Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N)
[Bai10, YC11], (n, t, n) [LHYZ12], (t, n)
[QD16, ZPWY12]. 0 [XHX+17], 1
[XHX+17]. 1, 2, 3 [SMDS11]. $100 [Sch16a],
11 [LJ17]. 13 [Blo15]. 2
[AM19, DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGLL10, WK18, WY12]. 22
[MNP12], 2^k [Sun16]. 3
[AP10, Bro19, 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 [AMVZ12]. 4
[COP+14, DWZ12, HLYS14]. $49.00
[Sch15a]. 5 [YN19]. 8 [LPO+17, ZSH+19].

$9 [APPVP15], = [JJUW10], + [PYH+18]. 2
[YNX+16]. 3 [LHM14]. M^T [HRB13]. \alpha
[TTL10]. c [KRDH13]. d [QD16]. d \times d
[KAI7]. \ell [ZTL15]. F_p + \nu F_p [WGF16]. \gamma
[DWZ12]. GF(2) [x] [SF12]. GF(2^m)
[HJ19, SKH15]. GF(2^n) [LBOX12]. K
[FXP12, FR16, CHX13, SG19a, XMY+17,
XLP+18, ZZC17, ZHT16]. L(1/4 + o(1))
[Jou13]. M [MMSD13, OS11]. F_{p^5000}
[AMORH13], F_q [SS13]. A/P [HN10].
GF(2^{15})^2 [GM16b], GF(2^{32}) [GM16b], GF(q)
[LPaS10]. LWE [BV14], \mu [Jia14a]. N
[FR16], n \times k (k \geq n/2) [MC11]. O(d_{13})
[KA17]. O(n^2) [KS11]. P [DG17, GT19], \pi
[EHKSS19]. \pm 1 [HZW+14]. q
[CZCD18, GMS11]. S [LJ15]. t
[HJM+11, Ob11]. w [Kre13].
-Encoded [DG17]. -Encoding [XHX+17].
Advert [MT17]. Advertisement [Ano16, AMBHJ10]. Advertises [AH13].
AEP [LZD+19]. AEP-PPA [LZD+19].
AES [ARG19, ABO+17, BW16, BBS13, BKR11, BB10, DGP10, FAA+18, FLYL16a, FLYL16b, GLMS18, GM16b, HMKG19, HF14a, LB13, Mar10c, MM14b, PBC14, RMT18, SY15a, VGA19, WJ19, YWF18].
AES-Like [BW16, WJ19]. AET [HTC+15].
Affiliation [VKK+19]. Affiliation-Hiding [XLM+12, XGLM14, XZLW15].
Affiliations [VKK+19]. Affine [BCEM15, LYL+18, GZHD12].
Affine-transformation-invariant [GZHD12]. Afraid [Par12a].
Africa [BL10]. Africacrypt [BL10]. after [Sch18].
Against [Ano17e, BVS+13, BCHC19, BL15, BL16, CW12b, CMA14, DZ18, DL17, FDY+19, GDLL18, GDC16, HCE1+12, HLC+19, KMZ19, MS+18, MW18, Sch13, SGL15, SLY+16, WSA15, AATM18, AS16, AYS14, BBS16, BBP13, BD18, BV12, BPR14a, BPR14b, BFK16, BSR+14, BK12b, BH19, Bud16, BCF15, CKHP19, Che15, CG14a, CGCS12, CBY16, CGH17, DHL10, DK17, Dya19, EWS14, FTV+10, zGW12, GSC17, HLLG18, HY+19, JSMT18a, JH12, LDC13, LHM+10, LYL+12, LYL+12a, WC14, MCL+19, Maf16, MBP19, MD12b, MNP12, NDN13, OF11, OSNZ19, QRW+18, SBB15, SEY14, SY15b, SD12, TLL13, WGN+12, Yon12, ZL15, ZHS+19, vV16].
Age [Bla12, SR14, Lan17, Sto12]. Aged [Ree15].
age [Ald11, K10, ABJ13].
agent [GPG12]. Aggregate [CCT+14, PSM17, WCD19, GLB+18, LLY15, LLL+18, ZQW10, ZD18, CLW16].
Aggregated [NLY15]. Aggregated-Proof [NLY15]. Aggregating [DP12].
Aggregation [ARWK19, BJL16, EKOS19, LH10, SP15b, YM18, ZHW+16, DXWD16, DZ16, GL+19, RR17, WMY16].
Aging [SKV12]. Agnes [Bur11, Joh15]. Agnostic [HFW+19]. Agreement [ADSH19, BSBB19, Ch16, HCL+14, HEC+12, KMZ19, MNS11, TM12, WSS12, XLM+12, XGLM14, XZLW15, YLS19, AAL19, AQRH+18, APK+18, AN15, BGAD12, CSD18, CTL13, DLK+16, EBA17, GH16, HPC12, HWB10, HWB12, ISC+16, IB11, IOV+18, KS11, KIH19, KB18, K1W+16, KDL+17, LLL13, LLY06, LIK+17, MHL18, NCL13, Nos11, Nos14, OD1+17, OSA19, PY19, hSZ15, TLL12, WXK+17, XCL13, XCY19, XMHD13, XHM14, YZZ+14, YY13, ZWQ+11, ZTZ16, ZG18a, ZC15, OH10].
agriculture [APK+18]. Aided [BGK12, BCGK12, BGB12, Gop19, GMSV14, LNWZ19, MV19, Vua10, ABBD13, LYL15, SGJ+18, SFA11, WFX17].
AIPISteg [AGL16].
air [AUMT16, KTM+18, VOG18, ZWX+18]. aircraft [XWZ16]. Airflow [RSCX18].
Airway [RSCX18]. AK [XHC+12]. AK-PPM [XHC+12]. AKA [LLLS13].
AKF [KDH15]. al [LWL16, LL17, WZ12, PLP13, SBS+12, Mac14, Keb15].
al-Qaeda [Mac14, Keb15].
al [ABJ13, S14].
Alan [CS12, Don14, Hel17, LCK12]. Algebra [PB17, Xie12b, BS15, Bu10b, CFF11, DWZ12, FG14, Nag19].
Algebraic [ACA+16, HIJ+19, HLC+19, LK19, SK11, Tam15, Wat10, WZ17, Bu10a, CFF11, FM+18, SA14, YTM+14].
Algorithm [AA19, ABC17, Ano11b, AK14b, BGJT14, BKL18, CN14, CS10, jCPB+12, DCM18, ESI12, GKS17, HZ15, JLH12, JSZ12, JH12, J16, KB10, LL11, LT14a, LLL17a, LLLH18, LYL+18, MSR+17, MRL+18, ND11M16, NV10, RR11, RVR12, WHZ12, WZC18, YPR17, YH16, ZSW+12, ZWWW17, AIA+18, Ang16].
Ant14, ARG19, BYDC13, BGMT13, BMB16, CG12b, CJL16, Chm10, EEAZ13, GJ19, HZW19, JK13, Jou13, KY10, KHM13, LC17, LR15, MS12a, MM14b, MNM+16, MN14, PGL110, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WGW+12, XTK10, XWK+17, YW+17, ZLW+12, ZL12, sCR9a, ÁĈZ16, ZOC10. **Algorithmic** [GO17, KRH18, RZ19, AY12a, AY12b]. **Algorithmics** [Gas13]. **Algorithms** [AMKA17, ABSSS19, AB10b, BCG12a, BR19, BJ10b, CN12, GP17, KRDH13, KHRG19, MR14a, MM17a, RPHJ11, TKM12, WH18, WRP70, YS15, ZW15, AGHP14, FLYL16a, Fri10a, KKH13, MR14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WGW+12, XTK10, XWK+17, YW+17, ZLW+12, ZL12, sCR9a, ÁĈZ16, ZOC10]. **Algorithmically** [GO17, KRH18, RZ19, AY12a, AY12b]. **Algorithmics** [Gas13]. **Algorithms** [AMKA17, ABSSS19, AB10b, BCG12a, BR19, BJ10b, CN12, GP17, KRDH13, KHRG19, MR14a, MM17a, RPHJ11, TKM12, WH18, WRP70, YS15, ZW15, AGHP14, FLYL16a, Fri10a, KKH13, MR14, PGLL10, PA10, PC14, SH11, SLM10, SWW+17, jT12b, TTL10, WGW+12, XTK10, XWK+17, YW+17, ZLW+12, ZL12, sCR9a, ÁĈZ16, ZOC10].
[BDK11, TG12]. anonymizing [TMK11]. Anonymous [APMCR13, CG12a, CZLC12a, CCF17, Chi12, DK12, FHH10b, FHZW18, HL+15, KP18, LK+17, LSQX19, LZCK14, Muf16, Per13, RSN14, SYWX19, TAKS10, Ver17, Wan14, WX+17, WYML16, ZJ14, ZMW16, AIKC18, AKS19, ATK11, BT18, CCSV11, Chi13a, CGH11, FSGW12, Gop19, GTSS19, HL14, ISC+16, KCS+18, LNK+18b, LZD+19, LWK+19, LHM14, LSQ15, LYL15, LY14, MYMY13, MML16, QMC17, VS11, WLS14, XXYC19, YZL+18, YYK+19].

ANSI [Ano11b]. answer [Pec12]. answers [Wu16]. Anti [Alz19, KKK+18b, QZ14]. Anti-Counterfeiting [Alz19]. anti-forensics [QZ14]. Anti-reversible [KKK+18b]. Antinoise [WXL+17]. Antispoofing [MR14b]. Antoine [AY12a, AY12b]. Any [BHT18, Goo12, LP11]. anything [Nor17]. AODV [SS15]. Apache [Lit14]. APBT [ZWWW17]. API [FLW12, PTRV18, QF19]. Append [YNR12b]. Append-Only [YNR12b]. Applicability [Ser18]. Application [AKP12, AK14b, BD15, BRT12, BS12, CCL+19, CCKM13, CCKM16, CCW+10, CWZ19, CST16, CECZ10, CHS15, JS18b, KÜP15, LW11a, LW12P12, MNS11, O102, SEHK12, SS13, JW+16, YWK10b, YTS12, ZH15, ZM16, AB10, BGE+18, BBP13, BT18, CCI15b, CBAY16, GLIC10, GSGM16, HURU11, HH15, JZU+19, JIA14b, LGK10, LWKPI4, MS+18b, NALT17, OTO18, SE18, SFCFCR+18, WYY+17, WDG19, HXH12, YY11, ZWWQ+11, ZAC17]. Application-Level [CCW+10]. Application-Specific [BD15]. Applications [AMVZ12, AEP18, ANA14, ABL+18, BBD19, BKPW12, Ber18, BKST18, BCG+12b, BJCHA17, BSV12, CZLC12a, CZLC12b, CPS16, CK18, DK02, DK07, DK15, FSK10, GKM16, GRL12, HSC19, HVS12, HJ19, HN10, HGOZ19, HVP+18, JW+17, LATV17, NAC12, NV10, Nie02, ÖDDS17, PJ12, RBS+17, RQD+15, SAS18, SCPNS10a, SCPNS10b, SG19b, Sha10, Shp03, SY+19, Ter11, TKY+12, WH17, YR11, ZQQ+19]. ZYY19, APMCR13, Ano11a, AKS19, BDK16, CFF11, CSZ+11, CQX18, CDA14, Dur15, EBFK13, FES10, Fri10a, GJJ18, GHDK19, Gil10, KKK+18b, KO16, LWZG10, LSQ15, LR15, LBOX12, LTT10, MS13c, MZL+19, MM14b, OSP+19, OK18, PHWM10, PKA15, SWW+17, WMC17, ZZ15, ZSMS18].

architecture-independent [BVIB12].

Architectures [AMKA17, BGG+13, BJCHA17, CMO+16, CHS15, DFKC17, FP19, MTKM18, MKAA17, MKASJ18, RMERM19, SRT12, ST19, FPBG14, HL14, LGP19, MK11, Nov10, SHC+16].

archiving [VBC+15].

Area [GMVV17, GM16b, HC17, LZCK14, RMTA18, WH17, ABO+17, KP18, LMJC11, LKK+17, LZZ19b, Nov10, SGJ+13, WDV18].

Area-Optimal [GM16b].

Area-Time [HC17].

Areas [MV12, JY14].

Argon2 [BDK16].

Argon2i [AB17].

argues [Dya19].

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

ARIA [PH12a].

ARITH [MSH+16, TBL19].

ARITH-26 [TBL19].

Arithmetic

[AIK14, AAB17, BF19, BD19, CATB19, DDE+19, EZW18, Fr10, GH11a, HSA14, IEE13, KHF10, MSH+16, PG12, Roh19, TBL19, TT18, ZAG19, DTZZ12, MO14].

ARM [BYDC19].

ARM-FPGA [BYDC19].

ARMv8 [SD18].

ARMv8-A [SD18].

Array [BL12, MCD12, NKWF14].

Arrays [LB13, TRD11, EAB+19, KM10a].

ARSENAL [SM18].

Art [ABJ13, BLM17a, BLM17b, LL18, OMNER19, Sen17, BD11].

Artificial [SG19b].

Arvind [Ano16a].

ARX [MPC10, SJKL18, BPB19].

ARX-Based [SJKL18].

ary [CZCD18].

ASA [YWF18].

ASIANCRYPT

[LW11a, Abe10].

ASIC

[CFZ+10, KMY18, MKAA17].

Asking [DL15].

ASM [Vle12].

ASM-Based [Vle12].

ASP.NET [DR11].

Assessing [CBL13].

assets [WHJ17].

Assignment [LMS16].

Assisted [KCC17, LLKA19, GM13b, GPR+19, HZW18, WDV18].

Associated [Sar10b].

associative [BS15].

Associativity [ABR12].

Assumption

[CCL+19, LZC12a, LZC14, ZG10].

Assumptions

[BDH11, CZF12, DN12, EKOS19, GKS17, KZZ17, KM10c, PDHN15, SMB15, ABW10].

Assurance

[BMM10, Bar15, KMP+11, RBNB15, WL11, Ser12].

Assured

[Tan15a, WMYR16].

Asymmetric

[DBG19, HG12, XLM+12, XZLW14, ZZQ+19, ZZQ+19, CSS+13, ZGL+18a].

asymmetric-histogram [CSS+13].

asymptotic [DTZZ12, TD14].

Asymptotically [LPS11].

Attack

[ABSS19, Ano15d, BRS17, BEM16, BMS12, Bro17, Che18, CWZ19, CJP12, DHT+19, DSB15, GQP+17, GQL18, GDCC16, HSC19, HETP+12, HLAI15, JH12, KP12, Kam19, LOSW16, LGL+12, LJ17, LCL17, LJ19, LBC18, LWKP12, LWKP12, LF19, MSS17, MSS+17, MPA+18, MWES19, MS12b, Pud12, SKE+18, SMB15, SP13, SS15, SDM+12, WLC12, XJW13, YTF+18, YWM19, Ano17a, AYSZ14, BD18, Blo15, BNST17, CAM19, CJ15, DDF13, FLZ+12, Goo12, GSAV18, KA17, LLY+12a, LC13, LYHH14, LWKP14, MBB12, MN12, NZL+15, OPS14, SB17, SXL16, SCBL16, WL13, vV16].

Attacker

[BCEO19, BCEO20, PLGMC18].

Attackers

[BL15, BL16].

Attacking

[Bon19, GJ19].

Attacks

[AMMV18, AB17, ARP12, Ano17e, BGK12, BCHK19, BHC19, BKF16, BKBK14, CZ19, CKHP19, CBRZ19, Che15, CMA14, DZS*18, DGS12, DL17, DHLW10, DHD16, EWS14, GPT14, HLLG18, HJ+19, Hay13, HLC+19, HR16, JSK+16, JWJ+17, KNR10, LL11, LWZ12, LH14, LJI18, LW19, LWCJ14, LWML16, LCL17b, LYD+18, LSG+19, MD12b, PDP+19, PYM+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, VWC19, WW14, WHN+12, XNG+14, YKA16, YL17, YCM+13, ZLQ15, ZHS+19, AATM18, ACD18, BBP13, BVIB12,
BCDN17, BZD+16b, BSR+14, BH19,
BCFK15, CBJY16, CGH17, dCCSM+12,
DCAT12, DJL+12, DK17, Dra16, Eng15,
EA12, FTV+10, FIO15, GPM+16, GLMS18,
GBNM11, HAK19, HAGtFr13, KM10a,
KPS10, LDC13, LHM+10, LWK11, MBP19,
NDNR13, OF11, PX13, SGP+17, TK19,
TS16a, TY16b, TLL13, VS11, WWBC14].
attacks [XWDN12]. attempt [Fel13].
Attestation [BWS19, FQZF18].
ATTiny [EGG+12]. Attribute [AAC+16, AHW+12,
BFK+10, Boy13, CD16b, CDL18, CDLW19,
CHH+19, FHR14, GZZ+13, GSW+16, Gli12,
GVW15, HSMY12, HBC+19, Her14, KGP12,
LW11b, LW11c, LW12, LJJC12, LYZ+13,
LHL+14, LAL+15, LHL15, LW16, OT12,
Ppa18, PB12, RVH+16, Rao17, SSW12,
TYM+17, WDC18, WHL15, WHL16,
WHL17, XMLC13, XWLJ16, XHX+17,
ZPM+15, ZQG15, ZMZM17, ZHW15, BTJ15,
CPPT18, FNWL18, HZL18, HZW18,
HY18, HKH13, JSMG18a, JSMG18b,
LCL+15, LFZ+17, LFSW15, LY15,
LJW+17, LJY18, LDZ19, Nam19,
QRW+18, RD17, SSL+19, WLG11,
WZC16, WXS17, ZXP+19, XTZ+19,
YSG19, YCT15, ZWM14, ZML17,
ZGL+18a, ZPY+19, Ver17].
Attribute-Based [AAC+16, BFK+10, Boy13,
CD16b, CDL18, CHH+19, FHR14,
GZZ+13, GSW+16, GVW15, HSMY12,
HBC+19, LW11b, LW11c, LW12,
LJJC12, LYZ+13, LHL+14, LAL+15,
LHL15, LW16, PB12, RVH+16, Rao17,
SSW12, TYM+17, WDC18, WHL15,
WHL16, WHL17, XMLC13, XMLJ16, XHX+17,
ZPM+15, ZQG15, ZMZM17, AHW+12, CDL18,
Her14, WHL16, CPPT18, HZL18, HY18,
HKH13, JSMG18a, JSMG18b, LCL+15,
LFZ+17, LFSW15, LY15, LJW+17,
LJY18, LDZ19, Nam19, QRW+18,
RD17, WLG11, WZC16, XWS17, ZXP+19,
XTZ+19, YSG19, YCT15, ZML17,
ZPY+19, Ver17]. Attribute-Hiding
[OT12, ZWM14]. Attributes
[CG12a, VKK+19, Yon11, LCL+17a].
Attribution [AIF+19, XHC+12, FNP+15].
Au-Id [HWZZ19]. Auction
[Con10, JWNS19, DDL15, HJM+11].
auctions [MR14c, QS18]. Audience
[DTE17]. Audio
[Ber18, DA12, FM15, GCK12, HGT15,
KD12a, KD12b, LSD12b, NXH+17,
QF19, TC10, wWnY+14, XNG+14,
XNRG15, XNP+18, ZS12, LSQ11a, SKEG14,
yWnL+11, WY12, YQH12].
Audio-Visual [LaL14]. Audit [YR12b].
Auditing [LMD16, LCDP15, TCN+17,
XW+17, YYS+16, YXA+16].
Augmenting [AV18]. August
[AB10a, JY14, MV12, Rab10]. Aura
[HFCR13]. Austin [IEE13]. AuthCropper
[KLK+19]. Authentic
[ASV+18, HLT+15, ZMK13].
Authenticate [HM12]. Authenticated
[Alo12, ADSH18, BSBB19, BCO13,
BDMLN16, CLR16, CLY14, CCS14, CRE+12,
DS11, EAA12, ESS12, FVS17, FLI12,
GT11, GL12, GZ12, HC12, HL10a, HCL+14,
HEC+12, KMY18, CLK+19, LKR10, LY16,
LH11c, LCCJ13, LTT10, MR14a, MMY12,
MMS17b, MHK14, MU13, PT16, Sar10b,
Smi11b, Tan11, TW14, WD18, XLM+12,
XHC+12, XGLM14, XZL15, Y12,
YLS19, YLW13, YRT+16, Yon12, ZPZ+16,
ZXH16, ABC+18, AIB+16, ABR15, CTL13,
FA14b, FIO15, GPM+12, GLM+11, HPC12,
HW10, HB12, HL11, HPY10, ISC+16,
JKA+18, KMTG12, LWS10, LHH11,
LML+13, NCL13, Nos11, Nos14, OD+17,
OSAN19, PPT15, P18, PPG19,
SMBA10, TCS14, Tso13, TKHK14, WZM2a,
WZM1b, WTT12, XWC14, XCL13,
XWZ+18, YC12, YZZ+14, YZL+18, YLL+18,
ZT16, ZGL+18a, ZXW18, ZG10, ZZC15].
Authenticating
[BS12, CHX13, GRL12, OKG+12, RPG12,
WY12, ZCW15, BCI8, Cer18,
Authentication

[AV18, AA19, ADM19, AAA+19, AMSPL19, ASO14, AAZ+16, ACAT+15, ACKB19, AUMT16, ABB19a, ATC17, BL12, BCE+12, BCM12, BNNH19, BSSV12, Bel18a, BKST18, BCD+12, Bis17, BF11, Boy16, BKPJ12, BSV12, CGCGPD12, CTC+15, C14, CSH+18, CRS+18, CCW+10, CCF17, C13, CD12, CJP12, CLH13, DL15, DCM18, DBPS12, DKW11, DP12, FLH18, LLG15].

Authentication

[AV18, AA19, ADM19, AAA+19, AMSPL19, ASO14, AAZ+16, ACAT+15, ACKB19, AUMT16, ABB19a, ATC17, BL12, BCE+12, BCM12, BNNH19, BSSV12, Bel18a, BKST18, BCD+12, Bis17, BF11, Boy16, BKPJ12, BSV12, CGCGPD12, CTC+15, C14, CSH+18, CRS+18, CCW+10, CCF17, C13, CD12, CJP12, CLH13, DL15, DCM18, DBPS12, DKW11, DP12, FLH18, LLG15].
PKA15, PRN+19, QMC17, QMW17, QLZ19, RR17, SSSA18, SCFB15, SPLHC14, SB17, SGGCR+16, Sar10a, SK18, SSNS15].

authentication

[SVY19, SGJ+18, hSZZ15, SCKH10, SYWX19, SNG+17, SCR19b, SA15, SYW17, SSS11, SKEG14, SA19, SMS+16, SHBC19, Tan12b, Tan15b, Tan18, TODQ18, TZTC16, TG17, TLL12, VSB+19, Wan13, WW14, WLZ+16, Wan18b, WCFW18, WXSH19, Wat14a, Wat15, WDKV19, WT10a, WKH11, WXK+17, XHH12, XWDN12, XHCH14, XXY19, XMHD13, XHM14, YI17, YHL16, YHHS16, YYK+19, YWK+10a, YSL+10, YMM13, YN19, YY13, YD17, ZYL+10, ZQWZ10, ZCLL14, ZQD16, ZGL+18b, ZDH18, ZZY+19, ZXX11, ZLY+19, ZZL+18, OHJ10].

authentication-chaining[EA11].

authenticators[SYY+17].

authenticity[ADF12, VBC+15].

Authority[LXNY15, XZLW15, ZQQ15, JB11, SLL+19, ZWY+19, ZZ12].

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

Authorized[GHY18, HTC+15, LLSW16, Ma17a, WZCH19].

Authorship[AIF+19, BTV15, BAG12, LCM+17].

Autoblocking[LHLL18, YH16].

Automata[CCD15, Gas13, dRSdlVC12, Ang16, DGL19, HBBRM+16, KEF19, SS11, WOLS12].

automata-based[SS11].

Automated[BHC19, CCK12, CCK16, DRS16, GLLSN12, JGP+18, LGM+16, Ste15a, Tom16, YSS14, BJ+14, GMMJ11, KKK+16].

Automatic[HWZZ19, MMP19, WW12, HL19].

Automation[BGK12, DZS+18, IEE11a, KPP16].

Automotive[HK18, LMS16, MPM+17].

Autonomic[SEK+19].

Autonomous[MPA+18, BT18, SMS+16].

Auxiliary[DMS+16, DL12, GGHW17, XXZ12, YCY12, Kom18].

