f, Bih92, Bih95b, Bih98b, BK98e, Bri99, BD95a, Bowxx, Bur98a, CV95, CD98a, Cra92, DYL98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, Gol95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kah98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LS98a, Lew92, Mat93, Mih96, Mil92, Moh92, Mor92, NS97c.

cryptanalysis [O'C95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZYR90, ZH90].
cryptanalyst [Rey96, Rey97, Rey99].
cryptic [Wri98].

CRYPTO [Fei91, ACM94b, Ame96b, And96a, Bar93a, Bar93b, BE90, HP98a, HMvT94, Koo97, LKB+94, Mah96, MPPS95, Neu97, Sch98c, Way95, Way96b, Neu95, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kah98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LS98a, Lew92, Mat93, Mih96, Mil92, Moh92, Mor92, NS97c].

Crypto-Chip [HMvT94].
Crypto-Coprocessors [HP98a].

Crypto-Engine [BE90]. Crypto'91 [DBGV93]. Crypto'95 [NS98b, NS98c].

CryptoAPI [Boy98]. CryptoBytes [Cry95, Riv95c]. cryptochip [PP96].
cryptograms [Har94, Web93].
Cryptographers [WP90]. Cryptographic [AG98a, AG98b, IBM93, Ano96f, AB97, BDPSNG95, BDPSNG97, BH93, BY93a, BGM97a, BGM97b, BBT94, BMT96, BFKL94, Bol98a, Bol98b, BDL97, BDP97, Bra95a, Bra96, BD91, CS96a, CJR98a, CJR98b, CPOR97, CF95, CD99, Cop94b, Cre97, DG9V, DC98a, Dam90a, Dam91a, Dan95, DIF94, DY90, DY91a, DY91d, DY91b, De 95, DS97a, DF91c, DK91, ECD+99, El98, FGR92, Fis98, FGY96a, Fun97, GI99, GS94a, GK99a, Gol96c, GS97, GQ95, Gut99, HHT93, HHT97, Hel94, Hwa97, Il96, Ivec91, JD+91, JD91, KM98a, Kal88, Kal98d, KV94, KS99, Kha93, KP99b, KT91b, KT98, KS97b, LMJW93, LL97a, LHB96, LM96, Mac94, MM99a, Mum96b, Mum97b, MS90a, Mil96b, Mjo93, Mos98, Mun91a, Mun91b, NM96b, Ng99, NS99b, NR94, NK98b, Nur94, Nys99, ÖPH+99].

Cryptography
ANS97, ANS98b, Ano99h, AA93, ABDS96, Avo98, BCD+94, BGG94, BGG95, BGR98a, Bel98, BBB+91, BBE92, Bir98, Bia93, BK95d, BL96b, BL96a, BGV93, Boy95a, Bra90a, Bra94a, Bus97, Cae96b, DDJ98a, DL96, DP98a, DP98b, Dav91, Dav96, DG96, De 93c, Des94a, DHQ98a, DHQ98b, Des98c, Dif90, DNN91a, Dro96, Dwo97, Ele99, Eri99, Fer96, Fis97, FBS97, FJM+96, FJRS96, FGLP96a, FGLP96b, Gant93, Gen97, Gol95a, Gol97a, Gol97b, Gon98, HK99a, HP98a, HSSI99, Hat96, Hed97, HL93b, Hir98, HAH94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLM96, HH98, HBKL99, JR96, JM97, Kal97a, Kal98c, KS98a, Kal99, KS98+92, Kun98a, Kub94, KA91, RSA93f, Lac93, LM94b, Lin96a, Los97, MY91, Mau99a, Mau99b, Mau97c, McC96, MP91, Mit92b, MKS99, NC97, Nic98a, Nic98b.

cryptography

PKA+98, Pat96, Pf95, PT95, PGCSN96, Por91, PB99b, RSA99b, Rad97, Rhe94, Rit99, Riv90b, Riv93b, Riv97b, Ros96d, RK99, Sal99, DP91, Sas99a, SKBxx, SSS98, Sch94g, Sch96a, Sch96b, Sch97a, Sch97b, SSv+98, Sch98f, Sch94b, SV93, SG96a, She93a, She93b, She93d, Smi94b, Smi97b, Sta99a, SW95b, Ste91, Sti95, Sti98b, Sut99, Sw97, TN96a, TN96b, Tv92, Tow98, Tsu92c, Wad98, Way96a, Wah99, Wah93b, Wor96, WC97, YWC97, YST99a, YY97f, YY97d, YST99b, ZYWR91, Zim98, dRHG+99, Uni96c, AA95, Ace97, Ada91, Alv98a, Ano97q, Ano97-30, ASM98, BH98, Ban94, Bea97a, BR96b, BFS92a, BFS92b, BHH999, BW97, BOMP+97b, BSS99, BBS98b, BD98b, BC96b, Com96, Con99, Dam96, DDB95a, DDB95b, DVL96, DiDP96, DNN91b, DN95b, Eng99, Far93, FM91, FK93b, Fra99, Fra93, Fri96.

cryptography

Gar96b, GZ91, Gol99a, Gol97c, Gre94, GTGW94, Hir97, Hru95b, Hwa91, Hwa93, IZ98, Iz99, Imp92, Joh97b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdL98, Luc95, MB94b, Mau93b, MY98, Mei96b, MV97, Mi97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Ny94, Org98a, Odi94b, PG97a, PG97b, PC98, PP92b, PGV93d, PR98, Riv98c, Rot95a, Sal90, Sal96, Sch92e, SSM+97, SMD+99, Sch99e, Sch90c, Sch97c, Sh99a, Shp99b, Sin99, Siu99, Sh98, SMS99, Sta96d, Ste98a, Tas98, TM99, USE96e, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wa99a, vS97, Sha99a.

cryptography-dedicated

[AN96b].

Cryptography-in-the-Large [Bl93].

Cryptoki [An96k].

CryptoLib [Lac93].

Cryptography [Ano93g, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dam90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ano97t, Bau97, Bec88, CW94, Cop95b, Cop95d, Dam91a, Dam99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, He94, IRM93, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lind90, Lip93, Mau96b, McC90b, Mei92, MV91, New97, Ny98, OiDP98, PSM95b, QV90, QG95, Rat96, Rue93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Unixxb, Uni95b, Web93, Wie99, Wil98a.

cryptology

[Bec97].

CRYPTON

[DB+98, Lim98, Lim99].

Cryptonomicon

[Ste99a].

Cryptoprocessor [Pai99b].

cryptos

[Hag98].

cryptoscheme

[MMI97].

Cryptosystem

[AM90, BI95, BDGI98, Ber97c, Bih91, BMS94, Ble97, Bon99, BM97, CC99b, CG99, CS91, CS98b, CW91b, Cus97, Gib91, Gib96, GC91, GC94, GGH97a, Gys96, HD96b,
HPS98, HJPT98b, Hwa91, Jab90, JS93b, Kie98, KS99b, KT91a, LR96, Lan97, LCL92, MM96b, NMR95, NS97a, NS97b, NS98d, NS99a, Ngu99a, Ngu99b, OU98a, SG99a, Sam98, ST91, Sun98a, Tak98a, Tak98b, Vau98a, Vau98c, Wal99c, Wan92a, WY93, Yam99, AMV93, AD97, AD99, Aa97, AAP92, ACBR90, Bao94, Bf94, BS97, Boy97, BCCG99, CC99a, C98, CW91a, CW97, CW97, C98, Cle96, CS97d, DW96, G95, G99d, HNSM91, HY93b, He92, HRF96, HJPT98a, HLLC96, IKNY98, Jon90, JQ98b, KASH90, KSK96, KM99d, KT93, K96, KM99d, KK96, LG97, L92, LC96b, LC96c, Lon91, MMT90, MM90a, MM90b, MI90, Mou91b.

cryptosystem
-[Miy90, NS97c, NS98e, OU98b, Ole95, Ped91c, Pet91, Roe99, SW95a, SH95a, SH95b, SM90, SS95b, SS95c, SX90, TY92, Tan90, TCC97, TC99b, TC99a, Ven92, Wan92b, Wu92, XLP99, XW97, Yu92, Zher96b, Zha91, vT90].

Cryptosystems
-[BDHJ98, BHSV98b, BHSV98a, BS91, BLM94, BS91c, BS97a, BS90b, CGJ+99, DP98c, ESST99, FY98a, FY98b, FY99, GJKR99, GPCS96, GGH97b, Gor93a, HS98, HM93, Hiro97, Iss90, Kal98g, KL95a, Kor93, KT93, KOT91, KP93, LH93a, Len99a, Men93, Men95a, Mic93a, Mic93b, Miy93b, MOM91, MM98a, MM98b, vO91a, Pai99a, Pai99d, Poi99, RY97, Rud91, Sma99, Son99, dWQ91b, Wie98b, WZ99, Yam98b, Y97b, YY99b, dWQ91a, vO91b, AA99, Ale92, And94b, APDS93, BC90, BS91a, BS90a, Bf92, BF96, BQ97, BBL95, BK98g, CZ90, Ca99, CC98, Cha95a, CL97a, CNST98, C99L, Con99, Des90b, Des90a, DF90, Des93, ES97, FK94, FSS94, FSMY97a, FMR99, Go90c, GH99, GP97, Has99, HNM98, Hor99, JM96a, Jar96, JQ98a, KM99a, Kob90, Kob91b, Koc95, Kos97].

cryptosystems [Kos99, LL96, Lan96, LS98a, Ler97, L90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odl90, OS91, OS92, Rac90, SS98a, SS98b, SS95a, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Y98a, YY98c, Zho94, ZPY96, vO92, vT94, Wa98].

CS [Ano93e, Ano94a, Pin98, SV98, Vau99b, Vau99c].

CS-cipher [Vau99b, Vau99c, SV98].

CSP [DS97d].

CTS [BR96a].

Cube [Per93].

cubic [CL99, GH99, Koy95, KK96].

cultivate [AHdJF97].

Cultural [UFC94].

cultures [Rat96].

Cunning [Beu94], Cunningham [YY98a].

Current [JJ98c, Ril96].

curve [AMV90, DP98c, Dem94, ESST99, Fer99b, HSSI99, Kal97a, Kal98g, KMK99, Kob98c, Len99a, LD99, Men93, Men95a, Miy93b, OFF93, RY97, SOOS95, SW93, WZ99, AM93, AS98, BC90, FM99, GP97, HNM98, IK99, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LL96, MV90, Miy99, SX90, VZ97].

Curves
-[Ano93n, BS91b, CTT94, De 98d, DMPW98, Hes97, JQ97, JM97, KMOV91, MS93, MM96b, Miy96, SNNP99, BR94, Bf910, BS91a, BS99, CPPK98, LL99, Eng99, FR94, Gal99, GLV99, GK99b, IS99, Kob91a, Koy95, KK96, Ler97, Mou91b, MV93, Miy93a, VZ97, XL98, Z98].

Curvilinear [SCG99].

cusick [YT96].

Custom [Nor95b].

customer [Nor95c].

customised [GN95c, HHD99].

Customising [NO96].

cut [BL99].

CutRes [BLM99].

Cuts
-[Gar98a, Den95].

cyaneide [Mar98b].

Cyber [Ano97i, Ano97-29].

Cyberbanking [Mur96].

CyberMall [Mar95a].

Cybernetics [LS98a].

Cyberpunk [HM91, HM92, HM95].

Cyberpunks [Zim96b].

Cyberspace [Ber97b, Col96, Gar97c].

Cyberwar [Kau96].

Cycle [GAGCDACF99].

Cyclic [PS97].

Cycling [SS99b].

Cylotomic [SW95a].

Cyclotomity [Bo90].
cylinder
DEFACTO [BDDG99]. Defeat [Luc98b].
Defects [Dav96]. defense [RS93, Bax97].
Definability [GM99b]. defined [Ler97].
Defining [BG93, BMRW98]. Definitions [Blo99, Uni96c]. Deformation [DFL99].
Deformations [NA95]. Deformed [Hru95a, Hru95b]. Degree [CTT94, Jak98, Paf99d]. Degrees [ACD94].
Delinquency [De 93b, De 98c]. Deliverables [Hru99a]. delivered [Sun98b]. Delivers [MB99a]. Delivery [HG97c].
Delusions [Rat96]. Demand [Gar97c].
Deportation [CFG96]. Denial [Nee94]. Denk [CWM+91]. Denmark [Dam90a, Dam91a, Mad92]. dense [Ort95b, Ort95a]. density [CJL+92].
denting [Gib95]. Denver [Sch99b].
Department [Cli97, Uni97d, UU97b].
dependency [MAO96]. Dependent [Con99b, DJL93, FB98, IOS94, Poi99]. depending [Gon92]. Deploying [CF95].
Deployment [Var99b]. Dept [Uni96c].
Depth [Mac98]. Derived [OO98].
Deriving [Ton91]. DES-based [Por93]. DES-CBC [KMS95a, MD98]. DES-II [Ano98c]. DES-Like [Kim93, KP93, Way93a, BS90a, BS91c, CCZ98].
DES-X [KSW97a, KSW97b]. descent [Jen99].
Description-Processing [IND99].
Descriptive [HKL94]. Descriptions [IKM99, IR99, MSHP99, SG95, TYD99, MCD98a].
Descripto [DSV99, GM99b, LMSV99, Sch99].
Descriptors [PNFK95, Sar99]. DESE [SM96, SM98b]. DESE-bis [SM98b].
DESEO [HDC99]. Desiderata [Lee99b].
Description-Processing [IND99].
SBTV99, VNM99, WL94, YS99].

Design-Space [KV99]. Designated
[Cha95b, JMSI96, Oka94]. Designed
[YY98d, YY98b]. Designer [MUSM98].

Designers [FM98b]. Designing
[AKF94, BV98a, BK95c, BM94b, CH99b,
DL99, DMVC99, Ger99a, Gor93a, HJ99,
JS93a, Kem99, PM99a, PD99b, Sch94c,
SW97a, SW97b, SZZ94b, Ste94a, SAS99b,
TL999, Zhe90, CG05, Hor99, HLC99].

Designs [DJHP98, FY95b, Jun96, KK95,
Mou99, RB99, Wot99, Ton96]. DESIRE
[JKVP99]. Desk [GRB99]. Desktop
[Ano97r, Fuc99, Los97]. Destination
[LTEH99]. Destruction [SY98]. DESV
[CCN95]. DESV-1 [CCN95]. DESX
[Rog96]. Detail [Zeg93]. DeTeBerkom
[GH96]. Detectable [Vt97]. Detecting
[Gor93a, Mad92, PM98, SG96b]. Detection
[BS95d, ENK99, HCDC99, Hr98, LH93b,
LKD98, LT98, LML98, Ruo94, TYD99,
ZTR99, HC96, MMHW98]. Determination
[Bie98]. deterrence [van96]. Developer
[CM99b, Di 97b, DT98b]. Developing
[CF95, SCT99]. Development
[Ano97h, Bar99, Bas93, GRB99, HNSS99,
IR99, LL93a, Nat99c, Natxx, VDDL99,
Way98, You96, AMV93, Ano97-30, LS98a,
Mli95, NBD+99, Sta97c]. developmental
[Ram92]. Developments
[Ano95a, PRB98a, Sim97]. Deviates
[Ran01]. Device
[Hru96, Ano91b, CM97c, Uni94b]. Devices
[BDHJ98, Hwa92b, Hwa92c, LS98a, Pos92,
Pos93, Uni94a]. devoted [FT99b]. DFC
[KR99a, Ste99c]. DGSA [FM98b]. DHCP
[Dra99]. DHWM [ADF98]. Diagnosis
[GX99, MR95a, PW99]. Diagnostics
[RRSW97a, RRSW97b]. Diameter [FP99].

Dickson [Pie93]. DICTA [KG93].

DICTA-93 [KG93]. Dictionary
[Jas96, Luc98b, BCR98]. Dictyostelium
[Ram92]. Diego

[ACM93b, IEE97b, Sch98b, USE96f].

Difference [LP94]. Different
[KBRS97, Sch99h, RT93]. Differential
[BB94, Ber93, BS90a, BS91c, BS91e, BS91d,
BS91f, Bi92, BS93b, BS93a, BS97a, BK98d,
BKPS93, CJ98, Con99b, Dae95, Din94, Fer98,
Haw98b, Haw98a, KTM+99, Kau96, KM98b,
Kob99, KJ99, Kwa93, LMM91, LH94,
Lan95, Mat96a, Miy93c, MS98, NK93,
OM94, Pai99a, Sch96c, SM98a, VK98,
Wag98a, YLH98, Ada92, CV95, KY95b,
KYxx, KM96b, LMM92, O'C95, OG95,
RP95b, TN97, Way95, YT95a, YT95b].

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

Differentially [Ny94b]. Differentials
[BB99a, Fer99a, KRW99, BBS98a].

Difficulty
[KP96b, Riv93a, ZZ96, Hor99, Riv95a].

Diffie [BY93c, BY93b, BBR99, BM99a,
BV96, Bon98b, Bon98a, CFS97, CS97d,
HY98b, HY98a, Ka97a, Koc95, Koc96b,
Lat98, Mau94, MW96c, MW96b, MW99,
RSA93b, Van95a, VW96, WM93, vOW96].

Diffusion [Mas99b]. Digest
[FHBH 97, GTC94, Kal91, Riv92a, Riv92b,
Riv90a, Riv91b]. Digit [TK99].

Digit-Recurrence [TK99]. Digital
[Ame95, Am96a, ANS98b, Ack98, ALO98,
AW94, AR97, Int91a, NIS94, Ano96e, Ano97-9,
ASW98, Aur96, BC90, BM99a, BM99b,
BdM94, Ber97b, BM94a, BM96a, BM96b,
BM96c, BS95b, BS98, BTH96, Boy97, Boy98,
Bra93a, Bi99, BWF99, Car95, CR91,
CPO+98, CHO+98, DDM98, DDM96,
E199, EGM90, EGM96, FWF99, FKMY98,
FBS98, Fr93, Fro97, FOM91, Gar97c,
Gar98b, GR97, GDB+97, GB98, G096c,
GQQ+91, HKS95, HG96, HG97c, HEC98,
HA96, HW97, IEE97c, IEE98d, JLO97,
Jue99, KKS97, Kob97, Kob98c, Kra93,
KH98a, LQ98S98, LM95, LW96, LL98, Lut98,
LR98, MSO96, Man98, MMST98, MB99a,
MW98b, Mer90b, Mer97, MTN97, Mos98,
DDNM98, DDP90, ECM96, Gal96, Max94, MTVZ92, PKOT94, PB99a, SiK93, SR96, YKB94, vHH97, BGH+95a, BMS96, BFS98, Bur94a, BD95b, CFS97, FL93, GBL94, HI97, Hwa92a, Hwa92b, Hwa92c, JLM+94, Kha93, LC96a, MY93b, Mu92, PS98e, Pos92, RRF97, SI93b, SY96b, Syv93, SM95b, TH99, VS95b, WM93. distribution-specific [Kha93].

Divergence [Sga90]. Diversity [Mau90].

divertibility [CDP95]. Divertible [BBS98b, BD91, NMV99]. dividers [PV90].

Dividing [MB99a]. divisibility [FR94]. Divisible [EO95b, EO95a]. Division [MB99a].


DMS [Bax97]. DNA [PC96]. Do [AW99, Ber97a, DDJ98c, DDJ98f, HK95, SS99a, Ber98, Ue98, Way95, ZKOY99].

dobb [Eri97a, Eri97b, SSM+97, SSv+98, SMD+99]. Document [BLMO94, BLMO95, BMO95, HSB96, LMB96, MML98, Max94, Sea95, Bur98a, HS91, van97b].

documentation [Sim95]. Documents [Rot95b, SB97, Ban94, DSS99, Rot95a, Sch93e, SH98].

dodson [Lip98]. Does [MGL+98, Mar96, Ril96].

Dollars [Ame96b]. Domain [ABB99, DVP92, Gar97a, Gar98b, Mon93, P99b, Ano97q, BBCP98b, BP98d, H97e, KMP99, NP98b, TK98].

Domains [Buu98, CGM97a, CK90, Mar97].

Donald [CFK+91]. Don’t [Hus99, Way96b, Chi99a, Chi99b]. door [Yu92].

doorbells [Law98]. Double [Ano92c, Cha90, HP99a, HP99b, Pai99b, Bar95, KL95b]. Double-Agent [Cha90].


Doubly-Iterated [ABDV98]. Down [GC97]. downgrader [Mch92].

Downgrading [KM92]. Downloaded [JPL99]. Downloading [Sch97d]. dpe [lPNdbbbprm91]. Dr.

[Er97a, Er97b, Gar97d, Riv93a, Riv95a, SSM+97, SSv+98, SMD+99]. Draft [Ano94b, An96k, An97b, Got99, Mic93b, Ame95, An96c, An95a]. Drawing [EMMN98, HEQL98].


Drive [GC97], Driven [CHLT99]. Drives [DJD98a, DIF94].

Dromquinna [IEE96c].

DS [TY94], DS/CDMA [TY94].

dSs002FP [Kuh98].

DSA [AA95, Acc97, Len96, Mi96, Sim93, Sim94d].

DSP [IEE97c].

DSP56000 [DK91].

DSPWS [LW96].

DSPWS-96 [LW96].

DSS [Nat91, BGM97a, BGM97b, GJKR96a, Koc95, Koe96b, Nat94c].

DTR [Ano93k].

DTR-1 [Ano93k].

DTS [BH95].

Dual [Jas96, LL99, FBT96]. Dual-workfactor [Jas96].

Duality [ZZ97, ZM91].

Dublin [IEE97a].

Duel [Got99].

Dump [Got99].

dumps [Me98].

during [Don98, Jol95, Rat96, Wil98a].

Dutch [vL96].

DV [GC97, LT98].

DVD-Video

[LT98].

Dwork [GHH97a, NS98d, NS98e].

Diana [KBS99].

dyes [SBTV99].

Dynamic [AGY95a, AGY95b, Ano97r, BDHK93, Dae98, DP99, DSS95, FT99a, FY99, FR95d, G97, NT99, SG99b, SP99, WWH95, BH93, BCDV94, Bhu95, BCDV96, CT99b, HC96, Po98, SS94].

Dynamical [AGY95b].

Dynamic-Resharing [AGY95b].

Dynamically [PS96b, RO96].

dynamics [Ohi99].

E-Cash [DFTY97, Yac99a, Yac99b].

e-commerce

[VM96, DD98c, Jak99b, Liz98, Gar97b].

E-mail [LF97, Ril96, Bac95, Sta94a, Ano93j, Got99, RS98b, Sch95c, Sch95d, SH97, An95c, Gar97b, Str93a, Str93b].

E.I.S.S.

[BFS92a, BFS92b].

E.I.S.S. [Dan95].

E.I.S.S.-Report [Dan95].

E2
KMA+98, Kob99, MT99a. EAP [BV98b].
early [Alv98c, Mar96]. Earth [YHK99].
Earthcam.com [Ano98j]. Ease [HJL99].
Easier [GMD98, BBR99, Sch98c, Way95].
East [Str95]. Easy [Sim94d, Ken95].
eavesdrop [Way93b]. eavesdropping [RK99].
Ecash [Sch98h]. ECC [Cer97, Kal98e].
ECC/DLP [Kal98e]. EccFan [PKA+98].
ECCp [BT97]. ECCp-97 [BT97]. Echo [GLB96].
eciphering [Blu97]. ECMMA-219 [ECM96].
ECMAST [Dan96]. Economic [Mos98].
Efficiency [Bas98, BM99a, DKKK98, KS97c, BBS93].
Efficient [AGS97, AGY95b, BBDW96, BDV93, BF97b, BF99c, BFP99, BDB92, CS97a, CMN99, C39, CG98, CDD+99, Cre97, DR99a, DT98a, DN94, FH94, FOM91, GSY99, GJK96b, GP97, Ho99, Hwa92b, Hwa92c, JMO95a, JOMP+98, LHY93, LLH96, LL99, Len99a, MSN99, MS93, MPL99, OS91, OS92, OFF93, OS93, PS98b, Sch90b, Sch90a, Sch91c, Sch93f, Sha94, Ste98b, Ueh95, Wie94, Wie96, Wie97, Wie98a, Zim99, dR95, DB95b, CPPK98, CSS97, Dhe98, FMY98, HK90, HJK99, KC95, KSK96, MI90, MS98b, PPKW97, Per91, Pf95, Sch93g, Sha95a, SKB97, VNM99, Von92a, Von92b, Xie92, ZI98]. Efficiently [Jas96, Bak92].
Effort [Natxx].
Eigenvalue [All98].
Eighth [ACM97b, IEE92b, ACM96b, USE99a].
Einstein [SvA+98]. Elastic [OMV98].
Election [CGS97]. Elections [CSFY96, Iee91, BT94, FO093].
Electrochemical [DDJ99]. Electronic [Avo98, Bar93a, Bar93b, BFP99, Brot95b, BLMO94, Cha92b, DB98c, DSS99, DF98, EO95a, EBF97, Ken95, LM98a, Lin98a, Lin98b, Man95, MZ98, OO90, Ped95, PW97c, Rv97a, STS99b, SB97, Sch99i, Sin98, TRS+93, Tra99, USE95c, USE96d, USE96b, USE98b, VJ98, AMS96, AC97, BH98, Com97, Cha92a, DMW94, DSS99, DF98, EO95a, FB97, Ken95, LM98a, Lin98a, Lin98b, Man95, Mit92a, RP97b, Sch93e, Sch95d, She96a, VNM99, Way93b]. Electronically [Ped99]. Electronics [IEE97g, IEE98c]. Elegance [Sch99c].
Elektronicznej [Sch95e]. Elementary [Mi192, Tat98, Tat99]. Elements [FC99].
Eleventh [CH96, IEE92d]. ElGamal [AA99, Ble96, KSK96, LK96, NK98a, TY98b, TY98a, VvT97, Zho94]. Eliminating [GGH97a]. Elimination [BLM99]. Elizbeth [Uni92]. Elliptic [AMV90, Ano95a, BS91b, BSS99, CTT94, De 98d, DP98e, DMPW98, Dem94, Eng99, ESST99, Fer99b, HSS99, Hi97, JQ97, JM97, Kal97a, Kal98g, KMKH99, Kob98c, KMOV91, KT93, Len99a, LD99, MS93, Men93, Men95a, MM96b, Miy93a, Miy93b, Miy96, Miy99, OFF93, KY97, SOOS95, SW93, SSNP99, VZ97, WZ99, AMV93, AS98, BGR94, BC90, BS91a, CNST98, CUP98, FMR99, Gal99, GK99b, GP97, HNM98, IS99, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LLH96, Ler97, Mau91b, MV90, MV93, SX90, XL98, ZI98]. Elliptic-Curve [Fer99b, Kal97a]. EMACS [McH92]. email [Kar96]. Embed
[Ano97o, MT94, Ano97-27, Zha96].

Embedded [BKS99, Bar99, DDJ98a, LT98, Lin98, BBCP98a, BP97b, CC95, KP99b].

Embedding [ACD94, DS97d, GO95, Gol96b, HK99h, ZK95, Sch91a].

embeddings [CT99b].

EMEF [Org98a].

Emergent [Jun99].

Emerging [Kal99, Org98a].

Empirical [WW98b].

Employing [Obe99].

emulator [Obe99].

EMV [Gui97].

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 [BR95a, Ber98, JSY99, Ril96, WT99, Rot97].

Encrypted [AW99, Bla98, GMCF95, GLZ99, Gil98, Jas96, YY91, BTD97, DF97, STW95, Kip97].

Encrypting [Ano97r, Bla94b, Lom94, Luc98b, EW99, SS99e, Beu94, KAK96].

Encryption [ASW99, AAB+97, Ada97b, Ada98, ARRW99, And98, ABK98a, Nat93b, Ano94c, Ano96c, Ano96l, Ano97h, Ano97b, Ano97v, Ano97x, Ano99c, Bac95, Bal97, Ban93, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b, BDP98, BS99b, BS99c, BRW99, BS93b, Bir95, BB95c, Bla96a, Bla96b, BF99b, Ble98a, BC95c, BFS96, BY92, Com94a, Com94b, CDNO97, CMN99, COP+95a, CH98, CMK98, CT99a, Cop94a, Cout93, DD98e, DDJ98c, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DS97c, Ele98, FIP94, FN94, FY95b, FY97, FH94, FO99a, FO99b, GSY99, Ga90, Gar97a, Gar97b, GC97, Gar98a, Gar98b, GK98, Got99, HG97a, HG97b, Hat96, HK98, HK99d, Hub98, Jol98, JM96b, Kal93a, KY95a, KR96a, Kal98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kum98].

Encryption [KBRS97, KH98b, KYDB98, Kwa93, Kwa97, RASA93f, Law98, Lef99, LK91, LW91, LM91b, Lin93a, LS98b, Luc97, Luc98c, Luc99c, LW90, MGL+98, Mat94a, Mat97, Mer91, Mey96, Mil95, Moe97, Mue99, Mii99, Nat93a, Nat94b, Nat94d, Nat97b, Nat98, Nat99a, Nat99c, Natxx, NBD+99, NHI90, Ohi99, Ola94, Ori96, Pat98a, Pat98c, Per91, PRZ99, Pin97, RSA93a, RSA94, RP94, Riv95c, Riv95b, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SvA+98, SKNO98a, SKNO98b, Sch99a, Sch99b, Sch93d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SWK+99d, SHK+99a, SWK+99e, SE96, See97, She95b, She92g, SB98, Sim95, SM96, SM98b, SB92, Sm93b, Sm97a, SB99, Sta97c, SW99b, Sto90, TPH+98, Uni97b, Uni98a, Uni98c, Uni98b, Uni98d, Uni98e, Uni99b, UU97a].

Encrypted [Uni97b, Uni98f, Uni98h, Uni98g, Uni97c, Uni98j, Uni98i, BV96, VR98, WSK97a, WSK97b, War98, Way93b, Way93c, WSFC99, Wei91a, Wei91b, Whe94, Wir98, Yin97, YY97c, Yu97, Zhe97b, Zie97, Zol93, Aus96, Abr97, Ala93a, All97, And94a, Ano90, Ano92b, Ano94c, Ano95c, Ano95k, Ano96d, Ano96m, Ano97a, At94, AM99, Ban94, BTD97, Bax97, Bea96, BR94b, BR95a, BDJR97, BR97b, BBI90, Bet95c, Bi97c, BFN98a, BC96a, BMS96, BFS98, Bow93, Bro96, Bus96, Com97, CCN95, Cha94b, CLW98, Cle96, Cl97, Cl99, 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, Kuo90, LM91a, Lam99, Lee95, LC97a, Los98, MR99, Mar95b, MM95, MLI97, Mol98, Mra95, Nat93c, Nor95c, Oel97, Pos92, Pos93, Pre95a, QN98a, Rev91,
Ril96, Riv95d, RKD94, Rot95a, Sab94, Sch98b, Sch94i, Sch98c, Sch99j, She96a, Sm97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, TX92, Tsy90, Tha91, Tho96, TY98b, TY98a, Ts90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vad95, Vau98e, Ven90, Vu95, Wad98, Wel95, Whi93, Wil93a, Wl93b, W590, You97, You97, Zaj97, Zan90, Zer96a, vOW91, vT93, An90j, An93j, Hon98].

