Title word cross-reference

#1  [Ble98a, Kal98b, KS98a, RSA93f, RSA93a].
#10 [Kal98c].  #11 [Ano95p, Ano96-28].
#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].

$\textbf{S}1\text{-Million}$ [GC97]. 128 [Ano97-51]. 16
[BS93a, GC94]. 2
[JV98b, KG95, Kob91b, MVZ98, SBVG99].

$\textbf{S}29.95$ [Hat96]. 2n [QG99]. 2R [YLD99]. 3
[Ben99, BALS99, CK95, KSW97b, Nas94, TK99, Wor96, YY99a]. 40 [Ano97-41]. 511
A * B (mod N) [Bak92]. A^2 [JS95b].
mod 2^2 [Ber93]. c [WD99b]. χ^2 [HG97b]. d
[BD99b]. f [DJL93]. F_2^n
[SS98a, Ler97]. F_p [Miy93a]. GF(2) [She95c].
GF(208) [Ros98a]. GF(p) [Gor93b, HNM98].
> [GQW+91]. k [Car97c, DJL93, HKS97a, HKS97b, KR99b, KS97b, WD99b].

$l$ [HL93a, KS97b]. L2 [Vau99a]. λ [RS99c].
L ≥ 2 [SVxW91]. << [GQW+91]. m
[Bla94a, FR94]. Z/nZ [MM96b]. Z_n [SE96].
GD(2^n) [Ara93]. GF(2^m) [FBT96]. F_2^m
[MVZ93]. Step_k,m [GC90]. N
[BS91e, BS91d, HKS97a, HKS97b, KSW99b, KSW99c, KK98, Per93, QG90, Tak97].
N = p'q [BDHG99a, BDHG99b]. N^{0.292}
HGS98, KTM+99, KSW99c, Mat96a, MW97, NK93, Riv98c, SZ96, Wol98, YY97a, ZS93, Ada92b, AGY95a, Ano97-52, BH93, CP94, Cop94a, Dam91b, Des90a, DY91f, Dre92, FY99, GQW+91, HA94b, HY98b, HY98a, JG95, KSW99b, KR96b, KOT95a, KOT95b, LL94a, LvD98, NY90, OK96b, RS93, SG98, WK97, Win93, YL97b.

Age
[Bar94, SB97, Uni98i, Wal95, BS97b, Car97a, Joh98, Mar95b, Uni97c, Duh90].

Agencies
[MKS99].

Agency
[Gar97a].

agenda
[Mad98f].

Agent

Agent-Based
[FK99, MM99b, SJS98].

Agent-Oriented
[BLH99].

Agents
[BGS98, FGS96, GB98, INDI99, Jun99, PW99, PWU99, RS98c, RS98d, SCT99, SSP90, Vig98, YY97c].

Agile
[KLZ99, THP+98].

Agenes
[Luj98a, Luj98b].

agnostic
[JY96].

Agree
[Gar97a, Ano97-47].

Agreement
[BWM99a, Bor95, Bor96, Cae96b, Gar94, Gar97c, JV96, LM94b, LP99, Mau93a, MW96a, Mau97a, RAS93b, Van95a, Wol98, vOW96, Ano96t, By93c, BY93b, HY98b, HY98a, LM94a, VV96, Zhe95a, Zhe95b, Wei99].

Agreements
[BM99a].

Agricultural
[Far93].

AI
[MG99a, MG99b].

Aid
[SBTV99].

Aided
[BQ95b, BQ95a, HCY96a, LYH93, LL95a, MW98d, MDF94, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a].

Aids
[Cra92].

AIR
[Ano97-33, DIF94, SvA+98].

AIR-BAG
[Ano97-33].

Airborne
[CMM93].

algorithm
[ZW99, ZPS93, AA95, Acc97, LL98a, Moc97, Sch93b, Sch94e, 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, QQ90, RS99a, Sch94g, Sch94j, Sch94e, Sch96a, SW97a, SW97b, Sch94h, Sed92, Sed93, Sho97, Sot98, SB99, Sp95, Ste96, VCF+90, AA95, Ano90, Ano98m, CPP09, CMM93, CJL+92, CadHSV96, DG96, DN95b.

Alfred
[Sha99a].

Algebra
[BK94a, Pes97, VG99, CMM93].

Algebraic
[Des98a, FL99a, Gog99, HR90, Kob98b, LW91, Mv93, Wat91, Ala97, BH90, SW98, CMM93, HN94, JM96a, Sch91a, SH94, ZPY96].

Algebraic-Code
[HR90, Mv93, Ala97, CLW98, SH94].

algebraic-geometric
[JM96a].

ALGOL
[RS99c].

Algorithm
[ANS97, Ada97b, IBM93, Ano96c, Ano96f, ADEDS99, COP+95a, CD91, DKR97b, DNRS97, Dra98, GX99, GKG98, GTG94, GN95c, HG97a, HG97b, HW98, Kal91, KY95a, KR96a, KY98, KMK99, Kob98c, Kra93, Kwa97, MD98, MW94, Mas94, Mat97, Mis97, MS90b, Mau99, Nat97b, PBG90, PRB98b, Riv92a, Riv92b, Riv95c, Riv95b, Riv98a, RC94a, RC94b, RH99, Sch93d, Sch94f, Sch95a, Sch95b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SS99c, She94b, SB98, SW93, Sta99b, Swa94, TK99, THP+98, VDK98, Whe94, Yin97, ZYR91, Ano97-41, BI94, BS95a, Bow93, CC98, CG94, ISO97, IK98, JML94, KY95b, KY97, KYxx, Kir95, LR93, LZ90, LZ91a, LL93b, Lon91, LC97b, MSS93, Mey99, MPL99, Mo98, Pa96, Riv90a, Riv91b, Riv95d, Sch91a, Sch94i, Tay94, VAD95, WN95, YL93, YL95b].

algorithm
[ZW99, ZPS93, AA95, Acc97, LL98a, Moc97, OA94, Sch93b, Sch94e, 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, QQ90, RS99a, Sch94g, Sch94j, Sch94e, Sch96a, SW97a, SW97b, Sch94h, Sed92, Sed93, Sho97, Sot98, SB99, Sp95, Ste96, VCF+90, AA95, Ano90, Ano98m, CPP09, CMM93, CJL+92, CadHSV96, DG96, DN95b.
Eve98, FR95a, GP97, HJ99, HP94, Imp92, KKL99, MS99c, OS91, OS92, Pvo96, QN98a, Sch91b, Smi93a, Tab94, TY92, Tay90, TV94].

Alive [BK90].  All-Or-Nothing [Riv97c, Ste98b, BMM99a, BMM99b, Boy99, SRY99].

Alleged [Gol97d].  Allegiance [Ano98a, Gar97c].

allied [lPNdbbbprm91, AK99].  allows [Bee96].

ALM [CH99b].  Almost [AMP99, Bra95d, CCD99, Mau90].

along [BDC+95].  alpha [Zim96a, Zim96b].

alphabet [PS97].  alternating [HGW94, Wer93a, Wer93b].  alternative [BrD94, Gar97c, Neu94, Smi93b, VvT97, BR96b].

alternatives [FL93].  Alto [ACM98a, IEE98c, IEE98b].

Altogether [Ano95f, Ano95e, Ano97e, Ano97f, Ano97g, Ano99b, Ano94f].

Announcements [Got99, Ano97-38].  Announce [Ano97h, Nat97b].

Annual [ACM94a, ACM97b, Ano95r, Bri92, Bri93, CH96, Cop95b, Cop95d, EIE92b, EIE93c, EIE94b, EIE94c, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE98f, IEE99a, Kra98, Sp93, St93b, St94, USE99d, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, HAI00, IEE92d, IEE95c, IEE97I, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, WC99].

anomalous [GLV99].  Anonymity [BD99a, DFTY97, FJ98, JMP+98, STS99b].

Anonymous [DF98, DF99, FT99b, GM997, JAC96, Juc99, MS99a, OKST97, PW97a, RSG98, STS99a, SP99, SGR97, Pfi95].

Anonymous [Coh96].  ANSI [Ano94b, Ano96c, BAK92, Bas98, BK98a, BK98b, Jol99, SS97].

Answer [WD99a, Ude98].

Answers [Di 97a, Fre94, Ano92a].  Ant [BP95a].  Anti [Ano93a].

Antique [Mer90b].  antitrust [Ano97-29].

Antivirus [Nac97].  Antonio [ACM99a, ACM97b, ACM98b, ACM99b, ACM99c, Com96, Des94b, HAI00, IEE92d, IEE95c, IEE97I, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, WC99].

anyone [Ude98].  AOL [GC97].

Apache [Bal99, Mec98].

aperiodic [Fri92b].

API [Gar98b, Got99, Lin96b, McM96].

APIs

[Gi97, KAK96, NT93].  Anchoring [CS99].

Ancient [Pää93, RRP97].

and/or [Sim90b, Sim91].

ANGFIS [ZHJ98].  Angeles [IEE98e].

Angiograms [BALS99].

Anglo [Gla99b].  Anglo-American [Gla99b].

Anguilla [Fra99, Hir97, Hir98].

Animation [HE98].

annimation [HEG98].

Anniversary [CFK+91].

annotating [DSSZ99].

Announcement [Ano99b, Nat92b].

Announcements [Ano95f, Ano95d, Ano97c, Ano97f, Ano97g, Ano99b, Ano94f].

Announces [Got99, Ano97-38].

Announcing [Ano97h, Nat97b].

Annual [ACM94a, ACM97b, Ano95r, Bri92, Bri93, CH96, Cop95b, Cop95d, EIE92b, EIE93c, EIE94b, EIE94c, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE98f, IEE99a, Kra98, Sp93, St93b, St94, USE99d, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, HAI00, IEE92d, IEE95c, IEE97I, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, WC99].

anomalous [GLV99].

Anonymity [BD99a, DFTY97, FJ98, JMP+98, STS99b].

Anonymous [DF98, DF99, FT99b, GM997, Jac96, Juc99, MS99a, OKST97, PW97a, RSG98, STS99a, SP99, SGR97, Pfi95].

Anonymous [Coh96].  ANSI [Ano94b, Ano96c, BAK92, Bas98, BK98a, BK98b, Jol99, SS97].

Answer [WD99a, Ude98].

answers [Di 97a, Fre94, Ano92a].  Ant [BP95a].

Anti [Ano93a].

Antique [Mer90b].  antitrust [Ano97-29].

Antivirus [Nac97].  Antonio [ACM99a, ACM97b, ACM98b, ACM99b, ACM99c, Com96, Des94b, HAI00, IEE92d, IEE95c, IEE97I, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, WC99].

anyone [Ude98].  AOL [GC97].

Apache [Bal99, Mec98].

aperiodic [Fri92b].

API [Gar98b, Got99, Lin96b, McM96].

APIs

[Gi97, KAK96, NT93].  Anchoring [CS99].

Ancient [Pää93, RRP97].

and/or [Sim90b, Sim91].

ANGFIS [ZHJ98].  Angeles [IEE98e].

Angiograms [BALS99].

Anglo [Gla99b].  Anglo-American [Gla99b].

Anguilla [Fra99, Hir97, Hir98].  Animation [HE98].

annimation [HEG98].  Ann

Anniversary [CFK+91].

annotating [DSSZ99].  Announcement [Ano99b, Nat92b].

Announcements [Ano95f, Ano95d, Ano97c, Ano97f, Ano97g, Ano99b, Ano94f].

Announces [Got99, Ano97-38].

Announcing [Ano97h, Nat97b].

Annual [ACM94a, ACM97b, Ano95r, Bri92, Bri93, CH96, Cop95b, Cop95d, EIE92b, EIE93c, EIE94b, EIE94c, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE98f, IEE99a, Kra98, Sp93, St93b, St94, USE99d, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, HAI00, IEE92d, IEE95c, IEE97I, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, WC99].

anomalous [GLV99].  Anonymity [BD99a, DFTY97, FJ98, JMP+98, STS99b].

Anonymous [DF98, DF99, FT99b, GM997, Jac96, Juc99, MS99a, OKST97, PW97a, RSG98, STS99a, SP99, SGR97, Pfi95].

Anonymous [Coh96].  ANSI [Ano94b, Ano96c, BAK92, Bas98, BK98a, BK98b, Jol99, SS97].

Answer [WD99a, Ude98].

answers [Di 97a, Fre94, Ano92a].  Ant [BP95a].

Anti [Ano93a].

Antique [Mer90b].  antitrust [Ano97-29].

Antivirus [Nac97].  Antonio [ACM99a, ACM97b, ACM98b, ACM99b, ACM99c, Com96, Des94b, HAI00, IEE92d, IEE95c, IEE97I, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, WC99].

anyone [Ude98].  AOL [GC97].

Apache [Bal99, Mec98].

aperiodic [Fri92b].

API [Gar98b, Got99, Lin96b, McM96].

APIs
[Gol96c, Gon98]. App [AW99]. Apparatus [SKBxx, MY98]. Apple [Gar97a, GO96c]. Applet [Ber97a]. applicability [KCCT94a, KCCT94b, HKM95, SPP98]. Application [IBM93, BS99a, BSN95, Bar99, BGG95, BL96b, BL96a, Dan90a, Dan91a, Dav91, De 95, ECM96, FJRS96, Fum97, GPT91a, GPT91b, Gog99, GQ95, HNSS99, HHY93, Hat97, Hel94, Hof99, IRM93, IR99, JDK+91, KMP99, KP99a, KI96, KK95, LOX99, LCN99, Mar98a, Man96b, Mun91a, Mun91b, NC97, PSN95b, QV90, QG95, Rog95, Rue93, SSS98, Sch99i, SZ93, SK98c, SK98b, SKT91, VDDR99, Ara93, BY93c, BY93b, CC98, DDB95a, DDB95b, DF97, GZ91, HP94, LL97b, MW94, Nyb98, Pet91, PK97, SL93b, SRL98, Siu99, Ste99b, SW98, SW99a, TY92, Wou90]. Applications [Aga92, BGR98a, BFW99, CG98, CJR98a, CJR98b, CGB+93, COZ99, Cre90, Dan96, DY91a, DFGH99, Du98, DN94, Dwo97, Ebe93, FM99, Far93, Fis98, IEE95a, IEE97a, IEE92b, IEE93c, IEE94c, IEE97b, JMS96, KSH97, KSH98, KSW99b, KSW99c, KM96a, Kun94b, KT91b, Lan97, MS95f, OiDP98, OOO90, PS96b, SY96a, DY91c, TN96a, TN96b, VW98, VP96, ZY91, vW94, vW99, AC99c, Ada91, An908k, An908q, BM90, Ber93, BMP+97b, BV97, Boy98, BP97b, Com96, CFG96, DiDPS96, Dix94, Dom96, Eng99, FQ98, GVP98, GEL98, Gre94, GS94b, HMP95, JV98a, Kal95, KW29, KG93, LY93, LN94, Lub96, Mei92, Mic97, MT98, NKC94, Pe91a, PC98, Rh95, Sch90c, Sch97b, Sha95a, SMM94, Sin95, Sta97c, SSG99, T+98, USE96e, Way98, YL93, ZY90]. Applied [BHJM99, HH98, MR95a, Sch94g, Sch96a, Sch94h, Sha99a, FFW99, FMR99, MVV97, PR98, CM93, Dav94]. applying [CO98, HO96, Jan99, KMP99, MW98a, War98, ARR99]. Appraisal [FGS96]. Approach [BBN96, BK94a, DGV94a, DS97c, GM99a, Hes97, Jak99b, KRJ98, LMSV99, Mar99, MS94, MI99, PL94, PWU99, PJ99, Rab98, SRS99b, She94a, WS99, ZHJ98, Ale97, BCK98, CM96, CH97b, DH96a, DMM98, GM91, GKS97, JW91, OG95, Pau98, PGV93b, PGV94, RO96, ZL99]. Approaches [CJRR99a, GF93, Mau91a, RDK98, VG93, ZS93]. Approaches [Gar98b]. approximate [MW94]. Approaching [SG95]. approximation [KG95, KR99b, MT99b, Mil96a, RS99a, CS97d, Gol96a, Ny9h95]. Approaches [KR94b, ST91, KR95a, KR96c]. April [ACM97a, An90c, An90c, An90c, Chr98, Chr99b, Dav91, IEE95c, IEE97d, IEE98d, KK99b, Lom97, QV90]. Aquarelle [ADF98]. Arab [AK98]. Arbiter [DY91f, JS95b, JS95a]. arbitrary [Pie93]. Arbitrated [DY91f, HW98c]. Arbitration [Joh94, Kur94, PLW99, DS93, KO95b]. arcane [Beu94]. Archaeological [An97-37]. Architectural [BS95c, PN92]. Architecture [IBM93, BCCD99, CJR98a, CJR98b, Con99a, Fei93, Fei93, Gut99, JDK+91, MM99b, Mup93, NH90, NK98b, Oh99, PF94, RBV94, Rus90, SS90, She92a, She93c, Tre99, Tua99, VG93, YS99, Kar96, LS98a, Con98, JD91, LM983, SVB99, SY92]. Architecture/390 [SY92]. Architectures [Ara93, Gon99, KV99, Lip99, LF99, Mas91, PSM97, SSS98, BGV97b, Kap98, LHW99, PJMB90, WDB97]. area [Fum93, LE99, Van95b]. areas [HA00, TM99]. aren't [Cha99a]. Arguments [BJY97, BD91, NOY93]. Arias [DHR96]. arising [AP93]. Arithmetic [BP98a, Bre99, BP97c, Bus97, CD98b, DBVD96, KK99b, LL99, LD99, Mih94, NM96a, PSR97, SSS98, SI93, CPP98, ISO97, JS93a, Kal92, Kal93b, KM99a, Pos93].
USE98a, USE98b, USE99a, Wie99, Yua92. AUSCRYPT [SP90, SZ93]. Austin [Ano94e, IEE98e]. Australasian [VPM97]. Australia [DG96, GN95b, KG93, KK99b, MSD90, PSN95b, SP90, SZ93, VPM97].

Austrian [CFK91, GN95b, Cae96a, Orl96, Ree97]. Austria [BS95e]. Authentic [BF97a, BWM98, BWM99a, Bor95, CHH97, Dan95, HCY96b, JY96, LC97a, Mau97a, RH93, SKWH96, BSNP96a, BSNP96b, BF99b, BR97b, DvW92, HY98b, HY98a, Yeu99]. Authenticating [ADSW99, Hel98a, KS99a, Mit92a, SK96a, Sha97, LC94].

Authentication [ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94k, AS96, Atk95a, AR98, AC97, BA97, Bak99, Bal99, Bec99, BR97a, BG90, BR94a, BCK96d, BCK96e, BM91a, BGS98, BR91, BBDF97, BGH91, Bi91, BHS99, BWM98, Bie98b, BV98b, Bor96, Bor93a, Bor93c, Boy92, Br98, BAN90, CV93, CGM97b, COZ99, DLF97, DVL92, DV90, DY91f, DvW92, DH90, Dra99, DMB97, DS97d, Dsw95, ECM96, EPR99b, EPR99a, FG98, FHBH97, FL96, GHB90, GLZ99, GL96, Geh94, Geh95, GN94, GM90, Gol90a, GBL94, Gu98b, Gui97, HK97, HA94a, HS94, HL92, HIl97, HJPB97, HP98b, JS98, JSS94, Joe98, Jol94, KR95b, Kau93, KA98a, Koh90, KN93, KC97a, KCCT94a, KCCT94b, Kra94b, Kra95, KBC96, KBC97, Kur94, KK95, KY99, KY92, KS97c, LAB91, LABW92].

Authorisation [Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Mau96a, MAM95, McM96, Mee98, MS95c, MS95d, MWW94, MTTV92, Mor97, Mye94a, Mye97, NPP97, OOG91, OM94, Opp96, POKT94, PS98c, PIWNS99, PSN91, PGV93c, Pre98a, Pre98c, MS95e, RS99b, RRSW97a, RRSW97b, Rog95, SNT93, SN93, ST94, SNT95, SNW98a, SNW98b, SSH93, SS96, SPH99, SA95, SC96a, SC97, Sch94d, Sch99k, Sga90, Sga91b, She97, She95a, Sha96, Sim96b, SVxW91, SW94c, SKAM99, St91b, SL99, TAP90, TA92, Tay95, TNS93, Tun99, Ude98, Van95b, Van93, Wf97, WKHG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92e, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC+98, Ano95g, Ano95o, Ano95x, Ano96v, Ano96x, Ano96y, Ano96-27, Ano97d, Ano97t, Ano97p, Ano97-27, Ano97-43, Ano97-53, Ano98s, Atk93]. authentication [BSNP97, BGR95, BCK98, BCB97, BGH91, BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gua90, HS96b, Hor95, HC95b, HLL+95, HW98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin89a, Low95, MSN97, MF97, Men91, MC96, Nac93, NT94, PS98e, PS98f, PS98h, RS98a, RS98f, Sch99, Sga91a, Sga93, SY96b, Sta99b, Sti91a, Sun98b, Syv93, Tsu92b, Tsu92a, TH99, Ver98b, Web99, WL94, XA98, Xie98, YL97a, YL97b, You97, Zuk98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a].

Automation [Des99a]. Automaton [DGV93, Gys96, ZM98, TCC97, TC99b]. automorphisms [VP96].

Autonomous [CK99, RZ99].

autoscritcher [Des99a, CF92, Cra92]. aux [Bec90].

Available [DD98c, Ano97n, Ano97-32, Ano97-46].

Avalanche [Cus96, CS96c, HT95, O'C94, ZZ95, ZZ95b, YT96]. avant [Blo98a]. AVBPA [BCB97]. Average [DLP93, Kob99]. average-case [AD97, AD99]. Avoided [NMR95].

avoiding [ZW99]. Award [DDJ98b]. Awarded [Eri97a]. Awards [Eri97a].

Aware [BCCD99]. Away [DDJ99].

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

b [Cli97, UU97b, Ano99f, HS90, Lam99].

B-Trees [HS90]. ba [IPNd99]. Babbage [Fra93, KT99]. Back [GC97, GO96c, WSFC99, IE97e, WG97].

Backup [Mah96]. backwards [BKR98a, BKR98b]. Bacon [Lea90].


Balkanizes [Mad99a]. Ballot [CFS96, BT94]. Ballots [Sal91].

Baltimore [ACM90, Ano96a, NIS92, USE92b]. Ban [Gar97a, BP98f, XZZ97]. BAN-like [ZXX97].

Bandwidth [Bla96a, Bla96b, JMP98, MM92b, Sim98b]. Bandwidth-Efficient [JMP98]. Banking [Ch92, Ano98k].

Barbara [Bri92, Bri93, Cop95b, Cop95d, Des94b, IEE97b, IE97a, IE98b, Kal97c, Kob96, Kra98, St93b, St94, W99]. Bargaining [Nur94]. Barrier [BGK99]. Barriers [Des92, RCM99]. base [SPP98]. Based [AW94, ADEDS99, BDP99, BG90, BJ97, BS99b, BS99c, Ben99, BLM94, BBT94, BMT96, Bie98, BPR99, BMS94, BM96b, BM96c, Ble98a, BPRF99, Bol98a, Bol98b, Bra95b, BP97c, CC99b, CJS91, Cre97, DGV93, Dae95, Dan95, DDM98, DSS95, D98, DDP90, DMP98, DDGM97, DQ94, Dem94, DF99, EKLM99, EN98, EK99, FCH99, FBS97, FK99, FMY98, FJ91, FS98, FR95d, GKR97, GKR99, GRB99, GN95c, Gys96, He97, HPS98, HJPT98a, J97, Jia99, JZ94, JJ99a, KK97, Ka98e, KR98, Kim93, KG95, KP96a, KP97, KM99b, KA99, KMOV91, Kra94b, KH98b, LM93a, LM93b, LHY93, LL97a, Len99a, L91, LN98, MNS97, MD99, MR95a, Mau93a, MM96a, MM99b, MM99c, MG91, MM98a, Mue99, MM98b, Mill99, NMR95, NM99, NOY93, NS98a, Nsc96].

Based [NS97b, NMV98, OMV98, OO93, OFF93, vO91a, P99d, Pen96, PL94, PR92, Po99, PB99a, PV98, PK99, Pre97a, PMP99, RSA99b, Ros98a, SSS98, SCT99, SC96a, SPS97, SE96, SJ98, Sh96, Sho96, SM91, ST91, SS99, SKT99, ST99a, Var99b, WCS95, WD99b, WS99, Y94, YY97b, ZL99, vO91b, Ala9a, AW95, Ale98, APS92, Ano98k, BSN96a, BSN96b, BSN97, BDJ97, BBC98, BSB97, BCD98, Bea97a, BB90, BCB97, BMP97a, BBL95, BFKL94, BCCG99, CC99a, CPS95, Cha95a, CW97, CS97c, CHH98, CLL90, CD95, Cus95, DD95, FS94, FGY96b, FGY96a, GM91, GH99, GK95a, HZ93, HY93b, Has99, HSW96, He92, H97, HLM93, HX94, HMP95, HW98a, HJPT98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JJ95, JG95, JG90, JY98, KM99a, KSL92, KM99d, Koy95].

based [Kuc92, KH97, KK96, LRW93, LvdLB96, LS98a, LHW99, LZ90, LCL95, MRS99, MS98a, MLA91, Mau91b, MC92, MZ98, MM95, MNT97, Mu92, MZ98, NS97c, NR95, OP99, U99b, Ole95, Pat91b, Pat91a, PS97, PC98, PGCS96, PBBC97,
Fra99, Hir97, Hir98, Don98, Hin93.

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

Broadcasting [CW91a, CY98, LC96b, CC95, HLLC96, LHW99, WY93, LC96c].

broke [Dav98a]. Broken [CP91, Mey99, MLLG95].

Brother [Wai95, Hof95, Des96a]. Brothers [Hat96].

Browser [GW96, Law98, She96b]. Browsers [DDK98]. Browsing [GGMM97].

Brute [CD98c]. BSA [Bar97]. Bucket [Rog95].

Budget [UU97a]. buffer [Mei98].

Bug [DDJ98c, Ano98t]. Builder [Pin98].

Building [HWKS98a, HWKS98b, Hat96, Hof95, MAM95, NT99, Wai95, Yor96, Zol93, FB97, NIS92, PvO95, Tas98]. Bulk [SVBJ96, Whe94]. Bulk-FFT [SVBJ96].


bureaucracy [Rat96]. burglars [Way95].


Bused [FVEA99]. Business [Ano93i, Ano96-29, Ano96-30, Ano97-33, Ano98t, AMP94, Av0h, CFK+91, GC97, Li94, MB90a, SM99, Uni98j, ZKL98, B+b96a, Kir95, Uni98k]. Businesses [MB99a].

butting [Sto98]. buyers [MB99a]. Byte [Mas94, PV98, YLC98a, YLC98b, CFK+91]. Byte-Oriented [Mas94, YLC98a, YLC98b]. Bytes [Yuv97]. Byzantine [Bea92, Bor95].

C [Sha99a, vdWS97, vS97, Bak92, Bas98, BMS99, DSB99, Gar98b, He98b, Kal92, MGL+98, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. C0YNTHIA [WBBL99].

C2 [Ste92]. CA [RD99a, Cop95b, IE93a, IE98c, SJ97, USE93, USE96g, USE96b, WI99]. Caching [STSW99]. Cactus [Ano97-33]. CADE [HB99]. CADE-16 [HB99]. cAESar [Koe99]. Calculating [CFK+91].

Calculation [HRV99]. Calculators [CWM+91]. Calculus [ABLP93, AG97b, AG97c, AG97a, RS99c].

California [ACM93b, ACM98a, Ano97a, Bri92, Bri93, Com96, Cop95d, Des94b, FJV97, IE92c, IE93b, IE94d, IE95b, IE97b, IE97j, IE97i, IE98a, IE98b, IE984, Kal97c, Kob96, Kra98, Nat98, RP97b, Sti93b, Sti94, USE92a, USE96e, USE96f, USE96d, USE96f, USE99d, Wie99, van96, Sch98b].

Call [VCF+90, Zav99, Mlo90]. Call-Coverage [Zav99]. called [Way95].

Cambridge [And94a, And96c, CFK+91, Chr99b, Gol96d, Lom97, RBC99, Sch94j].

came [Fro96]. Camera [Fri93, SKWH96].

Campbell [CFK+91]. Campbell-Kelly [CFK+91]. Campus [VNW94]. Can [Ano93c, BF99a, CP91, Cha93, CD98b, CMY97, DY91f, Ev91H, GSV99, NMVR95a, NMVR95b, NMR95, Rev98b, Sim98c, Ste95, BGV97a, CG05, Ev92, Ev93, LF97, NOV93, Sch91b, Ude98, Way95].

Canada [ACM94c, CFG96, GS94b, HA00, IE94f, IE96d, TM99, Yua92, Roh98b, Tai98].


capability [BC96a]. Capacity [BI99, FVEA99, Gar97a, Gar98b, MM92a, NNE97, VNW95, Uni96a].

Capstone [Y996]. carcinogenic [SBTV99]. Card [Bov98a, Bov98b, Chr99a, DV96, EN98, ENK99, Gar97a, GPVS98, HP98a, Hru96, HH99, Hus99, Kra99, Mar98a, Omu90, SGP98, Sut99, T+99, dWQ91b, dWQ91a, dWQ91c].
changeable [HYLT99]. changing [MW98a].
Channel [AO96, AVPN96, ADEDS99, BI99, Bro94, KSWH98a, KSWH98b, KSWH98c, MM99a, MM99b, OKST99, WB92, BM95, FC94, PSB97, P965]. Channels
[BD1996, Cre97, Des96a, vD97, KI97, Lip94, MM96a, MK94, MM94, PN92, SI94, Sch94e, Sim93, Sim96a, Sim97, VNW95, WD99a, Des96b, Gra98, Man91c, SI93b, Sch93b, Sim94e, Sim98a, Sim98b, Tod97, YL97a].


chi [XTmW94]. chi02 [HG97a]. Chicago [USE96a, USE99c]. chieh [XTmW94]. chin [XTmW94]. China [HOQ97, OiDP98, XTmW94].


Choice [Cha99a, Way98]. Choices [Hon98, Van95a, Wel95]. Chor [BFS98, SH95a, SH95b, Van98a, Van98c]. Chosen [Ble98a, CG99, CS99b, Dam91b, GC94, KSW98a, KSW98b, LL94a, PGBV90, RS91, ZS93, BJ97, CP94, NY90, SNT95, Sah99, SG98, Tze99, vT93].

chosen-ciphertext [Sah99].

chosen-message [SNT95]. chosen-plaintext [vT93].

chronicle [UFC94]. chronology [Kah98a].

Chua [YWC97]. Chump [Wa99b]. Chung [XTmW94]. Chung-kuo [XTmW94].

Church [Ole95]. CINDI [DSSZ99]. Cipher [Alv98c, AM97, ABK98a, ABK98c, KR94, BAK98, BD94, Boy90, BCA98, Car97b, Cla97, Cla98a, CJM95, DGV94a, Dae95, DK97b, DK97a, DW94, EM93, Gol97d, KR94a, KMA98, Kn98c, KR99a, Kuhl98, Lim98, LS97, Lip99, Luc98a, Luc99a, Luc99b, MNSV97, MD98, Mat94b, MT99a, Maul91d, Mil96a, Miy91, MSK98, MSK99b, PA98a, QG90, RDP98, RRSY98, Ros98a, SZ96, Sch94b, SK96c, SK96d, SKW98b, SKW98c, SKW98f, Sch98i, Sch98j, She94b, SMK98a, Van98d, WBDY98, Yi96, YL98, YL98a, YL98b, ZYW91].

China [HOQ97, OiDP98, XTmW94].


Choice [Cha99a, Way98]. Choices [Hon98, Van95a, Wel95]. Chor [BFS98, SH95a, SH95b, Van98a, Van98c]. Chosen [Ble98a, CG99, CS99b, Dam91b, GC94, KSW98a, KSW98b, LL94a, PGBV90, RS91, ZS93, BJ97, CP94, NY90, SNT95, Sah99, SG98, Tze99, vT93].

chosen-ciphertext [Sah99].

chosen-message [SNT95]. chosen-plaintext [vT93].

chronicle [UFC94]. chronology [Kah98a].

Chua [YWC97]. Chump [Wa99b]. Chung [XTmW94]. Chung-kuo [XTmW94].

Church [Ole95]. CINDI [DSSZ99]. Cipher [Alv98c, AM97, ABK98a, ABK98c, KR94, BAK98, BD94, Boy90, BCA98, Car97b, Cla97, Cla98a, CJM95, DGV94a, Dae95, DK97b, DK97a, DW94, EM93, Gol97d, KR94a, KMA98, Kn98c, KR99a, Kuhl98, Lim98, LS97, Lip99, Luc98a, Luc99a, Luc99b, MNSV97, MD98, Mat94b, MT99a, Maul91d, Mil96a, Miy91, MSK98, MSK99b, PA98a, QG90, RDP98, RRSY98, Ros98a, SZ96, Sch94b, SK96c, SK96d, SKW98b, SKW98c, SKW98f, Sch98i, Sch98j, She94b, SMK98a, Van98d, WBDY98, Yi96, YL98, YL98a, YL98b, ZYW91].

China [HOQ97, OiDP98, XTmW94].
Ciphers
[Ada97a, ABDV98, AAG99, BR99a, BR99b, BDR96, CD98, Cha94a, CS91, Cle91, DR99a, De99, Din94, Fi95, Gus96, JK97, Jak98, JJ99b, KSWH98a, KSWH98b, KSWH98c, Km94b, Km94a, KP96a, Km98b, Km99b, Kol99, LMM91, LM93a, LM93b, Lu96a, Lu96b, Mat96a, Mau91a, MS91, MT99c, PRS99, Pat99, PK95a, PK95b, Pen96, Pra96, Pre97a, Ree98, RP97a, Rob95a, Rob95b, Roe94, She94a, She94d, SM91, Van98b, Van99, YY89d, YY98b, ZM90, Zhe90, Abe98b, BKR98a, BKR98b, CD98a, Cou99, DGV94b, DXS91, FSN93, Gar96a, Gar97d, GSN94, Gol95b, Har96a, HLM93, HXM94, HSW94, Jak99a, JV98a, Lai92, LMM92, LRU93, Ny95b, PGV93b, PGV94, Rev91, RP95b, Roe95, SB95, SAM97, Tay94, Win93, Wri98b].

Ciphertext
[BK98d, Ble98a, CG99, CD97, CS98b, Dam91b, LL94a, MRS99, Miy93c, RS91, Riv93a, TOU94, ZS93, CP94, NY90, Sah99, SG98, Vu95].

Ciphertext-Only
[BK98d].

ciphertexts
[Des95].

circuits
[KT91b, KT98, WG99, JS93a, LMS97, YWC97].

circling
[Ano96-29].

Cirencester
[Boy95a, Boy95b, Dar97, Far93, Wal99a].

Cisco
[Sav96].

CISSF
[AA97].

City
[IEE99a, USE95b].

Claim
[GO96c].

Claims
[DS97a].

clandestine
[Wri98b].

Clara
[USE93].

Class
[vD97, Ou99, Uni96b, FR94, HWB93, KSB96a, LZ90, LZ91a, Zuk94, vT94].

Classes
[Haw98b, Paw9d, Haw98a, Sze98].

Classical
[Bra94a, MC92, Nic98a, Nic98b, CD98a, Mas99a].

Classification
[BD90, LSVV95, PNFK95, Uni96b].

Classifier
[CIBM99].

Claude
[Hor92].

Claw
[BHT98].

Claw-Free
[BHT98].

clearly
[Los98].

Click
[WSFC99, Ken95].

Client
[DL99, Kon95, Oh99, SL99, GGK99, Sin95].

client-relationships
[GGK99].

Client-Server
[DL99, Oh99, Sin95].

Client/Server
[Kon95].

clients
[AG95, Bee96].

Climate
[MGK99].

Climbing
[MCD99].

Clipper
[ Pri94, Fro96, Ban96, Bro96, Buc95a, Hof93, Kan96, MS95f, RKD94, Smi94a, Uni95a].

Clipper-like
[MS95f].

Clipping
[Hof93].

cliques
[JP96].

Cloak
[Gre90].

Clock
[DHH95, GO96b, Gal94, CS96b, CS97b, GM91, GO95, Men95b].

Clock-Controlled
[GO96b, GM91, GO95].

Clocks
[DG95, DGT96, Yab94, Gon92].

Closer
[Coh96].

Closure
[MOM91, PS93a].

Clueless
[RS98c, RS98d].

Clustering
[DD98a, HE98, Kum97].

CM
[CNST98, Kob91a].

CM-curves
[Kob91a].

CMOS
[BS95c, ECD99, YS99].

Co
[Gla99b, LFCK99, Sut99, NM96a].

Co-dimension
[LFCK99].

Co-operation
[Gla99b].

Co-Processor
[Sut99].

co-processors
[NM96a].

Co.
[CFK91].

Coast
[SZ93].

COBOL
[Gar97c].

code
[CJ99, HR90, JJ99a, Kip99a, Kur94, Mv93, PV98, QD91, Sch94g, Sch96a, Sch94h, Str95, Tod97, WK97, WF94, Zim95b, Ala97, Ano97l, BSNP97, CC98, CL98, GA98, HM97b, LJVW97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG99, Mea98].

Code-Breaking
[QD91].

code-cracking
[W96c].

Codebreakers
[HS93, Kah96b, Sni98b, Yu99].

Codebreaking
[Car97c, Car98, Dre92, Sch98a].

coded
[HG97e].

codemaker
[Mar98b].

CODER
[Sto90].

Codes
[ACM94b, AW94, AR98, BS96, BVFD99, CCZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, Goh91, Hof99, Joh94, JS95b, JJ99b, KKS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWNSN99, Pen96, Pre98a, RV99, Rus93a, SN93, SN98a, SN98b, SD99, Sga90, Sga91b, SB94, SVxW91, Sta96b, Sti91b, Ton96, Van95b, Wri98b, Ada91, Ala93a, AW95].
Commutative
[MB99a].

compact
[Ort95b, Ort95a].

Companies
[Ano97j, Ano97y].

Company
[GC97, Ano96g, Kar96].

Comparative
[Dac99, Ste92, AA99, Don98, She92g].

Comparing
[Bih99c, HSSI99, HKL94, KAK96, NM96b].

Comparison
[BALS99, Cus97, KH98, LM98b, Mas99a, May97, MG91, vO91a, QN98a, SKW^+99a, SKW^+99b, Wie98b, Wil93b, vO91b, GM91, Yeu99, ZH93, vO92].

Comparisons
[Fol99, SKW^+99c].

Compartmented
[GPSN98].

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, DSV99, GM99b, HKL94, HMS99, MMT90, MS94, MMM^*98, M99a, M99b, NMVR95a, NMVR95b, NOVV93, Sch99, Smi98a, Bao94, CS97d, DDP94b, F9K3b, GZ91, GN95a, Go97c, Hi94, MM90a, MS98a, MK92, Sh99b, SMK98b, Sze98].

Compliance
[Da96].

complies
[Ano96u].

Component
[NK98b].

Composite
[Pai99d, BBR99].

Composition
[ABDV98, GK96].

Compositional
[DJHP98, HJTW99, MM99a, Zwi98].

Comprehension
[MT95].

Comprehensiveness
[MT95].

Comprehensive
[SSP90].

Compress
[Ano96e, Dob97, Dob95a].

compressed
[CPO^+98, CHO^+98, HG96, HG97c, HG98].

Compressing
[G199].

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

Compromise
[Gar97c, Ano97u, Hed97].

CompuServe
[GC97].

computability
[BK98f].

Computable
[DSV99].

Computation
[BM99a, BM99b, CH98, Cra99, FH99, FH94, GM93b, HHT93, HHT97, HCY96a, KR94c, LO91a, LY93, LL95a, Mon93, Mor98, PK95a, PK95b, SN98a, Wat91, ARR99, Ata99, BH9R95, BM94c, CL97a, GM95, Hor98, LY93, MI97, PW93a, Sh99a, Xie92].

Computational
[CH96, HKL94, KRS99, PG90, Sab94, T9K99, BC95a, Ger99b, Mc90b, P90a, SS95a].

Computationally
[WP90].

Computations
[Cha90, C99+99, Mas91].

computed
[Ev92, EvH93].

Computer
[AC93a, ACM94a, ACM97a, Ano93d, Ano97-50, Ano98c, Bac95, BK90, Ber96b, Bre99, CWM^*91, CO98, De 98a, De 93b, De 98c, DQ93, De92, DEQ92, FJM^*96, GM98, HM91, HM92, HM95, Hig97a, Hig97b, Hor94, IEE92a, IEE92b, IEE92c, IEE93b, IEE93c, IEE94b, IEE94c, IEE94d, IEE94f, IEE96a, IEE96c, IEE97b, IEE97f, IEE98a, IEE99a, KT99, KK99b, LBMC94, LC95, MDP94, NIS92, Nae97, Net92, OD99, PG99d, Q^98, Sa91, SSS98, SK96a, SK99, Sho97, Ste91, SI93, V9P93, Ver98a, VG99, Wh90, AFB95, Ano93k, AC97, Bur98a, Car97c, Car98, CW91a, C9H94, GBL94, Gr98, HLC96, IEE92d, IEE95c, Joh98, LS98a, LFS94, LC96b, LC96c, Mat98, NT94, N91, PR98, Riv98c, Shp99a, UFC94, Wil93a, Woe97, W909].

Computer-Related
[De 93b, De 98c].

Computerized
[IE91].

Computers
[???97, BF99a, CWM^*91, H96, Kan96, Sch98c, C9K^*91].

Computing
[AC90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98a, ACM98b, ACM99b, BA92, BD999, BV96, Bra94a, C9F^*91, D9J984, D9J98b, D9J99, Dwo95, F99, GC98, GN95b, IEE94e, IEE96b, J99b, Kon95, Law98, MMM^*98, Mau94, MW99, NS98a, Pen96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b,
BGT96, CWM+91, DiDPS96, FM91, FJV97, HK99b, HC95a, KG93a, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK+91, PH91.


condition [Sta96b]. Conditional [DOR99, GK99a, KS97a, KG99]. conditionally [Des90b]. Conditions [GS99a, Rus93b, Gua99]. Conducts [Law98]. Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95r, Ano96r, Ano96a, ??97, Ano97f, Ano97g, Ano97a, Ano98b, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BS95e, CH96, Cha91, Cop95d, DDJ98a, Dan96, ES98, Far93, Fra99, Fun97, GNF95b, GQ95, Hir97, Hir98, IE99a, IE99a, IE99b, IE99c, IE99d, IE99e, IE99f, IE99g, IE99h, IE99i, IE99j, II97, IE97h, IE97i, IE97j, IE98c, IE98f, IE98e, IERM93, KG96, Kat97, KM96a, Kra98, LOX99, LP99, Mau96b, MSD90, NIS92, Nat98, Nat99b, Nyb98, OW95, OdF98, PSN95b, QG95, RD99a, RD99b, Sch94m, SJ97, SK93, St93b, St94, T+98, USE91, USE92a, USE94, USE95a, USE96a, USE99b, USE99d, Wal99a, Yu92, ACM99c, Ano93d, Boy95b, BD95b, Cop95b, Dar97, DG96, Des94b, HQ97, HI97, IE992d, IE95c, IE96f].

conference [IEE98b, Kal97c, KG93, Kob96, LM98a, SP90, Ste99b, USE96f, USE98c, USE98d, VPM97, Wie99, Ano95f]. Conferences [BDHK93, MZ98, Sch95f]. Conferenceing [Ano99f, KBRS97, WW98a, Lam99]. confidence [Chi99a, Chi99b, Graxx].

confident [Jan95]. Confidential [Bet95b, Bet95a, vD97]. Confidentiality [Ano98t, Jac96, Riv98d, ZG96, FT95, MI90]. Configurable [VMS97b, VMS97a]. configuration [HI97]. Confirmer [Oka94, Cha95b, MS98b]. conflict [All97]. Conflicts [ACM94b]. confounder [BTD98]. confrontation [Za97]. confused [LL98b].

Confusion [GC97]. Cong [Mye98]. Congress [Uni97a, Uni98c, Uni98d, Uni99e, Uni99c, Uni97b, Uni98f, Uni97c, Uni98d, Uni98e, Uni95a, Uni95k, Mad97]. Congressional [Sm97a, Mad96, UU97a]. congruence [Sch91a]. Congruential [Kra90]. conic [Cao99, Mra95]. Conjecture [Ja99, GHS93, Il94]. Conjectures [KP95].

Connect [Lic94]. Connection [Kas96, CV99]. Connections [RSG98, SGR97, Yu94a, Yu94h].

Connectivity [Pit96b]. Consequences [KP95, Sim94a]. Conservation [Bro94]. Considerations [Cra96, Hub91, Mos98, Bas95, Bou94, SY99, Bou94].

Considered [LT91]. Considering [HH94]. Considers [Ano95p]. consistency [ZY99].

consortium [Buc95a]. Conspiracy [WK97, Scu92]. constitution [Mad98b].


Constraint-Based [WS99]. Constraints [DS98b, Oo99, Koz96].

construct [Lon92, Sun91a, ZI98]. Constructed [Rus93a].

Constructing [Ada97a, AB99a, AB99b, DT93, Gal99, KTM+99, Kob91b, XL98, ZZ96].

Construction [BCK96c, BR99a, BR99b, CNST98, vD95a, DS99b, EM93, GPSNW98, Joh94, Kim93, KYDB98, NR98, BCK96c, BCK96b, BCK96c, B193, MPL99, OS91, OS92, Pet91, vD95b].
Constructions [AHV98, ABDS96, KRS99, SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE98c]. consumers [Weh99]. contactless [DS98a]. contain [Lea90]. Contemporary [Knu99b, Sim92].
Content [Ack98, JPLI99, KR98, MW98b, MR95b, PMP99, Ros93, SC96a, Way93a, SNT95].
Content-Addressable [Way93a]. Content-Based [PMP99]. Content-MD5 [MR95b, Ros93]. Contents [vHH97].
Contract [KE97]. Continues [Ano97-44, Ano97-45, Ano98q, DDJ98d, Ano96-29, Mad99b].
Continuous [BP95a, NHB98, She95a]. Convolutional [Cha99c, JJ99b, TY94]. Cool [Ano99c].
Correcting [AW94, AR98, BGS96, DLR97, KKS97, LC99, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, Ste95, Wan92a, YL97a, V94].
Correction [Ano96f, Cha99c, MG91, WN98a, WL92c, Ala93a, WL92a]. Correctness [FHM98, Gai90]. Correlation [CS91, HT99, JJ99a, JJ99b, KSB96a, MS91, PK95a, PK95b, Pen96, GO95, Har91, Mat95, SGSD99]. Corresponding [Oka93b].
Counteract [CJRR99a]. Counterfeit [ENK99, Ano93a, van96].
counterintelligence [Mon96]. Countess [KT99]. Counting [Kö96, MV93, KK98, SF97]. Countries [Gar97a]. County [IEE96c, IEE96f]. Course
court

Coverage

Crack

Cracked

Cracker

Cracking

creation

creator

CREDIBILITY

CITATION

CRYPTOGRAPHY

CRYPTANALYSIS
Bra98, Bri98, CP91, CRS98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a,
Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, Sti98a, Wil98b]. Crypto-Chip
[HMV’T94]. Crypto-Coprocessors [HP98a]. Crypto-Engine [BE90]. Crypto’91
[DBGV93]. Crypto’95 [NS98a, NS98b]. CryptoAPI [Boy98]. CryptoBytes
[Cry95, Riv95e]. cryptochip [PP96]. cryptograms [Har94, Web93].
Cryptographers [WP90]. Cryptographic
[AG98a, AG98b, IBM93, Ano96i, Ano98f, Ano98e, Ano98h, AB97, BDPNSN95,
BDPSN99, BH93, B93a, BGM97a, BGM97b, BBT94, BMT96, BFKL94, Bol98a,
Bol98b, BDL97, BD97, Bra95a, Bra96, BD91, CS96a, CJ98a, CJR98b, CPOR97,
CF95, CD99, Cop94b, Cre97, DGV92, DC98a, Dam90a, Dam91a, Dan95, DIF94,
DY90, DY91a, DY91d, DY91b, De 95, DS97a, DF91c, DK91, ECD+99, Ell98,
FGR92, F98, FG96a, Fum97, GI99, GS94a, GK99a, Gol96c, GS97, GQ95, Gut99,
HHT93, HHT97, Hel94, Hwa97, I96, I96, J91, JDK91, JD91, KN98a, Kal98f, Kal98d,
KV94, KSF99, Kh93, KP99a, KT91b, KT98, K97b, LMJ93, LL97a, LHB96,
LM96, Mac94, MM99a, Man96b, Man97b, MS90a, M96b, Mij98, Mus91, Mun91a,
Mun91b, NM96b, Ng99, NS99b, NR94].
Cryptographic
[NK98b, Nur94, Nys99, ‘OPH+99, Oka93a, OS98, PS99d, PV97, PS99b, PW98, PB98, PB99a,
Pre93a, PV93a, Pre93b, Pre94a, PB97, PR98b, Pre98c, PR98a, Pre99, Pre94b,
QV90, QG95, RSA93d, RS93, Ritxx, Rue93, SI94, SZ96, Sak96, ‘DY91c, Sch95f, SK96a,
Sch94d, SK98a, Sch91c, Sch93f, SPS97, SZ93, SZZ95c, Sha99a, She92d, SBY99, Sm90,
SY92, SM91, Ste96, Sy92, T+99, Tou91, Tou93, TY996, VCF+90, V98, Wai95,
YS99, YY97c, YY98a, ZZ95, ZM991, AN91, AN94, AN96, AG97b, AG97c, AG97a, Ano97-32,
Ano98g, BD92, Bol97, BV97, Com94c, CD95, CI99, DD95, Dan97, Dhe98, Di 99,
DFHR91, Don98, GY96b, Fro96, FL93, Gol96a, GEL98, Han95, Han97, Han99,
Har91, Hof95, IS99, Jen90, JW01, JP96, KS90, Kob91a, LRW93, Lai95, Lea90].
cryptographic
[Lev91, LL93b, Lub96, Mau91c, Mea95, Mol98, M92, IPNdbsbprm91, NT93, Nyb98,
Pau98, PKM97, Ros97c, Sch93g, SZZ94a, SZZ95b, Ste99b, Way98, WN94, XZZ97,
XZZ98, YS91, ZII97, ZXZ99].
Cryptographic-Token [Nys99].
Cryptographical [KP95, GvP98].
Cryptographically [BD98, Cha90, CvHP91, Hi94, PG92, ZZ96, DT93, IS97, KSB96a, MCD98b, SKB97, Bou94].
Cryptographically-secure [Bou94].
cryptohraphique [Bou94].
Cryptography
[ANS97, AN98s, Ano97k, Ano99k, AA93, AB966, Avo98, BCE+94, BGGG94, BGGG95,
BG98a, Bel98, BB+91, BBE92, Bir98, Bla93, BK95d, BL96b, BL96a, BGV93,
Boy95a, Bra90a, Bra94a, Bus97, Cae96b, DD99, DL96, DP98a, DP98b, Dav91,
Dav96, DG96, De 93c, Des94a, DHQ98a,
DHQ98b, Des98c, Dif90, DND91a, Dro96,
Dwo97, E99, Eri99, Fer99b, Fis97, FBS97,
FJM+96, FJRS96, FGPL96a, FGPL96b,
Gan93, Gem97, Gol95a, Gol97a, Gol97b,
Gon98, HK99a, PH98a, HSSI99, Hat96,
Hed97, HL93b, Hir98, HAH94, HKS97a,
HKS97b, Hr95a, Hru96, Hru98, HLM96,
HH98, HBLK99, JR96, JM97, Kal97a, Kal98e,
KS98a, Kal99, KSS+92, Kn98a, Kob94,
KA91, RSA93f, Lac93, LM94b, Lin96a, Los97,
Mad98b, My91, Mau99a, Mau99b, Mau97c,
Mc96, MP91, Mit92b, MKS99, NC97].
Cryptography
[Ni98a, Nic98b, PKA+98, Pat96, P95,
PT95, PGCSN96, Por91, PB99a, RSA99b,
Rad97, R94, R94, Riv90b, Riv93b,
Riv97b, Ros96d, RK99, Sal99, DP91, Sas99a,
SKBxx, SSS98, Sch94g, Sch96a, Sch96b,
Sch97a, Sch97b, Ssv+98, Sch98f, Sch94h, SV93, SG96a, She93a, She93b, She93d, Sni94b, Smi97b, Sta99a, SW95b, Ste91, Sti95, Sti98b, Sur99, Swi97a, TN96a, TN96b, Tv92, Tow98, Tsu92c, Wad98, Way96a, Wol99, Wol93b, Wor96, WC97, YWC97, YST99a, YY96, YY97a, YST99b, ZYWR91, Zim98, dRHG +99, Uni96b, AA95, Acc97, Ada92a, Ada91, Alv98a, Ano97-29, Ano97-52, ASM98, BH98, Ban94, Bea97a, BR96b, BFS92a, BFS92b, BHHR99, BW97, BMP+97b, BSS99, BBS98b, BD98b, BC96b, Buc95b, Com96, Coh99, Cou99, Dan96, DDB95a, DDB95b, DvQ96, DvPS96, DNN91b, DN95b, Eng99, Far93].

cryptography [FM91, FK93b, Fra99, Fra93, Fri96, Gar96b, GZ91, Gen99c, Gol99a, Gol97c, Gre94, GTGW94, HA00, Hir97, Hru95b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdL98, Luc95, MB94h, Mat98, Mau93b, MY98, Mei96b, MVV97, Mic97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Nyb94, Org98a, Od94b, Par96, PG97a, PG97b, PC98, PP92b, PV93d, PR98, Riv98c, Rot95a, Sal90, Sal96, Sch92c, SSM+97, SMD+99, Sch99e, Sch90c, Sch97c, SPP98, Sph99a, Sph99b, Sin99, Siu99, Sh98, SMS90, Sta96d, Ste98a, Tas98, TM99, USE96c, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wa99a, vS97, Sha99a].

cryptography-dedicated [NM96b].

