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

23 May 2015
Version 1.233

Title word cross-reference

(2, 2) [KSSY12]. (k, n) [YC11]. (n, t, n) [LHYZ12]. 2 [DBPS12, ESS12, JR13, MCDB12, PGLL10, WY12]. 22 [MNP12]. 3 [AP10, CG12b, DWWZ12, FWS13, GZHD12, GH11a, KWS+12, LJ15, MKH+12, SS10a, SS12a, SGS14, WSSO12, tWmC12, YT11a, YI14]. 3 [AMVZ12]. 4 [COP14, DWZ12, HLYS14]. $49.00$ [Sch15a]. $9$ [APPVP15]. = [JJUW10]. 3 [LHM14]. α [TTL10]. c [KRDH13]. t [ZTL15]. γ [DWZ12]. GF((2)[x] [SF12]. GF((2^m) [SKH15]. GF(2^μ) [LBOX12]. K [FXP12, CHX13]. L(1/4 + α(1)) [Jou13]. M [MMSD13]. F_{35569} [AMORH13]. F_q [SS13]. N/P [HN10]. GF(q) [LPdS10]. LWE [BV14]. μ [Jia14a]. $n \times k(k \geq n/2)$ [MC11]. O(n^2) [KS11]. ±1 [HZW+14]. q [GMS11]. S [LJ15]. t [HJM+11, Oba11]. w [Kre13].
/ [Ran10, Ran14].

0.13um [KLM+12].

1 [AAE+14, Ful10, MSas12]. 1—58488—551—3 [Ful10], ‘10 [Ano10], 10th
LGL+12, LLY+12a, LWCJ14, MD12b, MNP12, NDNR13, SEY14, SD12, TLL13, WHN+12, Yon12, ZLQ15. **Age** [Bla12, Sto12]. **Agency** [ABJ13, agent [GPVCdBRO12]. **Aggregate** [CCT+14, LLY15, ZQWZ10]. **Aggregated** [NLY15]. **Aggregated-Proof** [NLY15]. **Aggregating** [DP12]. **Aggregation** [LHKR10]. **Aging** [SKV12]. **Agreement** [HCL+14, HEC+12, MNS11, TM12, WSS12, XLM+12, XGLM14, BGAD12, CTL13, IB11, KS11, LLLS13, LLY06, Nos11, Nos14, TLL12, XCL13, XMHD13, YZZ+14, ZWQ+11, OHJ10]. **Aided** [BGK12, BCGK12, BGB12, GMSV14, Vua10, ABBD13, SSAF11]. **AK** [XHC+12]. **AK-PPM** [XHC+12]. **AKA** [LLLS13]. **AKF** [KDH15]. **al** [MWZ12, PLPW13, SBS+12]. **al.** [ABJ13]. **Alan** [CS12, Don14, LCKBJ12]. **Algebra** [Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14]. **Algebraic** [Gas13]. **Algorithms** [AB10b, BCG12a, BJ10, CN12, KRDH13, MR14a, TKM12, ZW15, Fri0a, Mac12, NC13, Xie12]. **Ali** [ABJ13]. **Alignment** [Don14]. **all-seeing** [Tox14]. **Allowing** [PRC12]. **Almost** [FFL12, Oba11]. **Alterna** [SMOP15]. **alternate** [ZW+12]. **Alternating** [BKLS12, KDH15]. **AMBTC** [KSSY12]. **America** [AB10a]. **American** [Sch15a]. **Americans** [ABJ13]. **among** [BP11]. **amount** [EEAZ13]. **Amplification** [ABF12, HMR14]. **Analog** [KOP12]. **Analysis** [GRL12]. **Analysis** [ABS+12, ARP12, BC14, BS14, CGL+12, FSWF11, GZZ+13, GLG12, HC12, HHH+13, IBM13a, IS12, KOP12, Kre13, LPS12, LCK11, LGLL12, MD12b, MRTV12, MR10, NDC+13, NSA15, PH12a, PFS12, RZZ+15, Rao10, SR12a, Shi11, SZDL14, SCGW+14, VKC15, WDDW12, YZLC12, ZH15, CFH+13, DHW+13, DMT12, FTV+10, FHM+12, HM10, MFH13, NLYZ12, RITF+11, TQL+14, TLMH13, Tso14, Ven14]. **Analysis-Based** [RZZ+15]. **Analytic** [Kuz11, Sha10, Shp03, ZW15]. **analytical** [TKMZ13]. **Analyzing** [HREJ14]. **Ancient** [Fox13, Rao10]. **and/or** [YLA+13]. **Android** [Chi13b, EBFK13, FHM+12, SFE10]. **Android-Powered** [SFE10]. **Anisotropic** [ZZCJ14]. **Annual** [Ano10, IEE10, IEE11b, PJ12, Gil10, Rab10]. **Anonymity** [CDFS10, HEC+12, MR10, SCGW+14, BAG12, HLR11, Par12b, WW14, ZK11]. **Anonymity-Based** [HEC+12]. **anonymization** [XTK10]. **anonymized** [BDK11, TG12]. **anonymizing** [TMK11]. **Anonymous** [CG12a, CZL12a, Chi12, DK12, FHM10b, LZC14, Per13, RSN14, TAKS10, Wan14, ZJ14, ATK11, CCSW11, Chi13a, CGH11, FSGW12, HL14, LHM14, LY14, MYYR13]. **ANSI** [Ano11b]. **anti** [QZ14]. **anti-forensics** [QZ14]. **Antispoofer** [MR14b]. **Antoine** [AY12]. **Apache** [Lit14]. **API** [FLW12]. **Append** [YNR12b]. **Append-Only** [YNR12b]. **Application** [AKP12, AK14, BRT12, CKLM13, CCW+10, CLCZ10, CHS15, Kiep15, LW11a, LWKP12, MNS11, O012, SEHK12, SS13, YWK10, YTS12, ZH15, Abe10, BBBP13, GLIC10, Jia14b, LGKY10, LWKP14, XHH12, YY11, ZWQ+11]. **Application-Level** [CCW+10].
Applications [ÁMVK12, Ana14, BKPW12, BCG+12b, BSV12, CZL12a, CZL12b, DK02, DK07, FSK10, GRL12, HvS12, HN10, Nac12, Nie02, PJ12, SCPSN10a, SCPSN10b, Sha10, Shp03, Ter11, TYK+12, YR11, Ano11a, CFR11, CSZ+11, CDA14, Dur15, EBK13, FES10, Fri10a, Gil10, LR15, LBOX12, LTT10, MI10c, MM14b, NV10].

Applied [BSS11, MR10, Xie12].

Applying [Bar12, Elb09].

Approach [HLAZ15, HLW12, MKN13, RP12, SLGZ12, Sia12, SH15, SC12, TLW12, Vle12, VKC15, WYCF14, ZW15, AT10, BSS11, CO11, DZS+12, KL13, LGCGCRP14, MCP15, NC13].

Approaches [LC15, SBV14, MKH+12].

Approximate [CN12, SGS14].

April [GLIC10, PJ12, vDKS11].

Arab [Bro11].

Arbitrary [FHR14, DWZ12, Gen10].

Arbitrary-State [FHR14].

Arbitration [Kip15].

Architectural [MD12b, VCK+12, ZWT13].

Architecture [BCE+10, HKL+14, KCR11, LGR14, MCDB12, MJGS12, MC11, RMP10, SWM+10, SLI11, Ao11b, BV1B12, LXMW12, MJ13, SSS13, SSPL+13, SAB10].

architecture-independent [BV1B12].

Architecture [BGG+13, CHS15, FPBC14, HL14, MK11, Nov10].

Area [LZCK14, LMJC11, Nov10].

Areas [MV12, YJ14].

Arguments [BC1+13].

ARIA [PH12a].

Arithmetic [A1K14, Frel0, GH11a, HSA14, KHF10, PG12, DZZ12, MO14].

Array [BL12, MCDB12, NKWF14].

Arrays [LB13, TRD11, KM10a].

Art [ABJ13, BDK11].

ARX [KN10].

ASIACRYPT [LW11a, Abe10].

ASM [Vle12].

ASM-Based [Vle12].

ASP.NET [DR11].

Assessing [CBL13].

Associated [Sar10b].

associative [BS15].

 Associativity [ABR12].

Assumption [LZC12a, LZC14, ZG10].

Assumptions [CZ12, DN12, KM10c, ABW10].

Assurance [KMP+11, WL11].

Assured [Tan15].

Asymmetric [HG12, XLM+12, XGL14, ZWQ+11, CSS+13].

asymmetric-histogram [CSS+13].

asymptotic [DTZZ12, TD14].

Asymptotically [LPS12].

Attack [BMS12, DS15, zGXR12, GV14b, HCTPT1+12, HLA15, JH12, JKP12, LGL+12, LWK12, LWPF12, Pud12, SP13, SDM+12, WLC12, XJWW13, DDFR13, FLZ+12, Goo12, LLY+12a, LC13, LYHH14, LWK14, MB11, MN1, NZL+15, WYL13].

Attacks [ARP12, BGG12, BKBK14, Che15, CMA14, DGI12, DHLAW10, EWS14, GPT14, Hay13, N10, LLC11, LWZ12, LW14, MD12b, PYM+13, PS12, Sac12, SEY14, SP15, SH15, WW14, WHN+12, YCM+13, ZLQ15, BBBBB13, BV1B12, BSR+14, dCCSM+12, DCAT12, DJL+12, EA12, FTV+10, GBNM11, KM10a, KPS10, LW11, ND13, PX13, TLL13, WWBC14, WWD12].

attempt [Fel13].

ATtiny [EGG+12].

Attribute [AHL+12, BFK+10, Boy13, FHR14, GZZ+13, Gil12, HSMY12, HR14, KGP12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, OT12, PB12, SSW12, XML13, ZHW15, YCT15, ZWM14].

Attribute-Based [BFK+10, Boy13, FHR14, GZZ+13, HSMY12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, PB12, SSW12, XML13, AHD+12, HR14, YCT15].

Attribute-Hiding [OT12, ZWM14].

Attributes [CG12a, Yon11].

Attribution [XH+12, FNP+15].

Auction [Con10, HJM+11].

auctions [MR14c].

Audio [DA12, GCK12, KD12a, KD12b, LSL12b, TC10, ZS12, LSQ11, yWpNyL11, YQH12].

Audit [YN12b].

August [AB10a, JY14, MV12, Rab10].

authentic [SZMK13].

Authentic [HM12].

Authenticated [Alo12, BCO13, CLY14, CCS14, CRE+12,
DS11, EAA12, FFL12, GTT11, GL12, GZ12, HC12, HL10a, HCL+14, HEC+12, LH11b, LC13J, LTT11, MR14a, MMY12, MHKS14, MSU13, Sar10b, Smi11b, TW14, XLM+12, XGLM14, YS12, YLW13, Yon12, CTL13, FA14b, GPN+12, HL11, LWS10, LHH11, LML+13, Nos11, Nos14, PPTT15, SMBA10, TCS14, Tso13, TKHK14, WZM12a, WZM12b, WTT12, WXCl14, XCL13, YC12, YZZ+14, ZG10].

Authenticating [CHX13, GRL12, OKG+12, RPG12, WY12, LFGCGCRP14, PGLL10].

Authentication [ASO14, BL12, BCE+12, BCM12, BSSV12, BCD+12, BF11, BJKP12, BSV12, CGCGPDMG12, CCW+10, CJ13, CD12, CLH13, DBPS12, DFKW12, DP12, FLH13, FMTR12, FD11, GHS14, Gli12, GI12, GM14, GU13, GCK12, HZC+12, HvS12, HLLC11, Har13, Hay13, HBC13, HM10, HCPLSB12, HETPL+12, HKL+12, HX+11, HCL11, JN12, JCM12, JAE10, KP12, KPC+11, KLY+12, KTA12, GKP12, KPKS12, KLM+12, KH10, LCC11, LCLL15, LN+13, LZCK14, LNX15, LLZ+12, MWZ12, MEFO12, MKH+12, MLBL12, Mor12, NR12, NLLJ12, NLY15, OdH12, OO12, OS12, PCDG14, PPRT12, PDT12, PWVT12, RS11, RWL11, RSN14, Saa12a, SBS+12, Sar12, SKV12, ST14, SD12, Shi11, SGC14, SSA13, SC12, SZDL14, SHS12, SAA12b, TYK+12, TM12, Vet10, WgmDZ1Z12, WHZ12, WZXL12, WgMW12, WSS12, WT10b, Xio12, YTP11, ZBR11, ZLDD12, ABK13, AZF+12, ACM12].

authentication [BS13a, BGAD12, BAL10, BMM12, BM11, CLM+12, CFF13b, CT12, CH10, CCSW11, CHS11, CLHJ13, CZ15, Chi13a, Chol14, CL11, DCAT12, DSCS12, DLN13, DZ12, DMT12, EA12, EA11, FPBG14, FHH10a, FLL+14, FXP12, Far14, FA14a, GI13, GMSW14, GCSAdD11, HDP1C, HZC+14, HL14, HCC10, HS11, IG11, IB11, JAS+11, KKG14, Kim11, LLLS13, LLY06, LH11a, LT13, LH10c, LNM+11, LMJC11, LXM12, LNKL13, LJJ14, LHM14, LH13, Lt14, LWL11, LBR12, LTT10, MM12, Mk12a, NCCG13, NLYZ12, NB13, OCGS11, OYHS14, PYP10, Par12b, PA10, Sar10a, SA15, SSS11, Tan12b, TLL12, Wan13, WW14, WT10a, WKH11, XHH12, XWDN12, XHC14, XMH13, YSL+10, YMM13, ZYL+10, ZW120, ZCLL14, XZ11, OHJ10].

authentication-chaining [EA11].

authenticity [ADF12].

Authority [LNXY15, JB11, ZZ12].

Authorization [CS14, JAE10, JAS+11].

authorship [BAG12].

Automata [Gas13, dRSdI1C12, SS11, WOLS12].

automata-based [SS11].

Automated [CCK12, GLLS12, YSS14, BJR+14].

Automatic [WW12].

Authentication [BGK12, IEE11a].

Auxiliary [DL12, XXZ12, YCY12].

Auxiliary-Input [XXZ12].

availability [ADF12].

average [Lim11, YL11].

avoid [CFZ+10].

avoiding [BHCdFR12].

Aware [LMHH14, MGP10, Wan13].

Awareness [MSas12, Li10].

axiomatic [AT10].

B [Tan12a].

B-Spline [Tan12a].

Back [YZLC12, Ran10].

Backdoor [Sch13, Fel13].

backup [Cor14a].

backward [BM11].

Bacterial [Kar12].

bad [RY10].

BAF [YNR12a].

