A Bibliography of Publications on Cryptography:
1990–1999

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

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

10 June 2023
Version 1.109

Title word cross-reference

#1
#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].

[SS98a, Ler97]. F_p [Miy93a]. GF(2) [She95c]. GF(208) [Ros98a]. GF(p) [Gor93b, HNM98].
\gg [GQW+91]. k [Car97c, DJL93, HKS97a, HKS97b, KR99b, KS97b, WD99b], t [HL93a, KS97b]. L2 [Vau99a]. \lambda [RS99c].
L \geq 2 [SVxW91]. \ll [GQW+91]. m [Bla94a, FR94]. Z/nZ [MM96b]. Z_n [SE96].
GD(2^n) [Ara93]. GF(2m) [FBT96]. F_{2^m} [MVZ93]. Step_{k,m} [GC90]. N [BS91e, BS91d, HKS97a, HKS97b, KSW99b, KSW99c, KK98, Per93, QG90, Tak97].
N = p/q [BDHG99a, BDHG99b]. N^{0.292}
Abuse [GJM99a, GJM99b, Des90b].
Abuse-Free [GJM99a, GJM99b, Des90b].
abuses [Des90a, Sch99g].
Academy [Tv92].
Accelerated [Luc99c].
AcceleratedX [Ano97-33].
Accelerating [Bir98].
Acceleration [TT99].
Accumulators [BP97a, BdM94].
Accuracy [BALS99].
Accurate [CH99b].
Achieve [Zhe97b, Sta94a].
Achieving [Cha92b, Cha92a].
ACISP’97 [VPM97].
ACM [ACM94c, ACM96b, ACM97a, AR97, ???97, D+98, ES98, HF97, KSS+92].
ACM-SIAM [ACM97b].
Acoustic [ME95].
Acoustics [IEE97d].
Acquires [GC97].
Acquiring [COM99, Stu99].
acquisition [Tod97].
ACSC+97 [IEEE97b].
Act [Ano97-50, Uni97a, Uni97b, Uni96c, Uni98f, Car96, Sin98, Uni98c, Uni98e, Uni97a, Uni97b].
Action [FJR96, Yam99].
Actions [Ros95b].
Active [BQ95b, BQ95a, Cra98, HCDC99, HHD99, HCY96a, LFCK99, MW97, Wai90, WHFG92, Wol98, BD95a, Cra97, HY98b, HY98a, Hor98].
ActiveX [Par98a].
Activities [Rhe93, Don98, SW94b, WS96c].
Acyclic [BM94a].
Ada [Car96, KT99, SVa+98].
Adapt [KMKH99].
Adaptable [PM99b].
Adaptation [GM99a, NAA99].
Adaptively [Beh96, FYM99, LL94a, ZS93, CP94].
Adaptively-Secure [FYM99].
addendum [WL92a].
adoption [Hol91].
Adding [Boy98, Men91, Eve98].
Addition [LYH93, SM91, ZNM99, CK93, LY93, dR95].
additional [UU97a].
Additive [Lai95].
Addressable [Way93a].
Addresses [Jac96].
Adds [Ach98].
Adelaide [KK99b].
Adaptable [PM99b].
Adaptable-secure [FYM99].
Eve98, FR95a, GP97, HJ99, HP94, Imp92, KKL99, MS99c, OS91, OS92, Pvo96, QN98a, Sch91b, Smi93a, Tab94, TY92, Tay90, TV94. 

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

All [Gol97d]. Alleged [Gol97d]. Alley [KR96a, PRB98b, Sch94f, Sch95a, Sch95b, Swa94]. 

Alliance [Ano98a, Gar97c]. Allied [LP9dbbbprm91, AK99]. Allows [Bee96]. 

ALM [CH99b]. Almost [AMP99, Bra95d, CCD99, Mau90]. Along [BDC+95]. Alpha [Zim96a, Zim96b]. 

Alphabet [PS97]. Alternating [HSW94, Wer93a, Wer93b]. Alternative [BsM94, Gar97a, Neu94, Smi93b, VvT97, BR96b]. 

alternatives [FL93]. Alto [Acm98a, IEE98a, IEE98b]. Always [Bra95d, Cha99a]. am [LC95]. 

Amazing [GC97]. America [HK99c]. American [Acc97, Bre97a, Bur99, Gla99b, Jno95, Mor92, Moy98, RK98b, Web93, Yar90]. 

Amiga [DDJ98c]. Among [BDPR98, Sch92b, Oka93a, SS95a, SZZ95a]. amounts [Ped95]. Amplification [ABDV98, BBCM95, MW97, CM95, Dl 99, Di99]. Amsterdam [Cha91]. 

Analog [GDS91, NT99]. Analog [Dem94, Cao99, SS95b, SS95c]. Analogues [LP94]. Analyses [SMK98b, BDHJ97]. 

Analysis [AO96, AMP94, BKS99, BR97a, BP98c, BS97a, BPRF99, Bro94, CM97b, CJRR99a, CRYY99, CH99b, DD99, Dra98, FM98a, FY95b, GS97, Gue98b, Gus96, Kea99, Ksf99, Kmt94b, KJJ99, LL97a, Lei99b, Lv98, MM99a, MT95, MD99, MO99, NA95, Pia99a, PB99a, Pre93a, PJ99, Sch99k, Sha99b, She95a, SVBJ96, SW93, Syv92, VNW94, W89a, WS96a, WS97, WB92, YMWP99, Yi96, AA99, Abr97, Bar91, BCK98, BM95, Cha94b, Don97, Don98, CEL98, KS90, LM96, LLG10, Nas94, Pau99, PS98b, RS93, RS99b, Tha91, vT94]. 

Analyze [MOM91]. Analyzing [Gil97, KAK96, NT93]. Anchoring [CS99]. 


annotating [DSSZ99]. Announcement [Ano99b, Nat92b]. Announcements [Ano95f, Ano95d, Ano95e, Ano97e, Ano97f, Ano97g, Ano98b, Ano94f]. Announces [Got99, Ano97-38]. Announcing [Ano97h, Nat97b]. Annual [ACM94a, ACM97b, Ano95r, Bri92, Bri93, Ch96, Copt95b, Copt9d, IEE92b, IEE93c, IEE94b, IEE94c, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE98f, IEE99a, Kra98, Spi95, Spi97, Spi98, USE99d, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, ACM99c, Com96, Des94b, HA10, IEE92e, IEE95c, IEE971, Kal97c, Kob96, TM99, USE96e, USE96f, USE98c, Wie99]. 

anomalous [GLV99]. Anonymity [BD99a, DFTY97, F-J98, JMP+98, STS99d]. 

Anonymous [DF98, DF99, FT99b, GMM97, Jae96, Jae99, MS99a, OKST97, PW97a, RSG98, STS99a, SP99, G91, Pfi95]. 

Anonymously [Coh96]. ANSI [Ano94b, Ano96c, Bak92, Bas98, BK98a, BK98b, Jno99, SS97]. 

Answer [WD99a, Ude98]. answers [Di 97a, Fre94, Ano92a]. Ant [BP95a]. Anti [Ano93a]. Anti-counterfeiter [Ano93a]. 

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

Antivirus [Nac97]. Antonio [ACM99a, IEE92b, USE98d]. Any [BM92, BJY97, DDP90, FJM+96, ZM90, Beu94, DF93, DKK98, Df99, HILL99, Pet98]. 

[Gol96c, Gon98]. App [AW99]. Apparatus [SKBxx, MY98]. Apple [Gar97a, GO96c]. Applet [Ber97a]. apples [GPO98a, GPO98b]. Appliances [Got99]. Applicability [KCCT94a, KCCT94b, HKM95, SPP98]. Application [IBM93, BS99a, BSN95, Bar99, BG995, BL96b, BL96a, Dam90a, Dam91a, Dav91, De 95, ECM96, FJR96, Fum97, GPT91a, GPT91b, Gog99, GQ95, HNNS99, HTH93, Hat97, Hel94, Hof99, IRM93, IR99, JKD+91, KMP99, KP99a, KI96, KK95, LOX99, LCN99, Mar98a, Mau96b, Mun91a, Mun91b, NC97, PNS95b, QV90, QG95, Rog95, Ru93, SSS98, Sch99i, SZ93, SK98c, SK98b, SKT97, VDD99, Ara93, BY93c, BY93b, CC98, DDB95a, DDB95b, DF97, G921, HP94, LL97b, MW94, Nyh98, Pet91, PK97, SII93b, SRR99, Siu99, Ste99b, SW98, SW99a, TY92, Woo90]. Applications [Aga92, BGR98a, BFW99, CG98, CJR98a, CJR98b, CGB+93, COZ99, Cre90, Dan96, DY91a, DFGH99, Du98, DN94, Dwo97, Ebe93, FM99, Far93, Fis98, IIE95a, IEE97a, IEE97b, IEE97c, IEE94c, IEE97b, JMS96, KH97, KSW98, KSW99b, KSW99c, KM96a, Knu94b, KT91b, Lan97, MS95f, ODP98, O900, PS96b, SY96a, DY91c, TN96a, TN96b, VW98, VP96, ZYR91, vW94, vW99, ACM99c, Ada91, Ano98k, Ano98q, BM90, Ber93, BMP+97b, BV97, Boy98, BP97b, Com96, CFG96, DIP996, DIX94, Dom96, Eng99, FO98, GP98, GEL98, Gre94, GS94b, HMP95, JV98a, Kal95, KKW92, KG93, LY93, LN94, Lub96, Mei92, Mic97, MT98, NKC94, Ped91a, PC98, Rh90, Sch90c, Sch97c, Sha95a, SSM94, Siu95, Sta97c, SSG99, T+98, USE96e, Way98, YL93, ZYR90]. Applied [BHJM99, HH98, MR95a, Sch94a, Sch96a, Sch94b, Sha99a, FFW99, FMR99, MV97, PR98, CMM93, Dav94]. apply [Cl97, UT97b]. Applying [CO98, HO96, Jan99, KMP99, MW98a, War98, ARR99]. Appraisal [FGS96]. Approach [BBN96, BK94a, DGV94a, DS97c, GM99a, Hes97, Jak99b, KJ98, LMS99, Mar99, MS94, MI99, PL94, PWU99, PJJ99, Rab98, STS99b, She94a, WS99, ZHJ98, Ale97, BCK98, CM96, CH97b, DH96a, DD98, GM91, GKS97, JW91, OG95, Pau98, PGV93b, PGV94, RO96, ZL99]. Approaches [CJRR99a, GFB93, Mau91a, RDK98, VGP93, ZS93]. Approves [Gar98b]. approximate [MW94]. Approximating [SG95]. Approxi mation [KG95, KR99b, MT99b, MI96a, RS99a, CS97d, G9096, Nyh95]. Appro ximations [KR94b, ST91, KR95a, KR96c]. April [ACM97a, Ano95b, Ano99c, A9c8, Ch98, Chr99b, Dav91, IE95c, IE97d, IE98d, K99b, Lam97, QV90]. Aquarelle [ADF98]. Arab [AK98]. Arbiter [D91f, JS95b, JS95a]. arbitrary [Pie93]. Arbitrated [D91f, HW98c]. Arbitration [Joh94, Kur94, PLW99, DS93, KO95b]. arcane [Beu94]. Archaeological [Ano97-37]. Architectural [BS95c, PN92]. Architecture [IBM93, BCC99, CJR98a, CJR98b, Con99a, Fei93, Fei96, Gut99, JKD+91, MM99b, Mun93, NH91, N98b, Oh99, PF94, RB94, Rus90, SS90, She92a, She93c, Tre99, Tua99, VGG93, Y999, Kar96, L98a, Con98, JD91, LMJW93, SV99, SY92]. Architecture/390 [SY92]. Architectures [Ara93, Gon99, KV99, Lee99b, Lip99, LF99, Mas91, P97, SSS98, BGV97b, Kap98, LH99, PBM90, WDBF97]. Area [Fun93, LE99, Van95b]. areas [HA00, TM99]. Aren’t [Cha99a]. Arguments [BJ97, BD91, NOV93]. Arias [DHMR96]. arising [AP93]. Arithmetic [BP98a, Bre99, BP97c, Bus97, CD98b, DB96, KK99b, LL99, LD99, Mih94, NM96a, P97, SSS98, SJ93, C998, ISO97, JS93a, Kal92, Kal93b, KM99a, Pos93].
USE98a, USE98b, USE99a, Wie99, Yu92a. AUSCRYPT [SP90, SZ93]. Austin [Ano94c, IEE98e]. Australasian [VPM97]. Australia [DG96, GN95b, KG93, KK99b, MSD90, PSN95b, SP90, SZ93, VPM97].

Australian [CFK+91, GN95b, Cae96a, Orl96, Ree97]. Australia [DG96, GN95b, KG93, KK99b, MSD90, PSN95b, SP90, SZ93, VPM97].

Australian [CFK+91, GN95b, Cae96a, Orl96, Ree97]. Austria [BS95e]. Authenticated [BF97a, BWM98, BWM99a, Bor95, CHH97, Dan95, HCY96b, JY96, LC97a, Mau97a, RH93, SKWH96, BSNP96a, BSNP96b, BF99b, BR97b, DwW92, HY98b, HY98a, Yen99].

Authenticated [ADSW99, Hel98a, KS99a, Mit92a, SK96a, Sha97, LC94]. Authentication [ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94k, AS96, Atk95a, AR98, AC97, BA97, Bak99, Bal99, Bec99, BR97a, BG90, BR94a, BCK96d, BCK96e, BM91a, BGS98, BR91, BBDF97, BGH+91, Bisk91, BHK+99, BWM98, Bn95b, BV98b, Bor96, Bor93a, Bor93c, Bor93e, Bru98, BAN90, CV93, CGM97b, COZ99, DLF97, DVPL92, DV90, DY91f, DwW92, DH90, Dra99, DMB97, DS97d, Dsw95, ECM96, EPR99b, EPR99a, FGS96, FH97, FL96, GKY90, GLZ99, G96, Geh94, Geh95, GN94, GM90, Go90a, GBL94, Gu98b, Gui97, HK97, HA94a, HS94, HL92, Hil97, HP99, HP99b, Ins95, IH98, JSG94, Joe98, Joh94, KR95b, Kau93, KA98a, Kau90, KN93, KCT94a, KCCT94b, Kra94b, Kra95, KBC96, KBC97, Kurf94, KK95, KY92, KY92b, K97c, LAB91, LABW91, LABW92].

Authentication [Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Man96a, MAM95, Mc96, Mee98, MS95c, MS95d, MWW94, MTV92, Mor97, Mye94a, Mye97, NG97, OOK91, OM94, Opp96, PKOT94, PS88c, PLWSN99, P91, PGV93c, Pre98a, Pre98c, M95e, RS99b, RRSW97a, RRSW97b, Rog95, SNT93, SN93, ST94, SNT95, SNW98a, SNW98b, SSH93, SS96, SP99, SA95, SC96a, SCxx, Sch94d, Sch99k, Sga90, Sga91b, She97, She95a, Sha96, Sim96b, SVxW91, SW94c, SKAM99, ST91b, SL99, TAP90, TA92, Tay95, TSN93, Tun99, Ude98, V95b, Van93, Wal95, WKHG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC+98, Ano95g, Ano95o, Ano95x, Ano96v, Ano96x, Ano96y, Ano96-27, Ano97d, Ano97t, Ano97p, Ano97-27, Ano97-43, Ano97-53, Ano98s, Atk93]. authentication [BSNP97, BGR95, BCK98, BC97, BBGF97, BGH+95a, BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gna90, HS96b, Hor95, HC95b, HLL+95, HV98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin89a, Low95, MSN97, MF97, Men91, MC96, Nac93, NT94, PS98e, PS98f, PS98h, RS98a, RS98f, Sch99, Sga91a, Sga93, SY96b, Sta99b, Sti91a, Sun80b, Syv93, Tsu92b, Tsu92a, TH99, Ver98b, Web99, WL94, XA98, Xie98, YL97a, YL97b, You97, Z98b, ZH93, VT93, Mye94b, Ala93b, Bor93b, WL92a].

Authentications [OO90, KSL92]. Authenticator [Zuk98a]. Authenticators [DF91a, SN96]. Authenticity [BK90, Lud97, Ano99j, MI90, Way91]. Authenticode [Fly97]. author [Lea90]. Authority [Ame95, Ame96a], authorities [CF96, CGS97, MO95a]. Authorisation [BDPSN95, Cas95, FL96, W90]. Auto [YY98c, YY99b]. auto-certifiable [YY98c]. Auto-Recoverable [YY98b, YY98c].


Automating [Bur99, Smi93a].
Por93, PGV91, PGV93b, PGV94, RP95b, SV94, SV95a, Sha94, SRL98, Sim98c, SM90, SS95b, SS95c, SMK98b, Son99, SKD94, Ste95, SS98b, SZT98b, Tan90, TA97, TAP90, TC91, VNM99, Ven92, Wan92a, WKHC97, Wi93a, WWW95, XA98, YWC97, YL97c, Zhe95b, ZPY96, vO92, vT94, CD96, YKY99, Dhe98, Por93, TY98b, TY98a.


Blacklisting [KRS99]. Blackmailing [Jak95]. BlackNet [MLLG95]. Bletchley [Ano97-48, Sal93, Cla89c, HS93, Smi98b]. Blind [CPS95, Eri97b, JLO97, LK99, LR98, NMV98, NMV99, Oht98, PS96c, RGV97, SY96a, SYMI98, HMP95, Tra97, XA98]. blindfolded [JY96]. Blinding [Bra95c, Kra99, FY95c]. Block [AB96a, ABK98b, AK98, BKR94, BAK98, CDN98, Cle91, CJM95, DGV94a, DKL97b, DKL99a, DR99a, DDDN98, De 99, DW94, JK97, Jak98, KR94a, KV99, Knu94b, KP96a, Knu98b, Kmu98c, Knu99b, Kob99, LM93a, LM93b, LM91b, Lim98, Luc98a, Luc99a, Luc99b, MNSV97, Mas94, Mat96a, Mat97, MT99a, MSK99b, Pa99, P97a, Q90, RRSY98, Rob95a, TZ96, Sch94b, SK96c, SK96d, SW98b, SW98c, SW98e, SW98f, Sch99d, Vau98b, V96, YL98, YLY98a, YLC99b, ZM90, Zhe90, Al93a, AW95, BKR98a, BKR98b, Br93, BS95a, Har96a, HLMW93, HX94, ISO97, Jak99a, KL95b, LM91a, Lai92, Mei94, MM97, NO96, Nyb95, PGV93b, PGV94, RT93, RP95b, Roe95, SB95, SAM97, SH99b, SKD94, TY94, YL97c].


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

Broadcast [ASW99, Ber91, BC95c, BC96a, BFS96, vD97, FN94, GSY99, KYDB98, LS98b, SW99b, WD99a, BMS96, BMS98, GBI94, 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, PV99, Tas98].

Bulk [SVBJ96, Whe94].

Bulk-FFT [SVBJ96].

Bull [Taa98].

Bulletin [CWM91].

Bulow [CWM91].

burden [Wil98a].

Bureau [Uni97d].

bureaucracy [Rat96].

burglars [Way95].

Burlington [IEE96a].

Burns [DDJ98b].

burst [Sch93a, UNU94].

Bus [CC99c, Kuh98].

bus-encryption [Kuh98].

Bused [FVEA99].

Business [Ano93i, Ano96-29, Ano96-30, Ano97-33, Ano98t, AMP94, Av99, CFK+91, GC97, Lic94, MB99a, SM99, Uni98j, ZKL98, B+96a, Kir95, Uni98k].

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, He98b, Kaj92, MGL+98, Sch94g, Sch96a, Sch94h, Sed92, Ste90a, Ste90b].

COYNTIA [WBBLL99].

C2 [Ste92].

CA [RD99a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE90g, USE96b, Wi99].

Caching [STSW99].

Cactus [Ano97-33].

CADE [HB99].

CADE-16 [HB99].

cAESar [Koe99].

Calculating [CFK+91].

Calculation [HRV99].

Calculators [CWM+91].

Calculus [AHL93a, AML93b, AM93c, AM93d, AM93e, AM93f, AM93g, AM93h, AM93i, AM93j, AM93k, AM93l, AM93m, AM93n, AM93o, AM93p, AM93q, AM93r, AM93s, AM93t, AM93u, AM93v, AM93w, AM93x, AM93y, AM93z].

California [ACM93b, ACM98a, Ano97a, Ano97b, Ano97c, Ano97d, Ano97e, Ano97f, Ano97g, Ano97h, Ano97i, Ano97j, Ano97k, Ano97l, Ano97m, Ano97n, Ano97o, Ano97p, Ano97q, Ano97r, Ano97s, Ano97t, Ano97u, Ano97v, Ano97w, Ano97x, Ano97y, Ano97z].
AHdJF97, Ano96g, Cha99b, CW97, Cha91, Di 97a, Di 97b, Kip97, Sha95a, Taa98, GPSV98, Bar99, Bro97, HNS99, SSM94, SKAM99. Cards [Ano96z, Ano99e, BDB92, Cha99a, CM99c, Con98, Con99a, Cor98, CH99a, DJ98d, DDJ98b, DDJ99, Deu97, Deu98, Fan96, FW91, FGLP96a, FGLP96b, FO97, GL96, Gut98a, HK99, JT97a, Koe99, KCCT94a, KCCT94b, MSN99, Mye96, NM96b, PV98, Roh99, SKW+98d, SS99a, Sch90b, SR96, Smi98a, Taa99, VV98, ABKL91, ABKL93, Ale97, Ano98q, BGV97a, Bro97, CJRR99b, DS98a, Dhe98, DT98b, DF97, Gau97, TJ97, AG99, Bak99, BF99a, Gir99, GSTY96, LW99, NF99q, cardT0AP [SGPV98].

Carl [Ano96h, Ano96s].

Carmichael [Pin97].

carrier [SVWMB95, SOB98, VSB95].

Carry [SM91, DF92].

carry-save [SM91, DF92].

cartesian [DVW90].

cascade [BCK96b, BCK96c, YL93].

cascades [BCK96b, BCK96c, YL93].

case-Based [DSSB95, FR95d, GR99, MD99, MR95a, PK99, Var99b, AD97, AD99, BHR99, DLF93, LMS97].

Case-Based [DSSB95, FR95d, GR99, MD99, MR95a, PK99, Var99b].

case/average [AD97, AD99].

Cases [MCM95, Blo99].

Cash [BFP99, Bra95b, Cha93, DFTY97, DT98a, En98, ENK99, FO97, Jak99b, LR98, NM98, OO90, ST99a, ST99b, Tra99, Yac99a, Yac99b, AMS96, VNM99].

CASL [Mos99].

CAST [Ada97a, Ada97b, Ada98, KSW97a, KSW97b, MSK98].

CAST-128 [Ada97b].

CAST-256 [Ada98].

casting [Pit96a].

cataloguing [DSS99].

catch [Way93b].

catching [WS96c].

Caught [Mei98].

Causal [RG95].

Cautionary [KM92, Roh99, CJRR99b, RS98f].

Cautious [Gl99b].

CBC [Eph98].

CBC-Mode [PA98a].

CBCM [BK98a, BK98b].

CBR [GAGCDAFC99].

CCI [WCS95].

CCI-Based [WCS95].

CD [Ano96r, GTGW94, Ros94, UFC94].

CD-ROM [Ano96r, GTGW94, Ros94, UFC94].

CD-ROMs [GTGW94, UFC94].

CDE [Ano97-33].

CDL [HHW99].

CDMA [KBK98, DGV93, HHW99, NC97, BMP+97b, BK98f, MZ98, NKC94, PV90, Sut99, WSK97a, WSK97b].

Center [Ano94e, Ano96a, IEE96f, NIS92, LWC96].

Centralized [KT96].

Centre [IEE97c].

Certain [CS91, MS93, MM92a, CFS97, Ev92, Kuk99].

Certificability [YY98c].

Certificate [Bra93a, FL99b, HPS99, RSA93c, Riv98b].

Certificates [Bra95b, Bra95c, NKP99, TAP90, TA92, DS90a, FF99].

Certification [Kal98c, KM99c, LA98, Ame95, Ame96a, GH96].

Certified [Kir91, Mer90b, RS98b, SG99a].

Certifying [BY93a, LN98].

CFB [PNRB94].

CFR [UU97b, Cli97].

Chaffing [Riv98d].

chain [JV98a].

Chaining [BKR94, CJS95, Jas96].

Chains [YY98a, dR95].

Challenge [Ano97c, Ano97-40, BCE+94, DDJ98e, DDJ98f, Sim96b, WD98, Wir98, BT97, Ano97c].

Challenges [Ano98i, BS97b, GB98, Mc99, Buc95b, Cer97, FM98b].

Challenging [CM99d].

Chamber [Var90].

Chameleon [AM97].

chan [XmTmW94].

Chance [GB98].

Chang [Bur94a, Bur94b, HLLC96].

Chang-Wu-Chen [Bur94a, Bur94b].

Change [FY99, Wal99b, HJT+96, MW98a].
changeable [HYLT99], changing [MW98a].
Channel [AO96, AVPN96, ADEDS99, BI99, Bro94, KSWH98a, KSWH98b, KSWH98c, MM92a, MM92b, OKST92, WB92, BM95, FC94, PSB97, P695]. Channels
[BDI+96, Cre97, Des96a, vD97, KI97, Lip94, MM96a, MK94, MM94, PN92, SI94, Sch94e, Sim93, Sim96a, Sim97, VNW95, WD99a, Des96b, Gru98, Man91c, SI93b, Sch93b, Sim94c, Sim98a, Sim98b, Tod97, YL97a].
Chaocipher [Joh98]. Chaos
[BGR94, BLM94, Ano96-29]. Chaotic
[Bih91, GKS97, HNSM91]. Chaotic-Map
[Bih91]. CHAP
[Sim96b]. Chapter
[Kal97b]. chapters
[Tat98, Tat99]. Character
[BL99, Sab94]. Characterisation
[SB95]. Characteristic
[KMKH99, Kob91b, MVZ98, SS98a]. Characteristics
[Fer98, Knu93b, SZZ95c, She95a, ZZ95, HT95, RP99b, SZZ95a, ZZ95b]. Characterization
[BS99b, BS99c, CCD99, DDP99, Ito91, PLWSN99]. Characterizations
[FY97, Sti91a]. Characterizing
[MW96a]. characters
[lPNdbbbprm91]. Charles
[Lip98, KT99]. Charlesworth
[CWM+91]. Charing
[Atk93]. Chasing
[Gar97b]. chausses
[Sch98e]. chausses-trappes
[Sch98e]. Cheap
[LT98]. cheaper
[Sch98c]. Cheaply
[Ano93j, Str93a, Str93b]. Cheater
[KOO95b, KOO95a, LH93b, HC96, HLC96]. Cheating
[GP99, Rab94, OK96b]. Check
[BK95c, Blo98c, Tay94]. checker
[Dan97]. Checkers
[Fis97, KA91]. Checking
[BGR99a, Bol98a, Bol98b, BD97, FL99b, FGY96a, GM98, PV98, BCR98, FGY96b, MHPS96, MW94]. Checks
[DT98a, PK95a, PK95b, Pen96]. Checksum
[PGBV90, LRW93]. Chen
[Ala97, Bur94a, Bur94b]. CHES
[KP99b]. chi
[XtTmW94]. chi02
[HG97a]. Chicago
[USE96a, USE99c]. chieh
[XtTmW94]. chin
[XtTmW94]. China
[HOQ97, OiDP98, XtTmW94]. Chinacrypt’94
[XtTmW94]. Chinese
[DiDSP96, GO96c, QD91, WW95, Yu99]. Chip
[Ban94, Bro96, Ele98, Gar97c, GC97, Got99, HMvT94, Lan97, MPPS95, MHW98, VVJD90, Way93b, DVP96, Kan96, Mac97, Pos98, RKD94, Sim94a, Uni95a]. Chipkarte
[Kip97, Kip99b]. Chips
[Ano99c, GO96c, Omu90, Ano97-29]. Choice
[Cha99a, Way98]. Choices
[Hon98, Van95a, Wel95]. Chor
[BFS98, SH95a, SH95b, Van98a, Van98c]. Chosen
[Ble98a, CG99, S99b, Dam91b, GC94, KSW98a, KSW98b, LL94a, PBBV90, RS91, ZS93, BJ97, CP94, NY90, SNT95, Sah99, SG98, Tze99, V93]. chosen-ciphertext
[Sah99]. chosen-message
[SNT95]. chosen-plaintext
[vT93]. chronicle
[UFC94]. chronology
[Kah98a]. Chua
[YWC97]. Chump
[Val99b]. Chung
[XtTmW94]. Chung-kuo
[XtTmW94]. Church
[Ole95]. CINDI
[DSSZ99]. Cipher
[Alv98c, AM97, ABK98b, ABK98c, BKR94, BAK98, BD94, Boy90, BCA98, Car97b, Cla97, Cla98a, CJM95, DGV94a, Dae95, DKR97b, DKR97a, DW94, EM93, Goll97d, KR94a, KMA98, Knu98c, KR99a, Kuh98, Lin98, LS97, Lip99, Luc98a, Luc99a, Luc99b, MNSV97, MD98, Mat94b, MT99a, Man91d, Mil96a, Miy91, MSK98, MSK99b, PA98a, QG90, RDP96, RRS98, Rocz98a, SZ96, Sch94b, SK96c, SK96d, SKW98b, SKW98c, SKW98f, Sch98i, She94b, SMK98a, Van98d, WBDY98, Yf96, YL998, YLCY98a, YLCY98b, YZWR91, Zhe97a, Lip98, Bar92a, Bar95, BK95a, BMP97a, BS95a, CS96b, CS97b, Cra92, Dav98a, Dav98d, Dav98c, Daw96, Fra93, Gad98, GGH98, Gol98b, Gol99b, ISO97, Kru98, Lew92, LCL95, Mac98, Mat93, MY93a, Mei94, RT93, Sei98b, YL97c, Zun98, SV98, Ers99, Van99b, Van99c]. Ciphering
Ciphers
[Ada97a, ABDV98, AAG+00, AB96a, BR99a, BDR+96, CDN98, Cha94a, CS91, Cle91, DR99a, De 99, Din94, Fli95, Gus96, JIK97, Jak98, JJ99b, KSW98a, KSW98b, KSW98c, Knu94b, Knu94a, KP96a, Knu98b, Knu99b, Kol99, LMM91, LM93a, LM93b, Luc96a, Luc96b, Mat96a, Mau91a, MS91, MT99c, PRS99, Pat99, PK95a, PK95b, Pen96, Pra96, Pre97a, Ree98, RP97a, Rob95a, Rob95b, Roe94, She94a, She94d, SM91, Van99b, Van99a, YY98d, YY98b, ZMI90, Zhe90, Abe98b, BKR98a, BKR98b, CD98a, Cog99, CD97, CS98b, Dam91b, DSLV99, HSW94, JKK99a, JV98a, Lai92, LMM92, LRW93, NY90, PGV93b, PGV94, Rev91, RP95b, Roe95, SB95, SAM97, Tay94, Win93, Wri98b].

Ciphertext
[BK98d, Ble98a, CG99, CD97, CS98b, Dam91b, DSLV99, HSW94, JKK99a, JV98a, Lai92, LMM92, LRW93, NY90, PGV93b, PGV94, Rev91, RP95b, Roe95, SB95, SAM97, Tay94, Win93, Wri98b].

Ciphertext-Only [BK98d].

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

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

Cisco [Sav96].

CISST [AA97].

City [IEE99a, USE95b].

Claim [GO96c].

Claims [DS97a].

clandestine [Wri98b].

Clar [USE93].

Class [vD97, Ou97, Uni96b, FR94, HWB93, KSB96a, LZ90, LZ91a, ZUK94, vT94].

Classes [Haw98b, Pau99d, Haw98a, Sze98].

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

Classification [BD90, LSV95, PNFK5, Uni96b].

Classifier [CIBM99].

Clau [Hor92].

Claw [BHT98].

Claw-Free [BHT98].

clearly [Los98].

Click [WSFC99, Ken95].

Client [DL99, Kon95, Oh99, SL99, GGK+99, Sin95].

client-relationships [GGK+99].

Client-Server [DL99, Oh99, Sin95].

Client/Server [Kon95].

clients [AG95, Bee96].

Climate [TGGK99].

Climbing [MCD99].

Clipper [Pri94, Fro96, Ban94, Bro96, Buch95a, Hof93, Kan96, MS95f, RKD94, Sni94a, Uni95a].

Clipper-like [MS95f].

Clipping [Hof93].

cliques [JP96].

Cloak [Gre90].

Clock [DHSS95, GO96b, Gal94, CS96b, CS97b, GM91, GO95, Men95b].

Clock-Controlled [GO96b, GM91, GO95].

Clocks [DG95, DGT96, Yah94, Gou92].

Closure [Coh96].

Co-dimension [LFC99].

Co-operation [Gla99b].

Co-Processors [Sut99].

co-processors [NM96a].

Co. [CFK+91].

Coast [SZ93].

COBOL [Gar97c].

Code [CJ99, HR90, JJ99a, Kip99a, Kur94, Mv93, PV98, QD91, Sch94g, Sch96a, Sch94h, Str95, Tod97, WK97, WF94, Zim95b, Ala97, Ano97, BSNP97, CC98, CLW98, GA98, HM97b, LJWH97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG+90, Mea98].

Code-Breaking [QD91].

code-cracking [WS96c].

Codebreakers [HS93, Kah96b, Sni98b, Yu99].

Codebreaking [Car97c, Car98, Dre92, Sch98a].

coded [HG97c].

codemaker [Mar98b].

CODER [Sto90].

Codes [ACM94b, AW94, AR98, BGS96, BVFD99, CCZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, Gill91, Hof99, Joh94, JS95b, JJ99b, KKS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWS999, Pen96, Pra98a, RV99, Rus93a, SN93, SNW98a, SNW98b, SD99, Sga90, Sga91b, SB94, SVx99, Sta99b, Sti91b, Ton96, Van95b, Wri98b, Ada91, Ala93a, AW95].
BSB97, BI93, Bru91, CC98, Cha95a, CMM93, FC94, Gre90, JM96a, Kah91a, KO95b, LYG94, LMS90, MSS93, MPL99, Moh92, SNT93, SNT95, Ste95, Sti91a, Su98, SS98b, TSN93, TY94, Wan92a, Wel97, Win93, YL97a, vT94, JS95a].
codewords [PS97]. Coding [Ber96b, IEE97e, KRS99, KH98b, LW91, Lip94, Sch99b, She94c, SW95b, Van95b, Wal99a, Ada91, Boy95a, Boy95b, Dar97, DiDPS96, Far93, Gan93, KSB96b, KSB97, Kujo90, Mit92b, Sab94, Sch98b, Sga91a, SVWMB95, SOB98, Shp99a, SMS99, TA97, Ger97].
coefficient [GK95b]. Coevolution [Nac97].
Coin [BN96, Jue99, PW97c, Ueh95]. Coins [EO95b, WSFC99, EO95a].
COIRS [YKY99].
Collaborators [Gla99b]. College [Far93, IEE97a, UFC94]. Collision [BP97a, Dob97, PGV91, Rus93b, Van93, vW94, vW99, Dob95a]. Collision-Free [BP97a, Dob97, Rus93b, Van93, Dob95a].
Collisionful [Gon95, BSNP96a, BSNP96b].
Collisions [Ano95a, CJ98, DBGV93, dB94, Gon95, Sim98c]. Colloquium [Ano97-28, vWN99].
Collusion [BS95b, BS98, EKK99, PW97b, LM96].
Collusion-Resistant [EKK99].
Collusion-Sécur [BS95b, BS98]. Colony [BP95a]. Color [ADED99a, NNE97].
Colorado [Sch99b]. Colossus [Ano97-48, Car97b, Car97c, Car98, Pin98].
Column [Bar94a, Bar94c, Bar95b, Bar95d].
columnar [Bar92a]. COMANDOS [TCH+91]. Combating [DN93].
combination [Rev91]. combinational [HL94]. combinations [RT93].
Combinator [SAS99b]. Combinatorial [FK94, KO95b, KO95a, KO96, KO97, LS98b, Rus93a, Sti91a, Zie97, FSS94, Sta97a].
Combinators [MWW94]. Combiner [SG99a]. Combiners [MS91]. Combining [KMK99, NA95, SA95]. comes [Fox98].
command [Mye94b]. Comment [DKKK98, LC96c, YT96, BMP97a].
commentaries [Ano97-37]. Commentary [BL99]. Comments [BMP97a, COP95a, Dun94, JW01, KSS+92, MC96, NC97, Ng99, Pr95b, SB93, WHL99, Ala97, Gib90].
Commerce [Av98, Cli97, DD98d, DB99, Jak99b, LHB96, Lut98, Un97a, USE95c, USE96d, USE96c, USE96b, Un97d, An97b, BH98, FB97, Gar97b, LM98a, Man95, Sin98, Tas98, VM96, UU97b, Un96b].
Commercial [Bhi96, BDR+96, Cae96a, WLEB96, Cha94b, Dix94, Joh90, Sta94a, JML94].
Commitment [Dam99a, IOS94, Sal98].
Committed [DF99]. Committee [Un97a, Un98d, Un98e, Un96c, Un97b, Un98f, Un98h, Un97c, Un95a, Un98k, Mad96, Un98c].
Commodity [Bea97].
Commodity-based [Bea97a]. Common [IBM93, Lin93c, Mau93a, Tze99, JDK+91, JD91, LMJ93].
Communication [???97, AR99, BF97a, Bet95b, BFS96, CHH97, CMN99, FJP96, FK99, FT99b, IKM99, Jam98, KFJP96, KRJ98, PW99, PM99a, SSN98a, Sim94a, WD99a, Wei99, BF99b, Bet95a, BMS96, Com97, CWY98, CK93, Cli97, DFKN93, Hamxx, Rivxx, Sch90c, Sch97c, SD97, Sta97a, UU97b, Ven92, Wirts98]. communication-privacy [CK93]. Communication-Storage [CMN99]. Communications [ACM93a, ACM94a, ACM97a, Ano93b, Aur96, IEE94f, IEE97k, KM93, Kat97, MB94b, Ve93, BY93c, BY93b, Car94, Cha94b, Cra96, HOQ97, Hwa93, IEE92d, IEE95c, JC93, M1995, Oht96, PP96, Par96, Rhe94, SW94b, Sch93a, Sch92c, Sz97a, ZG96].
communicators [Ano97-28]. Communities
Commutative [MB99a].
Compact [GPT91a, GPT91b].
Compact [Ort95a, Ort95b].
Companies [Ano97j, Ano97y].
Company [GC97, Ano96g, Kar96].
Comparative [Dae99, Ste92, AA99, Don98, She92g].
Company [GC97, Ano96g, Kar96].
Comparative [Ano97j, Ano97y].
Comparisons [Bih99c, HSSI99, HKL94, KAK96, NM96b].
Comparing [Bih99c, HSSI99, HKL94, KAK96, NM96b].
Comparison [BALS99, Cus97, KH98b, LM98b, Mas99a, May97, MG91, vO91a, QN98a, SKW+99a, SKW+99b, Wie98b, Wil93b, vO91b, GM91, Yen99, ZHI93, vO92].
Comparisons [Bih99c, HSSI99, HKL94, KAK96, NM96b].
Compartmented [GPSN98].
COMPASS [IEE94b].
Compatible [SK94, Wat99].
Competence [WS99].
Competing [Sta97c].
Compiler [NM99, SSCP99].
Complementarity [DD99, LM93c].
Complete [Tou91].
Completeness [Bro94, Sch94k].
Complex [NT99, MCD98a].
Complexity [Bus97, CH96, Cle91, DSV99, GM99b, HKL94, LMSV99, MMT90, MS94, MMM+98, Mun91a, Mun91b, NMVR95a, NMVR95b, NOVY93, Sch99l, Smi98a, Bao94, CS97d, DDP94b, FK93b, GZ91, GN95a, Gol97c, Hii94, MM99a, MS98a, MK1992, Shp99b, SMK98b, Sze98].
Compliance [Dav96].
complies [Ano96u].
Component [NK98b].
Composite [Pai99d, BBR99].
Composition [ABDV98, GK96].
Compositional [DJHP98, HJT99, MM99a, Zwi98].
Comprehension [MT95].
Comprehensions [MT95].
Comprehensive [SSP90].
Compress [Ano96e, Dob97, Dob95a].
compressed [CPO+98, CHO+98, HG96, HG97c, HG98].
Compressing [GI99].
Compression [CI96, DLF97, KPR99, Sch99b, BCR98, CW94, Cra96, Kop97, Oht96, Sab94, Sch98b, dB94].
Compromise [Gar97c, Ano97u, Hed97].
CompuServe [GC97].
computability [BK98f].
Computable [DSV99].
Computation [BM99a, BM99b, CH98, Cra99, FHM98, FH94, GM93b, HHT93, HHT97, HCY96a, KR94c, LO91a, LYH93, LL95a, Mon93, Mor98, PK95a, PK95b, SSN98a, Wat91, ARW99, Ata99, BHKR95, BM94c, CL97a, GM95, Hor98, LY93, MILY93, PW93a, Shp99a, Xie92].
Computational [CH96, HKL94, Kos97, KRS99, PG90, Sab94, TGK99, BC95a, Ger99b, MC90b, Pum90a, SS95a].
Comparisons [GC97, Ano96g, Kar96].
Computations [Cha90, CDD+99, Mas91].
computed [Ev92, EvH93].
Computer [ACM93a, ACM94a, ACM97a, Ano93d, Ano97-50, Ano98c, Bac95, BK90, Ber96b, Bre99, CWM+91, CO98, De 98a, De 93b, De 98c, DQ93, Des92, DEQ93, FJM+96, GMV98, HM91, HM92, HM95, Hig97a, Hig97b, Hor94, IEE92a, IEE92b, IEE92c, IEE93b, IEE93c, IEE94b, IEE94c, IEE94d, IEE94f, IEE96a, IEE97b, IEE97f, IEE98a, IEE99a, KT99, KK99b, LBMC94, LC95, MDP94, NIS92, Nae97, Nett92, OD99, PGV93d, Q+98, Sa91, SSS98, SK96a, SK99, Sho97, Ste91, SI99, VG93, Ver98a, VG99, Whi90, AFB95, Ano93k, AC97, Bur98a, Car97c, Car98, CW91a, Coh94, GBL94, Gru98, HLLC96, IEE92d, IEE95c, Joh98, LS98a, LFSY94, LC96b, LC96c, Mat98, NT94, Nos91, PR98, Riv98c, Shp99a, UFC94, Wil93a, Woe97, Woo90].
Computer-Related [De 93b, De 98c].
Computerized [Ive91].
Computers [??97, BF99a, CWM+91, HM96, Kan96, Sch98c, CFK+91].
Computing [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98a, ACM98b, ACM99b, Bak92, BDDG99, BV96, Bra94a, CFK+91, DDJ98d, DDJ98b, DDJ99, Dwo95, FP99, GC98, GN95b, IEE94e, IEE96b, JJ98b, Kon95, Law98, MMM+98, Mau94, MW99, N98a, Pen96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b,}
BGT96, CWM91, DiDPS96, FM91, FJV97, HK99a, HC95a, KG93a, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK91, PH91].
COMSEC [Mye98]. concatenated [LYG94]. concealed [Ano97i, CZ90, Lea90]. Concealing [CD97, Beu94, Joh97b]. Concept [Lin98, GM91, HLC99, YKY99]. Concept-Based [YKY99]. Conceptual [NL98, GM91, HLC99, YKY99]. Concepts [BFW99, Des99a, HL99, KG99, Lan98, SSP90, Ano96s]. Conceptual [Ako99, BPRF99, HL99, MI99, Snu99, VC99, Wed99]. Concerning [Cle91, Hub91, FR94, Fri96, GHS93, Gro94, Sim98b]. Conciliation [BBDF97]. Concrete [OO98, BCK96c, BDJR97]. Concurrency [SG99b, IEE94b]. Concurrent [BMT98, DO99, DS98b, RS99c, Zwi98, ARK99]. condition [Sta96b]. Conditionally [Des90b]. Conditions [GS99a, Rus93b, Gua99]. Conducts [Law98]. Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95r, Ano96r, Ano96a, ???97, Ano97i, Ano97g, Ano97a, Ano97b, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BS95e, CH96, Cha91, Cop95d, DDJ98a, Dan96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, Hir97, Hir98, IEE95a, IEE97a, IEE92b, IEE93c, IEE94b, IEE94c, IEE94e, IEE96b, IEE96c, IEE97b, IEE97c, IEE97h, IEE97d, IEE97l, IEE97j, IEE97k, IEE98c, IEE98f, IEE98e, IERM93, KG96, Kat97, KM96a, Kra98, LOX99, LP99, Mau96b, MS99a, NIS92, Nat98, Nat99b, Nyh98, OW95, ODF98, PSN95b, QG95, RD99a, RD99b, Sch94m, SJ97, SIK93, Sif93b, Sti94, T+98, USE91, USE92a, USE94, USE95a, USE96a, USE99b, USE99d, Wal99a, Ya92, ACM99c, Ano93d, Boy95b, BD95b, Cop95b, Dar97, DGC96, Des94b, HQ97, HI97, IEE92d, IEE95c, IEE96f]. Conference [IEE98b, KaI97c, KG93, Kob96, LM98a, SP90, Ste99b, USE96f, USE98c, USE98d, VM97, Wie99, Ano95f].

Constructions [AHV98, ABDS96, KRS99, SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE98c]. consumers [Weh99]. contactless [DS98a]. contain [Lea90]. Contemporary [Knu99b, Sim92].
Content [Ack98, JPLI99, KR98, MW98b, MR95b, PMP99, Ros93, SC96a, Way93a, SNT95].
Content-Addressable [Way93a]. Content-Based [PMP99]. Content-MD5 [MR95b, Ros93]. Contents [vHH97].
Contest [DDJ98a, EMMN98, HB99]. Context [COZ99, MM96a, Des90b, Des90a, Ili94].
Context-Based [MM96a]. context-free [Ili94]. Continue [Ano96-28]. Continued [KE97].
Continuous [BP95a, NHB98, She95a]. Contrasts [LC99, Mos98]. Correlation [CS91, HT99, JJ99a, JJ99b, KSB96a, MS91, PK95a, PK95b, Pen96, GO95, Har91, Mat95, SGSD99]. Corresponding [Oka93b].
Corrosion [LSVV95]. Corrected [Mer93]. CORSAIR [dWQ91b, dWQ91a]. cosine [TKS98].
Counteract [CJRR99a]. Counterfeit [ENK99, Ano93a, van96].
Controversy [Law98]. Convention [Ano94e, Ano96a, Ano98a, IEE96f, NIS92].
Conventional [PRB98a]. Convergence [GC97, Mos98]. Conversation [Woe97].
Cope [WI99, HJKY95]. Coprocessor [ECD99, SK96a, SK97c, YS99, DVQ96, Dia91]. Coprocessors [HP98a]. Copy [LvdLB96, LvdLL97, Lin98]. Copying [BLMO94]. Copyright [BBCP98a, BKZ98, Cohn, Gro98, Gur97, HG97c, Ib97, KZ95, LT98, LML98, NS99, Per97, Sch97d, ZK95, ZK96, And98, BBCP97, BOD95, BS97b, CPO98, CHO98, HPA99, OP98, PAK98, PA98b, RKDB96, YEA98, Zha96].
Correcting [AW94, AR98, BGS96, DLR97, KKS97, LC99, Pen96, Ada91, Al93a, AW95, Cha95a, CMM93, Ste95, Wan92a, YL97a, VT94].
Correction [Ano96f, Cha99c, MG91, WN98a, WL92c, Al93a, WL92a].
Correctness [FHH98, Gai90]. Correlation [CS91, HT99, JJ99a, JJ99b, KSB96a, MS91, PK95a, PK95b, Pen96, GO95, Har91, Mat95, SGSD99]. Corresponding [Oka93b].
Corrosion [LSVV95]. Corrupted [Mer93]. CORSAIR [dWQ91b, dWQ91a]. cosine [TKS98].
Counteract [CJRR99a]. Counterfeit [ENK99, Ano93a, van96].
counterintelligence [Mon96]. Countess [KT99]. Counting [Kor96, MVZ93, KK98, SF97]. Countries [Gar97a]. County [IEE96c, IEE96f]. Course
[CM99d, Kob94, Nic98a, Nic98b, Sch99d, Coh94, Ger97, PGV93d, PR98]. court [Ano96d]. cover [CZ90, PSB97]. Coverage [DS97a, Zav99].