Cryptography-in-the-Large [Bla93].

Cryptoki [Ano96-28].

CryptoLib [Luc93].

Cryptologia [Ers99, DKK+98, Joh98].

cryptologic [RK98b].

Cryptologie [Bra93b, Bec90, Sch98e].

Cryptologist [Pin98, Sei94].

Cryptography [Ano93g, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dan90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ano97-37, Bau97, Bec88, CW94, Cop95b, Cop95d, Dam91a, Dam99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, Hel94, IRM93, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mau96b, Mc97b, Mei92, MV91, New97, Nyb98, OiDP98, PSN95b, QV90, QG95, Rat96, Rue93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Uni95b, Web93, Wie99, Wil98a].

cryptography [Bec97].

CRYPTON [DBR+99, Lim98, Lim99].

Cryptography-dedicated [NM96b].

Cryptography-in-the-Large [Bla93].

Cryptoki [Ano96-28].

Cryptoplast [Hag98].

cryptos [Hag98].

cryptos [Hag98].

cryptos [Hag98].

Cryptosystem [AM90, BI95, BDGI98, Ber97c, Bih91, BMS94, Ble97, Bon99, BM97, CC99b, CC99, CJS91, CS98b, CW91b, Cus97, Gih91, Gih96, GC91, GC94, GG97a, Gys96, HD96b, HPS98, HJP98b, Hwa91, Jha90, JS93b, Kie98, KS99c, KT91a, LR96, Lan97, LCL92, MM96b, NMR95, NS97a, NK98a, NS97b, NS98d, NS99a, Ngu99a, Ngu99b, OU98a, SG99a, ST91, Sun98a, Tak98a, Tak98b, van98a, Vau98c, Wal99c, Wan92a, WY93, Yam99, AM93, AD97, AD99, Aia97, AAPS92, ACBR90, Ba94, BI94, BSB97, Boy97, BCC99g, CC99a, CS98a, CC98, CW91a, CW97, CS97c, CCH98, Cie96, CS97d, DWZ96, Gen99b, Gil95, Gro94, HNSM91, HY93b, He92, HFW96, HJP98a, HLLC96, IK98, Jon90, JQ98b, KASH90, KSR96, KM99d, KK96, LG97, LS92, LC96b, LC96c, Lon91, MMT90, MM90a, MM90b, MI90].

cryptosystem [Mau91b, Miy90, NS97c, NS98e, OU98b, Ole95, Ped91c, Pet91, Roe99, SW95a, SH95a, SH95b, SM90, SS95b, SS95c, SX90, TY92, Tan90, TCC97, TC97, TC99b, TC99a, Ven92, Wan92b, Wri98a, Wu92, XLP99, XW97, Yu92, Ze96b, Zha91, vT90, Ano96j].

Cryptosystems
cryptosystems

CS-cipher

CSP

CTS


D [Ben99, BALS99, CK95, Nas94, TK99, Wor96, YY99a]. D.E.S. [Cle91]. D.S.A. [NMVR95a, NMVR95b]. Dabbling [Ritxx].
DAEs [JV98b]. Dallas [ACM98b, USE91].

Daníel [DG94]. Daníel’s [Gib90]. dan [IPNdbbprm91]. Dark [YY96]. DASS [Kan93]. Data [Ada92a, All97, Ano92c, Nat93b, Ano95f, Ano96c, Ano97e, Ano97f, Ano97g, Ano97a, Ano97-40, Ano97-42, Ano98b, Ano99f, Ano99a, AVV99, BGL96, BRS99, Ber98, BS95b, BS98, BY92, BW98, BKZ98, Cle96, Con99b, CH99b, DC98c, DFGH99, EKL99a, Ga990, Gre90, Gu97, HS96a, Int91b, JML94, Kop97, KH98b, LvdLB96, LT98, MPPS95, MS99, Moc97, Nat93c, Nat93a, NHB98, OA94, Sch99b, Sch94m, See97, Sme97, Sto90, SZ96a, TYD99, Tyl90, TLS99, Way91, WSFC99,
Demultiplexer [SVBJ96]. Deniable [CDNO97]. Denial [Nee94]. Denk [CWM91].

Denmark [Dam90a, Dam91a, Mad92]. dense [Ort95b, Ort95a]. density [CJL92].

denting [Gib95]. Denver [Sch99b].

dependency [MAO96]. Dependent [Con99b, DJL93, FBS98, IOS94, Poi99].

depending [Gon95]. Deployment [Var99b]. Dept [Uni96b].

depth [Mae98]. Derived [OO98]. Deriving [Tou91].


Design-Space [KV99]. Designated [Cha95b, JMSI96, Oka94]. Designed [YY98d, YY98b, Mey97a]. 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].


DEsx [Rog96]. Detail [Zeg93].
DeTeBerkom [GH96]. Detectable [Vv97].

Detectable [Gor93a, Mad92, PM98, SG96b]. Detection
[Bie98].

Detecting [Vv97].

Detection [Gor93a, Mad92, PM98, SG96b]. Detection
[Bie98].

Determining [Vv97].

Development
[Ano97b, Bar99, Bas93, GRB99, HNSS99, IR99, LL93a, Nat99c, Natxx, VDDR99, Way98, You96, AMV93, Ano91-52, LS98a, Mi99, NBD99, Sta97c].

Developmental
[Ran92].

Developments
[Ano95a, PRB98a, Sim97].

Deviates
[Ran01].

Device
[Hru96, Ano91b, CM97c, Uni94b].

Devices
[BDJ98, Ano95t, Hwa92b, Hwa92c, LS98a, Pos92, Pos93, Uni94a].

devoted
[FT99b].

DFC
[KR99a, Ste99c].

DGSA
[FM98b].

DHCP
[Dra99].

DHWM
[ADF98].

Diagnosis
[GX99, MR95a, PW99].

Diagnostics
[Var99b, Lew92].

Diagrams
[Ou99].

Dial
[RRSW97a, RRRS97b].

Diameter
[FP99].

Dickson
[Pie93].

DICTA
[KG93].

DICTA-93
[KG93].

Dictionary
[Jac96, Luc98b, BCR98].

Dictyostelium
[Ram92].

Diego
[ACM93b, IE97b, Sch98b, USE96f].

Difference
[L94].

Different
[KBRS97, Sch99h, RT93].

Differential
[BB94, Ber93, BS90a, BS91c, BS91e, BS91d, BS91f, Bih92, BS93b, BS93a, BS97a, BK98d, BKPS93, C398, Con99b, Dae95, Din94, Fer98, Haw98b, Haw98a, KTM99, Kau96, KM98b, Kob99, KJJ99, Kwa93, LMM91, LH94, Lan95, Mat96a, Miy93c, MSK98, NK93, OM94, Pai99a, Sch96c, SMK98a, VKR98, Wag98a, YL98a, Ada92b, CV95, KY95b, KYx, KM96b, LMM92, O’C95, OG95, RP95b, TN97, Way95, YT95a, YT95b].

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

Differentially
[Nyb94].

Differentials
[BBS99a, Fer99a, KRW99, BBS98a].

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

Diffie
[Ano97a, BY93c, BY93b, BBR99, BWM99a, BV96, Bon98b, Bon98a, CPS97, CS97d, HY98b, HY98a, Kla97a, Koc96, Koc96b, Lat98, Man94, MW96c, MW96b, MW99, RSA93b, Van95a, VW96, WM93, vOW96].

Diffusion
[Mas99b].

Digest
[FHB+97, GTG94, Kla91, Riv92a, Riv92b, Riv90a, Riv91b].

Digit
[TK99].

Digit-Recurrence
[TK99].

Digital
[Ano95, Ano96a, ANS98b, Ack98, ALO98, AW94, AR97, Int91a, NISS94, Ano96f, Ano97-50, ASW98, Aur96, BG90, BM99a, BM99b, BdM94, Ber97b, BM94a, BM96a, BM96b, BM96c, BS95b, BS98, BTH96, Boy97, Boy98, Bra93a, Bf99, BWF99, Car95, CR91, CPO98, CHO98, DADN98, DMD96, E199, EGM90, EGM96, FFW99, Fox98, FKY98, FBS98, Fri93, Fro97, FOM91, Gar97c, Gar98b, GR97, GDD97, GB98, GO96c, GQW91, HKS95, HG96, HG97e, HEG98, HA96, HW97, IEE97c, IEE98d, JLO97, Jue99, KKS97, Kob97, Kob98c, Kra93, KH98a, LQR98, LM95, LW96, LL98a, Lut98, LR98, MS96, Man98, MMST98, MB99a, MW98b, Mer90b, Mer97, MNT97, Mos98, MBW97, Nat91, Nat94a, NH98, NV98, NIS93a, OOO93, Ot96, OFF93, Oko96, Per97, Pet98, Pf96c, PW93b].

Digital
[PG93c, RDK98, dR94b, Rot95b, SC96a, SC96b, SC96c, Sc96c, Sch93c, Sch94d, SK97b, SK97a, She97, She92e, Sim93, SB93, SY98, SH98, VP98, VNP98, VP99, Web98, WD96, WD97, WL99, Woo90, YK98, Ye99, Ye97, Ye98, YHY98, ZK96, ZKOY99, Zhe97b, vHH97, vTO94, AW95, Ano91b, Ano98e, BBPC98a, BHS93, BR96c, BGR98b, BCV97, BO96a, Bis90, BOD95, BS97b, BM91b, Bur98a, Com97, Car97a, CHL98, DD95, DMD98, DSSZ99, FC94, FB97, Gua90, HS91, HZ93, HW98b, Hwa93, Ibb97,
Irw98, KG93, KAK96, KH97, Mar95b, Mau91b, May97, Min97, MBy97, Mu92, NMVR95a, Nat97a, Nor95a, Nor95b, ODB96, OP97, OP98, OP/H99, Pit96a, RRP97, Ros94, RKDB96, Sch90c, Sch97c, SD97, Sin98, SS95b, SS95c, Til98, Wan92a, Wil93b, Wu92, XBA97, XA98, Xie98, YL95b, 


Disenrollment [BBCM93b, BBCM93a, BC96a]. Disk [DIF94, Gar98b]. Diskette [BE90]. Distortion [SVBJ96]. Distributed [ABLP93, Abe99, AD9F98, BHJM99, Bor96, BHKR95, Bur94c, CM98, DHRM96, DF91b, Dwe95, FM91, FK99, FY98a, FY99]. GJKR99, Gre94, GS97, GMV98, KI99, Kau93, Kem99, KRJ98, KYB92, LABW92, Law98, Mar99, MKS99, Muf93, NAA99, NKP99, Ped91a, PKM97, RZ99, Rei92, RG95, Sch94a, SKW96, SS90, She92a, TV94, Whi90, WL92b, Bea92, BP97b, FMY98, HK99b, Har90, LM98a, LABW91, Lie93, MS99c, TCH91, Wad93, WL92a, WL92c, Zim96b, BBN96]. distributed.net [An97o]. Distributing [Bre97b, Rei96]. Distribution [BR94a, BR95b, BDH93, BFS96, Bur94b, DNN98, DPD90, ECM96, Gal96, Max94, MTVZ92, PKOT94, PB99a, SIK93, SR96, YKB94, vHH97, An90e, BGS95a, BMS96, BFS98, Bur94a, BD95b, CFS97, FL93, GBL94, HI97, Hwa92a, Hwa92b, Hwa92c, JLM94, Kha93, LC96a, MY93b, Mu92, PF98e, Pos92, PPP97, SL93b, SY96b, Syv93, SM95b, TH99, VSB95, WM93]. distribution-specific [Kha93]. Divergence [Sga90]. Diversity [Man90]. divertibility [CDP95]. Divertible [BBS98b, BD91, NMV99]. dividers [PV90].
Dividing [MB99a], divisibility [FR94].

Do [AW99, Ber97a, DDJ98e, DDJ98f, HKS95, SS99a, Ber98, Ude98, Way95, ZKOY99].

Dobb [Eri97a, Eri97b, SSM+97, SSv+98, SMD+99].

Document [BLMO94, BLMO95, BO96b, Hei96b, LMOB95, MLM98, Max94, Sea95, Bur98a, HS91, LL98b, van97b].

documentation [Sim95]. Documents [Rot95b, SB97, Bar99, DSSZ99, Rot95a, Sch93e, SHG98].

Dodgson [Lip98].

Does [MGL+98, Mar96, Ril96]. Dollars [Ame96b].

Domain [ADBB99, DVPL92, Gar97a, Gar98b, Mon93, PD99b, Ano97-29, BCP99b, BP98d, HG97e, KMP99, KM98c, NP98b, TK98].

Domains [Bru98, CGM97a, CK90, Mar97].

Donald [CFK+91].

Don't [Hus99, Way96b, Chi99a, Chi99b].

Door [Yu92].

Double [Ano99c, Cha90, HP99a, Pae99b, Bar95, KL95b].

Double-Size [Pae99b].

DoubleTree [Nat98].

Doubly [ABD98].

Doubly-Iterated [ABD98].

Down [GC97, Fox98].

downgrader [McH92].

Downgrading [KM92].

Downloaded [JPL99].

Downloading [Sch97d].

dpe [IPNdbbbrpm91].

Dr. [Eri97a, Eri97b, Gar97d, Riv93a, Riv95a, SSM+97, SSv+98, SMD+99].

Draft [Ano94b, Ano96-28, Ano97b, Got99, Mic93b, An95, Ano96c, Ano95u].

Drawing [EMMN98, HEQL98].

Drawings [BMWR98].

Draws [Way93b].

DREO [Ano99f, Lam99].

Driscoll [Luj98a, Luj98b].

Drive [GC97].

Driven [CHLT99, Ano97-27].

Drives [DDJ98a, DIF94].

Dromquinna [IEE96c].

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

DS5002FP [Kuh98].

DSAP [IEE97c].

DSAPS [DK91].

DSP [Burr95, Koc95, Koc96b, Nat94e].

DTR [Ano93k].

DTR-1 [Ano93k].

DTS [BH95].

Dual [Jas96, LL99, FBT96].

Dual-workfactor [Jas96].

Duality [Z95, ZM91].

Dublin [IEE97a].

Duel [Got99].

Dumps [Mei98].

Dumps during [Dou98, Joh95, Rat96, Wil98a].

Dutch [PL96].

DVD [GC97, LT98].

DVD-Video [LT98].

Dwork [GGH97a, NS98d, NS98e].

DYANA [BKS99].

dyes [SBTV99].

Dynamic [AGY95a, AGY95b, Ano97-33, BDHK93, Da98, DP99, DHSS95, FT99a, FY99, FR95d, Gui7, NT99, SG99b, SP99, WWH95, BH93, BCV94, BH95, BCV96, CT99b, HC96, Pos98, SS94].

Dynamic-Resharing [AGY95b].

Dynamical [PS96b, RO96].

Dynamics [Ohi99].

E-Cash [DFTY97, Yac99a, Yac99b].

E-commerce [Ano98h, VM96, DDJ98d, Jak99b, Lut98, Gar97].

E-Mail [Ano93j, Ano95c, LF97, Ril96, Bac95, Sta94a, Got99, RS89b, Sch95c, Sch95d, SH97, Gar97b, Str93a, Str93b].

e-safe [B97].

E.I.S.S. [BFS92a, BFS92b].

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

E2 [KMA+98, Kob99, MT99a].

EAP [BV98b].

early [Alv98c, Mar96].

Earth [Fox98, YHK99].

Earthcam.com [Ano98t].

Ease [HJL99].

Eased [Ano96p].

Easier [GMS98, BBR99, Sch98c, Way95].

East [Str95].

Easy [Ano97p, Sim94d, Ken95].

Eavesdrop [Way93b].

Eavesdropping [Al 96].

Eavesdropping [RK99].

Ecash [Sch98h].

ECC [Cer97, Kal98e].

ECC/DLP [Kal98e].

EcoFan [PKA+98].

ECGP
Employing [BWM98]. EMV [Gui97]. enabled [Sch93e].

Encapsulating [Atk95b, KA98b].

ciphered [Lea90, Per91]. ciphering [Beu94].

Enciphering [HS90, OA94, Lin88a, Lin89a].

coded [DS97b, HG97d, QN98b]. Encoding [Til98, HG97d].

Encipherment [Obe99]. EMV [Gui97]. enable [Sch93e].

enabled [Cha99b]. Encabling [DS97b].

Encipher [Ano99g, BR95a, Ber98, JSY99, Ril96, WT99, Ano96e, Ano97-36, Rot97].

Encrypted [AW99, Bla98, GMCF95, GLZ99, GiI98, Jas96, SzW97a, YY91, Ano98o, BT998, Bre97b, DF97, STW95, Kip97].

Encryption [Ano97-33, Bla94b, Lom94, Luc98b, LW99, SS99c, Beu94, KAK96, LL98b].

Encryption [ASW99, AAB+97, Ada97b, Ada98, ARRW99, Ano98b, ABK98a, Na93b, Ano94c, Ano94d, Ano96c, Ano96m, Ano96q, Ano96o, Ano96p, Ano96-29, Ano97h, Ano97t, Ano97u, Ano97v, Ano97-39, Ano97-42, Ano98k, Ano99f, Bac95, Bal97, Ban93, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b, BDP98, BS99b, BS99c, BRW99, BS93b, Bir95, BB95c, Bla96a, Bla96b, BF99b, Ble98a, BC95c, BFS96, BY92, Buf95a, Com94a, Com94b, CDNO97, CMN99, COP+95a, CH98, CMK98, CT99a, Cop94a, Cou93, DDJ98e, DDJ98c, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DS97c, Ele98, FIP94, FN94, For99b, FY95b, FY97, FH94, FO99a, FO99b, GSY99, Ga90, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, Gen98a, Gen99a, Gen99b, GK98, Got99, H97b, H97b, Hat96].

Encryption [HK98, HK99d, Hub98, Joh90, JM96b, KaI93a, KY95a, KR96a, KaI98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kum98, KBRS97, KH98b, KDY98b, Kwa93, Kwa97, RSA93f, Law98, Lea99, LT91, LW91, LM91b, Lin93a, LS98b, Luc97, Luc98c, Luc99c, LW99, MGL+98, Mad97, Mad98c, Mad98d, Mat94a, Mat97, Mer91, Mey96a, Mi95, Moc97, Muc99, Mi99, Na93a, Na94b, Na94d, Na97b, Na98, Na99a, Na99c, Natxx, NBD+99, NH90, Oh99, Oka94, Ori96, Pai96, Par98a, Par98c, Per91, PRZ99, Pin97, RSA93a, RSA94, RP94, Riv95c, Riv95d, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SV+98, SKN98a, SKN98b, Sch99a, Sch99b, Sch99d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SE96, See97, She95b, She92g, SB98, Sim95].

Encryption [SM96, SM98b, SB92, Sni93b, Sni97a, SB99, Sta97c, SW99b, Sto90, SzW97b, THP+98, Un97a, Un98a, Un98e, Un98b, Un98d, Un98e, Un96c, U97a, Un97b, Un98f, Un98h, Un98g, Un97c, Un98j, Un98i, VB96, VKR98, WSK97a, WSK97b, War98, Way93b, Way93c, WSFC99, We91a, We91b, Whe94, Wir98, Wri99, Vin97, YY97c, Yu97, Ze97b, Zie97, Zol93, Aus96, Abr97, A93a, All97, And94a, Ano90, Ano92b, Ano94c, Ano95c, Ano95k, Ano95m, Ano95q, Ano95t, Ano95v, Ano95w, Ano96d, Ano96g, Ano96m, Ano96l, Ano96u, Ano96w, Ano96-30, Ano96-31, Ano97i, Ano97j, Ano97m, Ano97n, Ano97y, Ano97-31, Ano97-30, Ano97-35, Ano97-38, Ano97-41, Ano97-46, Ano97-49, Ano97-51, Ano98a, Ano98v, Ano98u, Ano99m, Ano99n, A94, AM99, Ban94, BTD98, Bax97, Bea96].

encryption [Bee96, Bee97, BR94b, BR95a, BDJ97, BR97b, BB90, Bet95c, Bih97c, BF99b, BC96a, BMS96, BFS98, Bow93, Bre97a, Bro96, Bus96, Com97, C99c, Cha94b, CLW98, Cle96, Cli97, Cli99, CJM96, Cra96, DH96a, DOR99, Dia91, DL98, Ele99, Ell97, Eng95, FC94, FB97, Gi97, Gol99b, Gol96d, GBL94, Goo96, GKS97, Har90, HK90, Hat97, Hel93, Hel98b, HT95, HP94, HY95, HCY96b, HCC98, Int91b, Jac90a, Jac90b, Jak99c, JT96, JT97b, KY95b, KY97, KYxx, Ken95, Kir95, Kn99c, Kop97, Kuc92, Kuh98, Kuo90,
Escrow [AAB+97, Bla96c, BDS98, Cae96a, CGM97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, IHWY95, Mad97, Mah96, Mar97, MS95f, MKS99, Nec96, SYM98, Sam96, SM95a, VvT97, VBD99, YY99b, An94f, BDHJ97, BR96b, DH96a, Des95, Fre94, KL94, Maa97, Un95a].

Escrowed [Bas95, Com94b, FIP94, Nat94d].

ESIGN [FOM91].

ESORICS [DEQ92, Q+98].

ESP [KA98b, Atk95b, KMS95a, KMS95b, MD98, MG98a, MG98b, PA98a]. espionage [HK99c].

Espoo [Nyb98].

Essential [Len96b, SSV+98, SSM+97, SMD+99].

Essentially [BR91]. Establishing [Des96a].

Estimate [Miy93c, UU97a].

Estimates [DLP93]. estimating [AI 96].

Estimation [VN95, JH98].

Ethernet [Bec99].

Etruscan [Nis91].

Euclid [LZ91a].


Eulerian [MS98].

Eurocast [MDP94].

EUROCRYPT [Bih91, Dan96, Dam90a, Dam91a, Dav91, De 95, Fum97, GQ95, He94, Man96b, MZ98, Nyb98, Pic98, QV90, QC95, Rue93, Ste99b, Ano98l, Bet98, BC98, CP98, Dam98, Dav98b, De 98b, Fum98a, Gue98a, QG98, He98c, Ing98, Man98, Pat95, QV98, Rue98].

Eurographics [Kui91, PH91].

Europe [Ano97k, And96a, Ano95f, Ano95k, Ano98a, Koo97, Mus92].

European [Dan96, DEQ92, Q+98, Spi95, T+98, Com97, Gar97c, VCF+90].

Eusipco [T+98].

Eusipco-98 [T+98]. evaluated [LMS97].

Evaluating [PA99a]. Evaluation [AG97, Ano97b, BGK99, BP95b, CJR98a, CJR98b, HW98, KBR99, PG97b, RIE95b, RIP95a, Rob93, Roh99, WT99, CJRR99b, KM97, PS99a, Sim95, VCF+90].

Evaluative [MI99].

Even [BCE+94, Bosxx, Ano95q].

Evening [Che92].

Event [Ruo94, SK97b, SK97a].
Rev91, Smi94b, Von92a, Von92b,YL93, dR95. Exponents [Wie90b, vOW96, Gro94, VW96, Vv97, Wie90a]. Export [Ame96b, DDJ98e, DDJ98f, Gar97b, GC97, Han95, Han99, Uni97d, Abr97, Ano97-51, Ano99m, Ban94, Cli97, Gen99a, Han97, Mad99a, Mad99b, Reo97, UU97b, UU97b]. Exportability [Wie91a, Wei91b]. Exportable [Eng95, Ano95v]. Exports [Bar96a, Buc95a, Sta97c]. Exported [MSK99a]. Exposing [Sil99]. Expressive [MTES99]. Extend [Ts'97]. Extended [ASW98, BFN98b, BV98c, BD90, BS91g, BD91, CvHP91, CK90, DDP90, DY91d, DDP99, DD99, DY91f, DF91a, Dob95a, EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, vHPP93, Bea97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, Ole95, Pa96]. Extended-Certificate [RSA93c]. Extending [Bad99, Hus94, Mi99]. Extensible [AV98b, WBDF97]. Extensions [CD91, DT98a, Law98, NW97, Atk93, GH99, GK95a, JD91]. Extensive [Av97-44, Sim95]. Externalization [OA99]. Extracting [Nis96]. Extraction [SD99]. Extraordinary [Jam98]. extremely [Ano90]. eyewitnesses [Ano97-37].

FA [Bao94]. Fabrication [DDJ99]. Face [DDJ98d, DMFB97]. Faces [GB98]. Fachtagung [BGH95b]. Facial [LMP99, HEG98]. facilitation [Cli99]. Facility [AKF94, Bi90, She96a, YS91, JMLW94, SY92]. facing [KG96]. facto [Pri94]. factor [KM98b, SYWMB95, VS95]. Factored [Ano96b]. Factoring [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pa99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, McC99, Mei96b, Riv95a]. Factoring-Based [Kal98c]. Factorisation [DH95a, Jon90, DH95b]. Factorization [Ale92, DDL94, MM98a, MM98b, Odl95, vO91a, Sho97, vO91b, LL93, M98, WH93, vO92]. Factorizations [BMS94, NS97b, NS97c]. Facts [Ano91b].

Failed [Alv98a]. fading [To97]. Fail [BP97a, PP97, SSNP99, vHPP93, And94b, Pf96c]. Fail-Stop [BP97a, PP97, SSNP99, vHPP93, Pf96c]. Failed [BCE+94]. fails [DH96b]. Failsafe [KL94]. Failure [Ano95a, Ber97c, Gar98a, TY99, FR95b]. Failures [CH98, JQ97, Moc92, Sim94b]. Fair [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, MS99, SS99c, SS99f, Tra97]. Fairfax [ACM93a, ACM94a]. Fairly [HD96a]. fail [Od90, Rob98b]. False [LD98, She92b]. Families [Kal98e, Per99]. Family [KT98, Mad98e, Mvy91, RP97a, ABC+98, BG99+5a, FSS94, It90, K90, SR98].

FAPKC [DYL98]. FAPKC3 [TCC97, TC97]. FAPKC4 [TC99a]. Far [Str95]. Fast [AGS97, AM90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bih97b, Bih97c, BHK+99, BD94, BK95d, BGV96, CS91, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DB96, DNR97, EPR99b, EPR99a, Gar97b, Gol96a, HJT98b, HP94, HCY96a, JJ99a, JJ99b, KR94a, KTM+99, KP99a, KP97, KR99a, Kma99c, KMK99, KA91, Koy95, LM95, Mau90, Mer91, Mih94, MM95, NS99a, NKP99, PR97, Pr95a, Rog95, SW97a, SW97b, SO95, SV93, SB98, Sho96, Sil97b, Tak97, Tak98a, Tak98b, T+99, Van98d, Van98e, AM93, AB96b, Ano98t, CGV94, DKR97b, DV96, GGH+98, HJPT98a, Jenxx, LRW93, LC98, MZ98, PvO95, RRSY98, She92c, SN94, SH99, SAM97, SGSS99, YL93, Gol96d, OA94]. Faster [Luc96a, Luc96b, WZ99, YY99b, Bosxx, Mih96, Sch98c]. Father
[CFK+91, DDJ99]. Fault
[BS97a, DHHSS95, GX99, OKST97, Pai99a, RBvR94, IE99b, TCH+91].
Fault-Tolerant [DHHSS95, RBvR94]. Faults
[BDHJ98, BDL97, CH94a, FY99, Gar94, JQBD97]. Fauvel [CFK+91]. Fax
[Ano91b, Int91b]. FaxModem [Ano93k]. FBI [Szw97a]. FC [Fra99, Hir97, Hir98].
Federal [Ano97h, Ano97-42, Lee99a, RP94]. Federated [SS99b]. Feedback [Jut98, Knu94a, SN93, SK96c, SK96d, Vau99a].
Fermat [LLMP93, McK99]. feud [Mad98e]. Few [FJRS96, Mel98]. FFT [DBGV93, MS90b, Sch91c, Sch93f, Sch93g, SVB93, Vau93].
FFT-Hash [DBGV93, Sch93g, Sch93h]. FFT-Hash-II [Vau93]. FFT-Hashing [Sch91c]. FGPAs [Nor95c].
Fibonacci [SMS99]. Fiduccia [CK99]. Fiduccia-Mattheyses [CKM99]. Field [CD98b, Kob98c, LL99, LLM90, LL93a, MR95b, Ros93, SY99, TT99, CDEH+96, Dav98a, GH99, Gor93b, HWB93, Has99, Pom94]. Fields
[BP98a, BMT96, BL96b, BL96a, BP97c, De 98d, LO91a, LO91b, Mas91, MFC95, PSR97, Ano90, Gal99, LN94, MVZ98, SW95a, Sch91a, Shp99a, Von92a, Von92b, ZPY96].
fifteen [Den90]. Fifteenth [CFK+91]. Fifth [SJ97, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni98h, Uni97c, Uni98k, ACM93b, USE95b].
Fight [De 93b, De 98c]. FIF [AB99a, AB99b]. FIL-MACs [AB99a, AB99b]. File [ANS98a, AW99, Ano97x, Ano97-34, Bla94b, Gil98, Man97b, RC95, HK97, MKKW99, SK97d]. FileDrive [Ano97-34]. Files [Bal99, PF94, Pop96, Ano98o, Gol99b].
Filesystem [HJR99, JJ91]. filling [BB90]. Film [Gar97c]. Filter [She92e]. Filtered [MS94]. Filtering [Sch97d, LLB98, LYG94]. Final
[RIP95b, RIP95a, BFS92a, BFS92b, BP95b]. finally [Ano98v]. Financial [BB95, ANS98b, FBS97, FL99b, Fra99, Hir97, Hir98, Lan97, Riv97b, Swi97]. Finding [BMR99, Cip95c, Ler97, Riv91a, Sim98c, YY98a, CC99, Car97c, Sta94a].
Fingerprint [DDJ98g, DDJ98h, HJ98].

Fingerprinting [Ano99l, BS95b, BS98, DF99, Hei96b, PS96a, PW97a, PW97b, Sas99a, YST99a, YST99b, DF98].
Fingerprinting [HJP97, OM193]. Fingers [RK93]. Finite
[BI95, BDG98, BMS94, BVFD99, CD98b, DKK98, Gys96, KPR99, KV94, Kob8c, LO91b, PS96b, She92e, Shp99a, Ano93k, Bao94, BI94, BGR95, DWZ96, DYL98, DF93, FSS94, Gal99, GH99, HWB93, Has99, Jun96, LN94, MK92, PS97, Pie93, Tao94, TCC97, TC99c, Von92a, Von92b, Wall98].
Finite-Impulse-Response [She92e].
Finite-Size-Particle [BVFD99]. Finland [Nyb98]. FIPS [Nat93b, Ano93f, Ano95, Nat93a, NIS93b, Nat94a, Nat95, Nat99a]. Fire [Way93b]. Firewalls [GLZ99, Opp97].
firm [Ano97d]. Firms [GC97]. Firmware [MNSV97]. Firmware-Oriented [MNSV97].
First [BCC97, GPSV98, Hir97, KT99, KP99b, KW99, Law98, Mat94a, Nat98, Nat99c, RD99b, ACM99b, And96c, Dob98, HO997, IZ98, NBD+99, Un97a, Un98c, Un98d, Un98e, Un97b, Un98f, Un98h, Un97c, Un98k, USE95c, RD99a].
First-Order [KW99]. Fish [BD94]. Fishermen [Ano96-29]. Fissures [DDJ98e, DDJ98f]. five [Han97, KAK96]. fix [Ano98t]. Fixed [FK93b, Mae98, HP94].


 Formal [BR97a, BFN98b, Bol98a, Bol98b, Boy92, GFB93, Gue98b, Mei95, PD99b, SM95b, Tou93, WK96, AhD9F97, AAP92, Ata94, BFN98a, JW91, ZLX99]. Formality [ACD94]. Format [CDF98, Nys99].

 Formats [AS92]. 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]. found [Eng95]. Foundation [Go95a].

 Foundations [Ada91, BDFM99, Gols9a, Gols9b, IEE92a, IEE96a, IEE96c, IEE97f, IEE98a, IEE99a, JR96]. Founder [Pin98].

 Four [Eve98, HKQ99, Koe99, Riv91a, DL95].


 [Boy92, DGV93, Hed97, PS99f, PW99, SL99, VP99, Com97, HN94, LS98a, Prf96c, Tass98, DT98b]. France [Ch98, DEQ92, FR95a, GQ95, QG95, Vau98e]. Francis [Lea90].

 Francisco [Ano97a, Ano98n, USE92a]. Franconia [IEE92a]. Franklin [WD99a].

 Fraud [Neu92, VGP93, VvT97]. Fraud-Detectable [VvT97]. frauds [Sga93]. Fray [Gar97b, Law98]. Free [BP97a, BHT98, DBl9+6, CD98b, Doh97, Eri97b, GJM99a, GJM99b, HBK99, Rus93b, SK95, All97, BT94, Des90b, Des96b, Doh95a, Il94, Sav96, Vau93]. Free-Space [HBK99]. Freedom [Cae96b, Uni97a, Uni98c, Uni98b, Uni98e, Uni96c, UU97a, Uni97b, Uni98f, HM96].

 freely [Ano97n]. FreeNIX [USE98c].

 French [Ano97y, Bl98b, Bou94]. Frenkel [CFK+91]. Frequency [BP98c, MSHP99, Ano90, Tod97].

 Freshness [KY92]. FRG [Oht96]. Friedman [U92]. friendly [Bus96].

 Friends [DDJ98e, DDJ98f, Sch92b].

 Frobenius [CPPK98, Graxx, KMK99].

 FROG [WFS99, Wag99b, GLC98, WFS98].

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

 frustrate [Szw97a]. FSE [Bih97e, Vau98e].

 FSE`99 [Knu99c]. FTP [SSH93].

 Fujiyoshida [IR93]. fulfilled [Mar96].

 Full [BS93a, DH90, SK98c, SK98b, Ano98a, Pos93]. Fuller [CFK+91]. Fully [BCD94, BCD96, HE98].

 Function [BJY97, BDP97, BP97c, CP91, DGB93, DGV93, Dae95, DCF98a, DDF90, Dob97, GGY96a, HILL99, HL99, MCD99, NSS99, PBD97, Sch91c, TOU94, AB96b, DK94, DDF94, DI99, GGY96b, KSB96b, KSB97, LTT95, MT98, MVZ98, PKM97, Sch91a, SRRL98, SS95b, SS95c, YL97c, ZPY96].
dB94]. **Functional** [Yam99]. **Functions** [AHV98, Ano95a, BDPSNG97, BCK96d, BCK96e, BHSV98b, BHSV98a, BGK99, BGS94, BGS96, BM94a, BL95, BHT98, CCD99, Car93, DGV93, DY91d, DY91b, DFL99, ECM96, EPR99b, EPR99a, FBS98, GJKR96b, JQ97, KTM99, Kim93, KP96a, Kra95, KS97b, LM93a, LM93b, LM95, MS99b, MS90a, Mer90a, Mer91, MS95f, Mi96a, Mon92, OS98, PW93b, PGV92, Pre93a, PGV93a, PGV93c, Pre97a, Pre99, Pre94b, QC90, Roe94, Sch91b, SZZ95c, SRY99, ZZ95, Zhe90, vW94, BSNP96a, BSNP96b, BD92, BGR95, BCK96b, BCK96c, BHHR99, BK98f, CCZ98, CDG95, Cus96, CS96c, Dam90b, Gol96a, Gon95, GHS93, HSK97, HLMW93, HXMW94, HYLT99, ISO97, JG95, KL95b, La95, MCD98b, O94, PGV91, PGV93b, Pre94a, PGV94, PrO95, RP95b, Roe95, Rom90b, SZZ94a, SZZ95b, Sim98c, Tsu92b].

**functions** [Tsu92a, Wer93a, Wer93b, YT96, ZI97].

**Fundamental** [Ano96s, IEE97e].

**Funds** [GBC93].

**Funktioniert** [MPS94].

**Further** [Pre95b, WKS97, Mad99a].

**Fusing** [DMFB97].

**fusion** [KH97].

**Future** [Fuc99, HP98b, Od95, PT95, PM99b, Sch97a, An98, BFS92a, BFS92b, For99b, Mar96, NIS92, SB92].

**Future-Adaptable** [PM99b].

**Fuzzy** [Blo99, CIBM99, FCH99, KKW99, Tro93, ZHI98, CS99].

**Fuzzy-Control** [KKW99].

**G** [KSW96].

**G-DES** [KSW96].

**Gabidulin** [Gib95, Gib96].

**GAC** [ZZ95].

**Gaithersburg** [IEE94b].

**Galois** [Mas91, PSR97].

**galerie** [FK94].

**Gamal** [Jab90].

**Gambling** [HS97].

**Game** [Ett98].

**Games** [Mye96].

**Gate** [TT99].

**Gateway** [KBRS97, MB99b].

**Gateways** [Bec99, VDD99].

**Gauss** [GvP98, Mon93].

**Gbit** [HK97].

**Gbit/second** [HK97].

**Geheimschrift** [Kip97, Kip99b].

**Gemnall** [Geh94].

**Gene** [Cap94, CO98].

**General** [BC95a, BK95b, BPR99, CL98, DFB93a, ISO97, IVE91, KKT91, KP93, NOV93, OK98, ST93a, Ben94, DD95, Des90b, FDB93b, GN95a, Pf96c, Sch91b, Sim98c].

**general-purpose** [Sch91b].

**Generalised** [GS99b].

**Generalization** [Jab90, HKM95, MS93, TC99a].

**Generalized** [BB95, BFS98, CT97, HL93a, Jut98, LH93a, LH93b, Mau96a, PS96b, Bad99, BRR99, BCCG99, KUR92, PA93, Por93, Son99].

**generate** [Wer93a, Wer93b].

**Generated** [SVBJ96].

**Generating** [Ble96, De98d, FMM99, Len96a, Len98, MS95f, WYY99, CH97b, SH99].

**Generation** [ARV99a, ARV99b, BG98, BGM97a, BGM97b, Bir98, BF97b, BD93, Cotic97, CD96, DF91a, GKJCR99, Gil99, Gut98b, HL99, Kal97b, KS98c, MWB99, Mat96b, Mau90, Mih94, PS98e, ROT94, RS98c, RS98d, SN96, Si97b, Wi99, Bou94, FMY98, GTS90, LLH96, MS99c, PS97, PS98, SH94, Bou94].

**Generator** [FIP93, HILL99, JK99, KS99, KW99, MS95b, PS98b, Daw93, Deux, KSF00, MS95a, Mih96, PC98, Rev91, Sin99, TS98, Wal90].

