
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/

22 October 2019
Version 1.489

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N)
[Bai10, YC11], (n, t, n) [LHYZ12], (t, n)
[QD16, ZPWY12]. 0 [XHX+17]. 1
[XHX+17]. 1, 2, 3 [SMDS11]. 11 [LJ17]. 13
[Blo15]. 2 [DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGLL10, WY12]. 22 [MNP12]. 2k
[Sun16]. 3 [AP10, Bro19, CG12b, DWZW12,
FWS13, GZHD12, GH11a, KWS+12, LJ17,
LJ15, MKH+12, RS16, SS10b, SS12a, SGS14,
WSSO12, tWmC12, YT11a, YI14, YPRI17].
32 x 32 [SA14]. 3 x 3 [ÁMVZ12]. 4
[COP+14, DWZ12, HLYS14]. $49.00
[Sch15a]. 5 [YN19]. 8 [LPO+17, ZSH+19].
$9 [APPVP15]. = [JJUW10]. + [PYH+18]. 2
[YNX+16]. 3 [LHM14]. MT [HRB13]. α

[TTL10]. c [KRDH13]. d [QD16]. d x d
[KA17]. ℓ [ZTL15]. Fp + νFp [WGF16]. γ
[DWZ12]. GF(2)[x] [SF12]. GF(2n)
[HJ19, SKH15]. GF(2n) [LBOX12]. K
[FXP12, FR16, CHX13, XMY+17, XLP+18,
ZZC17, ZHT16]. L(1/4 + o(1)) [Jou13]. M
[MMSD13, ÖS11]. F3659 [AMORH13]. Fq
[SS13]. NP [HN10]. GF(q) [LPdS10]. LWE
[BV14]. μ [Jia14a]. N [FR16].

n x k(k ≥ n/2) [MC11]. O(d134) [KA17],
O(n2) [KS11]. P [DG17]. π [EHKSS19]. ±1
[HZW+14]. q [GMS11]. S [LJ15]. t
[HJM+11, Oba11]. w [Kre13].

-band [MMSD13]. -Bit [LPO+17, ZSH+19].
-boxes [LJ15]. -Cheater [Oba11]. -Cipher
[EHKSS19]. -D [MCDB12]. -dimensional
[DWZ12, QD16]. -Diversity [ZTL15].
-Encoded [DG17]. -Encoding [XHX+17].  
-Means [KRDH13]. -Multiple [LTC+15b].  
-nearest [XMY+17]. -NN [ZZC17, ZHT16].  
-Round [COP+14, LJ17, Blo15]. -SDH [GMS11].  
.onion [Boy16].  
0.13um [KLM+12].  
1 [AAE+14, Ano15b, BH15, Bar16, CGCS12, Ful10, MSas12, SKP15].  
1-58488-551-3 [Full09]. *10 [Ano10].  
1024 [Bro17, Win17].  
10Gbps [PRGBSAC19].  
10th [LTW11, Pie10, Sah13].  
11th [GG10, Lin14b].  
128 [TSLL11].  
128-Bit [GV14b].  
12th [BC11, LH10a].  
13-round [TSLL11].  
13th [Che11].  
15th [Dan12, FBM12].  
16 [ZAG19].  
160 [WLC12].  
16th [Abe10].  
17th [LW11a, Wes16, Ano10].  
18th [MV12].  
192 [Blo15].  
1st [CBG+10].  
2.0 [NVM+17, PC16].  
2000 [ZC12].  
2003 [Sha10].  
2008 [Mei10].  
2010 [Ano10, Ano11b, CGB+10].  
2011 [Gre11, LCK11].  
2013 [IEE13].  
2016 [Wes16].  
21st [IEE13, JY14].  
256 [AKY13, App15, MAK+12].  
29th [Gil10].  
2D [HIDFGPC15].  
3 [ABM+12, BD15, jCPB+12, Ful10, LC17].  
30th [Rab10].  
31st [FJ12].  
384-bit [MMN12].  
3GPP [FPBG14].  
4 [Jac16, YYO15].  
42-step [AKY13].  
4765 [ABC+12].  
4G [FMA+18].  
4th [Yan11].  
5/3 [Ara13].  
512 [GV14b].  
512-bit [APPVP15].  
51st [IEE10].  
52nd [IEE11b].  
5G [CML+18, FMA+18].  
5th [BYL10, vDKS11].  
6 [Ano17b, Bai12, Mur10].  
65th [Nac12].  
72 [HYS18].  
8.8/11.2 [GLIC10].  
802.11 [FMA+18].  
802.11s [BOB13].  
802.15.4 [NBZ17].  
802.16e [Cl11].  
802.16m [FZZ+12].  
85 [WZM12a].  
959 [ÁCZ16].  
978 [Ano15b, Ano17b, Bai12, Mur10].  
978-0-691-14175-6 [Ano17b].  
978-0-8218-8321-1 [Sch15a].  
978-1-4200-4757-8 [Joh10].  
978-1-78548-004-1 [Ano15b].  
978-1-84832-615-6 [Bai12].  
978-3-540-49243-6 [Mur10].  
9798 [BCM12, BCM13].  
9th [Cra12, GLIC10, HWG10].  
AAA [BT18, MLM16].  
AAA-based [MLM16].  
AAoT [FQZF18].  
Abandon [Loe15].  
ABE [FJHJ12, HQZH14, HLC+19, OSNZ19, QZZ18, TY16a, YMC+17, ZSW+18b].  
abelian [CDSLY14, LR15].  
ability [WS12].  
absence [AGH+17].  
Abstract [Bul10a, CFR11, MZ17b].  
Abusing [VWC19].  
Accelerating [CMO+16, DOS15, SKH15, XZL+19].  
Accelerator [MSR+17, MRL+18, PC16, WOLP15].  
Accelerators [AW15, AW17, GP17, HKL+14, OSH16, BAB+13, KKJ+16].  
accelerometers [ZZL+18].  
Acceptance [SPM+13].  
Access [AWSS17, BFK+10, CO11, CGH11, DLZ+16b, FCM14, HLC+18, HP12, LGLK17, LPL15, MSI18, MK12b, NA10b, PV17, PB12, QZL+16a, RSN14, SGC14, SC12, WS13, XMLC13, XHZ+19, YTH17, YSS14, ARL13, ATRK+17, ACK+10, AMHJ10, CLH+16, Cra11, DFJ+10, FNWL18, FS18,  
AECG13].  
AECG13 [FJHJ12, HQZH14, HLC+19, OSNZ19, QZZ18, TY16a, YMC+17, ZSW+18b].  
abelian [CDSLY14, LR15].  
ability [WS12].  
absence [AGH+17].  
Abstract [Bul10a, CFR11, MZ17b].  
Abusing [VWC19].  
Accelerating [CMO+16, DOS15, SKH15, XZL+19].  
Accelerator [MSR+17, MRL+18, PC16, WOLP15].  
Accelerators [AW15, AW17, GP17, HKL+14, OSH16, BAB+13, KKJ+16].  
accelerometers [ZZL+18].  
Acceptance [SPM+13].  
Access [AWSS17, BFK+10, CO11, CGH11, DLZ+16b, FCM14, HLC+18, HP12, LGLK17, LPL15, MSI18, MK12b, NA10b, PV17, PB12, QZL+16a, RSN14, SGC14, SC12, WS13, XMLC13, XHZ+19, YTH17, YSS14, ARL13, ATRK+17, ACK+10, AMHJ10, CLH+16, Cra11, DFJ+10, FNWL18, FS18,
HZL18, HK17, JAS+11, LCL+17a, LCL+15, LHH+18, MDHM18, MLM16, NZM10, NAL17, QCX18, RR17, Shy15, Tan12b, TODQ18, Wan18, WS12, XHH12, XYML19, YWJ+19, ZF15, ZML17, ZVH14, ZW+16, ZWS+18, ZFH+18, ZL+18.


Aggregating [DP12]. Aggregation
[ARWK19, BJL16, LHKR10, SP15b,
ZHW+16, GLM’19, RR17, WMYR16].
Aging [SKV12]. Agnes [Bur11, Joh15].
Agreement [BSBB19, Chi16, HCL
+14, HEC+12, KMZS19, MNS11, TM12, WSS12,
XLM+12, XGLM14, XZJW15, YLSZ19,
APK+18, AN15, BGAD12, CSD18, CTL13,
DLK+16, GH16, HPC12, HWB10, HWB12,
ISC+16, IB11, IOV+18, KS11, KIH19, KP18,
KLW+16, XCL13, XXY19, XMHD13,
XHM14, YZ+14, ZWQ+11, ZT16,
ZGL+18, ZZ15, OHJ10]. agriculture
[APK+18]. Aided
[BGK12, BCGK12, BGB12, Gop19,
GMSV14, MV19, ABBD13, LYL15,
SGJ+18, SSAF11, WLFX17].
AIPISteg [AGLW16].
Air
[AUMT16, VOGB18, ZWX+18]. aircraft
[XWZW16]. Airflow [RSCX18]. Airway
[RSCX18]. AK [XHC+12]. AK-PPM
[XHC+12]. AKA [LLS13]. AKF [KDH15].
ai [LLW16, LLSW16, MWZ12, PLPW13,
SBS+12, Mac14, Keb15]. al-Qaeda
[Mac14, Keb15]. al. [ABJ13, SPLHC14].
Alan [CS12, Don14, Hel17, LCKBJ12].
Algebra
[PWB317, Xie12, BS15, Bul10b,
CFR11, DWZ12, FGPGP14]. Algebraic
[HIJ+19, HLC+19, SK11, Tam15, Wat10,
Bul10a, CFR11, SA14, YTM+14].
Algorithm
[AA19, ABCL17, Ano11b,
AK14, BGJT14, BKLS18, CNR14, jCPB+12,
DCM18, ESS12, GKS17, JLH12, JSZS12,
JHJN12, JLM16, KB10, LL14a, LLL17a,
LLLH18, MSR+17, MRL+18, NdMMW16,
NV10, RR11, RVRSCM12, WHZ12,
WZCC18, YPR17, YH16, ZSW+12, Ant14,
BGJT13, BMB16, CG12b, Chm10, EEAZ13,
JK13, Jon13, KY10, KHMB13, LC17, LR15,
MS12a, MM14b, MNM+16, MN14, PGLL10,
PA10, PC14, SH11, SLM10, SWW+17,
jT12b, TTL10, WGG+12, XTK10, YWL+17,
ZLW+12, ZL12, ÁCZ16, ZOC10].
Algorithmic [GO17, KRH18, AY12].
Algorithmics [Gas17]. Algorithms
[AMKA17, AB10b, BCG12a, BJ10b, CN12,
GP17, KRDH13, MR14a, MM17, TKM12,
WH18, YS15, ZW15, AGHP14, Fri10a,
LK10, Mac12, NACL12, NCI13, OO10,
OO18, Xie12]. Ali [ABJ13]. Aliens [Sch18].
Alignment [Don14, IA15]. All-But-Many
[CCL+19]. all-seeing [Tox14]. Allocation
[JWNS19]. Allowing [PRC12]. Allows
[Bro17]. Almost
[BKST18, FFL12, GDCC16, Ob11].
Almost-Tight [GDCC16].
Almost-Universal [BKST18]. Alpha
[MV18]. Altera [SMOP15]. alternate
[ZLW+12]. Alternating [BKLS12, KDH15].
AMBTC [KSSY12]. AMD
[Arn19, MZLS18]. America
[AB10a, Bha16, Fag17]. American
[Sch15a, Mun17]. Americans [ABJ13].
Amoeba [MPA+18]. among
[BP11, MPJ+16, SS17]. amount [EEAZ13].
Amplification [AFB12, HMR14]. Analog
[KOP12, SOS15]. Analyses [ZPXX17].
Analysing [GRL12]. Analysis
[ABS+12, ARP12, BRS17, BBB+16a, BC14,
BS14, BKLS18, CFE16, CGG+16, CGL+12,
DKMR15, FSWF11, GZZ+13, GWMW,
GLG12, GA19, HC12, HH+13, HZW17,
HB17, IBM13a, IS12, JRT12a, KE19, KOP12,
Kre13, LPS12, LTKP16, LCK11, LLW16,
LGL12, MD12b, MAS16, MRTV12, MR10,
NDC+13, NSA15, NAL17, PH2a, PFS12,
PS14, RZZ+15, Rao10, RBS+17, SK11,
SY15a, SR2a, Shl11, SRM18, SZDL14,
SCG+14, VCK15, WDDW12, YZLC12,
ZHI15, ZAG19, ZBPF18, Aia15, AFC16,
AN15, BNY14, CFH+13, CFL13, CDWM19,
DMV15, DK17, DHW+13, DIMT12,
FTV+10, FAA+18, FHM+12, HMI10, Lan11,
MF13, NLYZ12, OMPSP+19, PPA18,
PL16, QGGL13, RITF+11, SKEG14,
TQL+14, TLLM13, Tso13, VS11, Ven14,
Analysis-Based [RZZ+15]. Analytic [Kuz11, Sha10, ZW15]. analytical [CDPLCA16, TKMZ13]. analytically [BLV17].

Analysis-Based [RZZ+15], Analytic [Kuz11, Sha10, ZW15], Analytical [CDPLCA16, TKMZ13], analytically [BLV17].

analyzing [HREJ14, KLN15, YGD+17]. anchors [BCC+19]. Ancient [Fox13, Rao10], and/or [YLA+13].

Android [Chi13b, EBFK13, FHM+12, SFE10, YTF+18], Android-Powered [SFE10].

Angle-Based [ZPW16]. Angular [pNyWyY+14]. Anisotropic [ZZCJ14]. Annotated [ATS15].

Announcing [SBK+17]. Annual [Ano10, IEE10, IEE11b, PJ12, Gil10, Rab10].

anomaly [AKKY17]. Anonymisation [VV18]. Anonymity [CDFS10, HEC+12, MV16b, MR10, SCGW+14, TFS19, VFV17, WLY17, ZYZ+19, AIB+16, BAG12, GH15, GH16, HLR11, Par12b, PSJ+13, SGJ+18, WW14, YHL16, ZX11]. Anonymity-Based [HEC+12].

anonymity-preserving [AIB+16]. anonymization [XTK10]. anonymized [BDK11, TG12].

anonymising [TMK11]. Anonymous [APMCRI3, CG12a, CZLC12a, CCF17, Cht12, DK12, FHH10b, FHZW18, HLT+15, KP18, LK+17, LSQX19, LZCK14, Mufl6, Par13, RSN14, SYWX19, TAKS10, Wan14, WXL+17, WYML16, ZH14, ZMW16, AIK18, ATIK11, BT18, CCSW11, Chi13a, CGH11, FSGW12, Gop19, GTSS19, HL14, ISG+16, LNK+18b, LWK+19, LHM14, LSQ15, LYL15, LY14, MMYR13, QMC17, VS11, WLS14, XXCY19, YZL+18].


Antoine [AY12], any [Goo12, LP11]. Apache [Lit14]. API [FLW12, PTRV18, QF19]. Append [YNR12b]. Append-Only [YNR12b].

Applicability [Scr18]. Application [AKP12, AK14, BD15, BRT12, BS12, CCL+19, CKLM13, CCKM16, CCW+10, CSTR16, CLCZ10, CHS15, JS18, Kip15, LW11a, LWKP12, MNS11, OO12, SEHK12, SS13, XJW+16, YWK10b, YTS12, ZH15, ZM16, Abe10, BGE+18, BBBP13, BT18, CZ15b, GLIC10, HH15, JZU+19, Jia14b, LGKY10, LWKP14, MSM+18b, NAL17, OTO18, SE18, SGFCRM+18, XHH12, YY11, ZWQ+11, ZAC17]. Application-Level [CCW+10]. Application-Specific [BD15].

Applications [AMVZ12, Ana14, BBD19, BKPW12, Ber18, BKST18, BCG+12b, BJCHA17, BSV12, CZLC12a, CZLC12b, CPS16, CK18, DK15, FSK10, GKM16, GRL12, HvS12, HJ19, HN10, JWJ+17, Nac12, NV10, PJ12, RBS+17, RQD+15, Sasi18, SCPSN10a, SCPSN10b, Sha10, Ter11, TYK+12, WH17, YR11, ZZQ+19, APMCRI3, Ano11a, CFR11, CSZ+11, CQX18, CDA14, Dur15, EBFK13, FES10, Fri10a, GJJ18, GH19, Gil10, KO16, LWZ10, LSQ15, LR15, LBOX12, LTT10, MS13c, MM14b, OSP+19, OK18, PHWM10, PAK15, SWW+17, ZZ15, ZSM18]. Applied [BSS11, KP10, MR10, BTW15, OPHC16, Xie12]. Applying [Bar12, NML19].

Approach [CTC+15, Chi16, DZS+18, HLAZ15, HLW12, KRHR18, KKA15, MKN13, MZ17b, PS14, RP12, SLGZ12, Sia12, SH15, SC12, TCM+17, TLW12, Vle12, VKC15, WYCF14, yWXyZ+18, ZW15, AL15, AT10, BSS11, CLZ+17, CO11, CML16, DZS+12, GGH+16b, Ham19, JKA+18, KL13, LFCGCRP14, MCP15, NC13, PJ18, SE16, SPK17, SA19, Tan18, WMYR16].

Arbitration [Küp15]. Arbitrator [WSA15]. architect [GW14].

Architectural [MD12b, VCK+12, ZWT13].

Architecture [BCE+10, HKL+14, Int19, KS18, KCR11, KCC17, KAK18, LGR14, MCDB12, MJG12, MD11, NdMMW16, NVM+17, RMP10, SWM+10, SLI11, SM18, VDB+16, AL15, Ano13d, BVIB12, LXMW12, MJ13, SSA18, SSPL+13, XHM14, SAAB10].

architecture-independent [BVIB12].

Architectures [AMKA17, BGG+13, BJCHA17, CMO+16, CHS15, DFKC17, MTM18, MKAA17, MKASJ18, RMERM19, SRT12, ST19, FPBG14, HL14, LGP19, MK11, Nov10].

archiving [VBC+15].

Area [GMVV17, HC17, LZCK14, WH17, KP18, LMJC11, LIK+17, Nov10, SGJ+18].

Area-Time [HC17]. Areas [MV12, JY14].

Arguments [BCI+13, ABM+12, LLM+19].

ARIA [PHI12a]. Arithmetic [AIK14, AAB17, BF19, BDL19, Frc10, GH11a, HSA14, IEE13, KHF10, PG12, ZAG19, DTFZ12, MO14].

Array [BL12, MCB12, NKWF14]. Arrays [LB13, TRD11, KM10a]. ARSENAL [SM18]. Art [ABJ13, BLM17, LLK18, Sen17, BDK11].

ARX [KN10, SJLK18, PB19].

ARX-Based [SJLK18]. Asa [Bai12].

ASBUS [YWF18]. ASIACRYPT [LW11a, Abe10]. ASIC [CFZ+10, KMY18, MKAA17]. Asking [DL15].

ASM [Vle12]. ASM-Based [Vle12].

ASP.NET [DR11]. Assessing [CBL13].

assets [WHJ17]. Assignment [LMS16].

Assisted [KCC17, LLKA19, GPR+19, HZWZ18].

Associated [Sar10b]. associative [BS15].

Associativity [ABR12]. Assumption [CCL+19, LZC12a, LZC14, ZG10].

Assumptions [BDH11, CZF12, DN12, GKS17, KM10c, PDNH15, ABW10].

Assurance [BMBS10, Bar15, KMP+11, RNB15, WL11, Ser12]. Assured [Tan15a, WMYR16]. Asymmetric [HG12, XLM+12, XGLM14, XZLW15, ZZQ+19, ZWQ+11, CSS+13, ZGL+18].

asymmetric-histogram [CSS+13].

asymptotic [DTZ12, TD14].

Asymptotically [LPS12]. Attack [Ano15d, BRS17, BMS12, Bro17, Che18, CJP, DSB15, FXP+17, zGXW12, GV14b, GDCC16, HCETPL+12, HL25, JH12, KJP12, LSLW16, LGL+12, LJ17, LCLW17, LJ19, LWKP12, LWFP12, LFK19, MAP+18, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, YTF+18, Ano17a, BD18, B1o15, BNST17, CAM19, CJP, DFD13, FLZ+12, Goo12, GSAV18, KA17, LLY+12a, LC13, LYY1+13, LWKP14, MB11, MNP12, NZL+15, SB17, SXL16, WYL13]. attacker [PLGMCdF18]. Attackers [BL15]. Attacks [ARP12, Ano17e, BGD12, BCL19, BFK16, BKB14, CKHP19, CBRZ19, Che15, CMA14, DZS+18, DGIS12, DHLAW10, DHB16, EWS14, GPT14, HLLG18, HIJ+19, Hay13, HL1C+19, HRS16, JIK+16, JW1+17, KN10, LLL11, LWZ12, LW17, LC17b, MD12b, PDJ+19, PYM+13, PS12, Sas12, SE14, SY15a, SP15a, SH15, SVG16, SGH15, VWC19, WW14, WH12, XNG+14, YL17, YCM+13, ZLQ15, ZHS+19, AATM18, BBP13, BVIB12, BSR+14, CGH17, dCCS1+12, DCT12, DJL+12, DK17, Dra16, EA12, FVT1+10, FIO15, GPP+16, GBNM11, HAK19, HAGT1FR13, KM10a, KPS10, LDC13, LW11, NDN13, OF11, PX13, SGP+17, TK19, TS16a, TY16b, TLL13, VS11, WW14, XWD12]. attempt [Fel13]. attestation [FQZF18].

ATTiny [EGG+12]. Attribute [AAC+16, AHI+12, BFK+10, Boy13, CD16, CDL18, CHH+19, FHR14, GZZ+13, GSW+16, Gli12, GV14b, HSMY12, HBC+19, Her14, KGP12, LW11b, LW11c, LW12, LJLC12, LY+13, LHL+14, LAL+15, LHL15, LW16, OT12,
AP18, PB12, RVH⁺16, Rao17, SSW12, TMY⁺17, WDCL18, WHL15, WHLH16, XMCL13, XWL15, XHH⁺17, ZPM⁺15, ZQQ15, ZZM17, ZHW15, BTK15, CPPT18, FNWL18, HZL18, HZW18, HYS18, HHHK13, JSMG18, LCL⁺15, LFZ⁺17, LFWS15, LYL15, LJW⁺17, LJWY18, LDZW19, Nam19, QRW⁺18, RD17, SL⁺19, WLWG11, XWS17, XZP⁺19, XTZ⁺19, YCT15, ZWM14, ZML17, ZGL⁺18.

**Attribute-Based**

[AAC⁺16, BFK⁺10, Boy13, CD16, CHH⁺19, FHR14, GZZ⁺13, GSW⁺16, GVW15, HSMY12, HBC⁺19, LW11b, LW11c, LW12, LJLC12, LYZ⁺13, LHL⁺14, LAL⁺15, LHL15, LW16, PB12, RVH⁺16, Rao17, SSW12, TMY⁺17, WDCL18, WHL15, XMCL13, XWL15, XHH⁺17, ZPM⁺15, ZQQ15, ZZM17, AMLS⁺12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HHHK13, JSMG18, LCL⁺15, LFZ⁺17, LFWS15, LYL15, LJW⁺17, LJWY18, LDZW19, Nam19, QRW⁺18, RD17, WLWG11, XWS17, XZP⁺19, XTZ⁺19, YCT15, ZML17].

**Attributes**

[CG12a, Yon11, LCL⁺17a].

**Attribution**

[AIF⁺19, XHC⁺12, FNP⁺15].

**Auction**

[Con10, JNWS19, HJM⁺11].

**Auctions**

[MR14c, QS18].

**Audience**

[DET17].

**Audio**

[Bar18, DA12, FM15, GCK12, HGT15, KD12a, KD12b, SL12b, NXH⁺17, QF19, TC10, gWPNyY⁺14, XNG⁺14, XNRG15, XNP⁺18, ZS12, LSQ11a, SKE14, yWPNyL11, YWYZ12, YQH12].

**Audit**

[YNR12b].

**Auditing**

[LMD16, TCM⁺17, YYS⁺16, YXA⁺16].

**Augmenting**

[AV18].

**August**

[AB10a, JY14, MV12, Rab10].

**Aura**

[HFCR13].

**Austin**

[EE13].

**AuthCropper**

[KLK⁺19].

**Authentic**

[HLT⁺15, SZMK13].

**Authenticate**

[HM12].

**Authenticated**

[Alo12, BSBB19, BCO13, BDM116, CLL16, CLY14, CCS14, CRE⁺12, DS11, EAA12, ESS12, FVS17, FFL12, GT11, GL12, GZ12, HC12, HL10a, HCL⁺14, HEC⁺12, KMY18, KKL⁺19, LHKR10, LY16, LH11c, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHHK14, MSU13, PTT16, Sar10b, SMI11b, Tan11, TW14, XLM⁺12, XHC⁺12, XGLM14, XLW15, YS12, YLSZ19, YLW13, YRT⁺16, Yon12, ZP⁺16, ZXH16, AIB⁺16, ABR15, CTL13, FA14b, FIO15, GPN⁺12, GLM⁺11, HPC12, HWB10, HWB12, HL11, HPY10, ISC⁺16, JKA⁺18, KMTG12, LWS10, LHH11, LML⁺13, NCL13, Nos11, Nos14, PTT15, PJ18, SMBA10, TCS14, TSo13, TKHK14, WZM12a, WZM12b, WTT12, WXWC14, XL13, XWZ⁺18, YC12, YZZ⁺14, YZL⁺18, ZT16, ZGL⁺18, ZXWA18, ZG10, ZZZ15].

**Authenticating**

[BS12, CHX13, GRL12, OKG⁺12, RGP12, WY12, ZCMS15, Bel18b, Cer18, LFGCGCRP14, PGL10, RR16, ZLDD14].

**Authentication**

[AV18, AA19, ASO14, AAZ⁺16, ACAT⁺15, AUMT16, ABB19a, BL12, BCE⁺12, BCM12, BSSV12, Bel18a, BKST18, BCD⁺12, Bis17, BF11, Boy16, BKJP12, BS12, CGCGPDGM12, CTC⁺15, CC14, CSH⁺18, CCW⁺10, CCF17, CJ13, CD12, CJP12, CLH13, DL15, DCM18, DBPS12, DPKW12, DP12, FLH13, FR16, FMTR12, FD11, GHS14, Gl12, GID12, GMD19, GM14, GU13, GMVV17, GCK12, HZC⁺12, HvS12, HLLC11, Har13, Hay13, HBC13, HM10, HCPLSB12, HCCETPL⁺12, HKL⁺12, HFCR13, HXC⁺11, HLLC11, HRK18, IGR⁺16, JN12, JCM12, Jia17, JLX⁺19, JAE10, KP12, KS18, KLN15, KRM⁺10, KSD⁺17, KPC⁺11, KLY⁺12, KTA12, KGP12, Kim15, KPKS12, KLM⁺12, KO16, KH10, LLC11, LH12, LLG15, LCL15, LNZ⁺13, LZC14, LNY15, LLZ⁺12, MWZ12, MEFO12, MKH⁺12, MBC15, MKRT17, MRS⁺17, May15, MLBL12, Mor12, MSK17, MPM⁺17, NR11, NR12].

**Authentication**

[NSBM17, NLIJ12, NLY15, OdH12, O012, O12, O12].
OŚ12, PSSK19, PCDG14, PPRT12, PDT12, PWVT12, RS11, RWLL14, RSN14, SGG18, Saa12a, SBS+12, Sar12, SGC16, Sch15b, SKV12, ST14, SM12, SD12, Shi11, SGC14, SSA13, SPK17, SRRM18, SC12, SCMS18, SZDL14, SLS12, SAA12b, SRK+17, TGC16, TWNC18, TYK+12, TM12, Ve10, WGMdZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WAK+19, WT10b, Xio12, YTP17, ZBR11, ZHW+16, ZWZ17, ZLDD12, ZLDC15, AMN18, AaBT16, ACC+13, AN15, ACM12, BOP14, BS13a, BGE+18, BDM18, BDM+19, BLAN+16, BAL10, BMM12, BHoS15, BT18, BTW15, BM11, CLM+12, CML+18, CLP+13b, CAM19, CTL12, CJXX19, CSD18, CH10, CCESS11, CHS11].

authentication

[CLHJ13, CZ15a, Chi13a, CJP15, Cho14, CL11, CRS13, CDWM12, DCAT12, DSCS12, DRN16, DLK+16, DMV15, DLN13, DZS+12, DMT12, uHAN+18, EA12, ED19, EA11, FPBG14, FHH10a, FLL+14, FPX12, Far14, FA14a, FHZW18, FQZF18, FMA+18, FHM+10, FZZ+12, GJ13, GMSW14, GHD19, GEARR11, GPLZ13, GI15, GH16, GAI+18, Gop19, GCSAdP11, GM11, GLB+18, GBC19, GTSS19, HU15, HSH11, Ham12, Ham19, HW19, HHBS18, HDPC13, HZC+14, HK17, HZW17, HL12, HL14, HCM11, HLC16, HPL+19, HCC10, HS11, IMB17, IAA+19, IC17, IG11, IB11, IOV+18, Jac16, JNUU17, JKAU19, Jia16, JKL+16, JMW+16, JAS+11, JXLZ15, KPP16, Kem11, KKG14, KSB+17, KVvOS15, LLLS13, LLS+16, LC17, LH11b, LT13, LH10c, LNM+11, LMJC11, LXMW12, LNNH13, LNLK13, LXJ14, LK+17, LC17, LNK+18a, LWK+18, LNK+18b, LWK+19, LHM14].

authentication

[LH13, LSQ15, LHH+18, Lit14, LWWL11, LTC+15a, LYL15, LBR12, LTT10, MM12, MMLN15, MCN+18, MDHM18, MV11, MMP19, MA17, MMS17c, MCRB19, MK12a, NDS1A7, NR17, NACL12, NCCG13, NM18, NLYZ12, NML19, NB13, NXS10, NMX15, OSP+19, OF11, OCGD11, OYHSB14, PYH+18, PYP10, Par12b, PLGMCdF18, PZBF18, PA10, PAK15, PRN+19, QMC17, QMW17, QLZ19, RR17, SSA18, SCFB15, SPLHCB14, SB17, SGGCR+16, Sar10a, SK18, SSNS15, SYV19, SGJ+18, sZZ15, SCKH10, SYWX19, SNG+17, SCR19, SA15, SYW17, SSS11, SKEG14, SA19, SMS+16, SHBC19, Tan12b, Tan15b, Tan18, TODQ18, TZN16, TG17, TLL12, Wan13, WW14, WLZ+16, WCFW18, Wat14a, Wat15, WDKV19, WT10a, WKH11, WXK+17, XHI19, XWDN12, XHCH14, XXY19, XHMD13, XHM14, YI17, YHL16, YHHS16, YWK+10a, YSL+10, YMM13, YN19, YD17, ZYL+10, ZQZ10, ZCLL14].

authentication

[ZHH+17, ZX11, ZLY+19, ZLZ+18, OHJ10].

authentication-chaining

[EA11].

authenticators

[SYY+17].

authenticity

[ADF12, VBC+15].

Authority

[LNX15, XZ11, ZQ15, JB11, SLL+19, ZZ12].

Authorization

[CS14, LMGC17, MMP+17, YKK18, AL15, DFJ+17, FHM+10, JAE10, JAS+11].

Authorized

[HTC+15, LLSW16, WZCH19].

authorizing

[Bel18b].

Authorship

[AI+19, BTW15, BAG12, LC17].

Autoblocking

[LLLH18, YH16].

Automata

[CCD15, Gas13, dRSdlVC12, HBBRNM+16, SS11, WOLS12].

automata-based

[SS11].

Automated

[CC12, CCK16, DR16, GLLSN12, JGP+18, LGM+16, Ste15a, Tom16, YSS14, BJR+14, GMMJ11, KKK+16].

Automatic

[MMP19, WW12, HL19].

Automation

[BGK12, DZS+18, EEE11a, KPP16].

Automotive

[HK18, LMS16, MMP+17].
Based-Encryption [ZHW15].


Century [Wes16], Cerf [Cer15, Cer18], Certificate [GWWC15, HP12, LTH+15, WMS+12, YLZ+16, BJR+14, GLL+18, Lan13, LL16a, MFB+13, NPH+14, JB11].

Certificate-Based [GWWC15, HP12, LTH+15, WMS+12, YLZ+16, GLL+18, LL16a]. Certificateless [CT18, GWWC15, IL15, LZCK14, RSD19, SZS14, TCL15, WMS+12, YT11a, YT11b, ZSY19, HPC12, JXL15, LL16b, SGJ+18, ZQWZ10, ZY17b]. Certificates [Muf16, SC12, GIJ+12, HREJ14].

CertShim [NPH+14]. chaos [KHMB13]. Chain [EAA+16, FVK17, KPW13, QZL+16a, QZL+16b, YFT17, YFT18, CR12, Par18, CL16, SJW+17]. chaining [EA11]. Chains [JSK+17, HLYS14, JCHS16].


Chaotic [BCGH11, IAD10, LFX+18, Ye10, Bro19, GCH15, ISC+16, KILW+16, LWK+18, LW10, LZXK19, NES+14, WZG+12, ZT+14].

Chapman [Full0]. Character [SS12b]. Characteristic [BGJT14, SR10, ZWZ17, BGJT13, Jou13].

Characteristics [SSP19, TCMLN19, BEB+18]. Characterization [ALR13, BS13b, DPCM16, YZLC12, DDD14, PLGMCdf18].


Chosen-Ciphertext [RS10, FSGW12, LCT+14, GH12, LZC14].

