Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K_N) [Bai10, YC11], (n, t, n) [LHYZ12], (t, n) [QD16, ZPYW12]. 0 [XHX+17]. 1 [XHX+17]. 1, 2, 3 [SMDS11]. 11 [LJ17]. 13 [Bl05]. 2 [DBPS12, EAA+16, ESS12, JR13, MCD12, PGL10, WY12]. 22 [MN12]. 2k [Sun16]. 3 [AP10, CG12b, DWWZ12, FWS13, GZHD12, GH11a, KWS+12, LJ17, LJ15, MKH+12, RS16, SS10b, SS12a, SGS14, WSSO12, tWmC12, YT11a, Y14, YPRI17]. 32 × 32 [SA14]. 3 × 3 [ÂMVZ12]. 4 [COP14, D12, HLXS14]. $49.00$ [Sch15a]. 8 [LPO+17]. $89$ [APPVP15]. = [JUW10]. + [PYH+18]. 2 [YNX+16]. 3 [LHM14]. $^{MT}$ [HRB13]. α [TTL10]. c [KRDH13]. d [QD16]. $d \times d$ [KA17]. $t$ [ZTL15]. $F_{p + \nu F_{p}}$ [WGF16], $\gamma$ [D12]. GF(2)[x] [SF12]. GF(2m) [SKH15]. GF(2n) [LBOX12]. K [FXP12, FR16, CHX13, ZHT16]. L(1/4 + o(1)) [Jou13]. $M$ [MMSD13, ÔSî]. F_q producing [AMORH13]. $F_q$ [SS13]. $N\P$ [HN10]. GF(q) [Lp10]. LWE [BV14], µ [Jia14a]. N [FR16]. $n \times k(k \geq n/2)$ [MC11]. $O(d^{3})$ [KA17]. $O(n^{2})$ [KS11]. $P$ [DG17]. $\pm 1$ [HZW+14]. q [GMS11]. S [LJ15]. t [HJM+11, Ob11]. w [Kre13].

-private [HJM+11]. -Round
[COP14, LJ17, Blo15]. -SDH [GMS11].
-trimmed [TTL10].

.onion [Boy16].

0.13um [KLM+12].

1 [AAE+14, Ano15b, BH15, CGCS12, Ful10, MSas12, SKP15]. 1-58488-551-3 [Ful10].
’10 [Ano10]. 1024 [Bro17, Win17]. 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 [CGB+10].

2.0 [NVM+17, PC16]. 2000 [ZC12]. 2003
[Sha10]. 2008 [Mei10]. 2010
[Ano10, Ano11b, CGB+10]. 2011
[Wes16]. 21st [IEE13, JY14]. 256
[AKY13, App15, MAK+12]. 29th [Gil10].
2D [HIDFGPC15].

3 [ABM+12, jCPB+12, Ful10, LC17]. 30th
[Rab10]. 31st [PJ12]. 384-bit [MMN12].
3GPP [FPBG14].

4 [Jac16, YYO15]. 42-step [AKY13]. 4765

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]. 768-bit [KFL+10].

8.8/11.2 [GLIC10]. 802.11
[FLH13, ZBR11]. 802.11s [BOB13].
802.15.4 [NBZP17]. 802.16e [CL11]. 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]. A AoT [FQZF18]. Abandon
[Lec15]. ABE [FJHJ12, HQZH14, QZZ18,
TY16a, YMC+17, ZSW+18b]. abelian
[CDLSY14, LR15]. ability [WS12]. absence
[AGH+17]. Abstract
[Bull10a, CFR11, MZ17b]. abuse
[JSMG18, QRW+18]. Accelerating
[CMB+16, DOS15, SKH15]. Accelerator
[MRL+18, PC16, WOLP15]. Accelerators
[AQ17, GP17, HKL+14, BAB+13].
ACCENT [PP11]. Acceptance [SPM+13].
Access [AWSS17, BFK+10, CO11, CGH11,
DLZ+16b, FCM14, HP12, LPL15, MK12b,
NA10b, PB12, QZL+16a, RSN14, SC14,
SC12, WS13, XMCL13, YTH17, YSS14,
ATKH+17, ACK+10, AMHJ10, CLH+16,
Cra11, DFJ+10, FNWL18, FS18, HZL18,
JAS+11, LCL+17a, LCL+15, MLM16,
NZM10, NAL17, QCX18, Shy15, Tan12b,
TODQ18, Wan18, WS12, XHH12, ZZ15,
ZML17, ZVH14, ZDW+16, ZWS+18,
ZF+18]. AccessAuth [TODQ18].
accessing [CSD18]. Account [Bro11].
Accountable [SCGW+14, YMC+17, ZZ12].
Accumulable [SEX18]. accumulator
[KYH18, LZY+16]. accumulator-based
[LZY+16]. Accumulators [PTT16].
al-Qaeda
[Mac14, Keb15]. al.[ABJ13, SPLHCB14].
Alan [CS12, Don14, Hel17, LCKBJ12].
Algebra [Xie12, BS15, Bul10b, CFR11, DWZ12, FGPGP14]. Algebraic
[SK11, Tam15, Wat10, Bul10a, CFR11, DWZ12, FGPGP14].
Algorithm [ABCL17, Ano11b, AK14, BGT14, BKL18, CNR14, jCPB+12, ESS12, GKS17, JLL12, JSZ12, JHNN12, JL16, KB10, LL11, LT14a, LLL17a, MRL+18, NMMW16, NV10, RR11, RVRSM12, WHZ12, WZCC18, YPRL17, YH16, ZSW+12, Ant14, CG12b, Chm10, EEA13, JK13, Jou13, KY10, KHM13, LC17, LR15, MS12a, MM14b, MNX+16, MN14, PGL10, PA10, PC14, SH11, SL10, SWW+17, jTL12b, TTL10, WZG+12, XTK10, YWL+17, ZLW+12, ZL12, ACZ16, ZOC10].
Algorithmic [GO17, AY12].
Algorithmics [Gas13].
Algorithms [AMKA17, AB10b, BCG12a, BJ10, CN12, GP17, KRD13, MR14a, MM17, TKM12, WH18, YS15, ZW15, AGHP14, Fri10a, Mac12, NAACL12, NC13, O10, O18, Xie12].
Ali [ABJ13].
Alignment [Don14, IA15].
Allowing [PRC12]. Allows [Bro17].
Almost [BKST18, FFL12, GDCC16, Oba11].
Almost-Tight [GDCC16].
Almost-Universal [BKST18].
Alter [SMOP15].
alternate [ZLW+12].
Alternating [BKS12, HD15].
AMBTC [KSSY12].
America [AB10a, Bha16, Fag17].
American [Sch15a, Mun17]. Americans [ABJ13]. among [BP11, MP16+16, SS17].
amount [EEAZ13]. Amplification [ABF12, HMR14].
Analog [KOP12, SOS15].
Analyses [ZPXX17]. Analysing [GRL12].
Analysis
[ABS+12, ARD12, BRS17, BBB+16a, BC14, BS14, BKL18, CFE16, CC+16, CGL+12, DKMR15, FSWF11, GZZ+13, GWM16, GLG12, HC12, HHH+13, HZWW17, HB17, IBM13a, IS12, JT12a, KE19, KOP12, Kre13, LPS12, LTKP16, LCK11, LWW16, LG LL12, MD12b, MAS16, MRTV12, MR10, NDC+13, NSA15, NAL17, PH12a, PFS12, PS14, RZZ+15, Rao10, RBS+17, SK11, SY15a, SR12a, Shi11, SZDL14, SCGW+14, VK15, WDDW12, YZLC12, ZH15, ZAG19, Aia15, AC16, AN15, BNY14, CFH+13, CFL13, DMV15, DK17, DWH+13, DMIT12, FT10+10, FAS+18, FHM+12, HM10, Lan11, MFH13, NLYZ12, PPA18, PL16, QGGL13, RT10+11, SKE14, TOL+14, TLM13, Tso13, VS11, Ven14, ZZ17].
Analysis-Based [RZZ+15]. Analytic [Kuz11, Sha10, ZW15].
analytical [CDPLCA16, TKMZ13].
analyzing [HREJ14, YGD+17].
Ancient [Fox13, Rao10].
Android
[Chi13b, EB10, FHM+12, SFE10].
Android-Powered [SFE10].
Angle [ZPW16, PKS18].
Angle-Based [ZPW16].
Angular [pNyWyY+14].
Anisotropic [ZC14].
Annotated [ATS15].
Announcing [SBK+17].
Annual
[Ano10, EIE10, IE11b, PJ12, Gil10, Rab10].
anomaly [AKKY17].
Anonymity [CDFS10, HEC+12, MV16b, MR10, SCGW+14, VF17, WLY17, AIB+16, BAG12, GH16, HRL11, Par12b, PSJ+13, SGJ+18, WW14, YHL16, ZK11].
Anonymity-Based [HEC+12].
anonymity-preserving [AIB+16].
anonymization [XTK10]. anonymized [BDK11, TG12].
anonymizing [TMK11].
Anonymous
[CG12a, CZLC12a, CCF17, Chi12, DK12, FHH10b, FHZW18, HLT+15, KP18, LIK+17, LZ14, MF16, Per13, RSN14, TAKS10, Wan14, WXL+17, WYML16, ZJ14, ZMW16, AIK18, AT11, BT18, CCA11, Ch13a, CGH11, FSGW12, GT19, HL14, ISC+16, LNK+18b, LHM14, LYL15, LY14, MYYR13, QMC17, VS11, WLS14, YZL+18].
ANSI
[Ano15d, BRS17, BMS12, Bro17, CJP12, DSB15, FXP+17, zGXW12, GV14b, GDC16, HCETPL+12, HLAZ15, JHL12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LWKP12, LWPF12, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNST17, CJP15, DDFR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYHH14, LWKP14, MBB11, MNP12, NZL+15, SB17, SXL16, WYL13].

Attiacker [PLGMCdF18].

Attackers [BL15].

Attacks [ARP12, Ano17e, BGK12, BFK16, BKBK14, Che15, CMA14, DGIS12, DHLAW10, DHB16, EWS14, GPT14, HLLG18, Hay13, HRS16, JSDK+16, JWJ+17, KNR10, LLC11, LWZ12, LWCJ14, LCL17b, MD12b, PYM+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, WW14, WHN+12, XNG+14, YL17, YCM+13, ZLQ15, ZHS+19, AATM18, BBBP13, BVIB12, BSR+14, CGH17, dCCSM+12, DCAT12, DJL+12, DK17, Dra16, EA12, FTV+10, FIO15, GPP+16, GBNM11, KM10a, KPS10, LWK11, NDN13, OF11, PX13, SGP+17, TK19, TS16a, TY16b, TLL13, VS11, WWBC14, XWDN12].

Tryp[Fel13].

Attentation [FQZF18].

ATTiny [EGG+12].

Attribute [AAC+16, AHL+12, BFK+10, Boy13, CD16, CD18, FHR14, GZZ+13, GSW+16, GL12, GVW15, HSMY12, Her14, KGP12, LW11b, LW11c, LW12, LjlC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, OT12, PPA18, PB12, RVH+16, Rao17, SSW12, TYM+17, WDC18, WHL15, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQQ15, ZM17, AGL+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LY15, LWJ+17, LWY18, LDZW19, QRW+18, RD17, XWS17, YCT15, ZML17].

Attribute-Hiding [OT12, ZWM14].

Attributes [CG12a, Yon11, LCL+17a].

Attribution [AAC+16, BFK+10, Boy13, CD16, FHR14, GZZ+13, GSW+16, GVW15, HSMY12, HSS12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TYM+17, WDC18, WHL15, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQQ15, ZM17, AGL+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LY15, LWJ+17, LWY18, LDZW19, QRW+18, RD17, XWS17, YCT15, ZML17].

Attribute-Based [AAC+16, BFK+10, Boy13, CD16, FHR14, GZZ+13, GSW+16, GVW15, HSMY12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TYM+17, WDC18, WHL15, XMLC13, XWLJ16, XHX+17, ZPM+15, ZQQ15, ZM17, AGL+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LY15, LWJ+17, LWY18, LDZW19, QRW+18, RD17, XWS17, YCT15, ZML17].

Attributes [CG12a, Yon11, LCL+17a].

Attribution [XHC+12, FNP+15].

Auction [Con10, HJM+11].

Auctions [MR14c, QS18].

Audit [YNR12b].

Auditing [XMD+16, TCN+17, YYS+16, YXA+16].

August [AB10a, JY14, MV12, Rab10].

Austin [IEE13].

Authentic [HLT+15, SZMK13].

Authenticate [HM12].

Authenticated [Ao12, BCO13, BDM16, CLL16, CLY14, CCS14, CRE+12, DS11, EAA12, ESS12, FVS17, FFL12, GTT11, GL12, GZ12, HC12, HL10a, HCL+14, HEC+12, KMY18, LHK10, LY16, LH11b, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHKS14, MSU13, PTT16, Sar10b, Smi11b, Tan11, TW14, XL+12, XCH+12, XGLM14, XZL15, YS12, YLW13, YXT+16, Yon12, ZPZ+16, ZXH16, AIB+16, CTL13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HWB12, HL11, HPY10, ISC+16, KMTG12, LWS10, LHH11, LML+13, NCL13, Nos11, Nos14, PPTT15, PJ18, SMBA10, TCS14, Tso13, TKHK14, WZM12a, WZM12b, WTT12, XWXC14, XCL13, XWZ+18, YC12, YZZ+14, YZZ+18, ZT16, ZXWA18, ZG10, ZZZ15].

Authenticating [BS12, CHX13, GRL12, OKG+12, RGP12, WY12, ZCS15, Cer18, LFGCCGP14, PGL10, ZLDD14].

Authentication [ASO14, AAZ+16, AUMT16,
ABB19, BL12, BCE\textsuperscript{+12}, BCM12, BSSV12, Bel18, BKST18, BCD\textsuperscript{+12}, Bis17, BF11, Boy16, BKJP12, BS12, CGCGPDMG12, CTC\textsuperscript{+15}, CC14, CS\textsubscript{H}18, CCW\textsuperscript{+10}, CCF17, CJ13, CD12, CJ1P12, CLH13, DL15, DBPS12, DKPW12, DP12, FLH13, FR16, FMTR12, FD11, GHS14, Gli12, GI12, GM14, GU13, GMV17, GCK12, HZC\textsuperscript{+12}, HcS12, HLLC11, Har13, Hay13, HBCC13, HM10, HCP\textsubscript{L}SB12, HCETPL\textsuperscript{+12}, HKL\textsuperscript{+12}, HXC\textsuperscript{+11}, HLCL11, IGR\textsuperscript{+16}, JN12, JCM12, Jia17, JAE10, KP12, KS18, KRM\textsuperscript{+10}, KSD\textsuperscript{+17}, KPC\textsubscript{S}12, KLM\textsuperscript{+12}, KO16, KH10, LLC11, LH12, LLG15, LCLL15, LNZ\textsuperscript{+13}, LZCK14, LNXY15, LLZ\textsuperscript{+12}, MWZ12, MEFO12, MKH\textsuperscript{+12}, MBC15, MRRT17, MRS\textsuperscript{+17}, May15, MLBL12, Mor12, MSKRJ17, MPM\textsuperscript{+17}, NR11, NR12, NLLJ12, NLY15, OdH12, OOS12, PCDG14, PPRT12, PDT12.

**Authentication**

[PWVT12, RS11, RWLL14, RNS14, SGG18, Saa12a, SBS\textsuperscript{+12}, Sar12, SGC16, Sch15b, SKV12, ST14, SM12, SD12, Shi11, SGC14, SSA13, SC12, SZDL14, SHS12, SAA12b, SRK\textsuperscript{+17}, TGC16, TYK\textsuperscript{+12}, TM12, Vet10, WgMdZi12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, Xi1o, YTP11, YFT17, ZBR11, ZHW\textsuperscript{+16}, ZLDD12, ZLDC15, AMN18, AaBT16, ABK13, AATM18, Aia15, AL15, AHM\textsuperscript{+18}, APK\textsuperscript{+18}, Alp18, AIKC18, ACF16, AZF\textsuperscript{+12}, ATI\textsuperscript{+10}, AN15, ACM12, BS13a, BD18, BCM13, BGAD12, BLAN\textsuperscript{+16}, BAL10, BM12, BHvOS15, BT18, BTW15, BM11, CLM\textsuperscript{+12}, CML\textsuperscript{+18}, CLP\textsuperscript{+13b}, CTL12, CXX19, CSD18, CH10, CCSW11, CHS11, CLHJ13, CZ15a, Chi13a, CJ1P15, Cho14, CL11, DCAT12, DSCS12, DLK\textsuperscript{+16}, DMV15, DLN13, DZS\textsuperscript{+12}, DMT12, uHAN\textsuperscript{+18}, EA12, ED19, EA11, FPBG14, FH110a, FLL\textsuperscript{+14}, FP12, Far14, FA14a, FHZW18, FQZF18, FMA\textsuperscript{+18}.

**authentication**

[GJ13, GMSW14, GHD19, GLLZ13, GH16, GAI\textsuperscript{+18}, GCS\textsubscript{AddP}11, GLB\textsuperscript{+18}, GTSS19, HU15, HSH11, Ham12, Ham19, HDP13, HZC\textsuperscript{+14}, HZW17, HL14, HCM11, HLC16, HCC10, HS11, IMB17, IC17, IG11, IB11, IOV\textsuperscript{+18}, Jac16, JNUH17, JKAU19, Jia16, JKL\textsuperscript{+16}, JMW\textsuperscript{+16}, JAS\textsuperscript{+11}, JXLZ15, KPP16, Kem11, KKG14, KS\textsuperscript{B}17, KVvE18, Kza11, Kim16, KIH19, KP18, KPB17, KLV\textsuperscript{+16}, KDW\textsuperscript{+17}, LLLS13, LLZ\textsuperscript{+16}, LC17, LH11a, LT13, LH10c, LNM\textsuperscript{+11}, LMJC11, LX1MW12, NLLK13, LXC14, LIK\textsuperscript{+17}, LCM\textsuperscript{+17}, LNK\textsuperscript{+18a}, LWK\textsuperscript{+18}, LNK\textsuperscript{+18b}, LH14, LIT14, LW111, LTH\textsuperscript{+15a}, LLY15, LBR12, LTT10, MM12, MCN\textsuperscript{+18}, MvO11, MMP19, MA17, MS817c, MK12a, NR17, NAACL12, NCCG13, NLYZ12, NB13, OF11, OCDF11, OYH14, PYH\textsuperscript{+18}, PY10, Par12b, PLGM10A, PZBF18, PA10, PKA15, PRN\textsuperscript{+19}, QMC17, QMW17, SPLC14, SB17, SGGR\textsuperscript{+16}, Sar10a, SGI\textsuperscript{+18}, hSZ11, SCH10, SA15, SYW17, SSS11].

**authentication-chaining**

[EA11].

**authenticators**

[SYY17].

**authenticity**

[ADF12].

**Authority**

[LNXY15, XZLW15, ZQQ15, JB11, ZZ12].

**Authorization**

[CS14, LMGC17, MPM\textsuperscript{+17}, YKK18, AL15, DFJ\textsuperscript{+17}, JAE10, JAS\textsuperscript{+11}].

**Authorized**

[HTC15, LLSW16].

**Authorship**

[BTW15, BAG12, LCM\textsuperscript{+17}].

**Autoblocking**

[YS16].

**Automata**

[CCD15, Gas13, dRS12, HBBR1M\textsuperscript{+16}, SS11, WOLS12].

**automata-based**

[SS11].

**Automated**

[CCK12, CCC16, DRS16, GLLS12, LGM\textsuperscript{+16}, Ste15a, Tom16, YSS14].


Bandwidth-Efficient [LLZ$^{+12}$. Banking [KSD$^{+17}$, RBS$^{+17}$, KV+E18]. banned [Eve16]. BANs [BLL$^{+19}$. Baptiste [Dew11]. Barbara [Rab10]. Barcodes [WY12]. Barrier [JR14, KS11]. barriers [LKKL13]. base [MS12a, XSWC10]. Based [ADM12, AGW15, ASM12, AAC$^{+16}$, ABCI17, Ano11b, ASS15, AYS15, BWLA16, BL12, BBB$^{+16}$a, BSSV12, BH12, BKPW12, BRT12, BHH$^{+15}$, BS13b, BFK$^{+10}$, Bon12, BSJ15, Boy13, BKJP12, BDH11, BCF$^{+14}$, CML15, CL16, CGMO14, CCM17, CSH$^{+18}$, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST$^{+17}$, CGL$^{+12}$, CDD13, CGY$^{+13}$, CD12, Chl12, CK18, CD16, DSSM14, DA12, DLZ$^{+16}$b, EM12, EKB$^{+16}$, FM15, FHH10b, FHR14, FZT14, FGM10, FVS17, FSX12b, FSX12c, FSX12a, GWWC15, GZZ$^{+13}$, GSW$^{+16}$, GV14b, GI12, GY13, GDC16, GVW15, GJJ15, GJZ17, HZC$^{+12}$, HSMY12, HSM14, HL10a, HZX15, HCPLSB12, HK$^{+12}$, HG12, HMR12, HSA14, HPO$^{+15}$, HKR$^{+18}$, HGT15, HLC$^{+14}$, HLN$^{+10}$, Hul13, HRS16, HBG$^{+17}$, HEC$^{+12}$, HP12, JTH$^{+16}$, JHHN12, JEA$^{+15}$, JKH12, KS18, KZG10, KK12, KKA15, Kha10, KLY$^{+12}$, KSSY12, KPKS12, KRB12, KAK18, KS15].

Based [LMGC17, LMG$^{+18}$, LTKP16, LSL12a, LSL12b, LW11b, LW11c, LW12, LH12, LJLC12, LYZ$^{+13}$, LHL$^{+14}$, LTH$^{+15}$, LCC13, LWCJ14, LXXY15, LHL15, LWP$^{+17}$, LGPRH14, LDB$^{+15}$, LD13, LSC12, LBR12, LLH18, MWZ12, MLO17, MEF012, MCD12, MVV12, MD12b, MBC15, MKN13, MZ17b, MCS$^{+15}$, MMS17b, MKF$^{+16}$, MCF17, Men13a, Mor12, MSKR17, MKAA17, Mut16, NC12, NXH$^{+17}$, NXY15, NLLJ12, NLY15, pNyWyY$^{+14}$, OTD10, PB12, PTT16, PYH$^{+15}$, PGN15, PPS12b, PYS18, PG12, PAS13b, PNR17, RVH$^{+16}$, RZZ$^{+15}$, RS16, Rao17, RD17, RVRSCM12, BW12, SSW12, Sar18a, SSS13, Sen17, SJ12, SGP$^{+12}$, SP15b, SSA13, SRAA17, SH15, SGH15, TB18, TKR14, TWZ11, TW12, TWZ$^{+12}$, TMY$^{+17}$, TSH17, TT12, TTH15, TC10, VDB$^{+16}$, VGA15, Vle12, WY10, Wan10, WSS012].

Based [WgMW12, WYW$^{+13}$, Wan14, WZCC18, yWxyZ$^{+18}$, WDC18, WLH15, WCL$^{+18}$, WT10b, WMS$^{+12}$, XNC$^{+14}$, XNRG15, XZZ12, XMLC13, XQL11, Xia12, XGLM14, XWL16, XJW$^{+16}$, XJR$^{+17}$, XH4$^{+17}$, YE12, YZLC12, YXZ$^{+12}$, YGFL15, YTS12, Ye10, Ye14, YH16, YTH17, YYO15, Y$^{+17}$, YKNS12, YHK$^{+10}$, YMS11, YKC$^{+11}$, YFK$^{+12}$, YCZY12, ZPM$^{+15}$, ZJ11, ZXX$^{+11}$, YN12].
ZDL12, ZLH12, ZQQ15, ZMW16, ZXY16, ZZM17, ZPW16, ZHW15, ZVG16, ZPXX17, ZYM18, ZHL15, AMN18, AGLW16, AaBT16, AY14a, AHS14, AAT16, AA14, ASO14, AIA18, AKG13, ASVE13, Arai13, ATI10, AHI12, BS15, BDM18, BBBP13, BGA12, BASS13, BOB13, BWR12, BW13, BWA13, BMM12, BC18, BB16b, BK12b, CPPT18, CML18, CFL13, CFY10, CCL11, CT12L, CLSW12, CG12b, CSZ11, CHX13, CSS13, CW14a, CTHP13, CJP12, CJ15P, CCG10, CT13L, Chol14, Con12, dCCSM12, Cra11, CDL18, DSCS12, DZ14, DNL13].

Based [Dra16, uHAN18, EZ15, FI13, Far14, FA14a, FA14b, FIO15, Fay16, FHZW18, FNWL18, Gal13, GJ13, GMOGCC15, GMRT15, GKC11, GMP15, GCSAD11, GSS11, GLL18, HSH11, HT11, Ham19, HG11, HSM13, HZC14, HZL18, HF14a, HWD16, HZWW17, HZWL18, HBRMN16, HLR11, Her14, HWB12, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HY18, HP10, HKHK13, HCC10, Hwa11, IMB17, IM14, ISC16, IB11, IA15, IOV18, Jac16, JNU17, JKAU19, JK13, JL12, JZS10, JM16, JSM18, KPP16, KK13, KM10a, KHM13, KKG14, Kim11, KGO10, KLL1, KSH18, LX12L, LL16, LDU1, LLC10, LK14, LHI1c, LZX10, LNM11, LMLC11, LK12, LXMW12, LKAT12, LHS12, LNLK13, LXLJ14, LCL15, LZY16, LFZ17, LN18, LW18, LKT14, LFWS15, LLM19, LP10, Lin14a, LLY12a, LW10, LS11a, LS11b, LW11, LW13b, LZC14, LPZ15, LTC15a, LLY15, LY15, LFW17, LWY18].

Based-Encryption [ZHW15].

Bases [EVP10, TSH14, FES10].

Basing [Mat14, MN10].

Basis [BNA15, ERRMG15, CGI29, Har15, LLP18, Tam15].

Batch [ZPXX17, AGHP14, CGG10].

Batch-based [CGG10].

Batters [Ch13b].

Battles [A15e, A16f, Sch15c].

Bay [A10, DDS12].

Bayes [McC11].

Bayesian [WYW13, ZLW17].

Be [DSM14, Par12a, YM16, AZH11, Ana14, Eve16, Rec15, RK11].

BeagleBone [Cri16].

Beat [LTKP16].

BEACON [LLZ12].

Becomes [Bra13].

been [Ana14].

before [GST12, Goo12].

Beginning [Ch16].

Behavior [GSC17].

behavioral [HT11].

Behaviors [GAF15].

Behind [Fre10].

Beijing [BYL10, Yan10].

Beissinger [Ayu12].

Belief [BT12].

Bell [JEA15, QD16].

Benchmarked [MKAA17].

benchmarking [ZZKA17].

Benefit [HB14].

benefits [Wat14a].

Benford [AOT13].

Bessel [GJ13].

best [Cha13c].

Beth [CHTP13].

better [LCL17a].