encryption/authentication [Sch99j].
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 [Mc90b].
Endured [Che92].
Energy [DFL99].
Enforce [BDS98].
Enforcement [Cae96b, Cli99].
enforcers [Way93c].
Enforcing [Ano97n].
Engine [BE90, CM98, She92d].
Engineering [Ano98f, D5G99, EKLM99, IEE96d, LBHM99, SSS98, Sm98a, AN94, IEE97k].
Engines [T99, Way93a].
England [ES98, Cur98].
Enhance [FO99a].
Enhanced [An95c, AR98, Ken93, LK96, Zan90, Zeg93].
Enhancement [HWJ98, Lin93a, Lin88a, Lin89a].
Enhancements [JM96b].
enhancing [HY95].
Enigma [CWM*91, Har96b, Kip97, Kip99b, Obe99, Ano91c, Bl98a, Bl98b, Bl98c, Cra92, Kah91a, Kah98a, Kip97, Kru98, Mi96b, Mus92, Tu99, We97].
Enigmas [Gad91].
Enjoyable [CM99d].
Enough [CFK+91, De98b].
Enschede [Hei96a].
Ensuring [CM97, Rot95b, ZG96, Way91].
Enter [Wor96].
Enterprise [ECD*99, FY99, Mar95b, Wad93, SY92].
enterprise-wide [Wad93].
Enterprises [Joh98].
Entities [KM99c].
Entity [BR94a, BWM98].
Entrepreneur [Pin98].
Entropy [Bro94, EHMS99, KSH9W7, KSH9W8].
entwerfen [Hor99].
envelope [SOB98].
Environmental [RS98c, RS98d].
Environments [GST96, SKAM99, DNS99].
EPIC [Rot95a].
EPS [An96i].
equally [Ito91].
Equation [Cop95c, LG97].
Equations [Por98, RZ99, BMP97a, Cus95, G95b, LCL95, Lun92, Sun91a].
Equilibria [Ett98].
equip [Int91b].
Equitable [BDS98].
Equivalence [BS99b, BS99c, Fis98, KK98, Man94, AD97, AD99, LD9W].
Equivalent [BV98c, De98d, Gib91, GO93, HTY99, MM96b, Miy96, Oka94, P99c].
Era [DDJ98c].
Ergonomic [DDJ98c].
Erika [Mat99].
Errata [Con99a].
Erratum [An91a].
Error [AW94, AR98, BGS96, Cha99c, DLR97, KKS97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, DLP93, JY98b, 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 [GHH97a, SHK99b].
ESA [Spy95, YS91].
ESA/390 [YS91].
ESAT [PGV93d].
Escrow [AAB*97, Bla96c, BDS98, Cae96a, CM97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96a, HM98, KP98, KP96b, KB92, LWY95, M96b, Mar97, MS95f, MK99, Nec96, SYM98, Sam98, SM95a, Vt97, VDB99, YY99b, An94e, BDH97, BR96b, DH96a, Des95, Fre94, KL94, Mao97, Un95a].
Escrowed [Bas95, Com94b, FIP94, Nat94d].
ESIGN
EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, vHPP93, Bea97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, Ole95, Pai96). **Extended-Certificate** [RSA93c]. **Extending** [Bad99, Hus94, MI99]. **Extensible** [BV98b, WBDF97]. **Extension** [BP98a, CTT94, FHBH+97, MS90b, LMJW93, STW95]. **Extensions** [CD91, DT98a, Law98, NW97, Atk93, GH99, GKF95, 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]. **Facilitation** [BP98a, CTT94, FHBH+97, MS90b, LMJW93, STW95]. **Facility** [AKF94, Bis90, She96a, YS91, JMLW93, STW95]. facing [KG96]. facto [Pri94]. factor [KM98b, SVWMB95, VSB95]. Factored [Ano97b]. **Factoring** [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pai99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KKF98, McK99, Me96b, Riv95a]. **Factoring-Based** [Kal98e]. Factorisation [DHW95a, Jon90, DHW95b]. **Factorization** [Ale92, DDLM94, MM98a, MM98b, Odi95, vO91a, Sho97, vO91b, LLMP93, Mac98, Whi93, vO92]. **Factorizations** [BMS94, NS97b, NS97c]. **Facts** [Ano91b]. **Faded** [Alv98a]. fading [Tod97]. Fail [BP97a, PP97, SSNP99, vHPP93, And94b, Pfi96c]. Fail-Stop [BP97a, PP97, SSNP99, vHPP93, Pfi96c]. **Failed** [BCE+94]. fails [DH96b]. Failsafe [KL94]. **Failure** [Ano95a, Ber97c, Gar98a, TYD99, FR95b]. Failures [CH98, JQ97, Moo92, Sim94b]. **Fair** [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, MKS99, SS99e, SS99f, Tra97]. **Fairfax** [ACM93a, ACM94a]. **Fairly** [HD96a]. fall [Odi90, Rob98b]. False [LKD98, She92b]. **Families** [Kal98e, Per99]. **Family** [KT98, My91, RP97a, ABC+98, BGH+95a, FSS94, It991, Kobo9, SRRL98]. **FAPKC** [DYL98]. **FAPKC3** [TCC97]. **FAPKC4** [TC99a]. **Far** [Str95]. Fast [AGS97, AMV90, AO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bih97b, Bih97c, BHK+99, BD94, BK95d, BGV96, CS91, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBV96, DNR97, EPR99b, EPR99a, Gar97b, Go96a, HJPT98b, HP94, HCY96a, J99a, J99b, KR94a, KTM+99, KP99a, KP97, KR99a, Kmo99c, KMK99, KA91, Koy95, LM95, Maur90, Mer91, Mih94, MM95, NS99a, NK99, PRR97, Pre95a, R955, SW97a, SW97b, SOOS95, SV93, SB98, Sho96, Sil97b, Tak97, Tak98a, Tak98b, T+99, Vau98d, Vau98e, AMV93, AB96b, Ano98j, CV94, DKR7b, DV96, GGH+98, HJPT98a, Jenxx, LRW93, LC98, MZ98, Pv95, RRSY98, She92c, SN94, SH99, SAM97, SGSD99,YL93, Go96d, OA94]. **Faster** [Luc96a, Luc96b, WZ99, YY99b, Bosxx, Mih96, Sch98c]. **Father** [CFK+91, DDJ99]. Fault [BS97a, DSS95, GX99, OKST97, P99a, RB94, IEE94b, T9+91]. **Fault-Tolerant** [DSS95, RB94]. Faults [BDHJ98, BD97, CH94a, FY99, Gar94, JQBD97]. **Fauvel** [CFK+91]. Fax [Ano91b, Int91b]. FaxModem [Ano93k]. **FC** [Fra99, Hir97, Hir98]. **FCC** [Gar97b]. FCD [ISO97]. FDR [Low96]. **FEAL** [GC91, KR95a, MY93a, M90, M91, TN97, BS91e, BS91d]. **FEAL-** [M90]. **FEAL-8** [GC91]. **FEAL-N** [TN97]. **Fears** [Gar97c]. **Feasibility** [DN95a, NF97]. Feasible [Lip94]. Feature [Shar99, SD99]. Features [ADEDS99, Zav99]. **February** [ACM98a, Fra99, FJY97, Go96d, Hir97,
Hir98, IZ98, RP97b, SJ97, Wo93a, Wo93b, van96, Ano94c. Federal
[Ano97h, Ano97x, Lee99a, RP94].
Federated [SS99b]. Feedback
[CJM95, GKW95a, Ros98a]. Feistel [Jut98b, Knu94a, SN93, SK96c, SK96d, van99a].
Fermat [LLMP93, McK99]. Few [FJRS96, Mei98]. Feistel [Jut98b, Knu94a, SK96c, SK96d, van99a].
FFT [DBGV93, MS90b, Sch91c, Sch93f, SVBJ96, van93].
FFT-Hash [DBGV93, Sch93f, Sch93f].
FFT-Hash-II [Vau93].
FFT-Hashing [Sch91c].
FFPs [Nor95c]. FHFC [KKW99]. FHFC-Tool [KKW99].
Fiat [Nac93, OOK91, OO93]. Fiber [Tow98].
Fiber [HLMP96]. Fibonacci [SMS99].
Fiduccia [CKM99]. Fiduccia-Mattheyse [CKM99]. Field [CD98b, Knu98c, LL99].
LLMP90, LL93a, MR95b, Ros93, SY99, TT99, CDEH96, Dav98a, GH99, Gor98b, Hwh93, Has99, Pom94].
Fields [BP98a, BMT96, BL96b, BL96a, BP97c, De 98d, LO91a, LO91b, Mas91, MFG95, PS97, Ano90, Gal99, LN94, MVZ98, SW95a, Sch91a, Shp99a, Von92a, Von92b, ZPY96].
fifteen [Den90]. Fifteenth [CFK91]. Fifth [SJ97, Un97a, Un98c, Un98d, Un98e, Un97b, Uni98f, Uni98h, Uni97c, Uni98k, ACM93b, USE95b].
FIGHT [De 93b, De 98c].
FIL [AB99a, AB99b]. FIL-MACs [AB99a, AB99b].
File [ANS98a, AW99, Ano97a, Bln94b, Gil98, Mau97b, RC95, HSK97, MKKW99, SK97d].
Filtering [Sch97d, LL98b, LY94]. Final [RIP95b, RIP95a, BFS92a, BFS92b, BP95].
Financial [AA95, ANS98b, BFS97, FL99b, Fra99, Hir97, Hir98, Lan97, Rev97b, Sw97].
Finding [BMRW98, Cop95c, Ler97, Riv91a, Sim98c, YY98a, CC98, Car97c, Sta94a].
Fingerprint [DDJ98g, DDJ98h, HWH98].
Fingerprinting [Ano99b, BS95b, BS98, DF99, Hei96b, PS96a, PW97a, PW97b, Sas99a, YST99a, YST99b, DF98].
Fingerprints [HJPB97, OMI93].
Fingerprints [HJPB97, OMI93].
Finite [B95, BGD98, BMS94, BVFD99, CD98b, DKKK98, Gys96, KPR99, K94, Kob98c, LO91b, PS96b, She92e, Shp99a, Ano93k, Bao94, BI94, BGR95, DWF96, DYL98, DF93, FSS94, Gd99, GH99, HW93, Has99, Jun96, LN94, MK92, PS97, Pie93, Tao94, TCC97, TC99b, Von92a, Von92b, Wal98].
Finite-Impulse-Response [She92e].
Finite-Size-Particle [BVFD99]. Finland [Nyb98]. FIPS [Nat93b, Ano93f, Nat93a, NIS93b, Nat94a, Nat95, Nat99a].
Fire [Way93b]. Firewalls [GLZ99, Opp97].
Firms [GC97]. Firmware [MNSV97].
Firmware-Oriented [MNSV97]. First [BCB97, GPS98, Hir97, KP99b, KW99, Law98, Mat94a, Nat98, Nat99c, RD99b, ACM99b, And96c, Dob98, HOQ97, IZ98, NBD99, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni97c, Uni98k, USE95c, RD99a]. First-Order [KW99].
Fish [BD94]. Fishermen [Ano96].
Fissures [DDJ98e, DDJ98f]. five [AK96]. fix [Ano98j]. Fixed [FK93b, Mae98, HP94].
Flexibility [Wed99]. Flexible [JPL99, LL94b, AG95, BP97b, Ts90].
Floating [Gar97b]. Floating-Point [Gar97b]. Floradora [Fil95]. Florence [EE92d].
Florida [IEE93cc, IEE94c, IEE96f, IEE97]. Flow [STS99b]. Flowers [Pin98].
Flows [Per99, WL99]. fly [PS98h]. Focus [GO96c].
focusing [Com96, USE96c]. Foil [MB94a].
[AW94, GM97, LHL95b, LHL95a]. Forget
[DFIJ99]. Forgotten [Ano97t]. forimage
[XA98]. Form [Cha93, STP93]. Formal
BR97a, BFN98b, Bol98a, Bol98b, Boy92,
GF93, Gue98b, Mea95, PD99b, SM95b,
Tou93, WK96, AHJ97, AAPS92, Ata94,
BFN98a, JW01, ZLX99. Formality
[ACD94]. Format [CDFT98, Nys99].
Formats [ASZ96]. Formed [Gue98b]. forms
[Gar97c]. formed
[Mok97]. Formulae [KV94, WD99b]. Forty
[OW95, Uni96b, Far93, IEE93a].
Forty-Secure [BM99a, BM99b].
Foundation [Gol95a]. Foundations
[Ada91, BDFM99, Gol97a, Gol97b, IEE92a,
IEE96a, IEE96c, IEE97f, IEE98a, IEE99a,
JR96]. Founder [Pin98]. Four
[HK99, Koe99, Riv91a, DL95].  
Fourier [MS94, NA95]. fourteenth
[IEE95c]. Fourth
[OV95, Uni96b, Far93, IEE93a].
FPGA [GTG94, Kap98]. FPGAs [KP99a].
FR [HSSI99]. Fractal [DS96, SD99].
Fraction [BDF98]. fractional
[BR96b]. Fractions
[ISS90, KE97]. Fragments
[Gol95a]. Framework [Boy92, DGV93,
Hed97, PS99f, PW99, SL99, VP99, Com97,
HN94, LS98a, P99c, T998, DT98b].
France [Ch98, DEQ92, FR95a, GQ95,
GQ95, Van98c]. Francis [Lea90]. Francisco
[Ano97a, Ano98f, USE92a]. Franchon
[IEE92a]. Franklin [WD99a]. Fraud
[Neu92, VGP93, VvT97]. Fraud-Detectable
[VvT97]. frauds
[Sga93]. Fray [Gar97b, Law98]. Free
[BP97a, BHT98, BDI96, CD98b, Dob97,
Er97b, GJM99a, GJM99b, HBK99,
Rus93b, SK95, All97, BT94, Des90b, Des96b,
Dob95a, Ili94, Van93]. Free-Space
[HBK99]. Freedom
[Cae96b, Uni97a, Uni98c, Uni98b, Uni98e,
Uni96b, U97a, Uni97b, Uni98f, HM96].
FreeNIX [USE98c]. French
[Bl098b, Fut94]. Frenkel [CFK91].

Frequency
[BP98c, MSH99, Ano90, Tod97].
Freshness [KYG92]. FRG [Oht96].
Friedman [Uni92]. friendly [Bus96].
Friends [DD98e, DDS98, Sch92b].
Probenius [CPPK98, Graxx, KMK99].
FROG [WFS99, Wag99b, GLC98, WFS98].
Front [He97]. Frontier
[Bar93a, Bar93b, HM91, HM92, HM95].
FSE [Bil97c, Van98e]. FSE99 [Kmu99c].
FTP [SS93]. Fujiyoshina [IRM93].
fulfilled [Mar96]. Full
[BS93a, DH90, SK98c, SK98b, Pos93].
Fuller [CFK91]. Fully
[BC99a, BCD96, HE98]. Function
[BJY97, BDP97, BP97c, CP91, DGV93,
DG93, Dae95, DC98a, DDP90, Dob97,
FGY96a, HILL99, HL99, MCD99, NSS99,
PBD97, Sch91c, TOU94, AB96b, DK94,
DDFY94, DIF99, FGY96b, KS96b, KSB97,
LTT95, MIZ98, MVZ98, PK97, Sch91a,
SRL98, SS95b, SS95c, YL97c, ZPY96,
d94]. Functional [Yam99]. Functions
[AV98, Ano95a, BP98c, G97, BCK96d,
BCK96e, BNS98b, B99a, G99, BGS94, BM94a, 
BL95, BHT98, CDD90, Car93, DGV93, 
DY90, DY91d, DY91b, DFL99, ECM96, 
EPR99b, FP99a, FBS98, GJKR96b, JQ97, 
KTM99, Kim93, KP96a, Kra95, LM93a, LM93b,
LM95, MS99b, MS90a, Mer90a, Mer91,
MS95f, Mil96a, Mon93, NR98, OS98,
P93b, PGV92, Pre93a, PGV93a, PGV93c,
Pre97a, Pre99, Pre94b, Q90, Roe94,
Sch91b, SZZ95c, SRY99, ZZ95, Zhe90, 
vW94, BSN96a, BSN96b, BD92, BGR95,
BCK96b, BCK96c, B9HR99, BK98c, C99,
CDG95, Cus96, CS96c, Dam90b, Gol96a,
Gon95, GHS93, HSK97, HLM93,
HX94, HYLT99, ISO97, JC95, K95b,
Lai95, MCD98b, O’94, PGV91, PGV93b,
Pre94a, PGV94, PV95, RP95b, Roe95,
Rom90b, SZZ94a, SZZ95b, Sim98c, Tsu92b].

functions
fundamental [IEE97e]. Funds [GBC93].
Funktion [MPS94]. Further
[Pre95b, WKS+99, WD97]. Fusing
[DMFB97], fusion [KH97]. Future
[Fuc99, HP98b, OdI95, PT95, PM99b,
Sch97a, And98, BFS92a, BFS92b, Mar96,
NIS92, SB92]. Future-Adaptable [PM99b].
Fusing [DMFB97]. fusion [KH97]. Future
[Fuc99, HP98b, OdI95, PT95, PM99b,
Sch97a, And98, BFS92a, BFS92b, Mar96,
NIS92, SB92]. Future-Adaptable [PM99b].
Fusion [DMFB97]. fusion [KH97]. Future
[Fuc99, HP98b, OdI95, PT95, PM99b,
Sch97a, And98, BFS92a, BFS92b, Mar96,
NIS92, SB92]. Future-Adaptable [PM99b].
Fuzzy [Blo99, CIBM99, FCH99, KKW99,
Tro93, ZHJ98, CS99]. Fuzzy-Control
[KKW99].
G [KSW96]. G-DES [KSW96]. Gabidulin
[Gib95, Gib96]. GAC [ZZ95].
Gaithersburg [IEE94b]. Galois
[Mas91, PSR97]. galore [FK94]. Gamal
[Jab90]. Gambling [HS97]. Game [Et98].
Games [Mye96]. Gate [TT99]. Gateway
[KBR97, MB99b]. Gateways
[Bec99, VDDR99]. Gauss [GvP98, Mon93].
Gbt [HK97]. Gbt/second [HK97]. ge
[PNddbbbrmr91]. Gehteschrift
[Kip97, Kip99b]. Gemmell [Geh94]. Gene
[Cap94, CO98]. General
[BC95a, BK95b, BPRF99, CL98, FDB93a,
ISO97, Ive91, KKTQ91, KP93, NOV93,
OK98, St93a, Ben94, DD95, Des90b,
FDB93b, GN95a, Pf96c, Sch91b, Sim98c].
general-purpose [Sch91b]. Generalised
[GS99b]. Generalization
[Jac90, HKM95, MSS93, TC99a].
Generalized
[BBM95, BFS98, CT97, HL93a, Jut98,
LL93a, LH93b, Man96a, PS96b, Bad99,
BBR99, BCCG99, Kuc92, Por93, Son99].
generate [Wer93a, Wer93b]. Generated
[SVBJ96]. Generating
[Ble96, De 98d, FMM99, Len96, Len98,
MS95f, WBY99, CH7b, SH99].
Generation
[ARV99a, ARV99b, BG98, BGM97a,
BGM97b, Bir98, BF97b, BDF97, CD96,
DF91a, GJKR99, Gil99, Gut98b, HL99,
Kal97b, KS98c, MW99, Mat96b, Man90,
Mih94, PS98g, ROT94, RS98c, RS98d, SN96,
Si97b, WI99, Bout94, FMY98, GTS90,
LL96, M99c, PS97, PS98b, SH94, Bou94].
Generator
[FIP93a, HILL99, JK99, KSF99, KW99,
MS95b, PS98b, Daw93, Jenxx, M95a,
Mih96, PC98, Rev91, Sin99, TSY98, Wal90].
Generators [HL99, KSWH98d, Kra90,
ZYWR91, CS96b, CS97b, Imp92, Kos99,
Lag90, Pat91b, Por93, SGD99]. Generic
[Bel92, CM99a, MS98b, Tua99, ZK98].
Genetic [BS99a, LC99]. genigma [Obe99].
genius [Ano97]. Genomic [MUS98].
Geodesic [Blo99, LFCK99]. Geometric
[OAME99, Sim91, JRM93, JM96a, Mra95].
Geometrien [Wal98]. Geometries
[LS90, FS94, Jun96, Wal98]. Geometry
[Ben99, DFGH99, Tou96].
Geometry-Based [Ben99]. George
[Pin98, WG97]. Georgia [ACM99b].
Gerdes [CFK+91]. German
[Wei99, Cra92, Dav98a, FT95, Ger97, Hor99,
Jar97, Kah91a, KK97, Kip97, Kru98, Kuf98,
Wal98].
Germany [BFS92a, BFS92b, Fum97,
IEE97d, LM98a, Wal98, Rat96].
Geschichten [CWM+91]. Get
[Ano96j, Cae96b, DDJ98a, Sch98c, Ude98].
Geting [WG97]. Gets
[Gar98b, GO96c, Los97, Sch98c]. Getting
[Kwa93, Way95]. GF
[PSR97, DBVD96, LD99]. G1
[BGH95b, LM98a]. GI-Fachtagung
[BGH95b]. Gibbs [DP99]. Gilles [Bue91b].
Girault [SN98b]. Girl [Got99]. Girls
[Ros99]. Give [GB98]. Given
[BM92, BDF98, Ev9H1, Ev92]. gives
[Ano93k]. Giving
[Int91a, GQW+91, JLM+94]. Global
[JV98b, Or96, SS99b, TGK99, TL99,
Z995]. GMD [SBGK99]. Go [DDJ98d].
Goal [AMP94]. Goals [BP98e]. Goats
[SV95b]. Going [DDJ98c, Ano95k]. Gold
[SS93]. Goldreich [N99a, Ngu99b].
Goldreich-Goldwasser-Halevi
[Ngu99a, Ngu99b]. Goldwasser
Zhe90, vW94, AB96b, BSNP96a, BSNP96b, BD92, Dam90b, DK94, Gon95, HLMW93, HXMW94, HYLT99, JG95, KL95b, MZI98, PGV91, Pre94a, PrO95, RP95b, Roe95, SV95a, SRRL98, Sim98c, Tsu92b, Tsu92a, YL7c, DBGV93, Sch93g, EPR99b.

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, Sti91b, TZ94, BGV96, Bosxx, Gih90, PIBM90, Sahl94, Sch93g, Sta99b, ZPS93]. Hasn’t [Gar97a]. Hasty [Sch98i]. HAVAL [ZPS93]. Hawaii [???90]. head [Ano94h]. Header [Atk95a, KA98a, MR95b, Ros93]. Heads [GC97]. Health [GO96c, Mjo93]. Hearing [Uni98a, Uni98g, Uni98j, Uni98i, Uni97a, Uni98d, Uni96b, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k]. Heat [GC97].

Heats [Gar98b]. heaven [Gol97c]. Heimdal [DW98]. Held [Ano96k, BF99a, Far93, Uni98f]. Hellas [IEE97c]. Hellman [RSA93b, BY93c, BY93b, BRR99, BWM99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY99b, HY98a, Kail97a, Koc95, Koc96b, Mau94, MW96c, MW96b, MW99, NS97c, NS97b, Van95a, VW96, WM93, vW96]. Help [GRBR99, PAK+98, AK95]. Help-Desk [GRB99]. Henry [CFK+91]. Her [Ber96a]. Herd [Rit99]. Here [MK94]. Heterogeneous [DVPL92]. Heuristic [MCD98b, CKM99]. Heuristics [SBZ99, CD98a]. HF [RP94]. HFE [KS99b]. HFX [LR96]. HGF [Un94b]. HGF-94 [Un94b]. Hidden [BL95, CJD97, KP96, KS95, NS99b, Pat96, Sak96, PSB97, Ti99]. Hide [SV99a, SV99b, SvS98]. Hidell [Scu92]. Hiding [Aue98, BGLM96, BLMO95, CM97b, CD97, CDS94, GRS96, GLB96, HS96a, MS99a, MO99, Phi96a, Phi98, RGV97, SC96b, SZT96a, And96c, Beu94, Bra90d]. Hierarchically [LE99]. Hierarchical [FL96, OOK91, CMCPS97, GPCPSN96]. Hierarchies [Ruo94]. Hierarchy [Hwa97, YY99b]. hieroglyphs [Wri98]. High [ACM98a, ARV99a, ARV99b, Ano99c, Ano99e, BCR98, Bla96a, Bla96b, BMS99, Chi99a, Ch99b, DP98a, DP98b, Ebe93, FVEA99, FP99, Gar97a, Gar98b, GN95c, HR90, IEE94e, IEE96d, IMI93a, IMI93b, Kap98, Koc94, Kor93, KB92, LS97, MPPS95, MSP99, Rus90, SKN98a, SKN98b, She92d, She95b, Sut99, VNW94, Du98, Graxx, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Uni96a, Yeu97]. High-Assurance [IEE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Ch99a, Ch99b]. High-Frequency [MSP99]. High-level [Rus90]. High-Performance [ACM98a, BMS99, GN95c, IEE94e, Sut99, NO96]. high-quality [Yeu97]. High-Radix [Kor93]. High-Speed [ARV99a, ARV99b, Ano99c, DP98a, DP98b, Ebe93, IMI93b, Koc94, MPPS95, SKN98a, SKN98b, IMI93a, Nor95a]. Higher [Jark99a, KMKH99, Lea99, MSK98, SMK98a]. Higher-order [Jark99a]. Highly [MS99b, PV97, ARK99]. Highway [Ano94c]. Hill [MCD99]. Hints [JMK99]. Hiroshima [IEE96b]. Histogram [Mae98]. Histograms [BMS99]. historic [Bur98a]. Historical [Kob97]. History [Cal92, CFK+91, DGT96, DKK+98, Ers99, Hig97a, Kah96a, Sim96a, Ano97t, Dav98c, Joh99, Kip99a, Mac98, Ros97a, Sim98a, Wei93, CFK+91]. HKM [LR96]. HKM/HFX [LR96]. HMAC [BCK96a, BCK96c, BKC97, MG98a, MG98b, OG97, Sta99b]. HMAC-MD5 [BKC96, OG97]. HMAC-MD5-96 [MG98a]. HMAC-SHA-1-96 [MG98b]. Hoffman [Hat96, Wai95]. HOL [ACD94, Bra95a, Bra96]. Holder [OMI93].
Imagery [WD97].

IEE97g, IEE97d, IEE97j, IEE97k, IEE98c, IEE98d, IRM93, IZ98, IZ99, KG96, KM96a, Knu99c, KP99b, Lox98, Mad92, Mar97, Mau96b, MDS90, MKS99, MDP94, Nyb98, OiDP98, PSN95b, QG95, Sti93b, Sti94, TM99, Ved98b, Wat91, Yua92, And96c, Chr98, Cop95b, DC96, Des94b, Ele99, FR95a, HOQ97, Kau97c, Kob96, LM98a, Lom97, Pre95a, SP90, Sta97c, Ste99b, TV94, Vau98c, Wad98, Wei99, vWN99, [Int91a, Moc97, Sce97]. Internet [Cha99a, SS99d, Ano97z, Ano98b, Atk97, Bel98, B096a, B+96a, Bet95b, Bet95a, Bhi96, BDC+95, FFW99, FT99b, Fum98b, Gar97a, Gar97b, Gar97c, GC97, Gar96b, GO96c, HA94a, HPS99, HC95b, II96, Ken93, Lin88a, Lin98a, Lin93a, Los97, McC96, Mit92a, Opp97, Pau99, Rit99, Ros97c, Sar97, Sch99a, Sme97, Smi97b, SL99, TAP90, VJ98, WM96, Way98, Wri98, Zim98, dVdVI98, Sha99a].


MSN98, MSN99, MTVZ92, MAO96, MM98a, MM98b, NMR95, NS97a, Nec96, Neu97, NS99a, Oka94, OU97a, Oka98a, Oka98b, Omu90, vO91a, PSCR97, Pa99d, PKOT94, Pat95, Pin97, Poi99, PB99a, RSA93e, RSA94, ROT94, RS98c, RS98d, Ross96a, Ross96c, Ross97b, Ross98b, Ross98c, RCM99, SSN98a, SYMI98, Sam98, DP91, Sas99a, Sch94b, Skw98a]. Key
[SKWW95, SOOS95, SM95a, SE96, Sha99b, She94d, SiK93, SR96, Sta99b, ST91, SW99a, SH94, Sun98a, Sut99, TAP90, Uni98a, Van99a, Van93, VSH97, VvT97, VvD99, VM93, dWQ91b, WLEB96, WW98b, WKS+99, Wic96, We97, We98a, We98b, Woh98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vO96W, AA95, Acc97, Lip98, AD97, AD99, Al 96, Ano90, Ano96m, BSNP96a, BSNP96b, Bao94, BIo94, BD98, BD98a, BTD98, BSB97, BR96b, BCK97, BY93c, BY93b, BS91a, BFS99a, BG9+95a, BMP97a, BF96, Bie96, BMS96, BFS98, BM95, Boy97, Bur94a, BD95b, C990a, CW97, Cle96, Cral97, Cus95, DKr97b, DWZ96, DS90a, DH96a, Des95, DvQ96, Dhe98, DyW92, DN95b, ES97, FDB93b, FMY97a, Fre94, Fro96, FGL96a, FGL96b, FL93, Gar96b, GH96, Gib95, GBL94]. key
[GH99, GTS90, HNS91, HP99a, HP99b, HY93b, Haw98a, He92, HW96, HI9+97, HI97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93a, IZ98, IZ99, JLM94, Jon90, JY98, KASH90, KM99a, KSW97a, KSW97b, KL94, KR96b, Kir95, Koo97, KM99d, Kos99, Kums97, LG97, Lma91, Lon91, Lon92, Low95, MS98a, Mao97, MLA91, Man91b, MY93b, MB99a, Mu92, MLLG95, NM96a, NY90, Nat97a, Nee91, Odd94b, Oct95, PS98e, PS98f, Pet91, PP92b, RT93, Roe99, Sai90, Sai96, SW95a, Sch92c, Sha95a, Sha96a, Sh92c, SK97, SY96b, SM90, Sm93b, SS95b, SS95c, STW95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC99b, TC99b, Ts90, TC91, Tze99, TH99, Uni97c, Uni95a, V996, Ven92, Van92b, Wie94]. Key
knapsack-based [He92]. Knapsacks [CJS91, Ort95b, Ort95a]. Know [DDJ98b, Fly97, Hi97, Kir95, Mil95].
knowing [DDJ98b, Fly97, Hi97, Kir95, Mil95].

Knowledge [Bie96]. Knowledge-Based [Bie96]. Knowledge-Level [BMT98].
known [Ano91b, BK95a, MY93a, vOW91].
known-plaintext [vOW91]. KnowRight [BS95e].
Knowledge-Based [Bie96]. Knowledge-Level [BMT98].
Knoxville [IEE94e]. Knuth [CFK+91].
KoMoD [SY99]. Komputer [Ano97-29].
Konstanz [Fum97]. Korea [Ano93g, KM96a, Rho93].
Korea-Japan [Ano93g]. Korean [LL98].
Korteweg [GK95b]. Kruh [CFK+91, Ers98]. Krypto [FK93a]. Kryptographie [KK97].
KryptoKnight [BGH+95a, MTVZ92].
Kryptosysteme [Hor99]. KtSeqC [BG99].
Kudos [Sva+98]. Kunstliche [CWM+91].
kuo [XtTmW94]. Kuperee [DH96b, HS94, HS96b]. Kurz [Ger97].
Kyongju [KM96a]. Kyoto [Ano99c].

L [Lip98]. Labeling [BKZ98, KZ95, LvdLB96, LvdLL97]. Labels [ZK95].
Laboratories [Ano95d, Ano95e, Ano95j, Ano95m].
LABYRINTH [LS97]. Lac [CFG96].
Ladder [Bih97a]. Ladder-DES [Bih97a].
Lai [LLG10]. Lake [IEE96d, USE95b].
Lambda [HRV99, GLV99].
lambdaProlog [NM99]. Lancaster [WSFC99].
Lance [Hat96, Wai95]. Lane [DDJ98e, DDJ98f]. Language [APDS93, AKP99, IOS94, KI99, PW99].
II94, LS98a, PS93a, Sak97, vWN99]. LANs [She92f].
LANSCAPE [Ril96, Ano94g, Ano94f]. LapCAD [Ano93k].
Laptop [GPR98]. Large [Bla93, BDHG99a, BDHG99b, CS97a, LO91b].
LM95, NNEK97, PF94, Riv97a, SA95, SS90, She92a, Csi95, DT93, DL95, Fra90, FOO93, Has99, MSDS90, Yan95, Yua92]. Larger [PW97b]. Laser [Ano93h, JC93].
Last [dBB91, dB91]. Late [Bur99]. latencies [JG90].
Later [Sch95a, Gol97c, Roe95].

Latin [BSNP97, Son99]. Lattice [Ano97-29, BK95a, MY93a, vOW91].
Layout [BKZ98, KZ95, LvdLB96, LvdLL97].
Labels [ZK95].
Languages [ACD94, BD91, GMW91, PM99a, PD99b, SAS99b, ACM99a, Ata94, DDP94b, GA98].
II94, LS98a, PS93a, Sak97, vWN99]. LANs [She92f].
LANSCAPE [Ril96, Ano94g, Ano94f]. LapCAD [Ano93k].
Laptop [GPR98]. Large [Bla93, BDHG99a, BDHG99b, CS97a, LO91b].
LM95, NNEK97, PF94, Riv97a, SA95, SS90, She92a, Csi95, DT93, DL95, Fra90, FOO93, Has99, MSDS90, Yan95, Yua92]. Larger [PW97b]. Laser [Ano93h, JC93].
Last [dBB91, dB91]. Late [Bur99]. latencies [JG90].
Later [Sch95a, Gol97c, Roe95].

Legal [CYY98, HA96, Mos98, Rad97, Ros95b, Wri94, Ame95, Ame96a, Sch93c].
Length-3 [YY98a]. length-restricted


Leuven [PGV93d, Pre95a, PR98]. Level [BMT98, HVH98, MB99a, VNW94, AG95, Cla99, DF92, HWF96, Rus90]. Levels [Bor96, GTGW94, dVdVI98]. LFSR [Kra94b]. LFSR-Based [Kra94b]. Li [JW01, vT93]. Li-Wang [vT93]. li.vi.5 [CFK+91]. liberty [Ele99, Wad98].


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, DVQ96, VBD99]. Limiting [KI96]. Limits [And96b, AP98, EKK99, Swi97, BH98, SOC98]. Line [Bra95b, Cac95a, Cac95b, CDF95, DT98a, EII99, EGM90, EGM96, LMBO95, PUF99, SS99e, SS99f, Tra99, DL98, Gau97, Mao98, Nal97, VNM99]. Line/Off [EGM90, EGM96]. Linear [Ano95a, AMP99, BGS96, BK94a, BL95, BPV99, CFYS96, Dae95, DD99, Des98a, vD95a, DLR97, Gol95b, HO96, Haw98b, KR94b, KR95a, KTM+99, KR99b, L091b, LH94, MS94, Mat93, Mat94b, Mat96a, Nyb95, OA94, Ros98a, SZ96, SF97, Sch96c, Sch99l, Sel98a, SK98c, SK98b, TN97, TSM95, YMW99, ZYR91, Ala93a, AW95, BS95, Bao94, BI93, Bih95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, HKM95, Haw98a, Jak98, KY95b, KYYx, KR96c, Kuk99, Lai95, LLB98, Lan95, MM90a, MAO96, MK92, OG95, SKD94, Tze99, YT95a, YT95b, ZYR90, ZH90, vD95b, vT94, Duh90].

Linear-Time [KR99b]. linearity [SB95].


Links [Blo99, CV95, DDNM98, GL98]. L'inuktitut [Ano99g]. Linux [Cor98, DDJ98a, Eri97b, Mor97]. Lion [AB96a]. Lippman [vdWS97, vS97]. LISA [USE99b]. LISA'96 [USE96a]. list [LC97b, Un97d]. Lists [FGR92, Riv98b].

little [Ano91b]. little-known [Ano91b]. Lives [DDJ98d].

LO [FY95a]. LLL [Mis97]. Local [Fum93, IEE97l, IEE98f, MM95].

Localization [PJ99]. Locating [PK93].

Location [FJP96, Jac96, KFJP96, KRJ98, WHFG92, FT95]. locking [CS96b, CS97b].

Locate [Way95, CC95]. Locomotive [Var99b].

Loen [WL96]. Lofthus [Hel94].

Log [Bal99, GJKR99, Gor93a, PS98b, WD98, YY97b, Kob90, SS95a, SK97d].

logarithm [CP95, CS97d, FR94, FM99, HY93b, HI97, HMP95, McC90a, MVZ98, NR95].

Logarithms [BBT94, CH98, GM93b, LO91a, Mau94, MW99, vO91a, Scho97, Tes98, vO91b, vW94, Gor93b, HZ93, Odl94a, SS95b, SS95c, vO92].

LOGCFL [LMSV99]. Logging [Zol93].

Logic [AHMS99, BRS99, BAN90, CIBM99, CO98, DRR95, Gue98b, SG95, SM95a, SHK99b, CS99, Pos98]. Logical [PS99f, Wad93].

Logics [ADD99, GAGCDAFC99, KW99, Len99b, WK96, Bad99, ZZZ97].

Login [ARH95, DQ93, Hil97].

Logout [Poo95].
Logs [SK98a, SK99]. **LOKI** [BS91f, BKPS93, Knu92, Knu93c, Knu95, TSM95].

**LOKI91** [Knu93d, Knu93a, SF97]. **LOKI97** [BP598, RK98a, Ri99]. **London** [Ano93d, Ano97p]. **Lone** [Ano97r]. **LONE-TAR** [Ano97r]. **Long** [CHN97, Len96, RH93, SSS98, Pos93].

**Long-term** [CHN97, Len96, RH93, SSS98, Pos93]. **Longevity** [Rot95b].

**Look** [Coh96, Has99, Pfl95, Zha97, GTGW94, Way91]. **Look-up** [Has99]. **Looks** [Sch97b, vdWS97, vS97].

**Loops** [SvA +98, SHK99b]. **Lorenz** [Car97b, Dav98d]. **Lose** [GPR98, Way96b]. **Loses** [Law98]. **Loss** [PW97c]. **Lossy** [CI96]. **Lottery** [Riv97a]. **Lotto** [QD91]. **Lotus** [Dwo95]. **Louis** [Ers99]. **Louisiana** [ACM91, ACM97b, USE95a]. **Louvain** [Ano99c, T +99].

**Louvain-La-Neuve** [Ano99c, T +99]. **Low** [Aga92, Ano99c, Bla96a, Bla96b, CFPR96b, CFPR96a, CNS99b, DDQM98, DDP99, DDGM97, DFK993, GDD +97, Goo96, Jak98, KSHW97, KSHW98, KK99, KOT95a, KOT95b, Mil96a, Pia99b, PK95a, PK95b, Pen96, SKNO98a, SKNO98b, T +99, Ano90, CJL +92, DV996, Gol96a, MHW98].

**Low-Bandwidth** [Bla96a, Bla96b]. **Low-Cost** [KK99, Pia99b, DV996].

**low-density** [CJL +92]. **Low-Entropy** [KSHW97, KSHW98]. **Low-Exponent** [CFPR96b, CNS99b, CFPR96a].

**Low-Power** [Ano99c, T +99].

**Low-Randomness** [DDP99]. **Low-Weight** [PK95a, PK95b, Pen96].

**Lower** [BD97, CTT94, OK95, Sch99, Sga91b, St93a, vHPP93, GN95a, K996, KO97, Sph99]. **LR** [BP98c]. **LSI** [SKNO98a, SKNO98b]. **Lu** [LZ91b]. **Lu-Lee** [LZ91b].

**Luby** [BKR98a, BKR98b, Luc96a, Luc96b, PRS99]. **Luby-Rackoff** [BKR98a, BKR98b, Luc96a, Luc96b, PRS99].

**LU** [Smi93b]. **Lucas** [BB95, JQ97, LTT95, SS95b, SS95c, XLP99]. **Lucas-based** [BBL95]. **Lucent** [MB99a]. **Lucifer** [BB94, BS91f]. **lun** [XtTmW94]. **Lunch** [DDJ98e, DDJ98f]. **Lured** [Che92]. **Lurking** [Joh96]. **lustre** [Alv98a].

**LVQ** [LSVV95]. **Lynden** [Ano93d, Ano97p]. **London** [Ano97r].

**MAC** [IEE97c, WG97, Mau91b]. **M.A.P.** [BBC98]. **MACs** [Ano99a, AB99a, AB99b, BGR95, JV98a, NR98, PV98].

**Made** [GSV99, Kra94a, G976, KKL99].

**Maestro** [CFK +91]. **MAGENTA** [Bii99a, Hub98, BBF +98]. **Magic** [BD99a, JM99, AGL95, Kah98c, RK98b].

**MagiCol** [GLSM99].

**Mail** [Ano93d, DN93, Got99, Ken93, Lin93a, RS98b, Sch95c, Sch95d, Sh97, VJ98, Ano95c, Gar97b, LF97, Lin98a, Lin98b, Mit92a, Ri996, She96a, Str93a, Str93b, Bac95, Zeg93, Sta94a].

**MailSafe** [RSA94].

**Mainframes** [Deu97, Deu98].

**Mainstream** [Gar97b].

**Maintain** [Wed99].

**Maintaining** [CH94a, CHH97, Gar94].

**Majority** [Un194b]. **MAJORITY** [FUW99]. **Majority** [Ber96a].

**Majorities** [Cha90]. **Majority** [Mv93].

**Make** [Ano93c, GGM97, CM99d].

**Making** [Ame96b].

**Making** [ASW99, CKN99, DDJ98e, DDJ98f, Des90b, Hl93, Lut98, PRS99, Sar97, Tra97, VM96, Way98, BKR98a, BKR98b, Wri98, Zaj97].

