Title word cross-reference

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

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

$\$1$-Million$ [GC97]. 16 [BS93a, GC94]. 2 [JV98b, KG95, Koh91b, MVZ98, SBVG99].


F_{2^n} [MVZ93]. F_{2n} [SS98a, Ler97]. F_p [Miy93a]. GD(2^n) [Ara93]. GF(2) [She95c]. GF(208) [Ros98a]. GF(2^m) [FBT96]. GF(p) [Gar93b, HNM98]. $\gg$ [GQW+91]. k [Car97c, DJL93, HKS97a, HKS97b, KR99b, KS97b, WD99b]. l [HL93a, KS97b]. L2 [Vau99a]. $\lambda$ [RS99c]. L $\geq$ 2 [SVxW91]. $\ll$ [GQW+91]. m [Bla94a, FR94]. N [BS91e, BS91d, HKS97a, HKS97b, KSW99b, KSW99c, KK98, Per93, QG90, Tak97].

N = p'q [BDHG99a, BDHG99b]. $N^{0.292}$ [BD99b]. P [BS90b]. $p^kq$ [Tak98a, Tak98b]. r [BDHG99a, BDHG99b, FJRS96]. s [YT95a, YT95b]. $s^2$ [Knu93b]. Step_{k,m}

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

B [BA97, DS97c, DFKN93, HG97c, HG97d].
6 [IEE95c]. 2-adic [BK95a]. 2-key [HP99a, HP99b]. 2-Prover [DFKN93].
3


3 [HT98, KSW97a, Nat99a]. 3-Round [HT98]. 3-WAY [KSW97a]. 3.0 [WS96a, WS96b, WS97]. 3.4.1.1 [Ano97r].

300-nm [Gar97a]. 37th [IEE96a]. 384-bit [MLLG95]. 38th [IEE97f]. 3.3.9 [HT98, KSW97a]. 3.0 [WS96a, WS96b, WS97]. 3.4.1.1 [Ano97r].

300-nm [Gar97a]. 37th [IEE96a]. 384-bit [MLLG95]. 38th [IEE97f]. 3.3.9 [HT98, KSW97a]. 3.0 [WS96a, WS96b, WS97]. 3.4.1.1 [Ano97r].

300-nm [Gar97a]. 37th [IEE96a]. 384-bit [MLLG95]. 38th [IEE97f]. 3.3.9 [HT98, KSW97a]. 3.0 [WS96a, WS96b, WS97].
Win93, YL97b. Age
[Bar94, SB97, Uni98i, Wal95, BS97b, Car97a, Joh98, Mar95b, Uni97c, Duh90]. Agencies
[MKS99]. Agency [Gar97a]. Agent
[FK99, MM99b, SJS98]. Agent-Oriented
[BLH99]. Agents
[BGS98, FGS96, GB98, INDI99, Jun99, PW99, PWU99, RS98c, RS98d, SCT99, SSP90, Vg98, YY97c]. Agile
[KLZL99, THP+98]. Agnes
[Luj98a, Luj98b]. agnostic [JY96]. Agree
[Gar97a, Ano97-27]. Agreement
[BWM99a, Bor95, Bor96, Cae96b, Gar94, Gar97c, JV96, LM94b, LP99, Man93a, MW96a, Man97a, RSA93b, Van95a, WOl98, vOW96, BY93c, BY93b, HY98b, HY98a, LM94a, VW96, Zhe95a, Zhe95b, Wei99]. Agreements
[MB99a]. Agricultural
[Far93]. AH
[MG98a, MG98b]. AI
[Mas97, PMP99]. AI-STRATA [PMP99]. aid
[SBTV99]. Aided
[BQ95b, BQ95a, HCY96a, LYH93, LL95a, MW98d, MDP94, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. Aids
[Cra92]. AIR
[Ano97r, DIF94, SvA+98]. AIR-BAG
[Ano97r]. Airborne
[CKN99]. AIX
[Con93]. Aijat
[GGH97a, NS98d, NS98e]. Akelarre
[FS97a]. AKL
[AP94]. Acta
[Ano97-29]. Al
[CM99d, CFK+91]. al-Khwarizmi
[CFK+91]. Alan
[Hod97]. Alarm
[LKD98]. Albuquerque
[IEE91]. aléatoire
[Bou94]. Alek
[Scu92]. Alexandra
[LCW96]. Alexandria
[IEE94a, Man98]. Alf
[Dob95b]. Alfred
[Sha99a]. Algebra
[BK94a, Pes97, VG99, CMM93]. Algebraic
[Des98a, FL99a, Gog99, HR90, Kob98b, LW91, Mv93, Wat91, Ala97, BHRH99, CLW98, CMM93, HJ94, JM96a, Sch91a, SH94, ZPY96]. Algebraic-Code
[HR90, Mv93, Ala97, CLW98, SH94]. algebraic-geometric
[JM96a]. ALGOL
[RS99c]. Algorithm
[ANS97, Ada97b, IBM93, Ano96c, Ano96e, ADEDS99, COP+95a, CD91, DKR97b, DNRS97, Dra98, GX99, GK98, GTG94, GN95c, HG97a, HG97b, HW94, Kal91, KY95a, KR96a, KY98, KMKH99, Kob98c, Kra93, Kwa97, MD98, MW94, Mas94, Mat97, Mis97, MS90b, Mot99, 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, Sch94b, SB98, SW93, Sta99b, Swa94, TK99, THP+98, VKR98, Whe94, Yin97, ZYR91, BI94, BS95a, Bow93, CC98, CGV94, ISO97, IKNY98, JMLW94, KY95b, KY97, KYxx, Kir95, LRW93, Lz90, Lz91a, LL93b, Lon91, LC97b, MSS93, MPL99, Mol98, Pa96, Riv90a, Riv91b, Riv95d, Sch91a, Sch94i, Tay94, Vd95, WN95, YL93, YL95b, ZW99, ZPS93]. Algorithm
[AA95, Acc97, LL98, Moc97, QA94, Sch93b, Sch94c, See97, Sim93, Sta94b, WSK97a, WSK97b]. Algorithm-Agile
[THP+98]. Algorithms
[ACM97b, ANS97, Ano95a, Ano95b, Ano96b, Ano97c, AMP99, Ata99, BS99a, BP98a, BR96a, Bas98, BGM97a, BGM97b, BL96b, BL96a, Buc91a, DGV92, FCD98, GLC98, Gl99a, HEQL98, KM98a, KAK96, KB92, LC99, Lei99b, LD99, MT99b, PSR97, PA98a, PS93b, Por98, Pre97a, PRB98b, PRB98a, QG90, RS99a, Sch94g, Sch94j, Sch94c, Sch96a, SW97a, SW97b, Sch94h, Sed92, Sho97, Sot98, SB99, Sp95, Ste96, VCF+90, AA95, Ano90, CPPK98, CMM93, CJL+92, CadHSV96, DG96, DN95b, FR95a, GP97, HJ99, HP94, Imp92, KKL99, MS99c, OS91, OS92, Pr096, QN98a, Sch91b, Sim93a, Tab94, TY92, Tay90, TV94]. Alive
[BK90]. All-Or-Nothing
[Riv97c, Ste98b, BMM99a, BMM99b, Boy99, SRY99]. Alleged
[Go97d]. Alley
[KR96a, PRB98b, Sch94f, Sch95a, Sch95b, Swa94]. Alliance
[Gar97c]. allied
[DPnubb91, AK99]. ALM
[CH99b].
Almost [AMP99, Bra95d, CCD99, Mau90].
along [BDC+95]. alpha [Zim96a, Zim96b].
alphabet [PS97]. alternating [HSW94, Wer93a, Wer93b]. Alternative [BdM94, Gar97a, Neu94, Smi93b, VtV97, BR96b]. alternatives [FL93]. Alto [ACM98a, IEE98a, IEE98b]. Always [Bra95d, Cha99a]. am [LC95].
Analyze [MOM91]. Analyzing [Gil97, KAK96, NT93]. Anchoring [CS99].
Anguilla [Fra99, Hir97, Hir98]. Animated [HE98]. animation [HE98]. Ann [Dob95b]. Anniversary [CFK+91]. annotating [DSSZ99]. Announcement [Ano99b, Nat92b]. Announcements [Ano95f, Ano95d, Ano95c, Ano97e, Ano97f, Ano97g, Ano98a, Ano94e]. Announces [Got99, Ano97u]. Announcing [Ano97h, Nat97b]. Annual [ACM94a, ACM97b, Ano95i, Bri92, Bri93, CH96, Cop95b, Cop95d, IEE92b, IEE93c, IEE94b, IEE94c, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE98f, IEE99a, Kra98, Sp95, St93b, St94, USE99d, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, IEE92d, IEE95c, IEE97i, Kal97c, Kol96, TM99, USE96e, USE96f, USE98c, Wie99]. anomalous [GLV99]. Anonymity [BD99a, DFTY97, FJ98, JMP+98, STS99b]. Anonymous [DF98, DF99, FT99b, GMM97, Jae96, Jae99, MS99a, OKST97, PW97a, RSG98, STS99a, SP99, SGR97, Pfi95].
JDK+91, KMPS99, KP99a, KI96, KK95, LOX99, LC99, Mar98a, Man96b, Mun9a, Mun91b, NC97, PSN95b, QV90, QG95, Rog95, Rue93, SSS98, Sch99i, SZ93, SK98c, SK98b, SKIT99, VDDR99, Ara93, BY93c, BY93b, CC98, DDB95a, DDB95b, DF97, GZ91, HL97b, MW94, Nyb98, Pet91, PKM97, SI93b, SRL98, Siu99, Ste99b, SW98, SW99a, TY92, Woo90.

Applications [Aga92, BGR98a, BFW99, CG98, CJR98a, CJR98b, CGB93, COZ99, Cre90, Dan96, DY91a, DFGH99, Duf98, DN94, Dwo97, Ebe93, FMM99, Far93, Fis98, IEE95a, IEE97a, IEE92b, IEE93c, IEE94c, IEE97b, JMSI96, KSHW97, KSHW98, KSW99b, KSW99c, KM96a, Knu94b, KT91b, Lan97, MS95f, OdIP98, OO90, PS96b, SY96a, DY91c, TN96a, TN96b, VV98, VP96, ZRR91, vW94, vW99, ACM99c, Ada91, Ano98h, BM90, Ber93, BF97b, BV97, Boy98, BP97b, Com96, CFG96, DiDPS96, Dix94, Dom96, Eng99, FO98, GvP98, Gre94, GS94b, HMP95, JV98a, Kal95, KW92, KG93, LY93, LN94, Lub96, Mei92, Mic97, MT98, NKC94, Ped91a, PC98, Rh95, Sch97c, Sha95a, SSM94, Sin95, Sta97c, SSG99, T98, USE96e, Way98, YL93, ZVR90].

Applied [BHJM99, HH98, MR95a, Sch94g, Sch96a, Sha99a, FFW99, FMR99, MV97, PR98, CM93, Dav94]. apply [Clin97, UU97b]. Applying [CO98, HO96, Jan99, KMP99, MW98a, War98, ARR99].


Architecture [IBM93, BCCD99, CJR98a, CJR98b, Con99a, Fe93, Fe96, G699, JDK+91, MM99b, Muf93, NH90, NK98b, Oh99, PF94, RBvR94, Rus90, SS90, She92a, She93c, Tref99, Tua99, VVG93, YS99, Kar96, LS98a, Con98, JD91, LMJ93, SV99, SY92].


Aren’t [Cha99a]. Arguments [BJY97, BD91, NOV93]. Arias [DHMR96]. arising [APDS93]. Arithmetic [BP98a, Bre99, BP97c, Bus97, CD98b, DBVD96, KK99b, LL99, LD99, Mih94, NM96a, PSR97, SSS98, SJ93, CPP98, ISO97, JS93a, Kal92, Kal93b, KM99a, Pos93].

Arithmetically [De98d]. Arizona [IEE99b]. Army [Mee98, Me98, Dav98a, DR99b, Ros99].

Arnoldi [HRV99]. Array [MT95, DF92]. Arrays [BGS94, BGS96, BKK98, MT95, TT99, JM93]. Arresting [Mad92]. arsenal [Me98]. Art [Eri99, Lan98, NM96a, Pre98c, She92e, B992b, B992b, Beu94, B+96b, PGV93d, PR98]. article [Bur98b].

Artificial [An96l, SBTV99]. Arts [Tv92]. Asia [Un98c]. ASIACRYPT [IRM93, KM96a, PSN95b, PSN95a].


Assumption [Sak96, Sal98]. Assumptions [AB99a, AB99b, BD91, KRS99, NOVY99, Oko93a, Sim98c]. Assurance [IEE94b, IEE96d, KYG92]. Assuring [Car95].

AT&T [SSM94]. Athena [DS90a]. Athens [Kat97]. Atlanta [ACM99b]. Atlantic [Bra94b]. ATM [PS98c, PS98d, PS98f, PS99a, PS99c, PS99b, PS99e, THP+98, VSH97]. atomic [BBS98b]. Attack [BP98b, Ber97c, dBB91, BDF98, CG99, CS91, CLL99, Cop94b, CS98d, DBR+99, Doh96b, EH96, GC91, GC94, HK99d, JK97, KSW98a, KSW98b, LA98, Ly98b, Ma98, Mis97, MS98, OM94, PBFV90, RS91, SMK98a, SK98c, SK98b, TOU94, Wag99a, BP98c, BB95b, BK95a, BQ97, HA94b, Har98, JG95, Kuhl98, KOT95a, KOT95b, LZ90, Lon91, Low95, MRS99, MY93a, Men95b, Miy90, RS98f, SNT93, SG98, SGS99, dB91, vOW91].

Attack-Resistant [LA98]. Attacking [ESST99, Luc98c, SH95a, SH95b, IEE97e].

Attacks [BQ95b, BQ95a, BBS99b, BK98d, BW99, BWM99b, BHE98a, Bon99, BKR97, CTT94, CJR99a, CSV94, CNS99b, CMY98, Da99, Dam91b, D91f, FY95b, FG98, GGOQ98, GWW+91, GS99b, HGS98, HK98, Hwa92a, HCY96a, Jas96, JS95b, JJ99a, JJ99b, Jut98, KSW99d, Koc96b, Kwa93, KS97c, LR96, LL94a, Luc98b, MDS99, MS99b, PV97, PK95a, PK95b, Pen96, PAK98, PW93a, SVxW91, TJ99, W9a90, WK97, WZ99, W9a98, YY97b, ZS93, Bib94a, CP94, Cop94a, GO95, HY98b, HY98a, HLL+95, JS95a, KL95b, KM96b, Koc95, LM93c, NY90, OY91, SNT95, Tze99, TH99, YL97b, vDV98, vT93].


Attorney [Mer97]. attract [MB99a].

attractions [BDC+96]. Attracts [MB99a].

Attribute [ECM96, Ho99]. Attribute-Efficient [Hof99]. attributed [Lea90].


auditorialization [HW91]. Auditorium [IEE98b]. Aufenthaltssorten [FT95].

Augmented [TDT98, KT98]. August [B+96b, B92, Bri92, BS95e, Cop95b, Cop95d, Des94b, IEE98b, Kal97c, Kob96, KP99b, Kra98, MDS99, Nat98, RD99a, Sti93b, Sti94, TM99, USE90, USE98a, USE98b, USE99a, Wie99, Yu92].

AUSCRYPT [SP90, CZ93]. Austin [Ana94d, IE98e].

Australasian [VPM97].

Australia [DG96, GN95b, KG93, KK99b, MDS90, PS95b, SP90, SZ93, VM97].

Australian [CFK+91, GN95b, Ca96a, Or96]. Austria [BS95e].

Authenticated [BF97a, BWM98, BWM99a, Bo95, Ch99, Dan95, HCY96b, Jv96, LC97a, Man97a, RH93, SKWH96, BSN96a, BSN96b, BF99b, BR97b, DvW92, HY98b, HY98a, Yu99].

Authenticating [ADSW99, He98a, KS99a, Mi92a, SK96a, LC94].
Authentication [Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Mau96a, MAM95, McM96, Mee98, MS95c, MS95d, MWW94, MTVZ92, Mor97, Mye94a, Mye97, NP97, OOK91, OM94, Opp96, PKOT94, P98, PLWSN99, PSN91, PGV93c, Pre98a, Pre98c, MS95e, RRSW97a, RS98b, RRSW97b, Rog95, SNT93, SN93, ST94, SNT95, SN98b, SN98b, SSH93, SS96, SP99, SA95, SC96a, SC96b, Sch94d, Sch99k, Sga90, Sga91b, She97, She95a, Sho96, Sim96b, SV94c, SKAM99, Sti91b, SL99, TAP90, T95, TSN93, Tun99, Ude98, Van95b, Van93, Wal95, WK97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC+98, An97d, Atk93, BSN99, BGR95, BCK98, BCKxX, BCB97, BGH+95a, B99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gua90, HS96b, Hor95].

Authentication [HC95b, HLL+95, HW98c, JC98, JG90, KC95, KW92, KNT94, K95b, LC96a, LL95b, Lin88a, Lin89a, Low95, MSN97, MF97, Men91, MC96, Nac93, NT94, PS98a, PS98b, RS98a, RS98f, Sch99j, Sga91a, Sga93, SY96b, St99a, St99a, Sun98b, Sy93, Ts92b, Ts92a, TH99, Ver98b, WL94, XA98, Xie98, YL97a, YL97b, You97, Z98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a].

Authentications [O009, KSL92].

Authentication [Zuk98a]. Authenticators [DF91a, SN96]. Authenticity [BK90, Lud97, M90, Way91].

Authenticode [Fly97]. author [Lea90]. Authorisation [COZ99]. authorities [Ame95, Ame96a]. authority [CFSY96, CGS97, JMO95a]. Authorization [BDPSNG95, Cas95, FL96, WO090]. Auto [YY98c, YY99b]. auto-certifiable [YY98c].

Auto-Recoverable [YY99b, YY98c].


Automated [Dan97, FIP93a, FN93, FK99, GSN94, GDS91, She96a, SGPH98, VDDR99, W999, CD98a].

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

Automating [Bur99, Smi93a].

Automatic [Des98a]. Automaton [DG93, G96, DZW96, MZ98, T99, TCC97, TC99b]. automorphisms [VP96].

Autonomous [CKN99, RZ99].

autoscritcher [Dea98a, CF92, Cra92]. aux [Bec90]. Available [DJ98c]. Avalanche [Cas93, CS96c, HT95, OC94, Z99, SZZ94a, SZZ95b, YT96].


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

b [C97, UU97b, An99e, HS90, Lam99]. B-Trees [HS90]. ba [IPnbbbrm91].
Babbage [Fra93]. Back
[GC97, GO96c, WSFC99, IEE97e, WG97].
Backup [Mah96]. backwards
[BKR98a, BKR98b]. Bacon [Lea90]. Badge
[WHFG92], BAG [Ano97r]. Baker [PS96b].
Bal [IPNdbbbprm91]. Balance [RG99].
balanced [MCD98b, YT95a, YT95b].
Balatonfured [Rue93]. Ballot
[CFSY96, BT94]. Ballots [Sal91].
Baltimore
[ACM90, Ano96a, NIS92, USE92b]. Ban
[Gar97a, BP98f, XZZ97]. BAN-like
[XZZ97]. Bandwidth
[Bla96a, Bla96b, JMP98, MM92b, Sim98b].
Bandwidth-Efficient [JMP98]. Banking
[Chi92]. Barbara [Bri92, Bri93, Cop95b, Cop95d, Cre97, Cre97, CJS91, Cre97, DGV93, Da95, DNM98, DSB95, DS96, DPP90, DMPW98, DDGM97, DQ94, Dem94, DF99, EKLM99, EN98, ENK99, FCH99, FBS97, FK99, FKMY98, FJM+96, FBS98, FR95a, GKR97, GJKR99, GRB99, GN95c, Gys96, Hes97, HPS98, HJPT98b, JO97, Jia99, JSS94, JJ99a, KKS97, Kal98c, KR98, Kim93, KG95, KP96a, KP97, KM99b, KA99, KMOV91, Kra94b, KH98b, LM93a, LM93b, LY93, LL97a, Len99a, LW91, Lin98, MNSV97, MD99, MR95a, Mau93a, MM96a, MM99b, MM99b, MG91, MG91, MM98b, Mue99, MM98b, Mui99, NM95, NM99, NOV93, NS98a, Nec96]. Based
[NS97b, NMMV98, OMV98, OO93, OFF93, vO91a, Pa99a, Pen96, PL94, PRZ99, Po99, PB99a, PV98, PK99, Pre97a, PMP99, RSA99b, Ros98a, SSN98a, SCT99, SC96a, SPS97, SE96, SJS98, She92e, Sho96, SM91, ST91, SSN99, SKIT99, SZT98a, Var99b, WCS95, WD99b, WS99, YKB94, YY97b, ZL99, vO91b, Ala93a, AW95, Ale98, AAPS92, BSN96a, BSN96b, BSN97, BDH97, BBC98, BSB97, BCD98, Bea97a, BB90, BCB97, BMP97a, BBL95, BFK94, BCC99, CCA99a, CPS95, Cha95a, CW97, CS97c, CCH98, CLL99, CD95, Cus95, DD95, FSS94, FY96, FY96a, GM91, GH99, GK95a, HZ93, HY93b, Ha99, HSW96, He92, HI97, HLMW93, HMXW94, HMP95, HW98a, HJPT98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JI95, JG93, JG90, JY98, KM99a, KSL92, KM99d, Koy95, Ku92, KH97]. based
[BK96, LRW93, LvdLB96, LS98a, LHW99, Lz90, LCL95, MRR95, MS98a, MLA91, Mau91b, Mch92, MZ98, MM95, MTN97, Mu92, MV98, NS97c, NR95, OP999, OU98b, Ole95, Pat91b, Pat91a, PS97, PC98, PGCS96, PBBC97, Por93, PG91, PGV93b, PGV94, RP95b, SV94, SV95a, Sha94, SRRL98, Sim98c, SM90, SS95b, SS95c, SMK98b, Son99, SKD94, Ste95, SS98b, SZT98b, Tan90, TA97, TAP90, TC91, VNM99, Ven92, Wan92, WKH97, Wil93a, WWH95, XA98, YWC97, YL97c, Zhe95b, ZPY96, vO92, vT94, CD96, YKY99, Dhe98, Por93, TY98b, TY98a]. Bases
[BCE+94, MSDS90, Yua92]. Basic
[CF99, Des98a, vdL98, OK98, YHKI99, Zie97, van98, BDH97, Rac90, dVdV98, Hel98b]. Basics
[Ba99, IEE97]. Basis [FBS98, LL99, The95, Wil98, BK98g, Car98, FBT96]. Batch
[BGR98a, BY93c, BY93b, BFP99, Fia90, Fia97, BGR98b, YL95a]. Battle
[Ban93, Gar97a, Gar97b, Gar98b, SBR97, Fro96]. battleships [Jar97]. Bayesian
[BBDF97, Jen99]. BCH [CC98, FC94]. Be
[BF99a, BV98c, Cha93, CD98b, DY91f, EvH91, GSV99, NM95, Way93c, Ano90, Ano95c, Ano98h, CP91, Cs95, Ev92, Ev93, LF97, NMV95a, NMV95b, NOV93, Ros98c, Sch91b, Sim98c, van97a]. Beach
Byte-Oriented
[500, YLCY98a, YLCY98b]. Bytes
[500, Yuv97]. Byzantine
[500, Bea92, Bor95].

C [Sh99a, vdWS97, vS97, Bak92, Bas98, BMS99, DSB99, Gar98b, Hel98b, Kal92, MGL+98, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. C0YNTHIA [WBBL99]. C2 [Ste92]. CA
[RD99a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. Caching
[STSW99]. Cactus
[Ano97r]. CADE
[HB99]. CADE-16
[HB99]. cAESar
[Koe99]. Calculating
[CFK+91]. Calculation
[HRVV99]. Calculators
[CWM+91]. Caching
[STSW99]. Cactus
[Ano97r]. CADE
[HB99]. CADE-16
[HB99]. Caching
[CFK+91]. Calculation
[HRVV99]. Calculators
[CWM+91]. Calculus
[ABLP99, ACM98a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. Caching
[STSW99]. Cactus
[Ano97r]. CADE
[HB99]. CADE-16
[HB99]. Caching
[CFK+91]. Calculation
[HRVV99]. Calculators
[CWM+91]. Calculus
[ABLP99, ACM98a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. Caching
[STSW99]. Cactus
[Ano97r]. CADE
[HB99]. CADE-16
[HB99]. Caching
[CFK+91]. Calculation
[HRVV99]. Calculators
[CWM+91]. Calculus
[ABLP99, ACM98a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. Caching
[STSW99]. Cactus
[Ano97r]. CADE
[HB99]. CADE-16
[HB99]. Caching
[CFK+91]. Calculation
[HRVV99]. Calculators
[CWM+91]. Calculus
[ABLP99, ACM98a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. Caching
[STSW99]. Cactus
[Ano97r]. CADE
[HB99]. CADE-16
[HB99]. Caching
[CFK+91]. Calculation
[HRVV99]. Calculators
[CWM+91]. Calculus
[ABLP99, ACM98a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. Caching
[STSW99].
Yac99a, Yac99b, AMS96, VNM99]. CASL
[Mos99]. CAST [Ada97a, Ada97b, Ada98, KSW97a, KSW97b, MSK98]. CAST-128
[KM92a, CJRR99b, RS98f]. Cautious [Gla99b]. CB [Eph98]. CBC
[BR96a, KMS95a, MD98, PA98a]. CBC-Mode [PA98a]. CBCM
[BK98a, BK98b]. CBR [GAGCDAFC99]. CCI
[WCS95]. CCI-Based [WCS95]. CD
[Ano96i, GTGW94, Ros94, UFC94]. CD-ROM
[Ano96i, GTGW94, Ros94, UFC94]. CDE
[Ano97r]. CDL [HHW99]. CDMA
[KSB96a, KSB97, She94c, SKB97, TY94]. CDMF
[JMLW94]. Cell [Omu90]. Cellular
[BKK98a, DGV93, HHW99, NC97]. BEm3+79a, BK98f, MZ98, NK94, PV90, Sim99, WSK97a, WSK97b]. Center
[Ano94d, Ano96a, IEE96f, NIS92, LWC96]. Centered
[PM99, VC99]. Central
[ZTR99]. Centralized [KT96]. Centre
[IEE97c]. centric [BGT96]. Centroid
[LML98]. Century
[CWM+91, KC96, Alv98c, Sch96b]. Cerebellar
[FCH99]. Cerebral [DHQ98b]. Certain
[CS91, MS93, MM92a, CFS97, Ev92, Kuk99]. Certicom
[BT97]. certifiable [YY98c]. Certificate
[Bra93a, FL99b, HFPS99, RSA93a, Riv98b]. Certificates
[Bra95b, Bra95c, NK99, TAP90, DS90a, FFW99]. Certification
[Kal98c, KM99c, LA98, Ame95, Ame96a, GH96]. Certified
[Gir91, Mer90b, RS98b, SG99a]. Certifying
[BY93a, LN98]. CFB [PNRB94]. CFP
[Ano96d]. CFR [UU97b, Cif97]. Chaffing
[Riv98d]. chain [JV98a]. Chaining
[BKR94, CJM95, Jas96]. Chains
[YY98a, dR95]. Challenge
[Ano97c, Ano97w, BCE+94, DDJ98e, DDJ98f, Sim96b, WD98, Wir98, BT97, Ano97c]. Challenges
[Ano98c, BS97b, GB98, McC96, Cer97, FM98b]. Challenging
[CM99d]. Chamber
[Yar90]. Chameleon [AM97]. chan
[XtMn94]. Chance [GB98]. Chang
[Bur94a, Bur94b, HLC96]. Chang-Wu-Chen
[Bur94a, Bur94b]. Change
[FY99, Wal99b, MW98a]. changeable
[HYLT99]. changing [MW98a]. Channel
[AO96, AVPN96, ADESD99, BI99, Bro94, KSW98a, KSW98b, KSW98c, MM92a, MM92b, OKST97, WB92, BM95, FC94, PSB97, Pf95]. Channels
[BDI+96, CRe97, Des96a, dD97, Ki97, Lip94, MM96a, MK94, MM94, PN92, SI94, Sch94e, Sim93, Sim96a, Sim97, VN95, W99a, Des96b, Gr98, Mau91c, SI93b, Sch93b, Sim94c, Sim98a, Sim98b, T997, YL97a]. Chaocipher
[Joh98]. Chaos
[BGR94, BLM94, Ano96i]. Chaotic
[Bih91, GKS97, HNSM91]. Chaotic-Map
[Bih91]. CHAP [Sim96b]. Chapter
[Kal97b]. chapters [Ta98, Ta99]. Character
[BL99, Sab94]. Characterisation
[SB95]. Characteristic
[KMK99, Kob91b, MVZ98, SS98a]. Characteristics
[Fer98, Knu93b, SZZ95a, Sh95a, ZZ95, HT95, RP95b, SS99a]. Characterization
[BS99b, BS99c, CCD99, DDP99, Ito91, PLWSN99]. Characterizations
[YY97, St91a]. Characterizing
[APn999, Charles]. characters
[LPN999, Charles]. Lip98]. Charlesworth
[CWM+91]. Charon
[Atk93]. Chasing
[Gar97b]. chausses
[Sch98c]. chausses-trappes
[Sch98c]. Cheap
[LTV98]. cheaper [Sch98c]. Cheaply
[Ano93j, Str93a, Str93b]. Cheater
[KO99b, KO99a, LH93b, H96, HLC99]. Cheating
[GP99, Rab94, OK96b]. Check
[BK95c, Bl98c, 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]. Checks
[DT98a, PK95a, Pen96]. Checksum
[PBGV90, LRW93]. Chili
[USE96a, USE99c]. Chieh
[XtTmW94]. China
[HOQ97, OiDP98, XtTmW94]. Chinacrypt’94
[XtTmW94]. Chinese
[DiDP96, GO96c, QD91, WWH95, Yu99]. Chip
[Ban94, Bro96, Ele98, Gar97c, GC97, Got99, HMvT94, Lan97, MPPS95, MHMW98, VVDJ90, Way93b, DVQ96, Kan90, Moc97, Pos98, RKD94, Smi94a, Uni95a]. Chipkarte
[Kip97, Kip99b]. Chips
[Ano99c, GO96c, Omu90, Ano97-27, IEE98b]. Choice
[Cha99a, Way98]. Choices
[Hon98, Van95a, We95b]. Chor
[BFS98, SH95a, SH95b, Van98a, Vau98c]. Chosen
[Ble98a, CG99, CS98b, Dam91b, GC94, KSW98a, KSW98b, LL94a, PBGV90, RS91, ZS93, BJ997, CP94, NY90, SNT95, Sah99, SG98, Tze99, vT93]. chosen-ciphertext
[Sah99]. chosen-message [SNT95]. chosen-plaintext [vT93]. Circuits
[KT91b, KT98, WG99, JS93a, LMS97, YWC97]. circulating [Ano96i]. Cirencester
[Boy95a, Boy95b, Dar97, Far93, Wal99a]. CISST [AA97]. City
[IEE99a, USE95b]. Claim [GO96c]. Claims [DS97a]. clandestine [Wr98]. Clara [USE93]. Class
[vD97, Ou99, Uni96c, FR94, HW93, KSB96a, LS91, Lz91a, Zk98a, vT94].
Classes [Haw98b, Pai99d, Haw98a, Sze98].
Classical [Bra94a, MC92, Nic98a, Nic98b, CD98a, Mas99a].
Classification [BD90, LSVV95, PNKF95, Uni96c].
Classifier [CIBM99].
Claw [BHT98].
Claw-Free [BHT98].
Click [WSFC99, Ken95].
Client [DL99, Kon95, Oh99, SL99, GGK+99, Sin95].
client-relationships [GGK+99].
Client-Server [DL99, Oh99, Sin95].
Client/Server [Kon95].
clients [AG95].
Climate [TGKI99].
Climbing [MCD99].
Clipper [Pri94, Fro96, Ban94, Bro96, Hof93, Kan96, MS95f, RKD94, Smi94a, Uni95a].
Clipper-like [MS95f].
Clipping [Hof93].
cliques [JP96].
Cloak [Gre90].
Clock [DHSS95, GO95, GM91, GO95, Men95b].
Clock-Controlled [GO96b, GM91, GO95].
Clocks [DG95, DGT96, Yah94, Gon92].
Closure [Coh96].
Closure [MOM91, PS93a].
Closure [Coh96].
Closure [MOM91, PS93a].
Clueless [RS98c, RS98d].
Clustering [DDJ98a, HE98, Kue97].
CM [CNST98, Kob91a].
CM-curves [Kob91a].
CMOS [BS95c, ECD+99, YS99].
Co [Gl99b, LFCK99, Su99, NM96a].
Co-dimension [LFCK99].
Co-operation [Gl99b].
Co-Processors [Su99].
co-processors [NM96a].
Co. [CFK+91].
Coast [SZ93].
COBOL [Gar90].
Code [CJ99, HR90, J99a, Kip99a, Kur94, Mv93, PV98, Q91, Sch94, Sch96a, Sch94b, Str95, Tod97, DK97, WF94, Zim95b, Al97, Ano97i, BSNP97, CC98, CL9W98, GA98, HM97b, LJWH97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG+00, Mea98].
Code-Breaking [QD91].
code-cracking [WS96c].
Codebreakers [HS93, K99, Sni98b, Y99].
Codebreaking [Car97c, Car98, D92, Sch98a].
coded [HG97c].
codemaker [Mar98b].
CODER [Sto90].
Codes [ACM94b, AW94, AR98, BGS96, BVFD99, CZZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, GBo91, Ho99, Joh94, JS95b, J99b, KKS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWNS99, Pen96, Pre98a, RV99, Rus93a, SN93, SNW98a, SNW98b, SD99, Sga90, Sga91b, SB95, SVW91, Sta96b, St91b, Ton96, Van95b, W94, Ada91, A93a, AW95, BSB97, BI93, Br91, CC99, Cha95a, CMM93, FC94, Gre90, JM96a, Kahl1a, KO95b, LYG94, LMS90, MSS93, MPL99, Moh92, SNT93, SNT95, SKD94, Ste95, St91a, Su98, SS98b, TSN93, TY94, Wnn92a, Wel97, Win93, YL97a, vT94, JS95a].
codewords [PS97].
Coding [Ber96b, IEE97e, KRS99, KH98b, LW91, Lip94, Sch99b, She94, SW95b, Van95b, Wa99a, Ada91, Boy95a, Boy95b, Dar97, DID99, Far93, Gan93, KSB96b, KS97, Kue90, Mit92b, Sab94, Sch98b, Sga91a, SVW95b, SO98, Sh99a, SNS99, TA97, Ger97].
coefficient [K95b].
Coevolution [Nac97].
Coffee [Den97].
Cognitive [CF99, Ger99b, MMM+98, PUF99].
Cohen [PBGV90].
Coin [BN96, Jue99, PW97c, Ueh95].
Coins [EO95b, WSFC99, EO95a].
COIRS [YKY99].
Cold [Joh95].
Collaborating [CF99].
Collaborative [BV98a, Neut91, LS98a].
Collaborators [Gla99b].
College [Far93, IEE97a, UFC94].
Collision [BP97a, Dob97, PG91, Rus93b, Vau93, vW94, vW99, Dob95a].
Collision-Free [BP97a, Dob97, Rus93b, Vau93, Dob95a].
Collisionful [Gon95, BSNP96a, BSNP96b].
Collisions [Ano95a, CJ98, DBGV93, DB94, Gon95, Sim98c].
Colloquium [An97p, vWN99].
Collusion [BS95b, BS98, EKK99, PW97b, LM96].
Collusion-Resistant [EKK99].
Collusion-Secure [BS95b, BS98].
Colony [BP95a].
Color [ADEDS99, NNE97].
Colorado [S99b].
Colossus [Ano97-28, Car97b, Car97c, Car98, Pin98].
Column
[Bra94a, Dwo95, Bra90b, Bra90d, Bra95d].

cominar [Bar92a]. COMANDOS
[TCH+91]. Combatting [DN93].

combination [Rev91]. combination
[Hil94]. combinations [RT93].

Combinator [SAS99b]. Combinatorial
[FK94, Ko95b, Ko95a, Ko96, Ko97, LS98b, Rus93a, Sti91a, Zie97, FSS94, Sta97a].

Combinatorics [MWW94]. Combiner
[SG99a]. Combiners [MS91]. Combining
[KMKH99, NA95, SA95]. command
[Mye94b]. Comment
[DKKK98, LC96c, YT96, BMP97a].

commentaries [Ano97t]. Commentary
[BL99]. Comments [BMP+97b, COP+95a, Dum94, JW01, KSS+92, MC96, NC97, Ng99, Pre95b, SB93, WHL99, Ala97, Gib90].

Commerce [Avo98, Cli97, DDJ98d, DB99, Jak99b, LHB96, Lut98, USE95c, USE96d, USE96b, USE98b, Un97d, BH98, FB97, Gar97b, LM98a, Man95, Sin98, Tae98, VM96, UU97b, Uni96c]. Commercial
[Bhi96, BDR+96, Cae96a, WLEC96, Cha94b, Dix94, Joh90, Sta94a, JMLW94].

Commitment [Dam99a, IOS94, Sal98]. Committed
[DF99]. Committee [Uni98c].

commodity [Bea97a]. Commodity-based
[Bea97a]. Common [IBM93, Lin93c, Mau93a, Tze99, JKD+91, JD91, LMJW93].

Communication [???97, AR99, BF97a, Bet95b, BFS96, CH997, CMN99, FJP96, FK99, FT99b, IKM99, Jam98, KFJP96, KRJ98, PW99, PM99a, SSN98a, Sim94d, WD99a, Wei99, BF99b, Bet95a, BMS96, Com97, CYW98, CK93, Cli97, DFKN93, Hamxx, Rivxx, Sch90c, Sch97c, SD97, Sta97a, UU97b, Ven92, Wi98].

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, Rhe94, SW94b, Sch93a, Sch92c, ZG96]. communicators [Ano97p]. Communities
[MB99a]. Commutative
[GPT91a, GPT91b]. compact
[Ort95b, Ort95a]. companion [Ken95].

Company [GC97, Kar96]. Comparative
[Dae99, Ste92, AA99, Don98, She92g]. Comparing
[Bih99c, HSSI99, HKL94, KAK96, NM96b].

Comparison [BALS99, Cus97, KH98b, LM98b, Mas99a, May97, MG91, vO91a, QN98a, SKW+99a, SKW+99b, Wie98b, Wil93b, vO91b, GM91, Yeu99, ZH93, vO92]. Comparisons [Fol99, SKW+99c].

Compartmented [GPS98]. COMPASS
[IEE94b]. Compatible [SK94, Wat99]. Competence
[WS99]. competing [Sta97c].

Compiler [NM99, SSCP99].

Complementarity [DD99, LM93c].

Complete [Tou91]. Completeness
[Bro94, Sch94k]. Complex
[NT99, MCD98a]. Complexity
[Bus97, CH96, Cle91, DS99, GM99b, HKL94, LMSV99, MMT90, MS94, MMM+98, Mun91a, Mun91b, NMVR95a, NMVR95b, NOVY93, Sch99, Sni98a, Bao94, CS97d, DDP94b, FK93b, GZ91, GN95a, Gol97c, Hil94, MM90a, MS98a, MK92, Shp99b, SMK98b, Sze98]. Compliance
[Dav96]. Component [NK98b]. Composite
[Pal99d, BBR99]. Composition
[ABDV98, GK96]. Compositional
[DHF98, HJTW99, MM99a, Zwi98].

Comprehension [MT95].

Comprehensions [MT95]. Comprehensive
[SSP90]. Compress
[Dob97, Dob95a]. compressed
[CPO+98, CHO+98, HG96, HG97c, HG98].

Compressing [GI99]. Compression
[CI96, DLF97, KPR99, Sch99b, BCR98, CW94, Cra96, Kop97, Oht96, Sab94, Sch98b, dB94].

Compromise [Gar97c, Hed97].
CompuServe [GC97]. computability [BK98f]. Computable [DSV99].
Computability [BK98f]. Computable [BK98f]. Computable [DSV99].
Computability [BK98f]. Computable [DSV99].
Computational [CH96, HKL94, Kos97, KRS99, PG90, Sab94, BCI99, Ger99, McC90b, Pom90a, SS95a].
Computational [CH96, HKL94, Kos97, KRS99, PG90, Sab94, BCI99, Ger99, McC90b, Pom90a, SS95a].
Computations [Cha90, CDD +99, IVE91, Mas91].
Computations [Cha90, CDD +99, IVE91, Mas91].
Computer [ACM93a, ACM94a, ACM97a, Ano93d, Ano97-29, Ano98b, BAC95, BK90, Bre96b, Bre99, CWM +91, DQM93, GMV98, HW91, IVE92a, IVE92b, IVE93b, IVE93c, IVE94b, IVE94c, IVE94d, IVE94f, IVE96a, IVE96c, IVE97b, IVE97f, IVE98a, IVE99a, KK99b, LBMC94, LC95, MDP94, NIS92, Nats97, Neu92, OD99, PGM93d, Q998, Sal91, SSS98, SL96a, SK99, Slo98, Ste91, SIJ93, VGP93, Ver98a, VGP99, WH90, AFB95, Ano93k, AC97, Bu98a, Car97c, Car98, CWH91a, CWH94a, GBL94, Gru98, HLLC96, IVE92d, IVE95c, JWH98, LSS98a, LFSY94, LC96b, LC96c, NT94, NIS91, PFB98, RSH98c, Shp99a, UFC94, Wil93a, Woe97, Woo90].
Computer-Related [De 93b, De 98c].
Computerized [Iv91]. Computers [???97, BF99a, CWM *91, HM96, Kan96, Sch98c, CFW91]. Computing [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98a, ACM98b, ACM99b, Bak92, BDD99, BV96, Bra94a, CFK91, DDM90, DDM91, DDM99, DWW95, FPP99, GC98, GN95b, IVE94e, IVE96b, JWH95, Kon95, Law98, MMM *98, Mau94, MW99, NS98a, Pen96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b, BGT96, CWM *91, DDP99, FM91, FJ97, HK99b, HC95a, KG93, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFW91, PH91].
conditionally [Sta96b]. Conditional [DOR99, GK99a, KS97a, KG99].
Conditionally [Des99b]. Conditions [GS99a, Rus93b, Gua99]. Conducts [Law98]. Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95l, Ano96i, Ano96a, ??97, Ano97f, Ano97g, Ano97a, Ano98a, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BSH95e, CH96, Cha91, Cop95d, DD98a, Dah96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, H97, H98, IVE95a, IVE97a, IVE97c, IVE97d, IVE97e, IVE97f, IVE97k, IVE98c, IVE98f, IVE98e].
Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95l, Ano96i, Ano96a, ??97, Ano97f, Ano97g, Ano97a, Ano98a, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BSH95e, CH96, Cha91, Cop95d, DD98a, Dah96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, H97, H98, IVE95a, IVE97a, IVE97c, IVE97d, IVE97e, IVE97f, IVE97k, IVE98c, IVE98f, IVE98e].
Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95l, Ano96i, Ano96a, ??97, Ano97f, Ano97g, Ano97a, Ano98a, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BSH95e, CH96, Cha91, Cop95d, DD98a, Dah96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, H97, H98, IVE95a, IVE97a, IVE97c, IVE97d, IVE97e, IVE97f, IVE97k, IVE98c, IVE98f, IVE98e].
[BDHK93, MZ98, Sch95f]. Conferencing
[Ano99e, KBR97, WW98a, Lam99].