Church [ABJ13]. CHURNs [RNB15]. Cipher [BW16, BFM16, BCG+12b, CMSL15, CGCS12, DM18, DG12, DWWZ12, EHKSS19, Fis15, FXP+17, GLLSN12, GCS+13, HZ11, Hey17, IOM12, JKP12, KR11, KWS+12, LPS12, LW12, LJ17, LJ19, LWK12, LWPF12, MRTV12, MHC12, MS12b, OGG+15, PH12a, PR12, WSS12, WHN+12, YCL17, ZAG19, AMS+10, BNY14, CR12, FVK17, HKT11, Holt12, Jeo13, KDH15, Lew10, LC13, LYH14, LWK14,
MNP12, PL16, Ree15, RS14, Sar11, WYL14, WWBC14, ZSW+18a, LGL+12]. **Ciphers** [ABS+12, BMS12, BSS+13, BM18, BKL12, Bru12, CWP12, DGFH18, DGIS12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNL12, Has16, Hey17, IS12, KE19, KPC+16, Kla10, LCLW17, LGGL12, LJ16, MD12b, NN12, PDJ+19, Pud12, Sas12, SEHK12, SJK18, Vua10, WH18, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KMI10, LGP19, LWK11, MCL+19, MRT10, MHV15, MHY+18, QCGG13, SKK10, TQL+14, WB12]. **Ciphertext** [DSLB18, JEA16, AHL16, EGG12, SKK10, TQL]. **Classifiers** [KGG16, LCM+17]. **Cloud** [LW20, TSL11, SN16a, WB12]. **CLEFIA** [LWZ12, TSL11]. **CLEFIA-type** [WB12]. **Ciphertext** [ASM12, CTC+15, FD11, RAZS15, Vle12, FA14a, FA14b, JX+19, hSZZ15, WT10a]. **Claimant** [FA14b, hSZZ15]. **Clients** [Chi16, LWP19, LH13]. **Ciphertext** [ASM12]. **Ciphertext-Policy** [FA14b, hSZZ15]. **Ciphertext-only** [KA17]. **Ciphertext-Policy** [CHH+19, KA17]. **Ciphertext-Policy** [BDPS12, CWWL12, CHH+19, zGXW12, HIW12, JMG+16, JSMG18, KA17, LZC12a, LML12, MH14, PDHN15, PPS12b, Rao17, RZ12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWLJ16, YMI9, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, KTT12, LCT+14, LFWS15, LZW19, QRW+18, RD17, SGM16, WLFX17, XWS17, LAL+15, LHL15]. **Circuit** [KAR12, MTL11, XWS17, XWLJ16, LAU12, MS13a]. **Circuit** [SC10]. **Circuit** [CHH+19, KA17]. **Circuit** [AIK14, AS17, BR14, GGH+16a, GH11a, GVV15, MBF18, SS10b, SS12a]. **Circumventing** [BAG12]. **CISSP** [STC11]. **Cities** [SSSA18]. **Citizen** [ANO16d]. **City** [ANO17d, GAI+18, JZU+19, LNK+18a]. **Claimant** [YI17]. **Claims** [SKGY14]. **Class** [BCG12a, SY15a, XXYXY11, BJ16, Goo12, KK10]. **Classes** [AC216]. **Classical** [DSDL18, JEA+15, MSU13, SSU12, CR12, RK11]. **Classification** [CHH+19, HPC10, HS18, KAHKB17, SGP+12, ZLW+17, LHL+18]. **Classifiers** [KGG16, LCM+17]. **Classifiers** [Pow14]. **Cloud** [Hol12]. **CLEFIA** [LWZ12, TSL11, SN16a, WB12]. **CLEFIA-type** [WB12]. **Client** [ASM12, CTC+15, FD11, RAZS15, Vle12, FA14a, FA14b, JX+19, hSZZ15, WT10a]. **Client** [ASM12]. **Client-Centric** [FA14b, hSZZ15]. **Cloud** [CWH17]. **Cloud** [VA16]. **Cloud** [VTY18]. **Cloud** [WAL18]. **Cloud** [AJA16, BCQ+13, BT15, BCK17, CWL+14, CWL16, CDFZ16, CCT+14, CLW16, DK16a, DXA14, FCM14, FYY15, Her19, JLS12, JWN19, KMSM15, KSA18, KKA15, Kip15, LA15, LLP19, LYZ+13, LGR14, LCL+15, LNX15, MLO17, MGJ19, PSM17, Pe12, PBC+17, RSGG15, SGG18, SGJ+18, SKH17, SRA17, TV15, Vle12, WLFX17, WWW17, XNK15, XWSW16, XMLC13, XWLJ16, XJW+16, YDY+16, YHL16, YX18+16, YM+17, ZZQ+19, ZDL12, ZLDC15, ZVG16, ZLW+17, ZZL+18, AnBT16, AKKY17, AZPC14, AS014, AAZ+16, AKK+17, ADH17, ALL+18, Bel18b, BS19B19, BG14, BK12b, CFVP16, CSD18, CLH+16, CZ15b, CDL18, FH13, FNWL18, GLB+18, GZ18+18, HMS13, HZW18, HYS18, IM17, JEO13, KKA14, KKM+13, KKM+14, KSB+17, LHX+14, LZY+16, LAL+15, LW13a, LYL15, LHL15, LCY+16, LZC17, MLM16, NRI17, Nam19, NB13, PPA18, PP11, PWS19, RAO17, RR16, SSL+19, SY17+17, SAR18b, SLM10, SKB+17]. **Cloud** [SWW+16, SWW+17, SA19, TLM13, WIWG11, WL12, WSC14, WMX+17, WLS14, WS19, WC18, WL19, XXX15, XWD18, XTZ+19, XYML19, YSY16, YZC17, YHH18, YQOL17, YWT+12, ZYC+17, ZVH14, ZWD+16, ZZC17, ZWS+18, ZFH+18, ZLY+19, ZHT16]. **Cloud-aided** [SGJ+18, WLF17].
Cloud-Based [KS18, SRAA17, ASO14, BK12b, WCCH18].
Cloud-Manager-Based [KKA15].
Clouds [BCQ+13, HLC+18, RSN14, HFT16, IC17, JKL+16, LFWS15, LL16a, Wu17, YNX+16].
Clustered [DS11, KS18]. Clustering [KRDH13, VSV15]. CMAC [SKK10].
coal [KO16]. cocktail [OHJ10]. Code [AD12, Bud16, CCL+13, Cop10a, Fox13, HG12, KSSY12, Mun17, PYM+13, SS13, Sen17, Sti15, War11, ABBD13, Ant14, Bha16, Bri11, CLLU11, GIJ+12, GAB19, MCP15, McG11, McK12, Moe14, OF11, PTRV18, PA10, Wes15].
Code-Based [HG12, SS13, Sen17, GAB19, MCP15]. code-breaking [Ant14, Bud16].
Codebreaker [Car11]. codebreakers [Ano11c, Bud16, Maf16, McK12, Smi11a].
Codebreaking [Bai12, RS18, Cop10b, McK10, McK11]. Coded [She14].
Codes [Ano19b, BBC+13, Bay10, BKST18, DBPS12, DPW18, FMNV18, GMNS15, Grit15, HC17, KW14, MBR15, OTD10, PWBJ17, SEY14, ST14, TLW12, WGF16, WSS12, Xie12, YTP11, Yek10, ATI+10, Bul10a, CZ15a, Chi13a, Fag17, Hea15, LTT10, MG15, OSJ11, Tan15b, YSIL14, Ayu12, Low12].
Code-development [DF16]. Coding [Che11, CWL16, CJ13, CG14a, DG17, Hes12, LCLL15, Per13, AZF+12, Bul10b, CXX19, DTZZ12, JZS+10, KM11, LLP+18, NDR13, OF11, Tan15b, YTM+14, Kim15].
Collaboration [CRE+12, PCPK14, HYS18]. Collaboration-Preserving [CRE+12]. collaborative [LT14b, HB13]. collect [Sch15c]. Collision [BK12a, ZL12, AKY13, SKP15, SBK+17].
Collusions [GWV12]. Color [BCPV11, DD13, FR16, HD19, LW10, MR16, RMG18, yWxyZ+18, YWNW15, Bro19, MSM+18b, SNM14, yWpWypN13, WZH+12, YSC16].
colors [MMLN15]. Colossal [Hai17].
Colossal [Cop10a, Cop10b, Wil18]. Coloured [PSI14]. Column [FSI15].
combating [FTV+10]. combination [Wat14a]. combinational [MS13a].
Combinatorial [ZAC17]. Combined [PP16b, PDJ+19]. Combining [Chi13a, CDF+10]. Coming [SOG15].
Comment [LCLL15]. Comments [IC17, Kim15, hSZZ15, Tan11, TLC15, XWS17]. Commerce [Bla16, HsV12, Orm16, Ano11a].
Commitments [Pas13a, CSZ+11, LP11]. Committee [Bla16]. commodity [KKJ+16].
Common [CN12, DHB16, ESR14]. Communication [BPSD17, CCM17, CCW+10, FMS12b, Gas13, GPVCdRO12, KW14, Low12, OKG+12, Wan13, ZC13, ZHW+16, AASSAA18, ADG16, BBE+18, DLK+16, HCC11, HL15, HP10, KRM+10, KTUI6, LT13, LyWS10, MCN+18, QMC17, RK11, SSAF11, SSP+13, Tso13, WLZ+16, YKGG13, Zha13, vDKS11]. communication-efficient [Tso13, Zhu13].
Communication-resource-aware [Wan13]. Communications [FMC19, JTZ+16, KSD+17, KYEV+18].
OO12, RSD19, SMS14, AMN18, Edw17, FHH10a, Han12, LGFCCRP14, LLZ+16, MHY+18, RS15, WDZL13]. **Community** [BPS16]. **Commutative** [CLHC12, SLGZ12]. **Commutativity** [ABR12]. **Commuting** [Fuc11, AKG13]. **Compact** [CFOR12, CKLM13, EGG+12, LYX+19, LSQX19, MAS16, SJLK18, Seo18, TV19, VSR12, YM19, ZMW16]. **compacting** [CPPT18]. **Companion** [KR11]. **Comparable** [XHX+17]. **Comparative** [DDR+16, MHV15, BKR19, NR11]. **Comparison** [CGCS12, DWB12, HPC10, KU12, KA18, MZLS18, ST14, HM10, LCM+17]. **comparisons** [Mid10]. **compartmented** [EZ15]. **Compensated** [GKSB17]. **Compensation** [JSZS12]. **Competition** [jCPB+12]. **competitive** [MD15]. **Compilation** [CHS15]. **compiler** [LWS10]. **Compiling** [CR10]. **complementary** [MMLN15]. **Complete** [Ash14, BS14, FLH13, GHKL11]. **completely** [Win17]. **Completeness** [FKS+13]. **Completion** [MHW+19]. **Complex** [pNyWyY+14, VGA15, BW13, LZKX19]. **Complexity** [BBD19, BIKK14, BW12, DP12, FS15, Gas13, HHS+15, AAT16, DJL+12, Jou13, KGO10, LWW+10, SDM14]. **Compliance** [SOF12, Tay19]. **compliant** [BP10, Lan11]. **Component** [BKLS18, MV16a]. **components** [RITF+11]. **Composable** [DN12, KMO14]. **Composing** [TW14]. **Composite** [Dun12a, ZL19, BBDL+17, NDSA17]. **Composition** [LJS+14, NRZQ15, Ana14, AGH+17]. **compound** [BJ16, KPS10, jT12b]. **Comprehensive** [GSFT16, YFT17, ZBP18, Bul10a, KAS15]. **compress** [LC13]. **Compressed** [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16]. **Compressed-Domain** [WLZL12]. **Compressibility** [HN10]. **Compression** [CNT12, DA12, LD13, MAL10, PMZ13, PP10b, TCN+17, WHZ12, ZSP+19, Ara13, CMM17, DTZZ12, LK14, Li10, LPZJ15, PP11, QZ14, RSMA19, SI12]. **compression-based** [SI12]. **Compression/Decompression** [PP10b]. **Compressive** [CCZC13]. **Compromise** [YNR12b, GBNM11, PX13]. **Compromised** [DSSDW14, ZYL+10]. **Compromising** [BC14, BM18]. **Compulsory** [QRW+18]. **Comput** [HYS18]. **Computability** [Gas13]. **Computable** [LGH+17, FWS13]. **Computation** [ARH14, Ash14, Bee17, BDOZ11, Fri10b, GST12, GHW12, GHLK11, HP14, HC17, HXZ+18, IEE11a, Jin10, KW14, KMO14, LHM+15, LQD+16, MMP14, Mal13, NSMS14, PST13, SZHY19, SVCV15, SZQ+17, TM18, Wat10, ABDP15, AB10b, BHH19, LDDM12, PHGR16, TG12, vDKS11]. **Computational** [BBD19, BCO13, GKS17, RD17, TBCB15, HRS13, SDM14]. **Computations** [ARM15, CK18, KHPP16, Nac16, ADMM16, BK12b, LR15, SSAF11, TLMM13]. **Compute** [Vai12]. **Computer** [BGK12, BCGK12, BGB12, BD19, Bul10b, DF16, Gas13, IEE10, IEE11b, IEE13, LL15, Orn16, PWB17, Ter11, Vua10, ABB13, DK12, FGPG14, PHWM10, Sta11b]. **Computer-Aided** [BGK12, BCGK12, BGB12, ADMM16]. **Computers** [Mos18, Cop10b, LCKBJ12, Mac12, MvO11, PHWM10]. **Computing** [ACM10, ACM11, AJA16, Ano17e, BCG+12b, BTK15, Cer14, CGB+10, DXA14, EAA12, FES10, Gen10, JWN19, KSM15, KP17, LCK11, LT14a, LYZ+13, LLC+15, LLGJ16, LNX15, MLO17, OS16, PAF18, Pet12, RS18, SJWH+17, SLM10, Vai11, Vle12, XMLC13, XWL16, YE12, YHL16, ZLDC15, AaBT16, AAZ+16, And13, CZ15b, CST16, DKL+16, DWZ12, Gop19, HSM13,
FMNV14, GMDR19, MSKRJ17, PYP10, SCFB15, Sch15b, SRT12, Yam12, ZY17a, ZYM18, ZYH19, ARL13, BTW15, CXX19, CRS13, PLGMCdF18, SCR19.

Continuous-Tone [Yam12], contract [MMP19, Men13b]. contrast [DDD14, GLW13, LWL10a, MM14a].

Contributory [WQZ16]. Control [ATS15, BFK10, DLZ16b, HBC19, HHS15, HLC18, LGM16, LGLK17, MM17, MK12b, NA10b, PV17, QZL16a, RSN14, SGC14, TBCB15, XMLC13, XHZ19, YTH17, ARL13, ACH10, AMH10, CLH16, CO11, Cra11, FG19, FNLW18, FS18, GHD19, HPJ19, JAS11, LCL17a, LCL15, LHH18, MDHM18, NZM10, QCX18, RR17, Sch15c, SA15, Tan12b, Wan18, XHH12, XYML19, YYJ19, ZML17, ZWH14, ZWS18, ZPH18, ZZL18].

Controllable [FH13, ZLDC15, ZHT16]. Controlled [FMTR12, WP17, Har16, SM10c, XLC19].


Conversations [WBC10]. Converse [KPKS12]. Conversion [BJ10b].

Convertible [CLL16, LH11c, HL11, LHH11, XWX14].

Convolution [DWZ18, HW19].

convolutional [KMG17, MG15]. Cookie [FVJ19]. cookies [DCAT12]. Cooperative [LLZ12, SJWH17, ZLDC15, WQZ13].

Coordinate [YKK18]. Coppersmith [Dra16]. coprocessor [ABC12, BGG13, IBM13b].

coprocessors [GCVR17]. Copy [YT12, MHT13]. Copyright [SJ12, GJ13].

Core [LB13, YWF18, YS15, RS17, HLYS14]. Cores [MGG19]. cornerstone [Tan17b].

Correct [PST13, Lan11]. CorrectDB [BS13a]. correcting [AT10, LTT10, MCP15]. Correction [LSC15, yWXyZ18, Chi13a, Sun16].

Correctness [YGS17, WS13]. Correlated [RS10, Jia16, ZPZ16]. Correlation [BW12, FAA18, LD13, SDM12, WWBC14, XHH12, YCL17]. Correlations [Sar14]. Correspondence [SY14].

corresponding [DWZ12]. Corrigendum [HYS18, WZM12a]. Corrupted [Fyo19].


Counter [ARP12, KMJ18, MKASJ18, Fay16]. Counterexample [KPW13]. Counterfeit [YFT17]. Counterfeiting [Ano16c].


CovertBand [NTKG17]. Cozzens [Led16, Sch15a]. CP [TY16a, YMC17].

CP-ABE [YM17]. CPM [PYM13].

CPS [FQZF18]. CPU [ZBP18]. Crack [Fox13]. cracked [Ano13b, MG11, MK12, Moo14].


Credence [YLS19, JMW16, KKM13, XMHD13].


Crisis [ODH12]. Criteria [DY18, ZKA17].

Criteria-Based [DY18]. Crittografia [Sac14]. CRM [LHM15]. Cropper [KL19].

Cross
[AKK⁺17, CLY14, DSB15, LHM⁺15, MV16a, YGFL15, ZYL⁺18, ZXH16, ZTSR12, SS17, der10]. Cross-Border [ZTSR12].


Crowd [MJS⁺19]. Crypsis [GSC17]. Crypt [HHAW19]. Cryptanalysis [BW12, Bor10, CWP12, CGCS12, DG12, DJG⁺15, Far14, GST13, Gor10, Hin10, IOM12, Jeo13, JL18, Kha10, KN10, KWS⁺12, LH10b, LNX⁺11, LJF16, LFX⁺18, LSQX19, LJ16, MWZ12, MV19, NXB13, OTD10, PSOMPL13, SPLHCB14, SM10a, SM10b, TY16a, TG17, Vua10, Wag10, WWYZ11, WYYY11, WSSO12, WWY14, XQL11, YCL17, YMWS11, AP11, BMB16, BKR11, Bul10a, Bul10b, Con12, Eis10, FVK17, Her10, KDH13, LLKK10, LFW⁺16, Nov10, RITF⁺11, SDM10, SDM14, Sun11, SvT10, Tam15, TSSL11, WYL14, WWBC14, AY12].


Cryptographical [KU12]. Cryptographically [ADD10, BCGH11, BDL12, BKL18, MC11, NDG⁺17, PLSvdLE10, SVC15, CBL10, GCH15, HJM⁺11, SA14]. Cryptography [ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, Ano19a, Ano19b, App14, AAB17, ACM⁺17, ARM15, Bar12, BKG12, Bar15, BBCL19, BRT12, BCGN16, Bon12, BF19, BKKV10, BJ10b, Buc10, BLM17, BLM18, BCF⁺14, CNR14, CT18, CJFH14, Cas10, CGMO14, Che17, CST⁺17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dun12, DK15, DX14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, FHLD19, Fel10, FSK10, Fid18, FB12, Fre10, GO17, GFBF12, G’13, GPT12, GLW12, Ham17, He12, HG12, HKR⁺18, JS18, JT12a, KM10c, KP10, KAK18, LSL12a, Lin17, LWL10b, LQVY12, LMHH14, LGH⁺17, LWHS17, LPO⁺17, MO12, MS10, Mun12, Min13a, MR14c, Mic10b, MST18, MV12, MMB17, NNA10, NDR⁺19, NS12, Orm16, PP10a, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15].
Cryptography [Sch16, Sch18, Sen10, SS13, Sen17, SK12b, Sec18, She17, SA16a, Sim15a, SGS14, Sma16, Sta11a, Sta15a, VS16, WWL⁺14, WY12, Wes16, Yam12, Yan11, YTS12, YL17, YYY19, ZZCJ14, ZAC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBBD13, Ano11a, ABW10, ACK⁺10, BOB13, BB14, Ber14, BL14, BL17, BAB⁺13, Blö12, BSR⁺14, BSW12, BBB16b, CFR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSLY14, DDI14, DA18, Dav11, DDI3, DGMT19, Dur15, Far14, GCVR17, Har15, HH15, HZWW17, Hod19, Hof16, IM14, JLT⁺12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Li11d, LY14, MCN⁺18, MS13b, MD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSAF11].

Cryptography [Sta11b, Sti11, Svo14, UK18, VN17, WHJ17, WYK12, YL11a, YSC16, YXA⁺18, YDH⁺15, YR11, YN19, ZXW⁺18, vDKS11, Che11, LZJX10, Nac12, Cou12, Ful10, Gas13, Low12, Mei10, Mur10, Ter11].

cryptography-based [BOB13].

Cryptography-Related [Cil11]. Cryptol [Lau12]. Cryptology [BC11, Bro11, Dun12b, I1w11a, PWBJ17, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPP14, Gil10, GG10, Kia11, L1H10a, MZ17a, Pall16, Pie10, Rab10, HWG10, L1TW11, Kob10].

Cryptography [Cil11]. Cryptoprocessor [EHKSS19, GV14b, SWM⁺10].

Cryptosystem [CCT⁺14, LH10b, S1ZYH19, SW1⁺10, BS15, Ch13a, Gal13, GV14a, GLB⁺18, IB11, MM13, MG15, NZ10, SwT10, yYQ1WqZ13, YY11].

Cryptosystems [ADI11, CLND19, OTD10, P1SM17, ZSP⁺19, BNST17, FWS13, SA16b].

CS [LJ19]. Csec [AD12]. CT [Dun12b, Kia11, Pie10]. CT-RSA [Dun12b, Kia11, Pie10]. Cubic [HIJ⁺19, MS12b]. Cubic [RW12, VM14].

Cuckoo [BHKN13]. CUDA [DLV16].

cultural [Mid10]. Culture [Bla12, SR14].

Currencies [TS16b]. Current [DP17, GCK12, FPBG14].

curvature-feature [GJ13]. Curve [AD11, ARM15, BJ10b, FHL19, GPT12, LGH⁺17, LWHS17, PPH12, SG15, ANM18, BL14, BL17, BB16b, Cho14, Far14, FWS13, IB11, KK10, Kre13, MCN⁺18, MS13b, NZ10, SK15, WHJ17, JL16].

Curves [AK14, B1W12a, DW12, LL11, LT14a, MST18, PWBJ17, She17, YTS12, BL17, BP18].

Customization [OdH12].

Cyber [LJS⁺14, vdWEG18, GHD19, HZWW18, KSA16, QMC17].

Cyber-Espionage [LJS⁺14].

cyber-physical [GHD19, HZWW18, QMC17].

Cyber-security [vdWEG18]. Cybernetica [Ano17c].

Cybersecurity [DF16, Hel17, Lan17, LRW14, Mos18, Sch19, SPG⁺19].

Cycle [HG12, KU12, MK13].

Cycle-Based [MK13].

Cycles [WBA17, CLCZ10].

Cyclic [Che18, OTD10].

D [AP10, Bro19, CG12b, DBPS12, DWW12, EAA⁺16, GH1D12, KWS⁺12, L1J17, L1J15, MC12B12, MKH⁺12, P1GL110, RS16, S1GRG17, W1SO12, WY12, t1WmC12, Y114, YP1117].

D-Based [WSO12]. D-like [LJ15].

D-PUF [SRK⁺17].

D2D [Gop19].

D2D-Aided [Gop19].

Dana [Ano10].

Dandelion [VF17].

Dangerous [HLW12, GL17].

Dao [FMS12a].

Dao-Fa [FMS12a].

Daoism [FMS12a].

Darel [Xie12].

Darmstadt [FBM12, Sen10].

DASH [KCC17].

Data [ARW19, Ano13c, ADF12, Bar12, BJ1L16, BCD⁺12, BJ1L12, BW12, BKL18, CWL⁺14, CMLS15, CCW⁺10, CSV15, CCT⁺14, CLW16, CHH⁺19, DDS12, Dan12, DR12, DK16a, DMS⁺16, DA12, DCA18, DLZ⁺16b,
[Ano17e, Sch13]. **Defending**
[LWCJ14, YFT18]. **Defense**
[MPA+18, PSJ+13]. **Defenses** [AN17].
**Defensive** [PH10]. **Defined** [KYE18].
**definition** [LWL10a, WSC14, YKC+12].
**Definitions** [BBD19, GLW12, Mau12, CGKO11, KM14, KGO10, XWXC14].
**Degeneracy** [WH18]. **degradation**
[MS+17a]. **Degree** [KA18]. **degrees**
[MZ17a]. **Delay** [CCKM16, GMNS15, LFX+18, LBR12, JLT+12, WX13, MCL+19].
**Delegatable** [WZ11, XLC+19]. **Delegated**
[MZHY15, TMC15]. **Delegation** [FMTR12, SSW12, XWLJ16, YZ12, YAM+15, JSMG18, NAL17, XWS17, XZP+19, ZWM14].
**Deletion** [DNS+16, MGJ19, Real16]. **Delfs**
[Mur10]. **Delivery** [PSS+13, SSPC12].
**demand** [KKJ+16]. **Demodulation**
[KOP12]. **demonstrating** [HAL+16].
**demaicking** [HLC16]. **Demiability**
[TCS14]. **Deniable** [DF11, zGZW12, HLLC11, HS11, Jia14h, JXLZ15, LXX14].
**Denial** [BKBK14]. **Dense** [BFM12].
**Density** [LC15, LSQ11b]. **density-based**
[LSQ11b]. **Dependable** [BCQ+13].
**Dependency** [SGP+12]. **dependent**
[GM16, PKA15]. **deployed**
[MFH13, Ry10]. **deployment** [WXK+17].
**DepSky** [BCQ+13]. **Depth**
[GH11a, R16, SS10b, SS12a]. **Depth**-
[GH11a, SS10b, SS12a]. **Depth-Based**
[RS16]. **Derivation**
[LBR12, Cha13a, Lau12]. **Derivative**
[LSQ11a]. **Derivative-based** [LSQ11a].
**derived** [ZMM+10]. **DES-like** [CGCS12].
**Description** [WH18, PLSG11]. **Design**
[AMN18, Abe12, ARH+18b, AIB+16, ADD10, AUMT16, Bel18a, BKL+13, DZS+18, DHB16, DR11, FSK10, HSA14, JWC+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QLL17, RYF+13, Sch13, SAA10, SZDL14, TAK+13, VKPI17, WKB16, WDV19, ZWH16, BBPD16, CZ14, DRN16, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, SVGE14, ZYC+17]. **Designated**
[WH17, HYWS11, RPS10, SY15b].
**Designated-verifier** [WH17].
**Designation** [Che15, SLLQ18]. **designed**
[Goo12]. **Designer** [KMY18]. **Designing**
[CDK+10, DZS+18, FLW12, MRT10, PSD15, SR10]. **Designs** [BGK12, PCY+17, KDH15].
**desynchronisation** [LDC13]. **Detailed**
[DLV16, ZPXX17]. **Detect**
[JWJ+17, NCK15, WOLP15, Lan11].
**detectability** [LRW17]. **Detectable**
[Ess17]. **Detecting**
[BKBK14, Ess17, GAS+16, HLW12, KW14, SH15, YSC+15, LWW11]. **Detection**
[AMKA17, ATS15, ARWK19, CBO+18, DSB15, DF11, GZH17, HDWH12, KU14, LGL+12, LC15, MKRM10, MKAA17, MKASJ18, NDC+13, NSMS14, SAJJ16, SBV14, SXH+19, SP15a, SRAA17, SGS14, TM18, YFT17, AKKY17, AOT13, BM13, HB13, JCL13, KLC+10, LDC13, Maz13, MHT+13, WYL13, vdWEG18]. **Detective**
[Cho10]. **Detector** [LTKP16].
**Detector-Based** [LTKP16]. **Determine**
[FSWF11, Sto12]. **Determining**
[NN12, Scr18]. **Deterministic**
[MPS12, NIS12, XXZ12, DTZZ12].
**Deterring** [WGJT10]. **DEUCE** [YNQ15].
**develop** [Ham19]. **Developed** [Har16].
**Developing** [CH11]. **Development**
[Pau10]. **Developments** [GCK12, Vai11].
**Device** [ABCL17, CFXY17, DFKC17, HSUS11, KLM+12, SRK+17, TYK+12, ZSH+19, CRS13, GM16, KKG14, Km16, OSP+19, Par12b, SHB19, VV19, XTH12].
**Devices** [AAC+16, BDM+19, CSH+18, DLWW11, EGG+12, FMC19, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, May15, MS16, NVM+17, Sch15b, SFE10, SWF+19, VWC19, WKB16, WT10b, XJR+17, Aia15, CLP+13b, CFS13, CTL12, Ch13a, FRT13, GTSS19, IB11, KPP16, LKAT12, MvO11.
MHV15, NSBM17, OYHSB14, SSNS15, SCR19, SHBC19, TZTTC16, TG17, ZPZ16.

DFA \cite{PDJ19, WH17}. DFA-Resistant \cite{WH17}, \textit{DFT} \cite{DDFR13}, \textit{DHA} \cite{AKY13}, \textit{DHA-256} \cite{AKY13}, \textit{DHTs} \cite{YKGK13}.

Diagram \cite{WGD18}. dieckory \cite{NN15}.

dictionaries \cite{ABR15, Maf16, MBB11}.
did \cite{CMG18, Lin14b}.

Diego \cite{Ano10, Lin14b}.

Dies \cite{Mar10a, MMB17}.

dierence \cite{BS14, YTP11, JK13}.
dierences \cite{LHM13}.

dierencing \cite{LyWlZZ12, YWW10}.

dierent \cite{GZ12, HHH13, KU12, AKK17, ABW10}.

dierential \cite{BMS12, BNY14, CWP12, CGCS12, ESS15, FXP17, LKW12, LJ16, LJ15, LYYH14, MRTV12, PH12a, QGG13, RCP18, Sun11, WHN12, Blo15, DDFR13, LKLL10, MNP12, PBCC14, SDM10, SDM14, TSL11, TS16a, WYL14}.

dierentially \cite{RCBK19}.

dierentials \cite{WW12}.

diering \cite{GGHW17}.

diering-Inputs \cite{GGHW17}.

die \cite{LZC14, ABD15, Chi16, Hof16, HLCL11, HLYS14, LNL19, Orm16, RH10}.

Diffusion \cite{ZHL15, WB12, jT12b}.

DIG \cite{NKWF14}.

DigiNotar \cite{JB11}.

digit \cite{KWH16}.

Digital \cite{AYS15, BBC13, BM13, BCP14a, FMS12a, GP17, HPO15, Jin10, LZC12b, XYXYX11, XLP18, DWZ12, QD16}.

Dimensions \cite{Pal15, Pal15}.

Direction \cite{NS12}.

Directions \cite{BKBK14, CDFZ16, Hof16, PPA18}.

Directly \cite{LZC12a}.

directory \cite{SMBA10}.

disabled \cite{HFT16, disassociation}.

Disc \cite{NRZQ15, BBG17}.

disclosure \cite{NRZQ15, BBG17}.

Discovery \cite{MJS19, Ano11a, MMP19}.

Discrete \cite{BGJT14, CWW14, CGCS12, ESS15, FXP17, LJ16, LJ15, LYYH14, MRTV12, PH12a, QGG13, RCP18, Sun11, WHN12, Blo15, DDFR13, LKLL10, MNP12, PBCC14, SDM10, SDM14, TSL11, TS16a, WYL14}.

Discrete-Continuous \cite{SRT12}.

Discrete-Continuous \cite{SRT12}.

discrimination \cite{GPVCdBRO12}.

Discriminative \cite{YY14}.

Discussion \cite{Gli12, Wil18, Bul10a}.

Discussions \cite{KDT12b}.

Disk \cite{GM14, Ran16}.

Disks \cite{Mar10c}.

Disparate \cite{SSY12}.

Dispatching \cite{YTH17}.

dispersed \cite{ED19}.

Disreputable \cite{ABJ13}.

Disruption \cite{HK14}.

Distillation \cite{BJ16}.

Distributing \cite{Kup13, MS10}.

Distribution \cite{EAA16, JEA10, AASSA18, ABB15, BBN16, FMS12a, GP17, HPO15, Jin10, LZC12b, XYXYX11, XLP18, DWZ12, QD16}.

dithered \cite{UUN13}.

Diversity \cite{ZTL15}.


Doubling [Zha12]. Doubly [CZF12, CW14b]. Doubly-Spatial [CZF12].

Douglas [Ber16a]. Down [Ano17e, McG11].


Drive-Thru [SYC+17, SYW17]. Driven [BMP12, DLM+18, APMCR13, LSQ15].

driver [GBC19]. DriverAuth [GBC19].

DriverGuard [CDD13]. DRM [Pet12].


DTLS [AP13]. DTRAB [FTV+10]. Dual [BWR12a, CCG+16, CMG+18, HF14b, HPL+19, NLYZ12, PAF18, BW13, CFN+14].


Dynamic [ABB19a, EKB+16, FHR14, HH15, KHY18, LMH+15, MWZ12, MM12, NKWF14, PPS12a, PNRC17, SSW12, SY14, SKV12, SGC14, VMV15, XNK15, XWSW16, XZY+12, XZW+18, YLSZ19, ZXYL16, BSBBG19, CTL12, CSTR16, DSCS12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KH18, KPB17, LDC13, LXMW12, LHM14, LZC17, NPH+14, PSJ+13, SES+16, SSS11, SM10c, SGM16, WDZ19, XHM14, YZL+18, YD17, ZMS18, ZZL+18].

dynamic-identity [JZS+10].

dynamical [JT12b]. Dynamics [RSCX18, AaBT16, GEAHRI11, LTC+15, Lüd12, MCRB19, TZTC16].

dynamics-based [AaBT16].

dyslexic [Bha16].

e-commerce [Ano11a]. e-exam [Mor12].

E-health [WMX+17, IC17, OSP+19, YZL+18, JKL+16].

e-Learning [Yon11].

e-mail [BTW15]. E-passport [LZJX10].


EAP [FLH13, HZC+14, ZCLL14]. EAP-based [HZC+14, ZCLL14].

Early [Bel18a, Bro11, And13]. Earth [Har14].

easier [MBF+13]. Easy [Bel16, SMDS11, Tay14, Wu16, ZDW+16].

Eat [DSSDW14]. Eavesdropping [CWL16, Han12, PX13, YSJ14]. EC [Dra16, CFN+14, CCG+16, CMG+18]. ECC [BSSV12, CBL10, HJ19, JM+16, KRH18, ZSH+19].