Auxiliary-Input[XXZ12, Kom18].

Availability[CK11, ADF12, CFV16].

Available[Ano16e, HGOZ19].

AVC[JSZS12, JHKN12, LW13c].
averged[Lim11, YL11].

Avoid[CFZ+10].

Avoidance[RV+16].

Avoiding[AMMV18, BHcFR12].

AVR[LPO+17].

award[Ano16i, Orm16].

Awarded[Ten18].

Aware[ARWK19, BCF16, HFS+19, JSA17, LJ17, LMHH14, LMS16, QLL17, YTH17, ARL13, AKS19, DDY+19, GHD19, LWYM16, MGP10, TODQ18, Wan13, ZDHz18, ZFH+18].

Awareness[HSC19, MSas12, SAM+18, HPJ+19, Li10, MSas13].

axiomatic[AT10].

axis[WMU14].

Azure[Sti19].

B[Ben12a].

B-Spline[Tan12a].

B3G[NXS10].

Bacterial[Kar12].

Bad[KMZS19, CHH+13, Hai17, RY10].

BAF[YNR12a].

Bake[Boy16].

Balanced[TY11].

balancing[FXP12, PRN+19, Zha15a].

Balloon[AB17, BCGS16].

Ballot[vdG17].

Ballots[CW12b, LHF12].

balls[Svo14].

band[MMSD13].

Bandwidth[ST13, NR11, LLZ+12].

Bandwidth-Efficient[LLZ+12].

Banking[Eya17, KSD+17, RBS+17, GMMJ11, KVvE18].

banned[Eve16].

BANs[BLL+19].

Baptiste[Dew11].

Barbara[Rab10].

Barcodes[WW12].

Barriers[LY12].

base[DBT19, MS12a, XSWC10].

Based[ADM12, AD19, AGW15, ASM12, ABSS19, AAC+16, ABC17, Ano11b, ASS15, AY15, AT17, BWLA16, BL12]
BCEO19, BCEO20, BBΦ+16a, BSSV12, BHG12, BKPW12, BRT12, BHH+15, BBKL19, BS13b, BFK+10, Bon12, BSJ15, BF19, Boy13, BKJP12, BDH11, BCF+14, But17, CMLSI5, CLLL6, CGMO14, CKHP19, CMRHI7, CCM17, CSH+18, CZLC12a, CZLC12b, CLHCl12, CCZC13, CLY14, CZLC14, CST+17, CZCD18, CLND19, CGL+12, CDD13, CGY+13, CD12, Chi12, CK18, CD16b, CDLW19, CHH+19, DSM14, DHT+19, DL17, DS19, DA12, DLZ+16b, EM12, EKF18, FM15, FHH10b, FHR14, FZT14, FGRQ18, FGM10, FYD+19, FR15, FVS17, FP19, FSX12b, FSX12c, FSX12a, GT19, GWWC15, GDLL18, GZZ+13, GSW+16, GV14b, GI12, GY13, GCC16, GSV15, GJJ15, GJJ17, GRRZ18, HZC+12, HSMY12, HSM14, HBC+19, HEP+11, HIJ+19, HL10a, HXZ15, HWZP18, HCPLSB12, HKL+12. Based [HG12, HM12, HSA14, HWS+19, HPO+15, HKR+18, HGT15, HCL+14, HLN+10, HUi13, HRS16, HBG+17, HEC+12, HM19, HP12, HP17, JTZ+16, JP19, JHNN12, JEA+15, JKHv12, KMZ19, KS18b, KG10, KK12, KKA15, Kha10, KLY+12, KSSI12, KPKS12, KHRG19, KRB12, KAK18, KS15, LMG17, LMG+18, LXY+18a, LXY+19, LTK16, LSL12a, LKBK19, LSL12b, LW11b, LW11c, LW12a, LW12f, L12J, L12Jc, LZ+13, LHL+14, LTH+15, LCC+15, LDZ16, LITZ16, LLZ+17, LLLH18, LPL15, LSL15, LAL+15, LH11c, Lin15, LYL+18, LP12, LNWZ19, LNZ+13, LCCJ13, LWCJ14, LNX15, LHL15, LW16, LPO+17, LW18, LL1b, L19, L19a, LGPRH14, LDB+15, LD13, LSC12, LBR12, LL18, MWZ12, Mad17a, MLO17, MEF012, MCD12, MV12, MD12b, MBC15, MKN13, MZ17b, MCS+15, MMS17b, MKΦ+16, MCF17, Men13a, MST18, Mor12, MSKRJ17, MKAA17, Mu16, NIS15, NC12, NXX+17, NDR+19, NXB13, NLL12, NLY15, pNyWyY+14. Based [OTD10, PB12, PSSK19, PTT16, PYM+15, PDNH15, PPS12b, PY18, PG12, PAS13b, PNRC17, QJC+18, QF19, RVH+16, RSR+19, RZZ+15, RS16, Rao17, RRV11, RDZ+16, RVRSCM12, RW12, RJJ+18, SBS18, SSW12, Sar18a, SS13, Sen17, SLK18, SXH+19, SJ12, SGP+12, SPG+19, SP15b, SSA13, SRAA17, SNCK18, SH15, SG19, TKB14, TWZ11, TW12, TW+12, TYM+17, TSH17, TT12, TTH15, TFS19, TC10, VDB+16, VG15, VGA19, Vel12, WY10, Wan10, WSSO12, WgMW12, WYW+13, Wan14, WZCC18, wWxY+18, WDC18, WHL15, WHL17, WCL+18, W10b, WMS+12, WZ19, XNG+14, XNRG15, XXZ12, XMLC13, XQL09, XQL11, Xio12, XGML14, XW16, XJW+16, XJR+17, XHX+17, XHZ+19, YE12, YLZC12, Yxz+12, YGFL15, YHSW19, YTS12, Ye10, Ye14, YH16, YTH17, YYO15, Y+17, YKNS12, YHK+10, YMWS11, YKC+11, YFK+12, YCY+12, ZSP+19, ZPM+15, ZJ11, ZZZ+11, ZDL12, ZLH+12. Based [ZQQ15, ZMW16, ZXYL16, ZWW17, ZMM17, ZW17b, ZYZ+19, ZPW16, ZHW15, ZVG16, ZPX17, ZGCZ18, ZMY18, ZYH+19, ZHL15, AMN18, AGLW16, AaBT16, ARL13, AY14a, AHS14, AAL19, AAT16, AA14, ASO14, AIA+18a, AIM+19, AKG13, ASVE13, ACA+16, ARG19, AM19, Ara13, AT+10, ACC+13, AHL+12, BK19, AVA18, BS15, BDM18, BDL+19, BBP13, BD8, BGAD12, BAAS13, BBTC20, BDM+19, BOB13, BWR12a, BW13, BWA13, BMM12, BZD16a, BC18, BTK15, BBΠ16b, BK12b, CPPT18, CML+18, CXX+19, CFL13, CFY+10, CCL11, CTL12, CLSW12, CNF+18, CRS+18, CG12b, CSZ+11, CHX13, CSS+13, CW14a, CLC+19, CWZ19, CWXT19, CCM19, CTHP13, CJP12, CJP15, CCG10, CTL13, Cho14, Con12, CHL19, dCCSM+12, Cra11, CML18, DSCS12, DGMT19, DZ14, DL13, Dra16, uHAN+18, EZ15, FHI13, FG19, Far14, FA14a, FA14b, FIO15. Based [Fay16, FLY16b, FHZW18, FMC19,
FNWL18, Gal13, GJ13, GCH+19, GMOGCC15, GMRT+15, GKCK11, GJMP15, GCSâddP11, GAB19, GMS11, GLL+18, GBC19, HSH11, HT11, HKA+18, Ham19, HZV19, HW19, HHZS18, HGWY11, HSM13, HZC+14, HZL18, HF14a, HWDL16, HZW17, HZWS18, HBBRN+16, HLR11, Her14, HWB10, HB13, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HFY18, HPY10, HKHK13, HCC10, Hwa11, IMB17, IM14, ISC+16, IB11, IA15, IOV+18, Jâc16, JNUH17, JKAU19, JK13, JLT+12, JCL+18, JZS+10, JMW+16, JSMG18a, JSMG18b, JLX+19, JDV16, KFE19, KPF16, KK13, KM10a, KHMB13, KTM+18, KKG14, KCS+18, Kh18b, Kdz18, Kd18, KIm11, KGO10, KD19, LKW+17, KKD+18, KL11, KSH18a, KSH18b, LXL12, LLZ+16, Lâu12, LLC10, LK14, LHM13, LYG+10, LHM+10, LH10c, LZX10, LNM+11, LMCJ11, LK12, LNXW12, LKAT12, LLHS12, LNK13, LNX14, LDZ+14, LCL+15, LZY+16], based [LWYM16, LFZ+17, LNK+18a, LWK+18, LWW+19, LCT+14, LFWS15, LLM+19, LPdS10, Lin14a, LHL+18, LLY+12a, LW10, LSQ11a, LSQ11b, LWK11, LW13b, LZC14, LPZJ15, LFC+15a, LLZ15, LY15, LW+17, LW18, LDZ2W19, LW+10, LL16a, LW13c, LWY12, LY14, MCN+18, MCP15, MJGS12, MJJS13, MLM16, MWW+18, MZL+19, MMF15, MMZ12, MM13, Mes15, MCRB19, MBB11, MO14, MSGCDPSS18, MHT+13, MG15, MS17, Nam19, NR11, NM18, NCL13, NZL+15, NMX15, OMPSP+19, PPA18, PYH+18, PLWP13, PTK14, Par18, PWW10, PGLL10, PZL+19, PPD16, PLGMCdF18, PCK19, PS14, PL16, Pka15, PC14, PPR+12, QDZJ16, QRW+18, QYWX16, QMW17, QZL19, RD17, RG10, RS15, SPLHCB14, SERF12, SGGCR+16, SLL+19, SAM+19b, SI12, SD17, SYL13, SE14, SE16, SK18, SH11, SM11, SNM14, SZHY19, SR10, sSZ15, SCKH10, SA16b, SPK17, SSSAF11, SHC+16, SWW+16, SSS11]. based [SKEG14, SC19b, Sun16, SGM16, SHBC19, SS11, TPL16, TQL+14, Tia15, TH16, THA+13, TTL10, TPKT12, TKHK14, URK+19, VS11, VN17, WWY11, WWY11, WLWG11, WLDB11, WZC16, WLFX17, WMX+17, Wan18a, WXMZ19, WSX19, WZD19, WGZ+12, WHLH16, WS14, WS27, WTLT2, WOLS12, WCCH18, XH12, XWZW16, XW12, XCL13, XWS17, XZP+19, XHCH14, XWZ+18, XTZ+19, XMHD13, XHM14, YWL+17, YWJ+19, yQyWqZC13, Yan14, YTM+14, YCC16, XYA+18, YSMS19, YWY+19, YCT15, YTF+18, YY13, YLS12, YMSH10, YKC+12, YZL+16, XYA+16, YL11, ZZKA17, ZAAB17, ZYG17, ZLW+12, ZCLL14, ZT14, ZTZ16, ZQD16, ZML17, ZGL+18a, ZGL+18b, ZWY+19, ZZ12, ZHH+17, ZL12, ZVH14, ZDW+16, ZYM19, ZLY+19, LZJX10, Ver17, HZC+14, MM12, PP11, ZBR11, Kat13]. Based-Encryption [ZH15].

[ACAT+15]. **Bletchley** [Bai12, Ano11c, Bri11, Cop06, Cop10a, Cop10b, GMT+12, GW14, McK10, McK11, McK12, Pea11, Sim10, Smi11a, Smi15b, Smi15a]. **Blind** [AP10, Ano15a, BCPV11, LCLW17, LGPRH14, MR16, MN12, RS16, YMWS11, HKB14, MO14, RSM15, RMG18, WLB11, yWpWyYpN13]. **Blindfold** [Nac16]. **Blindfolded** [Vai11]. **Blinding** [CLHC12, KHHH14]. **Block** [AMVZ12, BRS17, BSS+13, BFMT16, BDGH15, BCG+12b, CWP12, DWZW12, EGG+12, FX+17, GLLS12, GT12, GST12, GNL12, IS12, KR11, KWS+12, LYK19, LWZ12, LJ17, LCLW17, LG11, LWKP12, LWPFD12, MCDB12, MRTV12, OKG+15, PH12a, PDJ+19, PRC12, Pud12, SJLK18, SG+12, SSA13, WW12, YCL17, ZSW+12, BNY14, Jel13, KM11, LGP19, LPZJ15, LC13, LYYH14, LWKP14, MCL+19, MNP12, MHV15, MHY+18, PL16, Sar11, SKK10, TQL+14, Tan17a, WB12, WWBC14, ZSW+18a, JKP12]. **Block-Parallel** [MCDB12]. **Block-Wise** [SSA13]. **Blocka** [CHL19]. **Blockchain** [Alz19, Ano19c, ATD17, AHWB20, CLC+19, Eya17, Hur16, HM19, JWNW19, KV18, NML19, Pec17, Scr18, SG19b, SZZG19, TBY17, VFS+19, ZXL19, HHBS18, JXL+19, LHH+18, Nor17, CHL19]. **Blockchain-Based** [HM19, HHBS18, JXL+19, LHH+18]. **Blockchain-Enabled** [KV18, NML19]. **Blockchain** [BNMH17, RM19, WSL+19]. blockc cipher [CMS17]. **Blockciphers** [LST12]. **Blocks** [JSK+17, Bra15]. **Bloom** [ATKH+17]. **Blowfish** [KB10]. **BLS** [BP18]. **BlueKrypt** [Gir15]. **Boardroom** [LHF12]. **Bodacious** [KM10c]. **Body** [LZCK14, LCR+18, ASO14, KP18,LIK+17, LZZ19b, SGJ+18, WDV18]. **body-sensor** [ASO14]. **bogus** [XWDN12]. **Bombe** [Bur11, Car10]. **Bonebrake** [SS10c]. **Boneh** [TK19]. **Bonneau** [Ano16a]. **Book** [Ano15b, Ano16a, Ano17b, Ayu12, Bar12, Dew11, Ful10, Jol10, Keb15, Koi10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12]. **Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LVV11, WT13, YCC16, ZZQ+19]. **Boolean-based** [CW14a, YCC16]. **Boomerang** [BCG10]. **Bootstrapping** [BGV14, GM14, KJ+16]. **Border** [LGM+16, ZTSR12]. **Born** [LJJY16]. **BotMosaic** [HB13]. **Botnet** [NSA15]. botnets [HB13]. **Bottom** [Smi11b]. **Bound** [GR19a, LST12, Raz19, WJ19, TK19]. **Bounded** [GVW12, GJO+13, PDNH15, QZ18, SS12a, ZYT13, IM14]. **Bounding** [ABB+19b, PYH+18]. **Bounds** [BCG19, CK17, Jia17, LJ15, SNJ11, SS10b, Sha10, Shp03]. **Bouzefrane** [Ano15b]. **Box** [BW16, BCGN16, BCKP17, BR14, CPS16, HHP17, KMO14, LYL+18, Mic10b, RMTA18, Rja12, SS10b, SWF+19, KOS16, KCS+18, LRW13, MSas13, RPM10, SGFCRM+18, ZZL12, ZSW+18a]. **Box/Inverse** [RMTA18]. **Boxes** [MM17b, NN12, WJ19, LJ15, SS11]. **Boyle** [Mat19]. **BRAMs** [DP10]. **Branch** [EPAG16, ZYY19]. **Branchless** [PBS+17]. **Brandt** [DDL15]. **Brave** [KM10c]. **Brazil** [BA18]. **Brazilian** [Uto13]. **Breach** [SD12, JB11]. **Break** [Ayu12, BP06, Win17]. **Breakers** [Sti15, Mun17]. **Breaking** [AP13, CN12, Che18, Cop10a, GMT+12, KS11, RSM19, TPL16, WGMdZJ12, Ant14, Bri11, SJ19]. **Breaks** [Ano17e]. breakthrough [Goo12]. **breath** [LSR13]. **Breathing** [CSH+18, CRS+18, HCYZ18]. **Breathing-Based** [CSH+18, CRS+18]. **BreatheLive** [HCYZ18]. **Bregman** [CCZC13]. **Bribery** [CW12b]. **Bridging** [LRW14, TMGP13]. **Briggs** [Bai12]. **Bring** [Zha15a]. **Bringing** [Ano15c, OYHBS14]. **Britain** [Ald11]. **British** [And13]. **Broadcast** [BS14, GMVV17, HMR14, KH10, LMGC17, LMG+18, PSM17, PPS12a, RMZW19,
SXH⁺¹⁹, WQZ⁺¹⁶, XJW⁺¹⁶, Yan14, ZHW15, CPPT18, DLN13, SM19b, WWYY11, WDZ19, XWDN12, XZP⁺¹⁹, YMM13, ZWQ⁺¹¹, ZZ12, Zhyu13.

Broadcasting

Browser


Carol [Xie12a, Xie12b]. Carry [GWM16].
Carrying [PV17]. Carved [LC15].
CASCA [DZS+18]. Cascade [WGD18].
cascaded [DGL19]. Cascading [GT12].
Case [Alo17c, DR11, Kni17, SBS+12, SY15a, SRT12, Uto13, YL17, Dya19, KD18, LKKL13, MD12a, SS17a]. Cases [SG19b].
Cash [YMWS11, Bro12, Pec12, Zor12]. Casting [CW12b].
cat [Pow14]. Catalan [SAM+19b]. Catalog [AHS13]. Catching [SXH+19]. CBA [KRM+10]. CCA [AHS14, BWLA16, CBJX19, CZLC14, HWS+19, LLPY19, LTZY16, LSLW15, LLG19, MSas12, PDNH15, SYL13, SLZ12, yYqWqZC13, ZYY19, ZY17a, ZSW+18b].
CDTA [YFT17]. cell [LLY+12a].
chaff [KHMB13]. Chain [EAA+16, FVK17, KPW13, QZL+16a, QZL+16b, YFT17, YSF+18, YFT18, CR12, Par18, CL16, SJWH+17]. Chaining [GGK18, YM18, EA11]. Chains [GKG19, JSDK+17, HLYS14, JCHS16].
Challenge [AD12, GHS14, SPK17, YDH+15, ZCC15]. Challenges [CN12, FREP17, FS15, Fra15, Lal14, LLG16, MRS+17, PCY+17, SBV14, TCMLN19, ALL+18, HTH16, KJN+16, WS14].
Changes [ALL+18]. Change [KMJ18, ZWT13].
Changeable [FGM10, ZCL+12]. changed [Mac12]. changes [PTRV18]. Changing [Abb12].
Channel [AMMV18, AN17, ASN11, ACA+16, Bar16b, BCHC19, Bul18, CDK+10, CBL13, CATB19, DZS+18, EWS14, GWM16, GPT14, HLH19, Kop12, LGR14, LWM16, NDC+13, PRC12, SG15, TT12, YL17, ZBF18, ADG16, 
BVB12, BCDN17, CPPT18, CAM19, DMWS12, DJL+12, GZSW19, GSAV18, 
JLT+12, LM14, LFK19, MFH13, ZGY18].
Channels [ASN12, BGN17, DKMR15, EPAG16, 
FDY+19, KW14, SS19, VCD16, Vu10, 
YDV19, AGH+17, BCND19, BEB+18, CL16, 
DMV15, DKL+16, LWZG10, MCL+19, 
NR11, SM19b, SRB+12, WMU14, ZPZ+16].
Chaos [AIA+18a, LW13c, RR11, 
RVRS12, ARG19, CCLL11, LW13b, 
JT12b, ZLW+12, SGFCRM+18].
chaos-and-Hamming [CCLL11].
Chaos-Based [RR11, RVRS12, 
AIA+18a, LW13c, ZLW+12]. Chaotic 
[BCGH11, IAD10, LFX+18, Ye10, Bro19,
GCH15, ISC+16, KCS+18, KLW+16, LWK+18, LWW+19, LW10, LZKX19, NES+14, WDG19, WGW+12, ZT14.

Chapman [Fa11]. Character [SS12b].

Characteristic [BGJT14, NR15, SR10, ZWZ17a, BGJT13, Jou13]. Characteristics [SPF19, TCMLN19, BEB+18].

Characterization [ALR13, BS13b, CRS+18, DPCM16, RZ19, YZLC12, YDV19, DDD14, PLGMCdF18].

Characterizing [Ash14, JR13, RVS+18, MPJ+16, MPJ+16]. Charging [CKHP19, LSY+16].

Chart [Pec17].

Chattarjee [Kat13].

Cheat [WS12].

Cheat-preventing [WS12]. Cheater [KI11, Oba11].

Chebyshev [HD19, LWW+19, LPdS10]. Check [GST12].

Check-before-Output [GST12]. Checkability [LHL+14]. Checkable [IW14].

Checking [FYMY15, YL17, SYY+17, YXA+16, PZL+19].

Check [GST12].

China [BYL10, IEE11a, LTW11, Yan10].

Chinese [HF14a].

Chip [Bis17, HZS+19, KS18a, LGLK17, MDAB10, BAB+13, BGG+13].

Chips [Man13, SOS15].

Cho [SPLHCB14].

Chocolate [Svo14].

Choice [LLP+18].

Choquet [SH11, SM11, SNM14].

Chosen [FSGW12, zGXW12, HLW12, JMG+16, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWLJ16, YM19, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT+14, LFWS15, LZC14, LDZW19, QRW+18, RD17, SGM16, WZC16, WLFX17, XWS17, LAL+15, LHL15].

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

Church [ABJ13].

CHURNs [RBNB15].

Cipher [BW16, BFMT16, BCG+12b, CMLS15, CGCS12, DM18, DG12, DWWZ12, EHKSS19, Fis15, FXP+17, GLLSN12, GCS+13, HZ11, Hey17, IOM12, JKP12, KI11, KWS+12, LPS12, LYK19, LJ17, LJ19, LWKP12, LWPF12, MRTC12, MH12, MS12b, OGG+15, PH12a, PRC12, WSSO12, WNY+12, YCL17, ZAG19, AMS+10, BNY14, CR12, FVK17, HKT11, Hol12, Jeo13, KDH15, Lew10, LC13, LYHH14, LWKP14, MNP12, PL16, Ree15, RS14, Sar11, WYL14, WWBC14, ZSW+18a, LGL+12].

Ciphers [ABS+12, BMS12, BSS+13, BM18, BKLS12, Bru12, CWP12, DGFH18, DGIS12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNL12, Has16, Hey17, IS12, KE19, KPC+16, Kha10, LCLW17, LGLL12, LJ16, MD12b, NN12, PDJ+19, Pud12, Sas12, SEHK12, SJLK18, Sta11a, Vua10, WH18, WW12, Xie12a, Xie12b, ZH15, ZSW+12, Zha12, Bay10, Bia12, Bors10, Die12, GMT+12, KM10a, LGP19, LWK11, MCL+19, MRT10, MHV15, MMY+18, QGGL13, SKK10, TQL+14, WB12].

Ciphertext [BDPS12, CWWL12, CHH+19, zGXW12, HLW12, JMG+16, JSMG18a, KA17, LC12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWLJ16, YM19, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT+14, LFWS15, LZC14, LDZW19, QRW+18, RD17, SGM16, WZC16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertext-only [KA17].

Ciphertext-Policy [CHH+19, Rao17, XMLC13, XWLJ16, ZHW15, JSMG18a, JSMG18b, LZC12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWLJ16, YM19, ZHW15, CPPT18, FSGW12, GLM+16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT+14, LFWS15, LZC14, LDZW19, QRW+18, RD17, SGM16, WZC16, WLFX17, XWS17, LAL+15, LHL15].

Ciphertexts [LLPY19, Sta12, WQZ+16, AHL+12, JSMG18b, LCT+14, NMP+13, WXLY16, ZYW+19].

Circle [SC01].

Circuit [AH19, EAAAA19, Kar12, MYT11, WQZ16, XWLJ16, Lau12, MS13a].

Circuit-Size [MYT11].

Circuits [AIK14, AS17, BCKP17, BR14, GGH+16a, GH11a, GVV15, MBF18, SS10b, SS12a].

circumstance [ZLY+19].

Circumventing [BAG12].

CISPP [STC11].

Cities [LZD+19, SSA18].

Citizen [Ano16e].

City [Ano17d, GAI+18, ZJU+19, NTK+18a].

Claimant [Y17].

Claims [SKGY14].

Clara [MSH+16].

