
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/

23 July 2020
Version 1.108

Title word cross-reference

#1
[Ble98a, Kal98b, KS98a, RSA93f, RSA93a].
#10 [Kal98c].
#11 [Ano95p, Ano96-28].
#12 [RSA99a].
#14 [BG98].
#15 [Nys99].
#3 [RSA93b].
#5 [RSA99b].
#6 [RSA93c].
#7 [Kal98f, Kal98d, RSA93d].
#8 [RSA93e].

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

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

$29.95$ [Hat96]. 2n [QG90]. 2R [YLD99]. 3
[Ben99, BALS99, CK95, KSW97b, Nas94,
TK99, Wor96, YY99a]. 40 [Ano97-41]. 511
[CC98]. 64 [MM97]. 8 [Miy90]. <<
[Zhe97b]. 2 [TZ94]. x [Hol91]. A [BMT96].
A * B (mod N) [Bak92]. A^2 [JS95b],
mod2^2 [Ber93]. c [WD99b]. x^2 [HG97b]. d
[BD99b]. ℓ [BR91]. f [DJL93]. F_2^n
[SS98a, Ler97]. F_p [Miy93a]. GF(2) [She95c].
GF(208) [Ros98a]. GF(p) [Gor93b, HNM98].
> [GQW+91]. k [Car97c, DJL93, HKS97a,
HKS97b, KR99b, KS97b, WD99b]. t
[HL93a, KS97b]. L2 [Vau99a]. λ [RS99c].
L ≥ 2 [SVxW91]. ≪ [GQW+91]. m
[Bla94a, FR94]. Z/nZ [MM96b]. Z_n [SE96].
GD(2^n) [Ara93]. GF(2^m) [FBT96]. F_2^m
[MVZ93]. Step_e, m [GC90]. N
[BS91e, BS91d, HKS97a, HKS97b, KSW99b,
KSW99c, KK98, Per93, QG90, Tak97].
N = p^q [BDH99a, BDHG99b]. N^{0.292}
[BD99b]. Ω [RFLW96]. P [BS90b]. $p^k q$
[Tak98a, Tak98b].
[BDH99a, BDH99b, FJRS96]. s
[YT95a, YT95b]. $s^2$ [Kmu93b]. t
[KOO95b, KOO95a]. $T^* P$ [GPSV98].
$y^2 + axy \equiv x^3 \pmod n$ [Koy95]. z [MSS93].
$Z/nZ$ [CLL99]. $Z_u$ [ML98]. $Z_n$
[KMOY91, OFF93, VZ97, KK98].

-Adic [KG95, Tak97]. -Bit
[QG90, Ano97-41, Ano97-51, MMI97].
-boxes [YT95a, YT95b]. -calculus [RS99c].
-Cascades [GC90]. -Cheater
[KOO95b, KOO95a]. -Codes
[JS95b, MSS93]. -D [CK95, TK99].
-Decorrelation [Vau99a]. -Dependent
[DDJ93]. -DES [Kmu93b]. -Dimensional
[Per93]. -divisibility [FR94]. -Fields
[BMT96]. -fold [BR91]. -formulæ
[WD99b]. -Hash [BS91c, BS91d]. -means
[SBVG99]. -Round [BS93a, GC94].
-sequences [Bla94a]. -Span [HI93a].
-Tuples [FJR98]. -WAY [KSW97b].
-wheel [Car97c].

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

1 [Ano93k, CCN95, Nat95]. 1.0.1 [Sun91b].
1.2 [DDJ98e, DDJ98f, Zuk98a]. 10
[CMM93]. 101 [Hon98]. 1040 [Lin88a].

105-1
[Uni98a, Uni98b, Uni98g, Uni98j, Uni98i].
105-263 [Uni98i].

105-415 [Uni98j]. 105th [Ano98n].
10th [Ano93d, CMM93, IEE94e, USE96a].
1113 [Lin89a]. 1186 [Riv90a]. 11th [SUJ93].

120 [DDLM94]. 128-Bit
[SKW+98b, Dkr97b, Kmu98c, Lin98].
Luc98a, Luc99a, Luc99b, SKW+98c].
12th
[Bri92, Bri93, KG96]. 130 [Ano96b].
1320 [Riv92a]. 1321 [Riv92b]. 1334 [LS92].

1395 [Un94a]. 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, KSc90, PBD97]. 16th
[Kob96, MSDS90]. 1704 [HA94a]. 1731
[Mye94a]. 1734 [Mye94b]. 17th
[Hei96a, Kal97c]. 180 [Nat95]. 180-1
[Ano95l, Nat95]. 1810 [Ton95]. 1824
[Dan95]. 1826 [Atk95a]. 1827 [Atk95b].
1828 [MS95c]. 1829 [KMS95a]. 1847
[GMCF95]. 1851 [KMS95b]. 1852
[MS95d, MS95e]. 1864 [MR95b]. 18th
[Kra98, Yua92]. 1915 [Kas96]. 1929 [Lee96].
194 [Uni94a]. 1940 [CWM+91]. 1961
1993 [ACM93b]. 1994
[Ano94f, Sim96b, Uni95a]. 1995
[Ame95, Dan95]. 1995/4 [Dan95]. 1996
[Ano95f, UU97b]. 1997
[ACM97a, ANS97, Acc97, Ano97k, MZ98].
Uni98a, Uni98c, Uni98b, Uni98d, Uni98e.
Uni97b, Uni98f, Uni98g, Uni98i].
1998
[ANS98b, OiDP98, RD99a]. 1999 [Wa99a].
19th [Ano96a, Tv92, Wie99]. 1B [Lea99].
1st [ACM93a].
App [AW99]. Apparatus [SKBxx, MY98]. Apple [Gar97a, GO96c].

Applet [Ber97a]. applets [GPO98a, GPO98b]. Appliances [Got99].

Applicability [KCCT94a, KCCT94b, HKM95, SPP98]. Application [IBM93, BS99a, BSN95, Bar99, BGG95, BL96b, BL96a, Dam90a, Dam91a, Dav91, De 95, ECM96, FJRS96, Fum97, GPT91a, GPT91b, Gog99, GQ95, HNSS99, HHY93, Hat97, He94, Hof99, IRM93, IR99, J+91, KMPS99, K99a, K96, K95, LOX99, LC99, Mar98a, Man96b, Mun91a, Mun91b, NC97, PSN95a, QV90, QG95, Rog95, Rue93, SSS98, Sch99i, SZ93, SK98c, SK98b, SKIT99, VDDR99, Ara93, BY93c, BY93b, CC98, DDB95a, DDB95b, DF97, G921, HP94, LL97b, MW94, Nyb98, Pet91, PK97, S93b, SRR98, Siu99, Ste99b, SW98, SW99a, TY92, Woo90].

Applications [Aga92, BGR98a, BFW99, CG98, CJ98a, CJ98b, CGB+93, COZ99, Cr90, Dan96, DY91a, DFGH99, Du98, DN94, Dw97, Ebe93, FM99, Far93, Fis98, IEE95a, IEE97a, IEE92b, IEE93c, IEE94c, IEE97b, JMS96, KSH97, KSHW98, KSW99b, KSW99c, KM96a, Knu94b, KT91b, Lan97, MS95f, ODP98, OOO90, PS96b, SY96a, DY91c, TN96a, TN96b, VW98, VP96, Z9R1, vW94, vW99, ACM99c, Ada91, An98k, An98q, BM90, Ber93, BMP+97b, BV97, Boy98, BP97b, Com96, CFG96, DDP96, DIX94, Dom96, Eng99, FO98, GP98, GEL98, Gre94, G94b, HMP95, JV98a, Ka95, KW92, K93, LY93, LN94, Lub96, Mei92, Mic97, VT98, NKC94, Ped91a, PC98, Rho95, Sch90c, Sch97c, Sha95a, SSM94, Sin95a, Sta97c, SSG99, T+98, USE96e, Way98, YL93, Z9R0].

Appraisal [FGS96]. Approach [BBN96, BK94a, DGV94a, DS97c, GM99a, He97, Jak99b, K93, LMS99, Mar99, MS94, MI99, PL94, P9U99, P99, Ra98, S99b, She94a, WS99, Z9J98, Ale97, BCK98, CM96, CH97b, DH96a, DMM98, GM91, GKS97, JW01, OG95, Pau98, PGV93b, PGV94, RO96, ZL99].


Architecture [IBM93, BCCD99, CJ98a, CJ98b, Con99a, Fei93, Fei93, Gut99, J+91, MM99b, Muf93, NH90, NK98b, Oh99, PF94, RBv94, Rs90, SS90, She92a, She93c, Tre99, Tua99, VGV93, YS99, Kar96, LS98a, Con98, JD91, LM97, SV99, SY92].


Arithmetic [BP98a, Bre99, BP97c, Bus97, CD98b, DB96, KK99b, LL99, LD99, M94, NM96a, PS97, SSS98, SL93, CP98, ISO97, JS93a, Ka92, Ka93b, KM99a, Pos93].
AUSCRYPT [SP90, SZ93].

Australia [DG96, GN95b, KG93, KK99b, MSDS90, PSN95b, SP90, SZ93, VPM97].

Austrian [CFK\(^{+}91\), GN95b, Cae96a, Orl96, Ree97].

Austin [Ano94e, IEE98e].

Australasian [VPM97].

Australia [DG96, GN95b, KG93, KK99b, MSDS90, PSN95b, SP90, SZ93, VPM97].

Australian [CFK\(^{+}91\), GN95b, Cae96a, Orl96, Ree97].

Austria [AS95e].

Authenticated [BF97a, BWM98, BWM99a, Borr95, CH97, Dan95, HCY96b, JV96, LC97a, Mau97a, RH93, SKWH96, BSNP96a, BSNP96b, BF99b, BR97b, DvW92, HY98b, HY98a, Yeu99].

Authenticating [ADSW99, Hel98a, KS99a, Mit92a, SK96a, Sha97, LC94].

Authentication [ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94k, AS96, Ate95a, AR98, AC97, BA97, Bak99, Bal99, Bec99, BR97a, BG90, BR94a, BCK96d, BCK96e, BM91a, BGS98, BR91, BBDF97, BGH\(^{+}91\), Bis91, BHK\(^{+}99\), BWM98, Ble98b, BV98b, Bor96, Bor93a, Borr9c, Boy92, Bru98, BAN90, CV93, CGM97b, COZ99, DLF97, DV99, DV90, DvW92, DH90, Dra99, DMB97, DS97d, Dsw95, ECM96, EPR99b, EPR99a, FGS96, FHHB\(^{+}97\), FL96, GHY90, GLZ99, GL96, Geh94, Geh95, GN94, GM90, Gol90a, GBL94, Gue98b, Gui97, HK97, HA94a, HS94, HL92, Hil97, HJP97, HP98b, Ins95, IH98, JSSZ94, Joe98, Joh94, KR95b, Kau93, KA98a, Koh90, KN93, KCCT94a, KCCT94b, Kae94b, Kra95, KBC96, KBC97, Kae94, KK95, KYG92, KY93, KS97c, LAB91, LAB92].

Authentication [Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Mau96a, MAM95, Mc96, Mee98, MS95c, MS95d, MWW94, MTV92, Mor97, Mye94a, Mye97, NP97, OG97, OOK91, OM94, OPP96, PKOT94, PS98c, PLW99, PGN91, PV93c, Pre98a, Pre98c, MS95e, RS99b, RS9W97a, RSW97b, Rog95, SNT93, SN93, ST94, SNT95, SN98a, SN98b, SSH93, SS96, SLP99, SA95, SC96a, SCxx, Sch94d, Sch99k, Sga90, Sga91b, She97, She95a, Sha96, Sin96b, SVxW91, SW94c, SKAM99, St91b, SL99, TAP90, TA92, Tay95, TSN93, Tun99, Ude98, Van95b, Van93, Wal93, WKH97, WK96, WABL93, WABL94, WLB92b, WLB92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC\(^{+}98\), Ano95g, Ano95a, Ano95x, Ano96v, Ano96x, Ano96y, Ano96-27, Ano97d, Ano97t, Ano97p, Ano97-27, Ano97-43, Ano97-53, Ano98s, Atk93].

Authentication [BSNP97, BGR95, BCK98, BCK97, BGD97, BGDH\(^{+}95a\), BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gau90, HS96b, Hor95, HC95b, HLL\(^{+}95\), HW98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin98a, Low95, MSN97, MF97, Men91, MC96, Nac93, NT94, PS98e, PS98f, PS98h, RS98a, RS98f, Sch99, Sga91a, Sga93, SY96b, Sta99b, Sti91a, Sun98b, Syv93, Tsu92b, Tsu92a, TH99, Ver98b, Web99, WL94, XA98, Xie98, YL97a, YL97b, Yon97, ZK98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a].

Authentications [OO90, KSL92].

Authenticate [Zuk98a].

Authenticators [DF91a, SN96].

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

Authenticon [Fly97].

author [Lea90].

Authorisation [COZ99].

authorities [Ame95, Ame96a].

authority [CFSY96, CGS97, JMO95a].

Authorization [BDPS95, Cas95, FL96, Woo90].

Auto [YY98c, YY99b].

auto-certifiable [YY98c].

Auto-Recoverable [YY99b, YY98c].


Automated [Dan97, FIP93a, FS93, FK99, GSN94, GDS91, She96a, SGPV98, VDDR99, WG99, CD98a].

Automatic [CWM\(^{+}91\), MM99a, Na97, SK97b, SK97a, Sch99k, WKH97, DF98, OAA99].

Automating [Bur99, Smi93a].
Blacklisting [KRS99]. Blackmailing [Jak95]. BlackNet [MLLG95]. Bletchley [Ano97-48, Sal93, Cla98c, HS93, Smi98b]. Blind [CPS95, Eri97b, JLO97, LK99, LR98, NMV98, NMV99, Oht98, PS96c, RGV97, SY96a, SYM98, HMP95, Tra97, XA98].
blindfolded [JY96]. Blinding [Bra95c, Kra99, FY95c]. Block [AB96a, ABK98b, AKR94, BAK98, CD9N8, Cle91, CJM95, DGV94a, DKR97b, DKR97a, DR99a, DDK99, De 99, DW94, DK97, DK99, KR94a, KVR9, Knu94b, KP96a, Knu98b, Knu98c, Knu99b, Kob99, Lm93a, LM93b, LM91b, Lim98, Luc98a, Luc99a, Luc99b, MNSV97, Mas94, Mat96a, Mat97, MT99a, MSDK99, Pat99, Pre97a, QC90, RRS99, Rob95a, SZ96, Sch94b, SK96c, SK96d, SKW98b, SKW98c, SKW98e, SKW98f, Sch99d, Vau98b, Vau99, YL98H, YL498a, YLC99b, ZM90, Zhe90, Al9a3a, AW95, BKR98a, BKR98b, B93, BS95a, Har96a, HLMW93, HX94, IS97, Jak99a, KL95b, LM91a, Lai92, Mei94, MM97, NO96, Nyl95, PGV93b, PGV94, RT93, RP95b, Roe95, SB95, SAM97, SH99b, SK99b, SKD94, TY94, YL97c].
[Fra99, Hir97, Hir98, Don98, Hin93].

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

Broadcasting [CW91a, CWY98, LC96b, CC95, HLLC96, LHW99, WY93, LC96c].

broke [Dav98a].

Broken [CP91, Mey99, MLLG95].

Bronze [Duh90].

Brother [Wai95, Hof95, Des96a].

Brothers [Hat96].

Browser [GW96, Law98, She96b].

Browsers [DDK98].

Browsing [GGMM97].

Brute [CD98c].

BSA [Bar97].

Bucket [Rog95].

Budget [UU97a].

buffer [Mei98].

Bug [DDJ98c, Ano98t].

Builder [Pin98].

Building [HWKS98a, HWKS98b, Hat96, Hof95, MAM95, NT99, Wai95, Yor96, Zol93, Fb97, NIS92, PVO95, Tas98].

Bulk [SVBJ96, Whe94].

Bulk-FFT [SVBJ96].

Bull [Taa98].

Bulletin [CWM+91].

B¨ulow [CWM+91].

burden [Wil98a].

Bureau [Uni97d].

bureaucracy [Rat96].

burglars [Way95].

Burlington [IEE96a].

Burns [DDJ98b].

burst [Sch93a, UNU94].

Bus [CC99c, Kuh98].

bus-encryption [Kuh98].

Bused [FVEA99].

Business [Ano93i, Ano96-29, Ano96-30, Ano97-33, Ano98t, AMP94, AvO98, CFK+91, GC97, Lic94, MB99a, SM99, Uni98].

Businesses [MB99a].

butting [Sto98].

buyers [MB99a].

Byte [Mas94, PV98, YLCY98a, YLCY98b, CFK+91].

Byte-Oriented [Mas94, YLCY98a, YLCY98b].

Bytes [Yuv97].

Byzantine [Bea92, Bor95].

C [Sha99a, vDWS97, vS97, Bak92, Bas98, BMS99, DSB99, Gar98b, Hel98b, Kaj92, MGL+98, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b].

C0YNTHIA [WBBL99].

C2 [Ste92].

CA [RD99a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, Wl99].

Caching [STSW99].

Cactus [Ano97-33].

CADE [HB99].

CADE-16 [HB99].

cAESar [Koe99].

Calculating [CFK+91].

Calculation [HRVV99].

Calculators [CWM+91].

Calculus [ABLP93, AG97b, AG97c, AG97a, RS99c].

California [AMC93b, ACM98a, Ano97a, Ano98t, Ano99, Com96, Cop95d, Des94b, FJ97, IEE92c, IEE93b, IEE94d, IEE95b, IEE97b, IEE97j, IEE97i, IEE98a, IEE98b, IEE98d, Kal97c, Kob96, Kra98, Nat98, RP97b, Sti93b, Sti94, USE92a, USE96e, USE96d, USE96f, USE99d, Wie99, van96, Sch98b].

Call [VCF+90, Zav99, Miy90].

Call-Coverage [Zav99].

called [Way95].

Cambridge [And94a, And96c, CFK+91, Chr99b, Gol96d, Lom97, RBCE99, Sch94j].

came [Fro96].

Camera [Fri93, SKWH96].

Campbell [CFK+91].

Campbell-Kelly [CFK+91].

Campus [VNW94].

Can [Ano93c, BF99a, CP91, Cha93, CD98b, CMY97, DY91f, EvH91, GSV99, NMVR95a, NMVR95b, NMR95, Riv98b, Sim98c, Ste95, BGV97a, CG05, Ev92, EvH93, LF97, NOVY93, Sch91b, Ude98, Way95].

Canada [AMC94c, CFG96, GS94b, HA00, IEE94f, IEE96d, TM99, Yua92, Roh99a, Tas98].

Canadian [CFG96, GS94b].

Candidate [Bas98, BCA+98, Dra98, GLC98, Gla99a, Huh98, KMA+98, Nat97b, Nat98, Nat99b, Out98, RD99a, RD99b, Sot98, SB99, GGH+98].


Cannot [BCE+94].

Can’t [WT99].

Cap [Lea99b].

capability [BC96a].

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

Capstone [YY96].

carcinogenic [SBTV99].

Card [Bov98a, Bov98b, Chr99a, DVLQ96, EN98, ENK99, Gar97a, GPS98, HP98a, Hru96, HH99, Hus99, Kra99, Mar98a, Omu90, SGPV98, Sut99, T+99, dWQ91b, dWQ91a].

[13]
Ciphers
[Ada97a, ABDV98, AAG\textsuperscript{+}00, AB96a, BR99a, BDR\textsuperscript{+}96, CDN98, Cha94a, CS91, Cle91, DR99a, De 99, Din94, Fi95, Gus96, JKR97, JKR98, JKR99b, KSW98a, KSW98b, KSW98c, Kn94b, Kn94a, KP96a, Kn98b, Kn99b, Kol99, LMM91, LM93a, LM93b, Luca6a, Lu96b, Mat96a, Mau91a, MS91, MT99c, PRS99, Pat99, PK95a, PK95b, Pen96, Pra96, Pre97a, Ree98, RP97a, Rob95a, Rob95b, Roe94, She94a, She94d, SM91, Vau98b, Vau99a, YY98d, YY98b, ZM90, Zhe90, Abe98b, BKR98a, BKR98b, CD98a, Cou99, DG94b, DXS91, FSN93, Gar96a, Gar97d, GSN94, Go95b, Har96a, HLMW93, HXMW94, HS94, Jak99a, JVR98a, Lai92, LMM92, LRW93, Ny95b, PGV93b, PG94, Rev91, RP95b, Roe95, SB95, SAM97, Tay94, Win93, Wri98b].

Ciphertext
[BK98d, Ble98a, CG99, CD97, CS98b, Dam91b, LL94a, MRS99, Miy93c, R91, Riv93a, T94, ZS93, CP94, NY90, Sah99, SG98, Vu95].

Ciphertext-Only
[BK98d].

ciphertexts
[Des95].

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

circulating
[Ano96-29].

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

Cisco
[Sav96].

CISST
[AA97].

City
[IEE99a, USE95b].

Claim
[GO96c].

Claims
[DS97a].

clandestine
[Wri98b].

Clar
[USE93].

Class
[vD97, Ou99, Uni96b, FR94, HWB93, KSB96a, LZ90, LZ91a, Zuk94a, vT94].

Classes
[Haw98b, Pa99d, Haw98a, Sze98].

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

Classification
[BD90, LSVV95, PFK95, Uni96b].

Classifier
[CBM99].

Claude
[Hor92].

Claw
[BHT98].

Claw-Free
[BHT98].

clearly
[Los98].

Click
[WSFC99, Ken95].

Client
[DL99, Kon95, Oh99, SL99, GGK\textsuperscript{+}99, Sin95].

client-relationships
[GGK\textsuperscript{+}99].

Client-Server
[DL99, Oh99, Sin95].

Client/Server
[Kon95].

clients
[AG95, Bee96].

Climate
[TGK99].

Climbing
[MCD99].

Clipper
[Pri94, Fro96, Ban96, Buc95a, Hof93, Kan96, MS95f, RK94, Smi94a, Uni95a].

Clipper-like
[MS95f].

Clipping
[Hof93].

cliques
[JP96].

Cloak
[Gre90].

Clock
[DHSS95, Go96b, Ga94, CS96b, CS97b, GM91, GO95, Men95b].

Clock-Controlled
[GO96b, GM91, GO95].

Clocks
[DG95, DT96, Yah94, Gon92].

Closer
[Coh96].

Closure
[MOM91, PS93a].

Clueless
[RS98c, RS98d].

Clustering
[DDJ98a, HE98, KUN97].

CM
[CNST98, Koh91a].

CM-curves
[Kob91a].

CMOS
[BS95c, ECD\textsuperscript{+}99, YS99].

Co
[Gla99b, LFCK99, Sut99, NM96a].

Co-dimension
[LFCK99].

Co-operation
[Gla99b].

Co-Processor
[Sut99].

co-processors
[NM96a].

Co.
[CFK\textsuperscript{+}91].

Coast
[SZ93].

COBOL
[Ga97c].

Code
[CJ99, HR90, JKR99a, Kip99a, Kur94, Mv93, PV98, QD91, Sch94g, Sch96a, Sch94h, Str95, Tod97, WK79, WF94, Zim95b, Ala97, Ano97i, BSNP97, CC98, CL98, GA98, HM97b, LJW97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG\textsuperscript{+}00, Mea98].

Code-Breaking
[QD91].

code-cracking
[WS96c].

Codebreakers
[HS93, Kah96b, Smi98b, Yu99].

Codebreaking
[Car97c, Car98, Dre92, Sch98a].

coded
[HG97c].

codemaker
[Mar98b].

CORDER
[St90].

Codes
[ACM94b, AW94, AR98, BGS96, BVFD99, CCZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, Gib91, Hof99, Joh94, JS95b, JJ99b, KKS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWSN99, Pen96, Pra96, Pre98a, RV99, Rus93a, SN93, SNW98a, SNW98b, SD99, Sga90, Sga91b, SB94, SVx91, Sta96b, Sti91b, Ton96, Van95b, Wri98b, Ada91, Ala93a, AW95].
Commutative [MB99a].
Companions

Companies [Ano97j, Ano97y].
Company [GC97, Ano96g, Kar96].
Comparative

Company [GC97, Ano96g, Kar96].
Comparisons

Computer [ACM93a, ACM94a, ACM97a, Ano93d, Ano97-50, Ano98c, Bac95, BK90, Ber96b, Bre99, CWM*91, CO98, De 98a, De 93b, De 98c, DQ93, Des92, DEQ92, FJM*96, GMV98, HM91, HM92, Hig97a, Hig97b, Hor94, IEE92a, IEE92b, IEE92c, IEE93b, IEE93c, IEE94b, IEE94c, IEE94d, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE99a, KT99, KK99b, LBMC94, LC95, MDP94, NIS92, Nac97, Neu92, OD99, PGV93d, Q98, Sa91, SSS98, SK96a, SK99, Sho97, Ste91, SJ93, VGP93, Ver98a, VGG99, Whi90, AFB95, Ano93k, AC97, Bur98a, Car97c, Car98, CW91a, Coh94, GBL94, Gru98, HLLC96, IEE92d, IEE95c, Joh98, LS98a, LFSY94, LC96b, LC96c, Mat98, NT94, Nis91, PR98, Riv98c, Sph99a, UCF94, Wil93a, Woe97, W090a].

Computer-Related [De 93b, De 98c].
Computers [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98a, ACM98b, ACM99b, Bak92, BDDG99, BV96, Br94a, CFK*91, DDDJ98d, DDDJ98b, DDJ99, Dwo95, FP99, GC98, GN95b, IEE94e, IEE96b, JJ98b, Kon95, Law98, MMM*98, Mau94, MW99, NS98a, Pen96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b, W90].

Comprehensions

Comprehensive [SSP90].

Comprehensions [MT95].
BGT96, CWM+91, DiDPS96, FM91, FJV97, HK99b, HC95a, KG93a, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK+91, PH91.

COMSEC [Mye98]. concatenated [LYG94]. concealed [Ano97i, CZ90, Lea90]. Concealing [CD97, Beu94, Joh97b].


Condition [Sta96b]. Conditionally [Des90b]. Conditions [GS99a, Rus93b, Ga99]. Conducts [Law98]. Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95r, Ano96r, Ano96a, ???97, Ano97i, Ano97g, Ano97a, Ano98b, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BS95e, CH96, Cha91, Cop95d, DDJ98a, Dan96, ES98, Far93, Fra99, Fum97, GN95b, GQ95, Hir97, Hir98, IE99a, IE99b, IE99c, IE99, IE99a, IE99b, IE99c, IE99d, IE99e, IE99f, IE99g, IE99h, IE99i, IE99j, IE99k, IE99l, IE99m, IE99n, IE99o, IE99p, IE99q, IE99r, IE99s, IE99t, IE99u, IE99v, IE99w, IE99x, IE99y, IE99z, IRM93, KG96, Kat97, KM96a, Kra98, LOX99, LP99, Mau96b, MSD99, NS92, Nat98, Nat99b, Nyb98, OW95, OD95b, PSS95b, QG95, RD99a, RD99b, Sc94m, Sj97, Sik93, Sti93b, Sti94, T+98, USE91, USE92a, USE92, USE95a, USE96a, USE99b, USE99d, Wal99a, Yu92, ACM99c, Ano93d, Boy95b, BD95b, Cop95b, Dar97, DG96, Des94b, HOQ97, HI97, IE99d, IE99e, IE99f, IE99g].

Conference [IE99b, Kal97c, KG93, Kob96, LM98a, SP90, Ste99b, USE96f, USE98c, USE98d, VPM97, Wie99, Ano95f]. Conferences [BDHK93, MZ98, Sch95f]. Conferenceing [Ano99f, KBR97, WW98a, Lam99].

Confidence [Chi99a, Chi99b, Graxx].

Confident [Jan95]. Confidential [Bet95b, Bet95a, vD97]. Confidentiality [Ano98t, Jac96, Riv98d, ZG96, FT95, MI90].

Configurable [VMS97b, VMS97a]. configuration [HI97]. Confiner [Oka94, Cha95b, MS98b]. conflict [All97].

Conflicts [ACM94b]. confounder [BT99]. confrontation [Za97]. confused [LL98b].

Confusion [GC97]. Cong [Mye98].

Congress [Uni97a, Uni98c, Uni98d, Uni98e, Uni99d, Uni97b, Uni98f, Uni97c, Uni95a, Uni98k, Mad97].


Connect [Lic94]. Connection [Kas96, CV99]. Connections [SG98, SGR97, Yu94a, Yu94b].

Connectivity [Pit96b]. Consequences [KP95, Sim94a]. Conservation [Bro94].

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

Considered [LT91]. Considering [HH94].

Considers [Ano95p]. consistency [ZY90].

consortium [Buc95a]. Conspiracy [WK97, Sc92]. constitution [Mad98b].

Constitutional [Bas95]. Constrained [Gol96b, Has99].

Constraint [SG95, WS99, GMLH94].

Constraint-Based [WS99]. Constraints [DS98b, Ou99, Koz96].

construct [Lon92, Sun91a, ZI98]. Constructed [Rus93a]. Constructing [Ada97a, AB99a, AB99b, DT93, Gal99, KTM+99, KBR97, XL98, ZZ96].

Construction [BCK96c, BR99a, BR99b, CNST98, vD95a, DSB99, EMD93, GPSW98, Joh94, Kim93, KYDB98, NR98, SVxW91, ZMI90, BCK96a, BCK96b, BCK96c, Bi93, MPL99, OS91, OS92, Pet91, vD95b].
Constructions [AHV98, ABDS96, KRS99, SNW98a, vHP93, MS98b, SC97].
Consumer [IEE97g, IEE98c]. consumers [Weh99]. contactless [DS98a]. contain [Lea90]. Contemporary [Knu99b, Sim92].
Content [Ack98, JPLI99, KR98, MW98b, MR95b, PMP99, Ros93, SC96a, Way93a, SNT95].
Content-Addressable [Way93a]. Content-Based [PMP99]. Content-MD5 [MR95b, Ros93]. Contents [vHH97].
Continued [KE97]. Content-Based [MM96a, context-free [Ili94]. Continue [Ano96-24]. Continued [Ke97].
Continues [Ano97-44, Ano97-45, Ano98q, DDJ98d, Ano96-29, Mad99b].
Continuous [BP95a, NHB98, She95a]. CONTENTS [vHH97]. Contents [vHH97].
Corresponding [Oka93b]. Correctness [FHM98, Gai90]. Correlation [CS91, HT99, JJ99a, CS97b, CW94, LL93b, LM93c, Mad99b, Mat91, MLA91, RO96, RT93, S99, Uni97d, WWW95].
Contrast [HKS97a, HKS97b]. Contrast-Opposed [HKS97a, HKS97b].
Contribution [Lud97, Mus92, SS97, AK98, Blo98b].
Contributions [Hill94]. Control [ABL93, Ban93, BDPS97, FDT97, FY99, FL96, Hwa97, JPLI99, Kas96, KA99, KKW99, Lin98, Mey96a, NW98, NAA99, NS98a, PRAM98, Per99, STS99b, She93a, She93b, Sim90b, Sim91, ZHJ98, ACC99, Ano93d, BGT96, CWM9+91, CS96b, CS97b, CW94, LL93b, LM93c, Mad99b, Mat91, MLA91, RO96, RT93, S99, Uni97d, WWW95].
Controllable [CTT94]. Controlled [GPR98, GO96b, Go94, Jak99e, SKBxx, GM91, GO95, Men95b]. Controller [CIBM99, FCH99]. Controls [Ame96b, Ban94, Cil97, UU97b].
Correcting [AW94, AR98, BGS96, DLR97, KKS97, LC99, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, Ste95, Wan92a, YL97a, VT94].
Correction [Ano96f, Cha99c, MG91, WN98a, WL92c, Ala93a, WL92a]. Correctness [FHM98, Gai90]. Correlation [CS91, HT99, JJ99a, JJ99b, KSB96a, MS91, PK95a, PK95b, Pen96, GO95, Har91, Mat95, SG9D99]. Corresponding [Oka93b].
Counteract [CJRR99a]. Counterfeit [ENK99, Ano93a, van96].
counterintelligence [Mon96]. Countess [KT99]. Counting [K996, MVZ93, KK98, SF97]. Countries [Gar97a]. County [IEE96c, IEE96f]. Course
[CM99d, Kob94, Nic98a, Nic98b, Sch99d, Coh94, Ger97, PGV93d, PR98]. *court*

[Ano96d, PSB97]. *Coverage*

[DS97a, Zav99]. *CPU*

[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. *CPL*

[Kea99]. *Crack*

[Ano96d, PSB97]. *Coverage*

[DS97a, Zav99]. *CPU*

[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. *CPL*

[Kea99]. *Crack*

[Ano96d, PSB97]. *Coverage*

[DS97a, Zav99]. *CPU*

[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. *CPL*

[Kea99]. *Crack*

[Ano96d, PSB97]. *Coverage*

[DS97a, Zav99]. *CPU*

[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. *CPL*

[Kea99]. *Crack*
Bra98, Bri98, CP91, CRS98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, Sti98a, Wil98b. Crypto-Chip [HMV94]. Crypto-Coprocessors [HP98a]. Crypto-Engine [BE90]. Crypto’91 [DBGV93]. Crypto’95 [NS98b, NS98c]. CryptoAPI [Boy98]. CryptoBytes [Cry95, Riv95e]. cryptochip [PP96]. cryptograms [Har94, Web93]. Cryptographers [WP90]. Cryptographic [AG98a, AG98b, IBM93, Ano96i, Ano98f, Ano98e, Ano98b, AB97, BDPNSN95, BDPSN97, BH93, BY93a, BGM97a, BGM97b, BBT94, BMT96, BFKL94, Bol98a, Bol98b, BDL97, BDP97, Bra95a, Bra96, BD91, CS96a, CJ99, CJ99, CP98a, CP98b, CPOR97, CF95, CD99, Cop94b, Cre97, DGV92, DC98a, Dam90a, Dam91a, Dan97, DIF94, DY90, DY91a, DY91d, DY91b, De 95, DS97a, DF91c, DK91, ECD+99, Ell98, FGR92, Fis98, FGR96a, Fum97, GI99, GS94a, GK99a, Gol96c, GS97, GQ95, Gut99, HHT93, HHT97, Hel94, Hwa97, Il96, Iev91, JDB+91, JD91, KN98a, Kal98f, Kal98d, KV94, KS99, Ka93, KP99b, KP99c, KT91b, KT98, KS97b, LMJW93, LL97a, LHB96, LM96, Mac94, MM99a, Man96b, Man97b, MS90a, Mii96b, Mjo93, Mos98, Mun91a, Mun91b, NM96b, Ng99, NS99b, NR94]. Cryptographic [NK98b, Nur94, Nys99, ÖPH+99, Oka93a, OS98, PS99d, PV97, PS96b, PW98, PBGV90, Pre93a, PGV93a, Pre93b, Pre94a, PD97, PR98b, Pre98c, PR98a, Pre99, Pre94b, QV90, QG95, RSA93d, RS93, Ritxx, Rue93, SI94, SZ96, Sak96, DY91c, Sch95f, SK96a, Sch98d, SK98a, Sch91c, Sch93f, SPS97, SZ93, SZZ95c, Sha99a, She92d, SBB99, Sm90, SY92, SM91, Ste96, Sy92, T+99, Tou91, Tou93, TY996, VCF+90, Vig98, Wai95, YS99, YY97c, YY98a, ZZ95, ZM91, AN94, AN96, AG97b, AG97c, AG97a, Ano97-32, Ano98g, BD92, Bol97, BV97, Com94c, CDG95, Cl99, DD95, Dan97, Dhe98, Di 99, DFR91, Don98, FGR96b, Fra96, FL93, Gol96a, GEL98, Han95, Han97, Han99, Har91, Hof95, IS99, Jen98, JW91, JP96, KS90, Kob91a, LRW93, Lai95, Lea90]. Cryptographic [Lev91, LL93b, Lub96, Mau91c, Mea95, Mol98, Mru92, IPNdbbbpr91, NT93, Nyb98, Pau98, PKM97, Ros97c, Sch93g, SZZ94a, SZZ95b, Ste99b, Way98, WN94, XZZ97, XZZ98, YS91, ZZ97, ZLX99]. Cryptographic-Token [Nys99]. Cryptographical [KP95, GvP98]. Cryptographically [BSD98, Cha90, CvHP91, H994, PGV92, ZZ96, DT93, IS97, KSB96a, MCD98b, SKB97, Bou94]. Cryptographically-secure [Bou94]. cryptography [ANS97, ANS98b, Ano97k, Ano99l, AA93, ABDS96, Av98, BCE+94, BGG94, BGG95, BGR98a, Bel98, BB+91, BBE92, Bir98, Bla93, BK95d, BL96b, BL96a, BGV93, Boy95a, Bra90a, Bra94a, Bus97, Cae96b, DDJ98a, DL96, DP98a, DP98b, Dav91, Dav96, DG96, De 93c, Des94a, DHQ98a, DHQ98b, Des98c, Dit90, DNN91a, Dro96, Dwe97, Ele99, Eri99, Fer99b, Fis97, FBS97, FJM+96, FJRS96, FGLP96a, FGLP96b, Gan93, Gem97, Gol95a, Gol97a, Gol97b, Gon98, HK99a, HP98a, HSS99, Hat96, Hed97, HL93b, Hir98, HAH94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLM96, HH98, HBLK99, JR96, KM97, Kal97a, Kal98e, KS98a, Kal99, KSS+92, Kn98a, Kob94, KA91, RSA93f, Lac93, LM94b, Lin96a, Los97, Mad98b, MY91, Mau99a, Mau99b, Mau97c, Mc96, MP91, Mit92b, Mks99, NC97]. Cryptography [Nic98a, Nic98b, PAK+98, Pat96, P95, PT95, PGCSN96, Por91, PB99b, RSA99b, Rad97, RHE94, Rit99, Riv90b, Riv93b, Riv97b, Ros96d, RK99, Sla99, DP91, Sas99a, SKB99, SSP98, Sch94c, Sch96a, Sch96b,
cryptography [FM91, FK93b, Fra99, Fra93, Fri96, Gar96b, GZ91, Gen99c, Gol99a, Gol97c, Gre94, GTGW94, HA00, Hir97, Hru95b, Hwa91, Hwa93, IZ98, IZ99, Imp92, Joh97b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Loc90, vdL98, Lue95, MB94h, Mat98, Mun93b, MY98, Mei96b, MVV97, Mic97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Nyb94, Org98a, Od94b, Par96, PG97a, PG97b, PC98, PP92b, PV93d, PR98, Riv98c, Rot95a, Sal90, Sal96, Sch92c, SM94+97, SMD99, Sch99e, Sch90c, Sch97c, SPP98, Shp99a, Shp99b, Sin99, Sin99b, Sh98, SMD99, Sta96d, Ste98a, Tas98, TM99, USE96c, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wa99a, vs97, Sha99a].
cryptography-dedicated [NM96b].
Cryptography-in-the-Large [Bla93].
Cryptography-in-the-Large [Bla93].
Cryptoki [Ano96-28].
Cryptol [Lac93].
Cryptologia [Ers99, DKK+98, Joh98].
cryptologic [RK98b].
Cryptologie [Bra93b, Bec90, Sch98e].
Cryptologist [Pin98, Sch94a].
Cryptology [Ano93g, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dam90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ana97-37, Bau97, Bec88, CW94, Cop95b, Cop95d, Dam91a, Dam99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, Hei94, IRM93, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mun96b, McC90b, Mei92, MV91, New97, Nyb98, OiDP98, PSN95b, QV90, QC95, Rat96, Ruc93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Unixxb, Uni95b, Web93, Wie99, Wil98a].
cryptography-dedicated [NM96b].
Cryptography-in-the-Large [Bla93].
Cryptoki [Ano96-28].
Cryptol [Lac93].
Cryptology [Ers99, DKK+98, Joh98].
cryptologic [RK98b].
Cryptologie [Bra93b, Bec90, Sch98e].
Cryptologist [Pin98, Sch94a].
Cryptology [Ano93g, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dam90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ana97-37, Bau97, Bec88, CW94, Cop95b, Cop95d, Dam91a, Dam99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, Hei94, IRM93, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mun96b, McC90b, Mei92, MV91, New97, Nyb98, OiDP98, PSN95b, QV90, QC95, Rat96, Ruc93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Unixxb, Uni95b, Web93, Wie99, Wil98a].
[BDHJ98, BHSV98b, BHSV98a, BS91b, BLM94, BS91c, BS97a, BS90b, CGJ+99, DP98c, ESST99, FY98a, FY98b, FY99, GJKR99, GPCSN96, GGH97b, Gor93a, HGS98, HMV93, Hes97, HR90, Iss90, Kal98g, KL95a, Kor93, KV93, KKOT91, KP93, LH93a, Len99a, Men93, Men95a, Mic93a, Mic93b, Mi93b, MOM91, MM98a, MM98b, vO91a, Pai99a, Pai99d, Poi99, RY97, Rud91, Sma99, Son99, dW91b, Wie98b, WZ99, Yam98b, YY99b, dW91q1a, vO91b, AA99, Ale92, And94b, APDS93, B190, BS91a, BS90a, Bih92, BF96, B197, BBL95, BK98g, CZ90, Ca90, CC98, Cha95a, CL97a, CNST98, C199, Com90, Des90b, Des90a, DF90, Des93, ES97, FK94, FSS94, FGMY97a, FM99a, GOL90, GH99, GP97, Has99, HNM98, Hor99, JM96a, Jar96, JQ98a, KM99a, Kob90, Kob91b, Koc90, Kob97].

cryptosystems [Kos99, LL96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Mi93a, Mi99, MS99c, Moo92, MV98, NM94, NY90, Odl90, OS91, OS92, Rac90, SS98a, SS98, SS98a, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, YM98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, Wai98].

CS [Ano93c, Ano94a, Pin98, SV98, Vau99b, Vau99c].

CSP [DS97d].

CTS [BR96a].

Cube [Per93].

cubic [CL99, GH99, Koy95, KK96].

cultivate [AHdJ97].

Cultural [UFC94].

cultures [Rat96].

Cumulative [GPSN98, JM93].

cunning [Ben94].

Cunningham [YY98a].

curbs [Ano99n].

Current [J98c, Ril98].

Curve [AMV90, DP98c, Dem94, ESST99, Fer99b, HSSI99, Kal97a, Kal98g, KMK99, Kob98c, Len99a, L99d, Men93, Men95a, Mi93b, OFF93, RY97, SOOS95, SW93, WZ99, AMV93, ASM98, BC90, FM99, GP97, HNM98, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LLH96, MV90, Mi99, SX90, VZ97, Wri98a].

Curves [Ano95u, BS91a, CTT94, De98d, DMPW98, Hes97, JQ97, KM97, KMOV91, MS93, MM96b, Mi96, SSNP99, BGR94, BBI90, BS91a, BSS99, CPPK98, DLL99, Eng99, FR94, Ga99, GLV99, GK99b, IS99, Kob91a, Koy95, KK96, Ler97, Mau91b, MVZ93, Mi93a, VZ97, XL98, Z98].

Curvilinear [SCG99].

Cusick [YT96].

Custom [Nor95b].

customer [Nor95c].

Customised [GN95c, HHD99].

Customising [NO96].

Cut [BLM99].

CutRes [BLM99].

Cuts [Gar98b, Den95].

cyaneide [Mar98b].

Cyber [An971, Ano97-50].

Cyberbanking [Mur96].

CyberMall [Mar95a].

cybernetics [LS98a].

Cyberpunks [HM91, HM92, HM95].

Cyberpunk [HM91, HM92, HM95].

Cyberpunking [Zm96b].

Cyberspace [Ber97b, Coh9b, Gar97c].

Cyberwar [Kan96].

Cycle [GAGCDAFC99].

cyclic [PS97].

Cycling [GS99b].

cyclotomic [SW95a].

Cyclo [Bos90].

cylinder [Cas90].

cylinder-cipher [Gad98].

Cylinder [An99d, CMKK98].

cyphers [Gar93].

czar [Saw97].

Czech [Ste99b, vWN99, Hru98].

D [Ben99, BALS99, CK95, Nas94, TK99, Wor96, YY99a].

D.E.S. [Cle91].

D.S.A. [NMVR95a, NMVR95b].

Dabbling [Ritxx].

DAEs [J98v].

Dallas [ACM98b].

Damgård [DG93].

Damgård’s [Rib90].

dan [IPNdbbbprm91].

Dark [YY96].

DASS [Kan93].

Data [Ada92a, Ali97, Ano92c, Nat93b, Ano95f, Ano96c, Ano97e, Ano97f, Ano97g, Ano97a, Ano97-40, Ano97-42, Ano98b, Ano99f, Ano99a, AWV99, BGML96, BRS99, Ber98, BS95b, BS98, BY92, BW98, BKZ98, Cle96, Con99b, CH99b, DC98c, DFGH99, EKLM99, Ga990, Gre90, Gui97, HS96a, Iut91b, JMLW94, Karp97, KH98b, LvdLB96, LT98, MPPS95, MSH99, Mc97, Nat93c, Nat93a, NHB98, OA94, Sch99b, Sch94m, See97, Sme97, Sto90, SZT96a, TYD99, Tay90, TLS99, Way91, WSFC99].