**Malaysia** [G96c, WSF99].

**Malicious** [PM98].

**Malleable** [DDN91a, BS99b, BS99c, DDN91b, Sah99].
Malo [GQ95, QG95]. Man [CFK+91, Mon96, IPNdbbprm91].
Mechanisms
[HL99, Mye94a, CGM96, HC95a, ZH93].
Mechanization [BoI97].
Mechanized [SM95a].
Medals [SM95a].
Mediated [FJ98].
Mediation [Kem99].
Medical [Cha99b].
Meet [FY99, Van95b].
meeting [Shp99a, Zim96b].
Mellen [Ers99].
Members [Par98c].
Membership [FGR92, Fis98, OOK91, SPH99, AK95, MW94, Sak97].
Memoir [Bar05].
memoirs [RK98b, Sel94].
Memorial [IEE98b].
Memory [ARV99a, ARV99b, CM97a, DHMR96, Fis97, Got99, KS99a, Le99b, MS91, Sha95a, Gut96, Has99, Ven90].
Memory-Bounded [CM97a].
Menezes [Sha99a, Kie98].
Mental [CF99, Jun99, KOT91].
Merged [GG97].
Merging [DV99].
Merkle [NS97c, NS97b].
mesh [PHF99].
Message [AGS97, AB99a, AB99b, Int91a, AS96, Bax97, BG90, BCK96d, BCK96e, BCKxx, Ber97c, Bie98, BHK+99, CDFT98, EPR99b, EPR99a, FH94, GLZ99, GT94, GQW+91, HK97, Kal91, KR95b, Kal98f, Kal98d, KI97, Kra95, KBC96, KBC97, LK99, Lin88a, Lin93a, Miy95, OM94, Pre98a, RSA93d, Rv92a, Rv92b, Rog95, Sho96, Tsu92b, Tsu92a, WSK97a, WSK97b, BSNP97, BGR95, BQ97, CLHL98, Cli99, HMP95, HCY96b, LC97a, Lin89a, Rv90a, Rv91b, Sta99a, Tze99, Yeu99].
Message-Digest [GT94, Rv92a, Rv92b].
Message-Efficient [FH94].
Message-Resend [Ber97c].
Messages [CFPR96b, vD97, SS99c, SKAM99, CFPR96a, Joh97b, Kip97, Mit92a, Par98b, Sch95d, War93b, Wri98].
Messaging [DD98c, AC97, DMW94].
Meta [EKLM99, FB97, HMP95, PS99f].
meta-blind [HMP95].
Meta-Logical [PS99f].
Meta-message [HMP95].
Meta-Object [EKLM99].
Meta-Protocols [FBS97].
MetaML [METAS99].
Metaphor [BP95a, Fue99].
Metaphors [BHJ99].
Metaproof [DY91a, DY91c].
Meteor [Sch93a, UN94].
Metering [SK96b, SK96e, Ros94].
Method [AG98a, AG98b, ADD99, BP98f, ESS99, GDD+97, HRVV99, KI97, KT93, LL94a, Mat94b, McM96, MS95f, Mi93c, SF97, SKBxx, Tes98, VNW94, CP94, CM97c, GTS90, JT96, JT97b, Joh98, KM98b, KAK96, KH97, LC98, Mat93, MY93a, McK99, Pit96a, RT93, SH99, Sn98, Vla95, YEA+98, ZH90].
méthodes [Bec90].
Methodology [CH99b, DD95, FM98a, NMR95, PN99, SSW98].
Methods [Bas93, Bir99, CL98, DB99, GSY99, IMI93b, KRS97, LdL97, LM98b, MCD99, Per99, SW94a, AhdJF97, Ale92, At94, Bau97, BGR95, Car97c, HLC99, IM93a, vdL98, QN98b, RT93, Rh95, Shp99b, TG94, Wh93, X98, Vn98].
Metric [Joc98, RS99b].
Metrics [LA98].
Metropolis [DP99].
Mexico [IEE91].
Meyer [Lu98a, Lu98b, JQ98b].
Meyer-Müller [JQ98b].
Mi [XtTm94].
Miami [IEE97f].
Mic [Zhe95a].
Micro [An97q, HSW96, Pri94].
Micro-payments [HS96].
Microcomputer [HNM98].
Microcontroller [Kuh98].
Microcontrollers [KK99].
MicroMint [RS96b, RS96c].
Micropayment [JQ97, RS96c, RS96b].
Micropayments [Rv97a].
Microprocessor [DD98d, Mar96].
microprocessors [NM96b].
Microsoft [Boy98, Fly97, Gar98a, SM98a, Ts’97].
Middle [BBS99b].
Middleware [CC09].
Might [DD98c, DD98f].
Military [An96n, Fri92a, Fri92b, LU95].
Millilcuent [Man95].
Million [Ran91, Riv91a].
Millions [Wal99b].
MIMD [DHW95a, HW95b].
MIMD-factorisation [DHW95a, HW95b].
MIME [An95c, An95n, An96k, Elk96, GMCF95].
Minefield [Han94]. Mini [Jak99b].
Mini-Cash [Jak99b]. Minimal [BDR†96, GM90]. Minimalistic [Jak99b].
minimally [CGM97b]. Minimax [All98].
Minimization [LE99, SBG99]. Minimizing [BR97b, SSN98a]. Minimum
[Ano95m, Ano97b, DK96, FO99a, CC98].
minimum-weight [CC98]. Mining [DC98c]. Minneapolis [IEE97l].
Minnesota [IEE97l]. Minorities [Cha90]. Minsky [GTGW94]. MIPS [Sil99].
Miss [BBS99b]. Missed [LKD98]. Mistrust [Bla93]. Mistrusting [CGM97a, Mar97].
MISTY [Mat97]. MITRE [Gol97a]. Mix [Abe98a, FJ98, SK95]. Mix-Mediated
[FJ98]. Mix-net [Abe98a]. Mix-servers [Abe98a]. Mix-Type [SK95]. Mixed
[HK97]. MnNet [IEE98e]. MMPC [SS99c]. Mobile [AGY95b, BGS98, COZ99, FGS96,
FJP96, Gar94, Got99, HP98b, KFJP96, KRJ98, LCN99, PKOT94, PW99, Pit96b,
She94a, Ved93, Vig98, YY97c, AGY95a, FC94, GA98, Hwa93, OY91].
Mobilfunkteilnehmern [FT95]. Mobility [SL99]. Mod [KSW99b, KSW99c]. Modal
[ADD99, BBDF97, Mas99a]. Mode [BK98a, BK98b, MT95, BP99c, CJM96,
PNBR94, PA98a]. Model [AR99, BMT98, BPBF99, Bole98a, Bol98b,
Cac98, DGV92, DDGM97, FCH99, Gon98, HS96a, Jia99, KW99, NT99, Oh99, PV98,
PMP99, VC99, WF94, ZTR99, Dan97, Gil97, ZK98, vW97, vS97]. Model-Based
[Jia99]. Model-Checking [Bol98a, Bol98b]. Modeling [DD99, KM98a, LM96, SS99a,
ZF98, ZFKP98, ZFK+98, Ano96d, CM97d].
Modelling [CK95, GACDFAFC99, HL92,
LKD98, NT93, PS99a, SM99, Tro93]. Models [Ben99, CH99b, DL99, DP99,
Ger99a, HHID99, LL97a, OMA98, PZ98, SY99, SZT98a, TGK99, CT99b, Nis91,
OMA97, SZT98b]. Modems [Gar97b]. Modern [Buc91b, Gol97a, Gol97b, Gol99a,
VG99, Dan99b, Unixxa]. moderne [Bra93b]. Modes [Ano96c, Bi99b, Bik96, Bik98a, Bik99b,
CV99, HP99a, HP99b, HRRV99, MT95, NA95, SHK99b, WAG98b, Bik95a, Nas94].
Modification [AKF94, FG98, Sel98b].
Modifications [NMR95, OMA98, Mol98]. Modified [BDGI98, NK98a, PBG90,
Wic90, CLW98, HW93, L91b]. Modular [BP99b, CJS91, Cop95c, HCY96a, Kor93,
MNSV97, Pai99b, PRAM98, SKBxx, TY92, TN96a, TN96b, VDDR99, Yam98b,
BG98b, BCK98, CK93, HN94, ISO97, KAK96, LC98, Lam98a].
Modification [BI99, She94e, SC96b, KSB96b, KSB97, SVWMB95, SOB98, VSB95]. Module
[Mee98]. Modules [Ano97r, IH98, Mor97, Com94c].
Moduli [MV91, Len98]. Modal [ADD99, BBDF97, Mas99a]. Mode [BK98a, BK98b, MT95,
BP99c, CJM96, PNBR94, PA98a]. Model [AR99, BMT98, BPBF99, Bole98a, Bol98b,
Cac98, DGV92, DDGM97, FCH99, Gon98, HS96a, Jia99, KW99, NT99, Oh99, PV98,
PMP99, VC99, WF94, ZTR99, Dan97, Gil97, ZK98, vW97, vS97]. Model-Based
[Jia99]. Model-Checking [Bol98a, Bol98b]. Modeling [DD99, KM98a, LM96, SS99a,
ZF98, ZFKP98, ZFK+98, Ano96d, CM97d].
Modelling [CK95, GACDFAFC99, HL92,
LKD98, NT93, PS99a, SM99, Tro93]. Models [Ben99, CH99b, DL99, DP99,
Ger99a, HHID99, LL97a, OMA98, PZ98, SY99, SZT98a, TGK99, CT99b, Nis91,
OMA97, SZT98b]. Modems [Gar97b]. Modern [Buc91b, Gol97a, Gol97b, Gol99a,
VG99, Dan99b, Unixxa]. moderne [Bra93b]. Modes [Ano96c, Bi99b, Bik96, Bik98a, Bik99b,
CV99, HP99a, HP99b, HRRV99, MT95, NA95, SHK99b, WAG98b, Bik95a, Nas94].
Modification [AKF94, FG98, Sel98b].
Modifications [NMR95, OMA98, Mol98]. Modified [BDGI98, NK98a, PBG90,
Wic90, CLW98, HW93, L91b]. Modular [BP99b, CJS91, Cop95c, HCY96a, Kor93,
MNSV97, Pai99b, PRAM98, SKBxx, TY92, TN96a, TN96b, VDDR99, Yam98b,
BG98b, BCK98, CK93, HN94, ISO97, KAK96, LC98, Lam98a].
Modification [BI99, She94e, SC96b, KSB96b, KSB97, SVWMB95, SOB98, VSB95]. Module
[Mee98]. Modules [Ano97r, IH98, Mor97, Com94c].
Moduli [MV91, Len98]. Modal [ADD99, BBDF97, Mas99a]. Mode [BK98a, BK98b, MT95,
BP99c, CJM96, PNBR94, PA98a]. Model [AR99, BMT98, BPBF99, Bole98a, Bol98b,
Cac98, DGV92, DDGM97, FCH99, Gon98, HS96a, Jia99, KW99, NT99, Oh99, PV98,
PMP99, VC99, WF94, ZTR99, Dan97, Gil97, ZK98, vW97, vS97]. Model-Based
[Jia99]. Model-Checking [Bol98a, Bol98b]. Modeling [DD99, KM98a, LM96, SS99a,
ZF98, ZFKP98, ZFK+98, Ano96d, CM97d].
Modelling [CK95, GACDFAFC99, HL92,
LKD98, NT93, PS99a, SM99, Tro93]. Models [Ben99, CH99b, DL99, DP99,
Ger99a, HHID99, LL97a, OMA98, PZ98, SY99, SZT98a, TGK99, CT99b, Nis91,
OMA97, SZT98b]. Modems [Gar97b]. Modern [Buc91b, Gol97a, Gol97b, Gol99a,
VG99, Dan99b, Unixxa]. moderne [Bra93b]. Modes [Ano96c, Bi99b, Bik96, Bik98a, Bik99b,
CV99, HP99a, HP99b, HRRV99, MT95, NA95, SHK99b, WAG98b, Bik95a, Nas94].
Modification [AKF94, FG98, Sel98b].
HEG98, LT98, QN98a, QN98b, SB98.
MPEG-2 [DS97c, HG97e, HG97d].
MPEG-4 [HEG98]. MPEG-encoded [DS97b]. MPEG2 [CPO+98, CHO+98, DDNM98].


Numbers [Cha93, Ell98, Gut98b, Kra99, Mac94, MSN99, Pin97, ST91, GK95a, PGCSN96, Yan95]. Numerical [Cha93, Ell98, Gut98b, Kra99, Mac94, MSN99, Pin97, ST91, GK95a, PGCSN96, Yan95].

Nyberg [NMV98]. Nyberg-Rueppel [NMV98].


Oakland [IEE92c, EIE93b, IEE94d, IEE95b, IEE97i, USE96d, USE96b]. Oakley [CH97a].


Oakland [IEE92c, EIE93b, IEE94d, IEE95b, IEE97i, USE96d, USE96b]. Oakley [CH97a].


Obtained [EvH93]. Obtaining [CLHL98].

Occam [GN95b]. Ochronon [Sch95e].

October [Ano93d, Ano93g, Ano96a, Cha91, FM91, IEE93a, IEE94a, IEE96a, IEE96d, IEE97f, IEE97h, IEE97j, IEE98f, IEE99a, NIS92, Oh96, OiD98, TV94, USE93, USE96a, Ame95]. Odds [McC90b]. ODES [Ru94]. ODMG [Wat99]. OECD [Org98a].

Off [Bra95b, DDD98e, DDD98f, DDD98a, Gar98a, Ros96c, Tra99, AC95, Ano94h, Ano96a, Mao98, Riv98c, VNM99]. Off-Line [Bra95b, DDD98a, EGM90, EGM96, Tra99, Mao98, VNM99]. Offer [Mar96]. Offers [Gar97a, GC97]. Office [Fuc99, UU97a, Uni96c]. Official [Zim95a].

On-Line [Cac95a, Cac95b, CDFI95, Ell99, EGM90, EGM96, FUF99, SSS99e, SS99f, Na97]. On-Line/Off-Line [EGM90, EGM96]. One [BJY97, BHSV98b, BHSV98a, BD94, BHH99, BM94a, BM96a, BM96b, BM96c, BKK98, B97c, DVG93, DDP90, Fii95, G96, HILL99, HT99, HYLT99, Mer90a, MSN99, New98, Riv98c, Roe94, Rom90b, Sch91b, Sch95a, TOU94, Un97a, Un98c, Un98e, Un98b, Un98b, Un98c, Un98c, Un98c, Z90, Ano97d, BD95a, BK98f, CB96, DI99, Dob98, Hwa92a, IE92d, M94b, MZ98, Roe95, Sim98c, Ste95, Sze98, Tao94, Tsu92b, Tsu92a, Wer93a, Wer93b, ZPS93, MAM95].

One-Bit [MS99]. One-hot [CB96].

One-Key [G96, Tao94]. One-round [Wer93a, Wer93b]. One-step [Ano97d].

One-Time [BM96a, Fi95, BM96b, BM96c, MAM95].

One-Time-Password [New98]. One-Way [BJY97, BD94, BM94a, B98K, DGG93, DDP90, Roe94, Sch91b, TOU94, Z90, BHH99, HILL99, HYLT99, Rom90b, BK98f, DI99, Dob98, Hwa92a, IE92d, M94b, MZ98, Roe95, Sim98c, Sze98, Tsu92b, Tsu92a, ZPS93].

One-Wayness [HT99]. Onion [RSG98, SGR97].


Ontology [ADBB99, Gu99, Mee99].


55

Poker [KKOT91]. Policies [HK99b]. Policy [ACM94b, And96a, Ano96f, Bar93a, Bar93b, CPOR97, Ell99, Gir99, Hat96, Wai95, Aus96, Abr97, Ban94, Bro96, Dam96, DJ96, Ele99, HAH94, Hof95, LKB+94, Rot95a, Tas98, Wad98, Zaj97].

VCF+90, ZMI91, BFKL94, BP95b, Di99].

**principle** [Dam90b, Gib90]. **Principles** [ACM99a, AN95, HGHD98, KK99a, KG99, MG91, PR98b, Zhe90, Sta99a]. **Printer** [Cou93].

**Privacy** [Dam90b, Gib90]. **Principles** [ACM99a, AN95, HGHD98, KK99a, KG99, MG91, PR98b, Zhe90, Sta99a].

**Printer** [Cou93].

**Privacy** [Ano94h, Ano95c, Ano97s, Avo98, Bac95, BBCM95, Ble98b, Car96, Cha92b, DL98, Elk96, FJP96, FHM99, Gar96b, Gar95a, IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, Ken93, KFJP96, Lin88a, Lin89a, Lin93a, Lut98, MW97, Mjo93, NKP99, Par98c, SY96a, SYM98, SB97, SG96a, Sta94a, Tho96, Tra99, Uni98a, Uni98i, Ban94, Bro96, CM95, Car94, Cha92a, CK93, Cl999, Dom96, HM96, JMLW94, Mar95b, Mei96a, Mil95, Rot95a, Smi94a, Sta95b, Uni98d, Uni97c, VPM97, Zim96a, Zim96b, Gar96c, Ros97a, SS97a, SS97b, Sta94a, Sta95a, Zeg93].

**Privacy-Protecting** [Tra99].

**Private** [BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, Mv93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts90, Wil93b, ZG96].

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

**Privelege** [ECM96].

**PRO** [Ano97r, Gar98c]. **Proactive** [CHN97, FGMY97b, HJKY95, HH97x, IBMxx, Jar96, Rab98, BCR98, FGMY97a].

**Probabilistic** [Jak98, JO97, SF97, Sch91b, Tont93, Gol99a, GO95, HK90, Imp92, Lon91, TX92].

**probabilities** [Lew92]. **Probability** [BDG99, Gol96b, Kob99, TY94, AI96, MHHMW98, MAO96, WM93].

**Probable** [BD93, NK93, DLP93, Graxx].

**Problem** [Bon98b, Bon98a, BN96, CS96a, Cha90, DD99, DJL93, GO96c, HM98, KM99b, KR99b, MT99b, NS99b, OM99, Per99, RS99a, CPS95, HY93b, H97b, HM97b, HMP95, LC97b, Mas97, MC90a, NR95, OA99, MSO96].

**Problem-Solving** [Per99].

**Problems** [AA93, BD95a, Bra90a, GGH97b, KRS99, MC92, Poi99, Smi90, APDS93, Bea92, BFKL94, FR95a, HC95a, IEE97e, Lew92].

**Procedure** [Ada97a]. **Procedures** [Hig97b, Lin93a, Lee95, Lin89a, Lin89a].

**Proceeding** [BPR99]. **Proceedings** [ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, Ano95i, Ano98f, Br92, Bri93, Com96, GN95b, IEE95a, IEE91, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96d, IEE97i, IEE97j, IEE97k, IEE97i, IEE98e, MZ98, Nat99b, OW95, P959a, Pit95, St93b, SJ93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96e, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94d, Bih97c, B+96b, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fr99, Fum97, Gol90b, HOQ97, Hr97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, KG93, Knu99c, KP99b, KK99b, Kra98, LOX99, LM98a, LW96, Lom97].

**proceedings** [MV91, Nyb98, OdP98, Pre95a, QV90, QQ95, Q+98, Rue93, SZ93, Sp95, Ste99b, TM99, TV94, T+98, TV92, USE90, USE98d, VPM97, Vau98e, Wat91, Wie99, Wol93b, Yu92, vWN99, ACM93b, CH96, Clar99b, IEE94e, Sti94, Wol99a, BCB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fei91, Gol96d, GQ95, GS94b, He94, IRM93, Kal97b, Kob96, Mau96b, P959b, SP90].

**Process** [AMP94, Knu99a, Rob98a, RS99c, YT96, CWM+91].

**Processes** [Gar98b, Bea92].

**Processing** [Ano97h, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97d, IEE97j, IE97k, IND99, KV99, LMP99, LW96, Pin98, Pit95, Ano96m, DO99, DF97, Man98, Sab94, T+98, Whi90].

**Processor** [Gar98a, RB99, SW97a, SW97b, She92e, Sut99, VVD90, Von92a, Von92b, DVQ96, She92c].
Processor-efficient [Von92a, Von92b].
Processors [Cla97, KK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
Prodigy [CFK+91]. produced [SSI97a, SSI97b]. Product
[GO96c, KWSH98a, KWSH98b, KWSH98c, GN95a, SS98a, Ano94i]. Products [Ano97f, Ano97g, Cha94b, Cli97, Los97, UV97b].
Professor [Swi97].
Programmable
[DMVC99, SVB99, TT99, WB94].
Programme [BG93]. Programmer
[Bre99, DDJ98a, Jol95, Ste94b, vdWS97, vS97]. Programmers [Gar97c, Joh97d, Ste94b, vdWS97, vS97].
Programming
[IBM93, BGS96, CO98, Ste94a, JDM+91, Ste90a, Ste90b, ACM99a, Gre94, GA98, LS98a, OA99, Sab94, vWN99]. Programs
[BK95c, DRR95, SHK99b, WBC99, Zwi98, B+97, DFHR91]. Progress
[Ano96b, Ano97e, BDI+96, KS96b, Wol93b, Wol93a].
Programs
[BPBV99, IBMxx, GH96, Man98, DS90b, RCM99].
Programming
[IBM93, BGS96, CO98, Ste94a, JDM+91, Ste90a, Ste90b, ACM99a, Gre94, GA98, LS98a, OA99, Sab94, vWN99].
Programme
[BK95c, DRR95, SHK99b, WBC99, Zwi98, B+97, DFHR91].
Projects
[ABK98b, ABK98c, ABK98a, BAK98b, ABK98a, BAK98, DR98a, KR94a, LM91b, Cli99, LM91a, RHAL92, RRSY98, Ban94].
Proposals
[DAE99, VT97].
Programming
[BO96a, Ble98b, Des90a, EHMS99, GMDS98, KRJ98, Lut98, Mar95b, MW98b, PT95, SYMI98, Tra99, VP99].
Protection
[BGG95, CHN97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LCR98, LA99, LvdLB96, LvdLL97, LML98, Per97, Smi90, Uni97a, Uni98i, ZK95, ZK96, Ale98, BCBP97, BCBP98a, BOD95, CPO+98, CHO+98, CLI99, DFHR91, GO96a, Ibb97, OPH+99, RP94, RKDB96, SY96a, Sta94a, TV92, TSN93, Uni97c, YEA+98, FT95].
Programs
[ATAY98, Ano95a, BWM99b, BV98b, Bra95a, Bre94, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HLY93, IS91, JLa97a, JM9+98, JQ97, Kas96, KSW98a, KSW98b, KS98b, Kra99, Um94, Mau94, MW99, Mey96, Moo92, NS98b, NS98c, OM93, RS96a, RS98b, SSN98a, SH97, SM98a, SM95a, Sim96b, SM96b, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CTSSxx, Dib98b, EHF93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS98f, SK97, Sim94b, TH99, WS97, WLS94, ZHE95a, GM93a, Sar97].
Protocol
[AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BG9+91, BWM98, BWM99a, BCBM93b, BLE98a, BOL98a, Bol98b, BDL97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dan99a, DGT96, DQ93, DS97d, Fie93, Fei96, FBS97, Fum98b, GM93a, Geh95, GSH7, GMV98, Gue98b, HT98, HMK99a, HL92, Hwa92d, HCY96a, IEE98e, KKOT91, KY92, KS97c, LY93, LL97a, LHB96, LL95a, LS92, LM96, MB94a,
MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, SI93a, Sch94g, Sch96a, Sch94h, Sch99k, SSP90, Tou91, Tou93, AN94, AG97b, AG97c, AG97a, Aba99, ABC+98, BDI97, BH93, BCK98, BGH+95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, CJ95, Dan97, Fei99, Hor98, HLL+95, JW01, LY93, LHW99, LL95b, Lon97, Man95, Mas97, MILY93, Mau95, MW98c, NT93, PS98e, 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, Mol98].

Provably [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, LM95, Man91d, Oka93b, PS96c, Sho96, ZM90, BH93, Dam94a, FOG98, Gol90c, NY90, PS95]. Provably-Secure [DY90, DY91d, DY91b, Mau91d]. prove [Zha96].

proven [DS93, Lea90].

provers [JY96, Pe91a]. Provide [BDR+96, SA95]. Provider [Tre99].

provides [MHW98]. Providing [Bra90a, SKM99, Ano95c]. Proving [Bos90, DR94c, DE99, FKO98, DF91b].

provisions [Cli97, UU97b]. proxies [LC94].

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

PRPs [HWKS98a, HWKS98b]. Prudent [AN94]. Pruning [AF94]. Pseudo [BG98, BGM97a, BGM97b, Imp92, MS95f, NR98, PS98b, Bou94, TSY98].

pseudo-aléatoire [Bou94].

Pseudo-Random [BG98, BGM97a, BGM97b, MS95r, NR98, Bou94].

pseudonymous [GGK+99]. Pseudonyms [KRJ98, Mjo93]. Pseudorandom [ARV98a, ARV98b, BCK96a, BCK96c, BGK99, EM93, HILL99, KSWH98d, KSF99, Lag90, Mac94, Pat91a, Sui99, ZYWR91, BGR95, Kos99, Pat91b, Rev91].

Pseudorandomness [Kob99, Lub96, LLG10, Gol99a, MM95].


Public [ANS97, AN98b, Acc97, AKP96, AN95, IBM93, Ano96m, Ano99f, Ano99h, AA93, BP98a, BI95, BDH98, BDG98, BCE+94, Bec99, BC95b, BHS98b, BHS98a, BDP98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, Ble97, BF99c, BS94, CC99b, CG99, CJ95, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De93c, DP98c, Dif90, Ell99, FY95a, FY98a, FYM99, FGLP96a, FGLP96b, FO99a, GH90, Gal96, Gar96b, Gih91, Gib96, Gir91, GGH97b, GH99, HK99a, HGS98, HP98a, HLY93b, HM93, HL93b, HJJ+xx, Hes97, HPS98, HFPS99, IZ98, IZ99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Mau93a, Man97a, Men93, MM96b, Mic93a, Mic93b, MM98a, MM98b, NS97a, NY90, Nec91, Nec96, NS99a].

Public [Odh94b, Oka94, OU98a, Om90, vO91a, PS97, Pa99d, Pat95, Pin97, Po99, RSA94, RCM99, Rud91, Sa90, Sa96, DP91, Sas99a, SE96, She94d, Sim93b, ST91, Sun98a, Sut99, TAP90, VSH97, dWQ91b, Wie98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zim96b, dWQ91a, vO91b, AA95, AD97, AD99, Ano90, ADS98, Bae94, BI94, BD98a, BS97, BS91a, Beu94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cus95, DW92b, Dam96, Den90, DVO96, Dhe98, DN95b, ES97, FGMY97a, GH96, Gib95, He92, HWF96, HJJ+97, JM96a, Jar96, Jon90, KASH90, KM99a, Kir95, KM99d, Kos99, LG97, Las92, LMJ93. Lee95, LC96a, LM94a, LZ90, LZ91a, LD94, LCL95, Lon91, Lon92, Low95, Mf90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Ra99, Roe99, SW95a, Sch92c, Sha95a, She96a].
Public-Key

Public-key

Public-key-Based

Public-Randomness

Publication

Published

Publicly

Pudding

Puerto

Purchase

Purple

Purpose

purposes

pursuant

Push

Pushes

Putting

puzzle

PVM

Q

Q&A

Q-Deformed

QoS

QPSK

Qu

Qu-Deformed

Quadratic

Quateryn

Quaternion

Quebec

Queensland

Queensland

Queries

Query

Question

Questions

Quick

QUIPU

Quisquater

Quorum

r

R1040

Rabdology

Rabin

Rabin-Williams

race

Rhacooff

Radial

Radio

Radiology

radios

RADIUS

Radix

Ramified

ramp

Rams

Random

BG98, BGM97a, BGM97b, Bir98, Cor99, Ell98, FW91, Fis98, FO90, FJRS96, GHR99, Gut98b, Jh99, KKS97, Mat96b, MP91, MS95f, MFG95, NR98, OS98, PS98b, Ran01, ROT94, Riv91a, Sil97b, W99, BR97b,
Bou94, Gol99b, IS97, Imp92, Jenxx, Kos99, Kuč92, Ler97, PC98, TSY98, Wal90.

Random-Number [ROT94, Bou94].

Randomisation [KI97]. Randomized [Mau91d, PSN91, BI94]. Randomness [BM99c, DIF94, DDP99, GW96, HL93b, KR94c, Nis96, DP91, Sot98, SB99, BGS95].

Randomness-Rounds [KR94c].


RC5 [Ano97c, BR96a, BK98e, BPV99, GPO98a, GPO98b, KY95a, KY97, KY98, KY99a, MAO96, Riv95c, Riv95b, Riv95d, Se99a, Yin97]. RC5-CBC [BR96a]. RC5-CBC-Pad [BR96a]. RC5-CTS [BR96a]. RC5P [KSW99b, KSW99c]. RC6 [BPV99, Con99b, CRRY99, RRSY98].

rDSA [ANS98b]. Re [FL99b, Jak99c, AGY95a, Bur98b, HG97d]. re-encoding [HG97d]. Re-encryption [Jak99c]. Re-issuance [FL99b]. re-sharing [AGY95a]. Reachability [DR94c].

Reached [Lea99]. Reaches [MB99a].


Real-Quadratic [BBT94, BMT96].


Reasoner [MD99]. Reasoning [AG97a, BM95c, DSSB95, KM99a, MR95a, PK99, Var99b, Ger99b]. reasons [Ril96].

Reassessing [Neu95]. Reassure [MB99a].

Rebroadcast [Sal91]. Receipt [BT94, SK95]. Receipt-Free [SK95, BT94]. receive [Way91]. received [Cli97, UU97b].


Rechnergestützte [MPS94]. Recipes [FB97].Recipient [WP90, Wal90, WK97].

Recognition [HCD99, HA96, WD99b].

Recognizer [WB94]. Recognizes [Pin98]. Recommendations [Ano95m, Kal98g].

Reconciliation [BS94, CM95]. Reconfigurable [BP99b, PJB99]. Reconstruc [HD96a]. Reconstruction [BC95b, BD98b, LH95]. Record [Har90, LCL92, Cha99b, CDEH+96, IEE96f, IEE98b, JLM+94]. Record-Oriented [LCL92]. Recoverable [YY99b, YY98c].


redistributors [DF98]. REDOC [Nor95a, BS91b, CW91b, GN95c].

REDOC-II [BS91f]. Reduce [Hig97b, SVWMB95]. Reduced [BBS99a, BKR97, MT99a, BBS99a, PNRB94].

Reducing [DS98b, JQ98b]. Reduction [CTT94, GG97b, BK98g, PP92a, PP95b, PP95a, SH95b, SOB98]. Reductions
NP98b, Pad98, PHF99, Rab94, SC96a, SZT96a, SZT96b, SZTB98, TKS98, ZK95, BBCP98b, BD97, FGY96b. Robustness [AN95, MMST98, YMW99, Irw98].

Rockland [GS94b]. Role [Car97b, DDJ98d, JJ95, Lin96a, VC99, DL96, Dam96, Gu99, Mau93b, Sh98]. Role-based [JJ95].

Role [Car97b, DDJ98d, JJ95, Lin96a, VC99, 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].

Root [Kob97]. Rooted [PB99a]. Rooted-Tree [PB99a].

Roots [Kob97]. Rooted [PB99a]. Rooted-Tree [PB99a].

Roosevelt [Kah98c]. Root [Cop95c, JJ91].

Rooted [PB99a]. Rooted-Tree [PB99a].

Roots [Kob97]. Rooted [PB99a]. Rooted-Tree [PB99a].

Roosevelt [Kah98c]. Root [Cop95c, JJ91].

Rooted [PB99a]. Rooted-Tree [PB99a].

Roots [Kob97].

Rosemont [IEE97g].

Rosenheim [Sha99a]. Rosser [Ole95].

Rosenheim [Sha99a]. Rosser [Ole95].

Rotation [OP97, OP98]. Rotations [Con99b]. Rotor [Wic90, Dav96]. Rough [Mic93b]. Round [BJY97, BS93a, DP94, Dob97, GC94, KTM+99, Nat99c, SZ96, SK98c, SK98b, BD95a, NBD+99, Wer93a, Wer93b, HT98].


Routing [GRS96, RSG98, SGR97, CadH96]. Rover [Bis90]. Royal [Far93, Tv92, Don98]. RPC [SSH93]. RSA [An94b, An95f, AA99, And93, An95d, An95c, An95a, An95j, An95m, An96b, An97e, An97f, An97g, An97u, An97v, An97a, An97w, An98a, An99a, BTD98, BQ95b, BQ95a, BR95a, BR96c, BJ97, Ble98a, BF97b, BDF98, BV98c, BD99b, Bon99, Bra95e, Bri90b, BM94c, Ca99, CH97b, CH98, CB96, CLL99, CMT994, CD91, Cle96, Coc97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, Cus97, Dav95, Dem94, DDL94, DN95a, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FGMY97b, FMY98, FY98b, FR95b, GJKR96b, GKR97, GGO99, Gil99, GM97, GTS90, Gro94, GS99b, HN98, HWF96, Hor98, Hub91, HP94, IM93a, IM93b, JQ97, JQBD97, JQ98a, KR95c, Ka97a, Ka98b, KS98a, Kir95, Ko94, Ko96a, Koc95, Koc96b, Koy95, KOT95a, KOT95b, KK96].

RSA [Len98, LHL94, LL95a, Lom91, MFB99, MLY93, Mau90, MW98d, MW98c, MSS98, Mis97, Mis98, MS99c, Mue99, Miel99, NS98b, NS98c, Oka98a, Oka98b, OS91, 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, VVD90, VNM99, Ven92, Vv97, Wal98, Way90b, Wie90a, Wir98, XL99, YW99, Zer96b, Zhou94].

RSA-120 [DDL94]. RSA-130 [An96b]. RSA-Based [CD96, GKR97, VNM99]. RSA-cryptosystem [Gro94].

RSA-Implementation [PP90]. RSA-key [FMY98]. RSA-keys [SSI97a, SSI97b].

RSA-Like [JQ97]. RSA-Moduli [Mau90]. RSA-signatures [Ev92]. RSA-type [BJQ97, JQBD97, CLL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b].


Runtime-Tunable [WF94]. Russia [CW94].

S [WG97, An95n, An96k, BD95a, DT93, ECD+99, Kim93, Mat95, MC96, PG97a, PG97b, SK98c, SK98b, Sto90, Un97c, YS99, YY98d]. S-box [BD95a, SK98c, SK98b].

S-Boxes [Kim93, PG97a, PG97b, DT93, Mat95].

S-CODER [Sto90]. S-Hrg. [Un98]. S.I.S.
[Eph98]. **S.I.S./CB** [Eph98]. **S/390** [ECD+99, YS99]. **S/KEY** [MC96].

**S/MIME** [Ano95n, Ano96k]. **S012** [KP95]. **s02DES** [TSM95]. **S390** [Deu97, Deu98]. **SAC** [Kim93, KS97b, NS99a, TM99]. **SAC/PC** [KS97b]. **SAFE** [Uni97a, Uni98b, UU97a, Uni97b, Hor99, VM96, Way95, Uni98c, Uni98e, Uni96b, GA98].

**S012** [KP95]. **S390** [Deu97, Deu98].

**SAC** [Kim93, KS97b, NS99a, TM99]. **SAC/PC** [KS97b]. **SAFE** [Uni97a, Uni98b, UU97a, Uni97b, Hor99, VM96, Way95, Uni98c, Uni98e, Uni96b, GA98]. **Safe-Tcl** [GA98]. **safeguarding** [Beu94].

**Safer** [Hir93, BM97, CMKK98, KSW96, KSW99a, Kel99, Mas94, Mas99b, Van95]. **Safety** [Ano94c, DDJ99, Cli99, IEE94b]. **Safford** [Bur98b, Kru98]. **Saint** [GQ95, QG95]. **Saint-Malo** [GQ95, QG95]. **Sales** [Gar97a]. **Salesman** [OMV98]. **salient** [CKLS96b]. **Salt** [USE95b]. **Samba** [Bla98].

**same** [Ude98]. **Scalable** [Hei96b, IEE94e, ADF98, BCCG93, BM99a, BM99b, BF99c, Boy90, BY92, CT97, CK95, Cop94b, DQ94, DKKK98, DN94, GH1990, GQW+91, HL93a, Hwa93, Hwa97, Iev91, IM93b, KKS97, KS98d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MSS98, Mi996, Mun99, Miu99, NMV98, OOK91, OO93, OFF93, Pat95, Pet98, PM99b, RGV97, Sch99i, Smi90, Ver95, ZL99, AW95, BD98a, CW97, CLHL98, CC95, CLW98, CMTN94, CS97, FO093, FO98, GMLH94, GPSN97, Gua90, Har91, HZ93, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM+S94, Ku92, LWC96, LLG10, MR989, MS98a, MLA91, Mau91b, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SSN98b, SVWMB95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WWH95, v939].

**Schemes** [AW94, BP97a, BC93a, BDPR98, BBB96, BK94a, AK97b, BM96b, BM96c, BDGV93, BDD+94, BFS96, BM99c, BV96, BD90, Br90a, BS91g, BLV98, BBD92, CS97a, CM99a, CD95, Dan99a, DGV90, DMPW98, DY91e, vD95a, DFKY91, DL97, FDB93a, FY97, FO093, FO99b, GPSN98, GP99, GS94a, HKS97a, HKS97b, IS91, JOM94, KPG99, KI96, KMOV91, KOS+S94, KO095b, KOO95a, LH98W, LM95, MH96, MIS98, MWW94, OK98, Oka93b, Pai98a, Pai98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SI93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SSN99, YLD99, Zha98, ARK99, BC95a, BR97b, BI93, BDSV93, BCDV94, BG95, Blu95, BC96a, BCDV96, BDGV96, BMS96, BD97, BFS98, BDV98, BD98b, BD99, Bur96, BM94c, CG919, CP95, CSV94].

**Scheduling** [KP93, Por98, SJS98, Sha99b].

**Schema** [Pit96b]. **Schemas** [Wed99].

**Scheme** [Int91a, ADF98, BCCG93, BM99a, BM99b, BF99c, Boy90, BY92, CT97, CK95, Cop94b, DQ94, DKKK98, DN94, GH1990, GQW+91, HL93a, Hwa93, Hwa97, Iev91, IM93b, KKS97, KS98d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MSS98, Mi996, Mun99, Miu99, NMV98, OOK91, OO93, OFF93, Pat95, Pet98, PM99b, RGV97, Sch99i, Smi90, Ver95, ZL99, AW95, BD98a, CW97, CLHL98, CC95, CLW98, CMTN94, CS97, FO093, FO98, GMLH94, GPSN97, Gua90, Har91, HZ93, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM+S94, Ku92, LWC96, LLG10, MR989, MS98a, MLA91, Mau91b, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SSN98b, SVWMB95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WWH95, v939].

