
Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

02 November 2023
Version 1.110

Title word cross-reference

#1
[Ble98a, Kal98b, KS98a, RSA93f, RSA93a]. #10 [Kal98c].
#3 [RSA93b]. #5 [RSA99b]. #6 [RSA93c]. #7 [Kal98f, Kal98d, RSA93d].
#8 [RSA93e].

((2^m) [PSR97]. (2^n ± 1) [Zim99]. (k, n)
[KOO95b, KOO95a]. (t, n) [LWC96]. +
[Zhe97b]. $1 [Gar97b]. 1 [JV98b].$

$1-Million [GC97]. 128 [Ano97-51]. 16
[BS93a, GC94]. 2
[JV98b, KG95, Kob91b, MVZ98, SBVG99].

$29.95 [Hat96]. 2n [QG90]. 2R [YLD99]. 3
[Ben99, BALS99, CK95, KSW97b, Nas94, TK99, Wor96, YY99a]. 40 [Ano97-41]. 511
[CC98]. 64 [MMi97]. 8 [Miy90]. <=
[Zhe97b]. 2 [TZ94]. x [Hol91]. A [BMT96].
A * B (mod N) [Bak92]. A^2 [JS95b].
mod2^2 [Ber93]. c [WD99b]. \chi^2 [HG97b]. d
[BD99b]. \ell [BR91]. f [DYL93]. F_{2^n}
[SS98a, Ler97]. \mathbf{F}_p [Miy93a]. GF(2) [She95c].
GF(208) [Ros98a]. GF(p) [Gor93b, HNM98].
> [GQW+91]. k [Car97c, DJL93, HKS97a, HKS97b, KR99b, KS97b, WD99b]. t
[HL93a, KS97b]. L2 [Vau99a]. \lambda [RS99c].
L \geq 2 [HV91]. \ll [GQW+91]. m
[Bla94a, FR94]. \mathbf{Z}/n\mathbf{Z} [MM96b]. \mathbf{Z}_n [SE96].
GD(2^n) [Ara93]. GF(2^m) [FBT96]. \mathbf{F}_{2^m}
[MVZ93]. \text{Step}_{e,m} [GC90]. N
[BS91e, BS91d, HKS97a, HKS97b, KSW99b, KSW99d, KKS98, Per93, QG90, Tak97].
N = p/q [BDHG99a, BDHG99b]. N^{0.292}
Adalard [Sha99a], *Algebra* [BK94a, Pes97, VG99, CMM93]. *Algorithm* [ANS97, Ada97b, IBM93, Ano96c, Ano96f, ADEDS99, COP+95a, CD91, DKR97b, DNR97, Dra98, GX99, GK98, GTG94, GN95c, HG97a, HG97b, HWJ98, Kal91, KY95a, KR96a, KY98, KMK99, Kobs98, Kra93, Kwa97, MD98, MW94, Mas94, Mat97, Mis97, MS90b, Mou99, Nat97b, PBGV90, PRB98b, Riv92a, Riv92b, Riv95c, Riv95b, Riv98a, RC94a, RC94b, RH99, Sch93d, Sch94f, Sch95a, Sch95b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SS99c, She94b, SB98, SW93, Sta99b, Swa94, TK99, THP+98, VR98, Whe94, Yin97, ZY991, Ano+97-41, BI94, BS95a, Bow93, CC98, CGV94, ISO97, IKNY98, JMLW94, KY95b, KY97, KYxx, Kir95, LRW93, LZ90, L91a, L91b, Lon91, LC97b, MSS99, Mey99, MPL99, Mo98, Pai96, Riv90a, Riv91b, Riv95d, Sch91a, Sch94i, Tay94, V95, WN95, YL95b].

*Algorithm* [ZW99, ZPS93, AA95, Acc97, LL98a, Moc97, OA94, Sch93b, Sch94e, See97, Sim93, Sta99b, WSK97a, WSK97b].

*Algorithmic* [THP+98]. *Algorithmic* [ACM97b, ANS97, Ano95a, Ano95b, Ano96b, Ano97c, AMP99, Ate99, BS99a, BP98a, BR96a, Bas98, BGM97a, BGM97b, BL96b, BL96a, Buc91a, DVG92, FCD98, G99c, Gl99a, HEQ98, KM99a, KAK96, KB92, LC99, Lei99b, L99d, M97a, P97, PA98a, P939b, Por98, Pre97a, P989b, P989a, Q90, R98a, Sch94g, Sch94j, Sch94c, Sch96a, SW97a, SW97b, Sch94h, Sed92, Sed93, Sho97, Sot98, SB99, Sp95, Ste96, VCF+90, AA95, Ano90, Ano98m, CPP98, CMM93, CJL+92, CadHSV96, DG96, DN95b,
USE98a, USE98b, USE99a, Wie99, Yu92.

**AUSCRYPT** [SP90, SZ93]. **Austin** [Ano94c, IEE98e]. **Australasian** [SPM97].

**Australia** [DG96, GN95b, KG93, KK99b, MSD90, PSN95b, SP90, SZ93, VPM97].

**Australian** [CFK +91, GN95b, Cae96a, Orl96, Ree97].

**Austria** [BS95e].

**Authenticated** [BF97a, BWM98, BWM99a, Bor95, CHH97, Dan95, HCY96b, JV96, LC97a, Mau97a, RH93, SKWH96, BSNP96a, BSNP96b, BF99b, BR97b, DwW92, HY98b, HY98a, Yeu99].

**Authenticating** [ADSW99, Hel98a, KS96a, Mit92a, SK96a, Sha97, LC94].

**Authentication** [ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94k, AS96, Atk95a, AR98, AC97, BA97, Bak99, Bal99, Bec99, BR97a, BG90, BR94a, BCK96d, BCK96e, BM91a, BGS98, BR91, BBDF97, BGH +91, Bis91, BHK +99, BWM98, Ble98b, BV98b, Bor96, Bor93a, Bor93c, Boy92, Bru98, BAN90, CV93, CGM97b, COZ99, DLF97, DVPL92, DW90, DY91f, DwW92, DH90, Dra99, DMFB97, DS97d, Dw95v, ECM96, EPR99b, EPR99a, FGS96, FHBB +97, FL96, GYH90, GLZ99, GL96, Geh94, Geh59, GN94, GM90, Gol90a, GBL94, Gu98b, Gui97, HK97, HA94a, HS94, HL92, HI97, HJP97, HP98b, Ins95, IH98, JS94, Joe98, Jol94, KR95b, Kau93, KA98a, Koh90, KN93, KCCT94a, KCCT94b, Kra94b, Kra95, KBC96, KBC97, Kur94, KK95, KYG92, KY932, KS97c, LABW91, LABW92].

**Authentication** [Lee96, LW91, Lie93, Lim93c, Lin93a, LS92, MB94a, Mau96a, MAM95, Mc96, Mee98, MS95c, MS95d, MWW94, MVTZ92, Mor97, Mye94a, Mye97, NP97, OG97, OOK91, OM94, Opp96, PKOT94, PS88e, PLWSN99, PSN91, PGV93c, Pre98a, Pre98c, MS95e, RS99b, RRSW97a, RRSW97b, Rog95, SNT93, SN93, ST94, SNT95, SNW98a, SNW98b, SSH93, SS96, SP99, SA95, SC96a, SCxx, Sch94d, Sh99k, Sga90, Sga91b, She97, She95a, Sha96, Simon96b, SVxW91, SW94c, SKAM99, St91b, SL99, TAP90, TA92, Tay95, TSN93, Tun99, Ude98, Van95b, Van93, Wal95, WKHG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC +98, Ano95g, Ano95o, Ano95x, Ano96v, Ano96x, Ano96y, Ano96-27, Ano97d, Ano97t, Ano97p, Ano97-27, Ano97-43, Ano97-53, Ano98s, Atk93]. authentication [BSNP97, BGR95, BCK98, BCKxx, BCB97, BGH +95a, BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gua90, HS96b, Hor95, HC95b, HLL +95, HW98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin98a, Low95, MS97, MF97, Men91, MC96, Nac93, NT94, PS98e, PS98f, PS98h, RS98a, RS98f, Sch99, Sga91a, Sga93, SY96b, Sta99b, Sti91a, Sun98b, Sve93, Tsu92b, Tsu92a, TH99, Ver98b, Web99, WL94, XA98, Xie98, YL97a, YL97b, Yon97, Zhek98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a].

**Authentications** [OO90, KSL92].

**Authenticator** [Zuk98a]. **Authenticators** [DF91a, SN96].

**Authenticity** [BK90, Lud97, Ano99i, MI90, Way91].

**Authenticide** [Fly97]. author [Lea90].

**Authorisation** [COZ99]. authorities [Ame95, Ame96a]. authority [CFSY96, CGS97, JMO95a]. Authorization [BDPSN95, Cas95, FL96, Woo90]. Auto [YY98c, YY99b]. auto-certifiable [YY98c].

**Auto-Recoverable** [YY99b, YY98c].

**Automata** [BI95, BDG98, Go92, HHW99, KPR99, KV94, MC92, NO97, vWN99, Bao94, BI94, BKK +97b, BK98b, DYL98, NKC94, Siu99, CK +91]. Automated [Dan97, FIP93a, FSN93, FKK99, GSN94, GDS91, She96a, SGPV98, VDDR99, WG99, CD98a].

**Automatic** [CWM +91, MM99a, Na97, SK97b, SK97a, Sch99k, WKHG97, DF98, OA99].

**Automating** [Bur99, Sni93a].
Automation [Des99a]. Automaton [DGV93, Gys96, MZI98, Tao94, TCC97, TC99b]. automorphisms [VP96].

Autonomous [CKN99, RZ99].

Autoscritcher [Dea98a, CF92, Cra92]. aux [Bec90]. Available

[DDJ98c, Ano97n, Ano97-32, Ano97-46]. Avalanche [Cus96, CS96c, HT95, O'C94, ZZ95, ZZ95b, YT96]. avant [Blo98a]. AVBPA [BCB97]. Average [AD97, AD99]. Avoided [NMR95].

Avoiding [ZW99]. Award [DDJ98b]. Awarded [Eri97a]. Aware [BCCD99]. Away [DDJ99].

Axis [AK99]. AXYTRANS [GBC93]. azo [SBTV99].

b [Cli97, UU97b, Ano99f, HS90, Lam99]. B-Trees [HS90]. Babbage [Fra93, KT99]. Babbage

Back [GC97, GO96c, WSFC99, EIE99e, WG97]. Backup [Mah96]. backwards

[BKR98a, BKR98b]. Bacon [Lea90]. Badge

[WHFG92]. BAG [Ano97-33]. Baker

[PS96b]. Bal [IPNdibbprn91]. Balance

[RG99]. balanced

[MD99b, YT95a, YT95b]. Balatonfured

[Rue93]. Balkanizes [Mad99a]. Ballot

[CFSY96, BT94]. Ballots [Sal91]. Baltimore

[ACM90, Ano96a, NIS92, USE92b]. Ban

[Gar79a, BP98f, XZZ97]. BAN-like

[XZZ97]. Bandwidth

[Bla96a, Bla96b, JMP+98, MM92b, Sim98b]. Bandwidth-Efficient [JMP+98]. Banking

[Ch192, Ano98k]. Barbara

[Bri92, Bri93, Cop95b, Cop95d, Des94b, IEE97h, IEE97j, IEE98d, Kal97c, Kob96, Kra98, Sti93b, Sti94, Wie99]. Bargaining

[Nur94]. Barrier [BGK99]. Barriers

[Des92, RCM99]. base [SPP98]. Based

[AW94, ADEDS99, BDPSNG95, BG90, BJY97, BS99b, BS99c, Ben99, BLM94, BBT94, BMT96, Bie98, BPR99, BMS94, BM96b, BM96c, Bla89a, BPRF99, Bla98a, Bla98b, Bra95b, BP97c, CC99b, CJ991, Cre97, DGV93, Dae95, Dan95, DDNM98, DSSB95, DS96, DDP90, DMPW98, DDGM97, DDG94, DD94, DP90, DF99, EKLM99, EN98, ENK99, FCH99, FBS97, F999, FKM98, FJ+96, FSB98, FR95d, GK97, GJ999, GRB99, G95c, Gys96, He97, HPS98, HJP98b, J997, Jia99, JSZ94, JJ99a, KKS97, Ke98e, KR98, K093, KG95, KP96a, KP97, KM99b, KA99, KMOV91, Kra94b, KH98b, LM93a, LM93b, LYH93, LL97a, Len99a, LW91, Lin98, MNSV97, MD99, MR95a, Mau93a, MM96a, MM99b, MM99b, MG91, MM98a, Mue99, MM98b, Mil99, M95, NM99, NOVY93, NS98a, Nec96]. Based

[NS97b, NMV98, OMV98, O093, OFF93, vO91a, Pai99d, Pen96, PL94, PR99, Poi99, PB99a, PV98, PK99, Pre97a, PM99, RSA99b, Ros98a, SS98a, SCT99, SC96a, SPS97, SE96, SJS98, She92e, Sho96, SM91, ST91, SS99, SKT99, SZT98a, Var99b, W995, WD99b, WS99, YK94, YY97b, ZL99, vO91b, Ala93a, AW95, A098, AAPS92, Ano98k, BSN96a, BSN96b, BSN97, BDC98, BCD98, Be97a, BBI90, BBC97, B97a, BBL95, BFKL94, BCC99, CC99a, CPS95, Cha95a, CW97, CS97e, CCH98, CLL99, CD95, Cus95, DD95, FSS94, FGY69b, FGY96a, GM91, GH99, GK95a, HZ93, HY93b, Has99, HSW96, He92, HI97, HLMW93, HXMW94, HMP95, HW98a, HJP98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JJ95, JC95, JC90, JY98, KM99a, KSL92, KM99d, Koy95]. based

[Kuc92, KH97, KK96, LRW93, LvdLB96, LS98a, LH99, LZ90, LCl95, MRS99, MS98a, MLA91, Mau91b, McH92, MZ98, MM95, MTN97, Nu92, MV98, NS97c, NR95, OP+99, OU98b, Ole95, Pat91b, Pat91a, PS97, PC98, PGCSN96, PPBC97,
Por93, PGV91, PGV93b, PGV94, RP95b, SV94, SV95a, Sha94, SRL98, Sim98c, SM90, SS95b, SS95c, SMK98b, Son99, SKD94, Ste95, SS98b, SRT98b, Tan90, TA97, TAP90, TC91, VNM99, Ven92, Wan92a, WKHC97, Wi93a, WHH95, XA98, WYC97, YL97c, Zhe95b, ZPY96, vO92, vT94, CD96, YKY99, Dhe98, Por93, TY98b, TY98a.

Bases [BCE+94, MSDS90, Yua92].

Basic [CF99, Des98a, vdL98, OK98, YHKI99, Zie97, van98, BDHJ97, Rac90, dVdVI98, Hel98b].

Basics [Bal99, IEE97e].

Basis [FBS98, LL99, The95, Wal98, BK98g, Car98, FBT96].

Batch [BGR98a, BY93c, BY93b, BFP99, Fia90, Fia97, BGR98b, YL95a].

Battle [Ban93, Gar97a, Gar97b, Gar98b, SB97, Ano96n, Fro96].

battleships [Jar97].

Bayesian [BBDF97, Jen99].

BayRS [Ano96x].

BCH [CC98, FC94].

Be [BF99a, BV98c, Cha93, CD98b, DQ93].

Begin [FJM+96, Rit99, Bax97].

Better [BF99a, Cha93, DQ93].

Between [BFS96, Mar98b, MW99, RCM99, SZZ95c, BS99b, BS99c, BMS96, CV95, Ga99, HT99, IKM99, Kem99, KT99, KM99c, LC97a, Mat95, Pes97, SI93a, ZMI91].

Beyond [BGK99, FKM98, Fu99, Gar98a, G99a, Opp97].

Bi [FOO91].

Bi-Proof [FOO91].

Biased [BN96, TSY98, Ueh95].

Bibliocryptography [Boo96].

bibliography [Lie93, Sab94].

Bicentenary [CFK+91].

bid [Ano94i].

bidirectional [Mit92a].

Big [Hat96, Wai95, Ho95, Kal93b, Des96a].

big-number [Kal93b].

BigDog [FL96].

bigraph [SBG99].

Biham [Ada92b, KSW97b, KSW97a].

Biham-DES [KSW97a, KSW97b].

bill [Mad99a, Mad97].

Billion [Gar97b, Ano99g].

Billion [Gar97b, Ano99g].

Biology [BHJM99, Ram92].

Biocomputing [DDJ98b].

biography [CFK+91].

BIND [FOO91].

biochemistry [Ram92].

biometric [Got99].

Biometrics [Got99].

Biometric API [Got99].

Bipartite [PS98a].

bipartite [PS98a].

Birth [Sch98a].

Birthday [BGK99, Jun98].

bis [SM98a].

Bisimulation [AG98a, AG98b].

Bit [Bar99, CWM+91, DF92, IOS94, MS99, PF94, QG90, Sal98, SKW+98b, SS91, ZYWR91, Ano97-41, Ano97-51, Bro97, DKB97, HNM98, ISO97, Knu98c, Lim98, Luc98a, Luc99a, Luc99b, Mey99, MMI97, MLLG95, PC98, Sch94b, SKW+98c].

Bit-level [DF92].

Bit-Sliced [PF94].

Bits [BV96, BDF98, FS97b, VVDJ90, Ano97v, Ano99g, CDEH+96, HN98, CH94b].

Bistream [HG97b].

Black [BL96b, BL96a, SV94, SV95a, Yar90, YY96, YY98d, YY98b, BD98b].

Black-Box [BL96b, BL96a, YY96, YY98d, YY98b].
Blacklisting [KRS99]. Blackmailing [Jak95]. BlackNet [MLLG95]. Bletchley [Ano97-48, Sal93, Cla98c, HS93, Smi98b]. Blind [CP59, Eri97b, JLO97, LD99, LR98, NVE99, NVM99, Oht98, PG97, SY96a, SYI98, HMP95, Tra97, XA98]. Blindfolded [JY96]. Blinding [Bra95c, Kra99, FY95c]. Block [AB96a, ABK98b, ABK98c, BKR94, BAK98, CDN98, Cle91, CJM95, DVD94a, DMR97b, DMR97a, DR99a, DNN98, De 99, DW94, J97, J98, KR94a, KV99, Knu94b, Knu95a, Kn98b, Kn98c, Kn99b, Koj99, LM93a, LM93b, LM91b, LM98, LM99b, LM99c, Luc98a, Luc99a, Luc99b, MNSV97, Mas94, Mat96a, Mat97, MT99a, MSK99b, Pat99, Pre97a, QG90, RRS98, Rob95a, Sz96, Sch94b, SK96c, Sk96d, SKW+98b, SKW+98c, SKW+98e, SKW+98f, Sch99d, Vau98b, V96, YL98, YLC98b, ZMI90, Zhe90, Ala93a, AW95, BKR98a, BK98b, B93, BS95a, Har96a, HLMW93, HXMW94, IS97, Jak99a, KL95b, LM91a, Lai92, Me94, MM97, NO96, Nyb95, PGV93b, PGV94, RT93, RP95b, Roe95, SB95, SAM97, SHK99b, SKD94, TY94, YL97c].


[Fra99, Hir97, Hir98, Don98, Hin93].

**Broadcast** [ASW99, Ber91, BC95c, BC96a, BFS96, vD97, FN94, GSY99, KYDB98, LS98b, SW99b, WD99a, BMS96, BFS98, GBL94, Sta97a, SW98, SW99a].

**Broadcasting** [CW91a, CWY98, LC96b, CC95, HLLC96, LHW99, YY93, LC96c].

**broke** [Dav98a].

**Broken** [CP91, Mey99, MLLG95].

**Bronze** [Duh90].

**Brother** [Wai95, Hof95, Des96a].

**Brothers** [Hat96].

**Browser** [GW96, Law98, She96b].

**Browsers** [DDK98].

**Browsing** [GGMM97].

**Brute** [CD98c].

**BSA** [Bar97].

**Bucket** [Rog95].

**Budget** [UU97a].

**buffer** [Mei98].

**Bug** [DDJ98c, Ano98t].

**Builder** [Pin98].

**Building** [HWKS98a, HWKS98b, Hat96, Hof95, MAM95, NT99, Wai95, Yor96, Zol93, FB97, NIS92, PV99, T98].

**Bulk** [SVBJ96, Whe94].

**Bulk-FFT** [SVBJ96].

**Bull** [Taa98].

**Bulletin** [CWM91].

**B¨ulow** [CWM91].

**burden** [Wil98a].

**Bureau** [Uni97d].

**bureaucracy** [Rat96].

**burglars** [Way95].

**Burlington** [IEE96a].

**Burns** [DDJ98b].

**burst** [Ch93a, UN04].

**Bus** [CC99c, Kuh98].

**bus-encryption** [Kuh98].

**Bused** [FVEA99].

**Business** [Ano93i, Ano96-29, Ano97-30, Ano97-33, Ano98t, AMP94, Av98, C99f, BC99, Li94, MB99a, SM99, Uni98u, ZKL98, B+96a, Kir95, Uni98k].

**Businesses** [MB99a].

**butting** [St98].

**buyers** [MB99a].

**Byte** [Mas94, PV98, YLCY98a, YLCY98b, CFR91].

**Byte-Oriented** [Mas94, YLCY98a, YLCY98b].

**Bytes** [Yuv97].

**Byzantine** [Bea92, Bor95].

**C** [Sha99a, vDWS97, vS97, Bak92, Bas98, BMS99, DSB99, Gar98b, He98b, Kali92, MGL98, Sch94a, Sch96a, Sch94b, Sc92, Ste90a, Ste90b].

**C0YNTHIA** [WBB99].

**C2** [St98].

**CA** [RD99a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE90g, USE96b, W199].

**Caching** [STSW99].

**Cactus** [Ano97-33].

**CADE** [HB99].

**CADE-16** [HB99].

**cAESar** [Koe99].

**Calculating** [CFK91].

**Calculation** [HRV99].

**Calculators** [CWM91].

**Calculus** [BLS93b, ACM98a, Ano97a, Ano96-29, Ano96-30, Ano97-33, Ano98t, AMP94, Avo98, CFK91, Chr99b, G99d, Lom97, RBC99, Sch94j].

**came** [Fro96].

**Camera** [Fro96].

**Camera** [Fri93, SKW96].

**Campbell** [CFK91].

**Campbell-Kelly** [CFK91].

**Campus** [VNW94].

**Can** [Ano93c, BF99a, CP91, Cha93, CD98b, CMY97, D91f, Ev91, G99b, NMR95, NMR95, H98b, Sim98c, Ste95, BGV97a, CG95, Ev92, Ev93, LF97, NOV93, Sch91b, Ude98, Way95].

**Canada** [ACM94c, CFG96, GS94b, HA00, IEE94f, IEE96d, TM99, Yua92, Rob98b, T98].

**Canadian** [CFG96, GS94b].

**Candidate** [Bas98, BCA94, Dra98, GL98, Gla99a, H98b, M99, Nat97b, Nat98, Nat99b, Out98, RD99a, RD99b, Sot98, SB99, GGH98].

**Candidates** [Bih99c, Cla99, HKQ99, Koe99, Rob99, Sha99b, Vau99d, CJRR99b, Kea99].

**Cannot** [BCE94].

**Can’t** [WT99].

**Cap** [Lea99].

**capability** [BC96a].

**Capacity** [B99, FVEA99, Gar97a, Gar98b, MM92a, NNEK97, VNW95, Uni96a].

**Capstone** [YY96].

**carcinogenic** [SBT99].

**Card** [Bov98a, Bov98b, Chr99a, DV96, ENK99, Gar97a, GPSV98, HP98a, Hru96, HH99, Hus99, Kra99, Mar98a, Omu90].

**SGPV98, Sut99, T+99, dWQ91b, dWQ91a, dWQ91c, dWQ91d, dWQ91e].
AHdJF97, Ano96g, Cha99b, CW97, Cha91, Di 97a, Di 97b, Kip97, Sha95a, Taa98, GPSV98, Bar99, Bro97, HNS99, SM94, SKAM99. Cards [Ano96e, Ano99e, BDB92, Cha99a, CM99c, Con98, Con99a, Cor98, CH99a, DDJ98, DDJ98b, DDJ99, Deu97, Deu98, Fan96, FW91, FGLP96a, FGLP96b, FOM91, GL96, Gut98a, HKQ99, JT97a, Koe99, KCC94a, KCCT93b, MS99, Mye96, NM96b, PV98, Roh99, SKW+98d, SS99a, Sch90b, SR96, Smi98a, Taa98, ABKL91, ABKL93, Ale97, Ano98q, BVG97a, Bro97, CRR99b, DSG98a, Dg98b, DT97b, DF97, Gau97, T97a, AG99, Bak99, BF99a, Gir99, GST96, LW99, NF99]. cardT0AP [SGP98]. Cards [Ano96z, Ano99e, BDB92, Cha99a, CM99c, Con98, Con99a, Cor98, CH99a, DDJ98, DDJ98b, DDJ99, Deu97, Deu98, Fan96, FW91, FGLP96a, FGLP96b, FOM91, GL96, Gut98a, HKQ99, JT97a, Koe99, KCC94a, KCCT93b, MS99, Mye96, NM96b, PV98, Roh99, SKW+98d, SS99a, Sch90b, SR96, Smi98a, Taa98, ABKL91, ABKL93, Ale97, Ano98q, BVG97a, Bro97, CRR99b, DSG98a, Dg98b, DT97b, DF97, Gau97, T97a, AG99, Bak99, BF99a, Gir99, GST96, LW99, NF99]. cardT0AP [SGP98]. Carl [Ano96h, Ano96s]. Carmichael [Pin97]. carrier [SVWMB95, SOB98, VSB95]. Carry [SM91, DF92]. carry-save [DF92]. Cartesian [DVW90]. cascade [BCK96b, BCK96c, YL93]. Cascades [GC90, Men95b]. Case [ABDV98, BY93a, BGC94, BR95b, BGM97a, BGM97b, BPR99, DSS9b5, Duh90, F99b, FR95d, GRR99, GM99a, LBHM99, Mad92, MD99, MR95a, Mar98a, PK99, Riv98c, Var99b, Ad97, AD99, BHR99, DL93, LMS97]. Case-Based cascades [DSS9b5, FR95d, GRR99, MD99, MR95a, PK99, Var99].
changeable [HYLT99]. changing [MW98a].
Channel [AO96, AVPN96, ADEDS99, BI99,
Bro94, KSWH98a, KSWH98b, KSWH98c,
MM92a, MM92b, OKST99, WB92, BM95,
FC94, PSB97, P995]. Channels
[BDI+96, Cre97, Des96a, vD97, Ki97, Lip94,
MM96a, MK94, MM94, PN92, SF94, Sch94e,
Sim93, Sim96a, Sim97, VNW95, WD99a,
Des96b, Gmu98, Man91c, SF93b, Sch93b,
Sim94c, Sim98a, Sim98b, Tod97, YL97a].
Chaocipher [Joh98]. Chaos
[BGR94, BLM94, Ano96-29]. Chaotic
[Bih91, GKS97, HNSM91]. Chaotic-Map
[Bih91]. CHAP [Sim96b]. Chapter
[Kal97b]. chapters [Tat98, Tat99].
Character [BL99, Sab94]. Characterisation
[SB95]. Characteristic
[KMKH99, Koe91, MVZ98, SS98a].
Characterization [FY97, Sti91a]. Characterizing
[IPNd98]. characters [Lip98, KT99].
Charlesworth [CWM+91]. Charing
[Atk93]. Chasing [Gar97b]. chausses
[Sch98e]. chausses-trappes [Sch98e].
Cheap [LT98]. cheaper [Sch98c]. Cheaply
[Ano93j, Str93a, Str93b]. Cheater
[KOO95b, KOO95a, LH93b, HC96, HLC96].
Cheating [GF99, Rab94, OK96b]. Check
[BK95c, Bto98c, Tay94]. checker [Dan97].
Checkers [Fis97, KA91]. Checking
[BGR98a, Bol98a, Bol98b, BDL97, FL99b,
FGY96a, GMV98, PV98, BCR98, FGY96b,
MHPS96, MW94]. Checks
[DT98a, PK95a, PK95b, Pen96]. Checksum
[PBGV90, LRW93]. Chen
[Ala97, Bur94a, Bur94b]. CHES [KP99b].
chi [XtTW94]. chio2 [HG97a]. Chicago
[USE96a, USE99c]. chieh [XtTW94]. chin
[XtTW94]. China
[HOQ97, OiDP98, XtTW94]. Chinacrypt’94 [XtTW94]. Chinese
[DiDPS96, GO96c, QD91, WHHW95, Yu99].
Chip
[Ban94, Bro96, Ele98, Gar97c, GC97, Got99,
HMvT94, Lan97, MPPS95, MHW98,
VVDJ90, Wai93b, Dyan96, Kau96, Kau97,
Pos98, RPD94, Sim94a, Uni95a]. Chipkarte
[Kip97, Kip99b]. Chips
[Ano99c, GO96c, Omu90, Ano97-49]. Ciphertext
[Ano99c, Vai95a, Vai98a, Vai98c].
Chosen
[Ble98a, CG99, CS98b, Dam91b,
GC94, KSW98a, KSW98b, LL94a, PBYV90,
RS91, ZS93, BJ97, CF94, NY90, SNT95,
Sah99, SG98, Tze99, vT93].
chosen-ciphertext [Sah99].
chosen-content [SNT95]. chosen-message
[BJ97, Tze99]. chosen-plaintext [vT93].
chronicle [UFCC94]. chronology
[Kah98a]. Chua [YWC97]. Chump
[WA99b]. Chung
[XtTW94]. Chung-kuo
[XtTW94]. Church [Ole95]. CINDI
[DSSZ99]. Cipher
[Alv98c, AM97, ABK98b, AK98c, BKK94,
B989, BD94, Boy90, BCA+98, Car97b,
Cla97, Cla98a, CJM95, DGV94a, Dae95,
DK97b, DK97a, DW94, EM93, Gol97d,
KR94a, KMA+98, Kmu98c, KR99a, Kuh98,
Lim98, LS97, Lip99, Luc98a, Luc99a,
Luc99b, MN97, MD98, Mat94b, MTT99a,
Mau91d, Mlu96a, Miy91, MSK98, MSK99b,
PA98a, QG90, RDP96, RRSY98, Ros98a,
SZ96, Sch94b, SK96c, SK96d, SKW+98b,
SKW+98c, SKW+98f, Sch98i, Sch98i,
She94b, SMK98a, Van98d, WBY98, Y96,
YLH98, YL97a, YL97b, YL97c, Zun98,
SV98, ERS99, Vau99b, Vau99c]. Ciphers
BSB97, BII3, B185, CC98, Cha95a, CMM93, FC94, Gre90, JM96a, Kah91a, KO95b, LYG94, LMS90, MSS93, MPL99, Moh92, SNT93, SNT95, Ste95, Sti91a, Su98, SS98b, TSN93, TY94, Wan92a, Wel97, Win93, YL97a, vT94, JS95a.

codewords [PS97]. **Coding** [Ber96b, IEE97e, KRS99, KH98b, LW91, Lip94, Sch99b, She94c, SW95b, Van95b, Wal99a, Ada91, Boy95a, Boy95b, Dar97, DiDP96, Far93, Gan93, KSB96b, KSB97, Kuo90, Mit92b, Sab94, Sch98b, Sga91a, SVWMB95, SOB98, S1p99a, SMS99, TA97, Ger97].

coefficient [GK95b]. **Coevolution** [Nac97].

**Coffee** [Deu97].

cognitive [CF99, Ger99b, MMM+98, PUF99]. Cohen [PBGV90].

coin [BN96, Jue99, PW97e, Ueh95]. **Coins** [EO95b, WSFC99, EO95a].

**COIRS** [YKY99].

cold [Joh95].

**Collaborating** [CF99].

collaboration [KT99].

**Collaborative** [BV98a, Neu91, LS98a].

colleagues [Gla99b].

**College** [Far93, IEE97a, UFC94].

collision [BP97a, Dob97, PGV91, Rus93b, Vau93, vW94, vW99, Dob95a].

**Collision-Free** [BP97a, Dob97, Rus93b, Vau93, Dob95a].

**Collisions** [Ano95a, CJ98, DBGV93, dB94, Gon95, Sim98c].

**Colloquium** [Ano97-28, vWN99].

**Collusion** [BS95b, BS98, EKK99, PW97b, LM96].

**Collusion-Resistant** [EKK99].

**Collusion-Secure** [BS95b, BS98].

**Colony** [BP95a].

**Color** [ADEDS99, NNEK97].

**Colorado** [Sch99b].

**Colossus** [Ano97-48, Car97b, Car97c, Car98, Pin98].

**Column** [Bra94a, Dwo95, Bra90b, Bra90d, Bra95d].

**columnar** [Bar92a].

**COMANDOS** [TCH+91].

**Combatting** [DN93].

combination [Rev91].

**combinational** [Hil94].

**combinations** [RT93].

**Combinator** [SAS99b].

**Combinatorial** [FK94, KO95b, KO95a, KO96, KO97, LS98b, Rus93a, Sti91a, Zie97, FSS94, Sta97a].

**Combinators** [MWW94].

**Combiner** [SG99a].

**Combiners** [MS91].

**Combining** [MKMH99, NA95, SA95].

**comes** [Fox98].

**command** [Mye94b].

**Comment** [DKKK98, LC96c, YT96, BMP97a].

**commentaries** [Ano97-37].

**Commentary** [BL99].

**Comments** [BMP+97b, COP+95a, Dun94, JW01, KSS+92, MC96, NC97, Ng99, Pre95b, SB93, WHL99, Aia97, Gilb90].

**Commerce** [Av98, Cli97, DDJ98d, DB99, Jak99b, LHB96, Lut98, Uni97a, USE95c, USE96d, USE96b, USE96b, Uni97d, Ano98h, BH98, FB97, Gar97b, LM98a, Man95, Sin98, Tas98, VM96, UV97b, Uni96b].

**Commercial** [Bhi96, BDR+96, Cae96a, WLEB96, Cha94b, D1x94, Joh90, Sta94a, JMLW94].

**Commitment** [Dam99a, IOS94, Sal98].

**Committed** [DF99].

**Committee** [Uni97b, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k, Mad96, Uni98c].

**Commodity** [Bea97a].

**Commodity-based** [Bea97a].

**Common** [IBM91, Lin93c, Mau93a, Tze99, JDK-91, JD91, LJM93].

**Communication** [??97, AR99, BF97a, Bet95b, BFS96, CHH97, CMM99, FJP96, FK99, FT99b, IKM99, Jam98, KFJP96, KRJ98, PW99, PM99a, SSN98a, Sim94d, WD99a, We99, BF99b, Bet95a, BMS96, Com97, CWY98, CK93, Cli97, DFKN93, Hamxx, Rivxx, Sch90c, Sch97c, SD97, Sta97a, UU97b, Ven92, Wir98b]. **communication-privacy** [CK93].

**Communication-Storage** [CMN99].

**Communications** [ACM93a, ACM94a, ACM97a, Ano93h, Aur96, IEE94f, IEE97k, KM93, Kat97, MB94b, Ved93, BY93c, BY93b, Car94, Cha94b, Cra96, HOQ97, Hwa93, IEE92d, IEE95c, JC93, Mil95, Oht96, PP96, Par96, Rhe94, SW94b, Sch93a, Sch92c, Szw97a, ZG96].

**communicators** [Ano97-28].

**Communities** [FB94, KO95b, KO95a, KO96, KO97, LS98b, Rus93a, Sti91a, Zie97, FSS94, Sta97a].

**Combinators** [MWW94].

**Combiner** [SG99a].

**Combiners** [MS91].

**Combining** [MKMH99, NA95, SA95].

**comes** [Fox98].

**command** [Mye94b].

**Comment** [DKKK98, LC96c, YT96, BMP97a].

**commentaries** [Ano97-37].

**Commentary** [BL99].

**Comments** [BMP+97b, COP+95a, Dun94, JW01, KSS+92, MC96, NC97, Ng99, Pre95b, SB93, WHL99, Aia97, Gilb90].

**Commerce** [Av98, Cli97, DDJ98d, DB99, Jak99b, LHB96, Lut98, Uni97a, USE95c, USE96d, USE96b, USE96b, Uni97d, Ano98h, BH98, FB97, Gar97b, LM98a, Man95, Sin98, Tas98, VM96, UV97b, Uni96b].

**Commercial** [Bhi96, BDR+96, Cae96a, WLEB96, Cha94b, D1x94, Joh90, Sta94a, JMLW94].

**Commitment** [Dam99a, IOS94, Sal98].

**Committed** [DF99].

**Committee** [Uni97b, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k, Mad96, Uni98c].

**Commodity** [Bea97a].

**Commodity-based** [Bea97a].

**Common** [IBM91, Lin93c, Mau93a, Tze99, JDK-91, JD91, LJM93].

**Communication** [??97, AR99, BF97a, Bet95b, BFS96, CHH97, CMM99, FJP96, FK99, FT99b, IKM99, Jam98, KFJP96, KRJ98, PW99, PM99a, SSN98a, Sim94d, WD99a, We99, BF99b, Bet95a, BMS96, Com97, CWY98, CK93, Cli97, DFKN93, Hamxx, Rivxx, Sch90c, Sch97c, SD97, Sta97a, UU97b, Ven92, Wir98b]. **communication-privacy** [CK93].

**Communication-Storage** [CMN99].

**Communications** [ACM93a, ACM94a, ACM97a, Ano93h, Aur96, IEE94f, IEE97k, KM93, Kat97, MB94b, Ved93, BY93c, BY93b, Car94, Cha94b, Cra96, HOQ97, Hwa93, IEE92d, IEE95c, JC93, Mil95, Oht96, PP96, Par96, Rhe94, SW94b, Sch93a, Sch92c, Szw97a, ZG96].

**communicators** [Ano97-28].

**Communities**
BGT96, CWM+91, DiDPS96, FM91, FJV97, HK99a, HC95a, KG93a, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK+91, PH91.