DeTeBerkom [GH96]. Detectable [Vv97]. Detecting [Gor93a, Mad92, PM98, SG96b]. Detection [BS95d, ENK99, H LCD98, LT98, LML98, Ruo94, TYD99, ZTR99, HC96, MHMW98]. Determination [Bie98]. deterrence [van96]. Developer [CM99b, Di 97b, DT98b]. Developing [CF95, SCT99]. Development [Ano97h, Bar99, Bas93, GRB99, HNSS99, IR99, LL93a, Nat99c, Natxx, VDDR99, Way98, You96, AMV93, Ano91-52, LS98a, Mi95, NBD99, Sta97c]. developmental [Ram92]. Developments [Ano95a, PRB98a, Sim97]. Deviates [Ran01]. Device [Hru96, Ano91b, CM97c, Uni94b]. Devices [BDHJ98, Ano95t, Hwa92b, Hwa92c, LS98a, Pos92, Pos93, Uni94a]. devoted [FT99b]. DFC [KR99a, Ste99c]. DGSA [FM98b]. DHCP [Dra99]. DICTA [KG93]. Dictionary [Jas96, Luc98b, BCR98]. Diction [P94]. Different [KBS97, Sch99b, RT93]. Differential [BB94, Ber93, BS90a, BS91c, BS91e, BS91d, BS91f, Bih92, BS93b, BS93a, BS97a, BK98d, BKPS93, CJ98, Con99b, Dae95, Din94, Fer98, Haw98b, Haw98a, KTM99, Kau96, KM98b, Kob99, KJJ99, Kwa93, LMM91, LH94, Lan95, Mat96a, Msr93c, MSK98, NK93, OM94, Pai99a, Sch96c, SMK98a, VKR98, Wag98a, YLH98, Ad92b, CV95, KY95b, KYxx, KMM96, LMM92, O’C95, OG95, RP95b, TN97, Way95, YT95a, YT95b]. Differential-Linear [Haw98b, LH94, Haw98a, Lan95]. Differently [Ny94]. Differentials [BBS99a, Fer99a, KRW99, BBS98a]. Difficulty [KP96b, Riv93a, ZZ96, Hor99, Riv95a]. Diffie [Ano97a, BY93c, BY93b, BRR99, BMW99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY98b, HY98a, Kal97a, Koe95, Koc96b, Lut98, Man94, MW96c, MW96b, MW99, RSA93b, Van95a, VW96, WM93, vOW96]. Diffusion [Mas99b]. Digest [FHBH97, GTG94, Kal91, Riv92a, Riv92b, Riv90a, Riv91b]. Digit [TK99]. Digit-Recurrence [TK99]. Digital [Ame95, Ame96a, ANS98b, Ack98, ALO98, AW94, AR97, Int91a, NIS94, Ano96f, Ano97b-50, ASW98, Aur96, BG90, BM99a, BM99b, BuM94, Ber97b, BM94a, BM96a, BM96b, BM96c, BS95b, BS98, BTH96, Boy97, Bra93a, B99, BWF99, Car95, CR91, CPO98, CHO98, DDM98, DDM96, Ell99, EGM90, EGM96, FFW99, Fox8, FKMY98, FLS98, Fri93, Fro97, FOM91, Gar97c, Gar98b, GR97, GDD97, GB98, GO96b, GQQ91, HKS95, HG96, HG97c, HEG98, HA96, HW97, IE97e, IEE98d, JLO97, Je99, KKS97, Kob97, Kob98c, Kra93, KH98a, LQ989, LM95, LW96, LL98a, Lut98, LR98, M596, M98b, Mer99b, Mer97, MT97, Mos98, MBW97, Nat91, Nat94a, NH98, NMV98, NIS93a, OOA93, Oht96, OFF93, Oko96, Per97, Pet98, Pf96c, PW93b]. Digital [PGV93c, RDK98, dr94b, Rot95b, SC96a, SCxx, Sch93c, Sch93e, Sch94d, SK97b, SK97a, She97, She92e, Sim93, SB93, SY98, SHG98, VP98, VNP98, VP99, Web98, WD96, WD97, WL99, Wored90, YK98, Yeu99, Yeu97, Yeu98, YYH98, ZK96, ZKYOY99, Zhe97b, vHH97, vTO94, AW95, An91b, An98e, BBCP98a, BHS93, BR96c, BGR98b, BCV97, BO96a, Bis90, BOD95, BS97b, BM91b, Bur98a, Com97, Car97a, CHL98, DD95, DDM98, DSS99, FC94, FB97, Gua90, HS91, HZ93, HW98b, Hwa93, Ibb97,
Dividing [MB99a]. divisibility [FR94].
Divisible [EO95b, EO95a]. Division [Han94, DF92, FBT96, HP94]. divisor [FR94].
Do [AW99, Ber97a, DDJ98e, DDJ98f, HKS95, SS99a, Ber98, Ude98, Way95, ZKOY99].
Dobb [Eri97a, Eri97b, SSM+97, SSv+98, SMD+99]. Document [BLMO94, BLMO95, BO96b, Hei96b, LMOB95, ML98, Max94, Sea95, Bur98a, HS91, LL98b, van97b].
documentation [Sim95]. Documents [Rot95b, SB97, Ban94, DSS99, Rot95a, Sch93e, SHG98].
Doddson [Lip98]. Does [MGL+98, Mar96, Ril96]. Dollars [Ame96b].
Domain [ADBB99, DVR92, Gar97a, Gar98b, Mon93, PDP99b, Ano97-29, BBCP98b, BP98d, HG97e, KMP99, KM98c, NP98b, TKS98].
Domains [Bru98, CM97a, CK90, Mar97].
Donald [CFK+91]. Don’t [Hus99, Way96b, Chi99a, Chi99b]. door [Yu92].
Doorbells [Law98]. Double [Ano92c, Cha90, HP99a, Pa99b, Bar95, KL95b]. Double-Agent [Cha90].
Doubly-Iterated [ABDV98]. Down [GC97, Fox98]. downgrader [McH92].
Downgrading [KM92]. Downloaded [JPL99]. Downloading [Sch97d]. dpe [lPNdbbbrpm91].
Dr. [Eri97a, Eri97b, Gar97d, Riv93a, Riv95a, SSM+97, SSv+98, SMD+99]. Draft [Ano94b, Ano96-28, Ano97b, Got99, Mic93b, Am95, Ano96c, Ano95u].
Driscoll [Luj98a, Luj98b]. Drive [GC97]. Driven [CHLT99, Ano97-27].
Drives [DDJ98a, DIF94]. Dromquinna [IIE96c]. DS [TY94]. DS/CDMA [TY94].
DS5002FP [Kuh98]. DSA [AA95, Acc97, Len96a, Miy96, Sim93, Sim94d]. DSP [IIE97c]. DSP56000 [DK91]. DSPWS [LW96].
DSS [Nat91, BGM97a, BGM97b, GJKR96a, Koc95, Koc96b, Nat94e]. DTR [Ano93k].
DTR-1 [Ano93k]. DTS [BHHR95]. Dual [Jas96, LL99, FBT96]. Dual-workfactor [Jas96].
dumps [Me98]. during [Don98, Joh95, Rat96, Wil98a]. Dutch [vL96]. DVD [GC97, LT98]. DVD-Video [LT98].
Dwork [GGH97a, NS98d, NS98e]. DYANA [BK99]. dyes [SBTV99].
Dynamic [AGY95a, AGY95b, Ano97-33, BDHK93, Dae98, DP99, DSS95, FT99a, FY99, FR95d, Gu97, NT99, SG99b, SP99, WH95, BH93, BCD94, Bl95, BCD96, CT99b, HC96, Pos98, SS94].
Dynamic-Resharing [AGY95b]. Dynamical [PS96b, RO96]. dynamics [Oh99].
E-Cash [DFTY97, Yac99a, Yac99b].
E-commerce [Ano98h, VM96, DDJ98d, Jak99b, Let98, Gar97b].
E-Mail [Ano93j, Ano95c, LF97, Ril96, Bac95, Sta94a, Got99, RS98b, Sch95c, Sch95d, SH97, Gar97b, Str93a, Str93b]. e-safe [BC97].
E.I.S.S. [BFS92a, BFS92b]. E.I.S.S. [Dan95]. E.I.S.S.-Report [Dan95].
E2 [KMA+98, Kob99, MT99a]. EAP [BV98].
early [Alv98c, Mar96]. Earth [Fox98, YHIK99]. Earthcam.com [Ano98t].
Ease [HJL99]. eased [Ano96p]. Easier [GMD98, BRR99, Sch98c, Way95]. East [Str95]. Easy [Ano97p, Sim94d, Ken95].
EccoFan [PKA+98]. ECCp
[BT97]. **ECCp-97** [BT97]. **Echo** [GLB96].

ecciphering [Blu97]. **ECMA-219** [ECM96].

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

**Economy** [CFGS99, Org98a, Tas98]. **ECP** [Mey96a].

Ed [DDJ98e, DDJ98f, MGL98].

**Edgar** [Sha99a, Ros97c].

**EDI** [Len93].

**EDIFACT** [RCM99].

**Edinburgh** [IEE95a].

**Editors** [Hat96, Joh99, Bur98b, Ano95h, Ano95i, Ano96k, Ano96l, Ano97q, Ano97r, Ano97s, Ano98j, 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].

**Effects** [CGB93, CI96].

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

**Efficient** [AGS97, AGY95b, BBDW96, BDV93, BF97b, BF96e, AKP96, BN99].

**Efficiently** [Jas96, Bak92].

**Efforts** [Ano96-28, Neu91].

**Eigenvalue** [All98].

**Eighth** [ACM97b, IEE92b, ACM96b, USE99a].

**Einstein** [SvA93, CI96].

**election** [CGS97].

**Elections** [CFYS96, Ie91, BT94, FOO93].

**Electrochemical** [DDJ99].

**Electronic** [Ano96m, Avo98, Bar93a, Bar93b, BFP99, Bra95b, BLMO94, Cha92b, DDJ98c, DB99, DT98a, EO95b, EN98, ENK99, HS97, Hir93, J97a, LHB96, Lin93a, LvD98, LKD98, LR98, Max94, MZ98, O090, Ped95, PW97e, Riv97a, STS97a, STS99b, SB97, Sch99i, Sin98, TRS97, Tra99, USE95c, USE96d, USE96b, USE98b, V98, Ame95, Ame96a, AMS96, Ano98d, AC97, BH98, Com97, Cha92a, DMW94, DSSZ99, DF98, EO95a, FB97, Ken95, LM98a, Lin88a, Lin89a, Man95, Mit92a, RP97b, Sch93e, Sch95d, She96a, VNM99, Way93b].

**Electrically** [Ped99, Ano98m].

**Electronics** [IEE97g, IEE98c].

**Elegance** [Sch99c].

**Elektronicznej** [Sch95e].

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

**Elements** [FC99].

**Eleventh** [CH96, IEE92d].

**ElGamal** [AA99, Ble96, KS96, LK96, NK98a, TY98b, TY98a, V97, Zhou94].

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

**Eliminating** [GGH97a].

**Elimination** [BLM99].

**Elizbeth** [Unit92].

**Elliptic** [AMV90, Ano95u, BS91b, BSS99, CT99, De98d, DP98c, DMPW98, Dem94, Eng99, ESST99, Fer99b, HSSI99, Hes97, Q97, JM97, Kal97a, Kal98g, KMKH99, Kob98c, KMOV91, KT93, Len99a, LD99, MS93, Men93, Men95a, MM96b, Miy93a, Miy93b, Miy96, Miy99, OFF93, KY7, SOOS95, SW93, SSNP99, V97, W99, AMV93, AS98, BGR94, BC90, BS91a, CNST98, CPPK96, FMR99, Gal99, GK99b, GP97, HN98, IS99, I98, JQ97, JQ98b, Q98b, KS96, Kob91b, KK98, KOT95a, KOT95b, LL996, Ler97, Mal91b, MV90, MV92, SX99, W99, XL98, Z98].

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

**Elusive** [Len96b].

**EMACS** [McH92].

**Embed** [Ano97z, MT94, Ano97-47, Zha96].

**Embedded** [BKS99, Bar99, DDJ98a, LT98, Lin98, BBP98a, BP97b, CC95, KP99b].

**Embedding** [ACD94, NS97d, GO95, Gold96b, HK99b, ZK95, Sch91a].

**embodiments** [CT99b].

**Embraces** [Ts97].

**EMEF** [Org98a].

**Emergent** [Jun99].

**Emerging** [Kal99, Org98a].

**Empirical**
[WW98b]. Employing [BWM98]. emulator
[Obe99]. EMV [Gui97]. enable [Sch93e].
enabled [Cha99b]. Enabling [DS97b].
Encapsulating [Atk95b, KA98b].
enciphered [Lea90, Per91]. enciphering
[Beu94]. Encipherment
[HS90, OA94, Lin88a, Lin89a]. encoded
[DS97b, HG97d, QN98b]. Encoding
[Th98, HG97d]. encodings [CGV94].
Encrypt [Ano99g, BR95a, Ber98, JSY99,
Ril96, WT99, Ano96e, Ano97-36, Rot97].
Encrypted
[AW99, Bla98, GMCF95, GLZ99, Gli98,
Jas96, Szw97a, YY91, Ano98o, BTD98,
Bre97b, DF97, STW95, Kip97]. Encrypting
[Ano97-33, Bla94b, Lom94, Luc98b, LW99,
SS99e, Beu94, KAK96, LL98b]. Encryption
[ASW99, AAB^97, Ada97b, Ada98,
ARRW99, And98, ABK98a, Nat93b, Ano94c,
Ano94d, Ano96c, Ano96m, Ano96q, Ano96o,
Ano96n, Ano96p, Ano96-29, Ano97h, Ano97t,
Ano97u, Ano97v, Ano97-39, Ano97-42, Ano98k,
Ano99f, Bac95, Bal97, Ban93, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b,
BDRP98, BS99b, BS99c, BRW99, BS93b,
Bir95, BB95c, Bla96a, Bla96b, BFN98b,
Ble98a, BC95c, BFS96, BY92, Buc95a,
Com94a, Com94b, CDNO97, CM999,
COP^+95a, CH98, CMKK98, CT99a, Cop94a,
Cou93, DDJ98c, DDJ98d, DDJ98g,
DDJ98h, DC98b, DK96, Den90, Den95, DB96,
Des99b, DS97c, Ele98, FIP94, FN94, For99b,
FY95b, FY97, FH94, FQ99a, FQ99b, GSY99,
Gai90, Gar97a, Gar97b, Gar97e, GC97,
Gar98a, Gar98b, Gen98a, Gen99a, Gen99b,
GK98, Got99, HG97a, HG97b, Hat96]. Encryption
[HK98, HK99d, Hub98, Joh90, JM96b,
Kal93a, KY95a, KR96a, Kal98b,
KY98, Kap98, Kas96, Koh90, KKL99, KM97,
Kum98, KRBS97, KH98b, KYDB98, Kwa93,
Kwa97, RSA93f, Law98, Lea99, LT91, LW91,
LM91b, Lin93a, LS98b, Luc97, Luc98c,
Luc98c, LW99, MGL^+98, Mad97, Mad98c,
Mad98d, Mat94a, Mat97, Mer91, Mey96a,
Mii95, Moc97, Mue99, Mii99, Nat93a,
Nat94b, Nat94d, Nat97b, Nat98, Nat99a,
Nat99c, Natxx, NBD^+99, NH90, Oh99,
Oka94, Orl96, Par96, Par98a, Par98c, Per91,
PRZ99, Pin97, RSA93a, RSA94, RP94,
Riv95c, Riv95b, Riv97c, Riv98c, Riv98d,
Riv98a, RD99a, RD99b, RC94a, RC94b,
Ros94, SvA^+98, SKNO98a, SKNO98b,
Sch99a, Sch99b, Sch99d, Sch94c, Sch95a,
Sch95b, SW97a, SW97b, SKW^+98e, Sch98g,
SKW^+99d, SHK^+99a, SKW^+99e, SE96,
See97, She95b, She92g, SB98, Sim95]. Encryption
[SM96, SM98b, SB92, Smi93b, Smi97a, SB99,
STA97c, SW99b, Sto90, Sz97b, THP^+98,
Un97a, Un98a, Un98c, Un98b, Un98d,
Un98e, Un99c, UU97a, Un97b, Un98f,
Un98h, Un98g, Un97c, Un98j, Un98i,
VB96, VKR98, WSK97a, WSK97b, War98,
Way93b, Way93c, WSFC99, We91a, We91b,
Whe94, Wir98, Wir99, Yin97, YY97c, Yur97,
Zhe97b, Zie97, Zol93, Aus96, Abr97, Ala93a,
All97, And94a, Ano90, Ano92b, Ano94f,
Ano95c, Ano95k, Ano95n, Ano95q, Ano95t,
Ano95v, Ano95w, Ano96d, Ano96g, Ano96m,
Ano96t, Ano96u, Ano96w, Ano96-30,
Ano96-31, Ano97i, Ano97j, Ano97m, Ano97n,
Ano97y, Ano97u, Ano97-31, Ano97-30,
Ano97-35, Ano97-38, Ano97-41, Ano97-46,
Ano97-49, Ano97-51, Ano98a, Ano98v,
Ano98u, Ano98m, Ano99a, Ata94, AM99,
Ban94, BTD98, Bax97, Bea96]. encryption
[Bee96, Bee97, BR94b, BR95a, BDJR97,
BR97b, BB90, Bet95c, Bih97c, BFN98a,
BC96a, BMS96, BFS98, Bow93, Bre97a,
Bro96, Bus96, Com97, CCM99, Cha94b,
CLW98, Cle96, Cli97, Cli99, CM96, Cra96,
DH96a, DOR99, Dia91, DL98, Ele99, Ell97,
Eng95, FC94, FB97, Gii97, Gol99b, Gol96d,
GBL94, Goo96, GKS97, Har90, HK90, Hat97,
Hel93, Hel98b, HT95, HP94, HY95, HC96b,
HCC98, Int91b, Jac90a, Jac90b, Jak99c,
JT96, JT97b, KY95b, KY97, KYYx, Ken95,
Kir95, Knu99c, Kop97, Kuc92, Kuh98, Kuo90,
LM91a, Lam99, Lee95, LC97a, Los98, Mad96, Mad98e, MRS99, Mar95b, Mey96b, MM95, MM97, Mol98, Mra95, Nat93c, Nfr95c, Oel97, Pos92, Pos93, Pre95a, QN98a, Ree97, Rev91, Rlv95d, Rkd94, Rot95a, Sah94, Sav96, Sch98b, Sch94i, Sch98c, Sch99j.

encryption
[She96a, Sme97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, Szw97c, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts'90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vdd95, Vau98e, Ven90, Vu95, Wad98, Weh97, Weh98, Weh99, Wel95, WN95, Wh93, Wll93a, Wll93b, Woo90, Yeu99, You97, Zaj97, Zan90, Zer96a, vOW91, vT93, An98t, An93j, Hon98].

encryption/authentication
[She96a, Sme97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, Szw97c, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts'90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vdd95, Vau98e, Ven90, Vu95, Wad98, Weh97, Weh98, Weh99, Wel95, WN95, Wh93, Wll93a, Wll93b, Woo90, Yeu99, You97, Zaj97, Zan90, Zer96a, vOW91, vT93, An98t, An93j, Hon98].

encryption/decryption
[Hat97, Vu95].

Encryption/MAC
[Yuv97].

encryption/multisignature
[HCC98].

Encryptions
[Mv93].

encryptor
[Ano97m, Ano98m, Ano99d].

Encryptors
[Ano99h].

Encyclopedia
[CFK+91, New97, UFC94].

End
[Bra94a, DDJ98c, Gar98a, NH90, Ano97y, WSFC99].

End-to-End
[NH90].

endlicher
[Wal98].

ends
[McC90b].

Endured
[Che92].

Energy
[DFL99].

Enforce
[BDS98].

Enforcement
[Cae96b, Cl99].

enforcers
[Way93c].

Enforcing
[Ano97w].

Engine
[BE90, CM98, She92d, Ano95n].

Engineering
[Ano98n, DFGH99, DB99, EKLM99, IEE96d, LBHM99, SSSW98, Sm98a, An94, An96, GEL98, IEE97k].

Engines
[T+99, Way93a].

England
[ES98, Cur98].

Enhance
[FO99a].

Enhanced
[Ano95c, AR98, Ken93, LZ96, Zan90, Zeg93].

Enhancement
[HWJ98, Lin93a, Lin88a, Lin89a].

Enhancements
[IM96e].

enhancing
[HY95].

Enigma
[CWM+91, Har96b, Kip97, Kip99b, Obe99, Ano91c, Blo98a, Blo98b, Blo98c, Cra92, Kah91a, Kah98a, Kip97, Kru98, Mil96b, Mus92, Sal93, Tur99, Wel97].

Enigmas
[Gad91].

Enjoyable
[CM99d].

Enough
[CFK+91, Dae98b].

Enschede
[Hei96a].

Ensuring
[Com97, Rot95a, ZG96, Way91].

Enter
[Wor96].

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

enterprise-wide
[Wad93].

enters
[Joh98].

Entities
[KM99c].

Entity
[BR94a, BWM98].

Entrepreneur
[Pin98].

Entropy
[Bro94, EHMS99, KSHW97, KSHW98].

Entrust
[Ano991].

entwerfen
[Hor99].

envelope
[SOB98].

Environment

Environmental
[RS98c, RS98d].

Environments
[GSTY96, SKAM99, DNS98].

EPIC
[Rot95a].

EPS
[An96r].

equally
[Ito91].

Equation
[Cop95c, LG97].

Equations
[Por98, RZ99, BMP97a, Cus95, GK95b, LCL95, Lon92, Sun91a].

Equilibrria
[Ett98].

equipment
[Int91b].

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

Era
[DDJ98c].

Ergonomic
[DDJ98c].

Erika
[Mat99].

Errata
[Con99a].

Erratum
[Ano91a].

Error
[AW94, AR98, BGS96, Cha99c, DLR97, KKS97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, DLP93, JV98b, Ste95, Wan92a, YL97a, vT94, CW94].

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

Error-Correction
[MG91].

Errors
[GGH97a, SHK99b].

ESA
[Sp95, YS91].

ESA/390
[YS91].

ESAT
[PGV93d].
Escrow [AAB+97, Bla96c, BDS98, Cae96a, CMG97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, LWHY95, Mad97, Mah96, Mar97, MS95f, MRS99, Nec96, SYMI98, Sam98, SM95a, VvT97, VBD99, YY99b, Ano94f, BDHJ97, BR96b, DH96a, Des95, Fre94, KL94, Mao97, Uni95a].

Escrowed [Bas95, Com94b, FIP94, Nat94d].

ESIGN [FOM91].

ESORICS [DEQ92, Q+98].

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

Espoo [Nyb98].

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

Essentially [BR91]. Establishing [Des96a].

Estimate [Miy93c, UU97a].

estimates [DLP93]. estimating [AI 96].

Estimation [VNW95, Jv98b].

Estimation of [Bec99].

Etruscan [Nis91].

Euclid [LZ91a].


Eulerian [RB99].

Eurocast [MDP94].

EUROCRYPT [Bih91, Dam90a, Dam91a, Dav91, De 95, Fum97, Gq95, Hel94, Man96b, MZ98, Nyb98, Pic98, QV90, QC95, Rue93, Ste99b, Ano98i, Bet98, BC98, CP98, Dam98, Dav98b, De 98b, Fum98a, Gue98a, GQ98, Hel98c, Ing98, Man98, Pat95, Qv98, Rue98].

Eurographics [Kui91, PH91].

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

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

Eusipco [T+98].

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

Evaluating [Pa99a].

Evaluating [AG97, Ano97b, BG99, BP95b, Cj98a, Cj98b, Hw98, KBS97, PD99].

Evaluative [MI99].

Even [BCE+94, Bosxx, Ano95q].

Evening [Che92].

Event [Ruo94, SK97b, SK97a].

Event-Stream [SK97b, SK97a].

Evaluated [Bas95, Com94b, FIP94].

Evidence [DR99b].

Evolution [Cas95, Jm96b, Knt94, Nm96b, PGV93d, Sin99, Wri99].

Evolutionary [Ger99a, GM99a, Hes97].

Evolve [GB98].

EW [IS97].

exact [BR96c, GEL98, Luc95, ZW99].

examination [Joh90]. examines [vdWS97, vs97].

Examining [RC95].

example [Kay95, Nee94].

Excellence [Eri97a].

Exchange [ASW98, ASZ96, BC90, BM94b, Dan94, Dim95, FH91, HHY93, Jas96, Luc98b, Msn98, RSA99a, Ssn98a, Soos95, Van93, Ano96q, BSNP96a, BSNP96b, BTD98, BCK98, BM95, Dan94a, LL95b, MS98a, SK97b, STW95].

changes [Dv92].

Executable [JPL99].

Executing [AW99].

Executive [Zer96a].

Exhausting [CR97].

Exhaustive [CR97, QD91, KR96b].

Existence [FDB93a, HT98, RV99, FDB93b].

Existentially [DN94].

Existing [SS99d, BB95a, NM96b]. expands [Ano99d].

Expansion [BO96b, Tak97].

Experience [ADB99, Gla99a, Ros96b, SVB99, Moy98, CWM+91].

Experiences [FC99, Lun90, GH96, MM95].

Experiment [AB97, DL95]. Experimental [BBB+91, Mat94a, SBB99].

Experimenting [DB99, MWB99].

Expert [BBDF97, Chi92, Stu99, ACC99].

Expiration [BD98].

Explained [Bmc95, Hat96, Lut98, Los98].

explanation [Gre90].

Explicit [LF99, MD98].

exploit [Luc95].

Exploiting [BS91h].

Exploration [KV99, Kip99a].

Explorer [Lea99].

Exploring [JJ98b, JH98a].

explosive [DL95].

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

Exponential [Dan95, CFS97, CDG95].

Exponentiation [BP99b, BK95d, Com90, HCY96a, LL94b, Pa99b, Ar93, BGR98b, CL97a, KAK96,
Rev91, Smi94b, Von92a, Von92b, YL93, dR95. Exponents [Wie90b, vOW96, Gro94, VW96, Vv97, Wie90a]. Export [Ame96b, DDJ98e, DDJ98f, Gar97b, GC97, Han95, Han99, Uni97d, Abr97, Ano97-51, Ano99m, Ban94, Cli97, Gen99a, Han97, Mad99a, Mad99b, Rec97, UU97b, UU97b]. Exportability [Wei91a, Wei91b]. Exportable [Eng95, Ano95v]. Exports [Bar96a, Buc95a, Sta97c]. Exposed [MSK99a]. Exposing [Sil99]. Expressive [MTES99]. Extend [Ts'97]. Extended [ASW98, BFN98b, BV98c, BD90, BS91g, BD91, CvHP91, CK90, DDP90, DY91d, DDP99, DD99, DY91f, DF91a, Dob95a, EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, hVH93, Bea97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, Ole95, Pa96]. Extended-Certificate [RSA93c]. Extending [Bad99, Has94, MI99]. Extensible [BV98b, WBD97]. Extension [BP98a, CTT94, FHBH+97, MS90b, LMJW93, STW95]. Extensions [CD91, DT98a, Law98, NW97, Atk93, GH99, GSK95a, JD91]. Extensive [Ano97-44, Sim95]. Externalization [OA99]. Extracting [Nis96]. Extraction [SD99]. Extraordinary [Jam98]. extremely eyewitnesses [Ano97-37].

FA [Bao94]. Fabrication [DDJ99]. Face [DDJ98d, DMFB97]. Faces [GB98]. Fachtagung [BGH95b]. Facial [LMP99, HE98]. facilitation [Cil99]. Facility [AKF94, Bi90, She96a, YS91, JMLW94, SY92]. facing [KG96]. facto [Pir94]. factor [KM98b, SVWMB95, VSB95]. Factored [Ane96b]. Factoring [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pa99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, McK99, Mei96b, Riv95a]. Factoring-Based [Kal98e]. Factorisation [DH95a, Jon90, DH95b]. Factorization [Ale92, DDLM94, MM99a, MM98b, Od95, vO91a, Sho97, vO91b, LLMP93, Mao98, Wh93, vO92]. Factorizations [BMS94, NS97b, NS97c]. Facts [Ano91b]. Faded [Alv98a]. fading [Ted97]. Fail [BP97a, PP97, SSNP99, vHPP93, An94b, Pf96c]. Fail-Stop [BP97a, PP97, SSNP99, vHPP93, Pf96c]. Failed [BCE+94]. fails [DH96b]. Failsafe [KL94]. Failure [Ano95a, Ber97c, Gar98a, TYD99, FR95b]. Failures [CH98, JQ97, Moo92, Sim94b]. Fair [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, MS99, SS99c, SS99f, Tra97]. Fax [AM93a, AM94a]. Fairly [HD96a]. fall [Od90, Rob98b]. False [LD98, She92b]. Families [Kal98e, Per99]. Family [KT98, Mad98e, Miy91, RP97a, ABC+98, BGH+95a, FSS94, Ito91, Kob90, SRR98]. FAPK3 [DYL98]. FAPK3 [TCC97, TC97]. FAPK4 [TC99a]. Far [Str95]. Fast [AG97, AMV90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bih97b, Bih97c, BHH+99, BD94, BK95d, BGV96, CS91, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBV96, DNR97, EPR99b, EPR99a, Gar97b, Gol96a, HHT98b, HP94, HHC96a, JJA99, JJA9b, KR94a, KTM+99, KP99a, KP79, KR99a, Kmt99c, CKMK99, KA91, Koy95, LM95, Mau90, Mer91, Mih94, MM95, SS99a, NKP99, PSR97, Pre95a, Rog95, SW97a, SW97b, SOOS95, SV93, SB98, Sho96, Sil97b, Tak97, Tak98a, Tak98b, T+99, Van98d, Van98e, AMV93, AB96b, Ano98t, CGV94, DRR97b, DV96e, GGH+98, HHT98a, Jenxx, LRW93, LC98, MZI98, PVO95, RRSY98, She92c, SN94, SH99, SAM97, SGSD99, YL93, Gol96d, OA94]. Faster [Luc96a, Luc96b, WZ99, YYY99b, Bosxx, Mih96, Sch98c]. Father
Functional [Yam99]. Functions [AHV98, Ano95a, BDPSNG97, BCK96d, BCK96e, BHSV98a, BGK99, BGS94, BGS96, BM94a, BL95, BHT98, CDD99, Car93, DGV93, DY91d, DY91b, DFL99, ECM96, EPR99b, EPR99a, FBS98, GJKR96b, JQ97, KTM+99, Kim93, KP96a, Kra95, KS97b, LM93a, LM93b, LM95, MS99b, MS90a, Mer90a, Mer91, MS95f, Mi96a, Mon96b, NR98, OS98, PW93b, PGV92, Pre93a, PGV93a, PGV93c, Pre97a, Pre99, Pre94b, QC90, Roe94, Sch91b, SZZ95c, SRY99, ZZ95, Zhe90, vW94, BSP96a, BSD99, BSR95, BCK96b, BCK96c, BHHR99, BK98f, CCZ98, CDG95, Cus96, CS96c, Dan90b, Gol96a, Gre95, GHS93, HK97, HLMW93, HXMW94, HLYT99, IS907, JG95, KL95b, Lai95, MCD98b, O'C99, PGV91, PGV93b, Pre94a, PGV94, Po95b, Roe95, Rom90b, SZZ94a, SZZ95b, Sim98c, Tsu92b].

functions [Tsu92a, Wer93a, Wer93b, YT96, ZZI97].

Fundamental [Ano96-37].

Funds [GBC93].

Funktioniert [MPS94].

Further [Pre95b, WKS+99, WD97, Mad99a].

Fusing [DMFB97].

fusion [KH97].

Future [Fuc99, HP98b, Od95, PT95, PM99b, Sch97a, And98, BFS92a, BFS92b, For99b, Mar96, NIS92, SB92].

Future-Adaptable [PM99b].

Fuzzy [Blo99, CBM90, FCH99, KKW99, Tro93, ZHJ98, CS99].

Fuzzy-Control [KKW99].
Germany [BFS92a, BFS92b, Fum97, IEE97d, LM98a, Wat91, Rat96].

Geschichten [CWM+91]. Get
[Ano96z, Cae96b, DDJ99a, Sch98c, Ude98].

Getting [WG97]. Gets [Gar98b, GO96c, Los97, A899vi, Gen99c, Sch98c, Weh97].

Getting [Kwa93, Way95]. [PSR97, DBVD96, LD99]. GI
[BGH95b, LM98a]. GI-Fachtagung [BGH95b].
Gibbs [DP99]. Gilles [Buc91b].
Girault [SSN98b]. Girl [Got99]. Girls
[Res99]. Give [GB98].

Given [BM92, BDF98, EvH91, Ev92]. gives
[Ano93k]. Giving
[Int91a, GQW+91, JLM+94]. Global
[JV98b, Or196, SS99b, TG999, TA92, TL99, Z995, Par96].
GMD [SBGK99]. Go
[DDJ98d]. Goal [AMP94]. Goals
[BP98e].

Goats [SV95b]. Going
[DDJ98d, Ano95q].

Gold
[PSR97, CBVD96, LD99].
Goldreich
[SSN98b].

Goldreich-Goldwasser-Halevi
[NGu99a, Ng99b].

Goldreich-Goldwasser-Halevi
[NGu99a, Ng99b].

Goldwasser
[NGu99a, Ng99b].

Goldwasser
[NGu99a, Ng99b].

Good
[Ano94i, AWV99, Elk96, Gar95, Gar98c, Ros97a, SS979, Sta94a, Sta95a, Kob91a, Ler97, Mei96a, SX90, Zim96a, Zim96b, Pin98].

Goppa
[GH91].

GOST
[KSW96, Sch95b].

Goucher
[Mus92].

Government
[RK949, SG99a, Ano94i, Bee96, Riv98c, Way93b, Wel99, A998u, Lee99a, Re997, Ros99].

Governments
[An996, BH98].

Grace
[GC97].

Gradient
[Jan99].

Graid
[Sai99].

Gran
[IPnddbpr99].

Grand
[FB99].

Graph
[BM998, BSV93, B998, BALS99, EMNN98, M99, LS98a, PD99a].

Graphic
[CON09, GO96c, IPnddbpr99].

Graphs
[Kui91, SHG98, Wor96].

Graphs
[BMM94a, HE98, LE99, WD99b, K992].

Gray
[Rus93a].

Greatest
[Mad92].

Greece
[IEE97c, KG96, Kat97, Pit95, Spi95, T+998].

Greg
[Ers99].

Grid
[LE99].

Gridless
[BVFD99].

Griгорochuk
[GZ91].

Gröbner
[BCE+94].

Grosch
[CWM+91].

Group
[Law98, A997u].

Group
[AT99, CS97a, CM99a, CW93, DDJ99, DKK998, Got99, GN95b, HY99a, LR98, NS97b, NMV99, Pet98, Rei92, SG99a, Sav97, Tra99, Wu92, Y98b, Y999, Ano97i, CP95, DF93, Fra90, FR94, Hwa91, Hwa92d, LWC96, NS97c, WHL99, Wer93a, Wer93b, Y98a, Dra99].

Group-Oriented
[SG99a, HY99a, LWC96].

Groups
[BMS94, CS97a, CH98, GPSN98, Got99, Mei96b, Pat99, SP99, CMPS97, Dam96, GZ91, GPCN96, HSW94, HCC98].

Grow
[DDJ98d].

Grown
[Gar97c].

Grows
[Lea99, Fra92].

Growth
[GC97, Ano979k].

GSM
[ATA99, MB99a, PW98, She94b, Ved98a].

GSS
[Lin96b, MCM6].

GSS-API
[Lin96b, MCM6].

Guaranteed
[Mos989].

Guarding
[GS98, Mar95a].

Guess
[BKK98].

Guessing
[KS97c].

Guest
[AKP96, BNP99].

Guide
[Bac95, End97, WSFC99, Zim95a, Bis90, Jac90a, Jac90b, Nic99, Pre97b, Sta95b].

Guided
[Mos99].

Guideline
[Lee99a].

Guidelines
[Bar97, CPOR97, Mer97, Ane95, Ane96a, Org98b].

GUMP
[FS97].

Guru
[Di 97a].

Gyi
[IPnddbpr99].

H
[Scu92, Ano95n, Lea99].

H-1B
[Lea99].

H-P
[Ano95n].

H.
[WG97].

H.R
[Uni97b, Uni98c, Uni96c].

H.R.
[Uni97a, Uni98b, Uni98e, UU97a, Uni98f].

Hacker
[Mei98].

Hackers
[GC97, HM91, HM92, HM95, Mei98].

Hacking
[MSK99a].

Hades
[Bie98].

Hagelin
[Hag98].

Haifa
[Bih97c].

Halevi
[NGu99a, Ng99b].

Halkidiki
[Pit95].

Halske
[Dav98c, Sel98b].

Hamburg
[LM98a].

Hamming
[She95c].

Hampshire
[IEE92a].

Hand
[BF99a].

Hand-Held
[BF99a].

Handbook
[Bac95, MCV97, Sha99a, Ata99].

H. [FG99a].

hands
[Ano94c, Riv98c].

Handshake
[Sim96b]. Harari [Ver95]. Harbor [Kah98b, Par98b]. Hard [MGL'98, Mar99, SS99a, BFKL94, Jon90]. Harder [Sch97b]. Hardness [BV96, NS99b, DI99, Kha93]. hardness-amplification [DI99]. Hardware [ACD94, Ano96a, Bir98, BP99b, Bri90b, BS91h, Ch98a, DGV92, GN95c, Koç96a, OS91, Wil93a, Wot99, YK98, BS95a, DN95b, Gai90, KP99b, L997, M798, Nor95a, Nor95b, Nor95c, NO96, See97, SN94, TY92, Way95, Zhe95b, Kui91]. Harmonic [RG99]. Hash [ANS97, AHV98, Ano93f, Ano95a, Ano95l, BDPS97, BCK96d, BCK96e, BS91e, BS91d, BDP97, BHT98, CP91, DBGV93, DG93, Da95, DY90, DY91d, DY91b, EPR99b, EPR99a, FIP93b, GHR99, SS94a, ISO97, KP96a, Kra95, LM93a, LM93b, LM95, Mer90a, Nat92b, N993b, Nat95, PR99, PW93b, PGV92, Pre93a, PGV93a, PGV93b, PGV93c, PGV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sc93f, SV94, SYR99, Sta94b, Vau93, Zhe90, vW94, AB96b, BSNP96a, BSNP96b, BD92, Dam90b, DK94, Gon95, HLMW93, HXMW94, HYLT99, JG95, KL95b, MZ98, PGV91, Pre94a, Pr95, RP95b, Roe95, SV95a, SRR98, Sim98c, T92, Tsu92a, YL97c, DBGV93, Sch93g, EPR99b]. Hash-and-Sign [GHR99]. Hash-Based [PRZ99]. Hash-Functions [QG90, ISO97]. Hash-Values [SS94a]. Hashing [AS96, BGG94, DC98b, FNS92, KP97, Kra94b, KBC97, PS93b, Rog95, Rus93b, Sch91c, Sch93f, Sho96, Shi91b, TZ94, BG96, Bosxx, Gib90, JBM90, Sa94, Sch93g, Sta99b, ZPS93]. Hasn’t [Gar97a]. Hasty [Sch98i]. HAVAL [ZPS93]. Hawaii [???90]. Head [Ano94i]. Header [At95a, KA98a, MR95b, Ros93]. Heads [GC97, St98]. Health [GO96c, Mj93]. Hearing [Un98a, Un98g, Un98j, Un98i, Un97a, Un98d, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k]. Heat [GC97]. heating [M98a]. Heats [Gar98b]. heaven [Gol97a]. heavily [An97-35]. Heimdall [DW98]. Held [Ano96-28, B99a, Uni98f]. Hellas [IEE97c]. Hellman [RSA93b, Ano97n, BY93c, BY93b, BBR99, BWM99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY98b, HY98a, Koç95, Koç96b, Mau94, MW96c, MW96b, MW99, NS97c, NS97b, Van95a, VW96, WM93, vW96]. Help [GR99, PKA+98, AK95]. Help-Desk [GR99]. Henry [CFK+91]. Her [Ber96a]. Herd [Rit99]. Here [MK94]. Heterogeneous [DV91]. Heuristic [MCD98b, C99]. Heuristics [SBG99, CD98a]. HF [RP94]. HFE [KS99b]. HFX [LR96]. HGF [Uni94b]. HGF-94 [Uni94b]. Hidden [BL95, CD97, JP96, KZ95, NS99b, Pat96, Sak96, PSB97, Til98]. Hide [SV99a, SV99b, S98]. Hidell [Sc92]. Hiding [Auc98, GML95, CM97b, CD97, CD94, GR96, GL96, HS96a, MS99b, MO99, P96a, Phi98, RV97, SC96b, SZT96a, And96c, Beu94, Bra90d]. Hierarchically [LE99]. Hierarchical [FL96, OOK91, C87, GP96]. Hierarchies [Ruo94]. Hierarchy [Hwa97, YY99b]. hieroglyphs [W98]. High [ACM98a, ARV99a, ARV99b, Ano99c, Ano99f, BCR98, Bla96a, Bla96b, BMS99, Ch99a, Ch99b, DP98a, DP98b, Ebe93, FVE99, FP99, Gar97a, Gar98b, GN95c, HR90, IEE94e, IEE96d, IM93a, IM93b, Kap98, Koç94, Kor93, KB92, LS97, MPP95, MSH99, Rus90, SKNO98a, SKNO98b, She92d, She95b, Sut99, VN94, An90y, Duf98, Gra94, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Uni96a, Yeu97]. High-Assurance [IE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Ch99a, Ch99b].
high-end [Ano97y]. High-Frequency [MSHP99]. High-level [Rus90].
High-Performance [ACM98a, BMS99, GN95c, IEE94e, Sut99, NO96].
High-quality [Yeu97]. High-Radix [Kor93]. High-Speed [ARV99a, ARV99b, Ano99c, DP98a, DP98b, Ebe93, IMI93b, Ko94, MPPS95, SKNO98a, SKNO98b, MI93a, Nor95a].
Higher [Jak99a, KMKH99, Lea99, MSK98, SMK98a].
Higher-order [Jak99a]. Highly [MS99b, PV97, ARK99].
Holiday [IEE94a]. Hold [Sch93e]. Holder [OMI93].
Holiday [IEE94a]. Holy [Sal99]. Home [Hus99, Ano97o, Hod97]
Homomorphic [FDB93a, Bet95c, FDB93b].
Homo[omorph][omorphism [Dom96].
Homomorphisms [Bur96, SK94].
Homophonic [HYHW98]. Honest [Rab94].
Hood [Sch93e]. Hook [Ros96c]. Hope [BCE+94].
Hopes [GO96c]. hopping [MMMW98, Tod97].
Hor [PNDibbbrm91]. horse [Sch99f]. Host [Kol95, BTG96].
host-centric [BTG96]. Hostile [GTY96, SKAM99, LC95].
Hot [IEE98b, EIE99b, Bra90b, CB96]. Hotel [LW96, Nat98].
HotOS [IEE99b]. HotOS-VII [IEE99b]. House [CUI97, DDJ99, Un97a, Un98c, Un98d, Un98e, Un99c, Un99b, Un99f, UU97b, BHHR99].
HTML-driven [Ano97-27]. HTTP [FHBH+97, Ude98]. Huang [PBGV90].
Huffman [Moh92]. Huge [HE98].
Hungary [Rue93]. hunger [WSFC99]. Hurt [Gar97a]. Hurt [Wel97].
Hwang [Aha97]. Hybrid [DD99, JLM+94, KA99, MD99, NT99, Var99a, BP97b, GMLH94, RO96].
Hyperchaotic [BCCG99]. Hypercubes [DHW95a, DHW95b].
Hyperelliptic [Sma99, BK98g, OS91, OS92, SS98a, SSI98].
Hypermedia [KI99]. HyperText [RS99a].
Hypotheses [ZMI90, Kuk99]. Hypothesis [MSM98].
I/O [Got99]. IBM [Ano96h, Ano96s, Com90, Gar98b, Gen98b, Zun98].
IC [DDJ98g, DDJ98h, JT97a, PC98].
ICALP'99 [vWN99]. ICARUS [Var99b].
ICE [Kwa97, VKR98]. ICICS [HO97].
ICIP [Ano94c, IEE96e]. ICIP-94 [Ano94e].
ICL [CFK+91]. ICSC [Nie99]. ID [CS97c, Hwa92a, Hwa92b, Hwa92c, IS99, JY98, LHW99, MS98a, Mu92, TC91, WSFC99].
ID-based [CS97c, Hwa92a, Hwa92b, Hwa92c, JY98, LHW99, MS98a, Mu92, TC91]. idea [OA99, BBS99b, BKR97, DGV94c, HO96, Haw98b, Haw98a, KSW96, Lip99, Mei94, Sch93d].
Ideal [ABDV98, BC93a, BD90, Bir90a, BP97c, Pa98a, Pa98b]. Idealised [RS99c].
Idealized [MTES99, MM92b]. Ideals [GPT91a, GPT91b].
Ideas [HGHD98, RS99d, TCH+91]. identical [BCCG99]. Identifiable [KOO95b, KOO95a]. Identification [BCCG93, BLMO94, BBD92, Cha94b, GS94a, KM99b, KI96, LMBO95, LML98, NP97, OO98, Oka93b, Sak96, Sch90b].
Ste94a, Ver95, BBC98, BM95, BM91b, DF91b, DF98, HLC99, IS99, Kum97, Mu92, SSN98b, Sch90a. Identities [MS99a, Sar99].
Identity [ALO98, Dan95, DQ94, FKMY98, HJP97, JC90, KP98, Len99a, SSN98a, Gua99, OU98b, Tan90]. Identity-Based [Dan95, DQ94, SSN98a, OU98b, Tan90].
IEEE [Int91a, GQW +91].
IEEE-IMS [IEE94a].
IETF [Ano97c].
If [GPR98].
IFIP [Kat97, LM98a].
IFIP/GI [LM98a].
II [Sch99b, AK99, Ano97-40, Ano98i, Ano99c, BS91f, CFG96, CK95, CW91b, Dav98a, Don98, Eri97b, Mit92b, Mon96, Mus92, Pin98, Rat96, Rey97, RP97b, Ros99, Sch93f, Sch93g, USE90, Van93, Wil98a]. III [Fri92b, Gan93, GN95c, Nor95a, Ree98, Rey99, USE92b]. iKP [HSW96].
illicit [SG96b].
Illinois [USE99c].
IMA [Boy95b, Dar97, Far93, Wal99a]. Image [BKZ98, BNP99, DS96, DP99, Fri93, HPA99, HPG98, HWJ98, IEE95a, IEE97a, IEE96e, IEE97h, IEE97j, KZ95, KM92, LMP99, Mae98, Man98, Pit95, PZ98, PNFK95, Sch99b, SC96a, SCxx, SJJ7, SD97, SZ96b, TOH98, VP99, Wal95, YKY99, BBP98b, BCD98, CCH98, JT96, JT97b, KS98c, KGC93, HK97, NP98b, OP97, OP98, OK96, PPBC97, Sch95b, Se95, SHG98, TKS98, VP96, VP98, Xie98, YM98, CFK +91].
Image-Adaptive [PZ98]. Imagery [WD97].
Images [BLMO95, BO96b, B99, Car95, J98c, KR98, KPR99, LvdLL97, Lv99, LS9V95, MFG95, NNEK97, Per97, SC96b, SZ96a, WD96, ZK95, BP98b, BP98c, BBCP97, BCBP98a, BCV97, BOD95, CKLS96c, HW98b, Ibb97, Irw98, Nas94, Nat97a, ODB96, ÖPH +99, Pit96a, RRP97, RKDB96, TA97, XBA97, ZL97]. Imaginary [HJP97b, HJP98a, ZPY96].
Imagination [Sha99a, Ros97c].
personification [SNT93]. Implementation [An96, Bih97b, Bra96, BS91h, Dae99, DGT96, DRR95, DBVD96, Ebe93, Fei93, Fei96, FOM91, Gla99a, HKQ99, HRV99, IM93b, KP99a, Koc94, Koc96a, Lan97, LCN99, NM99, OSA91, PL94, PP90, Ros96b, SJ98e, She95b, Tou92, Var99a, YKY99, You97, Zim99, BR96b, BC90, CKM99, Dia91, HNM98, IM93a, LS98a, LL98b, Men91, MV90, MZ98, MPL99, Nor95a, Pa96, Per91, SS98a, See97, SAM97, V95, XL98, Koe99].
Implementations [Bas98, Bri90b, G0n98, HK98, HK99d, Koc96b, Mos98, SV93, Wal99c, Web98, WS98, Gai90, KSK96, PA93, Zho94]. Implementing [SAS99b, Van95a, Lee99a]. Implications [Bas93, CMYY98, NS99b, PN92, Van95a, Wei95]. Implicit [Jam98, MILY93]. Implicitly [HRV99]. implies [LHL95b, LHL95a]. Importance [BDL97, Sch99b, CM97d]. important [Sta94a, Woe97]. Impossibility [MP91]. Impossible [BBS99a, Fer99a, BBS98a, OK96a].
Imprimitive [Pat99]. Improve [Fan92]. Improved [An96f, BK98e, Bo90, BS91g, CRRY99, CJL +92, JM99, JJ99b, KM96b, LD99, RP95b, SH97, SAM97, WS98, YL95b, YL95a, ZY99, Cao99, He92, NMVR95a, NMVR95b, SH95a, SH95b]. improvements [BB95b, Bir95]. Improvements [HIJ99, Kne90, IKNY98]. Improving [BHS93, BKPS93, GLV99, SF97, SZ94a, SMK98a, Sun98a, HM97b].
Impulse [She92c]. IMS [IEE94a]. In-memory [Ven90]. in/for [SHG98]. Inaccuracies [OD99]. inadequacy [Kah98b]. Including [DGV93, DW94, JS95b, JS95a, KL95b,
incorporation [Ano95c].

increased [HS96b]. Increasing [AP93, Bao94, BKR98a, BKR98b, Bla94a, KFJP96, Mar97]. Incremental [BGG94, BGG95, BD93, Fis97].

independence [RS98a]. Independent [Abe98a, Mau91c]. Index [MZ98, JV98b]. Index- [JV98b]. Indexing [ADEDS99, DRR95].