[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. CPU [Kea99].

[Ano96d]. cover [CZ90, PSB97]. Coverage [DS97a, Zav99].

[AO96, Bro94, Des96a, MM96a, MK94, PN92, VNW95, Whi90, WB92, JC93]. CPU [Kea99].

Crack [De 90, Way95, WB95].

Cracked [AAG+00, Gar96c, Ano97v, Ano97-41].

Cracker [Che92, Hur98, Kle90, Mad92, Ano97i, ES97].

Cracking [Ele98, GPO98a, GPO98b, Oel97, UFC94, WS96c, Bis92]. cracks [Sta96c].

Cramping [Sta97c].

Crans [BCB97].

Crans-Montana [BCB97].

Crash [Ano97-33]. Create [Ber97a]. Created [JJ98c, MB99a]. Creator [MUSM98].

Credibility [Fri93]. Credit [Ano96g, Kra99, Ano98q, Gau97]. Credit-card [Ano96g]. Crete [Duh90].

Crime [Ano97k]. Crimes [Ano97-50].

Criminals [Uni98j, Uni98k]. Criteria [Ano97b, KS97b, MS90a, Rob93, SZZ95a, Xie92]. Criterion [ZZ95, BBC98, YT96, Cus96, CS96c, O’C94].


cross-platform [Ano97].

crossing [SBG99].

Crossley [CFK+91]. Crucial [Gar97c]. Cryptanalysis [Bar92a, Bar95, BB90, BLM94, Bih91, BS91c, BS91d, BS93b, BS93a, Bih95a, Bih96, Bih97a, BK98a, BK98b, BBF+98, Bih98a, BBS98a, Bih99a, BBS99a, Bih99b, BBDR99, Bir95, BK98d, BP99a, BL95, BD99b, BPV99, BHT98, BO92, BKP93, Bur99, Bur94a, Bur94b, CS98a, CS91, CWSK98, Cus95, DGV93, Dae95, DWZ96, Daw93, Daw96, DFKYZD99, Dii94, Dob96a, Dobxx, FS97a, FY95a, Geh94, GDS91, GO96b, Gol97d, GC90, Gol94, HKSW98, HKRS99, HG97a, HG97b, Har96a, HM97a, HO96, Jak98, JS93b, JQ98a, KR94b, KTM+99, Kay95, KSW96, KSW98a, KSW98b, KSW98c, KSW99b, KSW99c, KS98d, KS99b, KG95, Km92, Km93d, Km93a, Km93c, KM99b, Koc95, KT91a, Kwa93, LMM91, LK96, LG97, LH94, MB94a, ML98, Mat94a, Mat94b, Mat96a, MT99a, MT99c, Miy93c, NS97b, NS98d, NS98e, NS99a].

Cryptanalysis [Ngu99a, Ngu99b, NK93, OA94, Pat95, Pes97, Pie93, PN98B94, Pre98a, Roe99, SZ96, SF97, Sch98a, Sch96c, SM98a, Sch99d, SV94, Se98a, She94a, She94b, SK93, SM98c, Sim94b, ST91, Tab94, VKR98, Vau98a, Vau98c, Vv97, Ver95, WSK97a, WSK97b, WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Wis90, Wie90b, Wie90a, WBDY98, YLD99, YLH98, ZY91, Ada92b, Alv98b, BNS95, BB94, Ber93, BS90a, BS91c, BS91f, Bih92, Bih95b, Bih98b, BK98e, Bir99, BD95a, Bowxx, Bur98a, CV95, CD98a, Cra92, DYL98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, Gol95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kal99b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LS98a, Lew92, Mat93, Mi96, Mi92, Moh92, Mor92, NS97c].

cryptanalysis [O’C95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZY90, ZH90].

cryptanalyst [Rey96, Rey97, Rey99].

cryptanalysis [Gla99b, KSW98d, MG91, vW99, Bih94a].

Cryptic [Wri98b]. CRYPTO

[Fei91, ACM94b, Ame96b, And96a, Ano96h, Ano98d, Bar93a, Bar93b, BE90, HP98a, HMvT94, Koo97, LKB+94, Mad98a, Mal96, MPPS95, Neu97, Sch98c, Way95, Way96b, Mad98f, Mad98g, Mad99a, Mad99b, Mey97b, Neu95, Sav97, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol90b, Kal97c, Kob96, Kra98, MZ98, MV91, St93b, St94, Wie99, BC98,
[Bra98, Bri98, CRS98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, Sti98a, Wil98b]. Crypto-Chip [HMvT94], Crypto-Coprocessors [HP98a]. Crypto-Engine [BE90]. Crypto’91 [DBGV93]. Crypto’95 [NS98b, NS98c]. CryptoAPI [Boy98]. CryptoBytes [Cry95, Riv95e]. cryptochip [PP96]. cryptograms [Har94, Web93]. Cryptographers [WP90]. Cryptographic [AG98a, AG98b, IBM93, Ano96i, Ano98f, Ano98e, Ano98b, AB97, BDPSNG95, BDPSNG97, BH93, BY93a, BGM97a, BGM97b, BBT94, BMT96, BFKL94, Bol98a, Bol98b, BD97, BD97, Bra95a, Bra96, BD91, CS96a, CJ98b, CP98b, CPOR97, CF95, CD99, Cop94b, Cre97, DGV92, DC98a, Dam90a, Dam91a, Dan95, DIF94, DY90, DY90, DY91d, DY91b, De 95, DS97a, DF91c, DK91, ECD99, Ell98, FGR92, Fis98, FGR96a, Fum97, GI99, GS94a, G99a, Gol96c, GS97, G99q, Gut99, HHT93, HHT97, Hel94, Hwa97, I996, I996, I996, J91, KDE91, JD91, KN98a, Kal98f, Kal98d, KV94, KSF99, Kha93, KP99b, KT91b, KT98, KS97b, LMMW93, LL97a, LHM96, LM96, Mac94, MM99a, Mau96b, Mau97b, MS90a, Mii96b, Mjo93, Mos98, Mun91a, Mun91b, NM96b, Ng99, NS99b, NR94]. Cryptographic [NK98b, Nur94, N999, ÖP98+99, Oka93a, OS98, PS99d, PV97, PS96b, PW98, PBGV90, Pre93a, PGV93a, Pre93b, Pre94a, PB97, PR98b, Pre98c, PR98b, Pre99, Pre94b, QV90, Q995, RSA93d, RS93, Ritxx, Rue93, SI94, SJ96, KS96b, I991c, S95f, SK96a, S98d, SK98a, Sch91c, Sch93f, SPS97, SZ93, SZZ95c, Sha99a, She92, SBV99, Sim90, SY92, SM91, Ste96, Syv92, T+99, Toy91, Tou93, TY96, VCF+90, Vig98, Wai95, YS99, YY97c, YY98a, Z95, ZM9I, AN91, AN94, AN96, AG97b, AG97c, AG97a, An97-32, AN98g, BD92, Bol97, BV97, Com94c, CD95, Cl99, DD95, Dan97, Dhe98, Di 99, DFHR91, Don98, FGR96b, Fro96, FL93, Gol96a, GEL98, Han95, Han97, Han99, Har91, Hof95, IS99, Jenxx, JW01, JP96, KS90, Kob91a, LRW93, La95, Lea90]. Cryptographic [Lev91, LL93b, Lub96, Mau91c, M95e, M95a, MU92, IPdhhpm91, NT93, Ny98b, Pau98, P98, PKM97, Ros97c, Sch93g, SZZ94a, SZZ95b, Ste99b, Way98, WN94, XZZ97, XZZ98, YS91, ZZ97, ZLX99]. Cryptographic-Token [Nys99]. Cryptographical [KP95, Gy95]. Cryptographically [BDS98, Cha90, CpHV91, Hi94, PGV92, ZZ96, DT93, I997, KS96a, MCD98b, SKB97, Bou94]. Cryptographically-secure [Bou94]. Cryptographiquemment [Bou94]. Cryptography [ANS97, ANS98b, An994, An999, AA93, AB936, Av98, BCE94, BGG94, BGG95, BGR98a, Bel98, BBB+91, BEB92, Bir98, Bla93, BK95d, BL96b, BL96a, BGV93, Boy95a, Bra90a, Bra94a, Bus97, Cae96b, DD98a, DL96, DP98a, DP98b, Dav91, Dav96, DG96, De 93c, Des94a, DHQ98a, DHQ98b, Des98c, Di90, DNN91a, Dro96, Dwo97, Ele99, Eri99, Fer99b, Fis97, FBS97, FJM96, FJ99S, FGLP96a, FGLP96b, Gan93, Gem97, Gol95a, Gol97a, Gol97b, Gon98, HK99a, HP98a, HSS99, Hat96, Hed97, HL93b, Hir98, HA94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLM96, HH98, HBK99, JR96, JM97, Kal97a, Kal98e, KS98a, Ka99, KSS+92, Kn98a, Kob94, K9A1, RSA93f, Lac93, LM94b, Lin96a, Los97, Mad98b, MY91, Mau99a, Mau99b, Mau97c, Mc996, MP91, Mit92b, MKS99, NC97]. Cryptography [Nic98a, Nic98b, P98a, Pat96, P98b, PT95, PGCS96, Por91, PB99b, RSA99b, Rad97, Rhe94, Rit99, Riv90b, Riv93b, Riv97b, Ros96d, RK99, Salon, DP91, Sas99a, SKBxx, SS99, Sch94g, Sch96a, Sch96b,
Sch97a, Sch97b, SSv+98, Sch98f, Sch94h, SV93, SG96a, She93a, She93b, She93d, Smi94b, Smi97b, Sta99a, SW95b, Ste91, Sti95, Sti98b, Sur99, Swi97a, TN96a, TN96b, Tv92, Tow92, Tsu92c, Wad98, Way96a, Wol99, Woh93b, Wor96, WC97, YWC97, YST99a, YY96, YY97a, YST99b, Zim98, dRHG

+99, Uni96b, AA95, Acc97, Ada92a, Ada91, Alv98a, Ano97-29, Ano97-52, ASM98, BH98, Ban94, Bea97a, BR96b, BFS92a, BFS92b, BHHR99, BW97, BMP+97b, BSS98, BDS98b, BD98b, BC96b, Buc95b, Com96, Coh99, Cou99, Dam96, DDB95a, DDB95b, DQV96, DiDPS96, DDN91b, DN95b, Eng99, Far93.
cryptography [FM91, FK93b, Fra99, Fra93, Fri96, Gar96b, GZ91, Gen99c, Gol99a, Gol97c, Gre94, GTGW94, HA00, Hir97, Hru95b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdL98, Luc95, MB94h, Mat98, Mau93b, MY98, Mei96b, MVV97, Mic97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Nyb94, Org98a, Odl94b, Pad96, PG97a, PG97b, PC98, PP92b, PV93d, PR98, Riv98c, Rot95a, Sal90, Sal96, Sch92c, SSM+97, SMD+99, Sch99c, Sch90c, Sch97c, SPP98, Shp99a, Shp99b, Sin99, Siu99, Sh98, SMS90, Sta96d, Ste98a, Ts98, TM99, USE96c, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wa99a, vS97, Sha99a].
cryptography-dedicated [NM96b].
Cryptography-in-the-Large [Bl93].
Cryptoki [An96-28].
Cryptolab [Lac93].
Cryptologia [Ers99, DKK+98, Joh98].
cryptologic [RK98b].
Cryptologie [Bra93b, Bec90, Sch98e].
Cryptologist [Pin98, Se94].
Cryptology [Ano93, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BHK, Cal92, Dan90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, Wei98, AK98, Ano97-37, Bau97, Bec88, CW94, Cop95b, Cop95d, Dam91a, Dan99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, Hei94, IRM93, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mau96b, MC90b, Mei92, MV91, New97, Nyb98, ODP98, PSN95b, PQV90, QG95, Rat96, Rue93, Scu92, SP90, SZ93, Seg92, Ste99b, Uni94c, Uni95b, Web93, Wie99, Wil98a].
cryptology [Bec97].
CRYPTON [DBR+99, Lim98, Lim99].
Cryptonomicon [Ste99a].
cryptos [Hag98].
cryptoscheme [MMI97].
Cryptosystem [AM90, BI95, BDGI98, Ber97c, Bil91, BMS94, Ble97, Bon99, BM97, CC99b, CG99, CJS91, CS98b, CW91b, Cus97, Gih91, Gih96, GC91, GC94, GHH97a, Gys96, HD96b, HPS98, JHPT98b, Hwa91, Jab90, JS93b, Kie98, KS99b, KT91a, LR96, Lan97, LCL92, MM96b, NMR95, NS97a, NK98a, NS97b, NS98d, NS99a, Ngu99a, Ngu99b, OU98a, SG99a, Sam98, ST91, Sun98a, Tak98a, Tak98b, Van98a, Van98c, Wa99c, Wan92a, WY93, Y99, AM93, AD97, AD99, Aila97, AAPS92, ACR98, Bao94, BI94, BSB97, Boy97, BCC99, CCG99a, CS98a, CC98, CW91a, CW97, CS97c, CCH96, Cle96, CS97d, DW96, Gen99b, Gil95, Gro94, HNS91, HY93b, He92, HWF96, JHPT98a, HLLC96, IKN98, Jon90, JQ98b, KASH90, KSR96, KM99d, KK96, LG97, La92, LC96b, LC96c, Lon91, MMT90, MM90a, MM90b, MI90].
cryptosystem [Mau91b, Mi90, NS97c, NS98e, OU98b, Olt95, Ped91c, Pet91, Roe99, SW95a, SH95a, SH95b, SM90, SS95b, SS95c, SX90, TY92, Tan90, TCC97, TC97, TC99b, TC99a, Ven92, Wan92b, Wri98a, Wu92, XLP99, XW97, Yu92, Zer96b, Zha91, vT90, Ano96j].
Cryptosystems
cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

cryptosystems [Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Odd90, OS91, OS92, Rac90, SS98a, SS98, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Tak97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Yam98a, YY99, YY98c, Zho94, ZPY96, vO92, vT94, WA98].

D [Ben99, BALS99, CK95, Nas94, TK99, Wor96, YY99a]. D.E.S. [Cle91]. D.S.A. [NMVR95a, NMVR95b]. Dabbling [Ritxx]. DAEs [JV98b]. Dallas [ACM98b, USE91]. Damgård [DGV93]. Damgård’s [Gib90]. dan [IPNdbbbprm91]. Dark [YY96]. DASS [Kan93]. Data [Ada92a, All97, Ano92c, Nat93b, Ano95f, Ano96c, Ano97c, Ano97f, Ano97g, Ano97a, Ano97-40, Ano97-42, Ano98b, Ano99f, Ano99a, AVV99, BMGL96, BRS99, Ber98, BS95b, BS98, BV92, BW98, BZ98, Cle96, Con99b, CH99b, DC98c, DFGH99, EKLM99, Ga90, Gre90, Gui97, HS96a, Int91b, JML94, Kop97, KD98b, LvdLB96, LT98, MPP95, MS99, Moc97, Nat93c, Nat93a, NHB98, OA94, Sch99b, Sch94m, See97, Sme97, Sto90, SZT96a, TYD99, Tav90, TLS99, Way91, WSFC99,.
Wel95, Whe94, YY91, ZTR99, Ano93k, Ano95j, Ano95q, Ano95t, Ano96c, Ano97-30, Ano99g, Ano99n, CCN95, Cha94b, Cli99, CS99, Cra96, Dam99b, DF97, Gil97, GTGW94, Gut96, Hel93, KAK96, Lam99, Los97, MSDS90, Mic97, Nor95b, PD99a, Rev91, Ros94, Rot97, Sch92a, Sch98b. data [Su98, Tha91, Tv92, Uni96a, Vad95, Way93c, Way95, Woo90, Yua92, ARRW99, Ano97-39, Bar91, BS93b, Bir95, Com94a, Cop94a, Den90, HK98, HK99d, Joh90, Kap98, KM97, Mat94a, Nat94b, Nat99a, Pai96, Per91, RP94, She95b, She92g, Sim95, SB92, Wil93a, Ano94i]. Data-Dependent [Con99b]. Data/Image [Sch99b, Sch98b]. Database [AKF94, BDPSNG95, KT96, LCL92, Ou99, S397, Wat99, HY95, IS97, Lee95].


Debugging [Wot99]. Debut [Gar98b]. December [And94a, Boy95a, Boy95b, Bra93a, CW94, Con99a, Dar97, Dar93, IEE92b, IEE93c, IEE94c, IEE97b, KG93, Org98a, PSN95b, Pre95a, SZ93, Tv92, Wal99a, WN98b, Zim96b]. Decentralized [BdM94]. Decidable [BRS99]. Deciding [Bra95a, Bra96]. decipherability [CGV94]. Deciphering [CJ99, Duh90, Has95, TG94, Bru91].


Decoration [Vau98b, Vau99a]. Decrypted [Bau97, DSB99]. Decrypting [Bar92b]. Decryption [GGH97a, HJPT98b, Oht98, CB96, GBL94, Hat97, HJPT98a, MS99a, MV99, Vu95].


Delegated [MV99]. Delegation [ABKL91, Ano99e, CM99c, Chr99a, GPR98, NKP99, ABKL93]. deletion [Gut96]. Delinquency [De 93b, De 98c].

Deliverables [Hru99]. delivered [Sun98b]. Delivers [MB99a]. Delivery [HG97c].

Delusions [Rat96]. Demand [Gar97c, Ano96-31]. Demise [Bra95e].
DeTeBerkom [GH96]. Detectable [Vv97]. Detecting
[Ram92]. Developments [Ano95a, PRB98a, Sim97]. Deviates [Ran01]. Device
[ACM93b, IE97b, Sch98b, USE96f]. Difference [LP94]. Different
[KBR597, Sch99h, RT93]. Differential
[BB94, Ber93, BS90a, BS91c, BS91e, BS91d, BS91f, Bih92, BS93b, BS93a, BS97a, BK98d, BKPS93, C398, Con99b, Dae95, DIn94, Fer98, Haw98b, Haw98a, KT9+99, Kau96, KM98b, Kob99, KJ999, Kwa93, LMM91, LH94, Lan95, Mat96a, Miy93c, MSK98, NK93, OM94, Pai99a, Sch96c, MK98a, VKR98, Wag98a, YLH98, Ada92b, CV95, KY95b, Kxyx, KM96b, LMM92, O’C95, OG95, RP95b, TN97, Way95, YT95a, YT95b]. Differential-Linear
[Haw98b, LH94, Haw98a, Lan95]. Differentially [Ny99]. Differentials
[BBS99a, Fer99a, KRW99, BBS98a]. Difficulty
[KP96b, Riv93a, ZZ96, Hor99, Riv95a]. Diffie
[Ano97n, BY93c, BY93b, BBR93, BM99a, BV96, Bon98b, Bon98a, CFS97, CS97d, HY98b, HY98a, Ka97a, Koc95, Koc96b, Lut98, Man94, MW96c, MW96b, MW99, RSA93b, Van95a, VW96, WM93, vOW96]. Diffusion [Mas99b]. Digest
[Ame95, Ame96a, AN98a, Ack98, ALO98, AW94, AR97, Int91a, NIS94, Ano96f, Ano97-50, AS98, Aur96, B90, BM99a, BM99b, Bd94, Ber97b, BM94a, BM96a, BM96b, BM96c, BS95b, BS98, BTH96, Boy97, Boy98, Bra93a, B99, BWF99, Car95, CR91, CPO9+8, CHO9+8, DDM98, DDM96, E99, EGM90, EGM96, FFW99, Fox8, FKM99, FSB98, Fri93, Fro97, FOM91, Gar97c, Gar98b, GR97, GDD9+7, GB98, GO96c, GQW9+91, HKS95, HG96, HG97e, HEG98, HA96, HW97, IE97e, IE98d, JLO97, Jue99, KKS97, Kob97, Kob98c, Kra93, KH98a, LQ989, LM95, LW96, LL98a, Lut98, LR98, MS96, Man98, MST98, MB99a, MW98b, Mer90b, Mer97, MNT97, Mos98, MBW97, Nat91, Nat94a, N98, NM98, NIS93a, O93, Oht96, OFF93, Ok96, Per97, Pet98, Pf96c, PW93b]. Digital
[PGV93c, RDK98, Dr94b, Rot95b, SC96a, SC96c, Sch98c, Sch93e, Sch94d, SK97b, SK97a, She97, She92e, Sim93, SB93, SY98, SH98, VP98, VP99, VP99, Web98, WD96, WD97, WL99, Woo90, YK98, Yeu99, Yeu97, Yeu98, YH98, ZK96, ZKOY99, Zhe97b, vHH97, vTO94, AW95, Ano91b, Ano98e, BBCP98a, BHS93, BR96c, BGR98b, BSV97, BO96a, BS90, BOD95, BS97b, BM91b, BS98a, Com97, Car97a, CH98, DD95, DDM98, DSS99, FC94, FB97, Gua90, HS91, HZ93, HW98b, Hwa93, Ibb97,
digital
[YL95a, YEA+98, ZL97, Zha96, ZK98, Zho94, dR94a, AA95, Acc97, Ban94, Nat92a, Nat94c, NMVR95b, Riv93c, Sch93b, Sch94e].

Digital-Image [VP99].

Digital-Signatures [HA96].

Digital-Watermarking [GB98].

digitally [BP98b, BP98c].

Digitized [BKZ98].

Digits [Ran01].

Digraphs [HEQL98].

DIMACS [FM91].

DIMCS [WN98b].
dimension [LFCK99].

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

Dimensions [HEQL98, Sta97b].

Dining [WP90].

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

Diophantine-knapsack [Wan92b].

diplomatic [Alv98b].

Direct [PP90, PWU99, MHMW98, Un94b].

Directed [BM94a, LL97b, MT99b].

direction [Un95b]. Directions [AT99, Wot99, BFS92a, BFS92b, Go97c, NM96b].

directly [BD98a]. DIS [GQW+91].

Disappearing [Way96a, vdWS97, vS97].

disciplinary [DFGH99].

Disclose [Cre90].

disclosed [Joh98].

Disclosure [Ste98b, Suv97].

Disco [WP90].

Discontinued [Ros98c].

Discounts [DD98c, DD98].

Discourage [BLMO94].

Discourse [Mi99].

Discrepancy [Si93a].

Discrete [ACM97b, BBT94, CH98, GJKR99, Gor93a, Gor93b, GM93b, GKS97, LO91a, Man94, MW99, MVZ98, NT99, Odl94a, vO91a, PS98b, Sh97, Tes98, WD98, YY97b, vO91b, vW94, CPS95, CS97d, FR94, FMR99, HZ93, HY93b, H97, HMP95, Kob90, McC90a, NR95, SS95a, SS95b, SS95c, TG94, TKS98, vO92].

Discrete-Log [GJKR99, YY97b].

Discrete-time [GKS97].

Discretionary [BDPSNG97].

discussed [An90].

Discusses [Gar97c].

Discussion [An90e, An90j, An90l, BS94, CH99a, Mau93a, Mau97a, SAS99a, ADNK90, CZA90].

Discussion-Trust [An90j].

Disenrollment
[BBCM93b, BBCM93a, BC96a].

Disk [DIF94, Gar98b].

Diskette [BE90].

Disks [Gar97a].

dispatches [Web93].

Display [Fuc99, Sab94].

Displays [Fuc99].

Disposable [OO90].

Disruption [MH96].

Disipation [SKNO98a, SKNO98b].

Distance
[CS96a, DDJ98e, DDJ98f, SCG99, A196].

Distances [Bla99].

distillation [Sch98].

Distortion [SVBJ96].

Distributed
[ABLP93, Abe99, AD9F89, BHJM99, Bor96, BHKR95, Bur94c, CM98, DHR96, DIF91b, Dwo95, FM91, FK99, FY98a, FY98b, GJKR99, Gre94, GS97, GMV98, KI99, Kau93, Kem99, KRJ98, K1992, LAB912, Law98, Mar99, MK99, Muf93, NAA99, NKP99, Ped91a, PKM97, RZ99, Rei92, RG95, Sch94a, SKW96, SSS90, She92a, TV94, Wh90, WL92b, Be92, BP97b, FMY98, HK99b, Har90, LM98a, LAB911, Lie93, MS99c, TCH+91, Wad93, WL92a, WL92c, Zim96b, BB99].

distributed.net [An97o].

Distributing [Bre97b, Rei96].

Distribution
[BR94a, BR95b, BDHK93, B9FS96, Bur94b, DDNM98, DDP90, ECM96, Ga96, Max94, MTVZ92, PKOT94, PB99a, Sk93, SR96, YKB94, vHH97, An96h, B9GH+95a, BMS96, BFS98, Bur94a, BD95b, DFS897, FL93, GBL94, HI97, Hwa92a, Hwa92b, Hwa92c, JLM+94, K9a93, LC96a, MY93b, Mu92, PS98e, Pos92, RRP97, SI93b, SY96b, Syv93, SM95b, TH99, VSB95, WM93].

distribution-specific [Kha93].

Divergence [Sga90].

Diversity [Mau90].

divertibility [CP95].

Divertible
[BBS98b, BD91, NMV99].

dividers [PV90].
Dividing [MB99a]. divisibility [FR94].
Divisible [EO95b, EO95a]. Division [Han94, DF92, FBT96, HP94]. divisor [HP94].
divisors [HP94].
Dkarp [lPNdbbbprm91]. DLP [Kal98e]. DM [KL95b]. DMS [Bax97]. DNA
[Fää93, RS99d]. DNEWS [Ano97-33]. DNS [Gal96].
Do [AW99, Ber97a, DDJ98c, DDJ98f, HKS95, SS99a, Ber98, Ude98, Way95, ZKOY99].
Dobb [Eri97a, Eri97b, SSr+97, SSw+98, SMD+99].
Document [BLMO94, BLMO95, BO96b, Hei96b, LMOB95, LML98, Max94, Sea95, Bur98a, HS91, LL98b, van97b].
documentation [Sim95]. Documents [Rot95b, SB97, Ban94, DSSZ99, Rot95a, Sch93e, SHG98].
Doggson [Lip98].
Donald [CFK+91]. Don’t [Hus99, Way96b, Chi99a, Chi99b]. door [Yu92].
Doorbells [Law98].
Double [Ano92c, Cha97, HP99a, Pa99b, Bar95, KL95b]. Double-Agent [Cha90].
Downgrading [KM92]. Downloaded [JPL99]. Downloading [Sch97d]. dpe [lPNdbbbprm91].
Dr. [Eri97a, Eri97b, Gar97d, Riv93a, Riv95a, SSM+97, SSs+98, SMD+99].
Draft [Ano94b, Ano96-28, Ano97b, Got99, Mic93b, Am95, Ano96c, Ano95u]. Drawing [EMMN98, HEQL98]. Drawings [BMRW98].
Draws [Way93b]. DREO [Ano99f, Lam99]. Driscoll [Luj98a, Luj98b].
Drive [GC97]. Driven [CHLT99, Ano97-27].
Drives [DDJ98a, DIF94]. Dromquinna [IEE96c]. DS [TY94]. DS/CDMA [TY94].
DS2002FP [Kuh98]. DSA [AA95, Acc97, Len96a, Miy96, Sim93, Sim94d]. DSP
[IEE97c]. DSP56000 [DK91]. DSP596 [IEE97c]. DSP596 [LW96]. DSP596 [LW96].
DSS [Nat91, BGM97a, BGM97b, GJKR96a, Koc95, Koc96b, Nat94c]. DTR [Ano93k].
DTR-1 [Ano93k]. DTS [BHPR95]. Dual [Jas96, LL99, FBT96]. Dual-workfactor [Jas96].
dumps [Mei98]. during [Dou98, Joh95, Rat96, Wil98a]. Dutch
[vL96]. DVD [GC97, LT98]. DVD-Video [LT98].
Dwork [GGH97a, NS98d, NS98e].
DYANA [BKS99].
Dynamic [AGY95a, AGY95b, Ano97-33].
Double-Agent [Cha90].
Dynamical [PS96b, RO96]. dynamics [Ohi99].
Early [KMA+98, Kob99, MT99a]. EAP [BV98b].
Ears [Alv98c, Mar96]. Ease [HJL99]. eased [Ano96p]. Easier
[GMDS98, BBR99, Sch98c, Way95]. Easy [Str95]. Easy [Ano97p, Sim94d, Ken95].
eavesdropping [Way93b]. eavesdropper
[Al 96]. Eavesdropping [RK99]. Ecahse
[Sch98h]. ECC [Cer97, Kal98e]. ECC/DLP [Kal98e]. EcoFan
[PKA+98]. ECCp
Employing [BWM98]. Emulator [Obe99]. EMV [Gui97]. enable [Sch93e]. enabled [Cha99b]. Enabling [DS97b]. Encapsulating [Atk95b, KA98b]. enciphered [Lea90, Per91]. ciphering [Beu94]. Cipherment [HS90, OA94, Lin88a, Lin89a]. encoded [DS97b, HG97d, QN98b]. Encoding [Til98, HG97d]. encodings [CGV94]. Encrypt [Ano99g, BR95a, Ber98, JSY99, Ril96, WT99, Ano96e, Ano97-36, Rot97]. Encrypted [AW99, Bla98, GMCF95, GLZ99, Gi98, Jas96, Szw97a, YY91, Ano98o, BTD98, Bre97b, DF97, STW95, Kip97]. Encrypting [Ano97-33, Bla94, Lom94, Luc98b, LW99, SS99c, Beu94, KAK96, LL98b]. Encryption [ASW99, AAB+97, Ada97b, Ada98, ARRW99, And98, ABK98a, Nat93b, Ano94c, Ano94d, Ano96c, Ano96m, Ano96q, Ano96o, Ano96p, Ano96-29, Ano97h, Ano97i, Ano97u, Ano97v, Ano97-39, Ano97-42, Ano98k, Ano99f, Bac95, Bar97, Bar91, Bar96a, Bas98, Bas95, Bea97b, BDP98, BS99b, BS99c, BRW99, BS93b, Bir95, BB95c, Bla96a, Bla96b, BFN98b, Ble98a, BC95c, BFS96, BY92, Buc95a, Com94a, Com94b, CDN97, CM999, COP+95a, CH98, CMK98, CT99a, Cop94a, Cot93, DDJ98e, DDJ98c, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DS97c, Ele98, FIP94, FN94, For99b, FY95b, FY97, HF94, FO99a, FO99b, GSY99, Gai90, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, Gen98a, Gen99a, Gen99b, GK98, Got99, HG97a, HG97b, Hat96]. Encryption [HK98, HK99d, Hub98, Joh90, JM96b, Kal93a, KY95a, KR96a, Kal98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kna98, KBRS97, KHB98, KYDB98, Kwa93, Kwa97, RSA93f, Law98, Lea99, LT91, LW91, LM91b, Lin93a, LS98b, Luc97, Luc98c, Luc98e, LW99, MGL+98, Mad97, Mad98c, Mad98d, Mat94a, Mat97, Mer91, Mey96a, Mil95, Moc97, Mue99, Mil99, Nat93a, Nat94b, Nat94d, Nat97b, Nat98, Nat99a, Nat99c, Natxx, NBD+99, NH90, Oh99, Oka94, Ori96, 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, Sch93d, Sch94c, Sch95a, Sch95b, SW97a, SW97b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SE96, See97, She95b, She92g, SB98, Sim95]. Encryption [SM96, SM98b, SB92, Smi93b, Smi97a, SB99, Sta97c, SW99b, Sto90, Szw97b, THP+98, Uni97a, Uni98a, Uni98c, Uni98b, Uni98d, Uni98e, Uni96c, UU97a, Uni97b, Uni98f, Uni98h, Uni98g, Uni97c, Uni98j, Uni98i, VB96, VKR98, WSK97a, WSK97b, War98, Way93b, Way93c, WSFC99, Wei91a, Wei91b, Whe94, Wir98, Wir99, Vin97, YY97c, Yuv97, Zhe97b, Zie97, Zol93, Aus96, Abr97, Ala93a, All97, And94a, Ano90, Ano92b, Ano94f, Ano95c, Ano95k, Ano95m, Ano95q, Ano95t, Ano95v, Ano95w, Ano96d, Ano96g, Ano96m, Ano96t, Ano96u, Ano96v, Ano96-30, Ano96-31, Ano97i, Ano97j, Ano97m, Ano97n, Ano97y, Ano97-30, Ano97-35, Ano97-38, Ano97-41, Ano97-46, Ano97-49, Ano97-51, Ano98a, Ano98v, Ano98u, Ano99m, Ano99a, Ata94, AM99, Ban94, BTD98, Bax97, Bea96]. encryption [Bee96, Bee97, BR94b, BR95a, BJD97, BR97b, BB90, Bet95c, Bi97c, BFN98a, BC96a, BMS96, BFS98, Bow93, Bre97a, Bro96, Bus96, Com97, CCM99, Cha94b, CLW98, Cle96, Cil97, Cil99, CMJ96, Cra96, DH96a, DOR99, Dia91, DL98, Ele99, Ell97, Eng95, FC94, FB97, Gi97, Gol99b, Gol96d, GLL94, Goo96, GKS97, Har90, HK90, Hat97, Hel93, Hel98b, HT95, HP94, HY95, HCY96b, HCC98, Int91b, Jac90a, Jac90b, Jak99c, JT96, JT97b, KY95b, KY97, KYY97, Ken95, Kir95, Knu99c, Kop97, Kuc92, Kuh98, Kuo90, Kuo90].
LM91a, Lam99, Lee95, LC97a, Los98, Mad96, Mad98e, MRS99, Mar95b, Mey96b, MM95, MIII97, Mol98, Mra95, Nat93c, Nor95c, Oel97, Pos92, Pos93, Pre95a, QN98a, Ree97, Rev91, Rii96, Riv95d, RKD94, Rot95a, Sab94, Sav96, Sch98b, Sch94i, Sch98c, Sch99j.

encryption
[She96a, Sme97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, Szw97c, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vau98e, Ven90, Vu95, Wad98, Weh97, Weh98, Weh99, Weh95, WN95, Whi93, Wil93a, Wil93b, Woo90, Yue99, You97, Zaj97, Zan90, Zer96a, vOW91, vT93, Ano98t, Ano93j, Hon98].

encryption/authentication
[Sch99j].

encryption/decryption
[Hat97, Vu95].

Encryption/MAC
[Yuv97].

encryption/multisignature
[HCC98].

encryptor
[Ano95m, Ano98m, Ano99d].

Encryptors
[Ano99h].

Encyclopedia
[CFK91, 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, Cli99].

enforcers
[Way93c].

Enforcing
[Ano97w].

Engine
[BE90, CM98, She92d, Ano95n].

Engineering
[Ano98n, DFGH99, DSBB99, EKLM99, IEE96d, LBHM99, SSSW98, Smi98a, AN94, AN96, GEL98, IEE97k].

Engines
[T99, Way93a].

England
[ES98, Cur98].

Enhance
[FO99a].

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

Enhancement
[HWJ98, Lin93a, Lin98a, Lin98a].

Enhancements
[JMM96].

enhancing
[HY95].

Enigma
[CWM+91, Har96b, Kip97, Kip99b, Obe99, Ano91c, Blo98a, Blo98b, Blo98c, Cra92, Kip91a, Kip98, Mil96b, Mus92, Sai93, Tur99, Weh97].

Enigmas
[Gad91].

Enjoyable
[CM99d].

Enough
[CFK+91, Dea98b].

Ensche
de
[Hei96a].

Ensuring
[Com97, Rot95b, ZG96, Way91].

Enter
[Wor96].

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

enterprise-wide
[Wad93].

enters
[Joh98].

Entities
[KM99c].

Entity
[BR94a, BM98].

Entrepreneur
[Pin98].

Entropy
[Bro94, EHMS99, KSHW97, KSHW98].

Entrust
[Ano99i].

entwerfen
[Hor99].

envelope
[SOB98].

Environment

Environmental
[RS98c, RS98d].

Environments
[GSTY96, SKAM99, DNS99].

EPIC
[Rot95a].

EPS
[Ano96r].

equally
[Ito91].

Equation
[Cop95c, LG97].

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

Equilibria
[Ett98].

equipment
[Int91b].

Ergonomic
[DDJ98c].

Erika
[Mat99].

Errata
[Con99a].

Erratum
[Ano91a].

Error
[AW94, AR98, BGS96, Cha99c, DL97, KKS97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, NTS99b, 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
[Spi95, YS91].

ESA/390
[YS91].

ESAT
[PGV93d].
Escrow [AAB+97, Bla96c, BDS98, Cae96a, CGM97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP96b, KB92, ILY95, Mad97, Mah96, Mar97, MS95f, MKS99, Nec96, SYM98, Sam98, SM95a, VvT97, VBD99, YY99b, Ano94f, BDDH97, BR96b, DH96a, Des95, Fre94, KL94, Mao97, Un95a].

Escrowed [Bas95, Com94b, FIP94, Nat94d].

ESIGN [FOM91].

ESORICS [DEQ92, Q+98].

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

Espoo [Nyb98].

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

Essentially [BR91]. Establishing [Des96a].

Estimate [Miy93c, UU97a].

estimation [DLP93]. estimating [AI 96].

Estimation [VNW95, JV98b].

Ethernet [Bec99].

Etruscan [Nis91].

Euclid [LZ91a].


Eulerian [MSN98].

Eurocast [MDP94].

EUROCRYPT [Bih91, Dam90a, Dam91a, Dav91, De 95, Fum97, GQ95, Hel94, Mau96b, MZ98, Nyb98, Pic98, QV90, QG95, Rue93, Ste99b, Ano98i, Bet98, BC98, CP98, Dam98, Dav98b, D 98b, Fum98a, Gue98a, GQ98, Hel98c, Ing98, Mau98, Pat95, QV98, Rue98].

Europics [Kui91, PH91].

Europe [An907k, And96a, Ano95j, Ano95k, Ano98a, Koo97, Mus92].

European [DEQ92, Q+98, Sp95, T+98, Com97, Dan96, Gar97c, VCF+90].

Eusipco [T+98].

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

Evaluating [Pa99a]. Evaluation [AGS97, Ano97b, BKG99, BP95b, CJR98a, CJR98b, HW98, KBR97, PDG99, RIP95b, RIP95a, Rob93, Roh99, WT99, CJRR99b, KM97, PS99a, Sim95, VCF+90].

Evaluative [Mi99].

Even [BCE+94, Bosxx, Ano95q].

Evening [Che92].

Event [Rua94, SK97b, SK97a].

Event-Stream [SK97b, SK97a].

Ever [Hil97]. every [An91b, Me98].

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

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

Evolutionary [Ger99a, GM99a, Hes97].

Evolve [GB98].

EW [IS97].

exact [BR96c, GEL98, Luc95, ZW99].

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

Examining [RC95].

example [Kay95, Nee94].

Excellence [Eri97a].

Exchange [ASW98, ASZ96, BCG90, BM94b, Dam94b, Dan95, D90, FW91, HY93, Jas96, Luc98b, MSN98, RSA99a, SSN98a, SOOS95, Van93, Ano96q, BSNP96a, BSNP96b, BTD98, BCK98, BM95, Dam94a, LL95b, MS98a, SK97, STW95]. exchanges [DvW92].

Executable [JPL99].

Executing [AW99].

Executive [Zer96a].

Exhausting [CR97].

Exhaustive [CR97, QD91, KR96b].

Existence [FDB93a, HT98, RV99, FDB93b].

Existentially [DN94].

Existing [SS99d, BB95a, NM96b].

expands [An99d].

Expansion [BO96b, Tak97].

Experience [ADBB99, Gla99a, Ros96b, SVB99, Moy98, CWM+91].

Experiences [FC99, Lin90, GH96, MAM95].

Experiment [AB97, DL95].

Experimental [BBB+91, Mat94a, SBG99].

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, JJ98a].

explosive [DL95].

Exponent [An95a, CFPR96b, CNS99b, CFPR96a, FR95b, KOT95a, KOT95b].

Exponential [Dan95, CFS97, CDG95].

Expiration [BD98].

Explained [BMC95, Hat96, Lut98, Los98]. explanation [Gre90].

Explicit [LF99, MD98].

exploit [Luc95].

Exploiting [BS91h].

Exploration [KV99, Kip99a].

Explorer [Lea99].

Exploring [JJ98b, JJ98a].

explosive [DL95].

Exponent [An95a, CFPR96b, CNS99b, CFPR96a, FR95b, KOT95a, KOT95b].
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, Chl97, Gen99a, Han97, Mad99a, Mad99b, Re97, UU97b, UU97b]. Exportability [Wei91a, Wei91b]. Exportable [Eng95, Ano95v]. Exports [Bar96a, Buc95a, Sta97c]. Exported [MSK99a]. Exposing [Sil99]. Expressive [MTES99]. Extend [Ts’97]. Extended [ASW98, BFN98b, BV98c, BD91, CVHP91, CK90, DDP90, DY91d, DDP99, DD99, DY91f, DF91a, Do95a, Ev91, FW91, Gsl99, MS91, MV93, Mom91, OOK91, RSA93c, Ru91, DP91, She93c, Tou91, ZM90, vHPP93, Be97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, Oly95, Pa96]. Extended-Certificate [RSA93c]. Extending [Bad99, Has94, Mi99]. Extensible [BV98b, WBDF97]. Extensions [CD91, DT98a, Law98, NW97, Atk93, GH99, GK95a, JD91]. Extensive [Ano97-44, Sim95]. Externalization [OA99]. Extracting [Nis96]. Extraction [SD99]. Extraordinary [Jam98]. extremely [Ano90]. eyewitnesses [Ano97-37].

FA [Bao94]. Fabrication [DD99]. Face [DDJ98d, DMFB97]. Faces [GB98]. Fachtagung [BGH95b]. Facial [LMP99, HEG98]. facilitation [Chl99]. Facility [AKF94, Bi90, She96a, YS91, JMLW94, SY92]. facing [KG96]. facto [Pri94]. factor [KM98b, SVWMB95, VSB95]. Factored [Ano96b]. Factoring [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pau99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, McK99, Me96b, Riv95a]. Factoring-Based [Kal98e]. Factorisation [DHWH95a, Jon90, DHWH95b]. Factorization [Ale92, DDLM94, MM98a, MM98b, Odl95, vO91a, Sho97, vO91b, LLMP93, Mao98, WH93, vO92]. Factorizations [BMS94, NS97b, NS97c]. Facts [Ano91b]. Faded [Alv98a]. fading [To97]. Fail [BP97a, PP97, SSNP99, vHPP93, And94b, Pfi96c]. Fail-Stop [BP97a, PP97, SSNP99, vHPP93, Pfi96c]. Failed [BCE+94]. fails [DH96b]. Failsafe [KL94]. Failure [Ano95a, Ber97c, Gar98a, TYD99, FR95b]. Failures [CH98, JQD97, Moo92, Sim94b]. Fair [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, MKS99, SS99c, SS99f, Tra97]. Fairfax [ACM93a, ACM94a]. Fairly [HD96a]. fall [OD90, Rob98b]. False [LD98, She92b]. Families [Kal98e, Per99]. Family [KT98, Mad98e, Mii91, RP97a, ABC+98, BG9+95a, FSS94, Ito91, Kob90, SRRL98]. FAPKC [DYL98]. FAPKC3 [TCC97, TC97]. FAPKC4 [TC99a]. Far [Str95]. Fast [AGS97, AMV90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bii97b, Bii97c, BHK+99, BD94, BK95d, BV96, C91, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBV96, DNR97, EPR99b, EPR99a, Gar97b, Gol96a, HJP98, HP94, HCY96a, JAJH99, JAJ99a, JAJ99b, KR94a, KT99+99, KP99a, KP97, KR99a, Kau96c, KMK99, KA91, Koy95, LM95, Mau90, Mer91, Mii94, MM95, NS99a, NKP99, PPR97, Prl95a, Rog95, SW97a, SW97b, SOOS95, SV93, SB98, Sho96, Sil97b, Tak97, Tak98a, Tak98b, T+99, Van98d, Van98e, AMV93, AB96b, Ano95t, CGV94, DK97b, DvQ96, GGH+98, HJP98a, Jenxx, LR9W3, LC98, MZI98, PV905, RRSY98, She92c, SN94, SH99, SAM97, SGSD99, YL93, Gol96d, OA94]. Faster [Luc96a, Luc96b, WZ99, YY99b, Bosxx, Mih96, Sch98c]. Father
[CFK+91, DDJ99]. Fault
[BS97a, DHSS95, GX99, OKST97, Pai99a, RBvR94, IEE94b, TCH+91].
Fault-Tolerant [DHSS95, RBvR94]. Faults
[BDHJ98, BDL97, CH94a, FY99, Gar94, JQBD97]. Fauvel [CFK+91]. Fax
[Ano91b, Int91b]. FaxModem [Ano93k]. FBI [Szw97a]. FC [Fra99, Hir97, Hir98].
FCC [Gar97b]. FCD [ISO97]. FDR [Low96]. FEAL [GC91, KR95a, MY93a, 
Miy90, Miy91, TN97, BS91e, BS91d]. FEAL- [Miy90]. FEAL-8 [GC91]. FEAL-N [TN97].
Fears [Gar97c]. Feasibility [DN95a, NFQ99]. Feasible [Lip94]. Feature
[Sar99, SD99]. Features [ADEDS99, Zav99]. February [ACM98a, Fra99, FJV97, Gol96d, Hir97, 
Hir98, IZ98, RP97b, SJ97, Wo93a, Wo93b, van96, Ano94f]. Federal
[Ano97h, Ano97-42, Lee99a, RP94]. Federated [SS99b]. Feds [Szw97c].
Feedback [CM95, GK95a, Ros98a]. Feistel
[Jut98, Knu94a, SN93, SK96c, SK96d, Vau99a]. Fermat [LLMP93, McK99]. feud
[Mad98e]. Few [FJRS96, Mei98]. FFT
[DBGV93, MS90b, Sch91c, Sch93f, Sch93g, SVBJ96, Vau93]. FFT-Hash
[DBGV93, Sch93g, Sch93f]. FFT-Hash-II
[Vau93]. FFT-Hashing [Sch91c]. FGPAs
[Nor95c]. FHFC [KKW99]. FHFC-Tool
[KKW99]. Fiat [Nac93, OOK91, OQ93].
Fiber [Tow98]. Fibers [HLMP96].
Fibonacci [SMS99]. Fiduccia [CMK99].
Fiduccia-Mattheyses [CKM99]. Field
[CD98b, Kob98c, LL99, LLMP90, LL93a, MR95b, Ros93, SY99, TT99, CDEH+96,
Dav98a, GH99, Gor93b, HWB93, Has99, Pom94]. Fields
[BP98a, BMT96, BL96b, BL96a, BP97c, De 98d, LO91a, LO91b, Mas91, MFC95,
PSR97, Ano90, Gal99, LN94, MV98, SW95a, Sch91a, Shp99a, Von92a, Von92b, ZPY96].
fifteen [Den90]. Fifteenth [CFK+91]. Fifth
[SJ97, Uni97a, Uni98c, Uni98d, Uni98e,
Uni97b, Uni98f, Uni98h, Uni97c, Uni98k, ACM93b, USE95b]. Fight [De 93b, De 98c].
FIL [AB99a, AB99b]. FIL-MACs
[AB99a, AB99b]. File [ANS98a, AW99,
Ano97x, Ano97-34, Bla94b, Gil98, Man97b, RC95, HSK97, MKKW99, SK97d].
FileDrive [Ano97-34]. Files
[Bal99, PF94, Pop96, Ano98o, Gol99b].
Filesystem [IHR99, JJ91]. filling [BB90]. Film [Gar97c]. Filter [She92e]. Filtered
[MS94]. Filtering [Sch97d, LLB98, LYG94].
Final
[RIP95b, RKP95a, BFS92a, BFS92b, BP95b].
finally [Ano98v]. Financial
[AA95, ANS98b, FBS97, FL99b, Fra99, 
Hir97, Hir98, Lan97, Riv97b, Swi97].
Finding [BMR99, Cop95c, Ler97, Riv91a, Sim98c, YY98a, CC98, Car97c, Sta94a].
Fingerprint [DDJ98g, DDJ98h, HWJ98].
Fingerprinting [Ano99l, BS95b, BS98,
DF99, Hei96b, PS96a, PW97a, PW97b, 
Sas99a, YST99a, YST99b, DF98].
Fingerprinting [HJP99, OMI93]. Fingers
[RK93]. Finite
[BI95, BDGI98, BMS94, BVFD99, CD98b, 
DKKK98, Gy96, KPR99, KV94, Kob98c, 
LO91b, PS96b, She92e, Shp99a, Ano93k, 
Bao94, BI94, BGR95, DW92, DLY98, 
DF93, FSS94, Gal99, GH99, HWB93, Has99, 
Jun96, LN94, MK92, PS97, Pie93, Tao94, 
TCC97, TC99b, Von92a, Von92b, Wal98].
Finite-Impulse-Response [She92e].
Finite-Size-Particle [BVFD99]. Finland
[Nyb98]. FIPS [Nat93b, Ano93f, Ano95l, Nat93a, NIS93b, Nat94a, Nat95, Nat99a].
Fire [Way93b]. Firewalls [GLZ99, Opp97].
firm [Ano97i]. Firms [GC97]. Firmware
[MNSV97]. Firmware-Oriented [MNSV97].
First [BCB97, GPSV98, Hir97, KT99, 
KP99b, KW99, Law98, Nat94a, Nat98,
Nat99c, RD99b, ACM99b, And96c, Dob98, 
HO97, IZ98, NBD+99, Uni97a, Uni98c, 
Uni98d, Uni98e, Uni97b, Uni98f, Uni98h, 
Uni97c, Uni98k, USE95c, RD99a].
First-Order [KW99]. Fish [BD94].
Fishermen [Ano96-29]. Fissures [DDJ98a, DDJ98b]. five [Han97, KAK96]. fix [Ano98t]. Fixed [FK93b, Mae98, HP94].
flawed [Ano96w]. Flexes [Cor98]. Flexibility [Wed99]. Flexible [JPL99, LL94b, Tartas98].
Floating [Gar97b]. Floating-Point [Gar97b]. Floradora [Fil95]. Florence [IEE92d]. Florida [IEE93c, IEE94c, IEE96f, IEE97f].
Formal [BR97a, BFN98b, Kel99, Bis92]. fold [BR91]. Folger [Mor92].
France [Chr98, DEQ92, FR95a, GQ95, QG95, Vau98e]. Francis [Lea90]. Francisco [Ano97a, Ano98n, USE92a]. Franconia [IEE92a]. Franklin [WD99a].
Fraud [Nes92, VGP93, VVT97]. Fraud-Detectable [VvT97]. frauds [Sga93].
Fray [Gar97b, Law98]. Free [BP97a, BHT98, DIF96, CD98b, Dob97, Eri97b, GJM99a, GJM99b, HBKL99, Rus93b, SK95, All97, BT94, Des90b, Des96b, Dob95a, Il94, Sav96, Vau93]. Free-Space [HBKL99]. Freedom [Cae96b, Uni97a, Uni98c, Uni98b, Uni98e, Uni96c, UU97a, Uni97b, Uni98f, HM96]. freely [Ano97n]. FreeNIX [USE98c].
French [Ano97y, Blo98b, Bou94]. Frenkel [CFK91]. Frequency [BP98c, MSHP99, Ano90, Tod97]. Freshness [KY92]. FRG [Olt96].
Friedman [Uni92]. friendly [Bus96].
Front [Hed97]. Frontier [Bar93a, Bar93b, HM91, HM92, HM95].
Frustrate [Szw97a]. FSE [Bia97c, Vau98e]. FSE'99 [Knu99c]. FTP [SH93].
Fujiyoshida [IRM93]. fulfilled [Mar96]. Full [BS93a, DH90, SK98c, SK98b, Ano98a, Pos93]. Fuller [CFK91]. Fully [BCDV94, BCD96, HE98]. Function [BJY97, BDP97, BP97e, CP91, DGV93, DGV93, Dae95, DC98a, DDP90, Dob97, FGY96a, HILL99, HL99, MCD99, NSS99, PBD97, Sch91c, TOU94, AB96b, DK94, DDFY94, DIF99, GGY96b, KSB96b, KSB97, LTT95, MZI98, MVZ98, PK97, Sch91a, SRRL98, SS95b, SS95c, YL97c, ZPY96].
Germany [BFS92a, BFS92b, Fum97, IEE97d, LM98a, Wat91, Rat96].