ECC-Based [BSSV12]. ECDSA [BBB+16a, DHB16]. ECG
[HW19, PLGMCdF18]. **ECG-based**
[PLGMCdF18]. **Echo** [DLM+18, HGT15].
**Echo-Based** [HGT15]. **economy** [WDZ19].
**Ecosystems** [RVS18].
**Ecosystems** [LDB15, MPP19].
**eCryptfs** [XZL19]. **Ed25519** [TV19]. **EDAK** [ABB19a].
**EdDSA** [JL16]. **Edge**
[AHM18, DF16, KA18, XHZ19, JZU19, MD15, PRN19, Sun16, XZP19].
**Edge-Based** [XZL19]. **Edge-centric**
[AHM18]. **edge-enabled** [JL16].
**Edition** [Cor14a, Kob19]. **Editorial**
[OK18, Ano19a]. **Editors** [BdD19, LLK18].
**Education** [LRW14].
**Edwards** [JL16, LT14a, YTS12]. **Edwards-curve** [JL16].
**EFADS** [WLS14]. **Effect**
[PLGMCdF18, WB12]. **Effective**
[HLT+15, KRDH13, WMX17]. **Effectively**
[YMC17]. **Effects**
[MAL10, SKV12, SHBC19]. **Efficiency**
[ABF12, Chi16, DG17, FRS16, HRV10, LML12, LCL17a, MS13b, WXL16].
**Efficient** [ABB13, ASBD16, ABB19a, BWLA16, BCGH11, BHG12, BV11, BV14, CG12a, CML18, CMLRHS13, CWWL12, CJ13, DA18, DWB12, Dun12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GT11, GPN12, GPT12, GJJ15, GH12, GZH17, GCH15, HZC12, HZC14, HZL18, HL10b, HBC13, HXZ15, HKL12, HDPG15, HCDM12, HH16, HC17, IAD10, KP11, Kim15, KHPP16, KKK18, KH10, LLP18, LDM12, LZT12, LNN13, LXX14, LCL15, LSIW15, LHYZ12, LWHS17, LZC17, LBOX12, MX13, MTY11, MVV12, MU12, MKASJ18, MCI11, MN14, NES14, NDMMW16, NZZ10, OS19, PB12, PA18, PCD12, PG12, PCP14, PNR17, RSD19, RHP15, SLL19, SGG11, SZZ14, SG16, TLF16, TZW11, TT12, TM18, USH19, WDCL18, WLS14, WQZ16, WC18, XLWZ16, XMLC13, XMY17, XHZ19, YHL16, YNR12a, YNR12b, YLW13, YNQ15, YLA13, YS15, ZQWZ10, ZLI12, ZSW12]. **Efficient** [ZJX14, ZXY16, ZCL19, ZHS19, ZPW16, ZHW15, ZC17, AZPC14, AZF12, ABR15, CH11, CCSW11, CLJJ13, CZ14, Chol14, Cral11, CGKO11, EA12, FLL14, Far14, FA14a, FA14b, FQ15, FZZ12, FNWL18, GH16, GLM11, HPC12, HYS18, ISC16, IB11, IOV18, JCS16, JZS10, KKG14, KI19, KL11, KSH18, LLLS13, LH11b, LH10c, LXM12, LAL15, MDH18, MLM16, Mes15, Nov10, NX10, OCGD11, PZBF18, PC14, Rao17, SZMK13, THA13, TLL12, Ts13, TKHK14, VN17, WYL13, WLZ16, WT10a, WXK17, WZW16, yYqWZ13, ZLY10, ZC17, ZCL14, ZTZ16, ZC15, Zhu13, LLZ12, TCL15]. **Efficiently**
[FWS13, LGH17, SLY16]. **Effort**
[RSBGN12]. **Effort-Release** [RSBGN12].
**EGHR** [CML18]. eHealth [TMGP13].
**eID** [SSCG16]. eight [Sun11].
eight-round [Sun11]. **Einführung** [Buc10].
**Einstein** [HR13, Wes15]. **Elbirt** [Bar12].
**Election** [Ess17, TMK12]. **Elections**
[CEL19, QS19]. **Electoral** [CEL19].
**Electrical** [VT18]. **electrocardiogram**
[BLL19, OMPS19].
**Electrocardiography** [LLLH18, YH16].
**Electromagnetic** [HH1+13]. **Electronic**
[Bl12, PWVT12, SR14, YWS11, CLC19].
**Elementary** [Led16, Sch15a, CM13].
**Elements** [Kra12]. **Elevation** [LZC12].
**ElGamal** [HLH19]. **ElGamal-like** [HLH19].
**Elliptic**
[AD11, AK14, ARM15, DW12, FHD19, GPT12, LGH17, LWHS17, MST18, PPH12, SG15, She17, AMN18, BAAS13, BL14, BL17, BBB16b, Chol14, Far14, IB11, KK10, MCN18, MS13b, NZZ10, SKH15, WHJ17].
**elliptic-curve** [BL17]. **ELmD** [BDML16].
**Elsevier** [Ano15b]. **Email**
[Bel16, CCS14, XJ+16, WR15]. **embed**
[KPS10]. **Embedded**
[AB15, BS12, BJCHA17, CFXY17, HJ19, HC17, JW1+17, LWHS17, MGG19, SOG15,
SK12b, SWF+19, SDM+12, WXY+17, YGD+17, YS15, ZSH+19, Ano11a, CVG+13, EIs10, MFH13, WHZ+19, XWZW16.

**Embedding** [KD12a, MCDB12, XNRG15, XNP+18, XZZ18, YE12, ZS12, EA11, LHM13, MKH+12, PWLL13]. **Embeddings** [FHS13].

**Emergable** [YT12]. **emerged** [McG11]. **Emergence** [LMB12]. **Emerging** [BSV12, KSA16, OS16, FPBG14, ZHH+19].

**Empirical** [gWpNyY+14, EBFK13, Sar14]. **Employees** [Mor12]. **Employing** [LGLK17].

**EMV** [Cho10]. **Enable** [SMS14]. **Enabled** [GPT12, HFT16, KV18, QZL+16a, QZL+16b, SGC16, SSPC12, YSF+18, BMM12, JZU+19, NML19, TODQ18, YFT18]. **Enabled/disabled** [HFT16]. **Enables** [IBM13a]. **Enabling** [FRS+16, GGYW+19, JSM+18, SSY12, WPZM16, YYS+16, MMP19, Sch12b]. **eNB** [CLM+12]. **Encrypt** [ADK12, BTHJ12, CWL+14, CWL16, Cor14a, CHH+19, DWB12, DCA18, FCM14, FRS+16, Fy019, Gen13, GLG12, GZH17, GYW+19, HTZR12, HB17, HCDM12, IMB17, IBM13a, JSMC17, Kaw15, KGV16, LA15, LGLK17, LQD+16, Lop12, Mur16, NBZP17, NNAM10, PBC+17, QLL17, SAKM16, SZHY19, Sia12, TM18, Vai12, WBC+10, XWSW16, YDY+16, ZDL12, ZXYL16, ZVG16, ZLW+17, AHM+18, AZH11, BBP16, BTPSL15, BGP+17, BKV13, BTK15, BL11, CH11, Cri16, CDL18, DKL+16, DRD11, DJ19, ED17, FTW+10, Gen10, GZS+18, HKA19, HH16, LKX+14, LZY+16, LHL+18, LW13a, MRR+18, OSSK16, PWS19, PBP19, PRZB12, SEXY18, SWW+17, Suc12, TKMZ13, WR15, WS19, WL19, XMY+17, XXY+18, Yaa19, XDY18, YQQL17, ZLY10, ZZC17, ZFH+18, ZHT16]. **Encrypting** [CC10, Mar10c, dRSdlVC12, Cia18, LFCCGCRP14, Poi14]. **Encryption** [ADM12, AV12, AUAIC18, AEF17, Alo12, AAC+16, Ano13c, Ano14, Ano15c, Ano17d, Arn19, AKP12, ABF12, AS16, BVS+13, BWLA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12a, BS14, BV18, Bla16, BKLS12, BDPS12, BHJP14, BDMN16, Boy13, BV11, BV14, BGV14, CVM14, CMO+16, CLL16, CWWL12, CN12, CZF12, CLHC12, Che15, Che18, CGL+12, Ch12, Chu16, CRE+12, Con18, CNT12, CLW16, CD16, DR10, DN12, DFJ+10, DSLB18, Des10b, DGFH18, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJH12, Fe19, FLL12, Fuc11, GWW15, GGH16a, GGHW17, GM13, GZZ+13, GSW+16, GH11a, GH11b, GHS12, GHP12, GDCC16, GW12, GV15, GM14, GL12, GKS17, Gue16, HSMY12, HLLG18, HZ11, H12, Hor19, HC17, HTC+15, HLH19, HP12, Int19, IAD10, JLS12, JHLH12, Jia14a, JR14, Kam13, KB10]. **Encrypted** [KME+12, KMY18, KTT12, KOS16, KKA15, KFOS12, KHP16, KKK+18, KML18, KS12, LMGC17, LMG+18, Lai17, Led16, LLWS16, LLPO19, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LCC+15, LZ16, LLL17a, LFX+18, LLLH18, SLLW15, LH11c, LSQL18, LB13, LY15, LW16, LYY+18, LLLM12, LH18, MZHY15, MLO17, MPP14, MR14a, MT11, MS18a, MVVR12, MMS17b, MSR+17, MRL+18, MBF18, MRPS12, MZLS18, MT12, MKRM10, MSas12, Nac16, NmMMW16, NTY12, NMS14, NAL17, OT12, OGK+15, PMZ13, PR12, PB12, PDHN15, PRGBSAC19, Per13, PTK12, PPS12a, PYS18, PMZ12, PCY+17, PRSV17, RVH+16, RCP+18, RZZ+15,
RM18, RSBGN12, RDZ+16, RVRSCM12, SGG18, Saa12a, SSW12, SERF12, Sar10b, Sch15a, SLGZ12, SXH+19, SZS14, She14, SWF+19, Smi11b, Sta12, SGH15, SMOP15, Tan11, TCN+17, TCL5, TMC15, Tan17b, TDTD13, TKR14, TT12, TFS19, Unr15.

**Encryption**

[Vai11, VSR12, VOG15, Wal18, WHC+15, WP17, WDC18, WSS12, Wat12, WLC12, WDDW12, WZ15, WWHL12, WMS+12, WQZ+16, WZCH19, XNKG15, XY18, XZ12, XJWW13, XLJ16, XJW+16, XHX+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC+11, YFK+12, YCY12, YKKL12, ZOC10, ZPM+15, ZQZ+19, ZDL12, ZYT13, ZWTM15, ZQQ15, ZMW16, ZZM17, ZYX+19, ZHW15, ZY17a, ZYM18, ZWS+18, ZYH+19, ZHZ+19, AHS14, AASSA18, ATKH+17, AKKY17, Ana14, Ano13b, Ano15e, Ano16f, ABR12, AMHJ10, ACD+15, AHL+12, BBL+19, BAAS13, BC18, BKR19, BG14, BSW12, BGP+17, BTK15, Bro19, CPPT18, CFVP16, CFZ+10, CW14b, CLH+16, CMMS17, CLC+19, CZ15b, CS11, Chu10, CW12a, CDF+10, CM13, CGKO11, DLZ16a, DDM17, DTZZ12, DMD18, Eve12, Eve16, FAA+18, FH13, FSGW11, FSGW12, Fay16, GMOGCC15, GH13, GHS13, GLM+16, GH12, GLL+18, GXZA19, HGWY11].

**encryption**

[HQZHJ4, HZLI18, HKA19, HDWL16, HZWZ18, HL19, HT13, HLR11, HL11, HFT16, HTH17, HYS18, HYF18, HHHW19, HKHK13, JZU+19, JCHS16, Jia14b, JSMG18, JHCC14, JSM+18, Kam16, KHM13, KKM+14, LLW16, LCL+17a, LGP19, LCL+15, LFZ+17, LCT+14, LFWS15, LLM+19, LPD10, LHH11, LW10, LK10, LW13b, LZC14, LPZ15, LCY+16, LZC17, LJW+17, LJJW18, LLL+18, LZXX19, LDZW19, LL16a, LSC13, LSC12, LLG19, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSAs13, NES+14, Nam19, OPHC16, OSNZ19, PPA18, Pet12, PBP19, QRW+18, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, SLL+19, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SVGE14, SGFCRM+18, SLM10, SKB+17, Spa16, SGP+17, SG16, Tan15, TPL16, jT12b, WGJT10, WY10, WYZZ11, WWYY11, WLVG11, WHY+12, WDLZ13, WLFX17, Wan18, WDG19, WGW+12, WLS14, WCH18, XWZW16, XWX14, XSWC10, XXX15, XWS17].

**encryption**

[XZP+19, XWZ+18, XTZ+19, XLC+19, YWJ+19, YT11b, yYqWqZC13, Yan14, YZCT17, YHHM18, YWY+19, YCT15, YLZ+16, YL11, ZCQ19, ZQW+11, ZZ11, ZLW+12, ZXJ+14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZYQ+17, ZGL+18, ZCL+19, ZZ12, ZL12, DZW+16, YZ17b, ZCZ+19, Zhu13, Wan14, LAL+15, Sar18a, Kat13].

**Encryption-based**

[SERF12, BC18, XWZ+18].

**Encryption/Decryption** [KB10].

**Encryptions**

[2GXW12, LG12, SLX+16, RD17].

**Encyclopedia** [vTJ11].

**End**

[Ano15c, BRR+15, BGP+17, CFE16, Chl16, RST15a, RST15b, Bel18b, Chi13a, JZU+19].

**End-to-End** [CFE16, RST15a, RST15b, Ano15c, BRR+15, BGP+17, JZU+19].

**endomorphism** [FWS13].

**Endomorphisms** [AK14, LGH+17].

**enemies** [Fag17].

**Enemy** [BC14, CAC14].

**Energetic** [PDMR12].

**Energy** [Ano15d, AZF+12, ABC+17, Bla16, CKHP19, GPR+19, JEA+15, LSC+15, PM12, PA18, TLF16, TCN+17, VNN17, CZ14, ZTZ16].

**Energy-Efficient** [MP12, TLF16].

**Energy-Harvesting** [ABC+17].

**Energy-time** [Ano15d].

**Enforced** [Set16].

**Enforcement** [LLZ+17, Tan15a, Cra11, CFG+17].

**engagement** [LSBN14].

**engaging** [ISC+16].

**engine** [BS15a].

**Engineering** [BCHL19, Bel18a, FSK10, GHD19, LLK18, MSM18a, MP12, PGL10, SNG+17].
TQL+14]. Engines [LB13, BGG+13].
Enhancement [CZ14, SLM10]. Enhanced [DTE17, KY10, KKM+13, MS17, SGG18, TV15, Y17, YCC16, AMN18, ACK++10, DLK+16, GM16, LNK13, YQL17].
Enhancement [FSX12b, LA15, NNA10, CHS11, SVY19].

Enhancements [Che18, FSX12c].

Enhancing [CSW12, IA15, Lan13, YS15].

Enigma [KM15, KM16, LHA+16, Ore14, Ano16c, Bur11, Kap11, Kap13, McG11, McK12].

Enigmas [Bat10]. Enough [JCM12, Ano14].

Enrollment [YWZ+12]. ensuing [SS17].

Entanglement [Ano15d, JEA+15].

Entanglement-Based [JEA+15].

Enterprise [TGC16, XZL+19, Din10, KLN15, NB13].

Enterprise-Level [XZL+19]. Enterprises [KCR11].

Environments [HLKL15, LQY10, PAS13b, TMGP13, XLP+18, CLHJ13, CTL13, KPP16, Kas15, LNK+18b, LW13a, LCY+16, NACLR12, SCY15, SA19, Tan12b, VDO14, VGL14].

EoF [Gup15]. ePassport [ABHC+16].


Equality [CHH+19, HTC+15, LLSW16, MZHY15, WZCH19, HTC17, ZCQ19, ZCL+19].


Equivalence [ABR12, CCK12, CCK16, GLW12, SS13, WGD18, HKT11]. Era [Mos18, QCX18, ABJ13]. Ergodic [IAD10].

Erratum [YFK+12]. Error [KW14, LSC+15, MCP15, MKASJ18, TCLF16, ATT+10, Chi13a, LTT10].


Establishing [DKL+16, GSFT16].

Establishment [ASN12, Ano11b, BCO13, DL12, NYR+14, BEB+18, GTSS19, SZMK13, ZPZ+16, ZXW+18].

Estimation [BCF16, GSN+16]. Estonian [Ano17c].

Ethernet [KCR11].

EU [PH12b].

EUROCRYPT [PJ12, Gil10]. Europe [GOPB12, Mid10]. European [GOPB12].

Evaluating [RAZS15, WP15]. Evaluation [BKLS18, CGCS12, DM15, DCA19, EGG+12, FXJ19, JGP+18, KVve18, KLM+12, MK13, MLBL12, SSSP19, SMOP15, ZLDD12, BKR19, FPPB14, K19, LQP19, THA+13, TPPT12, ZZKA17, ZLDD14].

Evaluations [ZM16]. evaluators [ZZKA17].

Evasive [BBC+14]. Eve [AAE+14, ERLM16, FHM+12].

Even [ARH14, Faa19, LPS12, Ana14, DK12]. Even-Mansour [LPS12].


Every [Hof16]. everyday [HST14].

Everyone [Ano15c]. Evidence [Bla12, SR14].

Everyday [SL11]. every [Hof16]. everyday [HST14].

Examin [SP13]. Example [KD12b].

Exchange [CLY14, CST+17, DG15, FVS17, GZ12, HC12, LK16, MSU13, TYM+17, WSA15, Wl10b, YS12, YLW13, YRT+16, Yon12, ZHZ16, AKG13, AIB+16, FHH10a, FA14b, FIO15, GBNM11, GLM+11, Jia14b,
Feasibility [AAC+16, FKS+13, OMPSP+19, WHC+15].

Feature [Ber18, SGP+12, FTV+10, GJ13, MHT+13].

Features [MHW+19, YI14, ZTL15, FNP+15, LCM+17, LTC+15a, NMX15].

Feauve [Ara13].

February [Ano10, DDS12, Dan12, Dun12b, Kla11, Lin14b].

FedCohesion [CCFM12].

Federated [BS13b, CCFM12, CSL+14, SAM+19, BMB10, BSG19, JAS+11, TODQ18].

federated-IoT-enabled [TODQ18].

Federations [SS10a, NB13].

federations [MMS+17a, MLM16].

Feedback [HZ11, Hey17, PYM+15, SKGY14, ZH15, LWK11].

Feedback-Based [PYM+15].

FEIPS [DG15].

Feistel [BFMT16, KDH15, Sats12, SEHK12].

FESSD [LGLK17].

FHE [CK18].

FHE-Based [CK18].

FHSF [SP15a].

FI [YNR12a].

FI-BAF [YNR12a].

Fiat [BD10+13].

Fibonacci [FM15, LLP+18].

Fibonacci-number [LLP+18].

Fidelity [BCP14a].

Field [CLF+17, GHPS13, HSA14, SS12a, TGC16, ZAG19].

Fields [ARH14, BGJT14, HVL17, ZL19, AA14, BGJT13, CZh15a, LBOX12, OJS11].

Fight [Ano16e, Wu16].

File [DMS+16, LY16, TLC16, XZL+19, ZGC16, YHH18].

Filling [BWR12a].

Filter [Kaw15, AKT+17].

filtered [HTC17].

filtered-equality-test [HTC17].

Filtering [LLZ+12, CDGC12].

Financial [Ano11b, Ber12, DDS12, Dan12].

Finding [Hof16, Ste15a].

Fine [CDD13, PV17, YTH17, ZM17, CLH+16, FSGW11, LHH+18, XYL19].

Fine-Grained [CDD13, PV17, YTH17, ZM17, CLH+16, LHH+18, XYL19].

FinFET [ZJ11].

FinFET-Based [ZJ11].

Finger [KLY+12, NSBM17].

Finger-drawn [NSBM17].

Fingerprint [DS19, MR14b, HW19, KKG14, ZHL+11, ZHH+17].

Fingerprint-Based [DS19].

Fingerprinting [QF19, SNK18, TSH17, ZS12, FLZ+12, RS17].

Finite [BGJT14, CHS15, GMNS15, HVL17, ZL19, AA14, BGJT13, CZh15a, GZLZ13, LBOX12, OJS11].

Finite-State-Machine [CHS15].

firms [Ano15e].

First [Ano17d, BH15, DR10, LFX+18, MS17, PC16, Wil18, AB10a, BCV12, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14].

First-Generation [BH15].

First-Order [LFX+18].

Fischlin [ABGR13].

Fishebone [KS19].

fistful [MPJ+16].

fit [KGO10].

Fix [DLV16, HLV10].

Fixed [Chn10, Lin11].

Flag [MBC+18].

Flame [Goo12].

Flaw [Moo12, SH15, Ste15a, ACC+13].

Flaw-Finding [Ste15a].

Flaws [DR11, FVJ19, HLV10].

FlexDPDP [EKB+16].

Flexible [LGWY12, PAF18, TV19, BGG+13, WZ19, WLS14, ZL12, ZFH+18].

Flexlist [EKB+16].

Flexlist-Based [EKB+16].

flip [Wag16].

Flow [ATS15, DJ19, HBC+19, WXL+17, CFG+17, KKL13, LWY12, PPR+12, SRB+12].

Flowers [Hai17].

Flows [CDD13, HKB14, WYL13].

fly [PS14].

Fog [FMC19, JWNS19, Gop19, JSMG18, KH18, QRW+18, Wan18, WDKV19, ZSW+18b, YXA+18].

Fog-based [FMC19].

Follows [Arm19].

FontCode [XXZ18].

Foolproof [FFL12].

Force [JR14, CJP12, CJP15].

forensic [Har14].

Forensics [Ber18, CFXY17, AKM+11, Har14, QZ14, SM13].

forged [HERJ14].

forgeries [YQH12].

Forgery [LC15, BM13, LWL11].

forgotten [And13].

form [DWZ12, Kre13].

Formal [ACF16, EWS14, HSA14, KGO10, PLC11, ZW15, Aia15, CDW19, THA+13, VXW14].

Formalized [YCR16, NML19].

Formally [KRM18].

formats [ZT14].

forms [TY16a].

formula [DWZ12].

forthcoming [MMP19].

FORTIS
[GSFT16]. **Forum** [Rau15]. **Forward** [ABD+15, BVS+13, BDH11, FLH13, GSFT16, HLT+15, KME+12, KZG10, LTH+15, NMS14, WLH15, XW12, Yon12, YHK+10, YKC+11, ATKH+17, BM11, TCS14, WL19, YFK+12]. **Forward-Secure** [BVS+13, KME+12, LTH+15, NMS14, WLH15, YKC+11, YFK+12]. **Forwarding** [Bal10]. **Found** [Moo12]. **Foundations** [BCHL19, Des10a, IEE10, IEE11b, Lin17, SN10, NS10, Sta11b, Ter11]. **Four** [LyWlZZ12]. **Four-Pixel** [LyWlZZ12]. **Fourier** [GJ13, yWpWyYpN13]. **Fourth** [Kob10]. **FOX** [LJF16]. **FPGA** [AMKA17, BCE+10, BDGH15, CFZ+10, CHS15, GFBF12, IIJ19, HF14b, MM14a, MAK+12, TV19, ZLQ15]. **FPGA/ASIC** [CFZ+10]. **FPGAs** [DGP10, SMOP15, VMV15]. **FRA** [AMKA17, BCE+10, BDGH15, CFZ+10, CHS15, GFBF12, IIJ19, HF14b, MM14a, MAK+12, TV19, ZLQ15]. **FRA** [CFZ+10]. **FPGA** [AMKA17, BCE+10, BDGH15, CFZ+10, CHS15, GFBF12, IIJ19, HF14b, MM14a, MAK+12, TV19, ZLQ15]. **FPGA/ASIC** [CFZ+10]. **FPGAs** [DGP10, SMOP15, VMV15]. **Fractal** [BJL16, Des10a, IEE10, IEE11b, Lin17, SN10, NS10, Sta11b, Ter11]. **Four** [LyWlZZ12]. **Four-Pixel** [LyWlZZ12]. **France** [Kap11]. **Francis** [Joh10]. **Francisco** [Dun12b, Kia11, Pie10]. **Francois** [SR14]. **Frank** [ABJ13, Joh10, Mar10a]. **frankencerts** [BJR+14]. **Fraud** [Ber12, CEL+19]. **Fred** [Xie12]. **Free** [App13, Boy16, HLH19, IL15, TWZ+12, TTH15, WZH19, ZLH+12, ATKH11, ED19, LL16a, SA12, SE16, YT11b]. **Free-View** [TWZ+12]. **FreeBSD** [MNNW15]. **Freedom** [Con18]. **Freestart** [SKP15]. **Freeze** [HHAW19]. **French** [Ant14]. **Frequency** [BBM15, KAHKB17, LTKP16, LWCJ14, TC10, CJP12, CJP15, EA12, NLYZ12]. **Frequency-Based** [LWCJ14]. **Freshness** [RBNB15]. **Friendly** [Fra16, KCC17, SZDL14, ACM12, BP18, KLW+16, RD17, WOLS12]. **Frontside** [DDR+16]. **FSR** [MD12b]. **FSR-Based** [MD12b]. **Fugue** [AP11]. **Fujisaki** [TFS19]. **Full** [Arm19, ALR13, DGFH18, HEC+12, LW12, VS16, WLC12, BKR11, DDM17, LC13, Ran16, SWW+17, SKP15, Tam15, TY16b]. **full-hiding** [DDM17]. **full-text** [SWW+17]. **Fully** [AKP12, BV11, BV14, BGP14, CM+16, CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, KKK+18, LMGC17, LSLW15, LSC12, MVV12, MSM18a, Nac16, NCCG13, PB12, SGH15, Vai11, VV19, WHC+15, XWZ+18, ZZ12, GH13, ZXJ+14, ZML17]. **Fully-Homomorphic** [GH11b]. **Fully-Homomorphic-Encryption** [CN12]. **Fun** [APPVP15]. **Function** [AMP14]. **bee17**, **BKF18**, **FLS+10**, **LyWlZZ12**, **MMS17b**, **SGY11**, **WSSO12**, **YWJ+19**. **AKY13**, **AP11**, **CMMS17**, **LK14**, **LP11**, **RS14**, **Sar11**, **XLL16**, **TQL+14**, **WYW14**. **Function-based** [YWJ+19]. **Functional** [AS16, BV18, BS12, Boy13, GGH+16a, GWV12, LQD+16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14]. **Functionalities** [JR13]. **Functions** [ACZ16, ALR13, BBC+14, BIKK14, BKWP12, BK12a, CCL+19, CPS16, DSS14, DQFL12, FY11, LVV11, NR12, Rja12, RW12, SMS14, SLY+16, TAN12a, YTP11, YL14a, BDPI11, CG12b, CQX18, CW12a, ESRI14, Gen10, HRV10, HL12, Li10, QZDJ16, WT13]. **Fundamentals** [Joh10]. **Further** [HCL+14, WHY+12]. **Fus**
Future-proof [Mon13]. Fuzzy

Glyph [XZZ18]. GMAC [SKK10].
Goal [BMP12]. Goal-Driven [BMP12].
Goes [BCD12, RY10]. Goldreich [Lin17].
Goldstrike [BH15]. Goliath [Sch15c].
Gong [LLW16]. Good [BCD12, RY10, SA14, WT13].
go15. Google [Har14, Loe15, VGN14].
Goldstrike [BH15]. Goliath [Sch15c].
Gong [LLW16]. Good [BCD12, RY10, SA14, WT13].
H.264 [JSZS12, JHHN12, LLHS12, LW13c, MU12, WDDW12, ZLDD12, ZLDD14].
H.264/AVC [JSZS12, JHHN12, LLHS12, LW13c, MU12, WDDW12, ZLDD12, ZLDD14].
H.265 [GKSB17]. H.265/HEVC [GKSB17].
Hack [DLV16, Fol16, Ran10, Ran14, Ran16].
Hacker [ZGC16]. Hacking [GHS14, Hea15, JEA15, Sta13].
Hand [GPT14, BSS11]. Hands-on [BSS11].
Handshake [KK12, KK13, SM10c, WZ11].
Hard [KPC11, Mar10c, ZWTM15, RPG12]. Hard-to-Invert [ZWTM15]. Hardcover [Joh10].
Harder [KTA12, Sch16]. Hardness
[BHKN13, SS13]. **Hardware**

[AW15, AW17, ARH+18a, BRPB13, BDMLN16, BJCHA17, CMLRHS13, DZS+18, DOS15, ERRMG15, GP17, GPR+19, GCVR17, GCS+13, HKL+14, HG12, HSA14, HC17, HLN+10, KAK8, LGH+17, LLKA19, LRWV14, MLCH10, MCS+15, MRL+18, MHY+18, NDC+13, NdMMW16, PC16, PG12, RMP10, SN10, Set16, Sti19, Tay17, WOLF15, YSF+18, ZL19, ZHS+19, ZAG19, AMN18, BDM18, BGG+13, KHF10, MD12a, NS10, Nov10]. **Hardware-Assisted** [LLKA19, GPR+19].

**Hardware-Based** [HLN+10].

**Hardware-Enabled** [YSF+18].

**Hardware-Enforced** [Set16].

**Hardware-Intrinsic** [SN10, NS10].

**Hardware/Software** [MRL+18].

**hardware** [SKH15]. **Hardy** [Xie12].

**Harmonic** [YWNW15].

**Harnessing** [DFKC17]. **Harvesting** [ABC+17, ZGC16].

**HAS-160** [WLC12]. **Hash** [Ano12, AMPH14, BHH+15, BKST18, BK12a, CLP13a, CPB+12, CZLC12a, CZLC12b, CZLC14, CJPI2, DCM18, EAA+16, FLN+10, GI12, HCPLSB12, Hül13, HRS16, HBG+17, LLY+19, MkF+16, MCF17, MKA17, MKASJ18, NTY12, NR12, NXR13, PTT16, Rja12, Sgy11, WSS012, ZZN17, ZHZ+19, AY14a, AKY13, AP11, CP15, ESR14, HIL12, KKG14, Par18, DBPB16, R14, SPLHC14, SXL16, WYW14, ZCZQ19].

**Hash-Based** [BHH+15, GI12, HCPLSB12, Hül13, HRS16, HBG+17, MkF+16, MCF17, MKA17, NXR13, CP12, CP15, PPB16, SPLHC14].

**Hash-Counter-Hash** [MKASJ18].

**Hashing** [AAE+14, ASbDS16, BHKN13, BKL+13, BP18, Kaw15, CP13]. **Haskell** [Rus15]. **hatching** [WYK12]. **HB** [HSH11, PYH+18]. **HDH** [PDNH15]. **Headline** [YGFL15]. **Health** [LYZ+13, LHL15, Rao17, ZVG16, BC18, CLC+19, Ham19, IC17, OSP+19, WMX+17, YZL+18, JK+16]. **Healthcare** [BN14, HLKL15, ZLDC15, ASO14, Kim16]. **Hearing** [Bla16]. **Heartbeat** [IA15]. **Heartbleed** [DKA+14, Ven14]. **hedging** [RY10]. **Heights** [Gen13]. **held** [Cho10]. **Helios** [CFE16]. **Hell** [Han12]. **Hellman** [ABD+15, CHi16, Hof16, HLCL11, HLYS14, LXC14, LNL+19, Orm16, RH10]. **Helmut** [Mur10]. **helped** [Smi11a]. **helper** [RWZ13]. **HeNB** [CLM+12]. **Herodotus** [Keb15, Mac14]. **heroine** [Fag17]. **Heterogeneous** [SP15b, AIKC18, ABB19a, SCKH10]. **Heuristic** [BGJT14]. **HEVC** [DG17, GKS17, HIBE]. **Hiding** [DCA18, GGH+16b, GL10, JHHN12, MK12b, OT12, XLM+12, XGL14, XZL15, Ara13, DDM17, HZL18, KHW16, LXY12, LT14b, UUN11, WH13, WZW15, ZWM14]. **hiera** [Lac15]. **Hierarchical** [ADM12, BSSV12, FSX12a, LSL15, NMS14, NLY15, OT12, SSA18, WLY16, ZWM14]. **High** [AW17, ASbDS16, Ano17d, ARM15, Bar15, BDL+11, DM15, DG17, FHL19, GL12, GCS+13, HZ11, KMP+11, KCP+16, KAK18, LTP12, LKC11, LLY+18, LPO+17, MS13b, MS13c, MSR+17, PCPK14, WYC14, WL11, XNR15, XLP+18, ABBD13, GHZ12, GCVR17, KL13, MAK+12, RS17, WLH13, WXL16, WZW13, WKH11]. **High-Assurance** [Bar15, KMP+11, WL11]. **high-capacity** [GHZ12]. **High-Dimensional** [Ano17d, XLP+18]. **High-Efficiency** [DG17]. **High-Impact** [DM15]. **High-Level** [AW17, KPC+16, ABBD13].
idempotent [Dur15]. Identical [Bow11].
Identifiable [Oba11]. Identification [FSX12b, FSX12c, FSX12a, VGA15, YGFL15, YKK18, AGL16, BOP14, CTHP13, CJP12, CJP12, DJ19, EA12, HQY+16, HL19, Ki11, KL13, NLYZ12, YTM+14]. identified [AZH11]. identifier [MJS13]. identifiers [Cer18]. Identifying [Bel18b, CSV15, SVG16, ZCWS15, CAM19]. identities [GLM+11]. Identity [AHN+18, AQD12, ASM12, ASVE13, Ano15b, ACAT+15, ASS15, BWLA16, BCF16, BHG12, BKPW12, BDFK12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CZLC12a, CZLC12b, CLHC12, CLC14, CLND19, CGL+12, CGY+13, Chii12, dCCSM+16, Faai19, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GOPB12, GY13, GDDC16, GJJ15, GJZ17, HZC+12, HvS12, HSM13, HSM14, HZK15, HYWS11, HYF18, JGP+18, KKA14, KRBl, Kuz11, LGM+18, LIX+19, LMB12, LSL12a, LKAT12, LXS14, LLLC15, LTZ15, LSLW15, LH11c, LSC12, LBR12, MLO17, MHW+19, MBF+13, MJGS12, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, Ser12, SXH19, SSPC12, SKGY14, SWW+16, SGH15, TFK14, Tia15, TH16, THA+13, TMGP13, TAP19, TFS19, Vlc12, WY10, Wan14, WZCH19, XZX12, XQL11, XJX+16, YZK+12, YTM+14, Yon11, YHK+10].

Identity [YKC+11, YFK+12, YCZ12, ZHL+12, ZMW16, ZYH+19, ZSD12, vdWEG18, ATKH+17, Ano13d, BM10, BOB13, BSBC819, BBG12, CTHP13, dCCS+16, DZ14, Din10, DWZ12, FA14b, GMRT+15, GPVcBR012, HJP+19, HZC+14, HWDL16, HZBW17, HLR11, HFCR13, HWW10, HWW12, H11, HP10, Hwa11, JZS+10, KKGK10, KK+13, KL11, LKKL13, LK12, LXMW12, LCT+14, MMS+17a, MD15, MGP10, MJS13, MLM16, MM13, NCL13, NLM19, ÖS11, PLCGS11, QYWX16, RG10, SSY12, SE14, SE16, SR10, hSSZ15, SA16b, Sim15b, SSAF11, SS11, SG16, VGL14, WWYZ11, WYY11, WSC14, WLFX17, WMX+17, WHZ+19, Wat14b, YWW17, XW12, XCL13, XHM14, YWL+17, YWW+19, yYqWqZC13, YXS+16, YMSH10, YKC+12, YXX+16, YNX+16, ZMYB17, ZZ12, LZX10, PN10, Sar18a, Kat13]. identity-authentication [NML19].

Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CLND19, CGL+12, CGY+13, Chii12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GY13, GJJ15, GJZ17, HZC+12, HSM14, HZ15, LGM+18, LYX+19, LSL12a, LLC+15, LTZ16, LSLW15, LH11c, LSC12, LBR12, MLO17, RDZ+16, SGH15, TFK14, TFS19, Wan14, WZCH19, XXZ12, XJW+16, YZK+12, YHK+10, YKC+11, YFK+12, YCZ12, ZHL+12, ZMW16, ZYH+19, ZPX17, ZYM18, ZYH+19, CSZ+11, HSM13, HYWS11, HYF18, LKAT12, LXS14, MJGS12, RS15, SXH+19, SWW+16, Tia15, TH16, ZDW+16, BOB13, BM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HWDL16, HZBW17, HLR11, HWW10, HWW12, HL11, HPY10, Hwa11, LK12, LCT+14, MJGS13, MM13, NCL13, QYWX16, RG10, SE14, SE16, hSSZ15, SA16b, SSAF11, SG16, WLF17, XW12, XCL13, YWW+17, YWW+19, yYqWqZC13, YKC+12, YXX+16, ZZ12, LZX10, Kat13]. Identity-Hidden [PSS+13]. Identity-Preserving [MHW+19].

Illusion [GHS14]. Illustrated [Cop10a]. Im [BGI+10, BGI+12]. IMA [Che11]. IMACC [Che11]. Image [Bai10, BAAS13, BDB14, CJFH14, DA10, DCM18, DS19, HD19, IAD10, JKHrY12, KPS10, KLk+19, LA15, LLL17a, LFX+18, LLLH18, LZKX19, MBC15, MAL10, MSM+18b, PWW10, QC+18, RS16, RVRSCM12, SH11, SM11, SZHY19, SJ12, SGP+12, SMSK18, SSA13, SRAA17, SZZT18, TB18, WHZ12, WZXL12, YWW+13, WYCF14, yWxyZ+18, WYK12, YLL+12, YWWW15, Ye10, Ye14, YH16, YXD18, ZXZ+11, ZWZ17, BWA13, BM13, Bro19, CT11a, CW14a, EA11, GKCK11, HAK19, HLC16, KMG17, KM11, LXCMM11, LW10, LWLW11, LW13b, LPZJ15, MO14, MS17, NES+14, PTK14, SE18, Sch12a, SM13, SM12, SMN14, SGFCRM+18, Sun16, jT12b, TTT10, TLL13, UUN11, UUN13, yWpWyYpN13, WHZ19, WGG+12, WKH11, WOLS12, XSWC10, YWL+17, YC11, YCC16, YSC16, ZLW+12, ZT14, ZSMM18, ZL12].


Imperceptibility [HTG15]. Imperfect [ABD+15, BHvOS15]. impersonation [AATM18, GBN11].

Implantable [BDM+19]. Implants [Mic16, SSPL+13]. Implausibility [GGHW17]. Implementation [AAUC18, BW16, BKLS18, BSJ15, BDMlN16, EGG+12, FHLD19, GP17, GL12, GPT12, GCS+13, HJ19, HF14b, KB10, KGV16, MFG16, MAS16, NdMMWW16, QLL17, RPM10, Sec18, TV19, VKP17, ZPM+15, AMN18, BDP+12, GH13, GAB19, HBBRNM+16, KY10, KSH18, MM14a, MNNW15, NES+14, PBCC14, SK14, SAAB10, SVGE14, SF12].

Implementations [BFCZ12, BFK16, BDGH15, BJ10b, Bru12, CMLRHS13, CBL13, ERRMG15, LGH+17, MLCH10, NDR+19, SJL18, Tom16, VV18, YZLC12, ZSH+19, ABBD13, ABF+14, BFG+14, BJF+14, CFN+14, CHG17, LBOX12, RSA19, Sta11b, ZSW+18a].

Implementing [Dav11, GH11b, HTZR12, LTC+15a, SG15, SVGE14, SL10, VOG15, SA16b].

Implications [DK16a, OSH16]. Implicit [BBD19, DWZ12, SS115]. Imly [ALR13, LRW17]. Importance [YL17, MLMSMG12]. Important [TC10].

Impossibility [ACM+17, BCF+14, Mat14]. Improbable [TS16a]. Improve [AQD12, PMG19]. Improved [Ber18, BCP14a, CII2, CGKO11, FVK17, GLLSN12, HI+19, IK15, JHL12, KZG10, LT14a, LWZ12, LJJ16, LHH11, LCCJ13, LC15, LLML12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZZ11, ZLDD12, CBL10, GLW13, HWB12, Nan19, PLL13, SDM10, XHH12, Wan14]. Improvement [FRS+16, LFX+18, LJ19, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNM+11].

improvements [EA12, HVR10, Ts13]. Improving [AB15, BCM+15, Chi16, FMS12b, GMS11, HLC11, MHC12, Sar10a, SS11, YWF18, YKBS10]. impulse [LXKX19]. IMS [GI11, MEFO12, VGL14].

In-Memory [PAF18]. In-Order [ZBP18]. Incentive [S MATERIAL+17, YTH17]. Incentive-Aware [YTH17]. Incident
[CCG⁺16, CMG⁺18]. **Inclusive** [FD11].


**Independent**

[FCM⁺14, MZT⁺11, MKRM⁺10, YE⁺12, ZTL⁺15, BVBD⁺12, DDR⁺14, SCR⁺19, VV⁺19]. Index [LHKK⁺10, PSS⁺13, ZXYL⁺16, Jou⁺13, LLHS⁺12, LW⁺13a]. Index-Based [ZXYL⁺16, LLHS⁺12]. indexed [WXLY⁺16].

**Indexing** [HCDM⁺12]. **India** [BC⁺11, CGB⁺10, GG⁺10]. **Indicator** [YT⁺12, Pari⁺16]. **Indirect** [ABS⁺12]. **Indistinguishability** [AS⁺16, BV⁺18, FMY⁺15, GHRH⁺14, GGH⁺16a]. **Indistinguishable** [LG⁺12]. Individual [LMB⁺12]. **INDOCRYPT** [BC⁺11, GG⁺10]. **Induced** [VDB⁺16]. induction [BBBP⁺13].

**Industrial** [GH⁺19, OSP⁺19]. **Industry** [AN⁺11b, QZL⁺16a, SXH⁺19, Chl⁺13c, LH⁺18, Men⁺13b, ZSMS⁺18]. **Infective** [GST⁺12]. **Inference** [Bro⁺11, DBPS⁺12, NC⁺12]. **Inferring** [BPSD⁺17, PTRV⁺18]. **Influence** [RSCX⁺18].

**Information** [AQD⁺12, ABCL⁺17, Bai⁺10, BF⁺11, CVM⁺14, CDGC⁺12, CBRZ⁺19, CGB⁺10, CST⁺17, CBL⁺13, Dew⁺11, DP⁺12, FHKP⁺17, FHS⁺13, HBC⁺19, HHH⁺13, IF⁺16, JHHΝ⁺12, LG⁺12, LW⁺11a, Low⁺12, MA⁺17, MAL⁺10, NTKG⁺17, SGC⁺14, STC⁺11, TWZ⁺11, WSS⁺12, XZZ⁺18, XHZ⁺19, Yan⁺10, Yek⁺10, ZZZ⁺15, ZHL⁺15, ZBPFP⁺18, AB⁺10a, Abe⁺10, AL⁺15, ASVE⁺13, BSS⁺11, BGP⁺17, CFG⁺17, DMWS⁺12, GLM⁺19, HPJ⁺19, KLI⁺3, LW⁺18, MKH⁺12, Mar⁺10b, SRB⁺12, WHZ⁺19, WW⁺13, Ano⁺19a, BYL⁺10, LH⁺10a].

**Information-Theoretic** [CVM⁺14, WSS⁺12, CDGC⁺12, GLM⁺19]. **Information-theoretical** [ZZ⁺15, KL⁺13]. **InfraStructs** [WW⁺13]. **Infrastructure** [GM⁺13, PN⁺10, GAI⁺18, JAE⁺10, SA⁺12].

**infrastructures** [FHM⁺10]. ingenious [Mac⁺12]. **Inhibiting** [GAS⁺16]. Initial [PAS⁺13b]. initialization [AN⁺15]. Injected [LL⁺12]. **Injecting** [BBGT⁺12, LZX⁺19]. Injection [ABS⁺12, AR⁺12, DDR⁺16, JWJ⁺17, PYM⁺13, YGD⁺17]. **Injections** [LC⁺17]. **Ink** [Keb⁺15, Mac⁺14]. Inner [ADM⁺12, LG⁺18, OT⁺12, YKN⁺12, DDM⁺17]. **Inner-Product** [YKNS⁺12].

**innovations** [JSM⁺18]. Input [GG⁺17, XXZ⁺12, PBC⁺14]. **Inputs** [GG⁺17]. **INSCRYPT** [BYL⁺10].


**Inspirations** [SP⁺19]. **Instability** [LM⁺12]. **Installment** [SYC⁺17]. instance [BRT⁺12].

**Instances** [HN⁺10]. instead [AGH⁺17]. **Institute** [Wel⁺16]. **Instruction** [ARP⁺12, AB⁺15, EKP⁺13, HZS⁺19, BVIB⁺12, SF⁺12]. **Instruction-Cache** [AB⁺15].

**Instruction-Level** [HZS⁺19]. **Instructions** [FHLD⁺19]. **Insulated** [FZ⁺13, LH⁺11c, HL⁺11, RG⁺10, RWZ⁺13, WW⁺13]. **Integer** [Con⁺12, LLY⁺18, AM⁺12, MM⁺13, Mes⁺15, MN⁺14, PC⁺14]. **Integers** [CN⁺12, CNT⁺12].

**Integral** [AY⁺14b, LW⁺12, ZSW⁺12, SM⁺11, SNM⁺14, SH⁺11]. **Integrated** [LY⁺15, MU⁺12, AL⁺15, SY⁺12]. **Integrating** [CFZ⁺10, LH⁺12, Od⁺12, AE⁺17, HLS⁺14, MCL⁺19].

**Integration** [AQD⁺12, Kar⁺12, ZYW⁺13]. **Integrity** [BCP⁺14a, BCK⁺17, DGF⁺18, FMY⁺15, MV⁺16a, PHI⁺12, SB⁺18, VBC⁺15, ED⁺17, SW⁺16, YXA⁺16, YNX⁺16]. **Intel** [Arm⁺19, MZLS⁺18, SF⁺12]. **Intelligence** [Dew⁺11, Ald⁺11, Bud⁺16, GW⁺14, Han⁺12, Maf⁺16].

**Intelligent** [AM⁺12, IEE⁺11a, SAJL⁺16, Wat⁺14a, HLS⁺14, MKH⁺12, SMS⁺16, ZCZ⁺19]. intensify...
[HL12]. Inter
[LBR12, OMPSPPL+19, BGAD12, SCKH10, SA15, SHBC19, YWK+10a]. Inter-domain
[LBR12, BGAD12, SCKH10, YWK+10a]. Inter-Pulse [OMPSPPL+19]. inter-router 
[SA15]. inter-session [SHBC19].

Inter-action [HSUS11, BBDP16, HK17]. Interactive [CFJH14, DF11, FSGW11, BCI+13, LH11a, Pas13a, PPR+12, Yan14].
Interceptor [Cho10]. Intercepts [Don14]. Intercloud [DCA19]. Interest [Sch19]. Interface [WBA17]. interference 
[BBCL19]. intermittent [CL16]. International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FBM12, GLIC10, JY14, LCK11, LW11a, LTY11, MV12, P1J12, Sen10, Wat10, Yau10, Yan11, AB10a, Abe10, Ano11a, BYL10, BL10, Gii10, GG10, HWG10, LH10a, IE11a].

Internet [Ano13d, LFGCGR14, TW14, AAC+16, Ano13b, BCHL19, Bel18b, CLF+17, CW12b, CEL+19, DRS16, DG15, Gel13, GMDR19, Ham19, HZL18, JKAU19, JTT+16, LNK+18b, LGH+17, LSG16, MJGS12, MJS13, MCF17, NLLJ12, NL15, Orm16, PLGMcD18, SB17, SXX+19, SS19, SYW17, SYC+17, SKEG14, VWC19, WCH18, XLC+19, YCT15, ZSY19]. Internet-Draft [MCF17]. Internetworking [SAAB10].

interoperability [HWK+15]. interplay [JW14]. Interpolation [JTZ+16, KU14].

Interpretation [MZ17b]. Interpretation-Based [MZ17b].

Interpreters [MS18]. intersection [LZY+16]. Interval [PPR+12, Cra11, DTZZ12, LWY12, MO14].
Interval-based [PPR+12, Cra11]. Intervals [OMPSPPL+19]. Intra [HF14b].

Intra-Masking [HF14b]. Intrinsic [HRK18, SN10, NS10, RCW15].

Intrinsically [SRK+17]. Introducing [Fay16]. Introduction
[BCHL19, BdD19, DK15, G13, JSK+17, LLK18, Low12, Mei10, Men13a, Sch15a, SOG15, Sta11b, CM13, Buc10, Led16, Sch15a, Fui10, Mur10]. Intrusion
[NSMS14, SAJL16, SBV14, YKC+12]. Intrusion-resilient [YKC+12]. Intrusive
[AARJ12, MFH13]. Invariance
[yWpNyL11]. Invariant [CSW12, NKWF14, RS16, WYW+13, YWNW15, GZHD12, LCM11]. Invariants
[NKWF14, CDSLY14, KI10, MZ17a, TTL13].

Invention [Orm16]. invents [Ant14]. Inverse [JS18, RMERM19]. inversion [KHHH14]. Invert [ZW15]. Inverted
[ZXYL16]. Invertible [SLY+16, UUN13]. Investigating [SP+13]. Investigations

InvisiMem [AN17]. INVISIONS [AARJ12]. Invited [SS19]. Invitation [Bru12].

Involving [HLCL11]. IoT
[AATM18, APMCR13, CCM17, CS18, FQZF18, FMC19, GAI+18, HHSB18, Hod19, LSQ15, LZZ+19, MNP19, NV17+17, SSA18, SGC16, SIJK18, TODQ18, TG17, WCFW18, WXK+17, XYML19, YWJ+19, YFT17, YFT18, YTH17, ZCWS15, ZLY+19].

IoT-Based [YTH17, ZLY+19].

IoT-Enabled [SGC16]. IoT-FBAC
[YWJ+19]. IoTs [SAJL16, ZSW+18a]. IP
[AGLW16, AZH11, PJ18, PA10, RS17, SP15a, TJJF12, WBC+10]. IP-SEC [PA10].

IPE [ZM16]. iPhone [Wu16]. IPs
[GSFT16, NDG+17]. IPv6 [KP12]. IRC
[HB13]. IRC-based [HB13]. IRIW

ISO [BCM12, BCM13, TS16a, WWBC14]. ISO/IEC [BCM12, BCM13]. Isogenies
[Y+17]. Isogeny
[BF19, KAK18, LAL17, LNL+19, ZSP+19]. Isogeny-Based [BF19, KAK18, ZSP+19].

Isolated [YS15, KKI+16]. Isolating
[LG12]. ISSAC [Wat10]. Issue
[Ano13d, Ano16a, Ano16b, Ano19a,
Nos11, Nos14, RR16, RG10]. key
[RWZ13, RPSL10, SES+16, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZZ15, SA15, SGP+17, SvT10, TK19, TCS14, TLL12, Tso13, TTKH14, VV19, VN17, WWYZ11, WDKV19, WMZ12a, WMZ12b, WT10a, WTT12, WQZ+13, WXK+17, WX12, WX13, XCL13, XXCY19, YXML19, XLC+19, XMBD13, XHM14, YT11b, YC12, Yan14, YZZ+14, YHHS16, YZL+18, YN19, YLZ+16, ZCZQ19, ZPZ+16, ZWQ+11, ZZ11, ZHL+11, ZCC15, ZTT16, ZGL+18, ZXW+18, ZXWA18, ZWS+18, ZCZ+19, ZHT16, CLW16, OHJ10, XJR+17]. Key-Aggregate
[CCT+14, PSM17, GLB+18, CLW16].
Key-Agreement
[WSS12, APK+18].
Key-Alternating
[BKLS12].
Key-Based
[Xio12].
key-correlations
[Sar14].
key-delegation
[JSMG18].
key-disclosure
[ZZC17].
Key-Establishment
[BCO13].
Key-Extraction
[GPT14].
key-hash
[KKG14].
Key-Insulated
[FZT13, LH11c, HL11, RG10, RWZ13, WWYZ11].
Key-Length
[GT12].
Key-Length-Based
[PNRC17].
Key-Policy
[GZZ+13, GSW+16, HSMY12, RVH+16].
Keyed
[KE19, MMS17b, YHHM18].
Keyed-Function
[MMS17b]. Keying
[TW14, BCPV11].
Keyless
[PDMR12, ZWX+18].
keyrings
[MBB11].
Keys
[ASN11, BF12, Bro17, CC10, HDWH12, LSGQ19, MS16, PSM17, TW14, ZMW16, CMG+18, HL14, IK15, LLY18, LH13, LW10, LLL+18, RWZ13]. keystream
[SM11].
Keystroke
[AaBT16, SP13, BGE+18, CTL12, GEAHRI11, LTC+15a, MCRB19].
Keyword
[CWL+14, Chet15, HCDM12, HLH19, LSQL18, WDCL18, XWSW16, XJWW13, ZXYL16, BL11, CLH+16, FSGW12, GZS+18, LKX+14, OSSK16, SY15b, WHY+12, WXLY16, XWY+18, XTZ+19, XLC+19, YZCT17].
Keywords
[CWWL12, ZZ11].
KGC
[YT11a].
kid
[Tan17a].
Kind
[WJ19].
King
[ABJ13].
kiss
[HU15, KYEV+18, Ros11].
KLEIN
[GNL12].
Klepto
[XY18].
Knapsacks
[Dun12a].
Knaves
[CEL19, MMS17b].
Keystroke
[AaBT16, SP13, BGE+18, CTL12, GEAHRI11, LTC+15a, MCRB19].
Keyword
[CWL+14, Chet15, HCDM12, HLH19, LSQL18, WDCL18, XWSW16, XJWW13, ZXYL16, BL11, CLH+16, FSGW12, GZS+18, LKX+14, OSSK16, SY15b, WHY+12, WXLY16, XWY+18, XTZ+19, XLC+19, YZCT17].
Keywords
[CWWL12, ZZ11].
KGC
[YT11a].
kid
[Tan17a].
Kind
[WJ19].
King
[ABJ13].
kiss
[HU15, KYEV+18, Ros11].
KLEIN
[GNL12].
Klepto
[XY18].
Knapsacks
[Dun12a].
Knaves
[CEL+19].
Knebl
[Mur10].
Knights
[CEL19].
knocking
[KSB+17].
Know
[BC14, CAC14, XTK10].
Knowledge
[CLP13a, COP+14, GJO+13, GOS12, IW14, MX13, MBC+18, MT12, OOR+14, Pan14, Ano11a, KPP16, LLM+19, MDHM18].
Known
[DWWZ12, JLL12, SEHK12].
Known-Key
[DWWZ12, JLL12, SEHK12].
Koblitz
[BJ10b].
Kode
[NN15].
Korea
[LH10a, LW11a].
KP
[FJHJ12, HQZH14].
KP-ABE
[FJHJ12, HQZH14].
Kristie
[Keb15].
Kryptografie
[Blo12], Kryptographie
[Blo12].
Kuala
[HWG10].
Kurtosis
[YYO15].

L
[Low12, Xic12].
LAAP
[Gop19].
Labs
[Ven14].
Labyrinth
[Fox13].
Lacks
[BBG13].
LAKE
[BCO13].
Land
[Sch18].
Landis
[BBB16b].
language
[Ksi12].
Languages
[MX13, Wat12].
LANs
[FLH13].
Lapin
[HKL+12].
Laptop
[GPT14].
Large
[AN12, DM15, FNWL18, JLS12, JKHtY12, KCR11, KU12, LW16, LQD+16, MC11, SP13, dCCSB+16, EEAZ13, FXP12, GSN+16, LFZ+17, LBOX12, SR10, ZZKA17, ZVH14].
Large-Scale
[DM15, JKHtY12, LQD+16, dCCSB+16, FXP12, GSN+16, SR10, ZZKA17, ZVH14].
LARK
[DS11].
Laser
[DDR+16, FNP+15, Lidd12].
Last
[Hof15, Hof16].
Latency
[AYS15, BCG+12b].
Latency-Optimized
[AYS15].
lateral
[SCY15].
Latest
[Ber17].
Latin
[AB10a].
LatinCrypt
[AB10a].
Lattice
[ADM12, Ano11b, AYS15, BSJ15, EM12, FGM10, IFO+15, HKR+18, LPO+17, MLO17, NDR+19, PG12, AAT16, Dra16, LLM+19].
Lattice-Based
[ADM12, Ano11b, AYS15, BSJ15, EM12,
HPO+15, HKR+18, LPO+17, MLO17, NDR+19, PG12, AAT16, LLM+19.

Lattices [Boy13, LYX+19, Lai17, TH16, XXZ12, ZQQ15, Kre13, Tia15, XWZ16, yYqWqZC13].)

Leakage-Resilient [IL15, TTH15].

Leakage-Resilience [LTZY16, Pan14, XZY16, ZZM14, ZCC15].

Leakage-Free [GV14a, GLL]

ZBPF18, CQX18, DLZ16a, DMWS12, learning-based [WS14].

GJ13, KMG17, Sch12a, WS14, BCV12.]

Left-to-right [BBG+13].

Leaves [Boy13, LYX+19, Lai17, TH16, XXZ12, ZQQ15, Kre13, Tia15, XWZ16, yYqWqZC13].

launch [Zet14].

Laurent [Ano15b].

Law [Bla12, SR14, Wu16, AOT13].

Layer [LHM+15, PRGBSA19, ZXY16, HQY+16, LKL13, ZHY+17].

Layered [Bel19, BS14, GRL12, WWL+14, JCHS16, Tan18, ZC12].

LBlock [KDH13, MNP12].

LDGM [BBC+13].

Lead [Arm19].

leader [KV12, KMP].

Learned [KMP+11, WL11].

Learning [CTC+15, KPC+11, KRJ12, SPG+19, Yon11, GJ13, KMG17, Sch12a, WS14, BCV12].

learning-based [WS14].

Leave [GA19, CMG+18].

Lecture [Hel17].

LED [IS12, JKP12, MRTV12].

Ledger [Mu16].

Leeds [vDKS11].

Left [BBG+17].

Left-to-right [BBG+17].

Legacy [CS12, Sni11b, CGH17].

Legal [ZTSR12].

LeGall [Ara13].

Legislation [PH12b].

Lemonade [DFKC17].

Lemons [DFKC17].

Length [AS17, GT2, Gir15, PDNH15, PNRC17, Zha12].

Length-Doubling [Zha12].

lens [PHN+12].

LEO [RM18].

LESPP [WLZ+16].

Less [TKR14, GM13, Kan16].

Lessons [KMP+11, TGC16, WL11, CMG+18].

Level [AW17, Ano15a, BBL19, BRPB13, BKJP12, CCW+10, DA10, Gl12, HZS+19, HS18, JWJ+17, KPC+16, KGP12, MV16a, XZL+19, ZLDC15, ABBD13, MEFO12, RS17, UUN13, VS11, YT11a, Bai12].

Leveled [BGV14].

leveling [LY15].

Levels [HLCL11, LRW17].

Leveraging [DM+16, GMDR19, HCM11, MvO11, SKGY14].

Lewis [Mar10a].

Lexicographic [ZAC17].

LFSR [HLC12, MRT10, WGD18].

LFSRs [QGL13].

Liability [Bra13].

Liars [Sch12b].

Libgcrypt [DK16b, Bro17, Win17].

Libra [GMV17].

Library [ACZ16, Bee17, BLS12, FLW12, KRH18].

Life [AK13, SCSM18, McK10, McK11, War11].

Lifecycle [Tan15a].

Lift [ZTSR12].

Light [WCF18, WWBC14, XWZ+18, XXCY19, XHM14, YCT15, ZSW+18a].

Light-Weight [SWF+19].

lightning [Ran10].

Lightweight [AMKA17, AARJ12, BCL19, BSS+13, BM11, CCGPD12, CWP12, CCF17, DS11, ESS12, EKP] .

light [BM11, CL11, DA18, FLW12, KPC].

Lessons [AS16, GV14a, KS12].

Limits [DR12].

Limited [DT17].

Limited-Use [DFKC17].

Limits [AS16, GV14a, KS12].

Lindell

M [Orm16, HvS12]. M-Identity [HvS12]. MA [ACM10]. MAC [Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN16]. MacGuffin [LGL+12]. Machine [AGHP14, Ano16c, CHS15, Sch12a,
ABBD13, GJ13, Gup15, LLZ+16, LHA+16, QMC17, RY10, TTL10, War11, WS14.

Machine-generated [AGH14].
machine-to-machine [QMC17]. Machines [Ber16a, HB17, BBDL+17, KSU13, PWW10].
Macrakis [Keb15]. MacWilliams [OS11].
Made [Orn16, Sma16]. magic [PHN+12].
Magnetic [VDB+16]. Magnifying [DKL+16]. Mail [BTW15].
Main [AMH+16, LY15, ZHZ+19, CS11, HHAW19]. Maintaining [WP15].
Make [Ayu12].
makes [Kem11]. Making [BG14, dCCSB+16, Gel13, LA10, ZDW+16].
Malaysia [HWG10]. Malicious [AAE+14, ARWK19, BL15, TM18, VGOA15, BK12b, OSNZ19, WTT12]. malleability [KTT12]. Malleable [CKLM13, DPW18, MSA12, CG14a, FVMN14, LP11, MSA13, OOR+14, Pas13a].
Mallory [FHM+12]. Malware [ATS15, GAF+15, JC13, GOO12, Yaa19]. man [And13, Bat10, Kap13, Moo14].
Management [ASM12, ABB19a, BD15, Bar16, BS13b, CCFS12, CSL+14, GOPB12, KP12, KKA14, Lop15b, MFKF16, BN10, TMGP13, Vle12, YXX+12, YSS14, ZJ11, ZTSR12, BMBS10, BBG19, BB16b, CFL13, Cha13b, dCCSM+12, dCCSB+16, Din10, KH18, MLMSMG12, MGP10, PLCGS11, Sch11, SK18, SR10, SA15, SWX+16, THA+13, WSC14, WDKV19, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, A015b]. Manager [KKA15, Kim16]. Managing [MD15, BC18]. MANET [KRU16].
Manuscript [An016d]. Many [CCL+19, LB13, HRS13, ZQWZ10].
March [Ano10, Cra12, DDS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, WZM12a].
Matching [Lin15, RCBK19, Tan12a, DA18, LH13, MR14c, MHT+13, PPT15, SS17, SM10c, YZL+18]. MathCW [Bec17].
Mathematical [Bec17, FGPG14, Ham17, IBM13a, Mei10, Sch15a, Wes16, KM14, OO10, Sta11b]. Mathematical-Function [Bec17].
Mathematician [A017e]. Mathematicians [A011]. Mathematics [A017b, A012, Led16, Sch15a, Ter11, CM13, Kra12, PHW10, Wes16].
MATLAB [TRD11]. Matrices [AMVZ12, BNA15, AKG13, EFS10]. Matrix [BFMT16, IAD10, KKK+18, LYY+18, SK12a, TDT13, Ye10, Cha13b, LLM+19, TK14].
matrix-vector [LLM+19]. Matter [Rau15, SS12a, DKA+14]. Max [And13].
Maximizing [DBPS12]. Maxims [Kob10].
McEliece [DN12, GVI4b, MBR15, MT12, MG15, OTD10, SW+10, VOG15]. McOE [FFI12]. MDPC [GAB19, HC17, VOG15].
ME [XHH12]. Mean [SZH19, TTL10].
Meaningful [LTC+15b, SA16a]. Means [KRDH13, AMHJ10, Kam16, Pal16].
Measure [DDD14]. Measure-independent [DDD14]. measurement [QLZ19, VGN14].
Measurements [DTE17].
Mechanical [RSCX18, Mat19]. Mechanism [ABB19a, KD12b, LL15, LLY+18, Lin15, PKTK12, Saa12a, SMOP15, ZHS+19, CL11, FXP12, KKJ+16, MCRB19, NXS10, PLPW13, PSJ+13, WB12, YXA+16, ZWM14].
Mechanisms [CBO+18, GPR+19, JWNS19, JSK+17, SGG18, FHH10a, KSA16, ZHS+19, CL11, FXP12, KKJ+16, MCRB19, NXS10, PLPW13, PSJ+13, WB12, YXA+16, ZWM14].
Mechanisms [CBO+18, GPR+19, JWNS19, JSK+17, SGG18, FHH10a, KSA16, ZHS+19, CL11, FXP12, KKJ+16, MCRB19, NXS10, PLPW13, PSJ+13, WB12, YXA+16, ZWM14].
Mechanisms [CBO+18, GPR+19, JWNS19, JSK+17, SGG18, FHH10a, KSA16, ZHS+19, CL11, FXP12, KKJ+16, MCRB19, NXS10, PLPW13, PSJ+13, WB12, YXA+16, ZWM14].
Multi-Party [ASS15, BBEPT14, BRT12, CWL+14, Chi12, GVW12, GJZ17, HIS11, HC12, HRS16, IG11, KTT12, KMO14, LyWSZ10, MZHY15, MEF012, MLBL12, NGAuHQ16, OKG+12, OSSK16, PSSK19, SK12b, TWZ+12, TYM+17, TFS19, Wan14, WOLP15, XWSW16, YWW10, Ye14, ZC13, ZQQ15, ZLDC15, BOP14, BGG+13, CPPT18, CLP+13b, CFVP16, CJXX19, CI2b, CLHJ13, CW14a, C15b, DRN16, DFJ+17, FHZW18, GMOCGCM15, GPvCDRO12, GZS+18, GBC19, HL14, HL11, HCC11, HLC12, ISC+16, JCHS16, KMI11, LXMW12, LXX+14, LCT+14, LH13, LW12, Mas17, QMC17, SCFB15, SLL+19, SCY15, SWW+16, SSS11, TLL12, WDL13, WXK+17, XLWZ16, XHH14, YCC16, YN19, ZZKA17. multi-agent [GPvCDRO12]. multi-authenticated [HL11].

Multi-Authority [ZQQ15, SLL+19].

Multi-Biometric [NGAuHQ16, MLBL12].

Multi-bit [TWZ+12]. multi-channel [CPPT18]. Multi-ciphertext [KTT12].

Multi-cloud [CFVP16, SWW+16].

multi-criteria [ZZKA17].

multi-crypto-processor [BGG+13].

Multi-domain [IG11, QMC17].

Multi-Factor [PSSK19, HC12, CLP+13b, DRN16].

multi-flow [LW12]. multi-gateway [WXK+17].

multi-generation [CJXX19].


Multi-precision [SK12b].


Multi-Receiver [TFS19, Wan14, Chi12].

Multi-sawtooth [Ye14]. multi-scale [CI2b]. multi-scroll [GMOCGCM15].

Multi-Secret [HIS11, ZC13, CW14a, HCC11, HLC12].

Multi-Segment [WOLP15]. multi-server [CLHJ13, FHZW18, HL14, ISC+16, LXMW12, LH13, SSS11, TLL12, XHM14, YN19]. Multi-Signature [ASS15].


Multicast [CC14, BAL10, HGWY11, LTT10, NAACL12]. Multicoupon [HIDFPC15]. Multidevice [DPCM16].

Multidimension [AJA16].

Multidimensional [Her10, WWB14, HMC12]. Multi-factor [MMY12, KS19]. Multigigabit [PP10b].

multihop [ADF12]. Multilayer [NXH+17].

Multilevel [FMS12b, IF14a, NSA15, SERF12].


Multimodal [GM16, SAR18a, AHM+18, ATI+10, MHT+13]. MultiObjective [ZAC17].

Multipartite [HR13].

Multiparty [BDYOZ11, CCL+13, Fri10b, ADMM16, BHH19, LDDAM12]. Multipath [HL12, OPHC16].

Multiple [DSB15, DUN12a, FR16, KBL11, LTC+15b, LQD+16, NDC+13, SY14, SC10, SKS+18, Sta12, WWL+14, XNP+18, GJJ18, GZS+18, LWG10, LTC+15a, LXC17, M14, RWZ13, TKHK14].

Multiple-Layered [WWL+14].

Multiple-Parameter [NDC+13].

multiple-precision [MN14].

Multiple-Secret [SC10]. Multiplication [AK14, CMO+16, HVL17, LNL+19, SK12b, YTS12, AAT16, SKH15, SF12].

Multiplicative [RMERM19, KHH14].


Offline/online [LJK+17]. Offloading [JHCC14]. Offs [ASBD16, BS14, GPR+19, SR10]. offsets [YQH12]. Okamoto [TF19]. Old [Che17, GY13]. On-Chip [LGLK17, BAB+13]. On-demand [KKJ+16]. On-Line [FLL12]. On-siteDriverID [SGGR+16]. On-the-fly [PS14]. One [CBJX19, CPS16, DSMM14, DCAT12, FD11, HP14, HG12, Mat14, NA10a, Par18, PC16, TYM+17, XW12, XYXYX11, XZLW15, Yon12, BM15, FFHH10a, GPLZ13, HRV10, LP11, LW10, LW13b, LML+13, RK11, Rus15, SM10a, SPK17, TCS14, ZQWZ10].


Optimizations [ZAG19]. Optimized [ARH+18a, AYSJ15, EKB+16, GAB19, HGT15, LNL+19, MBF+13, MBR15]. Optimizing [DWZ18, ZS18]. Optimum [oba11, YFF12]. Optional [PC16].