Indic [MZ98, JV98b]. Indicia [TYH96]. Indies [Fra99, Hir97, Hir98]. Indistinguishability [BS99b, BS99c, NR98].

Indistinguishability-Based [BS99b, BS99c]. Individual [IKM99, Uni98a, HN98, Uni98d, Wel95].


Industry [ANS98b, Kan96, Lea99, Uni98j, AA95, Acc97, CWM+91, Uni98k, Wel95, Zai97]. ineffective [Min97, MBY97].

inequalities [van97a]. Inequality [MS99b]. Inference [ZHJ98, Jan95]. Infinite [CK90, HKL94]. infinitely [Ito91]. infinitesimal [Mra95].

Influence [MM92b, NH98]. Infocom [IEE92d, IE94f, IE95c]. Inform [YT96]. Information [And96c, Int91a, Ano93g, Ano95p, Ano95r, Ano96a, Ano97b, Aur98, AR99, Bar94, Bas93, BDGV93, BLMO95, BS91g, Cac98, CFGS99, CW94, CFG96, Den99, DMFB97, GRS96, GHGD98, HOQ97, He96a, HH94, HRR0, IE99a, IE97k, ISO97, KG96, KR98, KM96a, LOX99, LBHM99, Lin96a, Mau93a, MW96a, Man97a, Mau99a, Mau99b, MO99, Nys99, OdDP98, Or96, Ped91d, PL94, Pl96a, Phi98, Pit96b, PB99a, PGV93c, Pre98c, RSA93e, RSA99a, RIP95a, Sch97d, Sga93, STP93, SC96b, Sti93a, Stu99, Uni98i, Uni98k, VPM97, Wol98, Ada91, Ano97-43, Ano98d, BDGV96, BP95b, BDC+95, Bra90d, CM95, CC95, CKGS98, DL96, Dav98c, DF98, FM98b, Gru98, Gua90, Han95, Han99, HW91, IE95c, Jae90a, Jae90b, Ken95, KS98c, KW92, Mar95b, Mau93b, NIS92, Ped91b, Ped91e, Rot95a, Sch90c].

information [Sch97c, SG96b, Sim92, Tas98, Uni97c, WSFC99, van97a, GS94b].

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

Information-Theoretically [Mau97a].

Informational [Sga90]. Infrared [DDJ98].

Infrastructure [HFPS99, Or9l6, SSS99d, VSH97, Ame95, Ame96a, FB97, GH96, HMT+98].

Infrastructures [Ano99j, BPK99, BFK99, RCM99].

Inherent [She94c, KSB96b, KSB97]. Initial [Bih98b, BBDR99, SVB99, Ano96h, JJ91].

Initialization [YY99b, Ano96h, Mey97b].

Ink [BD99a, JM99]. ink [AHMS99].

Inmarsat [Ano99f, Lam99]. Inmarsat-B [Ano99f, Lam99]. Inn [IEE92a, IEE94a, IEE97e]. Inner [SVa+98].

Innocuous [CD97]. Innovations [BPBV99].


insure [Mit92a]. Inslaw [Eri97b].

Instance [BDPSN95]. Instantiation [SHK99b].

Institute [Far93, IEE94b, Ber96b]. Instruction [Cla99, SSS98, Beu94, Kuh98].

Instruction-level [Cla99]. Instructions [Ros96a]. instrument [CWM+91].

instruments [Sch93c]. Insulator [NFQ99].

Insurance [Eri97b]. Integer [MM98a, MM98b, OdI95, vO91a, SM91, vO91b, KM99a, Mao98, Pos93, vO92].

Integrated [Ano96-28, KV99, Smi98a, YS91, SY92]. Integrating [BoI98a, BoI98b, GSY99, GL96, LBHM99, LC96a, ReI92, Smi98a, AP93].

Integration [Ala93a, Ano97-34, CHLT99, CKN99, FO99b,
Integrity [BP95b, Ou99, RIP95b, RIP95a, VCF+90, Sim92, Tay94]. Intel [Gar97b, GC97, GO96c, JK97, SW97a, SW97b, Wor96]. Inteligenz [CWM+91], Intellectual [BP95b, Ou99, RIP95b, RIP95a, VCF+90, Sim92, Tay94]. Intel [Gar97b, GC97, GO96c, JK97, SW97a, SW97b, Wor96]. 

De 93a, HRT96, IH99b, Kay95, Koh90, Kn93, KNT94, Lei99a, Lin96b, Lun90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts’97, Tun99, Yu94a, Yu94b]. Kernel [BCCG93, WB92]. Kerry [IEE96c]. KEY [YY98d, ANS97, ANS98b, AKP96, AAB97, Ano96o, Ano96w, Ano97k, An97v, An98f, BN97a, BNS96, BPS98, BT99a, BV90, BV91b, BV92a, BWH98, BWH99, BZ94, CC99a, CM97a, CN98, CN98b, CN99a, CN99b, CN99c, CN99d, CN99e, CN99f, CN99g, CN99h, CN99i, CN99j, CN99k, CN99l, CN99m, CN99n, CN99o, CN99p, CN99q, CN99r, CN99s, CN99t, CN99u, CN99v, CN99w, CN99x, CN99y, CN99z, CN99}. Key [HP99a, HP99b, HY93b, HY98a, HY98b, HY98c, HY98d, HY98e, HY98f, HY98g, HY98h, HY98i, HY98j, HY98k, HY98l, HY98m, HY98n, HY98o, HY98p, HY98q, HY98r, HY98s, HY98t, HY98u, HY98v, HY98w, HY98x, HY98y, HY98z, HY99a, HY99b, HY99c, HY99d, HY99e, HY99f, HY99g, HY99h, HY99i, HY99j, HY99k, HY99l, HY99m, HY99n, HY99o, HY99p, HY99q, HY99r, HY99s, HY99t, HY99u, HY99v, HY99w, HY99x, HY99y, HY99z].
Key-Agreement [RSA93b].
Key-clustering [Kum97].
Key-dependency [MAO96].
Key-Dependent [FBS98]. Key-Escrow [VvT97]. Key-Exchange [Dan95].
Key-management [MLA91].
Key-Recovery [Oka98a, Oka98b].
Key-Schedule [KSW96].
Key-Search [KP99a].
Key-Share [BWM99b].
Key-signing [Ros96a, Ros96e, Ros96f].
Key-specific [LMS97].
Keyboard [GO96c, She95a, Ale97].
Keyboards [CFK+91].
Keyed [Ano95a, BFN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pre95b, MS95e, BFN98a, Gon95, KBC96].
Keyed-Hashing [KBC97].
Keyed-MD5 [KBC96].
Keying [BCK96d, BCKxx].
KeyNote [BFK99].
Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Daeh8, EHMS99, Gir91, KSHW97, KSHW98, KM99c, Luc98b, MP91, PS98g, SV99a, SV99b, Ste94a, Vau96, Way96b, Ano96h, Bih94a, CH79b, Cll99, DG-V94c, JP96, KC95, Knu95, LL93b, MB99, MF97, Mok97, SSI97a, SSI97b, SV99a, SH99, Sta95a].
Keystream [CD98c].
Keystroke [JG90]. KG [Uni94a, Uni94b]. KG-94 [Uni94a, Uni94b].
KHF [Wag98a].
Khufu [BBS99b, GC94].
Khwarizmi [CFK+91].
Kid [FK93a].
kids [WS96c].
Kimba [KW99].
Kind [AM97, Gad91, SX90].
Kingdom [D+98, Lom97].
Kingston [HA00, TM99].
Kiosk [BO96a, Gar96b].
kit [Ano97-38, Sun91b].
Kleptographic [YY97b].
Kleptograph [YY97a].
KMOV [Ble97].
KN [SMK98a].
Knap sack [CP91, JS93b, ACBR90, CZ90, He92, JG95, LC97b, Odl90, Wan92b, Yu92, Zha91].
knapsack-based [He92].
Knapsacks [CJS91, Ort95b, Ort95a].
Know [DDJ98b, Fly97, Hill97, Kir95, Mil95].
knowing [Ble96].
Knowledge [ADBB99, BMT98, BG90, BG93, BJY97, Bie98, BD91, BDB92, COM99, Coc97, CDS94, CD98b, Dam99a, DP94a, DP99, DO99, DK93, DS98b, GMW91, GK96, GSV99, GO93, HT98, JKP99, NOV93, NM99, O99, RS91, SI93a, SY99, Stu99, Sy92, Tou91, BOGG+90, BB95a, BB95b, CDP95, DP94a, DF93, DF94, DF91b, Sah99, Sak97].
Knowledge-Based [Bie98].
Knowledge-Level [BMT98].
known [Ano91b, BK95a, MY93a, vOW91].
known-plaintext [vOW91].
KnowRight [BS95c].
KnowRight [IEE94a].
Knotn [CFK+91].
KoMod [ST99].
Komputer [Ano97-50].
Konstanz [Bie98].
Korea [Ano93g, KM96a, Rhe93].
Korea-Japan [Ano93g].
Korean [LL98a].
Korteweg [GK95b].
Kruh [CFK+91].
Krypto [FK93a].
Kryptographie [KK97].
Kryptosysteme [Hor99].
KtSeqC [BG99].
Kudos [SVa+98].
Künstliche [CWM+91].
kuo [XtTmW94].
Kupree [DH96b, HS94, HS96b].
Kurz [Ger97].
Kyongju [KM96a].
Kyoto [Ano99c].
SAS99b, ACM99a, Ata94, DDP94b, GA98, Il94, LS98a, PS93a, Sak97, vWN99. **LANs**
[She92f]. **LANSCAPE**
[Ri96, Ano94g, Ano94h]. **LapCAD**
[Ano93k]. **Laptop**
[GPR98]. **Large**
[Bla93, BDHG99a, BDHG99b, CS97a, LO91b, LM95, NNEK97, PF94, Riv91a, SA95, SS90, She92a, Csi95, DT93, DL95, Fra90, FO093, Has99, MDS00, Yan95, Yua92]. **Larger**
[PB97b]. **Laser**
[Ano93h, JC93]. **Last**
[dBB91, dB91]. **Late**
[Bur99]. **latencies**
[JG90]. **Later**
[Sch95a, Gol97c, Roe95]. **latest**
[Bee97]. **Latin**
[BSNP97, Son99]. **Lattice**
[Ano97-29, BK98g, CC99b, CNS99b, GGH97b, CC99a, SH95a, SH95b]. **Lattice-Based**
[CC99b, CC99a]. **Lattices**
[Dwo97, Ste98a, BV97]. **launch**
[Taa98]. **Launches**
[Gar97c]. **Lausanne**
[IEE96e]. **Law**
[And96a, Bro94, Cae96b, Swi97, Uni95a, Cli99, Way93c]. **laws**
[Ano97-50, Bre97a, Cha94b, Gen99a, Gen99b]. **Lawsuits**
[Lea99]. **Layer**
[BB95c, FK99, Sar97, Wu96, Mye97]. **Layered**
[Jun99, RC95]. **layers**
[AP93]. **Layout**
[BW98]. **LCN**
[IEE97l]. **LCN’98**
[IEE98f]. **LCT**
[ZYR90]. **League**
[PWU99]. **Leakage**
[WI99, HJKY95, SG96b]. **Learn**
[Hel98b]. **Learning**
[BV98a, COM99, FCH99, HC99, Ho99, KV94, Riv93b, SKIT99, BFKL94, Kh93, Kos97]. **Leave**
[Hus99]. **Lectures**
[Dam99b, Fri96, Pr98]. **Lee**
[Scu92, LZ91b]. **Lee/Alek**
[Scu92]. **legacy**
[Un91]. **Legal**
[CYY98, HA96, Mos98, Rad97, Ros95b, Wi94, Ame95, Ame96a, Sch93e]. **Legislation**
[RDK98, Mad98d, May97]. **legislative**
[Cli99]. **legislators**
[Bre97a]. **legitimate**
[Cli99]. **Leighton**
[Zhe95a]. **lemma**
[HKM95]. **Lempel**
[Mun91a, Mun91b]. **lend**
[Ri96]. **Length**
[BR99a, BR99b, GS94a, Sch94b, YY98a, CC98, Han94, KL95b, MPL99, Su98, ZPS93]. **Length-3**
[YY98a]. **length-restricted**
[MPL99]. **Lengths**
[BDR96, HMV93]. **Lens**
[FCD98]. **Lesions**
[ZTR99]. **Less**
[BDB99b, Vv97]. **lesson**
[Scu92, WL94]. **Lessons**
[McC96]. **Let**
[DDJ98e, DDJ98f]. **lets**
[Way93b]. **Lett**
[YT96]. **Letter**
[BCE94, Joh99]. **Letters**
[Bur98b, MGL98, PKA98, SaA98, BY92]. **Leuven**
[PGV93d, Pre95a, PR98]. **Level**
[BMT98, HV98, MB99a, VW94, AG95, Ano97-30, Cla99, DF92, HWF96, Rus90]. **Levels**
[Bor96, GTGW94, dVdV98]. **LFSR**
[Kra94b, MRR99]. **LFSR-Based**
[Kra94b]. **Li**
[FW01, vT93]. **Li-Wang**
[vT93]. **li.vi.5**
[CFK91]. **liberty**
[Ele99, Wad98]. **Libraries**
[AR97, BPBV99, DL99, IEE98d, SHG98, DSSZ99]. **Library**
[Ano97-39, DK91, KHB99, Dhe98, RRP97, Man98]. **licence**
[Ano97-51]. **License**
[AG99]. **Licenses**
[Ano97-39, TJ97]. **Licensing**
[Par98a]. **Life**
[CJ99, DDJ98e, DDJ98f, DQ94, GACDAFC99, Ros95a, CWM91]. **Life-Span**
[DQ94]. **Lift**
[Gar97a]. **liftings**
[CNST98]. **lifts**
[Ano99m]. **Light**
[Gar97b, HP98, YH98, BGF95]. **light-weight**
[BGF95]. **Like**
[JQ97, BS90a, BS91c, CC98, Kob99, MS95f, MT99c, Nac93, WSFC99, XZ97, Kim93, KP93, Way93a]. **Likely**
[Bar96a]. **Limit**
[Lea99, Way93c]. **Limitations**
[BM91a, CMY98, Fis98, KV94]. **Limited**
[AR99, BDR99, DQV96, VB99]. **Limiting**
[KR96]. **Limits**
[An96b, AP98, EKK99, Swi97, BH98, Coh99, SOB98]. **Line**
[Bra95b, Cac95a, Cac95b, CF95, DT98a, Eil99, EGM90, EGM96, LMO95, PF999, SS99e, SS99f, Tra99, DL98, Gau97, Mao98, Na91, BM99]. **Line/Off**
[EGM90, EGM96]. **Linear**
[Ano95a, AMP99, BGS96, BK94a, BL95, BPV99, CFSY96, Dae95, DD99, Des98a, vdV95a, DLR97, Goll95b, HO96, Hau98b, KR94b, KR95a, KTM99, KR99b, LO91b, LH94, MS94, Mat93, Mat94b, Mat96a, Nyb95, OA94, Ros98a, SZ96, SF97, Sch96c,
Sch991, Sel98a, SK98c, SK98b, TN97, TSM95, YMWP99, ZYR91, Ala93a, AW95, BSN95, Bao94, BI93, Bh95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, HKM95, Haw98a, Jak98, KY95b, KYxx, KR96c, Kuk99, Lai95, LL98, Lan95, MM90a, MAO96, MK92, OG95, SKD94, Tze99, YT95a, YT95b, ZYR90, ZH90, vD95b, vT94, Du90.

**Linear-Time** [KR99b].

**Linearity** [SB95].

**Linguistic** [CH99b].

**Link** [Ano98m].

**Linkage** [HCY96b, LC97a].

**Linked** [BRS99].

**Linking** [BLLV98, CM95, RP94, SM99].

**Links** [Blo99, CV95, DDNM98, JC93].

**L'inuktitut** [Ano99k].

**Linux** [Cor98, DDJ98a, Eri97b, Mor97].

**Lion** [AB96a].

**Lippman** [vdWS97, vS97].

**LISA** [USE99b].

**LISA'96** [USE96a].

**List** [LC97b, Uni97d].

**Lists** [FGR92, Riv98b].

**literate** [Sab94].

**little** [Ano91b].

**little-known** [Ano91b].

**Lives** [DDJ98d].

**LL** [FY95a].

**LLL** [Mis97].

**loadable** [Ano98m].

**Local** [Fum93, IEE97l, IEE98f, MM95].

**Localization** [PJ99].

**Locating** [KP93].

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

**lock** [Ano96o].

**Lock** [BC97, CS96b, CS97b].

**Locks** [Way95, CC95].

**Locomotive** [Var99b].

**Loen** [LW96].

**Loftus** [Hel94].

**Log** [Bal99, GJKR99, Gor93b, PS98b, WD98, YY97b, Koh90, SS95a, SK97d].

**logarithm** [CP95, CS97d, FR94, FMR99, HY93b, HI97, HMP95, Mc99a, MVZ98, NR95].

**Logarithms** [BBT94, CH98, GM93b, LO91a, Man94, MW99, vO91a, Sh97, Tes98, vO91b, vV94, Gor93b, HI97, Odl94a, SS95b, SS95c, vO92].

**LOGCFL** [LMSV99].

**Logging** [Zol93].

**Logic** [AHMS99, BR99a, BAN90, CIBM99, CO98, DRR95, Gue98b, SG95, SM95a, SHK99b, CS99, Pos98].

**Logical** [PS99f, Wad93].

**Logics** [ADD99, GAGCDACF99, KW99, Len99b, WK96, Bad99, XXZ97].

**Login** [ARH95, DQ93, Hil97].

**Logout** [Poo95].

**Logs** [SK98a, SK99].

**LOKI** [BS91f, BKPS93, Kn92a, Knu93c, Kn94, TSM95].

**LOKI91** [Kn93, Kn93a, SF97].

**LOKI97** [BPS99, RK98a, Rij99].

**London** [Ano93d, Ano97-28].

**Lone** [Ano97-33].

**LONE-TAR** [Ano97-33].

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

**Long-term** [CH97].

**Longevity** [Rot95b].

**Look** [Coh96, Has99, Pi95, Zha97, GTGW94, Han95, Han99, Way91].

**Look-up** [Has99].

**Looks** [Sch97b, Mad96, vdW97, vS97].

**Loops** [vA+98, SHK99b].

**Lorenz** [Car97b, Dav98d].

**Lose** [GPR98, Way96b].

**Loss** [Law98].

**Loss** [PW97c].

**Lossy** [CI96].

**Lottery** [Riv97a].

**Lotto** [QD91].

**Lottery** [QD91].

**Lotus** [Dwo95].

**Louisiana** [ACM91, ACM97b, USE95a].

**Louisiana** [ACM91, ACM97b, USE95a].

**Louvain** [Ano90, CJL+92, DQ96, G96a, MM9W98].

**Low-Bandwidth** [Bla96a, Bla96b].

**Low-Cost** [KK99, PA99b, DVQ96].

**low-density** [CJL+92].

**Low-Exponent** [CF99a].

**Low-Entropy** [KSH97, KSH98].

**Low-Exponent** [CF99a].

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

**Low-Randomness** [DP99].

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

**Lowell** [IEE98f].

**Lower** [BD97, CCT94, OK95, Sch991, Gsa91b, St93a, vHPP93, GN95a, KO96, KO97, Sh99b].

**LR** [BP98c].

**LSI** [SKNO98a, SKNO98b].

**Lu** [LA91b].

**Lu-Lee** [LA91b].

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

**Luby-Rackoff** [BKR98a, BKR98b, Luc96a, Luc96b, PRS99].
Masonic [Mor92]. Mass [USE98b, ZTR99].
Massachusetts [ACM96a, IEE95c, IEE98f, USE94].
MASSC [Tua99]. Massey [WLB93, LLG10]. Massive [Pos98].
Massively [GM93b]. Master [BF96, CWM91]. Master-key [BF96].
Mathematical [BDFM99, BPBV99, Car98, Lid90]. Mathematics [Far93, Mil96b, Cou99, Duf98, Sch91b].
Matsumoto [Pat95]. Mattheyses [CKM99]. Maximal [Bru91, Mau90, HJPT98a, HJPT98b].
Maxims [DSB99, Bau97]. Maximum [DJL93, Koh99]. May [ACM90, ACM91, ACM93, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, And96c, Ano97-28, BV98c, CH96, CFG96, CMM93, Dan90a, Dan91a, Dan96, De95, FIP93b, Fun97, GQ95, GS94b, Hei96a, Hei94, IEE92c, IEE93b, IEE94d, IEE94e, IEE95b, IEE97i, KG96, Mau96b, Niu98, PGV93d, QG95, Rue93, Ste99b, Un98d, Un99a, USE99c, Ano96b, Gen99b, Un98a]. McCain [Mad99a]. McCurley’s [WD98].
MD [IEE94b, NIS92, PvO95, USE92b]. MD-x [PvO95]. MD4 [Ano95a, dBB91, Dob95a, Dob96a, Dob98, Dobxx, Ka91, Riv90a, Riv91b, Riv92a, Van95, dB91].
MD5 [MG98a, Ano95b, BA97, BCKxx, Ber93, Dob96b, GTG94, KR95b, KBC96, MS95c, MR95b, OG97, Par98a, Pre95b, Riv92b, Ros93, Tou95, dB94]. MDx [SRRL98]. MDx-family [SRRL98].
(Masonic [Mor92]. Mass [USE98b, ZTR99].
Massachusetts [ACM96a, IEE95c, IEE98f, USE94].
MASSC [Tua99]. Massey [WLB93, LLG10]. Massive [Pos98].
Massively [GM93b]. Master [BF96, CWM91]. Master-key [BF96].
Mathematical [BDFM99, BPBV99, Car98, Lid90]. Mathematics [Far93, Mil96b, Cou99, Duf98, Sch91b].
Matsumoto [Pat95]. Mattheyses [CKM99]. Maximal [Bru91, Mau90, HJPT98a, HJPT98b].
Maxims [DSB99, Bau97]. Maximum [DJL93, Koh99]. May [ACM90, ACM91, ACM93, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, And96c, Ano97-28, BV98c, CH96, CFG96, CMM93, Dan90a, Dan91a, Dan96, De95, FIP93b, Fun97, GQ95, GS94b, Hei96a, Hei94, IEE92c, IEE93b, IEE94d, IEE94e, IEE95b, IEE97i, KG96, Mau96b, Niu98, PGV93d, QG95, Rue93, Ste99b, Un98d, Un99a, USE99c, Ano96b, Gen99b, Un98a]. McCain [Mad99a]. McCurley’s [WD98].
MD [IEE94b, NIS92, PvO95, USE92b]. MD-x [PvO95]. MD4 [Ano95a, dBB91, Dob95a, Dob96a, Dob98, Dobxx, Ka91, Riv90a, Riv91b, Riv92a, Van95, dB91].
MD5 [MG98a, Ano95b, BA97, BCKxx, Ber93, Dob96b, GTG94, KR95b, KBC96, MS95c, MR95b, OG97, Par98a, Pre95b, Riv92b, Ros93, Tou95, dB94]. MDx [SRRL98]. MDx-family [SRRL98].
Meet [FY99, Van95b]. meeting [Ship99a, Zim96b]. Mellen [Err99].
Members [Par98c]. Membership [FGR92, Fis98, OOK91, SPH99, AK95, MW94, Sak97]. Memoir [Bar95]. memoirs [RK98b, Sel94].
Message-Resend [Ber97c]. Messages [CFPR96b, vD97, SS99c, SKAM99, Bre97b, CFPR96a, Joh97b, Kip97, Mit92a, Par98b,
Model-Checking [Bol98a, Bol98b].
Modeling [DD99, KM98a, LM96, SS99a, ZFKP98, ZFK98, Ano93k, CM97d].
Modelling [CK95, GAGCDFAFC99, HL92, LK98, NT93, PS99a, SM99, Tro93].
Models [Ben99, CH99b, DL99, DP99, Ger99a, HHD99, LL97a, OMA98, PZ98, SY99, SHT98a, TKG99, CT99b, Nis91, OMA97, SZT98b].
Modems [Gar97b].
Modern [Buc91b, Gol97a, Gol97b, Gol99a, VG99, Dam99b, Unixxa]. moderne [Bra93b].
Modes [Ano96c, Bih94b, Bih96, Bih98a, Bih99b, CV99, HP99a, HP99b, HRV99, MT95, NA95, SHK99b, Wag98b, Bih95a, Nas94].
Modification [AKF94, FG98, Sel98b].
Modifications [NM95, OMA98, Moi98].
Modified [BDG98, NK98a, PBGV90, Wic90, CLW98, HWB93, LZ91b].
Modula [Bra93b].
Modula-3 [Bra93b]. Modular [Ano96c, Bih94b, Bih96, Bih98a, Bih99b, CV99, HP99a, HP99b, HRV99, MT95, NA95, SHK99b, Wag98b, Bih95a, Nas94].
Modular [Ano96c, Bih94b, Bih96, Bih98a, Bih99b, CV99, HP99a, HP99b, HRV99, MT95, NA95, SHK99b, Wag98b, Bih95a, Nas94].
Modulo [Bra93b].
Modulo-Place-Invariants [DM94c]. modulus [Tze99]. molecular [ARRW99, Ram92].
Molecules [GC98].
MON [YY98d]. Monetary [Gar97c].
Money [YY98d].
Monkey [YY98d, YY98b].
Monograph [Lea90]. Monomial [Pat96].
MOPonopolizingKEYs [YY98b].
Monstör [Gar98b]. Montages [AKP99].
Montana [BCB97]. Monterey [USE99d].
Montgomery [NM94, BP99b, Kal95, KAK96, Nac93, NMR95].
Montgomery-suitable [NM94, Nac93].
Montreal [ACM94c]. Moose [Ros96b].
moot [Ano96d]. Morphology [Blo99].
Morphometry [SCG99]. Morses [SCH98].
Moscow [CW94]. Most [BV96, KAK96]. motion [Nas94, ONT98, YEA98].
Motorola [DK91, Gar97a]. Mouth [DDJ98c]. MOV [HIS99]. movable [GMLH94].
MPEG-2 [DS97c, HG97e, HG97d]. MPEG-4 [HEG98]. MPEG-encoded [DS97b].
MPEG2 [HSS99]. MPEG2 [DS97b].
Multi-Agent [Lee99b, VCG99, DDNM98]. MR [DTDJ99].
MRA [BALS99, LFCK99]. Ms [CFK91, Gar98a]. MS-DOS [Gar98a].
MSC [WSFC99]. Müller [JQ98b]. Multi [CM99b].
Multi-agent [CM99b]. Multi [BBDF97, BDD94, BM99c, CC99c, CF99c, DHS99, DF97, FMH98, HS94, HTW99, HVH98, JvV96, KSB97, Lee99b, Mar98a, PM99a, SNW98b, SJS98, Sut99, TN96a, TN96b, VC99, CL97a, CGS97, HW98c, KSB96b, SVWMB95, SOB98, VSB95].
Multi-Agent [Lee99b, VCG99, HTW99, PM99a].
Multi-Application [Mar98a, DF97].
Multi-authority [CF99c, CGS97]. multi-carrier [SVWMB95, SOB98, VSB95].
Multi-disciplinary [DF97].
multi-exponentiation [CL97a].
Multi-function [KS97, KS96b].
Multi-Receiver [SNW98b]. Multi-Secret [BM99c, BDD94]. multi-senders [HHW98c].
Multi-Service [HS94]. Multi-tiered [CC99c]. Multi-user [SJS98].
Multi-variable [TN96a, TN96b].
Multi-application [Gir99, Tua99].
Multicast [CM99b, PB99a, Mit92a].
multicasting [CM96]. multicasts [W99].
Multidimensional [BMS99].
Multidrawing [BMRW98]. Multifeature [Bet95c]. Multifunction [She94c].
Multigroups [OOK91]. Multilevel [CGB+93, GPSN98, KT96, DN95a, ZH93].
Multimedia [ACM96a, ADF98, CLKS96a, CKLS97, Dan96, D+98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR97, LvdLB96, Lip99, NAA99, ZK96, CLKS96b, IEE97k, Kat97, LS98a, Oko97, PS97].
Multimedia [ACM96a, ADF98, CKLS96a, CKLS96b, Dan96, D+98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR97, LvdLB96, Lip99, NAA99, ZK96, CLKS96b, IEE97k, Kat97, LS98a, Oko97, PS97].
Multimodal [ACM96a, ADF98, CKLS96a, CKLS96b, Dan96, D+98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR97, LvdLB96, Lip99, NAA99, ZK96, CLKS96b, IEE97k, Kat97, LS98a, Oko97, PS97].
Multimodal [ACM96a, ADF98, CKLS96a, CKLS96b, Dan96, D+98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR97, LvdLB96, Lip99, NAA99, ZK96, CLKS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

n [ISO97, TN97]. n-bit [ISO97]. Naccache [Cus97]. Naccache-Stern [Cus97].
NAFTA [Mad98f]. nag [IPNdbbbprm91].
Nam [CLW98]. Name [Gar97a, Gar98b, Ano97-29, Lea90].
Nanomedicine [DDJ98e, DDJ98f]. Naor [Geh94]. Napa [IEE93a]. Napier [CWM+91], narrow [CC98], narrow-sense [CC98]. NASA [CWM+91]. National [Acc97, Ano96a, DDJ98b, Dan96, IEE94b, NIS92, Unis98a, Wei91a, Wei91b, Rat96, Unis98b, VB96].
Nations [Sch98a]. Natural [Dim94, KKL99].

[MSN99, Rus93b, Rom90b]. necessity [KK97].

Necessary [MSN99, Rus93b, Rom90b].

Net [Gar97a, Gar97b, Gar98a, GB98, Got99]. NetBill [CTSxx]. NetCard [AMS96].

Netherlands [Cha91, Hei96a, TV94, TV92]. netlist [CKM99]. Nets [Des98a, DR98b, KA99, YK98, NT93].

Netscape [DDJ98g, DDJ98h, GW96, Law98, She96b].
NetTracker [Ano97-34]. NetWare [ARH95]. Network [ACM98a, BK90, Coh99, DS90a, Ebe93, EH96, Fum93, GM93a, HS96a, Kan96, Koh90, KN93, KCCT94a, KCCT94b, Law98, Lee95, Len96b, Lom94, Mar99, MSK99a, MT99b, RS99a, She93d, SVB99, SS99d, Tun99, VDDR99, VN99, VN95, WKHG97, WN98b, Wu96, AP93, BGT96, Ha97, IS99, JJ95, SSM94, SY96b, Sta99a, UFC94, Yor96, ZG96].

network-centric [BGT96]. Network-Layer [Wu96].
networked [Ano97-28]. Networking [IEE98e, FJV97, LS98a]. Networks [ATAY98, AWV99, BF97a, Bra90a, CT99a, DQ93, HG97c, IEE97l, IEE98f, Jut98, KRJ98, Lea99, LSVVV95, OMV98, PKOT94, PT95, Por91, Sal91, SK96c, SK96d, SV94, STP93, THP98, Tow98, VSH97, Ver98a, Ano95q, Ano96j, ACBR90, Atk93, AC97, FB99b, CW91a, CWY98, Fra90, GBL94, HT95, Hor94, HLLC96, Jen99, LC96b, LC96c, NT94, Nor95a, O’C95, Opp96, PS98c, PS98d, PS98e, PS98f, PS99d, PS99a, PS99c, PS99b, SV95a, SBTV99, Zan90].


No-Transferable [Sak96]. nodes [GMLH94]. noise [PC98]. noise-based [PC98]. Noisy [Crc97, Lip94, MSHP99, MM92a, MFG95, GM91]. Nomikos [IEE97c]. Nominations [Nat97b]. Non [AVW99, BM90, BG90, BS99b, BS99c, BS91b, DY91a, DPP99, DR94c, DDN91a, DDN91b, FCD98, FDB93a, FDB93b, GPT91a, GPT91b, GP99, G93, HIPT98b, Jak98, KR96c, LW99, Mas99a, MY91, NO98, Pai98a, Pai98b, Ped91d, Ped91b, RS91, Sah99, DY91c, SCC99, TSY98, Yah94, Ano95q, BKR98a, BKR98b, DDB95b, Ell97, HIPT98a, LLB98, MY93b, SB95, Sin95, SBTV99, DDB95a]. non-Abelian [DDN91b, BS99b, BS99c, DDB95a]. non-biased [TSY98].

non-carcinogenic [SBTV99]. Non-classical [Mas99a].

Non-Commutative [GPT91a, GPT91b]. Non-Encrypting [LW99]. Non-Euclidean [SCG99]. Non-Existence [FDB93a, FDB93b]. Non-Interactive [DY91a, GO93, MY91, BM90, BG90, DDP99, Ped91d, Ped91b, RS91, DY91c, MY93b, Sah99]. Non-invertible [NO98, BKR98a, BKR98b]. Non-linear [FC99, Jak98, KR96c, LLB98].

non-linearity [SB95]. Non-Malleable [DDN91a, BS99b, BS99c, DDN91b, Sah99].

[ZW99]. Obstacle-avoiding [ZW99].
obstructs [Ree97], obtained [EvH93].
obtaining [CLHL98]. Occam [GN95b].
Ochrono [Sch95e]. October [Ano93d, Ano93g, Ano96a, Cha91, FM91, IEE93a, IEE94a, IE96a, IE96d, IE97f, IE97h, IEE75, IEE98f, IE99a, NIS92, Oht96, ODP98, TV94, USE93, USE96a, Ame95].
Odds [McC90b]. ODEs [Ruo94]. ODMG [Wat99].
OECD [Org98a]. Off [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AG95, Ano94i, Ano96-29, Mao98, Riv98c, VNM99].
Office [Fuc99, UU97a, Uni96b]. Official [Zim95a]. OiDP98, TV94, USE93, USE96a, Ame95.
Odds [McC90b]. ODEs [Ruo94]. ODMG [Wat99].
OECD [Org98a]. Off [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AG95, Ano94i, Ano96-29, Mao98, Riv98c, VNM99].
Office [Fuc99, UU97a, Uni96b]. Official [Zim95a]. OiDP98, TV94, USE93, USE96a, Ame95.
Odds [McC90b]. ODEs [Ruo94]. ODMG [Wat99].
OECD [Org98a]. Off [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AG95, Ano94i, Ano96-29, Mao98, Riv98c, VNM99].
Office [Fuc99, UU97a, Uni96b]. Official [Zim95a]. OiDP98, TV94, USE93, USE96a, Ame95.
Portable
[Smi98a, BY93c, BY93b, Car94]. Porting
[JJ91]. Portion [Len98]. Portland
[Aue96b, USE90]. Position
[BFK99, CM99c, YST99a]. Positive
[Dwo97, YY98a]. Possibilities [Jam98]. Possible
[Cae96b, MW96a, Ano96n, NM96b]. Post
[AA93]. Post-Markov [AA93]. Postage
[JJ91]. Potential
[GQW'91, Nor95c, Uni96a]. potentially
[Kma95]. Potomac [Ros99]. Power
[Ano99c, BS99a, CJRR99a, KJJ99, MDS99,
PRAM98, SKNO98a, SKNO98b, Sha99b,
T'99, Goo96, SOB98]. Power-Analysis
[CJRR99a]. PowerPC [UFC94]. powers
[SS95a]. pp [Ano97-48]. PPP
[BV98b, Kas96, Kum98, Mcc96a,
Sim96b, SM99b]. PPTP
[SM99b, DDAJ98c]. Practical
[ASW99, ADBB99, AB96a, AWV99, Aur96,
Av08, Bac95, Boxxx, CD96, CS98b,
Dam91b, Dam94b, Dam94a, D93, FO97,
HBKL99, IH99a, Jne99, KTM'99, Oka93b,
v99a, PRS99, PV90, Sak97, Sch92a, SW93,
Smi90, Sta96d, Z93, v901b, And93,
AM99e, BI93, Bou94, Fra90, FO039, FO98,
HZ93, HNM98, IH99, Jac90a, Jac90b, J95,
LR95b, PS98b, v902]. Practically
[Got98b, Knu94a]. Practice
[Bel99, DSB99, GN95b, IZ98, IZ99,
LABW92, AN94, AN96, Dam99b, Ger97,
LABW91, Sch93a, Sta99a, Sh95].
Practice-Oriented [Bel99]. Practices
[Des99a, JJ98b]. Prague [Ste99b, vWN99].
pratiques [Bou94]. Pre
[DO99, HG97c, Zim96a, Zim96b]. pre-alpha
[Zim96a, Zim96b]. Pre-compressed
[HG97c]. Pre-processing [DO99].
Preassigned [SW99b]. Precautions
[GQW'91]. precision [Kal92].
Precomputation [LL94b, dR95].
Predefined [Len98]. Predict [Kra90].
predicting [Gil97]. prefix [MPL99].
Prefix [ADD99]. Preliminary
[BC93a, BPBV99, DY91c, Zim96b]. prelude
[Unixx]. Preneel [WBDY98]. Preparations
[Law98]. Prepositioned [Sim90b].
Preprocessing [dR94b, dR94a]. Presence
[BDHJ99, CH94a, CHH97, Cra98, Gar94,
JQB97, Cra97]. present [Sim94c].
Presentation [KI99, LS98a].
Presentations [HMT'98]. Presented
[DBGV93, NS99a, Ano95r]. presents
[GLC98]. Preserving [NKP99, D99].
President [C197, C99, UV97b]. pressed
[An96]. Pretty [An94i. Elk96, Gar95,
Mei96a, Ros97a, Zim96a, Zim96b, Gar98c,
S917a, SS197b, Sta94a, Sta95a].
Prevalence [YY97b]. Preventing
[Jas96, SHK99b]. Prevention
[OG97, VNW94]. Previously [DH90].
PRFs [HWKS98a, HWKS98b]. Pricing
[DN93, Ros94]. Primacy
[Bo90, G99b, Lan99, Len90, Yan95].
primary [Ban94]. Prime
[LO91a, Scho, Boy97, DLP93, Graxx, ML98].
Primer [Sch94d, Di 97b]. Primes
[BD93, GS99b, Lan99, M94i, Riv91a,
RS98c, RSxx, S97b, S97a, DL95, YY99].
Primitive [S94, She95c, J98a].
Primitives [CF99, Pre98a, RIP95a, RIP95b,
VCF'90, ZMI91, BFKL94, BP95b, Di 99].
principle [Dam90b, GJ90]. Principles
[AC99a, AN95, HGD98, K99a, KG99,
MG91, PRB98b, Zhe90, Sta99a].
Printer [Con93]. Privacy
[An94i, An95c, An97-34, Avo98, Bac95,
BBC95, Ble88, Bar96, Cha92b, DL98,
Elk96, FJP96, FHM98, Gar95, IEE92c,
IEE93b, IEE94d, IEE95b, IEE97i, Ken93,
KFJP96, Lin88a, Lin89a, Lin93a, Lut98,
MW97, Mjo93, NKP99, Par98c, SY96a,
SYMI98, SB97, SG96a, Sta94a, Sto98, Tho96,
Tra99, Uni98a, Uni98i, Ada92a, Ban94, Bro96,
CM95, Car94, Cha92a, CK93, Cl99, Dom96,
HM96, JML99, Mar95b, Mei96a, Mid95,
Rot95a, S914a, Sta95b, Uni98d, Uni97c,
VPM97, Zim96a, Zim96b, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, Zeg93.

Privacy-Protecting [Tra99]. Private [BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, McV93, RSA93e, Dam96, DS90a, McV93, Sch95d, SS98b, Ts90, Wil93b, ZG96].

Privacy [BDF98, BD99b, CKGS98, HR90, Mv93, RSA93e, Dam96, DS90a, Sch95d, SS98b, Ts90, Wil93b, ZG96]. Private-Key [HR90, McV93, RSA93e, DS90a, SS98b]. Privilege [ECM96]. Prize [GC97, Pin98].

PRO [Ano97-33, Gar98c]. Proactive [CHN97, FGMY97b, HJKY95, HJJ+, 97, HJJ++xx, IBMxx, Jar96, Rab98, BCR98, FGMY97a]. Probabilistic [Jak98, JO97, SF97, Sch91b, Tou93, Gol99a, GO95, HK90, Imp92, Lon91, TX92].

probabilities [Lew92]. Probability [BDG99, Gol96b, Kob99, TY94, AI96, MHHMV98, MAO96, WM93]. Probable [BD93, NK93, DLP93, Graxx]. Problem [Bon98b, Bon98a, BN96, CS96a, Cha90, DD99, DJL93, GO96c, HM98, KM99b, KR99b, MT99b, NS99b, OMV98, Per99, RS99a, CPS95, HY93b, H91, HM97b, HMP95, LC97b, Mas97, McC90a, NR95, OA99, MS096].

Problems-Solving [Per99]. Problems [AA93, BD99a, Bra90a, GGH97b, KRS99, MC92, Poi99, Smi90, APDS93, Bea92, BFKL94, FR95a, Han95, Han99, HC95a, IEE97e, Lew92].

Procedure [Ada97a].

Proceedings [BPR99].

Proceeding [BPR99]. Proceedings [ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, Ano95r, Ano98m, Bri92, Bri93, Com96, GN95b, IEE95a, IEE99a, IE92b, IE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96e, IEE96d, IEE97d, IEE97f, IEE97h, IE98e, MZ98, Nat99b, OW95, PSN95a, Pit95, Sti93b, SIJ93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96c, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94e, Bih97c, B+96b, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fun97, Go90b, HO97q, HA90, Hir97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, K99, Kn99c, KP99b, KK99b, Kra98, LOX99, LM98a, LW96].

proceedings [Lom97, MV91, Nyb98, ODIP98, Pre95a, QV90, QG95, Q+98, Rue93, SZ93, Spi95, Ste99b, TM99, TV94, T+98, Tv92, USE90, USE98d, VPM97, Van98e, Wat91, Wie99, Wol93b, Yua92, vWN99, ACM93b, CH96, Chr99b, IEE94e, Sti94, Wal99a, BCB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fe91, Go96c, GQ95, GS94b, He94, IRR93, Kal97c, Ko96, Mau96b, PSN95b, SP90].

Process [AMP94, Kn99a, Rob98a, RS99c, YT96, CWM+91]. Processes [Gar98b, Bea92]. Processing [Ano97b, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97h, IEE97d, IEE97j, IEE97k, IND99, KV99, LMP99, LW96, Pin98, Pit95, Ano96-30, DO99, DF97, Man98, Sab94, T+98, Whi90].

Processor [Gar98a, RB99, SW97a, SW97b, She92e, Sut99, VVD190, Von92a, Von92b, DV996, She92c]. Processor-efficient [Von92a, Von92b]. Processors [Cla97, KK99a, She92e, BS95c, MPH96, NM96a].

Proctoring [SKW96]. Prodigy [CKF+91].

produced [SSI97a, SSI97b]. Product [GO96c, KS98a, KS98b, KS989c, GN95a, SS98b, Ano94i].

Products [Ano97-33, Ano97-34, Cha94b, CII97, Los97, UU97b]. Professor [Swi97]. Profile [Hor92, HFP99, MM90a, MK92].

Program [BDFM99, FG96a, LBMC94, FG96b, KT99, LS98a, Pre97b, Pre97c, Uni95a].

Programmable [DMVC99, SVB99, TT99, WB94].