Constructions [AHV98, ABDS96, KRS99, SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE98c]. consumers [Weh99]. contactless [DS98a]. contain [Lea90]. Contemporary [Knu99b, Sim92].
Content [Ack98, JPLI99, KR98, MW98b, MR95b, PMP99, Ros93, SC96a, Way93a, SNT95].
Content-Addressable [Way93a]. Content-Based [PMP99]. Content-MD5 [MR95b, Ros93]. Contents [vHH97].
Continue [Ano96-28]. Continued [KE97]. Continuing [Ano97-44, Ano97-45, Ano98q, DDJ98d, Ano96-29, Mad99b].
Continuous [BP95a, NHB98, She95a]. Contours [LFCK99]. Contract [GJM99a, GJM99b, KHB99, Ano99i].
Contractor [KHB99]. Contracts [Ped99]. Contrast [HKS97a, HKS97b].
Contrast-Optimal [HKS97a, HKS97b]. Contribution [Lud97, Mus92, SS97, AK98, Blo98b]. contributions [Hil94].
Control [ABL93, Ban93, BDPSN97, DFTY97, FY99, FL96, Hwa97, JPLI99, Kas96, KA99, KKW99, Lin98, Mey96a, NW98, NAA99, NS98a, PRAM98, Per99, STSW99, She93a, She93b, Sim90b, Sim91, ZHJ98, ACC99, Ano93d, BGT96, CWM+91, CS96b, CS97b, CW94, LL93b, LM93c, Mad99b, Mat91, MLA91, RO96, RT93, SS96, Uni97d, WW95].
Controllable [CTT94]. Controlled [GPR98, GO96b, Gol94, Jak99c, SKBxx, GM91, GO95, Men95b]. Controller [CIBM99, FCH99]. Controls [Ame96b, Ban94, Cli97, UU97b].
Cope [WI99, HJKY95]. Coprocessor [ECD+99, SK96a, SK97c, YS99, DvQ96, Dia91]. Coprocessors [HP98a]. Copy [LvdLB96, LvdLL97, Lin98]. Copying [BLMO94]. Copyright [BBCP98a, BKZ98, Coh96, Gr098, Gur97, HG97c, Ib97, KZ95, LT98, LML98, NS99, Per97, Sch97d, ZK95, ZK96, And98, BBPC97, BD95, BS97b, CPO+98, CHO+98, HPA99, OP9+99, PAK98, PA98b, RKDB96, YEA+98, Zha96].
Correcting [AW94, AR98, BG96, DL97, KKS97, LC99, Pen96, Ada91, Aha93a, AW95, Cha95a, CMM93, Ste95, War92a, YL97a, VT94].
Correction [Ano96f, Cha99c, MG91, WN98a, WL92c, Aha93a, WL92a].
Correctness [FHM98, Gai90]. Correlation [CS91, HT99, JJ99a, JJ99b, KSB96a, MS91, PK95a, PK95b, Pen96, GO95, Har91, Mat95, SGS99]. Corresponding [Oka93b].
Counteract [CJJR99a]. Counterfeit [ENK99, Ano93a, van96].
counterintelligence [Mon96]. Countess [KT99]. Counting [Kör96, MV293, KK98, SF97]. Countries [Gar97a]. County [IEE96c, IEE96f]. Course
[CM99d, Kob94, Nic98a, Nic98b, Sch99d, Coh94, Ger97, PGV93d, PR98]. court
[Ano96d, cover [CZ90, PSB97]. Coverage
[DS97a, Zav99]. Covert
[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. CPU
[Kea99]. Crack [De 90, Way95, WB95].
Cracked
[AAG+00, Gar96c, Ano97v, Ano97-41].
Cracker
[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. CPU
[Kea99]. Crack [De 90, Way95, WB95].
Cracking
[Ele98, GPO98a, GPO98b, Sch98c, Oel97, UFC94, WS96c, Bis92]. cracks [Sta96c].
Cramping
[Sta97c]. Crans
[BCB97].
Crans-Montana
[BCB97]. Crash
[Ano97-33]. Create [Ber97a]. Created
[JJ98c, MB99a]. Creator [MUSM98].
Credibility
[Fri93]. Credit
[Ano96g, Kra99, Ano98q, Gau97]. Credit-card
[Ano96g]. Crete [Duh90].
Crime
[Ano97k]. Crimes
[Ano97-50].
Criminals
[Uni98j, Uni98k]. Criteria
[Ano97b, KS97b, MS90a, Rob93, SZ95a, Xie92]. Criterion
[ZZ95, BBC98, YT96, Cus96, Cus96c, O’C94]. Critical
[CM97b, Gui97]. criticized
[Ano97-31, Ano97-35, Buc95a]. CRL
[HFPS99]. cross
[Ano97j, WG97].
cross-platform
[Ano97]. crossing
[SBG99]. Crossley [CFK+91]. Crucial
[Gar97c]. Cryptanalysis
[Bar92a, Bar95, BBF90, BLM94, Bih91, BS91c, BS91d, BS93b, BS93a, Bih95, Bih96, Bih97a, BK98a, BK98b, BBF+98, Bih98a, BBS99a, BBS99a, Bih99b, BBDR99, Bir95, BK98d, BPP99a, BL95, BD99b, BPV99, BHT98, BO92, BTK99, Burst99, Burt99, Bur94a, Bur94b, CS99a, CJS91, CWS98, Cus95, DGV93, Dae95, DWZ96, Daw93, Daw96, DFY93D99, Duy94, Dob96a, Dobxx, FS97a, FY95a, Geh94, GDS91, GO96b, Gol97d, GC90, Gol94, HKSW98, HKRS99, HG97a, HG97b, Har96a, HM97a, HO96, Jak98, JS93b, JQ98a, KR94b, KTM+99, Kay95, KSW96, KSW98a, KSW98b, KSW98c, KSW99b, KSW99c, KS98d, KS99b, KG95, Kmu92, Kmu93d, Kmu93a, Kmu93c, KM99b, Koc95, KT91a, Kwa93, LMM91, LK96, LG97, LH94, MB94a, ML98, Mat94a, Mat94b, Mat96a, MT99a, MT99c, Mi93c, NS97b, NS98d, NS98e, NS99a]. Cryptanalysis
[Ngu99a, Ngu99b, NK93, OA49, Pat95, Pes97, Pie93, PNRB94, Pre98a, RP95a, Roe99, SZ96, SF97, Sch98a, Sch96c, SM98a, Sch99d, SV94, Sel98a, She94a, She94b, SiK93, SMK98a, Sim94b, ST91, Tab94, VKR98, Vau98a, Vau98c, Vv97, Ver95, WSK97a, WSK97b, WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Vic90, Wie90b, Wie90a, WBDY98, YLD99, YLH98, ZYR91, Ada92b, Alv98b, BSN95, BB94, Ber93, BSN90a, BS91c, BS91f, Bih92, Bih95b, Bih98b, BK98c, Bir99, BD95a, Buxxx, Bur98a, CV95, CD98a, Cra92, DLY98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, Gol95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kali98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LSS98a, Lew92, Mat93, Mih96, Mil92, Moh92, Mor92, NS97c].
cryptanalysis
[O’C95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZYR90, ZHR90].
cryptanalyst
[Rey96, Rey97, Rey99]. Cryptanalytic
[Gla99b, KSW98d, MG91, vW99, Bih94a].
cryptic
[Wir98b]. CRYPTO
[Fei91, ACM94b, Ame96b, And96a, Ano96b, Ano98d, Bar93a, Bar93b, BE90, HP98a, HMV94, Koo97, LKB+94, Mad98a, Mal96, MPPS95, Neu97, Sch98c, Way95, Way96b, Mad98f, Mad98g, Mad99a, Mad99b, Mey97b, Neu95, Sav97, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol90b, Kal97c, Kob96, Kra98, MZ98, MV91, Sti93b, Sti94, Wie99, BC98,
Bra98, Bri98, CP91, CRS98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, Sti98a, Wil98b. **Crypto-Chip** [HMVT94]. **Crypto-Coprocessors** [HP98a]. **Crypto-Engine** [BE90]. **Crypto’91** [DBGV93]. **Crypto’95** [NS98b, NS98c]. **CryptoAPI** [Boy98]. **CryptoBytes** [Cry95, Riv95e]. **cryptochip** [PP96]. **cryptograms** [Har94, Web93]. **Cryptographers** [WP90]. **Cryptographic** [NK98b, Nur94, Nys99, ’OPH+99, Oka93a, OS98, PS99d, PV97, PS96b, PW98, PBGV90, Pre93a, PGV93a, Pre93b, Pre94a, PBD97, PRB98b, Pre98c, PRB98a, Pre99, Pre94b, QV90, QQ95, RSA93d, RS93, Ritzx, Rue93, SI94, SZ96, Sak96, DY91c, Sch95f, SK96a, Sch98d, SK98a, Sch91c, Sch93f, SPS97, SZ93, SZZ95c, Sha99a, She92d, SBVG99, Smi90, SY92, SM91, Ste96, Syv92, T+99, Tou91, Tou93, TY996, VCF+90, Vig98, Wai95, YS99, YY97c, YY98a, ZZ95, ZMI91, AN94, AN96, AG97b, AG97c, AG97a, Ano97-32, Ano98g, BD92, Bol97, BV97, Com94c, CDG95, CLI99, DD95, Dan97, Dhe98, DIF94, ECD+99, Ell94, HSSI99, Hat96, Hed97, HL93b, Hir98, HAHH94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLP96, HH98, HBKL99, JR96, JM97, Kal97a, Kal98e, KS98a, Kal99, KSS+92, KN98a, Kob94, KA91, RSA93f, Lac93, LM94b, Lin96a, Los97, Mad98b, MY91, Mau99a, Mau99b, Mau97c, McC96, MP91, Mit92b, MKS99, NC97]. **Cryptography** [Ans97, ANS98b, Ano97k, Ano99l, AA93, ABDS96, Av98, BCE+94, BGG94, BGG95, BGR98a, Bel98, BBE+91, BBE92, Bir98, Bla93, BK95d, BL96b, BL96a, BGV93, Boy95a, Bra90a, Bra94a, Bus97, Cae96b, DD98a, DL96, DP98a, DP98b, Dav91, Dav96, DG96, De93c, Des94a, DQ98a, DQ98b, Des98c, Dif90, DNN91a, Dro96, Dwo97, Ele99, Eri99, Ferr99b, Fs97, FB97, FMJ+96, FJRS96, FGLP96a, FGLP96b, Gan93, Gem97, Gol95a, Gol97a, Gol97b, Gon98, HK99a, HP98a, HSSI99, Hat96, Hed97, HL93b, Hir98, HAHH94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLP96, HH98, HBKL99, JR96, JM97, Kal97a, Kal98e, KS98a, Kal99, KSS+92, KN98a, Kob94, KA91, RSA93f, Lac93, LM94b, Lin96a, Los97, Mad98b, MY91, Mau99a, Mau99b, Mau97c, McC96, MP91, Mit92b, MKS99, NC97].
Sch97a, Sch97b, SSv+98, Sch98f, Sch94h, SV93, SG96a, She93a, She93b, She93d, Sni94b, Smi97b, Sta99a, SW95b, Ste91, Sti95, Sti98b, Sur99, Swi97a, TN96a, TN96b, Tv92, Tow92, Tsu92c, Wad98, Way96a, Wol99, Wol93b, Wor96, WC97, YWC97, YST99a, YY96, YY97a, YST99b, YZWR91, Zim98, dRHG+99, Uni96b, AA95, Acc97, Ada92a, Ada91, Alv98a, Ano97-29, Ano97-52, ASM98, BH98, Ban94, Bea97a, BR96b, BFS92a, BFS92b, BHHR99, BW97, BMP+97b, BSS99, BBS98b, BD98b, BC96b, Buc95b, Com96, Coh99, Cou99, Dam96, DDB95a, DDB95b, DQ96, DiDSP96, DDN91b, DN95b, Eng99, Far93].
cryptography [FM91, FK93b, Fra99, Fra93, Fri96, Gar96b, GZ91, Gen99c, Gol99a, Gol97c, Gre94, GTGW94, HA00, Hir97, Hru95b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdL98, Luc95, MB94h, Mat98, Mau93b, MY98, Mei96b, MIV97, Mic97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nlc91, Nec99, Nyb94, Org98a, OD94b, Par96, PG97a, PG97b, PC98, PP92b, PGV93d, PR98, Riv98c, Rot95a, Sal90, Sal96, Sch92c, SSM+97, SMD+99, Sch99e, Sch90c, Sch97c, SPP98, Shp99a, Shp99b, Sin99, Siu99, Sh98, SMS90, Sta96d, Ste98a, Tas98, TM99, USE96c, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wa99a, vS97, Sha99a].
cryptography-dedicated [NM96b].
Cryptography-in-the-Large [Bla93].
Cryptoki [Ano96-28].
CryptoLib [Lac93].
Cryptologia [Ers99, DKK+98, Joh98].
cryptologic [RK98b].
Cryptologic [Bra93b, Bec90, Sch98e].
Cryptologist [Pin98, Sei94].
Cryptology [Ano93g, Ber96b, Bea94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dam90a, DS99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Ste93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ano97-37, Bau97, Bec88, CW94, Cop95b, Cop95d, Dam91a, Dam99b, Dav91, De95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, Hel94, IRM93, Joh95, Kal97c, KM96a, Kobb96, Kra98, LOX99, Lid90, Lip93, Ma96b, Mc90b, Mei92, MV91, New97, Nym98, OdIP98, PSN95b, QV90, QQ95, Rat96, Rue93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Unixxb, Uni95b, Web93, Wie99, Wil98a].
cryptology [Bec97].
CRYPTON [DBR+99, Lim98, Lim99].
Cryptonomicon [Ste99a].
cryptos [Hag98].
cryptoscheme [MMI97].
Cryptosystem [AMV90, BI95, BDG98, Ber97c, Bii91, BMS94, Ble97, Bon99, BM97, CC99b, CQ99, CJ91, CS98b, CW91b, Cus97, Gib91, Gib96, GC91, GC94, GGH97a, Gys96, HD96b, HPS98, HJJ98b, Hwa91, Jab90, JS93b, Kie98, KS99b, KT91a, LR96, Lan97, LCL92, MM96b, NMR95, NS97a, NK98a, NS97b, NS98d, NS99a, Ngu99a, Ngu99b, Ou98a, SG99a, ST98, Sun98a, Tak98a, Tak98b, Van98a, Vau98c, Wai98c, Wan92a, WY93, Yam99, AMV93, AD97, AD99, Ala97, AAP92, ACA90, Bao94, BI94, BSB97, Boy97, BCC99, CC99a, CS98a, CC98, CW91a, CW97, CS97c, CCH96, Cle96, CS97d, DW96, Gen96b, Gi95, Gro94, HNSM91, HY93b, He92, HW96, HJJ98a, HLL96, IKNY98, Jon90, JQ98b, KASH90, KSR96, KM99c, KK96, LG97, LS92, LC96b, LC96c, Lon91, MMT90, MM90a, MM90b, MI90].
cryptosystem [Mau91b, M Yuan90, NS97c, NS98e, OU98b, Ole95, PED91c, Pet91, Roe99, SW95a, SH95a, SM90, SS95b, SS95e, SX90, TY92, Tan90, TTC97, TC97, TC99b, TC99a, Ven92, Wan92b, Wri98a, Wu92, XLP99, XK97, Yu92, Zer96b, Zha91, vT90, Ano96j].
Cryptosystems
Demultiplexer [SVBJ96]. Deniable [CDNO97]. Denial [Nee94]. Denk [CWM+91]. Denmark [Dam90a, Dam91a, Mad92]. dense [Ort95b, Ort95a]. density [CJL+92]. denting [Gib95]. Denver [Sch99b].
DeTeBerkom [GH96]. Detectable
[27]. Detecting
[GV93a, Mad92, PM98, SG96b]. Detection
[Bie98]. deterrence [van96]. Developer
[CM99b, Di 97b, DT98b]. Developing
[CF95, SCT99]. Development
[Ano97h, Bar99, Bas93, GRB99, HNSS99, IR99, LL93a, Nat99c, Nattxx, VDDR99, Way98, You96, AMV93, Ano97-52, LS98a, Mi99, NBD99, Sta97c]. developmental
[Ram92]. Developments
[Ano95a, PRB98a, Sim97]. Deviates
[Ran01]. Device
[Hru96, Ano91b, CM97c, Uni94b]. Devices
[BDHJ98, Ano95t, Hwa92b, Hwa92c, LS98a, Pos92, Pos93, Uni94a]. devoted [FT99b]. DFC
[KR99a, Ste99c]. DGSA
[FM98b]. DHCP
[Dra99]. Diagnosis
[GX99, MR95a, PW99]. Diagnostics
[Var99b, Lew92]. Diagrams
[Oh99]. Dial
[RSSW97a, RSSW97b]. Diameter
[FP99]. Dickson
[Pie93]. DICTA
[KG93]. DICTA-93
[KG93]. Dictionary
[Jas96, Luc98b, BCR98]. Dicytostellium
[Ram92]. Diego
[ACM93b, EE97b, Sch98b, USE96f]. Difference
[LP94]. Different
[KBRS97, Sch99h, RT93]. Differential
[BB94, Ber93, BS90a, BS91c, BS91e, BS91d, BS91f, Bli92, BS93b, BS93a, BS97a, BK98d, BKPS93, CJ98, Con99b, Dae95, Din94, Fer98, Haw98b, Haw98a, KTM99, Kau96, KM98b, Kob99, KJJ99, Kwa93, LMM91, LH94, Lan95, Mat96a, Miy92c, MSK98, NK93, OM94, Pai99a, Sch96c, SMK98a, VKR98, Wag98a, YLH98, Ad92b, CV95, KY95b, KYYc, KM96b, LMM92, O’C95, OG95, RP95b, TN97, Way95, YT95a, YT95b]. Differential-Linear
[Haw98b, LH94, Haw98a, Lan95]. Differentially
[Nyb94]. Differentials
[BBS99a, Fer99a, KRW99, BBS98a]. Difficulty
[KP96b, Riv93a, ZZ96, Hor99, Riv95a]. Diffie
[Ano97a, BY93c, BY93b, BBR99, BWM99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY98b, HY98a, Kain97a, Koc95, Koc96b, Lut98, Man94, MW96c, MW96b, MW99, RSA93b, Van95a, VW96, WM93, vOW96]. Diffusion
[Mas99b]. Digest
[FHHB97, GTG94, Kal91, Riv92a, Riv92b, Riv90a, Riv91b]. Digit
[TK99]. Digit-Recurrence
[TK99]. Digital
[Ano95, Ano96a, ANS98b, Ack98, ALO98, AW94, AR97, Int91a, NIS94, Ano96f, Ano97-50, AS98, Aub96, BG90, BM99a, BM99b, BdM94, Ber97b, BM94a, BM96a, BM96b, BM96c, BS95b, BS98, BTH96, Boy97, Boy98, Bia93a, Bia99, BWF99, Car95, CR91, CPO98, CHO98, DDM98, DDM96, EL99, EG90, EGM96, FFW99, Fox98, FKM98, FS98a, Fr93, Fro97, FOM94, Gar97c, Gar98b, GRR97, GDD97, GB98, GO96c, GQW91, HKS95, HC96, HG97e, HEG98, HA96, HW97, IEE97c, IEE98d, JLO97, Jue99, KKS97, Kob97, Kob98c, Kra93, KH98a, LER98, LM95, LW96, LL98a, Lut98, LR98, MS96, Man98, MST98, MB99a, MW98b, Mer90b, Mer97, MTN97, Mos98, MBW97, Nat91, Nat94a, NH98, NM98, NIS93a, OOG93, Oht96, OFF93, Oko96, Per97, Pet98, Pf96c, PW93b]. Digital
[PG93c, RDK98, dR94b, Rot95b, SC96a, SCxx, Sch93c, Sch93e, Sch94d, SK97b, SK97a, She97, She92e, Sim93, SB93, SY98, SH98, VP98, VP99, Web98, WD96, WD97, WL99, Woo90, YK98, Yeu99, Yeu97, Ye98, YHY98, ZK96, ZKO99, Zhe97b, vHH97, vTO94, AW95, Ano91b, Ano98e, BBCP98a, BHS93, BR96c, BGR98b, BCY97, BO96a, Bis90, BOD95, BS97b, BM91b, Bur98a, Com97, Car97a, CLHL98, DD95, DDM98, DSSZ99, FC94, FB97, Gua90, HS91, HZ93, HW98b, Hwa93, Ibb97,
digital [YL95a, YEA+98, ZL97, Zha96, ZK98, 
Zho94, Dr94a, AA95, Acc97, Ban94, Nat92a, 
Nat94c, NMVR95b, Riv93c, Sch93b, Sch94e].

Digital-Image [VP99].

Digital-Signatures [HA96].

Digital-Watermarking [GB98].

digitally [BP98a, BP98c].

digitized [BKZ98].

digits [Ran01].

digraphs [HEQL98].

DIMACS [FM91].

DIMCS [WN98b].
dimension [LFCK99].

Dimensional [FP99, OMA98, Per93, PS96b, 
MCD98a, OMA97].

Dimensions [HEQL98, Sta97b, Dining [WP90]].

Diophantine [BMP97a, Cus95, LG97, 
LCL95, Lon92, Sun91a, Wan92b].

Diophantine-knapsack [Wan92b].

diplomatic [Alv98b].

direct [PP90, PWU99, MHMW98, Uni94b].

Directed [BM94a, LL97b, MT99b].

direction [Uni95b].

Directions [AT99, 
Wot99, BFS92a, BFS92b, Go97c, NM96b].
directly [BD98a].

DIS [GQW+91].

Disappearing [Way96a, vdWS97, vS97].
disciplinary [DFGH99].

Disclose [Cré90].

disclosed [Joh98].

disclosure [Ste98b, Suv97].

Disco [WP90].

Discontinued [Ros98c].

discounts [DD98c, DD98f].

Discouragement [BLMO94].

Discourse [MI99].

Discrepancy [SI93a].

Discrete [ACM97b, BBT94, CH98, 
GJKR99, Gor93a, Gor93b, GM93b, GKS97, 
LO91a, Man94, MW99, MV98, NT99, 
Odl94a, vO91a, PS98b, Sch97, Tes98, WD98, 
YY97b, vO91b, vW94, CPS95, CS97d, FR94, 
FMR99, HZ93, HY93b, H97, HMP95, 
Kob90, McC90a, NR95, SS95a, SS95b, SS95c, 
TG94, TKS98, vO92].

Discrete-Log

[GJKR99, YY97b].

Discrete-time [GKS97].

Discretionary [BDPSNG97].

discussed [Ano90].

Discusses [Gar97c].

Discussion [Ano99e, Ano99j, Ano99l, BS94, Ch99a, 
Man93a, Man97a, Sas99a, ADK90, CZ90].

Discussion-Trust [Ano99j].

Disenrollment

[BBCM93b, BBCM93a, BC96a].

Disk [DIF94, Gar98b].

Diskette [BE90].

Disks [Gar97a].

dispatches [Web93].

Display [Fuc99, Sab94].

Displays [Fuc99].

Disposab [O90].

Disruption [MH96].

Dissipation [SKNO98a, SKNO98b].

Distance [CS96a, DD98c, DD98f, SC99, AI96].

Distances [Blo99].

distillation [Sl98].

Distortion [SVBJ96].

Distributed [ABLP93, A99, AD98, BHJ99, Bor96, 
BHKR95, Bu94c, CM98, DHR96, DF91b, 
Dwo95, FM91, FK99, F98a, F99].

GJKR99, Gre94, GS97, GMV98, KI99, Kau93, 
Kem99, KRJ98, KYB92, LAB92, Law98, 
Mar99, MKS99, Muf93, NAA99, NKP99, 
Ped91a, PKM97, R99, Re92, RG95, Sch94a, 
SKW96, SS90, She92a, TV94, Wh90, WL92b, 
Bea92, BP97b, FMY98, HK99b, Har90, 
LM98a, LAB91, Lie93, MS99c, T9+1, 
Wad93, WL92a, WL92c, Zin96b, BB96].

distributed.net [Ano97o].

Distributing [Bre97b, Re96].

Distribution [BR94a, BR95b, BDK93, B9S96, Bu94b, 
DDN98, DDP90, ECM96, Gal96, Max94, 
MTV92, PKOT94, PP99a, SK93, SR96, 
YKB94, vHH97, Ano96h, BG9+95a, BMS96, 
BFS98, Bu94a, BD95b, CFS97, FL93, 
G194, HI97, Hwa92a, Hwa92b, Hwa92c, 
JLM+94, Kh93, LC96a, MY93b, Mu92, 
PS98e, Pos92, RRP97, SI93b, SY96b, Svy93, 
SM95b, TH99, VSB95, WM93].

distribution-specific [Kha93].

Divergence [S90].

Diversity [Mau90].

divertibility [CDP95].

Divertible

[BBS98b, BD91, NMV99].

divers [PV90].
Dividing [MB99a]. divisibility [FR94].
Divisible [EO95b, EO95a]. Division
[Han94, DF92, FBT96, HP94]. divisor
[FR94], divisors [HP94]. dkar
[PNd99]. DLP [Kal98e]. DM
[KL95b]. DMS [Bax97]. DNA
[Fää93, RS99d]. DNEWS [Ano97-33]. DNS
[Gal96]. Do
[AW99, Ber97a, DDJ98e, DDJ98f, HKS95, SS99a, Ber98, Ude98, Way95, ZKOY99].
Dobb
[Eri97a, Eri97b, SSM+97, SSv+98, SMD+99].
Dobbel
[BLMO94, BLMO95, BO96b, Hei96b, LMM95, MLM98, Max94, Sea95, Bur98a, HIS91, LL98b, van97].
documentation [Sim95]. Documents
[Rot95b, SB97, Ban94, DSS99, Rot95a, Sch93e, SH93g]. Dodgson
[Lip98].
Domain
[ADBB99, DVPL92, Gar97a, Gar98b, Mon93, PD99b, Ano97-29, BB98, Ano99, PP98b, HP98d, HG97e, KMS99, KM98c, NP98b, TKS98].
Domains
[Bru98, CM97a, CK90, Mar97].
Donald
[CFK*91]. Don’t
[Hus99, Way96b, Chi99a, Chi99b]. door
[Yu92]. Doorbells
[Law98]. Double
[Ano92e, Cha97, HP99a, PA99b, Bar95, KL95b]. Double-Agent
[Cha90].
Double-Size
[Pa99b]. DoubleTree
[Nat98]. Doubly
[ABD99]. Doubly-Iterated
[ABD98]. Down
[GC97, Fox98]. downgrader
[McH92]. Downgrading
[KM92]. Downloaded
[PL97]. Downloading
[Sch97d]. dpe
[PNd99]. Dr.
[Eri97a, Eri97b, Gar97d, Riv93a, Riv95a, SSM+97, SSv+98, SMD+99]. Draft
[Ano94b, Ano96-28, Ano97b, Got99, Mic93b, Am95, Ano96c, Ano95u]. Drawing
[EMMN98, HEQL98]. Drawings
[BMRW98]. Draws
[Way93b]. DREO
[Ano99f, Lam99]. Driscoll
[Luj98a, Luj98b]. Drive
[GC97]. Driven
[CHLT99, Ano97-27]. Drives
[DDJ98a, DIF94]. Dromquinna
[IE96c]. DS [TY94]. DS/CDMA [TY94].
DS5002FP
[Kuh98]. DSA [AA95, Acc97, Len96a, Miy96, Sim93, Sim94d]. DSP
[IE97c]. DSP56000
[DK91]. DSPWS
[LW96]. DSPWS-96
[LW96]. DSS
[Nat91, BGM97a, BGM97b, GJKR96a, Koc95, Koc96b, Nat94e]. DTR
[Ano93k]. DTR-1
[Ano93k]. DTS
[BHKR95]. Dual
[Ja96, LL99, FBT96]. Dual-workfactor
[Ja96]. Duality
[ZZ97, ZMI91]. Dublin
[IE97a]. Duel
[Got99]. Dump
[Got99].
dumps
[Mei98]. during
[Don98, Joh95, Rat96, Wil98a]. Dutch
[vL96]. DVD
[GC97, LT98]. DVD-Video
[LT98]. Dwork
[GGH97a, NS98d, NS98e].
DYANA
[BKS99]. dyes
[SB99].
Dynamic
[AGY95a, AGY95b, Ano97-33, BDHK93, Dae98, DP99, DSS95, FT99a, FY99, FR95d, Gui97, NT99, SG99b, SP99, WWH95, BH93, BCDV94, Bl95, BCDV96, CT99b, HC96, Pos98, SS94].
Dynamic-Resharing
[AGY95b].
Dynamical
[PS96b, RO96]. dynamics
[Oh99].
E-Cash
[DFTY97, Yac99a, Yac99b].
E-commerce
[Ano98h, VM96, DDJ98d, Jak99b, Lut98, Gar97b]. E-Mail
[Ano93j, Ano95c, LF97, Ril96, Bac95, Sta94a, Got99, RS98b, Sch95c, Sch95d, SH97, Gar97b, Str93a, Str93b]. e-safe
[BC97]. E.I.S.S
[BFS92a, BFS92b]. E.I.S.S.-Report
[Dan95]. E2
[KMA+98, Kob99, MT99a]. EAP
[BV98b].
early
[Alv98c, Mar96]. Earth
[Fox98, YHK99]. Earthcam.com
[Ano98t]. Ease
[HJL99]. eased
[Ano96p]. Easier
[GMD98, BBR99, Sch98c, Way95]. East
[Str95]. Easy
[Ano97p, Sim94d, Ken95].
eavesdrop
[Way93b]. eavesdropper
[Al 96]. Eavesdropping
[RR99]. Eash
[Sch98h]. ECC
[Cer97, Kal98e]. ECC/DLP
[Kal98e]. EcoFan
[PKA+98]. ECP
[BT97]. **ECCp-97 [BT97].** Echo [GLB96].
eciphering [Blu97]. **ECMA-219 [ECM96].**
ECMAST [Dan96]. **Economic [Mos98].**
Economy [CFG99, Org98a, Tas98]. **ECP** [Mey96a].
Ed [DDJ98e, DDJ98f, MGL98].
Edgar [Sha99a, Ros97c]. **EDI [Len93].**
EDIFACT [RCM99]. Edinburgh [IEE95a].
Editor [Hat96, Joh99b, Ano95a, Ano96k, Ano97s, Ano98j, Pre95b].
Editorial [Eri99]. editors [Joh98, AKP96, BNP99].
eds [Ers99]. **EEC [BGV93].**
EEC-RACE [BGV93]. EEPROM [FG98].
EES [Com94b, FIP94, Nat94a].
EF [KP95]. Effect [OD99]. Effective [Fuc99, Min97b, MBY97].
Effectiveness [CGB93a, EN99]. Effects [CGB93, CI96].
Efficiency [Bas98, BM96a, CM99a, DKKK98, KS97c, Mar97, BHS93].
Efficient [AGS97, AGY95b, BBDW96, BDV93, BF97b, BF99c, BFP99, BDB92, CS97a, Cre97, CM99a, CG99, CG98, CDD99, Cre97, DR99a, DN94, FH94, FOM91, GSY99, GJKR96b, GP97, Ho99, Hwa92b, Hwa92c, JMO95a, JO97, JMP98, LYH93, LLH96, LL99, Len99a, MSNW99, MS93, MPL99, OS91, OS92, OFF93, OSA91, PS98b, Sch00b, Sch90a, Sch91c, Sch93f, Sha94, Ste98b, Ueh95, Wie94, Wie96, Wie97, Wie98a, Zim99, dR95, DB95b, CPPK98, CGS97, Dhe98, FMY98, HK90, HJ99, KC95, KSK96, MI90, MS98b, PPKW97, Per91, PA93, Pf95, Sch93g, Sha95a, SK97, VNM99, Von92a, Von92b, Xie92, Z198].
Efficiently [Jas96, Bak92]. Effort [Natxx].
Efforts [Ano96-28, Ne91]. **Eigenvalue [All98].**
**Eighth [ACM97b, IEE92b, ACM96b, USE99a].**
Einstein [Sv9+98]. Elastic [OMV98].
election [CGS97]. Elections [CFY96, Iev91, BT94, FOO93].
Electrochemical [DDJ99]. Electronic [Ano96m, Av98, Bar93a, Bar93b, BFP99, Bra95b, BLMO94, Cha92b, DDJ98c, DB99, DT98a, EO95b, EN98, ENK99, HS97, Hir93, JT97a, LHB96, Lin93a, Lvd98, LKD98, LR98, Max94, MZ98, O090, Ped95, PW97c, Riv97a, ST99a, ST99b, SB97, Sch99i, Sin98, TRS9, Tra99, USE95c, USE96d, USE96b, USE98b, VJ98, Ame95, Ame96a, AMS96, An98d, AC97, BH98, Com97, Cha92a, DMW94, DSSZ99, DF98, EO95a, FB97, Ken95, LM98a, Lin98a, Lin99a, Man95, Mit92a, RP97b, Sch93e, Sch95d, She96a, VNM99, Way93b]. **Electronically [Ped99, Ano98m].**
Electronics [IE97g, IEE98c]. **Elegance [Sch99c].**
Elektronicznej [Sch95e]. Elementary [Mii92, Tat98, Tat99]. Elements [FC99].
Eliminating [GGH97a]. Elimination [BLM99]. Elizabeh [Unit92]. Elliptic [AM90, Ano95a, BS91b, BSS99, CTT94, De98d, DP98c, DMPW98, Dem94, Eng99, ESST99, Fer99b, HSSI99, Hes97, JQ97, JM97, Ka97a, Ka97g, KMKH99, Kob98c, KMOV91, KT93, Len99a, LD99, MS93, Men93, Men95a, MM96b, Mi93a, Mi93b, Mi96, Mi99, OFF93, RY97, SOOS95, SW93, SNN99, VZ97, WZ99, AM93, AS98, BGR94, BC90, BS91a, CNST98, CPPK98, FM99, Gal99, GK99b, GP97, HNM98, IS99, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT99a, KOT95b, LLH96, Ler97, Mau91b, MV90, MVZ93, SX90, Wri98a, XL98, Z198].
Embed [Ano97z, MT94, Ano97-47, Zha96].
Embedded [BKS99, Bar99, DDJ98a, LT98, Lin98, BBCP98a, BP97b, CC95, KP99b]. Embedding [ACD94, DS97d, GO95, Gol96b, HK99b, ZK95, Sch91a].
embeddings [CT99b]. Embraces [Ts97].
EMEF [Org98a]. Emergent [Jun99].
Emerging [Kal99, Org98a]. Empirical
Employing [BWM98], 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].
Enciphering [Beu94]. Encipherment [Gu97, BS97b, PRZ99, Pin97, RZA93a, RZA94, RP94, Riv95c, Riv95b, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SvA+98, SKNO98a, SKNO98b, Sch99a, Sch99b, Sch99d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SE96, See97, She95b, She92g, SB98, Sim95].
Encryption [SM96, SM98b, SB92, Smi93b, Smi97a, SB99, Sta97c, SW99b, Sto90, Szw97b, THP+98, Un97a, Un98a, Un98c, Un98b, Un98d, Un98c, Un96c, UU97a, Un97b, Un98f, Un98h, Un98g, Un97c, Un98j, Un98i, VB96, VKR98, WSK97a, WSK97b, War98, Way93b, Way93c, WSFC99, Wei91a, Wei91b, W99a, Wir98, Wir99, Yin97, YY97c, Yu97, Zhe97b, Zie97, Zol93, Aus96, Abr97, Al93a, All97, And94a, An90, An92b, An94f, An95c, An95k, An95n, An95q, An95t, An95v, An95w, An96d, An96e, An96m, An96n, An96u, An96v, An96w, An96-30, An96-31, An97i, An97j, An97m, An97n, An97s, An97-31, An97-30, An97-35, An97-38, An97-41, An97-46, An97-49, An97-51, An97a, An98v, An98u, An98q, An99m, An99n, At94, AM99, Ban94, BTD98, Bax97, Bea96]. encryption [Bee96, Bee97, BR94b, BR95a, BDJR97, BR97b, BB90, Bet95c, Bih97c, BFN98a, BC96a, BMS96, BFS98, Bow93, Bre97a, Bro96, Bus96, Com97, CCM99, Cha94b, CLW98, Cle96, Cla97, Cla99, CJM96, Cra96, DH96a, DOR99, Dia91, DL98, Ele99, Ell97, Eng95, FC94, FB97, Gi97, Gol99b, Gol96d, GBL94, Goo96, GKS97, Har90, HK90, Hat97, Hel93, Hel98b, HT95, HP94, HY95, HCY96b, HCC98, Int91b, Jac90a, Jac90b, Jak99c, JT96, JT97b, KY95b, KY97, KYXx, Ken95, Kir95, Km99c, Kop97, Kuc92, Kuh98, Kuo90, Mil95, Moc97, Muc99,Mui99, Mi99a, Mi94b, Mi94d, Mi97b, Mi98, Mi99a, Mi99b, Mi99c, Natxx, NBD+99, NH90, Oh99, Oka94, Ori96, Par96, Par98a, Par98c, Per91, PRZ99, Pin97, RZA93a, RZA94, RP94, Riv95c, Riv95b, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SvA+98, SKNO98a, SKNO98b, Sch99a, Sch99b, Sch99d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SE96, See97, She95b, She92g, SB98, Sim95].
Encryption [AW99, Bla98, GMC95, GLZ99, Gi98, Jas96, Szw97a, YY91, An98o, BT98, Br97b, DF97, STW95, Kip97]. Encrypting [An97-33, Bla94b, Lom94, Luc98b, L99w, SS99c, Beu94, KAK96, LL98b]. Encryption [ASW99, AAB+97, Ada97b, Ada98, ARW99, An98, ABK98a, Na93b, An94c, An94d, An96c, An96m, An96q, An96o, An96p, An96-29, An97b, An97t, An97u, An97v, An97-39, An97-42, An98k, An99f, Bac95, Bal97, Ban93, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b, BDPR98, BS99b, BS99c, BRW99, BS93b, Bir95, BB95c, Bla96a, Bla96b, BFN98b, Ble98a, BC95c, BFS96, BY92, Buc95a, Com94a, Com94b, CNO97, CM999, COP+95a, CH98, CMK98, CT99a, Cop94a, Cou93, DDJ98e, DDJ98c, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DS97c, Ele98, FIP94, FN94, For99b, FY95b, FY97, FH94, FO99a, FO99b, GSY99, Ga990, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, Gen98a, Gen99a, Gen99b, GK98, Got99, HG97a, HG97b, Hat96]. Encryption [HK98, HK99d, Hub98, Joh90, JM96b, Kal93a, KY95a, KR96a, Kal98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kum98, KBRS97, HK98b, KDB98, Kwa93, Kwa97, RZA93f, Law98, Le99, LT91, LW91, LM91b, Lin93a, LS98b, Luc97, Luc98c, Luc98e, LW99, MGL+98, Mad97, Mad98c, Mad98d, Mat94a, Mat97, Mer91, Mey96a, Miy95, Moc97, Muc99, Mui99, Mi99a, Mi94b, Mi94d, Mi97b, Mi98, Mi99a, Mi99b, Mi99c, Natxx, NBD+99, NH90, Oh99, Oka94, Ori96, Par96, Par98a, Par98c, Per91, PRZ99, Pin97, RZA93a, RZA94, RP94, Riv95c, Riv95b, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SvA+98, SKNO98a, SKNO98b, Sch99a, Sch99b, Sch99d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SE96, See97, She95b, She92g, SB98, Sim95].
Escrow [AAB+97, Bla96c, BDS98, Cae96a, CGM97a, DDJ98g, DD96b, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, IWy95, Mad97, Mah96, Mar97, MS95f, MKS99, Nec96, SYM98, Sam98, SM95a, VvT97, VBD99, YY99b, Ano94f, BDHJ97, BR96b, DH96a, Des95, Fre94, KL94, Mao97, Uni95a].

Escrowed [Bas95, Com94b, FIP94, Nat94d].

ESIGN [FOM91].

ESORICS [DEQ92, Q98].

ESP [KA98b, Atk95b, KMS95a, KMS95b, MD98, MG98a, MG98b, PA98a].

Espionage [HK99c].

Espoo [Nyb98].

Essential [Len96b, SSM98, SMD99].

Essentially [BR91].

Estimating [Al96].

Estimation [VNW95, JV98b].

Ethernet [Bec99].

Etruscan [Nis91].

Euclid [LZ91a].


Eulerian [MSN98].

Eurocast [MDP94].

EUROCRYPT [Bih91, Dam90a, Dam91a, Dav91, De 95, Fum97, GQ95, Hel94, Man96b, MZ98, Nyb98, Pic98, QV90, QC95, Rue93, Ste99b, Ano98i, Bet98, BC98, CP98, Dam98, Dav98b, De 98b, Fum98a, Gue98a, GQ98, Hel98c, Ing98, Man98, Pat95, QV98, Rue98].

Eurographics [Kui91, PH91].

Europe [Ano97k, And96a, Ano95j, Ano95k, Ano98a, Koo97, Mus92].

European [DEQ92, Q98, Sp95, T98, Com97, Dan96, Gar97c, VCF+90].

Eusipco [T98].

Eusipco-98 [T98]. evaluated [LMS97].

Evaluating [Pai99a].

Evaluation [AGS97, Ano97b, BGK99, BP95b, CJR98a, CJR98b, HW98, KBRS97, PDG99, RJP95b, RJP95a, Rob93, Roh99, WT99, CJRR99b, KM97, PS99a, Sim95, VCF+90].

Evaluative [MI99].

Even [BCE94, Bosxx, Ano95q]. Evening [Che92].

Event [Ruo94, SK97b, SK97a].

Event-Stream [SK97b, SK97a].

Ever [Hi97].

every [Ano89b, Mei98].

Everyday [BOGG+90, MAM95]. Evidence [DR99b].

Evolution [Cas95, JM96b, KNT94, NM96b, PGV93d, Sin99, Wri99].

Evolutionary [Ger99a, GM99a, Hes97].

Evolve [GB98].

EW [IS97].

exact [BR96c, GEL98, Luc95, ZW99].

examination [Joh90]. examines [vdWS97, vS97].

Examining [RC95].

example [Kay95, Nee94].

Excellence [Eri97a].

Exchange [ASW98, AZ96, BCG90, BM94b, Dam94b, Dan95, DH90, FW91, HHY93, Jas96, Luc98b, MSN98, RSA99a, SSN98a, SOOS95, Van93, Ano96q, BSNP96a, BSNP96b, BT98, BCK98, BM95, Dam94a, LL95b, MS98a, SK97, STW95].

exchanges [DvW92].

Executable [JPL99].

Executing [AW99].

Executive [Zer96a].

Exhausting [CR97].

Exhaustive [CR97, QD91, KR96b].

Existence [FDB93a, HT98, RV99, FDB93b].

Existentially [DN94].

Existing [SS99d, BB95a, NM96b].

expands [Ano89d].

Expansion [BO96b, Tak97].

Experience [ADBB99, Gla99a, Ros96b, SVB99, Moy98, CWM91].

Experiences [FC99, Lun90, GH96, MAM95].

Experiment [AB97, DL95].

Experimental [BBB91, Mat94a, SBG99].

Experimenting [DB99, MWB99].

Expert [BBDF97, Chi92, Stu99, ACC99].

Expiration [BD98].

Explained [BMC95, Hat96, Lut98, Los98].

explanation [Gre90].

Explicit [LF99, M98].

exploit [Luc95].

Exploiting [BS91h].

Exploration [KV99, Kip99a].

Explorer [Lea99].

Exploring [JJ98b, JJ98a].

explosive [DL95].

Exponent [Ano95a, CFPR96b, CNS99b, CFPR96a, FR95b, KOT95a, KOT95b].

Exponential [Dan95, CF97, CD95].

Exponentiation [BP99b, BK95d, Com90, HCY96a, LL94b, Pai99b, Ara93, BGR98b, CL97a, KAK96,.
Rev91, Smi94b, Von92a, Von92b,YL93, dR95. **Exponents** [Wie90b, vOW96, Gro94, VW96, Vc97, Wie90a]. **Export** [Ame96b, DDJ98e, DDJ98f, Gar97b, GC97, Han95, Han99, Un97d, Abr97, Ano97-51, Ano99m, Ban94, Cli97, Gen99a, Han97, Mad99a, Mad99b, Re97, UU97b, UU97b]. **Exportability** [Wei91a, Wei91b]. **Exportable** [Eng95, Ano95v]. **Exports** [Bar96a, Buc95a, Sta97c]. **Exposed** [MSK99a]. **Exposing** [Sil99]. **Expressive** [MTES99]. **Extend** [Ts'97]. **Extended** [ASW98, BFN98b, BV98c, BD90, BS91g, BD91, CvHP91, CK90, DDP90, DY91d, DDP99, DD99, DY91f, DF91a, Dob95a, EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, vHPP93, Bea97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, OI95, Pa96]. **Extended-Certificate** [RSA93a]. **Extending** [Bad99, Has94, Mi99]. **Extensible** [BV98b, WBDF97]. **Extension** [BP98a, CTT94, FHBH+97, MS90b, LMJW93, STW95]. **Extensions** [CD91, DT98a, Law98, NW97, Atk93, GH99, GK95a, JD91]. **Extensive** [A97-44, Sim95]. **Externalization** [OA99]. **Extracting** [Nis96]. **Extraction** [SD99]. **Extraordinary** [Jam98]. **extremely** [Ano90]. **eyewitnesses** [Ano97-37].

**FA** [Bao94]. **Fabrication** [DDJ99]. **Face** [DDJ98d, DMFB97]. **Faces** [GB98]. **Fachtagung** [BGH95b]. **Facial** [LMP99, HEG98]. **facilitation** [Cli99]. **Facility** [AKF94, Bi90, She96a, YS91, JMLW94, SY92]. **facing** [KG96]. **facto** [Pri94]. **factor** [KM98b, SYWMB95, VB95]. **Factored** [Ano96b]. **Factoring** [Ano97c, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pa99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, Mck99, Mei96b, Riv95a]. **Factoring-Based** [Kal98c]. **Factorisation** [DH95a, Jon90, DH95b]. **Factorization** [Ale92, DDL94, MM98b, M98b, OD95, vO91a, Sho97, vO91b, LLMP93, Mao98, Whi93, vO92]. **Factorizations** [BMS94, NS97b, NS97c]. **Facts** [Ano91b]. **Faded** [Alv98a]. **fading** [Todd97]. **Fail** [BP97a, PP97, SSNP99, vHPP93, And94b, Pf96c]. **Fail-Stop** [BP97a, PP97, SSNP99, vHPP93, Pf96c]. **Failed** [BCE94]. **fails** [DH96b]. **Failsafe** [KL94]. **Failure** [Ano95a, Ber97c, Gar98a, TYD99, FR95b]. **Failures** [CH98, JQ97, Moc92, Sim94b]. **Fair** [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, MS99, SS99e, SS99f, Tra97]. **Fairfax** [ACM93a, ACM94a]. **Fairly** [HD96a]. **fail** [O90, Rob98b]. **False** [KL98, She92b]. **Families** [Kal98e, Per99]. **Family** [KT98, Mad98e, Miy91, RP97a, ABC95, BG95a, FSS94, It90, Kob90, SRL98]. **FAPKC** [DYL98]. **FAPKC3** [TCC97, TC97]. **FAPKC4** [TC99a]. **Far** [Str95]. **Fast** [AGS97, AMV90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bih97b, Bibh97c, BHK+99, BD94, BK95d, BGV96, CS91, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBVD96, DRS97, EP99b, EPR99a, Gar97b, Gol96a, HJT98b, HP94, HCY96a, JJ99a, JJ99b, KR94a, KTM99, KP99a, KP97, KR99a, Kmu99c, KMKH99, KA91, Koy95, LM95, Mau90, Mer91, Mih94, MM95, MS99a, NKP99, PSL97, Prew95a, Rog95, SW97a, SW97b, SOOS95, SV93, SB98, Sho96, Sil97b, Tak97, Tak98a, Tak98b, T+99, Van98d, Van98c, AM93, AB96b, Ano98t, CGV94, DKK97b, DV96, GGH+98, HJPT98a, Jenxx, LRW93, LC98, MZI98, PVO95, RRSY98, She92c, SN94, SH99, SAM97, SGS99, YL93, Gol96d, OA94]. **Faster** [Luc96a, Luc96b, WZ99, YY99b, Bosxx, Mih96, Sch98c]. **Father**
[CFK+91, DDJ99]. **Fault**
[BS97a, DHSS95, GX99, OKST97, Pai99a, RBvR94, IEE94b, TCH+91].
**Fault-Tolerant** [DHSS95, RBvR94]. **Faults**
[BDHJ98, BDL97, CH94a, FY99, Gar94, JQBD97].
**Fauvel** [CFK+91]. **Fax**
[Ano91b, Int91b]. **FaxModem** [Ano93k].
**FBI** [Szw97a]. **FC** [Fra99, Hir97, Hir98].
**FCC** [Gar97b]. **FCD** [ISO97].
**FDR** [Low96]. **FEAL** [GC91, KR95a, MY93a, Miy90, Miy91, TN97, BS91e, BS91d].
**FEAL-8** [GC91].
**FEAL-N** [TN97]. **Fears** [Gar97c].
**Feasibility** [DN95a, NFQ99]. **Feasible** [Lip94].
**Feature** [Sar99, SD99].
**Features** [ADEDS99, Zav99].
**February** [ACM98a, Fra99, FJV97, Gol96d, Hir97, Hir98, IZ98, RP97b, SJ97, Wol93a, Wol93b, van96, Ano94f]. **Federal**
[Ano97h, Ano97-42, Lee99a, RP94]. **Federated** [SS99b].
**Feedback** [Jut98, Knu94a, SN93, SK96c, SK96d, Vau99a]. **Fermat** [LLMP93, McK99].
**feud** [Mad98e]. **Few** [FJRS96, Mei98].
**FFT** [DBGV93, MS90b, Sch91c, Sch93f, Sch93g, SVBJ96, Vau93].
**FFT-Hash** [DBGV93, Sch93g, Sch93h]. **FFT-Hash-II** [Vau93].
**FFT-Hashing** [Sch91c]. **FGPAs** [Nor95c].
**FFHC** [KKW99]. **FFHC-Tool** [KKW99]. **Fiat** [Nac93, OOK91, OQ93].
**Fiber** [Tow98].
**Fibers** [HLMP96].
**Fibonacci** [SMS99].
**Fiduccia** [CKM99]. **Fiduccia-Mattheyses** [CKM99]. **Field**
[CD98b, Kob98c, LL99, LLMP90, LL93a, MR95b, Ros93, SY99, TT99, CDEH+96, Dav98a, GH99, Gor93b, HWB93, Has99, Pom94].
**Fields**
[BP98a, BMT96, BL96b, BL96a, BP97c, De 98d, LO91a, LO91b, Mas91, MFC95, PSR97, Ano90, Gal99, LN94, MVZ98, SW95a, Sch91a, Shp99a, Von92a, Von92b, ZPY96].
**fifteen** [Den90]. **Fifteenth** [CFK+91]. **Fifth**
[SJ97, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni98h, Uni97c, Uni98k, ACM93b, USE95b]. **Fight** [De 93b, De 98c].
**FIL** [AB99a, AB99b]. **FIL-MACs**
[AB99a, AB99b]. **File** [ANS98a, AW99, Ano97x, Ano97-34, Bla94b, Gil98, Man97b, RC95, HSK97, MKKW99, SK97d].
**FileDrive** [Ano97-34]. **Files**
[Bal99, PF94, Pop96, Ano98o, Gol99b]. **Filesystem** [IHR99, JJ91].
**filling** [BB190]. **Film** [Gar97c]. **Filter** [She92e]. **Filtered** [MS94].
**Filtering** [Sch97d, LLB98, LYG94].
**Final**
[RIP95b, RIP95a, BFS92a, BFS92b, BP95b].
finally [Ano98v]. **Financial**
[AA95, ANS98b, FBS97, FL99b, Fra99, Hir97, Hir98, Lan97, Riv97b, Swi97]. **Finding** [BMRW98, CQ95c, Ler97, Riv91a, Sim98c, YY98a, CC99, Car97c, Sta94a].
**Fingerprint** [DDJ98g, DDJ98h, HWJ98].
**Fingerprinting** [Ano99l, BS95b, BS98, DF99, Hei96b, PS96a, PW97a, PW97b, Sas99a, YST99a, YST99b, DF98].
**Fingerprints** [HJPB97, OMI93]. **Fingers**
[CK93]. **Finite**
[BI95, BDGI98, BMS94, BVFD99, CD98b, DKKK98, Gys96, KPR99, KV94, Kob98c, LO91b, PS96b, She92e, Shp99a, Ano93k, Bao94, BI94, BGR95, DWZ96, DYL98, DF93, FSS94, Gal99, GH99, HWB93, Has99, Jun96, LN94, MK92, PS97, Pie93, Tao94, TCC97, TC99b, Von92a, Von92b, Wal98].
**Finite-Impulse-Response** [She92e].
**Finite-Size-Particle** [BBV99].
**Finland** [Nyb98].
**Fire** [Way93b]. **Firewalls** [GLZ99, Opp97].
**firm** [Ano97i]. **Firms** [GC97]. **Firmware**
[MNSV97]. **Firmware-Oriented** [MNSV97].
**First**
[BCB97, GPSV98, Hir97, KT99, KP99b, KW99, Law98, Mat94a, Nat98, Nat99c, RD99b, ACM99b, AND96c, Dob98, HOQ97, IZ98, NBD+99, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni98h, Uni97c, Uni98k, USE95c, RD99a].
d94]. Functional [Yam99]. Functions
[AHV98, Ano95a, BDPSNG97, BCK96d,
BCK96e, BHSV98b, BHSV98a, BGK99,
BGS94, BGS96, BM94a, BL95, BHT98,
CCD99, Car93, DGV93, DY91d,
DY91b, DFL99, ECM96, EPR99b, EPR99a,
FBS98, GJKR96b, JQ97, KTM99, Kim93,
KP96a, Kra95, KS97b, LM93a, LM93b,
LM95, MS99b, MS90a, Mer90a, Mer91,
MS95f, Mi96a, Mon96, NR98, OS98,
PW93b, PGV92, Pre93a, PGV93a, PGV93c,
Pre97a, Pre99, Pre94b, QC90, Roe94,
Schi9b, SZ95c, SY99, ZZ95, Zhe90, vW94,
BSNP96a, BSNP96b, BD92, BGR95,
BCK96b, BCK96c, BHH99, BK98f, CCZ98,
CDG95, Cus96, CS96c, Dam90b, Gol96a,
Gon95, GHS93, HSK97, HLMW93,
HXMW94, HYLT99, ISO97, JG95, KL95b,
Lai95, MCD98b, O949, PGV91, PGV93b,
Pre94a, PGV94, Pr95b, Roe95,
Rom90b, SZ95c, SZZ95b, Sim98c, Tsu92b].
functions
[Tsu92a, Wer93a, Wer93b, YT96, ZZ97].
Fundamental [Ano96s, IEE97e]. Funds
[GBC93]. Funktioniert [MPS94]. Further
[Pre95b, WKS99, WD97, Mad99a]. Fusing
[DMFB97]. fusion [KH97]. Future
[Fuc99, HP98b, Od95, PT95, PM99b,
Schi97a, And98, BFS92a, BFS92b, For99b,
Mar96, NIS92, SB92]. Future-Adaptable
[PM99b]. Fuzzy [Blo99, CIBM99, FCH99,
KKW99, Tro93, ZHI98, 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
[KBRS97, MB99b]. Gateways
[Bec99, VDDR99]. Gauss [GvP98, Mon93].
Gbit [HK97]. Gbit/second [HK97]. ge
[LPNdbbprm91]. Geheimschrift