OR-Proof [FSX12c]. Oracle [CBJX19, GLM+16, HKT11]. Oracles [FZT14, FSX12a, GSW+16, XQL11, YS12, YKC+11, YLA+13, ZMY18, LLY15, RG10, SYL13, WWY11, YFK+12]. ORAM [RM18]. Order [DCA18, KS12, LFX+18, LWKP12, PR12, YKK11, ZDL12, ZSW+12, ZBF18, AKY13, BKR19, LW13a, LCV+16, LWKP14, gWpNyY+14, YL11]. Order-Hiding [DCA18].


Output [DK16b, G12, NR12, PBCC14]. Outputs [SNCK18]. Outright [AJB13].

output [XTZ+19]. Outsourceable [QZZ18]. Outsourced [FRS+16, LLC+15, LHL+18, LQD+16, PD14, RZD+16, XLP+18, YMA17, YMC+17, DFJ+10, FS18, HKA19, HMC12, LCL+15, LCV+16, LJW+17, QZDJ16, ZML17, ZSW+18b]. Outsourcing [DR12, LILC12, LHL+14, LJWY18, OSNZ19, SKB+17, SWV+16, XMY+17].

outwitted [Car11, Fag17]. Over-the-Air [VOGB18, ZXS+18]. Overcoming [BKKV10, DY13]. Oversead [AWSS17, BAI0, CCW+10, GHS12, RM18, ZJ11, RS17]. Overlay [CHS15, MJS13].

Oversight [Bla16]. overview [AA14, BDP+12]. own [Zha15a]. owner [ZZC17]. owners [GZS+18]. Ownership [FMTR12, RR11, HWYW14, KH18].

Oxford [Che11, Wes16]. Ozarow [ADG16].

P [ZSH+19]. P-256 [ZSH+19]. P2P [dCCSM+12]. P3 [HK18]. Packet [FGR+17, JTT+16, VPK17, XHC+12, AASSA18, MV16b, PJ18, PX13, XWN12].

Packets [Bi17]. Pads [NA10a, BM15].


Pairing-Based [Bon12, CST+17, KZG10, LGPRH14, Men13a, MST18, YTS12, Con12, KSH18].

Pairing-Free [WCH19, LL16a, Y11b].


[BLM18, VM14, BD15, Bar16, BBCL19].
Partial [CBJX19, DLV16, GFBF12, LG12, SGS14, TK19, WDDW12, Bax14]. Partially [KB10, XZP19, participants [KSU13, WTT12], participating [CH10].
particle [ZSMS18]. Parties [YCR16, Kup13]. Partitioned [FVS17].
Passive [DHB16, GSC17, SB17, BM13, uHAN18, LWL11, MK12a, passport [LZJX10]. Password [ASBdS16, BRT12, CLY14, DM15, DGMT19, FVS17, FD11, GAS16, HCL14, LWS10, WZM12a, WZM12b].
Password-Authenticated [HCL14, YRT16, ZHH16, LWS10, WZM12a, WZM12b]. Password-Based [BRT12, CLY14, FVS17, WgMW12, DGMT19, DSCS12, FA14a, FIO15, IOV18, TKHK14]. Password-Only [LYL13, KMTG12].
Privacy
[AKM+11, AKKY17, ABCL17, Ano19a, ALL+18, ACM12, ABHC+16, BN14, BCF16, BA18, BJL16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DCA19, DTE17, ESS15, FGR+17, Fei19, GZZ+13, HSMY12, HBCC13, HXC+11, HK18, JN12, JLG+19, KM10b, KKK+18, KLC17, KS12, KH18, LMGC17, LSBN14, LLG15, LXY15, LQD+16, MYYR13, MJS+19, MV18, MTM18, NSMS14, PD14, PSS+13, PPRT12, PSD15, Pet12, RVH+16, RSR+19, RCP+18, RWLL14, RBHP15, SS17, Set16, SZDL14, SZTT18, SOF12, TMLS12, TMGP13, WPZM16, WZCC18, WMYR16, YMM13, Yon11, ZHW15, ZHY16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, ALL+18, JLX+19, KH18, ZOSZ17, APMCR13, BBDP16, BLV17, FMA+18, GAI+18, HSH11, HKA19, LHL+18, LSQ15, PZBF18, QLZ19, RR16, SY+17, SMS+16, Tan12b, ZWY+13].

Private [BL14, BM13, Jia14a, LSQ19, MV19, QZL+16b, RCBK19, Sia12, WCL+18, Yek10, ZMW16, ZXYL16, BHH19, HIJM+11, HYF18, IK15, WR15].

Private-Key [MV19].

Privacy-Aware [BCF16, ARL13, MGP10].

Privacy-Based [BS13b].

Privacy-Enhanced [DTE17, ACK+10, YQOL17].

Privacy-Friendly [KCC17, ACM12].

Privacy-Preservation [LLG15].

Privacy-Preserved [SWW+17].

Privacy-Preserving [ABCL17, BJL16, BJL12, CWL+14, GZZ+13, HSMY12, KKK+18, LMGC17, LXY15, LQD+16, MJS+19, MTM18, NSMS14, PD14, PPRT12, Pet12, RVH+16, RSR+19, RBHP15, SZDL14, SZTT18, WPZM16, WZCC18, ZHW16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, ALL+18, JLX+19, KH18, ZOSZ17, APMCR13, BBDP16, BLV17, FMA+18, GAI+18, HSH11, HKA19, LHL+18, LSQ15, PZBF18, QLZ19, RR16, SY+17, SMS+16, Tan12b, ZWY+13].

Probabilistically [IW14].

Probability [DF11, HLC16].

Probability-based [HLC16].

Probably [MMS17b].

Problem [CLL16, GKS17, Hor19, LLG16, NA10b, TKM12, Mes15, MR14c, RH10, VM14].

Proactive [LLL10, WMYR16].

Processing [JGP+18, SAKM16, SZHY19, TMKZ13, VKP17, BKV13, HK18, LXY15, MS13b, PRZB12, WS14].

Productivity [Tay19].

Productive [ADM12, CCM+15, OT12, YKNS12, Cha13b, DDM17, YI17].

Products [LG+18, RS10].

Professional [STC11].

Profiles [BCF16].
Proving [Sar14, AGH+17]. Proxim... [ARL13]. Proximity [IW14, ARL13, Alp18]. proximity-based [ARL13]. Proxy [ASS15, GSW+16, GJ15, GJZ17, GZXA19, HWGY11, HZX15, KP12, LSLW15, LAL+15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WC12, WY10, WYML16, XJW+16, YMWS11, YCM+13, BGP+17, CLH+16, FSGW11, FSGW12, GI12, HWDL16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, LL16b, QMW17, SLZ12, SKB+17, Tia15, WHY+12, Wan18, WLS14, XWXC14, YZCT17, ZLY10, ZDW+16].

Proxy-invisible [SYL13]. Ps [HDWH12]. Pseudo [NN12, XYXYX11, CFY+10, KM10a, MG15, PLSvdLE10, SH11, SM11, XSWC10, Zim10].


Public [ZTL15]. Publicly [NMP+13, SZQ+17, YNR12a]. Publish [BGP+17, DLZ+16b, OFMR16, PRSV17, SLI11, TKR14, YSM14].

Publish/Subscribe [DLZ+16b, OFMR16, PRSV17, TKR14, YSM14]. published [MYYR13]. Publisher [Full0, Murr0]. Publishing [VS15, LLL+17b]. Puebla [AB10a]. PUF [BDM18, CCKM16, CCM17, DSB16, KPKS12, KLM+12, MVV12, SRK+17, VDB+16]. PUF-Based [CCM17, KPKS12, MVV12, BDM18].

Pufferfish [KM14]. PUFKY [MVV12]. PUFs [HRK18, IGR+16, LZZ+19, USH19].


Q&A [AHN+18, Hof15, Hof16]. Q3 [Ven14].

Qaeda [Mac14, Keh15]. QC [YJ14, GAB19, HC17, VOG15]. QC-MDPC [HC17]. QIM [LJK17]. QIP [JJUW10].

QoP [Ksi12]. QoP-ML [Ksi12]. QS [AZPC14, HDWH12]. Quadratic [KRD13].
[MS12b]. Quality [CSW12, Ks12, NN12, YCM+13, SS11, WZLW13, WKH11].
Quantifying [CBRZ19]. Quantitative [BL15, MLBL12, MV16b, HM10].
Quantization [SSA13].
Quantization-Based [SSA13]. Quantum [Ano15d, Ano16c, Ano17e, BB14, Ber14, BCF+14, Che17, CCL+13, Feh10, FKS+13, Fol16, JEA+15, JL18, Kar12, KP10, LKK18, LHA+16, MS16, MSU13, Mos18, MKAAl7, NNA10, NA10b, NDR+19, QCX18, RK11, RSM15, RS18, Sas18, Sti11, TKM12, Umr15, WCL+18, Y+17, ZWS+18, ABB+14, BJ16, BCN19, CML16, Edw17, FRT13, GJMP15, IM14, JSE+16, LKP+16, LWP+18, LyWS10, LCW+16, Lid12, QD16, SK14, Svo14, VV19, YDH+15, vDS11, Sen10, Yan11].
Quantum-Oblivious-Key-Transfer-Based [WCL+18].
Queries [GYW+19, HGW12, LHKR10, PBC+17, ZZQ+19, BKV13, CHX13, DFJ+17, GLM+19, HMCK12, PRZH12, TKM13, WLI9].
Query [DCA18, GA11, PCGD14, WCL+18, XLP+18, AZPC14, BS13a, BKR19, CH11, ED17, HWW+15, JCS16, LKK+14, LW13a, XMY+17, YQOL17, ZZZC17, ZHT16].
Query-preserving [GA11]. Quest [Fox13]. Question [TWNC18, Cha13b]. Quisquater [Nac12]. Quorum [Kar12].

R [BS12, LJV11, PP10b, WW14].
R3579X [BDK11]. Rabbit [FSWF11].
Rabin [Ch13a].
Radial [H19, pNyWyY+14, CG12b].
Radio [KAHKB17, CJP12, CJP15, EA12, Kim11, LNYZ12, RGP12].
radio-frequency [CJP12, CJP15].
radix [GKCK11].
RAGuard [ZHS+19]. Rail [HF14b].

Random-Grid [KS15]. Randomization [Gas13].
Randomized [ARP12, GT12, HHR11, SR12b, BWA13].
Randomness [AY14a, Ana14, ABF12, ACM+17, BWL16, KMS19, MS10, MS16, DTZ12, FRT13, RY10, TC11].
Range [DCA18, BKR19, HMKC12, JCHS16].
range-query [BKR19].
Rank [SS10b, FES10]. Ranked [CWL+14, XWS16, GZS+18, LXX+14].
Ranking [ZDL12, AT10].
Ransomware [MPA+18]. Rapid [KPC+16]. rare [Sch11].
RASP [AZPC14]. RASP-QS [AZPC14].
Rate [LJK17, PPS12b, PCPK14].
Ratio [FHKP17].
Rational [CK18, Ku14, KOTY17, NIS12, TWZ11, ZC13].
Rationality [GLR10, GLR13]. RBAC [VN16].
RC4 [GCS+13, Loec15, Reec15, RS14, Sar14].
RC4-like [RS14].
Re [ABR12, GSW+16, GZX19, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PSV17, WY10, XJW+16, BGP+17, CFZ+10, CLH+16, CZ15b, FSGW11, FSGW12, FXP12, GH12, HWD16, HYF18, KKM+14, LMJC11, LCT+14, LFWS15, LL16a, Par18, SYL13, SLZ12, SKB+17, Tia15, WGTJ10, WHY+12, Wam18, WLS14, XXX15, YZCT17, ZD+16, LA+15].
Re-authentication
[LBR12, FXP12, LMJC11]. **Re-Encryption**

[RFID] [CJP15, AATM18, BL12, BSSV12, BM11, CCOPDMMG12, CCF17, CJ12, Cho14, DSS+12, FLL+14, Far14, FMTR12, GMSW14, GH15, GSN+16, GMSW14, GI12, GSN+16, GH15, GAI+18, HSH11, HDPC13, HZY+16, HCPLSB12, HCETPL+12, LNZ+13, LEW19, MOC12, Mic16, MK12a, PPH12, PLsvdLE10, QZL+16a, QZL+16b, SBS+12, SPLHC14, T17, WH17, WCF18, YFT18]. RFID-Enabled [YFT18, QZL+16a, QZL+16b]. RFID/NFC [Mic16]. RFID [CJP15, AATM18, BL12, BSSV12, BM11, CCOPDMMG12, CCF17, CJ12, Cho14, DSS+12, FLL+14, Far14, FMTR12, GMSW14, GH15, GSN+16, GH15, GAI+18, HSH11, HDPC13, HZY+16, HCPLSB12, HCETPL+12, LNZ+13, LEW19, MOC12, Mic16, MK12a, PPH12, PLsvdLE10, QZL+16a, QZL+16b, SBS+12, SPLHC14, T17, WH17, WCF18, YFT18]. Revocation [RSD18, TL12, WSA15]. Revocable [AEHS15, CD16, QZZ18, SE14, SE16, SZZ14, SZDL14, TCL15, TT12, Unr15, FLL+14, LDZW19, WLFX17, WTT12]. Revocability [WHHL16].

LDZW19, LL16a, LL16b, LWY12, MCN+18, MMS17c, MK12a, MSas13, NR17, Nos14, NMX15, OSNZ19, PZBF18, QMC17, QMW17, RPSL10, SGGCR+16, SM11, SYWX19, SCR19, SMS+16, Tan12b, TY16a.

**scheme** [TK14, TD14, TLL13, TLL12, UUN11, WWYZ11, WWYY11, yWpNyL11, WLH13, WDLZ13, WLZ+16, WLFX17, Wan18, WHZ+19, WDKV19, WZ11, WH11, WOLS12, WXK+17, XXH12, XWZW17, XX15, XTZ+19, XXY19, XMHD13, YWJ+19, YC11, YC11, YHHM18, YWK+10a, YCT15, YXD18, YQOL17, YMSH10, ZYL+10, ZLY10, ZXJ+14, ZYC17, ZPWY12, ZHH+17, ZHY1b, ZFH+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12]. **Schemes** [AAUC18, ABF12, BVS+13, BFM12, BBEPT14, BSJ15, CMLRHS13, CLND19, CGL12, Chu16, Des10b, FHKP17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZK14, MLCH10, MR14b, MMS17b, MBF18, MKRM10, MKASJ18, Ob11, PB12, PDNH15, PH12b, Sch10, Shi11, SKH17, SSU12, VSR12, WGF16, YNR12a, YNR12b, Yek10, YWZ+12, AGHP14, AN15, AHL+12, BKRK19, CDGC12, CJXX19, CHS11, CCG10, CTL13, DDD14, DD13, DZ14, FPB14G, FGMP12, FMA+18, HK19, HWDL16, HM10, KU11, LHYZ12, MM12, MA17, NZL+15, QXYW16, SES+16, Sar10a, Sar11, hSSZ15, SAR18b, WW14, YT11b, ZCL+12, ZCLL14, ZT14]. **Schneider** [Sev16]. **Scholarship** [SPG+19]. **Scholarship-for-Service** [SPG+19]. **Science** [Bow11, Gas13, IEE10, IEE11b, Ter11, Bia12, PHWM10, Pet11]. **scientists** [Goo12]. **Scientometric** [Pal15, Pal16]. **Scope** [Bai12]. **Score** [GCSDP11, HW19]. **scoring** [OSK16]. **Scrambling** [LLL17a]. **Screen** [SPW+16, CTL12, IAA+19]. **Script** [Rao10, Bax14]. **Scripting** [DSB15]. **scroll** [GMOGC15]. **SDB** [HWK+15]. **SDDO** [PL16]. **SDDO-based** [PL16]. **SDH** [GMS11]. **SDIVIP** [YNX+16]. **SDN** [KCC17]. **SDVS** [Wan10]. **SE** [LLLS13]. **SE-AKA** [LLLS13]. **seals** [MN10]. **Seam** [LC15]. **Seam-Carved** [LC15]. **Search** [AHN+18, CWL+14, Che15, DCA18, FRS+16, GT11, HCDM12, HLH19, LSQL18, TMC15, WCDL18, WW12, XWSW16, XJWW13, ZXY16, BTK15, BL11, CLH+16, FH13, FSGW12, GZS+18, HKA19, HH16, MRR+18, OSK16, PWS19, SY15b, WHY+12, WXLY16, WY19, XYW+18, XTZ+19, XLC+19, YXD18, YQOL17, ZZ11]. **Searchable** [BHJ14, CWWL12, CLW16, CGK11, FJH12, HKA19, PBC+17, PCY+17, XNK15, ZZQ+19, CLC+19, DLZ16a, DRD11, HQZH14, HTC17, JCHS16, LZC17, LLL+18, RPSL10, WXLY16, WCH18, YZCT17]. **Searches** [Sia12, WR15]. **searching** [GPN+12]. **Seattle** [LCK11, KCR11]. **Seberry** [AHS14]. **SEC** [PA10]. **Secondary** [RS11]. **Secrecy** [ABD+15, BKST18, BCN19, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCW15, TCS14]. **Secrecy-preserving** [TSH14]. **Secret** [ASN11, ASN12, ADH17, AYN1, Bai10, BBB+16a, BFM12, BBEPT14, BCN19, Bri11, CCM+15, CFR12, CCL+13, DR12, Dew11, EM12, EA11, FHPK17, FR16, Fok12, HYS11, HL10a, Has16, HZ+18, JLS12, KU14, KS18, KOTY17, KK12, KK13, KSSY12, KS15, LHF12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Ob11, PCKP14, QS18, SLL10, SC10, SS10c, SSU12, Sti15, TLW12, TWZ11, WKB16, WGF16, Wil8, XZY+12, XJR+17, YFF12, YWZ+12, ZC13, Ald11, AIM+19, ADG16, AKK+17, Ara13, BJ16, BEB+18, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEAZ13, EZ15, FHH10a, GEAH11, GJMP15, GLW13, HFI4a, HH15, Hea15, HBBRM+16, HCCC11, HLC12, KI11, KU11, LXLY12, LHI11a, LTI13,
LyWSZ10, LHYZ12, LEW19, Mas17, 
McK10, McKi11, McKi12, MBB11, O010, 
Par18, Pea11, Par11, QD16, Rus15. secret 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key 
[SB17, SA12, SAR18b, SM10c, TQL+14, 
TD14, UUN11, UUN13, WYL13, WZ11, 
WS12, WOLS12, Wu17, XW13, YC11, 
YCC16, YSC16, ZCL+12, ZZ15, ZPY12, 
LSC+15, Bai12]. secret-key
Semi-homomorphic [BDOZ11].

single-factor [GMMJ11].
SIP-based [ZTZ16], SIPF [SYC+17]. Site [DSB15, SS10c]. siteDriverID [SGGCR]. Singular [Sas12]. single-generation [GMMJ11]. single-factor [DSB15, SS10c]. siteDriverID [SGGCR, LTM].
HLV10, KGF10, LBOX12, SF12, YWT18. Soft [Her19, Jin10, TLF16, SS17]. Soft-Error [TLF16]. Softw [WZM12a]. Software [B15, Bee17, EWS14, KYEV+18, LRVW14, MRL+18, MV16a, Seo18, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GJ+12, HLV10, KHF10, LBOX12, SF12, YWT+12].
Software-Defined [KYE+18]. Solan [CGB+10]. solid [CRI+16]. Solution [Fra15, GSFT16, HLLK15, Kam13, NA10b, YFT17, YFT18, Cor14a, MDHM18, SVGE14, SAM+19]. Solutions [Ano19c, BCHL19, LLGJ16, BLV17, KAS15, MMP19, OMPSPL+19, WW14]. Solved [IBM13a].
Solving [Ano17c, BB10, Hod19, Bull10a]. Some [AD12, Ber12, Dur15, LWL10b, Mid10]. Somewhat [HTC17, KOS16, MBF18]. Song [Con12]. Soood [MWZ12]. SOEMANUK [PC16]. SOT [PAF18]. SOT-MRAM [PAF18].
Sound [COP+14, LSR13, Sav15]. Source [Bis17, FKO15, MBC15, RLL14, ABF+14, LZC17, PX13, Pow14].
Spanish [Pet11, SGGCR+16]. Sparse [AGW15, AAT16, BBC+13, PMG19]. SPARTA [MMS+17a]. SpartanRPC [CS14]. Spatial [AV12, CZF12, PDM12, CW14b, NZL+15]. Spatiotemporal [DMT12, CXX+19].
Special [BJCHA17, PPRT12, RSR+19].

Smart-Card-Based [HCL+14].
SmartEdge [JZU+19]. Smartphone [MDMJ17, uHAN+18, DL15]. Smartphones [Cor14b, GSVA18]. smartwatches [NM18].
smashed [Fag17]. Smith [Ano16g]. Smooth [XYXYX11, YC11, ZBR11]. SMS [KRM+10, LH11a, PsDo+13, RV+18].
SMSCrypto [PsDo+13]. SMSes [SNG+17]. Snake [BBDP16]. Snakes [PC16]. SNOW [PC16]. Snowden [Tox14]. SoC [HZS+19, GSC17]. Social [BPSD17, KTA12, NSA15, NRZQ15, PY+15, Rog16, SKGY14, SZZT18, WLY+15, WZCH19, ZW15, Zha15b, ZHL15, BDK11, HYF18, LCM+17, LZC17, MSM+18b, SNG+17, SSK+18, Smi15a, YZL+18, vdfWEG18]. Society [Sch15a, Sch12b]. Socio [NS12]. Socio-Rational [NS12]. SoD [VN16]. Soft [Her19, Jin10, TLF16, SS17]. Soft-Error [TLF16]. Softw [WZM12a]. Software [B15, Bee17, EWS14, KYEV+18, LRVW14, MRL+18, MV16a, Seo18, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GJ+12, HLV10, KHF10, LBOX12, SF12, YWT+12].
Software-Defined [KYE+18]. Solan [CGB+10]. solid [CRI+16]. Solution [Fra15, GSFT16, HLLK15, Kam13, NA10b, YFT17, YFT18, Cor14a, MDHM18, SVGE14, SAM+19]. Solutions [Ano19c, BCHL19, LLGJ16, BLV17, KAS15, MMP19, OMPSPL+19, WW14]. Solved [IBM13a].
Solving [Ano17c, BB10, Hod19, Bull10a]. Some [AD12, Ber12, Dur15, LWL10b, Mid10]. Somewhat [HTC17, KOS16, MBF18]. Song [Con12]. Soood [MWZ12]. SOEMANUK [PC16]. SOT [PAF18]. SOT-MRAM [PAF18].
Sound [COP+14, LSR13, Sav15]. Source [Bis17, FKO15, MBC15, RLL14, ABF+14, LZC17, PX13, Pow14].
Spanish [Pet11, SGGCR+16]. Sparse [AGW15, AAT16, BBC+13, PMG19]. SPARTA [MMS+17a]. SpartanRPC [CS14]. Spatial [AV12, CZF12, PDM12, CW14b, NZL+15]. Spatiotemporal [DMT12, CXX+19]. Special [BJCHA17, PPRT12, RSR+19].
Specific
[BD15, BDFK12, KME^+12, ARH^+18a].
Specification
[HZ^+19, Int^19, SK11, SD10].
Specifications
[BMP12]. SPECK
[LFW^+16, AMKA17, BSS^+13]. Spectrum
[KD12a, TWZ^+12, XNRG15, XNP^+18, KPB17, LWY12, MMSD13].
Spectrum-Based
[TWZ^+12, XNRG15].
Speech
[AGW15, LJK17, SAA15, YMA17].
Speed
[ARM15, GL12, HZ11, KP17, LTKP16, MSR^+17, BDL^+11, KL13].
Speeding
[RVRSCM12]. Speedup
[Che18]. speedy
[FG19]. SPEKS
[Che15]. spell
[Bha16]. Sphere
[Sti19]. SPHINCS
[BHH^+15]. Spies
[Has16, Keb15, Fag17, Mac14]. Spin
[Fyo19]. Spintronic
[IGR^+16]. Splicing
[YSC^+15].
Spline
[Tan12a]. Split
[CGL14a, XZY^+12].
Split-State
[CGL14a, XZY^+12]. Splittable
[CP13]. Splitting
[MV19]. SPN
[LCLW17].
Spoken
[WBC^+10]. Sponge
[ARH^+18a, BDPI11]. Sponge-specific
[ARH^+18a]. SPONGENT
[BKL^+13]. spongy
[RS14]. Spoof
[SP15a]. sotty
[O'S1]. Spread
[HGT15, KD12a, PSJ^+13, TWZ^+12, XNRG15, XNP^+18, LWY12, MMSD13].
spreadsheets
[LT13]. Springer
[Mei10, Mur10]. Springer-Verlag
[Mei10]. Springs
[IEE11b]. Spritz
[RS14]. Spy
[AHS13, FKOV15, Bha16, Goo12]. Spying
[VWC19]. SQL
[BS13a, Suc12]. Square
[ARH14]. Squashing
[GHI11a]. SRAM
[KLM^+12]. SSD
[LGLK17, MPA^+18]. SSH
[YSS14, Cri16, Lit14, Rau10, der10]. SSL
[BJR^+14, Dav11, FH^+12, GJ^+12, HEJ14, NPH^+14, PP11, Tay19]. SSL/TLS
[BJR^+14, Dav11, PP11]. SSL/TLS-based
[PP11]. SSO
[MML16]. St
[DDS12, Dan12, MNS11]. ST-Numbering
[MNS11]. stack
[JS18]. stage
[Mas17]. stakeholders
[RR16]. STAMP
[WPZM16]. Standard
[Ano12, Ano13a, App13, ABC^+17, BCM12, BV11, BV14, CT18, GJJ15, GJZ17, HZ15, LXY^+19, Loc15, MVVR12, OGK^+15, RSD19, SZZ14, TCI15, WMHL12, You12, ZC13, BCM13, HTC17, KI11, LZZ12, LL16b, Mas17, TS16a, WZM12a, WM12b, WWBC14, YC12, ZCL^+19, AEB17, MRM10, NdMWW16]. Standardization
[TRD11]. Standards
[BCM^+15, Che17, DHW^+13, NIS13]. State
[BVS^+13, BLM17, CG14a, CCL^+13, CHS15, Dew11, DP17, FHR14, LLK18, MKF^+16, Sen17, WGD18, XZY^+12, BBDL^+17, CK11, CGH17, Ham12, Mid10, QD16, Sir16]. Stateful
[BVS^+13, NTY12, VKPI17, VSR12]. Stateless
[BHH^+15, GM11, MKAA17, NTY12, VDO14, BBPD16, DAC12]. Stateless/Stateful
[NTY12]. statement
[NIS13]. Static
[DKMR15, IF16, Lan11, TLM13]. Station
[Smi11a]. stationary
[ZLDD12]. Statistical
[Boh10, Bro11, DBP12, HZ11, Hey17, LTKP16, OOR^+14, SP13, Sin15a, SA19]. Statistical-Attack
[SP13]. Statistics
[gWpNyY^+14]. Statutory
[PH12b]. Stealing
[RWZ12, VWC19]. Steathy
[BRPB13]. Steering
[HR13]. Steganalysis
[Bdh10, DA12, Fri12, JHNN12, KD12b, LJK17, LC15, SGP^+12, Tan12a, YLL^+12, Yi14, YPR17, LHM13, LSQ11a, LSQ11b, Sch12a]. Steganography-Resistant
[YPR17]. Steganalytic
[Ber18, YPR17]. Steganographic
[DA10, HHS^+15, LyW12, WP15, AGLW16, LL10, CAC14]. Steganography
[AGW15, BCG12a, CL11, FR16, FMS12b, Fr10a, Fr12, HZW^+14, JH010, LJK17, LLY^+12b, MAL10, PDM12, Pau10, SK12a, SR12b, TJJF12, WWL^+14, WYYZ12, YWW10, ZSA12, AOT13, BDK11, BHCdFR12, EEAZ13, GKCK11, LyWS10, LR13, LRW17, LWW^+10, Maz13, ...]

stolen [Bha16]. Stopping [Sav13a].

StopWatch [LGR14]. Storage [BCQ+13, CWL16, CTT+14, CLW16, GLG12, HSM14, HLC+18, JSCM17, Kip15, LCK11, LMD16, LWCI14, PBC+17, QLI17, SKH17, XNK15, ZDL12, ZVG16, AY14a, AKK+17, BP10, CFVP16, CFZ+10, CLH+16, CDF+10, CDL18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, SLL+19, Sar10a, SYY+17, SWW+16, SWW+17, XWL13, YSS+16, YZCT17, ZYC+17, ZVH14].


Strangeness [Ber12]. Strategic [Sch12c].

Strategies [DSSDW14, TJZF12, YCM+13, AZF+12, DRN16, WW17]. Strategy [LH12, NRZQ15, FLZ+12]. Stratix [SMOP15, SMOP15]. Stream [ABS+12, BMS12, CMLS15, DM18, DGFH18, DG12, DGIS12, DJG+15, GKB17, GCS+13, HZ11, Hey17, IOM12, KE19, KPC+16, Kla10, MD12b, MHC12, MS12b, NN12, PNRC17, WH18, WHN+12, ZH15, Die12, KM10a, LW11, LW13b, MRT10, OCG11, QGGL13, RS14].


Structured [PMZ12]. Structures [GTT11, HHH+13, LHKR10, LPL15, PB12, DDFR13, MHK14, Shy15, WS12, XWZ+18, ZZ15].

STT [VDB16]. Students [PP10a, SPG+19]. Study [AIF+19, Ano17c, DDR+16, MZLS18, SY15a, SPG+19, STC11, CCG10, EBFK13, MH15, SS17, VGN14].

Stuxnet [Zet14]. Style [GHPS12, GHPS13]. Stylistic [GA19]. stylometry [BAG12].

sub [GPLZ13]. sub-passwords [GPLZ13].

Subcommittee [Bla16]. Subgroup [CCL+19]. subliminal [LWZ10].

submarines [McG11]. Subrecursive [BBD19]. Subscribe [BGP+17, DLZ+16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Subset [BS14, RP12, ZT11]. subspaces [ZWM14]. Substituted [HD19].

Substitution [DA10, SGFCRM+18, FVK17].

substitution-transposition [FVK17].

Substring [MRR+18]. substructure [MRT10].

Succinct [BCT+13, CKLM13].

sufficient [TD14]. suitable [Jeo13, SKB+17].

Suite [MTM18, NACLR12]. Sumo [BS12].

Sums [SS12b], sun [Cer15]. super [BCND19, MZ17a]. super-activation [BCND19].

Superpoly [HIJ+19].

Supersingular [Lau17, LNL+19, Y+17].

Supervised [CCT+15]. Supply [QZY+16a, QZY+16b, YFT17, YSF+18, YFT18].

Surreptitiously [SFKR15]. Surveillance [BPR14a, BPR14b, GZH17, KLK+19, Lan10, Ano16b, Fei19]. Survey [AAUC18, ABHC+16, ABB+19b, BGN17, BCTPL16, BJIIP14, BJCH17, GMDR19, HPC10, KMY18, KSD+17, LGM+16, MR14b, MSM18a, MS10, NDR+19, NV10, OFMR16, PWS19, SKH17, SSP19, TRD11, TS16b, VV18, AAZ+16, ABB+14, ADH17, BM13, BBG+13, BEB+18, FMA+18, HKA19, HT13, HAGTzdF13, KJN+16, KAS15, LK10, MPP19, MA17, Maz13, MH15, MR11, PPA18, TZT16, VBC+15, WW17].

Survival [YCM+13, MMS+17a]. Surviving [CFST17]. suspect [der10]. SVC [MU12, WDD12, ZLDD12, ZLDD14]. SVD [LP12, TB18, ZW17]. SVM [TLL13].

swarm [ZMS18]. Swarms [VOGB18]. SWIFT [PLCGS11]. Switching [CNT12, GHPS12, GHPS13, WB12, YWY12]. Sybil [dCCSM+12]. Sylvester [SS10b]. Symbolic [CBRZ19, Wat10]. Symmetric [BPR14a, BPR14b, BDP12, CVM14, FPS12, GFBF12, JCHS16, KTT12, Kha10, PR12, PCY+17, TWZ11, YKNS12, BGG+13, CGKO11, DLZ16a, FH13, GMRT+15, Gor10, GCVR17, KAS15, LZC17, SKK10, ZCZ+19]. Symmetric-Key [CVM14, KTT12].

symmetrical [RS17]. Symmetry [SS14]. Symposium [ACMi9, ACM11, Ano10, IEE10, IEE11b, IEE13, Wat10, Ano11a]. symptom [YZL+18]. symptom-matching [YZL+18]. Synchronization [BL12, VTY18, WXY+17, yWXyZ+18, AATM18, XNG+14].


Synergy [KRB12]. Synergy-Based [KRB12]. Synopses [RCBK19]. Synthesis [TCMLN19, RS17]. Syst [HYS18, WZM12a]. System [ADH11, Ano10, BBCL19, BD18, CZL12a, CZLC14, Cor14b, CRST15, DG15, GOP12, Har16, HHS+15, HZS+19, IAD10, JN12, JWJ+17, Jin10, KMP+11, LYX+19, LFX+18, Lop12, MLBL12, NSM14, PSSK19, QLL17, RSCX18, SMIK18, SRAA17, SLI11, XZL+19, YE12, YXZ+12, YKK18, ZMM17, ZPW16, ZLDC15, ZV16, AHM+18, BC18, BGG+13, Bul10a, CH11, CTL12, CZ14, CS11, FNWL18, GKCK11, GH15, HHBS18, HKW+15, HJM+11, HLYS14, JC13, LLLK10, LLL+17b, LHH+18, Lit14, LTC+15a, LLL+18. LKZ19, MS12a, MNNW15, PSMPL13, SSPL+13, WMX+17, WDZ19, WGZ+12, XWW16, XYML19, YZL+18, ZCZQ19, ZMM+10, ZML17, ZZZ+18, KKA14, Dew11].

System-Level [BBCL19, JWJ+17].

System-on-Chip [HZS+19]. Systematic [CCG+16, CBL13, PC16, IAA+19]. Systems [AN12, AB15, Ano19a, BL15, BS13b, BCTPL16, BB10, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HLN+10, HK18, KLK+19, LMD16, LQY10, LY16, LNZ+13, MR14b, MJ+19, O12, PRSV17, QZL+16b, RST15a, RST15b, SBS+12, SFKR15, Sev16, SKH17, SG14, SDM+12, STC11, SSP19, TSK14, YNR12a, AT10, ATI+10, BGE+18, CFVP16, CFZ+10, CLZ+17, Cla18, dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DZS+12, Eis10, FXP12, GMOGCC15, GH19, GSN+16, GPVCDbR12, HZW18, JSDK+16, JHCC14, KSA16, LCL+15, LWK+18, MDHM18, MLMSM12, MGP10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRB+12, SMS+16, WS14, YSM14, ZVH14, Zhu13, MA17, Ano11a]. Systolic [MCD12]. Systolic-Array [MCD12]. SZK [MX13].