**Generators** [HL99, KSWH98d, Kra90, ZYW91, CS96b, CS97b, Imp92, Kos99, Lag90, Pat91b, Por93, SGS99].

**Generic** [Bel92, CM99a, MS98b, Tua99, ZK98].

**Genetic** [BS99a, LC99].

**genigma** [Obe99].

**genius** [Ano97-37].

**Genomic** [MUS98].

**Geodesic** [Blo99, LFCK99].

**Geometric** [OMA98, Sim91, JM93, JM96a, Mau95].

**Geometrien** [Wal98].

**Geometries** [LMS90, FSS94, Jun96, Wal98].

**Geometry** [Ben99, DFGH99, Ton96].

**Geometry-Based** [Ben99].

**George** [Pin98, WG97].

**Georgia** [ACM99b].

**Gerdes** [CFK+91].

**German** [Wei99, Cra92, Dav98a, FT95, Ger97, Hor99, Jar97, Kah91a, KK97, Kip97, Kru98, Wal98].
Harari [Ver95]. Harbor [MGL+98, Mar99, SS99a, BFKL94, Jon90]. Harder [Sch97b]. Hardness [BV96, NS99b, DI99, Kha93]. hardness-amplification [DI99]. Hardware [ACD94, Ano96u, Bir98, BP99b, Bri90b, BS91h, Cla98a, DGV92, GN95c, Koc96a, OSA91, Wil93a, Wot99, YK98, BS95a, Gai90, KP99b, LMS97, MZ98, Nor95a, Nor95b, Nor95c, NO96, See97, SN94, TY92, Way95, Zhe95b, Kui91]. Harmonic [RG99]. Hash [ANS97, AN93f, Ano95a, Ano95l, BDPS97, BCK96d, BCK96e, 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, PR99, PW93b, PGV92, Pre93a, PGV93a, PGV93b, PGV93c, PGV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sch91c, Sch93f, SV94, SRY99, Sta94b, Vau93, Zhe90, vW94, AB96b, BSNP96a, BSNP96b, BD92, Dam90b, DK94, Gon95, HLMW93, HXMW94, HYLT99, JG95, KL95b, MZ98, PGV91, Pre94a, Pv905, RP95b, Roe95, SV95a, SRRL98, Sim98c, Tsu92b, Tsu92a, JL97c, DBGV93, Sch93g, EPR99b]. Hash-and-Sign [GHR99]. Hash-Based [PRZ99]. Hash-Functions [QG90, ISO97]. Hash-Values [GS94a]. Hashing [AS96, BGG94, DC98b, FNS92, KP97, Kra94b, KBC97, PS93b, Rog95, Rus93b, Sch91c, Sch93f, Sho96, Sth91b, TZR94, BGV96, Bosxx, Giv90, BJB90, Sab94, Sch93g, Sta99b, ZPS93]. Hasn’t [Gar97a]. Hasty [Sch98i]. HAVAL [ZPS93]. Hawaii [???90]. head [Ano94i]. Header [Atk95a, KA98a, MR95b, Ros93]. Heads [GC97, Sto98]. Health [GO96c, Mjo93]. Hearing [Uni98a, Uni98g, Uni98j, Uni98i, Uni97a, Uni98d, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k]. Heat [GC97]. heating [Mad98a]. Heats [Gar98b]. heaven [Gol97c]. heavily [Ano97-35]. Heimdall [DW98]. Held [Ano96-28, BF99a, Far93, Uni98f]. Hellas [IEE97c]. Hellman [RSA93b, Ano97n, BY93c, BY93b, BRR99, BWM99a, BV96, Bon98b, Bon98a, CS97, CS97d, HY98b, HY98a, Kal97a, Koc95, Koc96b, Mau94, MW96c, MW96b, MW99, NS97c, NS97b, Van95a, VW96, WM93, vO9W96]. Help [GRB99, PKA+98, AK95]. Help-Desk [GRB99]. Henry [CFK+91]. Her [Ber96a]. Herd [Rit99]. Here [MK94]. Heterogeneous [DVPL92]. Heuristic [MCD98b, CKM99]. Heuristics [SBG99, CD98a]. HF [RP94]. HFE [KS99b]. HFX [LR96]. HGF [Uni94b]. HGF-94 [Uni94b]. Hidden [BL95, CD97, JP96, KZ95, NS99b, Pat96, Sak96, PSB97, Til98]. Hide [SV99a, SV99b, SvS98]. Hidell [Sco92]. Hiding [Auc98, BGML96, BLMO95, CM97b, CD97, CD94, GR96, GLB96, HS96a, MS99a, MO99, Phi96a, Phi98, RGV97, SC96b, SZT96a, And96c, Beu94, Bra90d]. Hierarchically [LE99]. Hierarchical [FL96, OOK91, CMP97, GPC99]. Hierarchies [Ruo94]. Hierarchy [Hwa97, YY99b]. hieroglyphs [Wir98b]. High [AC98a, ARV99a, ARV99b, Ano99c, Ano99f, BCR98, Bla96a, Bla96b, BMS99, Chi99a, Chi99b, DP98a, DP98b, Ebe93, FVEA99, FP99, Gar97a, Gar98b, GN95c, HR90, IEE94e, IEE96d, IM93a, IM93b, KAP98, Koc94, Koc93, KB92, LS97, MPP95, MSHP99, Rus90, SKNO98a, SKNO98b, Sch92d, She95b, Sut99, VNW94, Ano97y, Duf98, Graxx, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Uni96a, Yeu97]. High-Assurance [IEE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Chi99a, Chi99b].
high-end [Ano97y]. High-Frequency [MSHP99]. High-level [Rus90].
High-Performance [ACM99a, BMS99, GN995c, IEE94e, Sut99, NO96]. high-quality [Yeu97]. High-Radix [Kor93]. High-Speed [ARV99a, ARV99b, Ano99c, DP98a, DP98b, Ebe93, IM99b, Ko94, MPP995, SK990a, SK990b, IM99a, Nor95a]. Higher [Jak99a, KMKH99, Lea99, MS99, Sut99].
Higher-order [Jak99a]. Highly [MS99b, PV97, ARK99]. Highway [Ano94d, hat96].
Hill [MCD99]. Hints [JM99]. Hiroshima [IEE96b].
Histogram [Mae98]. Histograms [BMS99]. historic [Bur98a]. Historical [Kob97].
History [Cal92, CTK94, DKK99, Ers99, Hi97a, Kah96a, Sim96a, Ano97-37, Dav98c, Jol99, Kip99a, Mac98, Ros97a, Sim98a, Web93, CFF99, hits [Mad97]. HKM [LR96]. HKM/HFX [LR96].
HMAC [BCK96a, BCK96c, KBC96, KBC97, MG98a, MG98b, OQ97, Sta99b]. HMAC-MD5 [KBC96, OG97]. HMAC-MD5-96 [MG98a]. HMAC-SHA-1-96 [MG98b].
Hoffman [Hat96, Wai95]. HOL [ACD94, Bra95a, Bra96]. Holder [OMI93].
Holiday [IEE94a]. Holy [Sal99]. Home [Hus99, Ano970, Hod97]. Homomorphic [FDB93a, Bet95c, FDB93b]. homomorphism [Dom96].
Homomorphisms [Bur96, SK94]. homophonic [HYHW98]. Honest [Rab94].
Hoo [Sch93a]. Hook [Ros96c]. Hope [BCE94]. Hopes [GO96c]. hopping [MHMW98, Tod97]. Hor [IPNDMM91].
horse [Sch99f]. Host [Kol95, BG976].
host-centric [BG976]. Hostile [GSTY96, SKAM99, LC95]. Hot [IEE98b, IE99b, Bra90b, CB96]. Hotel [LW96, Nat98]. HotOS [IEE99b].
HotOS-VII [IEE99b]. House [Cl97, DD99, Uni97a, Uni98c, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, UT97b, BH9R99]. Houthalen [QV90]. HP [GC97, Hed97].
hseuh [XtW94]. HTML [Ano97-27].
HTML-driven [Ano97-27]. HTTP [FHBH97, Ude98]. Huang [PBGV90].
Huffman [Moh92]. Hui [XtM94]. Human [DDGM97, GB98, KI96, Mat98, RP97b, OA99]. Hundred [Un97a, Un98c, Un98d, Un98e, Un96c, Un97b, Un98f, Un98h, Un97c, Un95a, Un98k]. Hungary [Rue93]. hunger [WS99]. Hurt [Gar97a]. Hurt [Wel97].
Hwang [Ala97]. Hybrid [DD99, LJM94, KA99, MD99, NT99, Var99a, BP97b, GML94, RO96].
hyperchaotic [BCCG99]. Hypercubes [DHW95a, DH95b]. Hyperelliptic [Sma99, BK98, OS91, OS98, SSI98].
Hypermedia [Kl99]. HyperText [RS96a]. Hypotheses [ZMI90, Kuk99]. Hypothesis [MUS98].
I/O [Got99]. IBM [Ano96b, Ano96c, Com90, Gar98b, Gen98b, Un998, IC [DDJ98g, DDJ98h, JT97a, PC98].
ICALP99 [vWN99]. ICARUS [Var99b].
ICE [Kwa97, VKR98]. ICICS [HO97].
ICIP [Ano94e, IEE96e]. ICIP-94 [Ano94e].
ICL [CFK91]. ICSA [Nic99]. ID [CS97c, Hwa92a, Hwa92b, Hwa92c, IS99, JY98, LH99, MS98a, Mu92, TC91, WSF99].
ID-based [CS97c, Hwa92a, Hwa92b, Hwa92c, JY98, LH99, MS98a, Mu92, TC91]. idea [OA99, BBS99b, BK97, DGV94c, HO96, Haw98b, Haw98a, KSW96, LIP99, Mei94, Sch93d].
 Ideal [ABDV98, BC93a, BD90, Bri90a, BP97e, Pai98a, Pai98b]. Idealised [RS99c].
Idealized [MT99, MM92b]. Ideals [GPT91a, GPT91b]. Ideas [HGH98, RS99d, TCH91]. identical [BCCG99]. Identifiable [KOO95b, KOO95a]. Identification [BCCG93, BLM904, BDB92, Cha94b, GS94a, KM99b, Ki96, LMBO95, LML98, NP97, OO98, Oka93b, Sak96, Sch90b].
Identities [MS99a, Sar99].
Identity [ALO98, Dan95, DQ94, FKMY98, HJP98, JG90, KP98, Len99a, SSN98a, Gua99, OU98b, Tan90]. Identity-Based [Dan95, DQ94, SSN98a, OU98b, Tan90].
IEC [Int91a, GQW + 91], IEEE
[Ano95u, CH96, Ano96-28, Ano97-48, Ano98r, IEE95c, IEE95b, IEE96d, Kal97a, KK99b, LW96, Pit95]. IEEE-IMS [IEE94a].
IETF [Ano97c]. If [GPR98]. IFIP [Kat97, LM98a]. IFIP/GI [LM98a]. II
[Sch99b, AK99, Ano97-40, Ano98i, Ano99c, BS91f, CFG96, CK95, CW91b, Dav98a, Don98, Eri97b, Mit92b, Mon96, Mus92, Pn98, Rat96, Rey97, RP97b, Ros99, Sch93f, Sch93g, USE90, Van93, Wil98a]. III
[Fri92b, Gau93, GN95c, Nor95a, Ree98, Rey99, USE92b]. iKP [HSW96]. illicit [SG96b]. Illinois [USE99c].
Image [BLMO95, BO96b, BI99, Car95, J98c, KR98, KPR99, LvdLL97, Lvd98, LSVV95, MFC95, NNEK97, Per97, SC96b, SZT96a, WD96, ZK95, BP98b, BP98c, BBCP97, BCCP98a, BCV97, BOD95, CKLS96c, HW98b, Ibx97, Irw98, Nas94, Nat97a, ODB96, ÔPH*99, Pit96a, RRP97, RKDB96, TA97, XBA97, ZL97]. Imagery [WD97]. Images [BLMO95, BO96b, B99, Car95, J98c, KR98, KPR99, LvdLL97, Lvd98, LSVV95, MFC95, NNEK97, Per97, SC96b, SZT96a, WD96, ZK95, BP98b, BP98c, BBCP97, BCCP98a, BCV97, BOD95, CKLS96c, HW98b, Ibx97, Irw98, Nas94, Nat97a, ODB96, ÔPH*99, Pit96a, RRP97, RKDB96, TA97, XBA97, ZL97]. Imaginary [HJP98b, HJPT98a, ZPY96]. Imagination [Sha99a, Ros97c]. Impact [Mar96, Ven90]. Imperceptible [CKLS96b]. Imperfect [MY98]. Imperfectly [BMC95]. impersonation [SNT93]. Implementation [Ano96, Bih97b, Bra96, BS91h, Dae99, DGT96, DRR95, DBVD96, Ebe93, Fei93, Fei96, FOM91, Gla99a, HKQ99, HRVV99, IM93b, KP99a, Kob98c, Koc94, Koc96a, Lan97, LCN99, NM99, OSA91, PL94, PP90, Ros96b, SJ98, She95b, Tou92, Var99a, YKY99, You97, Zim99, BR96b, BC90, CKM99, Dia91, HNM98, IM93a, LS98a, LL98b, Men91, MV90, MIZ98, ML99, Nor95a, Pa96, Per91, SS98a, See97, SAM97, Vadm95, XL98, Koe99]. Implementations [Bas98, Bri90b, Gau98, HK98, HK99d, Nor95a, Pa96, Per91, SS98a, See97, SAM97, Vadm95, XL98, Koe99]. Implementing [SAS99b, Van95a, Lee99a]. Implications [Bas93, CMYY98, NS99b, PN92, Van95a, We95]. Implicit [Jan98, MLY93]. Implicitly [HRVV99]. implies [LHL95b, LHL95a]. Importance [BDL97, Sch99h, CM97d]. important [Sta94a, Woe97]. Impossibility [MP91]. Impossible [BBS99a, Fer99a, BBS98a, OK96a]. Imprimitiv [Pat99]. Improve [Gar92]. Improved [Ano96f, BK98e, Bo90, BS91g, CRRY99, CJL"92, JM99, JJ99b, KM96b, LD99, RP95b, SH97, SAM97, WS98, YL95b, YL95a, ZYR91, Cao99, He92, NMVR95a, NMVR95b, SH95a, SH95b]. improvement [BB95b, Bir95]. Improvements [HJJ99, Kle90, IKNY98]. Improving [BHS93, BKPS93, GLV99, SF97, SZ98a, SMK98a, Sun98a, HM97b]. Impulse [She92c]. IMS [IEE94a]. In-memory [Ven90]. in/for [SHG98]. Inaccuracies [OD99]. inadequacy [Kah98b]. Including [DG93, DW94, JS95b, JS95a, KL95b].
incorporation [Ano95c].
increased [HS96b]. Increasing [AP93, Bao94, BKR98a, BKR98b, Bla94a, KFJP96, Mar97]. Incremental [BGG94, BGG95, BD93, Fis97].

independence [RS98a]. Independent [Abe98a, Mau91c]. Index [MZ98, JV98b]. Index- [JV98b]. Indexing [ADEDS99, DRR95]. Indic [lPNdbbbprm91]. Indicia [TYH96]. Indies [Fra99, Hir97, Hir98]. Indistinguishability [BS99b, BS99c, NR98]. Indistinguishability-Based [BS99b, BS99c]. Individual [IKM99, Uni98a, HN98, Uni98d, Wel95]. induced [PS99a]. Inducing [MCD98a]. Inductive [BP98e, BP98f, COM99, HB99, Pau99, Jan95, Pau98]. industrial [CWM+91, PGV93d, PR98]. industries [CWM+91]. Industry [ANS98b, Kan96, Lea99, Uni98j, AA95, Acc97, CWM+91, Uni98k, Wel95, Zai97]. ineffective [Min97, MBY97]. inequalities [van97a]. Inequality [MS99b]. Inference [ZHJ98, Jan95]. Infinite [CK90, HKL94]. infinitely [It90]. infinitesimal [Mra95]. Influence [MM92b, NH98]. Infocom [IEE92d, IEE94f, IEE95c]. Inform [YT96]. Information [And96c, Int91a, Ano93g, Ano95p, Ano95r, Ano96a, Ano97b, Auc98, AR99, Bar94, Bas93, BDGV93, BLMO95, BS91g, Cac98, CFGS99, CW94, CFG96, Den99, DMFB97, GRS96, GHGD98, HQ97, He96a, HH94, HR90, IE94a, IE97k, ISO97, KG96, KR98, KM96a, LOX99, LBHM99, Lin96a, Mao93a, MW96a, Man97a, Mau99a, Mau99b, MO99, Nys99, OD98, Or96, Ped91d, PL94, Pf96a, Phi98, Pit96b, PB99a, PGV93c, Pre98c, RSA93e, RSA99a, RIP95a, Sch97d, Sga93, STP93, SC96b, Sti93a, Stu99, Uni98i, Uni98k, VPM97, Wol98, Ada91, Ano97-43, Ano98d, BDGV96, BP95b, BDC+95, Bra90d, CM95, CC95, CKGS98, DL96, Dav98c, DF98, FM98b, Gru98, Gua90, Han95, Han99, HW91, IEE95c, Jac90a, Jac90b, Ken95, KS98c, KW92, Mar95b, Mau93b, NIS92, Ped91b, Ped91e, Rot95a, Sch90c].
information [Sch97c, SG96b, Sim92, Tas98, Uni97c, WSFC99, van97a, GS94b]. Information-Theoretic [Cac98, MW96a, Mau99a, Mau99b, MO99, Ped91d, Wol98, Sga93, Ped91b, Ped91e]. Information-Theoretically [Mau97a]. Informational [Sg90]. Infrared [DDJ98b]. Infrastructure [HFPS99, Or96, SS99d, VSH97, Am95, Ame96a, FB97, GH96, HMT+98].


Instruction-level [Cla99]. Instructions [Ros96a]. instrument [CWM+91]. instruments [Sch93c]. Insulator [NFQ99]. Insurance [EI97b]. Integer [MM98a, MM98b, Od95, vO91a, SM91, vO91b, KM99a, Mao98, Pos93, vO92].

Integrated [Ano96-28, KV99, Sm98a, YS91, SY92]. Integrating [Bo98a, Bol98b, GSY99, GL96, LBHM99, LC96a, Re92, Smi98a, AP93].

Integration [Ala93a, Ano97-34, CHLT99, CK99, FO99b].
De 93a, HRT96, IH99b, Kay95, Koh90, KN93, KNT94, Lei99a, Lin96b, Lun90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts’97, Tun99, Yu94a, Yu94b]. Kernel [BCCG93, WB92]. Kerry [IEE96c]. KEY [YY98d, ANS97, ANS98b, AKP96, AAB97, AN95, IBM93, Ano94b, Ano94d, Ano94f, Ano95a, Ano97c, Ano99j, Ano99l, AA93, BP98a, BI95, BDH98, BDG98, BCS90, BR94a, BR95b, BHSV98b, BHSV98a, BDP98b, Bes97c, BS91b, BS97a, Bir98, BMS94, BWW98, BWW99a, BWW99b, Bla94b, BDR96, Bla96c, BPK99, Ble97, BDHK93, BFS96, BD99b, BF99c, Boy90, BM94b, Bra95b, Bra95c, BS94, Bur94b, BDS98, Cae96a, CC99b, CG99, CDN98, CS91, CGM97a, CS98b, Cra98, Cur97, DDJ98g, Dae98, Dam91b, DN95b, DDP90, Dav96, De93c, DP98c, DB96, Dif90, DH90, ECM97, ECP98, ECP99, EFM99, FBS98, FO99a, Fun98c, Fun93, GHH90, Gt96a, Gan96a, GJKR99, Gib91, Gib96, Gil99, GM90, GGH97b, Gar96, HK99a, HGS98].

Key [HP98a, IS90, HMT98, HM93, Haw98b, HD96b, HJJ97, He92, HWF96, HY93b, HJT96, Haw97, Iss90, Jac96, JV96, Ka99, KPP99, KSW96, KS99a, Kel99, KS99b, KP98b, KM99c, KTS91a, KMOV91, KKT91, KP93, RSA93f, Lan99, LM94b, LW95, LMS97, LA98, LP99, Low96, Luc96b, Mah96, Mar97, Mat91, My91, Mau93a, MW96a, Mau97a, MP91, Men93, MM96b, Mic93a, MS95f, MM99c, MS99d, MS99e, MS99f, MS99g, MNS98b, MS99a, MNS99, MTVZ92, MAO96, MMS98b, MMS98c, MRS95, N96, Neu97, NS99a, Oka94, Oua98a, Oka98a, Oka98b, Om90, vO91a, P397, Pa99d, PK94, Pat95, Pin97, Pol99, PB99a, RAS93b, RSA93c, RSA94, R094, RS98c, RS98e, RS98e, Ros96a, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c, RCM99, SS98a, SYM98, Sam98b, DP91, Sas99a, Sch94b, SKW98a]. Key [SKWW99, SOOS95, SM95a, SE96, Sha99b, She94d, Si93, SR96, Slu98, Sta99b, ST91, SW99b, SH94, Sun98a, Sun99, TAP90, TA92, Uni98a, Van95a, Van93, VSH97, VV97, VBD99, WM93, dW991, WLE99, WW98b, WKS99, Wie96, Wie97, Wie98a, Wie98b, Wof98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vOW96, AA95, Acc97, Lip98, AD97, AD99, Al96, Ano90, Ano96q, Ano96o, Ano96w, Ano96-30, Ano97k, Ano97v, Ano98f, BSNP96a, BSNP96b, Bao94, BI94, BDN99, BD99b, BSR97, BR96b, BCK98, BY93c, BY93b, BS91a, BFS92a, BG98a, BMS96, BFS98, BM95, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Cra97, Cus95, DK97b, DW96, DS90a, DH96a, Des95, DQ96, Dhe98, DV92, DN95b, ES97, FDB93b, FM97a, FMY98, Fre94, Fro96].

key [FGLP96a, FGLP96b, FL93, Gar96b, GH96, Gb95, Gb95, GH99, GTS90, HNSM91, HP99a, HP99b, HY93b, HJJ97, Haw98a, He92, HW96, HJJ97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa93, IZ98, IZ99, JM96a, Jar96, JLM94, Jon90, JYS98, KASH90, KSM99a, KSW97b, KL94, KR96b, Kir95, KM98c, Koo97, KM99d, Kos99, Kum97, LG97, Lsd92, LM9J93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LL95b, LCM9, Lon91, Lon92, Low95, Mad98f, MS98a, Mao97, MLA91, Mau91b, MY93b, MK99b, Mu92, ML95b, NM96a, NY90, Nat97a, N96, O94b, Ole95, PS98e, PS98f, Pe91, PP92b, RFL96, RT93, Roch99, Sal90, Sal96, SW95a, Sch92c, Sha95a, She96a, She97c, SK97, SY96b, SM90, Sni93b, SS95b, SS94c, ST95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC97].
key [TC99b, TC99a, Ts90, TC91, Tze99, TH99, Uni97c, Uni95a, VW96, Ven92, Wan92b, Wif94, Wil93b, Xie92, Xie93, XL99a, XW97, Yam98a, YL97b, Yu92, Zha91, Zhe95a, Zhe95b, ZPY96, vO91,
vO92, vT90, MC96, Mad97, BFS92b.

Key-Agreement [RSA93b].

key-clustering [Kum97].

Key-dependency [MAO96].

Key-Dependent [FBS98]. Key-Escrow [VvT97]. Key-Exchange [Dan95].

key-management [MLA91].

Key-Recovery [Ok98a, Oka98b].

Key-Schedule [KSW96].

Key-search [KP99a].

Key-Share [BWM99b].

Key-signing [Ros96a, Ros96e, Ros96f].

Key-specific [LMS97].

key-vowel [Lip98].

Keyboard [GO96c, She95a, Ale97].

Keyboards [CFK91].

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, Da98, EHMS99, Gir91, KSW97, KSHW98, KM99c, Luc98b, MP91, PS98g, SV99a, SV99b, Ste94a, Vau96, Way96b, Ano96h, Bih94a, CH97b, Cli99, DG94c, JP96, KC95, Knu95, LL93b, MWB99, MF97, Mok97, SS97a, SS97b, SV98, SH99, Sta95a].

Keyspace [CD98c].

keystream [CS96b, CS97b]. keystroke [JG90]. KG [Uni94a, Uni94b]. KG-94 [Uni94a, Uni94b]. Khafer [BS91f].

KHF [Wag98a]. Khufu [BBS99b, GC94].


Kingdom [D*98, Lom97].

Kingston [HA00, TM99].

Kiosk [BO96a, Gar96b].

kit [An97-38, Sun91b].

Kleptographic [YY97b].

Kleptography [YY97a].

KMOV [Ble97].

KN [SMK98a].

KnapSack [CP91, JS93b, ACBR90, CZ90, He92, JG95, LC97b, Odl90, Wan92b, Yu92, Zha91].

knapsack-based [He92].

Knapsacks [CJS91, Ort95b, Ort95a].

Knock [DDJ98b, Fly97, Hil97, Kir95, Mil95].

KMN [DDJ98b, Fly97, Hil97, Kir95, Mil95].

knowing [Ble96].

Knowledge [ADBB99, BMT98, BG90, BG93, BJY97, Ble98, BD91, BDB92, COM99, Cec97, CDS94, CD98b, Dam99a, DDP94a, DDP99, DO99, DFK93, DS98b, GMW91, GK96, GSV99, GO93, HT98, JKV99, NOVY93, NM199, O090, RS91, SI93a, SY99, Stu99, Syv92, Tou91, BOGG+90, BBP95a, BBP95b, CDP95, DDP94a, DF93, DP94, DF91b, Sah99, Sak97]. Knowledge-Based [Bie98].

Knowledge-Level [BMT98].

known [Ano91b, BK95a, MY93a, vOW91].

known-plaintext [vOW91].

KnowRight [BS95e].

Knoxville [IEE94e]. Knuth [CFK91].

KoMoD [SY99].

Komputer [An97-50]. Konstanz [Fum97].

Korea [An93g, KM96a, Rhe93].

Korea-Japan [An93g].

Korean [LL98a].

Korteweg [GK95b].

Kruh [CFK91].

Krypto [FK93a].

Kryptographie [KK97].

KryptoKnight [BGH95a, MT92].

Kryptosysteme [Har99].

KtSeqC [BG99].

Kudos [Sva98].

Kunstliche [CWM91].

kuo [XTmW94].

Kuperee [DH96b, HS94, HS96b].

Kurz [Ger97].

Kyongju [KM96a].

Kyoto [An99e].

L [Lip98].

Labeling [BKV98, KZ95, LvdLB96, LvdLL97].

Labels [ZK95].

Laboratories [An95d, An95e, An95p, An95s].

LABYRINTH [LS97].

Lac [CFG96].

Ladder [Bih97a].

Ladder-DES [Bih97a].

Lai [LLG10].

Lake [IEE96d, USE95b].

Lambda [HRVV99, GLV99].

lambdaProlog [NM99].

LAN [An96v].

Lancaster [WSFC99].

Lance [Hat96, Wai95].

landmark [KT99].

Lane [DDJ98e, DDJ98f].

Language [APDS93, AKP99, IOS94, KI99, PW99, AAPS92, Kos97].

Language-theoretic [APDS93].

Languages [ACD94, BD91, GMW91, PM99a, PD99b,
SAS99b, ACM99a, Ata94, DDP94b, GA98, IlI94, LS98a, PS93a, Sak97, vWN99]. **LANs** [She92f]. **LANSCAPE** [Rili96, Ano94g, Ano94h]. **Laptop** [GPR98]. **Large** [Bla93, BDHG99a, BDHG99b, CS97a, LO91b, LM95, NNEK97, PF94, Riv91a, SA95, SS90, She92a, Csi95, DT93, DL95, Fra90, FOO93, Has99, MSDS90, Yan95, Yua92]. **Larger** [PW97b]. **Laser** [Ano93h, JC93]. **Last** [dBB91, dB91]. **Late** [Bur99]. **latencies** [JG90]. **Later** [Sch95a, Gol97c, Roe95]. **latest** [Bee97]. **Latin** [BSNP97, Son99]. **Lattice** [Ano97-29, BK98g, CC99b, CNS99b, GGH97b, CC99a, SH95a, SH95b]. **Lattice-Based** [CC99b, CC99a]. **Lattices** [Dwo97, Ste98a, BV97]. **launch** [Taa98]. **Launches** [Gar97c]. **Lausanne** [IEE96e]. **Law** [And96a, Bro94, Cae96b, Swi97, Uni95a, Cli99, Way93c]. **laws** [Ano97-50, Bre97a, Cha94b, Gen99a, Gen99b]. **Lawsuits** [Lea99]. **Layer** [BB95c, FK99, Sar97, Wu96, Mye97]. **layered** [Jun99, RC95]. **layers** [AP93]. **Layout** [BW98]. **LCN** [IEE97l]. **LCN’98** [IEE98f]. **LCT** [ZYR90]. **League** [PWU99]. **Leakage** [WI99, HJKY95, SG96b]. **Learn** [Hel98b]. **Learning** [BV98a, COM99, FCH99, SG96b]. **Library** [Ano97-39, CFK +91, DK91, KHB99, Dhe98, RRP97, Man98]. **licence** [Ano97-51]. **License** [AG99]. **Licenses** [Ano97-39, TJ97]. **Licensing** [Par98a]. **Life** [CJ99, DDJ98e, DDJ98f, DQ94, GACDAFC99, Ros95a, CWM +91]. **Life-Span** [DQ94]. **Lift** [Gar97a]. **liftings** [CNST98]. **lifts** [Ano99m]. **Light** [Gar97b, HPG98, YRH98, BGM +95a]. **light-weight** [BGM +95a]. **Like** [JQ97, BS90a, BS91c, CCZ98, Kob99, MS95f, MT99c, Nac93, WSFC99, XZ97, Kim93, KP93, Way93a]. **Likely** [Bar96a]. **Limit** [Lea99, Way93c]. **Limitations** [BM91a, CMY98, Pis98, KV94]. **Limited** [AR99, BDS98, DVQ96, VBD99]. **Limiting** [Kl96]. **Limits** [And96b, AP98, EKK99, Swi97, BH98, Coh99, SOB98]. **Line** [Bra95b, Cac95a, Cac95b, CDF195, DT98a, EII99, EGM90, EGM96, LMOB95, PUF99, SS99e, SS99f, Tra99, DL98, Gau97, Mao98, Na97, VNM99]. **Line/Off** [EGM90, EGM96]. **Linear** [Ano95a, AMP99, BGS96, BK94a, BL95, BPV99, CFSY96, Dae95, DD99, Des98a, vD95a, DLR97, Gol95b, HO96, Haw98b, KR94b, KR95a, KTM +99, KR99b, LO91b, LH94, MS94, Mat93, Mat94b, Mat96a, Nyb95, OA94, Ros98a, SZ96, SF97, Sch96c,
Sch99a, Sel98c, SK98b, TN97, TSM95, YMWP99, ZYR91, Ala93a, AW95, BSN95, Bao94, BI93, Bih95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, HKM95, Haw98a, Jak98, KY95b, KYxx, KR96c, Kuk99, Lai95, LLB98, Lan95, MM90a, MAO96, MK92, OG95, SKD94, Tze99, YT95a, YT95b, ZYR90, ZH90, vD95b, vT94, Duh90].

Linear-Time [KR99b].

linearity [SB95].

Linguistic [CH99b].

Link [Ano98].

linkage [HCY96b, LC97a].

Linked [BRS99].

Linking [BLLV98, CM95, RP94, SM99].

Links [Blo99, CV95, DDNM98, JC93].

L'inuktitut [Ano99k].

Linux [Cor93, DDJ98a, Eri97b, Mor97].

Lion [AB96a].

Lippman [vdWS97, vS97].

LISA [USE99].

LISA'96 [USE96a].

list [LC97b, Uni97d].

Lists [FGR92, Riv98b].

literate [Sab94].

little [Ano91b].

little-known [Ano91b].

Lives [DDJ98d].

LL [FY95a].

LLL [Mis97].

loadable [Ano98m].

Local [Fum93, IEE97l, IEE98f, MM95].

Localization [PJ99].

Locating [KP93].

Location [FJP96, Jac96, KFJP96, KR98, WHFG92, FT95].

lock [Ano90].

Locking [BC97, CM95, RP94, SM99].

Locks [Way95, CC95].

Locomotive [Var99b].

Loen [LVW96].

Loftus [Hel94].

Log [Bal99, GJKR99, Gor99b, PS98b, WD98, YY97b, Koh90, SS95a, SK97d].

logarithm [CP95, CS97d, FR94, FMR99, HY93b, H97, HMP95, Mc99a, MV98, NR95].

Logarithms [BBT94, CH98, GM93b, LO91a, Man94, MW99, vO91a, She97, Tes98, vO91b, vW94, Gor93b, HZ93, Od94a, SS95b, SS95c, vO92].

LOGCFL [LSMV99].

Logging [Zol93].

Logic [AHMS99, BRS99, BAN90, CIBM99, CO98, DRR95, Gue95b, SG95, SM95a, SHK99b, CS99, Pos98].

Logical [PS99f, Wad93].

Logics [ADD99, GAGCDAFC99, KW99, Len99b, WK96, Bad99, XZZ97].

Login [ARH95, DQ93, Hil97].

Logout [Poo95].

Logs [SK98b, SK99].

LOKI [BS91f, BKPS93, Knu92, Knu93c, Knu95, TSM95].

LOKI91 [Knu93d, Knu93a, SF97].

LOKI97 [BPS98, RK98a, Rij99].

London [Ano93d, Ano97-28].

Lone [Ano97-33].

LONE-TAR [Ano97-33].

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

Long-term [CH97].

Longevity [Rot95b].

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

Look-up [Has99].

Looks [Sch97b, Mad96, vdWS97, vS97].

Loops [svA98, SHK99].

Lorenz [Car97b, Dav98d].

Lose [GPR98, Way96b].

Loss [Law98].

Loss [PW97c].

Lossy [CI96].

Lottery [Riv97a].

Lotto [QD91].

Lotus [Dwo95].

Louis [Ers99].

Louisiana [ACM91, ACM97b, USE95a].

Louvain [Dan96, Q98].

Louvain-La-Neuve [Dan96, Q98].

Lovelace [KT99].

Low [Ag92, Ano99c, Bla96a, Bla96b, CFPR96b, CFPR96a, CNS99b, DDQM98, DDP99, DDGM97, DFKN93, GDD97, Goo96, Jak98, KSHW97, KSHW98, KKW99, KOT95a, KOT95b, Mil96a, Pai99b, PK95a, PK95b, Pen96, SKNO98a, SKNO98b, T99, Ano90, C9L92, DQ96, Go96a, MHW98].

Low-Bandwidth [Bla96a, Bla96b].

Low-Cost [KKW99, Pai99b, DQ96].

low-density [C9L92].

Low-Entropy [KSHW97, KSHW98].

Low-Exponent [CFPR96b, CNS99b, CFPR96a].

Low-Power [Ano99c, T99].

Low-Randomness [DDP99].

Low-Weight [PK95a, PK95b, Pen96].

Lowell [IEE98f].

Lower [BD97, CT94, OK95, Sch991, Sga91b, StI93a, vHPP93, GN95a, KO96, KO97, Shp99b].

LR [BP98c].

LSI [SKNO98a, SKNO98b].

Lu [LZ91b].

Lu-Lee [LZ91b].

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

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


Model-Checking [Bol98a, Bol98b].
Modeling [DD99, KM98a, LM96, SS99a, ZFKP98, ZFK+98, Ano93k, CM97d].
Modelling [CK95, GAGCDCAF99, HL92, LK98, NT93, PS99a, SM99, Tro93].
Models [Ben99, CH99b, DL99, DP99, Ger99a, HHD99, LL97a, OMA98, PZ98, SY99, SZT98a, TGK99, CT99b, Nis91, OMA97, SZT98b].
Models [DD99, KM98a, LM96, SS99a, ZFKP98, ZFK+98, Ano93k, CM97d].
Modern [Buc91b, Gol97a, Gol97b, Gol99a, VG99, Dam99b, Unixxa].
Modeme [Gar97b].
Modern [Buc91b, Gol97a, Gol97b, Gol99a, VG99, Dam99b, Unixxa].
Modular [BP99b, CJS91, Cop95c, HCY96a, Kor93, MNSV97, Pai99b, PRAM98, SKBxx, TY92, TN96a, TN96b, VDDR99, Yam98b, BGR98b, BCK98, CK93, HN94, ISO97, KAK96, LC98, Yami98a].
Modulation [Bi99, She94c, SC96b, KSB96b, KSB97, SVWMB95, SOB98, VS95].
Module [Mee98, Ano97-1, Modules [Ano97-1, IH98, Mor97, Com94c].
Moduli [Hub91, Len98, Mau90, Wal99c].
Modulo [DR94c, PP92a, PP95b, PP95a, Tak98a, Tak98b, Zim99, BBR99, SPP98].
Modulo-Place-Invariants [DR94c].
modulus [Tze99].
molecular [ARRW99, Ram92].
Molecules [GC98].
MON [YY98d].
Monetary [Gar97c].
Money [YY98d, YY98b].
monograph [Lea90].
Monomial [Pat96].
MONopolizingKEYs [YY98b].
Monstor [Gar98b].
Montages [AKP99].
Montana [BCC97].
Monterey [USE99d].
Montgomery [NM94, BP99b, Kal95, KAK96, Nac93, NMR95].
Montgomery-suitable [NM94, Nac93].
Montreal [ACM94c].
Moose [Ros96b].
moot [Ano96d].
Morphology [Bol99].
Morphometry [SCG99].
Morse [Sch98i].
Moscow [CW94].
Most [BV96, KAK96].
motion [Nas94, ONT98, VEA+98].
Motorola [DK91, Gar97a].
Mouth [DDJ98c].
MOV [HSSI99].
movable [GMLH94].
Moves [Weh98].
Moving [Gar98a, HHW99].
MP3 [MB99a].
MPEG [DS97b, DS97c, DSS98, HG97e, HG97d, HEG98, LT98, QN98a, QN98b, SB98].
MPEG-2 [DS97c, HG97e, HG97d].
MPEG-4 [HEG98].
MPEG-encoded [DS97b].
MPEG2 [CPO+98, CHO+98, DDMN98].
MR [DTDJ99].
MRA [BALS99, LFCK99].
Ms [CFK+91, Gar98a].
MS-DOS [Gar98a].
MSC [WSFC99].
Muller [JQ98b].
Multi [CM99b].
Multi-agent [CM99b].
Multi [BDGF97, BDD+94, BM99c, CFSY96, DFGH99, DF97, FH98, HJTW99, HV98, JV96, KSB97, Lee99b, Mar98a, PM99a, SNW98b, SJS98, Sut99, TN96a, TN96b, VC99, CL97a, CGS97, HW98c, KSB96b, SVWMB95, SOB98, VS95].
Multi-Agent [Lee99b, VC99, HJTW99, PM99a].
Multi-Application [Mar98a, DF97].
Multi-authority [CFSY96, CGS97].
multi-carrier [SVWMB95, SOB98, VS95].
Multi-disciplinary [DFGH99].
multi-exponentiation [CL97a].
Multi-function [KSB97, KSB96b].
Multi-Level [HV98].
Multi-Party [JW96, FH98].
Multi-Purpose [Sut99].
Multi-Receiver [SNW98b].
Multi-Secret [BM99c, BDD+94].
multi-senders [HW98c].
Multi-Service [HS94].
Multi-tiered [CC99c].
Multi-user [SJS98].
Multi-variable [TN96a, TN96b].
Multi-aplication [Gir99, Tua99].
Multicast [CM99b, PB99a, Mth92a].
multicasting [CM96].
multicasts [WL99].
Multidimensional [BMS99].
Multidrawing [BMRW98]. Multifeature [Bet95c]. Multifunction [She94c].
Multigroups [OOK91]. Multilevel [CGB+93, GPSN98, KT96, DN95a, ZH93].
Multimedia [ACM96a, ADF98, CKLS97, Dan96, D98, ES98, FJV97, GO96c, HF97,
IEE96b, IEE98e, IR99, KBR97, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k,
Kat97, LS98a, Oko97, PSB97]. Multitap [GMCF95]. Multipart [GMCF95].
Multipart/Signed [GMCF95]. Multiparts [GMCF95]. Multiparty [Cha90, CDD+99,
FW91, MH96]. Multipermutations [SV94, SV95a, Vau95].
Multiple [AS96, Bih98a, Boy90, DK96, GO96b, Han94, Kal92, KR94b, KR96a,
SS99c, SHK99b, Wag98b, Bih95a, GGK+99, GPSN97, KR95a, KSL92, KM98c, Ort95b,
Ort95a, SSM94]. Multiple-length [Han94]. multiple-iterated [Ort95b, Ort95a].
Multiple-precision [Kal92]. Multiplication [Abe99, KAK96, Kor93, MS93, Zim99,
FBT96, Han99, LC98, TY92]. Multiplications [MNSV97]. Multiplicative
[BBDW96, DDB95a, DDB95b, Mis97]. Multiplier [HMvT94, HWB93].
Multiprocessor [MHPS96]. Multiprocessors [Lei99b, HJ99]. Multireceiver
[SNW98a]. Multiresolution [BCV97, HW98b, SHT98a, SHT98b, XBA97,
KH98a]. Multithread [Geh94, Geh95]. Multisecret [DLR97, JMO94, WAMO94].
Multisecret-Sharing [DLR97]. Multisender [MSN97]. Multisignature
[O93, CLHL98, FD92, HZ93, HCC98, LHW99, LHL95b, LHL95a, PPKW97].
Multitude [Fuc99]. multuser [LS98a]. multivalued [CGV94]. multivariate
[M90]. Multiversion [KT96]. Munich [IEE97d]. munition [Buc95b]. munitions
[Uni97d]. Muscle [Cor98]. Musicians [MB99a]. Musings [Ins95]. must [Csi95].
Mutual [Bak99, ARK99, BO99, CS96b, CS97b].
Mutually [CGM97a, IS91, Mar97, HY93a, JMO95a, Wu92]. My [Cur98]. mystery
[Fra93]. Mythical [Sil99].
n [ISO97, TN97]. n-bit [ISO97]. Naccache [Cus97]. Naccache-Stern [Cus97].
NAFTA [Mad98f]. nag [PDPbbprm91]. Nam [CLW98]. Name
[Gar97a, Gar98b, Ano97-29, Lea90]. Nanomedicine [DDJ98e, DDJ98f]. Naor
[Geh94]. Napa [IEE93a]. Napier [CWM91]. narrow [CC98]. narrow-sense
[CC98]. NASA [CWM+91]. National [Akc97, Ano96a, DDJ98b, Dam96, IE94b,
NIS92, Un98a, W91a, W91b, R96, Un98d, VB96]. Nations [Sch98a]. Natural
[Dim94, KKL99]. Nature [IEM99a, IEM99b]. Naval
[Wei99, SW94b, Un95b, Win93]. navies
[Dal97]. NDRAM [Gar97b]. Near [Tay95].
neasy [Mra95]. Nearly [KR99b]. Neats
[Gar97b]. Necessary [MSN99, Rus93b, Rom90b]. necessity
[KK97]. Need
[DS98b, Fly97, RS98e, Van95]. Needed [RSxx]. Needham [Low95, Low96].
Needham-Schroeder [Low96]. Needs [FY99, Un98], Kir95, Un98k. negotiates
[Ano95k]. neighborhoods [Mra95]. Neos
[Pit95]. nested [BO99]. Net
[Gar97a, Gar97b, Gar98a, GB98, Got99, LL97a, MB99a, Way96a, Abe98a, BCW97].
NetBill [CTSxx]. NetCard [AM99]. Netherlands
[Cha91, Hei96a, TV94, TV92]. netlist [CKM99]. Nets
[Des98a, DR98b, KA99, YK98, NT93]. Netscape
[DDJ98g, DDJ98h, GW96, Law98, She96b].
NetTracker [Ano97-34]. NetWare [ARH95]. Network [ACM98a, BK90, Coh99, DS90a, Ebe93, EH96, Fum93, GM93a, HS96a, Kan96, Koh90, KN93, KCCT94a, KCCT94b, Law98, Lee95, Len96b, Lom94, Mar99, MSK99a, MT99b, RS99a, She93d, SVB99, SS98d, Tun99, VDDR99, VNW94, VNW95, WKH97, WN98b, Wu96, AP93, BGT96, Ha97, IS99, JJ95, SS99d, Sta99a, UCF94, Yor96, ZG96].

Network-centric [BGT96].

Network-Layer [Wu96].

Networked [Ano97-28].

Networking [IEE98e, FJV97, LS98a]. Networks [ATAY98, AWV99, BF97a, Bra90a, CT99a, DQ93, HG97c, IEE97l, IEE98f, Jut98, KR97, Lea99, LS98v, OM98, PKOT94, PT95, Por91, Sa91, SK96c, SK96d, SV94, STP93, TH97, Tow97, VSH97, Ver98a, Ano95q, Ano96j, ACBR90, Atk93, AC97, BF99b, CW91a, CW98, Fra90, GBL94, HT95, Hor94, HLL96, Jen99, LG96b, LC96c, NT94, Nor95a, O99, Opp96, PS98c, PS98d, PS98e, PS98f, PS98d, PS98a, PS98c, PS98b, SV95a, SBT99, Zan90].

Neuman [HLL+95]. Neumann-Stubblebine [HLL+95]. Neumann [CFK+91].

Neural [Mar99, ACBR90, SBTV99].

Neuro [ZHJ98]. Neuro-Fuzzy [ZHJ98].

Neurocybernetics [Mor98]. Neuropathy [MR95a].

Neuve [Dan96, Q+98]. Nevada [ACM95, AA97]. never [Mon96]. NewDES [KSW97a, KSW97b]. News [Ano93e, Ano94a, Ano95p, Ano97-29, Ano97-33, Bar97, Bar96a, DD98e, DD98c, DD98f, DD98a, DD98d, DD98b, DD98g, DD98h, DD98i, Er97b, Fox99, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, GB98, Go99, GO96c, Law98, Lea99, MB99a, Ros98b, T997, Taa98, WSFC99, Wor96, Bra90b].

Newton [AVPN96, Ber96b]. Next [Kal97b, SS91].


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

NIKS [Cop94b]. nine [Tat98, Tat99].

Nineteenth [Alv98c]. Ninth [Ano95r, IEE93c, IE94b, T+98, ACM97c, LL93].

NIST [Bra93a, Dha98, Nat92a, RHAL92, Riv93c, SB93]. NISZK [GSSV99]. NJR [TGK99].


Nomikos [IEE97c].

Nominations [Nat97b]. Non [AVW99, BM90, BG90, BS99b, BS99c, BS91b, DY91a, DDP98, DR94c, DNN91a, DNN91b, FCD98, FDB93a, FDB93b, GPT91a, GPT91b, GP99, GO93, HJPT98b, Jak98, KR96c, LW99, Mas99a, MY91, NO98, Pai98a, Pai98b, Ped91d, Ped91b, RS91, Sah99, DY91c, SCC99, TSY98, Yah94, Ano95q, BKR98a, BKR98b, DDB95b, Ell97, HJPT98a, LL98, MY93b, SB95, Sin95, SBT99, DDB95a].

non-Abelian [DDB95b, DDB95a]. Non-biased [TSY98].

non-carcinogenic [SBTV99].

Non-classical [Mas99a].

Non-Commutative [GPT91a, GPT91b]. Non-Encrypting [LV99]. Non-Euclidean [SCG99].

Non-Existence [FDB93a, FDB93b]. Non-Interactive [DY91a, GO93, MY91, BM90, BG90, DDP99, Ped91d, Ped91b, RS91, DY91c, MY93b, Sah99].

Non-invertible [NO98, BKR98a, BKR98b]. Non-linear [FCD98, Jak98, KR96c, LLB98].

non-linearity [SB95]. Non-Malleable [DNN91a, BS99b, BS99c, DNN91b, Sah99]. Non-maximal [HJPT98b, HJPT98a].

non-Oracle [Ano95q]. Non-perfect [Pai98a, Pai98b]. Non-Reachability [DR94c]. Non-repudiation [GP99].

non-secret [Ell97]. non-secure [Sin95].
Noncryptographic [Fei99]. Nondeterministic [Mo98].
nonce-based [KSL92]. Noninteractive [GSV99, Ped91e]. Noninterference [MC92].
Nonlinear [Gys96, KT91b, MS99b, Pit95, Gol99c, RD96b]. Nonlinearity [MS90a, SZ95c, SZZ95a].
Nonlinearly [MS94]. Nonmonotonic [COM99].
Nonoblivious [FNSS92]. Nonperfect [KOS +94, OKT93, OK98, OK95].
Nonrecursive [Ruo94]. Nonrepudiable [LHW98].
Nonrigid [Nas94]. Nonsecret [DDJ98g, DDJ98h]. Nonsense [FJM +96].
Nonsupersingular [BS91a, MS93]. Norm [TK99].
Normal [Bra90a, Ran01, Mok97]. Normalisation [ZTR99]. Norway [Hel94, LW96].
Norwegian [PP96, Sel94, Sel98b]. Not-So [Ano99e, CM99c, Chr99a]. Notable [Bar94].
Notarization [SK97b, SK97a]. Notation [Sch99c]. Note [Ano95i, Ano96k, Ano97q, Ano97a, Ano99j, Bih99c, BPK99, EKK99, KM92, Roh99, Blu95, CJR99b, ES97, GH993, LM93c, MS98a, TX92, YL97a, Yu92].
Notepad [Ano93k]. Notes [GB98, KSF99, KSF00, WN94, Dwo95]. Nothing [BMM99a, BMM99b, Boy99, GMW91, Riv97e, SRY99, Ste98b]. Nothingness [Way96a]. Notions [BDPR98, BS99b, BS99c]. Notwendigkeit [KK97]. Novel [Ger99a]. November [ACM93a, ACM94a, ACM96a, ???90, Ano94e, Cli97, DEQ92, GN95b, HOQ97, HF97, IEE91, IEE92b, IEE971, IEE98a, IRM93, KM96a, LOX99, PSN95b, USE96d, USE96b, USE99b, UU97b, XiTnW94]. Nox [Ts'90]. NP [BD91, DDP99, DFK93, GMW91, NOVY93, Sch94k].
NP-completeness [Sch94k]. NRC [Wor96]. NSA [Mad99b]. NSK [PP96]. NSN [Uni94a, Uni94b].
NSW [GN95b, KG93, VPM97]. NT [Bru98, Ano96v, Ano98s, Hi97, IH98, USE99a].
NTRU [HPS98]. Nuclear [HRV99]. NULL [GK98]. Number [Abe98a, Aga92, ARV99a, ARV99b, BG98, BGM97a, BGM97b, Bir98, Bor95, Buc91a, BP97c, De 98d, JK99, KSW98d, KSF99, Kob94, LLM90, LL93a, Lox90, Mat96b, Miy93c, PG90, ROT94, Sch90c, Sch97c, Shp99b, WI99, BMxx, Bou94, CS97c, CB96, Cou99, CDEH +96, Cus96, CS96c, Gor93b, Jenxx, Kali93b, KSF00, Kos99, KKI98, Lag90, LLM93, McC90b, Mei92, O'C94, Pom90a, Pom94, PP92a, PP92b, PP95b, PP95a, PR99b, Rev91, Shp99a, Sin99, SB99. Tat98, Tat99, TSY98, YT96]. Numbers [Cha93, Ell98, Gut98b, Kra99, Mac94, MSN99, Pin97, ST91, GK95a, PGCSN96, Yan95]. Numerical [She92e]. Nuts [Net98]. Nyberg [NMV98]. Nyberg-Rueppel [NMV98].

Oakland [IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, USE96d, USE96b]. Oakley [CH97a].
Object-Oriented [AK94, BDPSN95, BDPSN97, DS99, Ou99, PD99a, SG99b, BGV97a]. Objects [CK95, GS98, HHW99, Kem99, YY99a].
Oblivious [Bla96c, DF99, HHY93, Mic97, NP99, Bea93, BM90, BR96b, DOR99, GO96a, JY96].
Observation [MM99c, Mur99, Bih98b]. Observations [BBDR99, WKS+99].
Observers [CP93, DT98a, NT99]. Obstac
Obstacle-avoiding [ZW99].

obstructs [Roe97].

obtaining [CLHL98].

Ochrona [Sch95e].

October [Ano93d, Ano96a, Cha91, FM91, IEE93a, IEE94a, IEE96a, IEE96d, IEE97f, IEE97h, IEE97j, IEE98f, IEE99a, NIS92, Oht96, OiDP98, TV94, USE93, USE96a, Ame95].

Odds [McC90b].

ODEs [Ruo94].

ODMG [Wat99].

OECD [Org98a].

Oench [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AG95, Ano94i, Ano96-29, Mao98, Riv98c, VNM99].

Off-Line [Bra95b, DT98a, EGM90, EGM96, Tra99, Mao98, VNM99].

offer [Mar96].

offered [Ano96y].

offerings [Ano99d].

Offers [Gar97a, GC97, Sav96].

Office [Fuc99, UU97a, Uni96b].

offs [BFS96, BMS96, NMVR95a, NMVR95b].

Ohio [Dal97].

Oil [KS98d, KPG99].

OK [Gar98b].

Okamoto [Hwa92a, MS98a].

Okamoto-Tanaka [MS98a].

Old [IEE94a, Mar96].

Olympiad [DDJ98b].

Olympic [Mye96].

Omnidirectional [Pj99, SKIT99].

Omura [HWB93].

On-LAN [Ano96v].

On-Line [Cac95a, Cac95b, CDFI95, Ell99, EGM90, EGM96, PUF99, Saw96].

official [Zim95a].

offs [BFS96, BMS96, NMVR95a, NMVR95b].

Ohio [Dal97].

Oil [KS98d, KPG99].

One-Bit [MSN99].

One-Key [Gys96, Tao94].

One-round [Wet93a, Wer93b].

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

One-Time-Password [New98].

One-Way [BJ97, Bdn94, BM94a, BKK98, DGV93, DDP90, Roe94, Sch91h, TOU94, Zhe90, BHHRR99, HILL99, HILLY99, Rom90b, BK98f, DIF99, Dob98, Hwa92a, IEE92d, MB94b, MZI98, Roe95, Sim98c, Ste95, Sze98, Tao94, Tsu92b, Tsu92a, Wer93a, Wer93b, ZPS93, MAM95].

One-Key [Gys96, Tao94].

One-round [Wet93a, Wer93b].

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

One-Time-Password [New98].

One-Way [BJ97, Bdn94, BM94a, BKK98, DGV93, DDP90, Roe94, Sch91h, TOU94, Zhe90, BHHRR99, HILL99, HILLY99, Rom90b, BK98f, DIF99, Dob98, Hwa92a, MZI98, Sim98c, Sze98, Tao94, Tsu92b, Tsu92a, Wer93a, Wer93b, ZPS93, MAM95].

opening [Bur94c].

Open [AT99, BCE94, Con99a, DMVC99, GS97, HVH98, Lac98b, Muf93, Gen99c, Hor94, SY96b, Sta96b, Con98, Dra99].

OpenBSD [dRH99].

OpenGL [DDJ98e, DDJ98f].

Onthology-Driven [CHLT99].

Ontology [ADBB99, Gua99, Mee99].

Oorschot [Sha99a].

Op [MGL+98].

Op-Ed [MGL+98].

Op-Ed [MGL+98].

OpenPGP [CDFT98].

OpenCard [DT98b, HH99].

OpenGL [DDJ98e, DDJ98f].

Opening [Bur94c].

One-way [HT99].

Onion [RSC98, SGR97].

Online [FL99b, Jan98, MGL+98, MB99a].

Only [BK98d, TOU94, MRS99].

Ontario [GS94b, HA00, IEE96d, SIJ93, TM99].

Omnidirectional [Pj99, SKIT99].

Op-[MGL+98].

Op-Ed [MGL+98].

OpenCard [DT98b, HH99].

OpenGL [DDJ98e, DDJ98f].

OpenPGP [CDFT98].

OpenCard [DT98b, HH99].

OpenBSD [dRHG+99].

Operator [Uni94a, BP98c].

operators [BP98b].

Ophthalmical [FCD98].

OPIE [MAM95].

Op-Ed [MGL+98].

Opener [YY98].

Op-Ed [MGL+98].

Op-Ed [MGL+98].

Opportunistic [BR99].

Opportunities [MBB98].

oppose [Mad99b].

Optical [DHQ98a, FVEA99, HLMP96, Tow98, van96, van97b].

Optical [DHQ98a, FVEA99, HLMP96, Tow98, van96, van97b].

Optical [DHQ98a, FVEA99, HLMP96, Tow98, van96, van97b].

Optimal [BP98a, BR94b, BR95a, BJ97, BM96b, BM96c, Car94, FGMY97a, HKS97a, HKS97b, LC95, PRS99, PLWSN99, ST94, SW97a, SW97b, Tai95, BJ97, DP94, LL93b].