Balanced [YTP11].

balancing [FXP12].

Ballots [CW12b, LHF12].

balls [Svo14].

band [MMSD13].

Bandwidth [GST13, LLZ+12].

Bandwidth-Eficient [LLZ+12].

Baptiste [Dew11].

Barbara [Rab10].

Barcodes [WY12].

Barrier [JR14, KS11].

barriers [LKL13].

base [MS12, XSWC10].

Based [ADM12, ASM12, Ano11b, ASS15, BL12, BSSV12, BHH12, BKPW12, BRT12, BS13b, BFK+10, Bon12, BS15, Boy13, BKPJ12, BCF+14, CGMO14, CZLC12a, CZLC12b, CLHC12, CLY14, CZLC14, CGL+12, CDD13, CD12, Chi12, DSSM14, DA12, EM12,
Based on [RR11, RVRSCM12, SSW12, SS13, SJ12, SGP12, SSA13, SH15, TKR14, TWZ11, TW12, TWZ1+12, TT12, TTH15, TC10, Vle12, Wan10, WSSO12, WgMW12, Wan14, WT10b, WMS1+12, XXZ12, XMLC13, Xio12, XGLM14, YE12, YZLC12, YZX1+12, YGF15, YTS12, YKNS12, YMWS11, YCZY12, ZZJ1, ZZX1+11, ZDL12, ZLH1+12, ZHW15, ZHL15, AY1+1a, ASO14, AKG13, ASVE13, AHI1+12, BS15, BBBP13, BGAD12, BAAS13, BOB13, BWR12, BW13, BWA1, BMIM12, BK12b, CFY1+10, CQLL11, CTR1, CLS12, CG12b, CSZ1+11, CX13, CSS1+13, CW14a, CTHP13, CCG10, CT13, Chol14, Con12, dCCSM1+12, Cra11, DSCS12, DZ14, DNN13, EZ15, FHI13, Far14, FA14a, FA14b, Gal13, GJ13, GMRT1+15, GKCK11, GCSAdP11, GMS11, HT11, HGWW11, HSM13, HZC1+14, HF14a, HLRI11, Her14, HB13, HL14, HLI11, HLC12, HYWS11, HCC10, Hwa11, IM14, IB11, JK13, JLT1+12].

Based on [ZHW15]. Bases on [EVP10, TSH14, FES10]. Basing on [Mat14, MN10]. basis on [CG12b].

Based on [CCG10]. batch-based on [CCG10]. Batters on [Ch13b]. battles on [Sch15b].


Based on [DSMM14, Par12a, AZH11, Ana14, RK11]. BECAN on [LLZ1+12]. Becomes on [Bra13].

been on [Ana14]. before on [GST12, Goo12]. behavioral on [HT11]. Behind on [Fre10].

Beijing on [BYL10, Yan10]. Beissinger on [Ayu12]. Belief on [BT12]. Benford on [AOT13].

Bessel on [GJ13]. Beth on [CH13]. Between on [LRW14, CLM1+12, HLRI11, PBCC14, WDDW12].

Beyond on [LST12, MJS13, FNP1+15, JR14]. BGV on [GHPS12]. BGV-Style on [GHPS12].

Biclique on [BKR11, KDH13]. Big on [Mal13, LSBN14, WS14]. Biggs on [Low12].

bilateral on [JT12]. Bilinear on [AHC12, ASS15, YS12]. billions on [SBMA10].

Binary on [AD11, AK14, MBR15]. Binary-Ternary on [AD11]. Binding on [HEC1+12, ZLQ15]. bio on [GPVcBro12].

bio-inspired on [GPVcBro12]. Biometric on [DBW12, JN12, KHMB13, Sar12, SKV12, Vet10, DIMT12, GCSAdP11, HT11, LK12, MLBL12, Sar10a, SR10]. biometric-based on [SR10]. Biometrics on [BW13, SP13, LXYL12, LH10c, LNM1+11].

capability [LT13]. capacity
[GZHD12, PWLL13, WH13]. Capture
[NYS+14]. Card
[BDFK12, HMR12, HCL+14, PDT12,
CLHJ13, GLIC10, LNLK13, Cho10, SD12].
CARDIS [GLIC10]. Cards [BSJ15, LA10,
PWVT12, WgMdlZ12, WgMW12, CHS11,
HCC10, KY10, LH10c, LNM+11, LXWM12,
MM12, YZZ+14, YSL+10]. Carlo [CR12].
Carol [Xie12]. Carved [LC15].
Cascading [GT12]. Case
[DR11, SBS+12, LKKL13, MD12a]. Cash
[YMWS11]. Casting [CW12b]. cat [Pow14].
CCA [CZLC14, MSA12, SYL13, SLZ12].
CCA-Secure [CZLC14, SYL13]. CCA2
[Gal13, GV14b, MVVR12, RG10, ZZ12].
CCM [SKK10]. CDH [ZG10]. cell
[LLY+12a]. cell-counting-based
[LLY+12a]. Cellular
d[RSlV12, SS11, WOLS12]. centre
[McK10, McK11]. Centric
[BC11, BP10, PN10]. centroid [LWY12].
Centuries [Gri15, McG11]. Cerf [Cer15].
Certificate [HP12, LTH+15, WMS+12,
BJR+14, Lan13, MBB+13, NPH+14, JB11].
Certificate-Based
[HP12, LTH+15, WMS+12]. Certificateless
[LZCK14, SZS14, TCL15, WMS+12, YT11a,
YT11b, ZQWZ10]. Certificates
[SC12, GLJ+12, HREJ14]. Certification
[LDB+15]. Certified
[ABBD13, STC11, HL14, LH13, WXW14].
CertShim [NPH+14]. chaff [KHM13].
Chain [KWP13, CR12]. chaining [EA11].
chains [HLYS14]. Challenge
[AD12, GHS14, ZCC15]. Challenges
[CN12, Fra15, SBV14, WS14]. change
[ZWT13]. Changeable [FGM10, ZCL+12].
changed [Mac12]. Channel [ASN11,
CDK+10, CBL13, EWS14, GPT14, KOP12,
LRG14, NDC+13, PRC12, TT12, BVIB12,
DMWS12, DJL+12, JLT+12, MFH13].
Channels [ASN12, KW14, Vua10, SRB+12].
Chaos [LW13c, RR11, RVRSCM12,
CCL11, LW13b, JLT12, ZLW+12].
chaos-and-Hamming [CCL11].
Chaos-Based
[RR11, RVRSCM12, LW13c, ZLW+12].
Chaotic
[BCGH11, NES+14, WZG+12, ZT14].
Chapman [Full]. Character [SS12b].
Characteristic
[BGJT14, SR10, BGJT13, Jor13].
Characterization
[ALR13, BS13b, YZLC12, DDD14].
Characterizing [Ash14, JR13]. Chattarjee
[Kat13]. cheat [WS12]. cheat-preventing
[WS12]. Cheater [WI11, Oba11].
Chebyshev [LP1510]. Check [GST12].
Check-before-Output [GST12].
Checkability [LHL+14]. Checkable
[WI14]. Checking [FYMY15]. Chen
[LLLK10]. Chennai [BC11]. China
[BYL10, IEE11a, LTW11, Yan10]. Chinese
[LF14a]. Chip
[MDAB10, RAB+13, BGG+13]. Chips
[Man13]. Chirp [OWS12]. chocolate
[Svo14]. Choquet [SH11, SM11, SNM14].
Chosen [FSGW12, zGXW12, HLW12,
LCT+14, LZC12a, LLML12, MH14, RS10,
WWHL12, LZC14]. Chosen-Ciphertext
[RS10, FSGW12, LCT+14, LZC14]. Church
[ABJ13]. Cipher
[BCG+12b, DG12, DWWZ12, GLSN12,
GCS+13, HZ11, IOM12, JKP12, KWS+12,
LPS12, LWZ12, LWKP12, LWPF12,
MRTV12, MHC12, PH12a, PRC12,
WSSO12, WHN+12, AMS+10, CR12,
HT11, Hol11, Jor13, KDH15, Lew10, LC13,
LYHH14, LWKP14, MNP12, RS14, Sar11,
WYL14, WWBC14, LGL+12]. Ciphers
[ABS+12, BMS12, BKLS12, BrU12, CW12,
DG12, EGG+12, GT12, GST12, GNL12,
IS12, Kla10, LLL12, ML12b, NN12, Pud12,
Sas12, SEHK12, Vua10, WW12, Xie12,
ZH15, ZSW+12, Zha12, Bay10, Bla12, Bor10,
Die12, KM10a, LW11, MRT10, SKK10,
TQL+14, WB12]. Ciphertext
Ciphertext-Policy [XMLC13, ZHW15].
Ciphertexts [Sta12, AHL+12, LCT+14].
Circle [SC10].
Circuit [Kar12, MTY11, Lau12, MS13a].
Circuit-Size [MTY11].
Circuits [AIK14, BR14, GH11a, SS10a, SS12a].
Circumventing [BAG12].
CISSP [STC11].
Claims [SKGY14].
Class [BCG12a, XYXYX11, Goo12].
Classical [MSU13, CR12, RK11].
Classification [HPC10, SGP+12].
Classroom [Pow14].
Claudius [Hol12].
CLEFIA [LWZ12, TSL11, WB12].
CLEFIA-128 [TSL11].
CLEFIA-type [WB12].
Client [ASM12, FD11, Vle12, FA14a, FA14b, WT10a].
Client-Based [ASM12].
Client-Centric [Vle12].
client-server [FA14b].
clients [LH13].
cloaking [NZL+15].
Cloud [BCQ+13, CWL+14, CCT+14, DXA14, FCM14, JLS12, KMSM15, Kui+15, LA15, LYZ+13, LGR14, LL+15, LNY15, Pet12, RSGG15, Vle12, XMCL13, ZDL12, AZPC14, ASO14, BK12b, FH13, HSM13, Jee+13, KKA14, KKM+13, KKM+14, LXX+14, LW13a, NB13, PP11, SL10, TL1M13, WL12, YWT+12].
cloud-based [ASO14, BK12b].
Cloud-of-Clouds [BCQ+13].
Clouds [BCQ+13, RSN14].
Clustered [DS11].
Clustering [KRDH13, VSV15].
CMAC [SKK10].
Co [MBR15].
Co-Processor [MBR15].
cocktail [OH10].
Code [AD12, CCL+13, Fox13, HG12, KSSY12, PYM+13, SS13, War11, ABB13, Ant14, Bri11, CL1L11, GIJ+12, MCP15, MCG11, Mool14, PA10].
Code-Based [HG12, SS13, MCP15].
code-breaking [Ant14, Bri11].
Code-cracking [War11].
codebreaker [Car11].
codebreakers [Ano11c, Smi11a].
codebreaking [Cop10, McK10, McK11].
Coded [She14].
Codes [BBC+13, Bay10, BP06, Big08, DBPS12, FMV14, Gri15, KW14, MBR15, OTD10, SEY14, ST14, TL1W12, WSS12, Xie12, YTP11, Bul10a, CZ15, Chi13a, Hea15, LTT10, MG15, YSJL14, Ayu12, Low12].
Coding [Che11, CJ13, CG14, Hes12, LCLL15, Per13, AZF+12, Bul10b, DTZZ12, JZS+10, KM11, NDN+13, YTM+14].
CoDiP2P [NCCG13].
Coercion [CW12b].
Cognitive [PP11, Kim11, RPG12].
Coin [ALR13, CLP13a, DSMM14, Mat14, BB14].
Coins [Fok12].
Colbert [Dew11].
Collaboration [CRE+12, PCPK14].
Collaboration-Preserving [CRE+12].
collaborative [LLY06, LT14b, HB13].
collect [Sch15b].
Collision [BK12a, ZL12, AKY13].
Collision-based [ZL12].
Collision-Resistant [BK12a].
Collusion [MMS13, FLZ+12, GMRT+15].
collusion-resistant [GMRT+15].
Collusions [GV12].
Color [BCPV11, DD13, YNNW15, SNM14, yWpWyypN13, WGZ+12].
Colossus [Cop10].
combating [FTV+10].
combinational [MS13a].
Combined [PP10b].
Combining [Chi13a, PDF+10].
Coming [SG15].
Comment [LCLL15].
Comments [TCL15].
Commerce [HvS12, Ano11a].
Commitments [Pas13a, CSZ+11, LP11].
Common [CN12, ESRI14].
Communication [Big08, CCW+10, FMS12b, Gas13, GPVCdBO12, KW14, Low12, OKG+12, Wan13, ZC13, HCCC11, HLYS14, LT13, LyWSZ10, RK11, SSAF11, SSPL+13, Tso13, YLGK13, Zhn13, vDKS11].
communication-efficient [Tso13, Zhn13].
Communication-resource-aware [Wan13].
Communications [QO12, SMS14, FHH10a, LGCCRP14, WDZL13].
Commutative [CLHC12, SLGZ12].
Commutativity [ABR12].
Commuting [Fuc11, AKG13].
Compact
Comparison [DWB12, HPC10, KU12, ST14, HM10].

Compartmented [EZ15]. Compensation [JSZS12]. Competition [jCPB+12].

Compilation [CHS15]. compiler [LWS10].

Compiling [CR10]. Complete [Ash14, BS14, FLH13, GHKL11].

Completeness [FKS+13]. complex [BW13]. Complexity [BIKK14, BW12, DP12, Gas13, Shp03, DJL+12, Jon13, KGO10, LWW+10, SDM14].

Compliance [SOF12]. compliant [BP10].

Components [RITF+11]. Composable [DN12, KMO14]. Composing [TW14].


Computable [FWS13]. Computation [ARH14, Ash14, BDOZ11, Fri10b, GST12, GVW12, GHKL11, HP14, IEE11a, KW14, KMO14, LHM+15, MMP14, Mal13, NSMS14, PST13, WS10, AB10b, LDDAM12, TG12, vDKS11].

Computational [BCO13, TBCB15, HRS13, SDM14].

computations [BK12b, LR15, SSAF11, TLMM13].

Compute [Vai12]. Computer [BGK12, BCGK12, BGB12, Bu10b, Gas13, IEE10, IEE11b, LL15, Nie02, Ter11, Vua10, ABBD13, DK12, FGPGP14, Sta11b].

Computer-Aided [BGK12, BCGK12, BGB12, ABBD13].

Computers [Cop10, LCKBJ12, Mac12].


Conditionally [ZJ14]. Conference [BC11, CGB+10, Che11, Cra12, Dan12, Dun12b, FM12, GLIC10, IEE11a, JY14, LCK11, LW11a, LTW11, Lin14b, PJ12, SN11, Sah13, Yan10, AB10b, Abe10, BYL10, BL10, Gil10, GG10, HWG10, Kia11, LH10a, Pie10, Rab10, vDKS11].