Programme [BGV93]. Programmer [Bre99, DDJ98a, Jo195, Ste94b, vdWS97,
Programmers [Gar97c, Joh97a, Joh97b]. Programming [IBM93, BGS96, CO98, Erri97a, JDK+91, Ste90a, Ste90b, ACM99a, Gre98, LS98a, OA99, Sab94, vWN99]. Programs [BK95c, DRR95, SG95, SHK99b, WB95, Zwi98, B+96b, DFHR91]. Progress [Ano96-28, Ano97-45, BDI+96, KSB96b, Wol93b, Wol93a]. Progressions [Mih94]. Project [BPBV99, IBMxx, GH96, Man98, DS90b, RCM99]. PROMIS [SSCP99]. Promise [Law98, Los97, Mar96]. Promises [ABK98b, ABK98c, ABK98a, BAK98, DKF93, FS97b, GMW91, GO93, JMS96, CDP95, DP94, Gol99a, PS96d, Sak97]. Proof [Bol98a, Bol98b]. Proof-Based [BK95c, BG93, BD91, CD98b, DFR91]. Proofs [BG90, BG93, BD91, CD98b, DFKN93, FS97b, GM93a, GO93, JMS96, CDP95, DP94, Gol99a, PS96d, Sak97]. Propagation [GPR98, SG99b, SZZ95c]. Properties [Boy99, Con99b, KA99, MM90b, MS91, OK98, OS98, Tou93, VW98, WW98b, Zie97, BHH99, CD95, FSS94, KS96a, Kuh91a, PS99a, XZZ97]. Property [CFG99, DL99, LQR99, SRY99, Uni97b, Ale98, BS95c]. Proposals [ABK98b, ABK98c, ABK98a, BAK98, DR98a, KR94a, LM90b, Ano95n, Cl99, LM91a, RH92, RRS98, Ban94]. Protocols [Dae99, VvT97]. Propose [Gar98b]. Proposed [CP91, Lea99, LL98a, Nat92a, Riv93c, SB93, Wag98b, CMA96, Gu90, Mey96b]. Proposes [Gar97a]. Prosthesis [HHD99]. Protein [SV99]. Protect [Sch94, Sta95b, Cll99, KR96b, Way93b]. Protected [CH94b, DY91f, Mad98b]. Protecting [BO96a, Ble98b, Des90a, EHMS99, GMD98, KR98, Lut98, Mar95b, MW98b, PT95, SYM98, Tra99, VP99]. Protection [BG95, CH97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LQ98, LvdLB96, LvdLL97, LML98, Per97, Sm90, Uni97a, Uni98i, ZK95, ZK96, Ale98, BBC97, BBC98a, BOD95, CPO+98, CHO+98, Cl99, DFHR91, GO96a, Ibb97, OP+99, RP94, RKDB96, SY96a, Sta94a, Tev92, TSN93, Uni97c, YEA+98, FT95]. protections [HPPA99]. protects [Ano95m, Ano96j, Ano97-43, Ano98d, Ano98s]. protest [Ano97-52]. Protocol [ATAY98, Ano95a, BM99b, BV98b, Bra95a, Bra96, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JMP+98, JQ97, Kas96, KSW98a, KSW98b, Ks98b, Kra99, Kum98, Low96, Mau94, MW99, Mey96a, Moo92, NS98b, NS98c, OMI93, RS98a, RS98b, SSN98a, SH97, SM98a, SM95a, Sim96b, SM96, SM98b, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CM96, CTSxx, Des96b, EvH93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS98f, SK97, Sim94b, TH99, WS97, WL94, Zeh95a, GM93a, Sar97]. Protocols [AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BG98b, BWM98, BWM99a, BBC93b, Ble98a, Bol98a, Bol98b, BD91, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dan99a, DGT96, DQ93, DS97d, Fe93, Fe96, FBS97, Fum98b, GM93a, Geh95, GS97, GMV98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IEE98e, KKK91, KFG92, KS97c, LHY93, LL97a, LHB96, LL95a, LS92, LM96, MB94a, MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, SL93a, Sch94g, Sch96a, Sch94h, Sch99k, SSP90, Sy92, Tou91, Tou93, AN94, AN96, AG97b, AG97c, AG97a, Aba99, ABC+98, BDH97, BH93, BCK98, BG95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, CJ95, Dan97, FGH99, Fe99, GEL98, Hor98, HLL+95, JW01, LY93, LH99, LL95b, Lom97, Man95, Mas97, MLY93, Mea95, MW98c]. protocols [NT93, PS98e, PS98e, PS98f, Pau98, PW93a, PKM97, SSG99, Sy93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].
prototypes [Ano96-30]. Prototyping [AKP99].

Provably [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, LM95, Mau91d, Oka93b, PS96c, Sho96, ZMI90, BH93, Dam94a, FO98, GoI90c, NY90, PSW95]. Provably-Secure [DY90, DY91d, DY91b, Mau91d].

prove [Zha96]. proven [DS93, Lea90].

Prover [DY91a, GPSV98, HB99, DY91c, DFKN93]. provers [JY96, Ped91a].

Provide [BDR+96, SA95, Ano99i, Ano99h]. Provider [Tre99]. provides [MHMW98]. Providing [Bra90a, SKAM99, Ano95c].

processed [Ano96w, Ano96-30, Ano99j, Ano99l, AA93, BP98a, BI95, BDHJ98, BDG198, BCE+94, Bec99, BC95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BFK99, Ble97, BF99c, BS94, CC99b, CG99, CIS91, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De 93c, DP98c, Di90, El99, FY95a, FY98a, FYM99, GFLP96a, GFLP96b, FO99a, GHY90, Gal96, Gar96b, Gib91, Gib96, Gir91, GGH97b, GH99, HK99a, HGS98, HP98a, HY93b, HM93, HL93b, HJJ+xx, Hes97, HPS98, HPS99, IZ98, IZ99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKOT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Mau93a, Mau97a, Men93, MM96b, Mic93a, Mic93b, MM98a, MM98b, NS97a, NY90, Nec91, Nec96].

Public [NS99a, Odl94b, Oka94, OU98a, Omu90, vO99a, PSR97, Pat99d, Pat95, Pin97, Poi99, RSA94, RCM99, Rud91, Sal90, Sal96, DP91, Sas99a, SE96, She94d, Smi93b, ST91, Sun98a, Sut99, TAP90, TA92, VSH97, dwQ91b, Wie98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zin96b, dwQ91a, vO91b, AA95, AD97, AD99, Ano90, ADSW99, Bae94, BI94, BD98a, BSB97, BS91a, Beu94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cs95, DW96, Dam96, Den90, DQV96, Dhe98, DN95b, ES97, FGMY97a, GH96, Gib95, He92, HWF96, HJJ+97, JM96a, Jar96, Jon90, KASH90, KM99a, KI95, KM99d, Kos99, LG97, Las92, LMJW93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LCL95, Lon91, Lon92, Low95, MI90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rac90, Roe99, SW95a, Sch92c].

Psychoacoustic [Til98]. Psychovisual [DDM98]. PTY [LT98]. PTY-Marks [LT98]. PUB [Nat95, Nat99a, FIP93b, NS93b]. Public [ANS97, ANS98b, Ace97, AKP96, Ano95, IBM93, Ano96w, Ano96-30, Ano99j, Ano99l, AA93, BP98a, BI95, BDHJ98, BDG198, BCE+94, Bec99, BC95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BFK99, Ble97, BF99c, BS94, CC99b, CG99, CIS91, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De 93c, DP98c, Di90, El99, FY95a, FY98a, FYM99, GFLP96a, GFLP96b, FO99a, GHY90, Gal96, Gar96b, Gib91, Gib96, Gir91, GGH97b, GH99, HK99a, HGS98, HP98a, HY93b, HM93, HL93b, HJJ+xx, Hes97, HPS98, HPS99, IZ98, IZ99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKOT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Mau93a, Mau97a, Men93, MM96b, Mic93a, Mic93b, MM98a, MM98b, NS97a, NY90, Nec91, Nec96].
Rapid [KM93, GTS90]. Rate
[BDGV93, BS91g, LK998, Sti93a, Bla9a, BDGV96, KL95b, MHMW98]. Rates
[HK97, HR90]. Rational
[KG95, Koz96, ST91]. raw [HG96]. Ray
[Aga92, BAL99]. RBF [WKHG97]. RC2
[Ano97c, KSW97a, KSW97b, KR998, Riv98a]. RC4 [MT99c]. RC4-like [MT99c].
RC5 [Ano97-45, 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, RSSY98]. rDSA [ANS98b]. Re [FL99b, Jak99c, Sto98,
AGY95a, Bur98b, HG97d]. re-encoding [HG97d]. Re-encryption [Jak99c].
Reactor [HRV99]. Read
[Sta97b, Coh96, LF97]. Reading [Eri97b]. Real [BBT94, BMT96, BFW99, CM98,
CG+93, DDJ99, DJHP98, DDNM98, GFB93, GLSM99, IR99, JMP+98, Lut98,
MGL+98, Mar99, RH99, Sch94c, SKIT99, Yac99a, Yac99b, ACC99, IEE94b, Xie93].
Real-Quadratic [BBT94, BMT96].
Real-Time
[BFW99, CM98, CG+93, DDJ99, DJHP98, GFB93, IR99, JMP+98, MGL+98, Mar99,
RH99, Yac99a, Yac99b, ACC99]. realization [Tan90]. Really
[Ano93c, DDJ98a, Rit99, Sim90a]. Realms
[ARH95]. Reapplication [Sch99c].
Reasoner [MD99]. Reasoning
[AG97a, BMC95, DSSB95, KM99c, MR95a, PK99, Var98b, Ger99b]. reasons [Ri96].
Reassessing [Neu95]. Reassure [MB99a].
Recasting [Sal91]. Receipt [BT94, SK95]. Receipt-Free [SK95, BT94]. receive
[Way91]. received [Chi97, UU97b]. Receiver [SNW98b]. Receives [Pin98].
receiving [HCC98]. Recently [Wag98b]. Recently-Proposed [Wag98b].
Rechnergestützte [MP94]. Recipes
[FSB97]. Recipient [WP90, Wag90, WK97]. Recognition
Recommendations [Ano95a, Kal98g]. Reconciliation [BS94, CM95].
Reconfigurable [BP99b, PBM90]. Reconstruct [HD96a]. Reconstruction
[BC95b, BD98b, LH95]. Record
[Har90, LCL92, Cha99b, CDEH96, IEE96f, IEE98b, JLM+94, Mey99]. Record-Oriented
[LCL92]. records [Sav97]. Recoverable [YY99b, YY98c].
recovering [PBBC97]. Recovery
[AAB+97, Int91a, DC98c, GQW+91, LK99, Miy96, Oka98a, Oka98b, Uni98i, WLEB96,
HMP95, JLM+94, KM98c, Mad98f, NR95, Uni97c, Yeu99]. rectangles [Son99].
Recurrence [TK99, Tze99]. Recursive
Redesign [BKPS93, PRAM98]. Rédi
[Pie39]. Rédi- [Pie39]. Redistribution
[MSNW99]. redistributors [DF98]. REDOC
[Nor95a, BS91f, CW91b, GN95c].
REDOC-II [BS91f]. Reduce
[Hig97b, SVWMB95]. Reduced
[BBS99a, BKR97, MT99a, BBS98a, PNRB94]. Reducing
[DS98b, JQ98b]. Reduction
[CTT94, GGH97b, JK98g, PP92a, PP95b, PP95a, SH95a, SH95b, SPP98, SOR98].
Reductions
[FS98, HSSI99, OU98b]. Redundancy
[GM97, Mis97]. redundant
[SOB98, TY92]. Redux [JJ98c]. Reengineering [AMP94]. Reference
[Bar96b, CDF195, KMKH99, Pre97c]. refined [HWF96]. Refinement
[STW95, JS93a]. Reflecting
[Jan95]. Reflective
[BCCD99, DL99, KHB99].
Refunds [Hir93]. Regarding [Roh99, CJRR99b]. Regional [ADEDS99].
Register [CS96b, CS97b, GN95a, GM91]. Registrations [GO96b, Gol94, GO95, GK95a].
Registration [Bal97, TOH98]. Registry [PKA+98]. Reglementierung [MPS94].
Regular [SG95, DI99]. Regulated [Way93c]. Regulating [Riv98c].
regulation [Koo97, Ram92]. regulations [Ano96u, Ano97-49, Ano98u, Cha94b, Cli97, Szw97a, UU97b].
Reinventing [Yuv97]. Rejected [Eri97b]. Rejects [Gar97a, GC97].
Related [Ber97c, BV96, CH98, Cle91, CFPR96b, De 93b, De 98c, ECM96, GS97, KSW97a, KSW97b, WB95, Bih94a, CFPR96a, OU98b, Zer96a]. Related-key [KSW97a, KSW97b]. Related-Message [Ber97c]. relating [Aus96]. Relation [BHSV98b, BHSV98a, SK98c, SK98b].
Relations [BDPR98, Jak98, NMV99, Uni98c, Uni98d, Uni98e, Tze99]. Relationship [GSV99, HT99, MW99, Oka93a, SZZ95c].
Relationships [Kem99, Len99b, RG95, SS95a, SG99b, SZZ95a, GGK*99]. relaxes [Ano98v]. relay [Ano95m, Ano99h].
Release [Dam94b, Dam94a, DOR99, Sun91b, Zim96b]. Releases [DDJ98a]. Releases [Got99, Wor96]. Relevance [SS99d, Tra99].
relevant [Hi94]. reliability [BHS93, HS96b, IE94b]. Reliable [BF97a, BF99b, KM93, CM96, FD92]. relief [Mad99b].
Relinearization [KSS99b]. Relying [ZMI90, Sak97, Sch99c]. remainder [DDPS96, WW99].
Remark [CMTNY94, LHL94, FR94, MY93b]. Remarks [BY92, GPSN97, Gro94, Gui97, Oht98, BBL95, La92].
Remote [Ano97-36, BLM94, FMM99, HS97, He98a, LC95, RRST97a, RRST97b, SK97c, Ano97-27, Sha97a]. Remotely [BFN98b, Luc97, Luc99e, LW99, BFN98a].
Replay [OG97, YL97b]. Replicate [RB94]. Replicated [KB92]. Replicating [HS96b].
Replication [BLM94, Pit96b]. Reply [NC97, BMP+97b]. Report [Bra93a, BDI+96, Dra98, EMMN98, Kui91, Nat99c, Par98c, PH91, RIP95a, RD99a, Tou95, Vau99d, Wor96, Ano99e, BHS92a, BP95b, Bur98a, KSB96b, NBD+99, Org98a, RIP95b, UU97a, Zer96a, Dan95, BFS92b].
Representation [CK95, Ger99b, JKVP99, LE99, NA95, PNFK95, TY92].
Representations [FC99]. Representatives [Clin97, Uni97a, Uni98c, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, UU97b].
required [BGS95]. Requirement [Sil97a]. Requirements [Ano97b, BD92, Bel92, BC95c, FR95d, HJT99, HH94, VW98, Com94e, MW98a, SM95b, UN94].
Research [Ano99c, Boo96, DDJ98c, Dam96, Des92, Des98c, DEQ92, Ele98, IEE92c, IEE93b, IEE94d, IEE98d, Jan99, Q+98, Rhe93, Wol93b, Ano97-52, Wol93a].
researching [Uni96a]. Resend [Ber97c]. Reserve [Ano97-42]. Reshraring [AGY95b].
Residue [KKOT91, PP92b, CB96, PP92a, PP95b, PP95a]. Residuosity [Pai99d, DDP94b]. resilience [FGMY97a].
Resilient [BGS94, BGS96, MS99b, RS98a, GHS93].
Nat97a, NP98b, Pad98, PHF99, Rab94, SC96a, SZT96a, SZT96b, SZTB98, TKS98, ZK95, BBCP98b, BD97, FGY96b.

Robustness
[AN95, MMST98, YMWP99, Irw98].

Rockland [GS94b].

Rocky [Ano97u].

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

Role-based [JJ95].

Role-Centered [VC99].

ROLLING [PWU99].

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

Roman [Has95].

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

ROMs [GTGW94, UFC94].

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

Roosevelt [Kah98c].

Root [Cop95c, JJ91].

Rooted [PB99a].

Rooted-Tree [PB99a].

Roots [Kob97].

Rosemont [IEE97g].

Rosenheim [Sha99a].

Rosser [Ole95].

Rotation [OP97, OP98].

Rotations [Con99b].

Rotor [Wic90, Daw96].

Rough [Mic93b].

Round [BJY97, BS93a, DP94, Dob97, GC94, Han97, KTM+99, Nat99c, SZ96, SK98c, SK98b, BD99a, NBD+99, Wer93a, Wer93b, HT98].

Round-Optimal [BJY97, DP94].

Round1 [Bas98].

Rounding [BV97].

Rounds [BB99a, dBB91, Bor95, DBR+99, KR94c, BB98a, Dob98, PNR984, d91].

Routers [DMVC99, Ano96x].

Rover [GrS96, RSG98, SGR97, CadHsv96].

Royal [Bis90].

Royal [Far93, Tw92, Don98].

RPC [SSH93].

RSA [Ano94b, Ano95f, AA99, And93, Ano95d, Ano95e, Ano95a, Ano95p, Ano95s, Ano96b, Ano97e, Ano97f, Ano97g, Ano97x, Ano97-38, Ano97-41, Ano97-39, Ano97a, Ano97-40, Ano98b, Ano99a, BTD98, BQ95b, BQ95a, BR95a, BR96c, BJQ97, Ble98a, BF79b, BDF98, BV98c, BD99b, Bon99, Bra95e, Bri90b, BM94c, Ca99, CH97b, CH98, CB96, CLE99, CMTN94, CD91, Cle96, Coo97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, Cus97, Dav95, Dem94, DDL994, DN95a, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FGMY97b, FM98, FY98b, FR95b, GJKR96b, GKR97, GQQ98b, Gill99, GM97, GTS90, Gro94, GS99b, HN98, HW96, Hor98, Hub91, HP94, IM93a, IM93b, JQ97, JQBD97, JQ98a, KR95c, Kal97a, Kal98b, KS98a, Kir95, Koc94, Koc96a, Koc95, Koc96b, Koy95, KOT95a].

RSA [KOT95b, KK96, Len98, LHL94, LL95a, Lon91, MWB99, MLY93, Mau90, MW98d, MW98c, MSS98, Mis97, Mis98, MS99c,mue99, Mii99, NS98b, NS98c, Oka98a, Oka98b, OSA91, PPK97, PP90, PW93a, Poi99, PS98g, Rab98, RS98e, RSxx, SSI97a, SSI97b, Sam98, SKNO98a, SKNO98b, SSS98, Sch94m, SPP98, Sha95b, SV93, SH99, Sil97b, Sil97a, Smi93b, TY92, Tak97, Tak98a, Tak98b, T+99, TT99, VVD90, VNM99, Ven92, Vv97, Wal99c, Way98, W99b, W99a, Wir98, XL99, YY99, Zer96b, Zhou94].

RSA-120 [DDL994].

RSA-130 [Ano96b].

RSA-Based [CD96, GKK97, VNM99].

RSA-cryptosystem [Gro94].

RSA-Implementation [PP90].

RSA-key [FM98].

RSA-keys [SSI97a, SSI97b].

RSA-Like [JQ97].

RSA-Moduli [Mau90].

RSA-signatures [Ev92].

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

RSAb [MPPS95].

RSA-Euro [Bar96b].

RTD [KW92].

RTR [KV99].

Ruby [JS93a].

Rueppel [NMV98].

Rule [PL94].

Rule-Based [PL94].

Ruling [Eri97b].

Run [DF91c].

Runtime [DF91c].

Runtime-Tunable [WF94].

Russia [CW94].

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

S-box [BD95a, SK98c, SK98b].

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

Safford [Bur98b, Kru98]. Saint [GQ95, QG95]. Saint-Malo [GQ95, QG95]. Sales [Gar97a]. Salesman [OMV98]. same [Ude98]. Samba [Bl98]. same [Ude98]. Samas [KG96]. San [AC93b, ACM99a, Ano97a, Ano98a, Com96, CMM93, FJV97, IEE92b, IEE97b, RP97b, Sch98b, SJ97, USE92a, USE96c, USE96f, USE96g, USE98d, van96, XfTnW94]. Sand [SVxW91]. sandbox [MF97]. Santa [Bri92, Bri93, Cop95b, Cop95d, Des94b, IEE97b, IEE98d, Ka97c, Kob96, Kra98, St93b, St94, USE93, Wie99]. Sannino [IEE97c]. Saragosse [Mau96b]. Sardinias [MSS93]. SASL [Mye97, New98]. SAT [McH92]. Satellite [Ano99f, Gar97a, Gar98a, Lam99]. Satisfying [Kim93, Cus96, CS96c, O’C94, YT96]. save [DF92]. Saving [Ame96b]. says [Riv98c]. Scale [SA95, SS90, She92a, FO93, OP97, OP98]. Scaling [SA95]. SCALPS [DVQ96]. scanners [Me98]. Scanning [CO98]. Scenario [AMP94]. Scene [SZT98a, SZT98b]. Scene-Based [SZT98a, SZT98b]. scenes [BDC+95, MCD98a]. SCFS [IHR99]. Schedule [KSW96, KSW99a, Kel99, MM99c, Mur99, SK98a, SKW99, WKS+99]. Scheduler [KT96]. Schedulers [CDN98]. Scheduling [KM93, Por98, SJ98, Sha99b]. Schema [Pit96b]. Schemas [Wed99]. Scheme [Int91a, ADF98, BCC93, BM99a, BM99b, BF99c, Boy90, BY92, CT97, CK95, Cop94b, DQ94, DKKK98, DN94, GKY90, GQW+91, HL93a, Hwa93, Hwa97, Ie91, IM93b, KKS97, KS98d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MSS98, My96, Mue99, Mii99, NMV98, OOK91, OOF93, Pat95, Pet98, PM99b, RGV97, Sch99, Smi90, Ver95, ZL99, AW95, BD98a, CW97, CLHL98, CC95, CLW98, CMTNY94, CG97, FOO93, FO98, GMLH94, GPS97, Gua90, Har91, HZ93, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM+94, Ku92, LW96, LL98b, LLG10, MRS99, MS98a, MLA91, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SSN98b, SVWMB95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WWH95, vT93].

Schemes [AW94, BP97a, BC93a, BDPR98, BBDW96, BK94a, BK95b, BM96b, BM96c, BDGV93, BDD+94, BFS96, BM99b, BV96, BD90, Bri90a, BS91g, BLV98, BDB92, CS97a, CM99a, CD95, Dam99a, DVW90, DMPW98, DY91e, vD95a, DFKYZ99, DL97, FDB93a, FY97, FO091, FO99b, GPSNW98, GP99, GS94a, HK97a, HK97b, IS91, JMO94, KPG99, Ki96, KMOV91, KOS+94, KOO95b, KOO95a, LH98, LM95, MH96, Mis98, MWW94, OK98, Oka93b, Pai98a, Pai98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SK93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SSN99, YLD99, Zha98, ARK99, BC95a, BR97b, BI93, BDSV93, BCDV94, BGS95, Blu95, BC96a, BCDV96, BDGV96, BMS96, BD97, BFS98, BDV98, BD98b, BDGG99, Bur96, BM94c, CDGV91, CP95, CSV94].
schemes [DP96, DF93, DDB95a, DDB95b, Des99b, FDB93b, HY93a, HMP95, HCY96b, JM93, Koy95, KO95a, KO96, KO97, LS98a, LC97a, LHL95b, LHL95a, MS98b, MPSV99, MTN97, Mu92, NR95, OK96a, OKT93, OK95, Pad98, PS98a, PPKW97, Pd96c, PS96d, RD96a, RS96b, SI93b, Sha94, Sha95a, She92g, SW98, SW99a, SS94, SC97, Tj99, Tze99, VNM99, WAMO94, ZHS94, Z98, dr94a, vD95b]. Schernes [BBCM93a]. Schnorr [DBGV93, dR94b, dR94a]. Schoof [IKNY98]. school [Duf98]. Schools [DDJ98e, DDJ98f]. Schroeder [Low95, Low96]. Schussel [Pin98]. Schutz [FT95]. Schwierigkeit [Hor99]. Science [Ano93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97, IEE98a, Ste91, Bed90, Beu94, Sch97c, Shp99a, Sim92, WS98]. Sciences [Ano95r, Tv92]. Scientific [CHLT99, PH91, GTGW94, HW91]. Scientist [BCE +94]. scoop [Ano96-30]. Scots [Sin99]. Scott [Sha99a]. Scramble [JSY99]. Scramblers [GDS91]. Scanning [CN99]. ScriptEase [Ano97-34]. Scripting [SaV98a]. Scripts [Duh90, Sch99a, IPNdbbbrpm91]. Scritchers [Dun94]; scrutiny [Den90]. SDK [Ano97-34]. SDNS [NH90]. SDSC [Sch99j]. SEA [Sch99j, GC97]. SEAL [HG97a, HG97b]. Scalability [Por98]. Sealing [GS98]. Seamless [DFGH99]. Search [ADEDS99, BD93, CD98c, HS90, KP99a, LC99, Mih94, Sa99, V93a, Wie96, Wie97, Wie98a, vW94, vW99, CR97, GLV99, Gol90c, KR96b, KM98c, Kuh98, Wie94]. Searches [PKA+98]. Searching [BP95a, DDJ98c, DDJ98f, Jia99, DSSZ99]. seasons [WSFC99]. Seattle [HF97, USE98a, USE99b]. Second [Auc98, Cha91, DEQ92, Hir98, Nat99b, ACM90, AR97, Ano99g, FR95a, IZ99, Lea90, Pre95a, Uni96c, Uni95a, USE96d, VPM97, Hin93, PH91, HK97]. secondary [Atk93]. Secrecy [Aba99, BP98c, GM90, GTGW94, JR96, Moy98, Rat96, Sin99]. Secret [AGY95b, Ano97e, BC93a, BC95b, BCG90, Ben98, Ber91, BS97a, BK94a, BK95b, BG93, BM99c, BV96, Bra95b, Bra95c, BS94, BD90, Bri90a, BS91g, Cac95a, Cac95b, CT97, CMP97, CGMW97, CK90, CFSY96, DDJ98g, DJJ98b, Dae98, Dan94b, DDP94a, DKK98, DFJ99, vD95a, EHMS99, FW91, GPSNW98, GPSN98, HL93a, HD96a, HK97a, HCS97b, HCY96a, IS91, Kahl96b, Kf96, Kra94a, KOS+94, KO995b, KO90a, LY93, LF97, LM94a, LM94b, LP99, LH93b, MSNW99, Mau93a, MW96a, Mau97a, MSN98, MSN99, MT98, Mus92, NW98, OK98, PS98a, Pui98a, Pau98b, Ped91d, Pra96, Rey96, Rey97, Rey99, Sal91, Sch99, Sha99a, Sim90b, Sim91, Sim94a, Sti93a, Van93, W99, Wie90b, Wol98, AI 96, AGY95a, BC95a, BT94, BI93, Ble96, BD95V3, BCDV94, BDD+94, BGS95, BCDV96, BG96]. secret [BD97, BDV98, BD99, Bur96, CDG91, Dal97, Dan94a, Dvo91, El97, FOO93, FO98, GM95, GPSN97, Gre90, HNSM91, Hel93, HJKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, J96, JY98, KO95a, KO96, KO97, LY93, LH95, Me92, MPSV99, OK96a, OK93, OK96b, OK95, Pad98, Ped91b, Ped91c, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, Vv97, Wie90a, WS96c, Win99, Wri98b, ZHS94, vD95b, van97a]. Secret-Ballot [CFSY96, BT94]. Secret-Key [Ano97e, Bra95b, Bra95c, LM94b, Mau97a, Van93, Wol98, LM94a, J98]. secret-sharing [DR96a]. secret-sleuthing [WS96c]. Secretly [MT94]. Secrets [Cr90, DH90, DS99, E98, HH93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, Ano91b, Baud97, BDV93, CWY98, JMO95b, WW93, Chi92]. Section [Alv98c]. Secure [AH98, AB96a, Ano93c, Ano93f, Ano95l,
Ano99f, Ano99l, Atk97, AR98, Bal99, BQ95b, BQ95a, BMM99a, BM99b, BR91, BHK+99, BDHK93, BFS96, BS95b, BS98, BM94b, CG99, Car99, CG98, Cha90, CVHP91, CR91, CC95, C99, CKLS96b, CKLS96c, CKLS97, CD95, CD96, CS98b, CDD+99, Cra99, Dam91b, Dam94b, Dy90, Dy91d, Dy91b, Dy91f, DH90, F99, FB97, FYM99, FH94, FO99b, GGMM97, GH98, Gel95, GJKR99, GHR99, Gut96, IOS94, Jac90a, Jac90b, JT97a, KR95c, KM93, KT96, KSHW97, KSHW98, KS99a, Knu94a, KP97, Kon95, KBR97, KYDB98, LY93, LM95, Mar98a, Mau90, Mau91d, Mau97a, MW97, Mos98, NIS93b, Nat95, NS98b, NS98c, Oka93b, O98a, Ped91d, P99a, PGV92, RRP97, RS96a, RIP95a, SSH93, SSI98].

[192x578]+

Secure
[SK94, SSSW98, Sas99a, Sch94a, SK98a, SM95a, SB94, SSM94, Sho96, Smi93b, Str93a, Str93b, Tay95, WP90, WD99a, WK97, Web98, Yah94, YST99a, YST99b, ZMI90, Zhe90, ZL99, Zol93, vHH97, BH93, Bea93, Bea96, BMS96, BP95b, Bow93, BM95, BD95b, CNST98, CG997, CG05, Dam94a, Des90b, DS93, Des95, DV96, FO98, GGK+99, GM95, Go90c, GBL94, HJT+96, HY98b, HY98a, HC95a, Hwa93, HW98c, IS97, IKNY98, KC95, KSB96a, Lam99, Los97, MS98b, NY90, OK96b, Opp96, Ped91b, Ped91e, P99a, R98, RR97a, Rom90b, Sar97, Sch92c, SKB97, Sim98e, Sin95, Sta97c, Ven92, YL97b, ANS97, Ano93j, Nat92b, Sta94b, Bou94].

secured [Way98]. Securely
[RB94, Bre97b, DDFY94]. SecureNet
[Ano97-33]. SecurID [Ano96x]. Securing
[Bi96, Des95, Lin96a, RG95, SG98, V98b, Ano95q, DL96]. sécuritaire [Bou94].

sécurité [Sch98c]. Security
[ACM93a, ACM94a, ACM97a, AKP96, ADDS91, ARH95, ABDV98, Ala97, And94a, Ano91a, Int91a, Ano92c, Ano93g, Ano95f, Ano95b, Ano96r, Ano96a, Ano96y, ??97, Ano97e, Ano97f, Ano97g, Ano97a, Ano97-40, Ano97-42, Ano98b, Ano98c, Ano98q, Ano99a, Atk95b, AR98, Bal99, BCCG93, Bas93, BKR94, BDP98, Bel99, BG9K9. Bel92, Ber96b, BDR+96, Ble97, BPRF99, Bov98a, Bov98b, Boy99, Bra90a, BK94b, BNP99, Com96, Com94c, CM97a, CH94a, CH97, CG97+99, CS96a, CM97b, CT99a, Chr98, CGB+93, Coh99, CNS99a, Cor99, CN99, CG05, DM94, Dan95, DS98a, Dav95, DG95, De 93a, De 98a, DDK98, Des92, Di99, Dwo95, ECM96, Elk96, EH96, FGS96, FS97b, FO99a, Fum93, Fum98b, GM93a, GMCF95, Gan96b, Gar97c, Gar96c, Gib96, Gir99, GH95, Gon98, G98].

Security
[Gu99, HHT93, HHT97, HP99a, HP99b, HSK97, HH94, HLMW93, HMWM94, Hur98, IBMxx, IEEE92a, IEEE92b, IEEE93b, IEEE93c, IEEE94c, IEEE94d, IEEE95b, IEEE96, IEEE97b, IEEE97i, ISO97, IH99a, JD91, JLO97, KY95a, KR96a, KY98, K99, Kau93, KA98b, KM96a, Klev90, KRR98, K97c, LOX99, LBMC94, Len96b, LL94a, LL95a, Lom97, Luc97, Luc98a, Luc99a, Luc99b, MMST98, Mat96a, MSK99a, MW98d, MSS98, MM98a, Mue99, Muf93, MM98b, Mt99, Mye97, NS92, Ng99, NK93, OiDF98, O98, OU98b, Opp97, PS98d, PS99c, P997, PS96d, PS99b, Rei92, RBv94, Rob93, Rob98a, Rog96, Russ90, Sch94m, Sch95c, Sch95d, SH97, Sch97a, SSv+98, Sch98f, SS99a, Sch98h, She97, SSP90, SS90, She92a, She92f, She93c, She93d, She94c, She96b, SK97d, Sun98a, Uni97a, Uni98a, Uni98e, Uni96c, Uni98f].

Security
[Uni98j]. USE90, USE92b, USE93, USE95b, USE96e, USE96g, USE98d, USE99a, Van95a, VSH97, Van98b, Van99b, Vuu99c, Ved93, Ved98a, Ved98b, VG93, Ver98a, WCS95, Wol98, Wol99, ZS93, ZFKP98, ZFK+98, v94, Awa99, Awa92a, AFB95, Ano93d, Ano95o, Ano97x, Ano98h, Ano99h, Bec97, BR96c, BCK96c, BDJR97, BKR98a, BKR98b, BBN96, B+96a, Bet95c,
BHHR99, BCW97, Boy98, Bro96, Com97, Cha95a, CP94, Chi99a, Chi99b, CJ95, Cli99, CTSxx, Dam99b, DS90a, Den99, DEQ92, D+98, FHG99, FFW99, FM98b, Fra92, Gon92, GEL98, Gmu98, HN98, HK99b, HQQ97, HS96b, Hor94, HC95a, HC95b, HY95, HLLC96, IEE94b, JT96, JT97b, JJ95, KY97, KG96, Kat97, KSB96b, KSB97, KW92, Kuh98, Lai92, LTT95, Lee95, LHW99, Len93, LC95, MW94, Mar95b, MS97, Mas97, Mau91c, MKKW99].

security [MF97, Mei94, MW98c, Nor95b, PS99d, PS99a, PS99b, PS99e, PGV93d, PV996, PR98, Q+98, RIV98c, Ros94, SSN98b, Sah99, Sch92a, SSM+97, SMD+99, She92c, Sta94a, Sta99a, Sun98b, Tay90, Tho96, TY98b, TY98a, Tsu92c, Uni98d, Uni98k, VB96, VPM97, Ven90, WBDF97, Woe97, Xie92, XL99, XZ99b, dVdV98, van96, van97b, Chr99b, Far92, Uni98c, Uni98b, UU97a, Uni97b]. Security-analysis [vT94]. Security-preserving [DI99]. SecurID [Ano97-43]. See [Web98]. Seeing [JJ98b, JJ98a, Lut98]. Seek [Gar97b, SV99a, SV99b, SVS98]. Seeks [Gar98a, Ano96g]. Seeks [Ano96g]. Segmentation [DP99, LFCK99]. Segmented [BALS99]. Segregating [Kol95]. Seizing [Kah91a]. selectable [Gon95]. Selected [CW94, HA00, TM99, Cha91, CFG96]. Selecting [Bax97, CDF95]. Selection [Hub91, Len99a, PNFK95, BM94c, Fei99, UFC94]. Selections [DKK+98, Ers99]. Selective [GM97, HV98, IS97]. selectively [WY93]. Self [AW99, BCD98, Fis98, Gir91, GPR98, KI97, LC94, Mau91a, MS95b, OMV98, SG99a, Sch99d, Jan95, MS95a, Mil96, Sch90c, Sch97c]. Self-Certified [Gir91, SG99a]. self-confident [Jan95]. Self-Delegation [GPR98]. Self-Executing [AW99]. Self-Organizing [OMV98]. Self-Reductions [Fis98]. Self-shrinking [MS95b, MS95a, Mih96]. Self-similarity [BCD98, Sch90c, Sch97c]. Self-Study [Sch99d]. Self-synchronised [KI97]. Self-Synchronizing [Man91a, selling [Bee96]. Semantic [BPR99, Mee99]. Semantics [DI99]. Seniors [Ano95d]. Semiotics [Gog99]. Senate [Uni98h, Uni97c, Uni95a, Uni98k, Uni98g, Uni98i]. send [Way91]. Sender [WP90, Wai90]. senders [HW98c]. sendmail [BRW99]. Sense [Ame96b, CC98]. Sensitivity [LvD98]. Sensors [Fuc99]. SentryLink [Ano95t]. Seoul [Ano93g]. Separability [CM99a]. Separable [LY94, AM99], separate [WY93]. Separating [MKKW99, Tou92]. September [Ano98a, D+98, ES98, FR95a, IEE96e, IEE97e, IEE97k, Kat97, LW96, Q+98, Spi95, TV94, T+98, Uni97a, Uni96c, Uni98j, Uni98k, USE92b, USE96a, USE98b, Gar98a]. seq [Chl97, UU97b]. Sequence [LY93, GM91, LY93, MHH98]. Sequences [DSV99, JQ97, MS94, Mun91a, Mun91b, PMP99, SB94, Bla94a, GN95a, Gol99c, KSB96a, MK92]. sequential [LHW99]. ser [IPNdbbpr97]. Serial [SI93a, SSG99, Yor96]. Series [Ano95d, HEQL98, CJ98a, CJ98b]. Series-Parallel [HEQL98]. Serpent [ABK98c, ABK98b, ABK98a, BAK98]. servant [CWM+91]. serve [Sch93c]. Server [Ano97-33, Ano97-34, BQ95b, BQ95a, DL99, ECD+99, HS94, HCY96a, Kon95, LY93, LL95a, MW98d, NS98b, NS98c, Oh99, SVA+98, Wat99, Ano97d, BM94c, HS96b, Hor98, LY93, MW98c, PW93a, Sin95, Ts90]. Server-Aided [BQ95b, BQ95a, HCY96a, LY93, LL95a, MW98d, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. Server-Side [SVA+98]. servers [ABK98c, AG95, CGM97b, GGK+99, Lee95, Ude98].
Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau99, MB99a, RRSW97a, RRSW97b, Ros96e, Ros96f, Ros97b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, RFLW96, Zha96, Ber96a, KN93].
Service-Level [MB99a]. Serviceability [WP90].
Services [ANS98b, Cas95, HVH98, RB94, VSH97, Vedd98a, AA95, AC97, DB90b, Don98, KW92, PS99b, You97, Zer96a, AA95, Acc97].
Service-Level [MB99a].
Serviceability [WP90].
Services [ANS98b, Cas95, HVH98, RB94, VSH97, Vedd98a, AA95, AC97, DB90b, Don98, KW92, PS99b, You97, Zer96a, AA95, Acc97].

ses [Bou94].
Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k].
Session-Layer [BB95c]. Sessioneer [AG95].
Set [DJL93, FP99, IS91, Koz96, Mei92, SPP98, Sta96b, SX90, GB98, Kra99].
SETHEO [Sch99k].
Share [BWM99b, Csi95, DDFY94, Sim90a].
Shared [BF97b, DHMR96, DF91a, DH90, HD96a, IS91, Le99b, MB99, PS98g, RZ99, SN96, Sim90b, Sim91, Sim94a, WI99, YL97a].
Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [MSNW99, BDG99, CDGV91, OK95, ZHS94].
Sharing [AGY95b, BC93a, BC95b, BBDW96, BK94a, BK95b, BDGV93, BDD+94, BM99c, BD90, Bri90a, BS91g, Cac95a, Cac95b, CG98, CT97, CK90, DDP94a, DKKK98, vD95a, DLR97, FDB93a, FGY96a, GJKR96b, GPSNW98, GPSN98, HL93a, HK97a, HK97b, Kn96, Kra94a, KOS+94, KOO95b, KOO95a, LP99, LCL92, LH93b, Me92, MS95f, MS99N, NW98, OK98, Pai98a, Pai98b, Ped91d, Rab94, ROT94, Sch92b, Sch99i, Sti93a, Wil98a, AGY95a, BC95a, BE93, BDGV93, BDSV93, BCDV94, BG98, BCDV96, BDGV96, BD97, BDV98, BD99, Bar96, CDGV91, CMPS97, CGMW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FGY96b, FR95c, FO98, GM95, GPSN97, HJ95Y95, Hwa92d, HC96, HLC99, JM93, JMO95a, JMO95b, Jar96, KO95a, KO96, KO97, Ma90, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, PS98a, Ped91b, Ped91e]. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95b, van97a, Ko95].
Shark [RDP99, WG97]. Shawn [Sha99a].
Shedding [HP98, YY98].
Shelf [Hat96, AG95].
Shell [Car99, Sch99a].
Shift [GO96b, Go94, GN95a, Go91, GO95, PS97]. shift-register [GN95a].
Shifting [LMB95].
Ship [NS98a, RP98].
Ship-Board [NS98a].
Shipping [An995].
Shooting [Ag92].
Shop [An97-33].
Shortage [DD98a].
Should [Way93c, YY96, An95c, Riv98c]. show [Mad98g].
shrinking [MS95a, MS95b, Mi96].
SHS [NS93b, Nat92b].
shu [XtTm94].
SIAM [ACM97b].
siber [An97-50].
sichere [Hor99].
Side [KSW98a, KSW98b, KSW98c, SVA+98, YY96].
sides [MB94b].
Siege [EH96].
Siegenthaler [MS99b].
Siemens [An97-47, Bro97, Dav98c, Mac98, Sel98b, TJ97].
Sieve [LLMP90, LL93a, Per93, CDEH+96, Gor93b, Pom94].
sifrovani [Gar98c].
SIGACT [ACM99a].
SIGGRAPH [ACM99c, B+96b].
Sight [Phi98].
SIGINT [Mye98].
Sign [BM92, GR97, GHR99, Web98, BR96c].
Signal [IEE97c, IEE97d, IEE97k, LW96, Pit95, She92e, T+98]. **Signalling** [Lin98].

**Signals** [AK99, BTH96, DDNM98, MMH98].

**Signature** [AA95, Acc97, AW94, Int91a, NIS94, Ano96f, Ano97-50, BP97a, BM99a, BM99b, BM96d, BM96c, Bra93a, CS97a, CM99a, CG98, CH98, CK95, CDF95, CD95, DMPW98, DQ94, DY91c, DN94, FL99a, FMY98, FOM91, FOO91, GP99, GQW+91, HJJ+xx, KKS97, KS98d, KPG99, Kob98c, Kra93, LK96, LHW98, LK99, LHL94, LL98a, MT94, MB99a, Mer90b, Mer97, MH96, MSS98, Mis98, Miy96, Mon93, Nat91, Nat92a, Nat94c, Nat94a, NMVR95b, Na97, NMV98, NMY99, NIS93a, OFF93, Oka93b, PF94, Pet98, PM98, P99c, P99b, RG97, RDK98, Riv93c, dR94b, SC96a, Sch93b, Sch94e, SK97a, SE96, Sim93, Sin98, SB93, SSN99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, AR99, La93a, AW95, Ale97, Ano97p, BD98a, Bis90, Boy97, Bur96, CP95, CMT94, CSV94].

**signature** [DP96, FR95c, Gu90, HY93a, HJJ+97, Hor98, HMP95, KS99c, LWC96, Mau91b, May97, MS98b, Mu92, NMVR95a, NR95, P96c, Pit96a, PS96d, PS98h, Si93b, Sha94, SS95b, SS95c, Ste95, Ti98, Tra97, TJ99, Wan92a, Wi93b, Wu92, XA98, YL95b, YL95a, Yeu99, Zho94, dR94a].

**Signatures** [AN98b, ASW98, AT99, BD99a, BQ95b, BQ95a, BG90, BdM94, BM94a, BM96a, BC93b, BF99, Boy98, BS95d, CHP91, CR91, CDF95, Cop99, CD96, Dam94b, DF91a, EG90, EG96, EvH91, Fro97, GKR97, GHR99, GM97, GO93, HKS95, HA96, JM99, JQBD97, JLO97, Len96a, LSV95, LR98, MS96, Mis97, MB97, NW98, O98, Oka94, PP97, PW93b, PGV93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, She97, Tra99, Web98, Wri94, vHPP93, Ano98c, BR96c, BGR98b, Ble96, BCDP91, BM91b, Com97, CPS95, Cha95b, Dam94a, Ev92, EvH93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, P99a, P96c, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].

**Signcryption** [Zhe97b, BD98a, Yeu99, ZI98].

**Signed** [Ber97a, GMCF95, KAM99, Sun98b].

**Signer** [CvHP91].

**Signers** [TJ99].

**Significance** [DFG99, SBV99, SM91, YY98a, ZIZ97].

**Significant** [BS96].

**Signing** [BGG94, GMJ99a, GMJ99b, GS98, Ped99, Ros97b, Ros98h, Ros98b, Ros96a, Ros96c, Ros96f].

**Signs** [Eri97b].

**SIGPLAN** [ACM99a].

**SIGPLAN-SIGACT** [ACM99a]. Silicon [NFQ99].

**Silicon-On-Insulator** [NFQ99].

**Silk** [Mar98b].

**SIM** [Ved98a].

**SIMD** [Cla97].

**Similar** [Per99].

**similarity** [BMD98, Sch90c, Sch97c].

**Simmons** [Des96b].

**Simple** [End97, FBS97, GGM97, Jue99, MS95f, MM94, NR98, RS96c, Rus93a, Sch99, SW94c, CH97b, RS96b, RRS98, SVV99, GM93a, Mye97].