Class [BCG12a, SY15a].
XYXYX11, BJ16, Goo12, KK10. **Classes** [ACZ16]. **Classical** [BCDN17, DSLB18, JEA+15, MSU13, SSU12, CR12, RK11]. **Classical-quantum** [BCDN17].

**Classification** [CHH+19, HPC10, HS18, KAHK17, SGP+12, ZLW+17, ACMP19, HZW19, LHL+18]. **Classifiers** [KGV16, LCM+17]. **classroom** [Pow14].

**Claudius** [Hol12]. **Clean** [Fri13]. **CLEFIA** [Vle12]. **Client-Based** [ASM12]. **Client-Centric** [ASM12, CTC+15, FD11, RAZS15, Vle12, BK19, FA14a, FA14b, GSGM16, Jlx+19, MHL18, SG19a, hSZZ15].

**Cloaking** [NLZ+15]. **Clock** [VTY18].

**Cogging** [CHH+15]. **Close** [Wal18]. **Cloud** [AIA16, BDL+19, BCQ+13, BTK15, BCK17, CWL+14, CWL16, CDFZ16, CCT+14, CLW16, CDLW19, DK16a, DAX14, FYD+19, FCM14, FPY15, HWZP18, Her19, JLS12, JNS19, KMSM15, KS18b, KKA15, Kup15, LA15, LLPY19, LYZ+13, LGR14, LLC+15, LCPD15, LNXY15, MLO17, MJW+18, MGJ19, PSM17, Pet12, PBC+17, RSGG15, SG18, SG1+18, SK17, SRA17, SOR16, TV15, Vie12, VFFHF19, WLFX17, WRP70, WHLH17, WW17, XNKG15, XWSW16, XMCL13, XW1L16, XJW+16, YDY+16, YDZ19, YHL16, YJS18, YXA+16, YM+17, ZQQ+19, ZDL12, ZLD15, ZVG16, ZLW+17, ZZ1+18, AaBT16, Aky17, AZPC14, ASO14, AZ+16, A1K+17, ABR13, ADH17, ALL+18, Bel18b, BSBG19, BZ16a, BG14, BK12b, CFVP16, CSD18, CLH+16, CXWT19, CZ15b, CDL18, DDD+19, DZY+15, EAAA19, FH13, FLYL16a, FNWL18, GQH17, GLB+18, GZS+18, HSM13, HZW18, HK19, HYL+19, HYS18, IMB17, JEO13, KKA14, KKM+14, KSB+17]. **cloud** [KLW+17, KKD+18, LKX+14, LZY+16, LLH17, LZW19, LWW+19, LAL+15, LW13a, LYL15, LHL15, LCY+16, LIZC17, MLM16, MSGCDPSS18, NR17, Nam19, NB13, ODK+17, PPA18, PP11, PPG19, PWS19a, Rao17, RR16, SG19a, SLL+19, SYY+17, SAR18b, SKB+17, SWW+16, SW+17, SA19, TLM13, WLWG11, WL12, WSC14, WMX+17, WMXZ19, WDV18, WLS14, WS19, WCC11, WL19, XXX15, WXK+17, XWY+18, XTZ+19, XYML19, YYS+16, YZCT17, YHIM18, YQOL17, YQZ+19, WYT+12, ZYC+17, ZV14, ZDW+16, ZZ17, ZWS+18, ZFH+18, ZLY+19, ZHT16, ZZL+19].

**Cloud-aided** [SGJ+18, WLFX17]. **cloud-assisted** [WDV18]. **Cloud-Based** [KS18b, SRA17, ASO14, BK12b, WCC18]. **cloud-edge** [VTY18]. **Cloud-Edges** [BDL+19]. **cloud-hosted** [SG19a].

**Cloud-Manager-Based** [KKA15].

**Cloud-of-Clouds** [BCQ+13]. **Cloud/Fog** [JWNS19, LWW+19]. **Cloudier** [CFe16].

**Clouds** [BCQ+13, HLC+18, RHLK18, RSN14, HFT16, IC17, JKL+16, LFW15, LL16a, Wu17, YNX+16].

**Clouding** [SG19a].

**Cloud-based** [WDV18]. **Cloud-Edges** [BDL+19].

**Clouded** [SG19a].

**Cloudier** [Pow14].

**Clouding** [GW18].

**Cloudier** [SNS18].

**Clouds** [BCQ+13, HLC+18, RHLK18, RSN14, HFT16, IC17, JKL+16, LFW15, LL16a, Wu17, YNX+16].

**Cluster** [BYDC19].

**Clustered** [DS11, KS18b].

**Clustering** [FD11, KDS11, VSV15].

**CMAC** [SKK10].

**Co** [LFH18, MB15, MRL+18, HFCR13].

**Co-analysis** [LFH18]. **Co-Design** [MRL+18].

**Co-operative** [HFCR13].

**Co-Processor** [MBR15]. **coal** [KO16].

**cocktail** [OHJ10].

**Coda** [Ber16a].

**Code** [AD12, Bud16, CCL+13, Cop10a, Fox13, HG12, KSSY12, Mun17, PYM+13, SS13, Sen17, Sti15, War11, ABB13, Ant14, Bha16, Bri11, CCL11, CMB19, CBJ16, GIJ+12, GAB19, MCP15, McG11, Mc1K12, Moo14, OT11, PTV18, PA10, Wes15].

**Code-Based** [HG12, SS13, Sen17, CMB19, GAB19, MCP15].

**code-breaking** [Ant14, Bri11].

**Code-cracking** [War11].

**codebreaker** [Car11].

**Codebreakers**
Cop06, Cop10b, McK10, McK11. **Codebreaking** [Bai12, RS18, Cop06, Cop10b, McK10, McK11]. **Codes** [ACA+16, Ano19b, BBC+13, Bay10, BP06, BKST18, Big08, DBPS12, DPW18, FMNV14, GMNS15, Gri15, HC17, KW14, MBR15, OTD10, PWBJ17, SEY14, ST14, TLIW12, WGF16, WSL12, Xie12a, Xie12b, YTP11, Yek10, ATI+10, Bul10a, C75a, Chi13a, Fag17, Hea15, LTT10, MG15, OŚ11, Tan15b, YSJL14, Ayu12, Low12, Nag19]. **Collaborative** [DF16]. **Coding** [ACA+16, Che11, CWL16, CJ13, CG14a, DG17, Hes12, LCLL15, Per13, SSKL16, WCXZ17, AZF+12, Bul10b, CJXX19, DTZ12, JZS+10, KM11, LLP+18, NDNR13, OF11, Tan15b, YTM+14, Kim15]. **CoDiP2P** [NCCG13]. **Codon** [HEK18]. **Coefficients** [NCCG13]. **Cohen** [Pas13a, CSZ+11, LP11]. **Committee** [Bla16]. **Commitments** [Pas13a, CSZ+11, LP11]. **Committee** [Bla16]. **committing** [FTV+10]. **combination** [Watt14a]. **combinatorial** [MS13a]. **Combinatorial** [ZÁC17]. **Combined** [PP10b, PDJ+19, RMTA18]. **Combining** [AGBR19, Chi13a, CDF+10]. **Coming** [SOG15]. **Comment** [LCLL15, Ver17]. **Comments** [IC17, Kim15, hSZZ15, Tan11, TCL15, XWS17]. **Commerce** [Bla16, HvS12, Orm16, Ano11a]. **Commitment** [CK17]. **Commitments** [Pas13a, CSZ+11, LP11]. **Committee** [Bla16]. **commodity** [KK+16]. **Common** [CN12, DHB16, ESR14]. **Communication** [AD19, Alz19, BPS12, Big08, BCG19, CCM17, CCW+10, FMS12b, Gas13, GPVCdRQ12, KW14, Low12, OKG+12, Wan13, ZCI13, ZHV+16, AASSA18, ADG16, BB+18, DKL+16, GM13b, HCCC11, HLYS14, HPY10, KRM+10, KU16, LT13, LyWSZ10, MCN+18, QMC17, RK11, SSAF11, SSLP+13, Tso, WLZ+16, YKGK13, Zhu13, vDKS11]. **communication-efficient** [Tso, Zhu13]. **Communication-resource-aware** [Wan13]. **communicationless** [DGL19]. **Communications** [FMC19, JTZ+16, KSD+17, KYEV+18, O012, PSM+18, RSD19, SSKL16, SMS14, AMN18, Ang16, BC16, DMM10, DZC16, Edw17, FHH10a, Han12, LGFCGCRP14, LLZ+16, MHY+18, RS15, TKG+17, WDLZ13, ZZY+19]. **Community** [BPS16]. **Commutative** [CLHC12, SLGZ12]. **Commutativity** [ABR12]. **Commuting** [Fuc11, AKG13]. **Compact** [CFOR12, CKB13, EGG+12, LXY+19, LSQX19, MAS16, SJK18, SO18, TV19, VSR12, YM19, ZMW16].
Comparative [DDR+16, MHV15, BKR19, NR11].
Comparing [KTM+18]. Comparison [CGCS12, DWB12, HPC10, KU12, KA18, MZLS18, ST14, HM10, LCM+17].
comparisons [Mid10]. compartmented [EZ15]. Compensated [GKSB17].
Compensation [JSZS12, WMU14].
Competition [jCPB+12]. competitive [MD15].
Compilation [CHS15]. compiler [LWS10].
Complementary [MMLN15]. Complete [Ash14, BCEO19, BCEO20, BS14, FLH13, GHKL11]. completely [Con17, Win17].
Complexity [BBD19, BIKK14, BCG19, BW12, DP12, FS15, Gas13, HHS15, Shp03, AAT16, DJL+12, Jou13, KGO10, LWW+10, SDM14].
Composing [TW14]. Composite [Dun12a, GM16b, ZL19, BBDL+17, NDSA17].
Composite-Field [GM16b]. Composition [LJS+14, NRZQ15, Ana14, AGH+17]. compound [BJ16, KPS10, jT12b].
Comprehensive [GSFT16, YFT17, YJSL18, ZBPF18, Bull10a, Kas15]. compress [LC13]. Compressed [DG17, JSCM17, KD12a, SR12a, WLZL12, CLF11, Fay16].
Compressed-Domain [WLZL12].
Compressive [CCZC13]. Compromise [YNR12b, GBNM11, PX13]. Compromised [DSSDW14, DSSDW17, ZYL+10].
Compromising [BC14, BM18].
Compulsory [QRW+18]. Comput [HYS18].
Computability [Gas13]. Computable [CGCS12, DWB12, HPC10, KU12, KA18, MZLS18, ST14, HM10, LCM+17].
Computational [BBD19, BCO13, GKS17, RD17, RPHJ11, TBCB15, HRS13, SJ19, SDM14].
Computationally [BCEO19, BCEO20].
Computations [ARM15b, CK18, KHP16, Nac16, PH16, ADMM16, BK12h, LWW+19, LR15, SSAF11, TLMM13]. Compute [MJW+18, Vai12, PZ15].
Computer [BGK12, BCGK12, BGB12, BdD19, Bul10b, DF16, Gas13, HHS15, Shp03, AAT16, DJL+12, Jou13, KGO10, LWW+10, SDM14].
Computers [Mos18, Bre18, Cop06, Cop10b, Dya19, LCKBJ12, Mac12, MvO11, PHWM10].
Computing [ACM10, ACM11, AMMV18, Abbl2, AWA16, Aoa17e, BCG+12b, BTK15, CLB19, Cer14, CGB+10, DXA14, EAA12, FES10, Gen10, GB19, JWNS19, KMSM15, KP17, LCK11, LT14a, LYZ+13, LLC+15, LVI16, LNX15, MIO17, OS16, PAF18, Pet12, Rs18, Roh19, SJWH+17, SLM10, Vai11, Vle12, WRP70, XMLC13, XWLJ16, YE12, YZDZ19, YHL16, ZLDC15, AaBT16, AAZ+16, And13, And19].
Content [AAA+19, ADR18, BCP14a, KD19, MHT+13, PMZ13, PZPS15, WHZ12, WZX12, YT12, ZXZ+11, GPN+12, HPL+19, JS18a, YWY+19]. Content-based [KD19, MHT+13, YWY+19].


Context-Driven [SY+19]. contextual [YWY18, LGM]. Contributors [DDD14, GLW13, LWL10a, MM14a].

Contributory [WQZ+16]. Control [AMSP19, ATS15, BFK+10, DLZ+16b, GGG18, GRRZ18, HBC+19, HHS+15, HLC+18, LGM+16, LGKL17, LJP17, MM17a, MK12b, NA10b, PV17, QZL+16a, RSN14, SGC14, SY+19, TBCB15, XMLC13, XHZ+19, YTH17, ARL13, ACK+10, AMHJ10, BBTC20, CLH+16, CO11, Cra11, FG19, FNWL18, FS18, GH19, HPJ+19, JAS+11, LCL+17a, LCL+15, LLH17, LH+18, MDHM18, NZM10, QCX18, RR17, Sch15c, SA15, Tan12b, Wan18a, XHH12, XYL19, YWJ+19, ZML17, ZDZH18, ZVH14, ZWS+18, ZFH+18, ZZL+18].


Copyright [SJ12, ZWWW17, GJ13]. Core [BL13, YWF18, YS15, AVAH18, RS17c, HLYS14]. Cores [MGG+19].


CorrectDB [BS13a]. correcting [ATT+10, LT10, MCP15]. Correction [KSH18a, LSC+15, yWXyZ+18, Chi13a, Sun16]. Correctness [YGS+17, WS13].

Correlated [RS10, Jia16, ZPZ+16].

Correlation [BW12, FAA+18, LD13, SDM+12, WWBC14, XHH12, YCL17]. correlations [Sar14]. Correspondence [SY14]. corresponding [DWZ12].

Corrigendum [HYS18, WZM12a].

Corrupted [Fyo19]. cosmography [Pet11].


Counter [ARP12, KMJ18, MKASJ18, Fay16].

Counterexample [KRW13]. Counterfeit [YFT17].

Counterfeiting [Alz19, Ano16f, Bro12]. counterfeits
Countermeasure
[BBB+16a, MD12b, GJ19, HYL+19].

Countermeasures [BGN17, DZS+18, EWS14, PZPS15, DK17, FAA+18].

Counters [BM18]. Counting
[BBB+16a, MD12b, GJ19, HYL+19].

 Covers [KKM11]. Cover
[EPAG16, JTZ+16, NSA15, VCD16, YDV19, LT13, LyWSZ10, SRB+12]. Covert
[NTKG17]. Covert Band
[BM18]. Counting
[LLD19, ZBPF18]. CPUs
[AVAH18]. Crack
[Fox13]. cracking
[Ano13d, McG11, McK12, Moo14]. Cracking
[Gri15, GAS+16, War11]. crawlers
[GPN+12a]. CRC
[Ful10, Joh10, GMSW14]. CRC/Taylor
[Joh10]. Create
[DFKC17, HGOZ19]. creating
[Bre18, OO10, Pau19]. creation
[GJJ18]. Creativity
[WP15]. Credential
[YLSZ19, JMW+16, KKM+13, XMHD13]. Credentials
[CG12a, SSW12]. Credible
[ZW15]. credit
[Mar10b]. cribs
[Pea11]. Crisis
[OdH12]. Criteria
[PSY18, ZKZ17]. Cryptanalyzing
[LLL17a, LLLH18, ZW+12]. CryptDB
[PRZB12]. Cryptic
[Mar10a]. Crypto
[Ano13a, BCC+19, DMO+19, Goo12]. Cryptography
[Ano16a, BH15, Eya17, FVB+18, RM19]. Cryptocurrencies
[BNMH17, JSK+17, BH19]. Cryptocurrency
[Ano16a, BH15, Eya17, FVB+18, RM19]. cryptographic
[Shy15]. Cryptographer
[Dun12b, Kia11, Pie10]. Cryptographers
[Ano16a, BPS16, Goo12]. Cryptographic
[Abe12, AMKA17, AD12, ARH+18b]. ARH+18a, ÁMVZ12, App15, AHWB20, BMP12, BBD19, BEM16, BR19, BCGK12, BGB12, Bar15, BCM+15, BCHL19, BIKK14, BLS12, BDP11, BFCZ12, BDBGH15, Bla12, BKL+13, BSJ15, BNA15, CCK12, CCCC16, CK17, CFE16, jCPB+12, CBL13, CHN+18, Cor14b, CATB19, CFG+17, DB16, Des10a, DQFL12, DR11, Ess17, FKS+13, FY11, FLW12, Gir15, GM11, GLR10, GG11, Har16, HN10, HHH+13, HST14, HSA14, IBM13b, JR13, JHW+19, KOP12, LVV11, LLK18, Loe15, MVV12, MKK17, MP12, MKAA17, Muf16, MK12b, NIS13, NA10b, PTT16, PFS12, PS14, PJ12, RMP10, RSBD12, RPHJ11, Rja12, RBHP15, SK11, SEY14.
Cryptographic [AY14a, ABB+14, ABF+14, ABC+12, ABO+17, BYDC19, Bar19, BFG+14, BJ10a, Bon19, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGIJN14, EBFK13, ESR14, GGH+16b, GJJ18, Gil10, GLR13, HYL+19, JCL+18, KJ1+16, KSU13, KAS15, Ks12, KKK+16, LGKY10, LLL+17b, MS13c, Mat19, MMZ12, MM13, Mes15, MSGCDPSS18, MN10, NDNR13, Oo18, OMPs+19, Pal15, PLPW13, PSDo+13, QZDJ16, SD10, WT13, WXY+17, YSM14, ZHL+11, ZVH14, Sha10, SK11, SK12b, Seo18, She17, SA16a, Sim15a, SG14, Smal6, Sta11b, Ste15a, VS16, VGA19, YSK+14, WYL+14, WY12, Wes16, Yam12, Yam11, YTS12, YL17, YYW19, ZZCJ14, ZAC17, vRDHSP17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABB+13, And19, Ano11a, ABW10, ACH+10, BOB13, Bar14, Ber14, BL14, BL17, BAP+13, Biol2, BS+14, BSW12, BB16b, CF11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSLY14, DD14, DA18, DD13, DGMT19, Dur14, GCVR17, GAB19, Har15, HH15, HZW17, Hod19, Hof16, IM14, JLT+12, JY14, JW14, Kam19, KL08, KL15, KDH18, KKM11, KK10, KGO10, Kre13, KKD+18, KSH18b, KS13a, Lam13, LLLK10, Lin14b, LW10a, Liid12, LY14, MCN+18, MS13b, MD12a, MCP15, Mic10a, MHL18, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RI10, Sac14, Sah13, SK14, SSAF11, Sta11c, Sti11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YTL11a, YSC16, YX+18, YDH+15, YR11, YN19, ZXW+18, vDSS11, Che11, LZX10, NAc12, Cou12b, Fol10, Gas13, Low12, Mei10, Mur10, Ter11, BOB13, CIL11, CRYPTO [ADD10, BCGH11, BJ12, BKLS18, MC11, NDG+17, PLSvdLE10, SVC15, CBL10, GCH15, HJM+11, SA14]. Cryptography [ACZ16, Ako19, Ako15a, Ako16b, Ako16c, Ako16j, Ako19a, Ako19b, App14, AAB17, AG18, ACM+17, ARM15b, Bar12, BGK12, Bar15, BBCL19, BRT12, BCGN16, Big08, Bon12, BF19, BKKV10, BJ10b, Buc10, BLM17a, BLM17b, BLM18, BCF+14, CN14, CR18, CTFH14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK02, DK07, DK15, DXA14, DP17, DBT19, DHLAW10, DF16, DKS12, DR11, Els10, Elb09, FPS12, FHD19, Feh01, FSK10, Fid18, FBM12, Fre10, GT19, GO17, GFBE12, Gol19, G13, Gre19a, GPT12, GLW12, Ham17, HEp+11, Hes12, H12, HR19, HPS08, HKR+18, JS18b, JTT12a, KM10c, KP10, KKA18, LSL12a, Lin17, LWL10b, LGWY12, LMMH14, LGH+17, LWHS17, LPO+17, MO12, MS10, Man12, Men13a, MR14c, Mic10b, MST18, MV12]. Cryptography [MMB17, NNA10, NDR+19, Nie02, NS12, Orn16, PP10a, PAB+19, PPH12, PG12, RW12, Rog16, SY14, SG15, SO15, Sch16c, Sch18, Sch19b, Sen10, SS13, Sen17, SK12b, Seo18, She17, SA16a, Sim15a, SG14, Smal6, Sta11b, Ste15a, VS16, VGA19, WYL+14, WY12, Wes16, Yam12, Yam11, YTS12, YL17, YYW19, ZZCJ14, ZAC17, vRDHSP17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABB+13, And19, Ako11a, ABW10, ACK+10, BOB13, Bar14, Ber14, BL14, BL17, BAB+13, Biol2, BS+14, BSW12, BBB16b, CF11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSLY14, DD14, DA18, DD13, DGMT19, Dur14, GCVR17, GAB19, Har15, HH15, HZW17, Hod19, Hof16, IM14, JLT+12, JY14, JW14, Kam19, KL08, KL15, KDH18, KKM11, KK10]. cryptography [KKO10, Kre13, KKD+18, KSH18b, KSH18b, Lam13, Lan11, LLLK10, Lin14b, LW10a, Liid12, LY14, MCN+18, MS13b, MD12a, MCP15, Mic10a, MHL18, NLYZ12, Nov10, OK18, OTO18, Opp11, PHWM10, PP11, RI10, Sac14, Sah13, SK14, SSAF11, Sta11c, Sti11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YTL11a, YSC16, YX+18, YDH+15, YR11, YN19, ZXW+18, vDSS11, Che11, LZX10, NAc12, Cou12b, Fol10, Gas13, Low12, Mei10, Mur10, Ter11] cryptography-based [BOB13]. Cryptography-Related [Cil11]. Cryptol [Lau12]. Cryptol [Ako13b, Ako14a]. Cryptology [BC11, Bro11, Den12b, LW11a, Nag19, PWBJ17, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGPGP14, Gil10, GG10, Kia11, LH10a, MZ17a, Pal16, Pie10, Rab10, HWG10, LTW11, KOB10]. Cryptomania [Gen13]. Cryptoprocessor [EHKSS19, GV14b, SW+10]. cryptoscheme [SLXX16]. Cryptosystem [CCT+14, KD19, LH10b, SZHY19, SW+10, WSQ+16, Zaj19, ACD18, AK14a, BS15, Chi13a, Ga13, GV14a, GLB+18, IB11, LZ11, LYT+10, MM13, MG15, NZM10].
Cryptosystems [ADI11, CLND19, OTD10, PSM17, ZSP+19, AHG18, AJYG18, AVAH18, BNST17, FWS13, SA16b, ZYM19].

Cryptovirology [YY17a].

CryptRndTest [DB16], CS [LJ19], Csec [AD12], CT [Dun12b, Kia11, Pie10], CT-RSA [Dun12b, Kia11, Pie10], CTRL [HKK19].

CTRL-PACE [HKK19], Cube [HIJ+19, MS12b, YWM19].

Cubic [RW12, VM14].

Cuckoo [BHKN13, sCR19a].

CUDA [DLV16].

Cue [KTM+18].

Cue-based [KTM+18].

CueAuth [KTM+18].

cultural [Mid10].

Currencies [TS16b].

Currency [AHWB20, DMO+19, Cou12a].

Current [DP17, GCK12, FPBG14].

Curse [GG11, HB14].

curvature [GJ13].

Curvature-feature [GJ13].

Curves [AMMV18, ACA+16, AK14b, BSCTV17, BWR12a, CMRH17, DW12, Grc19a, LL11, LT1a4, MST18, Nag19, PBWJ17, Sch19b, She17, TX16, YTS12, BL17, BP18, FK19].

Custom [ÖDS517].

Customization [OdH12].

Cyber [LJS+14, vdWEG18, GQH17, GHD19, HZW18, KSA16, QMC17].

Cyber-Espionage [LJS+14].

Cyber-physical [GHD19, HZW18, QMC17].

Cyber-security [vdWEG18].

Cybernetica [Azo17c].

Cybersecurity [Bel15, DF16, Hel17, Lan17, LRW14, Mos18, Sch19a, SDC+17, SPG+19, YK16, AP18, GQH17].

CybSI [YK16].

D [AM19, AP10, Bro19, CG12b, DBPS12, DWWZ12, EAA+16, GZHD12, KWS+12, LJ17, LJ15, MCD12, MKH+12, PGL10, RS16, SGS14, SRK+17, SRK+18, WSSO12, WK18, WY12, tWmC12, YI14, YPR117].

D-Based [WSSO12].