T [SJWH+17]. T-Chain [SJWH+17]. Table
Tables [CCL+13, AY14a, LDDAM12].
Tag [PTT16, XHM14].
Tackling [USH19].
Tack [NNAM10, PPH12, CJP15, SPLHCB14, CJP12].
Tags [MO12, HSH11, HDPC13, HQY+16, LEW19, MK12a, PLSvdLE10, TG17, WCFW18].
Taipei [Yan11].
Taiwan [Yan11].
Takes [Ano16c].
Talking [FD11].
Tamed [NXB13].
Taming [BBDL+17].
tamper [MN10, NC13, WgMW12].
tamper-evident [MN10].
Tamperable [ACM+17].
Tampered [SSA13].
Tampering [CG14a, QJC+18, SRAA17, SGP+17].
TAO [Sta13].
Taormina [Cra12].
Tap [NM18, ADG16].
Tap-based [NM18].
taps [GSAV18].
target [APMCR13, HRS16, LSQ15].
target-driven [APMCR13, LSQ15].
Targeted [ABJ13].
Tasks [Abe12, FKS+13, CL16].
Taxonomy [AJA16, GAF+15, KMSM15, HAGTDFR13, MA17].
Taylor [Joh10].
Tc [XLC+19].
Tc-PEDCKS [XLC+19].
TCC [Cra12, Lin14b, Sah13].
TEASE [ZBR11].
tech [Ano15e].
technical [Sir16, TS16b, Wag16, JW14, Suc12].
Technique [HEK18, KBL11, ZLDD14].
BBP13, CPPT18, GCSAdp11, LH11a, Nam19, SM12, SK5+18, TS16a, ZWS+18].
Techniques [Bis17, DA12, GOS12, HFC10, HL10b, LW12, Mor12, PJ12, VV18, AB10b, BM13, FGPGP14, Gii10, HT13, KHF10, LH11b, OO18, VN17, WMX+17, Joh10].
Technologies [Int19, SJZG19, JAE10, JAS+11, Lan10, MMP19].
Technology [Ano19c, CGB+10, Foi16, IEE11a, MZLS18, Wu16, Ham19, IMB17].
telecare [LWK+18, MA17].
telephone [GMMJ11].
telephony [Cla18, SKEG14].
Television [DTE17].
Tell [Cer14].
Template [NGANuHQ16, SKV12, ATI+10, GCSAdp11].
Templates [DWB12, AHM+18, QLZ19].
temporal [JMW+16, MHT+13, XMHD13].
temporal-credential-based [JMW+16, XMHD13].
Tenant [TV15].
Terabit [LGP19].
terahertz [WW13].
Term [SS10b, JSK+17].
termination [SS10b].
TERMinator [MTM18].
Text [GA19, GdM16, SMSK18, XZZ18].
text-dependent [GdM16].
textbook [PP10a].
 Thanks [CBL10].
Theft [Ber12, Ber17, BTPLST15, ZMYB17].
Their [CZLC12b, CK18, FVJ19, JS18, JSK+17].
them [HLV10, JSK+16, Rus15].
Theological [SS10c].
Theorem [Lau12, HF14a].
Theorem-based [Lau12].
Theoretic [CVM14, MAL10, WSS12].
CDGC12, GLM+19, SD10, SKEG14].
theoretical [KL13, ZZ15, Gas13].
Theoretically [TWZ11].
Theories [ABR12].
Theory [ACM10, ACM11, AAUC18, CCKM16].
CDFZ16, CDFS10, Cra12, FGM10, FB12, FS15, Fes12, LW11a, Lin14b, Nac12, Per13, PJ12, RBHP15, RST15a, RST15b, Sah13, SAKM16, Sha10, Wes16, Yan10, Abe10, AB10b, Bul10b, CFR11, Gii10, LPZJ15, MZA+13, McG11, YTM+14, Cra12, Lin14b, Sah13, vDKS11].
theory-based [LPZJ15].
Theore [Cer15, Mc1K11, SM13].
Thin [Ch16, JXL+19].
Thin-client [JLX+19].
things [FQZF18, AAC+16, BCEL19, BSL18b, CLF+17, GMDR19, Ham19, HZL18, JKAU19, LNK+18b, LGH+17, NLLJ12, NLY15].
PLGMcDf18, SB17, SXH+19, SS19, VWC19, WCC18, XLC+19, YCT15, ZSY19].
Third
[jCPB+12, OSH16, QZL+16b, Sen10, BL10, ED19, Kip13]. Third-Party
[OSH16, QZL+16b]. Third-Round
[jCPB+12]. Thirty [AP13]. thou
[BDK11]. Threat
[CSYY18, ALL+18, Ven14, ZMYB17]. Threats
[AJA16, ERLM16, GSC17, LJS+14]. Three
[CZ15a, HXC+11, LLY+18, LZC+12b, PC16, Shi11, YKNS12, AIB+16, HWB10, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].
Three-Dimensional [LLY+18, LZC+12b].
Three-Factor [HXC+11, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b].
Three-party [HWB10, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].
Threshold [CT11b, Cil11, FGM10, GLW13, HYS11, LWL10b, SSU12, Sta12, Tan11, WYCF14, WHL15, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, HH15, OO10, QD16, SES+16, Shy15, SGM16, TD14, ZJX+14, ZPZY12].
thresholding [PC14]. thrive [Sch12b].
throughput [MAK+12]. Thru
[SYC+17, SYW17]. Thwart [LJS+14].
Thwarting [XTK10]. Ticket [XCH14].
Ticket-based [XHCH14]. tickets
[LMJC11]. tied [Men13b]. Ties [PYM+15].
Tight [GDC16, LPS12, LLH18, ZYH+19].
Tightly [HLGLG18]. Time
[ASBDs16, Ano17d, App14, AYS15, BBCL19, BJ16, Chem17, FDI11, GSC17, HC17, HGT15, IF16, JWJ+17, JEA+15, KME+12, CLC+17a, LFX+18, NA10a, Nov10, PNRC17, Ste15b, WLZL12, YE12, AY14a, Ano15d, BM15, CC14, Dacat12, FH10a, GPLZ13, HU15, LW10, LW13b, LML+13, MK11, Par18, SPK17, XLC+19, Ano16g].
Time-area [Nov10]. Time-Delay
[LFX+18]. Time-Memory [ASBDs16].
Time-Series [BJL16]. Time-Specific
[KME+12]. Time-Spread [HGT15]. Timed
[Jia14b, KFOS12, Tan15a, Unr15, WSS12].
Timed-Ephemeralizer [Tan15a].
Timed-Release [KFOS12, Unr15, WSS12].
Timeing [BGN17, GV14b, Hay13, LGR14, LF19, AGH+17, MCL+19, SRB+12]. Tiny
[ZOC10]. Titan [PP10b]. Titan-R [PP10b].
TLS [AV18, AP13, BBDL+17, BFCZ12, BJR+14, CFN+14, Dav11]. TLS-based
[PP10]. Today [Ber16a, Cla18, Mac12].
Toepplitz [Ye10]. Token [TYK+12, ZM16, IMB17, Jac16, OMPSPL+19]. token-based
[Jac16]. Token-Leakage [ZM16].
Tokenizationg [Mar10b]. tokenless
[Wat14a]. Tokens [Muf16, DCAT12, Hu15].
Tokyo [Sah13]. Tolerant
[HK14, ZM16, JLT+12, WMYR16, XW13].
toleratingg [ZWM14]. Tone [Yam12].
Too [DL15, DSSDW14, Ros11]. Tool
[ASM12, DMK15]. Toolbox
[AHS13, TRD11]. Toolkit [BJL12]. Tools
[Abe12, BKBK14, GO17, Sta15a, Lan11].
Top [SS12a, SS10c, Sta13, CHX13]. top-
[CHX13]. Top-Fanin [SS12a]. Top-Secret
[SS10c]. Topics [SCPSN10a, SCPSN10b, AB10b, Dun12b, Kia11, Piel10]. Topology
[HHMK14]. Topology-Preserving
[HHMK14]. Tor [LLY+12a]. Toronto
[ MV12]. Tossing
[ALR13, DSM14, Fok12, BB14]. Touch
[SPW+16, SHBC19, Alp18, CTL12, IAA+19, NSBM17, TZTC16]. touchstroke [Alp18].
Tower [ZAG19]. TPM [GY13]. TQC
[vDKS11]. Trace
[ABR12, GA19, PS14, AA14, WGTJ10].
Traceability [HCETPL+12, WYML16, WHL16, YFT17, Chi13a, YYS+16].
Traceable [LDZW19, QRW+18].
Traceable-then-revocable [LDZW19].
traceback [WLY12, PJ18, WYL13]. traces
[MYYR13]. Tracing
[LW16, PPS12b, WXH+17, MFH13, PP+12].
Track [Dun12b, Kia11, Piel10]. Tracking
[GZH17, MDMJ17, SNCK18]. Trade
[ASBDs16, BS14, GPR+19, SR10].
Trade-Offs
ASBdS16, BS14, GPR+19, SR10. Tradeoff
WDDW12, MV16b. Trading [TW12].
Traditional [SSP19]. Traffic
DRS16, HS18, KAHKB17, VV18, AZH11,
FVy+10, PPR+12, Tay19, VS11.
traffic-feature [FTV+10]. Training
[HM12]. Traitor [LW16, FPS12b, Bha16].
trajectory [LRYV10]. Transaction
BGAD12, MMLN15, KVvE18, OYHSB14.
Transaction-based [BGAD12].
transactional [SPK17]. Transactions
DG15, Mic16, Muf16, PAS13b, TV15, DK12,
FG19, MLMSMG12. Transceiver
NBZP17. Transcript [Gli12]. Transfer
DN12, FMTR12, HL10a, LCCJ13, WCL+18.
transferable [GZX19]. Transform
AN12, BCPV11, LSL12b, pNyWY+y14,
OWHS12, SM12, YWNN15, BW13, MO14,
Transformation
CRE+12, FJJHJ12, NXB13, TFS19,
tWnC12, GZH12, HQZH14, PGLL10.
transformations [CJXX19, SA14].
transition [CK11]. transmission
BCND19, PSIO+13, WQZ+13.
Transmissions [CBO+18]. Transmitter
KPBP17. Transparency [TJZF12].
Transparency-Orientated [TJZF12].
Transparent
CCW+10, XTK10, ZHS+19, CRS13.
Transport [RBHP15, TW14].
transportation [SMS+16]. transposition
[FVK17]. Trapdoor
BKPW12, CL19, CBXJ19, CWWL12,
Mat14, RPSL10, CSZ+11, CW12a.
treatment [YSM14]. Tree [BS14, HSH11,
XWZ18, BW13, BB16b, CFG+17].
Tree-based [HSH11]. Trees
SB18, BTPLST15. Trends
Fri12, GCK12, ZMS14, JAE10. Triangular
AMVZ12, RR16. Tricks [GY13]. Trigger
SS19. trimmed [TTL10]. TRIMS
MG10. Triple [LW13b, MS12a].
triple-base [MS12a]. Triple-image
[LG13b]. Triplet [JS18]. triumphant
McG11. Trivial [MS12b, SR12a].
TRNGs [YBS810]. Trojan [NDC+13].
Trojans [BRPB13]. True
FRT13, LTKP16, Fag17. TrueErase
DMS+16. Truly [LA10]. Truncated
KWS+12, WW12. Trust [Bar15, BCK17,
DCA19, Gli12, GM14, GSFT16, HHSB18,
IGR+16, KMSM15, KP12, PYM+15,
PH12b, PAS13b, Rai15, TMGP13, TV15,
WLY+15, Zha15b, BS19, CO11, KGO10,
MLMSMG12, MGP10, Sch12b, YT11a.
Trusted [AWSS17, EAA12, FPY15, YCR16,
ED19, HTC+10, Kip13, XZLW15, YI17].
trustworthy [KM10b]. Truth [MSJ+19].
TTP [ATK11]. TTP-free [ATK11]. TTPs
[KGO10, TAKS10]. Tulip [JB11]. Tunnel
tunnels [CRI16]. Tunny [COP10a]. Turing
Orn16, Bl612, Car10, CS12, Don14, Hai17,
Hel17, KUS13, LCKBJ12. Turtle
WZCC18. Tutorials [Lin17]. Tutte
[Hai17]. TV [CCSW11]. Tweakable
CMLRHS13, LST12, MLCH10, MKASJ18,
Sar11, Zha12]. tweet [BTW15].
twelve [BCV12]. twice [BM15]. TWINE
[TDH13, TY16b]. Twins [Bow11]. Twitter
[AlF+19]. Two
[Ash14, Bru12, CTL13, DZ14, ED19,
GGHR14, GLW12, HL10b, HP14, HWB10,
KMTG12, KOS16, KU12, LLC11, Li14,
NSMS14, OTD10, YSL+10, YZW13, ZM16,
AN15, BD18, CSD18, CHS11, DHW+13,
FIO15, GMM11, HPC12, HWDL16,
HWB12, JLT+12, JMW+16, Kem11, Li10,
MDHM18, MG11, NM15, OMPSP+19,
QYW16, Rus15, SM10b, hSB15, WW14,
Wat14a, YTF11b, ZCC15, GHKL11].
two-channel [JLT+12]. Two-Factor
[LLC11, ED19, Lit14, BD18, GMM11,
JMW+16, Kem11, MDHM18, NM15,
WW14, Wat14a]. Two-Party [Ash14,
HL10b, HP14, KOS16, NSMS14, ZM16,
FIO15, HPC12, HWB12, ZCC15, GHKL11].
Two-Round [GGHR14]. **Two-Server** [YLW13, KMTG12, CSD18]. Twofish [MD12a]. **TWS** [OKG+12]. **Type** [AKP12, CFL13, PFS12, SH15, BNST17, SYL13, WB12]. **Type-based** [CFL13, SYL13]. **Type-Flaw** [SH15]. **Types** [BCEM15]. **typing** [SCR19].


[ACM12, GMSW14, SB17]. **UMTS** [OHJ10, TM12]. **unaided** [CAM19]. **unattended** [BN14]. uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. unbreakable [Bha16]. Uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. **unaided** [CAM19]. **unattended** [BN14].

Unattended [BN14]. **unauthentic** [MLSMG12]. unbreakable [Bha16]. Uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. **unaided** [CAM19]. **unattended** [BN14].

[ACM12, GMSW14, SB17]. **UMTS** [OHJ10, TM12]. **unaided** [CAM19]. **unattended** [BN14]. uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. unbreakable [Bha16]. Uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. **unaided** [CAM19]. **unattended** [BN14].


[ACM12, GMSW14, SB17]. **UMTS** [OHJ10, TM12]. **unaided** [CAM19]. **unattended** [BN14]. uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. unbreakable [Bha16]. Uncalibrated [MLSMG12]. **Unauthorized** [CBO+18]. **Unbounded** [WL11c, YZ12]. **unaided** [CAM19]. **unattended** [BN14].


YHL16, YSL+10, YN19]. User-centric [BLV17]. User-controlled [Har16].
User-Friendly [SZDL14, WOLS12]. User-Generated [LCL17b]. User-Level [BKJP12]. user-participating [CH10].
User-related [GMDR19].
User-Transparent [ZHS+19]. Users [DPCM16, KKA15, TAKS10, WPZM16, ATK11, Bel18b, uHAN+18, FHM+10]. uses [Rus15]. Using [AA19, ABS+12, ABB+14, Ano15a, Ayu12, ARM15, BBC+13, BCPV11, Bee17, BFMT16, BKLS12, BJR+14, CST+17, CCL+13, DSB16, DR12, DA10, DBPS12, DL12, ERLM16, ERRMG15, FHLDD19, FMS12a, GH11a, GSC17, GAS+16, HEK18, HHS+15, HD19, IL15, Jia10, JEA+15, KBL11, Lac15, Lan11, LYZ+13, LLY+18, LLGG16, MM17, MBC15, MRL+18, MS16, NIS12, NGAuH1Q6, NNAM10, NN12, NSM14, PMZ13, PSS+13, PAF18, PDMR12, PDT12, PCPK14, RMERM19, VRVSCM12, SR12a, SFE10, SS19, SSA13, SRAA17, SC12, SR12b, Tan12a, TKR14, WWL+14, WgMdZ12, WY12, WAK+19, XNP+18, XZZ18, YWW10, YWW15, YCL17, YSS14, ZH15, ZWZ17, ZPW16, ZS12, dRSdVC12, AASSA18, ATKH+17, AHM+18, APK+18, ASVE13, BL+19, BOP14, BM13, CSH+18, CHS11, CR12, CLHJ13, CP13, CR16, DA18, Dav11, DTZZ12, DGFH18, DMD18, uHAN18, EEAZ13]. using [FES10, GSAV18, HAK19, Ham19, Har14, HK17, HZW17, HFCR13, HWB12, HL14, HPY10, HCC10, HS11, JKA+18, JCHS16, JMWM+16, K11+10, K11Y, KG14, KM11, KSU13, KTB17, KLW+16, LXYL12, LLP+18, LC17, LH11a, LH10c, LNM+11, LMXW12, LH13, LZXK19, LML+13, MM12, MMLN15, MS13a, MMSD13, MM14a, MKH+12, MRR17, MSR+17, MSM+18b, NTKG17, NSBM17, PBCC14, PBP19, PC14, QD16, RR17, RS15, RS17, SCFB15, Sar11, SGFCRM+18, SSK+18, SAR18b, SPK17, SA19, TLCPF16, TG17, TK14, TLL13, UUN11, yWpNyL11, gWpNyY+14, WMX+17, WHJ17, YWJ+19, YQH12, YZZ+14, YSL+10, YN19, ZZKA17, ZLW+12, ZYC+17, ZWX+18, ZZL+18].
utilization [NZM10]. Utilizing [BM18].
Vegas [IEE10]. Vehicular [HLKL15, ZHW+16, KM10b, SGCCR+16].
Vein [KLY+12]. Velskii [BBB16b].
Ventilated [RSCX18]. Vera [Ayu12].
Verifiability [RST15a, RST15b, VSR12, WWHL12, YMC+17, BRR+15, Hwa11].
Verifiable [CE16, CRST15, Fuc11, HYS11, HLC12, HLC+18, LLL+18, QD16, RDZ+16, SQZ+17, XWLJ16, YNR12a, YCR16, GLM+19, LZY+16, LJW+17, NMP+13, PGHR16, QS18, XWS17, ZZ15]. verifiably [SEXY18, ZLY+10]. Verification [AV18, App15, ABR12, BL15, CCK12, CC1K16, CM11, EWS+14, Ess17, GLLSN12,
watermarking [TPKT12, WLDB11, yWpNyL11, Wan13, yWpWyYpN13, WZLW13, YWT12, ZZKA17, ZSMS18]. Watermarking-Encryption [SLGZ12].

References

Akyildiz:2014:OTB


Abouaroek:2019:NAU

Musaeed Abouaroek and Khaleel Ahmad. Node authentication using NTRU algorithm in opportunistic

Applebaum:2017:AC

Abo-alian:2016:KDB

Ambrosin:2016:FAB

Albertini:2014:MHE

Arora:2012:ILM
Azzam:2018:SRC

Akleylek:2016:SPM

Aghili:2018:ISA

Acar:2018:SHE

Alizadeh:2016:AMC

Abdalla:2010:PCL
Michel Abdalla and Paulo S. L. M. Barreto, editors. *Progress in cryptology — Latincrypt 2010: first international conference on cryptography and information security in Latin America, Puebla, Mexico, August 8–11, 2010*, pro-


[ABB19b] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan Capkun, Gerhard Hancke, Süleyman Kardas, Chong Hee Kim, Cédric


[ABD+15] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Senior.


Almeida:2014:COS


Ananth:2013:SFP


Avoine:2016:SSP


Aid:2013:DIO


Acar:2013:SPA

Andreeva:2012:SAS


Arapinis:2012:RET


Applebaum:2010:PKC


Atighehchi:2015:NME


AlMashrafi:2012:AIM


Arias-Cabarcos:2015:BIP

[ACAT⁺15] Patricia Arias-Cabarcos, Florina Almenarez, Ruben Trapero, Daniel Diaz-Sanchez, and Andres Marin. Blended identity: Pervasive IdM for continuous au-

Armando:2013:AFB


Arnold:2015:NGH


Amoah:2016:FMA


Ardagna:2010:ECP


ACM:2010:PAI

REFERENCES


Aczel:2011:SWL


Alvarez-Cubero:2016:AVL


Aizatulin:2012:VCC

REFERENCES


REFERENCES

Andrychowicz:2016:SMC


Araldo:2018:CEC


Ahmed:2017:IRD


Attrapadung:2015:RGS


Antonopoulos:2017:DIS


Akinyele:2014:MGA

Joseph A. Akinyele, Matthew Green, Susan Hohenberger, and Matthew Pagano. Machine-generated algorithms, proofs and software for the batch verification of

**Abdollaziz:2016:AAI**


**Ahani:2015:SRB**


**Akhatar:2018:BSI**


**Appelbaum:2013:SSG**

J. Appelbaum, J. Horchert,
and C. Stöcker. Shopping for spy gear: Catalog advertises NSA tool-
international/world/catalog-reveals-nsa-has-backdoors-for-numerous-devices-
a-940994.html.

[AHS14] Murat Ak, Turgut Hanoy-
mak, and Ali Aydin Selçuk. IND-CCA se-
cure encryption based on a Zheng-Seberry scheme. Journal of Computational
and Applied Mathematics, 259 (part B)(??):529–535, March 15, 2014. CODEN
JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0377042713003403.

[AIa15] Mahdi Aiash. A formal
analysis of authentication
protocols for mobile de-
vices in next generation
networks. Concurrency
and Computation: Prac-
tice and Experience, 27
(12):2938–2953, August 25,
2015. CODEN CCPEBO.
ISSN 1532-0626 (print),
1532-0634 (electronic).

[Ala18] Zulfiqar Ali, Muham-
mad Imran, Mansour
Alsalaiman, Muhammad
Shoaib, and Sana Ul-
lah. Chaos-based ro-
bust method of zero-
watermarking for medical
signals. Future Gen-
eration Computer Systems,
88(??):400–412, November 2018. CODEN FG-
SEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0167739X18304709.

[Rul] Ruhul Amin, SK Hafizul
Islam, G. P. Biswas, Muhammad
Khurram Khan, Lu Leng, and Neeraj Kumar. De-
gn of an anonymity-
preserving three-factor au-
thenticated key exchange
protocol for wireless sen-
sor networks. Computer
Networks (Amsterdam,
Netherlands: 1999), 101
CODEN ?? ?? ISSN 1389-
1286 (print), 1872-7069
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1389128616000207.

[Alt] Malik H. Altakrori, Farkhund
Iqbal, Benjamin C. M.
Fung, Steven H. H. Ding,
and Abdallah Tubaihat. Ar-
ic authorship attribu-
tion: an extensive study
on Twitter posts. ACM
Transactions on Asian
REFERENCES


Applebaum:2014:HGA


Amin:2018:UAP


Ali:2019:PRD


Alhanahnah:2016:MTI


Azarderakhsh:2014:NDP

REFERENCES

COB4. ISSN 0018-9340 (print), 1557-9956 (electronic).


Riham AlTawy, Aleksandar Kircauskis, and Amr Youssef. Second order collision for the 42-step re-


Asharov:2013:FCF


Awad:2016:SSZ


Arnedo-Moreno:2010:JRA


Arsalan:2012:IRW


Ahir:2017:LAR


Abbasinezhad-Mood:2018:DHI

REFERENCES


[Arshad:2015:SAI] Hamed Arshad and Morteza Nikooghadam. Security analysis and improvement of two authentication and key agreement schemes for...

**Aga:2017:ISM**


**Anawis:2014:ARR**


**Anderson:2013:MNF**


**Anonymous:2010:NDS**


**Anonymous:2011:AIS**

Anonymous, editor. *ACIS international symposium on cryptography, and network security, data mining and knowledge discovery, e-comerce and its applications, and embedded systems*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA.
Anonymous:2011:AXL


Anonymous:2011:MCB


Anonymous:2012:SHS


Anonymous:2013:DSS


Anonymous:2013:NCI


Anonymous:2013:SSD


Anonymous:2013:SIS

Anonymous. Special issue on “Security and identity architecture for the future Internet”. *Com-
REFERENCES


Anon Anonymous: 2015: BSU [Ano15a]

Anon Anonymous: 2015: BRDa [Ano15b]

Anon Anonymous: 2015: QCS [Ano15c]

Anon Anonymous: 2015: UGB [Ano15d]
Anonymous. UK Government battles tech firms over encryption. Net-
Anonymous: 2016: CPSd


Anonymous: 2016: CPSe


Anonymous: 2016: EMT


Anonymous: 2016: FVM


Anonymous: 2016: GUP


Anonymous: 2016: MBE

Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

[Ano17a] Anonymous. BitErrant attack. Web site, March 6, 2017. URL http://biterrant.io/. The story describes how SHA-1 collision attacks could lead to bogus, and malware, file downloads via BitTorrent: the obvious solution, which should have been adopted long ago, is to use multiple checksum algorithms, and require all to match before concluding that two files are in fact identical.

Anonymous:2017:BRM


Anonymous:2016:HDQ

Princeton University Press.

Anonymous:2017:CCS

[Ano17c] Anonymous. Cybernetica case study: Solving the Estonian ID-card case. Web news story., December 13, 2017. URL https://cyber.ee/en/news/cybernetica-case-study-solving-the-estonian-id-card-case/. The story describes a poor choice of generating large (about 1024 bits) primes \( p \) and \( q \) that led to crackable RSA cryptography. The solution for Estonia was to switch to elliptic-curve cryptography that was also supported by the cards.

Anonymous:2017:HDQ

Anonymous:2017:MBH


Anonymous:2017:RV


Anonymous:2019:HCC


Anonymous:2019:GES


Anonymous:2019:PBT


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF


AlFardan:2013:LTB


Ali:2018:SUA


Alcaide:2013:AAP

Almudena Alcaide, Esther Palomar, José Montero-Castillo, and Arturo Ribagorda. Anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security*, 37(??):111-123, September 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-
REFERENCES

Applebaum:2013:GXG


Applebaum:2014:CCP


Appel:2015:VCP


Albrecht:2015:FBR


Al-Qarni:2012:EII


Arai:2013:MDH

REFERENCES


**Adj:2014:SRC**


**Altawy:2018:SLT**


**Altawy:2018:TCM**


**Agudo:2013:PA**


**Azarderakhsh:2015:PHS**

Armasu:2019:IFA


Ambrose:2012:RII


Alghamdi:2019:RAM


Artemenko:2017:PGO


Andrade:2016:LEP


Asharov:2014:TCC

[AS14] Gilad Asharov. Towards characterizing complete...

**Al-Sinani:2012:UCB**


**Ahmadi:2011:SKC**


**Ahmadi:2012:SKE**


**Ali:2014:ALD**


**Asaar:2015:IBM**


**Alsulaiman:2013:IVB**

[ASVE13] Fawaz A. Alsulaiman,

Altman:2010:AAP


Argyropoulos:2010:BTP


Au:2011:PPT


Al-Tariq:2017:SFP


Alam:2015:ACF

REFERENCES

Aslan:2016:DEM

Abdalla:2012:LRS

Abdou:2018:SLV

Altalaf:2015:LPM

Altalaf:2017:LHL

Awad:2017:OLO
REFERENCES


Alshammari:2011:CET


Blaner:2013:IPP


Brennan:2012:ASC


REFERENCES

Bax:2014:PPD


Baylis:2010:CC


Bulygin:2010:OSS


Bennett:2014:QCP


Barenghi:2016:FBS


Boumerzoug:2016:LKM

Hayette Boumerzoug, Boucif Amar Bensaber, and Ismail Biskri. A lightweight key management scheme based on an Adelson-Velskii and Landis tree and elliptic curve cryptography for wireless sensor networks.
REFERENCES


Barenghi:2013:FIT


Baldi:2013:ULC


Barak:2014:OEF


Barthe:2019:SLN


Baillot:2019:ICC

Patrick Baillot, Gilles Barthe, and Ugo Dal Lago. Implicit computational complexity of subrecursive definitions and applications to cryptographic proofs. Journal of Automated Reasoning, 63(4):813–855, December 2019. CODEN JAREEW. ISSN 0168-7433 (print), 1573-
REFERENCES


REFERENCES


**Bernstein:2011:PCI**


**Basin:2014:KYE**


**Bocu:2018:HEB**


**Balagurusamy:2019:CA**


**Bichsel:2012:DMA**

Patrik Bichsel, Jan Camenisch, Bart De Decker, Jorn Lapon, and Vincent Naessens. Data-minimizing authentication goes mobile.
REFERENCES

119


[Bahi:2012:SCS] Jacques M. Bahi, Jean-François Couchot, and Christophe Guyeux. Steganography: a class of se-
References

Borghini:2012:PLL

Baelde:2012:TPR

Bahi:2011:ECS

Barthe:2012:CA

Beunardeau:2016:WBC
Batina:2019:ISI


Bitansky:2013:SNI


Brandenburger:2017:DTC


Bernstein:2014:CKR


Basin:2012:PRI

REFERENCES


REFERENCES

[Basso:2011:BWC]

[BCQ+13]

[Blasco:2016:SWB]

[Biddle:2012:GPL]

[Barker:2015:RKM]

[Baruah:2018:TFA]
REFERENCES

Belkacem:2014:DCM

Bruguera:2019:GEI

Bender:2012:DSP

Bhasin:2015:EFB

Buchmann:2011:XPF

Backstrom:2011:WAT
REFERENCES

ISSN 0001-0782 (print), 1557-7317 (electronic).

Bernstein:2011:HSN


Barbareschi:2018:PBH


Belkhouja:2019:BBA


Bossuet:2016:EPA


Bendlin:2011:SHE


Bertoni:2011:CSF

Bertoni:2012:KIO


Boldyreva:2012:SSE


Bitansky:2013:WFS


Bottarelli:2018:PCW


Beebe:2017:MFC


REFERENCES

[102x681]


Berghel:2017:ELR


Berretti:2018:IAS


Bouman:2011:SAW


Bas:2012:BLK


Bos:2019:ACI


Bhargavan:2012:VCI

REFERENCES


REFERENCES

Battistello:2012:TBA

Barthe:2012:CA

Balagani:2018:IA

Barak:2010:IPO

Barak:2012:IPO
Boaz Barak, Oded Gol-


Brakerski:2014:LFH


Barkatullah:2015:GCF


Bhattacharjee:2016:SWC


Blasco:2012:FAS


Behnia:2012:SEI


Bernstein:2015:SPS

Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O’Hearn. SPHINCS. Practical stateless hash-based signatures. Lecture Notes in Computer Sci-
REFERENCES

Benhamouda:2019:SPD


Bosc:2014:SPS


Berman:2013:HPR


Bonneau:2015:PEI


Biagioli:2012:CCS


Beimel:2014:CCW


REFERENCES

134

Biswas:2017:SA

Bauer:2010:RV

Boc He:2016:DSK

Bouraoui:2017:HAE

Bogdanov:2012:UTC
REFERENCES

Benhamouda:2016:NFP


Brubaker:2014:UFA


Boldyreva:2012:NPG


Bouti:2012:SCB


Bhuyan:2014:DDD


Braun:2012:ULA

Bastian Braun, Stefan Kucher, Martin Johns, and Joachim Posegga. A user-level authentication scheme to mitigate Web session-based vulnerabilities. Lecture Notes in Computer
REFERENCES


Brakerski:2010:OHB


Bogdanov:2013:SDS


Bogdanov:2012:KAC

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, and Francois-Xavier Stan-
REFERENCES


**Bogdanov:2011:BCF**

**Bogatov:2019:CEO**

**Bibak:2018:AUH**

**Bothe:2013:EPS**

**Bernstein:2010:PCA**

**Byun:2011:SMC**
Jin Wook Byun and Dong Hoon Lee. On a security model of conjunctive keyword search...


REFERENCES


Banik:2012:DFA


N. Buckley, A. K. Nagar, and S. Arumugam.


Bailey:2014:UIA


Borgho:2010:CLC


Bowyer:2011:WSD


Boyen:2013:ABF


Boyle:2016:BOT


Burns:2010:SCR


Bohli:2011:RAP

REFERENCES

Budroni:2018:HGB


Brooke:2010:DCX


Bellare:2014:SSEa


Bellare:2014:SSEb


Boneh:2016:BCR


Balsa:2017:TIC

REFERENCES


[BRPB13] 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.

Benaloh:2015:EEV


Bag:2017:BBW


Baja:j:2013:CSE

Birrell:2013:FIM


Bhattacherjee:2014:CAT


Bagheri:2015:NNA


Bala:2019:SAG


Bendiab:2019:FNF


Boorghany:2015:CIL


Bala:2019:SAG


Bendiab:2019:FNF


Boorghany:2015:CIL

Bojinov:2014:NMC


Basin:2011:AIS


Beaulieu:2013:SSF


Batina:2012:HEB


Broustis:2012:GAN


Boneh:2012:FEN

Dan Boneh, Amit Sahai,

**Biskup:2012:RBR**


**BTK15**


**Braeken:2018:AAA**


**BTPLST15**


**Bosch:2012:SDR**

Brocardo:2015:AVM

Buchmann:2010:EKG

Bulygin:2010:AOP

Bulygin:2010:CAC

Burke:2011:AMD


REFERENCES


Bai:2016:ALC

Bhatnagar:2013:SRI

Bhatnagar:2012:IVE

Bhatnagar:2012:NRA

Bao:2010:ISC
Feng Bao, Moti Yung, and Dongdai Lin, editors. *Information security and cryptography: 5th international conference, INSCRYPT 2009*, Beijing,
REFERENCES


Staff:2014:KYS


Caldwell:2013:INP


Chakraborty:2019:TIP


Carter:2010:TB


Carlson:2011:JRW


Casselman:2010:VC


Chang:2019:KCS

[CBJX19] Jinyong Chang, Genqing Bian, Yanyan Ji, and Maozhi Xu. On the KDM–CCA security from partial trapdoor one-way fam-

Cheneau:2010:SIP


Cobb:2013:LMS


Chang:2018:DMU


Chattopadhay:2019:QIL


Cachin:2010:EKS

REFERENCES

Chang:2014:RR


Chadha:2016:AVE


Chretien:2015:SPP


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO

REFERENCES


[Chang:2011:SFW] Chin-Chen Chang, Kuo-Nan Chen, Chin-Feng Lee, and Li-Jen Liu. A secure fragile watermarking scheme based on chaos-

Cascudo:2015:SSN


Chatterjee:2017:PBS


Cho:2014:DGA


Chen:2011:EAA


Chu:2014:KA


Chen:2010:ALD

[CCW+10] Songqing Chen, Shiping Chen, Xinyuan Wang, Zhao Zhang, and Sushil Jajodia. An application-level data transparent authentication scheme with-


Hui Cui, Robert H. Deng, and Yingjiu Li. Attribute-based cloud storage with secure provenance over encrypted data. Future Generation Computer Systems, 79 (part 2)(??):461–


Coras:2016:AML


Costello:2014:CAS


Cremers:2019:SAG


Culnane:2019:KKR


Ceruzzi:2014:HFT


Cerf:2015:CTN


Cerf:2018:CSA

Vinton G. Cerf. Cerf’s up: Self-authenticating identifiers. Communications of
the Association for Computing Machinery, 61(12): 5, December 2018. CO-
DEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL
https://cacm.acm.org/
magazines/2018/12/232883/ fulltext.