**Simpler** [Fri92b, MTE99].

**Simplified** [CRRY99, CDS94, Rab98].

**Simplifying** [Ano96h, IR99, Sta96b].

**Simulated** [DD99].

**Simulating** [OD99].

**Simulation** [BVFD99, CM99d, Mac94, PWU99, RG99, SVBJ96, Var99a, DN95a, GO96a, LS98a, Moc97].

**simulations** [Ueh95].

**Simulator** [YHK99].

**Simultaneous** [Kwa93].

**simultaneously** [Ano96c].

**Singapore** [IEE97k, LOX99].

**Single** [ARH95, EO95a, EO95b, EM93, Lan97, VVDJ90, Wad93, Bar92a, Daw96].

**Single-Chip** [Lam97].

**Single-Term** [EO95b, EO95a].

**singular** [CLL99, Koy95, KK96].

**singularities** [TG94].

**site** [Ude98].

**Sites** [DMS95, BDC+95].

**Situation** [Bie98].

**Six** [DBR+99, Fri96, Los97, Wel97].

**Sixth** [ES98, IEE97a, ACM94c, Com96, USE96c, Kui91].

**Size** [An95a, BVFD99, DFL99, Pal99b, Ste94a, CDGV91, Csi95, OK95].
Sizes [PKA+98]. Skew [BS95d]. skill [Gre90]. Skipjack [BBS98a, Bih98b, BBS99a, BBDR99, KRW99].
[ABKL91, Ano96z, Ano99e, BE90, Bov98a, Bov98b, BDB92, Cha99a, Cha91, CM99c, Chr99a, Con98, Con99a, Cor98, CH99a, DDD98d, DDJ98b, DDJ99, Deu97, Deu98, Di 97a, DT98b, EN98, ENK99, Fan96, FGLP96a, FGLP96b, FOM91, Gar97a, GL96, GPSV98, Gt98a, HKQ99, HP98a, Hru96, HH99, Hua99, Koe99, KC97, KC97a, Mar98a, Mye96, NM96b, Omu90, PV98, Rho99, SKW+98d, SS99a, Sch90b, SR96, SGPV98, Smi98a, Sut99, Tua99, VV98, Ver98b, DWQ91b, DWQ91a, ABKL93, AHdJF97, Ake97, BG9V97a, Cha99b, CW97, CJRR99b, DS98a, Dhe98, DI 97b, DF97, Gau97, Kip97, Sha95a, TJ97, Taa98, AG99, Bak99, BF99a, Bro97, DVQ96, Gir99, GSTY96, HNS99, IW99, NFQ99, SMS94, SKAM99]. Smart-Cards [Roh99, ABKL91, ABKL93, CJRR99b]. Smartcard [Ano98q, Ano99b, USE99e, Ano97x, Ano97-47, Ara93, Ban97, Ano98p, CH94b, IH99b, KK99a]. Smartcards [Bla96a, Bla96b, Fan97, Sch90a, DR99a, IH99a, IHR99, MDS99]. SmartLink [Ano93k]. smooth [Odl94a, VZ97]. SNAKE [MSK99a]. Snesfru [BS91f]. SNMP
SOCKS [Lee96, McM96]. Soft [NS98a]. SoftID [Ano96-27]. Software [Abr97, Ano93j, Auc96, AG99, Bal97, Bih97b, BD94, CD97, Cla98a, CT99b, DBVD96, DF91c, DSB99, Gar97a, GO96a, Gt98b, HK97, J98c, KP96b, L95, Lac93, Lea99, Lut98, Mat96b, Mer91, MM97, RSA94, RC94a, RC94b, SW94a, Sch94c, SK96a, SK96b, SK96c, SW97a, SW97b, SK97c, She95b, You96, Ano94a, Ano95g, Ano96-27, Bih97c, BP97b, DH96a, Des95, Go96d, Knu99c, PA93, Pre95a, SS98a, SAM97, Str93a, Str93b, Szw97b, Vau98e, Woo90]. Software-Optimised [RC94a, RC94b]. software [MM95]. SOI [NFQ99]. Solaris [Sun91b]. SOLID [Ano97-33, CK95, Gut96]. solid-state [Gut96]. Solution [GO96c, Law98, LR98, WD98, Ano97-36, Ano98h]. Solutions [HM98, MSK99a, PW98]. solve [WSFC99]. Solved [Ano97c, Ano98i, Ree98]. Solving
[LO91b, Lew92, MSO96, OMV98, Per99]. SOM [BBN96]. Some
[Abe98b, AT99, BBL95, Bri90a, BS91g, CDG95, CRR99, CL98, Des98c, EKH91, FDB93a, Gib90, Gui97, HGHD98, Hub91, HCY96a, Knu99a, KP95, KYDB98, Las92, LP94, Lid90, MS98, OK98, Sim97, TCH+91, Wag98b, Cao99, Cha95a, FDB93b, G97c, Lan96, RD96a, SMK98b, TH99, Koo97]. Someone [MB99a]. Something [SvA+98]. Son [CFK+91]. soon [Pri94]. sophisticated [Mei98]. Sought [Ano97-45]. Sound
[CJRR99a, MGL+98, Ano96-29]. Soundness [DE99]. sounds [BC+95]. Source
[Sch94g, Sch96a, Sch94h, Zim95b, Gen99c, Zim96a, Zim96b]. sourcebook
[Ban94, Rot95a]. Sources
[ADBB99, Cor99, Uni94c]. Southcon
[IEE96f]. Southcon/96 [IEE96f]. Soviet
[COP+95a, HK99c]. SP [STP93]. Space
[AR99, BC95c, FP99, Gar97c, HBKL99,
KV99, KI96, SCG99, BBI90, Mra95, Pad98,
Sze98]. space-filling [BBI90]. spaced
[It091]. spacecraft [CWM+91]. Spaces
[BP95a, FDB93a, FHG99, FDB93b, Koz96,
Son99]. Space [Man96b]. Speake
[CFK+91]. Span [BDS98, DQ94, HL93a, VBD99].
Spanning [Aga92]. SPARC [Sun91b].
Sparse [LO91b]. Spass [WABC99].
Spatial [DSSB95, DDQM98, LLB98, MCD98a,
NP98b]. Speakeasy [LU95]. speaking
[LC95]. spearhead [Ano98q]. SPEC
[DDJ98a]. Special
[vD97, FT99b, MDP94, SS99e, SS99f].
Specific [ADBB99, EvH93, Kha93, LMS97].
Specification [GFB93, HJTW99, LL97a,
Ou99, SW94a, Tou92]. Specifications
[KS98a, Nat92b]. Specified [Gui97, HCC98].
Specifying [SW94a]. Specs [Got99].
Spectral [WF94]. Spectrum
[CKLS97, She94c, CKLS96b, CKLS96c,
Dix94, KSB96b, KSB97, LLB98, OP98].
Speech [DMMF97, Er97b, GDS91, IEE97d,
IEE97e, Lud97, SW95b, All97, CW94].
Speeches [Bar94]. Speed
[ARV99a, ARV99b, Ano99c, Ano99f, DP98a,
DP98b, Ebe93, FVA99b, IM93b, Koc94,
LS97, MPPS95, SKNO98a, SKNO98b,
SW97a, SW97b, She92d, She95b, IM93a,
Kap98, KAK96, Lam99, Nor95a, HKSW98,
HKR99, Zhe97a]. Speeding
[ADEDS99, KT93, McK99, Tes98]. speedy
[An99e]. spi [AG97b, AG97c, AG97a].
Spiculated [ZTR99]. Spin [RK99]. Spite
[Wai90]. SPJ [TLS99]. SPLICE [HC95b].
SPLICE/AS [HC95b]. Split [Coc97].
Splitting [Sga91b]. SPM [CV93]. SPN
[Kob99]. SPN-Structures [Kob99].
Spoofing [SVW91]. SPRC [Wol93b].
Spread [CKLS97, Dix94, She94c, CKLS96b,
IND99, JO97, Jia99, KI99, KW99, LMP99, LW95, LC99, MGL+98, MKL99, MR95a, Mar98a, Mau97b, MTV92, Mon93, NM99, NS98a, Nec96, PR99, PS99f, PK99, Rei92, Rus90, RH99, SYM98, SSS98, Sam98, STSW99, SCT99, SK96b, SK96e, Sch98f, SS90, SM99, SKT99, Tro93, Tun99, Var99b, WHFG92, WABC99, WW98a, WBB99, WABL94, ZK96, ACC99, Ano96h, BBCP98b, Bax97, BMP97a, Bur94a, BD95b, Car94, CB96, Cus95, DSSZ99, Des95, DH96b, FM98b, HN94, HI97, Hwa92a, HC95b, KM98b, Kum97, LC96a, LCL95, MY93b, MKKW99, Mey97b, MM95, Oel97, PS99e, PSW95, Sch99j, SY96b, SS95b, SS95c, TCH91, TC91, Ven90, WSFC99, WABL93, ADDS91, Ano91a, Bax97, Bel92, Dan95, JD91, RC95, YKY99, ZHJ98.

Systematic [BGH91, Zav99, Men95b].
Systematising [MKL99].
Systeme [BGH95b].
Systems [ABLP93, AKP96, AKF94, Ako99, Ano94k, Ano95a, Ano96a, ADEDS99, AA97, AMP99, BDPSN95, Bar99, Bas93, BR91, BBD97, BFN98a, CF95, DDJ98a, Dan91b, DFTY97, DY91a, DD99, DB96, ENK99, FJP96, FY95a, FY95b, FYM99, FOO91, GL96, GFB93, Gl98, GM90, GMW91, GK96, GS97, GV98, HG98, HJJ+97, HH94, HP98b, IEE93a, IEE96b, IEE96d, IEE98e, IEE99b, IHH99a, KV96, Koc96b, KA99, KY92b, LO91b, LQR98, LAB92, Lau99, Lee99b, Mar99, Mas99a, MS95f, MDP94, Mu93, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PS991, Pin97, Pit96b, PM99a, PD99b, RBv94, RG95, RPP95a, ST94, SN96, STS99b, DY91c, SOOS95, SS90, SH92a, SY92, Stu99, Tra99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a].

Systems [WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFKP98, ZFK+98, AR99, AHdJJ97, AMS96, AM99, AC97, BY93c, BY93b, BG96, BP95b, CG95, DM9W94, Dix94, Fri92b, Goo96, GKS97, Gr98, HJJ+97, IEE97k, KG96, KP99b, LM98a, LBW91, LS98a, Lie93, MSN97, NIS92, Oht96, Ole95, Opp96, PAK98, PA98b, PP92a, PP92b, PP95b, PP95a, RO96, SKB97, SY96b, SG96b, SK97d, STA97a, STA94a, Sun91b, VP98, WH92a, WH92c, ZG96, DQV96].

Systolic [SS98, DF92, PB9M90].

T [YT96, PDGI99].
T-Team [PDGI99].
T52 [Dar98c].
T52e [Sel98b].
Table [KMKH99, Has99, Hor95].
Tableaux [Mas99a].
Tableaux-99 [Mas99a].
Tables [DRR95, JC98, IPN9bbpm91].
Tactical [IKM99].
Tagging [Lud97].
Tailoring [CG99].
Taken [GQQ+91].
takes [Szw97c].
Tale [Kal98e, RS98f].
Talent [DDJ98b, DDJ98f].
Talk [Deu97, Lei99b, Wat99, BS91c, Sim91].
Talking [HH99].
Tamper [Ano96c, BDHJ98, KK99a, Zhe95b].
tamper-proof [Zhe95b].
Tamper-Resistant [Ano96c, KK99a].
tamperfree [Hwa92b, Hwa92e].
Tampering [CL98, CL97b].
Tanka [Hwa92a, MS98a].
Tandatangan [Ano97-50].
Taos [WABL93, WABL94].
tapestry [MB94b].
TAR [Ano97-33].
Targeted [Cap94].
Targets [Lea99, Way98].
TAS [Cop94b].
Tasty [Sch98].
Tate [FMR99].
Taxing [Gar97c].
Taxonomy [DB96, GS97, LBMC94].
TC [MB99b].
TC11 [Kat97].
TC6 [Kat97].
TC6/TC11 [Kat97].
TCFS [Man97b].
Tcl [GA98].
TCP [Ano96j, Fei93, Fei96].
TCP/IP [Ano96j, Fei93, Fei96].
TEA [KSW97a, KSW97b, NW97, WN95].
TecApro [GLC98].
Technical [Ano95e, Bar96b, CFK+91, CYY98, DS97c, Lan98, LM93c, Mos98, USE95a, USE99d, VG93, SM99, USE96f, USE98c].
Technique [DDNM98, Gue98b, KP93, WD97, BCV97, ONT98, Way95].

Techniques [Int91a, BGML96, BWM98, Bol98a, Bol98b, BLM04, CM97b, CD99, CMYY98, Dam90a, Dam91a, Dav91, DC98c, De 95, Des98a, Des96a, Fun97, Fun98c, GQ95, Hel94, JJJ99a, LvdLB96, MM99a, MSEN99, Mau96b, PS98e, PS98f, PK99, Pre93b, QV90, QG95, Rue93, S293, Car98, Cra96, Hel93, Hel98b, ISO97, Kay95, KG93, Nyb98, OPH+99, Ok096, PS99d, SD97, Ste99b, Way91, Woo90, ZH93, van96].

Technological [UFC94].

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

Technology [Int91a, Ano96-29, Ano96-30, Ano98t, AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, II96, IEE94a, IEE98d, Lic94, Lin93c, NFQ99, Riv98c, USE99c, Ano93a, Ano96u, DS97b, Gil97, ISO97, Ri96, Ros94, Sav96, Smi97a, VB96, CFK+91, Ers99, Ano99b].

Telecollaboration [Fuc99].

Telecommunications [IEE97e, UN94, Mac98]. Telematic [Ano97-50].

Telecomputer [Ano97-50].

Telephone [Gar97a, Sha97].

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

teletype [Mac98].

TELNET [SH93, Ala93b, Ano95w, Bor93a, Bor93b, Bor93c].

Temporal [KV99]. Temporary [KRJ98].

Tennessee [IEE94e].

TeraSpell [Ano97-34].

Term [EO95b, CHN97, EO95a].

Terminal [Con98, Con99a].

Terminals [Ano99f, ADSW99, Lam99].

Terminology [F96a].

Ternary [PKA+98].

Terrorists [Uni98j, Uni98k].

Terschelling [TV94].

Tesla [Ano97-37].

TESS [Dan95].

Test [DS97a, Law98, MOP91, SS91, DL93, Graxx, Gre90, ZY90].

Testing [Bas98, Bro94, De 99, MPPS95, Sot98, SB99, SY98, Wal99c, ARK99, Ano97-42, GKL99b, Len90, Yan95].


Tetherless [Law98].

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

Text [Bar93a, Bar93b, Ca96, CD97, LM98b, PF94, PBG90, CF9K+91, Sab94, SH98].

Textual [JKVP99].

Tejus [NM99].

Theft [Gur97].

Their [BK95c, BL96b, BL96a, Con99b, GPT91a, GPT91b, GM91, J196, K196, Len99b, O090, SY96a, SG99b, Tra99, VDD99, AA99, BS98b, BS98a, BY93c, BY93b, Car98, DDB95a, DDB95b, Don98, Eng99, HMP95, KT91b, LN94, LM96, NM96b, SS98, SI93b, TY92, YY98a].

them [Way95].

theme [IEE97k].

Theorem [AA93, FK99, GPS98, HB99, DdD99, SG99a, WW95].

Theoretic [Buc91a, C99, Cle91, MW96a, Mau99a, Mau99b, MO99, Ped91d, PB99b, STR93, W098, AP993, Kos97, Ped91b, Ped91c, S99a, S99b, S99b].

Theoretical [S97, van97a].

Theoretically [AR99, MA97a].

theories [T+98].

Theory [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, Ber96b, BMP+97b, Car97b, CF9+91, Dam90a, Dam91a, Dav91, De 95, DSB99, Fun97, GQ95, Hei96a, Hei94, IE94a, IRM93, IZ98, IZ99, K196a, K99a, Kob94, LO99, LABW92, LW91, MA96b, MA96a, MD94, N94, NC97, OD998, PSN95b, PG90, VQ90, Q95, R93, S93, Ada91, AAPS92, At99, CS97, CF96, Cou99, Dam99b, DX91, G97c, G97, GS94b, H94, Lag90, LABW91, Lo90, M98a, MA96b, MCC90b, M92, NY98, P90, R90, Sch93a, Sch90c, Sch97c, S99a, S99a, Ste99b, Sti95, Tat98, Tat99].

There [R96, Zha97, Way93b].

Therefore [FJM+96].

these [Ano98q].

They’re [W94].

Third [AAB+97, Fra99, MKS99, RS98b, SPI95, Uni95a, ACM91, GS94b, GK95b].

Third-Party [AAB+97].

Thirteenth [IEE94f, USE99b].

thirtieth [ACM98b].

thirty [ACM99b].

thirty-first [ACM99b].
Ano91a, JD91]. Transactions [FL99b, FKMY98, SSG99]. transcendental [PGCSN96]. Transcript [BD99a, Chr99a, Sas99a].
Transcript-Irrelevant [BD99a]. Transfer [Ano97-34, DF99, HHY93, NP99, RS96a, Bea93, BM90, BR96b, DOR99, Jae90a, Jae90b, SF93b]. Transferable [Sak96].
Transfered [Uni97d]. Transferring [SI94]. Transcript [BD99a, Chr99a, Sas99a].
Transform [Boy99, KMS95a, KMS95b, Kuo90, MS94, Riv97c, WF94, TKS98]. Transformability [MSO96]. Transformational [Zwi98].
Transformational [Zwi98]. Transformations [BDFM99]. Transfusion [ADBB99]. Transient [BDHJ98, CH94a, JQBD97]. Transistors [CWM+91]. Transition [Des98a, DR98b].
Translation [CFK+91, OP97, OP98]. Translucency [BR96b]. Transmission [NHB98, PSB97]. transmitting [CLI97, CLI99, UU97b]. Transparent [Bla93, DSN97c, Mau97b, SZT96b, ZG96].
Transport [Ano94b, BWM98, GBC93, Sar97]. Transportation [BPR99, UT98]. transposition [Bar92a, Bar95, GSN94]. Transputer [GN95b]. trap [YU92].
trap-door [YU92]. Trapdoor [Gib91, Gor93a, Pat99]. traps [Sch98e]. Travel [Sav97]. Traveling [OMV98, RS99a]. Transoars [Yun97]. treaties [Des90a].
Treatise [Tur99]. Treatise [Yun97]. treaties [Des90a]. Treatise [Tur99]. Treatment [BFN98b, Mau96a, O098, BDJR97, BFNO98a, Gen99c].
TREC’98 [LM98a]. Tree [BM96b, BM96c, GM99b, PB99a, LL93b, O’C95].
Tree-Based [BM96b, BM96c]. tree-structured [O’C95]. Tree-Width [GM99b]. Trees [AGA92, BP97a, HS90, ZW99, SSM92].
Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98e, DDJ98f, De 93b, De 98c, Hru98, EEE97k, Kan96, LM98a, MB99a, Koo97, Seg92]. Trial [Mye96].
Trials [CY992, PP96b, Ano93a]. Triangular [Por98]. Tribulations [CY98]. tribute [UNI92]. Trinity [IEE97a]. trip [CUR98].
Triple [Ano95p, Ano96c, Ano96-28, Bih96, BK98c, Bih99b, CJ95, HP99a, HP99b, KUS99, KUM98, LEC97, Mey97b, Per91, vOW91, JZ99, KSW96, ROT97, MEY96b].
Triple-DES [Ano95p, Ano96-26, BK98c, KUM98, KSW96, ROT97, MEY96b]. triples [CS97]. Thremiemius [Ree98]. Trojan [Sch99f]. True [Way91]. Truncated [KRW99].
Trunk [UNI94a, UNI94b]. Trust [Ano99j]. BPK99, BFK99, LA98, MR98, Re96, SA95, Sim94a, STA95a, YKB94, YY96, AHDF97, BH98, Com97, Chi99a, Chi99b, LN98]. Trust-Based [YKB94].
Trusted [AAB+97, Ano97d, IS91, MKS99, RS98b, SK97c, SS99e, SS99f, CGM97b, HY93a, JMO95a, LWC96, Ped91c, Wu92]. Trustee [Jue99].
Trustworthy [Fri93, Pos92]. Truth [For99a]. Try [Rot97]. TSP [Luc95]. TTP [BDHJ97]. TTP-based [BDHJ97]. TTPs [LAG98].
Twelf [PS99f]. Twenty [Ano95r, Bon99, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, GOL97]. twenty-eighth [ACM96b]. twenty-fifth [ACM95].
[Gar97a, Gar98b]. **Update**
[Ano94j, Ano95a, Ano95b, Ano95u, Ano96-28, Ano97c, Ano97-44, Ano97-45, Ano98r, MGL+98, Mey97b, Pin98, Ros95b, Ros96d, Ros97b, Ste99c, Wie97, Wie98a].
**updated** [Ano97-37]. **upon**
[BMP97a, CCH98, LCL95, SPP98]. **Upper**
[Fe r98, A l96, O94]. **Urge**
[GB98]. **Urgent** [Pra96]. **URL** [Zuk98b]. **USA** [???90, Ano98n, AA97, Auc98, Bri92, Bri93, Cop95d, Des94b, Han99, HF97, IEE97, IEE97c, Kal97c, Koh96, KP99b, Kra98, SJ97, Sti93b, Sti94, USE91, USE93, USE94, USE95b, USE95c, USE95a, USE96f, USE99a, USE99b, USE99c, USE99d, Wie99]. **Usability** [WT99, CG05]. **Usage** [End97]. **Use**
[ADBB99, BCE+94, Bra90a, CFGS99, Con99b, Gan96a, Gar97a, Gar97b, GC97, GK98, HJL99, Iss90, KR95c, Koh90, Lan99, MG98a, MG98b, Por91, Rud91, SB94, Zuk98a, BDH97, BR97b, Cha94b, Cli99, CG05, Gil97, Joh90, Ril96, Way93c, Zer96a]. **Used**
[GS94a, SZ96, Car97c, Car98, Gau97, Kuk99, Sch91b, SX90, van97a]. **USENET** [Bi91]. **Usenix** [USE99d, Com96, Ros96a, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c]. **User**
[AKF94, BE90, Bu96, Dra99, Gog99, Gol90a, GN95b, IS99, KCCT94a, KCCT94b, PMP99, RR99a, RR99b, SYM98b, SYM98c, S ST97, Web99, Zim95a, Ano95o, DF91b, MC96, Mu92, RSA94, RT93, SJS98, St 95b]. **User-Centered** [PMP99]. **User-Oriented** [AKF94]. **Username** [Le96]. **Users**
[Ano96-31, Hel98a, WK97, Sha97, Sta94a]. **Uses**
[Sw97, Ano97x, DKR97b, Sch99g]. **Using**
[ANS97, ANS98b, Ada97a, AGS97, AHdJF97, Ano99i, BDPSNG97, BCK96, BBS99a, BFP99, BW98, CIBM99, CK95, CM94d, Des96a, DS97d, EST99, FVE99, FW91, FY98b, GM97, GACDAFC99, GS99a, HNSS99, HRVV99, HJPB97, IR99, JM99, JJ98c, JQ97, KR94b, KS99a, KA99, KT93, Lon92, LF99, LML98, Low96, LW99, Lud97, MAM95, Mih94, MCD99, Mis97, MFG95, NT99, NHB98, NNEK97, Oh99, OOK91, Ou99, OMI93, PSE97, Pin97, PZ98, PJ99, QQ90, RB99, SG95, SK94, Sas99a, SK96a, SK97b, SK97a, SK97c, SD99, SRY99, SR96, Sim94d, SHK99b, Sun91a, SZT98a, TAP90, TA92, TYD99, TOU94, VN94, WKG97, WCSS95, Yam98b, Yam99, YST99a, YY97a, YST99b, AA95, All98, Ano97y, Ata94, BSNP96a, BSNP96b, BTD98, BGR95, BJR93, Bih94a, BB95a, BBS98a, BD95a]. **using**
[CW91a, CNST98, CC95, CGM97b, CPPK98, CB96, Cle96, Dan97, GK99b, GBL94, Gor93b, Hor95, ISO97, Jak95, JM96a, KR95a, KC95, Kar96, Kay95, Koc95, KH97, KH98a, LC96b, LC96c, LMBO95, MHPS96, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SSM94, SD97, Su98, SZT98b, SZTB98, Tak97, Til98, VZ97, VP98, Whi93, Wil93a, Y m9a, Zhe99, dR95]. **Utah**
[USE95b]. **Utility** [Zol93, Ano97m, Vu95]. **Utilization** [GRB99]. **Utilize** [MSO96]. **utilizing** [SW95a].

**V** [IEE92a]. **V1.0** [Lim99, RSA99a]. **v2.0** [Ano97-33, RSA99b]. **V32bis** [Ano93k]. **V5** [IH99b, KN93, Lee96, Ts’97]. **Validating** [Gal90]. **Validation**
[DDNM98, GS99a, RB99, Ste96, CM96]. **Validity** [GMW91, Kuk99]. **Value**
[Ack98, Eve98, Oke97, SPP98, Tay94]. **value-adding** [Eve98]. **Valued** [KW99].

**Values** [GS94a, Tho96]. **Vancouver** [Yua92]. **Vanstone**
[Kie98, NS97c, NS97b, Sha99a]. **Vaporware**
[DDJ98e, DDJ98f]. **Variable**
[BR99a, BR99b, DW94, GK95b, Sch94b, Su98, TN96a, TN96b, ZPS93]. **Variable-Input-Length** [BR99a, BR99b]. **Variable-Length** [Sch94b, Su98]. **Variance**
[Kas96]. **variant** [TC97]. **Variants**
[CRRY99, MSS98, RS99a, Sha95a].
variation [CCN95]. variations [Zho94].
varieties [Fri92b]. Various [GQW91].
Vasculature [BALS99]. Vatican [Alv98a].
Vector [ADEDS99, TK99, TYD99, CCH98,
MTN97, Pad98, dR95]. vectors
[LM93c, Mat91, MLA91]. Vegas
[ACM95, AA97]. Vehicle [CKN99].
Vendors [Gar97a, Gar97b, Gar98a, GB98].
Venon [HK99c, Pea97]. Venona
[HK99c, Pea97]. Ventura
[Nat98, RD99a]. Veri [SY99].
Verifiable [JMSI96]. Veri-KoMoD [SY99].
Verification [Abe98a, AB97, BGR98a, Bol98b,
CDFI95, DDF97a, GFB93, GS99a, HL92,
MM99a, Na97, OM93, PM98, PV98,
SM95a, SY99, Tou93, WW98b, YYY99a,
Ano97b, BGR98b, Bol97, BS95c, CM96,
Des90a, Dwo91, JC98, JW01, Mea95, Sha97,
YL95a, YM98, ZL99].
Verifier [JMSI96]. Verifiers [PM98].
Verify [DS97d, Chi99a, Chi99b].
Verifying [LHB96, Sal91, DN95b, Pau98].
Verlag [Hat96]. Verlässliche [BGH95b].
Vermont [IEE96a]. Verschlüsselung [MPS94].
Verschlüsselungssysteme [Wal98].
Verschlüsselungsverfahren [Ger97].
Version [Ano97-33, Ano97-34, BC93a,
BP998e, DBP96, FKK96, Gar97b, Kal98f,
Kal98c, Kal98d, Kal98b, KS98a, RSA93f,
Lim99, MT99a, MCM96, RSA93a, RSA94,
DY91c, SS99b, SM98b, WABC99, CLW98,
GM93a, Gih95, Bol93b, Lin96b].
Versus [MGL+98]. Vertraulichkeit [FT95].
Very [HMV93, MSD90, PF94, Yua92, SN94].
Veto [OK99a]. VHD [Oel97]. via
[BR96b, BCKxx, BM95, BS95d, DS90a,
DN95a, DN93, EPR99b, EPR99a, Fuc99,
HS94, JJ99b, NW98, UFC94].
Vibrations [NAS94, NA95].
VICS [Uni96a]. VICTOR
[OSA91]. Victorian [Abe98b]. Victory
[Mus92]. Video [Ano99f, BF999, DLF97,
DS97c, DSS98, HG97c, KBR97, KH98b,
LT98, MT94, SJ97, SB98, SQT98a,
WKH97, WW98a, ZL99, BB90, BCB97,
CPO+98, CHO+98, CKLS96c, DS97b, HG96,
HG97e, HG97d, HG98, HW97, HW98a,
Lan99, Oht96, QN98b, SH98, SQT98b].
Video-based [WKH97, BCB97].
Video-Steganography [MT94]. Vienna
View [CK95, Lan98, MUSM98, MM96a, STP93,
Ste91, ZL99, Ano97l, Pri94, UU97a, Wad93].
Viewpoint [Len96b, Ste91]. Views
[DDJ98e, DDJ98c, DDJ98f, DDJ98a,
DDJ98d, DDJ98b, DDJ98g, DDJ98h,
DDJ99, Eri97b, TLS99]. VII [IEE99b]. VIL
[AB99a, AB99b]. VIL-MACs
[AB99a, AB99b]. Village [Ber97b].
Vinegar [KS98d, KPG99]. VINO [DW94].
Virginia [ACM93a, ACM94a, EIE94a].
Virtual [DFGH99, GB98, HL99, CCH98, LS98a].
VirtuFlex [Ano97-34]. Virus
[BGG95, Hig97b, Nac97, LFSY94, OY91].
Viruses [Hig97a, Wh90, Coh94]. VIS
[BGH95b]. Visa [Lea99, Gau97]. Visibility
[LE99]. Visible [K196]. Vision
[CK99, HCDC99, PJ99, SW95b, SKIT99,
CS99, RP97b]. Vision-Based [SKIT99].
visit [QJ98a]. Visited [FY95b]. Visual
[ABDS96, B+96b, BD98b, DDGM97, Dro96,
HK97a, HKS97b, JKVP99, K196, NS95,
NP97, PKA+98, P98, PNFK95, Sha98,
Sti98b, BW97, Ger99b].
Visualisation [MM99b].
Visualization [Jan99, PH91, GTGW94].
Visual [BW98], VLDB [Yua92]. VLIW [Cla97].
VLSI
[CM99, Mas91, Pai96, Pos98, Vad95, Zim99].
VoD [GMDS98]. Voice [CM97b, MB99a,
Sha97, Cha94b, Int91b, PW98].
vol
[Ano97-48]. volume [Kat97]. Voting
[Boy90, JT97a, Mv93, NR94, SK94, SK95,
REFERENCES

X [Ano95x, Bel92, BALS99, KSW97a, KSW97b, Smi98b, Yu94a, Yu94b, PvO95].
XOR [BGR95]. XTEA [WN98a]. Xu [Ng99].

Y2K
[Ano98t, DDJ98b, Eri97b, Law98, MGL*98].
Yaksha [Gan96b]. Yarrow [KSF99, KSF00].
Yarrow-160 [KSF00]. Year [Sch95a, Sil99, Roe95].
[Bon99, Yin97, BC96b, CWM*91, Den90, Gol97c, Mar96, Mey97a].
yi [LPNdbbbrpm91]. Yield [GMW91].
Yokohama [Iz98]. York [IEE99a, USE95c].
Yu [BY92]. YY [Nat92b].

Y [Mau91b]. Z [Mau91b]. Z80180 [Kal93b]. Zero [BG90, BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOVY93, NMV99, OQ90, RS91, Si93a, BOGG*90, BBP95a, BBP95b, DF93, DP94, DF91b, Sah99].
Zero-Knowledge [BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GO93, HT98, NOVY93, NMV99, OQ90, RS91, Si93a, BOGG*90, BBP95a, BBP95b, DF93, DP94, DF91b].
zeta [Kob91c]. zeta-polynomials [Kob91c].
Zhang [JW01, Ng99, GP99, LH98]. Zhu [Ng99].
Zimmerman [Ros95a]. Zimmermann [Ros97a, Ros96c].
Zinc [RK93]. Ziv [Mun91a, Mun91b].
Zn0* [Boy97].

References

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

Anonymous:1997:ACC

ANSI:1988:FIE

Anshel:1993:PMT

ANSI:1995:ANS

**Arabnia:1997:ICI**


**Abdikalikov:1999:ERC**


**Abelson:1997:RKR**


**Almgren:2000:HWC**


**Andrasiu:1992:NCB**

Asmuth:1981:EAC


Anderson:1996:TPP


Anderson:1996:TFN


Ayadi:1997:VCP


An:1999:CVF


An:1999:CVM

Abadi:1999:STS


Anderson:1998:NFA


Ateniese:1996:CBV


Aiello:1998:SAC


Abe:1998:UVM


Abeles:1998:SVP


Abe:1999:RDM

REFERENCES


[SAB97] Susan Abraham. Software encryption export policy analysis. Thesis (B.A.), California Polytechnic State University, San
Auyong:1997:ASC


[AC97]


[ACC99]

An:1999:ODR


[ACC99]

Angelo:1994:DFS


[ACD94]

Alexi:1984:RRB


[ACGS84]

Alexi:1988:RRF

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


[ACM:1982:PFA]


[ACM:1983:PFA]


[ACM:1985:PSA]


[ACM:1986:PEA]


[ACM:1987:PNA]


[ACM:1988:PTA]

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


REFERENCES


REFERENCES


ACM:1997:PEA
ACM:1998:PTA
ACM:1999:PPA
ACM:1999:PTF
ACM:1999:SPCd


AD99


Ajtai:1999:PKC

Ahlswede:1981:BCG

R. Ahlswede and G. Dueck. Bad codes are good ciphers. Report, Universität Bielefeld, Bielefeld, Germany, 1981. Submitted in Nov. 1980 to the proceedings of the International Colloquium on Information Theory, to be held at Budapest in August 1981.

Adamek:1991:FCT


Adam:1992:DSC


Adams:1992:IAB

Adams:1997:CSC


[Ada97a]

Adams:1997:RCE


[Ada97b]

Adams:1998:CSA


[Adeeds99]

Achour:1999:UUK


[ADBB99]

Areces:1999:PRR


[ADD99]

Abraham:1991:TSS


[ADDS91]

Appas:1999:SVS

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

retrieval systems. Lecture Notes in Computer Science, 1611:205–??, 1999. CODEN LNCSBA. ISSN 0302-9743 (print), 1611-3349 (electronic).


Apostolico:1984:PMM

Apostolico:1985:CAW

Anderson:1995:SFS

Abadi:1997:RAC

Abadi:1997:CCPa

Abadi:1997:CCPb

Abadi:1998:BMCa
Abadi:1998:BMCb


Aura:1999:SLM


Agarwal:1992:RSO


Atkins:1995:MWS


Agnew:1987:RSC


Agnew:1988:RSC

REFERENCES


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


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


Aljabri:1996:UDU


Alabbadi:1993:IEC


Alagappan:1993:RTA


Alabbadi:1997:SCH


Alberti:1470:TC


Alexander:1945:CHG


Alexandris:1992:FMC


Alexandre:1997:BSC

Alexandre:1998:JBP


Allen:1997:DEC


Allen:1998:SUM


Ahituv:1987:VAI


Aiello:1998:FDI


Alvarez:1998:FLV

REFERENCES


Anderson:1997:CNK


Atanasiu:1999:ASE


ACE:1981:RPC


ANSI:1983:ANS


ABAECITC:1995:DSG


ABAECITDISC:1996:DSG


Ames:1996:SDM

REFERENCES


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

**Anderson:1995:RPP**


**Abadi:1996:PEP**


**Andrew:1986:CSI**


**Anderson:1993:PRT**


**Anderson:1994:FSE**

REFERENCES


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

Anonymous:1960:CNH

Anonymous:1976:CCA

Anonymous:1978:CSD

Anonymous:1978:NPAd

Anonymous:1978:ODA

Anonymous:1979:SSA

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

113

Anonymous:1981:CHP


Anonymous:1981:GIU


Anonymous:1982:BRCa


Anonymous:1982:CC


Anonymous:1982:ESS

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

Anonymous:1982:NNPa


Anonymous:1984:BRP

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

**Anonymous:1984:ESC**


**Anonymous:1985:BM**


**Anonymous:1985:DEA**


**Anonymous:1986:MM**


**Anonymous:1986:CPC**


**Anonymous:1986:RE**

REFERENCES


Anonymous:1987:EVE


Anonymous:1987:HSE


Anonymous:1987:MAU


Anonymous:1987:TWP


Anonymous:1988:BRCb


Anonymous:1988:CCJc


Anonymous:1988:CCJb

Anonymous:1988:DEK


Anonymous:1988:EVE


Anonymous:1988:ERH


Anonymous:1988:PED

REFERENCES

Anonymous:1988:RIA

Anonymous:1989:SZS

Anonymous:1990:SEL

Anonymous:1991:ESS

Anonymous:1991:FFL

Anonymous:1991:FFl

Anonymous:1991:AUd

Anonymous:1992:DES

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


REFERENCES

1993. CODEN DTMNAT.
ISSN 0011-6963.

Anonymous:1993:WND

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

Anonymous:1994:CNc


Anonymous:1994:DAX


Anonymous:1994:ERB


Anonymous:1994:GSK


Anonymous:1994:ICI


Anonymous:1994:Kee


Anonymous:1994:Lba

Anonymous:1994:LI

Anonymous:1994:PRP

Anonymous:1994:UC

Anonymous:1994:WAS

Anonymous:1995:AUM

Anonymous:1995:AULa

Anonymous:1995:AULb
[Ano95c] Anonymous. An E-mail encryption standard should be in place by April, providing for the incorporation of Privacy Enhanced Mail into the MIME standard. Open Systems Today, 16:2:26–??, February 1995. ISSN 1061-0839.

Anonymous:1995:ARLa

Anonymous:1995:ARLb
REFERENCES

Anonymous:1995:ARD


Anonymous:1995:DAS


Anonymous:1995:ENa


Anonymous:1995:ENb


Anonymous:1995:EEW


Anonymous:1995:ENE


Anonymous:1995:FSH


Anonymous:1995:FRE


Anonymous:1995:HPE

REFERENCES

Anonymous:1995:RLM


Anonymous:1995:SDE


Anonymous:1995:SUE


Anonymous:1995:SEE

Anonymous:1995:TEV


Anonymous:1995:XAV


Anonymous:1996:NIS


Anonymous:1996:RF


Anonymous:1996:ADX


Anonymous:1996:BCU


Anonymous:1996:CED


Anonymous:1996:CID

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


Anonymous:1996:CCC


Anonymous:1996:CSIa


Anonymous:1996:CPD


Anonymous:1996:EME


Anonymous:1996:EBS

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


Anonymous:1996:ERK


Anonymous:1996:ERM


Anonymous:1996:EKE


Anonymous:1996:ECC


Anonymous:1996:FDC


Anonymous:1996:GPT


Anonymous:1996:HET

REFERENCES

Anonymous:1996:LAW


Anonymous:1996:SCG


Anonymous:1996:SAS


Anonymous:1996:SUS


Anonymous:1996:SAO


Anonymous:1996:TBAa

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


Anonymous. Announcements: In this issue: The
REFERENCES


**Anonymous:1997:ARDa**


**Anonymous:1997:ARDb**


**Anonymous:1997:ADF**


**Anonymous:1997:BUF**


**Anonymous:1997:CFG**


**Anonymous:1997:CKG**


**Anonymous:1997:CVC**

Anonymous:1997:DEU


Anonymous:1997:DHE


Anonymous:1997:DNH


Anonymous:1997:EAS


Anonymous:1997:ENa


Anonymous:1997:ENb


Anonymous:1997:ENc


Anonymous:1997:EAJ


Anonymous:1997:ECR

Anonymous. Encryption compromise on rocky


Anonymous:1997:MNL


Anonymous:1997:MLE


Anonymous:1997:MEP


Anonymous:1997:NPP


Anonymous:1997:NPA


Anonymous:1997:NPNb

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

Anonymous:1997:PEH

Anonymous. PGP en-
Anonymous:1997:RAJ


Anonymous:1997:SAP

Anonymous. SecurlD authentication protects corporate information. *Net-
REFERENCES


Anonymous:1997:SUE


Anonymous:1997:SSA


Anonymous:1997:CBP


Anonymous:1997:TER


Anonymous:1997:UUS

REFERENCES


[Ano97-51]

[Ano97-52]
Anonymous. USACM participates in protest against restrictions on cryptography research and development. *Communications of the Association for Computing Machinery*, 40(11(S)):5–??, November 1997. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

[Ano97-53]

[Ano98a]

[Ano98b]

[Ano98c]

[Ano98d]
Anonymous:1998:CASb


Anonymous:1998:CASa


Anonymous:1998:CDR


Anonymous:1998:CSCb


Anonymous:1998:ICS


Anonymous:1998:EN


Anonymous:1998:EWB


Anonymous:1998:Ea

REFERENCES

Anonymous:1998:LEE [Ano98m]

Anonymous:1998:PCA [Ano98n]

Anonymous:1998:SEF [Ano98o]

Anonymous:1998:SIC [Ano98q]
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 [Ano98s]

Anonymous:1998:SAP [Ano98r]

Anonymous:1998:TBF [Ano98t]
Anonymous. Technology and business: a fast Y2K bug fix. Confidentiality without encryption...
REFERENCES

Anonymous:1999:AWS

Anonymous:1999:CCI

Anonymous:1999:CEV

Anonymous:1999:DSC

Anonymous:1999:DSV
Anonymous. DREO secure video conferencing and

Anonymous:1998:UGT

Anonymous:1998:UFR

Anonymous:1999:RDS

Anonymous:1999:AWS

Anonymous:1999:CCI

Anonymous:1999:CEV

Anonymous:1999:DSC

Anonymous:1999:DSV
Anonymous. DREO secure video conferencing and

Anonymous:1998:UGT

Anonymous:1998:UFR

Anonymous:1999:RDS
REFERENCES


Anonymous:1999:EDB


Anonymous:1999:EPFa


Anonymous:1999:EGC


Anonymous:1999:KNT

Anonymous. Key note: Trust management for public-key infrastructures: Discussion-trust management. Lecture Notes in Computer Science, 1550: 64–??, 1999. CODEN LNCSD0. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anonymous:1999:L

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

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

Anonymous;1999:ULE


Anonymous;1999:WDE


ANSI;1997:AXP


ANSI;1998:AXD


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


Abreu:1994:DAI


Anderson:1998:LS


Andrasiu:1993:LTP


Aruliah:1985:PIE


Allen:1997:PSA


Aumann:1998:AES


Aumann:1999:ITS


Arazi:1993:AEA


Arensberg:1921:CD


Arensberg:1922:CSP


Adamson:1995:JSR

Abdulla:1999:OMS


Adleman:1999:AMC


Adleman:1999:HPN


Adleman:1999:HSP


Alpern:1983:KEU


Atici:1996:UHM


REFERENCES


REFERENCES


Akl:1983:CSP


Ateniese:1999:SOI


Atallah:1999:ATC


Atanasiu:1993:AEU


Al-Tawil:1998:NAP


Atkins:1993:CKE


Atkinson:1995:RIA

REFERENCES

Atkinson:1995:RIE


Atkinson:1997:TMS


ATT:1986:AUS


Aucsmith:1996:TRS


Aucsmith:1998:SIW


Aura:1996:PID


AAGD:1996:RPR

REFERENCES

Aparicio:1999:ITD


Avolio:1998:PCP


Anderson:1996:NC


Alabbadi:1994:SDS


Alabbadi:1995:DSS


Angel:1999:JQH

Aspray:1988:RCD


AufderHeide:1999:PGP


Ayoub:1968:EKR


Ayoub:1968:EEK

F. Ayoub. Erratum: En-

\textbf{Ayoub:1981:EKR}  

\textbf{Ayoub:1983:DCE}  

\textbf{Bernstein:1996:ISB}  

\textbf{Blau:1996:VPA}  

\textbf{Baker:1997:RRM}  

\textbf{Bach:1988:HGF}  

\textbf{Bacard:1995:CPH}  
REFERENCES


Badia:1999:EDL


Baker:1992:CAB


Biham:1998:SNB


Bakker:1999:MAS


Ball:1997:ESS


Ball:1999:WSB


Bullitt:1999:GDI


Bamford:1982:PPR

James Bamford. *The puzzle palace: a report on America’s most secret agency.*


citations/journals/tocs/1990-8-1/p18-burrows/.


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


REFERENCES


**Barber:1991:1AD**

**Barber:1992:CSC**

**Barber:1992:DPP**

**Barber:1993:EFA**

**Barber:1993:EFP**

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

Barker:1995:CDT  [Bar95]

Barlas:1996:NKD  [Bar96a]

Barron:1996:RTR  [Bar96b]

Barias:1997:NBP  [Bar97]

Barnes:1999:ESJ  [Bar99]

Barron:2005:DWP  [Bar05]

Baskerville:1993:ISS  [Bas93]
REFERENCES

Bastian:1995:CCE


Bassham:1998:ETA

Lawrence E. Bassham III. Efficiency testing of ANSI C implementations of Round1 candidate algorithms for the Advanced Encryption Standard. In National Institute of Standards and Technology [Nat98], page 30. ISBN ???. LCCN ????. URL http://csrc.nist.gov/encryption/aes/round1/ri-ansic.pdf. See [RD99a] for a conference overview. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

Baudouin:1939:ECF


Baudouin:1946:ECF


Bauer:1982:KVM


Bauer:1997:DSM


Baxter:1997:SBE


Bowers:1960:PC


Bowers:1967:PC  

Blakley:1979:RSA  

Bennett:1989:EQC  

Ben-Aroya:1994:DCL  
REFERENCES


REFERENCES


Four volumes.

Blakley:1993:TSD


Blakley:1993:TPD


Bennett:1995:GPA


Barni:1997:RWS


Barni:1998:CPD


Barni:1998:DDS

REFERENCES


REFERENCES


Biham:1999:BGD


Biham:1998:CSR


Blaze:1998:DPA


Biham:1999:MMA


Biehl:1994:CPB


A. Beimel and B. Chor. Secret sharing with public reconstruction. Lecture
REFERENCES


Blundo:1995:SRB


Blundo:1996:BES


Brassard:1996:YQC


Baldwin:1997:LS


Blakley:1998:C


Burwick:1998:MCC


Barker:1988:ECT

IEEE Computer Society order number 895.

Bigun:1997:AVB


Blair:1999:DRA


Baritaud:1993:SPK


Bruco:1999:DHC


Bas:1998:SSB

REFERENCES


REFERENCES


REFERENCES

operation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).


Birnbaum:1986:VPS


Burmester:1991:ALN

Mike V. D. Burmester and Yvo Desmedt. All languages in NP have divert-


Feng Bao and Robert H. Deng. A signcryption scheme with signature directly verifiable by public key. Lecture Notes in
REFERENCES

Blundo:1998:VCS

Bao:1999:NTM

Boneh:1999:CRP

Burmester:1992:EZK

Branwyn:1995:IRA
REFERENCES

pp. LCCN TK5105.875.157


Blundo:1994:MSS


Bondalapati:1999:DDE


Boneh:1998:ARG


BenAyed:1999:MFP


Blundo:1999:PSS


Bao:1998:MFA

F. Bao, R. H. Deng, X. Gao, and Y. Igarashi. Modified finite automata public key cryptosystem. Lecture
REFERENCES

Blundo:1993:IRS


Blundo:1996:IRS


Bonheh:1999:FPL


Bonheh:1999:FL


Bao:1997:DAT


Bao:1998:BPK


Boneh:1993:PSK


**Burmester:1996:PRS**


**Bellare:1997:CST**


**Boneh:1997:ICC**


**Benaloh:1994:OWA**


**Bosselaers:1997:RCH**

Bellare:1998:RAN


Baraani-Dastjerdi:1995:CMO


Baraani-Dastjerdi:1997:UCH


Blaze:1996:MKL


Burmester:1998:EKE


Blundo:1993:GDS

Blundo:1993:ESM


[BDV93]

Blundo:1998:SSS


[BDV98]

Bright:1979:QRN


[BE79]

Barrett:1990:SDU


[Barrett:1993]

Beardsley:1972:YCI


[Beardsley:1972]

Beauquier:1992:TDP


[Beauquier:1992]

Beaver:1993:HBS


[Beaver:1993]
REFERENCES

Beaver:1996:ASE

Beaver:1997:CBC

Beaver:1997:PPE

Becker:1982:EDE

Beckett:1988:IC

Beckett:1990:IAM

Beckett:1997:ICP
REFERENCES

Reference 1: [Bec88] Updated edition of *Introduction to cryptology*.


and specifies solutions including Kerberos. Also talks about auditing in X.