Between [KA18, LRVW14].
SAKM16, CLM*12, HLR11, KPP16, Kim16, PBC14, WDDW12. Beyond
[LST12, MJS13, TS16b, FNP*+15, JR14]. BGP [SVG16]. BGV [GPHS12, GPHS13],
BGV-Style [GPHS12, GPHS13], biased [LLP*+18]. Biclique [BKR11, KDH13].
Bidirectional [GMNS15, GH12]. bifurcation [SE18]. Big [MLO17, Mal13, MMS17b, PNRC17, YDY*+16, ZLV*+17, FS18, SLSB14, QCX18, Tan17b, WS14].
Biggs [Low12]. bilateral [jT12b]. bile [RBS*+17]. Bilinear [Abe12, ASS15, IL15, LZY*+16, YS12, ZZ15, ZY17b].
Bilinear-map [LZY*+16]. billions [Hof16, SMBA10]. Binary
[ADI11, AK14, MBR15, MFB18, SA14]. Binary-Ternary [ADI11].
Binding [HEC*+12, ZLQ15]. Bio
[OK18, GPVCdBR012]. Bio-inspired
[OK18, GPVCdBR012]. BioAura
[MSKRII17]. biographical [Maf16].
Biometric
[Alp18, ATI*+10, BCTPL16, DWB12, JN12, KHMB13, LGM*+16, May15, NGAuH16, Sar12, SKV12, Vet10, AHM*+18, DMT12, GCSÁdP11, HT11, Ham19, LK12, LTC*+15a, MLBL12, Sar10a, Sar18a, SR10].
biometric-based [SR10]. Biometrics
[BW13, ERLM16, SP13, ZPW16, FHZW18, GM16, LXL12, LH10c, LNM*+11, LNK*+18a, MRRT17, SS17].
biometrics-based
[FHZW18, LXL12, LH10c, LNM*+11]. biosensor [Kim16]. Birkläuser [Sha10].
Birthday
[LST12, SXL16, Nac12].
Birthday-Bound [LST12]. Bit
[CG14a, GV14b, HG12, HS18, LJK17, LPO*+17, NIS12, Ros11, YLL*+12, APPVP15, KS11, KFL*+10, MN12, PLSdLE10, RH10, TWZ*+12, VN17]. Bit-Wise [CG14a].
BitCoding [HS18]. Bitcoin
[ADMM16, BRS17, BH15, Bra15, Chi13b, HB14, Hur16, JSK*+17, Mic16, Sir16, Tay17, TS16b, VFV17, WLY17, WHJ17]. Bitcoins
[MPJ*+16]. BitErrant [Ano17a]. Bits
[BF12, LLL17a, YCL17]. Bitstream
[SMOP15]. Bivariate [TWZ11]. Bivium
[EVP10]. BIX [Muf16]. BLAC [TAKS10].
Black [BR14, CPS16, HHP17, KOS16, KMO14, MSas13, JB11, Rja12, SS10b, DD13, SK14, YSC16, ZZ12, Cri16].
Black-Box [BR14, HHP17, KMO14, Rja12, SS10b, KOS16, MSas13, ZZ12]. Blackbox
[MSas12, SS12a]. BLAKE
[AMP14, GV14b]. BLAKE-512-Based
[GV14b]. Blanchette [SR14]. Blended
[ACAT*+15]. Bletchley
[Bai12, Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, McK11, McK12, Pea11, Smi11a, Smi15b, Smi15a]. Blind
[AP10, Ano15a, BCPV11, LCLW17, LGPRH14, MR16, MNN12, RS16, YMWS11, HK14, MO14, RSM15, RMG18, WLB11, yWpWypN13]. Blindfold
[Nac16]. Blindfolded [Vai11]. Blinding
[CLHC12, KHHH14]. Block
[AMVZ12, BRS17, BSS*+13, BFMT16, BDGH15, BCG*+12b, CWP12, DWWZ12, EGG*+12, FXP*+17, GLSN12, GT12, GST12, GNL12, IS12, KR11, KWS*+12, LWZ12, LJ17, LCLW17, LGLL12, LWKP12, LWPF12, MCB12, MRTV12, OGK*+15, PH12a, PRC12, Pud12, SG*+12, SSA13, WW12, YCL17, ZSW*+12, BNY14, Jeo13, KM11, LPZJ15, LC13, LYHH14, LWKP14, MNP12, MHV15, MHY*+18, PL16, Sar11, SKK10, TQL*+14, Tan17a, WB12, WWBC14, ZSW*+18a, JKP12]. Block-Parallel
[MCDB12]. Block-Wise [SSA13].
Blockchain [Hur16]. blockcipher
[CMMS17]. Blockciphers [LST12]. Blocks
[JSK*+17, Bra15]. Bloom [ATKH*+17].
Blowfish [KB10]. BLS [BP18]. BlueKrypt
[Gir15]. Boardroom [LHF12]. Bodacious
[KM10c]. Body
[LZCK14, ASO14, KP18, LK*+17, SGJ*+18]. body-sensor [ASO14]. bogus [XWDN12].
Bone
[Bur11, Car10]. Bonebrake
[SS10c]. Boneh [TK19]. Book
[Ano15b, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb10, Kob10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12].
Boolean [ACZ16, AS17, CW14a, DQFL12, FY11, LVV11, WT13, YCC16].
Boolean-based [CW14a, YCC16].
Bootstrapping [BGV14, GM14].
Border [LGM+16, ZTSR12].
BotMosaic [HB13].
Botnet [NSA15].
Botnets [HB13].
Bottom [Smi11b].
Bound [LST12, TK19].
Bounded [GVW12, GJO+13, PDNH15, QZZ18, SS12a, ZYT13, IM14].
bounding [PYH+18].
Bounds [Jia17, LJ15, SS11].
BRAMs [DGP10].
Branch [EPAG16].
Branchless [RBS+17].
Brave [KM10c].
Bringing [Ano15c, OYHSB14].
Britain [Ald11].
British [And13].
Broadcast [BS14, GMVV17, HMR14, KH10, LMG17, LMG+18, PSM17, PPS12a, WQZ+16, XJJ+16, Yan14, ZHW15, CPPT18, DNN13, WWYY11, XWDN12, YMM13, ZQW+11, ZZ12, Zhu13].
Broadcasting [OO12, MK11, OCG11, YY11].
broke [Bat10, Hea15].
Broken [MDAB10].
Broker [TKR14].
Broker-Less [TKR14].
brooders [Ree15].
Bruce [Sev16].
Brute [CJP12, JR14, CJP15].
Brute-Force [JR14, CJP12, CJP15].
BRW [CMLRHS13].
BTC [CLF11].
BTC-compressed [CLF11].
Buchwald [ABJ13].
Bucket [BKKV10].
Bug [Chi13b].
Building [BPS16, KMP+11, MJS13, Sev16, WL11, LCKBJ12].
Burdens [Blia2, SR14].
Bus [AN17].
Business [LDB+15].
Buyer [Fra16, KJN+16].
Buyer-Friendly [Fra16].
BYOE [Tan17a].
byte [Hof15, Hof16].
bytes [PBCC14].
Byzantine [KS11, LLKA19, YGKJ13].
Byzantine-resistant [YGKJ13].
C [AD12, ACZ16, Cra14, DJG14].
C1G2 [MK12a].
CA [ACM11, Dun12b, Kia11, Lin14b, Pie10, Rab10].
CABA [MSKRJ17].
CABE [XHX+17].
Cache [AB15, ADR18, DMK15, HLAZ15, SY15a, DJL+12, DK17].
CacheAudit [DMK15].
Caches [LLG16, CDPLCA16, DJL+12].
Caching [ADR18, HLAZ15].
CAD [PGL10].
Caernarvon [KMP+11].
Calculus [MR10, Jon13].
Calibrated [LC15].
California [Ano10, IEE11b].
Call [Ano16a, Ano16b, Ano16h, CS14, KRM+10].
Call-Back [KRM+10].
calls [Mur16].
cam [PKS18].
Cambridge [ACM10, PJ12].
Camellia [Blo15, LWKP12, LWPF12, LWKP14, SEHK12].
Camellia-192 [Blo15].
cameras [MKH+12].
Can [Alod12, AZH11, Bar15, DSM14, YM16, RK11, Rus15, Sto12, GMVV17, LMS16].
[GST12]. Checkability [LHL+14].
Checkable [IW14]. Checking
[FMYM15, YL17, SYY+17, YXA+16]. Chen
[LLLK10]. Chennai [BC11]. China
[BYL10, IEE11a, LTW11, Yan10]. Chinese
[HF14a]. Chip
[Bis17, MDAB10, BAB+13, BGG+13].
Chips [Man13, SOS15]. Chirp
[OWHS12]. Cho
[SPLHCB14]. chocolate [Svo14].
choice [LLP+18]. choosing [BL17].
Choquet [SH11, SM11, SNM14].
Chosen
[FSGW12, zGXW12, HLW12, HPY10,
LCT+14, LZC12a, LLML12, MH14, RS10,
WWHL12, GLM+16, GH12, LZC14].
Chosen-Ciphertext
[RS10, FSGW12, LCT+14, GH12, LZC14].
Church [ABJ13]. CHURNs
[RBNB15]. Cipher
[BW16, BFMT16, BCG+12b, CMLS15,
CGCS12, DM18, DWZW12, Fis15,
FXP+17, GLLSN12, GCS+13, HZ11, Hey17,
IOM12, JKP12, KR11, KWS+12, LPS12,
LWZ12, LJ17, LWKP12, LWPF12, MRTV12,
MHC12, MS12b, OGK+15, PH12a, PRC12,
WSSO12, WHN+12, YCL17, ZAG19,
AMS+10, BNY14, CR12, HKT11, Hol12,
Jeo13, KDH15, Lew10, LC13, LYHH14,
LWKP14, MNP12, PL16, Ree15, RS14, Sar11,
WYL14, WWBC14, ZSW+18a, LGL+12].
Ciphers
[ABS+12, BMS12, BSS+13,
BKLS12, Bru12, CWP12, DGIS12, DJG+15,
EGG+12, EKP+13, GT12, GST12, GNL12,
Has16, Hey17, IS12, KE19, KPC+16, Kla10,
LCW17, LLML12, LJ16, MD12b, NN12,
Pad12, Sas12, SEHK12, Vua10, WH18,
WW12, Xie12, ZH15, ZSW+12, Zha12,
Bay10, Bia12, Bor10, Die12, KM10a,
LWK11, MRT10, MHV15, MHY+18,
QGL13, SKK10, TQL+14, WB12].
Ciphertext
[BDPS12, CWWL12, zGXW12,
HLW12, JMG+16, JSMG18, KA17,
LZC12a, LLML12, MH14, PDNH15, PPS12b, Rao17,
RZW12, RS10, SSW12, VSR12, WWHL12,
XMLC13, XWLJ16, ZHW15, CPPT18,
FSGW12, GLM+16, GH12, HPY10,
HKHK13, KTT12, LCT+14, LFWS15,
LZC14, LDZW19, QRW+18, RD17, SGM16,
WLFX17, XWS17, LAL+15, LHL15].
Ciphertext-only [KA17].
Ciphertext-Policy
[Rao17, XMLC13, XWLJ16, ZHW15,
JSMG18, LFWS15, LDZW19, QRW+18,
XWS17, LAL+15, LHL15].
Ciphertexts
[BDPS12, CWWL12, zGXW12,
HLW12, JMG+16, JSMG18, KA17,
LZC12a, LLML12, MH14, RS10,
WWHL12, GLM+16, GH12, LZC14].
Claims
[SKGY14]. Class
[BCG12a, SY15a, XYXYX11, BJ16, Goo12, KK10].
Classes
[ACZ16]. Classical
[DSLB18, JEA+15, MSU13, SSU12, CR12, RRK11].
Classification
[HP10, HS18, KAHKB17, SGP+12, ZIW+17, LHL+18].
Classifiers
[KGV16, LCM+17]. classroom
[Pow14].
Claudius [Hol12]. CLEFIA
[LWZ12, TSSL11, TS16a, WB12].
CLEFIA-128 [TSSL11]. CLEFIA-type
[WB12]. Client
[ASM12, CTC+15, FD11, RAZS15, Vle12,
FA14a, FA14b, hSZZ15, WT10a].
Client-Based [ASM12]. Client-Centric
[Vle12]. client-server [FA14b, hSZZ15].
Clients
[CH16, LH13]. cloaking [NZL+15].
Close
[Wall18]. Cloud
[AJA16, BQ+C13, BCK17, CWL+14,
CWL16, CDFZ16, CCT+14, CLW16, DXA14,
FCM14, FPY15, JLS12, KMSM15, KS18,
KKA15, Kiip15, LA15, LZY+13, LGR14,
LLC+15, LNXY15, MLO17, PSM17, Pet12,
RSGG15, SGG18, SGJ+18, SKH17, SRAA17,
TV15, Vle12, WLFX17, WW17, XNKG15,
XWS16, XMLC13, XWLJ16, XJW+16,
[CN12, DHB16, ESR14]. Communication
[BPST17, CCM17, CWW+10, FMS12b, Gas13, GPVcDr12, KW14, Low12, OKG+12, Wan13, ZC+13, ZHW+16, ADG16, DKL+16, HCC11, HLY14, HPY10, KRM+10, KTU16, LT13, LyWSZ10, MCN+18, QMC17, RK11, SSAF11, SSPL+13, Tso13, WLZ+16, YKG13, Zhu13, vDKS11].

communication-efficient [Tso13, Zhu13].

Communication-resource-aware [Wan13].

Communications [JTZ+16, KSD+17, OO12, SMS14, AMN18, Edw17, FHH10a, Han12, LGGCC14, LLZ+16, MHY+18, RS15, WDLZ13].

Community [BPS16].

Commutative [CLHC12, SLGZ12].

Commutativity [ABR12].

Commuting [Fuc11, AKG13].

Compact [CFOR12, CKLM13, EG+12, MAS16, VSR12, ZMW16].

compacting [CPPT18].

Companion [KR11].

Comparable [XHX+17].

Comparative [DDR+16, MHV15, NR11].

Comparison [CGCS12, DWB12, HPC10, KU12, KA18, ST14, HM10, LCM+17].

comparisons [Mid10].

compartmented [EZ15].

Compensated [GKS17].

Compensation [JSZS12].

Competition [JCPB+12].

competitive [MD15].

Compilation [CHS15].

compiler [LWS10].

Compiling [CR10].

Complete [Ash14, BS14, FLH13, GHKL11].

completely [Win17].

Completeness [FKS+13].

Complex [pNyWyY+14, VBA15, BW13].

Complexity [BKI14, BW12, DP12, FS15, Gas13, HHS+15, AAT16, DJL+12, Jou13, KGO10, LW+10, SDM14].

Compliance [SOF12].

compliant [BP10, Lan11].

Component [BKLS18, MV16a].

components [RITF+11].

Composable [DN12, KMO14].

Composing [TW14].

Composite [Dun12a, BBBDL+17].

Composition

[LJS+14, NRZQ15, Ana14, AGH+17].

compound [BJ16, KPS10, jT12b].

Comprehensive

[GSFI16, YFT17, Bu10a, KAS15].

compress [LC13].

Compressed

[DG17, JSC17, KD12a, SR12a, WLZL12, CLF11, Fay16].

Compressed-Domain [WLZL12].

Compressibility [HN10].

Compression [CNI12, DA12, LD13, MAL10, PMZ13, PP10b, TCN+17, WHZ12, Ara13, CMMS17, DTZZ12, LK14, Li10, LPZ15, PP11, QZ14, SI12].

compression-based [SI12].

Compression/Decompression [PP10b].

Compressive [CCZC13].

Compromise [YNR12b, GBNM11, PX13].

Compromised [DSSD14, ZYL+10].

Compromising [BC14].

Compulsory [QRW+18].

Computability [Gas13].

Computable [LGH+17, FWS13].

Computation [ARH14, Ash14, Bee17, BDOZ11, Fri10b, GST12, GFW12, GHKL11, HP14, HC17, IEE11a, Jin10, KW14, KMO14, LHM+15, LQD+16, MMP14, Mal13, NSMS14, PST13, SVCV15, SZQ+17, TM18, Wat10, ABDP15, AB10b, LDDAM12, PHGR16, TG12, vDKS11].

Computational [BCO13, GKS17, RD17, TBCB15, HRS13, SDM14].

Computations [ARM15, CK18, KHPP16, Nac16, ADMM16, BK12b, LR15, SSAF11, TLM13].

Comput [Vai12].

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

computers [Cop10b, LCK11, Mac12, MvO11, PHWM10].

Computing [ACM10, ACM11, AIA16, Ano17e, BCG+12b, CR14, CGB+10, DXA14, EAA12, FES10, Gen10, KMSM15, KP17, LCK11, LT14a, LYZ+13, LLC+15, LGJ16, LNX15, MLO17, OS16, PAF18, PCT12, SJW+17, SL10, Vai11, Vle12, XMLC13, XWLJ16,
[DDD14, GLW13, LWL10a, MM14a]. Contributory [WQZ**16**]. Control [ATS15, BFK**10**, DLZ**16**b, HHS**15**+, LGM**16**+, MM17, MK12b, NA10b, QZL**16**a, RSN14, SGC14, TBC15, XLC13, YTH17, ACK**10**, AMHJ10, CLH**16**+, CO11, Cra11, FNWL18, FS18, GHD19, JAS**11**+, LCL**17**a, LCL**15**, NZM10, QCX18, Sch15c, SA15, Tan12b, Wan18, XHH12, ZML17, ZVH14, ZWS**15**, ZFH**18**]. Controllable [FH13, ZLDC15, ZHT16]. Controlled [FMTR12, WP17, Har16]. Controller [GMVV17]. Controllers [AMH**16**]. controls [CGH11]. controversy [McG11].

conundrum [Eve12]. Conversations [WBC**10**]. Converse [KPKS12].

Conversion [BJ10]. Convertible [DLL16, LH11b, HL11, LHH11, XWX14].


Coordinate [YKK18]. Coppersmith [Dra16]. coprocessor [ABC**12**, BGG**13**, IBM13b].

coprocessors [GCVR17]. Copy [YT12, MHT**13**]. Copyright [SJ12, GJ13].

Core [LB13, YWF18, YS15, RS17, HLYS14].


correcting [ATI**10**, LTT10, MCP15].

Correction [LSC**15**, yWXyZ**18**, Chi13a, Sun16].

Correctness [YGS**17**, WS13]. Correlated [RS10, Jia16, ZPZ**16**].

Correlation [BW12, FAA**18**, LD13, SDM**12**, WWBC14, XHH12, YCL17]. correlations [Sar14].

Correspondence [SY14].

corresponding [DWZ12]. Corrigendum [HYS18, WZM12a]. cosmography [Pet11].


Cost-Effective [HLT**15**, WMX**17**].

Costas [TRD11]. Costs [KHPP16].

couldn’t [Bha16]. Countdown [Zet14].

Counter [ARP12, Fay16].

Counterexample [KPKW13]. Counterfeit [YFT17]. Counterfeiting [Ano16e].

counterfeits [GSN**16**]. Countermeasure [BBB**16**a, MD12b]. Countermeasures [BGN17, EWS14, PZPS15, DK17, FAA**18**].

counting [LLY**12**a]. Coupling [SMS14].

cover [UUN13]. Covert [EPAG16, JTZ**16**, NSA15, LT13, LyWSZ10, SRB**12**].

CovertBand [NTKG17]. Cozzens [Led16, Sch15a]. CP [TY16a, YMC**17**].

CP-ABE [YMC**17**]. CPM [PYM**13**].

CPS [FQZF18]. Crack [Fox13]. cracked [Ano13b, McG11, McK12, Moo14].


Crisis [OdH12]. Criteria [PYS18, ZKAK17].

Criteria-Based [PYS18]. crittografia [Sac14]. CRM [LHM**15**].

Cropping [SR12b]. Cross [AKK**17**, CLY14, DSB15, LHM**15**, MV16a, YGFL15, YZL**18**, ZHX16, ZTSR12, SS17, der10].

Cross-Border [ZTSR12]. Cross-Domain [CLY14, YZL**18**]. Cross-group [AKK**17**].

Cross-Layer [LHM**15**, ZHX16].

cross-matching [SS17]. Cross-Site [DSB15].

Crossword [Mar10a]. Crypsis [GSC17].

Cryptanalysis [BW12, Por10, CWP12, CGCS12, DG12, DJG**15**, Far14, GST13, Gor10, Hin10, IOM12, Jee13, Kha10, KN10, KWS**12**, LH10b, LNM**11**, LIF16, LJJ16, MWZ12, N XB13, OTD10, PSOMPL13, SPLHCB14, SM10a, SM10b, TY16a, TQ17, Vua10, Wag10, WWYY11, WWYY11, WSOS12, WY14, XQL11, YCL17, YMSW11, AP11, BMB16, BKR11, Bul10a, Bul10b, Con12, Eis10, Zet14].
Her10, KDH13, LLLL10, LFW+16, Nov10, RITF+11, SMD10, SMD14, Sun11, SvT10, Tam15, TSSL11, WYL14, WWBC14, AY12]. Cryptanalyzing [LLL17a, ZLW+12]. CryptDB [PRZB12]. Cryptic [Mar10a]. Cryptography [ACZ16, Ano15c, Ano16a, Ano16b, Ano16h, Ano19, App14, AAB17, ACM+17, ARM15, Bar12, BGK12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BLM17, BCF+14, CTR14, CT18, CJSF14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, Fe10, FSK10, Fid18, FBM12, Fre10, GO17, GFBF12, G’13, GPT12, GLW12, Ham17, Het12, HGI2, HKR+18, JT12a, KM10c, KOP12, LSM12a, Lin17, LWL10b, LGW12, LMHH14, LGH+17, LWHS17, LPO+17, MO12, MSH10, Mau12, Men13a, MR14c, Mic10b, MV12, MMB17, NNA10, NS12, Orm16, PP10a, PPH12, PG12, RW12, SY14, SG15, SOG15, Sch16, Sen10, SS13, Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16]. Cryptographic-Key [SK11]. Cryptography [ACZ16, Ano15c, Ano16a, Ano16b, Ano16h, Ano19, App14, AAB17, ACM+17, ARM15, Bar12, BGK12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BLM17, BCF+14, CTR14, CT18, CJSF14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, Fe10, FSK10, Fid18, FBM12, Fre10, GO17, GFBF12, G’13, GPT12, GLW12, Ham17, Het12, HGI2, HKR+18, JT12a, KM10c, KOP12, LSM12a, Lin17, LWL10b, LGW12, LMHH14, LGH+17, LWHS17, LPO+17, MO12, MSH10, Mau12, Men13a, MR14c, Mic10b, MV12, MMB17, NNA10, NS12, Orm16, PP10a, PPH12, PG12, RW12, SY14, SG15, SOG15, Sch16, Sen10, SS13, Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16]. Cryptography-Related [BOB13]. Cryptographer [Dun12b, Kia11, Pie10]. Cryptographers [Ano16d, BPS16, Goo12]. Cryptographic [KSU13, KAS15, KKK+16, LGY10, LLL+17b, MS13c, MMZ12, MM13, Mes15, MN10, NDN13, O018, Pa15, PLPW13, PSO+13, QZD16, SD10, WT13, WMX+17, YSM14, ZVH14, Zim10, Sha10]. Cryptographic-Key [SK11]. Cryptographical [KU12]. Cryptographically [ADD10, BCGH11, BJL12, BKLS18, MC11, NDG+17, PLsdLE10, SVC15, GCH15, HJM+11, SA14]. Cryptography [ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, Ano19, App14, AAB17, ACM+17, ARM15, Bar12, BGK12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BLM17, BCF+14, CTR14, CT18, CJSF14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DXA14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, Fe10, FSK10, Fid18, FBM12, Fre10, GO17, GFBF12, G’13, GPT12, GLW12, Ham17, Het12, HGI2, HKR+18, JT12a, KM10c, KOP12, LSM12a, Lin17, LWL10b, LGW12, LMHH14, LGH+17, LWHS17, LPO+17, MO12, MSH10, Mau12, Men13a, MR14c, Mic10b, MV12, MMB17, NNA10, NS12, Orm16, PP10a, PPH12, PG12, RW12, SY14, SG15, SOG15, Sch16, Sen10, SS13, Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16]. Cryptography [Sta11a, Ste15a, VS16, WWL+14, WY12, Wes16, Yam12, Yan11, YTS12, YL17, ZZCJ14, ZAC17, vTJ11, AMN18, AMOR13, AEH17, AAT16, AA14, ABB13, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Bi12, BSR+14, BSW12, BB16b, CFR11, Ch13b, CQX18, Ch14, CSTR16, Con12, CDS14, DDD14, Dav11, DD13, Dur15, Far14, GCV17, Har15, HH15, HZWW17, Hof16, IM14, JLT+12, JY14, JW14, K10, KGO10, Krel3, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Li12, LY14, MCN+18, MS13b, MD12a, MCP15, Mic10a, NLY12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RY10, Sac14, Sah13, SK14, SSA11, Stat11b, Sti11, Svo14, UK18, VD14, VNI17, WJJ17, WKY12, YT11a, YSC16, YXXA+18, YDH+15, YR11, ZXW+18, vDKS11, Che11, LZJX10, Nac12]. Cryptography [Cou12, Ful10, Gas13, Low12, Mel10, Mur10, Ter11]. cryptography-based [BOB13]. Cryptography [Cou12, Ful10, Gas13, Low12, Mel10, Mur10, Ter11]. cryptography-based [BOB13}. Cryptol
[BTHJ12, SBV14, WCL+18, BL11, JHCC14, LW13a, PRZB12, Suc12, YXD18].

Databases
[FCM14, HPC10, JKHeY12, Kaw15, RP12, WP17, GA11, JK13, LCY+16, SS17, TG12].
datacenters [PRN+19]. Dataset [SP13].
datasets [LVRY10]. Daubechies [Ara13, SM12]. Daunting [IBM13a].
DCT [BDB14, LP12]. DDH [LZC12a].

DDoS [PSJ+13, SP15a].

De-synchronization [XNG+14, AATM18].
deathly [HLV10]. Dealing [Sha13, VN16].
Decade [SOG15]. December [Aba10, BYL10, BC11, Che11, GG10, HWG10, LH10a, LW11a, LTW11, Yan10, Yan11].
Decentralized [ABCL17, CD16, GZZ+13, HSMY12, HK14, PPS12a, PAS13b, RVH+16, RS14, TS16b].

Decentralizing [LW11b]. Deciding [CLCZ10, Sch12c].
Decipher [Cor14b].

Deciphering [Bla16, GMNS15].
Decisions [Bel18, YWK10b]. declarations [HWYW14].
Declassified [ABJ13].

Decodable [Yek10].
Decoding [DBPS12, GMNS15, Bax14, Bul10a].

Decomposition
[AGH+17, LSL12b, gWpNyY+14, BWA13].
Decompression [PP10b]. Deconstructing [Tar10]. Decrypted [Kob10].
Decryption [CR12].

Decryption [AN12, KB10, PTK12, FNWL18, LJW+17, LJWY18, SES+16, SM10a, SM10b, Wu16, ZSW+18b].
Dedicated [Lin17, Nac12].

deductive [ABF+14].

Deduplication [QLL17, SKH17, YDY+16, KH18, SAR18b, ZFH+18].

Deep [FGR+17]. defeated [Kap13].
defects [FES10].
defences [NDNR13].
Defend [ANO17e, Sch13].

Defending [LWCJ14].
defense [PSJ+13].

Defensive [Pfl10].

Defensive [Pfl10].

Definitions [GLW12, Maui2, CGK011, KM14, KGO10, XWCX14].
Degeneracy [WH18].

degradation [MMS+17a]. Degree [KA18].
degrees [MZ17a]. Delay [CCKM16, GMNS15, LBR12, JLT+12, XW13].

Delegatable [WZ11]. Delegated [MZY15, TMC15].

Delegation [FMTR12, SSW12, XWLJ16, YZ12, YAM+15, JSMG18, NAL17, XWS17, ZWM14].
Deletion [DMS+16, Rea16].
Delfs [Mur10].

Delivery [PSS+13, SSPC12].

Demodulation [KOP12].

demonstrating [LHA+16].
demosaicking [HLC16].

Deniability [TCS14].

Deniable [DF11, zGXW12, HLLC11, HS11, Jia14b, JXLZ15, LXJ14].

Denial [BKBK14].

Dense [BFM12].

Density [LC15, LSQ11b].
density-based [LSQ11b].

Dependable [BCQ+13].

Dependency [SGP+12].

dependent [GdM16, PKA15], deployed [MFH13, RY10].
deployment [WXK+17].

DepSky [BCQ+13].

Depth [GH11a, RS16, SS10b, SS12a].

Depth- [GH11a, SS10b, SS12a].

Depth-Based [RS16].

Derivation [LBR12, Cha13a, Lau12].

Derivative [LSQ11a].

Derived [ZMM+10].

DES-like [CGCS12].

Description [WH18, PLCGS11].

Design [AMN18, Abe12, ARH+18, AIB+16, ADD10, AUM16, Bel18, BKL+13, DHB16, DR11, FSK10, HSA14, JWJ+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QL17, RYF+13, Sch13, SAAB10, SZDL14, VKP17, WKB16, WDKV19, ZHX16, CZ14, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MUY+18, ZYC+17].

Designated [WHJ17, HYWS11, RPSL10, SY15b].

Designated-verifier [WHJ17].

Designation [Che15, LSQ11].
design [Goo12].

Designer [KMY18]. Designing

Designing
[CDK\textsuperscript{+}10, FLW12, MRT10, PSD15, SR10].

Designs [BGK12, PCY\textsuperscript{+}17, KDH15].

Detailed [DLV16, ZPXX17]. Detect [JWJ\textsuperscript{+}17, NSA15, WOLP15, Lan11].
detectability [LRW17]. Detectable [Ess17]. Detecting [BGK14, Ess17, GAS\textsuperscript{+}16, HLW12, KW14, SH15, YSC\textsuperscript{+}15, LWLW11].

Detection [AMKA17, ATS15, DSB15, DF11, GZH17, HDWH12, KU14, LGL\textsuperscript{+}12, LC15, MKRM10, MKAA17, NDC\textsuperscript{+}13, NSMS14, SAJL16, SBV14, SP15\textsubscript{a}, SRAA17, SGS14, TM18, YFT17, AKKY17, AOT13, BM13, HB13, JC13, KLC\textsuperscript{+}10, Maz13, MHT\textsuperscript{+}13, WYL13].

Detective [Cho10].

Detector [LTKP16]. Detector-Based [LTKP16].

Determine [FSWF11, Sto12]. Determining [NN12].

Deterministic [MPRS12, NS12, XXZ12, DTZZ12].

Deterring [WGJT10]. DEUCE [YNQ15].

develop [Ham19]. Developed [Har16].


Device [ABCL17, CFXY17, DFKC17, KLM\textsuperscript{+}12, SRK\textsuperscript{+}17, TYK\textsuperscript{+}12, GM16, KKG14, Kim16, Par12\textsubscript{b}, SHBC19, XHH12].

Devices [AAC\textsuperscript{+}16, CSH\textsuperscript{+}18, DLWW11, EGG\textsuperscript{+}12, GPT12, GaM16, GMSV14, HHH\textsuperscript{+}13, HDWH12, JMG\textsuperscript{+}16, LWHS17, MFG16, May15, MS16, NVN\textsuperscript{+}17, Sch15\textsubscript{b}, SFE10, WKB16, WT10\textsubscript{b}, XJR\textsuperscript{+}17, Aia15, CLP\textsuperscript{+}13, CFI13, CTL12, Chi13\textsubscript{a}, FRT13, GTSS19, IB11, KPP16, KAT12, Lv11, MHV15, OYHSB14, SHBC19, TG17, ZPZ\textsuperscript{+}16]. DFA [WH17]. DFA-Resistant [WH17]. DFT [DDFR13].

DHA [AY13]. DHA-256 [AKY13]. DHTs [YKGK13].

Diagram [WGD18].

dictionary [Maf16, MBB11]. did [CMG\textsuperscript{+}18].

Diego [Ano10, Lin14\textsubscript{b}]. Dies [Mar10a, MM17].

Difference [BS14, YTP11, JK13].

Differentiating [LYWZZ12, YWW10].

[CDK\textsuperscript{+}10, FLW12, MRT10, PSD15, SR10].

Differential [BMS12, BNY14, CWP12, CGCS12, ESS15, FXP\textsuperscript{+}17, KWS\textsuperscript{+}12, LGL\textsuperscript{+}12, LJF16, LJ15, LYYH14, MRTV12, PH12\textsubscript{a}, QQGL13, RCP\textsuperscript{+}18, Sun11, WHN\textsuperscript{+}12, Blo15, DDFR13, LKK10, MNP12, PBCC14, SDM10, SDM14, TSL11, TSL16, WYL14].

Differentials [WW12]. Differing [GZH17].

Differing-Inputs [GZH17]. Diffie [LZC14, ABD\textsuperscript{+}15, Chi16, Hof16, HLCL11, HLYS14, Orm16, RH10].

Diffusion [ZHL15, WB12, JT12\textsubscript{b}]. DIG [NKWF14].

DigitNotar [JB11]. digit [KWH16].

Digital [AYS15, BBC\textsuperscript{+}13, BM13, BCP14\textsubscript{a}, FMS12\textsubscript{a}, GP17, HPO\textsuperscript{+}15, Jin10, Joh10, JL16, LZZ\textsuperscript{+}12, MBF\textsuperscript{+}13, MSL10, MMS12, NC12, pNyWyY\textsuperscript{+}14, Orm16, PH12\textsubscript{b}, PAS13\textsubscript{b}, SAA15, SM13, SC12, SOS15, TC11, TS16\textsubscript{b}, Yon11, Y\textsuperscript{+}17, YLS12, dRsdLV12, AGHP14, BPP10, CCG10, FLZ\textsuperscript{+}12, Fri10\textsubscript{a}, GMS11, Har14, KMI11, Lan13, LWZG10, MS13\textsubscript{b}, MM14\textsubscript{a}, MO14, QCX18, Sim15\textsubscript{b}, SLM10, yWpNyL11, ZZKA17, Zet14, ZMS18, Ano13\textsubscript{a}, Ano15\textsubscript{b}, Mon15].

Dilly [Bat10].

Dimensional [Ano17\textsubscript{d}, LZZ\textsuperscript{+}12, XYXYX11, DWZ12, QD16]. dimensions [Pal15].

direct [GH12]. Directed [NLLJ12, KPS10]. Direction [NS12].

Directions [BKBK14, CDFZ16, Hof16, PPA18].

Directly [LZC12\textsubscript{a}]. directory [SMBA10].

disabled [HFT16]. disassociation [TMLS12]. Disaster [NRZQ15, BBG\textsuperscript{+}17].

disclosure [DZS\textsuperscript{+}12, PKA15, SB17, WGJT10].

discovery [Ano11\textsubscript{a}, MMP19]. Discrete [BGJ14, CLL16, HKR\textsuperscript{+}18, KLM\textsuperscript{+}12, Xie12, AMORH13, BGJT13, MM13, Mes15, TPL16, VM14].

discrimination [GPVcBRO12]. Discriminative [YI14].

Discussion [Gli12, Wil18, Bul10\textsubscript{a}].

Discussions [KD12\textsubscript{b}]. Disk [GM14, Ran16].

Disks [Mar10\textsubscript{c}]. disparate [SSY12].
Dispatching [YTH17]. dispersed [ED19].
Disreputable [ABJ13]. Disruption [HK14]. Disruption-Tolerant [HK14].
Dissection [Dun12a]. Dissent [SGW+14].
Distance [PYH+18]. Distillation [BJ16].
Distinguisher [DWWZ12, AMS+10].
Distinguishers [SEHK12, ZSV+12, AY14b, AP11].
Distinguishing [KM10a]. Distortion [FHS13, Jia17, LGWY12, MM17].
Distortions [WLZL12]. Distributed [Ano10, BKKB14, BCEO15, CGB+10, FCM14, HSM14, HX+11, HCL+14, LMD16, LL15, LN+13, LWCJ14, YZX+12, YKKL12, ZLDCl5, BLV17, CSTR16, dCCSB+16, GAI+18, NCCG13, PRN+19, TG12, WX13].
Distributed-Healthcare [ZLDC15].
Document-centric [BPP10]. Documents [Bla12, HCDM12, Sta13, XZZ18, ZDL12, CH1, GA11, SR14]. does [LRW17].
Doesn’t [RS11, SS12a]. dog [Ran14].
Dual-Mode [PAF18]. Dual-Rail [HF14b]. Dummy [GST12]. duplication [LWLW11]. Durable [LY15]. Durfee [TK19]. During [FGR+17, ABJ13, RS17]. DWT [LD13, SJ12]. dyadic [MO14]. Dynamic [ABB19, EKB+16, FHR14, HH15, KYH18, LHM+15, MWZ12, MM12, NKF14, PPS12a, PNRC17, SSW12, SY14, SVK12, SGC14, VMV15, XNKG15, XWSW16, XZY+12, XWZ+18, XYL16, CT12, CSTR16, DSCS12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KH18, KPB17, LWMX12, LHM14, LZC17, NPH+14, PSJ+13, SSS+16, SSS11, SGM16, XHM14, YZL+18, YD17, ZS18].
dynamic-identity [JZS+10]. dynamical [JT12b]. Dynamics [RSCX18, AaBT16, LTC+15a, Lüd12]. dynamics-based [AaBT16]. dyslexic [Bha16].
e-commerce [Ano11a]. e-exam [Mor12].
E-health
[WXM+17, IC17, YZL+18, JKL+16].
E-Learning [Yon11]. e-mail [BTW15].
E-passport [LZJX10]. e-rental [LY14].
E-Voting [LGPRH14, E2 [WYL14]. EAC
[LZJX10]. Each [YLL+12]. EAP
[FLH13, HZC+14, ZCLL14]. EAP-based
[HZC+14, ZCLL14]. Early
[Bel18, Bro11, And13]. Earth [Har14].
easier [MBF+13]. Easy
[Bel16, SMD11, Tay14, Wu16, ZDW+16].
Eat [DSSD14]. Eavesdropping
[CWL16, Han12, PX13, YSJL14]. EC
[Dra16, CFN+14, CCG+16, CMG+18]. ECC
[BSSV12, JMW+16]. ECC-Based
[BSSV12]. ECDSA [BBB+16a, DHB16].
ECG [PLGMcD18]. ECG-based
[PLGMcD18]. Echo [DLMM+18, HGT15].
Echo-Based [HGT15]. economy [Sir16].
Ecosystems [LDB+15, MMP19]. EDAK
[ABB19]. EdDSA [JL16]. Edge
[AHM+18, DF16, KAI8, MD15, PRN+19, Sun16].
Edge-centric [AHM+18]. Edition
[Cor14a, Kob10]. Editorial [OK18].
Editors [LLK18]. Education [LRVW14].
Edwards [JL16, LT14a, YTS12].
Edwards-curve [JL16]. EFADS [WLS14].
Effect [PLGMcDF18, WBB12]. Effective
[HLT+15, KRD13, WMX+17]. Effectively
[YMC+17]. Effects
[MAL10, SKV12, SHBC19]. Efficiency
[ABF12, Chl16, DG17, FR+16, HRV10, LLML12, LCL+17a, MS13b, WXY16].
Efficient
[ABB13, ASB16, ABB19, BWL16, BCGH11, BHG12, BV11, BV14, CG12a, CM18+18, CMLRHS13, CWWL12, CJ13, DWB12, Dn12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTH11, GPN+12, GPT12, GJJ15, GH12, GHH17, GCH15, HZC+12, HZC+14, HZL18, HL10b, HBCC13, HZX15, HKL+12, HDPFGP15, HCMD12, HH16, HC17, IAD10, KPC+11, Kim15, KH16, KH10, LLP+18, LDD12, LZO12, LXK+14, LCLL15, LSLW15, LHY12, LWSH17, LZC17, LBOX12, MX13, MTY11, MVVR12, MU12, MP12, MC11, MN14, NES+14, NdMMW16, NZZ10, PB12, PAF13, PRC12, PG12, PCPK14, PNRC17, RBHP15, SGY11, SZS14, SGM16, TLF16, TWZ11, T12, TM18, WDC18, WLS14, WQZ+16, WCCH18, XLMW16, XMCL13, YHL16, YNR12a, YNR12b, YLW13, YNQ15, YLA+13, YS15, ZQWZ10, ZLH12, ZSW+12, ZXJ+14, ZXYL16, ZCL+19, ZHS+19, ZPW16, ZHW15, AZPC14, AZF+12, CH11, CCW11]. efficient
[CLHJ13, C14, Cho14, Cra11, C18, C16, EA12, FLL+14, Far14, FA14a, FA14b, FIO15, FNWL18, GH16, GL+11, H12, HYS18, ISC+16, IB11, IOV+18, JCH16, JZS+10, KKK14, KHI19, KLI1, KSH18, LLLS13, LH11a, LH10c, LXM12, LAL+15, MLM16, Mes15, Nov10, OCG11, PZBF18, PC14, Rao17, S13, S13, S13, S13, T13, TKK14, VN17, WYL13, WLZ+16, WT10a, WXK+17, XXY16, y14, ZLY14, ZZ11, ZCLL14, ZTZ16, ZZC15, Zhu13, LLLZ+12, T15]. Efficiently
[FWS13, LGH+17, SLY+16]. Effort
[RSBN12]. Effort-Release [RSBN12].
EGHR [CML+18]. eHealth [TMGP13].
eID [SGGC+16]. eight [Sun11].
eight-round [Sun11]. Einführung [Buc10].
Einstein [HR13, W15]. Elbirt [Bar12].
Election [Ess17, TKM12]. elections [QS18].
electrocardiogram [BL+19].
Electrocardiography [YH16].
Electromagnetic [HHH+13]. Electronic
[Bla12, PWVT12, SR14, YMWS11].
Elementary [Led16, Sch15a, CM13].
Elements [Kra12]. Elevation [LZC+12b].
Elliptic [AD11, AK14, ARM15, DW12, GPT12, LGH+17, LWHS17, PP12, SG15, AMN18, BAAS13, BL14, BL17, BBB16b, Choi14, Far14, IB11, KK10, MCN+18, MS13b, NZZ10, SKH15, WH17].
eLLSE [BL17]. ELmD [BDML16].
Elsevier [Ano15b]. Email [Bel16, CCS14, XJW+16, WR15]. embed [KPS10]. Embedded [AB15, BS12, BJCHA17, CFXY17, HC17, JWJ+17, LWHS17, SOG15, SK12b, SDM+12, WXY+17, YGD+17, YS15, Ano11a, CVG+13, Eis10, MFH13, XWZW16].