Confidence [Chi99a, Chi99b, Grax].

Confident [Jan95].

Confidential [Bet95b, Bet95a, vD97].

Confidentiality [Ano98j, Jac96, Riv98d, ZG96, FT95, MI90].

Configurable [VMS97b, VMS97a].

configuration [HI97].

Conformer [Oka94, Cha95b, MS98b].

Conflict [All97].

Conflicts [ACM94b].

confounder [BTD98].

Confrontation [Zaj97].

Confusion [GC97].

Cong [Mye98].

Congressional [Smi97a, UU97a].

Congruence [Sch91a].

Congruential [Kra90].

Conic [Cao99, Mra95].

Conjecture [Jia99, GHS93, Ill94].

Conjectures [KP95].

Connect [Lic94].

Connection [Kas96, CV99].

Connectivity [Pit96b].

Connectives [KP95, Sim94a].

Considerations [Cra96, Hub91, Mos98, Bas95, Bou94, SY92, YS99, Bou94].

Considered [LT91].

Considering [HH94].

Considers [Ano95].

Consistency [ZYR90].

Conspiracy [WK97, Sch92].

Constitutional [Bas95].

Constrained [Gol96b, Has99].

Constraint [SG95, WS99, GMLH94].

Constraint-Based [WS99].

Constraints [DS98b, Ou99, Koz96].

construct [Lon92, Sun91a, ZB98].

Constructed [Ras93a].

Constructing [Ada97a, AB99a, AB99b, DT93, Gal99, KTM+99, Kok91b, XI98, ZK96].

Construction [BCK96e, BR99a, BR99b, CNST98, vD95a, DS99, EM93, GSPSW98, Job94, Kim93, KYDB98, NR98, SVXW91, ZMI90, BCK96a, BCK96b, BCK96c, BI93, MPL99, OS91, OS92, Pet91, vD95b].

Constructions [AHV98, ABDS96, KRS99, SNW98a, vHPP93, MS98b, SC97].

Consumer [EE97g, EE98c]. 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].

Context [DDJ98a, EMNN98, HDB99].

Context [COZ99, MM96a, Des90b, Des90a, III94].

Context-Based [MM96a]. context-free [III94].

Continue [Ano96k].

Continued [KE97].

Continues [Ano97y, Ano97z, Ano98h, DDJ98d, Ano96l].

Continuous [BP95a, NHB98, She95a].

Continuous [AF99, BB9C, CC9D, DFT97, FY99, FL96, Hwa97, JPLI99, Kas96, KAA99, KKW99, Lin98, Mey96, NW98, NAA99, NS98a, PRAM98, Per99, STS99b, She93a, She93b, Sim90b, Sim91, ZH98, ACC99, Ano93d, BGT96, CWM+91, CS96b, CS97b, CW94, LL93b, LM93c, Mat91, MLA91, RO96, RT93, SS96, Uni97d, WW99].

Controllable [CTT94].

Controlled [GPR98, GO96b, Gol94, Jak99c, SKBxx, GM91, GO95, Men95b].

Controller [CIBM99, FCH99].

Controls [Ame96b, Ban94, Cll97, UU97b].

Controversy [Law98].

Convention [Ano94d, Ano96a, Ano98f, IEE96f, NIS92].

Conventional [PR98a].

Convergence [GC97, Mos98].

Conversation [Woe97].

Conversational [LTEH99]. conversion

[Sab94].

Convert [Pet98].

Convertible [BCD91, DP96].

Convolutional

[Cha99c, JJ99b, TY94].

Cool [Ano99c].

Cooperative [Oh99].

Coordinating [Lee99b].

Coordination [COZ99, FL99a].
Vau98c, Vv97, Ver95, WSK97a, WSK97b, WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Wie90, Wie90b, Wie90a, WBDY98, YL99, YLH98, ZY91, Ada92, Alv98b, BSN95, BB94, Ber93, BS90a, BS91e, BS91f, BS91g, Bik92, Bik95b, Bik98b, BK98e, Bir99, BD95a, Bowxx, Bur98a, CV95, CD98a, Cra92, DYL98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, Gol95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kab98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LS98a, Lew92, Mat93, Mih96, Mil92, Mor92, NS97c; cryptanalysis [O'C95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZY90, ZH90]; cryptanalyst [Rey96, Rey97, Rey99]; Cryptanalytic [Gla99b, KSWH98d, MG91, vW99, Bih94a]; cryptic [Wri98]; CRYPTO [Fei91, ACM94b, Ame96b, Bar93a, Bar93e, BE90, HP98a, HMvT94, Koo97, LKB+94, Mih96, MPPS95, Neu97, Sch88c, Way95, Way96b, Neu95, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol98b, Kab97c, Kob96, Kra98, MZ98, MV91, St93b, St94, Wie99, BC98, Bra98, Bri98, CP91, CR98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kab98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, St98a, Wil98b]; Crypto-Chip [HMvT94]; Crypto-Coprocessors [HP98a]; Crypto-Engine [BE90]; CRYPTO '91 [DBGV93]; Crypto'95 [NS98b, NS98c]; CryptoAPI [Boy98]; CryptoBytes [Cr95, Riv95c]; cryptochip [PP96]; cryptograms [Har94, Web93]; Cryptographers [WP90]; Cryptographic [AG98a, AG98b, IBM93, Ano96f, AB97, BDPSNG95, BDPSNG97, BH93, BY93a, BGM97a, BGM97b, BBT94, BMT96, BFKL94, Bol98a, Bol98b, BDL97, BDP97, Bra95a, Bra96, BD91, CS96a, CJR98a, CJR98b, CPOR97, CF95, CD99, Cop94b, Cre97, DGV92, DC98a, Dam90a, Dam91a, Dan95, DIF94, DY90, DY91a, DY91d, DY91b, De95, DS97a, DF91c, DK91, ECD+99, El98, FGR92, Fis98, FGY96a, Fun97, GI99, GS94a, GK99a, Go96c, GS97, GQ95, Gut99, HHT93, HHT97, He98, Hwa97, I96, I96e, J97, JD91, KM98a, Kal98f, Kal98d, KV94, KS99, Kha93, KP99b, KT91b, KT98, KS97b, LM JW93, LL97a, LHB96, LM96, Mac94, MM99a, Mau96b, Mau97b, MS90a, Mil96b, Mjo93, Mos98, Mun91a, Mun91b, NM96b, Ng99, NS99b, NR94, NK98b, Nur94, N99s, ÖPH+99]; Cryptographic [Oka93a, OS98, PS99d, PV97, PS96b, PBGV90, Pre93a, PGV93a, Pre93b, Pre94a, PBD97, PRB98b, Pre98c, PRB98a, Pre99, Pre94b, QV90, QG95, RSA93d, RS93, Ritxx, Rue93, Si94, SZ96, Sak96, DY91c, Sch95f, SK96a, Sch98d, Sch98a, Sch91c, Sch93f, SPS97, SZ93, ZZ95c, Sha99a, Sch92d, SBVG99, Smi90, SY92, SM91, Ste96, T+99, Tou91, Tou93, TY9H96, VCF+90, V9g8, Way95, YS99, YY97c, YY98a, ZZ95, ZMI91, AN94, AG97b, AG97c, AG97a, BD92, Bol97, BV97, Com94c, CD95G, CI99, DD95, Dan97, Dhe98, Di99, DHFR91, Don98, FGY96b, Fro96, FL93, Gol96a, Har91, Hof95, IS99, Jenxx, JW01, JP96, Kob91a, LRW93, Lai95, Lea90, Lev91, LL93b, Lub96, Mau91c, Mea95, Mol98, Mu92, IPNdbbpprm91, NT93, Ny98b, Pau98, PK97, Ros97c]; cryptographic [S93g, ZZ94a, ZZ95b, Ste99b, Way98, WN94, XZZ97, ZZ98, YS91, ZZ97, ZL99]; Cryptographic-Token [N99s]; Cryptographical [KP95, Gy98]; Cryptographically [BDS98, Cha90, CvHP91, H194, PGV92, ZZ96, DT93, IS97, KSB96a, MCD98b, SKB97, B94]; Cryptographically-secure [Bou94]; cryptographiquement [Bou94]; Cryptography
[ANS97, ANS98b, Ano99h, AA93, ABDS96, Avp98, BCE94, BCG94, BGG95, BGR98a, Bel98, BB94b, BEE92, Bir98, Bla93, BK95d, BL96b, BL96a, BGV93, Boy95a, Bra90a, Bra94a, Bus97, Ca唐代6b, DDJ98a, DL96, DP98a, DP98b, Dar91, Dar96, DG96, De 93c, Des94a, DHH98a, DHH98b, Des98c, Dif90, DD91a, Dro96, Dwo97, Ele99, Er99b, Fer97, FSB97, FJM+96, FJRS96, FGLP96a, FGLP96b, Gan93, Gem97, Gol95a, Gol97a, Gol97b, Gon98, HK99a, HP98a, HSSL99, Hat96, Hed97, HL93b, Hir98, HAH94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLM96, HH98, HBKL99, JR96, JM97, Kal97a, Kal98c, KS98a, Kal99, KSS+92, Knu98a, Knu99, Knu99, KA91, RSA93f, Lac93, LM94b, Lin96a, Los97, MY91, Mau99a, Mau99b, Mau97c, McC96, MP91, Mit92b, MK98, NC97, Nic98a, Nic98b].

Cryptography
[PKA+98, Pat96, Pfl95, PT95, PGCSN96, Por91, PB99b, RSA99b, Rad97, Rhe94, Rit99, Riv90b, Riv93b, Riv97b, Ros96d, RK99, Sal99, DP91, Sal99a, SKBxX, SSS98, Sch94g, Sch96a, Sch96b, Sch97a, Sch97b, SSS+98, Sch98f, Sch94b, SV93, SG96a, She93a, She93b, She93d, Sni94b, Smi97b, Sta99a, SW95b, Ste91, Sti95, Sti98b, Sat99, SW97, TN96a, TN96b, Tv92, Tow98, Tsu92e, Wad99, Way96a, Wol99, Wol93b, Wor96, WC97, YWC97, YYY97, YYY97a, YYY97b, ZYWR91, Zim98, dRHG+99, Uni96c, AA95, Acc97, Ada91, Alv98a, Ano97q, Ano97-30, ASM98, BH98, Ban94, Bea97a, BR96b, BFS92a, BFG92b, HBR99, BW97, BMP+97b, BSS99, BBS98b, BD98b, BC96b, Com96, Con99, Dam96, DDB95a, DDB95b, DVL96, DiFP96, DNS91b, DN95b, Eng99, Far93, FMR91, FM91, FMM93b, Fra99, Fra93, Fri96].
cryptography
[Gar96b, GZ91, Gol99a, Gol97c, Gre94, GTGW94, Hr97, Hru95b, Hwa91, Hwa93, IZ98, IZ99, Imp92, Joh97b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdL98, Luc95, MB94b, Mau93b, MY98, Mei96b, MV97, Mic97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Nyb94, Org98a, Odi94b, PG97a, PG97b, PC98, PP92b, PV93d, PR98, Riv98c, Rot95a, Sali90, Sal96, Sch92e, SSM+97, SMD+99, Sch99e, Sch90c, Sch97c, Shp99a, Shp99b, Sin99, Siu99, Shu98, SMS99, Sta96d, Ste98a, Tas98, TM99, USE96e, Woe97, Wol93a, YL93, yan98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wai99a, v97, Sha99a].
cryptography-dedicated [NM96b].

Cryptography-in-the-Large [Bla93].
Cryptoki [ANO96k].
CryptoLib [Mac93].
Cryptography [Ers99, DKK+98, Jol98].
cryptologic [RK98b].
Cryptologie [Bra93b, Bec90, Sch98e].
Cryptologist [Pin98, Sel94].
Cryptology [Ano93g, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dam90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhee3, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ano97t, Bau97, Bec98, CW94, Cop95b, Cop95d, Dam91a, Dam99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Goli90b, GQ95, Hel94, IR93, Jol95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mau96b, McC90b, Mei92, MV91, New97, Nyo98, OiDP98, PSN95b, QV90, QG95, Rat96, Rue93, Sce92, SP90, SZ93, Seg92, Ste99b, Uni94c, Unixxb, Uni95b, Web93, Wie99, Wil98a].
cryptology [Bec97].
CRYPTON [DB+98, Lim98, Lim99].
Cryptonomicon [Ste99a].
Cryptoprocessor [Pan99b].
cryptos [Hag98].
cryptos [MMI97].
Cryptosystem [AMV90, BI95, BDGI98, Ber97c, Bih91, BMS94, BLE97, Bon99, BM97, CC99b, CG99, CJS91, CS99b, CW91b, Cus97, Gib91, Gib96, GC91, GC94, GGH97a, Gys96, HD96b,
cryptosystem [Miy90, NS97c, NS98e, OU98b, Ole95, Ped91c, Roe99, SW95a, SH95a, SH95b, SM90, SS95b, SS95c, SX90, TY92, Tan90, TCC97, TC99b, TC99a, Ven92, Wu92, XLP99, XW97, Yu92, Žer96b, Zha91, vT90].

Cryptosystems [BDHJ98, BHSV98b, BHSV98a, BS91b, BLM94, BS91c, BS97a, BS90b, CGJ+99, DP98c, ESST99, FY98a, FY98b, FY99, GJKR99, GPCSN96, GGH97b, Gor93a, HGS98, HMV93, Hes97, HR90, Iss90, Kal97a, Kal98a, KM99a, KM99b, KM99b, LK93a, Len99a, Men93, Men95a, Mic93a, Mic93b, Miy93b, MOM91, MM98a, MM98b, vO91a, Pai99a, Pai99d, Poi99, RY97, Rud91, Sma99, Son99, dWQ91b, Wie98b, WZ99, Yam98b, YJ97b, YY99b, dWQ91a, vO91b, AA99, Ale92, And94b, APDS93, BC90, BS91a, BS90a, Bih92, BF96, BQ97, BBL95, BK98g, CZ90, Ca99a, CC99b, Cha95a, CL97a, CNST97, CLL99, Con99, Des90b, Des90a, DF90, Des93, ES97, FK94, FSS94, FGM97a, FMR99, G909c, GH99, GP97, Has99, HNM98, Hor99, JM96a, Jan96, JQ98a, KM99a, Kob90, Kob91b, Koc95, Kos97].

Cryptosystems [Kos99, LL96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99e, Moo92, MVZ98, NM94, NY90, Odl90, OS91, OS92, Rac90, SS98a, SS98b, SS95a, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YYW99, YY98c, Zho94, ZPY96, vO92, vT94, Wal98].

CS [Ano93e, Ano94a, Pin98, SV98, Vau99b, Vau99c]. CS-cipher [Vau99b, Vau99c, SV98]. CSP [DS97d].


cunning [Ben94]. Cunningham [YY98a]. Current [JJ98c, RiI96]. Curve [AMV90, DP98c, Dem94, ESST99, Fer99b, HSSI99, Kal97a, Kal98a, KM99a, Kob98c, Len99a, LD99, Men93, Men95a, Miy93c, OFF93, RY97, SOOS95, SW93, WZ99, AMV93, AS98, BC90, FMR99, GP97, HNM98, IKNY98, QJ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LLH96, MV90, Miy99, SX90, VZ97].

Curves [Ano93a, BS91b, CTT94, De 98d, DMPW98, He97, JQ97, JM97, KMOV91, MS93, MM96b, Miy96, SNN99, BGR94, BBI90, BS91a, BSS99, CPPK98, CTT94, Eng99, FR94, Gal99, GLV99, G99b, IS99, Kob91a, Koy95, KK96, Ler97, Mao91b, MV93, Miy93a, VZ97, XL98, ZI98].

Curvilinear [SCG99]. Cusick [YT96]. Custom [Nor95b].

customer [Nor95c]. Customised [GN95c, HHD99]. Customising [NO96].


cyancide [Mar98b]. Cyber [Ano97i, Ano97-29].

cyberbanking [Mur96]. CyberMall [Mar95a].

cybernetics [LS98a].

cyberpunks [HM91, HM92, HM95].

cyberspace [Zim96b].

cyberspace [Ber97b, Col96, Gar97c].

cyberwar [Kan96]. Cycle [GAGCDAFC99].

cycloptic [PS97].

cycling [GS99b].

cylindrical [SW95a]. Cyclotomy [Boo90].

cylindrical [SW95a].


Dan [PNdbbbprm91]. \textit{Dark} [YY96]. \textit{DASS} [Kau93].

Data [All97, Ano92c, Nat93b, Ano95f, Ano96c, Ano97e, Ano97f, Ano97g, Ano97a, Ano97w, Ano97x, Ano98a, Ano99c, Ano99a, AVW99, BGML96, BRS99, Ber98, BS95b, BS98, BY92, BW98, BKZ98, Cle96, Con99b, CH99b, DC98c, DFGH99, EKLM99, Ga990, Gre90, Gu997, HS96a, Int91b, JMLW94, Kop97, HK98b, LvdLB96, LT98, MPSS95, MSH99, Moc97, Nat93c, Nat93a, NHB98, OA94, Sch99b, Sch94m, See97, Sme97, Sto90, SZT96a, TYD99, Tay90, TLS99, Way91, WSFC99, We95, Whe94, YY91, ZTR99, Ano93k, Ano95k, CCN95, Cha94b, Cli99, CS99, Cra96, Dan99b, DF97, Gil97, GTGW94, Gut96, Hel93, KAK96, Lam99, Los97, MS990, Mic97, Nor95b, PD99a, Rev91, Ros94, Rot97, Sch92a, Sch98b, Su98, Tha91, Tv92, Uni96a, Vad95, Way93c, Way95, Woo90, Yu92a, ARR99].

Data [Ano97v, Bar91, BS93b, Bir95, Com94a, Cop94a, Deu90, HK98, HK99d, Joh90, Kap98, KM97, Nat94a, Nat94b, Nat99a, Pai96, Per91, RP94, She95b, She92g, Sim95, SB92, Wili93a, Ano94h].

\textit{Data-Dependent} [Con99b]. \textit{Data/Image} [Sch99b, Sch98b]. \textit{Database} [AKF94, BDP9959, KT96, LCL92, Ou99, SJ97, Wat99, HY95, IS97, Lee95].

\textit{Databases} [BDPS997, CP93, GM99b, KB92, Len99b, PF94, RZ99, SG99b, Har90, Wad93, Ano95k].

\textit{datagram} [PSB97]. \textit{Datamation} [CWM+91]. \textit{Date} [GN95c]. \textit{David} [Ers99, Bar05]. \textit{Davies} [BB95b]. \textit{Dawson} [Roe99]. \textit{Dayton} [Dal97]. \textit{DC} [USE99a]. \textit{DCE} [Cas95, GH95, Kon95]. \textit{DCI} [Pin98]. \textit{DCT} [BBC98b, BBC98, HW98a, PBBC97, TA97]. \textit{DCT-based} [BBC98, HW98a, PBBC97, TA97]. \textit{DCT-domain} [BBC98b]. \textit{DDJ} [Con99a]. \textit{Deal} [FW91, Kn98c, Luc98a, Luc99a, Luc99b, Out98]. \textit{Dealer} [Rab94, BGS95]. \textit{Dealing} [Bec99, MSN99]. \textit{deals} [Joh97b]. \textit{Death} [CFK+91]. \textit{Deavours} [Ers99, CFK+91]. \textit{Debate} [Ano96f, Dum94, Uni98j, Wei91a, Wei91b, Fre94, Ho95, Ne95, RKD94, Tho96, Uni98k, Hat96, Wai95]. \textit{Debating} [Ano92b]. \textit{Debugging} [Wot99]. \textit{Debut} [Gar98b]. \textit{December} [And94a, Boy95a, Boy95b, Bra93a, CW94, Con99a, Dar97, Far93, IEE92b, IEE93c, IEE94c, IEE97b, K939, Org98a, PSN95b, Pre95a, SZ93, TV92, Wal99a, WN98b, Zim96b]. \textit{Decentralized} [BdM94]. \textit{Decidable} [BR99]. \textit{Deciding} [Ano96f, Dum94, Uni98j, Wei91a, Wei91b, Fre94, Ho95, Ne95, RKD94, Tho96, Uni98k, Hat96, Wai95]. \textit{Decipherability} [CGV94].


DESII [Ano98c]. DES-Like [Kim93, KP93, Way93a, BS90a, BS91c, CCZ98]. DES-X [KSW97a, KSW97b]. descent [Jen99].


Descriptions [PNFK95, Sar99]. DESE [SM96, SM98b]. DESE-bis [SM98b].

DESEO [HCDC99]. Desiderata [Lee99b].


SBTV99, VNM99, WL94, YS99].
Design-Space [KV99]. Designated
[Cha95b, JMSI96, Oka94]. Designed
[YY98d, YY98b]. Designer [MUSM98].
designers [FM98b]. Designing
[AKF94, BV98a, BK95c, BM94b, CH99b,
DL99, DMVC99, Ger99a, Gor93a, HJ99,
JS93a, Kem99, PM99a, PD99b, Sch94c,
SW97a, SW97b, SZZ94b, Ste94a, SAS99b,
TLS99, Zhe90, CG05, Hor99, HLC99].
Design [DJHP98, FY95b, Jun96, KK95,
Mou99, RB99, Wot99, Ton96]. DESIRE
[JKVP99]. Desk [GRB99]. Desktop
[Ano97r, Fuc99, Los97]. Destination
[LTEH99]. Destruction [SY98]. DESV
[CCN95]. DESX [CCN95]. DESX
[Log96]. Detail [Zeg93]. DeTeBerkom
[GH96]. Detectable [VvT97]. Detecting
[Gor93a, Mad92, PM98, SG96b]. Detection
[BS95d, ENK99, HCD99, Hur98, LH93b,
LKD98, LT98, LML98, Ruo94, TYD99,
ZTR99, HC96, MHMW98]. Determination
[Bie98]. deterrence [van96]. Developer
[CM99b, Di 97b, DT98b]. Developing
[CF95, SCT99]. Development
[Ano97h, Bar99, Bas93, GRB99, HNSS99,
IR99, LL93a, Nat99c, Natx, VDDR99,
Way98, You96, AMV93, Ano97-30, LS98a,
Mil95, NBD+99, Sta97c]. developmental
[Ram92]. Developments
[Ano95a, PRB98a, Sim97]. Deviates
[Ran01]. Device
[Hru96, Ano91b, CM97c, Uni94b]. Devices
[BDH98, Hwa92b, Hwa92c, LS98a, Pos92,
Pos93, Uni94a]. devoted [FT99b]. DFC
[KR99a, Ste99c]. DGSA [FM98b]. DHCP
[Dra99]. DHWM [ADF98]. Diagnosis
[GX99, MR95a, PW99]. Diagnostics
[RSS97a, RSS97b]. Diameter [FP99].
Dickson [Pie93]. DICTA [KG93].
DICTA-93 [KG93]. Dictionary
[Jas96, Luc98b, BCR98]. Dictyostelium
[Ram92]. Diego

[ACM93b, IEE97b, Sch98b, USE96f].

Difference [LP94]. Different
[KPRS97, Sch99h, RT93]. Differential
[BB94, Ber93, BS90a, BS91c, BS91e, BS91d,
BS91f, Bi92, BS93b, BS93a, BS97a, BK98d,
BKPS93, CJ98, Con99b, Dae95, Din94, Fer98,
Haw98b, Haw98a, KTM+99, Kau96, KM98b,
Kob99, KJ99, Kwa93, LMM91, LH94,
Lan95, Mat96a, Miy93c, MS98, NK93,
OM94, Pai99a, Sch96c, SM98a, VKR98,
Wag98a, YLH98, Ada92, CV95, KY95b,
KYxx, KM96b, LMM92, O'C95, OG95,
RP95b, TN97, Way95, YT95a, YT95b].

Differential-Linear
[Haw98b, LH94, Haw98a, Lan95].
Differentially [Nyb94]. Differentials
[BB99a, Fer99a, KR99, BBS98a].

Difficult [KP96b, Riv93a, ZZ96, Hor99, Riv95a].
Diffie [BY93c, BY93b, BR99, BWM99a,
BV96, Ben98b, Bon98a, CS97, CS97d,
HY98b, HY98a, Kaj97a, Koc95, Koc96b,
Lut98, Mau94, MW96c, MW96b, MW99,
RSA93b, Van95a, VW96, WM93, vOW96].

Diffusion [Mas99b]. Digest
[FH97, GTG94, Kal91, Riv92a, Riv92b,
Riv90a, Riv91b]. Digit [TK99].
Digit-Recurrence [TK99]. Digital [Ame95,
Ame96a, ANS98b, Ack98, ALO98, AW94,
AR97, Int91a, NIS94, Ano96e, Ano97-29,
AS98, Aur96, BC90, BM99a, BM99b,
Bm94d, Ber97b, BM94a, BM96a, BM96b,
BM96c, BS95b, BS98, BTH96, Boy97, Boy98,
Bra93a, Bf99, BF99, Car95, CR91,
CPO+98, CHO+98, DDM98, DDM96,
Eli99, EGM90, EGM96, FFW99, FKMY98,
FBS98, Fri93, Fro97, FOM91, Gar97c,
Gar98b, GR97, GDD+97, GB98, GO96c,
GQW+91, HKS95, HG96, HG97e, HEG98,
HA96, HW97, IEE97c, IEE98d, JLO97,
Jue99, KKS97, Kob97, Kob98c, Kra93,
KH98a, LQ99, LM95, LW96, LL98, Lut98,
LR98, MS96, Man98, MMST98, MB99a,
MW98b, Mer90b, Mer97, MT97, Mos98,
MBW97, Nat91, Nat94a, NH98, NMV98, NIS93a, OO93, Oht96, OFF93, Oko96, Per97, Pet98, Pf99c, PW93b, PG93c.
Digital [RDK98, dR94b, Rot95b, SC96a, SCxx, Sch93c, Sch94d, SK97b, SK97a, She97, She92e, Sim93, SB93, SY98, SH98, VP98, VNP98, VP99, Web98, WD96, WD97, WL99, Woo90, YK98, Yeu99, Yeu97, Yeu98, YYH98, ZK96, ZKOY99, Zhe97b, vHH97, vTO94, AW95, Ano91b, BBCP98a, BHS93, BR96c, BGR98b, BCV97, BO96a, Bis90, BOD95, BM91b, Bur98a, Com97, Car97a, CH98, CLHL98, DD95, DMM98, DSS99, FC94, FB97, Gau90, HS91, HZ93, HW98b, Hwa93, Ibb97, Irw98, KG93, KAK96, KH97, Mar95b, Mau91b, May97, Min97, MBY97, Mu92, NMVR95a, Nat97a, Nor95a, Nor95b, ODB96, OP97, OP98, OP99a, Pit96a, RR97, Ros94, RDK96, Sch90c, Sch97c, SD97, Sin91, SS95b, SS95c, Tl98, Wan92a, Wil93b, Wu92, XBA97, XA98, Xie98, YL95b, YL95a, YEA98.
Digitalization [HA96]. Digraphs [HEQL98]. DIMACS [FM91]. DIMCS [WN98b].
dimension [LFCK99]. Dimensional [BP98b]. Dimensions [HEQL98, Sta97b]. Dining [WP90].
Diophantine [BMP94a, Cus95, LG97, LCL95, Lon92, Sun91a, Wan92b]. Diophantine-knapsack [Wan92].
diplomatic [Alv98b]. Direct [PP90, PWW99, MHW98, Un94b].
Directed [BM94a, LL97b, MT99b].
direction [Un95b]. Directions [AT99, Wot99, BFS92a, BFS92b, Gol97c, NM96b]. directly [BD98a].
Disco [WP90]. Discontinued [Ros98c].
Discounts [DDJ98e, DDJ98f]. Discount [BLM94]. Discourage [MUSM98, RZ99].
Diocesan [SI93a]. Discrete [ACM97b, BBT94, CH98, GJKR99, Gor93a, Gor93b, GM93b, GKS97, LO91a, Mau94, MW99, MVZ98, NT99, Odl94a, vO91a, PS98b, Sho97, Tes98, WD98, YY97b, vO91b, vW94, CPS95, CS97d, FR94, FR99, HZ93, HY93b, HI97, HMP95, Kob90, McC90a, NR95a, SS95b, SS95c, TG94, TK98, vO92].
Discreto-Log [GJKR99, YY97b]. Discrete-time [GKS97].
Discretionary [BDPSNG97]. discussed [Ano90]. Discusses [Gar97c].
Discussion [Ano99d, Ano99f, Ano99h, BS94, Chr99a, Mau93a, Mau97a, Sas99a, ADK90, C290].
Discussion-Trust [Ano99f].
Disenrollment [BBCM93b, BBCM93a, BC96a]. Disk [DF94, Gar98b]. Diskette [BE90].
Distillation [Slu98]. Distortion [SVBJ96]. Distributed [ABLP93, Abe99, ADF98, BHJM99, Bor96, BHKR95, Bur94c, CM98, DHMR96, DF91b, Dwo95, FM91, FK99, FY98a, FYM99, GJKR99, Gre94, GS97, GMV98, KL99, Kau93, Kem99, KRJ98, KYB92, LAB92, Law98, Mar99, MKS99, Muf93, NAA99, NKP99, Ped91a, PKM97, RZ99, Re92, RG95, Sch94a, SKW96, SS90, She92a, TV94, Wh90, WL92b, Be92, BP97b, FMY98, HK99b, Har90, LM98a, LAB91, Lie93, MS99c, TCH91, Wad93, WL92a, WL92c, Zim96b, BBN96].
distributed.net [Ano97]. Distributing [Re96].
Distribution [BR94a, BR95b, BDHK93, BFS96, Bur94b,
[KMA+98, Kob99, MT99a]. **EAP** [BV98b].

**early** [Alv98c, Mar96]. **Earth** [YHKI99].

**Earthcam.com** [Ano98j]. **Ease** [HJL99].

**Easier** [GMD98, BBR99, Sch98c, Way95]. **East** [Str95]. **Easy** [Sim94d, Ken95].

**eavesdrop** [Way93b]. **eavesdropper** [Al96]. **Eavesdropping** [RK99]. **Ecash** [Sch98h].

**ECC** [Cer97, Kal98e]. **ECC/DLP** [Kal98e]. **EccoFan** [PKA+98]. **ECCp** [BT97].

**ECCp-97** [BT97]. **Echo** [GLB96]. **eciphering** [Blu97]. **ECMA-219** [ECM96].

**ECMAST** [Dan96]. **Economic** [Mos98].

**Economy** [CFGS99, Org98a, Tas98].

**Ed** [DDJ98e, DDJ98f, MGL+98]. **Edgar** [Sha99a, Ros97c].

**EDI** [Len93]. **EDIFACT** [RCM99].

**Editor** [Hat96, Joh99, Bur98b, Ano95g, Ano95h, Ano96g, Ano97l, Ano97m, Pre95b]. **Editorial** [Eri99].

**eds** [Ers99]. **EEC** [BGV93].

**EEPROM** [FG98].

**EF** [KP95].

**Effect** [OD99]. **Effective** [Fuc99, Min97, MBY97].

**Efficiency** [Bas98, BM96a, CM99a, DKKK98, KS97c, Mar97, BHS93].

**Efficient** [AGS97, AGY95b, BBDW96, BDV93, BF97b, BF99c, BFP99, BDB92, CS97a, CMN99, CG99, CG98, CDD99, Cre97, DR99a, DT98a, DN94, FH94, FOM91, GSY99, GJK96b, GP97, Ho99, Hwa92b, Hwa92c, JMO95a, JO97, JMP98, LHY93, LLH96, LL99, Len99a, MSNW99, MS93, MLL99, OS91, OS92, OFF93, OSA91, PS98b, Sch90b, Sch90a, Sch91c, Sch93f, Sha94, Ste98b, Ueh95, Wie94, Wie96, Wie97, Wie98a, Zim99, dR95, D95b, CPP98, CGS97, Dhe98, FMY98, HK90, HJ99, KC95, KSK96, MI90, MS98b, PPKW97, Per91, Pf95, Sch93g, Sha95a, SKB97, VNM99, Von92a, Von92b, Xie92, ZI98].

**Efficiently** [Jas96, Bak92]. **Effort** [Natxx].

**Eigenvector** [MVL98].

**Eighth** [AX98, BLP94, FFP99, Uo95b, BLMO94, Cha92b, DB99, DT98a, EO95b, EN98, En99, HS97, Hir93, JT97a, LHB96, Lin93a, Lvd98, LKD98, LR98, Max94, MZ98, O900, Ped95, PW97c, Riv97a, STS99a, STS99b, SB97, Sch99i, Sin98, TRS9, Ta99, USE95e, USE96d, USE96b, USE98b, V98, AMS96, AC97, BH98, Com97, Cha92a, DM94, DSS99, DF98, EO95a, FB97, Ken95, LM98a, Lin88a, Lin89a, Man95, M92a, RP97b, Sch93e, Sch95d, She96a, VNM99, Way93b].

**Electronically** [Ped99].

**Electronics** [IEE97g, IEE98c].

**Elegance** [Sch99c].

**Elektronicznej** [Sch95e].

**Elementary** [Mil92, Tat98, Tat99].

**Elements** [FC99].

**Eleventh** [CH96, IEE92d].

**ElGamal** [AA99, Ble96, KSK96, LK96, NK98a, TY98b, TY98a, V979, Zho94].

**ElGamal-based** [TY98b, TY98a].

**Eliminate** [Riv98b].

**Eliminating** [GGH97a].

**BLM99].

**Elizbeth** [Uni92].

**Elliptic** [AMV90, Ano95n, BS91b, BSS99, CTT94, De 98d, DF98c, DMPW98, Dem94, Eng99, ESST99, Fer99b, HSSI99, Hes97, JQ97, JM97, Ka97a, Ka97g, KM99H9, Kob98c, KMOV91, KT93, Len99a, LD99, MS93, Men93, Men95a, MM96b, Mi93a, Mi93b, Mi96, Mi99, OFF93, RY97, SOOS95, SW93, SSNP99, VZ97, WZ99, AMV93, AS98, BGR94, BC90, BS91a, CNST98, CPOP98, FMR99, Gal99, GK99b, GP97, HNM98, IS99, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LL96, Ler97, Mau91b, MV90, MVZ93, SX90, XL98, ZI98].

**Elliptic-Curve** [Fer99b, Kal97a].

**EMACS** [MC92].

**email** [Kar96].

**Embed**
Ril96, Riv95d, RKD94, Rot95a, Sab94, Sch98b, Sch94i, Sch98c, Sch99j, She96a, Sme97, Sta97a, SW98, SW99a, Str93a, Str93b, Suf98, Sun91b, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vad95, Vau98e, Ven90, Vu95, Wad98, Wel95, Wh93, Wil93a, Wil93b, Woo90, You97, You96, Zer96a, vOW91, vT93, Ano98j, Ano93j, Hon98J.

encryption/authentication [Sch99j].

encryption/decryption [Hat97, Vu95].

Encryption/MAC [Yuv97].

encryption/multisignature [HCC98].

Encryptions [Mv93].

Encrypts [Ano93k].

Encyclopedia [CFK +91, New97, UFC94].

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

End-to-End [NH90].

endlicher [Wal98].

Ends [McC90b].

Endured [Che92].

Energy [DFL99].

Enforce [BDS98].

Enforcement [Cae96b, Cli99].

enforcers [Way93c].

Enforcing [Ano97n].

Engine [BE90, CM98, She92d].

Engineering [Ano98f, DFGH99, EKLM99, IEE96d, LBHM99, SSSW98, Sm98a, AN94, IEE97k].

Engines [T+99, Way93a].

England [ES98, Cur98].

Enhance [FO99a].

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

Enhancement [HWJ98, Lin93a, Lin98a, Lin99a].

Enhancements [JM96b].

enhancing [HY95].

Enigma [CWM +91, Har96b, Kip97, Kip99b, Ob99, Ano91c, Bl98a, Bl98b, Bl98c, Cra92, Kah91a, Kah98a, Kip97, Kru98, Mlf96b, Mus92, Tu99, We97].

Enigmas [Gad91].

Enjoyable [CM99d].

Enough [CFK +91, Dea98b].

Enschede [Hei96a].

Ensuring [Com97, Rot95b, ZG96, Way91].

Enter [Wor96].

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

enterprise-wide [Wad93].

enters [Joh98].

Entities [KM99c].

Entity [BR94a, BWM98].

Entrepreneur [Pin98].

Entropy [Bro94, EHMS99, KSHW97, KSHW98].

entwerfen [Hor99].

envelope [SOB98].


Environmental [RS98c, RS98d].

Environments [GSTY96, SKAM99, DNS99].

EPIC [Rot95a].

EPS [Ano96i].

equally [Ito91].

Equation [Cop95c, LG97].

Equations [Por98, RZ99, BMP97a, Cus95, GK95b, LCL95, Lun92, Sun91a].

Equilibria [Ett98].

equipment [Int91b].

Equitable [BDS98].

Equivalence [BS99b, BS99c, Fis98, KK98, Man94, AD97, AD99, LDW94].

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

Era [DDJ98c].

Ergonomics [DDJ98c].

Erika [Mat99].

Errata [Con99a].

Erratum [Ano91a].

Error [AW94, AR98, BGS96, Cha99c, DLR97, KKS97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, DL99, Jv98b, Ste95, Wan92a, YL97a, vT94, CW94].

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

Error-Correction [MG91].

Errors [GGH97a, SHK99b].

ESA [Sp95, YS91].

ESA/390 [YS91].

ESAT [PGV93d].

Escrow [AAB +97, Bla96c, BDS98, Cae96a, CGM97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fre96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, LWY95, Mah96, Mar97, MS95f, MK99, Nec96, SYM98, Sun98, SM95a, VvT97, VBD99, YY99b, Ano94e, BDH97, BR96b, DH96a, Des95, Fre94, KL94, Mao97, Uni95a].

Escrowed [Bas95, Com94b, FIP94, Nat94d].