**Schemes** [AW94, BP97a, BC93a, BDPR98, BBB96, BK94a, AK97b, BM96b, BM96c, BDGV93, BDD+94, BFS96, BM99c, BV96, BD90, Br90a, BS91g, BLV98, BBD92, CS97a, CM99a, CD95, Dan99a, DGV90, DMPW98, DY91e, vD95a, DFKY91, DL97, FDB93a, FY97, FO093, FO99b, GPSN98, GP99, GS94a, HKS97a, HKS97b, IS91, JOM94, KPG99, KI96, KMOV91, KOS+S94, KO095b, KOO95a, LH98W, LM95, MH96, MIS98, MWW94, OK98, Oka93b, Pai98a, Pai98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SI93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SSN99, YLD99, Zha98, ARK99, BC95a, BR97b, BI93, BDSV93, BCDV94, BG95, Blu95, BC96a, BCDV96, BDGV96, BMS96, BD97, BFS98, BDV98, BD98b, BD99, Bur96, BM94c, CG919, CP95, CSV94].

**Scanners** [DP96, DF93, DDB95a, DDB95b, Des99b, FDB93b, HY93a, HMP95, HCY96b, JM93, Koy95, KO95a, KO96, KO97, LS98a, LC97a, LHL95b, LHL95a, MS98b, MPSV99, MTN97, Mu92, NR95, OK96a, OKT93,
OK95, Pad98, PS98a, PPKW97, Pf96c, PS96d, RD96a, RS96b, SI93b, Sha94, Sha95a, She92g, SW98, SW99a, SS94, SC97, TJ99, Tze99, VNM99, WAMO94, ZHS94, ZI98, dR94a, vD95b. Schernes [BBCM93a].

Schnorr [DBGV93, dR94b, dR94a]. Schnorr [IKNY98].

School [Duf98]. Schools [DDJ98e, DDJ98f].

Schroeder [Low95, Low96]. Schussel [Pin98].

Schütz [FT95]. Schwierigkeit [Hor99].

Science [Ano93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97f, IEE98a, IEE99a, Ste91, Bed90, Beu94, Sch90c, Sch97c, Shp99a, Sim90b, Sim91, Sim94a, Sti93a, Van93, W99, Wie90b, Wol98, Al96, AGY95a, BC95a, BT94, BI93, Ble96, BDSV93, BCDV94, BDD+94, BS95, BCDV94, BDV96].

secret [BD97, BDV98, BDG99, Bur96, CDGV91, Dal97, Dam94a, Dwo91, Elf97, FO93, FO98, GM95, GNS97, Gre90, HNSM91, Hel93, HK95b, Hwa92b, HSH6c, HLC99, JM93, JMO95a, Jan96, JY98, KO95a, KO96, KO97, LY93, LH95, Mei92, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, Ped91b, Ped91c, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, V97, Wie90a, WS96c, Win99, W99, ZHS94, vD95b, van97a].

Secret-Ballot [CSF96, BT94].

Secret-Key [An907e, Bra95b, Bra95c, LM94b, Van97a, Van93, Wol98, LM94a, JY98].

secret-sharing [RD96a]. secret-sleuthing [WS96c]. Secrecy [MIT94].

Secrets [C690, DH90, DSB99, Ele98, HY93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, An91b, Bau97, BDV93, CYW98, JMO95b, W93, Chi92]. Section [Alv98c].

Secure [AHV98, AB96a, An93c, An95i, An99c, An99h, Atk97, AR99, Bal99, BQ95b, BQ95a, BM99a, MM99b, BR95b, BM99a, BM99b, BR91, BHK+99, BDH93, BFS96, BS95b, BS98, BM94b, CG99, Car99, CG98, Cha90, CV91, CR91, CC95, CKLS96b, CKLS96a, CKLS96c,
CKLS97, CD95, CD96, CS98b, CDD +99, Cra99, Dam91b, Dam94b, DY90, DY91d, DY91b, DY91f, FIP93b, FB97, FYM99, FB94, FO99b, GMGM97, GHY90, Gal96, Geh95, GJKR99, GHR90, Gut96, IOS94, Jac90a, Jac90b, JT97a, JT97b, KHR95c, KM93, Kar96, KT96, KSHW97, KSHW98, KS99a, Km94a, KP97, Kon95, KBR97, KTY98, LY93, LM95, Mar98a, Man90, Man91d, Man97a, MW97, Mos98, NIS93b, Nat95, NS98b, NS98c, Oka93b, OU98a, Ped91d, PS96c, PB99a, PGV92, RRP97, RS96a, RSK95a, SSH93, SS95a]. Secure [SK94, SSSW98, Sas99a, Sch94a, SK98a, SK99, SM95a, SB94, SM94, Sho96, Smi93b, Str93a, Str93b, Tay95, WP90, WD99a, WK97, Web98, Yah94, YST99a, YST99b, ZM90, Zho90, ZL99, Zo93, vHH97, BH93, Bea93, Bea96, BMS96, BP95b, Bow93, BM95, BD95b, CNST95, CG97, CG05, Dam94a, Des90b, DS93, Des95, DQV96, FO98, GGK +99, GM95, Go90c, GBL94, HY98b, HY98a, HC95a, Hwa93, HW98c, IS97, IKN98, KC95, KSB96a, Lam99, Los97, MS98b, NY90, OK96b, Opp96, Ped91b, Ped91e, PSW95, Rho94, RRS98, Rom90b, Sar97, Sch92c, SK97, Sim98c, Sin95, Sta97c, Ven92, YL97b, AN97, An93a, Nat92b, Sta94b, Bov94]. secured [Way98]. Securely [RB94, DDFY94]. SecureNet [Ano97r]. Securing [Bhi96, Des95, Lin96a, RG95, SG98, V998, Ano95k, DL96]. sécurité [Bou94].
LHW99, Len93, LC95, MW94, Mar95b, MSN97, Mas97, Maur1c, MKKW99, MF97, Mei94, MW98c, Nor95b, PS99d, PS99a, PS99b, PS99c, PGEV93, PVC96, PR98.


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 [Chl97, UU97b]. Sequence [LY93, GM91, LY93, MHHMW98]. Sequences [DSV99, JQ97, MS94, Mun91a, Mun91b, PMP99, SB94, Bla94a, GN95a, Gol99c, KSB96a, MK92]. sequential [LHW99]. ser [IPNdbbprmr91]. Serial [SI93a, SS99, Yor96]. Series [Ano95d, HEQ98, CJR98a, CJR98b]. Series-Parallel [HEQ98]. Serpent [ABK98c, ABK98b, ABK98a, BAK98]. servant [CWM+91]. serve [Sch93c]. Server [Ano97r, Ano97s, BQ95b, BQ95a, DL99, ECD+99, HS94, HCY96a, Kon95, LY93, LL95a, MW98d, NS98b, NS98c, Oh99, SVA+98, Wat99, Ano97d, BM94c, HS96b, Hor98, LY93, MW98c, PW93a, Sin95, Ts’90]. Server-Aided [BQ95b, BQ95a, HCY96a, LY93, LL95a, MW98d, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. Server-Side [SVa+98]. servers [Abe98a, AG95, CM97b, GGK+99, Lee95, Udb98]. Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau93, MB99a, RRSW97a, RRSW97b, Ros96e, 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, DS90b, Don98, KW92, PS99b, You97, Zer96a, AA95, Acc97]. ses [Bon94]. Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f,
Session-Layer [BB95c]. Sessioneer [AG95]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB98, Kra99]. SETHEO [Sch99k]. sets [MT98]. settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB98, Kra99]. SETHEO [Sch99k]. SETHEO [Car97c]. Settled [Eri97a]. Severely [Gib95]. SG [Gue98b]. SHA [ANS97, MG98b, BGV97b, CJ98, MS95d, Sta94d]. SHA-0 [CJ98]. SHA-1 [ANS97]. Shakespeare [Lea90]. shallow [ACD94, WF94]. Shamir [She92g, Ada92, GGOQ98, 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, DH90, HD96a, IS91, Lei99b, MWB99, PS98g, RZ99, SN96, Sim90b, Sim91, Sim94a, Wi99, YL97b]. Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [MSNW99, BDG99, CDVG93, OK95, ZHS94]. Sharing [AGY95b, BC93a, BC95b, BBDW96, BK94a, BK95b, BDVG93, BDD+94, BM99c, BD90, Bri90a, B91g, Cac95a, Cac95b, CG98, CT97, CK90, DDP94a, DKK98, vD95a, DRL97, FDB93a, FGY96a, GJKR96b, GRSNW98, GRS98, HL93a, HKS97a, HKS97b, KI96, Kra94a, KOS+94, KOO95b, KOO95a, LP99, LCL92, LH93b, Mei92, MS95f, SNW98, OK98, Pai98a, Pai98b, Ped91d, Rab94, ROT94, Sch92b, Sch99i, S91a, Wil98a, AGY95a, BC95a, BI93, BDV93, BDS93, BCD94, BGS95, BCDV96, BDVG96, BD97, BDV98, BDG99, Bur96, CDVG91, CMP97, CGMW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FGY96b, FR95d, FO98, GM95, GRSNW98, HJKY95, Hwa92d, HC96, HLC99, JMI93, JMO95a, JMO95b, Jar96, KOO95a, KO96, KO97, Mao98, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, PS98a, Ped91b, Ped91e]. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95b, van97a, Ko99]. Shark [RDP96, WG97]. Shawn [Sha99a]. Shedding [HPG98, YHY98]. Shelf [Hat96, AG95]. Shell [Car99, Sch99a]. Shift [GO96b, G94, GN95a, GM91, GO95, PS97]. shift-register [GN95a]. Shifting [LMBO95]. Ship [NS98a, RP98]. Ship-Board [NS98a]. shipping [Ano95k]. Shooting [Aga92]. Shop [Ano97a]. Short [Kra94a, Ste94a, Wie90b, vOW96, BC95a, Coh94, Har94, Jo99, VW96, V97, Wie90a]. Shortage [DDJ98a]. Should [Way93c, YH96, Ano95c, Riv98c]. shrinking [MS95a, MS95b, Mih96]. SHS [NIS93b, Nat92b]. shu [XtTu94]. SIAM [ACM97b]. sihere [Hor99]. Side [KWS98a, KWS98b, KWS98c, SV+a98, Y96]. sides [MB94b]. Siege [EH96]. Siegenthaler [MS99b]. Siemens [Ano97-27, Bro97, Dav98c, Mac98, Sel98b, TJ97]. Sieve [LLMP90, LL93a, Per93, CDE+96, Gar93b, Pom94]. sifrovani [Gar98c]. SIGACT [ACM99a]. SIGGRAPH [ACM99c, B+99b]. Signal [IEE97c]. SIGINT [Myc98]. Sign [BM92, GR97, GHR99, WB98, BR96c]. Signal [IEE97c, IEE97d, LKW96, Pit95, She92e, T98]. Signalling [Lin98]. Signals [AK99, BTH96, DDM98, MHMW98]. Signature [AA95, Acc97, AW94, Int91a, NIS94, Ano96e, Ano97-29, BP97a, BM99a, BM99b, BM96b, BM96c, Bra93a, CS97a, CM99a, CG98, CH98, CK95, CDF95, CD95, DMPW98, DQ94, DY91c, DN94, FL99a, FKM98, FOM91, FO901, GP99, GQW+a91, HJ+a91, KKS97, K98d, KPG99, Kob98c, Kra93, LK96, LHW98, LK99, LM95, LHL94, L98, MT94, MB99a, Mer90b, Mer97, MH96, MSS98, Mis98, Mi96, Mon93, Nat91, Nat92a, Nat94c,
Bov98b, BDB92, Cha99a, Cha91, CM99c, Chr99a, Con98, Con99a, Cor98, CH99a, DDJ98d, DDJ98b, DDJ99, Deu97, Deu98, Di 97a, DT98b, EN98, ENK99, Fan96, FGLP96a, FGLP96b, FOM91, Gar97a, GL96, GPSV98, Gut98a, HKQ99, HP98a, Hru96, HH99, Hus99, Koe99, KCC94a, KCC94b, Mar98a, Mye96, NM96b, Omu90, PV98, Roh99, SWK98d, SS99a, Sch90a, SR96, SGPV98, Sut99, Tua99, VW98, Ver98b, DWQ91b, dWQ91a, ABKL93, AHJ97, Ae97, BGV97a, Cha99b, CW97, CJRR99b, DS98a, Dhe98, Di 97b, DF97, Gau97, Kip97, Sha95a, TJ97, Ta99b, AG99, Bak99, BF99a, Bro97, DV96, Gir99, GSTD96, HNS99, IW99, NK99, SS99, SM94, SKAM99].

Smart-Cards [Roh99, ABKL91, ABKL93, CJRR99b].

Smartcard [Ano98h, Ano99b, USE99a, Ano98g, CH94b, IH99b, KK99a].


Societeal [Sta97b]. Societies [IEE92d, EIE94f, IEE95c]. Society [Ano98f, IE92e, IE93b, IE94d, Mar96, DL96, KG96, Ta99b]. Socio [SM99]. Socio-technical [SM99]. Sockets [ZG96].

SOCKS [Lee96, McM96]. Soft [NS98a].

Software [Abr97, Ano93i, Anc96, AG99, Bal97, Bih97b, BD94, CD97, Cha98a, CT99b, DBV96, DF91c, DS99a, Gar97a, GO96a, Gut98b, HK97, JJ98c, KP96b, LU95, Lac93, Lea99, Luh98, Ma96b, Mer91, MME97, RSA94, RC94a, RC94b, SW94a, Sch9c, SK96a, SK96b, SK96c, SW97a, SW97b, SK97c, She95b, You96, And94a, Ano95k, Bih97c, BP97b, DH96a, Des95, Gol96d, Knu99c, Pre95a, SS98a, SAM97, Str93a, Str93b, Vau98e, Woo90].


Ou99, SW94a, Tou92]. Specifications
[KS98a, Nat92b]. Specified [Gui97, HCC98].
Specifying [SW94a]. Specs [Got99].
Spectral [WF94].
[CKLS97, She94c, CKLS96b, CKLS96c, Dix94, KSB96b, KSB97, LLB98, OP98].
Speech [DMFB97, Er97b, GDS91, IEE97d, IEE97e, Luc97, SW95b, All97, CW94].
Speakers [Bar94].
[ARV99a, ARV99b, Ano99c, Ano99e, DP98a, DP98b, Ebe93, FVEA99, IM93b, Koc94, LS97, MPPS95, SKNO98a, SKNO98b, SW97a, SW97b, She92d, She95b, IM93a, Kap98, KAK96, Lam99, Nor95a, HKSW98, HKRS99, Zhe97a].
Speeding [ADES99, KT93, McK99, Tes98].
[AG97b, AG97c, AG97a]. Spiculated [ZTR99].
Spin [RK99]. Spite [Wai90].
[SPJ TLS99]. SPLICE [HC95b].
SPLICE/AS [HC95b]. Split [Coc97].
Splitting [Sga91b].
SPM [CV93]. SPN [Kob99].
SPN-Structures [Kob99]. Spoofing
[SvW91]. SPRC [Wol93b]. Spread
[CKLS97, Dix94, She94c, CKLS96b, CKLS96c, KSB96b, KSB97, LLB98, OP98].
Spreading [SB94, KSB96a]. Spring
[DDJ98d]. Springer [Hat96].
Springer-Verlag [Hat96]. Spurs [Lea99].
SPX [Ala93b]. Spy [WS96c, Win91].
spy-catching [WS96c]. Synchronise
[Cha90]. SQL [CM98]. SQL*Net [Ano95k].
Square [DKR97b, DKR97a, EPR99b, EPR99a, Gar98a]. squares [BSNP97].
squeamish [AGLL95]. SRA [SS93]. SSH
[Sar97]. SSL
[Ano97r, FKK96, WS96a, WS96b, WS97]. ssmtp [BRW99]. Stabbing [Aga92].
Stability [Wed99, DXS91]. Stabilization
[YMW99]. Stabilizer [BS99a]. Stage
[Ano97d]. staircase [MK92]. Stakes
[GO96c]. stamp [HS91]. Stamping
[BLLV98, BH93]. Stamps [HS95].
Standard [AA95, Acc97, Int91a, Nat93b, Ano93f, NIS94, Ano95i, Ano95j, Ble98a, Com94a, Com94b, FIP93b, FIP94, Gar98a, Gar98b, Kal97a, RAS93f, Law98, Len96, LM91b, Nat91, Nat93a, NIS93b, Nat94a, Nat95, Nat97b, Nat98, Nat99a, Natxx, NIS93a, Nys99, RAS93d, RAS93e, RAS93e, RAS93a, RAS99b, RP94, RD99a, RD99b, SB93, Ano90, Ano95c, CCN95, LM91a, Nat93c, NMVR95a, Pri94, Rev91, Tha91, Un96a, Ada98, ARRW99, ABK98a, Ano94b, Ano95n, Ano97h, Ano97x, Bar91, Bas98, Bas95, BS93b, Bir95, CMK98, Cop94a, DDJ98a, Den90, Gai90, Gar98b, HK98, HK99d, Hub98, Joh90, Kap98, KM97, Mat94a, Nat92a, Nat92b, Nat94b, Nat94c, Nat94d, Nat99c, NMVR95b, NBD+99, Pai96, Per91, RASA93b, RP94, Riv93c, She95b, She92g, Sim95, SB92, SB99, Wil93a, Ano95c].
Standardisation [Ved98b].
Standardization [Ano96k, Pre93b].
Standardized [Ano95n]. Standards
[Ano90, Ano95n, Ano96k, Ano97y, Ano97z, Ano98i, DDJ98b, FBS97, Gar97a, Gar98b, Got99, GO96c, IEE94b, Kal93a, Kal99, MBB98, PP96, Ano92b]. Standards-Based
[FBS97]. Stanford [IEE98b]. Stanica
[YT96]. Stanley [vdWS97, vS97]. Star
[Ano97r, H97]. starts [Ano96l]. State
[FGS96, Lan98, LF99, Mj93, NM96a, Pre98c, PR98, Pre99, She92e, Wols93a, Wols93b, Zaj97, BFS92a, BFS92b, Gut96, PGV93d, Ril96].
State-industry [Zaj97]. State-of-the-Art
[She92e]. Stateless [BG99].
STATEMATE [DJHP98]. Statement
[HI96]. States
[Chl97, Cl99, Lev91, Mil95, UU97b].
statesman [Bed90]. Station
[BWM99b, Smi98b]. Station-to-Station
[BWM99b]. Statistical
[De 99, GC91, GSV99, Gus96, PNFK95, NO98, Tha91, GKS97]. Statistics
[BBDF97, IEE94a, F90]. Status
[Dob96b, FL99b, Nat99c, NBD+99, Ros95b].
Stay [MK94]. Staying [Rit99]. Steady
[MSP99]. Steal [Wal99b]. Steganalysis
Steganographia [Ree98].

Steganographic [ANS98a, CM97c, NHB98, ZFKP98, ZF9+98]. Steganographie [MPS94].

Steganography [All98, And96b, AP98, Cac98, Cra98, Cl96, DS96, FJM96, Joh97a, Joh97b, JJ98b, JJ98a, JJ98c, Kah96a, MT94, Man97c, NNEK97, Phi98, Rh905, WW98a, Cai96, Cra97].

Steiner [ZW99].

Steps [GO96b].

Stern [Cus97].

Still [BI99, Mei98, BBCP97].

Stockholders [MS99a].

Stop [BP97a, PP97, SSNP99, vHPP93, Pfi96c].

Storage [AR99, BFS96, CMN99, SJ97, WB92, BMS96, Sta97a].

Store [AW99, CadHSV96, Way91].

store-and-forward [CadHSV96].

stored [SV99a, SV99b, Lee95, Sv98a].

Story [DDJ98g, DDJ98h, El97, Hay98, H93, RK98b, We97].

STRATA [PMP99].

Strategies [AW99, CO98, Dae95, KFJP96].

Strategy [Gar97, KTM+99, OMV99].

Stream [AM97, BD94, Cha94a, CS91, Cla97, Cla98a, DC98b, Din94, DNR97, Gol97d, Gol99b, J99b, LS97, Mau91a, MS91, PK95a, PK95b, Pen96, Rob95b, Ros98a, SK97b, SK97a, She94a, She94d, War98, ZYW91, ZG96, BK95a, DGV94b, DX91, Gol95b, Gol98b, J99a, LRW93, Tay94]. Stream-Cipher [ZYW91]. Streams [GR97, PSB97].

Street [KS98b, Sim98c, HRT96, Law98].

Strength [HK98, HK99d, Cop94a, CM97, Mat95].

strengthen [BB95a]. Strengthened [DBP96].

Strengthening [MB94a].

Stretch [Pai99b].

Stretching [And96b]. strict [ZZ94a, YT96, Cus96, CS96c, O’C94].

string [Ole95].

string-rewriting [Ole94].

Strings [Go96b].

Strong [FS97b, MAM95, SVa+98].

Stronghold [An97r].

Strongly [Mat91d].

Strongly-Randomized [Mat91d].

Structural [BHJM99].

Structure [BCC90, HV98, Mat96a, PRAM98, LL93b, M95, PS98a, RD96a, Sch98a].

structured [FR95a, KS98c, O’C95, SK97d].

Structures [BRS99, EKLM99, Kob99, Lut98, MSNW99, SZZ95b, La95, Mic97, PD99a].

Structuring [HN99].

Struggle [Gl99b].

STS [BWM99b].

Stubblebine [HLL+95].

Stubs [AO96].

Subband [TK98].

Subcommittee [Uni98d, Uni97b, Uni95a].

Subcommittees [Uni98e].

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, SW+99b].

Submit [Law98].

Submit [Law98].

Subquadratic [BBP95a, BBP95b].

Subscribers [GC97].

subscribe [Mau91b].

Subsegments [KPR99].

Subset [NS99b, CJL+92].

Substitution [CT99a, HS90, PRAM98, SZZ94b, ZZ96, Ata94, FS93, Fri92b, HT95, O’C95, Zan90].

Substitution-Permutation [CT99a, HT95, O’C95, Zan90].

Subtitle [Mer90b].

substantial [Bli98c, TY94].

Subtitles [Gr97, PSB97].

Substitution [An97r].

Successful [HA94b].

sufficient [AI 96].

Successor [An97z].

Sufficient [MSN99, Rus93b, Rom90b].

Suggested [Bi91].

Suggestions [Mat96b].

suitable [CCZ98, K90, MZB98, Miy93a, Nac93, NM94, XL98, YL95a].

Sum [NS99b, CJL+92, JY98a].

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 [DMS95, She92c, Bam97].
Supercomputing [IEE91]. superhighway
[BDC+95]. Superimposing [YY91].
supersafe [PP96]. Superscalar [Cla97].
superscrire [Cra92, CF92]. Supersingular [BS91b].
Support [AKP99, BV98a, Bla98, Bld93, DTDJ99,
FR95d, GRB99, HKS95, KHB99, LBHM99,
LCN99, Mon93, Pit96b, SK98a, SK99, SL99,
TY999, Cli99, LS98a, TCH+91, Un94b].
Supporting [PK99, MI90]. Surmounting [CI96].
surrounding [GA98]. Surveillance
[CKN99, SB97]. Survey
[Bri90b, Gar97c, GFB93, Kal93a, Cle90,
Knu98b, Par98c, BO92, Ele99, CC99c,
CH04b, CM99d, DD99, DT98a, DTDJ99,
Far92, FK99, FO97, FR95d, Ga96b, Gar97a,
GRB99, Go90a, GSP98, GS99a, HJT99,
HDC99, HJL99, HE98, INDI99, JD97,
Jia99, KI99, KW99, LMP99, LWY95, LC99,
MGL+98, MLK99, MR95a, Mar98a, Mau97b,
MTV92, Mon93, NM99, NS98a, Nec96,
PRZ99, PS99f, PK99, Rei92, Rus90, RH99,
SYMI98, SSSW98, Sam98, STSW99, SCT99,
SK96b, SK96c, Sch98b, SSP90, SM99,
SKIT99, Tro93, Tun99, Var99b, WHFG92,
WAB99, WW98a, WBB99, WBB94,
ZK96, ACC99, BBC98b, Bax97, BM97a,
Bur94a, BD95b, Car94, CB96, Cus95,
DSS99, Des95, DH96b, FM98b, HN94].
system
[HI97, Hwa92a, HC95b, KM98b, Kru97,
LC96a, LCL95, MY93b, MKKW99, MM95,
Oel97, PS90e, PS95b, Sch99j, SY96b, SS95b,
SS95c, TCH+91, TC91, Ven90, WSFC99,
WABL93, ADD91, An91a, Bax97, Bel92,
Dan95, JD91, RC91, YK99, ZH98].
Systematic [BGH+91]. Synonyme
[MLK99]. System
[BH95b]. Systems
[ABL93, AKP96, AKF94, Ako99, An94j,
An95i, An96a, AEDS99, AA97, AMP99,
BDPSNG95, Bar99, Bas93, BR91, BBDF97,
BFN98a, CF95, DDJ98a, Dan91b, DFTY97,
DY91a, DD99, DB96, ENK99, FJP96,
FY95a, FY95b, FY99, FO99a, GL96,
GFB93, Gil98, GM90, GMW91, GK96, GS97,
GMV98, HGH98, HJJ+xx, HH94, HP98b, IEE93a, IEE96b, IEE96d, IEE98e, IEE99b, IH99a, KT96, Koc96b, KA99, KYB92, LO91b, LQRS98, LABW92, Lan99, Lee99b, Mar99, Mas99a, MS95f, MDP94, Mu93, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PSN91, Pin97, Pit96b, PM99a, PDR94, RG95, RIP95a, ST94, SN96, STS99b, DY91c, SOOS95, SS90, She92a, SY92, Tra99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a.

Systems
[WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFK98, ZFK+98, ARK99, AhdJF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BP95b, CG95, DMW94, Dix94, Fr92b, Goo96, GKS97, Gru98, HJJ+97, IEE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Oh96, Ole95, Opp96, PA98b, PP92a, PP92b, PP95b, PP95a, RO96, SK97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DV96].

Systolic
[SS98, DF92, PJBM90], SZK [Dav98d].

Targeted
[Cap94], Targets [Lea99, Way98].

TAS [Cop94b], Tasty [Sch98i], Tate [FMR99], Taxing [Gar97c], Taxonomy [DB96, GS97, LBMC94], TC [MB99b].

TC11 [Kat97], TC6 [Kat97], TC6/TC11 [Kat97], TCFS [Man97b], Tcl [GA98].

TCP [Fei93, Fei96], TCP/IP [Fei93, Fei96].

Team [KSW97a, KSW97b, NW97, WN95].

Technique [DDN98, Gue98b, KP93, WD97, BCV97, ONT98, Way95].

Techniques
[Int91a, BGML96, BW98, Bol98a, Bol98b, BL99, CM97b, CD99, CMYY98, Dan90a, Dan91a, Dav91, DC98c, De 95, Des98a, Des96a, Fun97, Fun98c, GQ95, Hel94, JJ99a, LvdLB96, MM99a, MSNW99, Man96b, Ps98e, Ps98f, PK99, Pre93b, QV90, QG95, Rue93, SZ93, Car98, Cra96, Hel93, Hel98b, ISO97, Kay95, KG93, Ny98, OP9+99, Oke96, Ps99d, SD97, Ste99b, Way91, Woo90, ZH93, van96].

Technological [UFC94].

Technologies
[Dan96, DSS98, Aus96, BGV97a, BK94b, BS95e, Oh96, Un96a], Technology [Int91a, An96l, An96m, An98j], AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, HH96, IEE94b, IEE98d, LC94, Lln93c, NFF99, Riv98c, USE99c, An93a, DS97b, Gil97, ISO97, Ril96, Ros94, Smi97a, VB96, CFF+.91, Ers99, An99b].

Telecollaboration [Fue99].

Telecommunications
[IEE97e, UN94, Mac98].

Telemedicine [An97-29].

Telephone [Gar97a], Telephony [Ban94, Gar97b, MB99a, Mar95b].

teletype [Mac98].

TELNET
[SSH93, Ala93b, Bor93a, Bor93b, Bor93c].
Traveling [OMV98, RS99a]. Travois [Yuv97]. treaties [Des90a]. Treatise [Tur99]. Treatment [BFN98b, Mau96a, OO98, BDJR97, BFN98a].

TREC’98 [LM98a]. Tree [BM96b, BM96c, GM99b, PB99a, LL93b, O’C95].

Tree-Based [BM96b, BM96c].

tree-structured [O’C95]. Tree-Width [GM99b].

Trees [Aga92, BP97a, HS90, ZW99, SSM92].

Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De93b, De98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].

Tree-Based [BM96b, BM96c].

tree-structured [O’C95]. Tree-Width [GM99b].

Trees [Aga92, BP97a, HS90, ZW99, SSM92].

Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De93b, De98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].

Tree-Based [BM96b, BM96c].

tree-structured [O’C95]. Tree-Width [GM99b].

Trees [Aga92, BP97a, HS90, ZW99, SSM92].

Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De93b, De98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].

Tree-Based [BM96b, BM96c].

tree-structured [O’C95]. Tree-Width [GM99b].

Trees [Aga92, BP97a, HS90, ZW99, SSM92].

Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De93b, De98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].
[ANS97, ANS98b, Ada97a, AGS97, AHdJF97, Ano99h, BDPSN97, BCK96e, BBS99a, BFP99, BW98, CIBM99, CK95, CM99d, Des96a, DS97d, ESST99, FVEA99, FW91, FY98b, GM97, GAGCDAFC99, GS99a, HNSS99, HRVV99, HJPB97, IR99, JM99, JJ98c, JQ97, KR94b, KS99a, KA99, KT93, Lon92, LF99, LML98, Low96, LW99, Lud97, MAM95, Mih94, MCD99, Mis97, MFG95, NT99, NHB98, NNEK97, Oh99, OOK91, Ou99, OMI93, PSB97, Pin97, PZ98, PJ99, QG90, RB99, SG95, SK94, Sas99a, SK96a, SK97b, SK97a, SK97c, SD99, SRY99, SR96, Sim94d, SHK99b, Sun91a, SZT98a, TAP90, TYD99, TOU94, VNW94, WKHG97, WCS95, Yam98b, Yam99, YST99a, YY97a, YST99b, AA95, All98, Ata94, BSNP96a, BSNP96b, BTD98, BGR95, B93, B99a, BB95a, BB98a, BD95a, CW91a, CNST98, CC95].

using [CGM97b, CPPK98, CB96, Cle96, Dan97, Jak95, JM96a, KR95a, KC95, Kar96, Kay95, Koe95, KH97, KH98a, LC96b, LC96c, LMBO95, MHP96, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SSM94, SD97, Su98, SZT98b, SZTB98, Tak97, Til98, VZ97, VP98, Whi93, Wil93a, Yam98a, Zho94, dR95].

Utility [Zol93, Vu95]. Utilization [GRB99]. Utilize [MSO96]. utilizing [SW95a].

**V** [IEE92a]. **V.1.0** [Lim99, RSA99a]. **v2.0** [Ano97r, RSA99b]. **V32bis** [Ano93k]. **V5** [IH99a, KN93, Lee96, Ts'97]. Validating [Gai90]. Validation


Values [GS94a, Tho96]. Vancouver [Yua92]. Vanstone [Kie98, NS97c, NS97b, Sha99a]. Vaporware [DD99e, DD98f]. Variable

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

**Variable-Input-Length** [BR99a, BR99b]. **Variable-Length** [Sch94b, Su98]. **Variance** [Kas96]. **Variants** [CRRY99, MSS98, R99a, Sha95a].

**variation** [CCN95]. **variations** [Zho94]. **varieties** [Fri92b]. **Various** [GQW9+91].

**Vascularature** [BALS99]. **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, GM95, Ped91d, Sch99i, VBD99, AGY95a, BD98a, Bur96, FO98, Mao97, MILY93, Ped91b, Ped91e, Sta96a]. **Verification** [Abe98a, AB97, BGR98a, Boi98a, Boi98b, CDFI95, DS97a, GFB93, GS99a, HL92, MM99a, Na97, OMI93, PM98, PV98, SM95a, SY99, Tou93, WW98b, YY99a, BGR98b, Boi97, BS95c, Des90a, Dwo91, JC98, JW01, Mea95, YL95a, YM98, ZLX99].

**Verifications** [GMV98]. **Verifier** [JMS96]. **Verifiers** [PM98]. **Verify** [DS97d, Chi99a, Chi99b]. **Verifying** [LHB96, Sa91, DN95b, Pau98]. Verlag [Hat96]. **Verlässliche** [BGH95b]. **Vermont** [IEE96a]. **Verschlüsselte** [Kip97, Kip99b].

**Verschlüsselung** [MPS94]. **Verschlüsselungssysteme** [Wal98]. **Verschlüsselungsverfahren** [Ger97].

**Version** [Ano97r, Ano97s, BC93a, BP98e, DBP96, FKK96, Gar97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, R93f, Lim99, MT99a, McM96, R93a, R94, DY91c, SS99b, SM98b, WABC99, CLW98, GM93a, Gib95, Bor93b, Lin96b]. **Versus** [MGL*98].

**Vertraulichkeit** [FT95]. **Very** [HMV93, MSDS90, PF94, Yua92, SN94].

**Veto** [OK96a]. **VHDL** [Oel97]. **via**
VoD [GMDS98]. Voice
[CM97b, MB99a, Cha94b, Int91b]. vol
[Ano97-28]. volume [Kat97]. Voting
[Boy90, JT97a, Mv93, NR94, SK94, SK95,
Schr99, FOO93]. vowel [Lie98]. Voyager
[AHMS99]. Vries [GK95b]. VRML
[Gar97b, Gar98a]. vs [DP99, GA98, Mus92,
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 [SFS97].
Wang [vT93]. Want [Rot97, Way93c].
Wanted [Bra95d, Hill97, PKA+98]. War
[Alv98b, AK99, Dav98a, Don98, Law98,
Mon96, Mus92, Rat96, Ros99, Wei99,
Wil98a, Dre92, Mar98b, Hin93, Joh95].
Warden [Cra98, Cra97]. Warehouse
[ELM99, TLS99]. Warehousing
[BMNL99]. warfare [Den99, Rot95a].
WARM [MPL99]. WARM-UP [MPL99].
Warned [Keh91b]. Warning [Gar97c].
Warrant [LWY95]. Warranty [FKMY98].
Warranty-Based [FKMY98]. Wars
[GC97]. warum [MPS94]. Was
[CFK+91, Dea98b, Koh90, Mon96].
Washington
[HF97, USE98a, USE99a, DDJ98c, DDJ98f].
WASS [PS99b, PS99c]. Watch
[Cha99a, Rit99, Sch99]. watchdog
[MPS96]. Water [WF94]. Watermark
[Ano97o, CKLS96a, OMT98, SY98, TRS*93,
WD96, vTO94, And98, Ano93a, CKLS96b,
CMYY97, PBBC97, TOH98, XBA97,
YEA+98]. watermarked
[BP98b, BP98c, RRP97]. Watermarking
[ACK98, ADF98, Ben99, Ber97b, BOD95,
BO96b, BFW99, Car97a, CKLS97, CMYY98,
DDM98, DDGM97, DSS98, EQ98, El99,
FBS98, GDD+97, GB98, GO96c, HG97c,
HG97d, HG98, KR98, Koh97, LQRS98,
MBB98, Mos98, OMA97, OMA98, PZ98, QN98b, RKDB96, SCxx, SZT96b, SZT98a, WK97, WD97, Xie98, YY99a, ZK96, BBCP97, BBCP98b, BBC98, BCD98, BP98d, BCV97, BO96a, CPO+98, CHO+98, CT99b, CKLS96c, CM97d, DQM98, DDM96, DDM98, DNSS98, HG96, HG97e, HEG98, HPA99, HW97, HW98a, HW98b, Irw98, KH97, KH98a, MNT97, Nat97a, NO98, NP98b, ODB96, OP97, OP98, OP99, Oko96, PHF99, SD97, SHG98, SZTB98, TA97, TKS98, VP96, VP98, VNP98, Ye97, Ye98, YM98, ZK98, ZKOY99.

Watermarks [Ano97n, BTH96, BI99, CL98, EKK99, HPG98, LvD98, LKD98, Mae98, MMST98, YYH98, CL97b, LLB98, Min97, MBY97, ZL97, Zha96].

Watson [CFK+91].

Wave [GO96c]. Waveguides [FVEA99].

Wavelet [LSVV95, KH97, KH98a, NO98, XA98]. wavelet-based [KH97].

Wavelets [Lut98].

Waves [Dal97]. Way [BJY97, BdM94, BM94a, BKK98, BP97c, DGV93, DDP90, GMDS98, Mer90a, Roe94, Sch91b, TOU94, Zhe90, BHH99, BK98f, D199, Dob98, HILL99, HYL99, Hwa92a, MZ98, Rom90b, Sim98c, Sta94a, Sze98, Tsu92b, Tsu92a, ZPS93, KSW97a, KSW97b].

