Title word cross-reference

(2, 2) [KSSY12, LTC+15b]. (K_N)
[Bai10, YC11]. (n, t_n) [LHYZ12], (t, n)
[QD16, ZPZY12]. 0 [XHX+17], 1
[XHX+17]. 1, 2, 3 [SMDS11]. 11 [LJ17], 13
[Blo15]. 2 [DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGLL10, WY12]. 22 [MNP12], 2^{k
}[Sun16]. 3 [AP10, CG12b, DWWZ12,
FWS13, GZHD12, GH11a, KWS+12, LJ17,
LJ15, MKH+12, RS16, SS10b, SS12a, SGS14,
WSSO12, tWmC12, YT11a, YI14, YPRI17],
32 \times 32 [SA14]. 3 \times 3 [ÁMVZ12]. 4
[COP14, DWWZ12, HL144]. $49.00$ [Sch15a].
8 [LPO+17]. $S9$ [APPVP15]. = [JUW10]. +
[PYH+18]. 2 [YNX+16]. 3 [LHM14], ^MT
[HRB13]. a [TTL10]. c [KRDH13]. d
[QD16], d \times d [KA]-1, t [ZTL15], F_p + \nu F_p
[WGF16]. \gamma [DWWZ12]. GF(2)[x] [SF12].
GF(2^m) [SKH15], GF(2^n) [LBOX12]. K
[FXP12, FR16, CHX13, ZHT16].
L(1/4 + o(1)) [Jou13]. M [MMSD13, ÖS11].
F_{3\text{typo}} [AMORH13]. F_q [SS13]. \mathbb N^P [HN10].
GF(q) [LPds10]. LWE [BV14], \mu [Jia14a]. N
[FR16]. n \times k(k \geq n/2) [MC11]. O(d13^d
[KA17]. O(n^2) [KS11]. P [DG17]. \pm 1
[HZW+14]. q [GMS11]. S [LJ15]. t
[JJUW11, Ob11]. w [Kre13].

-band [MMSD13]. -Bit [LPO+17]. -boxes
-dimension [DWWZ12, QD16]. -Diversity
[ZTL15]. -Encoded [DG17]. -Encoding
[XHX+17]. -Means [KRDH13]. -Multiple
[LTC+15b]. -NN [ZHT16]. -Party [JR13].
-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, LH10a]. 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]. AAT [FQZF18]. Abandon
[Lec15]. ABE [FJHJ12, HQZH14, QZZ18,
TY16a, YMC+17, ZSW+18b]. abelian
[CDSLY14, LR15]. ability [WS12]. absence
[AGH+17]. Abstract
[Bul10a, CFR11, MZ17b]. abuse
[JSMMG18, QRW+18]. Accelerating
[CMO+16, DOS15, SKH15]. Accelerator
[MRL+18, PC16, WOL15]. Accelerators
[AW17, 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, SGC14,
SC12, WS13, XMCL13, YTH17, YSS14,
ATKH+17, ACK+10, AMHJ10, CLH+16,
Cra11, DFJ+10, FNWL18, FS10, HZL18,
JAS+11, LCL+17a, LCL+15, ML16,
NZM10, NAL17, QCX18, Shy15, Tan12b,
TODQ18, Wan18, WS12, XHH12, ZZ15,
ZML17, ZDW+16, ZWS+18, ZFH+18].
AccessAuth [TODQ18]. accessing
[CSD18]. Account [Bro11]. Accountable
[SCGW+14, YMC+17, ZZ12]. Accumulable
[SEXY18]. accumulator [KYY18, LZY+16].
accumulator-based [LZY+16].
Accumulators [PTT16]. Accuracy
Alan [CS12, Don14, Hel17, LCKBJ12].
Apache [Lit14]. API [FLW12]. Append [YNR12b]. Append-Only [YNR12b].

Application [AKP12, AK14, BRT12, BS12, CKLM13, CCKM16, CCW+10, CSTR16, CLCZ10, CHS15, Küp15, LW11a, LWKP12, MNS11, Oo12, SEHK12, SS13, XJW+16, YWK10b, YTS12, ZH15, ZM16, Abe10, BBBP13, BT18, CZ15b, GLIC10, HH15, Jia14b, LGKY10, LWKP14, MSL+18b, NAL17, OTO18, SE18, SGCRM+18, XHH12, YY11, ZAC17].

Application-Level [CCW+10].

Applications [AMVZ12, Ana14, BKPW12, Ber18, BKST18, BCG+12b, BJCHA17, BSV12, CZLC12a, CZLC12b, CPS16, CK18, DK15, FSK10, GKM16, GRL12, Hs12, HN10, JW1+17, Nac12, NV10, PJJ12, RBS+17, Rudd+17, SCPSN10a, SCPSN10b, Sha10, Ter11, TYK+12, WH17, YR11, Ano11a, CFR11, CSZ+11, CQX18, CDA14, Dur15, EBPK13, FE10, Fri10a, Gill0, KO16, LWZG10, LR15, LBOX12, LTT10, MS13c, MM14b, OK18, PHWM10, PKN15, SW+17, ZZ15, ZMS18].

Applied [BSS11, KP10, MR10, Xie12].

Applying [Bar12].

Approach [CTC+15, Chi16, HLZ15, HLF12, KKA15, MKN13, MZ17b, PS14, RP12, SLGZ12, Sta12, SH15, SC12, TCC+17, TTL12, Vl12, VKC15, WYC14, yWxyZ+18, ZW15, AL15, AT10, BSS11, CLZ+17, CO11, CML16, DZS+12, FMB+18, GGH+16b, KL13, LFCCGCRP14, MCP15, NC13, PJJ18, SE16, WMY16].

Approaches [GWM16, LC15, SB14, MKH+12, OK18].

Approximate [SP15b].

Approximate [CN12, JSCM17, SG14].

AppSec [RQD+15].

April [BL12, MCDB12, NKWF14].

ARIA [PH12a].

Arithmetic [AK14, AAB17, Fre10, HSA14, IEE13, KIF10, PGL12, ZAG19, DTZ12, MO14].

Array [BL12, MCDB12, NKWF14].

Array-Based [SGJ+18].

ARX [KL13].

Assessing [CBL13].

assets [WHJ17].

Assignment [LMS16].

Assisted [KCC17, LLKA19, HZ18].

Associated [Sar10b].

associated [BS15].

Associate [ABR12].

Assumption [LV12, LZ14, ZG10].

Assumptions [BDH11, CZF12, DN12, GKS17, KM10c, PDH15, AB10].

Assurance [BMBS10, Bar15, KMP+11, RBNB15, WL11, Ser12].

Assured [Tan15a, WMY16].

Asymmetric [DG12, XLM+12, XGLM14, XZLW15, ZWQ+11, CSS+13].

asymmetric-histogram [CSS+13].

asymptotic [DTZ12, TD14].

Asymptotically [LPS12].

Attack [ano15d, BSR17, BMS12, Bro17, CJP12, DSB15, FXP+17, zGZW12, GV14b, GDC16, HCET+12, HLZ15, JHL12, JKP12, LLW16, LGL+12, LJ17, LCLW17, LWKP12, LWPF12, MS2b, Pud12, SP13].

architecture-independent [BVIB12].

Architectures [AMKA17, BGG+13, BJ17, CHS10, DF17, MKAA17, FPB14, HL14, MK11, Nov10].

Area [GMV17, HC17, LZZ14, WH17, KP18, LMJC11, LI+17, Nov10, SGJ+18].

Area-Time [HC17].

Areas [MV12, JD14].

Arguments [BGL+13, AB17].

Arithmetic [AK14, AAB17, Fre10, HSA14, IEE13, KIF10, PGL12, ZAG19, DTZ12, MO14].

Array [BL12, MCDB12, NKWF14].

Arrays [LB13, TRD11, KM10a].

Art [ABJ13, BL15, LK18, Sen17, BDP11].

ARX [KL13].

Atomic [Bai12].

ASBUS [YWF18].

ASIACRYPT [LW11a, Abe10].

ASIC [CFZ+10, KMY18, MKAA17].

Asking [DL15].

ASM [Vie14].

ASM-Based [Vie12].

ASP.NET [DR11].

Assessing [CBL13].

assets [WHJ17].

Assignment [LMS16].

Assisted [KCC17, LLKA19, HZ18].

Associated [Sar10b].

associated [BS15].

Associate [ABR12].

Assumption [LV12, LZ14, ZG10].

Assumptions [BDH11, CZF12, DN12, GKS17, KM10c, PDH15, AB10].

Assurance [BMBS10, Bar15, KMP+11, RBNB15, WL11, Ser12].

Assured [Tan15a, WMY16].

Asymmetric [DG12, XLM+12, XGLM14, XZLW15, ZWQ+11, CSS+13].

asymmetric-histogram [CSS+13].

asymptotic [DTZ12, TD14].

Asymptotically [LPS12].

Attack [ano15d, BSR17, BMS12, Bro17, CJP12, DSB15, FXP+17, zGZW12, GV14b, GDC16, HCET+12, HLZ15, JHL12, JKP12, LLW16, LGL+12, LJ17, LCLW17, LWKP12, LWPF12, MS2b, Pud12, SP13].
SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNST17, CJP15, DDFR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYH14, LWKP14, MBB11, MNP12, NZL+15, SB17, SXL16, WYL13. **attacker** [PLGMCdF18].

**Attackers** [BL15]. **Attacks** [ARP12, Ano17e, BGK12, BFK16, BKBK14, Che15, CMA14, DG15, DHLAW10, DHB16, EWS14, GPT14, HLLG18, Hay13, HRS16, JW+17, KGR10, LLC11, LWZ2, LWC14, LCL17b, MD12b, PNP13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SGG15, WW14, WHN+12, XNG+14, YL17, YCM+13, ZLQ15, AATM18, BBBP13, BVIB12, BSR+14, CGH17, dCCS12, DCAT12, DJL+12, DK17, Dra16, EA12, FIT+10, FIO15, GPP+16, GN11a, KPS10, LW11, NDNN13, OF12, PXL13, SIS16, TY16b, TLL13, VSI11, WWB14, XW12].

**attempt** [Fel13]. **attestation** [FQZF18].

**ATtiny** [EG+12]. **Attribute** [AAC+16, AHL+12, BFK+10, Boy13, CD16, CD18, FHR14, GZZ+13, GSW+16, Gli12, GVW15, HSMY12, Her14, KGP12, LW11b, LW11c, LW12, LJLC12, LLY+13, LLL+14, LAL+15, LL15, LW16, OT12, PPA18, PB2, RVH+16, Rao17, SSSW12, TMY+17, WDC18, WLH15, WHL16, XMLC13, XWL16, XHH+17, ZPM+15, ZQQ15, ZZM17, ZHW15, CPPT18, FNWL18, HZL18, HZWW18, HYS18, HKK13, JSMG18, LCL+15, LFZ+17, LFW15, LLY15, LLYW+17, LJJW18, QRR+18, RD+17, XWS17, YCT15, ZWM14, ZML17].

**Attribute-Based** [AAC+16, BFK+10, Boy13, CD16, FHR14, GZZ+13, GSW+16, GVW15, HSMY12, LW11b, LW11c, LW12, LJLC12, LLY+13, LLL+14, LAL+15, LL15, LW16, PB12, RVH+16, Rao17, SSSW12, TMY+17, WDC18, WLH15, XMLC13, XWL16, XHH+17, ZPM+15, ZQQ15, ZZM17, AHL+12, CDL18, Her14, WHL16, CPPT18, HZL18, HYS18, HKHK13, JSMG18, LCL+15, LFZ+17, LFW15, LLY15, LLYW+17, LJJW18, QRR+18, RD17, XWS17, YCT15, ZML17]. **Attribute-Hiding** [OT12, ZWM14].

**Attributes** [CG12a, Yon11, LCL17a]. **Attributes** [CG12a, Yon11, LCL17a]. **Attribution** [XHC+12, FNP+15]. **Auction** [B10a, YJ14, MV12, Rab10].

**Auction** [B10a, YJ14, MV12, Rab10]. **Audience** [DTE17]. **Audio** [Ber18, DA12, FM15, GCK12, HGT15, KD12a, KD12b, LSL12b, NXH+17, TC10, gWpNyY+14, XNG+14, XNRG15, ZSI2, LSQ11a, SKEG14, yWpNyL11, YQH12]. **Audit** [YNR12b]. **Auditing** [LMD16, TCN+17, YYS+16, YXA+16]. **August** [AB10a, YJ14, MV12, Rab10].

**Austin** [IEE13]. **Authentic** [HLT+15, SZMK13]. **Authenticate** [HM12]. **Authenticated** [Al10a, B10a, B12, BDMLN16, CLI16, CLY14, CCS14, CRE+12, DS11, EAA12, ESS12, FVS17, FFL12, GT11, GL12, GZ12, HC12, HLI0a, HCL+14, HEC+12, KMY18, LH16, LH11b, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHKS14, MSU13, PTT16, Sar10b, Smi11b, Tan11, TW14, XLM+12, XHC+12, XGLM14, XZLW15, YS12, YW13, YRT+16, Yon12, ZPZ+16, ZHH16, AIB+16, CT13, FA14b, FIO15, GPN+12, GL+11, HPC12, HLI1, HPY10, ISC+16, LWS10, LHH11, LML+13, NCL13, Nos11, Nos14, PPTT15, PJP18, SMBA10, TCS14, TSO13, TK14, WZM12a, WZM12b, WTT12, XW14, XCL13, XWW+18, YC12, YZ+14, YZL+18, ZT16, XW18, ZG10, ZCC15]. **Authentication** [BS12, CHX13, GRL12, OKG+12, RPG12, WY12, ZCWS15, Cer18, LFGCCCRP14, PGL10]. **Authentication** [AS14, AAz+16, ACAT+15, AUM16, BL12, BCE+12, BCM12, BSSV12, BLY18, BKST18, BCD+12, BS17, BF11, Boy16, BK12, BSV12, CGCGPDMG12, CTC+15, CC14, CSH+18, CCW+10, CFF17, CJ13, CD12, CJP12, CHL13, DL15, DBPS12, DKPW12, DP12, FLH13, FR16, FMTR12,}
Avoidance

Authorization

Authentication

Autoblocking

Automata

Availability

Auxiliary-Input
aware
Aware [BWF16, LMS16, QLL17, YTH17, MG10, TDDQ18, Wan13, ZFH18].
Awareness [MSas12, Li10, MSas13].
axiomatic [AT10].
B [Tan12a]. B-Spline [Tan12a]. Back [KRM10, SKS18, YZLC12, Ran10].
Backdoor [Sch13, Fel13]. Backside [DDR16].
back [Cor14a]. backward [BM11].
Bacterial [KMS12, Li10, MSas13].
Bart [HM17, RY10]. BAF [YNR12a]. Bake [Boy16]. Balanced [YTP11], balancing [FXP12, Zha15a].
Balls [CW12b, LHF12]. base [MS12a, XSWC10].
Based [ADM12, AGW15, ASM12, AAC16, ABCL17, Ano11b, ASS15, AYS15, BWLA16, BL12, BBB16a, BSSV12, BHG12, BKPW12, BRT12, BHH15, BS13b, BFK10, Bon12, BSJ15, BKPJ12, BDH11, BCF14, CML15, CL16, CGMO14, CCM17, CSH18, CZLC12a, CZLC12b, CLHC12, CCZC13, CLY14, CZLC14, CST17, CGL12, CDD13, CGY13, CD12, Chi12, CK18, CD16, DSM14, DA12, DLZ16b, EM12, EKB16, FM15, FHH10b, FHR14, FZT14, FGM10, FVS17, FSX12b, FSX12c, FSX12a, GWWC15, GZ13, GSW16, GV14b, GI12, GY13, GDCC16, GV15, GJJ15, GJJ17, HZC12, HSMY12, HMS14, HL10a, HXZ15, HCPLSB12, HKL12, HG12, HMR12, HSA14, HPO15, HKR18, HGT15, HCL14, HL10, Hii13, HRS16, HBG17, HEC12, HP12, JTZ16, JJH12, JEA15, JKHeY12, KS18, KZG10, KK12, KKA15, Kha10, KLY12, KSY12, KPK12, KRB12, KAK18, KS15].
Based [LMGC17, LMG18, LTKP16, LSL12a, LSL12b, LW11b, LW11c, LW12, LH12, LIJC12, LYZ13, LHL14, LTH15, LLC15, LTZY16, LLZ17, LPL15, LSLW15, LAL15, LH11b, Lin15, LP12, LNZ13, LCCJ13, LWCJ14, LNX15, LHL15, LW16, LIO15, LGPRH14, LDB15, LD13, LSC12, LBR12, LLH18, MWZ12, MLO17, MEF012, MCD12, MV12, MD12b, MBC15, MKN13, MZ17b, MRS15, MS17b, MF16, MCF17, Mor12, MSKR17, MA17, Muf16, NC12, NXH17, NXB13, NLLJ12, NLY15, pNyWy14, OD10, PB12, PTT16, FYM15, PDNH15, PPS12b, PYS18, PG12, PAS13b, PNRC17, RVH16, RZZ15, RS16, Rao17, RR11, RDZ16, RVRC12, RW12, SSW12, Sar18a, SS13, Sen17, SJ12, SGP12, SP15b, SSA13, SRA17, SH15, SGH15, TB18, TK14, TWZ11, TW12, TZ12, T12, TTH15, TC10, VDB16, VGA15, Vle12, WY10, Wan10, WSS12, WgMW12].
Based [WYW13, Wan14, WZC18, yWxY18, WDC18, WJ15, WCL18, WT10b, WMS12, XNG14, XNR15, XX12, XM13, XQI11, Xio12, XG14, XWLJ16, XJW16, XJR17, XHZ17, YE12, YZLC12, YZX12, YGFL15, YTS12, Ye10, Ye14, YH16, YTH17, YYO15, Y17, YKNS12, YHK10, YMS11, YK11, YFK12, YCY12, ZPM15, ZJ11, ZXZ11, ZDL12, ZLH12, ZQ15, ZW16, ZYL16, ZNM17, ZPW16, ZWH15, ZVG16, ZPXX17, ZYM18, ZHL15, AMN18, AG16, AaBT16, AY14a, AHS14, AAT16, AA14, ASO14, AIA18, AKG13, ASVE13, A13, ATI10, AHL12, BS15, BDM18, BBP13, BGLD12, BAA13, BO13, BWR12, BW13, BWA13, BMM12, BC18, BB16b, BK12b, CPPT18, CML18, CFL13, CFY10, CCL11, CTL12, CLSW12, CG12b, CSZ11, CHX13, CSS13, CW14a, CTH13, CJP12, CJ15, CCG10, CTL13, Cho14, Con12, dCCSM12, Cra11,
CDL18, DSCS12, DZ14, DLN13, Dra16].

based [uHAN+18, EZ15, FH13, Far14, FA14a, FA14b, FIO15, FAY16, FHZW18, FNWL18, Gal13, GJ13, GMOGCCC15, GMRT+15, GKC11, GJMP15, GCSÁddP11, GMS11, GLL+18, HSH11, HT11, HGWW11, HSM13, HZC+14, HZL18, HF14a, HWDL16, HZWW17, HZWW18, HBBRNM+16, HLR11, Her14, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HUF18, HPY10, HKHK13, HCC10, Hwa11, IMB17, IM14, ISC+16, IB11, IA15, IOV+18, Jac16, JNUH17, JK13, JLT+12, JZS+10, JMW+16, JSMG18, KPP16, KK13, KM10a, KHMB13, KKG14, Kim11, KGO10, KL11, KSH18, LXYL12, LLZ+16, Lau12, LC10, LK14, LH10c, LZJX10, LNM+11, LMJC11, LK12, LXMW12, LKAT12, LLHS12, LNL13, LXL14, LCL+15, LZY+16, LFZ+17, LNK+18a, LW1K+16, LCT+14, LFWS15, LPdS10, Lin14a, LLY+12a, LW10, LSQ11a, LSQ11b, LW1K11, LW13b, LZX14, LPZJ15, LTL+15a, LYL15, LLY+15, LZW+17, LJWW18, LWW+10, LL16a, LW13c, LWY12, LY14, MCN+18].

Based-Encryption [ZHW15].

Bases [EVP10, TSH14, FES10].

Basing [Mat14, MN10].

Basis [BNA15, ERRMG15, CG12b, Har15, LLP+18, Tam15].

Batch [ZPXX17, AGHP14, CCG10].

batch-based [CCG10].

Batters [Chi13b].

battles [Ano15e, Ano16f, Sch15c].

Bay [Ano10, DDS12].

Bayes [McG11].

Bayesian [WYW+13, ZLW+17].

Be [DSM14, Par12a, YM16, AZH11, Ana14, Eve16, Ree15, RK11].

BeagleBone [Cri16].

Beat [LTKP16].

BECAN [LLZ+12].

Becomes [Bra13].

been [Ana14].

before [GST12, Goo12].

Beginning [Chu16].

Behavior [GSC17].

behavioral [HT11].

Behaviors [GAF+15].

Behind [Fre10].

Beijing [BYL10, Yan10].

Beissinger [Ayu12].

Belief [BT12].

Bell [JEA+15, QD16].

Benchmarked [MKAA17].

benchmarking [ZZKA17].

Benefit [HB14].

benefits [Wat14a].

Benford [AOT13].

Bessel [GJ13].

best [Cha13c].

Beth [CTHP13].

better [LCL+17a].

Between [KA18, LRWW14, SAKM16, CLM+12, HLR11, KPP16, Kim16, PBCC14, WDDW12].

Beyond [LST12, MJS13, TS16b, FNP+15, JR14].

BGP [SVG16].

BGV [GHPS12, GHPS13].

BGV-Style [GHPS12, GHPS13].

biased [LLP+18].

Biclique [BKR11, KDH13].

Bidirectional [GMNS15, GH12].

bifurcation [SE18].

Big [ML017, Mal13, MMS17b, PNRC17, YDY+16, ZLW+17, FS18, LSBN14, 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, MBF18, SA14].

**Binary-Ternary** [ADI11]. **Binding**
[HEC+12, ZLQ15]. **Bio**
[OK18, GPVdBR012]. **Bio-inspired**
[OK18, GPVdBR012]. **BioAura**
[MSKRJ17]. **biographical** [Maf16].

**Biometric**
[Alp18, ATI+10, BCTPL16, DWB12, JN12, KHMB13, LGM+16, May15, NGAuHQ16, Sar12, SKV12, Vet10, AHM+18, DMT12, GCSÀddP11, HT11, LK12, LTC+15a, MLBL12, Sar10a, Sar18a, SR10]. **biometric-based** [SR10]. **Biometrics**
[BW13, ERLM16, SP13, ZPW16, FHZW18, GM16, LXLY12, LH10c, LNM+11, LNK+18a, MRRT17, SS17].

**biosensor** [Kim16]. **Birkauser** [Sha10].

**Birthday**
[LST12, SXL16, Nac12]. **Birthday-Bound** [LST12]. **Bit**
[CG14a, GV14b, HG12, HS18, LJK17, LPO+17, NIS12, Ros11, YLL+12, APPVP15, KS11, KFL+10, MNN12, PLStU1E10, RH10, TWZ+12, VN17]. **Bit-Wise** [CG14a].

**BitCoding** [HS18]. **Bitcoin**
[ADMM16, BRS17, BKJ15, Bra15, Chi13b, HB14, HUR16, JSK+17, Mic16, Sir16, Tay17, TS16b, VVH17, WHJ17]. **Bitcoins** [MPJ+16]. **BitErrant** [Ano17a]. **Bits**
[BF12, LLL17, YCL17]. **Bitstream** [SMOP15]. **Bivariate**
[TZW11]. **Bivium** [EV10]. **BIX** [Maf16].

**Black**
[BR14, CPS16, HHP17, KOS16, KMO14, MSas13, JB11, Rja12, SS10b, DD13, SK14, YSC16, ZZ12, CR16]. **Black-Box**
[BR14, HHP17, KMO14, Rja12, SS10b, KOS16, MSas13, ZZ12]. **Blackbox**
[MSas12, SS12a]. **BLAKE**
[AMPH14, 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, HKB14, MO14, RSM15, RMG18, WLD11, yWpWyYPN13]. **Blindfold** [Nac16]. **Blindfolded** [Vai11]. **Blinding**
[CLHC12, KHHH14]. **Block**
[AMVZ12, BRS17, BSS+13, BFMT16, BDGH15, BC+12b, CPW12, DWWZ12, EGG+12, FXP+17, GLLSN12, GT12, GST12, GNL12, IS12, KR11, KWS+12, LWZ12, LJ17, LCLW17, LGLL12, LWKP12, LWPF12, MDCB12, MRTV12, OGK+15, PH12a, PRC12, Pud12, SG+12, SSA13, WW12, YCL17, ZSW+12, BNY14, Jeo13, KM11, LPZJ15, LC13, LHYH14, LWKP14, MNP12, MRS15, MRS18, PL16, Sar11, SKK10, TQL+14, Tan17a, WB12, WWBC14, ZSW+18a, JKP12]. **Block-Parallel**
[MDCB12]. **Block-Wise** [SSA13].

**Blockchain** [Hur16]. **blockcipher**
[CMMS17]. **Blockciphers** [LST12]. **Blocks**
[JSK+17, Bra15]. **Bloom** [ATKH+17].

**Blowfish** [KB10]. **BlueKrypt** [Gir15].

**Boardroom** [LHF12]. **Bodacious** [KM10c].

**Body**
[LZCK14, ASO14, PK18, LIK+17, SGJ+18]. **body-sensor** [ASO14]. bogus [XWDN12].

**Bonbe** [Bri11, Car10]. **Bonebrake**
[SS10c]. **Book**
[Ano15b, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kob10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12].

**Boolean**
[ACZ16, AS17, CW14a, DQFL12, FY11, LVLV11, WT13, YCC16].

**Boolean-based** [CW14a, YCC16].

**Bootstrapping** [BGV14, GM14]. **Border**
[LGM+16, ZTSR12]. **Bot**
[HB13]. **Botnet**
[NSA15]. **botnets** [HB13]. **Bottom**
[Smi11b]. **Bound** [LST12]. **Bounded**
[GV12, GJO+13, PDNH15, QQZ18, SS12a, ZYT13, IM14]. **bounding** [PY+18].

**Bounds** [Jia17, LJ15, SNJ11, SS10b, Sha10].

**Bouzefrane** [Ano15b]. **Box**
Branch [EPAG16], Branchless [RBS+17]
Brave [KM10c], Break [SD12, JB11]
Break [Ayu12, Win17], Breach [Mun17]
breakthrough [Ano17e], breathing [KM10c], Brave [CS14]
Brokering [LSR13], Breathing-Based [CSTH+18], Breton
[CCZC13], Bribery [WC12b], Bridging [LRVW14, TMGP13], Briggs [Bai12]
Bringing [Ano15c, OYHSB14], Britain [Ald11], Brit
ish [And13], Broadcast [BS14, GMV17, HMR14, KH10, LMG17, LMG+18, FSM17, PPS12a, WQZ+16, XJW+16, ZHW15, CPPT18, DLN13, WYYY11, XWDN12, YM13, NZQ+11, ZZ12, ZHU13], Broadcasting [OO12, MK11, OCGG11, YY11], broke [Bai10, Hea15], Broken [MDAB10], Broker [TKR14], Broker-Less [TKR14], browser [GIJ+12], browsers [Ree15], Bruce [Sev16]
Brute [CJP12, JR14, CJP15], Brute-Force [JR14, CJP12, CJP15], BRW [CMRH13], BTC [CFL11], BTC-compressed [CFL11], Buchwald [ABJ13], Bucket [KVK10], Bug [Chi13b], Building [BPS16, KMP+11, MJS13, Sev16, WL11, LKJB12], Burdens [Bla12, SR14], Bus [AN17], Business [LDB+15], Buyer [Fral16, KJN+16], Buyer-Friendly [Fral16], BYOE [Tan17a], byte [Hof15, Hof16], bytes [PBCC14], Byzantine [KS11, LLKA19, YGK13], Byzantine-resistant [YGK13]

C [AD12, ACZ16, Cra14, DGJN14], C1G2 [MK12a], CA [ACM11, DUN12b, KIN11, Lin14b, Pie110, Rab10], CABA [MSKRJ17], CABE [XHH+17], Cache [AB15, ADR18, DKMR15, HLAZ13, SY15a, DJL+12, DK17], CacheAudit [DKMR15], Caches [LLGJ16, CDPLCA16, DJL+12], Caching [ADR18, HLAZ15], cackled [Bai12], CAD [PGLL10], Caernarvon [KMP+11], Calculus [MR10, JONIS+13], Calibrated [LC15], California [Ano10, JEE11b], Call [Ano16a, Ano16b, Ano16h, CR14, KMP+10], Call-Back [KMR+10], Calls [Mur16], cam [PKS18], Cambridge [ACM10, FJI2], Camellia [Blo10, LWP12, LWP12, LW14, SEH12], Camellia-192 [Blo15], cameras [MKH+12], Can [Alo12, AZH11, Bar15, DSSM14, YMI6, RK11, Rus15, Sto10, GMV17, LMS16], Canada [JY14, MV12], Cancellation [DLMM+18], Candidate [GGH+16a], candidates [ABM+12], canonical [Bai10a], CANS [HWG10, LT13], Can't [RAI15], CAOVerif [ABF+14], Capabilities [GFBF12, Lop15a], Capability [IA15, LLZ+17, LT13], Capability-Based [LLZ+17], Capacity [TODQ18, XNN15, YWW10, CLZ+17, GZHD12, PWLL13, WGLL13], Capacity-aware [TODQ18], Capacity-Raising [YWW10], CAPTCHA [OTO18, SEEK14], CAPTCHA-based [SEEK14], Capture [NYR+14], capturing [PKS18], Card [BDFK12, HMR12, HCL+14, PDT12, Ano17c, CLH13, GLC10, LNK13, Mar10b, Cho10, SD12], CARDIS [GLC10], Cards [BS15, LA10, PWVT12, WGMZ12, CHS11, HCC10, KY10, LH10c, LNM+11, LXM12, MM12, SGGCR+16, YZZ+14, YSL+10], care [FHV16], Carlo [CRI12], Carel [XIE12], Carry [GWM16], Carved [LC15], Cascade [WG18], Cascading [GT12], Case [Ano17c, DR11, SBS+12, SY15a, YL17, LK113, MD12a, SS17], Cash [YMWS11], Casting [CW12b], cat [Pow14], Catalog [AHS13], CBA [KMP+10], CCA
[AHS14, BWLA16, CZLC14, LTZY16, LSLW15, MSas12, PDNH15, SYL13, SLZ12, yYqWqZC13, ZY17a, ZSW+18b].

CCA-Secure [BWLA16, CZLC14, LTZY16, SYL13, yYqWqZC13, ZSW+18b]. CCA1 [MSas15]. CCA2 [Gal13, GV14b, LLW16, LLSW16, MVVR12, RG10, ZZ12, ZY17b].


Certificate-Based [GWCC15, HP12, LTH+15, WMS+12, YLZ+16, BJ+14, GLL+18, Lan13, LL16a, MBF+13, NPH+14, JB11].

Certificateless [CT18, GWCC15, IL15, LZC14, SJS14, TCL15, WMS+12, YT11a, YT11b, HPC12, JXLZ15, LL16a, SGJ+18, ZQWZ10, ZY17b]. Certificates [Mu16, SC12, GIJ+12, HREJ14].


Chosen-Ciphertext [RS10, FSGW12, LCT+14, GH12, LZC14]. Church [ABJ13]. CHURNs [RBNB15].
Cipher
[BW16, BFMT16, BCG+12b, CMLS15, CGCS12, DM18, DG12, DWZW12, Fis15, FXP+17, GLLSN12, GCS+13, HZ11, Hey17, IOM12, JPK12, KR11, KWS+12, LPS12, LWZ12, LJ17, LWPK12, LWPF12, MRTV12, MHC12, MS12b, OGK+15, PH12a, PRC12, WSSO12, WHN+12, YAG19, AMS+10, BNY14, CR12, HKT11, Hol12, Jeo13, KDH15, Lew10, LC13, LYHH14, LWPK14, 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, Kha10, LCLW17, LGLL12, LJ16, MD12b, NN12, Pud12, Sas12, SEHK12, Vua10, WH18, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bor10, Die12, KM10a, LWK11, MRT10, MH15, MY+18, QGGL13, SKK10, TQL+14, WB12].