Embedding [KD12a, MCDB12, XNRG15, XZZ18, YE12, ZS12, EA11, MKH+12, PWLL13].

Embedded [KPS10].

Embedded [AB15, BS12, BJCHA17, CFXY17, HC17, JWJ+17, LWHS17, SOG15, SK12b, SDM+12, WXY+17, YGD+17, YS15, Ano11a, CVG+13, Eis10, MFH13, XWZW16].

Embedding [KD12a, MCDB12, XNRG15, XZZ18, YE12, ZS12, EA11, MKH+12, PWLL13].

Embedded [KPS10].

Embedding [KD12a, MCDB12, XNRG15, XZZ18, YE12, ZS12, EA11, MKH+12, PWLL13].

Embedded [KPS10].

Embedding [KD12a, MCDB12, XNRG15, XZZ18, YE12, ZS12, EA11, MKH+12, PWLL13].

Embedded [KPS10].
WHC¹⁵, WP¹⁷, WDCL¹⁸, WSS¹², Wat¹², WLC¹², WDDW¹², WZ¹⁵, WWHL¹², WMS¹², WQZ¹⁶, XNKG¹⁵, XY¹⁸, XXZ¹², XJWW¹³, XWLJ¹⁶, XJW⁺¹⁶]. Encryption [XHX⁺¹⁷, YZ¹², YZX⁺¹², Ye¹⁰, Ye¹⁴, YH¹⁶, YKNS¹², YNQ¹⁵, YKC⁺¹¹, YFK⁺¹², YCZY¹², YKKL¹², ZC⁺¹⁰, ZPM⁺¹⁵, ZDL¹², ZTY¹³, ZWTM¹⁵, ZQK¹⁵, ZMW¹⁶, ZCM¹⁶, ZHW¹⁵, ZY¹⁷a, ZYM¹⁸, ZWS⁺¹⁸, AHSL⁴, AKTH⁺¹⁷, AKKY¹⁷, Ana¹⁴, Ano¹⁵b, Ano¹⁶f, ABR¹², AMHJ¹⁰, ACD⁺¹⁵, AHH⁺¹², BLL⁺¹⁹, BAAS¹³, BC¹⁸, BG¹⁴, BSW¹², BGP⁺¹⁷, CPPT¹⁸, CFVP¹⁶, CFZ⁺¹⁰, CW¹⁴b, CLH⁺¹⁶, CMMS¹⁷, Cizb⁵, CS¹¹, Chm¹⁰, CW¹²a, CDF⁺¹⁰, CM⁺¹³, CGKO¹¹, DLZ¹⁶a, DDM¹⁷, DTZZ¹², Eve¹², Eve¹⁶, FAA⁺¹⁸, FH¹³, FSGW¹¹, FSGW¹², FMB⁺¹⁸, Fay¹⁶, GMOGCCC¹⁵, GH⁺¹³, GHPS¹³, GLM⁺¹⁶, GH¹², GLL⁺¹⁸, HWYW¹¹, HQZH¹⁴, HZL¹⁸, HWDL¹⁶, HZWZ¹⁸, HT¹³, HLRI¹⁰, LCL⁺¹⁹, LLL⁺¹⁸, LDZW¹⁹, LL¹⁶a, LW¹³c, LSC¹², Mar¹²b, MMS¹⁷c, Mes¹⁵, Mid¹⁰, Mon¹³, MSAS¹³, NES⁺¹⁴, PPA¹⁸, Pet¹², QRW⁺¹⁸, Ran¹⁶, R¹⁰, RWZ¹³, RPSL¹⁰, SES⁺¹⁶, SE¹⁸, Sar¹¹, SYL¹³, SE¹⁴, SE¹⁶, SH¹¹, SM¹¹, SN¹⁴, SLZ², SYB¹⁵b, Shal¹³, SGFCRM⁺¹⁸, SLM¹⁰, SKB⁺¹⁷, Spa¹⁶, SGP⁺¹⁷, SGM¹⁶, Tam¹⁵, TPL¹⁶, tJ¹²b, WGJT¹⁰, WY¹⁰, WYYZ¹¹, WYYY¹¹, WHY⁺¹², WDZL¹³, WLFX¹⁷, Wan¹⁸, WGZ⁺¹², WLS¹⁴, WCCH¹⁸, XWZW¹⁶, XWXO¹⁴, XSWC¹⁰, XXX¹⁵, XWS¹⁷, XWZ⁺¹⁸, YT¹¹b, yYqWqZC¹³, Yan¹⁴, YZCT¹⁷, YHMM¹⁸, YCT¹⁵, YLZ⁺¹⁶, YL¹¹, ZWQ⁺¹¹, ZZ¹¹, ZLW⁺¹², ZXJ⁺¹⁴, ZWM¹⁴, ZT¹⁴, Zha¹⁵a, ZCC¹⁵, ZML¹⁷, ZYC⁺¹⁷, ZCL⁺¹⁹, ZZ¹², ZL¹², ZDW⁺¹⁶, ZY¹⁷b, Zhi¹³, Wan¹⁴, LAL⁺¹⁵, Sar¹⁸a, Kat¹³]. encryption-based [BC¹⁸, XZW⁺¹⁸]. Encryption/Decryption [KB¹⁰]. 

Encryptions [zGXW¹², LG¹², SLY⁺¹⁶, RD¹⁷]. Encryption/Decryption [KB¹⁰]. 

Encyclopedia [vTJ¹¹]. End [Ano¹⁵c, BRR⁺¹⁵, BGP⁺¹⁷, CFE¹⁶, Chn¹⁶, RST¹⁵a, RST¹⁵b, Chi¹³a]. End-to-End [CFE¹⁶, RST¹⁵a, RST¹⁵b, Ano¹⁵c, BRR⁺¹⁵, BGP⁺¹⁷]. endomorphism [FWS¹³]. Endomorphisms [AK¹⁴, LGH⁺¹⁷], enemies [Fag¹⁷], Enemy [BC¹⁴, CAC¹⁴]. Energetic [PDMR¹²]. Energy [Ano¹⁵d, AZF⁺¹², ABC⁺¹⁷, Bla¹⁶, JEA⁺¹⁵, LSC⁺¹⁵, MP¹², PAF¹⁸, TLCF¹⁶, TCN⁺¹⁷, VN¹⁷, CZ¹⁴, ZTZ¹⁶]. Energy-Efficient [MP¹², TLCF¹⁶]. Energy-Harvesting [ABC⁺¹⁷]. Energy-time [Ano¹⁵d], Enforced [Set¹⁶], Enforcement [LLZ⁺¹⁷, Tan¹⁵a, Cra¹¹]. engagement [LSBN¹⁴], engaging [ISC⁺¹⁶], engine [BS¹³a], Engineering [Bel¹⁸, FSK¹⁰, GHD¹⁹, LLK¹⁸, SM¹⁷a, MP¹², PGLL¹⁰, TQL⁺¹⁴]. Engines [LB¹³, BGC⁺¹³]. enhance [CZ¹⁴, SLM¹⁰]. Enhanced [DTE¹⁷, KY¹⁰, KKM⁺¹³, MS¹⁷, SGG¹⁸, TV¹⁵, YCC¹⁶, AMN¹⁸, ACK⁺¹⁰, DLK⁺¹⁶, GM¹⁶, LNKL¹³, YQOL¹⁷]. Enhancement [FSX¹²b, LA¹⁵, NNA¹⁰, CHS¹¹]. Enhancements [FSX¹²c], Enhancing [CSW¹², IA¹⁵, Lan¹³, YS¹⁵]. Enigma [KM¹⁵, KM¹⁶, LHA⁺¹⁶, Orel¹⁴, 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, Din¹⁰, NB¹³]. Enterprises [KCR¹¹]. Entities [GZ¹²]. Entity [BCM¹², BCM¹³], Entropy [DSSDW¹⁴, DK¹⁶, KPW¹³, VS¹⁶, YGFL¹⁵,
BNY14]. Entropy-Based [YGFL15].

tenTTs [YL17], enumerators [ÖS11].

Environment
[AARJ12, BCGN16, KKA15, MLO17, 
MRS+17, RQD+15, SGG18, TV15, YMA17, 
FHZW18, GA1+18, HLYS14, KKM+14, 
Kim16, NR17, Par12b, SKB+17, WL12, 
WCFW18, WT10a, XXX15, YWK+10a].

Environments [HLKL15, LQY10, PAS13b, 
TMGP13, CLHJ13, CTL13, KPP16, KAS15, φN18b, LW13a, LCY+16, NACLR12, 
SCY15, Tan12b, VDO14]. Eof [Gup15].

ePassport [ABIC16], Ephemerizer
[Tan15a].

Epistemic [Sch12c]. EPR
[UUN11]. Equality [HTC+15, LLSW16, 
MZN15, HTC17, ZCL+19]. Equational
[AHRJ12]. Equations [BB10, SR12a]. Equi
[PD14]. Equi-Join [PD14]. Equipollent
[Ber17]. Equijoin [WP17]. Equivalence
[AHRJ12, CCK12, CCCL16, GLW12, SS13, 
WGD18, HKT11]. era [QCHX18, ABJ13].

Ergodic [IAD10]. Erratum [YFK+12].

Error [KW14, LSC+15, MCP15, TCF16, 
ATI+10, Chl13a, LTT10]. Error-correcting
[MCP15, LTT10]. Errors [TM18, CSS+13].

ErsatzPasswords [GAS+16]. Escrow
[MR10, WLY17, ZLH+12, HXXK13].

Escrow-Free [ZLH+12]. Escrowable
[NCL13]. eSkyline [BKV13]. Espionage
[LIJ+14]. Essay [Bai12]. Essays [Nac12].

Establishing [DKL+16, GSFT16].

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

Estimation [BCF16, GSN+16]. Estonian
[Ano17c]. Ethernet [KCR11]. EU [PH12b].

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

Evaluating [RAZ15, WP15]. Evaluation
[BKL16, CGCS12, DM15, EGG+12, 
KV+E18, KLM+12, MKN13, MLBL12, 
SMOP15, ZLDD12, FPBG14, TPKT12, 
ZZKA17, ZLDD14]. Evaluations [ZM16].

Evaluators [ZZKA17]. Evasive [BBC+14].

Eve [AAE+14, ERLM16, FH+12]. Even
[AR14, LPS12, Ana14, DKS12].

Even-Mansour [LPS12]. EventGuard
[SL11], every [Hof16], everyday [HST14].

Everyone [Ano15c]. Evidence
[Bla12, SR14], evident [MN10]. Evolution
[LQY10, Tay17, BHvOS15]. Exact
[TKM12]. exam [Mor12]. Examination
[VCK+12]. Evaluating [SP13]. Example
[KDI12b]. Exchange [CLY14, CST+17, 
DG15, FVS17, GZ12, HC12, LY16, MSU13, 
TYM+17, WSA15, WT10b, YS12, YL13, 
YRT+16, Yon12, ZTH16, AKG13, AIB+16, 
FHH10a, FA14b, FIO15, GBNM11, 
GLM+11, Jia14b, KMTG12, LWS10, 
LML+13, SEXY18, TCS14, Tso13, TKKH14, 
WHJ17, WZM12a, WZM12b, WT10a, 
WT12, YW13, ZXY18, ZG10].

Excitation [SOS15]. Exclusive [Men13b].

Execution [AHRJ12, RQD+15, YS15].

Existing [FMA+18, HT13]. Expanding
[MS16, Sch15b]. Expansion [LTC+15b, 
TS16a, BAC+13, Die12, JMK13, Pet11].

Expectations [DY13]. Expected
[DMV15, KOTY17]. Experience [AD12].

Experiences [JAE10]. Experimental
[LCW+16, DHW+13]. Experimentally
[LHA+16]. Experts [Sto12]. Explicit
[AQD12, FHS13, FIO15, ZZC15].

Exploitability [CFN+14]. Exploitation
[MAK+12, NCCG13]. Exploiting
[ACK+10, BDG15, VDB+16, ZW+18].

Exploits [ZGC16]. Exploration
[AUMT16, ABDP15, RYF+13]. Exploring
[Cil11, FNP+15, TCF16, WHC+15].

Exponent [SM10a]. exponentially [RK11].

Exponentiation [VN17], exponents
[SM10b]. Exposing
[EYMT16, OF12, YQH12, YSC+15].

Exposure [BVS+13, TK19], expression
[WR15]. Extend [TMC15]. Extended
[BFMT16, DGP10, Gre17, HZW+14, 
HBG+17, SH15, Yam12, YSC16].

Extending [ZSW+12]. Extensible [YZ12].
Extension [ARH14, EKP+13, GFBF12, GT12, RW12, SGY11, HTC17, ZXJ+14]. Extensions [LWL10b, external [ZZKA17].

Extract [AN12]. Extract-Transform-Load [AN12].

Extractability [BCP14b]. Extractable [CZLC12b, CZLC14, GGH17].

Extraction [BWLA16, GST13, GPT14, PCKP14, GPP+16]. extractors [Zim10].

extraordinary [Hol12]. extreme [GJ13].

Extruded [CJFH14]. Eye [ERLM16, SM13, Tox14].

F5 [LLY+12b]. Fa [FMS12a]. fabricating [WW13]. Fabrication [VDB+16].

Fabrication-Induced [VDB+16]. Face [AQRD12, XHH12]. Facial [KRB12].

facilitate [Chi13a]. Facsimile [Ano16d].

Factor [HXC+11, LLC11, AIB+16, CLP+13b, DMWS12, ED19, HC12, IC17, JKL+16, JM16, Kem11, LNK+18a, LNK+18b, Lit14, WW14, Wat14a].

Factoring [APPVP15, LLML12, MM13].

Factorization [Cou12, FS15, KFL+10, Kuz11, YAM+15, Mes15, TPL16]. Failing [Cer14].

Fails [ABD+15]. Failure [WCL+18]. Fair [ALR13, CSV15, DMM14, DG15, WAS15, SEXY18].

Fair-Exchange [DG15]. Fairness [ALR13, Ash14, GHKL11, Wag16, MV16].

Fake [KU14]. Fallen [HCP12]. False [LLZ+12, CDG12].

Families [BSS+13, KU12]. Family [ARH+18, BMS12, BKST18, DG12, DJG+15, FLS+10, FFL12, GNL12, LYY+18, MGF16, YCL17].

Fanin [SS12a]. Fast [BLAN16, Bui12, CHS15, DSLB18, GSN+16, N12, PRSV17, WHZ12, WBA17, WQZ+13, ZHW+16, FHH10a, KHMB13, MB11].

FastAD [SMBA10].

Faster [CN12, HVL17, TH16, Ant14]. Fault [AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JT12a, LGL+12, LCLW17, LGLL12, MKRM10, MKAA17, PH12a, RZZ+15, SEY14, YGD+17, BBP13, PBCC14, WMYR16]. Fault-Based [BBB+16a]. fault-resistant [PBCC14].

fault-tolerant [WMYR16]. FBI [Bha16].

FC [DDS12, Dan12]. FEAD [ZWM14]. Feasibility [AAC+16, FKS+13, WHC+15].

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

Features [Y14, ZTL15, FNP+15, LCM+17, LTC+15a].

Fauveau [Ara13]. February [Ano10, DDS12, Dan12, Dun12b, K11a, Lin14b].

FedCohesion [CCFM12]. Federated [BS13b, CCFM12, CSL+14, CMBS10, JAS+11, TODQ18].


Fiat [BDG+13].

Fibonacci [FM15, LLP+18].

Fibonacci-number [LLP+18].

Fidelity [BCP14a].

Field [CLF+17, GHPS31, HSA14, SS12a, TGC16, ZAG19]. Fields [ARH14, BGT14, HVL17, AA14, BGT13, CZ15a, LBOX12, ŌS11].


Filter [Kaw15, ATKH+17].

filtered [HTC17]. filtered-equality-test [HTC17].

Filtering [LLZ+12, CDG12].

Financial [Ano11b, Ber12, DDS12, Dan12]. Finding [Hof16, Ste15a]. Fine [CDD13, YTH17, ZML17, CLH+16, FSG11].

Fine-Grained [CDD13, YTH17, ZML17, CLH+16].

FinFET [ZJ11]. FinFET-Based [ZJ11].

Finger [KLY+12].

Fingerprint [MR14b, KKG14, ZHH+17].

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

Finite [BGJT14, CHS15, GMNS15, HVL17, AA14, ...]
CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, LMGC17, LSLW15, LSC12, MVV12, MSM18a, Nac16, NCCG13, PB12, SGH15, Vai11, WHC+15, XWZ+18, ZZ12, GH13, XZJ+14, ZML17.

Fully-Homomorphic encryption [GH11b].

Fully-Homomorphic-Encryption [CN12].

Fun [APPVP15].

Function [AMPH14, Bee17, BKST18, FLS+10, LyWIZZ2, MMS17b, SGY11, WSSO12, AKY13, AP11, CMMS17, LK14, LP11, RS14, Sar11, SXL16, TQL+14, WYW14].

Functionalities [AS16, BV18, BSW12, Boy13, GGH+16a, GVW12, LQD+16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14].

Functionalities [JR13]. Functions [ACZ16, ALR13, BCB+14, BKK14, BKPW12, BK12a, CPS16, DQFL12, FLY11, LVV11, NR12, Rja12, RW12, SMS14, SLX+16, Tan12a, YTP11, AY14a, BDP11, CG12b, CQX18, CW12a, ESR14, Gen10, HRV10, Li10, QZDJ16, WT13].

Fundamentals [Joh10]. Further [HCL+14, WHY+12]. Fus [FMS12a].

Fusion [ABCL17].

Future [AYS15, BCB+14, Bon12, CDFZ16, GCK12, HYS18, Mon13, Aso13d, FBPBG14, Mac12, PPA18, PHWM10, MJS13].

Future-proof [Mon13].

Fuzzy [KRDH13, NCL12, SH11, XJJW13, Alp18, KHM13, MMS13, SM11, SN14].

FV [MRL+18].

G [HLYS14].

G2 [BP18].

G2C [BMP12].

GA [MMSD13].

GA-fuzzy [MMSD13].

Gadgets [Gel13].

Gait [XJR+17, XJR+17].

Gait-Based [XJR+17].

Gait-Key [XJR+17].

Gallai [SS10b].

Galois [CFR11, CLF+17, HSA14].

Gambling [Ana14].

Game [MZA+13, LPZJ15, SD10, SKEG14].

Game-theoretic [SD10, SKEG14].

Gap [LRWW14, TMGP13, PPA18].

Gaps [SPM+13, DKL+16].

Garbling [App13].

Gard [Kap11].

Gate [Kar12].

Gates [App13].

Gateway [WZM12a, WZM12b, WLI11, WXK+17].

Gateway-oriented [WZM12a, WZM12b].

Gaussian [HR1+18, YWL+17].

GCD [K111].

GCHQ [Ald11].

GCM [SKK10].

GCM/GMAC [SKK10].

GDL [MMZ12].

Gear [AHS13].

Geckos [GSC17].

Geese [Bai12].

GenePrint [HQY+16].

General [HYS18].

General [Bar16, CJXX19, FJHH12, GFBF12, Gue16, HP12, KOTY17, LPL15, PB12, SJWH+17, YFF12, ABDP15, Bai12, DGJN14, HQZH14, LWS10, WSI2, YCI11, ZYC+17].

General-Purpose [Gue16, ABDP15, DGJN14].

Generalisation [LR15].

Generalised [Hes12].

Generalization [GMNS15].

Generalized [BFMT16, LPL15, PC14, TY16b, Ye14, ZAC17, ADG16, BNST17, KLI11, NC13, YMSH10].

Generated [ADD10, LCL17b, NN12, XYXY11, AGHP14, LW13b].

Generating [Ano16e].

Generator [ADD10, BK12a, CDK+10, MVV12, NNAM10, NKWF14, CFY+10, LGK10, MRT10, PLSvdLE10, SH11, SM11, XSWC10].

Generators [AS17, DSB18, LTKP16, MFG16, NIS12, PFS12, CP13, HRV10, MG15, Sti11, Zim10].

Generic [BWL16, BR14, Chi16, GWWC15, HXC+11, Sar10b, SY15a, WCL+18, ZCLL14, HQY+16, YT11b].

generically [MHKS14].

Genetic [JK13, MM17, ASVE13, EEAZ13, PTK14].

Genius [Hai17].

Genomic [BKLS18, RCP+18].

Gentry [GH11b].

Genuine [HR13].

Genus [FWS13].

Geo [Har14].

Geolocation [Har14].

Geodesics
Handover [HBCC13, LBR12, CLM12, CML18, HZWW17, QMW17, YHL16, YHHS16, YLS12].

Hands [GPT14, BSS11], hands-on [BSS11].

Handshake [KK12, KK13, WZ11].


Hard-to-Invert [ZWTM15]. Hardcover [Joh10]. Harder [KTA12, Sch16]. Hardness [BHKN13, SS13]. Hardware [AW17, BRPB13, BDMLN16, BJCHA17, CMLRHS13, DOS15, ERRMG15, GP17, GCVR17, GCS13, HKL14, HSA14, HC17, HLN10, KAK18, LGH17, LLKA19, LRW14, MLCH10, MCS15, MRL18, MYH18, NDC13, NdMMW16, PC16, PG12, RPM10, SN10, Set16, Tay17, WOLP15, ZHS19, ZAG19, AMN18, BDM18, BGG13, KHF10, MD12a, NS10, Nov10]. Hardware-Assisted [LLKA19]. Hardware-Based [HLN10]. Hardware-Enforced [Set16]. Hardware-Intrinsic [SN10, NS10]. Hardware/Software [MRL18].

hardwares [SKH15]. Hardy [Xie12]. Harmonic [YWNW15]. Harnessing [DFKC17]. Harvesting [ABC17, ZGC16].

HAS-160 [WLC12].

Hash [Ano12, AMPH14, BHH15, BKST18, BK12a, CLP13a, jCPB12, CZLC12a, CZLC12b, CZLC14, CJP12, EAA16, FLS10, GI12, HCPLSB12, Hüll13, HRS16, HBG17, MKF16, MCF17, MKAA17, NTY12, NR12, NXB13, PTT16, Rja12, SGY11, WSSO12, ZZM17, AY14a, AKY13, AP11, CJP15, ESR14, KGG14, PPB16, RS14, SPLHCB14, SXL16, WWY14].

Hash-Based [BHH15, GI12, HCPLSB12, Hüll13, HRS16, HBG17, MKF16, MCF17, MKAA17, NXB13, CJP12, CJP15, PPB16, SPLHCB14].

Hashing [AAE14, ASBdS16, BHKN13, BKL13, BP18, Kaw15, CP13].

Haskell [Rus15].

hatching [WYK12].

Health [HSH11, PYH18]. HDH [PDNH15].

Headline [YGFL15]. Healthcare [BN14, HLKL15, ZLDC15, ASO14, Kim16].

Healing [Bla16].

Heartbeat [IA15].

Heartbleed [DKA14, Ven14].

hedging [RY10].

Heights [Gen13].

Helios [CFL16].

Hell [Han12].

Hellman [ABD15, Chi16, Hof16, HLCL11, HLYS14, LZC14, Orm16, RH10].

Helmut [Mur10].

helped [Smi11a].

helper [RWZ13].

HeNB [CLM12].

Herodotus [Keb15, Mac14].

heroine [Fag17].

Heterogeneous [SP15b, AIKC18, ABB19, SZMK13, SCKH10].

Heuristic [BGJ14]. HEVC [DG17, GKS17]. HIBE [LIW11c].

Hickory [NN15].

Hidden [FMS12b, PSS13, YLY12, ZYT13, BDK11, LCL17a, Sch15c, Smi15a].

Hiding [DCA18, GGH16b, GI10, JHNN12, MK12b, OT12, XLM12, XGLM14, ZXW15, Ara13, DDM17, HZ18, KWH16, LXLY12, LT14b, UUN11, WLH13, WZLW13, ZWM14].

hiera [Lac15].

Hierarchical [ADIM2, BSSV12, FSB12, WL11, NMS14, NLY15, OT12, WYML16, ZMW16, ZHW16, DSCS12, HYLB18, KPB17, LFZ17, NM10, RG10, SE14, SE16, WYY12].

Hierarchy [NA10b, VN16].

High [AW17, ASBdS16, Ano17d, ARM15, Bar15, BDL11, DM15, DG17, GL12, GCS13, HZ11, KMP11, KPC16, KAK18, LTKP16, LCK11, LPO17, MS13b, MS13c, PCPK14, WYCF14, WL11, XNRG15, ABB13, GZH12, GCVR17, K13, MAK12, RS17, WLH13, WXY16, WZ11, WKH11].

High-Assurance [Bar15, KMP11, WL11].

high-capacity [GZH12].

High-Dimensional [Ano17d].

High-Efficiency [DG17].

High-Impact
High-Level [AW17, KPC+16, ABBD13].
High-Performance [GCS+13, KAK18, LPO+17, GCVR17].
High-Rate [PCPK14].
High-Security [WYCF14, BDL+11].
High-Speed [ARM15, HZ11, LTKP16, BDL+11, KL13].
high-throughput [YCG14].
Higher [LWKP12, PRC12, gWpNyY+14, ZSW+12, LWKP14].
Higher-Order [LWKP12, PRC12, ZSW+12, gWpNyY+14, LWKP14].
Highly [SZDL14, ACD+15, DT13].
HIGHT [CWP12, WWBC14].
Hijacking [DCAT12].
Hill [KPW13, KA17].
Hillstone [XRT+16].
HILL [KOS16, HAK18].
Himimo [GMRT+15].
Hindering [BTPLST15].
HISS [DT13].
Historians [Cer14].
History [ABJ13, Ano19, Cer14, Cop10a, LT14b, McK10, McK11, SE16, Smi15a].
History-free [SE16].
Hitler [Hea15, Moo14].
HMAC [GWM16, MAK+16, YGS+17].
HMAC-DRBG [YGS+17].
HMAC-SHA256 [GWM16].
Hoc [SH12, PD14, She14, XHC+12, KM10b, LXJ14, SGGCR+16].
Hoffstein [Mei10].
Holden [Ano17b].
Holocaust [Han12].
Holy [Wat15, Mic10a].
home [KPP16, Cor14a].
Homogeneous [HT11].
Homomorphic
AKP12, BV11, BV14, BGV14, CMO+16, CN12, C13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHPS12, KOS16, KGV16, Kim15, Lai17, LCLL15, MLO17, MSM18a, MRL+18, MBF18, Nac16, PTKK12, RCP+18, Tan15b, Vai11, WHC+15, XZW+18, AKKY17, BDOZ11, BC18, C18JX19, CW12a, GH13, GHPS13, GLM+16, LL1W6, SEXY18, Tam15, WSC14, ZXJ+14, ZYC+17].
Homomorphism [Bra13].
Honey [JR14].
Hop [RWLL14, LCT+14].
Hop-by-Hop [RWLL14].
Hose [SR+14].
host [LKKL13, der10].
hostile [CDA14].
CJP12, CJP15, EA12, HQY+16, KI11, KL13, NLYZ12, YTM+14. **identified** [AZH11].

**identifier** [MJS13]. **identifiers** [Cer18].

**Identifying** [CSV15, SVG16, ZCWS15].

**identities** [GLM+11]. **Identity** [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, CZLC14, CGL+12, CGY+13, Chi12, FHH10b, FZT14, FSX12b, FSX12c, GY13, GJJ15, GJZ17, HZC+12, FSM14, HZK15, LMO12a, LMO12b, LMO17, MBF+13, MJGS12, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SS12a, SAAB10, Sch11, Ser12, SPPC12, SKGY14, SWW+16, SGH15, TKRK14, Tia15, TH16, TMGP13, Vle12, WY10, Wan14, XXZ12, XQL11, XJW+16, YXZ+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCYZ12, ZLH+12, ZMW16, ZD+16, ZPXX17, ZYM18, ZS12a, ZTSL12, AKH+17].

**identity** [Ano13d, BMBS10, BOB13, BM12, BBGT12, CTHP13, dCCSB+16, DZ14, Din10, DWZ12, FA14b, GMRT+15, GPVc14BO12, HZC+14, HWDL16, HZWW17, HLR11, HWW12, HL11, HPY10, Hwa11, JZS+10, KKGK10, KK+13, KLI11, LKKL13, LK12, LXMW12, LCT+14, MMS+17a, MD15, MGP10, MJS13, ML16, MM13, NCL13, ÖS11, PLCGS11, QYWX16, RG10, SSY12, SE14, SE16, SR10, hSSZ15, SA16b, Sim15b, SSAF11, SS11, SGM16, WYYZ11, WYXY11, WSC14, WLFX17, WM+17, Wat14b, WW17, WX12, XCL13, XHM14, YWL+17, yYqWqZC13, YYS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZZ12, LZJX10, PN10, Sar18a, Kat13].

**Identity-Based** [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL+12, CGY+13, Chi12, FHH10b, FZT14, FSX12b, FSX12c, GY13, GJJ15, GJZ17, HZC+12, FSM14, HZK15, LMO12a, LMO17, LTZ16, LSLW15, LI11b, LSC12, LBR12, LMO17, RDZ+16, SGH15, Tia15, TH16, ZD+16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HWDL16, HZWW17, HLR11, HWW12, HL11, HPY10, Hwa11, LK12, MJS13, MM13, NCL13, QYWX16, RG10, SE14, SE16, hSSZ15, SA16b, SSAF11, SGM16, WLFX17, WX12, XCL13, YWL+17, yYqWqZC13, YKC+12, YXA+16, ZZ12, LZJX10, Kat13].