D-like [LJ15].

D-PUF [SRK+17, SRK+18].

D2D [Gop19, PSM+18].

DDA-S [AAH+19].

DALP [LWYM16].

Dana [Aoz10a].

Dandelion [FV8+18, VFV17a, VFV17b].

Dangerous [HIL12, GIJ+12].

Dao-Fa [FMS12a].

Daoism [FMS12a].

Dare [Xie12a, Xie12b].

Darmstadt [FBM12, Sen10].

DASH [KCC17].

Data [AAA+19, ARWK19, Ano13c, ADF12, Bar12, BJL16, BCD+12, BJL12, BW12, BKLS18, CWL+14, CMLS15, CCW+10, CSV15, CCT+14, CLW16, CDLW19, CHH+19, DDS12, Dan12, DR12, DK16a, DMS+16, DA12, DCA18, DLZ+16b, Eb09, EKOS19, EKB+16, FYM15, FYD+19, FPY15, FRS+16, GTT11, GRZH18, HSM14, HWZP18, HLC+18, HLT+15, HVP+18, HXZ+18, HK14b, IBM13a, KR1D13, KGV16, KPB18, KDB19, LPPY19, LLLZ+17, LLSL19, LWCJ14, LCP15, LLZ+12, LZC+12b, Ma17a, MLO17, MSL17, MMS17b, MJW+18, MG19, MM14b, NNAM10, NR12, PV17, PD14, PSM17, PZL+19, PBC+17, PH12b, PH16, PNRC17, PWS+19b, QZL+16a, QZZ18, RCP+18, Rea16, RDK19, RS14, SAKM18, SAKM16, Sar10b, SSMK18, SP15b, SKH17, Sia12, SC19a, SL10, SOR16, TCN+17, Tan15a, Vai12, VSV15, WZCC18, WHLH17, XNK15, XWSW16, YDY+16, YZD19, YJSL18, YMC+17, ZXYL16, ZPXX17, ZTL15, ZLW17, ZM19, ZTL15].

Cycle Based [KMN13].

Cycles [KMN13].

Cycle [Che18, OTD10].
[ASO14, AIM+19, Ana14, Ano11a, Ara13, ADH17, ALL+18, BLL+19, BC16, BHH19, BTPLST15, Bc18, BC16, BKV13, BTK15, CD16a, CDGC12, CLH+16, CDF+10, CDL8, DGY+19, DFJ+10, DTZZ12, DRD11, DYZ+15, DZC16, ED17, FS18, GHD19, Gen10, GSAMCA18, GLB+18, GZS+18, HKA+18, HSM13, HKAA17, HWK+15, HL19, HK19, HMCK12, HH16, HYS18, HYF18, JKA+18, JLC18, JHC14, KCS+18, Kim16, KV19b, KH18, KWH16, LSBN14, LT14b, LKX+14, LZY+16, LLL+17b, LLH17, LHL+18, LZWZ19, LFS15, LAL+15, LCW+16, LZC17, LLL+18, LL16a, LHA+16, MHKS14, MRR+18, MSGCDPSS18, NJB19, Nami19, OI18, OSK16, OSANAM19, PPG19, PM19a, PW19a, PZ15, QCX18, QLZ19, RR16, RR17, SLL+19, Schl5c, SD17, SY+17, SM19a, SM19b, SAR18b, SPK17, SW+W+17, Tan17b, TMK11, TMKZ13, WL11g, WLL13, WMC17, WXMZ19, WDZ19, WLS14, WZLW13, WS14, WS19, WI19, XXX15]. data [XWZ+18, XWY+18, YYS+16, YQOL17, YQZ+19, YJC18, YXA+16, YNX+16, ZKK19, ZMM+10, ZYW+13, ZZC17, ZHT16, ZZZ+18, ZZL+19, AEEH17, HLYS14, SJ19, Sch15c, VJ+18].

Data-Centric [DLZ+16b].

Data-Compressor [KGV16].

Data-Independent [DA12].

Data-Minimizing [BCGS16].

Data-Oriented [NNAM10].

Database [ATHJ12, SBV14, WCL+18, AAH+19, BL11, HHCC14, LW13a, PBP19, PRZB12, SVGE14, Suc12, XMY+17, YX18].

database-as-a-service [AAH+19].

Databases [ABL+18, FCM14, HPC10, JKH12, Kw15, RP12, WP17, GA11, JK13, LCY+16, SS17a, TG12].

datacenters [PRN+19].

Dataset [SP13].

datasets [LVRY10].

DATS [HVP+18].

Daubechies [Ara13, SM12, ST15].

Daunting [IBM13a].

David [RNQ16].

MMPB17, Zet14, Hof16].

Days [Bai12, Bri11].

DB [PYH+18].

DBDH [CW14b].

DBMS [SERF12].

DC [LHF12].

DC-Net [LHF12].

DCT [DBB14, LP12, SS17b].

DDH [LZC12a].

DDoS [PSJ+13, SP15a].

De-synchronization [XNG+14, AATM18].

deadly [HL10].

Dealing [Sha13, VN16].

Death [Moo14].

Debate [Bla16].

Debiasing [USH19].

Debs [Smi15b].

debugging [MFH13].

Decade [SOG15].

December [Abe10, BYL10, BC11, Che11, GG10, HWG10, LH10a, LW11a, LTW11, Yan10, Yan11].

Decentralization [JP19].

Decentralized [ABC17, CD16b, GZ+13, HSMY12, HK14b, MT17, PPS12a, PAS13b, RVH+16, RS14, TS16b, TXZ+19, YM19, HHBS18, SL+19, WZ16].

Decentralizing [LW11b].

Deception [GA19, vdWEG18].

Deciding [CLZ10, Sch12c].

Decipher [Cor14b].

Deciphering [Bla16, GMNS15, GSAV18].

decision [PKA15, RPG12].

Decisional [CCL+19, LZC14].

Decisions [Bel18a, YWK10b].

declarations [HWWY14].

Declassified [ABJ13].

Decodable [Yek10].

decoder [PMG19a].

Decoding [DBPS12, GMNS15, Bax14, Bul10a].

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

Decompression [PP10b, SHC+16].

Deconstructing [Tar10].

Decoupling [DMO+19, IM16].

decoys [VSB+19].

decryptable [MBP19].

Decrypted [Kob10].

Decrypting [CR12, Tay19].

Decryption [AN12, KB10, PKTK12, FNWL18, LJW+17, LJYW18, SES+16, SM10a, SM10b, Wu16, XTZ+19, XYML19, ZSW+18].

Dedicated [Lin17, Nac12, NDF+18, AKS19, RNQ16].

deductive [ABF+14].

Deduplication [CDLW19, MGJ19, QLL17, SKH17, YDY+16, YZDZ19, ZHZ+19, KH18, SAR18b, ZF+18].

Deep [BNMH17, CRS+18, DLGT19, FGR+17, HCYZ18, Mor19b, RDK19].
RHLK18, WYL18, ACMP19. default
[BMDT19]. defeated [Kap13]. defects
[FES10]. defences [NDNR13]. Defend
[Ano17e, FDY+19, Sch13]. Defending
[LWC+14, YFT18]. Defense
[MPA+18, RCK17, YDV19, PSJ+13].
Defenses [AN17]. Defensive [Pfl10].
Defined [KYEV+18, SAM+18]. definition
[LWL10a, WSC14, YKC+12]. Definitions
[BBD19, GLW12, Mau12, CGKO11, KM14, KGO10, XWXC14]. Degeneracy
[WH18]. degradation [MMS+17a]. Degree
[CMRH17, KA18, LHW18]. degrees
[MZ17a]. Delay
[CCMK16, GMNS15, LFX+18, LBR12, MKK17, JLT+12, XW13, MCL+19].
Delegatable [WZ11, XLC+19]. Delegated
[MZHY15, TMC15]. Delegation
[FMTR12, GLL16, SSW12, XWLJ16, YZ12, YAM+15, JSMG18a, NAL17, XWS17, XZP+19, ZWN14]. Deletion
[DMS+16, MCG19, Rea16]. Delfs
[Mur10]. Delivery [PSS+13, SSC12]. demand
[KKJ+16, LWYM16]. demand-aware
[LWYM16]. Demodulation [KOP12]. demonstrating
[LHA+16]. Demonstration [GKG19]. demosaicking
[HLC16]. Deniability [TCS14]. Deniable
[DF11, zGWW12, HLLC11, GCH+19, HS11, Jia14b, JXZ15, LXJ14]. Denial
[BKBK14]. Dense
[BFM12]. Density
[Gre19b, LC15, LSQ11b]. density-based
[LSQ11b]. Dependable [BCQ+13].
Dependency [MWES19, SGP+12].
dependent [GdM16, PAK15]. deployed
[MFH13, RY10]. Deployment
[BAS+19, WXK+17]. DepSky [BCQ+13].
Depth [GH11a, RS16, SS10b, SS12a].
Depth- [GH11a, SS10b, SS12a].
Depth-Based [RS16]. Derivation
[LBR12, Cha13a, Lau12]. Derivative
[LSQ11a]. Derivative-based [LSQ11a].
derived [JS18a, ZMM+10]. DES-like
[AHG18, CGCS12]. Description
[WH18, PLCGS11]. Design
[AMN18, Abe12, ARH+18b, AIB+16, ADD10, AUMT16, Bel18a, BKL+13, DZS+18, DHB16, DR11, FSK10, HSA14, JZL18, JWJ+17, KPP16, KW14, KLW+17, Lop12, MS13a, MFG16, MRL+18, Mur16, NBZP17, NYR+14, PC16, QLL17, RYF+13, Sch13, SAAB10, SDDL14, THA+13, VKPI17, WKB16, WDKV19, YJC18, ZHX16, BBDP16, CZ14, DRN16, Gor10, KHF10, KDW+17, MNNW15, MAK+12, MHY+18, OSANAM19, SVGE14, ZYC+17]. Designated
[WHJ17, HYWS11, RPSL10, SY15b]. Designated-verifier [WHJ17].
Designation [Che15, LSQ11b]. designed
[Goo12]. Designer [KMY18]. Designing
[CDK+10, DZS+18, FLW12, MRT10, PSD15, SR10]. Designs
[BGK12, PCY+17, KDH15]. desynchronisation [LDC13]. Detailed
[DL16, ZPXX17]. Detect
[JWJ+17, NSA15, WOLP15, Lau11]. detectability [LRW17]. Detectable
[Ess17]. Detecting
[BKBK14, CZ19, Ess17, GAS+16, HLW12, KW14, SH15, VCD16, YSC+15, LWL11]. Detection
[AMKA17, ATS15, ARWK19, BEM16, CBO+18, DS15, DF11, GN16, GZH17, HDWH12, HCYZ18, KU14, LGL+12, LC15, MKRM10, MKAA17, MKAS18, NDC+13, NMS14, SAJJ16, SBV14, SXH+19, SP15a, SRAA17, SGS14, TLZ+17, TM18, YFT17, ZHS10, AKKY17, AOT13, BM13, CB16, HBI13, JC13, JDV16, KKK+18b, KLC+10, LCD13, Maz13, MMF15, MHT+13, WYL13, vdeWEG18]. Detective
[Cho10]. Detector [LTKP16]. Detector-Based [LTKP16].
determination [JK19]. Determine
[FSWF11, Sto12]. Determining
[Bar19, NN12, Scr18]. Deterministic
[MPRS12, NIS12, XXZ12, DTZZ12]. Distincting [WGJT10]. DEUCE [YNQ15].
develop [Ham19]. Developed [Har16].
developers [Ano14c]. Developing [CH11].
Development [Pau10]. Developments
[GCK12, Vai11]. Device [ADM19, ABC17, CFXY17, DFKC17, HSUS11, KLM+12, SRK+17, SRK+18, TYK+12, ZSH+19, CRS13, GM16a, KKG14, Kim16, OSP+19, Par12b, SHBC19, VV19, XHH12].
Device-to-Device [ADM19]. Devices
[AAC+16, ATC17, BDM+19, CSH+18, CRS+18, DLWW11, EGG+12, FMC19, GPT12, GdM16, GMSV14, HHH+13, HDWH12, HFS+19, JMG+16, LFH18, LWHS17, LLD19, MFG16, May15, MS16, NVM+17, RC18, RSX18, Sch15b, SFE10, SWF+19, VWC19, WKB16, WT10b, XJR+17, Aia15, BMDT19, CSH+18, CRS+18, DLWW11, EGG+12, FMC19, GPT12, GdM16, GMSV14, HHH+13, HDWH12, HFS+19, JMG+16, LFH18, LWHS17, LLD19, MFG16, May15, MS16, NVM+17, RC18, RSX18, Sch15b, SFE10, SWF+19, VWC19, WKB16, WT10b, XJR+17, Aia15, BMDT19, CSH+18, CRS+18, DLWW11, EGG+12, FMC19, GPT12, GdM16, GMSV14, HHH+13, HDWH12, HFS+19, JMG+16, LFH18, LWHS17, LLD19, MFG16, May15, MS16, NVM+17, RC18, RSX18, Sch15b, SFE10, SWF+19, VWC19, WKB16, WT10b, XJR+17].
Disreputable [ABJ13]. disrespecting [BZD+16b]. Disruptive
[HK14b]. Dissection [Dun12a]. Dissent [SCGW+14]. Distance
[ABB+19b]. HRK18, PYH+18, Lam13. Distance-Bounding
[ABB+19b]. Distillation [BJ16]. Distinguisher
[DWWZ12, AMS+10]. Distinguishers
[LJF19, SEHK12, ZSW+12, AY14b, AP11]. Distinguishing
[ADH19, Ano10a, BKBK14, BCEM15, HSM14, HEP+11, HXC+11, HCL+14, HZX+18, LMD16, LLY06, LL15, LNZ+13, LWJC14, PBC+17, SSKL16, SWF+19, SB18, YZX+12, YKKL12, ZLDC15, BLV17, CSTR16, CHL19, dCCSB+16, FG19, GAI+18, KKK+18b, LSY16, NDSA17, NCCG13, ODK+17, PRN+19, TG12, XU13]. Distributed-Healthcare [ZLDC15]. Distributed
[Küp13, MS16]. Distribution
[BCG19, EAA+16, JEAI+15, LWWL+17, Lop15b, MT17, MSU13, NNA10, SK11, SNJ11, Sas18, TC10, AASSA+18, ABB+14, BB14, BGP+17, CML16, FHZW18, JSK+16, JLT+12, LLP+18, LM14, NACL1R, SPD+10, VV19, WMU14, YWL+17, Yan14, YHHS16, YL11, ZWS+18]. distributively
[LJY16]. dithered [UUN13]. Diversity
[ZTL15]. Division
[HJ+19, HZSL05, SS12b, YWMM19, MN14]. Divisors
[CN12]. Divulges [ABJ13]. DLSeF [PRNC17]. Dmail [CCS14]. DNA
[AEH17, HEK18, WGZ+12]. DNP3
[AGW15, BDFK12, BBM15, CLY14, DG17, LA15, MR16, PMD12, SZHY19, SBY11, SAM+18, WLZL12, gWpNyY+14, ZWZ17b, AMK12, BGAD12, GJ13, IG11, LXCM11, LPZJ15, LBR12, PWW10, QMC17, SCKH11, vWpYyN13, YZL+18, YWK+10a, YCM+13]. Domain-Specific
[BCG10]. Double-Boomerang
[BCG10]. Double-SP [Sas12]. Doubling
[Zha12]. Doubly [CFZ12, CW14b]. Doubly-Spatial [CFZ12]. Douglas
[Ber16b]. Down [Ano17e, MCG11]. Download
[ZGC16]. DPA [MM17b, ZJ11]. Draft
[MCF17]. DRAM
[SRR+17, SRR+18]. DRAMs [LSC+15]. DRAW
[NSBM17]. DRAW-A-PIN
[NSBM17]. drawn [NSBM17]. DRBG
[YGS+17]. Dreams [Eya17]. Drive
[GKSB17, JSZS12]. Drift-Compensated
[GKSB17]. Driscoll [Bur11, J oh15]. Drive
[DGFH18, YC+17, Mac12, SYW17]. Drive-Thru
[YSC+17, SYW17]. Driven
[BMP12, DLM+18, SYv+19, APMCR13, LSQ15]. driver [GBC19]. DriverGuard
[GBC19]. DriverGuard
[DD13]. DRM
[Ano13c]. DSSH [YL12]. DTKI [YCR16]. DTLS
[AP13]. DTRAB [FTV+10]. Dual
[BLN16, BWR12a, CCG+16, CMG+18, HF14b, HHS18, HPL+19, Lz11, NLYZ12, PAF18, BW13, CNF+14]. Dual-Form

raw_text
Dual-key-binding [LZ11].
Dual-Mode [PAF18]. Dual-Rail [HF14b].
Dubai [Nor17]. Dual [VJH+18]. Dummy [GST12].
duplication [LWLW11]. Duqee [TK19].
During [FGR+17, ABJ13, BDM+19, RS17c].
DWT [AM19, LD13, SJ12]. dyadic [MO14].
Dyck [SAM+19]. Dynamic
[ABB19a, BK19, BCG10, EKB+16, FHR14, HH15, HK19, KYH18, LHM+15, MWZ12, MM12, NKWF14, OMNER19, PPS12a, PNC17, RC18, SSW12, SY14, SKV12, SGC14, SHC+16, VMV15, XNKG15, XWSW16, XZY+12, XWZ+18, YLSZ19, ZXYL16, BSBG19, CTL12, CBJY16, CSTR16, DSCS12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KH18, KBPB17, LDC13, LLY06, LXMW12, LHM14, LRC17, LZZ19b, NSX+18, NPP+14, PZL+19, PSJ+13, SES+16, SSS11, SM10c, SGM16, WZD19, XHM14, YZL+18, YD17, ZSMS18, ZZL+18].
dynamic-identity [JZS+10]. dynamical [JTL12b]. Dynamics
[RSCX18, AABT16, GEAHR11, LT+15a, Ld12, MCRB19, TZTC16].
dynamics-based [AABT16]. dyslexic [Bha16].
e-commerce [Ano11a]. E-exam [Mor12].
E-Health [AMSPL19, WMX+17, AKS19, IC17, OSP+19, YZL+18, JKL+16].
E-Learning [Yon11]. e-mail
[BTW15, Sch16b]. e-Passport [HKK19, LZZJ10]. e-Passports [LG10].
e-rental [LY14]. E-Voting
[KV18, LGPRH14, KZZ17]. E.T. [Sch16a].
E2 [WYL14]. E2E [KZZ17]. EAC [LZZ10].
Each [YLL+12]. EAP [FLH13, HZC+14, ZCLL14]. EAP-based
[HZC+14, ZCLL14]. Ear [GWP+19].
EarEcho [GWP+19]. Early
[Bel18a, Bro11, And13]. Earth [Har14].
easier [MBF+13]. Easy
[Bel16, SMS11, Tay14, Wu16, ZDW+16].
Eat [DSSDW14, DSSDW17].
Eavesdropping
[CLW16, Han12, PX13, YSLJ14]. EbH
[GMDFPLC17]. EC [Dra16, BLN16, CFN+14, CCG+16, CMG+18].
ECB4CI [YWZ+18]. ECC [BSSV12, CBL10, HJ19, JMW+16, KRH18, MMBS19, ZSH+19].
ECC-Based [BSSV12]. ECDSA
[BBB+16a, BH19, DHB16]. ECG
[GMDFPLC17, HZW19, HW19, PLGMCdf18, ZAA17]. ECG-based
[PLGMCdf18]. Echo
[DLMM+18, GWP+19, HGT15].
Echo-Based [HGT15]. economic [WDZ19].
economy [Sir16]. Ecosystem
[Fri13, RVS+18]. Ecosystems
[LDB+15, MMP19]. eCryptfs [XZL+19].
Ed25519 [TV19]. EDAK [ABB19a].
EdDSA [JL16]. Edge
[AHM+18, DF16, KA18, HXZ+19, CXWT19, JZU+19, MD15, PRN+19, Sm16, ZXP+19].
Edge-Based [HXZ+19]. edge-centric
[AHM+18]. edge-enabled [JZU+19]. Edges
[BDL+19]. Edition
[Cor14a, Kob10, Gre19b]. Editorial
[LSQZ17, OK18, Ano19a]. Editors
[BdD19, LKL18]. Education [LRVW14].
Edward [Ano16a, Sim10]. Edwards
[ADSH18, JL16, LT14a, YTS12].
Edwards-curve [JL16]. EFADS [WLS14].
Effect [PLGMCdf18, WB12]. Effective
[HLP+15, KRDH13, WHHL17, WMX+17].
Effectively [YMC+17]. effectiveness
[Eng15]. Effects
[ASV+18, MAL10, SKV12, SHBC19].
Efficiency
[ABF12, Chi16, DG17, FRS+16, HRV10, LLML12, LCL+17a, MS13b, WXLY16].
Efficient [ABBD13, ASBdS16, ABB19a, BWLA16, BCGH11, BHG12, BKKL19, BV11, BV14, CG12a, CML+18, CS10, CMLRHS13, CWWL12, CZCD18, CJ13, DA18, DZC16, DWB12, DUN12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTT11,
Emerging [BSV12, KSA16, OS16, FPBG14, GLL16, ZHH17]. emphasis [GMT12].

Empirical [gWpNyY14, EBFK13, Sar14].

Employees [Mor12]. Employing [LGLK17].

EMV [Cho10]. Enable [SMS14]. Enabled [GPT14, HFT16, KV18, QZL16a, QZL16b, SG12, SGCL16, SSPC12, YSF18, BMM12, JZU19, NML19, TODQ18, YFT18].

Enabled/disabled [HFT16]. Enables [IBM13a]. Enabling [FRS16, GYW19, JSM18, PSM18, SSY12, WPZM16, YYS16, MHP19, Sch12b].

eNB [CLM12]. Encapsulation [KG19].

Enciphering [CMLRHS13, HMR12, MLCH10, MKASJ18, Sar11]. Enclaves [WBA17]. Encoded [DG17, HS18].

encoder [PMG19a]. Encoding [BR14, CK18, SK12a, TJZF12, XHX17, CJL16, PC14, SM19a, Sun16].

Encounter [NA10a]. Encrypt [RAZS15, Ran14].

Encrypted [AD18, BTHJ12, BSA19, CWL14, CWL16, Cor14a, CDLW19, CHH19, DWB12, DCA18, FGRQ18, FCM14, FRS16, Fvo19, Gen13, GL12, GKG19, GZH17, GYW19, HWZP18, HTZR12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kaw15, KGV16, LA15, LGLK17, LQD16, Lop12, Mur16, NBPZ17, NNM10, PBC17, QLL1, Roh19, SAKM16, SZHY19, Sia12, SOR16, TM18, Uto13, Vai12, WBC10, XWSW16, YDY16, ZDL12, ZXY16, ZVG16, ZLW17, ACP19, AAH19, AHM18, AZH11, BBDP16, BTPSL15, BGP17, BKVI13, BTK15, BL11, CH11, Crl16, CDL18, DDDV19, DKL16, DRD11, DJ19, ED17, FTV10, Gen10, GSAMCA18, GZS18, GSMM16, HKA19, HH16, JCL18, KH18, LJKX14, LZY16, LHL18, LZWZ19, LW13a, MRR18, NJB19, OSSK16, PWS19a, PB19, PRZB12, SG19a, Schl16b, SEXY18, SM19b, SWW17, Suc12, TKMZ13, WR15, WS19, WL19, XMY17, XWY18, Yaa19, YX18, YQOL17].

encrypted [YQZ19, YJC18, ZLY10, ZZC17, ZFH18, ZHT16, ZWL19].

Encrypting [CC10, Mar10c, dRSdlVC12, Cla18, LGFGCCRP14, Pow14]. Encryption [ADJ12, AV12, AAUC18, AHE17, ALO12, AAC16, AEP18, Ano13e, Ano14b, Ano15c, Ano17d, Arm19, AKP12, ABF12, AS16, AG18, BVS13, BWLA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12a, BS14, BV18, Bla16, BKL12, BDP12, BHP14, BDLMN16, Boy13, BV11, BV14, BGV14, CVM14, CMO16, CLL16, CWWL12, CN12, CZF12, CLHC12, Che15, Che18, CGL12, Ch12, Chu16, CRE12, Con18, CNT12, CL16, CD16b, DR10, DN12, DFJ10, DLSB18, Des10b, DGFH18, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJHH12, Fei19, FFL12, Fuc11, GWWC15, GGH16a, GGH17, GM13a, GZ13, GSW16, GH11a, GH11b, GHS12, GHP12, GDCC16, GVW12, GVW15, GM14, GL12, GKS17, Gue16, HSMY12, HLLL18, HZ11, HG12, HWS19, Hor19, HC17, HTC15, HLH19, HP12, Int19, IAD10, JLS12, JSA17, JLH12].