Ciphertext
[BDPS12, CWWL12, zGXW12, HL12, JMG+16, JSMG18, KA17, LC12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RW12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWLJ16, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHIK13, KTT12, LCT+14, LFWS15, LZC14, QRW+18, RD17, SGM16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertext Policy
[Rao17, XMLC13, XWLJ16, ZHW15, JSMG18, LFWS15, QRW+18, XWS17, LAL+15, LHL15].

Ciphertexts
[Sa12, WQZ+16, AHL+12, LCT+14, NPM+13, WXYL+16].

Circle
[JC10].

Circuit
[Kar12, MTY11, XWS17, XWLJ16, Lau12, MS13a].

Circuit Size
[MTY11].

Circumventing
[BAG12].

CISSP
[STC11].

Citizen
[Ano16d].

City
[Ano17d, GAI+18, LN+18a].

Claims
[SKGY14].

Class
[BCG12a, SY15a, XYXX11, BJ16, Goo12, KK10].

Classes
[ACZ16].

Classical
[DSLB18, JEA+15, MS13, SU12, CR12, RK11].

Classification
[HPC10, HS18, KAHKB17, SG+12, ZLW+17, LHL+18].

Classifiers
[KGV16, LCM+17].

Cloud
[WZ12, TSL11, TS16a, WB12].

CLEFIA
[TSLL11].

CLEFIA-128
[TSLL11].

CLEFIA-type
[WB12].

Client
[ASM12, CTC+15, FD11, RAZS15, Vle12, FA14a, RA14b, hSSZ15, WT10a].

Client-Based
[ASM12].

Client-Centric
[Vle12].

Clouded
[FA14b, hSSZ15].

Cloud Manager
[SAR18b].

Cloud-aided
[SG+18, WLFX17].

Cloud-Based
[KS18, SRAA17, ASO14, BK12b, WC18].

Cloud-Manager-Based
[KKA15].
[CGCS12, DWB12, HPC10, KU12, KA18, ST14, HM10, LCM+17]. comparisons [Mid10]. compartmented [EZ15].

Compensated [GKS17]. Compensation [JSZ12]. Competition [JCPB+12].


Composition [LJS+14, NRZQ15, Ana14, AGH+17]. compound [BJ16, KPS10, jT12b].

Comprehensive [GSFT16, YFT17, Bul10a, KAS15]. compress [LC13]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16]. Compressed-Domain [WLZL12]. Compressibility [HN10].

Compression [CNT12, DA12, LD13, MAL10, PMZ13, PP10b, TCN+17, WHZ12, Ara13, CMMS17, DTZZ12, LK14, Li10, LPZJ15, PP11, QZ14, SI12].

compression-based [SI12].


Computable [LGH+17, FWS13].

Computation [ARH14, Ash14, Bee17, BDOZ11, Fri10b, GST12, GWV12, GHKL11, HP14, HC17, IEE11a, Jin10, KW14, KMO14, LHM+15, LQD+16, MMP14, Mal13, NSMS14, PST13, SVCV15, SZQ+17, TM18, Wat10, ABDP15, AB10b, LDDM12, PHGR16, TG12, vDKS11]. Computational [BCO13, GKS17, RD17, TBCB15, HRS13, SDM14].

Computations [ARM15, CK18, KHPP16, Nac16, ADMM16, BK12b, LR15, SSA11, TLMM13].

Compute [Vai12]. Computer [BGK12, BCGK12, BGB12, Bul10b, DF16, Gas13, IEE10, IEE11b, IEE13, LL15, Orm16, Ter11, Vau10, ABD13, DK12, FGP14, PHM10, Sta11b]. Computer-Aided [BGK12, BCGK12, BGB12, ABD13].

computers [Cop10b, LCKBJ12, Mac12, MV10, PHW10]. Computing [ACM10, ACM11, AJA16, Ano17c, BCG+12b, Cer14, CG+10, DXA14, EAA12, FES10, Gen10, KMS15, KP17, LCK11, LT14a, LYZ+13, LLC+15, LLGJ16, LNXY15, MLO16, OS16, Pet12, SJWH+17, SLM10, Vai11, Vie12, XMLC13, XWL16, YE12, YHL16, ZLCD15, AaBT16, AAZ+16, And13, CZZ15b, CSTR16, DKL+16, DWZ12, HSM13, HYS18, Joo13, JSMG18, KKA14, KKM+13, KKM+14, KSB+17, KH18, LXX+14, LYL15, LHL15, MSL2a, NR17, NCCG13, PPA18, PP11, PAK15, QZDJ16, QRW+18, Rao17, Tan12b, Wan18, XXX15, XYW+18, YHHM18, YWK+10a, YY11, ZWS+18, ZSW+18b, YXA+18].

conceal [EEAZ13]. Concept [TMC15]. Conceptual [PMZ12, SPM+13, TSH14].

Concrete [BS14]. Concurrent [CLP13a, FCM14, GJO+13, MKRM10, OOR+14, AKG13, SRB+12, XWZ16].

condition [TD14]. Conditional [HBCC13, KP13, LLG15, LSWL15, MLO17, XJW+16, FSGW11, FSGW12, HDWLJ16, HYF18, IOV+18, LCT+14, PZBF18, SKB+17, Tan12b]. Conditionally [ZJ14]. Conditions [Ano17d]. Conference [BC11, CGB+10, Che11, Cra12, Dan12, Dun12b, FBM12, GLIC10, IEE11a, JY14, LLA14].
LCK11, LW11a, LTW11, Lin14b, PJ12, SNJ11, Sahl13, Yan10, AB10a, Abe10, BYL10, BL10, Gil10, GG10, HWG10, Kia11, LH10a, Pei10, Rab10, vDKS11.

Confidential [HS11, AZPC14].

Confidentiality [BFK+10, HLLC11, OFMR16, SQZ+17, WDDW12, Bia12, CHX13, ZHT16].

Confidentiality-Preserving [OFMR16, SQZ+17].

Confined [BFK+10].

Configurable [CVG+13].

Configuration [Bis17].

Configurations [SS10b].

Congruence [VM14].

Conjecture [GV14a].

Conjunction [Kre13].

Consecutive [Tan12a].

Consensus [ABCL17, JSK+17, LLKA19].

Consequences [Eas17].

Consideration [CJP12, CJP15, KM10b].

Considerations [KD12b].

Considering [MLMSMG12].

Consistency [BCK17, SES+16].

Consolidated [KKA14].

Constant [App14, AEHS15, CWWL12, KOTY17, KHP16, KMO14, LP11, Pan14, ZM16, AHL+12, DWZ12, LCT+14, SGM16].

Constant-Round [KOTY17, KMO14, LP11].

Constant-Size [AEHS15, AHL+12, LCT+14, SGM16].

Constants [DWZ12].

Constrained [BS15, CSH+18, EAA12, JMG+16, YNR12a, Yon12, DM15, KAS15, LLZ+16, LCL+17a].

Constraints [CCMK16].

Construct [SGY11, WT13].

Constructed [Ye10, ZH15].

Constructing [CDSLY14, ZSW+12, HRV10].

Construction [BWLA16, DF11, EM12, FZT14, GWWC15, HHP17, KMO14, MSas12, Rog16, Sar10b, ST14, WZ15, WCL+18, WMS+12, XHX+17, LFZ+17, MSas13, SA14, YWL+17, YT11b, YKC+12, ZCLL14].

Constructions [BCF+14, DQFL12, HL10b, KOTY17, SNJ11, SES+16, CZ15a, CGKO11, NAL17, Zim10].

Constructive [Mau12, WB12].

Containing [XWDN12].

Contemporary [Opp11].

Content [ADR18, BCF14a, MHT+13, PMZ13, PZPS15, WHZ12, WZXL12, YT12, ZXX+11, GPN+12].

Content-based [MHT+13].

Contents [MM14b, SKS+18].

Consideration [Cra14].

Context [Fra16, ZCWS15].

Contextual [Svo14].

Continual [BKKV10, ZXY+12, YZ12, YCZY12].

Continual-Leakage [YZ12].

Continually [DLWW11].

Control [ATS15, BCF16, DHL10W, uHAN+18, FMNV14, MSKRJ17, PYP10, Sch15b, Yam12, ZY17a, ZYM18, PLGMCdF18].

Continuous-Tone [Yam12].

Contract [Men13].

Contrast [DDD14, GLW13, LW10a, MM14a].

Contributory [WQZ+16].

Control [ATS15, BFK+10, DLZ+16b, HHS+15, LGM+16, MM17, MK12b, NA10b, QZL+16a, RSN14, SGC14, TBCB15, XMLC13, YTH17, ACK+10, AMH10, CLH+16, CO11, Cra11, FNWL18, FS18, JAS+11, LCL+17a, LCL+15, NZM10, QCX18, Sch15c, SA15, Tan12b, Wan18, XHH12, ZML17, ZWS+18, ZFH+18].

Controllable [FH13, ZLDC15, ZHT16].

Controlled [FMTR12, WP17, Har16].

Controllers [AMH+16].

Controllers [CGH11].

Controversy [McG11].

Conundrum [Eve12].

Conversations [WBC+10].

Conversion [BJ10].

Convertible [CLL16, LH11b, HL11, LHH11, XWXC14].

Convolution [DWZ18].

Convolutional [MG15].

Cookies [DCAT12].

Cooperative [LLZ+12, SJWH+17, ZLDC15, WQZ+13].

Coordinate [YKK18].

Coppersmith [Dra16].

Coprocessor
coprocessors [GCVR17]. Copy
[YT12, MHT+13]. Copyright [SJ12, GJ13].
Core [LB13, YWF18, YS15, RS17, HLYS14].
cornerstone [Tan17b]. Correct
[PST13, Lan11]. CorrectDB [BS13a].
correcting [ATI10, LIT10, 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]. Core
[LB13, YWF18, YS15, RS17, HLYS14].
cornerstone [Tan17b]. Correct
[PST13, Lan11]. CorrectDB [BS13a].
correcting [ATI10, LIT10, 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]. corrections
[Sar14]. Correspondence [SY14].
corresponding [DWZ12]. Corrigendum
[HYS18, WZM12a]. cosmography [Pett11].
Cost [ABC+17, AMH+16, CMSL15, CPJ12, GI12, HLT+15, Man13, NVM+17, WMX+17, CZ14, CPJ15, LEW19, Sar10a, YL11].
Cost-Eective [HLT+15, WMX+17].
Costs [KHPP16].
couldn't [Bha16]. Countdown [Zet14].
Counter [ARP12, Fay16].
Counterexample [KPW13]. Counterfeit
[YFT17]. Counterfeiting [Ano16e].
counterfeits [GSN+16]. Countermeasure
[BBB+16a, MD12b]. Countermeasures
[BGN17, EWS14, FPZS15, DK17, FAA+18].
counting [LILY+12a]. Coupling [SMS14].
cover [UUN13]. Covert [EPAG16, JTZ+16, NSA15, LT13, LyWSZ10, SRB+12].
CovertBand [NTKG17]. Cozzens
[Led16, Sch15a]. CP [TY16a, YMC+17].
CP-ABE [YM+17]. CPM [PYM+13].
CPs [QFZ18]. Crack [Fox13]. cracked
[Ano13b, McG11, McK12, Moo14].
Cracking [Gri15, GAS+16, War11].
crawlers [GPN+12]. CRC
[Ful10, Joh10, GMSW14]. CRC/Taylor
[Joh10]. Create [DFKC17]. creating
[OO16]. Creativity [WP15]. credential
[JM+16, KKM+13, XMHD13].
Credentials [CG12a, SSW12]. Credible
Crisis [OdH12]. Criteria [PYS18, ZZKA17].
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, ZXH16].
cross-matching [SS17]. Cross-Site
[DSB15]. Crossword [Mar10a]. Crypsis
[GSC17]. Cryptanalysis
[BW12, Bos10, CWP12, CGCS12, DG12, DGJ+15, Far14, GST13, Goo10, Han10, IOM12, Jec13, Kha10, KN10, KWS+12, LH10b, LNM+11, LJJ16, YL11].
Cryptanalyzing [LLL17, ZLW+12].
CryptDB [PRZB12]. Cryptic [Mar10a].
Crypto
[Goo12, Pf10, Rab10, SCPSN10a, SCPSN10b, SMS18, WL11, BSR+14, BG+13].
Crypto-steego [SMSK18]. Cryptoclub
[Ayu12]. Cryptocurrencies [JSK+17].
Cryptocurrency [BH15]. cryptograms
[Shy15]. Cryptographer
[Dun12b, Kha11, Pie10]. Cryptographers
[Ano16d, BPS16, Goo12]. Cryptographic
[Abe12, AMKA17, AD12, ARH+18, AMVZ12, App15, BMP12, BCGK12, BGB12, Bar15, BCM+15, BIKK14, BLS12, BDP11, BFCZ12, BDGH15, Bha12, BKL+13, BSJ15, BNA15, CCK12, CCKC16, CFE16, jCPB+12, CBL13, Cor14b, Des10b, DQFL12, DR11, Ess17, FKS+13, FY11, FLW12, Gir15, GM11, GLR10, GG11, Har16, HN10, HH+13, HST14, HSA14, IBM13b, JR13,
KOP12, LVV11, LLK18, Loc15, MVV12, MP12, MKA17, Mu16, MK12b, NIS13, NA10b, PTT16, PFS12, PS14, PJ12, RMP10, RSBGN12, Rja12, RBHP15, SK11, SEY14, SFKR15, Sch12, Sev16, SGI11, SP15b, SDM1+12, SR14, SOF12, TW12, Tom16, YZLC12, YNR12a, YNR12b, YS15, ABDP10, AY14a, ABB14, ABF14, ABC12, BFG14, CFL13, Cha13a, CFZ10, CR10, CP13, CLCZ10, Cra11, DQJ14, EBFK13, ESR14, GGH16b, Gil10, GLR13.

cryptographic [KSU13, KAS15, KKK16, LGKY10, MS13c, MMZ12, MM13, Mes15, MN10, NDNR13, OO18, Pal15, PLPW13, PSdo1+13, QZDJ16, SD10, WT13, WMX17, YSM14, Zim10, Sha10].

Cryptographic-Key [SK11].

Cryptographical [KU12].

Cryptographically [ADD10, BCGH11, BJL12, BKLS18, MC11, NDG17+, PLsvdLE10, SVC15, GCH15, HJM1+11, SA14]. Cryptography [ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, App14, AAB17, ACM17, ARM15, Bar12, BKG12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BLM17, BCF1+14, CNR14, CT18, CQF1H14, Cas10, CGMO14, Che17, CST1+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK15, DX14, DP17, DHLAW10, DF16, DKS12, DR11, Eis10, FPS12, Fe10, FSK10, FBM12, Fre10, GO17, GFBF12, G1+13, GPT12, GLW12, Ham17, Hes12, HG12, HKR1+18, JT12a, KM10c, KP10, KAK18, LSL12a, Lin17, LWL10b, LGKY12, LMMH14, LGH1+17, LWHS17, LPO+17, MO12, MSI10, Mau12, MR14c, Mic10b, MV12, MM17, NNA10, NS12, Orm16, PP10a, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16, Sen10, SS13, Sen17, SK12b, SA16a, Sim15a, SGS14, Sma16, Sta11a, Ste15a, VS16].

Cryptography [WWL1+14, WY12, Wes16, Yam12, Yan11, YTS12, YL17, ZZZCJ14, ZAC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBD13, Ano11a, ABW10, ACK1+10, BOB13, BV14, Ber14, BL14, BAB1+13, Blu12, BSR1+14, BS12, BB16b, CFR11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDBS14, DDD14, Day11, DD13, Dur15, Far14, GCVR17, Har15, HI15, HZW17, Hof16, IM14, JLT1+12, JY14, JU14, KK10, KGO10, Kre13, KSH18, Lan11, LLLL10, Lin14b, LWW10a, Lid12, LY14, MCN1+18, MS13b, MD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, Ry10, Sac14, Sah13, SK14, SSAF11, Sta11b, Sti11, Svo14, UK18, VDO14, VN17, WHJ17, WY12, YT11a, YSC16, YXA18, YDH1+15, YR11, ZWX1+18, vDKS11, Che11, LZX10, Nac12, Cou12, Ful10, Gas13, Low12]. Cryptography [Me10, Mur10, Ter11].

cryptography-based [BOB13].

Cryptography-Related [Cil11]. Cryptol [Lau12].

Cryptology [BC11, Bro11, Dun12b, LW11a, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPG14, Gil10, GG10, Kia11, LH10a, MZ1a, Pal16, Pie10, Rab10, HWG10, LTW11, Kob10].

Cryptomania [Gen13]. Cryptoprocessor [GV14b, SWM1+10]. Cryptosystem [CCT1+14, LHI10b, SWM1+10, BS15, Ch13a, Gal13, GV14a, GLB1+18, IB11, MM13, MG15, NZM10, SV10, yYqWqZC13, YY11].

Cryptosystems [ADD11, OTD10, PSM17, BNST17, FWS13, SA16b]. Csec [AD12]. CT [Dun12b, Kia11, Pie10]. CT-RSA [Dun12b, Kia11, Pie10]. Cube [MS12b].

Cubic [RW12, VM14]. Cuckoo [BHKN13]. CUDA [DLV16]. cultural [Mid10].

Culture [Bla12, SR14]. Currencies [TS16b]. Current [DP17, GKCI2, FPBG14].

Curse [GG11, HB14]. curvature [GJ13]. curvature-feature [GJ13]. Curve [AD11, ARM15, BJ10, GPT12, LGH1+17, LWHS17, PPH12, SG15, AMN18, BL14, BBB16b, Cho14, Far14, FWS13, IB11, KK10, Kre13, MCN1+18, MS13b, NZ10,

D [AP10, CG12b, DBPS12, DWWZ12, EAA16, GZHD12, KWS12+, LJ17, LJ15, MCD12b, MKH12, PGLL10, RS16, SGS14, SRK17+, WSSO12, YY14, YPR17]. D-Based [WSSO12]. D-PUF [SRK17+]. Dana [Ano10]. Dana-Fa [FMS12a]. Dao [FMS12a]. Daoism [FMS12a]. Darel [Xie12]. Darmstadt [FBM12, Sen10]. DASH [KCC17]. Data [Ano13c, ADF12, Bar12, BJL16, BCD12+, BJL12, BW12, BKLS18, CWL14, CMLS15, CCW10, CSV15, CCT14, CLW16, DDS12, Dan12, DR12, DMS16, DA12, DCA18, DLZ16b, EKB16, FMY15, FY15, FRS16, GTT11, HSM14, HLT15, HK14, IBM13a, KRDH13, KGV16, LLZ17, LWJC14, LLZ12+, LZC12b, MLO17, Mal13, MMS17b, MM14b, NNAM10, NR12, PD14, PSM17, PH12b, PNRC17, QZL16a, QZ18, RCP18, Rea16, RSN14, SAKM16, Sar10b, SMSK18, SP15b, SKH17, Sia12, SLM10, TCN17+, Tan15a, Vai12, VSV15, WZCC18, XNKG15, XWSW16, YDY16+, YMC17, ZSY16, ZPXX17, ZTL15, ZLW17+, AP10, ASO14, Ana14, Ano11a, Ara13, ADH17, ALL18, BTPLST15, BC18, BKV13, CDGC12, CLH16, CDF10, CDL18, DF10+, DTZ12, DRD11, ED17, FS18, Gen10, GLB18, GZS18, HSM13, HKW15, HMCK12, HH16, HYS18, HYF18, JHCC14, Kim16, KH18, KWH16, LSBN14, LT14b, LXK14+. data [LZY16+, LHL18, LFW15, LAL15, LCW16, LZC17, LLL18+, LL16a, LHA16+, MHKS14, OO18, OSSK16, QCX18, Sch15c, SYY17, SAR18b, SW17+, Tan17b, TMK11, TKMZ13, WLH13, WZLV13, WS14, XXX15, XWZ18, XFY18, YYS16, YXA16, YNX16, ZZKA17, ZMM10, ZYW13+, ZHT16, AEH17, HLYS14, Sch15c]. Data-Centric [DLZ16b]. Data-Classifiers [KGV16]. Data-Compression [DA12]. Data-Minimizing [BCD12+]. Data-Oriented [NNAM10]. Database [BTHJ12, SBV14, WCL18+, BL11, JHCC14, LW13a, PRZ12, Suc12, YXD18]. Databases [FCM14, HPC10, JKHeY12, BL11, JHCC14, LW13a, PRZ12, Suc12, YXD18].

data [LZY16+, LHL18, LFW15, LAL15, LCW16, LZC17, LLL18+, LL16a, LHA16+, MHKS14, OO18, OSSK16, QCX18, Sch15c, SYY17, SAR18b, SW17+, Tan17b, TMK11, TKMZ13, WLH13, WZLV13, WS14, XXX15, XWZ18, XFY18, YYS16, YXA16, YNX16, ZZKA17, ZMM10, ZYW13+, ZHT16, AEH17, HLYS14, Sch15c]. Data-Centric [DLZ16b]. Data-Classifiers [KGV16]. Data-Compression [DA12]. Data-Minimizing [BCD12+]. Data-Oriented [NNAM10]. Database [BTHJ12, SBV14, WCL18+, BL11, JHCC14, LW13a, PRZ12, Suc12, YXD18]. Databases [FCM14, HPC10, JKHeY12, Kaw15, RP12, WP17, GA11, JK13, LCY16+, SS17, TG12]. Dataset [SP13], datasets [LV10].

[DBPS12, GMNS15, Bax14, Bul10a].

Decomposition
[AGH+17, LSL12b, gWpNyY+14, BWA13].

Decompression [PP10b]. Decomposing [Tar10]. Decryption [Koh10]. Decrypting [CR12]. Decryption [AN12, KB10, PKTK12, FNWL18, LJW+17, LJYW18, SES+16, SM10a, SM10b, Wu6, ZSW+18b].

Dedicated [Lin17, Nac12]. Deductive [ABF+14]. Deduplication [QLL17, SKH17, YDY+16, KH18, SAR18b, ZFH+18].


Degeneracy [WH18]. Degradation [MMS+17a]. Degree [KA18].

degrees [MZ17a]. Delay [CCKM16, GMNS15, LBR12, JLT+12, WX13].

Delegatable [Z11]. Delegated [MZH15, TMC15]. Delegation [FMTR12, SSW12, XWLJ16, YZ12, YAM+15, JSMG18, NAL17, XWS17, ZWM14].


Demodulation [KOP12]. demonstrating [LHA+16]. demosaicking [HLC16].


derived [ZMM+10]. DES-like [CGCS12].

Description [WH18, PLGSS11]. Design [AMN18, Abe12, ARH+18, AIB+16, ADD10, AUMT16, Bel18, BKL+13, DHB16, DR11, FSK10, HSA14, JWJ+17, KPP16, KW14, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QLL17, RYF+13, Sch13, SAAB10, SZDL14, VKPI17, WKB16, ZXH16, CZ14, Gor10, KHF10, KDW+17, MNW15, MAK+12, MHY+18, ZYC+17].

Designated [WHJ17, HYWS11, RPSL10, SY15b].

Designated-verifier [WHJ17].

Designation [Che15, LSQL18]. designed [Goo12]. Designer [KMY18]. Designing [CDK+10, FLW12, MRT10, PSD15, SR10].


detectability [LRW17]. Detectable [ESS17].

Detecting [BKBK14, Ess17, GAS+16, HLW12, KW14, SH15, YSC+15, LWLW11]. Detection [AMKA17, ATS15, DSB15, DF11, GZH17, HDWH12, KU14, LGL+12, LC15, MKR10, MKAA17, NDC+13, NSM14, SAJL16, SBV14, SP15a, SRAA17, SGS14, TM18, YFT17, AOT13, BM13, HB13, JC13, KLC+10, Maz13, MHT+13, YL13].

Detective [Cho10]. Detector [LTGP16]. Detector-Based [LTGP16]. Determine [FSWF11, Sto12]. Determining [NN12].

Deterministic [MPRS12, N12, XXZ12, DTZZ12].

Deterring [WGT10]. DEUCE [YNQ15].

Developed [Har16]. Developing [CH11].

Development [Pau10]. Developments [GCK12, Vai11].

Device [ABCL17, CFXY17, DKFC17, KLM+12, SRK+17, TYY+12, GM16, KKG14, Kim16, Par12b, HHH12].

Devices [AAC+16, CS+18, DLW11, EGG+12, GPT12, GdM16, GMSV14, HHH+13, HDWH12, JMG+16, LWHS17, MFG16, ZM17].
Difference [BS14, YTP11, JK13]. Differencing [LyWZZ12, YWW10].
Different [GZ12, HHH+13, KU12, AKK+17, ABW10].
Differential [BMS12, BNY14, CPW12, CGCS12, ESS15, FXP+17, KWS+12, LGL+12, LJ16, LJ15, 
LYHH14, MRTV12, PH12a, QGGL13, RCP+18, Sun11, WHN+12, Blo15, DDFR13, LLLK10, MNP12, PBCC14, SDM10, SDM14, 
TSL11, TS16a, WYL14]. Differentials [WW12]. Differing [GGHW17].
DigiNotar [JB11]. digit [KWH16]. Digital [AYS15, BBC+13, BM13, BCP14a, FMS12a, 
GP17, HPO+15, Jin10, Jhl16, Lzc12, MBF+13, MSI10, MNN12, NC12, 
PnyWyy14, Orm16, PH12b, PAS13b, SAA15, SM13, SC12, SOS15, TC11, TS16b, 
Yon11, Y+17, YLS12, dRSdiVCI12, AGHP14, BPP10, CCG10, FLZ+12, Fri10a, GMS11, 
Har14, KM11, Lan13, LWG10, MS13b, MM14a, MO14, QCX18, Sim15b, SLM10, 
yWpNyL11, ZZZ17, Zet14, ZS18, Aio13a, Aio15b, Mou15]. Dilly [Bat10].
Dimensional [Ano17d, Lcz12b, XYX+11, DWZ12, QD16]. dimensions [Pal15]. direct [GH12]. Directed 
[NN12, KPS10]. Direction [NS12]. Directions [BKBK14, DDFZ16, Hof16, PPA18].
Directly [LZC12a]. directory [SMB10].
disabled [HFT16]. disassociation [TML12]. Disaster [NRRQ15, BBG+17].
disclosure [DZS+12, PAK15, SB17, WGT10].
discovery [Ano11a]. Discrete [BGJT14, CLL16, HKR+18, KLM+12, Xie12, AMORH13, BGJT13, MM31, Mes15, 
TLP16, VM14]. discrimination [GPVcdBO12]. Discriminative [Y14].
Discussion [Gli12, Wil18, Bul10a].
Discussions [KD12b]. Disk [GM14, Ran16].
Disks [Mar10c]. disparate [SSY12].
Dispatching [YT17]. dispersed [ED19].
Disreputable [ABJ13]. Disruption [HK14]. Disruption-Tolerant [HK14].
Dissection [Don12a]. Dissent [SGW+14].
Distance [PY+18]. Distillation [BJ16].
Distinguisher [DWW12, AMS+10].
Distinguishers [SEHK12, ZSW+12, AY14b, AP11].
Distinguishing [KM10a]. Distortion 
[FHS13, Jia17, LGWY12, MM17].
Distortions [WZL12]. Distributed [Ano10, BKBK14, BCB15, CGB+10, 
FCM14, HSM14, HXC+11, HCL+14, LMD16, 
LL15, LN+13, LWJ14, YZX+12, YKL12, 
ZLDC15, BLV17, CSTR16, dCCSB+16, 
GAI+18, NCCG13, TG12, XW13].
Distributed-Healthcare [ZLDC15].
Distributing [Küp13, MS16]. Distribution 
[EEA+16, JEA+15, Lop15b, MSU13, 
NNA10, SK11, SNJ11, TC10, ABB+14, 
BB14, BGP+17, CML16, FHZW18, JSK+16, 
JLT+12, LLP+18, NACL12, YWL+17, 
YHHS16, YL11, ZWS+18]. dithered
[UUN13]. Diversity [ZTL15]. Division
[SS12b, MN14]. Divisors [CN12]. Divulges 
[ABJ13]. DLSef [PNRC17]. Dmail
[CSC14]. DNA [AEH17, HEK18, WGA+12].
DNP3 [ACF16]. DNS [HLAZ15]. Do
[Bow11]. doc [NN15]. Document
BTHJ12, BPP10, DBPS12].
Efficient [ABBD13, ASBdS16, BWLA16, BCGH11, BHG12, BV11, BV14, CG12a, CML+18, CMLRHS13, CWWL12, CJ13, DWB12, Dun12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTP+12, GPT12, GJJ15, GH12, GZH17, GCH15, HZC+12, HZC+14, HZL18, HZL10b, HBCC13, HZX15, HXL12, HYL12, HZH17, HCDM12, HH16, HC17, IA10, KPC+11, Kim15, KHP+16, KH10, LL+18, LDDAM12, LZT12, LXK+14, LCLL15, LSLW15, LHYZ12, LWHS17, LZC17, LBOX12, MX13, MTY11, MVVR12, MU12, MP12, MC11, MN14, NES+14, NdMMW16, NZ10, PB12, PAF18, PRC12, PG12, PCPK+14, PNRC17, RBHP15, SGY11, SZS14, SG16, TLCF16, TWZ11, TT12, TM18, WCCH18, XLZ16, XMCL13, YHL16, YNH12a, YNY12b, YLW13, YNQ15, YLA+13, YS15, ZQWZ10, ZHZ+12, ZSW+12, ZJX+14, ZXYL16, ZL+19, ZP16, ZHW15, AZPC14, AZT+12, CH11, CCSW11, CLHJ13, CZ14, Cho14].
efficient [Cra11, CGKO11, EA12, FLL+14, Far14, FA14a, FA14b, FIO15, FNWL18, GH16, GLM+11, HPC12, HYS18, ISC+16, IB11, IOV+18, JCHS16, JZS+10, KKG14, KL11, KSH18, LLLS13, LH11a, LH10c, LXMW12, LAL+15, MLM16, Mes+15, Nov10, OCGD11, PBF18, PC14, Rao17, SMK13, TLL12, Tso13, TKHK14, VN17, WYL13, WLZ+16, WT10a, WXK+17, XWZW16, yYqWqZC13, ZLY10, ZZ11, ZCZL14, ZTLZ16, ZCZ15, Zhu13, LL+12, TCL15].
Efficiently [FWS13, LGH+17, SLY+16].
Effort [RSBG12].
Effort-Release [RSBG12].
EGHR [CML+18].
eHealth [TMGP13].
eID [SgGrCr+16].
eight [Sun11].
eight-round [Sun11].
Einführung [Buc10].
Einstein [HR13, Wes15].
Elbirt [Bar12].
Election [Ess17, TKM12].
elections [QS18].
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, PPH12, SG15, AMN18, BAAS13, BL14, BBB16b, Cho14, Far14, IB11, KK10, MCN+18, MS13b, NZ10, SH15, WH17].
ELmD [BDML16].
Elsevier [Ano15b].
Email [Bel16, CCS14, XJW+16, WRL15].
Embedded [AB15, BS12, BJCHA17, CFXY17, HC17, JW+17, LWHS17, SG15, SK12b, SDM+12, WXY+17, YGD+17, YS15, Ano11a, CVG+13, Eis10, MFH13, XZW16].
Embedding [KD12a, MCDB12, XNRC15, XZ18, YR12, EA11, MKH+12, PWL13].
Embeddings [FHS13].
Emergable [YT12].
emerged [McG11].
Emergence [LMB12].
Emergency [HLKL15, YTH17, KLC+10].
Emerging [BSV12, KSA16, OS16, FPBG14, ZHZ+17].
Empirical [gWpNyY+14, EBFK13, Sar14].
Employees [Mor12].
EMV [Cho10].
Enable [SMS14].
Enabled [GPT12, HFT16, QZL+16a, QZL+16b, SG16, SSPC12, BMM12, TODQ18].
Enabled/disabled [HFT16].
Enables [IBM13a].
Enabling [FRS+16, JSM+18, SYY12, WPZM16, YYS+16, Sch12b].
eNB [CLM+12].
Enciphering [CMLRHS13, HMR12, MLCH10, Sar11].
Enclaves [WBA17].
Encoded [DG17, HS18].
Encoding [BR14, CK18, SK12a, TJZF12, XHZ+17, PC14, Sun16].
Encounter [NA10a].
Encrypt [RAZ15, Ran14].
Encrypted [ADR18, BTHJ12, CWL+14, CWL16, Cor14a, DWB12, DCA18, FCM14, FRS+16, Gen13, GLG12, GZH17, HZTR12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kav15, KGV16, LA15, LQD+16, Lop12, Mur16, NBZP17, NNAM10, QLL17, SAKM16, Sia12, TM18, Vai12, WBC+10, XWSW16, YDY+16, ZCE16].
ZDL12, ZXYL16, ZVGL6, ZLW+17, AHM+18, AZH11, BTPLST15, BGP+17, BKV13, BL11, CH1, Crl6, CDL18, DKL+16, DRD11, ED17, FTV+10, Gen10, GZS+18, HH16, KH18, LXX+14, LZY+16, LHL+18, LW13a, OSSK16, PRZB12, SEXY18, SWW+17, Suc12, TKMZ13, WR15, XWY+18, XDY18, ZLY10, ZFH18, ZHT16].