[Kip97, Kip99b]. Gemmell [Geh94]. Gene
[Cap94, CO98]. General
[BC95a, BK95b, BPRF99, CL98, FDB93a,
ISO97, IVE91, KKOT91, KP93, NOV93,
OK98, St93a, Beu94, DD95, Des90b,
FDB93b, GIN95a, Pi96c, Sch91b, Sim98c].
gegeneral-purpose [Sch91b]. Generalised
[GS99b]. Generalization
[Jab90, HKM95, MSS93, TC99a].
Generalized [BBC95, BFS98, CT97,
HL93a, Jut98, LH93a, LH93b, Mau96a,
PS96b, Bad99, BBR99, BCCGG99, Krc92,
PA93, Por93, Son99]. generate
[Wer93a, Wer93b]. Generated [SVBJ96].
Generating
[Ble96, De 98d, FMM99, Len96a, Len98,
MS95f, YWW99, CH97b, SH99]. Generation
[ARV99a, ARV99b, BG98, BGM97a,
BGM97b, Bir98, BF97b, BD93, Coc97, CD96,
DF91a, GJKR99, Gil99, Gut98b, HL99,
Kal97b, KS98c, M399, Mat96b, Mau90,
Mih94, P98c, ROT94, RS98c, RS98d, SN96,
Si97b, WI99, Bou94, FMY98, GTS90,
LL96, MS99c, PS97, PS98b, SH94, Bou94].
Generator [PIP93a, HILL99, JK99, KSF99,
KW99, MS95b, PS98b, Daw93, Jexux,
KSF99a, Mih96, PC98, Rev91, Sin99,
TS98, Wal90]. Generators
[HL99, KSW98d, Kra90, ZYWR91, CS96b,
CS97b, Imp92, Kos99, Lag90, Pat91b, Por93,
SGSD99]. Generic
[Bel92, CM99a, MS98b, Tua99, ZK98].
Genetic [BS99a, LC99]. genius [Obe99].
genius [Ano97-37]. Genomic [MUS98].
Geodesic [Blo99, LFCK99]. Geometric
[OMA98, Sim91, JM93, JM96a, Mra95].
Geometrien [Wal98]. Geometries
[LMS90, FSS94, Jun96, Wal98]. Geometry
[Ben99, DFGH99, Ton96].
Geometry-Based [Ben99]. George
[Pin98, WG97]. Georgia [ACM99b].
Gerdes [CFK+91]. German
[Wei99, Cra92, Dav88a, FT95, Ger97, Hor99,
Jar97, Kah91a, KK97, Kip97, Kru98, Wal98].
Harari [Ver95]. Harbor [Kah98b, Par98b]. Hard [MGL+98, Mar99, SS99a, BFKL94, Jon90]. Harder [Sch97b]. Hardness [BV96, DI99, Par98b, SS99a, BFKL94, Jon90]. Hardness-amplification [DI99]. Hardware [ACD94, Ano96a, Bir98, BP99b, Bri90b, BS91h, DGV92, GN95c, Koç96a, Gai90, KP99b, LMS97, MZI98, Nor95a, Nor95b, Nor95c, NO96, See97, SN94, TY92, Way95, Zhe95b, Kui91]. Harmonic [RG99]. Hash [ANS97, AHV98, Ano93f, Ano95a, Ano95l, BDPSNG97, BCK96d, BCK96e, BS91e, BS91d, BDP97, BHT98, CP91, DBGV93, DGV93, Da95, DY90, DY91d, DY91b, EPR99b, EPR99a, FIP93b, GHR99, GS94a, ISO97, KP96a, Kra95, LM93a, LM93b, LM95, Mer90a, Nat92b, NIS93b, Nat95, PR99, PW93b, PV92, Pre93a, PV93a, PGV93b, PGV93c, PGV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sch91c, Sch83f, SV94, SRY99, Sta94b, Vau93, Zhe90, vW94, AB96b, BSNP96a, BSNP96b, BD92, Dm90b, DK94, Gom95, HLMW93, HXMW94, HYLT99, JG95, KL95b, MZI98, PV91, Pre94a, Pr99, RP95b, Roe95, SV95a, SRRL98, Sim98c, Tsu92b, Tsu92a, YL97c, 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, Reg95, Rus93b, Sch91c, Sch93f, Sho96, Sti91b, TZ94, BG96, Bosxx, Gih90, PM90, Sab94, Sch93g, Sta99b, ZPS93]. Hasn’t [Gar97a]. Hasty [Sch98i]. HAVAL [ZPS93]. Hawaii [??90]. head [Ano94i]. Header [At95a, KA98a, MR95b, Ros93]. Heads [GC97, St98]. Health [GO96c, Mjo93]. Hearing [Un98a, Un98g, Un98j, Un98i, Un97a, Un98d, Un96c, Un97b, Un98f, Un98h, Un97c, Un95a, Un98k]. Heat [GC97]. heating [Mad98a]. Heats [Gar98b]. heaven [Go97c]. heavily [Ano97-35]. Heimdal [DW98]. Held [Ano96-28, BF99a, Bar93, Uni98f]. Helias [EVE97c]. Hellman [RSA93b, Ano97n, BY93c, BY93b, BWM99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY98b, HY98a, Koc95, Koc96b, MAu94, MW96c, MW96b, MW99, NS97c, NS97b, Van95a, VV96, WM93, vVW96]. Help [GRB99, PKA9+98, AK95]. Help-Desk [GRB99]. Henry [CFK+]. Her [Ber96a]. Herd [Rit99]. Here [MK94]. Heterogeneous [DVPL92]. Heuristic [MCD98b, CKM99]. Heuristics [SBG99, CD98a]. HF [RP94]. HFE [KS99b]. HFX [LR96]. HGF [Uni94b]. HGF-94 [Uni94b]. Hidden [BL95, CD97, JP96, KZ95, NS99a, Pat96, Sak96, PSB97, Til98]. Hide [SV99a, SV99b, SV98]. Hidell [Sau92]. Hiding [Auc98, BGML96, BLM095, CM97b, CD97, CD98a, GR96, GLB96, HS96a, MS99a, MO99, Ph96a, Phil98, RG97, SC96b, SNT96a, And96c, Beu94, Brr90d]. Hierarchically [LE99]. Hierarchical [FL96, OOK91, CMPS97, GPCSN96]. Hierarchies [Ruo94]. Hierarchy [Hwa97, YY99]. hieroglyphs [Wri98b]. High [ACM98a, ARV99a, ARV99b, An99c, An99f, BCR98, Bl98a, Bl98b, BMS99, Ch99a, Chi99b, DP98a, DP98b, Ebe93, FVE99, FP99, Gar97a, Gar98b, GN95c, HR90, IEE94e, IEE96d, IM93a, IM93b, Kap98, Koc94, Kor93, KB92, LS97, MPPS95, MSH99, Rs90, SKNO98a, SKNO98b, She92d, She95b, Sut99, VN94, An97y, Duf98, Graxx, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Un96a, Yeu97]. High-Assurance [IEE96d]. High-Bandwidth [Bl96a, Bl96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Ch99a, Ch99b].
High-end [Ano97y]. High-Frequency [MSHP99]. 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, Ko94, MPPS95, SKNO98a, SKNO98b, IMI93a, Nor95a]. Higher [Jak99a, KMKH99, Lea99, MSK98, SMK98a].


HKM [LR96]. HKM/HFX [LR96]. HMAC [BCK96a, BCK96c, KBC96, KBC97, MG98a, MG98b, OG97, Sta99b]. HMAC-MD5 [KBC96, OG97]. HMAC-MD5-96 [MG98a]. HMAC-SHA-1-96 [MG98b].

Hoffman [Hat96, Wai95]. HOL [ACD94, Bra95a, Bra96]. Holder [OMI93]. Holiday [IEE94a]. Holy [Sal99]. Home [Hus99, Ano97o, Hod97]. Homomorphic [FDB93a, Bet95c, FDB93b]. homomorphism [Dom96]. Homomorphisms [Bur96, SK94].


Houthalen [QV90]. HP [GC97, Hed97].


I/O [Got99]. IBM [Ano96h, Ano96s, Con90, Gar98b, Gen98b, Zun98]. IC [DD99, DD98, JJ97a, PT97a, PC98].


ICL [CFK+91]. ICSA [Nic99]. ID [CS97c, Hwa92a, Hwa92b, Hwa92c, IS99, JY98, LH99, MS98a, Mu92, TC91, WSFC99].

ID-based [CS97c, Hwa92a, Hwa92b, Hwa92c, JY98, LH99, MS98a, Mu92, TC91]. idea [OA99, BBS99b, BK97, DGV94c, HO99, Haw98b, Haw98a, KSW96, Lip99, Mei94, Sch93d].

Ideal [ABDV98, BC93a, BD90, Bir90a, BP97c, Pa98a, Pa98b]. Idealised [RS99c].

Idealized [MTES99, MM92b]. Ideals [GPT91a, GPT91b]. Ideas [HGDH98, RS99d, T+91]. identical [BCCG99]. Identifiable [KOO95b, KOO95a]. Identification [BCCG93, BLM94, BB92, Cha94b, GS94a, KM99b, KI96, LMBO95, LML98, NP97, OOA98, Oka93b, Sak96, Sch90b].
Ste94a, Ver95, BBC98, BM95, BM91b, DF91b, DF98, HLC99, IS99, Kum97, Mu92, SSN98b, Sch90a. **Identities** [MS99a, Sar99].
**Identity** [ALO98, Dan95, DQ94, FKMY98, HJPB97, JG90, KP98, Len99a, SSN98a, Gua99, OU98b, Tan90]. **Identity-Based** [Dan95, DQ94, SSN98a, OU98b, Tan90].

**IEC** [Int91a, GQW+91]. **IEEE** [Ano95u, CH96, Ano96-28, Ano97-48, Ano98r, IEE95c, IEE95b, IEE96d, Kal97a, KK99b, LW96, Pit95].
**IEEE-IMS** [IEE94a].
**IETF** [Ano97c].
**If** [GPR98].
**IFIP** [Kat97, LM98a].
**IFIP/GI** [LM98a].
**II** [Sch99b, AK99, Ano97-40, Ano98i, Ano99c, BS91f, CFG96, CK95, CW91b, Dav98a, Don98, Eri97b, Mit92b, Mon96, Mus92, Pni98, Rat96, Rey97, RP97b, Ros99, Sch93f, Sch93g, USE90, Van93, Wil98a].
**III** [Fri92b, Gau93, GN95c, Nor95a, Rec98, Rey99, USE92b].
**iKP** [HSW96].
**illicit** [SG96b].
**Illinois** [USE99c].
**IMA** [Boy95b, Dar97, Far93, Wal99a]. **Image** [BKZ98, BNP99, DS96, DP99, Fri93, HPA99, HPG98, HWJ98, IEE95a, IEE97a, IEE96c, IEE97b, IEE97j, KZ95, KM92, LMP99, Mae98, Man98, Pit95, PZ98, PNFK95, Sch99b, SC96a, SCx, SJ97, SD97, ST96b, TOH98, VP99, Wal95, YKY99, BBCP08b, BCD98, CCH98, JTR96, JT97b, KS98c, KG93, KH97, NPB98b, OP97, OP98, OK96, PBC97, SCH98b, Se95, SG98, TK98, VP96, VP98, Xie98, YM98, CFF+91].
**Image-Adaptive** [PZ98]. **Imagery** [WD97].

**Images** [BLMO95, BO96b, Bf99, Car95, J98c, KR98, KPR99, LvdLL97, Lvd98, LVV95, MFG95, NNEK97, Per97, SC96b, ST96a, WD96, ZK95, BP98b, BP98c, BBCP07, BCP08a, BCV07, BOD95, CLK96c, HW98b, Ibb97, Irw98, Nas94, Nat97a, ODB96, OP+99, Pit96a, RRP97, RKDB96, TA97, XBA97, ZL97]. **Imaginary** [HJP98b, HJP98a, ZPY96].

**Imagination** [Sha99a, Ros97c]. **Imaging** [AA97, RP97b, Yeu97]. **Imai** [Pat95]. **Imake** [Hus94]. **IMAP4** [Mye94a].
**Immunity** [SZ96]. **immunity** [Ada92b]. **Immunized** [FY95a]. **Impact** [Mar96, Ven90]. **Impending** [Bra95e].

**imperfect** [CKLS96b]. **imperfectly** [BMC95].
**Image-based** [TNT93]. **Implementation** [An96, Bib97b, Bra96, BS91h, Dae99, DGT96, DRR95, BV96, Ebe93, Fe97, Fe96, FOM91, Gla99a, KQ99, HRV99, IM93b, KP99a, Koc96, Koc96a, Lan97, LC99, NM99, OSA91, PL94, PP90, Ros96b, SJ98, She95b, Tou92, Var99a, YKY99, You97, Zim99, BR96b, BC90, CM99, Dia91, HNM98, IM93a, LS98a, LL98, Men91, MV90, MZ98, MPL99, Nor95a, Pal96, Per91, SS98a, See97, SAM97, V95, XL98, Koe99].
**Implementations** [Bas98, Bri90b, Gon98, HK98, HK99d, Nor95a, Pal96, Per91, SS98a, See97, SAM97, V95, XL98, Koe99].

**Impossible** [SAS99b, Van95a, Lee99a].

**Implications** [Bas93, CMYY98, NS99b, PN92, Van95a, We95].
**Implicit** [Jan98, MLY93].
**Implicitly** [HRV99].
**implies** [LHL95b, LHL95a]. **Importance** [BDL97, SCH99b, CM97d].
**important** [Sta94a, Woe97]. **Impoverish PM91].**

**Impossible** [BBS99a, Fer99a, BBS98a, OK96a].

**Imprimitve** [Pat99]. **Improve** [Far92]. **Improved** [An96f, BK98e, Bo90, BS91g, CRRY99, CJL+92, JMM99, JMM99b, KM96b, LD99, RP95b, SH97, SAM97, WS98, YL95b, YL95a, ZYR91, Cao99, He92, NM95a, NMVR95a, SH95a, SH95b].
**Improvements** [BB95b, Bir95].

**Improving** [BHS93, BKPS93, GLV99, SF97, SZ94a, SMK98a, Sun98a, HM97b].
**Impulse** [She92c]. **IMS** [IEE94a].
**In-memory** [M90].

**Inaccuracies** [OD99].
**inadequacy** [Kah98b]. **Including** [DG93, DW94, JS95b, JS95a, KL95b].
Irish [Got99]. irreducible [Ito91, Kob91c].
IRREGULAR [FR95a]. irregularly
[FR95a]. Irrelevant [BD99a]. Irreversible
[ANS97, AA95]. ISAAC [Jenxx]. ISAKMP
[CH97a]. ISBN [Hat96]. ISC [Ano93g]. ISO
[Int91a, Gar98b, VGV93].
ISO-OSI [VGV93]. ISO/IEC
[Int91a, QW’91]. ISocRob [AVLPF99].
isogenies [Gal99]. Isolation [GX99]. Israel
[Bih97c]. ISSAC [Wat91]. issuance
[FL99b]. Issue
[DF91c, Eri97b, FT99b, MDP94].
Issued [Gar97c]. Issues
[ACM94b, Ano97-28, AT99, BMNL99, Cle91,
Gar97c, PS98d, Por98, Rad97, Ros96d,
She92f, D89a, Fre94, GA98, Koo97, Org98b,
PS99c, Ros97a, Sm97a, Sta94a, Tay90].
IT-Systeme [BGH95b]. Italian
[Alv98b, Don98]. Italy
[De 95, IEE92d, Knu99c, Nat99b]. items
[Uni97d]. Iterated
[ABDV98, Pat99, BCKxx, Bih92, Har96a,
HLMW93, HXMW94, Ort95b, Ort95a].
iterating [HNSM91]. Iterative
[CDN98, Knu93b, MG91, LYG94]. itself
[Ri96]. IV
IEE93a, BP98e, Far93, MD98, USE93]. I’ve
[Bra95d]. IX [T’98].

J [Ers99, Hat96, Sha99a, Wa95]. Jack
[Pin98]. J acks [Bee99]. Jacobi
[BK98g, Kob91c]. Jacobians [Kob90].
James [Scu92, Sha99a]. Jammers [SV95b].
Jan [WL92a]. JANET [You97]. January
[ACM97b, ACM99a, Ano97k, Ano97a,
Bih97e, SP90, USE91, USE92a, USE95a,
USE96f, USE98d]. Japan
[An93g, Ano99c, IEE96b, IR93, IZ98,
IZ99, Ano97-49, Dre92, Win93]. Japanese
[DR99b, Mea98, Wei99, Win93]. Java
[ACM98a, Dra98, GA98, Ale98, AW99,
Ano97t, Ano97-38, Ano97-39, Ano97-47,
Bam97, Bar99, Ber97a, Ber98, Bro97,
DDJ98e, DDJ98f, DDJ98a, DDJ99, Di 97b,
DT98b, DE99, Fo99, Gar97a, Gar97b, GC97,
Gar98b, Gar96c, Gau97, GPO98a, GPO98b,
Gon98, GS98, HNSS99, HH98, KHB99,
Knu98a, Law98, MGL+98, MF97, NK98b,
PV98, TJ97, Tsa98, Tre99, WBDF97,
Way98, You96, Zuk98b, Zuk98a].
Java-based [Al98]. Java/Smart [Bro97].
JDesignerPro [Ano97-34]. Jede
[Ano97-50]. Jeopardy [Gar97c]. Jobs
[RH93]. Johnny
[WT99]. Joining [ARH95]. Joins
[Law98]. Joint
[Ano93g, Cla98a, F94, IEE94f,
IEE95c, Kat97, LW91, IEE92d, vT93]. Jose
[Com96, FJV97, RP97b, SJ97, USE96c,
USE96g, van96]. Jour
[Lut98]. Journal
[Ano97k, Er97a, Zol93, OW95].
Journal/Logging [Zol93]. Journyx
[Ano97-34]. JSafe
[Way98]. JTC
[Gar97a]. Juan [CMM93]. Judge
[GC97]. Judiciary
[Uni96c, Uni97b, Uni97c, Uni95a, Uni98k].
July
[AR97, AA97, BFS92a, BFS92b,
Com96, DG96, IEE95a, IEE97a, IEE94b,
IEE97c, IEE98e, Sch98b, Sch99b, SJ93,
Uni98c, Uni98f, Uni97c, USE95c, USE96e,
USE96g, VPM97, Wat91, vWN99, Uni98i].
Jump
[DRR95]. Jumps
[Gar97b].
Junction
[CIBM99]. June
[ACM95, And96c, AA97, GS94b, IEE92a,
IEE94b, IEE96b, IEE96c, IEE96f,
IEE97g, IEE98c, LM98a, Ny98b,
Pit95, PR98, SJ93, Uni98b, Uni98e, USE94,
USE95b, USE98c, USE99d]. Junk
[DN93].
JW
[Ano93g]. JW-ISC
[Ano93g].
45

De 93a, HRT96, IH99b, Kay95, Koh90,
Kn93, KNT94, Lei99a, Lin96b, Luns90,
Men91, N93a, Rus90, SA95, Sin95, Ste92,
Ts'97, Tun99, Yu94a, Yu94b]. **Kernel**
[BCCG93, WB92]. **Kerry** [IEE96c].

**KEY**
[YY98d, ANS97, ANS98b, AKP96, AAB+97,
AN95, IBM93, Ano94b, Ano94d, Ano94f,
Ano95a, Ano97c, Ano99j, Ano99l, AAM93,
BP98a, BI95, BES98, BDG98, BCE+94,
Bar96a, BCG90, BR94a, BR95b, BHSV98b,
BHSV98a, BDPR98, Be97c, BS91b, BS97a,
Bi98, BMS94, BWM98, BWM99a, BWM99b,
Bla94b, BDR+96, Bla96c, BPK99, BF99,
Ble97, BDHK93, BFS96, BD99b, BF99c,
Boy90, BM94b, Brou95b, Br95c, BS94,
Burl94b, BDS98, Ca96a, CC99b, CG99,
CDN98, CI99, CGM97a, CS98b, Cra98,
Cus97, DDJ98b, Dae98, Dom91b, DK96,
Dan95, DDP90, Dav96, De 93c, DP98c,
DB96, Dif90, DH90, ECM96, FW91,
FDB93a, FY95a, FY98a, FMY99, FBS98,
FO99a, Fun98c, Fun93, GHH90, Ga96,
Gan96a, GJKR99, Gi91, Gi96, Gi99,
GM90, GG97b, Gy96, HK99a, HQ99a].

**Key**
[HP98a, HS90, HMT+98, HMV93, Haw98b,
HD96b, HJJ+xx, He97, HPS98, HFS99,
HM98, HR90, Hwa97, Iss90, Jab90, Jas96,
JVF96, Ka99, KPa99a, KSW96, KSW99a,
Kel99, KS99b, KP96b, KM99c, KT91a,
KMOV91, KKT91a, KP93, RSA93f,
Lan91, LMB94b, LMY95, LMS97, LA98,
LP99, Low96, Luc98b, Mal96, Mar97,
Mat91, MY91, Mau93a, MW96a, Mau97a,
MP91, Mve93, Men93, MM96b, Mie93a,
Mic93b, MS95f, MM99c, MS99c, MS99,
MS98, MS99a, MTZ92, MAO96, MM98a,
MM98b, NMR95, NS97a, Nec96, Neu97,
NS99a, Ok94a, OHe98a, Ok98a, Ok98b,
Oml90, VO91a, PDR97, Pau97, PKOT94,
Pat95, Poi97, Poi99b, PB99a, RAS93b,
RSA93e, RSA94, RDT94, RS98c, RS98d,
Ros96a, Ros96c, Ros96f, Ros97b, Ros98b,
Ros98c, RCM99, SS98a, SYM98, Sam96,
DP91, Sas99a, Sch94b, SKW+98a]. **Key**
[SKWW99, SOOS95, SM95a, SE96, Sha99b,
She94d, SK93, SR96, Slu98, Sta99b, ST91,
SW99b, SH94, Sun98a, Sut99, TAP90, TA92,
Uni98i, Van95a, Van93, VSH97, Vv97,
VBD99, WM93, dWQ91b, WLE96b,
WW98b, WKS+99, Wie96, Wie97, Wie98a,
Wie98b, Woi98, Yam98b, YST99a, YST99b,
dWQ91a, vO91b, vOW96, A95, Ace97,
Lip98, AD97, AD99, Al96, Ano90, Ano96q,
Ano96o, Ano96w, Ano96o, Ano97k,
Ano97v, Ano98f, BS996a, BS996b,
Bao94, BI94, BDJ97, BD98a, BDT98,
BS97, BR96b, BCK98, BY93c, BY93b,
BS91a, BFS92a, BG97a, BMP97a, BF96,
Ble96, BMS96, BFS98, BM95, Boy97, Bur94a,
BD95b, CC99a, CW97, Cle96, Cra97, Cus95,
DK97b, DW96, DS90a, DH96a, Des95,
DV96, Dh98, Dv92, DN95b, ES97,
FDB93b, FMY97a, FMY98, Fre94, Fro96].

**Key**
[FGLP96a, FGLP96b, FL93, Gar96b, GH96,
Gib95, GHL94, GH99, GTS90, HNS91,
HP99a, HP99b, HY93b, HJT+96, Hwa98a,
He92, HWF96, IJJ+97, HI97, HY98b,
HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93,
IZ98, IZ99a, Jm96a, Jar96, JLM+94, Jon90,
JY98, KASH90, KM99a, KSW97a, KSW97b,
KL94, KR96b, Kf95, KM98c, Koo97, KM99d,
Kos99, Kim97, LG97, La92, LMJ93,
Lee95, LC96a, LMA94a, LZ90, LZ91a, LDW94,
L95b, LCL95, Lon91, Lon92, Low95,
Mad98f, MS98a, Ma97, MLA91, Mau91b,
MY93b, MKM99, Mu92, MLL95, NM96a,
NY90, Nat97a, Nec91, O94b, Ole95, PS98e,
PS98f, Pet91, P92b, RFL96, RT93, Roe99,
Sal90, Sal96, SW95a, Sch92c, Sha95a, She96a,
She92c, SK97, SY96b, SM90, Sm93b,
SS95b, SS95c, STW95, Sun91a, SS98b,
Syv93, SM95b, Tab94, Tao94, TCC97, TC97].

**Key** [TC99b, TC99a, Ts90, TC91, Tz99,
TH99, Uni97c, Uni95a, VW96, Ven92,
Wan92b, Wie94, Wil93b, Xie92, Xie93,
XLP99, WX97, Yam98a, YL97b, Yu92,
Zha91, Zhe95a, Zhe95b, ZPY96, vOW91,
vO92, vT90, MC96, Mad97, BFS92b.
Key-Agreement [RSA93b].
key-clustering [Kum97].
Key-dependency [MAO96].
Key-Dependent [FBS98]. Key-Escrow [VvT97]. Key-Exchange [Dan95].
key-management [MLA91].
Key-Recovery [Oka98a, Oka98b].
Key-Schedule [KSW96].
Key-Search [KP99a].
Key-Share [BWM99b].
Key-signing [Ros96a, Ros96e, Ros96f].
Key-specific [LMS97].
key-vowel [Lip98].
Keyboard [GO96c, She95a, Ale97].
Keyboards [CFK +91].
Keyed [Ano95a, BFN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pr95b, MS95e, BFS98a, GON95, KBC96].
Keyed-Hashing [KBC97].
Keyed-MD5 [KBC96].
Keying [BCK96d, BCKxx].
KeyNote [BFK99].
Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Dae98, EHMS99, Gir91, KSHW97, KSHW98, KM99c, Luc98b, MP91, PS98g, SV99a, SV99b, Ste94a, Vau96, Way96b, Ano96h, Bih94a, CH97b, CII99, DG94c, JP96, KC95, Knu95, LL93b, MB99, MF97, Mok97, SS197a, SS197b, SV99b, SH99, Sta95a].
Keypoint [CD98c]. keystream [CS96b, CS97b].
keystroke [JG90]. KG [Uni94a, Uni94b]. KG-94 [Uni94a, Uni94b]. Khafre [BS91f].
KHF [Wag98a]. Khufu [BBS99b, GC94].
Kingdom [D+98, Lom97]. Kingston [HA00, TM99].
Kiosk [BO96a, Gar96b].
kit [Ano97-38, Sun91b]. Klettingraphic [YY97b].
Kletography [YY97a]. KMOV [Ble97]. KN [SMK98a]. Knapsack [CP91, JS93b, ACBR90, CZ90, He92, JG95, LC97b, Odl90, Wan92b, Yu92, Zha91].
knapsack-based [He92]. Knapsacks [CJS91, Ort95b, Ort95a]. Know [DD98b, Fly97, Hill97, Kir95, Mii95].
knowing [Ble96]. Knowledge [ADBB99, BMT98, BG90, BG93, BJY97, Bie98, BD91, BDB92, COM99, Cc97, CDS94, CD98b, DAM99a, DDP94a, DDP99, DO99, DFK93, DS98b, GMW91, GK96, GSV99, GO93, HT98, JKVP99, NOVY93, NM99, O090, RS91, SIF93a, SY99, St99, Syv92, Tou91, BOQ+90, BBP95a, BBP95b, CDP95, DDP94b, DF93, DF94, DF91b, Sah99, Sak97]. Knowledge-Based [Bie98]. Knowledge-Level [BMT98]. known [Ano91b, BK95a, MY93a, vOW91].
known-plaintext [vOW91]. KnowRight [BS95c]. Knoxvilles [IEE94e]. Knuth [CFK +91].
KoMoD [SY99]. Komputer [Ano97-50].
Konstanz [Fum97].
Korean [Ano93g, KM96a, Rhe93].
Korea-Japan [Ano93g].
Korean [LL98a].
Kryptographie [KK97].
KryptoKnight [BGH+95a, MTVZ92].
Kryptosysteme [Hr99]. KtSecC [BG99].
Kudos [SVa98]. Kunstliche [CWM+91].
ku [XrTmW94]. Kuperee [DH96b, HS94, HS96b].
Kurz [Ger97].
Kyongju [KM96a]. Kyoto [Ano99c].
L [Lip98]. Labeling [BKZ98, KZ95, LvdLB96, LvdL97].
Labels [ZK95]. Laboratories [Ano95d, Ano95e, Ano95p, Ano95s].
LABYRINTH [LS97]. Lacs [CFG96].
Ladder [Bih97a]. Ladder-DES [Bih97a].
Lai [LLG10]. Lake [IEE96d, USE95b].
Lambda [HRV99, GLV99].
lambdaProlog [NM99]. LAN [Ano96v].
Lancaster [WSFC99]. Lance [Hat96, Wa95]. landmark [KT99]. Lane [DDJ98e, DDJ98f].
Languages [ACD94, BD91, GMW91, PM99a, PD99f].
She92f. **LANSCAPE**
[Ri96, Ano94g, Ano94h]. LapCad
[Ano93k]. **Laptop** [GPR98]. Large
[Bl93, BDHG99a, BDHG99b, CS97a, LO91b, LM95, NNEK97, PF94, Riv91a, SA95, SS90, She92a, Csi95, DT93, DL95, Fra90, FO93, Has99, MDS90, Yan95, Yuan92]. Larger
[PW97b]. **Laser** [Ano93h, JC93]. Last
dBB91, dB91. **Late** [Bur99]. latencies
[JG90]. **Later** [Sch95a, Gol97c, Roe95]. latest
[Bee97]. Latin [BSNP97, Son99].

**Lattice** [Ano97-29, BK98g, CC99b, CNS99b, GG97b, CC99a, SH95a, SH95b].
**Lattice-Based** [CC99b, CC99a]. **Lattices**
[Dwo97, Ste98a, BV97]. launch [Taa98].
**Launches** [Gar97c]. **Lausanne** [IEE96e].
Law [And96a, Bro94, Cae96b, Sw97, Uni95a, Cli99, Way93c]. laws
[Ano97-50, Bre97a, Cha94b, Gen99a, Gen99b].

**Lawsuits** [Lea99]. **Layer**
[BB95c, FK99, Sar97, Wu96, Mye97].
Layered [Jun99, RC95]. layers [AP93].
**Layout** [BW98]. LCN [IEE97]. LCN’98
[IEE98f]. **LCT** [ZVR90]. **League** [PWU99].
**Leakage** [WI99, HJ95, SG96b]. Learn
[Hel98b]. Learning
[BV98a, COM99, FCH99, FC99, Ho99, KV94, Riv93b, SKIT99, BFKL94, Kh93, Kos97].
**Leave** [Hum99]. Lectures
[Dam99b, Fri96, PR98]. **Lee** [Scu92, LZ91b].
Lee/Alek [Scu92]. legacy [Unир92].
Legal [CYY98, HA96, Mos98, Rad97, Ros95b, Wri94, Ame95, Ame96a, Sch93e].
Legislation [RDK98, Mad98d, May97].
legislative [Cl99]. **legislators** [Bre97a].
legitimate [Cl99]. Leighton [Zhe95a].
**lemma** [HK95]. **Lempel**
[Mun91a, Mun91b]. lend [Ri96]. Length
[BR99a, BR99b, GS94a, Sch94b, YY98a, CC98, Han94, KL95b, MPL99, Su98, ZPS93].
**Length-3** [YY98a]. length-restricted
[MPL99]. **Lengths** [BDR96, HMV93].

**Lens** [FCD98]. Lesions [ZTR99]. Less
[BD99b, Vv97]. lesson [Scu92, WL94].
Lessons [Mc96]. Let [DDJ98e, DDJ98f].
lets [Way93b]. Lett [YT96]. Letter
[BC+94, Joh99]. Letters
[Bur98b, MGL+98, PKA+98, SV+A+98, BY92].
Leuven [PGV93d, Pre95a, PR98]. Level
[BMT98, HV98, MB99a, VNW94, AG95, An97-30, Cla99, DF92, HWF96, Rus90].
Levels [Bor96, GTGW94, dVdV98]. LFSR
[Kra94b, MRR99]. **LFSR-Based** [Kra94b].
Li [JW01, vT93]. Li-Wang [vT93]. li.vi.5
[CFK+91]. liberty [Ele99, Wad98].
**Libraries** [AR97, BV99, DL99, IEE98d, SH98, DSSZ99]. Library
Licensing [Par98a]. Life
[CJ99, DDJ98e, DDJ98f, DQ94, GAGCAFC99, Ros95a, CWM+91].
Life-Span [DQ94]. Lift [Gar97a]. liftings
[CNST98]. lifts [An99]. Light
[Gar97b, HPG98, YYH98, BG98].
light-weight [BG98]. Like
[JQ97, BS90a, BS91c, CC98, Kob99, MS95f, MT99c, Nac93, WSFC99, ZZZ97, Kim93, KP93, Way93a]. Likely [Bar96a]. Limit
[Lea99, Way93c]. Limitations
BM91a, CMZ98, Fis98, KV94]. Limited
[AR99, BDS98, DQV96, VBD99]. Limiting
[KI96]. Limits [And96b, AP98, EKK99, Swi97, BH98, Cohn99, SOB98]. Line
[Bra95b, Cac95a, Cac95b, CDF95, DT98a, Ei99, EGM90, EGM96, LMBO95, PUF99, SS99e, SS99f, Tra99, DL98, Gau97, Mao98, Na97, VNM99]. Line/Off
[EGM90, EGM96]. Linear
[An95a, AMP99, BG96, BK94a, BL95, BPV99, CFSY96, Dae95, DD99, Des98a, vD95a, DL97, Gol95, HOF96, Haw98b, KR94b, KR95a, KTM+99, KR99b, LO91b, LH94, MS94, Mat93, Mat94b, Mat96a, Nyb95, OA94, Ros98a, SZ96, SF97, Sch96c,
Sch99l, Sel98a, SK98c, SK98b, TN97, TSM95, YMWP99, ZYR91, Ala93a, AW95, BSN95, Bao94, BI93, Bi95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, HKM95, Haw98a, Jak98, KY95b, KYxx, KR96c, Kuk99, Lai95, LL98e, Lan95, MM90a, MAO96, MK92, OG95, SKD94, Tze99, YT95a, YT95b, ZYR90, ZHR0, vD95b, vT94, Duh90.

Linear-Time [KR99b].

Linearity [SB95].

Linguistic [CH99b].

Link [Ano98m].

Linkage [HCY96b, LC97a].

Linked [BRS99].

Linking [BLLV98, CM95, RP94, SM99].

Links [Blo99, CV95, DDNM98, JC93].

L'inuktitut [Ano99k].

Linux [Cor93, DDJ98a, Eri97b, Mor97].

Lion [AB96a].

Lippman [vdWS97, vS97].

LISA [USE99b].

LISA'96 [USE96a].

List [LC97b, Uni97d].

Lists [FGR92, Riv98b].

Literate [Sab94].

Little [Ano91b].

Little-known [Ano91b].

Lives [DDJ98d].

LL [FY95a].

LLL [Mis97].

Loadable [Ano98m].

Local [Fum93, IEE97l, IEE98f, MM95].

Localization [PJ99].

Locating [KP93].

Location [FJP96, Jac96, KFJP96, KRJ98, WHFG92, FT95].

Lock [Ano96o].

Locking [BC97, CS96b, CS97b].

Locks [Way95, CC95].

Locomotive [Var99b].

Loen [LW96].

Loftus [Hel94].

Log [Bal99, GJKR99, Gor99b, PS98b, WD98, YY97b, Kob90, SS95a, SK97d].

Logarithm [CPS95, CS97d, FR94, FMR99, HY93b, H97, HMP95, Mc99a, MV98e, NR95].

Logarithms [BBT94, CH98e, GM93b, LG91a, Man94, MW99, vO91a, She97, Tes98, vO91b, vW94, Gor93b, HZ93, Odl94a, SS95b, SS95c, vO92].

LOGCFL [LMSV99].

Logging [Zol93].

Logic [AHMS99, BR99, BAN90, CIBM99, CO98, DRR95, Gue98b, SG95, SM95a, SHK99b, CS99, Pos98].

Logical [PS99f, Wad93].

Logics [ADD99, GAGCDAC99, KW99, Len99b, WK96, Bad99, XZZ97].

Login [ARH95, DQ93, Hil97].

Logout [Poo95].

Logs [SK98a, SK99].

LOKI [BS91f, BKPS93, Km92, Km93c, Km95, TSM95].

LOKI91 [Km93d, Km93a, SF97].

LOKI97 [BPS98, RK98a, Rij99].

London [Ano93d, Ano97-28].

Lone [Ano97-33].

LONE-TAR [Ano97-33].

Long [CH97, Len96a, RH93, SSS98, Pos93].

Long-term [CH97].

Longevity [Rot95b].

Look [Coh96, Has99, Pf95, Zha97, GTGW94, Han95, Han99, Way91].

Look-up [Has99].

Looks [Sch97b, Mad96, vDS97, vS97].

Loops [SvA+98, SHK99b].

Lorenz [Car97b, Dav98d].

Lose [GPR98, Way96b].

Loses [Law98].

Loss [PW97c].

Lossy [CI96].

Lottery [Riv97a].

Lotto [QD91].

Louis [Dwo95].

Louisiana [ACM91, ACM97b, USE95a].

Louvain [Dan96, Q+98].

Louvain-La-Neuve [Dan96, Q+98].

Loveland [KT99].

Low [Ag92, Ano99c, Bia96a, Bia96b, CFPR96b, CFPR96a, CNS99b, DDQM98, DDP99, DDGM97, DFKM93, GDD+97, Go96, Jak98, KSHW97, KSHW98, KKK99, KOT95a, KOT95b, Mil96a, Pai99b, PK95a, PK95b, Pen96, SKNO98a, SKNO98b, T+99, Ano90, CJL+92, DQ96, Go96a, MMWM98].

Low-Bandwidth [Bla96a, Bia96b].

Low-Cost [KKW99, Pai99b, DQ96].

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].

Lowell [IEE98f].

Lower [BD97, CTT94, OK95, Sch99l, Sga91b, Sti93a, vHPP93, GN95a, KO96, KO97, Shp99b].

LR [BP98c].

LSI [SKNO98a, SKNO98b].

Lu [LZ91b].

Lu-Lee [LZ91b].

Luly [BKR98a, BKR98b, Luc96a, Luc96b, PRS99].

Luly-Rackoff [BKR98a, BKR98b, Luc96a, Luc96b, PRS99].
LUC [Smi93b]. Lucas
[BBL95, QJ97, 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]. Lyndon [SM90, SSM92]. Lyon [FR95a].

M [IEE97c, WG97, Man91b]. M.A.P.
[BBC98]. M6 [KSW99b, KSW99c]. ma
[XtTmW94, KP99b]. MAC
[Mit92a, PV995, PV996, Pre97a, SRRL98,
SV99, Yuv97, An903434]. MacArthur
[Dre92]. MacGuffin [BS95a]. Machine
[KP99a, NM99, PF94, QD91, Riv93b, Wie90,
Cra92, Dav98d, Dav96, Kru98, McL92].
Machines [Bur99, CFK∗91, FM999,
SK99a, Dav98c, Jan95, Sl98b]. Macintosh
[Sch941]. Macquarie [KG93]. MACs
[AB99a, AB99b, BGR95, Jv98a, NR98,
Pv995]. Made
[GSV99, Kra94a, Gol97c, KKL99]. Maestro
[CFK∗91]. MAGENTA
[Bi99a, Hui98, BBF∗98]. Magic
[BD99a, JM99, AGLL95, Kahl98c, RK98b].
MagiCol [GLSM99]. magnetic
[An9034, Gut96]. Mail
[An9034, DN93, Got99, Ken93, Lin93a,
RS98b, Sch95c, Sch95d, SH97, VJ98, An90345c,
An9066m, Gar97b, LF97, Lin88a, Lin89a,
Mit92a, Ril96, She96a, Str93a, Str93b,
Bac95, Zeg93, Sta94a]. MailSafe [RSA94].
Maniframes [De97, De98]. Mainstream
[CH94a, CH97, Gar94]. maintenance
[Uni94b]. MAINZ [PWTU99]. Majesty
[Ber96a]. Major [Law98]. Majorities
[Cha90]. Majority [Mv93]. Make
[An90345c, GGMM97, CM99d]. Makes
[Ame96b]. Making
[ASW99, CK99, DDJ98e, DDJ98f, Des90b,
Hir93, Lut98, PRS99, Sar97, Tra97, VM96,
Way98, BKR98a, BKR98b, Wri98b, Za97].
Malaysia [GO96c, WSFC99]. Malicious
[PM98]. Malleable
[DDN91a, BS99b, BS99c, DDN91b, Sah99].
Malo [QG95, QQ95]. Man
[CFK∗91, Mon96, IPNdbbprm91].
Management
[An9099, AWV99, AG99, Bla94b, BPK99,
BFK99, Coh96, FJP96, FY98b,
Fum98c, Fun93, GM93a, GH96, KMS99,
KFP96, Neu97, Rob98a, SS99b, Yac99a,
Yac99b, An98f, CVM∗91, Hat97, LS98a,
ML91, MKK99, PS98f, Pos92, RFL996].
Manager [VDDR99]. managers [Sea95].
Managing [ADF98, Coh99, Ken99, Sta95a].
Mandarin [OSH91]. Mangement [Bra93a].
Manipulation [FMM99]. Manipulators
[ZH98b]. Manor [IEE96c, IEE97c]. manual
[Pre97c, RSA94, Uni94a, Uni94b].
manufacturer [An904c]. manuscript
[Mor92]. Many [BHSV98b, BHSV98a,
CFK∗91, DY91a, KW99, DY91c, BDV93,
Ito91, JMO95b, Me98]. Many-Prover
[DY91a, DY91c]. Many-to-One
[BHSV98b, BHSV98a]. Many-Valued
[KW99]. Map [Bih91, KMKH99, CPPK98,
HNS91, LY94, TOU94]. Maple [Yan95].
Mapper [BPR99]. mapping [FO90].
mappings [LF94, Nyb94]. March
[ACM98a, An905r, BCB97, IEE99b, IZ99,
Knu96c, Nat99b, Uni99b, Uni98b, Vau98e,
Uni98g]. Market [War96, Org98a, Sta97c].
Marketplace [GC97]. Markets [And96a].
Marking [BLMO94, LMBO95, LM99b,
PARK98, PA98b]. Markov [AA93, HSW94,
LM91, LMM92, MFG95, OG95]. Marks
[LT98, BBC98a]. Markup
[Uni98b, Uni98c, Uni98e]. Marling
[CFK∗91]. Marmaras [Pit95]. MARS
[BCA∗98, Con99b, Zm98]. Marvelous
Maryland [ACM90, An9064a]. MAS [CF99].
Machine [CVM∗91]. Masked [Web93].
Masking
[CIJ95, JMLW94, SZTB98, Tl99].
Messaging [DDJ98c, AC97, DMW94]. Meta
Multidrawing [BMRW98]. Multifeature [Bet95c]. Multifunction [She94c].
Multigroups [OOK91]. Multilevel [CGB+93, GPSN98, KT96, DN95a, ZH93].
Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, Dt’98, ES98, FJV97, GO96c, HF97,
IEE96b, IEE98c, IR99, KR597, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k,
Kat97, LS98a, Ok97, PS97]. Multitap [BMRW98]. Multitap/Encrypted [GMCF95].
Multitap/Signed [GMCF95]. Multipart [GMCF95]. Multipart/Encrypted [GMCF95].
Multipart/Signed [GMCF95]. Multiparts [GMCF95]. Multiparty [Cha90, CDD+99, FW91, MH96].
Multipermutations [SV94, SV95a, Vau95].
Multiple [AS96, Bih98a, Boy90, DK96, GO96b, Han94, Kal92, KR94b, KR96a, SS99c, SHK99b,
Wag98b, Bih95a, GK94+99, GPSN97, KR95a, KSL92, KM98c, Ort95b, Ort95a, SSM94].
multiple-iterated [Ort95b, Ort95a].
multiple-length [Han94].
Multiplication [Abe99, KAK96, Kor93, MS93, Zim99, FBT96, Ha99, LC98, TY92].
Multiplications [MNSV97].
Multiplicative [BBDW96, DDB95a, DDB95b, Mis97].
Multiplier [HMvT94, HWB93].
Multiprocessor [MHPS96].
Multiprocessors [Lei99b, HJ99].
Multireceiver [SNW98a]. Multiresolution [BCV97, HW99b, SZT98a, SZT98b, XBA97, KH98a].
Multitouch [Geh94, Geh95].
Multisecret [DLR97, JMO94, WAM094].
Multisecret-Sharing [DLR97].
Multisender [MSN97].
Multisignature [O093, CLHL98, FD92, HZ93, HCC98, LH99, LHL95b, LHL95a, PPKW97].
Multitude [Fuc99]. multiusur [LS98a].
multivalued [CGV94]. multivariate [M90].
Multiversion [KT96]. Munich [IEE97d].
munition [Buc95b]. munitions [Un197d].
Muscle [Cor98]. Musicians [MB99a]. Musings [Ins95]. must [Csi95].
Mutual [Bak99, ARK99, BO99, CS96b, CS97b].
Mutually [CGM97a, IS91, Mar97, HY93a, JMO95a, Wu92]. My [Cur98]. mystery [Fra93].
Mythical [Sil99].

n [ISO97, TN97]. n-bit [ISO97]. Naccache [Cus97]. Naccache-Stern [Cus97].
NAFTA [Mad98f]. nag [PNdbbbprm91].
Nam [CLW98]. Name [Gar97a, Gar98b, Ano97-29, Lea90].
Nanomedicine [DDJ98e, DDJ98f]. Naor [Geh94]. Napa [IEE93a]. Napier [CWM+91].
narrow [CC98]. narrow-sense [CC98]. NASA [CWM+91]. National [Acc97, Ano96a, DDJ98b, Dam96, IEE94b,
NIS92, Un98a, Wei91a, Wei91b, Rat96, Un98d, VB96]. Nations [Sch98a].
Natural [Din94, KKL99]. Nature [BMM99a, BM99b]. Naval [Wei99, SW94b, Uni95b, Win93].
NDRAM [Gar97b]. Near [Tay95].
necessity [KK97].
Need [DS98b, Fly97, RS98c, Van95]. Needed [RSxx]. Needham [Low95, Low96].
Neos [Pit95]. nested [BO99]. Net [Gar97a, Gar97b, Gar98a, GB98, Got99,
LL97a, MB99a, Way96a, Abe98a, BCW97].
NetBill [CTSxx]. NetCard [AMS96].
Netherlands [Cha91, Hei96a, TV94, Tv92]. netlist [CKM99].
Nets [Des98a, DR98b, KA99, YK98, NT93].
Netscape [DDJ98g, DDJ98h, GW96, Law98, She96b].
NetTracker [Ano97-34]. NetWare [ARH95]. Network [ACM98a, BK90, Coh99, DS90a, Ebe93, EH96, Fum93, GM93a, HS96a, Kan96, Koh90, KN93, KCCT94a, KCCT94b, Law98, Lee95, Len96b, Lom94, Mar99, MSK99a, MT99b, RS99a, She93d, SV99, SS99d, Tun99, VDDR99, VNW94, VNW95, WKHG97, WN98b, Wu96, AP93, BGT96, Ha97, IS99, JJ95, SS99a, SY96b, Sta99a, UCF94, Yor96, ZG96].

