A Bibliography of Publications on Cryptography:
1990–1999

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

31 January 2019
Version 1.102

Title word cross-reference

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

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

$1-Million [GC97]. 16 [BS93a, GC94]. 2
[JV98b, KG95, Kob91b, MVZ98, SBVG99].
$29.95 [Hat96]. 2n [QG90]. 2R [YLD99]. 3
[Ben99, BALS99, CK95, KSW97b, Nas94,
TK99, Wor96, YY99a]. 511 [CC98]. 64

/MMI97, 8 [Miy90]. <= [Zhe97b]. 2 [TZ94].
\( x \) [Hol91]. \( A \) [BMT96]. \( A * BN \) [Bak92]. \( A^2 \)
[JS95b]. mod2^a2 [Ber93]. c [WD99b]. \( \chi^2 \)
[HG97b]. d [BD99b]. \( \ell \) [BR91]. f [DJL93].
\( F_{2^n} \) [MVZ93]. \( F_{2^n} \) [SS98a, Ler97]. \( F_p \)
[Miy93a]. \( GD(2^n) \) [Ara93]. \( GF(2) \) [She95c].
\( GF(208) \) [Ros98a]. \( GF(2^{2^n}) \) [FBT96]. \( GF(p) \)
[Gor93b, HNN98]. \( \gg \) [GQQ91]. k
[Car97c, DJL93, HKS97a, HKS97b, KR99b,
KS97b, WD99b]. l [HL93a, KS97b]. L2
[Vau99a]. \( \lambda \) [RS99c]. \( L \geq 2 \) [SVxW91]. \( \ll \)
[GQQ91]. m [Bla94a, FR94]. \( N \)
[BS91e, BS91d, HKS97a, HKS97b, KSW99b,
KSW99c, KK98, Per93, QG90, Tak97].
\( N = p^4 \) [BDHG99a, BDHG99b]. \( N^{0.292} \)
[BD99b]. P [BS90b]. \( p^k \) [Tak98a, Tak98b].
\( r \) [BDHG99a, BDHG99b, FJRS96]. s
[YT95a, YT95b]. \( s^2 \) [Knu93b]. Step_k,m
[GC90]. \( t \) [KOO95b, KOO95a]. \( T^A P \)
[GPSV98]. \( y^2 + axy = x^3 \pmod n \) [Koy95].
z [MSS93]. \( Z/nZ \) [CLL99, MM96b]. \( Z_n \)
[ML98]. \( Z_n \)
[KMOV91, OFF93, VZ97, KK98, SE96].

-Adic [KG95, Tak97]. -Bit [QQ90, MM97].
-boxes [YT95a, YT95b]. -calculus [R99c].
-Cascades [GC90]. -Cheater
[KOO95b, KOO95a]. -Codes
[JS95b, MSS93]. -D [CK95, TK99].
-Decorrelation [Vau99a]. -Dependent
[DJL93]. -DES [Kmu93b]. -Dimensional
[Per93]. -divisibility [FR94]. -Fields
[BMT96]. -fold [BR91]. -formulae
[WD99b]. -Hash [BS91e, BS91d]. -means
[SBVG99]. -Round [BS93a, GC94].
-sequences [Bl99a]. -Span [HL93a].
-Tuples [FJR96]. -WAY [KSW97b].
-wheel [Car97c].

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

1 [Ano93k, CCN95, Nat95]. 1.0.1 [Sun91b].
1.2 [DDJ98e, DDJ98f, Zuk98a]. 10
[CMM93]. 101 [Hon98]. 1040 [Lin98a].
105-1
[Uni98a, Uni98b, Uni98g, Uni98j, Uni98i].
105-263 [Uni98i]. 105-322 [Uni98g].
105-415 [Uni98j]. 105th [Ano98f]. 10th
[Ano93d, CMM93, IEE94c, USE96a].
1113
[Lin98a]. 1186 [Riv90a]. 11th [SI93j].
120
[DLM94]. 128-Bit
[SKW98b, DKR97b, Knu98c, Lin98,
Luc98a, Luc99a, Luc99b, SKW98c].
12th
[Bri92, Bri93, KG96]. 130 [Ano96b].
1320
[Riv92a]. 1321 [Riv92b]. 1334 [LS92].
1395
[Uni94a]. 13th
[IEE97b, IEE97c, Sti93b, Sti94].
1409
[Bor93a]. 1411 [Bor93b]. 1412 [Ala93b].
1416 [Bor93c]. 1421 [Lin93a].
1446
[GM93a]. 14th [Des94b, KK99b].
15
[UU97b]. 1507 [Kau93].
1510 [KN93].
1511
[Lin93c]. 1544 [Ros93].
15th
[Cop95b, Cop95d, NIS92]. 16 [HB99]. 16-18
[Q+98]. 16-bit [Bro97].
160
BDP97, DBP96, PBD97. 16th
[Kooh6, MSD90]. 1704 [HA94a].
1731
[Mye94a]. 1734 [Mye94b]. 17th
[Hei96a, Kal97c]. 180 [Nat95].
180-1
[Ano95i, Nat95]. 1810 [Tom95].
182
[Dan95]. 1826 [Atk95a]. 1827 [Atk95b].
1828
[MS95c]. 1829 [KMS95a].
[1847]
[GMCF95]. 1851 [KMS95b].
[1852]
[MS95d, MS95e]. 1864 [MR95b]. 18th
[Kra98, Yua92].
1915 [Kae96].
1929 [Lee96].
194
[Uni94a]. 1940 [CWM*91]. 961
[McM96].
1964 [Lin96b].
[1968]
[Mey96].
1969
[SM96]. 1984 [IR96].
[1991]
[ASZ96].
1993
[ACM93b].
1994
[Ano94e, Sim96b, Uni95a].
1995
[Ame95, Dan95].
1995/4 [Dan95].
1996
[Ano95f, UU97b].
1997
[ACM97a, ANS97, Acc97, MZ98, Uni98a,
Uni98c, Uni98b, Uni98d, Uni98e, Uni98f,
Uni98g, Uni98i].
1998
[ANS98b, OiDP98, RD99a].
1999
[Wal99a].
19th
[Ano96a, Tv92, Wie99].
1B [Lea99].
1st
[ACM93a].
Win93, YL97b. Age [Bar94, SB97, Uni98i, Wal95, BS97b, Car97a, Joh98, Mar95b, Uni97c, Duh90]. Agencies [MKS99]. Agency [Gar97a]. Agent [BLH99, CF99, Cha90, COZ99, FK99, Lee99b, MM99b, PW99, PM99a, SJS98, VC99, CM99b, HJWT99]. Agent-Based [FK99, MM99b, SJS98]. Agent-Oriented [BLH99]. Agents [BGS98, FGS96, GB98, INDI99, Jun99, PW99, PWU99, RS98c, RS98d, SCT99, SSP90, Vig98, YY97c]. Agile [KLZL99, THP+98]. Agnes [Luj98a, Luj98b]. agnostic [JY96]. Agree [Gar97a, Ano97-27]. Agreement [BWM99a, Bor95, Bor96, Cae96b, Gar94, Gar97c, JV96, LM94b, LP99, Man93a, MW96a, Man97a, RSA93b, Van95a, Wol98, vOW96, BY93c, BY93b, HY98a, HY98a, LM94a, VW96, Zhe95a, Zhe95b, Wei99]. Agreements [MB99a]. Agricultural [Far93]. AH [MG98a, MG98b]. AI [Mas97, MPM99]. AL-STRATA [PMP99]. Aid [SBTV99]. Aided [BQ95b, BQ95a, HCY96a, LYH93, LL95a, MW98d, MDP94, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. Aids [Cra92]. AIR [Ano97r, DIF94, SVa+98]. AIR-BAG [Ano97r]. Airborne [CKN99]. AIX [Con93]. Ajat [GGH97a, NS98d, NS98e]. Alkerre [FS97a]. AKL [AP94]. Akta [Ano97-29]. AL [CM99d, CFK+91]. al-Khwārizmī [CFK+91]. Alan [Hod97]. Alarm [LKD98]. Albuquerque [IEE91]. aléatoire [Bou94]. Alek [Ssa92]. Alexandria [IEE94a, Man98]. Alf [Dob95b]. Alfred [Sha99a]. Algebra [BK94a, Pes97, VG99, CMM93]. Algebraic [Des98a, FL99a, Gog99, HR90, Kob98b, LW91, Mv93, Wat91, Ala97, BHHR99, CLW98, CMM93, HN94, JM96a, Sch91a, SH94, ZPY96]. Algebraic-Code [HR90, Mv93, Ala97, CLW98, SH94]. algebraic-geometric [JM96a]. ALGOL [RS99c]. Algorithm [ANS97, Ada97b, IBM93, Ano96e, ADEDS99, COP+95a, CD91, DKR97b, DNRS97, Dra98, GX99, GK98, GTG94, GN95c, HG97a, HG97b, HWJ98, Kal91, KY95a, KR96a, KY98, KMK99, Kob98c, Kra93, Kwa97, MD98, MW94, Mas94, Mat97, Mis97, MS90b, Mon99, Nat97b, PBG99, PRB99b, Riv92a, Riv92b, Riv95c, Riv95b, Riv98a, RC94a, RC94b, RH99, Sch93d, Sch94f, Sch95a, Sch95b, SKW+98a, Sch98g, SKW+99d, SHK+99a, SKW+99e, SS99c, She94b, SB98, SW93, Sta99b, Swa94, TK99, THP+98, VCR98, WHe94, Yin97, ZYR91, B194, BS94a, Bow93, CC98, CGV94, ISO97, IKNY98, JMLW94, KY95b, KY97, KYxx, Kir95, LRW93, LZ90, LZ91a, LL93b, Lon91, LC97b, MSS93, MPL99, Moh98, Pai96, Riv90a, Riv91b, Riv95d, Sch91a, Sch94i, Tay94, Vadv95, WN95, YL93, YL95b, ZW99, ZPS93]. Algorithm [AA95, Asc97, LL98, 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, GL98c, Gl98a, HEQ98, KM98a, KAK96, KB92, LC99, Lei99b, LD99, MT99b, PS97a, PA98a, PS93b, Por98, Pre97a, PRB98b, PRB98a, QG90, RS99a, Sch94g, Sch94j, Sch94c, Sch96a, SW97a, SW97b, Sch94h, Sed92, Sho97, Sot98, SB99, Sp95, Ste96, VCF+90, AA95, Ano90, CPP98, CMM93, CML+92, CadHSV96, DG96, DN95b, FR95a, GP97, HJ99, HP94, Imp92, KKL99, MS99c, OS91, OS92, PrO96, QN98a, Sch91b, Smi93a, Tab94, TY92, Tay90, TV94]. Alive [BK90]. All-Or-Nothing [Riv97c, Ste98b, BM99a, BMM99a, BOY99, SRY99]. Alleged [Go97d]. Alley [KR96a, PRB98b, Sch94f, Sch95a, Sch95b, Swa94]. Alliance [Gar97c]. allied [LPC98c, AK99]. ALM [CH99b].
Almost [AMP99, Bra95d, CCD99, Mau90].
along [BDC+95]. alphaf [Zim96a, Zim96b].
alphabet [PS97]. alternating
[HSW94, Wer93a, Wer93b]. Alternative
[BdM94, Gar97a, Neu94, Smi93b, VTV97, BR96b].
alternatives [FL93]. Alto
[ACM98a, IEE98a, IEE98b]. Always
[Bra95d, Cha99a]. am [LC95].
Amazing [GC97]. America
[HK99c]. American
[Acc97, Bur99, Gla99b, Joh95, Mor92, Moy98, RK98b, Web93, Yar90]. Amiga
[DDJ98c]. Among
[BDPR98, Sch92b, SS95a, SZZ95a]. amount
[Ped95]. Amplification
[ABDV98, BBCM95, MW97, CM95, Di 99, DJ99].
Amsterdam [Cha91]. Analog
[GS91, NT99]. Analogue
[Dem94, Cao99, SS95b, SS95c]. Analyses
[SMK98b, BDHJ97]. Analysis
[AO96, AMP94, BKS99, BR97a, BP98e, BS97a, BPR99, Bro94, CM97b, CJRR99a, CRRY99, CH99b, DD99, Dra98, FM98a, FY95b, GS97, Gue98b, Gis96, Kaa99, KS99, Kuu94b, KJJ99, L197a, Lei99b, Lvd98, MM99a, MT95, MDS99, MO99, NA95, Pai99a, PB99a, Pree93a, PJ99, Sch99k, Sha99b, She99a, SVB96, SW93, VN94, WS96a, WS96b, WS97, WB92, YMWP99, Y96, AA99, Abr97, Bar91, BCK98, BM95, Cha94b, Dan97, Don98, LM96, LLG10, Nas94, Pau99, PS98b, RS93, RS99b, Tha91, vT94].
Analyze [MOM91]. Analyzing
[Gil97, KAK96, NT93]. Anchoring
[CS99]. Ancient
[Paa93, RRRP97]. and/or
[Sim90b, Sim91]. ANFIS
[ZHJ98]. Angeles
[IEE98c]. Angiograms
[BAL99]. Angelo
[GL99b]. Anglo-American
[GL99b]. Anguilla
[Fra99, Hir97, Hir98]. Animated
[HE98]. animation
[HE98]. Ann
[Dob95b]. Anniversary
[CFK+91].
annotating
[DSSZ99]. Announcement
[Ano99b, Nat92b]. Announcements
[Ano95f, Ano95d, Ano95e, Ano97e, Ano97f, Ano97g, Ano98a, Ano94e]. Announces
[Got99, Ano97u]. Announcing
[Ano97h, Nat97b]. Annual
[ACM94a, ACM97b, Ano95l, Bri92, Bri93, CH96, Cop95b, Cop95d, IEE92b, IEE93c, IEE94b, IEE94c, IEE94f, IEE96a, IEE97b, IEE97i, IEE98a, IEE98f, IEE99a, Kra98, Spi95, Sti93b, Sti94, USE99d, ACM90, ACM91, ACM93b, ACM94e, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, IEE92d, IEE95c, IEE97i, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, Wie99]. anomalous
[GLV99]. Anonymity
[BD99a, DFTY97, FJ98, JMP+98, STS99b]. Anonymous
[DF98, DF99, FT99b, GGM97, Jae96, Jue99, MS99a, OKST97, PW97a, RSG98, STS99a, SP99, SGR97, Pfi95]. Anonymously
[Coh96]. ANSI
[Ano94b, Ano96c, Bak92, Bas98, BK98a, BK98b, Joh99, SS97]. Answer
[WD99a, Ude98]. answers
[Di 97a, Fre94, Ano92a]. Ant [BP95a]. Anti
[Ano93a]. Anti-counterfeit
[Ano93a]. Antique
[Mer90b]. antitrust
[Ano97q]. Antivirus
[Nac97]. Antonio
[ACM99a, IEE92b, USE98d]. Any
[BM92, BJY97, DDP90, FJM+96, ZMI90, Beu94, DF93, DKKK98, DJ99, HILL99, Pet98]. anyone
[Ude98]. AOL
[GC97]. Apache
[Bal99, Mec98]. aperiodic
[Fri92b]. API
[Gar98b, Got99, Lin96b, Mc96]. APIs
[Gol96c, Gou98]. App
[AW99]. Apparatus
[SKBx99, MY98]. Apple
[Gar97a, GO96c]. Applet
[Ber97a]. applets
[GPO98a, GPO98b]. Appliances
[Got99]. Applicability
[KCCT94a, KCCT94b, HKM95]. Application
[IBM93, BS99a, BS95, Bar99, BGG95, BL96b, BL96a, Dam90a, Dam91a, Dav91, De 95, ECM96, FJR96, Fun97, GPT91a, GPT91b, Gog99, GQ95, HNS999, HH93, Hat97, He94, Ho99, IR93, IR99.
JDK⁺91, KMPS99, KP99a, KL96, KK95, LOX99, LCN99, Mar98a, Man96b, Mun91a, Mun91b, NC97, PSN95b, QV90, QG95, Rog95, Rue93, SSS98, Sch99, SZ93, SK98c, SK98b, SKIT99, VDDR99, Ara93, BY93c, BY93b, CC98, DDB95a, DDB95b, DF97, GZ91, HL97b, MW94, Nyb98, Pet91, PKM97, SI93b, SRR98, Siu99, Ste99b, SW98, SW99a, TY92, Wuo90.

**Applications** [Aga92, BGR98a, BFW99, CG98, CJR98a, CJR98b, CG93, COZ99, Cre90, Dan96, DY91a, DFGH99, Duf98, DN94, Dwo97, Ebe93, FMM99, Far93, Fis98, IEE95a, IEE97a, IEE92b, IEE94c, IEE97b, JMSI96, KSHW97, KSHW98, KSW99b, KSW99c, KM96a, Km94b, KT91b, Lan97, MS95f, OiDP98, OO90, PS96b, SY96a, DY91c, TN96a, TN96b, VV98, VV96, ZYR91, vW94, vW99, ACM99c, Ada91, Ano98b, BM90, Ber93, BMP⁺97b, BV97, Boy98, BP97b, Com96, CFG96, DiDP96, Dix94, Dom96, Eng99, FO98, GvP98, Gre94, GS94b, HMP95, JV98a, Kala95, KW92, KG93, LY93, LN94, Lub96, Meif92, Mie97, MT98, NKC94, Ped91a, PC98, Rh95, Sch90c, Sch97c, Sha95a, SSM94, Sin95, Sta97c, SSC99, T⁺98, USE96e, Way98, YL93, ZYR90]. Applied [BJHM99, HH98, MR95a, Sch94h, Sha99a, FFW99, FM99, MVV97, PR98, CMM93, Dav94].

**Applied** [BHJM99, HH98, MR95a, Sch94g, Sch96a, Sha99a, FFW99, FMR99, MVV97, PR98, CMM93, Dav94].

**Applying** [CO98, HO96, Jan99, KMPS99, MW98a, War98, ARR99].

**Appraisal** [FGS96].


**Approaches** [CJR99a, GFB93, Man91a, RDK98, VP93, ZS93]. Approves [Gar98b].

**approximate** [MW94].

**Approximating** [SG95]. Approximation [KG95, LR99b, MII96a, RS99a, CS97d, Gol96a, Nyb95]. Approximations [KR94b, ST91, KR95a, KR96c]. April [ACM97a, Ano95c, Ano99c, Auc98, Chr98, Ch99b, Dav91, IEE95c, IEE97d, IEE98d, KK99b, Lon97, QV90]. Aquarelle [ADF98].

**Arab** [AK98]. Arbiter [DY91f, JS95b, JS95a]. arbitrary [Pie93].

**Arbitrated** [DY91f, HW98c]. Arbitration [Joh94, Kur94, PLWSN99, DS93, K905b].

Arcane [B94]. Archaeological [Ano97t].

**Architecture** [IBM93, BCCD99, CJR98a, CJR98b, Con99a, Fei93, Fei96, Gut99, JDK⁺91, MM99b, Muf93, NH90, NK98b, Oh99, PF94, RBv94, Rus90, SS90, She92a, She93c, Tre99, Tua99, VG93, YS99, Kar96, LS98a, Con98, JD91, LMJ93, SV99, SY92].

**Architectures** [B99, CN99, FS99, P99].

Area [Fum93, LE99, Van95b]. areas [TM99].

aren’t [Cha99a]. Arguments [BJY97, BD91, NOV93]. Arias [DHMR96].

arising [APD93]. Arithmetic [BP98a, Bre99, BP97c, Bus97, CD98b, DBVD96, KK99b, LL99, LD99, Mih94, NM96a, PR97, SSS98, SL93, CPP98, ISO97, JS93a, Kal92, Kal93b, KM99a, Pos93].

**Arithmetically** [De 98d]. Arizona [IEE99b].

Army [Mea98, Mye98, Dav98a, DR99b, Ros99].

**Arnoldi** [HRV99]. Array [MT95, DF92].

**Arrays** [BG94, BG96, BKK98, MT95, TT99, JM93].

**Assuming** [Mad92]. arsenal [Me98].

**Art** [Eri99, Lan98, NM96a, Pre98c, She92e, BFS92a, BFS92b, Ben94, B⁺96b, PGV93d, PR98].

article [Bur98b].

Artificial [Ano96l, SBTV99].

Asia [Uni98c]. ASIACRYPT [IRM93, KM96a, PSN95b, PSN95a].
Asimov [CFK+91]. asking [MILY93].
Aspect [LL99]. Aspects [Des98c, Sch98b, Ved93, ZTR99, Kob98b, Lid90, Pos98].
Aspray [CFK+91]. Assessment [Hwa97, RH99, GPSN97]. Assessment [EN98, ENK99, FL93].
asset [Oko97]. assign [LL93b]. Assignment [Hwa97, RH99, GPSN97]. Assistance [IS91, HY93a, Wu92].
Assumption [Sak96, Sal98]. Assumptions [AB99a, AB99b, BD91, KRS99, Lid90, Pos98].
Assurance [IEE94b, IEE96d, KYG92]. Assurance [Car95]. ASTRAL [Dan97].
Asymmetric [BWM98, FO99b, Jak99c, LM96b, Pat96, PG97a, PG97b, PS96a, PW97b, The95, BR94b, BR95a, MI90].
Asymptotic [SOB98]. Asynchronous [AMP99, TY94].
Auditability [VNW95]. Auditable [STS99a]. Auditing [SK97c]. auditorialization [HW91]. Auditorium [IEE98b]. Aufenthalsorts [FT95].
Augmented [BDT98, KT98]. August [B+96b, Bri92, Bri93, BS95e, Cop95b, Cop95d, Des94b, IE98b, Kaly97c, Kob96, KP99b, Kra98, MSD90, Nat98, RD99a, Sti93b, Sti94, TM99, USE90, USE98a, USE98b, USE99a, Wie99, Yua92].
AUSCRYPT [SP90, SZ93]. Austin [Ano94d, IE98e]. Australasian [VPM97]. Australia [DG96, GN95b, KG93, KK99b, MSD90, PSN95b, SP90, SZ93, VPM97].
Austrian [CFK+91, GN95b, Cae96a, Orl96]. Austria [BS95e]. Authenticating [BF97a, BWM98, BM99a, Box95, CH97, Dan95, HC97b, Jv96, LC97a, Mau97a, RH93, SKWH96, BSN96a, BSN96b, BF99b, BR97b, Dv992, HY98b, HY98c, Ye99].
Authentication [ADS99, He98a, KS99a, Mitt92a, SK96a, LC94].
Authentication [Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Mau96a, MAM95, McM96, MS95c, MS95d, MWW94, MTVZ92, Mor97, Mye94a, Mye97, NP97, OOK91, OM94, Opp96, PKOT94, PS98c, PLWSN99, PSN91, PGV93c, Pre98a, Pre98c, MS95e, RS99b, RRSW97a, RRSW97b, Rog95, SNT93, SN93, ST94, SNT95, SN98a, SN98b, SSH93, SS96, SPH99, SA95, SC96a, SCxx, Sch94d, Sch99k, Sgo90, Sgo91b, She97, She95a, Sho96, Sim96b, SVxW91, SW94c, SKAM99, Sti91b, SL99, TAP90, Tay95, TSN93, Tun99, Ude98, Van95b, Van93, Wai95, WKHG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC+98, Ano97d, Atk93, BSN97, BGR95, BCK98, BCKx, BC97, BGH+95a, BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gua90, HS96b, Hor95].

autentication [HC95b, HLL+95, HW98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin89a, Low95, MS97, MF97, Men91, MC96, Nac93, NT94, PS98e, PS98f, PS98h, RS98a, RS98f, Sch99], Sga91a, Sga93, SY96b, Sta99b, Sti91a, Sun98b, Syv93, Ts92b, Ts92a, TH99, Ver98b, WL94, XA98, Xie98, YL97a, YL97b, You97, Zuk98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a].

Authentications [OO90, KSL92].

Authenticator [Zuk98a].

Authenticators [DF91a, SN96].

Authenticity [BK90, Lud97, Ml90, Way91].

Authenticon [Fly97].

author [Lea90].

authorisation [COZ99].

Authorities [Ame95, Ame96a].

Authority [CFSY96, CGS97, JMO95a].

Authorization [BDPSNG95, Cas95, FL96, Woo90].

Auto [YY98c, YY99b].

auto-certifiable [YY98c].

Auto-Recoverable [YY99b, YY98c].


Automated [Dan97, FIP93a, FN93, FK99, GSN94, GDS91, She96a, GGPV98, VD999, DG99, CD98a].

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

Automating [Bf99, Sm93a].

Automaton [Des99a].

Automaton [DvG93, Gys96, DW96, MZI98, Tao94, TCC97, TC99b].

Automorphisms [VP96].

Autonomous [CKN99, RZ99].

autoscritcher [Dea98a, CF92, Cra92].

aux [Bec90].

Available [DJ98c].

Avalanche [Cas96, CS96c, IHT95, O'C94, ZKG95, SZZ94a, SZZ95b, YT96].

avan [Blo98a].

AVBPA [BCB97].

Average [DLP93, KB99].

average-case [AD97, AD99].

Avoided [NMR95].

avoiding [ZW99].

Award [Pin98].

Awarded [DJ98b].

Awards [Eri97a].

Aware [BCCD99].

Away [DJ99].

Axis [AK99].

AXYTRANS [GBC93].

azo [SBTV99].

b [Cly97, UU97b, Ano99e, HS90, Lam99].

B-Trees [HS90].

ba [IPndbbbrm91].
Babbage [Fra93]. Back [GC97, GO96c, WSFC99, IEE97e, WG97].
Bal [IPNdbbbprm91]. Balance [RG99].
balance [MD98b, Y95a, Y95b]. Balatonfured [Rue93]. Ballot [CFSY96, BT94]. Ballots [Sal91].
Baltimore [ACM90, Ano96a, NIS92, USE92b]. Ban [Gar97a, BP98f, XZZ97]. BAN-like [XZZ97].
Bandwidth [Bl96a, Bl96b, JM98, Sim98b]. Bandwidth-Efficient [JM98]. Banking [Ch92].
Barbara [Bri92, Bri93, Cop95b, Cop95d, Cre97, DGV93, Da95, IE98d, Kal97c, Koh96, Sti93b, Sti94, Wie99].
Bargaining [Nur94]. Barrier [BG99].
Barriers [Des92, RCM99]. Based [AW94, ADEDS99, BDPSN95, BG90, BJ97, BS99b, BS99c, Ben99, BLM94, BBT94, BMT96, Bie98, BPR99, BMS94, BM96b, BM96c, Ble98a, BPRF99, Bola98, Bola98, Bra95b, BP97c, CC99b, CJ98a, Cre97, DGV93, Da95, IE98d, Kal97c, Koh96, Kra98, Sti93b, Sti94, Wie99].
Bases [BCE94, MSDS90, Yua92]. Basic [CF99, Des98a, vdL98, OK98, YHKI99, Zie97, van98, BD97, Rac90, dVdV98, Hel98b].
Batch [BGR98a, BY93c, BY93b, BFP99, Fia90, Fia97, BGR98b, Y95a]. Battle [Ban93, Gar97a, Gar97b, Gar98b, SB97, Fro96].
battleships [Jar97]. Bayesian [BBDF97, Jen99]. BCH [CC98, FC94].
Be [BF99a, BV98c, Cha93, CD98b, DY91f, Ev91, GS99, NM95, Way93c, Ano90, Ano95c, Ano98b, CP91, Cs95, Ev92, Ev93, LF97, NMVR95a, NMVR95b, NOV93, Ros98c, Sch91b, Sim98c, van97a]. Beach
YLCY98b, CFK\textsuperscript{+91}. **Byte-Oriented** [Mas94, YLCY98a, YLCY98b]. **Bytes** [Yuv97]. **Byzantine** [Bea92, Bor95].

C [Sha99a, vdWS97, vS97, Bak92, Bas98, BMS99, DS99, Gar98b, Gel98b, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **CYNTIIA** [WBB99].

**C** [Sha99a, vS97, BS99, BB98, DH99, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **Byzantine** [Bea92, Bor95].

C [Sha99a, vS97, Bak92, Bas98, BMS99, DS99, Gar98b, Gel98b, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **CYNTIIA** [WBB99].

**C** [Sha99a, vS97, BS99, BB98, DH99, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **Byzantine** [Bea92, Bor95].

C [Sha99a, vS97, Bak92, Bas98, BMS99, DS99, Gar98b, Gel98b, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **CYNTIIA** [WBB99].

**C** [Sha99a, vS97, BS99, BB98, DH99, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **Byzantine** [Bea92, Bor95].

C [Sha99a, vS97, Bak92, Bas98, BMS99, DS99, Gar98b, Gel98b, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **CYNTIIA** [WBB99].

**C** [Sha99a, vS97, BS99, BB98, DH99, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **Byzantine** [Bea92, Bor95].

C [Sha99a, vS97, Bak92, Bas98, BMS99, DS99, Gar98b, Gel98b, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **CYNTIIA** [WBB99].

**C** [Sha99a, vS97, BS99, BB98, DH99, Kaj92, MGL\textsuperscript{+98}, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b]. **Byzantine** [Bea92, Bor95].
Checkers [Fis97, KA91]. Checking [BGR98a, Bol98a, Bol98b, BDL97, FL99b, FGY96a, GMV98, PV98, BCR98, FGY96b, MHPS96, MW94]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93]. Chen [Ala97, Bur94a, Bur94b]. CHES [KP99b]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93]. Chen [Ala97, Bur94a, Bur94b]. CHES [KP99b]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [PBGV90, LRW93].
Classes [Haw98b, Pai99d, Haw98a, Sze98].
Classical [Bra94a, MC92, Nic98a, Nic98b, CD98a, Mas99a]. Classification [BD90, LSVV95, PNFK95, Uni96c].
Click [WSFC99, Ken95]. Client [DL99, Kon95, Oh99, SL99, GGK+99, Sin95].
Climate [TGKI99]. Climbing [MCD99].
Clipper [Pri94, Fro96, Ban94, Bro96, Hof93, Kan96, MS95f, RKD94, Smi94a, Uni95a].
Clipper-like [MS95f]. Clipping [Hof93].
cliques [JP96]. Cloak [Gre90]. Clock [DHSS95, GM91, G095, GO95, Men95b]. Clock-Controlled [GO95b, GM91, GO95].
Clocks [DG95, DGT96, Yah94, Gon92]. Closer [Coh96]. Closure [MOM91, PS93a].
Clueless [RS98c, RS98d]. Clustering [DDJ98a, HE98, Kum97].
CM [CNST98, Kob91a]. CM-curves [Kob91a].
CMOS [BS95c, ECD+99, YSS99]. Co [Gla99b, LFCK99, Sut99, NM96a].
co-processors [NM96a]. Co. [CFK+91].
Coast [SZ93]. COBOL [Car97c]. Code [CJ99, H090, J09a, Kip99a, Kuru94, MV93, PV98, QD91, Sch94g, Sch96a, Sch94h, Str95, Tod97, WK79, WF94, Zim95b, Ala97, Ano97i, BSNP97, CC98, CLW98, GA98, HM97b, LJWh97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG+00, Mea98].
Codebreaking [Car97c, Car98, Dre92, Sch98a]. coded [HG97c]. codemaker [Mar98b]. CODER [Sto90]. Codes [ACM94b, AW94, AR98, BGS96, BVFD99, CCZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, Gib91, Hof99, Joh94, JS95b, J99b, KS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWS99].
Pen96, Pra96, Pre98a, RV99, Rus93a, SN93, SNW98a, SNW98b, SD99, Sga90, Sga91b, SB94, SVx99, STA96b, Sti91b, Ton96, Van95b, Wt98, Ada91, Ah93a, AW95, BSB97, BI93, Bu91, CC98, Cha95a, CMM93, FC94, Gre90, JM96a, Kah91a, K095b, LYG94, LMS90, MSS93, MPL99, Moh92, SNT93, SNT95, SK94, Ste95, Sti91a, Su98, SS98b, TSN93, TY94, W9n92a, Wel97, Win93, YL97a, vT94, JS95a].
codewords [PS97]. Coding [Ber96b, IEE97e, KRS99, KH98b, LW91, Lip94, Sch99b, She94c, SW95b, Van95b, WA99a, Ada91, Boy95a, Boy95b, Dar97, DDP97, Far93, Gan93, KSB96b, KSB97, Kuo90, Mit92b, Sah94, Sch98b, Sga91a, SVWM95, SOB98, Shp99a, SMS99, TA97, Ger97].
coefficient [GM95b]. Co-processor [PS97].
coefficient [OG96b, HE98, Kum97].
Collision [BP97a, Dob97, PGV91, RU93b, Vau93, V9W4, V9W9, Dob95a].
Collision-Free [BP97a, Dob97, RU93b, Vau93, Dob95a].
Collisionful [Son95, BSNP96a, BSNP96b].
Collisions [Ano95a, C98, DBGV93, DB94, Gon95, Sim98c].
Colloquium [Ano97b, vWN99]. Collusion [BP97a, BS95b, BKK99, PW97b, LM96].
Collusion-Resistant [EK99].
Collusion-Secure [BS95b, BS98]. Colony [BP95a]. Color [ADEDS99, NNIKE97].
Colorado [Sch99b]. Colossus [Ano97b, Car97b, Car97c, Car98, Pin98].
Column
[Bra94a, Dwo95, Bra90b, Bra90d, Bra95d].
columnar [Bar92a]. COMANDOS
[TCH+91]. Combatting [DN93].
combination [Rev91]. combinational
[Hil94]. combinations [RT93].
Combinator [SAS99b]. Combinatorial
[FK94, KO95b, KO95a, KO96, KO97, LS98b, Rus93a, Sti91a, Zie97, FSS94, Sta97a].
Combinatorics [TCH94]. Combinatorial
[FK94, KO95b, KO95a, KO96, KO97, LS98b, Rus93a, Sti91a, Zie97, FSS94, Sta97a].

Commentary
[Ano99a]. Commentary
[BL99]. Comments [BMP99, COP99a, Din94, JW01, KSS99a, MC96, NC97, Ng99, Pre95b, SB93, WHL99, Al97, Gib90].

Commentaries
[Ano99a]. Commentary
[Ma99a]. Comments [BMP99, COP99a, Din94, JW01, KSS99a, MC96, NC97, Ng99, Pre95b, SB93, WHL99, Al97, Gib90].

Commercial
[DDJ98d, DB99, Jak99b, LHB96, Lu98, USE95c, USE96d, USE96d, USE98b, Un97d, BH98, FB97, Gar97b, LM98a, Ma95, Sin98, Tas98, VM96, UU97b, Un96c].

Commercially
[IBM93, Lin93c, Mau93a, Tze99, JD91, JDI97, LIM93].

Communications
[ACM93a, ACM94a, ACM97a, Ano93b, Aur96, IEE94f, IEE97k, KM93, Kat97, MB94b, Ved93, BY93c, BY93a, Car94, Cha94b, Cra96, HOQ97, Hwa93, IEE92d, IEE95c, JC93, Mil95, Oht96, PP96, Rhe94, SW94b, Sch93a, Sch92c, ZG96].

Communicators
[Ano99a]. Communities
[MB99a]. Commutative
[GTP91a, GTP91d]. compact
[Ort95b, Ort95a]. companion [Ken95].

Company
[GC97, Kar96]. Comparative
[DAe99, Ste92, AA99, Don98, She92a].

Comparing
[Bih99c, HSS99, HKL94, KAK96, NM96b].

Comparison
[BALS99, Cus97, LH99b, LM98b, Mas99a, May97, MG91, vO91a, QN98a, SKW99b, SKW99c, Wle98b, Wle99b, vO91b, GM91, Yeu99, ZH93, vO92].

Comparisons
[Fol99, SKW99c].

Compressed
[CPO98, CHO98, HG96, HG97c, HG98].

Compression
[GI99].

Compromise
[Gar97a, Hed97].
CompuServe [GC97]. computability [BK98f]. Computable [DSV99].

Computation [BMM99a, BMM99b, CH98, Cra99, FH94, GM93b, HHT93, HHT97, HCY96a, KR94c, LO91a, LYH93, LL95a, Mon93, Mor98, PK95a, PK95b, SSN98a, Wat91, ARR99, Ata99, BHKR95, BM94c, CL97a, GM95, Hor98, LY93, MILY93, PW93a, Shp99a, Xie92].

Computable [BK98f]. 

Computationally [WP90].

Computational [CH96, HKL94, Kos97, KRS99, PG90, Sab94, TGKI99, BC95a, Ger99b, McC90b, Pom90a, SS95a].

Computations [Cha90, CDD99, Mas91].

Computed [Ev92, EvH93].

Computer [ACM93a, ACM94a, ACM97a, An93d, An97-29, An98b, Bac95, BK90, Ber96b, Bre99, CWM91, CO98, De98a, De93b, De98c, DQ93, Des92, DEQ92, FJM96, GMV98, HM91, HM92, Hig97a, Hig97b, Hor94, IEE92a, IEE92b, IEE92c, IEE93b, IEE93c, IEE94b, IEE94c, IEE94d, IEE94f, IE96a, IE96c, IE97b, IEE98a, IEE99a, K99b, LBMC94, LC95, MDP94, NIS92, Nac97, Neu92, OD99, PGV93d, Q98, Sal91, SSS98, SK96a, SK99, Sho97, Ste91, SI93, VGP93, Ver98a, VG99, Wli90, AFB95, An93k, AC97, Bur98a, Car97c, Car98, CW91a, Coh94, GBL94, Gr98, HLL95c, IEE92d, IEE95c, Joh98, LS98a, LFSY94, LC96b, LC96c, NT94, Nis91, Pr98, Ris98c, Shp99a, UFC94, Wil93a, Woe97, Woo90].

Computer-Related [De93b, De98c].

Computerized [B91]. Computers [??97, BF99a, CWM+91, HM96, Kan96, Sch98c, CFK+91]. Computing [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98a, ACM98b, ACM99b, Bak92, BDDG99, BV96, Bra94a, CFK+91, DDJ98d, DDJ98b, DDJ99, Dwo95, FP99, GC98, GN95b, IE94e, IE96b, J98b, Kon95, Law98, MMM+98, Mau94, MW99, NS98a, Pen96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b, BGT96, CWM+91, DiDPS96, FM91, FJV97, HK99b, HC95a, KG93, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK+91, PH91].


Concept [Lin98, GM91, HLC99, YKY99].


Concerning [Cle91, Hub91, FR94, Fri96, GHS93, Gro94, Sim98].

Conciliation [BBDF97]. Concrete [OO98, BCK96c, BDJR97]. Concurrency [SG99b, IEE94b]. Concurrent [BMT98, DO99, DS98b, RS98, Zwi98, AR99].

condition [Sta96b]. Conditional [DOR99, G99a, KS97a, KG99].

conditionally [Des90b]. Conditions [GS99a, Rus93b, Gu99].

Conducts [Law98].

Conference [ACM93a, ACM94a, ACM97a, AR97, An95, An96, An96a, ??97, An97f, An97g, An97a, An98a, An99a, AA97, BCB97, Boy95a, Bri92, Bri93, BS95, CH96, Cha91, Cop95d, DDJ98a, Dan96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, Hir97, Hir98, IEE95a, IEE97a, IEE92b, IEE93c, IEE94b, IEE94c, IEE94e, IEE96b, IEE96c, IEE97b, IEE97c, IEE97h, IEE97g, IEE97d, IEE97l, IEE97j, IEE97k, IEE98c, IEE98f, IEE98e. IRM93, KG96, Kat97, KM96a, Kra98, LOX99, LP99, Mau96b, MDS90, NIS92, Nat98, Nat99b, Nyb98, OW95, OD99b, PSN95b, QA95, RD99a, RD99b, Sch94m, SJ97, SI93, St93b, St94, T98, USE91, USE92a, USE94, USE95a, USE96a, USE99b, USE99c, Wa99a, Wu92, ACM99c, An93d, Boy95b, BD95b, Cop95b, Dar97, DG96, Des94b, HO97, HI97, IEE92d, IEE95c, IEE96f].

conference [IE98b, Kal97c, KG93, Kob96, LM98a, SP90, Ste99b, USE96f, USE98c, USE98d, VPM97, Wie99, An95f].