ESIGN

[AW94, GM97, LHL95b, LHL95a]. Forget [DFIJ99]. Forgotten [Ano97t]. Form [Cha93, STP93]. Formal [BR97a, BFN98b, Bo198a, Boy92, GFB93, Gue98b, Mea95, PD99b, SM95b, Tou93, WK96, AHdJF97, AAPS92, Ata94, BFN98a, JW01, ZLX99]. Formality [ACD94]. Format [CDFT98, Nys99]. Formats [ASZ96]. Formed [Gar97c]. forms [Mok97]. Formulae [KV94, WD99b]. Forty [CWM+91]. Forum [IEE98d, MB99a, Org98a, Ano97c, GO96c, KSS+92]. Forward [BM99a, BM99b, CadHSV96]. Forward-Secure [BM99a, BM99b]. Foundation [Gol95a]. Foundations [Ada91, BDFM99, Gol97a, Gol97b, IEE92a, IEE96a, IEE96b, IEE97f, IEE98a, IEE99a, JR96]. Founder [Pin98]. Four [HKQ99, Koe99, Riv91a, DL95]. Fourier [MS94, NA95]. fourteenth [IEE95c]. Fourth [OW95, Uni96b, Far93, IEE93a]. FRG [Oht96]. Friedman [Uni92]. friendly [Bus96]. Friends [DDJ98e, DDJ98f, Sch92b]. Frenkel [CFK+91]. Friendly [Bus96]. Fractions [Iss90, KE97]. Fractional [BD99b]. Fractals [DS96, SD99]. Fractions [Iss90, KE97]. Fractions [Gol95a]. Framework [Boy92, DGV93, Hed97, PS99f, PW99, SL99, WP99, Com97, HN94, LS98a, P996c, Tas98, DT98b]. France [Chr98, DEQ92, FR95a, GQ95, QG95, Vran98c]. Francis [Lea90]. Francisco [Ano97a, Ano98f, USE92a]. Franchia [IEE92a]. Franklin [W99a]. Fraud [Neu92, VGP93, Vr97]. Fraud-Detectable [VvT97]. frauds [Sga93]. Fray [Gar97b, Law98]. Free [BP97a, BHT98, BDI96, CD98b, Dob97, Eri97b, GJM99a, GJM99b, HBKL99, Rus93b, SK95, All97, BT94, Des90b, Des96b, Dob95a, Il94, Vran93]. Fraud-Detectable [VvT97]. frauds [Sga93]. Frey [Gar97b, Law98]. Free [BP97a, BHT98, BDI96, CD98b, Dob97, Eri97b, GJM99a, GJM99b, HBKL99, Rus93b, SK95, All97, BT94, Des90b, Des96b, Dob95a, Il94, Vran93]. Free-Space [HBKL99]. Freedom [Cae96b, Uni97a, Uni98c, Uni98b, Uni98e, Uni96b, U97a, Uni97b, Uni98f, HM96]. FreeNIX [USE98c]. French [Blo98b, Bou94]. Frenkel [CFK+91]. Frequency [BP98c, MSH99, Ano90, Tod97]. Freshness [KYG92]. FRG [Oht96]. Friedman [Uni92]. friendly [Bus96]. Friends [DDJ98e, DDJ98f, Sch92b]. Probenius [CPPK98, Graxx, KMK99]. FROG [W9599, W999b, GLC98, WFS98]. Front [Hed97]. Frontier [Bar93a, Bar93b, HM91, HM92, HM95]. FSE [Bih97c, Vau98c]. FSE'99 [Km99c]. FTP [SSF93]. Fujiiyoshida [IRM93]. fulfilled [Mar96]. Full [BS93a, DH90, SK98c, SK98b, Pos93]. Fuller [CFK+91]. Fully [BVD94, BVD96, HE98]. Function [BJY97, BDP97, BP97c, CP91, DBG93, DG93, Da95, DC98a, DDP90, Dob97, FGF96a, HIL99, HL99, MCD99, S999, PBD97, Sch91c, TOU94, AB96b, DK94, DDFY94, D999, FGY96b, KSB96b, KSB97, LTT95, MIZ98, MVZ98, PK997, Sch91a, SRR98, SS95b, SS95c, YL97c, ZPY96, d949]. Functional [Yam99]. Functions [AHV98, Ano95a, BDP99, BCK96d, BCK96e, BHS98b, BHS98a, BKG99, BGS94, BGS96, BM94a, BL95, BHT98, CDD99, Car93, DGV93, DY90, DY91d, DY91b, DFL99, ECM96, EPR99b, EPR99a, FBS98, GJKR96b, JQ97, KTM99, Kim93, KP96a, Kra95, LS97a, L979, LM93a, LM93b, LM95, MS99b, MS90a, Mer90a, Mer91, MS95f, Mil96a, Mon93, NR98, OS98, PW93b, PGV92, Pre93a, PGV93a, PGV93c, Pre97a, Pre99, Pre94b, Q909, Roe94, Sch91b, SZZ95c, S99Y, ZZ95, Zhe90, vW94, BSNP96a, BSNP96b, BD92, BGR95, BCK96b, BCK96c, BHH99, BK98f, CC98, CDG95, Cus96, CS96c, Dam90b, Gol96a, Gon95, GHS93, HSK97, HLMW93, HXM94, HYLT99, ISO97, JQ95, KL95b, Lai95, MCD98b, O'94, PGV91, PGV93b, Pre94a, PGV94, Pvo95, RP95b, Roe95, Rom90b, SZZ95a, SZZ95b, Sim98c, Tsu92b]. functions
[Ngu99a, Ngu99b]. Good
[Ano94h, AWV99, Elk96, Gar95b, Gar95a, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, Koh91a, Let97, Mei96a, SX90, Zim96a, Zim96b, Pin98]. Goppa [Gib91]. GOST [KSW96, Sch95b]. Goucher [Mus92]. Government
[RK94b, SG96a, Ano94h, Riv98c, Way93b, Wel95, Lee99a, Ros97a, governments [BH94]. Grace [GC97]. Gradient [Jen99]. Grail [Sal99]. gran [lPNdbbbprm91]. Grand [FBS97]. Graph
Guides
[Bac95, End97, WSFC99, Zim95a, Bis90, Jac90a, Jac90b, Nic99, Pre97b, Sta95b]. Guided [Mos99]. Guideline [Lee99a]. Guidelines [Bar97, CPOR97, Mer97, Ame95, Ame96a, Org98b]. GUMP [FBS97].
guru [Di97a]. gyi [lPNdbbbprm91].

H [Scu92, Lea99]. H-1B [Lea99]. H [WG97]. H.R [Un98c, Un96b, Un97b].
H.R. [Un97a, Un98b, Un98c, UU97a, Un98f]. hacker [Mei98]. Hackers [GC97, HM91, HM92, HM95, Mei98].
Halske [Dar98c, SeI98]. Hamburg [LM98a]. Hamming [She95c]. Hampshire [IEE92a]. Hand [BF99a]. Hand-Held [BF99a]. Handbook [Bac95, MV97, Sha99a, Ata99, Rey96, Rey97, Rey99].
Handles [Sar99]. Handling [BMS99, Dae98, HC95a, Mat91]. hands [Riv98c]. Handshake [Sim96b]. Harari [Ver95].
Harder [Sch97b]. Hardness [BV96, NS99b, DI99, Kha93]. hardness-amplification [DI99]. Hardware [ACD94, Bir98, BF99b, Bri90b, BS91b, Cla98a, DGV92, GN95c, Koc96a, OSA91, Wil93a, Wat99, YK95, BB95a, DN95b, Gai90, KP99b, LMS97, MZI98, Nor95a, Nor95b, Nor95c, NO96, See97, SN94, TY92, Way95, Zhe95b, Ku91]. Harmonic [RG99].

Hash [ANS97, AHV98, An93f, An95a, An95i, BDPS97, BCK96d, BCK96e, BS91c, BS91d, BDP97, BHT98, CP91,DBGV93, DGV93, Dae95, DY90, DY91d, DY91b, EPR99b, EPR99a, FIP93b, GHR99, GS94a, ISO97, KP96a, Kra95, LM93a, LM93b, LM95, Mer90a, Nat92b, NS93b, Nat95, PRZ99, PW93b, PV92, Pre93a, PV93a, PGV93b, PGV93c, PGV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sch91c, Sch93f, SV94, SRY99, Sta94b, Vau93,
Zhe90, vW94, AB96b, BSNP96a, BSNP96b, BD92, Dan90b, DK94, Gon95, HLMW93, HXMW94, HYLT99, JG95, KL95b, MZ98, PG91, Pre94a, PrO95, 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, Rog95, Rus93b, Sch91c, Sch93f, Sho96, Sti91b, TZ94, BGV96, Bosxx, Gih90, PIBM90, Sab94, Sch93g, Sta99b, ZPS93]. Hasn’t [Gar97a]. Hasty [Sch98i]. HAVAL [ZPS93]. Hawaii [???90]. Head [Ano94h]. Header [Atk95a, KA98a, MR95b, Ros93]. Heats [Gar98b]. heaven [Gol97c]. Heimdal [DW98]. Held [Ano96k, BF99a, Far93, Uni98f]. Hellas [IEE97c]. Hellman [RSA93b, BY93c, BY93b, BBR99, BWM99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY98b, HY98a, Kaj97a, Koc95, Koc96b, Mau94, MW96c, MW96b, MW99, NS97c, NS97b, Van95a, VW96, WM93, vOW96]. Help [GRB99, PAK98, AK95]. Help-Desk [GRB99]. Henry [CFK91]. Her [Ber96a]. Herd [Rit99]. Here [MK94]. Heterogeneous [DVPL92]. Heuristics [MCD98b, CMK99]. Heuristics [SBC99, CD98a]. HF [RP94]. HFE [KS99b]. HFX [LR96]. HGF [Uni94b]. HGF-94 [Uni94b]. Hidden [BL95, CJD97, KP96, KZ95, NS99b, Pat96, Sak96, PSB97, TI98]. Hide [SV99a, SV99b, SvS98]. Hidell [Scu92]. Hiding [Aue98, BGML96, BLMO95, CM97b, CD97, CDS94, GR96, GLB96, HS96a, MS99a, MO99, Phi96a, Phi98, RGV97, SC96b, SZT96a, And96c, Beu94, Bra90d]. Hierarchically [LE99]. Hierarchical [FL96, OOK91, CMPS97, GPCS96]. Hierarchies [Ruo94]. Hierarchy [Hwa97, YJ99b]. hieroglyphs [Wri98]. High [ACM98a, ARV99a, ARV99b, Ano99c, Ano99d, BCR98, Bia96a, Bia96b, BMS99, Chi99a, Chi99b, DP98a, DP98b, Ebe93, FVEA99, FP99, Gar97a, Gar97b, GN95c, HR90, IEE94e, IEE96d, IM93a, IM93b, Kap98, Ko94, Ko93, KB92, LS97, MPS95, MSHP99, Rus90, SKNO98a, SKNO98b, She92d, She95b, Sut99, VN94, Duf98, Graxx, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Uni96a, Yeu97]. High-Assurance [IEE96d]. High-Bandwidth [Bia96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Chi99a, Chi99b]. 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, IM93b, Ko94, MPS95, SKNO98a, SKNO98b, IM93a, Nor95a]. Higher [Jak99a, KMKH99, Lea99, MSK98, SMK98a]. Higher-order [Jak99a]. Highly [MS99b, PV97, ARK99]. Highway [Ano94c]. Hill [MCD99]. Hints [JM99]. Hiroshima [IEE96b]. Histogram [Mae98]. Histograms [BMS99]. historic [Bur98a]. Historical [Kob97]. History [Cal92, CFK91, DGT96, DKK98, Er99, Hig97a, Kah96a, Sim96a, Ano97t, Dav98c, Joh99, Kip99a, Mac98, Ros97a, Sim98a, Web93, CFK91]. HKM [LR96]. HKM/HFX [LR96]. HMAC [BCK96a, BCK96c, BCK97, 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].
Aho96a, Aho97h, Auc98, AR99, Bar94,
Bas93, BDGV93, BLMO95, BS91g, Cae98,
CFGS99, CW94, CFG96, Den99, DFMB97,
GRS96, HGHD98, HOQ97, Hei96a, HH94,
HR90, IEE94a, IEE97k, ISO97, KG96,
KRJ98, KM96a, LOX99, LBHM99, Lin96a,
Mau93a, MW96a, Mau97a, Mau99a, Mau99b,
MO99, Nys99, ODF98, Ori96, Ped91d, PL94,
Pi96a, Phi98, PIt96b, PB99a, PGV93c,
Pre98c, RSA93e, RSA99a, RIP95a, Sch97d,
Sga93, STP93, SC96b, Sti93a, Stu99, Uni98i,
Uni98k, VPM97, Wol98, Ada91, BDGV96,
BP95b, BDC95, Bra90d, CM95, CC95,
CKGS98, DL96, Dav98c, DF98, FM98b,
Gru98, Gua90, HW91, IEE95c, Jac90a,
Jac90b, Ken95, KS98c, KW92, Mar95b,
Mau93b, NIS92, Ped91b, Ped91e, Rot95a,
Schi90c, Sch97c, SG96b, Sim92, Tas98].

information

[Uni97c, WSFC99, van97a, GS94b].

Information-Theoretic

[Cac98, MW96a, Mau99a, Mau99b, MO99,
Ped91d, Wol98, Sga93, Ped91b, Ped91e].

Information-Theoretically

[Mau97a].

Informational

[Sga90].

Infrared

[DDJ98b].

Infrastructure

[HFPS99, Ori96, SS99d, VSH97, Ame95,
Ame96a, FB97, GH96, HMT98].

Infrastructures

[Ano99f, BPK99, BFK99, RCM99].

Inherent

[She94c, KSB96b, KSB97]. Initial

[Bih98b, BBDR99, SVB99, JI91].

Initialization

[YY99b]. Ink

[BD99a, JM99].

inka

[AHMS99].

Immarsat

[Ano99e, Lam99].

Immarsat-B

[Ano99e, Lam99].

Inn

[IEE92a, IEE94a, IEE97e].

Inner

[SvA98].

Innocuous

[CD97].

Innovations

[BPBV99].

Innovative

[PJ99].

Input

[BR99a, BR99b, Sah94].

inputs

[CHH97, CHN97].

inscriptions

[Lip93].

insecure

[Mit92a].

Inslaw

[Eri97b].

Instance

[BDPSNG95].

Instantiation

[SHK99b].

Institute

[Far93, IEE94b, Ber96b].

Instruction

[Cla99, SSS98, Ben94, Kuh98].

Instruction-level

[Cla99].

Instructions

[Ros96a].

instrument

[CWM91].

instruments

[Sch93e].

Insulator

[NFQ99].

Insurance

[Eri97b].

Integer

[MM98a, MM98b, Od99, vO91a, SM91,
vO91b, KM99a, Mao98, Pos93, vO92].

Integrated

[Ano96k, KV99, Smi98a, YS91, SY92].

Integrating

[Bol98a, Bol98b, GSY99, GL96,
LBHM99, LC96a, Rei92, Smi98a, AP93].

Integration

[Ala93a, Ano97s, CHLT99, CKN99, FO99b,
HGHD98, IH99b, NT99, Lee95].

Integrity

[BP95b, Ou99, RIP95b, RIP95a, VCF98,
Sim92, Tay94].

Intel

[Gar97b, GC97,
GO96c, KC97, GO96c, JK99, SW97a, SW97b, Wor96].

Inteligenz

[CWM91].

Intellectual

[BS95e, CFGS99, LQRS98, Ale98].

Intelligence

[AK99, Him93, Rat96, SW94b].

Intelligent

[AP94, CH99b, PD99b, SS99d].

Inter

[KMPS99, MB99b, TH99].

Inter-domain

[KMPS99].

Inter-protocol

[TH99].

Inter-working

[MB99b].

Interaction

[Abe99, Fuc99, Rud91].

Interactions

[KSW98a, KSW98b].

Interactive

[BFS96, BM91b, CD95, DY91a,
DNSS98, FOO91, GN94, GO93, HE98,
MY91, BM90, BG90, BMS96, BFS98,
Bra90b, DDNP99, EvH93, LS98a, MY93b,
Ped91d, Ped91b, RS91, Sah99, DY91c].

Intercession

[DL99].

Interconnection

[BW98, Por91].

Interconnects

[FVEA99].

interdisciplinary

[B+d96b].

Interface

[IBM93, Gog99, HVH98, LTEH99, JDK91].

Interfaces

[DMVC99].

Interferometric

[Hru96].

interleaving

[TH99].

Internals

[Zim95b].

International

[AR97, Ano99c, AA97, Auc98, BCB97,
Bih97e, Bri92, Bri93, Cha91, Chr99b,
CMM93, Cop95d, ES98, Fra99, Fum97,
Gol96d, GQ95, Hed97, Hir97, Hir98, IEE95a,
IEE97a, IE96b, IEE96e, IEE97c, IEE97h,
Jan [WL92a]. JANET [You97]. January [ACM97b, ACM99a, Ano97a, Bih97c, SP90, USE91, USE92a, USE95a, USE96f, USE98d].


Java-based [Ale98]. Java/Smart [Bro97]. JDesignerPro [Ano97s]. jede [MPS94].


Joint [Ano93g, Cla98a, FH94, IE94f, IE95c, Kat97, LW91, IEE92d, vT93]. Jose [Com96, FJV97, RP97b, SJ97, USE96e, USE96g, van96]. Jour [Lut98]. Journal [Eri97a, Zol93, OW95]. Journal/Logging [Zol93]. journyx [Ano97s]. JSafe [Way98].

JTC [Gar97a]. Juan [CMM93]. Judge [GC97]. Judiciary [Un96b, Un97c]. July [AR97, AA97, BFS92a, BPS99, Com96, DG96, IEE95a, IEE97a, IEE94b, IEE97c, IEE98e, Sch98b, Sch99b, SIJ93, Un98c, Un98f, Un97c, USE95c, USE96e, USE96g, VPM97, Wat91, vWN99, Un98i]. Jump [DHR95]. Jumps [Gar97b].

Junction [CIBM99]. June [ACM95, And96c, AA97, GS94b, IEE92a, IE94f, IEE94f, IEE96b, IEE96c, IEE97f, IEE98c, IEE98e, IE96c, IEE98e, LM98a, Ny98b, Pitr95, PR98, SIJ93, Un98b, Un98e, USE94, USE95b, USE98c, USE99d].

Junk [DN93]. JW [Ano93g], JW-ISC [Ano93g]. [IZ99]. Kansas [Sin98]. Kapera [CWM99].


[Kor94, ARH95, Ano93c, Atk93, BR97a, BP98e, BP98f, BM91a, Bor93b, Br98, BW92, DS90b, Dav95, DG95, DGT96, De93a, HRT96, IH99b, Kay95, Koh90, KN93, KNT94, Lei99a, Lin96b, Lmm90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts97, Tun99, Yu94a, Yu94b]. Kernel

[BCC93, WB92]. Kerry [IE96c]. KEY [YY98d, ANS97, ANS98b]. KDE [ACP96, AAB*97, AN95, IBM93, Ano94b, Ano94c, Ano94e, Ano95m, Ano97c, Ano99f, AA93, BP98a, BI95, BDH98, BDDG98, BCE94, Bar96a, BCG90, BR94a, BR95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BS97a, Bir98, BMS94, BWM98, BWM99a, BWM99b, Bla94b, BDR*96, Bla96c, BPK99, BFK99, Ble97, BDHK93, BFS96, BDF98, BD99b, BF99c, Boy90, BM94b, Bra95c, BS94, Bur94b, BDS98, Cae96a, CC99b, CG99, CD99, CJ99, CGM97a, CS99b, Cra98, Cus97, DDJ98g, DDJ98h, Dae98, Dam91b, DK96, Dan95, DPD90, Dav96, De93c, DP98c, DB96, Dif90, DH90, ECM96, FW91, FDB93a, FY95a, FY98a, FYM99, FBS98, FO99a, Fun98c, Fun93, GH90, Gal96, Gan96a, GJK99, Gib91, Gib96, Gill99, GM90, GGH97b, Gys96, HK99a, HQ98].

Key [HP98a, HS90, HMT98, HM93, Haw98b, HD96b, HJJ+, Xs97, HPS98, HFP99, HM98, HRR90, Hwa97, Iss90, Jab90, Jas96, JV96, Kal99, KP99a, KSW96, KSW99a, Ked99, KSW9b, KP96b, KM99c, KT91a, KMOV91, KKO91, KP93, RSA93f, Lan99, LM94b, LWY95, LSM97, LA98, LP99, Low96, Luc98b, Mah96, Mar97, Mat91, MY91, Mau93a, MW96a, Mau97a, MP91, Tv93, Men93, MM96b, Mic93a, Mic93b, MS95f, MM99c, MS99c, MKS99].
MSN98, MSN99, MTVZ92, MAO96, MM98a, MM98b, NMR95, NS97a, Nec96, Neu97, NS99a, Oka94, OU98a, Oka98a, Oka98b, Omu90, vO91a, PSL97, Pa99d, PKOT94, Pat95, Pin97, Poi99, PB99a, RSA93e, RSA94, ROT94, RS98c, RS98d, Ros96a, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, RCM99, SSN98a, SYMI98, Sam98, DP91, Sas99a, Sch94b, SKW +99, SKW +99, SOOS95, SM95a, SE96, Sha99b, She94d, SiK93, SR96, Sta99b, ST91, SW99b, SH94, Sun98a, Sut99, TAP90, Uni98i, Van95a, Van93, VSH97, Vv97, VBD99, WM93, dWQ91b, WLEB96, WW98b, WKS +99, Wie96, Wie97, Wie98a, Wie98b, Woh98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vOW96, AA95, Acc97, Lip98, AD97, AD99, AI 96, Ano90, Ano96m, BSNP96a, BSNP96b, Bao94, BI94, BDHJ97, BD98a, BT998, BSB97, BR96b, BCK98, BY93c, BY93b, BS91a, BFS92a, BGH +95a, BMP97a, BF96, Bje96, BMS96, BFS98, BM5, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Cra97, Cus95, DKR97b, DWZ96, DS90a, DH96a, Des95, DVG96, Dhe98, DvW92, DN95b, ES97, FDB93b, FGMY97a, FMY98, Fre94, Fro96, FGLP96a, FGLP96b, FL93, Gar96b, GH96, Gi95, GBL94]. Key [GH99, GTS90, HNSM91, HP99a, HP99b, HY93b, Hae99a, He92, HFD96, HJJ +97, H97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IZ89, IZ99, JM96a, Jar96, JLM +94, Jon90, JY98, KASH90, KM99a, KSW97a, KSW97b, KL94, KR96b, Kir95, Koo97, KM99d, Kos99, Kumm97, LF97, Las92, LM9W93, Lee95, LC96a, LMG94a, LZ90, LZ91a, LDW94, LL95b, LCL95, Lon91, Lon92, Low95, MS98a, Mao97, ML9A1, Man91b, MY93b, MKKW99, Mu92, MLLG95, NM96a, NY90, Nat97a, Nec91, Odl94b, Ole95, PS98e, PS98f, Pet91, PP92b, RT93, Roe99, Sal90, Sal96, SW95a, Sch92c, Sha95a, She96a, She92c, SKB97, SY96b, SM90, Sm93b, SS95b, SS95c, STW95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC99b, TC99a, Ts90, TC91, Tze99, TH99, Uni97c, Uni95a, VW96, Ven92, Wan92b, Wie94]. Key [Wil93b, Xie92, Xie93, XLP99, XW97, Yam98a, YL97b, Yu92, Zha91, Zhe95a, Zhe95b, ZPY96, vOW91, vO92, vT90, MC96, BFS92b]. Key-Agreement [RSA93b]. key-clustering [Kum97]. Key-dependency [MAO96]. Key-Dependent [FBS98]. Key-Escrow [Vv97]. Key-Exchange [Dan95]. key-management [ML9A1]. Key-Recovery [Oka98a, Oka98b]. Key-Schedule [KSW96]. Key-Search [KP99a]. Key-Share [BMW99b]. Key-signing [Ros96a, Ros96c, Ros96f]. Key-specific [LMS97]. key-vowel [Lip98]. Keyboard [GO96c, She95a, Ale97]. Keyboards [CFK +91]. Keyed [Ano95a, BFN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pre95b, MS95e, BFN98a, Gon95, KBC96]. Keyed-Hashing [KBC97]. Keyed-MD5 [KBC96]. Keying [BCK96d, BCKxx]. KeyNote [BFK99]. Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Dae98, EHS99, Gir91, KSHW97, KSHW98, KM99c, Luc98b, MP91, PS98g, SV99a, SV99b, Ste94a, Van96, Way96b, Bih94a, CH97b, CILL93, DGV94c, GP96, KC95, Koo95, LL93b, MWW99, MF97, Mok97, SS97a, SS97b, SV98, SH99, Sta95a]. Keyspace [CD98c]. keystream [CS96b, CS97b]. keystroke [JG90]. KG [Un94a, Un94b]. KG-194 [Un94a, Un94b]. KG-94 [Un94a, Un94b]. Khafe [BS91f]. KHF [Wag98a]. Khufu [BBS99b, GC94]. Khwarizmi [CF +91]. Kid [FK93a]. kids [WS96c]. Kimba [KW99]. Kind [AM97, Gad91, SX90]. Kingdom [D98, Lon97]. Kingston [TM99]. Kiosk [BO96a, Gar96b]. kit [An97u, Sun91b]. Kleptographic [YY97b]. Kleptography [YY97a]. KMOV [Ble97]. KN [SMK98a]. Knapsack
knapsack-based [He92]. 

Know [DDJ98b, Fly97, Hi97, Kir95, Mil95].

known [ADBB99, BM90, BG93, BHY97, Bie98, BD91, BDB92, COM99, Cox97, CDS94, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GKh96, GSV99, GO93, HT98, JVKP99, NOV93, NMV99, O90, R91, SI93a, SY99, St99, Tou91, BOGG+90, BBP95a, BBP95b, CDP95, DDP94b, DF93, DP94, DF91b, Sah99, Sak97]. Knowledge-Based [Bie98].

Knowledge-Level [BMT98].

known [Ano91b, BK95a, M93a, vOW91].

known-plaintext [vOW91]. KnowRight [BS95e].

Knoxville [IEE94e].

Knuth [CFK+91].

Knuthian [SY99].

KoMoD [BER90].

Komputer [Ano97-29].

Konstanz [Fum97].

Korea [Ano93g, KM96a, R93]. Korea-Japan [Ano95d, Ano95e, Ano95i, Ano95m].

Korteweg [GK95b].

Kruh [CFK+91, Ers98].

Krypto [FK93a]. Kryptographie [KK97].

KryptoKnight [BGH+95a, MT92].

Kryptosysteme [Hor99].

KtSeqC [BG99].

Kudos [SvA+98].

Kunstliche [CWM+91].

kuo [X'TmW94]. Kuperee [DH96b, HS94, HS96b]. Kurz [Ger97].

Kyoungju [KM96a]. Kyoto [Ano99c].

L [Lip98].

Labeling [BK98b, K95, LvdLB96, LvdLL97].

Labels [ZK95].

Laboratories [Ano95d, Ano95e, Ano95j, Ano95m].

LABYRINTH [LS97].

Lac [CF96].

Ladder [Bih97a]. Ladder-DES [Bih97a].

Lai [LLG10].

Lake [IE96d, USE95b].

Lambda [HR96v, GL99].

lambdaProlog [NM99].

Lancaster [WS99].

Lance [Hat96, Wa95].

Lane [DDJ98e, DDJ98f].

Language [AP93, AKP99, IOS94, K199, PW99, AAPS92, Kos97].

Language-theoretic [APDS93].

Languages [ACD94, BD91, GMW91, PM99a, PD99b, SAS99b, ACM99a, At94, DDP94b, GA98, I91, LI98a, PS93a, S99, vWN99].

LANs [She92f].

LANSCAPE [RI96, Ano94g, Ano94f].

Larger [PW97b]. Laser [Ano93h, JC93].

Last [dBB91, dB91].

Late [Bur99].

latencies [JG90].

Later [Sch95a, Gol97c, Roe95].

Latin [BS97, Son99].

Lattice [Ano97-29, BK98b, CC99b, CC99a].

Lattices [CC99b, CC99a].

launch [Taa98].

Launches [Gar98].

Launches [Gar97c].

Lausanne [IEE96c].

Law [And96a, Bro94, Cae96b, Swi97, Uni95a, Cli99, Way93c].

laws [Ano97-29, Cha94b].

Lawsuits [Lea99].

Layer [BB95c, FK99, Sar97, Wu96, M97].

Layered [Jun99, RC95].

layers [AP93].

Layout [BW98].

LCN [IEE97j]. LCN'98 [IEE98j].

LCT [Z98].

League [PU99].

Leakage [WI99, HJ95, SG96b].

Learn [Hel98b].

Learning [BV98a, COM99, FCH99, FC99, Hof99, KV94, R93b, SK199, BFKL94, Kh93, Kos97].

Leave [Hus99].

Lectures [Dam99b, Fri96, PR98].

Lee [Scu92, LZ91b].

Lee/Alek [Scu92].

legacy [Uni92].

Legal [CYY98, WA96, Mos98, Rad97, Ros95b, WR94, Ame95, Ame96a, Sch93e].

Legislation [RDK98, May97].

legislative [Cii99].

legitimate [Cii99].

Leighton [Zhe95a].

lemma [HK95].

Lempel [Mun91a, Mun91b].

lend [RI96].

Length [BR99a, BR99b, GS94a, Sch94b, Y98a, CC98, Han94, KL95b, MPL99, SU98, ZPS93].

Length-3 [Y98a].

length-restricted
Logs [SK98a, SK99]. LOKI [BS91f, BKPS93, Knu92, Knu93c, Knu95, TSM95].
LOKI91 [Kmu93d, Knu93a, SF97]. LOKI97 [BP98s, RK98a, Rij99]. London
[Ano93d, Ano97p]. Lone [Ano97r].
LONE-TAR [Ano97r]. Long
[CHN97, Len96, RH93, SSS98, Pos93].
Long-term [CHN97]. Longevity [Rot95b].
Look [Coh96, Has99, Pfl95, Zha97, GTGW94, Way91]. Look-up [Has99].
Looks [Sch97b, vdWS97, vS97]. Loops [SvA+98, SHK99b]. Lorenz
[Car97b, Dav98d]. Lose [GPR98, Way96b].
Losses [Law98]. Loss [PW97c]. Lossy
[CI96]. Lot [Riv97a]. Lotto [QD91].
Lotus [Dwo95]. Louis [Ers99]. Louisiana
[ACM91, ACM97b, USE95a]. Louvain
[Dan96, Q+98]. Louvain-La-Neuve
[Dan96, Q+98]. Low
[Ag92, Ano99c, Bla96a, Bla96b, CFPR96b, CFPR96a, CNS99b, DDQM98, DDP99, DDGM97, DFKN93, GDD+97, Gro96, Jak98, KSHW97, KSHW98, KKW99, KOT95a, KOT95b, Mil96a, Pfi99b, PK95a, PK95b, Pen96, SKNO98a, SKNO98b, T+99, Ano90, CJL+92, DVQ96, Gol96a, MHW98].
Low-Bandwidth [Bla96a, Bla96b].
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, KOP97, Shp99b]. LR
[BP98c]. LSI [SKNO98a, SKNO98b]. Lu
[LZ91b]. Lu-Lee [LZ91b]. Luby
[BKR98a, BKR98b, Luc96a, Luc96b, PRS99].
Luby-Rackoff
[BKR98a, BKR98b, Luc96a, Luc96b, PRS99].
Luc [Sm93b]. Lucas
[BBL95, JQ97, LTT95, SS95b, SS95c, XLP99].
Lucas-based [BBL95]. Lucent [MB99a].
Lucifer [BB94, BS91f]. lun [XtTw94].
Lunch [DDJ98e, DJ98f]. Lured [Che92].
Lurking [Joh96]. lustre [Alv98a]. LVQ
[LSVV95]. Lyndon [SM90, SSM92]. Lyon
[FR95a].
M [IEE97c, WG97, Mau91b]. M.A.P.
[BBC98]. M6 [KSW99b, KSW99c]. ma
[XtTw94, KP99b]. MAC
[Mit92a, PVO95, PVO96, Pre97a, SRRL98, SRY99, Yu97, Ano93k]. MacArthur
[De92]. MacGuffin [BS95a]. Machine
[KP99a, NM99, PF94, QD91, Riv93b, Wic90, Cra92, Dav98d, Dav96, Kru98]. Machines
[Bur99, CFK+91, FMM99, SK98a, Dav98c, Jan96, Sel98b]. Macintosh
[Sch94l]. Macquarie
[KG93]. MACs [AB99a, AB99b, BGR95, JY98a, NR98, PV95]. Made
[GSV99, Kra94a, Goli97c, KKL99].
Maestro
[CFK+91]. MAGENTA
[Bih99a, Hub98, BBF+98]. Magic
[BD97a, JM99, AGLL95, Kah98c, RK98b].
MagiCol
[GLSM99]. magnetic
[Ano90, Gut96]. Mail
[Ano93j, DN93, Got99, Ken93, Lin93a, RS98b, Sch95c, Sch95d, SH97, VJ98, Ano95c, Gar97b, LF97, Lin88a, Lin91a, Mit92a, Ril96, She96a, Str93a, Str93b, Bac95, Zeg93, Sta94a]. MailSafe
[RSA94]. Mainframes
[De97, De98]. Mainstream
[Gar97b]. Maintain
[Wed99]. Maintaining
[CH94a, CHH97, Gar94]. maintenance
[Uni94b]. MAINZ [PWU99]. Majesty
[Ber96a]. Major [Law98]. Majorities
[Cha90]. Majority
[Mv93]. Make
[Ano93c, GMM97, CM99d]. Makes
[Ame96b]. Making
[ASW99, CKN99, DDJ98e, DDJ98f, Des90b, Hir93, Lut98, PRS99, Sar97, Tra97, VM96, Way98, BKR98a, BKR98b, Wri98, Zaj97]. Malaysia
[GO96c, WSFC99]. Malicious
[PM98]. Malleable
[DDN91a, BS99b, BS99c, DDN91b, Sah99].
Mechanisms
[HL99, Mye94a, CGM96, HC95a, ZH93].
mechanization [BoI97]. Mechanized
[SM95a]. Medals [DJ98b]. Media
[DDJ98d, GB98, Hat96, MW98b, Ros94].
median [KR99b]. Mediated [FJ98]. Mediator
[Kem99]. medical [Cha99b]. Meet
[FY99, Van95b]. meeting
[Shp99a, Zim96b]. Mellen
[IEE98b]. Members [Par98c]. Membership
[FGR92, Fis98, OOK91, SPH99, AK95,
MW94, Sak97]. Memoir [Bar05]. memoirs
[RK98b, Sel94]. Memorial [IEE98b]. Memory
[ARV99a, ARV99b, CM97a, DHMR96, Fis97,
Got99, KS99a, Lei99b, MS91, Sha95a, Gut96, Has99, Ven90].
Memory-Bounded [CM97a]. Menezes
[Sha99a, Kie98]. Mental
[CF99, Jun99, KOT91]. Merced [GC97].
Merging [DVQ96]. Merkle [NS97c, NS97b].
mesh [PHF99]. Message
[AGS97, AB99a, AB99b, Int91a, ASZ96,
Bax97, BG90, BCK96d, BCK96c, BCKxx,
Ber97c, Bie98, BHK99, CDFT98, EPR99b,
EPR99a, FH94, GLZ99, GTG94, GQW91,
HK97, Kal91, KR95b, Kal98f, Kal98d, KI97,
Kra95, KBC96, KBC97, LK99, Lin88a,
Lin93a, Mi96, NR95, OM94, Pre98a,
RSA93d, Riv92a, Riv92b, Rog95, Sho96,
Ts92b, Ts92a, WSK97a, WSK97b,
BSNP97, BGR95, BJQ97, CLHL98, Cli99,
HM95, HCY96b, LC97a, Lin89a, Riv90a,
Riv91b, Sta99a, Tze99, Yeu99]. Message-Digest
[GTG94, Riv92a, Riv92b]. Message-Efficient
[FH94]. Message-Resend [Ber97c]. Messages
[CFPR96b, vD97, SS99c, SKAM99,
CFPR96a, Joh97b, Kip97, Mit92a, Par98b,
Sch95d, Wav93b, Wri98]. Messaging
[DDJ98c, AC97, DMW94]. Meta
[EKL99, FBS97, HMP95, PS99f].
meta-blind [HMP95]. Meta-Logical
[PS99f]. Meta-message [HMP95].
Meta-Object [EKL99]. Meta-Protocols
[FBS97]. MetaML [MTES99]. Metaphor
[BP95a, Fuc99]. Metaphors [BHJ999].
Metaproof [DY91a, DY91c]. Meteor
[Sch93a, UNU94]. Metering
[SK96b, SK96c, Ros94]. Method
[AG98a, AG98b, ADD99, BP98f, ESST99,
GDD97, HRV99, KI97, KT93, LL94a,
Mat94b, McM96, MS59f, Mi93c, SF97,
SKBxx, Tes98, VNW94, CP94, CM97c,
GTS90, JT96, JT97b, Joh98, KM98b,
KAK96, KH97, LC98, Mat93, MY93a, Mck99,
Pat6a, RT93, SH99, Su98, Vu95, YEA98, ZH90].
méthodes [Bec90]. Methodology [CH99b,
DD95, FM98a, NMR95, PNFK95, SSSW98].
Methods [Bas93, Bir99, CL98, DS999,
GSY99, IM93b, KBRS97, Lvd LL97, LM98b,
MCD99, Per99, SW94a, AhdJF97, Ale92,
Ata94, Bau97, BGR95, Car97c, HLC99,
IM93a, vdL98, QN98b, RT93, Rh95,
Shp99b, TG94, Whi93, XL98, van98].
Metric [Joe98, RS99b]. Metrics [LA98].
Metropolis [DP99]. Mexico [IEE91].
Meyer [Lu98, Lu98b, JQ98b].
Meyer-Müller [JQ98b]. Mi [XtTM94].
Miami [IEE97f]. Micali [Zhe95a]. Micro
[Ano97q, HSW96, Pri94]. Micro-payments
[HSW96]. microcomputer [HN98].
microcontroller [Kuh98]. Microcontrollers
[KKW99]. MicroMint
[RS96b, RS96c]. Micropayment
[JO97, RS96c, RS96b]. Micropayments
[Riv97a]. Microprocessor
[DDJ98d, Mar96]. microprocessors
[RM96b]. Microsoft
[Boy98, Fly97, Gar98a, SM98a, Ts97].
Middle [BBS99b]. Middleware [BCCD99].
Might [DDJ99c, DDJ98f]. Military
[Ano96m, Fri92a, Fri92b, LU95]. Millicent
[Man95]. Million [Ren91, Riv91a]. Millions
[Wal99b]. MIMD [DHW95a, DWH95b].
MIMD-factorisation [DHW95b, DWH95a].
MIME
[An95c, An95n, Ano96k, Elk96, GCF95].
Minefield [Han94]. Mini [Jak99b].
minimally [CGM97b]. Minimax [All98].
Minimization [LE99, SBG99]. Mining [BR97b, SS98a]. Minimum [Ano95a, Ano97b, DK96, FO99a, CC98].
minimum-weight [CC98]. Modern [Buc91b, Gol97a, Gol97b, Gol99a, VG99, Dam99b, Unixxa].
Moderne [Bra93b]. Modes [Ano96c, Bih94b, Bih96, Bih98a, Bih99b, CV99, HP99a, HP99b, HRV99, MT95, NA95, SHK99b, Wag98b, Bih95a, Nas94].
Modification [AKF94, FG98, Sel98b]. Modifications [NMR95, OMA98, Mol98].
Modified [BDG98, NK98a, PB99v, Wic90, CLW98, HWR93, LZ91b].
Modular [BP99b, CJS91, Cop99c, HCY96a, Kor93, MNSV97, Pia99b, PRAM98, SKBxx, TY92, TN96a, TN96b, VDDR99, Yam98b, BGR98b, BCK98, CK93, HN94, ISO97, KAK96, LC98, Yam98a].
Modulation [B99, She94c, SC96b, KSB96b, KSB97, SVWMB95, SOB98, VSB95].
Module [Mee98].
Modulo-Place-Invariants [DR94c].
Modulus [Tze99]. molecular [ARR99, Ram92]. Molecules [GC98].
MON [YY98d]. Monetary [Gar97c].
Montana [BCC97]. Monterey [USE99d].
Montréal [ACM94c]. Moose [Ros96b].
Moot [Ano96d]. Morphology [Blo99].
Morphometry [SC99]. Morsel [Sch98i].
Moscow [CW94]. Most [BV96, KAK96].
motion [NAS94, OHT98, YEA^+98].
Motorola [DK91, Gar97a]. Mouth [DDJ98c]. MOV [HSSI99]. movable [GMLH94].
Moving [Gar98a, HHW99].
MP3 [MB99a]. MPEG [DS97b, DS97c, DSS98, HG97e, HG97d].
HEG98, LT98, QN98a, QN98b, SB98.
MPEG-2 [DS97c, HG97e, HG97d].
MPEG-4 [HEN98]. MPEG-encoded
[DS97b]. MPEG2
[CO+98, CHO+98, DDNM98]. MR
[TDJ99]. MRA [BAL99, LFCK99]. MS
[CFK+91, Gar98a]. MS-DOS [Gar98a]. MSC
[WSFC99]. Müller [JQ98b]. Mult
[CM99b]. Multi-agent [CM99b]. Multi
[BBDF97, BDD+94, BM99c, CC99c, CSF96,
DFGH99, DF97, FHM98, HS94, HJTW99,
HV98, JV96, KSB97, Lee99b, Mar98a,
PMM9a, SNW98b, SS98, Su99, TN96a,
TN96b, VC99, CL97a, CG97, HV98c,
KSB96b, SVWM95, SOB98, VSB95].
Multi-Agent
[Lee99b, VC99, HJTW99, PM99a].
Multi-Application [Mar98a, DF97].
Multi-authority [CSF96, CG97].
multi-carrier [SVWM95, SOB98, VSB95].
Multi-disciplinary [DFGH99].
multi-exponentiation [CL97a].
Multi-function [KSB97, KSB96b].
Multi-Level [HV98]. Multi-Party
[JV96, FHM98]. Multi-Purpose [Su99].
Multi-Receiver [SNW98b]. Multi-Secret
[BMM99c, BDD+94]. multi-senders
[HW98c]. Multi-Service [HS94]. Multi-tiered
[CC99c]. Multi-user [JS98].
Multi-variable [TN96a, TN96b].
Multiaapplication [G199, Tu99a].
Multicast [CMN99, PB99a, Mi92a].
multicasts [WL99]. Multidimensional
[BMS99]. Multidrawing [BMR98].
Multifeature [Ba95]. Multifunction
[She94c]. Multigroups [O091].
Multilevel
[CGB+93, GPSN98, KT96, DN95a, Z93].
Multimedia
[ACM99a, ADF98, CLS96a, CLS97,
Dan96, D98, ES98, FJ97, GO96c, HF97,
IEE96b, IEE98c, IR99, KBS97, LvdLB96,
Lip99, NAA99, ZK96, CLS96b, IEE97k,
KAT97, LS98a, Oko97, PS97]. Multipart
[GM95]. Multipart/Encrypted
[GM95]. Multipart/Signed [GM95].
Multipart [GM95]. Multiparty
[Ch90, C90, FW91, MH96].
Multipermutations [SV94, SV95a, Vau95].
Multiple
[AS96, Bih98a, Boy90, DK96, GO96b, Han94,
Kah92, KR94b, KR96a, SS99c, SH99b,
Wag98b, Bih95a, GGK+99, GPSN97, KR95a,
KSL92, Or95b, Or95a, SM94].
multiple-iterated [Ot95b, Or95a].
Multiple-length [Han94].
Multiple-precision [Kah92], multiplexer
[SGD99]. Multiplication
[Abe99, KAK96, Kor93, MS93, Zim99,
FB96, Has99, LC98, TY92].
Multiplications [MNS97].
Multiplicative
[BBDW96, DDB95a, DDB95b, Mi97].
Multiplier [HMv94, HB93].
Multiprocessor [MHP96].
Multiprocessors [Le99b, HJ99].
Multireceiver [SNW98a]. Multi-resolution
[BCV97, HW98b, SZT98a, SZT98b, XBA97,
Kl98a]. Multiround [G94, G95].
Multisecret [DLR97, JMO94, WAM94].
Multisecret-Sharing [DLR97].
Multisender [MSN97]. Multisignature
[OO93, CL1H98, FD92, HZ93, HCC98,
LHW99, LHL95b, LHL9a, PPKW97].
Multitude [Fuc99]. multiuser [LS98a].
multivalued [CG94]. multivariate
[M90]. Mutliversion [K96]. Munich
[EE97d]. munitions [U97d]. Muscle
[C98]. Musicians [M99a]. Musings
[Ins95]. must [C95]. Mutual
[Bak99, ARK99, BO99, CS96b, CS97b].
Mutually [CG97a, IS91, MA97, HY93a,
JMO95a, Wu92]. My [Cur98]. mystery
[Fra93]. Mythical [Si99].

n [ISO97, TN97]. n-bit [ISO97]. Naccache
[Cus97]. Naccache-Stern [Cus97]. nag
[IPdbr91]. Nam [CLW98]. Name
[Gar97a, Gar98b, Ano97q, Lea90].
network-centric [BGT96].
Network-Layer [Wu96]. networked [Ano97p]. Networking

[IEE98e, FJV97, LS98a]. Networks [ATA98, AWV99, BF97a, Bra99, CT99a, DQ93, HG97c, IEE971, IEE98f, Jut98, KRJ98, Lea99, LSV95, OMV98, PKOT94, PT95, Por91, Sa91, SK96c, SK96d, SV94, STP93, THP+98, Tow98, VSH97, Ver98a, Ano95k, ACBR90, Atk93, AC97, BF99b, CW91a, CYW98, Fra90, GBL94, HT95, Hor94, HLC96, Jen99, LC96b, LC96c, NT94, Nor95a, O’C95, Opp96, PS98c, PS98d, PS98e, PS98f, PS99d, PS99a, PS99c, PS99b, SV95a, SBTV99, Zan90].
Neurocybernetics [Mor98]. Neuropathy [MR95a].
Neuve [Dan96, Q’98]. Nevada [ACM95, AA97], never [Mon96]. NewDES [KSW97a, KSW97b]. News [Ano93e, Ano94a, Ano95j, Ano97q, Ano97r, Bar97, Bar96a, DDJ98e, DDJ98c, DDJ98f, DDJ98a, DDJ98b, DDJ98g, DDJ98h, DDJ99, Eri97b, Fox99, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, GB98, Got99, GO96c, Law98, Lea99, MB99a, Ros98b, TJ97, Taa98, WSFC99, Wor96, Bra90b].
Newton [AVPN96, Ber96b]. Next [Kal97b, SS91].
NFS [DL95]. NHS [Zer96a].
NHSnet [Zer96a]. Niagara [IEE96d]. Nice [BMRW98].
Niederreiter [LDW94]. Nikola [Ano97t]. NIKS [Cop94b].
nine [Tat98, Tat99]. Nineteenth [Alv98c]. Ninth [Ano95i, IEE93c, IEE94b, T’98, ACM97c, LMP93]. NIST [Bra93a, Dra98, Nat92a, RHAL92, Riv93c, SB93]. NISZK [GSV99].
NJR [TGK99]. nm [Gar97a]. No [DDJ98c, DDJ98f, DH90, PS98e, Saks96, Ano97-28, BBR99, GBL94, Mei98, PS97, YT96]. No-Transferable [Sak96].

nodes [GMLH94]. noise [PC98]. noise-based [PC98]. Noisy [Cre97, Lip94, MSHP99, MM92a, MFG95, GM91].
Nomikos [IEE97c]. Nominations [Nat97b]. Non
[AWV99, BM90, BG90, BS99b, BS99c, BS99b, DY91a, DDP99, DR94c, DDN91a, DDN91b, FCD98, FDB93a, FDB93b, GPT91a, GPT91b, GP99, GO93, HJPT98b, Jak98, KR96c, LW99, Mas99a, MY93, NO98, Pai98a, Pai98b, Ped91d, Ped91b, RS91, Sah99, DY91c, SCG99, TSY98, Yah94, AN95d, BKR98a, BKR98b, DDB95b, Ell97, HJPT98a, LLL98, MY93b, SB95, Sin95, SBTV99, 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-Invertible [NO98, BKR98a, BKR98b].