Bellovin:1998:CI


Bellare:1999:POP


Bennett:1980:UWN


Bennett:1988:AEA


Bennett:1989:UMS


Benario:1998:TSU


Benedens:1999:GBW


Bertrand:1973:EOP

REFERENCES


Berson:1997:FMP


Berg:1998:JQHd


Bergmann:2009:DKR


Beth:1983:CPW


Bett:1985:ESG


Beth:1995:CCIIb

REFERENCES

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

Beth:1995:CCIa


Beth:1995:MST


Beth:1998:Ea


Beutelspacher:1994:CIA


Blaze:1996:MKC


Beimel:1997:RCP


Boneh:1997:EGS


REFERENCES


REFERENCES


[Blum:1985:EPP] Manuel Blum and Shafi Goldwasser. An efficient probabilistic public-key encryption scheme which hides all partial information. In Blakley and
REFERENCES


REFERENCES


REFERENCES

[186]


REFERENCES

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


REFERENCES


REFERENCES

ng/10/19/19/28/17/21/abstract.html.


REFERENCES

Black:1999:UFS


Bellare:1998:MTF


Bellare:1998:MOT


Bayer:1993:IER


Brassard:1998:QCH

REFERENCES


REFERENCES

Biham:1992:DCI


Biham:1994:NTC


Biham:1994:MOA


Biham:1995:CMM


Biham:1995:MLC


Biham:1996:CTM

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

Biham:1997:CL


Biham:1997:FNI

REFERENCES


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


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


REFERENCES

CODEN CMSYE2. ISSN 0895-6340.

Bishop:1988:FEP  

Bishop:1989:USS  

Bishop:1989:FEP  

Bishop:1990:AGD  

Bishop:1991:AMU  

Bishop:1992:FPC  

Bleichenbache:1997:NOC  

Bellare:1997:ROZ  

Book:1980:UDC  
R. V. Book and Sai Choi Kwan. On uniquely de-
cipherable codes with two
codewords. *IEEE Transactions on Computers*, C-
CODEN ITCOB4. ISSN
0018-9340 (print), 1557-
9956 (electronic). URL
org/stamp/stamp.jsp?tp=
&arnumber=1675571.

**REFERENCES**

[BK90] Fritz Bauspieß and Hans-
Joachim Knobloch. How to
keep authenticity alive in
a computer network. *Lec-
ture Notes in Computer Sci-
ence*, 434:38–??, 1990. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/0434/04340038.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340038.

**Bauspiess:1990:HKA**

[BK94a] G. R. Blakley and G. A.
Kabatianskii. Linear al-
gebra approach to secret
sharing schemes. *Lecture Notes in Computer Science*, 829:33–??, 1994. CO-
DEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Blakley:1994:LAA**

[BK94b] Thomas A. Brooks and
Michael M. Kaplan. Secu-
rity technologies. *AT&T
Technical Journal*, 73(5):
4–8, September/October
1994. CODEN ATJOEM.
ISSN 2376-676X (print),
8756-2324 (electronic).

**Blakley:1994:GPS**

A known plaintext attack
on the PKZIP stream cip-
her. *Lecture Notes in Com-
puter Science*, 1008:
144–??, 1995. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

**Blahm:1995:KPA**

[BK95b] G. R. Blakley and G. A. Ka-
batianski. On general per-
fected secret sharing schemes.
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

**Blum:1995:DPC**

Blum and Sampie
Kannan. Design-
ing programs that check
their work. *Journal of the
Association for Computing
Machinery*, 42(1):269–
291, January 1995. CO-
DEN JACOAH. ISSN 0004-
5411 (print), 1557-735X
(electronic). URL http://
www.acm.org/pubs/toc/
Abstracts/0004-5411/200880.

**Blum:1995:DPC**
REFERENCES


REFERENCES


REFERENCES

[199]

1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1998:LRB


Bakhmurov:1999:DEE


Burgett:1998:CLD


Boneh:1995:QCH


Boneh:1996:ABF


Boneh:1996:ABB

REFERENCES


Binsted:1999:CDS


Blatman:1975:MMC


Blakley:1979:SCK


Blahut:1983:TPE


Blakley:1985:ITF


Blanchard:1989:CSS

REFERENCES

[Blaze:1993:TMS]

[Blaze:1994:HEL]

[Blaze:1996:KME]

[Blaze:1996:HBE]

[Blaze:1996:OKE]

[Blair:1998:SEP]

[Bleichenbacher:1996:GES]
REFERENCES

[Ble97] Daniel Bleichenbacher. On the security of the KMOV
public key cryptosystem. Lecture Notes in Computer
Science, 1294:235–??, 1997. CODEN LNCS9D9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-
y.com/link/service/series/0558/bibs/1294/12940235.pdf.

[Ble98a] Daniel Bleichenbacher. Chosen ciphertext attacks against
protocols based on the RSA encryption standard PKCS
#1. Lecture Notes in Computer Science, 1462:
1–12, 1998. CODEN LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (electronic). URL http://link.springer-
y.com/link/service/series/0558/bibs/1462/1462001.pdf.

[Ble98b] Gerrit Bleumer. Biometric yet privacy protecting per-
son authentication. Lecture Notes in Computer Science,
1525:99–110, 1998. CODEN LNCS9D9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http://link.springer-
y.com/link/service/series/0558/bibs/1525/15250099.pdf.

[Ble99] K. S. Barber, T. H. Liu, and D. C. Han. Agent-
oriented design. Lecture Notes in Computer Science,
1647:28–40, 1999. CODEN LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[BLLV98] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson.
Time-stamping with binary linking schemes. Lecture
Notes in Computer Science, 1462:486–??, 1998. CODEN
LNCS9D9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[BLH99] K. S. Barber, T. H. Liu, and D. C. Han. Agent-
oriented design. Lecture Notes in Computer Science,
1647:28–40, 1999. CODEN LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[BLLV98] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson.
Time-stamping with binary linking schemes. Lecture
Notes in Computer Science, 1462:486–??, 1998. CODEN
LNCS9D9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[BLH99] K. S. Barber, T. H. Liu, and D. C. Han. Agent-
oriented design. Lecture Notes in Computer Science,
1647:28–40, 1999. CODEN LNCS9D9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[BM94] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson.
Time-stamping with binary linking schemes. Lecture
Notes in Computer Science, 1462:486–??, 1998. CODEN
LNCS9D9. ISSN 0302-9743 (print), 1611-3349 (electronic).

[Beth94] Thomas Beth, D. E. Lazic, and A. Mathias. Cryptanal-
ysis of cryptosystems based on remote chaos replica-
tion. In Desmedt [Des94b], pages 318–331. CODEN
LNCS9D9. ISBN 3-540-58333-5 (Berlin), 0-387-
58333-5 (New York). ISSN 0302-9743 (print), 1611-
3349 (electronic). LCCN
REFERENCES


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


[Blu98c] Brillhart:1975:NPC

[Blu83a] Blum:1983:CFT

[Blu82] Blum:1983:HES


REFERENCES

**Blum:1984:IUC**


**Blundo:1995:NDT**


**Blundon:1997:BCE**


**Bayer:1976:EST**


**Blum:1982:HGC**


**Blum:1984:HGC**

[BM84a] Manuel Blum and Silvio Micali. How to generate

**Boyer:1984:PCR**


**Blakley:1985:SRS**


**Beale:1989:EUR**


**Bellare:1990:NIO**


**Bellovin:1991:LKA**

REFERENCES

bell-labs.com/dist/kerblimit.
usenix.ps.Z; local --
- kerblimit.usenix.
ps.FTP - research.att.com:/dist/kerblimit.usenix.ps.
local - kerblimit.usenix.ps.

Brickell:1991:IID


Bellare:1992:HSG


Bleichenbacher:1994:DAG


Boyd:1994:DSK


Burns:1994:PSS


Boyd:1995:DAK

REFERENCES

**Bleichenbacher:1996:EOT**


**Bleichenbacher:1996:OTB**


**Bleichenbacher:1996:OTO**


**Brincat:1997:SC**


**Bellare:1999:FDS**


**Bellare:1999:FSD**


**Blundo:1999:RMS**


**Blackburn:19xx:NPP**

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


[Blackburn:1994:WPK]

[Bubak:1999:DHP]

[Blundo:1996:TOB]

[Biehl:1996:CPB]

REFERENCES


Book:1985:SNP


Book:1985:SNS


Book:1985:VTA

REFERENCES

Book:1985:CRE


Brickell:1988:CSR


Brickell:1992:CSR


Berghel:1996:IKP


Brassil:1996:WDI


Bull:1999:NMA


Ben-Or:1983:CSS

Michael Ben-Or, Benny Chor, and Adi Shamir. On

**Boland:1995:WDI**

**[BOD95]**

**Bolignano:1997:TMC**

**Bolignano:1998:IPB**

**Bolignano:1998:IPM**
D. Bolignano. Integrating proof-based and model-checking techniques for the formal verification of cryptographic protocols. *Lecture
REFERENCES

Notes in Computer Science, 1427:77–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bond:1947:FSC  [Bon47]


Boneh:1998:DDP  [Bon98a]


Boneh:1998:DDH  [Bon98b]


Booth:1981:ASU  [Boo81]


Bookstein:1996:RB  [Boo96]

REFERENCES

Borman:1993:RTAa


Borman:1993:RTAb


Borman:1993:RTAc


Borcherding:1996:LAD


Bosworth:1982:CCC


Bosma:1990:PPC


Bosselaers:19xx:EFH

A. Bosselaers. Even faster hashing on the Pentium. In ????, page ??, ???. ????, 19xx. ISBN ????. LCCN ????. URL ftp:
REFERENCES

//ftp.esat.kuleuven.ac.
be/pub/COSIC/bosselaer/
pentiumplus.ps.gz. Pre-
sented at the rump session
of Eurocrypt’97, Konstanz,
Germany, May 12-15, 1997,
and updated on November

[Bou85] Adam C. Bounas. Direct
determination of a “seed”
binary matrix. Information
Processing Letters, 20
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

[Bou94] M. Boucher. La génération
du pseudo-aléatoire cryptographique
ment sécuritaire et ses considérations pratiques.
(French) [Cryptographically-
secure random-number genera-
tion and its practical consid-
erations]. Masters thesis, Départment
d’I.R.O., Université de Montréal,
Montréal, QC, Canada, 1994.

[Bov98a] Ernst Bovenlander. Smart
card security. Lecture Notes
in Computer Science, 1528:
332–??, 1998. CODEN
LNCSDE. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1528/15280332.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1528/15280332.
pdf.

[Bov98b] E. Bovenlander. Smart card
security. Lecture Notes in
Computer Science, 1528:
332–337, 1998. CODEN
LNCSDE. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Digraphic substitution: the
Playfair cipher, the four
square cipher. Practical
cryptanalysis; v. 1. Amer-
ican Cryptogram Association,
Greenfield, MA, USA,
1959. 46 pp.

The bifid cipher. Practical
cryptanalysis; v. 2. Amer-
ican Cryptogram Association,
Greenfield, MA, USA,

The trifid cipher. Practical
cryptanalysis; v. 3. Amer-
ican Cryptogram Association,
Greenfield, MA, USA,
REFERENCES


CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).
ISSN 0302-9743 (print), 1611-3349 (electronic).

**Boyd:1995:CCC**


**Boyd:1995:CCI**


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

**Boyd:1997:DSP**


**Boyer:1998:DSM**


**Boyko:1999:SPO**


**Beker:1982:CSP**

REFERENCES


REFERENCES

1997. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

[BP97c] Buchmann:1997:OWF


G. Bella and L. C. Paulson. Mechanising BAN Kerberos by the inductive method. Lecture Notes in Computer
REFERENCES

Bleichenbacher:1999:SC

Blum:1999:MME


Birov:1999:PML

Bleichenbacher:1999:SC

Blaze:1999:KNT

Bishr:1999:PRS

Blobel:1999:SAD
REFERENCES


REFERENCES


**Bellare:1997:FAK**


**Bellare:1997:MUR**


**Bellare:1999:CVC**


**Bellare:1999:CVI**


**Branstad:1979:VHD**


**Brassard:1981:TLT**


**Bracha:1987:ERR**

Gabriel Bracha. An $O(\log n)$ expected rounds


REFERENCES


REFERENCES


REFERENCES

Breitrose:1997:DEM


Brent:1999:CAP


Brickell:1985:BIK


Brickell:1986:CKC


Brickell:1988:CKC


Brickell:1990:SIS

REFERENCES


Brownell:1981:ODN


Brooke:1986:BRB


Brown:1994:ECL


Brock:1996:CCP


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB

REFERENCES

231

(print), 1879-2294 (electronic).


Brown:1990:DPT


Beth:1991:NSE


Biham:1991:DCD


Biham:1991:DCFb


Biham:1991:DCFa

Eli Biham and Adi Shamir. Differential cryptanalysis of Feal and $N$-hash. Technical report CS91-17, Department of Applied Mathemat-


REFERENCES


Blaze:1995:MBC


Boneh:1995:CSF


Bose:1995:ATV


Bruckstein:1995:SSD


Brunnstein:1995:IPR

Biham:1997:DFA


Bramhill:1997:CCD


Boneh:1998:CSF


Baaleh:1999:AGA


Bellare:1999:NEE


Bellare:1999:NME


Barreiro:1997:PKC

Ernesto Reinaldo Barreiro, Jorge Estrada Sarlabous, and Jorge Alejandro Piñeiro Barcelo. A public key cryp-


[Bakhtiari:1995:APL]


[Bakhtiari:1996:PAK]


[Bakhtiari:1996:PBA]


[BSN97]


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

[BT94] Josh Benaloh and Dwight Tuinstra. Receipt-free


1445 (print), 1095-7200 (electronic).


**Burton:1984:RPKa**


**Burton:1984:RPKb**


**Burton:1985:EAC**


**Burnham:1988:DES**


**Burmester:1994:CCK**


**Burmester:1994:CCW**


**Burmester:1994:ROD**


Andries E. Brouwer and Peter van Emde Boas. A note on: “Master keys for group

[BV98a]

Boneh:1996:HCM


[BV98b]

Boneh:1997:RLC


dabo/papers/nonuniform.ps.gz.

[BV98c]

Boneh:1998:BRM


Blunk:1998:RPE


Boneh:1998:DWS

REFERENCES

stanford.edu/~dabo/papers/no_rsa_red.ps.gz.


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

[Blake-Wilson:1999:UKS]
S. Blake-Wilson and A. Menezes. Unknown key-share attacks on
the station-to-station (STS) protocol. Lecture Notes in Computer Science,

[Buchholz:1988:CQDc]
Werner Buchholz, Maurice V. Wilkes, Alfred W. Van Sinderen, C. J. Fern,
Jr., and W. L. van der Poel. Comments, queries, and debate: Babbage and
the Colossus; Babbage and Bowditch; Two Early European Computers;
Early Dutch Computer. Annals of the History of Computing, 10(3):218–221,
July/September 1988. CODEN AHCQE5. ISSN 0164-1239.

[BY92]
Colin Boyd and Tong Lai Yu. Remarks on a data
1992. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [YY91].

[Bellare:1993:CCT]
M. Bellare and M. Yung. Certifying cryptographic tools: The case of

[Beller:1993:BDK]
M. J. Beller and Y. Yacobi. Batch Diffie–Hellman key agreement systems and
their application to portable communications. Lecture Notes in Computer Science,

[Beller:1993:BDH]
Michael J. Beller and Ya-
cov Yacobi. Batch Diffie–
Hellman key agreement sys-
tems and their application
to portable communica-
tions. Lecture Notes in
Computer Science, 658:
208–??, 1993. CODEN
LNCSD9. ISSN 0302-9743
REFERENCES


REFERENCES

Cypher:1996:UAS

Caelli:1996:CKE

Caelli:1996:CPF
W. Caelli. Cryptography: Personal freedom and law enforcement — is it possible to get agreement? Lecture Notes in Computer Science, 1029:1–??, 1996. CODEN LNCS9D, ISSN 0302-9743 (print), 1611-3349 (electronic).

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

Calvocoressi:1980:TSU

Callimahos:1989:TAZ

Callimahos:1992:HC

Campagne:1971:REC


REFERENCES


REFERENCES

1996. CODEN ???? ISSN ????


REFERENCES


Chapman:1997:HHS


Clark:1998:OHA


Cramer:1998:ZPF

Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. Efficient multiparty computations secure against an adaptive adversary. Lecture Notes in Computer Science, 1592:311–??, 1999. CODEN LNCSD9. ISSN 0302-
REFERENCES


[CDNO97] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable encryption. In

Chen:1995:PDP


Cramer:1994:PPK


Certicom:1997:EC


Chaum:1987:DPD


REFERENCES

Callas:1999:FUI


Ceruzzi:1991:RCK


Chor:1994:TT


Coppersmith:1996:LRR

D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. Low-exponent RSA with related messages. Lecture
REFERENCES

Coppersmith:1996:LER


Canetti:1997:CES


Coppersmith:1975:GCA


Chor:1985:RRL

REFERENCES


REFERENCES

URL http://www.oreilly.com/catalog/securityusability


REFERENCES


Carrel:1997:RIO

[CH97a] D. Carrel and D. Harkins.

Chang:1997:SAG

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

Chen:1998:PFR

[CH98] Mark Chen and Eric Hughes.

Corcoran:1999:SCB

David Sims David Corcoran and Bob Hillhouse.

Cordon:1999:AMD

O. Cordon and F. Herrera.

Chaum:1979:UEM

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

Chaum:1981:UEM

D. Chaum.
REFERENCES


Chandler:1983:IMC


Chaum:1983:BSU


Chaum:1985:HKS


Chaum:1985:NSC


Chaum:1985:SIT

David Chaum. Security without identifica-
REFERENCES


**Chang:1986:DKL**


**Chapman:1986:NFS**


**Chaum:1990:SDA**


**Chaum:1991:SCS**


**Chaum:1992:AEPb**


**Chaum:1992:AEPa**

(print), 1946-7087 (electronic).


REFERENCES

17, 1999. CODEN ????
ISSN 1389-1286 (print),
1872-7069 (electronic). URL
http://www.elsevier.com/
cas/tree/store/comnet/
sub/1999/31/11-16/2182.
.pdf.

Chau:1999:QCE

H. F. Chau. Quantum
convolutional error correc-
tion codes. Lecture Notes
in Computer Science, 1509:
314–324, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Chesson:1973:CC

F. W. (Frederick William)
Chesson. Computers and
cryptology. Datamation, ??
CODEN DTMNAT. ISSN
0011-6963.

Cheswick:1992:EBW

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

Canetti:1997:MAC

R. Canetti, S. Halevi, and
A. Herzberg. Maintaining
authenticated communication in
the presence of break-ins. In Proc. 16th
ACM Symp. on Principles
of Distributed Computation,
page ?? ACM Press, New
York, NY 10036, USA, [CHLT99]
1997.

Chiopris:1992:SBE

Carlo Chiopris. The SE-
CReTS banking expert sys-
tem from phase 1 to phase
2. Lecture Notes in Com-
puter Science, 636:91–??,
ISSN 0302-9743 (print),
1611-3349 (electronic).

Chin:1999:HCD

Shiu-Kai Chin. High-
confidence design for secu-
rity: don’t trust — ver-
ify. Communications of
the Association for Com-
puting Machinery, 42(7):
33–37, July 1999. CO-
DEN CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http:
//www.acm.org:80/pubs/
citations/journals/cacm/
1999-42-7/p33-chin/.

Chin:1999:HDS

Shiu-Kai Chin. High-
confidence design for secu-
rity: don’t trust — ver-
ify. Communications of
the Association for Com-
puting Machinery, 42(7):
33–37, July 1999. CO-
DEN CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http:
//www.acm.org:80/pubs/
citations/journals/cacm/
1999-42-7/p33-chin/.

Christophides:1999:ODI

V. Christophides, C. Houstis.
S. Lalis, and H. Tsalap-
REFERENCES


Canetti:1997:PSL


Chor:1986:TIP


Chung:1998:DWCb


Christiansen:1978:SL


Christoffersson:1988:MAE


Christianson:1998:SPI

Christianson:1999:DSCb

Christianson:1999:SPI

Chuang:1989:NES

Currie:1996:SEL

Ciarcia:1986:BHD

Cao:1999:DTJ
REFERENCES

Clark:1995:SRP


Chabaud:1998:DCS


Collins:1999:DCL


Coster:1992:ILD


Coppersmith:1995:TCB


Coppersmith:1996:PMT


Charlwood:1998:EXA

REFERENCES


Chee:1991:CNP

REFERENCES


REFERENCES

Cox:1997:SSS

Chan:1988:IEC

K. Chang:1997:PCM

Cox:1997:PWR

Cox:1998:SGM
[CL98] I. J. Cox and J. P. M. G. Linnartz. Some general


REFERENCES


Clapp:1999:ILP

Cla99

Cleve:1991:CTI

Cle91

Clevenger:1996:DEU

Cle96
Mark Allen Clevenger. Data encryption using RSA public-key cryptosystem. Thesis (M.S.), Ball State University, Muncie, IN, USA, 1996. ii + 149 pp.

Chang:1998:SOM

CLHL98

Clinton:1997:AEC

Clin97
Bill Clinton. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 730 et seq. — received in the United States House of Representatives November 15, 1996, pursuant to 50 U.S.C. 1703(b). Washington, DC, USA, January 7, 1997. 5 pp. Referred to the Committee on International Relations. Shipping list no.: 97-0126-P.

Clinton:1999:LPM

Clis99
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 keys, and facilitation of access to the plaintext of data for legitimate law enforcement purposes. United States Government Printing Office, Washington, DC, USA, September 21, 1999. 40 pp. Referred to the Committee on the Judiciary and Government Reform. Shipping list no.: 2000-0018-P.

**Chua:1999:ART**


**Cheng:1998:MVR**


**CM79**


**Ciampi:1982:EVS**


**Chan:1985:NMP**

B. Chan and H. Meijer. A note on the method of puzzles for key distribution. *International Journal of Com-


Chen:1998:DRT


Camenisch:1999:SEG


Charlton:1999:DPM


Christianson:1999:DSCa


Coradeschi:1999:HMC


Chen:1998:SCC


Cohen:1993:AAA

G. Cohen, Teo Mora, and Oscar Moreno, editors. Applied algebra, algebraic algorithms, and

**Canetti:1999:ECS**


**Charnes:1997:SSH**


**Chor:1989:SCT**


**Chuan-Ming:1994:RTR**


**Craver:1997:CIW**

S. Craver, N. Memon, B. L. Yeo, and M. M. Ye-
REFERENCES


Chao:1998:CSE


Coltell:1998:AOL


Cocks:1997:SKG


Cohen:1987:CCI


Cohen:1987:IIP


Cohen:1994:SCC


Cohen:1996:RRA

REFERENCES


[Col64] F. N. Colaço. A criptografia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quase quer que sejam os caracteres empregados. (Portuguese) [Cryptography revealed, or, the art of translating and deciphering obscure writings, whatever the characters employed]. De Santos e Cia, Pernambuco, Brazil, 1864. 93 pp. LCCN Z104.C68 1846.


[Con99b] Scott Contini. On differential properties of data-


REFERENCES

Charnes:1995:CSE

Coppersmith:1995:ASA

Coppersmith:1998:C
REFERENCES


REFERENCES


REFERENCES

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


[Cra97] Scott Craver. On public-key steganography in the presence of an active warden.
REFERENCES

[Craver:1998:PKS]

[Cramer:1999:ISC]

[Crepeau:1990:VDS]

[Crepeau:1997:ECP]

[Contini:1999:IAS]

[Chaum:1983:ACP]

[Chaum:1998:Ca]
REFERENCES

1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Crypto:1981:ACP**


**CryptoBytes:1995:C**


**Cesarini:1983:ACC**


**Chepyzhov:1991:FCA**


**Chabaud:1996:CSS**


**Chambers:1996:RLM**


Cusick:1996:BNFb


Camenisch:1997:EGS


Chambers:1997:RLM


Coppersmith:1997:PAP


Chen:1997:NIC


Canteaut:1998:COM

Ronald Cramer and Victor Shoup. A practical public
key cryptosystem provably secure against adaptive chosen ciphertext attack. Lecture Notes in Computer Science, 1462:13–25, 1998. CODEN LNCS.D. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http:\link.springer-ny.com\link/service/series/0558/\bib\1462\14620013.htm; http:\link.springer-ny.com\link/service/series/0558\papers\1462\14620013.pdf.

Coradeschi:1999:ASV

Chaum:1989:SCF

Csirmaz:1995:SSM
L. Csirmaz. The size of a share must be large. Lecture Notes in Computer Science, 1556:43–??, 1999. CODEN LNCS.D. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coppersmith:1994:ABP

Chang:1997:GSS

Chen:1999:TPS
REFERENCES


Ciminiera:1989:AMM


Calvelli:1993:ARS


Chabaud:1995:LBD


Cohn:1999:MC


Chaum:1991:CSU


Chang:1991:BCC

REFERENCES


[CWM+91] Paul Ceruzzi, Eric A. Weiss, John Walker Mauer, Thomas Drucker, Peggy Aldrich Kidwell, and K. W. Smilie. Reviews: Grosch: Computer: Bit slices from a life; Tomayko: Computers in spaceflight: The NASA Experience; Billow: Denk, Maschine! Geschichten über Robotor, computer und Kunstliche Inteligenz; Napier: Rabdology; Charlesworth: Calculators & Computers; Calculators & Computers — The 20th Century; Transistors. forty years of computing, Datamation; Bennett: The industrial in-
REFERENCES


Coppersmith:1998:CT


Chang:1998:BSC


Craver:1998:TTL


Cao:1990:DKC


DeMillo:1983:ACC

REFERENCES


[Dam96]

[Dam98]

[Dam99a]

[Damgaard:1999:CSZ]

[Danisch:1995:RES]

[Danthine:1996:ECM]
REFERENCES

Dang:1997:AAC


Darnell:1997:CCI


Davida:1979:IHS


Davida:1981:CAR

George I. Davida. The case against restraints on non-governmental research in cryptography. Communications of the Association for Computing Machinery, 24(7):445–450, July 1981. CODEN CACMAM2. ISSN 0001-0782 (print), 1557-7317 (electronic). This is an opposing view published with [Ame81].

Davies:1985:MAA

REFERENCES

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


REFERENCES

Davies:1998:NIH


Davies:1998:LCM


Dawson:1993:CSG


Dawson:1996:CSR


Denning:1981:SRR


DenBoer:1988:CF

REFERENCES

[DB89]

[DB91]

[DB94]

[DB96]

[DB99]

**Daemen:1993:CSH**


**Dobbertin:1996:RSV**


**DHalluin:1999:ASR**


**DeWin:1996:FSI**


**deJonge:1986:ASR**


Desmedt:1995:MNA


Desmedt:1995:MNS


DeSantis:1994:HSF


Davio:1985:EHS


Delaigle:1997:LCW


DDJStaff:1998:NVS

DDJ Staff. News and views: a Standard Linux? cryptography contest; drives get smaller and smaller; Perl conference; really embedded systems; programmer

DDJStaff:1998:NVb

[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.

DDJStaff:1998:NVG

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

DDJStaff:1998:NVY

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

DDJ:1998:NVN


DDJStaff:1998:NVN

REFERENCES

DDJStaff:1998:NVc

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

DDK98

DDJStaff:1998:NVd


DDLM94

DDJstaff:1999:NVR


DePaoli:1998:WBS


Denny:1994:FR


Delaigle:1996:DW

REFERENCES


REFERENCES

DeSantis:1994:SSP

DeSantis:1994:KCQ

DeSantis:1999:NIZ

Darmstaedter:1998:LCS

deVries:1953:SMC
DeAlvare:1990:HCC


DeDecker:1993:USK


DeSchutter:1993:TFA


DeSoete:1993:PKC


DeSantis:1995:ACE


DeDecker:1998:ICS


DeSantis:1998:E


DeSchutter:1998:TFA

DeSmit:1998:GAE


DeMoliner:1999:STB


Drossopoulou:1999:DSJ


Deavours:1987:CPI


Deavours:1988:BPS


Deavours:1998:A


Kruh:1998:TBW


Demirdogen:1988:FDM

[Dem88] A. Caner Demirdogen. Flaw detection methods based on


REFERENCES


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


[Des90b] Yvo G. Desmedt. Making conditionally secure cryp-
tosystems unconditionally abuse-free in a general context (extended abstract).

CODEN LNCSDE9. ISSN 0302-9743 (print), 1611-3349 (electronic).


Desmedt:1996:EBB


Desmedt:1996:SPF


Desel:1998:BLA


Desmedt:1998:C


Desmedt:1998:SRR


Desfray:1999:ADP


Desmedt:1999:ES


Deugo:1997:CTS

Deugo:1998:SMS


Desmedt:1990:TC


Desmedt:1991:SGA


Desmedt:1991:SRT


Dawid:1992:BSC

[DF92] H. Dawid and G. Fei-


Domingo-Ferrer:1991:CTP


DiCrescenzo:1999:HFS


Ding-Feng:1999:CS


Donatini:1999:DES


Dwork:1993:LCP


Davida:1997:ACC

REFERENCES


[DH77] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the

REFERENCES

Association for Cryptologic Research.


REFERENCES


DiCrescenzo:1999:SPH


Dia91


Ding:1996:CRT


Dieringer:1988:TAE


Diffie:1982:CVP


Diffie:1982:CTF


Diffie:1988:FTY


Diffie:1990:APK

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

Dixon:1994:SSS

Damm:1998:CRT

Dessmark:1993:MDD

Deavours:1985:MCM

Damm:1998:CRT

Dessmark:1993:MDD

Deavours:1985:MCM
REFERENCES


Deavours:1989:CMH


Dusse:1991:CLM


Damgaard:1994:BAH


Deavours:1998:SCH


Desmedt:1998:CES

REFERENCES

Deavours:1987:CYT


Daemen:1997:BCSa


Daemen:1997:BCSb


Dodson:1995:NFL


Dam:1996:CRS


Diffie:1998:PLP

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


Demphlous:1999:DPL


Davoine:1997:VCP


DeMillo:1982:CP


Damgaard:1993:ACE


Ding:1997:LMS


delaStelle:1902:TCF


DeMillo:1983:PDS

REFERENCES

Duc:1997:PAF

DeWin:1998:PSS

Denning:1981:MMK

Dongarra:1995:TSS

Denazis:1999:DIO

D’Angelo:1994:SEM

Dwork:1993:PPC

Dwork:1994:EEU
Cynthia Dwork and Moni Naor. An efficient exis-

Dossis:1995:FSR


Dossis:1995:OVH


Ding:1997:TFS


Dittmann:1998:IWE


Desmedt:1986:CTA

REFERENCES


REFERENCES

329


Dobbertin:19xx:CM


DomingoFerrer:1996:NPH


Donini:1998:CSR


DiCrescenzo:1999:COTb


Santis:1991:PRP


DiCrescenzo:1994:ROP

REFERENCES


[LCCN]
REFERENCES


[dR95] Peter de Rooij. Efficient exponentiation using precomputation and vector addition chains. Lecture Notes

[Daemen:1998:APR]

[Desel:1998:PTP]

[Daemen:1999:EBC]

[Drea:1999:NEB]

[Dray:1998:RNJ]

[Drach:1999:RDO]

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

**Drea:1992:MUC**


**deRaadt:1999:COO**


**Dror:1989:SCG**


**Droste:1996:NRV**


**Dawson:1995:DIJ**


**Denning:1981:MKG**


**Dolev:1983:AAB**

REFERENCES


REFERENCES


References


Durand:1999:DCC

Detombe:1993:CLC

DeSolages:1998:EFO

DiGiorgio:1998:JDS

DuBoulay:1999:DDT

duCarlet:1644:CCV

Dufner:1998:ACH
Mark S. Dufner. Applications of cryptology in high school mathematics. Thesis (M.A.), Minot State University, 500 University Ave.
Duhoux:1990:DBA


Dumey:1994:CQD


deVivo:1998:ISA


DeDecker:1992:HID


Dhem:1996:SSC


DeSoete:1990:CAS

REFERENCES


REFERENCES


Dai:1996:CFA


Ding:1991:STS


DeSantis:1990:DPS

REFERENCES


REFERENCES


Ellis:1975:PKC

Edwards:1915:CCT

Epstein:1956:FBC

El-Gamal:1985:PCS

Even:1985:PCC

Even:1985:RPS


**ElGamal:1985:PKCa**


**ElGamal:1985:PKCb**


**ElGamal:1985:STA**


**Elkins:1996:RMS**


**Ellis:1997:SNS**


**Ellison:1998:CRN**


**Ellis:1999:PPN**


Even:1993:CCS


Eades:1998:GDC


Ehrsam:1978:CKM


Ezawa:1998:ATS


Endler:1997:PSU


English:1995:EEP


Enge:1999:ECT

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


[Eri97b] 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 ac-


demics to obtains a government license before discussing cryptographic research with scholars on the Internet.

**Erickson:1999:EAS**


**Erskine:1999:CDD**


**Emerald:1997:NPC**


**Effelsberg:1998:SAI**


**Escott:1999:AEC**


**Estell:1980:BW**


**Ettinger:1998:SGE**

Evertse:1992:WNR

Even:1985:CSW

Even:1998:FVA

Evertse:1993:WNR

Fäak:1986:SVH
REFERENCES

Faak:1987:CMM

Falk:1988:DST

Fancher:1996:SCa

Fancher:1997:YPS

Farago:1967:BSS

Farago:1969:BSS

Farrow:1992:HIY

Farrell:1993:CCC


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

[Ferris:1987:WBC]

[Ferguson:1998:UBD]

[Ferguson:1999:IDT]

[Fernandes:1999:ECC]

[Feynman:1982:SPC]

[Friedman:1957:SCE]

[Friedman:1955:CLS]
Feghhi:1999:DCA

Fung:1998:PAE

Fuchsberger:1996:PCS

Fuchsberger:1996:PKC

Frankel:1997:ORP

Frankel:1997:PR

Feigenbaum:1992:CPM
[FR92] Joan Feigenbaum, Eric


REFERENCES


REFERENCES


[Fis84] Warren W. Fisher. Cryptography for computer security: Making the deci-
REFERENCES


REFERENCES

URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/054414.html


Freeman:1997:MCN


[Fellows:1993:KKI]


REFERENCES


REFERENCES


Feustel:1998:DUI


Fairfield:1985:LRN


Fagundes:1999:EGA


Fairfield:1985:LDE

REFERENCES

Frey:1999:TPD


Frankel:1998:RED


Fiat:1992:NH


Fiat:1994:BE


Flajolet:1989:RMS


Flajolet:1990:RMS

REFERENCES

Fujisaki:1997:PEC


Fujisaki:1998:PPS


Fujisaki:1999:HES


Fujisaki:1999:SIA


Folmsbee:1999:AJT

REFERENCES


REFERENCES


Franksen:1984:MBS

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Publisher</th>
<th>Year</th>
<th>Pages</th>
<th>ISBN</th>
<th>LCCN</th>
</tr>
</thead>
</table>

Franklin:1985:MID

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Institution</th>
<th>Year</th>
<th>Pages</th>
<th>ISBN</th>
<th>LCCN</th>
</tr>
</thead>
</table>

Franksen:1985:MBS

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Publisher</th>
<th>Year</th>
<th>Pages</th>
<th>ISBN</th>
<th>LCCN</th>
</tr>
</thead>
</table>

Franksen:1986:SHM

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Pages</th>
<th>ISSN</th>
<th>URL</th>
</tr>
</thead>
</table>

Frankel:1989:TIC

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Conference</th>
<th>Year</th>
<th>Pages</th>
<th>ISBN</th>
<th>LCCN</th>
</tr>
</thead>
</table>

Francis:1992:PSG

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Pages</th>
<th>ISSN</th>
<th>CODEN</th>
</tr>
</thead>
</table>

Franksen:1993:BCM

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Pages</th>
<th>ISSN</th>
<th>CODEN</th>
</tr>
</thead>
</table>

Franklin:1999:FCT

<table>
<thead>
<tr>
<th>Ref</th>
<th>Author</th>
<th>Title</th>
<th>Publisher</th>
<th>Year</th>
<th>Pages</th>
<th>ISBN</th>
<th>LCCN</th>
</tr>
</thead>
</table>
REFERENCES


[Fri35c] Friedman:1935:ICA


[Fri39b] Friedman:1939:MC

[Fri41] Friedman:1941:MCP
REFERENCES


**Friedman:1992:MC**


**Friedman:1992:MCP**


**Friedmann:1993:TDC**


**Friedman:1996:SLC**


**Froomkin:1996:ICP**


**Froomkin:1997:DST**


**Fiat:1987:HPY**


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


REFERENCES


REFERENCES

Frankel:1995:CIL


Frankel:1995:EES


Franklin:1995:BWS


Frankel:1997:CEE


Frankel:1998:DPK


Frankel:1998:RMU

5/frankel.html. Special issue on security.

**Frankel:1999:CRA**


**Frankel:1999:ASD**


**Gritzalis:1998:SIS**


**Gaglione:1988:ITP**


**Gaglione:1988:SCT**

[Gag88b] A. M. Gaglione. Some complexity theory for cryp...
tography. *Computers and Security*, 7(5):519, Octo-
tober 1988. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/0167404888902714.

M. Gomez-Albarran, P. A. Gonzalez-Calero, B. Diaz-
Agudo, and C. Fernandez-
Conde. Modelling the CBR life cycle using description logics. *Lecture Notes in
Computer Science*, 1650:
147–??, 1999. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).

Helen Fouche Gaines. *Elementary cryptanalysis: a
study of ciphers and their solution*. American Photographic

Helen Fouche Gaines. *Elementary cryptanalysis: a
study of ciphers and their solution*. American Photographic

Helen Fouche Gaines. *Crypt-
analysis: a study of ci-

Helen Fouche Gaines. *Crypt-
analysis: a study of ci-
Formerly published under
the title: Elementary crypt-
analysis.

Jason Gait. *Validating the
correctness of hardware im-
plementations of the NBS
Data Encryption Standard*. U.S. National Bureau of Standards, Gaithersburg,
MD, USA, November 1977.
iv + 40 pp.
REFERENCES


[Gai90] Jason Gait. Validating the correctness of hardware implementations of the


REFERENCES


[Gam93]
Ganesan:1996:HUK


Ganesan:1996:YSS


Gardner:1977:MGN


Garlinski:1979:IEW


Garlinski:1980:EW


Garay:1994:RMA


Garfinkel:1995:PPG

REFERENCES


ey; 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(9):19–22, September 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://neumann.computer.org/co/books/co1997/pdf/r9019.pdf.


Gardner:1997:PTT


Garber:1998:NBM


Garber:1998:NBS


Garfinkel:1998:PPG


Gaudin:1997:VBJ

Sharon Gaudin. Visa boosts Java’s credit line: smart cards will redefine how plastic is used. Computerworld, 31(31):1, 16, August
A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino [CM82], pages 451–467. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.I4 I58. From Computing Reviews: “The article reports on the progress of an historical study using a computer for statistical analysis. The subject of the study is a mass of trial depositions of the Knights Templar. The purpose of the project is to find statistical regularities in the large amount of testimony and to create a model for similar studies. The Order of the Knights Templar, founded around 1100, was the first Christian military order. After the Crusades, in the early fourteenth century, 127 articles of accusation were brought against the order, including charges of idolatry, sacrilege, and sodomy. The data being studied are the responses of 900 men to each of 127 accusations. The article details the accusations and the way in which the responses are being coded. The statistical package SAS (Statistical Analysis System) will be used. Examples of the results to be sought are: tallies of guilty/innocent responses, tallies of offenses committed versus seen versus heard about, and correlations between, for example, age and other responses. Depositions that differ markedly from the average response will be identified.”.


Goethals:1980:CAL

Gollmann:1990:CC

Gollmann:1994:CPA

Garber:1997:NBJ
Lee Garber and David Clark. News briefs: Judge rejects US restrictions on export of encryption; Intel, HP unveil Merced chip; Java wars heat up; AOL acquires CompuServe subscribers; con-


Gershenfeld:1998:QCM


Goldburg:1991:ACA


[GDD+97] F. Goffin, J. F. De laigle, C. De Vleeschouwer,
REFERENCES


REFERENCES

Gengler:1999:ELM  [Gen99b]

Gengler:1999:NCG  [Gen99c]

Gersho:1982:ACR  [Ger82]

Gerling:1997:VKU  [Ger97]

Gersho:1998:C  [Ger98]

Gero:1999:NME  [Ger99a]

Gero:1999:RRA  [Ger99b]
REFERENCES


REFERENCES


Goldreich:1986:HCR


Goldreich:1986:HCR


Goldreich:1986:HCR


Gabber:1997:HMP

REFERENCES


Gilboa:1999:CCR

Gibson:1990:SCD

Gibson:1991:EGC

Gibson:1996:SGP

Gifford:1981:CSI

Gilder:1997:APD
REFERENCES

Giles:1998:EFS


Gilboa:1999:TPR


Gingerich:1970:BRB


Girling:1987:CCL


Girault:1999:SCP


Girard:1999:WSP


Givierge:1925:CC

REFERENCES

Givierge:1932:CC


Givierge:1978:CC


Garey:1979:CIG


Gifford:1982:CSI


Gennaro:1996:RTD


Gennaro:1996:RES

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).

**Gennaro:1999:SDK**


**Garay:1999:AFO**


**Garay:1999:AOC**


**Goresky:1995:FRB**


**Gurses:1995:VCT**


**Goldreich:1996:CZP**


**Glenn:1998:RNE**

REFERENCES


REFERENCES


REFERENCES


[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic


Gennaro:1995:VSS


Girault:1997:SFR


GomezdeSilvaGarza:1999:EAC


Grohe:1999:DDC


Galvin:1995:RSM


Griwodz:1998:PVE


Ghazi-Moghaddam:1994:OCH

REFERENCES

(Goldwasser:1985:PSS)
[Goldwasser:1985:PSS]

(Goldwasser:1988:DSS)
[Goldwasser:1988:DSS]

(Good:1945:GRT)
[Good:1945:GRT]

(Groote:1998:CVP)

(Goldreich:1987:HPM)
[Goldreich:1987:HPM]
Goldreich:1991:PYN

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

Gemmell:1994:CIA


Goettfert:1995:GLB


Gray:1995:PCT


Guerrero:1995:CHB

F. Guerrero and J. M. Noras. Customised hard-

**Goldwasser:1993:ISN**


**Goldreich:1996:SPS**


**Golic:1995:EPC**


**Golic:1996:CCC**


**Goguen:1999:IAS**

J. Goguen. An introduction to algebraic semiotics, with application to user interface design. *Lecture Notes...

**Goldomb:1967:SRS**


**Goldomb:1982:SRS**


**Goldwasser:1984:PET**


**Goldwasser:1990:SPS**


**Goldberg:1990:MUA**

REFERENCES


REFERENCES


Goldreich:1997:FMCa

Goldreich:1997:FMCb

Goldwasser:1997:NDC

Goldwasser:1998:C

Golic:1997:CAA

Golic:1998:RAS

Goldreich:1999:MCP
Oded Goldreich. Modern cryptography, proba-
REFERENCES


REFERENCES

Goodman:1996:LPS

Gordon:1985:SPE

Gordon:1993:DDT

Gordon:1993:DLU

Goth:1999:NBG

Guajardo:1997:EAE
REFERENCES


REFERENCES


Ghodosi:1998:CCS


Gore:1998:SDC


Gabadulin:1991:INC


Gleason:1985:ECP


G Guillou:1995:ACE

Louis C. Guillou and J.-J.

Gennaro:1997:HSD

Gray:1982:ICT
Grantham:19xx:FPP


Goeker:1999:DUC


Grehan:1990:CDE


Greenfield:1994:DPP


Grover:1982:CP


Grosek:1994:RCR


Grover:1998:FCP

REFERENCES

Goldschlag:1996:HRI


Grundler:1984:DEH


Grusho:1998:SCI


Gaines:1978:SSP


Grollmann:1984:CMP


Grollmann:1988:CMP


Girault:1994:LCH


Giddy:1994:ACT


Gobioff:1996:SCH


Gramata:1994:MMD


Grehan:1994:BCRa

REFERENCES

Gotoh:1990:MRR

Guarini:1904:MTT

Guan:1987:CAP

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

Guarino:1999:RIC

Gudes:1980:DCB

Guenther:1998:E

Guergens:1998:SLF
REFERENCES

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


REFERENCES


Goldberg:1996:RNB

Gao:1999:RDF

Gamow:1958:CAP
George Gamow and Martynas Yčas. The cryptographic approach to the problem of protein synthesis. In *Das Universum. Unser Bild vom Weltall. (German) [The Universe. Our picture of the Universe]*, page ???. Wiesbaden, Germany, 1958.