Confidential [HS11, AZPC14].

Confidentiality [BFK+10, HLLC11, WDDW12, Bia12, CHX13]. Configurable [CVG+13]. Configurations [SS10a].


Consecutive [Tan12a]. consideration [KM10b]. Considerations [KD12b].

considering [MLMSMG12]. Consolidated [KKA14]. Constant [CWWL12, KMO14, LP11, Pan14, AHH+12, DWZ12, LCT+14].

Constant-Round [KMO14, LP11]. constant-size [AHL+12, LCT+14].

constants [DWZ12]. Constrained [BSJ15, EAA12, YNR12a, Yon12, KAS15].

Construct [SGY11, WT13]. Constructed [ZH15]. Constructing [CDSLY14, ZSW+12, HRV10].
Construction [DF11, EM12, FZT14, KMO14, MSas12, Sar10b, ST14, WZ15, WMS+12, YT11b, YKC+12, ZCLL14].
Constructions [BCF+14, DQFL12, HL10b, SNJ11, CZ15, Zim10]. Constructive [Mau12, WB12], constructs [BP10].
Containing [XWDN12], contemporaries [LCKBJ12], Contemporary [Opp11].
Content [BCP14a, MHT+13, PMZ13, PZPS15, WHZ12, WZXL12, YT12, ZXZ+11, GPN+12].
Content-based [MHT+13], contest [Cra14].
Contextual [Svo14]. Continual [BKKV10, XZY+12, YZ12, YCZY12].
Continual-Leakage [YZ12]. Continually [DLWW11]. Continuous [DHLAW10, FMNV14, PYP10, Yam12].
Continuous-Tone [Yam12], contract [Men13].
Control [BFK+10, MK12b, NA10b, RSN14, SGC14, TBCB15, XMLC13, AMHJ10, CO11, Cra11, JAS+11, NZM10, Sch15b, SA15, Tan12b, XHH12].
Controlled [FMTR12], controls [CGH11].
Conversion [BJ10]. Convertible [HL11b, HL11, LHH11, XWXC14].
Convolutional [MG15], cookies [DCAT12].
Cooperative [LLZ+12, WQZ+13].
Coprocessor [ABC+12, BGG+13, IBM13b].
Copy [YT12, MHT+13]. Copyright [SJ12, GJ13]. Core [LB13, HLYS14].
Correct [PST13]. CorrectDB [BS13a].
correcting [LTT10, MCP15], correction [Chi13a]. correctness [WS13]. Correlated [RS10].
Correlation [BW12, SDM+12, WWWC14, XHH12].
correlations [Sar14]. Correspondence [SY14], corresponding [DWZ12].
Corrigendum [WZM12a]. cosmography [Pet11].
Cost [GI12, Man13, CZ14, Sar10a, YL11].
Countermeasure [MD12b].
Countermeasures [EWS14, PZPS15], counting [LLY+12a], Coupling [SMS14].
Cover [UUN13]. Covert [NSA15, LT13, LyWSZ10, SRB+12].
CRC/Taylor [Joh10]. credential [KKM+13, XMHD13]. Credentials [CG12a, SSW12].
Cropping [SR12b]. Cross [CLY14, DSB15, LHM+15, YGFL15, ZTSR12, der10].
Cross-Site [DSB15]. Cryptanalysis [BW12, Bor10, CWP12, DG12, Far14, GST13, Gor10, Hin10, IOM12, Jee13, Kha10, KN10, KWS+12, LH10b, LNM+11, MWZ12, NXB13, OTD10, PSOMPL13, SM10a, SM10b, Vua10, Wad10, WWY11, WWYY11, WSSO12, WY14, YMWS11, AP11, BKR11, Bull0a, Bul0b, Con12, Eisi0, Her10, KDH13, LLLK10, Nov10, RITF+11, SD10, SDM14, Sun11, SvT10, TSS11, WYL14, WWBC14, YJ12].
Cryptanalyzing [ZLW+12]. CryptDB [PRZB12].
Cryptography [Goo12, Pfi10, Rab10, SCPSN10a, SCPSN10b, WL11, BR+14, BGG+13].
Cryptoclub [Ayu12, BP06]. cryptograms [Shy15]. Cryptographer [Dun12b, Kla11, Pie10].
cryptographers [Goo12]. Cryptographic
[Abe12, AD12, AMVZ12, App15, BMP12, BCGK12, BGB12, BIKK14, BLS12, BDP11, BFCZ12, Bla12, BKL+13, BSJ15, CCK12, jCPB+12, CBL13, Cor14b, Des10a, DQFL12, DR11, FKS+13, FY11, FLW12, Gir15, GM11, GLR10, GG11, HN10, HHH+13].
Ana14, Ano11a, BTPLST15, BKV13, CDGC12, CDF+10, DFJ+10, DTZZ12, Gen10, HSM13, HMCK12, JHCC14, LSBN14, LT14b, LKX+14, MHKS14, Sch15b, TMK11, TKMZ13, WLH13, WZLW13, WS14, ZMM+10, ZWY+13, HLYS14, Sch15b].

Data-Compression [DA12].

Data-Minimizing [BCD+12].

Data-Oriented [NNAM10].


Decentralizing [LW11b]. Deciding [CLCZ10, Sch12c]. Decipher [Cor14b]. decision [RPG12]. Decisional [LZC14].


Defensive [PH10]. definition [LWL10a, YKC+12]. Definitions [GLW12, Mau12, KM14, KGO10, XWXC14]. Delay [LBR12, JLT+12, CXW13].

Delegatable [WZ11]. Delegated [MZH15, TMC15]. Delegation [FMTR12, SSW12, YZ12, YAM+15, ZWM14].

Delfs [Mur10]. Delivery [PSS+13, SPPC12].


Dependency [SGP+12]. deployed [MFH13, SY10]. DepSky [BCQ+13].


derived [ZMM+10]. description [PLCGS11]. Design [ABc12, ADD10, BKL+13, DR11, FSK10, HSA14, KW14, Lop12, MSL13a, NVR+14, RYF+13, Sch13, SAAB10, SZDL14, CZ14, Gor10, KHF10, MAK+12]. designated [HYWS11, RPSL10]. Designation [Che15].

designed [Goo12]. Designing [CDK+10, FLW12, MRT10, SR10]. Designs [BGK12, KDH15]. Detect [ASA15].

Detecting [BKBK14, HLW12, KW14, SH15, YSC+15, LWLW11]. Detection [DSB15, DF11, HDWH12, KU14, LGL+12, LC15, MKRM10, NDC+13, NSMS14, SBV14, SP15, SGS14, AOT13, BM13, HB13, KLC+10, Maz13, MHT+13, WYL13].

Detective [Che10]. Determine [FSWF11, StO12]. Determining [NN12].

Deterministic [MPRS12, NIS12, XXZ12, DTTZ12].

Deterring [WGJ10]. DEUCE [YNQ15].


Device [KLM+12, TYK+12, KKG14, Par12b, XHH12]. Devices [DLWW11, EGG+12, GPT12, GMSV14, HHH+13, HDWH12, SFE10, WT10b, CLP+13b, CTL12, Chi13a, FRT13, IB11, LKAT12, OYHSB14]. DFT [DDFR13].

DHA [AKY13]. DHA-256 [AKY13].

DHTs [YKG13]. dictionary [MBB11].

Diego [Ano10, Lin14b]. Difference [BS14, YTP11, JKH13].

Different
[BAB+13, Die12, JK13, Pet11].

Expectations [DY13]. Experience [AD12].
experiences [JAE10]. experimental
[DHW+13]. Experts [Stol12]. Explicit
[AQD12, FHS13]. exploitability [CFN+14].
exploitation [MAK+12, NCCG13].

exploration [RYF+13]. Exploring
[Cil11, FNP+15, WHC+15]. exponent
[SM10a]. exponentially [RK11].
exponents [SM10b]. Exposing
[OF12, YQH12, YSC+15]. Exposure
[BVS+13]. Extend [TMC15]. Extended
[DGP10, HZW+14, SH15, Yam12].

Extending [ZSW+12]. Extensible [YZ12].

F5 [LLY+12b]. Fa [FMS12a]. fabricating
[WW13]. Face [AQD12, XHH12]. Facial
[KRB12]. facilitate [Chien13a]. Factor
[HXC+11, LLC11, CLP+13b, DMWS12, HC12, Lit14, WW14]. Factoring
[APPVP15, LLML12, MM13].

Factorization
[Con12, Kuz11, YAM+15, Mes15]. Failing
[Cer14]. Fails [ABD+15]. Fair
[ALR13, CSV15, DSSM14]. Fairness
[ALR13, Ash14, GHKL11]. Fake [KU14].

Fallen [HCPLSB12]. False
[LLZ+12, CDGC12]. Families [KU12].

Family
[BMS12, DGIS12, FLS+10, FFL12, GNL12].

Fanin [SS12a]. Fast
[Bru12, CHS15, NR12, WHZ12, WQZ+13, FHH10a, KHMB13, MBB11]. Fast AD
[SMBA10]. Faster [CN12, Ant14]. Fault
[BMS12, GST12, JKP12, LGL+12, LGLL12, MKRM10, PHI12a, RZZ+15, SEY14, BBBBB13, PBCC14]. fault-resistant
[PBCC14]. FC [DDS12, Dan12]. FEAD
[ZWM14]. Feasibility [FKS+13, WHC+15].

Feature
[SGP+12, FTV+10, GJ13, MHT+13].
Features [YI14, ZTL15, FNP+15].

February [Ane10, DDS12, Dan12, Dun12b, Kla11, Lin14b]. FedCohesion [CCFM12].

Federated
[BS13b, CCFM12, CSL+14, JAS+11].

Federated [NB13]. Feedback
[HZ11, PYM+15, SKG14, ZH15, LWK11].

Feedback-Based
[PYM+15]. Feistel
[KDH15, Sasa12, SEHK12]. FHSD [SP15].

FI [YNR12a]. FI-BAF [YNR12a]. Fiat
[BDSG+13]. Fidelity [BCP14a]. Field
[ASA14, SS12a]. Fields
[ARH14, BGT14, BGT13, C15, LBOX12].

Filling
[BWR12]. Filtering
[LLZ+12, CDGC12]. Financial
[Ane11b, Ber12, DDS12, Dan12]. Fine
[CDD13, FSGW11]. Fine-Grained
[CDD13]. FinFET [ZJ11]. FinFET-Based
[ZJ11]. Finger
[KLY+12]. Fingerprint
[MRS14b, KKG14]. Fingerprinting
[ZS12, FLZ+12]. Finite
[BGT14, CHS15, BGT13, C15, LBOX12].

Finite-State-Machine
[CHS15]. First
[DR10, AB10a, BCV12, Kim11, LCKBJ12, Mic10a, Zet14]. Fischlin [ABGR13]. fit
[KGO10]. fix [HLV10]. Fixed
[Chen10, Lim11]. Flame [Goo12]. Flaw
[Moo12, SH15]. Flaws [DR11, HLV10].

Flexible
[LGWY12, BGG+13, ZL12]. flow
[KL13, LWY12, PPR+12, SRB+12]. Flows
[CDD13, HKB14, WYL13]. Foolproof
[FFL12]. Force [JR14], forensics
[AKM+11, QZ14, SM13]. forged [HREJ14].

forgerys [YQH12]. Forgery
[LC15, BM13, LWLW11]. forgotten
[And13]. form [DWZ12, Kre13]. Formal
[EWS14, HSA14, KGO10, PLGSI11, ZW15]

FPGA [BCE+10, CFZ+10, CHS15, GFBF12, HF14b, MM14a, MAK+12, ZLQ15].

FPGA/ASIC [CFZ+10], FPGAs [DGP10, SMOP15, VMV15]. fractal [KM11]. fractional [BW13, VM14]. Fragment [CHHW12, MCDB12, SSA13, CCLL11, PGLL10, WHZ12]. fragment [BPP10].


Fraud [Ber12]. Fred [Xie12]. Free [App13, TWZ+12, TTH15, ZLH+12, ATK11, SA12, YT11b]. Free-View [TWZ+12].

French [Ant14]. Frequency [LWCJ14, TC10, EA12, NLYZ12].

Frequency-Based [LWCJ14]. Friendly [SZDL14, ACM12, WOLS12]. FSR [MD12b].

FSR-Based [MD12b]. Fugue [AP11]. Full [ALR13, HEC+12, LW12, WLC12, BKR11, LC13]. Fully [AKP12, BV11, BV14, CN12, CFZ12, CNT12, GH1a, GH1b, GHS12, HLLC11, LSC12, MVV12, NCCG13, PB12, Vai11, WHC+15, ZZ12, GH13, ZXJ+14].

Fully-Homomorphic [GH11b].

Fully-Homomorphic-Encryption [CN12].

Fun [APPVP15]. Function [FLS+10, SGY11, WSSO12, AKY13, AP11, LK14, LP11, RS14, Sar11, TQL+14, WYW14]. Functional [BSW12, Boy13, GVV12, MVV12, Wat12, ZYT13, ZWTM15, ZWM14].

Functionalities [JR13]. Functions [ALR13, BBC+14, BIKK14, BKPK12, BK12a, DSSM14, DQFL12, FY11, NR12, Rja12, SMS14, Tan12a, YTP11, AY14a, BDP11, CG12b, CW12a, ESR14, Gen10, HRV10, Li10, WT13]. Fundamentals [Joh10]. Further [HCL+14, WHY+12]. Fus [FMS12a]. Future [BCE+12, BKBK14, Bon12, GCK12, Mon13, Ano13b, FPBG14, Mac12, MJS13]. Future-proof [Mon13]. Fuzzy [KRDH13, NC12, SH11, JXWW13, KHM13, MMSD13, SM11, SNM14].


Gateway [WZM12a, WZM12b, WL11].

Gateway-oriented [WZM12a, WZM12b].

GCD [KI11]. GCM [SKK10].

GCM/GMAC [SKK10]. GDL [MMZ12].

General [FJHJ12, GFBF12, HP12, PB12, YFF12, HQZH14, LWS10, WS12, YC11].

generalisation [LR15]. Generalised [Hes12]. Generalized [PC14, KL11, NC13, YMSH10]. Generated [ADD10, NN12, XXYYXX11, LW13b].

Generation [ABS+12, BCGH11, MR14a, MJGS12, NIS12, GMRT+15, KHM13, KKM+13, XW13].

Generator [ADD10, BK12a, CDK+10, MVV12, NNAM10, NWKF14, CFY+10, LGKY10, MRT10, PLSDLE10, SH11, SM11, XSWC10].