Non-linear [FCD98, Jak98, KR96c, LLL98].

Non-linearity [SB95].

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

Non-maximal [HJPT98b, HJPT98a].

Non-Oracle [Ano95d].

Non-Reachability [DR94c].

Non-Repudiation [GP99].

Non-secret [Ell97].

Non-Synchronized [Ye94].

Non-uniform [AWV99].

Nonadditive [RV99].

non-cryptographic [Fei99].

Nondeterministic [Mol98].

nonequivalence [Mol98].

Nongroup [SBV99].

Noninteractive [GSV99, Ped91c].

Noninterference [MC92].

Nonlinear [Gys96, KT91b, MS99b, Pit95, Gol99c, RD96b].

Nonlinearity [MS90a, SZZ95c, SZZ95a].

Nonoblivious [FNS92].

Nonperfect [KOS+94, OKT93, OK98, OK95].

Nonrecursive [Ru94].

Nonrepudiable [LHW98].

Not So [Ano99d, CM99c, Chu99a].

Notable [Bar94].

Notarization [SK97b, SK97a].

Note [Ano95g, Ano95h, Ano96g, Ano96h, Ano97k, Ano97m, Ano98d, Ano99f, Bih99c, BPK99, EKK99, KM92, Roh99, Bu95, CJR99b, ES97, GHS99, LM93c, MS98a, TX92, YL97a, Yu92].

Notebook [Ano93k].

Notes [GB98, KSF99, WN94, Dwo95].

Nothing [MM99a, MM99b, Boy99, GMW91, Riv97c, SRY99, Ste98b].

Nothingness [Way96a].

Notions [BDPR98, BS99b, BS99c].

Notwendigkeit [KK97].

Novel [Gren99a].

November [ACM93a, ACM94c, ACM96a, ???90, Ano94d, Cli97, DEQ92, GN95b, HOQ97, HF97, IEE91, IEE92b, IEE97l, IEE98a, IRM93, KM96a, LOX99, PSN95b, USE96d, USE96b, USE97b, UTMW94].

Nox [Ts'90].

NP [BD91, DDP99, DFK93, GMW91, NOV93, Sch94k].

NP-completeness [Sch94k].

NRC [Wor96].

NSK [PP96].

NSN [Uni94a, Uni94b].

NSW [GN95b, KG93, VPM97].

NT [Bru98, HIL98, IH98, USE98a].

NTRU [HPS98].

Nuclear [HRV99].

NULL [K98].

Number [Abe98a, Aga92, ARV99a, ARV99b, BG98, BGM97a, BGM97b, Bir98, Bor95, Buc91a, BP97c, De 98d, JK99, KSW98d, KS99, Koh94, LLM90, LL93a, Lo90, Mat96b, Miy93c, PG90, ROT94, Sch90c, Sch97c, Shp99b, WI99, BMx, Bou94, CS97c, CB96, Cou99, CDE9+96, Cus96, CS96c, C99b, Jenxx, Ka93b, Kos99, KK98, Lag90, LLM93, MC90b, Mei92, O'C94, Pom90a, Pom94, PP92a, PP92b, PP95b, PP95a].

O [Got99]. O. [Sca92]. OAEP [Boy99]. Oakland [IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, USE96d, USE96b]. Oakley [CH97a].


Occam [GN95b]. Ochrono [Sch95e].

October [Ano93d, Ano93g, Ano96a, Cha91, FM91, IEE93a, IEE94a, IEE96a, IEE96d, IEE97f, IEE97h, IEE97j, IEE98f, IEE99a, NIS92, Oht96, OD99, TV94, U93, USE96a, Ame95]. Odds [McC90b]. ODES [Rue94]. ODMG [Wat99]. OECD [Org98a].

Off [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AC95, Ano94h, Ano96i, Mao98, R98c, VNM99]. Off-Line [Bra95b, DT98a, EGM90, EGM96, Tra99, Mao98, VNM99]. offer [Mar96]. Offers [Gar97a, GC97]. Office [Fuc99, UU97a, Uni96c]. Official [Zim95a].


On-Line [Cac95a, Cac95b, CDF99, Ell99, EGM90, EGM96, PUF99, SS99e, SS99f, NaI97]. On-Line/Off-Line [EGM90, EGM96]. One [BJY97, BHSV98b, BHSV98a, BdM94, BHH99, BM94a, BM96a, BM96b, BM96c, BKK98, BP97c, DGV93, DDP90, Fi95, G96, HIL99, HT99, HYL99, Mer90a, MSN99, New98, Riv98c, Roe94, Rom90b, Sch91b, Sch95a, TOU94, Un91a, Un91c, Un91e, Un91f, Un91g, Un91h, Un91i, Un91k, Zhe90, Ano97d, BD95a, BK98a, CB96, D99, Dob98, Hwa92a, IEE92d, MB94b, MZ98, Roe95, Sim98c, Ste95, Sze98, Tao94, Tzu92a, Tzu92a, W93a, W93b, ZPS93, MAM95].

One-Bit [MSN99]. one-hot [CB96].

One-Key [G96, Tao94]. one-round [W93a, W93b]. one-step [An97d].

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

One-Time-Password [New98]. One-Way [BJY97, BdM94, BM94a, BKK98, DGV93, DDP90, Roe94, Sch91b, TOU94, Zhe90, BHH99, HIL99, HYL99, Rom90b, BK98a, BD99, Dob98, Hwa92a, IEE92d, MB94b, MZ98, Roe95, Sim98c, Sze98, Tzu92a, Tzu92a, ZPS93].


Hor94, SY96b, Sta96b, Con98, Dra99.
OpenBSD [dRHG+99]. OpenCard
[DT98b, HH99]. OpenGL
[DDJ98e, DDJ98f]. Opening [Bur94c].
OpenPGP [CDFT98]. Opera
[CH94b, IEE93a, IEE99b, Mar98a, WABL94, AHdJF97, FM98b, SG96b, WABL93].
Operation [Ano96c, Bih94b, Bih96, Bih98a, Bih99b, HP99a, HP99b, Wag98b, Bih95a, Glau99, Mon96, Pos92]. Operational
[Car97b, RZ99]. Operations
[DBVD96, Zie97, Win93]. Operator
[Uni94a, BP98c]. operators [BP98b]. Ophthalmical
[FCD98]. OPIE [MAM95]. opolizing
[YY98d]. Opportunistic
[BRW99]. Opportunities
[CD98a, FCD98]. Optimal
[BP98a, BR94b, BR95a, BJY97, BM96b, BM96c, Car94, FGMY97a, HKS97a, HKS97b, LC99, PRS99, PLWS99, ST94, SW97a, SW97b, Tav95, BJQ97, DP94, LL93b]. Optimality
[Mas99b]. optimally
[CGS97]. Optimisation
[MP98b]. Optimised
[RC94a, RC94b]. Optimising
[DN95b]. Optimistic
[AR99, DMM98, RP98]. Optimized
[EPR99b, EPR99a, SL99]. Optimizing
[Cla97, MS99b]. Optimum
[OK96b]. Option
[Dra99, Bor93a, Bor93c]. options
[Ros94, Sta97c]. Oracle
[Ano95k, GHR99, Ano95k, Got99, MS90b]. Oracles
[HTY99, MW96c, MW96b, BR97b, Br90d]. Orange
[IKE96e]. Order
[CH98, KW99, KS97b, Mil96b, MS96b, SMK98a, SVxW91, Boy97, Gol96a, GK95b, Jak99a, ML98, Mat95, She95c, VZ97]. ordering
[Sab94]. Orders
[BBT94, HJPT98b, KS97a, GV98, HJPT98a]. Ordinary
[Miy93b]. Oregon
[Auc98, USE90]. Organizational
[FY99]. organized
[Far93]. Organizing
[OMV98]. Orientation
[PJ99]. Oriented
[AK94, BDPS95, BDPS997, BLH99, Bel99, DSB99, LCL92, MNSV97, Mas94, Oum99, PD99a, Rei92, SG99a, SG99b, SCT99, YLC98a, YLC98b, BGV97a, CW97, Fra90, HY93a, Hwa91, Hwa92d, LG97, LW96, TCH+91, Wu92]. original
[CS98a, PBBC97]. Origins
[AK98, CKF+91]. Orlando
[IEE93c, IEE94c, IEE96f]. Orleans
[ACM91, ACM97b, B+96b, USE95a, USE98c]. ornamental
[PNgbbbr91]. ORTES
[ACC99]. Orthogonal
[BGS94, BGS96, YMWP99]. Orthography
[Ber96a]. ORYX
[WSD+98, WSDK99]. Osaka
[SKIT99]. OSI
[FL93, HS96a, Hor94, K92, She93c, VGV93]. OSPF
[MBW97]. OSS
[Pea97]. ossifrage
[AGL95]. Other
[Aga92, CG98, Des96a, Koc96b, KS97b, Koc95, Ros94, Wri98]. OTM
[STSW99]. Our
[Gad91, PT95]. Outlaws
[HM91, HM92, HM95]. Output
[CJM95, Bha94a, Sab94, ZPS93]. Outputs
[SK96a, SK97c]. Overcomes
[Mau97c]. Overview
[GML94]. overflows
[Mei98]. Overlap
[AMP99]. Override
[Bar97]. Overview
[AS98, BPP99, DHRM96, Lan98, Lin93c, PGV92, YS99, dRHG+99, Ger97, Ste98a, VNP98, YS91]. Ownership
[Car95, CMY99, BO96a, Oko96, QN98b]. ownerships
[CMY97, ZL97].

P [YT96, MS90b]. P-1 [MS90b]. P
[IEE97c]. P1363
[Ano96k, Ano97y, Ano97z, Ano98i, Kal97a]. PA
[AR97]. Pacific [Un98e, Win93]. Paciﬁco
[Z98]. Package
[BMS99, Riv97c, Sta94a]. packet
[TY94]. Packings
[Mou99]. Pact
[Bro97]. Pad
[BR96a, Fil95]. Padding
[CNS99a]. page
[Ano97r, Hod97]. Pager
[Garr98a]. Pair
[Sch95f]. pairing
[FMR99]. Pairs
[Kwa93, Mwy93c]. palace
[Bar92b]. PalmPilot
[DB99]. Palo
[KK98, MVZ93]. Poker [KKOT91]. policies [HK99b]. Policy [ACM94b, And96a, Ano96f, Bar93a, Bar93b, CPOR97, Ell99, Gir99, Hat96, Wai95, Aus96, Abr97, Ban94, Bro96, Dam96, DG96, Ele99, HAH94, Hof95, LKB+94, Rot95a, Tas98, Wad98, Zaj97].

VCF+ , ZMI\textsuperscript{+}, BFKL94, BP95b, Di99].
principle [Dam90b, Gib90].
Principles [ACM99a, AN95, HGHD98, KK99a, KG99, MG91, PRB98b, Zhe90, Sta99a].
Printer [Cov93].
Privacy [Ano94h, Ano95c, Ano97s, Avo98, Bac95, BBCM95, Ble98b, Car96, Cha92b, DL98, EIk96, FJP96, FHM99, Gar95b, Gar95a, IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, Ken93, KFJP96, Lin88a, Lin89a, Lin93a, Lut98, MW97, Mjo93, NKP99, Par98c, SY96a, SYMI98, SB97, SG96a, Sta94a, Tho96, Tra99, Uni98a, Uni98i, Ban94, Bro96, CM95, Car94, Cha92a, CK93, Cli99, Dom96, HM96, JMLW94, Mar95b, Mei96a, Mil95, Rot95a, Smi94a, Sta95b, Uni98d, Uni97c, VPM97, Zim96a, Zim96b, Gar95c, Ros97a, SS97a, SS97b, Sta94a, Sta95a, Zeg93].
Privacy-Protecting [Tra99].
Private [BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, Mv93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS90b, Ts90, Wil93b, ZG96].
Privilege [ECM96].
PRO [Ano97r, Gar98c].
Proactive [CHN97, FGM97b, HJKY95, HJJ+xx, IBMxx, Jar96, Rab98, BCR98, FGM97a].
Probabilistic [Jak98, JO97, SF97, Sch91b, Tou93, Gol99a, GO95, HK90, Imp92, Lon91, TX92].
probabilities [Lew92].
Probability [BDG99, Gol96b, Koh99, TY94, AI96, MHMW98, MAO96, WM93].
Probable [BD93, NK93, DLP93, Graxx].
Problem [Bon98b, Bon98a, BN96, CS96a, Cha90, DD99, DJL93, GO96c, HM98, KM99b, KR99b, MT99b, NS99b, OMV98, Per99, RS99a, CPS95, HY93b, H97b, HMB97, HMP95, LC97b, Mas97, McC90a, NR95, OA99, MSO96].
Problem-Solving [Per99].
Problems [AA93, BD95a, Bra90a, GGH97b, KRS99, MC92, Poi99, Smi90, APDS93, Be92, BFKL94, FR95a, 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, Ano95l, Ano98f, Bri92, Bri93, Com96, GN95b, IEE95a, IEE91, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96d, IEE97i, IEE97j, IEE97k, IEE97i, IEE98e, MZ98, Nat99b, OW95, PSN95a, Pit95, Sti93b, SLJ93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94d, Bih97c, B97c, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, DE95, DEQ92, FAR93, FM91, FR95a, Fra99, Fum97, GO90b, HOQ97, H97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE89d, IE98f, IZ98, IZ99, KM96a, KG93, Knu99, KP99b, KK99b, Kra98, LOX99, LM98a, LW96, Lom97].
proceedings [MV91, Nyb98, OiDP98, Pre95a, QV90, QQ95, Q95, Q95, Rue93, SZ93, Sp95, Ste99b, TM99, TV94, T99, Tv92, USE90, USE98, VP97, Vaut98e, Wat91, Wie99, Woi93b, Yua92, vWN99, ACM93b, CH96, C99b, IEE94e, Sti94, Wal99a, BCB97, Boy95b, C99m3, Cop95d, Dar97, Des94b, Fei91, Gol96d, G95, GS94b, He94, IRM93, Kal97c, Koh96, Mau96b, PSN95b, SP90].
Process [AMP94, Knu99a, Roh98a, RS99c, YT96, C99m*1].
Processes [Gar98b, Bea92].
Processing [Ano97b, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97d, IEE97j, IEE97k, IND99, KV99, LMP99, LW96, Pin98, Pit95, Ano96m, DO99, DF97, Man98, Sab94, T99, Wli90].
Processor [Gar98a, RB99, SW97a, SW97b, She92e, Sut99].
VVDJ90, Von92a, Von92b, DVQ96, She92c].
Processor-efficient [Von92a, Von92b].
Processors [Cla97, KK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
Prodigy [CFK+91]. produced [SS97c, SS97b]. Product [GO96c, KSW98a, KSW98b, KSW98c, GN95a, SS98b, Ano94h]. Products [Ano97r, Ano97a, Cha94b, Cli97, Los97, UU97b].
Professor [Swi97]. Profile [HFPS99, MM90a, MK92]. Program [BDFM99, FGY96a, LBMC94, FGY96b, LS98a, Pre97b, Pre97c, Uni95a].
Promotes [GO96c]. PROMS [IEE98e]. PROMS-MmNet [IEE98e].
Proposal [ABK98b, ABK98c, ABK98a, BAK98, DR98a, KR94a, LM91b, Cli99, LM91a, RHAL92, RRSY98, Ban94].
Prosthesis [HDD99]. Protean [SVB99]. Protect [Sch94a, Sta95b, CK96b, Way93b].
Protected [CH94b, DY91f]. Protecting [BO96a, Ble98b, Des90a, EHMS99, GMDS98, KRRJ98, Lut98, Mar95b, MW98b, PT95, SYM98, Tra99, VP99]. Protection [BGG95, CH97, CW94, DF91c, FGR92, F98, Gro98, H97c, 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, Tv92, TSN93, Uni97c, YE+98, FT95].
protections [HPP99]. protest [Ano97-30].
Protocol [ATAV98, Ano95a, BMW99b, BW98b, Bra95a, Bra96, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JMP+98, JQ97, Kas96, KSW98a, KSW98b, KS98b, Kra99, Kum98, Low97, Mau94, MW99, Mey96, Moo92, N98b, NS98c, OM93, RS96a, RS98b, SSN98a, SH97, SM98a, SM98b, SM98c, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CST98, D96b, EvH93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pan99, RS98f, SK97, Sim94b, TH99, WS97, WL94, Zhe95a, GM93a, Sar97].
Protocols [AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BG+91, BWM98, BW99a, BM93b, B98a, Bol98b, BDL97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dam99a, D97, D98, DQ93, DS97d, Fei93, Fei96, FBS97, Fum98b, GM93a, Geh95, GS97, GM98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IE98e, KKT91, KY92, KS97c, LY93, LL97a, LHB96, LL95a, LS92, LM96, MB94a,
MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nr94, SL93a, Sch94g, Sch96a, Sch94h, Sch99k, SPP90, Tou91, Tou93, AN94, AG97b, AG97c, AG97a, ABA99, ABC+98, BDH97, BH93, BCK98, BH98+95a, BBS98b, BM95, Bra90b, CMG96, Chr98, Chr99b, CJ95, Dan97, Fei99, HL+95, JW01, LY93, LHW99, LL95b, Lom97, Man95, Mas97, MLY93, Mea95, MW98c, NT93, PS98c, PS98e, PS98f, protocols [Pau98, PW93a, PKM97, SSG99, Syv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].

prototypes [Ano96m]. Prototyping [AKP99]. Provable [Bel99, CT99a, Mat96a, Mih94, SZ96, Vau98b, BOGG+90, Mol98].

Provably-Provable [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, LM95, Man91d, Oka93b, PS96c, Sho96, ZMI90, BH93, Dam94a, FO98, Gol90c, NY90, PSW95]. 

Provably-Secure [DY90, DY91d, DY91b, Man91d]. prove [Zha96]. proven [DS93, Lec90]. Prover [Tre99].

provably-provably [DY91a, GPSV98, HB99, DY91c, DFKN93].

provers [JY96, Ped91a]. Provide [BDR+96, SA95]. Provider [Tre99].

provides [MHW98]. Providing [Bra90a, SKAM99, Ano95c]. Proving [Bos90, DR94c, DE99, FK99, DF91b].

provisions [Clin97, UU97b]. proxies [LC94].


pseudo-àléatoire [Bou94].


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

psychoacoustic [Til98]. Psychovisual [DDM98]. PTY [LT98]. PTY-Marks [LT98]. PUB [Nat95, Nat99a, FIP93b, NIS93b]. Public [ANS97, ANS98b, Acc97, AKP96, AN95, IBM93, Ano96m, Ano99f, Ano99b, AA93, BP98a, BI95, BDH98, BG98, BCE+94, Bec99, BC95b, BHS98b, BHS98a, BDP98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BF99a, BF99c, BS94, CC99b, CG99, CJ95, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De 93e, DP98c, Di99, Ell99, FY95a, FY98a, FYM99, FGLP96a, FGLP96b, FO99a, GHT90, Ga96, Gar96b, Gib91, Gib96, Gir91, GGH97b, GH99, HK99a, HS98, HP98a, HY93b, HM93, HL93b, HJJ+xx, Hess97, HPS98, HFPS99, IZ98, IZ99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKOT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Man93a, Man97a, Men93, MM96b, Mic93a, Mic93b, MM98a, NS97a, NY90, Nerc91, Nerc96, NS99a].

Public [Odl94b, Oka94, Oua98a, Oum90, vO91a, PS97, Pai99d, Pat95, Pin97, Poi99, RSA94, RCM99, Rud91, Sa90, Sa96, DP91, Sas99a, SE96, She94d, Smi93b, ST91, Sun98a, Sut99, TAP90, VSH97, dWQ91b, Wiet98b, Yam98a, Yam98b, YS91a, YST99b, ZPY96, Zim96b, dWQ91a, vO91b, AA95, AD97, AD99, Ano90, ADS98, Bao94, BI94, BD98a, BS97, BS91a, Beuv94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cus95, DWZ96, Dam96, Den90, DVQ96, Dhe98, DN95b, ES97, FGM97a, GH96, Gib95, He92, HFW96, HJJ+97, JM96a, Jar96, Jon90, KASH90, KM99a, Kir95, KM99d, Koss9, LG97, Las92, LMJ93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LCL95, Lon91, Lon92, Low95, Mf90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rae90, Roe99, SW95a, Sch92c, Sha95a, She96a]. public
Bou94, Gol99b, IS97, Imp92, Jenxx, Kos99, Kuc92, Ler97, PC98, TSY98, Wal90.

Random-Number [ROT94, Bou94].

Randomisation [KI97]. Randomized [Man91d, PNSN91, BI94]. Randomness [BM99c, DIF94, DDP99, GW96, HL93b, KR94c, Nis96, DP91, Sot98, SB99, BGS95].


Rapid [KM93, GTS90]. Rate [BDGV93, BS91g, LKD98, Sti93a, Bla94a, BDGV96, KL95b, MHW98]. Rates [HK97, HR90].


RC2 [Ano97c, KSW97a, KSW97b, KRRR98, Riv98a]. RC4 [MT99c]. RC4-like [MT99c].

RC5 [Ano97z, BR96a, BK98e, BPV99, GPO98a, GPO98b, KY95a, KY95b, KY97, KY98, KYxx, KM96b, MAO96, Riv95c, Riv95b, Riv95d, Se98a, Yin97]. RC5-CBC [BR96a]. RC5-CBC-Pad [BR96a].

RC5-CTS [BR96a]. RC5P [KSW99b, KSW99c]. RC6 [BPV99, Con99b, CRRY99, RRSY98].

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

Reached [Lea99]. Reaches [MB99a].

Reaching [Gar94, HH94]. React [Par8c].

Reaction [HGS98]. Reactive [MK1].

Reactor [HRVV99]. Read [Sta97b, Coh96, LF97]. Reading [Eri97b].


Real-Quadratic [BBT94, BMT96].


Really [Ano93c, DDJ98a, Rit99, Sim90a]. Realms [ARH95]. Reappraisal [Sch99c].

Reasoner [MD99]. Reasoning [AG97a, BCM95, DSSB95, KM99c, MR95a, PK99, Var99b, Ger99b]. reasons [Ril96].

Reassessing [Neu95]. Reassure [MB99a].

Recasting [Sal91]. Receipt [BT94, SK95]. Receipt-Free [SK95, BT94]. receive [Way91]. received [Cl97, UU97b].


Recently-Proposed [Wag98b].

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

Recognition [HDC99, HA96, WD99b].

Recognizer [WB94]. Recognizes [Pin98].

Reconfigurable [BP99b, PJB99].

Reconcilable [BM99a].

Reconstruction [BC95b, BD98b, LH95]. Record [Har90, LCL92, Cha99b, CDEH+96, IEE96f, IE98b, JLM+94]. Record-Oriented [LCL92]. Recoverable [YY99b, YY98c].

recovering [PB97]. Recovery [AAB+97, Int91a, DC98c, GWQ+91, LL99, Miy96, Oka98a, Oka98b, Un98i, WLEB96, HMP95, JLM+94, NR95, Un97c, You99].


Recycling [SvA+98]. redefine [Gau97].


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

REDOC-II [BS91f]. Reduce [Hig97b, SVWMB95]. Reduced [BBS99a, BKR97, MT99a, BBS98a, PNRB94].

Reducing [DS98b, JQ98b]. Reduction [CTT94, GGH97b, BK98g, PP92a, PP95b, PP95a, SH95b, SOB98]. Reductions
NP98b, Pad98, PHF99, Rab94, SC96a, SZT96a, SZT96b, SZTB98, TKS98, ZK95, BBCP98b, BD97, FGY96b. **Robustness** [AN95, MMST98, YMWP99, Irw98].

**Rockland** [GS94b]. **Role** [Car97b, DDJ98d, JJ95, Lin96a, VC99, DL96, Dam96, Gua99, Mau93b, Sh98]. **Role-based** [JJ95]. **Role-Centered** [VC99]. **ROLLING** [PWU99]. **ROM** [Ano96i, GTGW94, Ros94, UFC94, Yuv97]. **Roman** [Has95]. **Rome** [Knu99c, Nat99b, Wol93b, Wol93a, 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]. **Rotations** [Con99b]. **Roter** [Mic93b]. **Round** [BJY97, BS93a, DP94, Dob97, GC94, KTM+99, Nat99c, SZ96, SK98c, SK98b, BD95a, NBD+99, Wer93a, Wer93b, HT98]. **Round-Optimal** [BJY97, DP94]. **Round1** [Bas98]. **Rounding** [BV97]. **Rounds** [BBS99a, dBB91, Bor95, DBR+99, KR94c, BBS98a, Dob98, PNR894, dB91]. **Routers** [DMVC99]. **Routing** [GRS96, RSG98, SGR97, CadHSV96]. **rover** [Bis90]. **Royal** [Far93, Tv92, Don98]. **RPC** [SSH93]. **RSA** [Ano94b, Ano95f, AA99, And93, Ano95d, Ano95c, Ano95a, Ano95j, Ano95m, Ano96b, Ano97e, Ano97f, Ano97g, Ano97u, Ano97v, Ano97a, Ano97w, Ano98a, Ano99a, BTDO98, BQ95b, BQ95a, BR95a, BR96c, BJQ97, Ble98a, BF97b, BDF98, BV98c, BD99b, Bon99, Bra95e, Bri90b, BM94c, Ca99, CH97b, CH98, CB96, CMM99, CMT9NY4, CD91, Cle96, Csc97, CFPR96b, CFPR96a, CN99a, CN99b, CN99, CNS99b, Cn99, CD96, Cus97, Dav95, Dem94, DDL9M94, DN95a, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FGMY97b, FMY98, FY98b, FR95b, GJKR96b, GKR97, GGOQ98, Gil99, GM97, GTS90, Gro94, GS99b, HN98, HWF96, Hor98, Hub91, HP94, IMI93a, IMI93b, JQ97, JQBD97, JQ98a, KR95c, Ka97a, Ka98b, KS98a, Kir95, Koc94, Ko96a, Koc95, Koc96b, Koy95, KOT95a, KOT95b, KK96]. **RSA** [Len98, LHL94, LL95a, Lou91, MWB99, MILY93, Mau90, MW98d, MW98c, MSS98, Mis97, Mis98, MS99c, Mue99, McL99, NS98b, NS98c, Oka98a, Oka98b, OSA91, PKP97, PP90, PW93a, Poi99, PS98g, Rab98, RS98e, RSxx, SSI97a, SSI97b, Sam98, SKNO98a, SKNO98b, SSS98, Sc94m, Sha95b, SV93, SH99, Sil97a, Sil97a, Sni93b, TY92, Tak97, Tak98a, Tak98b, T+99, T99, VV99, VNM99, Ven92, Vv97, Wal9c, Way98, Wie90b, Wie90a, Wir98, XL99, YWW, Zer96b, Zho94]. **RSA-120** [DDLM94]. **RSA-130** [Ano96b]. **RSA-Based** [CD96, GKR97, VNM99]. **RSA-Cryptosystem** [Gro94]. **RSA-Implementation** [PP90]. **RSA-Key** [FMY98]. **RSA-Keys** [SSI97a, SSI97b]. **RSA-Like** [JQ97]. **RSA-Moduli** [Mat90]. **RSA-Signatures** [Ev92]. **RSA-Type** [BJQ97, JQBD97, KL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b]. **RSA-Ab** [MP99]. **RSA-Euro** [Bar96b]. **Rtd** [KW92]. **RTR** [KV99]. **Ruby** [JS93a]. **Rueppel** [NMV98]. **Rule** [PL94]. **Rule-Based** [PL94]. **Ruling** [Eri97b]. **Run** [DF91c]. **Run-Time** [DF91c]. **Running** [RH93]. **Runtime** [WF94]. **Runtime-Tunable** [WF94]. **Russia** [CW94].

**S** [WG97, Ano95n, Ano96k, BD95a, DT93, ECD+99, Kim93, Mat95, MC96, PG97a, PG97b, SK98c, SK98b, St90, Uni97c, YS99, YY98d]. **S-Box** [BD95a, SK98c, SK98b]. **S-Boxes** [Kim93, PG97a, PG97b, DT93, Mat95]. **S-Coder** [St90]. **S.Hrg.** [Un98]. **S.I.S.**
[Eph98]. **S.I.S./CB** [Eph98]. **S/390** [ECD+99, YS99]. **S/KEY** [MC96].

**S/MIME** [Ano95n, Ano96k]. **S012** [KP95]. **S/390** [TSM95]. **S390** [Deu97, Deu98].

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

**Safer** [Hir93, BM97, CMKK98, KSW96, KSW98d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MS98, Miy96, Musee99, MV90, OOK91, OO93, OFF93, Pat95, Pet98, PM99b, RGV97, Sch99i, Smi90, Ver95, AW95, BD98a, CW97, CLHL98, CC95, CLW98, CMTN94, CGS97, FO93, FO98, GMLH94, GPS97, Gua90, Har91, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM+94, Ku92, LWC96, LLG10, MRR99, MS98a, MLA91, Mau91b, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SS98b, SVW9M95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WW95, v93]. **Schemes** [AW94, BP97a, BC93a, BDPR98, BD96w, BK94a, BK95b, BM96b, BM96c, BDG93, BD+94, BFS96, BM99c, BV96, BD90, Bri90a, BS91g, BLLV98, BBD92, CS97a, CM99a, CD95, Dan99a, DV990, DMPW98, DY91e, vD95a, DFKYZ99, DL97, FDB93a, FY97, FO093, FO99b, GPSN98, GP99, GS94a, HK97a, HK97b, IS91, JMO94, KPG99, KI96, KMOV19, KOS+94, KOO95b, KOO95a, LHW98, LM95, MH96, Mis98, MWW94, OK98, Oka93b, Pah98a, Pah98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SiK93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SSN99, YLD99, Zha98, ARK99, BC95a, BR97b, BI93, BDS93, BCD94, BG95, Blu95, BC96a, BCD96, BD96, BMS96, BD97, BFS98, BD98b, BD99b, Bur96, BM94c, CD9V91, CP95, CSV94].

**Scheduling** [KP93, Por98, SJS98, Sha99b]. **Schema** [Pit96b]. **Schemas** [Wed99].

**Scheme** [Int91a, ADF98, BCCG93, BM99a, BM99b, BF99c, BCS90, BY92, CT97, CK95, Cop94b, DQ94, DKKK98, DN94, GH90, GQW+91, HL93a, Hwa93, Hwa97, Iee91, IM93b, KKS97, KSK99d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MS98, Miy96, Musee99, MV90, OOK91, OO93, OFF93, Pat95, Pet98, PM99b, RGV97, Sch99i, Smi90, Ver95, AW95, BD98a, CW97, CLHL98, CC95, CLW98, CMTN94, CGS97, FO93, FO98, GMLH94, GPS97, Gua90, Har91, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM+94, Ku92, LWC96, LLG10, MRR99, MS98a, MLA91, Mau91b, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SSN98b, SVW9M95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WW95, v93]. **Schemes** [AW94, BP97a, BC93a, BDPR98, BD96w, BK94a, BK95b, BM96b, BM96c, BDG93, BD+94, BFS96, BM99c, BV96, BD90, Bri90a, BS91g, BLLV98, BBD92, CS97a, CM99a, CD95, Dan99a, DV990, DMPW98, DY91e, vD95a, DFKYZ99, DL97, FDB93a, FY97, FO093, FO99b, GPSN98, GP99, GS94a, HK97a, HK97b, IS91, JMO94, KPG99, KI96, KMOV19, KOS+94, KOO95b, KOO95a, LHW98, LM95, MH96, Mis98, MWW94, OK98, Oka93b, Pah98a, Pah98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SiK93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SSN99, YLD99, Zha98, ARK99, BC95a, BR97b, BI93, BDS93, BCD94, BG95, Blu95, BC96a, BCD96, BD96, BMS96, BD97, BFS98, BD98b, BD99b, Bur96, BM94c, CD9V91, CP95, CSV94].
OK95, Pad98, PS98a, PPKW97, Pf96c, 
PS96d, RD96a, RS96b, SI93b, Sha94, 
Sha95a, She92g, SW98, SW99a, SS94, SC97, 
TJ99, Tae99, VN99, WAM94, ZHS94, 
ZI98, 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, IEE97f, IEE98a, IEE99a, Ste91, 
Bed90, Beu94, Sch90c, Sch97c, Shp99a, 
Sim90b, Sim91, Sim94a, Sti93a, Van93, W199, 
Wie90b, W99, Al 96, AGY95a, BC95a, 
BT94, BI93, Ble96, BSV93, BCDV94, 
BDD+94, BG95, BCDV96, BG96]. 
Scientific [CHLT99, PH91, GTGW94, HW91]. 
Scientist [BCE+94]. scoop [Ano96m]. 
Scots [Sin99]. Scott [Sha99a]. Scramble 
[JSY99]. Scramblers [GDS91]. Screening 
[CN99]. ScriptEase [Ano97s]. Scripting 
[SvA+98]. Scripts [Dul90, Sch99a, IPNdbbbprnm91]. 
Scratchers [Dum94]. scrutiny [Den90]. 
SDK [Ano97s]. SDNS [NH90]. SDSC 
[Sch99]. SEA [Sch99], GC97]. SEAL 
[HG97a, HG97b]. Sealability [Por98]. 
Sealing [GS98]. Seamless [DFGH99]. 
Search [ADEC99, BD93, CD98c, HS90, 
KP99a, LC99, Mih94, Sal99, Way93a, Wie96, 
Wie97, Wie98a, vW94, vW99, CR97, GLV99, 
Gol90c, KR96b, Kuh98, Wie94]. Searches 
[PKA+98]. Searching [BP95a, DDJ98e, DDJ98f, Jia99, DSSZ99]. 
seasons [WFSF99]. Seattle [HF97, USE98a, USE99b]. Second 
[Auc98, Cha91, DFM92, Hir98, Nat99b, 
ACM90, AR97, FR95a, IZ99, Lea90, Pre95a, 
Uni96b, Uni95a, USE96d, VPM97, Hin93, 
PH91, HK97]. secondary [Atk93]. Secrecy 
[Aba99, BP98e, 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, CMS97, CGMW97, CK90, CFSY96, 
DDJ98g, DDJ98h, Da98, Dam94b, DDP94a, 
DKK98, DFIJ99, vD95a, EHM99, FW91, 
GPSNW98, GPSN98, H93a, HD96a, 
HK97a, HK97b, HCY96a, IS91, Kah96b, 
K96, Kra94a, KOS+94, KO995b, KO995a, 
LY93, LF97, LM94a, LM94b, LF99, LH93b, 
MSN99, Mau93a, MW96a, Mau97a, 
MS98, MS99, MT98, M92, NW98, 
OK98, PS98a, Pai98a, Pai98b, Ped91d, Pra96, 
Rey96, Rey97, Rey99, Sal91, Sch991, Sha99a, 
Sim90b, Sim91, Sim94a, Sti93a, Van93, W199, 
Wie90b, W99, Al 96, AGY95a, BC95a, 
BT94, BI93, Ble96, BSV93, BCDV94, 
BD97, BDV98, BG99, Bur96, CDGV91, 
Da97, Dam94a, Dwo91, El97, FOO93, 
FO98, GM95, GPSN97, Gre90, HNS91, 
HEL93, HJKY95, Hwa92d, H96, HLC99, 
J93, JMO95a, Jar96, JY98, KO95a, KO96, 
KO97, LY93, LH95, Mei92, MPSV99, OK96a, 
OK9, OK96b, OK95, Pad98, Ped91b, 
Ped91c, RD96a, RD96b, Ros97c, Sim90a, 
Sta96a, SC97, V97, Wie96a, WS96c, Win99, 
W98, ZHS94, vD95b, van97a]. Secret-Ballot [CFSY96, BT94]. 
Secret-Key [Ano97e, Bra95b, Bra95c, LM94b, Mai97a, 
Van93, Wol98, LM94a, JY98]. secret-sharing [RD96a]. secret-sleuthing 
[WS96c].Secretly [MT94]. Secrets 
[Cre90, DH90, DSB99, Ele98, HY93, 
MSK99a, Pes97, Rab94, Sch92b, Ste98b, 
We94, Ano91b, Bau97, BDV93, CWY98, 
JMO95b, W93, Ch92]. Section [Alv98c]. 
Secure [AHV98, AB96a, Ano93c, Ano93f, 
Ano95i, Ano99c, Ano99b, Atk97, AR99, 
Bal99, BQ95b, BQ95a, BM99a, BM99b, 
BR95b, BM99a, BM99b, BR91, BHK+99, 
BDHK93, BFS96, BS95b, BS98, BM94b, 
CG99, Car99, CG98, Cha90, Cy91, 
CR91, CC95, CKLS96b, CKLS96a, CKLS96c,
LHW99, Len93, LC95, MW94, Mar95b, MSN97, Mas97, Man91c, MKKW99, MF97, Mej94, MW98c, Nor95b, PS99d, PS99a, PS99b, PS99c, PGV93d, Pvo96, PR98.


September [Ano98f, D9+98, ES98, FR95a, IEE96c, IEE97e, IEE97k, Kat97, LW96, Q9+98, Spi95, TV94, T9+98, Uni97a, Uni96b, Uni98j, Uni98k, USE92b, USE98b, Gar98a]. seq [Cl97, UU97b]. Sequence [LY93, GM91, LY93, MHHMW98]. Sequences [DSV99, JQ97, MS94, Mun91a, Mun91b, PMP99, SB94, Bla94a, GN95a, Gol99c, KSB96a, MK92]. sequential [LHW99]. ser [IPndbbbrpm91]. Serial [SI93a, SSG99, Hor96]. Series [An95d, HEQL98, CJR98a, CJR98b]. Series-Parallel [HEQL98]. Serpent [ABK98c, ABK98b, ABK98a, BAK98]. servant [CWM9+91]. serve [Sch93c]. Server [An97r, An97s, BQ95b, BQ95a, DL99, ECD9+99, HS94, HCY96a, Kon95, LY93, LL95a, MW98d, NS98b, NS98c, Ol99, SVA9+98, Wat99, An97d, BM94c, HS96b, Hor98, LY93, MW98c, PW93a, Sin95, Ts90]. Server-Aided [BQ95b, BQ95a, HCY96a, LY93, LL95a, MW98d, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. Server-Side [SvA9+98]. servers [Abe98a, AG95, CGM97b, GGK+99, Lee95, Ude98]. Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau93, MB99a, RRSW97a, RRSW97b, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, Zha96, Ber96a, KN93]. Service-Level [MB99a]. Serviceability [WP90]. Services [ANS98b, Cas95, HVH98, RB94, VSH97, Ved98a, AA95, AC97, DS90b, Don98, KW92, PS99b, You97, Zer96a, AA95, Acc97]. ses [Bon94]. Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f,
Uni98h, Uni97c, Uni95a, Uni98k.