Conferences
[BDHK93, MZ98, Sch95f]. Conferencing [Ano96e, KQRS97, WW98a, Lam99].
confidence [Chii99a, Chii99b, Grax].
confident [Jan95]. Confidential
[Bet95b, Bet95a, vD97]. Confidentiality
[Ano98j, Jac96, Riv98d, ZG96, FT95, MI90].
Configurable [VMS97b, VMS97a].
configuration [HI97]. Confermer
[Oka94, Cha95b, MS98b]. conflict [All97].
Conflicts [ACM94b]. confounder [BTD98].
confrontation [Zaj97]. Confusion [GC97].
Conflicts [ACM94b]. confounder [BTD98].
confrontation [Zaj97]. Confusion [GC97].
Cong [Mye98]. Congressional
[Smi97a, UU97a]. congruence [Sch91a].
Congruential [Kra90], conic
[Cao99, Mra95]. Conjecture
[Jia99, GHS93, Ill94]. Conjectures [KP95].
Connect [Lic94]. Connection
[Kit96, CV99]. Connections
[RSG98, SGR97, Yu94a, Yu94b].
Connectivity [Pie96b]. Consequences
[Kit95, Sim94a]. Conservation [Bro94].
Considerations [Cra96, Hub91, Mos98,
Bas95, Bou94, SY92, YSS99, Bou94].
Considered [LT91]. Considering [HH94].
Considers [Ano95]. consistency [Zyr90].
Conspiracy [WK97, Sch92].
Constitutional [Bas95]. Constrained
[Gol96b, Has99]. Constraint
[SG95, WS99, GMLH94]. Constraint-Based [WS99]. Constraints
[DS98b, Ou99, Koz96]. construct
[Lon92, Sun91a, ZH98]. Constructed
[Rus93a]. Constructing
[Ada97, AB99a, AB99b, DT93, Gai99,
KTM+99, Koh91b, XL98, Z996].
Construction [BCK96c, BR99a, BR99b,
CNST98, vD95a, DS99, EM93, GSPSW98,
Joh94, Kim93, KYDB98, NR98, SVW91,
ZMI90, BCK96a, BCK96b, BCK96c, B193,
MPL99, OS91, OS92, Pet91, vD95].
Constructions [AHV98, ABDS96, KRS99,
SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE98c]. contactless
[DS98a]. contain [Lea90]. Contemporary
[Kmu99b, Sim92]. Content
[Ack98, JPLI99, KR98, MW98b, MR95b,
PMP99, Ros93, SC96a, Way93a, SNT95].
Content-Addressable [Way93a].
Content-Based [PMP99]. Content-MD5
[MR95b, Ros93]. Contents [vHH97].
Contest [DDJ98a, EMNN98, HD99].
Context
[COZ99, MM96a, Des90b, Des90a, Ill94].
Context-Based [MM96a]. context-free
[Ill94]. Continue [Ano96k]. Continued
[KE97]. Continues
[Ano97, Ano97, Ano98d, DDJ98d, Ano96].
Continuous [BP95a, NHB98, She95a].
Contours [LFCK99]. Contract
[GJM99a, GJM99b, KHB99]. Contractor
[KHB99]. Contracts [Ped99]. Contrast
[KHS97a, KHS97b]. Contrast-Optimal
[KHS97a, KHS97b]. Contribution
[Lud97, Mus92, SS97, AK98, Blo98].
contributions [Hil94]. Control
[ABL93, Ban93, BDPSN97, DFTY97,
FY99, FL96, Hwa97, JPLI99, Kas96, KA99,
KKW99, Lin98, Mey96, NW98, NA99,
NS98a, PRAM98, Per99, STS99b, She93a,
She93b, Sim90b, Sim91, ZH98, ACC99,
Ano93d, BGT96, CWM+91, CS96b, CS97b,
CW94, LL93b, LM93c, Mat91, MLA91,
RO96, RT93, SS96, Uni97d, WW95].
Controllable [CTT94]. Controlled
[GPR98, GO96b, Goli94, Jak99c, SKBxx,
GM91, GO95, Men95b]. Controller
[CIBM99, FCH99]. Controls
[Ame96b, Ban94, Cil97, UU97b].
Controversy [Law98]. Convention
[Ano94d, Ano96a, Ano98, IEE96f, NIS92].
Conventional [PRB98a]. Convergence
[GC97, Mos98]. Conversation [Woe97].
Conversational [LTEH99]. conversion
[Sab94]. Convert [Pet98]. Convertible
[BCDP91, DP96]. Convolutional
[Cha99c, JJ99b, TY94]. Cool [Ano99c].
Cooperative [Oh99]. Coordinating
[Lee99b]. Coordination [COZ99, FL99a].
Vau98c, Vv97, Ver95, WSK97a, WSK97b, WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Wie90, Wie90b, Wie90a, WBDY98, YLD99, YLH98, ZYR91, Ada92, Alv98b, BSN95, BB94, Ber93, BS90a, BS91e, BS91f, Bih92, Bih95b, Bih98b, BK98e, Bir99, BD95a, Bowxx, Bur98a, CV95, CD98a, Cra92, DYL98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, Gol95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kah98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LS98a, Lew92, Mat93, Mil96, Mil92, Moh92, Mor92, NS97c, cryptanalysis [O’C95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZYR90, ZH90].
cryptanalyst [Rey96, Rey97, Rey99].
cryptanalytic [Gla99b, KSWH98d, MG91, vW99, Bih94a].
cryptic [Wri98].
cRYPTO [Fei91, ACM94b, Ame96b, And96a, Bar93a, Bar93b, BE90, HP98a, HMvT94, Koo97, LKB+94, Mah96, MPPS95, Neu97, Sch98c, Way95, Way96b, Neu95, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol98b, Kal97c, Kob96, Kra98, MZ98, MV91, Sti93b, Sti94, Wie99, BC98, Bra98, Bri98, CP91, CR98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, Sti98a, Wil98b].
Crypto-Chip [HMvT94].
Crypto-Coprocessors [HP98a].
Crypto-Engine [BE90].
Crypto’91 [DBGV93].
Cryptography [Har94, Web93].
Cryptographers [WP90].
Cryptographic [AG98a, AG98b, IBM93, Ano96f, AB97, BDPSNG95, BDPSNG97, BH93, BY93a, BGM97a, BGM97b, BBT94, BMT96, BFKL94, Bol98a, Bol98b, BDL07, BDP97, Bra95a, Bra96, BD91, CS96a, CJR98a, CJR98b, CPOR97, CF95, CD99, Cop94b, Cre97, DG9V2, DC98a, Dam90a, Dam91a, Dan95, DIF94, DY90, DY91a, DY91d, DY91b, De 95, DS97a, DF91c, DK91, ECD+99, EL98, FGR92, Fis98, FGY96a, Fun97, GI99, GS94a, GK99a, Gol96c, GS97, GQ95, Gut99, HHT93, HHT97, Hel94, Hwa97, IH96, Ive91, JDK+91, JD91, KM98a, Kalh8f, Kal98d, KV94, KS99, Kha93, KP99b, KT91b, KT98, KS97b, LMJW93, LL97a, LHB96, LM96, Mac94, MM99a, Mau96b, Mau97b, MS90a, Mil96b, Mjo93, Mos98, Mun91a, Mun91b, NM96b, Ng99, NS99b, NR94, NK98b, Nur94, Nys99, OPH+99].
Cryptographic [Oka93a, OS98, PS99d, PV97, PS96b, PBGV90, Pre93a, PGV93a, Pre93b, Pre94a, PBD97, PRB98b, Pre98c, PRB98a, Pre99, Pre94b, QV90, QG95, RSA93d, RS93, Ritxx, Rue93, SI94, SZ96, Sak96, DY91c, Sch95f, SK96a, Sch98d, SK98a, Sch91c, Sch93f, SPS97, SZ93, SZ95c, Sha99a, She92d, SBVG99, Smi90, SY92, SM91, Ste96, T+99, Tou91, Tou93, TYH96, VCF+90, Vig98, Wai95, YSS99, YY97c, YY98a, ZZ95, ZMI91, AN94, AG97b, AG97c, AG97a, BD92, Bol97, BV97, Com94c, CDG95, Cl99, DD95, Dan97, Dhe98, Di 99, DFHR91, Don98, FGY96b, Fro96, FL93, Gol96a, Har91, Hof95, IS99, Jenxx, JW01, JP96, Kob91a, LRW93, Lai95, Lea90, Lev91, LL93b, Lub96, Mau91c, Mea95, Mo98, Mu92, IPNdbbbprm91, NT93, Ny98b, Pau98, PKM97, Ros97c].
cryptographic [Sch93g, SZZ94a, SZZ95b, Ste99b, Way98, WN94, XZZ97, XZZ98, YS91, ZZI97, ZL99].
Cryptographic-Token [Nys99].
Cryptographical [KP95, GV98].
Cryptographically [BDS98, Cha90, CvHP91, Hil94, PGV92, ZZ96, DT93, IS97, KSB96a, MCD98b, SKB97, Bou94].
Cryptographically-secure [Bou94].
cryptographiquement [Bou94].
Cryptography
Cryptography

Cryptography-in-the-Large [Bla93].
Cryptologic [RK98b]. Cryptologie [Bra93b, Bec90, Sch98e]. Cryptologist [Pin98, Sel94]. Cryptology [Ano93g, Ber96b, Bau97, Bec88, CW94, Cop95b, Dam91a, Dan99b, Dav91, De 95, Des94b, Duf98, Fei91, Fum97, Gol90b, GQ95, Hel94, IRM3, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mau96b, McC90b, Mei92, MV91, New97, Nyb98, OiDP98, PSN95b, QV90, QG95, Rat96, Rue93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Unixxb, Uni95b, Web93, Wie99, Wil98a].
cryptography [Bec97]. CRYPTO [DBR +99, Lim98, Lim99]. Cryptonomicon [Ste99a]. Cryptoprocessor [Pai99b]. cryptos [Hag98]. cryptoscheme [MMI97]. Cryptosystem [AMV90, BI95, BDGI98, Ber97c, Bih91, BMS94, Ble97, Bon99, BM97, CC99b, CG99, CJS91, CS99b, CW91b, Cus97, Gih91, Gib96, GC91, GC94, GGH97a, Gys96, HD96b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdL98, Luc95, MB94b, Mau93b, MY98, Mei96b, MV97, Mi92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Nyh94, Org98a, Od94b, PG97a, PG97b, PC98, PP92b, PGV93d, PR98, Ric98c, Rot95a, Sal90, Sal96, Sch92c, SSM+97, SMD+99, Sch99c, Sch90c, Sch97c, Shp99a, Shp99b, Sin99, Siu99, Slt98, SMS99, Sta96d, Ste98a, Tas98, TM99, USE96e, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wa99a, vS97, Sha99a].
cryptography-dedicated [NM96b].
HPS98, HJPT98b, Hwa91, Jab90, JS93b, Kie98, KS99b, KT91a, LR96, Lan97, LCL92, MM96b, NMR95, NS97a, NS98a, NS97b, NS98d, NS99a, Ngu99a, Ngu99b, OU98a, SG99a, Sam98, ST91, Sun98a, Tak98a, Tak98b, Vau98a, Vau98c, Wal99c, Wan92a, WY93, Yam99, AMV93, AD97, AD99, Ala97, AAPS92, ACBR90, Bao94, Bi94, BS97, Boy97, BCCG99, CC99a, CS98a, CC98, CW91a, CW97, CS97c, CCH98, Cle96, CS97d, DZ96, Gib95, Gro94, HNSM91, HY93b, He92, HWF96, HJPT98a, HLLC96, IKNY98, Jon90, JQ98b, KASH90, KSK96, KM99d, KK96, LG97, Laˇs92, LC96b, LC96c, Lon91, MMT90, MM90a, MM90b, Mi90, Mau91b.

cryptosystem
[Miy90, NS97c, NS98e, OU98b, Ole95, Ped91c, Roe99, SW95a, SH95a, SH95b, SM90, SS95b, SS95c, SX90, TY92, Tan90, TCC97, TC99b, TC99a, Ven92, Wan92b, Wu92, XL99, WX97, Yu92, Žer96b, Zha91, vT90].

cryptosystems
[BDHJ98, BHSV98b, BHSV98a, BS91b, BLM94, BS91c, BS97a, BS90b, CGJ99, DP98c, ESST99, FY98a, FY98b, FY99, GJKR99, GPCSN96, GH97b, Gor93a, HGS98, HMV93, Hrr97, Iss90, KMKH99, Kob98c, Len99a, LD99, Men93, Men95a, Miy93b, OFF93, RY97, SOOS95, SW93, ZW99, AMV93, AS98, BC90, FMR99, GP97, HNM98, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LL97b, Lon92, MMT90, MM90a, MM90b, Mi90, Mau91b].

CSP [DS97d].

CCTS [BR96a].

cubic [PLL99, GK99, K96].

cultivate [AHdJF97].

cultures [Rt96].

cunning [Beu94].

Current [JJ98c, Ril96].

Curve [AMV90, DP98c, Dem94, ESST99, Fer99b, HSSI99, Ka97a, Ka98g, KMKH99, Kob98c, Len99a, LD99, Men93, Men95a, Miy93b, OFF93, RY97, SOOS95, SW93, ZW99, AMV93, AS98, BC90, FMR99, GP97, HNM98, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LL97b, Lon92, MMT90, MM90a, MM90b, Mi90, Mau91b].

Curvilinear [SCG99].

CUSICK [YT96].

Cusick [YT96].

custom [Nor95b].

customer [Nor95c].

Customised [GN95c, HHD99].

Customising [NO96].

Cut [BLM99].

Cuts [BLM99].

Cyanide [Mar98b].

Cyber [Ano97i, Ano97-29].

Cyberbanking [Mur96].

CyberMall [Mar95a].

cybernetics [LS98a].

Cybersecurity [HMM91, HM92, HM95].

Cyberpunks [Zim96b].

Cyberspace [Ber97b, Col96, Gar97c].

Cyberwar [Kan96].

cycle [GAGCDACFC99].

cyclical [PS97].

Cycling [GS99b].

Cylotomic [SW95a].

Cyclotomy [Bo90].

cylinder
cylinder-cipher \cite{Gad98}, Cylink \cite{CMKK98}, cyphers \cite{Far93}, Czech \cite{Ste99b,vWN99,Hru98}.

D [Ben99, BALS99, CK95, Nas94, TK99, Wor96, YY99a]. \textbf{D.E.S.} \cite{JVT98b}, \textbf{Dallas} \cite{ACM98b,USE91}.

\textbf{Dabbling} \cite{Ritxx}, DAEs \cite{JV98b}.

\textbf{Dallas} \cite{ACM98b,USE91}.

\textbf{Damgård} \cite{DGV93}, Damgård’s \cite{Gib90}.

\textbf{Damas}, \textbf{Damas} \cite{BB95b}.

Dark \cite{YY96}.

\textbf{DASS} \cite{Kau93}.

\textbf{Davies} \cite{BB95b}.

\textbf{DDJ} \cite{Con99a}.

\textbf{Deal} \cite{Ano96f, Duh90, Hei93, KAK96, Lam99, Los97, MSHP99, Moc97, Nat93a, Nat93a, NHB99, Oa94, Sch99b, Sch94m, See97, Sme97, Sto90, STZ96a, TAY99, Tay90, TLS99, WSF99, Wf95, Wf94, YY91, ZTR99, Ano93k, Ano95k, CCN95, Ch94b, Cli99, CS99, Cra96, Dam99b, DF97, Gil97, GTGW94, Gut96, Hel93, KAK96, Lam99, Los97, MSHS90, Mic97, Nor95b, Pd99a, Rev91, Ros94, Rot97, Sch92a, Sch98b, Su98, Tha91, Tx92, Un96a, Vad95, Way93c, Way95, Wou90, Yua92, ARW99].

\textbf{Data} \cite{Ano97v, Bar91, BS93b, Bir95, Com95, Con94a, Cop94a, Deu90, Hk98, HK99d, Joh90, Kap98, Km97, Mat94a, Nat94b, Nat99a, Pai96, Per91, Rp94, She95b, She92g, Sim95, SB92, Wi93a, Ano94a]}

\textbf{Data-Dependent} \cite{Con99b]. \textbf{Data/Image} \cite{Sch99b, Sch98b}.

\textbf{Database} \cite{AKF94, BDPS95, KT96, LCL92, Ou99, SJ97, Wat99, HY95, IS97, Lee95].

\textbf{Databases} \cite{BDPS95, CP93, GM99b, KB92, Len99b, Pf94, RZ99, SG99b, Har90, Wad93, Ano95k].

\textbf{Datagram} \cite{PSB97}. \textbf{Datamation} \cite{CWM9+}, \textbf{Date} \cite{GN95c}, \textbf{David} \cite{Ers99, Bar05}, \textbf{Davies} \cite{BB95b}. \textbf{Dawson} \cite{Roe99}, \textbf{Dayton} \cite{Dal97}, \textbf{DC} \cite{USE99a}, \textbf{DCE} \cite{Cas95, GH95, Kon95}, \textbf{DCI} \cite{Pin98}.

\textbf{DCT} \cite{BBCP98b, BBC98, HW98a, PBBC97, TA97}.

\textbf{DCT-based} \cite{BBC98, HW98a, PBBC97, TA97}.

\textbf{DCT-domain} \cite{BBCP98b}, \textbf{DDJ} \cite{Con99a}.

\textbf{Deal} \cite{FW91, Knu98c, Lu98a, Luc99a, Luc99b, Out98}.

\textbf{Dealer} \cite{Rab94, BGS95}.

\textbf{Dealing} \cite{Bec99, MSN99}.

\textbf{Deals} \cite{Ano97v}.

\textbf{Death} \cite{CFK91}, \textbf{Deavours} \cite{Ers99, CFK91}.

\textbf{Debate} \cite{Ano96f, Dum94, Un98i, Wei91a, Wei91b, Fre94, Ho95, Neu95, RK94, Tho96, Uni98k, Hat96, Wai95]. \textbf{Debating} \cite{Ano92b}.

\textbf{Debugging} \cite{Wot99}.

\textbf{Debut} \cite{Gar98b}.

\textbf{December} \cite{And94a, Boy95a, Boy95b, Bra93a, CW94, Con99a, Dar97, Far93, IEE92b, IEE93c, IEE94c, IEE97b, KG93, Org98a, PSN95b, Pre95a, Sz93, V992, Wal99a, WN98b, Zim96b]. \textbf{Decentralized} \cite{BdM94}.

\textbf{Decidable} \cite{BRS99}.

\textbf{Deciding} \cite{BdM94}. \textbf{Decipherability} \cite{CGV94}.

\textbf{Deciphering} \cite{CJ99, Duh90, Has95, TG94, Bru91}.

\textbf{Decision} \cite{AA93, Bon98b, Bon98a, CKN99, DTDJ99, HTY99]. \textbf{Decision-Making} \cite{CKN99}.

\textbf{Decisions} \cite{Bar96a}.

\textbf{Declarations} \cite{SHK99b}.

\textbf{Declarative} \cite{Sch99c}.

\textbf{decode} \cite{Har94}.

\textbf{Decoding} \cite{CS96a, SY96a, SY98a, HG97d, HK99c, SK94]. \textbf{Decoherence} \cite{OD99}.

\textbf{Decomposition} \cite{All98, AMP94, KH99a, SC97}.

\textbf{Decomposiro} \cite{SP97, BDSV93}.

\textbf{Decorrelated} \cite{GGH98a, KR99a, Vau98a, Vau98b, Vau98d}.

\textbf{Decorrelation} \cite{Vau98b, Vau99a}.

\textbf{Decrypt} \cite{Bau97, DSB99}.

\textbf{Decrypting} \cite{Bar92b}.

\textbf{Decryption} \cite{GGH97a, HJPT98a, Oht98, CB96, BL94, Hat97, HJPT98a, MS99c, MNV99, V995].

\textbf{Decrypts} \cite{Pea97}.

\textbf{DEDICA} \cite{RCM99}.

\textbf{Dedicated} \cite{ISO97, DV96, NM96b}.

\textbf{Deduction} \cite{SGPV98}.

\textbf{Deductive} \cite{PS99f}.

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

**Designers** [FM98b]. **Designing** [AKF94, BV98a, BK95c, BM94b, CH99b, DL99, DMVC99, Ger99a, Gor93a, HJ99, JS93a, Kem99, PM99a, PD99b, Sch94c, SW97a, SW97b, SZ94b, Ste94a, SAS99b, TLS99, Zhe90, CG05, Hor99, HLC99].

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

**DESIRE** [JKVP99].

**Desk** [GRB99]. **Desktop** [Ano97r, Fuc99, Los97].

**Destination** [LTEH99]. **Destruction** [SY98].

**DESV** [CCN95].

**DESV-1** [CCN95].

**DESX** [Rog96].

**Detail** [Zeg93]. **DeTeBerkom** [GH96].

**Detectable** [VT97].

**Detecting** [Gor93a, Mad92, PM98, SG96b].


**Determination** [Bie98].

**deterrence** [van96].

**Developer** [CM99b, Di 97b, DT98b].

**Developing** [CF95, SCT99].

**Development** [Ano97h, Bar99, Bas93, GRB99, HNSS99, IR99, LL93a, Nat99c, Natxx, VDDR99, Way98, You96, AMV93, Ano97-30, LS98a, Mii95, NBD99, Sta97c].

**developmental** [Ram92].

**Developments** [Ano95a, PRB98a, Sim97].

**Deviates** [Ran01].

**Device** [HR96, Ano91b, CM97c, Uni94b].

**Devices** [BDH98, Hwa92b, Hwa92c, LS98a, Pos92, Post93, Uni94a].

**devoted** [FT99b].

**DFC** [KR99a, Ste99c].

**DGSA** [FM98b].

**DHCP** [Dra99].

**DHWM** [ADF98].

**Diagnosis** [GX99, MR55a, PW99].

**Diagnostics** [Var99b, Lew92].

**Diagrams** [Onu99].

**Dial** [RRSW97a, RRSW97b].

**Dickson** [Pie93].

**DICTA** [KG93].

**DICTA-93** [KG93].

**Dictionary** [Jas96, Luc98b, BCR98].

**Dictyostelium** [Ram92].

**Diego** [ACM93b, IEE97b, Sch98b, USE96f].

**Difference** [LP94].

**Different** [KBR97, Sch99b, RT93].

**Differential** [BB94, Ber93, BS90a, BS91c, BS91e, BS91d, BS91f, Bib92, BS93b, BS93a, BS97a, BK98d, BKPS93, CJ98, Con99b, Dae95, Din94, Fer98, Haw98b, Haw98a, KTM99, Kau96, KM98b, Kob99, KJJ99, Kwa93, LMM91, LH94, Lan95, Mat96a, Mly93c, MSK98, NK93, OM94, Pal99a, Sch96c, SKM98a, VR98, Wag98a, YLH98, Ada92, CV95, KY95b, KYxX, KM96b, LMM92, O’C95, OG95, RP95b, TN97, Way95, YT95a, YT95b].

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

**Differentially** [Ny94].

**Differentials** [BB99a, Fer99a, KRW99, BBS99a].

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

**Diffie** [BY93c, BY93b, BBR99, BWM99a, BV96, Bon98b, Bon98a, CF97, CS97d, HY98b, HY98a, Kala97a, Koc96b, Lut98, Mau94, MW96c, MW96b, MW99, RSA93b, Van95a, VW96, WM93, VO996].

**Diffusion** [Mas99b].

**Digest** [FBBH+97, GTG94, Kal91, Riv92a, Riv92b, Riv90a, Riv91b].

**Digit** [TK99].

**Digit-Recurrence** [TK99].

**Digital** [Ame95, Ame96a, ANS98b, Ack98, ALO98, AW94, AR97, Int91a, NIS94, Ano96e, Ano97-9, ASW98, Aur96, BC90, BM99a, BM99b, BdMD94, Ber97b, BM94a, BM96a, BM96b, BM96c, BS95b, BS98, BTH96, Boy97, Boy98, Bra93a, Bf99, BWF99, Car95, CR91, CPO+98, CHO98, DDM98, DDM96, Eil99, EGM90, EGM96, FF99, FKMY98, FBS98, Fri93, Fro97, FOM91, Gar97c, Gar98b, GR97, GDD+97, GB98, GO96c, GQQW+91, HK95, HG96, HG97c, HE98, HA96, HW97, IEE97c, IEE98d, JLO97, Jue99, KKS97, Kob97, Kob98c, Kra93, KH98a, LQ98S98, LM95, IW96, LL98, Lut98, LR98, MS996, Man98, MMST98, MB99a, MW98b, Mer90b, Mer97, MTN97, Mos98, ...

E-Cash [DFTY97, Yac99a, Yac99b]. e-commerce [VM96, DDJ98d, Jak99b, Lut98, Gar97b]. E-mail [LF97, Ril96, Bac95, Sta94a, Ano93j, Got99, RS98b, Sch95c, Sch95d, SH97, Ano95c, Gar97b, Str93a, Str93b]. E.I.S.S [BFS92a, BFS92b]. E.I.S.S. [Dan95]. E.I.S.S.-Report [Dan95]. E2
KMA98, Kob99, MT99a. EAP [BV98b].
early [Alv98c, Mar96]. Earth [YHK199].
Earthcam.com [Ano98j]. Ease [HJL99].
Easier [GDM98, BRR99, Sch98c, Way95].
East [Str95]. Easy [Sim94d, Ken95].
eavesdrop [Way93b]. eavesdropper [Al 96].
Eavesdropping [RK99]. Ecash [Sch98h].
ECC [Cer97, Kal98e]. ECC/DLP [Kal98e].
EccFan [PKA98]. ECP [BT97]. ECCp-97 [BT97].
EccoFan [PKA+98]. ECP [BV98b].
ECCp [BT97]. Echo [GLB96].
echiphering [Blu97]. ECMA-219 [ECM96].
ECMAST [Dan96]. Economic [Mos98].
Economy [CFG99, Org98a, Tas98].
ECP [Mey96]. Ed [DDJ98e, DDJ98f, MGL+98].
Edgar [Sha99a, Ros97c]. EDI [Len93].
EDIFACT [RCM99]. Edinburgh [IEE95a].
Editor [Hat96, Joh99, Bur98b, Ano95g, Ano95h, Ano96g, Ano96h, Ano97i, Ano97m, Ano98d, Pre95b].
Editorial [Eri99]. editors [Joh98, AKP96, BNP99].
eds [Ers99]. EEC [BGV93]. EEC-RACE [BGV93].
EEPROM [FG98]. EES [Com94b, FIP94, Nat94d]. EF [KP95].
Effect [OD99]. Effective [Fuc99, Min97, MBY97].
Effectiveness [CNS99b, ENK99]. Effects [CGB+93, CI96].
Efficiency [Bas98, BM99a, CM99a, DKK99, KS97c, Mar97, BHS93]. Efficient [AGS97, AGY95b, BBDW96, BDV93, BF97b, BF99c, BFP99, BDB2, CS97a, CM99, CG99, CG98, CDD+99, Cre97, DR99a, DT98a, DN94, FH94, FOM91].
Electrochemical [DDJ99].
Electronics [IEE97g, IEE98c].
Elegance [Sch99c].
Elektronicznej [Sch95e].
Elementary [Mil92, Tat98, Tat99]. Elements [FC99].
Elizebeth [Unii2]. Elliptic [AMV90, Ano95n, BS91a, BSS99, CTT94, De 98d, DP98c, DMPW98, Dem94, Eng99, ESST99, Fer99b, HSSI99, Hes97, JQ97, JM97, Kal97a, Kal98g, MKKH99, Kob98c, KMOV91, KT93, Len99a, LDD99, MS93, Men93, Men95a, MM96b, Miy93a, Miy93b, Miy96, Miy99, OFF93, RY97, SOOS95, SW93, SSNP99, VZ97, WZ99, AMV93, AS98, BGR94, BC90, BS91a, CNST98, CPPK98, FMR99, Gal99, GKP99b, GP97, HNM98, IS99, IKNY98, JQ98b, KS96, Kob91b, KK98, KOT95a, KOT95b, LL96, Ler97, Mau91b, MV90, MVZ93, SX90, XL98, ZI98].
Elliptic-Curve [Fer99b, Kal97a]. EMACS [McH92]. email [Kar96].
Embed
EMEF [Org98a].

Emergent [Kal99, Org98a].

Emerging [Kal99, Org98a].

Empirical [WW98b].

Emulating [BWM98].

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

Embeddings [CT99b].

Embraces [Ts'97].

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

Encrypted [AW99, Bla98, GMCF95, GLZ99, Gil98, Jas96, YY91, BT98, DF97, STW95, Kip97].

Encryption [AN97, Bla94, Lom94, Luc98b, EW99, SS99c, Beu94, KAK96].

Encryption [ASW99, AAB97, Ada97b, Ada98, ARRW99, And98, ABK98a, Nat93a, Ano94c, Ano96c, Ano96l, Ano97b, Ano97v, Ano97x, Ano99c, Bac95, Bal97, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b, BDP98, BS99b, BS99c, BRW99, BS93b, Bir95, BB95c, Bla96a, Bla96b, BF98b, Ble98a, BC95c, BF98d, BY92, Com94a, Com94b, CDNO97, CMN99, COP95a, CH98, CMK98, CT99a, Cop94a, Cou93, DDJ98e, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DSG97, Ele98, FIP94, FN94, FY95b, FY97, FH94, FO99a, FO99b, GSY99, Gai90, Gar97a, Gar97b, GC97, Gar98a, Gar98b, GK98, Got99, HG97a, HG97b, Hat96, HK98, HK99d, Hub98, Jol90, JM96b, Kal93a, KY95a, KR96a, Kal98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kum98].

Encryption [KBRS97, KH98b, KYDB98, Kwa93, Kwa97, RSA93f, Law98, Lea99, LT91, LW91, LM91b, Lin93a, LS98b, Luc97, Luc98c, Luc99c, LW90, MGL98, Mat94a, Mat97, Mer91, Mey96, Mii95, Moc97, Mue99, Mii99, Nat93a, Nat94b, Nat94d, Nat97b, Nat98, Nat99a, Nat99c, Nat9x, NB99, NH90, Ohi99, Ola94, Ori96, Pul96, Pur98a, Par98c, Per91, PR99, Pin97, RSA93a, RSA94, RP94, Riv95c, Riv95b, Riv97c, Riv98c, Riv98d, Riv98a, RD99a, RD99b, RC94a, RC94b, Ros94, SvA98, SKN98a, SKN98b, Sch99a, Sch99b, Sch93d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW98e, Sch98g, SKW99d, SHK99a, SKW99e, SE96, She97, She95b, She92g, SB98, Sim95, SM96, SM98b, SB92, Sm97a, SB99, Sta97c, SW99b, Sto90, TPH98, Uni97a, Uni98a, Uni98c, Uni98b, Uni98d, Uni98e, Uni96b, UU97a].

Encryption [Uni97b, Uni98a, Uni98b, Uni98c, Uni97b, Uni98a, Uni98b, Uni98c, Uni98d, Uni98e, Uni98f, Uni98g, Uni97c, Uni98j, Uni98i, VB96, VR98, WSK97a, WSK97b, War98, Way93b, Way93c, WSFC99, Wei91a, Wei91b, Wei94, Wir98, Yin97, YY97c, Yuv97, Zhe97, Zhe97, Zol93, Aus96, Abr97, Ala93a, All97, And94a, Ano90, Ano92b, Ano94c, Ano95c, Ano95k, Ano96d, Ano96m, Ano97a, At94, AM99, Ban94, BTD98, Bax97, Bea96, BR94b, BR95a, BDJ97, BR97b, BB99, Bet95c, Bih97, BF98a, BC96a, BMS96, BFS98, Bow93, Bro96, Bus96, Com97, CCN95, Cha94b, CLW98, Cle96, Cli97, Cli99, CJM96, Cra96, DH96a, DOR99, Dia91, DL98, Eke99, Eig97, FC94, FB97, Gil97, Gol99b, Gol96d, GBL94, Goo96, GKS97, Har90, HK90, Hat97, Hel93, He93b, HT95, HP94, HY95, HCY96b, HCC98, Int91b, Jac90a, Jac90b, Jak99c, JT96, JT97b, KY95b].

encryption [KY97, KYYx, Ken95, Kir95, Knu99c, Kop97, Ku92, Kub98, Kuo90, LM91a, Lam99, Lee95, LC97a, Los98, MRS99, Mar95b, MM95, MM97, Moli98, Mra95, Nat93c, Nor95c, Oel97, Pos92, Pos93, Pre95a, QN98a, Rev91,
Ril96, Riv95d, RKD94, Rot95a, Sab94, Sch98b, Sch94i, Sch98c, Sch99j, She96a, Sme97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vad95, Vau98e, Ven90, Vu95, Wad98, Wel95, Whi93, Wil93a, Wi93b, WO90, You97, You97, Zaj97, Zan90, Zer96a, vOV91, vT93, An98j, An93j, Hon98).

encryption/authentication [Sch99j].
encryption/decryption [Hat97, Vu95].
Encryption/MAC [Yuv97].
encryption/multisignature [HCC98].
Encryptions [Mv93].
encrypts [Ano93k].
Encyclopedia [CFK+91, New97, UFC94].
End [Bra94a, DDJ98c, Gar98a, NH90, WSFC99].
End-to-End [NH90].
endlicher [Wal98].
ends [Mc-C90b].
Endured [Che92].
Energy [DFL99].
Enforce [BDS98].
Enforcement [Cae96b, Cli99].
enforcers [Way93c].
Enforcing [Ano97n].
Engine [BE90, CM98, She92d].
Engineering [An98f, DFGH99, EKLM99, IEE96d, LBHM99, SS99w, Sm98a, AN94, IEE97k].
Engines [T99, Way93a].
England [ES98, Cur98].
Enhance [FO99a].
Enhanced [An95c, AR98, Ken93, LK96, Zan90, Zeg93].
Enhancement [HWJ98, Lin93a, Lin88a, Lin89a].
Enhancements [JM96b].
enhancing [HY95].
Enigma [CWM+91, Har96b, Kip97, Kip99b, Obe99, Ano91c, Bl98a, Bl98b, Bli98c, Cra92, Kahl91a, Kahl98a, Kip97, Kru98, Mia96b, Mus92, Tu99, We97].
Enigmas [Gad91].
Enjoyable [CM99d].
Enough [CFK+91, Dea98b].
Enschede [Hei96a].
Ensuring [Com97, Rot95b, ZG96, Way91].
Enter [War96].
Enterprise [ECD+99, FY99, Mar95b, Wad93, SY92].
enterprise-wide [Wad93].
enters [Joh98].
Entities [KM99c].
Entity [BR94a, BM98].
Entrepreneur [Pin98].
Entropy [Bro94, EHMS99, KSHW97, KSHW98].
entwerfen [Hor99].
envelope [SOB98].
Environmental [RS98c, RS98d].
Environments [GSTY96, SKAM99, DNS99].
EPIC [Rot95a].
EPS [Ano96i].
equally [Ito91].
Equation [Cop95c, LG97].
Equations [Por98, RZ99, BMP97a, Cus95, GK95b, LCL95, Luni92, Sun91a].
Equilibria [Ett98].
equipment [Int91b].
Equitable [BDS98].
Equivalent [BV98c, De98d, Gib91, GO93, HTY99, MM96b, Mi96, Oka94, Pai99c].
Era [DDJ98c].
Ergonomic [DDJ98c].
Erika [Mat99].
Errata [Con99a].
Erratum [An91a].
Error [AW94, AR98, BGS96, Cha99c, DLR97, KK97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, DLP93, JV98b, Ste95, Wan92a, YL97a, vT94, CW94].
Error-Correcting [AW94, BGS96, DLR97, KK97, Pn96, Ada91, Ala93a, AW95, Cha95a, CMM93, Ste95, Wan92a, YL97a, vT94].
Error-Correction [MG91].
Errors [GGH97a, SHK99b].
ESA [Sp95, YS91].
ESA/390 [YS91].
ESAT [PGV93d].
Escrow [AAB+97, BBl96c, BDS98, Cae96a, CM97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, LWW95, M99, Mza97, M95f, KKS99, Nce96, SY98, Sam98, SM95a, VvT97, VBD99, YY99b, An94e, BDH97, BR96b, DH96a, D95, Fre94, KL94, Mao97, Uni95a].
Escrowed [Bas95, Com94b, FIP94, Nat94d].
ESIGN
EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, vHPP93, Bea97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, Ole95, Pai96b. 


Externalization [OA99]. Extracting [Nis96]. Extraction [SD99]. Extraordinary [Jam98]. extremely [Ano90]. eyewitnesses [Ano97t]. 


Facility [AKF94, Bis90, She96a, YS91, JMLW93, STW95]. facing [KG96]. Factoring [Ano96b]. Factored [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pai99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, McK99, Me96b, Riv95a]. 

Factorisation [Kal98e]. Factorisation [DHW95a, Jon90, DHW95b]. Factorization [Ale92, DDLM94, MM98a, MM98b, Od95, vo91a, Sho97, vO91b, LLMP93, Mao98, Whi93, vo92]. Factorizations [BMS94, NS97b, NS97c]. Facts [Ano91b]. 

Faded [Alv98a]. fading [To97]. Fail [BP97a, PP97, SNNP99, vHPP93, And94b, Pf96c]. Fail-Stop [BP97a, PP97, SNNP99, vHPP93, Pf96c]. 

Failed [BCE+94]. fails [DH96b]. Failures [Ch98, QJ97, Moo92, Sim94b]. Fair [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, M KS99, SS99e, SS99f, Tra97]. 

Fairfax [ACM93a, ACM94a]. Fairly [HD96a]. fail [Od90, Rob98b]. False [LKD98, She92b]. 

Families [Kal98e, Per99]. Family [KT98, Miy91, RP97a, ABC+98, BGH+95a, FSS94, Ito91, Kob90, SRRL99]. FAPKC [DYL98]. FAPKC3 [TCC97]. FAPKC4 [TC99a]. Far [Str95]. Fast [AGS97, AMV90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bih97b, Bih97c, BHK+99, BD94, BK95d, BGV96, CS91, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBVD96, DNR97, EPR99b, EPR99a, Gar97b, Go96a, HJPT98b, HP94, HCY96a, JI99a, JI99b, KR94a, KTM+99, KP99a, KP97, KR99a, KmA99c, KM99h, KA91, Koy95, LM95, Mau90, Mer91, Mih94, MM95, NS99a, NK99, PR97, Pre95a, Rog95, SW97a, SW97b, SOOS95, SV93, SB98, Sho96, Si97b, Tak97, Tak98a, Tak98b, T+99, Vau98d, Vau98e, AMV93, AB96b, Ano98j, CGV94, DKR97b, DV96, GGH+98, HJPT98a, Jenxx, LRW93, LC98, MZ98, Pv95, RRS98, She92c, SN94, SH99, SAM97, SGSD99, YL93, Go96d, OA94]. 

Father [CFK+91, DDJ99]. 

Faul [BS97a, DHSS95, GX99, OKST97, Pai99a, RB94r, IEE94b, TCH+91]. Fault-Tolerant [DHSS95, RB94]. Faults [BDHJ98, BDL97, CH94a, FY99, Gar94, JQBD97]. Fauvel [CFK+91]. 

Fax [Ano91b, Int91b]. FaxModem [Ano93k]. FC [Fra99, Hir97, Hir98]. FCC [Gar97b]. 

FCD [ISO97]. FDR [Low96]. FEAL [GC91, KR95a, MY93a, Mi90, Miy91, TN97, BS91e, BS91d]. FEAL- [Mi90]. 

FEAL-8 [GC91]. FEAL-N [TN97]. Fears [Gar97c]. Feasibility [DN95a, NFQ99]. 