Generators [NIS12, PFS12, CP13, HRV10, MG15, Sti11, Zi10]. Generic
Guangdong [IEE11a]. Guaranteed [TBCB15]. Guess [FSWF11, Fok12].
Chi12, dCCSM+12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GOPB12, GY13, GJJ15, HZC+12, HvS12, HSM13, HSM14, HYWS11, KKA14, KRB12, Kzu11, LMB12, LSL12a, LKAT12, LXJ14, LLC+15, LH1b, LSC12, LBR12, MBF+13, MJGS12, MR10, OdH12, Par12a, PSS+13, PWVT12, SS10a, SS12a, SAAB10, Sch11, SSPC12, SKGY14, TKR14, Tian15, TMGP13, Vlc12, Wan14, XZX12, YZX+12, YTM+14, Yon11, YCZY12, ZLH+12, ZTSR12, Ano13b, BOBI3, BMM12, BBGT12, CTHP13, DZ14, DWZ12, FA14b, GMRT+15, GPVCdBR012, HZC+14, HLR11, Hwa11, JZS+10, KKGK10, KKM+13, KL11, LKKL13, LK12, LXMW12, LCT+14, MGP10, MJS13, MM13, PLCGS11, RG10, SSY12, SE14, SR10, SSAF11, SSS11].

Known [DWWZ12, JLH12, SEHK12]. Known-Key [DWWZ12, SEHK12]. Kobitz [BJ10].
Korea [LH10a, LW11a]. KP [FJHJ12, HQZH14]. KP-ABE [FJHJ12, HQZH14]. Kryptografie [Blö12].
Kryptographie [Buc10]. Kuala [HWG10].

Languages [MX13, Wat12]. LANs [FLH13]. Lapin [HKL+12]. Laptop [GPT14].
Large [AN12, JLS12, JKHeY12, KCR11, KU12, MC11, SP13, EEAZ13, FXP12, LBOX12, SR10]. Large-Scale [JKHeY12, FXP12, SR10]. LARK [DS11].
Lattice [ADM12, Ano11b, BSJ15, EM12, FGM10, HPO+15, PG12]. Lattice-Based [ADM12, Ano11b, BSJ15, EM12, HPO+15, PG12].
look [AY14a]. look-up [AY14a]. Looks [KTA12]. lookup [LDDAM12].
lookup-table [LDDAM12]. loop [DWZ12].
losing [SLZ12]. Lossless [DA12, LZC+12b, GJ13, TTL10, WLH13].
Lossy [BKWP12, CW12a, DN12, ASO14].
love [FHM+12a]. Low [BCO13, BCG+12b, DJL+12, FHS13, GSTR13, GL12, LBR12, Man13, WT10b, ZJ11, C2Z14, Chi13a, LGKY10, LKAT12].
Low-Bandwidth [GST13].
Low-complexity [DJL+12]. Low-Cost [GI12, Man13].
Low-Distortion [FHS13].
low-end [Chi13a]. Low-Latency [BCG+12b]. Low-Power [WT10b]. Lower [LJ15, Sha10, Shp03].
lp231 [LK14]. LPN [HKL+12]. LPSNR [LP12]. LR [YZ12, ZWM14].
LR-FEAD [ZWM14]. LR-UESDE [YZ12]. LTE [CLM+12, LLLS13, TM12].
LUT [HF14b]. Luther [ABJ13].
LWE [BV11]. LZZS [CFY12].
magic [PHN+12]. main [CS11]. Make [Ayu12, BP06].
Making [Gel13, LA10]. Malaysia [HWG10].
Malicious [AAE+14, BK12b, WTT12]. malleability [KTT12]. Malleable [CKLM13, MSas12, CG14, FMNV14, LP11, OOR+14, Pas13a]. Mallory [FHM+12]. malware [Goo12].
Mapping [CBL13, MM14a]. Mappings [MC11]. MapReduce [LJLC12]. maps [BAAS13]. March [Ano10, Cra12, DDS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, WZM12a].
Masking [HF14b, PYM+13]. Mass [BPR14a, BPR14b]. Masses [Ano15b].
mean [TTL10]. Means [KRDH13, AMHJ10]. Measure [DDD14]. Measure-independent [DDD14].
Multiple-Parameter [NDC‡13].
Multiple-Precision [HZSL05, MN14].
Multiple-Secret [SC10]. Multiplication
[AK14, SK12b, YTS12, SKH15, SF12].
Multiplicative [KHHH14]. Multi-receiver
[FHH05b]. multisecret [FGMP12].
Multitone [GL10]. multiwatermarking
[W12]. mutiwavelet [PWW10]. Munich
[Wat10]. musical [Ana14]. Mutt [Ran14].
Mutual
[GI12, GM14, SBS‡12, WT16b, Cho14, CL11,
FHH10a, Far14, HDPC13, IB11, XMHD13].
MVP [CD12]. My [GPT14].
Name [YCM‡13]. Names [ABJ13].
National [ABJ13]. nature [KL13]. Naval
[Don14]. Nazis [Hea15]. NDSS [Ano10].
nearest [LVRY10]. nearest-neighbor
[LVRY10]. necessary [TD14]. needs
[Sch12b]. Negligible [DF11]. neighbor
[LVRY10]. Neighborhood [DA10].
[ZMM‡10]. nested [FHH10a]. Net [LHF12].
Network
[Ano10, CJ13, CLH13, Hay13, HDWH12,
LCL15, LTIW11, MJGS12, NNA10,
NRZQ15, She14, TLW12, VKC15, YZLC12,
YSJL14, AKM‡11, Ano11a, AZF‡12, CL11,
FPBG14, HWG10, HB13, HKB14, JZS‡10,
LH11a, LKKL13, MZA‡13, MIJS13, NDNR13,
Sta11a, WYL13, WS14, YLS12, Ste15].
network-based [YLS12]. Network-Coded
[She14]. Networking
[LCK11, ZHL15, Kim11]. Networks
[BN14, CS14, DS11, FMS12b, HZC‡12,
HBCC13, HK14, KH10, LLC11, LL15,
LHM‡15, LZCK14, IWC14, LLZ‡12,
NSA15, NDR‡14, OO12, OKG‡12,
PYM‡15, PCPK14, RWLL14, SWYP12,
She14, Smit11b, SL11, WLY‡15, XHC‡12,
ZC13, ZW15, Zha15, ZLDD12, ZSA12,
ASO14, ADF12, BDK11, CDGC12, CLM‡12,
CLSW12, CL11, DCS12, DK12, DLN13,
EEAZ13, FA14b, HGWW11, HZC‡14,
One-Sided [HP14]. One-Time [NA10a, DCAT12, BM15, FHH10a, LWI13b, LML+13].
One-Time-Password [FD11]. One-Way [DSMM14, Mat14, HRV10, LP11, RK11].
Onion [KZG10]. Online [SKGY14, ZHL15, CCG10, LKAT12].
online/offline [LKAT12]. open [BB10, YNR12b, YLW13, Bul10a, Sar11].
open-source [ABF+14, Pow14, ZWQ+11].
Opening [LZC12a, LZC14]. Openings [SP13]. openness [Bia12].
OpenPGP [MBB11]. OpenStack [CSL+14]. Operating [KMP+11, CDA14].
Optimally [DSMM14, GT12]. Optimally-Fair [DSMM14]. Optimising [EVP10].
optimization [FLZ+12, GCSAddP11, KHF10, PTK14, RYF+13]. Optimized [MBF+13, MBR15].
Oracle [HKT11]. Oracles [FZT14, FSXi2a, YS12, YLA+13, LLY15, RG10, SYL13, WWYY11].
Order [KS12, LWKP12, PRC12, YKKL12, ZDL12, ZSW+12, AYK13, LW13a, LWKP14, YL11].
Order-Preserving [KS12, YKKL12, YL11]. Organization [RSGG15]. Orientated [TJZF12]. Oriented [NNAM10, RSGG15, WW12, WZM12a, WZM12b].
Outsourcing [DR12, LJLC12, LHL+14]. Outwitted [Car11]. Overcoming [BKKV10, DY13]. Overhead
[CCW+10, GHS12, ZJ11]. Overlay [CHS15, MJS13]. overview [BDP+12].
Ownership [FMTR12, RR11, HWYW14]. Oxford [Che11].

Pairing-Based [Bon12, KZG10, LGPRH14, YTS12, Con12]. pairing-free [YT11b]. Pairings
Pan [GOPB12]. Pan-European [GOPB12]. paper [SK14]. Papers
[LW13a, XW13, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. Paradigm
[ABGR13, BSV12, Mau12, MP12, WQZ+13]. Parallel [CGB+10, LB13, MDCB12, MC11, SMDS11, YE12, MRT10, RG10, WWYZ11].
Parameter [NDC+13]. parametric
[Bul10a]. Paranoia [Cor14a]. Park [Ano11c, Bri11, Cop10, McK10, McK11, Pea11, Sni11a]. part [VM14]. Partial
[GFBF12, LG12, SGS14, WDDW12, Bax14]. Partially [KB10]. participants
Party [Ash14, HL10b, HP14, JR13, KMO14, NSMS14, GVW12, LyWSZ10, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14, GHKL11]. Passau [GLIC10]. PASSERINE
[Saa12a]. passive
[BM13, LWLW11, MK12a]. passport [LZJX10]. Password
[BRT12, CLY14, FD11, HCL+14, Lop15, RS11, SD12, Shi11, WgMW12, YLW13, ABK13, CTL12, DSCS12, FA14a, HCC10, LWS10, LNKL13, MM12, Tso13, TKHK14, WZM12a, WZM12b, YC12].
Password-Authenticated
[HCL+14, LWS10, WZM12a, WZM12b].
Password-Based [BRT12, CLY14, WgMW12, DSCS12, FA14a, TKHK14].

Permutations [CGB+10]. Peaks [TC10].

Pecherskii [Kuz11]. peer [LLYO6, NCCG13, ZWY13]. peer-to-peer [NCCG13, ZWY13]. [Ran10, Ran14].


Stateful [NTY12]. Subscribe [TKR14].


Performance [Alo12, AB15, CGL12, CCG10, DBPS12, EGG+12, ESR14, FFPBG14, GLG12, GCS13, HKL14, LCK11, MHC12, SKY12, TPKT12, WDDW12, Xio12, ZLDD12, MS13c]. periodic [KPS10]. periodical [CLSW12]. permutation [GMSW14, LK14]. mutation-based [LK14].


Perspective [RSGG15, JW14, Suc12, ZWT13].

Perspectives [SPM+13]. Pervasive [BGC+12b, Tan12b]. Phase [ZWT13].

Phase-change [ZWT13]. Phone [SAA12b]. photo [OF12]. Photographic [YSC15].

photos [Pow14]. Phrases [WBC10].


Plaintext [BM15, JHLH12, MSas12].

Plaintexts [YKKL12]. Plane [YLL12].

Platform [YE12, ABF+14, NCCG13].

Platforms [HTZR12, SOG15, LT14b].


pollution [NDNR13]. Polylog [GHS12].

Polynomial [Ano11b, BGTJ14, NKF14, WSSO12, BGJT13, Bul10a, Bul10a].

Polynomial-Advantage [WSSO12].

Polynomials [CMLRHS13, SS12b, TWZ11, LPdS10].


Post [ZCC12, Sen10, Yan11].


Potential [Cil11, ZW15]. Power [ARP12, HHR11, MMP14, MD12b, SDM12, TQL14, WT10b, YAM15, ZH15, ZJ11].
Propagating [WWC+11, YZLC12].
Properties [CCK12, DQFL12, FY11, JR13, KU12, Sch12c, CLCZ10, WT13]. Property [HEC+12, PR12, Rja12]. Proportions [Ber12]. proposed [Bax14]. protect [BVIB12, CDF+10, dCCSM+12].
Protecting [BCP14a, CDA14]. Protection [CDD13, GST12, Lop12, RR11, SEY14, SJ12, HLYS14, KKM+13, IVRY10, TLL13, YWT+12]. protection-key [HLYS14].
Protocol [BL12, BC14, BSSV12, FLH13, FMTR12, GI12, HvS12, HC12, HL10a, HCPLSB12, HCEP12+12, HKL+12, KMO14, LNZ+13, LCCJ13, LNXY15, MR10, PSS+13, SBS+12, TYK+12, WT10b, YS12, YWZ+12, XZX+11, AKG13, BGAD12, CCSV11, EA12, FA14b, GMSW14, HL14, Kim11, LLLS13, LDDAM12, LKKL13, LSW0, LXMW12, LY14, LML+13, NLYZ12, OHJ10, Par12b, SSS11, SSPL+13, Tso13, TKKH14, WZM12a, WZM12b, WT10a, WTT12, XCL13, YC12, YWZ+14, YMM13, ZWQ+11, ZG10, ZK11, BOB13, LFCCGCR14, Ste15].
Protocols [AP13, BMP12, CCK12, Con10, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, MT12, NYR+14, NMS14, SBS+12, Sch12c, SOF12, TM12, Xio12, ACM12, CR10, CLCZ10, FTV+10, GBMN11, GLR13, HPDC13, HST14, KSU13, LLY06, LKKL13, MN10, Nos11, Nos14, SD10, YSL+10].
Provable [BKL12, YSMS10, ZK11, FA14a, HRS13, LH11, WB12, XCL13].
Providing [BKL12, YSMS10, ZK11, FA14a, HRS13, LH11, WB12, XCL13].
Provable [BCGAPM12, BCM12, BHJP14, FHH10a, LH11a, WMS+12, XJWW13, YC12, YWZ+14, ZG10, ABB13, XXW14].
Principle [An10a].
Provided [KS12].
Provided [Sch15a]. providers [BK12b, YWK10].
Providing [DLN13, HTWZ12].
Proving [Sar14].
Proximity [IW14].
Py-Family [DGIS12]. pyramid [MHT+13].

region-duplication [LWLW11]. Regions [AQD12], register [LWK11]. Registers [ZH15]. Regular [Wat12], regulating [DFJ+10], regulatory [BP10], regulatory-compliant [BP10]. Rekeying [DT13, CLSW12, DS11]. Related [Cil11, CMA14, DGLS12, Pud12, WLC12, MNP12].


Robust

EWS14, GPT14, KOP12, NDC+13, PRC12, SR12a, Vua10, BVIB12, DJL+12, MFH13.

Side-Channel
[CBL13, EWS14, GPT14, KOP12, NDC+13, PRC12, DMWS12, BVIB12, MFH13].

Sign-On [LL15, MEFO12, SPM+13].

Signature [Ano13a, ABF12, ASS15, BHG12, FGM10, GJJ15, GMSV14, HPO+15, LTH+15, LGPRH14, MNN12, NXB13, PH12b, TTH15, WZXL12, XGLM14, YMW11, YLA+13, ZJ14, ZHL+12, CLS12, CC10, DZ14, DNN13, HYWS11, Hwa11, JZS+10, Nos14, RSM10, SL10, YLS12, YKC+12, ZLY10].

signature-based [DLN13].