Optimality [Mas99b].

optimally [CGS97].
Paranoid [GGOQ98]. Paranoids [Sha95b]. Parasites [NMR95]. Park [Ano99c, Wei94, Ano97-48, Cla98c, HS93, Sa93, Sm98b]. Parity [AA95, ANS97, Acc97, ECM96, Fri92b, ISO97, Lin88a, Lin98a, Lin93a, Lud97, Chi97, UU97b].


Passport [MGL+98, vL96]. Password [Ber98, Bis92, Bla98, FIP93a, HK99a, Hor95, Jas96, Kle90, KS97c, Lee96, LT91, New98, Pop96, PM99b, RSA99b, Sch99a, BSN96a, BSN96b, BCR98, CW97, HJT+96, JC98, MW94, ZH93, KW92].

Password-Based [RSA99b, BSN96a, BSN96b]. Passwords [De 90, MAM95, Neu94].

Patent [Uni96b]. patents [Lev91]. Path [MPPS95, RS98a]. patient [Cha99b].

Pattern [Des99a, PNFK95, WD99b, Sch91b]. Patterns [Lut98]. Patterson [MSS93].


[SZT98a, CM97d, SZT98b, SZT98c]. perceptually [KL95b]. Perfect [BK95b, BS91g, DDP94a, DF93, vD95a, Joh94, JR96, Man91c, MW94, MK92, NOV93, BD98b, DP94, Pai98a, Pai98b, SC97, TSN93, vD95b]. Perfectly [BDK93]. Perfectly-Secure [BDK93]. Performance [ACM98a, Ano95b, BMS99, DMPW98, FC94, GN95c, HJL99, HWJ98, IEE94e, KR96a, Kea99, LL95a, LM98b, PRB98b, Roe94, Roe95, SKW+99, SKW+99a, SKW+99b, She92e, Sma99, Sut99, Tou95, VNN94, Wie98b, Nor95b, NO96, SSI98]. Performer [KS98b]. Period [RH99].

Periodic [Mun91a, Mun91b, Abe98b]. periods [GvP98]. Perl [DDJ98a]. Permit [Joh94]. Permits [Gar97b]. Permutation [BM92, BS90b, CT99a, EM93, Hm94, Pa99c, Pat99, CSV94, HT95, O'C95, Pat91b, Por93, Zan90].

Permutations [BY93a, DW94, FJRS96, SP97, CCZ98, Pat91a, Pie93, Sha94, SM98b]. Permutated [BCCG93, KM99b]. perpetual [HJK95]. Persistence [DL99]. Person [BBDF97, Ble98b, DLF97, DMFB97, WKHG97, CBC97]. Personal

[Ano97-34, BE90, Bar95, Cae96b, EHMS99, Gar97b, Ham97, Los97, Los98, RSA99a, Riv98, Cra96, Mil95, Wil93a]. Personified

Personalized
Perspectives [GO96c, Riv97b, Bro96, LKB+94].

pertaining [Cha94b]. Perugia [De 95].

pessimistic [Kru98]. Petard [WG97].

Peter [vdWS97, vS97]. Petho [Laˇs92].

Petre [CFK+91]. Petri [DR98b, KA99, LL97a, NT93, YK98]. PGM [HMvT94, MMT90, MM90a, MM90b]. PGP [An97-34, An97-35, ASZ96, Elk96, End97, Gar95, Gar98c, Joh96, Kar96, Ken95, MR98, MLLG95, Ros95a, Ros95b, Ros96a, Ros96b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, SA95, Sta94a, Sta95a, Sta95b, WCS95, WT99, Zim95a, Zim95b]. PGPmail [Pre97b, Pre97c]. Phantomic [Lip93]. Phase [BGV93, Chi92, ODB96, HY95]. Phases [Tou92].


Piloting [KW92]. Pinyin [OS91].


Pitfalls [Sch98f, SZZ94b]. pixels [BD98b]. PKC [IZ98]. PKC’99 [IZ99]. PKCS [Ano95p, Ano96-28, Ano97-44, Ano98r, Ble98a, Kal97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, Nys99, RSA93d, RSA93b, RSA93c, RSA93e, RSA93a, RSA99b, RSA99a]. PKCY [XW97]. PKZIP [BK95a]. Place [DR94c, Des98a, DR98b, Ano95c]. Place/Transition [Des98a, DR98b]. Place/Transition [FL93]. Plain


Point-to-Point [SM98a]. points [KK98, MVZ93]. Poker [KKOT91]. policies [Ano96-31, Ano98v, HK99b]. Policy [ACM94b, And96a, Ano96i, Bar93a, Bar93b, CPOR97, Ell99, Gar99, Hat96, Wai95, Aus96, Abr97, Ano97-31, Ban94, Bro96, Buc95a, Dam96, DG96, Ele99, Eng95, HAHH94, Hof95, LKB+94, Mad96, Mad98d, Mad98e, Mad99a, Rot95a, Tas98, Wad98, Zaj97].


Polynomial-Time [Sho97]. Polynomials [CE96, She95c, CW91a, CGMW97, Ito91, Kob91c, LC96b, Od94a, LC96c]. POP3 [Mye94b]. POPL [ACM99a]. popular [KAK96]. porpoises [Ano96-29]. Port
[Mei98]. **Portable**
Smi98a, BY93c, BY93b, Car94]. **Porting**
[JJ91]. **Portion**[Len98]. **Portland**
[Auc98, USE90]. **Position**
BFK99, CM99c, YST99a. **Positive**
Dwo97, YY98a. **Possibilities**[Jam98]. **Possible**
Cae96b, MW96a, Ano96n, NM96b]. **Post**
AA93]. **Post-Markov**[AA93]. **Postage**
TY9H6]. **Potential**
GQW+91, Nor95c, Uni96a. **potentially**
Knu95]. **Potomac**[Ros97]. **Power**
Ano99c, BS99a, CJRR99a, KJJ99, MDS99, PRAM98, SKNO98a, SKNO98b, Sha99b, T+99, Goo96, SOB98]. **Power-Analysis**
[CJRR99a]. **PowerPC**[UFC94]. **powers**
SS95a]. **pp**[Ano97-48]. **PPP**
BV98b, Kas96, Kumi98, LS92, Mce96a, Sim96b, SM96b. **PPTP**
[SM98a, DDJ98c]. **Practical**
ASW99, ADDB99, AB96a, AWV99, Auo98, Bac95, Bowxx, CDD99, CS98b, Dam91b, Dam94b, Dam94a, D93, F097, HBKL99, IH99a, Jue99, KTM+99, Oka93b, v091a, PIR99, PV90, Sak97, Sch92a, SW93, Smi90, Sta96d, Z93, v091b, And93, AM99, BI93, Bou94, Fra90, F003, FO98, HZ93, HNM98, HJJ99, Jac90a, Jac90b, J99, LL95b, PS98b, v092]. **Practically**
[Gut98b, Knu94a]. **Practice**
Bel99, DS99, G95b, IZ98, IZ99, LABW92, AN94, AN96, Dam99b, Ger97, LABW91, Sch93a, Sta99a, St95]. **Practice-Oriented**[Bel99]. **Practices**
[Des99a, JJ98b]. **Prague**[Ste99b, wVN99]. **pratiques**[Bou94]. **Pre**
DO99, H97c, Zim96a, Zim96b]. **pre-alpha**
Zim96a, Zim96b]. **Pre-compressed**
[H97c]. **Pre-processing**[DO99]. **Preassigned**[SW99b]. **Precautions**
[GQW+91]. **precision**[Kal92]. **Precomputation**[LL94b, dR95]. **Predetermined**[Len98]. **Predict**[Kra90]. **predicting**[Gil97]. **prefix**[MPL99]. **Prefix**[ADD99]. **Preliminary**
BC93a, BPBV99, DY91c, Zim96b]. **prelude**[Unixxa]. **Preneel**[WBDY98]. **Prepares**
[Law98]. **Prepositioned**[Sim90b]. **Preprocessing**[dR94b, dR94a]. **Presence**
BDHJ98, CH94a, CHH97, Cra98, Gar94, JQBD97, Cra97]. **present**[Sim94c]. **Presentation**[K99, LS98a]. **Presentations**[HMT+98]. **Presented**
[DBGV93, N99a, Ano95r]. **presents**[GLC98]. **Preserving**[NKP99, D199]. **President**[C197, C199, UU97b]. **pressed**[Ano96t]. **Pretty**[Ano94i, El96, Gar95, Mei96a, Ros97a, Zim96a, Zim98b, Gar98c, SSI97a, SSI97b, Sta94a, Sta95a]. **Prevalence**[YY97b]. **Preventing**
[Jas96, SHK99b]. **Prevention**
[OG97, VNW94]. **Previously**[DH90]. **PRFs**[HWK99a, HWK99b]. **Pricing**
DN93, Ros94]. **Primality**
[Ans90, K99b]. **Prime**
[LO91a, Sho97, Boy97, DLP93, Graxx, ML98]. **Prime**[Sch94d, Di 97b]. **Primes**
[BD93, GS99b, Lan99, Mil94, Riv91a, RS98e, RSxx, Si97b, Si97a, DL95, YY99]. **Primitive**[SI94, She95c, J98a]. **Primitives**[CF99, Pre98c, RIPv9b, RIPv9a, VCF+90, ZM91, BFKL94, BP95b, Di 99]. **principle**[Dam90b, G99]. **Principles**
[ACM99a, AN95, HGHD98, K99a, KG99, MG91, PR98a, Zhe90, Sta99a]. **Printer**
[Con93]. **Privacy**
[Ano94i, Ano95c, Ano97-34, Avo98, Bac95, BBCM95, Ble98b, Car96, Cha92b, DL98, El96, FJP96, FHM98, Gar95, EE92c, EE93b, EE94d, EE95b, EE97i, Ken93, KFJP96, Lin88a, Lin89a, Lin93a, Lut98, MW97, Mjo93, NKP99, Par99c, SY96a, SYMI98, SB97, GS96a, Sta94a, Sto98, Tho96, Tra99, Uni98a, Uni98i, Ada92a, Ban94, Bro96, CM95, Car94, Cha92a, CK93, Cl99, Dom96, HM96, JMLW94, Mar95b, Mei96a, Mil95, Rot95a, Smi94a, Sta95b, Uni98d, Uni97c,
VPM97, Zim96a, Zim96b, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, Zeg93].

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

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

Private-Key [HR90, Mv93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS98b].

Privilege [ECM96].

Prize [GC97, Pin98].

PRO [Ano97-33, Gar98c].

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

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

probabilities [Lew92].

Probability [BDG99, Gol96b, Kob99, TY94, AI 96, MMHW98, MAO96, WM93].

Probable [BD93, NK93, DL93, Graxx].

Problem [Bon98b, Bon98a, BN96, CS96a, Cha90, DD99, DJL93, GO95, HK90, Imp92, Lon91, TX92].

Provable [HRS99].

Problem-Solving [Per99].

Problems [AA93, BD95a, Bra90a, GGH97b, KR999, MC92, Poi99, Smi90, APDS93, Bea92, BFKL94, FR95a, Han95, Han99, HCM95a, 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, Ano95r, Ano98a, Bri92, Bri93, Com96, GN95b, IEE95a, IEE95b, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96e, IEE96d, IEE97b, IEE97e, IEE97j, IEE97k, IEE97i, IEE98e, MZ98, Nat99b, OW95, PSN95a, Pit95, Sti93b, SJ93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96e, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94e, Bih97c, B+96b, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fum97, Go190b, HOQ97, HA00, Hir97, Hir98, HF97, IEE92a, IE94b, IE97b, IE97e, IE98a, IE98d, IE98f, IZ98, IZ99, KM96a, KG93, Knu99c, KP99b, KK99b, Kra98, LOX99, LM98a, LW96].

proceedings [Lom97, MV91, Nyb98, OiDP98, Pre95a, QV90, QG95, Q+98, Rue93, ZS93, Spi95, Ste99b, TM99, TV94, T+98, Tv92, USE90, USE98d, VPM97, Van98e, Wat91, Wie99, Wol93b, Yua92, vWN99, ACM93b, CH96, Chr99b, IEE94e, Sti94, Wal99a, BCB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fe91, Go196d, GQ95, GS94b, He94, IRM93, Kal97c, Knu99a, GO96c, KSWH98a, KSWH98b, KSWH98c, GN95a, SS98b, Ano94i].

Products [Ano97-33, Ano97-34, Cha94b, Cli97, Los97, UU97b].

Professor [Swi97].

Profile [Hor92, HFPS99, MM90a, MK92].

Program [BDFM99, FGY96a, LMCM94, FGY96b, KT99, LS98a, Pre97b, Pre97c, Uni95a].

Programmable [DMVC99, SVB99, TT99, WB94].

Programme [BG93].

Programmer [Bre99, DDJ98a, Jol95, Ste94b, vdWS97,   }
Programmers [Gar97c, Joh97a, Joh97b]. Programming [IBM93, BGS96, CO98, Eri97a, JDK+91, Ste90a, Ste90b, ACM99a, Gre98, LS98a, QA99, Sab94, vWN99]. Programs [BK95c, DRR95, SG95, SHK99b, WB95, Zwi98, B+96b, DFHR91]. Progress [Ano96-28, Ano97-45, BDI+96, KSB96b, Woi93b, Woi93a]. Progressions [Miih94]. Project [BPBV99, IBMxx, GH96, Man98, DS90b, RCM99]. Promise [Law98, Los97, Mar96]. Progressions [Mih94]. Project [BPBV99, IBMxx, GH96, Man98, DS90b, RCM99]. Promise [Law98, Los97, Mar96]. PROMIS [SSCP99]. Promise [Law98, Los97, Mar96]. PROMIS-MmNet [IEE98e]. Promise [Law98, Los97, Mar96]. PROMS [IEE98e]. PROMS-MmNet [IEE98e]. Proof [Bol98a, Bol98b, CD99, CDS94, FO091, GMW91, GK96, NMY99, RS91, Zhe95b]. Proof-Based [Bol98a, Bol98b]. Proofs [BG90, BG93, BD91, CD98b, DFKN93, FS97b, GMW91, GO93, JMS96, CP95, DP94, Go99a, PS96d, Sak97]. Propagation [GPR98, SG99b, ZZ95c]. Properties [Boy99, Con99b, KA99, MM90b, MS91, OK98, OS98, Tou93, VW98, WW98b, Zie97, BHRR99, CD95, FSS94, KSB96a, Kob91a, PS93a, ZZ95c]. Property [CFGS99, DL90, LQR99, SRY99, Uni97b, Ale98, BS95c]. Proposal [ABK98b, ABK98c, ABK98a, BAK98, DR98a, KR94a, LM91b, Ano95n, Cli99, LM91a, RH92, RRR98, Ban94]. Proposals [Dae99, VvT97]. Propose [Gar98b]. Proposed [CP91, Lea99, LL98a, Nat92a, Riv93c, SB93, Wag98b, C96, Gu90, Mey96b]. Proposes [Gar97a]. Prosthesis [HHD99]. Protean [SV99]. Protect [Sch94, Sta95b, Cli99, KR96b, Way93b]. Protected [CH94b, DY91f, Mad98b]. Protecting [BO96a, Ble98b, Des90a, EHMS99, GMD98, KRJ98, Lut98, Mar95b, MW98b, PT95, SYM98, Tr99, VP99]. Protection [BG95, CHN97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LQ98, 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, Tev92, TSN93, Uni97c, YEA+98, FT95]. protections [HPA99]. protects [Ano95m, Ano96j, Ano97-43, Ano98d, Ano98s]. protest [Ano97-52]. Protocol [ATAY98, Ano95a, BWM99b, BV98b, Bra95a, Bra96, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JMP+98, JQ97, Kas96, KSW98a, KSW98b, KS98b, Kra99, Kum98, Low96, Mau94, MW99, Mey96a, Moo92, NS98b, NS98c, OMI93, RS96a, RS98b, SSN98a, SH97, SM98a, SM95a, Sim96b, SM96, SM98b, Ste98b, WS96a, WS96b, AP93, Bee93, Bol97, BO99, CM96, CTS96, Des96b, EvH93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS98f, SK97, Sim94b, TH99, WS97, WL94, Zhe95a, GM93a, Sar97]. Protocols [AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BG+91, BWM98, BWM99a, BBCM93b, Ble98a, Bol98a, Bol98b, BD97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dan99a, DGT96, DQ93, DS97d, Fei93, Fei96, FBS97, Fum98b, GM93a, Geh95, GS97, GMV98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IEE98e, KK97, K92, K92, LY93, LL97a, LHB96, LL95a, LS92, LM96, MB94a, MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, SL93a, Sch94a, Sch96a, Sch94h, Sch99k, SSP90, Syv92, Tou91, Tou93, AN94, AN96, AG97b, AG97c, AG97a, Aba99, ABC+98, BDH97, BH93, BCK98, BGH+95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, CJ95, Dan97, FGH99, Fe99, GEL98, Hor98, HLL+95, JW01, LY93, LH99, LL95b, Lom97, Man95, Mas97, MLY93, Mea95, MW98c]. protocols [NT93, PS98c, PS98e, PS98f, Pau98, PW93a, PKM97, SGG99, SYv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].
prototypes [Ano96-30]. Prototyping [AKP99].
Provable [Bel99, CT99a, GEL98, Mat96a, Mih94, Sz96, Van98b, BOGG+90, Mol98].
Provably [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, LM95, Mau91d, Oka93b, PS96c, Sho96, ZM190, BH93, Dam94a, FO98, Gol90c, NY90, PSW95]. Provably-Secure [DY90, DY91d, DY91b, Mau91d]. prove [Zha96]. proven [DS93, Lea90]. Prover [DY91a, GPSV98, HB99, DY91c, DFKN93]. provers [JY96, Ped91a]. Provide [BDR+96, SA95, Ano99i, Ano99h]. Provider [Tre99]. provides [MHMW98].
Proving [Bos90, DR94c, DE99, FK99, DF91b, FHG99].
provisions [Cli97, UU97b]. proxies [LC94].
Proxy [GP99, Jak99e, LHW98, Zha98, BBS98b].
PRPs [HWKS98a, HWKS98b]. Prudent [AN94, AN96]. Pruning [AP94]. Pseudo [BG98, BGM97a, BGM97b, Imp92, MS95f, NR98, PS98b, Bou94, TSY98].
pseudo-aléatoire [Bou94].
Pseudo-Random [BG98, BGM97a, BGM97b, MS95f, NR98, Imp92].
pseudonymous [GGK+99]. Pseudonyms [KRJ98, Mjo93]. Pseudorandom [ARV99a, ARV99b, BC96b, BCK6c, BGK99, EM93, HILL99, KSWH98d, KSF99, Lag90, Mac94, Pat91a, Siu99, ZYWR91, BGR95, KSF00, Kos99, Pat91b, Rev91].
Pseudorandomness [Kob99, Lub96, LLG10, BCKx, Gol99a, MM94].
psychoacoustic [Til98]. Psychovisual [DDM98]. PTY [LT98]. PTY-Marks [LT98]. PUB [Nat95, Nat99a, FIP93b, NIS93b]. Public [ANS97, ANS98b, Ace97, AKP96, AN95, IBM93, Ano96w, Ano96-30, Ano99j, Ano99l, AA93, BP98a, BI95, BDHJ98, BDGI98, BCE+94, Bec99, BC95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BFK99, Ble97, BF99c, BS94, CC99b, CG99, CIS91, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De 93c, DP98c, Di90, El99, FY95a, FY98a, FYM99, FQLP96a, FQLP96b, FO99a, GHY90, Gal96, Gar96b, Gib91, Gib96, Gir91, GGH97b, GH99, HK99a, HGS98, HP98a, HY93b, HLM93, HL93b, HJ1+xx, Has97, HPS98, HPFS99, IZ98, IZ99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKOT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Mau93a, Mau97a, Men93, MM96b, Mic93a, Mic93b, MM98a, MM98b, NS97a, NY90, Noc91, Nec96].
Public [NS99a, Odi94b, Oka94, OU98a, Omu90, vO91a, PS97, Pat99d, Pat95, Pin97, Poi99, RASA94, RCM99, Rud91, Sal90, Sal96, DP91, Sas99a, SE96, She94d, Sm93b, ST91, Sun98a, Sut99, TAP90, TA92, VHS97, dwQ91b, Wie98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zin96b, dwQ91a, vO91b, AA95, AD97, AD99, Ano90, ADSW99, Bae94, BI94, BD98a, BS97, BS91a, Bnt94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cs95s, Dw92, Dam96, Den90, DQ96, Dhe98, DN95b, ES97, FGMY97a, GH96, Gib95, He92, HWF96, HJ1+79, JM96a, Jar96, Jon90, KASH90, KM99a, Kir95, KM99d, Kos99, LG97, Las92, LMJW93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LCL95, Lon91, Lon92, Low95, MI90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rac90, Roe99, SW95a, Sch92c].
Public [Sha95a, She96a, She92c, SM90, SS95b, SS95c, Sta94a, Sta95a, Sun91a, Tab94, TCC97, TC97, TC99b, TC99a, Tze99, Ven92, Wan92b, Wil93b, Xie92, Xie93, XLP99, XX97, Yu92, Zha91, vO92, vT90, BFS92b, HMT+98]. Public-Key [AKP96, Ano99j, Ano99l, AA93, BP98a, BHSV98b, BHSV98a, BDPR98, Ber97c, BMS94, BPK99, BFK99, CC99b, CJ91, Cra98, Cus97, DP98c, Di90, FYM99, FO99a,
GHY90, GGH97b, HK99a, HGS98, HP98a, HMV93, Hes97, Iss90, Kal99, KM99c, KT91a, KMOV91, LM94b, Low96, MY91, Mic93a, Mic93b, NS97a, OU98a, vO91a, PSR97, Pai99d, DP91, Sasa99a, ST91, Sun98a, Yia98b, Yam98b, YST99a, YST99b, Ano96w, Ano96-30, BFS92a, FGLP96a, FGLP96b, GH99, HY93b, NY90, Nec91, Sal90, Sal96, Smi93b, Yam98a, AD97, AD99, BMP97a, CC99a, Cle96, Cra97, DPs99, Dhe98, DN95b, ES97, FGM97a, KASH90, KM99a, KM99d, LM94a, LZ91a, LDW94, LCL95, Lon92, Low95, Man91b, MY93b, NM96a, Ole95, SW95a, Sch92c, Sha95a, SS95b, SS95c, TC99b, Tze99, Ven92, Wan92b, XLP99, Yu92.


Refunds [Hir93]. Regarding [Roh99, CJRR99b]. Regional [ADEDS99]. Register [CS96b, CS97b, GN95a, GM91]. Registers [GO96b, Gol94, GO95, GK95a].


Regulated [Way93c]. Replicating [HS96b]. Replication [BLM94, Pit96b]. Reply [NC97, BMP+97b]. Report [Bra93a, BDI+96, Dra98, EMMN98, Kui91, Nat99c, Par98c, PH91, RIP95a, RD99a, Tou95, Vau99d, Wor96, Ano96o, BFS92a, BP95b, Bur98a, KB96b, NBD+99, Org98a, RIP95b, UU97a, Zer96a, Dan95, BFS92b].


Representations [FC99]. Representatives [Cli97, Uni97a, Uni98c, Uni98d, Uni98e, Uni99c, Uni99f, Uni99g].

Required [BGS95]. Requirement [Sil97a]. Requirements [Ano97b, BD92, Bel92, BC95c, FR95d, HJTW99, HH94, VW98, Com94c, MW98a, SM95b, UNU94].

Research [Ano99c, Boo96, DDJ98c, Dam96, Des92, Des98c, DEQ92, Ele98, IEE92e, IEE93b, IEE94d, IEE98d, Jan99, Q+98, Rhe93, Wol93b, Ano97-52, Wol93a].

researching [Uni96a]. Resend [Ber97c]. Reserve [Ano97-42]. Resharing [AGY95b]. Residue [KKOT91, PP92b, CB96, PP92a, PP95b, PP95a]. Residuosity [Pai99d, DDP94b].

resilience [FGMY97a]. Resilient [BGS94, BGS96, MS99b, RS98a, GHS93].

Robustness
[AN95, MMST98, YMWP99, Irw98].

Rockland
[GS94b]. rocky [Ano97u].

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

Role-based
JJ95.

Role-Centered
VC99.

ROLLING
PWU99.

ROM
Ano96r, GTGW94, Ros94, UFC94, Yuv97.

Roman
Has95.

Rome
Knu99c, Nat99b, Wol93a, Wol93b, DDJ98b.

ROMs
GTGW94, UFC94.

Ron
Riv93a, Riv95a, vdWS97, Woe97, vS97.

Roosevelt
Kah98c.

Root
Cop95c, JJ91.

Rooted
PB99a.

Rooted-Tree
PB99a.

Roots
Kob97.

Rosemont
IEE97g.

Rosenheim
Sha99a.

Rosenheim
Sha99a.

Rots
Kob97.

Rough
Mic93b.

Round
Bas98.

Round1
BV97.

Rounds
[BS98, Bas98, BV97, BV97a, BV97b, BV97c, BV97d, BV97e, BV97f, BV97g].

Routers
DMVC99, Ano96x.

Rover
[BS98, Bas98, BV97, BV97a, BV97b, BV97c, BV97d, BV97e, BV97f, BV97g].

Royal
Far93, Tv92, Don98.

RPC
Er93.

RSA
[Ano94b, Ano95f, AA99, And93, Ano95d, Ano95e, Ano95a, Ano95p, Ano95s, Ano96b, Ano96c, Ano97f, Ano97g, Ano97x, Ano97-38, Ano97-41, Ano97-39, Ano97a, Ano97-40, Ano98b, Ano99a, BTD98, BQ95b, BQ95a, BR95a, BR96c, BJQ97, Ble98a, BF79b, BV98c, BD99b, Bon99, Bra95c, Bri90b, BM94c, Ca99, CH97b, CH98, CB96, CLL99, CMTNY94, CD91, Cle96, Coc97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, CS97, Dav95, Dem94, DDL994, DN95b, Ev91, Ev92, Ev93, Eva90, Fia97, FS97b, FGM97b, FMY98, FY98b, FR95b, GJKR96b, GKR97, GGOQ98, Gil99, GM97, GTS90, Gro94, GS99b, HN98, HUF96, Hor98, Hub91, HP94, IM93a, IM93b, JQ97, JQBD97, JQ98a, KR95c, Ka97a, Ka98b, KS98a, Kir95, Koc94, Koc96a, Koc95, Koc96b, Koy95, KOT95a, RSA, KOT95b, KK96, Len98, LHL94, LL95a, Lon91, MWB99, MLY93, Mau90, MW98d, MW98c, MSS98, Mis97, Mis98, MS99c, Mee99, Miil99, NS98b, NS98c, Ok98a, Ok98b, OSA91, PPKW97, PP90, PW93a, Poi99, PS98g, Rab98, RS98e, RSxx, SS97a, SS97b, Sam98, SK98a, SK98b, SSS98, Sch94m, SPP98, Sha95b, SV93, SH99, Sil97b, Sil97a, Sil93b, TY92, Tak97, Tak98a, Tak98b, T99, TT99, VDV90, VNM99, Ven92, Vv97, Wal99c, Way98, Wie90b, Wie90a, Wir98, XL99, YWY99, Zer96b, Zho94.

RSA-120
[DDLM94]. RSA-130 [Ano96b].

RSA-Based
[CD96, GKR97, VNM99].

RSA-cryptosystem
Gro94.

RSA-Implementation
P90. RSA-key
[FM98]. RSA-keys
[SS97a, SS97b].

RSA-Like
JQ97.

RSA-Moduli
Mau90.

RSA-signatures
Ev92.

RSA-type
BQ97, JQBD97, CLL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b.

RSAb
[MP95s]. RSAeuro
Bar96.

RTD
KW92.

RTR
KV99.

Ruby
JSS93a.

Rueppel
NM98.

Rule
[PL94].

Rule-Based
PL94.

Running
DF91c.

Runtime
DF91c.

Runtime-Tunable
WF94.

Russia
CW94. S
WG97, Ano95u, Ano96-28, BD95a, DT93, ECD+99, Kim93, Mat95, MC96, PG97a, PG97b, SK98c, SK98b, Sto90, Uni97c, YS99, YY98d. S-box
BD95a, SK98c, SK98b.

S-Boxes
Kim93, PG97a, PG97b, DT93, Mat95.
S-CODER [Sto90]. S.Hrg. [Uni98j]. S.I.S. [Eph98]. S.I.S./CB [Eph98]. S/390 [ECD +99, YS99]. S/KEY [MC96]. S/MIME [Ano95u, Ano96-28]. S012 [KP95]. s02DES [TSM95]. S390 [Deu97, Deu98]. SAC [Kim93, KS97b, NS99a, TM99]. SAC/PC [KS97b]. SAC'99 [HA00]. SAFE [Uni97a, Uni98c, Uni98e, UU97a, Uni97b, BC97, Hor99, VM96, Way95, Uni96c, GA98]. Safe-Tcl [GA98]. safeguarding [Beu94]. Safer [Hir93, BM97, CMKK98, KSW96, KSW99a, Kel99, Mas94, Mas99b, Vau95]. Safety [Ano94d, Ano980, DDJ99, Cli99, IEE94b]. Safford [Bur98b, Kru98]. Saint [GQ95, QG95]. Saint-Malo [GQ95, QG95]. Sales [Gar97a]. Salesman [OMV98]. salient [CKLS96b]. Salt [USE95b]. Sam [Mad99g]. Samba [Bla98]. same [Ude98]. Scenario [AMP94]. Scene [SZT98a, SZT98b]. Scene-Based [SZT98a, SZT98b]. scenes [BP97a, BC93a, BDPR98, BBDW96, BK94a, BK95b, BM96b, BM96c, BDGV93, BSD +94, BS96, BB96, BC99b, BC99c, BV96, BV96, Bri90a, BS91g, BL98v, BBD92, CS97a, CM99a, CD95, Dam99a, DVW90, DMPW98, DY91e, vD95a, DF95, DL97, FDB93a, FY97, FO99b, GPSNW98, GP99, GS94a, HK97a, HK97b, IS91, JMO94, KPG99, KI96, KMOV91, KOS +94, KO95b, KOO95a, LHW98, LM95, MH96, Mis98, MWW94, OK98, OK98, Pai98a, Pai98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SIK93, Sim90b, Sim91, Sim94a, Ste94a, Sti93a, Sti98b, SW99b, SSNP99, YLD99, Zha98, ARK99, BC95a, BR97b, BI93, BDSV93, BCDV94, BGS95, Blu95, BC96a, BCDV96, BDGV96, BMS96, BD97, BFS98, BDV98, BD98b, BD999, Bur96, BM94c, CDGV91, CP95, CSV94].
schemes [DP96, DF93, DDB95a, DDB95b, Des99b, FDB93b, HY93a, HMP95, HCY96b, JM93, Koy95, KO95a, KO96, KO97, LS98a, LC97a, LHL95b, LHL95a, MS98b, MPSV99, MTNI97, Mu92, NR95, OK96a, OKT93, OK95, Pad98, PS98a, PPKW97, Pfi96c, PS96d, RD96a, RS96b, SIF93b, Sha94, Scha95a, Sh92g, SW98, SW99a, SS94, SC97, T99, Tze99, VNM99, WAMO94, ZHS94, Z98, dR94a, vD95b]. Schernes [BBCM93a]. Schnorr [DBGV93, dR94b, dR94a]. Schoof [IKNY98]. school [Duf98]. Schools [DDJ98e, DDJ98f]. Schroeder [Low95, Low96]. Schussel [Pin98]. Schutz [FT95]. Schwierigkeit [Hor99]. Science [Ano93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97f, IEE98a, IEE99a, Ste91, Bed90, Beu94, Sch90c, Sch97c, Shp99a, Sim92, WS96c]. Sciences [Ano95r, Tv92]. Scientific [CHLT99, PH91, GTGW94, HW91]. Scientist [BCE+94]. scoop [Ano96-30]. Scots [Sin99]. Scott [Sha99a]. Scramble [JSY99]. Scramblers [GDS91]. Scamper [CN99]. ScriptEase [Ano97-34]. Scripting [SVa+98]. Scripts [Duh90, Sch99a, IPNdbbbprn91]. Scrubbers [Dun94]. scrutiny [Den90]. SDK [Ano97-34]. SDNS [NH90]. SDSC [Sch99]. SEA [Sch99j, GC97]. SEAL [HG97a, HG97b]. Scalability [Por98]. Sealing [GS98]. Seamless [DFGH99]. Search [AEDS99, BD93, CD98c, HS90, KP99a, LC99, Mih94, Sa99, Wi93a, Wie96, Wie97, Wie98a, vW94, vW99, CR97, GLV99, Gol90c, KR96b, KM98c, Kuh98, Wi94]. Searches [PKA+98]. Searching [BP95a, DDJ98e, DDJ98f, Jia99, DSSZ99]. seasons [WSFC99]. Seattle [HF97, USE98a, USE99b]. Second [Auc98, Cha91, DEQ92, Hir98, Nat99b, ACM90, AR97, Ano99g, FR95a, IZ99, Lea90, Pre95a, Un96c, Un95a, USE96d, VPM97, Hin93, PH91, HK97]. secondary [Atk93]. Secrecy [Aba99, BP98c, GM90, GTGW94, JR96, Moy98, Rat96, Sin99]. Secret [AGY95b, Ano97e, BC93a, BC95b, BCG90, Ben98, Ber91, BS97a, BK94a, BK95b, BDGV93, BM99c, BV96, Bra95b, Bra95c, BS94, BD90, Bri90a, BS91g, Cac95a, Cac95b, CT97, CMPS97, CGMW97, CK90, CSFY96, DD98g, DDJ98h, Dae98, Dam94b, DDP94a, DKKK98, DF199, vD95a, EHMS99, FW91, GSPNW98, GSPN98, HL93a, HD96a, HK97a, HKS97b, HCY96a, IS91, Keh96b, KI96, Kra94a, KOS+94, KO99b, KO095a, LYH93, LF97, LM94a, LM94b, LP99, LH93b, MSNW99, Mau93a, MW96a, Mau97a, MSN98, MSN99, MT98, Mus92, NW98, OK98, PS98a, Pu98a, Pui98b, Ped91d, Pr96, Rey96, Rey97, Rey99, Sal91, Sch99, Sha99a, Sim90b, Sim91, Sim94a, St93a, Van93, W199, Wie90b, Wol98, Al 96, AG95a, BC95a, BT94, B193, Ble96, BSV93, BCDV94, BDD+94, BGS95, BCDV96, BDGV96]. secret [BD97, BDV98, BDG99, Cur96, CDGV91, Dal97, Dam94a, Dwo91, Ell97, FO93, FO98, GM95, GPSN97, Gre90, HNSM91, Hel93, HJKY95, Hwa92d, H96c, HLC99, JM93, JMO95a, Juv96, JY98, KO95a, KO96, KO97, LY93, LH95, Me92, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, Ped91b, Ped91c, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, Vv97, Wie90a, WS96c, Win99, Wri98b, ZHS94, vD95b, van97a]. Secret-Ballot [CSFY96, BT94]. Secret-Box [BCE+94]. secret-key [Ano97e, Bra95b, Bra95c, LM94b, Mau97a, Van93, Wol98, LM94a, JY98]. secret-sharing [RD96a]. successful-sleuthing [WS96c]. Secretly [MT94]. Secrets [Cre90, DH90, DS99, El98, HY93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, Ano91b, Bnt97, BDV93, CWY98, JMO95b, WY93, Ch92]. Section [Alv98c]. Secure [AHV98, AB96a, An93c, An93f, An95l,
BHHR99, BCW97, Boy98, Bro96, Com97, Cha95a, CP94, Chi99a, Chi99b, CJ95, C111, CT1x, Dam99b, DS90a, Den99, DEQ92, D+98, FHG99, FFW99, FM98b, Fra92, Gone92, GEL98, Gru98, HN98, HK99b, HOQ97, HS96b, Hor94, H95a, HC95b, HY95, HLLC96, IEE94b, JT96, JT97b, JI95, KY97, KG96, Kat97, KSB96b, KSB97, KW92, Kuh98, Lai92, LTT95, Lee95, LHW99, Len93, LC95, MW94, Mar95b, MS97, Mat97, Mau91c, MKKW99].

security [MF97, Mei94, MW98c, Nor95b, PS99d, PS99a, PS99b, PS99e, PGV93d, Py99, PR98, Q+98, Riv98c, Ros94, SSN98b, Sah99, Sch92a, SSM 97, SMD 99, She92c, Sta94a, Sta99a, Sun98b, Tay90, Tho96, TY98b, TY98a, Tsu92c, Uni98d, Uni98k, VB96, VPM97, Ven90, Wlatex, Wee97, Xie92, XL99, XZ96, vD99, van99b, van99b, Ch99b, Far92, Uni98c, Uni98b, U97a, Uni97b]. Security-analysis [vT94]. Security-preserving [DI99]. See [Web98].


Selected [CW94, HA00, TM99, Cha91, CFG96].

Selecting [Bax97, CDFI95]. Selection [HUB91, Len99a, PNFK95, BM94e, Fei99, U9CF94]. Selections [DKK+98, Ers99].

Selective [GM97, H9V99, IS97]. selectively [WY93]. Self [AW99, BCD98, Fis98, G911, GPR98, K97, LC94, Mau91a, M95b, OMV98, S99a, Sch99d, Jan95, S95a, Mih96, Sch90c, Sch97c].


Self-Organizing [OMV98].

Self-Reductions [Fis98]. Self-shrinking [MS95b, MS95a, Mi96]. Self-similarity [BCD98, Sch90c, Sch97c]. Self-Study [Sch99d].

Self-synchronised [K197].

Self-Synchronizing [Man91a]. selling [Bee96].

Semantics [BPR99, Mar99].


SentryLink [An95t]. Seoul [An93g].

Separability [CM99a]. Separable [LY94, AM99], separate [WY93].

Separating [MKKW99, Tom92].

September [An98a, D+98, ES98, FR95a, IE96e, IEE97e, IEE97k, Kat97, LW96, Q+98, Spi95, TV94, T+98, Uni97a, Uni96c, Uni98j].

Serial [Bee96].


selecting [Bax97, CDFI95]. selection [HUB91, Len99a, PNFK95, BM94e, Fei99, U9CF94]. selections [DKK+98, Ers99].

selective [GM97, H9V99, IS97]. selectively [WY93]. self [AW99, BCD98, Fis98, G911, GPR98, K97, LC94, Mau91a, M95b, OMV98, S99a, Sch99d, Jan95, S95a, Mih96, Sch90c, Sch97c].


self-reductions [Fis98]. self-shrinking [MS95b, MS95a, Mi96]. self-similarity [BCD98, Sch90c, Sch97c]. self-study [Sch99d]. self-synchronised [K197]. self-synchronizing [Man91a], selling [Bee96].

semantic [BPR99, Mar99].
Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau93, MB99a, RRSW97a, RRSW97b, Ros96c, Ros96d, Ros97b, Ros98b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, RFLW96, 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 [Bou94]. Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k]. Session-Layer [BB95c]. Sessioneer [AG95].


Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [MSN99, BGD99, CDGV91, OK95, ZHS94].

Sharing [AGY95b, BC93a, BC95b, BBDW96, BK94a, BK95b, BG99, BDD+94, BEM99c, BD90, Bri90a, BS91g, Cac95a, Cac95b, CG98, CT97, CK90, DDP94a, DKKK98, vD95a, DLR97, FDB93a, FGY96a, GJKR96b, GPSNW98, GPSN98, HL93a, HKS97a, HKS97b, KI96, Kra94a, KOS+94, KOO95b, KOO95a, LP99, LCL92, LH93b, Mei92, MS95f, MS99, NW98, OK98, Pai98a, Pai98b, Ped91d, Rab94, ROT94, Sch92b, Sch99i, Sti93a, Wil98a, AGY95a, BC95a, BI93, BDV93, BSV93, BCDV94, BS99, BCDV96, BGDV96, BD97, BD98, BDG99, Bur96, CDGV91, CMPS97, CGMW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FGY96b, FR95c, FO98, GM95, GPN97, HJK95, Hwa92d, HC96, HLC99, JM93, JMO95a, JMO95b, Jar96, KO95a, KO96, KO97, Mao98, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, PS99a, Ped91b, Ped91e]. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95b, van97a]. Shark [RDP99, WG97]. Shawn [Sha99a]. Shedding [HPG98, YY99]. 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 [Ano95q].

Shooting [Aga92]. Shop [Ano97-33]. Short [Kra94a, Ste94a, Wie90b, vOW96, BC95a, Coh94, Har94, Joh99, VV96, Vv97, Wie90a]. Shortage [DDJ98a]. Should [Way93c, YY96, Ano95c, Riv98c]. show [Mad98g]. shrinking [MS95a, MS95b, Mih96].

SHS [NS93b, Nat92b]. show [XuTaW94]. SIAM [ACM97b]. sichere [Hor99]. Side [KSW98a, KSW98b, KSW98c, SvA+98, YY96]. sides [MB94b].

Siege [EH96]. Siegenthaler [MS99b]. Siemens [Ano97-47, Bro97, Dav98c, Mac98, Sc98b, TJ97]. Sieve [LLMP99, LL93a, Per93, CDE96, Gor93b, Pom94]. sifrovani [Gar98c]. SIGACT [ACM99a].

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

Signals [AK99, BTH96, DDNM98, MHMW98].

Signature [AA95, Acc97, AW94, Int91a, INS94, Ano96f, Ano97-50, BP97a, BM99a, BM99b, BM96c, Br93a, CS97a, CM99a, CG98, CH98, CK95, CDF95, CD95, DMPW98, DQ94, DY91e, DN94, FL99a, FMY98, FOM91, FO901, GP99, GQW+91, HJJ+xx, KKS97, KS98d, KPG99, Kob98e, Kro93, LK96, LHW98, LK99, LHL94, LL98a, MTH94, MB99a, Mer90b, Mer97, MH96, MS98, Miy96, Mon93, Nat91, Nat92a, Nat94c, Nat94a, NMVR95b, Na97, NMV98, NMV99, NIS93a, OFF93, Oka93b, PF94, Pet98, PM98, PS96c, Pj99, RG97, RDK98, Riv93c, dR94b, SC96a, Sch93b, Sch94e, SK97a, SE96, Sim93, Sin98, SB93, SSNP99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, AR99, La93a, AW95, Ale97, Ano97p, BD98a, Bis90, Boy97, Bur96, CP95, CMTNY94, CSV94].

signature [DP96, FR95c, Gu90, HY93a, HJJ+97, Hor98, HMP95, KS98e, LWC96, Mau91b, May97, MS98b, Mu92, NMVR95a, NR95, Pf96c, Pit96a, PS96d, PS98h, SI93b, Sha94, SS95b, SSS95, Ste95, Ti98, Tra97, TJ99, Wan92a, Wi93b, Wn92, XA98, YL99b, YL95a, Yeu99, Zho94, dR94a].

Signatures [ANS98b, AS98, AT99, BD99a, BQ95b, BQ95a, BG90, BdM94, BM94a, BM96a, CB93b, BF99, Boy98, BS95d, CHP91, CR91, CDF95, Cop99, CD96, Dam94b, DF91a, EG900, EG996, Ev919, Fro97, GKR97, GHR99, GM97, GO93, HKS95, HA96, JM99, JQ99, JLO97, Len96a, LSV95, LR98, M996, Mis97, MB97, NW98, OO98, Oka94, PP97, PW93b, PPG93c, SI94, SY96a, Sch93e, Sch93c, Sch94d, SK97b, Sch90b, She97, Tra99, Web98, Wri94, vHP93, Ano98c, BR96c, BGR98b, Ble96, BCP91, BM91b, CP95, CS95, Cha95b, Dam94a, Ev92, EvH93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, Ped91a, Pf96c, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].

Signcryption [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SKAM99, Sun98b]. Signer [CvHP91]. signers [TJ99].


Sizes [PKA+98]. Skew [BS95d]. skill [Gre90]. Skipjack [BBS98a, Bih98b, BBS99a, BBD9R9, KRW99].
Skipjack-3XOR [BBD9R9, Bih98b]. Skolem [GS99a]. skullduggery [Beu94].
Slab [FVEA99]. slacken [Gen99b]. Slave [CFK+91]. Sleepy [Wu96]. slender
slides [DW98]. Sliding [FCH99, YY97c]. Slippery [Wal95]. Slisp [BP97b]. Slow
[KS99a]. Slim [ARV99a, ARV99b, BDF98, Cop95c, HVM93, JSY99, MB99a, SKNO98a, SKNO98b, Sta97c, T99, Ped95, SS98a].
Smaller [DDJ98a, DDJ98a]. Smallest [Got99]. Smalltalk [Lut98]. Smart
[ABK91, Ano96z, Ano99e, BE90, Bov98a, Bov98b, BDB92, Cha99a, Cha91, CM99c, Chr99a, Con98, Con99a, Cor98, CH99a, DDJ98d, DDJ98b, DDJ99, Deu97, Deu98, Di 97a, DT98b, EN98, ENK99, Fan96, FGLP96a, FGLP96b, FOM91, Gar97a, GL96, GPSV98, Gut98a, HKQ99, HP98a, Hru96, HH99, Hus99, Koe99, KCCT94a, KCCT94b, Mar98a, Mye96, NM96b, Omu90, PV98, Roh99, SKW+98e, SS99a, Sch90b, SR96, SGPV98, Smi98a, Sut99, Tua99, VW98, Ver98b, DW99b, DW99c, ABKL93, AHdLF97, Al97, BGV97a, Cha99b, CW97, CJRR99b, DS98a, Dhe98, Di 97b, DF97, Gau97, Hip97, Sha95a, TJ97, Taa98, AG99, Bak99, BF99a, Bro97, DVM96, Gir99, GSVT96, HNS99, IW99, NFQ99, SS94, SKAM99].
Smart-Card
[RS99, ABK91, ABK93, CJRR99b].
Smartcard
[Ano98q, Ano99e, USE99c, Ano97x, Ano97-47, Ara93, Ban97, Ano98p, CH94b, H99b, KK99a].
Smartcards
[Bla96a, Bla96b, Fan97, Sch90a, DR99a, H99a, IHR99, MDS99].
SmartLink
[Ano93k]. smooth [Odl94a, VZ97]. SNAKE
[MSK99a]. Snesfru [BS91f]. SNMP
[Sta96c, VDDR99]. SNMP-CORBA
[VDDR99]. SNMPv2 [GM93a]. snoop
Societal [Sta97b]. Societies
[IE92d, IE94f, IE95c]. Society
[Ano98n, IEE92c, IEE93b, IEE94d, Mar96, DL96, KG96, Ta99]. Socio [SM99].
Socio-technical [SM99]. Sockets [ZG96].
SOCKS
[Lee96, McM96]. Soft [NS98a].
SoftID [Ano96-27]. Software
[Abr97, Ano93j, Auc96, AG99, Bih97b, BD94, CD97, Cla98a, CT99b, DBVD96, DF91c, DSB99, Gar97a, GO96a, Gut98b, HK97, J98c, K96b, L95, L99, Lea99, Lut98, Mat96b, Mer91, MM97, RSA94, RC94a, RC94b, SW94a, Sch90c, SK96a, SK96b, SK96c, SW97a, SW97b, SK97c, She95b, You96, Ano94a, Ano95g, Ano96-27, Bih97c, BP97b, DH96a, Des95, Gol96d, Knu99c, PA93, Pre95a, SS98a, SAM97, Str93a, Str93b, Sz97b, Vau98e, Woo90].
Software-Optimised
[RC94a, RC94b].
software
[MM95, SOI [NFQ99]. Solaris
[Sun91b]. SOLID
[Ano97-33, CK95, Gut96].
solid-state
[GS96]. Solution
[GO96c, Law98, LR98, W98].
Solutions
[HM98, MSK99a, PW98]. solve
[WSFC99]. Solved
[Ano97c, Ano98i, Ree98].
Solving
[LO91b, Lew92, MSO96, OMV98, Per99].
SOM
[BBN96]. Some
[Abe98b, AT99, BBL95, Bri90a, BS91g, CD95, CRR99, CL98, Des98c, Ev91, FDB93a, Gib90, Gu97, HGH98, Hub91, HCY96a, Knu99a, KP95, KYYB99, L92, LP94, Lid90, MSS98, OK98, Sim97, TCH+91, Wag98b, Cao99, Cha95a, FDB93b, Gol97c, Lan96, RD96a, SMK98b, TH99, Koo97].
Someone
[MB99a]. Something
[SvA+98].
Son [CFK+91]. soon [Pri94]. sophisticated
[M98]. Sought
[Ano97-45]. Sound
[CJRR99a, MGL+98, Ano96-29]. Soundness
[DE99]. sounds [BDC+95]. Source
[Sch94g, Sch96a, Sch94h, Zim95b, Gen99c, Zim96a, Zim96b].
sourcebook
[Ban94, Rot95a]. Sources
[ADBB99, Cor99, Uni94c]. Southcon
[IEE96f]. Southcon/96 [IEE96f]. Soviet
[COP+95a, HK99c]. SP [STP93]. Space
[AR99, BC95c, FP99, Gar97c, HBLK99, KV99, Ki96, SGG99, BBI90, Mra95, Pad98, Sze98]. space-filling [BBI90]. spaced
[Ito91]. spaceflight [CWM+91]. Spaces
[BP95a, FDB93a, FHG99, FDB93b, Koz96, Son99]. Spain
[Mau96b]. Spake
[CFK+91]. Span
[BDS98, DQ94, HL93a, VBD99]. Spanning
[Aga92]. SPARC
[Sun91b]. Sparse
[LO91b]. Spass
[WABC99]. Spatial
[DSSB95, DDQM98, LLB98, MCD98a, NP98b]. Speakeasy
[LU95]. speaking
[LC95]. spearhead
[Ano98q]. SPEC
[DDJ98a]. Special
[vD97, FT99b, MDP94, SS99e, SS99f]. Specific
[ADBB99, EvH93, Kha93, LMS97]. Specification
[GFB93, HJTW99, LL97a, Ou99, SW94a, Tou92]. Specifications
[KS98a, Nat92b]. Specified
[Giu97, HCC98]. Specifying
[SW94a]. Specs
[Got99]. Spectral
[W94f]. Spectrum
[CKLS97, She94c, CKLS96b, CKLS96c, Dix94, KSB96b, KSB97, LLB98, OP98]. Speech
[DMFB97, Eri97b, GDS91, IEE97d, IEE97e, Lud97, SW95b, All97, CW94]. Speeches
[Bar94]. Speed
[ARV99a, ARV99b, Ano99f, Ano99l, DP98a, DP98b, Ebe93, FVEA99, IM93b, Koc94, LS97, MPPS95, SKNO98a, SKNO98b, SW97a, SW97b, She92d, She95b, IM93a, Kap98, KAK96, Lam99, Nor95a, HKSW98, HKS99, Zhe97a]. Speeding
[ADEDS99, KT93, McK99, Tes98]. speedy
[Ano98e]. spi
[AG97b, AG97c, AG97a]. Spiculated
[ZTR99]. Spin
[RK99]. Spite
[Wai90]. SPJ
[TL999]. SPLICE
[HC95b]. SPLICE/AS
[HC95b]. Split
[Coc97]. Splitting
[SG90]. SPM
[CV93]. SPN
[Kob99]. SPN-Structures
[Kob99]. Spoofing
[SVxxW91]. SPRC
[Wi93b]. Spread
Kal99, MBB98, PP96, Ano92b.