Feasible [Li94]. Feature [Sar99, SD99]. Features [ADEDS99, Zav99]. February [ACM98a, Fra99, FJV97, Go96d, Hir97,
Hir98, IZ98, RP97b, SJ97, Wol93a, Wol93b, van96, Ano94c. Federal [Ano97b, Ano97x, Lee99a, RP94].
Federa ted [SS99b]. Feedback [CJM95, GIK95a, Ros98a]. Fei stel [Jut98, Knu94a, SN93, SK96c, SK96d, Van99a].
Fermat [LLMP93, McK99]. Few [FJRS96, Mei98]. Feistel [Jut98, Knu94a, SN93, SK96c, SK96d, Van99a].
FFT-Hash [DBGV93, Sch93g, Sch93f]. FFT-Hash-II [Vau93]. FFT-Hashing [Sch91c].
FGPAs [Nor95c]. FHFC [KKW99]. FHFC-Tool [KKW99]. Fiat [Nac93, OOK91, OO93]. Fiber [Tow98].
Fibers [HLMP96]. Fibonacci [DMM99]. Fiat [Nac93, OOK91, OO93]. Fiber [Tow98].
Fifteen [Den90]. Fifteenth [CFK91]. Fifth [SJ97, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni97c, Uni98k, ACM93b, USE95b].
FIL [AB99a, AB99b]. FIL-MACs [AB99a, AB99b]. File [ANS98a, AW99, Ano97a, Bla94b, Gil98, Mau97b, RC95, HSK97, MKKW99, SK97d].
Filtering [Sch97d, LLBH98, LGY94]. Final [RIP95b, RIP95a, BFS92a, BFS92b, BP95b].
Financial [AA95, ANS98b, BFS97, FL99b, Fra99, Hnt97, Hnt98, Lan97, Rev97b, Swi97]. Finding [BMRW98, Cop95c, Ler97, Rev91a, Sim98c, YY98a, CC98, Car97c, Sta94a].
Fingerprint [DDJ98g, DDJ98h, HWJ98]. Fingerprinting [Ano99h, BS95b, BS98, DF99, Hei96b, PS96a, PW97a, PW97b, Sas99a, YST99a, YST99b, DF98].
 Finite-Im pulse-Response [She92e]. Finite-Size-Particle [BVFD99]. Finland [Nyb98]. FIPS [Nat93b, Ano93f, Ano95i, Nat93a, NIS93b, Nat94a, Nat95, Nat99a].
Fire [Way93b]. Firewalls [GLZ99, Opp97]. Firms [GC97]. Firmware [MNSV97].
Firmware-Oriented [MNSV97]. First [BCB97, GPSV98, Hir97, KP99b, KW99, Law98, Mat94a, Nat98, Nat99c, RD99b, ACM99b, And96c, Dob98, HOQ97, IZ98, NBD99, Uni97a, Uni98c, Uni98d, Uni98e, Uni97b, Uni98f, Uni97c, Uni98k, USE95c, RD99a]. First-Order [KW99].
Fish [BD94]. Fishermen [Ano96l]. Fissures [DDJ98e, DDJ98f]. five [KAK96]. fix [Ano98j]. Fixed [FK93b, Maeh8, HP94].
Flexibility [Wed99]. Flexible [JPL99, LL94b, AG95, BP97b, Ts90].
focusing [Com96, USE96c]. Foil [MB94a].
[AW94, GM97, LHL95b, LHL95a]. Forget [DFIJ99]. Forgotten [Ano97t]. Forimage [XA98]. Form [Cha93, STP93]. Formal [BR97a, BFN98b, Boi98a, Boi98b, Boy92, GF93, Gue98b, Mea95, P90b, SM95b, Tou93, WK96, AHdJF97, AAPS92, Ata94, BFN98a, JW01, ZLX99]. Formality [ACD94]. Format [CDF98, Nys99]. Formats [ASZ96]. Formed [Gar97c]. forms [Mok97]. Formulae [KV94, WD99b]. Forty [CWM+91]. Forum [IEE98d, MB99a, Org98a, Ano97c, GO96c, KSS+92]. Forward [BM99a, BM99b, CadHSV96]. Forward-Secure [BM99a, BM99b]. Foundation [Gol95a]. Foundations [Ada91, BDFM99, Gol97a, Goi97b, IEE92a, IEE96a, IEE96c, IEE97f, IEE98a, IEE99a, JR96]. Founder [Pin98]. Four [HKQ99, Koe99, Riv91a, DL95]. Fourier [MS94, NA95]. fourteenth [IEE95c]. Fourth [OW95, Uni96b, Far93, IEE99a]. FPGA [GTG94, Kap98]. FPGAs [KP99a]. FR [HSSI99]. Fractal [DS96, SD99]. Fraction [BDF98]. fractional [BR96b]. Fractions [Iss90, KE97]. Fragments [Gol95a]. Framework [Boy92, DGV93, Hed97, PS99f, PW99, SL99, VP99, Com97, HN94, LS98a, Pi96c, Tas98, DT98b]. France [Chr98, DEQ92, FR95a, GQ95, Vau98c]. Francis [Lea90]. Francisco [Ano97a, Ano98f, USE92a]. Francoonia [IEE92a]. Franklin [WD99a]. Fraud [Neu92, VGP93, VtV97]. Fraud-Detectable [VtV97]. frauds [Sga93]. Fray [Gar97b, Law98]. Free [BP97a, BHT98, BDI96, CD98b, Dob97, Eri97b, GJM99a, GJM99b, HBK199, Rus93b, SK95, All97, BT94, Des90b, Des96b, Dob95a, Il94, Van93]. Free-Space [HBK199]. Freedom [Cae96b, Uni97a, Uni98c, Uni98b, Uni98e, Uni96b, UU97a, Uni97b, Uni98f, HM96]. FreeNIX [USE98c]. French [Blo98b, Bou94]. Frenkel [CFK+91]. Frequency [BP98c, MSHP99, Ano90, Tod97]. Freshness [KYG92]. FRG [Oht96]. Friedman [Uni92]. friendly [Bus96]. Friends [DDJ98e, DDJ98f, Sch92b]. Probenius [CPPK98, Graxx, KMKH99]. FROG [WFS99, Wag99b, GLC98, WFS98]. Front [Hed97]. Frontier [Bar93a, Bar93b, HM91, HM92, HM95]. FSE [Bih97c, Vau98e]. FSE'99 [Km99c]. FTP [SSH93]. Fujiyoshida [IRM93]. fulfilled [Mar96]. Full [BS93a, DH90, SK98c, SK98b, Pos93]. Fuller [CFK+91]. Fully [BDRV94, BDRV96, HE98]. Function [BJY97, BDP97, BP97c, CP91, DBGV93, DGV93, Da95, DC98a, DDP90, Dob97, FGY96a, HILL99, HL99, MCD99, NSS99, PBD97, Sch91c, TO94, AB96b, DK94, DDFY94, DI99, FGY96b, KSB96b, KSB97, LTT95, MIZ98, MVZ98, PKM97, Sch91a, SRRL98, SS95b, SS95c, YL97c, ZPY96, dB94]. Functional [Yam99]. Functions [AVH98, Ano95a, BDP99c, BCK96d, BCK96e, BHSV98b, BHSV98a, BG99, BGS94, BGS96, BM94a, BL95, BHT98, CDD99, Car93, DGV93, DY90, DY91d, DY91b, DFL99, ECM96, EPR99b, EPR99a, FBS98, GJKR96b, JQ97, KTM99, Kim93, KP96a, Kra95, LS97b, LM93a, LM93b, LM95, MS99b, MS90a, Mer90a, Mer91, MS95f, Mil96a, Mon93, NR98, OS98, PW93b, PGV92, Pre93a, PGV93a, PGV93c, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, SZZ95c, SRY99, Z295, Zhe90, vW94, BSN96a, BSN96b, BD92, BGR95, BCK96b, BCK96c, BHR99, BK98f, CCZ98, CG95, Cus96, CS96c, Dam90b, Go96a, G95, GHS93, HSK97, HLW93, HXM94, HYTL99, ISO97, JQ95, KL95b, Lai95, MCD98b, O'C94, PGV91, PGV93b, Pre94a, PGV94, PV95, RP95b, Roe95, Rom90b, SZZ94a, SZZ95b, Sim98c, Ts92b]. functions
[Tsu92a, Wer93a, Wer93b, YT96, Z197].

fundamental [IEE97e]. Funds [GBC93].

Funktion [MPS94]. Further
[Pre95b, WKS+99, WD97]. Fusing
[DMFB97], fusion [KH97]. Future
[Fuc99, HP98b, Od95, PT95, PM99b,
Sch97a, And98, BFS92a, BFS92b, Mar96,
NIS92, SB92]. Future-Adaptable [PM99b].
Fuzzy [Blo99, CIBM99, FCH99, KKW99,
Tro93, ZHJ98, CS99]. Fuzzy-Control
[KKW99].

G [KSW96]. G-DES [KSW96]. Gabidulin
[Gib95, Gib96]. GAC [ZZ95].
Gaithersburg [IEE94b]. Galois
[Mas91, PSR97]. galore [FK94]. Gamal
[Jab90]. Gambling [HS97]. Game [Et98].
Games [Mye96]. Gate [TT99]. Gateway
[KBR97, MB99b]. Gateways
[Bec99, VDDR99]. Gauss [GvP98, Mon93].
Gbt [HK97]. Gbt/second [HK97].
ge [LPNdbbbprm91]. Geheimschrift
[Kip97, Kip99b]. Gemmell [Geh94]. Gene
[Cap94, CO98]. General
[BC95a, BK95b, BPRF99, CL98, FDB93a,
ISO97, Ive91, KKT091, KP93, NOVY93,
OK8, St93a, Ben94, DD95, Des90b,
FDB93b, GN95a, Pfi96c, Sch91b, Sim98c].
general-purpose [Sch91b]. Generalised
[GS99b]. Generalization
[Jab90, HKM95, MSS93, TC99a].
Generalized
[BBCC95, BFS98, CT97, HL93a, Jut98,
LH93a, LH93b, Man96a, PS96b, Bad99,
BRR99, BCCCG99, Kuc92, Por93, Son99].
generate [Wer93a, Wer93b]. Generated
[SVBJ96]. Generating
[Ble96, De98d, FMM99, Len96, Len98,
MS95f, YWW99, CH97b, SH99]. Generation
[ARV99a, ARV99b, BG98, BGM97a,
BGM97b, Bir98, BF97b, BD93, Cocz97, CD96,
DF91a, GJKR99, Gil99, Gut98b, HL99,
Kal97b, KS98c, MBB99, Mat96b, Man90,
Mih94, PS98g, ROT94, RS98c, RS98d, SN96,
Sil97b, WI99, Bou94, FMY98, GTS90,
LLH96, MS99c, PS97, PS98b, SH94, Bou94].
Generator
[FIP93a, HILL99, JK99, KSF99, KW99,
MS95b, PS98b, Dar93, Jen9x, MS95a,
Mih96, PC98, Rev91, Sinu99, TSY98, Wal90].
Generators [HL99, KSW98d, Kra90,
ZYWR91, CS96b, CS97b, Imp92, Kos99,
Lag90, Pat91b, Por93, SG99]. Generic
[Bel92, CM99a, MS98b, Tu99, ZK98].
Generic [BS99a, LC99]. genigma [Obe99].
genius [Ano97t]. Genomic [MUS98].
Geodesic [Blo99, LFCK99]. Geometric
[OM98, Sim91, JM93, JM96a, Mra95].
Geometrien [Wal98]. Geometries
[LMS90, FS98d, Jun96, Wal98]. Geometry
[Ben99, DFGH99, Tou96].
Geometry-Based [Ben99]. George
[Pin98, WG97]. Georgia [ACM99b].
Gerdes [CFK+91]. German
[Wei99, Cra92, Dav98a, FT95, Ger97, Hor99,
Jar97, Kah91a, KK7, Kip97, Kru98, Wal98].
Germany [BFS92a, BFS92b, Fun97,
IEE97d, LM98a, Wat91, Rat96]. Geschichten
[CWM+91]. Get
[Ano96j, Cae96b, DDJ98a, Sch98c, Ude98].
Getting [WG97]. Gets
[Gar98b, GO96c, Los97, Sch98c]. Getting
[Kwa93, Way95]. GF
[PSR97, DBVD96, LD99]. GI
[BGH95b, LM98a]. GI-Fachtagung
[BGH95b]. Gibbs [DP99]. Gilles [Buc91b].
Girault [SSN98b]. Girl [Got99]. Girls
[Ros99]. Give [GB98]. Given
[BM92, BDF98, Ev9H19, Ev92]. gives
[An93k]. Giving
[Int91a, GQW+91, JLM+94]. Global
[JV98b, Or96, SS99b, TGK99, TL999,
Z95]. GMD [SBGK99]. Go [DD98a].
Goal [AMP94]. Goals [BP98e]. Goats
[SV95b]. Going [DD98c, Ano95k]. Gold
[SZ93]. Goldreich [Ngu99a, Ngu99b].
Goldreich-Goldwasser-Halevi
[Ngu99a, Ngu99b]. Goldwasser
Guidelines [Bar97, CPOR97, Mer97, Ame95, Ame96a, Org98b]. GUMP [FBS97].
guru [Di 97a]. gyi [IPNdbbbprm91].

H [Scu92, Lea99]. H-1B [Lea99]. H. [WG97]. H.R [Uni98c, Uni96b, Uni97b].
H.R. [Uni97a, Uni98b, Uni98c, UU97a, Uni98f]. hacker [Mei98]. Hackers
[GC97, HM91, HM92, HM95, Mei98]. Hacking [MSK99a]. Hades [Bie98].
Hagelin [Hag98]. Haifa [Bil97c]. Halevi [Ngu99a, Ngu99b]. Halkidiki [Pot95].
Halske [Dav98c, Sel98b]. Hamburg [LM98a]. Hamming [She95c]. Hampshire
[IEE92a]. Hand [BF99a]. Hand-Held [BF99a]. Handbook [Bac95, MVV97, Sha99a, Att99, Rey96, Rey97, Rey99].
Handles [Sar99]. Handling
[BMS99, Dae98, HC95a, Mat91]. hands [Riv98c]. Handshake [Sim96b]. Harari
[Ver95]. Harbor [Kah98b, Par98b]. Hard [MGL98, Mar99, SS99a, BFKL94, Jon90].
Harder [Sch97b]. Hardness
[BV96, NS99b, Dif99, Kha93]. hardness-amplification [Di99]). Hardware
[ACD94, Bir98, BF99b, Bri90b, BS91h, Cla98a, DGV92, GN95c, Koc96a, OSA91, Will93a, Wot99, YK98, BB95a, DN95b, Gai90, KP99b, LMS97, MZI98, Nor95a, Nor95b, Nor95c, No96, Sec97, SN94, TY92, Way95, Zhe95b, Kui91]. Harmonic [RG99].
Hash
[ANS97, AHV98, Ano93f, Ano95a, Ano95i, BDPSNG97, BCK96, BCK96, BS91e, BS91d, BDP97, BHT98, CP91, DBGV93, DGV93, Dae95, DY90, DY91d, DY91b, EPR99b, EPR99a, FIP93b, GHR99, GS94a, ISO97, KP96a, Kra95, LM93a, LM93b, LM95, Mer90a, Nat92b, NS93b, Nat95, PRZ99, PW93b, PGV92, Pre93a, PGV93a, PGV93b, PGV93c, PGV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sch91c, Sch93f, SV94, SRY99, Sta94b, Vau93,
Holiday [IEE94a]. Holy [Sal99]. Home [Hus99, Ano97i, Hod97]. Homomorphic [FDB93a, Bet95c, FDB93b].

homomorphism [Dom96].

Homomorphisms [Bur96, SK94].

homophonic [HYHW98]. Honest [Rab94].

Homomorphic [FDB93a, Bet95c, FDB93b]. homomorphism [Dom96].

Homomorphisms [Bur96, SK94].

homophonic [HYHW98]. Honest [Rab94].

Hood [Sch93e]. Hook [Ros96c]. Hope [BCE+94]. Hopes [GO96c]. hopping [MHMW98, Tod97].

Hor [lPNdbbbprm91]. horse [Sch99f]. Host [Kol95, BGT96].

host-centric [BGT96]. Hostile [GSTY96, SKAM99, LC95].

Hot [IEE98b, IEE99b, Bra90b, CB96].

Hotel [LW96, Nat98]. HotOS [IEE99b].


Huang [PBGV90]. Huffman [Moh92].

Huge [HE98]. hui [XtTmW94].

Hungary [Rue93]. hunger [WSFC99]. Hurt [Gar97a]. Hut [We97f].

Hwang [Aia97]. Hybrid [DD99, JLM+94, KA99, MD99, NT99, Var99a, BP97b, GMLH94, RO96].

hyperchaotic [BCC99]. Hypercubes [DH95a, DH95b].

Hyperelliptic [Sma99, BLMO94, BDB92, Cha94b, GS94a, KM99b, KI96, LMOB95, LML98, NP97, O99, Oka93b, Sak96, Sch90b, Ste94a, Ver95, BBC98, BM95, BM91b, DF91b, DF98, HLC99, IS99, Kunn97, Mu92, SSN98b, Sch90a]. Identities [MS99a, Sar99].

Identity [ALO98, Dan95, DQ94, FKMY98, HJPB97, JG90, KP98, Len99a, SSN98a, O99, OU98b, Tan90]. Identity-Based [Dan95, DQ94, SSN98a, OU98b, Tan90]. IEC [Int91a, GQW+91]. IEEE [Ano95n, CH96, Ano96k, Ano97-28, Ano98i, IEE95c, IEE95b, IEE96d, Kal97a, K99b, LW96, Pit95]. IEEE-IMS [IEE94a]. IETF [Ano97c]. If [GPR98]. IFIP [Kat97, LM98a].

IFIP/GI [LM98a]. II [Sch99b, AK99, Ano97w, Ano98c, Ano99c, BS91f, CFG96, CK95, CW91b, Dav98a, Don98, Eri97b, Mit92b, Mon96, Mus92, Pin98, Rat96, Rey97, RP97b, Ros99, Sch93f, Sch93g, USE90, Van93, Wi98a]. III [Fri92b, Gan93, GN95c, Nor95a, Ree98, Rey99, USE92b]. iKP [HS96].

illicit [SG96b]. Illinois [USE99c]. IMA

[Boy95b, Dar97, Fur93, Wal99a]. Image [BZ98, BNP99, DS96, DP99, Fri93, HPA99, HPG98, HWJ98, IEE95a, IEE97a, IEE96e, IEE97p, IEE97j, K95, KM92, LMP99, Mac98, Man98, Pit95, PZ98, PNFK95, Sch99b, SC96a, SCxx, SJ97, SD97, SZT96b, TOH98, VP99, Wal95, YKY99, BCP99b, BCD98, CCH98, JT96, JT97b, KS98c, KG93, KH97, NP98b, OP97, OP98, Ok96].
PBBC97, Sch98b, Sea95, SHG98, TKS98, VP96, VP98, Xie98, YM98, CKF+91.

Image-Adaptive [PZ98]. Imagery [WD97].

Images [BLMO95, BO96b, B99, Car95, JJ98c, KR98, KPR99, LvdL97, LvD98, LSVV95, MFG95, NNEK97, Per97, SC96b, SZT96a, WD96, ZK95, BP98b, BP98c, BBCP97, BBCP98a, BCV97, BOD95, CKLS96c, HW98b, Ihb97, Iv998, Nas94, Nat97a, ODB96, ÓPH+99, Pit96a, RRP97, RKDB96, TA97, XBA97, ZL97]. Imaginary [HJPT98b, HJPT98a, ZPY96]. Imagination [Sha99a, Ros97c]. Imaging [AA97, RP97b, Yeu97]. Imai [Pat95]. Imake [Hus94]. IMAP4 [Mye94a]. Immunity [SZ96]. immunity [Ada92]. Immunized [FY95a]. Impact [Mar96, Ven90]. Impending [Bra95c]. imperceptible [CKLS96b]. imperfect [MY98]. Imperfectly [BMC95]. impersonation [SNT93]. Implementation [Ano96, Bib97b, Bra96, BS91h, Da99, DGT96, DRR95, DBVD96, Ebe93, Fei93, Fei96, FOM91, Gla99a, HKQ99, HRV99, IMI93b, KP99a, Kob98c, Koc94, Koc96a, Lan97, LCN99, NM99, OSA91, PL94, PP90, Ros96b, SJS98, She95b, Tou92, Var99a, YK999, You97, Zim99, BR96b, BC90, CKN99, Din91, HNM98, IMI93a, LS98a, Men91, MV90, MIZ98, MPL99, Nor95a, Pai96, Per91, SS98a, See97, SAM97, VAD95, XL98, Koe99]. Implementations [Bas98, Bri90b, Gon98, HK98, HK99d, Koc96b, Mos98, SV93, Wa99c, Web98, WS98, Gai90, KSK96, Zho94]. Implementing [SAS99b, Van95a, Lee99a]. Implications [Bas93, CMY98, NS99b, PN92, Van95a, Wel95]. Implicit [Jam98, MILY93]. Implicitly [HRVV99]. implies [LHL95b, LHL95a]. Importance [BDL97, Sch99h, CM97d]. important [Sta94a, Woe97]. Impossibility [MP91]. Impossible

[BBS99a, Fer99a, BBS98a, OK96a].

42

IEE97g, IEE97d, IEE97j, IEE97k, IEE98c, IEE98d, IRM93, IZ98, IZ99, KG96, KM96a, Knu99c, KP99b, Kru98, LOX99, Ma992, Mar97, Mau96b, MDS90, MKS99, MDP94, Nyb98, OW95, OiDP98, PSN95b, QG95, Sti93b, Sti94, TM99, Ved98b, Wat91, Yua92, And96c, Chr98, Cop95b, DC96, Des94b, Ele99, FR95a, HOQ97, Ka97c, Kob96, LM98a, Lom97, Pre95a, SP90, Sta97c, Ste99b, TV94, Vau98c, Wad98, Wie99, vWN99, [Int91a, Moc97, See97]. Internet [Cha99a, SS99d, Ano97z, Ano98b, Atk97, Bet95b, Bet95a, Bhi96, BDC+95, FFW99, FT99b, Fum98b, Gar97a, Gar97b, Gar97c, GC97, Gar96b, GO96c, HA94a, HFS99, HC95b, IK96, Ken93, Lin88a, Lin89a, Lin93a, Los97, Mcc96, Mit92a, Opp97, Pau99, Rit99, Ros97c, Sar97, Sch99a, Sme97, Smi97b, SL99, TAP90, VJ98, VM96, Way98, Wri98, Zim98, dVdVI98, Sha99a].


Introduction


Invited

[BE90, Bra90a, Bri90b, Dif90, Duh90, FK93a, Fuc99, HMT+98, Koh90, Lei99b, Sim90b, SB93, Smi90, Wat99, BS91c, Gol99c, Sim91].

Involving [FMM99, Bea92, Pos98]. IP [Ano95b, Atk95a, Atk95b, Fei93, Fei96, KA98a, KA98b, MB99a, MS95c, MS95d, OG97, MS95e]. IPSEC [Wu96, GK98].

Ireland [IEE97a, IEE96c]. Irish [Got99]. irreducible [It91, Kob91c].


Issued [Gar97c]. Issues [ACM94b, Ano97p, AT99, BMNL99, Cle91, Gar97c, PS98d, Por98, Rad97, Ros96d, She92f, DS98a, Fre94, GAK98, Koo97, Org98b, PS99c, Ros97a, Smi97a, Sta99a, Tay90].

IT-Systeme [BGH95b]. Italian [Alv98b, Don98]. Italy [De 95, IEE92d, Knu99c, Nat99b]. items [Uni97d]. Iterated

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

iterating [HNSM91]. Iterative [CDN98, Knu93b, MG91, LYG94]. itself [Ril96]. IV [IEE93a, BP98c, Far93, MD98, USE93]. I’ve [Bra95d]. IX [T+98].

Jan [WL92a]. JANET [You97]. January [ACM97b, ACM99a, Ano97a, Bih97c, SP90, USE91, USE92a, USE95a, USE96f, USE98d]. Japan [Ano93g, Ano99c, IEE96b, IRM93, IZ98, IZ99, Dre92, Win93]. Japanese [DR99b, Mea98, Wei99, Win93]. Java [ACM98a, Dra98, GA98, Ale98, AW99, Ano97u, Ano97v, Ano97-27, Bam97, Bar99, Ber97a, Ber98, Bro97, DDJ98e, DDJ98f, DDJ98a, DDJ99, Di 97b, DT98b, DE99, Fol99, Gar97a, Gar97b, GC97, Gar98b, Gar96c, Gau97, GPO98a, GPO98b, Gon98, GS98, HNS99, HH98, KHB99, Knm98a, Law98, MGL98, MF97, NK98b, PV98, TJ97, Tan98, Tre99, WBDF97, Way98, You96, Zuk98b, Zuk98a]. Java-based [Ale98]. Java/Smart [Bro97]. JDesignerPro [Ano97s]. jede [MPS94]. Jefferson [Bed90]. Jenayah [Ano97-29]. Jeopardy [Gar97c]. Jobs [RH93]. Johnny [WT99]. Joining [ARH95]. Joins [Law98]. Joint [Ano93g, Cla98a, FH94, IEE94f, IEE95c, Kat97, LW91, IEE92d, vT93]. Jose [Com96, FJV97, RP97b, SJ97, USE96c, USE96g, van96]. Jour [Lut98]. Journal [Eri97a, Zol93, OW95]. Journal/Logging [Zol93]. Journyx [Ano97s]. JSafe [Way98]. JTC [Gar97a]. Juan [CMM93]. Judge [GC97]. Judiciary [Uni96b, Uni97c]. July [AR97, AA97, BFS92a, BFS94, Com96, DG96, IEE95a, IEE97a, IEE94b, IEE97c, IEE98e, Sch98b, Sch99b, SIJ93, Un98c, Un98f, Un97c, USE95c, USE96e, USE96g, VPM97, Wat91, vWN99, Un98i]. Jump [DRR95]. Jumps [Gar97b]. Junction [CIBM99]. June [ACM95, And96c, AA97, GS94b, IEE92a, IEE94b, IEE94f, IEE96b, IEE96c, IEE97f, IEE98e, USE95c, USE96e, USE96g, VPM97, Wat91, vWN99, Un98i]. K-64 [Mas94]. Kahn [Ers99]. Kamakura [IZ99]. Kansas [Sin98]. Kapera [CWM91]. Kasmira [PNdbbbprm91]. Kawasaki [DP99]. kazdeho [Gar98c]. Keep [BK90, Riv98c, Sch95d, Way95]. Keeping [Dal97, Oko97]. Kelly [CFK91]. Kenmare [IEE96c]. KERBEROS [Hor94, ARH95, Ano93c, Atk93, BR97a, BP98a, BP98f, BM91a, Bar93b, Bru98, DW98, DS90b, Dav95, DG95, DGT96, De 93a, HRT96, IH99b, Kay95, Koh90, KN93, KNT94, Le199a, Lin96b, Lun90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts97, Tun99, Yu94a, Yu94b]. Kernel [BCC93, WB92]. Kerry [IEE96c]. KEY [YY98a, ANS97, ANS98b, AKP96, AAB97, AN95, IBM93, Ano94b, Ano94c, Ano94e, Ano95m, Ano97c, Ano99f, Ano99h, AA93, BP98a, BI95, BDH98, BDG98, BCE94, Bar96a, BCG90, BR94a, BR95b, BHSV98b, BHSV98a, BDP98, Ber97c, BS91b, BS97a, Bir98, BMS94, BWM98, BWM99a, BWM99b, Bla94b, BDT96, Bla96c, BPK99, BFK99, Ble97, BDHK93, BFS96, BDF98, BD99b, BF99c, Boy90, BM94b, Bra95b, Bra95c, BS94, Bur94b, BDS98, Cae96a, CC99b, CG99, CDN98, CJS91, CGM97a, CS98b, Cra98, Cus97, DDJ98g, DDJ98h, Dae98, Dam91b, DK96, Dan95, DDP90, Dav96, De 93c, DP98c, DB96, Di90, DH90, ECM96, FW91, FDB93a, FY95a, FY98a, FYM99, FBS98, FO99a, Fun98c, Fun93, GH90, Ga96, Gan96a, GKJ99, Gib91, Gih96, Gil99, GM90, GGH97b, Gys96, HK99a, HGS98]. Key [HP98a, HS90, HMT98, HMV93, Haw98b, HD96b, HJJ9x, Her97, HPS98, HFP99, HM98, HR90, Hwa97, Iss90, Jav90, Jas96, JV96, Ka99, KP99a, KSW96, KSW99a, Ke99a, KS99b, KP96b, KM99c, KT91a, KMOV91, KKOT91, KP93, RSA93f, Lan99, LM94b, LWY95, LSM97, LAA9, LP99, Low96, Low98b, Mah96, Mar97, Mat91, MY91, Mau93a, MW96a, Mau97a, MP91, Mv93, Men93, MM96b, Mic93a, Mic93b, MS95f, MM99c, MS99c, MKS99,
MSN98, MSN99, MTVZ92, MAO96, MM98a, MM98b, NMR95, NS97a, Nec96, Neu97, NS99a, Oka94, OU98a, Oka98a, Oka98b, Omm90, vO91a, PBR97, Pa99d, PKOT94, Pat95, Pin97, Poi99, PB99a, RSA93c, RSA94, ROT94, RS98c, RS98d, Ros96a, Ros96e, Ros97b, Ros98b, Ros98c, RCM99, SSN98a, SYMI98, Sam98, DP91, Sas99a, Sch94b, SKW99, SOOS95, SM95a, SE96, Sha99b, She94d, SiK93, SR96, Sta98, Sta99b, ST91, SW99b, SH94, Sun98a, Sut99, TAP90, Uni98i, Van95a, Van93, VSH97, VvT97, VBD99, WM93, dWQ91b, WLEB96, WW98b, WKS+99, Wie96, Wie97, Wie98a, Wie98b, Woh98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vW99, AAl95, Acc97, Lip98, AD97, AD99, AI 96, Ano90, Ano96m, BSNP96a, BSNP96b, Bao94, Bi94, BDHJ97, BD99a, BT99b, BSB97, BR96b, BCK98, BY93c, BY93b, BS91a, BFS92a, BGI+95a, BMP97a, BF96, Ble96, BMS96, BFS98, BM95, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Cra97, Cus95, DKR97b, DW96, DS90a, DH96a, Des95, Dv96b, Dv96, DN95b, ES97, FDB96a, FGLP96b, FL93, Gar96b, GH96, GIB94, GBL94]. Key [GH99, GTS90, HNSM91, HP99a, HP99b, HY93b, Haw98a, He92, HF96, HJJ+97, HI97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IZ98, IM96a, J96, JLM+94, Jon90, JY98, KASH90, KM99a, KSW97a, KSW97b, KL94, KIR96b, Kir95, Koo97, KM99d, Kos99, Kuu97, LG97, Las92, LM97b, Lee95, LC96a, LM94a, LZ90, LZ91a, LD94, LL95b, LCL95, Lon91, Lon92, Low95, MS98a, Mao97, MLA91, Man91b, MYY93b, MBB99, Mu92, MLL95, NM96a, NY90, Nat97a, Nec91, Odd94b, Ole95, PS98e, PS98f, Pet91, PP92b, RT93, Roe99, Sal90, Sal96, SW95a, Sch92c, Sh95a, She96a, She92c, SKB97, SY96b, SM90, Sm93b, SS95b, SS95c, STW95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC99b, TC99a, Ts90, TC91, Tze99, TH99, Uni97c, Uni95a, VW96, Ven92, Van92b, Wie94]. Key [Wil93b, Xie92, Xie93, XLP99, XW97, Yam98a, YL97b, Yua9, Zha91, Zhe95a, Zhe95b, ZPY96, vO91b, vW91, vO92, vT90, MC96, BFS92b]. Key-Agreement [RSA93c].

Key-dependency [MAO96].

Key-Dependent [FBS98]. Key-Escrow [vV97]. Key-Exchange [Dan95].

Key-management [MLA91].

Key-Recovery [Oka98a, Oka98b].

Key-Schedule [KSW96]. Key-Search [KP99a]. Key-Share [BWM99b].

Key-signing [Ros96a, Ros96b, Ros96f].

Key-specific [LMS97]. key-vowel [Lip98].

Keyboards [CFK+91].

Keyed [Ano95a, BFN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pre95b, MS95e, BFN98a, Gon95, KBC96]. Keyed-Hashing [KBC97]. Keyed-MD5 [KBC96]. Keying [BCK96d, BCKxx]. KeyNote [BFK99].

Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Dai98, EHS96, G91, KSH97, KSW98, KM99c, Luc98b, MP91, PS98e, SV99a, SV99b, Ste94a, Van96, Way96b, Bih94a, CH97b, CL99, DV94c, JP96, KC95, Km95, LL93b, MB99, MF97, Mok97, SS97a, SS97b, SV98, SH99, Sta95a].


Kleptographic [YY97b]. Kleptography [YY97a]. KMOV [Ble97]. KN [SKM98a].

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

knapsack-based [He92]. Knapsacks [CJS91, Ort95b, Ort95a].

Know [DDJ98b, Fly97, Hli97, Kir95, Mil95].

knowing [Ble96]. Knowledge [DDJ98b, Fly97, Hil97, Kir95, Mil95].

knowing [Ble96]. Knowledge-Based [Bie98].

Knowledge-Level [BMT98]. known [Ano91b, BK95a, MY93a, vOW91].

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

Knoxville [IEE94e]. Knuth [CFK+91].

KoMoD [SY99]. Komputer [Ano97-29]. Konstanz [Fum97].

Korea [Ano93g, KM96a, Rho93]. Korea-Japan [Ano93g].

Kudos [SvA+98]. Kunstliche [CWM+91].

kuo [XtTmW94]. Kuperee [DH96b, HS94, HS96b]. Kurz [Ger97].

Kyongju [KM96a]. Kyoto [Ano99c].

L [Lip98]. Labeling [BKZ98, KZ95, LvdLB96, LvdLL97]. Labels [ZK95].

Laboratories [Ano95d, Ano95e, Ano95j, Ano95m].

LABYRINTH [LS97]. Lac [CFG96].

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

Lai [LLG10]. Lake [IEE96d, USE95b].

Lambda [HRV99, GLV99].

lambdaProlog [NM99]. Lancaster [WSFC99].


LANs [She92f]. LANCASPE [Ril96, Ano94g, Ano94f].

Laptop [Ano93k].

Large [Bla93, BDHG99a, BDHG99b, CS97a, LO91b, LM95, NNEK97, PF94, Riv97a, SA95, SS90, She92a, Csi95, DT93, DL95, Frn90, FO093, Has99, MSDS90, Yan95, Yu92].

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

Last [dBB91, dB91]. Late [Bur99]. latencies [JG90].

Later [Sch95a, Gol97c, Roe95].

Latin [BSNP97, Son99]. Lattice [Ano97q, BK95a, CK99b, CC99a].

Lattice-Based [CC99b, CC99a]. Lattices [Dwo97, Ste98a, BV97]. launch [Tan98].

Launches [Gar97c]. Lausanne [IEE96e].

Law [And96a, Bro94, Cae96b, Swi97, Uni95a, Cli99, Way93c]. laws [Ano97-29, Cha94b]. Lawsuits [Lea99].

Layer [BB95c, FK99, Sar97, Wu96, Mye97].

Layered [Jun99, RC95]. layers [AP93].


Leave [Hus99]. Lectures [Dam99b, Fri96, PR98]. Lee [Sce92, LZ91b].

Lee/Alek [Sce92]. legacy [Un92].

Legal [CYY98, HA96, Mos98, Rad97, Ros95b, Wri94, Ame95, Ame96a, Sch93c].


Lempel [Mun91a, Mun91b]. lend [Ril96]. Length [BR99a, BR99b, GS94a, Sch94b, YY98a, CC98, Han94, KL95b, MPL99, Su98, ZPS93].

Length-3 [YY98a]. length-restricted
Logs [SK98a, SK99]. **LOKI** [BS91f, BKPS93, Knu92, Knu93c, Knu95, TSM95].

**LOKI91** [Knu93d, Knu93a, SF97]. **LOKI97** [BP598, RK98a, Rij95]. **London** [Ano93d, Ano97p]. **Lone** [Ano97r]. **LONE-TAR** [Ano97r]. **Lon** [CHN97, Len96, RHH93, SSS98, Pos93].

**Long-term** [CHN97], **Longevity** [Rot95b]. **Look** [Col96, Has99, Pf95, Zha97, GTGW94, Way91]. **Look-up** [Has99]. **Looks** [Sch97b, vD97, vS97]. **Loops** [SVA9+98, SH99b]. **Lorenz** [Car97b, Dav98d]. **Lose** [GPR98, Way96].

**Loss** [Law98]. **Lossy** [CI96]. **Lottery** [Riv97a]. **Lotto** [QD91]. **Lotus** [Dwo95]. **Louis** [Ers99]. **Louisiana** [ACM91, ACM97b, USE95a]. **Louvain** [Dan96, Q+98]. **Louvain-La-Neuve** [Dan96, Q+98]. **Low** [Ag92, Ano99c, Bla96a, Bla96b, CFPR96b, CFPR96a, CNS99b, DDQM98, DDP99, DDGM97, DFK99, GDD9+97, Goo96, Jak98, KSHW97, KSHW98, KKW99, KOT95a, KOT95b, Mil96a, Pia99b, PK95a, PK95b, Pen96, SKNO98a, SKNO98b, T99, Ano90, CJL9+92, DVQ96, Gol96a, MHW98].

**Low-Bandwidth** [BKV99, Pia99b, DVP96]. **low-density** [CJL9+92]. **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, CTT94, OK95, Sch99, Sga91b, St93a, vHPP93, GN95, KO96, KO97, Shp99b]. **LR** [BP98c]. **LSI** [SKNO98a, SKNO98b]. **Lu** [LZ91b], **L-Lee** [LZ91b]. **Luby** [BKR98a, BKR98b, Luc96a, Luc96b, PRS99]. **Luby-Rackoff** [BKR98a, BKR98b, Luc96a, Luc96b, PRS99]. **LUC** [Smi93b]. **Lucas** [BBL95, JQ97, LT95, SS95a, SS95c, XLP99]. **Lucas-based** [BBL95]. **Lucent** [MB99a]. **Lucifer** [BB94, BS91f]. **lun** [XITm94]. **Lunch** [DDJ98e, DDJ98f]. **Lured** [Che92]. **Lurking** [Joh96]. **lustre** [Alv98a]. **LVQ** [LSVV95].

**Lyon** [FR95a].

M [IEE97c, WG97, Mat91b]. **M.A.P.** [BBC98]. **M6** [KSW99b, KSW99c]. ma [XITm94, KP99b]. **MAC** [Mit92a, PVO95, PVO96, Pre97a, SRL98, SRY99, Yuv97, Ano93k]. **MacArthur** [Dre92]. **MacGuffin** [BS95a]. **Machine** [KP99a, NM99, PF94, QD91, Riv93b, Wic90, Cra92, Dav98d, Daw96, Kru98]. **Machines** [Bur99, CFK9+91, FMM99, SK98a, Dav98c, Jan95, Sel98b]. **Macintosh** [Sch94]. **Macquarie** [KG93]. **MACs** [AB99a, AB99b, BGR95, JV98a, NR98, PVO95]. **Made** [GSV99, Kra94a, Gol97c, KKL99]. **Maestro** [CFK9+91]. **MAGENTA** [Bib99a, Hub98, BBF9+98]. **Magic** [BD99a, JM99, AGLL95, Kah98c, RK98b].

**MagiCol** [GLSM99]. **magnetic** [Ano90, Gut96]. **Mail** [Ano93j, DN93, Got99, Ken93, Lin93a, RS98b, Sch95c, Sch95d, SH97, VJ98, Ano95c, Gar97b, LF97, Lin98a, Lin98a, Mit92a, Ri96, She96a, Str93a, Str93b, Bac95, Zeg93, Sta94a]. **MailSafe** [RSA94]. **Mainframes** [Deu97, Deu98]. **Mainstream** [Gar97b]. **Maintain** [Wed99]. **Maintaining** [CH94a, CHH97, Gar94]. **maintenance** [Uni94b]. **MAINZ** [PWU99]. **Majesty** [Ber96a]. **Major** [Law98]. **Majorities** [Cha90]. **Majority** [Mv93]. **Make** [Ano93e, GGM97, CM99d]. **Makes** [Ame96b].