Session-Layer [BB95c]. Sessioneer [AG95]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB98, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Settled [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB98, Kra99].


Shakespeare [Lea90]. Shallow [ACD94, WF94]. Shamir [She92g, Ada92, GGOQ98, Nac93, OOK91, OO93, The95]. Shamir-like [Nac93]. Shannonite [Sga91a]. Shannon-theoretic [Sga91a]. Shape [HHD99]. shapes [Ger99b]. Share [BWM99b, Csi95, DDFY94, Sim90a]. Shared [BF97b, DHMR96, DF91a, DH90, HD96a, IS91, Lei99b, MWB99, PS98g, RZ99, SN96, Sim00b, Sim91, Sim94a, Wi99, YL97b].

Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [MSNW99, BDG99, CDGV93, OK95, ZHS94]. Sharing [AGY95b, BC93a, BC95b, BBDW96, BK94a, BK95b, BDGV93, BDD+94, BM99c, BD90, Bri90a, BS91g, Cac95a, Cac95b, CG98, CT97, CK90, DDP94a, DKKK98, vD95a, DLR97, FDB93a, FG96a, GJKR96b, GPSNW98, GPS98, HL93a, HKS97a, HKS97b, KI96, Kra94a, Kos+94, KOO95b, KOO95a, LP99, LCL92, LH93b, Mei92, MS95f, SN98, OK98, Pai98a, Pai98b, Ped91d, Rab94, ROT94, Sch92b, Sch91, Shi93a, Wil98a, AGY95a, BC95a, Bli93, BDV93, BDSV93, BCDV94, BG95, BCDV96, BDGV96, BD97, BDV98, BDG99, Bur96, CDGV91, CMPS97, CGMW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FG96b, FR95c, FO98, GM95, GPS97, HJKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, JMO95b, Jar96, KOO95a, KO96, KO97, Mao98, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, PS98a, Ped91b, Ped91e. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95a, van97a, Kol95]. Shark [RDPB96, WG97]. Shawn [Sha99a].

Shedding [HPG98, YHY98]. Shelf [Hat96, AG95]. Shell [Car99, Sch99a]. Shift [GO96b, Go94, GN95a, GM91, GO95, PS97]. shift-register [GN95a]. Shifting [LMBO95]. Ship [NS98a, RP98].

Ship-Board [NS98a]. shipping [Ano95k]. Shooting [Ada92]. Shop [Ano97c]. Short [Kra94a, Ste94a, Wie90b, vOW96, BC95a, Coh94, Har94, Joh99, VW96, Vv97, Wie90a].

Shortage [DDJ98a]. Should [Way93c, YS96, Ano95c, Riv98c]. shrinking [MS95a, MS95b, Mih96]. SHS [NIS93b, Nat92b]. shu [XtTuW94]. SIAM [ACM97b].

si [Ano97-29]. sichere [Hor99]. Side [KSWH98a, KSWH98b, KSWH98c, Sa+98, YY96]. sizes [MB94b].

Siege [EH96]. Siegenthaler [MS99b]. Siemens [Ano97-27, Bro97, Dau98c, Mac98, Sel98b, TJ97]. Sieve [LLMP90, LL93a, Per93, CDEH+96, Ger93b, Pom94].


Signal [IEE97c, IEE97d, IEE97k, LW96, Pit95, She92e, T+98]. Signalling [Lin98].

Signals [AK99, BTH96, DDNM98, MHMW98].

Signature [AA95, Acc97, AW94, Int91a, NIS94, Ano96e, Ano97-29, BP97a, BM99a, BM99b, BM96b, BM96c, Bra93a, CS97a, CM99a, CG98, CH98, CK95, CDFI95, CD95, DMPW98, DQ94, DY91e, DN94, FL99a, FKM98, FOM91, FO091, GP99, GQW+91, HJJ+xx, KKS97, KS98d, KPG99, Kob98c, Kra93, LK96, LHW98, LK99, LM95, LHL94, LL98, MT94, MB99a, Mer90b, Mer97, MH96, MSS98, Mis8, Mi96, Mon93, Nat91, Nat92a, Nat94c,
Nat94a, NMVR95b, Na97, NMV98, NMV99, NIS93a, OFF93, Oka93b, PF94, Pet98, PM98, PS96c, PJ99, RGV97, RDK98, Riv93c, dR94b, SC96a, Sch93b, Sch94e, SK97a, SE96, Sim93, Sin98, SB93, SSNP99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, ARK99, Ala93a, AW95, Ale97, BD98a, Bis90, Boy97, Bur96, CP95, CMTNY94, CSV94, DP96.

signature [FR95c, Gua90, HY93a, HJJ97, Hor98, HMP95, KS98c, LWC96, Mau91b, May97, MS98b, Mu92, NMVR95a, NR95, Pfi96c, Pit96a, PS96d, PS98h, SI93b, Sha94, SS95b, SS95c, Ste95, Til98, Tra97, TJ99, Wan92a, Wil93b, Wu92, XA98, YL95b, YL95a, Yue99, Zho94, dR94a].

Signatures [AN98b, AW98, AT99, BD99a, BQ95b, BQ95a, BG90, BdM94, BM94a, BM96a, BC93b, BFP99, Boy98, BS95d, CVHP91, CR91, CDF915, Cop99, CD96, Dam94b, DF91a, EG90, EG90, EvH91, Fro97, GKR97, GHR99, GO97, GO93, HK95, HA96, JM99, JQ99, JLO97, Leu96, LSV95, LR98, MS96, Mis97, MB97, NW98, OO98, Oka94, PIP97, PW93b, PV93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, Sch97, Tra99, Web98, Wri94, vHP93, BR96c, BGR98b, Ble96, BCP91, BM91b, Com97, CPS95, Cha95b, Dam94a, Ev92, EvH93, FBO7, FY95c, GJK96a, Jak95, Lan95, LL97b, Ped91a, Pf96c, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98]. Signcryption [Zhe97b, BD98a, Yue99, ZH98]. Signed [Ber97a, GMCF95, KT93, SKAM99, Sun98b]. Signer [CVH91]. signers [TJ99].

Ou99, SW94a, Tou92. Specifications [KS98a, Nat92b]. Specified [Gui97, HCC98]. Specifying [SW94a]. Specs [Got99]. Spectral [WF94]. Spectrum [CKLS97, She94c, CKLS96b, DIX94, KSB96b, KSB97, LLB98, OP98]. Speech [DMFB97, Er97b, GDS91, IEE97d, IEE97e, Lu97, SW95b, All97, CW94].

Speeches [Bar94]. Speed [ARV99a, ARV99b, Ano99c, Ano99e, DP98a, DP98b, Ebe93, FVEA99, IM93b, Koc94, LS97, MPPS95, SKNO98a, SKNO98b, SW97a, SW97b, She92d, She95b, IM93a, Kap98, KAK96, Lam99, Nor95a, HKSW98, HKRS99, Zhe97a]. Speeding [ADEDS99, KT93, McK99, Tes98]. Splitting [Sga91b]. SPM [CV93]. SPN [Kob99]. SPN-Structures [Kob99]. Spoofing [SVxW91]. SPRC [Wol93b]. Spread [CKLS97, DIX94, She94c, CKLS96b, CKLS96c, KSB96b, KSB97, LLB98, OP98]. Spreading [SB94, KSB96a]. Spring [DDJ98d]. Springer [Hat96]. Springer-Verlag [Hat96]. Spurs [Lea99]. SPX [Ala93b]. Spy [WS96c, Win91]. spy-catching [WS96c]. Synchronized [Cha90]. SQL [CM98]. SQL*Net [Ano95k]. Square [DKR97b, Dkr97a, EPR99b, EPR99a, Gar98a]. squares [BSN97]. squeamish [AGLL95]. SRA [SSH93]. SSH [Dar97]. SSL [Ano97r, FKK96, WS96a, WS96b, WS97]. ssmail [BRW99]. Stabbing [Aga2a]. Stability [Wed99, DXS91]. Stabilization [YMWP99]. Stabilizer [BS99a]. Stage [Ano97d]. staircase [MK92]. Stakes [GO96c]. stamp [HS91]. Stamping [BLLV98, BHS93]. Stamps [HKS95]. Standard [AA95, Acc97, Int91a, Nat93b, Ano93f, NIS94, Ano95i, Ano95j, Ble98a, Com94a, Com94b, FIP93b, FIP94, Gar98a, Gar98b, Kal97a, RSA93f, Law98, Len96, LM91b, Nat91, Nat93a, NIS93b, Nat94a, Nat95, Nat97b, Nat98, Nat99a, Natxx, NIS93a, Nys99, RSA93d, RSA93c, RSA93e, RSA93a, RSA99b, RP94, RD99a, RD99b, SB93, Ano90, Ano95c, CCN95, LM91a, Nat93c, NMVR95a, Pr94, Rev91, Tha91, Uni96a, Ada98, ARR99, ABK98a, Ano94b, Ano95n, Ano97b, Ano97x, Bar91, Bas98, Bas95, BS93b, Bir95, CM99k, Cop94a, DDJ98a, Den90, Gai90, Gar98b, HK98, HK99d, Hub98, Jol90, Kap98, KM97, Mat94a, Nat92a, Nat92b, Nat94b, Nat94c, Nat94d, Nat99c, NMVR95b, NBD+99, Pail96, Per91, RSA93b, RP94, Riv93c, She95b, She92g, Sim95, SB92, SB99, W199a, Ano95c]. Standardisation [Ved98b]. Standardization [Ano96k, Pr93b]. Standardized [Ano95n]. Standards [Ano90, Ano95n, Ano96k, Ano97y, Ano97z, Ano98i, DDJ98b, FBS97, Gar97a, Gar98b, Got99, GO96c, IEE94b, Kal93a, Kal99, MBB98, PP96, Ano92b]. Standards-Based [FBS97]. Stanford [IEE98b]. Stanica [VT96]. Stanley [vdWS97, vS97]. Star [Ano97r, HI97]. starts [Ano96l]. State [FGS96, Lan98, LF99, Mjo93, NM96a, Pre98c, PR98, Pre99, She92e, W093a, W093b, Zaj97, BFS92a, BFS92b, Gut96, PGV93d, Ril96]. State-industry [Zaj97]. State-of-the-Art [She92c]. Stateless [BGK99]. STATEMATE [DJHP98]. Statement [IH96]. States [Cli97, Cli99, Lev91, Mil95, UU97b]. statesman [Bed90]. Station [BMW99b, Smi98b]. Station-to-Station [BMW99b]. Statistical [De 99, GC91, GSV99, Gus96, PNFK95, NO98, Tha91, GKS97]. Statistics [BBDF97, IEE94a, FO90]. Status [Doh96b, FL99b, Nat99c, NBD+99, Ros95b]. Stay [MK94]. Staying [Rit99]. Steady [MSHP99]. Steal [Wal99b]. Steganalysis
Summer [USE94, Mye96].

Supercomputer [DMS95, She92e, Bam97].

Supercomputing [CFK +91].

Superhighway [BDC+95].

Superimposing [YY91].

Superimposed [Kob91c].

Supersafe [PP96].

Superscalar [Cla97].

Superscript [Cra92, CF92].

Supersingular [BS91b].

Supervisory [KA99].

Surmounting [CI96].

Surrounding [GA98].

Surveillance [CKN99, SB97].

Survey [Bri90b, Gar97c, GFB93, Kal93a, Kle90, Knu98b, Par98c, BO92, Ele99, Mea95, She92e, Wad98, Zho94].

Surveys [Ell99].

Susceptibility [AW94].

Supported [LHL95b, LHL95a].

Swapping [TN97].

Swedish [LF97].

Switches [Bel92].

Switzerland [ACM90, ACM91, ACM93b, ACM94e, ACM95, ACM96b, ACM97b, ACM97c, ACM98b, ACM99b, Ano99c, Com96, CMM93, DEQ92, Hei96a, IEE92c, IEE93b, IEE94d, IEE95b, IEE96a, IEE97f, IEE97i, IEE98a, IEE98e, KK99b, Q+98, Spi95, SLJ93, USE92b, USE93, USE95b, USE96b, USE96g, USE98a, USE98d, USE99a, Wat91, Wol93a, Wol93b, Tv92].

Synchronised [KI97].

Synchronization [DHSS95, BCCG99].

Synchronized [Yah94, Con92].

Synchronizing [Mau91a].

Systematic [BCCG99].

Systematising [MKL99].

Systems [BGH95b].

Systems [ABL93, AKP96, AFK94, Ako99, Ano94j, Ano95i, Ano96a, ADEDS99, AA97, AMP99, BDPSNG95, Bar99, Bas93, BR91, BBDF97, BFN98a, CF95, DDJ98a, Dam91b, DFTY97, DLY91a, DD99, DB96, ENK99, FJP96, FY95a, FY95b, FYM99, FOO91, GL96, GB93, Gil98, GM90, GMW91, GK96, GS97].
GMV98, HGHD98, HJJ\(^+\)xx, HH94, HP98b, IEE93a, IEE96b, IEE96d, IEE98c, IEE99b, IH99a, KT96, Koc96b, KA99, KYB92, LO91b, LQRS98, LABW92, Lan99, Lee99b, Mar99, Mas99a, MS95f, MDP94, Mu993, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PS96b, PSN91, Pin97, Pit96b, PM99a, PP99b, RBvR94, RG95, RIP95a, ST94, SN96, STS99b, DY91c, SOOS95, SS90, She92a, SY92, Stu99, Tra99, USE96c, USE99a, VC99, Var99a, Way93a.

**Systems**

[WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFKP98, ZFK\(^+\)98, ARK99, AHdJF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BP95b, CG05, DMW94, Dix94, Fri92b, Goo96, GKS97, Gru98, HJJ\(^+\)97, IEE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Oh96, Ole95, Opp96, PA98b, PP92a, PP95b, PP95a, RO96, SK97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DV96].

**Systolic**

[SSS98, DF92, PJBM90].

**SZ42**

[Dav98d].

**SZK**

[GSV99].

**T**

[YT96, PDGI99].

**T-Team**

[PDGI99].

**T52**

[Day98c].

**T52e**

[Sel98b].

**Table**

[KMKH99, Has99, Hor95].

**Tableaux**

[Mas99a].

**Tableaux-99**

[Mas99a].

**Tables**

[DRR95, JC98].

**Tactical**

[IMK99].

**Tagging**

[Lud97].

**Tailoring**

[CGM96].

**Taken**

[GQW\(^+\)91].

**Tale**

[Kal98e, RS98f].

**Talent**

[DDJ98e, DDJ98f].

**Talk**

[Deu97, Lei99b, Wat99].

**Talking**

[HH99].

**Tamper**

[Auc96, BDH98, KK99a, Zhe95b].

**tamper-proof**

[Zhe95b].

**Tamper-Resistant**

[Auc96, KK99a].

**tamperfree**

[Hwa92b, Hwa92c].

**Tampering**

[CL98, CL97b].

**Tanaka**

[Hwa92a, MS98a].

**Tandatangan**

[Ano97-29].

**Taos**

[WABL93, WABL94].

**tapestry**

[MB94b].

**TAR**

[Ano97].

**Targeted**

[Cap94].

**Targets**

[Lea99, Way98].

**TAS**

[Cop94b].

**Tasty**

[Sch98i].

**Tate**

[FMR99].

**Taxing**

[Gar97c].

**Taxonomy**

[DB96, GS97, LBMC94].

**TC**

[MB99b].

**TC11**

[Kat97].

**TC6**

[Kat97].

**TC6/TC11**

[Kat97].

**TCFS**

[Mau97b].

**Tcl**

[GA98].

**TCP**

[Fei93, Fei96].

**TCP/IP**

[Fei93, Fei96].

**TEA**

[KSW97a, KSW97b, NW97, WN95].

**Team**


**TecPro**

[GLC98].

**Technical**

[Ano95e, Bar96b, CFK\(^+\)91, CYY98, DS97, Lan98, LM93c, Mos98, USE95a, USE99d, VGP93, SM99, USE96f, USE98c].

**Technique**

[DDNM98, Gne98b, KP93, WD97, BCV97, ONT98, Way95].

**Techniques**

[Int91a, BGML96, BW98, Bo98a, Bo98b, BLM094, CM97b, CD99, CMYY98, Da90a, Da91a, Dav91, DC98c, De 95, Des98a, Des96a, Funk97, Funk98c, GQ95, Hel94, J99a, LvdLB96, MM99a, MSNW99, Man96b, PS98e, PS98f, PK99, Pre93b, QV90, QQ95, Rue93, SZ93, Car98, Cra96, Hel93, Hel98b, ISO97, Kay95, KG93, Nyb98, OP\(^+\)99, Oke96, PS99d, SD97, Ste99b, Way91, Woo90, ZH93, van96].

**Technological**

[UFC94].

**Technologies**

[Dan96, DSS98, Aus96, BV97a, BK94b, BS95e, Oht96, UNI96].

**Technology**

[Int91a, Ano96i, Ano98j, AA97, Ban93, BDDG99, DKK\(^+\)98, Fol99, Gar98a, Gar98b, GN95b, Hat96, HH96, IE94b, IE98d, Lie94, L93c, NF99, Riv98c, USE99c, Ano93a, DS97b, Gil97, ISO97, Ril96, Ros94, Smi97a, VB96, CFK\(^+\)91, Ers99, Ano99b].

**Telecollaboration**

[Fuc99].

**Telecommunications**

[IEE97e, UNC94, Mac98].

**Telemedicine**

[Ano97-29].

**Teleperubatan**

[Ano97-29].

**Telephone**

[Gar97a].

**Telephony**

[Ba94, Gar97b, MB99a, Mar95b].

**teletype**

[Mac98].

**TELNET**

[SSH93, Ala93b, Bor93a, Bor93b, Bor93c].
RH99, Sch99f, Sho97, Tro93, VBD99,
Yac99a, Yac99b, ACC99, BP98d, BHS93,
BM96b, BM96c, BK98f, GKS97, HS91,
IEE94b, MAM95. time-stamp [HS91].
Time-Stamping [BLV98, BHS93].
Time-Stamp [KA99, DOR99]. timed-release [DOR99].
Timeliness [Yah94]. Timely [KYB92].
Timestamp [W99]. Timetabling [CC99c].
Timing [DS98b, EH96, HK98, HK99d,
Koc96b, MM92a, MM94, BS95e, Koc95].
Timken [Kar96]. tiny [WN95].
Tip [Zuk98b, Zuk98a]. TIRPITZ [Wei99].
TLS [Pau99]. TM [Sch98h]. Today
[Car98, UU97a]. Token
BE90, Nys99, YL97b. Tokens
[Jue99, KS99a]. Tolerance
PW97c, IEE94b, TCH+91. Tolerant
DHSS95, OKST97, RBvR94. Tomayko
[CWM+91]. Tommy [Pin98]. Tomorrow
Tool [AKP99, KKW99, Sch99k, WB92,
YY97c, Ano97u, Bur96, DFHR91, KKW99].
toolkit [BP97b, Way98, Rei96]. Tools
[BY93a, Des99a, GS97, RB99, WC97, DD95,
LS98a, Mee99]. Top
[Ben98, Hel93, MB99a, Mus92]. TOP500
[DS97d]. Topics [IEE99b]. Topological
[OMA98]. Topology [COZ99]. toral [VP96].
Torn [MR98]. Torok [Lip93]. Toronto
[IEE94f]. Toshiba [Got99]. Touches
[MB99a]. Toulouse [DEQ92]. Tour
[Han94, Mos99]. tourist [WSFC99]. Town
[IEE94a]. Traceability
[GSY99, SW99b, Des95, LHL95b, LHL95a].
Traceable [BW97, T99]. traceability
[Sta97a]. Traced [Pf996b]. Traces
[Vig98, HM97b]. Tracing [BF99c, CFN94,
Fia94, FT99a, Jue99, Mad92, NP98a]. Track
[USE98c, Fox99]. Trackies [SKIT99].
Tracking [HCDC99, Hur98]. Trade
[BFS96, BSM96, Un98d, Un98e, NMVR95a,
NMVR95b]. Trade-offs
[BF99, BMS96, NMVR95a, NMVR95b].
Trademark [Eri97b]. Tradeoff
[KR94c, CK93]. Tradeoffs [CMN99].
Trading [FMH98, DS97b]. Traditional
[Des92]. Traffic
Train [BW98]. Training
[ACBR90, DTDJ99, Jen99]. Traitor
[BF99c, FT99a, NP98a]. Traitors
[CFN94, Fia94, Pf99b]. Transaction
[ENK99, KT96, Oh99, CTSxx, ADDS91,
A091a, JD91]. Transactions
[FL99b, FKM98, SSG99]. transcendental
[PGCS96]. Transcript
[BD99a, Chr99a, Sas99a].
Transcript-Irrelevant [BD99a]. Transfer
[An97s, DF99, HHY93, NP99, RS96a,
Bea93, BM90, BR96b, DOR99, Jac90a,
Jac90b, SI93b]. Transferable [Sak96].
transferred [Un97d]. Transferring [SI94].
Transform [Boy99, KMS95a, KMS95b,
Kuo90, MS94, Riv97c, WF94, TK98].
Transformability [MS96]. Transformation
[SZ96, LS98a, Pet91]. Transformational
[Zwi98]. Transformations [BDFM99].
Transfusion [ADB99]. Transient
[BDH98, CH94a, JQBD97]. Transistors
[CWM+91]. Transition [Des98a, DR98b].
Translation [CFK+91, OP97, OP98].
Translucent [BR96b]. Transmission
[NHB98, PSB97]. transmitting
[Cl97, Cl99, UU97b]. Transparent
[Bla93, DS97c, Maul97b, SZT96b, ZG96].
Transport
[An94b, BWM98, GBC93, Sar97].
Transportation [BPR99, Uni98b].
transposition [Bar92a, Bar95, GSN94].
Transputer [GN95b]. trap [Yu92].
trap-door [Yu92]. Trapdoor
[BM92, BY93a, BHSV98b, BHSV98a, Pia99c,
RP97a, WBDY98, And93, Gar96a, Gar97d,
Ort95b, Ort95a, Way93b]. Trapped
[Gib91, Gor93a, Pat99]. trappes [Sch98e].
Traveling [OMV98, RS99a]. Travois [Yuv97]. treaties [Des90a]. Treatise [Tur99]. Treatment [BFN98b, Mau96a, O998, BDJR97, BFN98a]. TREC’98 [LM98a]. Tree [BM96b, BM96c, GM99b, PB99a, LL93b, O’C95].

Tree-Based [BM96b, BM96c]. tree-structured [O’C95]. Tree-Width [GM99b]. Trees [Aga92, BP97a, HS90, ZW99, SSM92]. Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De 93b, De 98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].

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

Tree-Based [BM96b, BM96c].

Tree-Structured [O’C95]. Tree-Width [GM99b]. Trees [Aga92, BP97a, HS90, ZW99, SSM92]. Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De 93b, De 98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].

Tree-Based [BM96b, BM96c].

Twenty [Ano95l, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, Gol97c]. twenty-eighth [ACM96b]. twenty-fifth [ACM93b].

Twenty-Ninth [Ano95l, ACM97c].

twenty-second [ACM90], twenty-seventh [ACM95], twenty-sixth [ACM94c], twenty-fifth [ACM93b], twenty-fourth [ACM92], twenty-third [ACM91], twenty-second [ACM90], twenty-first [ACM89b], twenty [ACM88b], nineteen [ACM87c], eighteen [ACM86c], seventeen [ACM85b], sixteen [ACM84b], fifteen [ACM83c], fourteen [ACM82b], thirteen [ACM81b], twelve [ACM80b], eleven [ACM79c], ten [ACM78c], nine [ACM77c], eight [ACM76c], seven [ACM75c], six [ACM74c], five [ACM73c], four [ACM72c], three [ACM71c], two [ACM70c], one [ACM69c].
Unbalanced [Jut98, KPG99, SK96c, SK96d], unclassified [KC95]. Unclassified [Bra90a].


UMAC [BHK+99]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97]. Uncompressed [NHB98, HG98].

Uncompressed [NHB98, HG98]. Unconditional [CM97a, FM98, GM90, WP90, Wai90, Wol99, MSN97].
[ANS97, ANS98b, Ada97a, AGS97, AHdJF97, Ano99h, BDP5NS97, BCK96e, BBS99a, BFP99, BW98, CIBM99, CK95, CM99d, Des96a, DS97d, EST99, FVEA99, FW91, FY98b, GM97, GAGCDAFC99, GS99a, HNSS99, HRVV99, HJPB97, IR99, JM99, JI98c, JQ97, KR94b, K99a, KA99, KT93, Lon92, LF99, LML98, LW99, LD97, MAM95, Mih94, MCD99, Mis97, MFG95, NT99, NHB98, NNEK97, Oh99, OOK91, Ou99, OMJ93, PS97, Ph97, PJ99, QG90, RB99, SG95, SK94, Sbs99a, SK96a, SK97b, SK97g, SK97c, SD99, SRY99, SR96, ShM94, SHK99b, Sun91a, STZ98a, TAP90, TYD99, TOU94, VN94, WKHG97, W9S95, Yam98b, Yam99, YST99a, YY97a, YST99b, AA95, Ait98, Ata94, BSN96a, BSN96b, BTD98, BGR95, B93, Bi94a, BB95a, BB95b, BB97a, BD95a, CW91a, CNST98, CC95].

using [CGM97b, CPPK98, CB96, Cle96, Dan97, Jak95, JM96a, KR95a, KC95, Kar96, Kay95, Koe95, KH97, K99a, LC96b, LC96c, LMBO95, MHP96, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SSM94, SD97, Su98, STZ98b, STZ98, Tk97, Til98, VZ97, VP98, Wh93a, Wil93a, Yam98a, Zho94, dR95].

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


Verschlüsselungsverfahren [Ger97]. Version [Ano97r, Ano97s, BC93a, BP98e, DBP96, FKK96, Gar97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, RSA93f, Lim99, MT99a, Mc96, RSA93a, RSA94, DY91c, SS99b, SM98b, WABC99, CLW98, GM93a, Gib95, Bo93b, Lin96b]. Versus [MGL+98].

Vertraulichkeit [FT95]. Very [HMV93, MSDS90, PF94, Yua92, SN94]. Veto [OK96a]. VHDL [Oel97]. via

MBB98, Mos98, OMA97, OMA98, PZ98, QN98b, RKDB96, SCxx, SZT96b, SZT98a, WK97, WD97, Xie98, YY99a, ZK96, BBCP97, BBCP98b, BBC98, BCD98, BP98d, BCV97, BO96a, CPO+98, CHO+98, CT99b, CKLS96c, CM97d, DDQM98, DDM96, DDM98, DNSS98, HG96, HG97e, HEG98, HPA99, HW97, HW98a, HW98b, Iw98, Kh97, KH98a, MTTN97, Nat97a, NO98, NP98b, ODB96, OP97, OP98, OPH+99, Oko96, PHF99, SD97, SHG98, SZTB98, TA97, TKS98, VP96, VP98, VN98, Ye97, Ye98, YM98, ZK98, ZKOY99.

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

Watson [CFK+91].

Wave [GO96c].

Waveguides [FVEA99].

Wavelet [LSVV95, KH97, KH98a, NO98, XA98].

wavelet-based [KH97].

Wavelets [Lut98].

Waves [Dal97].

Way [BJY97, BdM94, BM94a, BKK98, BP97c, DGV93, DDP90, GMDS98, Mer90a, Roe94, Sch91b, TOU94, Zhe90, BHH99, BK98f, DI99, Dob98, HILL99, HILY99, Hwa92a, MZI98, Rom90b, Sim98c, Sta94a, Sze98, Tsu92b, Tsn92a, ZPS93, KS97a, KS97b].

Wayner [vdWS97, vS97].

Wayness [HT99].

ways [Dun95].

WDAG [TV94].

Weak [DGV94c, DYL98, Haw98b, Pit96b, Sze98, Vau96, FY95c, Hau98a, Knu95, ISS97a, SS97b, YL97b].

Weakened [AB99a, AB99b].

Weakly [MP91].

Weakness [Cop99, KS99a, Kie98].

Weaknesses [BMS94, DY91e, Kel99, KP93, Lan96, PA98b, RK98a, Rij99, SZ96, DGV94b, She96b, ZZ97].

weapon [Ano97].

wepons [ Mei98].

Web [Ano97r, MR98, OW95, SA95, Sta95a, Ver98b, Ale98, Ano97d, Bal99, BMNI99, Cha99b, Dav95, DDK98, FL96, GGM97, GO96c, Law98, She96b, Ud98, WCSS95, You96, ZL99].

Web-Based [ZL99].

Web-enabled [Cha99b].

WebTime [Ano97s].

Weighing [KR96a].

Weight [PK95a, PK95b, Pen96, She95c, BGH+95a, CC98].

Weighted [MPSV99].

Welcome [Riv95c].

Wen [Xu99].

Weren't [Kab91b].

West [DDJ98c, Fra99, Hir97, Hir98].

wheel [Car97c].

Wheeler [Bar95].

Where [DDJ98e, DDJ98d, LHL95b, LHL95a, Van95b].

wherein [Lea90].

Which [Che92, EvH91, Ev92, EvH93, Gir99].

while [vdWS97, vS97].

Who [BCE+94, DDJ98d, Mar95a, Mon96].

whom [LC95].

Whose [Ano94j].

Wide [Ale98, Dav95, OW95, She96b, CDEH+96, Wad93, HC95b].

widespread [Cli99].

Width [GM99b].

Wie [MPS94].

Will [DDJ98d, Gar97b, GC97, Gar98a, Wor96, Ano98b, Goo97, Mi99, Sch93e, ZKOY99].

William [Lea90, Uni92, vdWS97, vS97].

Williams [JQ98b].

Window [Bel92, KT93, PKA+98].

Windows [USE98a, Boy98, Bru98, IH98, Ken95, RC95, ZG96].

Windsor [SJ93].

Winkel [Ers99].

Winnowing [Riv98d].

Winter [USE91, USE92a, USE96c].

WIPO [Gar97c].

Wire [Wal94].

Wireless [Gar98a, PS98d, She93d, Goo96, IEE97k, PS98e, PS99d, PS99a, PS99e, WSFC99, PS98c, PS98f].

Wiretap [Ele98].

wiretapping [DL98, RK94, Rot95a].

wisdom [JC98].

Wise [Ano96j].

Within [BGV93, BGM97a, BGM97b, FL93, HJTW99, KW92, MG98a, MG98b].

Without [BP97a, BMRW98, GHR99, Hus99, Len96, Luc98b, SG99a, Abe99, Ano98j, Ben94, Ble96, HY93a, HG97d, Hor95, IS91, JMO95a, JC98, KRS99, LM94a, LM94b, LWC96, Ped91c, BB97, Riv98d, Sak97, Smi94b, SS99c, SS99f, Wu92].

withstand [OY91].

Withstanding [SVxW91].

Witness [CDS94, FGY96b, FGY96a, RGV97].

Witness-based [FGY96b, FGY96a].

witnesses [She92b].

Woes
References

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

Anonymous:1997:ACC

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

Anonymous:1997:ACC

ANSI:1988:FIE

Anshel:1993:PMT

ANSI:1995:ANS

Abdikalikov:1999:ERC

Abelson:1997:RKR
Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John


REFERENCES


**Abe:1998:UVM**


**Abeles:1998:SVP**


**Abe:1999:RDM**

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

**Anderson:1998:SPA**


**Anderson:1998:SNBa**


**Anderson:1998:SNBb**


**Abadi:1991:ADS**

M. Abadi, M. Burrows, C. Kaufman, and B. Lampson. Authentication and

Abadi:1993:ADS


Abadi:1993:CAC


Abraham:1997:SEE


Auyong:1997:ASC


Apolloni:1990:TNN


ASCFS:1997:XPK

REFERENCES


[An:1999:ODR]


REFERENCES


REFERENCES


REFERENCES


REFERENCES

ucsb.edu/conferences/ java98/program.html.


Ajtai:1999:PKC


Ada91


Adams:1992:IAB


Adams:1997:RCE


Adams:1998:CSA


Achour:1999:UUK

REFERENCES


[ADL87] Leonard Adleman. Pre-RSA days: History and

Asokan:1999:APT


Alves-Foss:1995:ACS


Apostolico:1985:CAW


Anderson:1995:SFS


Abadi:1997:RAC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Alberti:1470:TC


Alexander:1945:CHG


Alexandris:1992:FMC


Alexandre:1997:BSC


Alexandre:1998:JBP


Allen:1997:DEC


Allen:1998:SUM


Ahituv:1987:PED

REFERENCES

//www.acm.org/pubs/toc/
Abstracts/0001-0782/30404.

[Aiello:1998:FDI]
W. Aiello, S. Lodha, and
R. Ostrovsky. Fast digital
identity revocation. Lecture
Notes in Computer Science,
1462:137–??, 1998. CODEN
LNCS09. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

David Alvarez. Faded lus-
tre: Vatican cryptography,
1815–1920. In Deavours
et al. [DKK+98], pages 191–
225. ISBN 0-89006-862-
US$78.20. URL http://
www.opengroup.com/open/
cbbooks/089/0890068623.
shtml. Third volume of se-
lected papers from issues of
Cryptologia.

David Alvarez. Italian
diplomatic cryptanalysis in
World War I. In Deavours
et al. [DKK+98], pages 181–
190. ISBN 0-89006-862-
US$78.20. URL http://
www.opengroup.com/open/
cbbooks/089/0890068623.
shtml. Third volume of se-
lected papers from issues of
Cryptologia.

[Akl:1985:FPR]
Selim G. Akl and Henk Mei-
jer. A fast pseudo ran-
dom permutation generator
with applications to cryp-
tology. In Blakley and
Chaum [BC85], pages 269–
275. CODEN LNCS09.
ISBN 0-387-15658-5; 3-540-
39548-7. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A1
C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&page=269. CRYPTO
84: a Workshop on the
Theory and Application of
Cryptographic Techniques,
held at the University of
California, Santa Barbara,
August 19–22, 1984, spon-
sored by the International
Association for Cryptologic
Research.
REFERENCES


REFERENCES

tronic). URL http://
link.springer-ny.com/ link/service/series/0558/
bibs/0658/06580482.htm;
http://link.springer-


link.springer-ny.com/
link/service/series/0558/
bibs/0963/09630236.htm;
http://link.springer-


REFERENCES


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

**Anonymous:1939:ITM**

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

**Anonymous:1960:CNH**


**Anonymous:1976:CCA**


**Anonymous:1978:CSD**


**Anonymous:1978:ODA**


**Anonymous:1980:ACS**


**Anonymous:1981:CHP**

Anonymous. Corrections: How Polish Mathematicians Deciphered the Enigma, 3(3) 232, Reviews: H. H.
REFERENCES

Anonymous:1981:GIU

Anonymous:1982:CC

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

Anonymous:1982:NNPa

Anonymous:1984:ESC

Anonymous:1985:BM
References


Anonymous:1991:E


Anonymous:1992:AUd


Anonymous:1992:DES


Anonymous:1992:DDS


Anonymous:1993:ACT


Anonymous:1993:BRd


Anonymous:1993:CKR


Anonymous:1993:CSA


Anonymous:1993:CNh


Anonymous:1993:FSH

REFERENCES


[Ano93k] Anonymous. What’s new: The DTR-1 is a notebook or a pen computer, the SmartLink V32bis FaxModem encrypts your data, LapCAD 5 for the Mac gives you finite modeling, and more. *BYTE Magazine*, 18(6):57–??, May 1993. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).


[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


Anonymous:1995:ARD


Anonymous:1995:ENAa


Anonymous:1995:ENb


Anonymous:1995:FSH


Anonymous:1995:NIX


Anonymous:1995:OIN


Anonymous:1995:PTN

REFERENCES

Anonymous:1995:RLM


Anonymous:1995:SUE


Anonymous:1996:NIS


Anonymous:1996:RF


Anonymous:1996:ADX


Anonymous:1996:BCU


Anonymous:1996:CID


Anonymous:1996:CPD


Anonymous:1996:ENa

REFERENCES


[Ano96k] Anonymous. Standards update: Standardization efforts for triple-DES continue; IEEE P1363 works toward integrated draft; PKCS #11 / Cryptoki Workshop held at MIT; more progress on S/MIME.

Anonymous:1997:ENb

Anonymous:1997:TBAa

Anonymous:1997:RDSa

REFERENCES


Anonymous:1997:DNH

Anonymous:1997:ENa

Anonymous:1997:ENb

Anonymous:1997:ENc

Anonymous:1997:EW

Anonymous:1997:HEW

Anonymous:1997:INI

Anonymous:1997:MNL
Anonymous:1997:NPA

Anonymous. New products: AcceleratedX Server Version 3.1; CDE Business Desktop; DNEWS News Server 4.0; SecureNet PRO v2.0; Dynamic Modules; Stronghold Encrypting SSL Web Server; SOLID Desktop; Lone Star LONE-TAR 2.2gn Shop; Cactus System Crash AIR-BAG 3.4.1.1. 


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:RCU


Anonymous:1997:RAJ


Anonymous:1997:RDL


Anonymous:1997:RDSb


Anonymous:1997:SFR


Anonymous:1997:SUE

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


**Anonymous:1997:SUR**


**Anonymous:1997:SSA**


**Anonymous:1997:CBP**


**Anonymous:1997:UUS**


**Anonymous:1997:UPP**

Anonymous. USACM participates in protest against restrictions on cryptography research and development. *Communications of the Association for Computing Machinery*, 40(11(S)):5–??, November 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

**Anonymous:1998:ARD**


**Anonymous:1998:CSIb**

Anonymous:1998:ICS


Anonymous:1998:EN


Anonymous:1998:Ea


Anonymous:1998:PCA


Anonymous:1998:SIb


Anonymous:1998:SIC

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

Anonymous:1998:SUP


Anonymous:1998:TBF

Anonymous:1999:RDS


Anonymous:1999:AWS


Anonymous:1999:CCI


Anonymous:1999:DSC


Anonymous:1999:DSV


Anonymous:1999:KNT


Anonymous:1999:L

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

124

Anonymous:1999:SFU

from this page; another alphabet table is shown in the colourlab.com URL.


ANSI:1997:AXP


Anderson:1996:CCA


Abbott:1993:INT


REFERENCES


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

**Adleman:1983:CCS**


**Aiello:1999:HPN**


**Aiello:1999:HSP**


**Ashenhurst:1987:ATA**

REFERENCES


USENIX:1988:CSSb


Asokan:1998:OFE


Abdalla:1999:TMB


Atkins:1996:RPM


Akl:1983:CSP


Ateniese:1999:SOI

REFERENCES


REFERENCES


[Aur96] T. Aura. Practical invisibility in digital communications. In Ander-
REFERENCES

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

Anderson:1996:NC

channel. In Anderson [And96c], pages 151–156. CODEN LNCS99. ISBN 3-540-

Alabbadi:1994:SDS

[AW94] M. Alabbadi and S. B. Wicker. Susceptibility of
digital signature schemes based on error-correcting
codes to universal forgery. Lecture Notes in Computer

Alabbadi:1995:DSS

scheme based on linear error-correcting block

Angel:1999:JQH

Dave Angel and Andy Wilson. Java Q and A: How
do I store a Java app in a self-executing encrypted
file? Dr. Dobb’s Journal of Software Tools, 24
URL http://www.ddj.com/1999/9902/9902toc.htm;

Aspray:1988:RCD

William Aspray, Maurice V. Wilkes, Albert C.
Lewis, Greg Mellen, Harold Clucker, Robert V. D.
Campbell, Wendy Wilkins, G. J. Tee, Ernest Braun,
and Arthur L. Norberg. Reviews: Carpenter and
Doran (eds.): A. M. Turing’s ACE Report of 1946
and Other Papers; Masani (ed.): Norbert Wiener: Collected
Works with Commentaries; Kozaczuk: Enigma: How
the German Machine Cipher Was Broken and How
It Was Read by the Allies in World War Two;
Worthy: William C. Norris: Portrait of a Maverick;
Harvard Computation Laboratory: A Manual of Op-
eration for the Automatic Sequence Controlled Cal-
REFERENCES


AufderHeide:1999:PGP

[AWV99]
REFERENCES


REFERENCES

Bakker:1999:MAS

Ball:1997:ESS

Ball:1999:WSB

Bullitt:1999:GDI

Bamforth:1997:JSS

Burrows:1989:LAb

Burrows:1989:LAa

Burrows:1990:LA
REFERENCES

Banisar:1993:BCE

Banisar:1994:CPS

Bao:1994:IRL

Barker:1961:CSC

Barker:1975:CSS

Barker:1977:CHC

Barker:1979:CEC

Barker:1979:HCCb
Wayne G. Barker, editor. *The history of codes and ciphers in the United States during the period between the World Wars*, volume 22,
REFERENCES


[Barker:1979:HCCa]


[Barker:1984:CSG]


[Barker:1987:IRS]


[Barker:1991:IAD]


[Barker:1992:CSC]


[Barlow:1992:DPP]

REFERENCES


REFERENCES


REFERENCES


REFERENCES


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

Bennett:1991:EQC


Barni:1998:MPI


Blakley:1993:TSD


Blakley:1993:TPD


Bennett:1995:GPA

REFERENCES


tion with the University of Saragossa.