**Identity-Hidden** [PSS+13]. **IdM** [ACAT+15]. **IDs** [SOS15]. **IEC** [BCM12, BCM13]. **IEEE** [IEE10, IEE11b, IEE13, Yan10, BOB13, CL11, FLH13, NBZP17, ZBR11].

**IEEE802.16e** [HLCL11]. if [ABJ13, Rus15].

**IFIP** [GLIC10]. **IFP** [MMZ12]. **Igor** [Sha10].

**II** [Mun17, SCPSN10b, SMOP15, ZWS+18].

**III** [SMOP15]. **Illegal** [ABJ13]. **Illogical** [Hel17]. **Illumination** [KLY+12]. **Illusion** [GHS14]. **Illustrated** [Cop10a]. **Im** [BGI+10, BGI+12]. **IMA** [Che11]. **IMACC** [Che11].

**Image** [Bai10, BAAS13, BDB14, BWR12, CJFH14, DA10, IAD10, JKHeY12, KPS10, LA15, LLL17a, MBC15, MAL10, MNS+18b, PWW10, RS16, VFRS12, SH11, SM11, SJ12, SGP+12, SMSK18, SSA13, SRAA17, SSZT18, TB18, WHZ12, WZXL12, WYW+13, WYCF14, yWXyZ+18, YWK12, YLL+12, YWW15, Ye10, Ye14, YH16, YXD18, ZXX+11, BWA13, BM13, CT11a, CW14a, EA11, FMB+18, GKCK11, HLC16, KM11, LXCM13, LW10, LWLW11, LW13b, LPZJ15, MO14, MS17, NES+14.
PTK14, SE18, Schi2a, SM13, SM12, SNM14, SGFCRM+18, Sun16, jT12b, TTL10, TLL13, UUN1, UUN13, yWpWyNp13, WGZ+12, WKh11, WdS12, XSWC10, YWL+17, YC11, YCC16, ZLY+12, ZT14, ZSMS18, ZL12]. **Image-Guided** [CJFH14].

**Image-Scrambling** [LLL17a].

**ImageMagick** [Tay14].

**Imagery** [BCP14a, Ara13].

**Images** [BCPV11, BBM15, CLF11, FR16, GL10, LC15, LLY+12b, MR16, Yam12, dRsdiVC12, AMK12, DD13, HWYW14, LW13b, MM14a, MKH+12, UUN13, WLH13, WZLW13].

**imaging** [WW13].

**IMFlexCom** [PAF18].

**IMI** [PN10].

**imitation** [Hai17].

**Impact** [Alo12, BLS12, DM15, SF12].

**Impartial** [BCF16].

**Imperceptibility** [HGT15].

**Imperceptible** [Lin14a].

**Imperfect** [ABD+15, BHvOS15].

**impersonation** [AATM18, GBNM11].

**Implants** [Mic16, SSPL+13].

**Implausibility** [GGHW17].

**Implementation** [BW16, BKLS18, BSJ15, BDMLN16, EGG+12, GP17, GL12, GPT12, GCS+13, HF14b, KB10, KGv16, MFG16, MAS16, NdMMW16, QLL17, RMP10, VKP17, ZPM+15, AMN18, BDP+12, GH13, HBBRM+16, KY10, KSH18, MM14a, MNNW15, NES+14, PBCC14, SK14, SAAB10, SF12].

**Implementations** [BFCZ12, BFK16, BDGH15, BJ10, Bru12, CMLRHS13, CBL13, ERRMG15, LGH+17, MLCH10, TOni16, YZLC12, ABBBD13, ABF+14, BFG+14, BJ+14, CFN+14, CGH17, LBOX12, Sta11b, ZSW+18a].

**Implementing** [Dav11, GH11b, HTZ12, LTC+15a, SG15, SLM10, VOG15, SA16b].

**implicit** [DWZ12].

**Imply** [ALR13, LRW17].

**Importance** [YL17, MLMSMG12].

**Important** [TC10].

**Impossibility** [ACM+17, BCF+14, Mat14].

**Impossible** [Blo15, CWP12, LJF16, TSL11, WYL14, WW12, MNP12, SDM10, SDM14].

**improbable** [TS16a].

**Improve** [AQD12].

**Improved** [Ber18, BCP14a, Chi12, CGKO11, GLLSN12, IK15, JHL12, KZG10, LT14a, LWZ12, LJF16, LHH11, LCC13, LC15, LLML12, PH12a, QZ14, SK12a, SEHK12, SS10a, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GL13, HWB12, PK12, SDM10, XHH12, Wan14].

**Improvement** [FRS+16, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNM+11]. **improvements** [EA12, HRV10, Tso13].

**Improving** [AB15, BCM+15, Chi16, FMS12b, GMS11, HLCL11, MHC12, Sar10a, SS11, YWF18, YKBS10].

**IMS** [IG11, MEFO12].

**In-Memory** [PAF18].

**Incentive** [SJWH+17, YTH17].

**Incentive-Aware** [YTH17].

**Incident** [CCG+16, CMG+18].

**Inclusive** [FD11].

**Inconsistencies** [YSC+15].

**inconsistent** [OF12].

**Increase** [NNAM10].

**Increasing** [AEH17, CLZ+17, PKS18].

**Incremental** [KKM+14, MPR12, CS11].

**Incrementing** [KS15].

**IND-CCA** [AHS14].

**IND-CCA2** [Gal13, MVVR12].

**indefinite** [Svo14].

**Independent** [FCM14, MTY11, MKRM10, YE12, ZTL15, BV12, DDD14].

**Index** [LHKR10, PSS+13, ZXYL16, Jou13, LLHS12, LW13a].

**Index-Based** [ZXYL16, LLHS12].

**Indexed** [WXLY16].

**Indexing** [HCDM12].

**India** [BC11, CGB+10, GG10].

**Indicator** [KU12].

**Indicators** [YT12, Pal16].

**Indirect** [ABS+12].

**Indistinguishability** [AS16, BV18, FMY15, GHGHR14, GG+16a].

**Indistinguishable** [LG12].

**Individual** [LMB12].

**INDOCRYPT** [BC11, GG10].

**Induced** [VDB+16].

**induction** [BBBP13].

**industrial** [GHD19].

**Industry** [Ano11b, ZQL+16a, Cha13c, Men13b, ZSMS18].

**Infective** [GST12].

**Inference** [Bro11, DBPS12, NC12].

**Inferring** [BPSD17].

**Influence** [RSCX18].

**Information** [AQD12, ABC17, Bai10, BF11, CVM14, CDGC12, CGB+10, CST+17, CBL13, Dew11, DP12, FHKP17, FHS13,
Intrusion
[NSMS14, SAJL16, SBV14, YKC+12].

Invention
[GSFT16, NDG+17, SCKH10, TW14].

Invariant
[CM13, Buc10, Led16, Sch15a, Ful10, Mur10].

Invariants
[BAAS13, ANS12, ABB19, BN14, BVS+13].

Inversion
[Orm16], [Ant14].

Inverted
[KHHH14], [ZWTM15].

Inversion-based
[YKC+12].

Inverting
[SLY+16, UUN13].

Inverses
[SPM+13].

Inversion-based
[Bla16, Har14].

Invisibility
[BN14].

Invisible
[Keh15, Mac14, SYL13].

InvisiMem
[AN17].

INVISOIS
[AARJ12].

Involving
[HLC11].

IOT
[AATM18, CCM17, CSH++18, FQZF18, GAI++18, MMP19, NVM++17, SGC16, TODQ18, TG17, WCFW18, WXX++17, YFT17, YTH17, ZCWS15, ZLY++19].

IoT-Based
[YTH17, ZLY++19].

IoT-Enabled
[SGC16].

IoTs
[SAJL16, ZSW+18a].

IP
[AGLW16, AZH11, PJ18, PA10, RS17, SP15a, TJZF12, WBC++10].

IP-SEC
[PA10].

IPE
[ZM16].

iPhone
[Wu16].

IPs
[GSFT16, NDG++17].

IPv6
[KP12].

IRC
[HB13].

IRC-based
[HB13].

IREW
[JKHeY12].

irregular
[YWL++17].

ISBN
[Ano15b, Ano17b, Bai12, Joh10, Mur10, Sch15a].

ISBN-13
[Joh10].

Isetl
[Dan12].

ISO
[BCM12, BCM13, TS16a, WWBC14].

ISO/IEC
[BCM12, BCM13].

Isogenies
[Y++17].

Isogeny
[KAK18, Lau17].

Isogeny-Based
[KAK18].

Isolated
[YS15].

Isolating
[LG12].

ISSAC
[Wat10].

Issues
[ABHC++16, PZPS15, JAE10, KJN++16, MHV15].

ISTE
[Ano15b].

Italian
[Sac14].

Italy
[Cra12].

items
[YD17].

Iterate
[HHR11].

Iterated
[LPS12].

Iteration
[CCZC13].

iterative
[SXL16].

ITUbee
[FXP+17].

J
[Bar12, Led16, Sch15a, WZM12a].

J2ME
[GPT12].

J2ME-Enabled
[GPT12].

Jacobian
[BAAS13].

Jacobian
[Hes12].

Jacques
[Nac12].

Jamming
[YSJL14].

Janet
[Ayu12].

Japan
[Sah13, Maf16].

Japanese
[Don14].

Java
[GPT12, XHH12].

Jaypee
[CGB+10].

Jean
[Dew11, Nac12, SR14].

Jean-Baptiste
[Dew11].

Jean-Francois
[SR14].

Jean-Jacques
[Nac12].

Jeffrey
[Mei10].

Jill
[Mei10].

Joe
[Car11].

John
[Wes16].

Johnny
HM12, RAZS15].

Join
[PD14].

Joint
[ABF12, LC15, PMZ13, TCN++17, LSQ11b, ZC12].

Jonathan
[Ful10, Mou15].

Jones
[Ber16a].

Jose
[ACM11].

Joseph
[Mei10].

Joshua
[Ano17b].

Journey
[CFST17].

Joux
[AY12].

JPEG
[AOT13, LSQ11b, LC15, MAL10, QZ14, SK12a, WHZ12, WLH13, ZC12].

JPEG-2000
[ZC12].

July
[Wat10].

Junction
[VDB+16].

June
[ACM10, ACM11, Gil10, Kap11, Wes16].

Juniper
[CCG++16, CMG++18].

Juraj
[Gas13].

Just
[Pfl10].

JXTA
[AMHJ10].

K2
[PS12].

Kalyna
[OGK+15].

Karatsuba
[BCL14, MRL++18].

Karpunen
[BCPV11].

KASE
[CLW16].

Katz
[Ful10, Mou15].

KDM
[MTY11].

Keccak
[BDP++12].

keep
[Rus15].

Keeping
[CG14b, Man13, Gup15].

KEM
[CSLC14].

kept
[Cha13c].

Kerberos
[SCKH10, TW14].

Key
[ASN12, Ano11b, ABB19, BN14, BVS++13, BL12, BBB++16a, Bar16, BCO13, BKLS12, BF11, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CJ13, Chi16, CCT++14, CNT12, Cou12, CMA14, DWWZ12, DL12, EAA++16, FZT13, FVS17, FBM12, GFBF12, GT12, GZZ++13, GSW++16, GST13, GPT14, Gir15, GKS17, GZ12, GLB++18, HSMY12, HLLG18, HC12, HL10a, HCL++14, HHT++15, HHT++15].
HEC + 12, Jia14a, JEA + 15, KP12, KTT12, KFOS12, Kim15, LLSW16, LCLL15, LQY10, LY16, LH11b, LSQ18, LCCJ13, LYY + 18, LBR12, LLH18, MZHY15, MVV12, MNP14, MTY11, MMY12, MPRS12, MNS11, MSU11, NNA10, NYR + 14, NTY12, Orm16, PSM17, PND15, PCK14, Pav12, PNRC17, RVH + 16, RSBGN12, RW12, San12a, SK11, SNJ11, SEHK12, SK12, SWM + 10, Sia12, SGH15, SLY + 16, TMC15, TYM + 17, TM12, WP17, WSS12, WLC12, WZ15, WCL + 18, WWHL12, WT10b, XNK15, XXZ12, Xio12, XLM + 12].

Key [XJWW13, XGLM14, XZLM15, XJR + 17, YM16, YZX + 12, YS12, YLW13, YRT + 16, YL17, Yon12, YK + 11, YFH16, YZ17a, AA14, AKH + 17, APK + 18, ABB + 14, AKG13, ABI + 16, ABW10, AN15, BSGD12, BB14, BJ16, BSW12, BGG + 13, BBB16b, CFL13, Cha13a, CSD18, CLZ + 17, CTL13, CML16, CLCZ10, DLK + 16, DGS12, Dur15, FHH10a, FA14b, FIO15, FHZ18, GMRT + 15, GPP + 16, GH16, GBNM11, GLM + 11, GTSS19, HPC12, HZWW17, HWB12, HL11, HLYS14, HTC17, IM14, ISC + 16, IB11, IOV + 18, JSDK + 16, JLT + 12, Jia14b, JSMG18, KDH15, KMTG12, KKG14, KIH19, KP18, KLG + 16, KDW + 17, LLLS13, LLP + 18, LWS10, LIK + 17, LP10b, LW13b, LZC14, LML + 13, MNP12, MRT10, NAACL12, NCL13, Nos11, Nos14, RG10, RW13, RPSL10, SES + 16, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZZ15, SA15, SGD + 17, SvT10, TK19, TSI14, TLL12, Tso13, TKHK14, VN17, WXYZ11, WDKV19].

Key-Aggregate
[CTT + 14, LSM17, GLB + 18, CLW16].

Key-Agreement
[WSS12, APK + 18].

Key-Alternating
[BKLS12].

Key-Based
[Xio12].

key-correlations
[Sar14].

key-delegation
[JSMG18].

Key-Establishment
[BCO13].

Key-Extraction
[GPT14].

Key-hash
[KKG14].

Key-Insulated
[FZT13, LH11b, HL14, IY15, LLLY15, LH13, LW10, LLL + 18, RW13].

Key-Length
[GT12].

Key-Length-Based
[PNRC17].

Key-Policy
[GZZ + 13, GSW + 16, HSMY12, RVH + 16].

Keyed
[KE19, MMS17b, YHMH18].

Keyed-Function
[MMS17b].

KEYing
[TW14, BCPV11].

Keyless
[PDPR12, ZW + 18].

keyrings
[MBB11].

Keys
[ASN11, BF12, Bro17, CC10, HDWH12, MS16, PSM17, TW14, ZMW16, CMG + 18, HL14, IY15, LLY15, LH13, LW10, LLL + 18, RW13].

Keystream
[SM11].

Keystroke
[AABT16, SP13, CTL12, LTT + 15a].

Keyword
[CLW + 14, Che15, HCDM12, LSQ18, WDDL18, XSW16, XJWW13, ZXY16, BL11, CLH + 16, FSGW12, GZS + 18, LKY + 14, OSSK16, SY15b, WH + 12, WXY16, XWY + 18, YZCT17].

Keywords
[CWWL12, ZZ11].

KGC
[YT11a].

kid
[Tan17a].

King
[ABJ13].

kiss
[HU15, Ros11].

KLEIN
[GNL12].

Kleur
[XY18].

Knapacks
[Du12a].

Knebl
[Mur10].

knocking
[KSB + 17].

Know
[BC14, CAC14, XTK10].

Knowledge
[CLP13a, COP14, GJO + 13, GOS12, IW14, MX13, MT12, OOR + 14, Fan14, TSH14, Ano11a, KPP16, LLL + 19].

Known
[DWWZ12, JLY12, SEHK12].

Known-Key
[DWWZ12, SEHK12].

Koblitz
[BJ10].

Kode
[NN15].

Korea
[HL10a, LW11a].

KP
[FIJH12, HQZH14].

KP-ABE
[FIJH12, HQZH14].

Kristie
[Keb15].

Kryptografie
[Bli12].

Kryptographie
[Buc10].

Kurtosis
[YY15].

Large-Scale [DM15, JKHeY12, LQD+16, dCCSB+16, FXP12, GSN+16, SR10, ZZKA17, ZVH14].


LBlock [KDH13, MNP12]. LDGM [BBC+13]. Leader [TKM12]. leak [BBG+17]. Leakage [AV12, BKKV10, CBL13, DCA18, DB16, FPS12, HHH+13, HHP17, IL15, LTZY16, NTKG17, NTY12, Pan14, SGR15, TTH15, Wan18, XZY+12, YLZ12, YZ12, YCZ12, ZYT13, ZWTM15, ZM16, ZZM17, ZY17a, ZY17b, ZYM18, CQX18, DLZ16a, DMWS12, GV14a, GLL+18, SGP+17, YLZ+16, ZWM14, ZCC15]. Leakage-Free [IL15, TTH15]. Leakage-Resilience [NTY12]. Leakage-Resilient [AV12, FPS12, LTZY16, Pan14, XZY+12, ZYT13, ZWM17, ZY17a, ZYM18, ZY17b, CQX18, DLZ16a, GV14a].


M [Orm16, HvS12]. M-Identity [HvS12].
MA [ACM10]. MAC
[Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN16]. MacGuffin [LGL+12]. Machine
[AGHP14, Año16c, CHS15, Sch12a, ABBD13, GJ13, Gup15, LLA+16, LHA+16, QMC17, RY10, TTL10, War11, WS14].
Machine-generated [AGHP14].

machine-to-machine [QMC17]. Machines
[Ber16a, HB17, BBDL+17, KS13, PWW10].

Machines [AGHP14].

machine-to-machine [QMC17]. Machines
[Ber16a, HB17, BBDL+17, KS13, PWW10].

Management
[ASM12, ABB19, Bar16, BS13b, CCFM12, CSL+14, GOLPB12, KP12, KKA14, Lop15b, MKF+16, PN10, TMG19, Ve12, YZX+12, YSS14, ZJ11, ZTSR12, BMBS10, BB16b, CFL13, Cha13c, dCCSM+12, dCCSB+16, Din10, KH18, MLMSMG12, GMP10, PLCGS11, Sch11, SR10, SA15, SWW+16, WSC14, WDKV19, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b].
Manager [KKA15, Kim16]. Managing
[MD15, BC18]. MANET [KTI16].
MANETs [Yan14]. Manhattan [S10c].
manipulation [OF12]. Mansour
[LB13, HRS13, ZQW10]. Many-Core [LB13]. many-to-one [ZQW10]. Map
[XYXY11, ISC+16, LZY+16, LWK+18, PC14, SE18, ZT14]. map-based [LWK+18].
Maple [G13]. Mapping
[CBL13, MS17, MM14a]. Mappings
[MC11, CDPLCA16]. MapReduce
[LJLC12]. Maps
[Ye14, BAA13, KLW+16, LW10]. March
[Año10, Cra12, DDS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, WZM12a]. Marche
[CCFM12]. Margaret [Led16, Sch15a].
Marian [Kap13]. market [YWK10].
marking [PI18]. Markov [CR12]. Marotto
[SE18]. Marshall [Don14]. Martin
[ABJ13, Hof16]. Maryline [Año15b].

Mashup [HTZR12]. Mashup-Providing
[HTZR12]. Masked [WH17]. Masking
[HF14b, PVM+13]. Mass
[BPR14a, BPR14b]. Masses [Ano15c].
Master [Dew11, Mar10a]. Matching
[Line15, Tan12a, MR14c, MHT+13, PPT15, SS17, YZL+18]. MathCW [Bee17].

Mathematical
[Bee17, FGPG14, Ham17, IBM13a, Mei10, Sch15a, Wes16, KM14, O010, Sta11].

Mathematical-Function [Bee17].
Mathematician [Año17e].

Mathematicians [Acz11]. Mathematics
[Ano17b, Año12, Led16, Sch15a, Ter11, CM13, Kra12, PHWM10, Wes16].
MATLAB [TRD11]. Matrices
[ÁMVZ12, BNA15, AKG13, FES10]. Matrix
[BFMT16, IAD10, LLT+18, SK12a, TDT913, Ye10, Cha13b, LLM+19, TK14].

matrix-vector [LLM+19]. Matter
[Rau15, SS12a, DKA+14]. Max [And13].

Maximizing [DBPS12]. Maxims [Kob10].
May [BL10, FB12, Gll10, Sen10]. maze
[LCC10]. mbedTLS [YGS+17]. MC
[HIDFGPC15]. MC-2D [HIDFGPC15].

McEliece [DN12, GV14b, MBR15, MT12, MG15, OTD10, SWM+10, VOG15]. McOE
[FFL12]. MDPC [HC17, VOG15]. ME
[XHH12]. mean [TTL10]. Meaningful
DRS16, Hay13, HDWH12, HS18, Kim15, KCC17, LH12, LCLL15, LY16, LTW11, MJGS12, NNAM10, NRZQ15, SGC16, She14, TLW12, VKPI17, VFF17, VGA15, VK15, WP15, YZLC12, YSJL14, AKM*11, AL15, Ano11a, AZF*12, CJXX19, CL11, DLK*16, FPBG14, HWG10, HB13, HKB14, JZS*10, KP18, LH11a, LKKL13, MZA*13, MJ13, NDN13, OF11, PL16, RCW15, Ser12, SCKH18, Sta11a, Tan15b, WYL13, WS14, YLS12, ZOSZ17, Ste15b].

Network-Assisted [KCC17].

network-based [YLS12]. Network-Assisted [She14]. Network-on-Chip [Bis17].

Networking [LCK11, LLZ*17, ZHL15, Kim11, LCM*17].

Networks [ABCL17, ABC*17, BN14, BPSD17, BFM16, CS14, CSH*18, DS11, DF16, FMS12b, GMV17, HZC*12, HBC13, HK14, KH10, LLC11, LL15, LHM*15, LZK14, LWJC14, LLZ*12, MPM*17, NSA15, NRY*14, O012, OKG*12, PYM*15, PCFK14, RWLL14, SWYP12, She14, SP15b, Sm11b, SL11, SZZT18, TCN*17, WXL*17, WLY*15, XHC*12, YM16, ZC13, ZW15, Zha15b, ZLDD12, ZSA12, Aia15, ASO14, APK*18, AIB*16, AIK18, ADF12, BDK11, BLAN*16, BJB16b, CDGC12, CLM*12, CML*18, CLSW12, CL11, DSCS12, DK12, DLN13, EEA13, FA14b, FMA*18, GH16, HGWW11, HZC*14, HZWW17, HCC11, HCM11, HTT*10, HYF18, JN1H17, JLT*12, JMW*16, KMI10b, KLC*10, KO16, KLV*16, KDW*17, LLLS13, LC17, LMC11, LX11, LIK*17, LNK*18b, MSM*18b, QMW17, RP12, SGGR*16, SA12, SGJ*18, SZMK13, LSZZ15, SKK10, TODQ18, TKH14, WGJ10, Wan13, WW14, WXX*17, XW13, XWDN12, XHCH14, XMHD13, YHHS16, ZWQ*11].

networks [ZBR11, ZCLL14, ZTZ16, ZLDD14, ZHH*17, ZX11, LNK*18a].

Neural [CSH*18, SKS*18, YZLC12, EEA13].

Neuroscience [BSR*14, JW14].

Neutrality [Kha10]. Neutrality-Based [Kha10].

Nevada [IEE10]. never [Bai12].

Newly [ABJ13].

Newman [And13].

News [Edw14, Edw17, Sav13a, Sav15, Sav16].

Next [MR14a, MJGS12, Aia15, ACD*15].

Next-Generation [MR14a].

NFC [LY14, Mic16].

NFSR [WGD18].

Niederreiter [HC17, MVVR12].

Nievergelt [Ter11].

Nize [Mac12, LYYH14].

NIZK [Pas13a].

NIZKs [CIKL13].

NN [ZHT16].

No [WDDW12, Wu16, KHH14, MPJ*16].

Nobody [Sto12].

Node [NYR*14, OKG*12, LC17, PX13, SAAB10].

Node-Capture [NYR*14].

Nodes [VGA15, ZYL*10].

Noise [AS11, YMA17, ZHH*17].

Noised [JLS12].

Noisy [AS12, HZW*14].

Non [AS17, AMH*16, BCI*13, C14a, CPS16, D1J*12, DPW18, EKP*13, FHKP17, FMNV14, HKB14, KTT12, LLG15, MFH13, MSas12, OOR*14, Pas13a, RMG18, Svo14, WgMW12, YNQ15, YKHL12, ZLDD12, AY14a, BS15, CS11, ESR14, GIJ*12, Kre13, Lan11, LP11, MA13, MES*16, SXL16, XSWC10, Yan14], non-adjacent [Kre13].

non-associative [BS15].

Non-Black-Box [CPS16].

Non-blind [HKB14, RGM18].

Non-Boolean [AS17].

non-browser [GIJ*12].

non-compliant [Lan11].

Non-contextual [Svo14].

non-cryptographic [AY14a, ESR14].

non-dynamic [SES*16].

Non-interactive [BC1*13, Pas13a, Yan14].

Non-intrusive [MFH13].

non-iterative [SXL16].

Non-Linear [EKP*13, XSWC10].

Non-Linear/Linear [EKP*13].

Non-malleability [KTT12].

Non-Malleable [DPW18, MSas12, C14a, FNMV14, OOR*14, Pas13a, LP11, MSas13].

Non-monopolizable [DJL*12].

Non-perfect [FHKP17].
Non-Repudiation [LLG15].
Non-stationary [ZLDD12]. Non-tamper [WgMW12]. Non-uniformly [YKKL12].
Non-Volatile [AMH+16, YNQ15, CS11]. NonInteractive [KOS16, GOS12].
Nonlinear [CCM+15, KW14, LW13a, Lüd12]. Norm [FHS13]. normal [TY16a].
Normalization [KLY+12, SJ12]. Normalized [YGFL15].
Norman [Low12]. Note [HYS11, Gal13, Hwa11, Lim11]. nothing [Cer15].
Notions [KFOS12, SNJ11, Sar12, BP11]. Novel [CLHC12, KRDH13, LLG15, LyWlZZ12, LH11b, MJGS12, MCS+15, SWM+10, SC12, VN16, WHZ12, WZXL12, YZX+12, Ye14, ZM17, BOB13, CH10, DDFR13, GPLZ13, HCCC11, JXLZ15, LCM11, LMJC11, LH13, LWW+10, LML+13, MRT10, NZL+15, PZBF18, SYW17, Sm16, TG17, jT12b, WYL13, WZG+12, YWT+12, ZBR11].
Number [ADH11, BKL12, CDK+10, DSB18, Fok12, Ham17, KA18, LTPK16, LCLW17, MFG16, NIS12, NNAM10, Sha10, SRAA17, SRK+17, CFY+10, CP13, LLP+18, LGKY10, Lim11, MSL12a, MRT10, Sh11, St11, SXWC10].
LH10a, vDKS11]. Paradigm
[ABGR13, BSV12, Mau12, MP12, WQZ+13].
Parallel [App14, ARM15, BBM15, CGB+10, GP17, LY16, LB13, MCD12, MC11, NdMMW11, SMD11, YE12, CST16, MRT10, RG10, RWZ13, WYY11].
Parameter [NDC+13]. Parameters [HRB13, MBF18]. parametric [Bul10a].
Paranoia [Cor14a]. Park [Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, McK12, Pea11, Smi11a, Smi15a, Smi15b, Bai12]. Part [Bar16, VM14].
Partial [DLV16, GFBF12, LG12, SGS14, TK19, WDDW12, Bax14]. Partially [KB10]. participants [KSU13, WTT12]. participating [CH10].
Particle [ZS18]. Parties [YCR16, Kip13]. Partitioned [FVS17].
Passau [GLIC10]. PASSERINE [Saa12a].
Passion [Hof15]. Passive [DHB16, GSC17, SB17, BM13, uHAN+18, LWL11, MK12a]. passport [LZJX10].
Password [ASBD16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Sh11, WgMW12, YLW13, YRT+16, ZHX16, ABK13, AIK18, CTL12, DSC12, FA14a, FIO15, FHV16, GPL13, HCC10, IOV+18, KMTG12, LWS10, LNK13, MM12, MvO11, Tso13, TKHK14, WZM12a, WZM12b, YC12, ZXWA18].
Password-Authenticated [HCL+14, YRT+16, ZXH16, LWS10, WZM12a, WZM12b]. Password-Based [BRT12, CLY14, FVS17, WgMW12, DSC12, FA14a, FIO15, IOV+18, TKHK14]. Password-Only [YLIW13, KMTG12].
Patient-Centric [ZVG16]. Pattern [DCA18, ATK17, uHAN+18, KPS10, OSSI16, PPT15]. Patterns [Ano16a, BPSD17, TSH17, WOLP15, BDK11].
Payment [DG15, SYC+17, SYW17]. Payments [RBHP15, MPJ+16]. PC [YE12].
Perfect [Pas13a, Sch13, CZ15a, FHK17, LL10, LW12, XW12]. perfectly [ADG16]. Performance [Alo12, AW17, AB15, CGL+12, CCG10, DLK+16, DBPS12, EGG+12, ESRI14, FPBG14, GL12, GCS+13, HKL+14, KAK18, LCK11, LPO+17, MH12, SKV12, TPKT12, WDDW12, X12, YWF18, ZLDD12, ABDP15, GCVR17, MMS+17a, MS13c, ZLDD14].
Perform [Ano17d].
perimeter [Cal13]. periodic [KPS10].
periodical [CLW12]. Permission [VN16].
Permutation [LK16, GMS14, LK14]. permutation-based [LK14].
Permutations [ARH+18, BKLS12, Mat14]. Persistent [CSY18, TYK+12, ALL+18, PKE15].
person [PN10]. person-centric [PN10].
Personal [ESS15, LY+13, Rao17, ALL+18, BC18, MvO11, LHL15]. Personalized [FRS+16, AT10]. Personnel [YTH17].
Perspective [KMY18, MSM18a, RSGG15].
LGKY10, LKAT12, QGGL13, RITF+11.

**POWER** [BAB+13]. Powered [SFE10].

**PowerEN** [HKL+14]. Powerful [IF16].

pp [Joh10, Sch15a, CGCS12]. PP-1 [CGCS12].

**PPFM** [MS17]. PPM [XHC+12].

**PQCrypto** [Sen10, Yan11]. Practical [ATK11, BHH+15, BDH11, CLSW12, CGH17, Cra11, DZY10, EA12, FPS12, FSK10, HSA14, HPO+15, HKR+18, LW16, LJWTY18, MBF18, PPTT15, RWWZ13, TSH17, WHLLH16, XW13, YZLC12, ZYD10, ZLW+17, AMS+10, BS13a, CFN+14, JSK+16, LFZ+17, PHGR16, WR15, YKGK13, ZSW+18a].

practicality [NDNR13, Zha15a]. Practice [ABD+15, CDFZ16, FM12, PWVT12, Rog16, RBHP15, RST15a, RST15b, SN10, SAKM16, NS10, Sta11a].

**Practice-Oriented** [Rog16]. Practitioners [PP10a]. Pre [YWL+17, YHHS16].

pre-distribution [YHHS16]. Pre-image [YWL+17]. Preaveraging [GWM16].

**PRECISE** [HYF18]. precision [MN14, SK12b]. Precomputation [GKM16]. Predicate [KHPP16, NMS14, YKNS12, ZYT13, FH13, HFT16].

**Predictability** [DK16]. prediction [CSS+13]. Predictive [TBCB15].


**Preservation** [BCP14a, LLG15, VSV15, Yon11, LVRY10, TMLS12].

**Preserve** [BAG12]. preserved [SWW+17].

**Preserving** [ABCL17, BJ16, BHK13, BJL12, CWL+14, CRE+12, GZZ+13, HSMY12, HLLC11, HXC+11, HHHK14, KS12, LMGC17, LNXY15, LQD+16, NSMS14, OFMR16, PR12, PD14, PSS+13, PPRT12, Pet12, RHV+16, RBHP15, SZDL14, SZQ+17, ZZT18, WPZM16, WZCC18, YKKL12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, AIB+16, ALL+18, BLV17, FH13, FMA+18, GH16, GAI+18, GA11, HSH11, IC17, IOV+18, JKL+16, KH18, LHL+18, LW13a, LCY+16, PZBF18, SY+17, Tan12b, TSH14, WLZ+16, YMM13, YNX+16, YL11, ZWY+13, ZOSZ17].

Press [Ano15b, Ano17b]. Press/Elsevier [Ano15b].


**PRIME** [ACK+10, GM13]. Primitive [App15, MCS+15].

Primitives [BSJ15, EAA12, HLN+10, SP15b, ABDP15, BSR+14, Gor10]. PRINCE [BCG+12b].

Princeton [Ano17b]. Principal [BKL18]. principle [WW14].


Priority [LMS16, Bia12]. Prisoners [Mac14, Keb15].