Standards-Based [FBS97]. Stanford [IEE98b]. Stanica [YT96]. Stanley [vdWS97, vS97]. Star [Ano97-33, HI97].

starts [Ano96-29]. State [FGS96, Lan98, LF99, Mjo93, NM96a, Pre98c, PR98, Pre99, She92e, Wol93a, Wol93b, Zaj97, BFS92a, BFS92b, Gut96, PGV93d, Ril96].

State-industry [Zaj97]. State-of-the-Art [She92e]. Stateless [BGK99]. STATEMATE [DJHP98]. Statement [II96]. States [Cli97, Uni99h, Uni97c, Uni95a, Uni98k, UU97b, Cli99, Lev97, Mil95, UU97b].

statesman [Bed90]. Station [BWM99b, Smi98b]. Station-to-Station [BWM99b]. Statistical [De 99, GC91, GSV99, Gus96, PNFK95, NO98, Tha91, GKS97]. Statistics [BBDF97, IEE94a, FO90].


Steganographic [ANS98a, CM97c, NHB98, ZFKP98, ZFK +98]. Steganographie [MP94]. Steganography [All98, And96b, AP98, Cac98, Cra98, CI96, DS96, FJM +96, Joh97a, Joh97b, JJ98b, Jo98a, Jo98c, Kah96a, MT94, Man97e, NNEK97, Phi98, Rho95, WW98a, Cai96, Cra97].

Steiner [ZW99]. step [Ano97d]. Steps [GO96b].

Stern [Cus97]. Still [Bla99, Mei98, BBCP97]. Stockholders [MS99a]. Stop [BP97a, PP97, SSNP99, vHPP93, Phi96c].


store-and-forward [CadHSV96]. Stored [SV99a, SV99b, Lee95, SvS98]. Story [DDJ98g, DDJ98h, Kah96b, Pra96, Ritxx, Eli97, Hay98, HS93, RK98b, Wei97].

Strand [FHC99]. STRATA [PMP99]. Strategies [AWV99, CO98, Da95, KFJP96]. Strategy [Gar97a, KTM +99, OMV98]. Stream [AM97, BD94, Cha94a, CS91, Cla97, Cla98a, DC98b, Din94, DRNS97, Go97d, Go99b, JJ99b, LS97, Man91a, MS91, PK95a, PK95b, Pen96, Rob95b, Ros98a, SK97b, SK97a, She94a, She94d, War98, ZYWR91, ZG96, BK95a, DGV94b, DXS91, Go95b, Go98b, JV98a, LRW93, Tay94]. Stream-Cipher [ZYWR91]. Streams [GR97, PSB97].

Street [Ano97k, KS98b, Sim98c, HRT96, Law98].

Strength [HK98, HK99d, Ano98a, Cop94a, KM97, Mat95, Wei99]. strengthen [BB95a]. Strengthened [DBP96].

Strengthening [MB94a]. Stretch [Pai99b].

Stretching [And96b]. strict [SZ99a, YT96, Cus96, CS96c, O'C94].

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

Strings [Gol96b]. Strong [Ano97-46, Ano98s, CvHP91, Gar97b, Gut98b, GS99b, PW97c, RS98e, RSxx, Sil97b, Sil97a, WD99b, Wa98, ZZ96, Ano96g, Bee96, DLP93, DT93, MCD98b, ZZ95b, Sze98, Ver98b, YW99].

Stronger [Ano95v, FS97b, MAM95, SVA +98].

Stronghold [Ano97-33]. Strongly [Mau91d]. Strongly-Randomized [Mau91d]. Structural [BHJM99].

Structure [BCC90, HV98, Mat96a, PRAM98, LL93b, Mra95, PS98a, RD96a, Sch98a]. structured [FR95a, KS98c, O'C95, SK97d]. Structures [BRS99, EKLM99, Kob99, Lut98, MSNW99, ZZ95b, Lai95, Mic97, PD99a]. Structuring [Hru99].

Struggle [Gla99b]. STS [BWM99b]. Stubblenine [HLL +95]. Stubs [AO96].

Student [Ste91]. Studied [Che92].

Studies [WD97, DN95a, Ger99b]. Study [BPR99, Da99, LBHM99, LL98a, Sch99d, Gua90, LMS97, Sta97a, Zho94].

subband [TKS98]. Subcommittee [Uni97a, Uni98k, Uni98d, Uni97b, Uni95a].

Subcommittees [Uni98e]. subgroup [Boy97].

Subjective
Subliminal [BDI+96, Gru98, KI97, SI93b, SI94, Sch93b, Sch94e, Sim93, Sim94d, Sim94c, Sim96a, Sim97, Des96b, Sim98a, Sim98b, YL97a].

Subliminal-Free [BDI+96].

Sublists [Rus93a].

Submanifolds [Mra95].

Submission [Ada98, CMKK98, BT97, Zun98].

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

Submit [Law98].

Subquadratic [BBP95a, BBP95b].

Subscribers [GC97].

Subscript [Mau91b].

Subsegments [KPR99].

Subset [NS99b, CJL+92].

Substitution [CT99a, HS90, PRAM98, SZZ94b, ZZ96, Ata94, FSN93, Fri92b, HT95, O'C95, Zan90].

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

Subtitle [Mer90b].

success [Blo98c, TY94].

successful [HA94b].

successfully [Al96].

Successor [Ano97-45].

Sufficient [MSN99, Rus93b, Rom90b].

Suggested [Bih91].

Suggestions [Mat96b].

Suit [Buc95b].

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

Sum [NS99b, CJL+92, JV98a].

Summary [CFGS99, DY91d, USE95a].

Summer [USE94, Mye96].

Summit [CFK+91].

sums [BK98g, CFS97, KOB1c, Sun].

Bro97, Gar98b, Got99, Law98, Szw97c.}

SunOS [Ste92, Sun91b].

Super [Sut99].

Supercomputer [DMS95, She92e, Ban97].

Supercomputing [IEEE91].

superhighway [BDC+95].

Superimposing [YY91].

supersafe [PP96].

Superscalar [Cla97].

superscritcher [Cla92, CF92].

Supersingular [BS91b].

Supervisory [Kap99].

Support [AKP99, BV98a, Bla98, Bla93, DTDJ99, FR95d, GR99, HKS95, KHB99, LBHM99, LC99, Mon93, Pit96b, SK98a, SK99, SL99, TYD99, Ano97], Ano98f, Clt99, LS98a, TCH+91, Uni94b].

Supporting [PK99, MI90].

Surmounting [CI96].

surrounding [GA98].

Surveillance [CKN99, SB97].

Survey [Bri90b, Gar97c, GFR93, Kal93a, Kle90, Knu98b, Nis96, Par98c, BO92, Ele99, Mea95, She92g, Wad98, Zho94].

Surveys [Ell99].

Susceptibility [AW94].

suspected [LHL95b, LHL95a].

swapping [TN97].

Swedish [LF97].

Swindles [Dob95b].

Switches [Bee99].

Switching [MOM91].

Switzerland [ACM97a, BCB97, IEE96c].

sword [Den95].

Sydney [KG93, SP90, VPM97].

Sylvester [Por98].

Symbolic [Wat91, AM99, BHKR95].

Symbols [Pes97, CS99].

Symmetric [Ada97a, Bir98, BDR+96, BFN98a, FO99b, Gsu96, QG90, Roe94, YY98d, YY98b, BDJR97, Cra96, GHS93, HJ99, Hwa93].

Symmetry [BS95d, PS97].

Symposium [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97b, ACM97c, ACM98b, ACM99b, Ano99c, Con96, CMM93, DEQ92, Hei96a, IEE92c, IEE93b, IEE94d, IEE95b, IEE96a, IEE97f, IEE97i, IEE98a, IEE99a, KK99b, Q998, Sp998, SL93, USE92b, USE93, USE95b, USE96e, USE96g, USE98a, USE98d, USE99a, Wat91, Wol93a, Wol93b, Tv92].

synchronised [K197].

Synchronization [DHSS95, BCCG99].

Synchronized [Yah94, Gon92].

Synchronizing [Mau91a].

Synchronous [AMP99, NT99, DGV94b].

Syndrome [CS96a, ZYR91, ZH90].

synopsis [Wri98a].

Syntax [Kal98f, Kal98c, Kal98d, RSA93d, RSA93c, RSA93e, RSA99a].

Synthesis [HL99, Sab94].

synthetic [PGV93b, PGV94].

System [ANS98a, Ano97-33, ADF98, AHMS99, BS99a, BLM99, BKS99, Bal97, BR97a, BM91a, Bis98, Bla94b, BLM99, BCG99, Bur94b, CIBM99, CD97, CM99b, Chi92, CC99c, CH94b, CM99d, DDP90, DT98a, DTDJ99, Far92, FK99, FO97, FR95d, Gan96b, Gar97a, GRB99, Gol90a, GPSV98, GS99a, HJTW99, HCDC99, HJL99, HE98,
INDI99, JO97, Jia99, KI99, KW99, LMP99, LW95, LCN99, MGL+98, MLK99, MR95a, Mar98a, Mau97b, MTV92, Mon93, NM99, NS98a, Nec96, PR99, PS99f, PK99, Rei92, Rus90, RH99, SYM1998, Sam98, STSW99, SCT99, SK96b, SK96e, Sch98h, SSP90, SM99, SKIT99, Tm99, Var99b, WHFG92, WABC99, WW98a, WBB99, WABL94, ZK96, ACC99, Ano96b, BCB99b, Bax97, BMP97a, Bur94a, BD95b, Car94, CB96, Cus95, DSSZ99, Des95, DD96b, FM98b, HN94, HI97, Hwa92a, HC95b, KM98b, Kum97, LC96a, LCL95, MY93b, MKKW99, Mey97b, MM95, Oel97, PS99e, PSW95, Sch99j, SY96b, SS95b, TCH91, TC91, Ven90, WSFC99, WABL93, ADDS91, Ano91a, Bax97, Bel92, Dan95, JD91, RC95, YKY99, ZH98.

Systematic [BGH91, Zav99, Men95b].

Systematising [MKL99].

Systeme [BGH95b].

Systems [ABLP93, AKP96, AKF94, Ako99, Ano94k, Ano95c, Ano96a, ADEDS99, AA97, AMP99, BDP99, Bar99, Bas93, BR91, BBD97, BFN98a, CF95, DDJ98a, Dan91b, DFT97, DY91a, DD99, DB96, ENK99, FJP96, FY95a, FY95b, FYM99, FO991, GL96, GFB93, Gl98, GM90, GM91, GK96, GS97, GMV98, HGH98, HJJ+97, HJ94, HP98b, IE93a, IE96b, IE96d, IE98e, IE99b, IH99a, KT96, Koc96b, K99, KY92b, LO91b, LQR98, LAB92, Lan99, Lee99b, Mar99, M99a, MS95f, MD94, Mu93, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PS99n, Pin97, Pit96b, PM99a, PD99b, RBvR94, RG95, RP95a, ST94, SN96, STS99b, DY91c, SOOS95, SS99, She92a, SY92, Su99, Tra99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a].

Systems [WL92b, WC97, Yac99a, Yac99b, YKB94, YMW99, ZFKP98, ZFK+98, ARK99, AHdJF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BP95b, CG05, DMW94, DIX94, Fri92b, Goo96, GKS97, Gr98, HJJ+97, IEE97k, KG96, KP99b, LM98a, LAB9W1, LS98a, Lie93, MS97, NIS92, Oht96, Ole95, Opp96, PAK98, PA98b, PP99a, PP99b, PP95b, PP95a, RO96, SKB97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DV96].

Systolic [SS98, DF92, PB99].

SZ42 [Dav98d].

SZK [GSV99].

T [YT96, PDG99].

T-Team [PDGI99].

T52 [Dar98c].

T52c [Sel98b].

Table [KMKH99, Has99, Hor95].

Tableaux [Mas99a].

Tableaux-99 [Mas99a].

Tables [DRR95, JC98, IPD99].

Tactical [KIM99].

Tagging [Lud97].

Tailoring [CGM96].

Taken [GQ+W91].

takes [Szw97c].

Tale [Ka98e, RS98].

Talent [DDJ98e, DDJ98f].

Talk [Deu97, Lei99b, Wat99, BS91c, Sim91].

Talking [HH99].

Tamper [Auc96, BDH99, KK99a, Zhe95b].

tamper-proof [Zhe95b].

Tamper-Resistant [Auc96, KK99a].

tamperfree [Hwa92b, Hwa92c].

Tampering [CL98, CL97b].

Tanaka [Hwa92a, MS98a].

Tandatangan [Ano97-50].

Taos [WABL93, WABL94].

tapestry [MB94b].

TAR [Ano97-33].

Targeted [Cap94].

Targets [Lea99, Way98].

TAS [Cop94b].

Tasty [Sch98].

Tate [FMR99].

Taxing [Gar97c].

Taxonomy [DB96, GS97, LBMC94].

TC [MB99b].

TC11 [Kat97].

TC6 [Kat97].

TC6/TC11 [Kat97].

TCFS [Mau97b].

Tcl [GA98].

TCP [Ano96j, Fei93, Fei96].

TCP/IP [Ano96j, Fei93, Fei96].

TEA [KSW97a, KSW97b, NW97, WN95].


TecApro [GLC98].

Technical [Ano95e, Bar96b, CFK+91, CY98, DS97c, Lan98, LM93c, Mos98, USE95a, USE99d, VGP93, SM99, USE96f, USE98c].
Technique [DDNM98, Gue98b, KP93, WD97, BCV97, ONT98, Way95].
Techniques [Int91a, BGML96, BWM98, Bol98a, Bol98b, BLM94, CM97b, CD99, CMYY98, Dam90a, Dam91a, Dav91, DC98c, De 95, Des98a, Des96a, Fun97, Fun98c, GQ95, Hel94, JJ99a, LvdLB96, MM99a, MSEN99, Mau96b, PS98e, PS98f, PK99, Pre93b, QV90, QG95, Rue93, SZ93, Car98, Cra96, Hel93, Hel98b, ISO97, Kay95, KG93, Nyb98, OPH+99, Oko96, PS99d, SD97, Ste99b, Way91, Woo90, ZH93, van96].
Technological [UFC94].
Technologies [Dan96, DSS98, Aus96, BGV97a, BK94b, BS95e, Oht96, Uni96a].
Technology [Int91a, Ano96-29, Ano96-30, Ano98t, AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, II96, IEE94b, IEE98d, Lic94, Lin93c, NFQ99, Riv98c, USE99c, Ano93a, Ano96u, DS97b, Gil97, ISO97, Rif96, Ros94, Sav96, Sni97a, VB96, CFK+91, Ers99, Ano99b].
Telecollaboration [Fuc99].
Telecommunications [IEE97e, UNU94, Mac98].
Telemedicine [Ano97-50].
Teleperubatan [Ano97-50].
Telephone [Gar97a, Sha97].
Telephony [Ban94, Gar97b, MB99a, Mar95b, PW98].
teletype [Mac98].
TELNET [SSH93, Ala93b, Ano95w, Bor93a, Bor93b, Bor93c].
Temporal [KV99].
Temporary [KRJ98].
Tennessee [IEE94e].
TeraSpell [Ano97-34].
Term [EO95b, CHN97, EO95a].
Terminal [Con98, Con99a].
Terminals [Ano99f, ADSW99, Lam99].
Terminology [Pf96a].
Ternary [PKA+98].
Terrorists [Uni98j, Uni98k].
Terschelling [TV94].
Tesla [Ano97-37].
TESS [Dan95].
Test [DS97a, Law98, MOM91, SS91, DL993, Graxx, Gre90, ZYR90].
Testing [Bas98, Bro94, De 99, MPPS95, Sot98, SB99, SY98, Wal99c, ARK99, Ano97-42, GK99b, Len90, Yan95].
Tetherless [Law98].
Texas [ACM97c, ACM98b, Ano94e, IEE92b, USE98d].
Text [Bar93a, Bar93b, Cai96, CD97, LM98b, PF94, PBGV90, CFK+91, T+91, Sab94, SH98].
Textual [JKVP99].
Teyjus [NM99].
Theft [Gur97].
Their [BK95c, BL96a, BL96b, Con99b, GPT91a, GPT91b, GM91, KI96, Len99b, OO90, SY96a, SG99b, Tra99, VDD99, AA99, BHSV98b, BHSV98a, BY93c, BY93b, Car98, DDB95a, DDB95b, Don98, Eng99, HMP95, KT91b, LN94, LM96, NM96b, SS98, SI93b, TY92, YY98a].

theme [IEE97k].
Theorem [AA93, FK99, GPS98, HB99, DdPS96, Sga91a, WWW95].
Theoretical [Buc91a, Cac98, Cle91, MW96a, Mau99a, Mau99b, MO99, Ped91d, PB99a, STP93, W98, APDS93, Kos97, Ped91b, PD91e, Sga91a, Sga93, Sph99b].

theoretical [Sak97, van97a].
Theoretically [AR99, Mau97a].
theories [T+98].
Theory [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, Ber96b, BMP+97b, Car97b, CFK+91, Dan90a, Dan91a, Dav91, De 95, DS99, Fun97, GQ95, Hei96a, Hei94, IE94a, IZ98, IZ99, KN96a, KR99a, Kob94, LOX99, LABW92, LW91, Mau96b, Mau96a, MPP94, NKC94, NC97, OiDP98, PSN95b, PG90, QV90, QG95, Rue93, SZ93, Ada91, AAP92, Ata99, CS97e, CFC96, Cou99, Dan99b, DXS91, Gol97c, Gol92, GS94b, Hii94, Lag90, LABW91, Lux90, MW98a, Mau93b, Mc90b, Mei92, Nyb98, Pom90a, Rac90, Sch93a, Sch90c, Sch97c, Sga91a, Sph99a, Ste99b, Sti95, Tat98, Tat99].
There [Ril96, Zha97, Way93b].
Therefore [FJM+96].
these [Ano98q].
They’re [Wr94].
Third [ABB+97, Fra99, MKS99, RS98b, Spi95, Uni95a, ACM91, Gol96d, GS94b, GK95b].
Third-Party [ABB+97].
Thirteenth [IEE94f, USE99b].
Tenth [ACM98b].
thirty [ACM99b].

thirty-first [ACM99b].
Thomas [CFK+91, Bed90]. Those [BCE+94]. Thoughts [Knu99a]. thousand [Ril96]. Threat [Hig97b, BCW97, Hed97]. Threaten [Gar97c]. Threats [EN98, Jam98, SS99a, WN98b]. Three [Ano95a, BR95b, HEQL98, KS97b, Ng99, OMA98, SN96, FR95b, OMA97, XZZ98].

Three-Dimensional [OMA98, OMA97]. Three-Party [Ng99, XZZ98]. Threshold [BBCM93b, BBCM93a, CGJ+99, DF90, Des93, Des94a, Des98c, FY98b, Gem97, HHT93, HHT97, JMO94, KOO95b, KOO95a, LH93a, LHL94, LHL95b, LHL95a, MKS99, NP98a, Oka98a, Oka98b, PM98, Rab98, Sti98b, SSNP99, Zha98, Blu95, CMTNY94, DDB95a, DDB95b, FD92, GJKR96a, Lan95, Lan96, LL97b, MPBV99, Ped91c, SG98, SS94, TJ99, WAMO94, XL99, CG99].


Tour [Han94, Mos99]. tourist [WSFC99].


Tracking [HCDC99, Hur98]. Trade [BFS96, BMS96, Uni98d, Uni98e, NMVR95a, NMVR95b]. Trade-offs [BFS96, BMS96, NMVR95a, NMVR95b]. Trademark [Eri97b]. Tradeoff [KR94c, CK93]. Tradeoffs [CM99].


Ano91a, JD91]. **Transactions** [FL99b, FKMY98, SS99]. transcendent 
**Transcript** [BD99a, Chr99a, Sas99a].

**Transcript-Irrelevant** [BD99a]. **Transfer** [Ano97-34, DF99, HHY93, NP99, RS96a, Bea93, BM90, BR96b, DOR99, Jac90a, 
Jac90b, SI93b]. **Transferable** [Sak96].

**Transferred** [Uni97d]. **Transferring** [SI94].

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

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

**Transformations** [BDFM99]. **Transfusion** [ADBB99]. **Transient** 
**Transistors** [CWM +91]. **Transit** [Des98a, DR98b].

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

**Transmission** [NHB98, PSB97]. **transmissions** [Ano97-30].

**transmitting** [Cli97, Cli99, UU97b]. **Transparent** 
[Bl93, DS97c, Mau97b, SZT96b, ZG96].

**Transport** [Ano94b, BWM98, GBC93, Sar97].

**Transportation** [BPR99, Uni98b].

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

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

**trap-door** [Yu92]. **Trapped**

**BM92, BY93a, BHSV98b, BHSV98a, Pai99c, RP97a, WBDY98, And93, Gar96a, Gar97d, 
Ort95b, Ort95a, Way93b].

**Trappeddoors** [Gib91, Gor93a, Pat99]. **trappes** [Sch98c].

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

**Travois** [Yu97]. **treaties** [Des90a].

**Treatise** [Tur99]. **Treatment** [BFN98b, 
Mau96a, O098, BDJ99, BFN98a, Gen99c].

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

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

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

[AG92, BP97a, HS90, ZW99, SSM92].

**Trellis** [SKD94]. **Trellis-based** [SKD94].

**Trends** [DDJ98c, DDR98c, De 93b, De 98c, 
Hru98, IEE97k, Kan96, LM98a, MB99a, 
Koo97, Seg92]. **Trial** [Mye96].

**Trials** [CY98, P96b, Ano93a]. **Triangular** 
[Por98]. **Tribulations** [CY98]. **tribute** 
[Uni92]. **Trinity** [IEE97a]. **trip** [Cur98].

**Triple** [Ano95p, Ano96c, Ano96-28, Bih69c, BK98c, 
Bih99b, CJM95, HP99a, HP99b, KMS95b, 
Kum98, Lue98c, CJM96, Mey97b, Per91, 
vOW91, Joh99, KSW96, Rot97, Mey96b].

**Triple-DES** [Ano95, Ano96-28, BK98c, 
Kum98, KSW96, Rot97, Mey96b]. **triples** 
[CF97].

**Trithemius** [Ree98]. **Trojan** 
[Sch99f]. **true** [Way91].

**Truncated** [KRW99]. **trunk** [Uni94a, Uni94b].

**Trust** [Ano99j, BPK99, BFK99, LA98, MR98, 
Re96, SA95, Sim94a, Sta95a, YKB94, YY96, 
AHdJF97, BH98, Com97, Chi99a, Chi99b, 
LN98]. **Trust-Based** [YKB94].

**Trusted** [AAB +97, Ano97d, IS91, MKS99, RS98b, 
SK97c, SS99e, SS99f, CGM97b, HY93a, 
JMO95a, LWC96, Ped91c, Wu92].

**Trustee** [Jue99]. **Trustworthy** [Fri93, Pos92].

**True** [For99a].

**Try** [Rot97]. **TSP** [Luc95].

**TTP** [BDHJ97].

**TTP-based** [BDHJ97].

**TTPs** [Lan98].

**Tübingen** [PDG99].

**tucked** [Ano91b].

**Tunable** [WF94].

**Tunneling** [SM98a].

**Tuples** [FJR96, MI90].

**Turbo** [J99a].

**Turbulence** [DIF94].

**Turing**

[CFK +91, Hod97, De98b, Tur99].

**Turnaround** [Gar97a].

**Tutorial** [Buc91b].

**Tutoring** [PD99b].

**TV** [DDN98, Fox98, Gar97c, Gar98b].

**Twelf** [PS99f].

**Twenty** [Ano95r, Bon99, ACM90, 
ACM91, ACM93b, ACM94c, ACM95, 
ACM96c, ACM97c, Gol97c].

**twenty-eighth** [ACM96b].

**twenty-fifth** [ACM93b].

**Twenty-Ninth** [Ano95r, ACM97c].

**twenty-second** [ACM90].

**twenty-seventh** [ACM95].

**twenty-sixth** [ACM94c].

**Twin** [Mac98].

**Two** [AB96a, Bea92, BMM99a, ...
BMM99b, BS99b, BS99c, BGH+91, dBB91, BKR97, Cha94a, CPPK98, Dob97, Gil99, Gol96b, HKQ99, HK98, HK99d, HEQL98, HLL+95, Kal98e, Koe99, LYH93, LM98b, Mad92, PPKW97, PS98g, RS96b, RS96c, WN94, Yin97, ZMI91, vT93, BDHJ97, Den95, Dob98, HWF96, H1Y95, JW01, LHW99, LC97b, MB94b, MCD98a, PwO96, WHL99, ZLX99, dB91, vOW91]. two-key [vOW91].

two-level [HWF96].

two-list [LC97b].

Two-Party [BMM99a, BMM99b, BGH+91, JW01, ZLX99]. two-phase [HY95].

Two-Round [Dob97]. Twofish [Fer98, Fer99a, MM99c, Mur99, SKW+98b, SKW+98c, SKW+98e, Sch98g, SKW+98a, SKW+98f, SKW+98d, SKW+99d, SHK+99a, SKW+99e, SKW999, WW98b, WS98, WKS+99, Wh99]. TWOPRIME [CWSK98, DNRS97].

TX [ACM99a, IEE98e, USE91]. Type [BD99a, BS90b, DE99, MC92, SN93, SK95, Cll99, Gk95b, Jq98a, Koy95, Kk96, Tak97, Tak98a, Tak98b, Wan92b, Xie93, BjQ97, JqB97]. Types [SG95, Bih94a].

Typing [She95a, Aba99].


U.S.C. [Cll97, UU97b]. übersicht [Ger97].

Ubiquitous [DDJ99, Cha99b]. UCC [Uni96a].

UK [Gol96d, Wai99a, And94a, Ano97i, Ano98u, Boy95b, Chr99b, Dar97, Dav91, IEE95a]. Ultra [Ben08, LS97, Blo98a, Blo98b, Blo98c, Dre92, Kahl89c, Bra94b, Mus92, Win91, Win99, Win93]. UMAC [BHK+99]. UML [BPRF99, Hr99, Km98a, Kmps99, On99],

UMLS [ADBB99]. unacceptability [Eng95].

unauthorized [Ano96d]. Unbalanced [Jut98, KPG99, Sk96c, Sk96d]. Uncertified [KC95]. Unclassified [Bra90a]. Uncle [Mad98g]. Uncompressed [NHB98, HG98],

Unconditional [CM97a, FHM98, GM90, WP90, Wai90, Wol99, MSN97].

Unconditionally [BFS96, Cha90, CvHP91, CR91, DY91f, Tay95, BMS96, Des90b, HW98c].

Uncorrupted [PBBC99]. Uncryptic [Pff95]. Undang [Ano97-50]. Undetectable [CvHP91, DY91e, FOO91, GKR97, SY96a, BCDP91, DP96, HY93a, Jak95, LWC96, Ped91a]. Underground [HLMP96].

Underlying [HL99, CGM96].

Understanding [MF97]. Underwater [MFG95]. Underway [Ano97-44]. unfair [Tra97]. Unforgeable [BC93b, DN94].

Unfortunately [Ril96]. unicity [Al 96].

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

Unit [Uni94b]. United [Cll97, Cli99, D+98, Lom97, Uni98h, Uni97c, Uni95a, Uni98k, UU97b, Cli99, Lev91, Mi98, Sch98a].

Univariate [Cop95c]. Universal [AW94, AS96, BE90, CadHSV96, EPR99b, EPR99a, KP99a, Sh96, St91b].

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

University [CFK+91, IEE98b, KG93, RBCE99, SKIT99, PDG199]. UNIX [Ano92a, Ano93c, Gar97c, IHR99, J91, LT91, USE90, USE92b, USE93, USE95b, WB92, Car99, De 93a, ZG96] Unanon [BWM99b, Pae99a]. Unlinkable [SSG99].


Untangling [Sch92c].

Untraceability [WP90, Wai90]. Untraceable [OO90]. Untrusted [SK98a].

Untruths [For99a]. Unveil [GC97, Gar98a].

Unveiling [Jam98]. Unveils
Gar97a, Gar98b. **Update**

[Ano94b, Ano95a, Ano95b, Ano95u, Ano96b, Ano96-28, Ano97c, Ano97-44, Ano97-45, Ano98r, MGL+98, Mey97b, Pin98, Ros95b, Ros96d, Ros97b, Ste99c, Wie97, Wie98a]. **updated** [Ano97-37]. **upon**

[BPMP97a, CCH98, LCL95, SPP98]. **Upper**

[Fer98, Al96, O’C94]. **Urge**

[GB98]. **Urgent** [Pra96]. **URL**

[Zuk98b]. **USA**

[??790, Ano98n, AA97, Auc98, Bri92, Bri93, Cop95d, Des94b, Han99, HF97, IEE97g, IEE97c, IE98e, Kal97c, Koh96, KP99b, Kra98, SJ97, St93b, St94, USE91, USE93, USE94, USE95b, USE95c, USE95a, USE96f, USE99a, USE99b, USE99c, USE99d, Wie99]. **Usability** [WT99, CG05]. **Usage** [End97]. **Use**

[AABB99, BCE+94, Brah90a, CFGS99, Con99b, Gan96a, Gar97a, Gar97b, GC97, GK98, HJL99, Iss90, KR95c, Koh90, Lan99, MG98a, MG98b, Por91, Rud91, SB94, Zuk98a, BDH97, BR97b, Ch94b, Cl99, CG05, GI97, Joh90, Ri96, Way93c, Zer96a]. **Used** [GS94a, SZ96, Car97c, Car98, Gau97, Kuk99, Sch91b, SX90, van97a]. **USENET** [Bis91]. **Usenix** [USE90d, Com96, Ros96a, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c]. **User**

[AKF94, BE90, Bus96, D99, Gog99, Gol90a, GN95b, IS99, KCC94a, KCC94b, PMP99, RR97a, RR97b, SYM98, SCT97, Web99, Zim95a, Ano95o, DF91b, MC96, Mu92, RSA94, RT93, SJS98, Sta95b]. **User-Centered [PMP99]. User-Oriented** [AKF94]. **Username** [Le96]. **Username/Password** [Le96]. **Users** [Ano96-31, Hel98a, WK97, Sha97, Sta94a]. **Uses** [Swi97, Ano97x, DK97b, Sch99g]. **Using**

[ANS97, ANS98b, Ada97a, AGS97, AHJF97, Ano991, BDPSNG97, BCK96e, BBS99a, BFP99, BW98, CIBM99, CK95, CM94d, Des96a, DS97d, ESS97, FVEA99, FW91, FY98b, GM97, GAGCDAFC99, GSS99a, HNS99, HRVV99, HJB97, IR99, JM99, JJ98c, JQ97, KR94b, KS99a, KA99, KT93, Lon92, LF99, LML98, Low96, LW99, L97, MAM95, Mih94, MCD99, Mis97, MFG95, NT99, NHB98, NNE97, Oh99, OOK91, Ou99, OMI93, PSE97, Pin97, PF98, PJ99, QQ90, RB99, SG95, SK94, Sas99a, SK96a, SK97b, SK97a, SK97c, SD99, SRY99, SR96, Sim94d, SHK99b, Sun91a, SZT98a, TA99, TA92, TYD99, TOU94, VN94, WKG97, WCS95, Yam98b, Yam99, YST99a, YY97a, YST99b, AA95, All98, Ano97, At94, BSNP96a, BSNP96b, BSD98, BGR95, BI93, Bih94a, BB95a, BBS98a, BD95a]. **using**

[CW91a, CNS98, CC95, CMG97b, CPP98, CB96, Cle96, Dan97, GK99b, GL94, Gor93b, Hor95, ISO97, Jak95, JM96a, KR95a, KC95, Kar96, Kay95, Koc95, KH97, KH98a, LC96b, LC96c, LMBO95, MHP96, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SSM94, SD97, Su98, SZT98b, ST98, T97, T198, V97, VP98, Wh93, Wil93a, Yam98a, Zho94, dR95]. **Utah**

[USE95b]. **Utility** [Zol93, Ano97m, Vu95]. **Utilization** [GRB99]. **Utilize** [MS96]. **utilizing** [SW95a].

V [IE92a]. **V.1.0** [Lim99, RSA99a]. **v2.0** [Ano97-33, RSA99b]. **V232bis** [Ano93k]. **V.5** [HH99b, KN93, Lee96, Ts’97]. **Validating** [Gai90]. **Validation**

[DDNM98, GS99a, RB99, S96, CM96]. **Validity** [GMW91, Kuk99]. **Value**

[Ack98, Eve98, Oke97, SPP98, Tay94]. **value-adding** [Eve98]. **Value** [KW99]. **Values** [GS94a, Th96]. **Vancouver** [Yua92]. **Vanstone** [Kie98, NS97c, NS97b, Sha99a]. **Vaporware**

[DDJ98e, DDJ98f]. **Variable**

[BR99a, BR99b, DW94, G95b, Sch94b, Su98, TN96a, TN96b, ZPS93]. **Variable-Input-Length** [BR99a, BR99b]. **Variable-Length** [Sch94b, Su98]. **Variance** [Kas96]. **variant** [TC97]. **Variants** [CRR99, MSS98, RS99a, Sha95a].
variation [CCN95]. variations [Zho94].
varieties [Fri92b]. Various [GQW+91].
Vasculature [BALS99]. Vatican [Alv98a].
Vector [ADEDS99, TK99, TYD99, CCH98, 
MT99, Pad98, dr95]. vectors
[LM93c, Mat91, MLA91]. Vegas
[ACN95, AA97]. Vehicle [CKN99].
Vendors [Gar97a, Gar97b, Gar98a, GB98].
Venona [HK99c, Pea97].
Ventura [Alv98a].
VerCheck [MGL+98].
Verdict [Wri94].
Veri [SY99].
Veri-KoMoD [SY99]. Verifiable
[Abe98a, AGY95b, CG98, Cr990, FR95c, 
GM95, Ped91b, Sch99i, VBD99, AGY95a, 
BD98a, Bur96, FO98, Mao97, MLY93, 
Ped91b, Ped91e, Sta96a]. Verification
[Abe98a, AB97, BGR95a, Bo98a, Bo98b, 
CDF93, DS97a, GFB93, GS99a, H92, 
MM99a, Na97, OM93, PM98, PV98, 
SM95a, SY99, Tou93, WW98b, YY99a, 
Aron97p, BGR98b, Bo97, BS95c, CM96, 
Des90a, Dwo91, JC98, JW01, Mea95, Sha97, 
YL95a, YM98, ZL99]. Verifications
[GMV98]. Verifier [JMSI96]. Verifiers
[PM98]. Verify [DS97d, Chi99a, Chi99b].
Verifying [LH96b, Sal91, DN95b, Pau98].
Verlag [Hat96]. Verlässliche [BGH95b].
Vermont [IEE96a]. Verschlüsselung [MPS94].
Verschlüsselungssysteme [W99].
Verschlüsselungsverfahren [Ger97].
Version [An97-34, An97-33, BC93a, 
BP98e, DBP96, FKK96, Gar97b, Kal98f, 
Kal98c, Kal98d, Kal98b, KS98a, R9a3f, 
Lim99, MT99a, Mc96, R9a3a, R9a4, 
DY91c, SS99b, SM98b, WABC99, CLW98, 
GM93a, G9b5, Bor93b, Lin96b]. Versus
[MGL+98]. Vertraulichkeit [FT95].
Very [HM93, MSD90, PF94, Y9a2, SN94].
Veto [OK96a]. VHDL [Oel97]. via
[BR96b, BCKxx, BM95, BS95d, DS90a, 
DN95a, DN93, EPR99b, EPR99a, Fuc99, 
HS94, JJ99b, NW98, UFC94]. Vibration
[Nas94, NA95]. VICS [Un96a]. VICTOR
[OSA91]. Victorian [Abe98b]. Victory
[Mus92]. Video [An99f, BF99, DLF97, 
DS97c, DSS98, HG97c, KBR97, KF98, 
LT99, M9T, SJ97, SB98, S9T98a, 
WKH97, WW98a, ZL99, BB90, BCB97, 
CPO+98, CH+98, CKLS96c, DS97b, HG96, 
HG97e, HG97d, HG98, HW97, HW98a, 
Lan99, Oht96, Q9N98b, SHG98, SZT98b].
Video-based [WKH97, BCB97].
Video-Steganography [MT94]. Vienna
View
[CK95, Lan98, MUSM98, MM96a, ST93, 
Ste91, ZL99, Ano97l, Pri94, U97a, Wad93].
Viewpoint [Len96b, Ste91]. Views
[DDJ98e, DDJ98d, DDJ98f, DDJ98a, 
DDJ98d, DDJ98b, DDJ98g, DDJ98h, 
DDJ99, Eri97b, L99]. VII [IE99b].
VIL [AB99a, AB99b]. VIL-MACs
[AB99a, AB99b]. Village [Ber97b]. Vinegar
[KS98d, KP99]. VINO [DW94]. Virginia
[ACM93a, ACM94a, EIE94a]. Virtual
[DFGH99, GB98, HL99, CCH98, LS98a].
VirtuFlex [An97-34]. Virus
[BGG95, Hig97b, Nac97, LF99, MC94, OY91].
Viruses [Hig97a, Wh90, Coh94].
VIS [BGH95b]. Visa [Lea99, Gau97].
Visibility [L99]. Visible [K96].
Vision
[CKN99, HCC99, PJ99, SW95b, SKIT99, 
CS99, RP97b]. Vision-Based [SKIT99].
visit [JQ98a]. Visited [FY95b]. Visual
[ABDS96, B96b, BD98b, DDGM97, Dro96, 
HK97a, HKS97b, JKVF99, KI96, N95, 
NP97, P99, P99, PN9K95, Sha98, 
St98b, BW97, Ger99b]. Visualisation
[MM99b]. Visualization
[Jan99, PH91, GTGW94].
VLSI
[ACM99, Mas91, Pai96, Pos98, Vad95, Zim99].
VoD [GMMS98]. Voice [CM97b, MB99a, 
Sha97, Cha94b, Int91b, PW98]. vol
[An97-48]. volume [Kat97]. Voting
[Boy90, JT97a, Mv93, NR94, SK94, SK95].
REFERENCES

X [Ano95x, Bel92, BALS99, KSW97a, KSW97b, Smi98b, Yu94a, Yu94b, PvO95].
X.9.44 [Ano94b]. X.952 [BK98a, BK98b, Ano96c]. X.9.F.1 [Joh99].

Y2K
[Ano98t, DDJ98b, Eri97b, Law98, MGL98].
Yaksha [Gan96b]. Yarrow [KSF99, KSF00].
Yarrow-160 [KSF00]. Year [Sch95a, Sil99, Roe95].
Years [Bon99, Vin97, BC06b, C WM+91, Den90, Gol97c, Mar96, Mey97a]. yi [IPNdbbpm91]. Yield [GMW91].
Yokohama [Iz98]. York [IEE99a, USE95c].
Yu [BY92]. YY [Nat92b].

Z [Mau91b]. Z80180 [Kal93b]. Zero [BG90, BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GSV99, G093, HT98, NOVY93, NMV99, OQ00, RS91, SI93a, BOGG90, BBP95a, BBP95b, DF93, DP94, DF91b, Sah99]. Zero-Knowledge [BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, G093, HT98, NOVY93, NMV99, OQ00, RS91, SI93a, BOGG90, BBP95a, BBP95b, DF93, DP94, DF91b]. zeta [Kob91c]. zeta-polynomials [Kob91c].

References

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

Anonymous:1997:ACC

ANSI:1988:FIE

Anshel:1993:PMT

ANSI:1995:ANS


Asmuth:1981:EAC


Anderson:1996:TPP


Anderson:1996:TFN


Ayadi:1997:VCP


An:1999:CVF


An:1999:CVM

Abadi:1999:STS


Anderson:1998:NFA


Ateniese:1996:CBV


Aiello:1998:SAC


Abeles:1998:SVP


Abe:1999:RDM

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


[ABK97] Susan Abraham. Software encryption export policy analysis. Thesis (B.A.), California Polytechnic State University, San

Auyong:1997:ASC

Apolloni:1990:TNN

ASCFS:1997:XPK

An:1999:ODR

Angelo:1994:DFS

Alexi:1984:RRB

Alexi:1988:RRF
Werner Alexi, Benny Z. Chor, Oded Goldreich, and Claus-P. Schnorr. RSA and Rabin functions: Certain parts are as hard as


REFERENCES


REFERENCES


REFERENCES

ACM:1997:PEA


ACM:1997:PTN


ACM:1998:AWJ


ACM:1998:PTA


ACM:1999:PPA


ACM:1999:PTF

ACM:1999:SPCd


Ajtai:1999:PKC


REFERENCE


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


Augot:1998:DSM


Alagappan:1990:PDA


Adleman:1979:SAD


Adleman:1983:BGK


Adleman:1987:PRD


Asokan:1999:APT


Alves-Foss:1995:ACS

REFERENCES


Abadi:1998:BMCb


Aura:1999:SLM


Agarwal:1992:RSO


Atkins:1995:MWS


Afanassiev:1997:FMA

[AGS97] Valentine Afanassiev, Christian Gehrmann, and Ben Smeets. Fast message authentication using efficient polynomial evalua-
REFERENCES

Alon:1995:DRV


[AGY95a]

Alou:1995:EDR


[AGY95b]

Alberda:1997:UFP


[AHdJF97]

Autexier:1999:SDI


[AHMS99]

Aiello:1998:NCS


[AHV98]

Akritas:1983:CEA

A. G. Akritas, S. S. Iyengar,

**Angluin:1995:WWM**


**Al-Kadi:1998:OCA**


**Alvarez:1999:AAS**


**Aberer:1994:DUO**


**Akoka:1999:CDP**


**Abdelguerfi:1996:GEI**


**Anlauf:1999:TSL**

M. Anlauf, P. W. Kutter, and A. Pierantonio. Tool support for language design and prototyping with


REFERENCES

tronic). URL http://
www.elsevier.com/gej-
ng/10/19/19/28/17/18/
abstract.html.

[Ale98] Thomas J. Alexandre. A
Java-based platform for in-
tellectual property protec-
tion on the World Wide
Web. Computer Networks
and ISDN Systems, 30(1–
CODEN CNISE9. ISSN
0169-7552 (print), 1879-
2324 (electronic). URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/072101.html;
http://www.elsevier.
com/cas/tree/store/comnet/
sub/1998/30/1-7/1863.
pdf.

[All97] Heber E. Allen. Data en-
cryption and conflict with
free speech. Thesis (Bach-
elor’s), Arizona State Uni-
versity, Tempe, AZ, USA,

[All98] Chaka Allen. Steganog-
raphy using the minimax
eigenvalue decomposition.
Thesis (M.S.), Iowa State
University, Ames, IA, USA,

[ALN87a] Niv Ahituv, Yeheskel Lapid,
and Seev Neumann. Pro-
cessing encrypted data.
Communications of the As-
sociation for Computing
Machinery, 30(9):777–780,
September 1987. CODEN
CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http:
//www.acm.org/pubs/toc/
Abstracts/0001-0782/30404.
html.

and Seev Neumann. Ver-
yfying the authentication
of an information sys-
tem user. Computers
and Security, 6(2):152–
157, April 1987. CODEN
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/0167404887900861

[ALN87b] Niv Ahituv, Yeheskel Lapid,
and Seev Neumann. Ver-
yfying the authentication
of an information sys-
tem user. Computers
and Security, 6(2):152–
157, April 1987. CODEN
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/0167404887900861

[ALO98] W. Aiello, S. Lodha, and
R. Ostrovsky. Fast digital
identity revocation. Lecture
Notes in Computer Science,
1462:137–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Alv98a] David Alvarez. Faded lust-
tre: Vatican cryptography,
1815–1920. In Deavours
et al. [DKK+98], pages 191–
225. ISBN 0-89006-862-
US$78.20. URL http://
REFERENCES


Alvarez:1998:IDC


Alvarez:1998:PCS


Akl:1985:FPR


Adams:1988:SRC


Akl:1985:FPR


Adams:1989:SRC

REFERENCES


REFERENCES


version of this paper has appeared in the Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy.

Anderson:1995:RPP


Abadi:1996:PEP


Andrew:1986:CSI


Anderson:1993:PRT


Anderson:1994:FSE

REFERENCES

Anderson:1994:WCF

Anderson:1996:CEM

Anderson:1996:SLS

Anderson:1996:IHF

Anderson:1998:EWF

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

Anonymous:1960:CNH

Anonymous:1976:CCA

Anonymous:1978:CSD

Anonymous:1978:NPAd

Anonymous:1978:ODA

Anonymous:1979:SSA

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


[Ano82c] Anonymous. Encryption scrambling the satellite signal for security, 1982. 1 sound cassette (75 min.).


