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/

21 April 2018
Version 1.101

Title word cross-reference

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

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

$1-Million [GC97]. 16 [BS93a, GC94]. 2 [JV98b, KG95, Koh91b, MVZ98, SBV99].$


[JS95b]. mod2^32 [Ber93]. c [WD99b]. $^2
[HG97b]. d [BD99b]. $ [BR91]. f [DJL93].
F_{2^n} [MVZ93]. F_{2n} [SS98a, Ler97]. F_p
[Miy93a]. G(D(2^n)) [Ara93]. GF(2) [She95c].
GF(208) [Ros98a]. GF(2) [FBT96]. GF(p)
[Gor93b, HNM98]. \geq [GQW+91]. k
[Car97c, DJL93, HKS97a, HKS97b, KR99b, KS97b, WD99b]. l [HL93a, KS97b]. L2
[Vau99a]. \lambda [RS99c]. L \geq 2 [SVxW91]. \leq [GQW+91]. m [Bla94a, FR94]. N
[BS91c, BS91d, HKS97a, HKS97b, KSW99b, KSW99c, KK98, Per93, QG90, Tak97].
N = p^l q [BDHG99a, BDHG99b]. N_{0,292}
[BD99b]. P [BS90b]. p^l q [Tak98a, Tak98b].
\ell [BDHG99a, BDHG99b, FJR96]. s
[YT95a, YT95b]. s2 [Knu93b]. Step_{k,m}
Acceleration [TT99]. Accelerator [T99].
acceptance [Gil97, Sta94a]. Access [ABL93, BDPS97, BGT96, FHBB97, GKK99, Iwa97, KS99a, KG99, MSNW99, NW98, She93a, She93b, SL99, VD999, Cha99b, CII99, DF91b, Gol99b, IS97, LL93b, PS98a, RD96a, S986, SSM94, Ver98b, W909, WWH95]. Accessibility [DFGH99].
accompany [UU97a]. account [Car97c]. Accounting [PUF99].
Accumulators [BP97a, BdM94].
Accuracy [BALS99].
Accurate [CH99b].
Achieve [Zhe97b, Sta94a].
Achieving [Cha92b, Cha92a].
ACISP'97 [VPM97].
ACM [ACM94c, ACM96b, ACM97a, AR97, ?98, D98, ES98, HF97, KS99b].
ACM-SIAM [ACM97b].
Acoustic [MFG95].
Acoustics [IEE97d].
Acquires [GC97].
Acquiring [COM99, Stu99].
Acquisition [Tod97].
ACSAC'97 [IEE97b].
Act [An97, An98a, AN98, UN98b, UN98c, UN98e, UN98f].
Action [FJRS96, YAM99].
Actions [Ros95b].
Active [BP95b, BQ95a, Cra98, HCD99, HHD99, HCY96a, LFCK99, MW97, W991, WHFG92, Wol98, B95a, Cra97, H98b, H98a, Hor98].
ActiveX [Par98b].
Activities [Rhe93, Don98, SW94b, WS96c].
Acyclic [BM94a].
Ada [Car96, SvA98].
Adapt [KM99a].
Adaptable [PM99b].
Adaptation [GM99a, NA99].
Adaptively [BE96, FMY99, LL94a, ZS93, CP94].
Adaptively-Secure [FMY99].
addendum [WL92a].
addiction [Hol91].
Adding [Boy98, Men91].
Addition [LYH93, SM91, Zin99, CK93, LY93, d95].
additional [UU97a].
Addable [Jac96].
Adds [Ack98].
Adelaide [KK99b].
Adequacy [Bra95a, Bra96].
Adequate [BDR96].
Adic [KG95, GK95a, Tak97].
ADL'98 [IEE98d].
Adleman [She92c].
Administration [CII97, USE96a, USE99b, U97b, Un95a, Un97d, U97b].
Administrative [Mea98].
Admiral [Fra93].
Adolescence [DI90], adopted [Ara93].
Adrift [DG95, DTG96].
ADSL [VDDR99].
Advances [Bra90c, Bri92, Bri93, Cop95b, Dam90a, Dam91a, Dav91, De 95, Fum97, Gol90b, IE98d, KM96a, K98, LOX99, LS98a, MV91, Ny98, ODP98, Pin98, PNFK95, QV90, Q95, Rue93, S93, Ste99b, St99b, Wie99, Gol98b, Lid90, Cop95d, Des94b, Fei91, GQ95, Hel94, IRM93, Kar97c, Kob96, Man96b, MZ98, PSN95b, SP90, St94].
adversarial [LHL95b, LHL95a].
Adversaries [CM97a, MW97, BH93].
Adversary [AGY95b, CDD99, AGY95a].
Advice [LTEH99].
advocate [An94d].
AES1 [BPS98].
affect [Win93].
Affine [KK95, Son99].
African [CFK91].
After [Dob96b].
Again [Gar97c, Gar96c].
Against [AGY95b, BQ95b, BQ95a, Ble98a, CM97a, CN97, CG99, CNS99b, CS98b, CDD99, Da99, De 93b, De 98c, FG98, HG98, KTM99, KSW99c, Mat96a, MW97, NK93, Riv98c, S96, W98, YY97a, ZS93, Ad92a, AGY95a, Ano97-30, BH93, CP94, Cop94a, Dam91b, Des90a, DY91f, Dre92, FY99, GQW91, HA94b, HY98b, HY98a, JG95, KSW99b, KR96b, KOT95a, KOT95b, LL94a, LyD98, NY90, OK96b, RS93, SG98, WK97]
Win93, YL97b]. **Age**
Bar94, SB97, Uni98i, Wal95, BS97b, Car97a, Joh98, Mar95b, Uni97c, Duh90l. **Agencies**
MK99, **Agency** [Gar97a, **Agent** BL99, CF99, Cha90, COZ99, FK99, Lee99b, MM99b, PW99, PM99a, SJS98, VC99, CM99b, HJTW99]. **Agent-Based** [FK99, MM99b, SJS98]. **Agent-Oriented** [BL99]. **Agents** [BGS98, FGS96, GB98, IN99, Jun99, PW99, PWU99, RS98c, RS98d, SCT99, SSP90, Vig98, YY97c]. **Agile** [KLZ99, THP+98]. **Agnes** [Luj98a, Luj98b]. **agnostic** [JY96]. **Agree** [Gar97a, Ano97c]. **Agreement** [BWM99a, Bor95, Bor96, Cae96b, Gar94, Gar97c, JV96, LM94b, LP99, Man93a, MW96a, Mau97a, RSA93b, Van95a, Wol98, vOW96, BY93c, BY93b, HY98a, HY98a, LM94a, VW96, Zhe95a, Zhe95b, Wei99]. **Agreements** [MB99a]. **Agricultural** [Far93]. **AH** [MG98a, MG98b]. **AI** [Mas97, PMP99]. **AI-STRATA** [PMP99]. **aid** [SBTV99]. **Aided** [BQ95b, BQ95a, HCY96a, LYH93, LL95a, MW98d, MD994, NS98b, NS98c, BM94c, Hor98, LY93, MW98c, PW93a]. **Aids** [Cra92]. **AIR** [Ano97r, DIF94, SVa+98]. **AIR-BAG** [Ano97r]. **Airborne** [CK99]. **AIN** [Con93, Ajai]. **AG** [GGH97a, NS98c, NS98c]. **Akalrre** [FS97a]. **AKL** [AP94]. **Akta** [Ano97-29]. **AL** [CM99d, CFK+91]. **al-Khwarizmi** [CFK+91]. **Alan** [Hod97]. **Alarm** [LKD98]. **Albuquerque** [IEE91]. **aléatoire** [Bou94]. **Ale** [Sac92]. **Alexandra** [LW96]. **Alexandria** [IEE94a, Man98]. **Alf** [Dob95b]. **Alfred** [Sha99a]. **Algebra** [BK94a, Pes97, VG99, CMM93]. **Algebraic** [Des98a, FL99a, Gog99, HR90, Kob98b, LW91, Mv93, Wat91, Ala97, BHHR99, CL98, CMM93, HN94, JM96a, Sch91a, SH94, ZPY96]. **Algebraic-Code** [HR90, Mv93, Ala97, CL98, SH94]. **algebraic-geometric** [JM96a]. **ALGOL** [RS99c]. **Algorithm** [ANS97, Ada97b, IBM93, Ano96c, Ano96e, ADEDS99, COP+95a, CD91, DCR97b, DNR97, Dra98, GX99, GK98, GTG94, GN95c, HG97a, HG97b, HW99, Kal91, KY95a, KR96a, KY98, KMM99, Kob98c, Kra93, Kwa97, MD98, MW94, Mas94, Mat97, Mis97, MS90b, Mon99, Nat97b, PBGV90, PRB98b, Riv92a, Riv92b, Riv95c, Riv95b, Riv98, RC94a, RC94b, RH99, Sch93d, Sch94f, Sch95a, Sch95b, SKW+98e, Sch98g, SKW+99d, SHK+99a, SKW+99e, SS99c, She94b, SB98, SW93, Sta99b, Swa94, TK99, THP+98, VKR98, Whe94, Yin97, ZYR91, BI94, BS95a, Bow93, CC98, CGV94, ISO97, IKNY98, JMLW94, KY95b, KY97, KYxx, Kir95, LRW93, LZ90, LZ91a, LL93b, Lon91, LC97b, MSS93, MPL99, Mol98, Pai96, Riv90a, Riv91b, Riv95d, Sch91a, Sch94i, Tay94, Vad95, WN95, YL93, YL95b, ZW99, ZPS93]. **Algorithm** [AA95, Acc97, LL98, Moc97, OA94, Sch93b, Sch94e, See97, Sim93, Sta94b, WSK97a, WSK97b]. **Algorithm-Agile** [THP+98]. **Algorithms** [ACM97b, ANS97, Ano95a, Ano95b, Ano96b, Ano97c, AMP99, Ata99, BS99a, BP98a, BR96a, Bas98, BGM97a, BGM97b, BL96b, BL96a, Buc91a, DGV92, FCD98, GLC98, Gl99a, HEQL98, KM98a, KAK96, KB92, LC99, Lei99b, LD99, MT99b, PSE97, PA98a, PS93b, Por98, Pre97a, PRB98b, PRB98a, QG90, RS99a, Sch94g, Sch94j, Sch94e, Sch96a, SW97a, SW97b, Sch94h, Sch97, Sot98, SB99, Sip95, Ste96, VCF+90, AA95, Ano90, CPPK98, CMM93, CJL+92, CadHSV96, DG96, DN95b, FR95a, GP97, HJ99, HP94, Imp92, KKL99, MS99e, O891, O892, PV96, QN98a, Sch91b, Sim93a, Tab94, TY92, Tay90, TV94]. **Alive** [BK90]. **All-Or-Nothing** [Riv97c, Ste98b, BMM99a, BMM99b, Boy99, SRY99]. **Alleged** [Go97d]. **Alley** [KR96a, PRB98b, Sch94f, Sch95a, Sch95b, Swa94]. **Alliance** [Gar97c]. **allied** [IPNdbbprm91, AK99]. **ALM** [CH99b].
Almost [AMP99, Bra95d, CCD99, Mau90].
along [BDC+95]. alpha [Zim96a, Zim96b].
alphabet [PS97]. alternating
[HSW94, Wer93a, Wer93b]. Alternative
[BdM94, Gar97a, Neu94, Smi93b, VlT97,
BR96b]. alternatives [FL93]. Alto
[ACM98a, IEE98a, IEE98b]. Always
[Bra95d, Cha99a]. am [LC95].
Amazing [GC97]. America
[HK99c]. American
[Acc97, Bur99, Gla99b, Joh95, Mor92,
Moy98, RK98b, Web93, Yar90]. Amiga
[DDJ98c]. Among
[BDPR98, Sch92b, Oka93a, SS95a, SZZ95a].
amounts [Ped95]. Amplification
[ABDV98, BBCM95, MW97, CM95, Di 99,
Di99]. Amsterdam [Cha91].
Analog
[GD59, NT99]. Analogue
[Dem94, Cao99, SS95b, SS95c]. Analogues
[LP94]. Analyses
[SMK98b, BJDH97]. Analysis
[AO96, AMP94, BKS99, BR97a, BP98c,
BS97a, BPRF99, Bro94, CM97b, CJRR99a,
CRYY99, CH99b, DD99, Dra98, FM98a,
FY95b, GS97, Gue98b, Gsu96, Kea99,
KSF99, Knu94b, KJ99, L197a, Lei99b,
Lv98d, MM99a, MT95, MDS99, MO99,
NA95, Pab99a, PB99a, Pre93a, PJ99, Sch99k,
Sha99a, She99a, SVB96, SW93, VN94,
WS96a, WS96b, WS97, WB92, YMWP99,
Y96, AA99, Abr97, Bar91, BCK98, BM95,
Cha94b, Dan97, Don98, LM96, LLG10, Nas94,
Pau99, PS98h, RS93, RS99b, Tha91, vT94].
Analyze [MOM91]. Analyzing
[Gi197, KAK96, NT93]. Anchoring
[CS99]. Ancient [Paa93, RRP97]. and/or
[Sim90b, Sim91]. ANFIS [ZHIJ98]. Angeles
[IEE98c]. Angiograms [BALS99]. Anglo
[Gl99b]. Anglo-American [Gl99b].
Anguilla [Fra99, Hiri97, Hiri98]. Animated
[HE98]. animation [HEG98]. Ann
[Dob95b]. Anniversary [CFK+91].
annotating [DSSZ99]. Announcement
[Ano99b, Nat92b]. Announcements
[Ano95f, Ano95d, Ano95e, Ano97e, Ano97f,
Ano97g, Ano98a, Ano94c]. Announces
[Got99, Ano97u]. Announcing
[Ano97h, Nat97b]. Annual
[ACM94a, ACM97b, Ano95, Bri92, Bri93,
CH96, Cop95b, Cop95d, IEE92h, IEE93c,
IEE94b, IEE94c, IEE94f, IEE96a, IEE97b,
IEE97f, IEE98a, IEE98f, IEE99a, Kra98,
Sp95, St93b, St94, USE99d, ACM90,
ACM91, ACM93b, ACM94c, ACM95,
ACM96b, ACM97c, ACM98b, ACM99b,
ACM99c, Com96, Des94b, IEE92d, IEE95c,
IEE971, Kal97c, Kof96, TM99, USE99e,
USE96f, USE98c, Wie99]. anomalous
[GLV99]. Anonymity
[BD99a, DFT97, FJ98, JMP+98, STS99b].
Anonymous
[DF98, DF99, FT99b, GGMM97, Jae96,
Jae96, MS99a, OKST97, PW97a, RSG98,
STS99a, SPH99, SGR97, Pf95].
Anonymously [Coh96]. ANSI
[Ano94b, Ano96c, Bak92, Bas98, BK98a,
BK98b, Jop99, SS97]. Answer
[WD99a, Ude98]. answers
[Di 97a, Fre94, Ano92a]. Ant [BP95a]. Anti
[Ano93a]. Anti-counterfeit [Ano93a].
Antique [Mer90b]. antitrust [Ano97q].
Antivirus [Nac97]. Anttonio
[ACM99a, IEE92b, USE98d]. Any
[BM92, BJY97, DDP90, FJM+96, ZMI90, Beu94,
DF93, DKKK98, DI99, HILL99, Pet98].
anyone [Ude98]. AOL [GC97]. Apache
[Bal99, Mee98]. aperiodic [Fri92b]. API
[Gar98b, Got99, Lin96b, McM96]. APIs
[Gol96c, Gou98]. App [AW99]. Apparatus
[SKB99, MM99]. Apple
[Gar97a, GO96c]. Applet [Ber97a]. applets
[GPO98, GPO98b]. Appliances [Got99].
Applicability
[KCCT94a, KCCT94b, HKM95]. Application
[IBM93, BS99a, BSN95, Bar99,
BGG95, BL96b, BL96a, Dam90a, Dam91a,
Dav91, De 95, ECM96, FJRS96, Fun97,
GPT91a, GPT91b, Gog99, QG95, HNSS99,
HHY93, Hat97, Heli94, Hof99, IRM93, IR99,
JDK+91, KMPS99, KP99a, KL96, KK95, LO99, LC99, Mar98a, Man96b, Mun91a, Mun91b, NC97, PSN95b, QV90, QG95, Rog95, Rue93, SSS98, Sch99i, SZ93, SK98c, SK98b, SKIT99, VDDR99, Ara93, BY93c, BY93b, CC98, DDB95a, DDB95b, DF97, GZ91, HL97b, MW94, Nyb98, Pet91, PKM97, Si93b, SRR98, Siu99, Ste99b, SW98, SW99a, TY92, Woo90.

Applications [Aga92, BGR98a, BFW99, CG98, CJR98a, CJR98b, CO93, Cre90, Dan96, DY91a, DFGH99, Duf98, DN94, Dwo97, Ebe93, FMM99, Far93, Fis98, IEE95a, EIE97a, EIE99b, EIE93c, EIE94c, EIE97b, JMS96, KSHW97, KSHW98, KSW99b, KSW99c, KM96a, Km94b, KT91b, Lan97, MS95f, OdP98, Oo90, PS96b, SY96a, DY91c, TN96a, TN96b, VV98, VP96, ZY91, vW94, vW99, ACM99c, Ada91, Ano98b, BM90, Ber93, BMF+97b, BV97, Boy98, BP97b, Com96, CFG96, DiPS96, Duf94, Dom96, Eng99, FO98, GvP98, Gre94, GS94b, HMP95, JY98a, Kat95, KW92, KQ93, LY93, LN94, Lub96, Me92, Mic97, MT98, NKC94, Ped91a, PC98, Rhe95, Sch90c, Sch97c, Sha95a, SSM94, Sin95, Sta97c, SGG99, T9+98, USE96e, Way98, YL93, ZY90].

Applied [BHJM99, HH98, MR95a, Sch94g, Sch96a, Sha99a, FFW99, FMR99, MV97, PR98, CMM93, Dav94]. apply [Cli97, UU97b]. Applying [CO98, HO96, Jan99, KMPS99, MW98a, War98, ARR99].


Architecture [IBM93, BCCD99, CJR98a, CJR98b, Con99a, Fei93, Fei96, Gut99, JDK+91, MM99b, Mu93, NH90, NK98b, Oh99, PF94, RBv94, Rus90, SSS90, She92a, She93c, Tre99, Tua99, VGG93, YSS99, Kar96, LSS98a, Con98, JD91, LM99, SV99, SY92].


Arithmetically [De 98d]. Arizona [IEE99b]. Army [Mea98, Mye98, Dar98a, DR99b, Ros99].

Arnoldi [HRVV99]. Array [MT95, DF92]. Arrays [BS94, BSG96, BKK98, MT95, TT99, JM93]. Arresting [Mad92]. arsenal [Me98]. Art [Eri99, Lan98, NM96a, Pre98c, She92e, BFS92a, BFS92b, Ben94, B+96b, PGV93d, PR98]. article [Bur98b]. Artificial [Ano96l, BTV99]. Arts [Tv92]. Asia [Uni98c]. ASIACRYPT [IRM93, KM96a, PSN95b, PSN95a].
Asimov [CFK +91]. asking [MILY93].
Aspect [LL99]. Aspects [Des98c, Sch98b, Ved93, ZTR99, Kob98b, Lid90, Pos98].
Aspray [CFK +91]. Assessing [MILY93].
Assessment [EN98, ENK99, FL93].
asset [Oko97].
assign [LL93b]. Assignment [Hwa97, RH99, GPSN97].
Assistance [IS91, HY93a, Wu92].
Assumption [Sak96, Sal98].
Assumptions [AB99a, AB99b, BD91, KRS99, NOVY99, Oka93a, Sim98c].
Assurance [IEE94b, IEE96d, KY92].
Assuring [Car95].
ASYNC [Dan97]. Async [Hwa97, RH99, GPSN97].
Asynchronous [AMP99, TY94].
Asymmetric [BWM98, FO99b, Jak99c, JM96b, Pat96, PG97a, PG97b, PS96a, PW97b, The95, BR94b, BR95a, MI90].
Asymptotic [SOB98].
AT&T [SSM94]. Athena [DS90b].
Athens [Kat97]. Atlanta [ACM99b]. Atlantic [Bra94b].
ATM [PS98c, PS98d, PS98e, PS98f, PS99a, PS99c, PS99b, PS99e, THP +98, VSH97]. atomic [BBS98b].
Attack [BF97a, Ber97c, DBB91, BDF98, CG99, CS91, CLE99, Cop94b, CS98b, DBR +99, Dob96b, EH96, G91, GC91, GC94, HK99c, JK97, KSW98a, KSW98b, LA98, Lvd98, Mae98, Mis97, MSK98, OM94, PBGV90, RS91, SMK98a, SK98c, SK98b, TOU94, Wag99a, BP98c, BB95b, BK95a, BJ979, HA94b, Hor98, JG95, Kuhl98, KOT95a, KOT95b, LZ90, Lou91, Low95, MRS99, MY99a, Men95b, Mi90, RS98f, SNT93, SG98, SGSD99, d91, vOW91].
Attacking [La98].
Auditing [ST99a]. Auditing [SK97c].
auditorialization [HW91]. Auditorium [IEE98b].
Aufenthaltsort [FT95].
Augmented [BT98, KT98]. August [B +96b, Bri92, Bri93, BS95e, Cop95b, Cop95d, Des94b, IEE98b, Kai97c, Kob96, KP99b, Kra98, MSD90, Nat98, RD99a, Sti93b, Sti94, TM99, USE90, USE98a, USE98b, USE99a, Wie99, Yau92].
AUSCRYPT [SP90, SZ93]. Austin [An94d, IEE98e].
Australasian [VPM97].
Australia [DG96, GN95b, KG93, KK99b, MSD90, PS95b, SP90, SZ93, VM97].
Austrian [CFK +91, GN95b, Cae96a, On96]. Austria [BS95e].
Authenticated [BF97a, BWM98, BWM99a, Bor95, CHH97, Dan95, HCY96b, JV96, LC97a, Mau97a, RH93, SKWH96, BSN96a, BSN96b, BF99b, BR97b, DvW92, HY98b, HY98a, Ye99].
Authentication [ADSW99, He98a, KS99a, MIT92a, SK96a, LC94]. Authentication
[ABKL91, ABKL93, AGS97, ATAY98, ADKN90, AB99a, AB99b, Ano94j, AS96, Atk95a, AR98, AC97, BA97, Bak99, Bal99, Bec99, BR97a, BG90, BR990, BCK96d, BCK96e, BM91a, BGS98, BR91, BBDF97, BGH+91, Bis91, BHK+99, BWM98, Ble98b, BV98b, Bor96, Bor93a, Bor93c, Boy92, Bru98, BAN90, CV93, CGM97b, COZ99, DL97, DVPL92, DVW90, DY91f, DvW92, DH90, Dra99, DMFB97, DS97d, Dwo95, ECM96, EPR99b, EPR99a, FGS96, FHBH+97, FL96, GHY90, GLZ99, GL96, Geh94, Geh95, GN94, GM90, Gol90a, GBL94, Gu98b, Gui97, HK97, HA94a, HS94, HL92, Hill97, HJP97, HP98b, Ins95, IH98, JS94, Joe98, Joli94, KR95b, Kau93, KA98a, Koh90, KN93, KCC94a, KCC94b, Kra94b, Kra95, KBC96, KBC97, Kur94, KK95, KY92, KY92, KS97c, LABW91, LABW92].

**Authentication** [Lee96, LW91, Lie93, Lin93c, Lin93a, LS92, MB94a, Mau96a, MAM95, McM96, Mee98, MS95c, MS95d, MWW94, MTV92, Mor97, Mye94a, Mye97, NP97, OOK91, OM94, Opp96, PKOT94, PS98c, PLWSN99, PSN91, PGV93c, Pre98a, Pre98c, MS95e, RS99b, RRSW97a, RRSW97b, Rog95, SNT93, SN93, ST94, SNT95, SN98a, SN98b, SSH93, SS96, SP99, SA95, SC96a, SCx, Sch94d, Sch99k, Sga90, Sga91b, She97, She95a, Sho96, Sim96b, SVW91, SW94c, SKAM99, Sti91b, SL99, TAP90, Tay95, TSN93, Tun99, Ude98, Van95b, Van93, Wal95, WKHG97, WK96, WABL93, WABL94, WL92b, WL92a, WL92c, Wu96, Yu94a, Yu94b, ZG96, AG95, ABC+98, Ano97d, Atk93, BSN97, BGR95, BCK98, BCKx, BCB97, BGH+95a, BO99, Car94, CW97, CGM96, DS90b, DS93, DH96b, Gu90, HS96b, Hor95].

**authentication** [HC95b, HLL+95, HW98c, JC98, JG90, KC95, KW92, KNT94, KO95b, LC96a, LL95b, Lin88a, Lin89a, Low95, MS97, MF97, Men91, MC96, Nac93, NT94, PS98e, PS98f, PS98h, RS98a, RS98f, Sch99j, Sga91a, Sga93, SY96b, Sta99b, Sti91a, Sun98b, Syv93, Tsu92b, Tsu92a, TH99, Ver98b, WL94, XA98, Xie98, YL97a, YL97b, You97, Zuk98b, ZH93, vT93, Mye94b, Ala93b, Bor93b, WL92a].

**Authentications** [OO90, KSL92].

**Authenticator** [Zuk98a].

**Authenticators** [DF91a, SN96].

**Authenticity** [BK90, Lud97, M90, Way91].

**Authentcode** [Fly97].

**author** [Lea90].

**authorisation** [COZ99].

**authorities** [Ame95, Ame96a].

**Authority** [CFSY96, CGS97, JMO95a].

**Authorization** [BDPSNG95, Cas95, FL96, WOO90].

**Auto** [YY98c, YY99b].

**auto-certifiable** [YY98c].

**Auto-Recoverable** [YY99b, YY98c].


**Automated** [Dan97, FIP93a, FS93, FK99, GSN94, GD91, She96a, SGF98, VDDR99, WGG99, CD98a].

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

**Automating** [Bur99, Smi93a].

**Automation** [Des99a].

**Automaton** [DGV93, Gys96, DW96, MZI98, Tao94, TCC97, TC99b].

**automorphisms** [VP96].

**Autonomous** [CKN99, RZ99].

**autoscritcher** [Dea98a, CF92, Cra92].

**aux** [Bec90].

**Available** [DDJ98c].

**Avalanche** [Cas95, Gys96, DW96, MZI98, Tao94, TCC97, TC99b].

**average-case** [AD97, AD99].

**Avoided** [NMR95].

**avoiding** [ZM96].

**Award** [Pin98].

**Awarded** [DDJ98b].

**Awards** [Eri97a].

**Aware** [BCCD99].

**Away** [DDJ99].

**Axis** [AK99].

**AXYTRANS** [GBC93].

**azo** [SBTV99].

**b** [C197, UU97b, Ano99e, HS90, Lam99].

**B-Trees** [HS90].

**ba** [IPNdbbprm91].
Babbage [Fra93]. Back
[GC97, GO96c, WSFC99, IEE97e, WG97].
Backup [Mah96]. backwards
[BKR98a, BKR98b]. Bacon [Lea90]. Badge
[WHFG92]. BAG [Ano97]. Baker [PS96b].
Bal [IPNdbbprm91]. Balance [RG99].
balanced [MCD98b, YT95a, YT95b].
Balatonfured [Rue93]. Ballot
[CFSY96, BT94]. Ballots [Sal91].
Baltimore
[ACM90, Ano96a, NIS92, USE92b]. Ban
[Gar97a, BP98f, ZZZ97]. BAN-like
[XZZ97]. Bandwidth
[Bla96a, Bla96b, JMP98, MM92b, Sim98b].
Bandwidth-Efficient [JMP98]. Banking
[Ch92]. Barbara [Bri92, Bri93, Cop95b, Cop95d, Des94b, IEE97f, IEE97g].
Bargaining [Nur94].
Barriers [Des92, RCM99]. Based
[AW94, ADEDS99, BDPSNG95, BG90, BJY97, BS99b, BS99c, Ben99, BLM94, BBT94, BMT96, Bie98, BPR99, BMS94, BM96b, BM96c, Bie98a, BPR99, BMS94, BM96b, Bie98a, BPR99, BMS94, BM96b, Bra95b, Bie97c, CJS91, Cres97, DGV93, Dau95, DNM98, DSS99, DS96, DPP0, DMPW98, DDGM97, DQ94, Dem94, DF99, DK97, EKL99, EN98, ENK99, FCH99, FBS97, FK99, FKMY98, FJM96, FB98, FR95d, GKR97, GK97, GKR99, GRB99, GNC5, GNC96, GNC96, Hac97, HPS98, HJ97, HO97, JIA97, JIA99, JSS94, JSS94, KKS97, KAL98, KR98, KIM93, KG95, KP96a, KP97, KM99b, KAK99, KMOV91, KRA94b, KH98b, LM93a, LM93b, LLY93, LLY97a, LNN99a, LW91, Lin98, MNSV97, MD99, MR95a, MTA93a, MM96a, MM99b, MM99b, MG91, MG98a, Mue99, MM98b, Mui99, NM95, NM99, NOV93, NS98a, Nse96].
Based
[NS97b, NMV98, OMV98, OO93, OFF93, vO91a, Pau99d, Pen96, PL94, PRZ99, Poi99, PB99a, PV98, PK99, Pre97a, PMP99, RSA99b, Ros98a, SS98a, SCT99, SC96a, SPS97, SE96, SJS98, She92e, Sho96, SH96, SM91, ST91, SSN99, SKIT99, SZT98a, Var99b, WSC95, WD99b, WS99, YKB94, Y)L97b, ZL99, vO91b, Ala93a, AW95, ALe98, AAPS92, BSN96a, BSN96b, BSN97, BDD97, BDC98, BSB97, BCD98, Bea97a, BBI90, BCB97, BMP97a, BBL95, BFKL94, BCC99a, CPS95, Cha95a, CW97, CS97c, CCH98, CLL99, CD95, Cus95, DDr95, FSS94, FY96b, FY96a, GM91, GH99, GK95a, HZ93, HY93b, Has99, HSW96, He92, H97, HLM93, HWMW94, HMP95, HW98a, HJ97, Hwa92a, Hwa92b, Hwa92c, Hwa93, IS99, JJ95, JG95, JG90, JY98, KM99a, KSL92, KM99d, Koy95, Kuc92, KH97].
B {
[CK96, LWR93, LdLB96, LS98a, LWW99, L90, LCL95, MRS99, MS98a, MLA91, Mau91b, MCh92, M98, MM95, MTN97, Mu92, MVZ98, NS97c, NR95, OP95b, OU98b, O95, Pat91b, Pat91a, PSB97, PC98, PGCSN96, PBBC97, Por93, PG91, PG93b, PG94, RP95b, SV95a, Sha94, SRRL98, Sim98c, SM90, SS95b, SS95c, SMK98b, Son99, SK94, Ste95, SS98b, SZT98b, Tan90, TA97, TAP90, TC91, VN99, Ven92, Wan92, WK97, W95, X98, YWC97, YLM97, Zhe95b, ZPY96, vO92, vT94, CD96, KY99, Dhe98, Por93, TY98b, TY98a].
Bases
[BCE94, MDS90, Yua92]. Basic
[CF99, Des98a, vdL98, OK98, YHK99, Zie97, van98, BD97, Rac90, dVD98, Hel98b].
Basics
[Ba99, IEE97e]. Basis [FBS98, LL99, The95, Wal98, BK98s, Car98, FBT96].
Batch
[BGR98a, BY93c, BY93d, BFP99, Fia90, Fia97, BGR98b, YL95a]. Battle
[Ban93, Gar97a, Gar97b, Gar98b, SB97, Fro96]. battleships [Jar97]. Bayesian
[BBDF97, Jen99]. BCH [CC98, FC94]. Be
[BF99a, BV98c, Cha93, CD98b, DY91f, EvH91, GSV99, NM95, Way93c, Ano90, Ano95c, Ano98b, CP91, Cis95, Ev92, Ev93, LF97, NMV95a, NMV95b, NOY93, Ros98c, Sch91b, Sim98c, van97a]. Beach
YLCY98b, CFK+91. **Byte-Oriented** [Mas94, YLCY98a, YLCY98b]. **Bytes** [Yuv97]. **Byzantine** [Bea92, Bor95].

C [Sha99a, vdWS97, vS97, Bak92, Bas98, BMS99, DSB99, Gar98b, Hei98b, Kal92, MGL+98, Sch94g, Sch96a, Sch94h, Ste90a, Ste90b]. **C0YNTHIA** [WBB99]. **C2** [Ste92]. **CA** [RD99a, Cop95b, IEE93a, IEE98c, SJ97, USE93, USE96g, USE96b, W199]. **Caching** [STSW99]. **Cactus** [Ano97a, CADE [HB99]. **CADE-16** [HB99]. **cAESar** [Koe99]. **Calculating** [CFK+91]. **Calculation** [HRVV99]. **Calculators** [CWM+91]. **Caching** [STSW99]. **Cactus** [Ano97a, CADE [HB99]. **CADE-16** [HB99]. **cAESar** [Koe99]. **Calculating** [CFK+91]. **Calculation** [HRVV99]. **Calculators** [CWM+91]. **California** [ACM93b, ACM98a, Ano97a, Bri92, Bri93, Com96, Cop95d, Des94b, FJV97, IEE92c, IEE93b, IEE94d, IEE95b, IEE97b, IEE97h, IEE97l, IEE98a, IEE98b, IEE98d, Kal97c, Kob96, Kra98, Nat98, RP97b, Sti93b, Sti94, USE92a, USE96c, USE96d, USE96f, USE99d, Vie99, van96, Sch98b]. **Call** [VCF+90, Zav99, Miy90]. **Call-Coverage** [Zav99]. **called** [Way95]. **Cambridge** [And94a, And96c, CFK+91, Chr99b, Gol96d, Lom97, RBCE99, Sch94j]. **came** [Fro96]. **Camera** [Fro96]. **Camera** [Fro96]. **Campbell** [CFK+91]. **Campbell-Kelly** [CFK+91]. **Campus** [VNW94]. **Can** [Ano93c, BF99a, CF91, Cha93, CD98b, CMYY97, DY91f, EvH91, GS99, NMVR95a, NMVR95b, NMVR95c, Riv98b, Sim98c, Ste95, BG97a, CG05, Ev92, EvH93, LF97, NOV93, Sch91b, Ude98, Way95]. **Canada** [ACM94c, CFG96, GS94b, IEE94f, IEE96d, TM99, Yua92, Rob98b, Tah98]. **Canadian** [CFG96, GS94b]. **Candidate** [Bas98, BCA+98, Dra98, GLC98, Gla99a, Hub98, KMA+98, Nat97b, Nat98, Nat99b, Out98, RD99a, RD99b, Sot98, SB99, GGH+98]. **Candidates** [Bih99c, Cla99, HKQ99, Koe99, Roh99, Sha99b, Vau99d, CJRR99b, Kea99]. **Cannot** [BCE+94]. **Can’t** [WT99]. **Cap** [Lea99]. **capability** [BC96a]. **Capacity** [Bih99, FVEA99, Gar97a, Gar98b, MM92a, NNEK97, VN95, Uni96a]. **Capstone** [YY96]. **carcinogenic** [SBTV99]. **Card** [Bov98a, Bov98b, Chr99a, DQ96, EN98, ENK99, Gar97a, GPSV98, HP98a, Hru96, HH99, Hus99, Kra99, Mar98a, Omu90, SG9V98, Sut99, T+99, wQ91b, wQ91a, AHdJF97, Cha99b, CW97, Cha91, Di 97a, Di 97b, Kip97, Sha95a, Ta98, GPSV98, Bar99, Bro97, HNSS99, SM94, SKAM99]. **Cards** [Ano96j, Ano99d, BDB92, Cha99a, CM99c, Con98, Con99a, Cor98, CH99a, DD98d, DD98d, DDJ98d, DDJ98d, Deu97, Deu98, Fan96, FW91, FGPL96a, FGPL96b, FOM91, GL96, Gut98a, HKQ99, JT97a, Koe99, KCCT94a, KCCT94b, MSN99, Mye96, NM96b, PV98, Roh99, SKW+98c, SS99a, Sch90b, SR96, Smi98a, Ta99, VV98, ABKL91, ABKL93, Ale97, Ano98h, BG97a, Bro97, CJRR99b, D98a, Dhe98, DT98b, DF97, Gau97, T97, AG99, BK99, BFF9a, Gir99, GSY96, LW99, NF99c]. **cardT0AP** [SGPV98]. **Carmichael** [Pin97]. **carrier** [SVWMB95, SOB98, VSB95]. **Carry** [SM91, DF92]. **carry-save** [DF92]. **Cartesian** [DVW90]. **cascade** [BCK96b, BCK96c, YL93]. **Cascades** [GC90, Men95b]. **Case** [ABDV98, BY93a, BGG94, BR95b, BGM97a, BGM97b, BPR99, DSSB95, Du90, FL99b, FR95d, GR99b, GM99a, LBHM99, Mad92, MD99, MR95a, Mar98a, PK99, Riv98c, Var99b, AD97, AD99, BHH99, DL93, LMS97]. **Case-Based** [DSSB95, FR95d, GRB99, MD99, MR95a, PK99, Var99b]. **case/average** [AD97, AD99]. **Cases** [BMC95, Blo99]. **Cash** [BFP99, Bro95b, Cha93, DFTY97, DT98a, EN98, EN99, F097, Jak99b, LR98, NMV98, OO90, TGS99a, TSS99b, Tra99,
Checkers [Fis97, KA91]. Checking [BGR98a, Bol98a, Bol98b, BDL97, FL99b, FGY96a, GMV98, PV98, BCR98, FGY96b, MHPS96, MW94]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [BGV90, LRW93].

Checking [BGR98a, Bol98a, Bol98b, BDL97, FL99b, FGY96a, GMV98, PV98, BCR98, FGY96b, MHPS96, MW94]. Checks [DT98a, PK95a, PK95b, Pen96]. Checksum [BGV90, LRW93].

Chen [Ala97, Bur94a, Bur94b]. CHES [KP99b].

chi [XtTmW94]. chi02 [HG97a].

Chi [Ala97, Bur94a, Bur94b]. CHES [KP99b].

China [HOQ97, OiDP98, XtTmW94]. Chinacrypt'94 [XtTmW94].

Chinese [DiDPS96, GO96c, QD91, WWH95, Yu99].

Chip [Ban94, Bro96, Ele98, Gar97c, GC97, Got99, HMvT94, Lan97, MPPS95, MHMW98, VVDJ90, Way93b, DVQ96, Kan96, Moc97, Pos98, RVD94, Sm94a, Un95a].

Chipkarte [Kip97, Kip99b].

Chips [Ano99c, GO96c, Omu90, Ano97-27, IEE98b].

Choice [Cha99a, Way98]. Choices [Hon98, Van95a, We95b].

Chosen [Ble98a, CG99, CS98b, Dam91b, GC94, KSW98a, KSW98b, LL94a, PVG90, RS91, ZS93, BJQ97, CP94, NY90, SNT95, Sah99, SG98, Tze99, vT93].

chosen-ciphertext [Sah99].

chosen-content [SNT95]. chosen-message [BJQ97, Tze99]. chosen-plaintext [vT93].

chronicle [UFC94]. chronology [Kah98a].

Chua [YWC97]. Chump [Wal99b].

Chung [XtTmW94]. Chung-kuo [XtTmW94].

Church [Ole95]. CINDI [DSS99]. Cipher [Alv98c, AM97, ABK98b, ABK98c, BKR94, BAK98, BD94, Boy90, BCA98, Car97b, Cla97, Cla98a, CJM95, DGV94a, Dae95, DKG97b, DKG97a, DW94, EM93, Gol97d, KR94a, KMA98, Knu98c, KR99a, Kuh98, Lim98, LS97, Lip99, Luc98a, Luc99a, Luc99b, MNSV97, MD98, Mat94b, MT99a, Mau91d, Mil96a, Miy91, MSK98, MSK99b, PA98a, QG90, RDPB96, RSY98, Ros98a, SZ96, Sch94b, SK96c, SK96d, SKW98c, SKW98f, Sch99d, Sch98i, She94b, SM98a, Van98d, WBDY98, Y996, YLF98, YLC98a, YLC98b, ZYWR91, Zhe97a, Lip98, Bar92a, Bar95, BK95a, BNP97a, BS95a, CS96b, CS97b, Cra92, Dav98a, Dav98d, Dav98c, Daw96, Fra93, Gad98, GGH98, Gol98b, Gol98b, ISO97, Kru98, Lew92, LCL95, Mac98, Mat93, MY93a, Mei94, RT93, Sel98b, YL97c, Zun98, SV98, Ers99, Van99b, Van99c].

Ciphering [DN97, CN95c, Mas94, Nor95a, Nor95b, NO96].

Ciphers [Ada97a, ABDV98, AAG97, AB96a, BR99a, BR99b, BDR96, CD90, Cha94a, CS91, Cle91, DR99a, De99, Din94, Fil95, Gau96, JF97, Jak98, J99b, KSW98a, KSW98b, KSW98c, Knu94a, Knu94b, Knu99b, Kob99, LMM91, LM93a, LM93b, Lnu99, Lnc93, Lnc96b, Mat96a, Mau91a, MS91, MT99c, PR99, Pat99, PK95a, PK95b, Pen96, Pra97a, Pre98, RP97a, Rob95a, Rob95b, Roe94, She94a, She94d, SM91, Van98b, Vau99a, YY98d, YY98b, ZM990, Zhe90, Abe98b, BKR98a, BKR98b, CD98a, Cot99, DGV94b, DXS91, FSN93, Gar96a, Gar97d, GSN94, Gol95b, Har96a, HLM93, HX94, J99a, JV98a, Lai92, LMM92, LRW93, Ny95, PVG93b, PV94, Rev91, RP95b, Roe95, SB95, SAM97, Tay94, Win93, Wri98].

Ciphertext [BK98d, Bl98a, CG99, CD97, CS98b, Dam91b, LL94a, MRR99, Miy93c, RS91, Riv93a, TOU94, ZS93, CP94, NY90, Sah99, SG98, V95].

CiphertextOnly [BK98d]. ciphertexts [Des95]. Circuits [KT91b, KT98, W989, JS93a, LMS97, YWC97]. circulating [Ano96].

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

CISST [AA97]. City [IEE99a, USE95b]. Claim [GO96c]. Claims [DS97a].

clandestine [Wri98]. Clara [USE93].