Privacy [AKM+11, AKKY17, ABCL17, ALL+18, ACM12, ABHC+16, BN14, BCF16, BJ16, BLV17, BS13b, BJL12, CVM14, CWL+14, CDFS10, DTE17, ESS15, FGR+17, GZZ+13, HSMY12, HBC13, HXC+11, JN12, KM10b, KCC17, KS12, KH18, LMGC17, LSBN14, LLG15, LNXY15, LQD+16, MYR13, NSMS14, PD14, PSS+13, PPRT12, PZPS15, PSD15, Pet12, RHV+16, RCP+18, RWLL14, RBHP15, SS17, Set16, SZDL14, SZTZ18, SO12, TMLS12, TMSGP13, WPZM16, WZCC18, WMYR16, YMM13, Yon11, ZHW+16, ZM16, ZOSZ17, ZHW15, ZLDC15, ZHL15, ZTL15, ACK+10, BP11, BAG12, CDF+10, DZS+12, FH13, FMA+18, GAI+18, HSH11, IC17, IOV+18, JKL+16, Kam16, KKK10, KM14, LHL+18, MZA+13, MGP10, PX13, PZBF18, Sav16, Sch11, SLZ12, SY+17, SCY15, SWW+17, Tan12b, WLZ+16, WWW17, WS13, YSS+16, YXA+18, YQOL17, YNX+16, ZWY+13].

Privacy-assured [WMYR16].
Privacy-Aware [BCF16, 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, LMGC17, LNXY15, LQD+16, NSMS14, PD14, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, SZZT18, WPZM16, WZCC18, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, ALL+18, KH18, ZOSZ17, BLV17, FMA+18, GAI+18, HSH11, LHL+18, PZBF18, SYY+17, Tan12b, ZWY+13].
Private [BKLS18, GM13, Jia14a, QZL+16b, Sia12, WCL+18, Yek10, ZMW16, ZXYL16, HJM+11, HYF18, IK15, WR15].
private-keys [IK15].
Privilege [Cha13c, QRW+18].
Privileged [Din10, WDZL13].
PRNG [DK16].
Proactive [SLL10, WMYR16].
Probabilistic [BFG+14, Rao10, WP17, KSU13].
Probabilistically [IW14].
Probability [DF11, HLC16].
Probability-based [HLC16].
probable [Sav13b].
Probably [MMS17b].
probe [Edw14].
Problem [CLL16, GKS17, LLGJ16, NA10b, TKMZ13, Mes15, MR14c, RH10, VM14].
Problems [Dun12a, Fra15, GTT11, KRDH13, KPC+11, RBS+17, SK14, TPL16, WS14].
Procedure [CS14, ŠO12].
Proceedings [LCK11, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Dun12b, FBM12, Gill10, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLC10, IEE11a, Kia11, Lin14b, Sah13].
Processing [SAKM16, TKMZ13, VP117, BKV13, HKW+15, MS13b, PRZB12, WS14].
Processor [BH15, CLF+17, HKL+14, LB13, MBR15, YS15, ABDP15, BAB+13, BGG+13, KSH18, SSP+13, Tar10].
Processors [GFB12, Gue16, RYF+13].
Product [ADM12, CCM+15, OT12, YKNS12, Cha13b, DZM17].
Products [LMG+18, RS10].
Professional [STC11].
Profiles [BCF16].
Profiling [DP12].
Profit [APPVP15].
Program [MZ17b, Wal18, CLZ+17, GGH+16b, MFH13].
Programmable [CLF+17].
Programming [Bee17, BCEE15, SY14, ASVE13, HLV10].
Programs [BGI+10, BGI+12, CL16].
Progress [AB10a, BL10, BC11, GG10].
Progressive [SA16a].
Project [ACK+10, SS10c, Wii18].
projective [CZ15a].
Prominent [ABJ13].
Promise [Pan10, PWVT12].
promised [HS11].
Proof [BDHG15, SG15].
Protected [BDGH15, SG15].
Protecting [BAX10a, BL10, BC11, GG10].
Protection [CDD13, GST12, Lop12].
Protected [BDHG15, SG15].
Proportions [Ber12].
Produce [BFMT16], proposed [Bax14].
Protect [CTC+15, YMC+17, BVB12, CDF+10, dCCSM+12].
Protected [BDHG15, SG15].
Protection [CDD13, GST12, Lop12].
Properties [CCK12, CCK16, DQFL12, FY11, JR13, KU12, Sch12c, CLCZ10, WT13].
Property [HEC+12, PR12, Rja12].
Properties [BGK12, BCGK12, BGB12, BCL12, BDSG+13, CLCZ12b, IW14, LNZ+13, Mau12, NTY12, Sav13b, WPZM16, AGH14, KPP16, KKK+16, Li10].
Propagate [GWM16].
Propagation [SK+18, WWC+11, YZLC12].
LNZ+13, LCCJ13, LNX15, MBC15, MR10, PSS+13, SBS+12, SGC16, TYK+12, WT10b, XJR+17, YS12, YWF18, YWZ+12, ZZ+11, AATM18, AKG13, AIB+16, AIKC18, AN15, BDM18, BGA12, CSD18, CCSW11, CJ15, DLK+16, EA12, FA14b, FIO15, GMWS14, GLM+11, HPC12, HWB12, HL14, IC17, IOV+18, JKL+16, JXZ15, Kim11, KO16, LLLS13, LDDAM12, LKK13, LWS10, LXMW12, LEW19, LY14, LML+13, NCL13, NLYZ12, OHJ10, Par12b, SB17, SBS+12, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13b, ACM12, CML+18, CR10, CLCZ10, DGNJ14, FTV+10, GBNM11, GLR13, HSH11, Ham12, HDPC13, HZW17, HST14, KJN+16, KU12, KKK+16, LKKL13, MN10, NR11, Nos11, Nos14, SD10, YSL+10.

Proving [DLN13, HTZR12, KS18, MLM16].
KFOS12, LLH18, MMP14, MPRS12, NTY12, Orm16, PDNH15, RSBN12, RW12, SK12b, SWM+10, Sia12, XNKG15, XJWW13, YKC+11, YFK+12, ZY17a, ABW10, IM14, LPaS10, LZC14, BSW12, RPSL10, SES+16, VN17, ZCC15, ZY17b.


ZOC10, ZPZ+16, Zim10. Random-Grid
[KS15]. Randomization [Gas13].
Randomized
[ARP12, GT12, HHR11, SR12b, BWA13].
Randomness
[AY14a, Ana14, ABF12, ACM+17, BWLA16, MS10, MS16, DTZL12, FRT13, RO10, TC11].
Range [DCA18, HMC12, JCHS16]. Rank
[SS10b, FES10]. Ranked
[CWL+14, XWSW16, GZS+18, LXX+14].
Ranking [ZDL12, AT10]. Rapid [KPC+16].
rare [Sch11]. RASP [AZPC14]. RASP-QS
[AZPC14]. Rate [LJK17, PPS12b, PCK14].
Ratio [FHKP17]. Rational [CK18, KU14, KOTY17, NS12, TWZ11, ZC13].
Rationality [GLR10, GLR13]. RBAC
[VN16]. RC4
[GCS+13, Loe15, Rec15, RS14, Sar14].
RC4-like [RS14]. Re
[ABR12, GSW+16, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PRSV17, WY10, XJW+16, BGP+17, CFZ+10, CLH+16, Cz15b, FSGW11, FSGW12, FXP12, GH12, HDWL16, HYF18, KKM+14, LMJC11, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGJ10, WHY+12, Wan18, WLS14, XXY15, YZC17, ZDW+16, LAL+15]. Re-authentication [LBR12, FXP12, LMJC11]. Re-Encryption
[GSW+16, KKA15, LSLW15, MLO17, NAL17, PRSV17, XJW+16, ABR12, LSC12, Pet12, WY10, BGP+17, CFZ+10, CLH+16, Cz15b, FSGW11, FSGW12, GH12, HDWL16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, WGJ10, WHY+12, Wan18, WLS14, XXY15, YZC17, ZDW+16, LAL+15].
re-signatures [Tia15]. Reachability
[SVG16]. Reactive [JR13]. read [Sto12].
readers [HDP13]. readership [Bai12].
Ready [GOPB12]. Real [Ano16h, Ano17d, AYS15, BFK16, BPS16, BNA15, Cer14, CC14, GSC17, JWJ+17, MK11, PNRC17, SK14, Tom16, WLZL12, YE12, AY14a].
Real-Time
[AY15, GSC17, JWJ+17, PNRC17, WLZL12, YE12, CC14, MK11, AY14a].
Real-valued [BNA15]. Real-World
[Ao16h, Ao17d, BFK16, BPS16, Tom16].
realistic [FRT13]. Realization
[KRM+10, MNM+16, SVT10]. Realizing
[WKB16, ZPWY12]. realm [OYH14].
Reasoning [TSH14]. Rebound
[KNR10, Sar12]. recall [LTC+15a].
recall-based [LTC+15a]. Receive [Orm16].
Receiver [Wan14, Chi12]. Recipes
[DGP10]. recoding [TMK11]. Recognition
[AOQ12, BCTPL16, BJCHA17, IA15, LGM+16, MR14b, BAG12, uHAN+18].
Recommendation [Bar16, Gir15, NIS12].
Reconfigurable
[HG12, HLN+10, MLCH10, NdMMW16, PP10b, PG12, SRK+17, ZLQ15, MD12a].
Reconfiguration [GFB12, VMV15].
Reconstruction
[CCM+15, KOTY17, HH15, IK15]. Record
[AP13, Con12]. Records
[LYZ+13, Rao17, ZVG16, LT14b, LHL15].
Recoverable [JLS12]. Recovery
[Bro17, DSSDW14, LYY+18, NRZQ15, SAA15, SSA13, WZ15, BM15, CHHW12, CGH17, PX13]. Rectangle [WLC12].
Recurrent [CSH+18, Pud12]. Recursive
[LXY12, WH18]. Redesigning [VFV17].
redistributed [LXC11]. Reduced
[BW12, DWWZ12, KNR10, LWZ12, LJF16, LPWF12, AKY13, AY14b, LF16].
Reduced-Round
[LWZ12, AY14b, LF16]. Reduction
[ABR12, LCLW17, LSC+15, YMA17].
Reductions [BHKN13, DW12]. Reference
[LLHS12, IM14]. Refinement [BCEM15].
Refinements [LL11]. reflections
[Hai17, OF12]. refractive [PHN+12].
Refresh [LSC+15]. Regaining [WBA17].
Region [CCFM12, HZW+14, KS15, FH16, LWLW11, WW13]. region-duplication
[LWL11]. Regions [AQD12, AKK+17].
Register [TLCF16, LWK11]. Registers [LLG16, ZH15]. Registration [ISG+16].
Regular [CQX18, Wat12, WR15].
 regular-expression [WR15]. regulating [DFJ+10]. regulatory [BP10].
regulatory-compliant [BP10].
Reinforcing [WXY+17]. Rejewski [Kap13].
Rekeying [DT13, QL17, CLSW12, DS11].
Rekeying-Aware [QLL17]. Related [Cil11, CMA14, DGIS12, HLL18, Pud12, WLC12, MNP12].
 Related-Key [CMA14, HLL18, Pud12, WLC12, DGIS12].
Relational [HPC10, RP12, WP17, BFG+14, BL11, GA11, JK13, PYP10]. Relations [BP11, FHS13, HLR11, WGD18, KGO10, LLM+19].
 Release [KFOS12, RSBN12, Um15, WSS12].
Relevance [Sim15a]. reliability [CZ14].
Reliable [AMKA17, ADG16, Bala10, CC14, WKB16, ACD+15, CL16, ZC12].
 Relying [TAKS10]. Remainder [HF14a].
remapping [PSJ+13]. Remarks [SSU12].
Remote [BCE10, CS14, FMY15, LCK14, Sar12, SY+17, VMV15, WgMDZ12, WgMW12, CHS11, Hu15, IB11, KKG14, LH10c, LNM+11, LNK13, LW+18, LH13, MM12, Sar10a, WQZ+13, YSL+10]. remotely [Wat14b, YHH18]. Removing [HKHK13].
Renewal [MY12]. renewed [GPLZ13].
rental [LY14]. Reordering [Alo12].
Repairing [BCM12, BCM13]. Repeatedly [TAKS10, ATK11]. Reply [ZL15].
Report [CPB+12]. reports [RPG12].
Repositories [Ano15a]. repository [RSM15].
 Representation [AGW15, BFM16, MHT+13].
Representation-Based [AGW15].
 Representatives [Bla16]. reproducible [CW12a]. Repudiation [LLG15].
 Repurposing [GY13]. Reputation [BL15, LHM+15, PAS13b, MGP10].
Reputation-Based [PAS13b].
 Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13]. Requirements [OS16]. requiring [KH14]. Rescue [TSH17].
 Resettable [CPS16]. Resettable [COP14]. Resettable-Sound [COP14].
Resilience [NY12, GLL+18]. Resiliency [YM16]. Resilient [AV12, BKKV10, FPS12, LTZ16, LD13, NRY+14, Pan14, PSS15, XZ+12, YZ12, YNR12b, YCZ12, ZYT13, ZW15, ZZZ17, ZY17, CQX18, DLZ16a, GV14a, KPS10, MMS13, SGP+17, Wan18, YSL14, YKC+12, YL+16, ZY17].
Resistance [GC12, PRC12, WLZ12, ZJ11, DLN13, FIO15]. Resistant [BK12a, CDK+10, GV14b, HF14b, WHZ12, WgMW12, WH17, YPR17, GMRT+15, HCC10, PBCC14, VCK+12, WTT12, YKG13]. resisting [SXL16, Tan15].
Resistive [DB16, TLF16].
Resource [CSH18, JMG+16, SZK13, YNR12a, AMHJ10, FQZF18, KAS15, LLZ+16, MV15, Wan13, XZW16, ZFP+16].
Resource-Constrained [CSH18, YNR12a, LLZ+16].
Resource-efficient [SZK13, XZW16].
Respiratory [RSC18].
Response [GHS14, HLL15, ZHW+16, MRRT17].
Resprining [TBC15]. restoration [WHZ12]. restricted [CLH+16]. result [ACK+10, ED17].
Results [DG12, LJF16, Hof16, KGO10].
Rethinking [Ch13, Hu15, LSG16, MV16a].
Retrieval [BBB+16a, BTH12, CJP12, HK14, JMG+16, JKH12, Yek10, XZ+11, CJP15, SWW+17]. returned [War11].
reusable [RS17]. Reuse [ABF12].
Reveal [Sta13]. Revealed [Ano15d]. Revealing [BT12, KK12, KK13]. reverse [TQL+14].
reversed [KHY18]. Reversibility [FSX12b, HWYW14]. Reversible [CLF11, CSS+13, HHS+15, MM17, MR16, NC12, AMK12, CT11a, HLC16, JK13, MM14a,
NC13, PWLL13, PC14, TK14, WOLS12.

Reversibly [MKH+12]. Review
[Ano15b, Ano17b, Ay12, Ayu12, Bai12, Bar12, Cou12, Dew11, Ful10, Gas13, Joh10, Kat13, Keh15, Koh10, Led16, Lop15b, Low12, Mei10, Mou15, Mor10, Sch15a, Sha10, Ter11, Xie12, JAS+11, MM12, TPKT12].

Reviewed [Sch15a]. Reviews [SR14].

Revised [DDS12, Dan12, MV12, BYL10, JY14, LHi10a, vDK11]. Revising [BT12].

revision [LT14b]. Revisited [CLY14, DKS12, GWCC15, KFOS12, LL11, Lop15a, PKTK12, Sar12, Tan12a, BCL14, HKT11, HYWS11, TS16a, ZCL+12]. Revisiting [TLW12, WSA15].

Revocability [WHL16]. Revocable [AEHS15, CD16, QZZ18, SE14, SE16, SZS14, SZDL14, TCL15, TT12, Urr15, FLL+14, LDZW19, WLFX17, WTT12]. Revocation [AEHS15, LLC+15, LW16, Lop15b, RDZ+16, XLML13, YWZ+12, ATK11, LJWY18].

Revoking [TAKS10]. Revolutionized [Orm16]. RFID [CJP15, AATM18, BL12, BSSV12, BM11, CGCGPDGM12, CCF17, CJP12, Cho14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, GAI+18, HSH11, HDPC13, HQY+16, HCP1LSB12, HCTETP+12, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLsvdLE10, QZL+16a, QZL+16b, SBS+12, SPLHC14, TG17, WH17, WCF18].


Riddle [Fox13, KM15, KM16]. Right [Bro17, SR12a, BBG+17, LHA+12, Sch11].

Rightful [RR11]. Rights [LRVY10].


Robotic [SWP+16]. Robust [BCGAPM12, BCG12a, CFOR12, GKB17, HZC+12, JSZ12, LSL12b, LHR13, MU12, MS16, MC11, pNYWY+14, OCGD11, RR11, RMC18, SJ12, SC12, SZZT18, TLC16, TK14, TTL10, WDB11, WgMdzI12, gWpNyY+14, XNG+14, YWNN15, YYO15, AP10, AIA+18, CLM+12, EAA+16, GZHD12, HZC+14, HZL18, IOV+18, KIH19, LNK+18a, LW10, PKS18, RS17, wWpNyL11, wWpWYpN13, YSL+10, ZHH+17].

Robustness [HGT15, YKBS10, AEH17].


Rotational [KN10, KN10]. Roulette [Ber17]. Round [Ber17, jCPB+12, COP14, DWW12, GH1R14, KOT17, KMO14, LW12, LJ17, Pan14, TYM+17, XZL15, Yon12, AY14b, ABM+12, Blo15, LP11, LF1+16, Sun11, TS11L, TQL+14, TCS14, XW12].

Round-Reduced [DWW12]. Rounds [GTS12, S12, LHY14, MN12]. Router [Bis17, SA15]. Routing [Ham12, KZG10, WLY+15, LSG16, LC17].

RSA [Dun12b, K11a, Pie10, APPVP15, BBP13, Bro17, BNST17, CLSW12, Chm10, GM13, GST13, Her14, Hin10, HLY14, IK15, KHH14, KFL+10, Lim11, M10a, SM10b, SM10c, SM10, SL10, TK19, Win17, YHK+10, YXA+16]. RSA-1024 [Bro17, Win17].


HIDFGPC15, KGV16, KAK18, LYX+13, LKA19, MBR15, QZL+16a, ATKH+17. GSN+16, MNX+16, WDLZ13, WLFX17, YC11, KCR11, KS11]. Scalar [YTS12, SKH15]. Scale [DM15, GU13, JKHeY12, LQD+16, CG12b, dCSCS+16, FXP12, GSN+16, SR10, ZZKA17, ZVH14].


Schedules [Pud12]. scheduling [MV16b].

Schema [AN12]. Scheme [AS15, Bai10, BHG12, BS14, BKJP12, BDH11, CMLS15, CLL16, CCW+10, CLHC12, CHHW12, CCZC13, CGY+13, CLHI3, CSW12, DA10, DS11, DKS12, FR16, FGM10, GZZ+13, GH11b, GJZ17, GLW12, GZH17, HY11, HIDFGPC15, HMR12, HYP+17, Hül13, HP12, IL15, JSZ12, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KLM+12, LSL12b, LHF12, LTH+15, LTZ16, LH11b, LGWY12, LTC+15b, LYX+18, LGRPH14, MWZ12, MVVR12, MRL+18, MNM12, MSas12, NXB13, NLLJ12, NLY15, Pet12, PDLT12, RVH+16, RMG18, SK12a, SJ12, SGF+12, SD12, She14, ST16, SP15b, SJWH+17, SSA13, Tan11, TDTD13, TWZ11, DLY+10, WgMdZ12, WgMW12, gWpNY+14, WHL15, XWSW16, XHC+12, XJW13, YM16, Yam12, YZX+12, Ye10, Ye14, YTH17, YL17, Y+17, YHK+10, YMSW11, ZPM+15, ZC13, ZQQ+15, ZLDD12, ZY17a, AMN18, AHS14, AKK+17, BOB13, BAL10, BMM12, BBB16b, CCLL11, CLSW12].

scheme [CH10, CT11a, CLJH13, CW14a, CTHP13, Cho14, DSCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, FHZW18, GHZ12, GJ13, GMRT+15, GPLZ13, GLM+16, GH16, GAI+18, GTBS19, HZW18, HBBRMN+16, HL11, HCCC11, HLC16, HCC10, Hwa11, IB11, JNUH17, JKAU19, JLT+12, JZS+10, JMW+16, KI11, KPP16, KDH15, KK13, KHMB13, KKM+13, KKM+14, KKG14, Kin16, KIH19, KP18, KLIW+16, KDW+17, KWH16, KL11, LXLY12, LLZ+16, LSR13, LH10c, LZXJ10, LNM+11, LMJC11, LK12, LLHS12, LNK13, LJK+17, LNK+18a, LWK+18, LNK+18b, LFWS15, LH13, LH11, LWL10a, LWLW11, LW13b, LZX14, LDZW19, LL16a, LL16b, LHYW12, MCN+18, MMS17c, MK12a, MSas13, NR17, Nos14, PZBF18, QMC17, QMW17, RPSL10, SGCR+16, SM11, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWZY11, WWYY11, yWpNYL11, WHL13, WDLZ13, WLZ+16, WLFX17, Wan18, WDKV19, WZ11, WKHI11, WOLS12, WXX+17, XHH12, XZW16, XWXC14, XXX15].

scheme [XMHD13, YC11, YCC16, YHMM18, YWK+10a, YCT15, YXD18, YQOL17, YMSH10, ZYL+10, ZLY10,
ZXJ+14, ZYC+17, ZPYW12, ZHH+17, ZY17b, ZFH+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12]. Schemes [ABF12, BVS+13, BFM12, BBEPT14, BSJ15, CMLRH13, CGL+12, Cmh16, Des10b, FHKP17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZCK14, MLCH10, MR14b, MMS17b, MFB18, MKRM10, Oba11, PB12, PDNH15, PH12b, Sch10, Shi11, SKH17, SSU12, VSR12, WGF16, Young12a, Young12b, Yek10, YWZ+12, AGHP14, AN15, AHT+12, CDGC12, CJXX19, CHS11, CCG10, CTL13, DDD14, DD13, DZ14, FPG14, FGMP12, FMA+18, HWDL16, HM10, KTUI16, LHYZ12, MM12, MA17, NZL+15, QYWX16, SES+16, Sar10a, Sar11, hSSZ15, SAR18b, WW14, YT11b, ZCL+12, ZC14].


SE-AKA [LLLS13]. seals [MN10]. Seam [LC15]. Seam-Carved [LC15]. Search [CWl+14, Che15, DCA18, FRS+16, GTT11, HCDM12, LSOQL18, TMC15, WDC18, WW12, XWWS16, XJWWW13, ZXYL16, BL11, CLH+16, FHI13, FSGW12, GZS+18, HH16, OSSK16, SY15b, WHY+12, WXLY16, XWY+18, YX1D8, YQOL17]. SDDO-based [PL16]. Searchable [BHJP14, CWWL12, CLW16, CGKO11, FJHJ12, PCY+17, XNKG15, DLZ16a, DRD11, HQZH14, HTC17, JCHS16, LZC17, LLL+18, RPS10, WXLY16, WCC18, YZCT17]. Searches [Sia12, WR15]. searching [GPN+12]. Seattle [LCK11, KCR11]. Seberry [AHS14]. SEC [PA10]. Second [AKY13, ABM+12]. Secondary [RS11]. Secrecy [ABD+15, BKT18, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCW15, TCS14]. Secrecy-preserving [TSH14]. Secret [ASN11, ASN12, ADH17, Ayu12, Bia10, BBB+16a, BFM12, BBEPT14, Bri11, CCM+15, CFOR12, CCL+13, DR12, Dew11, EM12, EA11, FHKP17, FR16, Fok12, HYS11, HL10a, Has16, JLS12, KU14, KS18, KOTY17, KK12, KK13, KSSY12, KS15, LHF12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Oba11, PCKP14, QS18, SLL10, SC10, SS10c, SSU12, St15, TRL12, TWZ11, WKB16, WGF16, Wil18, XZY+12, XJR+17, YFF12, YWZ+12, ZC13, Ald11, ADG16, AKK+17, Ara13, BJ16, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEAZ13, EZ15, FHH10a, GJMP15, GLW13, HF14a, HH15, Hea15, HBBRM+16, HCCC11, HLC12, K11, KTUI16, LXLY12, LT13, LyWSZ10, LHYZ12, LEW19, Mas17, McK10, McK11, McK12, MBB11, O010, Pea11, Pet11, QD16, Rus15, SB17, SA12, SAR18b, TQL+14, TD14, UUN11]. secret [UUN13, WYL13, WZ11, WSI2, WOLS12, Wu17, WX13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPYW12, LSC+15, Bia12]. secret-key [UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, WX13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPYW12, LSC+15, Bia12]. secret-key [UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, WX13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPYW12, LSC+15, Bia12]. Secret-Sharing [BBEPT14]. Secretion [RSCX18]. Secretocracy [Ber16b]. Secrets [BT12, CG14b, DLWW11, FMS12a, Kob10, Man13, Bha16, Cop10b, GGH+16b, Gup15, HRS13, Smi11a, Ano17b]. Secure [ADMM16, AARJ12, Ash14, AMH+16, BVS+13, BWLA16, BCGH11, BCG12a, BCQ+13, BWA13, BJL12, BHJP14, BF11, Bru12, BDH11, BEM15, CFOR12, CCM17, CZF12, CzLC14, Che15, CMA14, DMI8, DL15, DMS+16, DG15, DLZ+16, Edw17, FLH13, Fri10b, FDI11, FSX12a, zGXW12, GKM16, GGH14, GFBF12, GT12, GV14b, GHKL11, GM14, GZS+18, HvS12, HSM14,
HLLG18, Har16, HL10b, HP14, HTZR12, HMCK12, HLKL15, HYS18, HK14, IL15, Jac16, KW14, KME+12, Küp15, KH10, LJS+14, LL15, LH12, LYZ+13, LTH+15, LTY16, LSLW15, LGGJ16, LSQL18, LY15, LHL15, LLML12, LSC12, MLO17, MMP14, Mal13, MVVR12, MMS17b, MK12a, MKAA17, NBZP17, NDG+17, NR12, NMS14, NSMS14, PB12, FSM17, Per+13, PRN+19, QZL+16b, QZDJ16, QZZ18, RMP10, Rea16, RSGG15, SNJ11, SZS14, SYCV15, SP15b, SHK17, SRAA17, SAR18b, SSAF11, SVG16, SYW17. Secure [SYC+17, SMS14, SZDL14, SGH15, SLY+16, SR12b, TB18, TCL15, TWZ11, TG12, TGC16, VMV15, WgMW12, WKB16, WXYL16, WLY17, WDC18, WHL15, WBA17, WWHL12, WMS+12, tWmC12, XWSW16, XJWW13, YN12r, YN12b, YTH17, YTK+10, YKC+11, YAM+15, YGD+17, ZXZ+11, ZDLZ, ZVH14, ZVG16, ZHT16, ZL17, ZBR11, AHS14, APK+18, ABBD13, ACW16, AKK+17, ACD+15, BOB13, BSR+14, CCL11, CS18, CLH13, CW14a, CS11, CDL18, FHI10a, FLL+14, FSGB12, FA14b, FI10, FS18, Ga13, GAI+18, GLL+18, GCH15, HGWI11, HWK+15, HLYS14, HTC17, HPY10, IB11, JZS+10, KPP16, K14A, KRM+10, KU16, KDW+17, LL13S, LDDM12, LH11a, LL16, LSR13, LWK+18, LCT+14, LAL+15, LL16a, LL16b, LBOX12, MR14c, MHT+18, NR17, NAICR12, NAL17, PsbD+13, PLSvdLE10, Rao17, RG10, RYF+13, RITF+11, RS15, SGCC+16, SYL13, SWW+16, SSS11, SSLP+13, SX16, Tar10, TLL13, TL12, VS11]. Secure [WLZ+16, WMX+17, WDKV19, WCH18, WL19, WXWC14, XXX15, YC12, yYqWqZC13, YZZ+14, YZCT17, YQOL17, YY11, YLS12, YM10, ZL14, ZLL14, ZZ15, ZYC+17, ZG10, ZZ12, ZX11, ZY17b, ZC12, Zhu13, ZSW+18b, Ano12, DSB18, OKG+12, YS14, YFK+12]. Secure-TWS [OKG+12]. Secured [LC17, SGG18]. Securely [CC10, KP17, LHL+14, MS16, WXY+17, BC18, der10]. Securing [BK12b, CMLS15, CST+17, NPH+14, PMZ13, SFE10, SMS18, SL11, Ste15b, TK14, YMA17, Y12, CT10, Din10, SK18, SA15, Tox14]. Securities [WLW+14]. Security [ABJ13, ASBD16, Ano13d, Ano15a, Ano15d, ABF12, AN15, ABHC+16, AYS15, BCE+10, BCM+15, BRT12, BPR14a, BPR14b, BLS12, BCG16, BPS12, Bra15, BDH11, BP10, CFST17, CFE16, CHS11, CFX17, CCD15, CPS16, CM11, DDS12, Dan12, DR12, DFK17, FMA+18, Fid18, FSX12b, FSX12c, GZZ+13, GSC17, HC12, Hel17, HB17, HL12, HX+11, HL11, HLT+15, HLN+10, IS12, IGR+16, JN12, Jia14a, KBL11, KS18, KFOS12, KSD+17, KD12b, LPS12, LST12, LW11a, LK14, LW12, LLZ+17, LT11, LS18, LP12, LW17, LZA12a, LDB+15, LMS16, LLH18, MTH11, MKN13, MCS+15, MH14, Mou12, MV16a, ML12, MPM+17, Nac12, NN10, NDG+17, NVM+17, Nos11, Nos14, Orm16, OS16, Pas13a, PZPS15, PDH15, PS14, PL16, PDT12, PNRC17, RCP+18, RQD+15, RW12, Rog16, RS10, SG18, SN10, SN11]. Security [SBS+12, Sar12, Sch13, SD12, Shi11, SM10, STC11, SM15, SCGW+14, Tso13, TV15, Wal18, WYCF14, WSA15, WSS12, W18C+18, WS14, Yan10, YL12, YS17, YSS14, You11, Zha15b, ZY17a, vT11, AM11, AN18, AB10a, Abe10, ABGR15, ABM+12, Ano11a, ADH17, BYL10, BSS11, BDL+11, BL17, BM11, BL11, CO11, CTH13, CLC10, CVC+13, DLK+16, DWM+13, Edw14, FHM+12, FA14a, Fis15, GHD19, GM16, GLM+16, GMS11, GH12, HWD+16, HWG10, HL11, HRS13, HLT10, KSA16, KKK+16, Lan10, Lan13, LH10a, LXW12, LH11, LZC14, LS16, MZA+13, Men13b, MM14b, MS+18b, NS10, NHL13, NYL12, OK18, OYHSB14, PHW10, QYW1X6, Re15, RPS10, RH10, SA12,
Ser12, SLZ12, SY15b, Sir16, Sta11a, Tan17b, TODQ18, UUN11, VCK+12, WCFW18, XCL13, Zha15a, XW12, YKC+12, Bar12].

Security-Aware [LMS16, GHD19].

security-enhanced [AMN18].

security-modified [MM14b].

SEDURA [LY15].

Seed [AS17, LYHH14, Sun11].

seeing [Tox14]. seen [Goo12].

Segment [WOLP15].

Segmentation [WYW+13, ZZCJ14]. selectable [GLM+11].

Selected [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12].

Selection [KD12a, RP12, SEY14, FXP12].

Selective [DDS12, Dan12, MV12, JY14, LH10a, vDKS11, JY14, MV12].

Selective-Opening [LLH10a, LH12, LT13, LH13, SH11].

Self-adaptive [LHM14, FXP12, SH11].

Self-authenticating [Cer18].

Self-Authentication [LH12, LT13].

Self-Certified [CLL16, XWXC14, LH14, LH13].

self-composition [AGH+17].

Self-Controllable [ZLDC15].

Self-Identifying [CSV15].

Self-Recovery [SAA15, CHHW12].

Self-restoration [WHZ12].

Self-Synchronizing [DM18].

Sel-System [CHHW12].

SET [Frie15].

SET-MAC [Frie15].

Selective-Opening [DDC16].

Security-Aware [LY15].

Seed [AS17, LYHH14, Sun11].

seeing [Tox14]. seen [Goo12].

Segment [WOLP15].

Segmentation [WYW+13, ZZCJ14]. selectable [GLM+11].

Selected [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12].

Selection [KD12a, RP12, SEY14, FXP12].

Selective [BDCC16, LW12, LSC+15, LZC12a, LH18, LZC14, LW13c].

Selective-Opening [LLH18].

Self [Cer18, CLL16, CHHW12, CSV15, DM18, HZ11, LCL+17a, LH12, LHM14, SAA15, SM12, WHZ12, XWXC14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11].

Self-adaptive [LHM14, FXP12, SH11].

Self-authenticating [Cer18].

Self-Authentication [LH12, LT13].

Self-Certified [CLL16, XWXC14, HL14, LH13].

self-composition [AGH+17].

Self-Controllable [ZLDC15].

Self-Identifying [CSV15].

Self-Recovery [SAA15, CHHW12].

Self-restoration [WHZ12].

Self-Synchronizing [DM18].

Self-Synchronizing [HZ11].

Self-updateable [LCL+17a].

SELFinux [SFE10].

seller [KJN+16].

Semantic [YZCT17, HLR11, HTC17].

Semantics [CM11, Gl12, KGP12].