REFERENCES

Anonymous: 1987: EVE


Anonymous: 1987: HSE


Anonymous: 1987: MAU


Anonymous: 1987: TWP


Anonymous: 1988: BRCb


Anonymous: 1988: CCJc


Anonymous: 1988: CCJb

REFERENCES

Anonymous:1988:DEK [Ano88d]

Anonymous:1988:DESb [Ano88e]

Anonymous:1988:DESa [Ano88f]

Anonymous:1988:EVE [Ano88g]

Anonymous:1988:ERH [Ano88h]

Anonymous:1988:PED [Ano88i]
REFERENCES

Anonymous:1988:RIA


Anonymous:1989:SZS


Anonymous:1990:SEL


Anonymous:1991:ESS


Anonymous:1991:FFL


Anonymous:1991:E


Anonymous:1992:AUd


Anonymous:1992:DES


Anonymous:1992:DDS

Anonymous. Double data security. *Datamation*, 38(??):21–??, November 15,
Anonymous:1993:ACT


Anonymous:1993:BRd


Anonymous:1993:CKR


Anonymous:1993:CSA


Anonymous:1993:CNh


Anonymous:1993:FSH


Anonymous:1993:JIK


Anonymous:1993:LC


Anonymous:1993:SBh


Anonymous:1993:SMC

Anonymous. Secure E-Mail Cheaply With Software Encryption. Datamation, 39(23):48–??, December 01,
REFERENCES

1993. CODEN DTMNAT. ISSN 0011-6963.

Anonymous:1993:WND

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

Anonymous:1994:CNe


Anonymous:1994:DAX


Anonymous:1994:ERB


Anonymous:1994:HSK


Anonymous:1994:ICI


Anonymous:1994:Kee


Anonymous:1994:Lba

REFERENCES

Anonymous:1994:Ll

Anonymous:1994:PRP

Anonymous:1994:Uc

Anonymous:1994:WAS

Anonymous:1994:ARLa

Anonymous:1995:AUM

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

Anonymous:1995:ARLb

Anonymous:1995:AURa
Anonymous:1995:ARD


Anonymous:1995:DAS


Anonymous:1995:ENa


Anonymous:1995:ENb


Anonymous:1995:EEW


Anonymous:1995:ENE


Anonymous:1995:FSH


Anonymous:1995:FRE


Anonymous:1995:HPE

REFERENCES

Anonymous:1995:IUA


Anonymous:1995:NIX


Anonymous:1995:OIN


Anonymous:1995:PTN


Anonymous:1995:RLM


Anonymous:1995:SDE


Anonymous:1995:SUE


Anonymous:1995:SEE

Anonymous:1995:TEV


Anonymous:1995:XAV


Anonymous:1996:NIS


Anonymous:1996:RF


Anonymous:1996:ADX


Anonymous:1996:BCU


Anonymous:1996:CED


Anonymous:1996:CID

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


Anonymous:1996:CCC


Anonymous:1996:CSIa


Anonymous:1996:CPD


Anonymous:1996:EME


Anonymous:1996:EBS

Anonymous. Encryption battle sees possible break through. Network Security,
REFERENCES

Anonymous:1996:ERK


Anonymous:1996:ERM


Anonymous:1996:EKE


Anonymous:1996:ECC


Anonymous:1996:FDC


Anonymous:1996:GPT


Anonymous:1996:HET

REFERENCES

Anonymous:1996:SCG

Anonymous:1996:SAS

Anonymous:1996:SUS

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

Anonymous:1996:UDE


Anonymous:1997:RDSa


Anonymous:1997:AES


Anonymous:1997:AUC


Anonymous:1997:AWS


Anonymous:1997:AIR

Anonymous. Announcements: In this issue: The
REFERENCES


**Anonymous:1997:ARDa**


**Anonymous:1997:ARDb**


**Anonymous:1997:ADF**


**Anonymous:1997:BUF**


**Anonymous:1997:CFG**


**Anonymous:1997:CKG**


**Anonymous:1997:CVC**

Anonymous:1997:DEU


Anonymous:1997:DHE


Anonymous:1997:DNH


Anonymous:1997:EAS


Anonymous:1997:ENa


Anonymous:1997:ENb


Anonymous:1997:ENc


Anonymous:1997:EAJ


Anonymous:1997:ECR

Anonymous. Encryption compromise on rocky


Anonymous: 1997:MNL


Anonymous: 1997:MLE


Anonymous: 1997:MEP


Anonymous: 1997:NPP


Anonymous: 1997:NPA


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; TerraSpell 97; FileDrive File Transfer Server; journyx WebTime. *Linux Journal*, 43:??, November 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Anonymous: 1997:PEH

Anonymous. PGP en-
REFERENCES

Anonymous:1997:RAJ


Anonymous:1997:RAS


Anonymous:1997:RCU


Anonymous:1997:RBE


Anonymous:1997:SFR


Anonymous:1997:SAP

Anonymous. SecurID authentication protects corporate information. Net-
REFERENCES


Anonymous:1997:SUE


Anonymous:1997:TER


Anonymous:1997:UUS

REFERENCES


Anonymous:1997:UEL


Anonymous:1997:UPP


Anonymous:1997:VPA


Anonymous:1998:ABF


Anonymous:1998:ARD


Anonymous:1998:CSIb


Anonymous:1998:CPP

Anonymous:1998:Casb


Anonymous:1998:CasA


Anonymous:1998:CDR


Anonymous:1998:CSCb


Anonymous:1998:ICS


Anonymous:1998:EN


Anonymous:1998:EWB


Anonymous:1998:Ea

Anonymous:1998:LEE


Anonymous:1998:PCA


Anonymous:1998:SEF


Anonymous:1998:SIC


Anonymous:1998:SUP


Anonymous:1998:TBF

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


Anonymous:1998:UGT


Anonymous:1998:UFR


Anonymous:1998:RDS


Anonymous:1999:AWS


Anonymous:1999:CCI


Anonymous:1999:CEV


Anonymous:1999:DSC


Anonymous:1999:DSV

Anonymous. DREO secure video conferencing and

Anonymous:1999:EDB


Anonymous:1999:EPFa


Anonymous:1999:EGC


Anonymous:1999:KNT


Anonymous:1999:L

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


Anonymous:1999:ULE


Anonymous:1999:WDE


ANSI:1997:AXP


ANSI:1998:AXD


M. S. Anderson and M. A. Ozols. Covert channel analysis for stubs. In Anderson [And96c], pages 95–113. CODEN
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>
REFERENCES


Aumann:1998:AES


Aumann:1999:ITS


Arazi:1993:AEA


Arensberg:1921:CD


Arensberg:1922:CSP


Adamson:1995:JSR

Abdulla:1999:OMS


Adleman:1999:AMC


Adleman:1999:HPN


Aiello:1999:HSP


Alpern:1983:KEU


Atici:1996:UHM


Aiello:1999:HPN

REFERENCES


Akl:1983:CSP


Ateniese:1999:SOI


Atallah:1999:ATC


Atanasiu:1993:AEU


Atkins:1993:CKE


Atkinson:1995:RIA


Aparicio:1999:ITD


Avolio:1998:PCP


Anderson:1996:NC


Alabbadi:1994:SDS


Alabbadi:1995:DSS


Angel:1999:JQH

REFERENCES

Aspray:1988:RCD


AufderHeide:1999:PGP


Ayoub:1968:EKR


Ayoub:1968:EEK

[AYo68b] F. Ayoub. Erratum: En-

[F. Ayoub, 1981: EKR]


[F. Ayoub, 1983: DCE]


[B. Bernstein et al., 1996: ISB]


[B. Bernstein et al., 1996: VPA]


[B. Bach, 1988: HGF]


[A. Bacard, 1995: CPH]

REFERENCES


REFERENCES


[Bar75] Wayne G. Barker. Cryptanalysis of the simple sub-

[Barker:1977:CHC]

[Barker:1979:CEC]

[Barker:1979:HCCa]

[Barker:1979:HCCb]

[Barker:1984:CSG]

[Barrett:1987:IRS]
REFERENCES


ence Keynote Address, January 17, 1994; San Francisco, CA. Audio tape: 90 minutes.


REFERENCES


[BB97]
3. The Trifid cipher. — v.
4. Cryptographic ABC’S;
   Substitution and transposi-
   tion ciphers, by William
   G. Bryan. — v.
5. Cryptographic ABC’s; peri-
   odic ciphers, miscellaneous,
   by William G. Bryan.

**Bowers:1967:PC**

William Maxwell Bowers
and William G. Bryan.
*Practical cryptanalysis.* Amer-
ican Cryptojgm Association,
Greenfield, MA, USA, 1967.

**Blakley:1979:RSA**

G. R. Blakley and I. Borosh.
Rivest–Shamir–Adleman pub-
lic key cryptosystems do not
always conceal messages.
*Computers and Mathemat-
ics with Applications*, 5(3):
169–178, 1979. CODEN
CMAPDK. ISSN 0898-1221
(print), 1873-7668 (elec-
tronic).

**Bennett:1985:UQC**

Charles H. Bennett and
Gilles Brassard. An up-
date on quantum cryptog-
raphy. In Blakley and
Chaum [BC85], pages 475–
480. CODEN LNCSD9.
ISBN 0-387-15658-5; 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/

**Bennett:1989:EQC**

C. H. Bennett and G. Bras-
sard. Experimental quan-
tum cryptography: the
dawn of a new era for
quantum cryptography:
the experimental proto-
type is working. *ACM
SIGACT News*, 20(4):78–
80, November 1989. CO-
DEN SIGNDM. ISSN
0163-5700 (print), 1943-
5827 (electronic).

**Ben-Aroya:1994:DCL**

Ishai Ben-Aroya and Eli Bi-
ham. Differential crypt-
analysis of Lucifer. *Lecture
Notes in Computer Science*,
773:187–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Biham:1995:HSU**

E. Biham and A. Biryukov.
How to strengthen DES us-
ing existing hardware. *Lec-
ture Notes in Computer
Biham:1995:IDA


Blaze:1995:SLE


Baum:1981:RPC


Bennett:1991:EQC


Barni:1998:MPI


Blakley:1993:TSD

B. Blakley, G. R. Blakley, A. H. Chan, and J. L.
REFERENCES


Biham:1999:IOS


Blackburn:1996:EMS


Bennett:1992:QC


Bauer:1983:KDP


Biham:1998:CM


Bertilsson:1990:CVE

REFERENCES

Bleichenbacher:1995:SRL


Benantar:1996:AOS


Boyar:1995:SZ


Boyar:1995:SZK


Bennett:1988:PAP


Biham:1999:BGD

Biham:1998:CSR


Blaze:1998:DPA


Biham:1999:CSR


Biham:1999:MMA


Biehl:1994:CPB


Blakley:1985:ACP

REFERENCES

0558/tocs/t0196.htm; 
http://www.springerlink.com/content/cemajg0qmeev/ 
; http://www.springerlink.com/openurl.asp?genre= 
issue&issn=0302-9743& 
volume=196. CRYPTO 84: 
a Workshop on the Theory 
and Application of Crypto-
tographic Techniques, held 
at the University of Cali-
ifornia, Santa Barbara, Au-
gust 19-22, 1984, sponsored 
by the International Asso-
ciation for Cryptologic Re-
search.

Bender:1990:IEC

Andreas Bender and Guy 
Castagnoli. On the imple-
mentation of elliptic curve 
cryptosystems. Lecture 
Notes in Computer Science, 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

Beimel:1993:UIS

Amos Beimel and Benny 
Chor. Universally ideal se-
cret sharing schemes (pre-
liminary version). Lecture 
Notes in Computer Science, 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic). URL http://link.springer-
ny.com/link/service/series/0558/ 
bibs/0740/07400183.htm; 
http://link.springer-
ny.com/link/service/series/1

Bos:1993:PUS

J. N. E. Bos and D. Chaum. 
Provably unforgeable sig-
natures. Lecture Notes 
in Computer Science, 740: 
1–14, 1993. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

P. Béguin and A. Cresti. 
General short computa-
tional secret sharing schemes 
Lecture Notes in Computer 
CODEN LNCSD9. ISSN 
0302-9743 (print), 1611- 
3349 (electronic).

Beimel:1995:SSP

A. Beimel and B. Chor. 
Secret sharing with pub-
lic reconstruction. Lecture 
Notes in Computer Science, 
963:1–14, 1995. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic).

Blundo:1995:SRB

Carlo Blundo and Antonella 
Cresti. Space require-
ments for broadcast en-
cryption. Lecture Notes 
in Computer Science, 950: 
287–298, 1995. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (elec-
tronic). URL http:/
REFERENCES


Blair:1999:DRA


Baritaud:1993:SPK


Brucoli:1999:DHC


Bas:1998:SSB


Boyar:1991:CUS

REFERENCES


REFERENCES


[Beth:1998:Eb]

[Bellare:1996:HC]


[Bellare:1996:KHF]

[Bellare:1996:MAU]
REFERENCES


REFERENCES


**Bao:1999:NTM**


**BDC+95**


**Burmester:1992:EZK**


**Branwyn:1995:IRA**


**Blundo:1994:MSS**

REFERENCES


Bondalapati:1999:DDE

Boneh:1998:ARG

BenAyed:1999:MFP
R. Ben Ayed, J. Desharnais, M. Frappier, and A. Mill. Mathematical foundations for program transformations. Lecture Notes in Computer Science, 1559:

Blundo:1999:PSS

Bao:1998:MFA

Blundo:1993:IRS
REFERENCES


REFERENCES

Bellare:1997:CST

Boneh:1997:ICC

Benaloh:1994:OWA

Bosselaers:1997:RCH

Bellare:1998:RAN
REFERENCES


REFERENCES


[Bea97] Donald Beaver. Commodity-based cryptography (ex-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

**Beth:1998:Ea**

[T. Beth. Eurocrypt '82. Lecture Notes in Computer Science, 1440:9–12, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).]

**Beutelspacher:1994:CIA**


**Blaze:1996:MKC**


**Beimel:1997:RCP**


**Boneh:1997:EGS**


**Balfanz:1999:HHC**


**Beimel:1999:RCP**


**Blaze:1998:FTR**


**Boyd:1999:EEC**


**Beth:1992:PKC**


**Beth:1992:PCS**

REFERENCES


REFERENCES


Bellare:1993:DPK


Baldwin:1998:PPR


Boyapati:1999:KSD


Bellare:1994:ICC


Bellare:1995:ICA

REFERENCES


REFERENCES


REFERENCES


[BGT96] M. Benantar, R. Guski, and K. M. Troidle. Access control systems: From host-centric to network-

**Bosselaers:1993:CWP**


**Bosselaers:1996:FHP**


**Biget:1997:HSC**


**Bosselaers:1997:SDP**


**Beaver:1993:CPP**

Donald Beaver and Stuart Haber. Cryptographic protocols provably secure against dynamic adversaries. *Lecture Notes in
REFERENCES

Baker:1998:LTC

Beygelzimer:1999:OWF

Bhimani:1996:SCI

Black:1999:UFS

Bubeck:1995:DSC
T. Bubeck, M. Hiller, W. Kuchlin, and W. Rosen-
REFERENCES


Bayer:1993:IER


Bayer:1993:IER

Bellare:1998:MTF


Bellare:1998:MTF

Brassard:1998:QCH


Brassard:1998:QCH

Bertilsson:1993:CPS


Bertilsson:1993:CPS

Bao:1994:RAF

REFERENCES

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


REFERENCES


Biham:1994:MOA


Biham:1995:CMM


Biham:1995:MLC


Biham:1996:CTM

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

Biham:1997:CL


Biham:1997:FNI


Biham:1997:FSE


Biham:1998:CMM

REFERENCES

Biham:1998:IOS

Biham:1999:CM
http://www.nist.gov/aes. No slides for the conference talk are available.

Biham:1999:CTM
Eli Biham. Cryptanalysis of triple modes of operation.

Biham:1999:NCA
http://www.nist.gov/aes. No slides for the conference talk are available.

Birrell:1985:SCU
REFERENCES


[Bis89b] Matt Bishop. The fast encryption package. Moffett
REFERENCES


REFERENCES

Blakley:1994:LAA


Brooks:1994:ST


Biham:1995:KPA


Blakley:1995:GPS


Blum:1995:DPC


Bocharova:1995:FEC


Buydos:1997:C

REFERENCES


REFERENCES


Brown:1993:IRD

Bellare:1994:SCB

Borst:1997:TAR

Bellare:1998:LB1

Bellare:1998:LRB
REFERENCES

ny.com/link/service/series/0558/papers/1403/14030266.pdf. [BL96a]

Bakhmurov:1999:DEE


Burgett:1998:CLD


Boneh:1996:ABF


Boneh:1996:ABB


Binsted:1999:CDS

REFERENCES


Blahut:1983:TPE


Blakley:1985:ITF


Blanchard:1989:CSS


Blaze:1993:TMS


Blackburn:1994:IRO
REFERENCES

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

Blaize:1994:KME

Blaize:1996:HBE

Blaize:1996:HEL

Blaize:1996:OKE

Bleichenbacher:1996:GES

Bleichenbacher:1997:SKP

Bleichenbacher:1998:CCA
Daniel Bleichenbacher. Chosen ciphertext attacks against

Blair:1998:SEP

**Bleumer:1998:BYP**


**Barber:1999:AOD**


**Buldas:1998:TBL**


**Beth:1994:CCB**


**Baaz:1999:SDC**

REFERENCES


REFERENCES


**Blakley:1985:SRS**


**Beale:1989:EUR**


**Bellare:1990:NIO**


**Bellovin:1991:LKA**


**Brickell:1991:IID**

REFERENCES

CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic).


REFERENCES


REFERENCES

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

Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD


Blackburn:1997:CNP


Blackburn:1997:CTA


Biedl:1998:GMF


Blackburn:1994:WPK

[S] Simon Blackburn, Sean Murphy, and Jacques Stern.


REFERENCES


Book:1985:SNP

Book:1985:SNS

Book:1985:VTA

Book:1985:CRE
REFERENCES


REFERENCES


Bolignano:1997:TMC

Bolignano:1998:IPB

Bolignano:1998:IPM

Bond:1947:FSC


rfc/rfc1416.txt. Obsoleted by RFC1416 [Bor93c]. Status: EXPERIMENTAL.

Borman:1993:RTAb


Borman:1993:RTAc


Borcherding:1995:NAR


Borcherding:1996:LAD

[Bor96] M. Borcherding. Levels of authentication in distributed agreement. Lecture Notes in Computer Science, 1151:40–??, 1996. CODEN LNCS90. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bosworth:1982:CCC


Bosma:1990:PPC


Bosselaers:19xx:EFH


Bounas:1985:DDS

[Adam C. Bounas. Direct determination of a “seed”

[Bow59]

**Boucher:1994:GPA**


[Bou94]

**Bovenlander:1998:SCS**


[Bov98a]

**Bowers:1959:DSP**


[Bow59]

**Bowers:1960:BC**


[Bow60a]

**Bowers:1960:TC**


[Bow60b]

**Bowling:1993:SEA**


[Bow93]

**Bowers:19xx:PC**

REFERENCES

Boyd:1986:CPC


Boyd:1988:CCB


Boyar:1989:ISPb


Boyar:1989:ISPa


Boyd:1990:NMK


Boyd:1992:FFA


Boyd:1995:CCC

REFERENCES


Papers from the 5th IMA Conference on Cryptography and Coding. [Boy99]


REFERENCES

Beker:1989:CC


Bilchev:1995:ACM


Bosseelaers:1995:IPS


Baric:1997:CAF


Brinkley:1997:SFS


Buchmann:1997:OWF

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Bellare:1994:OAEa


Bellare:1995:OAE


Bellare:1995:PSS


Bellare:1996:TCA


Bellare:1996:ESD


Bellare:1996:RRC


Brassard:1987:IMC


Brassard:1988:MCT


Brassard:1989:CCb


Brassard:1989:CCa


Brand:1990:PNU


Brassard:1990:CCH


Brassard:1990:ACC

REFERENCES


Brands:1995:LEC

Brands:1995:RBS

Brassard:1995:CCB

Brassard:1995:IDR

Brackin:1996:DCP

Brassard:1998:C

Breitrose:1997:ALD

Breitrose:1997:DEM
REFERENCES


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

REFERENCES


Originally published as report of the Ad hoc Committee to Study the Communications Intelligence Activities of the United States, George A. Brownell, chairman.

Brooke:1986:BRB


Browne:1994:ECL


Brock:1996:CCP


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB


Brundrett:1998:KAW

Peter Brundrett. Kerberos authentication in Windows NT 5.0 domains. ;login: the USENIX Association newsletter, 23(3):??, May 1998. CODEN LOGNEM. ISSN 1044-6397. URL

**Bentley:1999:SOE**


**Bryan:1967:CA**


**Brillhart:1967:SFR**


**Branstad:1982:ISS**


**Brickell:1983:SRK**


**Benois:1986:CSE**


**Biham:1990:DCD**


**Brown:1990:DPT**

Lawrence Brown and Jennifer Seberry. On the design of permutation $P$ in DES type cryptosystems. *Lec-
REFERENCES


Beth:1991:NEC


Beth:1991:NSE


Biham:1991:DCD


Biham:1991:DCFb


Biham:1991:DCFa


Biham:1991:DCS

Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II,


REFERENCES

**Blaze:1995:MBC**


**Boneh:1995:CSF**


**Bose:1995:ATV**


**Bruckstein:1995:SSD**


**Brunnstein:1995:IPR**


**Biham:1997:DFA**

REFERENCES


S. Bakhtiar and R. Safavi-Naini. Application of PVM
REFERENCES


[BSW89] 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.


REFERENCES

BT:1997:BEC


Barmawi:1998:AEK


Boney:1996:DWA


Buck:1982:PCS


Buchmann:1991:NTA


Bucholtz:1995:EEC


REFERENCES


REFERENCES


REFERENCES

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


[BW98] U. Brandes and D. Wagner. Using graph lay-
out to visualize train inter-
connection data. Lecture
Notes in Computer Science,
1547:44–56, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).


REFERENCES


[CA81] Computer and Business Equipment Manufacturers
REFERENCES


REFERENCES


Adam Douglas Cain. Text steganography. Thesis (M.S.), University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, USA, 1996. vii + 90 pp.


Q. G. Campbell. Meteor burst communications protocols — the history and role of computing technology in radio...


Carter:1997:BLC

Carter:1997:CCC

Carter:1998:CCC

Carasik:1999:USS

Caswell:1995:EDA

Chren:1996:RDU

Clark:1981:ECC

Chen:1995:SIB
Jonathan Jen-Rong Chen and Henry Ker-Chang


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Christoffersson:1988:CUH


Crawford:1992:AS


Coe:1995:DDC


Castelfranchi:1999:BMA


Chouinard:1996:ITA


Callas:1999:FU1

REFERENCES

Ceruzzi:1991:RCK


Chor:1994:TT


Coppersmith:1996:LRR


Coppersmith:1996:LER

  bibs/1070/10700001.htm;


[Cramer:1996:MAS]

[Chor:1985:RRL]

[Cover:1987:OPC]
Thomas M. Cover and B. Gopinath, editors. Open Problems in Communication and Computation. Springer-Verlag, Berlin, Germany / Heidelberg,
REFERENCES


Chor:1988:UBS


Catalano:1998:NES


Canetti:1999:ETP


Cranor:2005:SUD


Clark:1993:EMS

REFERENCES

ac.uk/~fapp2/steganography/bibliography/031208.html


Canetti:1999:AST


Chen:1996:TAP


Chen:1997:KEM


Chen:1997:AUM


Chor:1985:VSS


Chen:1997:SSR


Cramer:1997:SOE

REFERENCES

E964 1997. Sponsored by the International Association for Cryptologic Research (IACR).


[CH97b] Chin-Chen Chang and Shin-Jia Hwang. A sim-

**Chen:1998:PFR**  

**Corcoran:1999:SCB**  

**Cordon:1999:AMD**  

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

**Chaum:1981:UEM**  

**Chandler:1983:IMC**  
REFERENCES

org/annals/an1983/a3260abs.htm.


[Cha86a] C. C. Chang. On the design
REFERENCES


**Chapman:1986:NFS**


**Chapman:1986:NFS**


**Chaum:1990:SDA**


**Chaum:1992:AEPb**


**Chaum:1992:AEPa**


**Chaum:1993:NCB**

B. Chambers. Two stream ciphers. *Lecture Notes in Computer Science*, 809:
REFERENCES

51–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chandler:1994:IAF


Chabaud:1995:SSC


Chaum:1995:DCS


Chaum:1998:Cb


Chadwick:1999:IWS


Chan:1999:WES


Chau:1999:QCE

REFERENCES


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


REFERENCES


Chor:1986:TIP


Chung:1998:DWCb


Christiansen:1978:SL


Christoffersson:1988:MAE


Christianson:1998:SPI


Christianson:1999:DSCb

Christianson:1999:SPI

Chuang:1989:NES

Currie:1996:SEL
D. L. Currie and C. E. Irvine. Surmounting the effects of lossy compression on steganography.


Ciarcia:1986:BHD

Cao:1999:DTJ

Clark:1995:SRP

Chabaud:1998:DCS
Collins:1999:DCL

Coster:1992:ILD

Coppersmith:1996:PMT

Coppersmith:1995:TCB

Charlwood:1998:EXA

Chari:1999:TSA


[CK95] P. A. R. Cole and M. S. Khan. Modelling 3-D rigid solid objects using the view signature II representation scheme. Lecture Notes in Computer Science, 970:
REFERENCES


References


Coradeschi:1999:IVD


Chan:1988:IEC


Chang:1997:PCM


Cox:1997:PWR


Cox:1998:SGM


Claudy:1912:TMS

REFERENCES


REFERENCES


REFERENCES

on RSA-type cryptosystems based on singular cubic curves over $\mathbb{Z}/n\mathbb{Z}$. 

**Cheng:1998:MVR**


**CM85**


**CM95**


**CM96**


**CM95**


**Callahan:1996:AVV**

John R. Callahan and Todd L. Montgomery. An approach to verification and

**Cachin:1997:USA**


**Chang:1997:CAS**


**Cooperman:1997:SMD**


**Cox:1997:RWI**


**Chen:1998:DRT**


**Camenisch:1999:SEG**

**Charlton:1999:DPM**


**Christianson:1999:DSCa**


**Coradeschi:1999:HMC**


**Chen:1998:SCC**


**Cohen:1993:AAA**

REFERENCES

0558/tocs/t0673.htm;
issue&issn=0302-9743&
volume=673.

Canetti:1999:ECS


Charnes:1997:SSH


Chor:1989:SCT

[CMS89] Benny Chor, Michael Merritt, and David B. Shmoys. Simple constant-time consensus protocols in realistic failure models. Journal of the Association


Chuan-Ming:1994:RTR


Craver:1997:CIW


Craver:1998:RRO

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


Crilly:1987:BPB

Coron:1999:SRPb


Coron:1999:SRPb

Coron:1999:SRPb

Coupé:1999:ELA


Coupé:1999:ELA

Chao:1998:CSE


Chao:1998:CSE
REFERENCES

Coltell:1998:AOL

Cocks:1997:SKG

Cohen:1987:CCI

Cohen:1987:IIP

Cohen:1994:SCC

Cohen:1996:RRA

Cohen:1999:MNSk

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

[Com94c]


[Com87]


[Com90]


[CSL:1994:DES]


[CERT:1996:PSA]

Computer Systems Laboratory (U.S.). *Escrowed Encryption Standard (EES)*.

[CSL:1994:EES]

Commission of the European Communities. *Ensuring security and trust*


[Con98] Allen W. M. Coombs. The making of Colossus. An-
REFERENCES

Coppersmith:1984:FEL


Coppersmith:1987:C


Coppersmith:1989:AID


Coppersmith:1994:DES


Charnes:1995:CSE

Coppersmith:1995:ACA


Coppersmith:1995:FSR


Coppersmith:1995:ACC


Coppersmith:1995:FSR


Corcoran:1998:MFS

David Corcoran. Muscle flexes smart cards into
REFERENCES


Coron:1999:SRSa


Coppersmith:1986:DL


Courville:1986:MCC


Courington:1993:PEA


Coutinho:1999:MCN


Cremonini:1999:CCA


Chaum:1987:ACE

REFERENCES


[CP99] Tae-Yun Chung, Kang-Seo Park, Young-Nam Oh, Dong-Ho Shin, and Sang-Hui Park. Digital water-
marking for copyright protection of MPEG2 compressed video. In IEEE [IEE98c], pages 336–337. CODEN DTPEEL. ISBN ???? ISSN 0747-668X. LCCN ???? IEEE catalog number 98CH36160.

Charney:1997:PSC

Cheon:1998:TEA

Camenisch:1995:BSB

Chor:1985:KTP

Carroll:1988:ACP

Carroll:1988:CC
REFERENCES

Chor:1988:KTP

Chaum:1991:USD

Caronni:1997:HEE

Crawford:1992:ASA
[Cra92] David J. Crawford. Autoscratcher and the super-

Craig:1996:CDC

Craver:1997:PSP

Craver:1998:PKS
REFERENCES


REFERENCES


REFERENCES

PLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [YT96].


REFERENCES


Chaum:1989:SCF


Csirmaz:1995:SSM


Coppersmith:1994:ABP


Chang:1997:GSS


Chen:1999:TPS


Collberg:1999:SWM


Cox:19xx:NST

Chao:1994:DEC


Currier:1998:MPT


Cusick:1996:BNFa


Cusick:1997:CRN


Ciminiera:1989:AMM

REFERENCES

Calvelli:1993:ARS


Chabaud:1995:LBD


Cohn:1999:MC


Chamou:1991:CSU


Chang:1991:BCC


Cusick:1991:RIC


Campbell:1993:G

REFERENCES

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

Chmora:1994:ECC


Chang:1997:SCO


Coppersmith:1998:CT

Don Coppersmith, David Wagner, Bruce Schneier, and John Kelsey. Cryptanalysis of TWOPRIME.

Ceruzzi:1991:RGC

REFERENCES


Chang:1998:BSC


Craver:1998:TTL


Cao:1990:DKC


DeMillo:1983:ACC


Dittmann:1998:MSW


D’Agapeyeff:1939:CC

REFERENCES

DAgapeyeff:1971:CC


Daemen:1995:HFC


Daemen:1998:MSK


Daemen:1999:RAI


Dalton:1997:KSW


Damgaard:1990:ACE


Damgaard:1990:DPH

REFERENCES


[Dam96] Kenneth W. Dam. The role of private groups in public policy: cryptography and the National Research Council. Occasional papers from the Law School, the University of Chicago; no.
REFERENCES

LCCN QA76.9.A25 D34 1996.


REFERENCES

Davies:1985:MAA


Davies:1991:ACE


Davies:1979:IHS


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].

Davida:1979:IHS


DRC:1985:AAN

[Dat85]

[Dat79]

[Dat81]
REFERENCES

540-54620-0 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E964 1991. Rev. and expanded papers from the meeting which was sponsored by the International Association for Cryptology Research (IACR) and others.


[Dav98d] Donald W. Davies. The Lorenz cipher machine
REFERENCES


REFERENCES


REFERENCES

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

**Dobbertin:1996:RSV**


**DHalluin:1999:ASR**


**DeWin:1996:FSI**


[DD95b] Y. Desmedt, G. Di Crescenzo, and M. Burmester. Multiplicative non-Abelian sharing schemes and their application to threshold cryptography. In Pieprzyk
and Safavi-Naini [PSN95a], pages 21–32.

DiSanti:1994:HSF


Davio:1985:EHS


Delaigle:1997:LCW


DDJStaff:1998:NVS


DDJStaff:1998:NVb

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

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

DDJStaff:1998:NVY

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

DDJ:1998:NVN

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

DDJStaff:1998:NVd

[DDJ98h] DDJ Staff. News and views: The secret story of nonsecret encryption; Netscape

**DDJstaff:1999:NVR**


**DePaoli:1998:WBS**


**Denny:1994:FR**


**Delaigle:1996:DW**


**Delaigle:1998:PAD**


**Dolev:1991:NC**

REFERENCES


References

DeSantis:1994:KCQ

DeSantis:1999:NIZ

Darmstaedter:1998:LCS

DeVries:1953:SMC

DeAlvare:1990:HCC

DeDecker:1993:USK

DeSchutter:1993:TFA
REFERENCES

LNCS.9 ISSN 0302-9743 (print), 1611-3349 (electronic).

DeSoete:1993:PKC


DeSantis:1995:ACE


DeSantis:1998:E


DeSchutter:1998:TFA


DeSmit:1998:GAE


DeMoliner:1999:STB


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

REFERENCES


REFERENCES

Notes in Computer Science, 718:3–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Desmedt:1994:TC


Desmedt:1994:ACC


Desmedt:1995:STC


Desmedt:1996:EBB


Desmedt:1996:SPF

Yvo Desmedt. Simmons’ protocol is not free of subliminal channels. In IEEE [IEE96c], pages 170–175. CODEN PCSWEZ. ISBN 0-8186-7522-5. ISSN 1063-6900. LCCN QA 76.9 A25
REFERENCES


issue&issn=0302-9743&
volume=435. Conference
held Aug. 20–24, 1989 at
the University of California,
Santa Barbara.

Desmedt:1991:SGA

[DF91a] Yvo Desmedt and Yair
Frankel. Shared generation
of authenticators and
signatures (extended ab-
stract). In Feigenbaum
[Fei91], pages 457–469. CO-
DEN LNCSD9. ISBN 0-
388-55188-3 (New York), 3-
540-55188-3 (Berlin). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/
0558/bibs/0576/05760457.
htm; http://link.springer-
ny.com/link/service/series/
0558/papers/0576/05760457.
pdf. Conference held Aug.
11–15, 1991, at the Uni-
versity of California, Santa
Barbara.

Domingo-Ferrer:1991:DUI

[DF91b] Josep Domingo-Ferrer. Dis-
tributed user identification
by zero-knowledge access
rights proving. Information
Processing Letters, 40
(5):235–239, December 13,
1991. CODEN IFPLAT.
ISSN 0020-0190 (print),
1872-6119 (electronic).

Domingo-Ferrer:1991:SRT

[DF91c] Josep Domingo-Ferrer. Soft-
ware run-time protection: a
cryptographic issue. Lecture
Notes in Computer Science,
473:474–??, 1991. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/0473/04730474.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0473/04730474.
pdf.

Dawid:1992:BSC

[DF92] H. Dawid and G. Fet-
tweis. Bit-level systolic
carry-save array division. In
GLOBECOM ’92. Commu-
nication for Global Users.
IEEE Global Telecommu-
nications Conference. Con-
ference Record, pages 484–
488 (vol. 1). IEEE Com-
puter Society Press, 1109
Spring Street, Suite 300,
Silver Spring, MD 20910,
USA, 1992. ISBN 0-
7803-0608-2 (softbound), 0-
7803-0609-0 (casebound),
0-7803-0610-4 (microfiche).
LCCN TK5101.A1 I243
catalog no. 92CH3130-2.

Desmedt:1993:PZS

Perfect zero-knowledge shar-
ing schemes over any fi-
nite Abelian group. In
R. Capocelli, A. De Santis,
and U. Vaccaro, edi-
tors, Sequences II: Methods


REFERENCES

Dwork:1993:LCP

Ding-Feng:1999:CS

Donatini:1999:DES

Davida:1997:ACC

Davison:1957:SCG

Davison:1996:CPA

Dawson:1996:KSC
Ed (Edward) Dawson and Jovan Golic, editors. Cryptography: policy and algorithms: international con-
REFERENCES


REFERENCES


[Diffie:1977:ECN]

[DH77]

[Diffie:1990:FSEK]

[DomingoFerrer:1990:FSEK]

[DH85a]

[Davis:1985:NRI]

[DH85b]

[Davis:1985:UFS]


[DomingoFerrer:1990:FSEK]

[Dawson:1996:AAS]
Ding:1996:WKA


Dhem:1998:DEP


Diffie:1980:CAM


Dechamboux:1996:ADS


Desmedt:1998:AOC


Desmedt:1998:CC


Dolev:1995:DFT


Damm:1995:MFH

REFERENCES


Damm:1995:MH


DiGiorgio:1997:ISC


DiGiorgio:1997:JDJ


DiCrescenzo:1999:SAC


DiCrescenzo:1999:SPH


DiazeLeon:1991:PIE


Ding:1996:CRT

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

Dieringer:1988:TAE

Diffie:1982:CVP

Diffie:1982:CTF

Diffie:1988:FTY

Diffie:1990:APK


Davis:1994:CRA

Ding:1994:DCD

[102x681]REFERENCES
[102x681]322


Dixon:1994:SSS


Damm:1998:CRT


Dessmark:1993:MDD


Deavours:1985:MCM


Deavours:1989:CMH


Dusse:1991:CLM

REFERENCES


REFERENCES

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

\[\text{Dodson:1995:NFL}\]


\[\text{Diffie:1998:PLP}\]


\[\text{Demphlous:1999:DPL}\]


\[\text{Davoine:1997:VCP}\]


\[\text{DeMillo:1982:CP}\]

Richard A. DeMillo, Nancy A. Lynch, and Michael J. Mer-

Damgaard:1993:ACE


Ding:1997:LMS


DelaStelle:1902:TCF


DeMillo:1983:PDS


Duc:1997:PAF


DeWin:1998:PSS


Denning:1981:MMK

REFERENCES

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


REFERENCES


REFERENCES


DiCrescenzo:1999:COTb [DOR99]

Santis:1991:PRP [DP91]

DiCrescenzo:1994:ROP [DP94]

Damgaard:1996:NCU [DP96]

Davida:1998:HC [DP98a]

Davida:1998:HSC [DP98b]


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


Joan Daemen and Vincent Rijmen. Efficient block ci-


Dror:1989:SCG

Asael Dror. Secret codes
(any good data security system
must rely on encryption). BYTE
CODEN BYTEDJ. ISSN 0360-5280.

Droste:1996:NRV

S. Droste. New results on
visual cryptography. Lecture
Notes in Computer Science,
1109:401–??, 1996.
CODEN LNCS-D9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Dawson:1995:DIJ

S. Dawson, C. R. Ramakrishnan,
and I. V. Ramakrishnan. Design
and implementation of jump tables
for fast indexing of logic
programs. Lecture Notes
in Computer Science, 982:
CODEN LNCS-D9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Denning:1981:MKG

Dorothy E. Denning and
Fred B. Schneider. Master
keys for group sharing.
Information Processing Letters,
12(1):23–25, February
13, 1981. CODEN IFPLAT.
ISSN 0020-0190 (print),
1872-6119 (electronic). See
also note [Bv82].

Dolev:1983:AAB

D. Dolev and H. R. Strong.
Authenticated algorithms
for Byzantine agreement.
SIAM Journal on Computing,
12(4):656–666, ???.
1983. CODEN SMJCAT.
ISSN 0097-5397 (print),
1095-7111 (electronic).

Davis:1990:NSP

Don Davis and Ralph
Swick. Network security
via private-key certificates.
Operating Systems Review,
CODEN OSRED8. ISSN
0163-5980 (print), 1943-
586X (electronic).

Davis:1990:WSK

Don Davis and Ralph
Swick. Workstation services
and Kerberos authentication
at Project Athena. Report
MIT/LCS/TM 424, Laboratory
for Computer Science, Massa-
chusetts Institute of Technology,
Cambridge, MA, USA, 1990.
8 pp.

Desmedt:1993:PPS

Y. Desmedt and J. Seberry.
Practical proven secure authen-
tication with arbitration.
Lecture Notes in Computer
CODEN LNCS-D9. ISSN
0302-9743 (print),
1611-3349 (electronic).
REFERENCES


REFERENCES


[DT99] A. De Solages and J. Traoré. An efficient fair off-line electronic cash system with extensions to checks and wal-


**DiGiorgio:1998:JDS**


**DuBoulay:1999:DDT**


**duCarlet:1644:CCV**


**Dufner:1998:ACH**


**Duhoux:1990:DBA**


**Dumey:1994:CQD**

 REFERENCES

[deVivo:1998:ISA]

[DeDecker:1992:HID]

[Dhem:1996:SSC]


[DvW92]

[DvW98]
Davida:1981:DES


Dwork:1991:VSS


Dwork:1995:DCC


Dwork:1997:PAL


deWaleffe:1991:CSC


Waleffe:1991:CSC

REFERENCES


REFERENCES


REFERENCES


**Ecker:1982:MGE**


**Ecker:1983:FSR**


**Ecker:1985:STS**


**ECMA:1996:EAP**


**Ellis:1975:PKC**


**Edwards:1915:CCT**

REFERENCES

0036-8733 (print), 1946-7087 (electronic). URL

Epstein:1956:FBC
Sam Epstein and Beryl Epstein. The first book of
codes and ciphers. Franklin Watts, New York, NY,
USA, 1956. LCCN Z104 .E68. Pictures by Laszlo
Roth.

El-Gamal:1985:PCS
T. El-Gamal. A public-key cryptosystem and a signa-
ture scheme based on discrete logarithms. IEEE
Transactions on Information Theory, IT-31(4):469–
472, 1985. CODEN IET-TAW. ISSN 0018-9448
(print), 1557-9654 (electronic).

Even:1985:PCC
S. Even and O. Goldreich. On the power of cas-
cade ciphers. ACM Transactions on Computer Sys-
tems, 3(2):108–116, May 1985. CODEN AC-
SYEC. ISSN 0734-2071. URL http://www.acm.
org:80/pubs/citations/journals/tocs/1985-3-2/
p108-even/.

Even:1985:RPS
Shimon Even, Oded Goldreich, and Abraham Lem-
pel. A randomized pro-
tocol for signing contracts.
Communications of the Association for Comput-
ing Machinery, 28(6):637–
647, June 1985. CODEN
CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http://
www.acm.org/pubs/toc/
Abstracts/0001-0782/3818.
html.

Even:1990:LLD
Shimon Even, Oded Gol-
dreich, and Silvio Micali. On-
line/off-line digital signa-
tures. Lecture Notes in Computer Science, 435:
263–??, 1990. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
link/service/series/0558/
0435/papers/04350263.
pdf

Even:1996:LLD
Shimon Even, Oded Gol-
dreich, and Silvio Micali. On-
line/off-line digital signa-
tures. Journal of Cryptology,
JOCREQ. ISSN 0933-2790
(print), 1432-1378 (elec-
tronic). URL http://
link.springer.de/link/
service/journals/00145/
bibs/9n1p35.html; http:
REFERENCES

//link.springer.de/link/service/journals/00145/bibs/9n1p35.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n1p35.tex; http://link.springer.de/link/service/journals/00145/tocs/00901.html.


[EKMN84] G. Eigenthaler, H. K. Kaiser, W. B. Müller, and W. Nöbauer., editors. Contributions to gen-

Evans:1974:UAS


EFF:1998:CSE


EPIC:1999:CLI


ElGamal:1985:PKCa


ElGamal:1985:PKCb

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.

ElGamal:1985:STA


Elkins:1996:RMS


Ellis:1997:SNS


Ellison:1998:CRN


Ellis:1999:PPN


Elvin:1987:CWW


Even:1993:CCS


Eades:1998:GDC

REFERENCES


REFERENCES


**Ephron:1998:SC**


**Eisenberg:1999:PSW**


**Er:1989:NAG**


REFERENCES


[ES98]

[ESST99]

[Ev92]

[Eve85]

[Eve98]


REFERENCES


REFERENCES


[FDB93a] Y. Frankel, Y. Desmedt, and M. Burmester. Non-existence of homomorphic

Frankel:1993:NG


Feak:1983:SIS


Feistel:1973:CCP


Feigenbaum:1991:ACC


Feit:1993:TIA

ture, troubleshoot, connect via bridges and routers.

**Feit:1996:TIA**


**Feigenbaum:1998:C**


**Feige:1999:NSP**


**Feldman:1987:PSN**


**Ferris:1987:WBC**


**Ferguson:1998:UBD**


**Ferguson:1999:IDT**

REFERENCES


REFERENCES


Frederickson:1984:PRT

REFERENCES


REFERENCES


[Fis98] M. Fischlin. Cryptographic limitations on parallelizing membership and equivalence queries with applications to random self-reductions. Lecture Notes in Computer Science, 1501:
72–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Fitzgerald:1989:QIP]

[Franz:1998:MMA]

[Franz:1996:CBS]

[Federrath:1996:MMC]

[Friedman:1996:AFR]

[Freeman:1997:MCN]
Martin Freeman, Paul Jardetzky, and Harrick M. Vin, editors. *Multimedia computing and networking 1997: 10–11 February, 1997, San Jose, California*, volume 3020 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA,
REFERENCES


REFERENCES

Fried:1996:BHA

Fiadeiro:1999:ASC

Fox:1999:OCS

Flowers:1983:DC

Feiertag:1977:PMS

Flynn:1997:WYN

Friedman:1976:ZTJ
REFERENCES


Fortune:1985:PP


Feigenbaum:1991:DCC


Faihe:1998:ADR


Feustel:1998:DUI


Fairfield:1985:LRN

REFERENCES

tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=•
0&spage=203. 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.

Fagundes:1999:EGA

[FMM99] L. G. Fagundes, R. F. Mello,
and C. E. Mdron. An en-
vironment for generating
applications involving re-
 mote manipulation of paral-
lel machines. Lecture Notes
in Computer Science, 1586:
395–??, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Fairfield:1985:LDE

[FMP85] R. C. Fairfield, A. Matuse-
vich, and J. Plany. An LSI
Digital Encryption Proces-
sor (DEP). In Blakley and
Chaum [BC85], pages 115–
143. CODEN LNCSD9.
ISBN 0-387-15658-5; 3-540-
39568-7. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=•
0&spage=115. 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.

Frey:1999:TPD

Gerhard Frey, Michael
Müller, and Hans-Georg
Rück. The Tate pairing and
the discrete logarithm ap-
plied to elliptic curve cryp-
tosystems. IEEE Transac-
tions on Information The-
CODEN IETTAW. ISSN
0018-9448 (print), 1557-
9654 (electronic).

Frankel:1998:RED

[FMY98] Yair Frankel, Philip D.
MacKenzie, and Moti Yung.
Robust efficient distributed
RSA-key generation. In
ACM [ACM98b], pages
663–672. ISBN 0-89791-
962-9. LCCN QA75.5 .A14
acm.org/pubs/articles/
proceedings/stoc/276698/
p663-frankel/p663-frankel.
df; http://www.acm.
.org/pubs/citations/proceedings/
stoc/276698/p663-frankel/.
ACM order number
508980.
REFERENCES


Fujisaki:1999:SIA


Folmsbee:1999:AJT


Fujikawa:1991:EED


Fujisaki:1999:SIA


Fujisaki:1991:IBS


Fujisaki:1993:PSV


Forte:1999:BUT


Francis:1992:PSG


Franksen:1993:BCM


Franklin:1999:FCT


Freund:1994:KED


Friedman:1935:ICA


Friedman:1935:MCP


Friedman:1935:PIS

<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>AUTHOR</th>
<th>TITLE</th>
<th>PUBLICATION details</th>
</tr>
</thead>
</table>
REFERENCES

Friedman:1976:EC

Friedman:1976:EMC

Friedman:1976:ICA

Friedman:1987:ICA

Friedman:1992:MCP

Friedman:1993:TDC
Friedman:1996:SLC
Froomkin:1996:ICP


Froomkin:1997:DST


Fiat:1987:HPY


Forsyth:1993:ACS

REFERENCES


REFERENCES


[Fumy:1998:E]


[Funy:1998:ISP]


[Funy:1998:KMT]


[Feldman:1999:HSH]

Fernandez:1987:ACA


Fischer:1991:MSK


Frankel:1995:EES


Franklin:1995:BWS


Frankel:1997:CEE

REFERENCES

Frankel:1998:DPK


Frankel:1998:RMU


Frankel:1999:CRA


Frankel:1999:ASD


Gritzalis:1998:SIS


Gabriel:1982:VP1


Gaddy:1991:BOP

David W. Gaddy. Breaking into our past: Enigmas
REFERENCES


REFERENCES


REFERENCES

QC100.A1U54 no. 500-20
19.


Gaj:1989:GCM


Galland:1970:HAB


Galland:1945:HABa


Galil:1988:SIC


Galvin:1996:PKD

[Gal99] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. LMS Journal of
REFERENCES


Gamble:1988:IDL

Ganley:1993:CCI

Ganesan:1996:HUK

Ganesan:1996:YSS

Gardner:1977:MGN

Garlinski:1979:IEW
REFERENCES


[Gar97a] Lee Garber. News briefs: Agency: Net use hasn’t hurt US phone system; Apple unveils turnaround strategy; JTC rejects Java standards plan; vendors plan 300-nm wafers; battle brews over smart card encryption; countries lift Internet telephone ban; Motorola proposes satellite system; vendors agree on high-


References

Garber:1998:NBS


Garfinkel:1998:PPG


Gaudin:1997:VBJ


Gilmour-Bryson:1982:CDT

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


Gilbert:1994:CPA


Garber:1997:NBJ


Gershenfeld:1998:QCM


Girault:1988:GBA


Goffin:1997:LCP

F. Goffin, J. F. DeJaiagle, C. De Vleeschouwer, B. Macq, and J. J. Quisquater. A low cost perceptive digital picture watermarking method. In Sethi and Jain [SJ97],
Goldburg:1991:ACA


Geffe:1973:HPD

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

Gehrmann:1994:CGN


Gehrmann:1995:SMA


Gray:1998:PSC


Gemmell:1997:ITC

REFERENCES


REFERENCES

[Ger98]

[Ger99a]

[Ger99b]

[GFB93]

[GGH97a]

[GGH97b]

[GGH98]
http://csrc.nist.gov/encryption/aes/round1/conf1/aesconf.htm;
http://www.nist.gov/aes

See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen "complete and proper" candidates.

Gabber:1999:SPC

Eran Gabber, Phillip B. Gibbons, David M. Kris-

Goldreich:1985:CAR

Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the crypto-
graphic applications of random functions (extended abstract). In Blakley and Chaum [BC85], pages 276–288. CODEN LNCSD9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (elec-

OPENURL.ASP?GENRE=ARTICLE&ISSN=????&VOLUME=0&ISSUE=0&PAGE=276. CRYPTO
84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19-22, 1984, sponsored by the International Association for Cryptologic Research.

Goldreich:1986:HCR

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

Gabber:1997:HMP

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

Gilbert:1998:ASR


Gittler:1995:DSS


Gehrke:1996:MPK


Gong:1999:PKC


Gennaro:1999:SHS

REFERENCES

Gopalakrishnan:1993:NCC


Galil:1990:SPK


Gilboa:1999:CCR


Gibson:1991:EGC


Gibson:1995:SDG


Gibson:1996:SGP

REFERENCES

Gifford:1981:CSI


Gilder:1997:APD


Giles:1998:EFS


Gilboa:1999:TPR


Gingerich:1970:BRB


Girling:1987:CCL


Girault:1991:SCP


REFERENCES  

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


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


REFERENCES

3491, July 1995. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Goldreich:1996:CZP


Glenn:1998:RNE


Goldschlag:1999:BCC


Goldwasser:1999:PTU


Gennaro:1997:RBU


Gotz:1997:DTC

REFERENCES

ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic). Special issue on chaos synchronization, control, and applications.

Gligor:1979:OMA

Guillou:1982:CT

Goldreich:1989:HCP

Gaskell:1996:ISC

Gladman:1999:IEA

Gladwin:1999:CCS
REFERENCES
119–??, 1999. ISSN 0268-4527 (print), 1743-9019 (electronic).


[Robert Gallant, Robert Lambert, and Scott Vanstone. Improving the parallelized Pollard lambda search on anomalous binary curves. Mathematics of Computation, 68(??):]
REFERENCES


REFERENCES


rfc/rfc1847.txt. Status: PROPOSED STANDARD.


Goldwasser:1988:DSS

Goldwasser:1989:KCI

Good:1945:GRT
I. Jack Good, Donald Michie, and Geoffrey Timms. General report on Tunny. GC&CS report HW 25/4,
British National Archives, 1945.


[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the Association for Computing Machinery*, 38(3):691–729, July 1991. CODEN JA-COAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http:// [GN94] /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.”.


**Gray:1995:PCT**


**Guerrero:1995:CHB**


**Goldwasser:1993:ISN**


**Golic:1995:EPC**


**Goldreich:1996:SPS**


**Golic:1996:CCC**


REFERENCES


Goldwasser:1990:SPS

Gollmann:1992:ATC

Gollmann:1994:CCC

Goldreich:1995:FCF

Golic:1995:LCS

Golic:1996:FLO

Golic:1996:CEP
REFERENCES

405

(print), 1095-7146 (electronic).