Geschichten [CWM*91]. Get
[Ano96z, Cae96b, DDJ98a, Sch98c, Ude98].

Getting [WG97]. Gets [Gar98b, GO96c, Los97, Ano99i, Gen99c, Sch98c, Weh97].

Getting [Kwa93, Way95].

GF [PSR97, DBVD96, LD99].

GI [BGH95b, LM98a].

GI-Fachtagung [BGH95b].

Gibbs [DP99].

Gilles [Buc91b].

Girault [SSN98b].

Girl [Got99].

Girls [Ros99].

Give [GB98].

Given [BM92, BDF98, EvH91, Ev92].

gives [Ano93k].

Giving [Int91a, GQW+91, JLM+94].

Global [JV98b, Or196, SS99b, TG99, TA92, TLS99, Z995, Par96].

GMD [SBGK99].

Go [DDJ98d].

Goal [AMP94].

Goals [BP98e].

Goats [SV95b].

Going [DDJ98c, Ano95q].

Gold [SZ93].

Goldreich [Ngu99a, Ngu99b].

Goldreich-Goldwasser-Halevi
[Ngu99a, Ngu99b].

Golden [Ano94i, AWV99, El996, Gar95, Gar98c, Ros97a, SS97a, SS97b, Sta94a, Sta95a, Kobl1a, Ler97, Me96a, SX90, Zim96a, Zim96b, Pin98].

Goppa [Gib91].

GOST [KSW96, Sch95b].

Goucher [Mus92].

Government [RKD94, SG96a, Ano94i, Bee96, Riv98c, Way93b, Wel95, Ano98u, Lee99a, Ree97, Ros99].

Governments [Ano96t, BH98].

Grace [GC97].

Gradient [Jen99].

Grail [Sal99].

gran [IPNdbbprm91].

Grand [FBS97].

Graph [BMRW98, BDSV93, BW98, BAL99, EMM98, MI99, LS99a, PD99a].

Graphical [COM99, GO96c, IPNdbbprm91].

Graphics [Kni91, SHG98, Wor96].

Graphs [BM94a, HE98, LE99, WD99b, Kuc92].

Gray [Rus93a].

Greatest [Mad92].

Greece [IEE97c, KC96, Kat97, Pit95, Spi95, T+98].

Greg [Ers99].

Grid [LE99].

Gridless [BVFD99].

Grigorchuk [GZ91].

Gröbner [CWM+91].

Ground [Law98, Ano97u].

Group [AT99, CS97a, CM99a, CW93, DDJ99, DKKK98, Got99, GN95b, HY93a, L984, NS97b, NMV99, Pet98, Rei92, SG99a, Sav97, Tra99, Wu92, Yam98b, Yam99, Ano97].

CP95, DF93, Fra90, FR94, Hwa91, Hwa92d, LWC96, NS97c, WHL99, Wer93a, Wer93b, Yam98a, Dra99].

Group-Oriented
[SG99a, HY93a, LWC96].

Groups
[BMS94, CS97a, CH98, GSPN98, Got99, Mei96b, Pat99, SP99, CMPS97, Dam96, GZ91, GPCSN96, HSW94, HCC98].

Grow [DDJ98d].

Grown [Gar97c].

Grows [Lea99, Fra92].

Growth [GC97, Ano97k].

GSM
[ATA98, MB99a, PW98, She94b, Ved98a].

GSS
[Lin96b, McM96].

GSS-API
[Lin96b, McM96].

Guaranteed [Mao98].

Guarding [GS98, Mar95a].

Guess [BKK98].

Guessing [KS97c].

Guest [AKP96, BNP99].

Guide
[Bac95, End97, WSFC99, Zim95a, Bis90, Jac90a, Jac90b, Nat99, Pre97b, Sta95b].

Guided [Mos99].

Guideline [Lee99a].

Guidelines
[Bar97, CPOR97, Mer97, Ame95, Ame96a, Org98b].

GUMP [FBS97].

guru [Di 97a].

gyi [IPNdbbprm91].

H
[Scu92, Ano95n, Lea99].

H-IB [Lea99].

H-P [Ano95n].

H. [WG97].

H.R
[Uni97a, Uni98b, Uni97f].

H.R.
[Uni97a, Uni98b, Uni98c, UU97a, Uni98f].

hacker [Me98].

Hackers
[GC97, HM91, HM92, HM95, Me98].

Hacking [MSK99a].

Hades [Bie98].

Hagelin [Hag98].

Haifa [Bih97c].

Halevi
[Ngu99a, Ngu99b].

Halkidiki [Pit95].

Halske [Dav98c, Sel98b].

Hamburg
[LM98a].

Hamming [She95c].

Hampshire
[IEE92a].

Hand [BF99a].

Hand-Held
[BF99a].

Handbook [Bac95, MV97, Sha99a, Ata99, Rey96, Rey97, Rey99].

handhelds [Ano99n].

Handles [Sar99].

Handling
[BMS99, Dae98, HC95a, Mat91].

hands [Ano94c, Riv98c].

Handshake
Ste94a, Ver95, BBC98, BM95, BM91b, DF91b, DF98, HLC99, IS99, Kum97, Mu92, SSN98b, Sch90a. **Identities** [MS99a, Sar99].

Identity [ALO98, Dan95, DQ94, FKMY98, HJPB97, JC90, KP98, Len99a, SSN98a, Gua99, OU98b, Tan90]. **Identity-Based** [Dan95, DQ94, SSN98a, OU98b, Tan90].

**IEC** [Int91a, GQW+91]. **IEEE** [Ano95u, CH96, Ano96-28, Ano97-48, Ano98r, IEE95c, IEE95b, IEE96d, Kal97a, KK99b, LW96, Pit95].

IEEE-IMS [IEE94a]. **IETF** [Ano97c]. **If** [GPR98]. **IFIP** [Kat97, LM98a]. **IFIP/GI** [LM98a]. **II** [Sch99b, AK99, Ano97-40, Ano98i, Ano99c, BS91f, CFG96, CK95, CW91b, Dav98a, Don98, Eri97b, Mit92b, Mon96, Mus92, 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** [BKV98, BNP99, DS96, DP99, Fri93, HPA99, HPG98, HWJ98, IEE95a, IEE97a, IEE96e, IEE97h, IEE97j, KZ95, KM92, LMP99, Mae98, Man98, Pit95, PZ98, PNFK95, Sch99b, SC96a, SCxx, SJ97, SD97, SZT96b, TO98, VP99, Wal95, YKY99, BCCP98b, BCD98, CCH98, JTP96, JTP97b, KS98c, KG93, KH97, NP98b, OP97, OP98, OK96, PBB97, Sch98b, Se95, SHG98, TKS98, VP96, VP98, Xie98, YM98, CFF+91].

**Image-Adaptive** [PZ98]. **Imagery** [WD97]. **Images** [BLMO95, BO96b, B99, Car95, J98c, KR98, KPR99, LvdLL97, Lvd98, LSVV95, MFC95, NNEK97, Per97, SC96b, SZT96a, WD96, ZK95, BP98b, BP98c, BCCP97, BCCP98a, BCV07, BOD95, CKLS96c, HW98b, Ilb97, Irv98, Nas94, Nat97a, ODB96, ÖPH+99, Pit96a, RRP97, RKDB96, TA97, XBA97, ZL97].

**Imaginary** [HJPT98b, HJPT98a, ZPY96]. **Imagination** [Sha99a, Ros97c]. **Imaging** [AA97, RP97b, Yeu97].

**Imake** [Pat95]. **Imake** [Hus94]. **IMAP4** [Mye94a]. **Immunity** [SZ96]. **immunity** [Ada92b]. **Immunized** [FY95a]. **Impact** [Mar96, Ven90]. **Impending** [Bra95c].

**imperceptible** [CKLS96b]. **imperfect** [MY98]. **Imperfectly** [BMC95]. **impersonation** [SNT93]. **Implementation** [An96, Bilh97b, Bra96, BS91h, Dac99, DGT96, DRR95, DBVD96, Ebe93, Fei93, Fei96, FOM91, Gla99a, HKQ99, HRV99, IM93b, KP99a, Kob98c, Koc94, Koc96a, Lan97, LCN99, NM99, OSA91, PL94, PP90, Ros96b, SJ98, She95b, Tou92, Var99a, YKY99, You97, Zim99, BR96b, BC90, CKM99, Dia91, HNM98, IM93a, LS98a, LL98b, Men91, MV90, MZ98, MPL99, Nor95a, Pa96, Per91, SS98a, See97, SAM97, Vad95, XL98, Koe99].

**Implementations** [Bas98, Bri90b, Gon98, HK98, HK99d, Kay99, Pa96, Per91, SS98a, See97, SAM97, Vad95, XL98, Koe99].

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

**Implications** [Bas93, CMYY98, NS99b, PN92, Van95a, Wei95]. **Implicit** [Jam98, MILY93]. **Implicitly** [HRV99].

**implies** [LHL95a, LHL95b].

**Importance** [BDL97, Sch99b, CM97d]. **important** [Sta94a, Woe97]. **Impossibility** [MP91].

**Impossible** [BB95b, Bir95]. **Importative** [Pat99]. **Improve** [Far92]. **Improved** [An96f, BK98e, Bol90, BS91g, CRRY99, CJL*92, JM99, JJJ99b, KM96b, LD99, RP95b, SH97, SAM97, WS98, YL95b, YL95a, ZYR91, Cao99, He92, NMV95a, NMV95b, SH95a, SH95b].

**Improvement** [BB95b, Bir95]. **Improvements** [HJL99, Kle90, IKNY98]. **Improving** [BHS93, BKPS93, GLV99, SF97, ZZ94a, SMK98a, Sun98a, HMB7b].

**Impulse** [She92c]. **IMS** [IEE94a]. **In-memory** [Ven90]. **in/for** [SHG98].

**Inaccuracies** [OD99]. **inadequacy** [Kah98b]. **Including** [DGV93, DW94, JS95b, JS95a, KL95b].
incorporation [Ano95c].
increased [HS96b].
increased [HS96b].
Increasing [AP93, Bao94, BKR98a, BKR98b, Bla94a, KFJP96, Mar97].
Incremental [BGG94, BGG95, BD93, Fis97].
independence [RS98a].
Independent [Abe98a, Mau91c].
Index [MZ98, JV98b].
Index- [JV98b].
Indexing [ADEDS99, DRR95].
Indic [lPNdbbbprm91].
Indicia [TYH96].
Indies [Fra99, Hir97, Hir98].
Indistinguishability [BS99b, BS99c, NR98].
Indistinguishability-Based [BS99b, BS99c].
Individual [IKM99, Uni98a, HN98, Uni98d, We95].
induced [PS99a].
Inducing [MCD98a].
Inductive [BP98e, BP98f, COM99, HB99, Pau99, Jan95, Pau98].
industrial [CWM +91, PGV93d, PR98].
industries [CWM +91].
Industry [ANS98b, Kan96, Lea99, Uni98j, AA95, Acc97, CWM +91, Uni98k, We95, Zaj97].
ineffective [Min97, MBY97].
inequalities [van97a].
Inequality [MS99b].
Inference [ZHJ98, Jan95].
Infinite [CK90, HKL94].
infinity [Ito91].
infinite [Ito91].
infrared [DDJ98b].
Infrastructure [HFPS99, Orl96, SS99d, VSH97, Ame95, Ame96a, FB97, GH96, HTM +98].
Infrastructures [Ano99j, BPK99, BFK99, RCM99].
Inherent [She94c, KSB96b, KSB97].
Initial [Bih98b, BBDR99, SVB99, Ano96h, JJ91].
Initialization [YY99b, Ano96h, Mey97b].
Ink [BD99a, JM99].
Inmarsat [Ano99f, Lam99].
Inmarsat-B [Ano99f, Lam99].
Inn [IEE92a, IEE94a, IEE97e].
Inner [SvA +98].
Innocuous [CD97].
Innovations [BPBV99].
Innovative [FJ99].
Input [BR99a, BR99b, Sab94].
inputs [Kos99].
Ins [CHH97, CHN97].
inscriptions [Lip93].
insecure [Mit92a].
Inslaw [Eri97b].
Instance [BDPSNG95].
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 [Bol98a, Bol98b, GSY99, GL96, LBHM99, LC96a, Rei92, Smi98a, AP93].
Integration [Ala93a, Ano97-34, CHLT99, CKN99, FO99b].
De 93a, HRT96, IH99b, Kay95, Koh90, KN93, KNT94, Lei99a, Lin96b, Lun90, Men91, NT94, Rus90, SA95, Sin95, Ste92, Ts’97, Tun99, Yu94a, Yu94b]. **Kernel** [BCCG93, WB92]. **Kerry** [IEE96c].

**KEY** [YY98d, ANS97, ANS98b, AKP96, AAB97, Ano96o, Ano96w, Ano97k, Ano97v, Ano98f, Ano99l, AA93, BP98a, Bla96b, BMS94, BWM98, BWM99a, BWM99b, Bla94b, BDP+96, Bla96c, BPK99, Ble97, BDK993, BFS96, BD99b, BF99c, Boy90, BM94b, Bra95c, BS94, Bur94b, BDS98, Ca96a, CC99b, CG99, CDN98, CJS91, CGM97a, CS98b, Cra98, Cs97, DDP+98, DDP98, Dae98, Dan19b, DK6, Dan95, DDP90, Dav96, De 93c, DP98c, DB96, Dif90, DH90, ECM96, FNY93a, FY98a, FY98b, FFB98, FO99a, Fun98c, Fun93, GHS98]. **Key** [HP98a, HS90, HMT+98, HVM93, Haw98b, HD96b, HJJ+xx, Hes97, HPS98, HHF98, HMR98, HR90, Hwa97, Iss90, Jab90, Jas96, JY96, Ka99, KP99a, KSW96, KSW99a, Kel99, KS99b, KP96b, KM99c, KT91a, KMOV91, KKOT91, KP93, RSA93f, Lan99, LM94b, LW95y, LMS97, LA98, LP99, Low96, Luc96b, Mah96, Mar97, Mat91, MY91, Mau93a, MW96a, Mau97a, MP91, Men93, MM96b, Mic93a, MS95f, MM99c, MS99, MSN98, MSN99, MTVZ92, MAO96, MM98a, MM98b, NMR95, NS97a, Nce96, Neu97, NS99a, Oka94, OU98a, Oka98a, Oka98b, Omu90, vO91a, PSR97, Ps99d, PKOT94, Pat95, Pin97, Poi99b, PB99a, RSA93b, RSA93e, RSA94, ROT94, RS98c, RS98d, Ros96a, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c, RC99, SS98a, SYM98, Sam98, DP91, Sas99a, Sch94b, SKW+98a]. **Key** [SKWW99, SOOS95, SM95a, SE96, Sha99b, She94d, Si93, SR96, Spl98, Sta99b, ST91, SW99b, SH94, Sun98a, Sut99, TAP90, TA92, Un98i, Van95a, Van93, VSH97, VvT97, VBD99, WM93, dWQ91b, WLE96, WW98b, WKS+99, Wh96, We97, Wie98a, Wie98b, Wof98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vOW96, AA95, Acc97, Lite97, Da99, Al 96, An90, An96q, An96o, An96w, An96o-30, An97k, An97v, An98f, BSN96a, BSN96b, Bao94, BI94, BD99b, BDD98, BM95, BS91a, BFS92a, BG95a, BMS96, BMS98, BM95, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Cra97, Cus95, DK97b, DWZ96, DS90a, DH96a, Des95, DV96, Dhe98, Dw92, DN95b, ES97, FDB93b, FMG97a, FNY98, Fre94, Fro96].

**key** [FGLP96a, FGLP96b, FL93, Gar96b, GH96, Gib95, GRL94, GH99, GTS90, HNS91, HP99a, HP99b, HY93b, HJJ+96, Hwa98a, He92, HGF96, HJJ+97, HI97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa93, IZ98, IZ99, J96, Jar96, JLM+94, Jon90, JY98, KASH90, KM99a, KSW97a, KSW97b, KL94, K96b, Kir95, KM98c, Koo97, KM99d, Kos99, Kum97, LG97, La92, LM97a, Lee95, LC96a, LM94a, LZ90, L91a, LDW94, LL95b, LCL95, Lon91, Lon92, Lov95, Mad98f, MS98a, Mao97, MLA91, Mau91b, MY93b, MMK99w, Mu92, ML95g, NM96a, NY90, Nat97a, Nec91, O94b, Ole95, PS98e, PS98f, Pet91, PP92b, RFLW96, RT93, Roe99, Sal90, Sal96, SW95a, Sch92c, Sha95a, She96a, She92c, SKB97, SY96b, SM90, Sm93b, SS95b, SS95c, STW95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC97]. **key** [TC99b, TC99a, Ts90, TC91, Tze99, TH99, Uni97c, Uni95a, WV96, Ten92, Wan92b, Wie94, Wil93b, Xie92, Xie93, XLP99, XW97, Yam98a, YL97b, Yu92, Zha91, Zhe95a, Zhe95b, ZPY96, vOW91,
46

vO92, vT90, MC96, Mad97, BFS92b.
Key-Agreement [RSA93b].
Key-clustering [Kum97].
Key-dependency [MAO96].
Key-Dependent [FBS98]. Key-Escrow [VvT97]. Key-Exchange [Dan95].
key-management [MLA91].
Key-Recovery [Okah98a, Oka98b].
Key-Schedule [KSW96].
Key-Search [KP99a].
Key-Share [BWM99b].
Key-signing [Ros96a, Ros96e, Ros96f].
Key-specific [LMS97].
key-vowel [Lip98].
Keyboard [GO96c, She95a, Ale97].
Keyboards [CFK +91].
Keyed [Ano95a, BFN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pre95b, MS95e, BFNS98a, Gon95, KBC96].
Keyed-Hashing [KBC97].
Keyed-MD5 [KBC96].
Keying [BCK96d, BCKxx].
KeyNote [BFK99].
Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Daeh88, EHMS99, Gir91, KSHW97, KSHW98, KM99c, Luc98b, MP91, PS98e, SV99a, SV99b, Ste94a, Vau96, Way96b, Ano96h, Bih94a, CH97b, Cl99, DG94c, JP96, KC95, Knu95, LL93b, MVB99, MF97, Mok97, SSI97a, SSI97b, SV98, SH99, Sta95a].
Kiosk [BO96a, Gar96b]. kit [Ano97-38, Sun91b]. Kleptographic [YY97b]. Kleptography [YY97a]. KMOV [Ble97]. KN [SMK98a]. Knapsack [CP91, JS93b, ACBR90, CZ90, He92, JG95, LC97b, Odl90, Wan92b, Yu92, Zha91]. knapsack-based [He92]. Knapsacks [CJS91, Ort95b, Ort95a]. Know [DDJ98b, Fly97, Hii97, Kir95, Mil95].
knowing [Ble96]. Knowledge [ADBB99, BMT98, BG90, BG93, BJY97, Bi98, BD91, BDB92, COM99, Coe97, CDS94, CD98b, Dam99a, DDP94a, DDP99, DO99, DFK93, DS98b, GMW91, GKh96, GS99, G093, HT98, JKVP99, NOVY93, NMV99, O090, RS91, SIF93a, SY99, Ste99, Syv92, Tou91, BOGG +90, BBP95a, BBP95b, CDP95, DDP94b, DF93, DF94, DF91b, Sah99, Sak97]. Knowledge-Based [Ble96].
Knowledge-Level [BMT98]. known [Ano91b, BK95a, MY93a, vOW91].
KryptoKnight [BH +95a, MTVZ92]. Kryptosysteme [Hor99]. KtSeqC [BG99]. Kudos [SvA +98]. Kunstliche [CWM +91]. kuo [XtTmW94]. Kuperee [DH96b, HS94, HS96b]. Kurz [Ger97].
Kyoungju [KM96a]. Kyoto [Ano99c].

L [Lip98]. Labeling [BZK98, ZK95, LvdLB96, LvdLL97]. Labels [ZK95]. Laboratories [Ano95d, Ano95e, Ano95p, Ano95s]. LABYRINTH [L97]. Lacs [CFG96].
Ladder [Bih97a]. Ladder-DES [Bih97a].
Lai [LGL10]. Lake [IE96d, USE95b].
Language [APDS93, AKP99, IOS94, KI99, PW99, AAPS92, Kos97]. Language-theoretic [APDS93]. Languages [ACD94, BD91, GMW91, PM99a, PD99b,
SAS99b, ACM99a, Ata94, DDP94b, GA98, Il94, LS98a, PS93a, Sak97, vWN99. LANS
[She92f]. LANSCAPE
[illi96, ano94g, ano94h]. LapCAD
[ano93k]. Laptop [GPR98]. Large
[bla93, BDHG99a, BDHG99b, CS97a, LO91b, LM95, NNEK97, FF94, Riv91a, SA95, SS90, She92a, Csi95, DT93, DL93, Fra90, FO093, Has99, MSDS90, Yan95, Yu92]. Larger
[PW97b]. Laser [ano93h, JC93]. Last
[dBB91, dB91]. Latest
[dBB91, dB91]. 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
[And97-50, 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, Ho99, KV94, Riv93b, SKIT99, BFKL94, Kh93, Kos97]. Leave
[Hus99]. Lectures
[Dam99b, Fri96, PR98]. Lee
[Scu92, LZ91b]. Lee/Alek
[Scu92]. legacy [Un92]. Legal
[CYY98, HA96, Mos98, Rad97, Ros95b, Wri94, Ame95, Ame96a]. Legislation
[RDK98, Mad98d, May97]. legislative
[Cli99]. legislatures [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
[BR99a, vWN99]. Lens
[FCD98]. Lesions
[ZTR99]. Less
[BD99b, Vv97]. lesson
[Scu92, WL94]. Lessons
[Mc99c]. Let
[DDJ98e, DDJ98f]. lets
[Way93b]. Lett
[YT96]. Letter
[BC97-94, Joh99]. Letters
[Bur98b, MGL+98, PKA+98, SvA+98, BY92]. Leuven
[PGV93d, Pr95a, PR98]. Level
[BMT98, HV98, MB99a, V984, AG95, An97-30, Cl99, DF92, H996, Rus90]. Levels
[Bor96, GTGW94, dMd98]. LFSR
[Kra94b, MRR99]. LFSR-Based
[Kra94b]. Li
[JW01, vT93]. Li-Wang
[vT93]. li.v.5
[CFK+91]. liberty
[Ele99, Wad98]. Libraries
[AR97, BKBV99, DL99, IEE98d, SH98, DSSZ99]. Library
[An97-39, DK91, KH99, Dhe98, RRP97, Man98]. licence
[An97-51]. License
[AG99]. Licenses
[An97-39, TJ97]. Licensing
[Par98a]. Life
[CJ99, DDJ98e, DDJ98f, DQ94, GAGCAFC99, Ros95a, CW91]. Life-Span
[DDQ94]. Lift
[Gar97a]. liftings
[CNST98]. lifts
[An99m]. Light
[Gar97b, HPG98, YYH98, BGF99]. light-weight
[BGF99]. Like
[JQ97, BS90a, BS91c, CCZ98, Kob99, MS95f, MT99c, Nac93, WSFC99, XZ97, Kim93, KP93, Way93a]. Likely
[Bar96a]. Limit
[Lea99, Way93c]. Limitations
[BM91a, CMY98, Fis98, KV94]. Limited
[AR99, BDS98, DQ96, VBD99]. Limiting
[K96]. Limits
[And96b, AP98, EK99, Swi97, BH98, Coh99, SOB98]. Line
[Bra95b, Ca95a, Cac95b, CDF95, DT98a, E999, EG90, EG96, LMB95, PUF99, SS99e, SS99f, Tra99, DL98, Gau97, Mao98, Nal97, VNM99]. Line/Off
[EG90, EG96]. Linear
[An95a, AMP99, BGS96, BK94a, BL95, BV99, CFSY96, Dae95, DD99, Des98a, vD95b, DLR97, Gi95b, HO96, Haw98b, KR94b, KR95a, KTM+99, KR99b, LO91b, LH94, MS94, Mat93, Mat94b, Mat96a, Ny95, OA94, Ros98a, SZ96, SF97, Sch96c,
Sch99l, Sel98a, SK98c, SK98b, TN97, TSM95, YMWP99, ZYR91, Ala93a, AW95, BSN95, Bao94, BI93, Bih95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, HKM95, Haw98a, Jak98, KY95b, KYYxx, KR96c, Kuk99, Lai95, LL98, Lan95, MM90a, MAO96, MK92, OG95, SKD94, Tze99, YT95a, YT95b, ZYR90, ZHR90, vD95b, vT94, Duh90].

Linear-Time [KR99b].

linearity [SB95].

Linguistic [CH99b].

Link [Ano98m].

linkage [HCY96b, LC97a].

Linked [BRS99].

Linking [BLLV98, CM95, RP94, SM99].

Links [Blo99, CV95, DDN98, JC93].

L'inuktitut [Ano99k].

Linux [Cor93, IEE97l, IEE98f, MM95].

Localization [PJ99].

Locating [KP93].

Location [FJP96, Jac96, KFVP96, KRJ98, WHFG92, FT95].

lock [Ano96o].

Locking [BC97, CS96b, CS97b].

Locks [Way95, CC97].

Locomotive [Var99b].

Loen [LW96].

Loftus [Hel94].

Log [Bal99, GJKR99, GR99b, PS98b, WD98, YY97b, Koh90, SS95a, SK97d].

logarithm [CP95, CS97d, FR94, FMR99, HY93b, H97, HMP95, Mc90a, MV98, NR95].

Logarithms [BBT94, CH98, GM93b, LO91a, Man94, MW99, vO91a, She97, Tes98, vO91b, vW94, Gor93b, HZ93, Odl94a, 95b, SS95c, vO92].

LOGCL [LMS99].

Logging [Zol93].

Logic [AHMS99, BR99a, BAN90, CIBM99, CO98, DRR95, Gue95b, SG95, SM95a, SK99b, CS99, Pos98].

Logical [PS91f, Wad93].

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

Login [ARH95, DQ93, Hil97].

Logout [Poo95].

Logs [SK98a, SK99].

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

LOK191 [Knu93d, Knu93a, SF97].

LOK197 [BPS98, RK98a, Rij99].

London [Ano93d, Ano97-28].

Lone [Ano97-33].

LONE-TAR [Ano97-33].

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

Long-term [CH97].

Longevity [Rot95b].

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

Look-up [Has99].

Logs [Sch97b, Mad96, vDS97, vS97].

Loops [AV98, SH99b].

Lorenz [Car97b, Dav98d].

Lose [GPR98, Way96b].

Loss [Law98].

Lossy [CIF96].

Lottery [Riv97a].

Lotto [QD91].

Lottery [QD91].

Louisiana [ACM91, ACM97b, USE95a].

Louvain [Dan96, Q98].

Louvain-La-Neuve [Dan96, Q98].

Lovelace [KT99].

Low [Aga92, Ano99c, Bla96a, Bla96b, CFPR96b, CFPR96a, CNS99b, DDQ98, DDP99, DDGM97, DFK93, GDD97, Goo96, Jak98, KSH97, KSH98, KKW99, KOT95a, KOT95b, Mil96a, Pai99b, PK95a, PK95b, Pen96, SKNO98a, SKNO98b, T99, Ano90, C91, D92, DVQ96, G96a, MMW98].

Low-Bandwidth [Bla96a, Bla96b].

Low-Cost [KKW99, Pai99b, D9Q96].

low-density [C91, D92].

Low-Entropy [H97, KSH98].

Low-Exponent [CFPR96b, CNS99b, CFPR96a].

Low-Power [Ano99c, T99].

Low-Randomness [DDP99].

Low-Weight [PK95a, PK95b, Pen96].

Lowell [IEE98f].

Lower [BD97, CT91, OK95, Sch991, S91b, S91a, vHP93, GN95a, KO96, KO97, Shp99b].

LR [BP98c].

LSI [SKNO98a, SKNO98b].

Lu [LZ91b].

Lu-Lee [LZ91b].

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

Luby-Rackoff [BKR98a, BKR98b, Luc96a, Luc96b, PRS99].
LUC [Smi93b]. Lucas
[BBL95, JQ97, LTT95, SS95b, SS95c, XLP99].
Lucas-based [BBL95]. Lucent
[BBL95, JQ97, LTT95, SS95b, SS95c, XLP99].
Lucifer [BB94, BS91f]. LUN [XtTM94].
Lunch [DDJ98e, DDJ98f]. Lured
[Che92]. Lurking [Joh96]. Lustre
[Alv98a]. LVQ [LSVV95]. Lyndon
[SM90, SSM92]. Lyon
[FR95a].
M [IEE97c, WG97, Man91b]. M.A.P.
[BBC98]. M6 [KSW99b, KSW99c]. ma
[XtTM94, KP99b]. MAC
[Mit92a, Pp995, Pp996, Pre97a, SRRL98,
SR99, Yuy97, Ana93k]. MacArthur
[Dre92]. MacGuffin [BS95a]. Machine
[KP99a, NM99, PF94, QD91, Riv93b, Wi90,
Cra92, Dav98d, Dav96, Kru98, McL92].
Machines [Bur99, CFK91, FMM99,
SK99a, Dav98c, Jan95, Se98b]. Macintosh
[Sch94]. Macquarie [KG93]. MACs
[AB99a, AB99b, BGR95, JV98a, NR98,
Pv995]. Made
[GSV99, Kral94a, Gol97c, KKL99]. Maestro
[CFK91]. MAGENTA
[Bih9a, Huh98, BBF98]. Magic
[BD99a, JMM99, AGLL95, Kahl98c, RK98b].
MagicCol [GLSM99]. magnetic
[Ana90, Gut96]. Mail
[Ana93j, DN93, Got99, Ken93, Lin93a,
RS98b, Sch95c, Sch95d, SH97, VJ98, Ana95c,
Ana96m, Gar97b, LF97, Lin89a, Lin98a,
Mit92a, Rii96, She96a, Str93a, Str93b,
Bac93, Zeg93, Sta94a]. MailSafe
[RSA94]. Mainframes [Deu97, Deu98]. Mainstream
[CH94a, CHH97, Gar94]. maintenance
[Uni94b]. MAINZ [PUW99]. Majesty
[Ber96a]. Major [Law98]. Majorities
[Cha90]. Majority [Mb93]. Make
[Ana93c, GGMM97, CM99d]. Makes
[Ame96b]. Making
[ASW99, CKN99, DDJ98e, DDJ98f, Des90b,
Hir93, Lut98, PR999, Sar97, Tra97, VM96,
Way98, BKR98a, BKR98b, Wri98b, Zaj97].
Malaysia [GO96c, WSFC99]. Malicious
[PM98]. Malleable
[DDN91a, BS99b, BS99c, DDM91b, Sah99].
Malo [QG95, QG95]. Man
[CFK91, Mon96, IPNdbbpr991]. Management
[Ana99j, AV999, AG99, Bla94b, BPK99,
BFK99, Coh96, Dae98, FJP96, FY98b,
Fum98c, Fun93, GM93a, GH96, KN99,
KFP96, Neu97, Rob98a, SS99b, Yac99a,
Yac99b, Ana98f, CWM91, Hat97, LSS98a,
MLA91, MKKW99, PS98f, Pos92, RFLW96].
Manager [VDDRR99, manangers [Sea95].
Managing [ADF98, Coh99, Ken99, Sta95a].
Mandarin [OSH91]. Mangement [Bra93a].
Manipulation [FMM99]. Manipulators
[ZH98]. Manor [IEE96, IEE97]. manual
[Pre97c, RSA94, Uni94a, Uni94b].
manufacturer [Ana94c]. manuscript
[Mor92]. Many [BHS98b, BHS98a,
CFK91, DY91a, KW99, DY91c, BDV93,
Ito91, JM995, Mei98]. Many-Prover
[DY91a, DY91c]. Many-to-One
[BHS98b, BHS98a]. Many-Valued
[KW99]. Map [Bih91, KMK99, CPP98,
HNS91, LYY94, TOU94]. Maple
[Yan95]. Mapper [BPR99]. mapping [FO90].
mappings [LFS94, Nyb94]. March
[ACM98a, Ana95r, BCB97, IEE99b, IZ99,
Knu99c, Nat99b, Uni97b, Uni98b, Vau98e,
Uni98g]. Market [Wor96, Org98a, Sta97c].
Marketplace [GC97]. Markets [And96a].
Marking [BLO94, LMB95, LM99b,
PAK98, PA98b]. Markov [AA93, HS94,
LMM91, MLM92, MFG95, OG95]. Marks
[LT98, BBCP98a]. Markup
[Uni98b, Uni98c, Uni98e]. Marling
[CFK91]. Marmaras [Pit95]. MARS
[BCA98, Con99b, Zun98]. Marvelous
Maryland [ACM90, Ana96a]. MAS [CF99].
Machine [CWM91]. Masked [Web93].
Masking
[CJM95, JMLW94, SMT98, TIl98].
Masonic [Mor92]. Mass [USE99b, ZTR99].
Massachusetts [ACM96a, IEE95c, IEE98f, USE94].
Massively [GM93b]. Master [BF96, CWM91]. Master-key [BF96].
match [CGM96, Gol97c]. Matching [HTY99, WD99b, Sch91b]. Math [Gar97b].
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, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, An96c, An97-28, BV98e, CH96, CFG96, CMM93, Dan90a, Dan91a, Dan96, De95, FIP93b, Fun97, GQ95, GS94b, He96a, He94, IEE92c, IEE93b, IEE94d, IEE94e, IEE95b, IEEE97i, KG96, Mau96b, Nau98, PGV93d, QG95, R6e93, Ste99b, Uni98d, Uni95a, Use99c, An96b, Gen99b, Uni98a].
McCain [Mad99a]. McCurley’s [WD98].
MD [IEE94b, NIS92, P905, USE92b]. MD-x [P905]. MD4 [An95a, DBB91, Dob95a, Dob96a, Dob98, Dobxx, Dan91, Riv90a, Riv91b, Riv92a, Van91b, DB1].
MD5 [MG98a, An95b, BA97, BCKxx, Ber93, Dob96b, GTG94, KR95b, KBC96, MS95c, MR95b, OG97, Par98a, Pre95b, Riv92b, Ros93, Tou95, DB94]. MDx [SRL98]. MDx-family [SRL98]. means [WD99b]. Measurement [RK99, SCG99]. Measurements [VNW94]. Mechanical [SY99]. Mechanics [PT95, Ros97a].
Mechanising [BP98]. Mechanism [BDPS99, Bis91, Lin96b, New98].
Meet [FY99, Van95b]. meeting [HMP99, Zim96b]. Mellen [Ers99].
Memory [ARV99a, ARV99b, CM97a, DHMR96, Fis97, Got99, KS99a, Le9b, MS91, Sha95a, Gut96, Has99, Ven90].
Memory-Bounded [CM97a]. Menezes [Sha99a, Kie98].
Mental [CF99, Jun99, KOTT91]. Merced [GC97].
Merging [DV99]. Merkle [NS97c, NS97b].
mech [PHF99]. Message [AGS97, AB99a, AB99b, Int91a, ASZ96, Bax97, BG90, BCK6d, BCK6e, BCKxx, Ber97c, Bie98, BHK99, CDFT98, EPR99b, EPR99a, FH94, GLZ99, GT94, GQW91, HK97, Kal91, KR95b, Kal96b, Kal98d, KI97, Kra95, KBC96, KBC97, LK99, Lin98a, Lin93a, My96, N95, OM94, Pre98a, RSA93d, Riv92a, Riv92b, Rog95, Sh96, Tsu92b, Tsu92a, WSK97a, WSK97b, BSN97, BGR95, BJQ97, CLHL98, CI99, HMP95, HCY96b, LC97a, Lin98a, Riv90a, Riv91b, Sta99b, Tze99, You99].
Message-Digest [GT94, Riv92a, Riv92b].
Message-Efficient [FH94].
Message-Resend [Ber97c]. Messages [CFPR96b, vD97, SS99c, SKAM99, Bre97b, CFPR96a, Joh97b, Kip97, Mit92a, Par98b,
Model-Checking [Bol98a, Bol98b].
Modeling [DD99, KM98a, LM96, SS99a, ZFKP98, ZFK+98, Ano93k, CM97d].
Modelling [CK95, GACDCAF99, HL92, LK98, NT93, PS99a, SM99, Tro93].
Models [Ben99, CH99b, DL99, DP99, Ger99a, HHD99, LL97a, OMA98, PZ98, SY99, SZT98a, TKG99, CT99b, Nis91, OMA97, SZT98b].
Modem [Gar97b].
Modern [Buc91b, Gol97a, Gol97b, Gol99a, VG99, Dam99b, Unix9a].
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, Mol98].
Modified [BDG98, NK98a, PBGV90, Wi90, CL98, HW93, LZ91].
Modula [Sed93].
Modula-3 [Sed93].
Modular [BP99b, CJ91, Cop95c, HCY96a, Kor93, MNSV97, Pai99b, PRAM98, SKBxx, TY92, TN96a, TN96b, VDDR99, Yam98b, BGR98b, BCK98, CK93, HN94, ISO97, KAK96, LC98, Yami98a].
Modulation [B199, She94c, SC96b, KSB96b, KSB97, SVWMB95, SOB98, VSB95].
Module [Mee98, Ano97-3, Modules [Ano97-33, IH98, Mor97, Com94c].
Moduli [Hub91, Len98, Mau90, Wal99].
Modulo [DR94c, PP92a, PP95b, PP95a, Tak98a, Tak98b, Zim99, BBR99, SPP98].
Modulo-Place-Invariants [DR94c].
modulus [Tze99].
molecular [ARRW99, Ram92].
Molecules [GC98].
MON [YY98d].
Monetary [Gar97e].
Money [DDJ98c, MR98, DD95].
Monkey [YY98d, YY98b]. monograph [Lea90].
Monomial [Pat96].
MONopolizingKEYs [YY98b].
Monstor [Gar98b].
Montages [AKP99].
Montana [BBC97].
Monterey [USE99d].
Montgomery [NM94, BP99b, KAl95, KAK96, Nac93, NMR95].
Montgomery-suitable [NM94, Nac93].
Montreal [ACM94c].
Moose [Ros96b].
moot [Ano96d].
Morphology [Bol99].
Morphometry [SCG99].
Morse [Sch98i].
Moscow [CW94].
Most [BV96, KAK96].
motion [Nas94, ONT98, YEA+98].
Motorola [DK91, Gar97a].
Mouth [DDJ98c].
MOV [HSSI99]. movable [GMLH94].
Moves [Weh98].
Moving [Gar98a, HHW99].
MP3 [MB99a].
MPEG [DS97b, DS97c, DSS98, HG97e, HG97d, HEG98, LT98, QN98a, QN98b, SB98].
MPEG-2 [DS97c, HG97e, HG97d].
MPEG-4 [HEG98].
MPEG-encoded [DS97b].
MPEG2 [CPO+98, CHO+98, DNN98].
MR [DTDJ99].
MRA [BAL99, LFCK99].
Ms [CFK+91, Gar98a].
MS-DOS [Gar98a].
MSC [WSFC99].
Müller [JQ98b].
Multi [CM99b]. Multi-agent [CM99b].
Multi [BBDF97, BDD+94, BM99c, CC99c, CFSY96, DFGH99, DF97, FH98, HS94, HJTW99, HV98, JV96, KSB97, Lee99b, Mar98a, PM99a, SNW98b, SJS98, Sut99, TN96a, TN96b, VC99, CL97a, CGS97, HW98c, KSB96b, SVWMB95, SOB98, VSB95].
Multi-Agent [Lee99b, VCB99, HJTW99, PM99a].
Multi-Application [Mar98a, DF97].
Multi-authority [CFSY96, CGS97].
multi-carrier [SVWMB95, SOB98, VSB95].
Multi-disciplinary [DFGH99].
multi-exponentiation [CL97a].
Multi-function [KSB97, KSB96b].
Multi-Level [HV98].
Multi-Party [JV96, FH98].
Multi-Purpose [Sut99].
Multi-Receiver [SNW98b].
Multi-Secret [BM99c, BDD+94].
Multi-tiers [HW98c].
Multi-Service [HS94].
Multi-[CC99c].
multi-user [SJS98].
Multi-variable [TN96a, TN96b].
Multi-application [Gir99, Tua99].
Multicast [CMN99, PB99a, Mit92a].
multicasting [CM96].
multicasts [WL99].
Multi-dimensional [BMS99].
Multidrawing [BMRW98]. Multifeature [Bet95c]. Multifunction [She94c]. Multigroups [OOK91]. Multilevel [CGB+93, GPSN98, KT96, DN95a, ZH93]. Multimedia [ACM96a, ADF98, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimediad [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimediad [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].

Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97]. Multimedia [ACM96a, ADF98, CKLS96a, CKLS97, Dan96, D'98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98e, IR99, KBR99, LvdLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PS97].
NetTracker [Ano97-34]. NetWare [ARH95]. Network [ACM98a, BK90, Coh99, DS90a, Ebe93, EH96, Fum93, GM93a, HS96a, Kan96, Koh90, KN93, KCCT94a, KCCT94b, Law98, Lee95, Len96b, Lon94, Mar99, MSK99a, MT99b, RS99a, She93d, SVB99, SS99d, Tun99, VDDR99, VNW94, VNW95, WKHG97, WN98b, Wu96, AP93, BGT96, Hat97, IS99, JJ95, Kan96, Koh90, KN93, KCCT94a, KCCT94b, Law98, Lee95, Len96b, Lon94, Mar99, MSK99a, MT99b, RS99a, She93d, SVB99, SS99d, Tun99, VDDR99, VNW94, VNW95, WKHG97, WN98b, Wu96, AP93, BGT96, Hat97, IS99, JJ95, SM94, 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, KR978, Lea99, LSVV95, OM98, POKT94, PT95, Por91, Sal91, SK96c, SK96d, SV94, STP93, THP98, Tow98, VSH97, Ver98a, Ano95q, Ano96j, ACBR90, Atk93, AC97, BF99b, CW91a, CW98, Fra90, GBL94, HT95, Hor94, HLLC96, Jen99, LC96b, LC96c, NT94, Nor95a, O’C95, Opp96, PS98c, PS98d, PS98e, PS98f, PS99d, PS99a, PS99c, PS99b, SV95a, SBT99, Zan90].

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

Neurocybernetics [Mor98].

Neuropathy [MR95a].

Neuve [Dan96, Q+98].

Nevada [ACM95, AA97]. never [Mon96].

NewDES [KSW97a, KSW97b].

News [Ano93e, Ano94a, Ano95p, Ano97-29, Ano97-33, Bar97, Bar96a, DDA98e, DJ98c, DDJ98f, DDJ98a, DDJ98d, DDJ98b, DDJ98g, DDJ98h, DJ99, Eri97b, Fox99, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, GB98, Got99, GO96c, Law98, Lea99, MB99a, Ros98b, TJ97, Taa98, WSFC99, Wor96, Bra90b].

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

NFS [DL95].

NHS [Zer96a].

NHSnet [Zer96a].

Niagara [IEE96d].

Nice [BMRW98].

Nicholas [Ano97k].

Niederreiter [LDW94].

Nikola [Ano97-37].

NIKS [Cop94b].

nine [Tat98, Tat99].

Nineteenth [Alv98c].