Encrypting [CC10, Mar10c, dRSdlVC12, LFGCGCRP14, Pow14].

Encryption [ADM12, AV12, AEH17, Alo12, AAC+16, Ano13c, Ano14, Ano15c, Ano17d, AKP12, ABF12, AS16, BVS+13, BWLA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12, BS14, BV18, Bla16, BKLS12, BDPS12, BHJP14, BDMLN16, Boy13, BV11, BV14, BVG14, CV14, CMO+16, CLL16, CWWL12, CN12, CFZ12, CLHC12, Che15, CGL+12, Chi2, Ch16, CRE+12, Con18, CNT12, CLW16, CD16, DR10, DN12, DFJ+10, DSB18, Des10b, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJH12, FFL12, Fuc11, GWWC15, GGH+16a, GGH17, GM13, GZZ+13, GSW+16, GH11a, GH11b, GHS12, GHP512, GDC16, GVW15, GM14, GL12, GKS17, Gue16, HSMY12, HLLG18, HZ11, HG12, HC17, HTC+15, HP12, IAD10, JLS12, JH12, Jia14a, JR14, Kam13, KB10, KME+12, KMY18, KTT12, KOS16, KKA15, KFOS12, KHP16].

Encryption [KS12, LGMC17, LGM+18, Laut17, Led16, LL16, LW11b, LW11c, LW12, LLJC12, LZY+13, LHL+14, LLC15, LTZ16, LLVM15, LH11b, LSQ18, LB13, LY15, LW16, LY+18, LLML12, LH18, MZH15, MLO17, MMP14, MR14a, MTY11, MSM18a, MVVR12, MSS17b, MRL+18, MFB18, MPRS12, MT12, MKRM10, MSas12, Nac16, NdMMW16, NTY12, NMS14, NAL17, OT12, OGK+15, PMZ13, PR12, PB12, PDNH15, Per13, PKTK12, PPS12a, PYS18, PMZ12, PCY+17, PRSV17, RH+16, RCP+18, RZZ+15, RSBGN12, RDZ+16, RVRSCM12, Saa12a, SSW12, Sar10b, Sch15a, SLGZ12, SZS14, Sch14, Sm11b, Sta12, SHG15, SMOP15, Tan11, TC+17, TCR15, TMC15, Tan17b, TDTD13, TRK14, TT12, Unr15, Vai11, VSR12, VOG15, Wal18, WHC+15, WP17, WDCL18, WSS12, Wat12, WLC12, WDDW12, WZ15, WWHL12, WMS+12, WQZ+16, XNKG15, XY18, XZ12, XJWW13, XWL16, XJW+16, XH+17].

Encryption [YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YK+11, YFK+12, YCZY12, YKKL12, ZOC10, ZPM+15, ZDL12, ZYT13, ZWTM15, ZQQ15, ZWM16, ZMM17, ZHW15, ZY17a, ZYM18, ZWS+18, AHS14, ATK+17, Ana14, Ana13b, Ana15e, Ana16f, ABR12, AMHJ10, ACD+15, APL+12, BAAS13, BC18, BG14, BSW12, BGP+17, CPPT18, CFVP16, CZ+10, CW14b, CLH+16, CMMS17, CZ15b, CM11, CM10, CW12a, CDF+10, CM13, CGKO11, DLZ16a, DDM17, DTZZ12, Eve12, Eve16, FAA+18, FH13, FSGW11, FSGW12, FMB+18, Fay16, GMOGCC15, GH13, GHP512, GLM+16, GH12, GLL+18, HG11, HZ14, HZL18, HWDL16, HZW18, HT13, HLR11, HL11, HFT16, HYS18, HYF18, HKHK13, JC16, Jia14b, JSGM18, JHCC14, JSM+18, Kam16, KHMB13, KKM+14, LLW16, LCL+17a, LCL+15, LFZ+17, LCT+14, LFW15, LD+10, LIH11, LW10, LW13b, LZC14, LPZJ15, LCT+16, LZC17, LJW+17, LJWY18, LLL+18, LL16a, LW13c.

encryption [LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSas13, NES+14, PPA18, Pet12, QRW+18, Ran16, RG10, RWZ13, RPSL10, RES+16, SE18, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sh13, SGFCRM+18, SLM10, SKB+17, Spa16, SGMM16, Tam15, TPL16, J12b, WGTJ10, WY10, WWY11, WHY+12, WDZL13, WFX17, Wan18, WQZ+12, WCCH18, XZW16, WX14, XSSC10, XXX15, WXS17, WQZ16, XWXC14, XSW16, XXX15, WXS17,
FOX [LJF16]. FPGA [AMKA17, BCE+10, BDGH15, CFZ+10, CHS15, GBF12, HF14b, MM14a, MAK+12, ZLQ15].


fractional [BW13, VM14]. Fragile [CHHW12, MCD12, SSA13, CCL11, PGLL10, WHZ12].

Fragile [CHHW12, MCDB12, SSA13, CCL11, PGLL10, WHZ12].

Fragmentation [BDPS12, CDFZ+10]. frame [FMB+18, YQH12]. Frames [DG17, IM14].

Framework [BJL16, CD12, DG17, HXC+11, KPC+16, LLG15, LSC+15, LY15, LQD+16, MSU13, SK11, SYC+17, TSH14, VKP17, ZJ14, ATKH+17, BHCDFR12, KKG+10, KM14, MMS+17a, MBF+13, PSO+13, PCLCGS11, PAK15, SD10, SA16b, SYW17, ZYC+17].

frameworks [LSBN14]. France [Kap11].

Francis [Joh10]. Francisco [SR14].

Frank [ABJ13, Joh10, Mar10a].

frankencerts [BJR+14]. Fraud [Ber12].

Fred [Xie12]. Free [App13, Boy16, IL15, TWZ+12, TTH+15, ZLH+12, ATKH11, ED19, LL16a, SA12, SE16, YTB11].

Free-View [TWZ+12]. FreeBSD [MBM15].

Freedom [Con18]. Freestart [SKP15].

French [Ant14]. Frequency [KAHK17, LTKP16, LWCJ14, TC10, CJP12, CJP15, EA12, NLYZ12].

Frequency-Based [LWCJ14]. Freshness [RBNB15]. Fresnelet [FMB+18]. Friendly [Fra16, KCC17, SD14, ACM12, KLB+16, RD17, WOLS12]. Freeside [DDR+16].

FSR [MD12b]. FSR-Based [MD12b].

Fugue [AP11]. Full [ALR13, HEC+12, LW12, VS16, WLC12, BK11, DDM17, LC13, RM16, SWW+17, SKP15, Tam15, TY16b]. full-hiding [DDM17]. full-text [SWW+17]. Fully [AKP12, BV11, BV14, BVG14, CMG+16, CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, LMGC17, LSLW15, LSC12, MV12, MSM18a, Nac16, NCCG13, PB12, SGH15, Vai11, WHC+15, XWZ+18, ZZ12, GH13, ZXJ+14, ZML17].

Fully-Homomorphic [GH11b].

Fully-Homomorphic-Encryption [CN12].

Fun [APPV15]. Function [AMPH14, Bee17, BKST18, FLS+10, LyWZ12, MMS17b, SGY11, WSSO12, AYY13, AY11, CMMS17, HK14, LP11, RS14, SAR11, SXL16, TQL+14, WYW14].

Functional [AS16, BV18, BW12, Boy13, GGH+16a, GGV12, LQD+16, MV12, Rus15, Wat12, ZYT13, ZWMT15, ZWM14].

Functionality [JL13]. Functions [ALR13, BBC+14, BIKK14, BKPW12, BK12a, CPS16, DMM14, DQFL12, FY11, LVV11, NR12, Rja12, RW12, SMS14, SLY+16, Tan12a, YP11, AY14a, BDP11, CG12b, CQX18, CW12a, ESR14, Gen10, HRV10, Li10, QDZJ16, WT13].

Fundamentals [JL13]. Further [HCL+14, WHY+12]. Fus [FMS12a].

Fusion [ABCL17]. Future [AYS15, BCE+12, BKBK14, Bon12, CDFZ16, GCK12, HYS18, Mon13, Aro13d, FPBG14, Mac12, PPA18, PHWM10, MJS13].

Future-proof [Mon13]. Fuzzy [KRDH13, NC12, SH11, XJWW13, Alp18, KBM13, MMS13, SM11, SN14].

FV [MRL+18].


Gateway-oriented \cite{WZM12a,WZM12b}. Gaussian \cite{HKR+18,YWL+17}. GCD \cite{KI11}. GCHQ \cite{Ald11}. GCM \cite{SKK10}. GCM/GMAC \cite{SKK10}. GDLP \cite{MMZ12}. Gear \cite{AHS13}. Geckos \cite{GSC17}. geese \cite{Bai12}. GenePrint \cite{HQY+16}. Gener \cite{HYS18}. General \cite{FJHJ12,GFBF12,Gue16,HP12,KOTY17,LPL15,PB12,SJWH+17,YFF12,ABDP15,Bai12,DGJN14,HQZH14,LWS10,WS12,YC11,ZYC+17}. General-Purpose \cite{Gue16,ABDP15,DGJN14}. Generalisation \cite{LR15}. Generalised \cite{Hes12}. Generalization \cite{GMNS15}. Generalized \cite{BFMT16,LPL15,PC14,TY16b,Ye14,ZAC17,ADG16,BNST15,CLZ+17,GMRT15,HQY16,YMSH10}. Generated \cite{ADD10,AGHP14,LW13b}. Generating \cite{Ano16e}. Generation \cite{ABS+12,BCGH11,HTC+15,BM14,MR14a,MJGS12,NKWF14,PLSvdLE10,SRK17,TH15,YC11,ZYC+17}. Generators \cite{AS17,DSL18,LTTP16,MGF16,NIS12,ST15}. Generic \cite{BWLA16,BR14,Chi16,GWWC15,HXC+11,Sar10b,SY15a,ZAC17,ZCL14,HQY16,YT11b}. generically \cite{MHKS14}. Genetic \cite{JK13,MM17,ASVE13,EEAZ13,PTK14}. genius \cite{Hai17}. Genomic \cite{BKLS18,RC+18}. Gentry \cite{GH11b}. Genuine \cite{HR13}. genus \cite{FWS13}. geo \cite{Har14}. geo-location \cite{Har14}. geodesics \cite{ZZCJ14}. Geographic \cite{LC17}. Geolocation \cite{FPY15}. Geometric \cite{DSB16,GTT11,WTZ12,YWNN15,CLZ+17,GZHD12}. Geometrically \cite{WYW+13}. Geometry \cite{tWmC12,C11,CLZ15a}. German \cite{BDFK12,Bl12,Buc10,Cop10a}. Germany \cite{FBM12,GLIC10,Sen10,Wat10}. Gesture \cite{LCL17b}. Gestures \cite{AUMT16,GCSAddP11}. Get \cite{GPT14,Sch11}. Getting \cite{ESS15}. GGH \cite{LH10b}. Ghost \cite{CDA14}. GHZ \cite{CCL+13}. GHZ-State \cite{CCL+13}. giant \cite{Joh15}. girls \cite{Mun17}. Girod \cite{GMNS15}. GLARM \cite{LLZ+16}. glimpse \cite{Mic10a}. Global \cite{CLP13a,CLH13}. Globally \cite{CCS14}. Glyph \cite{XZZ18}. GMAC \cite{SKK10}. Goal \cite{BMP12}. Goal-Driven \cite{BMP12}. Goes \cite{BCD+12,RY10}. Goldreich \cite{Lin17}. Goldstrike \cite{BH15}. Goliath \cite{Sch15c}. Gong \cite{LLW16}. Good \cite{DFQF12,FY11,LBSN14,SA14,W13}. goodbye \cite{HU15}. Google \cite{Har14,Loe15,VG14}. Goppa \cite{MBR15}. Gordon \cite{GW14}. GOST \cite{CL13,WYW14}. Government \cite{Ano15e}. GPG \cite{Ran14}. GPGPU \cite{RVRSCM12}. GPGPUs \cite{LFC16}. GPU \cite{BCGH11,GCH15,HBBRM+16,HJCC14,MB11,ZOC10}. GPUs \cite{VKP17}. Graded \cite{BR14}. grain \cite{Wat15,Mic10a}. Grain \cite{BMS12,FSGW11}. Grained \cite{CDD13,YTH17,ZML17}. Graph \cite{ATS15,GT11,W18,GMP15}. graph-based \cite{GMMP15}. graphical \cite{SKH15}. Graphical \cite{BCV12,CTL12,LT15}. graphical-based \cite{CTL12}. Graphics \cite{HHMK14,ABDP15,KY10,PGL10}. Graphs \cite{FBM12,KU12}. Gray \cite{DA10,NN12,RY10,SA14}. Gray-Level \cite{DA10}. great \cite{Acz11}. green \cite{DCSS+16}. Grey \cite{LW13}. Grey-box \cite{LRW13}. Grid \cite{CGB+10,DLZ+16,K15,LPL15,AMN18,JAS+11,MCN+18,WS12,Y11}. Grid-Based \cite{LPL15}. Grids \cite{SC10,CT11b,GLW13,SHY15}. Gröbner \cite{EVP10,FES10,TAM15}. Gro
[Dan12]. Ground [KP17]. Group [AEHS15, BSV12, CGY+13, CLW16, DT13, FVS17, HL10a, Har13, LLZ+16, LCCJ13, TW14, XLM+12, XGLM14, XZW15, ZHX16, AKK+17, CML+18, GBNM11, HCCC11, HPY10, IOV+18, LLLS13, LWS10, RS15, WDZL13, WTT12, YZL+18, ZZKA17, ZWQ+11]. Group-based [LLZ+16, CML+18]. group-key [IOV+18].

Grouping [LNZ+13]. Grouping-Proofs-Based [LNZ+13].

Groups [Abe12, GZ12, XNKG15, YS12, YKNS12, MZ17a, WQZ+13, ZZ15]. GRS [TD14]. GSR [LC17]. Guangdong [IEE11a]. Guaranteed [TBCB15].


Hamming [CCL11, KSSY12]. Hand [SR12a, Cho10]. hand-held [Cho10].

Handauth [HBBC13]. Handbook [Bee17, AB10b].

Handoff [HZC+12, HZC+14, XCH14, ZBR11, ZCLL14]. Handover [HBCC13, LBR12, CLM+12, CML+18, HZW17, QMW17, YHL16, YHHS16, YLS12]. Hands [GPT14, BSS11]. hands-on [BSS11].


Hans [Mur10]. haptic [ASVE13]. Hard [KPC+11, Mar10c, ZWTM15, RPG12].

Hard-to-Invert [ZWTM15]. Hardcover [Joh10]. Harder [KTA12, Sch16]. Hardness [BHKN13, SS13]. Hardware [AW17, BRPB13, BDMLN16, BJCHA17, CMLRHS13, DOS15, ERRMG15, GP17, GCVR17, GCS+13, HKL+14, HG12, HSA14, HC17, HLN+10, KAK18, LGH+17, LLKA19, LRVW14, MLCH10, MCS+15, MRL+18, MHY+18, NDC+13, NdMMW16, PC16, PG12, RMP10, SN10, Set16, Tay17, WOLP15, ZAG19, AMN18, BDM18, BGG+13, KHF10, MD12a, NS10, Nov10]. Hardware-Assisted [LLKA19]. Hardware-Based [HLN+10]. Hardware-Enforced [Set16].

Hardware-Intrinsic [SN10, NS10]. Hardware/Software [MRL+18]. hardwares [SKH15]. Hardy [Xie12].

Harmonic [YWNW15]. Harnessing [DFKC17]. Harvesting [ABC+17, ZGC16].

HAS-160 [WLC12]. Hash [Ano12, AMPH14, BHH+15, BKST18, BK12a, CLP13a, jCPB+12, CZLC12a, CZLC12b, CZLC14, CJP12, EAA+16, FLS+10, GI12, HCPLSB12, Hüll13, HRS16, HBG+17, MCF+16, MCF17, MKAA17, NTY12, NR12, NXB13, PTTT16, Rja12, SGY11, WSSO12, ZZM17, AY14a, AKY13, AP11, CJP15, ESRI14, KKG17, PP16, RS14, SPLHC14, SX1L16, WW14].

Hash-Based [BHH+15, GI12, HCPLSB12, Hüll13, HRS16, HBG+17, MCF+16, MCF17, MKAA17, NXB13, CJP12, CJP15, PP16, SPLHC14]. Hashing [AAE+14, ASbS16, BHHN13, BKL+13, Kaw15, CP13]. Haskell [Rus15].

hatching [WYK12]. HB [SHH11, PYH+18].

HDH [PDHN15]. Headline [YGF15].

Health [LYZ+13, LHL15, Rao17, ZVG16, BC18, IC17, WMX+17, YZL+18, JKL+16].

Healthcare [BN14, HLKL15, ZLDC15, ASO14, Kim16].
HVS [RMG18]. HWMP [BOB13]. Hybrid [ADI11, ARM15, KBL11, KKA15, LP12, NGAuHQ16, OO12, Per13, XWLJ16, EEAZ13, KP18, WXYL16, WS14, XWS17, BOB13]. Hybrid-Double [ARM15]. hybrid-indexed [WXYL16]. hybridization [MSM13]. Hyderabad [GG10]. Hyper [BL14, WGZ+12]. Hyper-and-elliptic-curve [BL14]. hyper-chaotic [WGZ+12]. Hyperchaotic [GMOGCCC15]. hyperelliptic [FWS13, Kre13]. hypergeometric [YL11]. i-NVMM [CS11]. I/O [CDD13]. i2b2 [RCP+18]. IB [CZLC14]. IBC [BOB13]. IBC-HWMP [BOB13]. IBC [ABC+12, ACD+15, BAB+13, HKL+14, JSM+18]. ICA [tWmC12]. ICICTA [IEE11a]. ICISC [LH10a]. ICs [GSFT16]. ID [Ano17c, CTL13, CDPLCA16, EZ15, HCC10, IB11, KGO10, LMGC17, LY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, TPL16, TT12, TTH15, Wan18, WT10b, WTT12]. ID-based [MM12, LMGC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WTT12]. ID-card [Ano17c]. ID2S [YRT+16]. IDEA [BNY14]. Ideal [LPO+17, WCL+18, HKT11, yQyWqZC13]. idealness [TD14]. ideas [Mac12]. idempotent [Dur15]. Identical [Bow11]. Identifiable [Oba11]. Identification [FSX12b, FSX12c, FSX12a, VGA15, YGFL15, YKK18, AGLW16, CTPH13, CJP12, CJP15, EA12, HQY+16, KII1, KL13, NLYZ12, YTM+14]. identified [AZH11]. identifier [JS13]. identifiers [Cer18]. Identifying [CSV15, SVG16, ZCWS15]. identities [GLM+11]. Identity [AQD12, ASM12, ASVE13, Ano15b, ACAT+15, ASS15, BWLA16, BC1F16, BHG12, BKPW12, BDFK12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CZLC12a, CZLC12b, CLHC12, CZLC14, CGL+12, CGY+13, Chi12, dCCSM+12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, GOPB12, CY13, GDC16, GJJ15, GJZ17, HZC+12, HvS12, HSM13, HSM14, HZX14, HYWS11, HYF18, KKA14, KRB12, Kaz11, LMG+18, LMB12, LSL12a, LKAT12, LXJ14, LCC+15, LTZY16, LSLW15, LH11b, LSC12, LBR12, MLO17, MBF+13, MGSP12, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, Ser12, SSC12, SKGY14, SWW+16, SGH15, TRK14, Tin15, TH16, TMGP13, Vle12, WV10, Wan14, XXZ12, XQL11, XJW+16, YXZ+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCZY12, ZLH+12, ZMW16, ZDW+16, ZPXX17, ZYM18, ZTSR12, ATKH+17]. identity [Ano13d, BMBS10, BOB13, BMM12, BBGT12, CTHP13, dCCSB+16, DZ14, Din10, DWZ12, FA14b, GMRT+15, GPVcDRO12, HZC+14, HWDL16, HZWW17, HLR11, HL11, HPY10, Hwa11, JZS+10, KKGK10, KK+13, KL11, LKKL13, LK12, LWM12, LCT+14, MSS+17a, MD15, MGP10, MJS13, MLM16, MM13, NCL13, OJS1, PLCGS11, QYWX16, RG10, SSSY12, SE14, SE16, SR10, hSSZ15, SA16b, Sim15b, SSAF11, SSS11, SGM16, WYYZ11, WNYY11, WLFX17, WMX+17, Wat14b, WWWW17, WX12, XCL13, YWL+17, yQyWqZC13, YYY+16, YMSH10, YKC+12, YXA+16, YNX+16, ZZ12, LZXJ10, PN10, Sar18a, Kat13]. Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL+12, CGY+13, Chi12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, CY13, GJZ17, HZC+12, HSM14, HZX15, LMG+18, LSL12a, LCC+15, LTZY16, LSLW15, LH11b, LSC12, LBR12, MLO17, MBF+13, MGSP12, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, Ser12, SSC12, SKGY14, SWW+16, SGH15, TRK14, Tin15, TH16, TMGP13, Vle12, WV10, Wan14, XXZ12, XQL11, XJW+16, YXZ+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCZY12, ZLH+12, ZMW16, ZDW+16, ZPXX17, ZYM18, ZTSR12, ATKH+17].
improvements [EA12, HRV10, Tso13].
Improving [AB15, BCM+15, Chi16, FMS12b, GMS11, HLCL11, MHC12, Sar10a, SS11, YWF18, YKBS10].
In-Memory [IG11, MEFO12].
Incentive [SJWH+17, YTH17].
In-Memory [PAF18].
Incentive-Aware [YTH17].
Incident [CCG+16, CMG+18].
Incremental [KKM+14, MPRS12, CS11].
IND-CCA [AHS14].
IND-CCA2 [Gal13, MVVR12].
Independent [FCM14, MTY11, MKRM10, YE12, ZTL15, BVIB12, DDD14].
Index [LHKR10, PSS+13, ZXYL16, Jon13, LLHS12, LW13a].
Index-Based [ZXYL16, LLHS12].
Indexing [HCDM12].
India [BC11, CGB+10, GG10].
Indicator [KU12].
Indicators [YT12, Pal16].
Indirect [ABS+12].
Indistinguishability [AS16, BV18, FYMY15, GGHR14, GG+16a].
Indistinguishable [LG12].
Individual [LMB12].
INDOCRYP [BC11, GG10].
Induced [VDB+16].
Industry [Aro11b, ZQZ+16a, Cha13c, Men13, ZSM+18].
Infected [GST12].
Inference [Bro11, DBPS12, NC12].
Inferring [BPSD17].
Influence [RSCX18].
Information [AQD12, ABCL17, Bai10, BF11, CVM14, CDGC12, CGB+10, CST+17, CBL13, Dew11, DP12, FHKP17, FHS13, HHH+13, IF16, JHHN12, LG12, LW11a, Low12, MA17, MAL10, NTKG17, SG14, STC11, TWZ11, WSS12, XZZ18, Yan10, Yek10, ZZ15, ZHL15, AB10a, Abe10, AL15, ASVE13, BSS11, BGP+17, DMWS12, KL13, LWK+18, MKH+12, Mar10b, SRB+12, WW13, BYL10, LH10a].
Information-Theoretic [CVM14, WSS12, CDGC12].
Information-theoretical [ZZ15, KL13].
InfraStructs [WW13].
Infrastructure [GM13, PN10, GAI+18, JAE10, SA12].
ingenuous [Mac12].
Inhibiting [GS+16].
Initial [PAS13b].
Inhibited [AN15].
Injected [LLZ+12].
Injection [ABS+12, ARP12, DDR+16, JW+17, PYM+13, YGD+17].
Injects [LCLW17].
In [Keb15, Mac14].
Inner [ADM12, LMG+18, OT12, YKNS12, DDM17].
Inner-Product [YKNS12].
Innovations [JSM+18].
Input [GGHW17, XXZ12, PBCC14].
Inputs [GGHW17].
INSCRYP [BYL10].
Insecure [BCGN16, Mur16, Lan17].
Insecurity [HYZ15, LRW17, SWYP12, WY10, Wan14].
insertion [XWDN12].
Insider [AJA16, ERLM16, LJS+14].
Inspection [FGR+17, VCK+12, AZH11].
Inspired [RMG18, BW13, GPVCdR12, OK18].
Instability [LMB12].
Installment [SYC+17].
instance [BRT12].
Instances [HN10].
instead [AGH+17].
Institute [Wes16].
Instruction [ARP12, AB15, EKP+13, BVIB12, SF12].
Instruction-Cache [AB15].
Insulated [FZT13, LH11b, HL11, RG10, RWZ13, WWY11].
Integer [Cou12, AMK12, MM13, Mst15, MN14, PC14].
Integers [CN12, CNT12].
Integral [AY14b, LWZ12, ZSW+12, SM11, SNM+14, SH11].
Integrated [LY15, MU12, AL15, SSM+12].
Integrating [CFZ+10, LH12, OdH12, AEHE17, HL11].
Integration [AQD12, Kar12, ZYW+13].
Integrity [BCP14a, BCK17, FYMY15, MV16a, PH12b, ED17, SWW+16, YXA+16, YNX+16].
Intel [SF12].
Intelligence [Dew11, Alld11, Bud16, GW14, Han12, Maf16].
Intelligent [AMK12, IEE11a, SAJL16, W14a, HLYS14, MKH+12].
Inter [LBR12, BGAD12, SCKH10, SA15, YWK+10a].
Inter-domain [LBR12, BGAD12, SCKH10, YWK+10a].
inter-router [SA15]. Interactive [CJFH14, DF11, FSGW11, BCI+13, Pas13a, PPR+12].
interceptor [Cho10]. Intercepts [Don14].
Interface [WBA17], intermittent [CL16].
International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FM12, GLIC10, JY+14, LCK11, LWI1a, LW11, MV12, P+12, Sen10, Wat10, Yan10, Yan11, AB10a, Abe10, Ano11a, BYL10, BL10, Gil10, GG10, HWG10, LH10a, IEE11a]. Internet [Ano13d, LFGCCRP14, TW14, AAC+16, Ano13b, CLF+17, CW12b, DRS16, DG15, Gel13, HZL18, JTZ+16, NKS+18b, LGH+17, LSG16, MJGS12, MJS11, MCF17, NLLJ12, NLY15, Ozn16, PLGMCdF18, SB17, SYW17, SYC+17, SKE1G, WC18, YCT15].
Internet Draft [MCF17].
Internetworking [SAAB10].
interoperability [HWK+15].
Interplay [JW14].
Interpolation [JTZ+16, KU14].
Interpretation [MZ17b].
Interpretation-Based [MZ17b].
intersection [LZY+16].
Interval [PPR+12, Cra11, DTZZ12, LWY12, MO14].
Interval-based [PPR+12, Cra11].
Intra [HF14b].
Intra-Masking [HF14b].
Intrinsic [SN10, NS10, RCW15].
Intrinsically [SRK+17].
Introducing [Fay16].
Introduction
DK15, Gas13, G’13, JSK+17, LLK18, Low12, Mei10, Sch15a, SOG15, Sta11b, CM13, Buc10, Led16, Sch15a, Ful10, Mur10].
Intrusion
[NSMS14, SAJL16, SBV14, YKC+12].
Intrusion-resilient [YKC+12].
Intrusive [AARJ12, MFH13].
invariance
[yWPnL11].
Invariant
[CSW12, NKF14, RS16, WYW+13, YWNN15, GHZD12, LXM11].
Invariants
[NKF14, CDSLY14, KK10, MZ17a, TLL13].
Invention [Ozn16].
invents
[Ant14].
inversion
[KHHH14].
Invert
[ZWTM15].
Inverted
[ZXYL16].
Invertible
[SLY+16, UUN13].
Inventing
[SPM+13].
Investigations
[Bla16, Har14].
Invisibility
[BN14].
 Invisible
[Keb15, Mack14, SYL13].
InvisiMem
[AN17].
INVISIOS
[AARJ12].
Involving [HLCL11].
Inotes
[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].
IRIW
[JHKYe12].
irregular
[YWL+17].
ISBN
[Ano15b, Ano17b, Bai12, Joh10, Mur10, Sch15a].
ISBN-13
[Joh10].
Islet
[Dan12].
ISO
[BC12, BCM13, TS16, WWBC14].
ISO/IEC
[BCM12, BCM13].
Isogenies
[Y+17].
Isogeny
[KAK18, Lau17].
Isogeny-Based
[KAK18].
Isolated
[YS15].
Isolating
[LG12].
ISSAC
[Wat10].
Issue
[Ano13d, Ano16a, Ano16b, Ano16h, CSYY18, GO17, LW13a, LK18, XW13, PHWM10, Sim15b].
Issues
[ABHC+16, PZPS15, JAE10, KJN+16, MVH15].
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].
Jacobians
[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 [Full0, Mou15].
Juniper [CCG’16, CMG’18]. Juraj [Gas13].
Just [Pfl10]. JXTA [AMHJ10].
KASE [CLW16]. Katz [Full0, Mou15].
KDM [MTY11]. Keccak [BDP’12]. keep [Rus15]. Keeping [CG14b, Man13, Gup15].
KEM [CZL14] kept [Cha13c]. Kerberos [SCH10, TW14]. Key [ASN12, Ano11b, BN14, BVS’13, BL12, BBB’16a, BCO13, BKLS12, BF11, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CJ13, Chii16, CCT’14, CNT12, Cou12, CMA14, DWZ12, DL12, EAA’16, FZT13, FVS17, FM12, GFBF12, GT12, GZZ’13, GSW’16, GST13, GPT14, Gir15, GKS17, GZ12, GLB’18, HSMY12, HLLG18, HC12, HL10a, HCL’14, HCT’15, HEC’12, Jia14a, JEA’15, KP12, KTT12, KFOS12, Kim15, LLSW16, LCLL15, LQY10, LY16, LH11b, LSQ18, LCCJ13, LYY’18, LBR12, LH118, MZHY15, MV12, MPP14, MT11, MMY12, MPR12, MNS11, MSU13, NNA10, NRY’14, NTY12, Orm16, PSM17, PDHN15, PCKP14, Pud12, PRNC17, RH1’16, RSBGN12, RW12, Saa12a, SK11, SN11, SHEK12, SK12b, SWM’10, Sia12, SGG15, SLV’16, TMC15, TMY’17, TM12, WP17, WSS12, WLC12, WZ15, WCL’18, WWHL12, WT10b, XNKG15, XXZ12, Xio12, XLM’12, XJWW13, XGLM14]. Key [XZLW15, XJR’17, YM16, YZX’12, YS12, YLW13, YRT’16, YL17, Yon12, YKC’11, YFK’12, ZXY16, ZY17a, AA14, ATKH’17, APK’18, ABB’14, AKG13, AIB’16, ABW10, AN15, BS15, BAGD12, BBI4, BJ16, BSW12, BGG’13, BBB16b, CFL13, Cha13a, CSD18, CLZ’17, CTL13, CML16, CLCZ10, DLD’16, DGIS12, Dur15, FH10a, FA14b, FIO15, FHZW18, GMRT’15, GPP’16, GH16, GBNM11, GLM’11, HPC12, HDZW17, HLI11, HLSY14, IM14, ISC’16, IB11, IOV’18, JSK’16, JLT’12, Jia14b, JSMG18, KDH15, KKG14, KP18, KLW’16, KDW’17, LLLS13, LLP’18, LWS10, LK’17, LPdS10, LW13b, LYZ14, LML’13, MNP12, MRT10, NACL12, NCL13, Nos11, Nos14, RG10, RWZ13, RP110, SES’16, Sar14, Sav16, SLZ12, SY15b, SZM13, lSZZ15, SA15, Svt10, TCS14, TLL12, Tso13, TKH14, VN17, WWYZ11, WZM12a, WZM12b, WT10a, WTT12, WQZ’13, WXK’17, WX12, WX13, XCL13, XMHD13, YT11b].
Key-Aggregate [CCT’14, PSM17, GLB’18, CLW16].
Key-Agreement [WSS12, APK’18].
Key-Alternating [BKLS12]. Key-Based [Xio12]. key-correlations [Sar14].
key-delegation [JSMG18].
Key-Establishment [BCO13].
Key-Length [GT12]. Key-Long-Based [PNRC17]. Key-Policy [GZZ’13, GSW’16, HSMY12, RVH’16].
Keyed [KE19, MMS17b, YHH18].
Keys [ASN11, BF12, Bro17, CC10, HDWH12, MS16, PSM17, TW14, ZMW16].
CMG +18, HL14, IK15, LLY15, LH13, LW10, LLL +18, RWZ13]. keystream [SM11].