Semi [BDOZ11, KKK+16, WHZ12, XZLW15, PGLL10].

Semi-automated [KKK+16].

Semi-fragile [WHZ12, PGLL10].

Semi-homomorphic [BDOZ11].

Semi-trusted [XZLW15].

Semia [SS10c].

semirings [Dur15].

Sender [WZ15].

Sensational [YGFL15].

sense [Kem11].

Sensing [CCZC13, Kar12, uHAN+18, RPG12, XWZW16, Fay16].

Sensitive [Kaw15, RQD+15, Tan15a, QCX18].

Sensitivity [YGD+17, LWW+10].

Sensor [ABC+17, BN14, CS14, DS11, KH10, LLC11, LLZ+12, NNN10, NVR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YIM16, ASO14, APK+18, AIB+16, AIC18, ADF12, BLAN+16, BBB16b, CGD12, CLSW12, DSCS12, DLN13, HTC+10, JNU17, JM+16, KLC+10, KO16, KLW+16, KDW+17, LC17, LNK+18b, PL16, SZMK13, SSK10, Wan13, WW14, WXK+17, XWDN12, XMHD13, ZYL+10].

Sensors [DL12, LIK+17].

Sensory [SCL14].

Sensing [CCZC13, Kar12, uHAN+18, RPG12, XWZW16, Fay16].

Sensitive [Kaw15, RQD+15, Tan15a, QCX18].

Sensitivity [YGD+17, LWW+10].

Sensor [ABC+17, BN14, CS14, DS11, KH10, LLC11, LLZ+12, NNN10, NVR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YIM16, ASO14, APK+18, AIB+16, AIC18, ADF12, BLAN+16, BBB16b, CGD12, CLSW12, DSCS12, DLN13, HTC+10, JNU17, JM+16, KLC+10, KO16, KLW+16, KDW+17, LC17, LNK+18b, PL16, SZMK13, SSK10, Wan13, WW14, WXK+17, XWDN12, XMHD13, ZYL+10].

Sensors [DL12, LIK+17].

Sensory [SCL14].

Seoul [LH10a, LW11a].

separation [MJS13].

Sequence [PFS12, WGZ+12].

Sequences [ADD10, Kla10, NN12, XYXYX11, HLC12, VM14].

Sequential [GLR10, GLR13, LLY15, WYL13].

Series [BJL16, Die12].

Serpent [PC16].

Server [BCO13, Che15, GMSV14, LSQL18, LYL15, YLW13, ATKH+17, CSD18, CLHJ13, FA14b, FHZW18, HDPC13, HL14, ISC+16, KMTG12, LXMW12, LH13, SY15b, bSZZ15, SsAF11, SsS11, TLL12, WT10a, XHM14].

Server-Aided [GMSV14, LYL15, SSF11].

Server-Designation [Che15, LSQ1L8].

Server-Side [BCO13]. servers [DRD11].

Service [BKBK14, CSS14, Hay13, LDB+15, LBR12, NRZQ15, RSGG15, SsPC12, St15, VS16, AaBT16, KPP16, LHL+18, LW13a, MMP19, MLM16, Par12b, Wu17, YWK10b, ZX11, YCM+13].

Service-Based [LDB+15].

Service-Oriented [RSGG15].

Services [Ano11b, DLZ+16b, MEFO12, OQ12, ZHL15, AZPC14, CSD18, CHX13, GAI+18, IMB17, IG11, NZL+15, PP11, WDKV19, XXX15].

Session [BS12, BKJP12, CFST17, SHS12, AN15, DCA12, SHBC19].

Session-Based [BKJP12].

Set [Cor14b, EKP+13, YZ12, Con12, TMK11].

set-valued [TMK11]. sets [SF12].

Setting [BKLS12, HHP17, MZHY15, TYM+17, XXZ12, ZHL15].

Settings [GZ12]. setup [Jia16].

Several [Sas12, ZT14].

SGX


Simulation [CPS16, LLH18, MS13a]. Simulation-Based [LLH18]. simulations [Ana14]. Simultaneous [YWZ+12].


SIP-based [ZTZ16]. SIPF [SYC+17]. Site [DSB15, SS10c]. siteDriverID [SGGCR+16]. Size [AS17, AEHS15, C13, CSW12, EAA12, Kim15, CLCL15, MTY11, ZMW16, AHI+12, LCT+14, PPTT15, SGM16, SHBC19].


Smart [AN17, ABC17, BSJ15, DL+16b, HCL+14, LA10, MFG16, PTD12, WGMdZ12, WgMW12, AMN18, CHS11, CLH13, GHD19, GAI+18, Ham19, HCC10, LH10c, LNM+11, LXMW12, LNK13, LNK+18a, LTC+15a, MM12, MNC+18, WMYR16, YZZ+14, YSL+10, Cho10, GLIC10, SD12].

Smart-Card-Based [HCL+14]. Smartphone [MDM17, uHAN+18, DL15]. Smartphones [Cor14b]. smashed [Fag17].


Snowden [Tox14]. SoC [GSC17]. Social [BPSD17, KTA12, NSA15, NRZQ15, PYM+15, Rog16, SKGY14, SZTZ18, WLY+15, ZW15, Zha15b, ZHL15, BDK11, HYF18, LCM+17, LZC17, MSM+18b, SSKS+18, Sni15a, YZL+18]. Society [Sch15a, Sch12b]. Socio [NS12].

Socio-Rational [NS12]. SoD [VN16]. Soft [Jin10, TLCF16, SS17]. Soft-Error [TLCF16]. Softw [WZM12a]. Software [Bar15, Bee17, EWS14, LRV14, MRL+18, MV16a, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GIJ+12, HLV10, KH10, LBOX12, SF12, YWT+12]. Solan [CGB+10]. solid [Cri16].

Solution [Fra15, GSF16, HLL15, Kam13, NA10b, YFT17, Cor14a]. Solutions [LLGJ16, BLV17, KAS15, MMP19, WW14].

Solved [IBM13a]. Solving [Ano17c, BB10, Bul10a]. Some [AD12, Ber12, Dur15, LW10b, Mid10].

Somewhat [ITC17, KOS16, MFB18]. Song [Con12]. Sood [MWZ12]. SOSEMANUK [PC16]. SOT [PAF18]. SOT-MRAM [PAF18]. Sound [COP14, LSR13, Sav15].

Source [Bis17, KFOV15, MBC15, RWLL14, ABF+14, LZC17, PX13, Pow14].

Source-Based [MBC15]. Sources [DHB16, BJ16, SSY12]. South [BL10, LW11a]. Soviet [Bu16]. SP [Sas12, SEHK12]. SPAPBox [FG+17].

Space [BWR12, BKL+13, NRY+14, RMG18, MSM+18b, RYF+13, ZZ15].


Spatiotemporal [DMT12]. Speaker [BJCHA17, PPRT12]. Special [An13d,
Ano16a, Ano16b, Ano16h, AB10b, CSYY18, GO17, LW13a, LLK18, PHWM10, XV13.
Specific [BDFK12, KME+12].
Specification [SK11, SD10]. Specifications [BMP12]. SPECK
[LFW+16, AMKA17, BSS+13]. Spectrum
[KD12a, TWZ+12, XNRG15, KP17, LWY12, MMSD13]. Spectrum-Based
[TWZ+12, XNRG15]. Speech
[AGW15, LJK17, SAA15, YMA17]. Speed
[ARM15, GL12, HZ11, KP17, LTKP16, BDL+11, KL13]. Speeding [RVRSCM12].
SPEKS [Che15]. spell [Bha16]. SPHINCS
[BHH+15]. Spies
[Has16, Keb15, Fag17, Mac14]. Spintronic
[IGR+16]. Splicing [YSC+15]. Spline
[Tan12a]. Split [CG14a, XZY+12].
Split-State [CG14a, XZY+12]. Splittable
[CP13]. SPN [LCL17]. Spoken
[WBC+10]. sponge [BDP11].
SPONGENT [BKL+13]. spongy [RS14].
Spoof [SP15a]. sputy [OS11]. Spread
[HGT15, KD12a, PSJ+13, TWZ+12, XNRG15, LWY12, MMSD13]. spreadsheets
[LT13]. Springer [Mei10, Mur10].
Springer-Verlag [Mei10]. Springs
[IEE11b]. Spritz [RS14]. Spy
[AHS13, FKO15, Bha16, Goo12]. SQL
[BS13a, Suc12]. Square [ARH14].
Squashing [GH11a]. SRAM [KLM+12].
SSH [YSS14, Cri16, Lit14, Ran10, der10].
SSL [BJR+14, Dav11, FHM+12, GIJ+12, HREJ14, NPH+14, PP11]. SSL/TLS
[BJR+14, Dav11, PP11]. SSL/TLS-based
[PP11]. SSO [MLM16]. St
[DDS12, Dan12, MSN11]. ST-Numbering
[MNS11]. stack [JSN+18], stage [Mas17].
STAMP [WPZM16]. Standard
[Ano12, Ano13a, App13, ABC+17, BCM12, BV11, BV14, CT18, GJJ15, GJZ17, HZX15, Loe15, MVVR12, OGK+15, SZS14, TCL15, WWH12, Yon12, ZC13, BCM13, HTC17, Kim11, LHT12, LL16b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, ZCL+19, AEH17, MKRM10, NdMMW16].
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, VPI17, VSR12]. Stateless
[BHH+15, GM11, MKAA17, NTY12, VDO14, DCA12].
Stateless/Stateful [NTY12]. statement
[NIS13]. Static
[DKMR15, IF16, Lan11, TLM13]. Station
[Smi11a]. stationary [ZLDD12]. Statistical
[Böhl10, Bro11, DBPS12, HZ11, Hey17, LTKP16, OOR+14, SP13, Sim15a].
Statistical-Attack [SP13]. Statistics
[gWpNyY+14]. Statutory [PH12b].
Stealing [RWZ12]. Steaky [BRPB13].
Steering [HR13]. Steganalysis
[Böhl10, DA12, Fri12, JHNN12, KD12b, LJK17, LC15, SG+12, Tan12a, YL+12, Y14, YPR17, LSQ11a, LSQ11b, Sch12a].
Steganalysis-Resistant [YPR17].
Steganalytic [Ber18, YPR17].
Steganographic
[DA10, HHS+15, LyWIZ12, WP15, AGL16, LLC10, CAC14]. Steganography
[AGW15, BCG12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZW+14, Joh10, LJK17, LLY+12b, MAL10, PDMR12, Pau10, SK12a, SR12b, TJZF12, WLL+14, YWW10, ZSA12, AOT13, BDK11, BHCdFR12, EEAZ13, GKKK11, LyWSS10, LRW13, LRW17, LWW+10, Maz13, MSM+18b, MS17, PHN+12, SI12, Sun16, WKH11, WOLS12, ZMS14]. Stego
[YLL+12, SMSK18]. Stego-Image
[YLL+12]. Stellenbosch [BL10]. step
[AKY13, YX+18]. Steps [Ano13c]. STES
[CML15]. Steven [Led16, Sch15a]. Still
[RAS15, UK18]. Stochastic [ADR18].
stolen [Bha16]. Stopping [Sav13a].
StopWatch [LGR14]. Storage [BCQ+13, CWL16, CCT+14, CLW16, GLG12, HSM14, JSCM17, Kül15, LCK11, LMD16, LWCJ14, QLL17, SKH17, XNKG15, ZDL12, ZVG16, AY14a, AKK+17, BP10, CFVP16, CFZ+10, CLH+16, CDF+10, CDL18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, Sar10a, SYY+16, YZCT17, ZYC+17, ZVH14].


STT [VDB+16]. Students [PP10a]. Study [Ano17c, DDR+16, SY15a, STC11, CCG10, EBFK13, MVH15, SS17, VG14]. Stuxnet [Zet14]. Style [GHP12, GHP13].

stylometry [BAG12]. sub [GPLZ13].

sub-passwords [GPLZ13]. Subcommittee [Bla16]. subliminal [LWZ10].


suitable [Jeo13, SKB+17]. suite [NACL12]. Sumo [BS12]. Sums [SS12b]. sun [Cer15]. super [MZ17a].


Surprises [Bow11]. Surrizontally [SFK15].

Surveillance [BPR14a, BPR14b, GZH17, Lan10, Ano16f].

Survey [ABHC+16, BGN17, BCTP16, BJJP14, BJC8A17, HPC10, KMY18, KSD+17, LGB+16, MR14b, GSM18a, MII10, NV10, OFMR16, SKH17, TRD11, TS16b, AAZ+16, ABB+14, ADH17, BIII13, BGG+13, FMA+18, HT13, KIN+16, KAS15, MIP19, MA17, Maz13, MVH15, NR11, PPA18, WW17].

Survival [YCM+13, MMS+17a]. Surviving [CFST17]. suspect [der10]. SVC [MU12, WDDW12, ZLDD12, ZLDD14].


Symmetric
Synchronizing [HZ11]. Synchronized [DM18, ACM12].
Symposium [ACM10, ACM11, Ano10, IEE10, IEE11b, IEE13, Wat10, Ano11a].
symptom [YZL18]. Synchronization [BL12, WXY17, yWXY18, AATM18, XNG14].
Synchronized [DM18, ACM12].
Synchronizing [HZ11]. SYND [MHC12].
Syndromes [BBC13]. Synergy [KRB12].
Synergy-Based [KRB12], synthesis [RS17]. Syst [HYS18, WZM12a]. System [AD11, Ano10, CZLC12a, CZLC14, Cor14b, CRST15, DG15, GOPB12, Har16, HHS15, IAD10, JN12, JW17, Jin10, KMP11, Lop12, MLBL12, NSM14, QL17, RSCX18, SMSG18, SRA17, SL11, YE12, YX12, YKK18, ZSM17, ZPW16, ZLDC15, ZVG16, AHM18, BC18, BGG13, Bu10a, CH11, CTL12, CZ14, CS11, FNW118, GCK11, HK15, HJ11, HLY14, JC13, LLLK10, LLL17b, Lit14, LTC15a, LLL18, MS12a, MNN15, PSOMP13, SSPL13, WMX17, WZ12, XWZW16, YZ18, ZMM10, ZML17, KKA14, Dew11].
System-Level [JW17]. Systematic [CCG16, CBL13, PC16]. Systems [AN12, AB15, BL15, BS13b, BCTPL16, BB10, CWL16, CCF17, CRE12, DLZ16b, GI12, HXC11, HCL14, HLN10, LMD16, LQY10, LY16, LNZ13, MR14b, OŠ12, PRSV17, QZL16b, RST15a, RST15b, SBS12, SFKR15, Sev16, SKH17, SGC14, SDM12, STC11, TKR14, YNR12a, AT10, AT10, CFVP16, CFZ10, CLZ17, dCCSM12, dCCSB16, CGH11, CVG13, CDA14, DZ12, E10, FXP12, GMOGCC15, GHD19, GSN16, GPVCdBRO12, HZW18, JKS16, JHCC14, KSA16, LCL15, LWK18, MLMSMG12, MG10, MFH13, NLY12, QMC17, SS10a, SR10, SRB12, WS14, YSM14, ZWH14, Zhu13, MA17, Ano11a]. Systolic [MCDB12], Systolic-Array [MCDB12], SZK [MX13].
T [SJWH17]. T-Chain [SJWH17]. Table [CCL13, AN14a, LDDAM12]. Tables [PTT16, XHM14]. Tag [NNM10, PPH12, CJP15, SPLHCB14, CJP12]. Tags [MO12, HSH11, HDPC13, HQY16, LEW19, MLD12a, PLSD1E10, TG17, WCFW18].
taming [BBDL17]. tamper [MN10, NC13, WGM12]. tamper-evident [MN10]. Tamperable [ACM17].
Tampered [SSA13]. Tampering [CG14a, SRA17, SG17]. TAO [Sta13].
TECC [Cra12, Linn14b, Sah13]. TEA [CWP12]. Teaching [GY13]. Team [LS14, Pf10, Ant14]. Tear [Boy16].
Technique [HEK18, KBL11, ZLDD14, BBBP13, CPPT18, GCSÁdd11, SM12, SKS18, TS16a, ZWS18]. Techniques [Bit17, DA12, GOS12, HPC10, HL14b, LW12, Mor12, PJ12, AB10b, BM13, FGFP14, Gil10, HT13, KHF10, LH11a, OO18, VN17, WMX17, Joh10].
technologies [JAE10, JAS11, Lan10, MWP19].
Technology [CGB10, Fol16, IEE11a, Wu16, Ham19, IMB17]. telecare [LWK18, MA17]. Telephone [SKE14].
Television [DTE17]. Tell [Cer14].
Template [NGA1H16, SKV12, AT1, GCSÁdd11].
Templates [DWB12, AHM+18]. temporal [JMWM+16, MHT+13, XMHD13].
temporal-credential-based [JMWM+16, XMHD13]. Tenant [TV15].
terahertz [WW13]. Term
[SKV12, CFVP16]. termination [SRB+12].
Ternary [AD11]. Test
[HTC+15, JEA+15, LSWM16, MZHY15, SS10b, WH18, HTC17, ZCL+19, Ano16g].
Testable [RMP10]. tester
[RPSL10, SY15b]. Testing
[Cou12, SS12a, AY14a, BJR+14]. Tests
[GLG12, MS12b, Sim15a]. Texas [IEE13].
Text [GdM16, SMSK18, ZZ18, CSR, SI12, SWW+17]. Text-dependent [GdM16].
Textbook [PP10a]. Texture [TSH17].
Theft [Ber12, Ber17, BTM15]. Their
[CZLC12b, CK18, JSK+17, NR12, CQX18, Hof16, IK15, KK10, Sti11]. them
[HLV10, JSK+16, Rus15]. Theological
[SS10c]. Theorem [Lau12, HF14a].
Theorem-based [Lau12]. Theoretical
[CVM14, MAL10, WSS12, CDGC12, SD10, SKEG14]. theoretical [KL13, ZZ15, Gas13].
Theoretically [TWZ11]. Theories
[ABR12]. 
Theory [ACM10, ACM11, CCKM16, CDFZ16, CDFS10, Cra12, FGM10, FBM12, FS15, 
Hes12, LW11a, Lin14b, Nac12, Per13, PJ12, RBP15, RST15a, RST15b, Sah13, SAKM16, 
Sh10, Wes16, Yan10, Abe10, AB10b, Bul10b, CFR11, Gil10, LPZJ15, MZA+13, McG11, 
YTM+14, Cra12, Lin14b, Sah13, vDKS11].
theory-based [LPZJ15]. There
[Cer15, MK10, Mck11, SM13]. Thin
[Chi16]. things [FQZF18, AAC+16, 
CLF+17, Ham19, HZL18, JKAU19, 
LNK+18b, LGH+17, NLLJ12, NLY15, 
PLGMCf18, SB17, WCCH18, YCT15].
Third [jCPB+12, QZL+16b, Sen10, BL10, 
ED19, Kip13]. Third-Party [QZL+16b].
Third-Round [jCPB+12]. Thirteen
[AP13]. thou [BDK11]. Threat
[CSYY18, ALL+18, Ven14]. Threats
[AJA16, ERLM16, GSC17, LJS+14]. Three
[CL15a, HXc+11, LZX+12b, PC16, Shi11, 
YKNS12, AIB+16, IC17, JKL+16, LNK+18a, 
LNK+18b, LML+13, Tso13, TKHK14, 
XCL13, YC12, YZZ+14].
Three-Dimensional [LZC+12b].
Three-Factor [HXC+11, AIB+16, IC17, 
JKL+16, LNK+18a, LNK+18b].
Three-party [LML+13, Tso13, TKHK14, 
XCL13, YC12, YZZ+14]. Threshold
[CT11b, Cil11, FGM10, GLW13, HYS11, 
LWL10b, SSU12, St12, Tan11, WYCF14, 
WLH15, YFF12, YHK+10, YLA+13, 
ZCL+12, DZ14, FGMP12, HF14a, HH15, 
OO10, QD16, SES+16, Shy15, SGM16, 
TD14, ZXJ+14, ZPWY12]. thresholding
[PC14]. thrive [Sch12b]. throughput
[MAK+12]. Thru [SYC+17, SYW17].
Thwart [LJS+14]. Thwarting
[TXT10]. Ticket [XHCH14]. Ticket-based
[XHCH14]. tickets [LMJC11]. tied
[Men13b]. Ties [PYM+15]. Tight
[GDCC16, LPS12, LLL18]. Tightly
[HLLG18]. Time [ASBD16, Ano17d, App14, 
AYS15, BJL16, Che17, FD11, GSC17, HC17, 
HGT15, IF16, JWJ+17, JEA+15, KME+12, 
LCL+17a, NA10a, Nov10, PNRC17, Ste15b, 
WLZL12, YE12, Ay14a, Ano15d, BM15, 
CC14, DCAT12, FHH10a, GPLZ13, HU15, 
LW10, LW13b, LML+13, MK11, Ano16g].
Time-area [Nov10]. Time-Memory
[ASBD16]. Time-Series [BJL16].
Time-Specific [KME+12]. Time-Spread
[HGT15]. Timed
[Ja14b, Kfos12, Tan15a, Unr15, WSS12].
Timed-Ephemerizer [Tan15a].
Timed-Release [KFO12, Unr15, WSS12].
Timing [BGN17, GY14b, Hay13, LGR14, 
AGH+17, SRB+12]. Tiny [ZOC10]. Titan
[PP10b]. Titan-R [PP10b]. TLS
[AP13, BBBD+17, BFCZ12, BJR+14, 
CFN+14, Dva11]. TLS-based [PP11].
Today [Ber16a, Mac12]. Toeplitz [Ye10].
Token [TYK+12, ZM16, IMB17, Jac16].
Top [SS12a, SS10c, Sta13, CHX13]. top- [CHX13]. Top-Fanin [SS12a]. Top-Secret [SS10c]. Topics [SCPSN10a, SCPSN10b, AB10b, Dun12b, Kial11, Pie10].
Topology [HHMK14]. Topology-Preserving [HHMK14]. Tor [LLY+12a]. Toronto [MV12]. Tossing [ALR13, DSMM14, Fok12, BB14].
Trusted [AWS17, EAA12, FPY15, YCR16, ED19, HTCS+10, Kip13, XZLW15].
Tunnels [Cir16]. Tunny [Cop10a]. Turing [DN12, FMTR12, HL10a, LCCJ13, WCL+18].
Transfer [AN12, BCPV11, LSL12b, pNyWyY+14, OWHS12, SM12, YWN1W5, BU13, MO14, NES+14, PC14, TK14, yWyWyYpN13].
Transformation [CRE+12, FJHJ12, XNB13, tWmCI2, GZH12, HQZH14, PGLL10]. transformations [CJXX19, SA14].
Transparency-Orientated [TJZF12]. Transparent [CCW+10, XTK10, ZHS+19]. Transport [RBHP15, TW14]. Trapdoor [BKWP12, CWWL12, Mat14, RPSL10, CSZ+11, CW12a]. treatment [YSM14].
Two-Round [HHG14]. Two-Server [YLW13, KMTG12, CSD18]. TwoFishe [MD12a]. TWS [OKG12]. Type [AKP12, CFL13, PFS12, SH15, BNST17, SYL13, WB12]. Type-based [CFL13, SYL13]. Type-Flaw [SH15]. Types [BCEM15].


updatable [LCL17a]. Update [BCE+10, KE19, LQY10, FS18, WFLX17].
updating [GCSAdP11, LJWY18]. Upper [AMVZ12]. URLs [AY14a]. USA [Dun12b, IEE13, Kia11, Lin14b, Pie10, Ral10, ACM10, ACM11, IEE10, IEE11b].
Usability [RAZS15]. Usable [DL15, TGC16]. usage [AKK17, BHCdFR12]. Use [CSV15, DFKC17, KOS16, NR12, YT12, der10, CZ15b, Die12, Hof16, KK10, MBF13, OO10, Sti11, UK18]. Used
useful

dCCSB\textsuperscript{+16}. **Usenet** [Bel18]. **User**
[BLK17, BKJP12, FLH13, Gdm16, Har16, JN12, LLC11, LCL17b, MZY15, MBC15, MM17, OdH12, PDT12, RW+16, SZDL14, SPM+13, WgMdZIZ12, WgMW12, ZHS+19, ZPW16, AaBT16, ATKH+17, APK+18, BT18, CH10, CHS11, CLJ13, DSCS12, GH16, GTSS19, HL14, KKM+13, KLW+16, KDW+17, LH10c, LNM+11, LNK13, LH13, MM12, OKG+12, hSZ15, SHBC19, WDKV19, WT01a, WOLS12, YHL+10]. **User-centric** [BLV17]. **User-controlled** [Har16]. **User-Friendly** [SZDL14, WOLS12]. **User-Generated** [LCL17b]. **User-Level** [BKJP12]. **user-participating** [CH10]. **User-Transparent** [ZHS+19].

users [Rus15]. **Using** [ABS+12, ABB+14, Ano15a, Ayu12, ARM15, BBC+13, BCPV11, Bee17, BFMT16, BKLS12, BJ+14, CST+17, IOV+18, LLG15, YM+13]. **utilization** [NZM10].

V2G [TODQ18, BT18]. **Validating** [GIJ+12]. **Validation** [FPY15, BJR+14]. **Validity** [BCF16]. **valuable** [Ana14]. **Value** [LSL12b, YWW10, BWA13, Svo14]. **valued** [BNA15, TMK11]. **VANET** [PZBF18, WLZ+16, Wu17]. **VANETs** [BMM12, CGCGPDMG12, CST+17, IOV+18, LLG15, YM+13]. **Variability** [VDB+16, SHBC19]. **Variable** [CHHW12, CMS17, DTZZ12]. **variable-interval** [DTZZ12]. **Variables** [BB10]. **Variant** [AAE+14, MVVR12, ZXWA18]. **Variants** [ASS15, BB10, Hin10]. **Variation** [DWZ12]. **Variations** [DSB16]. **Varied** [GZ12]. **varieties** [LR15]. **Varying** [GKCK11]. **vault** [KHMB13]. **VBF** [ACZ16]. **VBTree** [WL19]. **VDTNs** [PPS+13]. **Vector** [ACZ16, HHHK14, JHJN12, Kawa15, ZYT13, ZM16, DWZ12, LLM+19, PW010, TTL10, ZZ15]. **vector-form** [DWZ12]. **Vectorial**

[DDQL12, FY11]. **Vegas** [IEE10]. **Vehicular**

[HHKL15, ZWH+16, KM10b, SGCTR+16]. **Vein** [KLY+12]. **Velski** [BBB16b]. **Ventilated** [RSCX18]. **Vera** [Ayu12].

**Verifiability** [RST15a, RST15b, VSR12, WWHIL2, YMC+17, BRR+15, Hwa11].

**Verifiable** [CFE16, CRST15, Fuc11, HYS11, HLC12, LLL+18, QD16, RDZ+16, SZQ+17, XWJ16, YNR12a, YCR16, LZY+16, LJJ+17, NMP+13, PHGR16, QS18, XWS17, ZZ15]. **verifiably** [SEXY18, ZLY10]. **Verification** [App15, ABR12, BL15, CCK12, CC16, CCK16].

[CGCGPDMG12, BM15, MS13b].

[CGCGPDMG12, BM15, MS13b].

[CGCGPDMG12, BM15, MS13b].

W [Mar10a, Xie12, Hül13]. W-OTS [Hül13]. WA [LCK11]. Wakhnaghat [CGB+10]. Walker [Xie12]. Wallets [Chi13b]. Wallis [Wes16]. War [Has16, Mun17, Bud16, Car11, Sni11a]. Warbler [MFG16]. warriors [Bud16]. wartime [McK10, McK11]. was [Goo12, LHA+12]. Watermark [CHHW12, DLM+18, EMW14, Jin10, KBL11, LZC+12b, MCD12, SJ12, YE12, ZS12, HB13, TLL13, WYL13]. Watermark-Driven [DLM+18]. Watermarking [BCGAP12, BF12, BCP11, DDB14, BBM15, CG12b, CHHW12, CCZC13, DG17, FM15, Fra15, Fra16, GKB17, GP17, HPC10, HEK18, HGT15, HMK14, JSZS12, Joh10, JKH12, KDI2a, LSL12b, LP12, LD13, MM17, MR16, MU12, NGAuHQ16, NC12, NXH+17, pNyWY+14, OHWS12, RS16, RP12, RNI1, RUG18, SA20, SLGZ12, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, gWpNyY+14, WX+17, yWXyZ+18, tWmC12, XNG+14, XNMR15, YWNW15, YPR17, YK18, YYO15, ZZX+11, AP10, AIA+18, AMK12, BW13, BWA13, CCL11, CT11a, CSS+13, GZHD12, GA11, HKB14, HWYW14, JK13, KPS10, KJN+16, KM11, LSR13, LXC11, LLHS12, Lin14a, LKY12, MR16, SS10, TLL13, WYL13].

Watermarking [BCGAP12, BF12, BCP11, DDB14, BBM15, CG12b, CHHW12, CCZC13, DG17, FM15, Fra15, Fra16, GKB17, GP17, HPC10, HEK18, HGT15, HMK14, JSZS12, Joh10, JKH12, KDI2a, LSL12b, LP12, LD13, MM17, MR16, MU12, NGAuHQ16, NC12, NXH+17, pNyWY+14, OWHS12, RS16, RP12, RNI1, RUG18, SA20, SLGZ12, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, gWpNyY+14, WX+17, yWXyZ+18, tWmC12, XNG+14, XNMR15, YWNW15, YPR17, YK18, YYO15, ZZX+11, AP10, AIA+18, AMK12, BW13, BWA13, CCL11, CT11a, CSS+13, GZHD12, GA11, HKB14, HWYW14, JK13, KPS10, KJN+16, KM11, LSR13, LXC11, LLHS12, Lin14a, LKY12, MR16, SS10, TLL13, WYL13].
RS17, SKS+18, Tay14, TK14, TTL10, TPKT12, WLD11, yWpNyL11, Wan13, yWpWyYpN13, WZLW13, YWT+12, ZZKA17, ZSMS18.

Watermarking-Encryption [SLGZ12].

Watermarks [GL10, YT12]. WAVE

[AGW15, LSL12b, MR16, Ara13, AMK12, BW13, LXM11, MO14, yWpNyL11].

Wavelet-Domain [MR16]. wavelets

[BMM12]. Wavelet

[AGW15, LSL12b, MR16, Ara13, AMK12, BW13, LXM11, MO14, yWpNyL11].

weaknesses

[Nos11, Nos14]. weakness

[Nos11, Nos14]. weaknesses

[Zet14]. WECSR

[DDS12]. Weierstrass

[LL11]. weight

[OS11]. Weighted

[YLL+12, YTH17]. Weight

[GL10, DJG+15, ERRMG15, ZAG19]. WG-

[ERRMG15]. WG-16

[ZAG19]. Where

[CMM+18]. Whence

[DH11]. Whence

[DH11]. Whence

[DH11]. Where

[JCM12]. where

[McK10, McK11]. Western

[Han12]. Western

[BG14, GSW+16, GKS17, LTC+15b, NA10a, YLA+13, AZH11, BT12, BF11, BG14, CCW+10, DCA18, FSX12a, GH11a, GST12, GLM+16, HDPC13, ISC+16, LLV15, LGWY12, RG10, SY13, SLZ12, TAKS10, WWWW11, XQL11, XHM14, YS12, YKC+11, YFK+12, ZY17b, ZYM18]. Witness

[GGHW17]. WLAN

[KAHKB17]. woman

[Fag17]. women

[Hea15, McK10, McK11, McK12, MNN17]. Word

[WW12]. Word-Oriented

[WW12]. Words

[Gm16, KM10a]. Work

[RS11, Shp10, Tay14, BG14, Sch15a]. workbench

[CFH+13]. workflows

[BPP10]. working

[Wat14b]. Workload

[BCO13]. Workshop

[MV12, Sen10, Yan11]. Workshops

[DDS12]. World

[Ano16h, Ano17d, BFK16, BPS16, FKS+13, ...]
KM10c, LLK18, MDMJ17, Tom16, Con12, GIJ+12, Goo12, LCKBJ12, Pet11, SchH5c, Zet14, Mun17. world-class [Goo12].

**Worm** [WWC+11]. Worst [BIKK14].

**would** [McG11]. Wrapped [KM15, KM16].

**Write** [YNQ15]. Write-Efficient [YNQ15].

writing [LT14b]. wrong [LHA+12, UK18].

**WSN** [DL12]. WSNs [ABB19, ZYL+10].

Wu [LLK10]. **WW2** [Don14]. Wyner [ADG16].


ZIDS [NSMS14]. Zodiac [SDM10]. ZUC [WHN+12].

References

[AAC+16]

**Akyildiz:** Zootrace:2014:OTB


**Applebaum:** 2017:AC


**Abo-alian:** 2016:KDB


**Ambrosin:** 2016:FAB

Moreno Ambrosin, Arman Anzanpour, Mauro Conti, Tooska Dargahi, Sanaz Rahimi Moosavi, Amir M. Rahmani, and Pasi Liljeberg. On the fea-


Samir Athmani, Azeddine Bilami, and Djallel Eddine Boubiche. EDAK: An ef-
References


Almeida:2013:CCA

Arnold:2012:ICC

Ateniese:2017:LCS

Ambrosin:2017:OBB

Adrian:2015:IFS
David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot,


José Bacelar Almeida, Manuel Barbosa, Jean-Christophe Filliâtre, Jorge Sousa Pinto, and Bárbara Vieira.