Gollmann:1996:CA


Gollmann:1996:FSE


Goldreich:1997:FMCa


Goldreich:1997:FMCb


Goldwasser:1997:NDC


Golic:1997:CAA

J. D. Golic. Cryptanalysis of alleged A5 stream cipher.
REFERENCES


Goldwasser:1998:C


Golic:1998:RAS


Goldreich:1999:MCP


Golic:1999:SCE


Golomb:1999:CNS


Gong:1989:SCB


Gong:1992:SRD


Gong:1995:CKH

REFERENCES

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

**Gong:1998:JSM**


**Good:1979:EWC**


**Goodman:1996:LPS**


**Gordon:1985:SPE**


**Gordon:1993:DDT**


**Gordon:1993:DLU**

REFERENCES

Goth:1999:NBG


Guajardo:1997:EAE


Ghodosi:1999:RCN


Ghodosi:1999:RCN


Gladych:1998:CRJa


Gladych:1998:CRJb


REFERENCES

Gabiludin:1991:INR


Gleason:1985:ECP


Guillou:1995:ACE


Guillou:1998:E


Guillou:1991:PTA

REFERENCES


[Gro82] Derrick Grover. Cryptogra-
REFERENCES


Grosek:1994:RCR


Grover:1998:FCP


Goldschlag:1996:HRI


Grundler:1984:DEH


Grusho:1998:SCI


Gaines:1978:SSP


Grollmann:1984:CMP


REFERENCES

QA76.9.A25 C79 1999
Bar. URL http://link.
springer-ny.com/link/
service/series/0558/bibs/1
1666/16660372.htm; http://
link.springer-ny.com/
link/service/series/0558/
papers/1666/16660372.
pdf.

[GTG94] P. Gramata, P. Trebat-
icky, and E. Gramatova. The
MD5 message-digest
algorithm in the XILINX
FPGA. Lecture Notes
in Computer Science, 849:
126–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[GTGW94] Rick Grehan, Tom Thomp-
son, Raymond Ga Cote, and
Scott Wallace. Books and
CD-ROMs: Levels of se-
crecy: a look at cryp-
tography, Marvin Minsky on CD-
ROM, “plugs,” and visu-
alization of scientific data.
BYTE Magazine, 19(6):41–
??, June 1994. CODEN
BYTEDJ. ISSN 0360-5280
(print), 1082-7838 (elec-
tronic).

[GTG94] P. Gramata, P. Trebat-
icky, and E. Gramatova. The
MD5 message-digest
algorithm in the XILINX
FPGA. Lecture Notes
in Computer Science, 849:
126–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[GTGW94] Rick Grehan, Tom Thomp-
son, Raymond Ga Cote, and
Scott Wallace. Books and
CD-ROMs: Levels of se-
crecy: a look at cryp-
tography, Marvin Minsky on CD-
ROM, “plugs,” and visu-
alization of scientific data.
BYTE Magazine, 19(6):41–
??, June 1994. CODEN
BYTEDJ. ISSN 0360-5280
(print), 1082-7838 (elec-
tronic).

[GTG94] P. Gramata, P. Trebat-
icky, and E. Gramatova. The
MD5 message-digest
algorithm in the XILINX
FPGA. Lecture Notes
in Computer Science, 849:
126–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[GTG94] P. Gramata, P. Trebat-
icky, and E. Gramatova. The
MD5 message-digest
algorithm in the XILINX
FPGA. Lecture Notes
in Computer Science, 849:
126–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
REFERENCES

Gudes:1980:DCB


Genther:1998:E


Guergens:1998:SLF


Guillou:1997:SCR


Gullichsen:1983:BHS


Gunther:1988:ASG


Gunther:1988:ACE


Gurnsey:1997:CT


Gustafson:1996:SAS


Gutmann:1996:SDD


Guthery:1998:SC


Gutmann:1998:SGP


REFERENCES

Gylden:1931:CEI

Yves Gyldén. Chifferbyråernas insatser i världskriget till lands. (Swedish) [Cipher bureaus' operations in the World War on land]. Stockholm, Sweden, 1931.

Gylden:1933:CCB


Gylden:1936:AMC


Gylden:1938:APV

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

Gysin:1996:OKC


Garzon:1991:CGG


Haller:1994:RIA


Hendessi:1994:SAA

REFERENCES

Hollaar:1996:LRD


Heys:2000:SAC


[Hansen:1994:MLD] Per Brinch Hansen. Multiple-length division revisited:
REFERENCES


REFERENCES

[Harpes:1996:CIB]

[Harris:1996:E]

[Haskett:1984:PAU]

[Haastad:1987:OWP]

[Hastad:1988:SSM]

[Haselberger:1995:DRB]

[Hasan:1999:LTB]

[Hatefi:1996:MRE]
REFERENCES

Hatefi:1997:AED

Hawkes:1998:DWK

Hawkes:1998:DLW

Huang:1988:SWP

Hu:1995:YCE
REFERENCES

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


REFERENCES

He:1996:NKE

He:1992:IKB

Huang:1998:FAI

Hedberg:1997:FIC

Hartung:1998:DWM

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

Heidenman:1996:SIT


Heintze:1996:SDF


Hellman:1979:WTI


Hellman:1979:MPK


Hellman:1981:ACA


Held:1993:TSD


Helleseth:1994:ACE

Tor Helleseth, editor. *Advances in cryptology, EUROCRYPT ’93: Workshop on the Theory and Application of Cryptographic Techniques*, Lofthus, Norway,
REFERENCES


REFERENCES


REFERENCES


Hartung:1996:DWR

Hartung:1997:CPV

Hartung:1997:WME

Hartung:1997:DWM
REFERENCES


H. F. Hofmann and R. Hof-


Hochberger:1999:CDM


Harn:1993:OTP


Hirose:1997:CKD


Higenbottam:1973:CC


Highland:1983:BRCb


Highland:1987:CC


Highland:1987:DES


[Hig87c] Harold Joseph Highland. Encryption package. *Com-

[Hig87d] Highland:1987:HSY

[Hig87e] Highland:1987:HEM

[Hig88a] Highland:1988:PEM

[Hig88b] Highland:1988:RRC

[Hig88c] Highland:1988:TSC

[Hig88d] Highland:1988:TSV


[Hil94] Alain P. L. Hiltgen. Cryptographically relevant contributions to combinatorial

Hill:1997:MTY


Hastad:1999:PGO


Hirs:1993:BIS


Hirs:1997:MCR


Hirs:1997:FCF


Hirs:1998:FCS

REFERENCES

Hitt:1943:MSM

Helman:1999:DPE

HJH:1985:BRK

HJH:1997:PPK
A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public key and signature systems. In ???? [???97], page ??

HJH:1995:PSS
Hillerbrand:1999:SDW


Hong:1997:IAU


Huehnlein:1998:CBN


Herlea:1999:SBR


Hevia:1999:STD


Hromkovic:1994:CDC


Harpes:1995:GLC


Hachez:1999:IFA


Hall:1999:CS


Haber:1995:HDD


Hofmeister:1997:CKS

Hofmeister:1997:COS

Hall:1998:CS

He:1988:SDK

Hauser:1992:VMA

Harn:1993:SGS

Herzberg:1993:PRC

Han:1999:VFG


[Hafner:1991:COH]


[Hafner:1992:COH]


[Hafner:1995:COH]


[Hedlund:1996:CFP]

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

[Harpes:1997:PC]


[Hoogeboom:1997:CPT]


[Hoyle:1998:SKE]

REFERENCES


Horst:1995:MRM


Harkavy:1998:IPP


Harper:1993:PKC


Hennicker:1994:BAF

REFERENCES

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

Haastad:1998:SIR


Hasegawa:1998:PIE


Habutsu:1991:SKC


Hansmann:1999:SCA


Hawkes:1996:ALC


Hodges:1983:ATE


Hodges:1997:ATHa


Hoffer:1955:MAC

Carol M. Hoffer. On the mathematical approach to
REFERENCES

Hoffman:1993:CC

Hoffman:1995:BBB

Hofmeister:1999:ACA

Hogan:1988:PIS

Hollis:1987:TCA

Holloway:1991:RA

Honore:1919:STS

Hontanon:1998:EC
Ramón J. Hontañón. Encryption 101 — the choices.
REFERENCES


Hood:1980:EFS

Hoogendoorn:1982:SPK

Han:1997:ICS

Horgan:1985:TIT
J. Horgan. Thwarting the information thieves: Fear of spying through simple or sophisticated electronics has spawned an industry whose challenge is to block the illegal interception of intelligence. IEEE Spectrum, 22(7):30–41, July 1985. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Horgan:1992:CSP

Horan:1994:CSO

Horng:1995:PAU
REFERENCES


REFERENCES


Hollander:1996:KWS

[102x558]

[HRT96]

Harrison:1976:POS

[102x400]

[HRU76]

Hruby:1995:QDQ

[102x252]

[Hru95a]

Hruby:1995:QQC


Hruby:1996:SCI


Hruby:1998:TQC


Hruby:1999:SUD

Hernandez:1999:CLM


Haastad:1985:CST


Hammer:1987:EUH


Hardjono:1989:TCB


Hardjono:1990:SKS


Haber:1991:HTD


Hinsley:1993:CIS

REFERENCES


Hauser:1996:MBI


Hinsley:1979:BISSa


Heys:1995:ACS


Hada:1998:EZP


Hada:1999:RBO


Handschuh:1999:DOE


Huang:1988:APE


Huber:1991:SCC


[Hus94] Kamran Husain. Extending...


Hsu:1997:DWV


Hsu:1998:DBW


Hsu:1998:MWD


Hwang:1998:AUS


Hwang:1991:CGO


Hwang:1992:AOT


Hwang:1992:EIB

Hwang:1992:EIK


Hwang:1992:PGO


Hwang:1993:SSD


Hwang:1997:CKA


Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE


Hall:1998:BPPa

References


Hall:1998:BPPb


Hohl:1994:SIH


Harn:1993:GUS


Harn:1993:PKC


Hwang:1995:TPE


Hirose:1998:ADK


Hirose:1998:ADH

Shouichi Hirose and Susumu Yoshida. An authenticated Diffie–Hellman key


Three volumes. IEEE catalog no. 87CH2520-5.


REFERENCES


IEEE:1992:PEA


IEEE:1992:PIC


IEEE:1993:FIW


IEEE:1993:ICS


IEEE:1993:ICS

REFERENCES


IEEE:1994:PSH


IEEE:1994:TAJ


IEEE:1995:PIS


IEEE:1995:PII

IEEE:1996:ASF


IEEE:1996:IIC


IEEE:1996:PICa


IEEE:1996:SCR


IEEE:1997:SIC


IEEE:1997:ACS

IEEE:1997:JWS


IEEE:1997:ASF


IEEE:1997:ICI

IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144.


IEEE:1998:HCC


IEEE:1998:IIC


IEEE:1998:IIF


IEEE:1998:PIC


IEEE:1998:LPA


[IEEE:1999:ASF]

[IEEE:1999:SWH]

[Itoi:1998:PAM]

[Itoi:1999:PSS]

[Itoi:1999:SIK]
REFERENCES

[IHR99] Naomaru Itoi, Peter Hon-eyman, and Jim Rees. SCFS: a UNIX filesys-
tem for Smartcards. In USENIX [USE99c], page ??
URL http://www.usenix.
proceedings/smartcard99/
itoiSCFS.html.

[IKNY98] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Para-
rameters for secure elliptic curve cryptosystem —
Improvements on Schoof’s algorithm. Lecture Notes
in Computer Science, 1431: 253–??, 1998. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).

[III96] IAB and IESG. RFC 1984: IAB and IESG statement
on cryptographic technol-
ogy and the Internet, Au-
gust 1996. URL ftp://
ftp.internic.net/rfc/
rfc1984.txt; http://
www.math.utah.edu/pub/
rfc/rfc1984.txt. Status:
INFORMATIONAL.

[IKNY98] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Para-
rameters for secure elliptic curve cryptosystem —
Improvements on Schoof’s algorithm. Lecture Notes
in Computer Science, 1431: 253–??, 1998. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).

[II96] IAB and IESG. RFC 1984: IAB and IESG statement
on cryptographic technol-
ogy and the Internet, Au-
gust 1996. URL ftp://
ftp.internic.net/rfc/
rfc1984.txt; http://
www.math.utah.edu/pub/
rfc/rfc1984.txt. Status:
INFORMATIONAL.

[IIL89] R. Impagliazzo and M. Luby. One-way functions are es-
sential for complexity based
cryptography. In IEEE
[IEE89], pages 230–235.
CODEN ASFPDV. ISBN
0-8186-1982-1 (casebound),
0-8186-5982-3 (microfiche).
ISSN 0272-5428. LCCN QA
76 S979 1989. IEEE catalog
number 89CH2808-4.

[Ili94] Lucian Ilie. On a conjecture about slender context-
free languages. Theoretical
Computer Science, 132
(1–2):427–434, September
Imai:1986:AMC


Iwamura:1993:HIM


Iwamura:1993:HSI


Impagliazzo:1992:PGP


Impagliazzo:1989:ECS


Ito:1999:DPS

REFERENCES


REFERENCES

IRD:1991:DFV


Itoh:1994:LDS


Impagliazzo:1989:LPC


Ing:1999:SRT


Imai:1993:ACA


Irwin:1998:RWD

Lawrence W. Irwin. The robustness of watermarking in digital images. Thesis (Ph. D.), University of New Mex-
Ingemarsson:1991:PSS

Ikram:1997:CSE

Ikram:1999:UIN

Ito:1987:SSS

ISO:1997:ITS

Isselhorst:1990:UFP
Itoh:1991:CFI


Iversen:1991:CSC


Ingemarsson:1981:UAS


Imai:1998:PKC


Imai:1999:PKC


Jaburek:1990:GGP

W. J. Jaburek. A general-

Jackson:1987:NTS


Jackson:1990:SITa


Jackson:1990:SITb


Jackson:1996:AAC


Jakobsson:1995:BUU


Jakobsen:1998:CBC


Jakobsen:1999:HOC

Thomas Jakobsen. Higher-order cryptanalysis of block

Jakobsson:1999:MCM


Jakobsson:1999:QCA


Jakobsson:1999:QCA

Jamieson:1998:UEP


Jamieson:1998:UEP


Janek:1999:AVR


Janecek:1999:AVR


Jarecki:1996:PSS


Jarvis:1997:GB

Barry Jaspan. Dual-workfactor encrypted key exchange: Efficiently preventing password chaining and dictionary attacks. In
REFERENCES


Jaeger:1993:LCC


Jan:1998:PWP


Johnson:1991:TSS


Johnson:1991:CCA


Jeffery:1986:GCC


Jensen:1999:GDT


Jenkins:19xx:IFC

is based on cryptographic principles, and generates 32-bit random numbers. ISAAC-64 is similar, but requires 64-bit arithmetic, and generates 64-bit results.

Jevons:1874:PS


Joyce:1990:IAB


Joux:1995:PAA


Jian:1999:SDM


Jolitz:1995:RNS


Johnson:1998:ESS


Johnson:1998:CPE

Neil F. Johnson and Sushil Jajodia. Computing practices: Exploring steganography: Seeing the un-
REFERENCES


REFERENCES

Jones:1975:ESP


Johnson:1994:HKD


Juels:1997:SBD


Janwa:1996:MPK


Johnson:1996:AEE


Jurgensen:1984:SR1


Jackson:1993:CAG


Janwa:1996:MPK

[JM97] Aleksandar Jurisic and Alfred J. Menezes. Ellip-

**Jakobsson:1999:IMI**


**Johnson:1994:CDM**


**Jackson:1995:ESS**


**Jackson:1995:SMS**


**Jerichow:1998:RTM**

REFERENCES

Jakobsson:1996:DVP


Jarecki:1997:EMS


Joesang:1998:SMA


Johnson:1989:BDC


Johnson:1990:EDE


Johansson:1994:CPA

REFERENCES

Johnson:1995:ACD

Johnson:1996:LP

Johnson:1997:SP

JohnByrne:1998:CEC

Johnson:1999:LES
REFERENCES


Jolitz:1995:PB


Jones:1990:PKC


Josse:1885:CSA


JCryptology:1988:JCJ


Juels:1996:HCC

Jaeger:1999:FCD


Joye:1997:PFR


Joye:1998:CRT


Joye:1998:REC


Joye:1997:RTS


Jurgensen:1996:TFC


Jones:1993:DAC

Joux:1993:CAK


Johansson:1995:AIA


Johansson:1995:CIA


Jiwa:1994:BBA


Jan:1996:SIE


Jan:1997:SEV

REFERENCES

0164-1212 (print), 1873-1228 (electronic).


REFERENCES

[Jutla:1998:GBA]

[Just:1996:AMP]

[Jakubowski:1998:CSP]

[Jeannerod:1998:GEE]

[Ji:2001:CAF]

[Jakobsson:1996:OAB]
REFERENCES

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


Kompella:1991:FCC


Kent:1998:RIA


Koutsoukos:1999:HCS


Kahn:1963:PNU


Kahn:1966:MC

David Kahn. Modern cryptology. Scientific American,
REFERENCES


REFERENCES

Kahn:1991:WWW


Kahn:1996:HS


Kahn:1996:CSS


Kahn:1998:EC


Kahn:1998:PHI


Kahn:1998:RMU


Kak:1983:EMP


Kak:1984:MPK

[Kak84] S. C. Kak. On the method of puzzles for key distribu-

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

REFERENCES

Kaliski:1992:MAC


Kaliski:1993:SES


Kaliski:1993:ZBA


Kaliski:1995:MIA


Kaliski:1997:IPS


Kaliski:1997:PNG


Kaliski:1997:ACC

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


Kaliski:1998:EDF


Kaliski:1999:ESP

Burton S. Kaliski, Jr. Emerging standards for public-key cryptography.
Kaneshige:1996:ITC


Kaps:1998:HSF


Karger:1985:ADA


Karger:1986:ADA


Karger:1987:LDP


Kari:1989:CBP


Kari:1989:OCP

Jarkko Kari. Observations concerning a public-key

**Karkare:1996:SEA**


**Kasiski:1863:GDG**

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

**Kastenholz:1996:RVP**


**Kalipha:1990:NPK**


**Katzan:1977:SDE**


**Katsikas:1997:CMS**

Kaufman:1993:RDD


Kaufman:1996:DWC


Kawai:1987:LAI


Kay:1995:CTE


Krishnakumar:1992:HTE


Krawczyk:1996:HKM


Krawczyk:1997:RHK


Klein:1989:STR


REFERENCES

Emilie Fennek, 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


[KG95] Andrew Klapper and Mark Goresky. Cryptanalysis based on 2-adic rational ap-

Katsikas:1996:ISS


Kravitz:1999:CAC


Kundur:1997:RDI


Kundur:1998:DWU


Kunkelmann:1998:VEB


Kharitonov:1993:CHD

Karaorman:1999:CRJ


Kobara:1996:LVS


Kobara:1997:SSM


Katsumoto:1999:DPL


Kiefer:1998:WMV


Kilian:1988:FCO


Kim:1993:CLB

Kwango Kim. Construction of DES-Like S-boxes based on Boolean functions satisfying the SAC. Lecture Notes in Computer Science, 739:59–??, 1993. CODEN

...
REFERENCES

Kippenhahn:1997:VBG


Kippenhahn:1999:CBH


Kippenhahn:1999:VBG

Kak:1977:SEU


Kocher:1999:DPA


Kurosawa:1995:NBA


Kuwakado:1996:NRT

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

Kirby:1995:RPK

REFERENCES


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).


Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata,

Kabatianskii:1997:DSS


Kramer: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

Klein:1990:FCS


Kannan:1988:PFN


Klupsch:1999:ARR


Kurosawa:1988:CSP


Kurak:1992:CNI


IEEE Computer Society Press order number 3115. IEEE catalog number 92TH04070-5.

Kang:1993:PRR


Kim:1996:ACA

Kwangjo Kim and Tsu-
tomu Matsumoto, editors. Advances in cryptology—
ASIACRYPT ’96: International Conference on the
Theory and Applications of Cryptology and Informa-
tion Security, Kyongju, Korea, November 3–7, 1996: pro-
ceedings, volume 1163 of Lecture Notes in Computer
Science. Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, UK / etc., 1996. CODEN
0302-9743 (print), 1611-3349 (electronic). LCCN
QA76.9.A2515553 1996. [KM96b]

Knudsen:1996:IDA

L. Knudsen and W. Meier. Improved differential at-
CODEN LNCSD9. ISBN 3-540-61512-1. ISSN 0302-
9743 (print), 1611-3349 (electronic). LCCN
QA76.9.A2515553 1996. [KM98b]

Kosuda:1997:SED

Koji Kosuda and Tsutomu
Matsumoto. A strength
evaluation of the Data En-
ryption Standard. IMES
discussion paper 97-E-5, In-
stitute for Monetary and
Economic Studies, Bank of
Japan, Tokyo, Japan, 1997.
128 pp. [KM97]

Kaksonen:1998:OMC

R. Kaksonen and P. Maeho-
enen. Object modeling of
cryptographic algorithms
with UML 193. Lecture
Notes in Computer Science,
1438:193–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). [KM98a]

Kaufman:1998:DWF

C. W. Kaufman and S. M.
Matyas. Differential work
factor cryptography method
and system. US Patent

Knudsen:1998:SMD

Lars R. Knudsen and Keith M. Martin. In search
of multiple domain key re-
covery. Journal of Com-
puter Security, 6(4):219–
235, ????. 1998. CODEN
JCSIET. ISSN 0926-227X
REFERENCES

Kasahara:1999:NPK
Masao Kasahara and Yasuyuki Murakami. New
cryptosystems

[KM99a] based on arithmetic in integer ring.

Mem. Fac. Engrg.

Design Kyoto Inst. Tech.


(2000), 1999. ISSN 0911-

0305.

Knudsen:1999:CIS
L. R. Knudsen and W. Meier.
Cryptanalysis of an identification scheme based on the
permuted perceptron problem. Lecture Notes in Com-
ISSN 0302-9743 (print), 1611-3349 (electronic).

Kohlas:1999:RAP
Reto Kohlas and Ueli Maurer.
Reasoning about
public-key certification: On bindings between entities
and public keys. In Franklin [Fra99], pages 86–103.

[KMK99] ISBN 3-540-66362-2 (soft-
springer-ny.com/link/
service/series/0558/bibs/1648/16480086.htm;

http://link.springer-ny.com/
link/service/series/0558/papers/1648/16480086.
pdf.

Koscielny:1999:QBP
Czesław Kościelny and
Gary L. Mullen. A
quasigroup-based public-
key cryptosystem.

Int. J.

9(4):955–963, 1999. ISSN
1641-876X.

Kanda:1998:ECC
Masayuki Kanda, Shiho
Moriai, Kazumaro Aoki, Hi-
roki Ueda, Miyako Ohkubo,
Youichi Takashima, Kazuo
Ohta, and Tsutomu Mat-
sumoto. E2 — a can-
didate cipher for AES.

In National Institute of
Standards and Technology
[Nat98], page 89. ISBN
???? LCCN ???? URL
http://csrc.nist.gov/
encryption/aes/round1/
conf1/e2-slides.pdf. Only
the slides for the conference
talk are available.

Kobayashi:1999:FEC
T. Kobayashi, H. Morita,
K. Kobayashi, and F. Hoshino.
Fast elliptic curve algo-

rithm combining Frobenius
map and table reference
to adapt to higher char-
acteristic. Lecture Notes in
Computer Science, 1592:
176–??, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Konheim:1980:ICP
Alan G. Konheim, Mar-
ian H. Mack, Robert K. McNeill, Bryant Tucker-
man, and Gerald Wald-
baum. The IPS crypto-
graphic programs. IBM
Systems Journal, 19(2):
253–283, 1980. CODEN
IBMSA7. ISSN 0018-8670.

[KMOV91] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto,
and Scott A. Vanstone. New
public-key schemes based
on elliptic curves over the
ring $\mathbb{Z}_n$. Lecture Notes
in Computer Science, 576:
252–266, 1991. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
l ink/service/series/0558/
bibs/0576/05760252.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0576/05760252.
pdf.

[KMPS99] M. Mancona Kande, S. Maza-
her, O. Prnjat, and L. Sacks.
Applying UML to design an
inter-domain service man-
gement application. Lecture
Notes in Computer Science,
1618:200–?, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[KMS95a] P. Karn, P. Metzger, and
W. Simpson. RFC 1829:
The ESP DES-CBC trans-
form, August 1995. URL
ftp://ftp.internic.net/
rfc/rfc1829.txt; http://
www.math.utah.edu/pub/
rfc/rfc1829.txt. Status:
PROPOSED STANDARD.

[KMS95b] P. Karn, P. Metzger,
and W. Simpson. RFC
1851: The ESP triple
DES transform, September
1995. URL ftp://
/ftp.internic.net/rfc/
rfc1851.txt; http://
www.math.utah.edu/pub/
rfc/rfc1851.txt. Status:
EXPERIMENTAL.

RFC 1510: The Ker-
beros Network Authentica-
tion Service (V5), September
1993. URL ftp://
/ftp.internic.net/rfc/
rfc1510.txt; http://
www.math.utah.edu/pub/
rfc/rfc1510.txt. Status:
PROPOSED STANDARD.

[Kno79] H. D. Knoble. Algorithm
536: An efficient one-
way enciphering algorithm
[Z]. ACM Transactions on
Mathematical Software, 5
CODEN ACMSCU. ISSN
0098-3500 (print), 1557-
7295 (electronic).
REFERENCES

Kohl:1994:EKA


Knuth:1969:SNM


Knuth:1969:SA


Knuth:1973:FA


Knuth:1980:DLC


Knuth:1985:DLC


Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb

[L. R. Knudsen. Cryptanalysis of LOKI91. Lecture
Knudsen:1993:ICS


Knudsen:1993:CLc


Knudsen:1993:CLa


Knudsen:1994:PSF


Knudsen:1994:BCA


Knudsen:1995:NPW


Knudsen:1998:BCS

Knudsen:1998:DBC


Knudsen:1999:STA


Knudsen:1999:CBC


Knudsen:1999:FSE


Knurosa:1995:CIS


Knurosa:1995:CBA


Knurosa:1996:CLB


Knurosa:1997:CLB

1997. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Koblitz:1987:CNT


Koblitz:1987:ECC


Koblitz:1990:FJS


Koblitz:1991:CCG


Koblitz:1991:CEC


Koblitz:1991:JSI


Koblitz:1994:CNT


Koblitz:1996:ACC

[Kob96] Neal Koblitz, editor. Advances in cryptology, CRYPTO
REFERENCES


Kobayashi:1997:DWH


Koblitz:1998:C


Koblitz:1998:AAC


Koblitz:1998:ECI

Kobara:1999:PMA


Kochanski:1989:HSI


Koc:1994:HSR


Kocher:1995:CDR


Koc:1996:RHI


Kocher:1996:TAI

Paul C. Kocher. Timing attacks on implementations of
REFERENCES


Kocher:1999:B

Koeune:1999:CRI
http://www.nist.gov/aes. No slides for the conference talk are available.

Kohl:1990:UEK

Kolata:1977:NCC

Koland:1995:SSH

Konheim:1981:CP
REFERENCES

A Wiley-interscience publication.

Konheim:1985:CAE


Konheim:1989:RMC


Kong:1995:DES


Koopman:1986:OES


Kurosawa:1995:TIK

Kurosawa:1995:CIT

[102x681]REFERENCES

[102x681]


Koops:1997:CRE


Kopooshian:1997:DCE


Kornerup:1993:HRM


Korner:1996:PC


Koscielny:1983:PRD

[Czeslaw Koscielny. Programowa realizacja działan w ciałach skonczonych do zastosowanych w technice kodowania korekcyjnego i kryptografii, volume 61. 11 of Prace naukowe Instytutu Cybernetyki Tech-
Kurosawa:1994:NSS


Koshiba:1997:UPN


Kothari:1985:GLT

REFERENCES

Kurosawa:1995:LEAa

[KOT95a]

Kurosawa:1995:LEAb

[KOT95b]

Koyama:1982:CUM

[Koy82a]

Koyama:1982:MKR

[Koy82b]

Koyama:1983:MKR

[Koy83]

Koyama:1995:FRT

[Koy95]

Kozaczuk:1984:EHGa

[Koz84a]

Kozaczuk:1984:EHGb

[Koz84b]
Władysław Kozaczuk. Enigma: How the German Machine
REFERENCES


Kozen:1996:RSS


Kim:1989:PRP


Kwan:1993:GPT


Krajíček:1995:SCC


Knudsen:1996:HFB


Knudsen:1996:DSK

REFERENCES

Knudsen:1997:FSH

Kilian:1998:IE

Kaps:1999:FIF

Koc:1999:CHE

Kipnis:1999:UOV

Karhumaeki:1999:CSI
J. Karhumaeki, W. Plandowski, and W. Rytter. The com-


cryptobytes/crypto1n3.pdf.

Kaliski:1996:MEW

Kilian:1996:HPA

Knudsen:1996:DFC

Knudsen:1996:NAL

Kankanhalli:1998:CBW

Knudsen:1999:DLC

Knoliopoulos:1999:NLT
Krause:1984:DEI

Kranakis:1986:PC

Krawczyk:1990:HPC

Krawczyk:1994:SSM

Krawczyk:1994:LBH

Kravitz:1993:DSA
REFERENCES


[KRS99] R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklist-

Kruh:1998:WWS


Knudsen:1999:TDS


Kordes:1989:UMC


Kelsey:1997:CPO


Kurosawa:1997:DSP


Kwon:1997:SEA

Committee on Computer Communications [IEE97],
(casebound), 0-8186-8143-8 (microfiche). ISSN 0742-
1303. LCCN TK5105.5.C82
1997. IEEE Computer Society Press order number
PR08141. IEEE Order Plan number 97TB100179.

Kaliski:1998:RPRb

B. Kaliski and J. Staddon. RFC 2437: PKCS 
#1: RSA cryptography
specifications version 2.0,
October 1998. URL
ftp://ftp.internic.net/
rfc/rfc2313.txt; ftp://ftp.internic.net/rfc/
rfc2437.txt; http://
www.math.utah.edu/pub/
rfc/rfc2313.txt; http://
www.math.utah.edu/pub/
rfc/rfc2437.txt. Ob-
soletes RFC2313 [Kal98b].
Status: INFORMATIONAL.

Kelsey:1998:SPP

J. Kelsey and B. Schneier.
The street performer pro-
tocol. Technical report,
Counterpane Systems, 101
East Minnehaha Parkway,
Minneapolis, MN 55419,
November 1998. URL
http://www.counterpane.
com/street_performer.
html. Also published in The
Third USENIX Workshop
on Electronic Commerce
Proceedings, USENIX Press,
November 1998.

Kinoshita:1998:GST

H. Kinoshita and M. Satoh. Generation of the signature with the structured information of the image. In Theodoridis et al.
960-7620-06-2 (v. 1), 960-
7620-07-0 (v. 2). LCCN
TK5102.9.E97 1998. URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/bibliography/073141.html
Four volumes.

Kipnis:1998:COV

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

Kelsey:1999:AST

John Kelsey and Bruce
Schneier. Authenticating
secure tokens using slow
memory access. Technical
report, Counterpane Sys-
tems, 101 East Minnehaha
Parkway, Minneapolis, MN
55419, 1999. URL http://
www.counterpane.com/
slow-memory.html. First
USENIX Symposium on Smart Cards, USENIX
REFERENCES


REFERENCES


Kelsey:1997:SAL

REFERENCES

(ISW’97), September 1997, pp. 121–134 [KSHW98].

Kelsey:1998:SAL


Kim:1996:EIE


Kehne:1992:NBP


Knowles:1992:AFC


Kelsey:1996:KC1


Kelsey:1997:RCB


Kelsey:1997:RKC

[KSW97b] J. Kelsey, B. Schneier, and D. Wagner. Related-key

**Kelsey:1998:PICa**


**Kelsey:1998:PICb**


**Kelsey:1999:KSWa**


**Kelsey:1999:MCAa**


**Kelsey:1999:MCAb**

REFERENCES

Kelsey:1998:SCCa


Kelsey:1998:SCCb


Kelsey:1998:SCCc


Koyama:1991:NPC

Koyama:1993:SEC


Keefe:1996:MTS

IEEE Computer Society Press Order Number PR07629
IEEE Order Plan Catalog Number 96TB100076.

Koyama:1998:AFC


Kim:1999:AFC

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

Kanda:1999:SCF


Kuchlin:1987:PKE

Kucera:1992:GES


Kuhn:1998:CIS


Kuijk:1991:RSE


Kukorelly:1999:VCH


Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC

REFERENCES


**Kumar:1997:CSI**


**Kummert:1998:RPT**


**Kuo:1990:TEC**


**Kurosawa:1994:NBA**


**Kearns:1989:CLL**


**Kearns:1994:CLL**


REFERENCES

Kaliski:1997:SRE


Kaliski:1998:SRE


Kaliski:19xx:DLC

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

Kwok-Yan:1992:TAD


Kurosawa:1998:SBC


Kwok-Yan:1992:FAA


Kasami:1982:KMS

Tadao Kasami, Saburo Yamamura, and Kenichi Mori. A key management scheme for end-to-end encryption
and a formal verification of its security. *Systems-
DEN SYCCBB. ISSN 0096-8765.

**Koch:1995:TRH**

.uk/~fapp2/steganography/bibliography/1005.html. Two volumes.

**Levien:1998:ART**

.org/publications/library/proceedings/sec98/levien.html.

**Lampson:1991:ADS**


**Lacy:1993:CCS**


**Laffin:1964:CCS**


**Lagarias:1984:KPK**

J. C. Lagarias. Knapsack public key cryptosyst-


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


http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1014.html. [Lan81]

Lamport:1981:TNP


Lambert:1999:DSV


Landers:1946:RPR


Langie:1981:CSS


Landau:1989:SSC


Langford:1995:DCT


Langford:1996:WST

Lange:1997:SCI


Landrock:1998:TOC


Landrock:1999:PTU


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

Landwehr:1994:TCP

Low:1994:SAP

Lomas:1995:RBH

Lee:1996:IAP
Wei-Bin Lee and Chin-Chen Chang. Integrating authentication in public key distribution system. Information Processing Letters, 57(1):


REFERENCES


Leighton:1979:BRB


Leiserson:1999:ITD


Lempel:1979:CT


Lennon:1978:CAI


Lenstra:1987:FIE

REFERENCES

**Lenstra:1990:PT**


**Lenstra:1998:GRM**


**Lenstra:1999:EIB**


**Lenzerini:1999:DLT**


**Lercier:1997:FGR**

REFERENCES

**Levine:1958:VMS**


**Levine:1961:SAH**


**Levine:1961:SECa**


**Levine:1961:SECb**


**Levine:1983:USC**


**Levin:1985:OWF**


**Levine:1991:USC**


**Lewin:1978:UGW**

Lewin:1982:AMC


Lewis:1992:SCP


Laurin:1997:SSM

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

Lopes:1999:UES


Lorigo:1999:CDG


Li:1994:RMC


Laih:1997:CDE


Laih:1993:GTC


**Landwehr:1984:SMM**


**Lee:1998:ZNP**


**Lee:1999:STI**


**Lichtenthal:1994:CBT**


**Lidl:1985:CBP**


**Lidl:1990:SMA**

University in Sydney from 29 June to 7 July 1989.

**Lieberherr:1981:UCD**


**Liebl:1993:ADS**


**Lim:1998:CNB**


**Lim:1999:RVC**


**Linn:1988:RPE**

REFERENCES

Obsoletes RFC0989 [?]. Status: UNKNOWN.

[RFC1040]


[Linn:1989:RPE]


[Linn:1993:RPE]

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


REFERENCES

Lipton:1994:CNF


Abeles:1998:KVC


Lipmaa:1999:ICM


Litant:1987:BRC


Lindsay:1997:BC

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

Laïh:1996:CEE

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


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

Lim:1998:SPK


Lin:1998:CDE


Lee:1999:NAD


Luo:2010:PAE


Laih:1989:NTS

REFERENCES


REFERENCES

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


Leighton:1994:SKA


Leighton:1995:LPF


Low:1996:MCP


Lamersdorf:1998:TDS


Low:1998:PCT


Low:1995:DMI


REFERENCES


REFERENCES

LaMacchia:1991:SLS


Lomet:1983:HPU


Lomas:1994:ENT


Lomas:1997:SPI


Long:1991:PAA


Long:1992:UDE

[Lon92] Yong Hong Long. Using Diophantine equations to

**Loshin:1997:CGP**

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

**Loshin:1998:PEC**


**Lowe:1995:ANS**


**Lowe:1996:BFN**


**Loxton:1990:NTC**


**Lam:1999:ACA**

REFERENCES


REFERENCES

//link.springer-ny.com/  
link/service/series/0558/  
bibs/1525/15250158.htm;  
http://link.springer-ny.com/link/service/series/  
0558/papers/1525/15250158.pdf.

Luby:1986:PRP  
Pseudo-random permutation generators and cryptographic composition. In  
1986. URL http://www.acm.org/pubs/articles/  
proceedings/stoc/12130/  
p356-luby/p356-luby.pdf;  
http://www.acm.org/pubs/citations/proceedings/  
stoc/12130/p356-luby/.  
ACM order number 508860.

Lagarias:1988:UEP  
Unique extrapolation of polynomial recurrences. SIAM Journal  
(print), 1095-7111 (electronic). Special issue on cryptography.

Luby:1988:HCP  
[LR88b] Michael Luby and Charles  
Rackoff. How to construct pseudorandom permutations from pseudorandom  
functions. SIAM Journal on Computing, 17(2):  

Lai:1996:AHH  
Attacks on the HKM/  
HFX cryptosystem. Lecture Notes in Computer Science,  
1039:1–??, 1996. CODEN LNCSD9. ISSN 0302-9743  
(print), 1611-3349 (electronic).

Lysyanskaya:1998:GBD  
Group blind digital signatures: a scalable solution to electronic cash. Lecture Notes in Computer Science,  
1465:184–??, 1998. CODEN LNCSD9. ISSN 0302-9743  
(print), 1611-3349 (electronic).

Lai:1993:FCC  
[LRW93] X. Lai, R. A. Rueppel, and  
J. Woolfven. A fast cryptographic checksum algorithm based on stream ciphers. Lecture Notes in Computer Science,  

Lange:1925:TC  
[LS25] André Lange and E. A.  
Soudart. Traité de cryptographie. (French) [Treatise on cryptography]. Li-
 REFERENCES


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

Luby:1998:CBB


Lamport:1982:BGP

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

Livens:1995:CCI


Leung:1985:SCT

Leong:1991:UPE


Linnartz:1998:MPM


Langley:1999:ACI


Laih:1995:SLF


Lioen:1988:OMA


Lioen:1988:OMF


Lu:1979:EGC


Lu:1980:AEG

REFERENCES


REFERENCES


LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). [LZ91b]

Lodge:1994:SCC


Laih:1993:TES

Chi-Sung Laih, Sung-Ming Yen, and Lein Harn. Two efficient server-aided secret computation protocols based on the addition sequence. Lecture Notes in Computer Science, 739:450–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Li:1990:ACP


Li:1991:HBM


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN


MacLaren:1994:CPN

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


REFERENCES


REFERENCES

ny.com/link/service/series/0558/papers/1525/15250290.pdf.

Maher:1996:CBK


McDonald:1995:OTP


Manasse:1995:MPE


Manjunath:1998:IPA


Moriai:1996:KLP


Mao:1997:PVP

(print), 1611-3349 (electronic).

**Mao:1998:GCS**


**Mar:1970:CSS**


**Mar:1970:MEC**


**Mar:1976:ANE**


**Mar:1995:WGT**


**Mar:1995:PEI**


**Mar:1996:MSI**


**Mar:1997:IEI**

REFERENCES

Markantonakis:1998:CSM

Marks:1998:BSC

Martyna:1999:NNA

Massey:1983:LFC

Mastrovito:1989:VDM

Mastrovito:1991:VAC

Massey:1994:SKB
REFERENCES

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


Matsumoto:1998:HCC

Matsumura:1999:DTE


Mauborgne:1914:APC


Maurer:1990:FGS


Maurer:1991:NAD


Maurer:1991:DSS


Maurer:1991:PCS


Maurer:1991:PSS

REFERENCES


Maurer:1993:PSK


Maurer:1993:RIT


Maurer:1994:TEB


Maurer:1996:UGT


Maurer:1996:ACE

REFERENCES

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

Maurer:1997:ITS


Maurer:1998:E


Maurer:1999:IC


Maurer:1999:ITC


Maxemchuk:1994:EDD

N. F. Maxemchuk. Electronic document distribu-
REFERENCES

May:1997:CDS

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

Mao:1994:SAP

Massey:1994:CCT

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


Mintzer:1998:OWS


Moskowitz:1992:CAA


Mitchell:1996:CKU

REFERENCES

**McCarty:1975:AFP**

John McCarthy. ACM Fo-

**McC90a**

Kevin S. McCurley. The
discrete logarithm problem.
In Pomerance and Gold-
wasser [PG90], pages 49–
ISSN 0160-7634. LCCN
QA76.9.A25 C84 1990;
QA1 .A56 v.42 1990. Le-
cure notes prepared for the
American Mathematical So-
ciety short course, Cryp-
tology and computational
number theory, held in
Boulder, Colorado, August

**McC96**

K. S. McCurley. Cy-

**McC90b**

Kevin S. McCurley. Odds
and ends from cryptology
and computational number
theory. In Pomerance and
Goldwasser [PG90], pages
145–166. ISBN 0-8218-
0155-4. ISSN 0160-7634.
LCCN QA76.9.A25 C84
Lecture notes prepared for
the American Mathematical
Society short course, Crypto-
tology and computational
number theory, held in
Boulder, Colorado, August

**McC90c**

W. Millan, A. Clark, and
E. Dawson. Heuristic de-
sign of cryptographically
strong balanced Boolean
functions. *Lecture Notes in
Computer Science*, 1403:
489–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Millan:1999:BFD**

W. Millan, A. Clark, and
E. Dawson. Boolean func-
tion design using hill climb-

**Millan:1998:HDC**

W. Millan, A. Clark, and
E. Dawson. Heuristic design
of cryptographically strong
balanced Boolean functions. *Lecture Notes in
Computer Science*, 1403:
489–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Millan:1999:BFD**

W. Millan, A. Clark, and
E. Dawson. Heuristic de-
sign of cryptographically
strong balanced Boolean
functions. *Lecture Notes in
Computer Science*, 1403:
489–??, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
integer factoring algorithm that never requires arithmetic on numbers larger than the one to be factored.


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

Moreno-Diaz:1994:SIE


Messerges:1999:IPA


Meade:1920:KCE


Meadows:1995:FVC


Mead:1998:BJA


Meek:1998:AAM


Meersman:1999:SOT

REFERENCES

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


[Mei83] Henk Meijer. Cryptology computational complexity and applications. Thesis (Ph.D.), Queen’s University, Ottawa, ON, Canada, 1983. 2 microfiches (179 fr.).


[Mei98] Carolyn P. Meinel. How hackers break in ... and how they are caught: Port scanners, core dumps and buffer overflows are but a few of the many weapons in every sophisticated hacker’s arsenal. still, no hacker is invincible. Scientific Amer-

Mendelsohn:1939:CC

Mendelsohn:1989:CWI

Mendez:1991:AKA

Menezes:1993:ECP

Menezes:1995:ECC

Menicocci:1995:SAC

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

Merkle:1978:SCI


Merkle:1980:PPK


Merkle:1982:PPK


Merkle:1982:SAP

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

**Merkle:1988:DSB**


**Merkle:1989:CDS**


**Merkle:1990:OWH**


**Merkle:1991:FSE**

REFERENCES


REFERENCES

...ing the keys to Java security: the sandbox and authentication. *JavaWorld: IDG’s magazine for the Java community*, 2(5):??, May 1997. CODEN ????


**Murino:1995:RNU**


**Mihaljevic:1991:CCP**


**Madson:1998:RUHa**


**Merkle:1978:HIS**

Merkle:1981:SME


Michels:1996:RDS


McPherson:1998:CRH


Majzik:1996:MCU


Matsumoto:1988:PQP


Matsumoto:1990:EAC

Moulin:1999:ECG


Micciancio:1997:ODS


Micaeli:1993:FPC


Micaeli:1993:FPK


Micaeli:1993:FPC

Mihaljevic:1996:FCS


Millikin:1943:ECCa


Millikin:1943:ECCb


Millikin:1943:ECCc


Millen:1987:CCC


Millen:1987:CCC


Millen:1987:CCC

REFERENCES

Mills:1987:RDP


Millikin:1992:ECC


Mintzer:1997:EIDa


Misarsky:1997:MAU

Jean-François Misarsky. A multiplicative attack us-

### Misarsky:1998:HDR


### Mitchell:1976:EAD


### Mitchell:1989:MDS


### Mitchell:1992:AMI


### Mitchell:1992:CCI

Chris Mitchell. *Cryptography and coding II*. The In-

Miyaguchi:1990:FCC


Miyaguchi:1991:FCF


Miyaji:1993:ECS


Miyagi:1999:ECC

crete integrable systems (Kyoto, 1998).

**Mjolsnes:1993:PCP**

[102x598]


**Mori2:1992:PSP**

[102x598]


**Moskowitz:1994:CCH**

[102x598]


**Mazieres:1999:SKM**

[102x598]


**Maibaum:1999:SRS**

[102x598]


**Miyazaki:1999:TFI**

[102x598]

REFERENCES


REFERENCES

Meadows:1987:MSA

Magliveras:1990:LCP

Magliveras:1990:PCP

Moskowitz:1992:ICI

Moskowitz:1992:IDI

Moskowitz:1994:STC
Moldovyan:1995:FSE


Meadows:1996:CCC


Meyer:1996:PKC


Muller:1998:SPK


Marchignoli:1999:AVC


Meddes:1999:ABV

[MM99b] J. Meddes and E. McKenzie. An agent-based visuali-
REFERENCES


Moulin:1999:ITA


Mock:1997:BDS


Mohtashemi:1992:CHC


Matsumoto:1982:DTL


Mok:1997:KNF


Moldovyan:1998:NEP


Morita:1991:SCT

REFERENCES

Montgomery:1985:MMT

CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL

Monagan:1993:GPD

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

Montagu:1996:MWN


Moore:1992:PFC


Morland:1666:NMC


Morrice:1692:EB


Morrison:1983:SEA

REFERENCES

Morain:1988:IGP


Mora:1989:AAA


Morris:1992:FMC


Morgan:1997:PAM


MorenoDiaz:1998:NCC


Moskowitz:1998:C

Mosses:1999:CGT


Moura:1999:PAP


Mullin:1988:ONB


Moynihan:1998:SAE


Mevis:1986:SCP


McInnes:1991:IPK


Milidiu:1999:EIW


Mayerwieser:1995:THS

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


[MR98] Jeanette McLeod and Greg
REFERENCES


Mrakovcic:1995:EIN


Micali:1987:NSP


Micali:1988:NSP


Maitra:1999:COA


Mitchell:1989:RHF


Macalister:1976:SLI

REFERENCES


McEliece:1981:SSR


Muller-Schloer:1983:MBC


Moore:1987:CSK


Meier:1990:NCC


Montgomery:1990:FEP


Meier:1991:CPC


REFERENCES


[MSN99] Takaaki Mizuki, Hiroki Shizuya, and Takao Nishizeki. Dealing necessary and sufficient numbers of cards...

Martin:1999:BTE


Mambo:1996:HUT


Madonia:1993:GSP


Michels:1998:SSV


Mullender:1986:DCD

REFERENCES

Matsui:1994:VSH

Massey:1995:MCM

Molva:1998:SSA

Matsui:1999:CRV

Melkonian:1999:AAD
Mister:1999:CRL


Marayati:1987:AWA


Moggi:1999:IMS


Mackinnon:1985:OAA


Moriya:1997:DWS


Molva:1992:KAK


Mu:1992:ICS

Hao Mu. ID-based cryptographic schemes for user identification, key distri-
REFERENCES


Mueller:1999:SRB


Muftic:1988:SMC


Muftic:1993:SAO


Mulherin:1981:FDE


Mullin:1984:NMP


Mulligan:1989:UMA


Mullin:1989:LEN


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

Muller:1999:SRB


Mund:1991:ZCP


Mund:1991:ZLC


Muraszko:1987:CVR


Murphy:1996:CC


Murphy:1999:OST

Musser:1992:UVE


Maruyama:1998:TGH


Menezes:1990:IEC


Menezes:1991:ACC


Meijers:1993:EMV


Menezes:1998:C


Mu:1999:DD


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


Maurer:1993:RNI

REFERENCES


REFERENCES


Mihaljevic:1998:CAB


Merwin:1979:NCC


Nastar:1995:TRD


Nat-Abdesselam:1999:QCA


Naccache:1993:MSF

REFERENCES

Nachenberg:1997:CVA

Naik:1994:VMN

Nalwa:1997:AOS

Nanovic:1974:SWI

Nastar:1994:VMN

NBS:1977:DES

NBS:1980:MO
REFERENCES

NCSOTS:1984:ISR


NIST:1985:FPSa


NIST:1985:FPSb


NIST:1991:DSS


NIST:1992:DSS


NIST:1992:PYA


NIST:1993:FPD

REFERENCES


Shipping list no.: 94-0159. Issued February 9, 1994.


REFERENCES

March 1999. ISBN ???. LCCN ???. URL
http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm;
http://www.nist.gov/aes. 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.

[NBD+99]

[NBWH78]

[NC97]

**Neat:1975:NCC**


**Nechvatal:1991:PC**


**Nechvatal:1996:PKB**


**Needham:1994:DSE**


**NetworkAssociates:1998:NB**


**Neumann:1991:IRCd**


**Neumann:1992:IRF**


**Neumann:1994:IRA**

Peter G. Neumann. Inside RISKS: Alternative pass-
Neumann:1995:RCD


Neumann:1997:IRC


Ng:1999:CST


Newton:1997:EC


Newman:1998:ROT


Neve:1999:FSC

REFERENCES

586X (electronic). See [XZZ98].

Nguyen:1999:CGC


Nguyen:1999:CGG


Nelson:1990:SAE


Neubauer:1998:DWI


Neubauer:1998:CSD


Nichols:1998:CCCa


Nichols:1998:CCCb


[NIST:1993:DSS] NIST. *Digital Signature Standard*. Gaithersburg, MD 20899-8900, USA,
<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS PUB 186</td>
<td>February 1, 1993. ?? pp.</td>
</tr>
</tbody>
</table>
REFERENCES

Nakamura:1988:DRM


Naccache:1994:MSC


Naccache:1996:ACP


Naccache:1996:CSC


Nadathur:1999:SDT


Naccache:1995:CMP

REFERENCES

Nguyen:1998:NDC


Nguyen:1999:DZK


Naccache:1995:CDB


Naccache:1995:CDI


Nozaki:1997:LCS


Noras:1996:CHH


Nicchiotti:1998:NIS

G. Nicchiotti and E. Ottaviano. Non-invertible sta-
tical wavelet watermarking. In Theodoridis et al. [T+98], pages 2289–2292.
Four volumes.