Class [vD97, Ou99, Un96c, FR94, HEB93, KSB96a, L929, LZ91a, ZUK98a, vT94].
Classes [Haw98b, Pai99d, Haw98a, Sze98].
Classical [Bra94a, MC92, Nic98a, Nic98b, CD98a, Mas99a].
Classification [BD90, LSVV95, PNFK95, Unic96c].
Classifier [CIBM99].
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].
Climate [TGKI99].
Climbing [MCD99].
Clipper [Pri94, Fro96, Ban94, Bro96, Hof93, Kan96, MS95f, Smi94a, Uni95a].
Clipper-like [MS95f].
Clipping [Hof93].
clicks [JP96].
Cloak [Gre90].
Clock [DHSS95, GO96b, GM91, GO95, Men95b].
Clock-Controlled [GO96b, GM91, GO95].
Clocks [DG95, DGT96, Yah94, Gon92].
closer [Coh96].
closure [MOM91, PS93a].
Clueless [RS98c, RS98d].
Clustering [DDJ98a, HE98, Kuni97].
CM [CNST98, Kob91a].
CM-curves [Kob91a].
CMOS [BS95c, ECD+99, YSS99].
Co [Gla99b, LFCK99, Sut99, NM96a].
Co-dimensional [LFCK99].
Co-operation [Gla99b].
Co-Processor [Sut99].
co-processors [NM96a].
C. [CFK+91].
Coast [SZ93].
COBOL [Gar93].
Code [CJ99, HR90, JJ99a, Kip99a, Kur94, MV93, PV98, QD91, Sch94g, Sch96a, Sch94h, Str95, Tod97, WK97, WF94, Zim95b, Al97, Ano97i, BSNP97, CC98, CLW98, GA98, HM97b, LJWH97, Rey96, Rey97, Rey99, Sin99, SH94, WS96c, Zim96a, Zim96b, AAG+00, Mea98].
Code-Breaking [QD91].
code-cracking [WS96c].
Codebreakers [HS93, Smi98b, Yu99, Kahl96b].
Codebreaking [Car97c, Car98, Dre92, Sch98a].
coded [HG97e].
codemaker [Mar98b].
CODER [Sto90].
Codes [ACM94b, AW94, AR98, BGS96, BVFD99, CCZ98, CS96a, Cha99c, DLR97, DR99b, Far93, GN94, Gib91, Hof99, Joh94, JS95b, J99b, KKS97, KP96a, KP97, KK95, LC99, Mor98, OM94, PLWS99, Pen96, Pra96, Pre98a, RV99, Rus93a, SN93, SNW98a, SNW98b, SD99, Sga90, Sga91b, SB94, SVxW91, Sta96b, Sti91b, Ton96, Van95b, Wa98, Ada91, Al93a, AW95, BSB97, Bt93, Br91, CC98, Cha95a, CMM93, FC94, Gre90, J96a, Kah91a, KO95b, LYG94, LMS90, MSS93, MPL99, Mol92, SNT93, SNT95, SK94, Ste95, Sti91a, Su98, SS98b, TSN93, TY94, Wnn92a, Wn97, Wnn93, YL97a, vT94, JS95a].
codewords [PS97].
Coding [Ber96b, IEE97e, KRS99, KH98b, LW91, Lip94, Sch99b, She94c, SW95b, Van95b, Wa99a, Ada91, Boy95a, Boy95b, Dar97, DDP96, Far93, Gan93, KSB96b, KS97, Ku90, Mit92b, Sab94, Sch98b, Sqa91a, SVW95b, SOB98, Shp99a, SSS99, TA97, Ger97].
coefficient [GK95b].
Coffee [Den97].
Cognitive [CF99, Ger99b, MMM+98, PUF99].
Cohen [PBGV90].
Coin [BN96, Jue99, PW97c, Ueh95].
Coins [EO95b, WSFC99, EO95a].
COIRS [YKY99].
Cold [Joh95].
Collaborating [CF99].
Collaborative [BV98a, Neut91, LS98a].
Collaborators [Gla99b].
College [Far93, IEE97a, UFC94].
Collision [BP97a, Dob97, PGV91, Rus93b, Vau93, vW94, vW99, Dob95a].
Collision-Free [BP97a, Dob97, Rus93b, Vau93, Dob95a].
Collisionful [Gon95, BSNP96a, BSNP96b].
Collisions [Ano95a, C98, DBGV93, dB94, Gon95, Sim98c].
Colloquium [Ano97p, vWN99].
Collusion [BP95b, BS98, EKK99, PW97b, LM96].
Collusion-Resistant [EK99].
Collusion-Secure [BS95b, BS98].
Colony [BP95a].
Color [ADEDS99, NNEK97].
Colorado [Sch99b].
Colossus [Ano97-28, Car97b, Car97c, Car98, Pin98].
Column [Bra94a, Dwo95, Bra90b, Bra90d, Bra95d].
columnar [Bar92a]. COMANDOS [TCH+91]. Combatting [DN93].
combination [Rev91]. combinational [Hi9l9]. combinations [RT93].
Combinator [SAS99b]. Combinatorial [FK94, KO95b, KO95a, KO96, KO97, LS98b, 
Rus93a, Sti91a, Zie97, FSS94, Sta97a].
Combinatorics [MWW94]. Combiner [SG99a]. Combiners [MS91].
Combining [KMKH99, NA95, SA95]. command [Mye94b].
Comment [DKKK98, LC96c, YT96, BMP97a].
commentaries [Ano97t]. Commentary [BL99]. Comments [BMP+97b, COP+95a, 
Dum94, JW01, KSS+92, MC96, NC97, Ng99, Pre95b, SB93, WHL99, Ala97, Gib90].
Commerce [Avo99, Cli97, DDJ98d, DB99, 
Jakk9b, LHB96, Lut98, USE95c, USE96d, 
USE96b, USE98b, Uni97d, BH98, FB97, 
Gar97b, LM98a, Man95, Sin98, Tas98, 
VM96, UU97b, Uni96c]. Commercial 
[Bhi96, BDR+96, Cae96a, WLEB96, Cha94b, 
Dix94, Jol90, Sta94a, JML994].
Committed [DF99]. Committee [Uni98c].
Commodity [Bee99a]. Commodity-based [Bee97a].
Common [IBM93, Lin93c, 
Mau93a, Tzc99, JD91, JD91, LMJW93].
Communication [??97, AR99, BF97a, 
Bet95b, BFS96, CH9H9, CMN99, FJP96, 
FK99, FT99b, ICM99, Jam98, KFJP96, 
KRJ98, PW99, PM99a, SSN98a, Sim94d, 
WD99a, Wei99, BF99b, Bet95a, BMS96, 
Com97, CW98, CK93, Cli97, DFKN93, 
Hamxx, Rivxx, Sch90c, Sch97c, SD97, 
Sta97a, UU97b, Ven92, Wt98].
communication-privacy [CK93].
Communication-Storage [CMN99].
Communications [ACM93a, ACM94a, ACM97a, Ano93h, 
Aur96, IEE94f, IEE97k, KM93, Kat97, 
MB94b, Ved93, BY93c, BY93b, Car94, 
Cha94b, Cra96, HOQ97, Hwa93, IEE92d, 
IEE95c, JC93, Mil95, Oht96, PP96, Rhe94, 
SW94b, Sch93a, Sch92c, ZG96].
communicators [Ano97p]. Communities 
[MB99a]. Commutative 
[GPT91a, GPT91b]. compact 
[Ort95b, Ort95a]. companion [Ken95].
Company [GC97, Kar96]. Comparative 
[Dae99, Ste92, AA99, Don98, She92g].
Comparing 
[Bih99c, HSSI99, HKL94, KAK96, NM96b].
Comparison [BALS99, Cus97, KH98b, 
LM98b, Mas99a, May97, MG91, vO91a, 
QN98a, SKW+99a, SKW+99b, Wie98b, 
Wli93b, vO91b, GM91, Yeu99, ZH93, vO92].
Comparisons [Fo99, SKW+99c].
Compartmented [GPSN98]. COMPASS 
[IEE94b]. Compatible [SK94, Wat99].
Competence [WS99]. competing [Sta97c].
Compiler [NM99, SSCP99].
Complementarity [DD99, LM93c].
Complete [Tou91]. Completeness 
[Bro94, Sch94k]. Complex 
[NT99, MCD98a]. Complexity 
[Bus97, CH96, Cle91, DSV99, GM99b, 
HKL94, LMS99, MM90a, MS94, 
MM+98, Mun91a, Mun91b, NM95a, 
NMVR95b, NOVY93, Sch99, Smi98a, Bao94, 
CS97a, DDP94b, FK93b, GZ91, GN95a, 
Gol97c, Hi94, MM90a, SM98a, MK92, 
Shp99b, SMK98b, Sze98].
Compliance [Dav96]. Component [NK98b]. Composite 
[Fai99d, BBR99]. Composition 
[ABDV98, GK96]. Compositional 
[DHNP98, HJTW99, MM99a, Zwi98].
Comprehension [MT95].
Comprehensions [MT95]. Comprehensive [SPP90].
Compress [Dob97, Dob95a]. compressed 
[CPO+98, CHO+98, HG96, HG97c, HG98].
Compressing [G199]. Compression [C199, 
DLF97, KPR99, Sch99b, BCR98, CW94, 
Cra96, Kop97, Oht96, Sab94, Sch98b, dB94].
Compromise [Gar97c, Hed97].
CompuServe [GC97]. computability [BK98f]. Computable [DSV99].

Computation [BMM99a, BMM99b, CH98, Cra99, FHM98, FH94, GM93b, HHT93, HHT97, HCY96a, KR94c, LO91a, LYH93, LL95a, Mon93, Mor98, PK95a, PK95b, SSN98a, Wat91, ARRW99, Ata99, BK90, Ber96b, Bre99, CWM91, COL94, GM95b, Hor98, LY93, MILY93, PW93a, Shp99a, Xie92].

Computable [BMM99a, BMM99b, CH98, Cra99, FHM98, FH94, GM93b, HHT93, HHT97, HCY96a, KR94c, LO91a, LYH93, LL95a, Mon93, Mor98, PK95a, PK95b, SSN98a, Wat91, ARRW99, Ata99, BK90, Ber96b, Bre99, CWM91, COL94, GM95b, Hor98, LY93, MILY93, PW93a, Shp99a, Xie92].

Conceptual [Ch96, HHL94, Kos97, KR999, PG90, Saba94, TJK99, BC99a, Ger99b, McC90b, Pom90a, SS95a].

Computational [CH96, HKL94, Kos97, KR999, PG90, Saba94, TJK99, BC99a, Ger99b, McC90b, Pom90a, SS95a].

Computations [Cha90, CDD99, Mas91].

Computing [ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, ACM99a, ACM99b, Bak92, BDDG99, BV96, Bra94a, CFK91, DDJ98d, DDJ98b, DDJ99, Dwo95, FP99, GC98, GN95b, IE94e, IEE96b, J998b, Kon95, Law98, MMM98, Mao94, MW99, NS98a, Pen96, RS99d, Sch94a, TK99, Tes98, USE96c, VMS97b, BGT96, CWM91, DDPS96, FM91, FJV97, HK99b, HC95a, KG93, LS98a, Pf97, Sch90c, Sch97c, VMS97a, CFK91, PH91].

COMSEC [Mye98]. concatenated [LYG94]. concealed [Ano97i, CZ90, Lea90].

Concealing [CD97, Bent94, Jo97b].

Concept [Lin98, GM91, HLC99, YKY99].

COncept-Based [YKY99].

Conception [BFW99, Des99a, HL99, KG99, Lan98, SSM90].

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

Conciliation [BBDF97].

Concrete [CO98, BCK96c, BDJR97].

Concurrency [SG99b, IEE94b].

Concurrent [BMT98, DO99, DS98b, RS99c, Zwi98, AR99].

condition [Sta96b].

Conventionally [Des90b].

Conducts [Law98].

Conference [ACM93a, ACM94a, ACM97a, AR97, Ano95l, Ano96i, Ano96a, ??97, Ano97f, Ano97g, Ano97a, Ano98a, Ano99a, AA97, BCB97, Boy95a, Bri92, Bri93, BS95e, CH96, Cha91, Cop97d, DDJ98a, Dau96, ES98, Far93, Fra99, Fun97, GN95b, GQ95, Hir97, Hir98, IEE95a, IEE97a, IEE92b, IEE93c, IEE94b, IEE94c, IEE94e, IEE96b, IEE96e, IEE97b, IEE97a, IEE97b, IE97d, IE97f, IE97f, IE97k, IE98e, IE98f, IE98e. IRM93, KG96, Kat97, KM96a, Kra98, LOX99, LP99, Mau96b, MDS90, NIS92, Nat98, Nat99b, Ny998, OW95, OP95b, PS95b, QQ95, RD99a, RD99b, Sch94m, SJ97, SK93, Sti93b, Sti94, T+98, USE91, USE92a, USE94, USE95a, USE96a, USE99b, USE99d, Wa99a, Yua92, ACM99c, Ano93d, Boy95b, BD95b, Cop95b, Dar97, D96, Des94b, HQ97, HI97, IEE92d, IEE95c, IEE96f].

conference [IE98b, Kal97c, KG93, Kob96, LM98a, SP90, Ste99b, USE96f, USE98c, USE98d, VPM97, Wie99, Ano95f].

Conferences
Conferencing [BDHK93, MZ98, Sch95f]. Conflated [Ano99e, KBRS97, WW98a, Lam99].
Confidence [Chi99a, Chi99b, Graxx].
Confident [Jan95].
Confidential [Bet95b, Bet95a, vD97]. Confidentiality [Ano98j, Jac96, Riv98d, ZG96, FT95, MI90].
Configurable [VMS97b, VMS97a].
configuration [HI97].
Confirmer [Oka94, Cha95b, MS98b].
Conflict [All97].
Conflicts [ACM94b].
Confounder [BTD98].
Confliction [Zaj97].
Confusion [GC97].
Cong [Mye98].
Congressional [Smi97a, UU97a].
Congruence [Sch91a].
Congruential [Kra90].
Conic [Cao99, Mra95].
Conjecture [Jia99, GHS93, Ill94].
Conjectures [KP95].
Connect [Lic94].
Connection [Kas96, CV99].
Connections [RSG98, SGR97, Yu94a, Yu94b].
Connectivity [Pit96b].
Consequences [KP95, Sim94a].
Consideration [Cra96, Hub91, Mos98, Bas95, Bou94, SY92, YSS99, Bou94].
Considered [LT91].
Considers [Ano95].
Consistency [ZYR90].
Conspiracy [WK97, Scu92].
Constitutional [Bas95].
Constrained [Gol96b, Has99].
Constraint [SG95, WS99, GMLH94].
Constraint-Based [WS99].
Constraints [DS98b, Ou99, Kos96].
Construct [Lon92, Sun91a, Zl98].
Constructed [Rus93a].
Constructing [Ada97a, AB99a, AB99b, DT93, Gal99, KTM+99, Koh91b, XL98, Z996].
Construction [BCK96e, BR99a, BR99b, CNST98, vd95a, DS99, EM93, GPSNW98, Jof94, Kim93, KYDB98, NR98, SVxW91, ZMI90, BCK96a, BCK96b, BCK96c, BI93, MPL99, OS91, OS92, Pet91, vD95b].
Constructions [AHV98, ABDS96, KRS99, SNW98a, vHPP93, MS98b, SC97].
Consumer [IEE97g, IEE98c].
contactless [DS98a].
contain [Lea90].
Contemporary [Kmu99b, Sim92].
Content [Ack98, JPLI99, KR98, MW98b, MR95b, PMP99, Ros93, SC96a, Way93a, SNT95].
Content-Addressable [Way93a].
Content-Based [PMP99].
Content-MD5 [MR95b, Ros93].
Contents [vHH97].
Contest [DDJ98a, EMMN98, HD99].
Context [COZ99, MM96a, Des90b, Des90a, Ill94].
Context-Based [MM96a].
context-free [Ill94].
Continue [Ano96k].
Continued [KE97].
Continues [Ano97y, Ano97z, Ano98h, DDJ98d, Ano96l].
Continuous [BP95a, NHB98, She95a].
Contours [LFCK99].
Contract [GJM99a, GJM99b, KHB99].
Contractor [KHB99].
Contracts [Ped99].
Contracted [GJM99a, GJM99b, KHB99].
Contrast [HKS97a, HKS97b].
Contrast-Optimal [HKS97a, HKS97b].
Contribution [Lu97, Mus92, SS97, AK98, Blo98b].
contributions [HII94].
Control [ABLP93, Ban93, BDPSNG97, DFTY97, FY99, FL96, Hwa97, JPLI99, Kas96, KA99, KKW99, Lin98, Mey96, NW98, NA99, NS98a, PRAM98, Per99, STS99b, She93a, She93b, Sim90b, Sim91, WH98, ACC99, Ano93d, BGT96, CWM+91, CS96b, CS97b, CW94, LL93b, LM93c, Mat91, MLA91, RO96, RT93, SS96, Uni97d, WW95].
Controllable [CTT94].
Controlled [GPR98, GO96b, Gol94, Jak99c, SKBxx, GM91, GO95, Men95b].
Controller [CIBM99, FCH99].
Controls [Ame96b, Ban94, Cli97, UU97b].
Controversy [Law98].
Convention [Ano94d, Ano96a, Ano98f, IEE96f, NIS92].
Conventional [PRB98a].
Convergence [GC97, Mos98].
Conversation [Woe97].
Conversationally [LTEH99].
Conversion [Sah94].
Convertible [BCDP91, DP96].
Convolutional [Cha99c, JJ99b, TY94].
Cool [Ano99c].
Cooperative [Oh99].
Coordinating [Lee99b].
Coordination [COZ99, FL99a].
Vau98c, Vv97, Ver95, WSK97a, WSK97b, WFS98, WSD+98, Wag98b, Wag98a, WFS99, Wag99b, WSDK99, Wag99c, Wie90, Wie90b, Wie90a, WBDY98, YLD99, YLH98, ZYR91, Ada92, Alv98b, BSN95, BB94, Ber93, BS90a, BS91e, BS91f, Bh92, Bih95b, Bih98b, BK98e, Bir99, BD95a, Bowxx, Bur98a, CV95, CD98a, Cra92, DYL98, FSN93, Fri92a, Fri92b, Fri96, GSN94, GM91, Gol95b, Gol98b, Gol92, Gol99c, HKM95, Jak99a, Kah98b, KY95b, KR95a, KYxx, KSW97a, KSW97b, KR96c, Kos97, Kuk99, LMM92, Lan95, LS98a, Lew92, Mat93, Mil96, Mil92, Moh92, Mor92, NS97c].
cryptanalysis
[OC95, OG95, OSH91, RP95b, Rob98b, SV95a, Sha98, TN97, TSM95, Unixxa, Vau95, Way95, YT95a, YT95b, ZYR90, ZH90].
cryptanalyst
[Rey96, Rey97, Rey99].
cryptanalytic
[Gla99b, KSWH98d, MG91, vW99, Bih94a].
cryptic
[Wri98].
CRYPTO
[Fei91, ACM94b, Ame96b, An96a, Bar93a, Bar93b, BE90, HP98a, HMvT94, Koo97, LKB+94, Mah96, MPPS95, Neu97, Sch98c, Way95, Way96b, Neu95, Bra90c, Bri92, Bri93, Cop95d, Des94b, Gol98b, Kal97c, Kob96, Kra98, MZ98, MV91, Sti93b, Sti94, Wie99, BC98, Bra98, Bri98, CP91, CR98, Cha98, Cop98, Des98b, Fei98, Ger98, Gol98a, Kal98a, Kob98a, MV98, Ngu99a, Ngu99b, Odl98, Pom98, Sti98a, Wil98b].
Crypto-Chip
[HMvT94].
Cryptographic-Token
[Nys99].
cryptographic
[Sch93g, SZZ94a, SZZ95b, Ste99b, Way98, WN94, XZZ97, XZZ98, YS91, ZZZ97, ZLX99].
Cryptographically-Token
[Nys99].
cryptographical
[KP95, GyP98].
Cryptographically
[BD98, Cha90, CvHP91, Hil94, PGV92, ZZ96, DT93, IS97, KSB96a, MCD98b, SKB97, Bou94].
cryptographically-secure
[Bou94].
cryptographiquement
[Bou94].
Cryptography
[ANS97, ANS98b, Ano99h, AA93, ABDS96, Avo98, BCC+94, BGG94, BGG95, BGR98a, Bel98, BBB+91, BEE92, Bir98, Bia93, BK95d, BL96b, BL96a, BV993, Boy95a, Bra90a, Bra94a, Bus97, Cae96b, DDJ98a, DL96, DP98a, DP98b, Dav91, Dav96, DG96, De 93c, Des94a, DHQ98a, DHQ98b, Des98c, Dif90, DNN91a, Dro96, Dwo97, Ele99, Fer99b, Fin97, FBS97, FJM+96, FJRS96, FGLP96a, FGLP96b, Gan93, Gen97, Gol95a, Gol97a, Gol97b, Gon98, HK99a, HP98a, HSSI99, Hat96, Hed97, HL93b, Hir98, HAH94, HKS97a, HKS97b, Hru95a, Hru96, Hru98, HLMP96, HH98, HBKL99, JR96, JM97, Kal97a, Kal98c, KS98a, Kal99, KSS+92, Knu98a, Kob94, KA91, RSA93f, Lac93, LM94b, Lin96a, Los97, MY91, Mau99a, Mau99b, Mau97c, McC96, MP91, Mit92b, MKS99, NC97, Nic98a, Nic98b].

Cryptography
PKA+98, Pat96, Pf95, PT95, PGCSN96, Por91, PB99b, RSA99b, Rad97, Rhe94, Rit99, Riv90b, Riv93b, Riv97b, Ros96d, RK99, Sal99, DP91, Sas99a, SKBxx, SSS98, Sch94g, Sch96a, Sch96b, Sch97a, Sch97b, SSV+98, Sch98f, Sch94b, SV93, SG96a, She93a, She93b, She93d, Sni94b, Smi97b, Sta99a, SW95b, Ste91, Sti95, Sti98b, Sat99, Sw97, TN96a, TN96b, Tv92, Tow98, Tsu92e, Wad98, Way96a, Wol99, Wol93b, Wor96, WC97, YWC97, YST99a, YY97, YY97a, YST99b, ZYWR91, Zim98, dRHG+99, Uni96c, AA95, Ace97, Ada91, Alv98a, Ano97q, Ano97-30, ASM98, BH98, Ban94, Bea97a, BR96b, BFS92a, BFS92b, BBH99, BW97, BMP+97b, BSS99, BBS98b, BD98b, BC96b, Com96, Con99, Dam96, DDB95a, DDB95b, DVL96, DiF96, DNN91a, DN95b, Eng99, Far93, FM91, FK93b, Fra99, Fra93, Fri96].

cryptography
Gar96b, GZ91, Gol99a, Gol97c, Gre94, GTGW94, Hir97, Hru95b, Hwa91, Hwa93, IZ98, IZ99, Imp92, Joh97b, JY98, Kau96, KM98b, KK97, Kip97, Kob91c, Kob98b, Lag90, Lee99a, LM94a, LMS90, Lox90, vdl98, Luc95, MB94b, Mau93b, MY98, Mei96b, MvV97, Mic97, Mil92, Mur96, NM96a, NM96b, NKC94, NS95, Nec91, Nic99, Nyb94, Org98a, Od94b, PG97a, PG97b, PC98, PP92b, PGV93d, PR98, Riv98c, Rot95a, Sal90, Sal96, Sch92e, SS+97, SMD+99, Sch99c, Sch90c, Sch97c, Shp99a, Shp99b, Sin99, Siu99, Sh98, SMS99, Sta96d, Ste98a, Tas98, TM99, USE96e, Woe97, Wol93a, YL93, van98, Boy95b, Dar97, Dav94, Sch99b, vdWS97, Wai99a, vS97, Sha99a].
cryptography-dedicated [NM96b].

Cryptography-in-the-Large [Bla93].
Cryptoki [Ano96k].
CryptoLib [Lac93].
Cryptologia [Ers99, DKK+98, Joh98].
cryptologic [RK98b].
Cryptologie [Bra93b, Bec90, Sch98e].
Cryptologist [Pin98, Sel94].
Cryptology [Ano93g, Ber96b, Beu94, Bra90b, Bra90c, Bra90d, Bra94a, Bra95d, Bri92, Bri93, Buc91a, Buc91b, BK97, Cal92, Dam90a, DSB99, GPT91a, GPT91b, Kum97, MZ98, Pom90a, PG90, Pre98b, Rhe93, Rom90a, Sim92, Smi94a, Sti93b, Sti94, Tou92, Tro97, Van95b, We98, AK98, Ano97t, Bau97, Bec98, CW94, Cop95b, Cop96d, Dam91a, Dam99b, Dav91, De 95, Des94b, Du98, Fei91, Fum97, Gol90b, GQ95, Hef94, IRM93, Joh95, Kal97c, KM96a, Kob96, Kra98, LOX99, Lid90, Lip93, Mau96b, McC90b, Mei92, MV91, New97, Nyb98, OiDP98, PSN95b, QV90, QG95, Rat96, Rue93, Scu92, SP90, SZ93, Seg92, Ste99b, Un94c, Unixxb, Un95b, Web93, Wie99, Wil98a].
cryptography [Bec97].
CRYPTON [DPR+93, Lim98, Lim99].
Cryptonomicon [Ste99a].
Cryptoprocessor [Pai99b].
cryptos [Hag98].
cryptoscheme [MMI97].
Cryptosystem
[AMV90, BI95, BDGI98, Ber97c, Bih91, BMS94, Ble97, Bon99, BM97, CC99b, CG99, CJS91, CS98b, CW91b, Cus97, Gib91, Gib96, GC91, GC94, GGH97a, Gys96, HD96b,
cryptosystem

[Cryptosystems] [BDHJ98, BHSV98b, BHSV98a, BS91b, BLM94, BS91c, BS97a, BS90b, CGJ +99, DP98c, ESST99, FY98a, FY98b, FY99, GJKR99, GPCSN96, GGH97b, Gor93a, HGS98, HMOV3, HRR90, Iss90, Kal98g, KL95a, Kor93, KT93, KKT91, KKP93, LH93a, Len99a, Men93, Men95a, Mic93a, Mic93b, Miy93b, MOM91, MM98a, MM98b, vO91a, Pan99a, Pao99d, Pao99, PR97, Rud91, Sma99, Son99, dWQ91b, Wie98b, WZ99, Yam98b, Y197b, YY99b, dWQ91a, vO91b, AA99, Ale92, And94b, APDS93, BC90, BS91a, BS90a, Bfi92, BF96, BJQ97, BBL95, BK98g, CZ90, CA99, CC98, Cha95a, CL97a, CSN98, CLL99, Con90, Des90b, Des90a, DF90, Des93, ES97, FK94, FSS94, FGMY97a, FMR99, Go90c, GH99, GP97, Has99, HNM98, Hor99, JM96a, Jar96, JQ98a, KM99a, Kob90, Kob91b, Koc95, Kos97].

cryptosystems

[Kos99, LLH96, Lan96, LS98a, Ler97, LZ90, LZ91a, LZ91b, LDW94, LL97b, Lon92, MV90, Miy93a, Miy99, MS99c, Moo92, MVZ98, NM94, NY90, Od90, OS91, OS92, Pae90, SS98a, SS98b, SS95a, SH99, SG98, SMK98b, Sun91a, SH94, SS98b, Tab94, Taq97, Tao94, VZ97, Xie92, Xie93, XL98, XL99, Ym98a, YW99, YY98c, Zho94, ZPY96, vO92, vT94, Wa98].

CS

[Ano93e, Ano94a, Pin98, SV98, Vau99b, Vau99c].

CS-cipher

[Vau99b, Vau99c, SV98].

CSP

[DS97d].

CTS

[BR96a].

Cubic

[Per93].

Cultivate

[Ch99f].

Cultural

[UCF94].

Cultures

[Mat96].

Curvilinear

[SCG99].

Cusick

[YT96].

Custom

[Nor95b].

Customer

[Nor95c].

Customised

[GN95c, HHD99].

Customising

[NO96].

Cut

[BLM99].

Cuts

[Gar98a, Den95].

Cyanide

[Mar98b].

Cyber

[Gar98a, Den95].

Cyberbanking

[Mur96].

CyberMall

[Mar95a].

Cybernetics

[LS98a].

Cyberpunk

[HMM91, HM92, HM95].

Cyberpunk

[Zim96b].

Cyberspace

[Gar98a, Den95].

Cyberpunk

[Gar98a, Den95].

Cyberwar

[Kau96].

Cycle

[GAGCDFAFC99].

E-Cash [DFTY97, Yac99a, Yac99b].
e-commerce [VM96, DDJ98d, Jak99b, Lut98, Gar97b].
E-mail [LF97, Ri96, Bae95, Sta94a, Ano93j, Got99, RS98b, Sch95c, Sch95d, SH97, Ano95c, Gar97b, Str93a, Str93b]. E.I.S.S [BFS92a, BFS92b]. E.I.S.S. [Dan95].
E.I.S.S.-Report [Dan95]. E2
EAP [BV98b].


Electrochemical [DDJ99]. Electronic [Avo98, Bar93a, Bar93b, BFP99, Bra95b, BLMO94, Cha92b, DDJ98c, DB99, DT98a, EO95b, EN98, ENK99, HS97, Hir93, JTT97a, LHB96, Lin93a, Lvd98, LKD98, LR98, Max94, MZ98, OO90, Ped95, PW97c, Rtv97a, STS99a, STS99b, SB97, Sch99i, Sin98, TRS+93, Tra99, USE95c, USE96d, USE96b, USE98b, VJ98, AMS96, AC97, BH98, Com97, Cha92a, DMW94, DSSZ99, DF98, EO95a, FB97, Ken95, LM98a, Lin98a, Lin98a, Man95, Mit92a, RP97b, Sch93e, Sch95d, She96a, VNM99, Way93b]. Electronically [Ped99]. Electronics [IEE97g, IEE98c]. Elegance [Sch99c].

Electronicznej [Sch95e]. Elementary [Mil92, Tat98, Tat99]. Elements [FC99].

Eleventh [CH96, IEE92d]. ElGamal [AA99, Ble96, KSK96, LK96, NK98a, TY98b, TY98a, VvT97, Zho94]. ElGamal-based [TY98b, TY98a]. Eliminate [Riv98b]. Eliminating [GGH97a]. Elimination [BLM99]. Elizbeth [Uni92]. Elliptic [AMV90, Ano95n, BS91b, BSS99, CTT94, De 98d, DP98c, DMPW98, Dem94, Eng99, ESST99, Fer99b, HSS99, Hes97, JQ97, JM97, Kal97a, Kal98g, MKKH99, Kob98c, KMOV91, KT93, Len99a, LD99, MS93, Men93, Men95a, MM96b, Miy93a, Miy93b, Miy96, Miy99, OFF93, RY97, SOOS95, SW93, SNNP99, VZ97, WZ99, AMV93, AS98, BGR94, BC90, BS91a, CNST98, CPPK98, FMR99, Gal99, GKK99b, GP97, HNM98, IS99, IKNY98, JQ98b, KSK96, Kob91b, KK98, KOT95a, KOT95b, LL96, Ler97, Mau91b, MV90, MVZ93, SX90, XL98, ZI98].

Elliptic-Curve [Fer99b, Kal97a]. EMACS [McH92]. email [Kar96]. Embed
[Ano97o, MT94, Ano97-27, Zha96].
**Embedded** [BKS99, Bar99, DDJ98a, LT98, Lin98, BBCP98a, BP97b, CC95, KP99b].
**Embedding** [ACD94, DS97d, GO95, Gol96b, HK99h, ZK95, Sch91a].
**embeddings** [CT99b].
**Embraces** [Ts'97].
**EMEF** [Org98a].
**Emergent** [Jun99].
**Emerging** [Kal99, Org98a].
**Empirical** [WW98b].
**Employing** [BWM98].
**emulator** [Obe99].
**EMV** [Gui97].
**enable** [Sch93e].
**enabled** [Cha99b].
**Enabling** [DS97b].
**Encapsulating** [Atk95b, KA98b].
**enciphered** [Lea90, Per91].
**enciphering** [Beu94].
**Encipherment** [HS90, OA94, Lin88a, Lin89a].
**encoded** [DS97b, HG97d, QN98b].
**Encoding** [Til98, HG97d].
**encodings** [CGV94].
**Encrypt** [BR95a, Ber98, JSY99, Ril96, WT99, Rot97].
**Encrypted** [AW99, Bla98, GMCF95, GLZ99, Gil98, Jas96, YY99, BT98, DF97, STW95, Kip97].
**Encrypting** [Ano97r, Bla94b, Lom94, Luc98b, EW99, SS99c, Beu94, KAK96].
**Encryption** [SW97a, Uni97b, Uni97f, Uni98b, Uni97c, Uni98j, VB96, VR98, WS97a, WSK97b, War98, Way93b, Way93c, WSFC99, Wei91a, Wei91b, Whe94, Wir98, Yin97, YY97c, Yuv97, Zhe97, Zol93, Aus96, Abr97, Ata93a, All97, And94a, Ano90, Ano92b, Ano94e, Ano95c, Ano96d, Ano96m, Ano97u, Ata94, DR98, JR98, BR97b, BR97, BR97b, Bet95c, Bi97c, BF98a, BC96a, BMS96, BFS98, Bow93, Bro96, Bas96, Com97, CCN95, Cha94b, CLW98, Cle96, Cif97, Cif99, Cij96, Cra96, DH96a, DOR99, Dia91, DL98, Eek99, Ell97, FC94, FB97, Gil97, Gol99b, Gol96d, GBL94, Goo96, GKS97, Har90, HK90, Hat97, Hel93, Hel98b, HT95, HP94, HY95, HCY96b, HCC98, Int91b, Jac90a, Jac90b, Jak99c, JT96, JT97b, KY95b].
**encryption** [KY97, KYYx, Ken95, Kir95, Kn99c, COP95a, CH98, CMK98, CT99a, Cop94a, Cou93, DDJ98e, DDJ98f, DDJ98g, DDJ98h, DC98b, DK96, Den90, Den95, DB96, Des99b, DS97c, Ele98, FIP94, FN94, FY95b, FY97, FH94, FO99a, FO99b, GSY99, Ga90, Gar97a, Gar97b, Gar97c, GC97, Gar98a, Gar98b, GK98, Got99, HG97a, HG97b, Hat96, HK98, HK99d, Hub98, Jol98, JM96b, Kal93a, KY95a, KR96a, Kal98b, KY98, Kap98, Kas96, Koh90, KKL99, KM97, Kum98].
Ril96, Riv95d, RKD94, Rot95a, Sab94, Sch98b, Sch94i, Sch98c, Sch99j, She96a, Sm97, Sta97a, SW98, SW99a, Str93a, Str93b, Su98, Sun91b, TX92, Tay90, Tha91, Tho96, TY98b, TY98a, Ts90, Uni96a, Uni95a, Uni98k, Uni94a, Uni94b, Uni97d, UN94, UU97b, Vau98e, Ven90, Vu95, Wad98, We95, Wii93, Wil93a, Wi93b, Woo90, You97, You97, Zaj97, Zan90, Zer96a, vV98a, vV93, An98j, An93j, Hon98].

encryption/authentication [Sch99j].

cryptography/decryption [Hat97, Vu95].

Encryption/MAC [Yuv97].

crypts [Ano93k].

Encyclopedia [CFK+91, New97, UFC94].

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

End-to-End [NH90].

romosome [Wal98].

Endured [Che92].

Energy [DFL99].

Enforce [BDS98].

Enforcement [Cae96b, Cli99].

Enforcers [Way93c].

Enforcing [Ano97n].

Engine [BE90, CM98, She92d].

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

Engines [T+99, Way93a].

England [ES98, Cur98].

Enhance [FO99a].

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

Enhancement [HWJ98, Lin93a, Lin98a, Lin98a].

Enhancements [JM96b].

enhancing [HY95].

Enigma [CM91, Har96b, Kip97, Kip99b, Obe99, Ano91c, Blo98a, Blo98b, Blo98c, Cra92, Kah91a, Kah98a, Kip97, Kru98, Mi96b, Mus92, Tu99, We97].

Enigmas [Gad91].

Enjoyable [CM99d].

Enough [CFK+91, Dea98b].

Enschede [Hei96a].

Ensuring [Com97, Rot95b, ZG96, Way91].

Enter [Wor96].

Enterprise [ECD99, FY99, Mar95b, Wad93, SY92].

enterprise-wide [Wad93].

enters [Joh98].

Entities [KM99c].

Entity [BR94a, BWM98].

Entrepreneur [Pin98].

Entropy [Bro94, EHMS99, KSHW97, KSHW98].

entwerfen [Hor99].

envelope [SOB98].


Environmental [RS98c, RS98d].

Environments [GSTY96, SKAM99, DNS99].

EPIC [Rot95a].

EPS [Ano96i].

equally [Ito91].

Equations [Cop95e, LG97].

Equations [Por98, RZ99, BMP97a, Cus95, GK95b, LCL95, Luni92, Sun91a].

Equilibria [Ett98].

equipment [Int91b].

Equitable [BDS98].

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

Equivalent [Bv98c, De 98d, Gi91, GO93, HTY99, MM96b, Miy96, Oka94, Pia99c].

Era [DDJ98c].

Ergonomic [DDJ98c].

Erika [Mat99].

Errata [Con99a].

Erratum [Ano91a].

Error [AW94, AR98, BGS96, Cha99c, DLR97, KKS97, LC99, MG91, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, DLP93, Jv98b, Ste95, Wan92a, YL97a, vV94, CW94].

Error-Correcting [AW94, BGS96, DLR97, KKS97, Pen96, Ada91, Ala93a, AW95, Cha95a, CMM93, Ste95, Wan92a, YL97a, vV94].

Error-Correction [MG91].

Errors [GGH97a, SHK99b].

ESA [Spi95, YS91].

ESA/390 [YS91].

ESAT [PGV93d].

Escrow [AAB97, Bla96c, BHS98, Cae96a, CM97a, DDJ98g, DDJ98h, DB96, FY95b, FY97, Fro96, FO97, Gan96a, HD96b, HM98, KP98, KP99b, KB92, LW95, M96b, Mar97, MS95f, KMS99, Nec96, SYM98, Sam98, SM95a, VvT97, VBD99, YY99b, Ano94e, BDHJ97, BR96b, DH96a, Des95, Fre94, KL94, Mao97, Uni95a].

Escrowed [Bas95, Com94b, FIP94, Nat94d].

ESIGN
[FOM91].  **ESORICS** [DEQ92, Q9+].  **ESP** [KA98b, Atk95b, KMS95a, KMS95b, MD98, MG98a, MG98b, PA98a].  **Espionage** [HK99c].  **Espoo** [Ny99b].  **Essential** [SSv98, SSM97, SMD99].  **Essentially** [BR99].  **Establishing** [Des96a].  **Esterel** [RB99].  **Estimate** [Miy93c, UU97a].  **Estimates** [DLP93].  **estimating** [Al96].  **Estimation** [VNW95, JV98b].  **Ethernet** [Bec99].  **Etruscan** [Nis91].  **Euclid** [LZ91a].  **Euclidean** [Blo99, FP99, KR99b, LZ90, OMV98, SCG99, TK99, ZW99].  **Eulerian** [MSN98].  **Eurocast** [MDP94].  **EUROCRYPT** [Bih91, Dan90a, Dam91a, Dav91, De95, Fum97, GQ95, Hel94, Man96b, MZ98, Nyb98, QV90, QG95, Rue93, Ste99b, Ano98c, Bet98, BCI98, CP98, Dam98, Dav98b, De98b, Fum98a, Gue98a, GQ98, Hel98c, Ing98, Mau98, Pat95, QV98, Rue98, Pic98].  **Eurographics** [Kui91, PH91].  **Europe** [And96a, DEQ92, Q9+].  **European** [Dan96, DEQ92, Q9+, Spi95, T98, Com97, Gar97c, VCF90].  **Eusipco** [T98].  **Eusipco-98** [T98].  **evaluated** [LMS97].  **Evaluating** [Pai99a].  **Evaluation** [AGS97, Ano97b, BGK99, BP95b, CJR98a, CJR98b, HW9, KBR97, PDG91, RIP95b, RIP95a, Roh93, Roh99, WT99, CJR99b, KM97, PSS9a, Sim95, VCF90].  **Evaluative** [MI99].  **Even** [BCE94, Bosxx, Ano95k].  **Evening** [Che92].  **Event** [Ruo94, SK97b, SK97a].  **Event-Stream** [SK97b, SK97a].  **Ever** [Hill97].  **every** [Ano91b, Mei98].  **Everything** [BOGG90].  **MAM95).  **Evidence** [DR99b].  **Evolution** [Cas95, JM96b, KNT94, NM96b, PGV93d, Sim99].  **Evolutionary** [Ger99a, GM99a, Hes97].  **Evolve** [GB98].  **EW** [IS97].  **exact** [BR96c, Luc95, ZW99].  **examination** [Joh90].  **examines** [vdW97, vS97].  **Examining** [RC95].  **example** [Kay95, Nee94].  **Excellence** [Eri97a].  **Exchange** [ASW98, ASZ96, BCG90, BM94b, Dam94b, Dan95, DH90, FW91, HHH93, Jas96, Luc98b, MSN98, RSA99a, SSN98a, SOOS95, Van93, BSNP96a, BSNP96b, BTD98, BCK98, BM95, Dam94a, LL95b, MS98a, SK97, STW95].  **changes** [DvW92].  **Executable** [JPL99].  **Executing** [AW99].  **Executive** [Zer96a].  **Exhausting** [CR97].  **Exhaustive** [CR97, QD91, KR96b].  **Existence** [FD93a, HT98, RV99, FD93b].  **Existentially** [DN94].  **Existing** [SS99d, BB95a, NM96b].  **Expansion** [BO96b, Tak97].  **Experience** [AABB99, Gla99a, Ros96b, SV99, M98, CWM+91].  **Experiences** [FC99, Lum90, GH96, MAM95].  **Experiment** [AB97, DL95].  **Experimental** [BBB95].  **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** [Ano95a, CFPR96b, CNS99b, CFPR96a, FR95b, KOT95a, KOT95b].  **Exponential** [Dan95, CFS97, CDG95].  **Exponentiation** [BP99b, BK95d, Dam90, HCY96a, LL94b, Pa99b, Ara93, BGR98b, CL97a, KAK96, Rev91, Sim94b, Von92a, Von92b, YL93, dR95].  **Exponents** [Wei90b, vOW96, Gro94, VW96, Vv97, Wei90a].  **Export** [Ame96b, DDJ98e, DDJ98f, Gar97b, GC97, Uni97d, Abr97, Ban94, Cli97, SU97b, UU97b].  **Exportability** [Wei91a, Wei91b].  **Exports** [Bar96a, Sta97c].  **Exposed** [MSK99a].  **Exposing** [Si99].  **Expressive** [MTES99].  **Extend** [Ts97].  **Extended** [ASW98, BFN98b, BV98c, BD90, BS91g, BD91, CvHP91, CK90, DDP90, DY91d, DDP99, DD99, DY91f, DF91a, Dob95a].
EvH91, FW91, Gil99, MS91, Mv93, MOM91, OOK91, RSA93c, Rud91, DP91, She93c, Tou91, ZMI90, vHPP93, Bea97a, BCK98, BT94, CV93, Des90b, Des90a, Has99, LLG10, Ole95, Pai96. 


Externalization [OA99]. Extraordinary [Jam98]. extremely [Ano90]. eyewitnesses [Ano97t]. 

FA [Bao94]. Fabrication [DDJ99]. Face [DDJ98d, DMFB97]. Faces [GB98].

Fachtagung [BGH95b]. Facial [LMP99, HEG98]. facilitation [Cli99]. 

Facility [AKF94, Bis90, She96a, YS91, JMLW94, SY92]. facing [KG96]. facto [Pri94]. factor [KM98b, SVWMB95, VSB95]. Factored [Ano96b]. Factoring [Ano97e, BV98c, BDHG99a, BDHG99b, Kal98e, MM96b, MS90b, OU98a, Pai99c, Pom90b, Riv93a, She92b, SW93, BBR99, CDEH+96, KK98, McK99, Mei96b, Riv95a]. Factoring-Based [Kal98e]. Factorisation [DH95a, Jon90, DH95b]. Factorization [Ale92, DDLM94, MM98a, MM98b, Odi95, vo91a, Sho97, vO91b, LLMP93, Mao98, Whi93, vO92]. Factorizations [BMS94, NS97b, NS97c]. Facts [Ano91b].

Faded [Alv98a]. fading [Tod97]. Fail [BP97a, PP97, SSNP99, vHPP93, And94b, Pf96c]. Fail-Stop [BP97a, PP97, SSNP99, vHPP93, Pf96c].

Failed [BCE+94]. fails [DH96b]. Failsafe [KL94]. Failure [Ano95a, Ber97c, Gar98a, TYD99, FR95b]. Failures [CH98, JQ97, Moo92, Sim94b]. Fair [ASW98, CFGS99, DT98a, KL95a, LK99, LH95, Mic93a, Mic93b, MKS99, SS99e, SS99f, Tra97]. Fairfax [ACM93a, ACM94a]. Fairly [HD96a]. fall [Od90, Rob98b]. False [LK98a, She92b]. 

Families [Kal98a, Per99]. Family [KT98, Miy91, RP97a, ABC+98, BGH+95a, FSS94, It91, Kob90, SRRL98]. FAPKC [DY1998]. FAPKC3 [TCC97]. FAPKC4 [TC99a]. Far [Str95]. Fast [AGS97, AMV90, ALO98, And94a, BP98a, BQ95b, BQ95a, BGR98b, Bi97b, Bi97c, BHK+99, BD94, BK95d, BGV96, C991, Cla97, Cla98a, DDJ98e, DDJ98f, DC98b, DRR95, DBV96, DNR97, EPR99b, EPR99a, Gar97b, Gol96a, HJP98b, HP94, HCY96a, J99a, J99b, KR94a, KTM+99, KP99a, KP97, KR99a, Kau99c, KMK99, KA91, Koy95, LM95, Mau90, Mer91, Mih94, MM95, NS99a, NK99, PS97, Pre95a, Rog95, SW97a, SW97b, SOOS95, SV93, SB98, Sho96, Si97b, Tak97, Tak98a, Tak98b, T+99, Van98d, Van98e, AMV93, AB96b, Ano98j, CV949, DMR97b, DV96, GCH+98, HJP98a, Jenxx, LRW93, LC98, LZ98, P995, RRR98, She92c, SN94, SH99, SAM97, SGS99, YL93, Gol96d, OA94]. Faster [Luc96a, Luc96b, WZ99, YY99b, Bosxx, Mih96, Sch98c]. Father [CFK+91, DDJ99]. Fault [BS97a, DHSS95, GX99, OKST97, Pai99a, RBV94, IEE94b, TCH+91]. 