Encryption [Jia14a, JR14, Kam13, KB10, KME12, KMY18, KTT12, KOS16, KKA15, KFOS12, KHP16, KKKK18a, KM18, KS12, KHRG19, LMG17, LMG18, Lau17, Led16, LLSW16, LLPY19, LW11b, LW11c, LW12, LLLC12, LYY13, LHL14, LLC15, LTZY16, LLL17a, LXF18, LLLH18, LSLW15, LHIc, LSQL18b, LNWZ19, LB13, LY15, LW16, LYY18b, LAT17, LLL12, LLH18, MZYH15, MLO17, MPP14, MR14a, MT11, MS18a, MVVR12, M17b, MSR17, MRL18, MB18, MRS12, MZLS18, Mor19b, MT12, MKRM10, MS12, Nac16, NdMMW16, NT12, NMS14, NAL17, OT12, OGK15, ODS17, PMZ13, PR12, PB12, PDNH15, PRGBSAC19, Per13, PKTK12, PPS12a, PYS18, PMZ12, PCY17, PRSV17, PWS19b, RVH16, RCP18, RZZ15, RM18, RSBGN12, RDZ16.
RVRCM12, Roh19, SGG18, Saa12a, SSW12, SERF12, Sar10b, SJ19, Sch15a, SLGZ12, SXH+19, SZS14, She14, SWF+19, Smi11b].

Encryption
[Sta12, SGB15, SMDP15, Tan11, TCM+17, TCL15, TMC15, Tan17b, TDDT13, TKR14, TT12, TF19, Unr15, Vaii1, VSR12, VOG15, Wal18, WCH+15, WP17, WDCL18, WSS12, Wat12, WLC12, WDDW12, WZ15, WHLH17, WWHL12, WMS+12, WQZ+16, WZCH19, XNK15, XY18, XXZ12, XJWW13, XWLJ16, XHX+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC+11, YFK+12, YCZY12, YKK12, ZCO10, Za19, ZPM+15, ZQQ+19, ZDL12, ZYT13, ZWTM15, ZQ15, ZW16, ZM17, ZY19, WH15, ZY17a, ZY18, ZWS+18, ZYH+19, ZHZ+19, ABC+18, AHS14, AASSA18, ATKH+17, AKKY17, Ana14, Anglo16, Ano13d, Ano15e, Ano16b, ARG19, ABR12, AMHJ10, ACD+15, AHL+12, BLL+19, BAA13, BZD16a, BC18, BKR19, BG14, BSW12, BGP+17, BTK15, Bro19, CFPT18, CFVP16, CFZ+10, CW14b, CH1+16, CMS17, CLC+19, CXWT19, CZ15b, CS11, Clm10, CW12a, CJW+19, CDF+10]. encryption [CM13, CGKO11, DLZ16a, DDM17, DTZ12, DMD18, Eve12, Eve16, FAF+18, FH13, FSGW11, FSGW12, FMB12, Fay16, GMOG18CC15, GH13, GHP13, GLM+16, GH12, GLL+18, GZXA19, HG11, HQZH14, HZL18, HKA19, HWD16, HZWX18, HL19, HT13, HLR11, HK19, HL11, HYL+19, HFT16, HTC17, HYS18, HYF18, HAW19, HKHK13, JZU+19, JCHS16, JCL+18, Jia14b, JSMD18a, JSMD18b, JHCC14, JSM+18, Kam16, KHM13, KKM+14, KV19b, LLL16, LCL+17a, LGP19, LCL+15, LFZ+17, LW+19, LCT+14, LFWS15, LLM+19, LPS10, LHL11, LW10, LK10, LW13b, LZZ14, LPZ15, LCY+16, LZZ17, LJW+17, LJWY18, LLL+18, LKZ19, LDZ19, LL16a, LW13c, LSC12, LLG19, MBP19, Mar12, Mar10b, MMS17c, Mes15, MML16, Mid10, Mon13, MSaa13, NES+14, Nam19, OPHC16, ONS19, PPA18, Pet12, PBP19, QRA+18, Ran16, RGG10, RZW13, RPSL10, SES+16, SE18, SLL+19, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14].

encryption [SLZ12, SY15b, Sha13, SGGE14, SGFCRM+18, SLM10, SKB+17, Sp16, SGP+17, SGM16, Tam15, TPL16, jT12b, WGG10, W10, WYY11, WLLG11, WHY+12, WDL13, WZ16, WFX17, Wan18a, WM19, WDG19, WDL19, WGG+12, WLS14, WCC18, XWZ16, XWXC14, XSS10, XXX15, XWS17, XZP+19, XWZ+18, XTZ+19, XLC+19, YWJ+19, YTT11b, yYqWq13, Yan14, YZ17, YHM18, YSM19, YWY+19, YCT15, YJC18, YLZ+16, YL11, ZCQ19, ZAB17, ZWQ+11, Z11, ZLW+12, ZJ+14, ZWM14, ZT14, Zha15a, ZC15, ZLM17, ZYC+17, ZGL+18a, ZCL+19, ZY+19, ZZ12, ZL12, ZDW+16, ZY17b, ZCZ+19, Zlu13, Wan14, GMdFPLC17, LAL+15, Sar18a, Kat13].

Encryption-based
[SERF12, BC18, XWZ+18].

Encryption/Decryption
[KB10].

Encryptions
[zGXW12, LG12, SLY+16, RD17].

Encyclopedia
[vTJ11].

End
[Ano15c, BRR+15, BGP+17, CFE16, Ch16, MHS16, RST15a, RST15b, Bel18b, Bro12, Ch13a, JZU+19, Wan18b, Zor12],

end-devices [Wan18].

Endo-End
[CFE16, MHS16, RST15a, RST15b, Ano15c, BRR+15, BGP+17, JZU+19].

endomorphism
[FWS13].

Endomorphisms
[AK14b, LGH+17].

Endurance
[JS17]. Endurance-Aware
[JS17]. enemies
[Fag17]. Enemy
[BC14, CAC14].

Energetic
[PDMR12].

Energy
[Ano15d, AZF+12, ABC+17, Bla16, CKHP19, GPR+19, JEA+15, LSC+15, LLD19, MP12, PAF18, RPHJ11, TCL16,
TCN⁺17, VN17, AHG18, CZ14, Fai19, MMF15, URK⁺19, ZTZ16. energy-based [MMF15]. Energy-Efficient [LLD19, MP12, TLCF16, AHG18].

Energy-Harvesting [ABC⁺17].

Energy-time [Ano15d]. Enforced [Set16].

Enforcement [LLZ⁺17, Tan15a, Cra11, CFG⁺17]. Engage [SDG⁺17].

engaging [ISC⁺16]. engine [BS13a].

Engineering [BCHL19, Bel18a, FSK10, GHD19, MMKP16, LSM18a, MP12, PG1L10, SNG⁺17, TQL⁺14]. Engines [LB13, BGG⁺13]. Enhance [DHT⁺19, CZ14, SLM10]. Enhanced [DTE17, KY10, KKM⁺13, MS17, SG18, SS15, TV15, Yi17, YCC16, AMN18, AM19, ACK⁺10, DLK⁺16, DXWD16, GM16a, LNKL13, YWZ⁺18, YQLI17].

Enhancement [FSX12b, JSA17, LA15, NNA10, CMS11, SVY19]. Enhancements [Chel18, FSX12c]. Enhancing [CSW12, IA15, Lan13, MZL⁺19, YS15, AGBR19].

Enigma [KM15, KM16, LHA⁺16, Ore14, Ano16d, Bur11, Cas15, Kap11, Kap13, McG11, MK12, Tur18]. Enigmas [Bat10].

Enough [JCM12, Ano14b]. Enrollment [YWZ⁺12, DEL19]. ensuing [SIS17a].

Ensure [PWS⁺19b], entangled [EAB⁺19].

Entanglement [Ano15d, JEA⁺15].

Entanglement-Based [JEA⁺15].


Entrepreneur [IM16]. Entropy [DSDW14, DSDW17, DK16b, KP13, VS16, YGFL15, BNY14, TKB⁺18].

Entropy-Based [YGFL15, enTTS [YL17]. enumerators [OSI1]. Environment [AARJ12, BCG16, FYD⁺19, HQY⁺18, KKA15, MLO17, MRS⁺17, RQD⁺15, SG18, SAM⁺19a, TV15, VFFH19, YMA17, FHZW18, GAI⁺18, HL19, HLS14, KKM⁺14, Kim16, KS19, NR17, Par12b, RR16, SYWX19, SKB⁺17, WL12, WCFW18, WT10a, XXX15, YWK⁺10a].

Environment-Independent [HQY⁺18].

Environments [HXHP17, HLKL15, LQY10, PAS13b, TMGP13, VFS⁺19, XLP⁺18, CNF⁺18, CLHH13, CTL13, KPP16, KAS15, LNK⁺18b, LW13a, LCY⁺16, MHL18, NACLR12, SCY15, SA19, Tan12b, VDO14, VGL14].

Eof [Gup15]. ePassport [ABHC⁺16].


Equally [CHH⁺19, HTC⁺15, LLSW16, MZHY15, WZCH19, HTC17, ZCZQ19, ZCL⁺19].

Equational [ABR12]. Equations [BP10, SR12a, DGL19, ZYGT17]. Equi [Ma17a, PD14]. Equi-Join [PD14, Ma17a].

Equifax [Ber17]. Equijoin [WP17]. equipped [KNTU13]. Equivalence [ABR12, CCK12, CCC16, GLW12, LYL⁺18, SS13, WGD18, HKT11]. Era [Mos18, OMNER19, KVI19a, QCX18, ABJ13].

Ergodic [LAD10]. Erratum [YFK⁺12].

Error [GSGM16, KW14, LSC⁺15, MCP15, MKASJ18, TLCF16, Zaj19, ATI⁺10, BZD16a, Chi13a, CJW⁺19, LTT10].

Error-correcting [MCP15, LTT10].

error-tolerant [BZD16a]. Errors [TM18, CSS⁺13]. ErsatzPasswords [GAS⁺16].


eSkyl ine [BKV13]. ESORICS [Ver17].


Establishment [AS12, Ano11b, BCO13, DL12, NYR⁺14, BEB⁺18, GTSS19, SZMK13, ZPZ⁺16, ZWX⁺18].

Estimating [VJH⁺18, MMF15].

Estimation [BCF16, GSN⁺16].

Estonian [Ano17c].

Ethereum [Fai19].

Ethernet [KCR11]. EU

frail [AAA+19, CHHW12, MCDB12, SSA13, WK18, ZWZ17a, ZHS10, CCLL11, FGLL10, WHZ12]. fragile [BWP13, VM14].

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

Framework [BJL16, CD12, DG17, HXC+11, KPC+16, KYEV+18, LLG15, LSC+15, LY15, LQD+16, LQG19, MSU13, SK11, Scr18, SYC+17, SEK+19, TSH14, VPK17, XHZ+19, ZJ14, ATKH+17, BHCdFR12, CRS13, GQH17, GM13b, HPL+19, JZU+19, KKGK10, KM14, KS19, MMS+17a, MBF+13, PSDK+13, PCGLS11, PAK15, SD10, SA16b, SYW17, SA19, ZY+17]. frameworks [LSBN14]. France [Kap11].

Frank [AbJ13, Joh10, Mar10a]. frankencerts [BJR+14]. Fraud [Ber12, CEL+19, MT17]. Fred [Xie12a, Xie12b]. Free [App13, Boy16, CCD19, CCD20, HLH19, IL15, LSQZ17, LSQL18a, TWZ+12, TTH15, WZQ19, YY17b, ZLH+12, ZM18, AJY18, ATK11, ED18, LQD+10, LL16a, SA12, SE16, YT11b].


Frequency-Based [LWC14]. fresh [GJ19]. Freshness [RBNB15]. Freeselet [FMB+18].

Friendly [Fra16, KCC17, SZDL14, ACM12, BP18, FK19, KLW+16, RD17, WOLS12]. Frontside [DDR+16]. FSR [MD12b].

FSR-Based [MD12b]. Fugue [AP11]. Fujisaki [TFS19]. Full [Arm19, ALR13, DGFH18, HR19, HEC+12, LW12, VS16, WLC12, BKR11, DDM17, LC13, Ran16, SWW+17, SKP15, Tam15, TY16b].

full-hiding [DDM17]. full-text [SWW+17]. Fully [AKP12, BV11, BV14, BGV14, CMO+16, CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, KKK+18a, LMGC17, LSLW15, LJJ16, LATV17, LSC12, MV12, MSM18a, Nac16, NCCG13, PB12, SGH15, Val11, VV19, WHC+15, XWZ+18, ZZ12, DDL5, GH13, MBP19, ZY+14, ZML17]. Fully-Homomorphic [GH11b].

Fully-Homomorphic-Encryption [CN12]. Fun [APPVP15]. Function [AMPH14, Bec17, BKST18, BBKL19, CIZ13, FLS+10, GGK18, GKG19, GHY18, LJJF19, LyWZZ12, MMS17b, RJJ+18, SGY11, WSSO12, YWJ+19, AKY13, ABO+17, AP11, Bar19, BDPV12, CMM17, Con17, LK14, LP11, RS14, Sar11, SXL16, SCBL16, TQL+14, WYW14].

Function-based [YWJ+19]. Functional [AS16, BV18, BSW12, Boy13, GGH+16a, GVW12, LQD+16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14].

Functionalities [JR13]. Functions [ACZ16, ALR13, BBC+14, BKK4, BKPW12, BHT18, BKL12a, CCL+19, CPS16, DSSM14, DQFL12, FY11, LVV11, NIS15, NR12, Rja12, RW12, SMS14, SLY+16, Tan12a, WCXZ17, YTP11, AY+14a, BDP11, BDK16, BCGLS16, CG12b, CQX18, CW12a, ESRI14, Gen10, HRV10, HLI2, Kom18, Li10, QZDJ16, WT13].

fundamental [Bre18].

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

Fusion [ABCL17, YYK+17, HW19]. Future [AYS15, BCE+12, BKBK14, Bon12, BLU+15, CDF16, Fri13, GCK12, HYS18, KHN+11, Mon13, SG19b, AP18, Anol3f, Dya19, FPBG14, Mac12, PPA18, PHWM10, MJS13].

Future-proof [Mon13]. Fuzzy [HWZP18, KRDH13, NC12, SH11, USH19, XJWW13, Alp18, BSBG19, HK17, KHMB13, LYC+10, MMSD13, SM11, SNM14, SC19b].
GHZ-State [CCL +13]. giant [Joh15].
Global [CLP13a, CLH13, MR3 +17, GH16, LH11b, TMK11, ZX11, LNK +18a]. Globally [CCS14, LG10]. Glyph [XZZ18].
GMAC [SKK10]. Goal [BMP12]. Goal-Driven [BMP12]. Goes [BCD +12, RY10].
Goldfeder [Ano16a]. Goldreich [Lin17].
Goldstrike [BH15]. Goldwasser [Gol19].
Goliath [Sch15c]. Gong [LLW16]. Good [DQFL12, FY11, Raz19, LSN14, RY10, SA14, WT13]. goodbye [HU15].
Google [Har14, Loe15, VGN14]. Goppa [MBR15].
GPUs [AVAH18, VKP117]. gossip-based [FG19].
gossip [Wat15, Mic10a]. Grain [BMS12, SBM15, FSGW11].
Grained [CDD13, PV17, YTH17, CLH +16, LH3 +18, XYML19, ZML17]. Granular [SY +19].
Graph [ATS15, GTT11, WH18, GJM15].
graph-based [GJM15].
Graphical [BCV12, MC19, CTL12, Eng15, LTC +15a, MZL +19]. graphical-based [CTL12].
Graphics [HHMK14, ABDP15, KY10, PLL10].
Graphs [BFM12, KU12, KA18, Lau17, PMZ12, BBGT12, KLN15].
Grey [BCKP17, LRW13]. Grey-box [LRW13].
GREYC [AGBR19]. GREYC-Hashing [AGBR19].
Grid [CGB +10, DLZ +16b, KS15, LPL15, VTY18, AMN18, BC16, CDWM19, DZC16, JAS +11, MCN +18, WS12, YY11, ZZY +19].
Grid-Based [LPL15, WS12]. Grids [SC10, CT11b, GLW13, LWK +19, Shy15, JAE10].
Gröbner [EVP10, FES10, Tam15]. Gros [Dan12].
Grastl [ABO +17]. Ground [KP17]. Group [AEHS15, BSBB19, BSV12, CQ18, CGY +13, CLW16, DT13, FVS17, HL3 +10, Har13, LLZ +16, LCC13, LWL +17, TW14, XLM +12, XGLM14, XZLW15, YJSL18, ZKH16, AKK +17, CML +18, GBNM11, HCCC11, HPY10, IOV +18, LLLS13, LWS10, LML +19, PY19, RS15, SCL16, WDZL13, WTT12, YZZ +18, YLL +18, ZZKA17, ZWQ +11, ZGL +18a].
Group-based [LLZ +16, CML +18]. group-key [IOV +18]. Grouping [LNZ +13].
Grouping-Proofs-Based [LNZ +13].
Groups [Abe12, GZ12, HS +19, XNK15, YS12, YKNS12, LLY06, MZ17a, WQZ +13, ZZ15].
Grover [JL18]. GRS [TD14]. GSR [LC17].
Guangdong [IEE11a]. Guaranteed [TBCB15]. Guarantees [FVB +18].
Guerrillas [Has16].
Guess [FSWF11, Fok12].
Guessing [Che15, LCL17b, XJWW13, FIO15].
Guest [Ano19a, Gu15, BdD19, LK18].
Guidance [BD15].
Guided [CJFH14, ZSM18]. Guidance [DG14].
GVW [HLC +19]. gwAs [SAM +19a].
Gyroscopes [SNCK18]. GyroFinger [SNCK18].
Hand-held [SR12a, Cho10].

Hand [CCLL11, KSSY12]. Hand [SR12a, Cho10], hand-held [Cho10].

Handauth [HBC13]. Handbook [Bee17, AB10b]. Handheld [Bee17, AB10b].

Hall [Ran10]. HAIFA [DL17]. Half [BBKL19]. Halftone [GL10]. Hall [Full10, Don14].

Hamming [HRK18, CCLL11, KSSY12]. Hand [SR12a, Cho10], hand-held [Cho10].

Handshelf [Bee17, AB10b]. Handheld [RPHJ11, CTL12]. Handoff [HZC13].

Handover [HBC13, LBR12, CLM12, CML18, FLL11, LNN13, QMW17, YHL16, YHHS16, YLS12]. Hands [Bre18, GPT14, BSS11], hands-on [BSS11].

Handshake [KK12, KKL16, SM10c, WZ11].


Hard-to-Invert [ZWTM15]. Hardcover [Joh10]. Harder [KTA12, Sch16c].

Hardness [AH19, BKN13, SS13]. Hardware [AW15, AW17, ARH18a, ADSH18, BNMH17, BRP13, BDM11, BJCHA17, CMLRHS13, DZS18, DOS15, ERMCG5, GP17, GPR19, GCVR17, GM16b, GCS13, HKL14, HGI12, HSA14, HC17, HLN10, KAK18, LGH17, LLKA19, LRWV14, MLCH10, MCS15, MRL18, MYH18, NDC13, NdMMW16, PC16, PG12, RMP10, SN10, Set16, Sti19, Tay17, VCD16, WOLP15, YSF18, YDV19, ZLI19, ZHS19, ZAG19, AMN18, ABO17, BDM18, BGG13, EAB19, KHF10, MD12a, NS10, Nov10, PAB19]. Hardware-Assisted [LLKA19, GPR19]. Hardware-Based [HLN10]. Hardware-Enabled [YSF18].

Hardware-Enforced [Set16]. hardware-entangled [EAB19].

Hardware-Intrinsic [SN10, NS10]. Hardware/Software [MRL18].

hardwares [SKH15]. Hardy [Xie12a, Xie12b]. Harmonic [YNNW15].

Harnessing [DFKC17]. Harvesting [ABC17, ZGC16]. HAS-160 [WLC12]. Hash [Ano12, AMPH14, BHH15, BKST18, BK12a, But17, CLP13a, jCPB12, CZLC12a, CZLC12b, CZLC14, CZP12, DCM18, DL17, EAA16, FLS10, GI12, HCPSLB12, Hui13, HRS16, HBG17, LYY18a, LYX19, LJJF19, MST17, MKF16, MCF17, MKAA17, MKAJ18, NIS15, NTY12, NR12, NXB13, PTT16, Rja12, SGY11, WSO12, ZZM17, ZHZ19, AY14a, AKY13, ABO17, AP11, BCGS16, CJP15, Con17, ESR14, HL12, KKG14, Par18, PPB16, RS14, SPLHC14, SXL16, WYW14, ZCQ19].

Hash-Based [BH11, But17, DL17, GI12, HCPSLB12, Hui13, HRS16, HBG17, MKF16, MCF17, MKAA17, NXB13, CJP12, CJP15, PPB16, SPLHC14].

Hash-Counter-Hash [MKAJ18]. Hashing [AEE14, AB17, ASBD16, BHKN13, BKL13, BP18, Kaw12, BDK16, BCGS16, CP13, AGBR19]. Haskell [Rus15].

hatching [WYK12]. HB [SHI11, PYH18]. HDH [PDNH15].

Health [AMSP19, LY13, LHL15, Rao17, ZVG16, AKS19, BC18, CLC19, Ham19, IC17, OSP19, WXY17, YZL18, ZAA17, ZDHI18, JK16].

Healthcare [BN14, HLKL15, ZLDC15, ASO14, Kim16, ZGL18b].

Hearing [Bla16]. Heart [GMDFPLC17, HCYZ18]. Heartbeat [IA15].

Heartbleed [DKA14, Ven14].

Helios [CFE16]. Hell [Han12].

Hellman [ABD15, ABD19, Chi16, FHLOJRH18, Hof16, HLCL11, HLIS14, LC14, LNL19, Mc16, Om16, RH10].

Helmut [Mur10].

helped [Smi11a]. helper [RWZ13]. HeNB [CLM12]. HEPCloud [RJV18]. Here [Dya19].

Hermitian [ACA16]. Herodotus [Keb15, Mac14]. heroine [Fag17]. Hess [HP17].

Hess-Like [HP17]. Heterogeneous [KS18a, SP15b, YZDZ19, AIK18, ABB19a, SZMK13, SCCH10, SHC16].