Signcryption [CMA14, DYZ10, FZT13, FTZ14, LSL12a, EZ15, HS11, KL11, LK12, LST12, LKT12, YM110]. signer [Hwa11].

Signing [YAM+15].

Simple [CZF12, Ros11, Sar10b, TDTD13, ZH15, Zim10, CLM+12].

Simplified [PS12].

simulation [MS13a]. simulations [Ana14].

Simultaneous [YWZ+12].

Single [ABK13, LL15, MEFO12, Sas12, SPM+13].

Single-SP [Sas12].

Singular [LS12b, BWA13].

sins [HLV10].

SIP [KKGK10].

Site [DSB15, SS10b].

Size [CJ13, CSW12, EAA12, LCLL15, MTY11, AHW+12, LCM+14, PPTT15].

Size-Constrained [EAA12].

Skein [FLS+10, KN10].

Skin [AQD12].

skyline [BK13].

Slantlet [TK14].

Slide [IOM12, LC13].

SLMAP [HCETPL+12].

Slow [SMi11b].

Small [BGJT14, BKLS12, BB10, CJ13, LCLL15, BGJT13, Jou13].

Smart [BSJ15, HCL+14, LA10, PDT12, WGM12, WGM12, CHS11, CHJ13, HCC10, LHI0c, LNM+11, LXM12, LNL13, MM12, YZZ+14, YSL+10, Cho10, GLIC10, SD12].

Smart-Card-Based [HCL+14].

Smartphones [Cor14b].

Smooth [XYXY11, YCI11, ZBR11].

SMS [PSdO+13].

SMART [PS12].

SMSCrypto [PSdO+13].

Snowden [Fox14].

Social [KTA12, NSA15, NRZQ15, FMY+15, SKGY14, WLY+15, ZW15, Zha15, ZHL15, BDK11].

Society [Sch15a, Sch12b].

Socio-Rational [S12].

Softw [WZ12].

Software [EWS14, LRVW14, ADB+14, CFH+13, GLJ+12, Hly10, KHF10, LBOX12, SF12, YWT+12].

Solom [CGB+10].

Solution [Fra15, KAM13, NA10b, Cor14a].

solutions [KAS15, WW14].

Solved [IBM13a].

Solving [BB10, Bul10a].

Some [AD12, Ber12, Dur15, LWL10b].

Song [Cou12].

Sood [MWZ12].

Sound [COP14, LSR13, Sav15].

Source [RWLL14, ADB+14, PX13, Pow14].

sources [SSY12].

South [BL10, LW11a].

SP [Sas12, SEHK12].

Space [BWR12, BKL+13, NRY+14, RYF+13].

Space-Filling [BWR12].

Spaces [SH15].

Spanish [Pet11].

Sparse [BBC+13].

SpartanRPC [CS14].

Spatial [AV12, CZF12, PDM12, CW14b, NZL+15].

Spatiotemporal [DIMT12].

Speaker [PPRT12].

Special [Ano13b, AB10b, LW13a, XW13].

Specific [BDFK12, KME+12]. specification [SD10].

Specifications [BMP12].

Spectrum [KD12a, TWZ+12, LW12, MMD13].

Spectrum-Based [TWZ+12].

Speed [GL12, HZ11, BDL+11, KLI3].

Speeding [RVRS12].

SPEKS [Che15].

Splicing [YSC+15].

Spline [Tan12a].

Split [CG14, XZY+12].

Split-State [CG14, XZY+12].

Splittable [CP13].

Spoken [WBC+10].

Sponge [BDP11].

SPONGENT [BKM+13].

spongy [RS14].

Spoof [SP15].

Spread [KD12a, TWZ+12, LW12, MMD13].

spreadsheets [LT13].

Springer
[Mei10, Mur10]. Springer-Verlag [Mei10].


[YS14, Lit14, Ran10, der10]. SSL

[BJR+14, Dav11, FHM+12, GJ+12, HREJ14, NH+14, PP11]. SSL/TLS


ST-Numbering [MNS11]. Standard

[Azo12, Azo13a, App13, BCM12, BV11, BV14, GJ15, MVR12, SZS14, TCL15, WWH12, Yon12, ZC13, Kim11, LIT12, WZM12a, WZM12b, WWBC14, YC12, MKRM10]. Standardization [TRD11].

standards [DHW+13, NIS13]. State

[BVS+13, CG14, CL+13, CHS15, Dew11, FHR14, ZXS+12]. Stateful

[BVS+13, VSR12]. Stateless

[GM11, NTV12, VDO14, DCAT12]. Stateless/Stateful [NTY12]. statement [NIS13]. static [TLMM13]. Station

[Smi11a]. stationary [ZLD12]. Statistical

[Bro11, DBPS12, HZ11, OR+14, SP13, Sim15, Böhl0]. Statistical-Attack [SP13].

Statutory [PH12b]. Stealing [RWZ12].

Stealthy [BRPB13]. Steering [HR13].

Steganalysis [DA12, Fri12, JHHN12, KD12b, LC15, SGP+12, Tani12a, YLL+12, YI14, Böh10, LSQ11, Sch12a].

Steganographic [DA10, LLC10, CAC14]. Steganography

[BCG12a, FMS12b, Fri10a, Fri12, HZW+14, Jio10, LLY+12b, PDMR12, Pan10, SK12a, SR12b, TJZF12, ZSA12, AOT13, BDK11, BHdFR12, EEAZ13, GKK11, LyWSZ10, LRW13, LWW+10, Maz13, PHN+12, SI12, WKH11, WOLS12, ZMS14]. Stego

[YLL+12]. Stego-Image [YLL+12].

Stellenbosch [BL10]. step [AKY13].

Steven [Sch15a]. Stopping [Sav13a].

StopWatch [LGR14]. Storage

[BCQ+13, CTT+14, GLG12, HSM14, Küp15, LCK11, LWCJ14, ZDL12, AY14a, BP10, CFZ+10, CDF+10, FH13, HSM13, LBOX12, Sar10a, WS13]. Stored [RSN14]. Storing

[DLW11]. storm [ACM12]. Story

[Cer14, Hein15, Pea11, Pet11]. Strand

[SH15]. strange [Azc11]. Strangeness

[RR12]. Strategic [Sch12c]. Strategies

[DSSDW14, TJZF12, YCM+13, AZF+12]. Strategy

[NRZQ15, FL+12]. Stratix

[SMOP15, SMOP15]. Stream

[ABS+12, BMS12, DG12, DGS12, GCS+13, HZ11, IOM12, Kla10, MD12b, MHC12, NN12, WHN+12, ZH15, Die12, KM10a, LW11, LW13b, MRT10, OCGD11, RS14]. Streaming [ZSA12, ZC12]. Streams

[PCDG14, HM10, PYP10]. Street

[Gli12, KGP12]. Street-Level

[Gli12, KGP12]. Strengthen [BL12].

Stribog [AY14b]. strikes [Ran10]. Strong

[ADD10, KFOS12, PYM+15, SAA12b, Yon12, HYWS11, OYHSB14]. stronger [RK11]. Strongly [KW14, YS12].

structural [BDK11]. Structure

[HP12, LMHH14, LJ15, MKRM10, WYCF14, LLY12, ZLW+12]. Structure-Independent [MKRM10].

Structured [PMZ12]. Structures

[GGT11, HHH+13, LHKR10, PB12, DDFR13, MHKS14, Shy15, WS12]. Studies [PP10a]. Study

[STMC11, CCG10, EBFK13, VGN14]. Stuxnet [Zet14]. Style [GHPS12].


[BS14, RP12, ZK11]. subspace [ZWM14].

Substitution [DA10]. substructure [MRT10]. Succinct [BC13, CKLM13].

sufficient [TD14]. suitable [Joe13]. Sums

[SS12b]. sun [Cer15]. support

[CZ14, JAS+11, PW10, TTL10, VCK+12, ZMM+10, ZBR11]. Supporting

[FMTR12, HCDM12]. surfaces [CDLY14].

Surprises [Bow11]. Suppressed

[SFK12].


Third-Round [jCPB+12]. Thirteen [AP13]. thou [BDK11]. threat [Ven14]. Threats [LJS+14]. Three [CZ15, HXC+11, LZC+12b, Shi11, YKNS12, LML+13, Tso13, TJKH14, XCL13, YC12, YZZ+14].

Three-Dimensional [LZC+12b]. Three-Factor [HXC+11]. three-party [LML+13, Tso13, TJKH14, XCL13, YC12, YZZ+14]. Threshold [CT11b, Ci11, FGM10, GLW13, LWL10b, Sta12, WYCF14, YFF12, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, Shy15, TD14, ZJX+14].


Tight [LPS12]. Time [FD11, KME+12, NA10a, Nov10, Ste15, WLZL12, YE12, AY14a, BM15, DCA12, FHH10a, LW13b, LML+13, MK11].


Top-Fanin [SS12a]. Top-Secret [SS10b].

Topics [SCPSN10a, SCPSN10b, AB10b, DUN12b, KIA11, Piek10]. Topology [HMK14]. Topology-Preserving [HMK14]. Tor [LLY+12a]. Toronto [MV12].


Trace [ABR12, WGT10]. Traceability [HCETPL+12, Chi13a]. traceback [LYW12, WYL13]. traces [MYYR13].

Tracing [PPS12b, MFH13, PPR+12]. Track [Dun12b, KIA11, Pie10]. Trade [BS14, SR10]. Trade-Offs [BS14, SR10]. Tradeoff [WDDW12]. Trading [TW12].

traffic [AZH11, FTV+10, PPR+12]. traffic-feature [FTV+10]. Training [HM12]. Traitor [PPS12b]. trajectory [LVRY10].


Transform [AN12, BCPV11, LSL12b, OWHS12, YWNW15, BW13, MO14, NES+14, PC14, TK14, YWPYWP13].

Transformation [CRE+12, FJHJ12, NXB13, tWmC12, GZHD12, HQZ14, PGLL10]. transmission [PSdO+13, WQZ+13]. Transparency [TJZF12]. Transparency-Orientated [TJZF12]. Transparent [CCW+10, XTK10].

Transport [RBHP15, TW14]. Trapping [BKPW12, CW12L, Mat14, RPSL10, CSZ+11, CW12a]. TREE [BS14, BW13].

Trends [BTPLST15].

trees [BTPLST15].

Triangular [AMVZ12]. Tricks [GY13]. trimmed [TTL10]. TRIMS [MGP10]. Triple [LW13b, MS12]. triple-base [MS12].


Truncated [KWS+12, WW12]. Trust [GK11, GMS14, KMP15]. True [LA10].

Trusted [EAA12, HTC+10, KUP13]. trustworthy [YZZ+14].


REFERENCES


White-Box [Mic10b]. who [Bat10, Car11, Hea15, Mck10, Mck11, Moo14, XTK10].

Widespread [HGWY11, HZC+14, HCCC11, HTC+10, HLYS14, ILMJC11, NDNR13, SA12, SZMK13, SKK10, TKHK14, Wan13, WW14, XCH14, XMH13, ZBR11, ZCLL14].

Wiring [HTZR12]. Wise [CG14, SSA13].

WISP [PPH12]. Without [ASS15, CCL+13, FZT14, NA10a, YLA+13, AZH11, BT12, BF11, CCW+10, FSX12a, GH11a, GST12, HDPC13, LLY15, LGWY12, RG10, SYL13, SLZ12, TAKS10, WWYY11, YS12].


Workshops [DDS12]. World [FKS+13, KM10c, Con12, G12+12, Goo12, LCKBJ12, Pet11, Sch15b, Zet14].

world-class [Goo12]. Worm [WWC+11].

Worst [BIKK14]. would [McG11]. Write [YNQ15]. Write-Efficient [YNQ15].

writing [LT14]. wrong [LHA+12]. WSN [DL12]. WSNs [ZYL+10]. Wu [LLLK10].

WW2 [Don14].


XOR [App13]. XTEA [CWP12, IS12].

XTS [Mar10]. xviii [Sch15a].


Zero [BW12, CLP13a, COP14, GJO+13, GOS12, IW14, MX13, MT12, OOR+14, Pan14, SJ12, Zet14, TLL13, WWBC14]. Zero-Correlation [BW12, WWBC14]. Zero-Knowledge [CLP13a, GOS12, IW14, MX13, MT12, Pan14]. Zero-Watermark [SJ12, TLL13]. ZIDS [NSMS14]. Zodiac [SDM10].

ZUC [WHN+12].

References

Arora:2012:ILM


Abdalla:2010:PCL


Atallah:2010:ATC


Anand:2015:ICL


Alleaume:2014:UQK

Almeida:2013:CCA

Arnold:2012:ICC

Adrian:2015:IFS

Abe:2010:ACA

Abe:2012:TBG
REFERENCES

10.1007/978-3-642-33272-2_1.

Arriaga:2012:JSS


Almeida:2014:COS


Aid:2013:DIO


Acar:2013:SP

Arapinis:2012:RET


ALMashrafi:2012:AIM


Applebaum:2010:PKC


ACM:2010:PAI


ACM:2011:PAI


Avoine:2012:PFS

Gildas Avoine, Xavier Carpent, and Benjamin Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *Journal of Network and Computer Ap-

**Aczel:2011:SWL**


**Aizatulin:2012:VCC**


**Anyanwu:2010:DCS**


**Ayday:2012:DAA**


**Adikari:2011:HBT**


**Abdalla:2012:LBH**

REFERENCES

Attrapadung:2012:ABE


Applebaum:2014:HGA


Azarderakhsh:2014:NDP


Almulla:2013:CKE


Afanasyev:2011:PPN


Armknecht:2012:STH


Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodriguez-Henriquez. Weakness of \( F_{36509} \) for discrete logarithm cryptography. Report, University of Waterloo, Waterloo, ON,
Ahmadian:2010:PDS

Alvarez:2012:CAB

Albrecht:2012:SDL

Anawis:2014:ARR

Anderson:2013:MNF
Anonymous:2010:NDS


Anonymous:2011:AIS


Anonymous:2011:AXL


Anonymous:2011:MCB


Anonymous:2012:SHS


Anonymous:2013:DSS

Anonymous:2013:SIS


Anon:2015:BSU


Anonymous:2015:CEB


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF

Jean-Philippe Aumasson and Raphael C.-W. Phan. On the cryptanalysis of the hash function Fugue:


[G. Adj and F. Rodriguez-Henriquez. Square root computation over even ex-]
REFERENCES

Ambrose:2012:RII


Asharov:2014:TCC


Al-Sinani:2012:UCB


Ahmadi:2012:SKE


Ahmadi:2011:SKC


Ahmad:2014:RTN


Apavatjrut:2012:EEA


AlTawy:2014:IDR


Alshammari:2011:CET


Ayub:2012:BRB


Alavi:2014:RQE

REFERENCES

August 2014. CODEN ????. ISSN 2150-8097.