Hir98, Iz98, RP97b, SJ97, Wo93a, Wo93b, van96, Ano94c. **Federal**
[Ano97h, Ano97x, Lee99a, RP94].
**Federated** [SS99b]. Feedback
[CJM95, GK95a, Ros98a], Feistel [Jut98, Knu94a, SN93, SK96c, SK96d, Van99a].
**Fermat** [LLMP93, McK99]. Few
[FJRS96, Mei98]. Feistel [Jut98, Knu94a, SN93, SK96c, SK96d, Van99a].
**FFT** [DBGV93, MS90b, Sch91c, Sch93f, SVB96, Van93].
**FFT-Hash** [DBGV93, Sch93f, Sch93g].
**FFT-Hash-II** [Vau93].
**FFT-Hashing** [Sch91c].
**FGPAs** [Nor95c].
**FHFC** [KKW99].
**FHFC-Tool** [KKW99].
**Fiat** [Nac93, OOK91, OO93].
**Fiber** [Tow98].
**Fibers** [HLMP96].
**Fibonacci** [SMS99].
**Fiduccia** [CKM99].
**Field** [CD98b, Kob98c, LL99, LMP90, LL93a, MR95b, Ros93, SY99, T999, CDEH96, Dav98a, Gh99, Gori93b, HWB93, Has99, Hor93a, HP94].
**Fields** [BP98a, BMT96, BL96b, BL96a, BP97c, De 98d, LO91a, LO91b, Mas91, MFG95, PSR97, Ano93k, Bao94, BI94, BGR95, DW99, DLY98, DF93, FSS94, Gal99, GH99, HWB93, Has99, Jun96, LN94, MK92, PS97, Pie93, Tao94, TCC97, TC99b, Von92a, Von92b, War98].
**Fifteen** [Den90].
**Fifteenth** [CFK91].
**Fifth** [SJ97, Uni97b, Uni97c, Uni98a, Uni98b, Uni98c, Uni98d, Uni98f, Uni98g, Uni98h, Uni98i, Uni98k, USE95c, RD99a].
**First-Order** [KW99].
**Fire** [Way93b].
**Firewalls** [GLZ99, Opp97].
**Firms** [GC97].
**Firmware** [MNSV97].
**Firmware-Oriented** [MNSV97].
**Finite-Impulse-Response** [She92e].
**Finite-Size-Particle** [BVFD99].
**Finland** [Nybl98].
**FIPS** [Nat93b, Ano93f, Nat93a, NIS93b, Nat94a, Nat95, Nat99a].
**Fins** [GC97].
**Firmware-Oriented** [MNSV97].
**First-Order** [KW99].
**Fish** [BD94].
**Fishermen** [Ano96l].
**Fissures** [DDJ98e, DDJ98f].
**five** [KAK96].
**fix** [Ano98j].
**Fixed** [FK93b, Ma98, HP94].
**Fixed-parameter** [FK93b].
**Fixing** [Low96].
**Flaw** [Gar97c, Lea99].
**Flexes** [Cor98].
**Flexibility** [Wed99].
**Flexible** [JPL99, LL94b, AG95, BP97b, Ts’90].
**Floating** [Gar97b].
**Floating-Point** [Gar97b].
**Floradora** [Fil95].
**Florence** [IEE92d].
**Florida** [IEE93c, IEE94c, IEE96f, IEE97f].
**Flow** [STS99b].
**Flowers** [Pin98].
**Focus** [GO96c].
**focusing** [Com96, USE96e].
**Foil** [MB94a].
**Folger** [Mor92].
**folglich** [MPS94].
**Football** [RBCE99].
**Footwear** [MD99].
**Force** [CD98c].
**foreign** [Cha94b].
**Forensics** [Gro98].
**Forensics** [SK99].
**Forgery**
[AW94, GM97, LHL95b, LHL95a]. Forget [DFIJ99]. Forgotten [Ano97t]. forimage [XA98]. Form [Cha93, STP93]. Formal [BR97a, BFN98b, BoI98a, Boy92, GFB93, Gue98b, Mea95, PM9b, Tou93, WK96, AHdJF97, AAPS92, Ata94, BFN98a, JW01, ZLX99]. Formality [ACD94]. Format [CDFT98, Nys99]. Formats [ASZ96]. Formed [Gar97c]. formed [Mok97]. Formulae [KV94, WD99b]. Forty [CWM+91]. Forum [IEE98d, MB99a, Org98a, Ano97c, GO96c, KSS+92]. Forward [BM99a, BM99b, CadHSV96]. Forward-Secure [BM99a, BM99b]. Foundation [Gol95a]. Foundations [Ada91, BDFM99, Gol97a, Gol97b, IEE92a, IEE96a, IEE96c, IEE97e, IEE98a, IEE99a, JR96]. Founder [Pin98]. Four [HKQ99, Koe99, Riv91a, DL95]. Fourier [MS94, NA95]. fourteenth [IEE95c]. Fourth [OW95, Uni96b, Far93, IEE93a]. FPGA [GTG94, Kap98]. FPGAs [KP99a]. FR [HSSI99]. Fractal [DS96, SD99]. Fraction [BDF98]. fractional [BR96b]. Fractions [Iss90, KE97]. Framework [Boy92, DGV93, Hed97, PS99f, PW99, SL99, VP99, Com97, HN94, LS98a, Pi96c, Tsh98, DT98b]. France [Chr98, DEQ92, FR95a, GQ95, Vau98c]. Francis [Lea90]. Francisco [Ano97a, Ano98f, USE92a]. Franconia [IEE92a]. Franklin [WD99a]. Fraud [Neu92, VGP93, VT97]. Fraud-Detectable [VvT97]. frauds [Sga93]. Fray [Gar97b, Law98]. Free [BP97a, BHT98, BDI96, CD98b, Dob97, Eri97b, GJM99a, GJM99b, HBKL99, Rus93b, SK95, All97, BT94, Des90b, Des96b, Dob95a, IlI94, Vau93]. Free-Space [HBKL99]. Freedom [Cae96b, Uni97a, Uni98c, Uni98b, Uni98e, Uni96b, UU97a, Uni97b, Uni98f, HM96]. FreeNIX [USE98c]. French [Blo98b, Bou94]. Frenkel [CFK+91]. Frequency [BP98c, MSHP99, Ano90, Tod97]. Freshness [KYG92]. FRG [Oht96]. Friedman [Uni92]. friendly [Bus96]. Friends [DDJ98e, DDJ98f, Sch92b]. Probenius [CPPK98, Graxx, KMKH99]. FROG [WFS99, Wag99b, GLC98, WFS98]. Front [Hed97]. Frontier [Bar93a, Bar93b, HM91, HM92, HM95]. FSE [Bih97c, Vau98e]. FSE99 [Km99c]. FTP [SSH93]. Fujiyoshida [IRM93]. fulfilled [Mar96]. Full [BS93a, DH90, SK98c, SK98b, Pos93]. Fuller [CFK+91]. Fully [BCD94, BCD96, HE98]. Function [BJY97, BDP97, BP97c, CP91, DBGV93, DGV93, Dae95, DC98a, DD90, Dob97, FGY96a, HILL99, HL99, MCD99, NSS99, PBD97, Sch91c, TOU94, AB96b, DK94, DDFY94, DI99, FGY96b, KSB96b, KSB97, LTT95, MZ98, NV98, PK97, Sch91a, SRRL98, SS95b, SS95c, YL97c, ZPY96, dB94]. Functional [Yam99]. Functions [AHV98, Ano95a, BDP99b, BCK96d, BCK96e, BHS98b, BHS98a, BG99, BGS94, BGS96, BM94a, BL95, BHT98, CDD99, Car93, DGV93, DY90, DY91d, DY91b, DFL99, ECM96, EPR99b, EPR99a, FBS98, GJKR96b, JO97, KTM99, Kim93, KP96a, Kra95, LM93a, LM93b, LM95, MS99b, MS90a, Mer90a, Mer91, MS95f, Mili96a, Mon93, NR98, OS98, PW93b, PGV92, Pre93a, PGV93a, PGV93c, Pre97a, Pre99, Pre94b, QC90, Roe94, Sch91b, SZZ95c, SY99, ZZ95, Zhe90, vW94, BSNP96a, BNSP96b, BD92, BGR95, BCK96b, BCK96c, BHH99, BK98f, CCZ98, CDG95, Cus96, CS96c, Dam90b, Gol96a, Gon95, GHS93, HSK97, HLMW93, HXMW94, HYLT99, ISO97, JG95, KL95b, Lai95, MCD98b, O’C94, PGV91, PGV93b, Pre94a, PGV94, PVO95, RP95b, Roe95, Rom90b, SZZ94a, SZZ95b, Sim98c, Tsu92b]. functions


Gbit [HK97]. Gbit/second [HK97].

generate [Wer93a, Wer93b]. Generated [SVBJ96]. Generating [Ble96, De98d, FMM99, Len96, Len98, MS95f, YWY99, CH97b, SH97]. Generation [ARV99a, ARV99b, BG98, BGM97a, BGM97b, BIR98, BF97b, BD93, Coc97, CD96, DF91a, GJKR99, Gil99, Gut98b, HL99, Kal97b, KS98c, MWB99, Mat96b, Man90, Mih94, PS98g, ROT94, RS98c, RS98d, SN96, SIl97b, WI99, Bou94, FMY98, GTS90, LLH96, MS99c, PS97, PS98b, SH94, Bou94].

Generator [FIP93a, HILL99, JK99, KSF99, KW99, MS95b, PS98b, Daw93, Jen96, MS95a, Mih96, PC98, Rev91, Sin99, TSY98, Wal90].

Generators [HL99, KSWH98d, Kra90, ZYWR91, CS96b, C97b, Imp92, Kos99, Lag90, Pat91b, Por93, SGD99]. Generic [Bel92, CM99a, MS98b, Taa99, ZK98].


Geodesic [Blo99, LFCK99]. Geometric [OMA98, Sim91, JM93, JM96a, Mra95].


Geometry-Based [Ben99]. George [Pin98, WG97]. Georgia [ACM99b]. Gerdes [CFK+91]. German [Wei99, Cra92, Dav98a, FT95, Ger97, Hor99, Jar97, Kah91a, KK97, Kip97, Kru98, Kru98, Wal98].

Germany [BFS92a, BFS92b, Fum97, IEE97d, LM98a, Wat91, Rat96].

Geschichten [CWM+91]. Get [Ano96j, Cae96b, DDJ98a, Sch98c, Ude98].

Gething [WG97].

Gar98b, GO96c, Los97, Sch98c. Getting [Kwa93, Way95]. GF} [PSR97, DBVD96, LD99]. GI [BGH95b, LM98a]. GI-Fachtagung [BGH95b]. Gibbs [DP99]. Gilles [Buc91b].


Giving [Int91a, GQW+91, JLM+94]. Global [JV98b, Or96, SS99b, TGK99, TL999, ZZ95]. GMD [SBGK99]. Go [DDJ98d].

Goal [AMP94]. Goals [BP98e]. Goats [SV95b].

[Ngu99a, Ngu99b]. **Good** [Ano94h, AWV99, Elk96, Gar95, GM95a, Gar98c, Ros97a, SSI97a, SSI97b, Sta94a, Sta95a, Koh91a, Ler97, Mei96a, SX90, Zim96a, Zim96b, Pin98]. **Goppa** [Gib91]. **GOST** [KSW96, Sch95b]. **Goucher** [Mus92]. **Government** [RKD94, SG96a, Ano94h, Riv98c, Way93b, Wel95, Lee99a, Ros97a, goverments [BH98]. **Grace** [GC97]. **Gradient** [Jen99]. **Grail** [Sal99]. **gran** [lPNdbbbprm91]. **Grand** [FBS97]. **Graph** [BMRW98, BDSV93, BW98, BALS99, EMMN98, M199, LS98a, PD99a]. **Graphic** [COM99, GO96c, lPNdbbbprm91]. **Graphics** [Kui91, SHG98, Wor96]. **Graphs** [BM94a, HE98, LE99, WD99b, Ku92]. **Gray** [Rus93a]. **Greatest** [Mad92]. **Greece** [IEE97c, KG96, Kat97, Pit95, Spi95, T+98]. **Greg** [Ers99]. **Grid** [LE99]. **Gridless** [BVFD99]. **Grosch** [CWM+91]. **Ground** [Law98]. **Group** [AT99, CS97a, CM99a, CW93, DDJ99, DKKK98, Got99, GN95b, HY93a, LR98, NS97b, NM99, Pet98, Rei92, SG99a, Tra99, Wu92, Yam98b, Yam99, CP95, DF93, Fra90, FR94, Hwa91, Hwa92d, LWC96, NS97c, WHL99, Wer93a, Wer93b, Yam98a, Dra99]. **Group-Oriented** [SG99a, HY93a, LWC96]. **Groups** [BMS94, CS97a, CH98, GPSN98, Got99, Mei96b, Pat99, SP9H99, CMP97, Dam96, GZ91, GPCS96, HSW94, HCC98]. **Grow** [DDJ98d]. **Grown** [Gar97c]. **Grows** [Lea99, Fra92]. **Growth** [GC97]. **GSM** [ATAY98, MB99a, She94b, Ved98a]. **GSS** [Lin96b, McM96]. **GSS-API** [Lin96b, McM96]. **Guaranteed** [Mao98]. **Guarding** [GS98, Mar95a]. **Guest** [BKK98]. **Guessing** [KS97c]. **Guest** [AKP96, BNP99]. **Guide** [Bac95, End97, WSFC99, Zim95a, Bis90, Jac90a, Jac90b, Nie99, Pre97b, Sta95b]. **Guided** [Mos99]. **Guideline** [Lee99a]. **Guidelines** [Bar97, CPOR97, Mer97, Ame95, Ame96a, Org98b]. **GUMP** [FBS97]. **guru** [Di 97a]. **gyi** [lPNdbbbprm91]. **H** [Scu92, Lea99]. **H-1B** [Lea99]. **H.** [WG97]. **H.R** [Un198c, Un196b, Un197b]. **H.R.** [Un197a, Un198b, Un198c, UU97a, Un198f]. **hacker** [Mei98]. **Hackers** [GC97, HM91, HM92, HM95, Mei98]. **Hacking** [MSK99a]. **Hades** [Bie98]. **Hagelin** [Hag98]. **Haifa** [Bil97c]. **Halevi** [Ngu99a, Ngu99b]. **Halkidiki** [Pit95]. **Halske** [Dav98c, Sel98b]. **Hamburg** [LM98a]. **Hamming** [She95c]. **Hampshire** [IEE92a]. **Hand** [BF99a]. **Hand-Held** [BF99a]. **Handbook** [Bac95, MVV97, Sha99a, At99, Rey96, Rey97, Rey99]. **Handles** [Bar99]. **Handling** [BMS99, Dae98, HC95a, Mat91]. **hands** [Riv98c]. **Handshake** [Sim96b]. **Harari** [Ver95]. **Harbor** [Kah98b, Par98b]. **Hard** [MGL+98, Mar99, SS99a, BFKL94, Jon90]. **Harder** [Sch97b]. **Hardness** [BV96, NS99b, Di99, Kha93]. **hardness-amplification** [D199]. **Hardware** [ACD94, Bir98, BF99b, Bri90b, BS91h, Cla98a, DGV92, GN95c, Kocz96a, OSA91, Wil93a, Wot99, YK98, BB95a, DN95b, Gai90, KP99b, LMS97, MZI98, Nor95a, Nor95b, Nor95c, NO96, See97, SN94, TY92, Way95, Zhe95b, Kui91]. **Harmonic** [RG99]. **Hash** [ANS97, AHV98, An93f, An95a, An95i, BDPNS97, BCK96d, BCK96e, BS91e, BS91d, BDP97, BHT98, CP91, DBGV93, DGV93, Dae95, DY90, DY91d, DY91b, EPR99b, EPR99a, FIP93b, GHR99, GS94a, ISO97, KP96a, Kra95, LM93a, LM93b, LM95, Mer90a, Nat92h, NIS93b, Nat95, PRZ99, PW93b, PGV92, Pre93a, PGV93a, PGV93c, PGV94, PBD97, Pre97a, Pre99, Pre94b, QG90, Roe94, Sch91b, Sch91c, Sch93f, SV94, SRY99, Sta94b, Vau93.
Zhe90, vW94, AB96b, BSNP96a, BSNP96b, BD92, Dam90b, DK94, Gon95, HLMW93, HXMW94, HYL79, JG95, KL95b, MZ98, PG91, Pre9a, PrO95, RP95b, Roe95, SV95a, SRRL98, Sim98c, Tsu92b, Tsu92a, YL97c, DBGV93, Sch93g, EPR99b.

Hash-and-Sign [GHR99]. Hash-Based [PRZ99]. Hash-FUNCTIONS [QG90, ISO97]. Hash-VALUES [GS94a]. Hashing [AS96, BGG94, DC98b, FNSS92, KP97, Kra94b, KBC97, PS93b, Rog95, Rus93b, Sch91c, Sch93f, Sho96, Sti91b, TZ94, BGV96, Bos90, PJB90, Sab94, Sch93g, Sta99b, PS99a, SN98b, She92d, She95b, Sut99, VNW94, Du98, Graxx, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Un96a, Yeu97].

High-Assurance [IEE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Chi99a, Chi99b]. High-Frequency [MS99a]. High-level [Rus90]. High-Performance [ACM98a, BMS99, GN95c, IEE94e, Sut99, NO96]. high-quality [Yeu97]. High-Radix [Kor93].

High-Speed [ARV99a, ARV99b, Ano99c, BCR98, Bla96a, Bla96b, BMS99, Ch99a, Ch99b, DP98a, DP98b, Ebe93, FVE99, FP99, Gar97a, Gar98b, GRN95c, HR90, IEE94e, IEE96d, IM93a, IM93b, Kap98, Ko94, Ko93, KB92, LS97, MPPS95, MS99a, Ru90, SKNO98a, SKNO98b, She92d, She95b, Sut99, VNW94, Du98, Graxx, Lam99, Nor95a, Nor95b, NO96, She92c, She95c, Un96a, Yeu97].

High-Assurance [IEE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Chi99a, Chi99b]. High-Frequency [MS99a]. High-level [Rus90]. High-Performance [ACM98a, BMS99, GN95c, IEE94e, Sut99, NO96]. high-quality [Yeu97]. High-Radix [Kor93].

High-Speed [ARV99a, ARV99b, Ano99c, BCR98, Bla96a, Bla96b, BMS99, Ch99a, Ch99b, DP98a, DP98b, Ebe93, IM93b, Ko94, MPPS95, SKNO98a, SKNO98b, IM93a, Nor95a]. Higher [Jak99a, KM99, Lea99, MSK98, SM98a]. Higher-order [Jak99a]. Highly [MS99b, PV97, ARK99]. Highway [An94c].

High-Assurance [IEE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Chi99a, Chi99b]. High-Frequency [MS99a]. High-level [Rus90]. High-Performance [ACM98a, BMS99, GN95c, IEE94e, Sut99, NO96]. high-quality [Yeu97]. High-Radix [Kor93].

High-Speed [ARV99a, ARV99b, Ano99c, BCR98, Bla96a, Bla96b, BMS99, Ch99a, Ch99b, DP98a, DP98b, Ebe93, IM93b, Ko94, MPPS95, SKNO98a, SKNO98b, IM93a, Nor95a]. Higher [Jak99a, KM99, Lea99, MSK98, SM98a]. Higher-order [Jak99a]. Highly [MS99b, PV97, ARK99]. Highway [An94c].

High-Assurance [IEE96d]. High-Bandwidth [Bla96a, Bla96b]. High-Capacity [Gar97a, Gar98b]. High-confidence [Chi99a, Chi99b]. High-Frequency [MS99a]. High-level [Rus90]. High-Performance [ACM98a, BMS99, GN95c, IEE94e, Sut99, NO96]. high-quality [Yeu97]. High-Radix [Kor93].
Holiday [IEE94a]. Holy [Sal99]. Home [Hus99, Ano97t, Hod97]. Homomorphic [FDB93a, Bet95c, FDB93b].

Homomorphism [Dom96]. Homomorphisms [Bur96, SK94], homophonic [HYHW98]. Honest [Rab94].

Hood [Sch93e]. Hook [Ros96c]. Hope [BCE+94]. Hopes [GO96c]. hopping [MHMW98, Tod97]. Hor [IPNdbbbprm91].

horse [Sch99f]. Host [Kol95, BGT96]. host-centric [BGT96]. Hostile [GSTY96, SKAM99, LC95]. Hot [IEE98b, IEE99b, Bra90b, CB96].

Hotel [LW96, Nat98]. HotOS [IEE99b]. HotOS-VII [IEE99b]. Hundred [Uni97a, Uni98c, Uni98d, Uni98e, Uni96b, Uni97b, Uni98f, Uni98h, Uni97c, Uni99a, Uni98k]. Hungary [Rue93]. hunger [WSFC99]. Hurt [Gar97a]. Hut [We97f].


Hyperelliptic [Sma99, BKZ98, OS91, OS92, SS94a, KM99b, KI96, LMBO95, LML98, NP97, OO98, OKa93, SK90a]. Identities [MS99a, Sar99]. Identities-Based [Dan95, DQ94, SS98a, OKa93b, Sak96, Sch90b, Ver95, BBC98, BM95, BM91b, DF91b, DF98, LHC99, IS99, Kunn97, Mu92, SN98b, Sch90a].

Hypermix [K99]. HyperText [RS96a]. Hypotheses [ZMI90, Uni98d]. Hypothesis [MU98].

I/O [Got99]. IBM [Com90, Gar98b, Zun98]. IC [DDJ98g, DDJ98h, JT97a, PC98].

ICALP'99 [vWN99]. ICARUS [Var99b]. ICE [Kwa97, VK98]. ICICS [HO97].

ICIP [Ano94d, IEE96c]. ICIP-94 [Ano94d]. ICL [CFK+91]. ICISA [Nie99]. ID [CS97c, Hwa92a, Hwa92b, Hwa92c, JY98, LHW99, MS98a, Mu92, TC91]. ID-based [CS97c, Hwa92a, Hwa92b, Hwa92c, JY98, LHW99, MS98a, Mu92, TC91]. idea [OA99, BBS99b, BKR97, DGV94c, HO96, Haw98b, Haw98a, KSW96, Lip99, Me94, Sch93d].

Ideal [ABD97, BCR93a, BD90, BCR97, BP97c, Pai98a, Pai98b]. Idealised [RS99c].

Idealized [MTES99, MM92b]. Ideals [GPT91a, GPT91b]. Ideals [FGH99, RS99d, TCH+91]. Identical [BCCG99].

Identifiable [KOO95b, KOO95a]. Identification [BCCG93, BLM94, BDB92, Cha94b, GS94a, KM99b, KI96, LMBO95, LML98, NP97, OO98, OKa93, Sak96, Sch90b, Ste94a, Ver95, BBC98, BM95, BM91b, DF91b, DF98, LHC99, IS99, Kunn97, Mu92, SN98b, Sch90a]. Identities [MS99a, Sar99].

Identity [Al90, Dan95, DQ94, FMY98, HJP97, JG90, KP98, L999a, SS98a, Gua99, OU98b, Tan90]. Identity-Based [Dan95, DQ94, SS98a, OU98b, Tan90].

IEC [Int91a, GQW+91]. IEEE [Ano95n, CH96, Ano96k, Ano97-28, Ano98i, IEE95c, IEE95b, IEE96d, Kal97a, KK99b, LW96, Pit95]. IEEE-IMS [IEE94a]. IETF [Ano97c]. If [GPR98]. IFIP [Kat97, LM98a].

IFIP/GI [LM98a]. II [Sch99b, AK99, Ano97w, Ano98c, Ano99c, BS91f, CFG96, CK95, CW91b, Dav98a, Don98, Eri97b, Mit92b, Mon96, Mus92, Pin98, Rat96, Rey97, RP97b, Ros99, Sch93f, Sch93g, USE90, Van93, Wil98a]. III [Fir92b, Gan93, GN95c, Nor95a, Ree98, Rey99, USE92b]. iKP [HS96]. ilicit [SG96b]. Illinois [USE99c]. IMA [Boy95b, Dar97, Fur93, Wal99a]. Image [BKZ98, BNP99, DS96, DP99, Fri93, HPA99, HPG98, HWW98, IEE95a, IEE97a, IEE96e, IEE97h, IEE97j, KZ95, KM92, LMP99, Mac98, Man98, Pit95, PZ97, PNF95, Sch99b, SC95a, SCx9a, SJ97, SD97, SZ96b, TOH97, VP99, Wal95, YKY99, BCP99b, BCD98, CCH98, JT96, JT97b, KS98c, KG93, KH97, NP98b, OP97, OP98, Oko96].
PBBC97, Sch98b, Sea95, SHG98, TKS98, VP96, VP98, Xie98, YM98, CFK+91.

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

Images [BLMO95, BO96b, BI99, Car95, JI98c, KR98, KPR99, LvdLL97, Lvd98, LSV95, MFG95, NNEK97, Per97, SC96b, SZT96a, WD96, ZK95, BP98b, BP98c, BBCP97, BBCP98a, BCC97, BOD95, CKLS96c, HW98b, lbb97, Irw98, Nas94, Nat97a, ODB96, ÔPH+99, Pit96a, RRP97, RKB96, TA97, XBA97, ZL97]. Imaginary [HJPT98b, HJPT98a, ZPY96]. Imagination [Sha99a, Ros97c]. Imaging [AA97, RP97b, Yeu97].


Impact [Mar96, Ven90]. Impeding [Bra95c]. imperfectible [CKLS96b]. imperfect [MY98]. Imperfectly [BMC95]. impersonation [SNT93]. Implementation [Au96, Bi97b, Bra96, BS91b, Dae99, DGT96, DRR95, DBVD96, Ebe93, Fe'93, Fei96, FOM91, Gla99a, HKQ99, HRV99, IMI93b, KP99a, Kob98c, Koc94, Koc96a, Lan97, LCN99, NM99, OSA91, PL94, PP90, Ros96b, SJS98, She95b, Tou92, Var99a, YKY99, You97, Zim99, BR96b, BC90, CKM99, Dia91, HNM98, IMI93a, LSA98a, Men91, MV90, MZ98, MPL99, Nor95a, Pai96, Per91, SSS98a, See97, SAM97, VAD95, XL98, Koe99].

Implementations [Bas98, Bri90b, Gon98, HK98, HK99d, Koc96b, Mos98, SV93, Wai99c, Web98, WS98, Gai99, KSK96, Zho94].

Implementing [SAS99b, Van95a, Lee99a]. Implications [Bas93, CMYY98, NS99b, PN92, Van95a, We95]. Implicit [Jam98, MLY93]. Implicitly [HRVV99]. implies [LHL95b, LHL95a]. Importance [BDL97, Sch99b, CM97d]. important [Sta94a, Woe97]. Impossibility [MP91]. Impossible [BBS99a, Fer99a, BBS98a, OK96a].

Imprimitive [Pat99]. Improve [Far92]. Improved [Ano96e, BK98e, Boy90, BS91g, CRRY99, CJB+92, JMI99, JJ99b, KM96b, LD99, RP95b, SH97, SAM97, WS98, YL95b, YL95a, ZYR91, Cao99, He92, NMVR95a, NMVR95b, SH95a, SH95b]. improvement [BB95b, Bir95]. Improvements [HJL99, Kle90, IKNY98]. Improving [BHS93, BKP93, GLV99, SF97, SZZ94a, SMK98a, Sun98a, HM97b]. Impulse [She92c]. IMS [IEE94a]. In-memory [Ven90]. in/for [SH98]. Inaccuracies [OD99]. inadequacy [Kah98b]. Including [DGV93, DW94, JS95b, JS95a, KL95b, UU97a]. incorporation [Ano95c]. increased [HS96b]. Increasing [AP93, Bao94, BKR98a, BKR98b, Bla94a, KFJP96, Mar97]. Incremental [BGG94, BGG95, BD93, Fis97].


industrial [CWM+91, PGV93d, PR98]. industries [CWM+91]. Industry [ANS98b, Kan96, Lea99, Uni98b, AA95, Acc97, CWM+91, Uni98k, Wel95, Zaj97]. ineffective [Min97, MBY97]. inequalities [van97a]. Inequality [MS99b]. Inference [ZHI98, Jan95]. Infinite [CK90, HKL94]. infinitely [It91]. infinitesimal [Mra95]. Influence [MM92b, NH98]. Infocom [IEE92d, IEE94f, IEE95c]. Inform [YT96]. Information [And96c, Int91a, Ano93g, Ano95j, Ano95l, ...]
Ano96a, Ano97h, Auc98, AR99, Bar94, Bas93, BDGV93, BLMO95, BS91g, Cae98, CFGS99, CW94, CFG96, Den99, DMFB97, GRS96, HGHD98, HOQ97, Hei96a, HH94, HR90, IEE94a, IEE97k, ISO97, KG96, KRJ98, KM96a, LOX99, LBHM99, Lin96a, Mau93a, MW96a, Mau97a, Mau99a, Mau99b, MO99, Nys99, ODP98, Orl96, Ped91d, PL94, Phi96a, Phi98, Pit96b, P99a, PGV93c, Pre98c, RAS93e, RSA99a, RIP95a, Sch97d, Sga93, STP93, SC96b, Sti93a, Stu99, Uni98i, Uni98k, VPM97, Wol98, Ada91, BDGV96, BP95b, BDC95, Bra90d, CM95, CC95, CKGS98, DL96, Dav98c, DF98, FM98b, Gru98, Gua90, HW91, IEE95c, Jac90a, Jac90b, Ken95, KS98c, KW92, Mar95b, Mau93b, NIS92, Ped91b, Ped91e, Rot95a, Sch90c, Sch97c, SG96b, Sim92, Tas98.

MSN98, MSN99, MTVZ92, MAO96, MM98a, MM98b, NMR95, NS97a, Nec96, Neu97, NS99a, Oka94, OU98a, Oka98a, Oka98b, Omm90, vO91a, PSSR97, Pa99d, PKOT94, Pat95, Pio97, PB99a, RSA93b, RSA93e, RSA94, ROT94, RS98c, RS98d, Ros96a, Ros96c, Ros96f, Ros97b, Ros98b, Ros98c, RCM99, SS98a, SYM98, Sam98, DP91, Sas99a, Sch94b, SKW+98a]. Key
[SKW99, SOOS95, SM95a, SE96, Sha99b, Sh94d, SiK93, SR96, Sta99b, ST91, SW99b, SH4, Sun98a, Sut99, TAP90, Uni98i, Van95a, Van93, VSH97, VvT97, VBD99, VM93, dWQ91b, WLEB96, WW98b, WKS+99, Wie96, Wie97, Wie98a, Wie98b, Wob98, Yam98b, YST99a, YST99b, dWQ91a, vO91b, vW96, AA95, Acc97, Lip98, AD97, AD99, AI96, Ano90, Ano96m, BSNP96a, BSNP96b, Bao94, BI94, BDHJ97, BD98a, BT998, BSB97, BR96b, BCK98, BY93c, BY93b, BS91a, BFS92a, BGF+95a, BMP97a, BF96, Bc96, BMS96, BFS98, BM95, Boy97, Bur94a, BD95b, CC99a, CW97, Cle96, Craf97, Cus95, Dkr97b, DWZ96, DS90a, DH96a, Des95, DvQ96, Dhe98, Dy92, DN95b, ES97, FDB93b, FMY97a, Fre94, Fro96, FGL96a, FGL96b, FL93, Gar96b, GH96, Gib95, GBL94]. key
[GH99, GTS90, HNSM91, HP99a, HP99b, HY93b, Haw98a, He92, Hvf96, HJJ+97, HI97, HY98b, HY98a, Hwa92a, Hwa92b, Hwa92c, Hwa93, IZ98, IZ99, JM96a, Jar96, JLM+94, Jon90, YJ98, KASH90, KM99a, KS97a, KSW97b, KL94, KR96b, Kir95, Koo97, KM99d, Kos99, Kum97, LC97, Las92, LMJ93, Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LL95b, LCL95, Lon91, Lon92, Low95, MS98a, Mao97, MLA91, Man91b, MY93b, MkkW99, Mu92, MLL95, NM96a, NY90, Nat97a, Nee91, Odd94b, Oli95, PS98c, PS98f, Pet91, PP92b, RT93, Roe99, Sal90, Sal96, SW95a, Sch92c, Sha95a, She96a, She92c, SKB97, SY96b, SM90, Smi93b, SS95b, SS95c, STW95, Sun91a, SS98b, Syv93, SM95b, Tab94, Tao94, TCC97, TC99b, TC99a, Ts90, TC91, Tze99, TH99, Uni97c, Uni95a, VW96, Ven92, Wan92b, Wie94]. key
[Wil93b, Xie92, Xie93, XLP99, XW97, Yam98a, YL97a, Yu92, Zha91, Zhe95a, Zhe95b, vW91, vO92, vT90, MC96, BFS92b]. Key-Agreement [RSA93b].
Key-dependency [MAO96].
Key-Dependent [FBS98]. Key-Escrow [VvT97]. Key-Exchange [Dan95].
key-management [MLA91].
Key-Extraction [Oka98a, Oka98b].
Key-Schedule [KSW96]. Key-Search [SP99a]. Key-Share [BWM99b].
Key-signing [Ros96a, Ros96c, Ros96f].
Key-specific [LMS97]. Key-vowel [LP98].
Keyboards [CFK+91]. Keyed [Ano95a, BFN98b, KBC97, Luc97, Luc99c, LW99, MS95c, MS95d, Pre95b, MS95e, BFN98a, Gon95, KBC96]. Keyed-Hashing [KBC97].
Keyed-MD5 [KBC96]. Keying [BCK96d, BCKxx].
KeyNote [BFK99]. Keys [ACM94b, ADF98, BV96, BF97b, Bur94c, Da9e98, EHMS99, Gir91, KSHW97, KSHW98, KM99c, Luc98b, MP91, PS98g, SV99a, SV99b, Ste94a, Van96, Way96b, Bi94a, CH97b, Cli99, DGV94c, JP96, KC95, Lw95, LL93b, MW99, MF97, Mok97, SSI97a, SSI97b, Sv98, SH99, Sta95a].
Keyspace [CD98c]. keystream [CS96b, CS97b]. keystroke [JG90]. KG
[Uni94a, Uni94b]. KG-194 [Uni94a, Uni94b]. KG-94 [Uni94a, Uni94b].
KHF [Wag98a]. Khufu [BBS99b, GC94].
Khwarizmi [CFK+91]. Kid [FK93a]. kids [WS96c].
Kimba [KW99].
King [AM97, Gad91, SX90].
Kingdoms [D98, Lom97].
Kingston [TM99].
Kiosk [BO96a, Gar96b]. kit [An97u, Sm91b].
Kleptographic [YY97b]. Kleptography [YY97a]. KMOV [Ble97].
KNS [SMK98a].
Knapsack
knapsack-based [He92]. Knapsacks [CJS91, Ort95b, Ort95a]. Know [DDJ98b, Fly97, Hil97, Kir95, Mil95].


Lee/Alek [Scu92]. legacy [Uni92]. Legal [CYY98, HA96, Mos98, Rad97, Ros95b, Wri94, Ame95, Ame96a, Sch93e]. Legislation [RDK98, May97]. legislative [Cll99]. legitimate [Cll99]. Leighton [Zhe95a]. lemma [HKM95]. Lempel [Mun91a, Mun91b]. lend [Ril96]. Length [BR99a, BR99b, GS94a, Sch94b, YY98a, CC98, Han94, KL95b, MPL99, Su98, ZPS93]. Length-3 [YY98a]. length-restricted
Lengths [BDR+96, HMV93].
Less [FCD98], less [ZTR99].
Lessons [McC96], let [DDJ98c, DDJ98f],
lets [Way93b], let [YT96], letter [BCE+94, Joh99].
Letters [Bur98b, MGL^+98, PKA^+98, SVA^+98, BY92].
Leuven [PCE93d, Pre95a, PR98].
Levels [Bor96, GTGW94, dVdVI98].
LFSR [Kra94b].
LFSR-Based [Kra94b].
Li [JW01, vT93].
Li-Wang [vT93], li.vi.5 [CFK+91].
liberty [Ele99, Wad98].
Libraries [AR97, BPBV99, DL99, IEE98d, SHG98, DSSZ99].
Library [ANO97v, CFK+91, DK91, KHB99, Dhe98, RRP97, Man98].
License [AG99].
Licenses [ANO97v, TJ97].
Life [CJ99, DDJ98e, DDJ98f, DQ94, GAGCDAFC99, Ros95a, CWM+91].
Life-Span [DQ94].
Lift [Gar97a].
liftings [CNST98].
Light [Gar97b, HP98, YHY98, BGH^+95].
light-weight [BGH^+95].
Like [JQ97, BS90a, BS91c, CCZ98, Kob99, MS95f, MT99c, Nac93, WSCF99, XZZ97, Kim93, KP93, Way93a].
Likely [Bar96a].
Limit [Lea99, Way93c].
Limitations [BM91a, CM99, Fis98, KV94].
Limited [AR99, BDS98, DQ96, VB99].
Limiting [KI96].
Limits [And96b, AP98, EKK99, Swi97, BH98, SOB98].
Line [EKM90, EG96].
Linear [ANO95a, AMP99, BGS96, BK94a, BL95, BP99, CFSY96, Dae95, DD99, Des98a, vD95a, DLR97, Gol95b, HO96, Haw98b, KR94b, KR95a, KTM^+99, KR99b, LO91b, LH94, MS94a, Mat93, Mat94b, Mat96a, Nyb95, OA94, Ros98a, SZ96, SF97, Sch96c, Sch99l, Sel98a, SK98c, SK98b, TN97, TSM95, YMP99, ZYR91, Ala93a, AW95, BSN95, Bao94, BI93, Bh95b, BD95a, CC98, CV95, FCD98, FR95b, GN95a, KM95, Haw98a, Jak98, KY95b, KYx, KR96c, Kuk99, Lai95, LL98, Lan95, MM90a, MO96, MK92, OG95, SK94, Tze99, YT95a, YT95b, ZYR90, ZH90, vD95b, vT94, Duh90].
Linear-Time [KR99b].
linearity [SB95].
Linguistic [CH99b].
linkage [HCY96b, LC97a].
Linked [BRS99].
Linking [BLLV98, CM95, RP94, SM99].
Links [Blo99, CV95, DNM98, JC93].
L'inuktitut [ANO99g].
Linux [Cor98, DDJ98a, Eri97b, Mori97].
Lion [AB96a].
Lippman [vDWS97, vS97].
LISA [USE99b].
LISA'96 [USE96a].
list [LC97b, Uni97d].
literate [Sab94].
little [ANO91b].
lives [DDJ98d].
LL [FY95a].
LLL [Mis97].
Local [Fum93, IEE97l, IEE98f, MM95].
Localization [PJ99].
Locating [KP93].
Location [FJP96, Jac96, KFJP96, KR98, WHFG92, FT95].
locking [CS96b, C97b].
Locks [Way95, CC95].
Locomotive [Var99b].
Loen [LW96].
Loftus [Hel94].
Log [Bal99, GJKR99, Gor93a, PS98b, WD98, YYY7b, Kob90, SS95a, SK97d].
logarithm [CPS95, CS97d, FR94, FMR99, HY93b, HI97, HMP95, Mc99a, MVZ98, NR95].
Logarithms [BBT94, CH98, GM93b, LO91a, Mau94, MW99, vO91a, She97, Tes98, vO91b, vW94, Gor93b, HZ93, Odl94a, SS95b, SS95c, vO92].
LOGCFL [LSMV99].
Logging [Zol93].
Logic [AHMS99, BRS99, BAN90, CIBM99, CO98, DRR95, Gue98b, SG95, SM95a, SHK99b, CS99, Pos98].
Logical [PS99f, Wad93].
Logics [ADD99, GAGCDAFC99, KW99, Len99b, WK96, Bad99, XZZ97].
Login [ARH95, DQ93, Hil97].
Logout [Poo95].
Logs [SK98a, SK99]. LOKI [BS91f, BKPS93, Knu92, Knu93c, Knu95, TSM95].
LOKI91 [Knu93d, Knu93a, SF97]. LOKI97 [BP598, RK98a, Ri91j]. London
[Ano93d, Ano97p]. Lone [Ano97r].
LONE-TAR [Ano97t]. Long
[CHN97, Len96, RH93, SSS98, Pos93].
Long-term [CHN97]. Longevity [Rot95b].
Look [Coh96, Has99, Pfl95, Zha97, GTGW94, Way91]. Look-up [Has99].
Looks [Sch97b, vdWS97, vS97]. Loops [SvA98, SHK99b]. Lorenz
[Car97b, Dav98d]. Lose [GPR98, Way96b].
Loss [Law98]. Lossy [CI96]. Lo-Lo [BKR98a, BKR98b, Luc96a, Luc96b, PRS99].
Lucas-based [BBL95]. Lucent [MB99a].
Lucifer [BB94, BS91f]. lun [XtMn94].
Lunch [DDJ98e, DDJ98f]. Lured [Che92].
Lurking [Joh96]. lustre [Alv98a]. LVQ
[LSVV95]. Lyndon [SM90, SSM92]. Lyon
[FR95a].

M [IEE97c, WG97, Mau91b]. M.A.P.
[BBC98]. M6 [KSW99b, KSW99c]. ma
[XtMn94, KP99b]. MAC
[Mit92a, PVo95, PVo96, Pre97a, SRRL98, SRY99, Yuv97, Ano93k]. MacArthur
[De92]. MacGuffin [BS95a]. Machine
[KP99a, NM99, PF94, QD91, Riv93b, Wic90, Cra92, Dav98a, Daw96, Kru98]. Machines
[Bur99, CFK+91, FM999, SK98a, Dav98c, Jan95, Se99b]. Macintosh
[Sch94l]. Macquarie
[KG93]. MACs [AP99a, AP99b, BGR95, Jv98a, NR98, PVo95].
Made [GSV99, Kra94a, Gol97c, KKL99].
Maestro [CFK+91]. MAGENTA
[Bi99a, Hub98, BBF+98]. Magic
[BD99a, JM99, AGLL95, Kah98c, RK98b].
MagiCol [GLSM99]. magnetic
[Ano90, Gut96]. Mail
[Ano93j, DN93, Got99, Ken93, Lin93a, RS98b, Sch95c, Sch95d, SH97, VJ98, Ano95c, Gar97b, LF97, Lin88a, Lin89a, Mit92a, Ri96, She96a, Str93a, Str93b, Bac95, Zeg93, Sta94a].
MailSafe [RSA94]. Mainframes
[Deu97, Deu98]. Mainstream [Gar97b].
Maintain [Wed99]. Maintaining
[CH94a, CHH97, Gar94]. maintenance
[Uni94b]. MAINZ [PU99]. Majesty
[Ber96a]. Major [Law98]. Majorities
[Cha90]. Majority [Mv93]. Make
[Ano93c, GGMM97, CM99d]. Makes
[Ame96b]. Making
[ASW99, CKN99, DDJ98e, DDJ98f, Des90b, Hir93, Lut98, PRS99, Sar97, Tra97, VM96, Way98, BKR98a, BKR98b, Wri98, Zaj97].
Malaysia [GO96c, WSFC99]. Malicious
[PM98]. Malleable
[DDN91a, BS99b, BS99c, DDN91b, Sah99].
Malo [GQ95, QG95]. Man [CFK+91, Mon96, IPNddbbprm91].
Management [Ano99f, AWV99, AG99, Bla94b, BPK99, Col96, Dae98, FJP96, FY98b, Fun98e, Fun93, GM93a, GH96, KMP99, KFJP96, Neu97, Rob98a, SS99b, Yac99a, Yac99b, CWM+91, Hat97, L98a, MLA91, MKKW99, PS98f, Pos92]. Manager [VDDR99].
Masking [CJM95, JMLW94, SZTB98, Til98]. Masonic [Mor92]. Mass [USE98b, ZTR99]. Massachusetts [ACM96a, IEE95c, IEE98f, USE94].
Measurements [VNW94]. Mechanical [SY99]. Mechanics [PT95, Ros97a]. Mechanising [BP98]. Mechanism
Mechanisms
[HL99, Mye94a, CGM96, HC95a, ZH93].
mechanization [BoI97]. Mechanized
[SM95a]. Medals [DDJ98b]. Media
[DDJ98d, GB98, Hat96, MW98b, Ros94].
median [KR99b]. Mediated [FJ98].
Mediator [Kem99]. medical [SMA95].
Meet [FY99, Van95b]. meeting
[Shp99a, Zim96b]. Mellen
[Ers99]. Members [Par98c]. Membership
[FGR92, Fis98, OOK91, SPH99, AK95,
MW94, Sak97]. Memoir [Bar05]. memoirs
[RK98b, Sel94]. Memorial [IEE98b].
Memory [ARV99a, ARV99b, CM97a,
DHMR96, Fis97, Got99, KS99a, Lei99b,
MS91, Sha95a, Gut96, Has99, Ven90].
Memory-Bounded [CM97a]. Menezes
[Sha99a, Kie98]. Mental
[CF99, Jun99, KOT91]. Merced [GC97].
Merging [DVQ96]. Merkle [NS97c, NS97b].
Meta-Object [EKLM99]. Meta-Protocols
[FB95]. MetaML [MTE99]. Metaphor
[BP95a, Fue99]. Metaphors [BHM99].
Metaproof [DY91a, DY91c]. Meteor
[Sch93a, UNU94]. Metering
[SK96b, SK96e, Ros94]. Method
[AG98a, AG98b, ADD99, BP98f, ESST99,
GDD+97, HRVV99, KI97, KT93, LL94a,
Mat94b, McM96, MS95f, Mi93c, SF97,
SKBxx, Tes98, VNW94, CP94, CM97c,
GTS90, JT96, JT97b, Joh98, KM98b, KAK96,
KH97, LC98, Mat93, MY93a, McK99, Pit66a,
RT93, SH99, Su98, Vu95, YEA+98, ZH90].
méthodes [Bec90]. Methodology [CH99b,
DD95, FM98a, NMR95, PNFK95, SSSW98].
Methods [Bas93, Bir99, CL98, DS999,
GSY99, IM93b, KRBS97, LvdLL97, LM98b,
MCD99, Per99, SW94a, AhdJF97, ALE92,
At94, Bau97, BGR95, Car97c, HLC99,
IM93a, vdL98, QN98b, RT93, Rho95,
Shp99b, TG94, Whi93, XL98, van98].
Metric [Jose98, RS99b]. Metrics [LA98].
Metropolis [DP99]. Mexico [IEE91].
Meyer [Lu98a, Lu98b, JQ98b].
Meyer-Müller [JQ98b]. Mi [XiTmW94].
Miami [IEE97f]. Micali [Zhe95a]. Micro
[An97q, HSW96, Pri94]. Micro-payments
[HSW96]. microcomputer [HNM98].
microcontroller [Kuh98].
Microcontrollers [KKW99]. MicroMint
[RS96b, RS96c]. Micropayment
[JO97, RS96c, RS96b]. Micropayments
[Riv97a]. Microprocessor
[DDJ98d, Mar96]. microprocessors
[NM96b]. Microsoft
[Boy98, Fly97, Gar98a, SM98a, Ts97].
Middle [BBS99b]. Middleware [BCCD99].
Might [DDJ98c, DDJ98d, Military
[An96n, Fri92a, Fri92b, LU95]. Millicent
[Man95]. Million [Ran01, Riv91a]. Millions
[Wal99b]. MIMD [DHW95a, DHW95b].
MIMD-factorisation [DHW95a, DHW95b].
MIME
[An95c, An95n, An96k, Elk96, GMCF95].
HEG98, LT98, QN98a, QN98b, SB98].
MPEG-2 [DS97c, HG97e, HG97d].
MPEG-4 [HEG98].
MPEG-encoded [DS97b].
MPEG2 [CPO +98, CHO +98, DDNM98].
MRA [BAL98, LFCK99]. Ms [CFK +91, Gar98a].
MS-DOS [Gar98a].
MSC [WSFC99].
M¨uller [JQ98b].
Multi [CM99b]. Multi-agent [CM99b].
Multi-BBBF97, BDD +94, BM99c, CC99c, CFY96, DFGH99, DF97, FHM98, HS94, HWT99, H1V98, JV96, KSB97, Lee99b, Mar98a, PM99a, SNW98b, SJS98, Sut99, TN96a, TN96b, VCN99, CL97a, CGS97, HW98c, KSB96b, SVWMB95, SOB98, VSB95].
Multi-Agent [Lee99b, VCN99, HWT99, PM99a].
Multi-Application [Mar98a, DF97].
Multi-authority [CFSY96, CGS97].
multi-carrier [SVWMB95, SOB98, VSB95].
multi-exponentiation [CL97a].
multi-function [KSB97, KSB96b].
Multi-Level [H1V98]. Multi-Party [JV96, FHM98]. Multi-Purpose [Sut99].
Multi-Service [HS94]. Multi-tiered [CC99c]. Multi-user [SJS98].
Multi-variable [TN96a, TN96b].
Multiapplication [Gir99, Tua99].
Multicast [CMN99, PB99a, Mit92a].
Multifeature [Bet95c]. Multifunction [She94c]. Multigroups [OK91].
Multiplelevel [CGB +93, GPSN98, KT96, DN95a, ZH93].
Multimedia [ACM96a, ADF98, CLKL96a, CKLS97, Dan96, D +98, ES98, FJV97, GO96c, HF97, IEE96b, IEE98c, IR99, KBR98, LdvlLB96, Lip99, NAA99, ZK96, CKLS96b, IEE97k, Kat97, LS98a, Oko97, PSB97].
Multipart [GMCF95]. Multipart/Encrypted [GMCF95].
Multipart/Signed [GMCF95].
Multipart [GMCF95]. Multi-party [Cha90, CDD +99, FW91, MH96].
Multipermutations [SV94, SV95a, Vau95].
Multiple [AS96, Bih98a, Boy90, DK96, GO96b, Han94, Kall92, KR94b, KR96a, SS99c, SHK99b, Wag98b, Bih95a, GGK +99, GPSN97, KR95a, KSL92, Ort95b, Ort95a, SS99].
multiple-iterated [Ort95b, Ort95a].
Multiple-length [Han94].
Multiple-precision [Kal92]. multiplexer [SGSD99].
Multiplication [Abe99, KAK96, Kor93, MS93, Zim99, FB96, Has99, LC98, TY92].
Multiplications [MNSV97].
Multiplicative [BBDW96, DDB95a, DDB95b, Mis97].
Multiplier [HMvT94, HWB93].
Multiprocessor [MHPS96].
Multiprocessors [Lei99b, HJ99].
Multireceiver [SNW98a]. Multiresolution [BCV97, HW98b, SZT98a, SZT98b, XBA97, Kh98a].
Multiround [Geh94, Geh95].
Multisecret [DLR97, JMO94, WAMO94].
Multisecret-Sharing [DLR97].
Multisender [MSN97]. Multisignature [OO93, CLHL98, FD92, HZ93, HCC98, LHW99, LHL95b, LHL95a, PPKW97].
Multitude [Fuc99]. multiuser [LS98a].
multivalued [CGV94].
multiple [ISO97, TN97]. n-bit [ISO97].
Naccache [Cus97].
Naccache-Stern [Cus97]. nag [LPNdbbprm91].
Name [CLW98].
[Gar97a, Gar97b, Ano97q, Lea90]. 
Non-Abelian [DDB95b, DDB95a].
Non-biased [TSY98].
Non-carcinogenic [SBTV99].
Non-classical [Mas99a].
Non-Commutative [GPT91a, GPT91b].
Non-Encrypting [LW99].
Non-Euclidean [SCG99].
Non-Existence [FDB93a, FDB93b].
Non-Interactive [DY91a, GO93, MY91, BM90, BG90, DDP99, Ped91d, Ped91b, RS91, DY91c, SCG99, TSY98, Yah94, Ano95k, BKR98a, BKR98b, DDB95b, Ell97, HJPT98a, LL99, MY93b, SB95, Sin95, SBTV99, DDB95a].
Non-Abelian [DDB95b, DDB95a].
Non-Oracle [Ano95k].
Non-perfect [Pai98a, Pai98b].
Non-Reachability [DR94c].
Non-repudiation [GP99].
Non-secret [Ell97].
Non-secure [Sin95].
Non-Synchronized [Yah94].
Non-uniform [AWV99].
Nonadditive [RV99].
nonce [KSL92].
nonce-based [KSL92].
Noncryptographic [Fei99].
Nondeterministic [Mol98].
nonequivalence [Mol98].
nongroup [SBVG99].
Noninteractive [GSV99, Ped91c].
Noninterference [MC92].
Nonlinear [Gys96, KT91b, MS99b, Pit95, Gol99c, RD96b].
Nonlinearity [MS90a, SZZ95c, SZZ95a].
Nonlinearly [MS94].
Nonmonotonic [COM93].
Nonoblivious [FNS92].
Nonperfect [KOS+94, OKT93, OK98, OK95].
Nonrecursive [Ruo94].
Nonrepudiable [LHW98].