Chang-Fong:2016:CSC
[CFE16] N. Chang-Fong and A. Essex. The cloudier side of cryptographic end-to-
end verifiable voting: A security analysis of Helios. In ACM, editor, Pro-
cedings of the 32nd Annual Conference on Computer Security Ap-
lications (ACSAC 16: 5–9 December 2016, Hilton Los Angeles Universal
City, Los Angeles, CA, USA). ACM Press, New York, NY 10036, USA,

Crampton:2017:CEI
[CFG+17] Jason Crampton, Naomi Farley, Gregory Gutin, Mark Jones, and Bertram
Poettering. Cryptographic enforcement of information flow policies without pub-
535, ???? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (elec-
tronic).

Carter:2013:SSA
[CFH+13] Kyle Carter, Adam Foltzer, Joe Headrix, Brian Huff-
man, and Aaron Tomb. SAW: the software analysis workbench. ACM SIGADA
Ada Letters, 33(3):15–18, December 2016. CODEN AALEE5. ISSN 1094-3641
(print), 1557-9476 (electronic).

Centenaro:2013:TBA
Matteo Centenaro, Riccardo Focardi, and Flaminia L. Luccio. Type-based analy-
sis of key management in PKCS#11 cryptographic devices. Journal of Com-
(print), 1875-8924 (electronic).

Checkoway:2014:PED
Stephen Checkoway, Matthew Fredrikson, Ruben Nieder-
hagen, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bern-
stein, Jake Maskiewicz, and Hovav Schacham. On the practical exploitability of Dual EC in TLS imple-
mentations. In ????, editor, USENIX Security Sympo-

Cevallos:2012:USR
Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and


Weiling Chang, Binxing Fang, Xiaochun Yun, Shupeng Wang, and Xiangzhan Yu. A pseudorandom number generator based on LZSS. In 2010 Data Compression Conference (DCC), page 524. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010.


164
REFERENCES

Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-7675-5. LCCN ????

Caballero-Gil:2012:LAR


Chmiel:2012:EPC


Coull:2011:ACO


Cohney:2017:PSR


Curtmola:2011:SSE


Cheng:2012:PAI


Chandran:2014:PBC


Cheng:2013:NIB


Chen:2010:NUP


Chang:2011:DEQ


Chen:2013:MPQ


Chang:2013:OCK


Chappell:2013:PMI

REFERENCES


[14] Chen:2015:SSS


[16] Chen:2018:ESA

Yuzhao Cui, Qiong Huang, Jianye Huang, Hongbo Li, and Guomin Yang. Ciphertext-policy attribute-based encrypted data.


[Chi13b] R. Chigwin. Android bug batters Bitcoin wallets. The Register, ??(??): ??, ???, 2013. URL ????.


REFERENCES

[102x681] 0304-3975 (print), 18792294 (electronic).

**Choudary:2010:SCD**


**Chou:2014:EMA**


**Chen:2013:ATK**


**Cooke:2015:FSM**


**Chu:2016:BEE**


**Chen:2013:ATK**

Qian Chen, Haibo Hu, and Jianliang Xu. Authenticating top-k queries in location-based services with confidentiality. *Proceedings of the VLDB*

Cilardo:2011:EPT


Cheng:2013:EHM


Cao:2014:SCI


Cho:2012:CBF


Cho:2015:CBF


Chang:2019:GTS

Jinyong Chang, Yanyan Ji, Maozhi Xu, and Rui Xue. General transformations
from single-generation to multi-generation for homomorphic message authentication schemes in network coding. 


**Chandra:2011:AST**


**Chung:2018:ERN**


**Chang:2019:PPN**


**Chase:2013:SMN**


**Chuang:2011:LMA**

Ming-Chin Chuang and Jeng-Farn Lee. A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks. *Computer Networks (Amster-
Colin:2016:CTC


Claxson:2018:SVE


Chen:2019:BBS


Comon-Lundh:2010:DSP


Chang:2011:RSB


Chen:2017:PGF

Yajing Chen, Shengshuo Lu, Cheng Fu, David Blaauw, Ronald Dreslinski, Jr., Trevor Mudge, and Hun-Seok Kim. A programmable Galois field processor for the Internet of Things. *ACM SIGARCH Computer Ar-
REFERENCES

Chong:2013:ASG

Chen:2016:RPR

Chen:2012:NCB

Chen:2013:TSE

Chande:2016:NSC

Cao:2012:SRH
Jin Cao, Hui Li, Maode Ma, Yueyu Zhang, and Chengzhe Lai. A simple and robust handover

Chen:2019:IBS


Chen:2014:CDP

Liqun Chen, Hoon Wei Lim, and Guomin Yang. Cross-domain password-based authenticated key


Canetti:2013:PCC


Chang:2012:PRS


Cui:2016:KAS


Chen:2014:CDP

Liqun Chen, Hoon Wei Lim, and Guomin Yang. Cross-domain password-based authenticated key
REFERENCES


[CMG+18] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Colney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. Where did I leave my keys?: lessons from the Juniper Dual EC incident. *Communications of the Associa
Coles:2016:NAU


Cao:2018:EEG


Chakraborty:2013:EHI


Chakraborty:2015:SSC


Chen:2017:VME

Cao:2016:OMA


Chen:2012:FAA


Coron:2012:PKC


Chin:2011:ACS


Conitzer:2010:AP

REFERENCES


Sébastien Corthésy. Smartphones set out to decipher

[Coutinho:2012:RPT]

[Claessen:2013:SPN]

[Canard:2018:NTC]

[Chung:2016:NBB]

[Chen:2018:RLF]
REFERENCES


REFERENCES

Crichlow:2016:RSE


Crawford:2013:FCT


Culnane:2015:VVV


Chhabra:2011:NSN


Clark:2012:RLA


Chapin:2014:SRP


Chattaraj:2018:NTS

Durbadal Chattaraj, Monalisa Sarma, and Ashok Kumar Das. A new two-server authentication and key agreement protocol for

Chauhan:2018:BBA


Chadwick:2014:AFI


Chen:2013:RWM


Chen:2017:SIE


Ciegis:2016:ADP

Raimondas Ciegis, Vadi-mas Starikovicius, Natal-ija Tumanova, and Minvy-das Ragulskis. Application of distributed parallel computing for dynamic
REFERENCES


**Sébastien Canard and Viet Cuong Trinh.** Certificateless public key cryptography in the standard

**Calzavara:2015:SLA**


**Chin:2013:SMB**


**Chang:2012:GBP**


**Crenne:2013:CMS**


**Calmon:2014:ITM**

Flavio P. Calmon, Mayank...
REFERENCES


Choi:2012:LTF


Chung:2012:CBI


Chen:2014:SBB


Chen:2014:DSE


Cao:2014:PPM

REFERENCES


[CZ15a] Shangdi Chen and Xiaolian Zhang. Three constructions of perfect authentication codes from projective geometry over finite fields. *Applied Mathematics and Computation,*

Cheng:2015:OMU


Chen:2012:FSD


Dharwadkar:2010:SSG


Chen:2014:CSI


REFERENCES

Dou:2018:OHR


Dou:2019:DTE


Dacosta:2012:OTC


Cordeiro:2016:MPG


Cordeiro:2012:IMB

Ding:2018:NPH


DePrisco:2013:CVC


Datta:2017:SFH


DaRolt:2013:NDS


D’Arco:2014:MIC


Castro:2016:FVB


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

**Dodis:2010:CAC**


**Driessen:2013:ESA**


**Diem:2012:UES**


**Drosou:2012:SAH**


**Dinoor:2010:PIM**


**Dong:2019:FOI**

Ding:2015:CWF


Domnitser:2012:NMC


Dolev:2012:ATC


Delfs:2015:ICP


Delimitrou:2016:SID


Dorre:2016:ELO

Felix Dörre and Vladimir Klebanov. Entropy loss and output predictability in the Libgcrypt
REFERENCES


REFERENCES

**Dunkelman:2012:MCE**


**Dong:2012:UAS**


**DeLuca:2015:SUS**


**Degefa:2016:PSE**


**Djaziri-Larbi:2018:WDA**


**Dong:2013:PRS**

Qi Dong, Donggang Liu, and Peng Ning. Providing DoS resistance for signature-based broadcast authentication in sensor

**DiPietro:2016:CLD**


**Dodis:2011:SSC**


**Dai:2016:MLR**


**Duan:2016:SDC**


**DeCarneDeCarnavalet:2015:LSE**


**Daneshgar:2018:SSS**


REFERENCES

/Y. Doroz, E. Ozturk, and B. Sunar. Accelerating
fully homomorphic encryption in hardware. *IEEE
Transactions on Computers*, 64(6):1509–1521, ???.
2015. CODEN ITCOB4. ISSN 0018-9340 (print),
1557-9956 (electronic).

Christian A. Duncan and Vir V. Phoha. On the com-
plexity of aggregating information for authentication and profiling. *Lecture Notes in Computer
0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-28879-1_5/.

Jintai Ding and Albrecht Petzoldt. Current state of
15(4):28–36, July/August 2017. CODEN ???. ISSN
1540-7993 (print), 1558-4046 (electronic). URL
https://www.computer.org/csdl/mags/sp/2017/
04/msp2017040028-abs.html.

Aveek K. Das, Parth H. Pathak, Chen-Nee Chuah, and Prasant Mohapatra. Characterization of wire-
less multidevice users. *ACM Transactions on Internet Technology (TOIT)*, 16(4):29:1–29:??, December 2016. CODEN ???. ISSN 1533-5399 (print),
1557-6051 (electronic).

20:1–20:??, August 2018. CODEN JACOAH. ISSN
0004-5411 (print), 1557-735X (electronic).

Deshuai Dong, Longjiang Qu, Shaojing Fu, and Chao Li. New constructions of vectorial Boolean func-
tions with good cryptographic properties. *International Journal of Foundations of Computer Science (IJFCS)*, 23(3):749–
??, April 2012. CODEN IFCSEN. ISSN 0129-0541
(print), 1793-6373 (electronic).

Joan Daemen and Vincent Rijmen. The first 10 years of advanced encryp-
REFERENCES


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE


Dasgupta:2016:TDA


Dixon:2016:NTO

REFERENCES

[delRey:2012:EDI]

[Dini:2011:LLA]

[Dixit:2019:FBD]

[Das:2016:MPU]

[Das:2012:DPB]

[Deng:2018:SFE]
Lih-Yuan Deng, Jyh-
REFERENCES


Dachman-Soled:2014:COF


Dinis:2013:HHS


Dodos:2014:HEY


Deng:2012:VIA

Aidong Deng, Jianeng Tang, Li Zhao, and Cairong Zou. The variable-interval arithmetic coding using asymptotic de-

**Dunkelman:2012:MEK**


**Dunkelman:2012:TCC**


**Durcheva:2015:SAI**


**David:2012:PRE**


**Dorn:2012:ECE**

Dong:2012:KKD


Dong:2012:NDI


Dai:2018:OPC


Dodis:2013:O


Deng:2014:CCC


Dodis:2013:O


Dodis:2013:O
REFERENCES


REFERENCES

[102x681] 206

[206x645] Ekb

[229x645] erg:2012:AEP


[208x645] Ehdaie:2016:HCR


[219x271] Egele:2013:ESC


[208x464] Ehdaie:2016:HCR


[219x271] Egele:2013:ESC


[208x464] Ehdaie:2016:HCR


[219x271] Egele:2013:ESC

Edwards:2017:NSQ


El-Emam:2013:NSA


Eisenbarth:2010:CIP


Esiner:2016:FFB

Engels:2013:NLL
[EPAG16]


ElBansarkhani:2012:ELB
[ERLM16]


Embar:2014:PWO
[ERRMG15]

Essex:2017:DDU

Everett:2012:EC

Everett:2016:SES

Eibach:2010:OGB
Tobias Eibach, Gunnar Völkel, and Enrico Pilz. Optimising Gröbner bases

References:
REFERENCES


**Eldib:2014:FVS**


**Enos:2015:IBS**


**Fahd:2018:CPA**

REFERENCES


[Ferretti:2014:DCI] Luca Ferretti, Michele Colajanni, and Mirco

Fuglerud:2011:SIA

Fehr:2010:QC

Feigenbaum:2019:PSE

Felten:2013:LBA

Faugere:2010:CLR

Fleischmann:2012:MFA
REFERENCES

Fan:2019:OVG


Feng:2010:CTS


Farras:2012:LTM


Faugere:2014:MCA


Fan:2017:SSP


Fan:2013:CPP

REFERENCES


Fan:2010:PSN

Fan:2010:AMI

Farras:2017:IRN
Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. [FHM+12]

Faz-Hernandez:2019:HPI

Forne:2010:PAA

Fahl:2012:WEM
Sascha Fahl, Marian Harbach, Thomas Mudders,


Farash:2015:PSE


Fisher:2015:CS


Fei:2012:GTK


Fanti:2015:SVS


Fehr:2013:FCC


Fan:2013:CEM

REFERENCES

DEN ITDSEO. ISSN 1045-9219.

Fan:2014:RRS


Ferguson:2010:SHF


Feng:2012:CAO


Forler:2012:DAC


Ferrag:2018:SCN


Fallahpour:2015:AWB

REFERENCES


Faust:2014:CNM


Feng:2012:USD
REFERENCES

Ferreira:2015:LPA


Fu:2018:LUA


Fokkink:2012:TCG


Folger:2016:TQH


Fox:2013:RLQ


Faigl:2014:PEC

REFERENCES


REFERENCES

May 2016. CODEN ?????
ISSN 1559-1131 (print),
1559-114X (electronic).

[Frey:2010:ABC]

[Fri10a]

[Fri10b]

[Fri12]

[Fu:2016:EPS]

[Frauchiger:2013:TRR]

[Forbes:2015:CTC]
Michael A. Forbes and Amir Shpilka. Complexity

Fugkeaw:2018:SSA

Fang:2011:ICP

Fang:2012:CCS

Ferguson:2010:CED

Feng:2011:GDA

Fujioika:2012:SHI
[FSX12a] Atsushi Fujioika, Taichi Saito, and Keita Xa-
REFERENCES


---


REFERENCES


REFERENCES

Feng:2011:VBF


Fan:2015:IRD


[FZT14]


[FZT+12]


[FZZ+12]


Fu:2012:EHA


Fyodorov:2019:SGM

GomezPardo:2013:ICM


Gross-Amblard:2011:QPW


Grondahl:2019:TAA


Guimaraes:2019:OIQ


Gregio:2015:TTM


Gope:2018:LPP

Prosanta Gope, Ruhul Amin, S. K. Hafizul Islam, Neeraj Kumar, and Vinod Kumar Bhalla. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Future Generation Computer
Galindo:2013:NIC

Gasarch:2013:RBC

Gutierrez:2016:IDO

Gupta:2019:DRB

Gorantla:2011:MK

Guyeux:2015:ECS
Christophe Guyeux, Raphael Couturier, and Pierre-
REFERENCES


Guerin:2016:TDU


Giot:2011:UKD


Geller:2013:MIS


Gentry:2010:CAF


Gentry:2013:EMH


Gaspar:2012:SEF

Gong:2010:PCI


Grigg:2011:CCN


Garg:2016:HSS


Garg:2014:TRS


Garg:2017:IDI

Sanjam Garg, Craig Gentry, Shai Halevi, and Daniel Wichs. On the implausibility of differing-inputs obfuscation and ex-


REFERENCES

csd1/mags/sp/2014/05/msp2014050068-abs.html.


Grigoriev:2017:YMP


Gaj:2017:DCR


Guo:2010:HMW


Gouveia:2012:HSI


Guo:2018:KAA


Gorawski:2012:EAS


REFERENCES


García-Martínez:2015:HEB


García-Morchón:2015:HCR


Guo:2011:ISS


Guo:2014:SAS


Gao:2014:URA


Grossschadl: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


Green:2017:SSE

REFERENCES

Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Gupta:2018:SCA


Guha:2017:RTS


Guin:2016:FCS


Gong:2016:FSC


Gierlichs:2012:ICD

[BST12] Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael

Genkin:2013:RKE


Ge:2016:KPA


Gazi:2012:EOS


Gupta:2019:LAU


Goodrich:2011:EAD

Michael T. Goodrich, Roberto Tamassia, and Nikos Triandopoulos. Efficient authenticated data


Gorbunov:2015:ABE

Greenberg:2014:GWB

Gebotys:2016:PCP

Wang:2014:RAW

Gao:2015:GCC

Goh:2013:TOT
Weihan Goh and Chai Kiat Yeo. Teaching an old TPM new tricks: Repurposing for identity-based signatures. IEEE Se-

**Guo:2019:EER**


**Guo:2012:AKE**


**Guo:2017:EMD**


**Gao:2012:RHC**


**Guo:2018:SMK**


**Guo:2019:NTP**


REFERENCES

Hamlin:2017:NMC

Hamidi:2019:ADS

Hanyok:2012:EHH

Harn:2013:GA

Harrington:2014:GEF

Hardesty:2015:BAC

Hardesty:2016:SUC
Hastings:2016:SWS


Hayes:2013:NSA


Houmansadr:2013:BCN


Hetzelt:2017:SAE


Hernandez-Becerril:2016:GIS


Han:2019:ABI

Jinguang Han, Maoxuan Bei, Liqun Chen, Yang Xiang, Jie Cao, Fuchun Guo, and Weizhi Meng. Attribute-based information flow control. The Computer Journal, 62(8):1214–1231, August 2019. CODEN CM-PJA6. ISSN 0010-4620 (print), 1460-2067 (elec-
REFERENCES

He:2013:HEH


Hulsing:2017:XEH


Hao:2012:SAM


Hu:2017:ATE


Hwang:2010:RIB


Hsu:2011:NLM

Hore:2012:IED


Hernandez-Castro:2012:MTA


Huang:2014:FOS


Hernandez-Castro:2012:AFH


Hosny:2019:RCI

Khalid M. Hosny and Mohamed M. Darwish. Resilient color image watermarking using accu-

Han:2013:RMA

Song Han, Tharam Dillon, Vidy Potdar, and Elizabeth Chang. RFID mutual authentication protocols for tags and readers with and without a server. International Journal of Computer Systems Science and Engineering, 28(2):??, ???. 2013. CODEN CSSEEI. ISSN 0267-6192.

Heninger:2012:MYP


Hwangen:2012:ABA


Hamad:2018:DWU

REFERENCES

ISSN 1545-5963 (print), 1557-9964 (electronic).

Hellman:2017:TLC

Hermelin:2010:MLC

Herranz:2014:ABS

Herardian:2019:SUC

Hess:2012:GJC

Heys:2017:SCF

Harn:2014:MTS
REFERENCES


Yiliang Han, Xiaolin Gui, Xuguang Wu, and Xiaoyuan Yang. Proxy encryption based secure multicasting in wireless mesh networks. *Journal of Net-

[[Hoang:2014:IMD]]

[[Hoc:2013:COU]]

[[Hua:2016:EDP]]

[[Heyse:2012:TOC]]

[[Huang:2014:IMD]]

[[HFT16]]

[[HG12]]

[[HGT15]]

[[HG12]]

[[HGT15]]

[[HGWY11]]
REFERENCES


Harn:2015:DTS


Hu:2016:EWS


Huber:2019:FCL


Hammi:2018:BTD


Hayashi:2013:AEI


Huber:2014:TPW

[MHMK14] Stefan Huber, Martin

**Huang:2017:BBC**


**Haitner:2011:PRI**


**Hinarejos:2015:MES**


**Hao:2019:IDP**

REFERENCES

Hinek:2010:CRV


Harb:2019:FIE


Hinkelmann:2011:CPA


Hur:2014:SDR


Hasan:2017:UAF


Hussain:2018:PPP


Handa:2019:SES

[HKA19] Rohit Handa, C. Rama Krishna, and Naveen Ag-

**Houmansadr:2014:NBW**


**Hur:2013:REC**


**Heyse:2012:LEA**


**Heil:2014:APH**


**Howe:2018:PDG**


REFERENCES


Yupu Hu, Zhizhu Lian, Jiangshan Chen, Baocang Wang, and Shanshan Zhang. Algebraic attacks against several weak variants of GVW 13 ABE.
REFERENCES


**REFERENCES**

[Huffman:2010:SPR]

[Herranz:2011:RBS]

[Huhang:2015:CEA]

[Howard:2010:DSS]

[Hohenberger:2012:DDQ]

[Huang:2014:SW]
Hefeeda:2010:ASM

Herzberg:2012:TJA

Hwang:2019:BBR

Hore:2012:SMR

Hoang:2012:ESB

Hirt:2014:BA

Harnik:2010:CIC
Danny Harnik and Moni Naor. On the compressibility of $NP$ instances and cryptographic applications. *SIAM Journal
REFERENCES

Hodgson:2019:SSC


Hofmann:2015:LBQb


Hofmann:2016:LBQb


Hollings:2012:CCE


Horsman:2019:CPE


Hyla:2012:CBE


Hazay:2014:OSA

Carmit Hazay and Arpita Patra. One-sided adap-
REFERENCES

com/chapter/10.1007/978-3-642-54242-8_16/.

Halder:2010:WTR


He:2012:ECT


Hadlington:2019:ERW


Hurrah:2019:DWF


Howe:2015:PLB

REFERENCES


Jinsong Han, Chen Qian, Panlong Yang, Dan Ma, Zhiping Jiang, Wei Xi, and Jizhong Zhao. GenePrint: generic and accurate physical-layer identification for UHF RFID tags. IEEE/ACM Transactions on Networking, 24(2):846–858, April 2016. CODEN IANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).


Andreas Hülsing, Lea Rausch, and Johannes Buchman. Optimal parameters for XMSS$^{MT}$. Lecture Notes in Computer Science, 8128:194–208, 2013. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-
REFERENCES


Huang:2014:AFS


Hussain:2018:SSH


Herranz:2013:SMS


Hulsing:2016:MMT


Haitner:2010:EIC


Hwang:2011:CD

REFERENCES

Hubballi:2018:NTC

Homma:2014:TFD

Halevi:2011:TBH

Han:2013:IBD

Han:2014:IBS

Han:2012:PPD

Heather:2014:CPE
James Heather, Steve Schneider, and Vanessa Teague. Cryptographic protocols with everyday objects. *Formal Aspects
REFERENCES


REFERENCES


REFERENCES

(Fprint), 1557-735X (electronic).

Han:2012:MIA


Hammad:2019:PSF


Hwang:2011:NIB


Holbl:2010:TP1


Holbl:2012:ITP


He:2016:STI

REFERENCES


[He:2015:SSQ] Zhian He, Wai Kit Wong, Ben Kao, David Wai Lok Cheung, Rongbin Li, Siu Ming Yiu, and Eric Lo. SDB: a secure query processing system with data interoperability. Proceedings of the VLDB Endowment, 8(12): 1876–1879, August 2015. CODEN VLDBFR. ISSN 2150-8097.


Hao:2011:NTV


Huang:2018:CT


Huang:2011:IBS


Heys:2011:PSC


Han:2012:ERI


Huang:2011:IBS

Qi Han, Yinghui Zhang, Xiaofeng Chen, Hui Li,

**Han:2018:ERA**


**Huang:2019:ILA**


**Han:2014:ATS**


**He:2017:AHA**


**He:2018:LAB**

Qian He, Ning Zhang, Yongzhuang Wei, and Yan Zhang. Lightweight attribute based encryption scheme for mobile cloud as-
he:2015:iei


Hunt:2018:RDS


Islam:2015:MBA


Ibrahim:2019:RAM


Ismail:2010:EAE

I. A. Ismail, M. Amin, and H. Diab. An effi-


 REFERENCES


REFERENCES

Imai:2015:IRR


Islam:2015:LFP


Ioannou:2014:PKC


Intel:2019:IAM


Isobe:2012:SCL

Islam:2018:REP


Irshad:2016:EAM


Isobe:2012:SAL


Ishai:2014:PCP


Jacobs:2016:STB

Jie:2010:AAI

Jie:2011:RGA

Jho:2016:SSE

Jakobsson:2012:AWD

Chang:2012:TRR


Jiang:2014:UIS


Jiang:2014:TEA


Jiang:2016:MAC


Jiang:2017:BMA


Jin:2010:ADW


Jain:2010:QP

Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP =
PSPACE. Communica-
tions of the Association
for Computing Machinery,
53(12):102–109, December
2010. CODEN CACMA2.
ISSN 0001-0782 (print),
1557-7317 (electronic).

Jawad:2013:GAD

Khurram Jawad and Asi-
fullah Khan. Genetic algo-
rithm and difference expan-
sion based reversible wa-
termarking for relational
databases. The Journal
of Systems and Software,
86(11):2742–2753, November
2013. CODEN JS-
SODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0164121213001428.

Jamil:2018:SPU

Fuzel Jamil, Abid Khan,
Adeel Anjum, Mansoor
Ahmed, Farhana Jabeen,
and Nadeem Javaid. Se-
cure provenance using an
authenticated data struc-
ture approach. Computers &
Security, 73(??):34–
56, March 2018. CODEN
cpseed. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167404817302122.

Jan:2019:PBM

Mian Ahmad Jan, Fa-
zullah Khan, Muhammad
Alam, and Muhammad Us-
man. A payload-based mu-
trial authentication scheme
for Internet of Things. Fu-
ture Generation Computer
Systems, 92(??):1028–1039,
March 2019. CODEN FG-
SEVI. ISSN 0167-739X
(print), 1872-7115 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167739X17303898.

Jun:2012:IIR

Jong Yun Jun, Kunho Kim,
Jae-Pil Heo, and Sung eui
Yoon. IRIW: Image re-
trieval based image wa-
termarking for large-scale
image databases. Lecture
Notes in Computer Sci-
CODEN LNCS09. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-32205-1_12/.

Jiang:2016:PPT

Qi Jiang, Muhammad Khur-
ram Khan, Xiang Lu, Jian-
feng Ma, and Debiao He.
A privacy preserving three-
factor authentication pro-
tocol for e-Health clouds.
The Journal of Supercom-
puting, 72(10):3826–3849,
October 2016. CODEN
josued. ISSN 0920-8542
(print), 1573-0484 (elec-
tronic). See comments
[IC17].
Jovanovic:2012:FAL


Josefsson:2016:ECD


Jordan:2018:QCS


Jeong:2012:IKP


Jajoedia:2012:RET


Jia:2012:PKD


Jiang:2019:PPP


REFERENCES

Johnson:2015:NGA

Jou:2013:NIC

Juels:2014:HEE

Jaiyeola:2018:IPN

Jevdjic:2017:ASC
Jain:2016:APQ


Judmayer:2017:BCI


Jiang:2018:CPA


Jiang:2012:DCA


Y. Jiao, P. Wang, D. Niyato, and K. Suankaew-

**Jin:2015:NCD**


**JXLZ15**

**Jan:2019:SEE**


**JY14**


**JY14**

Shahram Khazaei and Siavash Ahmadi. Ciphertext-only attack on $d \times d$ Hill in $O(d^{34})$. *Information Pro-

**Khazaei:2017:COA**


REFERENCES

Kapera:2013:MRM  

Karafyllidis:2012:QGC  

Kong:2015:CSM  

Katz:2013:RIB  

Kawamoto:2015:LSH  

Karthigaikumar:2010:PPV  

Kallel:2011:SMM  
REFERENCES

**Kleinrouteweler:2017:SAP**


**Kim:2011:SSE**


**Koz:2012:ASE**


**Kraetzer:2012:PCS**


**Karakoc:2013:BCL**


**Karakoc:2015:AKA**

Kumari:2017:DSU


Kara:2019:ALS


Keblusek:2015:BRK


Kemshall:2011:WMT


Kleinjung:2010:FBR


Kikuchi:2012:SSN

Ryo Kikuchi, Atsushi Fujikura, Yoshiaki Okamoto,


Khazaei:2010:NBS


Kastner:2010:AOT


Kim:2014:MBM


Khalil-Hani:2013:BEB


Kim:2016:EPE


Kai:2011:CIS

Kiayias:2011:TCC


Kompara:2019:REM


Kim:2015:CEH


Kim:2016:MAS


Kim:2011:LBA


Khan:2016:BSW


Muhammad Khurram Khan, Saru Kumari, and Mridul K.
REFERENCES


Karopoulos:2010:FIP


Kim:2018:EPP


Kubota:2016:SAV


Kim:2018:EDC


Khan:2013:EDC

Abdul Nasir Khan, M. L. Mat Kiah, Sajjad A. Madani, Atta ur Rehman Khan,

**Khan:2014:IPR**


**Kushwah:2011:EIB**


**Khakpour:2013:ITA**


**Klapper:2010:PSS**


**Ko:2010:MME**

Kim:2019:AAI


Koeberl:2012:EPD


Kumari:2016:UFM


Kent:2015:AGA

Keller:2010:DAS

Khomejani:2010:PCT

Koblitz:2010:BNW

Kiani:2011:MPD

Kifer:2014:PFM

Koblitz:2015:RWE

Koblitz:2016:RWE
Neal Koblitz and Alfred

**Kasamatsu:2012:TSE**


**Kandi:2017:ELC**


**Kline:2018:CAR**


**Kiyoshima:2014:CRB**


**Karger:2011:LLB**

REFERENCES


[KO16] Shipra Kumari and Hari Om. Authentication protocol for wireless sensor networks applications like safety monitoring in coal
Koblitz:2010:BRB


Kasper:2012:SCA


Khamsemanan:2016:BBU


Kawachi:2017:GCR


Kollmitzer:2010:AQC


Kang:2012:AKM

Hyun-Sun Kang and Chang-Seop Park. An authentication and key management scheme for the

**Kolman:2017:SCG**


**Koya:2018:AHM**


**Kumar:2017:TAU**


**Kiltz:2011:EAH**


**Khalid:2016:RHL**

REFERENCES

Kocabaş:2012:CPB

Kang:2016:DSA

Kesselink:2010:IWD

Krenn:2013:CCR

Knudsen:2011:BCC

Krantz:2012:EAM
REFERENCES


[King:2011:BBB] Valerie King and Jared Saia. Breaking the \(O(n^2)\) bit barrier: Scalable Byzantine agreement with

**Kolesnik:2012:LPP**


**Kumar:2015:RGB**


**Karthiga:2018:PSA**


**Korac:2019:FMU**


**Kocabas:2016:ESM**


**Khan:2017:TPK**

REFERENCES

Kiljan:2017:SAC [KSD+17]

Kwon:2018:EIP [KSH18]

Ksiezopolski:2012:QMQ [Ksi12]

Kim:2012:SSS [KSSY12]

Klingler:2013:UPT [KSU13]

Kim:2012:SAH [KTA12]
Kawachi:2012:SKE

Kobayashi:2016:ASC

Klisowski:2012:CCP

Kai:2014:FSD

Kupcu:2013:DTT

Kupcu:2015:OAS
REFERENCES


Kuznetsov:2011:APP


Kshetri:2018:BEV


Kiljan:2018:EVA


Karpovsky:2014:DSS


Kuo:2016:SDD


Koyama:2012:NTD


Liang:2015:SEC


Langley:2013:EDC


Landau:2017:LCI


Launchbury:2012:TBC


Lauter:2017:POL

REFERENCES

Liu:2013:PAE


Luo:2012:ESI


Lupu:2012:IBK


Lu:2015:CSA


Liu:2013:CSA


Laxmi:2017:GGS

B. Prathusha Laxmi and A. Chilambuchelvan. GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks. *Future Generation Computer*
Liu:2013:IAG


Lathrop:2011:SPI


Li:2015:NAC


Lee:2017:SUE


Liu:2019:TTR


Liu:2019:VP


Lamo-Fernandez:2014:NAA


Luo:2019:SCT

REFERENCES


**Lopez-Garcia:2014:PBB**


**Li:2014:SCA**


**Liu:2012:FVC**


**Lee:2010:ISC**


**Lee:2010:CGC**

REFERENCES

Li:2010:EBB


Lin:2011:NIB


Lee:2011:IMS


Lertvoratham:2012:ISM


Lee:2011:PSE


Liao:2013:NMS


**Lenstra:2012:RWW**


**Lum:2016:QEM**


**Li:2012:BVS**


**Lin:2011:ICA**


**Lin:2018:BBB**

REFERENCES

Li:2010:AIS

Li:2014:SOA

Liu:2015:SSP

Lerc-Hostalot:2013:LMS

Lian:2014:SSA
Yanling Lian, Xinyi Huang, and Yi Mu. SA³: Self-adaptive anonymous authentication for dynamic authentication policies. *Future Generation Computer Systems*, 30(??):133–139, January 2014. CODEN


Liu:2016:LCP


Liu:2016:LCP

Li:2017:MMA


Li:2017:MMA

Liu:2019:ICA


Liu:2019:ICA

Li:2012:OEA


Li:2012:OEA

LJ16


LJ16

Li:2014:STC

Aron Laszka, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme. Secure team


REFERENCES


REFERENCES


Liu:2018:VSE


Li:2018:CIE


Li:2010:DCY


Lai:2013:SAS


Libert:2019:ZKA


Lu:2012:IEC

Xianhui Lu, Bao Li, Qixiang Mei, and Yamin Liu. Improved efficiency of cho-
REFERENCES

You can refer to the following references for more detailed information:

[LCS12] Lai:2018:EQU

[LPP+18] Lai:2018:EQQ

[LLW16] Lai:2018:EQK

[LWA16] Lai:2018:EQP

[LHY+12a] Lai:2018:EQR
Luo:2012:FSI


Lee:2015:SAS


Li:2018:WMH


Lu:2012:BBE


Lai:2016:GGB


Li:2017:CBS

[LL+17] Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su, Liang He, Kui Ren, Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su, Liang He,


*Li:2011:NRA* [LMJC11] Guangsong Li, Jianfeng Ma, Qi Jiang, and Xi Chen. A novel re-authentication scheme based on tickets in wireless local area net-

Lv:2013:NTP


Li:2013:ESC


Lv:2013:NTP


[LNKL13] Xiong Li, Jianwei Niu, Muhammad Khurram Khan, and Junguo Liao. An enhanced smart card based remote user password authentication scheme. *Journal of Network and Com-

**Liu:2015:SAB**


**Liu:2013:GPB**

Loeb:2015:MGM


Lopriore:2012:EPP


Lopriore:2015:PCR


Lopriore:2015:PMD


Low:2012:BRB


Lin:2011:CRN


Ling:2012:SHS

REFERENCES


Lukowiak:2014:CEB

Liskiewicz:2013:GBS

Liskiewicz:2017:SLS

Lane:2014:PBD
Julia I. Lane, Victoria...