Heuristic [BGJT14]. Heuristics [SKE18, KO14].
HEVC [DG17, GKS17]. HIBE
[LW11c, LSQX19]. Hickory [NN15].
Hidden
[FMS12b, PSS+13, YLL+12, ZYT13, ZYY19,
BDK11, LCL+17a, Sch15c, Smi15a, ZX+19].
Hiding
[AAA+19, DCA18, GGH+16b, GL10,
JHHN12, KD19, MK12b, OT12, XLM+12,
XGLM14, XZLW15, Ara13, DDM17, HZL18,
KWH16, LXLY12, LT14b, SM10a, UUN11,
WLH13, WZLW13, ZWM14]. hiera [Lac15].
Hierarchical [ADM12, BSV12, DBT19,
FSX12a, LSLW15, LHW18, NMS14, NLY15,
OT12, SSSA18, WLWG11, WYML16,
WHL17, ZMW16, ZHW+16, ZYZ+19,
DSCS12, HYS18, JCL+18, KBP17, LFZ+17,
NZM10, RG10, SE14, SE16, WWYZ11].
Hierarchies [MM10]. hierarchy
[NA10b, VN16]. High
[AW17, ASBm16, Ano17d, ARM15b, Bar15,
BDL+11, CLB19, DM15, DG17, FHLH19,
FYD+19, GL12, GCS+13, HMKG19, HZ11,
KFE19, KMP+11, KPC+16, KAK18,
LTKP16, LCK11, LLY+18, LPO+17, MS13b,
MS13c, MM17b, MSR+17, PCPK14,
WYCF14, WL11, XNRG15, XLP+18,
AHG18, ABBD13, GZH12, GCVR17,
JLC18, KLM13, MAK+12, PABC+19, RS17c,
WLH13, WXYL16, WZLW13, WKH11].
High-Assurance [Bar15, KMP+11, WL11].
High-capacity [GZH12d].
High-Dimensional [Ano17d, XLP+18].
High-Efficiency [DG17]. High-Impact
[DM15]. High-Level
[AW17, KPC+16, ABBD13]. High-Order
[FYD+19]. High-Performance
[GCS+13, KAK18, LPO+17, CLB19,
FHLH19, AHG18, GCVR17, PABC+19].
High-Rate [PCPK14]. High-Security
[WYCF14, BDL+11]. High-Speed
[ARM15b, HZ11, LTKP16, MSR+17,
BDL+11, KFE19, KL13].
High-Throughput [HMKG19, MAK+12].
Higher [LWK12, PRC12, gWpNyY+14,
ZSW+12, LWKP14]. Higher-Order
[LWK12, PRC12, ZSW+12, gWpNyY+14,
LWK14]. Highly
[CD16a, SZDL14, SC19b, AC1+15, DT13].
HIGHT [CWP12, WWBC14]. HiiMap
[HEP+11]. hijacking [BCFK15, DCAT12].
Hill [KPW13, KA17]. HIMMO
[GMRT+15]. himself [Pro15]. Hindering
[BTPPL15]. HISS [DT13]. histogram
[CSS+13, Lin14a]. Historians [Cer14].
Historical [Hai17, Han12]. History
[ABJ13, Ano19b, Cer14, COp10a, LT14b,
MK10, MK11, SE16, Sni15a].
history-free [SE16]. Hitler [Hea15, Moo14].
hitting [GR19b]. HIV [GSM16]. HMAC
[GWM16, MAK+12, YGS+17].
HMAC-DRBG [YGS+17].
HMAC-SHA256 [GWM16]. Hoc
[LH12, PD14, She14, SS15, XHC+12,
BBB19, KMO10, LJJ14, PY19, SGGR+16,
WXSH19]. Hoffstein [Mei10]. HOL4
[HK14a]. Holden [Ano17b]. Hole
[Ano15d, BKKV10, PC16, YKA16].
Holocaust [Han12]. holy [Wat15, Mic10a].
Home [BD18, HXHP17, KH+11, KPP16,
SYWX19, Cor14a]. Homes [VJH+18].
Homogeneous [HT11]. Homomorphic
[AAUC18, AKP12, BV11, BV14, BGV14,
CMO+16, CN12, CJ13, CK18, CNT12,
DOS15, GH11a, GH11b, GHS12, GHS12,
GHY18, KOS16, KG16, Kim15, KKK18a,
KRKG19, Lau17, LCLL15, LATV17,
ML017, M5M18a, MSR+17, MRL+18,
MBF18, Mor19b, Na16, ODSS17, PKTK12,
RCP+18, RMZ19, Roh19, RJV+18,
Tan15b, Vai11, WHC+15, WXXZ17,
XWZ+18, AKKY17, BDOZ11, BC18,
CJXX19, CW12a, DMD18, GH13, GHPS13,
GLM+16, LLW16, MBP19, SEXY18, Tam15,
WSC14, YJJ18, ZXY+14, ZY+17].
Homomorphically [SG19a].
Homomorphism [Bra13]. Honey
[JR14, CJW+19]. Hop [RWLL14, LCT+14].
Hop-by-Hop [RWLL14]. Hope [SD18].
Identity [LZJX10, PN10, Sar18a, Kat13].
Identity-as-a-Service [VFFHF19].
Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CLND19, CGL12, CGY13, Chi12, FHH10b, FZT14, FR15, FSX12b, FSX12c, FSX12a, GY13, GJJ15, GJZ17, HZC12, HSM14, HZX15, LGX18, LYX19, LSL12a, LLC15, LTZY16, LSLW15, LH11c, LSC12, LBR12, MLO17, RDZ16, SGH15, TKR14, TFS19, Wan14, WZCH19, XZX2, XJW16, YZX12, YHK10, YKC11, YFK12, YCZ12, ZLH12, ZMY12, ZYX19, ZPXX17, ZYM18, ZYH19, CSZ11, HSM13, HYYSH11, HYF18, LKAT12, LXJ14, MJGS12, RS15, SXX19, SWW16, Tia15, TH16, ZDW16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT15, HZC14, HWDL16, HZWW17, HLR11, HSW10, HBW12, HL11, HPY10, Hwa11, JCL18, LK12, LCT14, MJS13, MM13, NCL13, PZL19, QYWX16, RG10, SE14, SE16, hSZZ15, SA16b, SSA11, SGM16, WLFX17, XW12, XCL13, YWL17, YWJ19, yYqWqZC13, YKC12, YXA16, ZZ12, ZYM19, LZJX10, Kat13].

Identity-Enabled [SG12].
Identity-Hidden [PSS13].
Identity-Preserving [MHW19]. IdM [ACAT15].
IDs [SOS15]. IEC [BCM12, BCM13].
IEEE [IEE10, IEE11b, IEE13, IEE15, MSH16, TBL19, Yan10, Ano16g, BOB13, CL11, FLH13, FZZ12, NBZP17, ZBR11].
IEEE802.16e [HLCL11]. if [ABJ13, Pec17, Rus15]. IFIP [GLIC10]. IFF [MMZ12]. IFTTT [BD18]. Igor [Sha10]. II [Mun17, SCPSN10b, SM10, ZWS18].
III [SMOP15]. IIA [HZS19]. Illegal [ABJ13]. Illinois [Nor17]. Illogical [Hel17]. Illumination [KLY12]. Illusion [GHS14]. Illustrated [Cop10a]. Im [BG10, BG12]. IMA [Che11]. IMACC [Che11]. Image [BS11, Bai10, BAAS13, BDB14, BWR12a, CJIH14, CCC19, DA10, DC18, DS19, GRRZ18, HD19, IAD10, JKHeY12, KPS10, KL15, LLL17a, LFX18, LLLLH18, LZX19, MBC15, MAL10, MSM18b, PW10, QIC18, RS16, VRSCM12, SH11, SM11, SZHY19, SJ12, SG12, SMSK18, SS17b, SSA13, SRA1A, SZST18, TB18, VCA19, WHZ12, WX1L2, WYW13, WYCF14, yWXyZ18, WYK12, WYL18, YLL12, YWNN15, Ye10, Ye14, YH16, YXD18, ZXZ11, ZWW17, ZW17a, ZW17b, ZHS10, ARG19, AM19, BWA13, BM13, Bro19, CT11a, CW14a, EA11, FMB18, GKKC11, HAK19, HLC16, KMG17, KM11, KKK18b, LXXC11, LX10, LW13b, LW13b, LPZJ15, MO14, MS17, NES14, PTK14, SE18, Sch12a, SM13, SM12, SNM14, ST15, SGFCRM18, Sun16, jT12b, TTL10, TLL13, UUN11, UUN13, yWpWypN13, WDG19, WHZ19, WGY12, WSS19, WKH11, WOLS12,
XSWC10, YWL+17, YC11]. **Image** [YCC16, YSC16, ZLW+12, ZT14, ZSMS18, ZL12].

**Image-Guided** [CFJH14].

**Image-Scrambling** [LLL17a].

**ImageMagick** [Tay14].

**Imagery** [BCP14a, Ara13].

**Images** [BCPV11, BBM15, CLF11, FR16, GL10, LC15, LLY+12b, MR16, NC12, YAM12, dRSDlVC12, AM19, AMK12, DD13, HWYW14, LW13b, MM14a, MKH+12, UUN13, WLI13, WZLW13].

**Imaging** [WW13].

**IMFlexCom** [PAF18].

**IMI** [PN10].

**imitation** [Hai17, Pro15].

**Impact** [Alo12, ACC+13, ATD17, BLS12, DM15, SF12, vRDIHP17, BGE+18, HURU11].

**Impartial** [BCF16].

**Imperceptibility** [HGT15].

**Imperceptible** [Lin14a].

**Imperfect** [ABD+15, ABD+19, BHvOS15].

**Impersonation** [AATM18, GBNM11].

**Implantable** [BDM+19].

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

**Implausibility** [GGHW17].

**Implementation** [AAUC18, BW16, BKLS18, BSJ15, BDMLN16, EGC+12, FHLOJRH18, FHL19, GP17, GL12, GPT12, GM16b, GCS+13, HMKG19, HJ19, HF14b, JLZ18, KB10, KG16, LYL+18, MFG16, MAS16, NdMMW16, QL17, RMP10, Sco18, TV19, VKPI17, ZPM+15, AM18, Ang16, BDP+12, GH13, GAB19, HBBRMN+16, KFE19, KY10, KSH18a, KSH18b, MM14a, MNNW15, NES+14, PBCC14, SK14, SAAB10, VGE14, SF12].

**Implementations** [BFCZ12, BFK16, BDGH15, BJ10b, Bru12, CMLRHS13, CBL13, ERRM15, EKOS19, GZSW19, LGH+17, MLCH10, MWES19, NDR+19, SJLK18, SG19b, Tom16, VV18, YZLC12, ZSH+19, ABBD13, ABF+14, BFG+14, BJR+14, CFN+14, CGH17, LBOX12, RSMA19, Sta11c, ZSW+18a].

**Implementing** [Dav11, GH11b, HTZR12, KV19b, LTC+15a, SG15, SVGE14, SLM10, VOG15, SA16b].

**Implications** [DK16a, OSH16, SC19a].

**Implicit** [BBD19].

**Implies** [BHT18].

**Importance** [YL17, MLMSG12].

**Important** [TC10].

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

**improbable** [TS16a].

**Improve** [AQD12, PMG19a].

**Improved** [Ber18, BCP14a, Chi12, CGKO11, DL17, FVK17, GLLSN12, GR19a, HLS18, HIJ+19, IK15, JIH12, KZG10, LT14a, LW12, LJF16, LJF19, LHH11, LCCJ13, LC15, LYD+18, LS+19, LLML12, MM17b, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WCD19, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, ZL+19, CNF+18, CBL10, GLW13, HBB12, Nam19, PWLL13, SDM10, XHH12, YSQM19, Wan14].

**Improvement** [FRS+16, LFX+18, LYL+18, LJ19, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNM+11].

**Improving** [AB15, BCM+15, Chi16, FMS12b, GMS11, HCL11, MHC12, Sar10a, SS11, YWF18, YKBS10, ZHS10].

**In**-**browser** [ABR13].

**In-Memory** [PAF18].

**In-Order** [ZBPF18].

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

**Incentive-Aware** [YTH17].

**Incident** [CCG+16, CMG+18, GQH17].

**Incomplete** [FD11].

**Inconsistencies** [YSC+15].

**inconsistent** [OF12].

**Increase** [NNAM10].

**Increasing** [AEH17, CLZ+17, HSC19, PKS18, RSX18].

**Incremental** [KKM+14, MPRS12, CS11].

**Incrementing** [KS15].

**IND-CCA** [AHS14].

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

**indefinite** [Svo14].

**Independent** [FCM14, HQY+18, MTY11, MKRM10, YE12, ZTL15, BVIB12, BCGS16, DDD14, SCR19b, VV19].

**Index** [LKHR10, PSS+13, ZXY16, Jou13].
FQZF18, FMC19, GAI+18, HHBS18, Hod19, KV19a, KKK+18b, KKD+18, LSQ15, LZZ+19a, MMP19, NVM+17, OSANAM19, PCK19, RC18, SSSA18, SGC16, SJLK18, TODQ18, TG17, Wau18b, WCFW18, WZK+17, XYML19, YWJ+19, YFT18, YTH17, ZCWS15, ZLY+19.

IoT-Based [YTH17, ZLY+19].

IoT-Enabled [SGC16].

IoT-FBAC [YWJ+19].

IoTs [SAJL16, ZSW+18a].

IP [AGLW16, AZH11, LMS10, PJ18, PA10, RS17c, SP15a, TJJF12, WBC+11, WZM16].

Isolated [HB13].

IRC [HURU11].

Irregular [WYJ+17].

Isabelle [Kam19].

ISBN [ANO15b, Ano17b, Bai12, Joh10, Mur10, Sch15a].


Islet [Dan12].

ISO [BCM12, BCM13, TS16a, WWC14].

ISO/IEC [BCM12, BCM13].

Isogenous [Y+17].

Isogenous [AMMV14].

Isogeny [BF19, FHLJRH18, KD18, KAK18, Lau17, LNL+19, ZSP+19].

Isogeny-Based [BF19, KAK18, ZSP+19, KD18].

Isolated [GKG19, Sch19b, YS15, KJK+16].

Isolating [LG12].

Isolation [GGK18].

Isomorphic [AMMV14].

Isoleth [HGOZ19].

ISSAC [Wat10].

Issue [ANO15b, Ano16b, Ano16c, Ano16].

ISO [ANO15b, AHWB20, BCHL19, CWZL13, CSYY18, GO17, LW13a, LK18, XW13, YYW19, PHWM10, Sim15b].

Issues [ABHC+16, PZPS15, VKK+19, JAE10, KJN+16, MHV15, SVGE14].

ITE [ANO15b].

Italian [Sac14].

Italy [Cra12].

Item [CZ19].

Items [CZ19, YD17].

Iterate [HHR11].

Iterated [LP12].

Iteration [CCZ13].

Iterative [QJC+18, SX16].

ITU-Be [FXY+17].

ITUBee [FP+17].

iVector [RSR+19].

iVector-Based [RSR+19].

J [Bar12, Led16, Sch15a, WZM12a].

J2ME [GPT12].

J2ME-Enabled [GPT12].

Jacobian [BAAS13].

Jacobians [Hes12].

Jacques [Nac12].

Jamming [BCDN17, YS114].

Janet [Ayu12].

Jannie [KNU10].

Japanese [Dia14].

Java [GPT12, XHH12].

Jaypee [CGB+10].

Jean [Dew11, Nac12, SR14].

Jean-Baptiste [Dew11].

Jean-Jacques [Nac12].

Jeffrey [Mei10].

Jill [Mei10].

Joachim [Hom17].

Joe [Car11].

Johan [Ten18].

John [Wes16].

Johnny [HM12, RAZS15, RS19].

Join [PD14, Mal17a].

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

Joltik [LGS+19].

Joltik-BC [LGS+19].

Jonathan [Ful10, Mou15].

Jones [Ber16b].

Jose [ACM11, IEE15].

Joseph [Ano16a, Mei10].

Joshua [Ano17b].

Journey [CFST17, RS19].

 Joux [AY12a, AY12b].

JPEG [AOT13, DLGT19, LSQ11b, LC15, MAL10, QZ14, SK12a, SHC+16, WHZ12, WLH13, ZC12].

JPEG-2000 [ZC12].

Julia [KD18].

Julia/Nemo [KD18].

July [MSh+16, Wat10].

Junction [VDB+16].

June [ACM10, ACM11, Gill10, Kap11, TBL19, TTT18, Wes16].

Juniper [CCG+16, CMG+18].

Juraj [Gas13].

Just [Mil10].

JXTA [AMHJ10].

K2 [PS12].

Kaanie [Ver17].

Kahn [RN16].

Kalyna [ORK+15].

Karatsuba [BCL14, MSR+17, MRL+18].

Kashmuni [BCP11].

KASE [CL16].

Katz [Ful10, Mou15].

KDM [CBX19, MTY11].

Keccak [BDPV12, RS17a, BDP+12].

keep [Rus15].

Keeping [CG14b, Man13, Gup15].

KEM [CZLC14].

Kepler [LGP19].

kept [Cha13c].

Kerberos [SCKH10, TW14].

kernel [GM13b, HHA19], kernel-assisted [GM13b].

Key [ASN12, Alz19, ADSH18, Ano11b, ABB19a, BN14, BVS+13, BL12, BSBB19, BBB+16a, BD15, Bar16a, BR19, Ber16a, BM18, BCO13, BKLS12, BF11, BKKV10, BB10,
CVM14, CT18, CLY14, Che15, CLND19, CWZ19, CJ13, Chi16, CCT+14, CNT12, Con12b, CMA14, DWWZ12, DL12, EAA+16, EFGT18, FZT13, FHLOJR18, FVS17, FBM12, GDLL18, GFBF12, GT12, GZZ+13, GSW+16, GST13, GPT14, Gir15, GkS17, GZ12, GLB+18, GYW+19, HSMY12, HLLG18, HEP+11, HC12, HL10a, HWS+19, HCL+14, HFC+15, HEC+12, HLH19, Jia14a, JEA+15, KP12, KNZS19, KTT12, KFOS12, Kim15, KG19, LYX+19, LLSW16, LKBK19, LG0, LCLL15, LDZ16, LQY10, LY16, LH11c, LSQ18b, LCCJ13, LWL+17, LYY+18b, LBR12, LLH18, MJZHY15, MVV12, MMP14, MRY11, MMY12, MV19, MKK17, MPRS12, MNS11, MSU13, NAA10, NRY+14, NTY12, Omn16, PS17, PDNH15, PCPK14, Pud12, PRNC17]. Key [RVH+16, RSBG12, RW12, Saa1a, SK11, SNJ11, SEHK12, Sas18, SK12b, Seo18, SWM+10, Sia12, SD18, SGH15, GLB+18, TMC15, TYP+17, TM12, VAG19, WP17, WSS12, WLC12, WZ15, WCL+18, WWHL12, WT10b, WSQ+16, WXZ17, XNG15, XZ12, Xio12, XLM+12, XJWW13, XGML14, XZLW15, XR+17, YMY+16, YZ1+12, YS12, YLS19, YL13, YRT+16, YL17, Yon12, YKF+11, YFK+12, ZSP+19, ZKH16, ZY17a, AHG18, AAL19, AA14, AQHR+18, ATKh+17, APK+18, ABB+14, AKG13, AIB+16, ABW10, ABR13, AN15, AK14a, AYSZ14, AVAH18, BS15, BGAD12, BB14, BZD16a, BJ16, BS12, Bon19, BG+13, BBE+18, BBB16b, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLCZ10, DLK+16, DGIS12, Dur15, DMSD18, EBA71, FHH10a, FA14b, FIO15, FHZW18, GMRT+15, GPP+16, GLMS18, GMFPLC17, GH16, GBNM11, GLM+11, GSA18, GTSS19, HPC12, HZW17, Hod19, HWB10]. Key [HWB12, HL11, HYL+19, HLSY14, HT17C, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSMG18a, KDH15, KMTG12, KKG14, KV19b, KIH19, KP18, KI16, KDW+17, LLSL13, LLP+18, LLY06, LLI+10, LYY+10, LWS10, LDZ+14, LK+17, LPs10, LW13b, LZC14, LM14, LML+13, LLG19, MNP12, MHL18, MRT10, NAACL12, NCL13, Nos11, Nos14, OKD+17, OSAN19, PY19, RR16, RG10, RW13, RP10, SES+16, SP+10, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZZ15, SA15, SLXX16, SCBL16, SP+17, Svt10, TK19, TCS14, TLL12, Tso13, TKHK14, VV19, VN17, WWYZ11, WRP70, WM14, WDV18, WDKV19, WZM12a, WZM12b, WT10a, WTT12, WQQ+13, WXX+17, WX12, XW13, XCL13, XXY+19, YXIL19, XLC+19, XMHD13, XMH14, YTT11b, YC12, Yan14, YZZ+14, YHHS16, YLZ+18, YLLL+18, YN19, YYY13, YLZ+16, ZCQZ19, ZPZ+16, ZYGT17, ZYG18, ZWQ+11, ZZ11, ZHL+11, ZCC15, ZT16, ZGL+18a, ZXX+18]. Key [ZXWA18, ZCL+19, ZG10, ZZC15, Z1C17, ZY17b, ZWS+18, ZCZ+19, ZHT16, vV16, CLW16, OHJ10, XR17]. Key-Aggregate [CCT+14, PS17, GLB+18, CLW16]. Key-Agreement [WSS12, APK+18]. Key-Alternating [BKLS12]. Key-Based [Xio12]. key-correlations [Sar14]. key-delegation [JSG18a]. key-disclosure [ZZC17]. Key-Establishment [BCO13]. Key-Extraction [GPT14]. key-hash [KKG14]. Key-Insulated [FZT13, LDZ16, LH11c, HL11, LDZ+14, RG10, RW13, WWYZ11]. Key-Length [GT12]. Key-Length-Based [PRNC17]. Key-Policy [GZZ+13, GSW+16, HSMY12, RVH+16]. Keyed [KE19, MMS17b, YHHM18]. Keyed-Function [MMS17b]. KEYing [TW14, BCPV11, ABC+18, GJ19]. Keyless [PDM12, ZWX+18]. keyrings [MBB11]. Keys [ASN11, ABL+18, BF12, Bro17, CC10, HDWH12, LSWQ19, MS16, PS17, TW14, ZMW16, CMG+18, DMM10, HFH16, HL14,}
Lanczos [FYD+19]. Land [Sch18].
Landis [BBB16]. language [Ksi12].
Languages [MX13, Wat12]. LANs [FLH13].

Lapin [HKL+12]. Laptop [GPT14]. Large
[AN12, DM15, FNWL18, JLS12, JKHeY12, KCR11, KU12, LLSL19, LW16, LQD+16, MC11, SP13, And19, dCCSB+16, DEL19, EEAZ13, FXP12, GSN+16, LFZ+17, LBOX12, SR10, VSB+19, ZZKA17, ZVH14].
Large-Scale [DM15, JKHeY12, LLSL19, LQD+16, And19, dCCSB+16, DEL19, FXP12, GSN+16, SR10, ZZKA17, ZVH14].
LARK [DS11]. Laser
[DDR+16, FNP+15, Lii12]. Last
[Hof15, Hof16]. Latency
[AYS15, BCG+12b]. Latency-Optimized
[AYS15]. lateral [SCY15]. Latest [Ber17].
Latin [AB10a]. LatinCrypt [AB10a].
Lattice [ADM12, Ano11b, AYS15, BSJ15, EM12, EFGT18, FGM10, GCH+19, HPO+15, HKR+18, LNWZ19, LPO+17, MLO17, NDR+19, PG12, AAT16, AVAH18, BH19, Dra16, LLM+19, MGB19].
Lattice-Based [ADM12, Ano11b, AYS15, BSJ15, EM12, EFGT18, HPO+15, HKR+18, LNWZ19, LPO+17, MLO17, NDR+19, PG12, GCH+19, AAT16, LLM+19].
Lattices [Boy13, LYY+18a, LYX+19, Lau17, TH16, XXZ12, QZX15, Kre13, Tia15, XLWX16, yYqWqZC13]. launch [Zet14].
LAUP [BNNH19]. Laurent
[An15b, Ver17]. Law
[Bla12, SR14, Wu16, AOT13, ZHS10]. Layer
[HQY+18, LHM+15, PRGBSAC19, ZHX16, HQY+16, LKKL13, ZH+17]. Layered
[Bel19, BS14, GRL12, WWL+14, JCHS16, Tan18, ZC12]. Layering [YYK+17]. LBlock
[KDH13, MNP12]. LDGM [BBC+13]. Lead
[Arm19]. Leader [ADH19, TKM12]. leads
[An14a]. leak [BBG+17]. Leakage
[AV12, Bar16b, BKKV10, CBRZ19, CBL13, DCA18, DHB16, FSP12, GDLL18, HHH+13, HHP17, HHS18, IL15, Kom18, LTY16, LSQZ17, NTKG17, NTY12, Pan14, SGH15, TTH15, Wan18a, XYZ+12, YZLC12, YZ12, YCZY12, ZYTI13, ZWTM15, ZM16, ZMM17, ZY+19, ZYY19, ZY17a, ZY17b, ZYM18,
Leakage-Free [IL15, LSQZ17, TTH15].

Leakage-Resilience [NTY12].

Leakage-Resilient [AV12, FPS12, HHS18, LTZY15, Pan14, XZY+12, ZYT13, ZYM14, ZYT17a, ZYM18, ZY17a, HYL+19, LGL19, SGP+17, YLZ+16, ZWM14, ZCC15, ZYM19].

leakage-tolerating [ZWM14].

Leaking [BF11].

Leaks [CATB19, DLV16, JGP+18, Sav13a].

Learning [BNM17, Bar16b, CTC+15, CRS+18, GT12, Gir15, PDNH15, PNRC17, Zha12].

Length-Doubling [Zha12].

Lengths [BR19].

Lev [PHN+12].

LEO [RM18].

LESPP [WLZ+16].

Less [TKR14, GM13a, Kam16].

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

Level [AW17, A015a, CBC19, BKP13, BKJ12, CCW+10, DA10, FGRQ18, GLi12, HZS+19, HS18, JWJ+17, KPC+16, KGP12, MV16a, XZL+19, ZLDC15, ABB13, CGL16, MEFO12, RS17c, UUN13, VSI1, YT11a, B412].