Galil:1987:PEA

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

Gylden:1933:CCB

Gylden:1936:AMC

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


[HAHH94] Lance J. Hoffman, Faraz A. Ali, Steven L. Heckler, and Ann Huybrechts. Cryptography policy. *Com-
REFERENCES


Johan Hästad. One-way permutations in NC^0. *Information Processing Letters*, 26(3):153–155, Novem-


Hawkes:1998:DLW


Hutter:1999:DCI


Hughes:1999:PFS


Huang:1988:SWP


Hu:1995:YCE


Hwang:1995:SSA


Hwang:1996:DSS

S.-J. Hwang and C.-C Chang. A dynamic secret sharing scheme with

[HCC98]


[Hwang:1998:EMS]


[HCY96a]


[Hernandez:1999:DAV]


[HCDC99]


[Hwang:1998:EMS]


[Hwang:1996:AE]


[He:1996:HFR]


[He:1996:NKE]


[He:1992:IKB]


[He92]

Huang:1998:FAI

Hedberg:1997:FIC

Hartung:1998:DWM

Heidel:1676:JTP

Heideman:1996:SIT
G. H. L. M. Heideman, editor. 17th Symposium on Information Theory in the Benelux, Enschede, The Netherlands,

Heintze:1996:SDF


Heintze:1996:SDF


Heintze:1996:SDF

Hellman:1979:WTI


Hellman:1979:WTI


Hellman:1979:WTI


Hellman:1979:MPK


Hellman:1979:MPK


Hellman:1981:ACA


Hellman:1981:ACA

Held:1993:TSD


Held:1993:TSD

Helleseth:1994:ACE

Held:1998:ARU

Held:1998:LET

Helleseth:1998:E

Henry:1981:BJB

Henry:1982:FDA

Hong:1998:DAS

Herlestam:1978:CRS

Hershey:1981:DLP
J. E. (John E.) Hershey. The discrete logarithm public cryptographic system.
REFERENCES


[HG97a] H. Handschuh and H. Gilbert. chi02 cryptanalysis of the SEAL encryption algorithm. Lecture Notes in
Handschuh:1997:CSE


Hartung:1997:CPV


Hartung:1997:WME


Hartung:1997:DWM


Hartung:1998:WUA


Hoornaert:1985:EHI

Frank Hoornaert, Jo Goubert, and Yvo Desmedt. Efficient hardware implementation of the DES. In Blakley and Chaum [BC85], pages 147–173. CODEN LNCSD9. ISBN 0-
REFERENCES


Haddar:1998:ISI


Hall:1998:RAA


Hinsley:1979:BISb


Hofmann:1994:RQC


Hughes:1998:AJC


Husemann:1999:OTY

[HH99] Dirk Husemann and Reto Hermann. OpenCard: Talking to your smart


REFERENCES


REFERENCES


[Highland:1989:SDI]

[Hig97a]

[Hill:1929:CAA]

[Hill:1931:CCL]

[Hiltgen:1994:CRC]

[Hill:1997:MTY]


[Helm99] D. R. Helman and J. Jaja. Designing practical efficient algorithms for symmetric
REFERENCES


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

Herzberg:19xx:PPK


Herzberg:1995:PSS


Hillenbrand:1999:SDW


Hong:1997:IAU

REFERENCES

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

**Huehnlein:1998:CBN**

[HJPT98a]

[HJPT98b]

[HJTW99]

[HK90]

[HK97]

[HJTW99]

[HJT+96]

[HJPT98a]

[HJPT98b]

[HK90]

[HK97]

[HJT+96]
Alejandro Hevia and Mar- 
cos Kiwi. Strength of 
two Data Encryption Stan-
dard implementations un-
der timing attacks. Lecture 
Notes in Computer Science, 
1380:192–205, 1998. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http://
link.springer-ny.com/link/
service/series/0558/
bibs/1380/13800192.htm;
http://link.springer-ny.com/link/
service/series/0558/papers/1380/13800192.
pdf.

Hevia:1999:STD

Z[HK98]

Alejandro Hevia and Mar-
cos Kiwi. Strength of 
two Data Encryption Stan-
dard implementations un-
der timing attacks. Lecture 
Notes in Computer Science, 
1380:192–205, 1998. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http://
link.springer-ny.com/link/
service/series/0558/
bibs/1380/13800192.htm;
http://link.springer-ny.com/link/
service/series/0558/papers/1380/13800192.
pdf.

Hevia:1998:STD

Z[HK99c]

Shai Halevi and Hugo 
Krawczyk. Public-key cryp-
tography and password pro-
tocols. ACM Transactions 
on Information and Sys-
tem Security, 2(3):230–268, 
August 1999. CODEN 
ATISBQ. ISSN 1094-9224 
(print), 1557-7406 (elec-
acm.org/pubs/citations/journals/tissec/1999-2-
3/p230-halevi/.

Halevi:1999:PKC

Z[HK99d]

Udo Halfmann and Win-
fried E. Kühnhauser. Embed-
ning security policies into a 
distributed computing 
environment. Operating 
Systems Review, 33(2): 
51–64, April 1999. CODEN 
OSRED8. ISSN 0163-5980 
(print), 1943-586X (elec-
tronic).

Halfmann:1999:ESP

Z[HKL94]

John Earl Haynes and Har-
vey Klehr. Venona: de-
coding Soviet espionage in 
America. Yale University 
Press, New Haven, CT, 
USA, 1999. ISBN 0-
300-07771-8. xiii + 487 
pp. LCCN JK2391.C5 H39 
1999.

Haynes:1999:VDS

Z[HK99a]

Alejandro Hevia and Mar-
cos Kiwi. Strength of 
two Data Encryption Stan-
dard implementations un-
der timing attacks. ACM Transactions 
on Information and Sys-
437, November 1999. CO-
DEN ATISBQ. ISSN 1094-
9224 (print), 1557-7406 
(electronic). URL http://
www.acm.org/pubs/citations/journals/tissec/1999-2-
4/p416-hevia/.

Hevia:1999:STD

Z[HK99b]

J. Hromkovic, J. Karhu-
maeki, and A. Lepistoe. 
Comparing descriptive 
and computational com-
plexity of infinite words.
Harpes:1995:GLC


Hachez:1999:IFA


Hall:1999:CS


Haber:1995:HDD


Hofmeister:1997:CKS


Hofmeister:1997:COS


Hall:1998:CS


Tzonelih Hwang, Narn-Yih Lee, Chuan-Ming Li, Ming-Yung Ko, and Yung-Hsiang Chen. Two attacks on Neuman-Stubblebine authentication protocols. *Information Processing Let-*
Hwang:1996:SCW


[HM83]

Hughes:1996:QCU


[HM88]

Hohl:1993:SIH


[HLMW93]

Hunter:1983:ERA


[HLLC96]

Hule:1988:RCW


[HM91]

Hafner:1991:COH

REFERENCES


REFERENCES


Harkavy:1998:IPP


Harper:1993:PKC


Horvath:1994:PPM


Hennicker:1994:BAF


Haastad:1998:SIR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Hand98a] Helena Handschuh and Pascal Paillier. Smart card crypto-coprocessors for public-key cryptogra-


REFERENCES


Hernandez:1998:SML


Hoffstein:1998:NRB


Holland:1982:GSA


Hwang:1990:PKA


Hollander:1996:KWS

REFERENCES

[Harrison:1976:POS]

[Hruby:1995:QDQ]

[Hruby:1995:QCQ]

[Hruby:1996:SCI]

[Hruby:1998:TQC]

[Hruby:1999:SUD]

[Hernandez:1999:CLM]

[Haastad:1985:CST]
J. H˚ astad and A. Shamir. The cryptographic security of truncated linearly related variables. In ACM

Hammer:1987:EUH


Hardjono:1989:TCB


Hardjono:1990:SKS


Haber:1991:HTD


Hinsley:1993:CIS


Hardjono:1994:AMS


Handel:1996:HDO

Hardjono:1996:RKA


Hall:1997:REG


Helme:1997:SFF


Harasawa:1999:CMF


Hornauer:1994:MCA


Hauser:1996:MBI


Hinsley:1979:BISa

additional author C. A. G. Simkins.

Heys:1995:ACS


Hada:1998:EZP


Huber:1998:MAE


Huang:1999:RBO

slides or paper for the conference talk are available.


Hulaas:1998:MLI


Hardy:1975:ITN


Hartnell:1976:PFM


Hardy:1979:ITN


Huthnance:1988:UPP


Hotchkiss:1991:ASI


Hsu:1997:DWV

Hsu:1998:DBW


Hsu:1998:MWD


Hwang:1998:AUS


Hwang:1991:CGO


Hwang:1992:AOT


Hwang:1992:EIB


Hwang:1992:EIK


Hwang:1992:PGO

Hwang:1993:SSD


Hwang:1997:CKA


Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE


Hall:1998:BPPa


Hall:1998:BPPb

REFERENCES


REFERENCES

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

Hsieh:1999:OWH

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

Hardjono:1993:PDM

A practical digital multisignature scheme based on discrete logarithms. Lecture
Notes in Computer Science, 718:122–??, 1993. CODEN LNCS9D.
ISSN 0302-9743 (print), 1611-3349 (electronic).

Ibbotson:1997:CPI

ISSN 0140-511X.

Anonymous:1993:CCA


URL http://www.ibm.net.il/ibm_il/int-lab/Proactive/home.html.

IEEE:1974:ASS

[IEE74] IEEE, editor. 15th Annual Symposium on Switching and Automata Theory, October 14–16, 1974, the University of New Orleans. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1974.

IEEE:1979:ASF


IEEE:1980:PSS

REFERENCES


REFERENCES


IEEE:1988:FAC


IEEE:1989:ASF


IEEE:1991:PSA


IEEE:1992:CSF


IEEE:1992:PEA

IEEE:1992:PIC


IEEE:1992:PII


IEEE:1993:FIW


IEEE:1993:ICS


IEEE:1993:PNA

IEEE:1994:IW


IEEE:1994:CPN


IEEE:1994:PSH

REFERENCES


REFERENCES


IEEE:1997:IWS


IEEE:1997:ASF


IEEE:1997:IICa


IEEE:1997:ICI


IEEE:1997:PIS

IEEE:1997:PICa


IEEE:1997:PICb


IEEE:1998:ASF


IEEE:1998:HCC

REFERENCES

Auditorium, Stanford University, Palo Alto, California. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN ???. LCCN ???.


[IEEE:1998:IIF]


[IEEE:1998:LPA]


[IEEE:1999:ASF]
REFERENCES


REFERENCES


REFERENCES

Iwamura:1993:HIM


Iwamura:1993:HSI


Impagliazzo:1992:PGP


Impagliazzo:1989:ECS


Ito:1999:DPS


Ingemarsson:1998:E


Instenes:1995:MAA

REFERENCES

IRD:1979:DVE

IRD:1981:DE

IRD:1981:DTV

IRD:1984:DTV

IRD:1987:DTV

IRD:1988:DTV

Anonymous:1991:IIS

IRD:1991:DFV

Itoh:1994:LDS
References


Impagliazzo:1989:LPC


Ing:1999:SRT


Imai:1993:ACA


Irwin:1998:RWD


Ingemarsson:1991:PSS

REFERENCES

Ikram:1997:CSE


Ikram:1999:UIN


Ito:1987:SSS


ISO:1997:ITS


Isselhorst:1990:UFP


Itoh:1991:CFI


Iversen:1991:CSC

Kenneth R. Iversen. A cryptographic scheme for computerized general elec-
REFERENCES

Ingemarsson:1981:UAS


Imai:1998:PKC


Imai:1999:PKC


Jaburek:1990:GGP


Jackson:1987:NTS

T. H. Jackson. From number theory to secret codes.
REFERENCES


Jackson:1990:SITa


Jackson:1990:SITb


Jackson:1996:AAC


Jakobsson:1995:BUU


Jakobsen:1998:CBC


Jakobsen:1999:HOC


Jakobsson:1999:MCM


Jan:1998:PWP


Jeffery:1986:GCC


Jensen:1999:GDT


Jenkins:19xx:IFC

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

Jevons:1874:PS


Joyce:1990:IAB

[JG90] Rick Joyce and Gopal Gupta. Identity authentication based on keystroke


Neil F. Johnson and Sushil Jajodia. Steganalysis of images created using current steganography soft-

**Johansson:1999:FCA**


**Johansson:1999:IFC**


**Jakobsen:1997:IAB**


**Jun:1999:IRN**


**Jonker:1999:VTK**


**Jones:1975:ESP**


**Johnson:1994:HKD**

D. Johnson, A. Le, W. Martin, S. Matyas, and J. Wilkins. Hybrid key distribution scheme giving key record recovery. *IBM Technical Dis-
REFERENCES

Juels:1997:SBD


Jurgensen:1984:SRI


Jackson:1993:CAG


Janwa:1996:MPK


Johnson:1996:AEE


Jurisic:1997:ECC


Jakobsson:1999:IMI

REFERENCES


REFERENCES


Johnson:1996:LP

Johnson:1997:SP

Johnson:1999:LES

Jolitz:1995:PB

Jones:1978:WWB
R. V. (Reginald Victor) Jones. *The Wizard War:


REFERENCES

Johansson:1995:CIA


Jakobsson:1999:SAE


Jiwa:1994:BBA


Jan:1996:SIE


Jan:1997:SEV


Jan:1997:SIE


Juenemann:1981:DES

Robert R. Juenemann. The Data Encryption Standard

Juels:1999:TTS


Jung:1987:IRC


Jung:1988:IRC


Jungnickel:1996:DFG


Jung:1999:EMA


Jurgen:1986:SEI


Jutla:1998:GBA


Just:1996:AMP

[M. Just and S. Vaudenay. Authenticated multi-party key agreement. Lecture Notes in Computer Science, 1163:36–??, 1996. CODEN LNCSD9. ISSN 0302-9743]
REFERENCES

Jakubowski:1998:CSP


Jeannerod:1998:GEE


Ji:2001:CAF


Jakobsson:1996:OAB


Joye:1998:IBS

REFERENCES


[Kah96a] D. Kahn. The history of steganography. In Anderson [And96c], pages 1–5. CODEN
REFERENCES

Kahn:1996:CSS


Kahn:1998:EC


Kahn:1998:PHI


Kahn:1998:RMU


Kak:1983:EMP


Kak:1984:MPK


Kak:1985:ECC


Kaliski:1993:ZBA


Kaliski:1995:MIA


Kaliski:1997:IPS


Kaliski:1997:PNG

Burt Kaliski. PKCS: The next generation, chapter

Kaliski:1997:ACC


Kaliski:1998:C


Kaliski:1998:RPRa

B. Kaliski. RFC 2313: PKCS #1: RSA encryp-
REFERENCES


[Kan96] Thomas Kaneshige. Indust-
try trends: Cyberwar; Clipper chip; network comput-
 ers. Computer, 29(7):20–23, July 1996. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (elec-
 tronic). Contains news brief: Lots of Java brewing at conference.

Kaps:1998:HSF


Karger:1985:ADA


Karger:1986:ADA


Karger:1987:LDP


Karger:1989:CBP


Kari:1989:OCP

Jarkko Kari. Observations concerning a public-key cryptosystem based on iterated morphisms. Theoret-

Karkare:1996:SEA

Sonia Karkare. Secure email architecture using PGP at the Timken Company. Thesis (M.S.), Department of Mathematical and Com-
 puter Science, Kent State
REFERENCES

Kasiski:1863:GDG
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
Saad M. Kalipha, Ja-
far Wadi Abdul-Sada, and Hussain Ali Hussain. New public-key cryptosystem. [Kau96]

Katzan:1977:SDE
Harry Katzan, Jr. The Standard Data Encryption Algorithm. Petro-
016-0. viii + 134 pp. LCCN QA76.9 .A25K37.

Katsikas:1997:CMS

Kaufman:1993:RDD

Kaufman:1996:DWC
REFERENCES


Kawai:1987:LAI

Kay:1995:CTE

Krishnakumar:1992:HTE

Krawczyk:1996:HKM

Krawczyk:1997:RHK

Klein:1989:STR

Karp:1988:SDN
REFERENCES

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

Kunkelmann:1997:EDV


Kao:1995:ESA


Krajewski:1994:ASC


Krajewski:COMPSYS-7-1-75

Kam:1978:SDS


Kam:1979:SDS


Khinchin:1997:CF


Keating:1999:PAA

Geoffrey Keating. Performance analysis of AES candidates on the 6805 CPU
REFERENCES


Kelsey:1999:KSWb


Kemp:1988:EEF


Kemmerer:1989:AEP


Kemppainen:1999:DMM


Kent:1993:IPE


Kent:1995:PCW

REFERENCES


REFERENCES


Kobara:1996:LVS


Kobara:1997:SSM


Katsumoto:1999:DPL


Kiefer:1998:WMV


Kilian:1988:FCO


Kim:1993:CLB


Kippenhahn:1997:VBG

Kippenhahn:1999:CBH


Kippenhahn:1999:VBG


Kirby:1995:RPK


Kak:1977:SEU


Kocher:1999:DPA


Kurosawa:1995:NBA


Kuwakado:1996:NRT


Kelm:1997:NK

 REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/
bibliography/062338.html

Kunihiro:1998:ECN

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

[KK99a] Oliver Kommerling and
Markus G. Kuhn. Design
principles for tamper-
resistant Smartcard pro-
cessors. In USENIX
[USE99c], page ?? ISBN
1-880446-34-0. LCCN
URL
http://www.usenix.org/publications/library/
proceedings/smartcard99/
kommerling.html

Koren:1999:ISC

[KK99b] Israel Koren and Peter
Kornerup, editors. 14th
IEEE Symposium on
Computer Arithmetic: pro-
cedings: April 14–16, 1999,
Adelaide, Australia. IEEE
Computer Society Press,
1109 Spring Street, Suite
300, Silver Spring, MD
20910, USA, 1999. ISBN
0-7803-5609-8, 0-7695-0116-
8, 0-7695-0118-4. ISSN
1063-6889. LCCN QA76.6
S887 1999. URL
http://
/computer.org/conference/
home/arith/; http://
www.ecs.umass.edu/ece/
arith14/program.html.IEEE
Computer Society Order
Number PR00116. IEEE
Order Plan Catalog Number
99CB36336.

Koshelev:1999:EAM

[KKL99] Misha Koshelev, Vladik
Kreinovich, and Luc Longpré.
Encryption algorithms made
natural. SIGCSE Bul-
letin (ACM Special Inter-
est Group on Computer Sci-
ence Education), 31(4):50–
51, December 1999. CO-
DEN SIGSD3. ISSN 0097-
8418 (print), 2331-3927
(electronic).

Kurosawa:1991:GPK

[KKOT91] Kaoru Kurosawa, Yutaka
Katayama, Wakaha Ogata,
and Shigeo Tsujii. General
public key residue cryptosystems
and mental poker
protocols. Lecture Notes
in Computer Science, 473:
374–388, 1991. CODEN
LNCSD9. ISSN 0302-9743
(print). 1611-3349 (elec-
tronic). URL
http://link.springer-ny.com/
link/service/series/0558/
bibs/0473/04730374.htm;
http://link.springer-ny.com/link/service/series/
Kabatianskii:1997:DSS


Kramer:1999:FCD


Kothari:1984:CMW


Kilian:1994:FKE


Kilian:1995:FCR


Knudsen:1995:NAA


Klein:1990:FCS

Daniel Klein. Foiling the cracker: a survey of, and improvements to, password security. In USENIX Association [USE90], pages 5–

**Kannan:1988:PFN**


**Kannan:1988:PFN**


**Klupsch:1999:ARR**


**Kurosawa:1988:CSP**


**Kurak:1992:CNI**


**Kang:1993:PRR**


**Kim:1996:ACA**

REFERENCES


Knudsen:1996:IDA


Knudsen:1996:IDA

Knudsen:1998:SMD


Kaufman:1998:DWF

Kasahara:1999:NPK


Kasahara:1999:NPK
REFERENCES


Knudsen:1999:CIS


Kohlas:1999:RAP


Koscielny:1999:QBP


Kanda:1998:ECC


Kobayashi:1999:FEC


Konheim:1980:ICP


Koyama:1991:NPK

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


Kande:1999:AUD


Karn:1995:REC


Karn:1995:RET


Kohl:1993:RKN


Kno:1979:AEO


Kohl:1994:EKA

REFERENCES


Knuth:1969:SNM


Knuth:1969:SA


Knuth:1973:FA


Knuth:1980:DLC

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

Knuth:1985:DLC


Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb


Knudsen:1993:ICS

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

Knudsen:1993:CLc

Knudsen:1993:CLA

Knudsen:1994:PSF

Knudsen:1994:BCA

Knudsen:1995:NPW


Knudsen:1998:BCS

Knudsen:1998:DBC

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

**Knudsen:1999:CBC**


**Knudsen:1999:FSE**


**Kurosawa:1995:CIS**


**Kurosawa:1995:CBA**


**Kurosawa:1996:CLB**


**Kurosawa:1997:CLB**


**Koblitz:1987:CNT**

Neal Koblitz. *A course in number theory and cryptography*, volume 114 of *Graduate texts in mathematics*. Springer-Verlag, Berlin, Germany / Heidel-
Koblitz:1987:ECC

Koblitz:1990:FJS

Koblitz:1991:CCG

Koblitz:1991:CEC

Koblitz:1991:JSI

Koblitz:1994:CNT

Koblitz:1996:ACC
Neal Koblitz, editor. Advances in cryptology, CRYPTO ’96: 16th annual international cryptology conference, Santa Barbara, California, USA, August 18–22, 1996: proceedings, volume 1109 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London,
REFERENCES


Kobayashi:1997:DWH


Kob97

Koblitz:1998:AAC


Kob98a

Koblitz:1998:C


Kobara:1999:PMA

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

Standards and Technology

Kochanski:1989:HSI


Koc:1994:HSR


Koch:1995:CDR


Koc:1996:RHI


Kocher:1996:TAI


Koops:1997:CRE


Kopooshian:1997:DCE


Kornerup:1993:HRM


Korner:1996:PC


Koscielny:1983:PRD

REFERENCES


Kurosawa:1994:NSS


Koshiba:1997:CLT


Koshiba:1999:UPN


Kothari:1985:GLT


Kurosawa:1995:LEAa

REFERENCES


References


Koz:1996:RSS


Kim:1989:PRP


Kwan:1993:GPT


Krajicek:1995:SCC


Knudsen:1996:HFB


Knudsen:1996:DSK


Knudsen:1997:FSH

Lars Ramkilde Knudsen and Bart Preneel. Fast and secure hashing based on codes. Lecture Notes in Computer Science, 1294:
REFERENCES


Kilian:1998:IE


Kaps:1999:FIF


Koc:1999:CHE


Kipnis:1999:UOV


Karhumaeki:1999:CSI


Kaliski:1994:FBC

527

REFERENCES

Kaliski:1994:LCU

Kushilevitz:1994:RRT

Kaliski:1995:LCU

Kaliski:1995:MAM

Kaliski:1995:SUR

Kaliski:1996:MEW
Kilian:1996:HPA


Knudsen:1996:NAL


Kankanhalli:1998:CBW


Knudsen:1999:DFC


Kolliopoulos:1999:NLT


Krause:1984:DEI


Kranakis:1986:PC


Krawczyk:1990:HPC


Kra90

Krawczyk:1993:DSA


Kra93

Krawczyk:1994:SSM


Kra94a

Krawczyk:1994:LBH


Kra94b

Krawczyk:1995:NHF

REFERENCES

Krawczyk:1998:ACC


Krawczyk:1999:BCC


Krawczyk:1999:BCC


Kruh:1998:WWS


Kesdogan:1998:DTP


Kesdogan:1998:DTP


Kumar:1999:CCB


Kruh:1998:WWS

REFERENCES


REFERENCES


Kemp:1996:CPC

Kemp:1996:PRM

Kemp:1997:MFC

Kelsey:1999:NDA

Kelsey:2000:YND
REFERENCES


Kim:1996:EIE


Kehne:1992:NBP


Knowles:1992:AFC


Kelsey:1996:KCI


Kelsey:1997:RCB


Kelsey:1997:RKC


Kelsey:1998:PICa

J. Kelsey, B. Schneier, and D. Wagner. Protocol interactions and the chosen protocol attack. Technical


REFERENCES


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


Kuhn:1998:CIS


Kuijk:1991:RSE


Kukorelly:1999:VCH


Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC


Kumar:1997:CSI

Kummert:1998:RPT


Kuo:1990:TEC


Kurosawa:1994:NBA


Kearns:1989:CLL


Kearns:1994:CLL


Kaul:1999:IBP

Kirstein:1992:PAS


Konrad:1999:SDK


Kwan:1993:SAD


Kwan:1997:DIE


Kaliski:1995:SRE


Kaliski:1995:DLC

REFERENCES

...with the IEEE Computer Society Technical Committee on Security and Privacy.

**Kaliski:1997:SRE**


**Kaliski:1998:SRE**


**Kaliski:19xx:DLC**

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

**Kwok-Yan:1992:TAD**


**Kurosawa:1998:SBC**


**Kwok-Yan:1992:FAA**


**Kasami:1982:KMS**


**Koch:1995:TRH**

E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In Pitas [Pit95], pages 452–455. LCCN ???? URL
REFERENCES


Lagarias:1990:PNG


Lai:1992:DSB

Xuejia Lai. On the design and security of block ciphers. Hartung-Gorre Verlag, Konstanz, Switzerland, 1992. ISBN 3-89191-573-X. xii + 108 pp. LCCN QA76.9.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 iterating a weak round function several times are considered. Four basic constructions for the round function of an iterated cipher are studied.”.

Lai:1995:ALS


Lakshmivarahan:1983:APK


Lampson:1973:NCP


Lamport:1981:TNP

REFERENCES

770–772, November 1981. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


[Lan98] P. Landrock. TTPs overview — concepts and


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

REFERENCES


[LCCN QA 76.76 O63 U83 1989.]


[LC94]


[Lomas:1995:RBH]


[Lee:1996:IAP]

REFERENCES

Lin:1996:CBC


Lee:1997:AES


Lou:1997:PTL


Lin:1995:NPK


Lin:1999:SOE

References


REFERENCES


[Leclerc:1989:CRM]


[Lee:1995:NSI]


[Leech:1996:RUP]


[Lee:1999:GIC]

Annabelle Lee. Guideline for implementing cryptography in the Federal Govern-

[Leighton:1979:BRA]


[Leighton:1979:BRB]

REFERENCES


Leiss:1980:NSS


Leipold:1999:K


Leiserson:1999:ITD


Lempel:1979:CT


Lennon:1978:CAI


Lenstra:1987:FIE


Lenstra:1990:PT


Lennox:1993:ES

G. Lennox. EDI security. Lecture Notes in Computer
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lenstra:1996:GSD

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

Lenstra:1996:VNS

CODEN IIEASM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Lenstra:1998:GRM

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

Lenstra:1999:EIB

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

Lenzerini:1999:DLT

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

Lercier:1997:FGR

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

Levine:1958:VMS

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

Levine:1961:SAH

CODEN MCMPAF. ISSN 0025-5718 (print), 1612-7924 (electronic).

Lenstra:1999:VNS
553

References

Levine:1961:SECa


Levine:1961:SECb


Levine:1983:USC


Levin:1985:OWF


Levine:1991:USC


Lewin:1978:UGW


Lewin:1982:AMC


Lewis:1992:SCP

2. v + 253 + 12 pp. LCCN ????

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


[Chi-Sung Laih and Lein Harn. Generalized threshold cryptosystems. Lecture Notes in Computer Science, 739:159–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).]


Lin:1995:FRS


Lichota:1996:VCP


Li:1995:TSW


Li:1995:TMS


Li:1994:RTR


[Lie93] Armin Liebl. Authentication in distributed systems:

**Lim:1998:CNB**


**Lim:1999:RVC**


**RFC0989**


**RFC1040**

REFERENCES


[Jin89a]


[Lin93a]


[RFC1421]

Lin:1993:RCA


Lin:1996:IRC


Lin:1996:RKV


Linnartz:1998:TCC


Lippit:1993:PIC


Lipton:1994:CNF


Abeles:1998:KVC

Francine Abeles Stanley H. Lipson. The key-vowel ci-


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


REFERENCES

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

Landau:1994:CPP


Linnartz:1998:MFA


Lenstra:1993:DNF


Liaw:1993:OAA


Lim:1994:AMA

Chae Hoon Lim and Pil Joong Lee. Another method for attaining security against adaptively chosen ciphertext attacks. Lecture Notes in Computer Science, 773:420–??, 1994. CODEN LNCS9. ISSN 0302-9743
REFERENCES


[LL94b]


[LL95a]


[LL97a]


[LL97b]

(1998) Chae Hoon Lim and Pil Joong Lee. A study on the proposed Korean Digital Sig-


[Lenstra:1990:NFS] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Man-


**Lia:1991:PNB**


**Longley:1993:TNC**


**Lai:1993:HFBa**


**Longley:1993:TNC**


**Lai:1993:HFBb**

REFERENCES

Leighton:1995:LPF

Low:1996:MCP

Lamersdorf:1998:TDS

Low:1998:PCT

Low:1995:DMI


Lomet:1983:HPU


Lomas:1994:ENT


Lomas:1997:SPI


Long:1991:PAA


Long:1992:UDE


Loshin:1997:CGP

Pete Loshin. Cryptography gets personal — six products that promise to secure your data, both over the Internet and on your desktop.
REFERENCES


Loshin:1998:PEC


Lowe:1995:ANS


Lowe:1996:BFN


Loxton:1990:NTC


Lam:1999:ACA


Luciano:1987:CCC

Leszczynski:1994:SDA


Li:1999:CKA


Lacy:1998:IPP


Luby:1986:PRP

REFERENCES


REFERENCES


[LS98a]

Lu:1989:SCI


[LS89]

Lloyd:1992:RPA


[LS92]

Lin:1997:LNU


[LS97]

Luby:1998:CBB


[LS98b]
Lamport:1982:BGP

Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4 (3):382–401, July 1982. CODEN ATPS DT. 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 showed that the problem is solvable for any $n \geq t > 0$, where $n$ is the total number of processes and $t$ is the number of faulty processes.

Livens:1995:CCI


Leung:1985:SCT


Leong:1991:UPE


Linnartz:1998:MPM

J. P. M. G. Linnartz and J. C. Talstra. MPEG PTY-marks: Cheap detection of embedded copyright
REFERENCES


REFERENCES


[Luc98c] Stefan Lucks. Attacking triple encryption. In Vau-

Lucks:1999:SBB


Lucks:1999:SBC


Lucks:1999:ARK


Ludwig:1997:CQA


Lujan:1998:AMDa


Lujan:1998:AMDb


Lunt:1990:EK

Lutz:1998:NBM


Linnartz:1998:ASA


Langelaar:1996:CPM


Langelaar:1997:RLM


Long:1988:DLH


Li:1991:JAE

REFERENCES

[**Lervik:1996:IDS**]


[**Lenstra:1995:KES**]


[**Laih:1993:SAS**]


[**Lodge:1994:SCC**]


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


Madsen:1996:CCL


Madsen:1997:KEE


Madsen:1998:CPH


Madsen:1998:CPU


Madsen:1998:EDR


Madsen:1998:ELP

Madsen:1998:FFE

Madsen:1998:NCK

Madsen:1998:USC

Madsen:1999:MBF

Madsen:1999:NCO

Mae:1998:TPH

Mah:1996:CBK
REFERENCES

McDonald:1995:OTP


Mandelbrot:1960:BRJa


Manasse:1995:MPE


Mao:1997:PVP


Mao:1998:GCS

REFERENCES

Marsh:1970:CSS

Marsh:1970:MEC

Marion:1976:ANB

Marion:1995:WGT

Marks:1995:PEI

Markoff:1996:MIS

Martin:1997:IEI

Markantonakis:1998:CSM
C. Markantonakis. The case for a secure multi-application smart card operating system. Lecture Notes in Computer Science, 1396:188–??, 1998. CODEN
REFERENCES

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


REFERENCES


Massacci:1999:DRT


Massey:1999:OSD


Matyas:1991:KHC


Matsumi:1993:LCM


Matsumi:1994:FEC


Matsumi:1994:LCM

Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Helleseth [Hel94], pages 386–397. CODEN LNCS.D9. ISBN 3-
REFERENCES

Matsui:1995:CBO


Matsui:1996:NSB


Matthews:1996:SRN


Matsui:1997:NBE


Matsumoto:1998:HCC


Matsumura:1999:DTE


Mauborgne:1914:APC

Joseph O. Mauborgne. An advanced problem in
REFERENCES


[Mau93a] U. M. Maurer. Protocols for secret key agreement by

**Maurer:1993:RIT**


**Maurer:1994:TEB**


**Maurer:1996:UGT**


**Maurer:1996:ACE**


**Maurer:1997:ITS**

Ueli M. Maurer. Information-theoretically secure secret-
key agreement by NOT authenticated public discussion. In Fumy [Fum97],
pages 209–225. CODEN LNCSD9. ISBN 3-540-62975-0. ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
E964 1997. URL http://link.springer-ny.com/ link/service/series/0558/1

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

Mauriello:1997:TTC

Ermelindo Mauriello. TCFS: Transparent cryptographic file system. Linux Journal,
40:??, August 1997. CODEN LIJOEM. ISSN 1075-3583 (print), 1938-3827

Mauth:1997:SOC

Rainer Mauth. Steganography overcomes cryptography restrictions. BYTE
Magazine, ??(??):??, January 1997. CODEN BYTEDJ. ISSN 0360-5280
(print), 1082-7838 (electronic). URL http://


Maurer:1998:E

U. Maurer. Eurocrypt ’96. Lecture Notes in Computer Science, 1440:
199–206, 1998. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

Maurer:1999:IC

1999 Bar.

Maurer:1999:ITC

U. Maurer. Information-theoretic cryptography. Lecture Notes in Computer
Science, 1666:47–64, 1999. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic).

Maxemchuk:1994:EDD

N. F. Maxemchuk. Electronic document distribution. AT&T Technical Journal,
73(5):73–80, September/October 1994. CODEN ATJOEM. ISSN
2376-676X (print), 8756-2324 (electronic). URL
REFERENCES


REFERENCES

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


McCurley:1990:DLP


McCurley:1990:OEC


McCurley:1996:CIL


McCane:1998:ICS


Millan:1999:BFD


McHugh:1992:EBD

J. McHugh. An EMACS based downgrader for the SAT. In IEEE [IEE92b], pages 228–237. ISBN 0-8186-3115-5 (paperback), 0-
REFERENCES

8186-3116-3 (microfiche), 0-8186-3117-1 (casebound).

McIvor:1985:SC


McKee:1999:SFF


McLaughlin:1992:YAM


McMahon:1996:RGA


Madson:1998:REC


Main:1999:HCB


Moreno-Diaz:1994:SIE

REFERENCES


Meijer:1981:NCM

REFERENCES

August 13, 1981. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [LM80, Hel81].

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

Meijer:1985:MEN

Meijer:1992:SSA

Meijer:1994:SIB

Meierhofer:1996:PGP

Meijer:1996:GFC

Meinel:1998:HHB
Carolyn P. Meinel. How hackers break in ... and how they are caught: Port scanners, core dumps and buffer overflows are but a few of the many weapons in every sophisticated hacker’s arsenal. still, no hacker is invincible. Scientific American, 279(4):98–105, October 1998. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Mendelsohn:1939:CC

[I]S. Galland, Bibliography of ... cryptology, 1945, p. 124.

Mendelsohn:1989:CWI


Mendez:1991:AKA


Menezes:1993:ECP


Menezes:1995:ECC


Menicocci:1995:SAC


Mersenne:1644:CPM

the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

---

**REFERENCES**

598

---

the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

---

**REFERENCES**

598

---

the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

---

**REFERENCES**

598

---

the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

---

**REFERENCES**

598

---

the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

---

**REFERENCES**

598

---

the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, but could not test this claim. Euler showed in 1750 that $M(31)$ is prime. Lucas showed in 1876 that $M(127)$ is prime. Pervouchine showed in 1883 that $M(61)$ is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that $M(89)$ and $M(107)$ are prime, both missed by Mersenne. By 1947, it was known that the correct list is $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing 4,053,946 digits.

---

**REFERENCES**

598


REFERENCES

Abstracts/0001-0782/163380.html.


Murino:1995:RNU


Mihaljevic:1991:CCP


Mackenzie:1998:LPS


Merkle:1978:HIS


Merkle:1981:SME

REFERENCES

001-0782 (print), 1557-7317 (electronic).

Michels:1996:RDS


McPherson:1998:CRH


Majzik:1996:MCU


Matsumoto:1990:EAC


Moulin:1999:ECG


Michener:1988:TSK

John R. Michener. A tool


[Donald D. Millikin. Elementary cryptography and cryptanalysis, volume 56 of A Cryptographic series.]

REFERENCES


Millikin:1943:ECCb


Millikin:1943:ECCc


[Mill86]

Millen:1987:CCC


[Mill87a]

Miller:1986:UEC

REFERENCES

Millikin:1992:ECC

Miller:1995:HWK

Millan:1996:LOA

Miller:1996:CME

Matsumoto:1993:VIA

Mintzer:1997:EIDa

Misarsky:1997:MAU


Masakatu Morii and Masao Kasahara. Perfect staircase profile of linear complexity for finite sequences.
REFERENCES


Moskowitz:1994:CCH


Mazieres:1999:SKM


Maibaum:1999:SRS


Miyazaki:1999:TFI


Monge:1967:NMC


Maulucci:1987:HAC


Mao:1998:CPO


Matyas:1991:KSB


Muffett:1995:BPK


Meadows:1987:MSA


Meyer:1982:CND


Moler:1983:SVA


Matyas:1978:GDI

REFERENCES

[MM90a] Spyros S. Magliveras and Nasir D. Memon. The linear complexity profile of cryp-

[MM90b] Spyros S. Magliveras and Nasir D. Memon. Properties of cryptosystem PGM.
0302-9743 (print), 1611-3349 (electronic).

[MM92a] I. S. Moskowitz and A. R. Miller. The channel capacity of a certain noisy
1343, 1992. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). URL

[MM92b] I. S. Moskowitz and A. R. Miller. The influence of delay on an idealized
(paperback) 0-8186-2826-X (microfiche) 0-8186-2827-8 (casebound). LCCN QA

[MM94] A. Moldovyan and N. Moldovyan. Fast software encryption sys-
tem based on local pseudo-

[MM95] C. Meadows and I. Moskowitz. Covert channels — a con-
ISBN 3-540-61996-8 (soft-
cover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A251541.1
REFERENCES


John Doe

REFERENCES


Mock:1997:BDS


Mohtashemi:1992:CHC


Matsumoto:1982:DTL


Mok:1997:KNF


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

Moldovyan:1998:NEP


Morita:1991:SCT


Montgomery:1985:MMT

REFERENCES


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

Morris:1992:FMC


Morris:1992:FMC

Morgan:1997:PAM


MorenoDiaz:1998:NCC


Morgan:1997:PAM

Moskowitz:1998:C


Mosses:1999:CGT


Moura:1999:PAP

REFERENCES

Mullin:1988:ONB


Moynihan:1998:SAE


Mevis:1986:SCP


McInnes:1991:IPK


Milidiu:1999:EIW


Mayerwieser:1995:THS


Moller:1994:RSW


REFERENCES

Brook, Stony Brook, NY, USA, 1995. x + 213 pp.


[MS81] C. Müller-Schloer. A microprocessor-based cryptoprocessor. *IEEE Mi-
REFERENCES

Moore:1987:CSK


Meier:1990:NCC


Montgomery:1990:FEP


Meier:1991:CPC


Meier:1993:EMC


Massey:1994:FTA

James L. Massey and Shirlei Serconek. A Fourier transform approach


Silvio Micali and Ray Sidney. A simple method for generating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems. Lecture Notes in
REFERENCES

Mambo:1998:NCB


Michels:1998:GCS


MacKenzie:1999:AIH


Maitra:1999:HNR


Miyazaki:1999:KGD


McLeod:1990:VLD


Miksch:1999:ASQ

S. Miksch, A. Seyfang, W. Horn, and C. Popow. Abstracting steady qualitative descriptions over time
REFERENCES


### Moriai:1998:HOD


### McClure:1999:HEN


### Moriai:1999:IAB


### Martin:1997:MAS


### Mizuki:1998:ESK


### Mizuki:1999:DNS


### Martin:1999:BTE

[MSNW99] Keith M. Martin, Rei Safavi-Naini, and Huaxiong Wang. Bounds and techniques for efficient redis-

Mambo:1996:HUT


Madonia:1993:GSP


Michels:1998:SSV


Mullender:1986:DCD


Mullender:1986:DCD

Matsui:1994:VSH

Massey:1995:MCM

Mister:1999:CRL

Marayati:1987:AWA

Moggi:1999:IMS


Mackinnon:1985:OAA


Moriya:1997:DWS


Molva:1992:KAK


Mu:1992:ICS


Mueller:1999:SRB

Muftic:1988:SMC


Muftic:1993:SAO


Mulherin:1981:FDE


Mullin:1984:NMP


Mulligan:1989:UMA


Mullin:1989:LEN


Muller:1999:SRB

REFERENCES

link/service/series/0558/0558/papers/1587/15870135.pdf.

[Mun96]


[Mur99]


[Mus92]


[MUSM98]


[Mur96]


[Mur99]


[Mus92]


[MUSM98]


REFERENCES


MacNish:1998:BRD


Memon:1998:PDM


Merkle:1998:SSR


Maurer:1999:RBB


Malkin:1999:ESG

M. Malkin, T. Wu, and D. Boneh. Experimenting with shared generation
REFERENCES


puter Society Press order number PR9172.


of conference proceedings of CRYPTO and EUROCRYPT.

Mihaljevic:1998:CAB


Merwin:1979:NCC


Nastar:1995:TRD


Nat-Abdesselam:1999:QCA


Naccache:1993:MSF


Nachenberg:1997:CVA

REFERENCES

Naik:1989:CDS


Nalwa:1997:AOS


Nanovic:1936:SWI


Nanovic:1974:SWI


Nastar:1994:VMN


NBS:1977:DES


NBS:1980:MO


NCSOTS:1984:ISR


NIST:1985:FPSa

[Nat85a] National Institute of Standards and Technology.
REFERENCES


REFERENCES

NIST:1994:FPD

NIST:1994:EES

NIST:1994:DES

NIST:1994:DSS

NIST:1995:FPSb

Natarajan:1997:RPK
Balas Natarajan. Robust public key watermarking of digital images. Technical
REFERENCES


[Nat99c] National Institute of Standards and Technology. Status report on the first round of the development of the Advanced Encryp-
REFERENCES


NIST:19xx:AES


Nechvatal:1999:SRF


Neat:1975:NCC


Nechvatal:1991:PC


Nandi:1997:RCT


Nilsson:1978:OST


[Nechvatal:1996:PKB]

[Needham:1994:DSE]


[Neumann:1991:IRCD]

[Neumann:1992:IRF]

[Neumann:1994:IRA]

[Neumann:1995:RCD]


[NH90] Ruth Nelson and John Heimann. SDNS archi-


CODEN MJOKAP. ISSN 0030-1566.

**NIST:1985:FPC**


**Nissan:1989:AIM**


**Nissan:1991:EMF**


**NIST:1992:NCS**


**Nist:1993:DSS**


**NIST:1993:FPS**


**Anonymous:1994:DSS**


**Nisan:1996:ERH**

REFERENCES

Nyberg:1993:PSA

[102x681]


Nakamura:1998:MEC

[208x644]


Nikander:1998:JBC

[208x644]


Nandi:1994:TAC

[208x644]


Nikander:1999:PPD

[102x681]


Nakamura:1988:DRM

[102x681]


Naccache:1994:MSC

[102x681]


Naccache:1996:ACP

[102x681]

David Naccache and David M’Raïhi. Arithmetic co-processors for public-key cryptography: The state


Naccache:1995:CDI


Nozaki:1997:LCS


Noras:1996:CHH


Nicchiotti:1998:NIS


Nobauer:1984:CRS


Nobauer:1985:CRS

Nobauer:1988:CPK


Norman:1973:SWB


Noras:1995:CHHa


Noras:1995:CHHb


Noras:1995:PCE


Naor:1993:PZK


Naor:1997:VAI


Naor:1998:TTT

REFERENCES

Nikolaidis:1998:RIW


Naor:1999:OTA


Niemi:1994:CPV


Nyberg:1995:MRS


Naor:1998:UIS


Needham:1978:UEAa


Needham:1978:UEAb

REFERENCES


Nechaev:1998:DSB


Nguyen:1998:BQS


Nguyen:1998:BSR


Nguyen:1998:CAC


Nguyen:1998:CAD


Nguyen:1999:BQS


Nguyen:1999:HHS


Naccache:1999:HCF

Nieh:1993:MAC

Neuman:1994:KAS

Nadjm-Tehrani:1999:BHO

Nemetz:1988:RLS

Nurmi:1994:CPA

Needham:1997:TE

Naor:1998:ACS
Naor:1989:UOW


Naor:1989:UOH


Naor:1990:PKC


Nyberg:1995:LAB


Nyberg:1998:ACE

REFERENCES


[O’C95] L. O’Connor. A differential cryptanalysis of tree-structured substitution-


Andrew M. Odlyzko. On the complexity of computing discrete logarithms and factoring integers.
In Cover and Gopinath [CG87], pages 113–116.
US$25.00. URL http://
/www.research.att.com/~
amo/doc/arch/factoring.
logs.pdf; http://www.
research.att.com/~amo/
doc/arch/factoring.logs.
ps; http://www.research.
at.com/~amo/doc/arch/
factoring.logs.troff.

[Odlyzko:1987:ACC]
Andrew Michael Odlyzko, editor. Advances in cryp-
tology: CRYPTO '86: pro-
ceedings, volume 263 of Lecture Notes in Computer
Science. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 1987. CO-
DEN LNCS69. ISBN 3-
540-18047-8, 0-387-18047-
8. ISSN 0302-9743 (print),
1611-3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/0558/tocs/t0263.htm;
http://www.springerlink.
com/openurl.asp?genre=
issue&issn=0302-9743&
volume=263. Conference
held at the University of
California, Santa Barbara,

[Odlyzko:1990:RFK]
A. M. Odlyzko. The rise and
fall of knapsack cryptosys-
tems. In Pomerance and
Goldwasser [PG90], pages
75–88. ISBN 0-8218-0155-
4. ISSN 0160-7634. LCCN
QA76.9.A25 C84 1990: QA1
/www.research.att.com/
~amo/doc/arch/knapsack.
survey.pdf; http://
www.research.att.com/~
amo/doc/arch/knapsack.
survey.ps; http://www.
research.att.com/~amo/
doc/arch/knapsack.survey.
troff. Lecture notes pre-
pared for the American
Mathematical Society short
course, Cryptology and
computational number the-
ty, held in Boulder, Colorado,

[Odlyzko:1994:DLS]
A. M. Odlyzko. Discrete
logarithms and smooth
polynomials. In Gary L.
Mullen, P. Shiue, et al., edi-
tors, Finite Fields: The-
ory, Applications and Al-
gorithms, volume 168 of
Contemporary mathematics
(American Mathematical
Society), pages 269–278.
American Mathematical
Society, Providence, RI, USA,

[Odlyzko:1994:PKC]
Andrew M. Odlyzko. Pub-
lic key cryptography. AT&T
Technical Journal, 73(5):
17–23, September/October

Odlyzko:1995:FIF


Odlyzko:1998:C


Oelke:1997:VDE


Okamoto:1993:EDS


O'Connor:1995:UMA


Oehler:1997:RHM


Obana:1996:VIS


Ogata:1996:OSS


Ogata:1998:SBP


Okamoto:1988:DMS


Okamoto:1993:RAC


Okamoto:1993:PSP


Okamoto:1994:DCS

REFERENCES

ny.com/link/service/series/0558/bibs/0839/08390061.