Perfectly \[BDHK93\]. Perfectly-Secure \[BDHK93\]. Performance \[ACM98a, Ano95b, BMS99, DMPW98, FC94, GN95c, HJL99, HWJ98, IEE94e, KR96a, Kea99, LL95a, LM98b, PRB98b, Roe94, Roe95, SKW+99c, SKW+99a, SKW+99b, She92e, Sm99, Sut99, Tou95, VNW94, Wie98b, Nor95b, NO96, SS98\]. Performer \[KS98b\]. Period \[RH99\]. Periodic \[Mun91a, Mun91b, Abe98b\]. Periods \[GvP98\]. Perl \[DDJ98a\]. Permit \[Joh94\]. Permits \[Gar97b\]. Permutation \[BM92, BS90b, CT99a, EM93, HMvT94, Pai99c, Pat99a, Sha94, SMK98b\]. Permutations \[BY93a, DW94, FJRS96, SPS97, CCZ98, Pat91a, Pie93, Sha94, SMK98b\]. Permuted \[BCCG93, KM99b\]. perpetual \[HJKY95\]. Persistence \[DL99\]. Person \[BBDF97, Ble98b, DLF97, DMFB97, WKHG97, BCB97\]. Personal \[Ano97s, BE90, Bar05, Cae96b, EHMS99, Gar97b, Hamxx, Los97, Los98, RSA99a, Rivxx, Cra96, Mil99, Wi99a\]. Personalized \[GGMM97\]. Perspective \[Bre99, Cae96a, CM99b, Ori96, Swi97, UFC94\]. Perspectives \[GO96c, Riv97b, Bro96, LKB+94\]. pertaining \[Ch94b, Perugia \[De 95\]. pessimistic \[Kru98\]. Petard \[WG97\]. Peter \[vdWS97, vS97\]. Petro \[La92\]. Petre \[CFK+91\]. Petri \[DR98b, KA99, LL97a, NT93, YK98\]. PGM \[HMvT94, MMT90, MM90a, MM90b\]. PGP \[Ano97s, ASZ96, Elk96, End97, Gar95, GM95a, Gar98c, Joh96, Kar96, Ken95, MR98, MLLG95, Ros95a, Ros95b, Ros96a, Ros96b, Ros96e, Ros96f, Ros97b, Ros98b, Ros98c, SA95, Sta94a, Sta95a, Sta95b, WCSS95, WTZ99, Zim95a, Zim95b\]. 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 \[Fri93\]. Physical \[GBC93, Oka93a, Sal98\]. Physically \[Wai90\]. physics \[Sch97c, Sch97e\]. Picard \[BSB97\]. Picking \[Way95\]. Picture \[GDD+97, MT94, DDM98, YEA+98\]. pictures \[ONT98\]. Piecewise \[YMW99\]. PIL \[Sch99k\]. P/L/SETHEO \[Sch99k\]. piling \[HKM95\]. piling-up \[HKM95\]. Piloting \[KW92\]. Pinyin \[OSH91\]. pioneer \[RK98b, Pin98\]. Pioneers \[Unixxb, Riv98c\]. Pipelined \[RB99\]. Pipelining \[Pos93\]. Pirates \[Wai94\]. Pitfalls \[Sch98f, SZZ94b\]. pixels \[BD98b\]. PKC \[IZ98\]. PKC'99 \[IZ99\]. PKCS \[Ano95, Ano96k, Ano97b, Ano98i, Ble98a, Kal97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, Nys99, RSA93b, RSA93c, RSA93e, RSA93a, RSA99b, RSA99a\]. PKCY \[XW97\]. PKZIP \[BK95a\]. Place \[DR94c, Des98a, DR98b, Ano95a\]. Place/Transition \[Des98a, DR98b\]. Placement \[FL93\]. Plain \[Bar93a, Bar93b, Phi98\]. Plaintext \[GC94, WB94, WRi94, BK95a, Cli99, MY93a, SNT95, vOW91, vT93\]. Plan \[Gar97a, Gar98b, Ano94a\]. Planar \[L99\]. plane \[ZW99\]. Planet \[Sta97c, Fro96\]. planning \[Mas97\]. Plants \[PRAM98\]. Plasma \[BVFD99\]. plastic \[Gau97\]. platform \[Al98, LS98a, Way98\]. platforms \[Ril96\]. Play \[Bea97b, DDJ98d, IKM99\]. Players \[IKM99\]. Players-Team \[IKM99\]. Playing \[SvS98, SV99a, SV99b\]. plays \[Lea90\]. Pleasures \[Kö96\]. Plug \[Bea97b\]. Pluggable \[IH98, Mor97\]. plugs \[GTGW94\]. Plus \[Dav95\]. plutonium \[Ano96m\]. PMLP \[BPBV99\]. Pocono \[IE97e\]. Poctzy \[Sch95e\]. Poe \[Sha99a, Ros97c\]. poems \[Lea90\]. Point \[FP99, Gar97b, Lan98, STP93, Ken95, Shp99a, SM98a\]. point-&-click \[Ken95\]. Point-to-Point \[SM98a\]. points
Polynomial-Time \cite{sho97}, \textit{Pollard} \cite{BMxx, ESST99, GLV99, Tes98}, \textit{Polling} \cite{JO97, Mer93}, \textit{Polly} \cite{ES97}, \textit{Polyalphabetic} \cite{Abe98b}, \textit{Polygonal} \cite{OMA98, OMA97}, \textit{Polyhedral} \cite{Mou99}, \textit{Polymorphic} \cite{SG95}, \textit{Polynomial} \cite{AGS97, NMV99, Sho97, TN96a, TN96b, CS97d, MI90, Pet91, Xie93}, \textit{Polynomial-Time} \cite{sho97}, \textit{Polynomials} \cite{SE96, She95c, CW91a, CGMW97, Ito91, Kob91c, LC96b, Odl94a, LC96c}, \textit{POP3} \cite{Mye94b}, \textit{POPL} \cite{ACM99a}, \textit{popular} \cite{KAK96}, \textit{Port} \cite{Mei98}, \textit{Porting} \cite{JJ91}, \textit{Portion} \cite{Len98}, \textit{Portland} \cite{Auc98, USE90}, \textit{Position} \cite{BFK99, CM99c, YST99a}, \textit{Positive} \cite{Dwo97, YY98a}, \textit{Possibilistic} \cite{WD99b}, \textit{Possibilities} \cite{Jam98}, \textit{Post} \cite{AA93}, \textit{Post-Markov} \cite{AA93}, \textit{Postage} \cite{TYH96}, \textit{Predetermined} \cite{Len98}, \textit{Predict} \cite{Kra90}, \textit{predicting} \cite{Gil97}, \textit{prefix} \cite{MPL99}, \textit{Prefix} \cite{ADD99}, \textit{Preliminary} \cite{BC93a, BPBV99, DY91c, Zim96b}, \textit{pre-alpha} \cite{Zim96a, Zim96b}, \textit{Pre-compressed} \cite{HG97c}, \textit{Pre-processing} \cite{DO99}, \textit{Presence} \cite{BDHJ98, CH94a, CHH97, Cra98, Gar94, JQBD97, Cra97}, \textit{present} \cite{Sim94c}, \textit{Presentation} \cite{KI99, LS98a}, \textit{Presentations} \cite{HMT+98}, \textit{Presented} \cite{DBGV93, NS99a, Ano95l}, \textit{prevents} \cite{GLC98}, \textit{Preserving} \cite{NKP99, DII99}, \textit{President} \cite{Cli97, Cli99, UU97b}, \textit{Pretty} \cite{Ano94h, Elk96, Gar95, GM95a, Mei96a, Ros97a, Zim96a, Zim96b, Gar98c, SSI97a, SSI97b, Sta94a, Sta95a}, \textit{Prevalence} \cite{YY97b}, \textit{Preventing} \cite{Jas96, SHK99b}, \textit{Prevention} \cite{OG97, VN99}, \textit{Previously} \cite{DH90}, \textit{PRFs} \cite{HWKS98a, HWKS98b}, \textit{Pricing} \cite{DN93, Ros94}, \textit{Primality} \cite{Boz90, GKK99, Lan99, Len90, Yan95}, \textit{primary} \cite{Ban94}, \textit{Prime} \cite{LO91a, Sho97, Boy97, DLP93, Graxx, ML98}, \textit{Primes} \cite{Sch94d, Dtb7b}, \textit{Primitives} \cite{CF99, Pre98c, RIP95b, RIP95a}, AMS96, Bb93, Bb94, Fra90, FOO93, FO98, HZ93, HNM98, HJ99, Jac90a, Jac90b, JG95, LL95b, PS98b, vO92}, \textit{Practically} \cite{Gut98b, Knu94a}, \textit{Practice} \cite{Bel99, DSB99, GN95b, IZ98, IZ99, LABW92, AN94, Dam99b, Ger97, LABW91, Sch93a, Sta99a, Sti95}, \textit{Practice-Oriented} \cite{Bel99}, \textit{Practices} \cite{Des99a, JJ98b}, \textit{Pragmatic} \cite{Gut98b, Knu94a}, \textit{Practice-Oriented} \cite{Bel99}, \textit{Practice} \cite{Des99a, JJ98b}, \textit{Practical} \cite{ASW99, ADBB99, AB96a, AWV99, Ano96l, Avo98, Bac95, Bowxx, CD96, CS98b, Dam91b, Dam94b, Dam94a, DS93, FO97, HBK919, IH99a, Jne99, KTM+99, Oka93b, vO91a, PRS99, PV90, Sak97, Sch92a, SW93, Smi90, Sta96d, ZS93, vO91b, And93, pp [Ano97-28].
VCF+90, ZMI91, BFKL94, BP95b, Di99. **principle** [Dam90b, Gib90]. **Principles** [ACM99a, AN95, HGHD98, KK99a, KG99, MG91, PRB98b, Zhe90, Sta99a]. **Printer** [Cou93]. **Privacy** [Dam90b, Gib90]. **Printer** [ACM99a, AN95, HGHD98, KK99a, KG99, MG91, PRB98b, Zhe90, Sta99a]. **Printer** [Cou93]. **Privacy** [Ano94h, Ano95c, Ano97s, Avo98, Bac95, BBCM95, Ble98b, Car96, Cha92b, DL98, Elk96, FJP96, FHM99, Gar95, GM95a, IEE92c, IEE93b, IEE94d, IEE95b, IEE97i, Ken93, KFJP96, Lin88a, Lin89a, Lin93a, Lut98, MW97, Mjo93, NKP99, Par98c, SY96a, SYMI98, SB97, SG96a, Sta94a, Tho96, Tra99, Uni98a, Uni98i, Ban94, Bro96, CM95, Car94, Cha92a, CK93, Cli99, Dom96, HM96, JMLW94, Mar95b, Mei96a, Mil95, Rot95a, Smi94a, Sta95b, Uni98d, Uni97c, VPM97, Zim96a, Zim96b, Gar98c, Ros97a, SS97a, SS97b, Sta94a, Sta95a, Zeg93]. **Privacy-Protecting** [Tra99]. **Private** [BDF98, BD99b, CKGS98, HR90, KR94c, Law98, MP91, Mv93, RSA93e, Dam96, DS90a, Rac90, Sch95d, SS98b, Ts90, Wil93b, ZG96]. **Private-Key** [HR90, Mv93, RSA93e, DS90a, SS98b]. **Privilege** [ECM96]. **Prize** [GC97, Pin98]. **PRO** [Ano97r, Gar98c]. **Proactive** [CHN97, FGMY97b, HJKY95, HJJ+97, HJJ+xx, IBMxx, Jar96, Rab98, BCR98, FGMY97a]. **Probabilistic** [Jak98, JO97, SF97, Sch91b, Tou93, Gol99a, GO95, HK90, Imp92, Lon91, TX92]. **probabilities** [Leu92]. **Probability** [BDG99, Gol96b, Koh99, TY94, AI96, MHMW98, MAO96, WM93]. **Probable** [BD93, NK93, DLP93, Graxx]. **Problem** [Bon98b, Bon98a, BN96, CS96a, Cha90, DDD99, DJL93, GO96c, HM98, KN99b, KR99b, MT99b, NS99b, OM99, Per99, RS99a, CPS95, HY93b, H97, HM97b, HMP95, LC97b, Mas97, McC90a, NR95, OA99, MSO96]. **Problem-Solving** [Per99]. **Problems** [AA93, BD95a, Bra90a, GGH97b, KRS99, MC92, Poi99, Smi90, APDS93, Bea92, BFKL94, FR95a, HC95a, IEE97e, Lew92]. **Procedure** [Ada97a]. **Procedures** [Hig97b, Lin93a, Lee95, Lin98a, Lin98a]. **Proceeding** [BPR99]. **Proceedings** [ACM90, ACM91, ACM94c, ACM95, ACM96a, ACM96b, ACM97b, ACM97c, ACM98b, ACM99a, ACM99b, ACM99c, AR97, Ano95i, Ano98f, Bri92, Bri93, Com96, GN95b, IEE95a, IEE91, IEE92b, IEE92c, IEE92d, IEE93c, IEE94c, IEE94d, IEE95c, IEE95b, IEE96c, IEE96d, IEE97i, IEE97j, IEE97k, IEE97l, IEE98e, MZ98, Nat99b, OW95, PSN95a, Pit95, Sti93b, SL93, USE91, USE92a, USE94, USE95b, USE95c, USE95a, USE96e, USE96d, USE96f, USE98c, USE98a, USE98b, USE99a, USE99b, USE99c, And94a, And96c, Ano94d, Blih97, B+96b, BGH95b, BS95e, Chr98, Dam90a, Dam91a, Dav91, DG96, De 95, DEQ92, Far93, FM91, FR95a, Fra99, Fum97, God90b, HQ97, Hir97, Hir98, HF97, IEE92a, IEE94b, IEE97b, IEE97e, IEE98a, IEE98d, IEE98f, IZ98, IZ99, KM96a, KG93, Kno99c, KP99b, KK99b, Kra98, LOX99, LM98a, LW96, Lom97]. **proceedings** [MV91, Nyb98, OiDP98, Pre95a, QV90, QQ95, Q+98, Rue93, SZ93, Spi95, Ste99b, TM99, TV94, T+98, Tv92, USE90, USE98d, VPM97, Vau98e, Wat91, Wei99, Wol93b, Yua92, vWN99, ACM93b, CH96, Chr99b, IEE94e, Sti94, Wal99a, BCB97, Boy95b, CMM93, Cop95d, Dar97, Des94b, Fei91, Gol96d, GQ95, GS94b, He94, IR93, Kal97c, Kob96, Mau96b, PSN95b, SP90]. **Process** [AMP94, Knu98a, Rob98a, RS99c, YT96, CWM+91]. **Processes** [Gar98b, Bea92]. **Processing** [Ano97h, DN93, Gar98b, IEE95a, IEE97a, IEE96e, IEE97c, IEE97d, IEE97j, IEE97k, IND99, KV99, LMP99, LW96, Pin98, Pit95, Ano96m, DO99, DF97, Man98, Sab94, T+98, Whi90]. **Processor** [Gar98a, RB99, SW97a, SW97b, She92e, Sut99]. VVDJ90, Von92a, Von92b, DVQ96, She92c].
Processor-efficient [Von92a, Von92b]. Processors [Cia97, KKK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
Prodigy [CFK+91]. produced [SII97a, SII97b]. Processor [Von92a, Von92b]. Processors [Cia97, KKK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
Prodigy [CFK+91]. produced [SII97a, SII97b]. Processor [Von92a, Von92b]. Processors [Cia97, KKK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
Prodigy [CFK+91]. produced [SII97a, SII97b]. Processor [Von92a, Von92b]. Processors [Cia97, KKK99a, She92e, BS95c, MHPS96, NM96a]. Proctoring [SKW96].
MM99a, Mau93a, MW98d, Ng99, NR94, NK98b, Nur94, Sl93a, Sch94g, Sch96a, Sch94h, Sch99k, SS90, Tou91, Tou93, AN94, AG97b, AG97c, AG97a, Aba99, ABC+98, BDH97, BH93, BCK98, BGH+95a, BBS98b, BM95, Bra90b, CGM96, Chr98, Chr99b, CJ95, Dan97, Fei99, Hor98, HLL+95, JW01, LY93, LW99, LL95b, Lon97, Man95, Mas97, MLY93, Mea95, MW98c, NT93, PS98c, PS98e, PS98f, protocols [Pau98, PW93a, PKM97, SSG99, Syv93, SM95b, TH99, XZZ97, XZZ98, ZLX99, Zhe95b].

Prototyping [AKP99]. Provable [Bel99, CT99a, Mat96a, Ano96m]. Prototyping [AKP99]. Provable [Bel99, CT99a, Mat96a, Ano96m]. Proving [Bos90, DR94c, DE99, FK99, DF91b].


provisions [Cl97, UU97b]. proxies [LC94]. Proxy [GP99, Jak96c, LHW98, Zha98, BBS98b].


psychoacoustic [Til98]. Psychovisual [DDM98]. PTY [LT98]. PTY-Marks [LT98]. PUB [Nat95, Nat99a, FIP93b, NIS93b]. Public [ANS97, ANS98b, Acc97, AKP96, AN95, IBM93, Ano96m, Ano99f, Ano99b, AA93, BP98a, B195, BDH98, BDG98, BCE94, Bec99, BC95b, BHS98b, BHS98a, BDP98, Ber97c, BS91b, BFS92a, Bir98, BMS94, BPK99, BFK99, Ble97, BFK99c, BS94, CC99b, CG99, CJ95, CL97b, CS98b, Cra98, Cus97, DDJ98b, Dam91b, Dav96, De93e, DP98c, Di90, Ell99, FY95a, FY98a, FY99, FGL96a, FGL96b, FO99a, GHT90, Gal96, Gar96b, Gib91, Gib92, Gir91, GHH97b, GH99, HK99a, HGS98, HP98a, HY93b, HM93, HL93b, HJJ++x, Hes97, HPS98, HFPS99, IZ98, Iz99, Iss90, Jab90, Kal99, KS99b, KM99c, KT91a, KMOV91, KKT91, RSA93f, Lan99, LM94b, LA98, Low96, Luc98b, MY91, Man93a, Man97a, Men93, MM96b, Mic93a, Mic93b, MM98a, NS97a, NY90, Nes91, Nec96, NS99a]. Public [Od94b, Oka94, OU98a, Omu90, vO91a, PS97, Pai99d, Pat95, Pin97, Poi99, RSA94, RCM99, Rud91, Sal90, Sa96, DP91, Sas99a, SE96, She94d, Smi93b, ST91, Sun98a, Sut99, TAP90, V97, dWQ91b, Wei98b, Yam98a, Yam98b, YST99a, YST99b, ZPY96, Zim96b, dWQ91a, vO91b, AA95, AD97, AD99, Ano90, ADSW99, Bae94, BI94, BD98a, BS97, BS91a, Beu94, BMP97a, Boy97, CC99a, CW97, Cle96, Cra97, Gus95, DW926, Dam96, Den90, DVG96, Dhe98, DN95b, ES97, FGM97a, GH96, Gib95, He92, HFW96, HJJ++97, JM96a, Jar96, Jon90, KASH90, KM99a, Kir95, KM99d, Kos99, LG97, Las92, LMJ993. Lee95, LC96a, LM94a, LZ90, LZ91a, LDW94, LCL95, Lon91, Lon92, Low95, MF90, Mau91b, MY93b, NM96a, Nat97a, Ole95, Pet91, PP92b, Rae90, Roe99, SW95a, Sch92c, Sha95a, She96a]. public
[She92c, SM90, SS95b, SS95c, Sta94a, Sta95a, Sun91a, Tah94, TCC97, TC99b, TC99a, Tze99, Ven92, Wan92b, Wil93b, Xie92, Xie93, XLP99, WX97, Yu92, Zha91, vO92, vT90, BFS92b, HMT'98]. **Public-Key**

[AKP96, Ano99f, Ano99h, AA93, BP98a, BHSV98b, BHSV98a, BDFR98, Ber97c, BMS94, BPK99, CC99b, CJ991, Cra98, Cus97, DP98c, Dif90, FMY99, FO99a, GH99, GGH97b, HK99a, HGS98, HP98a, HVM93, Hess97, Iss90, Ka9b, KM99c, KT91a, KMOV91, LM94b, Low96, MY91, Mic93a, Mic93b, NS97a, OKa94, OU98a, vO91a, PSL97, Pai99d, DP91, Sasa99a, ST91, Sun98a, Wie98b, Yam98b, YST99a, YST99b, Ano96m, BFS92a, FGLP96a, FGLP96b, GH99, HY93b, NY90, Nec91, Sai90, Sai96, SMi93b, Yam98a, AD97, AD99, BMP97a, CC99a, Cle96, Cra97, DQ96, Dhe98, DN95b, ES97, FGM97a, KASH90, KM99a, KN99d, LM94a, LZ91a, LDW94, LCL95, Lon92, Low95, Mau91b, MY93b, NM96a, OLe95, SW95a, Sch92c, Sh95a, SS95b, SS95c, TC99b, Tze99, Ven92, Wan92b, XLP99, Yu92, vT90]. **Public-key**

[BFS92b]. **Public-Key-Based**

[Nec96, TAP90]. **Public-Randomness**

[DP91]. **Publication**

[Nat93b, HVH98, Nat92b, Nat93a, Nat94a]. **Publicly**

[Mao97, Sch99i, Sta96a, VBD99, FO98]. **Published**

[Ano97c, Ano97d]. **Publishes**

[Ano95j]. **Pudding**

[Sch98i]. **Puerto**

[CMM93]. **Pump**

[KM93, TY99D]. **Purchase**

[KS97a]. **Purchaser**

[RS99a]. **Purple**

[Cur98]. **Purpose**

[KP93, Sut99, Sch91b, Vu95]. **purposes**

[Cli99]. **pursuant**

[Cli97, UU97b]. **Push**

[Er97b]. **Pushes**

[Bar97]. **Putting**

[DDJ98c]. **puzzle**

[Bar92b, Gre90, WSFC99]. **PVM**

[BSN95]. **PVS**

[DS97d].

**Q** [AW99, Ber97a, Hru95a, Hru95b]. **Q&A**

[Ber98]. **Q-Deformed**

[Hru95a, Hru95b]. **QoS**

[NAA99]. **QPSK**

[SVWMB95, SOB98, VSB95]. **Qu**

[NS97c, NS97b]. **Qu-Vanstone**

[NS97c, NS97b]. **Quadratic**

[BBT94, MRT98, Per93, SK98c, SK98b, DDP94b, HJ98a, MVZ98, ZPY96]. **Qualitative**

[MSH99]. **Quality**

[HH94, NH98, Yeu97]. **quantification**

[Bad99]. **quantization**

[CCH98, MTN97]. **Quantum**

[BBB91, BBE91, BL95, Bra94a, BHT98, Cha99c, DDJ98d, GC98, Hru95a, Hru96, Hru98, HLMP96, HBKL99, MY98, OD99, PT95, ROT94, RK99, Sa98, Sa99, Sho97, Tow98, WG99, BC96b, Hru95b, Sin99, Slu98]. **quasigroup**

[KM99d]. **quasigroup-based**

[KM99d]. **Quaternary**

[KP96a]. **Quaternion**

[Cop99]. **Quebec**

[CFG96, ACM94c]. **Queen**

[Sin99]. **Queensland**

[DG96, SZ93]. **Queries**

[Dum94, Fis98, NP99, AK95]. **Query**

[AKF94]. **Question**

[Lud97, WD99a]. **Questioned**

[Ano95b]. **questions**

[Di97a]. **quick**

[Pre97b]. **QUIPU**

[Men91]. **Quisquater**

[NS98b, NS98c]. **Quorum**

[Jak99c, NW98].

r [Riv98a, Hol91]. **R1040**

[BP95b, RIP95b]. **Rabdology**

[CWM9+1]. **Rabin**

[BR96c, CW97, FS97b, JQ98b]. **Rabin-Williams**

[AK95b]. **race**

[Kah91a, Sch99f, BGV93, BP95b, RIP95b, RIP95a, VCF+90]. **Rackoff**

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

[DJ99]. **Radio**

[GB98, LU95, PKOT94, She92f, Tod97, UNU94]. **Radiology**

[DTDJ99]. **radios**

[RPS99]. **RADIUS**

[RRSW97a, RRSW97b]. **Radix**

[Kor93]. **ramified**

[GK95a]. **ramp**

[SW98, SW99a]. **Rampart**

[RPS99]. **RAMs**

[G096b]. **Random**

[BG98, BGM97a, BGM97b, Bir98, Cor99, Ell98, FW91, Fis98, FO90, FJRS96, GHR99, Gut98b, Jk99, KKS97, MAT96b, MP91, MS95f, MF95, NR98, OS98, PS98b, Rau01, ROT94, Riv91a, Sii97b, W99, BR97b].
Bou94, GoI99b, IS97, Imp92, Jenxx, Kos99, Kul92, Ler97, PC98, TSY98, Wal90.

Random-Number [ROT94, Bou94].

Redundancy [Fis98, HSSI99, OU98b]. Redundant [GM97, Mis97]. Redundant [BAR98, TY92].
Reengineering [DDJ98c]. Redux [DDJ98c]. Refinement [HWF96]. Reflecting [Jan95].
Redux [DDJ98c]. Reengineering [AMP94]. Reference [Bar96b, CDF95, KMKH99, Pre97c].
Reference [Bar96b, CDF95, KMKH99, Pre97c]. Reduced [GM97, Mis97].
Reduced [SOB98, TY92].
Refunds [Hir93]. Regional [ADEDS99]. Register [CS96b, CS97b, GN95a, GM91].
Register [CS96b, CS97b, GN95a, GM91]. Registers [GO96b, Go94, GO95, GK95a].
Registers [GO96b, Go94, GO95, GK95a]. Registration [Bal97, TOH98].
Registry [PKAC+98]. Reglementierung [MPS94]. Regular [SG95, DI99].
Regular [SG95, DI99]. Regulated [Way93c]. Regulating [Riv98c].
Regulation [Koo97, Ram92]. Regulations [Koo97, Ram92]. Reengineering [AMP94].
Reengineering [AMP94]. Reinventing [Yuv97]. Rejected [Eri97b].
Rejected [Eri97b]. Gar97a, GC97. Related [Ber97c, BV96, CH98, Cle91, CFPR96b, De 93b, De 98c,
ECM96, GS97, KSW97a, KSW97b, WB95, Bih94a, CFPR96a, OU98b, Zer96a].
Related-key [KSW97a, KSW97b]. Related-Message [Ber97c]. relating [Aus96]. Relation
[BHSV98b, BHSV98a, SK98c, SK98b]. Relations [BDPR98, Jak98, NMV99, Uni98c, Tze99].
Relationship [GSV99, HT99, MW99, Oka93a, SZ95c]. Relationships [Kem99, Len99b, RG95,
SS95a, SG99b, SZ95a, GGG-99]. Release [Dam94b, Dan94a, DOR99, Sun91b, Zim96b].
Released [DDJ98a]. Releases [Got99, Wor96]. Relevance [SS99d, Tra99].
relevant [Hil94]. reliability [BHS93, HS96b, IEE94b]. Reliable [BF97a, BF99b, KM93, FD92].
Relinearization [KS99b]. Relying [ZMI90, Sak97, Sch99e]. remainder
[DDP99e, WWH95]. Remark [CMTNY94, LHL94, FR94, MY93b].
Remarks [BY92, GPSN97, Gro94, Gui97, Oht98, BBL95, La92]. Remote
[BLM94, FMM99, HS97, He98a, LC95, RRSW97a, RRSW97b, SK97c]. Remotely
[BFN98b, Lu97, Luc99c, LW99, BFN98a]. Removing [LLB98, RCM99]. repair
[Zhe95a]. repeated [Syv93]. Replacement [Cap94, SN94]. Replay [OG97, YL97b].
Replicate [RB94]. Replicated [KB92]. Replicating [HS96b]. Replication
[BLM94, Pit96b]. Reply [NC97, BMP+97b]. Report [Bra93a, BD1+96, Dra98, EMN98,
Kui91, Nat99c, Par98c, PH91, RIP95a, RD99a, Tov95, Van99d, Wor96, BFS92a,
BP95b, Bur98a, KSB96b, NBD+99, Org98a, RIP95b, UU97a, Zer96a, Dan95, BFS92b].
Representation [CK95, Ger99b, JKV99, LE99, NA95, PNFK95, TY92].
Representations [FC99]. Representatives [Cl97, Uni97a, Uni98c, Uni98d, Uni98e,
Uni96b, Uni97b, Uni98f, UU97b]. Representing [HL99]. Republic
required [BGS95]. Requirement [Sil97a].
Requirements [Ano97b, BD92, Bel92, BC95c, FR95d, HJTW99, HH94, VW98,
Com94c, MW98a, SM95b, UN94].
Research [Ano99c, DDJ98c, Dan96, Des92, Des98c, DEQ92, Ele98, IEE92c, IE93b,
IE94d, IE98d, Jan99, Q+98, Rhe93, Wol93b, W99, W99]. Researching
[Un96a]. Resend [Ber97c]. Reserve
[An97x]. Resharing [AG95b]. Residue [KKOT91, PF92, CB96, PF92a, PP95a, PP95a].
Residuosity [Pa99d, DDP94b]. Resilience [FGMY97a]. Resilient
[BGS94, BGS96, MS99b, RS98a, GHS93].
Resistance [BKP93, Dae99, SY98, YT95a, YT95b, CL97b]. Resistant
[Auc96, BDH98, EKK99, KK99a, KS97c, LA98, GV91]. Resolution
[ADD99, BLM99, CH97a]. Resolvable
S/MIME [Ano95a, Ano96a]. S012 [KP95].
s02DES [TSM95]. S390 [Deu97, Deu98].
SAC [Kim93, KS97b, NS99a, TM99].
SAC/PC [KS97b]. SAFE [Uni97a, Uni98b, UU97a, Uni97b, Hor99, VM96, Way95, Uni98c, Uni98e, Uni96b, GA98].
Safe-Tcl [GA98].
safeguarding [Beu94].
Safe-T [Hir93, BM97, CMKK98, KSW96, KSW99a, Mur99, SKW+98a, SKWW99, WKS+99].
Safe-T [Bur98b, Kru98].
Safeguard [Hir93, BM97, CMKK98, KSW96, KSW99a, Kel99, Mas94, Mas99b, Van95]. Safety [Ano94c, DDJ99, Cli99, IEE94b].
Safford [Bur98b, Kru98].

Sacco [GQ95, QG95].
Sacks [Gar97a].
Salesman [OMV98]. salient [CKLS96b].
Salt [USE95b]. Samba [Bla98]. same [Ude98].
Samos [KG96]. San [ACM93a, ACM99a, Ano97a, Ano98f, Com96, CMM93, FJV97, IEE92b, IEE97b, RP97b, Sch98b, SJ97, USE92a, USE96c, USE96f, USE96g, USE98d, van96, XTM1994].
Sand [SVxW91].
sandbox [MF97].
Santa [Bri92, Bri93, Cop95b, Cop95d, Des94b, IEE97b, IEE97f, IEE98d, Ka97c, Kob96, Kra98, St93b, St94, USE93, Wef99].
Santorini [IEE97c].
Saragossa [Mau96b].
Sardinas [MSS93].
SASL [Mye97, New98].
SAT [McH92].
Scheduling [KP93, Por98, SJS98, Sha99b].
Schema [Pit96b]. Schemas [Wed99].
Scheme [Int91a, ADF98, BCCG93, BM99a, BB99b, BF99c, Boy90, BY92, CT97, CK95, Cop94b, DQ94, DKKK98, DN94, GHY90, GQW+91, HL93a, Hwa93, Hwa97, Iev91, IM93b, KKS97, KSW98d, KM99b, KR99b, LK96, LW91, LHL94, LH93b, MSS98, Mi96, Mun99, NMV98, OOK91, O993, OFF93, Pat95, Pet98, PM99b, RGV97, Sch99i, Sm90, Ver95, AW95, BD98a, CW97, CLHL98, CC95, CLW98, CMTNY94, CS97, FO99, FO98, GML94, GPN97, Gua90, Har91, HZ93, HK90, HY95, HC96, HW98c, HCC98, IS99, IM93a, JC98, JLM+94, Ku92, LWC96, LLG10, MRS99, MS98a, MLA91, Mau91b, MC96, Nac93, OK96b, Pat91b, Pat91a, RD96b, SSN98b, SVWMB95, Ste95, Tan90, Tod97, Tra97, Wan92a, Wu92, WWH95, v939].
Schemes [AW94, BP97a, BC93a, BDP98, BBDW96, BK94a, BK95b, BM96b, BM96c, BDDV93, BDD+94, BFS96, BM99c, BV96, BD90, Bri90a, BS91g, BLLV98, BBD92, CS97a, CM99a, CD95, Duan99a, DVF90, DMPW98, DY91e, vD95a, DFKY99, DLR97, FDB93a, FY97, FO99, FO99b, GPN98, GP99, GS94a, HKS97a, HKS97b, IS91, JMO94, KPG99, Ki96, KMOV91, KOS+94, KO99, KOO99b, LWH98, LM95, MH96, Mis98, MW994, OK98, Oka93b, Papi98a, Papi98b, PM98, PS96c, PB99a, RS96c, dR94b, SK95, Sak96, SE96, SiK93, Sim90b, Sim91, Sim94a, Ste94a, St93a, St98b, SW99b, SSS99, YLD99, Zha98, ARK99, BC95a, BR97b, B93, BDSV93, BCDV94, BG95, Blu95, BC96a, BCDV96, BGDV96, BMS96, BD97, BFS98, BDV98, BD98b, BD99, 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, MTN97, Mu92, NR95, OK96a, OKT93,
OK95, Pad98, PS98a, PPKW97, Pf96c, PS96d, RD96a, RS96b, SI93b, Sha94,Sha95a, She92g, SW98, SW99a, SS94, SC97, TJ99, Tze99, VNM99, WAM94, ZHS94, ZI98, dR94a, vD95b. Schernes [BBCM93a].

Schnorr [DBGV93, dR94b, dR94a]. Schnorr [IKNY98]. School [Duf98]. Schools [DDJ98e, DDJ98f]. Schroeder [Low95, Low96]. Schussel [Pin98]. Schutz [FT95]. Schwierigkeit [Hor99]. Science [Ano93i, AA97, DDJ98e, DDJ98f, Eri99, IEE96a, IEE97f, IEE98a, IEE99a, Ste91, Bed90, Beu94, Sch90c, Sch97c, Shp99a, Sim90b, Sim91, Sim94a, Sti93a, Van93, Wi99, Wie90b, Wol98, Al96, AGY95a, BC95a, BT94, BI93, Ble96, BDSV93, BCDV94, BDD94, BGS95, BCDV96, BDGV96, BD97].

Scientific [CHLT99, PH91, GTGW94, HW91]. Scientist [BCE94]. scoops [Ano96m].


secondary [Atk93]. Secrecy [Aba99, BP98e, GM90, GTGW94, JR96, Moy98, Rat96, Sin99]. Secret [AGY95b, Ano97e, BC93a, BC95b, BCG90, Ben98, Ber91, BS97a, BK94a, BK95b, BDGV93, BM99c, BV96, Bra95b, Bra95c, BS94, BD90, Bri90a, BS91g, Cac95a, Cac95b, CT97, CMP97, CGMW97, CK90, CFSY96, DDJ98g, DDJ98h, Dae98, Dam94b, DDP94a, DKK98, DFIJ99, vD95a, E HMS99, FW91, GSNW98, GPSN98, HL93a, HD96a, HKS97a, HKS97b, HCY96a, IS91, KI96, Kra94a, KOS94, KO95b, KOO95a, LY93, LF97, LM94a, LM94b, LP99, LH93b, MSNW99, Mau93a, MW96a, Mau97a, MS98, MS99, MT98, Ms92, NW98, OK98, PS98a, Pui98a, Pai98b, Ped91d, Ped96, Rey96, Rey97, Rey99, Sal91, Sch99i, Sha99a, Sim90b, Sim91, Sim94a, Sti93a, Van93, Wi99, Wie90b, Wol98, Al96, AGY95a, BC95a, BT94, BI93, Ble96, BDSV93, BCDV94, BDD94, BGS95, BCDV96, BDGV96, BD97].

secret [BDV98, BDGG99, Bur96, CDGV91, Da97, Dan94a, Dwo91, Ell97, FO093, FO98, GM95b, GPSN97, Gre90, HNSM91, He93, HIKY95, Hwa92d, HC96, HLC99, JM93, JMO95a, Jar96, JY98, Kah96b, KO95a, KO96, KO97, LY93, LH95, Mei92, MPSV99, OK96a, OKT93, OK96b, OK95, Pad98, Ped91b, Ped91c, RD96a, RD96b, Ros97c, Sim90a, Sta96a, SC97, VV97, Wie90a, WS96c, Win99, Wri98, ZHS94, vD95b, van97a]. Secret-Ballot [CFYS96, BT94].

Secret-First [Ano97e, Bra95b, Bra95c]. Secure [AHV98, AB96a, Ano93c, Ano95f, Ano95i, Ano99c, Ano99h, ATK97, AR99, Bal99, BQ95b, BQ95a, BMM99a, BMM99b, BR95b, BM99a, BM99b, BR91, BHK99, BDHK93, BFS96, BS95b, BS98, BM94b, CG99, Car99, CG98, Cha90, Ch9P91, CR91, CC95, CKLS96b, CKLS96a, CKLS96c, CKLS96d, CKLS96e, CKLS96f, CKLS96g, CKLS96h, CKLS96i, CKLS96j, CKLS96k, CKLS96l, CKLS96m, CKLS96n, CKLS96o, CKLS96p, CKLS96q, CKLS96r, CKLS96s, CKLS96t, CKLS96u, CKLS96v, CKLS96w, CKLS96x, CKLS96y, CKLS96z].

secret-sharing [RD96a]. secret-sleuthing [WS96c]. Secretly [MT94]. Secrets [Cr690, DH90, DSB99, Ele98, HY93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, Ano91b, Bau97, BDV93, CY98, JMO95b, YY93, Chi92].

section [Alv98c]. Secure [AHV98, AB96a, Ano93c, Ano93f, Ano95i, Ano99c, Ano99h, ATK97, AR99, Bal99, BQ95b, BQ95a, BMM99a, BMM99b, BR95b, BM99a, BM99b, BR91, BHK99, BDHK93, BFS96, BS95b, BS98, BM94b, CG99, Car99, CG98, Cha90, Cy9P91, CR91, CC95, CKLS96b, CKLS96a, CKLS96c, CKLS96d, CKLS96e, CKLS96f, CKLS96g, CKLS96h, CKLS96i, CKLS96j, CKLS96k, CKLS96l, CKLS96m, CKLS96n, CKLS96o, CKLS96p, CKLS96q, CKLS96r, CKLS96s, CKLS96t, CKLS96u, CKLS96v, CKLS96w, CKLS96x, CKLS96y, CKLS96z].

secret-slang [RD96a]. secret-sleuthing [WS96c]. Secretly [MT94]. Secrets [Cr690, DH90, DSB99, Ele98, HY93, MSK99a, Pes97, Rab94, Sch92b, Ste98b, Wei94, Ano91b, Bau97, BDV93, CY98, JMO95b, YY93, Chi92].
CKLS97, CD95, CD96, CS98b, CDD+99, Cra99, Dam91b, Dam94b, DY90, DY91d, DY91f, FIP93b, FB97, FYM99, FB94, FO99b, GM97, GGY90, GaI96, Geh95, GKJR99, GHR90, Gut96, IOS94, Jac90a, Jac90b, JT97a, KT96, KSB96a, KSB97, KY99b, Lam99, Mau90, Mau91d, Mau97a, MW97, Mos98, NS93b, Nat95, NS98b, NS98c, Oka93b, OU98a, Ped91d, PS96c, PB99a, PGV92, RRP97, RS96a, RIP95a, SSH93, SSI98]. Secure [SK94, SSSW98, Sas99a, Sch98a, SK99, SM95a, SB94, SSM94, Sho96, Str93a, Str93b, Tai95, WP90, WD99a, WK97, Web98, Yah94, YST99a, YST99b, ZMI90, Zhe90, ZL99, Zol93, vh997, BH93, Bea93, Bea96, BMS96, BP95b, Bow93, BM95, BD95b, CNST98, CG97, CG05, Dam94a, Des90b, DS93, Des95, DVG96, FO98, GGK+99, GM95b, Go90c, GBL94, HY98a, HY98b, HY98c, IS97, IKNY98, KC95, KSB96a, Lam99, Los97, MS98b, NY90, OK96b, Opp96, Ped91b, Ped91c, PSW95, RHE94, RRSY98, Rom90b, Sar97, Sch92c, SKB97, Sim98c, Sin95, Sta97c, Ven92, YL97b, ANS97, An90a, Nat92b, Sta94b, Bou94]. secured [Way98]. Securely [RB94, DDFY94].

SecureNet [Ano97r]. Securing [Bhi96, Des95, Lin96a, RG95, SG98, VJ98, Ano95k, DL96]. sécurité [Bou94].

Security [Sch98c]. Security [ACM93a, ACM94a, ACM97a, AKP96, ADDS91, AR95, ABV98, Al97, And94a, An90a, Inta91a, An92c, An93g, An95f, An95b, An96i, An96a, ??97, An97e, An97f, An97g, An97a, An97w, An97x, An98a, An98b, An98h, An99a, Atk95b, AR98, Bal99, BCCG93, Bast93, BKR94, BDR98, Bel99, BGGK99, Bel92, Ber96b, BDR+96, Ble97, BPRF99, Bov98a, Bov98b, Boy99, Bra90a, BK94b, BNP99, Com96, Com94c, CM97a, CH94a, CHN97, CGJ+99, CS96a, CM97b, CT99a, Chr98, CGB+93, CNS99a, Cor99, CN99, CG05, DMW94, Dn95, DS98a, Dav95, DG95, De 93a, De 98a, DDK98, Des92, DI 99, Dl99, Dwo95, ECM96, Elk96, EH96, FGS96, FS97b, FO99a, Fum93, Fum98b, GM93a, GM95f, GaB96, Ga97c, Gar96c, Gib96, Gir99, GH95, Gon98, GA98, Gut99, HHT93]. Security [HHT97, HP99a, HP99b, HSK97, HH94, HLMW93, HWMW94, Hur98, IBMxx, IEE92a, IEE92b, IEE92c, IEE93b, IEE94c, IEE94d, IEE95b, IEE96c, IEE97b, IEE97i, ISO97, IH99a, JD01, JLO97, KY95a, KR96a, KY98, KT+99, Kau93, KA98b, KM96a, Kle90, KRRR98, KS97c, LOX99, LBMC94, LL94a, LL95a, Lom97, Luc97, Luc98a, Luc99a, Luc99b, MMST98, Mat96a, MS99a, MW98d, MSS98, MM98a, Mue99, Mu93, MM98b, Mu95, Mye97, NIS92, Ng99, NK93, OiDP98, OI98, OUI98b, Opp97, PS98d, PS99c, PB97, PS96d, PS98h, Rei92, RBvR94, Rob93, Rob98a, Rog96, Rus90, Sch94m, Sch95c, Sch95d, SH97, Sch97a, SSv98, Sch98f, SS99a, Sch98h, She97, SSP90, SS90, She92a, She92f, She93c, She93d, She94c, She96b, SK97d, Sun98a, Uni97a, Uni98a, Uni98c, Uni96b, Uni98f, Uni98j, USE90, USE92b]. Security [USE93, USE95b, USE96c, USE96g, USE98d, USE99a, Van95a, VSH97, Van98b, Van99b, Vaa99c, Ved93, Ved98a, Ved98b, VGG93, Ver98a, WSC95, WO98, WO99, Z983, ZFK98, ZFK+98, v994, Aaa99, AFB95, An93d, Bec97, BR96c, BCK96c, BDR97, BKR98a, BKR98b, BBN96, B+96a, Bet95c, BHH99, Boy98, Bro96, Com97, Cha95a, CP94, Chi99a, Chi99b, Cj95, Cli99,CTSxx, Dan99b, DS90a, Den99, DEQ92, D+98, FW99, FM98b, Fra92, Gon92, Grt98, HN98, HK99b, HQ97, HS96b, Hor94, HC95a, HC95b, HY95, HLLC96, IEE94b, JT96, JT97b, JY95, KY97, KG96, Kat97, KS98b, KSB97, KW92, Kuh98, Lai92, LTT95, Lee95,
Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

Session-Layer [BB95c]. Sessioneer [AG95]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].