Ninth [Ano95r, IEE93c, IEE94b, T+98, ACM97c, LLMP93].

NIST [Bra93a, Bra98, Nat92a, RH29, Riv93c, SB93].

NISZK [GSV99].

NJR [TGK99].

No [DDJ98e, DDJ98f, DH90, RS98b, Sak96, Ano97-48, BBR99, GBL94, Me98, PS97, YT96].

No-Transferable [Sak96].

nodes [GMLH94].

noise [PC98].

noise-based [PC98].

Noisy [Crec97, Lip94, MSHP99, MM92a, MFG95, GM91].

Nomikos [IEE97c].

Nominations [Nat97b].

Non [AVW99, BM90, BG90, BS99b, BS99c, BS91b, DY91a, DDP99, DR94c, DD91a, DD91b, FCD98, FDB93a, FDB93b, GPT91a, GPT91b, GP99, GO93, HJPT98b, Jak98, KR96c, LW99, Mas99a, MY91, NO98, Pai98a, Pai98b, Ped91d, Ped91b, RS91, Sah99, DY91c, SCC99, TSY98, Yab94, Ano95q, BKR98a, BKR98b, DDB95b, Ell97, HJPT98a, LL98b, MY93b, SB95, Sin95, SBT99, DDB95a].

non-Abelian [DDB95b, DDB95a].

non-biased [TSY98].

non-carminogenic [SBTV99].

Non-Abelian [DD91b, DD91a, DD91b, Sah99].

non-invertible [NO98, BKR98a, BKR98b].

Non-linear [DD91c, MY93b, Sah99].

non-maximal [HJPT98b, HJPT98a].

non-Oracle [Ano95q].

non-secret [Ell97].

Non-Euclidean [SCG99].

Non-Existence [FDB93a, FDB93b].

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

Non-Malleable [DDN91a, BS99b, BS99c, DD91b, Sah99].

Non-maximal [HJPT98b, HJPT98a].

non-Oracle [Ano95q].

Non-Perfection [Pa98a, Pa98b].

Non-Reachability [DR94c].

Non-repudiation [GP99].

Non-secret [Ell97].

NSA [Mad99b]. NSK [PP96]. NSW [Uni94a, Uni94b]. NULL [GK98]. Number [Abe98a, Aga92, ARV99a, ARV99b, BG98, BGM97a, BGM97b, Bir98, Bor95, Buc91a, BP97c, De 98d, JK99, KSW99d, KSF99, Kob94, LLMP90, LL93a, Lox90, Mat96b, Miy93c, PG90, ROT94, Sch90c, Sch97c, Shp99b, W99, BMxx, Bou94, CS97c, CB96, Cou99, CDE99e, Cus96, CS96c, Gor93b, Jenx, Kal93b, KSF00, Kos99, KK98, Lag90, LLMP93, MC90b, Mei92, O’C94, Pom90a, Pom94, PP92a, PP92b, PP95b, PP95a, PRN94, Rev91, Shp99a, Sin99, SG99. Tat98, Tat99, TSY98, YT96]. Numbers [Cha93, Ell98, Gut98b, Kra99, Mac94, MS99, Pin97, ST91, GK95a, PGCS96, Yan95]. Numerical [She92e]. Nuts [Net98]. Nyberg [NMV98]. Nyberg-Rueppel [NMV98].
[ZW99]. Obstacle-avoiding [ZW99].

obstructs [Ree97]. obtained [EvH93].

obtaining [CLHL98]. Occam [GN95b].

Ochrono [Sch95e]. October [Ano93d, Ano96a, Cha91, FM91, IEE93a, IEE94a, IEE96a, IEE96d, IEE97f, IEE97h, IEE97j, IEE98f, IEE99a, NIS92, Oht96, OiDP98, TV94, USE93, USE96a, Ame95].

Odds [McC90b]. ODEs [Ruo94]. ODMG [Wat99].

OECD [Org98a]. Off [Bra95b, DDJ98e, DDJ98f, DT98a, Gar98a, Ros96c, Tra99, AG95, Ano94i, Ano96-29, Mao98, Riv98c, VNM99].


Office [Fuc99, UU97a, Uni96b]. Official [Zim95a]. offs [BFS96, BMS96, NMVR95a, NMVR95b].

Ohio [Dal97]. Oil [KS98d, KPG99]. OK [Gar98b]. Okamoto [Hwa92a, MS98a].

Okamoto-Tanaka [MS98a]. Old [IEE94a, Mar96]. Olympiad [DDJ98b].


On-LAN [Ano96v]. On-Line [Cac95a, Cac95b, CDF95, Eil99, EGM90, EGM96, PUF99, S99e, S99f, Na97].

On-Line/Off-Line [EGM90, EGM96]. One [BJY97, BHSV98b, BHSV98a, BdM94, BHH99, BM94a, BM96a, BM96b, BM96c, BKK98, BP97c, DGV93, DDP90, Fii95, Gys96, HILL99, HT99, HYL99, Mer90a, MS999, New98, Riv98c, Roe94, Rom90b, Sch91b, Sch95a, TOU94, Uni97a, Uni98c, Uni98d, Uni98e, Uni996, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k, Zhe90, Ano97d, BD95a, BKK98, CB96, DI99, Dob98, Hwa92a, IEE92d, MB94b, MZI98, Roe95, Sim98c, Ste95, Sze98, Tao94, Tsu2b, Tsu92a, Wer93a, Wer93b, ZPS93, MAM95].

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

One-Key [Gys96, Tao94]. one-round [Wer93a, Wer93b]. one-step [Ano97d].

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

One-Time-Password [New98]. One-Way [BJY97, BMD94, BM94a, BKK98, DGV93, DDP90, Roe94, Sch91b, TOU94, Zhe90, BHH99, HILL99, HYLT99, Rom90b, BK98f, DI99, Dob98, Hwa92a, MZI98, Sim98c, Sze98, Tsu92b, Tsu92a, ZPS93].

One-Wayness [HT99]. Onion [RSG98, SGR97]. Online [FL99b, Jam98, MGL+98, MB99a]. Only [BK98d, TOU94, MRS99]. Ontario [GS94b, HA00, IEE96d, SIJ93, TM99].


Open [AT99, BCF94, Con99a, DMVC99, GS97, HVT99, Luc98b, Mu93, Gen99c, Hor94, SY96b, Sta96b, Con98, Dra99].

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

OpenPGP [CDFT98]. Operand [SSS98].

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

Operation [Ano96c, Bih94b, Bih96, Bih98a, Bih99b, HP99a, HP99b, Wag98b, Bih95a, Gl99b, Mon96, Pos92].

Operational [Car97b, RZ99]. Operations [DBVD96, Zie97, Mey97b, Win93].

Operator [Uni94a, BP98c]. operators [BP98b]. Ophthalmical [FCD98]. OPIE [MAM95]. opolizing [YY98d].


Optimal [BP98a, BR94b, BR95a, BJY97, BM96b, BM96c, Car94, FGMY97a, HKS97a, HKS97b, LC99, PRS99, PLWSN99, ST94, SW97a, SW97b, Tay95, BJQ97, DP94, LL93b].

Optimality [Mas99b]. optimally [CGS97].
Optimisation [CD98a, FCD98]. Optimised [RC94a, RC94b]. Optimising [DN95b].
Optimistic [ASW98, GMJM99a, GMJM99b].
Optimization [ARK99, DDMN98, RP98]. Optimized [EPR99b, EPR99a, SL99].
Optimizing [Cla97, MS99b]. Optimum [OK96b]. Option [Dra99, Bor93a, Bor93c].
Options [Web99, Ros94, Sta97c]. Oracle [Ano95q, GHR99, Ano95q, Got99, MSO96, Web99].
Oracles [HTY99, MW96c, MW96b, BR97b, Bra90d]. Orange [IEE96f].
Order [CH98, KW99, KS97b, Mil96a, MSK98, SM98a, SyyxW91, Boy97, Gol96a, GK95b, Jak99a, ML98, Mat95, She95c, VZ97].
Ordinary [Miy93b]. Oregon [Auc98, USE90]. Organizational [FY99].
organized [Far93]. Organizing [OMV98].
Orientation [P99]. Oriented [AKF94, BDPSN95, BDPSN97, BLH99, Bel99, DS99, LCL92, MNSV97, Mas94, Ou99, PD99a, Rei92, SG99a, SG99b, SCT99, YLCv98a, YLCv98b, BGv97a, CW97, Fra90, HY93a, Hwa91, Hwa92d, LG97, LVCv96, TCh+91, Wu92].
original [CS98a, PPBC97]. Origins [AK98, CFK+91]. Orlando [IEE93c, IEE94c, IEE96].
Orleans [ACM91, ACM97b, B*96b, USE95a, USE98c].
ornamental [lPNd99bprm91]. ORTES [ACC99].
Orthogonal [BG94, BS96, YMWP99]. Orthography [Ber96a]. ORYX [WS94, WS96].
Osaka [SKTI99]. OSI [FL93, HS96a, Hor94, KW92, She93c, VGV93]. OSPF [MBW97].
OSS [Pe97]. ossifrage [AGLL95]. Other [Aga92, CG98, Des96a, Koc96b, KS97b, Koc95, Ros94, Wrr98b]. OTM [STSW99].
Our [Gad91, PT95]. Outlaws [HM91, HM92, HM95]. Output [CJM95, Bfa94a, Sab94, ZPS93]. Outputs [SK96a, SK97c].
Overcomes [Mau97c]. Overflow [GMLH94]. overflows [Me98].
Overlap [AMP99]. Override [Bar97].
Overview [ASM98, BPBV99, DHMR96, Lan98, Lin93c, PGv92, YS99, dRHG+99, Ger97, Ste98a, VNP98, YS91].
Ownership [Car95, CMYY98, B96a, Oko96, QN98b].
ownerships [CMYY97, ZL97].
P [YT96, Ano95n, MS90b]. P-1 [MS90b]. P [IEE97c]. P1363 [Ano96-28, Ano96-44, Ano97-45, Ano98, Kal97a]. PA [AR97].
page [Ano97o, Hod97]. Pager [Gar98a]. Pair [Sch95f]. pairing [FRM99]. Pairs [Kwa93, Mi93c].
palace [Bar92b].
PalmPilot [DB99].
Panama [DC98a, DC98b]. Panel [ADKN90, CFGS99, CPOR97, EQ98]. Papal [Alv98c].
Paper [BF99, Cha93, CM99c, Fuc99, Mer90b, YST99a, Gol99c]. Papers [SB97, Ano95r, Cha91, CFP96, RRP97, CW94].
Parallelisation [FCD98]. Parallelism [BS91h, Cha99, PP92b, Pos93, Pos98].
Parallelization [BVFD99, RG99].
Parametric [PRAM98]. Paramita [JC98].
paranoid [GGOQ98]. Paranoids [Sha95b].
Parasites [NM95]. Paris
[Chr98, Org98a, Vau98e]. Parity
[KT91b, KT98, PK95a, PK95b, Pen96].
Park [Ano99c, Wei94, Ano97-48, Cla98c,
HS93, Sa93, Sm89b]. Part [AA95, AN97, ACS97,
Acc97, ECM96, Fri92b, ISO97, Lin88a,
Lin9a, Lin93a, Lud97, Cli97, U97].
Part-of-Speech-Tagging [Lud97].
Partial [CDS94, Yac99a, Yac99b, Mao97].
Partially [BF97a, Car93, SK94, Xie92, BF99b, LMS97,
Mau91c]. Partially-Bent [Car93].
Participants [Tou91].
Participant [H99a].
participates [Ano97-52].
Particle [BVFD99].
Particular [Des90a]. Parties [PS98g, SS99e, SS99f].
Partitioning [HM97a, KV99, KB98b, CKM99].
partitions [BMxx]. Party [AAB+97,
BM99a, BM99b, BR95b, BG99, Gil99,
IS91, J96, N99, RS98b, FH9M98, HY93a,
JW91, Ped91c, Wu92, XZ99, ZL99].
Pass [AC97c].
Pass [IKM99].
Passes [DD99].
Passport [MGL+98, vL96]. Password
[Ber98, Bis92, Bha98, FIP93a, HK99a, Hor95,
J96, Kle90, KS97c, Lee96, LT91, New98,
Pop96, PM99b, RSA99b, Sch99a, BSN96a,
BSN96b, BCR98, CW97, HT97, J98,
MW94, ZH93, K92].
Password-Based
[RS99b, BSN96a, BSN96b].
Passwords [De 90, MA, Ne94].
Past [Gad91, SB92, Sim94c].
Patch [St96c].
Patent [Un96b].
patents [Le91].
Path [MP95, R98a].
Patient [Cha99b].
Pattern [Des99a, PN89, W99b, Sch91b].
Patterns [Lu98].
Pattern [MSS93].
Paul [Sha9a].
Pay [DD99e, DD99f, ZL99].
Pay-per-View
[ZA99].
Payload [Ped99].
Payload
[Atk95b, KA98b].
Payment
[DVO96, FJ98, HP98b, Sch98b, PSW95].
Payments [HSW96, Pe95].
PayWord
[SR96b, RS96c].
PC
Bec97, Com90, Fra92, GC97, GO96c,
Jac90a, Jac90b, KS97b, SVa98, Sch92a.
PCAT [GN95b].
PCKS [BG98].
PDEs [LP94].
peace [Des90a].
peacetime [Sch98a].
peak
[SVWM95, SOB98, VSB9].
Peaks
[Mc98].
Pearcey [CFK+91].
Pearl
[Kal98, Par98].
Peer [SK96, Sk96e].
Peer-to-Peer
[SK96, Sk96e].
pen
[Ano99k].
Pendragess [Bur98a].
Pennsylvania [AC96b, IE96e, CH96].
Penrose [Gar96a, Gar97d].
Penntum
[BGV96, Bosxx, SW97a, SW97b].
People
[DKK+98, Ers99, Sch94c, CI99, CG05,
IE95c].
Percept [GDD+97].
Perceptron [KM99b].
Perceptual
[SZ99a, CM97d, Z99b, ZTB98].
perceptually [CKLS96b].
Perfect
[BK95b, BS91g, DD94a, DF93, vD95a, Joh94,
J96, MA91c, MW94, MK92, NOY93, BD98b,
DP94, P98a, P98b, SC97, T93, vD95b].
Perfectly
[BD93].
Perfectly-Secure
[BDH93].
Performance
[AC98a, Ano95b, BM99, DMP98, FC94,
GN95c, HJ99, HW98, IEE94e,
KR96a, Koa98, LM98b, PRB98b,
Roe94, Roe95, SK+99c, SKW+99a,
SKW+99b, S92e, S99, Sut99, To95,
V9W94, W98b, NO96, S98].
Performer [KS98b].
Period [RH99].
Periodic
[Mu91a, Mu91b, Ab9b].
periods [Gv98].
Peril [DD99a].
Permit
[Joh94].
Permits [Gar97b].
Permutation
[BM92, BS90b, CT99a, EM93, Hm9T94,
Pa99c, Pat99, CV94, HT95, O95,
Pat91b, Por93, Zan90].
Permutations
[BY93a, DW94, FJ95, SP97, CC98,
Pat91a, Phen3, Sch94, SM98b].
Permutated
[BCG93, KM99b].
perm [HJ95].
Persistence
[DL99].
Person
[BB97, Be98b, DLF97, DMB97,
WKG97, BCB97].
Personal
[Ano97-34, BE90, Bar05, Cae96b, EMM99,
Gar97b, Hamxx, Los97, Los98, RSA99a,
Rivxx, Cra96, Mil95, Wil93a].
Personalized
Perspectives

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

pertaining

[Cha94b, Perugia [De 95]].

pessimistic

[Knu98].

Peter

[vdWS97, vS97].

Petre

[CFK+91].

Peter

[DR89b, KA99, LL97a, NT93, YK98].

PGM

[HMvT94, MMT90, MM90a, MM90b].

PGP

[Ano97-34, Ano97-35, ASZ96, Elk96, End97, Gar95, Gar98c, Joh96, Kar96, Ken95, MR98, MLLG95, Ros95a, Ros95b, Ros96a, Ros96b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, SA95, Sta94a, Sta95a, Sta95b, WCS95, WT99, Zim95a, Zim95b].

PGPmail

[Pre97b, Pre97c].

Phantomic

[Lip93].

Phase

[BGV93, Chi92, ODB96, HY95].

Phases

[Tou92].

Phil

[Ros95a, Ros96c, Ros97a].

Philadelphia

[ACM96b, AR97, CH96].

Philosophical

[Mos98].

Phone

[Gar97a].

Phones

[MB99a].

Photographic

[Fri93].

physically

[Wa90].

Physics

[Sch90c, Sch97c].

Picard

[BSB97].

Picking

[Way95].

picture

[ONT98].

PIL

[Sch99k].

PIL/SETHEO

[Sch99k].

piling

[HKM95].

piling-up

[HKM95].

Piloting

[KW92].

Pinyin

[OS91h].

pioneer

[KT99, RK98b, Pin98].

Pioneers

[Unixxb, Riv98c].

Pipelined

[Pos93].

Pirates

[Wal94].

Pitfalls

[Sch98f, SZZ94b].

pixels

[BD98b].

PKC

[IZ98].

PKC'99

[IZ99].

PKCS

[Ano95p, Ano96-28, Ano97-44, Ano98r, Ble98a, Kal97b, Kal98a, Kal98c, Kal98d, Kal98e, KS98a, Nys99, RSA93d, RSA93b, RSA93c, RSA93e, RSA93a, RSA99b, RSA99a].

PKCY

[XW97].

PKZIP

[BK95a].

Place

[DR94c, Des98a, DR98b, Ano95c].

Place/Transition

[Des98a, DR98b].

Placement

[FL93].

Plain

[Bar93a, Bar93b, Phi98].

plaintext

[GC94, WB94, Wri94, BK95a, Cii99, MY93a, SNT95, vOW91, vT93].

Plan

[Gar97a, Gar98b, Ano94i].

Planar

[LE99].

plane

[ZW99].

Plants

[PRAM98].

Plasmoid

[BVFD99].

Plastic

[Gau73].

platform

[Al98, Ano97j, LS98a, Way98].

Platforms

[Ri96].

Play

[Bea97b, DDD98d, ICM99, Ano97-32].

Players

[IKM99].

Playing

[SvS98, SV99, SV99b].

plays

[Lea90].

Plug

[Bea97b, Ano97-32].

Pluggable

[HI98, Mor97, Ano97-53].

Plugs

[GTGW94].

Plus

[Dav95].

plutonium

[Ano96-30].

PMLP

[BPBV99].

Pocket

[Fan97].

Pocono

[IEE97e].

Poczyt

[Sch95c].

Poetry

[Sha99a, Ros97c].

Point

[FP99, Gar97b, Lan98, STP93, Ken95, Shp99a, SM98a].

point-&-click

[Ken95].

Point-to-Point

[SM98a].

points

[KK98, MVZ93].

Poker

[KKOT91].

policies

[Ano96-31, Ano98v, HK99b].

Policy

[ACM94b, And96a, Ano96i, Bar93a, Bar93b, CPOR97, Ell99, Gar99, Hat96, Wai95, Aus96, Abr97, Ano97-31, Ban94, Bro96, Buc95a, Dan96, DG96, Ele99, Eng95, HAHH94, Hof95, LKB+94, Mad96, Mad98, Mad98e, Mad99a, Rot95a, Tsa98, Wad98, Zaj97].

Polish

[Blo98b, Blo98c].

Politics

[Ele98, PB99b, DL98, Mad98a].

Pollard

[BMxx, ESST99, GLV99, Tes98].

Polling

[JO97, Mer93].

Polly

[ES97].

polyalphabetic

[Abe98b].

Polygonal

[OM98, OMA97].

Polychromatic

[Mou99].

Polymorphic

[SG95].

Polynomials

[AGS97, NMV99, Sho97, TN96a, TN96b, CS97d, MI90, Pet91, Xie93].

Polynomial-Time

[Sho97].

Polynomials

[SE96, She95c, CW91a, CGMW97, Ito91, Kob91c, LC96b, Od94a, LC96c].

POLP

[Mye94b].

POLP

[ACM99a].

Popular

[KAK96].

porpoises

[Ano96-29].

port
VPM97, Zim96a, Zim96b, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, Zeg93.

Privacy-Protecting [Tra99]. Privacy
[BDF98, BD99b, CKGS98, HRR90, KR94c, Law98, MP91, MV93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts’90, Wil93b, ZG96].

Privacy-Key
[HR90, MV93, RSA93e, DS90a, SS98b].

Privilege
[ECM96].

Prize
[GC97, Pin98].

PRO
[Ano97-33, Gar98c].

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

Probabilistic
[Jak98, JO97, SF97, Sch91b, Tout93, Gol90a, GO95, HK90, Imp92, Lon91, TX92].

probabilities
[Lew92].

Probability
[BDG99, Gol96b, Kob99, TY94, AI96, MHHMV98, MAO96, WM93].

Probable
[BD93, NK93, DL93, Graxx].

Problem
[Bon98b, Bon98a, BN96, CS96a, Cha90, DD99, DJL93, GO95, HM98, KM99b, KR99b, MT99b, NS99b, OMV98, Per99, RS99a, CPS95, HY93b, HI97, HM97b, HMP95, LC97b, Mas97, McC90a, NR95, OA99, MSO96].

Problem-Solving
[Per99].

Problems
[AA93, BD95a, Bra90a, GGH97b, KR99, MC92, Po99, Smi90, APDS93, Bea92, BFKL94, FR95a, Han95, Han99, HC95a, IEE97e, Lew92].

Procedure
[Ada97a].

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

Proceeding
[BPR99].

Proceedings
[ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, Ano95, Ano98, Bri92, Bri93, Com96, GN95b, IEE95a, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96d, IEE97d, IEE97l, IEE97j, IEE97k, IEE97i, IEE98e, MZ98, Nat99b, OW95, PSN95a, Pit95, Sti93b, SIJ93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96e, USE96d, USE96f, USE98e, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94e, Bih97c, B+96b, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fum97, Go90b, HO97Q, HA00, Hm97, Hir98, HRF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, KG93, Knu99c, KP99b, KK99b, Kru98, LOX99, LM98a, LW96].

proceedings
[Lom97, MV91, Nyb98, ODP98, Pre95a, QV90, QG95, Q’98, Rue93, SZ93, Sp95, 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, Go96d, GQ95, GS94b, He94, IR93, Kal97c, Kob96, Mau96b, PSN95b, SP90].

Process
[AMP94, Knu98, Rob98a, RS99c, YT96, CWM+91].

Processes
[Gar98b, Bea92].

Processing
[Ano97h, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97h, IEE97d, IEE97j, IEE97k, IND99, KV99, LMP99, LW96, Pin98, Pol95, Ano96-30, DO99, DF97, Man98, Sab94, T’98, Wh90].

Processor
[Gar98a, RB99, SW97a, SW97b, She92e, Sat99, VVDJ90, Von92a, Von92b, DVG96, She92c].

Processor-efficient
[Von92a, Von92b].

Processors
[Cl97, KK99a, She92e, BS95c, MHPS96, NM96a].

Proctoring
[SKW96].

Prodigy
[CFK+91].

produced
[SSI97a, SSI97b].

Product
[GO96c, KSW98a, KSW98b, KSW98c, GN95a, SS98b, Ano94i].

Products
[Ano97-33, Ano97-34, Cha94b, C1997, Los97, UV97b].

Professor
[Swi97].

Profile
[Hor92, HFPS99, MM90a, MK92].

Program
[BDFM99, FGY96a, LBMC94, FGY96b, KTG99, LS98a, Pre97b, Pre97c, Uni95a].

Programmable
[DMVC99, SVB99, TT99, WB94].

Programme
[BG93].

Programmer
[Bre99, DDJ98a, Jol95, Ste94b, vdWS97, ...]
Programmers \cite{Gar97c, Joh97a, Joh97b}. Programming \cite{IBM93, BGS96, CO98, Eri97a, JDK+91, Ste90a, Ste90b, ACM99a, Gre98, LS98a, QA99, Sab94, vWN99}. Programs \cite{BK95c, DRR95, SG95, SHK99b, WB95, Zwi98, B+96b, DFHR91}. Progress \cite{Ano96-28, Ano97-45, BDI+96, KSB96b, Wol93b, Wol93a}. Progressions \cite{Mih94}. Project \cite{BPBV99, IBMxx, GH96, Man98, DS90b, RCM99}. PROMIS \cite{SSCP99}. Promise \cite{Law98, Los97, Mar96}. promises \cite{Way93b}. Promotes \cite{GO96c}. PROMS \cite{IEE98e}. PROMS-MmNet \cite{IEE98e}. Proof \cite{Bol98a, Bol98b, CD99, CDS94, FOO91, GMW91, GMV99, RS91, Zhe95b}. Proof-Based \cite{Bol98a, Bol98b}. Proofs \cite{BG90, BG93, BD91, CD98b, DFKN93, FS97b, GMW91, GO93, JMS96, CD95, DP94, Gol99a, PS96d, Sak97}. Proof-Based \cite{Bol98a, Bol98b}. Proofs \cite{BG90, BG93, BD91, CD98b, DFKN93, FS97b, GMW91, GO93, JMS96, CD95, DP94, Gol99a, PS96d, Sak97}. Propagation \cite{GPR98, SG99h, SZZ95c}. Properties \cite{Boy99, Con99b, KA99, MM90b, MS91, OK98, OS98, Tou93, VW98, WW98b, Zie97, BHH99, CD95, FSS94, KSB96a, Koh91a, PS93a, XZZ97}. Property \cite{CFG99, DL99, LQ99, SRY99, Uni97b, Ale98, BS95c}. Propos \cite{ABK98b, ABK98c, AKB98a, BAK98, DR98a, KR94a, LM91b, Ano95n, Cli99, LM91a, RH92, RS98y, Ban94}. Proposals \cite{DA99, VvT97}. Propose \cite{Gar98b}. Proposed \cite{CP91, Lea99, LL98a, Nat92a, Riv93c, SB93, Wag98b, CM96, Gu90, Mey96b}. Proposes \cite{Gar97a}. Prosthesis \cite{HHD99}. Protein \cite{SV99}. Protect \cite{Sch94, Sta95b, Cli99, KR96b, Way93b}. Protected \cite{CH94b, DY91f, Mad98b}. Protecting \cite{BO96a, Ble98b, Des90a, EHMS99, GMD98, KR98, Lut98, Mar95b, MW98b, PT95, SYM98, Tra99, VP99}. Protection \cite{BGG95, CHN97, CW94, DF91c, FGR92, FG98, Gro98, HG97c, LQ98, LvdLB96, LvdLL97, LML98, Per97, SM90, Uni97a, Uni98i, ZK95, ZK96, Ale98, BBC97, BBCP98a, BOD95, COP+98, CHO+98, Cli99, DFHR91, GO96a, Ib97, OPH+99, RP94, RKDB96, SY96a, Sta94a, Tev92, TSN93, Uni97c, YEA+98, FT95]. protections \cite{HPA99}. protects \cite{Ano95m, Ano96j, Ano97-43, Ano98d, Ano98s}. protest \cite{Ano97-52}. Protocol \cite{ATAY98, Ano95a, BWM99b, BV98b, Bra95a, Bra96, CH98, Dan95, Dra99, FKK96, Geh94, GS97, HHY93, IS91, JT97a, JMP+98, JQ97, Kas96, KSW98a, KSW98b, KS98b, Kra99, Kum98, Low96, Mau94, MW99, Mey96a, Moo92, NS98b, NS98c, OMI93, RS96a, RS98b, SSN98a, SH97, SM98a, SM95a, Sim96b, SM96, SM98b, Ste98b, WS96a, WS96b, AP93, Bea93, Bol97, BO99, CM96, CTSxx, Des96b, Ev93, Fra90, FR95b, HY98b, HY98a, KC95, KSL92, Low95, Pau99, RS98f, SK97, Sim94b, TH99, WS97, WL94, Zhe95a, GM93a, Sar97]. Protocols \cite{AG98a, AG98b, AN95, AB97, BCG90, BBT94, BMT96, BG98+91, BW98, BW99a, BBCM93b, BB98a, Bol98a, Bol98b, BDL97, BM94b, CG98, CD99, CDS94, CD95, Cre97, Dan99a, DGT96, DQ93, DS97d, Fe193, Fe96, FBS97, Fum98b, GM93a, Geh95, GS97, GMV98, Gue98b, HT98, HK99a, HL92, Hwa92d, HCY96a, IEE98e, KK97, KY92, KS97c, LHY93, LL97a, LHB96, LL95a, LS92, LM96, MB94a, MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nvr94, SL93a, Sch94g, Sch96a, Sch94h, Sch99k, SSP90, Syv92, Tou91, Tou93, AN94, AN96, AG97b, AG97c, AG97a, Ab99, ABC+98, BDH97, BH93, BCK98, BGH+95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, CJ95, Dan97, FGH99, Fe99, GEL98, Hor98, HLL+95, JW91, LY93, LHW99, LL95b, Lom97, Man95, Mas97, MIL93, Mea95, MW98c]. protocols \cite{NT93, PS98c, PS98e, PS98f, Pau98, PW93a, PKM97, SSG99, Syv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].
prototypes [Ano96-30]. Prototyping
[AKP99]. Provably
[Bel99, CT99a, GEL98, Mat96a, Mil94, SZ96, Van98b, BOGG+90, Mol98].

Provably [AB96a, AWV99, BR95b, BC93b, CS98b, Dam94b, DY90, DY91d, DY91b, LM95, Mau91d, Oka93b, PS96c, Sho96, ZMI90, BH93, Dam94a, FO98, Gol90c, NY90, PSW95]. Provably-Secure
[DY90, DY91d, DY91b, Mau91d]. prove [Zha96]. proven [DS93, Lea90].

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

Provide [BDR+96, SA95, Ano99i, Ano99h]. Provider [Tre99]. provides [MHMW98]. Providing
[Bra90a, SKAM99, Ano95c]. Proving
[Bos90, DR94c, DE99, FK99, DF91b, FHG99].

provisions [Cli97, UU97b]. proxies [LC94]. Proxy
[GP99, Jak99e, LHW98, Zha98, BBS98b].

PRPs [HWKS98a, HWKS98b]. Prudent
[AN94, AN96]. Pruning [AP94]. Pseudo
[BG98, BGM97a, BGM97b, Imp92, MS95f, NR98, PS98b, Bou94, TS98].

[ARV99a, ARV99b, BCK96b, BCK96c, BGK99, EM93, HILL99, KSWH98d, KSF99, Lag90, Mac94, Pat91a, Siu99, ZYWR91, BGR95, KSF90, Kos99, Pat91b, Rev91]. Pseudorandomness [Kob99, Lub96, LLG10, BCKXx, Gol99a, MM99].

psychoacoustic [Thi98]. Psychovisual
[DDM98]. PTY [LT98]. PTY-Marks
[LT98]. PUB
[Nat95, Nat99a, FIP93b, NIS93b]. Public
[ANS97, ANS98b, Ace97, AKP96, AN95, IBM93, Ano96w, Ano96-30, Ano99j, Ano99f, AA93, BP98a, BI95, BDHJ98, BDGI98, BCE+94, Bec99, BC95b, BHSV98b, BHSV98a, BDPR98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BFK99, Ble97, BF99c, BS94, CC99b, CG99, CIS91, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De 93c, DP98c, Di90, El99, FY95a, FY98a, FYM99, FGLP96a, FGLP9b, FO99a, GHY90, Gal96, Gar96b, Gib91, Gib96, Gir91, GGH97b, GH99, HK99a, HGS98, HP98a, HY93b, HM93, HL93b, HJJ+xx, Hes97, HPS98, HFP99, IZ98, IZ99, Isa90, 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, Odi94b, Oka94, OU98a, Omu90, vO91a, PS97, Pat99d, Pat95, Poi97, Poi99, RSA94, RCM99, Rud91, Sal90, Sal96, DP91, Sas99a, SE96, She94d, Sm93b, ST91, Sin98a, Sut99, TAP90, TA92, VSH97, dwQ91b, Wie98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zin96b, dwQ91a, vO91b, AA95, AD97, AD99, Ano90, ADSW99, Bae94, BI94, BD98a, BSB97, BS91a, Bue94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Cus95, DZ96, Dam96, Den90, DVQ96, Dhe98, DN95b, ES97, FGMY97a, GH96, Gib95, He92, HWF96, HJJ+97, JM96a, Jar96, Jon90, KASH90, KM99a, Kir95, KM99d, Kos99, LG97, Las92, LM90, Le95, LC96a, LM94a, LZ90, LZ91a, LDW94, LCL95, Lon91, Lon92, Low95, MIO90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rac90, Roe99, SW95a, Sch92c].

public [Sha95a, She96a, She92c, SM90, SS95b, SS95c, Sta94a, Sta95a, Sun91a, Tab94, TCC97, TC97, TC99b, TC99a, Tze99, Ven92, Wan92b, Wil93b, Xie92, Xie93, XLP99, XW97, Yu92, Zha91, vO92, vT90, BFS92b, HMT+98]. Public-Key
[AKP96, Ano99j, Ano99f, AA93, BP98a, BHSV98b, BHSV98a, BDPR98, Ber97c, BMS94, BPK99, BFK99, CC99b, CJS91, Cra98, Cus97, DP98c, Di90, FYM99, FO99a, FO99a,
GHY90, GGH97b, HK99a, HGS98, HP98a, HMV93, Hess97, Iss90, Kal99, KM99c, KT91a, KMOV91, LM94b, Low96, MY91, Mic93a, Mic93b, NS97a, OU98a, vO91a, PSR97, DP91, Sas99a, ST91, Sun98a, Y298b, Yam98b, YST99a, YST99b, Ano96w, Ano96-30, BFS92a, FGLP96a, FGLP96b, GH99, HY93b, NY90, Nec91, Sal90, Sal96, Smit93b, Yam98a, AD97, AD99, BMP97a, CA99a, Cle96, Cra97, DVT96, Dhe98, DN95b, ES97, FGM97a, KASH90, KM99a, KM99d, LM94a, LZ91a, LDW94, LCL95, Lon92, Low95, Man91b, MY93b, NM96a, Ole95, SW95a, Sch92c, Sha95a, SS95b, SS95c, TC99b, Tze99, Ven92, Wan92b, XLP99, Yu92


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


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].


Relying [ZMI90, Sak97, Sch99c]. remainder [DDPS96, WW99h]. Remark [CMNTY94, LHL94, FR94, MY93b].


Replace [OG97, YL97b]. Replicate [RB94]. Replicated [KB92]. Replicating [HS96b]. Replication [BML94, Pit96b]. Reply [NC97, BMP+97b]. Report [Bra93a, BDI+96, Dra98, EMN99, Kui91, Nat99c, Par98c, PH91, RIP95a, RD99a, Tou95, Vau99d, Wor96, Ano96a, BFS92a, BP95b, Bur98a, KS96b, NBD+99, Org98a, RIP95b, UU97a, Zer96a, Dan95, BFS92b].


Representation [CK95, Ger99b, JKV99, LE99, NA95, PNFK95, TY92].


Requirements [Ano97b, BD92, Be92, BC95c, FR95d, HJT99, HH94, VW98, Com94e, MW98a, SM95b, UNU94].

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]. Reshar ing [AGY95b].

Resource [KKOT91, PP92b, CB96, PP95b, PP95a]. Residuosity [Pai99d, DDP94b]. resilience [FGMY97a].

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

Nat97a, NP98b, Pad98, PHF99, Rab94, SC96a, SZT96a, SZT96b, STZ98, 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 [Wie90, Daw96].

Round [Mic93b].

Round-Optimal [BJY97, DP94].

Round1 [Bas98].

Rounding [BV97].

Rounds [BB99a, dBB91, Bor95, DBR 99, KR94c, BB98a, Dob98, PNR98, dB91].

Routers [DMVC99, Ano96x].

Routing [GRS96, RSG98, SGR97, CadHSV96].

S-box [BD95a, SK98c, SK98b].

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, BF98, BV98c, BD99b, Bon99, Bra95e, Bri90b, BM94c, Ca99, CH97b, CH98, CB96, CLL99, CMTNY94, CD91, Cle96, Coc97, CFPR96b, CFPR96a, CNS99a, CN99, CNS99b, Con99, CD96, Cus97, Dav95, Dem94, DDL99, DN95b, EvH91, Ev92, EvH93, Fia90, Fia97, FS97b, FGMY97b, FM98, FY98b, FR95b, GK96c, GKR97, GQO98, Gil99, GM97, GTS90, Gro94, GS99b, HN98, HFW96, Hor98, Hub91, HP94, IM193a, IM193b, JQ97, JQBD97, JQ98a, KR95c, Kal97a, Kal98b, KS98a, Kir95, Koc94, Koc96a, Koc95, Koc96b, Koy95, KOT95a].

RSA [KOT95b, KK96, Len98, LHL94, LL95a, Lon91, MWB99, MILY93, Mau90, MW98d, MW98c, MSS98, Mis97, Mis98, MS99e, Mue99, Mii99, M98b, NS99c, Oka98a, Oka98b, OSA91, PPK99, PP90, PW93a, Poi99, PS98g, Rab98, RS98e, RSxx, SII97a, SII97b, Sam98, SKNO98a, SKNO98b, SSH98, Sch94m, SPP98, Sha95b, SV93, SH99, Sli97b, Sli97a, Sli92b, TY92, Tak97, Tak98a, Tak98b, T99, TT99, VVDJ90, VNM99, Ven92, Vv97, Wal99c, Way98, Wie90b, Wie90a, Wir98, XL99, WW99, Zer96b, Zho94].

RSA-120 [DDL99].

RSA-130 [Ano96b].

RSA-Based [CD96, GKR97, VNM99].

RSA-cryptosystem [Gro94].

RSA-Implementation [PP90].

RSA-key [FM98].

RSA-keys [SSI97a, SSI97b].

RSA-Like [JQ97].

RSA-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].

Running-Time [DF91c].

Russia [CW94].

S [WG97, Ano95u, Ano96-28, BD95a, DT93, ECD+99, Kim93, Mat95, MC96, PG97a, PG97b, SK98c, SK98b, Sto90, Uni97c, Y99, YY98d].

S-box [BD95a, SK98c, SK98b].

S-Boxes [Kim93, PG97a, PG97b, DT93, Mat95].
S-CODER [Sto90]. S.Hrg. [Uni98j]. S.I.S. 
[ECD+99, YS99]. S/KEY [MC96]. 
S/MIME [An099, An096-28]. S012 
[KP95]. s02DES [TSM95]. S390 
[Deu97, Deu98]. SAC 
[Kim93, KS97b, NS99a, TM99]. SAC/PC 
[KS97b]. SAC’99 [HA00]. SAFE [Uni97a, 
Uni98c, Uni98b, UU97a, Uni97b, 
BC97, Hor99, VM96, Way95, Uni96c, GA98]. 
Safe-Tcl [GA98]. safegaurding [Beu94]. 
Safer [Hir93, BM97, CMKK98, KSW96, 
KSW99a, Kel99, Mas94, Mas99b, Van95]. 
Safety 
[Ano94d, Ano98o, DDJ99, Cli99, IEE94b]. 
Safford [Bur98b, Kru98]. Saint 
[GQ95, QG95]. Saint-Malo [GQ95, QG95]. 
Sales [Gar97a]. Salesman [OMV98]. 
salient [CKLS96b]. Salt [USE95b]. Sam 
[Mad99g]. Samba [Bl98a]. same [Ude98]. 
Samos [KG96]. San [ACM93b, ACM99a, 
Ano97a, Ano98u, Com96, CMM93, FJV97, 
IEE92b, IEE97b, RP97b, Sch98b, SJ97, 
USE92a, USE96c, USE96f, USE96g, USE98d, 
van96, XTN99]. Sand [SVxW91]. 
sandbox [MF97]. Santa 
[Bri92, Bri93, Cop95b, Cop95d, Des94b, 
IEE97b, IEE97j, IEE98d, Ka97c, Kob96, 
Kra98, St93b, St94, USE93, Wie99]. 
Santorini [IEE97c]. Saragossa [Man96b]. 
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]. 
Scalable [Hei96b, IEE94e, KH98b, LR98, 
RG99, SL99, Goo96]. Scale 
[SA95, SS90, She92a, FO093, OP97, OP98]. 
Scaling [SA95]. SCALPS [DVQ96]. 
scanners [Mei98]. Scanning [CO98]. 
Scenario [AMP94]. Scene 
[SZT98a, SZT98b]. Scene-Based 
[SZT98a, SZT98b]. scenes 
[BDC+95, MCD98a]. SCFS [IHR99]. 
Schedule [KSW96, KSW99a, Kel99, MM99c, 
Mur99, SKW+98a, SKWW99, WKS+99]. 
Schedular [KT96]. Schedules [CDN98]. 
Scheduling [KP93, Por98, SJS98, Sha99b]. 
Schema [Pit96b]. Schemas [Wed99]. 
Scheme [Int91a, ADF98, BCC93, BM99a, 
BM99b, BF99c, Boy90, BY92, CT97, CK95, 
Cop94b, DQ94, DKKK98, DN94, GY90, 
GQW+91, HL93a, Hwa93, Hwa97, Iev91, 
IM93b, KKS97, KS98d, KM99b, KR99b, 
L96, LW91, LHL94, LH93b, MSS98, M96, 
Mue99, Mii99, N98, OOK91, O93, 
OFF93, Pat95, Pet98, PM99b, RGV97, 
S99, Smi90, Ver95, ZL99, AW95, BD98a, 
CW97, CLHL98, CC95, CLW98, CMTNY94, 
CG97, FO93, FO98, GMLH94, GPSN97, 
Gua90, Har91, H93, HK90, HY95, HC96, 
HW98c, HCC88, IS99, IM93a, JC98, 
JLM+94, Ku9c2, LWC96, LL98b, LLG10, 
MR99, MS98a, MLA91, M99b, MC96, 
Nac93, OK96b, Pat91b, Pat91a, RD96b, 
SS98b, SVW95, Ste95, Tan90, Tod97, 
Tara97, Wan92a, Wu92, WWH95, vT93]. 
Schemes 
[AW94, BP97a, BC93a, BD98a, BB96, 
BK94a, BK95b, BM96b, BM96c, BDG93, 
BD+94, BFS96, BM99c, BV96, BD90, 
Bri90a, BS91g, BLV98, BDB92, CS97a, 
CM99a, CD95, Dam99a, DVW90, DMPW98, 
DY91e, vD95a, DFKY90, DL97, 
FDB93a, FY97, FO091, FO99b, GPSN98, 
GP99, GS94a, HKS97a, HS97b, IS91, 
JMO94, KPG99, K96, KM97, KO98, KOS+94, 
KO95b, KO95a, LHW98, LM95, MH96, 
N98, MWW94, OK98, Oka93b, PA98a, 
Pai98b, PM98, PS96c, PB99a, RS96c, dR94b, 
SK95, Sak96, SE96, S93, Sim90b, Sim91, 
Sim94a, Ste94a, St93a, St98b, SW99b, 
SS99, YLD99, Zha98, AR99, BC95a, 
BR97b, BII3, BDS93, BCD94, BGS95, 
Blu95, BC96a, BC96, BD96, BDG96, BMS96, 
BD97, BFS98, BD98b, BDG99, 
Bur96, BM94c, CDG91, CP95, CSV94].
schemes [DP96, DF93, DDB95a, DDB95b, Des99b, FDB93b, HY93a, HMP95, HCY96b, JM93, Koy95, KO95a, KO96, KO97, LS98a, LC97a, LHL95b, LHL95a, MS98b, MPSV99, MTNI97, Mu92, NR95, OK96a, OKT93, OK95, Pad98, PS98a, PPKW97, Pfi96c, PS96d, RD96a, RS96b, SH93b, Sha94, Sha95a, She92g, SW98, SW99a, SS94, SC97, Tj99, Tze99, VNM99, WAMO94, ZHS94, Zf98, 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 [An93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97f, IEE98a, IEE99a, Ste91, Bed90, Beu94, Sch90c, Sch97c, Shp99a, Sim92, WS96c]. Sciences [An95r, Tv92]. Scientific [CHLT99, PH91, BCF+94]. Scientist [BCE+94]. scoop [An96-30]. Scots [Sin99]. Scott [Sha99a]. Scramble [JSY99]. Escramblers [GDS91]. Screening [CN99]. ScriptEase [An97-34]. Scripting [SaA98]. Scripts [Duh90, Sch99a, IPNdbbbprm91]. Scritchers [Dum94]. scrutiny [Den90]. SDK [An97-34]. SDNS [NH90]. SDSC [Sch99]. SEA [Sch98, GC97]. SEAL [HG97a, HG97b]. Scalability [Por98]. Sealing [GS98]. Seamless [DFGH99]. Search [AEDS99, BD93, CD98e, HS90, KP99a, LC99, Mih94, Sa99, V93a, Wie96, Wie97, Wei98a, vW94, vW99, CR97, GLV99, Gol90c, KR96b, KM98c, Kuh98, Wie94]. Searches [PKA+98]. Searching [BP95a, DDJ98e, DDJ98f, Jia99, DSSZ99]. seasons [WSFC99]. Seattle [HF97, USE98a, USE99b]. Second [Auc98, Cha91, DEQ92, Hir98, Nat99b, ACM90, AR97, An99g, FR95a, IZ99, Lea90, Pre95a, Un196c, Un195a, USE96d, VPM97, Hin93, PH91, HK97]. secondary [Atk93]. Secrecy [Aba99, BP98e, GM90, GTGW94, JR96, Moy98, Rat96, Sin99]. Secret [AGY95b, An97e, BC93a, BC95b, BCG90, Ben98, Ber91, BS97a, BK94a, BK95b, BDGV93, BM99c, BV96, Bra95b, Bra95c, BS94, BD90, Bri90a, BS91g, Cac95a, Cac95b, CT97, CMPS97, CGM97, CK90, CFSY96, DDJ98g, DDJ98h, Dae98, Dam94b, DDPA94a, DKKK98, DF1J99, vD95a, EHMS99, FW91, GPNW98, GPSN98, HL93a, HD96a, HKS97a, HKS97b, HCY96a, IS91, Kau96b, KL96, Kra94a, KOS+94, KO95b, KO95a, LYH93, LF97, LM94a, LM94b, LP99, LH93b, MSNW99, Man93a, MW96a, Man97a, MSNW99, MSNW99, MT98, Mus92, NW98, OK98, PS98a, Piu98a, Piu98b, Ped91d, Pra96, Rey96, Rey97, Rey99, Sal91, Sch99, Sha99a, Sim90b, Sim91, Sim94a, Sti93a, Van93, Wi99, Wie90b, Wol98, Al96, AGY95a, BC95a, BT94, BI93, Ble96, BSDV93, BCDV94, BDD+94, BS95, BCDV96, BDGV96]. secret [BD97, BDV98, BDG99, Bur96, CDGV91, Dal97, Dam94a, Dwo91, Ell97, FOO93, FO98, GM95, GPSN97, Gre90, HNSM91, Hel93, HJKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, Jar96, JY98, KO95a, KO96, KO97, LY93, LH95, Me92, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, Ped91b, Ped91c, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, Vv97, Wie90a, WS96c, Win99, Wri98b, ZHS94, vD95b, van97a]. Secret-Ballot [CFSY96, BT94]. Secret-Key [An97e, Bra95b, Bra95c, LM94b, Mau97a, Van93, Wol98, LM94a, JY98]. secret-sharing [RD96a]. secret-sleuthing [WS96c]. Secretly [MT94]. Secrets [Cr90, DH90, DSB99, El98, HHY93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, An91b, Bau97, BVD93, CWY98, JMO95b, WY93, Chi92]. Section [Alv98c]. Secure [AHV98, AB96a, An93c, An93f, An95l,
Ano99f, Ano99l, Atk97, AR99, Bal99, BQ95b, BQ95a, BMM99a, BM99b, BR91, BH+99, BDHK93, BFS96, BS95b, BS98, BM94b, CG99, Car99, CG98, Cha90, CV99, CR91, CC95, C99, CKLS96a, CKLS96c, CD95, CD96, C95b, CDD99, Cra99, Dam91b, Dam94b, D90, DY91d, DY91b, DYf91, DH90, FIP93b, F97, FYM99, FH94, FO99b, GGM97, GY90, Ga96, Gel95, GJK99, GHR99, Gut96, IOS94, Jac90, Jac90b, JT97a, KR95c, KM93, Kf96, KT96, KSHW97, KSHW98, KM99a, Km94a, KP97, Kf95, KBR90, KYDB98, LY93, LM95, Mar98a, Man90, Man91d, Man97a, MW97, Mos98, NIS93b, Nat95, NS98b, NS98c, Oka93b, OU98a, Ped91d, PS96c, PB99a, PGV92, RRP97, RS96a, Rf95a, SSH93, SS98a.