Keystroke
[AaBT16, SP13, CTL12, LTC +15a].

Keyword [CWL +14, Che15, HCDM12, LSQL18, WDCL18, XWSW16, XJWW13, ZXYL16, BL11, CLH +16, FSGW12, GZS +18, LKX +14, OSSK16, SY15b, WHY +12, WXLY16, XWY +18, YZCT17].


NVM+17, RS17, SAJL16, WT10b, ZJ11, CZ14, Chi13a, FQZF18, LGKY10, LKAT12, LEW19, MHV15, NR11, ZPZ+16.

Low-Bandwidth [GST13, NR11].

Low-Bit-Rate [LJK17]. Low-complexity [DJL+12]. Low-Cost [ABC+17, GI12, Man13, NVM+17, LEW19].

Low-Distortion [FHS13]. Low-end [Chi13a]. Low-Latency [BCG+12b].


M [Orm16, HvS12]. M-Identity [HVs12].

MA [ACM10]. MAC [Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN16]. MacGuffin [GL+12]. Machine [AGHP14, Ano16c, CHS15, Sch12a, ABBD13, GJ13, Gup15, LLZ+16, LHA+16, QMC17, RY10, TTI10, War11, WS14].


makes [Ken11]. Making [BG14, dCCSB+16, Gel13, LA10, ZDW+16].

Malaysia [HWG10]. Malicious [AAE+14, BL15, TM18, VGA15, BK12b, WTT12]. malleability [KTT12]. Malleable [CKLM13, DPW18, M Sas12, CG14a, FMNV14, LP11, M Sas13, OOR+14, Pas13a].

Mallory [FHM+12]. Malware [ATS15, GAF+15, JC13, Goo12]. man [And13, Bat10, Kap13, Moo14].

Management [ASM12, BS13b, CCFM12, CSL+14, GOPB12, KP12, KKA14, Lop15b, MKF+16, PN10, TMSGP13, Vle12, YZX+12, YSS14, ZJ11, ZTSR12, BMBS10, BBB16b, CFL13, Cha13c, dCCSM+12, dCCSB+16, Din10, KH18, M LSMG12, MGP10, PLLGS11, Sch11, SR10, SA15, SWW+16, WWW17, WQZ+13, YZL+18, YLS12, ZMM+10, Ano15b]. Manager [KKA15, Kim16]. Making [MD15, BC18].


Might [Hur16]. Migration [SHS12].
MIKEY [TW14]. Military [HK14]. Miller [Sch15a, LL11, LT14a, Led16, LR15].
Millionaire [GKS17]. Mind [WP15].
Minimizing [BCD+12]. Minimum [KHPP16, DZS+12]. Mining [BH15, BJL12, HDWH12, WZCC18, ZW15, Ano11a].
Mitigations [BSR17, LGR14, DJL+12]. miTLS [BFK16]. MITM [TY16b]. mix [WGJT10].
mix-networks [WGJT10]. Mixed [ST16]. mMTC [CML+18]. Mo [RBS+17]. Mobile [BCD+12, FD11, GPT12, GD16, HvS12, HLKL15, KP12, KKA14, KKM+13, KKM+14, KKG14, KSB+17, LH13, OYHSB14, Par12b, hSZZ15, SSSF11, SKB+17, TKHK14, WT10a, YH18, YNX+16, ZDW+16, ZC12, MBF+13, SLL10]. mobile-cloud [KKM+13]. mobiles [GCSAddP11]. Mobility [CLH13, LNK+18a, CL11, GH16, LH11a, MYYR13, YLS12, ZXL11]. Mode [HZ11, Mar10c, PAF18, gWpNyY+14, WLC12, Fay16]. Model [AW17, App13, CT18, CLP13a, GLG12, GJO+13, GJJ15, GJZ17, HZ15, IA15, Kar12, KP17, LHM+15, LZC+12b, MMVR12, PYM+15, PNRC17, SZZ14, SPM+13, TBCB15, WWC+11, WWHHL2, XZY+12, Yon12, ZHL15, BL11, CK11, CDPLCA16, DFJ+17, HKT11, KSU13, LIT2, LCY+16, LL16b, MGP10, Mas17, MMY15, NB13, WYL13, WZM12a, WZM12b, YC12, ZCL+19, TCM+15]. Model-based [IA15].
Naive [ZLW+17]. Name [YCM+13].
Named [LLZ+17]. Names
[ABJ13, MPJ+16]. National [ABJ13].
Natural [ZCWS15]. Nature [KL13]. Naval
[Don14]. Navy [Maf16]. Nazis [Hea15].
NDSS [Ano10]. Nearest [LVRY10].
Nearest-Neighbor [LVRY10]. Nearly [PHGR16]. Necessary [TD14]. NECPPA
[PZBF18]. Needs [Sch12b]. Neglected
[Joh15]. Negligible [DF11]. Neighbor
[KA18, LVRY10]. Neighborhood needs
[DA10]. Neighboring [LSQ11b, LC15].
Neon [ZMM10]. Neon
[KA18, LVRY10]. Neighbors
[Sch12b]. Neighbors needs [LVRY10].
Neighborhood needs [PZBF18]. Nested
[HH10]. Nets [PS14]. Nets-Based [PS14].
Network [Ano10, Bis17, CWL16, CJ13,
CLH13, DRS16, Hay13, HDWH12, HS18,
Kim15, KCC17, LH12, LCLL15, LY16,
LTW11, MJGS12, NAMO10, NRZQ15,
SGC16, She14, TLW12, VKPI17, VFV17,
VGA15, VKC15, WP15, YZLC12, YSL14,
AKM+11, AL15, Ano11a, AZF+12, CL11,
DLK+16, FPBG14, HWG10, HB13, HKB14,
JZS+10, KP18, LH11a, LKKL13, MZA+13,
MJS13, NDNR13, OF11, FL16, RCW15,
Ser12, SCKH10, SKS+18, Sta11a, Tan15b,
WYL13, WS14, YLS12, ZOSZ17, Ste15b].
Network-Assisted [KCC17].
Network-Based [YL12]. Network-Coded
[She14]. Network-On-Chip [Bis17].
Networking
[LC11, LLZ+17, ZHL15, Kim11, LCM+17].
Networks
[ABCL17, ABC+17, BN14, BPSD17,
BFMT16, CS14, CHW+18, DS11, DF16,
FMS12b, GMV17, HZC+12, HBCC13,
HK14, KHI10, LLC11, LL15, LHM+15,
LZK14, LWCJ14, LLZ+12, MPM+17,
NSA15, NYR+14, O012, OKG+12, PYM+15,
PCPK14, RWLL14, SWYP12, She14, SP15b,
Smi11b, SL11, SZZT18, TCF+17, WXL+17,
WLY+15, XHC+12, YM16, ZC13, ZW15,
Zha15b, ZLDD12, ZSA12, Aia15, ASA14,
APK+18, AIB+16, AIKC18, ADF12, BDK11,
BLAN+16, BBB16b, CDGC12, CLM+12,
CML+18, CLSW12, CL11, DSCS12, DK12,
DLN13, EEA13, FA14b, FMA+18, GH16,
HGWH11, HZC+14, HZWW17, HCC11,
HCM11, HTC+10, HYF18, JNUH17,
JLT+12, JMW+16, KM10b, KLC+10, KO16,
KLW+16, KDW+17, LLLS13, LC17,
LMJC11, LXJ14, LIK+17, LNK+18b,
MSM+18b, QMW17, QPI12, SGGC+16,
SA12, SGJ+18, SZMK13, hSZZ15, SKK10,
TODQ18, TKHK14, WAT10, Wan13,
WW14, WXK+17, WX13, XWDN12,
XCH14, XMHD13, YHHS16, ZWQ+11].
Networks
[ZBR11, ZCLL14, ZTZ16,
ZMM10]. Networks
[LSQ11b, LC15]. Networks-Based
[PS14]. Networks-Assisted [KCC17].
Network-Based [YL12]. Network-Coded
[She14]. Network-On-Chip [Bis17].
Networking
[LC11, LLZ+17, ZHL15, Kim11, LCM+17].
Networks
[ABCL17, ABC+17, BN14, BPSD17,
BFMT16, CS14, CHW+18, DS11, DF16,
FMS12b, GMV17, HZC+12, HBCC13,
HK14, KHI10, LLC11, LL15, LHM+15,
LZK14, LWCJ14, LLZ+12, MPM+17,
NSA15, NYR+14, O012, OKG+12, PYM+15,
PCPK14, RWLL14, SWYP12, She14, SP15b,
Smi11b, SL11, SZZT18, TCF+17, WXL+17,
WLY+15, XHC+12, YM16, ZC13, ZW15,
Zha15b, ZLDD12, ZSA12, Aia15, ASA14,
APK+18, AIB+16, AIKC18, ADF12, BDK11,
BLAN+16, BBB16b, CDGC12, CLM+12,
CML+18, CLSW12, CL11, DSCS12, DK12,
DLN13, EEA13, FA14b, FMA+18, GH16,
HGWH11, HZC+14, HZWW17, HCC11,
HCM11, HTC+10, HYF18, JNUH17,
JLT+12, JMW+16, KM10b, KLC+10, KO16,
KLW+16, KDW+17, LLLS13, LC17,
LMJC11, LXJ14, LIK+17, LNK+18b,
MSM+18b, QMW17, QPI12, SGGC+16,
SA12, SGJ+18, SZMK13, hSZZ15, SKK10,
TODQ18, TKHK14, WAT10, Wan13,
WW14, WXK+17, WX13, XWDN12,
XCH14, XMHD13, YHHS16, ZWQ+11].
Networks
[ZBR11, ZCLL14, ZTZ16,
ZMM10]. Networks
[LSQ11b, LC15]. Networks-Based
[PS14]. Networks-Assisted [KCC17].
Non-Boolean [AS17], non-browser [GIJ12], non-compliant [Lan11],
Non-contextual [Svo14],
non-cryptographic [AY14a, ESR14],
non-dynamic [SES+16], Non-interactive [BCI+13, Pas13a], Non-intrusive [MFH13],
non-iterative [SXL16], Non-Linear [EKP+13, XSWC10], Non-Linear/Linear [EKP+13, Non-malleability [KTT12],
Non-Malleable [DPW18, MSas12, CG14a, FMNV14, OOR+14, Pas13a, LP11, MSas13], Non-monomizable [DJL+12],
Non-perfect [FHKP17],
Non-Repudiation [LLG15],
Non-stationary [ZLDD12], Non-tamper [WgMW12], Non-uniformly [YKL12],
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, Gall13, Hwa11, Lim11], nothing [Cer15],
Notions [KFO12, SNJ11, Sar12, BP11], Novel [CLHC12, KRDH13, LLG15, LyWZZ12, LH11b, MJGS12, MCS+15, SWM+10, SC12, VN16, WHZ12, WXZL12, YZX+12, Ye14, ZMZ17, BOB13, CH10, DDFR13, HCCC11, JXLL15, LXCM11, LMJ11, LHI3, LWW+10, LML+13, MRT10, NZL+15, PZBF18, SYW17, Smi16, TG17, jT12b, WYL13, WGZ+12, WYT+12, ZBR11],
November [Kap11, LCK11, Yan11], NSA [ABJ13, Ano13b, AHS13, Bud16, Men13, Sta13, Tox14],
NSDG [SSPC12], NTOW [BS15], NTRUEncrypt [DWZ18, KY10],
NTRUSign [Wan10], NTT [MCDB12],
NTRU-Based [MCDB12], Nuclear [Hel17],
Number [ADI11, BKLS12, CDK+10, DSLB18, Fok12, Ham17, KA18, LTKP16, LCLW17, MFG16, NIS12, NNAM10, Sha10, SRAA17, SRK+17, CFY+10, CP13, LLP+18, LGKY10, Lim11, MS12a, MRT10, SH11, Sti11, XSWC10],
Numbering [MNS11],
Numbers [BCGH11, CK18, FM15, Shp10, AZH11, Ana14, GCH15, SM1S11, ZOC10],
umeral [GKCK11],
Numerical [CML16],
Numerology [GG11],
O [CDD13],
Obfuscated [LMS16, OWHS12, ZM16],
Obfuscating [BGI+10, BGI+12],
Obfuscation [ABCL17, AS16, AWSS17, BBC+14, BV18, BCP14b, BR14, CZ15b, DRS16, EMW14, FKOV15, GGH14, GGH+16a, GGH17, MH14, BBGT12, CFVP16, GGH+16b, OSSK16],
Obfuscation-Based [ABCL17],
Obfuscators [PSD15],
ObfuscMem [AWS17],
Object [BCK17],
Oblivious [DN12, WCL+18, CGH11, RYF+13],
obscurity [Edw14],
observation [WHY+12],
Observations [HCL+14],
Obtaining [BB10],
Occasion [Nac12],
October [CGB+10, IEE10, IEE11b],
octonions [BS15],
o dd [GJMP15],
Oded [LIn17],
ODIN [ABCL17],
Odyssey [Car11],
OFDM [CLZ+17],
Off [GPT14, GH14, YMWS11],
Off-Line [YMWS11],
Off-Path [GIS14], offering [Par12b], Offers [Pau10],
Office [Mor12],
officers [Maf16],
Official [Küp15],
Offline [Ano15a, GAS+16, JMG+16, LJJ+17, LKAT12, RSM15],
Offline/online [LJW+17],
Offloading [JHC14],
Offs [ASBD16, BS14, SR10],
offsets [YQH12],
Old [Che17, GY13],
On-chip [BAB+13],
On-Line [FFL12],
On-siteDriverID [SG1C+16],
On-the-fly [PS14],
One [CPS16, DSM14, DCG12, FD11, HP14, HG12, Mat14, NA10a, PC16, TYM+17, XW12, XYXY11, XZLW15, Yon12, BM15, FHH10a, HRV10, LP11, LW10, LW13b, LML+13, RK11, Rus15, SM10a, TCS14,
One-Dimensional [XYXYX11].
One-Round [TYM+17, XZLW15, Yon12, XW12, TCS14].
One-Sided [HP14].
One-Time [NA10a, DCAT12, BM15, FHH10a, LW10, LW13b, LML+13].
One-Time-Password [FD11].
One-Way [CPS16, DSMM14, Mat14, HRV10, LP11, RK11].
Onion [KZG10].
Online [BPSD17, JMG+16, KSD12, LLH18, LW13, SKGY14, SZZT18, ZHL15].
Open [ABF+14, MHV15, Pow14, Win17].
open-source [ABF+14, Pow14].
OpenCL [ABDP15].
Opening [GDCC16, LZC12a, LLH18, LZC14].
Operation [GLLSN12, JB11, ALL+18, Fay16, Lin14a, SKK10, WZQ+11].
Openings [SP13].
opportunity [Sch11].
Optimal [AS17, DSSW14, HRT13, PDDN15, PPS12b, Cha13a, DDD14, PPTT15].
Optimally [MM17, SDM+12].
Optimally-Fair [DSMM14, GT12].
Optimised [CMO+16].
Optimising [EVP10].
Optimistic [WSA15, SEXY18].
Optimizations [ZAG19].
Optimum [Oba11, YFF12].
Optional [PC16].
Oracle [GLM+16, HKT11].
Order [FZT14, FSX12a, GSW+16, XQL11, YS12, YKC+11, YLA+13, ZYM18, LLY15, RG10, SYL13, WWYY11, YFK+12].
Order [DCA18, KS12, LWKP12, PRC12, YKKL12, ZDL12, ZSW+12, AKY13, LW13a, LCY+16, LWKP14, gWpNyY+14, YL11].
Order-Hiding [DCA18].
Order-Preserving [KS12, YKKL12, YL11].
organisational [Smi15a].
Organisation [RSGG15].
 Oriented [TJZF12].
Orthogonal [tWmC12].
Oscillator [YKBS10].
OSN [BCF16].
Outlive [Hur16].
Output [DK16, GST12, NR12, PBCC14].
Outright [ABJ13].
Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18, LQD+16, PD14, RDZ+16, YMA17, YMC+17, DFJ+10, FS18, HMCK12, LCL+15, LCY+16, LQD+16, QZDJ16, ZML17, ZSW+18b].
Outsourcing [DR12, LHL12, LHL+14, LJWY18, SKB+17, SWW+16].
outwitted [Car11, Fag17].
over-the-air [ZXW+18].
Overhead [AWSS17, Bai10, CCW+10, GHS12, ZJ11, RS17].
Overview [Bla16].
Ozarow [ADG16].
P2P [dCCSM12].
Packet [FGR+17, JTZ+16, VKP17, XHC+12, PD16, PJ16, PX13, XWDN12].
Packets [Bis17].
Pads [NA10a, BM15].
Paillier [Gal13].
Paillier-based [Gal13].
Pairing [Lin15].
Pair [Bon12, CWWL12, CST+17, KZG10, KHPP16, LGPRH14, YTS12, Con12].
KSH18, LL16a, LR15, YT11b, ZY17b.

**Pairing-Based** [Bon12, CST+17, KZG10, LGRPH14, YTS14, Con12, KSH18].

**Pairing-free** [LL16a, YT11b]. **Pairings** [ASS15, Hof15, LL15, LT14a, QYWX16, RS15, UK18]. **pairs** [MCP15]. **Pairwise** [DL12, YM16]. **Palash** [Kat13]. **Palm** [IEE11b]. **Pan** [GOPB12]. **Pan-European** [GOPB12]. **Paper** [TSH17, Ano16g, SK14, YFK+12]. **Papers** [Ano16a, Ano16b, Ano16h, LW13a, LW13, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. **Paradigm** [ABGR13, BS12, Mau12, MP12, WQZ+13].

**Parallel** [App14, ARM15, CGB+10, GP17, LY16, LB13, MCDB12, MC11, NdMMW16, SMD11, YE12, CSTR16, MRT10, RG10, RWZ13, WWY11]. **Parameter** [NDC+13]. **Parameters** [HBR13, MBF18]. **parametric** [Bu10a]. **Paranoia** [Cor14a]. **Park** [Ano11c, Bri11, Cop10a, Cop10b, GW14, Mck10, Mck11, Mck12, Pea11, Smi11a, Smi15b, Smi15a, Bai12]. **part** [VM14].

**Partial** [DL16, GBF12, LG12, SGS14, WDD12, Bax14]. **Partially** [KB10]. **participants** [KZ13, WTT12]. **participating** [Ch10]. **particle** [ZSMS18]. **Parties** [YCR16, Kip13]. **Partitioned** [FVS17]. **Partitioning** [ADR18, AP11].

**Party** [Ash14, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, QZL+16b, TYM+17, ZM16, ED19, FIO15, GVW12, HPC12, LyWSZ10, LML+13, Tso13, TKHK14, XLWZ16, XCL13, YC12, YZZ+14, ZC15, GHKL11].

**Passau** [GLC10]. **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, Shi11, WgMW12, YLW13, YRT+16, ZHX16, ABK13, AIKC18, CTL12, DSCS12, FA14a, FIO15, FHV16, HCC10, IOV+18, LWS10, LNLK13, MM12, MvO11, Tso13, TKHK14, WZM12a, WZM12b, YC12, ZXWA18].

**Password-Authenticated** [HCL+14, YRT+16, ZHX16, LWS10, WZM12a, WZM12b]. **Password-Based** [BRT12, CLY14, FVS17, WgMW12, DSCS12, FA14a, FIO15, IOV+18, TKHK14].

**Password-Only** [YWW13]. **Passwords** [BHvOS15, LCL17b, BCF12, Che13]. **Past** [Bon12]. **Patchwork** [NXH+17, XNG+14]. **Patchwork-Based** [NXH+17, XNG+14].

**Path** [DMS+16, GHS14, NLLJ12, ZW15, He12, RYF+13]. **Patient** [ZLDC15, ZVG16]. **Patient-Centric** [ZVG16]. **Pattern** [DCA18, ATKH+17, uHAN+18, KPS10, OSSK16, PPTT15].

**Patterns** [Ano16e, BPS17, TSH17, WOLP15, BDK11]. **PAWN** [JNUH17]. **pay** [CCSW11]. **pay-TV** [CCSW11]. **Payload** [CHW12, AZH11, JNUH17]. **payload-based** [JNUH17]. **Payment** [DG15, SYC+17, SYW17]. **Payments** [RBHP15, MPJ+16]. **PC** [YE12].

**PC-Based** [YE12]. **PCi** [IBM13b]. **PCM** [LY15]. **PCM-based** [LY15]. **PCPs** [MX13]. **PCs** [GPT14, GPP+16]. **PDCG** [CGB+10]. **Peaks** [TC10]. **pearl** [Rus15].

**Pecherskii** [Kuz11]. **peer** [NCCG13, ZWY+13]. **peer-to-peer** [NCCG13, ZWY+13]. **Per-File** [DMS+16].

**Perceived** [CSW12]. **perceptual** [MK11]. **PEREA** [ATK11]. **Perfect** [Pas13a, Sch13, CZ15a, FHKP17, LCC10, Lew10, XW12]. **perfectly** [ADG16]. **Performance** [Alo12, AW17, AB15, CGL+12, CCG10, DLK+16, DBPS12, EGG+12, ESR14, FPBG14, GL12, GCS+13, HKL+14, KAK18, LCK11, LPO+17, MHC12, SKV12, TPKT12, WDD12, Xia12, YFW18, ZLDD12, ABDP15, GCVR17, MMS+17a, MS13c]. **Performed** [Ano17d]. **perimeter** [Cal13]. **periodic** [KPS10]. **periodical** [CLSW12]. **Permission** [VN16]. **Permutation** [LJ16, GMSW14, LK14].
permutation-based [LK14].
Permutations [ARH^{+}18, BKLS12, Mat14].
Persistent
[CSYY18, TYK^{+}12, ALL^{+}18, PKA15],
person [PN10]. person-centric [PN10].
Personal
[ESS15, LYZ^{+}13, Rao17, ALL^{+}18, BC18, MoO11, LHL15]. Personalized
[FRS^{+}16, AT10]. Personnel [YTH17].
Perspective
[KKMY18, MSM18a, RSM13, Rao17, SVG16, HZL18, HQY^{+}16, ZHH^{+}17].
Perspectives [Sen17, SPM^{+}13].
Perturbation
[XZZ18]. Pervasive
[VRA{+}17b, BCG^{+}12b, YD17, SM15, SCY15, Tan12b, YWK^{+}10a]. Petri
[PS14]. PGP [RAS15]. Phase
[LD13, NBZ17, ZWT13, ZHH^{+}17]. Phase-change [ZWT13].
Phase-Encrypted [NBZ17]. Phone
[Mur16, SAA12b, KRM^{+}10, LTC^{+}15a]. photo [OF12]. Photographic
[YSC^{+}15]. photos [Pow14]. Phrases
[WBC^{+}10]. Physical
[GPT14, GPP^{+}16, HHH^{+}13, SMOP15, HQY^{+}16, HZWZ18, KSA16, QMC17, VCK^{+}12, WW13, YD17, ZHH^{+}17].
physical-layer [HQY^{+}16, ZHH^{+}17]. physio
[HT11]. physio-behavioral [HT11]. Pi
[MR10]. Pi-Calculus [MR10]. PICADOR
[BGP^{+}17]. PICARO [PRC12]. Piccolo
[IS12, Jec13]. picture [SM13]. piecewise
[GMOGCCC15]. PIN [MDA10]. Pinch
[DP10]. PinMe [MDMJ17]. Pinocchio
[PHGR16]. pioneer [Men13]. Pioneers
[Orr16]. Pipelineable [BDMLN16].
Pipelined
[HZ11, KB10, NdMMW16]. Pipher
[Me10]. Pixel
[DA10, LLL17, LyWZZ12, Lin15, LTC^{+}15b, SSA13, YWW10]. Pixel-Value
[YWW10]. Pixel-Wise [SA13]. Pixels
[PDMR12, Tan12a]. PKC [FBM12].
PKCS\#11 [CFL13]. PKDS
[HLC11, HLYS14]. PKE
[HTC^{+}15]. PKE-AET
[HTC^{+}15]. PKI
[Dav11, YCR16]. PKIs [KGO10]. PKZIP
[JLH12]. plain [LW13b]. Plaintext
[BM15, JLH12, MSas12, MSas13]. Plaintexts
[YKKL12]. Plane
[YLL^{+}12]. Platform
[YE12, ABF^{+}14, NCCCG13]. Platforms
[HTZR12, LMS16, SOG15, LT14b]. Plausibility
[KD12b]. Play
[Shp10, VGN14]. Player
[GJO^{+}13]. Pless
[Ayu12]. plugged
[PP11]. POB
[SRAA17]. Podol"sky
[HR13]. Point
[AK14, MH14, ZC13, ZM16]. Point-To-Point
[ZC13]. Point/Polynomial
[ZM16]. Pointers
[Lop12, PYM^{+}13]. Points
[SC12, Chm10, Lin11]. Poisoning
[HLAZ15, YCM^{+}13]. Polar
[YWWN15, PGLL10, YKK18]. policies
[Cra11, DFJ^{+}10, LHM14]. Policy
[GZZ^{+}13, GSW^{+}16, HSMY12, MK12b, RVH^{+}16, Rao17, SVG16, XMLC13, XWLJ16, ZHW15, FSGW11, FS18, HZL18, HKHK13, JSM18, LFW15, JLY18, QSW^{+}18, TY16a, XWS17, LAL^{+}15, LHL15]. Polish
[Kap11]. pollution
[NDNR13, OF11]. Poly
[AS17]. Poly-Size
[AS17]. Polylog
[GH12]. Polynomial
[An11b, BGJT14, DWZ18, ERRMG15, FS15, HVL17, NKWF14, WSSO12, ZM16, AAT16, BGJT13, Bul10a, Bul10a]. Polynomial-Advantage
[WSS12]. Polynomials
[CMLRHS13, SS12b, TW11, LP110]. Pont
[Kap11]. Popular
[Wal18]. port
[AZH11, KSB^{+}17]. Portability
[CHS15, ABDP15]. Portable
[Bee17, LA10]. posed
[Lan10]. Position
[BCF^{+}14, CGMO14, MS17, YXA^{+}18]. Position-Based
[BCF^{+}14, CGMO14]. Possession
[EKB^{+}16, ZPXX17, SYY^{+}17]. possibility
[BGI^{+}10, BGI^{+}12]. Possible
[BF12, Fra15, Orr16]. Post
[LLK18, MKAA17, Y^{+}17, ZCC15, YDH^{+}15, Sen10, Yan11]. Post-challenge
[ZCC15]. Post-Quantum
[LLK18, MKAA17, Y^{+}17,
YDH +15, Sen10, Yan11. **postcamera**
[Lin14a]. **Postfix** [HEK18]. **Postquantum** [Ano16a, Ano16b, BLM17, Lau17, YZCT17].

**Potential** [Ci11, VS16, ZW15]. **Power** [ARP12, AS16, HHR11, MMP14, MD12b, MAS16, MS17, SAJL16, SDM +12, TQL +14, WT10b, YAM +15, ZH15, ZJ11, FAA +18, LGKY10, LKAT12, QGGL13, RITF].

**POWER7** [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, FS10, HSA14, HPO +15, HKR +18, LW16, LJWY18, MFB18, PPTT15, RWZ13, TSH17, WHL16, XV13, YZLC12, ZYD10, ZLW +17, AMS +10, BS13a, CFN +14, JSK +16, LFZ +17, PHGR16, WR15, YKGK13, ZSW +18a].

practicality [NDNR13, Zha15a]. **Practice** [ABD +15, CDF16, FBM12, 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].

**Predictors** [EPAG16]. **Predistribution** [YM16]. **Preimage** [Li10]. **Preseeding** [Ran16]. **Presence** [BDPS12]. Present [Bon12, LJ16, WH17]. **PRESENT-like** [Li16]. **Preservation** [BCP14a, LLG15, VSV15, Yon11, LVRY10, TMLS12].

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

**Preserving** [ABCL17, BJL16, BHKN13, BJL12, CWL +14, CRE +12, GZZ +13, HSMY12, HLLC11, HXC +11, HMK14, KS12, LG16, MGC17, LNX15, LQD +16, NMS14, OFMR16, PR12, PD14, PSS +13, PPRT12, Pet12, RVH +16, RBHP15, SZDL14, SZQ +17, SZZT18, WPZM16, WZCC18, YKCL12, ZDL12, ZHW +16, ZM16, ZHW15, ZLDC15, ZTL15, AKM +11, AIB +16, ALL +18, BLV17, FH13, FMA +18, G11, HSH11, IC17, IOV18, JKL +16, KH18, LHL +18, LW13a, LCY +16, PZBF18, SY +17, Tan12b, TSH14, WLZ +16, YMM13, YNX +16, YL11, ZWY +13, ZOS17].

**Press** [Ano15b, Ano17b]. **Press/Elsevier** [Ano15b]. **Prevent** [HLAZ15, PYM +13, JSK +16]. **Preventing** [DCAT12, SKEG14, WS12].