SETHEO [Sch99k]. sets [MT98], settings [Car97c]. Set [DJL93, FP99, IS91, Koz96, Mei92, Sta96b, SX90, GB88, Kra99].
Nat94a, NMVR95b, Na97, NMV98, NMV99, NIS93a, OFF93, Oka93b, PF94, Pet98, PM98, PS96c, PJ99, RGV97, RDK98, Riv93c, dr94b, SC96a, Sch93b, Sch94e, SK97a, SE96, Sim93, Sin98, SB93, SSNP99, Zha98, Zhe97b, ZTR99, Ame95, Ame96a, ARK99, Ala93a, AW95, Ale97, BD99a, Bis90, Boy97, Bur96, CP95, CMNY94, CSV94, DP96.

signature [FR95c, Gua90, HY93a, HJJ97, Hor98, HMP95, KS98c, LWC96, Mau91b, May97, MS98b, Mus92, NMVR95a, NR95, Pf96c, Pit96a, PS96d, PS98h, SI93b, Sha94, SS95b, SS95c, Ste95, Til98, Tra97, TJ99, Wan92a, Wil93b, Wu92, XA98, YL95a, YL95a, Ye99, Zho94, dr94a].

Signatures [ANS98b, ASW98, AT99, BD99a, BQ95b, BQ95a, BG90, Bm94, BM94a, BM96a, BC93b, BFP99, Boy98, BS95d, CvHP91, CR91, CDF95, Cop99, CD96, Dam94b, DF91a, EGM90, EGM96, Ev91, Fro97, GKR97, GHR99, GM97, GO93, HK95, HA96, JM99, JQBD97, JLO97, Leu96, LSVV95, LR98, MS96, Mis97, MB97, NW98, OO98, Oka94, Pm97, PW93b, PGV93c, SI94, SY96a, Sch93c, Sch93e, Sch94d, SK97b, Sch90b, She97, Tra99, Web98, Wri94, vHP93, BR96c, BGR98b, Ble96, BCDP91, BM91b, Com97, CPS95, Cha95b, Dam94a, Ev92, Ev93, FB97, FY95c, GJKR96a, Jak95, Lan95, LL97b, Ped91a, Pf96c, Rom90b, Sch90a, Sin98, WHL99, WL99, Xie98].

Signcryption [FR95c, Gua90, HY93a, HJJ97, Hor98, HMP95, KS98c, LWC96, Mau91b, May97, MS98b, Mus92, NMVR95a, NR95, Pf96c, Pit96a, PS96d, PS98h, SI93b, Sha94, SS95b, SS95c, Ste95, Til98, Tra97, TJ99, Wan92a, Wil93b, Wu92, XA98, YL95a, YL95a, Ye99, Zho94, dr94a].

Signed [Ber97a, GMCF95, KT93, SIM99, Sun98b].

Signers [TJ99].

Significance [DFGH99, SBV99, SM91, YY98a, ZZI97].

Significant [BV96].

Sign [BG94, GJM99a, GJM99b, GS98, Ped99, Ros97b, Ros98b, Ros98c, KAK96, Ros96a, Ros96c, Ros96f].

Signs [ER97b].

SIGPLAN [ACM99a].

SIGPLAN-SIGACT [ACM99a].

Silicon [NFQ99].

Silicon-On-Insulator [NFQ99].

SIM [Ved98a].

SIMD [Cla97].

Similar [Per99].

similarity [BCD98, Sch90c, Sch97c].

Simmons [Des96b].

Simple [End97, FBS97, GGMM97, Jue99, MS95f, MM94, NR98, RS96c, Rus93a, Sch91i, SW94c, CH97b, RS96b, RRS98, SVWMB95, GM93a, Mye97].

Simpler [Fri92b, MTE99].

Simplifying [CRRY99, CD96].

Simplification [BV96].

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

Signs [ER97b].

SIGPLAN [ACM99a].

SIGPLAN-SIGACT [ACM99a].

Silicon [NFQ99].

Silicon-On-Insulator [NFQ99].

SIM [Ved98a].

SIMD [Cla97].

Similar [Per99].

similarity [BCD98, Sch90c, Sch97c].

Simmons [Des96b].

Simple [End97, FBS97, GGMM97, Jue99, MS95f, MM94, NR98, RS96c, Rus93a, Sch91i, SW94c, CH97b, RS96b, RRS98, SVWMB95, GM93a, Mye97].

Simpler [Fri92b, MTE99].

Simplifying [CRRY99, CD96].

Simplification [BV96].

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

Signs [ER97b].

SIGPLAN [ACM99a].

SIGPLAN-SIGACT [ACM99a].

Silicon [NFQ99].

Silicon-On-Insulator [NFQ99].

SIM [Ved98a].

SIMD [Cla97].

Similar [Per99].

similarity [BCD98, Sch90c, Sch97c].

Simmons [Des96b].

Simple [End97, FBS97, GGMM97, Jue99, MS95f, MM94, NR98, RS96c, Rus93a, Sch91i, SW94c, CH97b, RS96b, RRS98, SVWMB95, GM93a, Mye97].

Simpler [Fri92b, MTE99].

Simplifying [CRRY99, CD96].

Simplification [BV96].

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

Signs [ER97b].

SIGPLAN [ACM99a].

SIGPLAN-SIGACT [ACM99a].

Silicon [NFQ99].

Silicon-On-Insulator [NFQ99].

SIM [Ved98a].

SIMD [Cla97].

Similar [Per99].

similarity [BCD98, Sch90c, Sch97c].

Simmons [Des96b].

Simple [End97, FBS97, GGMM97, Jue99, MS95f, MM94, NR98, RS96c, Rus93a, Sch91i, SW94c, CH97b, RS96b, RRS98, SVWMB95, GM93a, Mye97].

Simpler [Fri92b, MTE99].

Simplifying [CRRY99, CD96].

Simplification [BV96].

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

Signs [ER97b].

SIGPLAN [ACM99a].

SIGPLAN-SIGACT [ACM99a].

Silicon [NFQ99].

Silicon-On-Insulator [NFQ99].
Bov98b, BDB92, Cha99a, Cha91, CM99c, Chr99a, Con98, Con99a, Cor98, CH99a, DDJ98d, DDJ98b, DDJ99, Deu97, Deu98, Di 97a, DT98b, EN98, ENK99, Fan96, FGLP96a, FGLP96b, FOM91, Gar97a, GL96, GPSV98, Gut98a, HKQ99, HP98a, Hru96, HH99, Hus99, Koe99, KCT94a, KCT94b, Mar98a, Mye96, NM96b, Onn90, PV98, Roh99, SKW*98d, SS99a, Sch90a, SR96, SGPV98, Smi98a, Sut99, Tua99, VW98, Ver98b, DWQ91b, DWQ91a, ABKL93, AHdJF97, Ale97, BGV97a, Cha99b, CW97, CJRR99b, DS98a, Dhe98, Di 97b, DF97, Gau97, Kip97, Sha95a, TJ97, Taa98, AG99, Bak99, BF99a, Bro97, DQV96, Gir99, GSTY96, HNS99, IWW99, NF99, SM94, SKAM99].

Smart-Card [Roh99, ABKL93, CJRR99b].

Smartcard [Ano98h, Ano99b, USE99c, Ano97-27, Ara93, Bam97, Ano98g, CH94b, IH99b, KK99a].

Smartcards [Bla96a, Bia96b, Sch90a, DR99a, IH99a, IHR99, MDS99].

SmartLink [Ano93k].

Software-Optimised [RC94a, RC94b].

software [MM95].

Smart-Cards [Roh99, ABKL93, CJRR99b].

Software [Abr97, Ano93j, Auc96, AG99, Bal97, Bih97b, BD94, CD97, Cha98a, CT99b, DBVD96, DF91c, DSB99, Gar97a, GO96a, Gut98b, HK97, JJ98c, KP96b, L95, Lac93, Lea99, Lu98, Mat96b, Mer91, MM97, RSA94, RC94a, RC94b, SW94a, Sch99c, SK96a, SK96b, SK96c, SW97a, SW97b, SK97c, She95b, You96, And94a, Ano95k, Bih97c, BP97b, DH96a, Des95, Gol96d, Knu99c, Pre95a, SS98a, SAM97, Str93a, Str93b, Vau98e, W90].

Software-Optimised [RC94a, RC94b].

software [MM95].

Software [ABKL93, ABKL97, CJRR99b].

Solved [Ano97c, Ano98c, Rec98].

Solving [LO91b, Lew92, MSO96, OMV98, Pen99].

SOM [BBN96].

SOM [BBN96].

Sourcebook [Ban94, Rot95a].

Sources [ADBB99, Cor99, Uni94c].

Southcon [IEE96f].

Southcon/96 [IEE96f].

Soviet [COP95a, HK99c].

Space [AR99, BC95c, FP99, Gar97c, HBKL99, KV99, KI96, SCG99, BB190, Mra95, Pad98, Sze98].

Spokes [BB99].

Space-filling [BB190].

Speaker [CWF91].

Spaceflight [CWM91].

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

Spanish [Mau96b].

Spanish [Mau96b].

Spain [Mau96b].

Spain [Mau96b].

Spain [Mau96b].

Spain [Mau96b].

Specific [ADBB99, EvH93, Kha93, LMS97].

Specification [GFB93, HJT99, LL97a].
Ou99, SW94a, Tou92. Specifications [KS98a, Nat92b]. Specified [Gui97, HCC98].
Specifying [SW94a]. Specs [Got99].
Spectral [WF94].
Spectrum [CKLS97, She94c, CKLS96b, CKLS96c, Dix94, KSB96b, KSB97, LLB98, OP98].
Speech [DMFB97, Er97b, GDS91, IEE97d, IEE97e, Lud97, SW95b, A197, CW94].
Speeches [Bar94].
Speed [ARV99a, ARV99b, Ano99c, Ano99e, DP98a, DP98b, Ebe93, FVEA99, IM93b, Koc94, LS97, MPPS95, SKNO98a, SKNO98b, SW97a, SW97b, She92d, She95b, IM93a, Kap98, KAK96, Lam99, Nor95a, HKSW98, HKRS99, Zhe97a].
Speeding [ADEDS99, KT93, McK99, Tes98].
spi [AG97b, AG97c, AG97a].
spiculated [ZTR99].
Spin [RK99].
Spite [Wai90].
SPJ [TLS99].
SPLICE [HC95b].
SPLICE/AS [HC95b].
Split [Coc97].
Splitting [Sga91b].
SPM [CV93].
SPN [Kob99].
SPN-Structures [Kob99]. Spooing [SVxW91].
SPRC [Wol93b].
Spread [CKLS97, Dix94, She94c, CKLS96b, CKLS96c, KSB96b, KSB97, LLB98, OP98].
Spreading [SB94, KSB96a].
Spring [DDJ98d].
Springer [Hat96].
Springer-Verlag [Hat96].
Spurs [Lea99].
SPX [Ala93b].
Spy [WS96c, Win91].
spy-catching [WS96c].
statesman [Bed90].
Station [BWM99b, Smi98b].
Station-to-Station [BWM99b].
Statistical [De 99, GC91, GSV99, Gus96, PNFK95, NO98, Tha91, GKS97].
Statistics [BBDF97, IEE94a, F090].
Status [Dob96b, FL99b, Nat99c, NBD+99, Ros95b].
Stay [MK94].
Staying [Rit99].
Steady [MSHP99].
Steganalysis [Cl97, Cli99, Lev91, Mil95, UU97b].
statesman [Bed90].
Station [BWM99b, Smi98b].
Station-to-Station [BWM99b].
Statistical [De 99, GC91, GSV99, Gus96, PNFK95, NO98, Tha91, GKS97].
Statistics [BBDF97, IEE94a, FO90].
Status [Dob96b, FL99b, Nat99c, NBD+99, Ros95b].
Stay [MK94].
Staying [Rit99].
Steady [MSHP99].
Steganalysis
[Daw93]. Summer [USE94, Mye96].
Summit [CFK+91]. sums
[BK98g, CFS97, Kob91c]. Sun
[Bro97, Gar98b, Got99, Law98]. SunOS
[Ste92, Sun91b]. Super [Sut99].
Supercomputer [DMS95, She92c, Bam97].
Supercomputing [IEE91]. superhighway
[BDC+95]. Superimposing [YY91].
supersafe [PP96]. Superscalar [Cla97].
superscritcher [Cra92, CF92]. Supersingular [BS91b].
Supervisory [KA99]. Support
[AKP99, BV98a, Bla98, Bld93, DTDJ99,
FR95d, GRB99, HKS95, KHB99, LBHM99,
LCN99, Mon93, Pit96b, SK98a, SK99, SL99,
TYD99, Cli99, LS98a, TCH+91, Un94b].
Supporting [PK99, MI90]. surmounting
[CI96]. surrounding [GA98]. Surveillance
[CKN99, SB97]. Survey
[Bri90b, Gar97c, GFB93, Kal93a, Kle90,
Knu98b, Nis96a, Par98c, BO92, Ele99, Mea95,
She92c, Wad98, Zho94]. Surveys [Ell99].
Susceptibility [AW94]. suspected
[LHL95b, LHL95a]. swapping [TN97].
Swedish [LF97]. Swindles [Dob95b].
Switches [Be99]. Switching [MOM91].
Switzerland [ACM97a, BC97, IEE96e].
sword [Den95]. Sydney
[KG93, SP90, VPM97]. Sylvester [Por98].
Symbolic [Wat91, AM99, BHR95].
Symbols [Pes97, CS99]. Symmetric
[Ada97a, Bir98, BDR+96, BFN98a, FO99b,
Gus96, QG90, Roe94, YY98d, YY98b,
BDJR97, Cra96, GHS93, HJ99, Hwa93].
Symmetry [BS95d, PS97]. Symposium
[ACM90, ACM91, ACM93b, ACM94c, ACM95,
ACM96b, ACM97b, ACM97c, ACM98b,
ACM99b, Ano99c, Com96, CMM93, DEQ92,
He96a, IEE92c, IEE93b, IEE94d, IEE95b,
IEE96a, IEE97f, IEE97i, IEE98a, IEE99a,
KK99b, Qi+98, Spi95, SI93, USE92b, USE93,
USE95b, USE96c, USE96g, USE98a, USE98d,
USE99a, Wat91, Wol93a, Wol93b, Tv92]. synchronised
[KI97]. Synchronization
[DHSS95, BCCG99]. Synchronized
[Yah94, Got92]. Synchronising [Mau91a].
Synchronous [AMP99, NT99, DGV94b].
Syndrome [CS96a, ZYR91, ZH90]. Syntax
[Kal98f, Kal98c, Kal98d, RSA93d, RSA93c,
RSA93e, RSA99a]. Synthesis [HL99, Sab94].
synthetic [PGV93b, PGV94]. System
[ANS99a, Ano97r, ADF98, AHMS99, BS99a,
BLM99, BKS99, Bal97, BR97a, BM91a,
Bien98, Bla94b, BHJ99, BG99, Bur94b,
CIBM99, CD97, CM99b, Chi92, CC99c,
CH94b, CM99d, DDP90, DT98a, DTDJ99,
Far92, FK99, FO97, FR95d, Gar96b, Gar97a,
GRB99, Go90a, GPSV98, GS99a, HJTW99,
HDC99, HJL99, HE98, INDI99, JO97,
Jia99, KI99, KW99, LMP99, LW95, LC99,
MGL+98, MLK97, MR95a, Mar98a, Mau97b,
MTV92, Mon93, NM99, NS98a, Nc96,
PRZ99, PS99f, PK99, Rei92, Rn90, RH99,
SYM99, SSSW98, Sam98, STSW99, SCT99,
SK96b, SK96c, Sch98h, SSP90, SM99,
SKIT99, Tro93, Tun99, Var99b, WHF92,
WABC99, WW98a, WBB99, WABL94,
ZK96, ACC99, BBCP98b, Bax97, BM97a,
Bur94a, BD95b, Car94, CB96, Cus95,
DSSZ99, Des95, DH96b, FM98b, HN94].
system
[HI97, Hwa92a, HC95b, KMB99, KMB97,
LC96a, LCL95, MY93b, MKK99, MM95,
Oel97, PS99e, PS95w, Sch99j, SY96b, SS95b,
SS95c, TCH+91, TC91, Ven90, WSFC99,
WABL93, ADDS91, Ano91a, Bax97, Bel92,
Dan95, JD91, RC91, YKY99, ZH98].
Systematic [BGH+90]. Systematising
[MKL99]. Systeme
[BGH95]. Systems
[ABL93, AKP96, AKF94, Ako99, Ano94j,
Ano95v, Aho96a, ADEDS99, AA97, AMP99,
BDPSNG95, Bar99, Bas93, BR91, BDBDF97,
BFN98a, CF95, DDJ98a, Dan91b, DFT97,
DY91a, DD99, DB96, ENK99, FJP96,
FY95a, FY95b, FYM99, FO091, GL96,
GFB93, Gil98, GM90, GMW91, GK97, GS97,
GMV98, HGH98, HJJ+xx, HH94, HP98b, IEE93a, IEE96b, IEE96d, IEE98c, IEE99b, IH99a, KT96, Koc96b, KA99, KYB92, LO91b, LGRS98, LABW92, Lan99, Lee99b, Mar99, Mas99a, MS95f, MDP94, Mu993, NT99, NAA99, Oka98a, Oka98b, PRAM98, Pes97, PL94, PS99f, PW97c, PS96b, PSN91, Pin97, Pin96b, PM99a, PD99b, RBvR94, RG95, RIP95a, ST94, SN96, STS99b, DY91c, SOOS95, SS90, She92a, SY92, Stu99, Tra99, USE96c, USE96a, USE99b, VC99, Var99a, Way93a.

Systems
[WL92b, WC97, Yac99a, Yac99b, YKB94, YMWP99, ZFK98, ZFK+98, ARK99, AhldJF97, AMS96, AM99, AC97, BY93c, BY93b, BGT96, BP95b, CG05, DMW94, Dix94, Fri92b, Goo96, GKS97, Gru98, HJJ+97, IEE97k, KG96, KP99b, LM98a, LABW91, LS98a, Lie93, MSN97, NIS92, Oht96, Ole95, Opp96, PAK98, PA98b, PP92a, PP92b, PP95b, PP99a, RO96, SK97, SY96b, SG96b, SK97a, Sta97a, Sta94a, Sun91b, VP98, WL92a, WL92c, ZG96, DV96].

Systolic
[SS98, DF92, PJBM90].

SZK
[Dav98d].

T
[YT96, PDGI99].

TEAM
[PDGI99].

T52
[Dav98c].

T52e
[Sei98b].

Table
[KMKH99, Has99, Hor95].

Tableaux
[Mas99a].

Tableaux-99
[Mas99a].

Tables
[DRR95, JC98, lPNdbbbprm91].

Tactical
[IKM99].

Tagging
[Lud97].

Tailoring
[CGM96].

Taken
[GGW+91].

Tale
[Kal98e, RS98f].

Talent
[DDJ98e, DDJ98f].

Talk
[Deu97, Lei99b, Wat99].

Talking
[HH99].

Tamper
[Auc96, BDHJ98, KK99a, Zhe95b].

tamper-proof
[Zhe95b].

Tamper-Resistant
[Auc96, KK99a].

tamperfree
[Hwa92b, Hwa92c].

Tampering
[CL98, CL97b].

Tanaka
[Hwa92a, MS98a].

Tandatangan
[Ano97-29].

Taos
[WABL93, WABL94].

tapestry
[MB94b].

TAR
[Ano97].

Targeted
[Cap94].

Targets
[Lea99, Way98].

TAS
[Cop94b].

Tasty
[Sch98i].

Tate
[FMR99].

Taxing
[Gar97c].

Taxonomy
[DB96, GS97, LBMC94].

TC
[MB99b].

TC11
[Kat97].

TC6
[Kat97].

TC6/TC11
[Kat97].

TCFS
[Mau97b].

TCl
[GAl98].

TCP
[Fei93, Fei96].

TCP/IP
[Fei93, Fei96].

TEA
[KSW97a, KSW97b, NW97, WN95].

Team

TecApro
[GLC98].

Technical
[Ano95e, Bar96b, CFK+91, CYY98, DS97c, Lan98, LM93c, 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, De95, Des98a, Des96a, Fun97, Fun98c, GQ95, Hel94, JJ99a, LvLB96, MM99a, MSNW99, Man96b, PS98e, PS98f, PK99, Pre93b, QV90, QQ95, Rue93, SZ93, Car98, Cra96, Hel93, He98b, ISO97, Kay95, KG93, Nyb98, OP9+99, Oke96, PS99d, SD97, Ste99b, Way91, Woo90, ZH93, van96].

Technological
[UFC94].

Technologies
[Ano96l, Ano96m, Ano98j, AA97, Ban93, BDDG99, DKK+98, Fol99, Gar98a, Gar98b, GN95b, Hat96, HH96, IEE94b, IEE98d, Lie94, Lnn93c, NFQ99, Rv98c, USE99c, Ano93a, DS97b, Gil97, ISO97, Rif96, Ros94, Sni97a, VB96, CFK+91, Ers99, Ano99b].

Telecollaboration
[Fuc99].

Telecommunications
[IEE97e, UN94, Mac98].

Telemedicine
[Ano97-29].

Teleperubatan
[Ano97-29].

Telephone
[Gar97a].

Telephony
[Bar94, Gar97b, MB99a, Mar95b].

teletype
[Mac98].

TELNET
[SSH93, Atl93b, Bor93a, Bor93b, Bor93c].
Rh99, Sch99I, Sho97, Tro93, Vbd99, Yac99a, Yac99b, Acc99, BP98d, Bhs93, BM96b, BM96c, BK98f, Gk97, HS91, Iee94b, MAM95. time-stamp [HS91].

Time-Stamping [BLV98, Bhs93].

Time-Stamps [HKS95].

Timed [BLLV98, BHS93].

Time-Stamping [BLLV98, BHS93].

Time-Stamps [HKS95].

Timed [KA99, DOR99].

timed-release [DOR99].

Timeliness [Yah94].

Timely [KYB92].

Timestamp [WI99].

Timetabling [CC99c].

Timing [DS98b, EH96, HK98, HK99d, Koc96b, MM92a, MM94, BS95c, Koc95].

Timken [Kar96].

tiny [WN95].

Tip [Zuk98b, Zuk98a].

TIRPITZ [Wei99].

TLS [Pau99].

Today [Fro97, ZKL98, Way95].

together [Car98, UU97a].

Token [BE90, Nys99, Yl97b].

Tokens [Jue99, KS99a].

Tolerance [PW97c, Iee94b, TCH+91].

Tolerant [DHSS95, OKST97, RBvR94].

Tomayko [CWM+91].

Tommy [Pin98].

Tomorrow [ZKL98].

Tonga [Gar97a].

Too [Bur99].

Tool [AKP99, KKW99, Sch99k, WB92, YY97c, An97u, Bur96, DFHR91, KKW99].

toolkit [BP97b, Way98, Rei96].

Tools [BY93a, Des99a, GS97, RB99, WC97, DD95, LS98a, Mee99].

Top [Ben98, Hel93, MB99a, Mus92].

TOP500 [DMS95].

Topics [IEE99b].

Topological [OMA98].

Topology [COZ99].

toral [VP96].

Torn [MR98].

Torok [Lip93].

Toronto [IEE94f].

Toshiba [Got99].

Touches [MB99a].

Toulouse [DEQ92].

Tour [Han94, Mos99].

tourist [WSFC99].

Town [IEE94a].

Traceability [GS97, SW99b, Des95, LHL95b, LHL95a].

Traceable [BW97, T99].

traceability [Sta97a].

Traced [Pf96b].

Traces [Vig98, HM97b].

Tracing [BF99c, CF94, Fia94, FT99a, Jue99, Mad92, NP98a].

Track [USE98c, Fox99].

Trackies [SKIT99].

Tracking [HCDC99, Hur98].

Trade [BFS96, BMS96, Un98d, Un98e, NMVR95a, NMVR95b].

Trade-offs [BFS96, BMS96, NMVR95a, NMVR95b].

Trademark [Eri97b].

Tradec [KR94c, CK93].

Tradeoffs [CMN99].

Trading [FHM98, DS97b].

Traditional [Des92].

Traffic [CIBM99, CK93].

Train [BW98].

Training [ACBR90, DTDJ99, Jen99].

Traitor [BP99c, FT99a, NP98a].

Tractors [CFN94, Fia94, Pf96b].

Transaction [ENK99, KT96, Oh99, CTSxx, ADDS91, An91a, JD91].

Transactions [FL99b, FKM98, SSG99].

transcendental

Transcript [BD99a, Chr99a, Saa99a].

Transcript-irrelevant [BD99a].

Transfer [An97s, DF99, HHY93, NP99, RS96a, Be93, BM90, BR96b, DOR99, Jac90a, Jac90b, SI93b]. Transferable [Sak96].

transferred [Un97d].

Transferring [SI94].

Transform [Boy99, KMS95a, KMS95b, Kuo90, MS94, Riv97c, WF94, TK98].

Transformability [MS96].

Transformation [SZ96, LS98a, Pet91].

Transformational [Zwi98].

Transformations [BDFM99].

Transfusion [ABB99].

Transient [BD98, CH94a, QJD97].

Transistors [CW95+91].

Transition [Dec98a, DR98b].

Translation [CF9+91, OP97, OP98].

Translucent [BR96b].

Transmission [NHB98, PS97].

transmitting

Transparent [Cii97, Cii99, UU97].

Transparency [Bl93, DS97c, Mau97b, SZ96b, ZG96].

Transport [An94b, BWM98, GBC93, Sar97].

Transportation [BPR99, Uni98b].

transposition [Bar92a, Bar95, GSN94].

Transputer [GN95b].

trap [Yu92].

trap-door [Yu92].

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

Trapped [Gib91, Gor93].

trappes [Sch98e].

Tree-Based [BM96b, BM96c].

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

Trees [Aga92, BP97a, HS90, ZW99, SSM92].

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

Trends [DDJ98e, DDJ98f, De 93b, De 98c, Hru98, IEE97k, Kan96, LM98a, MB99a, Koo97, Seg92].

Trial [Mye96].

Trials [CYY98, Pfi96b, Ano93a]. Triangular [Por98].

Tribulations [CYY98]. tribute [Uni92].

Trinity [IEE97a].

Trip [Cur98].

Triple [Ano96j, Ano96k, Bih96, BK98c, Bih99b, CMI95, HP99a, HP99b, KMS95b, Kum98, Lue98c, CM99e, Per91, vO9W1, Joh99, KSW96, Rot97].

Triple-DES [Ano95j, Ano96k, BK98c, Kum98, KSW96, Rot97].

triples [CFS97].

Trithemius [Ree98]. Trojan [Sch99f]. True [Way91].

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

Trust [Ano99f, BPK99, BFK99, LA98, MR98, Rei96, SA95, Sin94a, Sta95a, YKK94, YY99, AHdJ97, BH98, Com97, Chi99a, Chi99b, LN98].

Trust-Based [YKB94].

Trusted [AAB+97, Ano97d, IS91, MKS99, RS98b, SK97c, SS99e, SS99f, CMI97b, HY93a, JMO95a, LWC96, Ped91c, Wu92].

Trustee [Kue99].

Trustworthy [Fri93, Pos92].

Truth [Fort99].

Try [Rot97].

TSP [Luc95].

TTP [BDHJ97].

TTP-based [BDHJ97].

TTPs [Lan98].

Tübingen [PDR99].

tucked [Ano91b].

Tunable [WF94].

Tunneling [SM98a].

Tuples [FJRS96, M190].

Turbo [DD99b].

Turbulence [DF94].

Turing [CFF91, Hod97, Dea98b, Tur99].

Turnaround [Gar97a].

Tutorial [Buc91b].

Tutoring [PD99b].

TV [DDNM98, Gar97c, Gar98b].

Twelf [PS99f].

Twenty [Ano95t, Bon99, ACM90, ACM91, ACM93b, ACM94c, ACM95, ACM96b, ACM97c, Gol97c].

twenty-eighth [ACM96b].

twenty-fifth [ACM93b].

Twenty-Ninth [Ano95t, ACM97c].

twenty-second [ACM90].

twenty-seventh [ACM95].

twenty-sixth [ACM94c].

Twin [Mae98].

Two [AB96a, Bea92, BM99a, BM99b, BSH99, BS99c, BGH91, dBB91, BKR97, Cha94a, CPPK98, Dob97, Gil99, Gol96b, HKQ99, HK98, HK99d, HEQ98, HLL+95, Koe99, LHY93, LM98b, Mad92, PPK97, PS98g, RS96b, RS96c, WN94, Yin97, ZM91, vT93, BDH97, Den95, Dob98, HWF96, HY95, JW01, LHW99, LC97b, MB94b, MCD98a, Pr906, WHL99, ZLX99, dB91, vO9W1].

two-key [vO9W1].

two-level [HWF96].

two-list [LC97b].

Two-Party [BM99a, BM99b, BGH+91, JW01, ZLX99].

two-phase [HY95].

Two-Round [Dob97].

Tweak [Fer98, Fer99a, MM99c, Murr99, SK+98b, SK+98c, Sch98g, SK+98a, SK+98f, SK+98d, SKW+99d, SK+99a, SK+99e, SKW999, WW98b, WS98, WKS+99, WHi99].

TWOPRIME [CWS99, DNRS97].

TX [ACM99a, IE98e, USE91].

Type [BD99a, BS90b, DE99, MC92, SN93, SK95, CLL99, G95b, Q98a, Koy95, KKK6, Tak97, Tak98a, Tak98b, Wan92b, Xie93, BJ97, QB97, D979].

Types [SG95, Bili94a].

typing [She95a, Aba99].

U [Kah91a].

U-boat [Kah1a].

U.K. [And96c].

U.S. [ACM94b, Ban94, My998, Riv98c, SW94b, Sta97c, Uni97d, Unixxb, Uni96c, VB96, Way93c].

U.S.A. [LF97].

U.S.C. [C197, U97b].

übersicht [Ger97].

Ubiquitous [DD99a, Cha99b].

UC [Uni96a].

UK [Gol96d, Wal99a, And94a, Boy95b, Chr99b, Dar97, Dav91, IE99a].

Ultra [Ben98, LS97, Blo98a, Blo98b, Blo98c,

Unbalanced [Jut98, KPG99, SK96c, SK96d]. uncorrupted [PBBC97].

Uncertified [KC95]. Unclassified [Bra90a].

Uncompressed [NHB98, HC98].

Unconditional [CM97a, FM98, GM90, WP90, Wa90, Wol99, MSN97].

Unclassified [BPRF99, Hru99, KMPS99, Ou99].

Uncryptic [Pfl95].

Undang [Ano97-29].

Undang-undang [Ano97-29]. Undeniable [CvHP91, CR91, D91f, Tay95, BMS96, Des90b, HW98c].

Underground [HLMP96].

Underlying [HL99, CGM96].

Understanding [MF97].

Understanding [MF95].

Understanding [Ano97y].

Understanding [Ano97z].

Understanding [Ano97-30].

Understanding [AW94].

Understanding [Ano98f].

Understanding [BWM99b, Pai99a]. Unlinkable [SGS99].

Unmet [FM98b]. unperceivable [BBCP98a].

Unpredictability [Kos99, NR98]. Unproved [ZMI90].


Untraceability [WP90, Wa90].

Untraceable [OO90]. Untrusted [SK98a].

Untruths [For99].

Unveil [GA97, Gar98a].

Unveiling [Jan98]. Unveils [Gar97a, Gar98b].

Upon [BMP97a, CCH98, LCL95].

Urgent [Pra96]. URL [Zuk98b].

Usability [WT99, CG05]. USACM [Ano97-30]. Usage [End97].

Usage [BCE94].

Usage [GS94a, SZ96, Car97c, Car98, GA97, Kuk99, Sch91b, SX90, van97a].

Users [Hel98a, WK97, Sta94a]. Uses [Swi97, D9R97b, Sch99g]. Using
Variable-Input-Length [BR99a, BR99b].
Variable-Length [Sch94b, Su98]. Variance [Kas96].
Variants [CRRY99, MSS98, RS99a, Sha95a].
variation [CCN95]. variations [Zho94].
varieties [Fri92b]. Various [GQW+91].
Vascularature [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]. VerCheck [MGL+98].
Verdict [Wri94]. Veri [SY99].
Veri-KoMoD [SY99]. Verifiable
[Abe98a, AGY95b, CG98, Cri90, FR95c, GM95b, Ped91d, Sch99i, VBD99, AGY95a, BD98a, Bur96, FO98, Mao97, MLY93, Ped91b, Ped91e, Sta96a].
Verification [Abe98a, AB97, BGR98a, Bol98a, Bol98b, CDFI95, DS97a, GFB93, GS99a, HL92, MM99a, Na97, OMI93, PM98, PV98, SM95a, SY99, Tou93, WW98b, YI99a, BGR98b, Bol97, BS95c, Des90a, Dwo91, JC98, JW01, Mee95, YL95a, YM98, ZLX99].
Verifications [GMV98]. Verifier [JMSI96].
Verifiers [PM98]. Verify
[DS97d, Chi99a, Chi99b]. Verifying
[LHB96, Sa91, DN95b, Pau98]. Verlag
[Hat96]. Verlässliche [BGH95b]. Vermont [IEE96a]. Verschlüsselte [Kip97, Kip99b].
Verschlüsselung [MPS94].
Verschlüsselungssysteme [Wal98].
Verschlüsselungsverfahren [Ger97].
Version [An97r, An97s, BC93a, BP98e, DBP96, FKK96, Gar97b, Kal98f, Kal98c, Kal98d, Kal98b, KS98a, RS93f, Lim99, MT99a, McM96, RSA93a, RSA94, DY91c, SS99b, SM98b, WABC99, CLW98, GM93a, Gib95, Bor93b, Lin96b]. Versus [MGL+98].
Vertraulichkeit [FT95]. Very
[HMV93, MSDS90, PF94, Yua92, SN94].
Veto [OK96a]. VHDL [Oel97]. via
[DDJ98g, DDJ98h]. Wollongong [PSN95b]. women [Wil98a], won’t [AK95, ZKOY99].

Wollongong [GN95b]. Worchester [KP99b]. Word [LMOB95]. Words [HKL94, Ata94, AGIL95, CC98, SM90, Sta96b].

Work [Abe98a, Ano97y, BK95c, CFSY96, Gar98b, MGL98, BK98b].

Word [LMBO95]. Words [HKL94, Ata94, AGLL95, CC98, SM90, Sta96b].

Work [Abe98a, Ano97y, BK95c, CFSY96, Gar98b, MGL98, BK98b].

workfactor [Jas96, Kau96]. Working [DDJ99, Kat97, LM98a, MB99b].

Works [Ano96k, FJM96]. Workshop [ACM98a, And94a, ???90, Ano93g, Ano99b, Auc98, Bih97c, Bra93a, CW94, Chr99b, Dam90a, Dam91a, Dav91, De95, FM91, Gol96d, Hel94, IEE92a, IEE93a, IEE94a, IEE96c, IEE96d, IEE97e, IEE99b, IZ98, IZ99, Kmu99c, KP99b, Ku91, LW96, MDP94, Pit95, PH91, QV90, Rue93, Sch94j, SZ93, TM99, USE95c, USE96d, USE96b, USE96, USE99c, USE99, BFS92a, BFS92b, CFG96, Chr98, D+98, FR95a, GS94b, Lom97, Org98a, Pre95a, TV94, USE90, Vau98e, WL98b, Ano96k].

Workspaces [BV98a]. Workstation [DS90b, IEE93a].

Workstations [Gar98b]. World [Ano93d, DW98, Dav95, Hin93, Lut98, Ritxx, She96b, Blu97, CDEH96, IEE92d, LC95, Sta97c, WSFC99, Ale98, Alv98b, AK99, Dav98a, Don98, Mon96, Mus92, OW95, Rat96, Ros99, Wil98a].


worst-case [AD97, AD99, BHHR99]. worst-case/average-case [AD97, AD99].

Wrapping [Gar97a]. Wright [WD99a].

Write [Bra95d]. Writing [Sha99a, Kah66, Ros97c]. Wu [Bur94a, Bur94b, HLC96, Roe99].

Wu-Dawson [Roe99]. WW [Pin98].

WWOS [IEE93a]. WWOS-IV [IEE93a].

WWW [OW95, Zha96].


Y2K [Ano98j]. DDJ98b, Eri97b, Law98, MGL98. Yakeha [Gab96b]. Yarrow [KSF99]. Year [Sch95a, Si99, Roe95]. Years [Bon99, Yin97, BC96b, CWM91, Den90, Gol97e, Mar96].

yi [PNdbbprnn91]. Yield [GMW91]. Yokohama [IZ98]. York [IEE99a, USE95c].

Yu [BY92]. YY [Nat92b].

Z [Mau91b]. Z80180 [Kal93b]. Zero [BG90, BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOVY93, NMV99, O090, R91, SI93a, BOGG+90, BPP95a, BBP95b, DF93, DP94, DF91b, Sahl99].

Zero-Knowledge [BJY97, BD91, BDB92, CD98b, Dam99a, DDP94a, DDP99, DO99, DFKN93, DS98b, GMW91, GK96, GSV99, GO93, HT98, NOVY93, NMV99, O090, R91, SI93a, BOGG+90, BPP95a, BBP95b, DF93, DP94, DF91b].

zeta [Kob91c]. zeta-polynomials [Kob91c].

References

Anonymous:1990:IWH


Anonymous:1997:ACC


ANSI:1988:FIE


Anshel:1993:PMT


ANSI:1995:ANS


Arabnia:1997:IC1


Abdikalikov:1999:ERC


Abelson:1997:RKR

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

Almgren:2000:HWC

Andrasiu:1992:NCB

Asmuth:1981:EAC

Anderson:1996:TPP

Anderson:1996:TFN
REFERENCES


**Abadi:1993:ADS**


**Abadi:1993:CAC**


**Abraham:1997:SEE**


**Auyong:1997:ASC**


**Apolloni:1990:TNN**


**ASCFS:1997:XPK**

REFERENCES

[An:1999:ODR]

[ACD94]

[Alexi:1984:RRB]
W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA/Rabin bits are \(1/2 + 

[Alexi:1988:RRF]

[Ack98]

[ACM82]

[ACM83]
REFERENCES


REFERENCES


REFERENCES


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


REFERENCES

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

Areces:1999:PRR


Abraham:1991:TSS


Appas:1999:SVS


Augot:1998:DSM


Alagappan:1990:PDA


Adleman:1979:SAD


Adleman:1983:BGK


Adleman:1987:PRD

Leonard Adleman. PRDA days: History and
lessons. In Ashenhurst [Ash87], page ?? ISBN
0-201-07794-9. LCCN
Turing Award lecture.

Asokan:1999:APT

[ADSW99] N. Asokan, Hervé De-
bar, Michael Steiner, and
Michael Waidner. Authen-
ticating public ter-
ninals. Computer Net-
works (Amsterdam, Nether-
lands: 1999), 31(8):861–
870, April 23, 1999. CO-
DEN ???. ISSN 1389-1286
(print), 1872-7069 (elec-
elsevier.com/cas/tree/
store/comnet/sub/1999/
31/8/2125.pdf.

Alves-Foss:1995:ACS

[AFB95] Jim Alves-Foss and Sal-
vador Barbosa. Assess-
ing computer security vul-
nerability. Operating Sys-
tems Review, 29(3):3–13,
July 1995. CODEN OS-
RED8. ISSN 0163-5980
(print), 1943-586X (elec-
tronic).

Apostolico:1985:CAW

[AG84] A. Apostolico and R. Gi-
ancarlo. Pattern matching
machine implementation of
a fast test for unique de-
cipherability. Information
Processing Letters, 18(3):
CODEN IFPLAT. ISSN
0020-0190 (print), 1872-
6119 (electronic).

Apostolico:1985:CAW

Alberto Apostolico and Zvi
Galil, editors. Combinato-
torial algorithms on words
(Maratea, Italy, June 18–
22, 1984), volume 12 of
Springer-Verlag, Berlin,
Germany / Heidelberg,
Germany / London, UK /
etc., 1985. ISBN 0-387-
15227-X. LCCN QA164

Anderson:1995:SFS

Scot Anderson and Rick
Garvin. Sessioneer: flex-
ible session level authen-
tication with off the shelf
servers and clients. Com-
puter Networks and ISDN
Systems, 27(6):1047–1053,
April 3, 1995. CODEN
CNISE9. ISSN 0169-7552
(print), 1879-2324 (elec-
elsevier.com/cas/tree/
store/comnet/sub/1995/
27/6/1464.pdf.

Abadi:1997:RAC

M. Abadi and A. D. Gor-
don. Reasoning about
cryptographic protocols in
the Spi calculus. Lecture
Notes in Computer Science,
1243:59–??, 1997. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).
 REFERENCES


REFERENCES


0558/papers/1267/12670190.pdf.


REFERENCES


REFERENCES

Aberer:1994:DUO


Akoka:1999:CDP


Abdelguerfi:1996:GEI


Aljabri:1996:UDU


Alabbadi:1993:IEC


Alagappan:1993:RTA


Alabbadi:1997:SCH

M. M. Alabbadi. Security comments on the Hwang–Chen algebraic-code cryptosystem. Lecture Notes in Computer Science, 1334:
REFERENCES

274-??, 1997. CODEN LNCS99. ISSN 0302-9743 (print), 1611-3349 (electronic).

Alberti:1470:TC


Alexander:1945:CHG


Alexandris:1992:FMC


Alexandre:1997:BSC


Alexandre:1998:JBP


Alexander:1997:DEC


Allen:1998:SUM


Ahituv:1987:PED

REFERENCES


REFERENCES


REFERENCES


REFERENCES


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

**Anonymous:1939:ITM**

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

**Anonymous:1960:CNH**


**Anonymous:1976:CCA**


**Anonymous:1978:CSD**


**Anonymous:1978:ODA**


**Anonymous:1980:ACS**


**Anonymous:1981:CHP**

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


[Ano82b] Anonymous. Encryption scrambling the satellite signal for security, 1982. 1 sound cassette (75 min.).


REFERENCES

sored by the International Association for Cryptologic Research.

**Anonymous:1985:DEA**


**Anonymous:1987:EVE**


**Anonymous:1988:EVE**


**Anonymous:1988:ERH**


**Anonymous:1989:SZS**


**Anonymous:1990:SEL**


**Anonymous:1991:ESS**


**Anonymous:1991:FFL**

Anonymous:1991:E


Anonymous:1992:AUd


Anonymous:1992:DES


Anonymous:1992:DDS


Anonymous:1993:ACT


Anonymous:1993:BRd


Anonymous:1993:CKR


Anonymous:1993:CSA


Anonymous:1993:CNh


Anonymous:1993:FSH

[Ano93f] Anonymous. FIPS 180, Secure Hash Standard. NIST,
REFERENCES


Anonymous:1993:JIK


Anonymous:1993:LC


Anonymous:1993:SBh


Anonymous:1993:SMC


Anonymous:1993:WND

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

Anonymous:1994:CNc


Anonymous:1994:DAX


Anonymous:1994:HSK


Anonymous:1994:ICI

REFERENCES


Anonymous:1994:KEE


Anonymous:1994:Lba


Anonymous:1994:Li


Anonymous:1994:PRP


Anonymous:1994:Uc


Anonymous:1994:WAS


Anonymous:1995:AUC


Anonymous:1995:AUM


Anonymous:1995:EES

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


Anonymous:1995:ARLb


Anonymous:1995:ARD


Anonymous:1995:ENAa


Anonymous:1995:ENb


Anonymous:1995:FSH


Anonymous:1995:NIX


Anonymous:1995:OIN


Anonymous:1995:PTN

REFERENCES

Anonymous:1995:RLM

Anonymous:1995:SUE

Anonymous:1996:ADX

Anonymous:1996:BCU

Anonymous:1996:CID

Anonymous:1996:CPD

Anonymous:1996:ENa
REFERENCES

Anonymous:1996:ENb


Anonymous:1996:ECC


Anonymous:1996:SCG


Anonymous:1996:SUS


Anonymous:1996:TBAa


Anonymous:1996:TBSa


Anonymous:1997:RDSa

Anonymous:1997:AES


Anonymous:1997:AUC


Anonymous:1997:AWS


Anonymous:1997:AIR


Anonymous:1997:ARDa


Anonymous:1997:ARDb


Anonymous:1997:ADF


Anonymous:1997:CVC

Anonymous:1997:DNH


Anonymous:1997:ENa


Anonymous:1997:ENb


Anonymous:1997:ENC


Anonymous:1997:EWh


Anonymous:1997:HEW


Anonymous:1997:INI


Anonymous:1997:MNL

Anonymous:1997:NPA


Anonymous:1997:NPNb

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

Anonymous:1997:RAJ


Anonymous:1997:RDL


Anonymous:1997:RDSb


Anonymous:1997:SFR


Anonymous:1997:SUE

Anonymous:1997:SUR

Anonymous:1997:SSA

Anonymous:1997:CBP

Anonymous:1997:UUS

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

Anonymous:1998:ARD

Anonymous:1998:CSIb
Anonymous:1998:ICS


Anonymous:1998:EN


Anonymous:1998:Ea


Anonymous:1998:PCA


Anonymous:1998: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:SIb


Anonymous:1998:SUP


Anonymous:1998:TBF

REFERENCES


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

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


REFERENCES

Abreu:1994:DAI

Anderson:1998:LS

Andrasiu:1993:LTP

Aruliah:1985:PIE

Allen:1997:PSA

Aumann:1998:AES
REFERENCES


REFERENCES


**Araki:1998:OEC**

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

**USENIX:1988:CSSb**


**Asokan:1998:OFE**

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

**Abdalla:1999:TMB**


**Atkins:1996:RPM**


**Akl:1983:CSP**


**Ateniese:1999:SOI**

REFERENCES

[Atallah:1999:ATC]

[Atanasiu:1993:AEU]

[Al-Tawil:1998:NAP]

[Atkinson:1995:RIA]

[Atkinson:1995:RIE]

[Atkinson:1997:TMS]
REFERENCES

ATT:1986:AUS


Aucsmith:1996:TRS


Aucsmith:1998:SIW


Aura:1996:PID


AAGD:1996:RPR


Aparicio:1999:ITD


Avolio:1998:PCP

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

Anderson:1996:NC


Alabbadi:1994:SDS


Alabbadi:1995:DSS


Angel:1999:JQH


Aspray:1988:RCD


[Ayo68a]


[Ayo68b]


[Ayo81]


[AuferHeide:1999:PGP]


[AuferHeide:1999:PGP]

REFERENCES


Blau:1996:VPA


Baker:1997:RRM


Bach:1988:HGF


Bacard:1995:CPH


Badia:1999:EDL


Baker:1992:CAB


Biham:1998:SNB

REFERENCES

Bakker:1999:MAS


Ball:1997:ESS


Ball:1999:WSB


Bullitt:1999:GDI


Bamford:1982:PPR


Bamforth:1997:JSS

R. Bamforth. Java — from smartcard to supercomputer. In Anonymous [Ano97p], pages 1–?? ISSN 0963-3308. LCCN ????

Burrows:1989:LAb


Burrows:1989:LAa


Burrows:1990:LA

Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. ACM Transactions
REFERENCES

Banisar:1993:BCE

Banisar:1994:CPS

Bao:1994:IRL

Barker:1961:CSC

Barker:1975:CSS

Barker:1977:CHC

Barker:1979:CEC

Barker:1979:HCCb
Wayne G. Barker, editor. *The history of codes and ciphers in the United States during the period between the World Wars*, volume 22,
Naturally, the text is not readable in this format due to the image's quality hindering text extraction. Please, consider another format for better understanding.
REFERENCES


[Bar96a] 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


Barlas:1996:NKD


Barker:1995:CDT


[Bar94]
REFERENCES


REFERENCES


REFERENCES


[BB95a]

[BB95b]

[BB95c]

[BB95+]
Werner A. Baum, David H. Brandin, R. Creighton Buck, George I. Davida, George Handelman, Martin E. Hellman, Ira Michael Heyman, Wilfred Kaplan, and Daniel C. Schwartz. Report of the Public Cryptography Study Group, pre-

[BBCM93a]

Bennett:1991:EQC


[BBCM93b]

Bennett:1995:GPA


[BBCM95]

Barni:1998:MPI


[BBC98]

Blakley:1993:TSD


[BBCM93a]

Blakley:1993:TPD


[BBC98]
REFERENCES


REFERENCES

Bennett:1992:QC


Bauer:1983:KDP


Biham:1998:CM


Bertilsson:1990:CVE


Bleichenbacher:1995:SRL


Benantar:1996:AOS


REFERENCES


[BC93a] Amos Beimel and Benny Chor. Universally ideal secret sharing schemes (pre-
REFERENCES


Bos:1993:PUS


Beguin:1995:GSC


Beimel:1995:SSP


Blundo:1995:SRB


Blundo:1996:BES


Brassard:1996:YQC


Blakley:1998:C

G. R. Blakley and D. Chaum. Crypto ’84. Lecture Notes
REFERENCES


Burwick:1998:MCC

Barker:1988:ECT

Bigun:1997:AVB

Blair:1999:DRA

Baritaud:1993:SPK

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


REFERENCES


tology: proceedings of EUROCRYPT 84, a Workshop on the Theory and Application of Cryptographic Techni
delberg, Germany / Lon


[Bellare:1996:PFRa] M. Bellare, R. Canetti, and H. Krawczyk. Pseudo-


0558/tocs/t0209.htm; http://www.springerlink.com/openurl.asp?genre=
issue&issn=0302-9743&volume=209. Held at the University of Paris, Sorbonne.