Wayner [vdWS97, vS97]. Wayness [HT99].

ways [Den95]. WDAG [TV94]. Weak [DGV94c, DYL98, Haw98b, Pit96b, Sze98, Vau96, FY95c, Hae98a, Knu95, SSI97a, SSI97b, YL97b].

Weakened [AB99a, AB99b]. Weakly [MP91].

Weakness [Cop99, KSW99a, Kie98].

Weaknesses [BMS94, DY91e, Kel99, KP93, Lan96, PA98b, RK98a, Ri99, SZ96, DGV94b, She96b, ZZ97].

weapon [Ano97]. weapons [Me98].

Web [Ano97r, MR98, OW95, SA95, Sta95a, Ver98b, Ale98, Ano97d, Bal99, BMNN99, Cha99b, Dav95, DDK98, FL96, GGM997, GO96c, Law98, She96b, Ude98, WCSS95, You96, ZL99].

Web-Based [ZL99]. Web-enabled [Ch99].

WebTime [Ano97s]. Weighing [KR96]. Weight [PK95a, PK95b, Pen96, She95c, BGH+95a, CC98]. Weighted [MPS99]. Welcome [Riv95c]. wen [XrTuW94]. Weren’t [Kah91b]. West [DDJ98c, Fra99, Hir97, Hir98].

wheel [Car97c]. Wheeler [Bar95]. Where [DDJ98c, DDJ98d, LHL95b, LHL95a, Van95b].

wherein [Lea90]. Which [Che92, EvH91, Ev92, 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 [CLI99].

Width [GM99b]. Wie [MP994].

Will [DDJ98d, Gar97b, GC97, Gar98a, Wor96, Ano98h, Gau97, Mi9f, Sch93e, ZKOY99].

William [Lea90, Un92, vdWS97, vS97].

Williams [JQ98b]. Window [Bel92, KT93, PKA+98]. Windows [USE98a, Boy98, Br98, IH98, Ken95, RC95, ZG96].

Windsor [SIJ93]. Winkel [Ers99].

Winnowing [Riv98]. Winter [USE91, USE92a, USE96c]. WIPO [Gar97c].

Wire [Wal94]. Wireless [Gar98a, PS98d, She93d, Goo96, IEE97k, PS98e, PS99d, PS99a, PS99e, WSFC99, PS99c, PS99f]. Wiretap [Ele98].

wiretapping [DL98, RKL94, Rot95a].

wisdom [JC98]. Wise [Ano96j]. Within [BVG93, BGM97a, BGM97b, FL93, HJT99, K9W2, MG98a, MG98b].

Without [BP97a, BMRW98, GHR99, Hus99, Len96, Luc98b, SG99a, Abe99, Ano98j, Ben94, Ble96, HY93a, HG97d, Hor95, IS91, JMO95a, JC98, KRS99, LM94a, LM94b, LWC96, Ped91c, PBBC97, Riv98d, Sak97, Sm94b, SS99e, SS99f, Wu92].

withstand [OY91]. Withstanding [SVxW91]. Witness [CDS94, FGY96b, FGY96a, RGV97].

Witness-based [FGY96b, FGY96a]. witnesses [She92b]. Woes
[DDJ98g, DDJ98h]. Wollongong [PSN95b]. women [Wil98a]. won't [AK95, ZKOY99].
Woollongong [GN95b]. Worchester [KP99b]. Word [LMBO95]. Words [HKL94, Ata94, AGLL95, CC98, SM90, Sta96b].
Work [Abe98a, Ano97y, BK95c, CFSY96, Gar98b, MGL*98, B199b].
workfactor [Jas96, Kau96]. Working [DDJ99, Kat97, LM98a, MB99b]. Works [Ano96k, FJM+96].
Workshop [ACM98a, And94a, ???90, Ano93g, Ano99b, Auc98, Bih97c, Bra93a, CW94, Chr99b, Dam90a, Dam91a, Dav91, De 95, FM91, Gol96d, Hel94, IEE92a, IEE93a, IEE94a, IEE96b, IEE96c, IEE96d, IEE97c, IEE99b, IZ98, IZ99, Knt99c, KP99b, Kui91, LW96, MDP94, Pit95, PH91, QV90, Rue93, Sch94j, SZ93, TM99, USE95c, USE96d, USE96b, USE98b, USE99c, BF92a, BFS92b, CF96g, Chr98, D+98, FR95a, GS94b, Lom97, Org98a, Pre99a, TV94, USE90, Vau98e, W998b, Ano96k]. Workspaces [BV98a]. Workstation [DS90b, IEE93a].
Wrapping [Gar97a]. Wright [WD99a].
Write [Bra95d]. Writing [Kah96b, Sha99a, Ros97c]. Wu [Bur94a, Bur94b, HLC96, Roe99].
Wu-Dawson [Roe99]. WW [Pin98].
WWOS [IEE93a]. WWOS-IV [IEE93a].
WWW [OW95, Zha96].
X [Bel92, BALS99, KSW97a, KSW97b, Smi98b, Yu94a, Yu94b, PVO95]. X-ray


Y2K [Ano98j, DDJ98b, Eri97b, Law98, MGL+98].
Yaksha [Gan96b]. Year [Sch95a, Sil99, Roe95]. Years [Bon99, Yin97, BC96b, CWM+91, Den90, Gol97c, Mar96].
yi [IPNdbbprn91]. Yield [GMW91].
Yokohama [IZ98]. York [IEE99a, USE95c].
Yu [BY92]. YY [Nat92b].

Z [Mau91b]. Z80180 [Kal93b]. Zero [EG90, BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, D999, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOV93, NMV99, OO90, RS91, SI93a, BOGG+90, BBP95a, BBP95b, DF93, DP94, DF91b, Sah99].
Zero-Knowledge [BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, D999, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOV93, NMV99, OO90, RS91, SI93a, BOGG+90, BBP95a, BBP95b, DF93, DP94, DF91b, Sah99].
zeta [Kob91c]. zeta-polynomials [Kob91c].
Zhang [JW91, Ng99, GP99, LHW98]. Zhu [Ng99].
Zimmerman [Ros95a]. Zimmermann [Ros97a, Ros96c]. Zinc [RK93].
Ziv [Mun91a, Mun91b]. Zn* [Boy97]. Zur [KK97]. Zürich [ACM97a].
References

Anonymous:1990:IWH

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

Anonymous:1997:ACC


ANSI:1988:FIE


Anshel:1993:PMT


ANSI:1995:ANS


Arabnia:1997:IC1


Abdikalikov:1999:ERC


Abelson:1997:RKR

Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John


REFERENCES


REFERENCES


Abadi:1993:ADS


Abadi:1993:CAC


Abraham:1997:SEE


Auyong:1997:ASC


Apolloni:1990:TNN


ASCFS:1997:XPK

REFERENCES

An:1999:ODR


Angelo:1994:DFS


Alexi:1984:RRB


Alexi:1988:RRF


Acken:1998:HWA


ACM:1982:PFA


ACM:1983:PFA


REFERENCES


REFERENCES


REFERENCES

[UCSB98] ucsb.edu/conferences/java98/program.html


REFERENCES


REFERENCES


[Adl87] Leonard Adleman. Pre-RSA days: History and
lessons. In Ashenhurst [Ash87], page ?? ISBN
0-201-07794-9. LCCN
Turing Award lecture.

N. Asokan, Hervé De-
bar, Michael Steiner, and
Michael Waidner. Au-
thenticating public ter-
inals. Computer Net-
works (Amsterdam, Nether-
lands: 1999), 31(8):861–
870, April 23, 1999. CO-
DEN ???. ISSN 1389-1286
(print), 1872-7069 (elec-
elsevier.com/cas/tree/
store/comnet/sub/1999/
31/8/2125.pdf.

Jim Alves-Foss and Sal-
vador Barbosa. Assess-
ing computer security vul-
nability. Operating Sys-
tems Review, 29(3):3–13,
July 1995. CODEN OS-
RED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic).

A. Apostolico and R. Gi-
Ancarlo. Pattern matching
machine implementation of
a fast test for unique de-
cipherability. Information
Processing Letters, 18(3):
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

Alberto Apostolico and Zvi
Galil, editors. Combinato-
torial algorithms on words
(Maratea, Italy, June 18–
22, 1984), volume 12 of
Springer-Verlag, Berlin,
Germany / Heidelberg,
Germany / London, UK /
etc., 1985. ISBN 0-387-
15227-X. LCCN QA164

Scot Anderson and Rick
Garvin. Sessioneer: flex-
ible session level authen-
tication with off the shelf
servers and clients. Com-
puter Networks and ISDN
Systems, 27(6):1047–1053,
April 3, 1995. CODEN CNI-
SE9. ISSN 0169-7552
(print), 1879-2324 (elec-
elsevier.com/cas/tree/
store/comnet/sub/1995/
27/6/1464.pdf.

M. Abadi and A. D. Gor-
don. Reasoning about
cryptographic protocols in
the Spi calculus. Lecture
Notes in Computer Science,
1243:59–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
Abadi:1997:CCPa


Abadi:1997:CCPb


Abadi:1998:BMCa


Abadi:1998:BMCb


Aura:1999:SLM


Agarwal:1992:RSO


Atkins:1995:MWS

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Alberti:1470:TC

Alexander:1945:CHG

Alexandris:1992:FMC

Alexandre:1997:BSC

Alexandre:1998:JBP

Allen:1997:DEC

Allen:1998:SUM

Ahituv:1987:PED
Aiello:1998:FDI


Alvarez:1998:FLV


Alvarez:1998:PCS


Akl:1985:FPR


REFERENCES

[ABAECITDISC:1996:DSG]

[Ame96a]

[Ame96b]

[AMP99]

[AMS96]

[AMV90]

[AMV93]
REFERENCES


REFERENCES

Anderson:1993:PRT

Anderson:1994:FSE

Anderson:1994:WCF

Anderson:1996:CEM

Anderson:1996:SLS

Anderson:1996:IHF

Anderson:1998:EWF

Anonymous:1922:PUS
[Ano22] Anonymous. Practical uses for the spectroscope, secret

[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:1978:CSD]


[Anonymous:1980:ACS]


Anonymous. Corrections: How Polish Mathematicians Deciphered the Enigma, 3(3) 232, Reviews: H. H.
Goldstine: A History of Numerical Analysis, 3(3) 293.  
DEN AHCOE5. ISSN 0164-1239. URL http:// 
dlib.computer.org/an/books/an1981/pdf/a4400. 
pdf. See [Rej81, SWT+81].

**Anonymous:1981:GIU**

Bureau of Standards. *Federal information processing standards publication, FIPS PUB*. U.S. National Bureau 
of Standards, Gaithersburg, MD, USA, 1981. ISSN 0083-1816. 39 pp.

**Anonymous:1982:CC**

Anonymous. *A course in cryptanalysis*, volume 33, 34 of *Cryptographic series*. 
0-89412-052-2 (vol. 1), 0- 
89412-053-0 (vol. 2). LCCN ????

**Anonymous:1982:ESS**

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

**Anonymous:1982:NNPa**

Anonymous. News and notices: Pioneer Award Es-

tablished by Computer Society; Undergraduate Pa-
per Competition in Cryptology. *Annals of the His-
tory of Computing*, 4(2): 184, April/June 1982. CO- 
DEN AHCOE5. ISSN 0164-1239. URL http:// 
dlib.computer.org/an/books/an1982/pdf/a2184.pdf; 
http://www.computer. 
org/annals/an1982/a2184abs.htm.

**Anonymous:1984:ESC**

Anonymous. *EDP security: communications, database, end user, encryption: advanced security concepts*. 
Number 3 in FTP technical library EDP security. FTP, Port Jefferson Station, NY, USA, 1984. various pp.

**Anonymous:1985:BM**

Anonymous. Back matter. In Blakley and Chaum [BC85], page ?? CO- 
DEN LNCSD9. ISBN 0- 
387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 
com/openurl.asp?genre= 
article&issn=????&volume= 
0&issue=0&page=?. 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-
REFERENCES

sored by the International Association for Cryptologic Research.

Anonymous:1985:DEA


Anonymous:1987:EVE


Anonymous:1988:EVE


Anonymous:1988:ERH


Anonymous:1989:SZS


Anonymous:1990:SEL


Anonymous:1991:ESS


Anonymous:1991:FFL

REFERENCES


[Ano93f] Anonymous. FIPS 180, Secure Hash Standard. NIST,
REFERENCES


[Ano93k] 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:KEE


Anonymous:1994:Lba


Anonymous:1994:Li


Anonymous:1994:PRP

Anonymous. Product review: Pretty Good Privacy is a privacy advocate’s plan to head off the government’s bid to snoop on data. Open Systems Today, 162:56–??, October 1994. ISSN 1061-0839.

Anonymous:1994:Uc


Anonymous:1994:WAS


Anonymous:1995:AUC


Anonymous:1995:AUM


Anonymous:1995: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.
REFERENCES

Anonymous:1995:ARLa


Anonymous:1995:ARLb


Anonymous:1995:ARD


Anonymous:1995:ENAa


Anonymous:1995:ENb


Anonymous:1995:FSH


Anonymous:1995:NIX


Anonymous:1995:OIN


Anonymous:1995:PTN

REFERENCES

Anonymous:1995:RLM

Anonymous:1995:SUE

Anonymous:1996:NIS

Anonymous:1996:RF

Anonymous:1996:ADX

Anonymous:1996:BCU

Anonymous:1996:CID

Anonymous:1996:CPD

Anonymous:1996:ENa
Anonymous. Editor’s note. CryptoBytes, 2(1):
REFERENCES


Anonymous:1996:ENb


Anonymous:1996:ECC


Anonymous:1996:SCG


Anonymous:1996:SUS


Anonymous:1996:TBAa


Anonymous:1996:TBSa


Anonymous:1997:RDSa

REFERENCES

[Ano97b]

[Ano97c]

[Ano97d]

[Ano97e]
Anonymous. Announcements: In this issue: The RSA Data Security Factoring Challenge; the RSA

[Ano97f]

[Ano97g]

[Ano97h]

[Ano97i]
Anonymous:1997:DNH


Anonymous:1997:ENa


Anonymous:1997:ENb


Anonymous:1997:ENC


Anonymous:1997:EW


Anonymous:1997:HEW


Anonymous:1997:INI


Anonymous:1997:MNL

REFERENCES

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

Anonymous:1997:RCU


Anonymous:1997:RAJ


Anonymous:1997:RDL


Anonymous:1997:RDSb


Anonymous:1997:SFR


Anonymous:1997:SUE

Anonymous. Standards update: Extensive revisions to PKCS underway; P1363 work continues. CryptoBytes, 3(1):
REFERENCES


Anonymous:1997:SUR

Anonymous:1997:CBP

Anonymous:1997:UPP

Anonymous:1998:ARD

Anonymous:1998:CSIb
Anonymous:1998:ICS


Anonymous:1998:EN


Anonymous:1998:Ea


Anonymous:1998:PCA


Anonymous:1998:SIB


Anonymous:1998:SIC

[Ano98h] 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: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 Obijway 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
Anonymous:1999:SFU


ANSI:1997:AXP


Anderson:1998:CCA


Abbott:1993:INT

Abreu:1994:DAI


Anderson:1998:LS


Andrasiu:1993:LTP


Aruliah:1985:PIE


Allen:1997:PSA


Aumann:1998:AES

REFERENCES


[ARRW99] Leonard M. Adleman, Paul W. K. Rothemund, Sam


Araki:1998:OEC
CODEN LNCS-D9. ISSN 0302-9743 (print), 1611-3349 (electronic).

USENIX:1988:CSSb

Asokan:1998:OFE

Abdalla:1999:TMB

Atkins:1996:RPM

Akl:1983:CSP

Ateniese:1999:SOI
REFERENCES


REFERENCES


REFERENCES

the 12th Systems Administration Conference (LISA '98) December 6–11, 1998 [AW99]
Boston, Massachusetts, USA.


REFERENCES


REFERENCES


Bakker:1999:MAS


Ball:1997:ESS


Ball:1999:WSB


Bullitt:1999:GDI


Bamford:1982:PPR


Bamforth:1997:JSS


Burrows:1989:LAb


Burrows:1989:LAa

REFERENCES


Banisar:1993:BCE


Banisar:1994:CPS


Banisar:1994:IRL


Bao:1994:IRL


Barker:1961:CSC


E. Tuttle Co., Rutland, VT, USA, 1961. x + 1 + 140 pp. LCCN Z103 Z32.

Barker:1975:CSS


Barker:1977:CHC


Barker:1979:CEC


Barker:1979:HCCb

[Bar79b] Wayne G. Barker, editor. The history of codes and ciphers in the United States during the period between the World Wars, volume 22,

Barker:1979:HCCa


Barker:1984:CSG


Barrett:1987:IRS


Barker:1991:IAD


Barker:1992:CSC


Barlow:1992:DPP

REFERENCES


Barlow:1993:EFA


Barlow:1993:EFP


Barlow:1994:NSI


Barker:1995:CDT


Barlas:1996:NKD


Barron:1996:RTR

REFERENCES

[Barias:1997:NBP]

[Barnes:1999:ESJ]

[Barron:2005:DWP]

[Baskerville:1993:ISS]

[Bastian:1995:CCE]

Lawrence E. Bassham III. Efficiency testing of ANSI C implementations of Round1 candidate algorithms for the Advanced Encryption Standard. In National Institute of Standards and Technology [Nat98], page 30. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/ r1-ansic.pdf. See [RD99a] for a conference overview. 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.
REFERENCES


REFERENCES


**Bennett:1989:EQC**  

**Ben-Aroya:1994:DCL**  

**Biham:1995:HSU**  

**Biham:1995:IDA**  

**Blaze:1995:SLE**  

**Baum:1981:RPC**  
Werner A. Baum, David H. Brandin, R. Creighton Buck, George I. Davida, George Handelman, Martin E. Hellman, Ira Michael Heyman, Wilfred Kaplan, and Daniel C. Schwartz. Report of the Public Cryptography Study Group, pre-

[Bennett:1991:EQC]

[Barni:1998:MPI]

[Blakley:1993:TSD]

[Blakley:1993:TPD]

[Bennett:1995:GPA]
REFERENCES


tion with the University of Saragossa.


REFERENCES

[BBP95a]

[BBP95b]

[BBS98a]

[BBS98b]

[BBS99a]

[BBS99b]
E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. Lecture Notes in Computer Science,
REFERENCES

Biham:1999:MMA


Biehl:1994:CPB


Blakley:1985:ACP


Beimel:1993:UIS

[BC93a] Amos Beimel and Benny Chor. Universally ideal secret sharing schemes (pre-
REFERENCES


Bos:1993:PUS


Beguin:1995:GSC


Beimel:1995:SSP


Blundo:1995:SRB


Blundo:1996:BES


Brassard:1996:YQC


Blakley:1998:C

G. R. Blakley and D. Chaum. Crypto ‘84. Lecture Notes
REFERENCES


Burwick:1998:MCC


Barker:1988:ECT


Bigun:1997:AVB


Blair:1999:DRA


Baritaud:1993:SPK


Brucoli:1999:DHC

[BCG99] Michele Brucoli, Donato Cafagna, Leonarda Carn-


REFERENCES


REFERENCES

150


**Bergadano:1998:HDC**

**Berbecel:1997:MTW**

**Birnbaum:1986:VPS**

**Borucki:1974:MNN**

**Brickell:1990:CIS**
Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes (extended abstract). *Lecture Notes in Computer Science,*
REFERENCES


Burmester:1991:ALN
[BD91]

Bauspiess:1992:RCH
[BD92]

Brandt:1993:GPP
[BD93]
J. Brandt and I. Damgaard.


REFERENCES

Blundo:1997:LBR


Bao:1998:SSS


Blundo:1998:VCS


Bao:1999:NTM


Boneh:1999:CRP


Burmester:1992:EZK

REFERENCES

2067 (electronic). URL http://www3.oup.co.uk/computer_journal/Volume_35/Issue_01/Vol35_01.body.html#AbstractBurmester

Branwyn:1995:IRA


Blundo:1994:MSS


Bondalapati:1999:DDE


Boneh:1998:ARG


BenAyed:1999:MFP


Blundo:1999:PSS

C. Blundo, A. De Santis, and A. Giorgio Gaggia. Probability of shares in se-

**Bao:1998:MFA**


**BDGI98**

**Blundo:1993:IRS**


**BDGV93**

**Blundo:1996:IRS**


**Boneh:1999:FL**


**BDHG99a**

**Boneh:1999:FPL**


**BDHG99b**

**Bao:1997:DAT**

REFERENCES


REFERENCE


Boselaers:1997:RCH


[BDP97]

Bellare:1998:RAN


[BDPR98]

Baraani-Dastjerdi:1995:CMO


[BDPSNG95]

Baraani-Dastjerdi:1997:UCH


[BDPSNG97]

Blaze:1996:MKL

REFERENCES


REFERENCES

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

Beaver:1993:HBS

Beaver:1996:ASE

Beaver:1997:CBC

Beaver:1997:PPE

Becker:1982:EDE

Beckett:1988:IC

Beckett:1990:IAM
REFERENCES

ISBN 2-25-81941-6. 332 pp. LCCN ????


REFERENCES

Bellare:1999:POP


Bennett:1980:UWN


Bennett:1989:UMS


Benario:1998:TSU


Benedens:1999:GBW


Bertrand:1973:EOP


Berstis:1980:SPD


Bertrand:1983:EGE


Berkovits:1991:HBS

REFERENCES


REFERENCES

Bergmann:2009:DKR


Beth:1983:CPW


Beth:1998:Ea


Beutelspacher:1994:CIA

Albrecht Beutelspacher. *Cryptography: an introduction to the art and science of enciphering, encrypting, concealing, hiding, and safeguarding described without any arcane skullduggery but not without cunning wagglery for the delectation and instruction of the general public*. Spectrum series.
Mathematical Association of America, Washington, DC, USA, 1994. ISBN 0-88385-504-6. xvi + 156 pp. LCCN Z 103 B4813 1994. Cryptology was originally published in German by Vieweg. This edition has been extensively revised.

**References**


REFERENCES

Boneh:19xx:

Blaze:1999:KTM

Blum:1988:NIZ

Blaze:1998:PSS

Blaze:1998:FTR

[BFM88]
Blum:1988:NIZ

[BFN98a]

[BFN98b]
REFERENCES


Blundo:1998:GBC


Busch:1999:DWC


Blum:1985:EPP


Bellare:1990:NPD

REFERENCES

Bellare:1993:DPK


Baldwin:1998:PPR


Boyapati:1999:KSD


Bellare:1994:ICC


Bellare:1995:ICA


Bird:1991:SDT

REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES

Bellare:1998:MTF


Bellare:1998:MOT


Brassard:1998:QCH


Bertilsson:1993:CPS


Bao:1994:RAF


Bao:1995:BFA


Breitbach:1999:CCM

Markus Breitbach and Hideki Imai. On channel capacity and modulation of watermarks in digital still...

**Bar-Ilan:1989:NFC**


**Biermann:1998:HKB**


**Biham:1991:CCC**


**Biham:1992:DCI**


**Biham:1994:NTC**


**Biham:1994:MOA**


**Biham:1995:CMM**

E. Biham. Cryptanalysis of multiple modes of operation. *Lecture Notes


[Bih96] Eli Biham. Cryptanalysis of triple modes of operation. Technical reports CS885, Technion, Haifa, Israel, August 1996. This is a preliminary version of [6].


[Bih98b] Eli Biham. Initial observation on Skipjack: cryptanal-


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


[Bis91] Matt Bishop. An authentication mechanism for USENET. In USENIX
REFERENCES

Association [USE91], pages 281–288. LCCN QA 76.76 O63 U84 1992.


REFERENCES


**Biham:1995:KPA**


**Blakley:1995:GPS**


**Blum:1995:DPC**


**Bocharova:1995:FEC**


**Biham:1998:CAXa**


**Biham:1998:CAXb**


**Buydos:1997:C**

Biham:1998:TA


Biryukov:1998:DCC


Biryukov:1998:ICR


Buchholz:1998:TCF


Bukher:1998:LBR


Buchholz:1998:OGO


Brown:1993:IRD

[BKPS93] Lawrence Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry. Improving resistance to differential cryptanalysis and the redesign of LOKI. Lecture Notes in Computer Science,
REFERENCES

182

739:36–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


REFERENCES


**Bla85**


**Bla93**


**Bla93**


**Bla89**


**Bla94a**


**Bla94b**


**Bla96a**

REFERENCES

Blaze:1996:HEL


Blaze:1996:OKE


Blair:1998:SEP


Bleichenbacher:1996:GES


Bleichenbacher:1997:SKP


Bleichenbacher:1998:CCA


Bleumer:1998:BYP

Barber:1999:AOD

Buldas:1998:TBL

Beth:1994:CCB

Baaz:1999:SDC

Brassil:1994:EMI

Brassil:1995:HID
[BLMO95] J. Brassil, S. Low, N. F. Maxemchuk, and L. O’Gorman. Hiding information in doc-
REFERENCES


Brickell:1983:EAA


Brickell:1984:EAA


Bloch:1998:EBUa


Bloch:1998:EBUb


Bloch:1998:EAU


Bloch:1999:FMF

REFERENCES

Brillhart:1975:NPC


Blum:1982:CFT


Blum:1983:CFT


Blum:1983:HES


Blum:1984:IUC


Blundo:1995:NDT


Blundon:1997:BCE


Bayer:1975:EST

[BM75] Rudolf Bayer and J. K. Metzger. On the encipherment of search trees and random access files. In Kerr [Ker75], page 452.
REFERENCES


Bayer:1976:EST

Blum:1982:HGC

Blum:1984:HGC

Blakley:1985:SRS
REFERENCES

sored by the International Association for Cryptologic Research.

Beale:1989:EUR


Bellare:1990:NIO


Bellare:1992:HSG


Bleichenbacher:1994:DAG

REFERENCES


Boyd:1994:DSK

Boyd:1995:DAK

Burns:1994:PSS

Bleichenbacher:1996:EOT

Bleichenbacher:1996:OTB

Bleichenbacher:1996:OTO

Brincat:1997:SC
REFERENCES

Bellare:1999:FDS


Bellare:1999:FSD


Bento:1995:RCI


Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD


Blundo:1999:RMS


Blackburn:19xx:NPP

[BMxx] Simon R. Blackburn and Sean Murphy. The number of partitions in Pollard rho. Private communication., 19xx.

Blum:1999:ERT

REFERENCES

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

**[BMP97a]**


**[BMS94]**


**[BMS96]**


**[BMRW98]**


**Bubak:1999:DHP**


**Biehl:1996:CPB**


**Barker:1998:TKL**


**Blake:1985:CLG**


**Boppana:1996:BCP**


**Busch:1999:GEI**

[BNP99] Christoph Busch, Klara Nahrstedt, and Ioannis

**Book:1985:SNP**


**Book:1985:SNS**


**Book:1985:VTA**


**Book:1985:CRE**


**Brickell:1988:CSR**


**Brickell:1992:CSR**

REFERENCES


REFERENCES


Ben-Or:1988:CTN


Bolignano:1997:TMC


Bolignano:1998:IPB


Bolignano:1998:IPM


Boneh:1998:DDP


Boneh:1998:DDH


Bond:1947:FSC


Boneh:1998:DDH

REFERENCES


<table>
<thead>
<tr>
<th>REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Borcherding:1996:LAD</strong></td>
</tr>
<tr>
<td><strong>Bosworth:1982:CCC</strong></td>
</tr>
<tr>
<td><strong>Bosma:1990:PPC</strong></td>
</tr>
<tr>
<td><strong>Bosselaers:19xx:EFH</strong></td>
</tr>
<tr>
<td><strong>Bounas:1985:DDS</strong></td>
</tr>
<tr>
<td><strong>Boucher:1994:GPA</strong></td>
</tr>
<tr>
<td><strong>Bovelander:1998:SCS</strong></td>
</tr>
<tr>
<td><strong>Bovenlander:1998:SCS</strong></td>
</tr>
<tr>
<td>E. Bovenlander. Smart card security. <em>Lecture Notes in</em></td>
</tr>
</tbody>
</table>
REFERENCES


REFERENCES

January 1989. CODEN JA-
COAH. ISSN 0004-5411.
URL http://www.acm.
org/pubs/toc/Abstracts/
0004-5411/59305.html;
http://www.imada.sdu.
dk/~joan/.

[Boy90] Colin Boyd. A new mul-
tiple key cipher and an im-
proved voting scheme. Lecture
Notes in Computer Science,
434:617–??, 1990. CODEN
LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
//link.springer-nv.com/
link/service/series/0558/
bibs/0434/04340617.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340617.

[Boy92] Colin Boyd. A form-
al framework for authentic-
tation. Lecture Notes in Com-
puter Science, 648:273–??,
ISSN 0302-9743 (print),
1611-3349 (electronic).

[Boy95a] C. Boyd, editor. Cryptog-
raphy and coding: 5th Con-
ference — December 1995,
Cirencester, number 1025
in Lecture Notes in Com-
puter Science. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 1995.
ISBN 3-540-60693-9. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN

[Boy95b] Colin Boyd, editor. Cryptog-
raphy and coding: 5th IMA
conference, Cirence-
ter, UK, December 18–20,
1995, proceedings, volume
1025 of Lecture Notes in
Computer Science. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
ISBN 3-540-60693-9. ISSN
0302-9743 (print), 1611-3349
(electronic). LCCN QA268.C76
springer-nv.com/link/
service/series/0558/tocs/
t1025.htm; http://www.
springerlink.com/openurl.
asp?genre=issue&issn=
0302-9743&volume=1025.
Papers from the 5th IMA
Conference on Cryptogra-
phy and Coding.

[Boy97] C. Boyd. Digital signa-
ture and public key cryp-
tosystem in a prime order
subgroup of $\mathbb{Z}_n^*$. Lecture
Notes in Computer Science,
1334:346–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
REFERENCES


[BP95b] Antoon Bosselaers and Bart Preneel, editors. *Integrity primitives for secure information systems: final RIPE report of RACE Integrity Primitives Evaluation (R1040)*, volume 1007 of *Lecture Notes in Com-

[Wie99]


REFERENCES


Bishr:1999:PRS


Blobel:1999:SAD


Brown:1998:LA


**Beutelspacher:1991:EFS**


**Bellare:1994:EAK**


**Bellare:1995:PSS**

REFERENCES

LCCN QA 76.6 A13 1995.
ACM order no. 508950.

RFC 2040: The RC5, RC5-CBC, RC5-CBC-pad, and
RC5-CTS algorithms, October 1996. URL ftp://
ftp.internic.net/rfc/rfc2040.txt; http://
www.math.utah.edu/pub/rfc/rfc2040.txt. Status:
INFORMATIONAL.

[BR96a] Mihir Bellare and Ronald L.
Rivest. Translucent cryptography: an alternative
to key escrow and its im-
plementation via fractional
oblivious transfer. Technical
report MIT/LCS/TR-683, Massachusetts Insti-
tute of Technology. Labora-
tory for Computer Science,
Cambridge, MA, USA,

[BR96b] Mihir Bellare and Phillip
Rogaway. The exact se-
curity of digital signatures — how to sign with RSA
and Rabin. Lecture Notes
in Computer Science, 1070:
399–??, 1996. CODEN
LNCSDD. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1070/10700399.htm;

[BR96c] M. Bellare and P. Rog-
away. On the con-
struction of variable-input-
length ciphers. In Knudsen
[Knu99c], pages 231–244.
ISBN 3-540-66226-X (soft-
cover). LCCN QA76.9.A25
F77 1999 Bar.

[BR97a] M. Bellare and P. Rog-
away. Minimizing the use of ran-
don oracles in authentic-
ted encryption schemes. Lecture Notes in
CODEN LNCSDD. ISSN
0302-9743 (print), 1611-
3349 (electronic).

[BR97b] M. Bellare and P. Ro-
away. On the construction
of variable-input-length ci-
phers. Lecture Notes in
CODEN LNCSDD. ISSN
0302-9743 (print), 1611-
3349 (electronic).

[BR99a] M. Bellare and P. Ro-
away. On the con-
struction of variable-input-
length ciphers. Lecture Notes in
Brassard:1981:TLT


Bracha:1987:ERR


Brassard:1987:IMC


Brassard:1988:MCT


Brassard:1989:CCb


Brassard:1989:CCa


Brand:1990:PNU

Russell L. Brand. Problems with the normal use of cryptography for providing security on unclassified


[Bra94a] Gilles Brassard. Cryptology column – quantum com-

Bray:1994:UA

Brackin:1995:DCP

Brassard:1995:CCB

Brassard:1995:IDR

Brackin:1996:DCP
S. H. Brackin. Deciding cryptographic protocol adequacy with HOL: The implementation. Lecture Notes in Computer Science,
REFERENCES


REFERENCES


Brickell:1990:SHI


Brickell:1992:ACC


Brickell:1998:C


Brown:1975:BL

REFERENCES

Brownell:1981:ODN


Brooke:1986:BRB


Browne:1994:ECL


Brock:1996:CCP


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB

REFERENCES


REFERENCES


Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Technical report CS91-18, Department of Applied Mathematics and Computer Science,
REFERENCES

Weizmann Institute of Science, Rehovot, Israel, October 1991. 36 pp. [BS93a]


M. Blaze and B. Schneier. [BS95a]

[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]


[Brunnstein:1995:IPR]


[Biham:1997:DFA]

REFERENCES

[Bramhill:1997:CCD]

[Boneh:1998:CSF]

[Baaleh:1999:AGA]

[Bellare:1999:NME]

[Barreiro:1997:PKC]

[Bakhtiar:1995:APL]
S. Bakhtiar and R. Safavi-Naini. Application of PVM to linear cryptanalysis. In Gray and Naghdy [GN95b],


REFERENCES

BT:1997:BEC


Barmawi:1998:AEK


Boney:1996:DWA


Buchmann:1991:NTA


Buck:1991:MCT


Budge:1922:RS


Budge:1929:RSB


REFERENCES


REFERENCES

ISSN 0268-4527 (print), 1743-9019 (electronic).


[BV98b] L. Blunk and J. Vollbrecht. RFC 2284: PPP extensi-

**Boneh:1998:BRM**


**Briguglio:1999:PGF**


**Brandes:1998:UGL**

Biryukov:1999:SA


Blake-Wilson:1999:ADH


Blake-Wilson:1999:UKS


Buchholz:1988:CQDa


Boyd:1992:RDE


Bellare:1993:CCT

REFERENCES

Beller:1993:BDK


Beller:1993:BDH


CBEMA:1981:ANS


CBEMA:1983:ANSb


CBEMA:1983:ANSa


Cachin:1995:LSS

Cachin:1995:OSS


Cachin:1998:ITM


Cypher:1996:UAS


Caelli:1996:CKE


Caelli:1996:CPF


Cain:1996:TS


Calvocoressi:1980:TSU

REFERENCES


REFERENCES


REFERENCES


Chren:1996:RDU

[CB96]

Clark:1981:ECC

[CC81]

Chen:1995:SIB

[CC95]

Canteaut:1998:NAF

[CC98]

Cai:1999:LBPa

[CC99a]

Cai:1999:LBPb

[CC99b]

Chun:1999:DMT
H. W. Chun and S. H. C. Chan. The design of a

**Chaum:1988:MUS**


**Canteaut:1999:NCA**


**Chen:1998:VIC**


**Carter:1995:DVD**


**Carlet:1998:CBF**


**Coppersmith:1985:AF**


**Chuang:1991:MER**

REFERENCES

Cramer:1995:SSS

Cramer:1996:NGS

Clark:1998:OHA

Curtin:1998:BFS
Compton:1999:PTC

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

Cramer:1999:EMC

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

Cowie:1996:WWN


Congedo:1995:SRS


Callas:1998:ROM


Chang:1995:SCP


Capocelli:1991:SSS

R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares

[Carter:1998:KSI]

[Canetti:1997:DE]

[Chen:1995:PDP]

[Cramer:1994:PPK]

[Chaum:1986:CRN]
REFERENCES


[CF88] Per Christoffersson and Vi-
REFERENCES


Chouinard:1996:ITA


Callas:1999:FUI


Ceruzzi:1991:RCK

REFERENCES


[Don Coppersmith and Edna Grossman. Generators for certain alternating groups with applications to cryptography. SIAM Journal]
REFERENCES


REFERENCES


[Chen1997AUM] Liqun Chen, Dieter Gollmann, and Chris J. Mitchell. Authentication using mini-
REFERENCES


[CH94b] Paul C. Clark and Lance J.

Cai:1996:PEA


Carrel:1997:RIO


Chang:1997:SAG


Chen:1998:PFR


Corcoran:1999:SCB


Cordon:1999:AMD

Chaum:1979:UEM

Chaum:1981:UEM

Chaum:1983:BSU

Chaum:1985:HKS

Chaum:1985:NSC
[Cha85b] David Chaum. New secret codes can prevent a computerized big brother. 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.