**References**


REFERENCES


REFERENCES


Bos:1993:PUS


Beguin:1995:GSC


Beimel:1995:SSP


Blundo:1995:SRB


Blundo:1996:BES


Brassard:1996:YQC


Blakley:1998:C

REFERENCES


Burwick:1998:MCC


Barker:1988:ECT


Bigun:1997:AVB


Blair:1999:DRA


Baritaud:1993:SPK


Brucoli:1999:DHC

[BCCG99] Michele Brucoli, Donato Cafagna, Leonarda Carn-


REFERENCES


REFERENCES


nals of the History of Com- 

cputing, 5(4):411–427, October/December 1983. CO- 

DEN AHCOE5. ISSN 0164- 

1239. URL http://dlib. com- 

puter.org/an/books/ 

an1983/pdf/a4411.pdf; 


[BCR98] Francesco Bergadano, Bruno 

Crispo, and Giancarlo 

Ruffo. High dictionary com- 

pression for proactive pass- 

word checking. ACM Trans- 

actions on Information and 


25, November 1998. CO- 

DEN ATISBQ. ISSN 1094- 

9224 (print), 1557-7406 (electronic). URL http: 

//www.acm.org:80/pubs/ 

citations/journals/tissec/ 

1998-1-1/p3-bergadano/.

[Berbecel:1997:MTW] 

[BCV97] Gh. Berbecel, T. Cooklev,

and A. N. Venetsanopoulos. Multiresolution tech- 

nique for watermarking dig- 


[Birnbaum:1986:VPS] 

Martha Birnbaum, Larry A. 

Cohen, and Frank X. Welsh. 

Voice password system for 

access security. AT&T 

Technical Journal, 65(5): 

68–74, September 1986. 

CODEN ATJOEM. ISSN 

8756-2324.

[Borucki:1974:MNN] 

L. J. Borucki and J. B. Diaz. 

Mathematical notes: a note 

on primes, with arbitrary 

initial or terminal decimal 

ciphers, in Dirichlet arith- 

metic progressions. Ameri- 

can Mathematical Monthly, 

81(9):1001–1002, Novem- 

ber 1974. CODEN AM- 

MYAE. ISSN 0002-9890 (print), 1930-0972 (elec- 

tronic).

[Brickell:1990:CIS] 

Ernest F. Brickell and 

Daniel M. Davenport. On 

the classification of ideal se- 

cret sharing schemes (ex- 

tended abstract). Lecture 

Notes in Computer Science,


REFERENCES


REFERENCES

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

[BDC+95] Brannwyn:1995:IRA


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

[Bao:1998:MFA]


[BDGI98]

[Bao:1997:DAT]


[BDGV96]


[Boneh:1999:FL]


[Boneh:1999:FPL]

REFERENCES


REFERENCES


REFERENCES


REFERENCES

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

Beaver:1993:HBS


Beaver:1996:ASE


Beaver:1997:CBC


Beaver:1997:PPE


Becker:1982:EDE


Beckett:1988:IC


Beckett:1990:IAM

REFERENCES


REFERENCES

Bellare:1999:POP


Bennett:1980:UWN


Bennett:1989:UMS


Benario:1998:TSU


Benedens:1999:GBW


Bertrand:1973:EOP


Berstandis:1980:SPD


Bertrand:1983:EGE


Berkovits:1991:HBS

REFERENCES


REFERENCES


Mathematical Association of America, Washington, DC, USA, 1994. ISBN 0-88385-504-6. xvi + 156 pp. LCCN Z 103 B4813 1994. Cryptology was originally published in German by Vieweg. This edition has been extensively revised.


REFERENCES


Boneh:19xx:


Blaze:1999:KTM


Blaze:1994:CPB


Blum:1988:NIZ


Blaze:1998:PSS


Blaze:1998:FTR


REFERENCES

Blundo:1998:GBC


Busch:1999:DWC


Blum:1985:EPP


Bellare:1990:NPD

REFERENCES


REFERENCES

Bird:1995:KFL


Bruggermann:1995:VIS


Branstad:1977:RWC


Bellare:1997:PRN

REFERENCES


Blundo:1995:DRR


Bierbrauer:1996:OAR


Bierbrauer:1996:ACS


Bosselaers:1993:CWP

REFERENCES


REFERENCES


[BHHR99] Alina Beygelzimer, Lane A. Hemaspaandra, Christo-
pher M. Homan, and Jörg Rothe. One-way functions
in worst-case cryptography: algebraic and security prop-
erties are on the house. ACM SIGACT News, 30
(4):25–40, December 1999. CODEN SIGNDM. ISSN
0163-5700 (print), 1943-5827 (electronic).

[BHJM99] L. Boeleoni, R. Hao, K. Jun, and D. C. Marinescu. Struc-
tural biology metaphors ap-
p lied to the design of a
distributed object system. Lecture Notes in Computer
Science, 1586:275–??, 1999. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

P. Rogaway. UMAC: Fast and secure message authen-
tication. In Wiener
ISBN 3-540-66347-9. LCCN
QA76.9.A25 C79 1999
Bar. URL http://link.
springer-ny.com/link/
service/series/0558/bibs/
1666/16660216.htm; http:
//link.springer-ny.com/
link/service/series/0558/
papers/1666/16660216.
pdf.

stiel. Distributed sym-
bolic computation with
DTS. In Ferreira and Rolim
FR95a, pages 231–248.
ISBN 3-540-60321-2. LCCN

the efficiency and reliabil-
ity of digital time-stamping.
In R. M. Capocelli, A. De
Santis, and U. Vaccaro, edi-
tors, Sequences II: Methods
in Communication, Secu-


ry, and Computer Science,
pages 329–34. Springer-
Verlag, Berlin, Germany /
Bellare:1998:MTF


Bellare:1998:MOT


Brassard:1998:QCH


Bertilsson:1993:CPS


Bao:1994:RAF


Bao:1995:BFA


Breitbach:1999:CCM

Markus Breitbach and Hideki Imai. On channel capacity and modulation of watermarks in digital still
Bar-Ilan:1989:NFC


Biermann:1998:HKB


Biham:1994:NFC


Biermann:1994:MOA


Biham:1995:CMM

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


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


REFERENCES


REFERENCES

Bishop:1992:FPC

Bleichenbache:1997:NOC

Bellare:1997:ROZ

Blakley:1994:LAA

Brooks:1994:ST
Thomas A. Brooks and Michael M. Kaplan. Security technologies. *AT&T
Biham:1995:KPA

Blakley:1995:GPS

Blum:1995:DPC

Bocharova:1995:FEC

Buydos:1997:C

Biham:1998:CAXa

Biham:1998:CAXb
REFERENCES


[BK98i] Lawrence Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry. Improving resistance to differential cryptanalysis and the redesign of LOKI. Lecture Notes in Computer Science,
REFERENCES

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


REFERENCES


[Blah83] Richard E. Blahut. Theory and Practice of Error Control Coding. Addison-Wesley, Reading, MA, USA,

Blakley:1985:ITF


Blanchard:1989:CSS


Blaze:1993:TMS


Blackburn:1994:IRO


Blaze:1994:KME


Blaze:1996:HBE

REFERENCES


Barber:1999:AOD


Buldas:1998:TBL


Beth:1994:CCB


Baaz:1999:SDC


Brassil:1994:EMI


Brassil:1995:HID

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

uum images. In Anony-
mo [Ano95], pages 482–
489. LCCN ?? URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/1040.html.

[Ano95] Anonym
[Brickell:1983:EAA]

[BLO83] E. F. Brickell, J. C. La-
garias, and A. M. Odlyzko.
Evaluation of the Adleman
attack on multiply iterated
knapsack cryptosystems. In
Chaum et al. [CRS83],
pages 39–42. ISBN 1-4757-
0604-9 (print), 1-4757-0602-
2. LCCN QA76.9.A25 C79
1982.

[Brickell:1984:EAA]

[BLO84] E. F. Brickell, J. C. La-
garias, and A. M. Odlyzko.
Evaluation of the Adle-
man attack on multiply it-
erated knapsack cryptosys-
tems (abstract). In
Advances in cryptology (Santa
Barbara, Calif., 1983),
pages 39–42. Plenum, New

[Blo98a]
Gilbert Bloch. Enigma
avant ULTRA: (Enigma be-
fore ULTRA). In Deavours
et al. [DKK+98], pages 395–
401. ISBN 0-89006-862-
US$78.20. URL http://
www.opengroup.com/open/
cbooks/089/0890068623.
shtml. Third volume of se-
lected papers from issues of
Cryptologia.

[Blo98c]
Gilbert Bloch. Enigma
before ULTRA: Polish work
and the French contribu-
tion. In Deavours et al.
[DKK+98], pages 373–
386. ISBN 0-89006-862-
US$78.20. URL http://
www.opengroup.com/open/
cbooks/089/0890068623.
shtml. Third volume of se-
lected papers from issues of
Cryptologia.

[Blo99]
I. Bloch. Fuzzy morphology
and fuzzy distances: New
definitions and links in both
Euclidean and geodesic cases.
Lecture Notes in Computer
CODEN LNCS9. ISSN
0302-9743 (print), 1611-
3349 (electronic).
REFERENCES


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


REFERENCES

sored by the International Association for Cryptologic Research.

Beale:1989:EUR


Bellare:1990:NIO


Bellare:1992:HSG


Bleichenbacher:1994:DAG

REFERENCES


REFERENCES

Bellare:1999:FDS


Bellare:1999:FSD


Blundo:1999:RMS


Bento:1995:RCI


Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD


Blackburn:19xx:NPP

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

Blackburn:1997:CNP


Blackburn:1997:CTA


Biedl:1998:GMF


Blundo:1996:TOB

Carlo Blundo, Luiz A. Frota Mattos, and Douglas R. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. In Advances in cryptology—CRYPTO ’96 (Santa Barbara, CA), volume 1109 of Lecture Notes in Comput. Sci., pages 387–400. Springer-Verlag, Berlin, Ger-


[BNP99] Christoph Busch, Klara Nahrstedt, and Ioannis


REFERENCES


[Brassil:1996:WDI]

[Bull:1999:NMA]

[BO99]

[Ben-Or:1988:MIP]
M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability. In ACM

[Ben-Or:1990:EPP]

[Ben-Or:1983:CSS]
REFERENCES


Ben-Or:1988:CTN


Bolignano:1997:TMC


Bolignano:1998:IPB


Bolignano:1998:IPM


Boneh:1998:DDP


Boneh:1998:DDH

REFERENCES


M. Borcherding. On the number of authenticated rounds in Byzantine agreement. Lecture Notes in Computer Science, 972:230–??, 1995. CODEN LNCSD0. ISSN 0302-9743 (print), 1611-3349 (electronic).
Borcherding:1996:LAD


Bosworth:1982:CCC


Bosma:1990:PPC


Bosselaers:1994:GPA


Bounas:1985:DDS


Boucher:1994:GPA


Bovelander:1998:SCS


Bovenlander:1998:SCS

E. Bovenlander. Smart card security. *Lecture Notes in
REFERENCES

*Bowers:1959:DSP*

*Bowers:1960:BC*

*Bowers:1960:TC*

*Bowling:1993:SEA*

*Bowers:19xx:PC*

*Boyd:1986:CPC*

*Boyd:1988:CCB*

*Boyar:1989:ISPb*

*Boyar:1989:ISPa*
Joan Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of the Association for Computing Machinery,* 36(1):129–141,
References

Boyd:1990:NMK


Boyd:1992:FFA


Boyd:1995:CCC


Boyd:1997:DSP

REFERENCES


[Bosselaers:1995:IPS] Antoon Bosselaers and Bart Preneel, editors. *Integrity primitives for secure information systems: final RIPE report of RACE Integrity Primitives Evaluation (R1040)*, volume 1007 of *Lecture Notes in Com-
REFERENCES

ISSN 0302-9743 (print), 1611-3349 (electronic). 239 pp. LCCN QA76.9.A25
I553 1995.

Baric:1997:CAF

N. Baric and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without
LNCSKD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brinkley:1997:SFS

James F. Brinkley and Jeffrey S. Prothero. Slisp: a
flexible software toolkit for hybrid, embedded and
1997. CODEN SPFXBL.
ISSN 0038-0644 (print), 1097-024X (electronic).

Buchmann:1997:OWF

J. Buchmann and S. Paulus.
A one way function based on ideal arithmetic in number
fields. *Lecture Notes in Computer Science*, 1294:
385–??, 1997. CODEN LNCSKD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

Bailey:1998:OEF

Daniel V. Bailey and Christof Paar. Optimal extension fields for fast arithmetic in public-key algorithms. *Lecture Notes in
LNCSKD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/
lmktglink/service/series/0558/
bibs/1462/14620472.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1462/14620472.

Barnett:1998:AOD

IVPEK. ISSN 1350-245X.

Barnett:1998:FML

ELLEAK. ISSN 0013-5194
(print), 1350-911X (electronic).
<table>
<thead>
<tr>
<th>Author</th>
<th>Year</th>
<th>Title</th>
<th>Citation Details</th>
</tr>
</thead>
</table>
REFERENCES

Bishr:1999:PRS


Blobel:1999:SAD


Brown:1998:LA


Only the slides for the conference talk are available.

Borst:1999:LCR


Blobel:1999:FSA


Beguin:1995:FSR


Blakley:1988:CBA

G. R. Blakley and William Rundell. Cryptosystems based on an analog of

**Beutelspacher:1991:EFS**


**Bellare:1994:EAK**


**Bellare:1995:PSS**

REFERENCES

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

**Baldwin:1996:RRR**


**Bellare:1996:TCA**


**Bellare:1996:ESD**


**Bella:1997:FAK**


**Bellare:1997:MUR**


**Bellare:1999:CVC**


**Bellare:1999:CVI**

M. Bellare and P. Rogaway. On the construction of variable-input-length ciphers. *Lecture Notes in
REFERENCES

Brassard:1981:TLT

Bracha:1987:ERR

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

Brassard:1988:MCT

Brassard:1989:CCb

Brassard:1989:CCa

Brand:1990:PNU
Russell L. Brand. Problems with the normal use of cryptography for providing security on unclassified
REFERENCES


[Bra90]

[Bra93a]
Branstad:1993:RNW

[Bra93b]
Brassard:1993:CM

[Bra94a]
Brassard:1994:CCQ
Gilles Brassard. Cryptology column – quantum com-

Bray:1994:UA

Brackin:1995:DCP

Brassard:1995:CCB

Brassard:1995:IDR

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


Brassard:1998:C


Brent:1999:CAP


Brickell:1986:CKC


Brickell:1988:CKC


Brickell:1990:SIS

REFERENCES

0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340468.htm;

[Bri90b] Ernest F. Brickell. A survey of hardware implementations of RSA (invited),
(abstract). Lecture Notes in Computer Science, 435:368–??, 1990. CODEN LNCSD9. ISSN 0302-9743
link/service/series/0558/bibs/0434/04350368.htm;

International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992: Proceedings,
volume 740 of Lecture Notes in Computer Science. Springer-Verlag,
DM104.00.

[Bri98] E. F. Brickell. Crypto ’92. Lecture Notes in Computer Science, 1440:
540-57340-2 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic).

REFERENCES


Brundrett:1998:KAW

Bentley:1999:SOE

Bryan:1967:CA

Brillhart:1967:SFR

Brickell:1983:SRK

Benois:1986:CSE

Biham:1990:DCD

Brown:1990:DPT
REFERENCES


[Beth:1991:NEC]


[Beth:1991:NSE]


[Biham:1991:DCD]


[Biham:1991:DCFa]


[Biham:1991:DCS]

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

Brickell:1991:SIB


Broscius:1991:EPH


Biham:1993:DCF


Biham:1993:DCD


Brassard:1994:SKR


Blaze:1995:MBC

M. Blaze and B. Schneier.

[Boneh:1995:CSF]


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

[Bose:1995:ATV]


[Bruckstein:1995:SSD]


[Brunnstein:1995:IPR]


[Biham:1997:DFA]

REFERENCES

[Bramhill:1997:CCD]

[Boneh:1998:CSF]

[Baaleh:1999:AGA]

[Bellare:1999:NME]

[Bellare:1999:NME]

[Barreiro:1997:PKC]

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

pages 278–279. ISBN 90-5199-196-7. LCCN ????


[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) $p = 2^k \pm 1$ or $p = 4^k \pm 3$. (b) $M_p(= 2^p - 1)$ is prime. (c) $(2^p + 1)/3$ is prime.

BT:1997:BEC


Barmawi:1998:AEK


Boney:1996:DWA


Buchmann:1991:NTA


Buck:1991:MCT


Budge:1922:RS


Budge:1929:RSB

Sir E. A. Wallis (Ernest Alfred Wallis) Budge. The Rosetta Stone in the British Museum: the Greek, Demotic and Hieroglyphic texts of the decree inscribed on the Rosetta Stone conferring additional honours
REFERENCES


REFERENCES

Burmester:1994:CCW


Burmester:1994:ROD


Burmester:1996:HSS


Burke:1998:IHC


Burke:1998:LER


Burke:1999:AAC

REFERENCES

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


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


REFERENCES


REFERENCES

Beller:1993:BDK


Beller:1993:BDH


CBEMA:1981:ANS


CBEMA:1983:ANSa


Cachin:1995:LSS

C. Cachin. On-line secret sharing. Lecture Notes in Computer Science, 1025:190–??, 1995. CODEN LNCSD9. ISSN 0302-9743
Cachin:1995:OSS


Cachin:1998:ITM


Cypher:1996:UAS


Caelli:1996:CPE


Cain:1996:TS


Calvocoressi:1980:TSU

REFERENCES

Callimahos:1989:TAZ


Callimahos:1992:HC


Campagne:1971:REC


Campbell:1987:MBC


Cammack:1988:MDE


Cao:1999:CAR


Capecchi:1994:TGR


Carlet:1993:PBF


REFERENCES


Chren:1996:RDU


[CB96]

Clark:1981:ECC


[CC81]

Chen:1995:SIB


[CC95]

Canteaut:1998:NAF


[CC98]

Cai:1999:LBPa


[CC99a]

Cai:1999:LBPb


[CC99b]

Chun:1999:DMT

H. W. Chun and S. H. C. Chan. The design of a
REFERENCES


Chaum:1988:MUS


Canteaut:1999:NCA


Chen:1998:VIC


Carter:1995:DVD


Carlet:1998:CBF


Coppersmith:1985:AF


Chuang:1991:MER

REFERENCES

bibs/0537/05370140.htm;


Compton:1999:PTC


Cramer:1999:EMC


Callas:1998:ROM


Chang:1995:SCP


Cowie:1996:WWN


Congedo:1995:SRS


Capocelli:1991:SSS

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

[Carter:1998:KSI]

[Canetti:1997:DE]

[Chen:1995:PDP]

[Cramer:1994:PPK]

[Chaum:1986:CRN]
REFERENCES

[Cer97] Certicom:1997:EC


[CF78] Chaum:1978:ICP

Per Christoffersson and Vi-
REFERENCES


Chouinard:1996:ITA

Callas:1999:FUI

Ceruzzi:1991:RCK
REFERENCES


URL http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390257.htm;


[CG75] Don Coppersmith and Edna Grossman. Generators for certain alternating groups with applications to cryptography. SIAM Journal
REFERENCES


[CG85]

[CG88]

[CG98]

[CG99]
REFERENCES


Cranor:2005:SUD


Canetti:1999:AST


Chen:1996:TAP


Chen:1997:KEM


Chen:1997:AUM

Liqun Chen, Dieter Gollmann, and Chris J. Mitchell. Authentication using mini-


[CH94b] Paul C. Clark and Lance J.

Cai:1996:PEA


Corcoran:1999:SCB


Cordon:1999:AMD

REFERENCES


[Cha85b] D. Chaum. New secret codes can prevent a computerized big brother. In Blakley and

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.

Chaum:1985:SIT


Chaum:1986:SDA


Chang:1986:DKL


Chapman:1986:NFS


Chapman:1990:SFS

REFERENCES


REFERENCES

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

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

Chiopris:1992:SBE
[C. Chiopris. The SE-CReTS banking expert system from phase 1 to phase 2. Lecture Notes in Computer Science, 636:91–??, 1992. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).]

Chin:1999:HCD
[Shiu-Kai Chin. High-confidence design for security: don’t trust — verify. Communications of
REFERENCES


Chin:1999:HDS


Christophides:1999:ODI


Canetti:1997:PSL


Chor:1986:TIP


Chung:1998:DWCb


Christianson:1998:SPI


Christianson:1999:DSCb


Christianson:1999:SPI


Christianson:1999:SPI


Ciarcia:1986:BHD


Cao:1999:DTJ

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

Clark:1995:SRP


Chabaud:1998:DCS


Collins:1999:DCL


Coster:1992:ILD


Coppersmith:1995:TCB


Coppersmith:1996:PMT


Charlwood:1998:EXA

REFERENCES

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


Chari:1999:TSA


Chari:1999:CNR


No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

Chee:1991:CNP


Chor:1990:SSI

REFERENCES

[pdf]

Chor:1993:CPT

Cole:1995:MDR

Chor:1998:PIR

[CKLS96a]

Cox:1996:SRW

[CKLS96b]

Cox:1996:SIY

[CKLS96c]

Cox:1996:SSS
REFERENCES


Three volumes, IEEE order plan catalog number 97CB36144.
REFERENCES

Cox:1998:SGM


Claudy:1912:TMS


Clark:1977:MWBa


Clapp:1997:OFS


Clapp:1998:JHS


Clarke:1998:BP

Clapp:1999:ILP


Cleve:1991:CTI


Clevenger:1996:DEU


Chang:1998:SOM


Clinton:1997:AEC

[Cli97] Bill Clinton. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 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.

Clinton:1999:LPM

[ Cli99] Bill Clinton. A legislative proposal: message from the President of the United States transmitting a legislative proposal to protect the privacy, security and safety of the people of the United States through support for the widespread use of encryption, protection of the security of cryptographic


REFERENCES

Cachin:1995:LIR


Cachin:1997:USA


Chang:1997:CAS


Cooperman:1997:SMD


Cox:1997:RWI


D. Chen:1998:DRT


Camenisch:1999:SEG

REFERENCES


REFERENCES


[S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving rightful ownership with invisible watermarking techniques: Limitations, attacks and implications. IEEE Journal on Selected Areas in Communications,
REFERENCES


[Crilly:1987:BPB]

[Coron:1999:SRBs]

[Coron:1999:SRP]

[Coupe:1999:ELA]

[Chao:1998:CSE]
REFERENCES


[Coh87] Cohen:1987:IIP


[Col64] F. N. Colaço. A criptographia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quases quer que sejao 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.

[Col64] Colaco:1864:CRO


[Com87] Cominsky:1987:CAP


**CSL:1994:DES**


**CSL:1994:EES**


**CSL:1994:SRC**


**CERT:1996:PSA**


**CEC:1997:EST**


**Chiba:1999:AGD**

Conradi:1739:CDS


Conklin:1998:SCO


Conklin:1999:ESC


Contini:1999:DPD


Coombs:1983:MC


Coppersmith:1984:FEL


Coppersmith:1987:C

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


**Coppersmith:1989:AID** [Cop89]


**Coppersmith:1994:DES** [Cop94a]


**Coppersmith:1994:ACS** [Cop94b]


**Coppersmith:1995:AAC** [Cop95b]


**Coppersmith:1995:FSR** [Cop95c]

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


Sponsored by the International Association for Cryptologic Research.

Camion:1991:KHF


Chaum:1993:WDO


Chae:1994:AMA


Chen:1995:NGS


Chaum:1998:E


Chung:1998:DWCa


Charney:1997:PSC


Cheon:1998:TEA

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


**Crawford:1992:ASA**


**Craig:1996:CDC**

Richard Craig. Considerations of data compression and symmetric encryption techniques for a personal communications service. Thesis (M.S.), University of Mississippi, Oxford, MS, USA, 1996. various pp.

**Craver:1997:PSP**


**Crepeau:1990:VDS**


**Crepeau:1997:ECP**

REFERENCES

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


RSA Data Security, Inc., RSA Laboratories West, 2955 Campus Drive, Suite 400, San Mateo, CA 94403-1031, USA; RSA Laboratories East, 20 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.


[CS91] V. Chepyzhov and B. Smeets.

Chabaud:1996:CSS


Chambers:1996:RLM


Cusick:1996:BNFb


Camenisch:1997:EGS


Chambers:1997:RLM


Chen:1997:NIC

Coppersmith:1997:PAP


Canteaut:1998:COM


Cramer:1998:PPK


Coradeschi:1999:ASV


Chau:1989:SCF


Csirmaz:1995:SSM


Coppersmith:1994:ABP

Chang:1997:GSS


Chen:1999:TPS


Collberg:1999:SWM


Currier:1998:MPT


Cusick:1995:CPK

Thomas W. Cusick. Cryptanalysis of a public key


[CvHP91] David Chaum, Eugène van Heijst, and Birgit Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer (extended abstract). Lecture Notes in Computer Science,
REFERENCES

Chang:1991:BCC

Cusick:1991:RIC

Campbell:1993:G
K. W. Campbell and M. J. Wiener. DES is not a group.


Chmora:1994:ECC

Chang:1997:SCO

Ceruzzi:1991:RGC

Coppersmith:1998:CT

Chang:1998:BSC

Craver:1998:TTL

Cao:1990:DKC
REFERENCES

[DeMillo:1983:ACC]
Richard A. DeMillo et al.

[Dittmann:1998:MSW]

[Daemen:1995:HFC]

[Daemen:1998:MSK]

[Daemen:1999:RAI]


REFERENCES

bibs/0576/05760445.htm;

**Damgard:1994:PPS**


**Damgaard:1994:PPS**


**Dam:1996:RPG**


**Damgard:1998:E**


**Damgaard:1999:CSZ**


**Damgaard:1999:LDS**


**Danisch:1995:RES**

H. Danisch. RFC 1824: The Exponential Security
REFERENCES


Danthine:1996:ECM


Dang:1997:AAC


Darnell:1997:CCI


DRC:1985:AAN


Davida:1981:CAR

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

Davies:1985:MAA

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


Davies:1991:ACE


Davis:1994:RAC


Davis:1995:KPR


Davis:1996:CDP


David:1998:WWI

REFERENCES

Davies:1998:E


Davies:1998:NIH


Davies:1998:LCM


Dawson:1985:COL


Dawson:1993:CSG


Dawson:1996:CSR


Denning:1981:SRR

REFERENCES


REFERENCES

QA76.9.A25 C791 1985;
QA26.41 L43 no.218.
URL http://link.springer-
ny.com/link/service/series/0558/tocs/t0218.htm;
http://www.springerlink.com/content/978-0-387-16463-2;
0302-9743&volume=218.

0302-9743&volume=263. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.


DeSchutter:1999:ELC


Desmedt:1995:MNA


Desmedt:1995:MNS


DeSantis:1994:HSF


Davio:1985:EHS


Delaigle:1997:LCW


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

DDJ Staff. News and views: New trends in vaporware; distance ed might pay off; life in the fast lane; making friends in Washington; news on OpenGL 1.2; no discounts for schools; let’s do lunch; encryption export challenge?: Java fissures; searching for talent in science; nanomedicine. Dr. Dobb’s Journal of Software Tools, 23(6): 18, June 1998. CODEN DDJOEB. ISSN 1044-789X.

**DDJStaff:1998:NVc**

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

**DDJStaff:1998:NVd**


**DDJstaff:1999:NVR**


**DePaoli:1998:WBS**


**Denny:1994:FR**

REFERENCES


Davida:1990:KDS


DeSantis:1994:SSP


DeSantis:1994:KCQ


DeSantis:1999:NIZ


Darmstaedter:1998:LCS


| [De 98c] | B. De Schutter. Trends in the fight against computer-related delinquency. Lecture Notes in Computer Science,
DeSmit:1998:GAE


DeMoliner:1999:STB


Drossopoulou:1999:DSJ


Deavours:1987:CPI


Deavours:1988:BPS


Deavours:1998:A


Kruh:1998:TBW

REFERENCES


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


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


**Desmedt:1990:MCS**


**Desmedt:1992:BTC**


**Desmedt:1993:TC**


**Desmedt:1994:TC**


**Desmedt:1994:ACC**


**Desmedt:1995:STC**

References


[Deu97] Dwight Deugo. Coffee talk: From S390 mainframes to

**Deugo:1998:SMS**


**Desmedt:1990:TC**


**Desmedt:1991:SGA**


**Domingo-Ferrer:1991:DUI**


**Domingo-Ferrer:1991:SRT**

REFERENCES

Dawid:1992:BSC

Desmedt:1993:PZS

Domingo-Ferrer:1997:MAS

Domingo-Ferrer:1998:AFE

Domingo-Ferrer:1999:AFB

Deshpande:1999:VEM
V. Deshpande, L. Fornasier, E. A. Gertel, and N. Hilbrink. Virtual engineering of multi-disciplinary applications and the significance of seamless accessibility of geometry data.
REFERENCES


CODEN LNCS9D9. ISSN 0302-9743 (print), 1611-3349 (electronic).
REFERENCES

www.cl.cam.ac.uk/~fapp2/steganography/bibliography/071407.html.


[DGV94a] J. Daemen, R. Govaerts, and J. Vandewalle. A new...


Association for Cryptologic Research.


REFERENCES


REFERENCES


[Dif90] Whitfield Diffie. The adolescence of public-key cryptography (invited). Lecture Notes in Computer Sci-
REFERENCES


REFERENCES


Deavours:1989:CMH

[DK+89]
Cipher A. Deavours, David Kahn, et al., editors. Cryptology: machines, history, 
x + 508 pp. LCCN Z103.C75 1989. Second volume of selected papers from is-

Dusse:1991:CLM

[DK91]
Stephen R. Dusse and 
Burt S. Kaliski Jr. A cryp-
tographic library for the 
Motorola DSP56000. Lecture Notes in Computer Science, 473:230–??, 1991. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://

Desmedt:1998:CES

[DKKK98] 
Y. Desmedt, B. King, 
W. Kishimoto, and K. Kuros-
awa. A comment on the efficiency of secret shar-
ing scheme over any finite Abelian group. Lecture Notes in Computer Science, 1438:391–??, 1998. CO-
DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
Deavours:1987:CYT


Daemen:1997:BCSb


Daemen:1997:BCSa


Dodson:1995:NFL

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

ersmith [Cop95d], page ??
http://www.springerlink.com/openurl.asp?genre= issue&issn=0302-9743& volume=963. Sponsored by the International Association for Cryptologic Research (IACR), in co-
operation with the IEEE Computer Society Technical Committee on Security and Privacy.

Dam:1996:CRS


Diffie:1998:PLP

Whitfield Diffie and Susan Eva Landau. Privacy on the line: the politics


REFERENCES

uk/~fapp2/steganography/
bibliography/1004.html.


[Dwork:1994:EEU] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signa-


**DiCrescenzo:1999:CZK**


**Dobbertin:1995:EMC**


**Dobbertin:1995:ASA**


**Dobbertin:1996:CM**


**Dobbertin:1996:SMA**


**Dobbertin:1997:RTC**


**Dobbertin:1998:FTR**

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

Dobbertin:19xx:CM


DomingoFerrer:1996:NPH


Donini:1998:CSR


DiCrescenzo:1999:COTb


Santis:1991:PRP


DiCrescenzo:1994:ROP

Giovanni Di Crescenzo and Giuseppe Persiano. Round-optimal perfect zero-knowledge proofs. Information Pro-


References

Desmedt:1985:DOI


deRooij:1994:SPD


Desel:1994:PNR


deRooij:1995:EEU

Peter de Rooij. Efficient exponentiation using precom-


Dreher:1979:PSC


Drea:1992:MUC


dRaadt:1999:COO


Dror:1989:SCG


Droste:1996:NRV


Dawson:1995:DIJ


Denning:1981:MKG


Dolev:1983:AAB

REFERENCES

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


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


Duhoux:1990:DBA


Dumey:1994:CQD


DeDecker:1992:HID


Dhem:1996:SSC


DeSoete:1990:CAS

REFERENCES


**Diffie:1992:AAK**


**DiPorto:1994:VBC**


**Danielsson:1998:HKW**


**Davida:1981:DES**


**Dwork:1991:VSS**


**Dwork:1995:DCC**


**Dwork:1997:PAL**

REFERENCES


REFERENCES

DeSantis:1991:CAN

DY91a

DeSantis:1991:DPSb

DY91b

Santis:1991:CAN

DY91c

DeSantis:1991:DPSa

DY91d

Desmedt:1991:WUS

DY91e

Desmedt:1991:AUS

DY91f
Yvo Desmedt and Moti Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter’s attacks (extended abstract). *Lecture Notes in Computer Science*, 537:177–??, 1991. CODEN LNCS D9. ISSN 0302-9743
REFERENCES


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


REFERENCES


*Estrella:1999:DED*


*Eigenthaler:1984:CGA*


*Evans:1974:UAS*


*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

Shimon Even and Yishay Mansour. A construction

Eades:1998:GDC


Ehrsam:1978:CKM


Ezawa:1998:ATS


Endler:1997:PSU


Eng:1995:SDE


REFERENCES

tiff/471.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/472.tif;
http://www3.oup.co.uk/computer_journal/hdb/Volume_32/Issue_05/tiff/473.tif.


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


Wolfgang Effelsberg and Brian C. Smith, editors.


REFERENCES


Evertse:1993:WNR


Evertse:1993:WNR

Evertse:1993:WNR

Falk:1988:DST


Fancher:1996:SCa


Farago:1967:BSS


Farago:1969:BSS


Farrow:1992:HIY


Farrell:1993:CCC


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


[Fan:1999:DFS]


[Frankel:1993:NHG]


[Feak:1983:SIS]


[Feistel:1973:CCP]

REFERENCES


Feit:1993:TIA


Feigenbaum:1998:C


Feige:1999:NSP


Feldman:1987:PSN

Ferris:1987:WBC


Ferguson:1998:UBD


Ferguson:1999:IDT


Fernandes:1999:ECC


Feynman:1982:SPC


Friedman:1957:SCE


Friedman:1955:CLS

REFERENCES

Feghhi:1999:DCA

Fung:1998:PAE

Fuchsberger:1996:PCS

Fuchsberger:1996:PKC

Frankel:1997:ORP

Frankel:1997:PR

Feigenbaum:1992:CPM
[FGGR92] Joan Feigenbaum, Eric
REFERENCES


Farmer:1996:SMA


Frankel:1996:WCP


Frankel:1996:WBC


Friedman:1974:ETR


Franklin:1994:JEM


Franks:1997:REH

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


REFERENCES


[Fis98] M. Fischlin. Cryptographic limitations on parallelizing membership and equivalence queries with applications to random self-


REFERENCES

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


REFERENCES


Fortune:1985:PP


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

Feigenbaum:1991:DCC


Fairfield:1985:LRN


Faihe:1998:ADR


Feustel:1998:DUI

Fagundes:1999:EGA


Frey:1999:TPD


Frankel:1998:RED


Fiat:1994:BE

REFERENCES


Eiichiro Fujisaki and Tatsuaki Okamoto. Secure


REFERENCES


REFERENCES


[Fra99] Matthew Franklin, editor. Financial cryp-

Freund:1994:KED

Freund:1999:KED

Friedman:1935:ICA

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

Friedman:1939:MC

Friedman:1941:MCP
REFERENCES


REFERENCES


REFERENCES


Ferguson:1997:CA

Fischlin:1997:SSP

Forsyth:1993:ACS

Figueroa:1994:FCB

Federrath:1995:SVA

Fiat:1999:DTT
A. Fiat and T. Tassa. Dynamic traitor tracing. In

Frankel:1999:SID


Fuchs:1999:BDM


Fumy:1997:ACE


Fumy:1998:E


Fumy:1998:ISP

REFERENCES


Frankel:1998:RMU


Frankel:1999:CRA

REFERENCES


ican Cryptogram Association (George C. Lamb Collection).


REFERENCES


James M. Galvin. Public key distribution with se-


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


Garfinkel:1996:JSC


Garber:1997:NBAa


Garber:1997:NBB


Garber:1997:NBC


Gardner:1997:PTT

Martin Gardner. Penrose tiles to trapdoor ciphers, and the return of
REFERENCES


Garber:1998:NBM

[Gar98a]


Garber:1998:NBS

[Gar98b]


Garfinkel:1998:PPG


Gaudin:1997:VBJ

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

Gilmour-Bryson:1982:CDT

A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino (CM82), pages 451–467. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.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.”.


Dieter Gollmann and William G. Chambers. A


REFERENCES


[BIBLIOGRAPHY/063129.html


[Goldburg:1991:ACA]

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


REFERENCES


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


REFERENCES

Gingerich:1970:BRB [Gin70]

Girault:1991:SCP [Gir91]

Girard:1999:WSP [Gir99]


Givierge:1932:CC [Giv32]

Givierge:1978:CC [Giv78]

Garey:1979:CIG [GJ79]
Gifford:1982:CSI


Gennaro:1996:RTD


Gennaro:1999:SDK


Garay:1999:AFO

REFERENCES

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


REFERENCES


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

[375]

[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.

[Gla99b]
Lee A. Gladwin. Cautious collaborators: The struggle for Anglo-American
cryptanalytic co-operation, 1940–43. Intelligence and National Security,

[Gle57]
Andrew M. Gleason. Elementary course in probability. National Security
Agency, Office of Research and Development, Mathematical Research Division,
Revised by Walter F. Penney and Ronald E. Wylys.

[And96c]
A. Lu, and W. Bender. Echo hiding. In Anderson [And96c], pages 295–315. CODEN
LNCSD9. ISBN 3-540-61996-8 (softcover). ISSN 0302-9743 (print), 1611-
http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054134.html

[Gle86]
Andrew M. Gleason. Elementary course in probability for the cryptanalyst.
LCCN ?????

[Gle87]
Andrew M. Gleason, editor. Proceedings of the International Congress of Mathematicians,
volumes.

[GLC98]
Dianelos Georges Georgoudis, Damian Leroux, and Billy Simón Chaves. TecApro presents Frog: An
AES candidate algorithms.
REFERENCES

Gonzalez:1999:RMT


Gallant:1999:IPP


Gamage:1999:EMA


Goldwasser:1982:PEH


Goldwasser:1984:PE


Goodman:1985:NTK


Godlewski:1990:KMA

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

**Goldwasser:1985:PSS**


**Goldwasser:1988:DSS**

REFERENCES

Goldwasser:1989:KCI


Good:1945:GRT


Groote:1998:CVP


Goldreich:1987:HPM


Goldreich:1991:PYN

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

Gemmell:1994:CIA

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

Goettfert:1995:GLB

Gray:1995:PCT

Guerrero:1995:CHB

Goldwasser:1993:ISN

Golic:1995:EPC

Goldreich:1996:SPS
REFERENCES


Golic:1996:CCC


Grosky:1996:NAH


Goguen:1999:IAS


Golomb:1967:SRS


Golomb:1982:SRS


Goldwasser:1984:PET


Goldberg:1990:MUA

[Gol90a] David Goldberg. The MITRE user authentication
system. In USENIX Association [USE90], pages 1–4. LCCN QA 76.9 A25 U55 1990.

Goldwasser:1990:ACC

Goldwasser:1990:SPS

Goldreich:1995:FCF

Gollmann:1992:ATC

Gollmann:1994:CCC

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

Golic:1996:CEP


Gollmann:1996:CA


Gollmann:1996:FSE


Goldreich:1997:FMCa


Goldreich:1997:FMCb


Goldwasser:1997:NDC

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

Golic:1997:CAA


Goldwasser:1998:C


Golic:1998:RAS


Goldreich:1999:MCP


Golic:1999:SCE


Golomb:1999:CNS


Gong:1989:SCB


Gong:1992:SRD

Li Gong. A security risk of depending on synchronized

[**Gong:1995:CKH**]


[**Gong:1998:JSM**]


[**Good:1979:EWC**]


[**Goodman:1996:LPS**]


[**Gordon:1985:SPE**]


[**Gordon:1993:DDT**]

Gordon:1993:DLU


Goth:1999:NBG

Greg Goth. News briefs: Groups duel over new I/O standards; Oracle, Sun team up to dump the OS; bringing the net to mobile appliances; Irish girl invents new E-mail encryption; group releases draft biometric-API specs; Toshiba announces smallest memory chip. *Computer*, 32(3):18–20, March 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Guajardo:1997:EAE


Ghodosi:1999:RCN


Ghodosi:1996:CHG


Gladychev:1998:CRJa


Gladychev:1998:CRJb

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


**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.

**Gabidulin:1991:INR**


**Gleason:1985:ECP**


**Guillou:1995:ACE**

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

IEC DIS 9796 “Digital Signature Scheme Giving Message Recovery.”
ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


Grosek:1994:RCR

Grover:1998:FCP

Goldschlag:1996:HRI

Grundler:1984:DEH
Edward James Grundler. A data encryption hardware software package. Project (m.s.), California State University, Sacramento, CA, USA, 1984. vii + 81 pp.

Grusho:1998:SCI

Gaines:1978:SSP

Grollmann:1984:CMP


**Gribomont:1999:SDU**


**Gysin:1999:GCA**


**Gafni:1999:EMI**


**Gobioff:1996:SCH**


**Goldreich:1999:CSZ**


**Gafni:1999:EMI**

REFERENCES

//link.springer-ny.com/  
link/service/series/0558/  
papers/1666/16660372.  
[Gu04]
pdf.

Gramata:1994:MMD

Grehan:1994:BCRa

Gotoh:1990:MRR

Guarini:1904:MTT

Guan:1987:CAP

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

Guarino:1999:RIC
REFERENCES


REFERENCES


REFERENCES


(Swedish) [Cipher bureaus’ operations in the World War on land]. Stockholm, Sweden, 1931.

Gylden:1933:CCB


Gylden:1936:AMC


Gylden:1938:APV

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

Gysin:1996:OKC


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

Garzon:1991:CGG


Haller:1994:RIA


Hendessi:1994:SAA


Hollaar:1996:LRD

REFERENCES

Haddon:1984:BR

Hagelin:1998:SH

Hoffman:1994:CP

Hammer:1971:SS

Hamming:1980:CIT

Hamming:1986:CIT

Hamilton:19xx:PC

Hansen:1994:MLD
[Han94] Per Brinch Hansen. Multiple-length division revisited: a tour of the minefield.
Software—Practice and Experience, 24(6):579–601, June 1994. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). This paper derives an algorithm for division of long integers, and implements it as a literate program, although without identifier cross-references.