**Prevention** [CW16, VS11]. **Primality** [Cou12].

**PRIME** [ACK +10, GM13]. **Primitive** [App15, MCS +15]. **Primitives** [BSJ15, EAA12, HLN17].

**Presence** [AW11, BAG12, BLP11, BAG12, CDF +10, DZH +18, FH13, FMA +18, GAI +18].

**Print** [KPS10, PKS18]. **print-can** [PKS18].

**print-scan** [KPS10]. **Printer** [EMW14, FNP +15]. **Prior** [NA10a].

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

**Prisoners** [AM11, ABB12]. **Privacy** [AM11, ABB12].

**Privacy** [AKM +11, ABCL17, ALL +18, ACM12, ABHC +16, BN14, BCF16, BJL16, BLV17, BS13b, BJL12, CVM14, CWL +14, CDFS10, DTE17, ESS15, FGR +17, GZZ +13, HSMY12, HBC13, HXC +11, KN12, KM10b, KCC17, KS12, KL18, LG11, LNX15, LQD +16, MYY13, NMS14, PD14, PSS +13, PPRT12, PZPS15, PSS15, Pet12, RVH +16, RCP +18, RW114, RBHP15, SS17, Set16, SZZT18, SW14, SOF12, TMLS12, TMGP13, WPZM16, WZCC18, WMY16, YMM13, Yon11, ZHW +16, ZM16, ZOS17, ZHW15, ZLDC15, ZHL15, ZTL15, ACK +10, BP11, BAG12, CDF +10, DZH +18, FH13, FMA +18, GAI +18.
Privacy-assured [WMYR16].
Privacy-Aware [BCF16, MGP10].
Privacy-Based [BS13b].
Privacy-Based [BS13b].
Privacy-Enhanced [DTE17, ACK10].
Privacy-Friendly [KCC17, ACM12].
Privacy-Preservation [LLG15].
privacy-preserved [SWW17].
Privacy-Preserving [ABCL17, BJL16, BJL12, CWL14, GZZ13, HSMY12, LMGCI7, LNXY15, LQD+16, NSMS14, PD14, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, SZZT18, W张某, WZCC18, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, ALL+18, KH18, ZOSZ17, BLV17, FMA+18, GAI+18, HSH11, LHL+18, PZBF18, SYV+17, Tan12b, ZWY13].
Private [BKLS18, GM13, Jia14a, QZL16b, Sia12, WCL+18, Yek10, ZMW16, ZXYL16, HJM+11, HYF18, IK15, WR15].
private-keys [IK15]. Privilege [Cha13c, QRW+18]. Privileged [Din10, WZDL13]. PRNG [DK16].
Proactive [SLL10, WMYR16].
Probabilistic
[BFG14, Rao10, WP17, KSU13].
probe [Sav13b]. Probably [MMS17b].
Problem [CLL16, GKS17, LLGJ16, NA10b, TCM12, Mes15, MR14c, RH10, VM14].
Problems [Din12a, Fra15, GTT11, KRDH13, KPC+11, RBS+17, SK14, TPL16, WS14].
Procedure [CS14, O Ś12].
Procedures [LCK11, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Dun12b, FBM12, Gil10, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLIC10, IEE11a, Kin11, Lin14b, Sah13].
Processing [SAK16, TKMZ13, VKPI17, BKV13, HWK+15, MS13b, PRZB12, WS14].
Processor [BH15, CLF+17, HKL+14, LB13, MBR15, YS15, ABDP15, BAB+13, BGG+13, KSH18, SSPL+13, Tan10].
Process [BF16, CLF17, ACK10].
Products [LMG18, RS10]. Professional [Sm11].
Profiles [BFC16]. Profiling [DP12].
Programs [MZ17b, Wal18, CLZ+17, GGH+16b, MFH13].
Programmable [CLF+17]. Programming [Bec17, BCF16, SY14, ASVE13, HLV10].
Progress [AB10a, BL10, BC11, GG10].
Progressive [SA16a]. Project [ACK10, SS10c, Wil18].
Proof [BDGH15, SG15].
Protected [BDGH15, SG15].
Protected [BDGH15, SG15].
Protection [CDD13, GST12, Lop12, NGAuH16, NDG+17, RR11, SEY14, SJ12, AT1+10, HLNS14, KKM+13, LVR+10, RS17, TLL13, YWT+12].
proof-key
[HLYS14]. Protocol
[BL12, BC14, BCM+15, BSSV12, BFK16, CC14, CCM17, FLH13, FMTR12, Fra16, GI12, HvS12, HC12, HL+10a, HCPLSB12, HCETPL+12, HKL+12, JTZ+16, KMO14, LNZ+13, LCCJ13, LNX+15, MBC15, MR10, PSS+13, SBS+12, SGC16, TYK+12, WT10b, XJR+17, YS12, YWF18, YWZ+12, ZXZ+11, AAT18, AIB+16, AIKC18, AN15, BDM18, BGAD12, CSD18, CCSW11, CJP15, DLK+16, EA12, FA14b, FIO15, GMSW14, GLM+11, HPC12, HL14, IC17, IOV+18, JKL+16, JXLZ15, Kim11, KO16, LLLS13, LDDAM12, LKKL13, LWS10, LXMW12, LNM12, LY14, LML+13, NCL13, NLYZ12, OHJ10, Par12b, SPLHCB14, SB17, SGJ+18, SWW+16, SSS11, SSPL+13, TG17, Tso13, TJKH14, VS11, WCF18, WZM12a, WZM12b, WMYR16, WT10a, WTT12, WCC18, XCL13, YCI12, YYZ+14, YMM13, ZWQ+11, ZTJ16, ZYC+17, ZXX+18, ZXWA18, ZG10, ZSC15, ZX11, BOB13, CJP12, LFGCCRP14, Ste15b]. Protocols
[AP13, ABHC+16, BMP12, CCK12, CCK16, CCF17, CCD15, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KOS16, LY16, MS16, MT12, Mur16, NVR+14, NSMS14, PS14, SBS+12, Sch2c, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13b, ACM12, CML+18, CR10, CLCZ10, DGJ14, FTV+10, GBNM11, GLR13, HSH11, Ham12, HPDC13, HZWW17, HST14, KJN+16, KUS13, KKK+16, LKKL13, MN10, NR11, Nos11, SD10, YSL+10]. Prototyping
[KPC+16]. Provables
[BKL12, CC14, EKB+16, Rog16, YMSH10, ZX11, ZPXX17, FA14a, HRS13, LHH11, WB12, XCL13]. Provably
[BCCGPM12, BCM12, BCPM13, BJHP14, FHH10a, GLL+18, IL15, LH11a, LL16b, PSM17, WMS+12, XJWW13, YCI12, YZZ+14, ZG10, ABBD13, FIO15, SLX16, XWXC14]. prove
[DGJ14]. provenance
[CDL18, ZOSZ17]. Provide
[Ano15a]. Provided
[KS12]. Providence
[Sch15a]. provider
[DFJ+17]. provaders
[AKK+17, BK12b, YWK10b]. Proving
[DLN13, HTZR12, KS18, MLM16]. Proving
[Sar14, AGH+17]. Proximity
[IW14, Alp18]. Proxy
[ASS15, GSW+16, GJJ15, GJZ17, HGWW11, HZX15, KP12, LSLW15, LAL+15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW+16, YMWS11, YCM+13, BGP+17, CLH+16, FSGW11, FSGW12, GH12, HWDL16, HYF18, KKM+14, LCT+14, LFS15, LL16a, LL16b, QMW17, SLZ12, SKB+17, Tia15, WHY+12, Wan18, XWXC14, YZCT17, ZLY10, ZDW+16]. Proxy-invisible
[SYL13]. Ps
[HDWH12]. Pseudo
[NN12, XYXYX11, CFY+10, KM10a, MG15, PLsdlE10, SH11, SM11, XSC10, Zim10]. Pseudo-Random
[XXYXX11, CFY+10, KM10a, MG15, PLsdlE10, SH11, SM11, XSC10, Zim10]. Pseudonymous
[BDFK12]. Pseudoprime
[DW12]. Pseudorandom
[AS17, BCGH11, BK12a, Kla10, MFG16, CP13, GCH15, HRV10]. Pseudorandomness
[Sh10]. PSMPA
[ZLDC15]. PSO
[TLL13]. PSPACE
[JUW10]. Public
[Ano11b, ABW10, BVS+13, BB14, BKL12, BKKV10, CT18, CLP13a, Che15, CNT12, Cou12, FMBM12, GKS17, HTC+15, IM14, JLT+12, KFOS12, LLSW16, LFDs10, LSQ18, LZC14, LLH18, MZH15, MPP14, MT11, Mat14, MPSR12, Mu16, NTY12, Orm16, PDNH15, RSBGN12, RW12, RBHP15, Saa12a, SK12b, SWM+10, Sia12, SC12, SLY+16, SvT10, TMC15, TT12, WP17, WZ15, WWHL12, Wil18, XNK15, XZ12, Xio12, XJWW13, YL17, YKC+11, YKF+12, YMC+17, ZY17a, AA14, AKTH+17, BS15, BS12, Durr15, HZWW17, HL14, LSLB14, LL15, LFS15, LH13, LL16a, RPSL10, SES+16, SY15b, VN17, YT11b, YYS+16,
ZZ11, ZCC15, ZCL$^+$19, ZY17b, FBM12].

**Public-Coin** [CLP13a, Mat14].

**Public-Key** [BVS$^+$13, BKKV10, GKS17, KFOS12, LLH18, MMP14, MPRS12, NTY12, Orm16, PDNH16, RSBGN12, RW12, SK12b, SWM10, SES$^+$16, VN17, ZCC15, ZY17b].

**Publication** [ZTL15].

**Publicly** [NMP$^+$13, SZQ$^+$17, YNR12a].

**Publish** [BGP$^+$17, DLZ$^+$16b, OFMR16, PRSV17, SLI11, TKR14, YSM14].

**Publish/Subscribe** [DLZ$^+$16b, OFMR16, PRSV17, TKR14, YSM14].

**published** [MYYR13].

**Publisher** [Ful10, Mur10].

**Publishing** [VSV15].

**Puebla** [AB10a].

**PUF** [BDM18, CCKM16, CCM17, DSB16, KPKS12, KLM$^+$12, MVV12, SRK$^+$17, VDB$^+$16].

**PUF-Based** [CCM17, KPKS12, MVV12, BDM18].

**PUFKY** [MVV12].

**PUFs** [IGR$^+$16].

**pupil** [MRRT17].

**punctured** [MG15].

**puppet** [Lac15].

**Purpose** [GFBF12, Gue16, ADJP15, DGJN14, KM11].

**purposes** [ABB$^+$14].

**push** [Wu17].

**Pushdown** [CCD15].

**Pushing** [FHV16].

**Puzzle** [IBM13a].

**Puzzles** [RSBG12, dCCSM$^+$12, dCCSB$^+$16].

**Py** [DGIS12].

**Py-Family** [DGIS12].

**pyramid** [MHT$^+$13].

**Q&A** [Hof15, Hof16].

**Q3** [Ven14].

**Qaeda** [Mac14, Keb15].

**QC** [JY14, HC17, VOG15].

**QC-MDPC** [HC17].

**QIM** [LJK17].

**QIP** [JY14, HC17, VOG15].

**QS** [AZPC14, HDWH12].

**Quadratic** [KRDH13, SEY14, YDH$^+$15].

**Quadraticity** [MS12b].

**Quality** [CSW12, NN12, YCM$^+$13, SS11, WZLW13, WKH11].

**Quantitative** [BL15, MBLB12, MV16b, HM10].

**Quantization** [SSA13].

**Quantization-Based** [SSA13].

**Quantum** [Ano15d, Ano16c, Ano17d, Ano17e, BB14, Ber14, BCF$^+$14, Che17, CCL$^+$13, Feh10, FKS$^+$13, Fol16, JEA$^+$15, Kar12, KP10, LKK18, LHA$^+$16, MS16, MU13, MKA$^+$17, NNA10, NA10b, QCX18, RK11, RSM15, St11, TKM12, Unr15, WCL$^+$18, Y$^+$17, ZWS$^+$18, ABB$^+$14, BJ16, CML16, Edw17, FRT13, GMP15, IM14, JSK$^+$16, KKK$^+$16, LLP$^+$18, LyWSZ10, LCW$^+$16, Lüd12, QD16, SK14, Svo14, YDH$^+$15, vDKS11, Sen10, Yan11].

**Quantum-Oblivious-Key-Transfer-Based** [WCL$^+$18].

**Quasi** [BGJT14, OWHS12, OTD10, BGJT13].

**Quasi-Chirp** [OWHS12].

**Quasi-Cyclic** [OTD10].

**Quasi-Polynomial** [BGJT14, BGJT13].

**Quaternion** [YWNW15, yWpWyYpN13].

**Queries** [HLW12, LHRK10, BVK13, CHX13, DFJ$^+$17, HMCK12, PRZB12, TKM13].

**Query** [DCA18, GA11, PCDG14, WCL$^+$18, AZPC14, BS13a, CH11, ED17, HKF$^+$15, JCHS16, LKX$^+$14, LW13a, ZHT16].

**Query-preserving** [GA11].

**Quest** [Fox13].

**question** [Cha13b].

**Quisquater** [Nac12].

**Quorum** [Kar12].

**R** [BS12, LVV11, PP10b, WYW14].

**R3579X** [BDK11].

**Rabbit** [FWSF11].

**Rabin** [Chi13a].

**Radial** [pNyWyY$^+$14, CG12b].

**Radio** [KAHK17, CJP12, CJP15, EA12, Kim11, NLYZ12, RPG12].

**radio-frequency** [CJP12, CJP15].

**radix** [BGJT14, BGJT13].

**Rayleigh** [YWNW15, yWpWyYpN13].

**Ramanujan** [KK10].

**Ramifications** [ALR13].

**Random** [Ana14, CDK$^+$10, DSB18, EAA$^+$16, FZT14, FSX12a, GSW$^+$16, Gre17, KS15, LTKP16, LPL15, NIS12, NNAM10, NN12, SC10, SRK$^+$17, TM18, WS12, XYYXYX11, XQL11, YM16, YS12, YKC$^+$11, YFK$^+$12, YLA$^+$13, ZYM18, Ara13, CFY$^+$10, CUT1b, GLM$^+$16, GLW13, HKT11, KM10a, LGKY10, LLY15, YMA15].

**RAM** [IOM12].

**RAM** [RZF+13].

**Ramanujan** [KK10].

**Ramifications** [ALR13].

**Random** [Ana14, CDK$^+$10, DSB18, EAA$^+$16, FZT14, FSX12a, GSW$^+$16, Gre17, KS15, LTKP16, LPL15, NIS12, NNAM10, NN12, SC10, SRK$^+$17, TM18, WS12, XYYXYX11, XQL11, YM16, YS12, YKC$^+$11, YFK$^+$12, YLA$^+$13, ZYM18, Ara13, CFY$^+$10, CUT1b, GLM$^+$16, GLW13, HKT11, KM10a, LGKY10, LLY15, YMA15].

**Quanitary** [BL15, MBL12, MV16b, HM10].

**Quantization** [SSA13].

**Quantization-Based** [SSA13].

Random-Grid [KS15]. Randomization [Gas13]. Randomized [ARP12, GT12, HHR11, SR12b, BWA13].

Randomness [AY14a, Ana14, ABF12, ACM+17, BWLA16, MSI10, MS16, DTZZ21, FRT13, RY10, TC11].

Range [DCA18, HMCK12, JCHS16].

Rank [SS10b, FES10]. Ranked [CWL+14, XWSW16, GZS+18, LXK+14].

Ranking [ZDL12, AT10]. Rapid [KPC+16].

Rapid [KPC+16, XJW+16, BGP+17, CFZ+10, CLH+16, CZ15b, FSGW11, FSGW12, FXP12, GH12, HWDL16, HYF18, KKM+14, LMJC11, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGT10, WHY+12, Wan18, XXX15, YZCT17, ZDW+16, LAL+15].

Re-authentication [LBR12, FXP12, LMJC11]. Re-Encryption [GSW+16, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PRSV17, WX10, XJW+16, BGP+17, CFZ+10, CLH+16, CZ15b, FSGW11, FSGW12, FXP12, GH12, HWDL16, HYF18, KKM+14, LMJC11, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGT10, WHY+12, Wan18, XXX15, YZCT17, ZDW+16, LAL+15].


Ready [GOPB12]. Real [Ano16h, Ano17d, AYS15, BFK16, BPS16, BNA15, Cer14, CC14, GSC17, JWJ+17, MK11, PNRC17, SK14, Tom16, WLZL12, YE12, AY14a].

Real-Time [AYS15, GSC17, JWJ+17, PNRC17, WLZL12, YE12, CC14, MK11, AY14a].

Real-valued [BNA15]. Real-World [Ano16h, Ano17d, BFK16, BPS16, Tom16].

realistic [FRT13]. Realization [KRM+10, MMN+16, St10]. Realizing [WKBI6, ZPWI12]. realm [OYHSB14].

Reasoning [TSH14]. Rebound [KNR10, Sas12]. recall [LTC+15a].


Recommendation [Gir15, NIS12].

Reconfigurable [HG12, HLN+10, MLCH10, NdMMW16, PP10b, PG12, SRK+17, ZLQ15, MD12a].

Reconfiguration [FGBF12, VMV15].

Reconstruction [CCM+15, KOTY17, HH15, IK15]. Record [AP13, Con12]. Records [LYZ+13, RAC17, ZVG16, LT14b, LHL15].

Recoverable [JLS12]. Recovery [Bro17, DSSD14, LYY+18, NRZQ15, SSA15, SSA13, WZ15, BM15, CHHW12, CGH17, PX13]. Rectangle [WLC12].

Recurrent [CSH+18, Pud12]. Recursive [LXLY12, WH18]. Redesigning [VFV17].

redistributed [LXCM11]. Reduced [BW12, DWWZ12, KNR10, LWZ12, LBF16, LWPF12, AY14b, LFW+16].

Reduced-Round [LWZ12, AY14b, LFW+16]. Reduction [ABR12, LCLW17, LSC+15, YMA17].

Reductions [BHK13, DW12]. Reference [LLHS12, IM14]. Refinement [BCEM15].

Refinements [LL11]. reflections [Hai17, OF12]. refractive [PHN+12].

Refresh [LSC+15]. Regaining [WBA17].

Region [CCFM12, HZW+14, KS15, FHV16].
LWLW11, WW13]. region-duplication [LWLW11]. Regions [AQD12, AKK17].
Register [TLCF16, LWK11]. Registers [LLGJ16, ZH15]. Registration [ISC16].
Regular [CQX18, Wat12, WR15].
regular-expression [WR15]. regulating [DFJ10]. regulator [BP10].
regulatory-compliant [BP10]. Reinforcing [WXY17]. Rejewski [Kap13].
Rekeying-Aware [QLL17]. Related [Cil11, CMA14, DGlS12, HLLG18, Pud12, WLC12, MPN12].
Related-Key [CMA14, HLLG18, Pud12, WLC12, DGlS12].
Relational [HPC10, RP12, WP17, BFG10]. Relations [BP11, FHS13, HLR11, WGD18, KGO10].
Release [KFOS12, RSBGN12, Umr15, WSS12].
Relevance [Sim15a]. reliable [CZ14].
Reliable [AMKA17, ADG16, Bai10, CC14, WKB16, ACD15, CL16, ZC12].
Renewal [MMY12]. rental [LY14].
Reordering [Ala12]. Repairing [BCM12, BCM13]. Repeatedly [TAKS10, ATK11].
Repeat [jCPB12]. reports [RPG12].
Repositories [Ano15a]. repository [RSM15].
Representation [AGW15, BFMT16, MHT13].
Representation-Based [AGW15].
Representatives [Bla16]. reproducible [CW12a]. Repudiation [LG15].
Repurposing [GY13]. Reputation [BLi5, LHM15, PAS13b, MGP10].
Reputation-Based [PAS13b]. Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13].
Requirements [OS16]. requiring [KHHH14]. Rescue [TSH17].
Resettable [CPS16]. Resettably-Sound [COP14].
Resistance [CFG12, PRC12, WLZ12, ZJ11, DLN13, FI015]. Resistant [BK12a, CDK10, GV14b, HF14b, WHZ12, WG12, WH17, YPRI17, GMR15].
HCCI10, PBCC14, VCK12, WTT12, YKGV13. resisting [SXL16, Tan15].
Resource [DSB16, TLCF16]. Resource [CSH18, JMG16, SZMK13, YNR12a, AMH10, FQZF18, KAS15, LLZ16, MHV15, WM16, XWZW16, ZPZ16].
Resource-Constrained [CSH18, YNR12a, LLZ16]. Resource-efficient [SZMK13, XWZW16].
Respiratory [RSC18]. Response [GHS14, HLKL15, ZHW16, MRRT17].
Resprinting [TBC15]. restoration [WHZ12]. restricted [CLH16]. result [ACK10, ED17].
Results [DGJS12, LJF16, Hof16, GJG10].
Rethinking [Cela13]. Ruin [HUI5, LSG16, MV16a].
Retrieval [BBB16a, BTHJ12, CJP12, HK14, JMG16, JKH12, Yek10, XZ11, CJP15, SWW17]. returned [War11].
reusable [RS17]. Reuse [ABF12]. Reveal [Sta13]. Revealed [Uno15d]. Revealing [BT12, KK12, KK13]. reverse [TQL14].
reversed [KY18]. 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, Bail12, Bar12, Cou12, Dew11, Full10, Gas13, Joh10, Kat13, Keb15, Koh10, Led16, Lop15b, Loc12, Me10, Mou15, Mur10, Sch15a, Sha10, Ter11, Xie12, JAS+11, MM12, TPK12].

**Reviewed** [Sch15a]. **Reviews** [SR14].

**Revised** [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11].

**Revising** [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11].

**Revising** [LT14b]. **Revisited** [CLY14, DKPW12, DKS12, GWWC15, KFOS12, LL11, Lop15a, PKTK12, Sar12, Tan12a, BCL14, HKT11, HYWS11, TS16a, ZCL+12].

**Revisiting** [TL12, WAS15].

**Revocability** [WHLH16]. **Revocable** [AEHS15, CD16, QZZ18, SE14, SE16, SZS14, SZDL14, TCL15, TT12, Unr15, FLL+14, WLFX17, WTT12].

**Revocation** [AEHS15, LLC+15, LW16, Lop15b, RDZ+16, XMLC13, YWZ+12, ATK11, LJWY18].

**Revoking** [TAKS10]. **Revolutionized** [Orn16]. **RFID** [CJP15, AATM18, BL12, BSSV12, BM11, CGCGPMG12, CCF17, CJP12, Ch14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, GAI+18, HSH11, HDPC13, HQY+16, HCLPSB12, HCETPL+12, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLsdlE10, QZL+16a, QZL+16b, SBS+12, SPLHCB14, TG17, WH17, WCFW18].

**RFID-Enabled** [QZL+16a, QZL+16b]. **RFID/NFC** [Mic16].

**RFIDs** [KOP12]. **RGB** [SNM14, ST16]. **RI** [Sch15a]. **Rich** [CS12]. **Richman** [Xie12].

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

**Rightful** [RR11]. **Rights** [LVRY10].

**Rigorous** [DK17]. **Ring** [GHS12, HKL+12, XY18, YKBS10, YLA+13, ZJ14, DZ14, Hwa11]. **Ring-LPN** [HKL+12]. **Ring-LWE** [XY18]. **Rings** [YM16]. **rise** [Ano14]. **Risk** [Zha15b, PKA15]. **risks** [Lan10, SS17].

**RKA** [SLY+16]. **RKA-Secure** [SLY+16].

**RLCPS** [DDS12]. **RLWE** [ZXJ+14]. **RNG** [CGH17]. **RNGs** [DSDDW14]. **RNTS** [PSOMPL13]. **roaming** [SCHK10, XZ11].

**Robbery** [SPW+16]. **Robert** [Grec11].

**Robotic** [SPW+16]. **Robust** [BCGAPM12, BCG12a, CFFR12, GKS17, HZC+12, JSZ12, LSL12b, LSR13, MR16, MU12, MS16, MC11, pNwyY14, OC11, RR11, RMG18, SJ12, SC12, SZT18, TLF16, TK14, TTL10, WLB11, WgMzdZ12, yWpNyY14, XNG+14, YWNV15, YYO15, APA18, AIA+18, CLM+12, EAA+16, GZH12, HZC+14, HZL18, IOV+18, LNK+18a, LW10, PKS18, RS17, yWpNyL11, yWpWyYpN13, YSL+10, ZHH+17]. **Robustness** [HGT15, YKBS10, AEH17]. **ROCA** [Ano17f]. **Rochefort** [Car11]. **Rock** [Cri16].

**Rock-solid** [Cri16]. **Rodney** [DDS12].

**Rogozin** [Kuz11]. **Role** [PH12b, ZV16].

**Role-Based** [ZV16]. **Ron** [LH+12].

**Room** [Smil11b, Pea11]. **Root** [ARH14].

**Rosen** [HR13]. **Rosenhain** [CDSLY14].

**rotation** [LWLW11]. **Rotational** [KN10, KNR10]. **Roulette** [Ber17]. **Round** [Ber17, jCPB+12, COP14, DWWZ12, GGHR14, KOTY17, KMO14, LWZ12, Lj17, Pan14, TCM+17, XL15, Yon12, AY14b, ABM+12, Bl05, LP11, LF+16, Sun11, TSL11, TQL+14, TCS14, XW12].

**Round-Reduced** [DWWZ12]. **Rounds** [GST12, Sas12, LYHH14, MNP12]. **Router** [Bis17, SA15]. **Routing** [Ham12, KZG10, WLY+15, LSG16, LC17].

**RSA** [Dun2b, K1a11, Pie10, APPVP15, BBBP13, Bro17, BNST17, CLSW12, Chm10, GM13, GST13, Her14, Hin10, HLYS14, IK15, KHH14, KFL+10, Lim11, Moo12, SM10a, SM10b, SLM10, Win17, YHK+10, YXA+16].

**RSA-1024** [Bro17, Win17]. **RSEL** [FLL+14]. **RST** [LD13]. **rubber** [BSR+14].

**Rule** [KWP13, NC12, TW12, McG11].


Scal [YTS12, SKH15]. Scale [DM15, GU13, JKHeY12, LQD+16, CG12b, dCCSB+16, FX12, GSN+16, SR10, ZZKA17]. Scan [LWK11, DDFR13, KPS10]. Scan-based [LWK11]. scanning [Ara13]. Scattering [KA18]. Scenarios [DSB15]. Scheduling [MV16b]. Schema [AN12]. Scheme [ASS15, Bai10, BHG12, BS14, BKJP12, BDH11, CMGLS15, CLL16, CCW+10, CLHC12, CHHW12, CZZC12, CGY+13, CLH13, CSW12, DA10, DS11, DKS12, FR16, FGM10, GZZ+13, GH11b, GJZ17, GLW12, GZHI7, HYS11, HIDFGPC15, HMR12, HHP17, Hî+13, HP12, IL15, JZS12, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KL+13, LSL12b, LHF12, LTH+15, LTZ16, LH11b, LGYW12, LTC+15b, LYY+18, LGPRH14, MWZ12, MVVR12, MRL+18, MNN12, MSA12, NX13, NLLJ12, NY15, Pet12, PDT12, RVH+16, RMG18, SK12a, SJ12, SGP+12, SD12, She14, ST12, SP15b, SJWH+17, SSA13, Tan11, TTD13, TW11, WT10, WgMdZ12, WgMW12, gWpNyY+14, WLH15, XWSW16, XCH+12, XJW13, YM16, Yami12, YZX+12, Ye10, Ye14, YTH17, YL17, Y+17, YHK+10, YMW11, ZP+15, ZC13, ZQ15, ZLDD12, ZY17a, AMN18, AHS14, AYK+18, AKK+17, BO13, BAL10, BMM12, BB16b, CCLL11, CLSW12].

scheme [CH10, CT11a, CHJ13, CW14a, CTHP13, Cho14, DSCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, FHZW18, GZHD12, GJ13, GMRT+15, GLM+16, GH16, GAI+18, HZW18, HBBRM+16, HLI1, HCC11, HLC16, HCC11, Hwa11, IB11, JNUH17, JLT+12, JZS+10, JMW+16, KI11, KPP16, KDH15, KK13, KHMB13, KM+13, KKM+14, KKG14, Kim16, KP18, KLW+16, KDW+17, KWH16, KL11, LXY12, LL16, LS13, LH10c, LZJX10, LNM+11, LMJC11, LK12, LLHS12, LNN13, LNK+17, LNK+18a, LWK+18, LK+18b, LFWS15, LH13, LH11, LWW10a, LWL11, LW13b, LZZC14, LL16a, LL16b, LW12, MCN+18, MMS17c, MK12a, MS13, NR17, Nos14, PZBF18, QMC17, QMW17, RPSL10, SGCR+16, SM11, Tan12b, TY16a, TK14, TD14, TLL13, TLI2, UN11, WWY11, WWYY11, yWpNyL11, WLH13, WDLZ13, WLZ+16, WLFX17, Wan18, WZ11, WKH11, WOLS12, WXK+17, XHS12, XJW16, XWC14, XMX15, XMHD13, YC11, YC16, YHMM18, YWK+10a, YCT15].