**Making** [ASW99, CKN99, DDJ98e, DDJ98f, Des90b, Hir93, Lut98, PRS99, Sar97, Tra97, VM96, Way98, KBR98a, KBR98b, Wri98, Zaj97]. **Malaysia** [GO96c, WSFC99]. **Malicious** [PM98]. **Malleable** [DDN91a, BS99b, BS99c, DDN91b, Sah99].
Malo [QQG95, QG95]. Man [CFK+91, Mon96, IPNdbbbprm91].
Management [Ano99f, AWV99, AG99, Bla94b, BPK99, Col96, Dae98, FJP96, FY98b, Fun98c, Fun93, GM93a, GH96, KMP99, KFJ96, Neu97, Rob98a, SS99b, Yac99a, Yac99b, CWM+91, Hat97, L89a, MLA91, MKKW99, P89f, Pos92]. Manager [VDDR99]. managers [Sea95].
Maxims [DSB99, Bau97]. Maximum [DJK93, Kob99]. May [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, And96c, Ano97p, BV98c, CH96, CFG96, CMM99, Dam90a, Dam91a, Dan96, De 95, FIP93b, Fun97, GQ95, GS94a, Hei96a, Hei94, IEE92c, IEE93b, IEE94d, IEE94e, IEE95b, IEE97i, KG96, Man96b, Nyb98, PGV93d, QG95, Rue93, Ste99b, Un98d, Uni95a, USE99c, Uni98a].
McCurlcy's [WD98]. McEliece [Ber97c, CS98a, CC99, Gib91, Gib95, JM96a, KT91a, LDW94, Sm98a, vT90]. Mc Guiffin [RP95a]. McNeil [CFK+91]. MCS [Jia99]. MD [IEE94b, NIS02, PvO95, USE92b]. MD-x [PvO95]. MD4 [Ano95a, DBB91, Dob95a, Dob96a, Dob98, Dobxx, Ka91, Riv90a, Riv91b, Riv92a, Vau95, D91].
MD5 [MG98a, Ano95b, BA97, BCKxx, Ber93, Dob96b, GTJ94, KR95b, KBC96, MS95c, MR95b, OG97, Par98a, P95b, Riv92b, Ros93, T95, DB94]. MDx [SRL98]. MDx-family [SRL98]. ME [ZKOY99]. means [WD99b]. Measurement [RK99, SC99].
Mechanical [SYJ99]. Mechanics [PT95, Ros97a], Mechanising [BP98]. Mechanism
Minefield [Han94]. Mini [Jak99b].
minimally [CGM97b]. Minimax [All98].
Minimization [LE99, SBG99]. Minimizing [BR97b, SSN98a]. Minimum [Ano95m, Ano97b, DK96, FO99a, CC98].
minimum-weight [CC98]. Mining [DC98c]. Minneapolis [IEE97l]. Minnesota [IEE97l]. Minorities [Cha90].
MNNet [IEE98e]. MMPC [SS99c]. Mobile [AGY95b, BGS98, COZ99, FGS96, FJP96, Gar94, Got99, HP98b, KFJP96, KRJ98, LCN99, PKOT94, PW99, Pit96b, She94a, Ved93, Vig98, YY97c, AGY95a, FC94, GA98, Hwa93, OY91].
Modification [AKF94, FG98, Sel98b]. Modifications [NMR95, OMA98, Mol98].
Modified [BDGI98, NK98a, PBGV90, Wic90, CLW98, HWB93, LZ91b]. Modular [BP99b, CJS91, Cop95c, HCY96a, Kor93, MNSV97, Pai99b, PRAM98, SKBxx, TY92, N996a, TN996b, VDDR99, Yam98b, BGR98b, BCK98, CK93, HN94, ISO97, KAK96, LC98, Yam98a].
Modulation [BI99, She94c, SC96b, KSB96b, KSB97, SVWMB95, SOB98, VSB95]. Module [Mee98].
Modules [Ano97r, IH98, Mor97, Com94c]. Moduli [Hub91, Len98, Mau90, Wal99c]. Modulo [DR94c, PP92a, PP95b, PP95a, Tak98a, Tak98b, Zim99, BRR99].
Modulo-Place-Invariants [DR94c]. modulus [Tze99]. molecular [ARRW99, Ram92]. Molecules [GC98].
MON [YY98d]. Monetary [Gar97c].
Money [DDJ98c, MR98, DD95]. Monkey [YY98d, YY98b]. monograph [Lea90].
Montgomery [NM94, BP99b, Kal95, KAK96, Nac93, NMR95].
Montgomery-suitable [NM94, Nac93].
Montréal [ACM94c]. Moose [Ros96b].
moot [Ano96d]. Morphology [Blo99].
Morphometry [SC99]. Morse [Sch98i].
Moscow [CW94]. Most [BV96, KAK96].
motion [Nas94, ONT98, YEA+98].
MP3 [MB99a]. MPEG [DS97b, DS97c, DSS98, HG97e, HG97d].
HEG98, LT98, QN98a, QN98b, SB98].
MPEG-2 [DS97c, HG97e, HG97d].
AWV99, BM90, BG90, BS99b, BS99c, BS91b, DY91a, DDP99, DR94c, DD91a, DD91b, FCD98, FDB93a, FDB93b, GPT91a, GPT91b, GP99, GO93, HJPT98b, Jak98, KR96c, LW99, Mas99a, MY91, NO98, Pai98a, Pai98b, Ped91d, Ped91b, RS91, Sah99, DY91c, SCG99, TSY98, Yah94, An95k, BKR98a, BKR98b, DDB95b, Ell97, HJPT98a, LL99, MY93b, SB95, Sin95, SBTV99, DDB95a, non-Abelian [DD95b, DDB95a].
Non-biased [TSY98].
Non-carcinogenic [SBTV99].
Non-classical [Mas99a].
Non-Commutative [GPT91a, GPT91b].
Non-Encrypting [LW99].
Non-Euclidean [SCG99].
Non-Existence [DDB93a, DDB93b].
Non-Interactive [DY91a, GO93, MY91, BM90, BG90, DDP99, Ped91d, Ped91b, RS91, DY91c, MY93b, Sah99].
Non-invertible [NO98, BKR98a, BKR98b].
Non-linear [FCD98, Jak98, KR96c, LL99].
non-linearity [SB95].
Non-Malleable [DDN91a, BS99b, BS99c, DDN91b, Sah99].
Non-maximal [HJPT98b, HJPT98a].
non-Oracle [An95k].
Non-Perfect [Pai98a, Pai98b].
Non-Reachability [DR94c].
Non-repudiation [GP99].
non-secret [DDJ98g, DDJ98h].
Non-Synchronized [Yah94].
Non-uniform [AWV99].
Nonadditive [RV99]. nonce [KSL92]. nonce-based [KSL92].
Noncryptographic [Fei99].
Nondeterministic [Mol98].
nonequivalence [Mol98]. nongroup [SBVG99].
Noninteractive [GSV99, Ped91c].
Noninterference [MC92].
Nonlinear [Gys96, KT91b, MS99b, Pit95, Gol99c, RD96b].
Nonlinearity [MS90a, SZZ95c, SZZ95a].
Nonlinearly [MS94].
Nonmonotonic [COM93].
Nonoblivious [FNS92].
Nonperfect [KOS+94, OKT93, OK98, OK95].
Nonrecursive [Ruo94].
Nonrepudiable [LHW98]. non rigid [Nas94].
Nonsecret [DDJ98g, DDJ98h].
Nonsense [FJM+96].
Nonsupersingular [BS91a, MS93].
Norm [TK99].
Normal [Bra90a, Ran91, Mok97].
Normalisation [ZTR99].
Norwegian [Hel94, LW96].
Not-So [An99d, CM99c, Chr99a]. Notable [Bar94].
Notarization [SK97b, SK97a]. Notation [Sch99c]. Note [An95g, An95h, An96d, An96h, An97l, An97m, An98d, An99f, Bih99c, BPK99, EKK99, KM92, Roh99, Blu95, CJRR99b, ES97, GHS93, LM93c, MS98a, TX92, YL97a, Yu92].
Notions [BDPR98, BS99b, BS99c]. Notwendigkeit [KK97].
Novel [Ger99a].
November [ACM93a, ACM94a, ACM96a, ???90, An94d, Cio97, DEQ92, GN95b, HOQ97, HF97, IEE91, IEE92b, IEE97l, IEE98a, IRM93, KM96a, LO99, PS99b, USE96d, USE96b, USE99b, UU97b, XTM94]. Nox [Ts90].
NP [BD91, DDP99, DFKN93, GMW91, NOV93, Sch94k].
NP-completeness [Sch94k].
NRC [Wor96].
NSK [PP96].
NSN [Un94a, Un94b].
NSW [GN95b, KG93, VPM97].
NT [Bru98, Hil97, IH98, USE98a].
NTRU [HP98].
Nuclear [HRV99].
NULL [GK98].
Number [Ade98a, Aga92, AR99a, AR99b, BG98, BGM97a, BGM97b, Bi98, Bor95, Buc91a, BP97c, De 98d, JK99, KSW99d, KSF99, Koh94, LLMP90, LL93a, Lox90, Mat96b, Miy93c, PG90, ROT94, Sch90c, Sch97c, Shp99b, Wi99, BMxx, Bou94, CS97c, CB96, Cou99, CDE96, Cus96, CS96c, Gor93b, Jen96, Kall93b, K099, KK98, Lag90, LLMP93, McC90b, Me92, O'C94, Pom90a, Pom94, PP92a, PP92b, PP95b, PP95a,


On-Line [Cac95a, Cac95b, CDF95, Ell99, EGM90, EGM96, PUF99, SS99e, SS99f, Nai97]. On-Line/Off-Line [EGM90, EGM96]. One [BJY97, BHSV98b, BHSV98a, BdM94, BHH99, BM94a, BM96a, BM96b, BM96c, BKK98, BPK97c, DGV93, DDP90, Fab95, Gys96, HILL99, HT99, HYLT99, Mer90a, MSN99, New98, Riv98c, Ros94, Rom90b, Sch91b, Sch95a, TOU94, Un97a, Un97c, Un98a, Un98c, Un98d, Un98e, Un98f, Un98h, Un97b, Un98a, Un98c, Un98d, Un97c, Zhe90, Ano97a, BD95a, BK98f, CB96, DIB99, Dob98, Hwa92a, IE92d, MB94b, MZ98, Roe95, Sim98c, Ste95, Zhe90, Tao94, Tsu92b, Tsu92a, Wer93a, Wer93a, ZPS93, MAM95].

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

One-Key [Gys96, Tao94]. one-round [Wer93a, Wer93b]. one-step [Ano97].

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

One-Time-Password [New98]. One-Way [BJY97, BdM94, BM94a, BHH99, DDP90, Roe94, Sch91b, TOU94, Zhe90, BHH99, HILL99, HYLT99, Rom90b, BK98f, DIF99, Dob98, Hwa92a, IE92d, MB94b, MZ98, Roe95, Sim98c, Sze98, Tsu92b, Tsu92a, ZPS93].


Hor94, SY96b, Sta96b, Con98, Dra99].

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

OpenPGP [CDFT98].

Operating [CH94b, IEE93a, IEE99b, Mar98a, WABL94, AHdJF97, FM98b, SG96b, WABL93].

Operation [Ano96c, Bih94b, Bih96, Bih98a, Bih99a, HP99a, Wagh98b, Bih95a, Gla99b, Mon96, Pos92].

Operational [Car97b, RZ99].

Operations [DBVD96, Zie97, Win93].

Operator [Uni94a, BP98c]. operators [BP98b].

Ophthalmical [FCD98].

OPIE [MAM95].

opolizing [YY98d].

Opportunistic [BRW99].

Opportunities [MBB98].

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

Optimal [BP98a, BR94b, BR95a, BJJ97, BM96b, BM96c, Car94, FGMY97a, HK97a, HK97b, LC99, PR99, PLWSN99, ST94, SW97a, SW97b, Tay95, BJQ97, DP94, LL93b].

Optimality [Mas99b].

optimally [CGS97].

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

Optimising [DN95b].

Optimistic [ASW98, GJM99a, GJM99b].

Optimization [ARK99, DNNM98, RP98].

Optimized [EPR99b, EPR99a, SL99].

Optimizing [Cla97, MS99b]. Optimum [OK96b]. Option [Dra99, Bor93a, Bor93c]. options [Ros94, Sta97c].

Oracle [ANO95k, GHR99, Ano95k, Got99, MSO96].

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

Orange [IEE96f].

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

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

Ordinary [Mi93b]. Oregon [Auc98, USE90]. Organizational [FY99].

organized [Far93]. Organizing [OMV98].

Orientation [PJ99]. Oriented [AKF94, BDPSN95, BDPSN97, BLH99, Bel99, DB99, LCL92, MNSV97, Mas94, Ou99, PD99a, Rei92, SG99a, SG99b, SCT99, YLCY98a, YLCY98b, BGV97a, CW97, Fra90, HY93a, Hwa91, Hwa92d, LG97, LWC96, TCH+91, Wu92].

original [CS98a, PBBC97]. Origins [AK98, CFK+91]. Orlando [IEE93c, IEE94c, IEE96f].

Orleans [ACM91, ACM97b, B+96b, USE95a, USE98c].

ornamental [PNdbrpm91]. ORTES [ACC99].


Osaka [SKT99]. OSI [FL93, HS96a, Hor94, KW92, She93c, VG93].

OSPF [MBW97].

OSS [Pea97]. ossifrage [AGL95]. Other [Aga92, CG98, Des96a, Koc96b, KS97b, Koc95, Ros94, Wri98].

OTM [STSW99].

Our [Gad91, PT95]. Outlaws [HM91, HM92, HM95].

Output [CJM95, Bha94a, Sab94, ZPS93]. Outputs [SK96a, SK97c].

Overcomes [Mau97c].

Overview [GML94]. overflows [Mei98].

Overlap [AMP99]. Override [Bar97].

Overview [ASM98, BBP99, DMR96, Lan98, Lin93c, PGV92, YSS99, dRHG+99, Ger97, Ste98a, VNP98, YS91].

Ownership [Car95, CMYY98, BO96a, Oko96, QN98b].

ownerships [CMYY97, ZL97].

P [YT96, MS90b]. P-1 [MS90b]. P. [IEE97c]. P1363

A96k, Ano97y, Ano97z, Ano98i, Kal97a].

PA [AR97]. Pacific [Uni98e, Win93].

Pacifico [IZ98].

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

Packings [Mou99]. Pact [Bro97].

Pad [BR96a, Fil95]. Padding [CNS99a]. page [Ano97j, Hod97].

Pager [Gar98a]. Pair [Sch95f]. pairing [FRM99]. Pairs [Kwa93, Mi93c].

palace [Bar92b].

PalmPilot [DB99].

Palo
Panama [DC98a, DC98b]. 
Poker [KKOT91]. policies [KK98, MVZ93].
Policies [HK99b].

Polish [Blo98b, Blo98c]. Politics [Ele99, GLV99, Tes98]. Pollard [AM94b, And96a, Ano96f, Bar93a, Bar93b, CPOR97, Ell99, Gir99, Hat96, Wai95, Aus96, Abr97, Ban94, Bro96, Dam96, DJ96, Ele99, HAH94, Hof95, LKB+94, Rot95a, Tas98, Wad98, Zaj97].


Polynomials [SE96, She95c, CW91a, CGMW97, It991, Kob91c, LC96b, Odi94a, LC96c].

Positive [Dwo97, YY98a]. Positive [Jam98].

Positive [Jam98]. Positive [Dwo97, YY98a]. Positive [Jam98].

Potentially [Knu95]. Potomac [Ros99].

Potential [GQW+91, Nor95c, Uni96a]. potential [Knu95]. Potomac [Ros99].

Power [Ano99c, BS99a, CJKR99a, KI99, MDS99, PRAM98, SKNO98a, SKNO98b, Sha99b, T99+99, Goo96, SOB98].

Power [Ano99c, BS99a, CJKR99a, KI99, MDS99, PRAM98, SKNO98a, SKNO98b, Sha99b, T99+99, Goo96, SOB98].

Powers [SS95a]. pp [Ano97-28].

PPP [BV98b, Kas96, Kum98, LS92, Mey96, Sim96b, SM96, SM98b]. PPTP [SM98a, DDJ98c]. Practical [ASW99, ADBB99, AB96a, AWV99, Auv96, Av98, Bae95, Bowxx, CD96, CS98b, Dam91b, Dam94b, Dam94a, DS93, FO97, HBKL99, IH99a, Jne99, KTM+99, Ok93b, vO91a, PRS99, PV90, Sak97, Sch92a, SW93, Smi90, Sta96d, ZS93, vO91b, And93, AMS96, BI93, Bou94, Fra90, FOO93, FO98, HZ93, HNM98, HJ99, Jac90a, Jac90b, JG95, LL95b, PS98b, vO92]. Practically [Gut98b, Knu94a]. Practice [Bel99, DSB99, GN95b, IZ98, IZ99, LABW92, AN94, Dam99b, Ger97, LABW91, Sch93a, Sta99a, Sti95]. Practice-Oriented [Bel99].

Practice [Bel99, DSB99, GN95b, IZ98, IZ99, LABW92, AN94, Dam99b, Ger97, LABW91, Sch93a, Sta99a, Sti95].

Pre-assigned [SW99b]. Precautions [GQW+91]. Precision [Kal92].

Precomputation [LL94b, dR95]. Predetermined [Len98]. Predict [Kra90].

Predict [Kra90]. predicting [Gil97].

Prefix [MPL99].

Power-Analysis [CJRR99a].

PowerPC [UFC94].

Pricing [DN93, Ros94].

Pricing [DN93, Ros94]. Primality [Bos90, GJK99b, Lan99, Len90, Yan95].

Primality [Bos90, GJK99b, Lan99, Len90, Yan95].

Primary [Ban94].

Primary [Ban94].

Primary [Ban94].

Prime [Sch94d, Di97b]. Primes [BD93, GS99b, Lan99, Mih94, Riv91a, RS98e, RSxx, SII97b, SII97a, DII95, YWY99].

Primitives [SI94, She95c, JV98a].

Primitives [CF99, Pre98c, RIP95b, RIP95a].
principle [Dam90b, Gib90]. Principles [ACM99a, AN95, HGH98, KK99a, KG99, MG91, PRB98b, Zhe90, Sta99a]. Printer [Cou93]. Privacy [Ano94h, Ano95c, Ano97s, Avo98, Bac95, BBCM95, Ble98b, Car96, Cha92b, DL98, Elk96, FJP96, FHM98, Gar95b, Gar95a, IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, Ken93, KFJP96, Lin88a, Lin89a, Lin93a, Lut98, MW97, Mjo93, NKP99, Par98c, SY96a, SYMI98, SB97, SG96a, Sta94a, Tho96, Tra99, Uni98a, Uni98i, Ban94, Bro96, CM95, Car94, Cha92a, CK93, Cli99, Dom96, HM96, JMLW94, Mar95b, Mei96a, Mil95, Rot95a, Smi94a, Sta95b, Uni98d, Uni97c, VPM97, Zim96a, Zim96b, Gar95c, Ros97a, SS97a, SS97b, Sta94a, Sta95a, Zeg93]. Privacy-Protecting [Tra99]. Private [BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, Mv93, RSA93c, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts90, Wil93b, ZG96]. Private-Key [HR90, Mv93, RSA93e, DS90a, SS98b]. Privilege [ECM96]. Prize [GC97, Pin98]. PRO [Ano97r, Gar98c]. Proactive [CHN97, FGM97b, HJK97, HJ97, HJ9++, IBMxx, Jar96, Rab98, BCR98, FGM97a]. Probabilistic [Jak98, JO97, SF97, Sch91b, Tou93, Gol99a, GO95, HK90, Imp92, Lon91, TX92]. probabilities [Lew92]. Probability [BDG99, Gol96b, Koh99, TY94, AI96, MHH98, MA96, WM93]. Probable [BD93, NK93, DLP93, Gram]. Problem [Bon98b, Bon98a, BN96, CS96a, Cha90, DD99, DJL93, GO96c, HM98, KM99b, KR99b, MT99b, NS99b, OM99, Per99, RS99a, CPS95, HY93b, H97b, H97b, HMP95, LC97b, Mas97, Mc90a, NR95, O99, MS99]. Problem-Solving [Per99]. Problems [AA93, BD95a, Bra90a, GGH97b, KRS99, MC92, Poi99, Smi90, APDS93, Bea92, BFKL94, FR95a, HC95a, IEE97e, Lew92]. Procedure [Ada97a]. Procedures [Hig97b, Lin93a, Lee95, Lin88a, Lin94a]. Proceeding [BPR99]. Proceedings [ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, Ano95i, Ano98f, Br92, Bri93, Com96, GR95i, IEE95a, IEE91, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96d, IEE97i, IEE97j, IEE97k, IEE97i, IEE98e, MZ98, Nat99b, OW95, P99a, P99b, SL93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96e, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, A94d, Bl97c, B9++, B995b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fun97, Gol90b, HOQ97, Hir97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, KG93, Kun99c, KP99b, KK99b, Kra98, LOX99, LM98a, LW96, Lom97]. proceedings [MV91, Nyb98, OiDP98, Pre95a, QV90, QQ95, Q9++, Rue93, SZ93, Sp95, Ste99b, TM99, TV94, T98, Tv92, USE90, USE98d, VPM97, Vau98e, Wat91, Wie99, Wu93b, Yu92, vWN99, ACM93b, CH96, Clar99b, IEE94e, Sti94, Wal99a, BCB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fei91, Gol96d, GQ95, GS94b, He94, IRM93, Kal97c, Ko96b, Mau96b, PSN95b, SP90]. Process [AMP94, Knu99a, Roh98a, RS99c, YT96, CWM91]. Processes [Gar98b, Bea92]. Processing [Ano97h, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97d, IEE97j, IEE97k, INDI99, KV99, LMP99, LW96, Pin98, Pit95, Ano96m, DO99, DF97, Man98, S99a, T98, Wh90]. Processor [Gar98a, RB99, SW97a, SW97b, She92e, Sut99]. VVDJ90, Von92a, Von92b, DVQ96, She92c].
Processor-efficient [Von92a, Von92b].
Processors [Cla97, KK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
Prodigy [CFK+91]. produced [SSI97a, SSI97b]. Product
[GO96c, KSWH98a, KSWH98b, KSWH98c, GN95a, SS98b, Ano94h]. Products [Ano97r, Ano97s, Cha94b, Cli97, Los97, UU97b].
Professor [Swi97].
Program [BDFM99, FGY96a, LBMC94, FGY96b, LS98a, Pre97b, Pre97c, Uni95a].
[Bre99, DDJ98a, Jol95, Ste94b, vdWS97, vS97]. Programmers [Gar97c, Joh97a, Joh97b]. Programming
[IBM93, BGS96, CO98, Er97a, JDK+91, Ste90a, Ste90b, ACM99a, Gre94, GA98, LS98a, OA99, Sab94, vWN99]. Programs
[BK95c, DRR95, SG95, SH99b, WB95, Zwi98, B+96b, DFHR91]. Progress
[Ano96k, Ano97z, BDI+96, KSB96b, Woi93b, Woi93a]. Progressions [Mih94]. Project
[BPBV99, IB499, GH96, Mun98, DS90b, RCM99]. PROMIS [SSCP99]. Promise
[Law98, Los97, Mar96]. promises [Way93b]. Promotes [GO96c]. PROMS [IEE98e].
PROMS-MmNet [IEE98e]. Proof
[Bol98a, Bol98b, CD99, CDS94, FOO91, GMW91, 96, GMW96, NMV99, RS91, Zhe95b].
Proof-Based [Bol98a, Bol98b]. Proofs
[BG90, BG93, BD91, CD98b, DFK93, FS97b, GMW91, GO93, JMSI96, CDP95, DP94, Gol99a, PS96d, Sak97]. Propagation
[GPR98, SG99b, ZZ95c]. Properties
[Boy99, Con99b, KA99, MM90b, MS91, OK98, OS98, Tow93, VW98, WW98b, Zie97, BHH99, CD95, FSS94, KSB96a, Koh91a, PS93a, XZZ97]. Property
[CFGS99, DL99, LQRS98, SRY99, Uni97b, Ale98, BS95c]. Proposal
[ABK98b, ABK98c, ABK98a, BAK98, DR98a, KR94a, LM91b, Cli99, LM91a, RH92, RRSY98, Ban94].
Proposals [Dae99, VvT97]. Propose
[Gar98b]. Proposed
[CP91, Lea99, LL98, Nat92a, Riv93c, SB93, Wag98b, CJM96, Gua90]. Proposes
[SVB99]. Protect
[Sch94a, Sta95b, Cli99, KR96b, Way93b]. Protected
[CH94b, DY91f]. Protecting
[BO96a, Ble98b, Des90a, EHMS99, GMDS98, KRJ98, Lut98, Mar95b, MW98b, PT95, SYM98, Tra99, VP99]. Protection
[BGG95, CHN97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LQ98s, LvdLB96, LvdLL97, LML98, Per97, Sm90, Uni97a, Uni98i, ZK95, ZK96, Ale98, BBCP97, BBCP98a, BOD95, CPO+98, CHO+98, Cli99, DFHR91, GO96a, Ibb97, OPH+99, RP94, RKDB96, SY96a, Sta94a, T92, TSN93, Uni97c, YEA+98, FT95]. protections [HPA99]. protest
[Ano97-30]. Protocol
[ATAY98, Ano95a, BWM99b, BV98b, Bra95a, Bra96, Ch98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JIMP+98, JQ97, Kas96, KSW98a, KSW98b, KS98b, Kra99, Kum96, Low96, Mau94, MW99, Mey96, Moo92, NS98b, NS98c, OM93, RS96a, RS98b, SS98a, SH97, SM98a, SM95a, Sim96b, SM96, SM98b, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CTSxx, D96b, EVH93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS96f, SK97, Sim94b, TH99, WS97, WL94, Zhe95a, GM93a, Sar97].
Protocols [AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BG+91, BWM98, BWM99a, BCM93b, Ble98a, Bol98a, Bol98b, BD97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dam99a, DG96, DQ93, DS97d, Fei93, Fei96, FBS97, Fum98b, GM93a, Geh95, GS97, GMV98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IE98e, KKOT91, KGY92, KS97c, LHT93, LL97a, LHB96, LL95a, LS92, LM96, MB94a,
MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, SI93a, Sch94g, Sch96a, Sch94h, Sch99k, SSP90, Tou91, Tou93, AN94, AG97b, AG97c, AG97a, Aba99, ABC+98, BDIH97, BH93, BGOH+95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, C95, Dan97, Fei99, Hor98, HLL+95, JW01, LY93, LH99, LL95b, Lon97, Man95, Mas97, MILY93, Mau95, MW98c, NT93, PS98c, PS98e, PS98f, protocols [Pau98, PW93a, PKM97, SSG99, Syv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].

prototypes [Ano96m].

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

Provably [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, LM95, Mau91d, Oka93b, PS98e, Sh96, ZM90, BH93, Dam94a, FO98, Gol90c, NY90, PS95]. Provably-Secure [DY90, DY91d, DY91b, Mau91d]. prove [Zha96]. proven [DS93, Lea90].

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

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


Public [ANS97, ANS98b, Acc97, AKP96, AN95, IBM93, Ano96m, Ano99f, Ano99h, AA93, BBP98a, BI95, BDHJ98, BDG98, BCE+94, Bec99, BC95b, BHSV98b, BHSV98a, BDP98, Ber97c, BS91b, BFS92a, Bis98, BMS94, BPK99, BF99c, BSG4, CC99b, CG99, CJ95, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De 93c, DP98c, Di90, Eil99, FY95a, FY98a, FYM99, FGLP96a, FGLP96b, FO99a, GH97, Gal96, Gar96b, Gib91, Gib96, Gir91, GHH97b, GH99, HK99a, HSG98, HP98a, HY93b, HMS93, HL93b, HJJ+xx, Hess97, HPS98, HFPS99, IZ98, IZ99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MI91, Mau93a, Man97a, Men93, MM96b, Mic93a, Mic93b, MM98b, NS97a, NY90, Nek91, Nek96, NS99a].

Public [OD94b, Oka94, O99a, O99b, PS97, Pai99d, Pat95, Pin97, Po99, RSA94, RCM99, Rud91, Sa90, Sa96, DP91, Sas99a, SE96, She94d, Sni93b, ST91, Sun98a, Sut99, TAP90, VSH97, dWQ91b, We98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zim96b, dWQ91a, vO91b, AA95, AD97, AD99, Ano90, ADSW99, Bae94, BI94, BD98a, BS97, BS91a, Be94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cus95, DW92, Den90, DVQ96, Dhe98, DN95b, ES97, FGMY97a, GH96, Gib95, He92, HFW96, HJJ+97, JM96a, Jar96, Jon90, KASH90, KM99a, Kim95, KM99d, Kog9, LG97, La92, LMJW93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LCL95, Lon91, Lon92, Low95, M90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rae90, Roe99, SW95a, Sch92c, Sha95a, She96a].

Public
Public-Key [AKP96, Ano99f, Ano99h, AA93, BP98a, BFS98b, BFS98a, BDP98, Ber97c, BM94, BPK99, CF99b, CJ91, Cra98, Dif90, FO99a, GHR99, GHC99a, HG98a, HMV93, Iss90, Kal99, KM99c, KT91a, KMOV91, LM94b, Low96, MY91, Mic93a, Mic93b, NS97a, Oka94, OU99a, vO91a, PS97, Qin99, DP91, Sas99a, ST91, Sun98a, Wie98b, Yam98b, YST99a, YST99b, Ano96m, BFN92, FGLP96a, FGLP96b, GH99, HY93b, NY90, Nc90, Sal96, Smi93b, Yam98a, AD97, AD99, BMP97a, CC99a, Cle96, Cra97, DNV96, Dhe98, EN95b, ES97, FGM97a, KASH90, KM99a, KM99d, LM94a, LZ91a, LDW94, LCL95, Lon92, Low95, Mau91b, MY93b, NM96a, Ole95, SW95a, Sch92c, Sha95a, SS95b, SS95c, TC99b, Tze99, Ven92, Wan92b, XLP99, Yu92, vT90]. Public-key [BFS92b]. Public-Key-Based [Nec96, TAP90]. Public-Randomness [DP91]. Publication [Nat93b, HV98, Nat92b, Nat93a, Nat94a]. Publicly [Mao97, Sch99i, Sta96a, VBD99, FO98]. Published [Ano97c, Ano97d]. Publishes [Ano95j]. Pudding [Sch98i]. Puerto [CMM93]. Pump [KM93, TY99]. Purchase [KS97a]. Purchaser [RS99a]. Purple [Cur98]. Purpose [KP93, Sut99, Sch91b, Yu95]. purposes [Cl99]. pursuant [Cl97, UIT97b]. Push [Eri97b]. Pushes [Bar97]. Putting [DDJ9c]. puzzle [Bar92b, Gre90, WSFC99]. PVM [BSN95]. PVS [DS97d].


r [Riv98a, Hjo91]. R1040 [BP95b, R95b]. Raddology [CWM+91]. Rabin [BR96c, CW97, FS97b, QJ98b]. Rabin-Williams [JQ98b]. race [Kah91a, Sch99f, BGV93, BP95b, R95b, R95a, VCF+90]. Rackoff [BKR98a, BKR98b, Luc96a, Luc96b, PR99]. Radial [PJ99]. Radio [GB98, LU95, PK94, She92f, Tod97, UN94]. Radiology [DTDJ99]. radios [RP94]. RADIUS [RMR97a, RSMR97b]. Radix [Kor93]. ramified [KG95a]. ramp [SW98, SW99a]. Rampart [Re96]. RAMs [GO96a]. Random [BG98, BGM97a, BGM97b, Bir98, Cor99, Ell98, FW91, Fis98, FO90, FJRS96, GHR99, Gut98b, JH99, KK97, Mat96b, MP91, MS95f, MFG95, NR98, OS98, PS98b, Ran01, ROT94, Riv91a, Sil97b, W99, BR97b].
Bou94, Gol99b, IS97, Imp92, Jenxx, Kos99, Kuč92, Ler97, PC98, TSY98, Wal90.
Random-Number [ROT94, Bou94].
Randomisation [KI97]. Randomized [Mau91d, PSN91, BI94]. Randomness [BM99c, DIF94, DDP99, GW96, HL93b, KR94c, Nis96, DP91, Sot98, SB99, BGS95].
Rapid [KM93, GTS90]. Rate [BDGV93, BS91g, LKD98, Sti93a, Bla94a, BDGV96, KL95b, MHHMW98]. Rates [HK97, HR90].
Rational [KG95, Koz96, ST91]. raw [HG96]. Ray [Aga92, BALS99].
RBF [WKHG97]. RC2 [Ano97c, Bou94]. RC4 [MT99c]. RC4-like [MT99c].
RC5 [Ano97b, BR96a, BK98e, BPV99, GPO98a, GPO98b, KY95b, KY95a, KY97, KY98, KYxX, KM96b, MAO96, Riv95c, Riv95b, Riv95d, Sel98a, Yin97]. RC5-CBC [BR96a]. RC5-CBC-Pad [BR96a].
RC5-CTS [BR96a]. RC5P [KSW99b, KSW99c].
RC6 [BPV99, Con99b, CRRY99, RRSY98].
Re [FL99b, Jak99c, AGY95a, Bur98b, HG97d].
re-encoding [HG97d]. Re-encryption [Jak99c]. Re-issuance [FL99b]. re-sharing [AGY95a].
Reachability [DR94c].
Reached [Lea99]. Reaches [MB99a].
Reaching [Gar94, HH94]. React [Par98c].
Reaction [HGS98]. Reactive [MKI99].
Reactor [HRVV99]. Read [Sta97b, Coh96, LF97]. Reading [Eri97b].
Real-Quadratic [BBT94, BMT96].
Reapplication [Sch99c].
Reasoner [MD99]. Reasoning [AG97a, BM95c, DBS95, KM99c, MR95a, PK99, Var99b, Ger99b]. reasons [Ril96].
Reasessing [Neu95]. Reassure [MB99a].
Recasting [Sal91]. Receipt [BT94, SK95].
Receipt-Free [SK95, BT94]. receive [Way91]. received [Cli97, UU97b].
Recently-Proposed [Wag98b].
Rechnergestützte [MPS94]. Recipes [FBS97]. Recipient [WP90, Wai90, WK97].
Recognition [HCD99, HA96, WD99b].
Recognizer [WB94]. Recognizes [Pin98].
Recommendations [Ano95m, Kal98g].
Reconciliation [BS94, CM95].
Reconfigurable [BP99b, PJB99].
Reconstruct [HD96a]. Reconstruction [BC95b, BD98b, LH95]. Record [Har90, LCL92, Cha99b, CDEH+96, IEE96f, IEE98b, JML+94]. Record-Oriented [LCL92]. Recoverable [YY99b, YY98c].
recovering [PPB97]. Recovery [AAB+97, Int91a, DC98c, GQW+91, LK99, Miy96, Oka98a, Oka98b, Uni98i, WLEB96, HMP95, JML+94, NR95, Uni97c, Yeu99].
Recycling [SvA+98]. redefine [Gau97].
Redistribution [MSNW99].
redistributors [DF98]. REDOC [Nor95a, BS91f, CW91b, GN95c].
REDOC-II [BS91f]. Reduce [Hig97b, SVWM95]. Reduced [BBS99a, BKR97, MT99a, BBS98a, PNRB94].
Reducing [DSS98b, JQ98b]. Reduction [CTT94, GGH97b, BK98g, PP92a, PP95b].
Reductions
NP98b, Pad98, PHF99, Rab94, SC96a, SZT96a, SZT96b, SZTB98, TKS98, ZK95, BBCP98b, BD97, FGY96b. **Robustness** [AN95, MMST98, YMWP99, Irw98].

**Rockland** [G594b]. **Role** [Car97b, DDJ98d, JJ95, Lin96a, VC99, DL96, Dam96, Gua99, Mur93b, Sh98]. **Role-based** [JJ95]. **Role-Centered** [VC99]. **ROLLING** [PWU99]. **ROM** [Ano96i, GTGW94, Ros94, UFC94, Yuv97]. **Roman** [Has95]. **Rome** [Knu99c, Nat99b, Wol93a, Wol93b, DDJ98b]. **ROMs** [GTGW94, UFC94].

**Ron** [Riv93a, Riv95a, vdWS97, Woe97, vS97]. **Roosevelt** [Kah98c]. **Root** [Cop95c, JJ91]. **Rooted** [PB99a]. **Rooted-Tree** [PB99a]. **Roots** [Kob97]. **Rosemont** [IEE97g]. **Rosenheim** [Sha99a]. **Rosser** [Ole95].

**Rotation** [OP97, OP98]. **Rotations** [Con99b]. **Rotor** [Wic90, Daw96]. **Round** [BJY97, BS93a, DP94, Dob97, GC94, KTM+99, Nat99c, SZ96, SK98c, SK98b, BD95a, NBD+99, Wer93a, Wer93b, HT98]. **Round-Optimal** [BJY97, DP94]. **Round1** [Bas98]. **Rounding** [BV97]. **Rounds** [BBS99a, dB91, DBR+99, KR94c, BBS98a, Dob98, PNBR94, d91]. **Routers** [DMVC99]. **Rouge** [Mic93b]. **Rover** [Bis90].

**Royal** [Far93, Tv92, Don98]. **RPC** [SSH93]. **RSA** [Ano94b, Ano95f, AA99, And93, Ano95d, Ano95c, Ano95a, Ano95j, Ano95m, Ano96b, Ano97e, Ano97f, Ano97g, Ano97d, Ano97v, Ano97a, Ano97w, Ano98a, Ano99a, BT9D98, BQ95b, BQ95a, BR95a, BR96c, BQ97, Ble98a, BF97b, BDF98, BV98c, BD99b, Bon99, Bra95b, Bri90b, BM94c, ca99, Ch97b, CH98, CB96, CLL99, CMMTN94, CD91, Cle96, Coc97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, Cus97, Dav95, Dem94, DDL94, D9N5a, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FGY97b, FMY98, FY98b, FR95, GJK96b, GKR97, GGOQ98, Gill99, GM97, GTS90, Gro94, GS99b, HN98, HWF96, Hor98, Hub91, HP94, IM93a, IM93b, JQ97, JQBD97, JQ98a, KR95c, Ka97a, Kal98b, KS98a, Kir95, Koc94, Ko97a, Ko95b, KOT95a, KOT95b, KK96]. **RSA** [Len98, LHL94, LL95a, Lou91, MWA99, MLY93, Mau90, MW98d, MW98c, MSSF98, Mis97, Mis98, MS99c, Mue99, Mi999, NS98b, NS98c, Oka98a, Oka98b, OSA91, PP97, PP99, PW93a, Po999, PS98g, Rab98, RS98c, RSxx, SSI97a, SSI97b, Sam98, SKNO98a, SKNO98b, SSS98, Sch94m, Sha95b, SV93, SH99, Sil97b, Sil97a, Smil93b, TY92, Tak97, Tak98a, Tak98b, T+99, TT99, VV97, VMD90, VNM99, Ven92, Vv97, Wal98c, Way98, Wie90b, Wie90a, Wir98, XL99, YYY99, Zer96b, Zho94].

**RSA-120** [DDLM94]. **RSA-130** [Ano96b]. **RSA-Based** [CD96, GKR97, VNM99]. **RSA-cryptosystem** [Gro94]. **RSA-Implementation** [PP90]. **RSA-key** [FMY98]. **RSA-keys** [SSI97a, SSI97b]. **RSA-Like** [JQ97]. **RSA-Moduli** [Mau90]. **RSA-signatures** [Ev92]. **RSA-type** [BJQ97, JQBD97, CLL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b, T+99, TT99, VV97, VMD90, VNM99, Ven92, Vv97, Wal98c, Way98, Wie90b, Wie90a, Wir98, XL99, YYY99, Zer96b, Zho94].

**RSA-120** [DDLM94]. **RSA-130** [Ano96b]. **RSA-Based** [CD96, GKR97, VNM99]. **RSA-implementation** [Gro94]. **RSA-Implementation** [PP90]. **RSA-key** [FMY98]. **RSA-keys** [SSI97a, SSI97b]. **RSA-Like** [JQ97]. **RSA-Moduli** [Mau90]. **RSA-signatures** [Ev92]. **RSA-type** [BJQ97, JQBD97, CLL99, JQ98a, Koy95, KK96, Tak97, Tak98a, Tak98b, T+99, TT99, VV97, VMD90, VNM99, Ven92, Vv97, Wal98c, Way98, Wie90b, Wie90a, Wir98, XL99, YYY99, Zer96b, Zho94].
Secure
[SK94, SSSW98, Sas99a, Sch94a, SK98a, SK99, SM95a, SB94, SSM94, Sho96, Smi93b, Str93a, Str93b, Tay95, WP90, WD99a, WK97, Web98, Yah94, YST99a, YST99b, ZMI90, Zhe90, ZL99, Zo93, vHH97, BH93, Bea93, Bea96, BMS96, BP95b, Bow93, BM95, BD95b, CNST98, CGS97, CG05, Dam94a, Des90b, DS93, Des95, DVO96, FO98, GGK99, GM95, Gol90c, GB194, HY98b, HY98a, HC90a, Hwa93, HW98c, IS97, IKNY98, KC95, KS99a, Lam99, Los97, MS99b, NY90, OK96b, Opp96, Ped91b, Ped91e, PS95s, Rho94, RRSY98, Rom90b, Sar97, Sch92c, SKB97, Sim98c, Sin95, Sta97c, Ven92, YL97b, ANS97, Ano93j, Nat92b, Sta94b, Bou94]. secured
[Way98]. Securely
[RB94, DDFY94]. SecureNet
[Ano97r]. Securing
[BBi96, Des95, Lin96a, RG95, SG98, VJ98, Ano95k, DL96]. sécurité
[Sch98c]. Security
[AC93, ACM94a, ACM97a, AKP96, ADD91, AR95, ABDV98, Ala97, And04a, Ano91a, Int91a, Ano92c, Ano93g, Ano95f, Ano95b, Ano96i, Ano96a, ???97, Ano97e, Ano97f, Ano97g, Ano97a, Ano97w, Ano97x, Ano98a, Ano98b, Ano98h, Ano99a, Atk95b, AR98, Bal99, BCC93, Bas93, BKR94, BDPR98, Bel99, BG99, Bel92, Ber96b, BDR96b, Ble97, BPR99, Bov98a, Bov98b, Boy99, Bra90a, BK94b, BNP99, Com96, Com94c, CM97a, CH94a, CHN97, CGJ99, CG96a, CM97b, CT99a, Chr98, CGB93, CNS99a, Cor99, CN99, CG05, DMW94, Dan95, DS98a, Dav95, DG95, De93a, De98a, DDK98, Des92, Di99, DI99, Dwo95, ECM96, El96, EH96, FGS96, FS97b, FO99a, Fun93, Fum98b, GM93a, GMCF95, Gan96b, Gar97c, Gar96c, Gb96b, Gir99, GH95, Go98, GA98, Gut99, HHT93]. Security
[HHT97, HP99a, HP99b, HSK97, HH94, HLMW93, HXWM94, Hur98, IBMxx, IEE92a, IEE92b, IEE92c, IEE93b, IEE94c, IEE94d, IEE95b, IEE96c, IEE97b, IEE97i, ISO97, IH99a, JD91, JLO97, KY95a, KR96a, KY98, KTM99, Kau93, KA98b, KM96a, Kle90, KR989, KS97c, LOX99, LBMC94, LL94a, LL95a, Lom97, Luc97, Luc98a, Luc99a, MMST98, Mat96a, MS99a, MW98d, MSS98, MM98a, Mue99, Muf93, MM98b, Mü99, Mye97, NIS92, Ng99, NK03, Op99, OO98, OU98b, Opp97, PS98d, PS99c, PB97, PS96d, PS98h, Rei92, RB94, Rob93, Rob98a, Rog96, Rus90, Sch94m, Sch95c, SCH97, Sch97a, SSv98, Sch98f, SS99a, Sch98h, She97, SSP90, SS90, She92a, She92f, She93c, She93d, She94c, She94b, SK97d, Sun98a, Uni97a, Uni98a, Uni98b, Uni98c, Uni98d, Uni98e, Uni98j, USE90, USE92a]. Security
[USE93, USE95b, USE96e, USE96g, USE98d, USE99a, Van95a, VSH97, Van99b, Van99c, Ved93, Ved98a, Ved98b, VGG93, Ver98a, WCSS95, WOl98, Wol99, ZS93, ZFKP98, ZFK98, vT94, Ab99, AFB95, An093d, Bec97, BR96c, BCR96c, BDJR97, BKR98a, BKR98b, BBN96, B9+96, Bat95c, BHR99, Boy98, Bro96, Com97, Cha95a, CP94, Chi99a, Chi99b, CJ95, Cli99, CTSxx, Dan99b, DS90a, Den99, DEQ92, D*98, FF99, FM98b, Fra92, Gon92, Gru98, HN98, HK99b, HOQ97, HS96b, Hor94, HC95a, HC95b, HYS95, HLLC96, IEE94b, JT96, JT97b, JY95, KY97, KG96, Kat97, KS99b, KS97, KW92, Kuh98, Lai92, LTT95, Lee95,
LHW99, Len93, LC95, MW94, Mar95b, MSN97, Mas97, Man91c, MKKW99, MF97, Mei94, MW98c, Nor95b, PS99c, PS99a, PS99b, PS99c, PGV93d, PwO96, PR98.


Selecting [Bax97, CDFI95]. Selection [Hub91, Len99a, PNFK95, BM94c, Fei99a, GNI95a, Gol99c, KSB96a, MK92].

Self [AW99, BCD98, Fis98, Gir91, GPR98, Ki97, LC94, Man91a, MS95b, OMV98, SG99a, Sch99d, Jan95, MS95a, MiH96, Sch90c, Sch97c]. self-confident [Jan95].


Self-Reductions [Fis98]. Self-shrinking [MS95b, MS95a, MiH96]. Self-similarity [BCD98, Sch90c, Sch97c]. Self-Study [Sch99d]. Self-synchronised [KI97].


September [Ano98f, D+98, ES98, FR95a, IEE96c, IEE97e, IEE97k, Kat97, LW96, Q+98, Spi95, TV94, T+98, Uni97a, Uni96b, Uni98j, Uni98k, USE92b, USE96a, USE98b, Gar98a]. seq [Cl96, UU97b]. Sequence [LYH93, GM91, LY93, MHHMW98].