Elena Andreeva, Andrey Bogdanov, Bart Mennink, Bart Preneel, and Christian Rechberger. On secu-
References

Arapinis:2012:RET

[ABR12]

ALMashrafi:2012:AIM

[ABS+12]

Applebaum:2010:PKC

[ABW10]

Arias-Cabarcos:2015:BIP

[ACAT+15]

Arnold:2015:NGH
T. W. Arnold, M. Check, E. A. Dames, J. Dayka, S. Dragone, D. Evans, W. Santiago Fernandez, M. D. Hocker, R. Kisley, T. E. Morris, J. Petreshock, and K. Werner. The next generation of highly reliable and secure encryption for the...

**Amoah:2016:FMA**


**Ardagna:2010:ECP**


**ACM:2010:PAI**


**ACM:2011:PAI**


**Avoine:2012:PFS**


**Austrin:2017:ICT**

Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and


Giulio Aliberti, Roberto Di Pietro, and Stefano Guarino. Reliable and perfectly secret communication over the generalized Ozarow–Wyner’s wire-tap channel. *Computer Networks (Amsterdam, Netherlands:
THING ATTASENA:2017:SSC
TTATTASENA:2017:SSC

THING ADIKARI:2011:HBT
TTADIKARI:2011:HBT

THING ABDALLA:2012:LBH
TTABDALLA:2012:LBH

THING ANDRYCHOWICZ:2016:SMC
TANDRYCHOWICZ:2016:SMC

THING ARALDO:2018:CEC
TARALDO:2018:CEC

THING AHMED:2017:IRD
TAHMED:2017:IRD
Attrapadung:2015:RGS


Antonopoulos:2017:DIS


Ahani:2015:SRB


Attrapadung:2012:ABE

Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie de Panafieu, and

Ali:2018:ECM


Ak:2014:ICS


Aiash:2015:FAA


Ali:2018:CBR

REFERENCES


(M. Almulla, A. Kanso, and M. Ghebleh). A concur-


REFERENCES


**Awad:2016:SSZ**


**Arnedo-Moreno:2010:JRA**


**Arsalan:2012:IRW**


**Ahir:2017:LAR**


**Abbasinezhad-Mood:2018:DHI**

Adj:2013:WDC

Aumasson:2014:HFB

Albrecht:2012:SDL

Arshad:2015:SAI
Hamed Arshad and Morteza Nikooghadam. Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol. The Journal of Supercomputing, 71(8):3163–3180, August 2015. CODEN JOSUED. ISSN 0920-8542 (print), 1573-


Anonymous. *ANSI X9.98-2010: Lattice-Based Polynomial Public Key Establishment Algorithm for

Anonymous:2011:MCB


Anonymous:2012:SHS


Anonymous:2013:DSS


Anonymous:2013:NCI


Anonymous:2013:SSD


Anonymous:2013:SIS

Anonymous:2016:CPSd


Anonymous:2016:EMT


Anonymous:2016:FVM


Anonymous:2016:GUP


Anonymous:2016:MBE


Anonymous:2016:SWT

REFERENCES

Anonymous:2016:SIR

[Ano16h]

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

[Ano17b]

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

[Ano17d]

Anonymous:2017:MBH

[Ano17e]
Anonymous. Mathematician breaks down how to defend against quantum

**Anonymous:2017:RV**


**Anonymous:2019:HCC**


**Anthes:2014:FTI**


**Andriotis:2013:JSD**


**Agarwal:2010:BR**


**Aumasson:2011:CHF**

Jean-Philippe Aumasson and Raphael C.-W. Phan. On the cryptanalysis of the hash function Fugue: Partitioning and inside-out distinguishers. Information Processing Letters,
AlFardan:2013:LTB


Ali:2018:SUA


Applebaum:2013:GXG


Applebaum:2014:CCP


Applebaum:2015:VCP


Albrecht:2015:FBR

Martin R. Albrecht, Davide Papini, Kenneth G. Paterson, and Ricardo Villanueva-Polanco. Fac-
REFERENCES

toring 512-bit RSA mod-
uli for fun (and a profit
of $9,000). Report, In-
formation Security Group
Royal Holloway, Univer-
sity of London, London,
3 pp. URL https://
martinralbrecht.files.
wordpress.com/2015/03/
freak-scan1.pdf.

Al-Qarni:2012:EII

Garsah Farhan Al-Qarni
and Farzin Deravi. Ex-
licit integration of iden-
tity information from
skin regions to improve
face recognition. Lecture
Notes in Computer Sci-
CODEN LNCSD0. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-31298-4_4/.

Arai:2013:MDH

Kohei Arai. Method
for data hiding based
on LeGall 5/3 (Cohen–
Daubechies–Feauveau: CDF
5/3) wavelet with data
compression and random
scanning of secret imagery
data. International Journal
of Wavelets, Multiresolu-
tion and Information Pro-
cessing, 11(4):1360006, 18,
2013. CODEN IJWMIP.
ISSN 0219-6913 (print),
1793-690X (electronic).

Adj:2014:SRC

G. Adj and F. Rodriguez-
Henriquez. Square root
computation over even ex-
tension fields. IEEE Trans-
actions on Computers, 63
(11):2829–2841, November
ISSN 0018-9340 (print),
1557-9956 (electronic).

AlTawy:2018:TCM

Riham AlTawy, Raghven-
dra Rohit, Morgan He, Ka-
likinkar Mandal, Gangqiang
Yang, and Guang Gong.
Towards a cryptographic
minimal design: The sLiSCP
family of permutations.
IEEE Transactions on
Computers, 67(9):1341–
1358, 2018. CODEN
ITCOB4. ISSN 0018-
9340 (print), 1557-9956
(electronic). URL https:
//ieeexplore.ieee.org/
document/8305605/.

Azarderakhsh:2015:PHS

Reza Azarderakhsh and
Arash Reyhani-Masoleh.
Parallel and high-speed
computations of elliptic
curve cryptography using
hybrid-double multi-
pliers. IEEE Transac-
tions on Parallel and Dis-
tributed Systems, 26(6):
1668–1677, June 2015.
CODEN ITDSEO. ISSN
1045-9219 (print), 1558-
2183 (electronic). URL
http://csdl.computer.
Ambrose:2012:RII


Asharov:2016:LPI


Artemenko:2017:PGO

Ahmadi:2011:SKC


Ahmadi:2012:SKE


Ahmadi:2013:IVB


Asaar:2015:IBM


Alsulaiman:2013:IVB


Altman:2010:AAP

REFERENCES

Argyropoulos:2010:BTP


Au:2011:PPT


Al-Tariq:2017:SFP


Alam:2015:ACF


Aslan:2016:DEM


Abdalla:2012:LRS

Michel Abdalla and Jill-Jenn Vie. Leakage-resilient spatial encryption. *Lecture Notes in Computer*
REFERENCES


Altaf:2017:LHL


Awad:2017:OLO


Anzala-Yamajako:2012:RAC


Ahmad:2014:RTN


AlTawy:2014:IDR


Aysu:2015:FRT


[Blaner:2013:IPP] B. Blaner, B. Abali, B. M. Bass, S. Chari, R. Kalla, S. Kunkel, K. Lauricella, R. Leavens, J. J. Reilly, and P. A. Sandon. IBM POWER7+ processor on-chip accelerators for cryp-

[BAG12]

[BAL10]

[Bar12]

[Bar15]
REFERENCES

http://csdl.computer.org/csdl/mags/sp/2015/05/msp2015050086-abs.html. [Bay10]

**Barker:2016:RKM**


**Batey:2010:DMW**


**Bax:2014:PPD**


**Baylis:2010:CC**


**Bulygin:2010:OSS**


**Bennett:2014:QCP**


**Barenghi:2016:FBS**

Alessandro Barenghi, Guido M.
REFERENCES


Boumerzoug:2016:LKM


Barenghi:2013:FIT


Baldi:2013:ULC


Barak:2014:OEF


Beurdouche:2017:MSU

Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindo-

**Beimel:2014:MLS**


**Bollman:2015:PWI**


**Bernstein:2011:PCI**

REFERENCES


REFERENCES

0164-0925 (print), 1558-4593 (electronic).

Buhrman:2014:PBQ

Bahri:2016:CCO

Bahi:2012:SCS

Borhoph:2012:PLL

Baelde:2012:TPR

Bahi:2011:ECS
Jacques M. Bahi, Raphaél Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation

Barthe:2012:CACA


Beunardeau:2016:WBC


Bitansky:2013:SNI


Bernstein:2014:CKR

REFERENCES

Basin:2012:PRI

Basin:2013:PRI

Basin:2015:ISC

Bicakci:2013:LSS

Botta:2014:PCI

Boyle:2014:EO
REFERENCES

Basso:2011:BWC


Bessani:2013:DDS


Blasco:2016:SWB


Biddle:2012:GPL


Belkacem:2014:DCM


Bender:2012:DSP

Bhasin:2015:EFB


Buchmann:2011:XPF


Barbareschi:2018:PBH


Bossuet:2016:EPA


For additional references, please consult the original sources cited in the text.
REFERENCES

2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).


REFERENCES


REFERENCES

Berretti:2018:IAS


Bouman:2011:SAW


Bas:2012:BLK


Bhargavan:2012:VCI


Barthe:2014:PRV


Bobba:2010:ABM


REFERENCES


**BGG**+13\[BGG+13\]


**Barak:**2010:IPO\[BGI**+10**\]


**Barbulescu:**2013:QPA\[BGJT13\]


**Barbulescu:**2014:HQP\[BGJT14\]

REFERENCES

Barthe:2012:ACA


Biswas:2017:STC


Borcherski:2014:LFH


Barkatullah:2015:GCF


Bhattacharjee:2016:SWC

REFERENCES


Biagioli:2012:CCS


Beimel:2014:CCW


Biswas:2017:SA


Brumley:2010:CAI


Boche:2016:DSK


Bouraoui:2017:HAE

REFERENCES

DEN ????, ISSN 1539-9087 (print), 1558-3465 (electronic).


Braun:2012:ULA


Brakerski:2010:OHB


Bogdanov:2012:KAC


Bogdanov:2018:IEA

Dan Bogdanov, Liina Kumm, Sven Laur, and Ville Sokk. Implementation and evaluation of an algorithm for cryptographically private principal component analysis on genomic data. IEEE/ACM Transactions on Computational Biol-

Bellare:2012:IBL


Bibak:2018:AUH

[BKST18] Khodakhast Bibak, Bruce M. Kapron, Venkatesh Sri-

Bothe:2013:EPS


Bernstein:2010:PCA


Byun:2011:SMC

REFERENCES


Benzaid:2016:FAW

Bai:2019:LMD

Buchmann:2017:PCU

Blomer:2012:TKG

Blondeau:2015:IDA

Bernstein:2012:SIN
REFERENCES


REFERENCES

126


REFERENCES


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


Bojinov:2014:NMC


Basin:2011:AIS


Beaulieu:2013:SSF


Batina:2012:HEB


Broustis:2012:GAN

REFERENCES


REFERENCES


Buchmann:2010:EKG


Budiansky:2016:CWN


Bulygin:2010:AOP


Bulygin:2010:CA


Burke:2011:AMD


Brakerski:2011:EFH


Brakerski:2014:EFH

Zvika Brakerski and Vinod Vaikuntanathan. Efficient

**Bitansky:2018:IOF**


**Bayrak:2012:AII**


**Bogdanov:2012:ZCL**


**Bhatnagar:2013:BIW**


**Bai:2016:ALC**

REFERENCES


Carter:2010:TB

CODEN ???. ISSN 1177-1380. URL http://rutherfordjournal.org/article030108.html.

Carlson:2011:JR


Casselman:2010:VC


Cobb:2013:LMS


Cachin:2010:EKS


Chang:2014:RRT


Chadha:2016:AVE

REFERENCES


REFERENCES


REFERENCES


Chen:2011:EAA


Chu:2014:KAC


Chen:2010:ALD


Chen:2013:WSB


Chiasson:2012:MWB

REFERENCES


Cao:2012:ITM


Chari:2010:DSC


Cui:2018:ABC


Coras:2016:AML


Costello:2014:CAS


Ceruzzi:2014:HFT

Cerf:2015:CTN


Cerf:2018:CSA


Cen
tenaro:2013:TBA


Checkowa

ty:2014:PED

REFERENCES

ISBN ????  LCCN ????  
URL ????.

Cevallas:2012:USR

Carstensen:2011:AAA

Calzavara:2017:SWJ

Celesti:2016:ALT

Choo:2017:EDF

Chang:2010:PRN
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.

Chen:2010:IFA

Camenisch:2012:EAA

Che:2012:WAM


Pranay Chaudhuri, Sukumar Ghosh, Raj Kumar Buyya, Jian-Nong Cao, and Oeepak Oahiya, editors. *Proceedings of the 2010 1st International Conference on Parallel Distributed and Grid Computing (PDGC)*, Jaypee University of Information Technology Waknaghat,
REFERENCES


**Caballero-Gil:2012:LAR**


**Chmiel:2012:EPC**


**Coull:2011:ACO**


**Cohn:2017:PSR**


**Curtmola:2011:SSE**


**Cheng:2012:PAI**


**Chandran:2014:PBC**


**Cheng:2013:NIB**


**Chen:2010:NUP**


**Chang:2011:DEQ**


**Chan:2013:OCT**


**Chang:2013:MPQ**


**Chappell:2013:PMI**

Brian Chappell. Privilege management — the indus-

**Chen:2011:CCI**


**Cheswick:2013:RP**


**Chen:2015:SSS**


**Chen:2017:CSQ**


**Chen:2012:SRF**


**Chien:2012:IAM**

Hung-Yu Chien. Im-


REFERENCES


REFERENCES


Chung:2018:ERN

Heewon Chung and Myungsun Kim. Encoding of rational numbers and their homomorphic com-


Chandra:2011:AST


Chang:2019:GTS


Chung:2018:ERN

Heewon Chung and Myungsun Kim. Encoding of rational numbers and their homomorphic com-


Chase:2013:SMN


Chuang:2011:LMA


Colin:2016:CTC


Comon-Lundh:2010:DSP


Chang:2011:RSB


Chen:2017:PGF

Yajing Chen, Shengshuo Lu, Cheng Fu, David Blaauw, Ronald Deslinski, Jr., Trevor Mudge, and Hun-Seok Kim. A

**Chong:2013:ASG**


**Chen:2016:RPR**


**Chen:2012:NCB**

[CLHC12] Yu Chen, Song Luo, Jianbin Hu, and Zhong Chen. A novel commutative blind-ing identity based encryp-

**Chen:2013:TSE**


**Chande:2016:NSC**


**Cao:2012:SRH**

[CLM+12] Jin Cao, Hui Li, Maode

Canetti:2013:PCC


Castro:2013:RAM


Chen:2014:CDP

REFERENCES


Coles:2016:NAU


Cao:2018:EEG


Chakraborty:2013:EHI


Chakraborty:2015:SSC


Chen:2017:VME


Cao:2016:OMA

REFERENCES


[Con12] Lucian Constantin. Researchers set new cryptanalysis world record for

**Connolly:2018:FE**


**[Con18]**


**[Cop10a]**


**Chung:2014:RRS**


**[COP14]**


**[Cor14a]**

in a research project by Rama-sany Gowthami and Ar-jen Lenstra at the LACAL laboratory at EPFL, Lau-sanne, Switzerland.

Coutinho:2012:RPT

Claessen:2013:SPN

Canard:2018:NTC

Chung:2016:NBB

Chen:2018:RLF

Chevalier:2010:CSC
REFERENCES

Chen:2012:DCC


Crampton:2011:PEC


Cramer:2012:TCT


Craver:2014:UCC


Clear:2012:CPA


Crichlow:2016:RSE

REFERENCES

[CRST15]

[CS11]

[CS12]

[CS14]

[CSH+18]
05/mco2018050060-abs.html.

Chadwick:2014:AFI


Chen:2013:RWM


Chen:2017:SIE


Ciegis:2016:ADP


Chong:2015:SID


Chow:2012:EPV

Yang-Wai Chow, Willy Susilo, and Duncan S. Wong. Enhancing the perceived visual quality of a size invariant visual cryptography scheme. *Lec-
Chen:2018:SIA


Chen:2011:IBT


Chen:2011:ARI


Canard:2018:CPK


Calzavara:2015:SLA


Chin:2013:SMB

Ji-Jian Chin, Syh-Yuan Tan, Swee-Huai Heng, and

Chang:2012:GBP


Chou:2013:TIB


Crenne:2013:CMS


Calmon:2014:ITM


Choi:2012:LTF

REFERENCES


[CWP12] Jiazhe Chen, Meiqin Wang, and Bart Preneel. Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT.
Chen:2012:CKS
URL http://link.springer.com/chapter/10.1007/978-3-642-30428-6_15/.

Chen:2014:MLC

Chen:2015:TCP

Chen:2012:FSD

Chen:2012:AIB
Yu Chen, Zongyang Zhang,


REFERENCES

9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-27575-3.

Davies:2011:IST


Diong:2012:DAU


Dacosta:2012:OTC


Cordeiro:2016:MPG


Dou:2018:OHR


De Prisco: 2013: CVC


D’Arco: 2014: MIC


Da Rolt: 2013: NDS


Datta: 2017: SFH


Castro: 2016: FVB

REFERENCES


Danezis:2012:FCDa


Derhans:2010:USC


Desmedt:2010:ES


Dew:2011:BRB


Durmuth:2011:DEN

Markus Dürmuth and David Mandell Freeman. Deniable encryption with negligible detection probability: An interactive construction. Lecture Notes in Computer Science, 6632:
REFERENCES


REFERENCES

Computer Society Order Number P4244.

[Driessen:2013:ESA]

[Die12]

[Drosou:2012:SAH]

[Din10]

[Ding:2015:CWF]

[Domnitser:2012:NMC]


REFERENCES


[DLK+16] Fikadu B. Degefa, Donghoon Lee, Jiye Kim, Younsung Choi, and Dongho Won.

**Djaziri-Larbi:2018:WDA**


**DiPietro:2016:CLD**


**Djaziri-Larbi:2018:WDA**


**Dong:2013:PRS**


**Dodis:2011:SSC**


**Duan:2016:SDC**

Li Duan, Dongxi Liu, Yang Zhang, Shiping Chen, Ren Ping Liu, Bo Cheng, and Junliang Chen. Secure
REFERENCES


[DMV15]


[DM15]


[DM18]


[DMS+16]


[DMS+16]


[DMWS12]

Donovan:2014:ATM

Doroz:2015:AFH

Duncan:2012:CAI

Ding:2017:CSM

Das:2016:CWM

Dziembowski:2018:NMC
REFERENCES

Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dixon:2016:NTO

REFERENCES


Dachman-Soled:2014:COF


Dini:2013:HHS


Drosatos:2017:PET


Deng:2012:VIA

REFERENCES

1026-7778 (electronic), 1563-5163.

Dunkelman:2012:MEK

Dunkelman:2012:TCC

Durcheva:2015:SAI

David:2012:PRE

Dorn:2012:ECE

Dong:2012:KKD
REFERENCES

Dong:2012:NDI


Dai:2018:OPC


Deng:2014:CCC


Dodis:2013:OWE


Deng:2014:TNI


Doss:2012:MD

Robin Doss, Wanlei Zhou, Saravanan Sundaresan, Shui Yu, and Longxiang

[DWZ12]

[DY13]

[DZ14]

[DZS+12]
REFERENCES


REFERENCES

Egele:2013:ESC

Edwards:2014:NRP

Esiner:2017:QRI

Esiner:2019:TFA

El-Emam:2013:NSA


REFERENCES


Evtyushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC


Engels:2012:HLA


Ebadi:2015:DPN

References


[FA14a] Mohammad Sabzinejad
REFERENCES


Farash:2014:SEI


Farash:2014:CIE


Fahd:2018:CPA


Fagone:2017:WWS


Fay:2016:ICM

REFERENCES


Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptography. In
REFERENCES


[Fan:2013:CPP] Chun-I Fan and Shi-Yuan

Fan:2010:PSN


Fan:2010:AMI


Farras:2017:IRN


Fahl:2012:WEM


Fan:2014:ASA

REFERENCES


REFERENCES

Forler:2012:DA

Feng:2012:CAO

Fallahpour:2015:AWB

Ferrag:2018:SCN

Farwa:2018:FAI

Faust:2014:CNM
Sebastian Faust, Pratyay Mukherjee, Jesper Bons

Feng:2012:USD


Fraczek:2012:MSI


Ferreira:2015:LPA


Fu:2018:LUA

REFERENCES


Fokkink:2012:TCG


Folger:2016:TQH


Fox:2013:RLQ


en.wikipedia.org/wiki/Linear_B_script.

Faigl:2014:PEC


Faust:2012:PLR


Fu:2015:TVG

Dong Lai Fu, Xin Guang Peng, and Yu Li Yang. Trusted validation for geolocation of cloud data. *The Computer Journal*,
REFERENCES

[197]


REFERENCES

Friksen:2010:SMC


Fridric:2012:MTS


Fu:2016:EPS


Frauchiger:2013:TRR


Forbes:2015:CTC


Fugkea:2018:SSA


Fang:2011:ICP

Liming Fang, Willy Susilo, Chunpeng Ge, and Jian-
REFERENCES

199


Feng:2011:GDA


Fang:2012:CCS


Ferguson:2010:CED


Fujikoka:2012:SHI


Fujikoka:2012:SEI

REFERENCES


Fanyang:2012:SAK


January 2014. CODEN IFC-SEN. ISSN 0129-0541.

GomezPardo:2013:ICM


Gross-Amblard:2011:QPW


Gregio:2015:TTM


Gope:2018:LPP


Galindo:2013:NIC


Gasarch:2013:RBC

William Gasarch. Review of Theoretical Computer Science: Introduction to Automata, Computability,
REFERENCES


Gutierrez:2016:IDO

Gorantla:2011:MKC

Guyeux:2015:ECS

Gupta:2012:CDF

Gupta:2013:HPH

Guerra-Casanova:2011:SOT
J. Guerra-Casanova, C. Sánchez-Ávila, A. de Santos Sierra, and G. Bailador.

Granado-Criado:2017:HCH


Gong:2016:ATI


Guerin:2016:TDU


Geller:2013:MIS


Gentry:2010:CAF


Gentry:2013:EMH

Craig Gentry. Encrypted messages from the heights
Gaspar:2012:SEF


Gong:2010:PCI


Grigg:2011:CCN


Garg:2016:CIO


Garg:2016:HSS

REFERENCES


[Gope:2016:EMA] Prosanta Gope and Tzonelih Hwang. An efficient mutual authentication and key...


REFERENCES


Gu:2015:EIB


Gu:2017:IBM


Gravier:2015:WOD


Gravier:2016:MPA


Goyal:2013:CZK


REFERENCES


Gligor:2012:SLT

Gollmann:2010:SCR

Guo:2011:ED


Behrad Garmany and Tilo Müller. PRIME: Pri-

Gotzfried:2014:MAT

Gofman:2016:MBE

Giambruno:2015:GGB

Garcia-Martinez:2015:HEB

Garcia-Morchon:2015:HCR

Guo:2011:ISS
Fuchun Guo, Yi Mu, and Willy Susilo. Improving security of q-SDH based digi-


REFERENCES

Goo:2012:CBS


Garcia:2012:ERP


Gorski:2010:CDS


Groth:2012:NTN


Glowacz:2017:IDW


Gong:2013:NOT


Goodrich:2012:EVW


Genkin:2016:PKE


Grosschadl:2012:EJ1


Genkin:2014:GYH

Daniel Genkin, Itamar Pipman, 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

Discussion of suspected NSA-supported back door in the 2007 NIST standard for the Dual Elliptic-Curve default random number generator, and the associated RSA cryptographic library BSAFE. There is evidence that the back door exists in some older Canon laser printers.

Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Guha:2017:RTS


Guin:2016:FCS


Gong:2016:FSC


Gierlichs:2012:ICD

Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall. Infective computation and dummy rounds:
REFERENCES


[GTSS19] Michael T. Goodrich, Roberto Tamassia, and Nikos Triandopoulos. Efficient authenticated data structures for graph connectivity and geometric...

**Grosse:2013:AS**


**Gueron:2016:MEG**


**Gupta:2015:GEM**


**Galindo:2014:LCL**


**Ghosh:2014:BBB**


**Gorbunov:2012:FEB**

REFERENCES


Gorbunov:2015:ABE


Greenberg:2014:GWB


Gebotys:2016:PCP


Wang:2014:RAW


Gao:2015:GCC


Goh:2013:TOT

REFERENCES


Guo:2012:AKE

Guo:2017:EMD

Gao:2012:RHC

Guo:2018:SMK

Ge:2013:SAP
Haigh:2017:HRC


Hamamreh:2012:RPA


Hamlin:2017:NMC


Hamidi:2019:ADS


Hanyok:2012:EH


Harn:2013:GA


Harrington:2014:GEF

Surya Michael Harrington.

Hardesty:2015:BAC


Hardesty:2016:SUC


Hastings:2016:SWS


Hayes:2013:NSA


Houmansadr:2013:BCN


Hurlburt:2014:BBC


Hetzelt:2017:SAE


Hernandez-Becerril:2016:GIS

Rogelio Adrian Hernandez-Becerril, Ariana Guadalupe...
REFERENCES


Ching-Fang Hsu, Guo-Hua Cui, Qi Cheng, and


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 CSSEE1. ISSN 0267-6192.


Martin E. Hellman. Turing Lecture: Cybersecurity, nuclear security, Alan Turing, and illogical logic. *Communications of the Association for Comput-
REFERENCES

ing Machinery, 60(12):52–59, December 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL https://cacm.acm.org/magazines/2017/12/223042-
cybersecurity-nuclear-security-alan-turing-and-illogical-logic.


Huang:2016:EDP


Heyse:2012:TOC


Hua:2015:TSE


Han:2011:PEB


Harn:2015:DTS


Hu:2016:EWS


REFERENCES

Hinek:2010:CRV

Hinkelmann:2011:CPA

Hur:2014:SDR

Houmansadr:2014:NBW

Hur:2013:REC

Heyse:2012:LEA
REFERENCES

Heil:2014:APH


Howe:2018:PDG


Holenstein:2011:ERO


Harn:2010:AGK


Hazay:2010:EST


Hsu:2011:NIB

Hsieh:2014:AMU

Hmood:2015:A

Hu:2012:VMS

Hu:2016:PBR

Huang:2011:ISL


[Huang:2015:CEA] Xinyi Huang, J. K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou. Cost-effective authentic and anonymous data sharing with forward security. IEEE Transactions


[Huang:2015:CEA] Xinyi Huang, J. K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou. Cost-effective authentic and anonymous data sharing with forward security. IEEE Transactions
REFERENCES


Howard:2010:DSS


Hohenberger:2012:DDQ


Huang:2014:SWC


Hefeeda:2010:ASM


Herzberg:2012:TJA


Hore:2012:SMR

Bijit Hore, Sharad Mehrotra, Mustafa Canim, and Murat Kantarcioglu. Secure multidimensional range

[Hoang:2012:ESB]

[HMR12]

[HN10]

[Hoffmann:2015:LBQb]

[Hoffmann:2016:LBQb]

[Hol12]
REFERENCES

Hyla:2012:CBE


Hazay:2014:OSA


Halder:2010:WTR


He:2012:ECT


Howe:2015:PLB


Hur:2010:CCS


Herranz:2013:SMS

Hulsing:2016:MMT

Hwang:2011:CDA

Hubballi:2018:NTC

Haitner:2010:EIC

Homma:2014:TFD
Halevi:2011:TBH


Han:2013:IBD


Han:2014:IBS


Han:2012:PPD


Heather:2014:CPE


Shi:2015:CTS


Hamdy:2011:HPB

REFERENCES


David Hald and Alex Udakis. Rethinking remote authentication: time to kiss tokens goodbye? *Net-...
REFERENCES


Hulsing:2013:WOS

Hurlburt:2016:MBO

Harvey:2017:FPM

Han:2012:MIA

Hwang:2011:NIB

Holbl:2012:ITP
He:2016:STI


Heng:2010:CNS


He:2015:SSQ


Hsu:2014:VWR


Huang:2011:GFT


Huang:2018:PIB

[HYF18] Qinlong Huang, Yixian Yang, and Jingyi Fu. PRE-CISE: Identity-based private data sharing with conditional proxy re-encryption.
in online social networks. 


Hao:2011:NTV


Huang:2011:IBS


Heys:2011:PSC


Han:2012:ERI

REFERENCES

244

Han:2014:ERI

Han:2014:ATS

He:2017:AHA

He:2018:LAB
REFERENCES

He:2015:IEI


Islam:2015:MBA


Ismail:2010:EAE


IB11


IBM:2013:DMP


IBM:2013:IPC

REFERENCES

Irshad:2017:CPP


IEEE:2010:PIA


IEEE:2011:ICI


Imanimehr:2016:HPR


IEEE:2011:PIA


IEEE:2013:PIS


IEEE:2010:PIA
REFERENCES


[I:2017:ETB] Indu I., Rubesh Anand P. M., and Vidhyacharan Bhaskar. Encrypted token based authentication with adapted SAML tech-
REFERENCES


Yuval Ishai and Mor Weiss. Probabilistically checkable proofs of proximity with


Yuval Ishai and Mor Weiss. Probabilistically checkable proofs of proximity with

Jacobs:2016:STB


Jie:2010:AAI


Jie:2011:RGA


Prins:2011:DCA


Jain:2013:MSD


Jho:2016:SSE


Jiang:2014:UIS


Jiang:2014:TEA


Jiang:2016:MAC


Jiang:2017:BMA


Jin:2010:ADW


Jain:2010:QP


Jawad:2013:GAD

Khurram Jawad and Asifullah Khan. Genetic algorithm and difference expansion based reversible wa-
REFERENCES


[JN12] Anil K. Jain and Karthik Nandakumar. Biometric authentication: System se-

Jan:2017:PPB


Johnson:2010:BRF


Johnson:2015:NGA


Joux:2013:NIC


Jepps:2013:CCP


Juels:2014:HEE

JR14 Ari Juels and Thomas Ristenpart. Honey encryption: Encryption beyond the
CODEN ????. ISSN 1540-7993 (print), 1558-4046 (electronic). URL http://

**Jevdjic:2017:ASC**


**Jain:2016:APQ**


**Judmayer:2017:BCI**


**Jordan:2018:EPE**


**Jiang:2018:CPA**

Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Com-
REFERENCES


Jiang:2012:DCA


Joye:2012:FAC


Ji:2012:NBD

Tong:2012:NBD


Jiang:2016:CVI


Juels:2014:INC


Ioannis G. Karafyllidis. Quantum gate circuit
REFERENCES


REFERENCES


Kim:2011:SSE

Koz:2012:ASE

Kraetzer:2012:PCS

Karakoc:2013:BCL

Karakoc:2015:AKA

Kumari:2017:DSU
Saru Kumari, Ashok Kumar Das, Mohammad Wazid, Xiong Li, Fan Wu, Kim-Kwang Raymond Choo, and Muhammad Khurram Khan. On the design of a secure user authentication and key agreement scheme for...


REFERENCES


[KKGK10] Giorgos Karopoulos, Georgios Kambourakis, Ste-


**Klapper:2010:PSS**


**Ko:2010:MME**


**Koeberl:2012:EPD**


**Kumari:2016:UFM**


**Kim:2012:INS**

Keller:2010:DAS

Khomejani:2010:PCT

Koblitz:2010:BNW

Kiani:2011:MPD

Kifer:2014:PFM

Koblitz:2015:RWE
REFERENCES


REFERENCES


[Kavun:2018:SAE]

Kumari:2016:APW


[Koblitz:2010:BRB]


[Kasper:2012:SCA]

REFERENCES

**Khamsemanan:2016:BBU**


**Kawachi:2017:GCR**


**Kollmitzer:2010:AQC**


**Kang:2012:AKM**


**Kolman:2017:SCG**


**Koya:2018:AHM**

Kumar:2017:TAU

Kiltz:2011:EAH

Khalid:2016:RHL

Kocabaş:2012:CPB

Kang:2016:DSA

Keskinarkaus:2010:IWD
A. Keskinarkaus, A. Pramila.

Krenn:2013:CCR


Krudsen:2011:BCC


Krantz:2012:EAM


Kostinger:2012:SBL


Kannan:2013:NQF

REFERENCES

Krenn:2013:AWI


Kolesnikov:2012:LPP


Khan:2010:RCB


Kumar:2015:RGB


Karthiga:2018:PSA


King:2011:BBB


Kocabas:2016:ESM

[KSA16] Ovunc Kocabas, Tolga Soyata, and Mehmet K.