Schemes [YXD18, YMSH10, ZYL+10, ZLY10, ZX1+14, ZYC+17, ZPYY12, ZHH+17, ZY17b, ZFH+18, ZC12, ZBR11, DT13, LLZ+12].
Schneier [Sev16]. Science [Bow11, Gas13, IEE10, IEE11b, Ter11, Bia12, PHWM10, Pet11]. scientists [Goo12]. Scientometric [Pal15, Pal16]. Scope [Bai12]. Score [GCSAddP11]. scoring [OSSK16]. Scrambling [LLL17]. Screen [SPW¹+16, CTL12]. Script [Rao10, Bax14]. Scripting [DSB15]. scroll [GMOGCCC15]. SDB [HWK¹+15]. SDDO [PL¹+16]. SDDO-based [PL¹+16]. SDH [GMS11]. SDIVIP [YNX¹+16]. SDN [KCC17]. SDVS [Wan10]. SE [LLLS13]. SE-AKA [LLLS13]. seals [MN10]. Seam [LC¹+15]. Seam-Carved [LC¹+15]. Search [CWL¹+14, Che15, DCA18, FRS¹+16, GTT¹+11, HCDM12, LSQL18, TMC15, WDC18, WW¹+12, XWSW¹+16, XJWW¹+13, ZXYL¹+16, BL¹+11, CLH¹+16, FH¹+13, FSGW¹+12, GZS¹+18, HH¹+16, OSSK¹+16, SY¹+15b, WHY¹+12, WXLY¹+16, XXY¹+18, YXD¹+18, ZZ¹+11]. Searchable [BHJP¹+14, CWWL¹+12, CLW¹+16, CGKO¹+11, FJHJ¹+12, PCY¹+17, XKNG¹+15, DLZ¹+16a, DRD¹+11, HQZH¹+14, JCHS¹+16, LZC¹+17, LLL¹+18, RPSL¹+10, WXLY¹+16, WCCH¹+18, YZCT¹+17]. Searches [Sia12, WR¹+15]. searching [GPN¹+12]. Seattle [LCK¹+11, KCR¹+11]. Seberry [AHS¹+14]. SEC [PA¹+10]. Second [AKY¹+13, ABM¹+12]. Secondary [RS¹+11]. Secrecy [ABD¹+15, BKST¹+18, KZG¹+10, TSH¹+14, Yon¹+12, ATK¹+17, Bia¹+12, RCW¹+15, TCS¹+14]. Secrecy-preserving [TSH¹+14]. Secret [ASN¹+11, ASN¹+12, ADH¹+17, Ayu¹+12, Bai¹+10, BBB¹+16a, BFM¹+12, BBP¹+14, Bri¹+11, CCM¹+15, CFR¹+12, CCL¹+13, DR¹+12, Dew¹+11, EM¹+12, EH¹+15, FR¹+16, Fok¹+12, HYS¹+11, HL¹+10a, Has¹+16, KU¹+14, KS¹+18, KOT¹+17, KI¹+12, KI¹+13, KSS¹+12, KS¹+15, LHF¹+12, LPL¹+15, Lin¹+15, LCC¹+13, LTC¹+15b, LJ¹+16, LLKA¹+19, Men¹+13, MNS¹+11, NS¹+12, Oba¹+11, PCPK¹+14, QS¹+18, SLL¹+10, SC¹+10, SI¹+10c, SSU¹+12, Sti¹+15, TL¹+12, TWZ¹+11, WKB¹+16, WGF¹+16, Wu¹+18, XZY¹+12, XJR¹+17, YFF¹+12, YWZ¹+12, ZC¹+13, Ald¹+11, AG¹+16, AKK¹+17, Ara¹+13, BJ¹+16, Bud¹+16, Cha¹+13c, CT¹+11b, CW¹+14a, CLZ¹+17, DD¹+13, EEA¹+13, EZ¹+15, FHH¹+10a, GM¹+15, GL¹+13, FRI¹+14a, HH¹+15, Hea¹+15, HBBRNM¹+16, HCCI¹+11, HLC¹+12, KI¹+11, KU¹+16, LX¹+12, LT¹+13, LyWS¹+10, LHYZ¹+12, LEW¹+19, Mas¹+17, McK¹+10, McK¹+11, MB¹+11, OTO¹+11, Pea¹+11, Pet¹+10, QD¹+16, Rus¹+15, SB¹+17, SA¹+12, SAR¹+18b, TCL¹+14, TD¹+14, UU¹+11]. secret [UU¹+13, WYL¹+13, WZ¹+11, WS¹+12, WOLS¹+12, Wu¹+17, WX¹+13, YC¹+11, YCC¹+16, YSC¹+16, ZC¹+12, ZI¹+15, ZPY¹+12, LSC¹+15, Bia¹+12]. secret-key [BJ¹+16]. Secret-Sharing [BBP¹+14]. Secretion [RSCX¹+18]. Secretocracy [Ber¹+16b]. Secrets [BT¹+12, CG¹+14b, DLW¹+11, FMS¹+12a, KOb¹+10, Man¹+13, Bha¹+16, Cop¹+10b, GG¹+16b, Gup¹+15, HRS¹+13, Smi¹+11a, Ano¹+17b]. Secure [ADMM¹+16, AAR¹+12, Ash¹+14, AMH¹+16, BVS¹+13, BWL¹+16, BC²+17, BCG¹+12a, BQ¹+13, BWA¹+13, BLJ¹+12, BHJP¹+14, BF¹+11, Bru¹+12, BDH¹+11, BCEM¹+15, CFR¹+12, CCM¹+17, CZF¹+12, CZL¹+14, Che¹+15, CMA¹+14, DM¹+18, DL¹+15, DMS¹+16, DG¹+15, DLZ¹+16b, Edw¹+17, FLH¹+13, Fri¹+10b, FD¹+11, FSX¹+12a, zGXW¹+12, GKM¹+16, GGH¹+14, GF²+12, GT¹+12, GV¹+14b, GHKL¹+14, GM¹+14, GZ¹+18, Hv²+12, HSM¹+14, HLL¹+18, Har¹+16, HL¹+10b, HP¹+14, HTZ¹+12, HMCK¹+12, HLKL¹+15, HYS¹+18, HK¹+14, IL¹+15, Jac¹+16, KW¹+14, KME¹+12, KUp¹+15, KH¹+10, LJS¹+14, LL¹+15, LH¹+12, LYZ¹+13, LTH¹+15,
LTZY16, LSLW15, LLGJ16, LSQ18, LY15, LHL15, LLML12, LSC12, MLO17, MMP14, Mal13, MVVR12, MMS17b, MK12a, MKAA17, NBZP17, NDG+17, NR12, NMS14, NSMS14, PB12, PSM17, Per13, QZL+16b, QZDJ16, QZZ18, RMP10, Rea16, RSOG15, SNJ11, SZS14, SVC15, SP15b, SKH17, SRAA17, SAR18b, SSAF11, SVG16, SYW17, SYC+17]. Secure
[SMS14, SZDL14, SGH15, SLY+16, SR12b, TB18, TCL15, TWZ11, TGC16, VMV15, WgMW12, WKB16, WXLY16, WLY17, WDC18, WLI15, WBA17, WWHL12, WMS+12, tWmC12, XWSW16, XJWW13, YNR12a, YN12b, YTH17, YHK+10, YKC+11, YAM+15, YGD+17, ZXX+11, ZDL12, ZVG16, ZHT16, ZLW+17, ZBR11, AHS14, APK+18, ABBD13, ACF16, AKL+17, ACD+15, BOB13, BSR+14, CCLL11, CSL18, CLHJ13, CW14a, CS11, CDL18, FHI10a, FLL+14, FS14, FA14b, FIO15, FS18, Gal13, GAI18, GLL+18, GCH15, HG16, HGWY11, HHW+15, HL14, HPY10, IB11, JZS+10, KPP16, KKA14, KRM+10, KTV16, KDW+17, LLCS13, LDM12, LHL11, LLW16, LSR13, LWK+18, LCT+14, LAL+15, LL16a, LL16b, LBOX12, MR14c, MMY+18, NRI17, NACL12, NAL17, PS0+13, PSLvLE10, Rao17, RG10, RYF+13, RIT+11, RS15, SGCR+16, SYL13, SWW+16, SSS11, SSPL+13, SXL16, Tar10, TLMM13, TLI12, VS11, WLZ+16, WMX+17, WCH18].
secure
[XWXC14, XXX15, YC12, yYqWqZC13, YZZ+14, YZCT17, YY11, YLS12, YMSH10, ZLY10, ZCLL14, ZZ15, ZYC+17, ZG10, ZZ12, ZX11, ZY17a, ZC12, Zhu13, ZSW+18b, Ano12, DSB18, OKG+12, YSS14, YFK+12]. Secure-TWS [OKG+12]. Secured [LC17].
Securely [CC10, KP17, LHL+14, MS16, WXY+17, BC18, der10]. Securing
[BK12b, CMLS15, CST+17, NPH+14, PMZ13, SFE10, SMSK18, SLI11, Ste15b, TKR14, YMA17, YT12, CR10, Din10, SKS+18, SA15, Tox14]. Securities
[WWL+14]. Security [ABJ13, ASBdS16, Ano13d, Ano15a, Ano15d, ABF12, AN15, ABHC+16, AYS15, BCE+10, BCM+15, BRT12, BPR14a, BPR14b, BLS12, BCGN16, BDP12, Bra15, BDH11, BIP10, CFST17, CFE16, CHS11, CFXY17, CCD15, CPS16, CM11, DDS12, Dan12, DR12, DFKC17, FMA+18, FSX12b, FSX12c, GZZ+13, GSC17, HC12, Hel17, HB17, HLW12, HXI+11, HLC11, HLT+15, HLN+10, IS12, IGR+16, JN12, Jia14a, KBL11, KS18, KFOS12, KSD+17, KD12b, LPS12, LST12, LW11a, LK14, LW12, LLZ+17, LT11, LSQ18, LP12, LRIW17, LHC12a, LDB+15, LMS16, LLH18, MTY11, MKN13, MCS+15, MH14, Mau12, MV16a, MLBL12, MPM+17, Nac12, NNAM10, NDG+17, NVM+17, Nos11, Nos14, Orm16, OS16, Pas13a, PZPS15, PDH15, PS14, PL16, PDT12, PNRC17, RCP+18, RQD+15, RWZ12, Rog16, RS10, SN10, SNJ11, SBS+12, Sar12]. Security [Sch13, SD12, Shi11, SL10, STC11, SMOP15, SCGW+14, Tso13, TV15, Wal18, WYCF14, WS15, WSS12, WCL+18, WS14, Yan10, YZLC12, YGS+17, YSS14, Yon11, Zha15a, ZY17a, vTF11, AMN18, AB10a, Abe10, ABGR13, ABM+12, Ano11a, ADH17, BYL10, BSI11, BDL+11, BL17, BM11, BL11, CO11, CTHP13, CLCZ10, CVG+13, DLK+16, DHW+13, Edw14, FHM+12, FA14a, Fis15, GM16, GLM+16, GMS11, GH12, HDWL16, HWG10, HLR11, HRS13, HLV10, KAS16, KKK+16, Lan10, Lan13, LH10a, LXMW12, LH11, LHC14, LSG16, MZA+13, Men13, MM14b, MS+18b, NS10, NLC13, NLYZ12, OK18, OYHSB14, PHWM10, QYWX16, Ree15, RPS10, RH10, SA12, Ser12, SLZ12, SY15b, Sir16, Sta11a, Tan17b, TODQ18, UUN11, VCK+12, WCFW18, XCL13, Zha15a, XW12, YKC+12, Bar12]. Security-Aware [LMS16]. security-enhanced [AMN18].

Selected [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12].
Selection [KD12a, RP12, SEY14, FXP12].
Selective [BLTJ12, GDCC16, LW12, LSC+15, LZC12a, LLH18, 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-Synchronizing [HZ11].
Self-updatable [LCL+17a]. SELinux [SFE10]. seller [KJN+16].
Sematic [YZCT17, HLR11]. Semantics [CM11, Gli12, KGP12].
Semi [BDOZ11, KKK+16, WHZ12, XZLW15, PGLL10].
Seminarty [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, LW+10]. Sensor [ABC+17, BN14, CS14, DS11, KH10, LLC11, LLZ+12, NNM10, NYR+14, OKG+12, PX13, PCPK14, RWLL14, SP15b, YM16, ASO14, APK+18, AIB+16, AIKC18, ADF12, BLAN+16, BBB16b, CDGC12, CLSW12, DSCS12, DLN13, HTC+10, JNUH17, JM+16, KLC+10, KO16, KKW+16, KDW+17, LC17, LNK+18b, PL16, SZMK13, SKK10, Wan13, WW14, WXX+17, XWDN12, XMHD13, ZYL+10]. Sensors [DL12, LK+17]. Sensory [SGC14]. Seoul [LH10a, LW11a]. separation [MJS13].
Sequence [PF12, WZG+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, CS18, CLHJ13, FA14b, FHZW18, HDPC13, HL14, ISC+16, LXMW12, LH13, SY15b, hSZZ15, SSAF11, SSS11, TLL12, WT10a]. Server-Aided [GMSV14, LYL15, SSAF11].
Server-Designation [Che15, LSQL18].
Server-Side [BCO13]. servers [DRD11].
Service [KBK14, CCSI14, Hay13, LDB+15, LBR12, NRZQ15, RSGG15, SSPC12, Sti15, VS16, AaBT16, KPP16, LHL+18, LW13a, MLM16, Par12b, Wu17, YWK10b, ZXX1, YCM+13].
Service-Based [LDB+15].
Service-Oriented [RSGG15]. Services [AN11b, DLZ+16b, MEFO12, OO12, ZHL15, AZPC14, CDS18, CHX13, GAI+18, IMB17, IG11, NZL+15, PP11, XXX15]. Session [BS12, BKJP12, CFST17, HS12, AN15, DCAT12]. Session-Based [BKJP12].
set [Cor14b, EKP+13, YZ12, Con12, TMK11].
set-valued [TMK11]. sets [SF12]. Setting [BKLS12, HHP17, MZH15, TYM+17, XXZ12, ZHL15]. Settings [CZ12]. setup [Jia16].
Several [Sas12, ZT14]. SGX [WBA17]. SHA [AAE+14, ABM+12, App15, jCPB+12, LC17, MAK+12, SKP15]. SHA-1 [AAE+14, SKP15]. SHA-256 [App15, MAK+12]. SHA-3 [ABM+12, jCPB+12, LC17]. SHA1

Shapes [CJFH14, LMHH14, SY14, SGS14, ZZCJ14]. Share [LTC+15b, ZPWY12]. shareable [XWY+18]. Shared [DRD11, LNXY15, OKG+12, ZPWY12]. shared-secret [SA12]. Shares [CFOR12, KU14, SA16a, WY12]. Sharing [Bai10, BFM12, BBEPT14, CCM+15, CFOR12, CCL+13, CCT+14, CLW16, DR12, EM12, FHKP17, FR16, HIS1, HL10a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KS15, LYZ+13, LPL15, Lin15, LCCJ13, LTC+15b, LLKA19, NS12, Ob11, PSM17, QZZ18, SC10, SSU12, SZZT18, TLW12, TWZ11, WYCF14, WKB16, WGF16, XNKG15, XYZ+12, YFF12, YWZ+12, ZC13, AKB+17, ADH17, CT11b, CW14a, EZ15, EAI1, FGMP12, GJMP15, GLW13, GLB+18, HF14a, HBBRNM+16, HCCC11, HLC12, HYF18, KI11, KU116, KBP17, LXY12, LT13, LFWS15, LAL+15, LyWSZ10, LHYZ12, LHL15, LLL+18, LEW19, LL16a, Mas17, O100, O101, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WKH1, WS12, WOLS12, YC16, ZCL+12, ZZ15, ZPWY12, SLL10]. Shell [WZCC18, YS14, Tay14]. Shenzhen [IEE11a]. Shield [NDG+17, KGV16]. Shift [AKP12, ZH15, LWK11]. Shift-Type [AKP12]. Shifting [YWW10, CSS+13].


Shi [Cra12]. Side [AN17, BCO13, CF16, CDK+10, CBL13, DMWS12, DKMR15, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, SR12a, Via10, YL17, BVIB12, DJL+12, MFI13]. Side-Channel [CBL13, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, YL17, DMWS12, BVIB12, MFI13]. Sided [BP14]. Sift [VM14].

Signal [KU14, SA16a, WY12]. Sharing [Bai10, BFM12, BBEPT14, CCM+15, CFOR12, CCL+13, CCT+14, CLW16, DR12, EM12, FHKP17, FR16, HIS1, HL10a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KS15, LYZ+13, LPL15, Lin15, LCCJ13, LTC+15b, LLKA19, NS12, Ob11, PSM17, QZZ18, SC10, SSU12, SZZT18, TLW12, TWZ11, WYCF14, WKB16, WGF16, XNKG15, XYZ+12, YFF12, YWZ+12, ZC13, AKB+17, ADH17, CT11b, CW14a, EZ15, EAI1, FGMP12, GJMP15, GLW13, GLB+18, HF14a, HBBRNM+16, HCCC11, HLC12, HYF18, KI11, KU116, KBP17, LXY12, LT13, LFWS15, LAL+15, LyWSZ10, LHYZ12, LHL15, LLL+18, LEW19, LL16a, Mas17, O100, O101, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WKH1, WS12, WOLS12, YC16, ZCL+12, ZZ15, ZPWY12, SLL10]. Shell [WZCC18, YS14, Tay14]. Shenzhen [IEE11a]. Shield [NDG+17, KGV16]. Shift [AKP12, ZH15, LWK11]. Shift-Type [AKP12]. Shifting [YWW10, CSS+13].

Similarity-aware [ZFH+18]. Simon [AMS+10]. Simple [AMH+16].
CZF12, LYY+18, Ros11, Sar10b, Sma16, TDT13, ZH15, Zim10, CLM+12, MMS17c.
Simpler [TH16]. Simplified [PS12].
Simulation [CPS16, LLH18, MS13a].
Simulation-Based [LLH18], simulations [Ana14]. Simultaneous [YWZ+12].
Singapore [Abe10]. Single
[ABK13, LL15, MEF012, Sas12, SPM+13].
Single-SP [Sas12]. Singular
[LSLI2b, BWA13]. sins [HLV10]. SIP
[KKGK10, ZTZ16]. SIP-based [ZTZ16].
SIPF [SYC+17]. Site [DSB15, SS10c].
siteDriverID [SGGCR+16]. Size
[AS17, AEHS15, CJ13, CSW12, EAA12, Kim15, LCLL15, MTL11, ZMW16, AHL+12, LCT+14, PPTT15, SGM16].
Size-Constrained [EAA12]. Skein
[FLSI+10, KNR10]. Skin [AQD12]. skyline
[BKV13]. Slantlet [TK14]. Slicing
[MZ17b]. Slide [IOM12, LC13]. Sliding
[BBG+17, Bro17, Win17]. stLiSCP
[ARH+18]. SLMAP [HCETPL+12]. Slow
[Smi11b]. Small
[BGJT14, BKLS12, BB10, CJ13, Kim15, LCLL15, YM16, AAT16, BGJT13, Jou13].
Smart [AN17, ABCL17, BSJ15, DLZ+16b, HCL+14, LA10, MFG16, PDT12, WgMdZ12, WgMW12, AMN18, CHS11, CLHJ13, GAI+18, HCC10, LH10c, LNM+11, LXM12, LNKL13, LNK+18a, LTC+15a, MM12, MCN+18, WMYR16, YZZ+14, YSL+10, Cho10, GLC10, SD12].
Smart-Card-Based [HCL+14].
Smartphone [MDMJ17, uHAN+18, DL15].
Smartphones [Cor14b]. smashed [Fag17].
Smith [Ano16g]. Smooth
[XYYYX11, YC11, ZBR11]. SMS
[KRM+10, PSD0+13]. SMSCrypto
[PSD0+13]. Snakes [PC16]. SNOW [PC16].
Snowden [Tox14]. SoC [GSC17]. Social
[BPSSD17, KTA12, NSA15, NRZQ15, PYM1+15, Rog16, SKGY14, SZZT18, WLY+15, ZW15, ZHa15b, ZHL15, BDK11, HYF18, LCM+17, LZC17, MSM+18b, SKS+18, Sni15a, YZL+18]. Society
[Sch15a, Sch12b]. Socio [NS12].
Socio-Rational [NS12]. SoD [VN16]. Soft
[JJ10, TLCF16, SS17]. Soft-Error
[TLCF16]. Softw [WZM12a]. Software
[Bar15, Bee17, EWS14, LRWV14, MRL+18, MV16a, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GLJ+12, HLV10, KH10, LBOX12, SF12, YWT+12]. Solan [CGB+10]. solid [Cri16].
Solution [Fra15, GSFT16, HLKL15, Kam13, NA10b, YFT17, Cor14a].
Solutions [LLGJ16, BLV17, KAS15, WW14]. Solved
[IBM13a]. Solving [Ano17c, BB10, Bul10a].
Some
[AD12, Ber12, Dur15, LWL10b, Mid10].
Somewhat [KOS16, MBF18]. Song
[Con12]. Sood [MWZ12]. SOSEMANUK
[PC16]. SOT [PAF18]. SOT-MRAM
[PAF18]. Sound [COP14, LSR13, Sav15].
Source [Bis17, FKO15, MBC15, RWLL14, ABF+14, LZC17, PX13, Pow14].
Source-Based [MBC15]. Sources
[DHB16, BJ16, SSY12]. South
[BL10, LWL11a]. Soviet [Bud16]. SP
[Sas12, SEHK12]. SPABox [FGR+17].
Space [BWR12, BLK+13, NRY+14, RMG18, MSM+18b, RYF+13, ZZ15].
Space-Filling [BWR12]. Spaces [SH15].
spam [SKEG14]. Spanish
[Pet11, SGGCR+16]. Sparse
[AGW15, AAT16, BBC+13]. SPARTA
[MMS+17a]. SpartanRPC [CS14]. Spatial
[AV12, CZF12, PDMR12, CW14b, NZL+15].
Spatiotemporal [DMT12]. Speaker
[BJCHA17, PPRT12]. Special [Ano13d, Ano16a, Ano16b, Ano16h, AB10b, CSYY18, GO17, LW13a, LLK18, PHWM10, XW13].
Specific [BDFK12, KME+12].
Specification [SK11, SD10]. Specifications
[BMP12]. SPECK
[LFW+16, AMKA17, BSS+13]. Spectrum
[KD12a, TWZ+12, XNRG15, KBP17, LHY12, MMS13]. Spectrum-Based
[TWZ+12, XNRRG15]. **Speech**
[AGW15, LJK17, SAA15, YMA17]. **Speed**
[ARM15, GL12, HZ11, KP17, LTKP16, BDL+11, KL13]. **Speeding** [RVRSCHM12].
**SPEKS** [Che15]. **spell** [Bha16]. **SPHINCS**
[BHH+15]. **Spies**
[Has16, Keh15, Fag17, Mac14]. **Spintronic**
[IGR+16]. **Splicing** [YSC+15]. **Spline**
[Tan12a]. **Split** [CG14a, XZ+12].
**Split-State** [CG14a, XZ+12]. **Splittable**
[CP13]. **SPN** [LCW17]. **Spoken**
[WBC+10]. **spoon** [BDP11].
**SPONGENT** [BKL+13]. **spotty** [OS11].
**Spoof** [SP13a]. **spotty** [OS11]. **Spread**
[HGT15, KD12a, PSJ+13, TWZ+12, XNRRG15, LWY12, MMSD13]. **spreadsheets**
[LT13]. **Springer** [Mei10, Mur10]. **Springer-Verlag** [Mei10]. **Springs**
[IEE11b]. **Spritz** [RS11]. **Spy**
[AHS13, FKOV15, Bha16, Goo12]. **SQL**
[BS13a, Suc12]. **Square** [ARH14].
**Squashing** [GH11a]. **SRAM** [KLM+12].
**SSH** [YSY14, Cri16, Lit14, Ran10, der10].
**SSL** [BJR+14, Dav11, FH+12, GJ+12, HREJ14, NH+14, PP11]. **SSL/TLS**
[BJR+14, Dav11, PP11]. **SSL/TLS-based**
[PP11]. **SSO** [MLM16]. **St**
[DSS12, Dan12, MNS11]. **ST-Numbering**
[MNS11]. **stack** [JSM+18], **stage** [Mas17].
**STAMP** [WPZM16]. **Standard**
[Ano12, Ano13a, App13, ABC+17, BCM12, BV11, BV14, CT18, GJ15, GJZ17, HZX15, Loe15, MVVR12, OK+15, SZS14, TCL15, WWH12, Yon12, ZC13, BCM13, Kim11, LST12, LL16b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, ZCL+19, AER17, MKRM10, NdMWM16].
**Standardization** [TRD11]. **Standards**
[BCM+15, Che17, DHW+13, NIS13]. **State**
[BVS+13, BLM17, CG14a, CCL+13, CHS15, Dew11, DP17, FHR14, LKL18, MKF+16, Sen17, WGD18, XZ+12, BBDL+17, CK11, CGH17, Ham12, Id10, QD16, Sir16].
**Stateful**
[BVS+13, NTY12, VKP17, VSR12]. **Stateless** [BHH+15, GM11, MKAA17, NTY12, VDO14, DCAT12].
**Stateless/Stateful** [NTY12]. **statement**
[NIS13]. **Static**
[DKMR15, IF16, Lan11, TLMM13]. **Station**
[Smi11a]. **stationary** [ZLD12]. **Statistical**
[Böh10, Bro11, DBPS12, HZ11, Hey17, LTKP16, OOR+14, SP13, Sim15a].
**Statistical-Attack** [SP13]. **Statistics**
[gWpNY+14]. **Statutory** [PH12b].
**Stealing** [RW12]. **Stealthy** [BRPB13].
**Steering** [HR13]. **Steganalysis**
[Böh10, DA12, Fri12, JHHN12, KD12b, LJK17, LC15, SGP+12, Tan12a, YLL+12, Y14, YPR11, LSQ11a, LSQ11b, Sch12a].
**Steganalysis-Resistant** [YPR11].
**Steganalytic** [Ber18, YPR11].
**Steganographic**
[DA10, HHS+15, LyWIZZ12, WP15, AGLW16, LLC10, CAC14]. **Steganography**
[AGW15, BCG12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZ+14, Joh10, LJK17, LLY+12b, MAL10, PDMR12, Paul10, SK12a, SR12b, TJZF12, WWL+14, YW10, ZSA12, AOT13, BDK11, BHCdFR12, EEAZ13, GKCK11, LyWSZ10, LRW13, LRW17, LWW+10, Maz13, MSM+18b, MS17, PHN+12, SI12, Sun16, WKH11, WOL12, ZMS14]. **Stego**
[YLL+12, SMSK18]. **Stego-Image**
[YLL+12]. **Stellenbosch** [BL10]. **step**
[AKY13, YX+18]. **Steps** [Ano13c]. **STES**
[CMS15]. **Steven** [Led16, Sch15a]. **Still**
[RAS15, UK18]. **Stochastic** [ADR18].
**stolen** [Bha16]. **Stopping** [Sav13a].
**StopWatch** [LCR14]. **Storage** [BCQ+13, CWL16, CCT+14, CLW16, GLG12, HSM14, JSCM17, Kip15, LCK11, LMD16, LWJC14, QL17, SKH17, XNKG15, ZDL12, ZVG16, AY14a, AKK+17, BP10, CFVP16, CFZ+10, CHL+16, CDF+10, CDL18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, Sar10a, SYY+17, SWW+16, SWW+17].
WS13, YYS+16, YZCT17, ZYC+17. Stored [CMLS15, RSN14]. Stores [BCK17]. stories [Sm15b]. Storing [DLWW11, LZC17].


symptom [YZL+18]. symptom-matching [YZL+18]. Synchronization [BL12, WXY+17, yWxY+18, AAT18, XNG+14]. Synchronized [DM18, ACM12]. Synchronization [HZ1]. SYN [MHC12]. Syndromes [BBC+13]. Synergy [KRB12]. Synergy-Based [KRB12, synthesis [RS17]. Syst [HYS+WZM12a]. System [AD11, Ano10, CCL12, CZL14, Cor14b, CRST15, DG15, GOPB12, Har16, HHS+15, IAD10, JN12, JWJ+17, Jin10, KMP+11, Lop12, MLBL12, NSMS14, QLL17, RSC18, SMK18, SRAA17, SL11, YE12, YZX+12, YKK18, ZMM17, ZPL16, ZLC15, ZVG16, AHH+18, BC18, BGG+13, Bul10a, CH11, CTL12, CZ14, CS11, FNW18, GCK11, HKW+15, HJM+11, HLY14, JC13, LLLK10, Lit14, LTP+15, LLL+1, MS12a, MNW15, PSOM13, SPP+13, WMX+17, WZG+12, XZW16, YZX+18, ZMM+10, ZML17, KKA14, Dew11].

System-Level [JWJ+17]. Systematic [CCG+16, CBL13, PC16]. Systems [AN12, AB15, BL15, BS13b, BCTP16, BB10, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HLN+10, LMD16, LQY10, LY16, LNZ+13, MR14b, OŠ12, PRSV17, QZL+16b, RST15a, RST15b, SBS+12, SFRK15, Sev16, SKH17, SGC14, SDM+12, STC11, TKR14, YNR12a, AT10, AT1+10, CFVP16, CFZ+10, CLZ+17, dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DZS+12, EIs10, FXP12, GOMOGCC15, GSN+16, GVPCdBR12, HZWX18, JSDK+16, JHC14, KSA16, LCL+15, LWK+18, MLM18G12, MG10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRB+12, WS14, YSM14, Zhu13, MA17, Ano11a]. Systolic [MCDB12]. Systolic-Array [MCDB12]. SZK [MX13].

[Cou12, SS12a, AY14a, BJR+14]. Tests
[GLG12, MS12b, Sim15a]. Texas [EE13].
[Text] [GdM16, SMSK18, XZZ18, CR12, SI12, SWW+17], Text-dependent [GdM16].
Textbook [PP10a]. Texture [TSH17].
Theft [Ber12, Ber17, BTPLST15]. Their
[CLZ12b, CK18, JSK+17, NR12, CQX18, Hof16, I015, KK10, Sti11] them
[HLZ10, JSK+16, Rus15]. Theological
[SS10c]. Theorem [Lau12, HF14a].
Theorem-based [Lau12]. Theoretic
[CVM14, MAL10, WSS12, CDGC12, SD10, SKEG14]. theoretical [KL13, ZZ15, Gas13].
Theoretically [TWZ11]. Theories
[ABR12]. Theory
[ACM10, ACM11, CCKM16, CDFZ16, CDFS10, Cra12, FGM10, FB12, FS15, Hen12, LW11a, Lin14b, Nac12, Per13, PJ12, RBHP15, RST15a, RST15b, Sah13, SAKM16, Sha10, Wes16, Yan10, Abe10, AB10b, Bu10b, CFR11, Gil10, LPJ15, MZA+13, McG11, YTM+14, Cra12, Lin14b, Sah13, vDKS11].
theory-based [LPZJ15]. There
[Cer15, McK10, McK11, SM13]. Thin
[Chi16]. things
[FQZF18, AAC+16, CLF+17, HZL18, LNK+18b, LGH+17, NLLJ12, NLY15, PLGMCdF18, SB17, WCCH18, YCT15].
Third [jCPB12, QZL+16b, Sen10, BL10, Ed19, Kup13]. Third-Party [QZL+16b].
Third-Round [jCPB12]. Thirteen
[AP13]. thou [BDK11]. Threat
[CSY18, ALL+18, Ven14]. Threats
[AJA16, ERLM16, GSC17, LJS+14]. Three
[CZ15a, HXC+11, LZZ+12b, PC16, Shi11, YKNS12, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKHK14, XCL13, YC12, YZZ+14].
Three-Dimensional [LZZ+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, Sta12, Tan11, WYCF14, WHI5, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, HH15, O010, QD16, SES+16, S15y15, SGM16, TD14, ZJX+14, ZPYW12].
thresholding [PC14]. thrive [Sch12b]. throughput
[MAK+12]. Thru [SYC+17, SYW17].
Thwart [LJS+14]. Thwarting [XTK10]. Ticket
[XHCH14]. Ticket-based
[XHCH14]. tickets [LMJC11]. tied [Men13]. Ties
[PYM+15]. Tight
[GDC16, LPS12, LH18]. Tightly
[HLLG18]. Time
[ASBDs16, ANo17d, App14, AYS15, BJ16, Che17, FD11, GSC17, HC17, HGT15, IF16, JWWJ+17, JEA+15, KME+12, LCL+17a, NA10a, Nov10, PNRC17, Ste15b, WLZ12, YE12, AY14a, An015d, BM15, CC14, DCT12, FHH10a, HU15, LW10, LW13b, LML+13, MK11, An016g]. Time-area
[Nov10]. Time-Memory
[ASBDs16]. Time-Specific
[KME+12]. Time-Spread [HTG15]. Timed
[Jia14b, KFOS12, Tan15a, Unr15, WSS12].
Timed-Ephemizer [Tan15a]. Timed-Release [KFO12, Unr15, WSS12].
Timing [BG17, GV14b, Hay13, LG14, AGH+17, SRB+12]. Tiny [ZOC10].
Titan [PP10b]. Titan-R [PP10b]. TLS
[AP13, BBDL+17, BFCZ12, BJ14+14, CFN+14, D11].
TBS-based [PP11].
Today [Ber16a, Mac12]. Toeplitz [Ye10]. Token
[TYK+12, ZM16, IM17, Jac16].
token-based [Jac16]. Token-Leakage
[ZM16]. tokenisation [Mar10b]. tokenless
[Wat14a]. Tokens [Muf16, DCT12, HU15].
Tokyo [Sah13]. Tolerant
[HK14, ZH16, JL+12, WMY16, XW13]. tolerating [ZW14]. Tone [Yam12]. Too
[DL15, DSSW14, Ros11]. Tool
[ASM12, DCMR15]. Toolbox
[AHS13, TRD11]. Toolkit [BJ12].
Tools [Ake12, BKBK14, GO17, Ste15a, Lan11].
Top [SS12a, SS10c, Sta13, CH13]. top-
two-channel [JLT+12, JMW+16, Kem11, Li10, MG11, QYWX16, Rus15, SM10b, hSZ15, WW14, Wat14a, YT11b, ZC15, GHKL11].

Two-Channel [LLC11, ED19, Lit14, JMW+16, Kem11, WW14, Wat14a]. Two-Channel [GHR14].

Two-Server [YLW13, CSD18]. Two-Phase [MD12a]. TWS [OKG+12].

Type [AKP12, CFL13, PFS12, SH15, BST17, SYL13, WB12]. Type-based [CFL13, SYL13]. Type-Flaw [SH15]. Types [BCEM15].


Ukraine [OGK+15, ultra [AATM18, GW14, TG17, WCFW18]. Ultra-lightweight [AATM18, TG17, WCFW18].

UMTS [OHJ10, TM12]. Un-traceability [Chi13a]. Unattended [BN14], unauthentic [MLMSM12]. Unbounded [LW11c, YZ12].

Unbreakable [Bha16]. Uncalibrated [SGP+12], unsecured [Ald11]. Uncertainty [FS13, BBGT12].

Unclonable [Ano16e]. Unconditional [Jia14a]. Unconditionally [CFOR12, LHF12, SNJ11].

Unconditionally-Secure [CFOR12]. uncorrelated [MSM+18b]. Uncovering [FMS12a, WBC+10]. Undeciphered [Rao10].

Underenabling [BBBP13]. underhanded [Cra14]. Understanding [EPAG16, PP10a, Bar12]. Undisturbed [YCL17].

Unexpanded [SA16a]. Unforgeable [HHP17]. Unidirectional [LSC12, DKL+16]. Unified [ZSW+12], uniformly [YKKL12]. Unilaterally

[GRL12]. Unintended [Ess17]. union [BBDL+17, Bud16]. Unique [SSPC12, SOS15]. Unit [PP10b, Sta13, MS13a, MS13b, MS13c], units [ABDP15]. Universal [ASM12, BKST18, BJL12, NR12].


untraceable [AIKC18, JMW+16]. Untrusted [LQY10, MS16, ATKH+17, DRD11, MvO11, WS13]. updatable [LCL+17a]. Update [BCE+10, KE19, LQY10, FS18, WLF17].

upgrading [GCSA+11, LJWY18]. Upper [AMVZ12]. URLs [AY14a]. USA [Dun12b, IEE13, Kia11, Lin14b, Pie10, Rab10, ACM10, ACM11, IEE10, IEE11b].

Usability [RAZS15]. usable [DL15, TGC16]. usage [AKK+17, BHCdFR12]. Use [CSV15, DFKC17, KOS16, NR12, YT12, der10, CZ15b, Die12, Hof16, KK10, MFB+13, OO10, Sti11, UK18].

Used [CGCPDMG12, BM15, MS13b]. useful [dCCSB+16]. Usenet [Bel18]. User [BLV17, BKJF12, FLH13, GdM16, Har16, JN12, LLC11, LCL17b, MZHY15, MBC15, MDMJ17, OdH12, PDT12, PWVT12, RVH+16, SZDL14, SPM+13, WgMdZI12, WgMW12, ZPW16, AaBT16, ATKH+17, APK+18, BT18, CH10, CHS11, CLIJ13, DSCS12, GH16, HL14, KKM+13, KLW+16, KDW+17, LH10c, LNM+11, LNL13, LH13, MM12, OKG+12, hSZ15, WT10a, WOLS12, YHL16, YSL+10]. User-centric [BLV17].

User-controlled [Har16]. User-Friendly [SZDL14, WOLS12]. User-Generated

REFERENCES

[LLLK10]. Yuan [FMS12a]. YubiKey [Jac16]. Yves [Ter11].