Network-centric [BGT96].

Network-Layer [Wu96].

networked [Ano97-28].

Networking [IEE98e, FJV97, LS98a]. Networks [ATAY98, AWV99, BF97a, Bra90a, CT99a, DQ93, HG97c, IEE97l, IEE98f, Jut98, KR97, Lea99, LSVV95, OM98, PKOT94, PT95, Por91, Sal91, SK96c, SK96d, SV94, STP93, THP98, Tow98, VDD97, Ver98a, Ano95q, Ano96j, ACBR90, Atk93, AC97, BF99b, CW91a, CWY98, Fra90, GBL94, HT95, Hor94, HLL99, Jen99, LC96b, LC96c, NT94, Nor95a, OC95, Opp96, PS98c, PS98d, PS98e, PS98f, PS99d, PS99a, PS99c, PS99b, SV95a, SBT99, Zan90]. Neumann [HLL95]. Neumann-Stubblebine [HLL95]. Neumann [CFK91].

Neural [Mar99, ACBR90, SBTV99].

Neuro [ZHJ98].

Neurocybernetics [Mor98]. Neupathy [MR95a].

Neuve [Dan96, Q98].

Nebraska [ACM95, AA97].

newer [Mon96].

NewDES [KSW97a, KSW97b]. News [Ano93e, Ano94a, Ano95p, Ano97-29, Ano97-33, Bar97, Bar96a, DD98c, DD98e, DD98f, DD98a, DD98d, DD98b, DD98g, DD98h, DD99, Eri97b, Fox99, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, GB98, Got99, GO96c, Law98, Lea99, MB99a, Ros98b, T97, Taa98, WSFC99, Wor96, Bra90b].

Newton [AVPN96, Ber96b]. Next [Kai97b, SS91].

NFS [D95]. NHS [Zer96a].

NHSnet [Zer96a].

Niagara [IEE96d].

Nisbet [BMRW98]. Nicholas [Ano97k].

Niederreiter [LDW94]. Nikola [Ano97-37].

NIKS [Cop94b].

nine [Tat98, Tat99].

Nineteenth [Alv98c].

Ninth [Ano95r, IEE93c, IEE94b, T98, ACM97c, LLMP93].

NIST [Bra93a, Dra98, Nat92a, RHAL92, Riv93c, SB93].

NISZK [GSV99]. NJR [TGKI99].

No [DD98e, DD98f, DH90, RS98b, Sak96, Ano97-48, BBR99, GBL94, Mei98, PS97, YT96].

No-Transferable [Sak96]. nodes [GMLH94].

noise [PC98].

noise-based [PC98].

Noisy [C97, Lip94, MSH99, MM92a, MFG95, GM91].

Nomikos [IEE97c].

Nominations [Nat97b].

Non [AWV99, BM90, BG90, BS99b, BS99c, BS91b, DY91a, DD99, DR94c, DDN91a, DDN91b, FCD98, FDB93a, FDB93b, GPT91a, GPT91b, GP99, GO93, HJPT98b, Jak98, KR96c, LC99, Mas99a, MY91, NO98, Pai98a, Pai98b, Ped91d, Ped91b, RS91, Sah99, DY91c, SC99, TSY98, Yah94, Ano95q, BKR98a, BKR98b, DDB95b, Ell97, HJPT98a, LL99, MO93b, SB95, Sin95, SBT99, DDB95a].

non-Abelian [DDB95b, DDB95a].

Non-biased [TSY98].

non-carcinogenic [SBTV99].

Non-classical [Mas99a].

Non-Commutative [GPT91a, GPT91b].

Non-Encrypting [LW99].

Non-Euclidean [SCG99].

Non-Existence [FDB93a, FDB93b].

Non-Interactive [DY91a, GO93, MY91, BM90, G90, DD99, Ped91d, Ped91b, RS91, DY91c, MY93b, Sah99].

Non-invertible [NO98, BKR98a, BKR98b].

Non-linear [DDB95b, DDB95a].

non-linearity [SB95].

Non-Malleable [DDN91a, BS99b, BS99c, DDN91b, Sah99].

Non-maximal [HJPT98b, HJPT98a].

non-Oracle [Ano95q].

Non-perfect [Pai98a, Pai98b].

Non-Reachability [DR94c].

Non-repudiation [GP99].

non-secret [Ell97].

non-secure [Sin95].
Optimisation [CD98a, FCD98]. Optimised [RC94a, RC94b]. Optimising [DN95b].
Optimistic [ASW98, GMJ99a, GMJ99b].
Optimization [ARK99, DDNM98, RP98].
Optimized [EPR99b, EPR99a, SL99].
Optimizing [Cla97, MS99b]. Optimum [OK96b].
Option [Web99, Ros94, Sta97c]. Oracle [Ano95q, GHR99, Ano95q, Got99, MSO96, Web99].
Orange [IEE96f].
Ordinary [Miy93b].
Oregon [Auc98, USE90].
Organized [Far93]. Organizing [OMV98].
Overview [ASM98, BPBV99, DHMR96, Lan98, Lin93c, PGV92, YS99, dRHG+99, Ger97, Ste98a, VNP98, YS91]. Ownership [Car95, CMYY98, BO96a, Oko96, QN98b].
P [YT96, Ano95n, MS90b]. P-1 [MS90b]. P [IEE97c].
P1363 [Ano96-28, Ano97-44, Ano97-45, Ano98r, Kal97a]. PA [AR97].
Pacific [Uni98e, Win93]. Pacífico [IZ98].
pack [Ano98d].
package [Web99, Ros95, Sta97c].
packing [Mou99].
packings [Mou99].
Packings [Mou99].
Pack [Bro97].
packing [FMR99].
Pairs [Kwa93, Miy93c].
Pale [Bar92b].
PalmPilot [DB99].
Panama [DC98a, DC98b].
Panel [ADKN90, CFGS99, CPOR97, EQ98].
Papal [Alv98c].
Paper [BFK99, Cha93, CM99c, Fuc99, Mer90b, YST99a, Gol99c].
Papers [SB97, Ano95r, Cha91, CFG96, RRP97, CW94].
Paradigms [BG90, BFN98a, RS99d, Gre94].
Parallelisation [FCD98].
Parallelism [BS91h, Cla99, PP92b, Pos93, Pos98].
Parallelization [BVFD99, RG99].
parallelized [BL99a].
parallelizing [GLV99].
Parallels [Fis98].
Parallels [Fis98].
Parallels [PES97].
Parameter [BM94c, Len99a, FK93b].
Parameterized [Car95].
Parameters [Coc97, IKNY98, HEG98, HYLT99].
Parametric [PRAM98].
Paramita [JC98].
paranoid [GGOQ98]. Paranoids [Sha95b].
Parasites [NM95]. Paris
[Chr98, Org98a, Vau98c]. Parity
[KT91b, KT98, PK95a, PK95b, Pen96].
Paris [AA95, ANS97, Org98b, Smi98b]. Part
[AA95, ANS97, ECM96, Fri92b, ISO97, Lin88a,
Lin89a, Lin90a, Lin97b, Cli97, UU97b].
Part-of-Speech-Tagging [Lud97].
Partial [CDS94, Yac99a, Yac99b, Mao97].
Partially [BF97a, BF99b, Car93, SK94, Xie92,
LMS97, Mau91c]. Partially-Bent [Car93].
Participants [Tou91]. participates [Ano97-52].
Particle [BVFD99]. particular [Des90a]. Parties [PS98g, SS99e, SS99f].
Partitioning [HM97a, KV99, KH98b, CKM99].
partitions [BMxx]. Party [AAB97, BMM99a, BR95b, BG99, Gil99,
IS91, JV96, Ng99, RS98b, FHM98, HY93a,
JW91, Ped91c, Wu92, XZZ98, ZL99]. Paso
Passport [MGL98, vL96]. Password
[Ber98, Bis92, Bli98, FIP93a, HKE99, Hor95,
Jas96, Kle90, KS97c, Lee96, LT91, Nev98,
Pop96, PM99b, RSA99b, Sch99a, BSN96a,
BSN96b, BCR98, CW97, HJT96, JG98,
MW94, ZH93, KW92]. Password-Based
[RSA99b, BSN96a, BSN96b]. Passwords
[De 90, TAM95, Neu94]. Past
[Gad91, SB92, Sim94c]. Patching [Sta96c].
Patent [Uni96b]. patents [Lev91]. Path
[MP9895, RS98a]. patient [Cha99b].
Pattern
[Des99a, PN9K95, WD99b, Sch91b]. Patterns
[Lut98]. Patterson [MSS93].
Paul [Sha99a]. Pay
[DD98e, DD98f, ZL99]. Pay-per-View
[ZL99]. Paying [Ped99]. Payload
[Atk95b, KA98c]. Payment
[DV96, FJ98, HP98b, Sch98b, PSW95].
payments [HSW96, Ped95]. PayWord
[RS96b, RS96c]. PC
[Bec97, Com90, Fra92, GC97, GO96c,
Jac90a, Jac90b, KS97b, SvA98, Sch92a].
PCAT [GN95b]. PCAT-94 [GN95b].
PCKS [BG98]. PDEs [LP94]. peace
[Des90a]. peacetime [Sch98a]. peak
[SVWM95, SOB98, VSB95]. Peaks
[Mae98]. Pearcy [CFK91]. Pearl
[Kai98b, Par98b]. Peer [SK96b, SK96e].
Peer-to-Peer [SK96b, SK96e]. pen
[Ano93k]. Pendergass [Bur98a].
Pennsylvania [ACM96b, IEE97e, CH96].
Penrose [Gar96a, Gar97d]. Pentium
[BGV96, Bosxx, SW97a, SW97b]. People
[DKK98, Ers99, Sch94c, CI99, CG05,
IEE95c]. Perceptive [GDD97].
Perceptron [KM99b]. Perceptual
[SZT98a, CM97d, SVT98b, SVT98c].
perceptually [CL98]. Perfect [KB95b,
BS91g, DDP94a, DF93, vD99a, Joh94, J96,
Man91c, MW94, MK92, NOV99, BD98b,
DP94, Pai98a, Pa98b, SC97, TS93, vD95b].
Perfectly [BD9H93]. Perfectly-Secure
[BD9H93]. Performance
[ACM98a, Ano95b, BMS99, DMP98, FC94,
GN95c, HJ99, HWJ98, IEE94e, KR96a,
Kea99, LL95a, LM98b, PRB98b,
Roe94, Roe95, SKW99c, SKW99a,
SKW99f, She92e, Sm99a, Sut99, Tou95,
VNW94, Wie98b, Nor95b, NO96, SS98].
Performer [KS98b]. Period [RH99].
Periodic [Mun91a, Mun91b, Abe98b].
periods [Gv998, Perl [DD98a]. Permit
[Joh94]. Permits [Gar97b]. Permutation
[BM92, BS90b, CT99a, EM93, HMv94,
Pa99b, Pat99, CSV94, HT95, O'C95,
Pat91b, Por93, Zan90]. Permutations
[BY93a, DW94, FJ9896, PS97, CZZ98,
Pat91a, Pie93, Sha94, SM98b]. Permutated
[BCCG93, KM99b]. perpetual [HJKY95].
Persistence [DL99]. Person
[BBDF97, Ble98b, DLF97, DMFB97,
WKG97, BC97]. Personal
[Ano97-34, BE90, Bar05, Cae96b, EH9999,
Gar97b, Hamxx, Los97, Los98, R99a,
Rivxx, Cra96, Mil95, Wil93a]. Personalized
VPM97, Zim96a, Zim96b, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, Zeg93.

Privacy-Protecting [Tra99]. Private
[BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, Mr93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts’90, Wil93b, ZG96].

Private
[BD98, BD99b, CKGS98, HR90, Mv93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts’90, Wil93b, ZG96].

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

Privilege
[ECM96].

Prize
[GC97, Pin98].

PRO
[Ano97-33, Gar98c].

Proactive
[CHN97, FGMY97b, HJKY95, HJJ+97, HJJ+xx, IBMxx, Jar96, Rab98, BCR98, FGMY97a].

Probabilistic
[Jak98, JO97, SF97, Sch91b, Tou93, Gol99a, GO95, HK90, Imp92, Lon91, TX92].

probabilities
[Lew92].

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

Probable
[BD93, NK93, DL93, Graxx].

Problem
[Bon98b, Bon98a, RN93, CS96a, Cha90, DD99, DJL93, GO95, HM98, KM99b, KR99b, MT99b, NS99b, OMV98, Per99, RS99a, CPS95, HY93b, HI97, HM97b, HMP95, LC97b, Mas97, McC90a, NR95, OA99, MSO96].

Problem-Solving
[Per99].

Problems
[AA93, BD95a, Bra90a, GGH97b, KR999, MC92, Poi99, Sm90, APDS93, Bea92, BFKL94, FR95a, Han95, Han99, HC95a, IEE97e, Lew92].

Procedure
[Ada97a].

Procedures
[Hig97b, Lin93a, Lee95, Lin88a, Lin89a].

Proceeding
[BPR99].

Proceedings
[ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, AN95, AN98n, BKL92, Bri93, COM96, GN95b, IEE95a, IE91, IE92b, IE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96e, IEE96d, IEE97d, IEE97e, IEE97f, IEE97i, IEE98e, IEE98f, MZ98, Nat99b, OW95, PSN95a, Pit95, St93b, SLJ93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96e, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94e, Bih97c, B+96b, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fun97, Go90b, HO97, HA90, Hir97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, KG93, Knu99c, KP99b, KK99b, Kra98, LQ999, LM98a, LW96].

proceedings
[Lom97, MV91, Nyb98, OiDP98, Pre95a, QV90, QG95, Q+98, Rue93, SQ93, Spi95, Ste99b, TM99, TV94, T+98, Tv92, USE90, USE98d, VPM97, Van98e, Wat91, Wие99, Woll9b, Yua92, vWN99, ACM93b, CH96, Chr99b, IEE94e, St94, Wall99a, BCB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fe91, Go96d, GQQ5, GS94b, He94, IRM93, Kal97c, Ko99b, Mau96b, PSN95b, SP90].

Process
[AMP94, Ku99a, Ro98a, RS99c, YT96, CWM+91].

Processes
[Gar98b, Bea92].

Processing
[Ano97b, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97b, IEE97d, IEE97j, IEE97k, IN99, KV99, LMP99, LW96, Pin98, Pi95, Ano96-30, DO99, DF97, Man98, Sab94, T+98, Wh90].

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

Processor-efficient
[Von92a, Von92b].

Processors
[Cl97, KK99a, She92e, BS95c, MHP96, NM96a].

Proctoring
[SKW96].

Prodigy
[CFK+91].

produced
[SSI97a, SSI97b].

Product
[GO96c, KSH98a, KSH98b, KSH98c, GN95a, SS98b, Ano94i].

Products
[Ano97-33, Ano97-34, Cha94b, Cl97, Los97, UU97b].

Professor
[Swi97].

Profile
[Hor92, HFPS99, MM90a, MK92].

Program
[BDFM99, FGY96a, LBMC94, FGY96b, KT99, LS98a, Pre97b, Pre97c, Uni95a].

Programmable
[DMVC99, SVB99, TT99, WB94].

Programme
[BG93].

Programmer
[Bre99, DDJ98a, Jol95, Ste94b, vWS97,
Programmers [Gar97c, Joh97a, Joh97b]. Programming [IBM93, BGS96, CO98, Eri97a, JDK+91, Ste90a, Ste90b, ACM99a, Gre98, LS98a, OA99, Sab94, vWN99]. Programs [BK95c, DRR95, SG95, SHK99b, WB95, Zwi98, B+96b, DFHR91]. Progress [Ano96-28, Ano97-45, BDI+96, KSB96b, Wol93b, Wol93a]. Progressions [Miih94]. Project [BBPV99, IBMxx, GH96, Man98, DS90b, RCM99]. PROMIS [SSCP99]. Promise [Law98, Los97, Mar96]. PROMIS-MmNet [IEE98e]. Promises [Law98, Los97, Mar96]. promises [Way93b]. Promotes [GO96c]. PROMS [IEE98e]. PROMS-MmNet [IEE98e]. Proof [Bol98a, Bol98b, CD99, CDS94, FOO91, GMW91, GK96, NMY99, RS91, Zhe95b]. Proof-Based [Bol98a, Bol98b]. Proofs [BG90, BG93, BD91, CD98b, DFKN93, FS97b, GMW91, GO93, JMS96, CDP95, DP94, Gol99a, PS96d, Sak97]. Propagation [GPR98, SG99b, SZZ95c]. Properties [Boy99, Con99b, KA99, MM90b, MS91, OK98, OS98, Tou93, VW98, WW98b, Zie97, BHRR99, CDP95, FSS94, KSB96a, Koh91a, PS93a, XZZ97]. Property [CFG899, DL99, LQRS98, SRY99, Uni97b, Ale98, BS95c]. Proposal [ABK98b, ABK98c, ABK98a, BAK98, DR98a, KR94a, LM91b, Ano95n, Cil99, LM91a, RHAL92, RS98y, Ban94]. Proposals [Dae99, VvT97]. Propose [Gar98b]. Proposed [CP91, Lea99, LL98a, Nat92a, Riv93c, SB93, Wag98b, CM99a, Guo99, Mey96b]. Proposes [Gar97a]. Prosthesis [HHD99]. Protean [SV999]. Protect [Sch94i, Sta95b, Cil99, KR96b, Way93b]. Protected [CH94b, DY91f, Mad98b]. Protecting [BO96a, Ble98b, Des90a, EHMS99, GMD98, KR98, Lut98, Mar95b, MW98b, PT95, SYM98, Tra99, VP99]. Protection [BG98, CH97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LQRS98, LvdLB96, LvdLL97, LML98, Per97, Smi90, Uni97a, Uni98i, ZK95, ZK96, Ale98, BBCP97, BBCP98a, BOD95, CPO+98, CHO+98, Cli99, DFHR91, GO96a, Ibb97, OPH+99, RP94, RKDB96, SY96a, Sta94a, Te92, TSN93, Unt97c, YEA+98, FT95]. protections [HPA99]. protects [Ano95m, Ano96j, Ano97-43, Ano98d, Ano98f]. protest [Ano97-52]. Protocol [ATAY98, Ano95a, BWM99b, BV98b, Bra95a, Bra96, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JMP+98, JQ97, Kas96, KSW98a, KSW98b, KS98b, Kra99, Kum98, Low96, Man94, MW99, Mey96a, Mow92, NS98b, NS98c, OMI93, RS96a, RS98b, SSN98a, SH97, SM98a, SM95a, Sim96b, SM96, SM98b, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CM96, CTSxx, Des96b, EvH93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS98f, SK97, Sim94b, TH99, WS97, WL94, Zhe95a, GM93a, Sar97]. Protocols [AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BGH+91, BWM98, BWM99a, BBCM93b, Bel98a, Bol98a, Bol98b, BD97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dan99a, DGT96, DQ93, DS97d, Fei93, Fei96, FBS97, Fum98b, GM93a, Geh95, GS97, GMV98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IEE98e, KKK91, KY92, KS97c, LH93, LL97a, LHB96, LL95a, LS92, LM96, MB94a, MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, SL93a, Sch94g, Sch96a, Sch94h, Sch99k, SSP90, Sy92, Tou91, Tou93, AN94, AN96, AG97b, AG97c, AG97a, Aba99, ABC+98, BDH97, BH93, BCK98, BGH+95a, BBS98b, BM95, Bra90b, CG96, Chr98, Chr99b, CJ95, Dan97, FGH99, Fe99, GEL98, Hor98, HLL+95, JW91, LY93, LHW99, LL95b, Lon97, Man95, Mas97, MLY93, Mea95, MW98c]. protocols [NT93, PS98e, PS98f, PS98f, Pau98, PW93a, PKM97, SSG99, Sy93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].
GHY90, GGH97b, HK99a, HGS98, HP98a, HMV93, Hes97, Iss90, Kal99, KM99c, KT91a, KMOV91, LM94b, Low96, MY91, Mic93a, Mic93b, NS97a, OU98a, vO91a, PSR97, Pai99d, DF91, Sas99a, ST91, Sun98a, Wie98b, Yam98b, YST99a, YST99b, Ano96w, Ano96-30, BFS92a, FGLP96a, FGLP96b, GH99, HY93b, NY90, Nec91, Sal90, Sal96, Smi93b, Yam98a, AD97, AD99, BFP99a, CA99a, Cle96, Cra97, DQ96, Dhe98, DN95b, ES97, FGM97a, KASH90, KM99a, KM99d, LM94a, LZ91a, LDW94, LCL95, Lon92, Low95, Man91b, MY93b, NM96a, Ole95, SW95a, Sch92c, Sha95a, SS95b, SS95c, TC99b, Tze99, Wan92b, XLP99, Yu92.


Rejected [Eri97b]. Rejects [Gar97a, GC97]. Related [Ber97c, BV96, CH98, Cle91, CFPR96b, De 93b, De 98c, ECM96, GS97, KSW97a, KSW97b, WB95, Bih94a, CFPR96a, OU98b, Zer96a]. Related-key [KSW97a, KSW97b]. Related-Message [Ber97c]. relating [Aus96]. Relation [BHSV98b, BHSV98a, SK98c, SK98b]. Relations [BDPR98, Jak98, NMV99, Uni98c, Uni98d, Uni98e, Tze99]. Relationship [GSV99, HT99, MW99, Oka93a, SZZ95c]. Relationships [Kem99, Lef99b, RG95, SS95a, SG99b, SZZ95a, GK9+99]. relaxes [Ano98v]. relay [Ano95m, Ano99h].


Replay [OG97, YL97b]. Replicate [RB94]. Replicated [KB92]. Replicating [HS96b]. Replication [BLM94, Pit96b]. Reply [NC97, BMP+97b]. Report [Bra93a, BDI+96, Dra98, MMM98, Kni91, Nat99c, Par98c, PH91, RIP95a, RD99a, Tou95, Vau99d, Wor96, Ano96a, BF92a, BP95b, Bur98a, KSB96b, NBD+99, Org98a, RIP95b, UU97a, Zer96a, Dan95, BF92b].

Reports [Ano95e]. Repositories [CHLT99]. repository [HSK97]. Represent [MI99]. Representation [CK95, Ger99b, JKVP99, LE99, NA95, PNFK95, TY92]. Representations [FC99]. Representatives [Cl97, Uni97a, Uni98c, Uni98d, Uni98e, Uni99c, Uni97b, Uni98f, UU97b].


Research [Ano99c, Boo96, DDJ98c, Dam96, Des92, Des98c, DE92, Ele98, IEE92c, IEE93b, IEE94d, IEE98d, Jan99, Q+98, Rhe93, Wol93b, Ano97-52, Wol93a]. researching [Uni96a]. Resend [Ber97c]. Reserve [An97-42]. Resharing [AGY95b].

Residue [KKOT91, PP92b, CB96, PP92a, PP95b, PP95a]. Residuosity [Pai99d, DPD94b]. resilience [FGMY97a].


Resource-Aware [BCC99]. Resources
Nat97a, NP98b, Pad98, PHF99, Rab94, SC96a, SZT96a, SZT96b, SZT98, TKS98, ZK95, BBCP98b, BD97, FGY96b.

Robustness
[AN95, MMST98, YMWP99, Irw98].

Rockland
[GS94b]. rocky [Ano97u].

Role
[Car97b, DDJ98d, JJ95, Lin96a, VC99, DL96, Dam96, Mau93b, Par96, Sin98].

Role-based
[JJ95].

Role-Centered
[VC99].

ROLLING
[PWU99].

ROM
[Ano96r, GTGW94, Ros94, UFC94, Yuv97].

Roman
[Has95].

Rome
[Knu99c, Nat99b, Wol93a, Wol93b, DDJ98b].

ROMs
[GTGW94, UFC94].

Ron
[Riv93a, Riv95a, vdWS97, Woe97, vS97].

Roosevelt
[Kah98c].

Root
[Cop95c, JJ91].

Rooted
[PB99a].

Rooted-Tree
[PB99a].

Roots
[Kob97].

Rosemont
[IEE97g].

Rosenheim
[Sha99a].

Rosser
[Ole95].

Rotation
[OP97, OP98].

Routers
[DMVC99, Ano96x].

Routing
[GRS96, RSG98, SGR97, CadHSV96]. rover [Bis90].

Royal
[Far93, Tv92, Don98].

RPC
[SSH93].

RSA
[Ano94b, Ano95f, AA99, And93, Ano95d, Ano95e, Ano95a, Ano95p, Ano95s, Ano96b, Ano97e, Ano97f, Ano97g, Ano97x, Ano97-38, Ano97-41, Ano97-39, Ano97a, Ano97-40, Ano98b, Ano99a, BTD98, BQ95b, BQ95a, BR95a, BR96c, BJQ97, Ble98a, BF7b, BDF98, BV98c, BD99b, Bon99, Bra95e, Bri90b, BM94c, Ca99, CH97b, CH98, CB96, CLE99, CMTNY94, CD91, Cle96, Coc97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, Cus97, Dav95, Dem94, DDLM94, DN95a, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FGM97b, FMY98, FY98b, FR95b, GJKR96b, GKR97, GQQ98, Gil99, GM97, GTS90, Gro94, GS99b, HN98, HWF96, Hor98, Hub91, HP94, IM93a, IM93b, JQ97, JQBD97, JQ98a, KR95c, Ka97a, Ka98b, KS98a, Kir95, Koc94, Koc96a, Koc95, Koc96b, Koy95, KOT95a].

RSA
[KOT95b, KK96, Len98, LHL94, LL95a, Lon91, MWB99, MLY93, Mau90, MW98d, MW98c, MSS98, Mis97, Mis98, MS99c, Mue99, Miu99, NS98b, NS98c, Oka98a, Oka98b, OSA91, PPKW97, PP90, PW93a, Poi99, PS98g, Rab98, RS98e, RSxx, SS97a, SS97b, Sam98, SKNO98a, SKNO98b, SSS98, Sch94m, SPP98, Sha95b, SV93, SH99, Sll97b, Sll97a, Sll98, ST99a, ST99c, Oka98a, Oka98b, OSA91, Wir98, XL99, YY99, Zer96b, Zho94].

RSA-120
[DDLM94].

RSA-130
[Ano96b].

RSA-Based
[CD96, GKR97, VNM99].

RSA-cryptosystem
[Gro94].

RSA-Implementation
[PP90].

RSA-key
[FM98].

RSA-keys
[SSI97a, SSI97b].

RSA-Like
[JQ97].

RSA-Multi
[Man90].

RSA-signatures
[Ev92].

RSA-type
[BJQ97, JQBD97, CLL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b, T99, TT99, VVDJ90, VNM99, Ven92, Vv97, Wat99c, Way98, Wie90b, Wie90a, Wir98, XL99, YY99, Zer96b, Zho94].

RSA-120
[DDLM94].

RSA-130
[Ano96b].

RSA-Based
[CD96, GKR97, VNM99].

RSA-cryptosystem
[Gro94].

RSA-Implementation
[PP90].

RSA-key
[FM98].

RSA-keys
[SSI97a, SSI97b].

RSA-Like
[JQ97].

RSA-Multi
[Man90].

RSA-signatures
[Ev92].

RSA-type
[BJQ97, JQBD97, CLL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b].

RSA
[MPPS95].

RSA
[RSAeuro96b].

RTD
[KW92].

RTR
[KV99].

Ruby
[JS93a].

Rueppel
[NMV98].

Rule
[PL94].

Rule-Based
[PL94].

Ruling
[Eri97b].

Run
[DF91c].

Running
[WF94].

Runtime-Tunable
[WF94].

Russia
[CW94].

S
[SG97, Ano95u, Ano96-28, BD95a, DT93, ECD99, Kim93, Mat95, MC96, PG97a, PG97b, SK98c, SK98b, Sto90, Uni97c, YS99, YY98d]. S-box
[BD95a, SK98c, SK98b].

S-Boxes
[Kim93, PG97a, PG97b, DT93, Mat95].
S-CODER [Sto90]. S.Hrg. [Uni98j]. S.I.S. [Eph98]. S.I.S./CB [Eph98]. S/390 [ECD+99, YS99]. S/KEY [MC96]. S/MIME [Ano95u, Ano96-28]. S012 [KP95]. s02DES [TSM95]. S390 [Deu97, Deu98]. SAC [Kim93, KS97b, MS99a, TM99]. SAC/PC [KS97b]. SAC’99 [HA00]. SAFE [Unic97a, Unic98c, Unic98b, Unic98e, UU97a, Unic97b, BC97, Hor99, VM96, Way95, Deu97, Deu98]. Safe-Tcl [GA98]. safeguarding [Beu94]. Safer [Hir93, BM97, CMK98, KS96, KSW99a, Kel99, Mas94, Mas99b, Vau95]. Safety [Ano94d, Ano98b, DDJ99, Cl99, IEE94b]. Safford [Bur98b, Kru98]. Saint [GQ95, QG95]. Saint-Malo [GQ95, QG95]. Sales [Gar97a]. Salesman [OMV98]. salient [CKLS96b]. Salt [USE95b]. Sam [Mad99g]. Samba [Bl99a]. same [Ude98]. Samos [KG96]. San [ACM93b, ACM99a, Ano97a, Ano98u, Com96, CMM93, FJV97, IEE92b, IEE97b, RP97b, Sch98b, SJK97, USE92a, USE96c, USE96f, USE96g, USE98d, van96, XTit97a]. Sand [SVxW91]. sandbox [MF97]. Santa [Bri92, Bri93, Cop95b, Cop95d, Des94b, IEE97b, IEE98d, Ka97b, Kob96, Kra98, St93d, St99b, USE93, Wie99]. Santorini [IEE97c]. Saragossa [Mau96h]. Sardinas [MSS93]. SASL [Mye97, New98]. SAT [McH92]. Satellite [Ano99f, Gar97a, Gar98a, Lam99]. Satisfying [Kim93, Cus96, CS96c, O’C94, YT96]. save [DF92]. Saving [Ame96b]. says [Riv98c]. Scalable [Hei96b, IEE94e, KH98b, LR98, RG99, SL99, Goo96]. Scale [SA95, SS90, She92a, FO093, OP97, OP98]. Scaling [SA95]. SCALPS [DVQ96]. scanners [Mei98]. Scanning [CO98]. Scenario [AMP94]. Scene [SZT98a, SZT98b]. Scene-Based [SZT98a, SZT98b]. scenes [BDC+95, MCD98a]. SCFS [IHR99]. Schedule [KSW96, KSW99a, Kel99, MM99c, Mur99, SW98a, SW99a, WK98]. Scheduler [KT96]. Schedules [CDN98]. Scheduling [KP93, Por98, SJS98, Sh99b]. Schema [Pit96b]. Schemas [Wed99]. Scheme [Int91a, ADF98, BCC93, BM99a, BM99b, BF99c, BO90, BY92, CT97, CK95, Cop94b, DQ94, DK98a, DN94, GH98, GW98, HL93a, Hwa93, Hwa97, Iv91, IM93b, KS97, KS98d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MS98, Mi96, Mu99, Mi99, NV98, OOK91, O093, OFF93, Pat95, Pet98, PM99b, RG97, Sch99, Sm91, ZL99, AW95, BD98a, CW97, CL98, CC95, CL98, CMT99, CG97, FO093, FO98, GL94, GPS97, Gua90, Har91, HZ93, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM94, Ku92, LWC96, LL98b, LG10, MRS99, MS98a, MLA91, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SS98b, SVW95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WW95, vT93]. Schemes [AW94, BP97a, BC93a, BD98a, BB98b, BK94a, BK95b, BM96b, BM96c, BD93, BD98+4, BFS96, BM99c, BV96, BD90, Bri90a, BS91b, LVL98, BDB92, CS97a, CM99a, CD95, Dam99a, DFW90, DMP98, DY91e, vD95a, DF97, DFB93a, FY97, FOO91, FO99b, GPS97, GP99, GS94a, HK97a, HK97b, IS91]. JS90, K96, KMOV91, KOS9+4, KO95b, KCO95a, LHW98, LM95, MH96, Mis98, MW94, OK98, OKa93b, Pai98a, Pai98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SK93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SS99, YLD99, Zha98, ARK99, BC98a, BR97b, Br93, BDS93, BCD94, BG95, Bl95, BC96a, BCD96, BD96, BMS96, BD97, BFS98, BDV98, BD98b, BD99b, Bur96, BM94c, CD91, CP95, CSV94].
schemes [DP96, DF93, DDB95a, DDB95b, Des99b, FDB93, HY93a, HMP95, HCY96b, JM93, Koy95, KO95a, KO96, KO97, LS98a, LC97a, LHL95b, LHL95a, MS98b, MPSV99, MTN97, Mu92, NR95, OK96a, OKT93, OK95, Pad98, PS98a, PPKW97, P986c, P986d, RD96a, RS96b, SH93b, Sha94, Sha95a, She92g, SW98, SW99a, SS94, SC97, T999, Tze99, VNM99, WAMO94, ZHS94, Z98, dR94a, vD95b, Schernes [BBCM93a].

Schnorr [DBGV93, dR94b, dR94a].

Schoof [IKNY98].

School [Duf98].

Schools [DDJ98e, DDJ98f].

Schroeder [Low95, Low96].

Schussel [Pin98].

Schutz [FT95].

Schwierigkeit [Hor99].

Science [Ano93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97, IEE98a, Ste91, Bed90, Beu94, Sch90c, Sch97c, Shp99a, Sim92, WS96c].

Sciences [Ano95r, Tv92].

Scientific [CHLT99, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97, IEE98a, IEE99a, Ste91, Bed90, Beu94, Sch90c, Sch97c, Shp99a, Sim92, WS96c].

Scientist [BCE +94].

scoop [Ano96-30].

Scots [Sin99].

Scott [Sha99a].

Scramble [JSY99].

Scramblers [GDS91].

Screening [CN99].

ScriptEase [Ano97-34].

Scripting [SVA +98].

Scripts [Duh90, Sch99a, IPNdbbbbrm91].

Scritters [Dum94].

 scrutiny [Den90].

SDK [Ano97-34].

SDNS [NH90].

SDSC [Sch99].

SEA [Sch99j, GC97].

SEAL [HG97a, HG97b].

Scalability [Por98].

Sealing [GS98].

Seamless [DFGH99].


Searches [PKA +98].

Searching [BP95a, DDJ98e, DDJ98f, Jia99, DSSZ99].

seasons [WSFC99].

Seattle [HF97, USE98a, USE99b].

Second [Auc98, Cha91, DEQ92, Hir98, Nat99b, ACM90, AR97, Ano99g, FR95a, IZ99, Lea90, Pre95a, Uni96c, Uni95a, USE96d, VPM97, Hin93, PH91, HK97].

secondary [Atk93].

Secrecy [Aba99, BP98c, GM90, GTGW94, JR96, Moy98, Rat96, Sin99].

Secret [AGY95b, Ano97e, BC93a, BC95b, BCG90, Ben98, Ber91, BS97a, BK94a, BK95b, BDGV93, BM99c, BV96, Bra95b, Bra95c, BS94, BD90, Bri90a, BS91g, Cac95a, Cac95b, CT97, CMPS97, CGMW97, CK90, CFSY96, DDJ98g, DDJ98h, Dae98, Dam94b, DDP94a, DKK98, DFI99, vD95a, EHMS99, FW91, GSNW98, GSN98, HL93a, HD96a, HK97a, HKS97b, HCY96a, IS91, Kah96b, KI96, Kra94a, KOS +94, KOO95b, KOO95a, LYH93, LF97, LM94a, LM94b, LP99, LH93b, MSNW99, Mau93a, MW96a, Mau97a, MSN98, MSN99, MT98, Mus92, NW98, OK98, PS98a, Pai98a, Pai98b, Ped91d, Pra96, Rey96, Rey97, Rey99, Sal91, Sch99i, Sh99a, Sim90b, Sim91, Sim94a, Sti93a, Van93, WI99, Wie90b, Wol98, Al96, AGY95a, BC95a, BT94, BI93, Ble96, BSV93, BCDV94, BDD +94, BGS95, BCDV96, BDGV96].

secret [BD97, BDV98, BDG99, Bur96, CDGV91, Dal97, Dam94a, Dwo91, Ell97, FOO93, FO98, GM95, GPSN97, Gre90, HNSM91, Hel93, HJKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, Jar96, JY98, KO95a, KO96, KO97, LY93, LH95, Me92, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, Ped91b, Ped91c, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, Vv97, Wie90a, WS96c, Win99, Wri98b, ZHS94, vD95b, van97a].

Secret-Ballot [CFSY96, BT94].

Secret-Keys [Ano97e, Bra95b, Bra95c, LM94b, Mau97a, Van93, Wol98, LM94a, JY98].

secret-sharing [RD96a].

secre-t-sleuthing [WS96c].

Secretly [MT94].

Secrets [Cr90, DH90, DSB99, Elc98, HHY93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, Ano91b, Bau97, BDV93, CWY98, JMO95b, WY93, Chi92].

Section [Alv98c].

Secure [AHV98, AB96a, Ano93c, Ano93f, Ano95l,
BHHR99, BCW97, Boy98, Bro96, Com97, Cha95a, CP94, Chi99a, Chi99b, CJ95, Cli99, CTSxx, Dam99b, DS90a, Den99, DEQ92, D+98, FHG99, FFW99, FM98b, Fra92, Gon92, GEL98, Grn98, HN98, HK99b, HOQ97, HS96b, Hor94, HC95a, HC95b, HY95, HLLC96, IEE94b, JT96, JT97b, JJ95, KY97, KG96, Kat97, KSB96b, KSB97, KW92, Kuh98, Lai92, LTT95, Lee95, LHW99, Len93, LC95, MW94, Mar95b, MS97, Mas97, Mau91c, MKKW99].

security [MF97, Mei94, MW98c, Nor95b, PS99d, PS99e, PGV99, PfO96, PR98, Q+98, Riv98c, Ros94, SSN98b, Sah99, Sch92a, SSM97, SMD99, She92c, Sta94a, Sta99a, Sun98b, Tay90, Tho96, TY98b, TY98a, Tsu92c, Uni98j, Uni98k, VB96, VPM97, Ven90, WBDF97, Woe97, Xie92, XL99, XZ96, dVdVI98, van96, van97b, Chr99b, Far92, Uni98c, Uni98b, UU97a, UU97b]. Security-analysis [vT94]. Security-preserving [DI99]. Security-analysis [Ano97-43]. See [Web98]. Seeing [JJ98b, JJ98a, Lut98]. Seek [Gar97b, SV99a, SV99b, SV98]. Seeks [Gar98a, Ano96g]. Sees [Ano96n].


Selection [Bax97, CDF91]. Selection [Hub91, Len99a, PNFK95, BM94c, Fei99, UFC94]. Selections [DKK+98, Ers99]. Selective [GM97, HVH98, IS97]. selectively [WY93]. Self [AW99, BCD98, Fis98, Gir91, GPR98, K197, LC94, Man91a, MS95b, OMV98, SG99a, Sch99d, Jan95, MS95a, Mi96b, Sch90c, Sch97c].


Self-Reductions [Fis98]. Self-shrinking [MS95b, MS95a, Mi96]. Self-similarity [BCD98, Sch90c, Sch97c]. Self-Study [Sch99d]. Self-synchronised [KI97]. Self-Synchronizing [Man91a]. selling [Bee96]. Semantic [BPR99, Mane99].

Semantics [DJHP98, DE99, FL99a, RZ99, RS99c, SG99b, Syn92, WK96, Ts'90].

Semiconductor [Gar97c].

Self study [Ano95d]. Sensimetics [Gog99]. Senate [Uni98h, Uni97c, Uni95a, Uni98k, Uni98g, Uni98i]. send [Way91]. Sender [WP90, Wai90]. senders [HW98c].


SentryLink [Ano95e]. Seoul [Ano93g]. Separability [CM99a]. Separable [LY94, AM99]. separate [WY93]. Separating [MKKW99, Tou92]. September [Ano98a, D+98, ES98, FR95a, IE96e, IEE97e, IEE97k, Kat97, LW96, Q+98, Spi95, TV94, T+98, Uni97a, Uni96c, Uni98j, Uni98k, USE92b, USE96a, USE98b, Gar98a].

seq [Cly97, UU97b]. Sequence [LY93, GM91, LY93, MHMW98].

Sequences [DSV99, JQ97, MS94, Mun91a, Mun91b, PMP99, SB94, Bla94a, GN95a, Gol99c, KSB96a, MK92]. sequential [LHW99]. ser [IPDnbbpr99]. Serial [S193a, SSG99, Yor96].

Series [Ano95d, HEQL98, CJ98a, CJ98b]. Series-Parallel [HEQL98]. Serpent [ABK98c, ABK98b, ABK98a, BAK98].

servant [CWM+91]. serve [Sch93e]. Server [Ano97-33, Ano97-34, BP95b, 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, CGM97b, GGK+99, Lee95, Ude98].
Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau93, MB99a, RRSW97a, RRSW97b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, RFLW96, Zha96, Ber96a, KN93]. Service-Level [MB99a]. Serviceability [WP90]. Services [ANS98b, Cas95, HVH98, RB94, VSH97, VFD98a, A95, AC97, D99b, Don98, KW92, PS99b, You97, Zer96a, AA95, Acc97]. SES [Bou94]. Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AC95, Uni97a, Uni98c, Uni98d, Uni98e, Uni99e, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k]. Session-Layer [BB95c]. Sessioneer [AG95]. Set [DJL93, FP99, IS91, Koz96, Mei92, SPP98, Sta96b, SX90, GB98, Kra99]. SETHEO [Sch99k]. Sets [MT98]. settings [Car97c]. Settled [Eri97b]. Several [HGS98, LL95b, MH96, Sik93]. Severely [Gib95]. SG [Gue98b]. SHA [ANS97, MG98b, BGV97b, CJ98, MS95d, MS95e, Sta94b]. SHA-0 [CJ98]. SHA-1 [ANS97]. Shakespeare [Lea90]. Shallow [ACD94, WF94]. Shamir [She92g, Ada92b, GGOQ98, Nac93, OOK91, OO93, The95]. Shamir-like [Nac93]. Shannon [Hor92, Sga91a]. Shannon-theoretic [Sga91a]. Shape [HHD99]. shapes [Ger99b]. Share [BMW99b, Cs95, DDFY94, Sim90a]. Shared [BF97b, DHMR96, DF91a, DH90, HD96a, IS91, Le99b, MWB99, PS98g, RZ99, SN96, Sim90b, Sim91, Sim94a, W99, YL97b]. Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [MSNW99, BDG99, CDGV91, OK95, ZHS94]. Sharing [AGY95c, BC93a, BC95b, BBDW96, BK94a, BK95b, BDGV93, BDD+94, BM99c, BD90, Bri90a, BS91g, Cac95a, Cac95b, CG98, CT97, CK90, DDP94a, DKKK98, vD95a, DLR97, FDB93a, FGY96a, GJKR96b, GPSNW98, GPS98b, HL93a, HKS97a, HKS97b, KI96, Kra94a, KOS+94, KOO95b, KOO95a, LP99, LCL92, LH93b, Me195, MS95f, MSN99, NW98, OK98, Pai98a, Pai98b, Ped91d, Rab94, ROT94, Sch92b, Sch99i, Sti93a, Wil98a, AGY95a, BC95a, BI93, BDV93, BDSV93, BCDV94, BS95, BCDV96, BDGV96, BD97, BDV98, BDG99, Bur96, CDGV91, CMAP97, CGMW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FGY96b, FR95c, FO98, GM95, GPS97, HJKY95, Hwa92d, HC96, HLC99, JM93, JM905a, JM905b, Jar96, KO95a, KO96, KO97, Mao98, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, PS98a, Ped91b, Ped91e]. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95b, van97a, Kol95]. Shark [RDPB96, WG97]. Shawn [Sha99a]. Shedding [HPG98, YY99]. Shelf [Hat96, AG95]. Shell [Car99, Sch99a]. Shifted [GO96b, Ga94, GN95a, GM91, GO95, PS97]. shift-register [GN95a]. Shifting [DG95b, Ship [NS98a, RP98]. Ship-Board [NS98a]. shipping [Ano95q]. Shooting [Ag92]. Shop [Ano97-33]. Short [Kra94a, Ste94a, Wie90b, vOW96, BC95a, Coh94, Har94, Joh99, VW96, Vv97, Wie90a]. Shortage [DDJ98a]. Should [Way93c, YY96, Ano95c, Riv98c]. show [Mad98g]. shrinking [MS95a, MS95b, Mih96]. SHS [NS93b, Nat92b]. shu [XuTuW94]. SIAM [AC97b]. siber [Ano97-50]. sichere [Hor99]. Side [KSW98a, KSW98b, KSW98c, SvA+98, YY96]. sides [MB94b]. Siege [EH96]. Siegenthaler [MS99b]. Siemens [Ano97-47, Bro97, Dav98c, Mac98, Sel98b, T97]. Sieve [LLMP90, LL93a, Per93, CDEH+96, Gor93b, Pom94]. sifrovani [Gar98c]. SIGACT [AC97b]. SIGGRAPH [AC99c, B+96b]. Sight [Phi98]. SIGINT [Mye98]. Sign [BM92, GR97, GHR99, Web98, BR96c].
Signal [IEE97c, IEE97d, IEE97k, LW96, Pit95, She92e, T+98]. Signalling [Lin98].
Signals [AK99, BTH96, DDNM98, MHMW98].
Signature [AA95, Acc97, AW94, Int91a, NIS94, Ano96f, Ano97-50, BP97a, BM99a, BM99b, BM96c, Bra93a, CS97a, CM99a, CG98, CH98, CK95, CDF95, CD95, DMPW98, DQ94, DY91e, DN94, FL99a, FMKY98, FOM91, FO091, GP99, GQW+91, HJJ+xx, KKS97, KS98d, KPG99, Kob98c, Kra93, LK96, LHW98, LK99, LHL94, LL98a, MT94, MB99a, Mer90b, Mer97, MH96, MSS98, Mis98, Miy96, Mon93, Nat91, Nat92a, Nat94c, Nat94a, NMVR95b, NaI97, NMV98, NMV90, NIS93a, OVF93, Oka93b, PF94, Pet98, PM98, PS96c, Pj99, RGV97, RDK98, Riv93c, dR94b, SC96a, Sch93b, Sch94e, SK97a, SE96, Sim93, Sin98, SB93, SSSNP99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, ARK99, Ala93a, AW95, Ale97, Ano97p, BD98a, Bis90, Boy97, Bur96, CP95, CMTNY94, CSV94].
signature [DP96, FR95c, Gua90, HY93a, HJJ+97, Hor98, HMP95, KS98c, LWC96, Mau91b, May97, MS98b, Mu92, NMVR95a, NR95, Pi96c, Pi96d, PS96d, PS98b, SI93b, Sha94, SS95b, SS95c, Ste95, Tilt98, Tra97, TJ99, Wan92a, Wi93b, Wn92, XA98, YL95b, YL95a, Yeu99, Zho94, dR94a].
Signatures [ANS98b, ASW98, AT99, BD99a, BQ95b, BQ95a, BG90, BdM94, BM94a, BM96a, BC93b, BF99, Boy98, BS95d, CV991, CR91, CDF95, Cop99, CD96, Dam94b, DF91a, EG9M0, EM969, Ev9H1, Fro97, GKR97, GHR99, GM97, GO93, HKS95, HA96, JM99, JQBD97, JLO97, Len96a, LSV95, LR98, MS96, Mis97, MB97, NW98, OO98, Oka94, PP97, PW93b, PG93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, She97, Tra99, Web98, Wh94, vHP93, Ano98e, BR96c, BGR98b, Ble96, BCDP91, BM91b, Com97, CPS95, Cha95b, Dam94a, Ev92, EvH93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, Fed91a, Pi96c, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].
Signryption [Zhe97b, BD98a, Ye99, ZI98]. Signed [Ber97a, GMCF95, KT93, SKAM99, Sun98b]. Signer [CVHP91]. signers [TJ99].
Significance [DF9H99, SBVG99, SM91, YY98a, ZZI97]. Significant [BV96]. Signing [BG98a, GM99a, GS98, Ped99, Ros97b, Ros98b, Ros98c, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b]. SIGPLAN [ACM99a], SIGPLAN-SIGACT [ACM99a], Silicon [NFQ99].
Subliminal
[BDI+96, Gru98, KI97, SI93b, SI94, Sch93b, Sch94e, Sim93, Sim94d, Sim94c, Sim96a, Sim97, Des96b, Sim98a, Sim98b, YL97a].