Nobauer:1984:CRS

Nobauer:1985:CRS

Nobauer:1988:CPK

Norman:1973:SWB

Noras:1995:CHHa

Noras:1995:CHHb

Noras:1995:PCE

Naor:1993:PZK
M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung. Perfect zero-knowledge arguments for NP can be based on general complexity assumptions. Lecture Notes in Computer Science,
REFERENCES


REFERENCES

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


REFERENCES


REFERENCES


Nurmi:1994:CPA


Needham:1997:TE


Naor:1998:ACS


Naor:1990:PKC


Naor:1989:UOH


Nyberg:1994:DUM

REFERENCES


REFERENCES

Oberzalek:1999:GEE


OConnell:1981:CDE


OConnor:1994:UBN


OConnor:1995:DCT


Obenland:1999:SED


ORuanaidh:1996:PWD


Odlyzko:1984:CAM

REFERENCES


REFERENCES


Tatsuaki Okamoto, Atsushi Fujioka, and Eiichiro Fujisaki. An efficient digital signature scheme based on an elliptic curve over the ring $\mathbb{Z}_n$. *Lecture Notes*
REFERENCES


O'Connor:1995:UMA


Oehler:1997:RHM


Oh:1999:DCT


Ohira:1999:EDD


Ohta:1996:DCT


Ohta:1998:RBD

REFERENCES

Ohta:1998:ACA
Kazuo Ohta and Tingi (Dingyi) Pei, editors. Advances in cryptology —
Asiacrypt'98: International Conference on the Theory
and Applications of Cryptology and Information Security, Beijing, China,
October 18–22, 1998: proceedings, volume 1514 of
Lecture Notes in Computer Science. Springer-Verlag,
Berlin, Germany / Heidelberg, Germany / London,

Okada:1995:LBS
K. Okada and K. Kurosawa. Lower bound on the size of
shares of nonperfect secret sharing schemes. Lecture Notes in Computer
Science, 917:33–??, 1995. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

Obana:1996:VIS
Satoshi Obana and Kaoru Kurosawa. Veto is impossible in secret sharing
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Ogata:1996:OSS
W. Ogata and K. Kurosawa. Optimum secret sharing scheme secure against
cheating. Lecture Notes in Computer Science, 1070: 200–??, 1996. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ogata:1998:SBP
W. Ogata and K. Kurosawa. Some basic properties of general nonperfect
secret sharing schemes. J.UCS: Journal of Universal
Computer Science, 4(8): 690–??, August 28, 1998. ISSN 0948-6968. URL
http://medoc.springer.de:8000/jucs/jucs_4_8/
some_basic_properties_of.

Okamoto:1988:DMS
Tatsuaki Okamoto. A digital multisignature scheme using bijective public-key

Okamoto:1993:RAC
T. Okamoto. On the relationship among cryptographic physical assump-
Okamoto:1993:PSP


Okamoto:1994:DCS


Okamoto:1998:TKR


Okamoto:1998:TKS


Okon:1996:DWN


Okon:1997:KMA


Ogata:1997:FTA

REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/064437.html

Ogata:1993:NSS


Oleshchuk:1995:PKC


Oldehoeft:1984:SSU


Ohta:1994:DAM

[OM94] Kazuo Ohta and Mitsuru Matsui. Differential at-

Ohbuchi:1997:WTP


Ohbuchi:1998:WTD

Ozaki:1993:HVP


Omura:1990:PKC


Ochi:1998:NSO


O’Neil:1986:ETM


Ogawa:1998:WTM


Okamoto:1990:DZKb


Ohta:1993:DMS


Rolf Oppliger. *Authentication systems for se-


Orton:1995:MTD


Orton:1995:MIT


O'Shea:1988:CDU


Okamoto:1991:EAC


Okamoto:1992:EAC


Olejar:1998:CPR


Orup:1991:VER

REFERENCES


REFERENCES

Ou:1999:UUC


Outerbridge:1998:ACD


Ozarow:1984:WTC


OReilly:1995:WWW


Ostrovsky:1991:HWM


Pfitzmann:1993:MES

Andreas Pfitzmann and Ralf Aßmann. More efficient software implementations of (generalized)
REFERENCES 665


[Rajay R. Pai. VLSI implementation of the extended Data Encryption Standard algorithm. Thesis (M.S.), University of Texas at Arlington, Arlington, TX, USA, 1996. x + 85 pp.]


[Paillier:1999:LCD]


[PAK98]


[Parthasarathy:1985:DSG]


[Par96]


Preneel:1989:CHB


Preneel:1990:CTA


Petrie:1998:NBR


Pizzonia:1999:OOD


Popovic:1999:DIT


Plagge:1999:DET

[PDGI99] M. Plagge, B. Diebold, R. Guenther, and J. Ihlenburg. Design and evaluation of the T-Team of
REFERENCES

the University of Tübingen for RoboCup'98. Lecture Notes in Computer Science, 1604:464–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


Pedersen:1991:NII


Pedersen:1991:NIT


Pedersen:1995:EPS


Pedersen:1999:SCP


Pelta:1960:SP


Penzhorn:1996:CAS


Perret:1890:RCS

REFERENCES

Peralta:1985:TRN


Perry:1988:EBG


Perry:1991:EIT


Peralta:1993:QSD


Perrig:1997:CPE


Perkuhn:1999:DSC


Pesic:1997:SSS


Petho:1991:PTA

A. Pethö. On a polynomial transformation and its application to the construction of a public key

Petersen:1998:HCD


Panagopoulos:1994:BSS


Pfitzmann:1996:BEA


Pfitzmann:1996:IHT


Pfitzmann:1996:TTT


Pfitzmann:1996:DSS


[Pfleeger:1989:SC]

[Pfleeger:1995:ULC]

[Pfleeger:1997:SC]

[Pomerance:1990:CCNb]

[Patarin:1997:ACB]

[Patarin:1997:ACS]

[Pieprzyk:1996:CBT]
REFERENCES

Preneel:1991:CRH


Preneel:1992:CSH


Preneel:1993:CHF


Preneel:1993:HFB


Preneel:1993:IAH


Preneel:1993:CSI


Preneel:1994:HFB

Bart Preneel, Rene Govaerts, and Joos Vandewalle.
REFERENCES


Pohlig:1978:IAC


Post:1991:RSE


Praun:1999:RMW


Phillips:1998:SHI


Pichler:1986:ACE


Pichler:1998:E

REFERENCES

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

Pierce:1977:SSP


Pieper:1993:CRD


Pinch:1997:UCN


Piter:1995:PIW


Piter:1996:MSC


Pitoura:1996:RSS

connectivity in mobile information systems. Lecture Notes in Computer Science, 1134:510–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Price:1999:IAV


Panneerselvam:1990:RSA


Praehofer:1999:SRS


Penzhorn:1995:CLP


Penzhorn:1995:CLW


Pamplona:1998:LVC

August Pamplona, Mike
REFERENCES 679


Postma:1997:DCF


Park:1994:KDA


Petrounias:1994:RBA


Pless:1975:ESC


Pless:1977:ESC


Plimmer:1998:MIW

Beryl Plimmer. Machines invented for WW II code breaking. SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education), 30(4):37–
REFERENCES

40, December 1998. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Plumstead:1982:ISG


Plumstead:1983:ISP


Pei:1999:COA


Payne:1978:OEN


Petersen:1998:SST


Pitt:1999:DAC


Provos:1999:FAP

Niels Provos and David Mazieres. A future-


REFERENCES

**Pollard:1978:MCM**


**Pomerance:1988:ACC**


**Pomerance:1990:CCNa**


**Pomerance:1990:F**


**Pomerance:1994:NFS**


Pomerance:1998:C


Poole:1995:La


Popentiu:1989:SRK


Pope:1996:PF


Porges:1952:MNC


Porter:1984:CNS


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT

P. Poromaa. Parallel algorithms for triangular

**Posch:1992:TMD**


**Posch:1993:PFP**


**Posch:1998:MPC**


**Posch:1989:AEA**


**Pfitzmann:1990:HBD**


**Posch:1992:MRR**


**Posch:1992:RNS**

K. C. Posch and R. Posch. Residue number systems: a


Pieprzyk:1985:DPK


Pieprzyk:1985:MDI


Preneel:1998:SAA


Preneel:1998:RDD


Pratt:1939:SUS


Pratt:1996:SUS


Parra:1998:MPS

REFERENCES


[Pre97a] B. Preneel. Hash functions and MAC algorithms based


W. L. Price. Annotated bibliography of recent publications on data security and cryptography, volume 35/83
of *NPL-DITC*. National
Physical Laboratory, Ted-
dington, Middlesex, UK,
by permission of the Con-
troller of Her Britannic
Majesty's Stationery Office.
“PB84-169168.” Photocopy.
Springfield, VA: National
Technical Information Ser-
vice, [1983?]. 28 cm.

**Price:1994:MVC**

D. Price. Micro view. clip-
per: soon a de facto stan-
dard? *IEEE Micro*, 14
(4):80–80, 79, July/August
1994. CODEN IEMIDZ.
ISSN 0272-1732 (print),
1937-4143 (electronic).

**Pronzini:1980:MCC**

Bill Pronzini. *Mummy!: a
chrestomathy of cryp-tology.*
Arbor House, New York,
NY, USA, 1980. ISBN 0-
87795-271-X. xii + 273
pp. LCCN PN 6120.95 M77
M86 1980. US$10.95. Con-
tents: Doyle, A.C. Lot no.
249.–Poe, E.A. Some words
with a mummy.–Benson,
E.F. Monkeys.–Wollheim,
D.A. Bones.–Williams, T.
The vengeance of Nitocris.–
Gautier, T. The mummy's
foot.–Bloch, R. The eyes
of the mummy.–Powell, T.
Charlie.–Hoch, E.D. The
weekend magus.–Lansdale,
J.R. The princess.–Mayhar,
A. The eagle-claw rattle.–
Grant, C.L. The other
room.–Malzberg, B.N. Rev-
elation in seven stages.–
Bibliography.

**Proctor:1985:SSC**

Norman Proctor. A self-
synchronizing cascaded ci-
pher system with dynamic
control of error propaga-
tion. In Blakley and
Chaum [BC85], pages 174–
190. CODEN LNCS-D9.
ISBN 0-387-15658-5; 3-540-
39568-7. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&spage=174. CRYPTO
84: a Workshop on the
Theory and Application of
Cryptographic Techniques,
held at the University of
California, Santa Barbara,
August 19–22, 1984, spon-
sored by the International
Association for Cryptologic
Research.

**Patel:1999:TML**

S. Patel, Z. Ramzan, and
G. S. Sundaram. To-
wards making Luby-Rackoff
ciphers optimal and prac-
tical. In Knudsen [Knud99c],
pages 171–185. ISBN 3-540-
66226-X (softcover). LCCN
Peyravian:1999:HBE


Paun:1993:CPS


Pieprzyk:1993:DHA


Pfitzmann:1996:AF


Pfitzmann:1996:PSB


Pfitzmann:1996:SPS

REFERENCES


REFERENCES


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

[Patiyoot:1999:WWA]


[Pfenning:1999:SDT]


[Patel:1997:UDB]


 PIEPRZYK:1995:PA


 PIEPRZYK:1995:ACA

REFERENCES


REFERENCES


Parkes:1999:ACC


Purdy:1974:HSL


Puteanus:1627:EPC


Preparata:1990:PCD


Preneel:1997:HPC


Posegga:1998:BCV


Pluimakers:1986:ACS


Preneel:1995:MMB

[B. Preneel and P. C. van Oorschot. MD-x MAC and building fast MACs from hash functions. In Cooper-smith [Cop95d], pages 1–14.
REFERENCES


Preneel:1996:STM


Pfitzmann:1986:NUO


Power:1986:AHE


Pfitzmann:1987:NUO

REFERENCES

Power:1987:AHE


Pfitzmann:1993:APS


Piper:1993:DSH


Pfitzmann:1997:AF


Pfitzmann:1997:SLT


Piper:1998:CSV


**Piccardi:1999:CLD**


**Polani:1999:DAR**


**Podilchuk:1998:IAW**


**Quisquater:1998:CSE**


**Quisquater:1991:CLE**


**Quisquater:1989:BHF**

J. J. Quisquater and M. Girault. 2n-bit hash-functions using n-bit symmetric block cipher algorithms. In Quisquater and Vandewalle [QV89], page ?? ISBN 0-387-
REFERENCES


\textbf{Quisquater:1990:BHF}


\textbf{Quisquater:1995:ACE}


\textbf{Qiao:1998:CME}


\textbf{Qiao:1998:WMM}


\textbf{Qin:1988:RSS}

REFERENCES

SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Quisquater:1989:ACE

Quisquater:1990:ACE

Quisquater:1998:E

Rabin:1977:DS

Rabin:1981:HES

Rabin:1989:EDI
Michael O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. Journal of the
Rabin:1994:RSS

Rabin:1998:SAT

Rackoff:1990:BTP

Radlo:1997:LIC

Ramagopal:1992:DRB

Rand:1955:MRD

Randell:1982:CGC
REFERENCES


REFERENCES

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

Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA


Rogaway:1994:SOE


Russinovich:1995:EWL


Rubia:1999:RIB

[Montse Rubia, Juan Carlos Cruellas, and Manel Medina. Removing interoperability barriers between the X.509 and EDIFACT public key infrastructures: The DEDICA Project. Lecture Notes in Computer Science,
Renvall:1996:ASS

Renvall:1996:NSS

Roback:1999:CRF

Roback:1999:FAE

Rebel:1998:ADS
[RDK98] Thomas F. Rebel, Olaf Darge, and Wolfgang Koenig.

Rijmen:1996:CS
[RDPB96] V. Rijmen, J. Daemen, B. Preneel, and A. Bosselaers.
REFERENCES

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

Reeds:1979:CMC

Rees:1997:AGO

Reeds:1998:SCB

Reischuk:1985:NSB

Reiter:1992:ISG

Reiter:1996:DTR


Frank B. Rowlett and William F. Friedman. *Further

Reiter:1996:KMS

Reiter:1995:SCR

Rhodes:1999:SPH

Radu:1997:WHR

Rubin:1993:LRJ

Ryu:1999:PAA

Rivest:1992:RNP
Ronald L. Rivest, Martin E. Hellman, John C. Anderson, and John W. Lyons. Responses to NIST's proposal. Communications of
REFERENCES


[Rhee:1993:RAC]


[Rhee:1994:CSC] [Rij99]


[Rhoads:1995:SMA]

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

[Richards:1974:SWP]


[Rijmen:1999:WL] [Rih99]


[Rhoads:1995:SMA]

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

[Richards:1974:SWP]

[Rile96] 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.
References


and New York NY, USA)-Verlag, 1976, with mod. title.


REFERENCES


Rivest:1991:FFM


Rivest:1991:MMD


Rivest:1992:RMMa


Rivest:1992:RMMb


Rivest:1993:DRR


Rivest:1993:CML


Rivest:1993:NPD


Rivest:1995:DRR

REFERENCES


Rivest:1998:CWE


Rivest:1998:CAR


Rivest:1998:CWC

cryptobytes/crypt04n1.pdf.

Rivest:19xx:PC


Rhodes:1993:ZF


Rijmen:1998:WL


Rowlett:1998:SMM


Roy:1999:QCE

REFERENCES


Rosenson:1994:GWE


Ruanaidh:1996:WDI


Reeds:1985:NPR


Rao:1987:PKA


Rao:1989:PKA


Raisch:1996:ACH

J. Raisch and S. O’Young. A DES approach to control of hybrid dynamical systems.


REFERENCES

Rogaway:1995:BHA


Rogaway:1996:SD


Rohwer:1975:GIM


Rohwer:1977:CCB


Rohatgi:1999:CNR


Roman:1990:C


Rompel:1990:OWF

REFERENCES

Rose:1993:RCM


Rosen:1994:EMT


Rose:1995:PPZ

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.

Rose:1995:SUP


Rose:1996:IUP


Rose:1996:PMI


Rose:1996:PZH

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

Rose:1996:UCI


Rose:1996:UPKa

Greg Rose. USENIX PGP key-signing service. ;lo-
REFERENCES

718


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.).


REFERENCES

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


Raubert:1997:SDW


Rigney:1997:RRAa


Rigney:1997:RRAb


Rivest:1998:RBC


Rivest:1983:RET


Rivest:1984:HEE

Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. Communications of the Association for Computing Machinery,
REFERENCES


**Riordan:1998:EKGa**


**Riordan:1998:EKGb**


**Rivest:1998:SPN**


**Ryan:1998:ARA**


**Ravi:1999:AAT**


**Reiter:1999:AMA**


REFERENCES


RSA:1993:PEC


RSA:1993:PCM


RSA:1993:PPK


Laboratories:1993:PKC


RSA:1994:MPK


RSA:1999:PVPb


RSA:1999:PVPa


Reed:1998:ACO

REFERENCES

CODEN ISACEM. ISSN 0733-8716 (print), 1558-0008 (electronic). URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/072144.html

Reif:1988:EPP


Rezny:1993:BCM


Raleigh:1988:CDP


Rubin:1979:DSC


Rudolph:1982:HT1


Rudich:1991:UIP

REFERENCES


**REFERENCES**

**Ruskey:1993:SCG**


**Russell:1993:NSC**


**Roychowdhury:1999:ENQ**


**Reeds:1984:FSU**


**Robshaw:1997:ECC**


**Rytter:1986:SCU**


**Ras:1999:DES**


**S:1873:COD**

[S.73] H. S. Cryptographie, ou, Divers systèmes d’écrire secrète spécialement pour l’usage des cartes postales: combinaisons alphabétiques, correspondance chiffrée, écriture par signes: divers
REFERENCES

procédés pour la fabrication d’encres sympathiques.

Schiller:1995:SWT


Sabourin:1994:CCP


Sacco:1947:MC


Sacco:1951:MCF


Sacco:1977:MC


Sahai:1999:NMN

REFERENCES


Salomaa:1991:VRS

Sale:1993:EBP

Salomaa:1996:PC

Salvail:1998:QBC

Salvail:1999:SHG

Shimoyama:1997:IFS

Sameshima:1998:KES

Sansom:1986:BRC
REFERENCES


Sandhu:1988:CIT


Sarton:1928:BRBn


Sars:1997:STL


Sargent:1999:FID


Sasaki:1999:SFU


Swierstra:1999:DIC


Satyanarayanan:1989:ISL

M. Satyanarayanan. Integrating security in a large distributed system. ACM
Saunders:1989:IDE


Savarnejad:1996:COF


Savarnejad:1997:GAD


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Sorkin:1984:MCC


Smid:1992:DES

REFERENCES


[SB99] Juan Soto and Lawrence Bassham. Randomness testing of the Advanced Encryption Standard candidate algorithms. NIST internal report 6390, National
REFERENCES

Serpell:1985:PES

Stallmann:1999:HED

Siegberg:1999:TDG

Sztandera:1999:ANN
REFERENCES

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

**Shepherd:1999:NCS**


**Chen:1985:RGE**


**Schneider:1996:RCB**


**Smith:1996:MIH**


**Sun:1997:DCP**

REFERENCES

Schneider:19xx:DWI

Scacchitti:1986:CT

Styner:1999:BMD

Schwenter:1620:SSN

Schwenter:1633:SSA

Schroeder:1969:IC
Schroeder:1975:ESK


Schell:1983:SPA


Schroeder:1984:NTS


Schroeder:1986:NTS


Schnorr:1990:EISb


Schnorr:1990:EISa

REFERENCES

Schroeder:1990:NTS


Schmitt:1991:EAA


Schneier:1991:OHP

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

Schneier:1991:SSA

DEN COMLEF. ISSN 0749-2839.


Schneier:1994:BEA


Schneier:1994:CAW


Schneier:1994:NC


Schneier:1994:PYM


Schneier:1994:RDS


Schneier:1995:AAB


Schneier:1995:AAG


Schneier:1995:MS


Schneier:1995:MSH

REFERENCES


Schneier:1995:OPE


Schneier:1995:PCC


Schneier:1996:ACP


Schneier:1996:CC


Schneier:1996:DLC


Schneier:1997:IRC


Schneier:1997:WCH


Schroeder:1997:NTS

M. R. (Manfred Robert) Schroeder. Number the-

Schweighofer:1997:DIF


Schlesinger:1998:CPC


Schneier:1998:MDI


Schneier:1998:CBT


Schneier:1998:CDV

REFERENCES

Schneier:1998:CTS

Schneier:1998:SPC

Schneier:1998:TEA

Schoenmakers:1998:SAE

Schroeppel:1998:HPC
[RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

**Schaefer:1999:PES**


**Schmalz:1999:MDI**


**Schmidt:1999:RER**


**Schneier:1999:SSC**


**Schneier:1999:IRR**


**Schneier:1999:IRT**

**REFERENCES**

---

**Schneier:1999:IRU**


---

**Schneier:1999:IWC**


---

**Schoenmakers:1999:SPV**


---

**Schwentick:1999:DCL**


---

**Scerri:1999:UOS**

Scudder:1992:OLA


Smith:1986:GCC


Silvestre:1997:IWU


Schouten:1999:FEU


Sicherman:1983:AQR


Smillie:1986:RWA


Schwenk:1996:PKE

[SE96] Jörg Schwenk and Jörg Eisefeld. Public key encryption and signature schemes based on polynomials over
REFERENCES


**Seaton:1956:THS**

**Sears:1986:SWK**

**Seachrist:1995:DIM**

**Sedlak:1988:RCP**

**Sedgewick:1992:AC**
REFERENCES

0-201-51059-6. xiv + 656 pp. LCCN QA76.73.C153 S38 1992. [Sel94]


REFERENCES

239–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


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.


[Sha82] Adi Shamir. A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem. In *23rd annual symposium on founda-
REFERENCES


R. L. Sharp. Design of a certifiable one-way data-flow


Adi Shamir. Power analysis of the key scheduling of the AES candidates.
REFERENCES

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

Sherman:1986:CVT


Sherman:1987:CVT


Sherman:1988:CVV


Shepherd:1992:DSA


Shepherd:1992:FFW


Shepherd:1992:FHS

S. J. Shepherd. A fast, high security public key proces-
REFERENCES

Shepherd:1992:HSC


Shepherd:1992:NPS


Shepherd:1992:SIR


Sherrod:1992:DES


Shepherd:1993:ACCa


Shepherd:1993:ACCb


Shepherd:1993:EOS


Shepherd:1993:WNS

REFERENCES


S. J. Shepherd. Primitive polynomials over GF(2) of Hamming weight 3 and 5


REFERENCES


**Shumaker:1982:RCJ**


**Sakurai:1993:DBS**


**Sakurai:1993:SCS**


**Sidhu:1981:APG**


**Sieminski:1983:SBB**

Gregory C. Sieminski. The search for a balance be-

**Siegenthaler:1984:CIN**


**Shimbo:1993:CSC**


**Silverman:1983:RVS**


**Silverman:1987:MPQ**


**Silverman:1997:RSP**

R. D. Silverman. The requirement for strong primes


REFERENCES


Simmons:1983:PPS

Simmons:1984:HID

Simmons:1985:ATC

Simmons:1985:SCD

Simmons:1988:SSC

Simmons:1990:HRS
G. J. Simmons. How to (really) share a secret. In Goldwasser [Gol90b], pages 390–449. CODEN
REFERENCES


Simmons:1990:PSS


Simmons:1991:GSS


Simmons:1992:CCS


Simmons:1993:SCU


Simmons:1994:CTS


Simmons:1994:CPF


Simmons:1994:SCP


Simmons:1994:SCE


Simovits:1995:EDE


Simmons:1996:HSC


Simpson:1996:RPC

letes RFC1334 [LS92]. Status: DRAFT STANDARD.

**Simmons:1997:SCS**


**Simmons:1998:HSC**


**Simmons:1998:RCB**


**Simon:1998:FCO**


**Sinkov:1966:ECM**


**Sinkov:1968:ECMa**


**Sinkov:1968:ECMb**

[Sim98b] Abraham Sinkov. Elementary cryptanalysis: a


[SJ97] Ishwar K. Sethi and Ramesh C. Jain, editors. *Fifth Conference on Storage and Retrieval for Image and Video Database, 13–14 February 1997, San Jose, CA, USA*, volume 3022 of *SPIE proceedings series*. Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, USA,
Scott:1998:DAB


Sako:1994:SVU


Sako:1995:RFM


Schneier:1996:AOC


Schneier:1996:PPSa


Schneier:1996:UFNa

B. Schneier and J. Kelsey. Unbalanced Feistel networks and block cipher de-
REFERENCES


Schneier:1998:CSS


Shimoyama:1998:QRS


Shimoyama:1998:QRB


Schneier:1999:SAL


Stabell-Kulo:1999:PAM


Shepherd:1997:EKE

S. J. Shepherd, A. H. Kemp, and S. K. Barton. An ef-

Schell:19xx:CMC


Sorokine:1994:TBD


Suzuki:1999:AVB


Satoh:1998:HSR


Satoh:1998:HSS


Schneier:1996:DP


Schneier:1998:TKSa

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


[Schneier:1998:TBBa]


[Schneier:1998:TBBb]


[Schneier:1998:TBBc]


Schneier:1999:NRT


Schneier:1999:TEAb


REFERENCES

Schneier:1999:PCAA


Schneier:1999:PCAB


Schneier:1999:APC


REFERENCES

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

Schubert:1995:MLS


Syverson:1995:FRK


Sklower:1996:RPE


Sutcliffe:1999:LBM

REFERENCES

[Smart:1999:PHC]

[Schneier:1999:DDE]

[Smejkal:1997:DEI]

[Smith:1943:CSS]

[Smith:1944:CSS]

[Smith:1955:CSS]

[Smith:1971:CSS]

[Smith:1983:PKC]
John Smith. Public key cryptography: An introduction to a powerful cryptographic system for use on microcomputers. *BYTE*
This is a simple exposition of public key cryptography. [Smi93b]


Larry J. Smith. Cryptology, privacy and the Clipper chip. Thesis (M.S.), Texas Tech University, Lubbock, TX, USA, 1994. vi + 72 pp. [Smi97b]


7.80 REFERENCES


**Smith:1998:IES**


**Smith:1998:SXC**


**Shimoyama:1998:IHO**


**Son:1998:ASC**


**Stakhov:1999:IFC**


**Safavi-Naini:1993:FTA**


**Shepherd:1994:VFH**


**Safavi-Naini:1996:TSS**

R. Safavi-Naini. Three systems for shared generation

**Steiner:1988:KAS**


**Safavi-Naini:1993:ACU**


**Safavi-Naini:1995:ACP**


**Safavi-Naini:1998:BCM**


**Safavi-Naini:1998:NRM**


**Snyder:1979:IUC**

REFERENCES


MTKAAB. ISSN 0025-5793.

Seberry:1989:CIC


Seberry:1990:AAC


Schechter:1999:AAM


Spirakis:1995:AET

REFERENCES


Schwemmlein:1998:RMR


SPP98

Schuett:1997:CPB


SPS97

Shoup:1996:SKD


SR96

Saltzer:1984:EEA


SRC84

Shin:1998:NHF


SRRL98

Shin:1999:HFM


SRY99
REFERENCES


REFERENCES

Smith:1995:PCD


Smith:1995:PKC


Sandhu:1996:AAC


Silverman:1997:CAX


Sakai:1998:DHC


Sun:1998:PKC


Schneier:1999:BHD


First USENIX Symposium on Smart Cards, USENIX Press, to appear.


REFERENCES


S. J. Shepherd, P. W. Sanders, and A. Patel. A comprehensive security system — the concepts, agents

**Schmidt:1998:LOA**


**Salter:1998:TSS**


**Schneier:1998:DDE**


**StJohns:1984:RAS**


**StJohns:1985:RAS**

REFERENCES

Shawe-Taylor:1989:BRB


Stern:1991:CPK


StJohns:1993:RIP


Safavi-Naini:1994:OAS


Stark:1970:INT


Stark:1978:INT

[Sta78] Harold M. Stark. An introduction to number the-
REFERENCES


**Stallings:1994:PGP**

[Sta94a] William Stallings. Pretty Good Privacy: Privacy and security are important issues to commercial users of public E-mail systems. PGP, an E-mail security package, is finding acceptance as the way to achieve protection. *BYTE Magazine*, 19(7):193–??, July 1994. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

**Stallings:1994:SSH**


**Stallings:1995:PWT**


**Stallings:1995:PYP**


**Stadler:1996:PVS**


**Staiger:1996:CSW**


**Stallings:1996:PCS**


**Stallings:1996:PCI**

[Sta96d] William Stallings. Practical cryptography for internetworks. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
REFERENCES


Staddon:1997:CSC


Stallman:1997:SDR


Stark:1997:ESP


Stallings:1999:CNS


Stallings:1999:HAK


Stevenson:1976:MCI


Stern:1987:SLC

J. Stern. Secret linear congruential generators are not

Stevens:1988:CPR


Stephenson:1989:PPM


Stevens:1990:CPi


Stevens:1990:CPk


Steinberg:1991:VSV


Stewart:1992:SCK


Stern:1994:DIS


Stevens:1994:PBa

Stern:1995:COD


Stern:1996:VCA


Stern:1998:LCO


Stern:1998:NEA


Stephenson:1999:C


Stern:1999:ACE


Stern:1999:DU

aes. No slides for the conference talk are available.

Stinson:1991:CCA

Stinson:1991:UHA

Stinson:1993:NGL

Stinson:1993:ACC

Stinson:1994:ACC
REFERENCES


(print), 1611-3349 (electronic).


[Hiroki Sutoh. A high-performance public key cryptography co-processor for super multi-purpose smart card. In Anonymous [Ano99c], page ??]

REFERENCES


[SvA+98] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling

[SvA+98] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling

[SvA+98] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling

[SvA+98] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling

[SvA+98] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling
PC's; server-side scripting; stronger encryption; inner loops; Einstein kudos. *Dr. Dobb's Journal of Software Tools*, 23(3):8, 12, March 1998. CODEN DDJOEB. ISSN 1044-789X.

Sivakumar:1999:PPN


Shepherd:1995:SCS


Shamir:1998:PHS


Smeets:1991:CAC


Shulman:1961:GC

REFERENCES


References


Schneier:1997:FSEb


Stinson:1998:ARS


Stinson:1999:KPT


Swan:1994:AAb


Swire:1997:ULF

Salzer:1981:RHH


Sun:1989:TKE


Sun:1990:KGE


Salomaa:1986:PCB


Salomaa:1986:PKC


Smith:1992:ICF


Sakurai:1996:BDB

K. Sakurai and Y. Yamane. Blind decoding, blind undeniable signatures, and their applications to privacy protection. In Anderson [And96c],
REFERENCES


Shieh:1996:AKD


Sowers:1998:TDW


Sellini:1999:VKV


Syverson:1992:KBS


Syverson:1993:KDP

Seberry:1993:ACA


Sakurai:1996:CWR


Szepietowski:1998:WSO


Swanson:1996:RDH


Swanson:1996:TRI


Swanson:1998:MSB

REFERENCES

Swanson:1998:MSV


Swanson:1998:RAW


Szweda:1997:ESW


Szweda:1997:STF


Seberry:1994:ISA


Seberry:1994:PDS

Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng.

Seberry:1995:RAN


Seberry:1995:SCF


Seberry:1995:RBP


Seberry:1995:RBP


Seberry:1995:RBP


Tardo:1992:SGA


Tardo:1992:SGA
REFERENCES

1992. CODEN JCSIET.
ISSN 0926-227X (print),
1875-8924 (electronic).

[Tang:1997:DBC]
Weili Tang and Yoshino Aoki. DCT-based coding
of images in watermarking. In IEEE [IEE97k],
pages 510–512. ISBN 0-
7803-3676-3 (softbound,) 0-
7803-3677-1 (microfiche).
Three volumes. IEEE catalog number: 97TH8237.

[Taaffe:1998:NBL]
magazine for the Java community, 3(1):??, January 1998. CODEN ????
ISSN 1091-8906. URL http://www.javaworld.
htm.

[Tabatabaian:1994:CAP]
Seyed Jalil Tabatabaian. Cryptanalysis algorithms
for public key cryptosystems.
Thesis (Ph.D.), University of Newcastle upon

[Takagi:1997:FRT]
Tsuyoshi Takagi. Fast RSA-type cryptosystems using $n$-adic expansion. Lecture
Notes in Computer Science,
1294:372–384, 1997. CODEN LNCSD9. ISSN 0302-
link/service/series/0558/
bibs/1294/12940372.htm;
pdf.

[Takagi:1998:FRC]
T. Takagi. Fast RSA-type cryptosystem modulo $p^k q$. Lecture Notes in
Computer Science, 1462:
318–326, 1998. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[Takagi:1998:FRT]
Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo $p^k q$. Lecture Notes in
Computer Science, 1462:
318–??, 1998. CODEN LNCSD9. ISSN 0302-9743
link/service/series/0558/
bibs/1462/14620318.htm;
pdf.

[Tanaka:1990:RSI]
Hatsukazu Tanaka. A realization scheme for the


Taylor:1995:NOU


Tao:1985:FAP


Tao:1986:TVF


Tsuji:1991:NIB


Tao:1997:VPK


Tao:1999:GPK


Tao:1999:FAP

Tao:1997:FNF


Tangney:1991:SIS [Tes98]


Tedrick:1985:FES [Tes98]


Teske:1998:SPR


TI:1984:TTU [Tes98]

[Tex84] Texas Instruments Inc. TMS7500 TMS75C00 user’s guide, data encryption device: 8-bit microcomputer family. Texas Instruments, Dallas, TX, USA, 1984. various pp.

Tourigny:1994:DSD


Tanaka:1999:PCD


REFERENCES

Thomas:1996:PVS

Tarman:1998:AAE

Tsujii:1988:PKC

Tilki:1998:EHD

Tippett:1927:RSN

Taafe:1997:NSL

Tseng:1999:ATS


D. Theodoratos, S. Ligoudistianos, and T. Sellis. Designing the global data warehouse with SPJ views.
REFERENCES

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


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

Toussaint:1993:FVP


Tsunoo:1994:COA


Touch:1995:RRM


Townsend:1998:QCO


Thompson:1963:SDE


Traore:1997:MUF


Traore:1999:GST

REFERENCES


**REFERENCES**

**Trithemius:1621:CSI**


**Trithemius:1621:SHE**


**Tro97**


**Tirkel:1993:EW**


**Trostle:1993:MFT**


**Tirnock:1997:C**


**Tirkel:1993:EW**


**Terry:1988:MSV**


**TS88**

REFERENCES


Tsujii:1992:CS  

Thomlinson:1998:NBP  

Thersites:1984:IKE  

Thomas:1984:IKE  

Tiountchik:1999:RAF  

Tual:1999:MGA  

Tuchman:1966:ZT  
scribes this book as “re-count[ing] the political effects of the most important cryptogram solution in history”.

Tuchman:1979:HPN


Tuchman:1979:IHP


Tung:1999:KNA


Turing:1941:APC

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

Turing:1999:TTE

[Tur99] Alan Turing. Turing’s treatise on Enigma. Technical report, CERN, Geneva, Switzerland, 1999. URL http://home.cern.ch/~ frode/crypto/Turing/index.html. This document is 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


[TY98b] Yiannis Tsiounis and Moti Yung. On the security of ElGamal-based encryption. Lecture Notes in
REFERENCES


[Tze99]


[Ude98]

[Ueh95]


[Tzeng:1999:CMP]


[Ude98]

[Ueh95]

[TZ94] 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).

[Ueh95]

Udell:1994:BCRb


USASC:1923:EC


USASC:1940:CML


USASC:1942:ACC


USWD:1924:EC


USNBS:1977:DES

REFERENCES


REFERENCES


USGSA:1982:TGS


USNBS:1983:FPD


USGSAOIRM:1984:ISR


USGSAOIRM:1984:ISR


USGSAOERM:1984:ISR


**USNSACSSCCH:1992:FLT**


**USDOA:1994:OMT**


**USDOA:1994:UDS**


**USNSACS:1994:SC**


**USCSCJSTL:1995:ACC**


**USNSGC:1995:NDN**


REFERENCES

Shipping list no.: 97-0329-P. Serial no. 9.

USCSCJ:1997:EKR

USGAOOGC:1997:DCB

USCHCIR:1998:HEI

USCHCIR:1998:MHS

USCHCIR:1998:HSF

USCHCIRSIIEPT:1998:EIR
REFERENCES


USCHCIRSIEPT:1998:HSF


USCSCCST:1998:HEH


USCSCCST:1998:EHB

REFERENCES


United States. General Services Administration, Na-

[UNU85]


[USE88a]


[USE88b]

REFERENCES


REFERENCES


**USENIX:1995:PUT**


**USENIX:1995:PFUa**


**USENIX:1995:PFUb**


**USENIX:1995:PSUa**


**USENIX:1995:PSA**


**USENIX:1996:SAC**


**USENIX:1996:WEC**


**USENIX:1996:CSW**


**USENIX:1996:PSA**


USENIX:1996:PUA


USENIX:1996:USS


USENIX:1996:PUWa


USENIX:1998:PUWb


USENIX:1998:PFT


USENIX:1998:SUS

REFERENCES

USENIX:1999:PEU


USENIX:1999:PTSa


USENIX:1999:PUWa


USENIX:1999:UAT


USWD:1980:EC


USWD:1983:EC


USDOA:1989:BC

[UU89] United States. Dept. of the Army and United States
REFERENCES


**USCHCJ:1997:SFT**


**USPBC:1997:AEC**


**VanderBank:1988:CFM**


**Vadhri:1995:VID**

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**


**Vamos:1985:BRB**

VanTassel:1969:ACT

VanHeurck:1987:TNS

vanTilborg:1988:IC

VanTilburg:1993:SKE

vanOorschot:1995:DCS

VanTilborg:1995:ACA
vanRenesse:1996:OSC

vanDijk:1997:MIT

vanRenesse:1997:ODS

vanderLubbe:1998:BMC

Varaiya:1999:DSI

Varma:1999:IDD

Vaudenay:1993:FHI

Vaudenay:1995:NMC
S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4


REFERENCES


REFERENCES

Vandewalle:1990:ECC


Dijk:1995:LCP


vanDijk:1995:LCP


vandenAssem:1986:CPA


Vandermeulen:1999:ADM

F. Vandermeulen, P. De Meester, P. De Ceulener,

Lubbe:1998:BMC


Lubbe:1998:BMC

Wal:1997:PBR


Vedder:1998:GSS


Vedder:1998:ISI


Venema:1990:IEI


Venkaiah:1992:RBP


Vernam:1926:CPT

G. S. Vernam. Cipher printing telegraph systems


Vershuren:1993:IOS


vanFaber:1997:SDD


vanHeijst:1993:NCF


Vigna:1998:CTM


Vincent:1971:PAG


Vincent:1972:CPA

REFERENCES


REFERENCES


Kerckhoffs:1883:CMF


Varadharajan:1999:DER


Voyatzis:1998:DW


Venkataraman:1994:PAM


Venkataraman:1995:CE

REFERENCES


Paul C. van Oorschot.

Paul C. van Oorschot.

Rainer Vogel.

REFERENCES

LCCN ???? Chrono-
logically arranged, covering
period 1518–1940, and in-
dexed by authors.

Processor-efficient exponentiation
in finite fields. *Information Processing
Letters*, 41(2):81–86, February
14, 1992. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

Earth and Space
Science

Processor-efficient exponentiation
in finite fields. *Information Processing
Letters*, 41(2):81–86, February
14, 1992. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic).

[Vou80a] D. C. Voukalis. The
distance factor in cryptosys-
tems. *International Journal of Electronics
Theoretical & Experimental*, 49(1):73–75,
1980. CODEN IJELA2.
ISSN 0020-7217.

[Vou80b] D. C. Voukalis. A good
solution of the encryption
problem using matrix code,
distance factor and PN se-
ces. *Internat. J. Electron.*,

CODEN IJELA2. ISSN
0020-7217.

Paul C. van Oorschot
and Michael J. Wiener.
A known-plaintext attack on
two-key triple encryption.
In Damgård [Dam91a],
pages 318–325. CODEN
LNCS09. ISBN 0-387-
53587-X (New York), 3-540-
53587-X (Berlin). ISSN
0302-9743 (print), 1611-3349 (electronic). LCCN
DM69.00. URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/0473/04730318.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0473/04730318.
pdf.

Paul C. van Oorschot
and Michael J. Wiener. On
Diffie–Hellman key agree-
ment with short expo-
nents. In Maurer [Mau96b],
pages 332–343. CODEN
LNCS09. ISBN 3-540-
61186-X. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
E964 1996. URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/1070/10700332.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1070/10700332.
pdf. Sponsored by the
International Association for Cryptologic Research (IACR), in cooperation with the University of Saragossa.

Voyatzis:1996:ATA


Voyatzis:1998:DIW


Voyatzis:1999:PDI


Varadharajan:1997:ISP


Vassiliadis:1988:PEA


Volts:1941:BC

James D. Volts and David Shulman. Bibliography of


vanTilburg:1994:SAC


vanTilburg:1986:DBK


vanSchyndel:1994:DW


Vu:1995:CPM


Vazirani:1985:ESP


Valiant:1986:NED

L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. Theoretical Com-
Verheul:1997:CLS

Vandemeulebroecke:1990:SCB

Verheul:1997:BEF

VanOorschot:1996:DKA

Vedder:1998:SCR


REFERENCES


Wallace:1990:PRG


Wallich:1994:WP


Walton:1995:IAS

Walther:1998:VBE


Walker:1999:CCI


Wallich:1999:HSM


Walter:1999:MTI


Wen-Ai:1994:MTS

Wang:1986:UEA


Wang:1992:CDS


Wang:1992:DKT


Warren:1982:BTC


Ward:1998:ASE


Watler:1989:VAC


Watson:1999:DOC


Wayner:1991:TDL

Wayner:1993:CAS


Wayner:1993:ECD


Wayner:1993:SER


Wayner:1995:PCL


Wayner:1996:DCB


Wayner:1996:DLY


Wayner:1998:MJD

REFERENCES

Willcox:1992:TCS


Wagner:1994:PPR


Wolf:1995:ICR


Whittle:1999:SDC


Wallach:1997:ESA


Wu:1998:CRP


Wegman:1981:NHF

REFERENCES


Wang:1999:SCB


Wendling:1999:PRS


Weber:1993:MDC


Weber:1998:SWY


Webb:1999:UAO

Wedemeijer:1999:DFM


Wehde:1997:UGT


Wehde:1998:MBE


Wehde:1999:MSE


Weingarten:1983:CCP


Weiss:1988:BOP


Weissman:1991:IRA


Weissman:1991:IRN

Clark Weissman. Inside

Weierud:1994:SPB


Weierud:1998:C


Weierud:1999:TJG


Welchman:1982:HSS


Wells:1982:USE

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

Welchman:1986:PBB


Wells:1988:NAI


Welsh:1988:CC

Dominic Welsh. *Codes and cryptography*. Oxford

Welsh:1989:CC


Wells:1995:DEC


Welchman:1997:HSS


Werndorf:1993:OFG


Werndorf:1993:ORF


Worley:1994:PST

REFERENCES


REFERENCES


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

REFERENCES


for Data Internetworks, W. Stallings.


REFERENCES


REFERENCES

Winternitz:1984:SOH


Winterbotham:1989:US


Winterbotham:1991:US


Winton:1993:UPH


Winterbotham:1999:US


Wired:1998:REC


Wedel:1996:FSA


Watanabe:1997:SCR

H. Watanabe and T. Kasami. A secure code for recipient watermarking against conspiracy attacks by all users. In Han et al. [HOQ97], pages 413–423. CODEN LNCS629. ISBN 3-540-63696-X (softcover). ISSN
REFERENCES

Wechsler:1997:AVB

[WKHG97]

Whiting:1999:FOK

[WKS+99]

Woo:1992:ARC

[WL92a]

Woo:1992:ADS

[WL92c]

Woo:1992:CAD

[WL94]

Woo:1994:LAP

[WL99]

Wong:1999:DSF
Wagner:1985:PKC


Waldvogel:1993:PDD


Wheeler:1994:TCN


Wheeler:1995:TTE

Wheeler:1998:CX


Wright:1998:NTD


Woehr:1997:CRR


Wolfe:1943:FCCa


Wolfe:1943:FCCb


Wolfe:1943:FCCc


Wolfe:1970:SWC


Wolfe:1983:FCC


Wolfowicz:1993:SPR

REFERENCES

OF THE SYMPOSIUM ON
STATE AND PROGRESS
OF RESEARCH IN CRYPT-
TOGRAPHY 1993: 3rd. [ ],
Rome; Fondazione Ugo Bordoni, 1993.


[Wor96] Linda World. In the news: Intel and TI will enter 3D.

**Wotawa:1999:NDD**


**Waidner:1990:DCD**


**Wrixon:1989:CCS**


**Wright:1998:ECC**


**Wrixon:1998:CCO**


**Wright:1999:EAE**


**Williams:1979:SRC**


**Wagner:1996:ASPa**


**Wagner:1996:ASPb**


**Wiese:1996:SSS**


**Wagner:1997:ASP**

REFERENCES


REFERENCES


REFERENCES


**Wu:1992:GOC**


**Wu:1996:SNL**


**Williams:1979:CAA**


**Wah:1984:RAM**


**Westfeld:1998:SVC**

REFERENCES

0558/papers/1525/15250032.pdf.


[Xie92] Dong Qing Xie. Partially efficient computation and criteria of security for public key cryptosystems. Hunan Daxue Xuebao, 19(6):
REFERENCES

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


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

Xu:1998:STP

Yacobi:1999:RMC

Yacobi:1999:RME

Yahalom:COMPSYS-7-4-451

Yamamura:1998:PCU

Yamamura:1998:PKC

Yamamura:1999:FCU

Yan:1995:PTL
S. Y. Yan. Primality testing of large numbers in Maple. *Computers and Mathematics with Applications*, 29
REFERENCES


**Yao:1982:PSC**


**Yao:1982:TAT**


**Yao:1986:HGE**


**Yardley:1931:ABC**


**Yardley:1940:SSA**


**Yardley:1983:CBC**


**Yardley:1990:ABC**

Joshua:1998:VDW

Yeung:1997:DWH

Yeung:1998:DW

Yeun:1999:DSM

Yokokawa:1999:BDE

Yi:1996:DAN

Yin:1997:REA


Yen:1997:SAT


Ye:1999:CS


Yi:1997:NHF


Yi:1998:NBB


Yi:1998:NBO


REFERENCES


REFERENCES

Youssef:1995:RBB


Youssef:1995:RBS


Youssef:1996:CBN


Yu:1992:NTD


Yu:1994:KAX


Yu:XR-9-1-237


Yu:1999:CC


Yuan:1992:VLD

REFERENCES


Yung:1985:CSP


Yung:1985:SUK


Yuval:1997:RTE


Yang:1997:CBC


Yang:1999:GSP


Yu:1989:DEB

K. W. Yu and T. L. Yu. Data encryption based

**Yu:1991:SED**


**Young:1996:DSB**


**Young:1997:KUC**


**Young:1997:PKA**


**Young:1997:SEC**


Yeung:1998:DWS


Zafiropulo:1963:RAD


Zajacz:1997:SCE


Zang:1990:ESE


Zave:1999:SDC


Zegwaart:1993:PEM


Zeidler:1979:DDE

Howard M. Zeidler. Digital data encryption. SRI International, 333 Ravenswood Avenue, Menlo Park, CA
REFERENCES

94025-3493, USA, Tel: +1 415 859 6387, FAX: +1 415 859-6028, 1979. 20 pp. [ZFKP98]

Zergo:1996:UER


Zerovnik:1996:RC


Zollner:1998:MSS


Zuquete:1996:TAC


Zeng:1990:LSM


Zviran:1993:CPT

REFERENCES


Zhang:1991:BNK


Zha91

Zhao:1996:WSE


Zha96

Zhao:1997:LT


Zha97

Zheng:1990:PDS


Zh90

Zheng:1995:HBR


Zh95a

Zheng:1995:KAP


Zh95b

Zheng:1997:SC

Zheng:1997:DSH


Zheng:1994:RSS


Zilouchian:1998:ANF


Zhou:1994:SDS


Zieschang:1997:CPB

REFERENCES


Zhao:1995:ERL


Zhao:1996:DWS


Zhao:1998:GDW


Zhao:1998:BTT


Zhao:1999:DWW


Zeng:1997:RRO

Wenjun Zeng and Bede Liu. On resolving right-

Zhou:1999:SPP


Zhang:1999:AFV


Zheng:1990:CBC


Zheng:1991:DBT


Zolman:1993:BSJ


Zorpette:1987:BEC

Glenn Zorpette. Breaking the enemy’s code: British intelligence deciphered Germany’s top-secret military communications with Colossus, an
CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

[Zheng:1993:HOH]

[ZPS93]

[Zhu:1996:PKC]


[ZPY96]

[Zheng:1993:PAA]


[ZS93]

[Zheng:1993:HOH]


[ZTR99]


[Zukowski:1998:JTUa]


[Zukowski:1998:JTUb]

Nevenko Zunic. The MARS cipher — IBM submission to AES. In National Institute of Standards and ...
Zachariasen:1999:OAE


Zwiers:1998:CTD


Zeng:1990:LCT


Zeng:1991:ILS


Zeng:1991:PBG


Zhang:1995:GCG


Zhang:1996:DCC

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