Secure [SK94, SSSW98, Sas99a, Sch94a, SK98a, SM95a, SB94, SSM94, Sho96, Sm93b, Str93a, Str93b, Tay95, WP90, WD99a, WK97, Web98, Yah94, YST99a, YST99b, ZMI90, Zhe90, ZL99, Zol93, vHH97, BH93, Bea93, Bea96, BMS96, BP95b, Bow93, BM95, BD95b, CNST98, C97, CG05, Dam94a, Des90b, DS93, Des95, DV99, FO98, Ggk99, GM95, Go90c, GBL94, HJT96, HY98b, HY98a, HC95a, Hwa93, HW98c, IS97, IK99, KC95, KBB96a, Lam99, Los97, MS98b, NY90, OK96b, Opp96, Ped91b, Ped91e, PSW95, RHe94, RSSY98, Rom90b, Sar97, Sch92c, SK97, Sim98e, Sin95, Sta97c, Ven92, YL97b, ANS97, Ano93j, Nat92b, Sta94b, Bou94].


sécurité [Sch98e]. Security [ACM93a, ACM94a, ACM97a, AKP96, ADDS91, ARH95, ABDV98, Ali97, And94a, Ano91a, Int91a, Ano92c, Ano93g, Ano95f, Ano95b, Ano96r, Ano96a, Ano96y, ??97, Ano97e, Ano97f, Ano97g, Ano97a, Ano97-40, Ano97-42, Ano98b, Ano98c, Ano98q, Ano99a, At95b, AR98, Bal99, BCCG93, Bas93, BKR94, BDPR98, Bel99, BGK99, Bel92, Ber96b, BDR+96, Ble97, BPRF99, Bov98a, Bov98b, Boy99, Bra90a, BK94b, BP99, Com96, Com94c, CM94a, CH94a, CH97, CGJ+99, CS96a, CM97b, CT99a, Chr98, CGB+93, Coh99, C999a, Cor99, CN99, CG05, DMW94, Dan95, DS98a, Dav95, DG95, De 93a, De 98a, DDK98, Des92, Di 99, Dwo95, ECM96, Elk96, EH96, FG96, FSF97b, FO99a, Fum93, Fum98b, GM93a, GMCF95, Gan96b, Gar97c, Gar96c, Gib96, Gir99, GH95, Gon98, GA98].

Security [Gu99, HHT93, HHT97, HP99a, HP99b, HSK97, HH94, HLMW93, HXMW94, Hur98, IBMxx, IEE92a, IEE92b, IEE93b, IEE93c, IEE94c, IEE94d, IEE95b, IEE96c, IEE97b, IEE97i, ISO97, IH99a, JD91, JLO97, Ky95a, Kr96a, Ky98, KT99+99, Kuo93, KA98b, KM96a, Kf90, KRR98, KS97c, LOX99, LBMC94, Len96b, LL94a, LL95a, Lom97, Luc97, Luc98a, Luc99a, Luc99b, MMST98, Mat96a, MSK99a, MW98d, MSS98, MM98a, Muf99, Mu98b, Muf99, Mye97, NIS92, Ng99, NK93, OiDP98, O989, OU98b, Opp97, PS98d, PS99c, P897, PS96d, PS98h, Rei92, RBv94, Rob93, Rob98a, Rog96, Rus90, Sch94m, Sch95c, Sch95d, SH97, Sch97a, SSv98, Sch98f, SS99a, Sch98h, She97, SSP90, SS90, She92a, She92f, She93c, She93d, She94c, She96b, SK97d, Sun98a, Un97a, Un98a, Un98e, Un99c, Un99f].

Security [Un98j]. USE90, USE92b, USE93, USE95b, USE96c, USE96g, USE98d, USE99a, Van95a, VSH97, Van98b, Vau99b, Vau99c, Ved93, Ved98a, Ved98b, VG93, Ver98a, WCS95, Wol98, Wol99, ZS93, ZFKP98, ZFK+98, vT94, Aaa99, Ada92a, AFB95, Ano93d, Ano95o, Ano97x, Ano98h, Ano99h, Bec97, BR96c, BCK96c, BDJR97, BKR98a, BKR98b, BB96, B+96a, Bet95c,
BHHR99, BCW97, Boy98, Bro96, Com97, Cha95a, CP94, Chi99a, Chi99b, CJ95, Cli99, CTSSxx, Dam99b, DS90a, Den99, DEQ92, D+98, FHG99, FFW99, FM98b, Fra92, Gon92, GEL98, Grn98, HN98, HK99b, HOQ97, HS96b, Hor94, HC95a, HC95b, HY95, HLLC96, IEE94b, JT96, JT97b, JJ95, KY97, KG96, Kat97, KSB96b, KSB97, KW92, Kuh98, Lai92, LTT95, Lee95, LHW99, Len93, LC95, MW94, Mar95b, MS97, Mas97, Mau91c, MKKW99.

Service [FJ98, Gar98a, GH95, HS94, KMP99, Kau93a, MB99a, RRW97a, RRSW97b, Ros96c, Ros96f, Ros97b, Ros98c, Wu96, ZL99, Cra96, KNT94, Nee94, NT94, RFLW96, Zha96, Ber96a, KN93].

Service-Level [MB99a]. Serviceability [WP90].

Services [ANS98b, Cas95, HVH98, RB94, VSH98, Ved98a, AA95, AC97, DS90b, Don98a, KW92, PS99b, You97, Zer96a, AA95, Acc97]. ses [Bou94].

Session [BR95b, BB95c, CFGS99, CPOR97, EQ98, FL96, IR99, SR96, AG95, Uni97a, Uni98c, Uni98d, Uni98e, Uni96c, Uni97b, Uni98f, Uni98h, Uni97c, Uni95a, Uni98k].

Session-Layer [BB95c]. Sessioneer [AG95].


Shared-Memory [Lei99b]. shareholders [LHL95b, LHL95a, Mao98]. Shares [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, HKS97a, HKS97b, KI96, Kra94a, KOS+94, KOO95b, KOO95a, LP99, LCL92, LH93b, Mei92, MS95f, MSN99, NW98, OK98, Pai98a, Pai98b, Ped91d, Rab94, ROT94, Sch92b, Sch99i, Sti93a, Wil98a, AGY95a, BC95a, BI93, BDV93, BDSV93, BCDV94, BG98, BCDV96, BDGV96, BD97, BDV98, BDG99, Bur96, CDGV91, CMS97, CGMW97, DF93, DDB95a, DDB95b, Dwo91, FDB93b, FGY96b, FR95c, FO98, GM95, GPSN97, HJKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, JMO95b, Jar96, KO95a, KO96, KO97, Mao98, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, PS98a, Ped91b, Ped91e]. sharing [RD96a, RD96b, Sta96a, SC97, TC91, ZHS94, vD95b, van97a, Kol95]. Shark [RDP96, WG97]. Shawn [Sha99a].

Shedding [HPG98, YYH98]. Shelf [Hat96, AG95]. Shell [Car99, Sch99a]. Shift [GO96b, Go94, GN95a, GM91, GO95, PS97]. shift-register [GN95a]. Shifting [LMBO95]. Ship [NS98a, RP98].

Ship-Board [NS98a]. shipping [Ano95q].

Shooting [Aga92]. Shop [Ano97-33]. Short [Kra94a, Ste94a, Wie90b, vOW96, BC95a, Coh94, Har94, Joh99, VW96, Vv97, Wie90a].

Shortage [DDJ98a]. Should [Way93c, YY96, Ano95c, Riv98c]. show [Mad98g]. shrinking [MS95a, MS95b, Mih96].

SIB [NS93b, Nat92b]. shu [XtTuW94]. SIAM [ACM97b]. siber [Ano97-50]. sichere [Hor99]. Side [KSW98a, KSW98b, KSW98c, SVA+98, YY96]. sides [MB94b].

Siege [EH96]. Siegenthaler [MS99b].

Siemens [Ano97-47, Bro97, Dav98c, Mac98, Sel98b, TJ97]. Sieve [LMP90, LL93a, Per93, CDEH+96, Gor93b, Pom94].

sifrovan [Gar98c]. SIGACT [ACM99a].

SIGGRAPH [ACM99c, B+96b]. Sight [Phi98]. SIGINT [Mye98].

Sign [BM92, GR97, GHR99, Web98, BR96c].
Signal [IEE97c, IEE97d, IEE97k, LW96, Pit95, She92e, T98]. Signalling [Lin98].

Signals [AK99, BTH96, DDNM98, MHMW98].

Signature [AA95, Acc97, AW94, Int91a, NIS94, Ano96f, Ano97-50, BP97a, BM99a, BM99b, BM96c, Bra93a, CS97a, CM99a, CG98, CH98, CK95, CDF95, CD95, DMPW98, DQ94, DY91c, DN94, FL99a, FKMY98, FOM91, FOO91, GP99, GQW91, HJJ+xx, KKS97, KS98d, KPG99, Kob98e, Kra93, LK96, LHW98, LK99, LHL94, LL98a, MT94, MB99a, Mer90b, Mer97, MH96, MSS98, Mis98, Miy96, Mon93, Nat91, Nat92a, Nat94c, Nat94a, NMR95b, Na97, NMV98, NMV90, NIS93a, OFF93, Oka93b, PF94, Pet98, PM98, PS96c, Pj99, RGV97, RDK98, Riv93c, dR94b, SC96a, Sch93b, Sch94e, SK97a, SE91, Sim93, Sin98, SB93, SSNP99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, ARK99, Ala93a, AW95, Ale97, Ana97p, BD98a, Bis90, Boy97, Bur96, CP95, CMTNY94, CSV94].

signature [DP96, FR95c, Gu90, HY93a, HJJ+97, Hor98, HMP95, KS98c, LWC96, Mau91b, May97, MS98b, Mu92, NMR95a, NR95, Pj96c, Pit96a, PS96d, PS98h, SI93b, Sha94, SS95b, SS95c, Ste95, Til98, Tra97, TJ99, Wan92a, Wi93b, Wu92, XA98, YL95b, YL95a, Yeu99, Zhe94, dR94a].

Signatures [ANS98b, ASW98, AT99, BD99a, BQ95b, BQ95a, BG90, BdM94, BM94a, BM96a, BC93b, BF99, Boy98, BS95d, CHP91, CR91, CDF95, Cop99, CD96, Dam94b, DF91a, EG90, EG96, Ef91, Fro97, GKR97, GHR99, GM97, GO93, HKS95, HA96, JM99, JQB97, JLO97, Len96a, LSV95, LR98, MO96, Mis97, MBW97, NQ98, OQ98, Oka94, PP97, PW93b, PGV93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, She97, Tra99, Web98, Wri94, vHP93, Ano98e, BR96c, BGR98b, Ble96, BCP91, BM91b, Com97, CPS95, Cha95b, Dam94a, Ev92, EvH93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, Ped91a, Pj96c, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].

Signycryption [Zhe97b, BD98a, Yeu99, Zi98]. Signed [Ber97a, GMCF95, KT93, SKAM99, Sun98b]. Signer [CvHP91]. signers [TJ99].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].

Siagonage [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SM91, YY98a, ZI97].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].

Siagonage [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SM91, YY98a, ZI97].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].

Siagonage [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SM91, YY98a, ZI97].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].

Siagonage [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SM91, YY98a, ZI97].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].

Siagonage [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SM91, YY98a, ZI97].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].

Siagonage [Zhe97b, BD98a, Yeu99, ZI98]. Signed [Ber97a, GMCF95, KT93, SM91, YY98a, ZI97].

Significance [DFGH99, SBVG99, SM91, YY98a, ZI97]. Significant [BV96]. Signing [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98e, KAK96, Ros96a, Ros96c, Ros96f]. Signs [Eri97b].
Sizes [PKA98]. Skew [BS95d]. skill [Gre90]. Skipjack [BBS98a, Bih98b, BBS99a, BBDR99, KRW99].
Skipjack-3XOR [BBDR99, Bih98b]. Skolem [GS99a]. skullcudgery [Beu94].
Slab [FVEA99]. slacken [Gen99b].
Smaller [DDJ98a, DDJ98a]. Smallest [Got99]. Smalltalk [Lut98]. Smart
[ABKL91, Ano96z, Ano99e, BE90, Bov98a, Bov98b, BDB92, Cha99, CM99c, Chr99a, Con98, Con99a, Cor98, CH99a, DDJ98d, DDJ98b, DDJ99, Deu97, Deu98, Di 97a, DT98b, EN98, ENK99, Fan96, FGPL96a, FGPL96b, FOM91, Gar97a, GL96, GPSV98, Gut98a, HKQ99, HP98a, Hru96, HH99, Hus99, Koe99, KCC94a, KCCT94b, Mar98a, Mye96, NM96b, Omu90, PV98, Roh99, SKW98d, SS99a, Ste99b, SR96, SGPV98, Smi98a, Sut99, Tua99, VW98, Ver98b, dWQ91b, dWQ91a, ABKL93, AHDJF97, Al97, BG97a, Cha99b, CW97, CJRR99b, D98a, Dhe98, Di 97b, DF97, Gau97, Kip97, Sha95a, TJ97, Taa98, AG99, Bak99, BF99a, Bro97, DVS96, Gir99, GST96, HNS99, IW99, NFQ99, SM94, SKM99].
Smart-Cards [Roh99, ABKL91, ABKL93, CJRR99b].
Smartcard [Ano98q, Ano99b, USE99c, Ano97x, Ano97-47, ARA93, BAN97, Ano98p, CH94b, I99a, KK99a].
Smartcards [Bla96a, Bla96b, Fan97, Sch90a, DR99a, I99a, IHR99, MDS99].
SmartLink [Ano93k]. smooth [Odl94a, VZ97]. SNAKE [MSK99a].
Snefru [BS91f]. SNMP [Sta96c, VDDR99]. SNMP-CORBA [VDDR99]. SNMPv2 [GM93a].
Snoop [Ano94i]. Soar [Gar97b]. SOBER [BP99a].
Soccer [BL99, CM99d, IND99, PWU99].
Societal [Sta97b]. Societies [IEE92d, IEE94f, IEE95c].
Society [Ano98n, IEE92c, IEE93b, IEE94d, Mar96, DL96, KG96, Ta98].
Socio [SM99].
Socio-technical [SM99]. Sockets [ZG96].
SOCKS [Lee96, McM96]. Soft [NS98a].
SoftID [Ano96-27]. Software [Abr97, Ano93j, Aue96, AG99, Bih97b, BD94, CD97, Cla98a, CT99b, DBVD96, DF91c, DSB99, Gar97a, GO96a, Gut98b, HK97, J98c, KP96b, L95, Lac93, Lea99, Lut98, Mat96b, Mer91, MM97, RSA94, RC94a, RC94b, SW94a, Sch99c, SK96a, SK96b, SK96c, SW97a, SW97b, SK97c, She95b, You96, And94a, Ano95g, Ano96-27, Bih97c, BP97b, DH96a, Des95, Go96d, Knu99c, PA93, Pre95a, SS98a, SAM97, Str93a, Str93b, Sz97b, Vau98e, W90a].
Software-Optimised [RC94a, RC94b].
software [MM95]. SOI [NFQ99]. Solaris [Sun91b]. SOLID [Ano97-33, CK95, Gut96].
Solutions [HM98, MS99, PW98]. solve [WSFC99]. Solved [Ano97c, Ano98i, Ree98].
Solving

[LO91b, Lew92, M96, OMV98, Per99].
SOM [BBN96]. Some

[Ab98b, AT99, BBL95, B190a, BS91g, CD95, CRR99, CL98, Des98, Ev91, FDB93a, Gib90, Gui97, HGD98, Hub91, HCY96a, Knu99a, KP95, KYD98, L92, LP94, Lid90, MSS98, OK98, Sim97, TCH91, Wag98b, Cao99, Cha95a, FDB93b, Go97c, Lan96, RD96a, SMK98b, TH99, Koo97].
Someone [MB99a]. Something [SvA98].
Son [CFK98]. soon [P94]. sophisticated

[Me198]. Sought [Ano97-45]. Sound

[CJRR99a, MGL98, Ano96-29]. Soundness [DE99]. sounds [BDC95]. Source

[Sch94g, Sch96a, Sch94h, Zim95b, Gen99c, Zim96a, Zim96b]. sourcebook
Kal99, MBB98, PP96, Ano92b.


starts [Ano96-29]. State [FGS96, Lan98, LF99, Mjo93, NM96a, Pre98c, PR98, Pre99, She92e, W93a, W93b, Zaj97, BFS92a, BFS92b, Gut96, PGV93d, Ril96].

State-industry [Zaj97]. State-of-the-Art [IEE98b]. Stateless [BGK99]. STATEMATE [DJHP98]. Statement [II96]. States [C197, Uni98h, Uni95a, Uni98k, U97b, C199, Lev91, Mi95, U97b].

statesman [Bed90]. Station [BWM99b, Smi98b]. Station-to-Station [BWM99b]. Statistical [De 99, GSV99, Gus96, PNFK95, N98, Tha91, GKS97]. Statistics [BBDF97, IEE94a, FO90].

Status [Dob96b, FL99b, Nat99c, NBD99, Ros95b, Buc95b]. Stay [MK94]. Staying [Rit99]. Steady [MS99a]. Steal [Wal99]. Steganalysis [Ett98, J998c]. Steganographic [ANS98a, CM97c, NHB98, ZFKP98, ZFK+98]. Steganographie [MP94]. Steganography [All98, And96b, AP98, Cac98, Cra98, C196, DS96, FJM+96, Joh97a, Joh97b, J998b, Joh98a, Joh98c, Kah96a, MT94, Mau97c, NNE979, Phi98b, Rho95, WW98a, Cai96, Cra97], Steiner [ZW99]. step [Ano97d]. Steps [GO96b].

Stern [Cus97]. Still [B199, Mei98, BCCP97]. Stockholders [MS99a]. Stop [BP97a, PP97, SSNP99, vHPP93, Phi96c].

Storage [AR99, BFS96, CMN99, SJ97, WB92, BMS96, Sta97a]. Store [AW99, CadH96, Way91].

store-and-forward [CadH96]. Stored [SV99a, SV99b, Lee95, Sv998]. Store [DD98g, DD98h, Kah96b, Pra96, Ritxx, Eli97, Hag98, HS93, RK99b, Wei97].

Strand [FHC99]. STRATA [PMP99]. Strategies [AWV99, CO98, Dae95, KFJP96].

Strategy [Gar97a, KTM+99, OMV98]. Stream [AM97, BD94, Cha94a, CS91, Cla97, Cla98a, DC98, Din94, DRN97, Go97d, Go99b, J999b, LS97, Mau91a, MS91, PK95a, PK95b, Pen96, Rob95b, Ros98a, SK97b, SK97a, She94a, She94d, War98, ZYWR91, ZG96, BK95a, DG94b, DX91, Go95b, Go98b, JV98a, LR93, Tay94]. Stream-Cipher [ZYWR91]. Streams [GR97, PSB97].

Street [Ano97k, KS98b, Sim98c, HRT96, Law98]. Strength [HK98, HK99d, Ano98a, Cop94a, KM97, Mat95, Wei99]. strengthen [BB95a]. Strengthened [DBP96].

Strengthening [MB94a]. Stretch [Pai99b]. Stretching [And96b]. strict [SZ99a, YT96, Cus96, CS96c, O’C94]. string [Oel95]. string-re-writing [Oel95]. Strings [Gol96b]. Strong [Ano97-46, Ano98s, Cvi91, Gar97b, Gut98b, GS99b, PW97, RS98e, RXXx, Sii97b, Sii97a, WD99b, Wei98, ZZ96, Ano96g, Bee96, DL93, DT93, MCD98b, SZZ95b, Sze98, Ver98b, YW99]. Stronger [Ano95v, FS97b, MAM95, SVA+98].

Stronghold [Ano97-33]. Strongly [Mau91d]. Strongly-Randomized [Mau91d]. Structural [BHJ99].

Structure [BCC90, HV98, Mat96a, PRAM98, LL93b, M95, PS98a, RD96a, Sch98a]. structured [FR95a, KS98c, O’C95, SK97d]. Structures [BR98, EKLM99, Koh99, Lut98, MSN99, ZZ95b, LA95, Mic97, PD99a]. Structuring [Hru99]. Struggle [Gla99b]. STS [BWM99b]. Stubbbine [HLL+95]. Stubs [AO96]. Student [Ste91]. Studied [Che92].


Subjective
Subliminal [BDI+96, Gru98, KI97, SI93b, SI94, Sch93b, Sch94e, Sim93, Sim94d, Sim94c, Sim96a, Sim97, Des96b, Sim98a, Sim98b, YL97a].
Subliminal-Free [BDI+96].
Sublists [Rus93a].
Submanifolds [Mra95].
Submission [Ada98, CMKK98, BT97, Zun98].
Submissions [SKW+99a, SKW+99b].
Submit [Law98].
Subquadratic [BBP95a, BBP95b].
Subscribers [GC97].
Subscript [Mau91b].
Subsegments [KPR99].
Subset [NS99b, CJL+92].
Substitution [CT99a, HS90, PRAM98, SZZ94b, ZZ96, Ata94, FSN93, Fri92b, HT95, O'Ca95, Zan90].
Substitution-Permutation [CT99a, HT95, O'Ca95, Zan90].
Subtitle [Mer90b].
success [Blo98c, TY94].
successful [HA94b].
successfully [Al96].
Successor [Ano97-45].
Sufficient [MSN99, Rus93b, Rom90b].
Suggested [Bih91].
Suggestions [Mat96b].
Suit [Buc95b].
suitable [CCZ98, Kob90, MZI98, Miy93a, Nae93, NM94, XL98, YL95a].
Sum [NS99b, CJL+92, JV98a].
Summary [CFGS99, DY91d, Un96a].
summation [Daw94, E994, Mye96].
Summit [CFK+91].
sums [BK98g, CFS97, Kob91c].
Sun [Bro97, Gar98b, Got99, Law98, Swz97c].
SunOS [Ste92, Sun91b].
Super [Sut99].
Supercomputer [DSM95, She92b, Bam97].
Supercomputing [IEE91].
superhighway [BDC+95].
Superimposing [YY91].
supersafe [PP96].
Superscalar [Cla97].
superscript [Cra92, CF92].
Supersingular [BS91b].
Superisory [KA99].
Support [AKP99, BV98a, Bla98, Bla93, DTDJ99, FR95d, GR99, HKS95, KHB99, LBH99, LCN99, Mon93, Pit96b, SK98a, SK99, SL99, TYD99, Ano97, Ano98f, Clt99, LS98a, TCH+91, Un94b].
Supporting [PK99, MI90].
Surmounting [CI96].
surrounding [GA98].
Surveillance [CKN99, SB97].
Survey [Br90b, Gar97c, GFB93, Kal93a, Kle90, Knu98b, P99, Par98c, BO92, Ele99, Mea95, She92g, Wad98, Zho94].
Surveys [Ell99].
Susceptibility [AW94].
suspected [LHL95b, LHL95a].
swapping [TN97].
Swedish [LF97].
Swindles [Dob95b].
Switches [Bee99].
Switching [MOM91].
Switzerland [ACM97a, BCB97, IEE96c].
sword [Den95].
Sydney [KG93, SP90, VPM97].
Sylvester [Por98].
Symbolic [Wat91, AM99, BHK95].
Symbols [Pes97, CS99].
Symmetric [Ada97a, Bir98, BDR+96, BFN98a, FO99b, Gus96, QG90, R90e, YY98d, YY98b, BDJR97, Cra96, GHS93, H99, Hwa93].
Symmetry [BS95d, PS97].
Symposium [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97b, ACM97c, ACM98b, ACM99b, An99c, Com96, CMM93, DEQ92, He96a, IE992, IEE93b, IEE94d, IEE95b, IEE96a, IEE97f, IEE97i, IEE98a, IEE99a, KK99b, Q98, Sp99, S93, US92b, USE93, USE95b, USE96c, USE96g, USE98a, USE98d, USE99a, Wat91, Wol93a, Wol93b, Tv92].
synchronised [K97].
Synchronization [DS995, BB99].
Synchronized [Yah94, Gon92].
Synchronizing [Bih91].
Synchronous [AMP99, TT99, DG94b].
Syndrome [CS96a, ZY91, H90].
synopsis [Wri98a].
Syntax [Kal98f, Kal98e, Kal98d, RSA93d, RSA93c, RSA93e, RSA99a].
Synthesis [HL99, Sab94].
synthetic [PGV93b, PGV94].
System [ANS98a, An97-33, ADF98, AHMS99, BS99a, BLM99, BKS99, Ba97, BR97a, BM91a, Bie98, Bla94b, BLM99, BG99, Bur94b, CIBM99, CD97, CM99b, Ch92, CC99c, CH94b, CM99d, DDP90, DT98a, DT99f, Far92, FK99, FO97, FR95d, Gan96b, Gar97a, GR99b, Gol90a, GPSV98, GS99a, HJTW99, HCD99, HJL99, HE98,
INDI99, JO97, Jia99, KI99, KW99, LMP99, LWY95, LC99, MGL+98, MKL99, MR95a, Mar98a, Mau97b, MTVZ92, Mon93, NM99, NS98a, Nec96, PR99, PS99f, PK99, Rei92, Rus90, RH99, SY99, SSW98, Sam98, STSW99, SCT99, SK96b, SK96c, Sch98h, SSP90, SM99, SKT99, Tro93, Tun99, Var99b, WFG92, 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, M KK99, Me97b, MM95, Oel97, PS99e, PSW95, Sch99j, SY96b, SS95b, SS95c, TCH+91, TC91, Ven90, WSC99, WABL93, ADD91, Ann91a, Bax97, Bel92, Dan95, JD91, RC95, YKY99, ZH98].

Systematic [BGH95b].

Systemises [MKL99].

System [ABLP93, AKP96, AKF94, Ako99, Ano94k, Ano95r, Ano96a, ADED99, AEG97, AMP99, BDP99, Bar99, Bas93, BR91, BBD97, BF98a, CF95, DD98a, Dan91b, DFTY97, DY91a, DD99, DB96, ENK99, FJP96, FY95a, FY95b, FYM99, FO991, GL96, GFB93, Gl98, GM90, GMW91, GK96, GS97, GM98, HGH98, HJJ+91, H99, HP98b, IEE93a, IEE96b, IEE96d, IEE98e, IEE99b, I99a, KT96, Koc96b, K99, KY92b, L91b, LQ98b, LAB92, Lau99, Lee99b, Mar99, Mas99a, MS95f, MDP94, Muf93, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PS91, Pin97, Pit96b, PM99a, PD99b, RBV94, RG95, RPI95a, ST94, SN96, ST99b, DY91c, SO95, S90, She92a, SY92, St99, Tr99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a].

Systems [WL92b, WC97, Yac99a, Yac99b, YKB94, YMW99, ZFK98, ZFK+98, AR99K, AH4JF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BP95b, CG05, DMW94, DIX94, Fri92b, Goo96, GKS97, Gr98, HJJ+97, IEE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Oht96, Ole95, Opp96, PAK98, PA98b, PP99a, PP92b, PP95b, PP95a, RO96, SKB97, SY96b, SG96b, SK97d, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, Z96, D96, D96].

Systolic [SS98, DF92, PJB90].

SYST [DA98d].

SZK [GSV99].

T [YT96, PDGI99].

T-Team [PDGI99].

T52 [DA98c].

Table [KMK99, Has99, Hor95].

Tableaux [Mas99a].

Tableaux-99 [Mas99a].

Tables [DRR95, JC98, IPNdbbprm91].

Tactical [IKM99].

Tagging [Lud97].

Tailoring [CG96].

Taken [GQW91].

takes [Sz97].

Tale [Kal98, R99].

Talent [DD98b, DJ98].

Talk [Deu97, Lei99, Wat99, BS91].

Talking [HH99].

Tamper [Auc96, BDF98, KK99a, Zhe95b].

tamper-proof [Zhe95b].

Tamper-Resistant [Auc96, KK99a].

tamperfree [Hwa92b, Hwa92c].

Tampering [CL98, CL97].

Tanaka [Hwa92a, MS98a].

Tandatangan [Ano97-50].

Taos [WABL93, WABL94].

tapestry [MB94b].

Targeted [Cap94].

Targets [Lea99, Way98].

TAS [Cop94b].

Tasty [Sch98].

Tate [FM99].

Taxing [Gar97].

Taxonomy [DB96, GS97, LBMC94].

TC [MB99b].

TC11 [Kat97].

TC6/TC11 [Kat97].

TCFS [Man97b].

cel [GA98].

TCP [Ano96j, Fei93, Fei96].

TCP/IP [Ano96j, Fei93, Fei96].

TEA [KSW97a, KSW97b, NW97, WN95].


TecApro [GL98].

Technical [Ano95e, Bar96b, CFK+91, CYY98, DS97c, Lan98, L93c, Mos98, USE95a, USE99d, VGP93, SM99, USE96f, USE98c].
Technique [DDNM98, Gue98b, KP93, WD97, BCV97, ONT98, Way95].

Techniques [Int91a, BGML96, BWM98, Bol98a, Bol98b, BLMO94, CM97b, CD99, CMYY98, Dam90a, Dam91a, Dav91, DC98c, De 95, Des98a, Des96a, Fun97, Fun98c, GQ95, Hel94, JJ99a, LvdLB96, MM99a, MSNW99, Mau96b, PS98e, PS98f, PK99, Pre93b, QV90, QG95, Rue93, S293, Car98, Cra96, He99b, ISO97, Kay95, KG93, Ny98b, OPH+99, Oko96, PS99d, SD97, Ste99b, Way91, Woo90, ZHI93, van96].

Technological [UFC94].

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

Technology [Int91a, Ano96-29, Ano96-30, Ano98t, AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, II96, IEE94b, IEE96d, Lic94, Lin93c, NF99, Riv98c, USE99c, Ano93a, Ano96u, DS97b, Gil97, ISO97, Rif96, Ros94, Sav96, Smi97a, VB96, CDFK+91, Ers99, Ano99b].

Telecollaboration [Fuc99].

Telecommunications [IEE97e, UN94, Ma98]. Telemedicine [Ano97-50]. Teleperubatan [Ano97-50].

Telephone [Gar97a, Sha97]. Telephony [Ban94, Gar97b, MB99a, Mar95b, PW98].

teletype [Ma98]. TELNET [SSH93, Ala93b, Ano95w, Bor93a, Bor93b, Bor93c].

Temporal [KV99]. Temporary [KR98].

Tennessee [IEE94e]. TeraSpell [Ano97-34].

Term [EO95b, CHN97, EO95a]. Terminal [Con98, Con99a].

Terminals [Ano99f, ADSW99, Lam99]. Terminology [Phil96a].

Ternary [PKA+98]. Terrorists [Uni98j]. Terschelling [TV94].

Tesla [Ano97-37]. TESS [Dan95]. Test [DS97a, Law98, MOM91, SS91, DLP93, Graxx, Gre90, ZYR90].


Tetherless [Law98]. Texas [ACM97c, ACM98b, Ano94e, IEE92b, USE98f]. Text [Bar93a, Bar93b, Cad96, CD97, LM98b, PF94, PBGV90, CDFK+91, TB94, SH98].

Textual [JKVP99]. Tejus [NM99]. Theft [Gur97].

These [BK95c, BL96a, BL96b, Con99b, GPT91a, GPT91b, GMW91, JMS96, K196, Len99b, MO90, SY96a, SG98b, Tra99, VDDR99, AA99, BHSV98b, BHSV98a, BY93c, BY93b, Car98, DDB95a, DDB95b, Don98, Eng99, HMP95, KT91b, LN94, LM96, NM96b, SSI98, SI93b, TY92, YY98a].

them [Way95]. theme [IEE97k]. Theorem [AA93, FK99, GPSV98, HB99, DiDPS96, Sga91a, WW99].

Theoretic [UFC94], Theoretical [AAB+97]. theories [T+98]. Theory [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM98b, ACM99b, Ber96b, BMP+97b, Car97b, CDFK+91, Dam90a, Dam91a, Dav91, De 95, DSB99, Fun97, GQ95, Hel94a, Hel94, IE94a, IRM93, IZ98, IZ99, KY96a, KR99a, Keb94, LOX99, LABW92, LW91, Mau96b, Mau96a, MDP94, NKC94, NC97, OD99, PSS95b, PG90, QV90, QCG95, Rue93, SSI98, Ada91, AAP92, Ata99, CS97, CFC96, Cou99, Dan99b, DXS91, Gol97c, Gol92, GS94b, Hln94, Lag90, LABW91, Lox90, MV98a, Mau93b, Mc90b, Mei92, Ny98b, Pom90a, Rac90, Sch93a, Sch90c, Sch97c, Sga91a, SII99a, Ste99b, Sti95, Tat98, Tat99].

Third [RI96, Zha97, Way93b]. Therefore [FJM+96]. these [Ano89q]. They’re [Wri94].

Thomas [CFK+91, Bed90]. Those [BCE+94]. Thoughts [Knu99a]. thousand [Ril96]. Threat [Hig97b, BCW97, Hed97]. Threaten [Gar97c]. Threats [EN98, Jan98, SS99a, WN98b]. Three [Ano95a, BR95b, HEQL98, KS97b, Ng99, OMA98, SN96, FR95b, OMA97, XZZ98]. Three-Dimensional [OMA98, OMA97]. Three-Party [Ng99, XZZ98]. Threshold [BBCM93b, BBCM93a, CGJ+99, DF90, Des93, Des94a, Des94c, FY98b, Gem97, HHT93, HHT97, JMO94, KOO95b, KOO95a, LH93a, LHL94, LHL95b, LHL95a, MKS99, NP98a, Oka98a, Oka98b, PM98, Rab98, Str98b, SSNP99, Zha98, Blu95, CMTNY94, DDB95a, DDB95b, FD92, GJKR96a, Lan95, Lan96, LRL97b, MPSV99, Ped91c, SG98, SS94, TJ99, WAM094, XL99, CG99].


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


Trade-offs [BFS96, BMS96, NMVR95a, NMVR95b]. Trademark [Eri97b]. Tradeoff [KR94c, CK93]. Tradecoffs [CMN99].

Trading [FHM98, D97b]. Traditional [Des92].


Ano91a, JD91]. Transactions [FL99b, FKMY98, SS99]. transcendental [PGCSN96]. Transcript [BD99a, Chr99a, Sas99a].
Transcript-Irrelevant [BD99a]. Transfer [Ano97-34, DF99, HHY93, NP99, RS96a, Bea93, BM90, BR96b, DOR99, Jac90a, Jac90b, SF93b]. Transferable [Sak96].
Transfer [Ano97-34, DF99, HHY93, NP99, RS96a, Bea93, BM90, BR96b, DOR99, Jac90a, Jac90b, SF93b]. Transferring [SI94].
Transform [Boy99, KMS95a, KMS95b, Kuo90, MS94, Riv97c, WF94, TKS98]. Transformability [MSO96].
Transformation [SZ96, LS98a, Pet91]. Transformational [Zwi98].
Transformations [BDFM99]. Transfusion [ADBB99]. Transient [BDHJ98, CH94a, JQB97]. Transistors [CWM91 + 91]. Transition [Des98a, DR98b].
Translation [CFK+91, OP97, OP98]. Translucent [BR96b]. Transmission [NHB98, PSB97]. transmitting [CLI97, CLI99, UU97b].
Transparent [Bla93, DS97c, Mat97b, SZT96b, ZG96]. Transport [Ano94b, BW98, GBC93, Sar97].
transposition [Bar92a, Bar95, GSN94]. Transputer [GN95b]. trap [YU92]. trap-door [YU92]. Trapdoor [BM92, BY93a, BHSV98, BH98, BHSV98a, Pai99c, RP97a, WBDY98, And93, Gar96a, Gar97d, Ort95b, Ort95a, Way93b].
Trapdoors [Gib91, Gor93a, Pat99]. trappes [Sch98e]. travel [Sav97]. Traveling [OMV98, RS99a].
Travels [YU97]. treaties [Des90a]. Treatise [Tur99]. Treatment [BFN98b, Mau96a, OO98, BDJ97, BFN98a, Gen99c].
TREC’98 [LM98a]. Tree [BM96b, BM96c, GM99b, PB99a, LL93b, O’C95].
Tree-Based [BM96b, BM96c]. tree-structured [O’C95]. Tree-Width [GM99b]. Trees [Aga92, BP97a, HS90, ZW99, SS99a].
Trellis [SKD94]. Trellis-based [SKD94]. Trends [DDJ98c, DJJ98f, De 93b, De 98c, Hru98, IE97k, Kan96, LM98a, MB99a, Koo97, Seg92]. Trial [Mye96]. Trials [CY98, P96b, Ano93a].
Triangular [Por98]. Tribulations [CY98]. tribute [Un92]. Trinity [IE97a]. trip [Cur98].
Triple [Ano95p, Ano96c, Ano96-28, Bih96, BK98c, Bih99b, CJM95, HP99a, HP99b, KMS95b, Kum98, Luc98c, CJM96, Mey97b, Per91, vOW91, Joh99, KSW96, Rot97, Mey96b].
Triple-DES [Ano95p, Ano96-28, BK98c, Kum98, KSW96, Rot97, Mey96b]. triples [CF97]. Trithemius [Ree98]. Trojan [Sch99f]. True [Way91].
Truncated [KRW99]. trunk [Uni94a, Uni94b]. Trust [Ano99j, BPK99, BFK99, LA98, MR98, Re96, SA95, Sim94a, Sta95a, YK98, YY96, AHdJF97, BH98, Com97, Chi99a, Chi99b, LN98]. Trust-Based [YK98].
Trusted [AAB+97, Ano97d, IS91, MKS99, RS98b, SK97c, SS99e, SS99f, CGM97b, HY93a, JMO95a, LWC96, Ped91c, Wu92].
Turnaround [Gar97a]. Tutorial [Buc91b].
Two [AB96a, Bea92, BMM99a,
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 [Fer98, Al 96, O’C94]. Urge [GB98]. Urgent [Pra96]. URL [Zuk98b]. USA [???90, Ano98n, AA97, Auc98, Bri92, Bri93, Cop95d, Des94b, Han99, HF97, IEE97c, IEE97e, IEE98c, IE98e, Kal97c, Koh96, KP99b, Kra98, SJ97, Sti93b, Sti94, USE91, USE93, USE94, USE95b, USE95c, USE95a, USE96f, USE99a, USE99b, USE99c, USE99d, Wie99]. Usability [WT99, CG05]. USACM [Ano97-52]. 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, GI97, Joh90, Ri96, Way93c, Zer96a]. Used [GS94a, SG96, Car97c, Car98, Gau97, Kuk99, Sch91b, SX90, van97a]. USENET [Bi91]. Usenix [USE99d, Con96, Ros96a, Ros96b, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c]. User [AKF94, BE90, Bus96, Dra99, Gog99, Gol90a, GN95b, IS99, KCCT94a, KCCT94b, PMP99, RSSW99a, RSSW97b, SYM98, SCT99, Web99, Zim95a, Ano95o, DF91b, MC96, Mu92, RSA94, RT93, SJS98, Sta95b]. User-Centered [PMP99]. User-Oriented [AKF94]. Username [Le96]. Use
[Ano96-31, Hel98a, WK97, Sha97, Sta94a]. Uses [Si97, Ano97x, DKR97b, Sch99g]. Using
[ANS97, ANS98b, Ada97a, AG97, AHJ97, Ano99, BDPS979, BCK96e, BBS99a, BFP99, BW98, CIBM99, CK95, CM99d, Des96a, DS97d, EST99, FVEA99, FW91, FY98b, GM97, GAG09, GS99a, HN99, HRV99, 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, OM93, PSE97, Pin97, PZ98, PJ99, QQ90, RB99, SG93, SK94, Sas99a, SK96a, SK97b, SK97a, SK97c, SD99, SRY99, SR96, Sim94d, SHK99b, Sun91a, SZT98a, TAP90, TA92, TY99, TO94, VN94, WKG97, WCS95, Ym98b, Ym99, YST99a, YY97a, YST99b, AA95, All98, Ano97y, Ata94, BS96a, BS96b, BT98, BGR95, BI93, BIh94a, BB95a, BBS98a, BD95a]. using
[CW91a, CNST98, CC95, CM97b, CP99, CB96, Cle96, Dan97, GK99b, GBL94, Gor93b, Hor95, IS97, Jak95, JM96a, KR95a, KC95, Kar96, Kay95, Koc95, KH97, NH98a, LC96b, LC96c, LM95a, MHPS96, MS95c, MS95d, Mit92a, NT93, MS95e, RP94, RS98a, RT93, SS94, SD97, Su98, SZT98b, SZT98b, T97, Ti98, VZ97, VP98, Wh93, Wh93a, Yam98a, Zho94, dR95]. Utah
[USE95b]. Utility [Zol93, Ano97m, Vu95]. Utilization [GR95]. Utilize [MS96]. utilizing [SW95a].

[DDN98, GS99a, RB99, Ste96, CM96]. Validity [GMW91, Kuk99]. Value
[Yua92]. Vanstone
[Kie98, NS97c, NS97b, Sha99a]. Vaporware
[DDJ98e, DDJ98f]. Variable
[BR99a, BR99b, DW94, GKB95, Sch94b, Su98, TN96a, TN96b, ZPS93]. Variable-Input-Length [BR99a, BR99b]. Variable-Length [Sch94b, Su98]. Variance
[Kas96]. variant [TC97]. Variants
[CRR99, MSS98, RS99a, Sha95a].
variation [CCN95]. variations [Zho94].
varieties [Fri92b]. Various [GQW +91].
Vasculature [BALS99]. Vatican [Alv98a].
Vector [ADEDS99, TK99, TYD99, CCH98, MTN97, Pad98, dR95]. vectors
[LM93c, Mat91, MLA91]. Vegas
[ACM95, AA97]. Vehicle [CKN99].
Vendors [Gar97a, Gar97b, Gar98a, GB98].
Venona [HK99c, Pea97].
Ventura [Nat98, RD99a]. Veri
[SY99]. Veri-KoMoD [SY99]. Verifiable
[Abe98a, AGY95b, CG98, Cre90, FR95c, GM95, Ped91d, Sch99i, VBD99. AGY95a, BD98a, Bur96, FO98, Mao97, MLY93, Ped91b, Ped91e, Sta96a]. Verification
[Abe98a, AB97, BGR98b, BGR98a, Bo98a, BGR98b, CDF915, D97a, GFB93, GS99a, HL92, MM99a, Na97, OMR93, PM98, PV98, SM95a, SY99, Tou93, WW98b, YY99a, Ano97p, BGR98b, Bo97, BS95c, CM96, Des90a, Dwo91, J9C8, JW01, Mea95, Sha97, YL95a, YM98, ZLX99]. Verifications
[GMV98]. Verifier [JMSI96]. Verifiers
[PM98]. Verify [DS97d, Ch99a, Chi99b]. Verifying
[LHB96, Sa91, DN95b, Pau98]. Verlag [Hat96]. Verlassliche [BGH95b].
Vermont [IEE96a]. Verschlüsselte
[Kip97, Kip99b]. Verschlüsselung [MPS94].
Verschlüsselungssysteme [Wal98].
Verschlüsselungsverfahren [Ger97].
Version [Ano97-33, Ano97-34, BC93a, BP98e, DBP96, FKK96, Gar97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, RSA93f, Lim99, MT99a, McM06, RSA93a, RSA94, D9Y1c, SS99b, SM98b, WABC99, CLW98, GM93a, Gib95, Bor93b, Lin96b]. Versus
[MGL +98]. Vertraulichkeit [FT95]. Very
[HM93, MSDS90, PPF94, Yua92, SN94].
Veto [OK96a]. VHDLL [Oel97]. via
[BR96b, BCKxx, BM95, BS95d, DS90a, DN95a, DN93, EPR99b, EPR99a, Fuc99, HS94, JJ99b, NW98, UFC94]. Vibration
[Nas94, NA95]. VICS [Uni96a]. VICTOR
[OSA91]. Victorian [Abe98b]. Victory
[Mus92]. Video [Ano99f, BF999, DLF97, DS97c, DSS98, HG97c, KBR97, KH98b, LT98, MT94, SJ97, SB98, SZT98a, WKH97, WW98a, ZL99, BB90, BCB97, CPO +98, CHO +98, CKLS96c, DS97b, HG96, HG97e, HG97d, HG98, HW97, HW98a, Lan99, Oht96, QN98b, SHG98, SZT98b]. 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 [Kl96]. Vision
visit [QJ98a], Visited [FY95b]. Visual
[ABDS96, B +96b, BD98b, DDGM97, Dro96, HKS97a, HKS97b, JKVP99, K916, NS95, NP97, PKA +98, P998, PNFK99, Sha98, Sti98b, BW97, Ger99b]. Visualisation
[MM99b]. Visualization
[Jan99, PH91, GTGW94]. Visual
[BW98]. VLDB [Yua92]. VLIV [Cla97].
VLSI
[CKM99, 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,
Sch99i, FOO93]. vowel [Lip98]. Voyager
[AHMS99]. VPN [Ano99d]. Vries [GK95b].
VRML [Gar97b, Gar98a]. vs [DP99, GA98, Mus92, Tho96, Uni98a, Uni98d]. VSP
[YEA+98]. Vulnerabilities
[Ano97-53, Sch98d]. Vulnerability
[Gar97c, AF95, Ano95w, Ano95x].
W [YT96]. WA [USE99b]. Wafers
[Gar97a]. waggery [Beu94]. Waldmeister
[HJI99]. Wall [Ano97k, HRT96, Law98].
Wallet [CP93]. Wallets [DT98a].
Walsh [SPS97]. Wang [vT93]. Want
[Rot97, Way93c]. Wanted
[Bra95d, Hil97, PKA+98]. War
[Alv98b, AK99, Dav98a, Don98, Law98, Mon96, Mus92, Rat96, Ros99, Wei99, Wil98a, Dre92, Mar98b, Hin93, Jol95].
Warden [Cra98, Cra97]. Warehouse
[EKL99, TLS99]. Warehousing
[BMNL99]. warfare [Den99, Rot95a].
WARM [MPL99]. WARM-UP [MPL99].
Warned [Kah91b]. Warning [Gar97c].
Warrant [LWY95]. Warranty [FKMY98].
Warranty-Based [FKMY98]. Wars
[GC97]. warum [MP94]. Was
[CFK+91, Dea98b, Krn98, Mey97a, Mon96].
Washington
[HF97, USE98a, USE99a, DDJ98e, DDJ98f].
WASS [PS99b, PS99c]. Watch
[Cha99a, Rit99, Sch99h]. watchdog
[MPH95]. Water [WF94]. Watermark
[Ano97z, CKLS96a, ON98, SY98, TRS+93, WD96, vTO94, And98, Ano93a, CKLS96b, CMYY97, BB9C97, TOH98, XBA97, YEA+98]. watermarked
[BP98b, BP98c, RRP97]. Watermarking
[Ack98, AD98, Ben99, Ber97b, BOD95, BO96b, BF99, Car97a, CKLS97, CMYY98, DDM98, DDGM97, DSS98, EQ98, EL99, FBS98, GDD+97, GB98, GO96c, HG97c, HG97d, HG98, KR98, Kob97, LQRS98, MB98, Mos98, NH98, OMA97, OMA98, P298, QN98b, RKDB96, SCxx, SZT98a, SZT98b, TK97, WD97, Xie98, Y99a, ZK96, BBCP97, BBCP98b, BBC98, BCD98, BP98d, BCV97, BO96a, CPO+98, CHO+98, CT99b, CKLS96c, CM97d, DQMQ98, DMM96, DMM98, DNS98, HG96, HG97e, HEG98, HPA99, HW97, HW98a, HW98b, Irv98, KKH, KH98a, MTN97, Nat97a, NO98, NP98b, ODB96, OP97, OP98, OPo+99, Oko96, PHF99, SD97, SHG98, SZT98b, SZTB98, TA97, TKS98, VP96, VP98, VNP98, Yeu97, Yeu98, Y98b, Z98b, ZKOY99].
Wavelet [LSV95, KH97, KH98a, NO98, XA98]. wavelet-based [KH97]. Wavelets [Lut98].
Waves [JAI97]. Way
[BJ9Y7, Bd9M94, BM94a, BKK98, BP97c, DG93, DD9P90, GM9S98, MR90a, Roe94, Sch91b, TOU94, Zhe90, BHR99, BK98f, DI99, Dob98, HILL99, HIL97, Hwa92a, M9Z98, Rom99b, Sim98c, Sta94a, S9e8, T9u92b, T9u92a, ZPS93, KSW97a, KSW97b].
Wayner [vdW97, vH97]. Wayness [H99]. ways [Den95]. WDA9 [TV94]. Weak
[DG94c, DLY98, H9w9b, Pit96b, S9e8, Vau96, FY95c, H9w9a, Knu95, S9197a, S9l97b, YL97b]. Weakened
[AB99b, AB99c]. Weakly [MP91].
Weakness [Cop99, KSW99a, Kie98]. Weaknesses [B9S94, DY91e, Kel99, KP93, Lan96, PA98b, RK98a, RJ99, S296, DG94b, Sh96b, XZ97]. weapon
[Ano97]. weapons [Mei98]. weather
[Ano95j]. Web [Ano97-33, MR98, OW95, SA95, Sta95a, Ver98b, Ale98, Ano97d, Ano98k, BAI99, BMNL99, Cha99b, Dav95, DD98, FL96, GGM99, GO96c, LAW98, Sh96b, Ude98, W9595, You96, ZL99].
Web-Based [ZL99, Ano98k]. Web-enabled
[Cha99b]. WebTime [Ano97-34]. Weighing
References

Anonymous:1990:IWH

IT Workshop, Hawaii, USA, November 27–30, 1990.