Haastad:1988:SSM


Haselberger:1995:DRB


Hasan:1999:LTB


Hatefi:1996:MRE


Hawkes:1998:DWK


Hawkes:1998:DLW

Hutter:1999:DCI


Hughes:1999:PFS


Hu:1995:YCE


Hwang:1995:SSA


Hwang:1996:DSS


Hwang:1998:EMS


Hernandez:1999:DAV


REFERENCES

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


REFERENCES


REFERENCES


Handschuh:1997:CCS

Handschuh:1997:CSE

Handschuh:1997:WME

Hartung:1997:DWM


Hartung:1997:CPV

REFERENCES


Hartung:1998:WUA


Hoornaert:1985:EHI


Haddar:1998:ISI


Hall:1998:RAA


Hinsley:1979:BISb


Hofmann:1994:RQC


Hughes:1998:AJC


Husemann:1999:OTY


Hutton:1999:ASM


Harn:1989:PAU


Han:1993:TCC


Han:1997:TCC

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


REFERENCES

Hiltgen:1994:CRC

Hill:1997:MTY

Hirschfeld:1997:FCF

Hinsley:1993:BIS

Hirschfeld:1997:MER

Haastad:1999:PGO
REFERENCES


REFERENCES


[HK77] Shai Halevi and Hugo Krawczyk. MMH: Software message authentication in the Gbit/second...

Hevia:1998:STD


Halevi:1999:PKC


Halffmann:1999:ESP


Haynes:1999:VDS


Hevia:1999:STD

REFERENCES


REFERENCES


REFERENCES


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


**Harkavy:1998:IPP**


**Hoffman:1998:RIF**


**Horvath:1994:PPM**


**Hennicker:1994:BAF**


**Haastad:1998:SIR**

puter Society Press order number PR9172.


REFERENCES

Hoogendoorn:1982:SPK


Han:1997:ICS


Horan:1994:CSO


Horng:1995:PAU


Horng:1998:AAP


Horster:1999:SSK


Herzberg:1987:PPS

REFERENCES


REFERENCES

Hoffstein:1998:NRB

Holland:1982:GSA

Hwang:1990:PKA

Hollander:1996:KWS

Harrison:1976:POS

Hruby:1995:QDQ
REFERENCES

[Hruby:1995:QQC]

[Hruby:1996:SCI]

[Hruby:1998:TQC]

[Hruby:1999:SUD]

[Hernandez:1999:CLM]

[Hammer:1987:EUH]


REFERENCES


REFERENCES

Hunter:1985:ARK


Hurwicz:1998:CTM


Husain:1994:EI


Husemann:1999:SCD


Hulaas:1998:MLI


Hardy:1975:ITN

[HW75] Godfrey H. Hardy and Edward M. Wright. An Introduction to the Theory of
REFERENCES


REFERENCES

Hwang:1998:AUS

Hwang:1991:CGO

Hwang:1992:AOT

Hwang:1992:EIB

Hwang:1992:EIK

Hwang:1992:PGO

Hwang:1993:SSD

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

Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE


Hall:1998:BPPa


Hall:1998:BPPb


Hohl:1994:SIH


Harn:1993:GUS

L. Harn and S. Yang. Group-oriented undeniable

Harn:1993:PKC


Hwang:1995:TPE


Hirose:1998:ADK


Hirose:1998:ADH


Hsieh:1998:H


Hsieh:1999:OWH

Hardjono:1993:PDM


Ibbotson:1997:CPI


Anonymous:1993:CCA


IBM:19xx:PSP


IEEE:1979:ASF


IEEE:1980:PSS


IEEE:1981:CLC

IEEE:1982:ASF

IEEE:1982:CFP

IEEE:1982:PSS

IEEE:1983:ASF

IEEE:1985:FOC

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

IEEE:1987:ASF

IEEE:1987:IIG

IEEE:1987:PIS

IEEE:1988:FAC

IEEE:1989:ASF
IEEE, editor. 30th an-
REFERENCES


REFERENCES

Computer Society Press order number 2825.

[IEE92d]

[IEE93a]

[IEE93b]

[IEE93c]

[IEE94a]


REFERENCES

Order Plan catalog number 96TB100057.


IEEE:1997:ACS


IEEE:1997:ICD


IEEE:1997:IICb


IEEE:1997:IWS


IEEE:1997:ASF

[IEE97f] IEEE, editor. 38th Annual
REFERENCES


REFERENCES


IEEE:1997:PAC


IEEE:1998:HCC


IEEE:1998:IIC


REFERENCES


REFERENCES

Izu:1998:PSE

Israel:1983:AOS

Impagliazzo:1989:OWF

Ilie:1994:CAS

Imai:1986:AMC

Iwamura:1993:HIM

Iwamura:1993:HSI
Ímpagliazzo:1992:PGP


Ímpagliazzo:1989:ECS


Íto:1999:DPS


Íngemarsson:1998:E


Ínstenes:1995:MAA

REFERENCES

IRD:1984:DTV

IRD:1987:DTV

IRD:1988:DTV

Anonymous:1991:IIS

IRD:1991:DFV

Itoh:1994:LDS

Impagliazzo:1989:LPC


N. Ikram and S. J. Shepherd. User identification


Ingemar Ingemarsson and C. K. Wong. Use authentication scheme for shared data based on a trap-door one-way function. *Information Processing Letters,*
REFERENCES

IZ98

IZ99

IZ98

IZ99

IZ99
Keith M. Jackson. Secure information transfer:
REFERENCES


Jackson:1996:AAC

Jakobsson:1995:BUU

Jakobsen:1999:HOC

Jakobsson:1999:MCM

Jakobsson:1999:QCA

Jamieson:1998:UEP
Lauren Jamieson. Unveiling the extraordinary possibili-

Jantke:1995:RSI


Janecek:1999:AVR


Jarecki:1996:PSS


Jarvis:1997:GB


Jaspan:1996:DWE


Jaeger:1993:LCC


Jan:1998:PWP

REFERENCES

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


Joyce:1990:IAB


[JG95] A. Joux and L. Granboulan. A practical attack against knapsack based hash functions. Lecture Notes in Computer Science, 950:
REFERENCES


REFERENCES


[Jackson:1995:ESS]


[Jackson:1995:SMS]


[Jerichow:1998:RTM]


[Jakobsson:1996:DVP]


[Jarecki:1997:EMS]

REFERENCES

[Joe98]

[Johnson:1989:BDC]

[Johnson:1990:EDE]

[Johnson:1995:ACD]
REFERENCES


REFERENCES


REFERENCES

Joye:1998:REC


Joye:1997:RTS


Jurgensen:1996:TFC


Jones:1993:DAC


Joux:1993:CAK


Johansson:1995:AIA


Johansson:1995:CIA

REFERENCES


Jungnickel:1996:DFG


Jung:1999:EMA


Jutla:1998:GBA


Just:1996:AMP


Jakubowski:1998:CSP


Jeannerod:1998:GEE


Ji:2001:CAF

REFERENCES

[Jakobsson:1996:OAB]
M. Jakobsson and M. Yung. On oblivious, agnostic, and blindfolded provers. In
Koblitz [Kob96], pages 186–200. CODEN LNCS09. ISBN 3-540-61512-1. ISSN
URL http://link.springer.com/link/service/series/0558/tocs/t1109.htm;
by the International Association for Cryptologic Research (IACR), in co-
operation 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).

[Joye:1998:IBS]
Marc Joye and Sung-Ming Yen. ID-based secret-key cryptography. Operating
1943-586X (electronic).

[Kompella:1991:FCC]
K. Kompella and L. Adleman. Fast checkers for cryptography. Lecture Notes
in Computer Science, 537:515–??, 1991. CODEN LNCS09. ISSN 0302-9743
(print), 1611-3349 (electronic).

[Kent:1998:RIA]
www.math.utah.edu/pub/rfc/rfc1826.txt; http://
www.math.utah.edu/pub/rfc/rfc2402.txt. Obso-
letes RFC1826 [Atk95a]. Status: PROPOSED STAN-
DARD.

[Kent:1998:RIE]
S. Kent and R. Atkinson. RFC 2406: IP Encapsulat-
ing Security Payload (ESP), November 1998. URL ftp://
internic.net/rfc/rfc2406.txt; http://
www.math.utah.edu/pub/rfc/rfc1827.txt; http://
www.math.utah.edu/pub/rfc/rfc2406.txt. Obso-
letes RFC1827 [Atk95b]. Status: PROPOSED STAN-
DARD.

[Koutsoukos:1999:HCS]
X. D. Koutsoukos and P. J. Antsaklis. Hybrid control
systems using timed Petri
nets: Supervisory control


REFERENCES

[102x681] uk/~fapp2/steganography |
bibliography/1009.html.

Kahn:1991:SER


Kahn:1991:WWW


Kahn:1996:HS


Kahn:1996:CSS


Kahn:1998:EC


Kahn:1998:PHI


Kahn:1998:RMU

REFERENCES

Kak:1983:EMP


Koc:1996:ACM


Kaliski:1991:MMD


Kaliski:1985:WAE


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.

Kaliski:1991:MMD

[Kal91] Burt S. Kaliski Jr. The MD4 message digest al-
Kaliski:1995:MIA

Kaliski:1997:IPS

Kaliski:1997:PNG

Kaliski:1997:ACC
Burton S. Kaliski, editor. *Advances in cryptography, CRYPTO ’97: 17th annual international cryptography conference, Santa Barbara, California, USA, August 17–21, 1997: proce


Kaliski:1998:RPCa


Kaliski:1998:RPCb


Kaliski:1998:RPCc


Kaliski:1998:EDF


Kaliski:1998:RPRa


Kaliski:1998:RPCa

REFERENCES

Kaliski:1998:REC


Kaliski:1999:ESP


Kaps:1998:HSF


Karger:1985:ADA


Karger:1987:LDP


Kari:1989:CBP


Kaneshige:1996:ITC

Kari:1989:OCP


Karkare:1996:SEA


Kasiski:1863:GDG

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

Kastenholz:1996:RVP


Katzan:1977:SDE


Katsikas:1997:CMS

REFERENCES

Kaufman:1993:RDD

Kaufman:1996:DWC

Kawai:1987:LAI

Kay:1995:CTE

Krishnakumar:1992:HTE

Krawczyk:1996:HKM

Krawczyk:1997:RHK

Klein:1989:STR
Shmuel T. Klein, Abraham Bookstein, and Scott Deerwester. Storing text retrieval systems on CD-ROM. compression and

**Karp:1988:SDN**


**Kunkelmann:1997:EDV**


**Kao:1995:ESA**


**Krajewski:1994:ASC**


**Krajewski:COMPSYS-7-1-75**

**Kam:1978:SDS**


**Kam:1979:SDS**

0018-9340 (print), 1557-9956 (electronic).

**Khinchin:1997:CF**


**Keating:1999:PAA**


**Kelsey:1999:KSWb**


**Kemppainen:1999:DMM**


**Kent:1993:IPE**

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


[KG93] Andrew Klapper and Mark Goresky. Cryptanalysis based on 2-adic rational ap-


Karaorman:1999:CRJ


Kobara:1996:LVS


Kobara:1997:SSM


Kilian:1988:FCO


Kim:1993:CLB

 REFERENCES  

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

**Kippenhahn:1997:VIB**
Rudolf Kippenhahn. *Ver- 
enschlüsselte Botschaften: Geheim-

[Kip97]  
schrift, Enigma und Chip-
karte. (German) [Encrypted 
messages: cryptography, 
Enigma and smart card]. 
Rowohlt, Reinbek bei Ham-
burg, Germany, 1997. ISBN 
LCCN ????. DM 45.00.

**Kippenhahn:1999:CBH**
Rudolf Kippenhahn. *Code 
breaking: a history and ex-
ploration*. Overlook Press, 
Woodstock, NY, USA, 
1999. ISBN 0-87951-919-
3. 283 pp. LCCN Z103 
.K5613 1999. Translated 
from the German original, 
Verschlüsselte Botschaften, 
in collaboration with the 
author, by Ewald Osers.

**Kippenhahn:1999:VIB**
Rudolf Kippenhahn. *Ver- 
enschlüsselte Botschaften: Geheim-
schrift, Enigma und Chip-
karte*, volume 60807 of 
rororo rororo-Sachbuch sci-
ence. Rowohlt-Taschenbuch-
Verl., Reinbek bei Ham-
ISBN 3-499-60807-3. 361 
pp. LCCN ????

**Kirby:1995:RPK**
Jeff Kirby. The RSA public 
key encryption algorithm 
and what a business needs 
to know about it. Thesis 
(B.S.), California Polytechnic 
State University, San 
Luis Obispo, CA, USA, 

**Kak:1977:SEU**
S. C. Kak and N. S. Jayant. 
On speech encryption using 
waveform scrambling. *The 
Bell System Technical Jour-
nal*, 56(5):781–808, May– 
June 1977. CODEN BST-
JAN. ISSN 0005-8580. URL 
http://bstj.bell-labs.
.com/BSTJ/images/Vol56/
bstj56-5-781.pdf.

**Kocher:1999:DPA**
P. Kocher, J. Jaffe, and 
B. Jun. Differential power 
analysis. In Wiener [Wie99], 
pages 388–397. ISBN 
3-540-66347-9. LCCN 

**Kurosawa:1995:NBA**
K. Kurosawa and S. Kageyama. 
New bound for affine re-
solvable designs and its 
application to authentication 
codes. *Lecture Notes in 
Computer Science*, 959: 
292–??, 1995. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

**Kuwakado:1996:NRT**
Hidenori Kuwakado and 
Kenji Koyama. A new RSA-
type cryptosystem based

**Kelm:1997:NK**


**Kunihiro:1998:ECN**

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**

Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata,

**Kabatianskii:1997:DSS**


**Krammer:1999:FCD**


**Kothari:1984:CMW**


**Kilian:1994:FKE**


**Kilian:1995:FCR**


**Knudsen:1995:NAA**

L. R. Knudsen and X. Lai. New attacks on all double block length hash functions of hash rate 1, including the
REFERENCES


[KM93] Kwangjo Kim and Tsu-


[KM93] Kwangjo Kim and Tsu-


[KM93] Kwangjo Kim and Tsu-


[KM93] Kwangjo Kim and Tsu-


[KM93] Kwangjo Kim and Tsu-
REFERENCES


Knudsen:1996:IDA


[Knudsen:1996:IDA]

Kosuda:1997:SED


Kaksonen:1998:OMC


Kaufman:1998:DWF


Kasahara:1999:NPK

REFERENCES

Knudsen:1999:CIS


Kohlas:1999:RAP


Koscielny:1999:QBP


Kanda:1998:ECC


Kobayashi:1999:FEC


Konheim:1980:ICP


Koyama:1991:NPK


**Kande:1999:AUD**


**Karn:1995:REC**


**Kno79**


**Kohl:1994:EKA**

REFERENCES


REFERENCES

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

Knudsen:1993:CLc


Knudsen:1993:CLA


Knudsen:1994:PSF


Knudsen:1994:BCA


Knudsen:1995:NPW


Knudsen:1998:BCS


Knudsen:1998:DBC


Knudsen:1999:STA

L. Knudsen. Some thoughts on the AES process. Com-
ment submitted to NIST., April 1999.

Knudsen:1999:CBC


Knudsen:1999:FSE


Kurosawa:1995:CIS


Kurosawa:1995:CBA


Kurosawa:1996:CLB


Kurosawa:1997:CLB


Koblitz:1987:CNT

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


REFERENCES


Kobayashi:1997:DWH


Koblitz:1998:AAC


Koblitz:1998:ECI


Kobara:1999:PMA

Kazukuni Kobara. Pseudorandomness and maximum average of differential probability of block ciphers with SPN-structures like E2. In National Institute of
Standards and Technology
[Nat99b], page ?? ISBN
???? LCCN ???. URL
http://csrc.nist.gov/
encryption/aes/round1/
conf2/aes2conf.htm;
http://csrc.nist.gov/
encryption/aes/round1/
conf2/agenda-final.pdf;
http://www.nist.gov/
aes. No slides for the con-
ference talk are available.

Kochanski:1989:HSI

safe is it? (computer se-
curity). BYTE Magazine,
CODEN BYTEDJ. ISSN
0360-5280.

Koc:1994:HSR

[Koç94] Çetin Kaya Koç. High-
speed RSA implementa-
tion. Technical report
TR 201, RSA Data Se-
curity, Inc., Redwood
City, CA, USA, November
1994. 73 pp. URL ftp:
//ftp.rsasecurity.com/
pub/pdfs/tr201.pdf. Ver-
sion 2.0.

Koc:1996:RHI

[Koç96a] Çetin Kaya Koç. RSA
hardware implementation.
Technical report TR-801,
RSA Data Security, Inc.,
Redwood City, CA, USA,
April 19, 1996. ii +
rsasecurity.com/pub/ps/
rsasecurity.com/pub/ps/
tr801.ps. Version 1.0.

Kocher:1996:TAI

[Koc95] P. Kocher. Cryptanaly-
sis of Diffie-Hellman, RSA,
DSS, and other cryptosys-
tems using timing attacks.
In Coppersmith [Cop95d],
pages 171–183. CODEN
LNCS09. ISBN 3-540-
60221-6 (Berlin). ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer-
ny.com/link/service/series/0558/0558toc.html;
http://www.springerlink.
com/openurl.asp?genre=
issue&issn=0302-9743&
volume=963. Sponsored
by the International As-
sociation for Cryptologic
Research (IACR), in co-
operation with the IEEE
Computer Society Techni-
cal Committee on Security
and Privacy.
Kocher:1999:B

Koeune:1999:CRI

Kohl:1990:UEK

Kolata:1977:NCC

Koland:1995:SSH

Konheim:1981:CP

Konheim:1985:CAE
REFERENCES


Koops:1997:CRE


Kopooshian:1997:DCE


Korn:1996:PC


Kościelny:1983:PRD

technique and cryptogra-
phy. Summary in English and Russian; legends and table of contents also in En-

**Kurosawa:1994:NSS**


[126x548]+[132x548]

Kaoru Kurosawa, Koji
Okada, Keiichi Sakano,
Wakaha Ogata, and Shi-
geo Tsujii. Nonperfect se-
cret sharing schemes and
matroids. Lecture Notes
in Computer Science, 765:
126–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
bibs/0765/07650126.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0765/07650126.
pdf.

**Koshiba:1997:CLT**


T. Koshiba. Computational
learning theoretic crypt-
analysis of language theo-
retic cryptosystems. Lecture
Notes in Computer Science,
1334:28–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Koshiba:1999:UPN**


Takeshi Koshiba. Un-
predictability of pseudo-
random number genera-
tors on public key cryp-
tosystems with random in-
puts. Sūrikaisekikenkyūsho
Kōkyūroku, 1093:162–167,
1999. Models of com-
putation and algorithms
(Japanese) (Kyoto, 1999).

**Kothari:1985:GLT**

[102x681]Kothari:1985:GLT

S. C. Kothari. Generalized
linear threshold scheme.
In Blakley and Chaum [BC85],
pages 231–241. CODEN
3-540-39568-7. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&page=231. CRYPTO
84: a Workshop on the
Theory and Application of
Cryptographic Techniques,
held at the University of
California, Santa Barbara,
August 19-22, 1984, spon-
sored by the International
Association for Cryptologic
Research.

**Kurosawa:1995:LEAa**


Kaoru Kurosawa, Koji
Okada, and Shigeo Tsu-
jii. Low exponent attack
against elliptic curve RSA.
Information Processing Let-
ters, 53(2):77–83, January
27, 1995. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).


REFERENCES


REFERENCES


Kaliski:1995:MAM [KR95b]

Kaliski:1995:SUR [KR95c]


REFERENCES


Kravitz:1993:DSA


Krawczyk:1994:SSM


Krawczyk:1994:LBH


Krawczyk:1995:NHF


Krawczyk:1998:ACC

REFERENCES


Krawczyk:1999:BCC

Kesdogan:1998:DTP

Knudsen:1998:DSR

Kumar:1999:CCB

Kruh:1998:WWS

Knudsen:1999:TDS
L. R. Knudsen, M. J. B. Robshaw, and D. Wagner. Truncated differentials and Skipjack. In

Kordes:1989:UMC


Kelsey:1997:CPO


Kurosawa:1997:DSP


Kwon:1997:SEA


Kaliski:1998:RPRb

soletes RFC2313 [Kal98b]. Status: INFORMATIONAL.


REFERENCES


[KSF99] J. Kelsey, B. Schneier, and N. Ferguson. Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In Sixth Annual Workshop on Selected Ar-


[Kim96] Yong-Tae Kim, Kwang-Suk Suh, and Chang-Han Kim. On the efficient im-

...

[Kehne:1992:NBP]


[Knowles:1992:AFC]


[Kelsey:1996:KCI]


[KSW97a]


[KSW97b]


[KSW98a]

REFERENCES


Kelsey:1998:PICb


Kelsey:1999:MCAa


Kelsey:1999:SCCa


Kelsey:1998:KSWa


Kelsey:1999:MCAb


Kelsey:1998:KSWb


Kelsey:1999:KSWb


Kelsey:1998:KSWc


Koyama:1998:AFC


Kanda:1999:SCF


Kuchlin:1987:PKE

W. Küchlin. Public key encryption. SIGSAM Bul-

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

Kuo:1990:TEC
Kurosawa:1994:NBA


Kearns:1989:CLL


Kearns:1994:CLL


Kaul:1999:IBP


Kirstein:1992:PAS


Konrad:1999:SDK

[KW99] K. Konrad and D. A. Wolfram. System description: Kimba, a model generator for many-valued first-order logics. Lecture Notes in Computer Science, 1632:
REFERENCES

282–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


Kaliski:19xx:DLC

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

Kwok-Yan:1992:TAD


Kurosawa:1998:SBC


Kwok-Yan:1992:FAA


Kasami:1982:KMS


Koch:1995:TRH


Levien:1998:ART


Lampson:1991:ADS

Butler Lampson, Martín Abadi, Michael Burrows,

**Lampson:1992:ADS**


**Lacy:1993:CCS**


**Laffin:1964:CCS**


**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.”.


REFERENCES

of Cryptology, by J. S. Gal-
land. American Mathematical
Monthly, 53(6):330–331,
June/July 1946. CODEN
AMMYAE. ISSN 0002-9890
(print), 1930-0972 (elec-
tronic).

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

[Lan95] Susan K. Langford. Differential-
linear cryptanalysis and
threshold signatures. Thesis
(Ph.D.), Department
of Electrical Engineering,
Stanford University, Stan-
ford, CA, USA, 1995. xi +
98 pp.

[Lan96] Susan K. Langford. Weak-
nesses in some threshold
cryptosystems. Lecture
Notes in Computer Science,
1109:74–82, 1996. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Lan97] N. Lange. Single-chip im-
plementation of a cryp-
tosystem for financial ap-
lications. Lecture Notes in
Computer Science, 1318:
135–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Lan98] P. Landrock. TTPs overview — concepts and
review of the state of the art from a technical point
of view. Lecture Notes in
Computer Science, 1528:
241–263, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Lan99] Peter Landrock. Primality
tests and use of primes in
public key systems. Lecture
Notes in Computer Science,
1561:127–133, 1999. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/1561/15610127.htm;
http://link.springer-
ny.com/link/service/series/0558/papers/1561/15610127.pdf.

Lassek:1985:CCA

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

Lassak:1992:SRP


Lauer:1981:CSC


Lawton:1998:NBS


Lee:1988:OSM


Lee:1989:WBL


Lee:1989:WLB


Leake:1999:IIR

D. B. Leake, L. Birnbaum, K. Hammond, and C. Marlow. Integrating information resources: a case study
of engineering design support. Lecture Notes in Computer Science, 1650:482–??, 1999. CODEN LNCS90. ISSN 0302-9743 (print), 1611-3349 (electronic).

Landwehr:1994:TCP


Low:1994:SAP


Lomas:1995:RBH


Lee:1996:IAP


Lin:1996:BCC


Lin:1996:CBC


Lee:1997:AES

REFERENCES


REFERENCES


//ftp.internic.net/rfc/rfc1929.txt; http://


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


REFERENCES

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


REFERENCES


REFERENCES

stoc/22145/p363-levin/. ACM order no. 508850.

Levine:1991:USC


Levin:1978:UGW


Levin:1982:AMC


Lewis:1992:SCP


Laurin:1997:SSM


Lopes:1999:UES


Lorigo:1999:CDG


Li:1994:RMC


REFERENCES


**Li:1995:TSW**


**Li:1995:TMS**


**LWL98**

Li:1998:ZNP


**Lee:1999:STI**


**Lichtenthal:1994:CBT**


**Lidl:1985:CBP**

Lidl:1990:SMA


Lieberherr:1981:UCD


Liebl:1993:ADS


Lim:1998:CNB


Lim:1999:RVC


RFC0989

[Lin88b, Lin89b]. Status: UNKNOWN.

**[Lin1988:RPE]**


**[RFC1040]**


**[RFC1113]**

REFERENCES


[Linn:1993:RPE]


[Linn:1996:IRC]


[Linn:1996:RKV]

REFERENCES

Linnartz:1998:TCC


Lippit:1993:PIC


Lipton:1994:CNF


Abeles:1998:KVC


Lipmaa:1999:ICM


Litant:1987:BRC


Lindsay:1997:BC

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

[Laih:1996:CEE]

[Lee:1999:MRF]

[Landau:1994:CPP]

[Linnartz:1998:MFA]

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


Chi Sung Laih, Jau Yien Lee, and Lein Harn. A new threshold scheme and its
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

**Lam:1996:EGE**

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

**Lenstra:1990:NFS**


**Lenstra:1993:FNF**

CODEN MCMPAF. ISSN 0025-5718 (paper), 1088-6842 (electronic). See [LLMP90].

**Langie:1922:C**


**Luccio:1980:CMC**

CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See notes [Mei81, Hel81].

**Lidl:1984:PPR**


**Leighton:1985:HBC**

REFERENCES

QA267.A1 L43 no.196.
article&issn=????&volume=0
issue=0&page=101.CRYPTO
84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


Longo:1990:GCC


Leonard:1997:CSP


Lautemann:1999:DCA

REFERENCES

LaMacchia:1983:CDL

LaMacchia:1991:CDL

LaMacchia:1991:SLS

Lomet:1983:HPU

Lomas:1994:ENT

Lomas:1997:SPI

Long:1991:PAA
Yong Hong Long. A probabilistic attack algorithm for

**Long:1992:UDE**


**Loshin:1997:CGP**

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

**Loshin:1998:PEC**


**Lowe:1995:ANS**


**Lowe:1996:BFN**


**Loxton:1990:NTC**

REFERENCES

**Lam:1999:ACA**


**Li:1999:CKA**


**Luciano:1987:CCC**


**Leszczynski:1994:SDA**


from the library of the 4th Sga-rga Khams-sprul Rin-poche.


REFERENCES

Lai:1993:FCC


Lange:1925:TC


Lange:1981:TC


Lin:1997:LNU


Lloyd:1992:RPA


Lasker:1998:ACC


Lu:1989:SCI

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.


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

REFERENCES


Shyue Ching Lu. Addition to: “The existence of


Lucks:1998:OKE


Lucks:1998:ATE


Lucks:1999:SBB


Lucks:1999:SBC


Lucks:1999:ARK


Ludwig:1997:CQA


Lujan:1998:AMDa

REFERENCES

Lujan:1998:AMDb


Lunt:1990:EK


Lutz:1998:NBM


Linnartz:1998:ASA


Lungelaar:1996:CPM


Lungelaar:1997:RLM


Long:1988:DLH

Douglas L. Long and Avi Wigderson. The discrete

**Li:1991:JAE**


**Lervik:1996:IDS**


**Lucks:1999:RKE**


**Lin:1996:GTU**


**Lenstra:1995:KES**


**Laih:1993:SAS**

C.-S. Laih and S.-M. Yen. Secure addition sequence
Lodge:1994:SCC


Laih:1993:TES


Li:1991:BCP


Li:1991:HBM


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN

REFERENCES


REFERENCES

proceedings/security95/mcdonald.html.

**Mandelbrot:1960:BRJ**


**Manasse:1995:MPE**


**Manjunath:1998:IPA**


**Moriai:1996:KLP**


**Mao:1997:PVP**


**Mao:1998:GCS**


**Marsh:1970:CSS**


**Marsh:1970:MEC**

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

Marion:1976:ANB

Marion:1995:WGT

Marks:1995:PEI

Markoff:1996:MIS

Martin:1997:IEI

Markantonakis:1998:CSM

Marks:1998:BSC
REFERENCES

Martyna:1999:NNA


Massey:1983:LFC


Mastrovito:1989:VDM


Mastrovito:1991:VAC


Massey:1994:SKB


Massacci:1997:BSP


Massacci:1999:DRT


Massey:1999:OSD

Matyas:1979:DSO


Matyas:1991:KHC


Matsui:1993:LCM


Matsui:1994:FEC


Matsui:1994:LCM


Matsui:1995:CBO

Matsui:1996:NSB


Matthews:1996:SRN


Matsui:1997:NBE


Matsumura:1999:DTE


Mauborgne:1914:APC


Maurer:1990:FGS


Maurer:1991:NAD

Maurer:1991:DSS


Maurer:1991:PCS


Maurer:1991:PSS


Maurer:1993:PSK


Maurer:1993:RIT


Maurer:1994:TEB

Maurer:1996:UGT

Maurer:1996:ACE

Maurer:1997:ITS

Mauriello:1997:TTC
REFERENCES

Mauth:1997:SOC


Maurer:1998:E


Maurer:1999:IC


Maurer:1999:ITC


Maxemchuk:1994:EDD


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

James L. Massey and Richard E. Blahut. *Communications and cryptography: two sides of one tapestry.*

Mehrotra:1999:NOA


Mitra:1999:DCT


Mintzer:1998:OWS


Mintzer:1997:ROD


Moskowitz:1992:CAA


Mitchell:1996:CKU


McCarty:1975:AFP


McCurley:1990:DLP

McCurley:1996:CIL


McCane:1998:ICS


Millan:1998:HDC


Millan:1999:BFD


McHugh:1992:EBD


McIvor:1985:SC


McKee:1999:SFF

REFERENCES


REFERENCES

Meierhofer:1996:PGP


Meijer:1996:GFC


Meinel:1998:HHB


Menezes:1993:ECP

Communications and Information Theory.

Menezes:1995:ECC

Menicocci:1995:SAC

Mersenne:1644:CPM
Marin Mersenne. *Cogitata Physica-Mathematica ... (Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theoretica, practica. Et Mechanica phaenomena. Ballistica et acontrismologia)*. Antonii Bertier, Paris, France, April 1, 1644. 30, 40 24, 41–370, 16], 96, 8, 138, 34 + 40 [Mer78]. 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. Pervoucheine showed in 1883 that \( M(61) \) is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that \( M(89) \) and \( M(107) \) are prime, both missed by Mersenne. By 1947, it was known that the correct list is 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is \( M(13466917) \), a number containing 4,053,946 digits.

Merkle:1978:SCI
Ralph C. Merkle. Secure communications over insecure channels. *Communications of the Association for Computing Machinery*, 21(4):294–299, April 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-
REFERENCES

Merkle:1980:PPK

Merkle:1982:PPK

Merkle:1982:SAP

Merkle:1988:DSB

Merkle:1989:CDS

Merkle:1990:OWH

Merkle:1990:CDS
REFERENCES


Merkle:1991:FSE


Mercuri:1993:IRC


Merrill:1997:ARD


Meyer:1996:RPE


McGraw:1997:UKJ


Murino:1995:RNU

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


Michels:1996:RDS


McPherson:1998:CRH


Majzik:1996:MCU


Matsumoto:1988:PQP


Matsumoto:1990:EAC


Moulin:1999:ECG


Michener:1988:TSK

[MI88] John R. Michener. A tool for secret key cryptography. Dr. Dobb’s Journal of Soft-


Preda Mihai


REFERENCES

LCCN ????

Millikin:1943:ECCb


Millikin:1943:ECCc


Miller:1976:RHT


Miller:1985:PES


Miller:1986:UEC


Milen:1987:CCC


Mills:1987:RDP

REFERENCES


Millikin:1992:ECC

Miller:1995:HWK

Millan:1996:LOA

Miller:1996:CME

Matsumoto:1993:VIA

Mintzer:1997:EIDA

Misarsky:1997:MAU
REFERENCES


Mitchell:1976:EAD


Mitchell:1989:MDS


Mitchell:1992:AMI


Mitchell:1992:CCI

Miyaguchi:1990:FCC


Miyaguchi:1991:FCF


Miyaji:1993:ECS


Miyaji:1993:OEC


Miyano:1993:MEN


Miyaji:1996:MRS


Miyaji:1999:ECC


Mjolsnes:1993:PCP


Morii:1992:PSP

REFERENCES


Moskowitz:1994:CCH


Mazieres:1999:SKM


Maibaum:1999:SRS


Miyazaki:1999:TFI


Monge:1967:NMC


Maulucci:1987:HAC

Mao:1998:CPO

Matyas:1991:KSB

Muffett:1995:BPK

Matyas:1978:GDI

Meyer:1982:CND

Moler:1983:SVA

Meadows:1987:MSA
REFERENCES


REFERENCES

cl.cam.ac.uk/~fapp2/steganography/bibliography/054230.html


Mock:1997:BDS


Moltashemi:1992:CHC


Matsumoto:1982:DTL


Mok:1997:KNF


Moldovyan:1998:NEP


Morita:1991:SCT


Montgomery:1985:MMT

REFERENCES


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


Mullin:1988:ONB


Moynihan:1998:SAE


Mevis:1986:SCP


McInnes:1991:IPK


Milidiu:1999:EIW


Mayerwieser:1995:THS


Moller:1994:RSW

REFERENCES

uk/~fapp2/steganography/
bibliography/042160.html

Morillo:1999:WTS


Malek:1995:DCB


Mrakovcic:1995:EIN


Myers:1995:RCM


McLeod:1998:TMP

REFERENCES


REFERENCES

Montgomery:1990:FEP

Meier:1991:CPC

Massey:1994:FTA

Meier:1995:SG

Meier:1995:SSG

Metzger:1995:RIAa


Metzger:1995:RIAb


RFC1852


Micali:1995:SMG


Mambo:1998:NCB


Michels:1998:GCS

M. Michels and M. Stadler. Generic constructions for secure and efficient conRatifier signature schemes. Lecture Notes in Computer
REFERENCES

MacKenzie:1999:AIH


Maitra:1999:HNR


Miyazaki:1999:KGD


McLeod:1990:VLD


Miksch:1999:ASQ

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

Moriai:1998:HOD


McClure:1999:HEN

REFERENCES

Moriai:1999:IAB


Martin:1997:MAS


Mizuki:1998:ESK


Mizuki:1999:DNS


Martin:1999:BTE


Mambo:1996:HUT


Madonia:1993:GSP

[MSS93] M. Madonia, S. Salemi, and T. Sportelli. A gen-

#### Michels:1998:SSV


#### Mullender:1986:DCD


#### Matsui:1994:VSH


#### Massey:1995:MCM

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


REFERENCES


Moriya:1997:DWS


Molva:1992:KAK


Mu:1992:ICS


Mueller:1999:SRB


Muftic:1988:SMC


Muftic:1993:SAO


Mulherin:1981:FDE


Mulligan:1989:UMA

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


REFERENCES


[Mv93] Joost Meijers and Johan van Tilburg. Extended majority voting and private-
key algebraic-code encryptions. Lecture Notes in Computer Science, 739: 288–??, 1993. CODEN LNCS:DS. ISSN 0302-9743 (print), 1611-3349 (electronic).

Menezes:1998:C


Mu:1999:DD


Menezes:1997:HAC


Menezes:1993:CPE


Muller:1998:DLB


Manber:1994:AAM


Maurer:1996:TCW

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

Maurer:1996:DO

Maurer:1996:DHO

Maurer:1997:PAS

MacNish:1998:BRD

Memon:1998:PDM

Merkle:1998:SSR
Merkle:1998:SSA


Maurer:1999:RBB


Malkin:1999:ESG


Mitchell:1994:CPA


Maurer:1991:NIP


Matsui:1993:NMK

M. Matsui and A. Yamagishi. A new method

**Maurer:1993:RNI**


**Mayers:1998:QCI**


F. Nat-Abdesselam and N. Agoulmine. QoS con-

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


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


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


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


**Nanovic:1936:SWI** [Nan36]


**Nanovic:1974:SWI** [Nan74]


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

REFERENCES


NBS:1977:DES


NBS:1980:MO


NCSOTS:1984:ISR


NIST:1985:FPSa


NIST:1985:FPSb


NIST:1991:DSS


NIST:1992:DSS

REFERENCES

Abstracts/0001-0782/129904.


[Nat94c] National Institute of Standards and Technology (U. S.). Digital Signature Standard (DSS). Federal information processing standards publication 186, National Institute for...
References

NIST:1994:EES


NIST:1995:FPSb


NIST:1997:ARC


NIST:1998:FAE


NIST:1999:FPD


Neumann:1992:IRF  

Neumann:1994:IRA  

Neumann:1995:RCD  

Neumann:1997:IRC  

Newton:1997:EC  

Newman:1998:ROT  

Neve:1999:FSC  
[Amaury Nève, Denis Flandre, and Jean-Jacques Quisquater. Feasibility of Smart Cards in silicon-on-insulator (SOI) tech-
REFERENCES


Ng:1999:CST


Nguyen:1999:CGC


Nguyen:1999:CGG


Nelson:1990:SAE


Neubauer:1998:DWI


Neubauer:1998:CSD

Nichols:1998:CCCa


Nichols:1998:CCCb


Nichols:1999:IGC


Niederreiter:1986:KTC


Niederreiter:1988:SNC


NIST:1985:FPC


Nissan:1989:AIM


Nissan:1991:EMF


NIST:1992:NCS

REFERENCES


Nguyen:1998:NDC

Nguyen:1999:DZK

Naccache:1995:CDB

Naccache:1995:CDI

Nozaki:1997:LCS

Noras:1996:CHH

Nicchiotti:1998:NIS [NO98]

Nobauer:1984:CRS [Nöb84]

Nobauer:1985:CRS [Nöb85]

Nobauer:1988:CPK [Nöb88]

Norman:1973:SWB [Nor73]

Noras:1995:CHHa [Nor95a]

Noras:1995:CHHb [Nor95b]

Noras:1995:PCE [Nor95c]
Naor:1993:PZK


Naor:1997:VAI


Naor:1998:TTT


Nikolaidis:1998:RIW


Naor:1999:OTA


Niemi:1994:CPV


Nyberg:1995:MRS

Naor:1998:UIS


Needham:1978:UEAa


Needham:1978:UEAb


Needham:1987:AR


Neuman:1988:AUE


Norris-Saucedo:1989:DAD


Naor:1995:VC


Naccache:1997:NPK

David Naccache and Jacques Stern. A new public-

Nguyen:1997:MRC


Nguyen:1997:MHR


Nguyen:1997:CAC


Nechaev:1998:DSB


Nguyen:1998:BQS


Nguyen:1998:BSR

Nguyen:1998:CAD


Nguyen:1999:CFP


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


Naor:1990:PKC

REFERENCES

p427-naor/. ACM order no. 508900.

Nyberg:1994:DUM


Nyberg:1995:LAB


Nyberg:1998:ACE


Nystrom:1999:PCT


Ohta:1994:LCF


Ohsuga:1999:EHI

REFERENCES

Oakley:1978:RPC

Oberzalek:1999:GEE

OConnell:1981:CDE

OConnor:1994:UBN

O Connor:1995:DCT

Obenland:1999:SED

O'Ruanaidh:1996:PWD

Odlyzko:1984:CAM
[Odl84] Andrew M. Odlyzko. Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's


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

[Odl94a]

[Odl94b]

[Odl95]

[Odl98]

[Oel97]
Thomas Oelke. VHDL design of a DES encryption cracking system. Thesis (M.S.), Rochester Institute of Technology, Rochester,
REFERENCES


REFERENCES


REFERENCES

441, November 1988. CO-
DEN ACSYEC. ISSN
0734-2071. URL http:
//www.acm.org:80/pubs/
citations/journals/tocs/
1988-6-4/p432-okamoto/.

Okamoto:1993:RAC

T. Okamoto. On the re-
lationship among crypto-
graphic physical assump-
tions. Lecture Notes in
Computer Science, 762:
369–378, 1993. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Okamoto:1993:PSP

T. Okamoto. Prov-
bably secure and prac-
tical identification schemes
and corresponding signa-
ture schemes. Lecture Notes
in Computer Science, 740:
31–53, 1993. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Okamoto:1994:DCS

Tatsuaki Okamoto. Design-
nated confirmmer signatures
and public-key encryption
are equivalent. In Desmedt
[Des94b], pages 61–74. CO-
DEN LNCSD9. ISBN 3-
540-58333-5 (Berlin), 0-387-
58333-5 (New York). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-

ny.com/link/service/series/0558/bibs/0839/08390061.
htm; http://link.springer-
ny.com/link/service/series/0558/papers/0839/08390061.
pdf.

Okamoto:1998:TKR

T. Okamoto. Threshold
key-recovery systems for
RSA. Lecture Notes in
Computer Science, 1361:
191–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Okamoto:1998:TKS

T. Okamoto. Threshold
key-recovery systems for
RSA. Lecture Notes in
Computer Science, 1361:
191–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Okon:1996:DWN

Chris Okon. Digital water-
marking: New techniques
for image ownership brand-
ing. Advanced Imaging, 11
(10), October 1996. CO-
DEN ADIMEZ. ISSN 1042-
0711.