Leveled [BGV14].

leveling [LY15].

Levels [HLCL11, LRW17].

Leveraging [DSM+16, GMDR19, HCM11, MV10, SKGY14, ZYGY18].

Lewis [Mar10a].

Lexicographic [ZAC17].

LFSR [HLZ12, MRT10, WGD18].

LFSRs [QGGL13].

Liability [Bra13].

Liars [Sch12b].

Liberation [Eya17].

Libgcrypt [DK16b, Bro17, Win17].

LiBrA [GMVV17].

Library [ACZ16, Bee17, BL12, FL12, KR18].

Licensing [EAAA19].

Life [HK13, SCS18, MK10, MK11, War11].

Lifecycle [Tan15a].

Lifetime [HSUS11].

Lifting [LSL12b].

Light [JEA+15, SWF+19, PCK19, SJ19, ARH+18a].

Light-Weight [SWF+19].

Lightning [Ran10].

Lightweight [ADM19, AMSL19, AMKA17, AAR12, BLN19, BCL19, BSS+13, BFMT16, BKL+13, BM11, CGCPDMG12, CWP12, CCF17, DS11, ESS12, EKP+13, FB+18, FQZF18, G11, G14+18, Gop19, GMV17, GMS14, HZW18, HCETPL+12, IS12, IOM12, KE19, MO12, MFG16, MPM+17, PCD14, SBS18, She14, YN19, ZYW+13, ZSY19, ZLY+19, ZS+19, AMN18, AAT18, AMKC19, AKKY17, BLL+19, BC16, BBBBB, BBR16b, CL11, DA18, FL+14, GH15, GTSS19, KD15, L15+16, MCN+18, MN12, M15, M+18, OSAN19, P18, PSO+13, SGJ+18, Tan12b, TG17, WLZ+16, WCF18, WWB14, WXZ+18, XX19, XHM14, YCT15, ZZY+19, ZSW+18a].

Like [BW16, ERL16, HP17, WJ19, AHG18, CGCS12, CGL13, HL19, KO16, LJ15, RJ16, RS14].

Lilliput [BFMT16].

Limitations [CK17, DR12].

Limited [DFK17, ZC17].

Limited-Use [DFK17].

Limits [AS16, GV14a, KS12].

Lindell [Ful10].

Line [FF12, LKBK19, YMWS11].

Linear [BC1+13, BW12, CGCS12, CMA14, EKP+13, FG12, HK14a, LGLL12, LJ15, LJ16, LW+16, WF16, YCL17, BBE14, Bul10a, DMD18, FES10, GMGCCC15, H10, HCC11, L11, Œ11, SA14].
Method
[AGW15, Ara13, BBB+16a, CZ19, FLH13, GLLSN12, GMNS15, HXHP17, HHS+15, KTM19, LyWZZ12, LP12, LD13, LBR12, MU12, OWHS12, PS14, PWS+19b, QF19, SAA15, SY15a, SXH+19, SP15a, SZDL14, USH19, WZXL12, WZCC18, WJ19, XNG+14, XNRRG15, YYO15, AGLW16, AIA+18a, ARG19, BLL+19, CSS+13, DJ19, Dra16, FVK17, JS18a, JDV16, Khi18, KHHH14, LLC10, LH11a, LT13, LT14b, LPZJ15, Mar12, MO14, PWW10, SH12, WT13, YWT+12, ZYGT17].

Methodology
[CBL13, Uto13, ZZKA17].

Methods
[BCEO19, BCEO20, BKBK14, Kob10, LW12, GMT+12, GSGM16, IAA+19, KSB+17, KVvE18, OO10, TMK11, TPKT12].

Metric
[YGFL15, DMWS12].

Metrics
[CVM14, PGLCX17, SSP19, BC18].

Mexico
[AB10a].

Meyer
[Bur11, Joh15].

MIBS
[CWZ19].

Microarchitectural
[MS18].

Microarchitecture
[ZBPF18].

Microcontroller
[GL12].

Microcontrollers
[LPO+17].

Microcosmic
[WWC+11].

Micropayment
[RM19].

microphones
[GSAV18].

Microprocessors
[SK12b].

Microsoft
[Lee15].

Mid
[AUMT16, KTM+18].

Mid-Air
[AUMT16, KTM+18].

Middle
[LL17, LJ18, LYO+18, LSG+19, LWKP12, LWFP12, LWKP14, vV16].

Middleware
[FGRQ18, FGR+17].

Middleware-Based
[FGRQ18].

Midway
[Car11].

Might
[Hur16].

Migration
[SHS12].

MIKEY
[TW14].

Military
[HK14b].

Miller
[Ano16a, Sch15a, LL11, LT14a, Led16, LR15].

million
[Sch16a].

Millionaire
[GKS17].

MILP
[CWZ19].

MILP-based
[CWZ19].

MIMETIC
[ACMP19].

Mind
[SNG+17, WP15].

mines
[KO16].

MinHash
[HWZP18].

MinHash-Based
[HWZP18].

Miniature
[HWS+19].

Minimal
[ARH+18b, BDH11, MZ17a, SBM15].

Minimalism
[DKS12].

Minimally
[AARJ12].

Minimization
[AH19].

Minimizing
[BCD+12].

Minimum
[KHPP16, DZS+12].

Mining
[BH15, BJ12, CZ19, DK16a, HDWH12, WZCC18, ZW15, Ano11a, ZMYB17].

Minus
[NXB13].

miracles
[MR14c].

Mirror
[Ano10a].

Misson
[Ano10a].

Mistakes
[DHB16].

misuse
[EBFK13].

Mitigate
[BKJP12, SS15].

Mitigating
[EPAG16, HRS16, SNG+17].

Mitigation
[BRS17, DHT+19, LGR14, DJL+12].

miTLS
[BFK16].

MitM
[TY16b].

mix
[WGJT10].

mix-networks
[WGJT10].

Mixed
[ST16].

ML
[Ksi12].

mMTC
[CML+18].

MNC
[IM16].

Mo
[RSB+17].

Mobile
[ATC17, BCD+12, CBYY16, FD11, GPT12, GdM16, HvS12, HFS+19, HLKL15, KP12, KKA15, LH12, LBC18, May15, NRZQ15, PH16, RX18, Sch15b, SFE10, She14, SS15, SAA12b, WPZM16, WT10b, XHH12, XNKG15, XHC+12, YHL16, Yon11, ZLDD12, Aia15, AAZ+16, ALL+18, CLP+13b, CTL12, CCSV11, CWXW16, CTL13, CRS13, uHAN+18, FHH10a, FA14b, FHZW18, FH+10, GM16a, GH16, HZWW17, HZWZ18, HL14, IAA+19, IB11, Kem11, KKA14, KKM+13, KKM+14, KKG14, KSB+17, KS19, LH11a, LZD+19, LH13, MLH18, ODK+17, OYHSB14, Par12b, SSA18, SLL+19, SSN15, hSZZ15, SM19b, SCR19b, SASF11, SKB+17, SHBC19, TZTC16, TKHK14, WSC14, WT10a, YHHM18, YNX+16, ZLDD14, ZDW+16, ZC12, ACMP19, MBB+13, SLL10].

mobile-cloud
[KKM+13].

mobiles
[GCS+11].

Mobility
[CLH13, LNK+18a, CL11, GH16, LH11b, MYYR13, THA+13, YLS12, ZSI11].

Modal
[HFS+19, BOP14, GBC19, SCFB15].

Modality
[SSP19].

Mode
[HZ11, Mar10c, PAF18, gWpNyY+14, WLC12, ZHZ+19, Fay16].

Model
multi-cloud [CFVP16, SWW+16].
multi-crypto-processor [BGG+13].
multi-dimensional [LZWZ19].
Multi-Directional [JS18a].
Multi-Domain [SAM+18, IG11, QMC17]. multi-exponentiation [WSQ+16].
Multi-Factor [PSSK19, HC12, CLP+13b, DRN16].
Multi-fault [BEM16]. multi-flow [LWY12].
multi-gateway [WK+17].
multi-generation [CJX+19]. multi-hop [LCT+14].
Multi-instance [BRT12].
Multi-Keyword [CWL+14, XWSW16, OSSK16, DDY+19, GZS+18, LK+14, YQZ+19]. multi-lateral [SCY15]. multi-layered [JCHS16].
Multi-Level [ZLDC15, MEO12].
Multi-linear [BBEPT14]. Multi-Modal [HFS+19, BOP14, GBC19, SCFB15].
Multi-Party [ABL+18, KMO14, TYM+17, GVW12, LyWSZ10, DGL19, XLSZ16].
Multi-Proxy [ASS15, GJZ17].
Multi-scale [DLGT19, CG12b]. multi-scroll [GMOGCC15].
Multi-Secret [HYS11, ZC13, CW14a, HCC11, HLC12].
Multi-Segment [WOLP15]. multi-server [CLHJ13, FHZW18, HL14, ISC+16, LXMW12, LH13, SSS11, TLL12, XHM14, YN19, YY13]. Multi-Signature [ASS15].
multibit [KPS10]. Multicast [CC14, PSM+18, BAL10, DMM10, HGWY11, LTT10, NACL12]. Multicore [RJV+18, SHC+16]. Multicoupon [HIDFGPC15]. multidesignated [AYSZ14].
Multidevice [DPCM16]. Multidimension [AJA16]. Multidimensional [Her10, WWBC14, HMCK12, JLC18].
Multifactor [MMY12, KS19].
Multigigabit [PP10b]. multihop [ADF12].
Multikey [LAT17]. Multilayer [NXH17]. Multilevel [FMS12b, HF14a, NSA15, SERF12].
multilinear [CJL16]. Multimedia [BCG10, NSA15, PMZ13, PZPS15, PYM+15, WLY+15, ZW15, Zha15b, ZSA12, GJ18, HM10, HWYW14, HPL+19, LLLK10, WN13, XWSZ16, TW14].
Multimodal [GM16a, Sar18a, ACM19, AHM18, ATI+10, MHT+13]. MultiObjective [ZAC17].
Multipartite [HR13].
Multi-party [BDZ11, CCL+13, Fri10b, ADMM16, BHH19, LDDAM12]. Multipath [LH12, OPHC16].
Multiple [DSB15, Dn12a, FR16, HWZP18, HZSL05, KBL11, LCC+15b, LQ+16, M17a, NDC+13, SY14, SC10, SKS+18, Sta12, WWL+14, XNP+18, GJ18, GZS+18, LWZG10, LCC+15a, LCC17, MN14, PZL+19, RWZ13, TKHK14, YQZ+19, YJ18].
Multiple-Layered [WWL14].
Multiple-Parameter [NDC+13].
Multiple-Precision [HZS15, MN14].
Multiple-Secret [SC10]. Multiplication [AR+15a, AK14b, CMO+16, GL19, HL17, LNL19, NR15, SK12b, YTS12, AAT16, DGK18, Khl18, SKH15, SF12].
Multiplicative [RMER19, KHH14].
multiplicity [MH14]. Multipliers [AR+15b, GT19]. Multireceiver [FFH10b].
multisecret [FGPM12]. multiserver [CNF+18].
Multiset [Fa19, MST17].
Multispectral [DGM18]. Multistream [WX+17]. Multi-threaded [TL+17].
Multitone [GL10]. Multivariate [CLND19, DP17, ST16, YT16, YL17, YDH15].
multiview [WSS+19]. multewatermarking [WL12]. multiwavelet [PWW10].
Music [NTK17, Wes16]. musical
ZWQ+11, ZBR11, ZCLL14, ZTZ16, ZLDD14, ZHH+17, ZX11, LNK+18a.
Neural [CHS+18, RSX18, SKS+18, YZLC12, EEAZ13, HZW19, HW19, KMG17].
Neuroscience [BSR+14, JW14].
Neutrality [KH10]. Neutrality-Based [KH10].
Neutrosophic [JS18b]. Nevada [IEE10]. NEVER [Bai12].
News [And19, Edw14, Edw17, Lam13, Sav13a, Sav15, Sav16]. Next [HEP+11, MR14a, MJGS12, Aia15, ACD+15].
Next-Generation [MR14a]. NFC [LY14, Mic16].
NFSR [WG18]. Niederreiter [HC17, MVVR12].
Nievergelt [Ter11]. Nine [Mac12, LYHH14].
NIST [MMKP16, ZSH19]. NIZK [Pas13a].
NIZKCTF [MBC+18]. NIZKs [CKLM13].
NLM [OPS14]. NN [ZZC17, ZHT16]. NORM [WDDW12, Wu16, KHHH14, MPJ+16].
Non- [Sto12]. Node [AA19, ARWK19, NKR+14, OKG+12, GM13b, LC17, PX13, SAAB10].
Non-Capture [NYR+14]. Nodes [VGA15, ZYL+10]. Noise [ASN11, Fyo19, LKBK19, YMA17, BCND19, QLZ19, ZHH+17].
Noised [JLS12]. Noisy [ASN12, HZW+14]. Non [AH19, AS17, AMH+16, BCL19, BCI+13, CG14a, CPS16, DJL+12, DPW18, EKP+13, FHKP17, FMNV14, GL19, GZX19, HWS+19, HKB14, JSA17, KTT12, TK18, LG15, MAFH13, MSA12, OOR+14, Pas13a, QJC+18, RM18, SM18, WgMW12, XZL+19, YNQ15, YKDL12, ZLDD12, AY14a, AM19, BS15, CS11, ESR14, GIJ+12, Kre13, Lan11, LJY16, LP11, MSA13, SES+16, SXL16, VBC+15, XSWC10, Yan14, Kh18]. Non- [AH19].
Non-abelian [HWS+19]. non-adjacent [Kre13, Kh18]. non-associative [BS15].
Non-Black-Box [CPS16]. Non-blind [HKB14, RMG18]. Non-Boolean [AS17].
non-browser [GIJ+12]. non-compliant [Lan11]. Non-contextual [SV14].
Non-Coprime [GL19].
non-cryptographic [AY14a, ESRI14].
non-dynamic [SES+16]. Non-interactive [BCI+13, LK18, Pas13a, LJY16, Yan14].
Non-interference [BBCL19].
Non-intrusive [MFH13]. non-iterative [SXL16]. Non-Linear [EKP+13].
Non-Malleability [KTT12].
Non-Malleable [DPW18, MSas12, CG14a, FMNV14, OOR+14, Pas13a, LP11, MSas13].
Non-medical [AM19]. Non-negotiable [DL1+12].
Non-Perfect [FHK17].
Non-Repudiation [LLG15, VBC+15].
Non-stationary [ZLDD12]. Non-tamper [WgMW12].
Non-transferable [GZX19].
Non-uniform [QJC+18]. Non-uniformly [YKDL12]. Non-Volatile [AMH+16, JSA17, RM18, SM18, XZL+19, YNQ15, CS11].
Nonce [BZD+16b, KMS19, BH19].
Nonce-Based [KMZ19].
Nonce-Disrespecting [BZD+16b].
NonInteractive [KOS16, GOS12, MBC+18].
Nonlinear [CCM+15, KW14, LW13a, Lid12].
Nonlinearity [MM17b]. Nonlinearly [Fyo19].
Nonvolatile [ZH+19]. Norm [FHS13]. Normal [RMER19, TY16a].
Normalizability [KLY+12, SJ12].
Normalizability [YJFL15]. Normal [Low12].
Note [HYS11, Gal13, GR19b, Hwa11, Lim11].
nothing [Cer15]. Notifications [LBC18].
Notions [KFOS12, SNJ1, Sar12, BP11].
Novel [CLHC12, DCM18, KRKH13, LYY+18a, LXY+19, LLG15, LyWZZ12, LH11c, MJGS12, MCS+15, SSK16, SWM+10, SC12, VN16, WHZ12, WZXL12, YZZ+12, YLS19, Ye14, ZMM17, BOB13, BSBG19, BBB19, CH19, DDFR13, GPLZ13, HZW19, HCCC11, JXL15, LCM11, LMC11, LH13, LWW+10, LML+13, MRT10, NZL+15,
PZBF18, SAM^+19b, SCR19b, SYW17, Sun16, TG17, jT12b, WYL13, WMXZ19, WGZ^+12, YWT^+12, ZYGT17, ZBR11.
November [Kap11, LCK11, Yan11]. NSA [ABJ13, Ano13d, AHS13, Bud16, Men13b, Sta13, Tox14]. NSDG [SSPC12]. NTOW [BS15]. NTRU [AA19, CJL16, vV16]. NTRUEncrypt [DWZ18, KY10]. NTRUSign [Wan10]. NTT [MCDB12]. NTT-Based [MCDB12]. Nuclear [Hel17]. Number [ADI11, BKLS12, CDK^+10, DSLB18, DFE^+19, Fok12, Ham17, KA18, LTKP16, LCLW17, MFG16, NIS12, NNAM10, Sha10, Shp03, SRAA17, SRK^+17, SRK^+18, WJ19, CFY^+10, CP13, LLP^+18, LGKY10, Lim11, MS12a, MRT10, SH11, Si11, XSWC10, Gre19b].

O [CDD13]. Obfuscated [LMS16, OWHS12, ZM16]. Obfuscating [BGI^+10, BGI^+12]. Obfuscation [ABCL17, AS16, AWS17, BBC^+14, BCKP17, BV18, BCP14b, BR14, C15b, DRS16, EMW14, FKOV15, GGH14, GGH^+16a, GGH17, MH14, ZL19, BBGT12, CFVP16, GGH^+16b, OSSK16]. Obfuscation-Based [ABCL17].
Obfuscator [FDY^+19]. Obfuscators [PSD15]. ObfusMem [AWSS17]. Object [BCK17, SSSA18]. Objects [LLY^+18, ZCWS15, Bel18b, HST14, SMBA10, WW13]. Oblivious [DN12, WCL^+18, CGH11, GLM^+19, RYF^+13]. Obscure [GLM^+19].
Obscuring [VGL14]. obscuring [Edw14]. observation [WHY^+12]. Observations [CJZ13, HCL^+14]. Obtaining [BB10].
Occasion [Nac12, RNQ16]. Ocean [FG19]. October [CGB^+10, IEE10, IEE11b].

Offs [ASBdS16, BS14, GPR^+19, SR10]. offsets [YQH12]. Okamoto [TFS19]. Old [Che17, FREP17, GV13]. On-Cloud [LGL17, BAB^+13]. On-cloud [EAAMA19].
On-demand [KKJ^+16]. On-Line [FFL12]. On-siteDriverID [SGGCR^+16].
On-the-fly [PS14]. One [BHT18, CBX19, CRH17, CPS16, DMM14, DCAT12, FD11, HP14, HG12, Mat14, NA10a, Par18, PC16, TYM^+17, WCXZ17, XW12, XXYX11, XZLW15, Yon12, BM15, FHH10a, GZL13, HRV10, JK19, Kom18, LP11, LW10, LW13b, LML^+13, Nor17, RK11, Rus15, SM10a, SPK17, SCBL16, TCS14, ZQWZ10].
One-Dimensional [XXYX11]. One-Round [TYM^+17, XZLW15, Yon12, XW12, JK19, TCS14]. One-Sided [HP14].
One-Time [NA10a, DCAT12, Par18, BM15, FHH10a, GPLZ13, LW10, LW13b, LML^+13, SPK17].
One-Time-Password [FD11]. One-Way [BHT18, CBX19, CPS16, DMM14, Mat14, WCXZ17, HRV10, Kom18, LP11, RK11, SCBL16]. Onion [KZG10]. Online [KZG10]. Online [KZG10].
Online [KZG10]. Online/Offline [KZG10]. Only [BB10, YNR12b, YLW13, Bul10a, KMTG12].
KA17, Sar11]. Open [SS19, ABF+14, MHV15, Pow14, Win17, ZWQ+11].
open-source [ABF+14, Pow14]. OpenCL [ABDP15]. Opening
[GDCC16, LZY12a, LLH18, LZY14]. Openings [SP13]. openness [Bia12].
OpenPGP [MBB11]. OpenStack
[CSL+14]. Operable [BCF16]. Operand [MSI18]. Operating
[KMP+11, CDA14, MNNW15]. Operation
[GLLSN12, JB11, SBS18, ALL+18, Fay16, Lin14a, SKK10, WAZ+12]. Operational
[CRE+12, CM11, RZ19]. Operations
[Cil11, SEY14, SZHY19, YWW10, KKJ+16, LZY+16]. operative [HFCR13].
Opportunistic [AA19]. Opportunities
[Lau17, Mci10b]. opportunity [Sch11]. Optical [PRGBSAC19]. Optimal
[AS17, CK17, DSSDW14, DSSDW17, GJJ18, GM16b, HRB13, PPS12b, QJC+18, TX16, WMU14, Cha13a, CXWT19, DDD14, MCL+19, PPTT15, SYV19].
Optimality [MM17a, SDM+12]. Optimally
[DSMM14, CT12]. Optimally-Fair
[DSMM14]. Optimised [CMO+16].
Optimising [EVP10]. Optimistic
[WASA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12, GCSÁddp11, KHF10, PTK14, RYF+13, ZSM18, sCR19a]. Optimizations [ZAG19].
Optimized
[ARH+18a, AYS16, EKB+16, GAB19, HGT15, LNL+19, MBF+13, MBR15, JS18a].
Optimizing [DWZ18, ZSM18]. Optimum
[Oba11, YFF12]. Optional [PC16].
OR-Proof [FSX12c]. Oracle
[CBJX19, GLM+16, HKT11]. Oracles
[FZT14, FSX12a, GSW+16, XLQ09, XQL11, YS12, YKC+11, YLA+13, ZYM18, LLY15, RG10, SYL13, WWYY11, YFK+12].
ORAM [RM18]. Order
[DCA18, FYD+19, KS12, LFX+18, LWP12, PRC12, YKKL12, ZDL12, ZSW+12, ZBP18, AKY13, BKR19, LW13a, LKY+16, LWP14, gWpNyY+14, YL11].
Order-Hiding [DCA18]. Order-Preserving [KS12, YKL12, YL11]. order-revealing [BKR19]. ordered
[AAL19]. organisational [Bia15a]. Organization [RSGG15]. Orientated
[TJZIF12]. Oriented
[NNAM10, Rog16, RSGG15, WW12, NML19, SK18, WZM12a, WZM12b]. Origins [SZJG19]. Orthogonal
[FYD+19, tWmC12, XNP+18]. Oscillator
[YKBS10]. OSN [BCF16, BBDP16]. OSNs
[SZX18, PZPS15]. other [BDK16, Smi15b].
OTS [He113]. outliers [Sch12b]. Outline
[Hur16]. Output [DK16b, GST12, NIS15, NR12, Uto13, PBCC14]. Outputs
[SNCK18]. Outright [ABJ13]. outsourced
[FRS+16, LLC+15, LHL+18, LQD+16, PD14, RDZ+16, XLP+18, YMA17, YMC+17, DFJ+10, FS18, HKA19, HMCK12, LCL+15, LCO+16, LWJ+17, QZD16, YSQM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+14, LLSL19, LJWY18, OSNZ19, LWW+19, SKB+17, SWW+16, XMY+17]. outwitted [Car11, Fag17].
Over-the-Air [VGB18, ZWX+18]. Overcoming [BKKV10, DY13]. Overhead
[AWS17, Bia10, CCW+10, GHS12, RM18, ZJ11, CXWT19, RS17c]. Overheads
[TSB18]. Overlay [CHS15, MJS13].
Overview [Bla16]. overview
[AA14, BDP+12]. owner [Kum10, NA14, Zha15a]. owner [ZZC17].
owners [GZS+18, YQZ+19]. Ownership
[AMS19, FMTR12, RR11, HWYW14, KH18]. Oxford [Che11, Wes16]. Ozarow
[ADG16].
Packet-Level [FGRQ18].


Pair [Lin15, SLXX16]. Pairing [Bon12, CMRH17, CWWL12, CST+17, KZG10, KHPP16, LKBK19, LSQ18a, LGPRH14, Men13a, MST18, WZCH19, YTS12, YY17b, ZM18, BP18, Con12, FK19, KSH18a, KSH18b, LL16a, LR15, MSGCDPS18, YT11b, ZY17b].

Pairing-Based [Bon12, CMRH17, CST+17, KZG10, LGPRH14, Men13a, MST18, YTS12, Con12, KSH18a, KSH18b, MSGCDPS18].

Pairing-Free [LSQ18a, WZCH19, YY17b, ZM18, LL16a, YT11b]. pairing-friendly [BP18, FK19].