Subliminal-Free [BDI+96].

Sublists [Rus93a].

Submanifolds [Mra95].

Submission [Ada98, CMKK98, BT97, Zun98].

Submissions [SKW+99a, SKW+99b].

Submit [Law98].

Subquadratic [BBP95a, BBP95b].

Subscribers [GC97].

Subscript [Mau91b].

Subsegments [KPR99].

Subset [NS99b, CJL+92].

Substitution [CT99a, HS90, PRAM98, SZZ94b, ZZ96, Ata94, FS93, Fri92b, HT96, O’C95, Zan90].

Substitution-Permutation [CT99a, HT96, O’C95, Zan90].

Subtitle [Mer90b].

success [Blo98c, TY94].

successful [HA94b].

successfully [Al96].

Successor [Ano97-45].

Sufficient [MSN99, Rus93b, Rom90b].

Suggested [Bih91].

Suggestions [Mat96b].

Suit [Buc95b].

suitable [CCZ98, Kob90, MZI98, Miy93a, Nac93, NM94, XL98, YL95a].

Sum [NS99b, CJL+92, JV98a].

Summary [CFG99, DY91d, Daw94, USE94, Mye96].

Summit [CFK+91].

sums [BK98g, CSFS97, Kob91c].

Sun [Bro97, Gar98b, Got99, Law98, Szew97].

SunOS [Ste92, Sun91b].

Super [Sut99].

Supercomputer [DMS95, She92e, Ban97].

Supercomputing [IEEE91].

superhighway [BDC+95].

Superimposing [YY91].

supersafe [PP96].

Superscalar [Cla97].

superscript [Cra92, CF92].

Supersingular [BS91b].

Supervisory [KAP99].

Support [AKP99, BV98a, Bla98, Bla93, DTD99, FR95d, GR99, HKS95, KHB99, LBHM99, LC99, Mon93, Pit96b, SK98a, SK99, SL99, TY99, Ano97],

Ano98f, Cli99, LS98a, TCH+91, Uni94b].

Supporting [PK99, MI90].

Surmounting [CI96], surrounding [GA98].

Surveillance [CKN99, SB97].

Survey [Bri90b, Gar97c, GFB93, Kal93a, Kle90, Kmu98b, Nis96, Par98c, BO92, Ele99, Mea95, She92g, Wad98, Zho94].

Surveys [Ell99].

Susceptibility [AW94].

suspected [LHL95b, LHL95a].

swapping [TN97].

Swedish [LF97].

Swindles [Dob95b].

Switches [Bee99].

Switching [MOM91].

Switzerland [ACM97a, BCB97, IEEE96c].

sword [Den95].

Sydney [KG93, SP90, VPM97].

Sylvester [Por98].

Symbolic [Wat91, AM99, BHK95].

Symbols [Pes97, CS99].

Symmetric [Ada97a, Bin98, BDR+96, BFN98a, FO99b, Gus96, QG90, Roe94, YY98d, YY98b, BDJR97, Cra96, GHS93, HJ99, Hwa93].

Symmetry [BS95d, PS97].

Symposium [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97b, ACM97c, ACM98b, Ano99c, Com96, CMM93, DEQ92, Hei96a, IE93b, IE94d, IE95b, IE96a, IE97f, IE97i, IE98a, IE99a, KK99b, Q98b, Spi95, SLJ93, USE92b, USE93, USE95b, USE96e, USE96g, USE98a, USE98d, USE99a, Wat91, Wol93a, Wol93b, TV92].

synchronised [KI97].

Synchronization [DHSS95, BCCG99].

Synchronized [Yah94, Gen92].

Synchronizing [Mau91a].

Synchronous [AMP99, NT99, DGV94b].

Syndrome [CS96a, ZYR91, ZH90].

synopsis [Wri98a].

Syntax [Kale98, Kale98c, Kale98d, RSA93d, RSA93c, RSA93e, RSA99a].

Synthesis [HL99, Sab94].

synthetic [PGV93b, PGV94].

System [ANS98a, Ano97-33, ADF98, AHMS99, BS99a, BLM99, BKS99, Bal97, BR97a, BM91a, Bie98, Bla94b, BLH99, BC99, Bur94b, CIBM99, CD97, CM99b, Chi92, CC99e, CH94b, CM99d, DDP90, DT98a, DTDJ99, Far92, FK99, FO97, FR95d, Gan96b, Gar97a, GRB99, Gol90a, GPSV98, GS99a, HJTW99, HCD99, HJL99, HE98,
INDI99, JO97, Jia99, KI99, KW99, LMP99, LWY95, LCN99, MGL+98, MKL99, MR95a, Mar98a, Mau97b, MTVZ92, Mon93, NM99, NS98a, Nec96, PR99, PS99f, PK99, Rei92, Rus90, RH99, SY99, SSSW98, Sam98, STSW99, SCTR99, SK66b, SK66c, Sch98a, SSP90, SM99, SKIT99, Tro93, Tun99, Var99b, WHFG92, WABC99, WY98a, WBL99, WABL94, ZK6, ACC99, AN96, BCB99b, Bax97, BMP97a, Bur94a, BD95b, Car94, CB96, Cus95, DSSZ99, Des95, DH96b, FM98b, HN94, HI97, Hwa92a, HC95b, KM99, Mey97b, MM95, Oel97, PS99e, PSW95, Sch99j, SS95c, TCH91, TC91, Ven90, WSFC99, WABL93, ADDS91, AOK99a, Bax97, Be92, Dan95, JD91, RC95, YKY99, ZH98.

Systematic
[BGH91, Zav99, Men95b].

Systematising
[MKL99].

Systeme
[BGH95b].

Systems
[ABLP93, AKP96, AKF94, Ako99, Ano94k, Ano95r, AOK99a, AOK99b, ADK99, AA97, AMP99, BDPSNG95, Bar99, Bas93, BR91, BBD97, BFN98a, CF95, DDJ98a, Dani91b, DFTY97, DY91a, DD99, DB96, ENK99, FJP96, FY95a, FY95b, FYM99, FO99, GL96, GFB93, Gil98, GM90, GMW91, GKO96, GS97, GMV98, HG98H, HI99, HP98b, IE99a, IEE96b, IEE96d, IEE98e, IEE99b, IEE99a, KT96, Koc96b, KAO99, KF92, LQR99, LABW92, Lan99, Lee99b, Mar99, Mas99a, MS95f, MDP94, Muf93, NT99, NAA99, OK98a, Oka98, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PS99a, Pin97, Pit96b, PM99a, PD99b, RB99, RG95, RIO95a, ST94, SN96, STS99b, DY91c, SOOS95, SS99, She92a, SY92, Stu99, Tra99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a].

Systems
[WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFKP98, ZFK+98, AR99, AHdJF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BP95b, CG95, DM99, DIX94, Fri92b, Goo96, GKS97, Gr98, HJJ+97, IEE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Olt96, Ole95, Opp96, PAK98, PA98b, PP99a, PP99, PP99b, PP99c, RO96, SKB97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DV96].

Systolic
[SS98, DF92, PJB90].

Systs
[DS92, PJBM90].

SZ42
[DA98d].

SZK
[GSV99].

T
[TY96, PDG99].

T-Team
[PDG99].

T52
[DA98c].

Table
[KMK99, Has99, Hor95].

Tableaux
[Mas99a].

Tableaux-99
[Mas99a].

Tables
[DRL95, JC98, IPD99].

Tactical
[IKM99].

Tagging
[Lud97].

Tailoring
[CGM96].

Tnken
[GQ97c].

Tale
[Ka97e, RS98].

Talent
[DD98e, DD98f].

Talk
[De97, Lei99b, Wat99, BS91c, Sim91].

Talking
[HH99].

Tamper
[Auc96, BDH98, KK99a, Zhe95b].

tamper-proof
[Zhe95b].

Tamper-Resistant
[Auc96, KK99a].

tamperfree
[Hwa92b, Hwa92c].

Tamperfree
[Hwa92b, Hwa92c].

Tampering
[CL98, CL97b].

Tanaka
[Hwa92a, MS98a].

Tandatangan
[An97-50].

Taos
[WABL93, WABL94].

tapestry
[MB94b].

TAR
[An97-33].

Targeted
[Cap94].

Targets
[Lea99, Way98].

TAS
[Cop94b].

Tasty
[Sch98].

Tate
[FM99].

Taxing
[Gar97c].

Taxonomy
[DB96, GS97, LBMC94].

TC
[MB99b].

TC11
[Kat97].

TC6
[Kat97].

TCF5
[MB97b].

Tcl
[GA98].

TCP
[An96j, Fe93, Fe96].

TCP/IP
[An96j, Fe93, Fe96].

TEA
[KSW97, KS97, NW97, NW95].

Team

TecApro
[GL98].

Technical
[An95e, Bar96b, CF9+91, CYY98, DS97c, Lan98, LM93c, Mos98, USE95a, USE99d, VGP93, SM99, USE96f, USE98c].
Technique [DDNM98, Gue98b, KP93, WD97, BCV97, ONT98, Way95].

Techniques [Int91a, BGML96, BWM98, Bol98a, Bol98b, BLM94, CM97b, CD99, CMYY98, Dam90a, Dam91a, Dav91, DC98c, De 95, Des98a, Des96a, Fun97, Fun98c, GQ95, Hel94, JI99a, LvidLB96, MM99a, MSEN99, Mau99b, PS98e, PS98f, PK99, Pre93b, QV90, QG95, Rue93, SZ93, Car98, Cra96, Hel93, Hel98b, ISO97, Kay95, KG93, Nyb98, OPH+99, Oko96, PS99d, SD97, Ste99b, Way91, Woot90, ZH93, van96].

Technological [UFC94].

Technologies [Dan96, DSS98, Aus96, BGV97a, BK94b, BS95e, Oht96, Uni96a].

Technology [Int91a, Ano96-29, Ano96-30, Ano98t, AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, II96, IEE94b, IEE98d, Li94, Lin93c, NFQ99, Riv98c, USE99c, Ano93a, Ano96u, DS97b, Gil97, ISO97, Ril96, Ros94, Svi97a, VB96, CFK+91, Ers99, Ano99b].

Telecollaboration [Fuc99].

Telecommunications [IEE97e, UNU94, Mac98].

Telemedicine [Ano97-50].

Teleputeraban [Ano97-50].

Telephone [Gar97a, Sha97].

Telephony [Ban94, Gar97b, MB99a, Mar95b, PW98].

teletype [Mac98].

TELNET [SSH93, Al93b, Ano95w, Bor93a, Bor93b, Bor93c].

Temporal [KV99].

Temporary [KRJ98].

Tennessee [IEE94e].

TeraSpell [Ano97-34].

Term [EO95b, CH97, EO95a].

Terminal [Con98, Con99a].

Terminals [Ano99f, ADSW99, Lam99].

Terminology [Pi96a].

Ternary [PKA+98].

Terrorists [Uni98j, Uni98k].

Terschelling [TV94].

Tesla [Ano97-37].

TESS [Dan95].

Test [DS97a, Law98, MOM91, SS91, DLP93, Graxx, Gre90, ZYR90].

Testing [Bas98, Bro94, De 99, MPPS95, Sot98, SB99, SY98, Wal99c, ARK99, Ano97-42, GK99b, Len90, Yan95].


Tetherless [Law98].

Texas [ACM97c, ACM98b, Ano94e, IEE92b, USE98d].

Text [Bar93a, Bar93b, Cai96, CD97, LM98b, PF94, PBGV90, CFK+91, Sab94, SHG98].

Textual [JKVP99].

Teyjus [NM99].

Theft [Gur97].

Their [BK95c, BL96b, BL96a, Con97, GPT91a, GPT91b, JMS96, KL96, Len99b, OO90, SY96a, SG99b, Tra99, VDD99, AA99, BHSV98b, BHSV98a, BY93c, BY93b, Car98, DDB95a, DDB95b, Don98, Eng99, HMP95, KT91b, LN94, LM96, NM96b, SSI98, SI93b, TY92, YY98a, them [Way95].

theme [IEE97k].

Theorem [AA93, FK99, GPS98, HB99, DlDPS96, Sga91a, WWH95].

Theoretic [Buc91a, Cac98, Cle91, MW96a, Mau99a, Mau99b, MO99, Ped91d, PB99a, STP93, Wo98, APDS93, Kos97, Ped91b, Ped91e, Sga91a, Sga93, Shp99b].

theoretical [Sak97, van97a].

Theoretically [AR99, Mau97a].

theories [T+98].

Theory [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, Ber96b, BMP+97b, Car97b, CFK+91, Dam90a, Dam91a, Dav91, De 95, DSB99, Fun97, GQ95, Hel96a, Hel94, IEE94a, IRM93, IZ98, Iz99, KY96a, KR99a, Kob94, LOX99, LBW92, LW91, Mau96b, Mau96a, MDP94, NKC94, NC97, ODP98, PSN95b, PG90, QV90, QC95, Rue93, SSI98, SSI99, Sca91a, Sca93, Shp99b].

thereafter [Sak97, van97a].

These [Ano98q].

They’re [Wri94].

Third [AAB+97, Fra99, MKS99, RS98b, Spi95, Uni95a, ACM91, Gol96d, GS94b, GK95b].

Third-Party [AAB+97].

Thirteenth [IEE94f, USE99b].

thirtieth [ACM98b].

thirty [ACM99b].

thirty-first [ACM99b].
Ano91a, JD91]. **Transactions**
[FL99b, FKMY98, SSG99]. transcendental
[PGCSN96]. **Transcript**
[BD99a, Chr99a, Sas99a].

**Transcript-Irrelevant** [BD99a]. **Transfer**
[Ano97-34, DF99, HHY93, NP99, RS96a, Bea93, BM90, BR96b, DOR99, Jac90a, Jac90b, SF93b]. transferable
[Sak96].

**Transfer**
[Ano97-34, DF99, HHY93, NP99, RS96a, Bea93, BM90, BR96b, DOR99, Jac90a, Jac90b, SF93b].

**Transform**
[Boy99, KMS95a, KMS95b, Kuo90, MS94, Riv97c, WF94, TKS98]. transformability
[MSO96].

**Transformation**
[SZ96, LS98a, Pet91]. transformational
[Zwi98].

**Transformations**
[BDFM99].**Transfusion**
[ADBB99]. **Transient**
[BDHJ98, CH94a, JQBD97]. **Transistors**
[CWM +91]. **Transition**
[Des98a, DR98b].

**Translation**
[CFK +91, OP97, OP98]. translucent
[BR96b].

**Transmission**
[NHB98, PSB97]. transmissions
[Ano97-30]. transmitting
[Cli97, Chi99, UU97b]. **Transparent**
[Bla93, DS97c, Mt97b, SZT96b, ZG96].

**Transport**
[Ano94b, BW98, GBC93, Sar97].

**Transportation**
[BP99, Un98].

**transposition**
[Bar92a, Bar95, GSN94].

**Transputer**
[GN95b]. **trap**
[Yu92].

**trap-door**
[Yu92]. **Trapdoor**
[BM92, BY93a, BHSV98b, BHSV98a, Pai99c, RP97a, WBDY98, And93, Gar96a, Gar97d, Ort95b, Ort95a, Way93b].

**Trappeddoors**
[Gib91, Gor93a, Pat99]. traps
[Sch98e].

**travel**
[Sav97]. **Traveling**
[OMV98, RS99a].

**Travai**
[Un99].

**Travais**
[Des90a].

**Treatise**
[Tur99]. **Treatment**
[BF99b, Mau96a, OQ98, BDJR97, BF99a, Gen99c].

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

**Tree-Based**
[BM96b, BM96c].

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

**Trellis**
[SK94]. **Trellis-based**
[SK94].

**Trends**
[DD98e, DD98f, De 93b, De 98c, Hru98, IE97k, Kan96, LM98a, MB99a, Koo97, Seg92]. **Trial**
[Mye96]. **Trials**
[CY98, P96b, Ano93a]. **Triangular**
[Por98]. **Tribulations**
[CY98]. **tribute**
[Un92]. **Trinity**
[IE97a]. **trip**
[Cur98].

**Triple**
[Ano95p, Ano96c, Ano96-28, Bih96, BK98c, Bih99b, CJM95, HP99a, HP99b, KMS95b, Kum98, Luc98c, CJM96, Mey97b, Per91, vOV91, Joh99, KSW96, RM97, Mey96b].

**Triple-DES**
[Ano95p, Ano96-28, BK98c, Kum98, KSW96, RM97, Mey96b]. triples
[CFS97]. **Trithemius**
[Re98]. **Trojan**
[Sch99f]. True
[Way91]. **Truncated**
[KRW99]. **trunk**
[Un94a, Un94b]. **Trust**
[Ano99j, BPK99, BFK99, LA98, MR98, Rei96, SA95, Sim9a, Sta95a, YKB94, YY96, AHdJF97, BH98, Com97, Chi99a, Chi99b, LN98]. **Trust-Based**
[YKB94]. **Trusted**
[AAB +97, Ano97d, IS91, MKS99, RS98b, SK97c, SS99e, SS99f, CGM97b, HY93a, JMO95a, LWC96, Ped91c, WU92].

**Trustee**
[Jue99]. **Trustworthy**
[Fr93, Pos92]. Trust
[For99a]. **Try**
[Rot97]. **TSP**
[Luc95]. **TTP**
[BDHJ97]. **TTP-based**
[BDHJ97]. **TTTs**
[Lan98]. **Tübeningen**
[PDG99]. tucked
[Ano91b]. **Tunable**
[WF94]. **Tunneling**
[SM98a]. Tuples
[FJRS96, MI90].

**Turbo**
[JJ99a]. **Turbine**
[SS99b]. **Turbo**
[LJ99a]. **Turbulence**
[DIF94]. **Turing**
[CFK +91, Hod97, De98b, Tur99].

**Turnaround**
[Gar97a]. **Tutorial**
[Buc91b].

**Tutoring**
[PD99b]. TV
[DDN98, Fox98, Gar97c, Gar98b]. **Twelf**
[PS99f]. **Twenty**
[Ano95r, Bon99, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, Gol97]. **twenty-eighth**
[ACM96b]. **twenty-fifth**
[ACM95].

**Twenty-Ninth**
[Ano95r, ACM97c]. **twenty-second**
[ACM90]. twenty-seventh
[ACM95]. **twenty-sixth**
[ACM94c]. **Twin**
[Mac98]. Two
[AB96a, Bea92, BMM99a, 182]
[Gar97a, Gar98b]. **Update**
[Ano94j, Ano95a, Ano95b, Ano95u, Ano96-28, Ano97-44, Ano97-45, Ano98r, MGL+98, Mey97b, Pin98, Ros95b, Ros96d, Ros97b, Ste99c, Wie97, Wie98a].

**updated** [Ano97-37]. **upon** [BMP97a, CCH98, LCL95, SPP98].

Upper [Fer98, Al96, O’C94]. **Urgent** [Pra96]. **URL** [Zuk98b]. **USA** [???90, Ano98n, AA97, Auc98, Bri92, Bri93, Cop95d, Des94b, Han99, HF97, IEE97g, IE97e, IEE98c, IE98e, Kali97c, Kob96, KP99b, Kra98, SJ97, Sti93b, Sti94, USE91, USE93, USE94, USE95b, USE95c, USE95a, USE96f, USE99a, USE99b, USE99c, USE99d, Wie99]. **Usability** [WT99, CG05]. **Usage** [End97]. **Use** [ADBB99, BCE+94, Bra90a, CFGS99, Con99b, Gan96a, Gar97a, Gar97b, GC97, GK98, HJL99, Iss90, KR95c, Koh90, Lan99, MG98a, MG98b, Por91, Rud91, SB94, Zuk98a, BDH97, BR97b, Cha94b, Cli99, CG05, Gll97, Joh90, Ri96, Way93c, Zer96a].

**Used** [GS94a, SZ96, Car97c, Car98, Gau97, Kuk99, Sch91b, SX90, van97a]. **USENET** [Bi91]. **Usenix** [USE99d, Com96, Ros95a, Ros96c, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c].

**User** [AKF94, BE90, Bus96, Dra99, Gog99, Gol90a, GN95b, IS99, KKC94a, KKC94b, MP99, RRS97a, RRS97b, SY98, SCT97, Web99, Zim95a, Ano950, DF91b, MC96, Mu92, RSA94, RT93, SJS98, Sta95b]. **User-Centered** [PF99]. **User-Oriented** [AKF94]. **Username** [Le96].

**Username/Password** [Le96]. **Users** [Ano96-31, Hel98a, WK97, Sha97, Sta94a].

**Uses** [Swi97, Ano97x, DK97b, Sch99g].

**Using** [ANS97, ANS98b, Ada97a, AGS97, AHJ97, Ano991, BDPSN97, BCK96e, BBS99a, BFP99, BW98, CIBM99, CK95, CM94d, Des96a, DS97d, ESST99, FVEA99, FW91, FY98b, GM97, GAGC999, GS99a, HNSS99, HRVV99, HJPB97, IR99, JM99, J98c, JQ97, KR94b, KS99a, KA99, KT93, Lon92, LF99, LML98, Low96, LW99, Lud97, MAM95, Mih94, MCD99, Mis97, MFG95, NT99, NHB98, NNEK97, Oh99, OOK91, Ou99, OM93, PSE97, Pin97, PZ98, PJ99, QQ90, RB99, SC95, SK94, Sas99a, SK96a, SK97b, SK97a, SK97c, SD99, SRY99, SR96, Sim94d, SHK99b, Sun91a, SZT98a, TAP90, TA92, TYD99, TOU94, VN94, WKHG97, WCS95, Yam98b, Yam99, YST99a, YY97a, YST99b, AA95, All98, Ano97y, At9a, BSNP96a, BSNP96b, BTD98, BGR95, BJR93, Bih94a, BB95a, BBS98a, BD95a]. **using** [CW91a, CNST98, CC95, CM97b, CHPK98, CB96, Cle96, Dan97, GK99b, GBL94, Gor93b, Hor95, IS97, Jak95, JM96a, KR95a, CK95, Kar96, Kay95, Koc95, KH97, KH98a, LC96b, LC96c, LMBO95, MHPS96, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SSM94, SD97, Su98, SZ98a, SFT98b, Tai97, Ti98, VZ97, VP98, Whi93, WJ93a, Yam98a, Zho94, dr95]. **Utah** [USE95b]. **Utility** [Zol93, Ano97m, Vu95]. **Utilization** [GR98b]. **Utilize** [MSO96].

**utilizing** [SW95a].

**V** [IEE92a]. **V1.0** [Lim99, RSA99a]. **v2.0** [Ano97-33, RSA99b]. **V32bis** [Ano93k].

**Validating** [Gal90]. **Validation** [DDNM98, GS99a, RB99, Ste96, CM96].

**Validity** [GMW91, Kuk99]. **Value** [Ack98, Eve98, Oke97, SPP98, Tay94].

**value-adding** [Eve98]. **Valued** [KW99].

**Values** [GS94a, Tho96].

**Vancover** [Yua92].

**Vancouver** [Yua92].

**Vanstone** [Kie98, NS97c, NS97b, Sha99a]. **Vaporware** [DDJ98e, DDJ98f]. **Variable** [BR99a, BR99b, DW94, GK95b, Sch94b, Su98, TN96a, TN96b, ZPS93].

**Variable-Input-Length** [BR99a, BR99b].

**Variable-Length** [Sch94b, Su98]. **Variance** [Kas96]. **variant** [TC97]. **Variants** [CRR99, MSS98, RS99a, Sha95a].
variation [CCN95]. variations [Zho94].
varieties [Fri92b]. Various [GQW+91].
Vasculation [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, Crè90,
GM95, Ped91d, Sch99i, VBD99, AGY95a,
BD98a, Bur96, FO98, Mao97, MLY93,
Ped91b, Ped91e, Sta96a]. Verification
[Abe98a, AB97, BGR98a, Bo98a, Bo98b,
CDF95, D97a, GFB93, GS99a, HL92,
MM99a, Na97, OMI93, PM98, PV98,
SM95a, SY99, Tou93, WW98b, YY99a,
A907g, BGR98b, Bo97, BS95c, CM96,
Des90a, Dwo91, JC98, JW01, Mea95, Sha97,
YL95a, YM98, ZL99]. Verifications
[GMV98]. Verifier [JMSI96]. Verifiers
[PM98]. Verify [DS97d, Chi99a, Chi99b].
Verifying [LHB96, Sal91, DN95b, Pau98].
Verlag [Hat96]. Verlässliche [BGH95b].
Vermont [IEE96a]. Verschlüsselung
[كرش, كي99b]. Verschlüsselungssysteme
[Wal98]. Verschlüsselungsverfahren
[Ger97].
Version [Ano97-33, Ano97-34, BC93a,
BP98e, DBP97, DB98c, BKP96, FKK96,
Gar97b, Kal98f, Kal98c, Kal98d, Kal98b,
KS98a, RSA93f, Lim99, MT99a, MCM06,
RSA93a, RSA94, DY91c, SS99b, SM98b,
WABC99, CLW98, GM93a, Gih95, Bor93b, Lin96b]. Versus
[MGL+98]. Vertraulichkeit [FT95]. Very
[HH93, MS90, PF94, Yua92, SN94].
Veto [OK96a]. VHDL [Oel97]. via
[BR96b, BCKxx, BM95, BS95d, DS90a,
DN95a, DN93, EPR99b, EPR99a, Fuc99,
HS94, JJ99b, NW98, UFC94]. Vibration
[Nas94, NA95]. VICS [Uni96a]. VICTOR
[OSA91]. Victorian [Abe98b]. Victory
[Mus92]. Video [Ano99f, BF99, DLF97,
DS97c, DSS98, HG97c, KBR97, KH98b,
LT98, MT94, SJ97, SB98, SZT98a,
WK98, WW98a, ZL99, BB90, BCB97,
CPO+98, CHO+98, CKLS96c, DS97b, HG96,
HG97e, HG97d, HG98, HW97, HW98a,
La99, Oht96, QN98b, SH98, SZT98b].
Video-based [WK98, BCB97].
Video-Steganography [MT94]. Vienna
View [CK95, Lan98, MUSM98, MM96a, STP93,
Ste91, ZL99, Ano97l, Pri94, UU97a, Wad93].
Viewpoint [Len96b, Ste91]. Views
[DDJ98e, DDJ98c, DDJ98f, DDJ98a,
DDJ98d, DDJ98b, DDJ98g, DDJ98h,
DD99, Eri97b, TSL99]. VII [IEE99b]. VIL
[AB99a, AB99b]. VIL-MACs
[AB99a, AB99b]. Village [Ber97b]. Vinegar
[KS98d, KPG99]. VINO [DW94]. Virginia
[ACM93a, ACM94a, EIE94a]. Virtual
[DFGH99, GB98, HL99, CCH98, LS98a].
VirtuFlex [Ano97-34]. Virus
[BGG95, Hig97b, Nac97, LFSY94, OY91].
Viruses [Hig97a, Wh90, Coh94]. VIS
[BGH95b]. Visa [Lea99, Gau97]. Visibility
[LE99]. Visible [K196]. Vision
[CKN99, HCD99, PJ99, SW95b, SKIT99,
CS99, RP97b]. Vision-Based [SKIT99].
visit [QJ98a]. Visited [FY95b]. Visual
[ABDS96, B+96b, BD98b, DGD97, Dro96,
HKS97a, HKS97b, JKVP99, K196, NS95,
NP97, PKA+98, P98, PNFK95, Sha98,
St98b, BW97, Ger99b]. Visualisation
[MM99b]. Visualization
[Jan99, PH91, GTGW94]. Visualize
[BW98]. VLDB [Yua92]. VLIW [Cla97].
VLSI
[CKM99, Mas91, Pai96, Pos98, VAD95, Zim99].
VoD [GMD98]. Voice [CM97b, MB99a,
Sha97, Cha94b, Int91b, PW98]. vol
[Ano97-48]. volume [Kat97]. Voting
[Boy90, JT97a, MV93, NR94, SK94, SK95,


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, BHHR99, BK98f, DI99, Dob98, HILL99, HYLT99, 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, Haw98a, Kn95, SSI97a, SSI97b, YL97b]. Weakened [AB99a, AB99b]. Weakly [MP91].

Weakness [Cop99, KSW99a, Kie98]. Weaknesses [BMS94, DYT91e, Kel99, KP93, Lan96, PA98b, RK98a, Rij99, S296, DGV94b, She96b, XZ97]. weapon [Ano97]. weapons [Mei98]. weather [Ano95j].

Web [Ano97-33, MR98, OW95, SA95, Sta95a, Ver98b, Ale98, An97d, Ano98k, Bal99, BMNL99, Cha99b, Dav95, DKK98, FL96, GGM997, GO96c, Law98, She96b, Ude98, WCSS95, You96, ZL99].

Web-Based [ZL99, Ano98k]. Web-enabled [Cha99b]. WebTime [Ano97-34]. Weighing
REFERENCES

X [Ano95x, Bel92, BALS99, KSW97a, KSW97b, Smi98b, Yu94a, Yu94b, PvO95].
X9F1 [Ano95p, SS97]. XC6200-series [CJR98a, CJR98b]. XCS6200 [CJR98a, CJR98b].
XCs6200-series [CJR98a, CJR98b]. XCS6200 [CJR98a, CJR98b]. xDSL [MB99a]. Xiao [JW01]. Xidian [XtTmW94]. XIII [USE99b].
XTEA [WN98a]. Xu [Ng99].

Y2K
[Ano98t, DDJ98b, Eri97b, Law98, MGL+98]. [Yaksha] [Gan96b]. Yarrow-160 [KSF97].
Year [Sch95a, Sil09, Roe95]. Years [Bon99, Yin97, BC96b, CWM+91, Den90, Gol97c, Mar96, Mey97a].
y [IPNdbbp99]. Yield [GMW91].
Yokohama [Iz98]. York [IEE99a, USE95c].
Yu [BY92]. YY [Nat92b].

Z [Mau91b]. Z80180 [Kal93b]. Zero [BG90, BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOVY93, NMV99, OQ90, RS91, SI93a, BOGG+90, BBP95a, BBP95b, DF93, DF94, DF91b, Sah99].
Zero-Knowledge [BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOVY93, NMV99, OQ90, RS91, SI93a, BOGG+90, BBP95a, BBP95b, DF93, DF94, DF91b].
zeta [Kob91c]. zeta-polynomials [Kob91c].
Zhang [JW01, Ng99, GP99, LH98]. Zhu [Ng99]. Zimmerman [Ros95a]. Zimmermann [Ros97a, Ros96c].
Zinc [RK93]. Ziv [Mun91a, Mun91b]. ZnO* [Boy97]. Zur [KK97]. Züri [ACM97].

References

Anonymous:1990:IWH

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

Anonymous:1997:ACC


ANSI:1988:FIE


Anshel:1993:PMT

Iris Lee Anshel and Michael Anshel. From the post-Markov theorem through decision problems to public-key cryptography. American Mathematical Monthly, 100(9):835-844, November 1993. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

ANSI:1995:ANS


Abadi:1999:STS


Anderson:1998:NFA


Ateniese:1996:CBV


Aiello:1998:SAC


Abe:1998:UVM


Abeles:1998:SVP


Abe:1999:RDM

[M. Abe. Robust distributed multiplication without interaction. In Wiener [Wie99], pages 130–147.
REFERENCES

Anderson:1998:SPA

[ABK98a]

Anderson:1998:SNBa

[ABK98b]

Anderson:1998:SNBb

[ABK98c]

Abadi:1993:ADS

[ABKL93]

Abadi:1993:CAC

[ABLP93]

Abraham:1997:SEE

[Abr97]
Susan Abraham. Software encryption export policy analysis. Thesis (B.A.), California Polytechnic State University, San
REFERENCES


[ACGS88] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA and Rabin functions: Certain parts are as hard as


ACM, editor. *Proceedings of the twentieth annual ACM
REFERENCES


ACM:1989:PEA


ACM:1989:PSN


ACM:1989:PTF


ACM:1989:PTF


ACM:1991:PTT


ACM:1993:FAC


ACM:1993:PTF

REFERENCES


REFERENCES


ACM:1999:SPCd


Ahlswede:1981:BCG


Ajtai:1997:PKC


Ajtai:1999:PKC


Adamek:1991:FCT


Adam:1992:DSC


Adams:1992:IAB


A. R. Appas, A. M. Darwish, A. El-Dessouki, and S. I. Shaheen. Speeding the vector search algorithm for regional color channel features based indexing and
REFERENCES


Augot:1998:DSM


Alagappan:1990:PDA


Adleman:1979:SAD


Adleman:1983:BGK


Adleman:1987:PRD


Asokan:1999:APT


Alves-Foss:1995:ACS

Apostolico:1984:PMM


Apostolico:1985:CAW


Anderson:1995:SFS


REFERENCES

Abadi:1998:BMcB


Aura:1999:SLM


Agarwal:1992:RSO


Atkins:1995:MWS


Agnew:1987:RSC


Agnew:1988:RSC


Afanassiev:1997:FMA

Valentine Afanassiev, Christian Gehrmann, and Ben Smeets. Fast message authentication using efficient polynomial evalua-
REFERENCES

103


Alon:1995:DRV


Alon:1995:EDR


Aiello:1999:SDI


Aiello:1998:NCS


Alberda:1997:UFS

[AIR83] A. G. Akritas, S. S. Iyengar,


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Anton:1994:GDS [AMP94]

Arnal:1999:SAP [AMP99]

Anderson:1996:NPE [AMS96]

Agnew:1993:DFE [AMV93]

Andrew:1986:TCB [AN86]

Abadi:1994:PEP [AN94]
version of this paper has appeared in the Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy.

Anderson:1995:RPP

Abadi:1996:PEP

Andree:1952:C

Andelman:1979:MLE

Andrew:1986:CSI

Anderson:1993:PRT
REFERENCES

Anderson:1994:WCF

Anderson:1996:CEM

Anderson:1996:SLS

Anderson:1996:IHF

Anderson:1998:EWF

Anonymous:1922:PUS
Anonymous:1939:ITM
Anonymous. Introductory talk to members of the William and Mary College cryptanalysis class. Technical report, William and Mary College, Williamsburg, VA, USA, 1939. 7 pp.

Anonymous:1960:CNH

Anonymous:1976:CCA

Anonymous:1978:CSD

Anonymous:1978:NPAd

Anonymous:1978:ODA

Anonymous:1979:SSA

Anonymous:1980:ACS
Anonymous. An assessment of civil sector uses of digital data encryption. Technical report, Department of Engineering and Public Policy, Department of Social Sciences and School of Urban and Public Af-
REFERENCES


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


Anonymous. The puzzle palace: a report on NSA, America’s most
REFERENCES


Anonymous:1984:ESC


Anonymous:1985:BM


Anonymous:1985:DEA


Anonymous:1985:MTT


Anonymous:1986:CPC


Anonymous:1986:RE

REFERENCES

Anonymous:1987:EVE


Anonymous:1987:HSE


Anonymous:1987:MAU


Anonymous:1987:TWP


Anonymous:1988:BRCb


Anonymous:1988:CCJb


Anonymous:1988:CCJc

REFERENCES


REFERENCES

Anonymous:1988:RIA

Anonymous:1989:SZS

Anonymous:1990:SEL

Anonymous:1991:E

Anonymous:1991:FFL

Anonymous:1991:ESS

Anonymous:1991:AUd

Anonymous:1992:AUd

Anonymous:1992:DES

Anonymous:1992:DDS
Anonymous. Double data security. *Datamation*, 38(??):21–??, November 15,
REFERENCES

1992. CODEN DTMNAT. ISSN 0011-6963.


REFERENCES

Anonymous:1993:WND

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

Anonymous:1993:ENC


Anonymous:1994:HSG


Anonymous:1994:ICI


Anonymous:1994:ERB


Anonymous:1994:KES


Anonymous:1994:LSA

Anonymous:1994:L1


Anonymous:1994:PRP


Anonymous:1994:Uc


Anonymous:1994:WAS


Anonymous:1995:AUC


Anonymous:1995:AUM


Anonymous:1995:EES

[Ano95c] Anonymous. An E-mail encryption standard should be in place by April, providing for the incorporation of Privacy Enhanced Mail into the MIME standard. *Open Systems Today*, 168:26–??, February 1995. ISSN 1061-0839.

Anonymous:1995:ARLa


Anonymous:1995:ARLb

REFERENCES

Anonymous:1995:ARD


Anonymous:1995:DAS


Anonymous:1995:ENa


Anonymous:1995:ENb


Anonymous:1995:EEW


Anonymous:1995:ENE


Anonymous:1995:FSH


Anonymous:1995:FRE


Anonymous:1995:HPE

REFERENCES

Anonymous:1995:IUA

Anonymous:1995:NIX

Anonymous:1995:OIN

Anonymous:1995:PTN

Anonymous:1995:RLM

Anonymous:1995:SDE

Anonymous:1995:SUE

Anonymous:1995:SEE
Anonymous:1995:TEV


Anonymous:1995:XAV


Anonymous:1996:NIS


Anonymous:1996:RF


Anonymous:1996:ADX


Anonymous:1996:BCU


Anonymous:1996:CED


Anonymous:1996:CID

Anonymous. Correction to “Improved Digital Signature Algorithm”. *IEEE
REFERENCES


Anonymous:1996:CCC


Anonymous:1996:CSIa


Anonymous:1996:CPD


Anonymous:1996:CPT


Anonymous:1996:ENa


Anonymous:1996:ENb


Anonymous:1996:EME


Anonymous:1996:EBS

Anonymous. Encryption battle sees possible breakthrough. Network Security,
REFERENCES


Anonymous:1996:ERK


Anonymous:1996:ERM


Anonymous:1996:EKE


Anonymous:1996:ECC


Anonymous:1996:FDC


Anonymous:1996:GPT


Anonymous:1996:HET

REFERENCES

Anonymous: 1996: LAW

Anonymous: 1996: PKE

Anonymous: 1996: SAB

Anonymous: 1996: SAO

Anonymous: 1996: SCG

Anonymous: 1996: SAS

Anonymous: 1996: SUS

Anonymous: 1996: TBAa
[Ano96-29] Anonymous. Technology and business: Artificial blood starts circulat-
REFERENCES

Anonymous:1996:TBSa

Anonymous:1996:UDE

Anonymous:1996:RDSa

Anonymous:1997:AES

Anonymous:1997:AUC

Anonymous:1997:AWS

Anonymous:1997:AIR
Anonymous. Announcements: In this issue: The
REFERENCES


**Anonymous:1997:ARDa**


**Anonymous:1997:ARDb**


**Anonymous:1997:ADF**


**Anonymous:1997:BUF**


**Anonymous:1997:CKG**


**Anonymous:1997:CVC**

Anonymous: 1997: DEU


Anonymous: 1997: DHE


Anonymous: 1997: DNH


Anonymous: 1997: EAS


Anonymous: 1997: ENa


Anonymous: 1997: ENb


Anonymous: 1997: ENc


Anonymous: 1997: EAJ

Anonymous:1997:ECR


Anonymous:1997:EKB


Anonymous:1997:EW


Anonymous:1997:FSU


Anonymous:1997:FCR


Anonymous:1997:HEW


Anonymous:1997:HDR


Anonymous:1997:INI

Anonymous, editor. *Issues for networked interpersonal communicators: Colloquium — May 1997, London*, number 139 in COL-
REFERENCES

LOQUIUM DIGEST - IEE
LCCN ????

Anonymous:1997:MNL


Anonymous:1997:MLE


Anonymous:1997:MEP


Anonymous:1997:NPP


Anonymous:1997:NPA

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

Anonymous:1997:NPNb

Anonymous. New products: NetTracker 3.0; ScriptEase: Integration SDK; JDesignerPro 2.1; VirtuFlex 2.0; PGP Version 5.0 for Personal Privacy; TeraSpell 97; FileDrive File Transfer Server; journyx WebTime. Linux Journal, 43:??, November 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).
Anonymous:1997:PEH


Anonymous:1997:RAS


Anonymous:1997:RCU


Anonymous:1997:RAJ


Anonymous:1997:SFR


Anonymous:1997:RBE


Anonymous:1997:SAP

[Ano97-41] Anonymous. SecurID authentication protects corporate information. *Net-
Anonymous:1997:SUE


Anonymous:1997:SUR


Anonymous:1997:SEA


Anonymous:1997:SSA


Anonymous:1997:CBP


Anonymous:1997:TER


Anonymous:1997:UUS

REFERENCES


Anonymous:1998:ABF

Anonymous:1998:ARD

Anonymous:1998:CSIb

Anonymous:1998:CPP
Anonymous:1998:CASb


Anonymous:1998:ICS


Anonymous:1998:CDR


Anonymous:1998:CSCb


Anonymous:1998:EN


Anonymous:1998:EWB


Anonymous:1998:Ea

REFERENCES

Anonymous:1998:LEE


Anonymous:1998:PCA


Anonymous:1998:SEF


Anonymous:1998:SIC

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

Anonymous:1998:SAP


Anonymous:1998:TBF

Anonymous. Technology and business: a fast Y2K bug fix. confidentiality without encryption...

Anonymous:1999:UGT

[Ano98u]

Anonymous:1999:UFR

[Ano98v]

Anonymous:1999:RDS

[Ano99a]

Anonymous:1999:AWS


Anonymous:1999:CCI


Anonymous:1999:CEV


Anonymous:1999:DSC


Anonymous:1999:DSV

Anonymous. DREO secure video conferencing and
high speed data encryption tests for Inmarsat-B satellite terminals. Technical memorandum AD-a371 256, Defence Research Establishment Ottawa, Ottawa, ON, Canada, 1999. 51 pp. [Ano99j]

Anonymous:1999:EDB


Anonymous:1999:EPFa


Anonymous:1999:EGC


Anonymous:1999:KNT


Anonymous:1999:L

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

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

Anonymous:1999:ULE


Anonymous:1999:WDE


ANSI:1997:AXP


Anderson:1998:SFS


ANSI:1998:AXD


Anderson:1996:CCA

M. S. Anderson and M. A. Ozols. Covert channel analysis for stubs. In Anderson [And96c], pages 95–113. CODEN
Abbott:1993:INT


Abreu:1994:DAI


Anderson:1998:LS


Andrasiu:1993:LTP


Aruliah:1985:PIE


Allen:1997:PSA

Aumann:1998:AES

Aumann:1999:ITS

Arazi:1993:AEA

Arensberg:1921:CD

Arensberg:1922:CSP

Adamson:1995:JSR
Abdulla:1999:OMS


Aiello:1999:HPN


Aiello:1999:HSP


Alpern:1983:KEU


Atici:1996:UHM

REFERENCES


REFERENCES


Akl:1983:CSP


Ateniese:1999:SOI


Atallah:1999:ATC


Atanasiu:1993:AEU


Al-Tawil:1998:NAP


Atkins:1993:CKE


Atkinson:1995:RIA

REFERENCES

Atkinson:1995:RIE


Atkinson:1997:TMS


ATT:1986:AUS


Aucsmith:1998:SIW


Aur96


AAGD:1996:RPR

<table>
<thead>
<tr>
<th>REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aparicio:1999:ITD</strong></td>
</tr>
<tr>
<td><strong>Alabbadi:1994:SDS</strong></td>
</tr>
<tr>
<td><strong>Alabbadi:1995:DSS</strong></td>
</tr>
<tr>
<td><strong>Avolio:1998:PCP</strong></td>
</tr>
<tr>
<td><strong>Angel:1999:JQH</strong></td>
</tr>
<tr>
<td><strong>Anderson:1996:NC</strong></td>
</tr>
</tbody>
</table>
Aspray:1988:RCD


AufderHeide:1999:PGP


Ayoub:1968:EKR


Ayoub:1968:EEK

F. Ayoub. Erratum: En-


REFERENCES

149


REFERENCES


Bamforth:1997:JSS
R. Bamforth. Java — from smartcard to supercomputer. In Anonymous [Ano97-28], pages 1–??. ISSN 0963-3308. LCCN ????

Burrows:1989:LAB

Burrows:1989:LAa

Burrows:1990:LA

Banisar:1993:BCE

Banisar:1994:CPS

Bao:1994:IRL

Barker:1961:CSC

Bartek:1974:EDS
Douglas J. Bartek. Encryption for data security. Hor-
eywell Computer Journal, 8 (2):86–89, ???? 1974. CO-
DEN HNCJA3. ISSN 0046-7847.

Wayne G. Barker. Crypt-
analysis of the simple sub-
stitution cipher with word
divisions using non-pattern
word lists. A Cryptographic
series. Aegean Park Press,
Laguna Hills, CA, USA,
1975. ISBN ???? 20 + 108
pp. LCCN Z103 .B3.

Wayne G. Barker. Crypt-
analysis of the Hagelin
cryptograph, volume 17
of A Cryptographic series.
Aegean Park Press, Laguna
Hills, CA, USA, 1977. ISBN
0-89412-022-0. xi + 223 pp.
LCCN ????

Wayne G. Barker. Crypt-
analysis of an enciphered
code problem: where an
“additive” method of en-
cipherment has been used.
A Cryptographic series.
Aegean Park Press, Laguna
Hills, CA, USA, 1979. ISBN
LCCN Z103 .B333.