Okon:1997:KMA

Chris Okon. Keeping up
multimedia asset value. Ad-
vanced Imaging, 12(7):42–
43, July 1997. CODEN
ADIMEZ. ISSN 1042-0711.
Ogata:1997:FTA


Ogata:1993:NSS


Oleshchuk:1995:PKC


Ohta:1994:DAM


Ohbuchi:1997:WTP


Ohbuchi:1998:WTD


Ozaki:1993:HVP

S. Ozaki, T. Matsumoto,

Omura:1990:PKC

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

Ochi:1998:NSO


ONeil:1986:ETM


Ogawa:1998:WTM


Okamoto:1990:DZKb


Ohta:1993:DMS


ORuanaidh:1998:RST


ORuanaidh:1999:CCP


Oppler:1996:ASS

Rolf Oppliger. *Authentication systems for secure networks*. The Artech House computer science library. Artech House
REFERENCES


[Ort95a] G. Orton. A multiple-iterated trapdoor for dense

**Orton:1995:MIT**


**OShea:1988:CDU**


**Okamoto:1991:EAC**


**Okamoto:1992:EAC**


**Olejar:1998:CPR**


**Orup:1991:VER**

REFERENCES


Ong:1991:TCM


Ong:1985:ESS


Okamoto:1998:NPK


Okamoto:1998:SIB

REFERENCES


The World Wide Web Journal is a quarterly publication that provides timely, in-depth coverage of the issues, techniques, and research developments in the World Wide Web. The December issue contains the Conference Proceeding papers that were chosen for the 4th International World Wide Web conference in Boston, MA.


<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Journal</th>
<th>Volume/Issue</th>
<th>Pages</th>
<th>Year</th>
<th>ISBN</th>
<th>LCCN</th>
<th>URL</th>
</tr>
</thead>
</table>
REFERENCES


Aiyaswamy Parthasarathy. Digital signature generator for cryptographic applications. Thesis (M.S.), South Dakota School of Mines and Technology, Rapid City, SD, USA, 1985. 148 pp. [Par85]


Wayne Patterson. Mathematical cryptology for computer scientists and mathematicians. Rowman and
REFERENCES


Patarin:1991:PPB


Patarin:1991:NRP


Patarin:1995:CMI


Patarin:1996:ACH


Paterson:1999:IPG


Paulson:1998:IAV


Paulson:1999:IAI

REFERENCES


Poovendran:1999:ITA

Proctor:1999:PC

Piva:1997:DBW

Preneel:1997:CHF

Preneel:1989:CHB

Preneel:1990:CTA
REFERENCES

Petrie:1998:NBR

Pizzonia:1999:OOD

Plagge:1999:DET

Pearcey:1980:EDS

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

[PC98]
[PD99a]
[PD99b]
REFERENCES


Pedersen:1991:NIS


Pedersen:1991:TCT


Pedersen:1991:NII


Pedersen:1991:NIT


Pedersen:1995:EPS

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


REFERENCES

(Perrig:1997:CPE)
Perrig:1997:CPE


(Perkuhn:1999:DSC)
Perkuhn:1999:DSC


(Pesic:1997:SSS)
Pesic:1997:SSS


(Petho:1991:PTA)
Petho:1991:PTA


(Petersen:1998:HCD)
Petersen:1998:HCD


(Panagopoulos:1994:BSS)
Panagopoulos:1994:BSS


(Pfitzmann:1995:BEA)
Pfitzmann:1995:BEA

REFERENCES

Pfitzmann:1996:IHT


Pfitzmann:1996:TTT


Pfitzmann:1996:DSS


Pfleeger:1989:SC


Pfleeger:1995:ULC


Pfleeger:1997:SC


Pomerance:1990:CCNb

REFERENCES


Patarin:1997:ACB


Patarin:1997:ACS


Pieprzyk:1996:CBT


Preneel:1991:CRH


Preneel:1992:CSH


Preneel:1993:CHF


Preneel:1993:HFB

[PGV93b] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block

Preneel:1993:IAH


Preneel:1993:CSI


Preneel:1994:HFB


Pohlig:1978:IAC


Post:1991:RSE


Praun:1999:RMW

REFERENCES


Phillips:1998:SHI

Pichler:1986:ACE

Pichler:1998:E

Pierce:1977:SSP

Pieper:1993:CRD

Pinch:1997:UCN

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

Pitas:1995:PIW


Pitas:1996:MSC

Pitas:1996:RSS

Pitoura:1996:RSS

Popek:1979:ESC

REFERENCES


REFERENCES

Petrounias:1994:RBA


Pless:1975:ESC


Pless:1977:ESC


Plimmer:1998:MIW


Plumstead:1982:ISG


Plumstead:1983:ISP


Pei:1999:COA

REFERENCES


Payne:1978:OEN


Petersen:1998:SST


Pitt:1999:DAC


Proctor:1992:AIC


Pudil:1995:ASM

Preneel:1994:CCM


Pointcheval:1999:NPK


Pollard:1974:TFP


Pomerance:1988:ACC


Pomerance:1990:CCNa

Carl Pomerance. Cryptology and computational


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT


Posch:1992:TMD


Posch:1993:PFP


Posch:1998:MPC


Posch:1989:AEA


Pfitzmann:1990:HBD

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


Posch:1992:MRR


Posch:1992:RNS


Posch:1995:MRRb


Posch:1995:MRRa


Pakstas:1996:SNN


Pedersen:1997:FSS


Park:1997:TER


Peleg:1979:BSC


Preneel:1998:SAA


Pratt:1939:SUS


Pratt:1996:SUS


Parra:1998:MPS


Preneel:1998:RDD


REFERENCES

[Price:1983:ABR]


[Pronzini:1980:MCC]

[Proctor:1985:SSC]

[Patel:1999:TML]
S. Patel, Z. Ramzan, and G. S. Sundaram. Towards making Luby-Rackoff ciphers optimal and practi-
REFERENCES


**Parker:1997:GFA**


**Padro:1998:SSS**


**Patel:1998:EDL**


**Patiyoot:1998:APW**


**Patiyoot:1998:SIW**


**Patiyoot:1998:TAPa**

REFERENCES

Patiyoot:1998:TAPb


Poupart:1998:GSR


Poupart:1998:SAP


Patiyoot:1999:MES


Patiyoot:1999:WSS


Patiyoot:1999:SIA


Patiyoot:1999:CST

REFERENCES

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

Patiyoot:1999:WWA


Pfenning:1999:SDT


Patel:1997:UDB


Pieprzyk:1991:RAS


Pieprzyk:1995:PA


Pieprzyk:1995:ACA

REFERENCES

Paar:1997:FAA


Paer:1997:FAA

Pomerance:1980:PSW


Pfitzmann:1995:HBA


Phoenix:1995:QCP

S. J. D. Phoenix and P. D. Townsend. Quantum cryptography: Protecting our future networks with quantum mechanics. Lecture Notes in Computer Science,
REFERENCES


REFERENCES

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

Preneel:1996:STM


Pfitzmann:1986:NUO


Pfitzmann:1993:APS


Piper:1993:DSH

REFERENCES

ISBN 1-85617-211-2. LCCN ????.


REFERENCES


REFERENCES

## Radlo:1997:LIC


## Ramagopal:1992:DRB


## Rand:1955:MRD


## Randell:1982:ODC


## Rand:2001:MRD


## Rao:1984:JEE


## Ratcliff:1996:DIN

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

Rhodes-Burke:1982:RSA


Reiter:1994:HSR


Ramesh:1999:VPP


Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA

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


REFERENCES


REFERENCES


REFERENCES


[Richards74] 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.


Riley:1996:LET

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

Ripe:1995:IPS


Ripe:1995:RIP


Ritter:1999:IWC


Ritchie:19xx:DCW


Rivest:1974:HCA


Rivest:1974:AAR

Ronald L. Rivest. Analysis of associative retrieval algorithms. Technical Report TR.54, Institut de la Recherche en Informatique et Automatique, now Institut National de Recherche en Informatique et Automa-
REFERENCES

676


Rivest:1979:CRC


Rivest:1980:DSC


Rivest:1985:RCP


Rivest:1987:EDR


Rivest:1990:RMM


Rivest:1990:C

REFERENCES


[Riv1991:FFM]


REFERENCES


REFERENCES

[Rivest:1998:RDR]

[Rivest:1998:CWE]

[Rivest:1998:CAR]

[Rivest:1998:CWC]

[Rivest:19xx:PC]
R. Rivest. Personal communication. ????, 19xx.

[Rhodes:1993:ZF]

[Rijmen:1998:WL]

[Rowlett:1998:SMM]
REFERENCES

Roy:1999:QCE


Rosenson:1994:GWE


Ruanaidh:1996:WDI


Reeds:1985:NPR


Rao:1987:PKA


Rao:1989:PKA

REFERENCES

Raisch:1996:ACH


Roberts:1993:ECI


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Roe:1994:PSC


Roe:1995:PBC


Roelse:1999:CWD

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

**Rogaway:1995:BHA**


**Rogaway:1996:SD**


**Rohwer:1975:GIM**


**Rohwer:1977:CCB**


**Rohatgi:1999:CNR**

Pankaj Rohatgi. A cautionary note regarding evaluation of AES candidates on smart-cards. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ???? LCCN ???? No slides for the conference talk are available.

**Roman:1990:C**


**Rompel:1990:OWF**

J. Rompel. One-way functions are necessary and sufficient for secure signatures. In ACM [ACM90], pages
REFERENCES


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


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

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

February 1996. CODEN LOGNEM. ISSN 1044-6397.


REFERENCES


[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.).


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

**Rauber:1997:SDW**


**Rigney:1997:RRAa**


**Rigney:1997:RRAb**


**Rivest:1998:RBC**


**Rivest:1983:RET**

REFERENCES


REFERENCES

Riordan:1998:EKGa


Riordan:1998:EKGb


Rivest:1998:SPN


Ryan:1998:ARA


Ravi:1999:AAT


Reiter:1999:AMA


REFERENCES


REFERENCES


REFERENCES


[Rus90] D. Russel. High-level security architecture and the


[S.73] H. S. *Cryptographie, ou, Divers systèmes d’écrire*
secretely spécialement pour l’usage des cartes postales: combinations alphabétiques, correspondance chiffrée, écriture par signes: divers procédés pour la fabrication d’encres sympathiques.


Schiller:1995:SWT


Sabourin:1994:CCP


Sacco:1936:MC


Sacco:1947:MC


Sacco:1951:MCF


Sacco:1977:MC


Sahai:1999:NMN


**Salomaa:1996:PC**


**Salvail:1998:QBC**


**Salvail:1999:SHG**


**Shimoyama:1997:IFS**


**Sameshima:1998:KES**


**Sansom:1986:BRC**


**Sandhu:1988:CIT**

REFERENCES


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Smid:1992:DES


Smid:1993:RCN


Shepherd:1994:UBS


Shepherd:1995:CNL


Schneier:1997:EPP

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>
Siegberg:1999:TDG


Sztandera:1999:ANN


Shepherd:1999:NCS


Chen:1985:RGE


Schneider:1996:RCB

REFERENCES


**Smith:1996:MIH**


**Sun:1997:DCP**


**Schneider:19xx:DWI**


**Scacchitti:1986:CT**

Fred A. Scacchitti. The cryptographer’s toolbox.

**Styner:1999:BMD**


**Schwenter:1620:SSN**

Verlegung Simon Halbmayers.

**Schwenter:1633:SSA**


**Schroeder:1975:ESK**


**Schell:1983:SPA**


**Schroeder:1984:NTS**


**Schroeder:1986:NTS**


**Schnorr:1990:EISb**

REFERENCES

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

Schnorr:1990:EISa

Claus P. Schnorr. Efficient identification and signatures for smart cards (abstract). Lecture Notes
in Computer Science, 434:688–??, 1990. CODEN LNCSDE. ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340688.htm;

Schroeder:1990:NTS

M. R. (Manfred Robert) Schroeder. Number theory in science and communication: with applications
in cryptography, physics, digital information, computing, and self-similarity, volume 7 of Springer series
in information sciences. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
xix + 374 pp. LCCN QA241 S318 1990.

Schmitt:1991:EAA

Joachim Schmitt. An embedding algorithm for algebraic congruence function fields. In Watt [Wat91],
citations/proceedings/issac/120694/p187-schmitt/.

Schneier:1991:OHF

Bruce Schneier. One-way hash functions: Probabilistic algorithms can be used for general-purpose pattern
ISSN 1044-789X.

Schnorr:1991:FHE

C. P. Schnorr. FFT-hashing, an efficient cryptographic hash function. In Feigenbaum [Fei91], page ??
REFERENCES


Schifreen:1992:PPD


Schneier:1992:SSA


Schneier:1992:UPC


Schilling:1993:MBC


Schneier:1993:SCD


Schneier:1993:DS


Schneier:1993:IEA


Schneier:1993:UHD

REFERENCES


CODEN DDJOEB. ISSN 1044-789X.

**Schneier:1995:MS**


**Schneier:1995:MSH**


**Schneier:1995:OPE**


**Schneier:1995:PCC**

Bruce Schneier. A pair of cryptographic conferences.

**Schneier:1996:ACP**


**Schneier:1996:CC**


**Schneier:1996:DLC**


**Schneier:1997:IRC**

Bruce Schneier. Inside risks: Cryptography, security, and the future. *Communications of the Association for
Schneier:1997:WCH

Schroeder:1997:NTS

Schweighofer:1997:DIF

Schlesinger:1998:CPC

Schmalz:1998:MDI

Schneier:1998:CBT
Bruce Schneier. The crypto bomb is ticking: Crack-

Schneier:1998:CDV


Schneier:1998:CTS


Schneier:1998:SPC


Schneier:1998:TEA


Schoenmakers:1998:SAE


Schroeppel:1998:HPC

REFERENCES


**Schneier:1999:IRT**


**Schneier:1999:IRU**


**Schneier:1999:IWC**


**Schoenmakers:1999:SPV**


**Schroeder:1999:SEA**


**Schumann:1999:PST**

REFERENCES

Schwentick:1999:DCL


Scerri:1999:UOS

[P. Scerri, S. Coradeschi, and A. Toerne. A user oriented system for developing behavior based agents. Lecture Notes in Computer Science, 1604:173–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).]

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**

REFERENCES

URL http://link.springer-ny.com/link/service/series/0558/tocs/t0293.htm
CRYPTO '87, a Conference on the Theory and Applications of Cryptographic Techniques, held at the University of California, Santa Barbara ... August 16–20, 1987.


REFERENCES


Saeednia:1999:SCG


Sapir:1999:DRT


Sgarro:1990:IDB


Sgarro:1991:STC


Sgarro:1991:LBA


Sgarro:1993:ITB

REFERENCES


REFERENCES


[Sha48a] Claude Shannon. A mathematical theory of communication. The Bell System Technical Journal, 27(3):379–423, July 1948. CODEN BSTJAN. ISSN 0005-8580. From the first page: “If the base 2 is used the resulting units may be called binary digits, or more briefly, bits, a word suggested by J. W. Tukey.”. This is the first known printed instance of the word ‘bit’ with the meaning of binary digit.


REFERENCES

Shamir:1982:PTA

Shamir:1983:ECC

Shamir:1983:GCS

Shamir:1984:PTA

Shamir:1985:IBC

Shamir:1986:SPS

Shamir:1987:CSS
Adi Shamir. Cryptography: State of the science. In Ashenhurst [Ash87],
REFERENCES

721


**Sherman:1986:CVT**


**Shepherd:1992:FFW**


**Shepherd:1992:FHS**


**Shepherd:1992:HSC**


**Shepherd:1992:NPS**

[She92e] S. J. Shepherd. A numerical processor with supercomputer performance based on state-of-the-art finite-impulse-response filter digital signal processors. Internal Research Note 5, Electronic and Electrical Engineering Department, Uni-
REFERENCES


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


REFERENCES


Shparlinski:1999:FFT


Shparlinski:1999:NTM


Shulman:1980:BRB


Shulman:1976:ABC


Shulman:1982:BRB


Sakurai:1993:DBS

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


Sakurai:1993:SCS


Sakurai:1994:SCT


Sidhu:1981:APG


Sieminski:1983:SBB


Siegenthaler:1984:CIN


Siegenthaler:1985:DCS

Earl Swartzlander, Jr., Mary Jane Irwin, and Graham Jullien, editors. Proceedings: 11th Symposium...
REFERENCES


Simmons:1979:HID


Simmons:1979:CCA


Simmons:1979:SAE


Simmons:1982:SAC


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC

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

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.


Gustavus J. Simmons. Geometric shared secret and/

Simmons:1992:CCS


Simmons:1993:SCU


Simmons:1994:CTS


Simmons:1994:CPF


Simmons:1994:SCP


Simmons:1994:SCE

Gustavus J. Simmons. Subliminal communication is

**Simovits:1995:EDE**


**Simmons:1996:HSC**


**Simmons:1998:RCB**


**Simmons:1997:SCS**


**Simmons:1998:SCS**


**Simmons:1998:RCB**

REFERENCES


Simon:1998:FCO


Sinkov:1966:ECM


Sinkov:1968:ECMa


Sinkov:1968:ECMb


Sinkov:1968:ECM


Sinkot:1977:CTC


Singh:1985:IPS


Sinha:1995:KNC


Singer:1998:ECD

Anthony Martin Singer. Electronic commerce: dig-

**Singh:1999:CBE**


**Siu:1999:PNG**

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

**Sambur:1976:SEM**


**Sethi:1997:FCS**


**Scott:1998:DAB**


**Sako:1994:SVU**

REFERENCES


REFERENCES


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

**Schneier:1997:AESa** [SK98a]

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

**Stabell-Kulo:1997:SLS**

**Schneier:1998:CSS**

**Shimoyama:1998:QRS**
REFERENCES

Shimoyama:1998:QRB

Schneier:1999:SAL

Shepherd:1997:EKE

Schell:19xx:CMC

Sorokine:1994:TBD

Suzuki:1999:AVB
[SKIT99] S. Suzuki, T. Kato, H. Ishizuka, and Y. Takahashi. An application of vision-based learning in RoboCup for a real robot with an omnidirectional vision system and

Satoh:1998:HSR


Satoh:1998:HSS


Schneier:1996:DP


Schneier:1998:TKSa


Schneier:1998:TBBa


Schneier:1998:TBBb

REFERENCES


Schneier:1999:APC

Schneier:1999:NRT

Schneier:1999:TEAb

Schneier:1996:AC

Schneier:1999:TKS

Sufatrio:1999:IMS
Slutsky:1998:KDQ


Schobi:1983:FAT


Siromoney:1990:PKC


Staffelbach:1991:CSC


Schubert:1995:MLS


Syverson:1995:FRK


Sklower:1996:RPE

REFERENCES


Schneier:1998:CMP


Smart:1999:PHC


Schneier:1999:DDE


Smejkal:1997:DEI


Sutcliffe:1999:LBM


Sklower:1998:RPE


Sutcliffe:1999:LBM


[Smith:1943:CSS]


[Smith:1944:CSS]


[Smith:1955:CSS]


[Smith:1971:CSS]


[Smith:1983:PKC]


[Smith:1990:PPC]


[Smith:1993:ADA]
REFERENCES


REFERENCES


REFERENCES


Sorkis:1980:USM


Soto:1998:RTA


Smith:1979:UFP


Seberry:1989:CIC


Seberry:1990:ACA

Schechter:1999:AAM


Spirakis:1995:AET


Saltzer:1984:EEA


Shin:1998:NHF

REFERENCES


1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). [SS95a]


REFERENCES


**Schneier:1999:BHD**


**Schoenhoff:1999:GVM**


**Shapiro:1999:MAE**


**Sloomonides:1999:REI**


**Stubblebine:1999:FLA**


**Stubblebine:1999:FOA**


**Subramanian:1987:DTP**

Siromoney:1988:CPL

Saito:1999:DPC

Smith:1981:VEP

Stubblebine:1999:UST

Safford:1993:SRA

Sakai:1997:WRK
Y. Sakai, K. Sakurai, and I. Ishizuka. On weak RSA-keys produced from Pretty Good Privacy. Lecture Notes in Computer Science,
REFERENCES


Susilo:1999:FST


Shepherd:1990:CSS


Schmidt:1998:LOA


Salter:1998:TSS


Schneier:1998:DDE


StJohns:1984:RAS

REFERENCES

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

**StJohns:1985:RAS**


**Shawe-Taylor:1989:BRB**


**Stern:1991:CPK**


**StJohns:1993:RIP**


**Safavi-Naini:1994:OAS**

Stark:1970:INT


Stark:1978:INT


Stallings:1994:PGP

William Stallings. Pretty Good Privacy: Privacy and security are important issues to commercial users of public E-mail systems. PGP, an E-mail security package, is finding acceptance as the way to achieve protection. *BYTE Magazine*, 19(7):193–??, July 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Stallings:1995:PWT


Stallings:1995:PYP


Stadler:1996:PVS


Staiger:1996:CSW

REFERENCES

Stallings:1996:PCS


Stallings:1996:PCI


Staddon:1997:CSC


Stallman:1997:SDR


Stark:1997:ESP


Stallings:1999:CNS


Stallings:1999:HAK

[Sta99b] William Stallings. The HMAC algorithm: Key hashing for message authentication. *Dr. Dobb’s Jour-
REFERENCES

Stevenson:1976:MCI

Stevens:1970:CPi

Stevens:1990:CPk

Steinberg:1991:VSV

Stewart:1992:SCK

Stern:1994:DIS
REFERENCES


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


[Ste99a] Neal Stephenson. Crypto-

REFERENCES


REFERENCES


[Sto65] Stout:1965:DRN


[Sto89] Stoll:1989:CET


[Sto90] Stout:1990:SDE

Sivabalan:1993:DSN


[STP93]

Stripp:1987:BJC


[Str87]

Stripp:1989:CFE


[Str89]

Strauss:1993:SEC


[Str93a]

Strauss:1993:SMC


[Str93b]

CODEN DTMNAT. ISSN 0011-6963.

Stripp:1995:CBF


[Str95]

Sander:1999:AAE


[STS99a]

Sander:1999:FCN


[Sandholm:1999:DOC]

Sandholm:1999:DOC

REFERENCES

**Stumme:1999:AEK**


**Steiner:1995:REE**


**Su:1998:DEM**


**Summers:1984:OCS**


**Sun:1991:RSE**


**Sum: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 ??.


Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling PC’s; server-side scripting; stronger encryption; inner loops; Einstein kudos. Dr. Dobb’s Journal of Software Tools, 23(3):8, 12, March 1998. CODEN DDJOEB. ISSN 1044-789X.


REFERENCES

0558/papers/0473/04730306.pdf.


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


REFERENCES

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


REFERENCES

Swanson:1998:MSV


Swanson:1998:RAW


Seberry:1994:ISA


Seberry:1995:RAN


Seberry:1995:SCF

REFERENCES

Seberry:1995:RBP

Theodoridis:1998:NES

Takano:1999:CAC
Kohji Takano et al. A cryptographic accelerator card with small fast low-power RSA engines. In Anonymous [Ano99c], page ??

Tang:1997:DBC

Taaffe:1998:NBL

Tabatabaian:1994:CAP

Takagi:1997:FRT
REFERENCES


REFERENCES


REFERENCES

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

[Tao:1999:GPK]

[Tao:1999:FAP]

[Tao:1997:FNF]

[Tangney:1991:SIS]

[Tedrick:1985:FES]

[Teske:1998:SPR]
REFERENCES


Thomas:1986:SDE

Thompson:1987:RTT

Thomas:1996:PVS

Tarman:1998:AAE

Tsujii:1988:PKC

Tilki:1998:EHD

Tippett:1927:RSN

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


Four volumes.


Takagi:1996:MMP


Takagi:1996:MVM


Terada:1997:LDC


Todorovic:1997:CAS


Tirkel:1998:IWR


Tonchev:1996:CDG


Toussaint:1991:DCK

REFERENCES

link/service/series/0558/  
bibs/0576/05760024.htm;  
http://link.springer-  
ny.com/link/service/series/  
0558/papers/0576/05760024.  
pdf.


REFERENCES


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


REFERENCES

Two volumes. Second biennial conference of the Australian Pattern Recognition Society.

[TS88]

[TS93]
Terry:1988:MSV

[TS93]
T. Tokita, T. Sorimachi, and M. Matsui. Linear cryptanalysis of LOKI and s02DES. Lecture Notes in Computer Science, 917: 293–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Ts'90]

[Ts'97]
Tso:1990:NPK

[TSN93]

[Ts'97]
Tombak:1993:ACP

[TSN93]

[Ts'92a]
Tsudik:1989:DAI

[Ts'92a]

[Ts'92a]
REFERENCES

2860. IEEE catalog number 92CH3133-6.


REFERENCES

Tuchman:1966:ZT


Tuchman:1979:HPN


Tung:1999:KNA


Turing:1941:APC

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

Tijdeman:1992:CDP

R. Tijdeman and Jacobus Henricus van Lint. Cryptography and data protection: proceedings of a symposium at the Royal

Tel:1994:DAI


Tan:1992:NPE


Takagi:1992:MMH


Trabelsi:1994:PPS


REFERENCES


[Tax:1999:PFD]

[Tygar:1996:CPI]

[Tillich:1994:HS]

[Tzeng:1999:CMC]

[Ude98] 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).

[Uehara:1995:ESB]
 REFERENCES

Udell:1994:BCRb


USASC:1923:EC


USASC:1940:CML


USASC:1942:ACC


USDOS:1970:BC


USNBS:1977:DES


REFERENCES


USNSACSSCCH:1992:FLT


USDOA:1994:OMT


USDOA:1994:UDS


USNSACS:1994:SC


USCSCJSTL:1995:ACC


USNSGC:1995:NDN

REFERENCES


[Uni96c] United States Patent and Trademark Office. Class 380 Cryptography... Patent Classification Definitions... Patent And Trademark Of-


REFERENCES

Docs. Shipping list no.: 98-0348-P.

USCHCIRSIEPT:1998:EIR

[Uni98d]

USCHCIRSIEPT:1998:HSF

[Uni98f]

USCHCSCST:1998:HEH

[Uni98g]
REFERENCES

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


[UNN85] United States. General Services Administration, National Communications System (U.S.). Office of Technology and Standards, and

[USE88a] USENIX, editor. UNIX Security Workshop Proceed-
REFERENCES

Portland, OR. USENIX
Association, Berkeley, CA, [USE88b]
USA, 1988. LCCN QA76.8.U65
U55 1988(1)-1990(2)//.

USENIX:1988:PFU

USENIX Association, editor. Proceedings of the
(First) USENIX Security Workshop, August 29–
30, 1988, Portland, OR, [USE90]
USA. USENIX Association,
LCCN QA76.8.U65 U55
1988(1)-1990(2)//.

USENIX:1988:UCPb

USENIX Association, editor. USENIX Conference Proceeding
(Dallas, TX, USA). USENIX Association,
LCCN ????

USENIX:1989:UCPb

USENIX, editor. USENIX Conference Proceeding,
Summer, 1989. Baltimore,
MD. USENIX Association,
Berkeley, CA, USA, Summer
1989.

USENIX:1989:PSU

USENIX Association, editor. Proceedings of the Summer
1989 USENIX Conference: June 12 — June 16,
1989, Baltimore, Maryland
USA. USENIX Association,
Berkeley, CA, USA, 1989.
LCCN QA 76.76 O63 U83 [USE93]
1989.

USENIX:1990:USI

USENIX Association, editor. UNIX Security II: USENIX workshop proceedings, August 27–28, 1990,
Portland, Oregon. USENIX Association,
Berkeley, CA, USA, 1990. LCCN QA 76.9
A25 U55 1990.

USENIX:1991:PWU

25, 1991, Dallas, TX, USA. USENIX Association,
Berkeley, CA, USA, 1991. LCCN QA 76.76 O63 U84

USENIX:1992:PWU

USENIX Conference: January 20 — January 24,
1992, San Francisco, California. USENIX Association,

USENIX:1992:USI

Baltimore, MD. USENIX Association, Berkeley, CA,
LCCN ????

USENIX:1993:USI

USENIX Association, editor. UNIX Security IV
REFERENCES


REFERENCES


REFERENCES

[USENIX:1998:SUS]

[USENIX:1999:PEU]

[USENIX:1999:PTSa]

[USENIX:1999:UAT]

[USWD:1980:EC]
REFERENCES

USWD:1983:EC


USDOA:1989:BC


USCHCJ:1997:SFT


USPBC:1997:AEC


Vadhri:1995:VID

[Vad95] Kumar S. Vadhri. VLSI implementation of the data encryption algorithm. Thesis (M.S.), Department of Electrical Engineering, University of Hawaii at Manoa, Manoa, HI, USA, 1995. x + 89 pp.

Valerio:1892:C

REFERENCES


REFERENCES

vanRenesse:1996:OSC


vanDijk:1997:MIT


vanRenesse:1997:ODS


vanderLubbe:1998:BMC


Varaiya:1999:DSI


Varma:1999:IDD


Vaudenay:1993:FHI


REFERENCES


References

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


REFERENCES

Lubbe:1998:BMC


Wal:1997:PBR


Vedder:1993:SAM


Vedder:1998:GSS


Vedder:1998:ISI


Venema:1990:IEI


Venkaiah:1992:RBP


Vernam:1926:CPT


Veron:1995:CHI

P. Veron. Cryptanalysis of Harari’s identification
REFERENCES


**Verschuren:1998:SCN**


**Verschuren:1998:SAS**


**VonzurGathen:1999:MCA**


**Vandewalle:1993:TAT**


**Vallee:1988:HBO**


**Vallee:1989:HGR**


**Verschuren:1993:IOS**


REFERENCES


Kerckhoffs:1883:CMF


Varadharajan:1999:DER


Voyatzis:1998:WDO


Venkataraman:1994:PER


Venkataraman:1995:CEA


Oorschot:1991:CPP

Paul C. van Oorschot. A comparison of practical public-key cryptosystems based on integer factorization and discrete log-

REFERENCES

VonZurGathen:1992:PEF


Voukalis:1980:DFC


Voukalis:1980:GSE


vanOorschot:1996:DHK


vanOorschot:1996:KPA


Voyatzis:1996:ATA

REFERENCES

Voyatzis:1998:DIW


Voyatzis:1999:PDI


Varadharajan:1997:ISP


Vassiliadis:1988:PEA


Volts:1941:BC

James D. Volts and David Shulman. Bibliography of cryptography. U. S. Army, Cincinnati, OH, USA, 1941. 93 pp. LCCN Z103.A1 V6 1941. Typewritten (carbon copy) Three heavy leaves precede sections II-IV (not included in pagination). This copy was made especially for the United States Army from the original manuscript. Third copy: pencilled note on cover. Contents: pt.1. Cryptogra-
REFERENCES  815

PHY; PT. 2. TITLES RELATING INDIRECTLY TO CRYPTOGRAPHY; PT. 3. REJECTED TITLES; PT. 4. AUTHOR INDEX.


vanTilburg:1986:DBK


vanSchyndel:1994:DW


Vu:1995:CPM


Vazirani:1985:ESP


Valiant:1986:NED


Verheul:1997:CLS

Vandemeulebroecke:1990:SCB


Verheul:1997:BEF


VanOorschot:1996:DKA


Vedder:1998:SCR


vanOorschot:1999:PCS

REFERENCES

tronie). URL http://
link.springer.de/link/
service/journals/00145/
bibs/12n1p1.html; http://
link.springer.de/link/
service/journals/00145/
papers/12n1p1.pdf; http://
link.springer.de/link/
service/journals/00145/
papers/12n1p1.tex.

vanEmdeBoas:1999:ALP
[vWN99]

P. van Emde Boas, J. Wiedermann, and M. Nielsen, editors. Automata, lan-
guages and programming: 26th international collo-
quium, ICALP’99, Prague, Czech Republic, July 11–15, 1999: pro-
ceedings, volume 1644 of Lecture Notes in Computer Science. Spring-
er-Verlag, Berlin, Germany / Heidelberg, Ger-
many / London, UK / etc., 1999. ISBN 3-540-66224-

Vanstone:1997:ECC
[VZ97]

Scott A. Vanstone and Robert J. Zucherato. Elliptic curve cryptosyst-
systems using curves of smooth or-
der over the ring $\mathbb{Z}_n$. IEEE
Transactions on Information Theory, 43(4):1231–
1237, 1997. CODEN IET-
TAW. ISSN 0018-9448 (print), 1557-9654 (elec-
tronic).

Waber:1987:VEC
[Wab87]

John James Waber. Voice
cryption for cellular tele-
phones. Thesis (M.S.), Uni-
versity of Colorado, Boul-
der, CO, USA, 1987. x +
124 pp.

Weidenbach:1999:SDS
[WABC99]

C. Weidenbach, B. Af-
shordel, U. Brahms, and
C. Kohrs. System descrip-
tion: Spass version 1.0.0.
Lecture Notes in Computer
CODEN LNCSDD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Wobber:1993:ATO
[WABL93]

Edward Wobber, Martín
Abadi, Michael Burrows,
and Butler Lampson. Au-
thentication in the Taos op-
erating system. Operating
Systems Review, 27(5):
CODEN OSRED8. ISSN
0163-5980 (print), 1943-
586X (electronic).

Wobber:1994:ATO
[WABL94]

Edward Wobber, Martín
Abadi, Michael Burrows,
and Butler Lampson. Au-
thentication in the Taos op-
erating system. ACM
Transactions on Computer
Systems, 12(1):3–32, Febru-
ary 1994. CODEN AC-
SYEC. ISSN 0734-2071
(print), 1557-7333 (elec-
tronic). URL http://
www.acm.org:80/pubs/
Wade:1993:SLV


Wadsen:1998:CLI


Wagner:1993:F


Wagner:1998:DCK


Wagner:1998:CSR


Wagner:1999:BA


Wagner:1999:CFb

REFERENCES


Unconditional sender and recipient untraceability in spite of active
attacks. In Quisquater and Vandewalle [QV90], page ??
CODEN LNCSD9. ISBN 0-387-53433-4 (New York), 3-
540-53433-4 (Berlin). ISSN 0302-9743 (print), 1611-

Book review: Building in Big
Brother: The Cryptographic
Policy Debate, Lance J.
Hoffman. Operating Sys-
tems Review, 29(3):2, July
ISSN 0163-5980 (print),
1943-586X (electronic).

[Wal98] Ursula Walther.
Verschlüsselungssysteme auf
Basis endlicher Geometrien. (German) [Cryptosystems on the basis of fi-
Giessen, Giessen, Germany, 1998. iii + 151 pp.

[Walker:1999:CCI]

[Wal99a]

[Wal99b]

[WAMO94]

[Wang:1986:UEA]

Dacheng Wang. Cryptosystem and digital signature scheme based on


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).


Two volumes.
REFERENCES


The World Wide Web Journal is a quarterly publication that provides timely, in-depth coverage of the issues, techniques, and research developments in the World Wide Web. The December issue contains the Conference Proceeding papers that were chosen for the 4th International World Wide Web conference in Boston, MA.

[Wolfgang:1996:WDI]


[Wolfgang:1997:WTD]


[Wang:1999:SCB]


[Wendling:1999:PRS]

Weber:1979:USD

Weber:1983:MDC

Weber:1998:SWY

Wedemeijer:1999:DFM

Weiss:1988:BOP

Weissman:1991:IRA
References

Weissman:1991:IRN

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
REFERENCES


REFERENCES


[WHFG92] Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbons. The active badge location system.


REFERENCES


for Data Internetworks, W. Stallings.

**Wiener:1997:EKS**


**Wilkins:1641:MSS**


**Wilkes:1968:TSCa**


**Wilkes:1968:TSCb**


**Wilkes:1972:TSC**

REFERENCES


Williams:1980:MRP


Williams:1982:CHP


Willett:1983:TKS


Williams:1983:PAP


Williams:1985:SPK


Williams:1986:PKE

REFERENCES

Williams:1986:ACC

Williams:1986:CTU

Wiles:1993:HBE

Williams:1993:CPK

Wilcox:1998:SBW

Wiles:1998:HBE

Winterbotham:1969:SP
F. W. (Frederick William) Winterbotham. Secret and
REFERENCES

Winterbotham:1974:US


Winterbotham:1974:USF


Winterbotham:1975:US


Winterbotham:1978:NC


Winterbotham:1978:US


Winterbotham:1991:US


Winternitz:1983:POW


Winternitz:1984:SOH


Winternitz:1989:US

[Win89] Robert S. Winternitz. Secure one-way hash function built from DES.


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


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


REFERENCES

Wolf:1999:USC


Woolsey:1990:DDE


Worth:1975:CMA


Wortmann:1987:BRB


Wotawa:1999:NDD


Waidner:1990:DCD

REFERENCES


Wagner:1997:ASP


Wagner:1998:CO


Whiting:1998:ITI


White:1999:CBA


Weatherford:1999:NGA

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

**Wagner:1997:CCMa**

[WSK97a]


**Wagner:1997:CCMb**

[WSK97b]


**Whitten:1999:WJC**

Weiss:1985:RCM


Wu:1992:GOC


Wu:1996:SNL


Williams:1979:CAA


Wah:1984:RAM

REFERENCES

Westfeld:1998:SVC


Whiting:1998:EVT


Wu:1995:DAC


Wu:1993:CSB


Xie:1998:BWB

bibliography/073183.html

Four volumes.

[Xia:1997:MWD]

[Xie:1992:PEC]

[Xie:1993:IPK]

[Xie:1998:WDI]

[XL98]

[XL99]

[XLP99]

[XtTmW94]
G. (Gozhen) Xiao, Tsung to Tai, and Yu min Wang, editors. Mi ma hsueh chin chan = Chinacrypt'94: ti san chieh Chung-kuo mi ma hsueh shu hui i lun wen chi: 11–15 November 1994 at Xidian, China. Ko
hsueh chu pan she, Pei-
ing, China, 1994. ISBN
7-03-004363-4. LCCN ????

**Xu:1997:BPK**

Maozhi Xu and Efang
Wang. A break of public key
cryptosystem PKCY. *Science in
China. Series E, Technological
SCETFO. ISSN 1006-9321
(print), 1862-281X (elec-
tronic).

**Xu:1997:PCP**

Shouhuai Xu, Gendu Zhang,
and Hong Zhu. On the
properties of cryptographic
protocols and the weak-
nesses of the BAN-like log-
ics. *Operating Systems Re-
view*, 31(4):12–23, Octo-
ber 1997. CODEN OS-
RED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic).

**Xu:1998:STP**

Shouhuai Xu, Gendu Zhang,
and Hong Zhu. On the
security of three-party cryp-
tographic protocols. *Oper-
ating Systems Review*, 32
(3):7–20, July 1998. CO-
DEN OSRED8. ISSN 0163-
5980 (print), 1943-586X (elec-
tronic). See comments
[Ng99].

**Yacobi:1999:RMC**

Y. Yacobi. Risk manage-
ment for E-cash systems
with partial real-time audit.
*Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

**Yacobi:1999:RME**

Y. Yacobi. Risk manage-
ment for E-cash systems
with partial real-time audit.
In Franklin [Fra99], pages
(softcover). LCCN HG1710.
F35 1999.

**Yahalom:COMPSYS-7-4-451**

Raphael Yahalom. Secure
timeliness: On the cost
of non-synchronized clocks.
*Computing Systems*, 7(4):
451–465, Fall 1994. CO-
DEN CMSYE2. ISSN 0895-
6340.

**Yamamura:1998:PCU**

Akihiro Yamamura. Public-
key cryptosystems using the
modular group. *Lecture
Notes in Computer Science*,
1431:203–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Yamamura:1998:PKC**

Akihiro Yamamura. Public-
key cryptosystems using the
modular group. *Lecture
Notes in Computer Science*,
1431:203–216, 1998. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349

Yamamura:1999:FCU

Yan:1995:PTL

Yao:1982:PSC

Yao:1986:HGE

Yardley:1931:ABC

Yardley:1940:SSA
Yardley:1983:CBC


Yardley:1990:ABC


Yoshiura:1998:VDW


Yeung:1997:DWH


Yeung:1998:DW


Yeung:1999:DSM


Yokokawa:1999:BDE

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

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

Yi:1996:DAN


Yin:1997:REA


Yakovlev:1998:PND


Yahalom:1994:TBN


Yang:1999:DIC


Yen:1993:FCE


Yen:1995:IDSb


Yen:1995:IDSa

REFERENCES


Yang:1997:NEC


Yen:1997:SAT


Yi:1997:NHF


Yi:1998:NBB


Yi:1998:NBO


Ye:1999:CS


Yi:1998:DCB


REFERENCES


Yu:1999:CC


Yuan:1992:VLD


Yung:1985:CSP


Yung:1985:SUK


Yuval:1997:RTE


Yang:1997:CBC

REFERENCES

Yang:1999:GSP


Yu:1989:DEB


Yu:1991:SED


Young:1996:DSB


Young:1997:KUC


Young:1997:PKA

REFERENCES

Young:1997:SEC


Young:1998:ARA


Young:1998:MBB


Young:1998:FLP


Young:1998:MBS


Yeo:1999:WOV

REFERENCES


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


REFERENCES

Zheng:1990:LSM


Zhao:1997:LT


Zheng:1995:HBR


Zheng:1990:PDS


**Zheng:1997:SC**


**Zheng:1997:DSH**


**Zilouchian:1998:ANF**


**Zhao:1994:DS**


**Zheng:1994:RSS**


**Zheng:1998:HCE**

Zieschang:1997:CPB


Zim:1948:CSW


Zimmermann:1995:OPU


Zimmermann:1995:PSC


Zimmermann:1996:PGPa


Zimmermann:1996:PGPb


Zimmermann:1998:CI


Zimmermann:1999:EVI

Reto Zimmermann. Efficient VLSI implementa-

Zhao:1995:ERL


Zhao:1996:DWS


Zhao:1998:GDW


Zhao:1998:BTT


Zhao:1999:DWW

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

Zeng:1997:RRO


Zhou:1999:SPP


Zhang:1999:AFV


Zheng:1990:CBC


Zheng:1991:DBT


Zolman:1993:BSJ

Leor Zolman. Building a secure journal/logging util-

**Zheng:1993:HOH**


**Zhu:1996:PKC**


**Zheng:1993:PAA**


**Zwiggelaar:1999:DCM**


**Zukowski:1998:JTUb**


**Zukowski:1998:JTUa**


**Zunic:1998:MCI**

Nevenko Zunic. The MARS cipher — IBM submission to AES. In National Institute of Standards and

Zachariasen:1999:OAE


Zwiers:1998:CTD


Zeng:1991:ILS


Zeng:1991:PBG


Zeng:1990:LCT


Zhang:1995:GCG


Zhang:1996:DCC

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