Anonymous:1997:ACC


ANSI:1988:FIE


Anshel:1993:PMT


ANSI:1995:ANS


Asmuth:1981:EAC


Anderson:1996:TPP


Anderson:1996:TFN


Ayadi:1997:VCP


An:1999:CVF


An:1999:CVM

Abadi:1999:STS


Anderson:1998:NFA


Ateniese:1996:CBV


Aiello:1998:SAC


Abe:1998:UVM


Abeles:1998:SVP


Abe:1999:RDM

[M. Abe.] Robust distributed multiplication without interaction. In Wiener [Wie99], pages 130–147.
Anderson:1998:SPA


Anderson:1998:SNBa


Anderson:1998:SNBb


Abadi:1993:ADS


Abadi:1993:CAC


Abraham:1997:SEE

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

Auyong:1997:ASC


Apolloni:1990:TNN


ASCFS:1997:XPK


An:1999:ODR


Angelo:1994:DFS


Alexi:1984:RRB


Alexi:1988:RRF

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


References


[ACM97b]


[ACM98b]


[ACM99a]


[ACM99b]


[ADBB99]


[ADD99]


[ADES99]

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

**Augot:1998:DSM**


**Alagappan:1990:PDA**


**Adleman:1979:SAD**


**Adleman:1983:BGK**


**Adleman:1987:PRD**


**Asokan:1999:APT**


**Alves-Foss:1995:ACS**

Apostolico:1984:PMM


Apostolico:1985:CAW


Anderson:1995:SFS


Abadi:1997:RAC


Abadi:1997:CCPa


Abadi:1997:CCPb


Abadi:1998:BMCa

REFERENCES

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

**Abadi:1998:BMCb**


**Aura:1999:SLM**


**Agarwal:1992:RSO**


**Atkins:1995:MWS**


**Agnew:1987:RSC**


**Agnew:1988:RSC**


**Afanassiev:1997:FMA**

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


REFERENCES


Angluin:1995:WWM


Al-Kadi:1998:OCA


Alvarez:1999:AAS


Aberer:1994:DUO


Akoka:1999:CDP


Abdelguerfi:1996:GEI


Anlauff:1999:TSL

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


Alagappan:1993:RTA


Alberti:1470:TC


Alexander:1945:CHG


Alexandris:1992:FMC


Alexandre:1997:BSC

REFERENCES


REFERENCES


Alvarez:1998:IDC

Alvarez:1998:PCS

Akl:1985:FPR

Adams:1988:SRC

Adams:1989:SRC
REFERENCES


REFERENCES


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

Anderson:1995:RPP


Abadi:1996:PEP


Andree:1952:C


Andelman:1979:MLE


Andelman:1980:MLE


Andrew:1986:CSI


Anderson:1993:PRT


Anderson:1994:FSE

REFERENCES


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


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


REFERENCES


Anonymous:1987:EVE


Anonymous:1987:HSE


Anonymous:1987:MAU


Anonymous:1987:TWP

Anonymous:1988:DEK


Anonymous:1988:EVE


Anonymous:1988:ERH


Anonymous:1988:PED


Anonymous:1988:DESb


Anonymous:1988:DESa

Anonymous:1988:RIA


Anonymous:1989:SZS


Anonymous:1990:SEL


Anonymous:1991:ESS


Anonymous:1991:FFL


Anonymous:1991:E


Anonymous:1992:AUd


Anonymous:1992:DES


Anonymous:1992:DDS

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

Anonymous:1993:BRd

Anonymous:1993:CKR

Anonymous:1993:CSA

Anonymous:1993:CSM
Anonymous. Secure E-Mail Cheaply With Software Encryption. Datamation, 39(23):48–??, December 01,
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:HSH


Anonymous:1994:IC


Anonymous:1994:K


Anonymous:1994:L

Anonymous:1994:Ll


Anonymous:1994:PRP


Anonymous:1994:Uc


Anonymous:1994:WAS


Anonymous:1994:AUL


Anonymous:1995:AUM


Anonymous:1995:EES

[Ano95b] Anonymous. An E-mail encryption standard should be in place by April, providing for the incorporation of Privacy Enhanced Mail into the MIME standard. *Open Systems Today*, 168:26–??, February 1995. ISSN 1061-0839.

Anonymous:1995:ARLa


Anonymous:1995:ARLb

REFERENCES

Anonymous:1995:ARD


Anonymous:1995:DAS


Anonymous:1995:ENa


Anonymous:1995:ENb


Anonymous:1995:EEW


Anonymous:1995:ENE


Anonymous:1995:FSH


Anonymous:1995:FRE


Anonymous:1995:HPE

Anonymous:1995:IUA


Anonymous:1995:RLM


Anonymous:1995:SDE


Anonymous:1995:SUE


Anonymous:1995:SEE


Anonymous:1995:TEV


Anonymous:1995:XAV


Anonymous:1996:NIS


Anonymous:1996:RF


Anonymous:1996:ADX


Anonymous:1996:BCU


Anonymous:1996:CED


Anonymous:1996:CID

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


Anonymous:1996:CCC


Anonymous:1996:CSIa


Anonymous:1996:CPD


Anonymous:1996:CPT


Anonymous:1996:ENa

Anonymous:1996:ENb

Anonymous:1996:EME

Anonymous:1996:EBS


Anonymous:1996:EBS
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:SAB

Anonymous:1996:SAO

Anonymous:1996:SAS

Anonymous:1996:SUS

Anonymous:1996:TBAa
Anonymous. Technology and business: Artificial blood starts circulat-

Anonymous:1996:TBSa


Anonymous:1996:UDE


Anonymous:1996:RDSa


Anonymous:1997:AES


Anonymous:1997:AUC


Anonymous:1997:AWS


Anonymous:1997:AIR

[Ano97e] 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:ECR


 Anonymous:1997:EKB


Anonymous:1997:EW


Anonymous:1997:FSU


Anonymous:1997:FCR


Anonymous:1997:HEW


Anonymous:1997:HDR


Anonymous:1997:INI

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

Anonymous:1997:MNL


Anonymous:1997:MLE


Anonymous:1997:MEP


Anonymous:1997:NPP


Anonymous:1997:NPA


Anonymous:1997:NPNb

Anonymous:1997:PEH


Anonymous:1997:RAS


Anonymous:1997:RCU


Anonymous:1997:RAJ


Anonymous:1997:RDL


Anonymous:1997:RDSb


Anonymous:1997:RBE


Anonymous:1997:SFR


Anonymous:1997:SAP

Anonymous. SecurID authentication protects corporate information. *Net-
Anonymous:1997:SUE
[Ano97-44]

Anonymous:1997:SUR
[Ano97-45]

Anonymous:1997:SEA
[Ano97-46]

Anonymous:1997:UBS
[Ano97-47]

Anonymous:1997:CPS
[Ano97-48]

Anonymous:1997:TER
[Ano97-49]

Anonymous:1997:UUS
[Ano97-50]
REFERENCES


Anonymous:1997:UEL


Anonymous:1997:UPP

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

Anonymous:1997:VPA


Anonymous:1998:ABF


Anonymous:1998:ARD


Anonymous:1998:CSIb


Anonymous:1998:CPP

Anonymous:1998:CASb

Anonymous:1998:CASa

Anonymous:1998:CDR

Anonymous:1998:CSCb

Anonymous:1998:ICS

Anonymous:1998:EN

Anonymous:1998:EBW

Anonymous:1998:EA
Anonymous:1998:Lee


Anonymous:1998:PCA


Anonymous:1998:SEF


Anonymous:1998:SIC

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

Anonymous:1998:SAP


Anonymous:1998:TBF

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


Anonymous:1999:UGT


Anonymous:1999:UGT


Anonymous:1999:UGT

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:1999:EDB


Anonymous:1999:EPFa


Anonymous:1999:EGC


Anonymous:1999:KNT


Anonymous:1999:L

[Ano99k] Anonymous. L’inuktitut. World-Wide Web document., 1999. URL http://colourlab.com/arctic/inuktitut.htm; http://www.culture.fr/edm/fr/index.html. Follow the navigation panel link “Les écritures” to inuktitut. The author observes that the syllabary used for the Inuit language, Inuktitut, was created at the end of the 19th Century by James Evans, a Wesleyan missionary, inspired by stenography. Originally intended for transcription of the Ojibway language, it was later used for Cree and Inuktitut; only these three languages have been written in this syllabary. Examples of the syllabary are shown in links that can be followed from this page; another alphabet table is shown in the colourlab.com URL.
Anonymous:1999:SFU

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

Anonymous:1999:ULE


Anonymous:1999:WDE


ANSI:1997:AXP


Anderson:1998:SFS


ANSI:1998:AXD


Anderson:1996:CCA

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


Aumann:1998:AES


Aumann:1999:ITS


Arazi:1993:AEA


Arensberg:1921:CD


Arensberg:1922:CSP


Adamson:1995:JSR


M. Atici and Douglas R. Stinson. Universal hashing and multiple authentication. *Lecture Notes in Computer Science*, 1109:
REFERENCES


Ashenhurst:1987:ATA


Araki:1998:OEC


USENIX:1988:CSSb


Asokan:1998:OFE


Abdalla:1999:TMB


Atkins:1996:RPM

REFERENCES


Al-Tawil:1998:NAP

Atkinson:1995:RIA
REFERENCES

Atkinson:1995:RIE


Atkinson:1997:TMS


ATT:1986:AUS


Aucsmith:1998:SIW


Aura:1996:PID


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

[Ayo68b] F. Ayoub. Erratum: En-


REFERENCES


REFERENCES


Bamforth:1997:JSS

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

Burrows:1989:La


Burrows:1989:LaA


Burrows:1990:La


Banisar:1993:BCE


Banisar:1994:CPS


Bao:1994:IRL


Barker:1961:CSC


Bartek:1974:EDS

D. J. Bartek. Encryption for data security. Honeywell
REFERENCES


REFERENCES


Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.


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

90 Sherman Street, Cambridge, MA 02140, USA,


**Bastian:1995:CCE**


**Bassham:1998:ETA**


**Bau39**


**Bau46**


**Bau82**


**Bau97**


**Bax97**

Mark Darrell Baxter. Selecting the best encryption
REFERENCES


REFERENCES

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

**Ben-Aroya:1994:DCL**


**Biham:1995:HSU**


**Biham:1995:IDA**


**Blaze:1995:SLE**


**Baum:1981:RPC**


**Bennett:1991:EQC**

REFERENCES


REFERENCES


Bertilsson:1990:CVE


Benantar:1996:AOS


Bleichenbacher:1995:SRL


Boyar:1995:SZ


Boyar:1995:SZK

REFERENCES


REFERENCES

Blakley:1985:ACP


Bender:1990:IEC

Andreas Bender and Guy Castagnoli. On the implementa-

Beimel:1993:UIS


Bos:1993:PUS


Beguin:1995:GSC

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


a Trusted Mach system.

Bigun:1997:AVB


Blair:1999:DRA


Baritaud:1993:SPK


Brucoli:1999:DHC


Bas:1998:SSB

REFERENCES

Four volumes.


REFERENCES

[Bellare:1996:HC]

[Bellare:1996:PFRa]

[Bellare:1996:PFRb]

[Bellare:1996:KHF]
REFERENCES

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


Bellare:1996:MAU


Bellare:19xx:KMM


Bellare:1998:MAD

Bellare:19xx:KMM

Bromley:1983:RFM


Burmester:1991:ALN
Mike V. D. Burmester and Yvo Desmedt. All languages in NP have divertible zero-knowledge proofs and arguments under cryptographic assumptions (extended abstract). Lecture Notes in Computer Science, 473:1–??, 1991. CODEN LNCS99. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bauspiess:1992:RCH

Brandt:1993:GPP

Baur:1994:FFS

Baur:1995:PLC

Baur:1995:SEC

Blundo:1997:LBR
REFERENCES


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


Bao:1998:MFA


Boneh:1999:FL


Boneh:1999:FPL


Bao:1997:DAT


Boneh:1998:BPK

REFERENCES


[BDP97] Antoon Bosselaers, Hans Dogbberit, and Bart Pro-


REFERENCES

Blundo:1993:GDS

Blundo:1993:ESM

Blundo:1998:SSS

Bright:1979:QRN

Barrett:1990:SDU

Beardsley:1972:YCI

Beauquier:1992:TDP
[Bea92] J. Beauquier. Two distributed problems involving

**Beaver:1993:HBS**


**Beaver:1996:ASE**


**Beaver:1997:CBC**


**Beaver:1997:PPE**


**Becker:1982:EDE**


**Beckett:1988:IC**


**Beckett:1990:IAM**

Brian Beckett. *Introduction aux méthodes de la cryptologie*, volume 5 of
REFERENCES


[Bel77] Ernest L. Bell. *An initial view of Ultra as an American weapon*. T S U Press, Keene, NH, USA, 1977. iii
REFERENCES

Bellcore:1992:GRX


Bellovin:1998:CI


Bellare:1999:POP


Bennett:1980:UWN


Bennett:1988:AEA


Bennett:1989:UMS


Benario:1998:TSU


Benedens:1999:GBW

REFERENCES

[178]

books/cg1999/pdf/g1046.pdf.

**Bertrand:1973:EOP**


**Berstis:1980:SPD**


**Bertrand:1983:EGE**


**Berkovits:1991:HBS**


**Berson:1996:HMO**


**Berson:1996:NIC**


**Berg:1997:JQHh**

REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>
REFERENCES


REFERENCES


Blum:1994:CPB

Blum:1988:NIZ

Blaze:1998:FTR

Blaze:1998:PSS

Boyd:1999:EEC

Beth:1992:PCS
REFERENCES

Beth:1992:PKC

BFS92b

BFS98

BFW99


REFERENCES


REFERENCES


Bellare:1999:SEP


Bellare:1997:PNG


Bellare:1997:PRN


Bellare:1995:XMN

[BGR95] Mihir Bellare, Roch Guérin, and Phillip Rogaway. XOR MACs: New methods for message authentication using finite pseudorandom functions. In Coppersmith [Cop95d], pages 15–35. CODEN LNCS9D. ISBN 3-540-60221-6 (Berlin). ISSN 0302-9743 (print), 1611-
REFERENCES

URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm;
issue&issn=0302-9743&volume=963. Sponsored
by the International Association for Cryptologic
Research (IACR), in cooperation with the IEEE
Computer Society Technical Committee on Security
and Privacy.

Bellare:1998:BVA

[BGR98a] M. Bellare, J. A. Garay,
and T. Rabin. Batch verification
with applications to
cryptography and checking.
Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Bellare:1998:FBV

[BGR98b] Mihir Bellare, Juan A.
Garay, and Tal Rabin. Fast
batch verification for modular
exponentiation and digital
signatures. Lecture Notes
in Computer Science,
1403:236–??, 1998.
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
link/service/series/0558/
bibs/1403/14030236.htm;
http://link.springer-
y.com/link/service/series/0558/papers/1403/14030236.
pdf.

Bierbrauer:1994:BRF

Jürgen Bierbrauer, K. Gopalarakrishnan,
and Douglas R. Stinson. Bounds
for resilient functions and
orthogonal arrays. In
Desmedt [Des94b], pages
247–256. CODEN LNCSD9.
ISBN 3-540-58333-5 (Berlin),
ISSN 0302-9743 (print),
1611-3349 (electronic). LCCN
URL http://link.springer-ny.com/link/service/series/
0558/bibs/0839/08390247.htm;
http://link.springer-ny.com/link/service/series/
0558/papers/0839/08390247.pdf.

Blundo:1995:DRR

C. Blundo, A. Giorgio Gag-
gia, and D. R. Stinson.
On the dealer’s randomness
required in secret sharing
schemes. Lecture Notes
in Computer Science, 950:
35–46, 1995. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Bierbrauer:1996:OAR

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

**Berkovits:1998:AMA**


**Benantar:1996:ACS**


**Bosselaers:1996:FHP**


**Biget:1997:HSC**

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

Bosselaers:1997:SDP


Beaver:1993:CPP


Baker:1998:LTC


Beygelzimer:1999:OWF


Bhimani:1996:SCI


Boeleoni:1999:SBM

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


B. Brassard: 1998: QCH


B. Bertilsson: 1993: CPS


F. Bao: 1994: RAF


F. Bao: 1995: BFA


M. Breitbach: 1999: CCM


J. Bar-Ilan: 1989: NFC


J. Biermann: 1998: HKB

REFERENCES


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


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

Biham:1997:FSE


Biham:1999:CM

Eli Biham. Cryptanalysis of MAGENTA. In National Institute of Standards and Technology [Nat99b], page ?? ISBN ????

Biham:1999:CTM

Biham:1999:NCA


Birrell:1985:SCU


Biryukov:1995:CID


Birman:1998:ACH


Biryukov:1999:MC


Bishop:1988:AFDa


Bishop:1988:AFDb


Bishop:1988:AFDc


Bishop:COMPSYS-1-3-221

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


REFERENCES

0558/papers/1233/12330280.pdf.

**Book:1980:UDC**


**Bauspiess:1990:HKA**


**Blakley:1995:GPS**


**Blalkey:1994:LAA**


**Blakley:1995:DPC**


**Bocharova:1995:FEC**

**Buydos:1997:C**

**Biham:1998:CAXa**

**Biham:1998:CAXb**

**Biham:1998:TA**

**Biryukov:1998:DCC**

**Biryukov:1998:ICR**

**Buchholz:1998:TCF**
Thomas Buchholz and Martin Kutrib. On time computability of functions in one-way cellular automata.
REFERENCES


Bellare:1998:LBI [BKR98a] M. Bellare, T. Krovetz, and

Bellare:1998:LRB


Bakhmurov:1999:DEE


Burgett:1998:CLD


Boneh:1995:QCH


Boneh:1996:ABF


Boneh:1996:ABB


[Binsted:1999:CDS]


[Blatman:1975:MMC]


[Blakley:1979:SCK]


[Blahut:1983:TPE]


[Blakley:1985:ITF]


F. Blanchard. Certain sofic systems engendered

**Blaze:1993:TMS**


**Blaze:1994:KME**


**Blaze:1996:HBE**


**Blaze:1996:HEL**


**Blaze:1996:OKE**


**Blair:1998:SEP**

REFERENCES


Beth:1994:CCB


Baaz:1999:SDC


Brassil:1994:EMI


Brassil:1995:HID


Brickell:1983:EAA


Brickell:1984:EAA


REFERENCES


[Blu82] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random


Bellovin:1991:LKA


Brickell:1991:IID


Bellare:1992:HSG


Bleichenbacher:1994:DAG


Boyd:1994:DSK


Burns:1994:PSS

REFERENCES


REFERENCES


Blackburn:19xx:NPP

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

Bento:1995:RCI


Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD


Blackburn:1997:CNP


Beimel:1997:CTA

REFERENCES


REFERENCES

Barker:1998:TKL


Blake:1985:CLG


Boppana:1996:BCP


Busch:1999:GEI


Book:1985:SNP


Book:1985:SNS

REFERENCES


REFERENCES


Bolignano:1998:IPM


Bond:1947:FSC


Boneh:1998:DDP


Boneh:1998:DDH


Boneh:1999:TYA


Booth:1981:ASU

REFERENCES

[Bookstein:1996:RB]

[Borman:1993:RTAa]

[Borman:1993:RTAb]

[Borman:1993:RTAc]

[Borcherding:1995:NAR]

[Borcherding:1996:LAD]

[Bosworth:1982:CCC]

[Bosma:1990:PPC]
W. Bosma. *Primality Proving with Cyclotomy*. Doc-

**Bosxx**


**Bou85**


**Bou94**


**Bov98a**


**Bov98b**


**Bow59**


**Bow60a**

REFERENCES


REFERENCES

**Boyd:1992:FFA**


**Boyd:1995:CCC**


**Boyd:1995:CCI**


**Boyd:1997:DSP**


**Boyer:1998:DSM**


**Boyko:1999:SPO**


**Beker:1982:CSP**


REFERENCES


**Buchmann:1997:OWF**


**Bailey:1998:OEF**


**Barnett:1998:AOD**


**Barnett:1998:FML**


**Bassia:1998:RAW**


**Bella:1998:KVI**

REFERENCES

Bella:1998:MBK


Bleichenbacher:1999:SC


Blum:1999:MME


Birov:1999:PML


Blaze:1999:KNT


Bishr:1999:PRS


Blobel:1999:SAD

REFERENCES

Brown:1998:LA

Borst:1999:LCR

Beguin:1995:FSR

Beguin:1995:FSA

Blakley:1988:CBA

Beutelspacher:1991:EFS
REFERENCES

Bellare:1994:EAK


Bellare:1994:OAE


Bellare:1995:OAE


Bellare:1995:PSS


Baldwin:1996:RRR


Bellare:1996:TCA

<table>
<thead>
<tr>
<th>REFERENCES</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[Bra75b]</strong></td>
<td>D. K. Branstad. Encryption protection in computer data communications,. In ???, editor, <em>Fourth Data Communications Symposium</em>, 7–9 October 1975, Quebec City, Canada, page ?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1975.</td>
</tr>
</tbody>
</table>
Branstad:1979:VHD


Brassard:1981:TLT


Bracha:1987:ERR


Brassard:1987:IMC


Brassard:1988:MCT


Brassard:1989:CCb


Brassard:1989:CCa


Brand:1990:PNU

[Bra90a] Russell L. Brand. Problems with the normal use...


Brassard:1994:CCQ


Bray:1994:UA


Brackin:1995:DCP


Brassard:1995:CCB


Brands:1995:LEC


Brands:1995:RBS


Brackin:1996:DCP

S. H. Brackin. Deciding cryptographic protocol

**Brassard:1998:C**


**Breitrose:1997:ALD**


**Breitrose:1997:DEM**


**Brent:1999:CAP**


**Brickell:1985:BIK**

sored by the International Association for Cryptologic Research.

**Brickell:1986:CKC**


**Brickell:1988:CKC**


**Brickell:1990:SIS**


**Brickell:1990:SHI**


**Brickell:1992:ACC**


**Brickell:1993:ACC**

REFERENCES


Brickell:1998:C

Brown:1975:BL

Brownell:1981:ODN

Brooke:1986:BRB

Browne:1994:ECL

Brock:1996:CCP
REFERENCES

Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB


Brundrett:1998:KAW


Bentley:1999:SOE


Bryan:1967:CA


Brillhart:1967:SFR


Branstad:1982:ISS

REFERENCES


REFERENCES


REFERENCES


Bruckstein:1995:SSD


Brunnstein:1995:IPR


Biham:1997:DFA


Bramhill:1997:CCD


Boneh:1998:CSF


Baaleh:1999:AGA


Bellare:1999:NEE

[BS99b] M. Bellare and A. Sahai. Non-malleable encryption: Equivalence between two notions, and an

[Bellare:1999:NME]


[Barreiro:1997:PKC]


[Bakhtiari:1995:APL]


Ian F. Blake, G. Seroussi, and Nigel P. Smart. Elliptic

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


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

Buck:1982:PCS


Buchmann:1991:NTA


Buck:1991:MCT


Bucholtz:1995:EEC


Bucholtz:1995:SCS


Budge:1922:RS


Budge:1929:RSB


M. Burmester. Cryptanalysis of the Chang-Wu-Chen
key distribution system. 
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

**Burmester:1994:CCW**

Mike V. D. Burmester. Cryptanalysis of the Chang-Wu-Chen key distribution system. 

**Burmester:1994:ROD**


**Burmester:1996:HSS**

M. Burmester. Homomorphisms of secret sharing schemes: a tool for verifiable signature sharing. 

**Burke:1998:IHC**


**Burke:1998:LER**

Burke:1999:AAC


Busse:1996:UFE


Buss:1997:BAC


Brouwer:1982:NMK


Boneh:1996:HCM


Boneh:1997:RLC


Barros:1998:DWS

REFERENCES

Blunk:1998:RPE

Boneh:1998:BRM

Briguglio:1999:PGF

Beker:1985:KMS

Biehl:1997:TVC

Brandes:1998:UGL
U. Brandes and D. Wagner. Using graph lay-


[BY93a] M. Bellare and M. Yung. Certifying cryptographic
Cachin:1995:OSS


Cachin:1998:ITM


Cypher:1996:UAS


Caelli:1996:CKE


Caelli:1996:CPF


Cain:1996:TS


Calvocoressi:1980:TSU

REFERENCES


[Callimahos:1989:TAZ]


[Callimahos:1992:HC]


[Campanigne:1971:REC]


[Campbell:1987:MBC]


[Cammack:1988:MDE]


[Cao:1999:CAR]


[Capecchi:1994:TGR]

[Car93] C. Carlet. Partially-bent functions. Lecture Notes in Computer Science, 740:
Carlsen:1994:OPA


Caronni:1995:AOR


Carter:1997:BLC


Carter:1997:CCC


Carter:1998:CCC


Carasik:1999:USS

REFERENCES


Chun:1999:DMT


Chaum:1988:MUS


Canteaut:1999:NCA


Chen:1998:VIC


Carter:1995:DVD


Carlet:1998:CBF


Coppersmith:1985:AF


Chuang:1991:MER


Compton:1999:PTC


Cramer:1999:EMC


Cowie:1996:WWN


Congedo:1995:SRS


Callas:1998:ROM


Chang:1995:SCP

Capocelli:1991:SSS


Carter:1998:KSI


Canetti:1997:DE


Chen:1995:PDP


Cramer:1994:PPK


Chaum:1986:CRN

REFERENCES


[CF78] Chaum:1978:ICP


[CF95] Chaum:1978:ICP

[CF99] Chaum:1978:ICP


[Castelfranchi:1999:BMA] C. Castelfranchi and R. Falcone. Basic mental at-

**Chouinard:1996:ITA**


**Callas:1999:FUI**

REFERENCES


[CG75] Donald Coppersmith and Edna Grossman. Generators for
REFERENCES


**Chor:1985:RRL**

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

**[CG85]**


**[CG98]**

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

**[CG99]**


**Cover:1987:OPC**


**Chor:1988:UBS**


**Catalano:1998:NES**

**[CG98]**


**Canetti:1999:ETP**

Cranor:2005:SUD


Clark:1993:EMS


Canetti:1999:AST


Chen:1999:KEM


Chen:1997:AUM


Canetti:1999:AST
REFERENCES


REFERENCES


References

Notes in Computer Science, 1642:15–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


[Cha85b] CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

David Chaum. New secret codes can pre-


[Cha91] David Chaum, editor. Smart card 2000: selected papers from the Second
REFERENCES


REFERENCES

Chadwick:1999:IWS


Chan:1999:WES


Chau:1999:QCE


Chesson:1973:CC


Cheswick:1992:EBW

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

Canetti:1997:MAC


Chiope:1992:SBE


Chin:1999:HCD

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

Chin:1999:HDS


Christophides:1999:ODI


Canetti:1997:PSL


Chor:1986:TIP


Chung:1998:DWCb


Christiansen:1978:SL


Christoffersson:1988:MAE

Per Christoffersson. Message authentication and en-


Ciarcia:1986:BHD

Cao:1999:DTJ

Clark:1995:SRP

Chabaud:1998:DCS

Collins:1999:DCL

Coster:1992:ILD

Coppersmith:1995:TCB


[Chee:1991:CNP]
REFERENCES

link/service/series/0558/1
bibs/0576/05760204.htm;
http://link.springer-ny.com/link/service/series/1
0558/papers/0576/05760204.pdf.

[CK90]
bibs/0435/04350299.htm;
http://link.springer-ny.com/link/service/series/1
0558/papers/0435/04350299.pdf.

[CK93]

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


Chor:1998:PIR

Cox:1996:SRW

Cox:1996:SIY
Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure, imperceptible yet perceptually salient, spread spec-
REFERENCES


Cox:1996:SSS


Cox:1997:SSS


Caldwell:1999:DIF


Coradeschi:1999:IVD


Chan:1988:IEC


Chang:1997:PCM

REFERENCES


[C. S. K. Clapp. Joint hardware/software design of a fast stream cipher. Lecture]
REFERENCES

Clark:1998:TIT


Clarke:1998:BP


Clapp:1999:ILP


Clevenger:1996:DEU

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


Clinton:1997:AEC

Bill Clinton. Administration of export controls on encryption products: communication from the President.
REFERENCES

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.

[Cl99] 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.


[CM82] Constantino Ciampi and A. A. Martino, editors.
REFERENCES


Chan:1985:NMP

Cachin:1995:LIR

Cachin:1997:USA

Chang:1997:CAS
Cooperman:1997:SMD

Marc Cooperman and Scott A. Moskowitz. Stegano-
graphic method and de-
vice, March 18, 1997. URL
http://www.cl.cam.ac.
uk/˜fapp2/steganography/
bibliography/1047.html.
US Patent 5,613,004.

Cox:1997:RWI

Ingemar J. Cox and Matt L.
Miller. A review of wa-
termarking and the impor-
tance of perceptual model-
ing. In Rogowitz and Pap-
pas [RP97b], pages 92–99.
TS510.S63 v.3016. URL
http://www.cl.cam.ac.
uk/˜fapp2/steganography/
bibliography/1045.html.

Chen:1998:DRT

D. Chen and A. K. Mok. Design of a real-time SQL
engine in the distributed en-
vironment. Lecture Notes
in Computer Science, 1553:
27–38, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Camenisch:1999:SEG

J. Camenisch and M. Michels
Separability and efficiency
for generic group signa-
ture schemes. In Wiener
[Wie99], pages 413–430.
ISBN 3-540-66347-9. LCCN

Charlton:1999:DPM

P. Charlton and E. Mam-
dani. A developer's per-
spective on multi-agent sys-
tem design. Lecture Notes
in Computer Science, 1647:
41–51, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

Christianson:1999:DSCa

Bruce Christianson and
James A. Malcolm. Delega-
tion and not-so smart cards
(position paper). Lecture
Notes in Computer Science,
1550:154–157, 1999. CO-
DEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibs/1550/15500154.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1550/15500154.
pdf.

Coradeschi:1999:HMC

S. Coradeschi and D. Malec.
How to make a challenging
al course enjoyable using
the RoboCup soccer simula-
tion system. Lecture Notes
in Computer Science,
1604:120–??, 1999. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
REFERENCES

Chen:1998:SCC


Cohen:1993:AAA


Canetti:1999:ECS


Charnes:1997:SSH


Chor:1989:SCT

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


[Coron:1999:SRP] Jean-Sébastien Coron, David Naccache, and Julien P. Stern. On the secu-

Coupe:1999:ELA


Chao:1998:CSE


Coltell:1998:AOL


Cocks:1997:SKG


Cohen:1987:CCI


Cohen:1987:IIP

REFERENCES


[Col64] F. N. Colaço. A criptografia revelada, ou, Arte de traduzir e decifrar as escrituras obscuras, quase-quer que sejão os caracteres empregados. (Portuguese)


REFERENCES


Conklin:1998:SCO


Conklin:1999:ESC


Contini:1999:DPD


Coombs:1983:MC


Coppersmith:1984:FEL


Coppersmith:1987:C


Coppersmith:1989:AID

[D. Coppersmith. Analysis of ISO/CCITT document...
REFERENCES

[102x681]REFERENCES


Coppersmith:1994:DES


Coppersmith:1994:ACS


Coppersmith:1995:ACA


Coppersmith:1995:FSR


Coppersmith:1995:ACC

Don Coppersmith, editor. *Advances in cryptology,
REFERENCES


[Cop99] D. Coppersmith. Weakness in quaternion signatures. In


REFERENCES


REFERENCES

Chaum:1993:WDO

Chae:1994:AMA

Chen:1995:NGS

Chaum:1998:E

Chung:1998:DWCa

Charney:1997:PSC

Cheon:1998:TEA

Camenisch:1995:BSB
[CPS95] J. L. Camenisch, J.-M. Piv-
etante, and M. A. Stadler. Blind signatures based on
the discrete logarithm problem. *Lecture Notes in Com-
ISSN 0302-9743 (print), 1611-3349 (electronic).

**Chor:1985:KTP**

Benny Chor and Ronald L. Rivest. A knapsack type
public key cryptosystem based on arithmetic in
finite fields (preliminary draft). In Blakley and
ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43 no.196. URL
issn=????&volume=0&issue=0&page=54. See also re-
vised version in [CR88c].

**Carroll:1988:ACP**

John M. Carroll and Lynda Robbins. The automated
cryptanalysis of polyalphabetic ciphers. *Comput-
CPSEDU. ISSN 0167-4048 (print), 1872-6208 (elec-

**Carroll:1988:CC**

223, Department of Computer Science, University of
1070-0. 55 pp.

**Chor:1988:KTP**

Benny Chor and Ronald L. Rivest. A knapsack-type
public key cryptosystem based on arithmetic in finite
fields. *IEEE Transactions on Information Theory*, IT-
0018-9448 (print), 1557-9654 (electronic).

**Chaum:1991:USD**

David Chaum and Sandra Roijakkers. Uncondi-
tionally secure digital signatures. *Lecture Notes in Com-
ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/
link/service/series/0558/
bibs/0537/05370206.htm;
http://link.springer-ny.com/link/service/series/0558/
papers/0537/05370206.pdf.

**Caronni:1997:HEE**

Germano Caronni and Matt Robshaw. How exhaust-
ing is exhaustive search?


**Crawford:1992:ASA**


**Craig:1996:CDC**

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

**Craver:1997:PSP**


**Craver:1998:PKS**


**Cramer:1999:ISC**


**Crepeau:1990:VDS**


**Crepeau:1997:ECP**

REFERENCES


Contini:1999:IAS


Chaum:1983:ACP


Chaum:1998:Ca


Crypto:1981:ACP


CryptoBytes:1995:C


Cesarini:1983:ACC

REFERENCES

Chepyzhov:1991:FCA


Chabaud:1996:CSS


Chambers:1996:RLM


Cusick:1996:BNFb


Camenisch:1997:EGS


Chambers:1997:RLM


Chen:1997:NIC

REFERENCES

January 1997. CODEN CSSEEI. ISSN 0267-6192.

Coppersmith:1997:PAP


Canteaut:1998:COM


Cramer:1998:PPK


Coradeschi:1999:ASV


Chaum:1989:SCF


Csirmaz:1995:SSM


Coppersmith:1994:ABP

Don Coppersmith, Jacques Stern, and Serge Vaudenay. Attacks on the birational permutation signature schemes. Lecture

Chang:1997:GSS


Chen:1999:TPS


Collberg:1999:SWM


Currier:1998:MPT

Cusick:1995:CPK

Cusick:1996:BNF

Cusick:1997:CRN

Ciminiera:1989:AMM

Calvelli:1993:ARS

Chabaud:1995:LBD

Cohn:1999:MC

Chaum:1991:CSU
[CvHP91] David Chaum, Eugène van Heijst, and Birgit Pfitzmann. Cryptographically


Chin-Chen Chang and Tzong-Chen Wu. A smart card oriented password authentication scheme based

**Ceruzzi:1991:RGC**


**Coppersmith:1998:CT**


**Chang:1998:BSC**


**Craver:1998:TTL**


**Cao:1990:DKC**

Zhen Fu Cao and Bao Dong Zheng. A discussion on knapsack cryptosystems

DeMillo:1983:ACC


Dittmann:1998:MSW


Daemen:1999:RAI

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

**Dalton:1997:KSW**


**Damgaard:1990:ACE**


**Damgaard:1990:DPH**


**Damgaard:1991:ACE**


**Damgaard:1991:TPP**

REFERENCES

Damgard:1994:PPS

Damgaard:1994:PPS

Damgard:1998:E

Damgaard:1999:CSZ

Damgaard:1999:LDS

Dam:1996:RPG
Danisch:1995:RES


Danthine:1996:ECM


Dang:1997:AAC

Dang, Zhe. Automated analysis of cryptographic protocols using the ATSTARL model checker. Thesis (M.S.), University of California, Santa Barbara, Santa Barbara, CA, USA, 1997.

Darnell:1997:CCI


DRC:1985:AAN


Davida:1979:IHS


Davida:1981:CAR

Davida, George I. The case against restraints on non-governmental research in cryptography. Communications of the Association for Computing Machinery, 24(7):445–450, July 1981. CODEN CACMA2. ISSN
Davies:1985:MAA


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

Davies:1991:ACE


Davis:1994:RAC


Davis:1995:KPR


Davis:1996:CDP

Don Davis. Compliance defects in public key cryptography. In USENIX Association [USE96g], pages 171–178. URL http://www.usenix.org/publications/
REFERENCES

library/proceedings/sec96/davis.html.

**David:1998:WWI**


**Davies:1998:E**


**Davies:1998:NIH**


**Davies:1998:LCM**


**Dawson:1985:COL**


**Dawson:1993:CSG**


**Dawson:1996:CSR**

REFERENCES


REFERENCES


Daswani:1999:ECC


Boer:1991:ALT


Dobbertin:1996:RSV


DHalluin:1999:ASR


DeWin:1996:FSI


Daemen:1993:CSH

deJonge:1986:ASR

deJonge:1987:SVR

Daemen:1998:PCF

Daemen:1998:FHS

DeOca:1998:DRD
REFERENCES


Association for Cryptologic Research.

[Delaigle:1997:LCW]


[DDJStaff:1998:NVS]


[DDJ98a]

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.

[DDJ98b]

DDJ Staff. News and views: New trends in vaporware; distance ed might pay off; life in the fast lane; making friends in Washington; news on OpenGL 1.2; no discounts for schools; let’s do lunch; encryption export challenge?; Java fissures; searching for talent in...
REFERENCES

305

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


T. Denny, Bruce Dodson, Arjen K. Lenstra, and Mark S. Manasse. On the factorization of RSA-120. Lecture Notes in
REFERENCES


REFERENCES


[DQM98] V. Darmstaedter, J.-F. DeLaigle, J. J. Quisquater,


DeSantis:1998:E


DeSchutter:1998:TFA


DeSmit:1998:GAE


DeMoliner:1999:STB


Drossopoulou:1999:DSJ


Deavours:1987:CPI


Deavours:1988:BPS


Deavours:1998:A

REFERENCES

Kruh:1998:TBW


Demirdogen:1988:FDM


Demytko:1994:NEC


Denning:1979:SPC


Denning:1979:EOS


Denning:1982:CDS


Denning:1984:DSR


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


References


REFERENCES

Desmedt:1999:ES


Deugo:1997:CTS


Deugo:1998:SMS


Desmedt:1990:TC


Desmedt:1991:SGA


Domingo-Ferrer:1991:DU1


Domingo-Ferrer:1991:SRT

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

Dawid:1992:BSC

nications Conference. Conference Record, pages 484–488 (vol. 1). IEEE Com-
puter Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
USA, 1992. ISBN 0-7803-0608-2 (softbound), 0-7803-0609-0 (casebound),
catalog no. 92CH3130-2.

Desmedt:1993:PZS

Y. Desmedt and Y. Frankel. Perfect zero-knowledge shar-
ing schemes over any fi-
mite Abelian group. In R. Capocelli, A. De Santis, and U. Vaccaro, edi-
tors, Sequences II: Methods in Communication, Security, and Computer Science,

Domingo-Ferrer:1997:MAS

Josep Domingo-Ferrer. Multi-
application smart cards and encrypted data, processing. Future Generation
Computer Systems, 13(1): 65–74, June 20, 1997. CO-
DEN FGSEVI. ISSN 0167-
739X (print), 1872-7115 (electronic). URL http:
//www.elsevier.com/gej-
ging/10/19/19/28/17/21/abstract.html.

Domingo-Ferrer:1998:AFE

J. Domingo-Ferrer. Anony-
mous fingerprinting of elec-
tronic information with au-
1304, June 25, 1998. CO-
DEN ELLEAK. ISSN
0013-5194 (print), 1350-
911X (electronic). URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/073122.html.

Domingo-Ferrer:1999:AFB

J. Domingo-Ferrer. Anony-
mous fingerprinting based on committed oblivious transfer. Lecture Notes in
Computer Science, 1560:
43–52, 1999. CODEN
REFERENCES


REFERENCES


Daemen:1994:NAB


Daemen:1994:RWS


Daemen:1994:WKI


Daumen:1994:WC


Diffie:1976:NDC


Diffie:1976:PKC


Diffie:1977:ECN

REFERENCES

CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).


REFERENCES

Dhem:1998:DEP


Diffie:1980:CAM


Dechamboux:1996:ADS


Desmedt:1998:AOC


Desmedt:1998:CC


Dolev:1995:DFT


Damm:1995:MFH

Damm:1995:MH


DiGiorgio:1997:ISC


DiGiorgio:1997:JDJ


DiCrescenzo:1999:SAC


DiCrescenzo:1999:SPH


DiazdeLeon:1991:PIE


Ding:1996:CRT

REFERENCES


REFERENCES

0558/papers/0473/04730230.pdf.


Dodson:1995:NFL


Diffie:1998:PLP


Demphlous:1999:DPL


Davoine:1997:VCP

REFERENCES


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

**Dongarra:1995:TSS**


**Denazis:1999:DIO**


**D Angelo:1994:SEM**


**Dwork:1993:PPC**


**Dwork:1994:EEU**


**Dossis:1995:FSR**


**Dossis:1995:OVH**


**Ding:1997:TFS**


**Dittmann:1998:IWE**


**Desmedt:1986:CTA**


**DiCrescenzo:1999:CZK**


**Dobbertin:1995:EMC**

[H. Dobbertin. Extended MD4 compress is not collision-free. Unpublished abstract., October 1995.]

**Dobbertin:1995:ASA**

Dobbertin:1996:CM


Dobbertin:1996:SMA


Dobbertin:1997:RTC


Dobbertin:1998:FTR


Dobbertin:19xx:CM


DomingoiFerrer:1996:NPH


Donini:1998:CSR

[Don98] Luigi Donini. The cryptographic services of the Royal (British) and Italian navies: a comparative analysis of their activities during World War II. In Deavours et al. [DKK+98], pages
REFERENCES


DiCrescenzo:1999:COTb


Santis:1991:PRP


DiCrescenzo:1994:ROP


Damgaard:1996:NCU


Davida:1998:HC


Davida:1998:HSC

REFERENCES

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

DeWin:1998:ECP


Descombes:1999:MVK


DeWaleffe:1993:BLP


Delos:1994:IBS


Desmedt:1985:DOI

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


Daemen:1999:EBC


Drea:1999:NEB


Dray:1998:RNJ


Drach:1999:RDO


Dreher:1979:PSC


Drea:1992:MUC


deRaadt:1999:COO


[Dro89] Asael Dror. Secret codes (any good data security system must rely on encryp-


[DRR95] S. Dawson, C. R. Ramakrishnan, and I. V. Ramakrishnan. Design and imple-


[Davis:1990:WSK] Don Davis and Ralph Swick. Workstation services and Kerberos authen-

REFERENCES

1993. CODEN LNCS D9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


[DTS98] A. De Solages and J. Traore. An efficient fair off-line elec-

[DiGiorgio:1998:JDS]


[DT98b]

DiBoulay:1999:DDT


[DTDJ99]

duCarlet:1644:CCV


[du 44]

Dufner:1998:ACH


[Duf98]

Duhoux:1990:DBA


[Duh90]

Dumey:1994:CQD

REFERENCES


Johan Danielsson and Assar Westerlund. Heimdal — Kerberos 5 for the world (slides). In USENIX

Davida:1981:DES


[DWK81]

Dwork:1991:VSS


[Dwo91]

Dwork:1991:VSS


[Waleffe:1991:CSC]


[Dwo95]

REFERENCES


Dai:1996:CFA


DeSantis:1990:DPS


DeSantis:1991:CAN


DeSantis:1991:DPSb


Santis:1991:CAN

Alfredo De Santis and Moti Yung. Cryptographic applications of the non-interactive metaproof and

**DeSantis:1991:DPSa**


**Desmedt:1991:AUS**


**Dai:1998:WIF**


**Eberle:1993:HSI**


**ECMA:1996:EAP**


**Ellis:1975:PKC**


**Edwards:1915:CCT**

E. C. Edwards. Cipher
codes and their uses. *Scientific American*, 113(1):9, July 3, 1915. CO-
DEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic). URL http://www.nature.com/


English:1996:NSU


Ellison:1999:PSK


Ellison:2000:PSK


Ergun:1999:NLC


Estrella:1999:DED

REFERENCES


REFERENCES


ElGamal:1985:STA


Elkins:1996:RMS


Ellis:1999:PPN


Elvin:1987:CWW


Even:1993:CCS


Eades:1998:GDC

REFERENCES


REFERENCES


Ephron:1998:SC


Ephron:1998:SC

Etzel:1999:SHF


Etzel:1999:QHA


Etzel:1999:QHA

Eizenberg:1998:PSW


Eizenberg:1998:PSW

Er:1989:NAG


REFERENCES


Evertse:1991:WNR


Evertse:1993:WNR


Faak:1986:SVH


Faak:1987:CMM


Falk:1988:DST


Fancher:1996:SCa

REFERENCES


[FBS98] Jiri Fridrich, Arnold C. Baldoza, and Richard J. Simard. Robust digital watermarking based on key-dependent basis functions. Lecture Notes in
REFERENCES


Fenn:1996:MDD


Ferland:1994:PBC


Firoiu:1999:LER


FontdecabaBaig:1998:PNL


Fan:1999:DFS


Frankel:1992:PRT


Frankel:1993:NEH

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

Frankel:1993:NHG


Feak:1983:SIS


Feistel:1970:CCD


Feistel:1973:CCP


Feistel:1974:BCC


Feigenbaum:1991:ACC

REFERENCES


REFERENCES

Ferguson:1999:IDT

Friedman:1955:CLS

Feghhi:1999:DCA

Fung:1998:PAE
REFERENCES


REFERENCES

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

Frankel:1996:WCP

Frankel:1996:WBC

Friedman:1974:ETR

Franklin:1994:JEM

Franks:1997:REH

Fabrega:1999:SSP
REFERENCES

[Frederickson:1984:PRT]

[Frieze:1988:RTI]

[Fitzi:1998:TCP]

[Fiat:1990:BR]

[Fiat:1994:TT]

[Fiat:1997:BR]
service/journals/00145/tocs/01002.html.