Sequences [DSV99, JQ97, MS94, Mun91a, Mun91b, PMP99, SB94, Bla94a, GNI95a, Gol99c, KSB96a, MK92]. sequential [LHW99].
s [IPndbbbrpr91]. Serial [SI93a, SSG99, Yor96]. Series [Ano95s, HEQL98, CJR98a, CJR98b].

Series-Parallel [HEQL98]. Serpent [ABK98b, ABK98b, ABK98a, BAK98].

Servant [CWM+91]. serve [Sch93c]. Server [Ano97g, Ano97h, BQ95b, BQ95a, DL99, ECD+99, HS94, HCY96a, Kon95, LYH93, LL95a, MW98d, NS98b, NS98c, Oh99, SVA+98, Wat99, Ano97d, BM94c, HS96b, Hor98, LY93, LW93, MW93a, PW93a, Sin95, Ts90].

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

Server-Side [SvA+98]. servers [Abe98a, AG95, CCMG97, GGK+99, Lee95, Ude98].

Service [FJ98, Gar98a, GH95, HS94, KMPS99, Kan93, MB99a, RRSW97a, RRSW97b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, Zha96, Ber96a, KN93].

Service-Level [MB99a]. Serviceability [WP90]. Services [ANS98b, Cas95, HV98, RB94, VSH97, Ved98a, AA95, AC97, DS90b, Don98, KW92, PS99b, You97, Zer96a, AA95, ACC97]. ses [Bon94]. Session [BR95b, BB95c, CFG99, CPM97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f,
Uni98h, Uni97c, Uni95a, Uni98k.

**Session-Layer** [BB95c]. **Sessioneer** [AG95]. **Set** [DJL93, FP99, IS91, Ko96, Mei92, Sta96b, SX90, GB98, Kra99].

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

**SHA** [ANS97, MG98b, BGV97b, CJ98, MS95d, MS95e, Sta94b]. **SHA-0** [CJ98]. **SHA-1** [ANS97].

**Shakespeare** [Lea90]. **Shallow** [ACD94, WF94].

**Shamir** [She92g, Ada92, GGOQ98, Nac93, OOK91, OO93, The95]. **Shamir-like** [Nac93].

**Shannon** [Sga91a]. **Shannon-theoretic** [Sga91a].

**Shape** [HHD99]. shapes [Ger99b].

**Shared** [BF97b, DHMR96, DF91a, DH90, HD96a, IS91, Lei99b, MWB99, PS98g, RZ99, SN96, Sim90b, Sim91, Sim94a, W199, YL97b].

**Shared-Memory** [Lei99b]. shareholders [LHL95b, LHL95a, Mao98].

**Shares** [MSNW99, BGD99, CDGV93, OK95, ZHS94].

**Sharing** [AGy95b, BC93a, BC95b, BBDW96, BK94a, BK95b, BDGV93, BD+94, BM99c, BD90, Bri90a, BSI91, Cac95a, Cac95b, CG98, CT97, CK90, DDP94a, DKK98, vD95a, DDL97, FDB93a, FGy96a, GJKR96b, GPSNW98, GPS98, HL93a, HKS97a, HKS97b, K196, Kra94a, KOS+94, KO99b, KOO95a, LP99, LCL92, LH93b, Mei92, MS95f, SN98, OK98, Pia98a, Pia98b, Ped91d, Rab94, ROTT4, Sch92b, Sch91, St93a, Wil98a, AGY95a, BC95a, BI93, BDV93, BDSV93, BCDV94, BGS95, BCDV96, BDGV96, BD97, BDV98, BG99, Bur96, CDGV91, CMAP97, CMGW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FGy96b, FR95c, FO98, GM95, GPSNW97, HJKY95, Hwa92d, HC96, HLC99, JMO95a, JMO95b, Jar96, KO95a, KO96, KO97, Mao98, MPSV99, OK95a, OKT93, OK96b, OK95, Pad98, PS98a, Ped91b, Ped91e]. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95a, van97a, Ko99].

**Shark** [RDPB96, WG97].

**Shawn** [Sha99a].

**Shedding** [HPG98, YHY98].

**Ship-Board** [NS98a]. shipping [An95k].

**Shooting** [Aga92]. **Shop** [An90t]. **Short** [Kra94a, Ste94a, Wie90b, vOW96, BC95a, Coh94, Har94, Joh94, VW96, Vv97, Wie90a].

**Shortage** [DDJ98a]. **Should** [Way93c, Y99, An95c, Riv98c]. shrinking [MS95a, MS95b, Mih96].

**SIE** [MS95a, Nat92b].

**SigACT** [ACM99a]. **SIGGRAPH** [ACM99c, B96b].

**Signal** [IEE97c, IEE97d, IEE97k, LW96, Pit95, She92]. **Signalling** [Lin98].

**Signals** [AK99, BTH96, DDNM98, MHHMW98].

**Signature** [AA95, Acc97, AW94, Int91a, NIS94, An96e, An97-29, BP97a, BM99a, BM99b, BM96b, BM96c, Bra93a, CS97a, CM99a, CG98, CH98, CK95, CDFI95, CD95, DMPW98, DQ94, DY91e, DN94, FL99a, FKM98, FOM91, FO99, GQW+91, HJJ+xx, KKS97, KS98d, KPG99, Kob98c, Kra93, LK96, LHW98, LK99, LM95, LHL94, LL98, MT94, MB99a, Mer90b, Mer97, MH96, MHHMW98, Mis98, Miy96, Mon93, Nat91, Nat92a, Nat94c.
Nat94a, NMVR95b, Na97, NMV98, NMV99, NIS93a, OFF93, Oka93b, PF94, Pet98, PM98, PS96c, PJ99, RGG97, RDK98, Riv93c, dR94b, SC96a, Sch93b, Sch94e, SK97a, SE96, Sim93, Sin98, SB93, SNSNP99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, ARK99, Ala93a, AW95, Ale97, BD98a, Bis90, Boy97, Bur96, CP95, CMTNY94, CSV94, DP96.

signature [FR95c, Gua90, HY93a, HJJ97, Hor98, HMP95, KS98c, LWC96, Mau91b, May97, MS98b, Mut92, NMVR95a, NR95, Pf96c, Pit96a, PS96d, PS98h, SI93b, Sha94, SS95b, SS95c, Ste95, Ti98, Tra97, TJ99, Wan92a, Wi93b, Wu92, XA98, YL95a, YL95a, Ye99, Zhao94, dR94a].

Signatures [ANS98b, ASW98, AT99, BD99a, BQ95b, BQ95a, BD99a, BM94a, BM96a, BC93b, BF99, Boy98, BS95d, CV99, CR91, CF915, Cq99, CD96, DM94b, DF91a, EG90, EM96, Ev91, Fro97, GKR97, GHR99, GM97, GO93, HK95, HA96, JM99, JQ99, JLO97, Leu96, LSV95, LR98, MS96a, Mis97, MBW97, NW98, OO98, Oka94, PJP97, PW93b, PV93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, Shi97, Tra99, Web98, Wri94, vHPP93, BR96c, BGR98b, Ble96, BCP91, BM91b, CM97, CPS95, Cha95b, Dam94a, Ev92, Ev93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, Ped91a, Pi96e, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].

Signicryption [Zhe97b, BD98a, Ye99, ZH98].

Sign [Ber97a, GM95, KT93, SKAM99, Sm98b].

Signer [Cv99, JQ99, JLO97, Leu96, LSV95, LR98, MS96a, Mis97, MBW97, NW98, OO98, Oka94, PJP97, PW93b, PV93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, Shi97, Tra99, Web98, Wri94, vHPP93, BR96c, BGR98b, Ble96, BCP91, BM91b, CM97, CPS95, Cha95b, Dam94a, Ev92, Ev93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, Ped91a, Pi96e, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].

Significant [DF999, SBV999, SM91, YY98a, ZZZ97].

Significant [BV96].

Signing [BGG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98c, KAK96, Ros96a, Ros96c, Ros96f].

Signs [E97b].

SIGPLAN [AC99a].

SIGPLAN-SIGACT [AC99a].

Silicon [NFQ99].

Silicon-On-Insulator [NFQ99].

[Mar98b].

SIM [V98a].

SIMD [C97].

Similar [P99].

similarity [B98c, Sch90c, Sch97c].

Simmons [D96b].

Simple [E97b].

Simple [E97b].

Significance [DF999, SBV999, SM91, YY98a, ZZZ97].

Significant [BV96].
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*98d, SS99a, Sch90a, SR96, SGPV98, Smi98a, Sut99, Tua99, VW98, Ver98b, DWQ91b, dWQ91a, ABKL93, AHdJJF97, Ale97, BGV97a, Cha99b, CW97, CJRR99b, DS98a, Dhe98, Di 97b, DF97, Gau97, Kip97, Sha95a, TJ97, Taa98, AG99, Bak99, BF99a, Bro97, DVQ96, Gir99, GTP96, HNS99, IW99, NFF99, SM94, SKAM99.

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

Smartcard [Ano98h, Ano99b, USE99c, Ano97-27, Ara93, Bam97, Ano98g, CH94b, IH99a, KK99a].

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

SmartLink [Ano93k].

Smooth [Odl94a, VZ97].

Snake [MSK99b].

Snefru [BS91f].

SNMP [Sta96c, VDDR99].

SNMP-CORBA [VDDR99].

SNMPv2 [GM93a, snoop [Ano94h]].

SOBER [Gar97b].

SOBER [BP99a].

Soccer [BL99, CM99d, INDI99, PWU99].

Societal [Sta97b].

Societies [IEE92d, IEE94f, IEE95c].

Society [Ano98f, IEE92c, IEE93b, IEE94d, Mar96, DL96, KG96, Taa98].

Socio [SM99].

Socio-technical [SM99].

Sockets [ZG96].

SOCKS [Lee96, McM96].

Soft [NS98a].

Software [Abr97, Ano93j, Anc96, AG99, Bal97, Bih97b, BD94, CD97, Cha98a, CT99b, DBVD96, DF91c, DSB99, Gar97a, GO96a, Gut98b, HK97, JJ98c, KP96b, LU95, Lac93, Lea99, Lut98, Mat96b, Mer91, MMB97, RSA94, RC94a, RC94b, SW94a, Sch99c, SK96a, SK96b, SK96c, SW97a, SW97b, SK97c, She95b, You96, And94a, Ano95k, Bih97c, BP97b, DH96a, Des95, Gol96d, Knu99c, Pre95a, SS98a, SAM97, Str93a, Str93b, Vau98e, Woo90].

Software-Optimised [RC94a, RC94b].

Software [MM95].

Solaris [NFQ99].

Solaris [Sun91b].

SOLID [Ano97c, CK95, Gut96].

Solution [GO96c, Lw98, LR98, WD98].

Solutions [HM98, MSK99a].

Solved [Ano97c, Ano98c, Ree98].

Solving [LO91b, Lew92, MSO96, OMV98, Per99].

SOM [BBN96].

Some [Ano98b, AT99, BBL95, BSI91g, CDG95, CRR99, CL98, Des98c, EvH91, FDB93a, Gd90, Gui97, HGH98, Hub91, HCY96a, Knu99a, KP95, KY9B98, La92, LP94, Lid90, M99, OK98, Sim97, TCH*91, Wag98b, Cao99, Cha95a, FDB93b, Gol97c, Lan96, R99a, SMK99b, TH99, Koo97].

Someone [MB99a].

Something [SvA+98].

Son [CFK+91].

soon [Pri94].

Sophisticated [Mei98].

Sought [Ano97z].

Sound [CIR99a, MGL+98, Ano96l].

Soundness [DE99].

sounds [BDC+95].

Source [Sch94g, Sch96a, Sch94b, Zim95b, Zim96a, Zim96b].

Sourcebook [Ban94, Rot95a].

Sources [ADB99, Cor99, Uni94c].

Southcon [IEE96f].

Southcon/96 [IEE96f].

Soviet [COP+95a, HK99c].

Space [SP [STP93]].

Space [AR99, BC95c, FP99, Gar97c, HK9L99, KV99, KI96, SCC99, BB190, Mra95, Pad98, Sze98].

space-filling [BB90].

spaced [Ito91].

spaceflight [CWM+91].

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

Spain [Mau96b].

spake [CFK+91].

Span [D9798, DQ94, HL93a, VBD99].

Spanning [Aag92].

SPARC [Sun91b].

Sparse [LO91b].

Spass [WABC99].

Spatial [SS95, DDQM98, LBB98, MCD98a, NP98b].

SPEakeasy [LU95].

speaking [LC95].

spearhead [Ano98h].

SPEC [DDJ98a].

Special [vD97, FT99b, MDP94, SS99e, SS99f].

Specific [ADB99, EvH93, Kha93, LMS97].

Specification [GBF93, HJTW99, LL97a].
[Daw93]. Summer [USE94, Mye96].
Summit [CFK+91]. sums
[BK98g, CFS97, Kob91c]. Sun
[Bro97, Gar98b, Got99, Law98]. SunOS
[Ste92, Sun91b]. Super [Sut99].
Supercomputer [DMS95, She92e, Bam97].
Supercomputing [CFK+91]. superhighway
[BDC+95]. Superimposing [YY91].
supersafe [PP96]. Super scalar [Cla97].
superscript [Cra92, CF92]. Supersingular [BS91b]. Supervisory [KA99].
Surrounding [GA98]. Surveillance [CKN99, SB97].
Survey [Bri90b, Gar97c, GFS93, Kal93a, Kle90, Knu98b, Par98c, BO92, Ele99, Mea95, She92b, Wad98, Zho94].
Syntactical [AW94], suspected
[LHL95b, LHL95a]. swapping [TN97].
Swedish [LF97]. Switches [Bec99]. Switching [MOM91]. Switzerland [ACM97a, BCB97, IEE96e].
sword [Den95]. Sydney [KG93, SP90, VPM97]. Sylvester [Por98].
Symbolic [Wat91, AM99, BH95R9].
Symbols [Pes97, CS99]. Symmetric
[Ada97a, Bir98, BDR+96, BFN98a, FO99b, Gom96, QG90, Roe94, YY98d, YY98b, BDJR97, Cra96, GHS93, HJ99, Hwa93].
Symmetry [BS95d, PS97]. Symposium
[ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97b, ACM97c, ACM98b, ACM99b, An99c, Com96, CM93, DEQ92, He96a, IEE92c, IEE93b, IEE94d, IEE95b, IEE96a, IEE97f, IEE97i, IEE98a, IEE99a, KK99b, Q+98, Spi95, S1J93, USE92b, USE93, USE95b, USE96c, USE96g, USE98a, USE98d, USE99a, Wat91, Wol93a, Wol93b, Ty92]. Synchronised
[Ki97]. Synchronization
[DHSS95, BCCG99]. Synchronised
[Yah94, Kon92]. Synchronizing [Mau91a].
Synchronous [AMP99, NT99, DGV94b]. Syndrome [CS96a, ZYR91, ZH90]. Syntax
[Kal97, Kal98a, Kal98b, RSA93d, RSA93e, RSA93e, RSA99]. Synthesis [HL99, Sab94].
Synthetic [PGV93b, PGV94]. System
system
[H97, Hwa92a, HC95b, KM98b, Kum97, LC96a, LCL95, MY93b, MKKV99, MM95, Oel97, PS90e, PWS95, Sch99j, SY96b, SS95b, SS95c, TCH+91, TC91, Ven90, WSFC99, WABL93, ADDS91, An91a, Bax97, Bel92, Dan95, JD91, RC91, Y99, ZH98]. Systematic
[BGH91, Zav99, Men95]. Systematising
[MKL99]. Systems
[BGH95b]. Systems
[ABL93, AKP96, AKF94, Ako99, Ano94j, Ano95l, Ano96a, ADEDS99, AA97, AMP99, BDP99, Bar99, Bas93, BR91, BBDF97, BFN98a, CF95, DDJ98a, Dam91b, DFTY97, DY91a, DD99, DB96, EN99, FJP96, FY95a, FY95b, FYM99, FO99b, GL96, GFB93, Gil98, GM90, GMW91, GK96, GS97,
GMV98, HGHD98, HJJ^xx, HH94, HP98b, IEE93a, IEE96b, IEE96d, IE98e, IEE99b, IH99a, KT96, Koc96b, KA99, KYB92, LO91b, LQRS98, LABW92, Lan99, Lee99b, Mar99, Mas99a, MS95f, MDF94, Mu93b, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes87, PL94, PS99f, PW97c, PS96b, PSN91, Pin97, Pit96b, PM99a, PD99b, RBvR94, RG95, RPS95a, ST94, SN96, STS99b, DY91c, SOOS95, SS90, SHE89, SY92, Stu99, Tra99, USE96c, USE99a, VC99, Var99a, Way93a.

Systems
[WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFJK98, ZFK^98, ARK99, AHdJF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BF95b, CG05, DMW94, Dix94, Fro92a, Goo96, GK97, Gru98, HJJ^97, IEE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Oht96, Ole95, Opp96, PAK98, PA98b, PP92a, PP92b, PP95b, PP95a, RO96, SK97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DV96].

Systolic
[SSS98, DF92, PJBM90].

SZ42
[Dav98d].

SZK
[GSV99].

T
[YT96, PDGI99].

T-Team
[PDGI99].

T52
[Dav98c].

T52e
[Sel98b].

Table
[KK98].

Tableaux
[Mas99a].

Tableaux-99
[Mas99a].

Tables
[DRR95, JC98, lPNdbbbprm91].

Tactical
[IKM99].

Tagging
[Lud97].

Tailoring
[CGM96].

Taken
[GQW^91].

Tale
[Kal98e, RS98f].

Talent
[DDJ98e, DDJ98f].

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

Talking
[HH99a].

Tamper
[Auc96, BDHJ98, KK99a, Zhe95b].

tamper-proof
[Zhe95b].

Tamper-Resistant
[Auc96, KK99a].

tamperfree
[Hwa92b, Hwa92c].

Tampering
[CL98, CL97b].

Tanaka
[Hwa92a, MS98a].

Tandatangan
[Ano97-29].

Taos
[WABL93, WABL94].

tapestry
[MB94b].

TAR
[Ano97y].

Targeted
[Cap94].

Targets
[Lea99, Way98].

TAS
[Cop94b].

Tasty
[Sch98i].

Tate
[FRM99].

Taxing
[Gar97c].

Taxonomy
[DB96, GS97, LBM94].

TC
[MB99b].

TC11
[Kat97].

TC6
[Kat97].

TC6/TC11
[Kat97].

TCFS
[Mau97b].

Tcl
[GA98].

TCP
[Fei93, Fei96].

TCP/IP
[Fei93, Fei96].

TEA
[KSW97a, KSW97b, NW97, WN95].

Team

TecPro
[GLC98].

Technical
[Ano95e, Bar96b, CFK^91, CYY98, DS97c, Lan98, LM93c, Mos98, USE99a, USE99d, VGP93, SM99, USE96f, USE98c].

Technique
[DDN98, Gne98b, KP93, WD97, BCV97, ONT98, Way95].

Techniques
[Int91a, BGML96, BWM98, Bol98a, Bol98b, BLM94, C99b, CD99, CMYY98, Dam90a, Dam91a, Dav91, DC98c, De 95, Des98a, Des96a, Gum97, Fun98c, GQ95, He94, JJ99a, LMDL96, MM99a, MSW99, Man96b, PS98e, PS98f, PK99, Pre93b, QV90, QQ95, Rue93, SZ93, Car98, Cra96, Hel93, He98b, ISO97, Kay95, KG93, Ny98, OP9^99, Oko96, PS99d, SD97, Ste99b, Way91, Woo90, ZH93, van96].

Technological
[UFC94].

Technologies
[Dan96, DSS98, Aus96, BGV97a, BK94b, BS95c, Oht96, Uni96a].

Technology
[Int91a, Ano96l, Ano98j, AA97, Ban93, BDDG99, DKK^98, Fol99, Gar98a, Gar98b, GN95b, Hat96, IH96, IEE94b, IEE98d, Lie94, Lin98c, NFQ99, Riv98c, USE99c, Ano93a, DS97b, Gil97, ISO97, Rit96, Ros94, Smi97a, VB96, CFK^91, Ers99, Ano99b].

Telecollaboration
[Fuc99].

Telecommunications
[IEE97e, UN94, Mac98].

Telemedicine
[Ano97-29].

Teleperubatan
[Ano97-29].

Telephone
[Gar97a].

Telephony
[Ban94, Gar97b, MB99a, Mar95b].

Teletteypewriter
[Mac98].

TELNET
[SSH93, Ala93b, Bor93a, Bor93b, Bor93c].
RH99, Sch99l, Sho97, Tro93, VBD99, Yac99a, Yac99b, ACC99, BP98d, BHS93, BM96b, BM96c, BK98f, GKS97, HS91, IEE94b, MAM95. time-stamp [HS91].


Univariate [Cop95c]. Universal [AW94, AS96, BE90, CadHSV96, EPR99b, EPR99a, KP99a, Sho96, Sti91b]. Universality [SS91]. Universally [Abe98a, BC93a]. Universe [Ros95a].


Untraceability [WP90, Wai90]. Untraceable [OO90]. Untrusted [SK98a]. Untruths [For99]. Unveil [GC97, Gar98a]. Unveiling [Jan98]. Unveils [Gar97a, Gar98b]. Update [Ano94i, Ano95a, Ano95n, Ano96b, Ano96k, Ano97v, Ano97y, Ano97z, Ano98i, MGL+98, Pin98, Ros95b, Ros97b, Ste99c, Wie97, Wie98a]. updated [Ano97t].

upon [BMP97a, CCH98, LCL95]. Upper [FM98b]. Usage [End97]. Use [ADBB99, BCE+94, Bra90a, CFGS99, Con99b, Gan96a, Gar97a, Gar97b, GC97, G98, HJL99, Iss90, KR95c, Koh90, Lan99, MG98a, MG98b, Port91, Rud91, SB94, Zuk98a, BDHJ97, BR97b, Cha94b, Cli99, CG05, Gil97, Jol90, Ril96, Way93c, Zer96a].

Used [GS94a, SZ96, Car97c, Car98, Gau97, Kuk99, Sch91b, SX90, van97a]. USENET [Bis91]. Useunix [USE99d, Com96, Ros96a, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c].

User [AKF94, BE90, Bus96, Dra99, Gog99, Gol90a, GN95b, IS99, KCCT94a, KCCT94b, PMP99, RRSW97a, RRSW97b, SYMI98, SCT99, Zim95a, DF91b, MC96, Mu92, RSA94, RT93, JS98, Sta95b].


Username/Password [Lee96]. Users [Hel98a, WK97, Sta94a]. Uses [Swi97, DKR97b, Sch99g]. Using
ANS97, ANS98b, Ada97a, AGS97, AHdJF97, Ano99h, BDP5NSG97, BC96e, BBS99a, BFP99, BW98, CIBM99, CK95, CM99d, Des96a, DS97d, ESST99, FVEA99, FW91, FY98b, GM97, GAGCDAFC99, GS99a, HNSS99, HRVV99, HJPB97, IR99, JM99, JI98c, JQ97, KR94b, K99a, KA99, KT93, L992, LF99, ML98, LW99, LD97, MAM95, Mih94, MCD99, Mis97, MFG95, NT99, NHB98, NNEK97, Oh99, OOK91, Ou99, OMI93, PSB97, Pin97, PZ98, PJ99, QG90, RB99, SG95, SK94, S99a, SK96a, SK97b, SK97a, SK97c, SD99, SRY99, SR96, Sim94d, SHK99b, Sun91a, SZT98a, TAP90, TY99, Tou94, VN94, WKG97, WCS95, Yam98b, Yam99, YST99a, Y97a, YST99b, A99, Alt98, Ata94, BSNP96a, BSNP96b, BT99, BGR95, B93, Bih94a, BB95a, BB98a, BD95a, CW91a, CNST98, CC95].

Using [CGM97b, CPPK98, CB96, Cle96, Dan97, G99, 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, SZTB98, Tak97, V97, VP98, Whi93, WII93a, Yam98a, Zho94, dR95].

Utility [Zol93, Vu95]. Utilization [GBR99]. Utilize [MSO96]. utilizing [SW95a].


Veri-KoMoD [SY99]. Verifiable [Abe98a, AGY95b, CG98, Cre90, FR95c, GM95, Ped91d, Sch99i, VBD99, AGY95a, BD98a, Bur96, FO98, Mao97, MIL93, Ped91b, Ped91e, Sta96a]. Verification [Abe98a, AB97, BGR98a, Bo98a, Bo98b, CDF95, DS97a, GFB93, GS99a, HL92, MM99a, Na97, OMI93, PM98, PV98, SM95a, SY99, Tou93, WW98b, Y99a, BGR98b, Bo97, BS95c, Des90a, Dwo91, JC98, JW01, Mea95, YL95a, YM98, ZL99].


Verschlüsselungssysteme [Wal98]. Verschlüsselungsverfahren [Ger97]. Version [Ano97r, Ano97s, BC93a, BP98e, DBP96, FKK96, Gar97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, R93f, Lim99, MT99a, Mc96, R93a, R94, DY91c, SS99b, SM98b, WABC99, CLW98, GM93a, Gi95, Bor93b, Lin96b]. Versus [MGL+98].

Vertraulichkeit [FT95]. Very [HMV93, MSDS90, PF94, Yua92, SN94]. Veto [OK96a]. VHDL [Oel97]. via
[BR96b, BCKxx, BM95, BS95d, DS90a, DN95a, DN93, EPR99b, EPR99a, Fac99, HS94, JJJ99b, NW98, UFC94].  
Vibration  
[Nas94, NA95].  
VICS  
[OSA91].  
VICTOR  
[Pay99].  
Victorian  
[Abe98b].  
Victory  
[Mus92].  
Video  
[Ano97, BFW99, DLF97, DS97c, DSS98, HG97c, KRBS97, KH98b, LT98, MT94, SJ97, SB98, SZT98a, WKH97, WW98a, ZL99, BB90, BCB97, CPO98, CHO98, CKLS96c, DS97b, HG96, HG97e, HG97d, HG98, HW97, HW98a, Lam99, Oht96, QN98b, SHG98, SZT98b].  
Video-based  
[WKH97, BCB97].  
Video-Steganography  
[MT94].  
Vienna  
[BS95e].  
Viet  
[Mye98].  
Vietnam  
[Mye98].  
View  
[CK95, Lan98, MUSM98, MM96a, STP93, Ste91, ZL99, Ano97i, Pr99, UU97a, Wad93].  
Viewpoint  
[Ste91].  
Views  
[DDJ98e, DDJ98c, DDJ98f, DDJ98a, DDJ98d, DDJ98b, DDJ98g, DDJ98h, DDJ99, Eri97b, TLS99].  
VII  
[IEE99b].  
VIL  
[AB99a, AB99b].  
VIL-MACS  
[AB99a, AB99b].  
Village  
[Ber97b].  
Vinegar  
[KS98d, KPG99].  
VINO  
[DV94].  
Virginia  
[ACM93a, ACM94a, IEE94a].  
Virtual  
[DFGH99, GB98, HL99, CCH98, LS98a].  
VirtuFlex  
[Ano97b].  
Virus  
[BGG95, Hig97b, Nac97, LFS94, OY91].  
Viruses  
[Hig97a, Wh90, Coh94].  
VIS  
[BGH95b].  
Visa  
[Lea99, Gau97].  
Visibility  
[LE99].  
Visible  
[K96].  
[CK99, HCDC99, P99, SW95b, SKIT99, CS99, PR97b].  
Vision-Based  
[SKIT99].  
visit  
[JQ98a].  
Visited  
[FF95b].  
Visual  
[ABDS96, B96b].  
Visualisation  
[MM99b].  
Visualization  
[Jan99, PH91, GTGW94].  
Visualize  
[BW98].  
VLDB  
[Yu92].  
VLIW  
[Cha97].  
VLSI  
[CKM99, Mas91, Pai96, Pos98, Vad95, Zim99].  
VoD  
[GMDS98].  
Voice  
[CM97b, MB99a, Cha94, Int91b].  
vol  
[Ano97-28].  
volume  
[Kat97].  
Voting  
[Boy90, JT97a, Mv93, NR94, SK95, Sch99i, FOO93].  
Voyager  
[AHMS99].  
Vries  
[GLC95b].  
VRML  
[Gar97b, Gar98a].  
VSP  
[YEA98].  
Vulnerabilities  
[Sch98d].  
Vulnerability  
[Gar97c, AFB95].  
W  
[YT96].  
WA  
[USE99b].  
Wafers  
[Gar97a].  
Waggery  
[Ben94].  
Waldmeister  
[HLL99].  
Wall  
[HRT96, Law98].  
Wallet  
[CP93].  
Wallets  
[DT98a].  
Walsh  
[SPS97].  
Wang  
[vT93].  
Want  
[Rot97, Way93c].  
Wanted  
[Bra95d, Hil97, P98a].  
War  
[Alv98b, AK99, Dav98a, Don98, Law98, Mon96, Mus92, Rat96, Ros99, Wei99, Wil98a, Dre92, Mar98b, Hin93, Jol95].  
Warden  
[Cra98, Cra97].  
Warehouse  
[ERL99, TLS99].  
Warehousing  
[MMN99].  
ware [Den99, Rot95a].  
WARM  
[MPL99].  
WARM-UP  
[MPL99].  
Warned  
[Kah91b].  
Warning  
[Gar97c].  
Warrant  
[LW95].  
Warranty  
[FKMY98].  
Warranty-Based  
[FKMY98].  
Wars  
[GC97].  
warum  
[MP94].  
Was  
[CFK91, De98b, Kru98, Mon96].  
Washington  
[HHF97, USE98a, USE99a, DDJ98e, DD98f].  
WASS  
[PS99b, PS99c].  
Watch  
[Cha99a, R99a, Sch99b].  
watchdog  
[MP98].  
Water  
[WF94].  
Watermark  
[Ano97o, CL96a, ONT98, SY98, TRS93, WD96, vTO94, And98, An93a, CL96b, CMM97, PBB97, TOH98, XBA97, YEA98].  
watermarked  
[BP98b, BP98c, RRP97].  
Watermarking  
[Ahc98, ADF98, Ben99, Ber97b, BOD95, BO96b, BW99, Car97a, CL97c, CMM98, DDM98, DDM97, DSS98, EQ98, EL99, FBS98, GD97, GB98, GO96c, GH97c, HG97d, HG98, KR98, Kob97, LQ989].  
Was
MBB98, Mos98, NH98, OMA97, OMA98, PZ98, QN98b, RKDB96, SCxx, SZT96b, SZT98a, WK97, WD97, Xie98, YY99a, ZK96, BCCP97, BCCP98b, BBC98, BCD98, BP98d, BCV97, BO96a, CPO+98, CHO+98, CT99b, CKLS96c, CM97d, DQM98, DDM96, DDM98, DNSS98, HG96, HG97e, HG97d, HP99, HW97, HW98a, HW98b, Iw98, KH97, KH98a, MNN97, Nat97a, NO98, NP98b, ODB96, OP97, OP98, OP98b, Oke96, PHF99, SD97, SH98, SZT98b, TA97, TKS98, VP96, VP98, VNP98, Yeu97, Yeu98, YK98, ZKOY99.

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

Watson [CFK+91].

Wave [GO96c]. Waveguides [FVEA99].

Wavelet [LSVV95, KH97, KH98a, NO98, XA98]. wavelet-based [KH97]. Wavelets [Lut98]. Waves [Dal97]. Way [BJY97, BdM94, BM94a, BKK98, BP97c, DGV93, DDP90, GMDS98, Mer90a, Roe94, Sch91b, TOU94, Zhe90, BHH99, BK98f, DI99, Dob98, HILL99, HYLT99, Hwa92a, MZ98, Rom90b, Sim98c, Sta94a, Sze98, Tsu92b, Tsn92a, ZPS93, KSW97a, KSW97b].

Wayner [vdWS97, vS97]. Wayness [HT99]. ways [Den95], WDAG [TV94]. Weak [DGV94c, DYL98, Haw98b, Pit96b, Sze98, Vau96, FY95c, Haw98a, Knu95, SSI97a, SSI97b, YL97b]. Weakened [AB99a, AB99b]. Weakly [MP91].

Weakness [Cop99, KSW99a, Kie98]. Weaknesses [BMS94, DY91e, Kel99, KP93, Lan96, PA98b, RK98a, Rij99, SZ96, DGV94b, She96b, ZZ97]. weapon [Ano97]. weapons [Mie98]. Web [Ano97r, MR98, OW95, SA95, Sta95a, Ver98b, Ale98, Ano97d, Bal99, BMNL99, Cha99b, Dav95, DDK98, FL96, GGM97, GO96c, Law98, She96b, Ude98, WSC95, You96, ZL99].

Web-Based [ZL99]. Web-enabled [Cha99b]. WebTime [Ano97s]. Weighing [KR96a]. Weight [PK95a, PK95b, Pen96, She95c, BGH+95a, CC98]. Weighted [MPS99]. Welcome [Riv95e]. wen [XtTuW94]. Weren't [Kahn91b]. West [DDJ98c, Fra99, Hir97, Hir98]. wheel [Car97c]. Wheeler [Bar95]. Where [DDJ98c, DDJ98d, LHL95b, LHL95a, Van95b]. wherein [Lea90]. Which [Che92, EvH91, Ev92, EvH93, Gir99]. while [vdWS97, vS97]. Who [BCE+94, DDJ98d, Mar95a, Mon96]. whom [LC95]. Whose [Ano94j]. Wide [Al98, Dav95, OW95, She96b, CDEH+96, Wad93, HC95b]. widespread [Cll99]. Width [GM99b]. Wie [MPS94]. Will [DDJ98d, Gar97b, GC97, Gar98a, Wor96, Ano98b, Gau97, Mil98, Sch93e, ZKOY99].


Wisdom [JC98]. Wise [Ano06]. Within [BGV93, BGM97a, BGM97b, FL93, HJTJ99, KW92, MG98a, MG98b].

Without [BP97a, BMRW98, GHR99, Hus99, Len96, Luc98b, SG99a, Abe99, Ano98j, Ben94, Ble96, HY93a, HG97d, Hor95, IS91, JMO95a, JC98, KRR99, LM94a, LM94b, LWC96, Ped91c, PBBC97, Riv98d, Sak97, Smi94b, SS99e, SS99f, Wu92]. withstand [OY91]. Withstanding [SVxW91]. Witness [CDF94, FGY96b, FGY96a, RGV97]. Witness-based [FGY96b, FGY96a]. witnesses [She92]. Woes
| [DDJ98g, DDJ98h], Wollongong [PSN95b]. | women [Wil98a], won’t [AK95, ZKOY99]. |
| Woollongong [GN95b]. | Worchester [KP99b]. |
| Word [LMBO95]. | Words [HKL94, Ata94, AGLL95, CC98, SM90, Sta96b]. |
| Work [Abe98a, Ano97y, BK95c, CFSY96, Gar98b, MGL+98, Bko98b, KM98b]. | workfactor [Jas96, Kau96]. Working [DDJ99, Kat97, LM98a, MB99b]. Works [Ano96k, FJM+96]. |
| Words [HKL94, Ata94, AGLL95, CC98, SM90, Sta96b]. | Word [DDJ98g, DDJ98h], Wollongong [PSN95b]. |
| X-ray [Bel92, BALS99, KSW97a, KSW97b, Smi98b, Yu94a, Yu94b, PVO95]. | X [Bel92, BALS99, KSW97a, KSW97b, Smi98b, Yu94a, Yu94b, PVO95]. |
References

Anonymous:1990:IWH

Anonymous:1997:ACC

ANSI:1988:FIE

Anshel:1993:PMT

ANSI:1995:ANS

Arabnia:1997:IC1

Abdikalikov:1999:ERC

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


REFERENCES


W. Aiello, M. Bellare, G. Di Crescenzo, and R. Venkatesan. Security amplification by composition: The case...

**Abe:1998:UVM**


**Abeles:1998:SVP**


**Abe:1999:RDM**


An:1999:ODR


Angelo:1994:DFS


Alexi:1984:RRB


Alexi:1988:RRF


Acken:1998:HWA


ACM:1982:PFA


ACM:1983:PFA

REFERENCES


ACM:1985:PSA


ACM:1986:PEA


ACM:1987:PNA


ACM:1988:PTA


ACM:1989:PEA


ACM:1989:PSN


ACM:1989:PTF


REFERENCES


ACM:1998:PTA


ACM:1999:PPA


ACM:1999:PTF


REFERENCES


Asokan:1999:APT


Alves-Foss:1995:ACS


Apostolico:1985:CAW


Anderson:1995:SFS


Abadi:1997:RAC

REFERENCES

Abadi:1997:CCPa

Abadi:1997:CCPb

Abadi:1998:BMCa

Abadi:1998:BMCb

Aura:1999:SLM

Agarwal:1992:RSO

Atkins:1995:MWS
REFERENCES


REFERENCES


Aberer:1994:DUO


Akoka:1999:CDP


Abdelguerfi:1996:GEI


AlJabri:1996:UDU


Alabbadi:1993:IEC


Alagappan:1993:RTA


Alabbadi:1997:SCH

REFERENCES

Alberti:1470:TC

Alexander:1945:CHG

Alexandris:1992:FMC

Alexandre:1997:BSC

Alexandre:1998:JBP

Allen:1997:DEC

Allen:1998:SUM

Ahituv:1987:PED


References

Adams:1988:SRC

Adams:1989:SRC

Anderson:1997:CNK

Atanasiu:1999:ASE

ACE:1981:RPC

ANSI:1983:ANS

ABAECITC:1995:DSG
REFERENCES

ABAECITDISC:1996:DSG


AMES:1996:SDM


ANTON:1994:GDS


ARNAL:1999:SAP


ANDERSON:1996:NPE


AGNEW:1990:FEC


AGNEW:1993:DFE

REFERENCES


[AN86] Andrew:1986:TCB


[AN86] Andrew:1986:CSI


REFERENCES


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


Anonymous:1939:ITM


Anonymous:1960:CNH


Anonymous:1976:CCA


Anonymous:1978:CSD


Anonymous:1978:ODA


Anonymous:1980:ACS


Anonymous:1981:CHP

REFERENCES

Goldstine: A History of Numerical Analysis, 3(3) 293. 
DEN AHCOE5. ISSN 0164-1239. URL http://
dlib.computer.org/an/
books/an1981/pdf/a4400.
pdf. See [Rej81, SWT+
81].


89412-053-0 (vol. 2). LCCN ????

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

[Ano82c] Anonymous: 1982: NNPa
Anonymous. News and notices: Pioneer Award Es-
184, April/June 1982. CO-
DEN AHCOE5. ISSN 0164-
1239. URL http://dlib.
computer.org/an/books/
an1982/pdf/a2184.pdf;
http://www.computer.
.org/annals/an1982/a2184abs.
htm.


Anonymous. Back matter. In Blakley and Chaum [BC85], page ?? CO-
DEN LNCSD9. ISBN 0-
387-15658-5; 3-540-39568-
7. ISSN 0302-9743 (print),
article&issn=????&volume=1
0&issue=0&page=?. CRYPTO
84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, spon-
REFERENCES

sored by the International Association for Cryptologic Research.

Anonymous:1985:DEA


Anonymous:1987:EVE


Anonymous:1988:EVE


Anonymous:1988:ERH


Anonymous:1989:SZS


Anonymous:1990:SEL


Anonymous:1991:ESS


Anonymous:1991:FFL

Anonymous:1991:E


Anonymous:1992:AUd


Anonymous:1992:DES


Anonymous:1992:DDS


Anonymous:1993:ACT


Anonymous:1993:BRd


Anonymous:1993:CKR


Anonymous:1993:CSA


Anonymous:1993:CNh


Anonymous:1993:FSH

REFERENCES


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


Anonymous:1994:CNc

Anonymous:1994:DAX

Anonymous:1994:HSK

Anonymous:1994:ICI

REFERENCES

Anonymous:1994:KEE


Anonymous:1994:Lba


Anonymous:1994:PRP

Anonymous. Product review: Pretty Good Privacy is a privacy advocate’s plan to head off the government’s bid to snoop on data. Open Systems Today, 162:56–??, October 1994. ISSN 1061-0839. [Ano94h]

Anonymous:1994:Uc


Anonymous:1994:WAS


Anonymous:1995:AUC


Anonymous:1995:AUM


Anonymous:1995:EES

Anonymous. An E-mail encryption standard should be in place by April, providing for the incorporation of Privacy Enhanced Mail into the MIME standard. Open Systems Today, 168:26–??, February 1995. ISSN 1061-0839. [Ano95d]
REFERENCES


REFERENCES

Anonymous:1995:RLM

Anonymous:1995:SUE

Anonymous:1996:NIS

Anonymous:1996:RF

Anonymous:1996:ADX

Anonymous:1996:BCU

Anonymous:1996:CID

Anonymous:1996:CPD

Anonymous:1996:ENa
REFERENCES

Anonymous:1996:ENb

Anonymous:1996:ECC

Anonymous:1996:SCG

Anonymous:1996:SUS
Anonymous. Standards update: Standardization efforts for triple-DES continue; IEEE P1363 works toward integrated draft; PKCS #11 / Cryptoki Workshop held at MIT; more progress on S/MIME.

Anonymous:1996:TBAa

Anonymous:1996:TBSa

Anonymous:1997:RDSa
Anonymous:1997:AES

Anonymous:1997:AUC

Anonymous:1997:AWS

Anonymous:1997:AIR

Anonymous:1997:ARDa

Anonymous:1997:ARDb

Anonymous:1997:ADF

Anonymous:1997:CVC
REFERENCES

Anonymous:1997:DNH
[Ano97j]

Anonymous:1997:ENa
[Ano97k]

Anonymous:1997:ENb
[Ano97l]

Anonymous:1997:ENC
[Ano97m]

Anonymous:1997:EW
[Ano97n]

Anonymous:1997:HEW
[Ano97o]

Anonymous:1997:INI
[Ano97p]

Anonymous:1997:MNL
[Ano97q]
Anonymous:1997:NPA


Anonymous:1997:NPNb

[Ano97s] Anonymous. New products: NetTracker 3.0; ScriptEase: Integration SDK; JDesignerPro 2.1; VirtuFlex 2.0; PGP Version 5.0 for Personal Privacy; TeraSpell 97; FileDrive File Transfer Server; journyx WebTime. Linux Journal, 43:??, November 1997. CODEN LIJOFX. ISSN 1075-3583 (print), 1938-3827 (electronic).