Chang:1986:DKL


Chapman:1986:NFS


Chapman:1990:SDA


Chang:1991:SCS

David Chaum, editor. Smart card 2000: selected papers from the Second International Smart Card 2000 Conference, Amster-
REFERENCES

Chaum:1992:AEPb


Chaum:1992:AEPa


Chaum:1993:NCB


Chambers:1994:TSC


Chaum:1995:DCS


Chaum:1998:Cb


Chandler:1994:IAF


Chabaud:1995:SSC

REFERENCES

Chadwick:1999:IWS


Chau:1999:QCE


Cheswick:1992:EBW

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

Canetti:1997:MAC


Chiopris:1992:SBE


Chin:1999:HCD

Shiu-Kai Chin. High-confidence design for security: don’t trust — verify. *Communications of


Christian:1999:DSCb


Christian:1999:SPI


Chuang:1989:NES


Currie:1996:SEL


Ciarcia:1986:BHD


Cao:1999:DTJ

Y. J. Cao, N. Ireson, L. Bull, and R. Miles. Design of a traffic junction controller using classifier system and fuzzy logic. Lecture Notes in Computer Sci-
REFERENCES


Clark:1995:SRP


Chabaud:1998:DCS


Collins:1999:DCL


Coster:1992:ILD


Coppersmith:1995:TCB


Coppersmith:1996:PMT


Charlwood:1998:EXA

REFERENCES

LCNSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


Chari:1999:TSA


Chari:1999:CNR


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.

Chee:1991:CNP


Chor:1990:SSI


REFERENCES


Cox:1997:SSS


Caldwell:1999:DIF


Coradeschi:1999:IVD


Chan:1988:IEC


Chang:1997:PCM


Cox:1997:PWR

REFERENCES

Cox:1998:SGM


Claudy:1912:TMS


Clapp:1997:OFS


Clapp:1998:JHS


Clarke:1998:BP

REFERENCES


[Clinton:1999:LPM] 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

**Chua:1999:ART**


**Cheng:1998:MVR**


**Culik:1979:SIS**


**Ciampi:1982:EVS**


**Chan:1985:NMP**

REFERENCES

Cachin:1995:LIR

Cachin:1997:USA

Chang:1997:CAS

Cooperman:1997:SMD

Cox:1997:RW1

Chen:1998:DRT

Camenisch:1999:SEG
Charlton:1999:DPM


Christianson:1999:DSCa


Coradeschi:1999:HMC


Chen:1998:SCC


Cohen:1993:AAA

REFERENCES

Canetti:1999:ECS

Charnes:1997:SSH

Chor:1989:SCT

Chuan-Ming:1994:RTR

Craver:1997:CIW

Craver:1998:RRO
REFERENCES


Crilly:1987:BPB


Coron:1999:SRSb


Coron:1999:SRP


Coupe:1999:ELA


Chao:1998:CSE

Coltell:1998:AOL


Cocks:1997:SKG


Cohen:1987:IIP


Cohen:1994:SCC


Cohen:1996:RRA


Colaco:1864:CRO

F. N. Colaço. A criptographia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quases quer que sejam os caracteres empregados. (Portuguese) [Cryptography revealed, or, the art of translating and deciphering obscure writings, whatever the characters employed]. De Santos e Cia, Pernambuco, Brazil, 1864. 93 pp. LCCN Z104.C68 1846.

Cominsky:1987:CAP


Comba:1990:ECI

REFERENCES


Conradi:1739:CDS

Conklin:1998:SCO

Conklin:1999:ESC

Contini:1999:DPD

Coombs:1983:MC

Coppersmith:1984:FEL

Coppersmith:1987:C
[Cop87] D. Coppersmith. Cryptography. IBM Journal of Re-
REFERENCES

Coppersmith:1989:AID


Coppersmith:1994:DES


Coppersmith:1994:ACS


Coppersmith:1995:AAC


Coppersmith:1995:FSR

D. Coppersmith. Finding a small root of a univariate modular equation. IBM
REFERENCES


Coppersmith:1995:ACC

Coppersmith:1998:C

Coppersmith:1999:WQS

Corcoran:1998:MFS

Coron:1999:SRSa

Coppersmith:1986:DL
Courville:1986:MCC


Courington:1993:PEA


Coutinho:1999:MCN


Cremonini:1999:CCA


Chaum:1987:ACE


Chaum:1988:ACE

Sponsored by the International Association for Cryptologic Research.

Camion:1991:KHF


Chaum:1993:WDO


Chae:1994:AMA


Chen:1995:NGS


Chaum:1998:E


Chung:1998:DWCa


Charney:1997:PSC


Cheon:1998:TEA

[CPPK98] Jung Hee Cheon, S. M. Park, S. W. Park, and D. Kim. Two efficient algorithms for arithmetic of


REFERENCES


REFERENCES

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


REFERENCES


[Cus95] Thomas W. Cusick. Cryptanalysis of a public key

**REFERENCES**


REFERENCES

http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760470.htm;

Chang:1991:BCC


Cusick:1991:RIC


Campbell:1993:G

K. W. Campbell and M. J. Wiener. DES is not a group.

Chang:1997:SCO


Chmora:1994:ECC


Chang:1997:SCO
Ceruzzi:1991:RGC

Coppersmith:1998:CT

Chang:1998:BSC

Craver:1998:TTL

Cao:1990:DKC
REFERENCES

DeMillo:1983:ACC


Dittmann:1998:MSW


D’Agapeyeff:1939:CC


D’A71


Daemen:1995:HFC


Daemen:1998:MSK


Daemen:1999:RAI

REFERENCES


REFERENCES


H. Danisch. RFC 1824: The Exponential Security
REFERENCES


[Danthine:1996:ECM]

[Dang:1997:AAC]

[Darnell:1997:CCI]

[Davida:1981:CAR]
George I. Davida. The case against restraints on non-governmental research in cryptography. Communications of the Association for Computing Machinery, 24(7):445–450, July 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is an opposing view published with [Ame81].

[Davies:1985:MAA]
Donald Watts Davies. A message authenticator algorithm suitable for a mainframe computer. In Blakley and Chaum [BC85], pages 393–400. CODEN LNCSD9. ISBN 0-
REFERENCES


cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.


REFERENCES

**denBoer:1988:CF**

**Denning:1989:EET**

**denBoer:1991:ALT**

**denBoer:1994:CCF**

**Denning:1996:TKE**

**Daswani:1999:EEC**
N. Daswani and D. Boneh. Experimenting with elec-
REFERENCES


[dBB91] [DBGV93] [DBVD96] [dC86] [DBP96]


REFERENCES

URL http://link.springer-ny.com/link/service/series/0558/tocs/t0218.htm;


[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; unscrambling 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/.


[DDJ98f] DDJ Staff. News and views: New trends in vaporware; distance ed might pay off; life in the fast lane; making friends in Washington; news on OpenGL 1.2; no discounts for schools; let’s
REFERENCES


DDJStaff:1998:NVc

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:1999:NVR


DePaoli:1998:WBS


Denny:1994:FR


DDJ99

[DDJ98g]

[DDJ98h]

[DDLM94]
REFERENCES


Davida:1990:KDS


DeSantis:1994:SSP


DeSantis:1994:KCQ


DeSantis:1999:NIZ


Darmstaedter:1998:LCS


REFERENCES


[Dea87]

DeSmit:1998:GAE


[Dea88]

DeMoliner:1999:STB


[Dea98a]

Deavours:1987:CPI


[Dea87]

Deavours:1988:BPS


[Dea88]

Deavours:1998:A


[Kruh:1998:TBW]

REFERENCES

lected papers from issues of Cryptologia.


Denniston:1986:GCC


Denning:1990:DES


Denning:1995:ESC

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

Denning:1999:IWS


Deswarte:1992:CSE


Desmedt:1988:SGC


Desmedt:1990:PAA

Yvo Desmedt. Protecting against abuses of cryptosystems in particular in the context of verification of peace treaties (extended

**Desmedt:1990:MCS**


**Desmedt:1992:BTC**


**Desmedt:1993:TC**


**Desmedt:1994:BTC**


**Desmedt:1995:STC**


Dwight Deugo. Coffee talk: From S390 mainframes to


References


[DFGH99] V. Deshpande, L. Fornasier, E. A. Gertiesen, and N. Hilbrink. Virtual engineering of multi-disciplinary applications and the significance of seamless accessibility of geometry data.

REFERENCES

Lecture Notes in Computer Science, 1593:702–??, 1999. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).


DiCrescenzo:1999:HFS


Donatini:1999:DES


Dwork:1993:LCP


Davida:1997:ACC


J. Daemen, R. Govaerts, and J. Vandewalle. A new

Daemen:1994:RWS


Daemen:1994:WKI


Diffie:1976:NDC


Diffie:1977:ECN


Davis:1985:NRI


Davis:1985:UFS

Association for Cryptologic Research.

**DomingoFerrer:1990:FSK**


**Dawson:1996:AAS**


**Ding:1996:WKA**


**Dhem:1998:DEP**


**Diffie:1980:CAM**


**Dechamboux:1996:ADS**


**Desmedt:1998:AOC**

References


Whitfield Diffie. The adolescence of public-key cryptography (invited). Lecture Notes in Computer Sci-
REFERENCES

ence, 434:2–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


Davis:1994:CRA


Ding:1994:DCD


Dixon:1994:SSS


Damm:1998:CRT


Dessmark:1993:MDD


Deavours:1985:MCM

REFERENCES


Deavours:1987:CYT


Daemen:1997:BCSa


Dodson:1995:NFL

[DL95] B. Dodson and A. K. Lenstra. NFS with four large primes: An explosive experiment. In Cop-

Demphlous:1999:DPL

Davoine:1997:VCP

DeMillo:1982:CP

Damgaard:1993:ACE

Ding:1997:LMS

delaStelle:1902:TCF

DeMillo:1983:PDS
UK/~FAPP2/STEGANOGRAPHY/BIBLIOGRAPHY/1004.html.

Duc:1997:PAF


DeWin:1998:PSS


Denning:1981:MMK


Dongarra:1995:TSS


Denazis:1999:DIO


D’Angelo:1994:SEM


Dwork:1993:PPC


Dwork:1994:EEU

[DN94] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signa-

Dossis:1995:FSR


Dossis:1995:OVH


Desmedt:1986:CTA


DiCrescenzo:1999:CZK


Dobbertin:1995:EMC


Dobbertin:1995:ASA


Dobbertin:1996:CM


Dobbertin:1998:FTR

H. Dobbertin. The first two rounds of MD4 are not one-way. In Vaudenay [Vau98e], page ?? CODEN LNCSD9. ISBN 3-540-64265-X (paperback). ISSN
REFERENCES


**[DP96]**

**[DP99]**

**[DQ93]**

**[DP98a]**

**[DP98b]**

**[DP98c]**

**[Des99]**


Desmedt:1985:DOI


[Desmedt:1985:DOI]

Desel:1994:PNR


deRooij:1994:SPD


[Desel:1994:PNR]

deRooij:1995:EEU

Peter de Rooij. Efficient exponentiation using precom-

[Daemen:1998:APR]


[Desel:1998:PTP]


[Daemen:1999:EBC]


[Drea:1999:NEB]


[Dray:1998:RNJ]


[Drach:1999:RDO]

REFERENCES


1983. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).


REFERENCES

Dutertre:1997:UPE

David:1998:SIC

Dwork:1998:CZR

Dwight:1999:BOO
George B. Durham, Dioditis Spinellis, and Mariá Bieliková. Bookshelf: Object-oriented software design and construction with C++: Decrypted secrets: Methods and max-
REFERENCES


Mark S. Dufner. Applications of cryptology in high school mathematics. Thesis (M.A.), Minot State University, 500 University Ave.

**Duhoux:1990:DBA**


**Dumey:1994:CQD**


**deVivo:1998:ISA**


**DeDecker:1992:HID**


**Dhem:1996:SSC**


**DeSoete:1990:CAS**

REFERENCES


[Diffie:1992:AAK]


[Danielssson:1998:HKW]

[Davida:1981:DES]

[Dwork:1991:VSS]

[Dwork:1995:DCC]

[Dwork:1997:PAL]
REFERENCES


[DeSantis:1991:CAN]

[DeSantis:1991:DPSa]


[Desmedt:1991:WUS]


[Desmedt:1991:AUS]

Yvo Desmedt and Moti Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks (extended abstract). *Lecture Notes in Computer Science*, 537:177–??, 1991. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic). URL http:/
lk.springer-ny.com/
link/service/series/0558/
bibs/0537/05370177.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0537/05370177.
pdf.


[ECM96] ECMA. ECMA-219: Authentication and Privilege
REFERENCES


**Ellis:1975:PKC**


**Epstein:1956:FBC**


**El-Gamal:1985:PCS**


**Even:1985:PCC**


**Even:1985:RPS**

REFERENCES


REFERENCES

0558/papers/1592/15920140.pdf

**Estrella:1999:DED**


**Eigenthaler:1984:CGA**


**Evans:1974:UAS**


**EFF:1998:CSE**


**EPIC:1999:CLI**


**ElGamal:1985:PKCa**

(print), 1557-9654 (electronic).


Eades:1998:GDC


Ehrsam:1978:CKM


Ezawa:1998:ATS


Endler:1997:PSU

David Endler. PGP: a simple usage guide. Sys


Enge:1999:ECT


Ezawa:1999:AEC


Eng:1995:SDE


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.

Erickson:1999:EAS


Erskine:1999:CDD


Emerald:1997:NPC


Effelsberg:1998:SAI

Wolfgang Effelsberg and Brian C. Smith, editors.

Escott:1999:AEC


Estell:1980:BW


Ettinger:1998:SGE


Evertse:1992:WNR


Even:1985:CSW


Evertse:1991:WNR

REFERENCES


**Ford:1997:SEC**


**Fox:1997:GGU**


**Fridrich:1998:RDW**


**Fenn:1996:MDD**


**Ferland:1994:PBC**


**Firoiu:1999:LER**


**FontdecabaBaig:1998:PNL**

E. Fontdecaba Baig, J. M. Cela Espin, and J. C. Duersteler Lopez. On

Fan:1999:DFS


Fan:1992:PRT


Frankel:1993:NEH


Frankel:1993:NHG


Feak:1983:SIS


Feistel:1973:CCP


Feigenbaum:1991:ACC


Feit:1993:TIA


Feit:1996:TIA


Feigenbaum:1998:C


Feige:1999:NSP


Feldman:1987:PSN


Feige:1999:NSP

REFERENCES


REFERENCES


[FGR92] Joan Feigenbaum, Eric (print), 1611-3349 (electronic).


REFERENCES


Farmer:1996:SMA


Frankel:1996:WCP


Frankel:1996:WBC


Friedman:1974:ETR


Franklin:1994:JEM


Franks:1997:REH

J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, and L. Stewart. RFC 2069: An extension to HTTP: Digest access authentication,
REFERENCES


Filby:1977:TPT


Filby:1978:BRM


Filby:1995:FUB


FIPS:1993:APG


FIPS:1993:SHS


FIPS:1994:EES


Fischlin:1997:ICM


Fischlin:1998:CLP

M. Fischlin. Cryptographic limitations on parallelizing membership and equivalence queries with applications to random self-


REFERENCES

CODEN LNCS99. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fellows:1993:FPC


Fellows:1994:CCG


Franke:1999:SDM


Freier:1996:SPV


Frankel:1998:BIW


Fumy:1993:PCK

REFERENCES


REFERENCES


Faihe:1998:ADR

[FM98a]

[FM98b]

Feustel:1998:DUI

[FM98b]

Fairfield:1985:LRN

[FM85]

Faihe:1998:ADR

[FM98a]

Feustel:1998:DUI

[FM98b]

Fairfield:1985:LRN

[FM85]
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.

Fagundes:1999:EGA


Frey:1999:TPD


Frankel:1998:RED


Fiat:1994:BE

Amos Fiat and Moni Naor. Broadcast encryption. Lecture Notes in Computer Science, 773:480–??, 1994. CODEN LNCSD9. ISSN 0302-


integration of asymmetric and symmetric encryption schemes. In Wiener
Bar. URL http://link.
springer-ny.com/link/
service/series/0558/bibs/
1666/16660537.htm; http://
link.springer-ny.com/
link/service/series/0558/
papers/1666/16660537.

Folmsbee:1999:AJT

Alan Folmsbee. AES Java
technology comparisons.
In National Institute of
Standards and Technology
Nat99b], page 28. ISBN
???? LCCN ???? URL
http://csrc.nist.gov/
encryption/aes/round1/
conf2/Folmsbee.pdf. Only
the slides for the conference
talk are available.

Fujioka:1991:EED

[FOO91] A. Fujioka, T. Okamoto,
and K. Ohta. Interactive
bi-proof systems and un-
deniable signature schemes.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Fujioka:1993:PSV

[FOO93] A. Fujioka, T. Okamoto,
and K. Ohta. A practical
secret voting scheme for
large scale elections.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Forte:1999:BUT

Dario Forte. Biometrics:
Untruths and the truth.
;lo-
gin: the USENIX Asso-
ciation newsletter, 24(2):
??, April 1999. CODEN
LOGNEM. ISSN 1044-
6397. URL http://www.
usenix.org/publications/
login/1999-4/biometrics.
.html.

Foster:1982:CM

Caxton C. Foster. Crypt-
analysis for microcompu-
ters. Hayden Book Co.,
Rochelle Park, NJ, USA,
REFERENCES


Franksen:1984:MBS


Franklin:1985:MID


Franksen:1985:MBS


Franksen:1986:SHM


Frankel:1989:TIC


Frankel:1990:PPL


Francis:1992:PSG


Franksen:1993:BCM


Franklin:1999:FCT

Matthew Franklin, editor. Financial cryptogra-
REFERENCES


Freund:1994:KED

Friedman:1935:ICA

Friedman:1935:MCP

Friedman:1935:PIS

Friedman:1939:CAC
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 ???

Friedman:1939:MC

Friedman:1941:MCP
REFERENCES


REFERENCES


REFERENCES


**Ferguson:1997:CA**


**Fischlin:1997:SSP**


**Forsyth:1993:ACS**


**Figueroa:1994:FCB**


**Federrath:1995:SVA**


**Fiat:1999:DTT**

A. Fiat and T. Tassa. Dynamic traitor tracing. In


Fumy:1997:ACE


Fumy:1998:E


Fumy:1998:ISP

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


ican Cryptogram Association (George C. Lamb Collection).


REFERENCES


James M. Galvin. Public key distribution with se-


Martin Gardner. Mathematical games: A new kind of cipher that would take millions of years to break. Scientific American, 237
REFERENCES


REFERENCES


Garber:1998:NBM


Garber:1998:NBS


Garfinkel:1998:PPG


Gaudin:1997:VBJ

Sharon Gaudin. Visa boosts Java’s credit line: smart cards will redefine how plastic is used. Computerworld, 31(31):1, 16, August 4, 1997. CODEN CMP-WAB. ISSN 0010-4841.

Gilmour-Bryson:1982:CDT

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 K662.14 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.”.

Forouzan Golshani and Robin Baldwin. In the news: Digital-watermarking faces challenges; virtual human agents evolve; vendors urge, give SET a chance; radio on the net; media notes. *IEEE MultiMedia*, 5(3):6–9, July–September 1998. CO-


Dieter Gollmann and William G. Chambers. A

Gilbert:1991:SAF

Henry Gilbert and Guy Chassé. A statistical attack of the FEAL-8 cryp-

Gilbert:1994:CPA


Garber:1997:NBJ


Gershenfeld:1998:QCM

Girault:1988:GBA

Goffin:1997:LCP

Goldburg:1991:ACA

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].

Gehrmann:1994:CGN

Gehrmann:1995:SMA
REFERENCES

0558/papers/0921/09210158.


REFERENCES

tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
/www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&page=276. 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.

Goldreich:1986:HCR

Oded Goldreich, Shafi
Goldwasser, and Silvio
Micali. How to con-
struct random functions.
Journal of the Associa-
tion for Computing Machin-
ery, 33(4):792–807, Octo-
ber 1986. CODEN JA-
COAH. ISSN 0004-5411.
URL http://www.acm.
.org/pubs/toc/Abstracts/
0004-5411/6503.html. A
computational complexity
measure of the randomness
of functions is introduced,
and, assuming the exis-
tence of one-way functions,
a pseudo-random function
generator is presented.

Gabber:1997:HMP

E. Gabber, P. B. Gibbons,
Y. Matias, and A. Mayer.
How to make personalized
Web browsing simple, se-
cure, and anonymous. In

Hirschfeld [Hir97], pages
ISBN 3-540-63594-7. ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
HG1710 .F35 1997. URL
http://www.cl.cam.ac.
.uk/"fapp2/steganography/|
bibliography/071123.html |

Gilbert:1998:ASR

Henri Gilbert, Dipankar
Gupta, Andrew Odlyzko,
and Jean-Jacques Quisquater.
Attacks on Shamir’s ‘RSA
for paranoids’. Informa-
tion Processing Letters,
68(4):197–199, November
30, 1998. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
research.att.com/"amo/
doc/rsa.for paranoids.
pdf; http://www.research.
att.com/"amo/doc/rsa.
for paranoids.ps; http://
www.research.att.com/ 
"amo/doc/rsa.for paranoids.
tex

Gittler:1995:DSS

Frederic Gittler and Anne C.
Hopkins. The DCE secu-
{

rit y service. Hewlett-Pack-
{ard Journal: technical in-
nformation from the labo-
ratories of Hewlett-Pack-
{ard Company, 46(6):41–48,
December 1995. CODEN
HPJOAX. ISSN 0018-1153.
URL http://www.hp.com/ 
hpj/95dec/dec95_41.pdf;
REFERENCES


Gehrke:1996:MPK

Gong:1999:PKC

Gennaro:1999:SHS

Gopalakrishnan:1993:NCC

Galil:1990:SPK

Gilboa:1999:CCR

Gibson:1990:SCD
J. K. Gibson. Some comments on Damgård’s hashing principle. Electronics

Gibson:1991:EGC


Gibson:1995:SDG


Gibson:1996:SGP


Gifford:1981:CSI


Gilder:1997:APD


Giles:1998:EFS


Gilboa:1999:TPR

REFERENCES


REFERENCES

Gifford:1982:CSI


Gennaro:1996:RTD


Gennaro:1996:RES


Gennaro:1999:SDK


Gennaro:1999:RES


Garay:1999:AFO

REFERENCES

LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Garay:1999:AOC


Goresky:1995:FRB


Gurses:1995:VCT


Goldreich:1996:CZP


Goldschlag:1999:BCC


Goldwasser:1999:PTU

Gennaro:1997:RBU


Gotz:1997:DTC


Gligor:1979:OMA


Goldreich:1989:HCP


Gaskell:1996:ISC


Gladman:1999:IEA

Brian Gladman. Implementation experience with AES candidate algorithms. In National Institute of Standards and Technology...

Gleason:1986:ECP


Gleason:1987:PIC


References


REFERENCES


M. Grohe and J. Mariño. Definability and descriptive

Galvin:1995:RSM


Griwodz:1998:PVE


Ghazi-Moghaddam:1994:OCH


Goldwasser:1985:PSS


Goldwasser:1988:DSS


[GMW91] 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 JA-COAH. 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.”.


[GN94] Peter Gemmell and Moni Naor. Codes for interactive authentication. *Lecture Notes in Computer Sci-


system. In USENIX Association [USE90], pages 1–4. LCCN QA 76.9 A25 U55 1990.

Goldwasser:1990:ACC

Goldwasser:1990:SPS

Goldmann:1992:ATC

Goldmann:1994:CCC

Goldreich:1995:FCF

Golic:1995:LCS

Golic:1996:FLO
J. D. Golic. Fast low order approximation of cryptographic functions. Lecture
REFERENCES

Golic:1996:CEP


Gollmann:1996:CA


Gollmann:1996:FSE


Goldreich:1997:FMCa


Goldreich:1997:FMCb


Goldwasser:1997:NDC

S. Goldwasser. New directions in cryptography: twenty some years later (or cryptography and complexity theory: a match made in heaven). In

[Golic:1997:CAA]


Goldwasser:1998:C


Golic:1998:RAS


Goldreich:1999:MCP


Golic:1999:SCE


Golomb:1999:CNS


Gong:1989:SCB


Gong:1992:SRD

Li Gong. A security risk of depending on synchronized...

**Gong:1995:CKH**


**Gong:1998:JSM**


**Good:1979:EWC**


**Goodman:1996:LPS**


**Gordon:1985:SPE**


**Gordon:1993:DDT**

(print), 1611-3349 (electronic).

Gordon:1993:DLU


Goth:1999:NBG


Guajardo:1997:EAE


Ghodosi:1996:CHG


Ghodosi:1999:RCN


Ghodosi:1999:RCN


Gladychev:1998:CRJa


Gladychev:1998:CRJb

Pavel Gladychev, Ahmed Patel, and Donal O’Mahony.
REFERENCES


Goldreich:1998:SCP


Goldreich:1997:RMA


Ghodosi:1998:SSM


Ghodosi:1998:CCS


Gore:1998:SDC


Gabidulin:1991:INC

E. M. Gabidulin, A. V. Paramonov, and O. V.


[QW+91] Louis C. Guillou, Jean-Jacques Quisquater, Mike Walker, Peter Landrock, and Caroline Shaer. Precautions taken against various potential attacks in ISO/
REFERENCES


REFERENCES


REFERENCES

**Grollmann:1988:_CMP**
CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

**Girault:1994:LCH**

**Gulliver:1994:ITA**

**Gritzalis:1997:CPO**

**Gong:1998:SSG**
L. Gong and R. Schemers.

**Gribomont:1999:SDU**


**Gysin:1999:GCA**


**Gafni:1999:EMI**


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.

Gudes:1980:DCB


Guenther:1998:E


Guergens:1998:SLF


Guillichsen:1983:BHS


Gunther:1988:ASG


Gunther:1988:ACE


REFERENCES

Guy:1976:HFN


Gao:1998:GPO


Griffiths:1976:AMR


Goldberg:1996:RNB

[GW96] Ian Goldberg and David Wagner. Randomness and the Netscape browser. Dr.


Gao:1999:RDF


Gamow:1958:CAP


Galil:1987:PEA


Gylden:1931:CEI

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Volume</th>
<th>Pages</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gylden:1936:AMC</td>
<td>Yves Gylden. Analysis of model C-36 cryptograph from the viewpoint of cryptanalysis.</td>
<td></td>
<td>22</td>
<td>1936</td>
</tr>
<tr>
<td>Gylden:1938:APV</td>
<td>Yves Gylden. Analysis from the point of view of cryptanalysis of “cryptograph type C-36,” provided with six key wheels, 27 slide bars, the latter having movable projections, single or multiple.</td>
<td></td>
<td>10</td>
<td>1938</td>
</tr>
</tbody>
</table>
REFERENCES

0272-1732 (print), 1937-4143 (electronic).

Haddon:1984:BRS


Hagelin:1998:SHC


Hoffman:1994:CP


Hammer:1971:SSC


Hamming:1980:CIT


Hamming:1986:CIT


Hamilton:19xx:PC

[Hanxx] V. Hamilton. Personal communication. ???, 19xx.

Hansen:1994:MLD

[Han94] Per Brinch Hansen. Multiple-length division revisited: a tour of the minefield.
REFERENCES

Software—Practice and Experience, 24(6):579–601, June 1994. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). This paper derives an algorithm for division of long integers, and implements it as a literate program, although without identifier cross-references.

Hardjono:1990:RED


Harari:1991:CCS


Hart:1994:DSC


Harpes:1996:CIB


Harris:1996:E


Haskett:1984:PAU


Haastad:1987:OWP

Haastad:1988:SSM


Haselberger:1995:DRB


Hasan:1999:LTB


Hatefi:1996:MRE


Hatefi:1997:AED


Hawkes:1998:DWK


REFERENCES


Heidel:1676:JTP

REFERENCES

13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM80, Mei81].


REFERENCES


[John M. Hardy, Dorothy W. Fuller, Douglas R. Long, Jane C. Hartin, and Faye Davis. Electronic cryptographic communications equipment specialist (AFSC 30650). Extension Course
REFERENCES

Housley:1999:RIX


Hartung:1996:DWR


Hartung:1997:CPV


Hartung:1997:WME


Hartung:1997:DWM


REFERENCES


Hofmann:1994:RQC


Hughes:1998:AJC


Husemann:1999:OTY


Hutton:1999:ASM


Harn:1989:PAU


Han:1993:TCC


Han:1997:TCC

Yenjo Han, Lane A. Hemaspaanda, and Thomas Thierauf. Threshold computation and cryptographic security. SIAM Journal
REFERENCES


Hochberger:1999:CDM


Harn:1993:OTP


Hirose:1997:CKD


Higenbottam:1973:CC


Highland:1997:HCV


Highland:1997:PRC


Hill:1929:CAA


Hill:1931:CCL

Lester S. Hill. Concerning certain linear transfor-
REFERENCES


Hiltgen:1994:CRC


Hill:1997:MTY


Haastad:1999:PGO


Hinsley:1993:BIS


Hirschfeld:1993:MER


Hirschfeld:1997:FCF

Hirschfeld:1998:FCS


Hitt:1943:MSM


Helman:1999:DPE


Herzberg:1997:PPK

[HJJ+97] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public key and signature systems. In ?? ?? [???97], page ??

Herzberg:19xx:PPK


Herzberg:1995:PSS

REFERENCES


[HK97] Shai Halevi and Hugo Krawczyk. MMH: Software message authentication in the Gbit/second...

Hevia:1998:STD


Halfmann:1999:ESP


Haynes:1999:VDS


Hevia:1999:STD

Hromkovic:1994:CDC


Harpes:1995:GLC


Hachez:1999:IFA


Hall:1999:CS


Haber:1995:HDD


Hofmeister:1997:CKS


Hofmeister:1997:COS

REFERENCES

**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


tions based on block ciphers. In Stinson [Sti93b], pages 379–390. ISBN 0-387-

Hunter:1983:ERA


Hule:1988:RCW


Hafner:1991:COH

past few years. One of the co-authors is the New York Times reporter who broke the Stoll story to the public.


P. Horster, M. Michels, and H. Petersen. Meta-message recovery and meta-blind signature schemes based on

[Harkavy:1998:IPP]

[Harper:1993:PKC]

[Horvath:1994:PPM]

[Haastad:1998:SIR]
REFERENCES

puter Society Press order number PR9172.


Abstracts/0001-0782/162691.html.


REFERENCES


REFERENCES


REFERENCES

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

REFERENCES


REFERENCES

Hall:1997:REG


Helme:1997:SFF


Harasawa:1999:CMF


Hornauer:1994:MCA


Hauser:1996:MBI


Hinsley:1979:BISa


Heys:1995:ACS

REFERENCES


REFERENCES


REFERENCES


[Hartnell:1976:PFM]


[Hardy:1979:ITN]


[Huthnance:1988:UPP]


[Hotchkiss:1991:ASI]


[Hsu:1997:DWV]


[Hsu:1998:DBW]


[Hsu:1998:MWD]

Hwang:1998:AUS  

Hwang:1991:CGO  

Hwang:1992:AOT  

Hwang:1992:EIB  

Hwang:1992:PGO  

Hwang:1993:SSD  

Hwang:1997:CKA  
M.-S. Hwang. A cryptographic key assignment scheme in a hierarchy for access control. Mathematical and computer modelling,
Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE


Hall:1998:BPPa


Hall:1998:BPPb


Hohl:1994:SIH


Harn:1993:GUS

L. Harn and S. Yang. Group-oriented undeniable
signature schemes without
the assistance of a mutually trusted party. *Lecture
Notes in Computer Science*, 718:133–??, 1993. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Harn:1993:PKC]
L. Harn and S. Yang. Public-key cryptosystem
based on the discrete logarithm problem. *Lecture
Notes in Computer Science*, 718:469–??, 1993. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Hwang:1995:TPE]
Min-Shiang Hwang and Wei-Pang Yang. A two-
phase encryption scheme for enhancing database security. *The Journal of Sys-
CODEN JSSODM. ISSN 0164-1212 (print), 1873-
1228 (electronic).

[Hirose:1998:ADK]
S. Hirose and S. Yoshida. An authenticated Diffie–
Hellman key agreement protocol secure against active
attacks. *Lecture Notes in Computer Science*, 1431:
135–??, 1998. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[Hsieh:1998:H]
Tsu-Miin Hsieh, Yi-Shiung Yeh, Yung-Cheng Hsieh,
(6):317–320, June 30, 1998. CODEN IFPLAT. ISSN
0020-0255 (print), 1872-6291 (electronic).

[Hsieh:1999:OWH]
One-way hash functions with changeable parameters. *Information Sciences*,
118(1):223–239, September 1999. CODEN ISIJBC.
ISSN 0020-0255 (print), 1872-6291 (electronic).
REFERENCES


[IEE81] IEEE, editor. 6th Conference on Local Computer Networks, Hilton Inn, Minneapolis, Minnesota, October 12–14, 1981. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD
REFERENCES

IEEE:1982:ASF

IEEE:1982:CFP

IEEE:1983:PSS

IEEE:1984:ASF

IEEE:1985:FOC

IEEE:1986:CEC
IEEE. Colloquium on "Encryption for Cable and
IEEE:1986:ASF


IEEE:1987:ASF


IEEE:1987:IIG


IEEE:1987:PIS


IEEE:1988:FAC


IEEE:1989:ASF

[IEE89] IEEE, editor. *30th an-


REFERENCES

Order Plan catalog number 96TB100057.


IEEE:1997:ACS


IEEE:1997:ICD


IEEE:1997:IICb


IEEE:1997:ASF


IEEE:1997:IICa


IEEE:1997:ICI


IEEE:1997:PICa


IEEE:1997:PICb


IEEE:1997:PICc

IEEE, editor. Proceedings of 1997 International
REFERENCES


REFERENCES


H. Igarashi, S. Kosue, and M. Miyahara. Individual tactical play and pass with communication between players-team descriptions of Team Miya2. Lecture Notes in Computer Science, 1604:364–??, 1999. CODEN LNCSD9. ISSN [IKM99]
REFERENCES


REFERENCES


[IRD:1979:DVE]

[IRD:1981:DE]

[IRD:1981:DTV]

IRD:1984:DTV


IRD:1987:DTV


IRD:1988:DTV


Anonymous:1991:IIS


IRD:1991:DFV


Itoh:1994:LDS


Impagliazzo:1989:LPC


REFERENCES


Imai:1998:PKC


Imai:1999:PKC


Jaburek:1990:GGP


Jackson:1987:NTS


Jackson:1990:SITa


Jackson:1990:SITb

Keith M. Jackson. Secure information transfer:

Jackson:1996:AAC


Jakobsson:1995:BUU


Jakobsen:1999:HOC


Jakobsson:1999:MCM


Jakobsson:1999:QCA


Jamieson:1998:UEP

Lauren Jamieson. Unveiling the extraordinary possibiliti-

**Jantke:1995:RSI**


**Jancek:1999:AVR**


**Jarecki:1996:PSS**


**Jarvis:1997:GB**


**Jaspan:1996:DWE**


**Jaeger:1993:LCC**


**Jan:1998:PWP**


[Jefferson:19xx:IFC] Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Web site, 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.


REFERENCES


Jian:1999:SDM


Jolitz:1991:PUI


Jolitz:1995:RNS


Johnson:1998:ESS


Johnson:1998:CPE


Johnson:1998:SIC


Johansson:1999:FCA

T. Johansson and F. Joensson. Fast correlation attacks based on turbo code...


Jackson:1995:ESS


Jackson:1995:SMS


Jerichow:1998:RTM


Jakobsson:1996:DVP


Jarecki:1997:EMS


Michael K. Johnson. Lurk-

**Johnson:1997:SP**


**Johnson:1997:SPS**


**Jolitz:1995:PB**


**Jones:1978:WWB**


**Jones:1978:MSW**

REFERENCES


Jakobsson:1999:SAE


Jiwa:1994:BBA


Juels:1999:TTS


Juenemann:1981:DES


Jung:1987:IRC


REFERENCES


[KA99] X. D. Koutsoukos and P. J. Antsaklis. Hybrid control systems using timed Petri nets: Supervisory control...


REFERENCES

[102x681]uk/~fapp2/steganography/

bibliography/1009.html.

Kahn:1991:SER


Kahn:1991:WWW


Kahn:1996:HS

bibliography/054141.html.

Kahn:1996:CSS


Kahn:1998:EC


Kahn:1998:PHI


Kahn:1998:RMU

REFERENCES

Kak:1983:EMP


Kak:1984:MPK


Kak:1985:EEC


Koc:1996:ACM


Kaliski:1984:AWA


Kaliski:1985:WAE


Kaliski:1991:MMD

[Burt S. Kaliski Jr. The MD4 message digest al-


Kaliski:1998:EDF


Kaliski:1998:RPCa


Kaliski:1998:RPCb


Kaliski:1998:RPRa


Kaliski:1998:RPRb


Kaliski:1998:RPCb


Kaliski:1998:RPCc

REFERENCES

Kaliski:1998:REC


Kaliski:1999:ESP


Kaneshige:1996:ITC


Kaps:1998:HSF


Karger:1985:ADA


Karger:1987:LDP


Kari:1989:CBP

Kari:1989:OCP

[102x681]REFERENCES


Karkare:1996:SEA


Kasiski:1863:GDG

[102x681][Kas63] Friedrich Wilhelm Kasiski. Die Geheimschriften und die Dechiffrierkunst, Mit besonderer Berücksichtigung der deutschen und französischen Sprache. (German) [Secret writing and the art of deciphering, with special reference to the German and French languages]. E. S. Mittler und Sohn, Berlin, Germany, 1863. viii + 95 + 4 pp. LCCN ????