Wayne G. Barker. Crypt-
analysis of shift-register
generated stream cipher sys-
tems, volume 39 of A CRYPTO-
tographic series. Aegean
Park Press, Laguna Hills,
CA, USA, 1984. ISBN 0-
89412-062-X. ix + 247 pp.
LCCN Z 104 B37 1984.

Paul Barrett. Implement-
ing the Rivest, Shamir
and Adleman public-key
encryption algorithm on a
standard digital signal
processor. In Odlyzko
[Odl87b], pages 311–323.
CODEN LNCSD9. ISBN

[Barker:1991:IAD]

[Barker:1992:CSC]

[Barker:1992:DPP]

[Barlow:1993:EF]


[Barlow:1994:NS]
John Perry Barlow. Notable Speeches of the Information Age. O’Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and
REFERENCES


[Bas93] Richard Baskerville. Information systems security design methods: Implications

### Bastian:1995:CCE


### Bassham:1998:ETA

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.

### Baudouin:1939:ECF


### Baudouin:1946:ECF


### Bauer:1982:KVM


### Bauer:1997:DSM


### Baxter:1997:SBE

Mark Darrell Baxter. Selecting the best encryption

**Bowers:1960:PC**


**Bowers:1967:PC**


**Blakley:1979:RSA**


**Bennett:1985:UQC**


**Bennett:1989:EQC**

REFERENCES

0163-5700 (print), 1943-5827 (electronic).


REFERENCES

Barni:1998:MPI


Four volumes.

Blakley:1993:TSD


Blakley:1993:TPD


Blakley:1993:TPD

Bennett:1995:GPA


Barni:1997:RWS


Blakley:1993:TPD

Barni:1998:CPD


Barni:1998:DDS

Mauro Barni, Franco Bartolini, Vito Cappellini, and Alessandro Piva. A DCT-domain system for
REFERENCES


Biguen:1997:ECM


Biguen:1997:ECM


Biham:1999:IOS


Bennett:1992:QC


Bauer:1983:KDP


Biham:1998:CM

[BBDF97] E. Biham, A. Biryukov, Niels Ferguson, Lars R. Knudsen, Bruce Schneier, and Adi Shamir. Crypt-
REFERENCES


REFERENCES

Blakley:1985:ACP


Bender:1990:IEC


Beimel:1993:UIS


Bos:1993:PUS


Beguin:1995:GSC

REFERENCES

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


W. C. Barker, P. Cochrane, and M. Branstad. Embedding cryptography into


REFERENCES

Four volumes.


REFERENCES

Beth:1985:ACP


Beth:1998:Eb


Bellare:1996:HC


Bellare:1996:PFRa


Bellare:1996:PFRb


Bellare:1996:KHF

ny.com/link/service/series/0558/papers/1109/11090001.pdf; http://www.research.ibm.com/security/. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Bellare:1996:MAU


Bellare:1998:MAD


Bellare:19xx:KMM


Bromley:1983:RFM

REFERENCES


Bergadano:1998:HDC

Berbecel:1997:MTW

Birnbaum:1986:VPS

Bishop:1997:TNI

Borucki:1974:MNN

Brickell:1990:CIS
Burmester:1991:ALN


Bauspiess:1992:RCH


Brandt:1993:GPP


Bloomer:1994:FFS


Bloomer:1995:PLC


Bloomer:1995:SEC


Blundo:1997:LBR

REFERENCES

[Bao:1998:SSS]

[BD98a]

[BD99a]

[B Boneh:1999:CRP]

[Blundo:1998:VCS]

[BDB92]

[BDC+95]
Gareth Branwyn, Luke Duncan, Sean Carton, Donald Rose, Tom Lichty, Shannon R. Turlington, and Jan Weingarten. *Internet...*
REFERENCES

roadside attractions: sites, sounds and scenes along the information superhighway. [BDF98]

Blundo:1994:MSS

Boneh:1998:ARG

BenAyed:1999:MFP

Blundo:1999:PSS

Bondalapati:1999:DDE
REFERENCES

[Bao:1998:MFA]

[Blundo:1999:FL]

[Blundo:1996:IRS]

[Blundo:1996:IRS]

[Bao:1997:DAT]

[Blundo:1996:IRS]

[Bao:1998:BPK]
REFERENCES

Blundo:1993:PSK

Burmester:1996:PRS

Bellare:1997:CST

Boneh:1997:ICC

Benaloh:1994:OWA

Bosselaers:1997:RCH
Antoon Bosselaers, Hans Dogbbertin, and Bart Pre-

**Bellare:1998:RAN**


**Baraani-Dastjerdi:1995:CMO**


**Baraani-Dastjerdi:1997:UCH**


**Blaze:1996:MKL**


**Burmester:1998:EKE**

REFERENCES

[174]

Blundo:1993:GDS


Blundo:1993:ESM


Blundo:1998:SSS


Bright:1979:QRN


Barrett:1990:SDU


Beardsley:1972:YCI


Beauquier:1992:TDP

J. Beauquier. Two distributed problems involving
REFERENCES


Ernest L. Bell. An initial view of Ultra as an American weapon. T S U Press, Keene, NH, USA, 1977. iii
REFERENCES

Bellcore:1992:GRX


Bellovin:1998:CI


Bellare:1999:POP


Bennett:1980:UWN


Bennett:1988:AEA


Bennett:1989:UMS


Benario:1998:TSU


Benedens:1999:GBW

REFERENCES

[178]


REFERENCES

Berghel:1997:DVW


Berson:1997:FMP


Berg:1998:JQHd


Bergmann:2009:DKR


Beth:1983:CPW


Betts:1988:ESG

com/science/article/pii/0167404888905470.


REFERENCES


REFERENCES

Blum:1994:CPB

Blum:1988:NIZ

Blaze:1998:FTR

Blaze:1998:PSS

Boyd:1999:EEC

Beth:1992:PCS
REFERENCES


Beth:1992:PKC


Busch:1999:DWC


REFERENCES

Bellare:1994:ICC


Bellare:1995:ICA


Bird:1991:SDT


Bird:1995:KFL


Bruggermann:1995:VIS


Branstad:1977:RWC

[BGK77] Dennis K. Branstad, Jason Gait, and Stuart Katzke, editors. Report of the

References


[BGR95] Mihir Bellare, Roch Guérin, and Phillip Rogaway. XOR MACs: New methods for message authentication using finite pseudorandom functions. In Coppersmith [Cop95d], pages 15–35. CODEN LNCS93. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-
REFERENCES


Bellare:1998:BVA


Bellare:1998:FBV


Bierbrauer:1994:BRF


Blundo:1995:DRR


Bierbrauer:1996:OAR

Jürgen Bierbrauer, K. Gopalakrishnan, and D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and lin-

**Berkovits:1998:AMA**


**Benantar:1996:ACS**


**Bosselaers:1993:CWP**


**Bosselaers:1996:FHP**


**Biget:1997:HSC**

Patrick Biget, Patrick George, and Jean-Jacques Vandewalle. How smart cards can benefit from object-oriented technolo-
REFERENCES


**Boselaers:1997:SDP**


**Baker:1998:LTC**


**Beygelzimer:1999:OWF**


**Bhimani:1996:SCI**


**Boeleoni:1999:SBM**

L. Boeleoni, R. Hao, K. Jun,

**Black:1999:UFS**


**Bubeck:1995:DSC**


**Bayer:1993:IER**


**Bellare:1998:MOT**


**Bellare:1998:MOT**

REFERENCES


REFERENCES


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


[Bih97b] E. Biham. A fast new DES implementation in software. Lecture Notes in Computer
Biham:1997:FSE


Biham:1998:CMM


Biham:1998:IOS


Biham:1999:CM


Biham:1999:CTM

Biham:1999:NCA


Birrell:1985:SCU


Biryukov:1995:CID


Birman:1998:ACH


Biryukov:1999:MC


Bishop:1988:AFDa


Bishop:1988:AFDb


Bishop:1988:AFDc


Bishop:COMPSYS-1-3-221

[Bis88d] Matt Bishop. An application of a fast data encryp-
REFERENCES


REFERENCES

0558/papers/1233/12330280.pdf.


REFERENCES


Buhler:1998:LBR [BKR94]


Buchholz:1998:OGO [BKK98]


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, 739:36–??, 1993. CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1994:SCB


Borst:1997:TAR

J. Borst, L. R. Knudsen, and V. Rijmen. Two attacks on reduced IDEA. Lecture Notes in Computer Science, 1233:1–??, 1997. CODEN LNCS09. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1998:LBI

M. Bellare, T. Krovetz, and


Dan Boneh and Richard J. Lipton. Algorithms for


Blaze:1993:TMS

Blaze:1994:IRO

Blaze:1994:KME

Blaze:1996:HBE

Blaze:1996:HEL

Blaze:1996:OKE

Blair:1998:SEP


REFERENCES


REFERENCES

Blum:1983:HES


Blum:1984:IUC


Blundo:1995:NDT


Blundon:1997:BCE


Bayer:1975:EST


Bayer:1976:EST


Blum:1982:HGC

[BM82] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random

**Blum:1984:HGC**


**Boyer:1984:PCR**


**Blakley:1985:SRS**


**Beale:1989:EUR**


**Bellare:1990:NIO**

REFERENCES


REFERENCES

org/stamp/stamp.jsp?tp=&arnumber=262121.


REFERENCES


Blackburn:19xx:NPP

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

Bento:1995:RCI


Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD

Blackburn:1997:CNP


Blackburn:1997:CTA

REFERENCES


**Biedl:1998:GMF**


**Blackburn:1994:WPK**


**Bubak:1999:DHP**


**Blundo:1996:TOB**

REFERENCES

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


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.


REFERENCES


REFERENCES


Ben-Or:1983:CSS


Ben-Or:1988:MIP


Ben-Or:1988:CTN


Boland:1995:WDI


Bolignano:1997:TMC


Bolignano:1998:IPB

[D. Bolignano. Integrating proof-based and model-checking techniques for the formal verification of cryptographic protocols. Lecture Notes in Computer Science, 1427:77–??, 1998. CODEN LNSD9. ISSN 0302-9743

Bolignano:1998:IPB

D. Bolignano. Integrating proof-based and model-checking techniques for the formal verification of cryptographic protocols. Lecture Notes in Computer Science, 1427:77–??, 1998. CODEN LNSD9. ISSN 0302-9743

Ben-Or:1988:MIP

REFERENCES


REFERENCES


W. Bosma. *Primality Proving with Cyclotomy*. Doc-
Bovelaers:19xx:EFH


Bounas:1985:DDS


Boucher:1994:GPA


Bovelander:1998:SCS


Bovenlander:1998:SCS


Bowers:1959:DSP


Bowers:1960:BC

REFERENCES


Boyd:1992:FFA


Boyd:1995:CCC


Boyd:1995:CCI


Boyd:1997:DSP


Boyer:1998:DSM


Boyko:1999:SPO


Beker:1982:CSP

REFERENCES


[BP97b] James F. Brinkley and Jeffrey S. Prothero. Slisp: a

**Buchmann:1997:OWF**


**Buchmann:1997:OWF**

**Bailey:1998:OEF**


**Barnett:1998:AOD**


**Barnett:1998:FML**


**Bassia:1998:RAW**


**Bella:1998:KVI**


REFERENCES

Brown:1998:LA

Borst:1999:LCR

Beguin:1995:FSR

Beguin:1995:FSA

Blakley:1988:CBA

Beutelspacher:1991:EFS


REFERENCES

Bellare:1996:ESD


Bellare:1997:FAK


Bellare:1999:CVC


Bellare:1999:CVI


Branstad:1975:DGI


Branstad:1975:EPC

REFERENCES


[Brand] Russell L. Brand. Problems with the normal use
REFERENCES


Brassard:1994:CCQ

Bray:1994:UA

Brackin:1994:DCP

Brassard:1995:CCB

Brands:1995:RBS

Brackin:1995:DCP

Brasses:1995:IDR


REFERENCES

sored by the International Association for Cryptologic Research.


REFERENCES


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB


Brundrett:1998:KAW


Bentley:1999:SOE


Bryan:1967:CA


Brillhart:1967:SFR


Branstad:1982:ISS

Brickell:1983:SRK

Benois:1986:CSE

Biham:1990:DCD

Brown:1990:DPT

Beth:1991:NSE


REFERENCES


REFERENCES

//www.almaden.ibm.com/journal/rd39-1.html#twelve


[Blake:1999:ECC] Ian F. Blake, G. Seroussi, and Nigel P. Smart. Elliptic

Bateman:1989:NMC

P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr. The new Mersenne conjecture. American Mathematical Monthly, 96(2):125–128, February 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). See letter to the editor [Mul89b]. The authors state: New Mersenne Conjecture. If two of the following statements about an odd positive integer \( p \) are true, then the third one is also true. (a) \( p = 2^k + 1 \) or \( p = 4^k + 3 \). (b) \( M_p = 2^p - 1 \) is prime. (c) \( (2^p + 1)/3 \) is prime.

Benaloh:1994:RFS


Boney:1996:DWA


BT:1997:BEC


Barmawi:1998:AEK

Press order number PR07436
IEEE Order Plan catalog number 96TB100057.


REFERENCES


[Bur94a] M. Burmester. Cryptanalysis of the Chang-Wu-Chen

CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Burmester:1994:CCW**


**Burmester:1996:HSS**


**Burke:1998:IHC**


**Burke:1998:LER**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Author(s)</th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
</table>
REFERENCES


**Beller:1993:BDK**


**Beller:1993:BDH**


**CBEMA:1981:ANS**


**CBEMA:1983:ANSb**


**CBEMA:1983:ANSa**


**Cachin:1995:LSS**

C. Cachin. On-line secret


REFERENCES


C. Carlet. Partially-bent functions. *Lecture Notes in Computer Science*, 740:


Casson:1976:SAD


Caswell:1995:EDA


Chren:1996:RDU


Clark:1981:ECC


Chen:1995:SIB


Canteaut:1998:NAF


Cai:1999:LBPa

REFERENCES

CODEN INFCEC. ISSN 0890-5401 (print), 1090-2651 (electronic).


[Coppersmith:1985:AF] D. Coppersmith and J. H. Davenport. An applica-
REFERENCES

Chuang:1991:MER

Cramer:1995:SSS

Cramer:1996:NGS

Chapman:1997:HHS

Clark:1998:OHA

Cramer:1998:ZPF
R. Cramer and I. Damgaard. Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for...
REFERENCES


REFERENCES


[CDNO97] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable encryption. In Kaliski [Kal97c], pages 90–104. CODEN LNCS9D.


 chops
REFERENCES


Certicom:1997:EC


Christoffersson:1988:CUH


REFERENCES

[Coe:1995:DDC]

[CF95]

[CFGS99]

[CFG96]

[Callas:1999:FUI]

[CF99]

[CFK+91]

[Castelfranchi:1999:BMA]
REFERENCES


Chor:1994:TT


Coppersmith:1996:LRR


Coppersmith:1996:LER


Canetti:1997:CES


Cramer:1996:MAS

REFERENCES


Coppersmith:1975:GCA


Chor:1985:RRL

Benny Chor and Oded Goldreich. RSA/Rabin least significant bits are $1/2 + \frac{1}{\log N}$ secure (extended abstract). In Blakley and Chaum [BC85], pages 303–313. CODEN LNCS9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic).

Catalano:1998:NES

Canetti:1999:ETP


Canetti:1999:AST


Cranor:2005:SUD

REFERENCES


[CH94a] Ran Canetti and Amir Herzberg. Maintaining security in the presence of transient faults. In Desmedt
REFERENCES


Clark:1994:BSP


CH97a

[CH97a]

Chang:1997:SAG


Chen:1998:PFR

REFERENCES

Corcoran:1999:SCB

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

Cordon:1999:AMD


Chaum:1979:UEM

David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Thesis (M.S. in Computer Science), University of California, Berkeley, Berkeley, CA, USA, June 1979.

Chaum:1981:UEM

CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL


Chandler:1983:IMC


Chaum:1983:BSU


Chaum:1985:HKS

REFERENCES

Chaum:1985:NSC


Chaum:1985:SIT


Chang:1986:DKL


Chapman:1986:NFS


Chaum:1990:SDA

David Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. Lec-
REFERENCES

ture Notes in Computer Science, 435:591–??, 1990. CO- 
DEN LNCSD9. ISSN 0302- 
9743 (print), 1611-3349 
(electronic). URL http: [Cha93] 
//link.springer-ny.com/ 
l ink/service/series/0558/ 
bibs/0435/04350591.htm; 
http://link.springer- 
ny.com/link/service/series/ 
0558/papers/0435/04350591. 
pdf.

[Cha91] David Chaum, editor. [Cha94a] 
Smart card 2000: selected 
papers from the Second 
International Smart Card 
2000 Conference, Amster-
 dam, The Netherlands, 4– 
6 October 1989. North-
Holland, Amsterdam, The 
0-444-89266-4. LCCN 

[Cha92a] D. Chaum. Achieving 
electronic privacy. Sci-
cientific American [Interna-
tional Edition], 267(2):76– 
81, August 1992. CODEN 
SCAMAC. ISSN 0036-8733 
(print), 1946-7087 (elec-
tronic).

[Cha92b] David Chaum. Achieving 
electronic privacy. Sci-
cientific American, 267(2):96– 
?? (Intl. ed. 76–81), Au-
gust 1992. CODEN SCAM-
MAC. ISSN 0036-8733

[Cha93] D. Chaum. Numbers can 
be a better form of cash 
than paper. Lecture Notes 
in Computer Science, 741: 
174–178, 1993. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

[Cha94a] B. Chambers. Two stream 
ciphers. Lecture Notes 
in Computer Science, 809: 
51–??, 1994. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

[Cha94b] James P. Chandler. Iden-
tification and analysis of 
foreign laws and regula-
tions pertaining to the use 
of commercial encryption 
products for voice and data 
communications. Technical 
Report K/DSRD/SUB/93- 
RF105/3, National Insti-
tute for Standards and 
Technology, Gaithersburg, 
MD 20899-8900, USA, Jan-

[Cha95a] Florent Chabaud. On 
the security of some cryp-
tosystems based on error-
correcting codes. Lecture 
Notes in Computer Science,
Chaum:1995:DCS


Chaum:1998:Cb


Chadwick:1999:IWS


Chan:1999:WES


Chau:1999:QCE


Chesson:1973:CC


Cheswick:1992:EBW

[Che92] Bill Cheswick. An evening with Berferd in which a cracker is lured, endured, and studied. In USENIX [USE92a], pages 163–174.

Canetti:1997:MAC

REFERENCES

Chiopris:1992:SBE


Chin:1999:HCD


Chin:1999:HDS


Chiopris:1992:SBE


Chung:1998:DWCb

Tae-Yun Chung, Min-Suk Hong, Young-Nam Oh, Dong-Ho Shin, and Sang-Hui Park. Digital watermarking for copyright protection of MPEG2 compressed video. *IEEE Transactions on Consumer...
Electronics, 44(3):895–901, August 1998. CODEN ITCEDA. ISSN 0098-3063. [Chr99a]


REFERENCES

Chuang:1989:NES


Currie:1996:SEL


Ciarcia:1986:BHD


Cao:1999:DTJ


Clark:1995:SRP


Chabaud:1998:DCS


Collins:1999:DCL


Coster:1992:ILD


technical papers for most of the fifteen “complete and proper” candidates. [CK93]


REFERENCES

A secure, robust watermark for multimedia.


REFERENCES


Mark Allen Clevenger. Data encryption using RSA public-key cryptosystem. Thesis (M.S.), Ball State University, Muncie, IN, USA, 1996. ii + 149 pp.

Chin-Chen Chang, Jyh-Jong Leu, Pai-Cheng Huang and Wei-Bin Lee. A scheme for obtaining a message
REFERENCES


[Clinton:1997:AEC]
Bill Clinton. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 730 et seq. — received in the United States House of Representatives November 15, 1996, pursuant to 50 U.S.C. 1703(b). Washington, DC, USA, January 7, 1997. 5 pp. Referred to the Committee on International Relations. Shipping list no.: 97-0126-P.

[Chua:1999:ART]

[Cheng:1998:MVR]
REFERENCES

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


REFERENCES


Chang:1997:CAS


Camenisch:1999:SEG


Charlton:1999:DPM


Christianson:1999:DSCa

Coradeschi:1999:HMC

Chen:1998:SCC

Canetti:1999:ECS
Charnes:1997:SSH


Chor:1989:SCT


Chuan-Ming:1994:RTR


Craver:1997:CIW


Craver:1998:RRO


Crilly:1987:BPB


Coron:1999:SRSb

Jean-Sébastien Coron and David Naccache. On the


Cohen:1987:CCI


Cohen:1987:IIP


Cohen:1994:SCC


Cohen:1996:RRA


Cohen:1999:MNSk


Colaco:1864:CRO

F. N. Colaço. A criptografia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quase 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.

CPI:1976:CMS


Cominsky:1987:CAP

Isabeth Cominsky. Cryptology: ancient problem modern solutions. Thesis (M.S.), State University of New York, College of
REFERENCES


Comba:1990:ECI


CSL:1994:DES


CSL:1994:EES


CSL:1994:SRC


CERT:1996:PSA


CEC:1997:EST


Chiba:1999:AGD

K. Chiba, H. Ohwada, and

Conradi:1739:CDS


Conklin:1998:SCO


Conklin:1999:ESC


Contini:1999:DPD


Coombs:1983:MC


Coppersmith:1984:FEL

D. Coppersmith. Fast evaluations of logarithms in fields of characteristic two.

**Coppersmith:1987:C**


**Coppersmith:1989:AID**


**Coppersmith:1994:DES**


**Coppersmith:1994:ACS**

[Cop94b] Don Coppersmith. Attack on the cryptographic scheme NIKS–TAS. In


**Coppersmith:1995:ACA**

Coppersmith:1995:FSR


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
Camion:1991:KHF


Chaum:1993:WDO


Chae:1994:AMA


Chung:1998:DWCa


Charney:1997:PSC

REFERENCES

Cheon:1998:TEA

Camenisch:1995:BSB

Chor:1985:KTP

Carroll:1988:ACP

Carroll:1988:CC

Chor:1988:KTP
REFERENCES


Crepeau:1990:VDS


Crepeau:1997:ECP


Contini:1999:IAS


Chaum:1983:ACP


Crypto:1981:ACP


CryptoBytes:1995:C

Crosby Drive, Bedford, MA 01730-1402, USA. CryptoBytes is the technical newsletter on cryptography from RSA Laboratories, a division of RSA Data Security, Inc. It is a free publication, and all issues are available on the World Wide Web.

Cesarini:1983:ACC


Chepyzhov:1991:FCA


Chabaud:1996:CSS


Chambers:1996:RLM


Cusick:1996:BNFb


Camenisch:1997:EGS

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

**Chambers:1997:RLM**


**Chen:1997:NIC**


**Coppersmith:1997:PAP**


**Canteaut:1998:COM**


**Cramer:1998:PPK**


**Coradeschi:1999:ASV**


**Chaum:1989:SCF**

David Chaum and Ingrid Schaumuller-Bichl, editors. *Smart card 2000: the future of IC cards: proceedings of the IFIP WG 11.6 International Conference on Smart Card 2000—the Future of IC...*
Csirmaz:1995:SSM

Coppersmith:1994:ABP

Chang:1997:GSS

Chen:1999:TPS

Collberg:1999:SWM

Chao:1994:DEC
REFERENCES

Currier:1998:MPT


Cusick:1995:CPK


Cusick:1996:BNFa


Cusick:1997:CRN


Ciminiera:1989:AMM


Calvelli:1993:ARS


Chabaud:1995:LBD

F. Chabaud and S. Vaudenay. Links between dif-


[CW94] Andrew Chmora and Stephen B. Wicker, editors. Error control, cryptography, and speech compression: Workshop on Information Protection, Moscow, Russia, December 6–9, 1993: Selected Papers, volume 829 of Lecture Notes in Computer Science. Springer-Ver-
REFERENCES


Chang:1997:SCO


Ceruzzi:1991:RGC


Chang:1998:BSC

Craver:1998:TTL


Cao:1990:DKC


DeMillo:1983:ACC


Dittmann:1998:MSW


D'A90


D'A71


Daemen:1995:HFC


Daemen:1998:MSK


Daemen:1999:RAI


Damgaard:1990:ACE


Damgaard:1990:DPH

plication of Cryptographic
techiques, Aarhus, Den-
mark, May 21–24, 1990:
proceedings, volume 473 of
Lecture Notes in Com-
puter Science. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 1991. CO-
DEN LNCSD9. ISBN 0-
387-53587-X (New York), 3-
540-53587-X (Berlin). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
DM69.00.


REFERENCES

[Damgaard:1999:CSZ]

[Damgaard:1999:LDS]

[Danisch:1995:RES]

[Danthine:1996:ECM]

[Dang:1997:AAC]

[Darnell:1997:CCI]

[Datapro:1985:AAN]
Datapro Research Corporation. All about network ac-


[Dav81] 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].


[Dav94] Donald T. Davis. Review: Applied Cryptography. ;lo-

Davis:1995:KPR


Davis:1996:CDP


David:1998:WWI


Davies:1998:E


Davies:1998:NIH


Davies:1998:LCM


Dawson:1985:COL

M. J. Dawson. Cryptanalysis of ornithological literature, volume 4 of Caliologists’ series. Oriel Stringer,
REFERENCES


[dB94] B. den Boer and A. Bosselaers. Collisions for the compression function of MD5. In Stinson [St94], pages 293–304. CODEN
REFERENCES


REFERENCES

and corrected version is available at ftp.esat.kuleuven.ac.be directory /pub/COSIC/bosselae/ripemd/).

D'Halluin:1999:ASR

DeWin:1996:FSI

deJonge:1986:ASR

deJonge:1987:SVR

Daemen:1998:PCF

Daemen:1998:FHS
Joan Daemen and Craig S. K. Clapp. Fast hashing and stream encryp-

DeOca:1998:DRD


DAmiano:1995:MDM


DeSchutter:1999:ELC


Desmedt:1995:MNA


Desmedt:1995:MNS


DeSantis:1994:HSF


Davio:1985:EHS

Marc Davio, Yvo Desmedt, Jo Goubert, Frank Hoornaert, and Jean-Jacques Quisquater. Efficient

[DJ98c]


[DJ98f]


[DJ98g]

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.

[DJ98h]

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.

[DJ98i]

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 con-
times 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/.

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


[DDJ99] DDJ Staff. News and views: Real-time Java working group; simulated safety; A house of smart cards; father of ubiquitous computing passes away; electrochemical fabrication. Dr.
REFERENCES


Dottolo:1998:WBS


DePaoli:1998:WBS

Denny:1994:FR


Denny:1994:FR

Delaigle:1996:DW


Delaigle:1996:DW

Delaigle:1998:PAD


Delaigle:1998:PAD

Dolev:1991:NC


Dolev:1991:NC

Dolev:1991:NMC


Dolev:1991:NMC

Darmstaedter:1998:BBW


DeDecker:1998:ICS


DeSantis:1998:E


DeSchutter:1998:TFA


DeSmit:1998:GAE


DeMoliner:1999:STB


Drossopoulou:1999:DSJ


Deavours:1987:CP1

Cipher A. Deavours. Cryptanalytic programs for the IBM PC. A Cryptographic series. Aegean Park Press,
REFERENCES


Deavours:1988:BPS


Deavours:1998:A


Kruh:1998:TBW


Demirdogen:1988:FDM


Demytko:1994:NEC


Denning:1979:SPC


Denning:1979:EOS

REFERENCES


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


**Desmedt:1988:SGC**


**Desmedt:1990:PAA**


**Desmedt:1992:BTC**


**Desmedt:1993:TC**


**Desmedt:1994:TC**


REFERENCES


Desmedt:1998:SRR


Desfray:1999:ADP


Desmedt:1999:ES


Deugo:1997:CTS


Deugo:1998:SMS


Desmedt:1990:TC


Desmedt:1991:SGA

REFERENCES


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


REFERENCES


REFERENCES

bibs/0434/04340665.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340665.
pdf.

[DHMR96]

**Dawson:1996:AAS**


[DH96a]

**Ding:1996:WKA**


[DH96b]

**Dhem:1998:DEP**


[Dhe98]

**Diffie:1980:CAM**


[DH98]

**Deschamboux:1996:ADS**


[DHMR96]

**Desmedt:1998:AOC**


[DHQ98a]

**Desmedt:1998:CC**


[DHQ98b]

**Dolev:1995:DFT**

REFERENCES


REFERENCES

DiazdeLeon:1991:PIE


Ding:1996:CRT


Dieringer:1988:TAE


Diffie:1975:PRN


Diffie:1982:CVP


Diffie:1982:CTF


Diffie:1988:FTY


Diffie:1990:APK

REFERENCES

Davis:1994:CRA


Ding:1994:DCD


Dix:1994:SSS


Damm:1998:CRT


Dessmark:1993:MDD


Deavours:1985:MCM

Deavours:1989:CMH


Dusse:1991:CLM


Damgaard:1994:BAH


Damgaard:1996:MEM


Deavours:1998:SCH


Desmedt:1998:CES


Deavours:1987:CYT

[DKKM87] Cipher A. Deavours, David Kahn, Louis Kruh, and
REFERENCES


**Daemen:1997:BCSb**


**Daemen:1997:BCSa**


**Dodson:1995:NFL**


**Dam:1996:CRS**


**Diffie:1998:PLP**

REFERENCES


Demphlous:1999:DPL


Davoine:1997:VCP


DeMillo:1982:CP


Damgaard:1993:ACE


Ding:1997:LMS


delaStelle:1902:TCF


DeMillo:1983:PDS

REFERENCES

Duc:1997:PAF


DeWin:1998:PSS


Denning:1981:MMK


Dongarra:1995:TSS


Denazis:1999:DIO


DAngelo:1994:SEM


Dwork:1993:PPC


Dwork:1994:EEU

[DN94] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signature scheme and its applications. In Desmedt

**Dossis:1995:FSR**


**Dossis:1995:OVH**


**Ding:1997:TFS**

[DNRS97] C. Ding, V. Niemi, A. Renvall, and A. Salomaa.

**Dittmann:1998:IWE**


**Desmedt:1986:CTA**

REFERENCES

DiCrescenzo:1999:CZK


Dobbertin:1995:EMC


Dobbertin:1995:ASA


Dobbertin:1996:CM


Dobbertin:1996:SMA


Dobbertin:1997:RTC


Dobbertin:1998:FTR

Dobbertin:19xx:CM


DomingoFerrer:1996:NPH


Donini:1998:CSR


DiCrescenzo:1999:COTb


Santis:1991:PRP


DiCrescenzo:1994:ROP

REFERENCES

331


REFERENCES


[Daemen:1998:APR]

[Desel:1998:PTP]

[Daemen:1999:EBC]

[Drea:1999:NEB]

[Dray:1998:RNJ]

[Drach:1999:RDO]

[Dreher:1979:PSC]
Felix F. Dreher. Privacy and security in computer based systems using encryption. Pittsburgh State
REFERENCES


[Drea:1992:MUC]

[deRaadt:1999:COO]

[Dro89]

[Dro96]

[Dawson:1995:DIJ]

[Denning:1981:MKG]

[Dolev:1983:AAB]


Dutertre:1997:UPE


David:1998:SIC


Dwork:1998:CZR


Durham:1999:BOO


Dittmann:1998:RMV


Dave:1995:CBS


Desai:1999:CSC

REFERENCES

Durand:1999:DCC

Detombe:1993:CLC

DeSolages:1998:EFO

DiGiorgio:1998:JDS

DuBoulay:1999:DDT

duCarlet:1644:CCV

Dufner:1998:ACH
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


REFERENCES


A. De Santis and M. Yung. Cryptographic applications of the non-interactive metaproof
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alfredo De Santis and Moti Yung. On the design of provably-secure cryptographic hash

Alfredo De Santis and Moti Yung. Arbitrated unconditionally secure authentication can be uncondition-
al protected against arbioter’s attacks (extended abstract). Lecture Notes in Computer Science, 537:
177–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
Dai:1998:WIF


Eberle:1993:HSI


Easter:1999:PES


Ecker:1982:MGE


Ecker:1983:FSR


Ecker:1985:STS


ECMA:1996:EAP

ECMA. *ECMA-219: Authentication and Privilege*
REFERENCES


Ellis:1975:PKC

Edwards:1915:CCT

Epstein:1956:FBC

El-Gamal:1985:PCS

Even:1985:PCC

Even:1985:RPS


Even:1990:LLD

Ellison:1999:PSK

Ellison:2000:PSK


ElGamal:1985:PKCa


ElGamal:1985:PKCb


ElGamal:1985:STA


Elkins:1996:RMS


Ellis:1997:SNS


Ellison:1998:CRN


Ellis:1999:PPN

Elvin:1987:CWW


Even:1993:CCS


Eades:1998:GDC


Ehrsam:1978:CKM


Ezawa:1998:ATS


Endler:1997:PSU


English:1995:EEP


Engen:1999:ECT

Andreas Engen. Elliptic curves and their applications to cryptography: an introduction. Kluwer


REFERENCES


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

Erickson:1999:EAS

Erskine:1999:CDD

Emerald:1997:NPC

Effelsberg:1998:SAI

Escott:1999:AEC

Estell:1980:BW

Ettinger:1998:SGE


Viiveke Fäk. Software versus hardware encryption — is there any difference today? *Computers and Security*, 5(2): 167, June 1986. CODEN CPSEDU. ISSN 0167-4048...
 REFERENCES

Faak:1987:CMM

Falk:1988:DST

Fancher:1996:SCa

Fancher:1997:YPS

Farago:1967:BSS

Farago:1969:BSS

Farrow:1992:HIY

Farrell:1993:CCC


REFERENCES

Feistel:1974:BCC


Feigenbaum:1991:ACC


Feit:1996:TIA


Feigenbaum:1998:C


Feige:1999:NSP

U. Feige. Noncryptographic selection protocols. In IEEE [IEE99a], pages 142–152. CODEN ASF-

Feldman:1987:PSN


Ferris:1987:WBC


Ferguson:1998:UBD


Feynman:1982:SPC


Friedman:1957:SCE

that some author other than William Shakespeare wrote the plays commonly attributed to him. Cambridge University Press, New York, NY, USA, 1957. 4 + vii–xvi + 1 + 302 + 1 pp. LCCN PR2937.F7.

Friedman:1955:CLS


Feghhi:1999:DCA


Fung:1998:PAE


Fuchsberger:1996:PCS


Fuchsberger:1996:PKC


Frankel:1997:ORP


[Fia90] Amos Fiat. Batch RSA. Lecture Notes in Computer Science, 435:175–??, 1990. CODEN LNCSF9. ISSN 0302-9743 (print), 1611-
REFERENCES

3349 (electronic). URL


REFERENCES


REFERENCES


Federrath:1996:MMC

Friedman:1996:AFR

Freeman:1997:MCN

Fellows:1993:KKI

Fellows:1993:FPC

Fellows:1994:CCG
Michael Fellows and Neal Koblitz. Combinatorial cryptosystems galore! In
REFERENCES


[FL99b] B. Fox and B. LaMacchia. Online certificate sta-
REFERENCES


Flowers:1983:DC

Feiertag:1977:PMS

Flynn:1997:WYN
java/9702/java9702.toc.html.

Friedman:1976:ZTJ

Fortune:1985:PP

Feigenbaum:1991:DCC
Joan Feigenbaum and Michael Merritt. Distributed computing and cryptogra-

Faihe:1998:ADR


Feustel:1998:DUI


Fairfield:1985:LRN


Fagundes:1999:EGA


Fairfield:1985:LDE

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.


Flajolet:1989:RMS


Flajolet:1990:RMS


Fujisaki:1997:PEC


Fujisaki:1998:PPS


Fujisaki:1999:HES

REFERENCES


[Forte:1999:FAE] Dario Forte. The future of the Advanced En-
REFERENCES


the Rump Session of Crypto '95, Santa Barbara, CA.


Francis:1992:PSG


Franksen:1993:BCM


Franklin:1999:FCT


Friedman:1935:ICA


Friedman:1935:MCP


Friedman:1935:PIS


Friedman:1939:CAC

REFERENCES

War Department, Office of the Chief Signal Officer, Washington, DC, USA, 1939. 24–36 pp. LCCN ???.


REFERENCES

Friedman:1976:EMC

Friedman:1987:ICA

Friedman:1992:MCP

Friedmann:1993:TDC

Friedman:1996:SLC

Froomkin:1996:ICP
A. Michael Froomkin. It came from planet clipper: the battle over cryp-
tographic key “escrow”.
Technical report, University of Chicago Law School, Chicago, IL, USA, 1996.


**Federrath:1995:SVA**


**Fiat:1999:DTT**


**Frankel:1999:SID**


**Fuchs:1999:BDM**


**Fumy:1993:LAN**


**Fumy:1997:ACE**

REFERENCES

62975-0. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1997. Sponsored by the International Association for Cryptologic Research (IACR).


REFERENCES


[FY98a] Yair Frankel and Moti Yung. Distributed public


Gaglione:1988:ITP


Gaglione:1988:SCT


Gomez-Albarran:1999:MCL


Gaines:1939:ECS


Gaines:1940:ECS


Gaines:1943:ECS


Gaines:1944:CSC


**Gaines:1956:CSC**


**Gait:1977:VCH**


**Gait:1980:MTD**


**Gait:1980:VCH**


**Gait:1990:VCH**


**Gaj:1989:GCM**

REFERENCES

Galland:1945:HABa


Galland:1945:HABb


Galland:1970:HAB


Galil:1988:SIC


Galvin:1996:PKD


Galbraith:1999:CIB


Gamble:1988:IDL

Robert Oscar Gamble. Investigation of discrete logarithmic encryption algorithms. Thesis (M.S.), Uni-
REFERENCES


REFERENCES


Lee Garber. News briefs: Sun gets OK to propose Java standards; domain name plan delayed; encryption battle heats up; monstor processes to debut in 1998; work begins on API for digital TV; ISO approves C++ Standard; new standard for paral-

**Garfinkel:1998:PPG**


**Gaudin:1997:VBJ**


**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.I4 I58. From *Computing Reviews*: “The article reports on the progress of an historical study using a computer for statistical analysis. The subject of the study is a mass of trial depositions of the Knights Templar. The purpose of the project is to find statistical regularities in the large amount of testimony and to create a model for similar studies. The Order of the Knights Templar, founded around 1100, was the first Christian military order. After the Crusades, in the early fourteenth century, 127 articles of accusation were brought against the order, including charges of idolatry, sacrilege, and sodomy. The data being studied are the responses of 900 men to each of 127 accusations. The article details the accusations and the way in which the responses are being coded. The statistical package SAS (Statistical Analysis System) will be used. Examples of the results to be sought are: tallies of guilty/innocent responses, tallies of offenses committed versus seen versus heard about, and correlations between, for example, age and other responses. Depositions that differ markedly from the average response will be identified.”.

**Golshani:1998:NDW**

Forouzan Golshani and Robin Baldwin. In the news: Digital-watermarking faces challenges; virtual human agents evolve; vendors

Geoffroy:1993:APF


Gong:1994:AKD


Goethals:1980:CAL


Gollmann:1990:CC


Gilbert:1991:SAF


Gilbert:1994:CPA

[GC94] Henri Gilbert and Pascal Chauvaud. A chosen plaintext attack of the


B. Goldburg, E. Dawson, and S. Sridharan. The automated cryptanalysis of

**Geffe:1973:HPD**
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**

**Gelb:1974:RWD**

**Gray:1998:PSC**

**Gemmell:1997:ITC**
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.

Gabber:1999:SPC

Goldreich:1986:HCR

Gabber:1997:HMP
E. Gabber, P. B. Gibbons, Y. Matias, and A. Mayer. How to make personalized Web browsing simple, secure, and anonymous. In

Gilbert:1998:ASR


Gittler:1995:DSS


Gehrke:1996:MPK


Gong:1999:PKC


Gennaro:1999:SHS


REFERENCES


Gifford:1981:CSI

Gilder:1997:APD

Giles:1998:EFS

Gilboa:1999:TPR

Gingerich:1970:BRB

Girdansky:1971:DPC

Girdansky:1972:CCD

Girling:1987:CCL


Gennaro:1996:RES


Gennaro:1999:SDK


Garay:1999:AFO


Garay:1999:AOC


Goresky:1995:FRB

M. Goresky and A. Klapper. Feedback registers


Gotz:1997:DTC

Gligor:1979:OMA

Guillou:1982:CT

Goldreich:1989:HCP

Gaskell:1996:ISC

Gladman:1999:IEA
REFERENCES

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


E. Gonzalez, H. Loaiza, A. Surez, and C. Morenoet.
REFERENCES


REFERENCES


Golic:1991:NCC


Galvin:1993:RSP


Gordon:1993:MPC


Gennaro:1995:VSS


Girault:1997:SFR


GomezdeSilvaGarza:1999:EAC


Grohe:1999:DDC

M. Grohe and J. Mariño. Definability and descriptive

**Galvin:1995:RSM**

**Griwodz:1998:PVE**

**Ghazi-Moghaddam:1994:OCH**

**Goldwasser:1985:PSS**

**Goldwasser:1988:DSS**


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

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

ence, 773:355–??, 1994. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/0773/07730355.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0773/07730355.
pdf.

Goettfert:1995:GLB

[GN95a] R. Goettfert and H. Nieder-
reiter. A general lower
bound for the linear com-
plexity of the product
of shift-register sequences.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Gray:1995:PCT

[GN95b] J. P. Gray and F. Naghdy,
editors. Parallel Comput-
ing: Technology and Prac-
tice. PCAT-94. Proceed-
ings of the 7th Australian
Transputer and Occam User
Group Conference: Wool-
longong, NSW, Australia,
8–9 November 1994, vol-
ume 43 of Transputer and
occam engineering series.
IOS Press, Postal Drawer
10558, Burke, VA 2209-
0558, USA, 1995. ISBN 90-
5199-196-7. LCCN ???

Guerrero:1995:CHB

[GN95c] F. Guerrero and J. M.
Noras. Customised hard-
ware based on the RE-
DOC III algorithm for high-
performance date ciphering.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Goldwasser:1993:ISN

S. Goldwasser and R. Os-
trovsky. Invariant signa-
tures and non-interactive
zero-knowledge proofs are
equivalent. Lecture Notes
in Computer Science, 740:
228–245, 1993. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Golic:1995:EPC

J. D. Golic and L. O’Connor.
Embedding and probabilis-
tic correlation attacks on
clock-controlled shift regis-
ters. Lecture Notes in Com-
puter Science, 950:230–243,
ISSN 0302-9743 (print), 1611-
3349 (electronic).

Goldreich:1996:SPS

Oded Goldreich and Rafail
Ostrovsky. Software pro-
tection and simulation on
oblivious RAMs. Journal
of the Association for Com-
puting Machinery, 43(3):
431–473, May 1996. CO-
DEN JACOAH. ISSN 0004-
5411 (print), 1557-735X
(electronic). URL http:


REFERENCES

Goldwasser:1990:ACC


Goldwasser:1990:SPS

Gollmann:1992:ATC

Gollmann:1994:CCC

Goldreich:1995:FCF

Golic:1995:LCS

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

Notes in Computer Science, 1070:268–??, 1996. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:1996:CEP

Gollmann:1996:CA

Gollmann:1996:FSE

http://link.springer-ny.com/link/service/series/0558/tocs/t1039.htm;

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]


[Goldreich:1999:MCP]


[Golic:1999:SCE]


[Golomb:1999:CNS]


[Gong:1989:SCB]


[Gong:1992:SRD]

Li Gong. A security risk of depending on synchronized

<table>
<thead>
<tr>
<th>Gong:1995:CKH</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Gong:1998:JSM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Good:1979:EWC</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Goodman:1996:LPS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Gordon:1985:SPE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Gordon:1993:DDT</th>
</tr>
</thead>
</table>
Gordon:1993:DLU


Goth:1999:NBG


Guajardo:1997:EAE


Ghodosi:1999:RCN


Ghodosi:1996:CHG


Gladychev:1998:CRJa


Gladychev:1998:CRJb

[181x198] [GPO98b] Pavel Gladychev, Ahmed Patel, and Donal O’Mahony.

**Goldreich:1998:SCP**


**Ghodosi:1997:RMA**


**Ghodosi:1998:SSM**


**Ghodosi:1998:CCS**


**Gore:1998:SDC**


**Gabidulin:1991:INC**

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


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


REFERENCES


[Refs]
REFERENCES

DMAPEW. ISSN 0924-9265.


Gritzalis:1997:CPO


Gong:1998:SSG


Gribomont:1999:SDU


Gysin:1999:GCA


Giddy:1994:ACT


Gobioff:1996:SCH

REFERENCES

Goldreich:1999:CSZ

Gafni:1999:EMI

Grehan:1994:BCRa

Gotoh:1990:MRR

Guarini:1904:MTT
**REFERENCES**

<table>
<thead>
<tr>
<th>Author</th>
<th>Title and Details</th>
</tr>
</thead>
</table>
simplification for the crypt-analysis of the NBS Data Encryption Standard. Thesis (M.Sc.), University of British Columbia, Ottawa, ON, Canada, 1983. 3 microfiches (265 fr.).

**Gunther:1988:ASG**


**Gunther:1988:ACE**


**Gurnsey:1997:CT**


**Gustafson:1996:SAS**


**Gutmann:1996:SDD**

REFERENCES

**Guthery:1998:SC**


**Gutmann:1998:SGP**


**Gutmann:1999:DCS**


**Guy:1976:HFN**


**Gao:1998:GPO**


**Griffiths:1976:AMR**


**Goldberg:1996:RNB**

REFERENCES


[GYl38] Yves Gyldén. 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. A. B. Teknik co., Stockholm, Sweden, 1938. 10 pp.


REFERENCES


[Had84] Bruce K. Haddon. Book review of “Security, IFIP/

[Ham71] Carl Hammer. Signature simulation and certain cryptographic codes. Communications of the Association

[Had84] Bruce K. Haddon. Book review of “Security, IFIP/

[Ham71] Carl Hammer. Signature simulation and certain cryptographic codes. Communications of the Association

Haddon:1984:BRS

Hoffman:1994:CP

Hammer:1971:SSC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC

Hagelin:1998:SHC


REFERENCES


REFERENCES

Haselberger:1995:DRB

Hasan:1999:LTB

Hatefi:1996:MRE

Hatefi:1997:AED

Haugen:1974:RSS

Hawkes:1998:DWK

Hawkes:1998:DLW
REFERENCES


REFERENCES

CODEN CSSEEI. ISSN 0267-6192.


REFERENCES

Hartung:1998:DWM


Heidel:1676:JTP


Heideman:1996:SIT


Heintze:1996:SDF


Hellman:1976:SPN

M. E. Hellman. Statement to participants at
REFERENCES


Hellman:1979:WTI


Hellman:1979:MPK


Hellman:1981:ACA


Held:1993:TSD

Gilbert Held. Top secret data encryption techniques.