Behnia:2013:IEB


Blaner:2013:IPP


Brennan:2012:ASC


Berbecaru:2010:FSM


Barbay:2012:BRB


Batey:2010:DMW

REFERENCES

Baal:2010:CC

Bulygin:2010:OSS

Bennett:2014:QCP

Barenghi:2013:FIT

Baldi:2013:ULC
REFERENCES

Barak:2014:OEF


Beimel:2014:MLS


Boldi:2012:IUG


Bernstein:2011:PCI


Basin:2014:KYE


Bichsel:2012:DMA

Badrignans:2010:SSA

Balfanz:2012:FA

Buhrman:2014:PBQ

Bahi:2012:SCS

Borghoff:2012:PLL

Baelde:2012:TPR
David Baelde, Pierre Courtieu, David Gross-Amblard, and Christine Paulin-Mohring.


REFERENCES


REFERENCES

CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).


*Barthe:2014:PRV*


*Battistello:2012:TBA*


*Beimel:2012:SSS*


*Bobbia:2010:ABM*


*Barthe:2012:CACb*

REFERENCES


Barthe, Benjamin Grégoire, and César Kunz. Automation in computer-aided cryptography: Proofs.


Biggs:2008:CII \[Big08\] Norman Biggs. *Codes: An introduction to Information Communication and
REFERENCES


Beimel:2014:CCW


Brumley:2010:CAI


Bogdanov:2012:UTC


Brubaker:2014:UFA


Boldyreva:2012:NPG

Alexandra Boldyreva and Virendra Kumar. A new pseudorandom generator from collision-resistant hash functions. Report, School of Computer Science, Georgia Institute of Technology, Atlanta,
REFERENCES


[BKLS12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, and Francois-Xavier Standaert. Key-alternating ci-

Bellare:2012:IBL


Bogdanov:2011:BCF


Bothe:2013:EPS


Bernstein:2010:PCA


Byun:2011:SMC

Jin Wook Byun and Dong Hoon Lee. On a security model of conjunctive keyword search over encrypted relational database. The Journal
Bai:2012:SSR


Bernstein:2012:HEC


Blanchette:2012:BPC


Blomer:2012:TKG


Bernstein:2014:HEC


Burmester:2011:LRA

REFERENCES


[Babamir:2014:AKP]

[BOB13] Ben-Othman:2013:IHN
Jalel Ben-Othman and

Böhme:2010:ASS


Boneh:2012:PBC


Borghoff:2010:CLC


Bowyer:2011:WSD


Boyen:2013:ABF


Beissinger:2006:CUM

Janet Beissinger and Vera Pless. The Cryptoclub: Using Mathematics to Make and Break Secret Codes. A.
Burns:2010:SCR


Bohli:2011:RAP


Brooke:2010:DCX


Bellare:2014:SSEa


Bellare:2014:SSEb


Brakerski:2014:VBB

Zvika Brakerski and Guy N. Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding. Lecture Notes in Computer Science, 8349: 1–25, 2014. CODEN LNCSD9. ISSN 0302-9743
REFERENCES


Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL http://people.umass.edu/gbecker/BeckerChes13.pdf.


REFERENCES

Batina:2012:HEB


Broustis:2012:GAN


Boneh:2012:FEN


Blasco:2015:HDT

REFERENCES

[102x681] REFERENCES


[BVS+13] Joonsang Baek, Quang Hieu Vu, Abdulhadi Shoufan,

Bogdanov:2012:ZCL


Bhatnagar:2013:BIW


Bhatnagar:2013:SRI


Bhatnagar:2012:IVE


Bao:2010:ISC


Chadha:2012:A


Chou:2013:UGS


Chang:2011:SFW


Cho:2014:DGA


Chen:2011:EAA

REFERENCES

Chu:2014:KA


Chen:2010:ALD


Ciriani:2010:CFE


Criswell:2014:VGP


Cheng:2013:DVB


Cheng:2013:DVB


Ciriani:2010:CFE

Ciriani:2010:TPA

Cao:2012:ITM

Chari:2010:DSC

Costello:2014:CAS

Ceruzzi:2014:HFT

Cerf:2015:CTN
Vinton G. Cerf. Cerf's up: There is nothing new under the sun. *Communications of the Association for Computing Machinery*, 58(2):7, February 2015. CODEN CACMA2. ISSN 0001-0782
REFERENCES


Coull:2011:ACO


Cheng:2012:PAI


Chen:2010:NUP


Chandran:2014:PBC


Chan:2013:OCK


Chang:2013:MPQ

REFERENCES

(2011): CCI


[Che11]

Cheswick:2013:RP


[Che13]

Chen:2015:SSS


[Che15]

Chien:2012:IAM


[Chi12]

Chien:2013:CR

Hung-Yu Chien. Combining Rabin cryptosystem and error correction codes

[CHHW12]


[Chien:2012:SRF]


Patrick Cooke, Lu Hao, and Greg Stitt. Finite-state-machine overlay architectures for fast FPGA compilation and application portability. *ACM*

Chen:2013:ATK


Cilardo:2011:EPT


Cheng:2013:EHM


Cao:2014:SCI


Chase:2013:SMN


Chuang:2011:LMA

Comon-Lundh:2010:DSP


Chong:2013:ASG


Chen:2012:NCF


Chen:2013:TSE


Cao:2012:SRH


Canetti:2013:PCC


REFERENCES

Chen:2012:FAA


CNRS:2014:NAS


Coron:2012:PKC


Conitzer:2010:AP


Constantin:2012:RSN

networkworld.com/news/
2012/061912-researchers-
set-new-cryptanalysis-
world-260338.html.

**Copeland:2010:CSB**

[B. Jack Copeland, editor. *Colossus: the secrets
of Bletchley Park’s code-
breaking computers*.
Oxford University Press, Walton
0-19-284055-X (hardcover),
0-19-957814-1 (paperback).
xvi + 462 + 16 pp. LCCN
D810.C88 C66 2010.]

**Chung:2014:RRS**

[Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, and
Muthuramakrishnan Venk-
tasubramaniam. 4-
round resettably-sound [Cor14a]
zero knowledge. *Lecture
Notes in Computer Sci-
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-54242-8_9/.]

**Cordova:2014:EBS**

[Tim Cordova. Encrypted [CP13]
backup solution: Home
Paranoia Edition. *Linux
3,??, January 2014. CO-
DEN LJJOFX. ISSN 1075-
3583 (print), 1938-3827
(electronic).

**Corthesy:2014:SSD**

[Sébastien Corthé. Smart-
phones set out to decipher
a cryptographic system. *Sci-
cientific Computing*, August
www.sciencetech.co.uk/news/2014/08/smartphones-
set-out-decipher-cryptographic-
system. The article de-
scribes use of thousands
of mobile phones to at-
tempt a parallel brute-
force attack on elliptic-
curve and RSA algorithms,
in a research project by Ra-
masany Gowthami and Ar-
jen Lenstra at the LACAL
laboratory at EPFL, Lau-
sanne, Switzerland.]

**Coutinho:2012:RPT**

[S. C. Coutinho. Review of *Primality Testing
and Integer Factorization in
Public Key Cryptogra-
phy* by Song Y. Yan. *ACM
SIGACT News*, 43(2):33–
35, June 2012. CODEN
SIGNDM. ISSN 0163-5700
(print), 1943-5827 (elec-
tronic).

**Claessen:2013:SPN**

[Koen Claessen and Michal H.
Palka. Splittable pseudo-
dorandom number genera-
tors using cryptographic
hashing. *ACM SIGPLAN
Notices*, 48(12):47–58, De-
REFERENCES


Chhabra:2011:NSN

Clark:2012:RLA

Chapin:2014:SRP

Chadwick:2014:AFI

Chen:2013:RWM

Chong:2015:SID
REFERENCES


REFERENCES


**Chen:2012:FSD**


**Chen:2012:AIB**


**Chen:2012:IBE**


**Dharwadkar:2010:SSG**


**Djebbar:2012:ASB**

Fatiha Djebbar and Beghdad Ayad. Audio steeganal-

**Danezis:2012:FCDb**


**Davies:2011:IST**


**Diong:2012:DAU**


**Dacosta:2012:OTC**


**Cordeiro:2012:IMB**

Weverton Luis da Costa Cordeiro, Flávio Roberto Santos, Gustavo Huff Mauch, Marinho Pilla Barcelos, and Luciano Paschoal Gaspary. Identity management based on adaptive puzzles to protect P2P systems from Sybil attacks. *Computer Networks*


REFERENCES


[DG12] Ding:2012:CLS


[DGIS12] Ding:2012:NRR

L. Ding, J. Guan, and
REFERENCES


Drimer:2010:DBP


Dodis:2010:CAC


Driessen:2013:ESA


Diem:2012:UES


Drosou:2012:SAH


Domnitser:2012:NMC

Leonid Domnitser, Aamer Jaleel, Jason Loew, Nael Abu-Ghazaleh, and Dmitry Ponomarev. Non-monopolizable caches: Low-complexity mitigation of cache side channel attacks. *ACM*
REFERENCES


Delfs:2002:ICP


Delfs:2007:ICP


Dolev:2012:ATC


Durumeric:2014:MH


Dodis:2012:MAR


Dunkelman:2012:MCE

Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The Even–Mansour

Dong:2012:UAS


Dong:2013:PRS


Demme:2012:SCV


David:2012:UCO


Donovan:2014:ATM


Donald:2014:ATM

REFERENCES


Duncan:2012:CAI


Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


delRey:2012:EDI

REFERENCES


Deng:2012:VIA


Dunkelman:2012:MEK


Dunkelman:2012:TCC


Durcheva:2015:SAI


David:2012:PRE

Dorn:2012:ECE


Dong:2012:KGD


Dong:2012:NDI


Deng:2014:CCC


Dodis:2013:OFE


Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. An empirical study of cryptographic misuse in An-
REFERENCES


**Embar:2014:PWO**


**Estebanez:2014:PMC**


**Engels:2012:HLA**


**Ebadi:2015:DPN**


**Eibach:2010:OGB**


**Enos:2015:IBS**


**Farash:2014:ECC**


**Farash:2014:SEI**


**Farash:2014:CIE**


**Fischlin:2012:PKC**

Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors. *Public Key Cryptography — PKC 2012: 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt,*
REFERENCES


Ferretti:2014:DCI


Fuglerud:2011:SIA


Fehr:2010:QC


Felten:2013:LBA


Faugere:2010:CLR


Fleischmann:2012:MFA


REFERENCES


REFERENCES


[Fan:2013:CEM]


[Forler:2012:DAC]


[Feng:2012:CAO]

[FLZ+12] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. Continuous non-malleable codes. *Lecture Notes in Computer Sci-
REFERENCES

Feng:2012:USD

Fraczek:2012:MSI

Fernandez-Mir:2012:SRA

Ferreira:2015:LPA
See also [?].

Fokkink:2012:TCG

Fox:2013:RLQ
Margalit Fox. The Rid-
REFERENCES


REFERENCES


Fridrich:2012:MTS


Frauchiger:2013:TRR


Feng:2011:ICP


Fang:2012:CCS


Ferguson:2010:CED


Feng:2011:GDA

Xiutao Feng, Zhenqing Shi, Chuankun Wu, and Deng-guo Feng. On guess and determine analysis of Rabbit. International Journal of Foundations of Com-
REFERENCES

Fujioka:2012:SHI


Fadlullah:2010:DCA


Fuchsbeuer:2011:CSV


Fulton:2010:BRB

Ben Fulton. Book review: Introduction to Modern Cryptography, by Jonathan


Jia Fan, Yuliang Zheng, and Xiaohu Tang. A new


REFERENCES


Lubos Gaspar, Viktor Fischer, Lilian Bossuet, and Robert Fouquet. Secure extension of FPGA general purpose processors for symmetric key cryptography with partial reconfiguration capabilities. *ACM Transactions on Reconfig-


REFERENCES


Gentry:2012:RSB


Gentry:2012:FHE


Gilad:2014:PHI


Georgiev:2012:MDC


Gilbert:2010:ACE

Henri Gilbert, editor. Advances in cryptology — Eu-
REFERENCES


REFERENCES


Gotzfried:2014:MAT


Garcia-Morchon:2015:HCR


Guo:2011:ISS


Guo:2014:SAS


Gao:2014:URA


Gong:2012:KNF

http://link.springer.com/chapter/10.1007/978-3-642-25286-0_1.

Goodin:2012:CBS

Dan Goodin. Crypto breakthrough shows Flame was designed by world-class scientists: The spy malware achieved an attack unlike any cryptographers have seen before. Web document., June 7, 2012. URL http://arstechnica.com/security/2012/06/flame-cryptobreakthrough/.

Garcia:2012:ERP


Gorski:2010:CDS


Groth:2012:NTN


Grosch:2012:EJI


Genkin:2014:GYH

Daniel Genkin, Itamar Pippman, and Eran Tromer. Get your hands off my laptop: Physical side-channel...
key-extraction attacks on PCs. Report, Technion and Tel Aviv University, Tel Aviv, Israel, July 31, 2014. 25 pp. URL http://www.cs.tau.ac.il/~tromer/handsoff/.

Gonzalez-Pardo:2012:CID


Greengard:2011:MRM


Girlichs:2012:ICD


Genkin:2013:RKE

REFERENCES


**Gazi:2012:EOS**


**Goodrich:2011:EAD**


**Grosse:2013:AS**


**Galindo:2014:LCL**


**Ghosh:2014:BBB**


**Gorbunov:2012:FEB**

REFERENCES


Houmansadr:2013:BCN

He:2013:HEH

Hao:2012:SAM

Hwang:2010:RIB

Hsu:2011:NL

Hore:2012:IED
Hernandez-Castro:2012:MTA


Hernandez-Castro:2012:AFH


Huang:2014:FOS


Huang:2014:FOS


Heninger:2012:MYP


Heath:2015:HNS

Nick Heath. Hacking the
REFERENCES


Hwang:2012:ABA


Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Harn:2014:MTS


Hoang:2014:IMD

REFERENCES

(1936-7414 (electronic).