[BCI98]

Bellare:1996:KHF


Bellare:1996:MAU


Bellare:1998:MAD


Bellare:19xx:KMM


Bromley:1983:RFM


[REFERENCES]


Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes (extended abstract). Lecture Notes in Computer Science,
REFERENCES


Burmester:1991:ALN [BD91]

Bauspiess:1992:RCH [BD02]

Brandt:1993:GPP [BD93]
J. Brandt and I. Damgaard.


Bloomer:1994:FFS [BD94]

Bloomer:1995:PLC [BD95a]

Burmester:1995:SEC [BD95b]
REFERENCES

Blundo:1997:LBR

Bao:1998:SSS

Blundo:1998:VCS

Bao:1999:NTM

Boneh:1999:CRP

Burmester:1992:EZK
REFERENCES

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

[BDC+95]

[BDD+94]

[BDF98]

[BDFM99]

[BG99]
C. Blundo, A. De Santis, and A. Giorgio Gaggia. Probability of shares in se-


[BDGI98]


[BDG93]


[BDHJ97]


[Boneh:1999:FPL]

[BDH99a]

[Boneh:1999:BFL]


REFERENCES


REFERENCES


REFERENCES

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

Beaver:1993:HBS


Beaver:1996:ASE


Beaver:1997:CBC


Beaver:1997:PPE


Becker:1982:EDE


Beckett:1988:IC


Beckett:1990:IAM

REFERENCES

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

Beckett:1997:ICP


Beck:1999:DPE


Bedini:1990:TJS


Beesly:1981:CIW


Behrens:1954:EUP


Bell:1977:IVU


Bellcore:1992:GRX


Bellovin:1998:CI

REFERENCES


REFERENCES

[Berson:1993:DCA]

[Berson:1996:HMO]

[Berson:1996:NIC]

[Berson:1997:FMP]

[Berg:1997:JQHd]


Albrecht Beutelspacher. *Cryptography: an introduction to the art and science of enciphering, encrypting, concealing, hiding, and safeguarding described without any arcane skullduggery but not without cunning wag-gery for the delectation and instruction of the general public*. Spectrum series.
REFERENCES

Mathematical Association of America, Washington, DC, USA, 1994. ISBN 0-88385-504-6. xvi + 156 pp. LCCN Z 103 B4813 1994. Cryptology was originally published in German by Vieweg. This edition has been extensively revised. [BF99a]


REFERENCES


[BFM88] Boneh:19xx:


[BFKL94] Blum:1994:CPB


[BFN98a] Blaze:1999:KTM


Boyd:1999:EEC


Beth:1992:PKC


Blundo:1996:TBC


REFERENCES

[168]


REFERENCES


REFERENCES

Bender:1996:TDH


Balkin:1994:CEC


Bellare:1995:XMN


Bellare:1995:BVA


Bellare:1998:FBV


Bierbrauer:1994:BRF

Jürgen Bierbrauer, K. Gopalakrishnan, and Douglas R. Stinson. Bounds for resilient functions and
REFERENCES


Blundo:1995:DRR


Bierbrauer:1996:OAR


Berkovits:1998:AMA


Benantar:1996:ACS


Bosselaers:1993:CWP

REFERENCES


REFERENCES


REFERENCES

[174]

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

Bellare:1998:MTF


Bellare:1998:MOT


Brassard:1998:QCH


Bertilsson:1993:CPS


Bao:1994:RAF


Bao:1995:BFA


Breitbach:1999:CCM

[BI99] Markus Breitbach and Hideki Imai. On channel capacity and modulation of watermarks in digital still

**Bar-Ilan:1989:NFC**


**Biermann:1998:HKB**


**Biham:1991:CCC**


**Biham:1992:DCI**


**Biham:1994:NTC**


**Biham:1994:MOA**


**Biham:1995:CMM**

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].


[Bih98a] Eli Biham. Initial observation on Skipjack: cryptanal-
REFERENCES


REFERENCES


[Bis91] Matt Bishop. An authentication mechanism for USENIX.
REFERENCES

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

Bishop:1992:FPC


Bleichenbache:1997:NOC


Bellare:1997:ROZ


Book:1980:UDC


Bauspiess:1990:HKA


Blakley:1994:LAA


Brooks:1994:ST

Thomas A. Brooks and Michael M. Kaplan. Security technologies. AT&T
REFERENCES

Biham:1995:KPA


Biham:1998:CAXa


Biham:1998:CAXb


Biham:1997:C


Blakley:1995:GPS


Blum:1995:DPC


Bocharova:1995:FEC

REFERENCES

Biham:1998:TA


Biryukov:1998:DCC


Biryukov:1998:ICR


Buchholz:1998:TCF


Buhler:1998:LBR


Buchholz:1998:OGO


Brown:1993:IRD

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

Bellare:1994:SCB [BKR94]

Borst:1997:TAR [BKR97]

Bellare:1998:LBI [BKR98a]

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

Bellare:1998:LRB [BKR98b]

Bakhmurov:1999:DEE [BKS99]

Burgett:1998:CLD [BKZ98]
S. Burgett, E. Koch, and J. Zhao. Copyright labeling of digitized image data. IEEE Communications Magazine, 36(3):94–100, March
REFERENCES


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


REFERENCES


REFERENCES

Barber:1999:AOD

Buldas:1998:TBL

Beth:1994:CCB

[BLH99]

Brassil:1994:EMI

Brassil:1995:HID
J. Brassil, S. Low, N. F. Maxemchuk, and L. O’Garman. Hiding information in doc-


REFERENCES


REFERENCES


Bayer:1976:EST


Blum:1982:HGC


Boyer:1984:PCR


Blakley:1985:SRS

REFERENCES

sored by the International Association for Cryptologic Research.

Beale:1989:EUR


Bellare:1990:NIO


Bellare:1992:HSG


Bellobin:1991:LKA


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

Brickell:1991:IID


Bellare:1992:HSG


Bleichenbacher:1994:DAG

REFERENCES


REFERENCES

Bellare:1999:FDS


Bellare:1999:FSD


Bento:1995:RCI


Beimel:1999:ANN


Beimel:1999:ANT


Bhowmick:1999:WWD

Blackburn:1997:CNP


Blackburn:1997:CTA


Blackburn:1994:WPK


Blundo:1996:TOB


**Bubak:1999:DHP**


**Biehl:1996:CPB**


**Barker:1998:TKL**


**Blake:1985:CLG**


**Boppana:1996:BCP**


**Busch:1999:GEI**

Christoph Busch, Klara Nahrstedt, and Ioannis

**Book:1985:SNP**


**Book:1985:SNS**


**Book:1985:CRE**


**Book:1985:VTA**


**Book:1985:CSR**


**Brickell:1992:CSR**

REFERENCES


REFERENCES


Ben-Or:1988:CTN


Bolignano:1997:TMC


Bolignano:1998:IPB


Bolignano:1998:IPM


Bond:1947:FSC


Boneh:1998:DDP


Boneh:1998:DDH
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[BP95b] Antoon Bosselaers and Bart Preneel, editors. *Integrity primitives for secure information systems: final RIPE report of RACE Integrity Primitives Evaluation (R1040)*, volume 1007 of *Lecture Notes in Com-
REFERENCES


REFERENCES


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

**Beutelspacher:1991:EFS**


**Bellare:1994:EAK**


**Bellare:1995:PSS**

REFERENCES

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

Baldwin:1996:RRR


Bellare:1996:TCA


Bellare:1996:ESD


Bella:1997:FAK


Bellare:1997:MUR


Bellare:1999:CVC


Bellare:1999:CVI

REFERENCES


REFERENCES


REFERENCES


REFERENCES

[Bre99]

[Bri85]

[Bri86]

[Bri88]

[Bri90a]

[Bri90b]
Ernest F. Brickell. A survey of hardware implementations of RSA (invited),
REFERENCES


Brickell:1992:ACC


Brickell:1993:ACC


Brown:1975:BL


Brownell:1981:ODN

George A. Brownell, chairman.

Brooke:1986:BRB


Browne:1994:ECL


Brock:1996:CCP


Brown:1997:JBC


Benedikt:1999:DLD


Bruyere:1991:MCB


Brundrett:1998:KAW

REFERENCES


[Beth:1991:NSE]


[Biham:1991:DCFb]


[Biham:1991:DCFa]


[Biham:1991:DCS]


REFERENCES


D. Boneh and J. Shaw. Collusion-secure fingerprint-

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

Bose:1995:ATV


Bruckstein:1995:SSD


Brunnstein:1995:IPR


Biham:1997:DFA


Bramhill:1997:CCD

REFERENCES

[Baaleh:1999:AGA]

[Bakhtiari:1995:APL]

[Bakhtiari:1996:PAK]
REFERENCES

219


[Bakhtiari:1996:PBA]

[Bakhtiari:1997:MAC]


[BT94]

[Blake:1999:ECC]


[BT97]

[Benaloh:1994:RFS]

[Bateman:1989:NMC]

[BSW89] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr. The new Mersenne conjecture. *American Mathematical Monthly*, 96(2):125–128, February 1989. CODEN AMMYAE. ISSN 0002-9890 (print), 1300-0972 (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 = 2k ± 1 or p = 4k ± 3. (b) $M_p(= 2^p - 1)$ is prime. (c) $2^p + 1)/3$ is prime.

[BT:1997:BEC]

[BT:1997:BEC]

REFERENCES

labs.bt.com/projects/security/crackers/p-97.txt. [Buc91b]

Barmawi:1998:AEK


Boney:1996:DWA


Buchmann:1991:NTA


Buck:1991:MCT


Budge:1922:RS


Budge:1929:RSB


Budge:1976:RSB

Sir E. A. Wallis (Ernest Alfred Wallis) Budge. The Rosetta stone in the British Museum: the Greek, demotic, and hieroglyphic
texts of the decree inscribed
on the Rosetta stone con-
ferring additional honours
on Ptolemy V Epiphanes
(203-181 B.C.) with English
translations and a short his-
tory of the decipherment
of the Egyptian hieroglyphs,
and an appendix contain-
ing translations of the ste-
lae of San (Tanis) and Tall
al-Maskhutah. AMS Press,
ISBN 0-404-11362-1. 325 +
22 pp. LCCN PJ1531.R5 B8
1976.

Burchard:1981:NNF
Hank Burchard. News
and notices: Finerman and
Lee Receive ACM Awards;
summer positions at Dig-
tal Computer Museum;
CBI Fellowship 1982–1983;
GMD activities in the his-
tory of computing; re-
quest for articles; Edwards
speaks at Digital Com-
puter Museum; exhibit of
cipher machines. Annals
of the History of Compu-
ting, 3(4):410–413, Octo-
ber/December 1981. CO-
DEN AHCOE5. ISSN 0164-
1239. URL http://dlib.
computer.org/an/books/
an1981/pdf/a4410.pdf.

Burton:1984:RPKb
Charles E. Burton. RSA:
a public key cryptography
system part II. Dr. Dobb’s
Journal of Software Tools, 9
(4):32–??, April 1984. CO-
DEN DDJOEB. ISSN 1044-
789X.

Burton:1984:RPKb
Charles E. Burton. An
enhanced ADFGVX cipher
system. Dr. Dobb’s Journal
of Software Tools, 10(2):48–
??, February 1985. CODEN
DDJOEB. ISSN 1044-789X.

Burden:1994:CCK
M. Burmester. Cryptanaly-
sis of the Chang-Wu-Chen
key distribution system. Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Burden:1994:CCW
Mike V. D. Burmester. Cryptanalysis of the Chang-
Wu-Chen key distribution
system. Lecture Notes in Computer
Science, 765:
440–??, 1994. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http:///
lk.springer-ny.com/
link/service/series/0558/4
bibs/0765/07650440.htm;
REFERENCES


Burmester:1994:ROD


Burmester:1996:HSS


Burke:1998:IHC


Burke:1998:LER


Burke:1999:AAC


Busse:1996:UFE

REFERENCES


[Boneh98:BRM] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may not be equivalent to factoring (extended


**Blake-Wilson:1999:ADH**


**Blake-Wilson:1999:UKS**


**Buchholz:1988:CQDc**


**Boyd:1992:RDE**


**Bellare:1993:CCT**


**Beller:1993:BDK**

REFERENCES

[BY93c] Michael J. Beller and Ya-
cov Yacobi. Batch Diffie–
Hellman key agreement sys-
tems and their applica-
tion to portable commu-
nications. Lecture Notes
in Computer Science, 658:
208–??, 1993. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer-ny.com/
l ink/service/series/0558/
0658/papers/06580208.
pdf.

[CA81] Computer and Business
Equipment Manufacturers
Association and American
National Standards Insti-
tute. American National
Standard Data Encryption
Algorithm. American Na-
tional Standards Institute,
1430 Broadway, New York,
NY 10018, USA, December
30, 1981. 16 pp. LCCN ????
ANSI X3.92-1981.

[CA83a] Computer and Business
Equipment Manufacturers
Association and American
National Standards Insti-
tute. American National
Standard for Information
Systems: Data Encryption
Algorithm — modes of op-
eration. ???? ANSI X3.106-
1983, American National
Standards Institute, 1430
Broadway, New York, NY
10018, USA, May 16, 1983.
16 pp.

[CA83b] Computer and Business
Equipment Manufacturers
Association and American
National Standards Insti-
tute. American National
Standard for Information
Systems: Data link encryp-
tion. ???? ANSI X3.105-
1983, American National
Standards Institute, 1430
Broadway, New York, NY
10018, USA, May 16, 1983.
20 pp.

[Cac95a] C. Cachin. On-line secret
sharing. Lecture Notes in
Computer Science, 1025:
190–??, 1995. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Cac95b] C. Cachin. On-line secret
sharing. Lecture Notes in
Computer Science, 1025:
190–??, 1995. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic).

[Cac98] Christian Cachin. An
information-theoretic model

Cypher:1996:UAS


Cai96


Cai96

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

Cai96


Cai96


Cai96


**Campaigne:1971:REC**


**Campbell:1987:MBC**


**Cammack:1988:MDE**


**Cao:1999:CAR**


**Capecchi:1994:TGR**


**Carlet:1993:PBF**


**Carlsen:1994:OPA**


**Caronni:1995:AOR**

Germano Caronni. Assuring ownership rights for digital

Carter:1996:BAP


Carr:1997:WDA


Carter:1997:BLC


Carter:1997:CCC


Carter:1999:CCC

Frank Carter. Codebreaking with the Colossus computer: an introduction to the techniques used, together with their mathematical basis. Technical report, Bletchley Park Trust, Bletchley Park, UK, 1998. 24 pp. [Car99]

Carasik:1999:USS


Caswell:1995:EDA


Chren:1996:RDU

W. A. Chren, Jr. and C. H. Brogdon. RSA decryption using the one-hot
residue number system. In IEEE 39th Midwest symposium on Circuits and Systems, 1996, volume 1, pages 551–554. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. CODEN ???. ISSN ????

Clark:1981:ECC

Chen:1995:SIB

Canteaut:1998:NAF

Cai:1999:LBPa

Cai:1999:LBPb

Chun:1999:DMT

Chaum:1988:MUS

**Canteaut:1999:NCA**


**Chen:1998:VIC**


**Carter:1995:DVD**


**Carlet:1998:CBF**


**Coppersmith:1985:AF**


**Chuang:1991:MER**


**Cramer:1995:SSS**

REFERENCES

Cramer:1996:NGS

Chapman:1997:HHS

Clark:1998:OHA

Cramer:1998:ZPF

Curtin:1998:BFS

Compton:1999:PTC

Cramer:1999:EMC
Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. Efficient multiparty computations secure against an


Canetti:1997:DE


Chen:1995:PDP


Cramer:1994:PPK


Chaum:1986:CRN


Certicom:1997:EC


Chaum:1987:DPD

REFERENCES


Jean-Yves Chouinard, Paul Fortier, and T. Aaron Gulliver, editors. Information theory and applications II: 4th Canadian workshop, Lac Delage, Quebec, Canada, May 28–30, 1995: selected papers, volume 1133 of Lecture Notes in Computer Science. Springer-Ver-
REFERENCES


REFERENCES


[Chor85] Benny Chor and Oded Goldreich. RSA/Rabin least significant bits are $\frac{1}{2} + \frac{1}{polylog N}$ secure (extended abstract). In Blakley and Chaum [BC85], pages 303–313. CODEN LNCS9. ISBN 0-387-15658-5; 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25

Cover:1987:OPC


Chor:1988:UBS


Catalano:1998:NES


Canetti:1999:ETP


Cranor:2005:SUD

REFERENCES

xvii + 714 pp. LCCN QA76.9.A25; QA76.9.A25
S3533 2005; QA76.9.A25
S43 2005eb; QA76.9.A25
S43 2005. US$44.95, CDN$62.95, UK£31.95.
URL http://www.oreilly.com/catalog/securityusability/

Clark:1993:EMS


[CGM97a]

Canetti:1999:AST


[CGMA85]

Chen:1997:KEM


[CGM97b]

Chen:1997:AUM


[CGM96]

Chor:1985:VSS

Chen:1997:SSR


Cramer:1997:SOE


Capocelli:1994:FAU


Canetti:1994:MSP


Clark:1994:BSP


Cai:1996:PEA

REFERENCES


Carrel:1997:RIO


Chang:1997:SAG


Chen:1998:PFR


Corcoran:1999:SCB


Cordon:1999:AMD


Chaum:1979:UEM


Chaum:1981:UEM

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the Association for

Chandler:1983:IMC


Chanda:1985:NSC


Chaum:1985:HKS


Chaud:1985:NSC

REFERENCES

Chaum:1985:SIT

Chang:1986:DKL

Chapman:1986:NFS

Chaum:1990:SDA

Chaum:1991:SCS

Chaum:1992:AEPa

Chaum:1992:AEPb
REFERENCES

tific American, 267(2):96–?? (Intl. ed. 76–81), August 1992. CODEN SCA-
MAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Chaum:1993:NCB


Chambers:1994:TSC


Chandler:1994:IAF


Chabaud:1995:SSC


Chaum:1995:DCS


Chadwick:1999:IWS

REFERENCES


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


[Chi99b] Shiu-Kai Chin. High-confidence design for security: don’t trust — verify. Communications of
Christophides:1999:ODI


Canetti:1997:PSL


Chor:1986:TIP


Chung:1998:DWCb


Christianson:1998:SP1


Christianson:1999:DSCb

REFERENCES


REFERENCES


low.density.tex.


References


[CK95] P. A. R. Cole and M. S.


REFERENCES


REFERENCES

*Scientific American*, 107 (17):346, October 26, 1912.
CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).


REFERENCES

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

Clevenger:1996:DEU

Chang:1998:SOM

Clinton:1997:AEC
[ Cli97] Bill Clinton. Administration of export controls on encryption products: communication from the President of the United States transmitting revisions to the provisions that apply to the Department of Commerce in the Export Administration regulations, 15 CFR part 730 et seq. — received in the United States House of Representatives November 15, 1996, pursuant to 50 U.S.C. 1703(b). Washington, DC, USA, January 7, 1997. 5 pp. Referred to the Committee on International Relations. Shipping list no.: 97-0126-P.

Clinton:1999:LPM
[ Cli99] Bill Clinton. A legislative proposal: message from the President of the United States transmitting a legislative proposal to protect the privacy, security and safety of the people of the United States through support for the widespread use of encryption, protection of the security of cryptographic keys, and facilitation of access to the plaintext of data for legitimate law enforcement purposes. United States Government Printing Office, Washington, DC, USA, September 21, 1999. 40 pp. Referred to the Committee on the Judiciary and Government Reform. Shipping list no.: 2000-0018-P.

Chua:1999:ART
[ CLL99] Seng Kiat Chua, Ka Hin Leung, and San Ling. Attack on RSA-type cryptosystems based on singular cubic curves over \( \mathbb{Z}/n\mathbb{Z} \). Theoretical Computer Science, 226(1–2):19–27, September 17, 1999. CODEN TC-

Cheng:1998:MVR


Culik:1979:SIS


Ciampi:1982:EVS


Chan:1985:NMP


Cachin:1995:LIR


Cachin:1997:USA

REFERENCES


Chang:1997:CAS

Cooperman:1997:SMD

Cox:1997:RWI


Camenisch:1999:SEG

Charlton:1999:DPM

Christianson:1999:DSCa
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 simulation system. Lecture Notes in Computer Science, 1604:120--??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1998:SCC
enryption/aes/round1/ 
conf1/saferpls-slides. 
pdf. Only the slides for the conference talk are available.

Cohen:1993:AAA
G. Cohen, Teo Mora, and Oscar Moreno, editors. Applied algebra, 
algebraic algorithms, and error-correcting codes: 10th 
International Symposium, 
AAECC-10, San Juan de 
Puerto Rico, Puerto Rico, 
May 10–14, 1993: proceedings, volume 673 of Lecture Notes in Computer Science. Springer-Verlag, 
Berlin, Germany / Heidelberg, Germany / London, 
UK / etc., 1993. CODEN LNCSD9. ISBN 3-
540-56686-4 (Berlin), 0-387-
ny.com/link/service/series/ 
0558/tocs/t0673.htm; 
issue&issn=0302-9743& 
volume=673.

Canetti:1999:ECS
/link.springer-ny.com/ 
l/service/series/0558/ 
bibs/1592/15920459.htm; 
http://link.springer- 
ny.com/link/service/series/ 
0558/papers/1592/15920459. 
pdf.
REFERENCES


[Coron:1999:SRSb] Jean-Sébastien Coron and David Naccache. On the

**Coron:1999:SRP**


**Coupe:1999:ELA**


**Chao:1998:CSE**


**Coltell:1998:AOL**


**Cocks:1997:SKG**

REFERENCES


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


REFERENCES


REFERENCES


REFERENCES

Coppersmith:1998:C


Coppersmith:1999:WQS


Corcoran:1998:MFS


Coron:1999:SRSa


Coppersmith:1986:DL


Courville:1986:MCC


Courington:1993:PEA


Coutinho:1999:MCN

S. C. Coutinho. The mathematics of ciphers: number
REFERENCES


REFERENCES

1611-3349 (electronic).

Chae:1994:AMA


Chen:1995:NGS


Chaum:1998:E


Chung:1998:DWCa


CODEN DTPEEL. ISBN ???? ISSN 0747-668X. LCCN ???? IEEE catalog number 98CH36160.

Charney:1997:PSC


Cheon:1998:TEA


Camenisch:1995:BSB


Chor:1985:KTP

[Berry Chor and Ronald L. Rivest. A knapsack type


[CR96] Richard Craig. Considerations of data compression and symmetric encryption techniques for a personal communications ser-
vice. Thesis (M.S.), University of Mississippi, Oxford, MS, USA, 1996. various pp. [Cré96]


REFERENCES


Chaum:1998:Ca


Crypto:1981:ACP


CryptoBytes:1995:C


Cesarini:1983:ACC


Chepyzhov:1991:FCA


Chabaud:1996:CSS

REFERENCES

Chambers:1996:RLM


Chambers:1997:RLM


Cusick:1996:BNFb


Cusick:1997:BNFb


Camenisch:1997:EGS


Camenisch:1997:EGS


Camenisch:1997:EGS


Cantenaut:1998:COM

Anne Canteaut and Nicolas Sendrier. Cryptanalysis of the original McEliece cryptosystem. Lecture Notes
Cramer:1998:PPK

Coradeschi:1999:ASV

Chaum:1989:SCF

Csirmaz:1995:SSM

Coppersmith:1994:ABP

Chang:1997:GSS

Chen:1999:TPS
Z.-G. Chen and S. E. Tavares. Toward provable security of substitution-permutation encryption

**Collberg:1999:SWM**


**Cox:19xx:NST**


**Chao:1994:DEC**


**Currier:1998:MPT**


**Cusick:1995:CPK**


**Cusick:1996:BNFa**

REFERENCES

1872-6119 (electronic). See comment [YT96].


[Cha91b] Chin-Chen Chang and Tzong-Chen Wu. Broadcasting cryptosystem in computer networks using


Chang:1997:SCO


[CWM+91] Paul Ceruzzi, Eric A. Weiss, John Walker Mauer, Thomas Drucker, Peggy Aldrich Kidwell, and K. W. Smilie. Reviews: Grosch: Computer: Bit slices from a life; Tomayko: Computers in spaceflight: The NASA Experience; Bülow: Denk, Maschine! Geschichten über Röbort, computer und Kunsthliche Inteligenz; Napier: Rabdology; Charlesworth: Calcu-

[CWSK98]


[CY98]


[CY98]


[CY98]


Damgaard:1990:ACE


Damgaard:1990:DPH


Damgaard:1991:ACE


Damgaard:1991:TPP


Damgaard:1994:PPS

REFERENCES


A. Danthine, editor. European Conference on Mul-
REFERENCES


Dang:1997:AAC


Darnell:1997:CCI


Davida:1981:CAR

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

Davies:1985:MAA

August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


REFERENCES


[DB89] Dorothy Elizabeth Robling Denning and William E. Baugh, Jr. Encryption and evolving technologies: tools of organized crime and
REFERENCES


denBoer:1991:ALT  [DB91]
http://link.springer-ny.com/link/service/series/0558/tocs/t0576.htm;

Denning:1996:TKE  [DB96]

Daswani:1999:EEC  [DB99]

Boer:1994:CCF  [dBB91]
http://link.springer-
REFERENCES


REFERENCES


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.

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

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

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

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

**DDJStaff:1998:NVd**


**DDJStaff:1999:NVR**


**DePaoli:1998:WBS**


**Denny:1994:FR**


**Delaigle:1996:DW**

REFERENCES


[DPP90] [DDP90]

Davida:1990:KDS

George I. Davida, Yvo Desmedt, and René Perlita. A key distribution system based on any one-way function (extended abstract). *Lecture Notes in Computer Science*, 434: 75–??, 1990. CODEN LNCS90. ISSN 0302-9743

Delsarte:1985:FCM

(print), 1611-3349 (electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibbs/0434/04340075.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340075.

DeSantis:1994:SSP
Alfredo De Santis, Giovanni 
Di Crescenzo, and Giuseppe 
Persiano. Secret sharing 
and perfect zero-knowledge. 
Lecture Notes in Computer 
CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic).

DeSantis:1994:KCQ
[DDP94a] Alfredo De Santis, Giovanni 
Di Crescenzo, and Giuseppe Persiano. 
Secret sharing and perfect 
zero-knowledge. Lecture Notes in 
CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http://
link.springer-ny.com/
link/service/series/0558/
bibbs/0434/04340075.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340075.

DeSantis:1999:NIZ
[DDP99] A. De Santis, G. Di 
Crescenzo, and G. Persiano. 
Non-interactive 
zero-knowledge: a low-
randomness characterization 
of NP (extended abstract). 
Lecture Notes in 
Computer Science, 1644: 
271–??, 1999. CODEN 
LNCSD9. ISSN 0302-9743 
(print), 1611-3349 (electronic).

Darmstaedter:1998:LCS
[DDQM98] V. Darmstaedter, J.-F. Delaigle, 
J. J. Quisquater, and B. Macq. Low 
cost spatial watermarking. 
Computers and Graphics, 22(4):417–424, 
August 1, 1998. CODEN 
COGRD2. ISSN 0097-8493 
elsevier.com/cas/tree/
store/cag/sub/1998/22/ 

DeVries:1953:SMC
M. de Vries. Statistical 
methods in cryptanalysis. 
Rapport ZW 1953-
014. Math. Centrum 
Amsterdam, Amsterdam, 
The Netherlands, 1953. 15 pp.

DeAlvare:1990:HCC
Ana Maria De Alvare. How crack- 
ers crack passwords.
In USENIX Association [USE90], pages 103–112. LCCN QA 76.9 A25 U55 1990.


B. De Smit. Generating arithmetically equivalent number fields with elliptic curves. Lecture Notes


DENNING:1995:ESC

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

DENNING:1999:IWS


DESWARTE:1992:CSE


DESmedt:1990:PAA


DESmedt:1990:MCS

REFERENCES

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

**Desmedt:1992:BTC**


**Desmedt:1993:TC**


**Desmedt:1994:TC**


**Desmedt:1994:ACC**


**Desmedt:1995:STC**


**Desmedt:1996:EBB**

[Des96a] Y. Desmedt. Establishing Big Brother using covert channels and other covert techniques. In Anderson [And96c],


Desmedt:1990:TC


Desmedt:1991:SGA


Domingo-Ferrer:1991:DUI


Domingo-Ferrer:1991:SRT


Dawid:1992:BSC

References

7803-0609-0 (casebound), 0-7803-0610-4 (microfiche).

Desmedt:1993:PZS

Domingo-Ferrer:1997:MAS

Domingo-Ferrer:1998:AFE

Domingo-Ferrer:1999:AFB

Deshpande:1999:VEM

Domingo-Ferrer:1991:CTP
REFERENCES


**Dawson:1996:CPA**


**Dawson:1996:CPA**

[DG96]


**Daemen:1992:HDM**


**Daemen:1993:FDO**


**Daemen:1994:NAB**


**Daemen:1994:RWS**

REFERENCES

[Daemen:1994:WKI]

[Diffie:1976:NDC]

[Diffie:1977:ECN]

[Davis:1985:NRI]

[Davis:1985:UFS]

[DomingoFerrer:1990:FSK]
REFERENCES

Dawson:1996:AAS

Ding:1996:WKA

Dhem:1998:DEP

Diffie:1980:CAM

Dechamboux:1996:ADS

Desmedt:1998:AOC

Desmedt:1998:CC

Dolev:1995:DFT


REFERENCES


REFERENCES


**Damgaard:1994:BAH**


**Damgaard:1996:MEM**


**Deavours:1998:SCH**


**Desmedt:1998:CES**


**Deavours:1987:CYT**


**Daemen:1997:BCSb**

J. Daemen, L. Knudsen, and V. Rijmen. The block


REFERENCES

Davoine:1997:VCP


DeMillo:1982:CP


Damgaard:1993:ACE


Ding:1997:LMS


delaStelle:1902:TCF


DeMillo:1983:PDS


Duc:1997:PAF


DeWin:1998:PSS

[DMPW98] E. De Win, S. Mister, B. Preenel, and M. Wiener. On the performance of signature schemes based on el-
REFERENCES


DAngelo:1994:SEM


Dongarra:1995:TSS


Dwork:1994:EEU


Dossis:1995:FSR


Dossis:1995:OVH


Ding:1997:TFS


Dittmann:1998:IWE


Desmedt:1986:CTA


DiCrescenzo:1999:CZK


Dobbertin:1995:EMC

References


Donini:1998:CSR


DiCrescenzo:1999:COTb


Santis:1991:PRP


DiCrescenzo:1994:ROP


Damgaard:1996:NCU


Davida:1998:HC


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

Peter de Rooij. On
Schnorr’s preprocessing for
digital signature schemes.
*Lecture Notes in Computer
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer-
y.com/link/service/series/0558/bibs/0765/07650435.htm;
http://link.springer-

Peter de Rooij. Efficient ex-
ponentiation using precom-
putation and vector addi-
tion chains. *Lecture Notes
in Computer Science*, 950:
389–399, 1995. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL
http://link.springer-
y.com/link/service/series/0558/bibs/0950/09500389.htm;
http://link.springer-

J. Daemen and V. Rijmen.
AES proposal: Rijndael.
NIST AES Proposal, June
1998.
REFERENCES

**Desel:1998:PTP**


**Daemen:1999:EBC**


**Drea:1999:NEB**


**Dray:1998:RNJ**


**Drach:1999:RDO**


**Dreher:1979:PSC**


**Drea:1992:MUC**


Desmedt:1993:PPS


Davern:1996:FBI


Devanbu:1997:CVT


Dittmann:1997:TAT


Dittertre:1997:UPE


David:1998:SIC

REFERENCES

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

Dwork:1998:CZR


Durham:1999:BOO


Dittmann:1998:RMV


Dave:1995:CBS


Desai:1999:CSC


Durand:1999:DCC


Detombe:1993:CLC


**DeSolages:1998:EFO**


**DiGiorgio:1998:JDS**


**DuBoulay:1999-DDT**


**duCarlet:1644:CCV**


**Dufner:1998:ACH**


**Duhoux:1990:DBA**

Dumey:1994:CQD


DeVivo:1998:ISA


DeDecker:1992:HID


Dhem:1996:SSC


DeSoete:1990:CAS


Diffie:1992:AAK


DiPorto:1994:VBC

REFERENCES

Dwork:1995:DCC

Dwork:1997:PAL

Dwork:1991:VSS

Danielsson:1998:HKW

Davida:1981:DES

Dwork:1997:PAL

Dwork:1991:VSS

DeWaleffe:1991:CSC

Waleffe:1991:CSC
Dominique de Waleffe and Jean-Jacques Quisquater.
REFERENCES


Dai:1996:CFA


Ding:1991:STS


DeSantis:1990:DPS


DeSantis:1991:CAN


DeSantis:1991:DPSb


H. Eberle. A high-speed DES implementation for network applications. *Lect-

[Eck85]


[ECM96]


[ECW75]

the 100th IEEE Milestone Award for the first discovery (albeit long secret) of public-key cryptography.


Even:1996:LLD


English:1996:NSU


Ellison:1999:PSK


Ergun:1999:NLC


Estrella:1999:DED


Eigenthaler:1984:CGA

REFERENCES


Evans:1974:UAS


EFF:1998:CSE


ElGamal:1985:PKCa


ElGamal:1985:PKCb

REFERENCES

Gust 19–22, 1984, sponsored by the International Association for Cryptologic Research.


REFERENCES


REFERENCES

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


[Est80] Robert G. Estell. Bench-
marks and watermarks. ACM SIGMETRICS Per-
formance Evaluation Re-
CODEN ???? ISSN
0163-5999 (print), 1557-
9484 (electronic).

[Estell:1980:BW]

[Ev92] Jan-Hendrik Evertse and
Eugène van Heyst. Which
new RSA-signatures can be
computed from certain
given RSA-signatures? 
Journal of Cryptology, 5(1):
41–52, 1992. CODEN
JOCREQ. ISSN 0933-2790
(print), 1432-1378 (elec-
tronic).

[Even:1985:CSW]

[Eve85] Shimon Even. On the
complexity of some word
problems that arise in test-
ing the security of proto-
cols. In Apostolico and
Galil [AG85], pages 299–

[Ev93] Jan-Hendrik Evertse and
Eugène van Heyst. Which
new RSA-signatures can be
computed from RSA signa-
tures, obtained in a specific
interactive protocol? 
Lecture Notes in Com-
puter Science, 658:378–88, 
1993. CODEN
LNCSD9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/0658/06580378.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0658/06580378.

[Even:1993:WNR]

[Ett98] J. Mark Ettinger. Ste-
ganalysis and game equi-
libria. Lecture Notes in
Computer Science, 1525:
319–328, 1998. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
link/service/series/0558/
bibs/1525/15250319.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1525/15250319.

[Ettinger:1998:SGE]

Falk:1988:DST  

Fancher:1996:SCa  

Farago:1967:BSS  

Farago:1969:BSS  

Farrow:1992:HIY  

Farrell:1993:CCC  

Ford:1997:SEC  

Fox:1997:GGU  
B. Fox, B. Beckman, and D. Simon. *GUMP: Grand unified meta-protocols recipes* for simple, standards-based financial cryptography. Lec-
REFERENCES

...ture Notes in Computer Science, 1318:375–??, 1997. CODEN LNCS.D9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES

Frankel:1992:PRT


Frankel:1993:NEH


Frankel:1993:NHG


Feak:1983:SIS


Feistel:1973:CCP


Feigenbaum:1991:ACC


Feit:1993:TIA

[Fei93] Sidnie Feit. TCP/IP: Archi-
REFERENCES


Ferguson:1999:IDT


Fernandes:1999:ECC


Feynman:1982:SPC


Friedman:1957:SCE


Friedman:1955:CLS


Feghhi:1999:DCA


Fung:1998:PAE


REFERENCES


REFERENCES


Filby:1978:BRM


Filby:1995:FUB


FIPS:1993:APG


FIPS:1993:SHS


FIPS:1994:EES


Fischlin:1997:ICM


Fischlin:1998:CLP


Franz:1998:MMA

克斯特:1996:CBS


Franc:1996:CBS


Frederrath:1996:MNC


Federrath:1996:MNC

REFERENCES

Fellows:1994:CCG


Franke:1999:SDM


Freier:1996:SPV


Frankel:1998:BIW


Fumy:1993:PCK


Fried:1996:BHA

proceedings/ec96/index.html.

Fiadeiro:1999:ASC


Fox:1999:OCS


Flowers:1983:DC


Feiertag:1977:PMS


Flynn:1997:WYN


Friedman:1976:ZTJ


Fortune:1985:PP

REFERENCES

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

Feigenbaum:1991:DCC


Faihe:1998:ADR


Fagundes:1999:EGA

L. G. Fagundes, R. F. Mello, and C. E. Mdron. An en-

Feustel:1998:DUI


Fairfield:1985:LRN


**Fairfield:1985:LDE**


**Frey:1999:TPD**


**Frankel:1998:RED**


**Fiat:1994:BE**


**Fiat:1992:NH**

Amos Fiat, Moni Naor, Jeanette P. Schmidt, and


papers/1666/16660537.pdf.


REFERENCES


REFERENCES

Franklin:1985:MID


Frankalsen:1985:MBS


Frankalsen:1986:SHM


Frankel:1989:TIC


Frankel:1990:PPL


Francis:1992:PSG


Frankalsen:1993:BCM


Franklin:1999:FCT

REFERENCES


[Fri56] Friedman:1956:CCC

[Fri63] Friedman:1963:SLC

[Fri76a] Friedman:1976:AMC

[Fri76b] Friedman:1976:CEC

[Fri76c] Friedman:1976:CCA
William F. (William Frederick) Friedman. *Cryptography and cryptanalysis arti-

[Fri76d] Friedman:1976:EC

[Fri76e] Friedman:1976:EMC

[Fri87] Friedman:1987:ICA

[Fri92a] Friedman:1992:MC
William F. (William Frederick) Friedman. *Military
REFERENCES

Friedman:1992:MCP

Friedmann:1993:TDC

Friedman:1996:SLC

Froomkin:1996:ICP

Froomkin:1997:DST

Fiat:1987:HPY
REFERENCES


Mark Frankel and Al Teich. Special issue devoted
REFERENCES


REFERENCES

Funk:1978:DUS


Funny:1993:KM


Futrelle:1973:BTM


Feldman:1999:HSH


Fischer:1991:MSK


Frankel:1995:CIL


Frankel:1995:EES

[FY95b] Yair Frankel and Moti Yung. Escrow encryption systems visited: Attacks,
REFERENCES


Franklin:1995:BWS


Franklin:1997:CEE


Frankel:1998:DPK


Frankel:1998:RMU


Frankel:1999:CRA


Frankel:1999:ASD


REFERENCES


Gaines:1943:ECS


Gaines:1944:CSC


Gaines:1956:CSC


Gait:1977:VCH


Gait:1978:EEP


Gait:1980:CST


Gait:1980:MTD


Gait:1980:VCH


Gait:1990:VCH

Jason Gait. *Validating the correctness of hardware implementations of the*
REFERENCES


Gaj:1989:GCM


Galland:1945:HABa


Galland:1945:HABb


Galil:1988:SIC


Galvin:1996:PKD

Galbraith:1999:CIB


Gamble:1988:IDL


Ganley:1993:CCI


Ganesan:1996:HUK


Ganesan:1996:YSS


Gardner:1977:MGN

REFERENCES


[Gar97a] Lee Garber. News briefs: Agency: Net use hasn’t hurt US phone system; Apple unveils turnaround strat-
egend; JTC rejects Java standards plan; vendors plan 300-nm wafers; battle brews over smart card encryption; countries lift Internet telephone ban; Motorola proposes satellite system; vendors agree on high-capacity disks; “wrapping” software sales; Tonga offers domain name alternative. *Computer*, 30(9):19–22, September 1997. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://neumann.computer.org/co/books/co1997/pdf/r9019.pdf.


**Garber:1998:NBM** [Gar98a] Lee Garber. News briefs; moving 3D beyond VRML; US, Microsoft will square off on September 8; satellite processor failure cuts net, pager service; US seeks encryption standard; vendors unveil Bluetooth wireless technology; the end of MS-DOS. *Computer*, 31(7):18–21, July 1998. CO-
REFERENCES


Garber:1998:NBS


Garfinkel:1998:PPG


Gaudin:1997:VBJ

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

Gilmour-Bryson:1982:CDT

A. Gilmour-Bryson. Coding of the depositions of the Templars. In Ciampi and Martino [CM82], pages 451–467. ISBN 0-444-86413-X (set), 0-444-86414-8 (vol. 1), 0-444-86415-6 (vol. 2). LCCN K662.14 I58. From Computing Reviews: “The article reports on the progress of an historical study using a computer for statistical analysis. The subject of the study is a mass of trial depositions of the Knights Templar. The purpose of the project is to find statistical regularities in the large amount of testimony and to create a model for similar studies. The Order of the Knights Templar, founded around 1100, was the first Christian military order. After the Crusades, in the early fourteenth century, 127 articles of accusation were brought against the order, including charges of idolatry, sacrilege, and sodomy. The data being studied are the responses of 900 men to each of 127 accusations. The article details the accusations and the way in which the responses are being coded. The statistical package SAS (Statistical Analysis System) will be used. Examples of the re-
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.


Henry Gilbert and Guy Chassé. A statistical attack of the FEAL-8 cryptosystem. Lecture Notes


[GD+97] F. Goffin, J. F. Delaigle, C. De Vleeschouwer,
REFERENCES


the IEEE Communications Society with the cooperation of the Dept. of Electrical and Computer Engineering, University of California, Santa Barbara.” — Verso of t.p. “August 20, 1982.” Includes bibliographies.


REFERENCES

tronic). URL http://
/link.springer-ny.com/
link/service/series/0558/|
bibs/1294/12940112.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/1294/12940112.
.pdf.

Gilbert:1998:DFC  [GGH+98]
H. Gilbert, M. Girault,
P. Hoogvorst, F. Noilhan,
T. Pornin, G. Poupard,
J. Stern, and S. Vaude-
nay. Decorrelated fast ci-
pher: an AES candidate.
In National Institute of
Standards and Technology
[Nat98], page ?? ISBN
???? LCCN ???. URL
http://csrc.nist.gov/
encryption/aes/round1/
conf1/aesconf.htm;
See [RD99a] for a confer-
cence overview. No formal
proceedings were published,
but the conference Web site
contains pointers to slides
and/or technical papers for
most of the fifteen “com-
plete and proper” candi-
dates.

Gabber:1999:SPC  [GGK+99]
Eran Gabber, Phillip B.
Gibbons, David M. Krist-
tol, Yossi Matias, and
Alain Mayer. On secure
and pseudonymous client-
relationships with multiple
servers. ACM Transactions
on Information and Sys-
tem Security, 2(4):390–415,
November 1999. CODEN
ATISBQ. ISSN 1094-9224
(print), 1557-7406 (elec-
acm.org/pubs/citations/
journals/tissec/1999-2-
4/p390-gabber/.