Anonymous:1997:RCU


Anonymous:1997:RAJ


Anonymous:1997:RDL


Anonymous:1997:RDSb


Anonymous:1997:SFR


Anonymous:1997:SUE

Anonymous:1997:SUR


Anonymous:1997:SSA


Anonymous:1997:CBP


Anonymous:1997:UUS

Anonymous. *Undang-undang siber: Akta Tan-

Anonymous:1998:ARD


Anonymous:1998:CSIb

REFERENCES

Anonymous:1998:ICS

Anonymous:1998:EN

Anonymous:1998:Ea

Anonymous:1998:PCA

Anonymous:1998:SIb

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

Anonymous:1998:SUP

Anonymous:1998:TBF
REFERENCES


[Ano99g] Anonymous. L’inuktitut. World-Wide Web document., 1999. URL http://colourlab.com/arctic/inuktitut.htm; http://www.culture.fr/edm/fr/index.html. Follow the navigation panel link “Les écritures” to inuktitut. The author observes that the syllabary used for the Inuit language, Inuktitut, was created at the end of the 19th Century by James Evans, a Wesleyan missionary, inspired by stenography. Originally intended for transcription of the Ojibway language, it was later used for Cree and Inuktitut; only these three languages have been written in this syllabary. Examples of the syllabary are shown in links that can be followed.
from this page; another alphabet table is shown in the colourlab.com URL.

Anonymous:1999:SFU


ANSI:1997:AXP


Anderson:1996:CCA


Abbott:1993:INT

REFERENCES


Aumann:1999:ITS

Arazi:1993:AEA

Arensberg:1921:CD

Arensberg:1922:CSP

Adamson:1995:JSR

Abdulla:1999:OMS

**Adleman:1983:CCS**


**Aiello:1999:HPN**


**Aiello:1999:HSP**


**Ashenhurst:1987:ATA**

REFERENCES


REFERENCES

Atallah:1999:ATC


Atanasiu:1993:AEU


Al-Tawil:1998:NAP


Atkins:1993:CKE


Atkinson:1995:RIA


Atkinson:1995:RIE


Atkinson:1997:TMS

REFERENCES


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

Anderson:1996:NC


Alabbadi:1994:SDS


Alabbadi:1995:DSS


Angel:1999:JQH


Aspray:1988:RCD


REFERENCES


REFERENCES


REFERENCES


[Bar75]

Banisar:1993:BCE


[Bar93]

Banisar:1994:CPS


[Bar94]

Bao:1994:IRL


[Baro4]

Barker:1961:CSC


[Bar61]

Barker:1975:CSS


[Bar75]

Barker:1977:CHC


[Bar77]

Barker:1979:CEC


[Bar79a]

Barker:1979:HCCb

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


[Barker:1979:HCCa]

[Barker:1984:CSG]

[Barker:1991:IAD]

[Barker:1992:CSC]

[Barlow:1992:DPP]

REFERENCES


Barías:1997:NBP


Barnes:1999:ESJ


Barron:2005:DWP


Baskerville:1993:ISS


Bastian:1995:CCE


Bassham:1998:ETA

REFERENCES


REFERENCES


[BB89] Bennett:1989:EQC


Four volumes.

Barni:1997:RWS


Barni:1998:CPD


Barni:1998:DDS


Biguen:1997:ECM


Biham:1999:IOS


Blackburn:1996:EMS

REFERENCES

Bennett:1992:QC


Bauer:1983:KDP


Biham:1998:CM


Bertilsson:1990:CVE


Bleichenbacher:1995:SRL

REFERENCES


REFERENCES


Biham:1999:MMA


Biehl:1994:CPB


Blakley:1985:ACP


Bender:1990:IEC


Beimel:1993:UIS

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


REFERENCES


Burwick:1998:MCC

Barker:1988:ECT

Bigun:1997:AVB

Blair:1999:DRA

Baritaud:1993:SPK

Brucoli:1999:DHC
Michele Brucoli, Donato Cafagna, Leonarda Carn-

**Bas:1998:SSB**


**Blundo:1994:FDS**


**Blundo:1996:FDS**


**Barkee:1994:WYC**

REFERENCES


REFERENCES


Bellare:1996:KHF


Bellare:1996:MAU


Bellare:1998:MAD


Bellare:19xx:KMM


Bromley:1983:RFM

REFERENCES


REFERENCES


[Burmeister:1991:ALN]


[Bauspiess:1992:RCH]


[Brandt:1993:GPP]


[Bloecher:1994:FFS]


[Bloecher:1995:PLC]


REFERENCES


REFERENCES

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

Branwyn:1995:IRA


Blundo:1994:MSS


Bondalapati:1999:DDE


Boneh:1998:ARG


BenAyed:1999:MFP


Blundo:1999:PSS

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


[BDGI98]


[BDGV93]


[BDHG99a]


[Boneh:1999:FPL]

REFERENCES


[BDHJ98]


[BDHK93]


[BDI+96]


[BDJR97]


[BDL97]

REFERENCES


REFERENCES


REFERENCES

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

Beaver:1993:HBS


Beaver:1996:ASE


Beaver:1997:CBC


Beaver:1997:PPE


Becker:1982:EDE


Beckett:1988:IC


Beckett:1990:IAM

REFERENCES

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

Beckett:1997:ICP


Beck:1999:DPE


Bedini:1990:TJS


Beesly:1981:CIW


Behrens:1954:EUP


Bell:1977:IVU


Bellcore:1992:GRX


Bellovin:1998:CI

REFERENCES


REFERENCES


REFERENCES

163


[Bergmann:2009:DKR]

[Beth:1983:CPW]

[Beth:1995:MST]

[Beth:1998:Eu]

[Beutelspacher:1994:CIA]
Albrecht Beutelspacher. Cryptology: an introduction to the art and science of enciphering, encrypting, concealing, hiding, and safeguarding described without any arcane skullduggery but not without cunning wagery for the delectation and instruction of the general public. Spectrum series.
REFERENCES

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

Blaze:1996:MKC


Beimel:1997:RCP


Boneh:1997:EGS


Balfanz:1999:HHC


Beimel:1999:RCP


Boneh:1999:EPK

REFERENCES

Boneh:19xx
D. Boneh, Ed Felten, Bill Aiello, and Matt Franklin. 

Blaze:1999:KTM

Blum:1988:NIZ

Blaze:1998:PSS

Blaze:1998:FTR
Boyd:1999:EEC


Beth:1992:PCS


Blundo:1996:TBC


REFERENCES

**Bellare:1993:DPK**


**Baldwin:1998:PPR**


**Boyapati:1999:KSD**


**Bellare:1995:ICA**


**Bellare:1995:ICA**


**Bird:1991:SDT**

Bird:1995:KFL


Bruggermann:1995:VIS


Branstad:1977:RWC


Bellare:1999:SEP


Bellare:1997:PNG


Bellare:1997:PRN

REFERENCES


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


Blundo:1995:DRR


Bierbrauer:1996:OAR


Berkovits:1998:AMA


Benantar:1996:ACS


Bosselaers:1993:CWP

REFERENCES


REFERENCES


REFERENCES

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

**Bellare:1998:MTF**


**Bellare:1998:MOT**


**Brassard:1998:QCH**


**Bertilsson:1993:CPS**


**Bao:1994:RAF**


**Bao:1995:BFA**


**Breitbach:1999:CCM**

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


BIERMANN:1998:HKB


BIHAM:1991:CCC


BIHAM:1992:DCI


BIHAM:1994:NTC


BIHAM:1994:MOA

Biham:1995:MLC


Biham:1995:MLC

Biham:1996:CTM

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

Biham:1996:CTM

Biham:1997:CL


Biham:1997:CL

Biham:1997:FSE


Biham:1997:FSE

Biham:1997:FNI


Biham:1997:FNI

Biham:1998:CMM


Biham:1998:CMM

Biham:1998:IOS

E. Biham. Initial observation on Skipjack: cryptanal-


REFERENCES

Biryukov:1999:MC

Bishop:1988:AFDa

Bishop:1988:AFDb

Bishop:1988:AFDc

Bishop:COMPSYS-1-3-221

Bishop:1988:FEP

Bishop:1989:USS

Bishop:1989:FEP

Bishop:1990:AGD

Bishop:1991:AMU
[102x34] [Bis91] Matt Bishop. An authentication mechanism for USENET. In USENIX
REFERENCES

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


REFERENCES


Biham:1995:KPA


Blakley:1995:GPS


Blum:1995:DPC


Bocharova:1995:FEC


Buydos:1997:C


Biham:1998:CAXa


Biham:1998:CAXb

REFERENCES


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

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


REFERENCES


[Bla83] Richard E. Blahut. *Theory and Practice of Error Control Coding*. Addison-Wesley, Reading, MA, USA,
REFERENCES


REFERENCES


Barber:1999:AOD


Buldas:1998:TBL


Beth:1994:CCB


Baaz:1999:SDC


Brassil:1994:EMI


Brassil:1995:HID

J. Brassil, S. Low, N. F. Maxemchuk, and L. O’Garman. Hiding information in doc-
REFERENCES


REFERENCES

Brillhart:1975:NPC

Blum:1982:CFT

Blum:1983:CFT

Blum:1983:HES

Blum:1984:IUC

Blundo:1995:NDT

Blundon:1997:BCE

Bayer:1975:EST
[BM75] Rudolf Bayer and J. K. Metzger. On the encipherment of search trees and random access files. In Kerr [Ker75], page 452.
REFERENCES


REFERENCES

sored by the International Association for Cryptologic Research.


REFERENCES


REFERENCES

Bellare:1999:FDS


Bellare:1999:FSD


Blundo:1999:RMS


Bento:1995:RCI


Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD


Blackburn:19xx:NPP

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


Blackburn:1997:CTA


Biedl:1998:GMF


Blackburn:1994:WPK


Blundo:1996:TOB


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.


[Christoph Busch, Klara Nahrstedt, and Ioannis]

**Book:1985:SNP**


**Book:1985:SNS**


**Book:1985:VTA**


**Book:1985:CRE**


**Brickell:1988:CSR**


**Brickell:1992:CSR**

REFERENCES

Berghel:1996:IKP


Brassil:1996:WDI


Bull:1999:NMA


Ben-Or:1983:CSS


Boland:1995:WDI


Ben-Or:1990:EPP


Ben-Or:1988:MIP

REFERENCES


Ben-Or:1988:CTN


Bolignano:1997:TMC


Bolignano:1998:IPB


Bolignano:1998:IPM


Bolignano:1998:DDP


Bond:1947:FSC

Boneh:1998:DDP


Boneh:1998:DDH

REFERENCES


REFERENCES


[Bov98b] E. Bovenlander. Smart card security. Lecture Notes in
Bowers:1959:DSP

Bowers:1960:BC

Bowers:1960:TC

Bowling:1993:SEA

Bowers:19xx:PC

Boyd:1986:CPC

Boyd:1988:CCB

Boyar:1989:ISPb

Boyar:1989:ISPa
REFERENCES

[102x681]REFERENCES

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


[Boy97] Papers from the 5th IMA Conference on Cryptography and Coding.

REFERENCES


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


Baric:1997:CAF


Brinkley:1997:SFS


Buchmann:1997:OWF


Bailey:1998:OEF


Barnett:1998:AOD


Barnett:1998:FML

REFERENCES


Only the slides for the conference talk are available.

Beutelspacher:1991:EFS


Bellare:1994:EAK


Bellare:1994:OAEa


Bellare:1995:OAE


Bellare:1995:PSS

REFERENCES

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

Baldwin:1996:RRR


Bellare:1996:TCA


Bellare:1996:ESD


Bella:1997:FAK


Bellare:1997:MUR


Bellare:1999:CVC


Bellare:1999:CV1

Brassard:1981:TLT

Brach:1987:ERR

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

Brassard:1988:MCT

Brassard:1989:CCb

Brassard:1989:CCa

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

### [Brasard:1990:CCH]


### [Brassard:1990:ACC]


### [Brassard:1990:CCH]


### [Branstad:1993:RNW]


### [Brassard:1993:CM]


### [Brassard:1994:CCQ]

Gilles Brassard. Cryptology column – quantum com-

Bray:1994:UA


Brackin:1995:DCP


Brackin:1996:DCP

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

211


REFERENCES


REFERENCES

Brownell:1981:ODN


Brooke:1986:BRB


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB

REFERENCES

Brundrett:1998:KAW

Bentley:1999:SOE

Bryan:1967:CA

Brillhart:1967:SFR

Brickell:1983:SRK

Benois:1986:CSE

Biham:1990:DCD

Brown:1990:DPT
Lawrence Brown and Jennifer Seberry. On the design of permutation $P$ in DES type cryptosystems. *Lecture Notes in Computer Science, 434*:696–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349
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, LOKI and Lucifer. Technical report CS91-18, Department of Applied Mathematics and Computer Science,
Weizmann Institute of Science, Rehovot, Israel, October 1991. 36 pp.


M. Blaze and B. Schneier.

Boneh:1995:CSF


Bose:1995:ATV


Bruckstein:1995:SSD


Brunnstein:1995:IPR


Biham:1997:DFA

REFERENCES


Bakhtiari:1996:PAK


Bakhtiari:1996:PBA


Bakhtiari:1997:MAC


Blake:1999:ECC


Bateman:1989:NMC

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

Benaloh:1994:RFS

REFERENCES

org/pubs/citations/proceedings/stoc/195058/p544-benaloh/. ACM order no. 508930.


Budge:1976:RSB


Bur81


Bur84a


Bur84b


Bur85


Bur94a

REFERENCES


REFERENCES

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


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


Biryukov:1999:SA


Blake-Wilson:1999:ADH


Blake-Wilson:1999:UKS


Buchholz:1988:CQDc


Boyd:1992:RDE


Bellare:1993:CCT

REFERENCE

Beller:1993:BDK


Beller:1993:BDH


CBEMA:1981:ANS


CBEMA:1983:ANSa


CBEMA:1983:ANSb


Cachin:1995:LSS

REFERENCES


Callimahos:1989:TAZ

Callimahos:1992:HC

Campaigne:1971:REC

Campbell:1987:MBC

Cannam:1998:MDE

Cao:1999:CAR

Capecchi:1994:TGR

Carlet:1993:PBF
REFERENCES

**Carlsen:1994:OPA**


**Caronni:1995:AOR**


**Carter:1996:BAP**


**Carr:1997:WDA**


**Carter:1997:BLC**


**Carter:1997:CCC**


**Carter:1998:CCC**


**Carasik:1999:USS**


**Caswell:1995:EDA**

[Cas95] Deborah L. Caswell. An evolution of DCE authorization services. *Hewlett-
REFERENCES


Chren:1996:RDU


Clark:1981:ECC


Chen:1995:SIB


Canteaut:1998:NAF


Cai:1999:LBPa


Cai:1999:LBPb


Chun:1999:DMT

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

Chaum:1988:MUS


Canteaut:1999:NCA


Chen:1998:VIC


Carter:1995:DVD


Carlet:1998:CBF


Coppersmith:1985:AF


Chuang:1991:MER


REFERENCES


REFERENCES


REFERENCES

Certicom:1997:EC


Chaum:1987:DPD


Chaum:1978:ICP


Christoffersson:1988:CUH


Crawford:1992:AS


Coe:1995:DDC


Castelfranchi:1999:BMA

REFERENCES


REFERENCES


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

Chor:1985:RRL


Chor:1988:UBS


Catalano:1998:NES


Canetti:1999:ETP

REFERENCES


Cranor:2005:SUD

Canetti:1999:AST

Chen:1996:TAP

Chen:1997:KEM

Chen:1997:AUM
Liqun Chen, Dieter Gollmann, and Chris J. Mitchell. Authentication using mini-
REFERENCES


[B] Chor:1985:VSS


[C] Chen:1997:SSR


[CH94b] Paul C. Clark and Lance J.

Cai:1996:PEA


Carrel:1997:RIO


Chang:1997:SAG


Chen:1998:PFR


Corcoran:1999:SCB


Cordon:1999:AMD


[Cha85b] 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.

[Cha85c] David Chaum. New secret codes can prevent a computerized big brother. In Blakley and...
REFERENCES


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

Chaum:1985:SIT


Chang:1986:DKL


Chapman:1986:NFS


Chapman:1990:SDA


Chang:1986:DKL


Chapman:1986:NFS


Chapman:1990:SDA


Chang:1986:DKL

REFERENCES


REFERENCES

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

Chadwick:1999:IWS [Cha99a]

Chan:1999:WES [Cha99b]

Chau:1999:QCE [Cha99c]

Chesson:1973:CC [Che73]

Cheswick:1992:EBW [Che92]
Bill Cheswick. An evening with Berfer di whi c ha cracker is lured, endured, and studied. In USENIX [USE92a], pages 163–174.

Canetti:1997:MAC [CHH97]

Chiopris:1992:SBE [Chi92]

Chin:1999:HCD [Chi99a]
Shiu-Kai Chin. High-confidence design for security: don’t trust — verify. Communications of


REFERENCES


[CIBM99] Y. J. Cao, N. Ireson, L. Bull, and R. Miles. Design of a traffic junction controller using classifier system and fuzzy logic. Lecture Notes in Computer Sci-
REFERENCES

Clark:1995:SRP


Chabaud:1998:DCS


Collins:1999:DCL


Coster:1992:ILD


Coppersmith:1995:TCB


Coppersmith:1996:PMT


Charlwood:1998:EXA

REFERENCES

Charlwood:1998:EXS

Chari:1999:TSA

Chari:1999:CNR

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

Chee:1991:CNP

Chor:1990:SSI
REFERENCES

0558/papers/0435/04350299.pdf.

Chor:1993:CPT


Cole:1995:MDR


Chor:1998:PIR


Cox:1996:SRW


Cox:1996:SIY


Cox:1996:SSS

REFERENCES


REFERENCES


[Clint97] Bill Clinton. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 730 et seq. — received in the United States House of Representatives November 15, 1996, pursuant to 50 U.S.C. 1703(b). Washington, DC, USA, January 7, 1997. 5 pp. Referred to the Committee on International Relations. Shipping list no.: 97-0126-P.

[Clint99] Bill Clinton. A legislative proposal: message from the President of the United States transmitting a legislative proposal to protect the privacy, security and safety of the people of the United States through support for the widespread use of encryption, protection of the security of cryptographic

Chua:1999:ART


Cheng:1998:MVR


Culik:1979:SIS


Ciampi:1982:EVS


Chan:1985:NMP


| REFERENCES | 256 |

**[CM99b]**


**[CMKK98]**


**[CM99d]**

Canetti:1999:ECS

Charnes:1997:SSH

Chor:1989:SCT

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


REFERENCES


[Col64] F. N. Colaço. *Cryptography revealed, or, the art of translating and deciphering obscure writings, whatever the characters employed*. (Portuguese) De Santos e Cia, Pernambuco, Brazil, 1864. 93 pp. LCCN Z104.C68 1846.


REFERENCES


**CSL:1994:DES**


**CSL:1994:EES**


**CSL:1994:SRC**


**CERT:1996:PSA**


**CEC:1997:EST**


**Chiba:1999:AGD**

Conradi:1739:CDS


Conklin:1998:SCO


Conklin:1999:ESC


Contini:1999:DPD


Coombs:1983:MC


Coppersmith:1984:FEL


Coppersmith:1987:C

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


Coppersmith:1989:AID


Coppersmith:1994:DES


Coppersmith:1994:ACS


Coppersmith:1995:ACA


Coppersmith:1995:FSR

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


[263]


Corcoran:1998:MFS


Coron:1999:SRSa


Coppersmith:1986:DL

REFERENCES

Courville:1986:MCC


Courington:1993:PEA


Coutinho:1999:MCN


Cremonini:1999:CCA


Chaum:1987:ACE


Chaum:1988:ACE

Sponsored by the International Association for Cryptologic Research.

Camion:1991:KHF


Chaum:1993:WDO


Chae:1994:AMA


Chen:1995:NGS


Chaum:1998:E


Chung:1998:DWCa


Charney:1997:PSC


REFERENCES


[CS91] V. Chepyzhov and B. Smeets.

**Chabaud:1996:CSS**


**Chambers:1996:RLM**


**Cusick:1996:BNFb**


**Chamenisch:1997:EGS**


**Chambers:1997:RLM**


**Chen:1997:NIC**

REFERENCES


REFERENCES


REFERENCES

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

**Cusick:1996:BNFa**


**Cusick:1997:CRN**


**Ciminiera:1989:AMM**


**Calvelli:1993:ARS**


**Chabaud:1995:LBD**


**Cohn:1999:MC**


**Chaum:1991:CSU**

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


Chang:1991:BCC


Cusick:1991:RIC


Campbell:1993:G

[CW93] K. W. Campbell and M. J. Wiener. DES is not a group.


Chmora:1994:ECC


Chang:1997:SCO

Ceruzzi:1991:RGC

Coppersmith:1998:CT

Chang:1998:BSC

Craver:1998:TTL

Cao:1990:DKC
REFERENCES


Dalton:1997:KSW

---


---

Damgaard:1990:ACE

---


---

Damgaard:1990:DPH

---


---

Damgaard:1991:TPP

---


---
REFERENCES


**Damgaard:1994:PPS**


**Damgaard:1994:PPS**


**Dam:1996:RPG**


**Damgaard:1998:E**


**Damgaard:1999:CSZ**


**Damgaard:1999:LDS**


**Danisch:1995:RES**

H. Danisch. RFC 1824: The Exponential Security

Danthine:1996:ECM


Dang:1997:AAC


Darnell:1997:CCI


DRC:1985:AAN


Davida:1981:CAR

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

Davies:1985:MAA

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


REFERENCES

Davies:1998:E


Davies:1998:NIH


Davies:1998:LCM


Davies:1998:NIH


Dawson:1985:COL


Dawson:1993:CSG


Dawson:1996:CSR


Denning:1981:SRR

REFERENCES

**denBoer:1988:CF**


**Denning:1989:EET**


**denBoer:1991:ALT**


**denBoer:1994:CCF**


**Denning:1996:TKE**


**Daswani:1999:ECC**

[DB99] N. Daswani and D. Boneh. Experimenting with elec-


REFERENCES

DeSchutter:1999:ELC


Desmedt:1995:MNA


Desmedt:1995:MNS


DeSantis:1994:HSF


Davio:1985:EHS


Delaigle:1997:LCW


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

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

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


**DDJStaff:1998:NVc**

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

**DDJ98g**

**DDJStaff:1998:NVd**


**DDJ98h**


**DDK98**

Delaigle:1996:DW


Delaigle:1998:PAD


Dolev:1991:NC


Dolev:1991:NMC


IEEE Computer Society order no. 2190.

Darmstaedter:1998:BBW


Delsarte:1985:FCM

Davida:1990:KDS


DeSantis:1994:SSP


DeSantis:1994:KCQ


DeSantis:1999:NIZ


Darmstaedter:1998:LCS

deVries:1953:SMC


DeAlvare:1990:HCC


DeDecker:1993:USK


DeDecker:1998:ICS


DeSchutter:1993:TFA


DeSantis:1995:ACE


DeDecker:1998:ICS


DeSchutter:1998:TFA


REFERENCES

lected papers from issues of Cryptologia.

**Demirdogen:1988:FDM**


**Demytko:1994:NEC**


**Denning:1979:EOS**


**Denning:1982:CDS**


**Denning:1984:DSR**


**Denning:1984:FEA**

REFERENCES

Denniston:1986:GCC


Denning:1990:DES


Denning:1995:ESC

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

Denning:1999:IWS


Deswarte:1992:CSE


Desmedt:1988:SGC


Desmedt:1990:PAA

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


[Des96b] Y. Desmedt. Simmons’ protocol is not free of subliminal channels. In IEEE [IEE96c],
IEEE catalog number 96TB100047.

Notes in Computer Science, 1492:257–308, 1998. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic).


Dwight Deugo. Coffee talk: From S390 mainframes to

Dego:1998:SMS


Desmedt:1990:TC


Desmedt:1991:SGA

[DF91a] Yvo Desmedt and Yair Frankel. Shared generation of authenticators and signatures (extended ab-


Domingo-Ferrer:1991:DUI


Domingo-Ferrer:1991:SRT

REFERENCES


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

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

Domingo-Ferrer:1991:CTP


DiCrescenzo:1999:HFS


Dwork:1993:LCP


Ding-Feng:1999:CS


Donatini:1999:DES


Davida:1997:ACC

REFERENCES


REFERENCES

Association for Cryptologic Research.

[DomingoFerrer:1990:FSK]

[DH90]

[Dawson:1996:AAS]

[DH96a]

[Ding:1996:WKA]

[DH96b]

[Dhem:1998:DEP]

[Dhe98]

[Diffie:1980:CAM]

[DHM80]

[Dechamboux:1996:ADS]

[DHMR96]

[Desmedt:1998:AOC]
REFERENCES

Damm:1995:MH


DiGiorgio:1997:ISC


DiGiorgio:1997:JDJ


DiCrescenzo:1999:SAC

REFERENCES

[DiC99]

[Dia91]

[Ding96]

[Die88]

[Die82a]

[Die82b]

[Die88]

[Die90]
Whitfield Diffie. The adolescence of public-key cryptography (invited). Lecture Notes in Computer Sci-
REFERENCES

oice, 434:2–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340002.htm;

[DIF94]

[Din94]

[Dixon:1994:SSS]

[DJHP98]

[Dessmark:1993:MDD]

[Deavours:1985:MCM]
REFERENCES


REFERENCES

Deavours:1987:CYT


Daemen:1997:BCSb


Daemen:1997:BCSa


Dodson:1995:NFL

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


Daemen:1996:CRS


Diffie:1998:PLP


Demphlous:1999:DPL


Demphlous:1999:DPL

[DL99]


Davoine:1997:VCP

[DLF97]


DeMillo:1982:CP

[DM82]


Ding:1997:LMS


DeMillo:1983:PDS


delaStelle:1902:TCF

REFERENCES

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


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


REFERENCES

309


REFERENCES


[DOR99] Giovanni Di Crescenzo and Giuseppe Persiano. Round-optimal perfect zero-knowledge proofs. Information Pro-


REFERENCES


Peter de Rooij. Efficient exponentiation using precom-


Dreher:1979:PSC


Drea:1992:MUC


deRaadt:1999:COO


Dror:1989:SCG


Droste:1996:NRV


Dawson:1995:DIJ


Denning:1981:MKG


Dolev:1983:AAB

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


REFERENCES

Dutertre:1997:UPE


David:1998:SIC


Dwork:1998:CZR


Durham:1999:BOO

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

Dittmann:1998:RMV


Dave:1995:CBS


Desai:1999:CSC


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


**Duhoux:1990:DBA**

**Dumey:1994:CQD**

**De Vivo:1998:ISA**

**DeDecker:1992:HID**

**Dhem:1996:SSC**

**De Soete:1990:CAS**
REFERENCES


Diffie:1992:AAK


DiPorto:1994:VBC


Danielsson:1998:HKW


Davida:1981:DES


Dwork:1991:VSS


Dwork:1995:DCC


Dwork:1997:PAL


REFERENCES


REFERENCES


(ECD+99) ECMA. ECMA-219: Authentication and Privilege

Ellis:1975:PKC

Edwards:1915:CCT

Epstein:1956:FBC

El-Gamal:1985:PCS

Even:1985:PCC

Even:1985:RPS
REFERENCES


Estrella:1999:DED


Eigenthaler:1984:CGA


Evans:1974:UAS


EFF:1998:CSE


EPIC:1999:CLI


ElGamal:1985:PKCa

REFERENCES

ElGamal:1985:PKCb

ElGamal:1985:STA

Elkins:1996:RMS

Ellis:1997:SNS

Ellison:1998:CRN

Ellis:1999:PPN

Elvin:1987:CWW

Even:1993:CCS
Shimon Even and Yishay Mansour. A construction

Eades:1998:GDC


Ehrsam:1978:CKM


Ezawa:1998:ATS


Endler:1997:PSU


Enge:1999:ECT


Ezawa:1999:AEC


Eng:1995:SDE


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


Escott:1999:AEC


Estell:1980:BW


Evertse:1992:WNR


Even:1985:CSW


Evertse:1991:WNR


Evertse:1993:WNR

Falk:1988:DST

Fancher:1996:SCa

Farrow:1992:HIY

Farrell:1993:CCC

Ford:1997:SEC


Fox:1997:GGU


Fridrich:1998:RDW


Fenn:1996:MDD


Ferland:1994:PBC


Firoiu:1999:LER


FontdecabaBaig:1998:PNL

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

Fan:1999:DFS


Frankel:1999:NHG


Feak:1983:SIS


Feistel:1973:CCP


Feigenbaum:1991:ACC

Joan Feigenbaum, editor. *Advances in cryptology — CRYPTO ’91: proceedings*, volume 576 of *Lecture Notes in Computer Science*. Springer-Verlag,
REFERENCES


Feit:1993:TIA


Feit:1996:TIA


Feigenbaum:1998:C


Feige:1999:NSP


Feldman:1987:PSN

REFERENCES


Feghhi:1999:DCA


Fung:1998:PAE


Fuchsberger:1996:PCS


Fuchsberger:1996:PKC


Frankel:1997:ORP


Frankel:1997:PR


Feigenbaum:1992:CPM

[FGR92] Joan Feigenbaum, Eric


[FHBH97] J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, and L. Stewart. RFC 2069: An extension to HTTP: Digest access authentication,

Frederickson:1984:PRT


Frieze:1988:RTI


Fitzi:1998:TCP


Fiat:1990:BR


Fiat:1994:TT


Fiat:1997:BR

Filby:1977:TPT

Filby:1978:BRM

Filby:1995:FUB

Fips:1993:APG

Fips:1993:SHS

Fips:1994:EES

Fischlin:1997:ICM

Fischlin:1998:CLP
M. Fischlin. Cryptographic limitations on parallelizing membership and equivalence queries with applications to random self-

[Franz:1998:MMA]


[Franz:1996:CBS]


[Friedman:1996:AFR]


[Freeman:1997:MCN]


[Fellows:1993:KK1]

REFERENCES

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


REFERENCES


REFERENCES


[Crypto84] CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


Fagundes:1999:EGA

Frey:1999:TPD

Frankel:1998:RED

Fiat:1994:BE


Eiichiro Fujisaki and Tatsuaki Okamoto. Secure

Folmsbee:1999:AJT


Fujiooka:1991:EED


Forte:1999:BUT


REFERENCES


**Frankel:1990:PPL**


**Franklin:1999:FCT**

Matthew Franklin, editor. *Financial cryptogra-


**Franklin:1999:FCT**

Matthew Franklin, editor. *Financial cryptogra-


**Franklen:1989:TIC**


**Franklen:1990:PPL**


**Franklen:1990:PPL**


**Franklen:1990:PPL**


REFERENCES


REFERENCES


Ferguson:1997:CA


Fischlin:1997:SSP


Forsyth:1993:ACS


Figueroa:1994:FCB


Federrath:1995:SVA


Fiat:1999:DTT

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

Frankel:1999:SID


REFERENCES


References

Frankel:1995:EES

Franklin:1995:BWS

Frankel:1997:CEE

Frankel:1998:DPK

Frankel:1998:RMU

Frankel:1999:CRA
REFERENCES


ian Cryptogram Association (George C. Lamb Collection).


REFERENCES

Gait:1990:VCH

Gaj:1989:GCM

Galland:1945:HABa

Galland:1970:HAB

Galil:1988:SIC

Galvin:1996:PKD
James M. Galvin. Public key distribution with se-

[Gal99] 

[Gam88] 

[Gan93] 

[Gan96a] 

[Gan96b] 

[Gar77] 
Martin Gardner. Mathematical games: A new kind of cipher that would take millions of years to break. Scientific American, 237
REFERENCES


REFERENCES


Garfinkel:1996:JSC


Garber:1997:NBAa

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-capacity disks; “wrapping” software sales; Tonga offers domain name alternative. Computer, 30(4):25–27, April 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Garber:1997:NBC


Garner:1997:PTT


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

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


Girault:1988:GBA


Goffin:1997:LCP


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

Gemmell:1997:ITC


Gersho:1982:ACR


Gerling:1997:VKU


Gersho:1998:C


Gero:1999:NME


Gero:1999:RRA


Ghezzi:1993:RSS

[GGH97a] Oded Goldreich, Shafi Goldwasser, and Shai Halevi.

[GGH97b] Oded Goldreich, Shafi Goldwasser, and Shai Halevi.


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


REFERENCES

[102x681]REFERENCES
[102x681]368

RONIC). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http:/
/ww.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&page=276. CRYPTO
84: a Workshop on the
Theory and Application of
Cryptographic Techniques,
held at the University of
California, Santa Barbara,
August 19-22, 1984, spon-
sored by the International
Association for Cryptologic
Research.

[GGM86] Oded Goldreich, Shafi
Goldwasser, and Silvio
Micali. How to con-
struct random functions.
Journal of the Associa-
tion for Computing Machin-
ery, 33(4):792–807, Octo-
ber 1986. CODEN JA-
COAH. ISSN 0004-5411.
URL http://www.acm.
.org/pubs/toc/Abstracts/
0004-5411/6503.html. A
computational complexity
measure of the randomness
of functions is introduced,
and, assuming the exis-
tence of one-way functions,
a pseudo-random function
generator is presented.

[GH95] Frederic Gittler and Anne C.
Hopkins. The DCE secu-


[GH95] Frederic Gittler and Anne C.
Hopkins. The DCE secu-


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

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

Hopkins. The DCE secu-


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

[GGQ98] Henri Gilbert, Dipankar
Gupta, Andrew Odlyzko,
and Jean-Jacques Quisquater.
Attacks on Shamir’s ‘RSA
for paranoids’. Information
Processing Letters,
68(4):197–199, November
30, 1998. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
research.att.com/~amo/
doc/rsa.for.paranoids.
pdf; http://www.research.
att.com/~amo/doc/rsa.
for.paranoids.ps; http:
//www.research.att.com/
/~amo/doc/rsa.for.paranoids.
tex

[GGMM97] E. Gabber, P. B. Gibbons,
Y. Matias, and A. Mayer.
How to make personalized
Web browsing simple, se-
cure, and anonymous. In

[GGM97] Frederic Gittler and Anne C.
Hopkins. The DCE secu-


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

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

[GGMM97] E. Gabber, P. B. Gibbons,
Y. Matias, and A. Mayer.
How to make personalized
Web browsing simple, se-
cure, and anonymous. In


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

Gibson:1991:EGC

Gibson:1995:SDG

Gibson:1996:SGP

Gifford:1981:CSI

Gilder:1997:APD

Giles:1998:EFS

Gilboa:1999:TPR
REFERENCES

QA76.9.A25 C79 1999
Bar. URL http://link.
springer-ny.com/link/
service/series/0558/bibs/1666/16660116.htm; http://link.springer-nyc
link/service/series/0558/papers/1666/16660116.pdf.

Gingerich:1970:BRB


Girault:1991:SCP


Girard:1999:WSP

Pierre Girard. Which security policy for multiapplication Smart Cards? In USENIX [USE99c], page ??

Givierge:1925:CC


Givierge:1932:CC


Givierge:1978:CC


Garey:1979:CIG


REFERENCES

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

**Garay:1999:AOC**


**Goresky:1995:FRB**


**Gurses:1995:VCT**


**Goldreich:1996:PTU**


**Goldschlag:1999:RCC**


**Goldwasser:1999:PTU**


**Glenn:1998:RNE**


**Goldschlag:1999:BCC**

Gennaro:1997:RBU

Gotz:1997:DTC

Gligor:1979:OMA

Goldreich:1989:HCP

Gaskell:1996:ISC

Gladman:1999:IEA
Brian Gladman. Implementation experience with AES candidate algorithms. In National Institute of Standards and Technology
REFERENCES

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


In National Institute of Standards and Technology [Nat98], page 19. ISBN ???. LCCN ???. URL


REFERENCES

Gonzalez:1999:RMT


Gallant:1999:IPP


Gamage:1999:EMA


Goldwasser:1982:PEH


Goldwasser:1984:PE


Goodman:1985:NTK


Godlewski:1990:KMA


**Goldwasser:1985:PSS**


**Goldwasser:1988:DSS**

REFERENCES

Goldwasser:1989:KCI

Good:1945:GRT

Groote:1998:CVP

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

Gemmell:1994:CIA
Peter Gemmell and Moni Naor. Codes for interactive authentication. *Lecture Notes in Computer Sci-
REFERENCES

Goettfert:1995:GLB


[GN95a]

Goettfert:1995:GLB

Gray:1995:PCT


[GO95]

Goldwasser:1993:ISN


[GO93]

Golic:1995:EPC


[GO95]

Goldreich:1996:SPS


[GO96a]
REFERENCES


Golic:1996:CCC

Grosky:1996:NAH

Goguen:1999:IAS

Golomb:1967:SRS

Golomb:1982:SRS

Goldwasser:1984:PET

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


Golic:1996:CEP


Gollmann:1996:CA


Gollmann:1996:FSE


Goldreich:1997:FMCa


Goldreich:1997:FMCb


Goldwasser:1997:NDC

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


[102x144][Gong:1992:SRD] Li Gong. A security risk of depending on synchronized

**Gong:1995:CKH**


**Gong:1998:JSM**


**Good:1979:EWC**


**Goodman:1996:LPS**


**Gordon:1985:SPE**


**Gordon:1993:DDT**

REFERENCES


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


**Gabidulin:1991:INR**


**Gleason:1985:ECP**


**Guillou:1995:ACE**


**Guillou:1998:E**


**Guillou:1991:PTA**

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


Gennaro:1997:HSD


Greenfield:1994:DPP

REFERENCES


Grosek:1994:RCR

Grover:1998:FCP

Goldschlag:1996:HRI

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

Grusho:1998:SCI

Gaines:1978:SSP

Grollmann:1984:CMP
REFERENCES

Grollmann:1988:CMP

Girault:1994:LCH

Gulliver:1994:ITA

Gritzalis:1997:CPO

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


Gudes:1980:DCB


Gullichsen:1983:BHS


Gunther:1988:ASG


Gunther:1988:ACE


Gurnsey:1997:CT


Gustafson:1996:SAS


Gutmann:1996:SDD


Guthery:1998:SC


Gutmann:1998:SGP


Gutmann:1999:DCS

REFERENCES


Goldberg:1996:RNB


Gylden:1933:CCB

[102x681]REFERENCES

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

Gylden:1936:AMC


Gylden:1938:APV


Gysin:1996:OKC


Gylden:1933:CCB

Gylden:1936:AMC

Gylden:1938:APV

Gysin:1996:OKC

Garzon:1991:CGG


Haller:1994:RIA


Hendessi:1994:SAA


Hollaar:1996:LRD

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

**Haddon:1984:BRS**


**Hagelin:1998:SHC**


**Hoffman:1994:CP**


**Hammer:1971:SSC**


**Hamming:1980:CIT**


**Hamming:1986:CIT**


**Hamxx**

V. Hamilton. Personal communication. ???.

**Hansen:1994:MLD**

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

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

Hardjono:1990:RED


Harari:1991:CCS


Hart:1994:DSC


Harpes:1996:CIB


Harris:1996:E


Haskett:1984:PAU


Haastad:1987:OWP

REFERENCES

Haastad:1988:SSM


Haselberger:1995:DRB


Hasan:1999:LTB


Hatefi:1996:MRE


Hatefi:1997:AED


Hawkes:1998:DWK


Hawkes:1998:DLW


Hwang:1996:SAA


Hwang:1996:AES


He:1996:HFR


He:1996:NKE


He:1992:IKB


Huang:1998:FAI


Hedberg:1997:FIC


Hartung:1998:DWM

REFERENCES

Held:1993:TSD

Helleseth:1994:ACE

Held:1998:ARU

Held:1998:LET

Helleseth:1998:E

Henry:1981:BJB
REFERENCES


REFERENCES


[HG97e] Frank Hartung and Bernd Girod. Digital watermarking of MPEG-2 coded video
REFERENCES


[HGHD98]


[HGS98]


[Haddar:1998:ISI]


[Hall:1998:RAA]


[Hinsley:1979:BISb]


Hofmann:1994:RQC

Hughes:1998:AJC

Husemann:1999:OTY

Hutton:1999:ASM

Harn:1989:PAU

Han:1993:TCC

Han:1997:TCC
Yenjo Han, Lane A. Hemaspaandra, and Thomas Thierauf. Threshold computation and cryptographic security. SIAM Journal
REFERENCES

409


Hochberger:1999:CDM


Hochberger:1999:CDM

Harn:1993:OTP


Harn:1993:OTP

Hirose:1997:CKD


Hirose:1997:CKD

Hig73


Hig73

Hig97a


Hig97a

Hig97b


Hig97b

Hil29


Hil29

Hil31

Lester S. Hill. Concerning certain linear transfor-
REFERENCES

Hiltgen:1994:CRC

Hill:1997:MTY

Haastad:1999:PGO

Hinsley:1993:BIS

Hirschfeld:1993:MER

Hirschfeld:1997:FCF
REFERENCES


REFERENCES

Hillenbrand:1999:SDW


Hong:1997:IAU


Huehnlein:1998:CBN


Herlea:1999:SBR


Harn:1990:EPE


Halevi:1997:MSM

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

**Hevia:1998:STD**


**Halfmann:1999:ESP**


**Haynes:1999:VDS**


**Hevia:1999:STD**

REFERENCES


REFERENCES


Hwang:1995:TAN


Hwang:1996:SCW


Hughes:1996:QCU


Hohl:1993:SIH


Hunter:1983:ERA


Hule:1988:RCW


Hafner:1991:COH

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


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


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


puter Society Press order number PR9172.