Helleseth:1994:ACE


Held:1998:ARU


[Her89] Jeffrey Stuart Hersch. Digital signature analysis of


[HG97b] Helena Handschuh and Henri Gilbert. \( \chi^2 \) cryptanalysis of the SEAL en-
cryption algorithm. Lecture Notes in Computer Science, 1267:1–??, 1997. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-
ny.com/link/service/series/0558/bibs/1267/12670001.htm; http://link.springer-


REFERENCES

Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


REFERENCES


Higenbottam:1973:CC


Highland:1983:BRCb


Highland:1987:CC


Highland:1987:DES


Highland:1987:ERIC


Highland:1987:HEM

REFERENCES

Highland:1988:PEM


Highland:1988:RRC


Highland:1988:TSC


Highland:1988:TSV


Highland:1988:EAE


Highland:1988:SIT


Highland:1989:SDI

Highland:1997:HCV

Highland:1997:PRC

Hill:1929:CAA

Hill:1931:CCL

Hiltgen:1994:CRC

Hill:1997:MTY

Haastad:1999:PGO
REFERENCES


[HJH85] HJH. Book review: Kahn on codes: Secrets of the new
REFERENCES

cryptology. David Kahn
247, September 1985. CODEN CPSEDU. ISSN 0167-

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

[HJJ+xx] A. Herzberg, M. Jakobsson,
S. Jarecki, H. Krawczyk,
and M. Yung. Proactive
public key and signature
systems. ???, 19xx. URL http://
thory.lcs.mit.edu/cis/
cis-publications.html.

Herzberg:1995:PSS

[HJKY95] A. Herzberg, S. Jarecki,
H. Krawczyk, and M. Yung.
Proactive secret sharing, or:
How to cope with perpetual
leakage. In Coppersmith
[Cop95d], pages 339–352.
CODEN LNCSD9. ISBN 3-
540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-
URL http://link.springer-
ny.com/link/service/series/0558/tocs/t0963.htm;
issue&issn=0302-9743&volume=963. Sponsored
by the International Association for Cryptologic
Research (IACR), in cooperation with the IEEE
Computer Society Technical
Committee on Security and Privacy.

Hillenbrand:1999:SDW

[HJL99] T. Hillenbrand, A. Jaeger,
and B. Loechner. System
description: Waldmeister —
improvements in performance and ease of use. Lecture
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-
3349 (electronic).

Hong:1997:IAU

[HJPB97] L. Hong, A. Jain, S. Pankanti,
and R. Bolle. Identity authen-
tication using fingerprints. Lecture Notes in
Computer Science, 1206:
103–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Huehnlein:1998:CBN

[HJPT98a] D. Huehnlein, M. J. Jacobson,
S. Paulus, and T. Takagi.
A cryptosystem based on non-maximal imaginary
quadratic orders with fast


Herlea:1999:SBR


Halevi:1997:MSM


Herlea:1999:SBR


Halevi:1997:MSM


Hevia:1998:STD

[Alejandro Hevia and Marcos Kiwi. Strength of

**Halevi:1999:PKC**

**Halfmann:1999:ESP**

**Haynes:1999:VDS**

**Hevia:1999:STD**

**Hromkovic:1994:CDC**

**Harpes:1995:GLC**
C. Harpes, G. G. Kramer, and J. L. Massey. A generalization of linear cryptanaly-


Jing Min He and Kai Cheng Lu. The security and de-

**Hauser:1992:VMA**


**Harn:1993:SGS**


**Herzberg:1993:PRC**


**Han:1999:VFG**


**Hwang:1999:CDC**


**Hwang:1995:TAN**


**Hwang:1996:SCW**

Tzonelih Hwang, Narn-Yih Lee, Chuan-Ming Li, and Chin-Chen Chang. On the security of Chang and Wu’s


REFERENCES


REFERENCES


[Habutsu:1991:SKC] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and

**Hansmann:1999:SCA**


**Hawkes:1996:ALC**


**Hodges:1983:ATE**


**Hodges:1997:ATHa**


**Hoffer:1955:MAC**


**Hoffman:1993:CC**


**Hoffman:1995:BBB**

Hofmeister:1999:ACA


Hogan:1988:PIS


Hollis:1987:TCA


Holloway:1991:RA


Honore:1919:STS


Hontanon:1998:EC


Hood:1980:EFS


Hoogendoorn:1982:SPK

REFERENCES


[Patrick Horster. Von der Schwierigkeit, sichere Kryptosysteme zu entwerfen. (German) [The difficulty of designing safe cryptosystems]. In Angewandte Mathematik, insbesondere Informatik, pages 82–117. Vieweg & Sohn, Braunschweig, Germany, 1999.]
REFERENCES


[HPG98] Juan Ramón Hernández and Fernando Pérez-González. Shedding more light on image watermarks. *Lecture...
REFERENCES

Hoffstein:1998:NRB

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http: 
//link.springer-ny.com/link/service/series/0558/bibs/1423/14230267.htm;
 http://link.springer- 

Hwang:1990:PKA

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http: 
//link.springer-ny.com/link/service/series/0558/bibs/0434/04340657.htm;
 http://link.springer- 

Holland:1982:GSA


Hollander:1996:KWS

org/publications/library/proceedings/sec96/hollander.html.

Harrison:1976:POS

7317 (electronic).
Hruby:1995:QDQ


Hruby:1995:QQC


Hruby:1996:SCI


Hruby:1998:TQC


Hruby:1999:SUD


Hernandez:1999:CLM


Haastad:1985:CST

REFERENCES

Hammer:1987:EUH


Hardjono:1989:TCB


Hardjono:1990:SKS


Haber:1991:HTD


Hinsley:1993:CIS


Hardjono:1994:AMS


Handel:1996:HDO


Hardjono:1996:RKA

[HS96b] T. Hardjono and J. Seberry. Replicating the Kuperee authentication server for increased security and
Hall:1997:REG


Helme:1997:SFF


Harasawa:1999:CMF

REFERENCES


ican Cryptogram Association (George C. Lamb Collection).

[Hun85]  

[Hus94]  

[Hus99]  

[HVH98]  
REFERENCES

Hardy:1975:ITN


Hartnell:1976:PFM


Hardy:1979:ITN


Huthnance:1988:UPP


Hotchkiss:1991:ASI


Hsu:1997:DWV


Hsu:1998:DBW


Hsu:1998:MWD

[HW98b] Chion-Ting Hsu and Ja-Ling Wu. Multiresolution watermarking for digital im-


Hwang:1997:CKA


Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE


Hall:1998:BPPa


Hall:1998:BPPb


Hohl:1994:SIH


1999. CODEN ISIJBC. ISSN 0020-0255 (print), 1872-6291 (electronic).

**Hardjono:1993:PDM**


**Ibbotson:1997:CPI**


**Anonymous:1993:CCA**


**IBM:19xx:PSP**


**IEEE:1974:ASS**


**IEEE:1979:ASF**


**IEEE:1980:PSS**


**IEEE:1981:CLC**

IEEE, editor. *6th Conference on Local Computer

REFERENCES


IEE:1986:CEC


IEE:1986:ASF


IEE:1987:PIS


IEEE:1987:ASF


[IEEE:1994:CPN]


[IEEE:1994:PAC]


[IEEE:1994:PSH]


[IEEE:1994:TAJ]
REFERENCES


REFERENCES


**IEEE:1997:ASF**


**IEEE:1997:IICa**


**IEEE:1997:PICa**


IEEE, editor. International Conference on
REFERENCES


Igarashi:1999:ITP


Izu:1998:PSE


Israel:1983:AOS


Impagliazzo:1989:OWF


Ilie:1994:CAS


Imai:1986:AMC


Iwamura:1993:HIM

Iwamura:1993:HSI


Impagliazzo:1992:PGP


Impagliazzo:1989:ECS


Ito:1999:DPS


Ingemarsson:1998:E


Instenes:1995:MAA


IRD:1979:DVE


IDC:1981:DE

International Data Corporation. *Data encryption*. Research memorandum IDC #ISPS-M81-10,
REFERENCES

International Data Corporation, Framingham, MA, USA, October 1981. 30 pp.

**IRD:1981:DTV**


**IRD:1984:DTV**


**IRD:1987:DTV**


**IRD:1988:DTV**


**Anonymous:1991:IIS**


**IRD:1991:DFV**


**Itoh:1994:LDS**

IMPAGLIAZZO:1989:LPC


ING:1999:SRT


IMAI:1993:ACA


IRWIN:1998:RWD


INGEMARSSON:1991:PSS


IKRAM:1997:CSE

[IS97] N. Ikram and S. J. Shepherd. A cryptographically secure EW database with selective random access. In ???, editor, Proceedings of
Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikram:1999:UIN

Ikra
REFERENCES


Ingemarsson:1981:UAS


Imai:1998:PKC


Jaburek:1990:GGP


Jackson:1987:NTS


Jackson:1990:SITa

Keith M. Jackson. *Secure information transfer:
References


Jackson:1990:SITb


Jackson:1996:AAC


Jakobsson:1995:BUU


Jakobsen:1998:CBC


Jakobsen:1999:HOC


Jakobsson:1999:MCM


Jakobsson:1999:QCA

REFERENCES

Jamieson:1998:UEP

Jantke:1995:RSI

Janecek:1999:AVR

Jarecki:1996:PSS

Jarvis:1997:GB

Jaspan:1996:DWE

Jaeger:1993:LCC

Jan:1998:PWP
REFERENCES

elsevier.com/cas/tree/
store/jss/sub/1998/42/
1/6026.pdf.

[JD91] D. B. Johnson and G. M. Dolan. Transaction Se-
tegrity System extensions
to the Common Crypto-
graphic Architecture. IBM
Systems Journal, 30(2):
IBMSA7. ISSN 0018-8670.

Johnson:1991:TSS

Le, and S. M. Matyas. Common Cryptographic Archi-
tecture Cryptographic Ap-
plication Programming In-
terface. IBM Systems Jour-
CODEN IBMSA7. ISSN
0018-8670.

Johnson:1991:CCA

[Jef86] Keith Jeffery. The Gov-
ernment Code and Cypher
School: A memorandum by
Lord Curzon. Intelligence
and National Security, 1
(3):454–??, 1986. ISSN
0268-4527 (print), 1743-
9019 (electronic).

Jeffery:1986:GCC

[JG90] Rick Joyce and Gopal
Gupta. Identity authenti-
cation based on keystroke
latencies. Communications of the Associa-
tion for Computing Ma-
chinery, 33(2):168–176,
February 1990. CODEN
CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http:
//www.acm.org/pubs/toc/
Abstracts/0001-0782/75582.
html.

Jevons:1874:PS

Jenkins: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, Accu-
mulate, 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.

Jenkins:19xx:IFC

Joyce:1990:IAB

W. Stanley Jevons. The
Principles of Science. ???,
????, 1874. ??–?? pp.

Jevons:1874:PS
REFERENCES


REFERENCES

Johansson:1999:FCA


Johansson:1999:IFC


Jakobsen:1997:IAB


Jun:1999:IRN


Juels:1997:SBD


Jonker:1999:VTK


Jones:1975:ESP


Jonker:1999:VTK


Jonsson:1999:FCA


Jonsson:1999:IFC


Jonsson:1999:VTK


Jonsson:1999:FCA


Jonsson:1999:IFC


Jonsson:1999:VTK

REFERENCES

link/service/series/0558/ibib/1294/12940150.htm;

**Jurgensen:1984:SRI**


**Jackson:1993:CAG**


**Janwa:1996:MPK**


**Johnson:1996:AEE**


**Jurisic:1997:ECC**


**Jakobsson:1999:IMI**


**Johnson:1994:CDM**

REFERENCES

Jackson:1994:MTS

Jackson:1995:ESS

Jackson:1995:SMS

Jakobsson:1996:DVP
URL http://www.bell-labs.com/user/markusj/dvp.ps. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Jarecki:1997:EMS
REFERENCES

Joesang:1998:SMA

Johnson:1989:BDC

Johnson:1990:EDE

Johansson:1994:CPA

Johnson:1995:ACD
REFERENCES


Johnson:1996:LP


Johnson:1997:SP


Johnson:1997:SPS


JohnByrne:1998:CEC


Johnson:1999:LES


Jolitz:1995:PB


Jones:1978:WWB


Jones:1978:MSW

REFERENCES


Josse:1885:CSA


Juels:1996:HCC


Joye:1997:PFR


Joye:1998:CRT

Marc Joye and Jean-Jacques Quisquater. Cryptanalysis of RSA-type ciphersystems: a visit. In
REFERENCES


Joye:1998:REC


Joye:1997:RTS


Jurgensen:1996:TFC


Jones:1993:DAC


Joux:1993:CAK


Johansson:1995:AIA


Johansson:1995:CIA

REFERENCES


Jung:1988:IRC


Jungnickel:1996:DFG


Jung:1999:EMA


Jurgen:1986:SEI


Jutla:1998:GBA


Just:1996:AMP


Jakubowski:1998:CSP


Jeannerod:1998:GEE

C. P. Jeannerod and J. Visconti. Global error esti-
REFERENCES


Joye:1998:IBS


Kompella:1991:FCC


Kent:1998:RIA

REFERENCES

/Kwww.math.utah.edu/pub/rfc/rfc2402.txt/. Obso-
/letes RFC1826 [Atk95a]. Status: PROPOSED STAN-
/DARD. [Kah66]

/KKent:1998:RIE

/K[KA98b] S. Kent and R. Atkinson. RFC 2406: IP Encapsulat-
/ing Security Payload (ESP), November 1998. URL
/ftp.internic.net/rfc/rfc2406.txt; https://
/Kwww.math.utah.edu/pub/rfc/rfc2406.txt/. Obso-
/letes RFC1827 [Atk95b]. Status: PROPOSED STAN-
/DARD. [Kah67a]

/KKoutsoukos:1999:HCS

/K[KA99] X. D. Koutsoukos and P. J. Antsaklis. Hybrid control
/systems using timed Petri nets: Supervisory control
design based on invariant properties. Lecture Notes
/in Computer Science, 1567: 142–162, 1999. CODEN
/LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
/tronic). [Kah67b]

/KKahn:1963:PNU

/David Kahn. Plaintext in the new unabridged: an exami-
/nation of the definitions on crypto- 
/logy in Web-
/ster's Third New Interna-
tional Dictionary. Crypto Press, New York, NY, USA,
/1963. 35 pp. [Kah74]

/KKahn:1966:MC

/David Kahn. Modern cryptography. Scientific American,
/215(1):38–46, July 1966. CODEN SCAMAC. ISSN
/0036-8733 (print), 1946-7087 (electronic). URL
/http://www.nature.com/
/scientificamerican/journal/

/KKahn:1967:CSSa

/David Kahn. The codebreakers: the story of secret 
/writing. MacMillan Publishing Company, New York,
/uk/~fapp2/steganography/
bibliography/1000.html.

/KKahn:1967:CSSb

/David Kahn. The codebreakers: the story of secret 
/writing. Weidenfeld and Nicolson, London, UK, 

/KKahn:1974:C

/David Kahn. The Codebreakers. Weidenfeld and 
Kahn:1976:TC


Kahn:1979:CGP


Kahn:1982:GLC


Kahn:1983:KCS


Kahn:1984:COS


Kahn:1991:SER


Kahn:1991:WWW


Kahn:1996:HS


Kahn:1996:CSS


[Koc96] Çetin Kaya Koç, Tolga Acar, and Burton S. Kaliski, Jr. Analyzing and comparing Montgomery multiplication algorithms — assessing five algorithms that speed up modular exponentiation, the most popular method of encrypting and signing digital data. *IEEE Micro*, 16
REFERENCES


Kaliski:1984:AWA

Kaliski:1985:WAE

Kaliski:1991:MMD

Kaliski:1992:MAC

Kaliski:1993:SES

Kaliski:1993:ZBA
Burt S. Kaliski, Jr. The Z80180 and big-number arithmetic. Dr. Dobb’s Journal of Software Tools, 18(9):50, 52, 54, 56, 58, 90–91, September 1993. CO-
DEN DDJOEB. ISSN 1044-789X.

Kaliski:1995:MIA

Kaliski:1997:IPS

Kaliski:1997:PNG

Kaliski:1997:ACC

Kaliski:1998:C

Kaliski:1998:RPRa
REFERENCES


REFERENCES

Kaps:1998:HSF


Karger:1985:ADA


Karger:1986:ADA


Karger:1987:LDP


Kari:1989:CBP


Kari:1989:OCP


Karkare:1996:SEA


Kasiski:1863:GDG

[Friedrich Wilhelm Kasiski. Die Geheimschriften und die Dechiffrikunst, Mit besonderer Berücksichtigung der deutschen und französischer 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 ????


REFERENCES

CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).


REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>
aes. No slides for the conference talk are available.


Kundur:1997:RDI


Kundur:1998:DWU


Kunkelmann:1998:VEB


Kharitonov:1993:CHD


Karaornan:1999:CRJ


Kobara:1996:LVS

K. Kobara and H. Imai. Limiting the visible space visual secret sharing schemes and their application to human identification. Lecture Notes in Computer Science, 1163:185–??, 1996. CODEN
REFERENCES

Kobara:1997:SSM

Katsumoto:1999:DPL

Kiefer:1998:WMV

Kilian:1988:FCO

Kim:1993:CLB

Kippenhahn:1997:VBG

Kippenhahn:1999:CBH
Verschlüsselte Botschaften, in collaboration with the author, by Ewald Osers.


N. Kunihiro and K. Koyama. Equivalence of counting the...
number of points on elliptic curve over the ring \( \mathbb{Z}_n \) and factoring \( n \). Lecture Notes in Computer Science, 1403:47–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Kommerling:1999:DPT**


**Koren:1999:ISC**


**Koshelev:1999:EAM**


**Kurosawa:1991:GPK**


**Kabatianskii:1997:DSS**

G. Kabatianskii, E. Krouk, and B. Smeets. A digital signature scheme based on random error-correcting codes. Lecture Notes in
REFERENCES


Kramer:1999:FCD


Kothari:1984:CMW


Kilian:1995:FCR


Knudsen:1995:NAA


Klein:1990:FCS


Kannan:1988:PFN

R. Kannan, A. K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic

**Klupsch:1999:ARR**


**Kurosawa:1988:CSP**


**Kurak:1992:CNI**


**Kang:1993:PRR**


**Kim:1996:ACA**

REFERENCES

Knudsen:1996:IDA


Kosuda:1997:SED


Kaksonen:1998:OMC


Kaufman:1998:DWF


Knudsen:1998:SMD


Kasahara:1999:NPK


Knudsen:1999:CIS

L. R. Knudsen and W. Meier. Cryptanalysis of an identification scheme based on the permuted perceptron problem. Lecture Notes in Computer Science, 1592:363–369,
1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kohlas:1999:RAP


Koscielny:1999:QBP


Kanda:1998:ECC


Kobayashi:1999:FEC


Konheim:1980:ICP


Koyama:1991:NPK

REFERENCES

Kande:1999:AUD

Karn:1995:REC

Karn:1995:RET

Kohl:1993:RKN

Kno:1979:AEO

Kohl:1994:EKA

Knuth:1969:SNM
Donald E. Knuth. Semi-numerical Algorithms, volume 2 of The Art of Com-
REFERENCES


Knuth:1969:SA


Knuth:1973:FA


Knuth:1980:DLC

Donald E. Knuth. Deciphering a linear congruential encryption. Report 024800, Department of Computer Science, Stanford University, Stanford, CA, USA, 1980.

Knuth:1985:DLC


Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb


Knudsen:1993:ICS


Knudsen:1993:CLc

Lars Ramkilde Knudsen. Cryptanalysis of LOKI. Lecture Notes in Computer
REFERENCES


Knudsen:1993:CLa

Knudsen:1994:PSF

Knudsen:1994:BCA

Knudsen:1995:NPW


Knudsen:1998:BCS

Knudsen:1998:DBC

Knudsen:1999:STA

Knudsen:1999:CBC
0302-9743 (print), 1611-3349 (electronic).

Knudsen:1999:FSE


Kurosawa:1995:CIS


Kurosawa:1995:CBA


Kurosawa:1996:CLB


Kurosawa:1997:CLB


Koblitz:1987:CNT


Koblitz:1987:ECC

Neal Koblitz. Elliptic curve cryptosystems. Math-


REFERENCES

issn=0302-9743&volume=1109. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).


Kochanski:1989:HSI


Koc:1994:HSR


Kocher:1995:CDR


Koc:1996:RHI


Kocher:1996:TAI


Kocher:1999:B

REFERENCES 522


REFERENCES

Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Konheim:1989:RMC


Kong:1995:DES


Koopman:1986:OES


Kurosawa:1995:TIK


Kurosawa:1995:CIT


Koops:1997:CRE

[Koo97] Bert-Jaap Koops. Crypto

Kopooshian:1997:DCE

[Hrag H. Kopooshian. Data compression and encryption. Thesis (M.S.), California State University, Northridge, Northridge, CA, USA, 1997. vi + 127 pp.]

Kornerup:1993:HRM


Korner:1996:PC


Koscielny:1983:PRD


Kurosawa:1994:NSS

[Kaoru Kurosawa, Koji Okada, Keiichi Sakano,
REFERENCES


Koyama:1982:CUM


Koyama:1982:MKR


Koyama:1983:MKR


Koyama:1995:FRT


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kozen:1996:RSS

Kim:1989:PRP

Kwan:1993:GPT

Krajicek:1995:SCC

Knudsen:1996:HFB

Knudsen:1996:DSK

Knudsen:1997:FSH
REFERENCES


Kilian:1998:IE


[KP98]

Kaps:1999:FIF


[KP99a]

Koc:1999:CHE


[KP99b]

Kipnis:1999:UOV


[KPG99]

Karhumaeki:1999:CSI


[KPR99]

Kaliski:1994:FBC

REFERENCES

Kaliski:1994:LCU


Kaliski:1995:MAM


Kaliski:1995:SUR


Kaliski:1996:MEW


Kilian:1996:HPA

[J. Kilian and P. Rogaway. How to protect DES against exhaustive key search. In Koblitz [Kob96],...
Knudsen:1996:NAL


Kankanhalli:1998:CBW


Knudsen:1999:DFC


Kolliopoulos:1999:NLT


Krause:1984:DEI


Kranakis:1986:PC

REFERENCES


REFERENCES


Krawczyk:1999:BCC


Kesdogan:1998:DTP


Knudsen:1998:DSR


Kumar:1999:CCB


Kruh:1998:WWS

Jackson:1998:RPRb


Kurosawa:1997:DSP


Knudsen:1999:TDS


Kordes:1989:UMC


Kelsey:1997:CPO


Kwon:1997:SEA

REFERENCES

Kelsey:1998:SPP

The street performer protocol.

Kipnis:1998:COV

Cryptanalysis of the oil and vinegar signature scheme.

Kipnis:1999:CHP

Cryptanalysis of the HFE public key cryptosystem by relinearization.

Kemp:1996:CPC

A. H. Kemp, S. J. Shepherd, and S. K. Barton. Corre-
REFERENCES


Kelsey:1997:SAL


Kelsey:1998:SAL


Kim:1996:EIE

Yong-Tae Kim, Kwang-Suk Suh, and Chang-Han Kim. On the efficient implementations of the ellip-


**Kelsey:1998:PICb**


**Kelsey:1999:KSWa**


**Kelsey:1999:MCAa**


**Kelsey:1998:SCCa**


**Kelsey:1998:SCCb**

J. Kelsey, B. Schneier, D. Wagner, and C. Hall.


Koyama:1998:AFC


Kim:1999:AFC

[KT99] Eugene Eric Kim and Betty Alexandra Toole. Ada and the first computer: The collaboration between Ada, Countess of Lovelace, and computer pioneer Charles Babbage resulted in a landmark publication that described how to program the world’s first computer. Scientific American, 280(5):76–81, May 1999. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). See also [AAG+00].

Kanda:1999:SCF


Kuchlin:1987:PKE


Kucera:1992:GES


Kuhn:1998:CIS

Kuijk:1991:RSE


Kukorelly:1999:VCH


Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC


Kumar:1997:CSI


Kummert:1998:RPT

REFERENCES

Kuo:1990:TEC


Kurosawa:1994:NBA


Kearns:1994:CLL


Kaul:1999:IBP


Kirstein:1992:PAS

Kwan:1999:SDK


Kwan:1993:SAD


Kwan:1997:DIE


Kaliski:1995:SRE


Kaliski:1995:DLC


Kaliski:1997:SRE

REFERENCES

Kaliski:1998:SRE


Kaliski:19xx:DLC

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

Kwok-Yan:1992:FAA


Kasami:1982:KMS


Koch:1995:TRH


Levien:1998:ART

Raph Levien and Alex Aiken. Attack-resistant trust metrics for public key certification. In USENIX
REFERENCES


Lampson:1991:ADS


Lacy:1993:CCS


Laffin:1964:CCS


Lampson:1992:ADS


Lagarias:1984:KPK


Lagarias:1984:PAS


Lagarias:1990:PNG


**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.”.

**Lai:1995:ALS**


**Lakshivarahan:1983:APK**


**Lampson:1973:NCP**


**Lamport:1981:TNP**


**Lambert:1999:DSV**

James D. Lambert. DREO secure video conferencing and high speed data encryption tests for Inmarsat-
REFERENCES


Landers:1946:RPR


Langie:1981:CSS


Langford:1995:DCT


Langford:1996:WST


Lange:1997:SCI


Landrock:1998:TOC


Landau:1989:SSC

REFERENCES

Landrock:1999:PTU

Lawton:1998:NBS

Lee:1989:WBL
REFERENCES


REFERENCES


**Lopez:1999:IAE**


**Li:1994:EMN**


**Lin:1999:AMG**


**Leary:1999:NBE**

Leclerc:1989:CRM

Lee:1995:NSI

Leech:1996:RUP

Lee:1999:GIC

Lee:1999:DAA


Leighton:1979:BRA

Leighton:1979:BRB
Albert C. Leighton. Book review: *An annotated bib-
biography of cryptography.
xvi + 372 pp. illus. $35.00. Historia Mathematica, 6(2):
213–218, May 1979. CODEN HIMADS. ISSN 0315-
0860 (print), 1090-249X (electronic). URL http://
www.sciencedirect.com/science/article/pii/0315086079900934

Leiss:1980:NSS

E. Leiss. A note on a signature system based on probabilistic logic. Information
0020-0190 (print), 1872-6119 (electronic).

Leipold:1999:K

Cosimo Leipold. Kerberos. Linux Journal, 68:??, December 1999. CODEN LJ-
JOFX. ISSN 1075-3583 (print), 1938-3827 (electronic). URL http://
noframes.linuxjournal.com/1j-issues/issue68/3329.html.

Leiserson:1999:ITD

C. E. Leiserson. Invited talk: Design and analysis of algorithms for shared-

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

Lempel:1979:CT

285–303, December 1979. CODEN CMSVAN. ISSN
0010-4892.

Lennon:1978:CAI

Richard E. Lennon. Cryptography architecture for information security. IBM

Lenstra:1987:FIE

H. W. Lenstra, Jr. Factoring integers with elliptic curves. Annals of
Mathematics, 126(3):649–
673, 1987. CODEN AN-
MAAH. ISSN 0003-486X
(print), 1939-8980 (elec-
tronic). URL http://
www.jstor.org/stable/
1971363.

Lenstra:1990:PT

Arjen K. Lenstra. Primality
testing. In Pomerance and
Goldwasser [PG90], pages
13–25. ISBN 0-8218-0155-
4. ISSN 0160-7634. LCCN
QA76.9.A25 C84 1990; QA1
.A56 v.42 1990. Lecture
notes prepared for the
American Mathematical So-
ciety short course, Crypt-
tology and computational
REFERENCES

number theory, held in Boulder, Colorado, August 6–7, 1989.

[Len93]

[Len96a]

[Len96b]

[Len98]

[Lev58]
Levine:1961:SAH


Levine:1961:SECa


Levine:1961:SECb


Levine:1983:USC


Levine:1985:OWF

REFERENCES

[Lewis:1992:SCP]

[Lexar:1976:END]

[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]

[Laih:1997:CDE]

[Laih:1993:GTC]
REFERENCES

[LHB96]

Lin:1993:GSS


[LH93b]


[LH94]


[Li:1994:RTR]


[Li:1995:TSW]


[Li:1995:TMS]

Chuan-Ming Li, Tzonelih Hwang, and Narn-Yih Lee.

### Landwehr:1984:SMM

### Lee:1998:ZNP

### Lichtenthal:1994:CBT

### Lidl:1985:CBP

### Lidl:1990:SMA
University in Sydney from 29 June to 7 July 1989.


REFERENCES

Obsoletes RFC0989 [?]. Status: UNKNOWN.

**RFC1040**


**RFC1113**

[Linn:1989:RPE]


**RFC1421**

[Linn:1993:RPE]

[JLin93a] J. Linn. RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures,


REFERENCES

Lipton:1994:CNF

[Rip94]
R. J. Lipton. Coding for noisy feasible channels. In IEEE [IEE94a], pages 27–??
IEEE Catalog No. 94TH8100.

Abeles:1998:KVC

[Lip98]

Lipmaa:1999:ICM

[Lip99]

Litant:1987:BRC

[Lit87]

Lindsay:1997:BC

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

Laih:1996:CEE

[LK96]
C.-S. Laih and W.-C. Kuo. Cryptanalysis of the enhanced ElGamal’s signature
REFERENCES


**Lee:1999:MRF**


**Landau:1994:CPP**


**Linnartz:1998:MFA**


**Lenstra:1993:DNF**


**Liaw:1993:OAA**


[LL97b] Chae Hoon Lim and Pil Joong Lee. Directed signatures and application to thresh-


REFERENCES

Lam:1996:EGE


Lenstra:1990:NFS


Lenstra:1993:FNF


Luccio:1980:CMC


Lidl:1984:PPR


Leighton:1985:HBC

Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


Tom Leighton and Silvio Micali. Secret-key agreement without public-key cryptography. Lecture
Leighton:1994:SKA


Leighton:1995:LPF


Low:1996:MCP


Lamersdorf:1998:TDS


Low:1998:PCT


Low:1995:DMI


REFERENCES

570


Leonard:1997:CSP


Lautemann:1999:DCA


Lidl:1994:IFF


Lehti:1998:CT


Lagarias:1985:SLD


LaMacchia:1991:CDL

LaMacchia:1991:SLS


Lomas:1994:ENT


Lomas:1997:SPI


Long:1991:PAA


Lomas:1997:SPI


Long:1991:PAA


Long:1992:UDE

Yong Hong Long. Using Diophantine equations to
REFERENCES


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


Lam:1999:ACA

REFERENCES


Luby:1986:PRP


Lagarias:1988:UEP


Lai:1996:AHH


Lysyanskaya:1998:GBD


Lai:1993:FCC


Lange:1925:TC

André Lange and E. A. Soudart. \textit{Traité de cryptographie}. (French) [Treatise on cryptography].
REFERENCES


[LS98a] 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,

[Luby:1998:CBB]

[Lamport:1982:BGP]
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.

[Livens:1995:CCI]

[Leung:1985:SCT]


Leong:1991:UPE


Linnartz:1998:MPM


Langley:1999:ACI


Laih:1995:SLF


Lioen:1988:OMA


Lioen:1988:OMF


Lu:1979:EGC


Lu:1980:AEG

REFERENCES


**Lackey:1995:SMS**


**Lub96**


**Lucks:1995:HEI**


**Lucks:1996:FLC**


**Lucks:1996:FLR**


**Lucks:1997:SRK**


**Lucks:1998:SBB**


REFERENCES


REFERENCES


Lodge:1994:SCC


Laih:1993:TES


Li:1990:ACP


Li:1991:HBM


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN


MacLaren:1994:CPN

N. MacLaren. Cryptographic pseudorandom
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Mache:1998:SCT**


**Madsen:1992:GCD**


**Madsen:1996:CCL**


**Madsen:1997:KEE**


**Madsen:1998:CPU**


**Madsen:1998:EDR**

REFERENCES

Madsen:1998:ELP

Madsen:1998:FFE

Madsen:1998:NCK

Madsen:1998:USC

Madsen:1999:MBF

Madsen:1999:NCO

Maes:1998:TPH
REFERENCES


(print), 1611-3349 (electronic).

Mao:1998:GCS


Marion:1995:WGT


Marks:1995:PEI


Markoff:1996:MIS


Martin:1997:IEI


REFERENCES

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

[Mat79]

[Mat91]

[Matsui:1993:LCM]

[Matsui:1994:FEC]
Matsui:1994:LCM


Matsui:1995:CBO


Matsui:1996:NSB


Matsui:1997:NBE


Matsumoto:1998:HCC


Matthews:1996:SRN

Matsumura:1999:DTE


Mauborgne:1914:APC


Maurer:1990:FGS


Maurer:1991:NAD


Maurer:1991:DSS


Maurer:1991:PCS


Maurer:1991:PSS

REFERENCES


CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).


URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390271.htm;

CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).

REFERENCES

openurl.asp?genre=issue&issn=0302-9743&volume=1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Maurer:1997:ITS


Sponsored by the International Association for Cryptologic Research (IACR).

Maurer:1998:E


Maurer:1999:IC


Maurer:1999:ITC


Maxemchuk:1994:EDD

N. F. Maxemchuk. Electronic document distribu-
REFERENCES

May:1997:CDS


Milner-Barry:1986:ADL

P. S. Milner-Barry. ‘Action This Day’: The letter from Bletchley Park cryptanalysts to the Prime Minister, 21 October 1941. Intelligence and National Security, 1(2):??, 1986. ISSN 0268-4527 (print), 1743-9019 (electronic).

Mao:1994:SAP


Massey:1994:CCT


Mehrotra:1999:NOA

Rajiv Mehrotra and Robin Baldwin. In the news: Online auctions attract buyers; xDSL reaches out and touches someone; business trends; Lucent delivers IP telephony; MP3: Dividing communities; the net attracts top musicians; service-level agreements reassure small businesses; digital signature for GSM phones; voice XML forum created. IEEE MultiMedia, 6(2):4–8, April–June 1999. CODEN IEMUE4. ISSN 1070-986X (print), 1941-0166
REFERENCES


REFERENCES


McHugh:1992:EBD


McIvor:1985:SC


McKee:1999:SFF


integer factoring algorithm that never requires arithmetic on numbers larger than the one to be factored.

McLaughlin:1992:YAM


McMahon:1996:RGA


Madson:1998:REC


Main:1999:HCB

J. Main and T. S. Dillon. A hybrid case-based reasoner for footwear design. Lecture
REFERENCES

Moreno-Diaz:1994:SIE

Messerges:1999:IPA

Meedor:1920:KCE

Meadows:1995:FVC

Mead:1998:BJA

Meek:1998:AAM

Meersman:1999:SOT
R. A. Meersman. Semantic ontology tools in IS design. Lecture Notes in Computer
REFERENCES

Science, 1609:30–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

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


Meierhofer:1996:PGP


Meijer:1996:GFC


Meinel:1998:HHB

Carolyn P. Meinel. How hackers break in . . . and how they are caught: Port scanners, core dumps and buffer overflows are but a few of the many weapons in every sophisticated hacker’s arsenal. still, no hacker is invincible. Scientific Amer-

Mendelsohn:1939:CC

Mendelsohn:1989:CWI

Mendez:1991:AKA

Menezes:1993:ECP

Menezes:1995:ECC

Menicocci:1995:SAC

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


REFERENCES

sis (Ph.D.—Stanford University, 1979).

Merkle:1988:DSB


Merkle:1989:CDS


Merkle:1991:FSE


McGraw:1997:UKJ


Murino:1995:RNU


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:1988:PQP


Matsumoto:1990:EAC

[Tsutomu:1990:EAC] Tsutomu Matsumoto and Hideki Imai. An efficient asymmetric cryptosystem supporting authenticity and confidentiality with public multivariate polynomial tu-
REFERENCES

Moulin:1999:ECG

Michener:1988:TSK

Micali:1993:FPC

Micali:1993:FPK

Micciancio:1997:ODS

Mihailescu:1994:FGP
Mihaljevic:1996:FCS


Millikin:1943:ECCa


Millikin:1943:ECCb


Millikin:1943:ECCc


Miller:1976:RHT


Miller:1985:PES


Miller:1986:UEC

REFERENCES

Millen:1987:CCC


Mills:1987:RDP


Millikin:1992:ECC


Miller:1995:HWK

Misarsky:1997:MAU


Misarsky:1998:HDR


Mitchell:1976:EAD


Mitchell:1989:MDS


Mitchell:1992:AMI


Mitchell:1992:CCI


Miyaguchi:1990:FCC


Miyaguchi:1991:FCF


Miyagi:1993:ECS


Miyagi:1993:OEC


Miyano:1993:MEN


Miyagi:1996:MRS


REFERENCES

Monge:1967:NMC

Maulucci:1987:HAC

Mao:1998:CPO

Matyas:1991:KSB

Muffett:1995:BPK

Matyas:1978:GDI

Meyer:1982:CND
REFERENCES

Moler:1983:SVA


Meadows:1987:MSA


Magliveras:1990:LCP


Magliveras:1990:PCP


Moskovitz:1992:CCC


Moskovitz:1992:IDI


Moskovitz:1994:STC

REFERENCES


Moldovyan:1995:FSE


Meadows:1996:CCC


Meyer:1996:PKC


Mueller:1998:SPK


Muller:1998:SPK


Marchignoli:1999:AVC

D. Marchignoli and F. Martinelli. Automatic verification of cryptographic protocols through compositional analysis techniques. Lecture Notes in Computer Sci-


[MRaihi:1997:XFO] David M'Raihi, David Naccache, Jacques Stern, and


Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi. A switching closure test
REFERENCES

616


**Montgomery:1985:MMT**


**Monagan:1993:GPD**


**Montagu:1996:MWN**


**Moore:1992:PFC**


**Morland:1666:NMC**


**Morrice:1692:EB**


**Morrison:1983:SEA**

D. R. Morrison. Subtractive encryptors: alternatives to the DES. *ACM*


REFERENCES

CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).


[Mosses:1999:CGT]

[Moura:1999:PAP]

[Mullin:1988:ONB]


[Mevis:1986:SCP]

[McInnes:1991:IPK]

[Milidiu:1999:EIW]

[Mayerwieser:1995:THS]
Wolfgang Mayerwieser, Karl C. Posch, Reinhard Posch, and Volker Schindler. Testing a high-speed data: Path


[MR98] Jeanette McLeod and Greg
REFERENCES


Mrakovcic:1995:EIN


Micali:1987:NSP


Micali:1988:NSP


Maitra:1999:COA


Mitchell:1989:RHF


Macalister:1976:SLI

REFERENCES


McEliece:1981:SSR


Muller-Schloer:1983:MBC


Moore:1987:CSK


Meier:1990:NCC


Montgomery:1990:FEP


Meier:1991:CPC

Meier:1993:EMC


Massey:1994:FTA


Meier:1995:SG


Meier:1995:SSG


Metzger:1995:RIAa


Metzger:1995:RIAb


REFERENCES

McLeod:1990:VLD


Miksch:1999:ASQ


Moriai:1998:HOD


Mizuki:1998:ESK


McClure:1999:HEN


Moriai:1999:IAB


Martin:1997:MAS


Mizuki:1999:DNS

[Takaaki Mizuki, Hiroki Shizuya, and Taka Nishizeki. Dealing necessary and sufficient numbers of cards]

**Martin:1999:BTE**


**Mambo:1996:HUT**


**Madonia:1999:BTE**


**Michels:1998:SSV**


**Meyer:1972:PCC**


**Mullender:1986:DCD**

REFERENCES

K. Matsui and K. Tanaka.


B. C. Massey and E. Tick.


R. Molva and G. Tsudik.


M. Matsui and T. Tokita.

REFERENCES


Mu:1992:ICS


Mu:1992:ICS

Mueller:1999:SRB


Mueller:1999:SRB

Muftic:1988:SMC


Muftic:1988:SMC

Muftic:1993:SAO


Muftic:1993:SAO

Mulherin:1981:FDE


Mulherin:1981:FDE

Mullin:1984:NMP


Mullin:1984:NMP

Mulligan:1989:UMA


Mulligan:1989:UMA

Mullin:1989:LEN

REFERENCES


\[ M_n(= 2^n - 1) \]

is the product of two distinct primes only if \( n \) is either a prime \( p \) or the square of a prime \( q \), in which case precisely one prime factor of \( M_n \) is Mersenne, vis. \( M_q \)."


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.

Musser:1992:UVE

Maruyama:1998:TGH

Menezes:1990:IEC

Menezes:1991:ACC

Meijers:1993:EMV

Menezes:1998:C


REFERENCES

Maurer:1996:DHO

Maurer:1997:PAS

MacNish:1998:BRD

Memon:1998:PDM

Merkle:1998:SSR

Merkle:1998:SSA

**Maurer:1999:RBB**


[MWB99]


[Malkin:1999:ESG]

**Malkin:1999:ESG**


[MY91]

**Maurer:1991:NIP**

[Ueli M. Maurer and Yaacov Yacobi. A remark on]

[MW99]

**Maurer:1999:RBB**


[MWB99]

**Malkin:1999:ESG**

[Matsui:1993:NMK]


[MY93a]

**Matsui:1993:NMK**

[Ueli M. Maurer and Yaacov Yacobi. A remark on]
REFERENCES

a non-interactive public-key distribution system. Lecture Notes in Computer Science, 658:458–??, 1993. CO-
link/service/series/0558/0658/papers/06580458.pdf.

D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In IEEE [IEE98a],
pages 503–509. CODEN ASFPDV. ISBN 0-8186-
9172-7 (softbound), 0-7803-
5229-7 (casebound), 0-
8186-9174-3 (microfiche).
ISSN 0272-5428. LCCN QA267 .S95 1998 Sci-


 REFERENCES

 selected papers from issues of Cryptologia.


David Naccache. A Montgomery-suitable Fiat–Shamir-like authentication
REFERENCES


Nachenberg:1997:CVA


Naik:1989:CDS


Nalwa:1997:AOS


NBS:1977:DES


Nanovic:1936:SWI


Nastar:1994:VMN


NBS:1977:DES


REFERENCES

NIST:1993:FPD


Anonymous:1993:FPD


NIST:1993:DES


NIST:1994:FPD


NIST:1994:DES


NIST:1994:DSS


NIST:1994:EES


NIST:1999:SAC

NIST:1999:SRF

NBS:1975:EAC
NBS. Encryption algorithm for computer data protection: requests for comments. Federal Register, 40(?):12134–??, March 17, 1975. CODEN FEREAC. ISSN 0097-6326.

NBS:1975:NPF
NBS. Notice of a proposed federal information process-

**NBS:1976:NWC**


**Nilsson:1978:OST**


**Nandi:1997:RCT**


**Neat:1975:NCC**


**Nechvatal:1991:PC**


**Nechvatal:1996:PKB**


**Needham:1994:DSE**

References


REFERENCES


Neve:1999:FSC


Ng:1999:CST


Nguyen:1999:CGC


Nguyen:1999:CGG


Nelson:1990:SAE


Neubauer:1998:DW1


REFERENCES

Nissan:1991:EMF


NIST:1992:NCS


NIST:1993:DSS

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

NIST:1993:FPS


Anonymous:1994:DSS


Nisan:1996:ERH


Nyberg:1993:PSA


Nakamura:1998:MEC


Nikander:1998:JBC

Pekka Nikander and Arto Karila. A Java beans component architecture for
REFERENCES

cryptographic protocols. In USENIX [USE98d], page ??.

Nandi:1994:TAC


Nikander:1999:PPD


Naccache:1994:MSC


Naccache:1996:ACP


Naccache:1996:CSC

REFERENCES

Nadathur:1999:SDT


Naccache:1995:CMP


Naccache:1995:CDB


Nguyen:1998:NDC

REFERENCES


REFERENCES

Niemi:1994:CPV


Nyberg:1995:MRS


Naor:1998:UIS


Neuman:1988:AUE


Norris-Saucedo:1989:DAD

[NS89] Steven Joseph Norris-Saucedo. Development and application of data encryption using a data shuffling technique. Thesis (M.S.), Department of Electrical Engi-
REFERENCES


[NS98c] P. Nguyen and J. Stern. The Beguin-Quisquater server-
aided RSA protocol from Crypto'95 is not secure. Lecture Notes in Computer Science, 1514:372–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Nguyen:1998:CAD


Nguyen:1999:CAC


Nguyen:1999:HHS


Naccache:1999:HCF


Nieh:1993:MAC


Neuman:1994:KAS

Nadjm-Tehrani:1999:BHO


Nemetz:1988:RLS


Nurmi:1994:CPA


Needham:1997:TE


Naor:1998:ACS


Naor:1989:UOW


Naor:1989:UOH

Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In ACM-TOC’89 [ACM89c], pages 33–43. ISBN 0-89791-
REFERENCES


Naor:1990:PKC

Nyberg:1994:DUM

Nyberg:1995:LAB

Nyberg:1998:ACE

Nystrom:1999:PCT

Ohta:1994:LCF
REFERENCES


Martin Oberzalek. *genigma*: Enigma emulator. GPL-licensed software., 1999. URL [http://home.pages.at/kingleo/genigma-1.2.tar.gz](http://home.pages.at/kingleo/genigma-1.2.tar.gz);


Odlyzko:1984:CAM


Odlyzko:1985:DLF


Odlyzko:1987:CCD


Odlyzko:1987:ACC

REFERENCES


REFERENCES


[Oht96] Naohisa Ohta, editor. Digital compression technologies and systems for video


Okamoto:1988:DMS


Okamoto:1993:RAC


Okamoto:1993:PSP


Okamoto:1994:DCS


Okamoto:1998:TKR


Okamoto:1998:TKS


Okon:1996:DWN

Chris Okon. Digital watermarking: New techniques

**Okon:1997:KMA**


**Ogata:1997:FTA**


**Ogata:1993:NSS**


**Oleshchuk:1995:PKC**


**Oldehoeft:1984:SSU**


**Ohta:1994:DAM**


**Ohbuchi:1997:WTP**

Ryutaro Ohbuchi, Hiroshi Masuda, and Masaki Aono. Watermarking three-dimensional polygonal mod-


Ohta:1993:DMS


Ohta:1998:CST


Ohta:1991:MAH


ORuanaidh:1997:RST


ORuanaidh:1998:RST

REFERENCES

ORuanaidh:1999:CCP


[OR87]

Oppliger:1996:ASS


[Org98]

OECD:1998:OEM


[Org98b]

OECD:1998:CPG

REFERENCES


REFERENCES


**Olejar:1998:CPR**


**Orup:1991:VER**


**Ong:1991:TCM**


**Ong:1985:ESS**


**Okamoto:1998:NPK**

Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. *Lecture
REFERENCES


nal 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.