Heyse:2012:TOC


Han:2011:PEB


Hayashi:2013:AEI


Huber:2014:TPW


Haitner:2011:PRI


Hinarejos:2015:MES

M. Francisca Hinarejos, Andreu Pere Isern-Deyà, Josep-Lluís Ferrer-Gomila, and Magdalena Payeras-Capellà. MC-2D: an efficient and scalable multi-coupon scheme. *The Com-
REFERENCES


Hinek:2010:CRV


Hinkelmann:2011:CPA


Hur:2014:SDR


Houmansadr:2014:NBW


Heyse:2012:LEA


Heil:2014:APH

Holenstein:2011:ERO


Harn:2010:AGK


Haza
[y:2010:EST


Hsieh:2014:AMU


Hmood:2015:ACA

Haider Salim Hmood, Zhitaung Li, Hasan Khalaf Abdulwahid, and Yang Zhang. Adaptive caching approach...
REFERENCES

143

**Hu:2012:VMS**


**Huang:2011:ISL**


**Huffmire:2010:SPR**


**Herranz:2011:RBS**


REFERENCES


[Hohenberger:2012:DDQ]


[Huang:2014:SWC]


[Herzberg:2012:TJA]


[Hore:2012:SMR]

REFERENCES

Hoang:2012:ESB


Hirt:2014:BA


Harnik:2010:CIC


Hyla:2012:CBE


Hazay:2014:OSA


Halder:2010:WTR

REFERENCES


[146]


REFERENCES

Herranz:2013:SMS

Haitner:2010:EIC

Hwang:2011:CDA

Homma:2014:TFD

Han:2013:IBD

Han:2014:IBS

Han:2012:PPD
Jinguang Han, Willy Susilo, Yi Mu, and Jun Yan. Privacy-preserving decen-
REFERENCES


REFERENCES


**Islam:2011:MDA**


**Ioannou:2014:PKC**


**Isobe:2012:SAL**


**Isobe:2012:SCL**


**Isobe:2012:SAL**


**Jie:2010:AAI**

Jie:2011:RGA


Prins:2011:DCA


Jakobsson:2012:AWD


Chang:2012:TRR


Jeong:2013:CBC


Jo:2014:ODE

REFERENCES


REFERENCES


REFERENCES

Jou13

JR13

JT12

JW14
Ari Juels and Bonnie Wong. The interplay of neuroscience and cryptography: technical perspective. Communications of the Association for Computing Machinery, 57(5):
REFERENCES

109, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


Katz:2013:RIB


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kim:2011:SSE


Koz:2012:ASE


Kraetzer:2012:PCS

REFERENCES

Karakoc:2013:BCL


Karakoc:2015:AKA


Kikuchi:2012:SSN


Kramer:2010:FDC


Kim:2012:SLT


Kwon:2010:SEB

REFERENCES

Khazaei:2010:NBS

Kastner:2010:AOT

Kim:2014:MBM

Khalil-Hani:2013:BEB

Kai:2011:CIS

Kiayias:2011:TCC
REFERENCES


REFERENCES

162


REFERENCES

[KLC+10] Ko, Jeonggil; Hyun; Lim, Yin; Chen, Rváz; Musvaloiu-E, Andreas; Terzis, Gerald M.; Masson, Tia; Gao, Walt; Destler, Leo; Selavo, and Richard P. Dutton. MEDiSN: Medical emergency detection in sensor networks. ACM Transactions on Embedded Computing Systems, 10(1): 11:1–11:??, August 2010. CODEN ??? ISSN 1539-9087.


Ayesha Kanwal, Rahat Masood, Muhammad Awais Shibli, and Rafia Mumtaz. Taxonomy for trust

**Khovratovich:2010:RCA**


**Khovratovich:2010:RRA**


**Koblitz:2010:BRB**


**Kasper:2012:SCA**


**Kang:2012:AKM**


**Kiltz:2011:EAH**

Kocabas:2012:CPB

[ KPKS12 ]


Keskinarkaus:2010:IWD

[ KPS10 ]


Krenn:2013:CCR

[ KPW13 ]


Krantz:2012:EAM

[ Kra12 ]


Kostinger:2012:SBL

[ KRB12 ]


Kannan:2013:NQF

[ KRDH13 ]

REFERENCES

Krenn:2013:AWI


King:2011:BBB


Kolesnikov:2012:LPP


Kim:2012:SSS


Klingler:2013:UPT


Kim:2012:SAH

REFERENCES


Karpovsky:2014:DSS


Koyama:2012:NTD


Kamal:2010:EIN


Kate:2010:PBO


Lu:2010:MSC


Lathey:2015:IEE


Lackey:2015:UHP

REFERENCES

Langley:2013:EDC

Launchbury:2012:TBC

Liu:2013:PAE

Luo:2012:ESI
Jianqiang Luo, Kevin D. Bowers, Alina Oprea, and Lihao Xu. Efficient software implementations of large finite fields GF(2^n) for secure storage applications. ACM Transactions on Storage, 8(1):2:1–2:??, February 2012. CODEN ????. ISSN 1553-3077 (print), 1553-3093 (electronic).

Lupu:2012:IBK

Lu:2013:CSA

Liu:2015:IAC
Qingzhong Liu and Zhongxue Chen. Improved approaches with calibrated neighboring joint density to steganalysis and seam-carved forgery detection

### Liu:2013:IAG


### Lathrop:2011:SPI


### Lavington:2012:ATH


### Li:2015:CEH


### Liang:2014:CCS


Li:2012:FDM

Li:2012:LFA

Liu:2012:FV

Lopez-Garcia:2014:PBB

Li:2014:SCA

Liu:2012:LF

Lee:2010:ISC
REFERENCES


Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe

[Li:2012:BVS]

[Li:2011:ICA]

[LHHR10]

[Jin:2014:SOA]

[LHM14]
REFERENCES

[176]

cross-layer reputation com-
putation model in wire-
less networks. The Com-
puter Journal, 58(4):656–
667, April 2015. CODEN
CMPJA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
comjnl.oxfordjournals.org/content/58/4/656.

[LHYZ12] Yan-Xiao Liu, Lein Harn,
Ching-Nung Yang, and
Yu-Qing Zhang. Efﬁ-
cient (n, t, n) secret shar-
ing schemes. The Jour-
nal of Systems and Soft-
ware, 85(6):1325–1332,
June 2012. CODEN JS-
SODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0164121212000234.

[Li10] Mengdong Li. Preimage
awareness proofs of two
compression functions. In
Yang [Yan10], pages 660–
664. ISBN 1-4244-6942-
2. LCCN QA76.9.A25.
URL http://ieeexplore.
ieee.org/servlet/opac?pu
number=5680738.

on the average number of
RSA ﬁxed points. Theo-
retical Computer Science,
412(35):4729–4737, August
2011. CODEN TC-
SCDI. ISSN 0304-3975
(print), 1879-2294 (elec-
tronic).

[Lin14a] Pei-Yu Lin. Impercepti-
ble visible watermarking
based on postcamera his-
togram operation. The
Journal of Systems and
Software, 95(??):194–208,
September 2014. CODEN
JSSODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0164121214001071.

[Li14b] Yehuda Lindell, editor.
Theory of cryptography:
11th Theory of Crypto-
graphy Conference, TCC
2014, San Diego, CA,
USA, February 24–26,
2014 proceedings, volume
8349 of Lecture Notes in
Computer Science. Spring-
er-Verlag, Berlin, Ger-
many / Heidelberg, Ger-
many / London, UK / etc.,
2014. ISBN 3-642-
54241-7 (paperback), 3-
642-54242-5 (ebk.). ISSN
0302-9743 (print), 1611-
3349 (electronic). LCCN
URL http://www.springerlink.
com/content/978-3-642-
54242-8.

[Lin15] Pei-Yu Lin. Double veriﬁ-

**Litton:2014:TFA**


**Liu:2015:LBD**


**Li:2012:OEA**


**Laszka:2014:STC**


**Li:2012:BIB**


**Lee:2014:SPB**

REFERENCES


Li:2012:IBO


Lev:2013:ABN

[LKAT12]


Lee:2015:TSS

[LKCLKL13]


Lee:2010:PMB


Lee:2011:TA

Li:2015:IBE


Li:2012:RIB


Lee:2006:DCK


Lai:2013:SAS


Lu:2012:IEC


Lee:2006:DCK

REFERENCES


REFERENCES

CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Li:2011:NRA

Lv:2011:NTP

Li:2013:ESC

Liu:2015:SAB
Liu:2013:GPB


Lopriore:2012:EPP


Lopriore:2015:PCR


Ling:2012:SHS


**Lee:2013:CCM**


**Le:2014:IMX**


**Lee:2014:NDH**


**Li:2015:FSC**


**Lysanskaya:2010:AEC**


**Lin:2011:CNS**

[LTW11] Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, ed-


Allison Lewko and Brent Waters. Decentralizing attribute-based encryp-
REFERENCES

187


[LWCJ14] Hongbo Liu, Hui Wang, Yingying Chen, and Day-
REFERENCES


Liu:2011:SBA


Liu:2012:HOM


Liu:2010:NDC


Liu:2010:SET


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-27890-7_3/

Li:2011:NIW


Li:2014:IBD


Li:2014:EMK


Lai:2012:RHB


Li:2012:ESD


Luo:2014:ARP

Jia Ning Luo and Ming Hour Yang. An anonymous e-rental protocol based on ID-based cryptography and NFC. The Journal of
REFERENCES


Lu:2014:DAN

Lu:2014:DAN


Liao:2010:MPC

Liao:2010:MPC


Li:2013:SSS

Li:2013:SSS


Liu:2012:SOCa


Luo:2012:LVT

Luo:2012:LVT


Liu:2014:PKE

Liu:2014:PKE

Shengli Liu, Fangguo Zhang, and Kefei Chen. Public-key encryption scheme with selective opening chosen-ciphertext security

**Liu:2014:CRA**


**Li:2010:PES**


**Li:2012:ESS**


**MacCormick:2012:NAC**


**Michail:2012:EHT**

Malkin:2013:SCB


Mangard:2013:KSL


Martin:2010:XMA


Matsuda:2014:IBP


Maurer:2012:CCN


Mazurczyk:2013:VSD


Milo:2011:FGB

Malone:2013:MOD


Massolino:2015:OSC


Mukhopadhyay:2011:PEA


Madanayake:2012:BPS


McGrayne:2011:TWH


McKay:2010:SLB

Sinclair McKay. *The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there*. Aurum, London,
REFERENCES


REFERENCES

cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf.


REFERENCES

Marmol:2010:TPA


Matsuda:2014:CCS


Meziani:2012:IPS


Miller:2014:ADS


Mou:2013:CBC


Micciancio:2010:FGC

REFERENCES

Michiels:2010:OWB

Martinez-Julia:2012:NIB

Martinez-Julia:2013:BSI

Mohanty:2011:RTP

Moessner:2012:SAS

Muller:2012:HPC

Malik:2012:AIC
Sana Ambreen Malik, Asifullah Khan, Mutawarra

Marconato:2013:VLC


Mancillas-Lopez:2010:RHI


Manzanares-Lopez:2012:ICU

Pilar Manzanares-Lopez, Josemari Malgosa-Sanahuja, and Juan Pedro Munoz-Gea. The importance

**Madhusudhan:2012:DIB**


**Meshram:2013:IBC**


**Maity:2014:FIR**


**Mondal:2014:DSM**


**Moldovyan:2012:BBD**

Mahmoody:2014:PPK


Maity:2013:CRS


Matsuo:2012:MAK


Meshram:2012:IBC


Mukhopadhyay:2014:EMP

Minier:2012:RK1


Mizuki:2011:ASN


Maimut:2012:LCR


Minamoto:2014:BDI


Mone:2013:FPE


Moore:2012:RFF

Moo:2014:DMW


Morad:2012:OEA


Minier:2012:EEC


Mironov:2012:IDP


Mukhamedov:2010:IEP


Maimut:2014:AET


Marasco:2014:SAS

Emanuela Marasco and Arun Ross. A survey on antispooﬁng schemes for

**Micali:2014:CMS**


**Moghadam:2010:DRN**


**Mendel:2012:DAL**


**Maitra:2012:NAC**


**Maitra:2013:DSM**


**Maitra:2013:HEM**

Subhashis Maitra and Amitabha Sinha. High efficiency MAC unit used in digital signal process-

**Maitra:2013:HPM**


**Myers:2012:BCM**


**Marton:2010:RDC**


**Mosca:2013:QKD**


**Morozov:2012:ZKP**


**Malkin:2011:ECS**

Tal Malkin, Isamu Teranishi, and Moti Yung. Ef-
References


K. Preetha Mathew, Sachin Vasant, Sridhar Venkatesan, and C. Pandu Rangan. An efficient IND-CCA2 secure variant of the Niederreiter encryption scheme in the standard model. Lecture

Ma:2012:CIS


[MWZ12] Chun-Guang Ma, Ding Wang, and Qi-Ming Zhang.


Manshaei:2013:GTM


Ma:2015:PKE

[NA10a] Naya Nagy and Selim G. Akl. One-time pads without prior encounter. Parallel Processing Letters,
REFERENCES

Nagy:2010:QCS

Naccache:2012:CST

Noureddine:2013:AMT

Naskar:2012:FIR

Naskar:2013:GTL

Naranjo:2013:FD
J. A. M. Naranjo, F. Cores, L. G. Casado, and F. Guirado. Fully distributed authentication with locality exploitation for the CoDiP2P peer-to-peer computing

Narasimhan:2013:HTD


Newell:2013:PCD


Naeem:2014:EIC


Niev negotel:2002:FLM


NIST:2012:RRN

REFERENCES

Special Publication 800-90, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

[NLY15] NIST:2013:CSS


[NLYZ12] Ning:2012:DCA


REFERENCES


Salman Niksefat, Babak Sadeghiyan, Payman Mohassan, and Saeed Sadeghian. ZIDS: a privacy-preserving...

Nguyen:2012:LRS


Nguyen:2010:LAS


Nie:2013:CHB


Newell:2014:NCR


Niu:2015:NAS

Ben Niu, Xiaoyan Zhu, Qinghua Li, Jie Chen, and Hui Li. A novel attack to spatial cloaking schemes in location-based services. *Future Generation Com-
REFERENCES


Oliveira:2012:STA


Ohtake:2012:AAH


Orlandi:2014:SCN


Oppliger:2011:CC


Orejel:2014:E


Owczarek:2012:LPL

Okamoto:2012:AAH


Otmani:2010:CTM


Ohzeki:2012:NWM


Ortiz-Yepes:2014:BSA


Praba:2010:MAC


Pandey:2014:ACR

REFERENCES


REFERENCES

Pippal:2012:SVU

Pearson:2011:NWC

Persichetti:2013:SAH

Peterson:2011:SWS

Petrlic:2012:PRE

Pfleeger:2010:CJD


Marios Papas, Thomas Houit, Derek Nowrouzezahrai, Markus Gross, and Wojciech Jarosz. The magic lens: refractive steganography. *ACM Transactions*
REFERENCES

on Graphics, 31(6):186:–
186:??, November 2012.
CODEN ATGRDF. ISSN
0730-0301 (print), 1557-
7368 (electronic).