Goldreich:1985:CAR
Oded Goldreich, Shafi
Goldwasser, and Silvio Mi-
cali. On the crypto-
graphic applications of ran-
dom functions (extended
abstract). In Blakley and
Chaum [BC85], pages 276–
288. CODEN LNCS-D9.
ISBN 0-387-15658-5; 3-540-
39568-7. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25
C791 1984; QA267.A1 L43
no.196. URL http://
/www.springerlink.com/
openurl.asp?genre=article&
issn=????&volume=0&issue=
0&spage=276. CRYPTO
84: a Workshop on the
Theory and Application of
Cryptographic Techniques,
held at the University of
California, Santa Barbara,
August 19–22, 1984, spon-
sored by the International
Association for Cryptologic
Research.

Goldreich:1986:HCR
Oded Goldreich, Shafi
Goldwasser, and Silvio Mi-
cali. How to con-
struct random functions.
Journal of the Associa-
tion for Computing Machin-
A computational complexity measure of the randomness of functions is introduced, and, assuming the existence of one-way functions, a pseudo-random function generator is presented.

Gabber:1997:HMP


Gilbert:1998:ASR


Gittler:1995:DSS


Gehrke:1996:MPK


Gong:1999:PKC

Guang Gong and Lein Harn. Public-key cryp-


Gibson:1995:SDG


Gibson:1996:SGP


Gifford:1981:CSI


Gilder:1997:APD


Giles:1998:EFS


Gilboa:1999:TPR


Gingerich:1970:BRB


REFERENCES


Gamage:1999:EMA


Goldwasser:1982:PEH


Goldwasser:1984:PE


Goldwasser:1984:PE


Golic:1991:NCC


[GMCF95] J. Galvin, S. Murphy, S. Crocker, and N. Freed.
/ftp.internic.net/rfc/rfc1847.txt; http://
www.math.utah.edu/pub/rfc/rfc1847.txt. Status:
PROPOSED STANDARD.

Griwodz:1998:PVE

C. Griwodz, O. Merkel, J. Dittmann, and R. Stein-
metz. Protecting VoD the easier way. In Effelsberg
ac.uk/~fapp2/steganography/


bibliography/073127.html. ACM order number 43398.

Ghazi-Moghaddam:1994:OCH

F. Ghazi-Moghaddam, I. Lam-
badaris, and J. F. Hayes. Overflow constraint in hy-
brid nodes with movable boundary scheme. Lecture
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).


Goldwasser:1985:PSS

Shafi Goldwasser, Silvio Mi-
cali, and Ronald L. Rivest. A "paradoxi-
cal" solution to the signature
problem. In Blakley and Chaum [BC85], page
467. CODEN LNCSD9.


Goldwasser:1988:DSS

Shafi Goldwasser, Silvio Mi-
cali, and Ronald L. Rivest. A digital signa-
ture scheme secure against adaptive chosen-message
308, April 1988. CODEN SMJCAT. ISSN 0097-5397
(print), 1095-7111 (elec-
tronic). Special issue on cryptography.


Shafi Goldwasser, Silvio Mi-
cali, and Charles Rackoff. The knowledge complex-
ity of interactive proof systems. SIAM Journal on
SMJCAT. ISSN 0097-5397
(print), 1095-7111 (electronic).

**Good:1945:GRT**


**Groote:1998:CVP**


**Goldreich:1987:HPM**


**Goldreich:1991:PYN**

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the Association for Computing Machinery*, 38(3):691–729, July 1991. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0004-5411/116852.html. They show that for a language $L$ in $NP$ and a string $w$ in $L$, there exists a probabilistic interactive proof that efficiently demonstrates membership of $x$ in $L$ without conveying additional information. Previously, zero-knowledge proofs were known only for some problems that were in both $NP$ and co- $NP$. A preliminary version of this paper appeared in *Proc. 27th Ann. IEEE Symp. On Foundations of Computer Science*, 1986, under the title “Proofs that yield nothing but their validity and a methodology of cryptographic protocol design.”.

**Gemmell:1994:CIA**

Goettfert:1995:GLB


Gray:1995:PCT


Guerrero:1995:CHB


Goldwasser:1993:ISN


Golic:1995:EPC


Goldreich:1996:SPS


Golic:1996:CCC

J. D. Golic and L. O’Connor. A cryptanalysis of clock-controlled shift registers

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


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

Goldwasser:1990:ACC

Goldwasser:1990:SPS

Gollmann:1992:ATC
D. Gollmann. Automata theory and cryptanalysis.


Gollmann:1994:CCC

Goldreich:1995:FCF

Golic:1995:LCS

Golic:1996:FLO


REFERENCES

Golic:1997:CAA

Goldwasser:1998:C

Golic:1998:RAS

Goldreich:1999:MCP

Golic:1999:SCE

Golomb:1999:CNS

Gong:1989:SCB

Gong:1992:SRD
Li Gong. A security risk of depending on synchronized clocks. Operating Systems Review, 26(1):49–53, Jan-
Gong:1995:CKH

Gong:1998:JSM

Good:1979:EWC

Goodman:1996:LPS

Gordon:1985:SPE

Gordon:1993:DDT


REFERENCES


Goldreich:1998:SCP


Ghodosi:1997:RMA


Ghodosi:1998:SSM


Gore:1998:SDC


Gabidulin:1991:INC

E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptography. Lecture Notes in


[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». In Damgård [Dam91a],]
Gennaro:1997:HSD  

Grantham:19xx:FPP  

Goeker:1999:DUC  

Greenfield:1994:DPP  

Grover:1982:CP  
REFERENCES

org/content/25/3/400-c.full.pdf+html.

Grosek:1994:RCR


Grover:1998:FCP


Goldschlag:1996:HRI


Grundler:1984:DEH


Grusho:1998:SCI


Gaines:1978:SSP


Grollmann:1984:CMP


Grollmann:1988:CMP

Joachim Grollmann and Alan L. Selman. Complexity measures for public-


References


REFERENCES


E9641 1988. Sponsored by the International Association for Cryptologic Research.

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

Gao:1998:GPO


Griffiths:1976:AMR


Goldberg:1996:RNB


Gylden:1931:CEI


Goldberg:1999:RDF


Gamow:1958:CAP

[GY58] George Gamow and Martynas Ycas. The cryptographic approach to the problem of protein synthesis. In *Das Universum. Unser Bild vom Weltall. (German) [The Universe. Our picture of the Universe]*, page ???? ????

Wiesbaden, Germany, 1958.

Galil:1987:PEA

Gylden:1933:CCB


Gylden:1936:AMC


Gylden:1938:APV

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

Gysin:1996:OKC


Garzon:1991:CGG


Haller:1994:RIA


Hendessi:1994:SAA


Hollaar:1996:LRD


[Hamxx] V. Hamilton. Personal communication. ???. 19xx.

REFERENCES

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.


Johan Håstad. Solving simultaneous modular equa-


REFERENCES


**Hughes:1999:PFS**


**Hu:1995:YCE**


**Hwang:1995:SSA**


**Hwang:1996:DSS**


**Hwang:1998:EMS**


**Hernandez:1999:DAV**


**Hwang:1996:SAA**

S.-J. Hwang, C.-C. Chang, and W.-P. Yang. Some ac-

**Hwang:1996:AES**


**He:1996:HFR**


**He:1996:NKE**


**He:1992:IKB**


**Huang:1998:FAI**


**Hedberg:1997:FIC**


**Hartung:1998:DWM**

Heidel:1976:JTP

Held:1993:TSD

Held:1998:ARU

Held:1998:LET

Helleseth:1994:ACE

Helleseth:1998:E

Henry:1981:BJB
REFERENCES

Hong:1998:DAS

Herlestam:1978:CRS

Hershey:1981:DLP

Hess:1997:PKC

Hollan:1997:AMP

Hardy:1985:ECC
John M. Hardy, Dorothy W. Fuller, Douglas R. Long, Jane C. Hartin, and Faye Davis. Electronic cryptographic communications equipment specialist (AFSC 30650). Extension Course
REFERENCES

Institute, Air University, ????, 1985. various pp.

Housley:1999:RIX


Hartung:1996:DWR


Handschuh:1997:CCS


Handschuh:1997:CSE


Hartung:1997:CPV


Hartung:1997:WME


Hartung:1997:DWM

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

Hartung:1998:WUA


Hoornaert:1985:EHI


Haddar:1998:ISI


Hall:1998:RAA


Hinsley:1979:BISb

REFERENCES


[H47]

Hofmann:1994:RQC


[HH94]

Hughes:1998:AJC


[HH98]

Husemann:1999:OTY


[HH99]

Hutton:1999:ASM


[HHD99]

Harn:1989:PAU


[HHL89]

Han:1993:TCC


[HHT93]

Han:1997:TCC


[Lester S. Hill. Concerning certain linear transfor-
REFERENCES

Hiltgen:1994:CRC


Hill:1997:MTY


Haastad:1999:PGO


Hinsley:1993:BIS


Hirschfeld:1993:MER


Hirschfeld:1997:FCF

REFERENCES


[HJ97] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public key and signature systems. In ???? [???97], page ??


REFERENCES

[412]

Hillenbrand:1999:SDW


Hong:1997:IAU


Huehnlein:1998:CBN


Huhle:1998:CBN


Harn:1990:EPE


Halevi:1997:MSM

Shai Halevi and Hugo Krawczyk. MMH: Software message authentication in the Gbit/second
Hevia:1998:STD


Halfmann:1999:ESP


Haynes:1999:VDS


Hevia:1999:STD

Hromkovic:1994:CDC


Harpes:1995:GLC


Hachez:1999:IFA


Hall:1999:CS


Haber:1995:HDD


Hofmeister:1997:CKS


Hofmeister:1997:COS


REFERENCES

Hwang:1995:TAN

Hwang:1996:SCW

Hughes:1996:QCU

Hohl:1993:SIH

Hunter:1983:ERA

Hule:1988:RCW

Hafner:1991:COH
past few years. One of the co-authors is the New York Times reporter who broke the Stoll story to the public.

[Hafner:1992:COH]

[Hafner:1995:COH]

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

[Harpes:1997:PC]

[Hoogeboom:1997:CPT]

[Hoyle:1998:SKE]

[Horster:1995:MRM]
P. Horster, M. Michels, and H. Petersen. Meta-message recovery and meta-blind signature schemes based on...

Harkavy:1998:IPP


Harper:1993:PKC


Horvath:1994:PPM


Hennicker:1994:BAF


Haastad:1998:SIR

REFERENCES

puter Society Press order number PR9172.


REFERENCES

Hoogendoorn:1982:SPK


Han:1997:ICS


Horan:1994:CSO


Horng:1995:PAU


Horng:1998:AAP


Horster:1999:SSK


Herzberg:1987:PPS

REFERENCES


Hung:1994:FRD


Handschuh:1998:SCC


Horn:1998:APF


Handschuh:1999:SDK


Heileman:1999:IWC


Hernandez:1998:SML

REFERENCES

Hoffstein:1998:NRB


Holland:1982:GSA


Hwang:1990:PKA


Hollander:1996:KWS


Harrison:1976:POS


Hruby:1995:QDQ

Hruby:1995:QQC


Hruby:1996:SCI


Hruby:1998:TQC


Hruby:1999:SUD


Hernandez:1999:CLM


Haastad:1985:CST


Hammer:1987:EUH

REFERENCES

Hardjono:1989:TCB

Hardjono:1990:SKS

Haber:1991:HTD

Hinsley:1993:CIS

Hardjono:1994:AMS

Handel:1996:HDO

Hardjono:1996:RKA
REFERENCES

Hall:1997:REG


Helme:1997:SFF


Harasawa:1999:CMF


Hornauer:1994:MCA


Hauser:1996:MBI


Hinsley:1979:BISa


Heys:1995:ACS

Hada:1998:EZP


Hada:1999:RBO


Handschar:1999:DOE


Huang:1988:APE


Huber:1991:SOC


Huber:1998:MAE


Hulme:1898:CHP

REFERENCES

Hunter:1985:ARK


Hurwicz:1998:CTM


Husain:1994:EI


Husemann:1999:SCD


Hulaas:1998:MLI


Hardy:1975:ITN

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

Hartnell:1976:PFM

Hardy:1979:ITN

Huthnance:1988:UPP

Hsu:1997:DWV

Hsu:1998:DBW

Hsu:1998:MWD


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

Hasan:1993:MMO


He:1996:TLR


Hong:1998:FIE


Hall:1998:BPPa


Hall:1998:BPPb


Hohl:1994:SIH


Harn:1993:GUS

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


Hardjono:1993:PDM


Ibbotson:1997:CPI


Anonymous:1993:CCA


IBM:19xx:PSP


IEEE:1974:ASS

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

IEEE:1979:ASF


IEEE:1980:PSS


IEEE:1981:CLC

[IEE81] IEEE, editor. 6th Conference on Local Computer Networks, Hilton Inn, Minneapolis, Minnesota, October 12–14, 1981. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD
IEEE:1982:ASF


IEEE:1982:CFP


IEEE:1983:PSS


IEEE:1984:ASF


IEEE:1985:FOC


IEEE:1986:CEC

IEE. Colloquium on "Encryption for Cable and


REFERENCES

Computer Society Press order number 2825.


IEEE:1994:CPN

IEEE:1994:PIC

IEEE:1994:PSH

IEEE:1994:TAJ


IEEE:1996:PICb


IEEE:1996:PIH


IEEE:1996:PICa


IEEE:1996:SCR


IEEE:1997:SIC


IEEE:1997:IICa


IEEE:1997:PIS


IEEE:1997:PICa


IEEE:1997:PICb

IEEE, editor. Proceedings of 1997 International
REFERENCES

IEEE:1997:PAC


IEEE:1998:HCC


IEEE:1998:IIC


IEEE:1998:ASF

REFERENCES


REFERENCES

IEEE Computer Society
Press, 1109 Spring Street,
Suite 300, Silver Spring,
MD 20910, USA, 1999.
ISBN 0-7695-0237-7, 0-
7695-0238-5 (case), 0-7695-
0239-3 (microfiche). LCCN
QA76.76.O63 W6666 1999.
IEEE Computer Society
Press order number PR00237 [HR99]

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

N. Ito and P. Honey-
man. Practical security sys-
tems with Smartcards. In
IEEE [IEEE99b], pages 185–
190. ISBN 0-7695-0237-7, 0-
7695-0238-5 (case), 0-7695-
0239-3 (microfiche). LCCN
QA76.76.O63 W6666 1999.
IEEE Computer Society
Press order number PR00237 [HR99]

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

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

IAB and IESG. RFC 1984: IAB and IESG statement
on cryptographic technology and the Internet, August 1996. URL ftp://
INFORMATIONAL.

H. Igarashi, S. Kosue, and
M. Miyahara. Individual tactical play and pass
with communication be-
tween players-team descrip-
tions of Team Miy2. Lecture Notes in Computer
CODEN LNCSD9. ISSN
REFERENCES

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


Impagliazzo:1992:PGP

Impagliazzo:1989:ECS

Ito:1999:DPS

Instenes:1995:MAA


IRD:1984:DTV

IRD:1987:DTV

IRD:1988:DTV

Anonymous:1991:IIS

IRD:1991:DFV

Itoh:1994:LDS

Impagliazzo:1989:LPC


[IW81] Ingemar Ingemarsson and C. K. Wong. Use authentication scheme for shared data based on a trap-door one-way function. Information Processing Letters,
REFERENCES


Jac90b] Keith M. Jackson. Secure information transfer:
REFERENCES


Jackson:1996:AAC


Jakobsson:1995:BUU


Jakobsen:1999:HOC


Jakobsson:1999:MCM


Jakobsson:1999:QCA


Jamieson:1998:UEP

Lauren Jamieson. Unveiling the extraordinary possibili-

Jantke:1995:RSI


Jantke:1995:RSI

Jaspan:1996:DWE


Jaeger:1993:LCC


Jan:1998:PWP

REFERENCES


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


Jian:1999:SDM


Jolitz:1991:PUI


Jolitz:1995:RNS


Johnson:1998:ESS


Johnson:1998:CPE


Johnson:1998:SIC


Johansson:1999:FCA

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


REFERENCES

Jurgensen:1984:SRI

Jackson:1993:CAG

Janwa:1996:MPK

Johnson:1994:CDM

Jakobsson:1999:IMI

Johnson:1994:MTS
REFERENCES


Michael K. Johnson. Lurk-
REFERENCES


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


Jakobsson:1999:SAE


Jiwa:1994:BBA


Jan:1996:SIE


Jan:1997:SIE


Juenemann:1981:DES


Juels:1999:TTS


Jung:1987:IRC


REFERENCES

<table>
<thead>
<tr>
<th>Jakobsson:1996:OAB</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Joye:1998:IBS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Kompella:1991:FCC</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Kent:1998:RIA</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Kent:1998:RIE</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Koutsoukos:1999:HCS</th>
</tr>
</thead>
</table>


uk/~fapp2/steganography/bibliography/1009.html.

**Kahn:1991:SER**


**Kahn:1991:WWW**


**Kahn:1996:HS**


**Kahn:1996:CSS**


**Kahn:1998:EC**


**Kahn:1998:PHI**


**Kahn:1998:RMU**

REFERENCES

[102x681] REFERENCES


Kaliski:1992:MAC


Kaliski:1993:SES


Kaliski:1993:ZBA


Kaliski:1993:MAC


Kaliski:1997:IPS


Kaliski:1997:PNG


Kaliski:1997:ACC

Kaliski:1998:RPRa


Kaliski:1998:RPCa


Kaliski:1998:RPCb


Kaliski:1998:RPCc


Kaliski:1998:EDF


Kaliski:1998:RPCa


Kaliski:1998:RPCb


Kaliski:1998:RPCc


Kaliski:1998:RPCa


Kaliski:1998:EDF

REFERENCES

Kaliski:1998:REC

Kaliski:1999:ESP

Kaps:1998:HSF

Karger:1985:ADA

Karger:1987:LDP

Kari:1989:CBP

Kaneshige:1996:ITC
REFERENCES

[472]

Kari:1989:OCP


Karkare:1996:SEA


Kasiski:1863:GDG

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

Kastenholz:1996:RVP


Kalipha:1990:NPK


Katzan:1977:SDE


Katsikas:1997:CMS


Kaufman:1993:RDD


Kaufman:1996:DWC


Kawai:1987:LAI


Kay:1995:CTE


Krishnakumar:1992:HTE


Krawczyk:1996:HKM


Krawczyk:1997:RHK


Klein:1989:STR

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

Karp:1988:SDN


Kunkelmann:1997:EDV


Kao:1995:ESA


Krajewski:1994:ASC


Krajewski:COMPSYS-7-1-75


Kam:1978:SDS


Kam:1979:SDS

REFERENCES

Khinchin:1997:CF

Keating:1999:PAA

Kelsey:1999:KSWb

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

Kemp:1988:EEF

Kemmerer:1989:AEP

Kemppainen:1999:DMM

Kemp:1999:CF
http://www.nist.gov/aes. No slides for the conference talk are available.
REFERENCES


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

Katsikas:1996:ISS


Kundur:1998:DWU


Kundelmann:1998:VEB


Kravitze:1999:CAC


Kharitonov:1993:CHD

REFERENCES

Karaorman:1999:CRJ

Kobara:1996:LVS

Kobara:1997:SSM

Katsumoto:1999:DPL

Kiefer:1998:WMV

Kilian:1988:FCO

Kim:1993:CLB

Karaorman:1999:CRJ

Kobara:1996:LVS

Kobara:1997:SSM

Katsumoto:1999:DPL

Kiefer:1998:WMV

Kilian:1988:FCO

Kim:1993:CLB
REFERENCES

Kippenhahn:1997:VBG

Kippenhahn:1999:CBH

Kippenhahn:1999:VBG

Kirby:1995:RPK

Kak:1977:SEU

Kocher:1999:DPA

Kurosawa:1995:NBA

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


Kelm:1997:NK


Kunihiro:1998:ECN

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

Kommerling:1999:DPT


Koren:1999:ISC


Koshelev:1999:EAM


Kurosawa:1991:GPK

[Kaoru Kurosawa, Yutaka Katayama, Wakaha Ogata,

Kabatianskii:1997:DSS


Kramer:1999:FCD


Kothari:1984:CMW


Kilian:1994:FKE


Kilian:1995:FCR


Knudsen:1995:NAA

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

Klein:1990:FCS


Kannan:1988:PFN


Klupsch:1999:ARR


Kurosawa:1988:CSP


Kurak:1992:CNI


Kang:1993:PRR


Kim:1996:ACA

[102x681]Kwangjo Kim and Tsu-
REFERENCES


Knudsen:1996:IDA


Kosuda:1997:SED


Kaksonen:1998:OMC


Kaufman:1998:DWF


Kasahara:1999:NPK

REFERENCES

Knudsen:1999:CIS


Kohlas:1999:RAP


Koscielny:1999:QBP


Kanda:1998:ECC


Kobayashi:1999:FEC


Konheim:1980:ICP


Koyama:1991:NPK

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

Kande:1999:AUD


Karn:1995:REC


Kohler:1994:EKA

REFERENCES


Knuth:1969:SNM


Knuth:1973:ACP


Knuth:1980:DLC

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

Knuth:1985:DLC


Knuth:1987:CT


Knudsen:1992:CL


Knudsen:1993:CLb


Knudsen:1993:ICS


Knudsen:1993:CLc


REFERENCES

Knudsen:1999:FSE


Kurosawa:1995:CIS


Kurosawa:1995:CBA


Kurosawa:1996:CLB


Kurosawa:1997:CLB


Koblitz:1987:CNT


Koblitz:1987:ECC


International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB).

**Kobayashi:1997:DWH**


**Koblitz:1998:C**


**Koblitz:1998:AAC**


**Koblitz:1998:ECI**


**Kobara:1999:PMA**

REFERENCES

Kochanski:1989:HSI


Koc:1994:HSR


Kocher:1995:CDR


Koc:1996:RHI


Kocher:1996:TAI


Kocher:1999:B

REFERENCES


REFERENCES

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


[Koo97] Bert-Jaap Koops. Crypt

Kopooshian:1997:DCE


Kornerup:1993:HRM


Korner:1996:PC


Koscielny:1983:PRD


Kurosawa:1994:NSS

[Kaoru Kurosawa, Koji Okada, Keiichi Sakano,


REFERENCES

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

[Koyama:1982:CUM]

[Koyama:1982:MKR]

[Koyama:1983:MKR]

[Koyama:1995:FRT]

[Kozaczuk:1984:EHGa]

[Kozaczuk:1984:EHGb]

[Kozen:1996:RSS]
REFERENCES

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

Kim:1989:PRP

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

Kwan:1993:GPT

Matthew Kwan and Josef
Pieprzyk. A general pur-
pose technique for locating
key scheduling weaknesses
in DES-like cryptosystems.
Lecture Notes in Computer
CODEN LNCSDO. ISSN
0302-9743 (print), 1611-
3349 (electronic).

Krajicek:1995:SCC

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

Knudsen:1996:HFB

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

Knudsen:1996:DSK

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

Knudsen:1997:FSH

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


Kaps:1999:FIF


Koc:1999:CHE


Kipnis:1999:UOV


Karhumaeki:1999:CSI


Kaliski:1994:FBC

REFERENCES


J. Kilian and P. Rogaway. How to protect DES against exhaustive key search. In Koblitz [Kob96],
Knudsen:1996:NAL


Kranakis:1986:PC


Krawczyk:1990:HPC

REFERENCES

link/service/series/0558/bibs/0435/04350138.htm;

Dry W. Kravitz. Digital
signature algorithm. US
Patent No. 5,231,668A.,
July 26, 1993. URL

H. Krawczyk. Secret shar-
ing made short. In Stin-
son [Sti94], pages 136–146.
CODEN LNCSD9. ISBN 3-
540-57766-1 (Berlin), 0-
387-57766-1 (New York). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/0558/tocs/t0773.htm;
http://link.springer-ny.com/link/service/series/0558/papers/0773/07730301.htm;

Hugo Krawczyk. LFSR-
based hashing and au-
thentication. In Desmedt
[Des94b], pages 129–139.
CODEN LNCSD9. ISBN 3-
540-58333-5 (Berlin), 0-387-
58333-5 (New York). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://link.springer-
ny.com/link/service/series/0558/bibs/0839/08390129.htm;

Hugo Krawczyk. New hash
functions for message authen-
tication. Lecture Notes
in Computer Science, 921:
301–310, 1995. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
/link.springer-ny.com/
l ink/service/series/0558/bibs/0921/09210301.htm;

Hugo Krawczyk, editor. Ad-
vances in cryptology —
CRYPTO '98: 18th An-
nual International Cryptol-
ogy Conference, Santa Bar-
rara, California, USA Au-
gust 23–27, 1998 proceed-
ings, volume 1462 of Le-
cature Notes in Computer
Science. Springer-Verlag,
Berlin, Germany / Hei-
delberg, Germany / Lon-
don, UK / etc., 1998.
ISBN 3-540-64892-5 (pa-
perback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25 C79 1998. 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, University of California, Santa Barbara (UCSB).


F. L. G. Kordes and J. J. Schuerman. The use of


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


Kinoshita:1998:GST

Kipnis:1998:COV

Kemp:1996:CPC
and CDMA with inherent security. In ????, editor, 
EPSRC Annual Conference on Communications, Signal 
Processing and Coding, 30– 
31 January 1996, Sheffield, 
LCCN ????.

[KSB97] A. H. Kemp, S. J. Shepherd, 
and S. K. Barton. Multi-
function coding and modu-
lation for spread spectrum 
and CDMA with inherent 
security. In ????, editor, 
EPSRC Annual Conference 
on Communications, Signal 
Processing and Coding, 22– 
23 January 1997, Sheffield, 
LCCN ????.

[KSF99] J. Kelsey, B. Schneier, and 
N. Ferguson. Notes on 
the design and analysis of 
the Yarrow cryptographic 
pseudorandom number gen-
erator. In Sixth Annual 
Workshop on Selected Ar-
ées in Cryptography, page ????. 
Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, 
UK / etc., 1999. ISBN 
????? LCCN ????? URL 
http://www.counterpane.
com/yarrow-notes.html.

[KSHW97] J. Kelsey, B. Schneier,
C. Hall, and D. Wagner. 
Secure applications of low-
entropy keys. Technical 
report, Counterpane Sys-
tems, 101 East Minnehaha 
Parkway, Minneapolis, MN 
55419, September 1997. 
URL http://www.counterpane.
com/low-entropy.html. Also 
published in 1997 Informa-
tion Security Workshop 
(ISW’97), September 1997, 
pp. 121–134 [KSHW98].

[KSHW98] J. Kelsey, B. Schneier, 
C. Hall, and D. Wagner. 
Secure applications of low-
entropy keys. Lecture Notes 
in Computer Science, 1396: 
121–134, 1998. CODEN 
LNCS-D9. ISSN 0302-
9743 (print), 1611-3349 
(electronic). URL http:
//www.counterpane.com/
low-entropy.html. See [KSHW97].

[Kim:1996:EIE] Yong-Tae Kim, Kwang-
Suk Suh, and Chang-Han 
Kim. On the efficient imple-
mentations of the elliptic 
curve ElGamal cryptosys-
tem. Bull. Honam 
Math. Soc., 13:249–256, 
1996. ISSN 1225-2921.

and H. Langendörfer. A 
nonce-based protocol for 
multiple authentications.
REFERENCES


Knowles:1992:AFC


Kelsey:1996:KCI


Kelsey:1997:RKC


Kelsey:1998:PICa


Kelsey:1998:PICb

J. Kelsey, B. Schneier, and D. Wagner. Protocol i-

**Kelsey:1999:KSWa**


**Kelsey:1999:MCAa**


**Kelsey:1999:MCAb**


**Kelsey:1998:SCCa**


**Kelsey:1998:SCCb**


**Kelsey:1998:SCCc**

J. Kelsey, B. Schneier,
Kelsey:1998:CAP


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

Kanda:1999:SCF

Kuchlin:1987:PKE

Kucera:1992:GES


Kuhn:1998:CIS

Kuijk:1991:RSE

Kukorelly:1999:VCH
REFERENCES

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

Kullback:1935:SMC


Kullback:1938:SMC


Kullback:1967:SMC


Kullback:1976:SMC


Kumar:1997:CSI


Kummert:1998:RPT


Kuo:1990:TEC


Kurosawa:1994:NBA


Kwan:1997:DIE


Kaliski:1995:SRE


Kaliski:1995:DLC


Kaliski:19xx:DLC


Kwok-Yan:1992:TAD

[LamKwok92] Lam Kwok-Yan and Thomas Beth. Timely authentication in distributed

**Kurosawa:1998:SBC**


**Kwok-Yan:1992:FAA**


**Kasami:1982:KMS**


**Koch:1995:TRH**


**Levien:1998:ART**


**Lampson:1991:ADS**


**Lampson:1992:ADS**

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


[Lag84b] J. C. Lagarias. Performance analysis of Shamir’s attack on the basic Merkle–Hellman knapsack cryp-


[Lai92] Xuejia Lai. *On the design and security of block ciphers*. Hartung-Gorre Verlag, Konstanz, Switzerland, 1992. ISBN 3-89191-573-X. xii + 108 pp. LCCN QA76.9.A25L35 1992. This is the author’s Ph.D. dissertation. “Secret-key block ciphers are the subject of this work. The design and security of block ciphers, together with their application in hashing techniques, are considered. In particular, iterated block ciphers that are based on iter-
ating a weak round function several times are consid-
ered. Four basic constructions for the round func-
tion of an iterated cipher are studied.”

[Lai95] X. Lai. Additive and linear structures of crypto-
graphic functions. Lecture Notes in Computer Science,
1008:75–??, 1995. CODEN LNCSD9. ISSN 0302-9743
(print), 1611-3349 (electronic).

[Lak83] S. Lakshmivarahan. Algorithms for public key cryp-
tosystems: theory and application. In Advances in
computers, Vol. 22, volume 22 of Adv. in Com-
put., pages 45–108. Academic Press, New York,
NY, USA, 1983.

[Lam73] Butler W. Lampson. A note on the confinement prob-
lem. Communications of the Association for Compu-
ting Machinery, 16(10):613–615, October 1973. CO-
DEN CACMA2. ISSN 0001-0782 (print), 1557-
uk/~fapp2/steganography/bibliography/1014.html.

[Lam81] Leslie Lamport. Technical note: Password authentica-
tion with insecure communication. Communications
of the Association for Computing Machinery, 24(11):
770–772, November 1981. CODEN CACMA2. ISSN
0001-0782 (print), 1557-7317 (electronic).

[Lam99] James D. Lambert. DREO secure video conferencing
and high speed data encryption tests for Inmarsat-
B satellite terminals. Technical memorandum DREO
TM 1999-084, Defence Research Establishment Ot-
tawa, Ottawa, ON, Canada, 1999. xiii + 17 + 21 pp.

[Lan46] A. W. Landers. Recent publications: Reviews: An His-
torical and Analytical Bibliography of the Literature
of Cryptology, by J. S. Galland. American Mathemati-
AMMYAE. ISSN 0002-9890 (print), 1930-0972 (elec-
tronic).

[Lan81] Andre Langie. Cryptogra-
phy: a study on secret writ-
ings, volume 38 of A Cryp-
tographic series. Aegean

Landau:1989:SSC


Langford:1995:DCT


Langford:1996:WST


Lange:1997:SCI


Landrock:1998:TOC


Landrock:1999:PTU


Lassek:1985:CCA

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


REFERENCES

[Lou:1997:PTL]

[Lou:1998:FMM]


[Leung:1999:DIM]

[Lopez:1999:IAE]

[Li:1994:EMN]
Yuan Xing Li, Robert H. Deng, and Xin Mei Wang.

**Lin:1999:AMG**


**Leary:1987:CSM**


**Leary:1990:SCS**

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

**Lear:1999:NBE**


**Leclerc:1989:CRM**


**Lee:1995:NSI**

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

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


Leiss:1980:NSS


Leipold:1999:K


Leiserson:1999:ITD


Lempel:1979:CT

Abraham Lempel. Cryptology in transition. ACM
REFERENCES

Lennon:1978:CAI


Lenstra:1987:FIE


Lenstra:1990:PT


Lenstra:1996:GSD


Lenstra:1998:GRM


Lenstra:1999:EIB


Lenzerini:1999:DLT


REFERENCES


REFERENCES


[Li:1994:RTR] Chuan-Ming Li, Tzonelih Hwang, and N.-Y. Lee. Threshold-
REFERENCES


REFERENCES


[Linn88] J. Linn. RFC 1040: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and

**RFC1040**


**RFC1113**

REFERENCES


REFERENCES


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.

**Laih:1996:CEE**


**Lee:1999:MRF**


**Landau:1994:CPP**


**Linnartz:1998:MFA**


**Lenstra:1993:DNF**

REFERENCES


REFERENCES


REFERENCES

Lam:1996:EGE


Lenstra:1990:NFS


Lenstra:1993:FNF


Langie:1922:C


Luccio:1980:CMC


Lidl:1984:PPR


Leighton:1985:HBC

REFERENCES

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


Leighton:1994:SKA


Leighton:1995:LPF


Low:1996:MCP


Lamersdorf:1998:TDS


Low:1998:PCT


Three volumes. IEEE catalog number 95CH35759. IEEE Computer Society Press order number PR06990.


REFERENCES


REFERENCES

539


**Loshin:1997:CGP**

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

**Loshin:1998:PEC**


**Lowe:1995:ANS**


**Lowe:1996:BFN**


**Loxton:1990:NTC**


**Lam:1999:ACA**


REFERENCES


REFERENCES

Luby:1998:CBB


Lamport:1982:BGP

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

Livens:1995:CCI


Leung:1985:SCT


Leong:1991:UPE

[LT91] Philip Leong and Chris Tham. UNIX password

**Linnartz:1998:MPM**


**Langley:1999:ACI**


**Laih:1995:SLF**


**Lioen:1988:OMA**


**Lu:1979:EGC**


**Lu:1980:AEG**


**Lackey:1995:SMS**

REFERENCES


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

[547]
denay [Vau98e], pages 239–253. CODEN LNCS09.
ISBN 3-540-64265-X (paperback). ISSN 0302-9743
(print), 1611-3349 (electronic). LCCN QA76.9.A25F77
service/series/0558/bibs/Lud97
1372/13720239.htm; http://
link.springer-ny.com/
link/service/series/0558/
papers/1372/13720239.
pdf.

[547]
Lucks:1999:SBB

S. Lucks. On the security of the 128-bit block
cipher DEAL. Lecture
Notes in Computer Science,
1636:60–70, 1999. CODEN
LNCS09. ISSN 0302-9743
(print), 1611-3349 (electronic).

[547]
Lucks:1999:SBC

S. Lucks. On the security of the 128-bit block
cipher DEAL. In Knudsen
[Knu99c], pages 60–70.

[547]
Lucks:1999:ARK

Stefan Lucks. Accelerated remotely keyed encryption.
In Knudsen [Knu99c],
pages 112–123. ISBN 3-540-
66226-X (softcover).
LCCN QA76.9.A25 F77 1999
Bar. URL http://link.springer-ny.com/link/

[547]
Ludwig:1997:CQA

B. Ludwig. A contribution to the question of authenticity of Rhesus using part-of-speech-tagging. Lecture
Notes in Computer Science,
1303:231–??, 1997. CODEN
LNCS09. ISSN 0302-9743
(print), 1611-3349 (electronic).

[547]
Lujan:1998:AMDa

Susan M. Lujan. Agnes
Meyer Driscoll. Cryptolog,
??(??):??, August 1998.
ISSN 0740-7602.

[547]
Lujan:1998:AMDb

Susan M. Lujan. Agnes
Meyer Driscoll. In Deavours
et al. [DKK+98], pages 269–278.
www.opengroup.com/open/
cbooks/089/0890068623.
shtml. Third volume of selected papers from issues of Cryptologia.

[547]
Lunt:1990:EK

Steven Lunt. Experiences
with Kerberos. In USENIX
Association [USE90], pages
113–120. LCCN QA 76.9
A25 U55 1990.
Lutz:1998:NBM

[102x681] REFERENCES

[548]

Lutz:1998:New


Linnartz:1998:ASA


Langelaar:1996:CPM


Langelaar:1997:RLM


Long:1988:DLH


Li:1991:JAE

REFERENCES


Laih:1993:TES


Li:1990:ACP


Li:1991:BCP


Li:1991:HBM


Ma:1979:RAD


Meijer:1981:DSS


MacPherson:1987:CUN


MacLaren:1994:CPN


Mache:1998:SCT

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


REFERENCES


**Manjunath:1998:IPA**


**Moriai:1996:KLP**


**Mao:1997:PVP**


**Mao:1998:GCS**


**Marsh:1970:CSS**


**Marsh:1970:MEC**


**Marion:1976:ANB**


**Marion:1995:WGT**


REFERENCES


Mastrovito:1989:VDM


Mastrovito:1991:VAC


Massey:1994:SKB


Massacci:1997:BSP


Massacci:1999:DRT


Massey:1999:OSD


Matyas:1979:DSO

Matyas:1991:KHC

Matyas: 1991: KHC

Matyas: 1991: Key handling with control vectors.

Matsui:1993:LCM

Matsui: 1993: LCM


Matsui:1994:FEC

Matsui: 1994: FEC


Matsui:1994:LCM

Matsui: 1994: LCM


Matsui:1995:CBO

Matsui: 1995: CBO


Matsui:1996:NSB

Matsui: 1996: NSB


Matthews:1996:SRN

Matthews: 1996: SRN

REFERENCES


Matsumura:1999:DTE


[Mau91c] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In

Maurer:1991:NAD


Maurer:1991:PSS


Maurer:1993:PSK


Maurer:1993:RIT


Maurer:1994:TEB


Maurer:1996:UGT


Maurer:1996:ACE

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

Maurer:1993a
REFERENCES

Maurer:1997:ITS


Mauriello:1997:TTC


Mauth:1997:SOC


Maurer:1998:E

REFERENCES


Mehrotra:1999:NOA


Mitra:1999:DCT


Mintzer:1998:OWS


Mintzer:1997:EIDb


Moskowitz:1992:CAA


Murphy:1997:ROD

REFERENCES


Millan:1998:HDC


Millan:1999:BFD


McHugh:1992:EBD


McIvor:1985:SC


McKee:1999:SFF


McMahon:1996:RGA


Madson:1998:REC


REFERENCES

Meersman:1999:SOT

Meijer:1981:NCM

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

Meijer:1985:MEN

Meijer:1992:SSA

Meier:1994:SIB

Meierhofer:1996:PGP

Meijer:1996:GFC

Meinel:1998:HHB
Carolyn P. Meinel. How hackers break in ... and how they are caught: Port scanners, core dumps and buffer overflows are but a


Marin Mersenne. *Cogitata Physica-Mathematica ... Tractatus de mensuris
References

poneribus atque nummis
... Hydraulica pneumatica; arsque navigandi. Harmonia theoriae, 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 pp. URL http://www.mersenne.org/prime.htm;
http://www.mersenne.org/status.htm. Three volumes. This is the book that introduced the conjecture that numbers of the form \( M(n) = 2^n - 1 \) are prime for \( n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \) and 257, but could not test this claim. Euler showed in 1750 that \( M(31) \) is prime. Lucas showed in 1876 that \( M(127) \) is prime. Pervouchine showed in 1883 that \( M(61) \) is prime, finally disproving the Mersenne conjecture. Powers in the early 1900s showed that \( M(89) \) and \( M(107) \) are prime, both missed by Mersenne. By 1947, it was known that the correct list is 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 and 127, so Mersenne had five errors in his list: 67 and 257 should have been removed, and 61, 89, and 107 added. By late 2001, 39 Mersenne primes were known, the five largest having been found by massive distributed computing efforts through the Great Internet Mersenne Primes Search (GIMPS) project. The largest of these is \( M(13466917) \), a number containing 4,053,946 digits.


Merkle:1988:DSB


Merkle:1989:CDS


Merkle:1990:OWH


Merkle:1990:CDS


Merkle:1991:FSE

REFERENCES


REFERENCES


Madson:1998:RUHb

Mackenzie:1998:LPS

Merkle:1978:HIS

Merkle:1981:SME

Michels:1996:RDS

McPherson:1998:CRH
REFERENCES


[MI96] I. Majzik:1996:MCU

Matsumoto:1988:PQP


Matsumoto:1990:EAC


[Mi90] Tsutomu Matsumoto:1990:EAC

Moulin:1999:ECG


Michener:1988:TSK


Micali:1993:FPC


Micali:1993:FPK


[Mic93b] Silvio Micali:1993:FPK
Micciancio:1997:ODS


Mihaljevic:1996:FCS


Millikin:1943:ECCa


Millikin:1943:ECCb


Millikin:1943:ECCc


Miller:1976:RHT

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


REFERENCES

Millan:1996:LOA

Miller:1996:CME

Matsumoto:1993:VIA

Mintzer:1997:EIDa

Misarsky:1997:MAU

Misarsky:1998:HDR

Mitchell:1976:EAD
James Melvin Mitchell. Encryption algorithm for data security based on a polyalphabetic substitution scheme and a pseudorandom number generator. Thesis (M.S.), University of Tennessee, Knoxville,


Miyaji:1993:OEC


Miyano:1993:MEN


Miyaji:1996:MRS


Miyaji:1999:ECC


Mjolsnes:1993:PCP


Mori:1992:PSP


Moskowitz:1994:CCH


Mazières:1999:SKM

David Mazières, Michael Kaminsky, M. Frans

Maibaum:1999:SRS


Miyazaki:1999:TFI


Monge:1967:NMC


Maulucci:1987:HAC


Mao:1998:CPO


Matyas:1991:KSB

REFERENCES

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


I. S. Moskovitz and A. R. Miller. The channel capacity of a certain noisy timing channel. *IEEE Transactions on Informa-
REFERENCES

Moskowitz:1992:IDI


Moskowitz:1994:STC


Moldovyan:1995:FSE


Meadows:1996:CCC


Meyer:1996:PKC


Mueller:1998:SPK

S. Mueller and W. B.


Magliveras:1990:CTC


Muller:1981:SRP


Muller:1986:CDS


MRaihi:1997:XFO


Moulin:1999:ITA


Mock:1997:BDS


Mohtashemi:1992:CHC

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


Matsumoto:1982:DTL

Mok:1997:KNF

Moldovyan:1998:NEP

Morita:1991:SCT
REFERENCES


REFERENCES

Masonic Book Club, Bloomington, IL, USA, 1992. xxxii + 255 pp. [Mos99]


REFERENCES


Malek:1995:DCB


Myers:1995:RCM


McLeod:1998:TMP


Mrakovcic:1995:EIN


Micali:1987:NSP


Micali:1988:NSP


Maitra:1999:COA

Mitchell:1989:RHF


Macalister:1976:SLI


McEliece:1981:SSR


Muller-Schloer:1983:MBC


Meier:1990:NCC


Montgomery:1990:FEP


REFERENCES


Metzger:1995:RIAb


[RFC1828

Mambo:1998:NCB


Michels:1998:GCS


MacKenzie:1999:AIH


Maitra:1999:HNR


[Miyazaki:1999:KGD]

[McLeod:1990:VLD]

[Miksch:1999:ASQ]
S. Miksch, A. Seyfang, W. Horn, and C. Popow. Abstracting steady qualitative descriptions over time from noisy, high-frequency data. Lecture Notes in Computer Science, 1620:281–??, 1999. CODEN LNCS39. ISSN 0302-9743 (print), 1611-3349 (electronic).
REFERENCES

Mizuki:1998:ESK


Mizuki:1999:DNS


Martin:1999:BTE


Mambo:1996:HUT


Madonia:1993:GSP


Michels:1998:SSV

REFERENCES

Mullender:1986:DCD


Matsui:1994:VSH


Massey:1995:MCM


Molva:1998:SSA


Matsui:1999:CRV

M. Matsui and T. Tokita.
REFERENCES


REFERENCES

Molva:1992:KAK

Mu:1992:ICS

Muftic:1993:SAO

Muftic:1988:SMC

Mulligan:1989:UMA

Mullin:1989:LEN
Conjectures that $M_n = 2^n - 1$ is the product of two distinct primes only if $n$ is either a prime $p$ or the square of a prime $q$, in which case precisely one prime factor of $M_n$ is Mersenne, vis. $M_q$.

Muller:1999:SRB


Mund:1991:ZCP


Mund:1991:ZLC


Muraszko:1987:CVR


Murphy:1996:CC


Murphy:1999:OST

REFERENCES

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


Menezes:1997:HAC


Menezes:1993:CPE


Muller:1998:DLB


Manber:1994:AAM


Maurer:1996:TCW


Maurer:1996:DO


Maurer:1999:RBB


Malkin:1999:ESG


Mitchell:1994:CPA


Maurer:1991:NIP


Matsui:1993:NMK


Maurer:1993:RNI

REFERENCES

Mayers:1998:QCI

Mayers:1996:TAS

Myers:1997:RSA

Myers:1998:VCS

McCurley:1998:ACE

Mihaljevic:1998:CAB


Merwin:1979:NCC


Nastar:1995:TRD


Nat-Abdesselam:1999:QCA


Naccache:1993:MSF

REFERENCES


REFERENCES

NCSOTS:1984:ISR


NIST:1985:FPSa


NIST:1985:FPSb


NIST:1991:DSS


NIST:1992:DSS


NIST:1992:PYA


NIST:1993:FPD

REFERENCES

Anonymous:1993:FPD


NIST:1993:DES


NIST:1994:FPD


NIST:1994:DES


NIST:1994:DSS


NIST:1994:EES

REFERENCES

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

NIST:1995:FPSb

Natarajan:1997:RPK

NIST:1997:ARC

NIST:1998:FAE

NIST:1999:FPD

NIST:1999:SAC
March 1999. ISBN ???
LCCN ???
URL
http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm;
http://www.nist.gov/aes. No formal proceedings were published, but the conference Web site contains pointers to slides and/or technical papers for most of the fifteen “complete and proper” candidates.

[NIST:1999:SRF]

[NBWH78]

[Nandi:1997:RCT]
REFERENCES


Neat:1975:NCC


Nechvatal:1991:PC


Nechvatal:1996:PKB


Needham:1994:DSE


NetworkAssociates:1998:NB


Neumann:1991:IRCd


Neumann:1992:IRF


Neumann:1994:IRA

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


Neumann:1997:IRC


Neve:1999:FSC


Ng:1999:CST

REFERENCES

Nguyen:1999:CGC


Nguyen:1999:CGG


Nelson:1990:SAE


Neubauer:1998:DWI


Neubauer:1998:CSD


Nichols:1998:CCCa


Nichols:1998:CCCb

REFERENCES


REFERENCES

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

[NIST:1993:FPS]

[NIS93b] NIST.