<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Par85</td>
<td>Aiyawamy Parthasarathy. Digital signature generator</td>
</tr>
</tbody>
</table>
Parker:1996:RCG


Parent:1998:ALM


Parker:1998:UMP


Parrish:1998:RMM


Patterson:1987:MCC


Patarin:1991:PPB


Patarin:1991:NRP

Patarin:1995:CMI


Patarin:1996:ACH


Paterson:1999:IPG


Paulson:1998:IAV


Paulson:1999:IAI


Poovendran:1999:ITA


Proctor:1999:PC

REFERENCES


Pizzonia:1999:OOD


Popovic:1999:DIT


Plagge:1999:DET


Pearcey:1980:EDS


Peke:1997:OVD


Pedersen:1991:DPA


Pedersen:1991:NIS

**Pedersen:1991:TCT**

**Pedersen:1991:NIT**

**Pedersen:1995:EPS**

**Pedersen:1999:SCP**

**Pelta:1960:SP**
Penzhorn:1996:CAS


Perret:1890:RCS


Peralta:1985:TRN


Perry:1988:EBG


Perry:1991:EIT


Peralta:1993:QSD


Perrig:1997:CPE

REFERENCES


REFERENCES


REFERENCES

| Preneel:1993:IAH | B. Preneel, R. Govaerts, and J. Vandewalle. Information authentication:
REFERENCES


Preneel:1993:CSI


PH91


Preneel:1994:HFB


PHF99


Phillips:1998:SHI

REFERENCES

DEN CCUJEX. ISSN 1075-2838.

**Piecher:1986:ACE**

**Piecher:1998:E**

**Piecher:1998:SSP**

**Pieper:1993:CRD**

**Pieper:1997:UCN**

**Piner:1998:CUW**
REFERENCES

Pitas:1995:PIW

Pitas:1996:MSC

Pitoura:1996:RSS

Price:1999:IAV


Panneerselvam:1990:RSA

Popek:1979:ESC

Penzhorn:1995:CLP

Popek:1979:ESC


Penzhorn:1995:CLW


Praehofer:1999:SRS


Pamplona:1998:LVC


Postma:1997:DCF


Park:1994:KDA


Petrounias:1994:RBA

Pless:1975:ESC


Pless:1977:ESC


Plimmer:1998:MIW


Plumstead:1983:ISP


Pei:1999:COA


Payne:1978:OEN


[Bart Preneel, Marnix Nuttin, Vincent Rijmen, and Johan Buelens. Cryptanalysis of the CFB mode of the DES with a reduced number of rounds. Lecture Notes in Computer Science, 773:212–??, 1994. CODEN

References
REFERENCES

[685]

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


[Pollard:1978:MCM]


[Pollard:1974:TFP]

[Pomerance:1988:ACC]


[Pomerance:1990:CCNa]

number theory, held in Boulder, Colorado, August 6–7, 1989.


Porter:1984:CNS


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT


Posch:1992:TMD


Posch:1993:PFP


Posch:1998:MPC


Posch:1989:AEA

K. C. Posch and R. Posch. Approaching encryption at ISDN speed using partial
parallel modulus multiplication. IIG report 276, Institutes for Information Processing Graz, Graz, Austria, November 1989. 9 pp.

Pfitzmann:1990:HBD


Posch:1992:MRR


Posch:1995:MRRa


Posch:1995:MRRb


Posch:1992:SNN

Algirdas Pakstas and Sonata Pakstiene. Standards: NSK: A Norwegian cryptochip for supersafe com-

**Pedersen:1997:FSS**


**Park:1997:TER**


**Peleg:1979:BSC**


**Pieprzyk:1985:DPK**


**Pieprzyk:1985:MDI**


**Preneel:1998:SAA**

REFERENCES

Pratt:1939:SUS

Pratt:1996:SUS

Parra:1998:MPS

Preneel:1998:RDD

Preneel:1998:AAP

Preneel:1993:SCT

Preneel:1993:ADC

Preneel:1994:CHF
Bart Preneel. Cryptographic hash functions. European transactions on
REFERENCES

Prenel:1994:CHF


Preneel:1995:FSE


Preneel:1995:EFC


Preneel:1997:HFM


PGP:1997:PGPa


PGP:1997:PGPb


Preneel:1998:CMA


Preneel:1998:IC

Preneel:1998:CPI


Preneel:1999:SCH


Pritchard:1980:DE


Price:1983:ABR


Price:1994:MVC


Pronzini:1980:MCC

A. The eagle-claw rattle.—Grant, C.L. The other room.—Malzberg, B.N. Revelation in seven stages.—Bibliography.

**Proctor:1985:SSC**


**Patel:1999:TML**


**Peyravian:1999:HBE**


**Paun:1993:CPS**


**Pieprzyk:1993:DHA**


**Pfitzmann:1996:AF**

B. Pfitzmann and M. Schunter. Asymmetric fingerprinting. In Maurer [Mau96b], pages
REFERENCES


Patiyoot:1999:MES

Patiyoot:1999:WSS

Patiyoot:1999:SIA

Patiyoot:1999:CST

Patiyoot:1999:WWA

Pfenning:1999:SDT

Patel:1997:UDB

Pieprzyk:1991:RAS
Józef P. Pieprzyk and Reihaneh Safavi-Naini. Ran-
Pieprzyk:1995:PA


Pieprzyk:1995:ACA


Paar:1997:FAA


Pomerance:1988:PAF

Pomerance:1980:P


Pfitzmann:1995:HBA


Phoenix:1995:QCP


Parkes:1999:ACC


Purdy:1974:HSL


Puteanus:1627:EPC


Preparata:1990:PCD

Peinado:1997:HPC


Posegga:1998:BCV


Pluimakers:1986:ACS


Preneel:1995:MMB


Preneel:1996:STM

REFERENCES

with the University of Saragossa.


REFERENCES


[PWU99] Christine I. Podilchuk and Wenjun Zeng. Image-

Quisquater:1998:CSE


Quisquater:1991:CLE


Quisquater:1989:BHF


Quisquater:1990:BHF


Quisquater:1995:ACE


REFERENCES


Quisquater:1998:E


Rabin:1977:DS


Rabin:1981:HES


Rabin:1989:EDI


Rabin:1994:RSS


Rabin:1998:SAT


Ratcliff:1996:DIN


Rhodes-Burke:1982:RSA


Rabin:1989:VSS


Reiter:1994:SAF


**Rogaway:1994:SEA**


**Rogaway:1994:SOE**


**Russinovich:1995:EWS**


**Rubia:1999:RIB**


**Renvall:1996:ASS**


**Renvall:1996:NSS**


**Roback:1999:CRF**


REFERENCES


[Rejxx] Marian Rejewski. Enigma

**Revello:1991:CEC**


**Reynard:1996:SCB**


**Reynard:1997:SCB**


**Reynard:1999:SCB**


**Reiter:1995:SCR**


**Reiter:1996:KMS**


**Rowlett:1935:FAP**


Radu:1997:WHR


Rubin:1993:LRJ


Ryu:1999:PAA


Rivest:1992:RNP


Rhee:1993:CSC


Rhee:1994:SMA


Rhoads:1995:SMA

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

Rihaczek:1987:T

Rijmen:1999:WL

Riley:1996:LET
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 DTNAT. ISSN 0011-6963.

Ripe:1995:IPS

Ripe:1995:RIP

Ritter:1999:IWC
Terry Ritter. Internet watch: Cryptography: Is staying with the herd really best? Computer, 32(8):94–95, August 1999. CODEN CPTRB4. ISSN 0018-
REFERENCES


[Riv85] Ronald L. Rivest. RSA chips (past/present/future). In Beth et al. [BCI85], pages 159–163. CODEN
REFERENCES


REFERENCES


REFERENCES


[Riv98c] Ronald L. Rivest. Chaffing and winnowing: Confidentiality without encryp-
REFERENCES

Rivest:19xx:PC

R. Rivest. Personal communication. ???, 19xx.

Rhodes:1993:ZF


Rijmen:1998:WL


Rowlett:1998:SMM


Roy:1999:QCE


Rosenson:1994:GWE


Ruanaidh:1996:WDI


Reeds:1985:NPR

J. A. Reeds and J. L. Manferdelli. DES has no per round linear factors. In Blakley and


D. W. Roberts. Security management — the process. Lecture Notes in
REFERENCES

Robinson:1998:FRC

Roe:1994:PSC

Roe:1995:PBC

Roe:1999:CWD

Rogaway:1995:BHA

Rogaway:1996:SD

Rohwer:1975:GIM
REFERENCES

ISBN 3-87943-383-6. 356 pp. LCCN ????. See also English translation [Roh77].

Rohwer:1977:CCB


Rohatgi:1999:CNR


Roman:1990:C


Rompel:1990:OWF


Rose:1993:RCM


Rosen:1994:EMT


Rosen:1995:PPZ

[Ros95b] Greg Rose. Status update on PGP and legal actions. 


REFERENCES


[Rotenberg:1995:ECP]


[Rotenberg:1995:ELD]

REFERENCES

Rothke:1997:WED


Routh:1984:PAA


Roy:1986:CBI

[Roy86] Marc Paul Roy. A CMOS bit-slice implementation of the RSA public key encryption algorithm. Thesis (M.Sc.(Eng.)), Queen’s University, Ottawa, ON, Canada, 1986. 3 microfiches (210 fr.).

Redding:1994:LPF


Rijmen:1995:CM


Rijmen:1995:ICD


Rijmen:1997:FTC


Rogowitz:1997:HVE

[RP97b] Bernice E. Rogowitz and Thrasyvoulos N. Pappas, editors. Human vision and
REFERENCES


Rivest:1996:PMTa


Rivest:1996:PMTb


Reiter:1998:RAU


Riordan:1998:CMP


Riordan:1998:EKGa


Riordan:1998:EKGb


the Association for Computing Machinery, 21(2): 120–126, February 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). The basics of trap-door functions and the famous RSA public key cryptosystem are presented in this paper.


RSA Laboratories. PKCS #8: Private-Key Information Syntax Standard. RSA Data Security, Inc.,

RSA Laboratories: 1993: PKC


RSA: 1994: MPK


RSA: 1999: PVPb


RSA: 1999: PVPa


T. M. Raleigh and R. W. Underwood. CRACK: a
REFERENCES

730

Rubin:1979:DSC


Rudolph:1982:HTI


Rudich:1991:UIP


Rueppel:1993:ACE


Rueppel:1998:E


Ruggiu:1985:CCT

G. Ruggiu. Cryptol-
ogy and complexity theories. In Beth et al. [BCI85], pages 3–9. CO-
DEN LNCSD9. ISBN 0-
387-16076-0 (USA). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/0558/tocs/t0209.htm;
http://www.springerlink.
com/openurl.asp?genre=
issue&issn=0302-9743&
volume=209. Held at the
University of Paris, Sor-
bonne.

Ruohonen:1994:EDO

K. Ruohonen. Event detec-
tion for ODEs and nonre-
cursive hierarchies. Lecture
Notes in Computer Science,
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Russel:1927:CMS

Henry Norris Russell. Ci-
pher messages of the stars.
Scientific American, 137
(2):118–119, August 1927.
CODEN SCAMAC. ISSN
0036-8733 (print), 1946-
7087 (electronic). URL
http://www.nature.com/
scientificamerican/journal/
v137/n2/pdf/scientificamerican0827-
118.pdf.

Russell:1990:HLS

D. Russel. High-level se-
curity architecture and the
Kerberos system. Computer
Networks and ISDN Sys-
CODEN CNISE9. ISSN
0169-7552 (print), 1879-
2324 (electronic).

Ruskey:1993:SCG

F. Ruskey. Simple combi-
natorial gray codes con-
built by reversing sub-
lists. Lecture Notes in Com-
puter Science, 762:201–208,
ISSN 0302-9743 (print),
1611-3349 (electronic).

Russell:1993:NSC

A. Y. Russell. Necessary
and sufficient conditions for
collision-free hashing. Lecture
Notes in Computer Science,
740:433–441, 1993. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Roychowdhury:1999:ENQ

V. P. Roychowdhury and
F. Vatan. On the exis-
tence of nonadditive quan-
tum codes. Lecture Notes
in Computer Science, 1509:
325–336, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Reeds:1984:FSU

James A. Reeds and Pe-
ter J. Weinberger. File se-
curity and the UNIX system
crypt command. ATT Bell
REFERENCES


Robshaw:1997:ECC


Rytter:1986:SCU


Ras:1999:DES


S:1873:COD


Schiller:1995:SWT


Sabourin:1994:CCP

Sacco:1936:MC

Luigi Sacco. *Manuale di crittografia*. (Italian) [Manua
of cryptography]. Tipografia Santa Barbara, Roma, Italia, sec

Sacco:1947:MC

Luigi Sacco. *Manuale di
crittografia*. (Italian) [Manu
al of cryptography]. Istituto Polygrafico Dello Stato, Roma, Italia, third edi
tion, 1947. xii + 374 pp.

Sacco:1951:MCF

Luigi Sacco. * Manuel

Sacco:1977:MC

Luigi Sacco. *Manual of

Sahai:1999:NMN

A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-

Saks:1989:RNP


Sakurai:1996:HCA

K. Sakurai. A hidden cryptog
raphic assumption in non-

Sakurai:1997:PPK

REFERENCES

Saltzer:1973:PCI

Saltzer:1978:DS

Salomaa:1985:PKC

Salomaa:1988:PKC

Salomaa:1990:PC

Salomaa:1991:VRS

Sale:1993:EBP

Salomaa:1996:PC
Arto Salomaa. Public-key cryptography. Texts in theoretical computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
REFERENCES


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


Savarnejad:1996:COF


Savarnejad:1997:GAD

[Atoosa Savarnejad]. Group asks for disclosure of travel

Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Sorkin:1984:MCC


Smid:1992:DES


Smid:1993:RCN


Shepherd:1994:UBS

Shepherd:1995:CNL


Schneier:1997:EPP


Shi:1998:FMV


Soto:1999:RTA


Serpell:1985:PES


REFERENCES


Schneider:1996:RCB


Schneider:19xx:DWI


Scacchitti:1986:CT


Styner:1999:BMD


Schwenter:1620:SSN

Daniel Schwenter. Steganologia & steganographia nova:
REFERENCES

Geheime magische, natürliche Red und Schreibkunst, einem in der nahe und ferne Alsbalden oder in gewisser Zeit, so woln in Schimpff als Ernst, etwas verborgens vnnd geheimes zu eröffnen durch Reden, Schreiben und mancherley Instrumenta: item wie verborgene Schrifften zu machen, auffzulosen, und mit sonderlichen Kunst zu schreiben. Resene Gibronte Runeclus Hanedi, Nürnberg, Germany, 1620. 16 + 299 + 5 pp. LCCN KK276 .E36 1575; Z103.5. Publication year uncertain. Publicirt vnnd an Tag gegeben durch Resene Gibronte Runeclus Hanedi ... Nurnberg: Inn Verlegung Simon Halbmayers.


REFERENCES


REFERENCES


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.

Schneier:1991:FHE


Schifreen:1992:PPD


Schneier:1992:SSA


Schneier:1992:UPC


Schilling:1993:MBC


Schneier:1993:SCD

DEN CSJLDR. ISSN 0277-0865. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/031624.html

Schneier:1993:DS

Schneier:1993:IEA

Schneier:1993:UHD

Schneier:1993:FHI

Schnorr:1993:FIE

Schiller:1994:SDC

Schneier:1994:DNV

Schneier:1994:DEA
IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, August 1994. ISBN ????. LCCN ????.


[Sch94l] Bruce Schneier. *Protect Your Macintosh*. Peachpit Press, Inc., 1085 Keith Avenue, Berkeley, CA 94708,

**Schneier:1994:RDS**


**Schneier:1995:AAB**


**Schneier:1995:AAG**


**Schneier:1995:MS**


**Schneier:1995:OPE**


**Schneier:1995:PCC**


**Schneier:1996:ACP**

REFERENCES


Stephen Schlesinger. Crypt-
REFERENCES


Schmalz:1998:MDI


Schneier:1998:CDV


Schneier:1998:CTS


Schneier:1998:SPC

REFERENCES


Schmidt:1999:RER


Schneier:1999:SSC


Schneier:1999:IRT


Schneier:1999:IRU


Schneier:1999:IWC

Schoenmakers:1999:SPV


Schoenmakers:1999:SPV

Schroeder:1999:SEA


Schumann:1999:PST


Scerri:1999:UOS


Scudder:1992:OLA


Smith:1986:GCC


Silvestre:1997:IWU

Schouten:1999:FEU


Sicherman:1983:AQR


Smillie:1986:RWA


Schwenk:1996:PKE


Seaton:1956:THS

Sears:1986:SWK


Seachrist:1995:DIM


Sedlak:1988:RCP


Sedgewick:1992:AC


Sedgewick:1993:AM


Seeley:1989:PCG


0558/papers/1267/12670114.pdf.


REFERENCES


REFERENCES

Sun:1994:KGA


Schnorr:1995:ACC


Schnorr:1995:ACR


Shannon:1945:MTC


Shannon:1948:MTCa

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

Shamir:1985:IBC

Shamir:1987:CSS

Sharp:1988:DCO

Sharp:1994:ESS

Shamir:1995:MEV
REFERENCES


Supervised by Ronald Linn Rivest.


Shepherd:1992:SIR

Sherrod:1992:DES

Shepherd:1993:ACCa

Shepherd:1993:ACCb

Shepherd:1993:EOS

Shepherd:1993:WNS

Shepherd:1994:ACM

Shepherd:1994:CGA
S. J. Shepherd. Cryptanalysis of the GSM A5 cipher algorithm. In *IEE Colloquium on Security and Cryptography Applications to Ra-
ISBN ???, LCCN ???
Commercial-in-confidence.


ISBN ???, LCCN ???

ISBN ???, LCCN ???


ISBN ???, LCCN ???
REFERENCES


Wayne Shumaker. *Renaissance curiosa: John Dee’s conversations with angels, Girolamo Cardano’s horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno’s Universal language*, volume 8 of *Medieval and Renaissance texts and studies*. Center for Medieval and


REFERENCES


[Sil99] Robert D. Silverman. Exposing the mythical MIPS year. Computer, 32(8):
REFERENCES


Simonetta:1404:LTC

Cicco Simonetta. [Little tract on cryptanalysis]. ?????, ?????, 1404. ???? pp.

Simmons:1979:HID


Simmons:1979:CCA


Simmons:1979:SAE


Simmons:1982:SAC


Simmons:1982:SAE


Simmons:1983:PPS

Simmons:1984:HID


Simmons:1985:ATC


Simmons:1985:SCD


Simmons:1988:SSC


Simmons:1990:HRS


Simmons:1990:PSS

Gustavus J. Simmons. Prepositioned shared secret and/or shared control

Simmons:1991:GSS


Simmons:1992:CCS


Simmons:1993:SCU


Simmons:1994:CTS


Simmons:1994:CPF

Simmons:1994:SCP


Simmons:1994:SCE


Simovits:1995:EDE


Simmons:1996:HSC


Simmons:1997:SCS


Simmons:1998:HSC

G. J. Simmons. The history of subliminal channels. IEEE Journal on Selected Areas in Communications,
REFERENCES


[Sin85] Kamaljit Singh. On improvements to password se-


Sako:1995:RFM


Schneier:1996:AOC


Schneier:1996:PPSa


Schneier:1996:UFSNa

REFERENCES


**Shimoyama:1998:QRS**


**Shimoyama:1998:QRB**


**Schneier:1999:SAL**


**Stabell-Kulo:1999:PAM**


**Shepherd:1997:EKE**


**Schell:19xx:CMC**


**Sorokine:1994:TBD**

V. Sorokine, F. R. Kschischang, and V. Durand.


REFERENCES


Schneier:1998:TBBb


Schneier:1998:TSC


Schneier:1998:TBE


Schneier:1998:TNB


Schneier:1999:PCAa


Schneier:1999:PCAb

[SKW+99b] B. Schneier, J. Kelsey, D. Whiting, D. Wagner,
C. Hall, and N. Ferguson. Performance comparison of the AES submissions. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ????? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/conf2/Schneier.pdf. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

[SKW+99c] Schneier:1999:APC


[SKW99] Schneier:1999:NRT


Schneier:1999:TEAb


Schneier:1996:AC


Schneier:1999:TKS

B. Schneier, J. Kelsey, D. Whiting, and D. Wagner.

**Sufatrio:1999:IMS**


**Slutsky:1998:KDQ**


**Schobi:1983:FAT**


**Siromoney:1990:PKC**


**Staffelbach:1991:CSC**


**Schubert:1995:MLS**


**Syverson:1995:FRK**

REFERENCES

1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sklower:1996:RPE


Schneier:1998:CMP


Smart:1999:PHC


Schneier:1999:DDE

Dobb’s CD-ROM library. Miller Freeman Publica-
[Sm71a]tions, San Francisco, CA, USA, 1999. LCCN
QA76.9.A25 D7 1999 Interactive Learning Center.
Books on CD-ROM.

[Sm97] Denise Smejkal. Data encryp-
[Sm71b]tion and the Internet. Thesis (Honors), University

[Sm43] Laurence Dwight Smith. Cryptography, the science
of secret writing. W. W. Norton & Co., New York, NY,
USA, 1943. 164 pp. LCCN Z104 .S5.

[Sm44] Laurence Dwight Smith. Cryptography, the science
of secret writing. G. Allen and Unwin, London, UK,
1944. 164 pp. LCCN Z104 .S5.

[Sm55] Laurence Dwight Smith. Cryptography; the science of
secret writing. Dover Publications, Inc., New York,
unabridged republication of the first edition with correc-
tions.”.

[Sm71c] J. L. Smith. The design of Lucifer, a cryptographic
device for data communications. Research Report
RC-3326, IBM T. J. Watson Research Center, Yorktown
Heights, NY, USA, 1971.

[Sm71d] Laurence Dwight Smith. Cryptography, the science
of secret writing. Dover Publications, Inc., New York,
LCCN Z 104 S65c 1971. “This Dover edition, first
published in 1955, is an unabridged and corrected
republication of the work originally published by W.
W. Norton and Company in 1943.” “Copyright re-

[Sm74] J. L. Smith. Recirculating block cipher cryptographic

[Sm83] John Smith. Public key cryptography: An introduc-
tion to a powerful cryptographic system for use on
microcomputers. BYTE Magazine, 7(??):198–218,
January 1983. CODEN BYTEDJ. ISSN 0360-5280.
This is a simple exposition of public key cryptography.

Smith:1987:AUW


Smith:1990:PPC


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


Stakhov:1999:IFC


Safavi-Naini:1993:FTA


Shepherd:1994:VFH


Safavi-Naini:1996:TSS

REFERENCES

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

Smith:1972:EAC


Steiner:1988:KAS


Safavi-Naini:1993:ACU


Safavi-Naini:1995:ACP


Safavi-Naini:1998:BCM


Safavi-Naini:1998:NRM


Snyder:1979:IUC

Samuel S. Snyder. Influence of U.S. Cryptologic Organizations on the digital com-


REFERENCES


REFERENCES


Sakurai:1995:RAC


Smith:1995:PCD


Smith:1995:PKC


Sandhu:1996:AAC


Silverman:1997:CAX


Sakai:1998:DHC


Sun:1998:PKC

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


W. Susilo, R. Safavi-Naini, and J. Pieprzyk. Fail-stop threshold signature schemes based on elliptic curves. *Lecture Notes in
REFERENCES

Shepherd:1990:CSS

Schmidt:1998:LOA

Salter:1998:TSS

Schneier:1998:DDE

StJohns:1984:RAS

StJohns:1985:RAS
REFERENCES


Shawe-Taylor:1989:BRB


Stern:1991:CPK


Stark:1970:INT

[Sta70] Harold M. Stark. *An introduction to number the-


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).


REFERENCES

Stallings:1996:PCI

Staddon:1997:CSC

Stallman:1997:SDR

Stark:1997:ESP

Stallings:1999:CNS

Stallings:1999:HAK

Stevenson:1976:MCI
William Stevenson. A man
REFERENCES


REFERENCES


Stinson:1991:CCA


Stinson:1991:UHA


Stinson:1993:NGL


Stinson:1993:ACC


Stinson:1994:ACC

REFERENCES


Sivabalan:1993:DSN


Stripp:1987:BJC


Stripp:1989:CFE


Strauss:1993:SEC


Sander:1999:AAE


Sandholm:1999:DOC

Stumme:1999:AEK


Steiner:1995:REE


Su:1998:DEM


Sun:1991a


Sun:1991b


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 [SV93]

Schnorr:1994:BBC [SV94]

Schnorr:1995:BBC [SV95a]

Shepherd:1995:GJ [SV95b]

Stern:1998:CC [SV98]

Shamir:1999:PHS [SV99a]

Shamir:1999:PSS [SV99b]
REFERENCES

**Samuels:1998:LSA**

[SvA+98] 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 PCs; server-side scripting; stronger encryption; inner loops; Einstein kudos. *Dr. Dobb’s Journal of Software Tools*, 23(3):8, 12, March 1998. CODEN DDJOEB. ISSN 1044-789X.

**Sivakumar:1999:PPN**


**Shepherd:1996:SAD**


**Shamir:1998:PHS**


**Shepherd:1995:SCS**


**Smeets:1991:CAC**


REFERENCES

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

**Swire:1997:ULF**


**Salzer:1981:RHH**


**Sun:1990:KGE**


**Salomaa:1986:PCB**


**Salomaa:1986:PKC**


**Smith:1992:ICF**

REFERENCES

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


REFERENCES

**Syverson:1993:KDP**


**Seberry:1993:ACA**


**Sakurai:1996:CWR**


**Szepietowski:1998:WSO**


**Swanson:1996:RDH**


**Swanson:1996:TRI**

REFERENCES

ac.uk/~fapp2/steganography/ bibliography/1037.html.
Three volumes. IEEE cata-
log number 96CH35919.

Swanson:1998:MSB  [Szw97a]
M. D. Swanson, B. Zhu,
and Ahmed H. Tewfik. Multires-
olution scene-based video
watermarking using perceptual
models. IEEE Journal on Selected
Areas in Communications, 16(4):
540–550, May 1998. CO-
DEN ISACEM. ISSN
0733-8716 (print), 1558-
0008 (electronic). URL
http://www.cl.cam.ac.
uk/~fapp2/steganography/
bibliography/072157.html.

Swanson:1998:MSV  [Szw97b]
Mitchell D. Swanson, Bin
Zhu, and Ahmed H. Tew-
fik. Multiresolution scene-
based video watermarking
using perceptual models.
IEEE Journal on Selected
Areas in Communications,
CODEN ISACEM. ISSN
0733-8716 (print), 1558-
0008 (electronic).

Swanson:1998:RAW  [Szw97c]
M. D. Swanson, B. Zhu,
Robust audio watermarking
using perceptual mask-
ing. Signal Process-
inging, 66(3):337–355, May
1998. CODEN SPRODR.
ISSN 0165-1684. URL
http://www.cl.cam.ac.
uk/~fapp2/steganography/
bibliography/073173.html.

Szweda:1997:ECF  [Szw97a]
Roy Szweda. Encrypted
communications frustrate
FBI. Network Security, 1997(10):
4, October 1997. CODEN NTSCF5.
ISSN 1353-4858 (print), 1872-
9371 (electronic). URL
com/science/article/pii/
S1353485897900994.

Szweda:1997:ESW  [Szw97b]
Roy Szweda. Encryption
software for Windows.
Network Security, 1997(7):
8, July 1997. CODEN
NTSCF5. ISSN 1353-4858
(print), 1872-9371 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485897898777.

Szweda:1997:STF  [Szw97c]
Roy Szweda. Sun takes
on Feds over US encryp-
tion regulations. Network
Security, 1997(7):
6, July 1997. CODEN
NTSCF5. ISSN 1353-4858
(print), 1872-9371 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485897898704.

Seberry:1994:ISA  [SZZ94a]
Jennifer Seberry, Xian Mo
Zhang, and Yuliang Zheng.
Improving the strict avalanche
REFERENCES


**Seberry:1994:PDS**


**Seberry:1995:RAN**


**Seberry:1995:SCF**


**Seberry:1995:RBP**


**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 ??.

**Tardo:1992:SGA**


**Tang:1997:DBC**


**Taaffe:1998:NBL**


**Tabatabaian:1994:CAP**


**Takagi:1997:FRT**


**Takagi:1998:FRC**


**Takagi:1998:FRT**


Laura Mignon Taylor. *Data security issues and encryption algorithms.* Thesis
REFERENCES


REFERENCES


Tanaka:1999:PCD


Tzeng:1999:IPI


Thao:1991:SAD


Theobald:1995:HBS


Thomas:1974:RPS


Thompson:1984:RTT


Thomas:1986:SDE

Thompson:1987:RTT


Thomas:1996:PVS


Tarman:1998:AAE


Tsujii:1988:PKC


Tilki:1998:EHD


Tippett:1927:RSN


Taaffe:1997:NSL


Tseng:1999:ATS


**Takagi:1999:DRA**


**Tzovaras:1998:RIW**


**Theodoratos:1999:DGD**


**Tavares:1999:SAC**


**Takagi:1996:MMP**


**Takagi:1996:MVM**

T. Takagi and S. Naito. The multi-variable modul-


REFERENCES

Toussaint:1993:FVP

Tsunoo:1994:COA

Touch:1995:RRM

Tow98

Thompson:1963:SDE

Traore:1997:MUF

Traore:1999:GST
REFERENCES

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

**Tremblett:1999:JPA**


**Trithemius:1518:PLS**


**Trithemius:1606:CGT**


**Trithemius:1606:CSI**


**Trithemius:1606:SHE**

Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendii certa*. Mat-thiae Beckeri, Frankfurt, Germany, 1606. 8 + 180 pp. LCCN Z103.T84 S 1606. Authore ... Ioanne Trithemio ... praeax est huic operi sua clauis, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Francofurt. Ex officina typographica Matthiae Beckeri, sumptibus Ioannis Berneri, anno 1606.

**Trithemius:1621:CGT**

Johannes Trithemius. *Clauis generalis triplex in libros steganographicos Iohannis Trithemij ... Balthasar Hofmann, Darmstadt, Germany, 1621. 7 + 1 pp. LCCN Z103.T84 S 1621. Ab ipso authore conscripta ... Darmbstadij. Excudebat Balthasar Hofmann, impen-
sis Iohannis Berneri, bibliop. Francof., anno 1621.

**Trithemius:1621:CSI**


**Trithemius:1621:SHE**

Johannes Trithemius. *Steganographia: hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa.* Balthasaris Aulaeandi, Darmstadt, Germany, 1621. 8 + 152 + 2 pp. LCCN Z103 .T84 1621. *Authore ... Iohanne Trithemio ...; praefixa est huic operi sua claus, seu vera introductio ab ipso authore concinnata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta.* Darmbstadij. Ex officina typographica Balthasaris Aulaeandi, sumptibus vero Iohannis Berneri, bibliop. Francof., anno 1621.

**Trostle:1993:MFT**


**Tronson:1997:C**


**Tirkel:1993:EW**


**Terry:1988:MSV**

Tso:1990:NPK


Tso:1997:MEE


Tombak:1993:ACP


Tsudik:1989:DAI


Tsudik:1992:MAOb


Tsudik:1992:MAOa

REFERENCES

Tsujii:1992:CS


Thomlinson:1998:NBP


Thersites:1984:IKE


Thomas:1984:IKE


Tiountchik:1999:RAF


Tual:1999:MGA


Tuchman:1966:ZT

scribes this book as “recount[ing] the political effects of the most important cryptogram solution in history”.

Tuckerman:1970:SVV


Tuchman:1979:HPN


Tuchman:1979:IHP


Tung:1999:KNA


Turing:1941:APC


Turing:1941:SR


Turing:1999:TTE

Alan Turing. Turing’s treatise on Enigma. Technical report, CERN, Geneva, Switzerland, 1999. URL http://home.cern.ch/~frode/crypto/Turing/index.html. This document is reyped from the original (undated??) Turing typescript by the editors Ralph Erskine, Philip Marks and Frode...
REFERENCES

Weierud. Chapters 1, 2, and 6 (of 8) are available; the remainder are in preparation.


Y. Tsiounis and M. Yung. On the security of ElGamal-based encryption. Lecture Notes in Computer Science,
REFERENCES


[TZ94]

Tsiounis:1998:SEB


[TY98b]

Tax:1999:PFD


[TYD99]

Tygar:1996:CPI


[TYH96]

Tillich:1994:HS


[TZ94]

Tzeng:1999:CMC


[Tze99]

Udell:1998:HAW

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).

[Ude98]
REPRESENTATIONS

[Uehara:1995:ESB]

[Udell:1994:BCRb]

[USASC:1923:EC]

[USWD:1924:EC]

[USASC:1940:CML]

[USASC:1942:ACC]

[USDOS:1970:BC]

[USNBS:1977:DES]
REFERENCES


REFERENCES


USGSA:1982:TGS


USNBS:1983:FPD


USGSAOIRM:1984:ISR


USGAOPEMD:1987:PDD


USDA:1988:CED


USNBS:1988:DES


[UCC:1996:SRP]

[USPTO:1996:CCP]

[USCHCJ:1996:SFT]

[USCHCCSTTCP:1997:SFT]

[USCHCJSCIP:1997:SFT]
REFERENCES


REFERENCES


REFERENCES


USENIX:1994:PSU


USENIX:1995:PUT


USENIX:1995:PFUa


USENIX:1995:PFUb


USENIX:1996:SAC


USENIX:1996:WEC


USENIX:1996:CSW


USENIX:1996:PSUa

REFERENCES


[USE98d] USENIX, editor. Seventh USENIX Security Symposium proceedings: conference proceedings: San Anto-
REFERENCES


REFERENCES


**USDOA:1989:BC**


**USCHJC:1997:SFT**


**USPBC:1997:AEC**


**VanderBank:1988:CFM**


**Vadhri:1995:VID**


**Valerio:1892:C**

REFERENCES


REFERENCES

vanRenesse:1996:OSC

vanDijk:1997:MIT

vanRenesse:1997:ODS

vanderLubbe:1998:BMC

Varaiya:1999:DSI

Varma:1999:IDD

Vaudenay:1993:FHI
Vaudenay:1995:NMC


Vaudenay:1996:WKB


Vaudenay:1998:CCC


Vaudenay:1998:PSB


Vaudenay:1998:CCR


Vaudenay:1998:DFC


Vaudenay:1998:FSE


REFERENCES

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


Vandermeulen:1999:ADM


Lubbe:1998:BMC


Wal:1997:PBR


Vedder:1993:SAM


Vedder:1998:GSS


Vedder:1998:ISI


Venema:1990:IEI


Venkaiah:1992:RBP

REFERENCES

Vernam:1926:CPT


Veron:1995:CHI


Verschuren:1998:SCN


Verschuren:1998:SAS


VonzurGathen:1999:MCA


Vandewalle:1993:TAT


Vallee:1988:HBO


Vallee:1989:HGR

[VGT89] Brigitte Vallée, Marc Girault, and Philippe Toffin. How to guess $l$th roots modulo $n$ by reducing lattice bases. In Mora [Mor89],
Verschuren:1993:IOS


vanFaber:1997:SDD


vanHeijst:1993:NCF


Vigna:1998:CTM


Vincent:1971:PAG


Vincent:1972:CPA

REFERENCES

URL http://stacks.iop.org/0022-3735/5/i=6/a=521. See [Vin71].

**Vandenwauver:1998:SIE**


**Voydock:1983:SMH**


**Voydock:1984:SMT**


**VanRompay:1998:DCI**


**Lingen:1996:NDP**


**Vigil:1996:MIS**


**Villasenor:1997:CCb**

REFERENCES


ditability of network covert channels. In IEEE [IEE95b],
pages 186–198. ISBN 0-
7803-2540-0, 0-8186-7015-0,
0-7803-2541-9. LCCN QA
76.9 A25 143 1995. URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/1018.html.
IEEE Catalog Number [vO92]
95CH35760.

Paul C. van Oorschot.
A comparison of practical
public-key cryptosystems
based on integer factorization
and discrete logarithms. Lecture Notes
in Computer Science, 537:
576–??, 1991. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http:/
/link.springer-ny.com/
link/service/series/0558/
bibs/0537/05370576.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0537/05370576.
pdf.

Paul C. van Oorschot.
A comparison of practical
public-key cryptosystems
based on integer factorization
and discrete logarithms. In Conte-
emporary cryptology, pages 289–322.
IEEE Computer Society
Press, 1109 Spring Street,
Suite 300, Silver Spring,
MD 20910, USA, 1992.

Rainer Vogel. On the linear
complexity of cascaded
sequences. In Beth et al.
[BCI85], pages 99–109. CO-
DEN LNCSD9. ISBN 0-
387-16076-0 (USA). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/
0558/tocs/t0209.htm;
http://www.springerlink.
com/openurl.asp?genre=
issue&issn=0302-9743&
volume=209. Held at the
University of Paris, Sor-
bonne.

James D. Volts. Bibli-
ography of cryptography:
REFERENCES

Part I: Cryptography. U. S. Army, Cincinnati, OH, USA, 1941. various pp. LCCN ???? Chronologically arranged, covering period 1518–1940, and indexed by authors.

VonZurGathen:1992:PEE


VonZurGathen:1992:PEF


Voukalis:1980:DFC


Voukalis:1980:GSE


vanOorschot:1991:KPA


vanOorschot:1996:DHK

ny.com/link/service/series/0558/papers/1070/10700332.pdf. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Voyatzis:1996:ATA


Voyatzis:1998:D1W


Vassiliadis:1988:PEA


Varadharajan:1997:ISP


Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993.

vanTilburg:1994:SAC [vT94]

vanTilburg:1986:DBK [vTB86]

vanSchyndel:1994:DW [vTO94]

Vu:1995:CPM

Vazirani:1985:ESP [VV85]

Valiant:1986:NED [VV86]
L. G. Valiant and V. V. Vazirani. NP is as easy

**Verheul:1997:CLS**


**Vandeumeulebroecke:1990:SCB**


**VanOorschot:1994:PCS**


**VanOorschot:1996:DKA**


**Vedder:1998:SCR**

K. Vedder and F. Weikmann. Smart cards — re-


REFERENCES

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

Wobber:1994:ATO

Wade:1993:SLV

Wadsen:1998:CLI

Wagner:1983:F

Wagner:1998:DCK

Wagner:1998:CSR

Wagner:1999:BA
REFERENCES

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


Walton:1995:IAS


Walther:1998:VBE


Walker:1999:CCL


Wallich:1999:HSM


Walter:1999:MTI


Wen-Ai:1994:MTS

Jackson Wen-Ai, Keith M. Martin, and Christine M.

Wang:1986:UEA

Wang:1992:CDS

Wang:1992:DKT

Warren:1982:BTC

Warren:1998:ASE

Watler:1989:VAC
Miguel Watler. VLSI architectures and circuits for RSA encryption. Thesis (M.Sc.), Queen’s University, Ottawa, ON, Canada, 1989. 137 pp.

Watt:1991:IPI

Watson:1999:DOC

Wayner:1991:TDL
Peter Wayner. True data: a look at techniques for ensuring the authenticity of
the data you send, receive, or store. *BYTE Magazine*, 16(9):122–124, 126, 128, September 1991. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

**Wayner:1993:CAS**


**Wayner:1993:ECD**


**Wayner:1993:SER**


**Wayner:1995:PCL**

Peter Wayner. Picking the crypto locks — with today’s hardware and a new technique called differential cryptanalysis, it’s getting easier for data burglars to crack your safe. what can you do to keep them out? *BYTE Magazine*, 20 (10):77–??, October 1995. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

**Wayner:1996:DCB**


**Wayner:1996:DLY**


**Wayner:1998:MJD**

Peter Wayner. Making Java development JSafe — RSA’s cryptographic toolkit targets Java as the platform
REFERENCES


**Willcox:1992:TCS**


Two volumes.

**Wagner:1994:PPR**


**Wolf:1995:ICR**


**Whittle:1999:SDC**


**Wallach:1997:ESA**


**Wu:1998:CRP**


**Wegman:1981:NHF**

Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set


Weber:1998:SMD


Wang:1999:SCB


Wendling:1999:PRS


Weber:1979:USD


Weber:1993:MDC


Weber:1998:SWY


Webb:1999:UAO

REFERENCES

Wedemeijer:1999:DFM


Wehde:1997:UGT


Wehde:1998:MBE


Wehde:1999:MSE


Wehde:1999:DFM

Wehde:1997:UGT

Wehde:1998:MBE

Wehde:1999:MSE

Weingarten:1983:CCP


Weiss:1988:BOP


Weissman:1991:IRA

REFERENCES

Weissman:1991:IRN


Weierud:1994:SPB


Weierud:1998:C


Weierud:1999:TIJ


Wells:1980:ADB


Welchman:1982:HSS


Wells:1982:USE

David L. Wells. The use of subkey encryption to counter traffic analysis in communications networks. Technical report CSE 8201, Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX, USA, February 1982. 24 pp.

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

REFERENCES


Y. Watanabe and H. Imai. Shared generation of random number with timestamp: How to cope with the leakage of the CA’s secret. Lecture Notes in Computer Science, 1560: 290–305, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

REFERENCES

Wichmann:1990:CMR


Wiedemann:1986:QC


Wiener:1990:CSRb


Wiener:1990:CSRa


Wiener:1994:EKS


Wiener:1996:EKS

for Data Internetworks, W. Stallings.


M. V. (Maurice Vincent) Wilkes. *Time-sharing com-
REFERENCES


REFERENCES


Wil86


Wil86b


Wil86c


Wil93

[Wil98a] Jennifer E. Wilcox. *Sharing the burden: women in cryp-
proquest.safaribooksonline.com/0112010014SI; http://
proquest.safaribooksonline.com/640.

Science, 1440:49–54, 1998. CODEN LNCS-9D. ISSN
0302-9743 (print), 1611-
3349 (electronic).

0321-0. 192 pp. LCCN
D810.S7 W48: D810.S7
W73.

secret*. Weidenfeld
8. xiii + 199 pp. LCCN
D810.C88 W56.

secret: the first ac-
count of the most astounding
cryptanalysis coup of
World War II — how the
British broke the German
code and read most of the
signals between Hitler and
his generals throughout the
war*. Harper & Row, New
York, NY, USA, 1974. ISBN
0-06-014678-8. xiii + 199
pp. LCCN D810.C95 W73
1974.

secret*. Dell, New York, NY,
USA, 1975. ISBN ????. 286
pp. LCCN D810.C88 W56
1976.

connection*. Harper & Row,
pp. LCCN D810.S8 .W538
1978.

[Win83] Robert S. Winternitz. Producing a one-way hash func-
tion from DES. In Chaum
et al. [CRS83], pages 203–
207. ISBN 1-4757-0604-
9 (print), 1-4757-0602-2.
LCCN QA76.9.A25 C79
1982.
REFERENCES

Winternitz:1984:SOH


Winterbotham:1989:US


Winterbotham:1991:US


Winton:1993:UPH


Winterbotham:1999:US


Wired:1998:REC


Wedel:1996:FSA


Watanabe:1997:SCR

Wechsler:1997:AVB

Whiting:1999:FOK

Woo:1992:ARC


Tom:1994:LAP

Chung Kei Wong and Simon S. Lam. Digital signatures for flows and multicasts. IEEE/ACM Transactions on Networking, 7(4):502–513, Au-
REFERENCES


REFERENCES


[Wright:1998:NTD]

[Woehr:1997:CRR]

[Wolfe:1943:FCCa]

[Wolfe:1943:FCCb]

[Wolfe:1943:FCCc]


[Wolfowicz:1993:SPR]
W. Wolfowicz, editor. State and progress of research in cryptography: 3rd Symposium — February 1993, Rome. PROCEEDINGS
REFERENCES


REFERENCES

883


REFERENCES


REFERENCES


Wagner:1997:CCMb


Whitten:1999:WJC


Weiss:1985:RCM


**Wu:1992:GOC**


**Wu:1996:SNL**


**Williams:1979:CAA**


**Wah:1984:RAM**


**Westfeld:1998:SVC**


REFERENCES

50–56, 70, 1992. CODEN HDAXE3. ISSN 1000-2472.


REFERENCES

[181x634] RED8. ISSN 0163-5980 (print), 1943-586X (electronic).

[181x622] Xu:1998:STP


[XZZ98]

[Yac99a]


[Yac99b]


[Yah94]


[Yahalom:COMPSYS-7-4-451]

Yamamura:1998:PCU


[Yam98a]


Yamamura:1998:PKC

Yamamura:1999:FCU


[Yam99]

Yamamura:1999:FCU

Yahalom:COMPSYS-7-4-451

Yan:1995:PTL

S. Y. Yan. Primality testing of large numbers in Maple. *Computers and Mathematics with Applications*, 29
REFERENCES


Yao:1982:PSC


Yao:1982:TAT


Yao:1986:HGE


Yardley:1931:ABC


Yardley:1940:SSA


Yardley:1983:CBC


Yardley:1990:ABC

lished by Bobbs-Merrill, Indianapolis, IN, USA, 1931.


REFERENCES

Yin:1997:REA


Yakovlev:1998:PND


Yahalom:1994:TBN


Yang:1997:NCE


Yen:1995:IDSb


Yen:1995:IDSa


Yang:1997:NCEa

Ching-Nung Yang and Chi-Sung Laih. A note on

**Yen:1997:SAT**


**Yi:1997:NHF**


**Yi:1998:NBO**


**Ye:1999:CS**


**Yeung:1998:IWI**

REFERENCES

Yfoulis:1999:SOP


York:1996:BSN


Yourdon:1996:JWS


Young:1997:IJA


Yeh:1991:EIC


Yoshiiura:1999:SFU

REFERENCES


Yuan:1992:VLD


Yung:1985:CSP


Yung:1985:SUK


Yuval:1997:RTE


Yang:1997:CBC

Yang:1999:GSP


Yu:1989:DEB


Yu:1991:SED


Young:1996:DSB


Young:1997:KUC


Young:1997:PKA


Young:1997:SEC

[YY97c] Adam Young and Moti Yung. Sliding encryption:


REFERENCES

[102x644] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES

[102x681] REFERENCES
REFERENCES


REFERENCES


Reto Zimmermann. Efficient VLSI implementa-
REFERENCES


Zhao:1998:DWW

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

Zhao:1999:DWW


Zhao:1999:BTT

Jian Zhao and Eckhard Koch. A digital watermarking system for multi-

Zhao:1998:GDW

Zhao:1996:DWS

Zhao:1999:ERL

Zhao:1995:ERL


[ZK96] Jian Zhao and Eckhard Koch. A digital watermarking system for multi-


REFERENCES


Zeng:1997:RRO


Zhou:1999:SPP


Zhang:1999:AFV

Yuqing Zhang, Jihong Li, and Guozhen Xiao. An approach to the formal verification of the two-party cryptographic proto-

Zheng:1990:CBC


Zheng:1991:DBT


Zolman:1993:BSJ

Leor Zolman. Building a secure journal/logging util-

[ZMI90]

[ZMI91]

[Zol93]

Zorpette:1987:BEC

Zheng:1993:HOH

Zhu:1996:PKC

Zheng:1993:PAA

Zwiggelaar:1999:DCM

Zukowski:1998:JTUb

Zukowski:1998:JTUa