Fischlin:1998:CLP


Fitzgerald:1989:QIP


Franz:1998:MMA


Franz:1996:CBS


Friedman:1996:AFR


Freeman:1997:MCN

Martin Freeman, Paul Jardetzky, and Harrick M. Vin, editors. *Multime-
REFERENCES

Fellowes:1993:KKI


Fellowes:1993:FPC


Fellowes:1994:CCG

Michael Fellows and Neal Koblitz. Combinatorial cryptosystems galore! In

Frankel:1998:BIW


Fumy:1993:PCK

Walter Fumy and Matthias Leclerc. Placement of cryp-

**Fried:1996:BHA**


**Fiadeiro:1999:ASC**


**Fox:1999:OCS**


**Flowers:1983:DC**


**Feiertag:1977:PMS**


**Flynn:1997:WYN**

REFERENCES

[Friedman:1976:ZTJ]

[Fortune:1985:PP]

[Feigenbaum:1991:DCC]

[Faihe:1998:ADR]

[Feustel:1998:DUI]

[Fairfield:1985:LRN]
R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart. An LSI ran-
REFERENCES


Fagundes:1999:EGA


Frey:1999:TPD


Frankel:1998:RED

REFERENCES


REFERENCES


[FP99] D. V. Finocchiaro and M. Pellegrini. On comput-


References


[Fre94] Lois A. Freund. The key escrow debate: issues and answers. Thesis (M.A.), Barry University, Mi-
REFERENCES


**Friedman:1935:ICA**


**Friedman:1935:MCP**


**Friedman:1935:PIS**


**Friedman:1939:CAC**


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

**Friedman:1939:MC**


**Friedman:1941:MCP**


**Friedman:1942:MC**


**Friedman:1956:CCC**

REFERENCES


REFERENCES


REFERENCES


[Fun78] Mark Robert Funk. A digital ultrasound system for data collection, imaging, and tissue signature analysis. Thesis (M.S.), Department of Electrical Engineering, Michigan State Uni-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


【Gal70】Joseph Stanislaus Galland. *An historical and analytical bibliography of the literature of cryptology*. Number 10 in Northwestern University studies in the humanities.
REFERENCES


Galil:1988:SIC


Galvin:1996:PKD


Galbraith:1999:CIB


Gamble:1988:IDL


Ganley:1993:CCI


Ganesan:1996:HUK


Ganesan:1996:YSS

Ravi Ganesan. The Yaksha security system. Communications of the As-
REFERENCES


Gardner:1977:MGN


Garlinski:1979:IEW


Garlinski:1980:EW


Garay:1994:RMA


Garfinkel:1995:PPG


Gardner:1996:PTT

REFERENCES

Garfinkel:1996:IKP


Garfinkel:1996:JSC


Garber:1997:NBAa


Garber:1997:NBB


Garber:1997:NBC


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."


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


REFERENCES

Goldreich:1997:EDE


Goldreich:1997:PKC


Gabber:1999:SPC


Goldreich:1985:CAR

REFERENCES

Goldreich:1986:HCR


Gabber:1997:HMP


Gittler:1995:DSS


Goldreich:1986:HCR


Gabber:1997:HMP


Gittler:1995:DSS

REFERENCES


Gibson:1991:EGC


Gibson:1995:SDG


Gibson:1996:SGP


Gifford:1981:CSI


Gilder:1997:APD


Giles:1998:EFS


Gilboa:1999:TPR


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).

** REFERENCES **

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>


REFERENCES


REFERENCES


Only the slides for the conference talk are available.


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


Shafi Goldwasser and Silvio Micali. Probabilistic


REFERENCES

Gennaro:1995:VSS


GomezdeSilvaGarza:1999:EAC


Grohe:1999:DDC


Galvin:1995:RSM


Griwodz:1998:PVE


Ghazi-Moghaddam:1994:OCH


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


ware based on the RE-
DOC III algorithm for high-
performance date ciphering. Lecture Notes in Computer


REFERENCES


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


REFERENCES

[406]

Gollmann:1992:ATC


Gollmann:1994:CCC


Goldreich:1995:FCF


Golic:1995:LCS


Golic:1995:FLO


Golic:1996:CEP


Gollmann:1996:CA


Gollmann:1996:FSE

REFERENCES

http://link.springer-ny.com/link/service/series/0558/tocs/t1039.htm;
http://www.springerlink.com/content/978-3-540-60865-3;

Goldreich:1997:FMCa


Goldreich:1997:FMCb


Goldwasser:1997:NDC


Golic:1997:CAA


Goldwasser:1998:C


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
Greg Goth. News briefs: Groups duel over new I/O standards; Oracle, Sun team up to dump the OS; bringing the net to mobile appliances; Irish girl invents new E-mail encryption; group releases draft biometric-API specs; Toshiba announces smallest memory chip. Computer, 32(3):18–20, March 1999. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://dlib.computer.org/co/books/co1999/pdf/r3018.pdf.

Guajardo:1997:EAE
REFERENCES


(Ghodosi:1998:SSM) H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini. Se-


REFERENCES


Guillou:1998:E


Guillou:1991:PTA

Louis C. Guillou, Jean-Jacques Quisquater, Mike Walker, Peter Landrock, and Caroline Shaer. Precautions taken against various potential attacks in ISO/IEC DIS 9796 «Digital Signature Scheme Giving Message Recovery».

Guillou:1998:PTA


Gray:1982:ICT

P. E. Gray. Information control I: Technology transfer at issue: The academic viewpoint: Educators believe efforts to limit transfer of knowledge at the university level are likely to weaken the U.S. lead in innovation. IEEE Spectrum, 19(5):64–68, May 1982. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).
Grantham:19xx:FPP


Goeker:1999:DUC


Grehan:1990:CDE


Greenfield:1994:DPP


Grossman:1974:GTR


Grover:1982:CP


Grosek:1994:RCR


[GS94a] Marc Girault and Jacques Stern. On the length of cryptographic hash-values used in identifica-
Gulliver:1994:ITA


Gritzalis:1997:CPO


Gong:1998:SSG


Gribomont:1999:SDU

E. Pascal Gribomont and N. Salloum. System description: Using OBDD’s for the validation of Skolem verification conditions. Lecture Notes in Computer Science, 1632:222–??, 1999. CODEN LNCSD9. ISSN 0302-9743


Grehan:1994:BCRa

Gotoh:1990:MRR

Guan:1987:CAP

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

Guarino:1999:RIC

Gudes:1980:DCB


REFERENCES

Gurnsey:1997:CT


Gustafson:1996:SAS


Gutmann:1996:SDD


Guthery:1998:SC


Gutmann:1998:SGP


Gutmann:1999:DCS


Guy:1976:HFN

R. K. Guy. How to factor
REFERENCES

a number. In Hartnell and Williams [HW76], pages 49–89.


Griffiths:1976:AMR


Goldberg:1996:RNB


George Gamow and Martynas Ycas. The cryptographical 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.


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

Gylden:1933:CCB


Gylden:1936:AMC


Gylden:1938:APV

[Gyl38] Yves Gylden. Analysis from the point of view of cryptanalysis of “cryptograph type C-36,” provided with six key wheels, 27 slide bars, the latter having movable projections, single or multiple. A. B. Teknik co., Stockholm, Sweden, 1938. 10 pp.

Gysin:1996:OKC


Garzon:1991:CGG


Haller:1994:RIA


Hendessi:1994:SAA


Hollaar:1996:LRD

REFERENCES

Heys:2000:SAC


Haddon:1984:BRS

Bruce K. Haddon. Book review of “Security, IFIP/
REFERENCES


Hagelin:1998:SHC


Hoffman:1994:CP


Hammer:1971:SSC


Hamelin:1980:CIT


Hamming:1986:CIT


Hamilton:19xx:PC

V. Hamilton. Personal communication. ????, 19xx.

Hansen:1994:MLD

Per Brinch Hansen. Multiple-length division revisited: a tour of the minefield. Software—Practice and Experience, 24(6):579–601, June 1994. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic). This paper derives an algorithm for division of long integers, and
implements it as a literate program, although without identifier cross-references. [Har90]

Hancock:1995:ECI


Hancock:1997:UCE


Hancock:1999:ECI


Hardjono:1990:RED


Harari:1991:CCS


Hart:1994:DSC


Harpes:1996:CIB

REFERENCES

pp. Published by Hartung-Gorre, Konstanz, Switzerland.


Farid G. Hatefi. Application of encryption/decryption in


[Hu:1995:YCE] Ping Hu and Bruce Christianson. Is your computing


[HD96a] J. He and E. Dawson. How to fairly reconstruct

**He:1996:NKE**


**He:1992:IKB**


**Huang:1998:FAI**


**Hedberg:1997:FIC**


**Hartung:1998:DWM**


**Heidel:1676:JTP**

Wolfgango Ernesto Heidel. *Johannis Trithemii primo Spanheimensis deinde Divi Jacobi Penopolitani abbatis Steganographia: quae hu-cus[que] a nemine intel lecta sed passim ut sup posititia, pernicos a, magica & necromantica rejecta, elusa, damnata & senten tiam inquisitionis passa, nunc tandem vindicata, reserata et illustrata ubi post vindicias Trithemii clarissime explicantur conjurationes spirituum ex Arabi cis, Hebraicis, Chaldaicis & Graecis spirituum nominibus juxta quosdam con globatae, aut secundum alios ex barbaris & nihil sign ificantibus verbis concinnatae: deinde solvantur & exhibentur artificia nova
REFERENCES

steganographica a Trithemio
in literis ad Arnoldum
Bostium & Polygraphia
promissa, in hunc diem
a nemine capta, sed pro
paradoxis & impossibilibus
habita & summe desider-
ata. Wornatiense, Mo-
guntiae. Sumptibus Joannis
Petri Zubrodt, 1676. 8 +
394 (or 396) + 4 pp. LCCN
Z103 .T84 1676. Includes
Heidel’s life of Trithemius
and his vindication of the
Steganographia.

[Hei96a] G. H. L. M. Heideman,
editor. 17th Symposium on
Information Theory in the
Benelux, Enschede, The
Netherlands, May, 1996.
Werkgemeenschap voor
Informatie- en Communica-
tietheorie, Enschede, The
Netherlands, 1996. ISBN
90-365-0812-6. LCCN
????.

[Hei96b] N. Heintze. Scalable
document fingerprinting.
In USENIX [USE96d], pages
LCCN HF5004 .U74 1996. URL
http://www.cl.cam.ac.uk/∼fapp2/steganography/
bibliography/054137.html

[M. E. Hellman. Statement
to participants at
NBS workshop on cryptog-
raphy in support of computer
security. Unpublished memo-
randum, ???. ???, September
21, 1976.

will be totally insecure within
ten years’. IEEE Spectrum,
16(7):32–40, July 1979. COD-
EN IEESAM. ISSN 0018-
9235 (print), 1939-9340
(electronic).

mathematics of public-key
cryptography. Scientific
American, 241(2):146–157
(Intl. ed. 130–139), August
1979. CODEN SCAMAC.
ISSN 0036-8733 (print),
1946-7087 (electronic).

cryptanalytic attack on “A
cryptosystem for multiple
communication” [Inform.
Process. Lett. 10(4–5), 5
July 1980, pp. 180–183]. In-
formation Processing Let-
ters, 12(4):182–183, August
13, 1981. CODEN IF-
PLAT. ISSN 0020-0190
(print), 1872-6119 (elec-
tronic). See [LM80, Mei81].

[Hel93] Gilbert Held. Top secret
data encryption techniques.

Helleseth:1994:ACE


Helleseth:1994:ACE


Helleseth:1998:E


Henry:1981:BJB


Henry:1982:FDA

REFERENCES


[Hardy85] John M. Hardy, Dorothy W. Fuller, Douglas R. Long, Jane C. Hartin, and Faye Davis. *Electronic cryptographic communications equipment specialist (AFSC 30650)*. Extension Course
Institute, Air University, Various pp., 1985.

**Housley:1999:RIX**


**Hartung:1996:DWR**


**Handschiuh:1997:CCS**


**Handschiuh:1997:CSE**


**Hartung:1997:CPV**


**Hartung:1997:WME**


**Hartung:1997:DWM**

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


Hofmann:1994:RQC

Hughes:1998:AJC

Husemann:1999:OTY

Hutton:1999:ASM

Harn:1989:PAU

Han:1993:TCC

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

Hochberger:1999:CDM


Harn:1993:OTP


Hirose:1997:CKD


Higenbottam:1973:CC


Highland:1983:BRCb


Highland:1987:CC


Highland:1987:DES


Highland:1987:HSY


Highland:1987:HEM


Highland:1988:RRC

[Highland:1988:RRC]

Highland:1988:TSC

[Highland:1988:TSC]

Highland:1988:TSV


Highland:1988:EAE


Highland:1988:SIT


Highland:1989:SDI


Highland:1997:HCV


Highland:1997:PRC


Hill:1929:CAA


Hill:1931:CCL

[Lester S. Hill. Concerning certain linear transformation apparatus of cryp-
REFERENCES


[**Hiltgen:1994:CRC**]


[**Hill:1997:MTY**]


[**Haastad:1999:PGO**]


[**Hirschfeld:1993:MER**]


[**Hirschfeld:1997:FCF**]

REFERENCES


Hillenbrand:1999:SDW


Hong:1997:IAU


Huehnlein:1998:CBN


Hauser:1996:RSP


Herlea:1999:SBR

D. E. Herlea, C. M. Jonker,

**Harn:1990:EPE**


**Halevi:1997:MSM**


**Hevia:1998:STD**


**Halevi:1999:PKC**


**Halfmann:1999:ESP**

REFERENCES

-Haynes:1999:VDS-


-Hevia:1999:STD-


-Hromkovic:1994:CDC-


-Harpes:1995:GLC-


-Hacher:1999:IFA-


-Hall:1999:CS-


-Haber:1995:HDD-


[Hwang:1999:CDC]


[Hwang:1995:TAN]


[Hwang:1996:SCW]


[Hughes:1996:QCU]


[Hohl:1993:SIH]


[Hunter:1983:ERA]


Hoyle:1998:SKE


Horster:1995:MRM


Horvath:1994:PPM

Hennicker:1994:BAF


Haastad:1998:SIR


Hasegawa:1998:PIE


Habutsu:1991:SKC


Hansmann:1999:SCA


Hawkes:1996:ALC


Hodges:1983:ATE

REFERENCES

Hodges:1997:ATHa


Hoffer:1955:MAC


Hoffman:1993:CC


Hofmeister:1999:ACA


Hogan:1988:PIS


Hollis:1987:TCA


Holloway:1991:RA


Honore:1919:STS

F. Honore. The secret telephone, are sound waves

<table>
<thead>
<tr>
<th>Author</th>
<th>Year</th>
<th>Title</th>
</tr>
</thead>
</table>


REFERENCES

Horan:1994:CSO


Horng:1995:PAU


Horng:1998:AAP


Horster:1999:SSK


Herzberg:1987:PPS


Hung:1994:FRD


Handschuh:1998:SCC


Horn:1998:APF

G. Horn and B. Preneel. Authentication and payment in future mobile systems. *Lecture Notes in Computer Science*, 1485:
REFERENCES


REFERENCES


REFERENCES


Hornauer:1994:MCA


Hauser:1996:MBI


Hinsley:1979:BISa


Heys:1995:ACS


Hada:1998:EZP


Hada:1999:RBO


Handschoh:1999:DOE


Huang:1988:APE

HUBER:1991:SCC


HUBER:1998:MAE


HULME:1898:CHP


HUNTER:1985:ARK


HURWICZ:1998:CTM

Michael Hurwicz. Cracker tracking: Tighter security with intrusion detection. BYTE Magazine, 23(5):
REFERENCES


Husain:1994:EI


Husemann:1999:SCD


Hulaas:1998:MLI


Hardy:1975:ITN


Hartnell:1976:PFM


Hardy:1979:ITN


Huthnance:1988:UPP

REFERENCES


REFERENCES


REFERENCES

Hirose:1998:ADH

Hsieh:1998:H

Hsieh:1999:OWH

Hardjono:1993:PDM

Ibbotson:1997:CPI

Anonymous:1993:CCA
IBM. Common Cryptographic Architecture: Cryptographic Application Programming Interface — Public Key Algorithm. IBM Corporation, San Jose, CA, USA, April 1993. ?? pp. IBM publication SC40-1676.

IBM:19xx:PSP
REFERENCES


IEEE:1983:PSS


IEEE:1984:ASF


IEEE:1985:FOC


IEEE:1986:CEC


IEEE:1986:ASF


IEEE:1987:ASF

REFERENCES


[IEEE:1992:CSF]


[IEEE:1992:PEA]


[IEEE:1992:PIC]


[IEEE:1992:PII]


[IEEE:1993:FIW]

REFERENCES


IEEE:1994:PIC


IEEE:1994:PSH


IEEE:1994:TAJ


IEEE:1995:PIC


IEEE:1995:PIS


IEEE:1995:PII

[IEE95c] IEEE, editor. *Proceedings: IEEE INFOCOM '95, the conference on computer communications: fourteenth annual Joint Conference of the IEEE Computer and Communic-

IEEE Order Plan Catalog Number 96TB100076.

IEEE:1996:PICa


IEEE:1996:SCR


IEEE:1996:ACS


IEEE:1997:ICD

IEEE:1997:IICb


IEEE:1997:ASF


IEEE:1997:IICa


REFERENCES


Igarashi:1999:ITP


Izu:1998:PSE


Israel:1983:AOS


Impagliazzo:1989:OWF

R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In IEEE
REFERENCES


[Int81a] International Data Corporation. *Data encryption. Research memorandum IDC #ISPS-M81-10*.

**Anonymous:** 1991: IIS


**IRD:** 1991: DFV


**Itoh:** 1994: LDS


**Impagliazzo:** 1989: LPC


**Ing:** 1999: SRT


**Imai:** 1993: ACA

REFERENCES


[IZ99] Hideki Imai and Yuliang Zheng, editors. Public key cryptography: second International Workshop on
REFERENCES


Jakobsen:1998:CBC


Jakobsen:1999:HOC


Jakobsson:1999:MCM


Jakobsson:1999:QCA


Jamieson:1998:UEP


Janke:1995:RSI


Janecek:1999:AVR


Jarecki:1996:PSS


[Jen99] F. V. Jensen. Gradient descent training of Bayesian networks. Lecture Notes in Computer Science, 1638:
Jenkins:19xx:IFC
Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Web site, 19xx. URL http://burtleburtle.net/bob/rand/isaacafa.html. ISAAC (Indirection, Shift, 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

Joux:1995:PAA

Jian:1999:SDM

Jolitz:1991:PUI

Jolitz:1995:RNS

Johnson:1998:ESS
N. F. Johnson and S. Jajodia. Exploring steganog-
Johnson:1998:CPE


Johnson:1998:SIC


Johansson:1999:FCA


Johansson:1999:IFC


Jakobsen:1997:IAB


Jun:1999:IRN

REFERENCES


metric encryption: Evolution and enhancements. 


_Jurisic:1997:ECC [JM97]_  

_Jakobsson:1999:IMI [JM99]_  

_Johnson:1994:CDM [JMLW94]_  

_Jackson:1994:MTS [JMO94]_  

_Jackson:1995:ESS [JMO95a]_  

_Jackson:1995:SMS [JMO95b]_  

_Jerichow:1998:RTM [JMP+98]_  
A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitz-

**Jakobsson:1996:DVP**


**Jarecki:1997:EMS**


**Joesang:1998:SMA**


**Johnson:1989:BDC**


**Johnson:1990:EDE**


**Johansson:1994:CPA**

Thomas Johansson. On the construction of perfect authentication codes that permit arbitration. *Lec-
REFERENCES


[Johnson:1995:ACD]


[Johnson:1996:LP]


[Johnson:1997:SP]


[Johnson:1997:SPS]

Alan Johnson. Steganography for DOS programmers — steganography is a branch of cryptography that deals with concealing messages. Dr. Dobb’s Journal of Software Tools, 22(1):48–??, January 1997. CODEN DDJOEB. ISSN 1044-789X.

[JohnByrne:1998:CEC]

REFERENCES

Johnson:1999:LES


Jolitz:1995:PB


Jones:1978:WWB


Jones:1978:MSW


Jones:1986:DEB

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

Jones:1990:PKC


Josse:1885:CSA


JCryptology:1988:JCJ

Juels:1996:HCC


Jaeger:1999:FCD


Joye:1997:PFR


Joye:1998:REC


Jurgensen:1996:TFC

REFERENCES


REFERENCES

**Jan:1997:SEV**


**Jan:1997:SIE**


**Juenemann:1981:DES**


**Juels:1999:TTS**


**Jung:1988:IRC**


**Jungnickel:1996:DFG**


**Jung:1999:EMA**


**Jurgen:1986:SEI**


**Jutla:1998:GBA**


**Just:1996:AMP**


**Jakubowski:1998:CSP**


**Jeanerod:1998:GEE**


**Jakobsson:1996:OAB**


**Ji:2001:CAF**

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

**Joye:1998:IBS**


**Kompella:1991:FCC**


**Kent:1998:RIA**


**Kentsoukos:1999:HCS**


**Kahn:1963:PNU**

David Kahn. *Plaintext in the new unabridged: an examination of the definitions on cryptology in Webster’s Third New Interna-
REFERENCES

Kahn:1966:MC

Kahn:1967:CSSa

Kahn:1967:CSSb

Kahn:1967:CSSb

Kahn:1979:CGP

Kahn:1982:GLC

Kahn:1983:KCS

Kahn:1984:COS

[Kahn:1991:SER]

[Kahn:1991:WWW]

[Kahn:1996:HS]

[Kahn:1996:CSS]

[Kahn:1998:EC]

[Kahn:1998:PHI]

[Kahn:1998:RMU]
REFERENCES

volume of selected papers
from issues of Cryptologia.


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

Kaliski:1991:MMD


Kaliski:1992:MAC


Kaliski:1993:SES


Kaliski:1993:ZBA


Kaliski:1995:MIA


Kaliski:1997:IPS


Kaliski:1997:PNG


Kaliski:1997:ACC

[Bal97c] Burton S. Kaliski, editor. *Advances in cryptology, CRYPTO ’97: 17th annual international cryptol-

Kaliski:1998:C


Kaliski:1998:RPCb


Kaliski:1998:RPRa


Kaliski:1998:RPCc


Kaliski:1998:EDF


Kaliski:1998:RPCa

rfc/rfc2315.txt. Status: INFORMATIONAL.

Kaliski:1998:REC


Kaliski:1999:ESP


Kaneshige:1996:ITC


Kaps:1998:HSF


Karger:1985:ADA


Karger:1986:ADA


Karger:1987:LDP

REFERENCES


Kari:1989:CBP


Kari:1989:OCP


Karkare:1996:SEA


Kasiski:1863:GDG

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

Kastenholz:1996:RVP


Kalipha:1990:NPK


Katzan:1977:SDE

Katsikas:1997:CMS


Kaufman:1993:RDD


Kaufman:1996:DWC


Kawai:1987:LAI


Kay:1995:CTE


Krishnakumar:1992:HTE


Krawczyk:1996:HKM


Krawczyk:1997:RHK

[H. Krawczyk, M. Bellare, and R. Canetti. RFC 2104: HMAC: Keyed-hashing for...
REFERENCES


[KD78] John B. Kam and George I. Davida. A structured design of substitution-permutation encryption network. In
REFERENCES

*Kam:1979:SDS*


*Khinchin:1997:CF*


*Keating:1999:PAA*

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

*Kelsey:1999:KSWb*

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

*Kemmerer:1989:AEP*

Kemppainen:1999:DMM


Kent:1993:IPE


Kent:1995:PCW


Kesdogan:1996:LMS


Kit:1993:DDI

Fung Ka Kit and Athula Ginige, editors. DICTA-93: digital image computing: techniques and appli-
Klapper:1995:CBA


Katsikas:1996:ISS


Kravitz:1999:CAC


Kundur:1997:RD1


Kundur:1998:DWU


Kunkelmann:1998:VEB

Kharitonov:1993:CHD


Karaorman:1999:CRJ


Kobara:1996:LVS


Karaorman:1999:CRJ


Kobara:1999:DPL


Kiefer:1998:WMV


Kilian:1988:FCO

Joe Kilian. Founding cryptography on oblivious trans-
REFERENCES

Kim:1993:CLB

Kim:1997:VBG

Kirby:1995:RPK

Kak:1977:SEU

Kocher:1999:DPA
Kurosawa:1995:NBA

Kuwakado:1996:NRT

Kelm:1997:NK

Kunihiro:1998:ECN

Kommerling:1999:DPT

Koren:1999:ISC
REFERENCES

Number PR00116. IEEE Order Plan Catalog Number 99CB36336.

Koshelev:1999:EAM


Kurosawa:1991:GPK


Kabatianskii:1997:DSS


Kramer:1999:FCD


Kothari:1984:CMW


Kilian:1994:FKE

REFERENCES

Kilian:1995:FCR


Knudsen:1995:NAA


Klein:1990:FCS


Kannan:1988:PFN


Klupsch:1999:ARR


Kurosawa:1988:CSP


Kurak:1992:CNI

REFERENCES

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

Kang:1993:PRR


Kim:1996:ACA


Kosuda:1997:SED


Kaksonen:1998:OMC

R. Kaksonen and P. Macihoenen. Object modeling of cryptographic algorithms

Knudsen:1996:IDA


**Kaufman:1998:DWF**


**Knudsen:1998:SMD**


**Kasahara:1999:NPK**


**Knudsen:1999:CIS**


**Kohlas:1999:RAP**


**Koscielny:1999:QBP**


**Kanda:1998:ECC**

REFERENCES

http://csrc.nist.gov/encryption/aes/round1/conf1/e2-slides.pdf. Only the slides for the conference talk are available.

Kobayashi:1999:FEC


Konheim:1980:ICP


Koyama:1991:NPK


Kande:1999:AUD


Karn:1995:REC


Karn:1995:RET

REFERENCES


REFERENCES

Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb


Knudsen:1993:ICS


Knudsen:1993:CLc


Knudsen:1994:PSF


Knudsen:1994:BCA


Knudsen:1995:NPW


Knudsen:1998:BCS


Knudsen:1998:DBC


Knudsen:1998:STA


Knudsen:1999:CBC


Knudsen:1999:FSE


Kurosawa:1995:CIS


Kurosawa:1995:CBA


Koblitz:1994:CNT


Koblitz:1996:ACC


Kobayashi:1997:DWH


Koblitz:1998:C


Koblitz:1998:AAC

Koblitz:1998:ECI

Kobara:1999:PMA

Kochanski:1989:HSI

Koc:1994:HSR

Kocher:1995:CDR
REFERENCES

Computer Society Technical Committee on Security and Privacy.

Koc:1996:RHI


Kocher:1996:TAI


Kocher:1999:B


Koeune:1999:CRI


Kohl:1990:UEK


Kolata:1977:NCC

REFERENCES


[Koo86] Raymond F. Koopman. The orders of equidistribution of subsequences of some
REFERENCES


Kurosawa:1995:TIK


Kurosawa:1995:CIT


Koops:1997:CRE


Kopooshian:1997:DCE


Kornerup:1993:HRM


Korner:1996:PC


Kurosawa:1995:LEAa


Kurosawa:1995:LEAb


Koyama:1982:CUM


Koyama:1982:MKR


Koyama:1983:MKR


Koyama:1995:FRT

Kozaczuk:1984:EHGa


Kozaczuk:1984:EHGb


Kozen:1996:RSS


Kim:1989:PRP


Kwan:1993:GPT


Krajicek:1995:SCC

REFERENCES

Knudsen:1996:HFB


Knudsen:1996:DSK


Knudsen:1997:FSH


Kilian:1998:IE


Kaps:1999:FIF


Koc:1999:CHE


Knudsen:1999:DFC


Kolliopoulos:1999:NLT


Krause:1984:DEI


Kranakis:1986:PC


Krawczyk:1990:HPC


Krawitz:1993:DSA


Krawczyk:1994:SSM

REFERENCES

Krawczyk:1994:LBH


Krawczyk:1995:NHF


Krawczyk:1998:ACC


Kesdogan:1998:DTP

REFERENCES

ac.uk/~fapp2/steganography/
bibliography/073140.html.

Knudsen:1998:DSR


Kumar:1999:CCB


Kruh:1998:WWS

com/open/cbbooks/089/0890068623.shtml. Third volume of selected papers from issues of Cryptologia.

Knudsen:1999:TDS


Kordes:1989:UMC


Kelsey:1997:CPO


Kurosawa:1997:DSP

[KS97b] Kaoru Kurosawa and Takashi Satoh. Design of SAC/PC(l) of order k Boolean

Kwon:1997:SEA


Kaliski:1998:RPRb


Kelsey:1998:SPP


Kinoshita:1998:GST


Kipnis:1998:COV

[Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil and vinegar signature scheme. Lecture Notes

REFERENCES

**Kelsey:1999:AST**


**Kipnis:1999:CHP**


**Kemp:1996:CPC**


**Kipnis:1999:CHP**


**Kemp:1997:MFC**


**Kelsey:1999:NDA**

J. Kelsey, B. Schneier, and N. Ferguson. Notes on the design and analysis of the Yarrow cryptographic

Kelsey:2000:YND


Kelsey:1997:SAL


Kelsey:1998:SAL


Kim:1996:EIE


Kehne:1992:NBP


Knowles:1992:AFC


Kelsey:1996:KC1

REFERENCES


Kelsey:1999:MCAb


Kelsey:1998:SCCa


Kelsey:1998:SCCb


Kelsey:1998:SCCc


Kelsey:1998:CAP


Korzhik:1991:CMPP

Valery I. Korzhik and Andrei I. Turkin. Cryptanalysis of McEliece's publickey cryptosystem. Lecture Notes in Computer Science, 547:68–??, 1991. CODEN LNCSD9. ISSN 0302-
Koyama:1991:NPC


Koyama:1993:SEC


Keefe:1996:MTS


IEEE Computer Society Press Order Number PR07629.

IEEE Order Plan Catalog Number 96TB100076.

Koyama:1998:AFC


Kim:1999:AFC

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

Kanda:1999:SCF

Masayuki Kanda, Youichi Takashima, Tsutomu Matsumoto, Kazumaro Aoki, and Kazuo Ohta. A strategy for constructing fast

Kuchlin:1987:PKE


Kucera:1992:GES


Kuhn:1998:CIS


Kuijk:1991:RSE


Kukorelly:1999:VCH


Kullback:1935:SMC


Kullback:1938:SMC

Solomon Kullback. *Statistical methods in cryptanalysis*. War Department, Office

**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


REFERENCES

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

Kwok-Yan:1992:FAA

Kasami:1982:KMS

Lampson:1991:ADS

Koch:1995:TRH

Koch:1992:ADS

Levien:1998:ART

Lampson:1992:ADS

Lacy:1993:CCS
John B. Lacy. CryptoLib: Cryptography in software. In USENIX Association [USE93], pages 1–


REFERENCES


[Langford:1995:DCT]

[Las85] Teresa A. Lassek. *Cryptography and the computer age*. Thesis (Honors), University of Nebraska at Omaha, Omaha, NE, USA, 1985. 58 pp.

[Lassek:1985:CCA]


[Lassak:1992:SRP]


[Landrock:1999:PTU]


[Lassak:1992:SRP]


[Langford:1996:WST]


[Lange:1997:SCI]


References


REFERENCES


[Lomas:1995:RBH]


[Lee:1996:IAP]


[Lee:1997:AES]


[Lou:1997:PTL]


[Lou:1998:FMM]
REFERENCES


REFERENCES


REFERENCES

Lennon:1978:CAI


Lenstra:1987:FIE


Lenstra:1990:PT


Lenstra:1996:GSD


Lenstra:1996:VNS


Lenstra:1998:GRM


Lenstra:1999:EIB


Lenzerini:1999:DLT

M. Lenzerini. Description logics and their relation-

**Lercier:1997:FGR**


**Levine:1958:VMS**


**Levine:1961:SAH**


**Levine:1961:SECa**


**Levine:1961:SECb**


**Levine:1983:USC**


**Levin:1985:OWF**


**Levine:1991:USC**

REFERENCES


http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/034404.html


REFERENCES


Linn:1988:RPE


Linn:1989:RPE

[RFC1040]


[RFC1113]


REFERENCES

Linnartz:1998:TCC

Lippit:1993:PIC

Lipton:1994:CNF

Abeles:1998:KVC

Lipmaa:1999:ICM

Litant:1987:BRC

Lindsay:1997:BC
REFERENCES

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.

[LKB+94]


[LKD98]


[LK96] Laih:1996:CEE

[LK99] Lee:1999:MRF

[LK94] Landau:1994:CPP


[LKD98] Linnartz:1998:MFA

REFERENCES


REFERENCES


Lin:1998:CDE


Lim:1999:SPK


Lec:1997:PNB


Lin:1999:NAD


Langelaar:1998:RSS

REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073147.html
Four volumes.


[Bibliography: p.158.]

[Luccio:1980:CMC]
REFERENCES


REFERENCES

Lagarias:1985:SLD


LaMacchia:1991:CDL


LaMacchia:1991:SLS


Lomet:1983:HPU


Lomas:1994:ENT


Lomas:1997:SPI

Mark Lomas, editor. *Security protocols: international workshop: Cam-
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. *BYTE Magazine*, 22(11):121–??, November 1997. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Loshin:1998:PEC


Lowe:1995:ANS


Lowe:1996:BFN


Loxton:1990:NTC

REFERENCES


Lam:1999:ACA


[LOX99]

Luciano:1987:CCC


[LP87]

Leszczynski:1994:SDA


[LP94]

Li:1999:CKA


[LP99]


Lcan lun Pandita Nag-dban-blo-bstan-pa’i-rgyal mtshan. Rgya dkar nag rgya ser Kasmira Bal Bod Hor gyi yi ge dan dpe ris rnam gran man ba: graphic tables of Indic and


REFERENCES

Lasker:1998:ACC
G. E. (George Eric) Lasker and Timothy K. Shih, editors. Advances in computer cybernetics; multimedia computing and networking, multimedia presentation, interactive multimedia support systems, multiuser virtual worlds, platform architecture for multimedia tools, management schemes for collaborative computing, program transformation systems, cryptanalysis and cryptosystems, graph transformation framework, simulation based design and development, design and implementation of programming languages, object systems design, abstracting devices. International Institute for Advanced Studies in Systems Research and Cybernetics, Windsor, ON, Canada, 1998. ISBN 0-921836-54-6. LCCN ????

Lamy:1998:CBB

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

Livens:1995:CCI
REFERENCES


**Lu:1979:EGC**


**Lu:1980:AEG**


**Lackey:1995:SMS**


**Luby:1996:PCA**


**Lucks:1995:HEI**


**Lucks:1996:FLC**


**Lucks:1996:FLR**

REFERENCES

Lucks:1997:SRK


Lucks:1998:SBB


Lucks:1998:OKE


Lucks:1998:ATE


Lucks:1999:SBB


Lucks:1999:SBC


Lucks:1999:ARK

Ludwig:1997:CQA


Lujan:1998:AMDa


Lujan:1998:AMDb


Lutz:1998:NBM


Linnartz:1998:ASA


Langelaar:1996:CPM

G. C. Langelaar, J. C. A. van der Lubbe, and J. Biemond. Copy protection for multimedia data based on labeling techniques. In Hei-
REFERENCES

580

deman [Hei96a], pages 33–40. ISBN 90-365-0812-6. LCCN ??? URL

Langelaar:1997:RLM


Long:1988:DLH


Li:1991:JAE


Lervik:1996:IDS


Lucks:1999:RKE


Lin:1996:GTU

REFERENCES


[Ma79] Robert Ma. Review and analysis of the Data Encryption Standard. Master of science, plan ii., De-
REFERENCES

582

partment of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA, 1979. 70 pp.

Meijer:1981:DSS

MacPherson:1987:CUN

MacLaren:1994:CPN

Mache:1998:SCT

Madsen:1992:GCD

Madsen:1996:CCL

Madsen:1997:KEE


M. Manasse. The Milli- lenc protocols for electronic commerce. ????
REFERENCES


REFERENCES


REFERENCES

Matsui:1991:KHC


Matsui:1993:LCM


Matsui:1994:FEC


Matsui:1994:LCM


Matsui:1995:CBO


Matsui:1996:NSB


Matthews:1996:SRN

REFERENCES

Matsui:1997:NBE

Matsumoto:1998:HCC

Matsumura:1999:DTE

Mauborgne:1914:APC

Maurer:1990:FGS

Maurer:1991:NAD

Maurer:1991:DSS
Ueli M. Maurer. A digital signature scheme and a public-key cryptosystem based on elliptic curves over $\mathbb{Z}_n$. DIMACS technical report 91-39, DIMACS, Center for Discrete
mathematics and theoretical computer science, rutgers, nj, usa, may 1991. 11 pp.

Maurer:1991:PCS

Maurer:1993:RIT

Maurer:1994:TEB

Maurer:1996:UGT


U. M. Maurer. A unified and generalized treatment

**Maurer:1996:ACE**


**Maurer:1997:ITS**


**Mauriello:1997:TTC**


**Mauth:1997:SOC**

REFERENCES


**Maurer:1998:E**


**Maurer:1999:IC**


**Maurer:1999:ITC**


**Maxemchuk:1994:EDD**


**May:1997:CDS**


**Milner-Barry:1986:ADL**

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

**Mao:1994:SAP**


**Massey:1994:CCT**


Mehrotra:1999:NOA

Mitra:1999:DCT

Mintzer:1998:OWS

Murphy:1997:ROD

Mintzer:1997:EIDb
Three volumes. IEEE Computer Society order number PR08183. IEEE order plan catalog number 97CB36144. 


McCane:1998:ICS

Millan:1998:HDC

Millan:1999:BFD

McHugh:1992:EBD

McIvor:1985:SC

McKee:1999:SFF

McLaughlin:1992:YAM


Meierhofer:1996:PGP


Meijer:1996:GFC


Meinel:1998:HHB


Mendelsohn:1989:CWI


Mendez:1991:AKA


Menezes:1993:ECP

Communications and Information Theory.

Menezes:1995:ECC


Menicocci:1995:SAC


Mersenne:1644:CPM

[Mer44] Marin Mersenne. *Cogitata Physica-Mathematica ... [Tractatus de mensuris ponderibus atque nummis ... Hydraulica pneumatica; arsque navigandi. Harmonia theoretica, practica. Et Mechanica phaenomena. Ballistica et acontismologia]*. Antonii Bertier, Paris, France, April 1, 1644. [30], 40 [24], 41–370, [16], 96, [8], 138, [34] + 40 [Mer78] pp. URL http://www.mersenne.org/prime.htm; http://www.mersenne.org/status.htm. Three volumes. This is the book that introduced the conjecture that numbers of the form $M(n) = 2^n - 1$ are prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, 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 $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is $M(13466917)$, a number containing $4,053,946$ digits.

Merkle:1978:SCI

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


Merkle:1991:FSE


Merrill:1997:ARD


Mercuri:1993:IRC


Meyer:1973:DCC


Meyer:1996:RPE


Meyer:1996:PMT


REFERENCES


[MHPS96] I. Majzik, W. Hohl, A. Pataricza, and V. Sieh. Multiprocessor checking using

**Matsumoto:1988:PQP**


**Matsumoto:1990:EAC**


**Michener:1988:TSK**


**Matsumoto:1993:FPC**


**Matsumoto:1993:FPK**

Micciancio:1997:ODS


Mihailescu:1994:FGP


Millikin:1943:ECCa


Millikin:1943:ECCb


Millikin:1943:ECCc


Miller:1976:RHT

REFERENCES

Miller:1985:PES


Miller:1986:UEC


Miller:1995:HWK


Millan:1996:LOA


Mills:1987:RDP


Millikin:1992:ECC

REFERENCES

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


[Matsumoto:1993:VIA]

[Mintzer:1997:EIDa]

[Misarsky:1997:MAU]

[Misarsky:1998:HDR]


C. Mitchell. Multi-destination secure electronic mail. The Com-
Mitchell:1992:AMI


Mitchell:1992:CCI


Miyaguchi:1990:FCC


Miyaguchi:1991:FCF


Miyaji:1993:ECS


Miyaji:1993:OEC

Atsuko Miyaji. On ordinary elliptic curve cryp-
Miyano:1993:MEN


Miyaji:1996:MRS


Miyaji:1999:ECC


Mjolsnes:1993:PCP


Morii:1992:PSP


Moskowitz:1994:CCH


Mazieres:1999:SKM

REFERENCES

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

Maibaum:1999:SRS

T. S. E. Maibaum, P. Kan, and K. Lano. Systematis-
ing reactive system design. Lecture Notes in Computer
Science, 1548:17–22, 1999. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic).

Miyazaki:1999:TFI

Shingo Miyazaki, Ikuko Kuroda, and Kouichi Saku-
rai. Toward fair international key escrow — an attempt by dis-
tributed trusted third agencies with threshold crypt-
tography. Lecture Notes in Computer Science, 1560:
171–187, 1999. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic). URL
http://link.springer-ny.com/
link/service/series/0558/
bibs/1560/15600171.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1560/15600171.
df.

Monge:1967:NMC

Alf Monge and O. G. Lands-
verk. Norse medieval cryp-
tography in runic carvings.
Norseman Press, Glendale,
LCCN E105 .M65. Includes
bibliographies.

Maulucci:1987:HAC

Ruth A. Maulucci and
J. A. N. Lee. Happen-
ings: The 25th Annivers-
sary of Committee X3;
The Code-Breaking Com-
puters of 1944. Annals
of the History of Compu-
ting, 9(3/4):345–356, July/
September 1987. CODEN
AHCOE5. ISSN 0164-
1239. URL http://dlib.
computer.org/an/books/
an1987/pdf/a3345.pdf;
http://www.computer.
org/annals/an1987/a3345abs.
htm.

Mao:1998:CPO

Wenbo Mao and Chae Hoon
Lim. Cryptanalysis in prime
order subgroups of $\mathbb{Z}_n^*$. Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Matyas:1991:KSB

S. M. Matyas, A. V. Le, and
D. G. Abraham. A key-
management scheme based on
control vectors. IBM
Systems Journal, 30(2):
175–191, 1991. CODEN
IBMSA7. ISSN 0018-8670.

Muffett:1995:BPK

A. Muffett, P. Leyland,
A. Lenstra, and J. Gillo-
gly. The BlackNet 384-bit
PGP key has been BRO-
KEN. Message posted to

Matyas:1978:GDI


Meyer:1982:CND


Moler:1983:SVA


Meadows:1987:MSA


Magliveras:1990:LCP


Magliveras:1990:PCP


Moskovitz:1992:CCC

REFERENCES

Moskowitz:1992:IDI


Meadows:1996:CCC


Meyer:1996:PKC


Mueller:1998:SPK


Moldovyan:1995:FSE

REFERENCES


REFERENCES


Matsumoto:1982:DTL

Tsutomu Matsumoto, Tomoko Okada, and Hideki Imai.

Mok:1997:KNF


Moldovyan:1998:NEP


Morita:1991:SCT

Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi.

Montgomery:1985:MMT


Monagan:1993:GPD


Montagu:1996:MWN


Moore:1992:PFC


Morland:1666:NMC

Morrice:1692:EB

Morrison:1983:SEA

Morain:1988:IGP

Mora:1989:AAA

Morris:1992:FMC
REFERENCES


[MP86] Howard Mevis and Janet Plant. *Satellite communications: a practical guide to satellite TV encryption with tips on installing decoders, solving reception

McInnes:1991:IPK


Milidiu:1999:EIW


Mayerwieser:1995:THS


Moller:1994:RSW


Mori:2002:CSD


Morillo:1999:WTS

REFERENCES


[Mra95]

[MR95a]

[MRS7]

[MR95b]

[MRS87]

[MR98]

[MRS99]

[MR98]
S. Maitra, B. K. Roy, and P. Sarkar. Ciphertext only attack on LFSR based en-

**Mitchell:1989:RHF**


**Macalister:1976:SLI**


**McEliece:1981:SSR**


**Muller-Schloer:1983:MBC**


**Moore:1987:CSK**


**Meier:1990:NCC**

REFERENCES

Montgomery:1990:FEP

Meier:1991:CPC

Massey:1994:FTA

Meier:1995:SG

Meier:1995:SSG

Metzger:1995:RIAa


Metzger:1995:RIAb


Micali:1995:SMG


Mambo:1998:NCB


Michels:1998:GCS

REFERENCES

MacKenzie:1999:AIH


Maitra:1999:HNR


Miyazaki:1999:KGD


McLeod:1990:VLD


Miksch:1999:ASQ

S. Miksch, A. Seyfang, W. Horn, and C. Popow. Abstracting steady qualitative descriptions over time from noisy, high-frequency data. Lecture Notes in Computer Science, 1620:281–??, 1999. CODEN LNCS.D9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moriai:1998:HOD


McClure:1999:HEN

REFERENCES


[Mambo:1996:HUT]


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

Michels:1998:SSV


Meyer:1972:PCC


Mullender:1986:DCD


Matsui:1994:VSH

REFERENCES


Mackinnon:1985:OAA

Moriya:1997:DWS

Molva:1992:KAK

Mu:1992:ICS

Mueller:1999:SRB

Muftic:1988:SMC

Muftic:1993:SAO
REFERENCES

Mulherin:1981:FDE


Mullin:1984:NMP


Mulligan:1989:UMA


Mullin:1989:LEN


Muller:1999:SRB


Mund:1991:ZCP


Mund:1991:ZLC

[Mun91b] Sibylle Mund. Ziv–Lempel complexity for periodic sequences and its crypto-

Muraszko:1987:CVR


Murphy:1996:CC


Murphy:1999:OST


Musser:1992:UVE


Maruyama:1998:TGH


Menezes:1990:IEC

REFERENCES


[Mv93] Volker Müller, Scott Vanstone, and Robert Zuc-

Manber:1994:AAM


Maurer:1996:TCW


Maurer:1996:DHO


Maurer:1997:PAS


MacNish:1998:BRD

C. K. MacNish and M.-A. Williams. From belief revision to design revision: Applying theory change to

**Memon:1998:PDM**


**Merkle:1998:SSR**


**Merkle:1998:SSA**


**Maurer:1999:RBB**


**Malkin:1999:ESG**


**Mitchell:1994:CPA**

Chris Mitchell, Michael Walker, and Peter Wild. The combinatorics of per-
fect authentication schemes.
SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

**Maurer:1991:NIP**

Ueli M. Maurer and Yaacov Yacobi. Non-interactive public-key cryptography.
*Lecture Notes in Computer Science*, 547:498–??, 1991. CODEN LNCS09. ISSN
0302-9743 (print), 1611-3349 (electronic). URL http://link.springer
ny.com/link/service/series/0558/bibs/0547/05470498.htm;

**Matsui:1993:NMK**

*Lecture Notes in Computer Science*, 658:81–??, 1993. CODEN LNCS09. ISSN
0302-9743 (print), 1611-3349 (electronic).

**Maurer:1993:RNI**

Ueli M. Maurer and Yaacov Yacobi. A remark on a non-interactive public-key distribution system.
*Lecture Notes in Computer Science*, 658:458–??, 1993. CODEN LNCS09. ISSN
link/service/series/0558/bibs/0658/06580458.htm;

**Mayers:1998:QCI**

D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In IEEE [IEE98a],
pages 503–509. CODEN ASFPDV. ISBN 0-8186-9172-7 (softbound), 0-7803-
5229-7 (casebound), 0-8186-9174-3 (microfiche). ISSN 0272-5428. LCCN
number PR9172.