REFERENCES


[LTC+15a] Chiao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang, Wang-Jui Tsai, and Pokai Zhong. Implementing multiple biometric features for a recall-based graph-

**Liu:2015:MSG**


**Li:2015:FSC**


**Lao:2016:BFD**


**Lysyanskaya:2010:AEC**


**Lin:2011:CNS**

REFERENCES

UK / etc., 2011. CODEN LNCS9D. ISBN 3-642-25512-4. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-25512-0

Li:2016:LRC

Ludge:2012:NLD

Lucchese:2010:RPT

Lafitte:2011:CBF

Liu:2010:CIE
REFERENCES

www.sciencedirect.com/science/article/pii/S0898121110001938


CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/59/7/983.


CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

(Li:2018:SCM) Xiong Li, Fan Wu, Muhammad Khurram Khan, Lili

Li:2019:PSA


Liu:2010:NDC


Liu:2010:SET

REFERENCES


Liu:2011:PIA


Lu:2012:MMA


Li:2010:GCP


Lou:2010:NAS


Luo:2012:ICB

Li:2012:IIA


Lin:2010:DSM


Li:2011:NIW


Li:2014:IBD


Li:2014:EMK


Lai:2012:RHB

REFERENCES


Liao:2012:NSM


Liao:2010:MPC


Lai:2019:NIB


Liu:2018:SKR


Li:2013:SSS


Luo:2012:LVT


Liu:2014:PKE


Liu:2017:ESS


Liu:2014:CRA


Li:2010:PES


Stefan Mangard. Keeping secrets on low-cost chips.
REFERENCES


[Matthiessen:2019:RCM] Dana Matthiessen. The rise of cryptographic metaphors in Boyle and their use for the mechanical phi-
Maurer:2012:CCN


Mayron:2015:BAM


Mazurczyk:2013:VSD


Milo:2011:FGB


Mao:2015:PUA


Matias:2018:NNZ

Malone:2013:MOD


Migliore:2018:PPF


Massolino:2015:OSC


Mukhopadhyay:2011:PEA


Madanayake:2012:BPS


McGrew:2017:IDH

McGrayne:2011:TWH


McKay:2012:SLC


Ma:2019:TOP


Mahmood:2018:ECC

Marquez-Corbella:2015:ECP


Mhenni:2019:DSA


Mathew:2015:NMB


Mansouri:2012:ACA


Mansfield-Devine:2015:MIC

REFERENCES

www.sciencedirect.com/
science/article/pii/S1353485815700103

Murdoch:2010:CPB


Malina:2018:SET


Mosenia:2017:PTS


Maachaoui:2012:MLA


Meiklejohn:2010:BRB


Menezes:2013:IPB

Alfred Menezes. An introduction to pairing-based cryptography. Report, Department of Mathematics, University of Waterloo, Waterloo, ON,


Wenjuan Meng, Jianhui Ge, and Tao Jiang. Se-

**Marmol:2010:TPA**


**Matsuda:2014:CCS**


**Miller:2014:ADS**


**Mou:2013:CBC**


<table>
<thead>
<tr>
<th>REFERENCES</th>
<th>366</th>
</tr>
</thead>
</table>
Muller:2012:HPC


Mozaari-Kermani:2017:FDA


Mozaari-Kermani:2018:ERE


McGrew:2016:SMH


Malik:2012:AIC


Marconato:2013:VLC

G. Vache Marconato, M. Kaâniche,

**Mozaffari-Kermani:2010:CSI**


**Montecchi:2012:QSE**


**Mancillas-Lopez:2010:RHI**


**Mendez:2016:PES**


**Manzanares-Lopez:2012:ICU**


Maity:2017:ODC

Mulholland:2017:DCD

Maeng:2015:TAU

Moldovyan:2012:BBD

Mahmood:2014:PPK

Marino:2019:ACN


Chandrashekar Meshram, Suchitra A. Meshram, and Mingwu Zhang. An ID-based cryptographic mech-

**Moran:2010:BCP**


**Mukhopadhyay:2014:EMP**


This paper provides a correction to the algorithm presented in [?], and also supplies a complicated correctness proof.

**Monz:2016:RSS**


**McKusick:2015:DIF**


**Minier:2012:RKI**

REFERENCES

Mizuki:2011:ASN

Maimut:2012:LCR

Minamoto:2014:BDI

Mone:2013:FPE

Moore:2012:RFF

Moody:2014:DMW

Morad:2012:OEA
REFERENCES


[Miglioire:2018:HSC] Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Ar-

**Moataz:2018:SSE**


**Martinovic:2017:AUP**


**Matsumoto:2017:ACG**


**Moghadam:2010:DRN**


**Mendel:2012:DAL**

[Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varici. Differential analysis of the LED

**Maitra:2012:NAC**


**Mroczkowski:2012: CAS**


**Maitra:2013:DSM**


**Maitra:2013:HEM**


**Maitra:2013:HPM**


**Miller:2016:RPS**

REFERENCES


REFERENCES

Martins:2018:SFH


Muhammad:2018:ISU


Migliore:2017:HSA


Miret:2018:PBC


Mosca:2013:QKD


Morozov:2012:ZKP

Mouris:2018:TSB


Malkin:2011:ECS


Meerwald:2012:ERW


Muftic:2016:BCC


Mundy:2017:CGU


Murphy:2010:BRB

REFERENCES

CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [?, ?].

Murdoch:2016:IDP


Miri:2012:SAC


Min:2016:RSC


Mishra:2016:AFP


Modersheim:2018:ABP


Mefenza:2019:CSA

Thierry Mefenza and Damien Vergnaud. Cryptanalysis of server-aided RSA protocols with private-key splitting. The Computer Jour-
Mannan:2011:LPD


Maes:2012:PFF


Mahmood:2013:LEZ


Mathew:2012:EIC


Ma:2012:CIS


Ma:2013:PVP


Marko:2017:MDI


Mastroeni:2017:APS


Manshaei:2013:GTM


Ma:2015:PKE


Mofrad:2018:CSI


Nagy:2010:OTP

Nagy:2010:QCS


Naccache:2012:CST


Naccache:2016:FHE


Naranjo:2012:SAK


Nunez:2017:PRE


Namasudra:2019:IAB

Suyel Namasudra. An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency
REFERENCES


Noureddine:2013:AMT


Nain:2017:SPE


Naskar:2012:FIR


Naskar:2013:GTL


Naranjo:2013:FDA

Ni:2013:EIB


**NdMMW16**


**Ngo:2017:CSS**


**Nedjah:2016:PYP**


**Newell:2013:PCD**


**Nejatollahi:2019:PQL**


REFERENCES


REFERENCES


REFERENCES

Nguyen:2017:DPA


Niksefat:2014:ZPP


Nandakumar:2017:CAI


Nguyen:2012:LRS


Nguyen:2010:LAS

REFERENCES


Ben Niu, Xiaoyan Zhu, Qinghua Li, Jie Chen, and


Onica:2016:CPP


Oliynykov:2015:NES


Ou:2010:CPA


Ogiela:2018:EBI


Oliveira:2012:STA


Ortiz-Martin:2019:FAI

REFERENCES


Obert:2016:PAE

REFERENCES

[Rolf Oppliger:2011:CC]

[Jorge Luis Orejel:2014:ENIGMA]

[Jim Ormond:2016:CPR]


[Emma Osborn and Andrew Simpson:2016:SSR]


REFERENCES


Park:2012:APO


Park:2018:OTP


Pass:2013:USP

REFERENCES


REFERENCES

Pun:2014:GIT


Paul:2016:TSO


Papadopoulos:2014:LQA


Premnath:2014:EHR


Poh:2017:SSE


Pang:2014:PPA


Peterson:2011:SWS

Petrlic:2012:PRE

Pfleeger:2010:CJD

Peinado:2012:CAT

Poppelmann:2012:TEA

Peng:2010:SFW
REFERENCES


REFERENCES


Pointcheval:2012:ACE


Patel:2018:LLA


Premaratne:2015:LDD


Pramila:2018:ICA

REFERENCES

www.sciencedirect.com/science/article/pii/S0164121217302522

Peter:2012:AHE


Phuc:2016:SAS


Perez:2011:FDS


Peris-Lopez:2018:EAC


Pang:2013:IMA


Peris-Lopez:2010:CSP

Pedro Peris-Lopez, Enrique San Millán, Jan


Niu:2014:RDW


Powers:2014:OSCa


Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC


P:2018:ABE


Pereira:2016:SHB

[PPB16] Geovandro C. C. F. Pereira, Cassius Puodzius, and Paulo S. L. M. Bar-
REFERENCES


**Pendl:2012:ECC**


**Pyun:2012:IBF**


**Pathak:2012:PPS**


**Phan:2012:DDB**


**Phan:2012:MBT**

Papadopoulos:2015:PAP


Pandey:2012:PPS


Piret:2012:PBC


Perez-Resa:2019:SSE


Puthal:2019:SAL


Polyakov:2017:FPR

[Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntanathan. Fast proxy re-encryption for publish/subscribe sys-

**Popa:2012:CPQ**


**Priemuth-Schmid:2012:ASV**


**Permpoonthanalarp:2014:FTG**


**Perazzo:2015:DRL**


**Pereira:2013:SLC**


**Phatak:2013:SIN**

Dhananjay Phatak, Alan T.

Patranabis:2017:PSK


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Pankhuri:2019:PBM


Papamanthou:2013:SCC

Papakostas:2014:MBL

Pudovkina:2012:RKA

Paletov:2018:ICA

Papamanthou:2016:AHT

Padget:2017:FGA

Pellikaan:2017:CCC
REFERENCES


[PYM+13] Pieter Philippaerts, Yves

Pei:2015:SWT


Papadopoulos:2010:CAR


Phuong:2018:CBE


Pournaghi:2018:NNE


Patsakis:2015:PSM


Qiu:2019:CPT


Qiu:2017:AAS


Qiu:2017:PSB


Qiao:2018:CTC


Quaglia:2018:SVA


Qin:2016:STI

[QYWX16] Zhen Qin, Chen Yuan, Yilei Wang, and Hu Xiong. On the security of two identity-based signature schemes based on pair-
Qian:2014:IAF


Qiang:2016:SCF


Qi:2016:SID


Qi:2016:SPR


Qin:2018:BRO


Rabin:2010:ACC

Tal Rabin, editor. *Advances in cryptology — Crypto 2010: 30th annual cryptology conference*, Santa Barbara, CA, USA,


[RBP+18] Jean Louis Raisaro, Gwang-bae Choi, Sylvain Pradervand, Raphael Colsenet, Nathalie Jacquemont, Nicolas Rosat, Vincent Mooser, and Jean-Pierre Hubaux. Protecting privacy and security of genomic data in i2b2 with homomorphic

**Rabbachin:2015:WNI**

**Rao:2017:CFA**

**Ren:2016:IBE**

**Reardon:2016:SDD**

**Reeve:2015:ARC**

**Ren:2010:CSH**
Yanli Ren and Dawu Gu. CCA2 secure (hierarchical) identity-based parallel key-insulated encryption without random or-
REFERENCES


Oded Regev and Bo’az Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In ACM [ACM11], pages 31–40. ISBN ????. LCCN ????. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..


Aniket Roy, Arpan Kumar Maiti, and Kuntal Ghosh. An HVS inspired robust non-blind watermarking scheme in YCbCr
REFERENCES


REFERENCES


Rhee:2010:TSS


Ren:2015:ASE


Rawat:2011:CBR


Razaque:2016:TDP


Razaque:2017:SDA


Rosen:2010:CCS


Reeder:2011:WPD

[102x681] Robert W. Reeder and Stuart Schechter. When

**Rivest:2014:SSR**


**Rossi:2015:IBS**


**Rana:2016:DBV**


**Roy:2017:LOS**


**Roetteler:2018:QCC**


**Rangasamy:2012:ERP**


Ren:2018:IAS


Rastegari:2019:ECS


Ribeiro:2015:QBS


Resende:2019:BMI


Ruj:2014:DA

Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak. Decentralized access control with anonymous authentication of
data stored in clouds. 


**Rahulamathavan:2019:PPI**


**Rahulamathavan:2016:UCA**


**Rajalakshmi:2019:BEC**


**Russo:2015:FPT**

Alejandro Russo. Functional pearl: two can keep a secret, if one of them uses Haskell. ACM SIGPLAN Notices, 50(9):280–288, September 2015. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

**Ryan:2015:EEVb**

[RVSCM12] Juan José Rodríguez-Vázquez, Sixto Romero-Sánchez, and Miguel Cárdenas-Montes. Speeding up a chaos-based image encryption algorithm using GPGPU. Lecture Notes
REFERENCES 429


Reaves:2018:CSS


Roettger:2012:PKC


Ren:2014:HHM


Rogaway:2012:SCS


Ren:2013:PPK


Ristenpart:2010:WGR

Thomas Ristenpart and Scott Yilek. When good randomness goes bad: Virtual machine

Ren:2013:DSE


[Rajendran:2015:FAB


[Sang:2012:SSF


[Sakalli:2014:ACC


[Somanatha:2015:RAK

REFERENCES


[SAAB10] Simon Schütz, Henrik


[SAJL16]


[Sac14]


[Sahai:2013:TCT]


[Saled:2016:PED]

Eyad Saleh, Ahmad Alsa’deh, Ahmad Kayed, and Christoph Meinel. Processing over encrypted data: Between theory and practice. SIGMOD Record (ACM Special Interest Group on Management of Data), 45(3):5–16, September 2016. CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

[Sadat:2019:SSG]

ITCBCY. ISSN 1545-5963 (print), 1557-9964 (electronic).


Safkhani:2017:PSD


Shwartz:2018:DMI


Stevens:2017:AFS


Safkhani:2012:SMA


Santos:2014:ACD


Shyu:2010:VMS


Srinivasan:2012:RAP

Avinash Srinivasan and


Bruce Schneier. Liars and outliers: enabling the trust


REFERENCES

blog/2015/3/13/part_2_bruc_schneier_on_the

Schneier:2016:CHT


Schneier:2018:CAA


Schneier:2019:CPI


Shrestha:2010:KBA


Stobert:2018:TAL


Seberry:2010:CTAa


Seberry:2010:CTAb

REFERENCES


Scriber:2018:FDB


Smith-Creasey:2019:NWI


Shu:2015:PML


Saleh:2010:GTF


Shen:2012:PAS


Shakiba:2010:IID

Souissi:2012:OCP

Shakiba:2014:CCI

Seo:2014:RHI

Salman:2018:BMM

Sasaki:2012:IKK
Staples:2019:SAB


Sendrier:2010:PQC


Sendrier:2017:CBC


Seo:2018:CSI


Serrato:2012:IAN


Sallam:2012:EBM

Sakai:2016:CDN

Sethumadhavan:2016:HEP

Severance:2016:BSB

Savas:2014:SMQ

Su:2012:IIN
Shabtai:2010:SAP


Schneier:2015:SWC


Sasdric:2015:ICS


Shu:2014:DAS


Saxena:2016:API


Silva-García:2018:SBG

www.sciencedirect.com/science/article/pii/S009630031830184X.


Shankar:2012:BDF

Sun:2017:PKE

Sipiran:2014:SCA

Shaolan:2011:EDE

Seyedzadeh:2011:IEA

Song:2015:ADT


**Shparlinski:2010:NWP**


**Suorananta:2012:ASM**


**Shyu:2015:VCR**


**Satir:2012:CBT**


**Siad:2012:NAP**


**Simion:2015:RST**

Simmonds:2015:DII  [Sim15b]

Sirer:2016:TPS  [Sir16]

Shakeri:2012:RZW  [SJ12]

Seo:2018:CIA  [SJLK18]

Shin:2017:CGI  [SJWH17]

Sherman:2019:OVB  [SJZG19]
REFERENCES


REFERENCES

Soupionis:2014:GTA

Sirivianos:2014:LSF

Seo:2015:AEC

Shin:2017:SSD

Szalachowski:2010:CCG

Stevens:2015:FCF


Voundi Koe Arthur Sandor, Yaping Lin, Xielhua Li, Feng Lin, and Shiweng Zhang. Efficient decentralized multi-authority attribute based encryption for mobile cloud data

**Somani:2010:IDS**

U. Somani, K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. In Chaudhuri et al. [CGB+10], pages 211–216. ISBN 1-4244-7675-5. LCCN ???

**Sun:2016:RSP**


**Shao:2012:AKP**


**Sarkar:2010:CRM**


**Sarkar:2010:CRT**


**Sorniotti:2010:PSS**

Seyedzadeh:2011:IES


Sengupta:2012:SAI


Sencar:2013:DIF


Swami:2018:AAS


Smart:2016:CMS


Stanton:2010:FAD

Paul T. Stanton, Benjamin McKeown, Randal

**Salmon:2011:PRN**

John K. Salmon, Mark A. Moraes, Ron O. Dror, and David E. Shaw. Parallel random numbers: as easy as 1, 2, 3. In Lathrop et al. [LCK11], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ???

**Salmon:2011:SSX**


**Salmon:2011:RBA**


**Salmon:2011:DBP**


**Swierczynski:2015:PSE**


**Stankovski:2014:CFE**

REFERENCES


REFERENCES


Safa-Naini:2011:USC

Seyedzadeh:2014:RCI

Suriadi:2012:PCV

Schaumont:2015:IEP

Suresh:2015:AGU

Serwadda:2013:ELK
Abdul Serwadda and Vir V. Phoha. Examining a large keystroke biometrics dataset for statistical-

**Shiaeles:2015:FII**


**Shim:2015:SDA**


**Spafford:2016:SE**


**Sherman:2019:PBL**


**Skracic:2017:AAU**


Arijit Sur and Vignesh

Stanton:2014:BRB

Singh:2017:SCB

Stefan:2012:ACT

Sutar:2017:DPI

Sluaganovic:2018:ARE
Sethumadhavan:2012:CHD


[SRT12]

Saklikar:2010:IFV


[SS10a]

Saxena:2010:SGC


[SS10b]

Sopka:2010:BTS


[SS10c]

Szaban:2011:IQB


[SS11]

Saxena:2012:BIT


[SS12a]
Shparlinski:2012:CSD


Sendrier:2013:HCE


Sadhya:2017:PRE


Siegel:2019:UOC


Singh:2013:QBF


Smith:2011:SMC


Spiez:2012:RCT


Sahai:2012:DCC


Schillewaert:2014:CCA


Shen:2016:RMM


Sethumadhavan:2019:SA


REFERENCES


REFERENCES


Shen:2015:CSC


Song:2016:IAR


Shmueli:2014:IDE


Svozil:2014:NCC


Svaba:2010:PKC


ShanmugaPriya:2019:PAS


Le-Tian Sha, Fu Xiao, Hai-Ping Huang, Yu Chen, and Ru-Chuan Wang. Catching escapers: a detection method for advanced persistent escapers in industry

**Su:2016:PSN**


**Sahillioğlu:2014:SCM**


**Savas:2015:GMA**


**Shao:2015:SAS**


**Song:2017:SSI**


**Seo:2013:PIC**

Jae Woo Seo, Dae Hyun Yum, and Pil Joong Lee. Proxy-invisible CCA-

Song:2017:SAM


Shuai:2019:AAS


Shen:2017:RDP


Sui:2014:DAH


Shah:2019:PCB

Shi:2013:REA


Sun:2017:CPP


Shen:2014:ERC


Tsang:2010:BRR


Tamayo:2015:AFH

Matthew Tamayo. Algebraic full homomorphic

Tan:2011:CTA


Tan:2012:SLM


Tan:2012:LCP


Tang:2015:ETE


Tang:2015:HAC


Tankard:2017:BNK


REFERENCES


[Tan:2017:JDC] Rui Tan, Sheng-Yuan Chiu, Hoang Hai Nguyen, David K. Y. Yau, and De-

**Tian:2014:DFS**


**Tiplea:2014:NSC**


**Tao:2013:SMS**


**Terai:2011:BRB**


**Tseng:2019:AMR**

REFERENCES


Zhaohui Tang, Hoon Wei Lim, and Huaxiong Wang. Revisiting a secret sharing approach to network codes. *Lecture Notes in
REFERENCES

Tsay:2012:VUL

Tsoutsos:2018:EDM

Tang:2015:ECP

Tormo:2013:IMP

Terrovitis:2011:LGR

Terrovitis:2012:PPD
Manolis Terrovitis, Nikos Mamoulis, John Liagouris, and Spiros Skiadopoulos. Privacy preservation by
REFERENCES


Tao:2018:AAC


Tomb:2016:AVR


Toxen:2014:NSS


Tsougenis:2012:PEM


Tan:2016:BIB


Tang:2014:PAB

Ming Tang, Zhenlong Qiu, Weijie Li, Weijin Sun, Xiaobo Hu, and Huangguo Zhang. Power analysis


REFERENCES

July 2011. CODEN JS-SODM. ISSN 0164-1212.


REFERENCES

Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG


Toor:2018:VQA


Tartary:2011:EIT


Tian:2012:SSB


[uHAN+18] Muhammad Ehatisham ul Haq, Muhammad Awais Azam, Usman Naeem, Yasar Amin, and Jonathan Loo. Continuous authentication of smartphone users based on activity pattern


REFERENCES

Viennot:2014:MSG

Vu:2015:NAN

Vasiliadis:2017:DIS

Vleju:2012:CCA

Vivek:2014:CSC

Vliegen:2015:SRD
Velooudis:2016:NPH


Vollala:2017:EEM


VonMaurich:2015:IQM


Varadharajan:2018:AUR


Vembuselvi:2011:LLL


Vassilev:2016:ESU


REFERENCES

Valente:2019:SSA


Wagstaff:2010:C


Wagner:2016:TPF


Woo:2019:UEM


Walter:2018:RCS


Wang:2010:NSB

REFERENCES


REFERENCES

[Watts:2014:ICB]

[Watts:2014:PYI]

[Watts:2015:HGA]

[Wang:2012:PCE]

[Weisse:2017:RLC]

[Wright:2010:USP]

[Wu:2018:ESS]
Libing Wu, Biwen Chen, Kim-Kwang Raymond Choo, and Debiao He. Efficient and secure search-

[Wang:2018:SSEA]


[WCFW18]


[Wei:2018:GCQ]

Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and Athanasios V. Vasilakos. Design of secure key management and user authentication scheme for fog computing services. *Future Generation Computer


REFERENCES


**Wang:2010:DVT**

Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deter-
ring voluntary trace disclosure in re-encryption mix-
18:1–18:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-
7406 (electronic).

**Wang:2012:BRR**

Ding Wang, Chun guang Ma, Sen dong Zhao, and Chang li Zhou. Break-
ing a robust remote user authentica-
tion scheme using smart cards. *Lecture Notes in Computer Sci-
ence*, 7513:110–118, 2012. CODEN LNCSDO. ISSN 0302-9743 (print), 1611-
3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-
3-642-31540-4_9/.

**Wang:2012:SPB**

Ding Wang, Chun guang Ma, and Peng Wu. Secure password-based remote
user authentication scheme with non-tamper resistant smart cards. *Lecture
Notes in Computer Science*, 7371:114–121, 2012. CODEN LNCSDO. ISSN
com/chapter/10.1007/978-
3-642-31540-4_9/.

**Wang:2010:DVT**

Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deter-
ring voluntary trace disclosure in re-encryption mix-
18:1–18:??, February 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-
7406 (electronic).

**Wang:2012:BRR**

Ding Wang, Chun guang Ma, Sen dong Zhao, and Chang li Zhou. Break-
ing a robust remote user authentica-
tion scheme using smart cards. *Lecture Notes in Computer Sci-
ence*, 7513:110–118, 2012. CODEN LNCSDO. ISSN 0302-9743 (print), 1611-
3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-
3-642-31540-4_9/.

**Wang:2012:SPB**

Ding Wang, Chun guang Ma, and Peng Wu. Secure password-based remote
user authentication scheme with non-tamper resistant smart cards. *Lecture
Notes in Computer Science*, 7371:114–121, 2012. CODEN LNCSDO. ISSN
com/chapter/10.1007/978-
3-642-31540-4_9/.

**Wei:2012:NCI**

Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, and Shiguo Lian. A
novel color image en-
cryption algorithm based on DNA sequence operation and hyper-chaotic
2012. CODEN JS-
SODM. ISSN 0164-1212 (print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
service/article/pii/S0164121211002147.

**Wang:2017:DRM**

Yi Wang and Yajun Ha. A DFA-resistant and masked PRESENT with area opti-
mization for RFID appli-
cations. *ACM Transactions on Embedded Com-
puting Systems*, 16(4):
102:1–102:??, August 2017. CODEN ????. ISSN 1539-
9087 (print), 1558-3465 (electronic).

**Wang:2018:GAD**

Lin Wang and Zhi Hu. On
graph algorithms for de-

**Wang:2015:EFF**


**Wang:2017:DVP**


**Wei:2016:PAB**


**Wang:2012:FOP**


**Wang:2012:NFS**


**Wang:2012:DAA**


[Wang:2019:RSI]


[Wang:2019:MBN]


[Williams:2018:FDP]


[Winder:2017:ROS]


[Wang:2019:DRS]

REFERENCES

Wu:2011:HQI


Weissman:2011:LLB


Wang:2012:MCE


Wu:2019:VFS


Wei:2012:IRK

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–??, April 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Wang:2011:RBM


Wang:2017:CAS

Changji Wang, Yuan Li, Jian Fang, and Jianguo Xie. Cloud-aided scal-


Qi Wang, Xiangxue Li, and Yu Yu. Anonymity for Bitcoin from secure escrow address. *IEEE Access*, ??(??): 1, ???? 2017. ISSN 2169-3536.

[Wang:2016:LLE]

[Wang:2012:RTC]

[Wu:2012:PSC]

[Wang:2017:CES]

[Wang:2015:HAD]
Xing Wang, Nga Lam Or,


(print), 1558-2566 (electronic).

Wu:2016:CBE


Wei:2015:TPE


Williams:2013:APC


Whitworth:2014:SPC


Woodworth:2019:SSS


**Wu:2010:IBM**


**Wang:2013:NMC**


**Wu:2012:RIB**


**Wu:2016:LTN**


**Wu:2017:SPM**


**Wu:2012:AST**

[WW12] Shengbao Wu and Ming-sheng Wang. Automatic


REFERENCES


Wahaballa:2014:MLS


Werner:2017:CIM


Wang:2011:CIB


Wang:2011:CHI


Wu:2017:EAK


Wang:2017:FWA

Ran Wang, Guangquan

Wang:2016:SHI


Wang:2017:SRS


Wang:2010:IIB

Wang:2017:NAI


Weir:2012:AFC


Wang:2014:NAI


REFERENCES


REFERENCES

Wei:2012:GOP

Wang:2012:NIS

Xiong:2013:NIB

Xu:2014:AHA

Xu:2012:APA
REFERENCES

com/chapter/10.1007/978-3-642-33338-5_8/.

**Xu:2014:TBH**


**Xi:2012:MDA**


**Xue:2014:LDP**


**Xue:2017:CNC**


**Xue:2019:SEA**

Xie:2012:RAA


Xiong:2012:PPK


Xu:2016:CIB


Xu:2013:PKE


Xu:2019:TPT


Rui Xu, Kirill Morozov, Yanjiang Yang, Jianying Zhou, and Tsuyoshi Takagi. Efficient outsourcing of secure k-nearest neighbour query over encrypted database. *Comput-


[XNKC10] Hong Xin, Zhu Shujing, Chen Weinbin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In
Xiao:2010:TAT


Xie:2012:ORI


Xie:2013:SIP


Xiong:2012:CBP

REFERENCES


[XWZ+18] Jian Xu, Laiwen Wei, Yu Zhang, Andi Wang, Fu-


Xu:2019:SIC


Xing-Yuan:2011:PRS


Xiao:2019:NEA


Xu:2015:ORA


Xiong:2019:PPH


Xiong:2012:CLR

[XZY+12] Hao Xiong, Cong Zhang,


REFERENCES


[Yang:2011:PQC]

[Yang:2011:GSS]

[Yang:2012:PST]

[Yang:2016:EBB]
REFERENCES


[YD17] Meng-Day (Mandel) Yu

**Yasuda:2015:MQC**


**Yan:2016:DEB**


**Ye:2014:NIE**


**Yekhanin:2010:LDC**


Yang:2015:SHI


Ye:2017:VCS


Ye:2016:IEA


Yang:2018:RKF


Yu:2010:IBF

Jia Yu, Rong Hao, Fanyu Kong, Xiangguo Cheng,
REFERENCES


REFERENCES

Yu:2012:IRI


Yum:2012:OPE


Young:2013:TPC


Yang:2018:AIW


Yoshino:2012:SIP


Yum:2011:ACO


REFERENCES


Yi:2017:ICM


Yuen:2013:ELT


You:2012:DDS


Yang:2019:NAK


Yang:2012:WSI


REFERENCES


REFERENCES


REFERENCES

Yang:2015:EPS


Yang:2016:ECV


Yang:2018:HEP


Yao:2014:NCR


Yeh:2010:TRR


Yuen:2014:TCT

[Ylonen:2014:SAA]

[Yang:2011:CCK]

[Yang:2011:CPK]

[Yamada:2012:UEW]

[Ye:2018:VBA]

[Yeh:2017:SIB]


Yao:2010:ASP


Yan:2017:PIS


Yang:2015:RCI


Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


YANG:2010:CRS

WANG:2018:CIW

YANG:2019:SCC

YAN:2012:SMA

YU:2012:SME

YU:2016:CDI
Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, and Jian Shen. Cloud data...
integrity checking with an identity-based auditing mechanism from RSA. [YY11]


Yang:2016:EPA


Yang:2017:SKS


Yu:2019:PSI


Yang:2012:LUC


Yang:2018:CDD


Yang:2012:BPN

Shuguo Yang, Yongbin Zhou, Jiye Liu, and Danyang Chen. Back prop-


Kai Zhang, Jie Chen, Hyung Tae Lee, Haifeng Qian, and Huaxiong Wang. Efficient public key encryption with equality test
Zhang:2014:GCS


Zeng:2019:PKE


Zhang:2012:AOP

REFERENCES


REFERENCES

Gao:2012:DES

Zadeh:2015:ASP

Zhang:2012:LDC

Zhang:2015:BYO

Zhang:2015:STR

Zhao:2017:RAS
Caidan Zhao, Minmin Huang, Lianfen Huang, Xiaojian Du, and Mohsen Guizani. A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. Computer Networks (Amsterdam, Netherlands: 1999),
REFERENCES
544


REFERENCES


Zhou:2015:EPP


Zhang:2016:PPV


Zuo:2019:WDH


Zimand:2010:SEC


Zhang:2011:FBP


Zeng:2014:NFC

Zhou:2012:CBF


Zhang:2019:CCF


Zhou:2015:PPS


Zhao:2012:IAS


Zhao:2014:TAH


Zhang:2012:EEF

Yummei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho Au, and Willy Susilo. Efficient escrow-free identity-based signature. *Lecture

Zhang:2015:RBA


Zhang:2012:CCB


Zhu:2017:PSN


Zhang:2010:ESP


Zhou:2019:LIB


Zhang:2016:TL

Mingwu Zhang and Yi Mu. Token-leakage tolerant and

Zhang:2015:RBA


Zhang:2012:CCB


Zhu:2017:PSN


Zhang:2010:ESP


Zhou:2019:LIB


Zhang:2016:TL

Zhang:2017:FGA


Zhang:2016:CAH


Zhang:2010:NSS


Zielinska:2014:TS


Zaeem:2017:MAI

Zafar:2010:GRN


Zhang:2017:PPN


Zavattoni:2015:SIA


Zheng:2016:EUV


Zhao:2012:SSS


Zhou:2017:IBB


**Zenger:2016:AKE**


**Zhang:2015:MAA**


**Zhang:2010:EMO**


**Zmudzinski:2012:WEU**


**Zhao:2012:SSM**


**Zhou:2019:LIN**

Lu Zhou, Chunhua Su, Zhi Hu, Sokjoon Lee, and Hwa- jeong Seo. Lightweight implementations of NIST p-256 and SM2 ECC on
Zheng:2018:GDP


Zanon:2019:FKC


Zhang:2012:EH0


Zhou:2018:TPW


Zuo:2018:CSA

Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. CCA-secure ABE with outsourced decryption for fog computing. *Future Generation Computer Systems*, 78 (part 2)(??):730–


**Zhou:2014:SAC**


**Zhang:2014:LFL**


**Zhang:2011:AGK**


**Zhou:2018:QTA**

Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki,


[ZXZA+18] Jun Zhang, Yang Xiang, Wanlei Zhou, Lei Ye, and Yi Mu. Secure image retrieval based on visual content and watermarking

**Zhou:2017:CLR**


**Zhou:2017:LRC**


**Zhang:2017:GFD**


**Zheng:2010:PS**


**Zhou:2019:CLR**

REFERENCES

<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume, Issue, Pages</th>
<th>doi</th>
<th>URL</th>
</tr>
</thead>
</table>
REFERENCES

Zhang:2015:ITS


Zheng:2015:EPT


Zhu:2018:CA


Zaidan:2017:NDW


Zh:2014:SAC


ZZ15


ZZC15


ZZC17


ZZKA17


Zaidan:2017:NDW


**Zhang:2017:NL**

**Zeng:2019:SAE**