Okamoto:1998:TKR


Ogata:1997:Fta


Okamoto:1998:TKS


Oko98a


Oko97


Oko96


Oko97


Oldehoeft:1984:SSU

Arthur E. Oldehoeft and Robert McDonald. A software scheme for user-controlled file encryption.
REFERENCES


Ohta:1994:DAM


Ohbuchi:1997:WTP


Ohbuchi:1998:WTD


Ozaki:1993:HVP


Omura:1990:PKC

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

Ochi:1998:NSO

REFERENCES


ORuanaidh:1997:RST


ORuanaidh:1998:RST


ORuanaidh:1999:CCP


Oppliger:1996:ASS


Oppliger:1997:ISF


Otway:1987:ETM

Dave Otway and Owen Rees. Efficient and timely


REFERENCES


H. Ong, C. P. Schnorr, and


REFERENCES


Paabo:1993:AD


Padro:1998:RVS


Pai:1996:VIE


Paillier:1998:INS


Paillier:1998:INS


Paillier:1999:EDF


Paillier:1999:LCD


Paillier:1999:TPE


Lawrence C. Paulson. Inductive analysis of the Internet protocol TLS. *ACM
REFERENCES


Poovendran:1999:ITA


Proctor:1999:PC


Piva:1997:DBW


Preneel:1997:CHF


Preneel:1989:CHB


Preneel:1990:CTA

Bart Preneel, Antoon Bosselaers, René Govaerts, and Joos Vandewalle. A chosen text attack on the modified cryptographic checksum algorithm of Cohen and Huang. Lecture Notes in Computer Science, 435:154–??, 1990. CODEN LNCSD9. ISSN 0302-9743


REFERENCES

Pedersen:1995:EPS


Pedersen:1999:SCP


Pelta:1960:SP


Penzhorn:1996:CAS


Perret:1890:RCS


Peralta:1985:TRN


Perry:1988:EBG


Pfitzmann:1995:BEA


Pfitzmann:1996:IHT


Pfitzmann:1996:TTT


Pfleeger:1989:SC


Pfleeger:1995:ULC

REFERENCES

Pomerance:1990:CCNb

Patarin:1997:ACB

Pieprzyk:1996:CBT

Pieprzyk:1997:ACB

Preneel:1991:CRH

Preneel:1992:CSH
B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographically secure hash

Preneel:1993:CHF

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

Preneel:1993:HFB


Preneel:1993:IAH


Preneel:1993:CSI


Preneel:1994:HFB


Pohlig:1978:IAC


Post:1991:RSE

REFERENCES


Piner:1998:CUW


Pitas:1995:PIW


Pitas:1996:MSC


Pitoura:1996:RSS


Price:1999:IAV


Panneerselvam:1990:RSA

REFERENCES


**Popek:1979:ESC**


**Penzhorn:1995:CLP**


**Penzhorn:1995:CLW**


**Praehofer:1999:SRS**


**Pamplona:1998:LVC**


**Postma:1997:DCF**


**Park:1994:KDA**

Choonsik Park, Kaoru Kurosawa, Tatsuaki Okamoto, and Shigeo Tsuji. On key distribution and authentication in mobile ra-

**Petrounias:1994:RBA**


**Pless:1975:ESC**


**Pless:1977:ESC**


**Plimmer:1998:MIW**


**Plumstead:1982:ISG**


**Plumstead:1983:ISP**


ac.uk/~fapp2/steganography/bibliography/021136.html. Two volumes.

**Pudil:1995:ASM**


**Preneel:1994:CCM**


**Pointcheval:1999:NPK**


**Pollard:1974:TFP**


**Pollard:1978:MCM**


**Pomerance:1988:ACC**

REFERENCES


REFERENCES

Poole:1995:La

Popentiu:1989:SRK

Pope:1996:PF

Porges:1952:MNC

Porter:1984:CNS

Portz:1991:UIN

Portz:1993:GDB

Poromaa:1998:PAT

Posch:1992:TMD
Reinhard Posch. Trustworthy management of distribution and operation of encryption devices. Report 344, Institutes for Information Processing, Graz, Aus-


**Posch:1995:MRRa**


**Pakstas:1996:SNN**


**Pedersen:1997:FSS**


**Park:1997:TER**


**Peleg:1979:BSC**


**Pieprzyk:1985:DPK**


REFERENCES


Preneel:1993:ADC

Preneel:1993:SCT

Preneel:1994:CHF

Preneel:1994:CHF

Preneel:1995:FSE


Preneel:1995:EFC


Preneel:1997:HFM


PGP:1997:PGPa

Pretty Good Privacy, Inc. Pretty Good Privacy PGP-mail 4.5 program: quick guide. Pretty Good Privacy,
REFERENCES

PGP:1997:PGPb


Preneel:1998:CMA


Preneel:1998:IC


Preneel:1998:CPI


Preneel:1999:SCH


Pritchard:1980:DE


Price:1983:ABR


**Price:1994:MVC**


**Pronzini:1980:MCC**


**Proctor:1985:SSC**

Norman Proctor. A self-synchronizing cascaded cipher system with dynamic control of error propaga-


**Patel:1999:TML**


**Peyravian:1999:HBE**


**Paun:1993:CPS**

Gheorghe Păun and Arto Salomaa. Closure properties

**Pieprzyk:1993:DHA**


**Pfitzmann:1996:AF**


**Pichler:1996:FDG**


**Pointcheval:1996:PSB**


**Pointcheval:1996:SPS**


**Parker:1997:GFA**

M. G. Parker and S. J. Shepherd. The generation of finite alphabet code-words with no cyclic shift or reversal symmetry. In ???:, editor, *Proceedings of*
REFERENCES


Patiyoot:1998:SIW


Patiyoot:1998:TAPa

USA, 1998. ISBN ???. LCCN ???.


REFERENCES


[PSR97] Christof Paar and Pedro Soria-Rodriguez. Fast


Purdy:1974:HSL


Puteanus:1627:EPC


Preparata:1990:PCD


Peinado:1997:HPC


Posegga:1998:BCV


Pluimakers:1986:ACS


Preneel:1995:MMB


The workshop was sponsored by International Association for Cryptologic Research . . . [et al.]”–T.p. verso.


REFERENCES

PW93a

PW93b

PW97a

PW98

PW99
C. Piccardi and F. Wotawa. A communication language

Polani:1999:DAR


Podilchuk:1998:IAW


Quisquater:1990:BHF


Quisquater:1991:CLE


Quisquater:1989:BHF

[QG90] J. J. Quisquater and M. Girault. 2^n-bit hash-functions using n-bit symmetric block cipher algorithms. In Quisquater and Vandewalle [QV90], pages 102–?? CO-

Quisquater:1995:ACE


Quisquater:1989:ACE

Jean-Jacques Quisquater and Joos Vandewalle, editors. Advances in Cryptology EUROCRYPT ’89: Workshop on the Theory and Application of Cryptographic
REFERENCES


Quisquater:1990:ACE


Quisquater:1998:E


Rabin:1977:DS


Rabin:1981:HES


Rabin:1989:EDI


Rabin:1994:RSS

Tal Rabin. Robust sharing of secrets when the


Rhodes-Burke:1982:RSA


Reiter:1994:HSR


Ramesh:1999:VPP


Rowstron:1999:CUR

A. Rowstron, B. Bradshaw, D. Crosby, and T. Edmonds. The Cambridge University Robot Football Team description. Lecture
Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA


Rogaway:1994:SOE


Russinovich:1995:EWL


Rubia:1999:RIB

REFERENCES


Rees:1997:AGO


Reeds:1998:SCB


Reischuk:1985:NSB


Reiter:1992:ISG


Reiter:1996:DTR


Rejewski:1977:ATP


REFERENCES


REFERENCES

[Rhee:1993:RAC]

[Rhee:1994:CSC]

[Rhoads:1995:SMA]

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

[Rihaczek:1987:T]

[Rijmen:1999:WL]

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

[Ripe:1995:IPS]
RIPE. Integrity primitives for secure information systems. final report of RACE integrity primitives evaluation (RIPE-RACE 1040). In Bosselaers and Preneel
REFERENCES


RIPE:1995:RIP


Ritter:1999:IWC


Ritchie:19xx:DCW


Rivest:1974:HCA


Rivest:1974:AAR


Rivest:1979:CRC

REFERENCES

DEN NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL http:
issn=0006-3835&volume=
19&issue=2&spage=274. See
[Her78].

[Riv80] R. L. Rivest. A description of a single-chip imple-
mentation of the RSA ci-
pher. Lambda: the mag-
azine of VLSI design, 1
(3):14–18, Fourth Quarter
1980. CODEN VDES.
ISSN 0273-8414.

[Riv85] Ronald L. Rivest. RSA
chips (past/present/future).
In Beth et al. [BCI85],
pages 159–163. CODEN
LNCS. ISBN 0-387-
16076-0 (USA). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/0558/tocs/t0209.htm;
issue=0302-9743&
volume=209. Held at the
University of Paris, Sor-
bonne.

[Riv87] Ronald L. Rivest. The
eary days of RSA: History
and lessons. In Ashen-
hurst [Ash87], page ??
QA76.24 A33 1987. ACM
Turing Award lecture.

1186: MD4 message di-
gest algorithm, October
1, 1990. URL ftp://
/ftp.internic.net/rfc/
rfc1186.txt; http://
www.math.utah.edu/pub/
rfc/rfc1186.txt. Status:
INFORMATIONAL.

[Riv90b] Ron Rivest. Cryptogra-
phy. In Jan van Leeuwen,
editor, Handbook of The-
oretical Computer Science,
pages 717–755. Elsevier,
Amsterdam, The Nether-
lands, 1990. ISBN 0-444-
88075-5 (Elsevier: set), 0-
444-88071-2 (Elsevier: vol.
A), 0-444-88074-7 (Elsevier:
vol. B), 0-262-22040-7 (MIT
Press: set), 0-262-22038-5
(MIT Press: vol. A), 0-262-
B). LCCN QA76 .H279
1990.

four million large random
primes. Lecture Notes
in Computer Science, 537:
625–??, 1991. CODEN
LNCS. ISSN 0302-9743
REFERENCES

[ Rivest:1991:MMD ]

[ Rivest:1992:RMMa ]

[ Rivest:1992:RMMb ]

[ Rivest:1993:CML ]

[ Rivest:1993:NPD ]

[ Rivest:1995:DRR ]

[ Rivest:1993:REAb ]
R. L. Rivest. The RC5 encryption algorithm. In


R. L. Rivest. Can we eliminate certificate revocations


[RK93] Beth Rosenson, Stephen Thomas Kent, and Dorothy Elizabeth Robling Denning.
REFERENCES


REFERENCES


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Rogaway:1995:BHA

REFERENCES

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


Rose:1993:RCM

REFERENCES

leted by RFC1864 [MR95b].
Status: PROPOSED STAN-
DARD.

Rosen:1994:EMT

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

Rose:1995:SUP

Rose:1996:IUP

Rose:1996:PMI

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

Rose:1996:UCI

Rose:1996:UPKa
Greg Rose. USENIX PGP key-signing service. ;lo-

Rose:1996:UPKb
Greg Rose. USENIX PGP key-signing service. ;lo-
REFERENCES


REFERENCES

JMOPEW. ISSN 0950-0340 (print), 1362-3044 (electronic). URL http://www.tandfonline.com/doi/abs/10.1080/09500349414552281


[Roy:1986:CBI] 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.).


[RP95b] V. Rijmen and B. Preneel. Improved characteristics for differential cryptanalysis of hash functions based on block ciphers. *Lecture Notes*
REFERENCES


 REFERENCES  


Status: PROPOSED STAN- DARD.


Status: PROPOSED STAN- DARD.


C. Roeckl and D. Sangiorgi. A $\lambda$-calculus process semantics of concurrent idealised
Rozenberg:1999:DCN


Rivest:1978:MOD


Rivest:1982:MOD


Rivest:1983:MOD


RSA:1993:PRE


RSA:1993:PDH

RSA Laboratories. PKCS #3: Diffie–Hellman Key Agreement Standard. RSA Data Security, Inc., Redwood City, CA, USA,


Reif:1988:EPP


Rezny:1993:BCM


Raleigh:1988:CDP


Rubin:1979:DSC


Rudolph:1982:HTI


Rudich:1991:UIP

REFERENCES


[Rus93a] F. Ruskey. Simple combinatorial gray codes con-

Russell:1993:NSC


Roychowdhury:1999:ENQ


Reeds:1984:FSU


Robshaw:1997:ECC


Rytter:1986:SCU


Ras:1999:DES


S:1873:COD

[H. S. Cryptographie, ou, Divers systèmes d’écrire secrète spécialement pour l’usage des cartes postales: combinaisons alphabétiques, correspondance chiffrée, écriture par signes: divers procédés pour la fabrication d’encre sympathiques. G. Jousset, Paris, France,
Schiller:1995:SWT


Sabourin:1994:CCP


Sacco:1936:MC


Sacco:1947:MC


Sacco:1951:MCF


Sacco:1977:MC


Sahai:1999:NMN

REFERENCES


Salomaa:1991:VRS


Sale:1993:EBP


Salomaa:1996:PC


Salvail:1998:QBC


Salvail:1999:SHG


Shimoyama:1997:IFS


Sameshima:1998:KES


Sansom:1986:BRC

REFERENCES

**Sandhu:1988:CIT**


**Sar28**


**Sars:1997:STL**


**Sas99a**


**Saw99b**


**Sat89**

M. Satyanarayanan. Integrating security in a large distributed system. *ACM
REFERENCES

Sawirudin:1955:PND

Schumuller-Bichl:1982:ADE

Sorkin:1984:MCC

Smid:1992:DES


Juan Soto and Lawrence Bassham. Randomness testing of the Advanced Encryption Standard candidate algorithms. NIST internal report 6390, National
REFERENCES


Serpell:1985:PES


Smillie:1985:RFM


Stallmann:1999:HED


Siegberg:1999:TDG


Sztandera:1999:ANN

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


REFERENCES


REFERENCES

Schroeder:1975:ESK


Schell:1983:SPA


Schroeder:1984:NTS


Schroeder:1986:NTS


Schnorr:1990:EISb


Schnorr:1990:EISA

Schroeder:1990:NTS


Schmitt:1991:EAA


Schneier:1991:OHP

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

Schneier:1992:SSA

DEN COMLEF. ISSN 0749-2839.

**Schneier:1992:UPC**


**Schneier:1993:IEA**


**Schneier:1993:UHD**


**Schneier:1993:DS**


**Schneier:1993:SCD**


**Schneier:1993:FIE**


**Schneier:1993:FHI**

REFERENCES


REFERENCES

Schneier:1994:BEA

Schneier:1994:CAW

Schneier:1994:NC

Schneier:1994:PYM

Schneier:1994:RDS

Schneier:1995:AAB

Schneier:1995:AAG

Schneier:1995:MS

Schneier:1995:MSH
REFERENCES


M. R. (Manfred Robert) Schroeder. *Number the-
REFERENCES


Schweighofer:1997:DIF


Schlesinger:1998:CPC


Schneier:1998:CBT


Schneier:1998:CDV

Schneier:1998:CTS


Schneier:1998:SPC


Schneier:1998:TEA


Schoenmakers:1998:SAE


Schroeppel:1998:HPC

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

**Schaefer:1999:PES**


**Schmalz:1999:MDI**


**Schmidt:1999:RER**


**Schneier:1999:SSC**


**Schneier:1999:IRR**


**Schneier:1999:IRT**

REFERENCES


REFERENCES


[SE96] Jörg Schwenk and Jörg Eisfeld. Public key encryption and signature schemes based on polynomials over

Seaton:1956:THS


Sears:1986:SWK


Seachrist:1995:DIM


Sedlak:1988:RCP


Sedgewick:1992:AC

REFERENCES


REFERENCES

Seshadri:1981:KPP

[Ses81]

Sakurai:1997:ILC

[SF97]

Saglam:1995:ACL

[SG95]

Shearer:1996:GCR

[SG96]

Shieh:1996:DIL

[SG96b]

Shoup:1998:STC

[SG98]

Saeednia:1999:SCG
S. Saeednia and H. Ghodsi. A self-certified group-oriented cryptosystem without a combiner. Lecture

[SG99a]

Sapir:1999:DRT


Sgarro:1990:IDB


Sgarro:1991:STC


Sgarro:1991:LBA


Sgarro:1993:ITB


Slater:1998:CAD

A. Slater, R. Gore, J. Posegga, and H. Vogt. cardT0AP: Automated deduction on a smart card. Lecture Notes in Computer Science, 1502:
REFERENCES

Syverson:1997:ACO

Simpson:1999:FCA

Sun:1994:KGA

Schnorr:1995:ACC

Schnorr:1995:ACR

Schneier:1997:IMS


[Shi:1999:FGM]


[Shannon:1945:MTC]


[Shannon:1949:CTS]


[Shamir:1979:HSS]


[Shamir:1979:HSS]

Adi Shamir. A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem. In *23rd annual symposium on founda-
REFERENCES


R. L. Sharp. Design of a certifiable one-way data-flow

**Shamir:1994:ESS**


**Shamir:1995:MEV**


**Shamir:1995:RP**


**Shaw:1997:VVA**


**Shamir:1998:VC**


**Shallit:1999:RHA**


**Shamir:1999:PAK**

Adi Shamir. Power analysis of the key scheduling of the AES candidates.
REFERENCES


Sherman:1986:CVT


Sherman:1987:CVT


Sherman:1988:CVV


Shepherd:1992:DSA


Shepherd:1992:FFW


Shepherd:1992:FHS

[She92c] S. J. Shepherd. A fast, high security public key proces-
REFERENCES


Shepherd:1992:HSC

Shepherd:1992:NPS

Shepherd:1992:SIR

Sherrod:1992:DES

Shepherd:1993:ACCa

Shepherd:1993:ACCb

Shepherd:1993:EOS

Shepherd:1993:WNS


S. J. Shepherd. Primitive polynomials over GF(2) of Hamming weight 3 and 5.


Victor Shoup. On fast and provably secure message authentication based on universal hashing. Lecture


**Shumaker:1982:RCJ**


**Sakurai:1993:DBS**


**Sakurai:1993:SCS**


**Sakurai:1994:SCT**


**Sidhu:1981:APG**


**Sieminski:1983:SBB**

Gregory C. Sieminski. The search for a balance be-
tween scientific freedom and
national security: a case
study of cryptology. Thesis (M.S.), Defense Intelli-
genence College, Washington,
DC, USA, November 1983.
v + 73 pp.

Siegenthaler:1984:CIN
T. Siegenthaler. Correlation-
immunity of nonlinear com-
bining functions for crypto-
graphic applications. IEEE
Transactions on Information
Theory, IT-30(5):776–
780, 1984. CODEN IET-
TAW. ISSN 0018-9448
(print), 1557-9654 (elec-
tronic).

Siegenthaler:1985:DCS
T. Siegenthaler. Decrypting
a class of stream ciphers us-
ing ciphertext only. IEEE
Transactions on Computers,
C34:81–85, 1985. CODEN
ITCOB4. ISSN 0018-9340
(print), 1557-9956
(electronic). This paper
breaks the cipher of [Gef73].

Swartzlander:1993:SCA
Earl Swartzlander, Jr.,
Mary Jane Irwin, and Gra-
ham Jullien, editors. Pro-
cedings: 11th Symposium
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.
IEEE Transactions on Com-
puters 43(8), 1994.

Shimbo:1993:CSC
Atsushi Shimbo and Shin-
ichi Kawamura. Cryptanal-
ysis of several conference
key distribution schemes.
Lecture Notes in Computer
CODEN LNCSG9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Silverman:1983:RVS
Jonathan M. Silverman.
Reflections on the verifica-
tion of the security of an op-
erating system kernel. Op-
erating Systems Review, 17
CODEN OSRED8. ISSN
0163-5980.

Silverman:1987:MPQ
Robert D. Silverman. The
multiple polynomial quadratic
sieve. Mathematics of Com-
putation, 48(177):329–339,
January 1987. CODEN
MCMPAF. ISSN 0025-5718
(print), 1088-6842 (elec-
tronic).

Silverman:1997:RSP
R. D. Silverman. The re-
quirement for strong primes


REFERENCES


Simmons:1983:PPS

Simmons:1984:HID

Simmons:1985:ATC

Simmons:1985:SCD

Simmons:1988:SSC

Simmons:1990:HRS
G. J. Simmons. How to (really) share a secret. In Goldwasser [Gol90b], pages 390–449. CODEN
Simmons:1990:PSS


Simmons:1991:GSS


Simmons:1992:CCS


Simmons:1993:SCU


Simmons:1994:CTS


Simmons:1994:CPF


Simmons:1994:SCP


Simmons:1994:SCE


Simovits:1995:EDE


Simmons:1996:HSC


Simpson:1996:RPC

REFERENCES

letes RFC1334 [LS92]. Status: DRAFT STANDARD.

**Simmons:1997:SCS**

G. J. Simmons. Subliminal channels: Some recent developments. In Anonymous [Ano97a], page ??
LCCN ???. URL http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061457.html

**Simmons:1998:HSC**


**Simmons:1998:RCB**


**Simon:1998:FCO**


**Sinkov:1966:ECM**


**Sinkov:1968:ECMa**


**Sinkov:1968:ECMb**

Abraham Sinkov. *Elementary cryptanalysis: a*


REFERENCES


Scott:1998:DAB


Sako:1994:SVU


Sako:1995:RFM


Schneier:1996:AOC


Schneier:1996:PPSa


Schneier:1996:UFNa

B. Schneier and J. Kelsey. Unbalanced Feistel networks and block cipher de-


Schneier:1998:CSS


Schneier:1999:SAL


Stabell-Kulo:1999:PAM


Shepherd:1997:EKE

S. J. Shepherd, A. H. Kemp, and S. K. Barton. An ef-

Schell:19xx:CMC


Sorokine:1994:TBD


Suzuki:1999:AVB


Satoh:1998:HSR


Satoh:1998:HSS


Schneier:1996:DP


Schneier:1998:TKSa

[SKW+98a] B. Schneier, J. Kelsey, D. Whiting, D. Wagner,
REFERENCES


Schneier:1998:TBBa


Schneier:1998:TBBb


Schneier:1998:TSC


Schneier:1998:TBE


Schneier:1998:TNB

<table>
<thead>
<tr>
<th><strong>REFERENCES</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Schneier:1999:PCAa</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Schneier:1999:PCAb</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Schneier:1999:NRT</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Schneier:1999:TEAb</th>
</tr>
</thead>
</table>
REFERENCES


REFERENCES

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


REFERENCES


[Smi83] John Smith. Public key cryptography: An introduction to a powerful cryptographic system for use on microcomputers. *BYTE*
REFERENCES

*Magazine*, 7(??):198–218, January 1983. CODEN BYTEDJ. ISSN 0360-5280. This is a simple exposition of public key cryptography. [Smi93b]

**Smith:1987:AUW**


**Smith:1987:AUW**


**Smith:1990:PPC**


**Smith:1993:LPE**


**Smith:1994:CPC**


**Smith:1994:CE**


**Smith:1997:ETC**


**Smith:1997:IC**

REFERENCES


Smith:1998:IES


Smith:1998:SXC


Shimoyama:1998:IHO


Son:1998:ASC


Stakhov:1999:IFC


Safavi-Naini:1993:FTA


Shepherd:1994:VFH


Safavi-Naini:1996:TSS

R. Safavi-Naini. Three systems for shared generation
Steiner:1988:KAS


Safavi-Naini:1993:ACU


Safavi-Naini:1995:ACP


Safavi-Naini:1998:BCM


Safavi-Naini:1998:NRM


Snyder:1979:IUC

Snyder:1980:CAP


Shepherd:1998:ALP


Sonnino:1999:CBL


Schroeppel:1995:FKE


Sorkis:1980:USM


Soto:1998:RTA


Smith:1979:UFM

REFERENCES

MTKAAB. ISSN 0025-5793.

Seberry:1989:CIC

Seberry:1990:ACA

Spender:1987:ICU

Schechter:1999:AAM

Spirakis:1995:AET
REFERENCES


Schwemmlein:1998:RMR


Schuett:1997:CPB


Shoup:1996:SKD


Saltzer:1984:EEA


Shin:1998:NHF


Shin:1999:HFM

Shamir:1984:CCV

Siromoney:1986:PKC

Shepherd:1989:CSS

Shepherd:1990:DSA

Schrift:1991:UNB

Sun:1994:DTS

Sakurai:1995:RAC
REFERENCES

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


Smith:1995:PKC


Sandhu:1996:AAC


Silverman:1997:CAX


Sakai:1998:DHC


Sun:1998:PKC


Schneier:1999:BHD

REFERENCES

Schoenhoff:1999:GVM


Shapiro:1999:MAE


Solomonides:1999:REI


Stubblebine:1999:FLA


Stubblebine:1999:FOA


Subramanian:1987:DTP


Siromoney:1988:CPL


First USENIX Symposium on Smart Cards, USENIX Press, to appear.
Saito:1999:DPC


Smith:1981:VEP


Stubblebine:1999:UST


Safford:1993:SRA


Sakai:1997:WRK


Sakai:1997:WRP


REFERENCES


**Schmidt:1998:LOA**


**Salter:1998:TSS**


**Schneier:1998:DDE**


**StJohns:1984:RAS**


**StJohns:1985:RAS**

REFERENCES

**[ST89]**

**[ST91]**

**[St.93]**

**[Sta70]**

**[Sta78]**
Harold M. Stark. *An introduction to number the-
REFERENCES

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:1994:SSH


Stallings:1995:PWT


Stallings:1995:PYP


Stadler:1996:PVS


Staiger:1996:CSW


Stallings:1996:PCS


Stallings:1996:PCI

William Stallings. Practical cryptography for internetworks. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
REFERENCES


[Ste87] J. Stern. Secret linear congruential generators are not

Stevens:1988:CPR


Stephenson:1989:PPM


Stevens:1990:CPi


Stevens:1990:CPk


Steinberg:1991:VSV


Stewart:1992:SCK


Stern:1994:DIS


Stevens:1994:PBa

REFERENCES

Stern:1995:COD

Stern:1996:VCA

Stern:1998:LCO

Stern:1998:NEA

Stephenson:1999:C

Stern:1999:ACE

Stern:1999:DU
aes. No slides for the conference talk are available.


REFERENCES


Stinson:1995:CTP

Stinson:1998:C

Stinson:1998:VCT

Stout:1965:DRN

Stoll:1989:CET

Stout:1990:SDE

Stone:1998:RBH

Sivabalan:1993:DSN
REFERENCES


REFERENCES

**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**


**Shand:1993:FIR**

REFERENCES

Schnorr:1994:BBC

Schnorr:1995:BBC

Shepherd:1995:GJ

Stern:1998:CC

Shamir:1999:PHS

Shamir:1999:PSS

Samuels:1998:LSA
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
REFERENCES

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


REFERENCES


REFERENCES


Schneier:1997:FSEb

Stinson:1999:ARS

Stinson:1999:KPT

Swan:1994:AAb

Swire:1997:ULF
Salzer:1981:RHH

Salomaa:1986:PCB

Salomaa:1986:PKC

Smith:1992:ICF

Sakurai:1996:BDB
K. Sakurai and Y. Yamane. Blind decoding, blind undeniable signatures, and their applications to privacy protection. In Anderson [And96c],...
of knowledge models in the mechanical design field. 
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Sakurai:1998:KES**


**Syverson:1992:KBS**


**Syverson:1993:KDP**

REFERENCES

Seberry:1993:ACA


Sakurai:1996:CWR


Szepietowski:1998:WSO


Swanson:1996:RDH


Swanson:1996:TRI


Swanson:1998:MSB

REFERENCES


Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng.

Seberry:1995:RAN


Seberry:1995:SCF


Seberry:1995:RBP


Theodoridis:1998:NES


Takano:1999:CAC

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

Tardo:1992:SGA

REFERENCES


Tang:1997:DBC


[Ta97]

Taaffe:1998:NBL


[Taa98]

Tabatabaian:1994:CAP


[Tab94]

Takagi:1997:FRT


[Tak97]

Tanaka:1990:RSI

Hatsukazu Tanaka. A realization scheme for the


**Tao:1994:FAO**


**Tardo:1990:PKB**


**TFEC:1998:CPF**


**Tattersall:1999:ENT**


**Taylor:1990:DSI**


**Taylor:1994:ICV**

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


REFERENCES


**Tzeng:1999:IP1**


**Thao:1991:SAD**


**Theobald:1995:HBS**


**Thomas:1974:RPS**


**Thompson:1984:RTT**


**Thomas:1986:SDE**


**Thompson:1987:RTT**

Thomas:1996:PVS

Tarman:1998:AAE

Tsujii:1988:PKC

Tilki:1998:EHD

Tippett:1927:RSN

Taaffe:1997:NSL

Tseng:1999:ATS
REFERENCES


Terada:1997:LDC


Todorovic:1997:Cas


Tirkel:1998:IWR


Tonchev:1996:CDG


Toussaint:1991:DCK


Toussaint:1992:SSI

Toussaint:1993:FVP


Tsunoo:1994:COA


Touch:1995:RRM


Townsend:1998:QCO


Thompson:1963:SDE


Traore:1997:MUF


Traore:1999:GST

Tremblett:1999:JPA


Trithemius:1518:PLS


Trithemius:1606:CGT

Trithemius. Clausis generalis triplex in libros steganographicos Iohannis Trithemij .... Iohannis Bernerii, Frankfurt, Germany, 1606. 7 + 1 pp. LCCN Z103.T84 S 1606. Ab ipso authore conscripta ... Darmbstadij: Excudebat Balthasar Hofmann, impensis Iohannis Berneri, bibliopolam Francofurtensem, anno 1606.

Trithemius:1606:CSI


Trithemius:1606:SHE

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

Trithemius:1621:CGT

REFERENCES

Trithemius:1621:CSI


Trithemius:1621:SHE


Trostle:1993:MFT


Tronson:1997:C


Tirkel:1993:EW


Terry:1988:MSV

Tso:1990:NPK

Tso:1997:MEE

Tokita:1995:LCL

Tombak:1993:ACP

Tsudik:1989:DAI

Tsudik:1992:MAOb

Tsudik:1992:MAOa
Tsujii:1992:CS


Thomlinson:1998:NBP


Tual:1999:MGA


Tuchman:1966:ZT

scribes this book as “re-count[ing] the political ef-
facts of the most important cryptogram solution in his-

Tuchman:1979:HPN

W. Tuchman. Hellman presents no shortcut sol-
solutions to DES. *IEEE Spectrum*, 16(7):40–41, July
1979. CODEN IEESAM. ISSN 0018-9235 (print),
1939-9340 (electronic).

Tuchman:1979:IHP

W. Tuchman. IV. ‘Hellman presents no shortcut sol-
solutions to the DES’. *IEEE Spectrum*, 16(7):40–41, July
1979. CODEN IEESAM. ISSN 0018-9235 (print),
1939-9340 (electronic).

Tung:1999:KNA

Brian Tung. *Kerberos: a Network Authentication System*. Addison-Wesley,

Turing:1941:APC

Alan M. Turing. The applications of probabili-
ty to cryptography. Report, GCHQ, Cheltenham,
UK, 1941. URL http://
http://home.cern.ch/~
frode/crypto/Turing/index.html. This document is re-
typed 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 re-
mainder are in preparation.

Tijdeman:1992:CDP

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

Tel:1994:DAI


[TY94]


Trabelsi:1994:PPS


Tsiounis:1998:SEE


Tsiounis:1998:SEB

Tan:1992:NPE


[TX92]


Takagi:1992:MMH
REFERENCES


[102x475]

Tax:1999:PFD [TYD99]


[102x339]

Tygar:1996:CPI [TYH96]


[102x515]

Tzeng:1999:CMC [Tze99]


[102x529]

Udell:1998:HAW [Ude98]

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

[102x236]

Uehara:1995:ESB [Ueh95]

Udell:1994:BCRb


USASC:1923:EC


USASC:1940:CML


USASC:1942:ACC


USWarDept:1924:EC


USWD:1924:EC

United States. War Dept. Elements of cryptanalysis.

USDOS:1970:BC


USNBS:1977:DES


REFERENCES


USNSACSSCCH:1992:FLT


USDOA:1994:OMT


USDOA:1994:UDS


USNSACSSCCH:1992:FLT


USCSCJSTL:1995:ACC


USNSGC:1995:NDN

REFERENCES


REFERENCES

Shipping list no.: 97-0329-P. Serial no. 9.

**USCSCJ:1997:EKR**


**USGAOOGC:1997:DCB**


**USCHCIR:1998:HEI**


**USCHCIR:1998:MHS**


**USCHCIR:1998:HSF**


**USCHCIRSIEPT:1998:EIR**

REFERENCES


USCHCIRSIEPT:1998:HSF


USCSCCST:1998:EHB


USCSCCST:1998:HEH

REFERENCES


USCSCJ:1998:HEK


USCSCJ:1998:HED


USCSCJSTTGT:1998:EDC


USGSA:1983:ISR

United States. General Services Administration, Na-
REFERENCES


REFERENCES


REFERENCES


USENIX:1996:PUA


USENIX:1996:USS


USENIX:1998:PUWa


USENIX:1998:PUWb


USENIX:1998:FPT


USENIX:1998:SUS
REFERENCES


**USCHCJ:1997:SFT**


**USPBC:1997:AEC**


**VanderBank:1988:CFM**


**Vadhri:1995:VID**

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

**Valerio:1892:C**


**Vamos:1985:BRB**

References

VanTassel:1969:ACT


Vandeberg:1986:ICS


VanHeurck:1987:TNS


vanTilborg:1995:IC


VanTilburg:1993:SKE


VanOorschot:1995:DCS


VanTilborg:1995:ACA

vanRenesse:1996:OSC


vanDijk:1997:MIT


vanRenesse:1997:ODS


vanderLubbe:1998:BMC


Varaiya:1999:DSI

P. Varaiya. Design, simulation, and implementation of hybrid systems. *Lecture Notes in Computer Science*, 1639:1–??, 1999. CODEN LNCSN0. ISSN 0302-9743 (print), 1611-3349 (electronic).

Varma:1999:IDD


Vaudenay:1993:FHI


Vaudenay:1995:NMC

S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4


F. Vandermeulen, P. De Meester, P. De Ceuleners,

**Lubbe:1998:BMC**


**vdL98**


**vdWS97**

[Ver26] G. S. Vernam. Cipher printing telegraph systems

**Vernam:1926:CPT**


**Veron:1995:CHI**


**Verschuren:1998:SCN**


**Verschuren:1998:SAS**


**VonzurGathen:1999:MCA**


**Vandewalle:1993:TAT**


**Vallee:1988:HBO**


**Vallee:1989:HGR**

REFERENCES

Verschuren:1993:IOS


VanFaber:1997:SDD


Vincent:1971:PAG


Vincent:1972:CPA


Vigna:1998:CTM

REFERENCES


[VK84] Voydock:1984:SMT


[vL96] Lingen:1996:NDP


[VMS97a] Villasenor:1997:CCb

References


Kerckhoffs:1883:CMF


Varadharajan:1999:DER


Voyatzis:1998:DW0


Venkataraman:1994:PAM


Venkataraman:1995:CEA

REFERENCES

Oorschot:1991:CPP

Paul C. van Oorschot.
A comparison of practical public-key cryptosystems based on integer factorization and discrete logarithms.
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370576.htm;

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

Rainer Vogel. On the linear complexity of cascaded sequences.
URL http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm;
Held at the University of Paris, Sorbonne.

Volts:1941:BCP

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

**VonZurGathen:1992:PEE**


**VonZurGathen:1992:PEF**


**Voukalis:1980:DFC**


**Voukalis:1980:GSE**


**vanOorschot:1991:KPA**


**vanOorschot:1996:DHK**

REFERENCES

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

[Voyatzis:1996:ATA]

[Voyatzis:1998:DIW]

[Voyatzis:1999:PDI]

[Varadharajan:1997:ISP]

[Vassiliadis:1988:PEA]

[Volts:1941:BC]
James D. Volts and David Shulman. Bibliography of
cryptography. U. S. Army, Cincinnati, OH. USA, 1941. 93 pp. LCCN Z103.A1 V6 1941. Typewritten (carbon copy) Three heavy leaves precede sections II-IV (not included in pagination). This copy was made especially for the United States Army from the original manuscript. Third copy: penciled note on cover. Contents: pt.1. Cryptography; pt.2. Titles relating indirectly to cryptography; pt.3. Rejected titles; pt.4. Author index.


vanTilburg:1994:SAC


vanTilburg:1986:DBK


vanSchyndel:1994:DW


Vu:1995:CPM


Vazirani:1985:ESP


Valiant:1986:NED

L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. Theoretical Com-
REFERENCES

Verheul:1997:CLS

Vandemeulebroecke:1990:SCB

Verheul:1997:BEF

vanOorschot:1994:PCS

VanOorschot:1996:DKA

Vedder:1998:SCR
K. Vedder and F. Weikmann. Smart cards — requirements, properties, and applications. *Lecture Notes
REFERENCES


REFERENCES


REFERENCES

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

Wagstaff:1999:C

Waidner:1990:USR

Waite:1995:BRB

Walden:1900:ADB
John William Henry Walden, August, Duke of Braunschweig-Luneburg: The cryptomenytic and cryptography of Gustavus Selenus: in nine books: wherein is also contained a most clear elucidation of the Steganographia, a book at one time composed in magic and enigmatic form by Johannes Trithemius. ?????. ???. 1900. LCCN Z103 .A95 1900.

Wallace:1990:PRG

Wallich:1994:WP

Walton:1995:IAS
REFERENCES

18–20, 22, 24, 26, 82, 84–87, April 1995. CODEN DDJOEB. ISSN 1044-789X.


REFERENCES


Wayner:1993:CAS


Wayner:1993:ECD


Wayner:1993:SER


Wayner:1995:PCL


Wayner:1996:DCB


Wayner:1996:DLY


Wayner:1998:MJD

REFERENCES


REFERENCES


Wang:1999:SCB


Wendling:1999:PRS


Weber:1979:USD


Weber:1988:NPK


Weber:1993:MDC


Weber:1998:SWY


Webb:1988:NPK

REFERENCES

Wedemeijer:1999:DFM


Wehde:1997:UGT


Wehde:1998:MBE


Wehde:1999:MSE


Weingarten:1983:CCP


Weiss:1988:BOP


Weissman:1991:IRA


Weissman:1991:IRN

[Wei91b] Clark Weissman. Inside
REFERENCES


Dominic Welsh. *Codes and cryptography*. Oxford


REFERENCES


[Wagner:1999:CFa]

[Wilkes:1982:MRJ]

[Wescombe:1997:GBS]

[Williams:1999:ADQ]


[Want:1992:ABL]
Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbons. The active badge location system.
REFERENCES


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

Wichmann:1987:NAR

REFERENCES


for Data Internetworks, W. Stallings.

**Wiener:1997:EKS**


**Wiener:1998:EKS**


**Wiener:1998:PCP**


**Wiener:1999:ACC**


**Wilkins:1641:MSS**


**Wilkes:1968:TSCa**


**Wilkes:1968:TSCb**


**Wilkes:1972:TSC**


**Wilkes:1975:TSC**

[Wil75] M. V. (Maurice Vincent) Wilkes. *Time-sharing com-
puter systems. Computer monographs. Macdonald
444-19525-4 (American Elsevier). ii + 166 pp. LCCN
QA76.53 .W54 1975.

[Wil82c]

H. C. Williams. A modification of the RSA public-
key encryption procedure. IEEE Transactions on In-
IETTAW. ISSN 0018-9448 (print), 1557-9654 (elec-
tronic).

[Wil83a]

Michael Willett. Trapdoor knapsacks without superin-
creasing structure. Information Processing Letters,
17(1):7–11, July 19, 1983. CODEN IFPLAT. ISSN
0020-0190 (print), 1872-6119 (electronic).

[Wil83b]

M. H. Williams. The problem of absolute privacy. Infor-
CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (elec-
tronic).

[Wil85]

H. C. Williams. Some public-key crypto-functions as intractable as factor-
ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
REFERENCES


Williams:1986:PKE


Williams:1986:ACC


Williams:1986:CTU


Wiles:1993:HBE


Williams:1993:CPK


Winternitz:1984:SOH


Winterbotham:1989:US


Winterbotham:1991:US


Winton:1993:UPH


Wintertin:1984:SOH

Winterbotham:1999:US


Wired:1998:REC


Wedel:1996:FSA


Watanabe:1997:SCR

H. Watanabe and T. Kasami. A secure code for recipient watermarking against conspiracy attacks by all users. In Han et al. [HOQ97], pages 413–423. CODEN LNCSD9. ISBN 3-540-63696-X (softcover). ISSN

Wechsler:1997:AVB

Wechsler:1997:AVB

Whiting:1999:FOK

Whiting:1999:FOK

Woo:1992:ADS

Woo:1992:ADS

Woo:1992:CAD

Woo:1992:CAD

Woo:1994:LAP

Woo:1994:LAP

Wong:1999:DSF
Chung Kei Wong and Simon S. Lam. Digital signatures for flows and multicasts. IEEE/ACM Transactions on Networking, 7(4):502–513, Au-
REFERENCES


**Walker:1996:CKR**


**Wagner:1985:PKC**


**Waldvogel:1993:PDD**


**Wheeler:1994:TCN**


**Wheeler:1995:TTE**

REFERENCES


[Wright:1998:NTD]

[Woehr:1997:CRR]

[Wolfe:1943:FFCCa]


[Wolfowicz:1993:SPR]
W. Wolfowicz, editor. State and progress of research in cryptography: 3rd Symposium — February 1993, Rome, PROCEEDINGS
OF THE SYMPOSIUM ON
STATE AND PROGRESS
OF RESEARCH IN CRYPT-
TOGRAPHY 1993: 3rd. [],
Rome; Fondazione Ugo Bor-
doni, 1993.

Wolfowicz:1993:SPS


Wolf:1998:SSAb


Wolf:1999:USC


Wood:1982:FAC


Woolsey:1990:DDE


Worth:1975:CMA


Wortmann:1987:BRB


World:1996:NIT

[Wor96] Linda World. In the news: Intel and TI will enter 3D
REFERENCES


Wotawa:1999:NDD
[WP90]

Waidner:1990:DCD
[Wri98a]

Wrixon:1989:CCO
[Wri89]

Wrixon:1998:CCO


Wrixon:1998:CCO


Wrixon:1998:CCO


**Wright:1999:EAE**


**Williams:1979:SRC**


**Wagner:1996:ASPb**


**Wiese:1996:SSS**


**Wagner:1997:ASP**


**Wagner:1996:ASPa**

REFERENCES


Whiting:1998:ITI


Whiting:1999:CBA


Wagner:1998:CO


Wagner:1999:CO


Weatherford:1999:NGA


Wagner:1997:CCMa

References

Wagner:1997:CCMb


Webster:1986:DB


Whitten:1999:WJC


Weiss:1985:RCM


[WW96] Williams:1979:CAA


REFERENCES


Dong Qing Xie. Partially efficient computation and criteria of security for public key cryptosystems. Hunan Daxue Xuebao, 19(6)
REFERENCES

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

Xie:1993:IPK

Xie:1998:WDI

Xu:1998:CEC

Xu:1999:NTR

Xiong:1999:LPK

Xiao:1994:MMH

Xu:1997:BPK

Xu:1997:PCP
REFERENCES

Xu:1998:STP


Yacobi:1999:RM


Yacobi:1999:RME


Yahalom:COMPSYS-7-4-451


Yamamura:1998:PCU


Yamamura:1999:FCU


Yan:1995:PTL

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


Yao:1982:PSC

Yao:1982:PSC

Yao:1982:PSC

Yao:1982:TAT

Yao:1982:TAT

Yao:1986:HGE

Yao:1986:HGE

Yao:1986:HGE

Yardley:1940:SSA

Yardley:1940:SSA

Yardley:1940:SSA

Yardley:1983:CBC

Yardley:1983:CBC

Yardley:1983:CBC

Yardley:1990:ABC

Yardley:1990:ABC

Yardley:1990:ABC


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

**Yoshiura:1998:VDW**


**Yeung:1997:DWH**


**Yeung:1998:DW**


**Yeun:1999:DSM**


**Yokokawa:1999:BDE**


**Yi:1996:DAN**


**Yin:1997:REA**


Yen:1997:SAT


Ye:1999:CS


Yi:1998:DCB


Yeung:1998:IWI


Yfoulis:1999:SOP

REFERENCES


REFERENCES

Youssef:1995:RBB


Yu:1992:NTD


Yu:1994:KAX


Yu:1999:CC


Yuan:1992:VLD

REFERENCES


Yung:1985:CSP


Yung:1985:SUK


Yung:1985:CSP

Yuval:1997:RTE


Yang:1997:CBC


Yang:1999:GSP


Yu:1989:DEB

K. W. Yu and T. L. Yu. Data encryption based


REFERENCES

Yeo:1999:WOV

Young:1999:ARC

Young:1999:ARA

Young:1998:MBB

Young:1998:MBS

Young:1998:ARA

Young:1998:MBB


Yeung:1998:DWS


Zafiropulo:1963:RAD


Zajacz:1997:SCE


Zang:1990:ESE


Zave:1999:SDC


Zegwaart:1993:PEM


Zeidler:1979:DDE

Howard M. Zeidler. *Digital data encryption*. SRI International, 333 Ravenswood Avenue, Menlo Park, CA
REFERENCES

94025-3493, USA, Tel: +1 415 859 6387, FAX: +1 415 859-6028, 1979. 20 pp. [ZFKP98]

Zergo:1996:UER


Zerovnik:1996:RC


Zollner:1998:MSS


Zuquete:1996:TAC


Zeng:1990:LSM


Zviran:1993:CPT

Zhang:1991:BNK

Zhao:1996:WSE

Zhao:1997:LT

Zheng:1990:PDS

Zheng:1995:HBR

Zheng:1995:KAP

Zheng:1997:SC
REFERENCES

[Zheng:1997:DSH]


[Zilouchian:1998:ANF]

[Zho94]


[Zieschang:1997:CPB]
REFERENCES

Zimmermann:1995:OPU


Zimmermann:1995:PSC


Zimmermann:1996:PGPa


Zimmermann:1996:PGPb


Zimmermann:1998:C1


Zimmermann:1999:EVI


Zhao:1995:ERL


Zhao:1996:DWS


Zhao:1998:GDW


Zhao:1998:BTT


Zhao:1999:DWW


Zeng:1997:RRO

Wenjun Zeng and Bede Liu. On resolving right-


Zheng:1993:HOH


Zheng:1993:PAA


Zhukowski:1998:JTUb


Zhukowski:1998:JTUa


Zunic:1998:MC1

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

**Zachariasen:1999:OAE**


**Zwiers:1998:CTD**


**Zeng:1990:LCT**


**Zeng:1991:ILS**


**Zeng:1991:PBG**


**Zeng:1995:GCG**


**Zhang:1996:DCC**

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