Kastenholz:1996:RVP


Kalipha:1990:NPK


Katzan:1977:SDE


Katsikas:1997:CMS

REFERENCES


Kaufman:1993:RDD


Kaufman:1996:DWC


Kawai:1987:LAI


Kay:1995:CTE


Krishnakumar:1992:HTE


Krawczyk:1996:HMK


Krawczyk:1997:RHK


Klein:1989:STR

Shmuel T. Klein, Abraham Bookstein, and Scott Deerwester. Storing text retrieval systems on CD-ROM. compression and

Karp:1988:SDN


Kunkelmann:1997:EDV


Kao:1995:ESA


Krajewski:1994:ASC


Krajewski:COMPSYS-7-1-75

Krajewski:COMPSYS-7-1-75

Kam:1978:SDS


Kam:1979:SDS

REFERENCES

Khinchin:1997:CF


Keating:1999:PAA


Kelsey:1999:KSWb


Keating:1999:PPA


Kemp:1999:EEF


Keppher:1989:AEP


Kemppainen:1999:DMM


Kent:1993:IPE

Stephen T. Kent. Internet privacy enhanced mail. *Communications of the Association for Computing Machinery*, 36(8):
REFERENCES

476

Kent:1995:PCW


Kerr:1975:PIC


Kerr:1989:SNM


Knoble:1979:EOW


Khesdogan:1996:LMS


Kit:1993:DDI


Klapper:1995:CBA

Andrew Klapper and Mark Goresky. Cryptanalysis based on 2-adic rational ap-

Katsikas:1996:ISS


Kravitiz:1999:CAC


Kundur:1998:DWU


Kunkelmann:1998:VEB


Kharitonov:1993:CHD

REFERENCES

Karaorman:1999:CRJ

Kobara:1996:LVS

Kobara:1997:SSM

Kilian:1988:FCO

Kim:1993:CLB
REFERENCES

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

Kippenhahn:1997:VBG


Kippenhahn:1999:CBH


Kippenhahn:1999:VBG

Kak:1977:SEU


Kocher:1999:DPA


Kurosawa:1995:NBA


Kuwakado:1996:NRT

Hidenori Kuwakado and Kenji Koyama. A new RSA-type cryptosystem based

Kirby:1995:RPK


**Kelm:1997:NK**


**Kunihiro:1998:ECN**

N. Kunihiro and K. Koyama. Equivalence of counting the number of points on elliptic curve over the ring \( Z_n \) and factoring \( n \). *Lecture Notes in Computer Science*, 1403:47–??, 1998. CODEN LNCS93. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Kommerling:1999:DPT**


**Koren:1999:ISC**


**Koshelev:1999:EAM**


**Kurosawa:1991:GPK**

Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata,
REFERENCES

481


Kabatianskii:1997:DSS


Kilian:1994:FKE


Kilian:1995:FCR


Knudsen:1995:NAA


Kothari:1984:CMW


**Klein:1990:FCS**


**Kannan:1988:PFN**


**Klupsch:1999:ARR**


**Kurosawa:1988:CSP**


**Kurak:1992:CNI**


**Kang:1993:PRR**


**Kim:1996:ACA**

[KM96a] Kwangjo Kim and Tsu-
REFERENCES

Knudsen:1996:IDA

Kosuda:1997:SED

Kaksonen:1998:OMC

Kaufman:1998:DWF

Kasahara:1999:NPK

Knudsen:1999:CIS


Kohlas:1999:RAP


Koscielny:1999:QBP


Kanda:1998:ECC


Kobayashi:1999:FEC


Konheim:1980:ICP


REFERENCES


Knuth:1969:SNM


Knuth:1969:SA


Knuth:1973:FA


Knuth:1980:DLC


Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb


Knudsen:1993:ICS

REFERENCES


L. Knudsen. Some thoughts on the AES process. Com-
REFERENCES


Neal Koblitz. *A course in number theory and cryptography*, volume 114 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidel-
REFERENCES


REFERENCES


Kobayashi:1997:DWH


Koblitz:1998:C


Kobara:1999:PMA

Kazukuni Kobara. Pseudorandomness and maximum average of differential probability of block ciphers with SPN-structures like E2. In National Institute of

Koblitz:1998:AAAC


Koblitz:1998:ECI

Standards and Technology

[Nat99b], page ?? ISBN ???
LCCN ???. URL
http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm;
http://www.nist.gov/aes. No slides for the conference talk are available.

Kochanski:1989:HSI

Martin Kochanski. How safe is it? (computer security). BYTE Magazine,

Koc:1989:HSI


Kocher:1995:CDR

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

Koc:1996:RHI


Kocher:1996:TAI

REFERENCES

ny.com/link/service/series/0558/papers/1109/11090104.pdf.


REFERENCES


Koops:1997:CRE


Kopooshian:1997:DCE


Korner:1996:PC


Koscielny:1983:PRD

technique and cryptography. Summary in English and Russian; legends and table of contents also in English. Bibliography: p. 109–110.


[Kos99] Takeshi Koshiba. Unpredictability of pseudo-random number generators on public key cryp-

Kurosawa:1994:NSS


Kurosawa:1995:LEAa

REFERENCES

Kurosawa:1995:LEAb


Koyama:1982:CUM


Koyama:1982:MKR


Koyama:1983:MKR


Koyama:1995:FRT


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Krawczyk:1999:BCC


Kesdogan:1998:DTP


Knudsen:1998:DSR


Kumar:1999:CCB


Kruh:1998:WWS


Knudsen:1999:TDS

L. R. Knudsen, M. J. B. Robshaw, and D. Wagner. Truncated differentials and Skipjack. In

**Kordes:1989:UMC**


**Kelsey:1997:CPO**


**Kurosawa:1997:DSP**


**Kwon:1997:SEA**


**Kaliski:1998:RPRb**

soletes RFC2313 [Kal98b].
Status: INFORMATIONAL. 

Kelsey:1998:SPP

The street performer protocol. Technical report, 
Counterpane Systems, 101 East Minnehaha Parkway, 
Minneapolis, MN 55419, November 1998. URL 
Also published in The Third USENIX Workshop 
on Electronic Commerce Proceedings, USENIX Press. 
November 1998. 

Kinoshita:1998:GST

Generation of the signature with the structured 
information of the image. In Theodoridis et al. 
960-7620-06-2 (v. 1), 960-7620-07-0 (v. 2). LCCN 
TK5102.9.E97 1998. URL 
Four volumes. 

Kipnis:1998:COV

[KS98d] Aviad Kipnis and Adi 
Shamir. Cryptanalysis of 
the oil and vinegar signature scheme. Lecture Notes 
in Computer Science, 1462: 
257–266, 1998. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic). 

Kelsey:1999:AST

[KS99a] John Kelsey and Bruce 
Schneier. Authenticating 
secure tokens using slow 
memory access. Technical report, Counterpane Sys-
tems, 101 East Minnehaha Parkway, Minneapolis, MN 
slow-memory.html. First 
USENIX Symposium on 
Smart Cards, USENIX Press, to appear. 

Kipnis:1999:CHP

[KS99b] Aviad Kipnis and Adi 
Shamir. Cryptanalysis of 
the HFE public key cryp-
tosystem by relineariza-
tion. Lecture Notes in 
Computer Science, 1666: 
19–30, 1999. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic). URL 
http://link.springer-ny.com/ 
link/service/series/0558/
bibs/1666/16660019.htm; 

Kemp:1996:CPC

A. H. Kemp, S. J. Shepherd, 
and S. K. Barton. Corre-
lation properties of a class 
of cryptographically secure 
spreading sequences. In
REFERENCES


Kelsey:1998:SAL


Kelsey: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-

Kemp:1996:PRM

Kemp:1997:MFC

Kelsey:1997:SAL

Kelsey:1998:SAL

Kelsey:1999:NDA

Kim:1996:EIE


Kelsey:1999:NDA

Kemp:1997:MFC

KSB96b]

KSB97]

KSHW97]

KSHW98]

KSHW99]

KSF99]

KSF99]

KSF99]

KSK96]

KSK96]

Kim:1996:EIE

Yong-Tae Kim, Kwang-Suk Suh, and Chang-Han Kim. On the efficient im-


REFERENCES


REFERENCES

Kelsey:1998:SCCb


Kelsey:1998:SCCc


Kelsey:1998:CAP


Korzhik:1991:CMP


Koyama:1991:NPC


Koyama:1993:SEC


Keefe:1996:MTS


**Koyama:1998:AFC**


**Kanda:1999:SCF**


**Kuchlin:1987:PKE**


**Kucera:1992:GES**


**Kuhn:1998:CIS**


**Kuijk:1991:RSE**

REFERENCES

364, December 1991. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).


Kurosawa:1994:NBA


Kearns:1989:CLL


Kearns:1994:CLL


Kaul:1999:IBP


Kirstein:1992:PAS


Konrad:1999:SDK

K. Konrad and D. A. Wolfram. System description: Kimba, a model generator for many-valued first-order logics. Lecture Notes in Computer Science, 1632:


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.

Kurosawa:1998:SBC


Kwok-Yan:1992:TAD


Kwok-Yan:1992:FAA


Kasami:1982:KMS


Koch:1995:TRH


Levien:1998:ART


Lampson:1991:ADS

Butler Lampson, Martín Abadi, Michael Burrows,
REFERENCES


[Lai:1992:DSB] 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.”.


of Cryptology, by J. S. Gal- 
land. American Mathematical 
Monthly, 53(6):330–331, 
June/July 1946. CODEN 
AMMYAE. ISSN 0002-8980 
(print), 1930-0972 (elec-
tronic).

[Lan81] 
Andre Langie. Cryptogra-
phy: a study on secret writ-
ing, volume 38 of A Cryp-
tographic series. Aegean 
Park Press, Laguna Hills, 
CA, USA, 1981. ISBN 0-
89412-061-1. vii + 192 
Translation of: De la cryp-
tographie. Reprint of an un-
specified previous ed. Bibli-
ography: p. 158.

Landau:1989:SSC

Charles R. Landau. Secu-
irty in a secure capability-
based system. Operating 
Systems Review, 23(4):2–4, 
October 1989. CODEN OS-
RED8. ISSN 0163-5980.

Langford:1995:DCT

Susan K. Langford. Differential 
linear cryptanalysis and 

Langford:1996:WST

Susan K. Langford. Weak-
nesses in some threshold 
cryptosystems. Lecture 
Notes in Computer Science, 
1109:74–82, 1996. CODEN 
LNCS .D9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

[Lan97] 
N. Lange. Single-chip im-
plementation of a cryp-
tosystem for financial ap-
lications. Lecture Notes in 
Computer Science, 1318: 
135–??, 1997. CODEN 
LNCS .D9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

Landrock:1998:TOC

P. Landrock. TTPs overview — concepts and review of the state of the art from a technical point 
of view. Lecture Notes in 
Computer Science, 1528: 
241–263, 1998. CODEN 
LNCS .D9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

Landrock:1999:PTU

Peter Landrock. Primality 
tests and use of primes in 
public key systems. Lecture 
Notes in Computer Science, 
1561:127–133, 1999. CO-
DEN LNCS .D9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http: 
//link.springer-ny.com/ 
link/service/series/0558/
bibs/1561/15610127.htm; 
http://link.springer-
Lassek:1985:CCA
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

Lee:1988:OSM

Lee:1989:WBL

Lee:1989:WLB

Leake:1999:IIR
D. B. Leake, L. Birnbaum, K. Hammond, and C. Marlow. Integrating information resources: a case study
of engineering design support. Lecture Notes in Computer Science, 1650:482–??, 1999. CODEN LNCSDO. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES

(print), 1611-3349 (electronic).


REFERENCES


[Lei79] Albert C. Leighton. Book review: An annotated bib-


REFERENCES

CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lempel:1979:CT


Lennon:1978:CAI


Lenstra:1987:FIE


Lenstra:1990:PT


Lennox:1993:ES


Lenstra:1996:GSD


Lenstra:1998:GRM


Lenstra:1999:EIB

LENZERINI:1999:DLT


LERCIER:1997:FGR


LEVINE:1958:VMS


LEVINE:1961:SAH


LEVINE:1961:SECa


LEVINE:1961:SECb


LEVINE:1983:USC


LEVIN:1985:OWF

REFERENCES

Levine:1991:USC


Lewin:1978:UGW


Lewin:1982:AMC


Lewin:1992:SCP


Laurin:1997:SSM

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.

Lopes:1999:UES


Lorigo:1999:CDG


Li:1994:RMC

REFERENCES


**Li:1995:TSW**


**Li:1995:TMS**


**Lichtenthal:1994:CBT**


**Lidl:1985:CBP**

R. Lidl. On cryptosystems based on polynomials.

Lidl:1990:SMA


Lieberherr:1981:UCD


Liebl:1993:ADS


Lim:1998:CNB


Lim:1999:RVC


RFC0989

[Lin88b, Lin89b]. Status: UNKNOWN.

**Linn:1988:RPE**


**RFC1040**


**RFC1113**


**Linn:1989:RPE**
REFERENCES


Linnartz:1998:TCC


Lippit:1993:PIC


Lipton:1994:CNF


Abeles:1998:KVC


Lipmaa:1999:ICM


Litant:1987:BRC


Lindsay:1997:BC

introduced by Russell Baker
Performers: Derek Jacobi,
Alun Armstrong, Richard
Johnson, Harold Pinter,
Amanda Root, Prunella
Scales The story of Alan
Turing, British mathematic-
ical genius and designer of
the computer that broke the
German Enigma code dur-
ding World War II, whose ad-
mittance to homosexuality
at a time when it was illegal
presented problems for him,
for his family, for his col-
leagues, and for the State's
preoccupation with national
security Close-captioned.

[Laih:1996:CEE]
C.-S. Laih and W.-C. Kuo.
Cryptanalysis of the en-
hanced ElGamal's signature
scheme. Lecture Notes in
Computer Science, 1029:
228–??, 1996. CODEN
LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Lee:1999:MRF]
Message recovery fair blind
signature. Lecture Notes in
Computer Science, 1560:
97–111, 1999. CODEN
LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Landau:1994:CPP]
Susan Landau, Stephen
Kent, Clinton C. Brooks,
Scott Charney, Dorothy E.
Denning, Whitfield Diffie,
Anthony Lauck, Douglas
Miller, Peter G. Neumann,
and David L. Sobel. Crypto
policy perspectives. Com-
munications of the Asso-
ciation for Computing
Machinery, 37(8):115–121,
August 1994. CODEN
CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http:
//www.acm.org/pubs/toc/
Abstracts/0001-0782/179726.

[Linnartz:1998:MFA]
Jean-Paul Linnartz, Ton
Kalker, and Geert Depo-
vore. Modelling the false
alarm and missed detect-
ion rate for electronic wa-
temarks. Lecture Notes in
Computer Science, 1525:
329–343, 1998. CODEN
LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
l ink/service/series/0558/
bibs/1525/15250329.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1525/15250329.
pdf.

[Lenstra:1993:DNF]
A. K. Lenstra and H. W.
Lenstra, Jr. The De-
velopment of the Number
Field Sieve, volume 1554
of Lecture Notes in Math-
ematics. Springer-Verlag,
REFERENCES


[Lee:1997:PNB]


[Lim:1997:DSA]


[Lim:1998:SPK]


[Luo:2010:PAE]


[Laih:1989:NTS]

Chi Sung Laih, Jau Yien Lee, and Lein Harn. A new threshold scheme and its


REFERENCES

QA267.A1 L43 no.196.
article&issn=????&volume=0
issn=101.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.

[Lai:1991:PNB]
ibib/0473/04730389.htm;
http://link.springer-ny.com/link/service/series/
0558/papers/0473/04730389.pdf. See [LLG10] for proofs of requirements on the number of rounds.

[Lia:1993:HFBa]

[Lai:1993:HFBb]
ibib/0658/06580055.htm;

[Longley:1993:TNC]
D. Longley and S. M. Matyas. Technical note: Complementarity attacks


[LM95] Leighton:1995:LPF


[LM96] Low:1996:MCP


REFERENCES


Three volumes. IEEE catalog number 95CH35759. IEEE Computer Society Press order number PR06990.


Longo:1990:GCC


Leonard:1997:CSP


Lautemann:1999:DCA


Lidl:1994:IFF


Lehti:1998:CT


Lagarias:1985:SLD

REFERENCES


Yong Hong Long. A probabilistic attack algorithm for

[Long:1992:UDE]

[Loshin:1997:CGP]
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]

[Loxton:1990:NTC]
REFERENCES

Lam:1999:ACA

Li:1999:CKA

Luciano:1987:CCC

Leszczynski:1994:SDA

from the library of the 4th Sga-rje Khams-sprul Rinpoche.


Lai:1993:FCC

Lange:1925:TC

Lange:1981:TC

Lin:1997:LNU

Lu:1989:SCI

Lloyd:1992:RPA

Lin:1997:LNU

Lasker:1998:ACC
G. E. (George Eric) Lasker and Timothy K. Shih, editors. Advances in computer cybernetics; multimedia computing and networking, multimedia presentation, interactive multimedia
support systems, multiuser virtual worlds, platform architecture for multimedia tools, management schemes for collaborative computing, program transformation systems, cryptanalysis and cryptosystems, graph transformation framework, simulation based design and development, design and implementation of programming languages, object systems design, abstracting devices. International Institute for Advanced Studies in Systems Research and Cybernetics, Windsor, ON, Canada, 1998. ISBN 0-921836-54-6. LCCN ???.


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 ATPSDT. 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 \( n \geq t > 0 \), where \( n \) is the total number of processes and \( t \) is the number of faulty processes.


REFERENCES


Lu:1980:AEG [Lu80] Shyue Ching Lu. Addition to: "The existence of

**Lackey:1995:SMS**


**Luby:1996:PCA**


**Lucks:1995:HEI**


**Lucks:1996:FLC**


**Lucks:1996:FLR**


**Lucks:1996:FLR**


**Lucks:1997:SRK**


**Lucks:1998:SBB**

Lucks:1998:OKE


Lucks:1998:ATE


Lucks:1999:SBC


Lucks:1999:ARK


Ludwig:1997:CQA


Lujan:1998:AMDa

REFERENCES

Lujan:1998:AMDb


Lunt:1990:EK


Lutz:1998:NBM


Linnartz:1998:ASA


Langelaar:1996:CPM


Langelaar:1997:RLM


Long:1988:DLH

Douglas L. Long and Avi Wigderson. The discrete

**Li:1991:JAE**


**Lervik:1996:IDS**


**Lucks:1999:RKE**


**Lin:1996:GTU**


**Lenstra:1995:KES**


**Laih:1993:SAS**

C.-S. Laih and S.-M. Yen. Secure addition sequence

**Lodge:1994:SCC**


**Laih:1993:TES**


**Li:1991:ACP**


**Li:1991:BCP**


**Li:1991:HBM**


**Ma:1979:RAD**


**Meijer:1981:DSS**


**MacPherson:1987:CUN**

[Mac94]
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Mac98]

[Mad92]
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 ????.

[Mae98]

[Mah96]

[MAM95]
REFERENCES

proceedings/security95/mcdonald.html.

Mandelbrot:1960:BRJa


Manasse:1995:MPE


Manjunath:1998:IPA


Moriai:1996:KLP


Mao:1997:PVP


Mao:1998:GCS


Marsh:1970:CSS


Marsh:1970:MEC

REFERENCES

ISSN 0002-9890 (print), 1930-0972 (electronic).

Marion:1976:ANB

Marion:1995:WGT

Marks:1995:PEI

Markoff:1996:MIS

Martin:1997:IEI

Markantonakis:1998:CSM

Marks:1998:BSC
REFERENCES


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

Matyas:1979:DSO


Matyas:1991:KHC


Matsui:1993:LCM


Matsui:1994:FEC


Matsui:1994:LCM


Matsui:1995:CBO

Matsui:1996:NSB


Matthews:1996:SRN


Matsui:1997:NBE


Matsumura:1999:DTE


Maurer:1990:FGS


Maurer:1991:NAD


Mauborgne:1914:APC

REFERENCES


REFERENCES

Maurer:1996:UGT


Maurer:1996:ACE


Maurer:1997:ITS


Mauriello:1997:TTC

Mauth:1997:SOC


Maurer:1998:E


Maurer:1999:IC


Maurer:1999:ITC


Maxemchuk:1994:EDD


May:1997:CDS


Milner-Barry:1986:ADL


Mao:1994:SAP


Massey:1994:CCT


Fred Mintzer, Gordon W. Braudaway, and Minerva M.

Moskowitz:1992:CAA


Mitchell:1996:CKU


McCarthy:1975:AFP


McCurley:1990:DLP


McCurley:1990:OEC

REFERENCES


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

Meierhofer:1996:PGP


Meijer:1996:GFC


Meinel:1998:HHB


Mendelsohn:1989:CWI


Mendez:1991:AKA


Menezes:1993:ECP

communications and Information Theory.

**Menezes:1995:ECC**


**Menicocci:1995:SAC**


**Mersenne:1644:CPM**

[Mer44] Marin Mersenne. *Cogitata Physico-Mathematica ... Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theoretica, practica. Et Mechanica phaenomena. Ballistica et aeronautismologia*. 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 $2, 3, 5, 7, 13, 17, 19, 31, 67, 89, 107$ 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 CACMA2. ISSN 0001-0782 (print), 1557-
REFERENCES


REFERENCES

Merkle:1991:FSE


Merrill:1997:ARD


Meyer:1996:RPE


McGraw:1997:UKJ


Murino:1995:RNU

[MFG95] V. Murino, E. Frumento, and F. Gabino. Restoration of noisy underwater acoustic images using Markov

Abstracts/0001-0782/163380.html.

**Mihaljevic:1991:CCP**


**Madson:1998:RUHa**


**Madson:1998:RUHb**


**Mackenzie:1998:LPS**


**Merkle:1978:HIS**


**Merkle:1981:SME**

Michels:1996:RDS


McPherson:1998:CRH


Majzik:1996:MCU


Matsumoto:1990:EAC


Moulin:1999:ECG


Matsumoto:1988:PQP


Michener:1988:TSK

John R. Michener. A tool for secret key cryptography. *Dr. Dobb’s Journal of Soft-

Micali:1993:FPC


Micali:1993:FPK


Micciancio:1997:ODS


Mihaljevic:1996:FCS


Millikin:1943:ECCa

REFERENCES


REFERENCES


Millikin:1992:ECC


Miller:1995:HWK


Millan:1996:LOA


Miller:1996:CME


Matsumoto:1993:VIA


Mintzer:1997:EIDa


Misarsky:1997:MAU

REFERENCES


REFERENCES


Moskowitz:1994:CCH


Mazieres:1999:SKM


Maibaum:1999:SRS


Miyazaki:1999:TFI


Monge:1967:NMC


Maulucci:1987:HAC


[MM83] Cleve Moler and Donald Morrison.

[MMLG95] A. Muffett, P. Leyland, A. Lenstra, and J. Gillogly.


[MM87] Stephen M. Matyas and Carl H. Meyer.

REFERENCES


MattosBrasil:1998:CCC


Matheson:1998:RSD


Magliveras:1990:CTC


Muller:1986:CDS


MRaihi:1997:XFO


Moulin:1999:ITA

REFERENCES

Mock:1997:BDS


Mohtashemi:1992:CHC


Matsumoto:1982:DTL


Mok:1997:KNF


Moldovyan:1998:NEP


Morita:1991:SCT


Montgomery:1985:MMT

REFERENCES


Teo Mora, editor. *Applied algebra, algebraic algorithms, and error-correcting


[Morgan:1997:PAM]


[Mosses:1999:CGT]


[Moura:1999:PAP]


REFERENCES


REFERENCES

Montgomery:1990:FEP


Meier:1991:CPC


Massey:1994:FTA


Meier:1995:SG


Meier:1995:SSG


Meier:1993:EMC


[MS99]

Metzger:1995:RIAb


[MS98b] M. Michels and M. Stadler. Generic constructions for secure and efficient con- firmer signature schemes. Lecture Notes in Computer
REFERENCES


MacKenzie:1999:AIH

Maitra:1999:HNR

Miyazaki:1999:KGD

McLeod:1990:VLD

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).

Moriai:1998:HOD

McClure:1999:HEN
REFERENCES


**Michels:1998:SSV**


**Mullender:1986:DCD**


**Matsui:1994:VSH**


**Massey:1995:MCM**

B. C. Massey and E. Tick. Modes of comprehension: Mode analysis of arrays and

Molva:1998:SSA


Matsui:1999:CRV


Melkonian:1999:AAD


Mister:1999:CRL


Marayati:1987:AWA


Moggi:1999:IMS


Mackinnon:1985:OAA

REFERENCES

CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=
&arnumber=1676635.

Moriya:1997:DWS

Takehiro Moriya, Youichi Takashima, Takao Nakamura, and Naoki Iwakami.
Digital watermarking schemes based on vector quantization. In IEEE [IEE97e],

Molva:1992:KAK

Refik Molva, Gene Tsudik, Els Van Herreweghen, and Stefano Zatti. Krypto
Knight authentication and key distribution system. Lecture Notes in Computer
Science, 648:155–162, 1992. CODEN LNCSD9. ISSN 0302-9743 (print),
1611-3349 (electronic).

Mu:1992:ICS

Hao Mu. ID-based cryptographic schemes for user identification, key distri-
bution, and digital signature. Thesis (M.S.), Computer Science Tele-
communication Program. University of Missouri-Kansas City, Kansas City, MO,
USA, 1992. ix + 54 pp.

Mueller:1999:SRB

S. Mueller. On the security of an RSA based encryption scheme. Lecture Notes
in Computer Science, 1587:135–148, 1999. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

Muftic:1988:SMC

Sead Muftic. Security mechanisms for computer networks. current results of the CEC COST-11 ter

Muftic:1993:SAO


Mulherin:1981:FDE

Michael Hugh Mulherin. A file data encryption system using Galois fields. Thesis
(M.Sc.Cs.), University of New Brunswick, Ottawa, ON, Canada, 1981. 174 pp. 2
microfiche(s) (174 fr.).

Mulligan:1989:UMA

Timothy Mulligan, editor. ULTRA, MAGIC, and the Allies, volume 1 of Covert
REFERENCES


Murphy:1996:CC


Murphy:1999:OST


Musser:1992:UVE


Maruyama:1998:TGH


Menezes:1990:IEC


Menezes:1991:ACC


Meijers:1993:EMV

Joost Meijers and Johan van Tilburg. Extended majority voting and private-

**Menezes:1998:C**


**Menezes:1993:CPE**


**Muller:1998:DLB**


**Manber:1994:AAM**


**Maurer:1996:TCW**

U. Maurer and S. Wolf. Towards characterizing when information-theoretic secret key agreement is possible. *Lecture Notes in
REFERENCES


Maurer:1996:DO

[MW96b]


Maurer:1996:DHO

[MW96c]


Maurer:1997:PAS

[MW97]


MacNish:1998:BRD

[MW98a]


Memon:1998:PDM

[MW98b]


Merkle:1998:SSR

[MW98c]

Merkle:1998:SSA


Maurer:1999:RBB


Malkin:1999:ESG


Mitchell:1994:CPA


Maurer:1991:NIP


Matsui:1993:NMK

M. Matsui and A. Yamagishi. A new method

**Maurer:1993:RNI**


**Mayers:1998:QCI**

REFERENCES


[NAA99] F. Nat-Abdesselam and N. Agoulmine. QoS con-

**Naccache:1993:MSF** [Nac93]


**Nachenberg:1997:CVA** [Nac97]


**Naik:1989:CDS** [Nai89]


**Nalwa:1997:AOS** [Nal97]


**Nanovic:1936:SW1** [Nan36]


**Nanovic:1974:SW1** [Nan74]


**Nastar:1994:VMN** [Nas94]

References


REFERENCES

Abstracts/0001-0782/129904.html.


REFERENCES


[NBWH78] Arne Nilsson, Rolf Blom,


Amaury Nève, Denis Flandre, and Jean-Jacques Quisquater. Feasibility of Smart Cards in silicon-on-insulator (SOI) tech-
REFERENCES


Nichols:1998:CCCa


Nichols:1998:CCCb


Nichols:1999:IGC


Niederreiter:1986:KTC


Niederreiter:1988:SNC


NIST:1985:FPC


Nissan:1989:AIM


Nissan:1991:EMF


NIST:1992:NCS

REFERENCES


REFERENCES


Nicchiotti:1998:NIS


Nobauer:1984:CRS


Nobauer:1985:CRS


Nobauer:1988:CPK


Nobauer:1984:CRS


Noras:1995:CHHa


Noras:1995:CHHb


Noras:1995:PCE

Naor:1993:PZK


Naor:1997:VAI


Naor:1998:TTT


Nikolaidis:1998:RIW


Naor:1999:OTA


Niemi:1994:CPV


Nyberg:1995:MRS

REFERENCES

Naor:1998:UIS

Needham:1978:UEAa

Needham:1978:UEAb

Naor:1995:VC

Neuman:1988:AUE

Norris-Saucedo:1989:DAD

Naor:1997:NPK
[NS97a] David Naccache and Jacques Stern. A new public-

Nguyen:1997:MRC


Nguyen:1997:MHR


Nguyen:1997:CAC


Nguyen:1998:BQS

REFERENCES


Nemetz:1988:RLS


Nurmi:1994:CPA


Needham:1997:TE


Naor:1998:ACS


Naor:1989:UOW


Naor:1989:UOH


Naor:1990:PKC

REFERENCES


REFERENCES

Oakley:1978:RPC


Oberzalek:1999:GEE


OConnell:1981:CDE


OConnor:1994:UBN


OConnor:1995:DCT


Obenland:1999:SED


ORuanaidh:1996:PWD


Odlyzko:1984:CAM

Andrew M. Odlyzko. Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir’s...


[Odl90] A. M. Odlyzko. The rise and fall of knapsack cryptosys-


Thomas Oelke. VHDL design of a DES encryption cracking system. Thesis (M.S.), Rochester Institute of Technology, Rochester,
Okamoto:1993:EDS


O'Connor:1995:UMA


Oehler:1997:RHM


Oh:1999:DCT


Ohira:1999:EDD


Ohta:1996:DCT

REFERENCES


Okamoto:1993:RAC


Okamoto:1993:PSP


Okamoto:1994:DCS


Okamoto:1998:TKR


Okamoto:1998:TKS


Okon:1996:DWN


Okon:1997:KMA

REFERENCES

Ogata:1997:FTA


Ogata:1993:NSS


Oleshchuk:1995:PKC


Ohta:1994:DAM


Oishi:1997:HVP


Ohbuchi:1998:WTD


Ozaki:1993:HVP

[S. Ozaki, T. Matsumoto,

Omura:1990:PKC

J. Omura. A public key cell design for smart card chips. In ????. [??90], pages 983–985.

Ochi:1998:NSO


O’Neil:1986:ETM


Ogawa:1998:WTM


Okamoto:1990:DZKb


Ohta:1993:DMS


REFERENCES


Oppliger:1997:ISF


Otway:1987:ETM


OECD:1998:OEM


OECD:1998:CPG


Orlowski:1996:EGI


Orton:1987:VIP


Orton:1995:MTD

G. Orton. A multiple-iterated trapdoor for dense
REFERENCES


Orton:1995:MIT


O'Shea:1988:CDU


Okamoto:1991:EAC


Olejar:1998:CPR


Orup:1991:VER

REFERENCES


REFERENCES

Ou:1999:UUC


Outerbridge:1998:ACD


Ozarow:1984:WTC

Lawrence H. Ozarow and Aaron D. Wyner. Wiretap channel II. AT&T Bell Lab. tech. j, 63(10 part 1): 2135–2157, 1984. CODEN ABLJER. ISSN 0748-612X.

OReilly:1995:WWW


Ostrovsky:1991:HWM


Pereira:1998:REC

REFERENCES


REFERENCES


[Pai99]


[PAK98]


[Par85]


[Par98a]


[Par98b]


[Par98c]


[Pat87]

Wayne Patterson. Mathematical cryptology for computer scientists and mathematicians. Rowman and
Patarin:1991:PPB

Patarin:1991:NRP

Patarin:1995:CMI

Patarin:1996:ACH

Paterson:1999:IPG

Paulson:1998:IAV

Paulson:1999:IAI
REFERENCES


Poovendran:1999:ITA


Poovendran:1999:ITA

Proctor:1999:PC


Proctor:1999:PC

Piva:1997:DBW


Piva:1997:DBW

Preneel:1997:CHF


Preneel:1997:CHF

Preneel:1989:CHB


Preneel:1989:CHB

Preneel:1990:CTA


Pedersen:1991:DPA  T. P. Pedersen. Distributed provers with applications to undeniable signatures. In Davies [Dav91],
Pedersen:1991:NIS


Pedersen:1991:TCT


Pedersen:1991:NII

Torben Pryds Pedersen. Electronic payments of small amounts.
Technical Report DAIMI PB-495, Aarhus University, Computer Science Department, Aarhus, Denmark, August 1995.

Pedersen:1999:SCP


Pelta:1960:SP


Penzhorn:1996:CAS


Perret:1890:RCS


Peralta:1985:TRN


Perry:1991:EIT


Peralta:1993:QSD


REFERENCES


B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographic hash functions. In Wolowicz [Wol93b], pages 161–171. LCCN ???.


Preneel:1993:IAH


Preneel:1993:CSI


Preneel:1994:HFB


Pohlig:1978:IAC


Post:1991:RSE


Praun:1999:RMW

REFERENCES


Phillips:1998:SHI


Pichler:1986:ACE


Pichler:1998:E


Pierce:1977:SSP


Pieper:1993:CRD


Pinch:1997:UCN


Piner:1998:CUW

Mary-Louise G. Piner. CS update; WW II cryptologist [Jack Good] receives Pioneer Award; Colossus builder Tommy Flowers (1905–1998); DCI founder [George Schussel] receives Entrepreneur Award; 1998


**Penzhorn:1995:CLP**


**Penzhorn:1995:CLW**


**Praehofer:1999:SRS**


**Pamplona:1998:LVC**


**Postma:1997:DCF**


**Park:1994:KDA**

[Petrounias:1994:RBA]

[Pluss:1975:ESC]

[Pluss:1977:ESC]

[Plimmer:1998:MIW]

[Plumstead:1982:ISG]

[Plumstead:1983:ISP]

[Pei:1999:COA]
REFERENCES


Payne:1978:OEN


Petersen:1998:SST


Pitt:1999:DAC


Provos:1999:FAP


Prie:1999:ASU


Proctor:1992:AIC


Pudil:1995:ASM


Carl Pomerance. Cryptology and computational


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT


Posch:1992:TMD


Posch:1993:GDB


Posch:1998:MPC


Posch:1989:AEA


Pfitzmann:1990:HBD

B. Pfitzmann and A. Pfitzmann. How to break the direct RSA-implementation of MIXes. In Quisquater and Vandewalle [QV90], pages 373–?? CODEN
REFERENCES

Posch:1992:MRR


Posch:1992:RNS


Pakstas:1996:SNN


Pedersen:1997:FSS


Park:1997:TER


Peleg:1979:BSC


Preneel:1998:SAA


Preneel:1998:RDD


Pratt:1939:SUS


Pratt:1996:SUS


Parra:1998:MPS

REFERENCES

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


REFERENCES

**Preneel:1997:HFM**


**Preneel:1998:CMA**


**Preneel:1998:IC**


**Preneel:1999:SCH**


**PGP:1997:PGPa**


**PGP:1997:PGPb**


**Pritchard:1980:DE**

Price:1983:ABR


Price:1994:MVC


Pronzini:1980:MCC


Proctor:1985:SSC


Patel:1999:TML

[PRS99] S. Patel, Z. Ramzan, and G. S. Sundaram. Towards making Luby-Rackoff ciphers optimal and practi-
REFERENCES


Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.


[PS96d] D. Pointcheval and J. Stern. Security proofs for signa-


REFERENCES


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

Patiyoot:1999:WWA


Pfenning:1999:SDT


Patel:1997:UDB


Pieprzyk:1991:RAS


Pieprzyk:1995:PA


Pieprzyk:1995:ACA


REFERENCES


Parkes:1999:ACC


Purdy:1974:HSL


Puteanus:1627:EPC

[Erycius Puteanus. Eryci Puteani Cryptographia Tassiana, sive, Clandestina scripti. Typis Cornelii Coenesteynii, Louvanii, 1627. 18 + 2 pp. LCCN Z103.5 .P88 1627.]