Khan:2017:TPK


Kiljan:2017:SAC


Kwon:2018:EIP


Kim:2012:SSS


Klingler:2013:UPT

REFERENCES

Kim:2012:SAH


Kawachi:2012:SKE


Kobayashi:2016:ASC


Klisowski:2012:CCP


Kai:2014:FSD


Kupcu:2013:DTT

Kupcu:2015:OAS


Kuznetsov:2011:APP


Kiljan:2018:ETA


Koyama:2012:NTD


Karpovsky:2014:DSS


Kuo:2016:SDD


Kamal:2010:EIN


Kuo:2018:DRA


Kate:2010:PBO


Lu:2010:MSC


Lathey:2015:IEE


Lackey:2015:UHP


Liang:2015:SEC

Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, and Anjia Yang. A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. Future Generation Computer...


2013. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Luo:2012:ESI


Lupu:2012:IBK


Lu:2013:CSA


Liu:2015:IAG


Laxmi:2017:GGS


Liu:2013:IA

[Yining Liu, Chi Cheng, Jianyu Cao, and Tao Jiang. An improved authenticated

**Lathrop:2011:SPI**


**Lavington:2012:ATH**


**Li:2015:NAC**


**Lee:2017:SUE**


**Liu:2017:GAU**

Can Liu, Gradeigh D. Clark, and Janne Lindqvist. Guessing attacks on user-generated gesture passwords. *Proceedings of the ACM on Interactive, Mobile, Wearable

Li:2015:CEH


Li:2017:RNF


Liang:2014:CCS


Liu:2016:EQD

REFERENCES


Liu:2016:NOP


Liu:2019:TTR


Launchbury:2012:ELT


Lieden:2016:RME

George Ledin, Jr. Re-


REFERENCES

tice and Experience, 29 (17), September 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


[LGM+16] Ruggero Donida Labati,
REFERENCES


Lopéz-Garcia:2014:PBB


Li:2014:SCA


Liu:2012:FVC


Lee:2010:ISC


Lee:2010:CGC

REFERENCES

Li:2010:EBB


Lee:2011:PSE


Lin:2011:NIB


Lertvorramatham:2012:ISM


Liao:2013:NMS


Lenstra:2012:RWW

Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, Whit is right. Report, EPFL IC LACAL, Lausanne, Switzerland,


REFERENCES


Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP


Li:2017:MMMA


Li:2016:IRI


Li:2017:SQS

Li:2012:OEA


Laszka:2014:STC


Liu:2018:PAB


Liu:2017:OOA


Lee:2014:SPB

Jooyoung Lee and Daesung Kwon. Security of permutation-based com-
REFERENCES

expression function \(lp231\).


Le:2011:RMA

Le:2015:TSS

Lu:2016:PFC
REFERENCES


REFERENCES

Liu:2018:VSE

Libert:2019:ZKA

Li:2010:DCY

Lu:2012:IEC

Lai:2018:EQK
Hong Lai, Mingxing Luo, Josef Pieprzyk, Zhiguo Qu, and Mehmet A. Orgun. Efficient quantum key distribution using Fibonacci-

Lee:2016:CAM


LLSW16


Luo:2012:FSI


Lee:2016:AGA


LLW16


LLY+12a

[LLZ+12] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui

[LLY+12b] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui

Luo:2012:BBE

Lee:2015:SAS


REFERENCES


Xiong Li, Jianwei Niu, Saru Kumari, Fan Wu, and Kim-Kwang Raymond Choo. A robust biometrics based three-factor authentication scheme for Global Mobility Networks

**Li:2018:TFA**


**Li:2013:ESC**


**Li:2011:CIB**


**Liu:2015:SAB**


**Liu:2013:GPB**

Hong Liu, Huansheng Ning, Yan Zhang, Daojing He, Qingxu Xiong,


Ling:2012:SHS


Lima:2010:PKE


Lian:2015:GRG


Liu:2017:HPI


Lampe:2012:ATS


Liu:2015:GTB


[LQD+16] [LRV14]


[LQY10] [LRW13]


[LRW17] [LRV14]

REFERENCES

Lane:2014:PBD

Luo:2012:FSU

Lin:2015:SSE

Lychev:2016:RSI

Lee:2012:IBS

Lei:2012:RAW
Baiying Lei, Ing Yann Soon, and Zhen Li. A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition.


Will Landecker, Thomas Shrimpton, and R. Seth

**Lee:2013:CCM**


**Le:2014:IMX**


**Lee:2014:NDH**


**Liu:2015:IMB**


**Liu:2015:MSG**

REFERENCES

Li:2015:FSC

Lao:2016:BFD

Lysyanskaya:2010:AEC

Lin:2011:CNS

Li:2016:LRC
REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Pages</th>
<th>Year</th>
<th>DOI</th>
<th>URL</th>
</tr>
</thead>
</table>

**Note:** The URLs provided are for the respective papers, where available.
Lu:2014:HOM


Liu:2010:NDC


Liu:2010:SET


Liu:2011:PIA


Liu:2012:MMA

REFERENCES

10.1007/978-3-642-34117-5_13/.

Li:2010:GCP


Lou:2010:NAS


Luo:2012:ICB


Li:2012:IA


Lin:2010:DSM


Li:2011:NIW

REFERENCES

Li:2014:IBD


Li:2014:EMK


Lai:2012:RHB


Luo:2014:ARP


Liu:2015:SDS

Chen Liu and Chengmo Yang. Secure and durable (SEDURA): an integrated encryption and wear-leveling framework for PCM-based...


Liu:2014:CRA


Li:2010:PES


Li:2012:ESS


Li:2016:BMA


Masdari:2017:STA


MacCormick:2012:NAC

REFERENCES

stable/10.2307/j.ctt7t71s.
With a foreword by Christopher M. Bishop.

[Mac14]

[Maf16]

[MAK+12]

Moskowitz:2010:ITE

Malkin:2013:SCB

Mangard:2013:KSL

Martin:2010:FWL
Douglas Martin. Frank W. Lewis, master of the cryptic crossword, dies at
REFERENCES


Martin:2010:PCC


Martin:2010:XMA


Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP


Maurer:2012:CCN

Maieron:2015:BAM


Mazurczyk:2013:VSD


Milo:2011:FGB


Mao:2015:PUA


Malone:2013:MOD


Migliore:2018:PPF

REFERENCES


secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there. Gardners Books, 2011. ISBN 1-84513-633-0. ?? pp. LCCN ???.


REFERENCES


Mansfield-Devine:2015:MIC


Morduc:2010:CPB


Mosenia:2017:PTS


Maachaoui:2012:MLA


Meiklejohn:2010:BRB


Menezes:2013:IPB

Alfred Menezes. An introduction to pairing-based cryptography. Report, Department of Mathem-


**Micciancio:2010:FGC**


**Michiels:2010:OWB**


**Michael:2016:RNI**


**Midgley:2010:SEE**


**Martinez-Julia:2012:NIB**


**Martinez-Julia:2013:BSI**

Mohanty:2011:RTP


Moessner:2012:SAS


Muller:2012:HPC


Mozaffari-Kermani:2017:FDA


McGrew:2016:SMH


Malik:2012:AIC

REFERENCES

Marconato:2013:VLC


Mozafari-Kermani:2010:CSI


Mancillas-Lopez:2010:RHI


Mendez:2016:PES


Montecchi:2012:QSE

REFERENCES


[MM14b] Subijit Mondal and Subhashis Maitra. Data security-modified AES algorithm and its applica-
REFERENCES


Maity:2017:ODC


Mulholland:2017:DCD


Moldovyan:2012:BBD


Mahmood:2014:PPK


Marino:2019:ACN


Macedo:2017:SSP

Ricardo Macedo, Leonardo Melniski, Aldri Santos,

Mazumder:2017:PSK


Mazumder:2017:SAE


Maity:2013:CRS


Matsuo:2012:MAK


Meshram:2012:IBC

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


Minier:2012:RKI


Mizuki:2011:ASN

Takaaki Mizuki, Satoru Nakayama, and Hideaki Sone. An application of ST-numbering to secret key agreement. *International Journal of Foundations of Computer Science*...

Maimut:2012:LCR


Minamoto:2014:BDI


Mone:2013:FPE


Moo:2012:RFF


Moody:2014:DMW


Morad:2012:OEA


Moulick:2015:RDS

Minier:2012:EEC


Meiklejohn:2016:FBC


Mundhenk:2017:SAN


Mironov:2012:IDP


Mukhamedov:2010:IEP


Maimut:2014:AET

[MR14a] Diana Maimut and Reza Reyhanitabar. Authen-

**Marasco:2014:SAS**


**Micali:2014:CMS**


**Manimehalai:2016:NRR**


**Migliore:2018:HSC**


**Martinovic:2017:AUP**


**Matsumoto:2017:ACG**

Stephanos Matsumoto, Raphael M. Reischuk, Pawel Szalachowski, Tiffany Hyun-Jin Kim, and Adrian Perrig. Authentication challenges in a global environment. *ACM Transac-
REFERENCES

335

tions on Privacy and Security (TOPS), 20(1):1–1:??, February 2017. CO-
DEN ????. ISSN 2471-2566 (print), 2471-2574 (elec-
tronic).

I. Zarei Moghadam, A. S. Rostami, and M. R. Tan-
hatalab. Designing a random number generator with novel parallel LFSR
substructure for key stream ciphers. In 2010 Interna-
tional Conference on Computer Design and Applica-
IEEE Computer Society Press, 1109 Spring Street,
Suite 300, Silver Spring, MD 20910, USA, 2010.
URL http://ieeexplore.
.ieee.org/stamp/stamp.
.jsp?tp=&arnumber=5541188.

Florian Mendel, Vincent Rijmen, Deniz Toz, and
Kerem Varici. Differential analysis of the LED
block cipher. Lecture Notes in Computer Sci-
CODEN LNCSDO. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
.com/chapter/10.1007/978-
3-642-34961-4_13/.

Subhashis Maitra and
Amitabha Sinha. A new
algorithm for computing
triple-base number system.
ACM SIGARCH Computer
Architecture News, 40(4):
3–9, September 2012. CO-
DEN CANED2. ISSN
0163-5964 (print), 1943-
5851 (electronic).

Piotr Mroczkowski and Janusz Szmidt. The cube
attack on stream cipher Trivium and quadraticity
tests. Fundamenta Informaticae, 114(3–4):309–318,
August 2012. CODEN FUMAJ.
ISSN 0169-2968
(print), 1875-8681 (elec-
tronic).

Subhashis Maitra and
Amitabha Sinha. Design
and simulation of MAC
unit using combinational
circuit and adder. ACM
SIGARCH Computer Ar-
33, December 2013. CO-
DEN CANED2. ISSN
0163-5964 (print), 1943-
5851 (electronic).

Subhashis Maitra and
Amitabha Sinha. High ef-
ciciency MAC unit used
in digital signal processing and elliptic curve
REFERENCES


Kinga Marton, AlinSuciu, and Iosif Ignat. Randomness in digital cryptography: a survey. Romanian Journal of Information Science and
REFERENCES


Mosenia:2017:CCA

Martins:2018:SFH

Muhammad:2018:ISU

Mosca:2013:QKD

Morozov:2012:ZKP

Malkin:2011:ECS
Tal Malkin, Isamu Teranishi, and Moti Yung. Efficient circuit-size independent public key encryption with KDM security. Lecture Notes in
Muftic:2016:BCC


Mundy:2017:CGU


Miri:2012:SAC

Ali Miri and Serge Vaudenay, editors. Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11–12, Revised Selected Papers, volume 7118 of Lecture Notes in Computer


Ma:2015:PKE


Nagy:2010:OTP


Nagy:2010:QCS


Naccache:2012:CST


Naccache:2016:FHE


Naranjo:2012:SAK


Nunez:2017:PRE


REFERENCES


REFERENCES


Nafea:2016:HMB


[NGAuHQ16]

NIST:2012:RRN

NIST. Recommendation for random number generation using deterministic random bit generators. Special Publication 800-90, National Institute for Standards and Technology, Gaithersburg, MD 20890, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

NIST:2013:CSS


[NG13]

Nguyen:2014:DDI


[NKWF14]

[NIS12]

Ning:2012:DPB


Ning:2015:APB

Huansheng Ning, Hong Liu, and Laurence T. Yang.

**Ning:2012:DCA**


**Nieto:2013:PVC**


**Nieto:2014:FSH**


**Nguyen:2012:DQB**


**Neville-Neil:2015:KVH**

Nagy:2010:KDV


Navin:2010:ETU


Nose:2010:SWA


Nose:2014:SWS


Novotny:2010:TAE


Nichols:2014:CSS

Nguyen:2011:APB


Nguyen:2012:SOU


Namasudra:2017:NSA


Niu:2015:CRS


Naccache:2010:THI


Nojoumian:2012:SRS


Noorman:2017:SLC

Nie:2013:CHB

Natgunanathan:2017:PBM

Newell:2014:NCR

Niu:2015:NAS

Nikooghadam:2010:EUE
REFERENCES


[Obana:2011:AOC]

Obana:2011:AOC


[Oba11]

Obrenovic:2012:IUC


[OdH12]

Oliynykov:2015:NES

Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymirov, Victor Ruzhentsev,

[OGK15]


[OFC11]


[OCDG11]

Olieri:2011:REA


[OF11]

Onica:2016:CPP


[OFMR16]
REFERENCES


Ogiela:2018:LTC


Orlandi:2014:SCN


Ormond:2016:CPR


Ozen:2011:MIS

Owczarek:2012:LPL


Osborn:2016:SSR


Orencik:2016:MKS


Okamoto:2012:AAH


Otmani:2010:CTM


Ogiela:2018:VCA

Urszula Ogiela, Makoto Takizawa, and Lidia Ogiela. Visual CAPTCHA application in linguistic cryptog-


REFERENCES

Pandey:2014:ACR

Parent:2012:WAI

Park:2012:APO

Pass:2013:USP

Pranata:2013:MDR

Paulson:2010:SDO

Pandit:2012:EFS
Tapas Pandit and Rana


REFERENCES

ISSN 1550-4859 (print), 1550-4867 (electronic).

Poh:2017:SSE


Pang:2014:PPA


Paul:2012:KSS


Pereira:2015:PKE


Pippal:2012:SVU


Pearson:2011:NWC

Joss Pearson, editor. Neil Webster’s cribs for victory: the untold story of Bletchley Park’s secret...
REFERENCES


Jong Hyuk Park, Sajid Hussain, Guilin Wang, and Yi Mu. Special issue of computers and mathematics with applications on


Pramila:2018:ICA


Peter:2012:AHE


Phuc:2016:SAS


Perez:2011:FDS


Peris-Lopez:2018:EAC


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-

**Pendl:2012:ECC**


**Pyun:2012:IBF**


**Pathak:2012:PPS**


**Phan:2012:DDB**


**Phan:2012:MBT**

Papadopoulos:2015:PAP


Pandey:2012:PPS


Piret:2012:PBC


Puthal:2019:SAL


Polyakov:2017:FPR


Popa:2012:CPQ

[Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. CryptDB: pro-

**Priemuth-Schmid:2012:ASV**


**Permpoon:2014:FTG**


**Perazzo:2015:DRL**


**Pereira:2013:SLC**


**Phatak:2013:SIN**


REFERENCES


Philippaerts:2013:CMC


Pei:2015:SWT


Papadopoulos:2010:CAR


Phuong:2018:CBE


Pournaghi:2018:NNE


Patsakis:2015:PSM

Constantinos Patsakis, Athanasios Zigomtros, Achilleas Papageorgiou, and Agusti Solanas. Privacy and security for multimedia content shared on OSNs: Issues and countermeasures. The Com-


signature-based handover authentication scheme for LTE wireless networks. \[\text{QYWX16}\]


**Qiao:2018:CTC**

[QRW+18]

Huidong Qiao, Jiangchun Ren, Zhiying Wang, Haihe Ba, and Huaijie Zhou. \[\text{QZ14}\]


**Qin:2016:STI**


**Qian:2014:IAF**


**Qiang:2016:SCF**

Qi:2016:SID


Qi:2016:SPR


Qin:2018:BRO


Rabin:2010:ACC


Rankin:2010:HLH


Rankin:2014:HEY


Rankin:2016:HSP

REFERENCES


REFERENCES


Reardon:2016:SDD


Rhee:2015:ARC


Ren:2010:CSH


Roh:2010:BSW


Robert-Inacio:2011:SAP


Rjascko:2012:BBP


Regev:2011:QOW

Oded Regev and Bo’az Klartag. Quantum one-way communication can be exponentially stronger


REFERENCES

Rhee:2010:TSS

Ren:2015:ASE

Rawat:2011:CBR

Rosen:2010:CCS

Reeder:2011:WPD

Rivest:2014:SSR

Rossi:2015:IBS
Francesco Rossi and Giovanni Schmid. Identity-based secure group communications using pairings. Computer Networks
REFERENCES


See also news story [Ano15a].

**Ruj:2014:DAC**


**Rus15**


**Rahulamathavan:2016:UCA**


**RVRSCM12**

Juan José Rodríguez-Vázquez, Sixto Romero-Sánchez, and Miguel Cardenas-Montes. Speeding up a chaos-based image encryption algorithm using
REFERENCES


Roettger:2012:PKC


Ren:2014:HHM


Rogaway:2012:SCS


CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-27549-4_76.

Ren:2013:PPK


Ristenpart:2010:WGR


Ren:2013:DSE

Ling Ren, Xiangyao Yu, Christopher W. Fletcher,


Siad:2016:NFI


Saarinen:2012:PPK


Suoranta:2012:SAM


Sarreshtedari:2015:WMD


Schutz:2010:DIN


Sacco:2014:MC


Sahai:2013:TCT


Sarier:2012:SNB


Sarkar:2014:PEK


Sarier:2018:MBI


Singh:2018:SDD


Sasaki:2012:DSW


Savage:2013:NSL


Savage:2013:PP

REFERENCES

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES


REFERENCES

3/13/data_and_goliath_bruceschneier_on; http://www.democracynow.org/blog/2015/3/13/part_2_bruceschneier_on_the

Schneier:2016:CHT


Shrestha:2010:KBA


Seberry:2010:CTAa


Seberry:2010:CTAb


Shu:2015:PML


Saleh:2010:GTF

REFERENCES


Shen:2012:PAS

[SD12]

Shakiba:2010:IID

[SDM10]

Souissi:2012:OCP

[SDM+12]

Shakiba:2014:CCI

[SDM14]

Seo:2014:RHI

[SE14]

Seo:2016:RHI
Jae Hong Seo and Keita Emura. Revocable hierarchical identity-based encryption via history-free approach. Theoretical Computer Science, 615(??):45–60, February 15, 2016. CODEN TC-


[Sakai:2016:CDN] Yusuke Sakai, Keita Emura, Jacob C. N. Schuldt, Goichiro Hanaoka, and Kazuo Ohta. Constructions of dynamic and non-dynamic threshold public-key encryption schemes...

**Simha Sethumadhavan:2016:HEP**


**Charles Severance:2016:BSB**


**Jae Hong Seo, Keita Emura, Keita Xagawa, and Kazuki Yoneyama:2018:AOF**


**Erkay Savas:2014:SMQ**


**Chen Su and Haining Fan:2012:IIN**


**Asaf Shabtai:2010:SAP**

REFERENCES


Prabu S, Gpinath Ganapathy, and Ranjan Goyal. Enhanced data security for public cloud environment with secured hy-

**Sanchez-Garcia:2016:SSA**


**Sun:2015:FSW**


**Shen:2018:CAL**


**Susilo:2016:EDT**


**Shankar:2012:BDF**

REFERENCES


[SHS12] Sanna Suoranta, Jani Heikkinen, and Pekka Sil-
References


Shyu:2015:VCR


Satir:2012:CBT


Simion:2015:RST


Simmonds:2015:DI


Sierer:2016:TPS

Shakeri:2012:RZW


Shin:2017:CGI


Sabri:2011:AFS


Sachnev:2012:IME


Seo:2012:MPM


Scarani:2014:BPQ


P. Szalachowski, B. Ksiezopolski, and Z. Kotulski. CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block

**Stevens:2015:FCF**


**Singh:2018:MWT**


**Scheidat:2012:STT**


**Schmitz:2012:NAC**


**Srivatsa:2011:ESA**

REFERENCES


**[SM10]** 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 ???.


REFERENCES


REFERENCES

Smith:2011:RBA

Smith:2015:HHB

Smith:2015:DBP

Świerczynski:2015:PSE

Stankovski:2014:CFE

Sharma:2018:CSS

Sadeghi:2010:THI
[Ars10] Ahmad-Reza. Sadeghi and David Naccache, edit-


Serwadda:2013:ELK


Shiaeles:2015:FII


Spafford:2016:SE


Safkhani:2014:CCA


Shim:2015:SDA


Sun:2013:IUP

San-Tsai Sun, Eric Pospisil.


REFERENCES

2330-1643 (print), 2330-1643 (electronic).


Szaban:2011:IQB


Saxena:2012:BIT


Shparlinski:2012:CSD


Sendrier:2013:HCE


Sadhya:2017:PRE


Singh:2013:QBF

Durgesh Singh, Shivendra Shivani, and Suneeta Agarwal. Quantization-based fragile watermarking using block-wise authentication and pixel-wise recovery scheme for tampered image. *International Jour-
REFERENCES


Daniel Stolte. Experts determine age of book ‘nobody can read’. UANews,


REFERENCES


Sahillioglu:2014:SCM


Savas:2015:GMA


Shao:2015:SAS


Song:2017:SSI


Song:2017:SAM

REFERENCES


[SZZT18] Weiwei Sun, Jiantao Zhou, Shuyuan Zhu, and Yuan Yan. Robust privacy-preserving image sharing

Tsang:2010:BRR


Tamayo:2015:AFH


Tan:2011:CTA


Tan:2012:SLM


Tan:2012:LCP


Tang:2015:ETE

[Tan15a] Qiang Tang. From ephemeralizer to timed-ephemeralizer: Achieve assured lifecycle enforcement for sensitive data. The Computer Journal,
REFERENCES


Tilli:2015:GCR


Tuan:2010:AWB


Taylor:2011:DR


Tang:2015:CER


Tan:2017:JDC


Tian:2014:DFS

REFERENCES

Tiplea:2014:NSC

Tao:2013:SMS

Terai:2011:BRB

Tassa:2012:SDC

Tewari:2017:CNU

Theofanos:2016:SUE
Tian:2016:IBS

Tian:2015:IBP

Tian:2012:TOE

Thabit:2014:RRW

Takayasu:2019:PKE

Tu:2014:EPB
REFERENCES


[Tani:2012:EQA]

[Tu:2013:PAQ]

[Tariq:2014:SBL]

[Tan:2016:ESE]

[Tsaur:2012:ESM]

[Tsai:2013:ZWS]
Hung-Hsu Tsai, Yen-Shou Lai, and Shih-Che Lo. A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection. The Journal of Systems and
REFERENCES


Gines Dolera Tormo, Felix Gomez Marmol, Joao

**Terrovitis:2011:LGR**

**Terrovitis:2012:PPD**

**Toa:2018:AAC**

**Tomb:2016:AVR**

**Toxen:2014:NSS**

**Tsougenis:2012:PEM**
Tan:2016:BIB


Tang:2014:PAB


Taylor:2011:CAS


Tezcan:2016:IID


Tschorsch:2016:BBT


**Toreini:2017:TRP**

**Tang:2011:IDC**

**Tso:2013:SAI**

**Tseng:2012:ERI**

**Tseng:2015:LFI**

**Tsai:2010:RLI**
June 2010. CODEN JS-SODM. ISSN 0164-1212.

**Tupakula:2015:TES**


**Thorpe:2012:CRB**


**Tripunitara:2014:CKM**


**Wu:2012:SWG**


**Tartary:2011:EIT**


**Tian:2012:SSB**

Ty:2016:CCA


Tolba:2016:GMA


Trammel:2012:DTP


Uzunkol:2018:SWU

Osmanbey Uzunkol and


REFERENCES


[Vatajelu:2016:SMB]

[vanDam:2011:TQC]

[Vetter:2010:ABV]

[Venkatakrishnan:2017:DRB]


REFERENCES

www.sciencedirect.com/
science/article/pii/S0747717113001703


www.sciencedirect.com/
science/article/pii/S0020019016301715


REFERENCES

Vivek:2012:CSE


Vlacohos:2015:DPC


vanTilborg:2011:ECS


Vuagnoux:2010:CAC


Wagstaff:2010:C


Wagner:2016:TPF


Walter:2018:RCS

REFERENCES

Wang:2010:NSB

Wang:2013:CRA

Wang:2014:IIB

Wang:2018:LRI

Ward:2011:CCM

Wat:2010:IPI
REFERENCES

Waters:2012:FER

Watts:2014:ICB

Watts:2014:PYI

Watts:2015:HGA

Wang:2012:PCE

Weisse:2017:RLC

Wright:2010:USP
Charles V. Wright, Lucas Ballard, Scott E. Coull,


REFERENCES


Xianfang Wang, Jian Gao, and Fang-Wei Fu. Secret sharing schemes from linear codes over $F_p + \nu F_p$. *International Journal of Foundations of Com-
Wang:2010:DVT

Xiaofeng Wang, Philippe Golle, Markus Jakobsson, and Alex Tsow. Deter-
ing 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, Chunjian Ma, Sendong Zhao, and Changli Zhou. Breaking a robust remote user
CODEN LNCSDD. ISSN 0302-9743 (print), 1611-
3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-
3-642-35606-3_13/.

Wei:2012:NCI

Xiaopeng Wei, Ling Guo, Qianguang Zhang, Jianxin Zhang, and Shiguo Lian.
A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic
CODEN JS-SODM. ISSN 0164-1212 (print), 1873-1228 (electronic). URL http://

Wang:2017:DRM

Yi Wang and Yajun Ha. A DFA-resistant and masked
PRESENT with area optimization for RFID appli-
cations. *ACM Transactions on Embedded Com-
CODEN ???? ISSN 1539-
9087 (print), 1558-3465 (electronic).

Wang:2018:GAD

Lin Wang and Zhi Hu. On
graph algorithms for de-
genecity test and recursive
description of stream ci-

**Wang:2015:EFF**


**Wang:2017:DVP**


**Wei:2016:PAB**


**Wu:2012:DAA**


**Wang:2012:NFS**


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).


Jianghong Wei, Wenfen Liu, and Xuexian Hu. Forward-secure threshold attribute-based signature

Wei:2014:EEF


Wang:2016:LLE


Wang:2012:RTC


Wu:2012:PSC


[Wang:2017:PPK] Yujue Wang and Hwee-


Williams:2013:APC


Whitworth:2014:SPC


Wang:2015:RSA


Wang:2014:NDH


Watanabe:2012:ITT


Wang:2012:PAC

REFERENCES


**Wu:2012:AST**


**WWBC14**


**Wen:2014:MZC**


**Willis:2013:IFI**


**Wang:2014:ATF**


Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, and Ashok Kumar Das. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in


[Wang:2014:NAI] Xiaojing Wang, Qizhao Yuan, Hongliang Cai, and
REFERENCES


**Wei:2012:IHV**


**Wang:2013:NSW**


**Wei:2016:APS**


**Wang:2013:BSB**


**Wei:2014:IDC**


**Wang:2014:CGR**

REFERENCES

Wen:2011:DSH

Wei:2015:CPK

Wang:2018:AMB

Weng:2013:VWI

Wei:2012:CSO

Wei:2012:GOP
Fushan Wei, Zhenfeng Zhang, and Chuangui


[XHCH14] Li Xu, Yuan He, Xiaofeng Chen, and Xinyi Huang. Ticket-based handoff authentication for wireless mesh networks. Computer Networks (Amster-
Xi:2012:MDA


Xue:2014:LDP


Xue:2017:CNC


Xue:2012:RAA


Xiong:2012:PPK

Xu:2017:GKG


Xu:2016:CIB


Xu:2013:PKE


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

Xue:2012:AH}


Xiang:2016:EMP


Xue:2013:TCB

Kaiping Xue, Changsha Ma, Peilin Hong, and Rong Ding. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Ap-
Xie:2013:ECP


Xiang:2014:PBA


Xia:2015:SPK


Xiang:2015:SSB


Xiong:2011:CIB


Xin:2010:IEB

[XSWC10] Hong Xin, Zhu Shujing, Chen Weinbin, and Jian Chongjun. An image encryption base on

Xiao:2010:TAT


Xie:2010:ORI


Xie:2013:SIP


Xiong:2012:CBP


Xu:2016:CCP

Xiong:2017:CCC


Xia:2016:SDM


Xie:2014:SCP


Xu:2018:SKS


Xu:2018:DFH

Xiao:2016:REM


Xiong:2015:SRE


Xie:2012:DPK


Xiao:2018:KRL


Xing-Yuan:2011:PRS


Xu:2015:ORA

REFERENCES


[YD17] Meng-Day (Mandel) Yu and Srinivas Devadas. Pervasive, dynamic authentication of physical items. *Communications of the Association for Comput-

Yasuda:2015:MQC


Yan:2016:DEB


Ye:2010:ACC


Yamada:2012:PBR


Ye:2014:NIE


Yekhanin:2010:LDC


Ye:2016:IEA

[YH16]

Yang:2016:IHA

[YHHS16]

Yu:2010:IBF

[YHK+10]

Yang:2016:RKF

[YHL16]
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Yang:2014:MDF</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Yoo:2010:IRR</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Yang:2018:AIW</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Yu:2012:IRI</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Young:2013:TPC</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Yang:2018:AIW</strong></td>
</tr>
</tbody>
</table>
REFERENCES

Yum:2012:OPE

Yoshino:2012:SIP

Yuen:2013:ELT


Yu:2017:ACA


Ying:2013:PPB


Yu:2010:PSI


Yu:2011:CLE


Young:2015:DWE


Yavuz:2012:BFB


Yang:2012:EMA


Yin:2017:QPE


Yengisetty:2011:AVC


Yumbul:2015:EEP

REFERENCES

Yang:2015:EPS

Yeh:2010:TRR

Yao:2014:NCR

Yeh:2016:ECV

Yuen:2014:TCT

Ylonen:2014:SAA
REFERENCES

Yang:2011:CCK


Yang:2011:CPK


Yamada:2012:UEW


Yeh:2017:SIB


Yang:2014:IBI


Yang:2011:ACD


Yasuda:2012:ASM

[Takanori Yasuda, Tsuyoshi}

Yang:2018:IAC


Yang:2018:IA


Yan:2017:PIS

Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


Yang:2010:CRS


Wang:2018:CIW


Yu:2012:SME

REFERENCES

Yu:2016:CDI

Yang:2018:PBC

Ye:2018:ISS

Yoon:2011:SBC

Yesilyurt:2015:RWM

Yang:2013:ECS
Xiao yuan Yang, Li qiang Wu, Min qing Zhang, and Xiao-Feng Chen. An ef-

Yang:2016:EPA


Yang:2012:LUC


Yang:2017:SKS


Yang:2018:CDD


Yang:2012:BPN

Shuguo Yang, Yongbin Zhou, Jiye Liu, and Danyang Chen. Back propagation neural network


**Zhu:2012:JLS**


**Zh:2013:RMS**


**Zhang:2015:PCL**


**Zhang:2012:TCS**


**Zhang:2019:EPK**


**Zhang:2014:GCS**

Yinghui Zhang, Xiaofeng Chen, Jin Li, and Hui Li. Generic construction for se-

[**Zhang:2015:IAI**]


[**Zet14**]


[**Zhou:2018:SAE**]

Zhao:2010:PSA


Zhou:2016:HFD


Gao:2012:DES


Zadeh:2015:ASP


Zhang:2012:LDC


Zhang:2015:BYO

REFERENCES


Zhao:2013:TSC


Zhou:2015:EPP


Zhang:2016:PPV


Zimand:2010:SEC


Zeng:2014:NFC


Zhou:2012:CBF

Qing Zhou and Xiaofeng Liao. Collision-based flex-

Zhou:2015:PPS


Zhang:2012:EEF


Zhao:2014:TAH


Zhang:2012:IAS


Zhang:2015:RBA

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

Zhang:2012:CCB


Zhu:2017:PSN


Zhang:2010:ESP


Zhou:2019:LIB


Zhang:2016:TLT


Zhang:2017:FGA

Rui Zhang, Hui Ma,

**Zhang:2010:NSS**


**Zielinska:2014:TS**


**Zhang:2016:CAH**


**Zafar:2010:GRN**


**Zhang:2017:PPN**

REFERENCES


REFERENCES


REFERENCES


Zhou:2016:SRB


Zhou:2014:SAC


Zhang:2014:LFL


Zhang:2011:AGK

Zhou:2018:QTA


Zilberberg:2013:PCM


Zhang:2015:FER


Zhang:2013:LPP


Zhou:2011:PSA


Zhang:2016:PAG


Zhang:2014:EFH

Xiaojun Zhang, Chunxiang Xu, Chunhua Jin, Run Xie,

**Zhang:2018:AKE**


**Zhang:2018:VPA**


**Zhang:2016:DEP**


**Zhang:2011:SIR**


**Zhou:2017:CLR**


hidden vector predicate. 


[BZ17] B. B. Zaidan, A. A. Zaidan, H. Abdul. Karim, and