REFERENCES

Abstracts/0001-0782/162691.html


REFERENCES

[Hoogendoorn:1982:SPK]

[Han:1997:ICS]

[Horng:1995:PAU]

[Horng:1998:AAP]

[Horster:1999:SSK]

[Herzberg:1987:PPS]
REFERENCES


REFERENCES

Hoffstein:1998:NRB

Holland:1982:GSA

Hwang:1990:PKA

Hollander:1996:KWS

Harrison:1976:POS

Hruby:1995:QDQ
REFERENCES

Hruby:1995:QQC


Hruby:1996:SCI


Hruby:1998:TQC


Hruby:1999:SUD


Hernandez:1999:CLM


Haastad:1985:CST


Hammer:1987:EUH

[H89]

[HS90]

[H91]

[H96a]

[H96b]


REFERENCES

[Hada:1998:EZP]

[Hada:1999:RBO]

[Handschuh:1999:DOE]

[Huang:1988:APE]

[Huber:1998:MAE]

[Hulme:1898:CHP]
Hunter:1985:ARK


Hurwicz:1998:CTM


Husain:1994:EI


Husemann:1999:SCD


Hulaas:1998:MLI


Hardy:1975:ITN

Godfrey H. Hardy and Edward M. Wright. An Introduction to the Theory of


7130 (print), 1558-125X (electronic).


REFERENCES

Hasan:1993:MMO

He:1996:TLR

Hong:1998:FIE

Hall:1998:BPPa

Hall:1998:BPPb

Hohl:1994:SIH

Harn:1993:GUS
L. Harn and S. Yang. Group-oriented undeniable

[Harn:1993:PKC]

[Hwang:1995:TPE]

[Hirose:1998:ADK]

[Hirose:1998:ADH]

[Hsieh:1998:H]

[Hsieh:1999:OWH]
Hardjono:1993:PDM


Ibbotson:1997:CPI


Anonymous:1993:CCA


IBM:19xx:PSP


IEEE:1974:ASS


IEEE:1979:ASF


IEEE:1980:PSS


IEEE:1981:CLC

IEEE:1982:ASF


IEEE:1982:CFP


IEEE:1983:PSS


IEEE:1984:ASF


IEEE:1985:FOC


IEEE:1986:CEC

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


IEEE:1987:ASF


IEEE:1987:IIG


IEEE:1988:FAC


IEEE:1989:ASF

REFERENCES

IEEE:1991:PSA


IEEE:1992:PIC

IEEE Computer Society Press order number 2825.


[IEEE:1993:FIW]


IEEE:1995:PIC


IEEE:1995:PIS


IEEE:1995:PII


IEEE:1996:ASF


IEEE:1996:IIC

Order Plan catalog number 96TB100057.


IEEE:1997:ACS


IEEE:1997:ICD


IEEE:1997:IICb


IEEE:1997:IWS


IEEE:1997:ASF

[IEE97f] IEEE, editor. 38th Annual

**IEEE:1997:PICa**


**IEEE:1997:PICb**


**IEEE:1997:IICa**


**IEEE:1997:ICb**


**IEEE:1997:PICa**


**IEEE:1997:PICb**
REFERENCES

IEEE:1997:PAC

IEEE:1997:ASF

IEEE:1998:HCC

IEEE:1998:IIC


REFERENCES

IEEE Computer Society
Press, 1109 Spring Street,
Suite 300, Silver Spring,
MD 20910, USA, 1999.
ISBN 0-7695-0237-7, 0-
7695-0238-5 (case), 0-7695-
0239-3 (microfiche). LCCN
QA76.76.O63 W6666 1999.
IEEE Computer Society
Press order number PR00237[IHR99]

[IH98] Naomaru Itoi and Peter
Honeyman. Pluggable
authentication modules for
Windows NT. In USENIX
[USE98a], page ?? ISBN
1-880446-95-2. LCCN
QA76.76.O63 U885 1998.
URL http://www.usenix.
.org/publications/library/
proceedings/usenix-nt98/
itoi.html; http://www.
usenix.org/publications/
library/proceedings/usenix-
nt98/itoi_slides.

[IH99a] N. Itoi and P. Honey-
man. Practical security sys-
tems with Smartcards. In
IEEE [IEE99b], pages 185–
190. ISBN 0-7695-0237-7, 0-
7695-0238-5 (case), 0-7695-
0239-3 (microfiche). LCCN
QA76.76.O63 W6666 1999.
IEEE Computer Society
Press order number PR00237[IHR99]

[IH99b] Naomaru Itoi and Pe-
ter Honeyman. Smart-
card integration with Ker-
beros V5. In USENIX
[USE99c], page ?? ISBN
1-880446-34-0. LCCN
URL http://www.usenix.
.org/publications/library/
proceedings/smartcard99/
itoiKerberos.html.

[Itoi:1999:SUF] Naomaru Itoi, Peter Hon-
eyman, and Jim Rees.
SCFS: a UNIX filesystem
for Smartcards. In USENIX
[USE99c], page ?? ISBN
1-880446-34-0. LCCN
URL http://www.usenix.
.org/publications/library/
proceedings/smartcard99/
itoiSCFS.html.

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

[Igarashi:1999:ITP] H. Igarashi, S. Kosue, and
M. Miyahara. Individual
tactical play and pass
with communication be-
tween players-team descrip-
tions of Team Miya2. Lect-
ure Notes in Computer Sci-
CODEN LNCSD9. ISSN
REFERENCES

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


REFERENCES


Impagliazzo:1992:PGP


Impagliazzo:1989:ECS


Ito:1999:DPS


Ingemarsson:1998:E


Instenes:1995:MAA


IRD:1979:DVE


IDC:1981:DE

[International Data Corporation. Data encryption. Research memorandum IDC #ISPS-M81-10., International Data Corporation, Framingham, MA, USA, October 1981. 30 pp.]

IRD:1981:DTV

[International Resource Development, Inc. Data, text, and voice encryption equipment. Report 183, IRD, 30 High St., Norwalk, CT]

[IRD:1984:DTV]


[IRD:1987:DTV]


[IRD:1988:DTV]

Anonymous:1991:IIS


[IRD:1991:DFV]


[Itoh:1994:LDS]


[IR89]

REFERENCES


[Ing81] Ingemar Ingemarsson and C. K. Wong. Use authentication scheme for shared data based on a trap-door one-way function. Information Processing Letters,
REFERENCES


Imai:1998:PKC


Imai:1999:PKC


Jaburek:1990:GGP


Jackson:1987:NTS


Jackson:1990:SITa


Jackson:1990:SITb

Keith M. Jackson. Secure information transfer:

Jackson:1996:AAC


Jakobsson:1995:BUU


Jakobsen:1999:HOC


Jakobsson:1999:MCM


Jakobsson:1999:QCA


Jamieson:1998:UEP

Lauren Jamieson. Unveiling the extraordinary possibiliti-


REFERENCES


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


REFERENCES


Jian:1999:SDM


Jolitz:1991:PUI


Jolitz:1995:RNS


Johnson:1998:ESS


Johnson:1998:SIC


Johansson:1999:FCA

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


REFERENCES

Jurgensen:1984:SRI


Jackson:1993:CAG


Janwa:1996:MPK


Johnson:1996:AEE


Jurisic:1997:ECC


Jakobsson:1999:IMI


Johnson:1994:CDM


Jackson:1994:MTS

REFERENCES


**Jackson:1995:ESS**


**Jackson:1995:SMS**


**Jerichow:1998:RTM**


**Jakobsson:1996:DVP**


**Jarecki:1997:EMS**


REFERENCES


John W. Jones. Data encryption based on the logarithm problem. Thesis (M.A.Sc.), University of Ottawa, Ottawa, ON, Canada, 1986. 2 microfiches (103 fr.).


REPRESENTATIONS


G. Jones and M. Sheeran. Designing arithmetic circuits by refinement in Ruby.


Jakobsson:1999:SAE


Jiwa:1994:BBA


Jan:1996:SIE


Juels:1999:TTS


Jung:1987:IRC

REFERENCES

Jungnickel:1996:DFG

[Jun96]

Jung:1999:EMA

[Jun99]

Jutla:1998:GBA

[Jut98]

Just:1996:AMP

[JV96]

Jakubowski:1998:CSP


Jeannerod:1998:GEE


Ji:2001:CAF

REFERENCES

[MJ96]
M. Jakobsson and M. Yung. On oblivious, agnostic, and blindfolded provers. In
URL http://link.springer.com/link/service/series/0558/tocs/t1109.htm;
by the International Association for Cryptologic Research (IACR), in co-opera-
tion 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).

[KA98a]
letes RFC1826 [Atk95a]. Status: PROPOSED STAN-
DARD.

[KA98b]
S. Kent and R. Atkinson. RFC 2406: IP Encapsulating Security Payload (ESP),
letes RFC1827 [Atk95b]. Status: PROPOSED STAN-
DARD.

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


REFERENCES

Kahn:1991:SER


Kahn:1991:WWW


Kahn:1996:HS


Kahn:1996:CSS


Kahn:1998:EC


Kahn:1998:PHI


Kahn:1998:RMU

Kak:1983:EMP


Kak:1984:MPK


Kak:1985:EEC


Koc:1996:ACM

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

Kaliski:1984:AWA


Kaliski:1985:WAE


Kaliski:1991:MMD

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


Kaliski:1998:RPCc


Kaliski:1998:EDF


Kaliski:1998:RPCa

Kaliski:1998:REC


Kaliski:1999:ESP


Kaneshige:1996:ITC


Kaps:1998:HSF


Karger:1985:ADA


Karger:1987:LDP


Kari:1989:CBP

Kari:1989:OCP


Karkare:1996:SEA


Kasiski:1863:GDG

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

Kastenholz:1996:RVP


Kalipha:1990:NPK


Katzan:1977:SDE


Katsikas:1997:CMS

REFERENCES


Kaufman:1993:RDD


Kaufman:1996:DWC


Kawai:1987:LAI


Kay:1995:CTE


Krishnakumar:1992:HTE


Krawczyk:1996:HKM

H. Krawczyk, M. Bellare, and R. Canetti. HMAC-MD5: Keyed-MD5 for message authentication. Internet draft draft-ietf-ipsec-hmac-md5-txt.00., March 1996.

Krawczyk:1997:RHK


Klein:1989:STR

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


REFERENCES

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

Khinchin:1997:CF

Keating:1999:PAA

Kelsey:1999:KSWb

Kemp:1988:EEF

Kemmerer:1989:AEP

Kemppainen:1999:DMM

Kent:1993:IPE
Stephen T. Kent. Internet privacy enhanced mail. Communications of the Association for Computing Machinery, 36(8):
REFERENCES


Kent:1995:PCW


Kerr:1975:PIC


Kerr:1989:SNM


Knoble:1979:EOW


Kesdogan:1996:LMS


Kit:1993:DDI


Klapper:1995:CBA

[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

REFERENCES


REFERENCES

Kippenhahn:1997:VBG

Kippenhahn:1999:CBH

Kippenhahn:1999:VBG

Kirby:1995:RPK

Kak:1977:SEU

Kocher:1999:DPA

Kurosawa:1995:NBA

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


Kelm:1997:NK


Kunihiro:1998:ECN

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

Kommerling:1999:DPT


Koren:1999:ISC


Koshelev:1999:EAM


Kurosawa:1991:GPK

Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata,

**Kabatianskii:1997:DSS**


**Kram:1999:FCD**


**Kothari:1984:CMW**


**Kilian:1994:FKE**


**Kilian:1995:FCR**


**Knudsen:1995:NA**

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**


**Kang:1993:PRR**

[KM93] Kwangjo Kim and Tsu-
Knudsen:1996:IDA


Kosuda:1997:SED


Kaksonen:1998:OMC


Kaufman:1998:DWF


Kasahara:1999:NPK


**Knudsen:1999:CIS**


**Knudas:1999:RAP**


**Koscielny:1999:QBP**


**Kanda:1998:ECC**


**Kohayashi:1999:FEC**


**Konheim:1980:ICP**


**Koyama:1991:NPK**

Kenji Koyama, Ueli M. Maurer, Tatsunari Okamoto, and Scott A. Vanstone. New


REFERENCES


Knuth:1969:SNM


Knuth:1973:ACP


Knuth:1980:DLC

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

Knuth:1985:DLC


Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb


Knudsen:1993:ICS


Knudsen:1993:CLc

REFERENCES

Knudsen:1993:CLa


Knudsen:1994:PSF

Knudsen:1994:BCA

Knudsen:1995:NPW

Knudsen:1998:BAC

Knudsen:1998:NPW

Knudsen:1998:DBC

Knudsen:1999:STA

Knudsen:1999:CBC
Knudsen:1999:FSE


Kurosawa:1995:CIS


Kurosawa:1995:CBA


Kurosawa:1996:CLB


Kurosawa:1997:CLB


Koblitz:1987:CNT


Koblitz:1987:ECC

REFERENCES

1987. CODEN MCMPAF.
ISSN 0025-5718 (paper),
1088-6842 (electronic).

Koblitz:1990:FJS

[Kob90] Neal Koblitz. A family
of Jacobians suitable for
 discrete log cryptosystems.
Lecture Notes in Computer
CODEN LNCS-9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Koblitz:1991:CCG

[Kob91a] Neal Koblitz. CM-curves
with good cryptographic
properties. Lecture Notes
in Computer Science, 576:
279–287, 1991. CODEN
LNCS-9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Koblitz:1991:CEC

[Kob91b] Neal Koblitz. Constructing
eLLiptic curve cryptosystems
in characteristic 2. Lecture
Notes in Computer Science,
LNCS-9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Koblitz:1991:JSI

[Kob91c] Neal Koblitz. Jacobi
sums, irreducible zeta-
polynomials, and crypto-
graphy. Bulletin canadien
de mathématiques = Cana-
dian Mathematical Bulletin,
CODEN CMBUAA3. ISSN
0008-4395 (print), 1496-
4287 (electronic).

Koblitz:1994:CNT

[Kob94] Neal Koblitz. A Course in
Number Theory and Cryp-
tography, volume 114 of
Graduate texts in mathe-
ematics. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., second edition,
0-387-96576-9 (New York),
3-540-96576-9 (Berlin). x
+ 235 pp. LCCN QA241
K672 1994.

Koblitz:1996:ACC

[Kob96] Neal Koblitz, editor. Ad-
vances in cryptology, CRYPTO
'96: 16th annual inter-
national cryptology con-
ferece, Santa Barbara,
California, USA, August
18–22, 1996: pro ceed-
ings, volume 1109 of
Lec-
ture Notes in Computer
Science. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 1996. CODEN
LNCS-9. ISBN 3-540-
61512-1. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C79 1996. URL http://
/link.springer-ny.com/
link/service/series/0558/
tocs/t1109.htm; http://
www.springerlink.com/
openurl.asp?genre=issue&
issn=0302-9743&volume=
1109. Sponsored by the
International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

Kobayashi:1997:DWH


Koblitz:1998:C


Koblitz:1998:AAC


Kobara:1999:PMA

REFERENCES

**Kochanski:1989:HSI**


**Koc:1994:HSR**


**Kocher:1995:CDR**


**Koc:1996:RHI**


**Kocher:1996:TAI**


**Kocher:1999:B**

REFERENCES

Koeune:1999:CRI


Kohl:1990:UEK


Kolata:1977:NCC


Koland:1995:SSH


Konheim:1981:CP


Konheim:1985:CAE

REFERENCES

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


[Koo97] Bert-Jaap Koops. Crypto
REFERENCES


Kopooshian:1997:DCE


Kornerup:1993:HRM


Korner:1996:PC


Koscielny:1983:PRD


Kurosawa:1994:NSS

[KOS+94] Kaoru Kurosawa, Koji Okada, Keiichi Sakano,
REFERENCES


Koyama:1982:CUM


Koyama:1982:MKR


Koyama:1983:MKR


Koyama:1995:FRT


Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kozen:1996:RSS

TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://
www.elsevier.com/cgi-
bin/cas/tree/store/tcs/
cas_sub/browse/browse.
cgi?year=1996&volume=
167&issue=1-2&aid=2272.

Kim:1989:PRP
Su Hee Kim and Carl
Pomerance. The probabil-
ity that a random probable
prime is composite. Math-
ematics of Computation,
53(188):721–741, October
1989. CODEN MCMPAF.
ISSN 0025-5718 (paper),
1088-6842 (electronic).

Kwan:1993:GPT
Matthew Kwan and Josef
Pieprzyk. A general pur-
pose technique for locating
key scheduling weaknesses
in DES-like cryptosystems.
Lecture Notes in Compu-
ter Science, 739:237–??,
ISSN 0302-9743 (print),
1611-3349 (electronic).

Krajicek:1995:SCC
J. Krajicek and P. Pud-
lak. Some consequences of
cryptographical conjectures
for S012 and EF. Lecture
Notes in Computer Science,
960:210–??, 1995. CODEN
LNCS9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Knudsen:1996:HFB
L. Knudsen and B. Pre-
neel. Hash functions based
on block ciphers and qua-
ternary codes. Lecture
Notes in Computer Science,
1163:77–??, 1996. CODEN
LNCS9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Knudsen:1996:DSK
Lars R. Knudsen and Tor-
ben P. Pedersen. On the
difficulty of software key
escrow. Lecture Notes in
Computer Science, 1070:
237–??, 1996. CODEN
LNCS9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1070/10700237.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1070/10700237.
pdf.

Knudsen:1997:FSH
Lars Ramkilde Knudsen
and Bart Preneel. Fast
and secure hashing based
on codes. Lecture Notes
in Computer Science, 1294:
485–??, 1997. CODEN
LNCS9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1294/12940485.htm;
Kilian:1998:IE

Kaps:1999:FIF

Kipnis:1999:UOV

Karhumaeki:1999:CSI

Kaliski:1994:FBC
REFERENCES

Kaliski:1994:LCU


Kushilevitz:1994:RRT


Kaliski:1995:MAM


Kaliski:1995:SUR


Kaliski:1996:MEW


Kilian:1996:HPA

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


Knudsen:1996:NAL


Knudsen:1999:DFC


Kolliopoulos:1999:NLT


Kranakis:1986:PC


Krawczyk:1990:HPC

REFERENCES


Krawczyk:1999:BCC


Kesdogan:1998:DTP


Knudsen:1999:DSR


Kumar:1999:CCB


Kruh:1998:WWS


Knudsen:1999:TDS


Kordes:1989:UMC

F. L. G. Kordes and J. J. Schuurman. The use of...
MEBAS in creating a simulation environment for compression and encryption. [KS97c]

Kelsey:1997:CPO


Kurosawa:1997:DSP


Kwon:1997:SEA


Kaliski:1998:RPRb


Kelsey:1998:SPP

J. Kelsey and B. Schneier. The street performer protocol. Technical report, Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55419,

Kinoshita:1998:GST


Kipnis:1998:COV


Kemp:1996:CPC


Kelsey:1999:AST


Kipnis:1999:CHP


Kemp:1996:PRM

A. H. Kemp, S. J. Shepherd, and S. K. Barton. Progress report on multifunction coding and modulation for spread spectrum...


REFERENCES


Knowles:1992:AFC


Kelsey:1996:KCI


Kelsey:1997:RCB


Kelsey:1998:PICa


Kelsey:1998:PICb

Kelsey, B. Schneier, D. Wagner. Protocol in-

**Kelsey:1999:KSWa**


**Kelsey:1999:MCAa**


**Kelsey:1999:MCAb**


**Kelsey:1998:SCCa**


**Kelsey:1998:SCCb**


**Kelsey:1998:SCCc**

J. Kelsey, B. Schneier,


Koyama:1998:AFC


Kanda:1999:SCF


Kuchlin:1987:PKE


Kucera:1992:GES


Kuhn:1998:CIS


Kuijk:1991:RSE


Kukorelly:1999:VCH

English text with German abstract. Published by Hartung-Gorre, Konstanz, Switzerland.

Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC


Kumar:1997:CSI


Kummert:1998:RPT


Kuo:1990:TEC


Kurosawa:1994:NBA

REFERENCES

Kearns:1989:CLL


Kearns:1994:CLL


Kaur:1999:IBP


Kirstein:1992:PAS


Konrad:1999:SDK


Kwan:1993:SAD


Lam Kwok-Yan and Thomas Beth. Timely authentication in distributed

**Kurosawa:1998:SBC**


**Kwok-Yan:1992:FAA**


**Kasami:1982:KMS**


**Koch:1995:TRH**


**Levien:1998:ART**


**Lampson:1991:ADS**


**Lampson:1992:ADS**

Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed


[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.A25L35 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 iter-
ating a weak round function several times are considered. Four basic constructions for the round function of an iterated cipher are studied.”.


REFERENCES


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


REFERENCES


**Lin:1999:AMG**


**Leary:1987:CSM**


**Leary:1990:SCS**

[Lea90] Penn Leary. *The second cryptographic Shakespeare: a monograph wherein the poems and plays attributed to William Shakespeare are proven to contain the en-

**Leary:1999:NBE**


**Leclerc:1989:CRM**


**Lee:1995:NSI**

Hsun-Ming Lee. Network security integration by public key encryption and stored procedures of database servers. Thesis (M.S.E.), Arizona State
REFERENCES

University, Tempe, AZ, USA, 1995. ix + 90 pp.

[Leech:1996:RUP]

[Lee:1999:GIC]

[Lee:1999:DAA]

[Leipold:1999:K]

[Leiserson:1999:ITD]

[Leichton:1979:BRB]


[Leiss:1980:NSS]

[Lei99b]

[Lempel:1979:CT]
Abraham Lempel. Cryptology in transition. ACM
REFERENCES


Lercier:1997:FGR


Levine:1958:VMS


Levine:1961:SAH


Levine:1961:SECa


Levine:1961:SECb


Levine:1983:USC


Levin:1985:OWF


Levine:1991:USC

Jack Levine. *United States cryptographic patents, 1861–1989*. Cryptologia, Terre Haute, IN, USA, second edi-
REFERENCES


REFERENCES


[LHL95a] C.-M. Li, T. Hwang, and N.-Y. Lee. Threshold-


J. Linn. RFC 1040: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and...

RFC1040


Linn:1989:RPE


RFC1113

REFERENCES


REFERENCES

Lippit:1993:PIC


Lipton:1994:CNF


Abeles:1998:KVC


Lipmaa:1999:ICM


Litant:1987:BRC


Lindsay:1997:BC

German Enigma code during World War II, whose admission to homosexuality at a time when it was illegal presented problems for him, for his family, for his colleagues, and for the State’s preoccupation with national security. Close-captioned.


REFERENCES

[Liaw:1993:OAA]

[LL94a]

[LL94b]

[Lim:1994:AMA]

[Lim:1995:SPP]


REFERENCES


[LLH96] Lam:1996:EGE


[LLMP93] Lenstra:1993:FNF


[Langie:1922:C] Langie:1922:C


REFERENCES

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


[Tom Leighton and Silvio Micali. Secret-key agreement without public-key cryptography. Lecture
REFERENCES

Leighton:1994:SKA


[LM95] Low:1996:MCP

[LM96] Low:1998:PCT

Lamersdorf:1998:TDS
marking and identification
using both line and word
shifting. In IEEE [IEE95c],
pages 853–860. ISBN 0-
7803-2525-7 (microfiche).
ISSN 0743-166X. LCCN
TK 5105.5 I33 1995. URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
/bibliography/1039.html.

Three volumes. IEEE cat-
alog number 95CH35759.
IEEE Computer Society
Press order number PR06990.

A. V. Le, S. M. Matyas,
D. B. Johnson, and J. D.
Wilkins. A public key
extension to the Com-
mon Cryptographic Archi-
tecture. IBM Systems Jour-
CODEN IBMSA7. ISSN

S. H. Low, N. F. Maxem-
chuk, and A. P. Lapone.
Document identification for
copyright protection using
centroid detection. IEEE
Transactions on Com-
munications, 46(3):372–
383, March 1998. CO-
DEN IECMBT. ISSN
0090-6778 (print), 1558-
0857 (electronic). URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
/bibliography/071150.html.

X. Lai, J. L. Massey, and
S. Murphy. Markov ciphers
and differential cryptanal-
ysis. Lecture Notes in Com-
puter Science, 547:17–38,
ISSN 0302-9743 (print),
1611-3349 (electronic).

X. Lai, J. L. Massey, and
S. Murphy. Markov ciphers
and differential cryptanal-
ysis. In ????, editor, Ad-
vances in Cryptology, Pro-
cedings of EUROCRYPT
91, volume 547 of Lecture
Notes in Computer Science,
pages 17–38. Springer-Ver-
lag, Berlin, Germany / Hei-
delberg, Germany / Lon-

H. Lee, K.-A. Moon, and J.-
W. Park. Design of a par-
allel processing system for
facial image retrieval. Lec-
ture Notes in Computer Sci-
CODEN LNCS4D9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

G. Longo, M. Marchi, and
A. Sgarro. Geometries,
codes and cryptography,
volume 313 of Courses and
lectures. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 1990. ISBN 3-
211-82205-4 (Wien), 0-387-
REFERENCES

Leonard:1997:CSP

Lautemann:1999:DCA

Lidl:1994:IFF

Lehti:1998:CT

Lagarias:1985:SLD

LaMacchia:1991:CDL
REFERENCES

LaMacchia:1991:SLS


Lomet:1983:HPU


Lomas:1994:ENT


Lomas:1997:SP1


Long:1991:PAA


Long:1992:UDE

Yong Hong Long. Using Diophantine equations to

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


REFERENCES


Luciano:1987:CCC


Leszczyński:1994:SDA


Li:1999:CKA


Lacy:1998:IPP


REFERENCES


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


[LT91] Philip Leong and Chris Tham. UNIX password

**Linnartz:1998:MPM**


**Langley:1999:ACI**


**Laih:1995:SLF**


**Lioen:1988:OMA**


**Lu:1979:EGC**


**Lu:1980:AEG**


**Lackey:1995:SMS**

REFERENCES

Luby:1996:PCA

Lucks:1996:HEI

Lucks:1996:FLC

Lucks:1996:FLR

Lucks:1997:SRK

Lucks:1998:SBB

Lucks:1998:OKE

Lucks:1998:ATE
Stefan Lucks. Attacking triple encryption. In Vau-
REFERENCES

[102x681] REFERENCES

547


[Lucks:1999:SBB]


[Lucks:1999:SBC]


[Lujan:1998:AMDa]


[Lujan:1998:AMDb]


[Lunt:1990:EK]

[102x681] REFERENCES


REFERENCES


REFERENCES

Laih:1993:TES


Li:1990:ACP


Li:1991:BCP


Li:1991:HBM


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN


MacLaren:1994:CPN


Mache:1998:SCT

Wolfgang W. Mache. The Siemens cipher teletype in the history of telecommunications. In Deavours et al. [DKK*98], pages 433–453. ISBN 0-89006-862-

[Madsen:1992:GCD]
Jørgen Bo Madsen. The greatest cracker-case in Denmark: The detecting, tracing, and arresting of two international crackers. In USENIX [USE92b], pages 17–40. ISBN 1-880446-46-4. LCCN ????.


[Mah96]

[Man95]

[Mandelbrot:1960:BRJa]

[Manasse:1995:MPE]
M. Manasse. The Millicent protocols for electronic commerce. ????,

Manjunath:1998:IPA


Moriai:1996:KLP


Mao:1997:PVP


Mao:1998:GCS


Marsh:1970:CSS


Marsh:1970:MEC


Marion:1976:ANB


Marion:1995:WGT

REFERENCES


REFERENCES


Mastrovito:1989:VDM


Mastrovito:1991:VAC


Massey:1994:SKB


Massacci:1997:BSP


Massacci:1999:DRT


Massey:1999:OSD


Matyas:1979:DSO

Matyas:1991:KHC


Matsui:1993:LCM


Matsui:1994:FEC


Matsui:1995:CBO


Matsui:1996:NSB


Matthews:1996:SRN

Matsui:1997:NBE


Matsumura:1999:DTE


Maurer:1990:FGS


Maurer:1991:NAD


Maurer:1991:DSS


Maurer:1991:PCS

Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In
REFERENCES


IEEE Computer Society order no. 2190.

Maurer:1991:PSS


Maurer:1993:PSK


Maurer:1993:RIT


Maurer:1994:TEB


Maurer:1996:UGT


Maurer:1996:ACE

Ueli Maurer, editor. Advances in cryptology, EUROCRYPT ’96: Inter-
REFERENCES


REFERENCES

[Maurer:1999:IC]

[Maurer:1999:ITC]

[Maxemchuk:1994:EDD]

[May:1997:CDS]

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

[Mao:1994:SAP]

[Massey:1994:CCT]
REFERENCES

Mehrotra:1999:NOA


Mitra:1999:DCT


Mintzer:1998:OWS


Mintzer:1997:EIDb


Moskowitz:1992:CAA

Mitchell:1996:CKU


McCarty:1975:AFP


McCurley:1990:DLP


McCurley:1990:OEC


McCurley:1996:CIL


McCane:1998:ICS

Millan:1998:HDC


Millan:1999:BFD


McHugh:1992:EBD


McIvor:1985:SC


McKee:1999:SFF


McMahon:1996:RGA


Madson:1998:REC


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


Carolyn P. Meinel. How hackers break in ... and how they are caught: Port scanners, core dumps and buffer overflows are but a

**Mendelsohn:1939:CC**


**Mendelsohn:1989:CWI**


**Mendez:1991:AKA**


**Menezes:1993:ECP**


**Menezes:1995:ECC**


**Menicocci:1995:SAC**


**Mermenne:1644:CPM**

Marin Mermenne. *Cogitata Physica-Mathematica ... Tractatus de mensuris...*
... Hydraulica pneumatica; arsque navigandi. Harmonia theoriae, practica. Et Mechanica phaenomena. Ballistica et acon-tismologia]. 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. Pervou-chine 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:1988:DSB


Merkle:1989:CDS


Merkle:1990:OWH


Merkle:1990:CDS


Merkle:1991:FSE

REFERENCES

Mercuri:1993:IRC


Merrill:1997:ARD


Meyer:1996:RPE


McGraw:1997:UKJ


Murino:1995:RNU


Mihaljevic:1991:CCP


Madson:1998:RUHa


REFERENCES


Micciancio:1997:ODS


Mihaljevic:1996:FCS


Millikin:1943:ECCa


Millikin:1943:ECCb


Millikin:1943:ECCc


Miller:1976:RHT

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


**Miller:1985:PES**

**Miller:1986:UEC**

**밀런:1987:CCC**

**Mills:1987:RDP**

**Milliken:1992:ECC**

**Miller:1995:HWK**
REFERENCES

Millan:1996:LOA


Miller:1996:CME


Matsumoto:1993:VIA


Mintzer:1997:EIDa


Misarsky:1997:MAU


Mitchell:1976:EAD

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

**Mitchell:1989:MDS**


**Mitchell:1992:AMI**


**Mitchell:1992:CCI**


**Miyaguchi:1990:FCC**


**Miyaguchi:1991:FCF**


**Miyaji:1993:ECS**

REFERENCES

Miyaji:1993:OEC

Miyano:1993:MEN

Miyaji:1996:MRS

Miyaji:1999:ECC

Mjolsnes:1993:PCP

Morii:1992:PSP

Moskowitz:1994:CCH

Mazières:1999:SKM
David Mazières, Michael Kaminsky, M. Frans

Maibaum:1999:SRS


Miyazaki:1999:TFI


Mao:1998:CPO


Matyas:1991:KSB

References

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


REFERENCES


[Mm98a] S. Mueller and W. B.


REFERENCES

Magliveras:1990:CTC

Muller:1981:SRP

Muller:1986:CDS

MRaihi:1997:XFO

Moulin:1999:ITA

Mock:1997:BDS

Mohtashemi:1992:CHC
Mojdeh Mohtashemi. On the cryptanalysis of Huffman codes. Thesis (M.S.), Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, May

Matsumoto:1982:DTL


Mok:1997:KNF


Moldovyan:1998:NEP


Morita:1991:SCT


Montgomery:1985:MMT


Monagan:1993:GPD


Montagu:1996:MWN

REFERENCES

Moore:1992:PFC


Morland:1666:NMC


Morrice:1692:EB


Morrison:1983:SEA


Morain:1988:IGP


Mora:1989:AAA


Morris:1992:FMC

[213x644] Stephen Brent Morris. The Folger manuscript: the cryptanalysis and interpretation of an American Masonic manuscript, volume 23 of Publications of the Masonic Book
REFERENCES


[Mor97] Morgan:1997:PAM


[Mor98] MorenoDiaz:1998:NCC


REFERENCES


Mitchell:1989:RHF


Macalister:1976:SLI


McEliece:1981:SSR


Muller-Schloer:1983:MBC


Meier:1990:NCC


Montgomery:1990:FEP

REFERENCES

Meier:1991:CPC


Meier:1993:EMC


Massey:1994:FTA


Meier:1995:SG


Meier:1995:SSG


Metzger:1995:RIAa

REFERENCES


REFERENCES


Mizuki:1998:ESK


Mizuki:1999:DNS


Martin:1999:BTE


Mambo:1996:HUT


Madonia:1993:GSP


Michels:1998:SSV


M. Matsui and T. Tokita.
REFERENCES


Melkonian:1999:AAD


Mister:1999:CRL


Marayati:1987:AWA

rasa’i’il al-Kindi wa-Ibn ’Adlan wa-Ibn al-Durayhim.

Moggi:1999:IMS


Mackinnon:1985:OAA


Moriya:1997:DWS


REFERENCES

[BSW89]. Conjectures that “$M_n := 2^n - 1$ is the product of two distinct primes only if $n$ is either a prime $p$ or the square of a prime $q$, in which case precisely one prime factor of $M_n$ is Mersenne, viz. $M_q$.”

[Muller:1999:SRB]


[Mund:1991:ZCP]


[Mund:1991:ZLC]


[Mur87]

[Mur96]

[Mur99]

[Muraszko:1987:CVR]


[Murphy:1996:CC]


[Murphy:1999:OST]

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

Musser:1992:UVE


Maruyama:1998:TGH


Menezes:1990:IEC


Menezes:1991:ACC


Meijers:1993:EMV


Menezes:1998:C


Mu:1999:DD

Yi Mu, Vijay Varadharajan, and Khan Quac Nguyen.


REFERENCES


Mihaljevic:1998:CAB


Merwin:1979:NCC


Nastar:1995:TRD


Nat-Abdesselam:1999:QCA


Naccache:1993:MSF

REFERENCES


**REFERENCES**

REFERENCES


Shipping list no.: 94-0159.
Issued February 9, 1994.

[Nat95] National Institute of Standards and Technology. 


[Nat97a] National Institute of Standards and Technology. 


NIST:1999:SRF


NIST:19xx:AES


Nechvatal:1999:SRF


Nilsson:1978:OST


Nandi:1997:RCT


[Neu94] Peter G. Neumann. Inside RISKS: Alternative pass-
Neumann:1995:RCD


Neumann:1997:IRC


Ng:1999:CST

586X (electronic). See [ZXX98].

Nguyen:1999:CGC


Nguyen:1999:CGG


Nelson:1990:SAE


Neubauer:1998:DWI


Neubauer:1998:CSD


Nichols:1998:CCCa


Nichols:1998:CCCb


[NIS93a] NIST. *Digital Signature Standard*. Gaithersburg, MD 20899-8900, USA,
REFERENCES

February 1, 1993. ?? pp. FIPS PUB 186.

NIST:1993:FPS


Anonymous:1994:DSS


Nisan:1996:ERH


Nyberg:1993:PSA


Nakamura:1998:MEC


Nikander:1998:JBC


Nandi:1994:TAC

&arnumber=338094.

Nikander:1999:PPD

REFERENCES

Nakamura:1988:DRM

Naccache:1994:MSC

Naccache:1996:ACP

Naccache:1996:CSC

Naccache:1999:SDT

Nguyen:1998:NDC
Nguyen:1999:DZK


Naccache:1995:CDB


Naccache:1995:CDI


Nozaki:1997:LCS


Noras:1996:CHH


Nicchiotti:1998:NIS


http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073157.html
Four volumes.


REFERENCES

Naor:1998:TTT


[NP98a]

Naor:1998:UIS


[NP99]

Niemi:1994:CPV


[NR94]

Nyberg:1995:MRS


[NR95]

Nikolaides:1998:RIW


[NP98b]

Naor:1999:OTA


[NP99]

[NR98]

Needham:1978:UEAa

R. M. (Roger Michael) Needham and Michael D.

**Needham:1978:UEAb**

**Needham:1987:AR**

**Neuman:1988:AUE**

**Norris-Saucedo:1989:DAD**

**Naor:1995:VC**

**Naccache:1997:NPK**
Nguyen:1997:MRC


Nguyen:1997:MHR


Nechaev:1998:DSB


Nguyen:1998:BQS


Nguyen:1998:BSR


Nguyen:1998:CAC


Nguyen:1998:CAD


Nguyen:1999:CFP

[NS99a] P. Nguyen and J. Stern. Cryptanalysis of a fast public key cryptosystem pre-
REFERENCES


REFERENCES


Nyberg:1994:DUM


Nyberg:1995:LAB

K. Nyberg. Linear approximation of block ciphers.
REFERENCES


Nyberg:1998:ACE


Nystrom:1999:PCT


Ohta:1994:LCF


Ohsuga:1999:EHI


Oakley:1978:RPC


Oberzalek:1999:GEE

REFERENCES

O'Connell:1981:CDE

O'Connor:1994:UBN

O'Connor:1995:DCT

Obenland:1999:SED

ORuanaidh:1996:PWD

Odlyzko:1984:CAM
Odlyzko:1985:DLF


Odlyzko:1987:CCD


Odlyzko:1987:ACC


Odlyzko:1990:RFK


Odlyzko:1994:DLS


Odlyzko:1994:PKC


Odlyzko:1995:FIF


Odlyzko:1998:C


Oelke:1997:VDE


Okamoto:1993:EDS

REFERENCES


Toru Ohira. Encryption with delayed dynamics.


Kazuo Ohta and Ting i (Dingyi) Pei, editors. Advances in cryptology — Asiacrypt'98: International Conference on the Theory


REFERENCES

Okamoto:1993:PSP


Okamoto:1994:DCS


Okamoto:1998:TKR


Okamoto:1998:TKS


Okon:1996:DWN


Okon:1997:KMA


Ogata:1997:FTA


Ochi:1998:NSO


ONeil:1986:ETM

Patrick E. O’Neil. The Escrow transactional method. 


Ogawa:1998:WTM

Hiroshi Ogawa, Takao Nakamura, and Youichi Takashima. Watermark technique for motion pictures. 


Okamoto:1990:DZKb

Tatsuaki Okamoto and Kazuo Ohta. Disposable zero-knowledge authentications and their applications to untraceable electronic cash. 


Ohta:1993:DMS


_Lecture Notes in Computer Science_, 739:139–??, 1993. CODEN LNCS.D9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ohta:1998:CST


REFERENCES

Ohta:1991:MAH


ORuanaidh:1997:RST


ORuanaidh:1998:RST


ORuanaidh:1999:CCP


Oppliger:1996:ASS


Oppliger:1997:ISF

Rolf Oppliger. Internet se-

Otway:1987:ETM


OECD:1998:OEM


OECD:1998:CPG


Orlowski:1996:EGI


Orton:1987:VIP


Orton:1995:MTD


Orton:1995:MIT

Glenn A. Orton. A multiple-iterated trapdoor

O'Shea:1988:CDU


Okamoto:1991:EAC


Okamoto:1992:EAC


Olejar:1998:CPR


Orup:1991:VER


Ong:1991:TCM

Sing Guat Ong, Jennifer Seberry, and Tho-

[Ong:1985:ESS]


[OSS85]

[OU98a]


[OU98b]


[OU99]

(print), 1611-3349 (electronic).

**Outerbridge:1998:ACD**


Only the slides for the conference talk are available.

**Ozarow:1984:WTC**


**OReilly:1995:WWW**


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

**Ostrovsky:1991:HWM**


**Pereira:1998:REC**


**Petitcolas:1998:WCM**

Pai:1996:VIE


Pai:1998:INP


Pai:1999:EDE


Pai:1999:LCD


Pai:1999:TPE

REFERENCES

Paillier:1999:PKC


Petitcolas:1998:ACM


Parthasarathy:1985:DSG


Parent:1998:ALM


Parker:1998:UMP


Parrish:1998:RMM


Patterson:1987:MCC

REFERENCES

Patarin:1991:PPB


Patarin:1991:NRP


Patarin:1995:CMI


Patarin:1996:ACH


Paterson:1999:IPG


Paulson:1998:IAV


Paulson:1999:IAI


Petrie:1998:NBR


Pizzonia:1999:OOD


Popovic:1999:DIT


Plagge:1999:DET


Pearcey:1980:EDS


Peake:1997:OVD


Pedersen:1991:DPA

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

Pedersen:1991:NIS

Pedersen:1991:NII

Pedersen:1991:NIT

Pedersen:1991:TCT

Pedersen:1995:EPS

REFERENCES


REFERENCES


[Pet91] A. Pethő. On a polynomial transformation and its application to the construction of a public key cryptosystem. In Computational number theory (De-


[Pfi96a] B. Pfitzmann. Information hiding terminology. In Anderson [And96c],
Pfitzmann:1996:TTT


Pfitzmann:1996:DSS


Pfleeger:1989:SC


Pfleeger:1995:ULC


Pfleeger:1997:SC


Pomerance:1990:CCNb

REFERENCES


[Patarin:1997:ACB]

[Patern:1997:ACS]

[PGCSN96]

[PGV91]

[Preneel:1992:CSH]

[Preneel:1993:CHF]
B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographic hash functions. In Wolowicz [Wol93b], pages 161–171. LCCN ????