Preparata:1990:PCD


Peinado:1997:HPC


Posegga:1998:BCV


Preneel:1995:MMB

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


REFERENCES

Quisquater:1998:CSE


Quisquater:1991:CLE


Quisquater:1989:BHF


Quisquater:1995:ACE


Qiao:1998:CME


**Qiao:1998:WMM**


**Qin:1988:RSS**


**Quisquater:1989:ACE**


**Quisquater:1990:ACE**


**Quisquater:1998:E**

[J.-J. Quisquater and J. Vandewalle. Eurocrypt ’89. Lecture Notes in Computer
REFERENCES


[Rat96] Rebecca Ann Ratcliff. *Delusions of intelligence: national cultures of cryptography, secrecy and bureaucracy in Germany and Britain during World War*

Rhodes-Burke:1982:RSA


Reiter:1994:HSR


Ramesh:1999:VPP


Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA

P. Rogaway and D. Coppersmith. A software-optimised encryption algorithm. *Lecture Notes

Rogaway:1994:SOE


Russinovich:1995:EWL


Rubia:1999:RIB


Renvall:1996:ASS


Renvall:1996:NSS


Roback:1999:CRF


Michael Reiter. Integrating security in a group oriented distributed system. Operating Systems Review, 26(2):
REFERENCES


REFERENCES


Rivest:1992:RNP


Rhee:1993:RAC


Rhee:1994:CSC


Rihaczek:1987:T


Rijmen:1999:WL

Riley:1996:LET

W. D. Riley. LANSCAPE—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.

Ripe:1995:IPS


Ripe:1995:RIP


Ritter:1999:IWC


Ritchie:19xx:DCW


Rivest:1974:HCA


Rivest:1974:AAR

REFERENCES

676


REFERENCES


REFERENCES


Raisch:1996:ACH


Roberts:1993:ECI


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Roe:1994:PSC


Roe:1995:PBC


Roelse:1999:CWD

[Roe99] Peter Roelse. Cryptanalysis of the Wu-Dawson pub-
REFERENCES


jurgen rohwer. geleitzugschlachten im marz 1943: fuhrungsprobleme im hoehepunkt der schlacht im atlantik. (german) [convoy in march 1943: implementation problems in the climax of the battle of the atlantic]. motorbuch, stuttgart, germany, 1975. isbn 3-87943-383-6. 356 pp. lccn ???. see also english translation [roh77].

jurgen rohwer. the critical convoy battles of march 1943: the battle for hx.229/sc122. naval institute press, annapolis, md, usa, 1977. isbn 0-87021-818-2. 256 + 32 pp. lccn d770 .r59313. revised english translation by derek masters of the german original [roh75].

pankaj rohatgi. a cautionary note regarding evaluation of aes candidates on smart-cards. in national institute of standards and technology [nat99b], page ?? isbn ???. lccn ???. no slides for the conference talk are available.

steven roman. cryptology. modules in mathematics. innovative textbooks, irvine, ca, usa, second edition, 1990. isbn 1-878015-06-0. various pp. lccn ???.

j. rompel. one-way functions are necessary and sufficient for secure signatures. in acm [acm90], pages
REFERENCES


Greg Rose. PGP, Phil Zimmerman, Life, the universe, and so on. ;login: the USENIX Association newsletter, 20(2):4–7, April 1995. CODEN LOGNEM. ISSN 1044-6397.


Greg Rose. Phil Zimmermann is off the hook. ;login: the USENIX Association newsletter, 21(2):6–??, April 1996. CODEN LOGNEM. ISSN 1044-6397.

Greg Rose. Update on cryptography issues. ;login: the USENIX Association newsletter, 21(1):4–??,
REFERENCES

February 1996. CODEN LOGNEM. ISSN 1044-6397.


REFERENCES


REFERENCES


to the journal Cryptologia, but never published. For the story behind the suppression of publication, see [Ritxx]. Internal technical memoranda TM 78-1271-10, TM 78-1273-2., 1978.


REFERENCES


REFERENCES


REFERENCES


Roeckl:1999:CPS

Rozenberg:1999:DCN

Rivest:1982:MOD

Rivest:1983:MOD

RSA:1993:PRE
REFERENCES


**RSA:1993:PDH**


**RSA:1993:PEC**


**RSA:1993:PCM**


**RSA:1993:PPK**


**RSA:1994:MPK**


**RSA:1999:PVPb**


**RSA:1999:PVPa**


**RSA:1999:PVPc**

REFERENCES

Reed:1998:ACO


Reif:1988:EPP


Rezny:1993:BCM


Raleigh:1988:CDP


Rubin:1979:DSC


Rudolph:1982:HTI


Rudich:1991:UIP

REFERENCES

Rueppel:1993:ACE

Rueppel:1998:E

Ruggiu:1985:CCT

Russell:1927:CMS

Ruohonen:1994:EDO

Russel:1990:HLS
D. Russel. High-level security architecture and the
REFERENCES


**Ruskey:1993:SCG**


**Russell:1993:NSC**


**Roychowdhury:1999:ENQ**


**Reeds:1984:FSU**


**Robshaw:1997:ECC**


**Rytter:1986:SCU**


**Ras:1999:DES**


**S:1873:COD**

[S.73] H. S. *Cryptographie, ou, Divers systèmes d’écritre*
secreta specialmente per l'uso des carte postales: combinations alphabétiques, correspondance chiffrée, écriture par signes; divers procédés pour la fabrication d'encre sympathiques.


Schiller:1995:SWT


Sabourin:1994:CCP


Sacco:1936:MC


Sacco:1947:MC


Sacco:1951:MCF


Sacco:1977:MC


Sahai:1999:NMN

REFERENCES


[Sal91] A. Salomaa. Verifying and recasting secret ballots in
Salomaa:1996:PC


Salvail:1998:QBC


Salvail:1999:SHG


Shimoyama:1997:IFS


Sameshima:1998:KES


Sansom:1986:BRC


Sandhu:1988:CIT

Sarton:1928:BRBn


Sars:1997:STL


Sargent:1999:FID


Sasaki:1999:SFU


Swierstra:1999:DIC


Satyanarayanan:1989:ISL


Saunders:1989:IDE

Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Smid:1992:DES


Smid:1993:RCN


Shepherd:1994:UBS


Shepherd:1995:CNL


Schneier:1997:EPP

REFERENCES


Smillie:1985:RFM


REFERENCES


[Sc86] Fred A. Scacchitti. The cryptographer's toolbox.


REFERENCES

Verlegung Simon Halbmayers.

[Schwenter:1633:SSA]


REFERENCES

URL http://link.springer-ny.com/link/service/series/0558/tocs/t0435.htm;
Conference held Aug. 20–24, 1989 at the University of California, Santa Barbara.

Schnorr:1990:EISa


Schroeder:1990:NTS


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**


**Schneier:1993:SCD**


**Schneier:1993:DS**


**Schneier:1993:IEA**


**Schneier:1993:UHD**

REFERENCES

Schnorr:1993:FHI

Schnorr:1993:FIE

Schiller:1994:SDC

Schneier:1994:DNV

Schneier:1994:DEA

Schneier:1994:PAD

Schneier:1994:SCD

Schneier:1994:AAad


[Sch95f] Bruce Schneier. A pair of cryptographic conferences.


REFERENCES


Bruce Schneier. The crypto bomb is ticking: Crack-

**Schneier:1998:CDV**


**Schneier:1998:CTS**


**Schneier:1998:SPC**


**Schneier:1998:TEA**


**Schoenmakers:1998:SAE**


**Schroeppel:1998:HPC**

REFERENCES


See [RD99a] for a conference overview. 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.


Schwentick:1999:DCL


Scerri:1999:UOS


Scudder:1992:OLA


Smith:1986:GCC


Silvestre:1997:IWU


Schouten:1999:FEU


Sicherman:1983:AQR


Smillie:1986:RWA

K. W. Smillie and Ralph Erskine. Reviews: W. Aspray, Should the Term Fifth Generation Computers Be Banned?; C. A.

**Schwenk:1996:PKE**


**Seaton:1956:THS**


**Sears:1986:SWK**


**Seachrist:1995:DIM**


**Sedlak:1988:RCP**

REFERENCES


Sedgewick:1992:AC


Seeley:1989:PCG


Seethamraju:1997:HII


Segal:1992:NTC


Selcuk:1998:NRL


Selmer:1994:MNC


Selmer:1998:NMS

REFERENCES

shtml. Third volume of selected papers from issues of Cryptologia.

Serpell:1985:CES

Seshadri:1981:KPP

Sakurai:1997:ILC

Shearer:1996:GCR

Shieh:1996:DIL

Shoup:1998:STC
REFERENCES

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

[Sga91a]

[Sga91b]

[Sga93]

[Sgarro:1999:SCG]

[Sga99a]

[Sapir:1999:DRT]

[Sga90]
REFERENCES


[SH97] B. Schneier and C. Hall. An improved E-mail security protocol. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN.
REFERENCES


Shi:1999:FGM


Shannon:1945:MTC


Shannon:1948:MTCa

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:MTCb


Shannon:1949:CTS


Shamir:1979:HSS

Shamir:1982:PTA


Shamir:1983:ECT


Shamir:1983:GCS


Shamir:1984:PTA


Shamir:1985:IBC


Shamir:1986:SPS


Shamir:1987:CSS

Adi Shamir. Cryptography: State of the science. In Ashenhurst [Ash87],
REFERENCES

Sharp:1988:DCO

Shamir:1994:ESS

Shamir:1995:MEV

Shamir:1995:RP

Shamir:1998:VC

Shallit:1999:RHA

Shamir:1999:PAK


[She92d] S. J. Shepherd. A numerical processor with supercomputer performance based on state-of-the-art finite-impulse-response filter digital signal processors. Internal Research Note 5, Electronic and Electrical Engineering Department, Unio-


[Sherrod:1992:DES]


[Shepherd:1993:ACCa]

[She93b] S. J. Shepherd. Access control and cryptography. In ???, editor, Proceedings of

[Shepherd:1993:ACCb]


[Shepherd:1993:EOS]


[Shepherd:1994:ACM]

[She94b] S. J. Shepherd. Cryptanalysis of the GSM A5 cipher al-

[Shepherd:1994:CGA]

**Shepherd:1994:MCM**


**Shepherd:1994:PKS**


**Shepherd:1995:CAA**


**Shepherd:1995:PPH**


**Shepherd:1995:HSS**


**Shen:1996:APK**


**Shepherd:1996:SWN**

REFERENCES


Shparlinski:1999:FFT


Shparlinski:1999:NTM


Shulman:1980:BRB


Shulman:1976:ABC


Shumaker:1982:RCJ


Sakurai:1993:DBS

K. Sakurai and T. Itoh. On the discrepancy between serial and parallel of zero-knowledge protocols. *Lecture Notes in Computer Sci-
REFERENCES


REFERENCES


Cicco Simonetta. [Little tract on cryptanalysis]. ???, ???, 1404. ???. pp.
Simmons:1979:HID


Simmons:1979:CCA


Simmons:1979:SAE


Simmons:1982:SCA


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC

[Sim85a] Gustavus J. Simmons. Authentication theory/coding
REFERENCES


Simmons:1985:SCD


Simmons:1988:SSC


Simmons:1990:HRS


Simmons:1990:PSS


Simmons:1991:GSS

Gustavus J. Simmons. Geometric shared secret and/

Simmons:1992:CCS


Simmons:1993:SCU


Simmons:1994:CTS


Simmons:1994:CPF


Simmons:1994:SCP


Simmons:1994:SCE

Gustavus J. Simmons. Subliminal communication is


G. J. Simmons. Results concerning the bandwidth of subliminal channels. *IEEE Journal on Selected Areas in Communications*, 16(4):463–473, May 1998. CODEN ISACEM. ISSN
REFERENCES


[Sin98] Anthony Martin Singer. Electronic commerce: dig-

**Singh:1999:CBE**


**Siu:1999:PNG**

Chi Sang Obadiah Siu. Pseudorandom number generator by cellular automata and its application to cryptography. M.Phil., Chinese University of Hong Kong, Hong Kong, 1999. 68 pp.

**Sambur:1976:SEM**


**Sethi:1997:FCS**


**Scott:1998:DAB**


**Sako:1994:SVU**

REFERENCES

[Sako:1995:RFM]

[Schneier:1996:AOC]

[Schneier:1996:PPSa]

[Schneier:1996:UFNa]

[Schneier:1996:UFNb]

[Schneier:1996:PPSb]
REFERENCES


**Schneier:1997:AESb** [SK97d]

**Schneier:1997:AESa** [SK97a]

**Schneier:1997:RAS** [SK97c]

**Stabell-Kulo:1997:SLS**

**Schneier:1998:CSS** [SK98a]

**Shimoyama:1998:QRS** [SK98b]
Shimoyama:1998:QRB


Schneier:1999:SAL


Stabell-Kulo:1999:PAM

Tage Stabell-Kuls, Ronny Arild, and Per Harald Myrvang. Providing authentication to messages signed with a Smart Card in hostile environments. In USENIX [USE99c], page ??

Shepherd:1997:EKE


Schell:19xx:CMC


Sorokine:1994:TBD


Suzuki:1999:AVB

S. Suzuki, T. Kato, H. Ishizuka, and Y. Takahashi. An application of vision-based learning in RoboCup for a real robot with an omnidirectional vision system and
REFERENCES

the team description of Osaka University "Trackies". Lecture Notes in Computer Science, 1604:316–??, 1999. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).


Schneier:1998:TBSa


Schneier:1998:TBBb
REFERENCES


REFERENCES


Schneier:1999:NRT


Schneier:1999:TKS


Schneier:1999:TEAb


Schneier:1996:AC


Schneier:1999:TKS


Sufatrio:1999:IMS

Slutsky:1998:KDQ


Schobi:1983:FAT


Siromoney:1990:PKC


Staffelbach:1991:CSC


Schubert:1995:MLS


Syverson:1995:FRK


Sklower:1996:RPE

REFERENCES

rfc/rfc1969.txt; http://www.math.utah.edu/pub/rfc/rfc2419.txt. Obso-
leted by RFC2419 [SM98b].

Status: INFORMATIONAL.


letes RFC1969 [SM96]. Status: PROPOSED STAN-
DARD.


REFERENCES


Smith:1993:LPE


Smith:1994:CPC


Smith:1994:CE


Smith:1997:ETC


Smith:1997:IC


Smith:1998:IES


Smith:1998:SXC


Shimoyama:1998:IHO


Son:1998:ASC

REFERENCES

Stakhov:1999:IFC


Safavi-Naini:1993:FTA


Shepherd:1994:VFH


Safavi-Naini:1996:TSS


Steiner:1988:KAS


Safavi-Naini:1993:ACU


Safavi-Naini:1995:ACP

Safavi-Naini:1998:BCM


Safavi-Naini:1998:NRM


Snyder:1979:IUC


Snyder:1980:CAP


Shepherd:1998:ALP


Sonnino:1999:CBL


Schroeppel:1995:FKE

REFERENCES


Schechter:1999:AAM


Spirakis:1995:AET


Shoup:1996:SKD


Saltzer:1984:EEA


Shin:1998:NHF


REFERENCES

749

(Sprint), 1611-3349 (electronic).


REFERENCES


Sakurai:1995:RAC

Smith:1995:PCD

Smith:1995:PKC

Sandhu:1996:AAC

Silverman:1997:CAX

Sakai:1998:DHC

Sun:1998:PKC
Hung-Min Sun and Shih-Pyung Shieh. On private-key cryptosystems based on product codes. Lecture Notes in Computer Science,
REFERENCES


Schneier:1999:BHD

Schoenhoff:1999:GVM

Shapiro:1999:MAE

Solomonides:1999:REI

Stubblebine:1999:FLA

Stubblebine:1999:FOA

Subramanian:1987:DTP
REFERENCES

Siromoney:1988:CPL


Saito:1999:DPC


Smith:1981:VEP


Stubblebine:1999:UST


Safford:1993:SRA


Sakai:1997:WRK

Y. Sakai, K. Sakurai, and I. Ishizuka. On weak RSA-keys produced from Pretty Good Privacy. Lecture Notes in Computer Science,
REFERENCES


[Sakai:1997:WRP]


[Subramanian:1992:LT]


[Sherman:1994:SNA]


[Schneier:1997:DDE]


[Saeednia:1998:SGI]


[Saeednia:1998:SGI]
Susilo:1999:FST


Shepherd:1990:CSS


Schmidt:1998:LOA


Salter:1998:TSS


Schneier:1998:DDE


StJohns:1984:RAS

bib. Obsoleted by RFC0931
[St.85]. Status: UNKNOWN.

rfc931.txt. Obsoleted RFC1413 [St.93]. Obsoletes RFC0912 [St.84]. Status:
UNKNOWN.

John Shawe-Taylor. Book review: Cryptography: an introduction to computer
security, by Jennifer Seberry and Josef Pieprzyk. Prentice-Hall Inter-
national, Hemel Hempstead, United Kingdom, 1988, Price £17.95 (paper-
September 1989. CODEN SCPGD4. ISSN 0167-6423 (print), 1872-7964 (elec-

Jacques Stern and Philippe Toffin. Cryptanalysis of a public-key cryptosystem
based on approximations by rational numbers. Lecture Notes in Computer Science,
473:313–317, 1991. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349

R. Safavi-Naini and L. Tombak. Optimal authentication systems. Lecture Notes in
Computer Science, 765: 12–??, 1994. CODEN LNCS9D. ISSN 0302-9743
(print), 1611-3349 (electronic). URL http://
/link.springer-nv.com/link/service/series/0558/
REFERENCES

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:1995:PWT

Stallings:1995:PYP

Stadler:1996:PVS

Staiger:1996:CSW
REFERENCES

Stallings:1996:PCS

Stallings:1996:PCI

Staddon:1997:CSC

Stallman:1997:SDR

Stark:1997:ESP

Stallings:1999:CNS

Stallings:1999:HAK
William Stallings. The HMAC algorithm: Key hashing for message authentication. *Dr. Dobb’s Jour-
REFERENCES

Stevenson:1976:MCI


Stevens:1988:CPR


Stephenson:1989:PPM


Stern:1987:SLC


Stern:1994:DIS

REFERENCES

Stevens:1994:PBa


Stern:1995:COD


Stern:1996:VCA


Stern:1998:LCO


Stern:1998:NEA


Stephenson:1999:C


Stern:1999:ACE

REFERENCES


REFERENCES


Stinson:1998:C


Stout:1965:DRN


Stoll:1989:CET


Stout:1990:SDE

REFERENCES


Stumme:1999:AEK

Steiner:1995:REE

Su:1998:DEM

Summers:1984:OCS

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**


**Stern:1998:CC**


**Shamir:1999:PHS**


**Shamir:1999:PSS**

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.


0558/papers/0473/04730306.pdf.

**Shulman:1961:GC**


**Smith:1983:HCR**


**Silverman:1993:PAE**


**Saeki:1994:SSS**


**Safford:1994:UNC**


**Snow:1994:SA**


**Scheidler:1995:PKC**


**Stansfield:1995:CCS**

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

**Schneier:1997:FSEa**


**Schneier:1997:FSEb**


**Stinson:1998:ARS**


**Stinson:1999:ARS**


**Stinson:1999:KPT**


**Swan:1994:AAb**


REFERENCES

CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).


REFERENCES

Seberry:1993:ACA


Sakurai:1996:CWR


Szepietowski:1998:WSO


Swanson:1996:RDH


Swanson:1996:TRI


Swanson:1998:MSB

REFERENCES


Seberry:1995:RBP


Theodoridis:1998:NES


Takano:1999:CAC

Kohji Takano et al. A cryptographic accelerator card with small fast low-power RSA engines. In Anonymous [Ano99c], page ??

Takagi:1997:FRT


Tang:1997:DBC


REFERENCES

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

[Tao:1999:GPK]

[Tao:1999:FAP]

[TCC97]

[Tangney:1991:SIS]

[Tedrick:1985:FES]

[Teske:1998:SPR]
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.


Thomas:1986:SDE

Thompson:1987:RTT

Thomas:1996:PVS

Tarman:1998:AAE

Tsuji:1988:PKC

Tilki:1998:EHD

Tippett:1927:RSN

Taaffe:1997:NSL
Joanne Taaffe and Margaret Johnston. News: Siemens licenses Java for...


[TLS99] Four volumes.


REFERENCES


REFERENCES


J. Traore. Making unfair a “fair” blind signature scheme. Lecture Notes


[Tri06c] Johannes Trithemius. Steganographiae: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa. Matthiae Beckeri, Frankfurt, Germany, 1606. 8 + 180 pp. LCCN Z103.T84 S 1606. Authore . . . Ioanne Trithemio . . . ; praefixa est huic operi sua clausis, seu vera introductio ab ipso authore concinnata . . . nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Francofurti. Ex officina typographica Matthiae Beckeri,
REFERENCES

sumptibus Ioannis Berneri, anno 1606.


uk/~fapp2/steganography/bibliography/1051.html. Two volumes. Second biennial conference of the Australian Pattern Recognition Society. [TSM95]

[Terry:1988:MSV]


[Tso:1990:NPK]


[Tso:1997:MEE]


[Tokita:1995:LCL]

T. Tokita, T. Sorimachi, and M. Matsui. Linear cryptanalysis of LOKI and s02DES. Lecture Notes in Computer Science, 917:293–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Tombak:1993:ACP]


[Tsudik:1989:DAI]


[Tsudik:1992:MAOb]

G. Tsudik. Message authentication with one-way hash functions. In IEEE [IEE92d], page ?? Three volumes. IEEE Computer Society order number
REFERENCES


[Tsujii:1992:CS]


[Thomlinson:1998:NBP]


[Tual:1999:MGA]
REFERENCES


[Tur41a] Alan M. Turing. The applications of probability to cryptography. Report, GCHQ, Cheltenham, UK, 1941. URL http://home.cern.ch/~frode/crypto/Turing/index.html. This document is retyped from the original (undated?) Turing typescript by the editors Ralph Erskine, Philip Marks and Frode Weierud. Chapters 1, 2, and 6 (of 8) are available; the remainder are in preparation.


Tel:1994:DAI


Tan:1992:NPE


Takagi:1992:MMH


Trabelsi:1994:PPS


Tsiounis:1998:SEE


Tsiounis:1998:SEB

Yiannis Tsiounis and Moti Yung. On the security of ElGamal-based encryption. Lecture Notes in
REFERENCES


Jon Udell. HTTP authentication — worried that anyone can get into your site? authentication is the answer, but not all Web servers do it the same. *BYTE Magazine*, 23(1):89–??, January 1998. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).


Udell:1994:BCRb


USASC:1923:EC


USASC:1940:CML


USASC:1942:ACC


USDOS:1970:BC


USNBS:1977:DES

REFERENCES


Supersedes FIPS PUB 46, 1977 January 15. Shipping list no.: 88-367-P. Reaf-
firm 1988 January 22.

United States National Security Agency/Central Security Service Center for
Cryptologic History. The Friedman legacy: a tribute to William and Elize-
beth Friedman, volume 3 of United States cryptologic history. Sources in cryp-

United States. Dept. of the Army. Operator’s manual for trunk encryption de-
vices KG-94 (NSN 5810-01-187-9909) and KG-194 (NSN 5810-01-283-1395).

United States. Dept. of the Army. Unit and direct sup-
port maintenance manual for trunk encryption device
KG-94 (NSN 5810-01-187-9909): KG-194 (NSN 5810-
01-283-1395) … HGF-94 (NSN 5810-01-083-2896).
Headquarters, Dept. of the Army, Washington, DC, USA, April 1994. ?? pp. Su-


United States. Congress. Senate. Committee on the Judiciary. Subcommittee on
Technology and the Law. The administration’s Clip-
per chip key escrow encryption program: hearing be-
fore the Subcommittee on Technology and the Law of the Committee on the Ju-
diciary, United States Senate, One Hundred Third Congress, second session … May 3, 1994. Senate hearing; 103-1067 103-1067, United States Government Printing Office, Washing-

cryptology. Naval Security Group Command, Wash-
ington, DC, USA, 1995. 12 pp. URL http://
UCC:1996:SRP

USCHCJ:1996:SFT

USPTO:1996:CCP

USCHCSCSTTCP:1997:SFT

USCHCJSCIP:1997:SFT


REFERENCES

G. Meade, MD, USA, 19xx. 6 pp.

[Unixxb]

[USNSACS:19xx:PUC]


[USGSA:1983:ISR]


[USGSA:1994:TIR]


[UNU94]

USENIX, editor. UNIX Security Workshop Proceed-
REFERENCES


[USE93] USENIX Association, editor. *UNIX Security IV*
REFERENCES


REFERENCES


USENIX:1996:PSA


USENIX:1996:PUA


USENIX:1996:USS


USENIX:1998:PUWa


USENIX:1998:PUWb


USENIX:1998:PFT

REFERENCES

proceedings/usenix98/freenix/.

USENIX:1998:SUS


USENIX:1999:PEU


USENIX:1999:PTSa


USENIX:1999:PUWa


USENIX:1999:UAT


USWD:1980:EC

REFERENCES

USWD:1983:EC


USDOA:1989:BC


USCHCJ:1997:SFT


USPBC:1997:AEC


Vadhri:1995:VID

[Vad95] Kumar S. Vadhri. 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

REFERENCES


REFERENCES

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

vanRenesse:1996:OSC

vanDijk:1997:BMC

Varaiya:1999:DSI

Varma:1999:IDD

Vaudenay:1993:FHI


Vaudenay:1998:DFC

Vaudenay:1998:FSE


Lubbe:1998:BMC


Wal:1997:PBR


Venema:1990:IEI


Vedder:1998:ISI


Vedder:1998:GSS


Venkaiah:1992:RBP


Vernam:1926:CPT


Veron:1995:CHI

P. Veron. Cryptanalysis of Harari’s identification
REFERENCES


vanFaber:1997:SDD


IEEE Computer Society Press order number PR08274.
IEEE order plan catalog number 97TB100213.

vanHeijst:1993:NCF


Vigna:1998:CTM


Vincent:1971:PAG


Vincent:1972:CPA


Vandenwauwer:1998:SIE

Voydock:1983:SMH


Voydock:1984:SMT


VanRompay:1998:DCI


Vigil:1996:MIS


Villasenor:1997:CCb


**vanOorschot:1991:CPP**


**vanOorschot:1992:CPP**


**Vogel:1985:LCC**


**Volts:1941:BCP**


**VonZurGathen:1992:PEE**

REFERENCES

VonZurGathen:1992:PEF


Voukalis:1980:DFC


Voukalis:1980:GSE


vanOorschot:1991:KPA


vanOorschot:1996:DHK


Voyatzis:1996:ATA

REFERENCES

Voyatzis:1998:DIW

Voyatzis:1999:PDI

Varadharajan:1997:ISP

Vassiliadis:1988:PEA

Volts:1941:BC
James D. Volts and David Shulman. *Bibliography of cryptography*. U. S. Army, Cincinnati, OH, USA, 1941. 93 pp. LCCN Z103.A1 V6 1941. Typewritten (carbon copy) Three heavy leaves precede sections II-IV (not included in pagination). This copy was made especially for the United States Army from the original manuscript. Third copy: pencilled note on cover.

Contents: pt.1. Cryptogra-
phy; pt.2. Titles relating indirectly to cryptography; pt.3. Rejected titles; pt.4. Author index.

**vanderWal:1997:PBR**


**VanEetvelt:1995:DPF**


**Varadharajan:1997:SSP**


**vanTilburg:1990:MPK**


**vanTilburg:1993:TCP**


**vanTilburg:1994:SAC**


[VV85] Umesh V. Vazirani and Vijay V. Vazirani. Efficient and secure pseudo-


0938-1279 (print), 1432-0622 (electronic).

Vandemeulebroecke:1990:SCB

Verheul:1997:BEF

Vedder:1998:SCR

vanOorschot:1999:PCS
 REFERENCES


Wagstaff:1999:C

Waidner:1990:USR

Waite:1995:BRB

Walden:1900:ADB


Wallach:1994:WP

Walton:1995:IAS

Walther:1998:VBE
Giessen, Giessen, Germany, 1998. iii + 151 pp.

**Walker:1999:CCI**


**Wallich:1999:HSM**


Describes an off-shore credit card fraud scheme that in late 1998 accounted for as much as 4% of Visa chargebacks, and stole as much as US$45M from bogus US$19.95 transactions.

**Walter:1999:MTI**


**Wen-Ai:1994:MTS**


**Wang:1986:UEA**


**Wang:1992:CDS**

Dacheng Wang. Cryptosystem and digital signature scheme based on

Wang:1992:DKT


Wang:1992:DKT


Watler:1989:VAC


Watt:1991:IPI

Wayner:1993:CAS

Wayner:1993:ECD


Wayner:1993:SER


Wayner:1995:PCL


Wayner:1996:DCB


Wayner:1996:DLY


Wayner:1998:MJD


Willcox:1992:TCS

REFERENCES


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.


Three volumes. IEEE catalog number 96CH35919.


Weber:1979:USD


Weber:1993:MDC


Weber:1998:SWY


Wedemeijer:1999:DFM


Weiss:1988:BOP


Weissman:1991:IRA

REFERENCES

Weissman:1991:IRN


Weierud:1994:SPB


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


Wells:1995:DEC


Welchman:1997:HSS


Wernsdorf:1993:OFG


Wernsdorf:1993:ORF


Worley:1994:PST


Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbons. The active badge location system.
REFERENCES


REFERENCES

Wichmann:1990:CMR


Wiedemann:1986:QC


Wiener:1990:CSRb


Wiener:1990:CSRa


Wiener:1996:EKS

for Data Internetworks, W. Stallings.

**Wiener:1997:EKS**


**Wiener:1998:EKS**


**Wiener:1998:PCP**


**Wiener:1999:ACC**


**Wilkins:1641:MSS**


**Wilkes:1968:TSCa**


**Wilkes:1968:TSCb**


**Wilkes:1972:TSC**


**Wilkes:1975:TSC**

[Wil75] M. V. (Maurice Vincent) Wilkes. *Time-sharing com-
puter systems. Computer
monographs. Macdonald
and Jane’s, London, UK,
third edition, 1975. ISBN 0-
444-19525-4 (American El-
sevier). ii + 166 pp. LCCN
QA76.53 .W54 1975.

[Wil80] H. C. Williams. A modifi-
cation of the RSA public-
key encryption procedure.
IEEE Transactions on In-
formation Theory, 26(6):
726–729, 1980. CODEN
IETTAW. ISSN 0018-9448
(print), 1557-9654 (elec-
tronic).

[Wil82] Hugh C. Williams. Compu-
tationally “hard” problems
as a source for cryptosys-
tems. In Secure commu-
nications and asymmetric
cryptosystems, volume 69 of
AAAS Sel. Sympos. Ser.,
pages 11–39. Westview,

[Wil83a] Michael Willett. Trapdoor
knapsacks without superin-
creasing structure. Informa-
tion Processing Letters,
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

[Wil83b] M. H. Williams. The prob-
lem of absolute privacy. In-
formation Processing Let-
ters, 17(3):169–171, Octo-
ber 5, 1983. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

[Wil85] H. C. Williams. Some
public-key crypto-functions
as intractable as factoriza-
tion. In Blakley and Chaum
[BC85], pages 66–70. CODEN
3-540-39568-7. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&spage=66. CRYPTO 84:
a Workshop on the Theory
and Application of Crypt-
ographic Techniques, held
at the University of Cali-
ifornia, Santa Barbara, Au-
gust 19–22, 1984, sponsored
by the International Asso-
ciation for Cryptologic Re-
search.

[Wil86a] H. C. Williams. An
M^3 public-key encryption
scheme. In Advances in
cryptography—CRYPTO ’85
(Santa Barbara, Calif.,
1985), volume 218 of Lect-
ure Notes in Comput. Sci.,
pages 358–368. Springer-
Verlag, Berlin, Germany /
Williams:1986:ACC


Williams:1986:CTU


Wiles:1993:HBE


Williams:1998:SBW


William:1998:C


Winterbotham:1969:SP

F. W. (Frederick William) Winterbotham. Secret and

Winterbotham:1974:US

Winterbotham:1974:USF

Winterbotham:1975:US

Winterbotham:1978:NC

Winternitz:1983:POW

Winternitz:1984:SOH

Winterbotham:1989:US

Winterbotham:1991:US
REFERENCES


Woo:1992:ARC

Woo:1992:ADS

Woo:1992:CAD

Woo:1994:LAP

Wong:1999:DSF

Walker:1996:CKR

Wagner:1985:PKC
Neal R. Wagner and Marianne R. Magyarik. A public-key cryptosystem based on the word prob-

Waldvogel:1993:PDD


Wheeler:1995:TTE


Wheeler:1998:CX


Wright:1998:NTD


Woehr:1997:CRR

Jack Woehr. A conversation with Ron Rivest: How
important is cryptography and computer security? Dr. Dobb’s Journal of Software Tools, 22(10):18–20, 22, 24, October 1997. CODEN DDJOEB. ISSN 1044-789X.

Wolfe:1943:FCCa


Wolfe:1943:FCCb

Wolfe:1943:FCCc

Wolfe:1983:FCC


Wolfowicz:1993:SPR


Wolfowicz:1993:SPS


Wolf:1998:SSAb

Wolf:1999:USC


Woolsey:1990:DDE


Worth:1975:CMA


Wortmann:1987:BRB


World:1996:NIT


Wotawa:1999:NDD


Waidner:1990:DCD

REFERENCES


[Wagner:1997:ASP]

[WS97]

[Wagner:1998:CO]

[WS98]


[WSDK99]

[White:1999:CBA]

[WSFC99]

[Weatherford:1999:NGA]
Margaret Weatherford, Keri Schreiner, Jenny Ferrero, and Crystal Chweh. News: Guide for all seasons: Lancaster’s wireless tourist information system; coins (and billions) back Malaysia’s


Weiss:1985:RCM


Wu:1992:GOC


Wu:1996:SNL


Williams:1979:CAA


Wah:1984:RAM


Wu:1996:SNL


Williams:1979:CAA


Wah:1984:RAM

REFERENCES

Westfeld:1998:SVC


Whiting:1998:EVT


Wu:1993:CSB


Wiener:1999:FAE


Xie:1998:BWB

REFERENCES

[846]

Four volumes.


[XtTmW94] G. (Gozhen) Xiao, Tsung to Tai, and Yu min Wang, editors. *Mi ma hsheh chin chan = Chinacrypt’94: tsan chieh Chung-kuo mi ma hsheh hsheh shu i lun wen chi: 11–15 November 1994 at Xidian, China*. Ko
REFERENCES

hsueh chu pan she, Pei-ching, China, 1994. ISBN 7-03-004363-4. LCCN ????

Xu:1997:BPK


Xu:1997:PCP


Xu:1998:STP


Yacobi:1999:RME


Yahalom:COMPSYS-7-4-451


Yamamura:1998:PCU


Yamamura:1998:PKC

REFERENCES

Yamamura:1999:FCU

Yan:1995:PTL

Yao:1982:PSC

Yao:1982:TAT

Yao:1986:HGE

Yardley:1931:ABC

Yardley:1940:SSA
Yardley:1983:CBC


Yardley:1990:ABC


Yoshiura:1998:VDW


Yeung:1997:DWH


Yeung:1998:DW


Yeun:1999:DSM


Yokokawa:1999:BDE

M. Yokokawa, S. Habata, S. Kawai, and H. Ito. Basic design of the Earth simulator. *Lecture Notes in Computer Science*, 1615:
REFERENCES

269–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


Yang:1997:NEC

Yen:1997:SAT

Yi:1997:NHF

Yi:1998:NBB

Yi:1998:NBO

Ye:1999:CS

Yi:1998:DCB
Yeung:1998:IWI


Yfoulis:1999:SOP


York:1996:BSN


Yourdon:1996:JWS


Young:1997:IJA


Yeh:1991:EIC


Yeh:1999:CCC


Yoshiura:1999:SFU

REFERENCES


**Yshiura:1999:SFU**


**Youssef:1995:RBB**


**Youssef:1995:RBS**


**Youssef:1996:CBN**


**Yu:1992:NTD**


**Yu:1994:KAX**


**Yu:XR-9-1-237**

REFERENCES

Yu:1999:CC


Yuan:1992:VLD


Yuval:1997:RTE


Yang:1997:CBC

[T'ao Yang, Chai Wah Wu, and Leon O. Chua. Cryptography based on Chua’s circuits. Technical Report UCB/ERL M97/6, Electronics Research Labora-
REFERENCES


REFERENCES


REFERENCES

/dlib.computer.org/cg/books/cg1999/pdf/g1036.pdf.


[Zeg93] Erik Zegwaart. Privacy Enhanced Mail in more...

**Zeidler:1979:DDE**


**Zergo:1996:UER**


**Zerovnik:1996:RC**


**Zollner:1998:MSS**


**Zuquete:1996:TAC**

REFERENCES

CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic). URL
http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061171.html


1611-3349 (electronic).

[Yu95b] Yuliang Zheng. On key agreement protocols based

**Zheng:1997:SC**


**Zheng:1997:DSH**


**Zilouchian:1998:ANF**


**Zhou:1994:SDS**


**Zheng:1994:RSS**


**Zheng:1998:HCE**


Reto Zimmermann. Efficient VLSI implementa-

Zhao:1995:ERL


Zhao:1996:DWS


Zhao:1998:BTT


Zhao:1999:DWW

Jian Zhao, Eckhard Koch, Joe O’Ruanaidh, and Minerva M. Yeung. Digital wa-


[IEE97h] Zhou:1999:SPP


[ZMI91] Zhang:1999:AFV


Zheng:1990:CBC


Zheng:1991:DBT


Zolman:1993:BSJ

Leor Zolman. Building a secure journal/logging util-

**Zheng:1993:HOH**


**Zhu:1996:PKC**


**Zheng:1993:PAA**

No slides for the conference talk are available.

Zachariasen:1999:OAE


Zwiers:1998:CTD


Zeng:1990:LCT


Zeng:1991:ILS


Zeng:1991:PBG


Zhang:1995:GCG


Zhang:1996:DCC

Xian-Mo Zhang and Yuliang Zheng. On the diffi-