References

[AAC+16]

Akyildiz:2014:OTB


Applebaum:2017:AC


Abo-alian:2016:KDB


Ambrosin:2016:FAB

REFERENCES


**Arora:2012:ILM**


**Akleylek:2016:SPM**


**Abdalla:2010:PCL**


REFERENCES

74

Almeida:2014:COS

Ananth:2013:SFP

Avoine:2016:SSP
Aid:2013:DIO


Acar:2013:SPA


Andreeva:2012:SAS


Arapinis:2012:RET


ALMashrafi:2012:AIM

Mufeed ALMashrafi, Harry Bartlett, Leonie Simpson, Ed Dawson, and Kenneth Koon-Ho Wong. Analysis of indirect message injection for MAC generation using stream ci-

Patricia Arias-Cabarcos, Florina Almenarez, Ruben Trapero, Daniel Díaz-Sanchez, and Andres Marin.

Claudio A. Ardagna, Jan Camenisch, Markus Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio.
REFERENCES

0926-227X (print), 1875-8924 (electronic).


Aizatulin:2012:VCC


Anyanwu:2010:DCS


Ayday:2012:DAA


Aliberti:2016:RPS


Attasena:2017:SSC


Adikari:2011:HBT

Abdalla:2012:LBH


Andrychowicz:2016:SMC


Araldo:2018:CEC


Ahmed:2017:IRD


Attrapadung:2015:RGS


Antonopoulos:2017:DIS

ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).


J. Appelbaum, J. Horchert, and C. Stöcker. Shop-
ping for spy gear: Catalog advertises NSA tool-
box. Der Spiegel, ??(??):??, December 29, 2013. URL
http://www.spiegel.de/international/world/catalog-
reveals-nsa-has-back-
doors-for-numerous-devices-
a-940994.html.

Ak:2014:ICS

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

Aia:2015:FAA

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

Aik:2014:ICA

Benny Applebaum, Yuval
Ishai, and Eyal Kushile-
vitz. How to garble arith-
metic circuits. SIAM Jour-
nal on Computing, 43(2):
905–929, ???:?? 2014. CO-
DEN SMJCAT. ISSN
0097-5397 (print), 1095-
7111 (electronic).

Amin:2016:DAP

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

Ali:2018:CBR

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

AIB+16

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

AIB+16

Benny Applebaum, Yuval
Ishai, and Eyal Kushile-
vitz. How to garble arith-
metic circuits. SIAM Jour-
nal on Computing, 43(2):
905–929, ???:?? 2014. CO-
DEN SMJCAT. ISSN
0097-5397 (print), 1095-
7111 (electronic).
Amin:2018:UAP


Alhanahnah:2016:MTI


Azarderakhsh:2014:NDP


Almulla:2013:CKE


Anada:2017:CGS


Afanasyev:2011:PPN

[AKM+11] Mikhail Afanasyev, Tadayoshi Kohno, Justin Ma, Nick Murphy, Stefan Savage, Alex C. Snoeren, and Geoffrey M. Voelker. Privacy-preserving network forensics. *Communications of the Association for Computing Ma-
REFERENCES


Ahir:2017:LAR


Abbasinezhad-Mood:2018:DHI


Adj:2013:WDC


Aumasson:2014:HFB


Ahmadian:2010:PDS


Alvarez:2012:CAB

REFERENCES


REFERENCES


REFERENCES


Anonymous:2015:QCS


Anonymous:2015:UGB


Anonymous:2016:CPSd


Anonymous:2016:EML


Anonymous:2016:FVM

Anonymous:2016:GUP


Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

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

Anonymous:2017:BRM


Anonymous:2017:CCS

The story describes a poor choice of generating large (about 1024 bits) primes \( p \) and \( q \) that led to crackable RSA cryptography. The solution for Estonia was to switch to elliptic-curve cryptography that was also supported by the cards.

Anonymous:2017:HDQ


Anonymous:2017:MBH


Anonymous:2017:RV


The ROCA vulnerability affects millions of smartcards, and devices using TPM (Trusted Platform Modules). It allows recovery of the private key from knowledge of the RSA public key, and thus, facilitates malicious cloning of the cards, and decrypting of some encrypted filesystems.

Anonymous:2017:MBH


Anonymous:2017:RV


The ROCA vulnerability affects millions of smartcards, and devices using TPM (Trusted Platform Modules). It allows recovery of the private key from knowledge of the RSA public key, and thus, facilitates malicious cloning of the cards, and decrypting of some encrypted filesystems.

Anonymous:2017:MBH


Anonymous:2017:RV


The ROCA vulnerability affects millions of smartcards, and devices using TPM (Trusted Platform Modules). It allows recovery of the private key from knowledge of the RSA public key, and thus, facilitates malicious cloning of the cards, and decrypting of some encrypted filesystems.
REFERENCES


Appel:2015:VCP


Albrecht:2015:FBR


Al-Qarni:2012:EI


Arai:2013:MDH


Adj:2014:SRC


AlTawy:2018:TCM

Riham AlTawy, Raghvendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang, and Guang Gong. Towards a cryptographic

**Azarderakhsh:2015:PHS** [ARM15]


**Ambrose:2012:RII** [ARP12]


**Asharov:2016:LPI** [AS16]


**Artemenko:2017:PGO**


**Andrade:2016:LEP**


**Asharov:2014:TCC**

Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. *Lecture
Al-Sinani:2012:UCB


Ahmadi:2011:SKC


Ahmadi:2012:SKE


Asaar:2015:IBM


Alsulaiman:2013:IVB

Fawaz A. Alsulaiman, Nizar Sakr, Julio J. Valdés, and Abdulmotaleb El Sad-

**Altman:2010:AAP**


**Argyropoulos:2010:BTP**


**Au:2011:PPT**


**Al-Tariq:2017:SFP**


**Alam:2015:ACF**

Aslan:2016:DEM


Abdalla:2012:LRS


Altafa:2017:LHL


Awad:2017:OLO


Anzala-Yamajako:2012:RAC


Ahmad:2014:RTN


AlTawy:2014:IDR

Riham AlTawy and Amr M. Youssef. Integral distin-
REFERENCES


[BAAS13] S. Behnia, A. Akhavan, A. Akhshani, and A. Sam-sudin. Image encryption


Jérémy Barbay. Book re-

**[Bar15]**


**[Bat10]**


**[Bax14]**


**[Bay10]**


**[Bulygin:2010:OSS]**


**[Bennett:2014:QCP]**

Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560 (part 1)(??):7–11, December 4, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (elect-


REFERENCES

Beurdouche:2017:MSU

Beimel:2014:MLS

Bernstein:2011:PCI

Bernstein:2017:SRD
Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Tanja Lange, Christine van Vredendaal, and Yuval Yarom. Sliding right into disas-

Boldi:2012:IUG

Basin:2014:KYE
David Basin and Cas Cremers. Know your enemy: Compromising ad-

**Bocu:2018:HEB**


**Bichsel:2012:DMA**


**Badrignans:2010:SSA**


**Balfanz:2012:FA**


**Bugliesi:2015:ART**


**Buhrman:2014:PBQ**

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail

**Bahri:2016:CCO**


**Bahri:2012:SCS**


**Borghoff:2012:PLL**

[BCG+12b] Julia Borghoff, Anne Can-
REFERENCES

**Barthe:2012:CA**


**Beunardeau:2016:WBC**


**Bitansky:2013:SNI**


**Brandenburger:2017:DTC**


**Bernstein:2014:CKR**


**Basin:2012:PRI**

REFERENCES


[Basso2011:BWC] Alessandro Basso, Davide Cavagnino, Victor Pomponiu, and Annamaria Ver-
REFERENCES


Bessani:2013:DDS


Blasco:2016:SWB


Biddle:2012:GPL


Belkacem:2014:DCM


Bender:2012:DSP


Bhasin:2015:EFB

Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Wei He. Exploiting
REFERENCES


[Buchmann:2011:XPF]

[Backstrom:2011:WAT]

[BDK11]

[Bossuet:2016:EPA]


REFERENCES


Bellovin:2016:EEE


Bellovin:2018:UAE


Berghel:2012:ITF


Bera:2014:QC


Berghel:2016:DJT


Berghel:2016:S


Berghel:2017:ELR


Berretti:2018:IAS

Stefano Berretti. Improved audio steganalytic feature and its applications.
Bouman:2011:SAW


Bas:2012:BLK


Bhargavan:2012:VCI


Barthe:2014:PRV


Bobba:2010:ABM

REFERENCES


REFERENCES

http://link.springer.com/accesspage/chapter/10.1007/978-3-642-33125-1_1.


REFERENCES

114


Behnia:2012:SEI


Bosc:2014:SPS


Bernstein:2015:S


Bonneau:2015:PEI

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. Passwords and the evolution of imperfect authentication. Communications of the Association for Computing Machinery, 58(7):78–87, July 2015. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electron-
Biagioli:2012:CCS

Beimel:2014:CCW

Biswas:2017:SAT

Brumley:2010:CAI

Boche:2016:DSK

Bouraoui:2017:HAE
REFERENCES


REFERENCES

comjnl.oxfordjournals.org/content/57/4/537.full.pdf+html.

**Braun:2012:ULA**


**Brakerski:2010:OHB**


**Bogdanov:2018:IEA**

REFERENCES

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

Bellare:2012:IBL


Bogdanov:2011:BCF


Bibak:2018:AUH


Bothe:2013:EFS


Bernstein:2010:PCA


Byun:2011:SMC

Jin Wook Byun and Dong Hoon Lee. On a security model of conjunctive keyword search over encrypted relational


REFERENCES


[Berryman:2012:SI]

[Berryman:2012:SI]

[Berryman:2012:SI]
REFERENCES

ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

[BMBS10]

Birajdar:2013:DIF


[BM13]

Bard:2015:PRO


[BM15]

Benamara:2016:ICA


[BMB16]

Baldwin:2010:AFI


[BMBS10]

Biswas:2012:IBA


[BMB16]

Backes:2012:GCP

REFERENCES

Banik:2012:DFA


Babamir:2014:AKP


Buckley:2015:RVV


Bunder:2017:GAR


Biryukov:2014:DEA


Ben-Othman:2013:IHN

Jalel Ben-Othman and Yesica I. Saavedra Benitez. IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s. *Concurrency and Compu-
REFERENCES

Bohme:2010:ASS

Bon12

Borghoff:2010:CLC

Bowyer:2011:WSD

Boyen:2013:ABF

Boyce:2016:BOT

Burns:2010:SCR
Randal Burns and Zachary Peterson. Security con-

**Bohli:2011:RAP**


**Brooke:2010:DCX**


**Bellare:2014:SSEa**


**Bellare:2014:SSEb**


**Boneh:2016:BCR**


**Balsa:2017:TIC**

Ero Balsa, Cristina Pérez-Solà, and Claudia Díaz. Towards inferring communication patterns in online social networks. *ACM*
REFERENCES


Brakerski:2014:VBB


Brakerski:2013:WHT


Bradbury:2015:BSB


Briggs:2011:SDC


Broemeling:2011:AES


Brook:2017:LSR


Becker:2013:SDL

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
Benaloh:2015:EEV


Bag:2017:BBW


Bellare:2012:MIS


Brumley:2012:SFI


Bergsma:2012:PAW


Bajaj:2013:CSE

REFERENCES


REFERENCES


REFERENCES


[Bul10b] Stanislav Bulygin. Computer algebra in coding theory and cryptanalysis. Südwestdeutscher Verlag für Hochschulschriften,
REFERENCES

Saarbrücken, Germany, 2010. ISBN 3-8381-0948-1. ???. pp. LCCN ????

**Burke:2011:AMD**


**Brakerski:2011:EFH**


**Brakerski:2014:EFH**


**Bitansky:2018:IOF**


**Bayrak:2012:AI**


**Baek:2013:SPK**


**Bogdanov:2012:ZCL**

Andrey Bogdanov and Meiqin Wang. Zero-

**Bhatnagar:2013:BIW**


**Bai:2016:ALC**


**Bhatnagar:2013:SRI**


**Baek:2016:EGC**


**Bhatnagar:2012:IVE**


**Bao:2010:ISC**

Feng Bao, Moti Yung, and Dongdai Lin, editors. *Information security and cryptology: 5th in-
ternational conference, IN-SCRYPT 2009, Beijing, China, December 12–15, 2009. revised selected pa-
ners, volume 6151 of Lecture notes in computer science. Springer-Verlag, Berlin, Germany / Heidel-
berg, Germany / London, UK / etc., 2010. ISBN 3-642-16341-6 (softcover). LCCN ???

Sta:2014:KYS [Cas10]
C ACM Staff. Know your steganographic en-
my. Communications of the Association for Com-
puting Machinery, 57(5):8, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-
tronic).

[CAL14]

C Caldwell:2013:INP [Cal13]
www.sciencedirect.com/
science/article/pii/S1353485813700515.

[CBL13]

C Carter:2010:TB [Car10]
rutherfordjournal.org/
article030108.html.

[CCL10]

C Carlson:2011:JRW

[Casselman:2010:VC]
www.ams.org/notices/
201003/.

[Cobb:2013:LMS]
William E. Cobb, Rusty O. Baldwin, and Eric D. Laspe. Leakage mapping: a systematic methodology for assessing the side-channel information leakage of cryptographic implementa-

[CC10]
Christian Cachin and Jan Camenisch. Encrypting

Chang:2014:RRT


Chadha:2016:AVE


Chretien:2015:SPP


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO

REFERENCES

Checkoway:2016:SAJ

Chadha:2012:AVE

Chatterjee:2016:TAD

Chou:2013:UGS

Chang:2011:SFW

Cascudo:2015:SSN
Ignacio Cascudo, Ronald Cramer, Diego Mirandola,

[CCM17] Chatterjee:2017:PBS


Chen:2013:WSB

Chu:2014:KAC

Chen:2010:ALD
Guoming Chen, Qiang Chen, Dong Zhang, and...


Choo:2016:CCT


Cao:2012:ITM


Chari:2010:DSC


Cui:2018:ABC


Coras:2016:AML

Florin Coras, Jordi Domingo-Pascual, Darrel Lewis, and Albert Cabellos-Aparicio. An analytical model for Loc/ID mappings caches.

Costello:2014:Cas

Ceruzzi:2014:Hft

Cerf:2018:Csa

Chang-Fong:2016:Csc

Carter:2013:Ssa
Centenaro:2013:TBA

Checkoway:2014:PED

Cevallos:2012:USR

Carstensen:2011:AAA

Calzavara:2017:SWJ

Celesti:2016:ALT
Antonio Celesti, Maria Fazio, Massimo Villari, and Antonio Puliafito. Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems. *Journal of Network and Computer Applications*, 59(??):208–218,
REFERENCES


**Cho:2017:EDF**


**Chang:2010:PRN**


**Chen:2010:IFA**


**Camenisch:2012:EAA**


**Che:2012:WAM**


**Cheraghchi:2014:NMC**

REFERENCES

Corrigan-Gibbs:2014:KS


Chaudhuri:2010:PIC


Caballero-Gil:2012:LAR


Chmiel:2012:EPC


Coull:2011:ACO


Cohney:2017:PSR

Shaanan Cohney, Matthew D. Green, and Nadia Heninger. Practical state recovery attacks against legacy RNG implementations. Report, University of Pennsylvania and The Johns Hop-
REFERENCES


REFERENCES


[Che17] Lidong Chen. Cryptography standards in quan-
REFERENCES

Chen:2012:SRF

Chen:2012:IAM

Chien:2013:CR

Chiren:2013:ABB

Chien:2016:GAI

Chmielowiec:2010:FPR

**Choudary:2010:SCD**


**Chou:2014:EMA**


**Chen:2013:ATK**

Qian Chen, Haibo Hu, and Jianliang Xu. Authenticating top-k queries in location-based services...
REFERENCES


Shalini Chandra and Raees Ahmad Khan. Availability state transition model.
REFERENCES


Chung:2018:ERN

Chung:2011:LMA

Chase:2013:SMN

Chase:2016:CTC

Comon-Lundh:2010:DSP

Chang:2011:RSB
Chin-Chen Chang, Chih-Yang Lin, and Yi-Hsuan Fan. Reversible steganography for BTC-compressed

**Chen:2017:PGF**


**Chong:2013:ASG**


**Chen:2016:RPR**

[CLH+16] Zhenhua Chen, Shundong Li, Qiong Huang, Yilei Wang, and Sufang Zhou. A restricted proxy re-encryption with keyword search for fine-grained data access control in cloud stor-

**Chen:2012:NCB**


**Chen:2013:TSE**


**Chande:2016:NSC**

Manoj Kumar Chande, Cheng-Chi Lee, and Chun-


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkoway:2018:WDL</td>
<td>Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Colney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav</td>
</tr>
</tbody>
</table>

Coles:2016:NAU


Cao:2018:EEG


Chakraborty:2013:EHI


Chakraborty:2015:SSC


Chen:2017:VME

REFERENCES

29(7):??, April 10, 2017. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).


[CMO+16] [CNT12] [Chen:2012:FAA] [Chin:2011:ACS] [Conitzer:2010:AP]


Corthesy:2014:SSD


Coutinho:2012:RPT


Claessen:2013:SPN


Canard:2018:NTC


Chung:2016:NBB


Chen:2018:RLF

Cramer:2012:TCT

Craver:2014:UCC

Clear:2012:CPA
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-33383-5_13./

Crichlow:2016:RSE


Culnane:2015:VVV


Chhabra:2011:NSN


Clark:2012:RLA


Chapin:2014:SRP


Chattaraj:2018:NTS


Chauhan:2018:BBA

Jagmohan Chauhan, Suranga Seneviratne, Yining Hu,


Stephen Chong, Christian Skalka, and Jeffrey A. Vaughan. Self-identifying data for fair use. *Jour-
REFERENCES

Chow:2012:EPV

Chen:2011:ARl

Chen:2011:TVS

Canard:2018:CPK

Calzavara:2015:SLA
Stefano Calzavara, Gabriele Tolomei, Andrea Casini, Michele Bugliesi, and Sal-

Chin:2013:SMB


Chang:2012:GBP


Chou:2013:TIB


Crenne:2013:CMS


Calmon:2014:ITM

Choi:2012:LTTF


Chung:2012:CBI


Chen:2014:SBB


Chen:2014:DSE


Cao:2014:PPM


Chen:2014:EPN


Cheng:2014:OMU


Chen:2012:FSD

Cheng Chen, Zhenfeng Zhang, and Dengguo Feng.


Cordeiro:2012:IMB


DePrisco:2013:CVC


DaRolt:2013:NDS


Datta:2017:SFH

SCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397516307526.

Castro:2016:FVB

Stephan De Castro, Jean-
Max Dutertre, Bruno
Rouzeyre, Giorgio Di
Natale, and Marie-Lise
Flottes. Frontside versus
backside laser injection: a
comparative study. ACM
Journal on Emerging Tech-
nologies in Computing Sys-
tems (JETC), 13(1):7:1–
7:??, December 2016. CO-
DEN ???? ISSN 1550-
4832.

Danezis:2012:FCDa

George Danezis, Sven Diet-
rich, and Kazue Sako, ed-
itors. Financial Cryptog-
raphy and Data Security:
FC 2011 Workshops, RL-
CPS and WECSR 2011,
Rodney Bay, St. Lucia,
February 28 — March 4,
2011, Revised Selected Pa-
pers, volume 7126 of Lecture
Notes in Computer
Science. Springer-Verlag,
Berlin, Germany / Heidel-
berg, Germany / London,
UK / etc., 2012. CO-
DEN LNCS.D9. ISBN 3-
642-29888-5. ISSN 0302-
9743 (print), 1611-3349
(electronic). URL http://
www.springerlink.com/
content/978-3-642-29888-2.

Desmedt:2010:CF

Yvo Desmedt. Crypto-
graphic Foundations, chap-
ter 9, pages 1–15. Vol-
ume 2 of Atallah and Blan-
ton [AB10b], second edi-
tion, 2010. ISBN 1-58488-
820-2. LCCN QA76.9.A43
A433 2010. URL http://
www.crcnetbase.com/
doi/abs/10.1201/9781584888215-
c9.

Desmedt:2010:ES

Yvo Desmedt. Encryption
Schemes, chapter 10, pages
1–30. Volume 2 of Atallah and Blan-
ton [AB10b], second edi-
tion, 2010. ISBN 1-58488-820-
2. LCCN QA76.9.A43
A433 2010. URL http://
www.crcnetbase.com/
doi/abs/10.1201/9781584888215-
c10.

Dew:2011:BRB

Nicholas Dew. Book re-
view: The Information
Master: Jean-Baptiste Col-
bert’s Secret State Intelli-
gence System. Isis, 102(4):
765, December 2011. CO-
DEN ISISA4. ISSN 0021-
REFERENCES


Durmuth:2011:DEN

DuPont:2016:ECC

DeCapitanidiVimercati:2010:EPR

Deng:2017:LLH

Ding:2012:CLS
REFERENCES


Djuric:2015:FSF


Dutta:2017:EFC


Dupressoir:2014:GGP


Ding:2012:NRR


Drimer:2010:DBP


Dubeuf:2016:EPA

REFERENCES


REFERENCES


**Dolev:2012:ATC**


**Dolev:2012:ATC**


**Dore:2016:ELO**


**Doychev:2017:RAS**


**Dorurumeric:2014:MH**


[DK12]

[DK16]

[DK17]

[DKA+14]
REFERENCES


REFERENCES


Degefa:2016:PSE


Dong:2013:PRS


DiPietro:2016:CLD


Dijaziri-Larbi:2018:WDA


Dodis:2011:SSC


Dai:2016:MLR

Shuguang Dai, Huige Li, and Fangguo Zhang. Memory leakage-resilient searchable symmetric encryption. Future Generation Computer Systems,
REFERENCES


REFERENCES


David:2012:UCO


[DN12]

Donovan:2014:ATM


[Don14]

Doroz:2015:AFH


[DPCM16]

Duncan:2012:CAI


[DP12]

Ding:2017:CSM


[DPC17]

Das:2016:CWM


[DPCM16]
REFERENCES

Dziembowski:2018:NMC


Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE

Dixon:2016:NTO


DelRey:2012:EDI


Dini:2011:LLA


Das:2015:DCS


Das:2016:MPU


Das:2012:DPB


REFERENCES

[Deng:2012:VIA]

[Dunkelman:2012:MEK]

[Dunkelman:2012:TCC]

[Durcheva:2015:SAI]

[David:2012:PRE]

[Dorn:2012:ECE]


[DZ14] Lunzhi Deng and Jiwen Zeng. Two new identity-based threshold ring sig-
REFERENCES


[Dent:2010:PS]


[Eslami:2011:SIS]

REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-30921-2_1/.


REFERENCES

El-Emam:2013:NSA

Eisenbarth:2012:CIP

Eisenbarth:2010:CCE

Esiner:2016:FFB

Engels:2013:NLL

ElBansarkhani:2012:ELB
REFERENCES

Embar:2014:PWO


Evtushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC


Engels:2012:HLA

REFERENCES

10.1007/978-3-642-25286-0_2.

Ebadi:2015:DPN


Essex:2017:DDU


Eibach:2010:OGB


Eldib:2014:FVS

Enos:2015:IBS


Farash:2014:ECC


Farash:2014:SEI


Fahd:2018:CPA


Fagone:2017:WWS


Farash:2014:CIE

REFERENCES


Edward Felten. The Linux backdoor attempt
REFERENCES


Faugere:2010:CLR

Fleischmann:2012:MFA

Feng:2010:CTS

Farras:2012:LTM

Faugere:2014:MCA

Fan:2017:SSP
Jingyuan Fan, Chaowen
References


Fan:2013:CPP


Fan:2010:AMI


Fan:2010:PSN


Fan:2010:AMI


Fan:2010:PSN


Farras:2017:IRN


Fahl:2012:WEM

Fan:2014:ASA


Fawzi:2013:LDN


Florencio:2016:PSD


Feng:2018:ABB


Farash:2015:PSE


Fisher:2015:CS

REFERENCES

[190]

dl.acm.org/ft_gateway. cfm?id=2846057&ftid=1645792& dwn=1&CFID=565418796& CFTOKEN=98912420.

Fei:2012:GTK


[184]

Fan:2015:SVS


Fehr:2013:FCC


[184]

Fan:2014:RRS


Ferguson:2010:SHF

Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Report, (various),
REFERENCES


Feng:2012:USD


Feng:2012:USD

Fraczek:2012:MSI


Fraczek:2012:MSI

Fernandez-Mir:2012:SRA


Fernandez-Mir:2012:SRA

Ferreira:2015:LPA


Ferreira:2015:LPA

Fu:2018:LUA

REFERENCES


[FPY15] Dong Lai Fu, Xin Guang Peng, and Yu Li Yang. Trusted validation for ge-

Feng:2018:ALA


Fathimal:2016:SSS


Frattolillo:2015:WPP


Frattolillo:2016:BFM


Frey:2010:ABC


Fridrich:2010:SDM

REFERENCES

Friksen:2010:SMC


Fridrich:2012:MTS


Fu:2016:EPS


Frauchiger:2013:TRR


Forbes:2015:CTC


Fugkeaw:2018:SSA


Fang:2011:ICP

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


Fang:2012:CCS


Ferguson:2010:CED


Feng:2011:GDA


Fujikawa:2012:SHI


Fujikawa:2012:SEI

REFERENCES


REFERENCES

[FXP12] Fanyang, Naixue Xiong, and Jong Hyuk Park.

[FYMY15] Xinyu Fan, Guomin Yang, Yi Mu, and Yong Yu.


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,


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

Granado-Criado:2017:HCH


Granado-Criado:2017:HCH


Gong:2016:ATI


Guerin:2016:TDU


Geller:2013:MIS


Gentry:2010:CAF

Craig Gentry. Encrypted messages from the heights


Prosanta Gope and Tzonelih Hwang. An efficient mutual authentication and key...


REFERENCES


REFERENCES

comjnl.oxfordjournals.org/content/58/4/792.

Gravier:2015:WOD

Goyal:2013:CZK

Gu:2017:IBM

Geetha:2011:VRN

Goyal:2013:CZK

Grigoriev:2017:YMP
REFERENCES


REFERENCES


go to page 207


go to page 209


[GLM+16] Linming Gong, Shundong Li, Qing Mao, Daoshun Wang, and Jiawei Dou. A homomorphic encryption scheme with adaptive chosen ciphertext security but without random oracle. *Theoretical Computer Science*, 609 (part 1)(??):253–261, January 4, 2016. CODEN TCSCDI. ISSN 0304-


Gao:2014:URA


Gong:2012:KNF


Garay:2017:SIA


Groza:2017:LCL


Goo:2012:CBS

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

Garcia:2012:ERP


Gorski:2010:CDS


Groth:2012:NTN


Glowacz:2017:IDW


Goodrich:2012:EVW


Genkin:2016:PKE


Grossschadl:2012:EJII

Genkin:2014:GYH

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

Gonzalez-Pardo:2012:CID


Greengard:2011:MRM


Green:2017:SSE


Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Galindo:2014:LCL


Ghosh:2014:BBB


Gorbunov:2015:ABE


Greenberg:2014:GWB


Gorbunov:2012:FEB


Gorbunov:2015:ABE


Wang:2014:RAW

Xiangyang Wang, Pan

**Gao:2015:GCC**


**Goh:2013:TOT**


**Guo:2012:AKE**


**Gao:2017:EMD**


**Gao:2012:RHC**

Guo:2018:SMK

Ge:2013:SAP

Haigh:2017:HRC

Hamamreh:2012:RPA

Hamlin:2017:NMC

Hanyok:2012:EHH
REFERENCES


Harn:2013:GA


Harrington:2014:GEF


Hardesty:2015:BAC


Hayes:2013:NSA


Houmansadr:2013:BCN


Hurlburt:2014:BBC

G. F. Hurlburt and I. Bojanova. Bitcoin: Benefit or


Hwang:2010:RIB


Hsu:2011:NLM


Hore:2012:IED


Hernandez-Castro:2012:MTA


Huang:2014:FOS


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-35416-8_13/.

Hamad:2018:DWU


Hellman:2017:TLC


Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Heys:2017:SCF


Harn:2014:MTS

Lein Harn and Miao Fuyou. Multilevel threshold secret sharing based on the

**Hoang:2014:IMD**


**Hua:2015:TSE**


**Han:2011:PEB**


**Heyse:2012:TOC**


**Hu:2016:EWS** [HHP17]


**Hayashi:2013:AEI** [HHR11]


**Huber:2014:TPW** [HHS+15]


**Hu:2016:EWS** [HHP17]


**Haitner:2011:PRI**


**Hong:2015:RSM**

Wien Hong, Gwoboa Horng, Chih-Wei Shiu, Tung-Shou Chen, and Yu-Chi Chen. Reversible steganographic


[Hinkelmann:2011:CPA] Markus Hinkelmann, Andreas Jakoby, Nina Moe,


Hur:2014:SDR


**Heyse:2012:LEA**


**Holenstein:2011:ERO**


**Heil:2014:APH**


**Harn:2010:A**


**Hazay:2010:EST**

Carmit Hazay and Yehuda Lindell. Efficient Secure Two-Party Protocols:

Hsu:2011:NIB


Hsieh:2014:AMU


Hmood:2015:ACA


Hu:2012:VMS


Hu:2016:PBR


REFERENCES


REFERENCES


Herzberg:2012:TJA


Hore:2012:SMR


Hoang:2012:ESB


Hirt:2014:BA


Harnik:2010:CIC


Hoffmann:2015:LBQb


Hoffmann:2016:LBQb

Leah Hoffmann. Last byte: Q&A: Finding new directions in cryptography:


**Hur:2010:CCS**


**Han:2016:GGA**


**Han:2014:GTK**


**He:2013:GME**


**Hulsing:2013:OPX**

REFERENCES


Neminath Hubballi and Mayank Swarnkar. Bit-Coding: Network traffic classification through encoded bit level signa-
REFERENCES


**Homma:2014:TFD**


**Halevi:2011:TBH**


**Han:2013:IBD**


**Han:2014:IBS**


**Han:2012:PPD**


**Heather:2014:CPE**

Shi:2015:CTS

Hamdy:2011:HPB

Henson:2013:MES

Hu:2010:TTW

Huang:2015:PAP

Herbert:2012:SMP
REFERENCES


REFERENCES


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


[Hao:2011:NTV] Rong Hao, Jia Yu, and


Qi Han, Yinghui Zhang, Xiaofeng Chen, Hui Li, and Jiaxiang Quan. Efficient and robust identity-based handoff authentication for EAP-based wireless networks. *Concurrency and Computation: Practice and Experience*, 26(8):
REFERENCES

Han:2018:ERA

Han:2014:ATS

He:2018:LAB

He:2015:IEI

Islam:2015:MBA


Ismail:2010:EAE


Islam:2011:MES


IBM:2013:DMP


IBM:2013:IPC


Irshad:2017:CPP

IEEE:2010:PIA


IEEE:2011:ICI


IEEE:2013:PIS


Imanimehr:2016:HPR


Islam:2011:MD

REFERENCES


Islam:2018:REP


Isobe:2012:SAL


Irshad:2016:EAM


Ishai:2014:PCP


Jacobs:2016:STB

REFERENCES


Prins:2011:DCA


Jain:2010:AAI


Jho:2016:SSE


Jakobsson:2012:AWD

REFERENCES


Jiang:2014:TEA

Jiang:2016:MAC

Jiang:2017:BMA

Jin:2010:ADW

Jain:2010:QP

Jawad:2013:GAD

Jun:2012:IIR
Jong Yun Jun, Kunho Kim,


Jia:2012:PKD


Jiang:2016:OOC


Jiang:2016:UTC


Jain:2012:BAS


Jan:2017:PPB


Johnson:2010:BRF

REFERENCES

Johnson:2015:NGA

Joux:2013:NIC

Jepps:2013:CCP

Juels:2014:HEE

Jevdjic:2017:ASC

Jain:2016:APQ
Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt, and Gerd Leuchs. Attacks on practical quantum key distribution sys-
tems (and how to prevent them). *Contemporary Physics*, 57(3):366–??, 2016. CODEN CT- 
PHAF. ISSN 0010-7514 (print), 1366-5812 (electronic).

**Judmayer:2017:BCI**


**Jiang:2018:CPA**


**Jordan:2018:EPE**


**Jiang:2012:DCA**


**Joye:2012:FAC**

Marc Joye and Michael Tunstall, editors. *Fault Analysis in Cryptography*. Information Security

Tong:2012:NBD


Jiang:2012:SLD


Jin:2015:NCD

REFERENCES

doi/full/10.1080/1206212X.1
2016.1188564.