[Preneel:1993:HFB]


Bart Preneel, Rene Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: a synthetic approach. Lecture Notes in Computer Science, 773:


REFERENCES

Phillips:1998:SHI


Pichler:1986:ACE


Pichler:1998:E


Pierce:1977:SSP


Pieper:1993:CRD


Pinch:1997:UCN


Piner:1998:CUW

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


REFERENCES

December 1979. CODEN CMSVAN. ISSN 0010-4892.


I. Petrounias and P. Loucopoulos. A rule-based approach

**Pless:1975:ESC**


**Pless:1977:ESC**


**Pless:1982**


**Plummer:1998:MIW**


**Plummer:1983:ISP**


**Plummer:1983:ISPa**


**Pei:1999:COA**

Dingyi Pei, Yuqiang Li, Yejing Wang, and Rei Safavi-Naini. Characterization of optimal authentication codes with arbitration. *Lecture Notes in Computer Science*, 1587:
REFERENCES


**Payne:1978:OEN**


**Petersen:1998:SST**


**Pitt:1999:DAC**


**Provos:1999:FAP**


**Prie:1999:ASU**


**Proctor:1992:AIC**


**Pudil:1995:ASM**

[PNFK95] P. Pudil, J. Novovicova, F. Ferri, and J. Kittler. Advances in the statisti-
REFERENCES


Pomerance:1990:CCNa


Pomerance:1990:F


Pomerance:1994:NFS


Pomerance:1998:C


Poole:1995:La


Popentiu:1989:SRK

REFERENCES

Porges:1952:MNC


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT


Posch:1992:TMD


Posch:1993:PFP


Posch:1998:MPC


Posch:1989:AEA


Pfitzmann:1990:HBD

[PP90] B. Pfitzmann and A. Pfitzmann. How to break the


Torben Pryds Pedersen and Birgit Pfitzmann. Fail-stop


**[PRee1998:RDD]** B. Preneel, V. Rijmen, and A. Bosselaers. Recent developments in the design of conventional cryptographic

**Preneel:1998:AAP**


**Preneel:1993:ADC**


**Preneel:1993:SCT**


**Preneel:1994:CHF**


**Preneel:1995:FSE**


**Preneel:1995:EFC**

cryptobytes/crypto1n2.pdf.

**Preneel:1997:HFM**


**PGP:1997:PGPa**


**PGP:1997:PGPb**


**Preneel:1998:CMA**


**Preneel:1998:IC**


**Preneel:1998:CP1**


**Preneel:1999:SCH**


**Pritchard:1980:DE**

REFERENCES


[ Pri83 ]


[ Pri94 ]


[ Pro85 ]


[ Pri80 ]

REFERENCES

Patel:1999:TML

Peyravian:1999:HBE

Paun:1993:CPS

Pieprzyk:1993:DHA

Pfitzmann:1996:AF

Pichler:1996:FDG

Pointcheval:1996:PSB
REFERENCES (print), 1611-3349 (electronic).


[PS98e] D. Patiyoot and S. J. Shepherd. Techniques for authentication protocols and key distribution on wireless

**Patiyoot:1998:TAPb**


**Poupard:1998:GSR**


**Poupard:1998:SAP**


**Patiyoot:1999:MES**


**Patiyoot:1999:WSS**


**Patiyoot:1999:SIA**

REFERENCES

Patiyoot:1999:CST


Patiyoot:1999:WWA


Pfenning:1999:SDT


Patel:1997:UDB


Pieprzyk:1991:RAS


Pieprzyk:1995:PA


Pieprzyk:1995:ACA

REFERENCES


Paar:1997:FAA


Pomerance:1988:PAF


Pfitzmann:1995:HBA


Phoenix:1995:QCP


REFERENCES

Computer Society Technical Committee on Security and Privacy.

[B.Preteel: 1996: STM]


[P-fitzmann:1986: NUO]


sored by International Association for Cryptologic Research … [et al.]"—T.p. verso.

[P-fitzmann:1987: APS]


[Piper:1993: DSH]


REFERENCES

Quisquater:1998:CSE


Quisquater:1991:CLE


Quisquater:1989:BHF


Quisquater:1995:ACE


Qiao:1998:CME

[QN98a] Lintian Qiao and Klara


Qiao:1998:WMM


Qin:1988:RSS


Quisquater:1989:ACE


Quisquater:1990:ACE


Quisquater:1998:E

REFERENCES

Rabin:1977:DS


Rabin:1981:HES


Rabin:1989:EDI


Rabin:1994:RSS


Rabin:1998:SAT


Rackoff:1990:BTP

REFERENCES


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

Rhodes-Burke:1982:RSA


Reiter:1994:HSR


Ramesh:1999:VPP


Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA

REFERENCES


REFERENCES

RoRaback:1999:FAE


Rebel:1998:ADS


Rijmen:1996:CS


Reeds:1979:CMC


Reeds:1998:SCB


Reischuk:1985:NSB


Reiter:1992:ISG

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


REFERENCES

Reynard:1997:SCB


Reynard:1999:SCB


Rowlett:1935:FAP


Reiter:1995:SCR


Rhodes:1999:SPH


Radu:1997:WHR


Rubin:1993:LRJ


Ryu:1999:PAA

M. Ryu and S. Hong. A period assignment algorithm for real-time system design. Lecture Notes in Computer
REFERENCES


[Rich74] 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.


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


REFERENCES


Rivest:1979:CRC


Rivest:1980:DSC


Rivest:1985:RCP


Rivest:1987:EDR


Rivest:1990:RMM


Rivest:1990:C


REFERENCES

[Rivest:1998:RDR]

[Rivest:1998:CWE]

[Rivest:1998:CAR]

[Rivest:1998:CWC]

[Rivest:1998:PC]
R. Rivest. Personal communication. ??, 19xx.

[Rhodes:1993:ZF]

[Rijmen:1998:WL]

[Rowlett:1998:SMM]
REFERENCES


REFERENCES

Raisch:1996:ACH


Roberts:1993:ECI


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Roe:1994:PSC


Roe:1995:PBC


Roelse:1999:CWD

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

**Rogaway:1995:BHA**


**Rogaway:1996:SD**


**Rohwer:1975:GIM**


**Rohwer:1977:CCB**


**Rohatgi:1999:CNR**

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

**Roman:1990:C**


**Rompel:1990:OWF**

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


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


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

Greg Rose. Update on cryptography issues. ;login: the USENIX Association newsletter, 21(1):4–??,
February 1996. CODEN LOGNEM. ISSN 1044-6397.


REFERENCES


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


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

**Rauber:1997:SDW**


**Rigney:1997:RRAa**


**R../../Rrivest:1998:RBC**


**Rivest:1983:RET**

REFERENCES

[Rivest:1984:HEE]

[Rackoff:1991:NIZ]

[Rackoff:1993:CDA]

[Rescorla:1996:SHT]

[Rivest:1996:PMTa]

[Rivest:1996:PMTb]

[Reiter:1998:RAU]

[Riordan:1998:CMP]
J. Riordan and B. Schmeier. A certified E-mail protocol with no trusted third party. Technical


REFERENCES


REFERENCES


REFERENCES

Rueppel:1993:ACE


Rueppel:1998:E


Russel:1927:CMS

REFERENCES


Ruskey:1993:SCG


Rus93a

Russell:1993:NSC


Rus93b

Roychowdhury:1999:ENQ


RV99

Reeds:1984:FSU


RW84

Robshaw:1997:ECC


RY97

Rytter:1986:SCU


Ryt86

Ras:1999:DES


RZ99

S:1873:COD

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

G. Jousset, Paris, France, 1873. 8 pp. LCCN Z104 H16 1873.

[Schiller:1995:SWT]

[Sabourin:1994:CCP]

[Sahai:1999:NMN]


[Sak91] A. Salomaa. Verifying and recasting secret ballots in...

**Salomaa:1996:PC**


**Salvail:1998:QBC**


**Salvail:1999:SHG**


**Shimoyama:1997:IFS**


**Sameshima:1998:KES**


**Sansom:1986:BRC**


**Sandhu:1988:CIT**

REFERENCES


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Smid:1992:DES


Smid:1993:RCN


Shepherd:1994:UBS


Shepherd:1995:CNL


Schneier:1997:EPP

REFERENCES


Stallmann:1999:HED


Siegberg:1999:TDG


Sztandera:1999:ANN


Shepherd:1999:NCS


Chen:1985:RGE


Schneider:1996:RCB

REFERENCES

0-7803-3672-0 (CD-ROM).
LCCN TK8315.1222 1996.
Three volumes. IEEE catalog number 96CH35919.


URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054163.html


[Sca86] Fred A. Scacchitti. The cryptographer’s toolbox.

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


Schwenter:1633:SSA


Schroeder:1975:ESK


Schell:1983:SPA


Schroeder:1984:NTS


Schroeder:1986:NTS


Schnorr:1990:EISb

REFERENCES


\[\text{Schnorr:1990:EISa}\]

\[\text{Schroeder:1990:NTS}\]

\[\text{Schmitt:1991:EAA}\]

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

\[\text{Schnorr:1991:FHE}\]
REFERENCES


Schnorr:1993:FHI


Schnorr:1993:FIE


Schiller:1994:SDC


Schneier:1994:DNV


Schneier:1994:DEA


Schneier:1994:PAD


Schneier:1994:SCD


Schneier:1994:AAd

REFERENCES


[Sch95b] Bruce Schneier. Algorithm alley: The GOST encryption algorithm. Dr. Dobb's Journal of Software Tools,
REFERENCES


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


REFERENCES

Schneier:1997:WCH

Schroeder:1997:NTS

Schweighofer:1997:DIF

Schlesinger:1998:CPC

Schmalz:1998:MDI

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


Schaefer:1999:PES


Schmalz:1999:MDI


Schmidt:1999:RER


Schneier:1999:SSC


Schneier:1999:IRR


Schneier:1999:IRT


Schneier:1999:IRU


Schneier:1999:IWC


Schoenmakers:1999:SPV


Schroeder:1999:SEA


Schumann:1999:PST
REFERENCES

Schwentick:1999:DCL


[Sch99]

Scerri:1999:UOS


[SCT99]

Scudder:1992:OLA


[Scu92]

Smith:1986:GCC


[SD86]

Silvestre:1997:IWU


[SD97]

Schouten:1999:FEU


[SD99]

Sicherman:1983:AQR


[SDV83]

Smillie:1986:RWA


Schwenk:1996:PKE


Seaton:1956:THS


Sears:1986:SWK


Seachrist:1995:DIM


Sedlak:1988:RCP

REFERENCES


[Sedg1992:AC] [Sel94]


[Selcuk:1998:NRL]


[Selcuk:1998:NMS]


[Sedgewick:1992:AC] [Sel94]


[Seeley:1989:PCG] [Sel98a]


[Segal:1992:NCT]
REFERENCES

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

[Ser85] Serpell:1985:CES


[SG95] Saglam:1995:ACL

[SG96a] Shearer:1996:GCR


REFERENCES

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

[Sga91a]

Saeednia:1999:SCG

S. Saeednia and H. Gho- [SG99a]

[Saeednia:1999:SCG]

[Sga91b]

[Sapir:1999:DRT]


[Sapir:1999:DRT]

[Sga90]


[Sgarro:1990:IDB]

[Sgarro:1991:STC]


[Sgarro:1991:LBA]


[Sgarro:1993:ITB]


REFERENCES


Shi:1999:FGM


[Shannon:1945:MTC]


Shannon:1948:MTCa

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

Shannon:1948:MTCb


Shannon:1949:CTS


Shamir:1979:HSS

Shamir:1982:PTA


Shamir:1983:ECC


Shamir:1983:GCS


Shamir:1984:PTA


Shamir:1985:IBC


Shamir:1986:SPS


Shamir:1987:CSS

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

721


[She86] Sherman:1986:CVT

[Sherman:1987:CVT]


[Sherman:1987:CVT]


[Sherman:1987:CVT]


[Sherman:1987:CVT]

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


[Shepherd:1994:MCM]


[Shepherd:1994:PKS]


[Shepherd:1994:CAA]


[Shepherd:1995:HSS]


[Shepherd:1995:PPH]


[Shepherd:1995:CAA]


[Shepherd:1996:APK]

S. J. Shepherd. Security weaknesses in the Netscape World Wide Web browser. In ???, editor, IEE Colloquium on Public Uses of Cryptography, Savoy Place,
REFERENCES


Shecter:1997:SAD


Su:1998:GID


Schneier:1999:TEAa


Shoup:1996:FPS


Shor:1997:PTA

Shparlinski:1999:FFT


Shparlinski:1999:NTM


Shulman:1980:BRB


Shulman:1976:ABC


Shulman:1982:BRB


Sakurai:1993:DBS

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


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

on Computer Arithmetic, 
June 29–July 2, 1993, 
Windsor, Ontario. IEEE 
Computer Society Press, 
1109 Spring Street, Suite 
300, Silver Spring, MD 
20910, USA, 1993. ISBN 
0-7803-1401-8 (softbound), 
0-8186-3862-1 (casebound), 
0-8186-3861-3 (microfiche). 
ISSN 0018-9340 (print), 
1557-9956 (electronic). LCCN 
QA 76.9 C62 S95 1993. 

Shimbo:1993:CSC


Silverman:1983:RVS


Silverman:1987:MPQ


Silverman:1997:RSP


Silverman:1997:FGR


Silverman:1999:EMM


Simonetta:1404:LTC

Simmons:1979:HID


Simmons:1979:CCA


Simmons:1979:SAE


Simmons:1982:SAC

Gustavus J. Simmons, editor. Secure communications and asymmetric cryptosystems, volume 69 of AAAS Selected Symposia Series.


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC

Gustavus J. Simmons. Authentication theory/coding

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

Simmons:1985:SCD


Simmons:1988:SSC


Simmons:1990:HRS


Simmons:1990:PSS


Simmons:1991:GSS

Gustavus J. Simmons. Geometric shared secret and/
or shared control schemes (invited talk). *Lecture Notes in Computer Science*, 537:216–??, 1991. CO-
link/service/series/0558/bibs/0537/05370216.htm; http://link.springer-ny.com/link/service/series/
0558/papers/0537/05370216.pdf.

**Simmons:1992:CCS**

Gustavus J. Simmons, editor. *Contemporary Cryptology: the science of information integrity*. IEEE Com-
puter Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-87942-

**Simmons:1993:SCU**

G. J. Simmons. The subliminal channels in the US Digital Signature Al-
gorithm (DSA). In Wol-
lowicz [Wol93b], pages 35–
54. LCCN 93056016 URL http://www.cl.cam.ac.
.uk/~fapp2/steganography/bibliography/022612.html

**Simmons:1994:CTS**

link/service/series/0558/bibs/0765/07650448.htm; http://link.springer-ny.com/link/service/series/
0558/papers/0765/07650448.pdf.

**Simmons:1994:CPF**

Gustavus J. Simmons. Cryptanalysis and protocol failures. *Communications of the Association for Com-
puting Machinery*, 37(11): 56–65, November 1994. CO-
DEN CACMA2. ISSN 0001-
html.

**Simmons:1994:SCP**

Gustavus J. Simmons. Subliminal channels; past and present. *European trans-
actions on telecommunications and related technolo-
.uk/~fapp2/steganography/bibliography/034412.html

**Simmons:1994:SCE**

Gustavus J. Simmons. Subliminal communication is

Simovits:1995:EDE


Simmons:1996:HSC


Simmons:1997:SCS


Simmons:1998:RCB


Simpson:1996:RPC

REFERENCES


Anthony Martin Singer. Electronic commerce: dig-

**Singh:1999:CBE**


**Siu:1999:PNG**

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

**Sambur:1976:SEM**


**Sethi:1997:FCS**

REFERENCES


REFERENCES


Shimoyama:1998:QRB


Schneier:1999:SAL


Stabell-Kulo:1999:PAM

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

Shepherd:1997:EKE


Schell:19xx:CMC


Sorokine:1994:TBD


Suzuki:1999:AVB

S. Suzuki, T. Kato, H. Ishizuka, and Y. Takahashi. An application of vision-based learning in RoboCup for a real robot with an omnidirectional vision system and
the team description of Osaka University "Trackies". 

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

Satoh:1998:HSR

A high-speed small RSA encryption LSI with low 
power dissipation. Lecture Notes in Computer Science, 
1396:174–??, 1998. CODEN LNCS9D. ISSN 0302-9743 
(print), 1611-3349 (electronic).

Satoh:1998:HSS

A high-speed small RSA encryption LSI with low 
power dissipation. Lecture Notes in Computer Science, 
1396:174–??, 1998. CODEN LNCS9D. ISSN 0302-9743 
(print), 1611-3349 (electronic).

Schneier:1996:DP

[SKW96] B. Schneier, J. Kelsey, and J. Walker. Distributed 
East Minnehaha Parkway, Minneapolis, MN 55419, 
September 1996. URL http://www.counterpane.com/
distributed_proctoring.html. Also published in 
ESORICS 96 Proceedings, Springer-Verlag, September 

Schneier:1998:TKSa

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, 
C. Hall, and N. Ferguson. On the Twofish 
key schedule. Technical report, Counterpane 
Systems, 101 East Minnehaha Parkway, Minneapolis, MN 
twofish-keysched.html. To appear in Fifth Annual 
Workshop on Selected Areas in Cryptography, Springer-Verlag, August 1998.

Schneier:1998:TBBa

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, 
C. Hall, and N. Ferguson. Twofish: a 128-bit block 
East Minnehaha Parkway, Minneapolis, MN 55419, 
twofish-paper.html.

Schneier:1998:TBBb

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, 
C. Hall, and N. Ferguson. Twofish: a 128-bit block 
cipher. Evaluation CD-1: 
Documentation, National 
Institute of Standards and 
Technology, August 1998.
REFERENCES


REFERENCES


Slutsky:1998:KDQ


Schobi:1983:FAT


Siromoney:1990:PKC


Staffelbach:1991:CSC


Schubert:1995:MLS


Syverson:1995:FRK


Sklower:1996:RPE

REFERENCES

B. Schneier and Mudge.
Cryptanalysis of Microsoft’s Point-to-Point Tunneling Protocol (PPTP).

K. Sklower and G. Meyer.

A. G. Sutcliffe and S. Minocha.


REFERENCES


[Smi83] John Smith. Public key cryptography: An introduction to a powerful cryptographic system for use on microcomputers. BYTE Magazine, 7(??):198–218, January 1983. CODEN BYTEDJ. ISSN 0360-5280. This is a simple exposition of public key cryptography.


REFERENCES


REFERENCES


Safavi-Naini:1998:BCM


Safavi-Naini:1998:NRM


Snyder:1979:IUC


Snyder:1980:CAP


Shepherd:1998:ALP


Sonnino:1999:CBL


Schroeppel:1995:FKE


Juan Soto, Jr. Randomness testing of the AES candidate algorithms. In National Institute of Standards and Technology [Nat98], page 9. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round1/r1-rand.pdf. See [RD99a] for a conference overview. No formal proceedings were published, but the conference web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.


REFERENCES

[Schechter:1999:AAM]

[Spi95]

[Schuetz:1997:CPB]

[Shoup:1996:SKD]

[Saltzer:1984:EEA]

[Shin:1998:NHF]
References


REFERENCES

1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). [SS96]

[Sakurai:1995:RAC]

[Smith:1995:PCD]

[Smith:1995:PKC]

[Sandhu:1996:AAC]

[Silverman:1997:CAX]

[Sakai:1998:DHC]

[Sun:1998:PKC]
REFERENCES


REFERENCES

(1872-6119 (electronic).

Siromoney:1988:CPL


Saito:1999:DPC


Smith:1981:VEP


Stubblebine:1999:UST


Safford:1993:SRA


Sakai:1997:WRK

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


Susilo:1999:FST


Shepherd:1990:CSS


Schmidt:1998:LOA


Salter:1998:TSS


Schneier:1998:DDE


StJohns:1984:RAS

REFERENCES

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

StJohns:1985:RAS


Shawe-Taylor:1989:BRB


Stern:1991:CPK


StJohns:1993:RIP


Safavi-Naini:1994:OAS

REFERENCES

Stark:1970:INT

Stark:1978:INT

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

Stallings:1995:PYP

Stadler:1996:PVS

Staiger:1996:CSW
Stallings:1996:PCS

Stallings:1996:PCI

Staddon:1997:CSC

Stallman:1997:SDR

Stark:1997:ESP

Stallings:1999:CNS

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

Stevenson:1976:MCI

Stern:1987:SLC

Stevens:1988:CPR

Stephenson:1989:PPM

Stevens:1990:CPi

Stevens:1990:CPk

Steinberg:1991:VSV

Stewart:1992:SCK

Stern:1994:DIS
REFERENCES


Stevens:1994:PBa

Stern:1995:COD

Stern:1996:VCA

Stern:1998:LCO

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

Stern:1999:ACE

Stehenson:1999:C


[D. R. Stinson, editor. Advances in Cryptol-
REFERENCES


REFERENCES


Stumme:1999:AEK


Steiner:1995:REE


Su:1998:DEM


Summers:1984:OCS


Sun:1991:UDE


Sun:1991:RSE


Sun:1998:ISM


Sundsted:1998:SDI


SuperMacSoftware:1988:SDE


Sutoh:1999:HPP

[Sut99] Hiroki Sutoh. A high-performance public key cryptography co-processor
for super multi-purpose smart card. In Anonymous [Ano99c], page ??


Samuels:1998:LSA

[SVWMB95] Adam D. Samuels, Jerry van Dijk, Dawn Amore, Shlomi Fish, Scott Schwendinger, Arvid R. Hand, Jr., and Howard Mark. Letters: Something in the air; more on Ada; recycling PCs; server-side scripting; stronger encryption; inner loops; Einstein kudos. Dr. Dobb’s Journal of Software Tools, 23(3):8, 12, March 1998. CODEN DDJOEB. ISSN 1044-789X.

Sivakumar:1999:PPN


Shepherd:1995:SCS


Smeets:1991:CAC


Shamir:1998:PHS

Shulman:1961:GC


Smith:1983:HCR


Silverman:1993:PAE


Saeki:1994:SSS


Safford:1994:UNC


Snow:1994:SA


Scheidler:1995:PKC


Stansfield:1995:CCS


REFERENCES

Swire:1997:ULF


Salzer:1981:RHH


Sun:1989:TKE


Sun:1990:KGE


Salomaa:1986:PCB


Salomaa:1986:PKC


Smith:1992:ICF

REFERENCES

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

Sakurai:1996:BDB


Shieh:1996:AKD


Sowers:1998:TDW


Sellini:1999:VKV


Sakurai:1998:KES


Syverson:1993:KDP

REFERENCES

Seberry:1993:ACA


Sakurai:1996:CWR


Szepietowski:1998:WSO


Swanson:1996:RDH


Swanson:1996:TRI


Swanson:1998:MSB

M. D. Swanson, B. Zhu, and A. H. Tewfik. Multiresolution scene-based video watermarking using perceptual models. IEEE
REFERENCES


REFERENCES

119–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Seberry:1995:RBP [SZZ95c]


Takagi:1997:FRT [Tak97]

Tang:1997:DBC [TA97]

Taaffe:1998:NBL [Taa98]

Tabatabaian:1994:CAP [Tab94]
REFERENCES


Tattersall:1998:ENT


Tattersall:1999:ENT


Taylor:1995:NOU


Taylor:1990:DSI


Taylor:1994:ICV


Tao:1985:FAP


Tao:1986:TVF


Tsujii:1991:NIB

REFERENCES

Tao:1999:GPK

Tao:1999:FAP

Tao:1997:FNF

Tangney:1991:SIS

Tedrick:1985:FES

Teske:1998:SPR
REFERENCES

TI:1984:TTU
Texas Instruments Inc. TMS7500 TMS75C00 user's guide, data encryption device: 8-bit microcomputer family. Texas Instruments, Dallas, TX, USA, 1984. various pp.

[Tex84]

Tourigny:1994:DSD

[TG94]

Tanaka:1999:PCD

[TGKI99]

Tzeng:1999:IP1

[TH99]

Thao:1991:SAD

[Tha91]

Theobald:1995:HBS

[The95]

Thomas:1974:RPS

[Tho74]

Thompson:1984:RTT


[TJ97] Joanne Taaffe and Margaret Johnston. News: Siemens licenses Java for


Takagi:1996:MMP


Takagi:1996:MVM


Terada:1997:LDC


Todorovic:1997:CAS


Tirkel:1998:IWR


Tonchev:1996:CDG


Toussaint:1991:DCK

REFERENCES


Traore:1999:GST


Tremblett:1999:JPA


Trithemius:1518:PLS


Trithemius:1606:CGT

Johannes Trithemius. Claus generalis triplex in libros steganographicos Iohannis

Trithemij .... Iohannis Berneri, Frankfurt, Germany, 1606. 7 + 1 pp. LCCN Z103.T84 S 1606. Ab ipso authore conseripta ... Darmstadtij: Excudebat Balthasar Hofmann, impensis Iohannis Berneri, bibliop. Francof., anno 1606.

Trithemius:1606:CSI


Trithemius:1606:SHE

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

**Trithemius:1621:CGT**


**Trithemius:1621:CSI**


**Trithemius:1621:SHE**


**Tronson:1997:C**


**Tirkel:1993:EW**

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


[Ts'90] Tso:1990:NPK

[Ts'97] Tso:1997:MEE


REFERENCES

2860. IEEE catalog number 92CH3133-6.

[Tsu92a]

[Tsu92b]

[Tsu92c]

[TSY98]

[Tua99]


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.

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


[TY98b] Yiannis Tsiounis and Moti Yung. On the security of ElGamal-based encryption. Lecture Notes in


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).


REFERENCES


DEPT. OF THE ARMY, HEADQUARTERS, WASHINGTON, DC, USA (??), MAY 14, 1982. 35 PP.

**USGSA:1982:TGS**


**USNBS:1983:FPD**


**USGSAOIRM:1984:ISR**


**USGAOPEMD:1987:PDD**


**USDA:1988:CED**


**USNBS:1988:DES**


USNSACSSCCH:1992:FLT


USDOA:1994:OMT


USDOA:1994:UDS


USNSACS:1994:SC


USCSCJSTL:1995:ACC


USNSGC:1995:NDN


UCC:1996:SRP


USCHCJ:1996:SFT


USPTO:1996:CCP

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

USCHCCSTTCP:1997:SFT


USCHCJSCIP:1997:SFT


REFERENCES

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


REFERENCES

USCSCCST:1998:EHB


USCSCJ:1998:HEK


USCSCJSTTGI:1998:EDC


USNSACS:19xx:BPM

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


REFERENCES


REFERENCES


USENIX:1994:PSU


USENIX:1995:PUT


USENIX:1995:PFUa


USENIX:1995:PFUb


USENIX:1996:SAC


USENIX:1996:WEC


USENIX:1996:CSW


USENIX:1996:PSUa

REFERENCES


REFERENCES

USWD:1983:EC


USDOA:1989:BC


USCHCJ:1997:SFT


USPBC:1997:AEC


Vadhri:1995:VID

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

Valerio:1892:C

References

Vamos:1985:BRB


VanTassel:1969:ACT


Vandeberg:1986:ICS


VanHeurck:1987:TNS


vanTilborg:1988:IC


VanTilburg:1993:SKE


VanOorschot:1995:DCS


VanTilburg:1995:ACA

REFERENCES

vanRenesse:1996:OSC

vanDijk:1997:MIT

vanRenesse:1997:ODS

vanDijk:1997:MIT

Varaiya:1999:DSI

Varma:1999:IDD

Vaudenay:1993:FHI
Vaudenay:1995:NMC


Vaudenay:1996:WKB


Vaudenay:1998:CCC


Vaudenay:1998:PSB


Vaudenay:1998:CCR


Vaudenay:1998:DFC


Vaudenay:1998:FSE

REFERENCES


Vandewalle:1990:ECC


Dijk:1995:LCP


Dijk:1997:SCB


Vandermeulen:1999:ADM

REFERENCES

Lubbe:1998:BMC

Wal:1997:PBR

Vedder:1993:SAM

Vedder:1998:GSS

Vedder:1998:ISI

Venema:1990:IEI

Venkaiah:1992:RBP

Vernam:1926:CPT

Veron:1995:CHI
P. Veron. Cryptanalysis of Harari’s identification
REFERENCES


REFERENCES

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

[vanFaber:1997:SDD]

[vanHeijst:1993:NCF]

[Vigna:1998:CTM]
G. Vigna. Cryptographic


[Vincent:1971:PAG]

[Vincent:1972:CPA]

[Vandenwauver:1998:SIE]


REFERENCES

Kerckhoffs:1883:CMF


Varadharajan:1999:DER


Voyatzis:1998:DSW


Four volumes.

Venkataraman:1995:CEA


IEEE Catalog Number 95CH35760.

Oorschot:1991:CPP

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

VARADHARAJAN:1999:DER

VENKATARAMAN:1995:CEA

VOYATZIS:1998:DSW

OORSCHOT:1991:CPP
arithms. Lecture Notes in Computer Science, 537:
576–??, 1991. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic). URL http://
link.springer-ny.com/ [Vog85]
link/service/series/0558/\nbiib/0537/05370576.htm;
http://link.springer-ny.com/link/service/series/\n0558/papers/0537/05370576.\n
vanOorschot:1991:CPP

Paul C. van Oorschot. A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms. Lecture Notes in Computer Science, 537:
576–??, 1991. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic). URL http://
[Vol41]
link.springer-ny.com/ [Vol85]
link/service/series/0558/\nbibs/0537/05370576.htm;
http://link.springer-ny.com/link/service/series/\n0558/papers/0537/05370576.\n
vanOorschot:1992:CPP

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

Vogel:1985:LCC

volume=209. Held at the University of Paris, Sorbonne.

Volts:1941:BCP


VonZurGathen:1992:PEE

REFERENCES

[102x681]REFERENCES
[102x681]813
[181x646](print), 1872-6119 (electronic).

VonZurGathen:1992:PEF


Voukalis:1980:DFC


Voukalis:1980:GSE


vanOorschot:1991:KPA


vanOorschot:1996:DHK


Voyatzis:1996:ATA

REFERENCES

7803-3258-X (softbound), 0-7803-3259-8 (casebound),
0-7803-3260-1 (microfiche), 0-7803-3672-0 (CD-ROM).
LCCN TK8315.I222 1996.
Three volumes. IEEE catalog number 96CH35919.

[Voyatzis:1998:DIW]
G. Voyatzis and I. Pitas.
Digital image watermarking using mixing systems.
CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic).

[Voyatzis:1999:PDI]
George Voyatzis and Ioannis Pitas.
January/February 1999. CODEN ICGADZ. ISSN 0272-1716 (print),
1558-1756 (electronic). URL http://computer.org/cga/cg1999/g1018abs.htm;

[Varadharajan:1997:ISP]
Vijay Varadharajan, Josef Pieprzyk, and Yi Mu, editors.
*Information security and privacy: second Australasian conference, ACISP’97, Sydney, NSW, Australia, July 7–9, 1997: proceedings*, volume 1270 of
*Lecture Notes in Computer Science*. Springer-Verlag,
Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997.
CODEN LNCSD9. ISBN 3-540-63232-8 (paperback). ISSN 0302-9743 (print),

[Vassiliadis:1988:PEA]
Stamatis Vassiliadis, Michael Putrino, and Eric M. Schwarz.
CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

[Volts:1941:BC]
93 pp. LCCN Z103.A1 V6 1941. Typewritten (carbon copy) Three heavy leaves precede sections II–IV (not included in pagination).
This copy was made especially for the United States Army from the original manuscript. Third copy: pencilled note on cover.
Contents: pt.1. Cryptogra-


vanTilburg:1986:DBK


vanSchyndel:1994:DW


Vu:1995:CPM


Vazirani:1985:ESP


Valiant:1986:NED


Verheul:1997:CLS

REFERENCES

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

Vandemeulebroecke:1990:SCB


Verheul:1997:BEF


vanOorschot:1999: PCS


VanOorschot:1996:DKA


Vedder:1998:SCR


vanOorschot:1999:PCS

REFERENCES

vanEmdeBoas:1999:ALP

Vanstone:1997:ECC

Waber:1987:VEC

Weidenbach:1999:SDS

Wobber:1993:ATO

Wobber:1994:ATO
REFERENCES

citations/journals/tocs/ 1994-12-1/p3-wobber/.

Wade:1993:SLV


Wadsen:1998:CLI


Wagner:1983:F


Wagner:1998:DCK


Wagner:1999:BA


Wagner:1999:CFb

REFERENCES


Giessen, Giessen, Germany, 1998. iii + 151 pp.


Wayner:1993:ECD


Wayner:1993:SER


Wayner:1995:PCL

[Way95] Peter Wayner. Picking the crypto locks — with today’s hardware and a new technique called differential cryptanalysis, it’s getting easier for data burglars to crack your safe. what can you do to keep them out? *BYTE Magazine*, 20(10):77–??, October 1995. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wayner:1996:DCB


Wayner:1996:DLY


Wayner:1998:MJD


Willcox:1992:TCS

REFERENCES


[WB94]


[WB95]


[WBL99]


[WBDY98]


[WBDY98]


[WC81]


[WCS95]

Wolfgang:1996:WDI


Wolfgang:1997:WTD


Weber:1998:SMD


Wang:1999:SCB


Wendling:1999:PRS

Weber:1979:USD


Webb:1988:NPK


Weber:1993:MDC


Weber:1998:SWY


Wedemeijer:1999:DFM


Weiss:1988:BOP


Weissman:1991:IRA

REFERENCES


[WHFG92] Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbons. The active badge location system.
White:1990:CDP


White:1993:NMM


Whiting:1999:TNR


Wang:1999:CTG


Watanabe:1999:SGR

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).

Wichmann:1987:NAR

REFERENCES

Wichmann:1990:CMR


Wiedemann:1986:QC


Wiener:1990:CSRb


Wiener:1990:CSRa


Wiener:1994:EKS


Wiener:1996:EKS

for Data Internetworks, W. Stallings.


Wiener:1998:EKS


Wiener:1998:PCP


Wiener:1999:ACC


Wilkins:1641:MSS

[Wil41] John Wilkins. *Mercury, or the Secret and Swift Messenger*. ????, ????, 1641. ????.

Wilkes:1968:TSCa


Wilkes:1968:TSCb


Wilkes:1972:TSC


Wilkes:1975:TSC

[M. V. (Maurice Vincent) Wilkes. *Time-sharing com-
Williams:1980:MRP


Williams:1982:CHP


Willett:1983:TKS


Williams:1983:PAP


Williams:1985:SPK


Williams:1986:PKE

Heidelberg, Germany / London, UK / etc., 1986.


F. W. (Frederick William) Winterbotham. Secret and
Winterbotham:1974:US


Winterbotham:1974:USF


Winterbotham:1975:US


Winterbotham:1978:NC


Winterbotham:1979:US


Winterbotham:1980:US


Winterbotham:1981:US


Winterbotham:1982:US


Winterbotham:1986:US


Winterbotham:1987:US


Winterbotham:1988:US


Winterbotham:1989:US


Winterbotham:1990:US


Winterbotham:1991:US

REFERENCES


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


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


REFERENCES

Wolf:1999:USC


Woolsey:1990:DDE


Worth:1975:CMA


Wortmann:1987:BRB


World:1996:NIT


Wotawa:1999:NDD


Waidner:1990:DCD

REFERENCES

Wrixon:1989:CCS

Wright:1994:IRV

Wrixon:1998:CCO

Williams:1979:SRC

Wagner:1996:ASPa

Wagner:1996:ASPb

Wiese:1996:SSS
REFERENCES


Westfeld:1998:SVC


Whiting:1998:EVT


Wu:1995:DAC


Wu:1993:CSB


Wiener:1999:FAE


Xie:1998:BWB

REFERENCES

bibliography/073183.html

Four volumes.


[XtTmW94] G. (Gozen) Xiao, Tsung to Tai, and Yu min Wang, editors. *Mi ma hsueh chin chan = Chinacrypt'94: ti san chieh Chung-kuo mi ma hsueh shu hui i lun wen chi: 11–15 November 1994 at Xidian, China*. Ko
Xu:1997:BPK


Xu:1997:PCP


Xu:1998:STP


Yacobi:1999:RMC


Yacobi:1999:RME


Yahalom:COMPSYS-7-4-451


Yamamura:1998:PCU


Yamamura:1998:PKC


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

269–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). [YKY99]

Yi:1996:DAN


Yin:1997:REA


Yakovlev:1998:PND


Yahalom:1994:TBN


Yang:1999:DIC


Yen:1993:FCE


Yen:1995:IDSb


Yen:1995:IDSa

REFERENCES


Yang:1997:NEC


Yen:1997:SAT


Yi:1997:NHF


Yi:1998:NBB


Yi:1998:NBO


Ye:1999:CS


Yi:1998:DCB


REFERENCES


**YST99b**


**YT95a**


**YT95b**


**YT96**


**Yu92**


**Yu94a**


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

REFERENCES

Yu:1999:CC

Yuan:1992:VLD

Yung:1985:CSP

Yun85b

Yuval:1997:RTE

Yang:1997:CBC
REFERENCES


REFERENCES


REFERENCES

Young:1999:ARC

Yeung:1998:DWS

Zafiropulo:1963:RAD

Zajacz:1997:SCE

Zang:1990:ESE

Zave:1999:SDC

Zegwaart:1993:PEM
Erik Zegwaart. Privacy Enhanced Mail in more

**Zeil79**


**Zergo:1996:UER**


**Zerovnik:1996:RC**


**Zollner:1998:MSS**


**Zuquete:1996:TAC**

REFERENCES

Zeng:1990:LSM


Zviran:1993:CPT


Zhao:1997:LT


Zhang:1998:TPS


Zhao:1991:BNK


Zhao:1996:WSE


Zheng:1990:PDS


Zheng:1995:HBR


Zheng:1995:KAP

[Yuliang Zheng. On key agreement protocols based
REFERENCES

Zheng:1997:SC


Zheng:1997:DSH


Zilouchian:1998:ANF


Zhou:1994:SDS


Zhen:1994:RSS


Zhen:1998:HCE

Zieschang:1997:CPB


Zim:1948:CSW


Zimmermann:1995:OPU


Zimmermann:1995:PSC


Zimmermann:1996:PGPa


Zimmermann:1996:PGPb


Zimmermann:1998:CI


Zimmermann:1999:EVI

Reto Zimmermann. Efficient VLSI implementa-
tion of modulo \( (2^n \pm 1) \) addition and multiplication. In Koren and Kro-
nruper [KK99b], pages 158–167. ISBN 0-7803-5609-8, 0-7695-0116-8, 0-7695-
0118-4. ISSN 1063-6889. LCCN QA76.6 .S887 1999. URL http://euler.ece-
 umass.edu/paper/final/paper-127.pdf; http://euler.ece.umass.edu/
paper/final/paper-127. [ZK98]

J. Zhao and E. Koch. Embedding robust labels into images for copyright protection. In Brunnstein and Sint [BS95e], pages 242–252. ISBN 3-486-23483-8 (Oldenbourg, Munchen), 3-7029-0408-5 (Oldenbourg, Wien), 3-85403-082-7 (Oster-
.uk/~fapp2/steganography/bibliography/1006.html.

[Zhao:1998:GDW]


[Zhao:1999:BTT]

.uk/~fapp2/steganography/bibliography/073184.html.

[Zhao:1999:DWW]

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

**Zeng:1997:RRO**


**Zhou:1999:SPP**


**Zhang:1999:AFV**


**Zheng:1990:CBC**


**Zheng:1991:DBT**


**Zolman:1993:BSJ**

Leor Zolman. Building a secure journal/logging util-
ity with encryption. Sys
Admin: The Journal for
UNIX Systems Administrators, 2(6):75–??, Novem-
ber/December 1993. CO-
DEN SYADE7. ISSN 1061-
2688.

[ZPS93] Y. Zheng, J. Pieprzyk, and
J. Seberry. HAVAL — a
one-way hashing algorithm
with variable length and
output. In Seberry and
Zheng [SZ93], pages 83–104.
CODEN LNCSD9. ISBN 0-
387-57220-1 (New York), 3-
540-57220-1 (Berlin). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN

[Zhu:1996:PKC] Yuefei Zhu, Dingyi Pei,
and Dingfeng Ye. Public
key cryptosystems based on
imaginary quadratic alge-
bric function fields. Progr.
Natur. Sci. (English Ed.),
6(2):217–226, 1996. ISSN
1002-0071.

Practical approaches to
attaining security against
adaptively chosen cipher-
text attacks. Lecture Notes
in Computer Science, 740:
292–304, 1993. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[ZTR99] R. Zwiggelaar, C. J. Taylor,
and C. M. E. Rubin. De-
tection of the central mass
of spiculated lesions — sig-
nature normalisation and
model data aspects. Lecture
Notes in Computer Science,
1613:406–??, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

46: Use Java 1.2’s Authenti-
cator class. Java-
World: IDG’s magazine for
the Java community, 3(2):
??, February 1998. CODEN
???? ISSN 1091-8906. URL
http://www.javaworld.
com/javaworld/javatips/
jw-javatip46.htm.

47: URL authentication re-
visited. JavaWorld: IDG’s
magazine for the Java com-
nunity, 3(2):??, February
1998. CODEN ?? ?? ISSN
1091-8906. URL
http://www.javaworld.
com/javaworld/javatips/
jw-javatip47.htm.

cipher — IBM submission
to AES. In National Insti-
tute of Standards and