Anonymous.


[Nis96] N. Nisan.


[NK96] Nisan.


[NK98a] N. Pekka Nikander and Arto Karila.


[NK99] Pekka Nikander.


[NK99b] Pekka Nikander and Arto Karila.


[NK99c] Pekka Nikander and Arto Karila.


[NK99d] Pekka Nikander and Arto Karila.


[NK99e] Pekka Nikander and Arto Karila.


[NK99f] Pekka Nikander and Arto Karila.


[NK99g] P. Nikander.


REFERENCES

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

Nguyen:1999:DZK


Naccache:1995:CDB


Naccache:1995:CDI


Nozaki:1997:LCS


Noras:1996:CHH


Nicchiotti:1998:NIS

REFERENCES

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

Nobauer:1984:CRS

Nobauer:1985:CRS

Nobauer:1988:CPK

Norman:1973:SWB

Noras:1995:CHHa

Noras:1995:CHHb

Noras:1995:PCE

Naor:1993:PZK

Naor:1997:VAI
Moni Naor and Benny Pinkas. Visual authen-
REFERENCES

Naor:1998:TTT


Naor:1998:UIS


Niemi:1994:CPV


Nyberg:1995:MRS


Naor:1999:OTA


Needham:1978:UEAa

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


REFERENCES

**Nguyen:1997:MRC**


**Nguyen:1997:MHR**


**Nechaev:1998:DSB**


**Nguyen:1998:BQS**


**Nguyen:1998:BSR**


**Nguyen:1998:CAC**


**Nguyen:1998:CAD**


**Nguyen:1999:CFP**

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

Nguyen:1999:HHS


Naccache:1999:HCF


Nieh:1993:MAC


Neuman:1994:KAS


Nadjm-Tehrani:1999:BHO


Nemetz:1988:RLS


Nurmi:1994:CPA

REFERENCES

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


K. Nyberg. Linear approximation of block ciphers.
REFERENCES


Nyberg:1998:ACE


Nystrom:1999:PCT


Ohsuga:1999:EHI


Oakley:1978:RPC


Oberzalek:1999:GEE

REFERENCES

OConnell:1981:CDE


O'Connor:1994:UBN


OConnor:1995:DCT


Obenland:1999:SED


ORuanaidh:1996:PWD


Odlyzko:1984:CAM

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Ochi:1998:NSO


ONeil:1986:ETM


Okamoto:1990:DZKb

[OO90] Tatsuaki Okamoto and Kazuo Ohta. Disposable zero-knowledge authentica-

Ohta:1993:DMS


Ohta:1998:CST


Ogawa:1998:WTM

Ohta:1991:MAH


ORuanaidh:1997:RST


ORuanaidh:1998:RST


ORuanaidh:1999:CCP


Oppliger:1996:ASS


Oppliger:1997:ISF

Rolf Oppliger. Internet se-
REFERENCES

Otway:1987:ETM


Otrow:1996:EGI


Orton:1995:MTD


Orton:1995:MIT


Orton:1998:CPG

REFERENCES


O'Shea:1988:CDU


Okamoto:1991:EAC


Okamoto:1992:EAC


Olejar:1998:CPR


Orup:1991:VER


Ong:1991:TCM

Sing Guat Ong, Jennifer Seberry, and Tho-


[Ong:1985:ESS]


[Ou:1999:UUC]
REFERENCES

Outerbridge:1998:ACD


Ozarow:1984:WTC

Lawrence H. Ozarow and Aaron D. Wyner. Wiretap channel II. ATT Bell Lab. tech. j, 63(10 part 1): 2135–2157, 1984. CODEN ABLJER. ISSN 0748-612X.

OReilly:1995:WWW


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

Ostrovsky:1991:HWM


Pereira:1998:REC


Petitcolas:1998:WCM

uk/~fapp2/papers/acm98-weaksesses.doc.

Paabo:1993:AD


Padro:1998:RVS


Pai:1996:VIE


Paillier:1998:INS


Paillier:1999:EDF


Paillier:1999:LCD


Paillier:1999:TPE

References

Paillier:1999:PKC


Petitcolas:1998:ACM


Parthasarathy:1985:DSG


Parent:1998:ALM


Parker:1998:UMP


Parrish:1998:RMM


Patterson:1987:MCC

Patarin:1991:PPB


Patarin:1991:NRP


Patarin:1995:CMI


Patarin:1996:ACH


Paterson:1999:IPG


Paulson:1998:IAV


Paulson:1999:IAI

REFERENCES


REFERENCES


REFERENCES

Perrig:1997:CPE


Perkuhn:1999:DSC


Pesic:1997:SSS


Petho:1991:PTA


Petersen:1998:HCD


Panagopoulos:1994:BSS


Pfitzmann:1995:BEA


Pfitzmann:1996:IHT

[Pfi96a] B. Pfitzmann. Information hiding terminology. In Anderson [And96c],
REFERENCES


Patarin:1997:ACB

[PG97a]

Patarin:1997:ACS

[PG97b]

Pieprzyk:1996:CBT

[PGCSN96]

Pieprzyk:1996:CBT

[PGV91]

Preneel:1992:CSH

[PGV92]

Preneel:1993:CHF

[PGV93a]
B. Preneel, R. Govaerts, and J. Vandewalle. Cryptographic hash functions. In Wolfovicz [Wol93b], pages 161–171. LCCN ???.

Preneel:1993:HFB

[PGV93b]
REFERENCES


Preneel:1993:IAH


Preneel:1993:CSI


Preneel:1994:HFB


Pohlig:1978:IAC


Post:1991:RSE


Praun:1999:RMW

REFERENCES

Phillips:1998:SHI

Pichler:1986:ACE

Pichler:1998:E

Pierce:1977:SSP

Pieper:1993:CRD

Pinch:1997:UCN

Piner:1998:CUW
Mary-Louise G. Piner. CS update; WW II cryptologist [Jack Good] receives Pioneer Award; Colossus builder Tommy Flowers (1905–1998); DCI founder [George Schussel] receives Entrepreneur Award; 1998 Bell Prize recognizes advances in parallel process-
ing. Computer, 31(12):70–73, December 1998. CO-
DEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic). URL http://
dlib.computer.org/co/
books/co1998/pdf/rz070.
pdf.

Pitas:1995:PIW

[Pit95]
I. (Ioannis) Pitas, edi-
tor. Proceedings of 1995
IEEE Workshop on Nonlin-
ear Signal and Image Pro-
cessing (Neos Marmaras,
Halkidiki, Greece, June 20–
22, 1995). IEEE Computer
Society Press, 1109 Spring
Street, Suite 300, Silver
Spring, MD 20910, USA,
1995. LCCN ???? Two vol-
umes.

Pitas:1996:MSC

[Pit96a]
I. Pitas. A method for sig-
nature casting on digital im-
ages. In IEEE [IEE96e],
pages 215–218. ISBN 0-
7803-3258-X (softbound),
0-7803-3259-8 (casebound),
0-7803-3260-1 (microfiche),
0-7803-3672-0 (CD-ROM).
LCCN TK8315.I222 1996.
ac.uk/~fapp2/steganography/
bibliography/063160.html

Three volumes. IEEE cata-
log number 96CH35919.

Pitoura:1996:RSS

[Pit96b]
E. Pitoura. A replication
schema to support weak
connectivity in mobile in-
formation systems. Lecture

Notes in Computer Science,
1134:510–??, 1996. CODEN
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic).

Price:1999:IAV

An innovative approach to
vision, localization and ori-
entation using omnidirec-
tional radial signature analy-
sis. Lecture Notes in Com-
puter Science, 1604:299–??,
ISSN 0302-9743 (print), 1611-3349 (electronic).

Panneerselvam:1990:RSA

[PJB90] G. Panneerselvam, G. A.
Jullien, S. Bandyopadhyay,
and W. C. Miller. Recon-
figurable systolic architec-
tures for hashing. In Pro-
cedings — Parbase-90 In-
ternational Conference on
Databases, Parallel Archi-
tectures, and Their Ap-
plications (Mar 7–9 1990:
Miami Beach, FL, USA),
pages 543–?? IEEE Com-
puter Society Press, 1109
Spring Street, Suite 300,
Silver Spring, MD 20910,
USA, 1990. IEEE catalog
number 90CH2728-4.

Popek:1979:ESC

[PK79] Gerald J. Popek and
Charles S. Kline. Encryp-
tion and secure computer
networks. ACM Comput-
ing Surveys, 11(4):331–356,
REFERENCES

December 1979. CODEN CMSVAN. ISSN 0010-4892.

Penzhorn:1995:CLP

Penzhorn:1995:CLW

Praehofer:1999:SRS

Pamplona:1998:LVC

Postma:1997:DCF

Park:1994:KDA

Petrounias:1994:RBA
I. Petrounias and P. Loucopoulos. A rule-based approach

**Pless:1975:ESC**


**Pless:1977:ESC**


**Plimmer:1998:MIW**


**Plumstead:1982:ISG**


**Plumstead:1983:ISP**


**Plumstead:1983:ISPa**


**Pei:1999:COA**

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


Payne:1978:OEN


Petersen:1998:SST


Pitt:1999:DAC


Provos:1999:FAP


Prie:1999:ASU


Proctor:1992:AIC


Pudil:1995:ASM

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


**Pomerance:1990:CCNa**


**Pomerance:1990:F**


**Pomerance:1994:NFS**


**Pomerance:1998:C**


**Poole:1995:La**


**Pope:1996:PF**

Porges:1952:MNC


Portz:1991:UIN


Portz:1993:GDB


Poromaa:1998:PAT


Posch:1992:TMD


Posch:1993:PFP


Posch:1998:MPC


Posch:1989:AEA


Pfitzmann:1990:HBD

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


Torben Pryds Pedersen and Birgit Pfitzmann. Fail-stop


[B. Preneel, V. Rijmen, and A. Bosselaers. Recent developments in the design of conventional cryptographic...

Preneel:1998:AAP


Preneel:1993:ADC


Preneel:1993:SCT


Preneel:1994:CHF


Preneel:1994:CHF


Preneel:1995:FSE


Preneel:1995:EFC

cryptobytes/crypto1n2.pdf.


**Price:1983:ABR**


**Price:1994:MVC**


**Pronzini:1980:MCC**


**Proctor:1985:SSC**

REFERENCES


REFERENCES

Pointcheval:1996:SPS


Parker:1997:GFA


Padro:1998:SSS


Patel:1998:EDL


Patiyoot:1998:APW


Patiyoot:1998:SIW


Patiyoot:1998:TAPa

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

**Patiyoot:1998:TApb**


**Poupard:1998:GSR**


**Poupard:1998:SAP**


**Patiyoot:1999:MES**


**Patiyoot:1999:WSS**


**Patiyoot:1999:SIA**

REFERENCES

Patiyoot:1999:CST


Patiyoot:1999:WWA


Pfenning:1999:SDT


Patel:1997:UDB


Pieprzyk:1991:RAS


Pieprzyk:1995:PA


Pieprzyk:1995:ACA


REFERENCES


REFERENCES

Computer Society Technical Committee on Security and Privacy.

Preamel:1996:STM


Pfitzmann:1986:NUO


Pfitzmann:1987:NUO


Pfitzmann:1993:APS


Piper:1993:DSH

REFERENCES


REFERENCES

Quisquater:1998:CSE


Quisquater:1991:CLE


Quisquater:1989:BHF


Quisquater:1990:BHF


Qiao:1998:CME

Lintian Qiao and Klara


REFERENCES


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

Rhodes-Burke:1982:RSA


Reiter:1994:HSR


Ramesh:1999:VPP


Rowstron:1999:CUR


Rabin:1989:VSS


Reiter:1994:SAF


Rogaway:1994:SEA


**Rogaway:1994:SOE**


**Russinovich:1995:EWL**


**Rubia:1999:RIB**


**Renvall:1996:ASS**


**Renvall:1996:NSS**


**Roback:1999:CRF**

REFERENCES

Roback:1999:FAE


Rebel:1998:ADS


Rijmen:1996:CS


Reeds:1979:CMC


Reeds:1998:SCB


Reischuk:1985:NSB


Reiter:1992:ISG

Reiter:1996:DTR


Rejewski:1977:ATP


Rejewski:1981:HPM


Rejewski:19xx:EMH


Revello:1991:CEC


Reynard:1996:SCB


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


REFERENCES

[Rili96] W. D. Riley. LANSCAPE — encrypt this!! — there are a thousand reasons to use encryption. Unfortunately, the current state of technology does not lend itself to e-mail platforms. *Datamation*, 42(9):27–??, 1996. CODEN DTM-NAT. ISSN 0011-6963.

[Ripe:1995:IPS]

[Ripe:1995:RIP]


REFERENCES


Rivest:1980:DSC


Rivest:1985:RCP


Rivest:1987:EDR


Rivest:1990:RMM


Rivest:1990:C

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Raisch:1996:ACH


Roberts:1993:ECI


Robshaw:1995:BC


Robshaw:1995:SC


Roberts:1998:SMP


Robinson:1998:FRC


Roe:1994:PSC


Roe:1995:PBC


Roelse:1999:CWD

Peter Roelse. Cryptanalysis of the Wu-Dawson pub-

**Rogaway:1995:BHA**


**Rogaway:1996:SD**


**Rohwer:1975:GIM**


**Rohwer:1977:CCB**


**Rohatgi:1999:CNR**

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

**Roman:1990:C**


**Rompel:1990:OWF**

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


[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.


REFERENCES

February 1996. CODEN LOGNEM. ISSN 1044-6397.

[Ros96e] Greg Rose. USENIX PGP key-signing service. ;logi


n: the USENIX Association newsletter, 21(3):10–??, June 1996. CODEN


LOGNEM. ISSN 1044-6397.

[Ros96f] Greg Rose. USENIX PGP key-signing service. ;logi


n: the USENIX Association newsletter, 21(4):8–??, August 1996. CODEN


LOGNEM. ISSN 1044-6397.


[Ros97c] Shawn James Rosenheim. The cryptographic imagina-


[Ros98a] G. Rose. A stream cipher based on linear feedback over GF(208). Lecture Notes in Computer Science, 1438:135–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electroni-


c).

REFERENCES


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


REFERENCES

687
to the journal Cryptologia, but never published. For the story behind the suppression of publication, see [Ritxx]. Internal technical memoranda TM 78-1271-10, TM 78-1273-2, 1978.

[Rauber:1997:SDW]


[Rappe:1997:RRWa]


[Rigney:1997:RRAwb]


[Rivest:1998:RBC]


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


REPRESENTATIONS


Roeckl:1999:CPS


Rozenberg:1999:DCN


Rivest:19xx:SPN


Rivest:1978:MOD


Rivest:1982:MOD


Rivest:1983:MOD


RSA:1993:PRE

[RSA93a] RSA Laboratories. PKCS #1: RSA Encryption Standard, Version 1.5. RSA Data Security, Inc., Redwood City, CA, USA,
REFERENCES


[RSG98] M. G. Reed, P. F. Syver-son, and D. M. Goldschlag. Anonymous con-
nexions and onion routing. IEEE Journal on Selected
uk/~fapp2/steganography/
bibliography/072144.html

ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

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


[Rud91] Steven Rudich. The use of interaction in public cryp-


[Rudich:1991:UIP] Steven Rudich. The use of interaction in public cryp-
References

Rueppel:1993:ACE


Rueppel:1998:E


Ruohonen:1994:EDO

Rueppel:1998:E


Russell:1927:CMS

D. Russel. High-level security architecture and the

**Ruskey:1993:SCG**


**Russell:1993:NSC**


**Roychowdhury:1999:ENQ**


**Reeds:1984:FSU**


**Robshaw:1997:ECC**


**Rytter:1986:SCU**


**Ras:1999:DES**


**S:1873:COD**

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


Schiller:1995:SWT


Sabourin:1994:CCP


Sabourin:1994:CCP

Luigi Sacco. Manuale di crittografia. (Italian) [Manu-

Sacco:1947:MC


Sacco:1947:MC

Luigi Sacco. Manuale di crittografia. (Italian) [Manu-

Sacco:1951:MCF


Sacco:1977:MC


Sahai:1999:NMN


A. Salomaa. Verifying and recasting secret ballots in

**Salomaa:1996:PC**


**Salomaa:1996:PC**


**Salvail:1998:QBC**


**Salvail:1999:SHG**


**Shimoyama:1997:IFS**


**Sameshima:1998:KES**


**Sameshima:1999:SHG**


**Sansom:1986:BRC**


**Sandhu:1988:CIT**

REFERENCES


Sawirudin:1955:PND


Schaumuller-Bichl:1982:ADE


Smid:1992:DES


Smid:1993:RCN


Shepherd:1994:UBS


Shepherd:1995:CNL


Schneier:1997:EPP

REFERENCES


Shi:1998:FMV


Soto:1999:RTA


Serpell:1985:PES


Smillie:1985:RFM


REFERENCES


Smith:1996:MIH


Sun:1997:DCP


Styner:1999:BMD


Schwenter:1620:SSN


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

Scacchitti:1986:CT

Fred A. Scacchitti. The cryptographer’s toolbox.
REFERENCES

Verlegung Simon Halbmayr.


REFERENCES

Schnorr:1990:EISa

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


Schifreen:1992:PPD


Schneier:1992:SSA


Schneier:1992:UPC


Schilling:1993:MBC


Schneier:1993:SCD


Schneier:1993:DS


Schneier:1993:IEA


Schneier:1993:UHD

REFERENCES

Schnorr:1993:FHI


Schnorr:1993:FIE


Schiller:1994:SDC


Schneier:1994:DNV


Schneier:1994:DEA


Schneier:1994:PAD


Schneier:1994:SCD


Schneier:1994:SCD


Schneier:1994:AAa

REFERENCES


REFERENCES

CODEN DDJOEB. ISSN 1044-789X.

Schneier:1995:MS


Schneier:1995:MSH


Schneier:1995:OPE


Schneier:1995:PCC


Schneier:1996:ACP


Schneier:1996:CC


Schneier:1996:DLC


Schneier:1997:IRC

Schneier:1997:CBT
Bruce Schneier. The crypto bomb is ticking: Crack-

Schneier:1998:CDV

Schneier:1998:CTS

Schneier:1998:SPC

Schneier:1998:TEA


Schoenmakers:1998:SAE


Schroeppel:1998:HPC

REFERENCES


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


Scerri:1999:UOS


Scudder:1992:OLA


Smith:1986:GCC


Silvestre:1997:IWU


Schouten:1999:FEU


Sicherman:1983:AQR


Smillie:1986:RWA

K. W. Smillie and Ralph Erskine. Reviews: W. Aspray, Should the Term Fifth Generation Computers Be Banned?; C. A.


REFERENCES


REFERENCES


Sgarro:1990:IDB

Sgarro:1991:STC

Sgarro:1991:LBA

Sgarro:1993:ITB

Slater:1998:CAD

Syverson:1997:ACO


REFERENCES

DKDAEM. ISSN 1001-0548.

**Shannon:1945:MTC**


**Shannon:1948:MTCa**

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

**Shannon:1948:MTCb**


**Shannon:1949:CTS**


**Shamir:1979:HSS**


**Shamir:1982:PTA**


**Shamir:1983:ECT**

Adi Shamir. Embedding cryptographic trapdoors in

**Shamir:1983:GCS**


**Shamir:1984:PTA**


**Shamir:1985:IBC**


**Shamir:1986:SPS**


**Shamir:1987:CSS**


**Sharp:1988:DCO**


**Shamir:1994:ESS**


[She86] Jeffrey Shallit. Reviews:
REFERENCES


Sherrod:1992:DES

Shepherd:1993:ACCa

Shepherd:1993:ACCb

Shepherd:1993:EOS

Shepherd:1993:WNS

Shepherd:1994:ACM

Shepherd:1994:CGA

Shepherd:1994:MCM
[She94c] S. J. Shepherd. Multifunction coding and modula-
REFERENCES


[Shparlinski:1999:FFT] Igor E. Shparlinski. *Finite fields: theory and computation: the meeting point of number theory, computer science, coding theory, and cryptography*, volume 477 of *Mathematics and its appli-
REFERENCES


REFERENCES


[Sakurai:1994:SCT]

[Sidhu:1981:APG]

[Siegenthaler:1984:CIN]

[Siegenthaler:1985:DCS]

[Swartzlander:1993:SCA]
REFERENCES


Shimbo:1993:CSC

Silverman:1983:RVS

Silverman:1987:MPQ

Silverman:1997:RSP

Silverman:1997:FGR

Silverman:1999:EMM

Simonetta:1404:LTC
Cicco Simonetta. [Little tract on cryptanalysis]. ?????, ????, 1404. ????? pp.

Simmons:1979:HID
Simmons:1979:CCA


Simmons:1979:SAE


Simmons:1982:SCA


Simmons:1982:SAE


Simmons:1983:PPS


Simmons:1984:HID


Simmons:1985:ATC

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

 Simmons:1985:SCD


 Held at the University of Paris, Sorbonne.

 Simmons:1988:SSC


 Simmons:1990:HRS

REFERENCES

Simmons:1992:CCS

Simmons:1993:SCU

Simmons:1994:CTS

Simmons:1994:CPF

Simmons:1994:SCP

Simmons:1994:SCE
REFERENCES


REFERENCES


[Schneier:1996:AOC]

[Schneier:1996:PPSa]

[Schneier:1996:UFNa]

[Schneier:1996:PPSb]

[Schneier:1997:AESb]
B. Schneier and J. Kelsey. Automatic event-stream notarization using digital signature. Lecture Notes in

Schneier:1997:AESa


Schneier:1997:RAS


Stabell-Kulo:1997:SLS


Schneier:1998:CSS


Shimoyama:1998:QRS


Shimoyama:1998:QRB

REFERENCES


A high-speed small RSA encryption LSI with low power dissipation. Lecture Notes in Computer Science, 1396:174–??, 1998. CODEN LNCS79. ISSN 0302-9743 (print), 1611-3349 (electronic).

Satoh:1998:HSS

A. Satoh, Y. Kobayashi, H. Niijima, and N. Ooba. [SKNO98b]
A high-speed small RSA encryption LSI with low power dissipation. Lecture Notes in Computer Science, 1396:174–??, 1998. CODEN LNCS79. ISSN 0302-9743 (print), 1611-3349 (electronic).

Schneier:1996:DP


Schneier:1998:TSC


Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. AES performance comparisons. In National Institute of Standards and Technology [Nat99b], page 44. ISBN
REFERENCES

?? ?? LCCN ?? URL http://csrc.nist.gov/encryption/aes/round1/conf2/Schneier.pdf; http://www.counterpane.com/twofish. Only the slides for the conference talk are available, but technical reports are available at the authors’ Web site.

Schneier:1999:NRT


Schneier:1999:TKS


Sufatrio:1999:IMS

REFERENCES


REFERENCES


[Sma99] N. P. Smart. On the performance of hyperelliptic cryp-


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


REFERENCES


Safavi-Naini:1993:FTA


Safavi-Naini:1993:ACU


Safavi-Naini:1994:VFH


Safavi-Naini:1996:TSS


Safavi-Naini:1998:BCM


Safavi-Naini:1998:NRM

[SN98b] Reihaneh Safavi-Naini and Huaxiong Wang. New re-


[Sot98] Juan Soto, Jr. Randomness testing of the AES candidate algorithms.
REFERENCES

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

Smith:1979:UFM


Seberry:1989:CIC


Seberry:1990:ACA


Seberry:1990:ACA

Schechter:1999:AAM

REFERENCES


REFERENCES


Smith:1995:PCD


Smith:1995:PKC


Sandhu:1996:AAC


Silverman:1997:CAX


Sakai:1998:DHC


Sun:1998:PKC


Schneier:1999:BHD

on Smart Cards, USENIX Press, to appear.

**Schoenhoff:1999:GVM**


**Shapiro:1999:MAE**


**Solomonides:1999:REI**


**Stubblebine:1999:FLA**


**Stubblebine:1999:FOA**


**Subramanian:1988:DTP**


**Siromoney:1988:CPL**

REFERENCES


Sherman:1994:SNA


Schneier:1997:DDE


Saeednia:1998:NIK


Saeednia:1998:SGI


Susilo:1999:FST


Shepherd:1990:CSS


Schmidt:1998:LOA

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


REFERENCES

Stern:1991:CPK

StJohns:1993:RIP

Safavi-Naini:1994:OAS

Stark:1970:INT

Stark:1978:INT

Stallings:1994:PGP
William Stallings. Pretty Good Privacy: Privacy and security are important issues to commercial users of public E-mail systems. PGP, an E-mail security package, is finding acceptance as the way to achieve protection. BYTE Mag.
REFERENCES

Stallings:1994:SSH

Stallings:1995:PWT

Stallings:1995:PYP

Stadler:1996:PVS

Stallings:1996:PCS

Stallings:1996:PCI

Staddon:1997:CSC

Staiger:1996:CSW
REFERENCES


[Ste89] Peter Stephenson. Personal and private (microcomputer
REFERENCES


Stern:1998:LCO


Stern:1998:NEA


Stephenson:1999:C


Stern:1999:ACE


Stern:1999:DU


Stinson:1991:CCA


REFERENCES


[Str93a] P. Strauss. Secure E-mail cheaply with software

**Strauss:1993:SMC**


**Stripp:1995:CBF**


**Sandholm:1999:DOC**

REFERENCES


Sun:1991:UDE


Sun:1991:RSE


Sun:1998:ISM


Sun: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

REFERENCES

Schnorr:1995:BBC


Shepherd:1995:GJ


Stern:1998:CC


Shamir:1999:PSS


Shepherd:1996:SAD


**Shamir:1998:PHS**


**Shepherd:1995:SCS**


**Smeets:1991:CAC**


**Shulman:1961:GC**


**Smith:1983:HCR**


**Silverman:1993:PAE**


**Saeki:1994:SSS**

M. Saeki and K. Wenyin. Specifying software specification and design methods.
REFERENCES


[Safford:1994:UNC]

[Snow:1994:SA]

[Scheidler:1995:PKC]

[Stansfield:1995:CCS]

[Schneier:1997:FSEa]

[Schneier:1997:FSEb]
REFERENCES


Stinson:1998:ARS


Stinson:1999:ARS


Stinson:1999:KPT


Swan:1994:AAb


Swire:1997:ULF


Salzer:1981:RHH

REFERENCES

org/annals/an1981/a3289abs.htm. See minor correction [Ano81a].

Sun:1989:TKE


Sun:1990:KGE


Salomaa:1986:PKC


Salomaa:1986:PCB


Smith:1992:ICF


Sakurai:1996:BDB


Shieh:1996:AKD

REFERENCES


Sze98
Andrzej Szepietowski. Weak and strong one-way space complexity classes. In-
PLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Swanson:1996:RDH
M. D. Swanson, B. Zhu, and A. H. Tewfik. Robust data hiding for images. In Lervik
and Waldemar [LW96], pages 37–40. ISBN 0-7803-
3629-1 (softbound), 0-7803-
3630-5 (microfiche), 82-993923-0-6 (Norway) (?invalid checksum??). LCCN
TK5102.9.I3 1996. URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/1035.html.

Swanson:1996:TRI
M. D. Swanson, B. Zhu, and A. H. Tewfik. Transparent robust image water-
marking. In IEEE [IEE96e],
pages 211–214. ISBN 0-
7803-3258-X (softbound),
0-7803-3259-8 (casebound),
0-7803-3260-1 (microfiche),
0-7803-3672-0 (CD-ROM).
LCCN TK8315.I222 1996.
ac.uk/~fapp2/steganography/
bibliography/072157.html.

Swanson:1998:MSB
M. D. Swanson, B. Zhu, and A. H. Tewfik. Multiresolution scene-based video
watermarking using perceptual models. IEEE
Journal on Selected Areas in Communications, 16(4):-
540–550, May 1998. CO-
DEN ISACEM. ISSN
0733-8716 (print), 1558-
0008 (electronic). URL
http://www.cl.cam.ac.
.uk/~fapp2/steganography/
bibliography/1037.html.

Swanson:1998:MSV
Mitchell D. Swanson, Bin
Zhu, and Ahmed H. Tew-
fik. Multiresolution scene-
based video watermarking
using perceptual models. IEEE
CODEN ISACEM. ISSN
0733-8716 (print), 1558-
0008 (electronic).

Swanson:1998:RAW
M. D. Swanson, B. Zhu,
A. H. Tewfik, and L. Boney.
Robust audio watermarking using perceptual masking. Signal Process-
ing, 66(3):337–355, May
1998. CODEN SPRODR.
ISSN 0165-1684. URL
http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073173.html

Seberry:1994:ISA


Seberry:1994:PDS


Seberry:1995:RAN


Seberry:1995:SCF


Seberry:1995:RBP


Theodoridis:1998:NES


REFERENCES


Tanaka:1990:RSI

Tao:1994:FAO

Tardo:1990:PKB

TFEC:1998:CPF

Tattersall:1998:ENT

Tattersall:1999:ENT

Taylor:1990:DSI
REFERENCES

Taylor:1994:ICV


Taylor:1995:NOU


Tao:1985:FAP


Tao:1986:TVF


Tsuji:1991:NIB


Tao:1999:GPK


Tao:1999:FAP

REFERENCES


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


REFERENCES


Thomas D. Tarman, Robert L. Hutchinson, Lyndon G.
REFERENCES


Tsujii:1988:PKC

Tilki:1998:EHD

Tippett:1927:RSN

Taaffe:1997:NSL

Tseng:1999:ATS

Takagi:1999:DRA
<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>
REFERENCES


[Tou94] Yukiyaou Tsunoo, Eiji Okamoto, and Tomohiko Uyematsu. Ciphertext only attack for one-way func-


[Des94b]

Touch:1995:RRM


[Tou95]

Townsend:1998:QCO


[Tow98]

Thompson:1963:SDE


[TP63]

Traore:1997:MUF


[Tra97]

Traore:1999:GST


[Tre99]

Tremblett:1999:JPA


[Tre99]
REFERENCES

[Tri18]

[Tri06a]

[Tri06b]

[Tri06c]

[Tri21a]

[Tri21b]
scripturam animi sui voluntatem absentibus aperiendi certa. Balthasaris Aulaeandri, Darmstadt, Germany, 1621. 8 + 152 + 2 pp. LCCN Z103 .T84 1621. Authore ... Ioanne Trithemio ...; praefixa est huic operi sua clausis, seu vera introductio ab ipso authore concinncata ... nunc vero in gratiam secretioris philosophiae studiosorum publici iuris facta. Darmbstdij. Ex officina typographica Balthasaris Aulaeandri, sumptibus vero Ioannis Berneri, bibliop. Fran- cof., anno 1621.


Theodore Ts'o. Mi-

**Tokita:1995:LCL**


**Tombak:1993:ACP**


**Tsujii:1992:CS**


**Thomlinson:1998:NBP**


**Tsudik:1989:DAI**


**Tsudik:1992:MAOb**


**Tsudik:1992:MAOa**

Thersites:1984:IKE


Thomas:1984:IKE


Tiountchik:1999:RAF


Tual:1999:MGA


Tuchman:1966:ZT


Tuchman:1979:HPN


Tung:1999:KNA

Turing:1941:APC


Turing:1941:SR


Turing:1999:TTE

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

Tijdeman:1992:CDP


Tel:1994:DAI


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).


References


USWD:1924:EC


USASC:1940:CML


USASC:1942:ACC


USDOS:1970:BC


USNBS:1977:DES


USCSC: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 United States, Washington, DC, USA. 1979. ?? pp. [Uni82b]


REFERENCES


USGAOPEMD:1987:PDD


USDA:1988:CED


USNBS:1988:DES


USNSACSSCCH:1992:FLT


USDOA:1994:OMT


USDOA:1994:UDS

United States. Dept. of the Army. Unit and direct support maintenance manual for trunk encryption device KG-94 (NSN 5810-01-187-
REFERENCES


United States Patent and


REFERENCES


**USCHCIR:1998:HEI**


**USCHCIR:1998:MHS**


**USCHCIR:1998:HSF**


**USCHCIRSIEPT:1998:EIR**


**USCHCIRSIEPT:1998:HSF**

REFERENCES


Shipping list no.: 98-0120-P.

USCHCNS:1998:HSF


USCSCCST:1998:HEH


USCSCJ:1998:HED


USCSCJ:1998:HEK

REFERENCES


[USE88b]


[USE89a]


[USE89b]


[USE89c]


[USE89d]


[USE89e]

REFERENCES

USENIX:1990:USI

USENIX:1991:PWU

USENIX:1992:PWU

USENIX:1992:USI

USENIX:1993:USI

USENIX:1994:PSU

USENIX:1995:PUT

USENIX:1995:PFUa

USENIX:1995:PFUb


USENIX:1996:SAC


USENIX:1996:WEC


USENIX:1996:CSW


USENIX:1996:PSUa


USENIX:1996:PSA


USENIX:1996:PUA


USENIX:1996:USS

[USE96g] USENIX Association, editor. 6th USENIX Se-
REFERENCES


REFERENCES


REFERENCES


**vanTilborg:1988:IC**


**VanTilburg:1993:SKE**


**VanOorschot:1995:DCS**


**VanTilborg:1995:ACA**


**vanRenesse:1996:OSC**


**vanDijk:1997:MIT**


**vanRenesse:1997:ODS**

REFERENCES

Includes CD-ROM.

vanderLubbe:1998:BMC


Varaiya:1999:DSI


Varma:1999:IDD


Vaudenay:1993:FHI


Vaudenay:1995:NMC


Vaudenay:1996:WKB


Vaudenay:1998:CCC


Vaudenay:1998:PSB


Vaden:1996:ETU


Viswanathan:1999:PVK


Vally:1999:CRC


Vandewalle:1990:ECC


Dijk:1995:LCP

vanDijk:1995:LCP

Dijk:1997:SCB

Vandermeulen:1999:ADM

Lubbe:1998:BMC

Wal:1997:PBR

Vedder:1993:SAM

Vedder:1998:GSS


REFERENCES


**Vincent:1971:PAG**


**Vincent:1972:CPA**


**Vandenwauver:1998:SIE**


**Voydock:1983:SMH**


**Voydock:1984:SMT**


**VanRompay:1998:DCI**

REFERENCES


REFERENCES

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073181.html

Four volumes.

Venkataraman:1994:PAM


Venkataraman:1995:CEA


IEEE Catalog Number 95CH35760.

vanOorschot:1991:CPP


vanOorschot:1992:CPP

REFERENCES

Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992.


vanOorschot:1996:DHK


Voyatzis:1996:ATA


Voyatzis:1999:PDI


Varadharajan:1997:ISP

Vijay Varadharajan, Josef Pieprzyk, and Yi Mu, editors. Information secu-

ciety Press order number PR08141. IEEE Order Plan number 97TB100179.


[VV85] Umesh V. Vazirani and Vijay V. Vazirani. Efficient and secure pseudo-
random number generation (extended abstract).
In Blakley and Chaum [BC85], pages 193–202. CO-
DEN LNCS9D9. 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 http://www.springerlink.
com/openurl.asp?genre=
article&issn=????&volume=
0&issue=0&spage=193.

Valiant:1986:NED

L. G. Valiant and V. V.
Vazirani. NP is as easy
as detecting unique solu-
tions. Theoretical Com-
puter Science, 47(1):85–93,
???? 1986. CODEN TC-
SCDI. ISSN 0304-3975
(print), 1879-2294 (elec-
tronic).

Verheul:1997:CLS

Eric R. Verheul and Henk
C. A. van Tilborg. Crypt-
analysis of “less short” RSA
secret exponents. Applica-
table algebra in engineering,
communication and com-
CODEN AAECEW. ISSN [vW94]

Vandemeulebroecke:1990:SCB

André Vandemeulebroecke,
Etienne Vanzieleghem, Tony
Denayer, and Paul G. A.
Jespers. A single chip 1024
bits RSA processor. Lect-
er Notes in Computer Sci-
ence, 434:219–??, 1990. CO-
DEN LNCS9D9. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/0434/04340219.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340219.
pdf.

Verheul:1997:BEF

Eric R. Verheul and Henk
C. A. van Tilborg. Binding
ElGamal: a fraud-
detectable alternative to
key-escrow proposals. Lect-
er Notes in Computer Sci-
CODEN LNCS9D9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL http:
//link.springer-ny.com/
link/service/series/0558/
bibs/0434/04340219.htm;
http://link.springer-
ny.com/link/service/series/
0558/papers/0434/04340219.
pdf.

vanOorschot:1994:PCS

P. C. van Oorschot and


Weidenbach:1999:SDS


Wobber:1993:ATO


Wobber:1994:ATO


Wade:1993:SLV


Wadsen:1998:CLI


Wagner:1983:F


Wagner:1998:DCK

D. Wagner. Differential cryptanalysis of KHF. *Lecture Notes in Computer Sci-
REFERENCES

ence, 1372-293–??, 1998.
CODEN LNCS:DC. ISSN
0302-9743 (print), 1611-
3349 (electronic).

[Wag99c]

David Wagner. Crypt-anal-
thesis of some recently-
proposed multiple modes of operation. In Vaude-
nay [Vau98e], pages 254–
269. CODEN LNCS:DC.
ISBN 3-540-64265-X (pa-
perback). ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). LCCN QA76.9.A25F77
berkeley.edu/~daw/multmode-fse98.ps

[Wag98b]

D. Wagner. The boomerang attack. In Knudsen
[Knu99c], pages 156–170.
ISBN 3-540-66226-X (soft-
cover). LCCN QA76.9.A25
F77 1999 Bar.

[Wag99a]

David Wagner. Cryptanalysis of FROG. In National
Institute of Standards and Technology [Nat99b],
page ?? ISBN ???
LCCN ???.
URL http://csrc.nist.gov/
encryption/aes/round1/
conf2/aes2conf.htm;
http://csrc.nist.gov/
encryption/aes/round1/
conf2/agenda-final.pdf;
http://www.nist.gov/
aes. No slides for the con-
ference talk are available.

[Wag99b]

Samuel S. Wagstaff, Jr.
Cryptanalysis. In Atallah
ISBN 0-8493-2649-4. LCCN

[Wagstaff:1999:C]

M. Waidner. Unconditional
sender and recipient unre-
traceability in spite of active
attacks. In Quisquater and
Vandewalle [QV90], page ??
CODEN LNCS:DC. ISBN 0-
387-53433-4 (New York), 3-
540-53433-4 (Berlin). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
QA76.9.A25 E964 1989;
DM98.00. URL http://
www.c1.cam.ac.uk/~fapp2/
steganography/bibliography/1024.html.

[Waidner:1990:USR]

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

[Waite:1995:BRB]

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

Wallace:1990:PRG


Wallach:1994:WP


Walton:1995:IAS


Walther:1998:VBE


Walker:1999:CCI


Wallich:1999:HSM

as US$45M from bogus US$19.95 transactions.

**Walter:1999:MTI**


**Wen-Ai:1994:MTS**


**Wang:1986:SEA**


**Wang:1992:CDI**


**Wang:1992:DKT**


**Ward:1998:ASE**


**Watler:1989:VAC**

Wayner:1993:ECD


Wayner:1993:SER


Wayner:1995:PCL

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

Wayner:1996:DCB

Peter Wayner. *Disappearing Cryptography: Being and Nothingness on*

Wayner:1996:DLY


Wayner:1998:MJD


Willcox:1992:TCS


Wagner:1994:PPR


Wolf:1995:ICR


Whittle:1999:SDC


Wallach:1997:ESA

[WBDF97] Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Extensible security architectures...

**Wu:1998:CRP**


**Wegman:1981:NHF**


**Wynn:1997:CTS**


**Weeks:1995:CBW**


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

**Wolfgang:1996:WDI**


Three volumes. IEEE catalog number 96CH35919.

**[Web98]**

Weber:1998:SMD


**[Webb:1988:NPK]**


**[Web93]**

Wendling:1993:PRS


**[Web:1998:SWY]**

Wedemeijer:1999:DFM


Weiss:1988:BOP


Weissman:1991:IRA


Weissman:1991:IRN


Weierud:1994:SPB


Weierud:1998:C


Weierud:1999:TJG


Wells:1980:ADB

David L. Wells. Achieving data base protection through the use of sub-key encryption. Thesis (Doctor of Engineering), University of Wisconsin-


[Wernsdorf:1993:OFG]

[Wernsdorf:1993:ORF]


[Wagner:1999:CFa]

[Wilkes:1982:MRJ]

[Worley:1994:PST]


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


**Wang:1999:CTG**


**Watanabe:1999:SGR**


**Wichmann:1987:NAR**


**Wichmann:1990:CMR**


**Wiedemann:1986:QC**


**Wiener:1990:CSRb**


**Wiener:1990:CSRa**


Wiener:1994:EKS


Wiener:1996:EKS


Wiener:1997:EKS


Wiener:1998:EKS


Wiener:1998:PCP


Wiener:1999:ACC

REFERENCES


[Wil83b] M. H. Williams. The problem of absolute privacy. *In-

[Wil85]


[Wil86a]


[Wil86b]

[Wil86c]


[Wiles:1993:HBE]

Gary Scott Wiles. Hardware based encryption for the personal computer using the Data Encryption
REFERENCES


Williams:1993:CPK


Wilcox:1998:SBW


Williams:1998:C


Winterbotham:1969:SP


Winterbotham:1974:US


Winterbotham:1974:USF


Winterbotham:1975:US


Winterbotham:1978:NC

REFERENCES


G. Wedel and V. Kessler. Formal semantics for authentication logics. Lecture Notes in Computer Science, 1146:219–??, 1996. CODEN LNCSD9. ISSN 0302-9743
REFERENCES


**Wheeler:1995:TTE**


**Wheeler:1998:CX**


**Wright:1998:NTD**


**Woehr:1997:CRR**


**Wolfe:1943:FCCa**


**Wolfe:1943:FCCb**


**Wolfe:1943:FCCc**


**Wolfe:1970:SWC**

Wolfe:1983:FCC


Wolfowicz:1993:SPR


Wolfowicz:1993:SPS


Wolf:1998:SSAb

Wolf, S. *Strong security against active attacks in information-theoretic secret-key agreement.* Lecture Notes in Computer Science, 1514:405–??, 1998. CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wolf:1999:USC


Woolsey:1990:DDE

Woolsey, Matthew A. *Digital data encryption techniques with application to computer software access authorization.* Thesis (M.S.E.), University of Arkansas, Fayetteville, Fayetteville, AR, USA, May 1990. viii + 125 pp.

Worth:1975:CMA


Wortmann:1987:BRB

REFERENCES

**World:1996:NIT**


**Wotawa:1999:NDD**


**Waidner:1990:DCD**


**Wrixon:1989:CCS**


**Wright:1994:IRV**


**Wrixon:1998:CCO**


**Williams:1979:SRC**

REFERENCES


[Wagner:1996:ASPa]

[Wagner:1996:ASPb]

[Wiese:1996:SSS]

[Wagner:1997:ASP]


[White:1999:CBA]
S. White and D. Sleeman. A constraint-based approach
REFERENCES

842


[Wagner:1998:CO]


[Wagner:1999:CO]


[Weatherford:1999:NGA]


[Wagner:1997:CCMa]


[Wagner:1997:CCMb]

REFERENCES


URL http://link.springer.com/link/service/series/0558/tocs/t0218.htm;
http://www.springerlink.com/content/978-0-387-16463-2;

http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/0Reilly.pdf;


Chih-Kuo Wu. Group oriented cryptosystem and


[WWH95] Tzong-Chen Wu, Tzong-Sun Wu, and Wei-Hua

Wu:1993:CSB


Wiener:1999:FAE


Xie:1992:PEC


Xie:1993:IPK


Xie:1998:BWB


bibliography/073183.html

Four volumes.

Xie:1997:MWD


Xie:1998:WDI

REFERENCES


[Xac99a] Y. Yacobi. Risk management for E-cash systems

Yacobi:1999:RME


Yahalom:COMPSYS-7-4-451


Yamamura:1998:PCU


Yamamura:1998:PKC


Yamamura:1999:FCU


Yan:1995:PTL


Yao:1982:PSC


Yao:1982:TAT

[Yao82b] A. C. Yao. Theory and application of trapdoor func-
REFERENCES


Minerva Ming-Yee Yeung. Digital watermarking for


269–??, 1999. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES

Yang:1999:DIC


Yen:1993:FCE


Yen:1995:IDSb


Yen:1995:IDSa


Yang:1997:NEC


Yen:1997:SAT


Yi:1997:NHF

REFERENCES

LnCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


REFERENCES

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


REFERENCES

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

Yung:1985:SUK


Yuval:1997:RTE


Yang:1997:CBC


Yu:1989:DEB


Yu:1991:SED


Young:1996:DSB

A. Young and M. Yung. The dark side of black-box cryptography, or: Should we

REFERENCES


[Zaf63] Jean Zafiropulo. Le rôle de l’analogie dans le
REFERENCES


Zajacz:1997:SCE


Zang:1990:ESE


Zave:1999:SDC


Zegwaart:1993:PEM


Zei79


Zer96b


Zollner:1998:MSS

J. Zöllner, H. Federrath, H. Klimant, A. Pfitz-

Zoellner:1998:MSS


Zuquete:1996:TAC


[ZH90]

Zhang:1991:BNK


Zhao:1996:WSE


Zhao:1997:LT


Zhang:1998:TPS


Zheng:1990:PDS


Zheng:1995:HBR


Zheng:1995:KAP


Zheng:1997:SC


Zheng:1997:DSH


Zhilouchian:1998:ANF

REFERENCES

Zhou:1994:SDS

Zheng:1994:RSS

Zheng:1998:HCE

Zieschang:1997:CPB

Zim:1948:CSW

Zimmermann:1995:OPU

Zimmermann:1995:PSC
REFERENCES


Zimmermann:1996:PGPa


Zimmermann:1996:PGPb


Zimmermann:1998:Cl


Zimmermann:1999:EI


Zhao:1995:ERL


Zhao:1996:DWS

[ZK96] Jian Zhao and Eckhard Koch. A digital watermarking system for mul-
REFERENCES

862


Zhao:1998:GDW


Zhao:1998:BTT


Zhao:1999:DWW


ACM order number 428990.

Zeng:1997:RRO


Zhou:1999:SPP


Zhang:1999:AFV

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


Zwiggelaar:1999:DCM

Zukowski:1998:JTUb

Zukowski:1998:JTUa

Zunic:1998:MCI

Zwiers:1998:CTD

Zeng:1990:LCT
REFERENCES