[Joux:2014:SAC]

[Jiang:2010:EDI]

[KA18]

[Kurkcu:2018:CBE]

[Koryczy:2017:RFT]

[Koziel:2018:HPS]
Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari Kermani. A high-performance and scalable hardware architecture for isogeny-based cryptogra-
Kamp:2013:MES

Kamp:2016:MEM

Kapera:2013:MRM

Karafyllidis:2012:QGC

Kong:2015:CSM

Katz:2013:RIB
Jon Katz. Review of *Identity-based encryption*
REFERENCES


**Kawamoto:2015:LSH**


**Karthigaikumar:2010:PPV**


**Kallel:2011:SMM**


**Kleinrouweler:2017:SAP**


**Kim:2011:SSE**


**Koz:2012:ASE**

Kraetzer:2012:PCS


Karakoc:2013:BCL


Karakoc:2015:AKA


Kumari:2017:DSU


Kara:2019:ALS


Keblusek:2015:BRK

REFERENCES


REFERENCES

Khedr:2016:SSH

Kwon:2010:SEB

Koo:2018:PPD

Khazaei:2010:NBS

Kastner:2010:AOT

Kim:2014:MBM


REFERENCES


Khan:2015:CMB

Khan:2014:MEK

Karopoulos:2010:FIP

Kubota:2016:SAV

Khan:2013:EDC
Khan:2014:IPR

Kushwah:2011:EIB

Khakpour:2013:ITA

Klapper:2010:PSS

Ko:2010:MME

Koeberl:2012:EPD
Patrick Koeberl, Jiangtao Li, Roel Maes, Anand Rajan, Claire Vishik, and Marcin Wójcik. Evaluation of a PUF device authentication scheme on a discrete

**Kumari:2016:UFM**


**Kim:2012:INS**


**Keller:2010:DAS**


**Khomejani:2010:PCT**


**Koblitz:2010:BNW**

REFERENCES

Kiani:2011:MPD

Kifer:2014:PFM

Koblitz:2015:RWE

Koblitz:2016:RWE

Kasamatsu:2012:TSE

Kiyoshima:2014:CRB
REFERENCES

Karger:2011:LLB

Kanwal:2015:TTM

Kavun:2018:SAE

Khovratovich:2010:RCA

Khovratovich:2010:RRA

Kumari:2016:APW

Koblitz:2010:BRB
Neal Koblitz. Book review: *Decrypted Secrets: Methods and Maxims of
REFERENCES


Kasper:2012:SCA


Khamsemanan:2016:BBU


Kawachi:2017:GCR


Kollmitzer:2010:AQC


Kang:2012:AKM


Kolman:2017:SCG

Eyal Kolman and Benny Pinkas. Securely computing a ground speed model.

Koya:2018:AHM


Kumar:2017:TAU


Kiltz:2011:EAH


Khalid:2016:RHL


Kocabas:2012:CPB

Kang:2016:DSA

ISSN 0920-8542 (print), 1573-0484 (electronic).

Keskinarkaus:2010:IWD

ISSN 0164-1212.

Krenn:2013:CCR

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

Knudsen:2011:BCC

ISBN 3-642-17341-1, 3-642-17342-X (ebook).
ISSN 1619-7100 (print), 2197-845X (electronic).
xiv + 267 pp.

Krantz:2012:EAM

ISBN 1-4398-9834-0 (hardcover).
xvi + 351 pp.

Kostinger:2012:SBL

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

Koskinarkaus:2010:IWD

Krenn:2013:CCR

Kostinger:2012:SBL
REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-32717-9_20/.


Karthiga:2018:PSA


Kocabas:2016:ESM


Kiljan:2017:SAC


Kwon:2018:EIP


Kim:2012:SSS

REFERENCES


REFERENCES


Koyama:2012:NTD


Koyama:2012:NTD

Kamal:2010:EIN


Kamal:2010:EIN

Kuo:2018:DRA


Kuo:2018:DRA

Kate:2010:PBO


Kate:2010:PBO

Lu:2010:MSC


Lu:2010:MSC

Lathey:2015:IEE


Lathey:2015:IEE

Lackey:2015:UHP

Liang:2015:SEC

Landau:2017:LCI

Launchbury:2012:TBC

Lauter:2017:POL
REFERENCES


[LC17] B. Prathusha Laxmi and A. Chilambuchelvan. GSR: Geographic Secured Routing using SHA-3 algorithm

Liu:2013:IAG


Lathrop:2011:SPI


Lavington:2012:ATH


Li:2015:NA


Lee:2017:SUE

Kwangsu Lee, Seung Geol Choi, Dong Hoon Lee, Jong Hwan Park, and Moti Yung. Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency. Theoretical Computer Sci-
References

Liu:2017:GAU


Liu:2017:RNF


Li:2015:CEH


Li:2017:CCF


Liang:2014:CCS

Liu:2016:EQD


Liu:2016:NOP


Louchene:2013:WMR


Lotz:2015:SCS


Launchbury:2012:ELT


Ledin:2016:RME

George Ledin, Jr. Re-

**Lewand:2010:PC**


**Liu:2019:DVP**


**Liang:2015:CPA**


**Li:2017:PCL**


**Liu:2016:LCR**


**Lago-Fernandez:2014:NAA**


Ruggero Donida Labati,

Lop€ez-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

Lertvorratham:2012:ISM

Liao:2013:NMS

Lenstra:2012:RWW
[LHA+12] 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,
Lum:2016:QEM

[102x681] REFERENCES


Lum:2016:QEM


Li:2012:BVS


Lin:2011:ICA

Han-Yu Lin, Chien-Lung Hsu, and Shih-Kun Huang.


Li:2010:AIS


Li:2014:SOA


Liu:2015:SSP

Jianghua Liu, Xinyi Huang, and Joseph K. Liu. Secure

**Li:2018:OPP**


**Lian:2014:SSA**


**Liu:2015:CND**


**Liu:2012:ESS**


**Li:2010:PAP**


Litton:2014:TFA


Liu:2015:LBD


Li:2017:MMMA


Li:2016:IRI


Li:2017:SQS


pression function $\text{lp231}$.


**[Li:2012:IBO]**


**[LL11]**

Levä:2013:ABN


**[LL15]**

Lee:2015:TSS


**[LL16a]**


Lin Lyu, Shengli Liu,


REFERENCES

Li:2010:DCY

Lai:2013:SAS

Lu:2012:IEC

Lai:2018:EQK

Lee:2016:CAM

Lee:2016:AGA
REFERENCES


REFERENCES


REFERENCES


[Li:2011:CIB]


[Li:2013:GPB]


[Loeb:2015:MGM]


[Lopriore:2012:EPP]

REFERENCES


Lopriore:2015:PCR


Lopriore:2015:PMD


Low:2012:BRB


Lin:2011:CRN


Ling:2012:SHS


Lima:2010:PKE

REFERENCES


REFERENCES


REFERENCES

Lin:2015:SSE


Lychev:2016:RSI


Lee:2012:IBS


Lei:2012:RA


Liang:2015:EFC

REFERENCES


REFERENCES


[LTKP16] Yingjie Lao, Qianying Tang, Chris H. Kim, and Keshab K. Parhi. Beat frequency detector-

Lysyanskaya:2010:AEC


Lin:2011:CNS


Li:2016:LR


Ludge:2012:NLD


Lucchese:2010:RPT

Claudio Lucchese, Michail

Laﬁtte:2011:CBF


Liu:2010:CIE


Lee:2011:ACA


Lewko:2011:DAB


Lewko:2011:UHA

Lewko:2012:NPM


Liu:2013:SIP


Liu:2013:TIE


Liu:2013:CBS


Liu:2016:PAB


Liu:2014:DAF

Hongbo Liu, Hui Wang, Yingsong Chen, and Dayong Jia. Defending against frequency-based attacks


Liu:2010:NDC

Liu:2010:SET

Liu:2011:PIA

Lu:2012:MMA

Li:2010:GCP

Lou:2010:NAS
Luo:2012:ICB


Li:2012:IIA


Lin:2010:DSM


Li:2011:NIW


Li:2014:IBD


Li:2014:EMK

Ruixuan Li, Zhiyong Xu, Wanshang Kang, Kin Choong Yow, and Cheng-Zhong Xu. Efficient multi-keyword ranked query over encrypted data in cloud computing. Future Generation Computer Systems, 30(??):179–190, Jan-


[LYHH14] Jiqiang Lu, Wun-Shie Yap,


Shengli Liu, Fangguo Zhang, and Kefei Chen. Selective opening chosen ci-


[Li:2012:ESS] Li:2012:ESS


REFERENCES

Michail:2012:EHT


Moskowitz:2010:ITE


Malkin:2013:SCB


Mangard:2013:KSL


Martin:2010:FWL


Martin:2010:PCC


Martin:2010:XMA


Mao:2015:PUA


Mao:2015:PUA

Malone:2013:MOD


Malone:2013:MOD

Migliore:2018:PPF


Migliore:2018:PPF

Massolino:2015:OSC


Massolino:2015:OSC

Mukhopadhya:2011:PEA


Mukhopadhya:2011:PEA

Madanayake:2012:BPS

H. L. P. Arjuna Madanayake, R. J. Cintra, V. S. Dim-

**McGrew:2017:IDH**


**McK11**


**McGrayne:2011:TWH**


**McKay:2011:SLB**


**McKay:2012:SLC**

Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Kumar, Xiong Li, and Arun Kumar Sangaiiah. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81(??):557–565, April 2018. CODEN FGSEVI. ISSN 0167-739X

Marquez-Corbella:2015:ECP


Mathew:2015:NMB


Majzoub:2012:MRH


Mansouri:2012:ACA


Mansfield-Devine:2015:MIC


Murdoch:2010:CPB

Steven J. Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. Chip and PIN is broken. In IEEE, editor, 2010 *IEEE Symposium on Security and Privacy*, 16–19 May 2010, Oakland, CA, USA, pages 433–446. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA,
Mosenia:2017:PTS


Maachaoui:2012:MLA


Meiklejohn:2010:BRB


Menn:2013:ESC


Meshram:2015:EIB


Mandal:2016:DIW

REFERENCES


REFERENCES

Mou:2013:CBC


Mohd:2015:SLB


Micciancio:2010:F GC


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


Mozaari-Kermani:2017:FD

Mehran Mozaari-Kermani, Reza Azarderakhsh, and Anita Aghaie. Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on
McGrew:2016:SMH


Malik:2012:AIC


Marconato:2013:VLC


Mozaffari-Kermani:2010:CSI


Montecchi:2012:QSE


Meshram:2013:IBC


Maity:2017:ODC


Maity:2014:FIR


Maity:2014:DSM


Mulholland:2017:DCD


Moldovyan:2012:BBD


Meshram:2012:IBC


Moran:2010:BCP


Mukhopadhyay:2014:EMP


Monz:2016:RSS


McKusick:2015:DIF


Minier:2012:RKI

Marine Minier and Maria Naya-Plasencia. A related key impossible differential attack against 22


Ameer H. Morad. Office employees authen-
tication based on E-
CODEN LNCSDD. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-34478-7_8/.

ACM SIGACT News, 46 (1):10–12, March 2015. CODEN SIGNDM. ISSN
0163-5700 (print), 1943-5827 (electronic).

Marine Minier and Raphael C.-W. Phan. Energy-efficient cryptographic en-
CODEN LNCSDD. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-27585-2_7/.

Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Da-
mon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of Bit-
coins: characterizing payments among men with no names. Communications of
the Association for Computing Machinery, 59(4):86–93, April 2016. CODEN
CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://
cacm.acm.org/magazines/2016/4/200174/fulltext.


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


Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin.

Matsumoto:2017:ACG


Moghadam:2010:DRN


Mendel:2012:DAL


Maitra:2012:NA


Mroczkowski:2012:CAS

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


Myers:2013:BBC


Marton:2010:RDC


Mosenia:2017:CCA


Martins:2018:SFH


Muhammad:2018:ISU


Mosca:2013:QKD

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Manshaei:2013:GTM


Ma:2015:PKE


Nagy:2010:QCS


Naccache:2012:CST


Naccache:2016:FHE

REFERENCES


Naranjo:2013:FDA


Ni:2013:EIB


Narasimhan:2013:HTD


Ngo:2017:CSS


Nedjah:2016:PYP

Newell:2013:PCD


Naeem:2014:EIC


Nafea:2016:HMB


NIST:2012:RRN


NIST:2013:CSS


Nguyen:2014:DDI

REFERENCES


Ning:2012:DPB


Ning:2015:APB


Ning:2012:DCA


Nieto:2013:PVC


Nieto:2014:FSH


Nguyen:2012:DQB

References

Neville-Neil:2015:KVH


Nagy:2010:KDV


Navin:2010:ETU


Nose:2011:SW


Nose:2014:SWS


Novotny:2010:TAE

Martin Novotny. Time-area efficient hardware architectures for cryptography and cryptanalysis, volume 12 of IT-
REFERENCES

Nichols:2014:CSS

Nguyen:2011:APB

Nguyen:2012:SOU

Namasudra:2017:NSA

Niu:2015:CRS

Naccache:2010:THI
David Naccache and Ahmad-Reza Sadeghi. Towards hardware-intrinsic security: foundations and practice. Information Security

**[Nojoumian:2012:SRS]**


**[NS12]**

**[Natarajan:2015:MAD]**


**[NSA15]**

**[NTKG17]**


**[Nandakumar:2017:CAI]**

REFERENCES

Nguyen:2010:LAS


Noorman:2017:SLC


Nie:2013:CHB


Natgunanathan:2017:PBM


Newell:2014:NCR

REFERENCES


**Ou:2010:CPA** [OHJ10] Hsia-Hung Ou, Min-Shiang Hwang, and Jinn-Ke Jan. A cocktail protocol with the Authentication and

**Ohtake:2012:AAH**


**Opp11**


**Orejel:2014:E**


**Ormond:2016:CPR**

Jim Ormond. Cryptography pioneers receive ACM A. M. Turing Award: Diffie and Hellman’s invention

Ozen:2011:MIS


Owczarek:2012:LPL


Osborn:2016:SSR


Orencik:2016:MKS


Okamoto:2012:AAH


REFERENCES

Pranata:2013:MDR


Paulson:2010:SDO


Pandit:2012:EFS


Park:2014:FRI


Pun:2014:GIT


Paul:2016:TSO


Alberto Peinado and Amparo Fuster-Sabater. Cryptographic analysis of a

Poppelmann:2012:TEA


Peng:2010:SFW


Park:2012:IDF


Pohls:2012:RDI


Parno:2016:PNP

REFERENCES

354


Papas:2012:MLR


Park:2010:SIC


Pieprzyk:2010:TCC


Pointcheval:2012:ACE


Patel:2018:LLA


CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

**Peris-Lopez:2018:EAC**


**Pang:2013:IMA**


**Poh:2012:SEC**


**Pande:2013:SMC**

Poursakidis:2010:TPC


Puthal:2017:DDK


Niu:2014:RDW


Powers:2014:OSCa


Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC


Duong Hieu Phan, David Pointcheval, and Mario

Phan:2012:MBT


Papadopoulos:2015:PAP


Pandey:2012:PPS


Piret:2012:PBC


Polyakov:2017:FPR


**Patranabis:2017:PSK**


**Picazo-Sanchez:2013:CRS**


**Park:2013:PPM**


**Papakostas:2014:MBL**


Charalampos Papamanthou:2016:AHT

**Pudovkina:2012:RKA**


**Pei:2013:ARW**


**Poller:2012:EIC**


**Peng:2010:IWM**


**Pongaliur:2013:SNS**


**Pagnin:2018:HDB**

Elena Pagnin, Anjia Yang, Qiao Hu, Gerhard Hancke, and Aikaterini Mitrokotsa.


REFERENCES


[QMC17] Yue Qiu, Maode Ma, and Shuo Chen. An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems. Computer Networks (Amsterdam, Netherlands: 1999), 129 (part 1):??.


[QMC17] Yue Qiu, Maode Ma, and Shuo Chen. An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems. Computer Networks (Amsterdam, Netherlands: 1999), 129 (part 1):??.
Qiu:2017:PSB

Qiao:2018:CTC

Quaglia:2018:SVA

Qin:2016:STI

Qian:2014:IAF

Qiang:2016:SCF
Weizhong Qiang, Kang Zhang, Weiqi Dai, and Hai Jin. Secure cryp-

Qi:2016:SID


Qi:2016:SPR


Qin:2018:BRO


Rabin:2010:ACC


Rankin:2010:HLH


Rankin:2014:HEY

REFERENCES


[RBNB15] Kenneth Radke, Colin Boyd, Juan Gonzalez Ni-


Reardon:2016:SDD

[Rea16]

Reeve:2015:ARC

[Ree15]

Ren:2010:CSH

[RG10]

CODEN JSSODM. ISSN 0164-1212.

Roh:2010:BSW


Robert-Inacio:2011:SAP


Rjasko:2012:BBP


Regev:2011:QOW

Oded Regev and Bo’az Klartag. Quantum one-

Roy:2018:HIR


[Roy18]

[Ros11]


[Ros11]

[Rog16]


[Rog16]

[Roa:2012:SSA]


[Roa:2012:SSA]

[RPG12]


Francesco Rossi and Giovanni Schmid. Identity-based secure group communications using pairings. *Computer Networks*


J. Ribeiro, A. Souto, and P. Mateus. Quantum blind signature with an offline

**Ruj:2014:DAC**


**Ryan:2015:EEVa**


**Ryan:2015:EEVb**


**Russo:2015:FPT**

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

**Rahulamathavan:2016:UCA**


**Rodriguez-Vazquez:2012:SCB**

[Juan José Rodríguez-Vázquez, Sixto Romerosánchez, and Miguel Cárdenas-Montes. Speeding up a chaos-based image encryption algorithm using ]

Roettger:2012:PKC


Ren:2014:HHM


Rogaway:2012:SCS


Ren:2013:PPK


Ristenpart:2010:WGR


Ren:2013:DSE

Ling Ren, Xiangyao Yu, Christopher W. Fletcher,
REFERENCES


REFERENCES


REFERENCES


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


Shyu:2010:VMS


Srinivasan:2012:RAP


Syta:2014:SAA


Schoenmakers:2010:VS


Schwartz:2011:IMP


Schaathun:2012:MLI

Schneier:2012:LOE


Schneier:2012:DES


Schneier:2013:HDD


Schaefer:2015:BRB


Schaefer:2015:ECA


Schneier:2015:DGH

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


Shen:2012:PAS

Shakiba:2010:IID

Souissi:2012:OCP


Seo:2014:RHI

Salman:2018:BMM


Sasaki:2012:IKK


Sendrier:2010:PQC


Sendrier:2017:CBC


Serrato:2012:IAN


Sakai:2016:CDN

Yusuke Sakai, Keita Emura, Jacob C. N. Schuld, Goichiro Hanaoka, and Kazuo Ohta. Constructions of dynamic and non-dynamic threshold public-key encryption schemes...
REFERENCES


REFERENCES

ISSN 1540-7993 (print), 1558-4046 (electronic).

Bruce Schneier, Matthew Fredrikson, Tadayoshi Kohno, and Thomas Ristenpart.


Yuanchao Shu, Yu Jason Gu, and Jiming Chen.


Sun:2015:FSW


Shen:2018:CAL


Susilo:2016:EDT


Shankar:2012:BDF


Sipiran:2014:SCA

REFERENCES

October 2014. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Shaolan:2011:EDE

Seyedzadeh:2011:IEA

Song:2015:ADT

Shallit:2010:BRB

Shaw:2013:DE

Shen:2014:LES
REFERENCES

SEO. ISSN 1045-9219 (print), 1558-2183 (electronic). URL http://
www.computer.org/csdl/abs.html.


www.ams.org/notices/201003/.

com/chapter/10.1007/978-3-642-27937-9_2/.


Simion:2015:RST


Simmonds:2015:DII


Sirer:2016:TPS


Shakeri:2012:RZW


Shin:2017:CGI


Sabri:2011:AFS


Seo:2015:AEC


Shin:2017:SSD


Szalachowski:2010:CCG


Stevens:2015:FCF


Singh:2018:MWT


Scheidat:2012:STT


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


Sarkar:2010:CRM


Sarkar:2010:CRT


Sayedzadeh:2011:IES


Sengupta:2012:SAI


Sencar:2013:DIF


Smart:2016:CMS

Stanton:2010:FAD


Salmon:2011:PRN

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

Smith:2011:SSX


Smith:2011:RBA

Sean W. Smith. Room at the bottom: Authenti-
Stankovski:2014:CFE

Sharma:2018:CSS

Safavi-Naini:2011:USC

Seyedzadeh:2010:THI
Suriadi:2012:PCV

Schaumont:2015:IEP

Suresh:2015:AGU

Serwadda:2013:ELK

Shiaeles:2015:FII

Shim:2015:SDA
REFERENCES

trans//td/2015/08/06875932-abs.html.

Spaord:2016:SE


Safkhani:2014:CCA


See [CJP12].

Sun:2013:IUP


Serwadda:2016:TRR


Shaikh:2010:CTO


Schilling:2012:ATU

Thorsten Ernst Schilling and Havard Raddum. Analysis of Trivium using compressed right hand

**Sur:2012:SSU**


**Stanton:2014:BRB**


**Singh:2017:SCB**


**Stefan:2012:ACT**


**Sutar:2017:DPI**

REFERENCES

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


Sendrier:2013:HCE


Sadhya:2017:PRE


Singh:2013:QBF


Smith:2011:SMC


Shrivastava:2012:UIE


Strydis:2013:SAP

REFERENCES


REFERENCES

Stallings:2011:CNS


Stanoyevitch:2011:ICM


Stanek:2012:TEM


Sta:2013:ITD


Stewart:2011:CCI


Steel:2015:APF


Stenn:2015:SNT

Harlan Stenn. Securing

Stipčević:2011:QRN


Stickev:2015:CBS


Stolte:2012:EDA


Suciu:2012:SED


Sun:2016:NEB


Shen:2015:CSC

Emily Shen, Mayank Varia,


Sun:2017:CPP


Shen:2014:ERC


Sun:2018:RPP


Tsang:2010:BRR


Tamayo:2015:AFH


Tan:2011:CTA


[Tarnovsky:2010:DSP] Christopher Tarnovsky. Deconstructing a secure


[TCL15] Ying-Kai Tang, Sherman S. M. Chow, and Joseph K. Liu. Com-


REFERENCES


[TK14] Rasha Thabit and Bee Ee Khoo. Robust reversible


REFERENCES


REFERENCES

CODEN ????  ISSN 1540-7993 (print), 1558-4046 (electronic). URL

Toxen:2014:NSS


Tsougenis:2012:PEM


Tan:2016:BIB


Tang:2014:PAB


Taylor:2011:CAS


Tezcan:2016:HD

Cihatir Tezcan and Ali Aydin Selçuk. Improved improbable differential attacks on ISO standard CLEFIA: Expansion tech-
Tschorsch:2016:BBT


Tao:2014:CFS


Toreini:2017:TRP


Tang:2011:IDC


Tso:2013:SAI


Tseng:2012:ERI


REFERENCES


[TY16b] Yangguang Tian, Guomin Yang, Yi Mu, Shiwei Zhang, Kaitai Liang, and Yong Yu. One-round attribute-based key exchange in the multi-party setting. *International Journal of Foundations of Computer Sci-
Ehatisham-ul-Haq:2018:CAS


Uzunkol:2018:SWU


Ulutas:2011:MIS


Ulutas:2013:ISI


Vaikuntanathan:2011:CBN

REFERENCES

Vaikuntanathan:2012:HCE


Valamehr:2012:IRM


Vatajelu:2016:SMB


vanDam:2011:TQC


Visegrady:2014:SCV


VenafiLabs:2014:VLQ

Vetter:2010:ABV


Venkatakrishnan:2017:DRB


Vernize:2015:MNI


Viennot:2014:MSG


Vasiliadis:2017:DIS


Vleju:2012:CCA

Mircea Boris Vleju. A client-centric ASM-based approach to identity man-

**Vivek:2014:CSC**


**Vliegen:2015:SRD**


**Veloudis:2016:NPH**


**Vollala:2017:EEM**


**VonMaurich:2015:IQM**


**Vembuselvi:2011:LLL**

[VS11] C. Vembuselvi and S. Selvakumar. LISISAP: link level signature based secure anonymous protocol


Michail Vlachos, Johannes Schneider, and Vassilios G. Vassiliadis. On data publishing with clustering preservation. ACM Transactions on Knowledge Discovery from Data (TKDD), 9(3):23:1–23:??, April 2015. CODEN ????. ISSN 1556-4681 (print), 1556-472X (electronic).


Ward:2011:CCM


Watt:2010:IPI


Waters:2012:FER


Watts:2014:ICB


Watts:2014:PY1


Watts:2015:HGA


Wang:2012:PCE


[Wang:2018:SEA] Haijiang Wang, Xiaolei Dong, Zhenfu Cao, and...


Xianfang Wang, Jian Gao,

**Wang:2010:DVT**


**Wang:2012:BRR**


**Wei:2012:NCI**


**Wang:2012:SPB**


**Wang:2017:DRM**

Wang:2018:GAD


Wang:2015:EFF


Wang:2017:DVP


Wei:2016:PAB


Wu:2012:DAA


Wang:2012:FOP

Wang:2012:NFS


Williams:2018:FPD


Winder:2017:ROS


Wang:2016:DRS


Wu:2011:HQI


Weissman:2011:LLB

Wang:2012:MCE


Wei:2012:IRK


Wang:2011:RBM


Wang:2017:CAS


Wang:2013:HCL


Wei:2015:FST

Wu:2015:TRM


Wang:2017:ABS


Wang:2016:LLE


Wang:2012:RTC

[WLZL12] Liyun Wang, Hefei Ling, Fuhao Zou, and Zhengding Lu. Real-time compressed-domain video watermarking resistance to geometric distortions. *IEEE Multi-

Wu:2012:PSC


Wang:2017:CES


Won:2016:PA

[WMYR16] Jongho Won, Chris Y. T. Ma, David K. Y. Yau,
and Nageswara S. V. Rao.


Wang:2015:RSA


Watanabe:2012:ITT


Wang:2012:PAC


Wu:2010:EUA


Wu:2010:IBM


Wang:2013:NMC

Qichun Wang and Chik Ho Tan. A new method to construct Boolean functions with good cryptographic properties. *Infor-
Wu:2012:RIB


Wu:2016:LTN


Wu:2017:SPM


Wu:2012:AST


Wang:2014:ATF

Ding Wang and Ping Wang. On the anonymity of two-factor authentication schemes for wireless sensor networks: At-


Wang:2011:CIB

Wang:2011:CHI

Wang:2016:SHI

Wang:2017:EAK

Wang:2017:FWA


[Wang:2014:NAI] Yuechuan Wei, Xiaoyuan Yang, and Chao Li. Impos-


REFERENCES

[442]


Xu:2014:AHA

Xu:2012:APA

Xu:2014:TBH

Xi:2012:MDA

Xue:2017:CNC
Xie:2012:RAA


Xiong:2012:PPK


Xu:2017:GKG


Xu:2016:CIB


Xu:2013:PKE


Xu:2012:AHA

Xiang:2016:EMP


Xue:2013:TCB


Xie:2013:ECP


Xiang:2014:PBA


Xia:2015:SPK


Xiang:2015:SSB

[XNRG15] Yong Xiang, I. Natgunanathan, Yue Rong, and Song Guo. Spread spectrum-based high embedding capacity water-

Xiong:2011:CIB


Xin:2010:IEB


Xiao:2010:TAT


Xiong:2012:CBP

Kaiqi Xiong, Ronghua Wang, Wenliang Du, and Peng Ning. Containing bogus packet insertion at-

[XWSW16]


[XWXC14]


[XWY+18]

Li Xu, Chi-Yao Weng, Lumphin Yuan, Mu-En Wu, Raylin Tso, and Hung-Min Sun. A shareable keyword search over encrypted data in cloud com-


[YCC16] Ching-Nung Yang, Cheng-


Yu:2017:PDA

Yasuda:2015:MQC

Yan:2016:DEB

Ye:2014:NIE

Yamada:2012:PBR

Ye:2014:NIE


[YGFL15] Zhen Yang, Kaiming Gao, Kefeng Fan, and Yingxu Lai. Sensational headline identification by normalized cross entropy-based

\[\text{Ye:2017:VCS}\]


\[\text{Ye:2016:IEA}\]


\[\text{Yang:2018:RKF}\]


\[\text{Yang:2016:IHA}\]


\[\text{Yu:2010:IBF}\]

Yang:2016:EHA


Yang:2014:MDF


Yoo:2010:IRR


Yu:2011:FSI


Yu:2012:IRI


Young:2013:TPC

Maxwell Young, Aniket Kate, Ian Goldberg, and Martin Karsten. Towards practical communication in Byzantine-resistant DHTs.

YANG:2018:AIW


YUM:2011:ACO


Yi:2017:ICM


Yuen:2013:ELT

Tsz Hon Yuen, Joseph K. Liu, Man Ho Au, Willy

Yang:2012:WSI

[YLW13]

You:2012:DDS

[YL+12]

Yi:2013:ETS

[YLZ+16]

Yu:2016:CBE

[YLZ+16]

Yagan:2016:WSN

[YM16]


REFERENCES


Yang:2012:EMA


Yengisetty:2011:AVC


Yi:2016:IPA


Yang:2012:SAK


Yumbul:2015:EEP


Yang:2015:EPS

Bin Yang, Xingming Sun, Xianyi Chen, Jianjun Zhang, and Xu Li. Ex-


REFERENCES


Yang:2018:IAC


Yao:2010:IDA


Yan:2010:ASP


Wang:2011:RDA

Xiangyang Wang, Panpan Niu, and Mingyu Lu. A robust digital audio watermarking scheme using


[Yu:2016:CDI] Yong Yu, Liang Xue,

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 efficient CCA-secure cryptosystem over ideal lattices from identity-based encryption. *Computers and Mathematics with Applications*, 65(9):1254–1263, May 2013. CODEN CMAPDK. ISSN 0898-
REFERENCES


Yang:2016:EPA


Yang:2018:CDD


Yang:2012:LUC


Yang:2012:BPN

Yang:2012:NIB


Yang:2014:PST


Zidaric:2019:HOA


Zhang:2011:TNT


Zhang:2015:IAI


Zhang:2012:AOP


Zhou:2016:IBP


Zetter:2014:CZD


Zhou:2018:SAE


Zhao:2010:PSA

Jianjie Zhao and Dawu Gu. Provably secure authenti-

Zhou:2016:HFD


Gao:2012:DES


Zadeh:2015:ASP


Zhang:2012:LDC


Zhang:2015:BYO


Zhang:2015:STR

REFERENCES

ZHao:2017:RAS

Zhu:2013:TSC

Zhu:2015:IDM

ZHW15

Zhu:2016:SCI

Zhou:2015:EPP

ZHW15

Zhang:2016:PPV
Lei Zhang, Chuanyan Hu, Qianhong Wu, Josep
REFERENCES


**Zimand:2010:SEC**


**Zhang:2011:FBP**


**Zeng:2014:NFC**


**Zhou:2012:CBF**


**Zhou:2015:PPS**

Zhao:2012:IAS


Zhang:2012:EEF


Zhang:2012:CCB


Zhu:2017:PSN


Zhang:2010:ESP

REFERENCES


[ZOC10] Fahad Zafar, Marc Olano, and Aaron Curtis. GPU random numbers via the Tiny Encryption Algorithm. In ??? ?, editor, HPG ’10 Proceedings of the Conference on...
REFERENCES


Zhang:2017:PPN


Zavattoni:2015:SIA


Zheng:2016:EUV


Zhou:2017:IBB


Zenger:2016:AKE

Christian T. Zenger, Mario Pietersz, Jan Zimmer, Jan-Felix Posielek, Thorben Lenze, and Christof Paar. Authenticated

**Zhang:2015:MAA**


**Zhang:2010:EMO**


**Zmudzinski:2012:WEU**


**Zhao:2012:SSM**


**Zheng:2018:GDP**


Zhang:2012:EHO


Zhang:2014:NCM


Zhou:2018:TPW


Zhu:2015:PPD


Zuo:2018:CSA


Zhang:2014:EFH

Zhang:2018:AKE

Zhang:2018:VPA

Zhang:2016:DEP

Zhang:2011:SIR

Zhou:2017:CLR
Zhou:2017:LRC


Zhang:2017:GFD


Zheng:2010:PS


Zhang:2010:ASL


Zhou:2018:CLR