Pieprzyk:2010:TCC

Josef Pieprzyk, editor. Topics in cryptology —
CT-RSA 2010: the 10th cryptographers’ track at
the RSA conference 2010,
San Francisco, CA, USA,
March 1–5, 2010. Pro-
cceedings, volume 5985 of
Lecture notes in computer
science. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2010. ISBN
3-642-11924-7 (softcover).
LCCN ???.

Pointcheval:2012:ACE

David Pointcheval and
Thomas Johansson, editors. Advances in Crypt-
tology — EUROCRYPT
2012: 31st Annual In-
ternational Conference on
the Theory and Applica-
tions of Cryptographic
Techniques, Cambridge,
UK, April 15–19. Proceed-
ings, volume 7237 of Lec-
ture Notes in Computer
Science. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2012. COD-
DEN LNCS9. ISBN 3-
642-29010-8. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://

Peter:2012:AHE

Andreas Peter, Max Kron-
berg, Wilke Trei, and Ste-
fan Katzenbeisser. Add-
itively homomorphic en-
cryption with a double de-
cryption mechanism, re-
visited. Lecture Notes in
Computer Science, 7483:
242–257, 2012. COD-
DEN LNCS9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-33383-5_15/.

Perez:2011:FDS

Alejandro Pérez, Gabriel
López, Óscar Cánovas,
and Antonio F. Gómez-
Skarmeta. Formal descrip-
tion of the SWIFT iden-
tity management frame-
work. Future Generation
Computer Systems, 27(8):
1113–1123, October 2011.
CODEN FGSEVI. ISSN
0167-739X (print), 1872-
7115 (electronic).

Pang:2013:IMA

Liaojun Pang, Huixian Li,
Qingqi Pei, and Yu-
mín Wang. Improvement
on Meshram et al.’s ID-
based cryptographic mech-
anism. Information Pro-
cessing Letters, 113(19-
21):789–792, September/
Peris-Lopez:2010:CSP


Poh:2012:SEC


Poursakidis:2010:TPC


Powers:2014:OSCa


Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC


Pendl:2012:ECC


Pyun:2012:IBF


Pathak:2012:PPS


Phan:2012:DDB

Duong Hieu Phan, David Pointcheval, and Mario Streifer. Decentralized dynamic broadcast encryption. Lecture Notes in
REFERENCES


Phan:2012:MBT


Papadopoulos:2015:PAP


Pandey:2012:PPS


Piret:2012:PBC


Popa:2012:CPQ


Priemuth-Schmid:2012:ASV

Deike Priemuth-Schmid. Attacks on simplified ver-
REFERENCES

com/chapter/10.1007/978-3-642-25261-7_9/.

Pereira:2013:SLC


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC


Papakostas:2014:MBL

REFERENCES


Pudovkina:2012:RKA


[Pei2013:ARW]


[PWLL13]

Pongaliur:2013:SNS


[PWVT12]


[Poller:2012:EIC]


[Philippaerts:2013:CMC]

REFERENCES

Pei:2015:SWT


Papadopoulos:2010:CAR


Patsakis:2015:PSM


Qian:2014:IAF


Rabin:2010:ACC


Rankin:2010:HLH


Rankin:2014:HEY

[Ran14] Kyle Rankin. Hack and /: encrypt your dog (Mutt


Regev:2011:QOW


Rahaman:2010:STB


Rose:2011:KBT


Rao:2012:SSA


Rifa-Pous:2012:AHD


Rhee:2010:TSS

Hyun Sook Rhee, Jong Hwan Park, Willy Susilo, and Dong Hoon Lee. Trapdoor security in a searchable public-key encryption scheme with a designated tester. The Journal of Sys-


See also news story [Ano15a].


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


[Sar12] Neyire Deniz Sarier. Security notions of biometric remote authenti-


REFERENCES


REFERENCES


Seberry:2010:CTAa


Seberry:2010:CTAb


Saleh:2010:GTF


Shen:2012:PAS


Shakiba:2010:ID


Souissi:2012:OCP

[YSC12] Youssef Souissi, Nicolas Debande, Sami Mekki, Sylvain Guilley, and Ali

**Maalaoui.**

[2012:MK]


**Shakiba:2014:CCI**

[SDM14]


**Seo:2014:RHI**

[SE14]


**Sendrier:2010:PQC**


**Sasaki:2012:IKK**

[SEHK12]


**Savas:2014:SMQ**
Su:2012:IIN

Shabtai:2010:SAP

Shankar:2012:BDF

Sipiran:2014:SCA
Shaolan:2011:EDE


Seyedzadeh:2011:IEA


Song:2015:ADT


Shallit:2010:BRB


Shen:2014:LES


Shim:2011:SAT

REFERENCES


Shparlinski:2003:CAA

Shparlinski:2010:NWP

Suoranta:2012:ASM

Shyu:2015:VCR

Satir:2012:CBT

Siad:2012:NAP
Amar Siad. A new approach for private searches on public-key encrypted data. Lecture Notes in Computer Science, 7394:160–173, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-


Seo:2015:AEC

Szalachowski:2010:CCG

Scheidat:2012:STT

Schmitz:2012:NAC

Srivatsa:2011:ESA

Schultz:2010:MMP
[SL10] David Schultz, Barbara Liskov, and Moses Liskov. MPSS: Mobile Proactive


### References

**Seyedzadeh:2014:RCI**


**Suriadi:2012:PCV**


**Shiaeles:2015:FI**


**Schaumont:2015:IEP**


**Serwadda:2013:ELK**


**Sun:2013:IUP**

San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray

Shaikh:2010:CTO


Schilling:2012:ATU


Sur:2012:SSU


Stefan:2012:ACT


Saxena:2010:SGC


REFERENCES

CODEN ???? ISSN 0219-4678.

Smith:2011:SMC

Shrivastava:2012:UIE

Sahai:2012:DCC

Sood:2011:SDI

Strydis:2013:SAP
REFERENCES


REFERENCES

Stipcevic:2011:QRN


Stolte:2012:EDA


Suciu:2012:SED


Sung:2011:DCE


Svozil:2014:NCC


Svaba:2010:PKC


Shoufan:2010:NCA

A. Shoufan, T. Wink, H. G. Molter, S. A. Huss, and

**Sahillioglu:2014:SCM**


**Seo:2013:PIC**

Jae Woo Seo, Dae Hyun Yum, and Pil Joong Lee. Proxy-invisible CCA-secure type-based proxy re-encryption without rand...


REFERENCES


Ferucio Laurentiu Tiplea and Constantin Catalin Dragan. A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme. Information...
REFERENCES


Tao:2013:SMS


Terai:2011:BRB

Tamir Tassa and Ehud Gudes. Secure distributed computation of anonymized views of shared databases. ACM Trans-

Tassa:2012:SDC


Tian:2012:TOE


Tian:2015:IBP


Tian:2012:TOE

Rasha Thabit and Bee Ee Khoo. Robust reversible watermarking scheme using Slantlet transform matrix. The Journal of Systems and Software, 88(??):74–86, Febru-

Thabit:2014:RRW

Tu:2014:EPB

[TKHK14] Hang Tu, Neeraj Kumar, Debiao He, and Jongsung Kim. An efficient password-based
three-party authenticated multiple key exchange protocol for wireless mobile networks. The Journal
of Supercomputing, 70(1): 224–235, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-

Tani:2012:EQA

???? ISSN 1942-3454 (print), 1942-3462 (electronic).

Tu:2013:PAQ

[TKMZ13] Stephen Tu, M. Frans Kaashoek, Samuel Madden, and Nickolai Zeldovich. Processing analytical
queries over encrypted data. Proceedings of the VLDB Endowment, 6(5): 289–300, March 2013. CO-
DEN ????. ISSN 2150-8097.

Tariq:2014:SBL


Tsaur:2012:ESM

[TLL12] Woei-Jiunn Tsaur, Jia-Hong Li, and Wei-Bin Lee. An efficient and secure multi-server authentica-
SODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://

Tsai:2013:ZWS

Hung-Hsu Tsai, Yen-Shou Lai, and Shih-Che Lo. A zero-watermark scheme with geometrical invari-
ants using SVM and PSO.

**Tetali:2013:MSA**


**Tang:2012:RSS**


**Tsay:2012:VUL**


**Tormo:2013:IMP**


Jia Tao, Giora Slutzki, and Vasant Honavar. A conceptual framework for secrecy-preserving reasoning in knowledge bases. *ACM


REFERENCES


REFERENCES

Ulutas:2013:ISI


Vaikuntanathan:2011:CBN


Vaikuntanathan:2012:HCE


Valamehr:2012:IRM


vanDam:2011:TQC

REFERENCES

January–February 2014. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Venafi Labs: 2014: VLQ


Vetter: 2010: ABV


Viennot: 2014: MSG


Vu: 2015: NAN


Vleju: 2012: CCA


Vivek: 2014: CSC


Vliegen: 2015: SRD


Xiang Wang. A new SDVS based on NTRUSign. In...

Wang:2013:CRA


Wang:2014:IIA


Ward:2011:CCM


Watt:2010:IPI


Waters:2012:FER


Wang:2012:PCE

Qingju Wang and Andrey Bogdanov. The provable constructive effect of diffusion switching mechanism in CLEFIA-type


Yuechuan Wei, Chao Li, and Dan Cao. Improved related-key rectangle attack on the full HAS-160 encryption mode. International Journal of Foundations of Computer Science (IJFCS), 23(3):733–735, April 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).


Kan Wang, Zhe-Ming Lu, and Yong-Jian Hu. A high capacity lossless data hiding scheme for JPEG images. The
REFERENCES


Wu:2015:TRM


Wang:2012:RTC


Wu:2012:PSC


Wu:2010:IBM


Wang:2013:NMC


Wu:2012:RIB


Wu:2012:AST


Willis:2013:IFI


Wang:2014:ATF

Ding Wang and Ping Wang. On the anonymity of two-factor authentication schemes for wire-

Wen:2014:MZC


Wen:2014:MMW


Weng:2012:NCC


Wang:2011:CIB


Wang:2011:CHI

REFERENCES

2011. CODEN JSSODM. ISSN 0164-1212.

Weir:2012:AVC

Wang:2014:NAI

Weir:2012:IHV

Wang:2013:NSW

Wei:2014:IDC

Wang:2014:CGR
Wen:2011:DSH


Wei:2015:CPK


Weng:2013:VWI


Wei:2012:CSO


Wei:2012:GOP


Wang:2012:NIS

REFERENCES


[XCL13]

[XHCH14]

[XHCH12]
Xie:2012:RAA


Xiong:2012:PPK


Xu:2013:PKE


Xue:2013:TCB


Xie:2013:ECP

REFERENCES

Xin:2010:IEB


Xiao:2010:TAT


Xie:2012:ORI


Xie:2012:SCP

Qi Xie, Guilin Wang, Fubiao Xia, and Deren Chen. Self-certified proxy convertible authenticated en-
Xie:2012:DPK


Xing-Yuan:2011:PRS


Xiong:2012:CLR


Yamaguchi:2012:EVC


Yu:2015:SDS


Yang:2010:PII

[Yan10] Yixian Yang, editor. Pro-

Yang:2011:PQC


Yang:2011:GSS


Yang:2012:PST


Yuan:2013:PVQ


Yao:2015:LAB

Xuanxia Yao, Zhi Chen,

**Yuen:2012:IBE**


**Yamada:2012:PBR**


**Yoshida:2012:OGT**


**Yang:2015:SHI**


**Yang:2014:MDF**

Yo:2010:IRR


Yu:2012:IRI


Young:2013:TPC


Yum:2012:OPE


Yoshino:2012:SIP


Yum:2011:ACO

Yuen:2013:ELT


Yang:2012:WSI


You:2012:DDS


Yi:2013:ETS


Ying:2013:PPB


Yu:2010:PSI

Gang Yu, Xiaoxiao Ma, Yong Shen, and Wenbao Han. Provable se-

Yu:2011:CLE


Young:2015:DWE


Yavuz:2012:BFB


Yong:2011:SPP


Yoneyama:2012:ORA

Kazuki Yoneyama. One-

Yang:2012:EMA


Yengisetty:2011:AVC


Yang:2012:SAK


Yang:2015:EPS


Yao:2014:NCR


Yeh:2010:TRR

Kuo-Hui Yeh, Chunhua Su,

Ylonen:2014:SAA


Yang:2011:CCK


Yang:2011:CPK


Yang Yang, Xiaohu Tang, and Udaya Parampalli. Authentication codes from difference balanced functions. *International Journal...*
Yasuda:2012:ASM


Yao:2010:ASP


Yang:2015:RCI


Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM

Zhiwei Yu, Chaokun Wang, Clark Thomborson, Jianmin Wang, Shiguuo Lian,

**[Yu:2012:SME]**


**[Yoon:2011:SBC]**


**[Yang:2012:BPN]**


**[Yang:2012:NIB]**


**[Yang:2012:LUC]**


**Yang:2014:PST**

[YZZ+14]

[ZC13]


**Zhang:2011:TNT**

[ZBR11]

[ZCC15]

[ZCL+12] Zhifang Zhang, Yeow Meng Chee, San Ling, Mulan Liu, and Huaxiong Wang. Threshold changeable se-

**Zhang:2014:GCS**


**Zhang:2012:AOP**


**Zetter:2014:CZD**


**Zhao:2010:PSA**


**Gao:2012:DES**


**Zadeh:2015:ASP**

Abdullah Abdulah Zadeh and Howard M. Heys. Application of simple power analysis to stream ciphers.

**Zhang:2012:LDC**


**Zhang:2015:STR**


**Zhu:2015:IDM**


**Zhu:2013:TSC**


**Zhou:2015:EPP**


**Zimand:2010:SEC**

REFERENCES

4, 2010. CODEN TC-SCDl. ISSN 0304-3975 (print), 1879-2294 (electronic).


[ZLQ15] Jiliang Zhang, Yaping Lin, and Gang Qu. Reconfigurable binding against FPGA replay attacks. *ACM Transactions on De-

Zhang:2012:CCB

Zhang:2010:ESP

Zhang:2010:NSS

Zielinska:2014:TS

Zafar:2010:GRN
REFERENCES


REFERENCES

Zwattendorfer:2012:CBL


Zhang:2015:FAA


Zhang:2014:LFL


Zilberberg:2013:PCM


Zhang:2015:FER


Mingwu Zhang, Bo Yang, and Tsuyoshi Takagi. Bounded leakage-resilient functional encryption with hidden vector predicate.
REFERENCES


Zhang:2011:EPK


Zhao:2012:FCS