**Myers:1994:RIA**


**Myers:1994:RPA**

REFERENCES


Myers:1996:TAS


Myers:1997:RSA


Myer:1998:VCS


McCurlie:1998:ACE


Mihaljevic:1998:CAB


Merwin:1979:NCC

Richard E. Merwin, Jacqueline T. Zanca, and Mer-
REFERENCES


John Leonard Nanovic. Secret writing: an introduction to cryptograms, ciphers


NIST:1991:DSS


NIST:1992:DSS


NIST:1992:PYA


NIST:1993:FDP


Anonymous:1993:FPD


NIST:1993:DES


NIST:1994:FPD


National Institute of Standards and Technology, editor. The First Advanced
REFERENCES


[Nat99a]

[Nat99c]

[Natxx]
REFERENCES

Nechvatal:1999:SRF

NBS:1975:EAC

NBS:1975:NPF

NBS:1976:NWC

Nilsson:1978:OST

Nandi:1997:RCT

Neat:1975:NCC
Angeles, CA, USA, 1975. xxi + 203 pp.


REFERENCES

Nguyen:1999:CGG


Nelson:1990:SAE


Neubauer:1998:DWI


Neubauer:1998:CSD


Nichols:1998:CCCa


Nichols:1998:CCCb


Nichols:1999:IGC

REFERENCES


REFERENCES


Nisan:1996:ERH


Nyberg:1993:PSA


Nakamura:1998:MEC


Nikander:1999:PPD


Nakamura:1988:DRM


Nandi:1994:TAC


Nguyen:1999:DZK


Naccache:1995:CDB


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

REFERENCES


**Naor:1998:TTT**


**Niemi:1994:CPV**


**Nyberg:1995:MRS**


**Naor:1998:UIS**


**Needham:1978:UEAa**

REFERENCES


REFERENCES

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

Nguyen:1997:MHR


Nechaev:1998:DSB


Nguyen:1998:BQS


Nguyen:1998:BSR


Nguyen:1998:BSR


Nguyen:1998:BSR


Nguyen:1999:HHS


Nguyen:1999:HHS

[NS99b] P. Nguyen and J. Stern. The hardness of the hidden sub-
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>[NT99]</td>
<td>Naccache:1999:HCF</td>
</tr>
<tr>
<td>[NT93]</td>
<td>Nieh:1993:MAC</td>
</tr>
<tr>
<td>[NT94]</td>
<td>Neuman:1994:KAS</td>
</tr>
<tr>
<td>[NW97]</td>
<td>Needham:1997:TE</td>
</tr>
</tbody>
</table>
TEA [WN95] and extension
XXTEA [WN98a].

[Naor:1998:ACS]

[Naor:1989:UOW]

[Naor:1990:PKC]

[Nyb94]

[Nyb95]

[Nyb98]


REFERENCES


**[O’C95] O’Connor:1995:DCT**


**[OD99] Obenland:1999:SED**


**[Odl84] Odlyzko:1984:CAM**


**[Odl85] Odlyzko:1985:DLF**

REFERENCES


REFERENCES


Okamoto:1994:DCS

Okamoto:1998:TKR

Okamoto:1998:TKS

Okon:1996:DWN

Okon:1997:KMA

Ogata:1997:FTA

Ogata:1993:NSS

Oleschchuk:1995:PKC
Vladimir A. Oleschchuk. On public-key cryptosystem based on Church–Rosser string-rewriting systems (extended abstract).
REFERENCES


Kazuo Ohta, Tatsuaki Okamoto, and Kenji Koyama. Membership authentication for hierarchical multigroups using the extended Fiat–
REFERENCES

Shamir scheme. Lecture Notes in Computer Science, 473:446–??, 1991. [OPH+99] CO-

ORuanaidh:1997:RST [OP97]

Joseph J. K. O’Ruanaidh and Thierry Pun. Rotation, scale and translation in-
variant digital image watermarking. In IEEE [IEE97h], pages 536–539. ISBN 0-
IEEE Computer Society order number PR08183. IEEE order plan catalog number
97CB36144.

ORuanaidh:1998:RST [OP98]

Joseph J. K. O’Ruanaidh and Thierry Pun. Rotation, scale and transla-
tion invariant spread spectrum digital image watermarking. Signal Process-

ORuanaidh:1999:CCP

Joseph Ó Ruanaidh, Holger Petersen, Alexander Herrigel, Shelby Pereira, and
Thierry Pun. Cryptographic copyright protection for digital images based on water-
17, 1999. CODEN TCSCD. ISSN 0304-3975 (print), 1879-2294 (elec-
tronic). URL http:// /www.elsevier.com/cgi-
bin/cas/tree/store/tcs/cas_sub/browse/browse. cgi?year=1999&volume=
226&issue=1-2&aid=3230.


Rolf Oppliger. Authentication systems for secure networks. The Artech House com-

Oppliger:1997:ISF [Opp97]

Rolf Oppliger. Internet security: Firewalls and beyond. Communications of the Asso-
Otway:1987:ETM


OECD:1998:OEM


OECD:1998:CPG


Ort95a


Ort95b

Glenn A. Orton. A multiple-iterated trapdoor for dense compact knapsacks. Lecture Notes in

Orlowski:1996:EGI


Orton:1987:VIP


Orton:1995:MTD

REFERENCES


Sing Guat Ong, Jennifer Seberry, and Thomas. Hardjono. Towards


REFERENCES


REFERENCES


[Par98c] Edward A. Parrish. Report to members: Members react to privacy and

**Patterson:1987:MCC**


**Patterson:1991:PPB**


**Pattarin:1991:NRP**


**Patarin:1995:CMI**


**Patarin:1996:ACH**


**Paterson:1999:IPG**


**Paulson:1998:IAV**

REFERENCES


Paulson:1999:IAI


Poovendran:1999:ITA


Proctor:1999:PC


Preneel:1989:CHB


Preneel:1997:CHF

REFERENCES


Pedersen:1991:NIT

Pedersen:1995:EPS

Pedersen:1999:SCP

Pelta:1960:SP

Penzhorn:1996:CAS

Perret:1890:RCS

Peralta:1985:TRN


REFERENCES

(PF94) G. Panagopoulos and C. Faloutsos. Bit-sliced signature files
for very large text databases on a parallel machine
architecture. Lecture Notes
in Computer Science, 779:
379–392, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

(PF95) B. Pfitzmann. Breaking an
efficient anonymous chan-
nel. Lecture Notes in
Computer Science, 950:332–
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/032627.html

(PF96a) B. Pfitzmann. Information hiding terminol-
ogy. In Anderson [And96c],
pages 347–350. CODEN
LNCSD9. ISBN 3-540-
61996-8 (softcover). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
Revision of thesis (Ph. D.)–University of
Hildesheim, 1993.

(Pf89) Charles P. Pfleeger. Secu-
rity in computing. Prenti-
tice-Hall, Inc., Upper Sad-
dle River, NJ 07458, USA,
1989. ISBN 0-13-798943-
1. xxi + 538 pp. LCCN


REFERENCES

URL http://link.springer-|"y.com/link/service/series/|0558/tocs/t0576.htm;
issue&issn=0302-9743&|
volume=576. Conference |
held Aug. 11–15, 1991, at |
the University of Califor-|nia, Santa Barbara.

Preneel:1992:CSH

p. 186].

Preneel:1993:CHF


Preneel:1993:HFB


Preneel:1993:IAH


Preneel:1993:CSI


Preneel:1994:HFB


Preneel:1993:CSI

Pohlig:1978:IAC

S. C. Pohlig and M. E. Hellman. An improved algo-

**Post:1991:RSE**


**Praun:1999:RMW**


**Phillips:1998:SHI**


**Pic86**


**Pic98**


**Pierce:1977:SSP**

REFERENCES

Pieper:1993:CRD  

Pinch:1997:UCN  

Piner:1998:CUW  

Pitas:1995:PIW  

Pitas:1996:MSC  

Pitoura:1996:RSS  

Price:1999:IAV  
[A. R. Price and T. Jones.]

Panneerselvam:1990:RSA


Popek:1979:ESC


Penzhorn:1995:CLW


Pennehorn:1995:CLP


Pamplona:1998:LVC

REFERENCES

Postma:1997:DCF


Park:1994:KDA


Petrounias:1994:RBA


Pless:1975:ESC


Pless:1977:ESC


Plummer:1998:MIW


Plumstead:1982:ISG

Joan Boyar Plumstead. Inferring a sequence generated by a linear congruence. In IEEE [IEE82a], pages 153–159. CODEN ASFPDV. ISBN ???? ISSN
REFERENCES


[PM99c] Y. Prie, A. Mille, and J.-M. Pinon. AI-STRATA: a user-centered model for content-based description
REFERENCES


**Proctor:1992:AIC**


**Pudil:1995:ASM**


**Preneel:1994:CCM**


**Pointcheval:1999:NPK**


**Pollard:1974:TFP**


**Pollard:1978:MCM**

References


Ponting:1989:TCB


Poole:1995:La


Popentiu:1989:SRK


Pope:1996:PF


Porges:1952:MNC


Porter:1984:CN


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT

P. Poromaa. Parallel algorithms for triangular

**Posch:1992:TMD**


**Posch:1993:PFP**


**Posch:1998:MPC**


**Posch:1989:AEA**


**Pfitzmann:1990:HBD**


**Posch:1992:MRR**


**Posch:1992:RNS**


REFERENCES


[LCCN QA76.9.A25S735 1998.]


[LCCN Z104 .P92 1939.


REFERENCES

(PROD), 1611-3349 (electronic).

[PRB98b] Bart Preneel, Vincent Rijmen, and Antoon Bosselaers. Algorithm al-
ley: Principles and performance of cryptographic algorithms. Dr. Dobb’s
Journal of Software Tools, 23(12):126–131, December

(Ph.D.), Katholieke Universiteit Leuven, Leuven, Bel-
fullcit/f64276.

[Pre93b] B. Preneel. Standardization of cryptographic tech-
iques. Lecture Notes in Computer Science, 741:
162–173, 1993. CODEN LNCSDF9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[Pre94a] Bart Preneel. Cryptographic hash functions. European transactions on
telecommunications and related technologies, 5(4):431–
448, 1994. CODEN ETTTET. ISSN 1120-3862.

[Pre94b] B. Preneel. Cryptographic hash functions. European transactions on telecommu-
nications and related technologies, 5(4):431–??, July
1, 1994. CODEN ETTTET. ISSN 1120-3862.

[Pre95a] Bart Preneel, editor. Fast software encryption: sec-
ond international workshop, Leuven, Belgium, December
14–16, 1994: proceedings, volume 1008 of Lecture Notes in Computer
Science. Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, UK / etc., 1995. CODEN
LNCSDF9. ISBN 3-540-60590-8 (softcover). ISSN
0302-9743 (print), 1611-3349 (electronic). LCCN

[Pre95b] Bart Preneel. To the Editor: Further comments on
keyed MD5. CryptoBytes, 1
cryptobytes/crypto1n2.pdf.

[Pre97a] B. Preneel. Hash functions and MAC algorithms based
REFERENCES


PGP:1997:PGPa


PGP:1997:PGPb


Preneel:1998:CMA


Preneel:1998:IC


Preneel:1999:SCH


Pritchard:1980:DE


Price:1994:MVC


Pronzini:1980:MCC


Proctor:1985:SSC


Patel:1999:TML

Peyravian:1999:HBE


Psan:1993:CPS


Pieprzyk:1993:DHA


Pfitzmann:1996:AF


Pointcheval:1996:PSB


Pointcheval:1996:SPS

REFERENCES

694

Parker:1997:GFA


Padro:1998:SSS


Patel:1998:EDL


Patiyoot:1998:APW


Patiyoot:1998:SIW


Patiyoot:1998:TAPa


REFERENCES

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

Patiyoot:1999:WWA


Pfenning:1999:SDT


Patel:1997:UDB


Pieprzyk:1991:RAS


Pieprzyk:1995:PA


Pieprzyk:1995:ACA

[Paar:1997:FAA]

[PST97]

[PST88]

[Pfitzmann:1995:HBA]


[Phoenix:1995:QCP]
S. J. D. Phoenix and P. D. Townsend. Quantum cryptography: Protecting our future networks with quantum mechanics. Lecture Notes in Computer Science,
REFERENCES

Parkes:1999:ACC

Purdy:1974:HSL

Puteanus:1627:EPC

Preparata:1990:PCD

Peinado:1997:HPC

Posegga:1998:BCV

Pluimakers:1986:ACS

Preneel:1995:MMB
B. Preneel and P. C. van Oorschot. MD-x MAC and building fast MACs from
hash functions. In Coppersmith [Cop95d], pages 1–14.
CODEN LNCSD9. ISBN 3-540-60221-6 (Berlin). ISSN
0302-9743 (print), 1611-3349 (electronic). LCCN
URL http://link.springer-ny.com/link/service/series/0558/tocs/t0963.htm;
issue&issn=0302-9743&
volume=963. Sponsored
by the International Association for Cryptologic
Research (IACR), in cooperation with the IEEE
Computer Society Technical Committee on Security
and Privacy.

B. Preneel and P. van Oorschot. On the security of two MAC algorithms. In Maurer
[Mau96b], page ??. CODEN LNCSD9. ISBN 3-540-61186-X. ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25
link/service/series/0558/tocs/t1070.htm;
issue&issn=0302-9743&volume=
1070. Sponsored by the International Association for Cryptologic Research (IACR), in cooperation

with the University of Saragossa.

A. Pfitzmann and M. Waidner. Networks without user observability — design options. In Pichler
0302-9743 (print), 1611-3349 (electronic). LCCN
URL http://www.cl.cam.ac.uk/~fapp2/steganography/
bibliography/1020.html.
“The workshop was sponsored by International Association for Cryptologic Research ... [et al.]”–T.p.
verso.

June M. Power and Steve R. Wilbur. Authentication in a heterogeneous environment.

Andreas Pfitzmann and Michael Waidner. Networks without user observability. Computers and Security,
6(2):158–166, April 1987. CODEN CPSEDU. ISSN 0167-4048. URL http:/
Power:1987:AHE


Pfitzmann:1993:APS


Pfitzmann:1993:SLT


Pfitzmann:1997:AF


Pfitzmann:1997:AFL


Piper:1993:DSH

REFERENCES


[QG89] J. J. Quisquater and M. Girault. 2n-bit hash-functions using n-bit sym-


[QSA88] Bin Qin, Howard A. Sholl, and Reda A. Ammar. RTS: a system to simulate the real time cost behaviour...
of parallel computations. 

**Quisquater:1989:ACE**


**Quisquater:1990:ACE**


**Rabin:1977:DS**


**Rabin:1981:HES**


REFERENCES

Randell:1982:CGC


Randell:1982:ODC


Rand:2001:MRD


Rao:1984:JEE


Ratcliff:1996:DIN


Rhodes-Burke:1982:RSA


Reiter:1994:HSR

Ramesh:1999:VPP


Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA


Rogaway:1994:SOE


Russinovich:1995:EWL


Rubia:1999:RIB

[Montse Rubia, Juan Carlos Cruellas, and Manel Med-]


REFERENCES


Rejewski:1977:ATP


Rejewski:1981:HPM


Rejewski:19xx:EMH


Revello:1991:CEC


Reynard:1996:SCB


Reynard:1997:SCB


Reynard:1999:SCB

REFERENCES


Rivest:1992:RNP


Rhee:1993:RAC


Rhee:1994:CSC


Richards:1974:SWP

[Ric74] Sheila R. Richards. *Secret writing in the public records: Henry VIII–George II*. London, 1974. x + 173 + 4 plates pp. UK£4.50. Contains one hundred documents, all but one of which are written wholly or partially in cipher and are now deciphered and printed in full for the first time. Includes letters in French or Italian, with a summary in English.

Rihaczek:1987:T


Rijmen:1999:WL


Riley:1996:LET

[Ril96] 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.


REFERENCES


REFERENCES


[Riv95e] Ronald L. Rivest. Welcome to CryptoBytes. Crypto-


REFERENCES


REFERENCES

[**Roy:1999:QCE**]


[**Rosenson:1994:GWE**]


[**Ruanaidh:1996:WDI**]


[**Reeds:1985:NPR**]


[**Rao:1987:PKA**]


[**Rao:1989:PKA**]

Raisch:1996:ACH


Roberts:1993:ECI


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Roe:1994:PSC


Roe:1995:PBC


Roelse:1999:CWD

Peter Roelse. Cryptanalysis of the Wu-Dawson pub-


[Rom90b] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In ACM [ACM90], pages
REFERENCES


[Ros95a] 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.


February 1996. CODEN LOGNEM. ISSN 1044-6397.

**Rose:1996:UPKa**


**Rose:1996:UPKB**

[102x681] February 1996. CODEN LOGNEM. ISSN 1044-6397.

**Rose:1997:ZP**


**Rose:1997:UPU**


**Rosenheim:1997:CIS**


**Rose:1998:SCB**


**Rose:1998:NUP**


**Rose:1998:UPK**

REFERENCES


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


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


**Ruskey:1993:SCG**


**Ruskey:1993:NSC**


**Ruskey:1993:SCG**


**Rytter:1986:SCU**


**Ras:1999:DES**

REFERENCES


[Sah99] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In


Sansom:1986:BRC


Sandhu:1988:CIT


Sarton:1928:BRBn


Sars:1997:STL


Sargent:1999:FID


Sasaki:1999:SFU


Swierstra:1999:DIC

Satyanarayanan:1989:ISL


Saunders:1989:IDE


Savarnejad:1996:COF


Savarnejad:1997:GAD


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Sorkin:1984:MCC

REFERENCES


REFERENCES

uk/~fapp2/steganography/bibliography/073169.html
ACM order number 43398. [SBET85]

Soto:1999:RTA

Serpell:1985:PES

Smillie:1985:RFM

Stallmann:1999:HED

Siegberg:1999:TDG
Sztandera:1999:ANN

Shepherd:1999:NCS

Chen:1985:RGE

Schneider:1996:RCB

Smith:1996:MIH
REFERENCES

Sun:1997:DCP

Schneider:19xx:DWI

Scacchitti:1986:CT

Styner:1999:BMD

Schwenter:1620:SSN

Schwenter:1633:SSA
Verlegung Jeremiae Dumlers [between 1633 and 1636].


REFERENCES


[Sch91c] Bruce Schneier. One-way hash functions: Probabilistic algorithms can be used for general-purpose pattern matching. Dr. Dobb’s Journal of Software Tools, 16(9):148–151, September 1, 1991. CODEN DDJOEB. ISSN 1044-789X.


REFERENCES


REFERENCES


Schnorr:1993:FIE


Schiller:1994:SDC


Schneier:1994:DNV


Schneier:1994:DEA


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

Schneier:1994:PAD


Schneier:1994:SCD


Schneier:1994:AAAd


Schneier:1994:ACP

REFERENCES

Schneier:AC94

Schneier:1994:CAW

Schneier:1994:NC

Schneier:1994:PYM

Schneier:1994:RDS

Schneier:1995:AAG

Schneier:1995:MS
REFERENCES

http://www.counterpane.com/email-japanese.html
Japanese translation of [Sch95d].

**Schneier:1995:MSH**


**Schneier:1995:OPE**


**Schneier:1995:PCC**


**Schneier:1996:ACP**


**Schneier:1996:CC**


**Schneier:1996:DLC**


**Schneier:1997:IRC**

REFERENCES


Bruce Schneier. The crypto bomb is ticking: Cracking encryption gets easier as computers get faster and cheaper. now what? BYTE Magazine, 23(5):97–??, May 1998. CODEN BYTEDJ. ISSN 0360-5280.
REFERENCES


REFERENCES


Schaefer:1999:PES


Schmalz:1999:MDI


Schmidt:1999:RER


Schneier:1999:SSC


Schneier:1999:IRR

Schneier:1999:IRT


Schneier:1999:IRU


Schneier:1999:IWC


Schoenmakers:1999:SPV


Schroeder:1999:SEA


Schumann:1999:PST


Schwentick:1999:DCL

REFERENCES

Scerri:1999:UOS


[SD99]

Scudder:1992:OLA


[Scu92]

Smith:1986:GCC


[SD86]

Silvestre:1997:IWU


[SD97]


Schouten:1999:FEU


[Schouten:1999:FEU]

Sicherman:1983:AQR


Smillie:1986:RWA


Schwenk:1996:PKE


Seaton:1956:THS


Sears:1986:SWK


Seachrist:1995:DIM


Sedlak:1988:RCP

REFERENCES

com/openurl.asp?genre=
issue&issn=0302-9743&
volume=293. CRYPTO ’87,
[See97]
a Conference on the Theory
and Applications of Crypto-
graphic Techniques, held at
the University of California,
Santa Barbara . . . August

[Sed92] Robert Sedgewick. Algo-
rithms in C++. Addison-
Wesley, Reading, MA, USA,
0-201-51059-6. xiv + 656
pp. LCCN QA76.73.C153

[Sed93] Robert Sedgewick. Algo-
rithms in Modula-3. Addi-
son-Wesley, Reading, MA,
USA, 1993. ISBN 0-201-
53351-0. xiv + 656 pp.
LCCN QA76.73.M63 S43
1993.

[See89] Donn Seeley. Password
cracking: a game of wits.
Communications of the
Association for Comput-
ing Machinery, 32(6):700–
703, June 1989. CODEN
CACMA2. ISSN 0001-
0782 (print), 1557-7317
(electronic). URL http://[Sel98b]
//www.acm.org/pubs/toc/
Abstracts/0001-0782/63529.html.

[Sel94] E. Selmer. From the mem-
oirs of a Norwegian cryp-
tologist. Lecture Notes
in Computer Science, 765:
142–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Sel98a] A. Aydin Selcuk. New re-
results in linear cryptanal-
ysis of RC5. Lecture Notes
in Computer Science, 1372:1–??,
1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Sel98b] Ernst S. Selmer. The Nor-
wegian modification of the
Siemens and Halske T52e ei-
pher machines. In Deavours

Serpell:1985:CES

Seshadri:1981:KPP

Sakurai:1997:ILC

Saglam:1995:ACL

Shearer:1996:GCR

Shieh:1996:DIL


REFERENCES


REFERENCES


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


REFERENCES

Shamir:1979:HSS


Shamir:1982:PTA


Shamir:1983:ECT


Shamir:1983:GCS


Shamir:1984:PTA


Shamir:1985:IBC


Shamir:1986:SPS

[Sha86] A. Shamir. The search for provably secure identification schemes. In Gleason
REFERENCES


Shepherd:1992:FFW


Shepherd:1992:FHS


Shepherd:1992:HSC


Shepherd:1992:NPS


Shepherd:1992:SIR


Sherrod:1992:DES


Shepherd:1993:ACCa


Shepherd:1993:ACCb

REFERENCES


REFERENCES

Smaus:1999:PIE


Shoup:1996:FPS


Shor:1997:PTA


Shparlinski:1999:FFT


Shparlinski:1999:NTM


Shulman:1976:ABC

Shulman:1980:BRB

Shulman:1980:BRU

Shumaker:1982:RCJ

Sakurai:1993:DBS

Sakurai:1993:SCS

Sakurai:1994:SCT
CODEN IFESEX. ISSN [Sie85]
0916-8508 (print), 1745-1337 (electronic). URL


REFERENCES


Simmons:1979:SAE


Simmons:1982:SCA


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC


Simmons:1985:SCD

Gustavus J. Simmons. The subliminal channel and digital signatures. In Beth et al.
REFERENCES


Simmons:1988:SSC


Simmons:1990:HRS


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

Gustavus J. Simmons. The
REFERENCES


Simpson:1996:RPC


Simmons:1997:SCS


Simmons:1998:HSC


Simmons:1998:RCB


Simmons:1998:FCO


Sinkov:1966:ECM

Abraham Sinkov. Ele-
REFERENCES

Sinnott:1977:CTC

Sinkov:1968:ECMa

[Sin68a]
[Sin95]

Sinkov:1968:ECMb

[Sin68b]
[Sin98]

Singh:1985:IPS

[Sin85]

Singer:1998:ECD

[Sin99]

Sinkov:1968:ECM

Sinhott:1977:CTC

Singer:1999:CBE


[Sin99]

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

[Siu99]

Sinha:1995:KNC

[Sin95]
REFERENCES


Schneier:1996:PPSa


Schneier:1996:UFNa


Schneier:1996:UFNc


Schneier:1996:PPSb


Schneier:1997:AESb


Schneier:1997:AESa


REFERENCES


**Stabell-Kulo:1999:PAM**


**Shepherd:1997:EKE**


**Schell:19xx:CMC**


**Sorokine:1994:TBD**


**Suzuki:1999:AVB**


**Satoh:1998:HSR**


**Satoh:1998:HSS**

REFERENCES

Schneier:1996:DP


Schneier:1998:TKSa


Schneier:1998:TBBa


Schneier:1998:TBBb


Schneier:1998:TSC


Schneier:1998:TBE

ference 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.

Schneier:1998:TNB


Schneier:1999:PCAa


Schneier:1999:PCAb


Schneier:1999:NRT

Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. New results on the Twofish encryp-
REFERENCES

Sufatrio:1999:IMS


Schobi:1983:FAT


Schneier:1996:AC


Schneier:1999:TEAb


Schneier:1999:TKS


Schneier:1999:TEAb


Schneier:1999:TKS


REFERENCES
REFERENCES

Siromoney:1990:PKC

Staffelbach:1991:CSC

Schubert:1995:MLS

Syverson:1995:FRK

Sklower:1996:RPE

Schneier:1998:CMP

Sklower:1998:RPE
[K. Sklower and G. Meyer. RFC 2419: The PPP DES encryption protocol, version 2 (DESE-bis),

Sutcliffe:1999:LBM


Smart:1999:PHC


Schneier:1999:DDE


Smith:1943:CSS


Smith:1944:CSS


Smith:1955:CSS

This is a simple exposition of public key cryptography.


REFERENCES

Stakhov:1999:IFC


Safavi-Naini:1993:FTA


Shepherd:1994:VFH


Safavi-Naini:1996:TSS


Smith:1972:EAC


Steiner:1988:KAS


Safavi-Naini:1993:ACU


Safavi-Naini:1995:ACP

REFERENCES

[Safavi-Naini:1998:BCM]

[Safavi-Naini:1998:NRM]

[Snyder:1979:IUC]

[Snyder:1980:CAP]

[Shepherd:1998:ALP]

[Sonnino:1999:CBL]
REFERENCES


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


REFERENCES


[Schechter:1999:AAM]


[Spirakis:1995:AET]


[Schwemmlein:1998:RMR]


[Schuett:1997:CPB]

Shoup:1996:SKD  

Shin:1998:NHF  

Saltzer:1984:EEA  

Shepherd:1989:CSS  
Shepherd:1990:DSA


Schrift:1991:UNB


Sun:1994:DTS


Sakurai:1995:RAC


Smith:1995:PKC


Sandhu:1996:AAC

Ravi Sandhu and Pierangela Samarati. Authentication, access control, and
Silverman:1997:CAX


Sakai:1998:DHC


Sun:1998:PKC


Schneier:1999:BHD


Schoenhoff:1999:GVM


Shapiro:1999:MAE

Solomonides:1999:REI

Stubblebine:1999:FLA

Stubblebine:1999:FOA

Subramanian:1987:DTP

Siromoney:1988:CPL

Saito:1999:DPC

Smith:1981:VEP

[Safford:1993:SRA]


[Sakai:1997:WRK]


[Sakai:1997:WRP]


[Subramanian:1992:LT]


[Sherman:1994:SNA]

REFERENCES

Schneier:1997:DDE


Saeednia:1998:NIK


Saeednia:1998:SGI


Susilo:1999:FST


Shepherd:1990:CSS


Schmidt:1998:LOA


Salter:1998:TSS

### REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>
StJohns:1993:RIP


Safavi-Naini:1994:OAS


Stark:1970:INT


Stallings:1994:PGP

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

Stallings:1994:SSH

[Sta94b]

Stallings:1995:PWT

William Stallings. The PGP web of trust: Managing public keys with the PGP (Pretty Good Privacy) web

**Stallings:1995:PYP**


**Stadler:1996:PVS**


**Staiger:1996:CSW**


**Stallings:1996:PCS**


**Stallings:1996:PCI**


**Staddon:1997:CSC**


**Stallman:1997:SDR**

Stark:1997:ESP


Stallings:1999:CNS


Stallings:1999:HAK


Stevenson:1976:MCI


Stern:1987:SLC


Stevens:1988:CPR


Stephenson:1989:PPM


Stevens:1990:CPi

REFERENCES

Stevens:1990:CPk


Steinberg:1991:VSV


Stewart:1992:SCK


Stevens:1994:PBa


Stern:1995:COD


Stern:1996:VCA


Stern:1998:LCO


Stern:1998:NEA


Stevens:1994:PBa

REFERENCES


Stephenson:1999:C


Stern:1999:ACE


Stinson:1999:UHA


Stinson:1999:DU


Stinson:1991:CCA


36, 38–43, April 1998. CODEN DDJOEB. ISSN 1044-789X. URL \url{http://www.ddj.com/}.

**Stout:1965:DRN**


**Stoll:1989:CET**


**Stout:1990:SDE**


**Stone:1998:RBH**


**Sivabal:1993:DSN**


**Stripp:1987:BJC**


**Stripp:1989:CFE**


**Strauss:1993:SEC**


**Strauss:1993:SMC**

REFERENCES

CODEN DTMNAT. ISSN 0011-6963.

Stripp:1995:CBF


Sander:1999:AAE


Sander:1999:FCN


Sandholm:1999:DOC


Stumme:1999:AEK


Steiner:1995:REE


Su:1998:DEM


Summers:1984:OCS


Sun:1991:UDE

REFERENCES

Sun:1991:RSE

Sun:1998:ISM

Sun91b

Sun:1998:SDI

Sun98a

Sundsted:1998:SDI

SuperMacSoftware:1988:SDE

Sutoh:1999:HPP
Hiroki Sutoh. A high-performance public key cryptography co-processor for super multi-purpose smart card. In Anonymous [Ano99c], page ??

Shand:1993:FIR

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

Sivakumar:1999:PPN


Shepherd:1996:SAD


Shamir:1998:PHS

Adi Shamir and Nicko van Someren. Playing hide and

Shepherd:1995:SCS


Smeets:1991:CAC


Shulman:1961:GC


Smith:1983:HCR


Silverman:1993:PAE


Saeki:1994:SSS


Safford:1994:UNC

Laurance F. Safford and J. N. Wenger. *U.S.
REFERENCES


REFERENCES

com/fast_software_encryption.html.


Qi Sun and Rong Xiao. Two kinds of elliptic curves over $F_q$ used to set up cryptosystems. Sichuan Daxue Xuebao, 26(1):39–43, 1989. CO-
REFERENCES

DEN SCTHAO. ISSN 0490-6756.

Sun:1990:KGE


Salomaa:1986:PCB


Salomaa:1986:PKC


Smith:1992:ICF


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

Sakurai:1996:BDB


Shieh:1996:AKD


Sowers:1998:TDW

Sellini:1999:VKV


Sakurai:1998:KES


Syverson:1992:KBS


Syverson:1993:KDP


Seberry:1993:ACA


Sakurai:1996:CWR

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


Three volumes. IEEE catalog number 96CH35919.


REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073173.html


**Seberry:1995:RBP**


**Theodoridis:1998:NES**


**Takano:1999:CAP**

Kohji Takano et al. A cryptographic accelerator card with small fast low-power RSA engines. In Anonymous [Anon99c], page ??

**Tardo:1992:SGA**


**Tang:1997:DBC**


**Taaffe:1998:NBL**


**Tabatabaian:1994:CAP**

Seyed Jalil Tabatabaian. *Cryptanalysis algorithms*


[TC86] Ren Ji Tao and Shi Hua Chen. Two varieties of finite

Tsujii:1991:NIB


Tao:1999:VPK


Tsujii:1991:NIB


Tao:1999:GPK


Tsujii:1991:NIB


Tao:1999:VPK


Tao:1999:GPK

REFERENCES


[Tex84] Texas Instruments Inc. TMS7500 TMS75C00 User’s guide, data encryption device: 8-bit microcomputer family. Texas Instruments, Dallas, TX, USA, 1984. various pp.


REFERENCES

Theobald:1995:HBS


Thomas:1974:RPS


Thomas:1984:RTT


Thomas:1986:SDE


Thompson:1987:RTT


Thomas:1996:PVS


Tarman:1998:AAE


Tsujii:1988:PKC

REFERENCES


Tilki:1998:EHD


Tippett:1927:RSN


Taaffe:1997:NSL


Tseng:1999:ATS


Takagi:1999:DRA


Tzovaras:1998:RIW

Theodoratos:1999:DGD


Tavares:1999:SAC


Takagi:1996:MMP


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

rfc/rfc1810.txt. Status: INFORMATIONAL.


[Tri06b] Johannes Trithemius. Clavis Steganographiae Ioannis
Johannes Trithemius. *Steganographia*: *hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*. Matthiae Beckeri, Frankfurt, Germany, 1606. 8 + 180 pp. LCCN Z103.T84 S 1606. Authore ... Ioanne Trithemio ...; praefixa est huic operi sua clavis, seu vera introductio ab ipso authori concinnavta ... nunc vero in gratiam secretioris philosophiae studiorum publici iuris factura. Francofurti. Ex officina typographica Matthiae Beckeri, sumptibus Ioannis Berneri, anno 1606.

Johannes Trithemius. *Clavis generalis triplex in libros steganographicos Iohannis Trithemij* ... Balthasar Hofmann, Darmstadt, Germany, 1621. 7 + 1 pp. LCCN Z103 .T84 1621. Ab ipso authori conscripta ... Darmbstadij. Excudebat [Tri21a]


J. T. Trostle. Modelling a fuzzy time system. In

---

**References**

822


*Trithemius:1606:SHE*

[JTri06c]

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

*Trithemius:1606:CGT*

[Tri21c]


*Trithemius:1606:SHE*

[Tri21b]

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

*Trithemius:1606:CGT*

[Tri21c]

Johannes Trithemius. *Clavis Steganographiae Ioannis Trithemij ...*. Balthasar Hofmann, Darmstadt, Germany, 1621. 7 + 1 pp. LCCN Z103 .T84 1621. Ab ipso authori conscripta ... Darmbstadij. Excudebat [Tri21a]

Balthasar Hofmann, impen-


REFERENCES

Tombak:1993:ACP

Tsudik:1989:DAI

Tsudik:1992:MAOb

Tsudik:1992:MAOa

Tsujii:1992:CS

Thomlinson:1998:NBP

Thersites:1984:IKE

Thomas:1984:IKE
REFERENCES

[Tt99]

[Tua99]

[Tuc66]

[Tuc70]

[Tuc79a]

[Tuc79b]

[Tuc99]

[Tun99]
REFERENCES


[Tur99] Alan Turing. Turing’s treatise on Enigma. Technical report, CERN, Geneva, Switzerland, 1999. URL http://home.cern.ch/~frode/crypto/Turing/index.html. This document is retyped from the original (undated??) Turing typescript by the editors Ralph Erskine, Philip Marks and Frode Weierud. Chapters 1, 2, and 6 (of 8) are available; the remainder are in preparation.


REFERENCES

**Tan:1992:NPE**


**Takagi:1992:MMH**


**Trabelsi:1994:PPS**


**Tsiounis:1998:SEE**


**Tsiounis:1998:SEB**


**Tax:1999:PFD**


**Tygar:1996:CPI**

REFERENCES


[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).


USWD:1924:EC


USASC:1940:CML


USASC:1942:ACC


USDOS:1970:BC


USNBS:1977:DES


USCSSC:1978:CSD


USCSSC:1978:USN


USNA:1979:CS

United States.National Archives and Records Service. Cryptology studies. Records of the National Security Agency RG457, National Archives of the
REFERENCES


**USNSG:1979:IRW**


**USNBS:1981:GIU**


**USDA:1982:SMM**


**USDA:1982:TGM**


**USGSA:1982:TGS**


**USNBS:1983:FPD**


**USGSAOIRM:1984:ISR**

REFERENCES


REFERENCES


USNSACS:1994:SC


USCSCJSTL:1995:ACC


USNSGC:1995:NDN


UCC:1996:SRP


USPTO:1996:CCP


USCHCJ:1996:SFT


REFERENCES


REFERENCES

Shipping list no.: 98-0120-P.

**USCHCNS:1998:HSF**


**USCSCCST:1998:HEH**


**USCSCCST:1998:EHB**


**USCSCJ:1998:HEK**


**USCSCJ:1998:HED**


**USCSCJSTTGI:1998:EDC**


USNSACS:19xx:BPM


USNSACS:19xx:PUC


USGSA:1983:ISR


USGSA:1985:ISR

REFERENCES

Federal standard 1028. Federal information processing standards publication, FIPS PUB 141.


REFERENCES

USENIX:1996:SAC

USENIX:1996:WEC

USENIX:1996:CSW

USENIX:1996:PSUa

USENIX:1996:PSA

USENIX:1996:PUA

USENIX:1996:USS

USENIX:1998:PUWa
USENIX, editor. Proceedings of the 2nd USENIX Windows NT Symposium:
REFERENCES


[UU97b] United States.President Bill Clinton and United States.Congress.House.Committee on International Relations. Administration of export controls on encryption products: communication from the President of the United States transmit-

VanderBank:1988:CFM


[Vad95] Kumar S. Vadhir. 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.


VanTassel:1969:ACT


Vandeberg:1986:ICS


VanHeurck:1987:TNS

References

vanTilborg:1988:IC

VanTilburg:1993:SKE

VanOorschot:1995:DCS

VanTilborg:1995:ACA

vanRenesse:1996:OSC

vanDijk:1997:MIT

vanRenesse:1997:ODS
### REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>
Vaudenay:1998:CCR


Vaudenay:1998:DFC


Vaudenay:1998:FSE


Vaudenay:1999:FCD


Vaudenay:1999:SC


Vaudenay:1999:SCC


Vaudenay:1999:RAC


Vaden:1996:ETU


Viswanathan:1999:PVK


Vally:1999:CRC


Vandewalle:1990:ECC


Dijk:1995:LCP

vanDijk:1995:LCP

Dijk:1997:SCB

vandenAssem:1986:CPA

Vandermeulen:1999:ADM

Lubbe:1998:BMC

Wal:1997:PBR


REFERENCES


[vHPP93] Eugène van Heijst, Torben Pryds Pedersen, and Birgit Pfitzmann. New constructions of fail-stop signatures and lower bounds (extended abstract). Lecture Notes in Computer Sci-
REFERENCES


Vigna:1998:CTM


Vincent:1971:PAG


Vincent:1972:CPA


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

Vincent:1972:CPA


Voydock:1983:SMH


Voydock:1984:SMT


VanRompay:1998:DCI

REFERENCES


Lingen:1996:NDP


Vigil:1996:MIS


Villasenor:1997:CCa


Kerckhoffs:1883:CMF


Varadharajan:1999:DER


Voyatzis:1998:DWO


Venkataraman:1994:PAM


Venkataraman:1995:CEA


Oorschot:1991:CPP


vanOorschot:1991:CPP

vanOorschot:1992:CPP


Vogel:1985:LCC


Volts:1941:BCP


VonZurGathen:1992:PEE


VonZurGathen:1992:PEF


Voukalis:1980:DFC


Voukalis:1980:GSE

D. C. Voukalis. A good solution of the encryption problem using matrix code,

**vanOorschot:1991:KPA**


**Voyatzis:1996:ATA**


**Voyatzis:1998:DIW**


**Voyatzis:1999:PDI**

REFERENCES

Varadharajan:1997:ISP


Vassiliadis:1988:PEA


Volts:1941:BC


vanderWal:1997:PBR


VanEetvelt:1995:DPF

REFERENCES

856

Varadharajan:1997:SSP

vanTilburg:1990:MPK

vanTilburg:1993:TCP

vanTilburg:1994:SAC

vanTilburg:1986:DBK

vanSchyndel:1994:DW
REFERENCES

Number 6950-02. IEEE catalog number 94CH35708.

[Vu:1995:CPM]

[Vv:1997:CLS]

[VV85]

[VV86]

[Vv97]

[VvD90]

[VvT97]
Eric R. Verheul and Henk C. A. van Tilborg. Binding ElGamal: a fraud-

**vanOorschot:1994:PCS**


**VanOorschot:1996:DKA**


**Vedder:1998:SCR**


**vanOorschot:1999:PCS**


**vanEmdeBoas:1999:ALP**

3. LCCN QA267 .I23 1999
Bar.

**Vanstone:1997:ECC**


**Waber:1987:VEC**


**Weidenbach:1999:SDS**


**Wobber:1994:ATO**


**Wade:1993:SLV**


**Wadsen:1998:CLI**

Wagner:1983:F

Wagner:1998:DCK

Wagner:1998:CSR

Wagner:1999:BA

Wagner:1999:CFb

Wagstaff:1999:C

Waidner:1990:USR
REFERENCES

Waite:1995:BRB


Walden:1900:ADB


Wallace:1990:PRG


Wallich:1994:WP


Walton:1995:IAS


Walther:1998:VBE


Walker:1999:CCI

Wallich:1999:HSM


Walter:1999:MTI


Wen-Ai:1994:MTS


Wang:1986:UEA


Wang:1992:CDS


Wang:1992:DKT


Warren:1982:BTC

REFERENCES


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

[Watt:1991:IP1]

[Watson:1999:DOC]

[Wayner:1993:CAS]

[Wayner:1993:ECD]

[Wayner:1993:SER]
Wayner:1995:PCL


Wayner:1996:DCB


Wayner:1996:DLY


Wayner:1998:MJD


Willcox:1992:TCS


Wagner:1994:PPR


Wolf:1995:ICR

[WB95] Thomas Wolf and Andreas Brand. Investigating DEs with CRACK and related programs. SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation), 29(2S (special issue)):
REFERENCES

1–8, June 1995. CODEN SIGSBZ. ISSN 0163-5824 (print), 1557-9492 (electronic).

Whittle:1999:SDC


Wallach:1997:ESA


Wu:1998:CRP


Wegman:1981:NHF


Wynn:1997:CTS


Weeks:1995:CBW

REFERENCES


REFERENCES


REFERENCES


[Wei83]

[Wei88]

[Wei91a]

[Wei91b]

[Wei93]

[Wei94]

[Wei98]

[Wei99]

[Wel80]
David L. Wells. Achieving data base protection through the use of subkey encryption. Thesis (Doctor of Engineering),


REFERENCES


REFERENCES


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

White:1990:CDP


REFERENCES


Wiener:1994:EKS


Wiener:1996:EKS


Wiener:1997:EKS


Wiener:1998:EKS


Wiener:1998:PCP


Wiener:1999:ACC

REFERENCES


REFERENCES


[Wil98a]


[Wil86c]


[Wil98b]


[Wil93a]


[Wil93b]


[Win9a]


[Win74a]

REFERENCES

Winterbotham:1974:USF

Winterbotham:1975:US

Winterbotham:1978:NC

Winternitz:1983:POW

Winterbotham:1989:US

Winternitz:1984:SOH

Winterbotham:1991:US

Winton:1993:UPH
REFERENCES

Winterbotham:1999:US


Wired:1998:REC


Wedel:1996:FSA


Watanabe:1997:SCR


Wechsler:1997:AVB


Whiting:1999:FOK


Woo:1992:ARC

REFERENCES


REFERENCES

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

Waldvogel:1993:PDD


Wheeler:1994:TCN


Wheeler:1995:TTE


Wheeler:1998:CX


Wright:1998:NTD


Woehr:1997:CRR


Wolfe:1943:FCCa


REFERENCES


[Wri89] Fred B. Wrixon. Codes, ci-
phers, and secret language.

Wright:1994:IRV

Wright:1998:ECC

Wrixon:1998:CCO

Wagner:1996:ASPa
REFERENCES


Wagner:1996:ASPb


Wiese:1996:SSS


Wagner:1997:ASP


Whiting:1998:ITI


White:1999:CBA


Wagner:1998:CO


Whitten:1999:WJC


Wu:1992:GOC


Wu:1996:SNL


Williams:1979:CAA

P. W. Williams and D. Woodhead. Computer assisted


REFERENCES


Xiong:1999:LPK


Xiao:1994:MMH


Xu:1998:STP


Yacobi:1999:RMC


Yacobi:1999:RME


Yahalom:COMPSYS-7-4-451

REFERENCES

[Yamamura:1998:PCU]

[Yamamura:1998:PKC]

[Yamamura:1999:FCU]

[Yan:1995:PTL]

[Yao:1982:PSC]

[Yao:1982:TAT]

[Yao:1986:HGE]

[Yardley:1931:ABC]
Herbert O. Yardley. The American Black Chamber. Faber & Faber Limited,
REFERENCES

London, UK, 1931. x + 264 + 1 pp. LCCN D639.S7 Y3 1931b. The history and work of the Cryptographic bureau, officially known as section 8 of the Military intelligence division (MI-8).


REFERENCES

Yeun:1999:DSM

Yokokawa:1999:BDE

Yi:1996:DAN

Yin:1997:REA

Yakovlev:1998:PND

Yahalom:1994:TBN

Yang:1999:DIC
Yen:1993:FCE


Yen:1995:IDSb


Yen:1995:IDSa


Yang:1997:NEC


Yen:1997:SAT


Yi:1997:NHF


Yi:1998:NBB

Yi:1998:NBO


Ye:1999:CS


Yi:1998:DCB


Yeung:1998:IWI


Ye:1998:DBW


York:1996:BSN


Yourdon:1996:JWS


Young:1997:IJA

REFERENCES


REFERENCES


Yung:1985:SUK


Yuval:1997:RTE


Yang:1997:CBC


Yang:1999:GSP


Yu:1989:DEB


Yu:1991:SED


Young:1996:DSB

Young:1997:KUC


Young:1997:PKA


Young:1997:SEC


Young:1998:FLP


Young:1998:MBS


Young:1998:ARA

Adam Young and Moti Yung. Auto-recoverable auto-certifiable cryptosystems. *Lecture Notes in
REFERENCES

Young:1998:MBB


Yeo:1999:WOV


Zafiropulo:1963:RAD

Jean Zafiropulo. Le rôle de l’analogie dans le déchiffrement de l’écriture mycéenne linéaire B. (French) [The role of analogy in deciphering Myce-
REFERENCES


Zajacz:1997:SCE


Zang:1990:ESE


Zave:1999:SDC


Zegwaart:1993:PEM


Zei79


Zer96a


Zer96b


ZFK+98


Zoellner:1998:MSS


Zuquete:1996:TAC


Zeng:1990:LSM


Zhao:1996:WSE


Zviran:1993:CPT


Zhang:1991:BNK


REFERENCEs

Zhao:1997:LT

Zhao:1997:LT

Zheng:1990:PDS

Zheng:1995:HBR

Zheng:1995:KAP

Zheng:1997:SC

Zheng:1997:DSH

Zilouchian:1998:ANF
A. Zilouchian, D. W. Howard, and T. Jordanides. An adaptive neuro-fuzzy inference System (ANFIS) approach to control of robotic manipulators. Lec-
REFERENCES

Zhou:1994:SDS


Zheng:1994:RSS


Zheng:1998:HCE


Zieschang:1997:CPB


Zim:1948:CSW


Zimmermann:1995:OPU


Zimmermann:1995:PSC

Zimmermann:1996:PGPa


[Zim96a]

Zimmermann:1996:PGPb


[Zim96b]

Zimmermann:1998:CI


[Zim98]

Zimmermann:1999:EVI


Zhao:1995:ERL


Zhao:1996:DWS

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

Zhao:1998:GDW


Zhao:1998:BTT


Zhao:1999:DWW


Zhao:1999:SPP


Zhang:1999:AFV

Yuqing Zhang, Jihong Li, and Guozhen Xiao. An approach to the formal verification of the two-party cryptographic proto-
Zheng:1990:_CBC


Zheng:1991:DBT


Zolman:1993:BSJ


Zorpette:1987:BEC


Zheng:1993:HOH


Zhu:1996:PKC

REFERENCES


REFERENCES


[ZZ95] Xian-Mo Zhang and Yuliang Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions.

ZZ96

URL http://www.iicm.edu/gac_the_criterion_for_global_avalanche_characteristics_of_cryptographic_functions.

ZZ96


ZZ97