Paper [TSH17, Ano16i, SK14, YFK+12]. Papers [Ano16b, Ano16c, Ano16j, CWZL13, LW13a, XW13, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. Paradigm [ABGR13, BSV12, Mau12, MP12, TAP19, Gop19, KKK11, WQZ+13]. Parallel [AAH+19, App14, ARM15b, BBM15, BTK15, CGB+10, GP17, HW19, LY16, LB13, MCD12, MC11, NdMMW16, NR15, SMD11, YE12, ZGL+18b, CST16, FLYL16a, FLYL16b, MRT10, RG10, RWZ13, WWYZ11]. parallelism [SD17].

Parameter [NDC+13, MZ15]. parameterized [GR19b]. Parameters [HRB13, MBF18, LZX19]. parametric [Bull10a]. Paranoia [Cor14a]. Parity [Raz19].

Park [Ano11c, Bri11, Cop96, Cop10a, Cop10b, GMT+12, GW14, McK10, McK11, McK12, Pca11, Sim10, Smi11a, Smi15b, Smi15a, Bai12]. Parsing [MHW+19]. Part [BLM18, VM14, BD15, Bar16a, BBC19]. Partial [CBJX19, DLV16, GFBF12, HFW+19, LG12, SGS14, TK19, WDDW12, Bax14, EBAÇ17]. Partial-Shape [HFW+19]. Partially [KB10, XZP+19]. participants [KSU13, WTT12]. participating [CH10].

[Bon12]. **Patching** [BCFK15]. **Patchwork** [NXH+17, XNG+14]. **Patchwork-Based** [NXH+17, XNG+14]. **Path** [DSM+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13]. **Patient** [ZLDC15, ZVG16]. **Patient-Centric** [ZVG16]. **Pattern** [DCA18, PSSK19, YTF+18, ATKH+17, DA18, uHAN+18, KPS10, OSSK16, PTT+15]. **Pattern-Based** [PSSK19]. **Patterns** [Ano16f, BPSD17, TSH17, WOLP15, BDK11, BCGS16, LHM13, NML19, SPK17]. **PAWN** [JNUH17]. **Pay** [EAAA19, CCSW11]. **Pay-per-use** [EAAA19]. **pay-TV** [CCSW11]. **Payload** [CHHW12, AZH11, JNUH17, JKAU19]. **payload-based** [JNUH17, JKAU19]. **Payment** [DG15, SYC+17, CHH+13, SYW17]. **Payments** [RBHP15, MPJ+16]. **PC** [YE12]. **PC-Based** [YE12]. **PCie** [BMM13b]. **PCM** [LY15]. **PCM-based** [LY15]. **PCPs** [GPT14, GPP+16]. **PDF** [Con17]. **PDGC** [CGV+10]. **PEA** [ZGL+18b]. **Peaks** [TC10]. **pearl** [Rus15]. **Pecherskii** [Kuz11]. **PEDCKS** [XLC+19]. **peer** [LLY06, NCCG13, ZYW+13]. **peer-to-peer** [NCCG13, ZYW+13]. **PEKS** [ZQD16]. **People** [Söd13]. **Per-File** [DMS+16]. **Per-session** [DGMT19]. **Perceived** [CSW12]. **perceptions** [GMMJ11]. **Perceptive** [DCM18, MK11]. **PEREA** [ATK11]. **Perfect** [Pas13a, Sch13, C215a, FHKP17, LLC10, Lew10, XW12]. **perfectly** [ADG16]. **Performance** [Alo12, AW15, AW17, AB15, ABPP16, BM18, CRS+18, CGL+12, CCG10, DHT+19, DLK+16, DGFIH18, DBPS12, EGG+12, ESR14, FPBG14, GLG12, GRP+19, GCS+13, HKL+14, KHKG19, KAK18, LCK11, LGP19, LPO+17, MHC12, SKV12, SSP19, TPKT12, WRP70, WDDW12, Xio12, YWF18, ZLDD12, vRDSH17, ABDP15, AHG18, BGE+18, CLB19, FHL19, FLYL16a, GCVR17, HURU11, JLC18, MCL+19, MMS+17a, MS13c, PÁBC+19, ZLDD14]. **performances** [CBL10]. **Performed** [Ano17d]. **Perils** [FMA+19]. **perimeter** [Cal13]. **periodic** [KPS10]. **periodical** [CLSW12]. **Permission** [VN16]. **Permutation** [LJ16, NIS15, Bar19, GMSW14, LC14]. **Permutation-Based** [NIS15, LC14]. **Permutations** [ARH+18b, ARH+18a, BKL12, Saa19, Mat14]. **Persistent** [CSY18, SXH+19, TYK+12, ALL+18, KV19b, PKA15]. **person** [PN10]. **person-centric** [PN10]. **Personal** [ESS15, LZY+13, Rao17, RSD19, ALL+18, BC18, MV011, SYV19, WHZ+19, LHL15]. **Personalized** [FSA+16, VGA19, AT10]. **Personnel** [YTH17]. **Perspective** [ADH19, KMY18, MSM18a, RSGG15, Sir16, Wag16, Bon19, JW14, Suc12, ZWT13]. **Perspectives** [PMG+19b, Sen17, SPM+13]. **Perturbation** [XZ18]. **Pervasive** [ACAT+15, BCG+12b, FHM+10, YD17, JSM+18, PKA15, SCY15, Tan12b, YWK+10a]. **Petri** [PS14]. **PGP** [RAZ15]. **Pharmaceutical** [YSF+18]. **Phase** [KM18, LD13, NBZP17, ZWT13, ZHH+17]. **Phase-change** [ZWT13]. **Phase-Encrypted** [NBZP17]. **philosophy** [Mat19]. **phishing** [HAK19]. **Phone** [Mur16, SAA12b, KRM+10, LTC+15a]. **photo** [CLY18, OF12]. **photo-to-caricature** [CLY18]. **Photographic** [YSC+15]. **Photographs** [TCMLN19]. **Photorealistic** [MHW+19]. **photos** [Pow14]. **Phrases** [WBC+10]. **Physical** [BEH+18, CK17, GPT14, GPP+16, HQY+18, HH+13, PRGSS19, SMOP15, GHD19, HQY+16, HZW18, KSA16, QMC17, VCK+12, WW13, YD17, ZHH+17]. **Physical-Layer** [HQY+18, HQY+16, ZHH+17]. **physicist** [Dya19]. **physio** [HT11]. **physio-behavioral** [HT11]. **Pi** [MR10, EHKS19]. **Pi-Calculus** [MR10].

PPM [XHC+12]. PQCrypto [Sen10, Yan11]. Practical

[AB17, ATK11, AG18, BHH+15, BSA+19, BDF11, CLSW12, CGH17, Cra11, DZY10, EA12, FPS12, FLYL16a, FSK10, GDLL18, HSA14, HPO+15, HKR+18, LW16, LJYW18, MFB18, OPS14, PPTT15, PDJ+19, RWZ13, TSH17, WHLH16, WX13, YZLC12, ZYD10, ZLW+17, AMS+10, BS13a, BZH+16b, CFN+14, Con17, JSDK+16, LFZ+17, PHGR16, WR15, YJC18, YKGGK13, ZSW16].

practicality [NDNR13, Zha15a]. Practice [ABD+15, BMNH17, CDFZ16, FM12, PWVT12, ROG16, RBHP15, RST15a, RST15b, SN10, SAKM16, ABP+19, NS10, Sta11b]. Practice-Oriented [ROG16].

practices [Tay19]. Practitioners [PP10a]. Pre [ARM15a, TX16, YWL+17, YHHS16]. Pre-Computation [ARM15a, TX16].

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

precaution [AQRH+18]. Precise [MC19, HYF18]. Precision [EZW18, HZLS05, MN14, SK12b].

Precomputation [GKM16, Bon19]. Predicate [KHP16, LNZW19, NMS14, YKNS12, ZYT13, FH13, HFT16].

Predictability [DK16b]. prediction [CSS+13]. Predictive [TBCB15].

Predictors [EPAG16]. Predistribution [YM16].

Prefix [Yao19c, YYW19].


Preservation [BCP14a, LLG15, VSV15, YJSL18, Yon11, FZZ+12, LVRY10, TML152]. preserve [BAG12]. preserved [SWW+17].


Primitive [App15, MCS15]. Primitives [BSJ15, CK17, EAA12, HLN+10, SP15b, ABDP15, BSR+14, Gor10, WSL+19].


print [KPS10, PKS18]. print-cam [PKS18]. print-scan [PKS10].

Printer [EMW14, FNP+15]. Prior [NA10a].

Priority [LMS16, Bia12]. Prisoners [Mac14, GSGM16, Keib15]. PriSTE [CXX+19]. Privacy [AKM+11, AKKY17, ABCL17, Ano19a, ABR13, ALL+18, ACM12, ABHC+16, BN14, BCF16, BAA18, BJL16,
Privacy-assured [WMYR16].
Privacy-Aware [BC16, BBDP16, BLV17, BS13b, CVM14, CWL+14, DCA19, DTE17, ESS15, EKOS19, FGR+17, Fei19, Fri13, GZZ+13, HSMY12, HBC13, HXH17, HXC+11, HK18, IEE15, JK12, JLX+19, JM10b, KKK+18a, KLK+19, KCC17, Kn17, KS12, KH18, LMGC17, LSBN14, LLG15, LCDP15, LNXY15, LSY+16, LQD+16, MYYR13, MJS+19, MV18, Mor19b, MTM18, NSMS14, PD14, PSS+13, PPRT12, PZPS15, PSD15, Pet12, PH16, RVH+16, RSR+19, RCP+18, RWLL14, Roh19, RHLK18, RBHP15, SS17a, SG12, Set16, SZDL14, SZZT18, VFFHF19, WPZM16, WZCC18, ZHW+16, ZLDC15, ZTL15, AMK+11, AKKY17, AL+18, JLX+19, KH18, LCP15, WMC17, ZOSZ17, APMC13, BC16, BBPD16, BLV17, CCMC19, DZC16, FMA+18, GAI+18, HSH11, HKA19, JLC18, LZD+18, LZY+18, MGB19, PZBF18, QLZ19, RR16, SY+17, SMS+16, Tan12b, WZC16, Wan18b, YY+19, ZWY+13].
Privacy-Protecting [Roh19, CD16a].
Privacy-supporting [ABR13].
Private [BBKL19, BKLS18, GM13a, Jia14a, LSQX19, MV19, QZL+16b, RCBK19, RDK19, Sia12, WC+18, Yek10, ZMW16, ZXYL16, BHH19, DLIL5, HJM+11, HYF18, IK15, WR15, vV16].
Privacy-based [HLC16].
probabilities [Kam19].
Probability [DF11, HLC16].
Problem [AH19, Dun12a, Fra15, GTT11, KRDH13, KPC+11, Lai14, RBS+17, CJL16, SK14, TPL16, WS14].
Problems [AH19, Dun12a, Fra15, GTT11, KRDH13, KPC+11, Lai14, RBS+17, CJL16, SK14, TPL16, WS14].
Procedure [CS14, OS12].
Proceedings [LCK11, TT18, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Dun12b, FBM12, Gil10, GG10, HWG10, IEE10, IEE11b, IEE13, LW11a, LTL11, PLe10, P12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLIC10, IEE11a, Kia11, Lin14b, Sah13].
process [CWZL13]. **Processing** [JGP+18, SAKM16, SZHY19, TKMZ13, VKP17, BKV13, HKW+15, MS1+3b, PRZB+12, WS14].

**Processor** [BH15, CLF+17, HKL+14, LB13, MBR+15, RJV+18, YL16, YS15, ABDP15, BAB+13, BGG+13, KSH18b, SSPL+13, TAr10, KSH18a]. **Processors** [GBBF12, Gue16, SJK18, RYF+13].

PrODACT [FY+19]. **producer** [CHL19].

**Product** [ADM12, CC+15, OT12, YKNS12, And13b, Cha13b, DDM17, YI17].

productivity [Tay19]. **Products** [LMG+18, RS10].

Professional [HGOZ19, STC11]. **Profiled** [Bar16b].

Profiles [BCF16]. **Profiling** [DP12]. **Profit** [APPV15].

Program [MI+17b, TLZ+17, Wall18, CLZ+17, DDM18, GGH+16b, MFH13]. **Programmability** [HP18].

Programmable [APPP16, CLF+17, Ang16, EAB+19].

Programming [Bee17, BCEM15, LLS19, SY14, ASVE13, GLMS18, HL10].

Programs [BGI10, BGI+12, CL16].

Progress [AB10a, BL10, BC11, GG10].

Progressive [SA16a]. **Prohibition** [Hor19].

Project [SPG+19, Aoi14c, Ron11], ACK+10, SS10c, Wil18].

Project-Based [SPG+19]. **projective** [CZ15a].

Prominent [ABJ13]. **Promise** [Pau10, PWVT12].

promised [HS11]. **Proof** [BDSG+13, Bla12, CLZC12a, CLZC14, FSX12c, GKG19, Kuz11, LYY+18a, LXY+19, LW12, LYY+16, NLY15, SR14, Ste15a, ZMZ17, HLS18, Mon13, PPTT15, VBC+15, WHJ17, ZCQZ19].

**Proof-of-Concept** [GKG19].

**Proof-of-Knowledge** [LY+16]. **Proofs** [BBD19, BK12, BCG12, BGB12, BCI+13, BDSG+13, CLZC12b, DKL+19, IW14, LNZ+13, Mau12, NTY12, RB17, Sav13b, WPZM16, AGHP14, KPP16, KKK+16, Li10].

Propagate [GWM16]. **Propagation** [SKS+18, WWC+11, YZLC12, CWXW16].

Properties [CCK12, CCCK16, DQFL12, FY11, HIJ+19, JS18b, JR13, KU12, Sch12c, CLCZ10, SAM+19b, WT13]. **Property** [HIJ+19, HEC+12, PR12, Rja12, YWM19, Bar19].

Proportions [Ber12]. **Propose** [BFM16]. **proposed** [Bax14, HWB10].

Protect [CTC+15, CKHP19, YMC+17, BVIB12, CDF+10, dCCSM+12]. **Protected** [BDGH15, SG15, AGBR19]. **Protecting** [BCP14a, GSFT16, LLFY19, Mar10b, RCP+18, Roh19, SCY15, Wat14b, ATKH+17, CD16a, CXX+19, CDA14, FLYL16b].

Protection [AIM+19, BHC19, CDD13, DCA19, EAAAA19, GST12, GPR+19, HXHP17, JP19, Lop12, NGanH16, NDG+17, RR11, SEY14, SJ12, ZWWW17, AIA+18b, ATI+10, HLYS14, HPL+19, KKM+13, Ksi12, LZ11, LWYM16, LVRY10, RS17c, TLL13, YWT+12, ZZY+19].

**protection-key** [HLYS14]. **Protocol** [ADSH18, BL12, BC14, BCM+15, BNH19, BSSV12, BK16, BBK19, CC14, CCM17, DCA19, FLH13, FHOJRH18, FMTR12, Fra16, GI12, HvS12, HC12, HL10a, HCP16, HETPL+12, HKL+12, JTZ+16, JHW+19, KMZS19, KMO14, LNZ+13, LCCJ13, LNX15, LYY+16, MBC15, MR10, PSS+13, SBS+12, SG16, SS15, TWC18, TYK+12, WT10b, XJR+17, YS12, YWF18, YLSZ19, YWZ+12, ZZ+11, ZSY19, AATM18, AMK19, AQY+18, AKG13, AIB+16, AIKC18, AN15, BDM18, BGAD12, CSD18, CWSW11, CCMB19, CJP15, DKL+16, DDL15, EA12, EBA17, FA14b, FIO15, GMSW14, GH15, Gop19, GLM+11, HPCI12, HWB12, HL14, IC17, IOV+18, JK19, JKL+16, JXZ15, Kim11, KO16, LLS13, LDDM12, LKK13, IWS10, LXMW12, LZD+19, LEW19, LY14, LML+13, NCL13, NLY12, NML19, OHJ10, Par12b, SSA18, SPLHC14, SB17, SGJ+18, SWW+16, SSS11, SSPL+13, TG17, THA+13, Tso13].

**protocol** [TKKH14, VS11, WM17, WYZ+17, Wan18b, WCFW18, WDZ19, WDV18, WZM12a, WZM12b, WLS14, WMYR16, WT10a, WTT12, WC18].
XCL13, XHM14, YC12, YZZ+14, YYK+19, YMM13, YN19, ZWQ+11, ZTZ16, ZYC+17, ZXW+18, ZXWA18, ZG10, ZZZ15, ZX11, BOB13, CJP12, LFGCGCRP14, Ste15b].

Protocols [ADH19, AP13, ABHC+16, BMP12, BSBB19, CCK12, CCCK16, CMRH17, CCF17, CZCD18, CDD15, CDDD19, CDDD20, Con10, CM11, EFGT18, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KL08, KOS16, LY16, LWL+17, MV19, MS16, MT12, Mur16, NVR+14, NSMS14, PS14, RB17, SBS+12, SBS18, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13d, AKS19, ACC+13, ACM12, BJ10a, BK19, CML+18, CR10, CLCZ10, DGNJ14, FTV+10, GBNM11, GLR13, HSH11, HLS18, Ham12, HDPC13, HZWW17, HST14, HWB10, KJN+16, KSU13, KKK+16, LDC13, LLY06, LKKL13, MN10, NR11, Nos11, Nos14, SD10, WU10, WM14, YSL+10].

Prototype [Bar16b]. Prototyping [KPC+16]. Provably [BCL19, CC14, EKB+16, Rog16, YJS18, YMS10, YY19, ZX11, ZPXX17, FA14a, HRS13, LHH11, SYWX19, WB12, XCL13].

Provably [BCGAPM12, BCM12, BCM13, BCGS16, BHJP14, FHH10a, GLL+18, IL15, LLH11, LDZ+14, LL16b, ODK+17, PSM17, RMZW19, WMS+12, XLQ09, XJWW13, YC12, YZZ+14, ZG10, ABBD13, FIO15, KCS+18, KLW+17, LZD+19, LWK+19, SM10c, SX16, XWWC14].


Proximity [IW14, ARL13, Alp18]. proximity-based [ARL13]. Proxy [ASS15, DHT+19, GSW+16, GJJ15, GJZ17, GZXA19, HG14, HZ15, K12, LK18, LSL15, LAL+15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW+16, YMS11, YCM+13, BGP+17, CLH+16, FSGW11, FSGW12, GH12, HWD16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, LL16b, QMW17, SLZ12, SKB+17, T1a15, WHY+12, W18a, WXZ19, WLS14, XWXC14, ZYT17, ZLY10, ZDW+16]. Proxy-invisible [SYL13]. Ps [HDWH12]. Pseudo [NN12, XXYXY11, Zaj19, CFY+10, KM10a, MG15, PLsv10E, SH11, SM11, XSWC10, Zim10].


PSMPA [ZLDC15]. PSO [TLL13]. PSPACE [JJU10]. PTAS [JLX+19]. Public [Alz19, An11b, ABW10, BVS+13, BB14, BM18, BKL12, BKVK10, CT18, CLP13a, Che15, CLND19, CNT12, Con12b, EKOS19, FBM12, GKS17, HEP+11, HWS+19, HTC+15, HLH19, IM14, JLT+12, JWS19, KF12, LYX+19, LSW16, LG10, LHA+12a, LPS10, LSQL18b, LZC14, LCPD15, LL18, MZH15, MMP14, MTK11, Mat14, MRPS12, Mur16, NTY12, Omm16, PDH15, RPSB12, RVS+18, RW12, RBHP15, SG18, Saa12a, Sch19a, SK12b, Seo18, SWM+10, Sia12, SC12, SLY+16, SGP+17, ST10, TMC15, TT12, WP17, WZ15, WWHL12, Will18, WSQ+16, XNK15, XZZ12, Xio12, XJWW13, YL17, YKC+11, YKF+12, YMC+17, ZCQ19, ZY17a, AA14, ATK+17, AK14a, AVAH18, BS15, BZ16a, BS12, CFG+17, Dur15, HZWW17, Hrd19, HL14, HYL+19, HTC17, LSN14, LLY15, LFWS15, LH13, LL16a, LL19, RPS10, SES+16, SY15b, SLXX16,
VN17, XWK+17, XLC+19, YT11b, YYS+16, YN19, ZZ11]. public [ZCC15, ZCL+19, ZY17b, FBM12].
Public-Coin [CLP13a, Mat14].
Puzzle [IBM13a]. Puzzles [RSGN12, dCCSM+12, dCCSB+16]. Py [DGIS12]. Py-Family [DGIS12]. pyramid [MHT+13].
R [Gre19a, BS12, DB16, LVV11, LJF19, PP10b, WYW14]. \textbf{R3579X} [BDK11].


\textbf{Random-Grid} [KS15]. \textbf{Randomization} [DDE+19, Gas13]. \textbf{Randomized} [ARP12, CATB19, GDDL18, GT12, HHR11, SR12b, BWA13]. \textbf{Randomness} [AY14a, Ana14, ABF12, ACM+17, BWL16, DB16, HJKK19, KMZS19, MSA10, MS16, CHH+13, DTZ122, FRT13, RY10, TC11]. \textbf{Range} [DCA18, BKR19, HM12, JCHS16, LZW19]. \textbf{range-query} [BKR19]. \textbf{Rank} [SS10b, FES10]. \textbf{Ranked} [CWL+14, XWSW16, DDC+19, GZ18, LXX+14, NBJ19, YQZ+19]. \textbf{Ranking} [ZDL12, AT10]. \textbf{ransom} [Ano13b].

\textbf{Ransomware} [MPA+18, YY17a]. \textbf{Rapid} [KPC+16]. \textbf{rare} [Sch11]. \textbf{RASP} [AZPC14]. \textbf{RASP-QS} [AZPC14]. \textbf{Rate} [LJK17, PPS12b, PCPK14]. \textbf{Rates} [ZHS10]. \textbf{Ratio} [FHKP17]. \textbf{Rational} [CK18, HR19, KU14, KOTY17, NS12, TWZ11, ZC13]. \textbf{Rationality} [GLR10, GLR13]. \textbf{RBAC} [VN16]. \textbf{RC4} [GCS+13, Loc15, Ree15, RS14, Sar14]. \textbf{RC4-like} [RS14]. \textbf{RCB} [ABC+18]. \textbf{Re} [ABR12, Bre18, GSW+16, GZAXA19, KKA15, LK18, LSLW15, LSC12, LBR12, MLO17, NAL17, Pan19, Pet12, PRSV17, WY10, XJW+16, ABC+18, BGP+17, CFZ+10, CLH+16, CZ15b, DEL19, FSGW11, FSGW12, FXP12, GH12, GI19, HDW16, HY18, KKM+14, LMGJ11, LCT+14, LFWS15, LL16a, Par18, SYL13, SLZ12, SKB+17, Tia15, WGJT10, WHY+12, Wan18a, WXMZ19, WLS14, XXX15, YZCT17, ZDW+16, LAL+15].

\textbf{Re-authentication} [LBR12, FXP12, LMJC11]. \textbf{Re-creating} [Bre18, Pan19]. \textbf{Re-Encryption} [GSW+16, KKA15, LSLW15, MLO17, NAL17, PRSV17, XJW+16, ABR12, GZAXA19, LSC12, Pet12, WY10, BGP+17, CFZ+10, CLH+16, CZ15b, FSGW11, FSGW12, GH12, HDW16, HY18, KKM+14, LMC, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGJT10, WHY+12, Wana, WXMZ19, WLS14, XXX15, YZCT17, ZDW+16, LAL+15].

\textbf{Real-Time} [AEP18, AYS15, CSS17, JWJ+17, PNRC17, RHLK18, SK14, Tom16, Tur18, WLZL12, YE12, AY14a, Con12a, Kus13, NSX+18].
WgMdZlZ12, WgMW12, CHS11, HU15, HL12, IB11, KKG14, LH10c, LNM+11, LNKl13, LWK+18, LH13, MCL+19, MM12, Sar10a, WQZ+13, YSL+10, YN19, PZL+19. remotely [Wat14b, YHHM18]. Removing [HKHK13]. renewable [URK19].

Renewal [MMY12]. renewed [GPLZ13]. rental [LY14]. Reordering [Alo12].


Representation-Based [AGW15]. Representatives [Bla16]. reproducible [CW12a]. Reproducing [Söd13].

Repudiation [LLG15, VBC+15]. Repurposing [GY13]. Reputation [BL15, LHM+15, Pas13b, MGP10].

Reputation-Based [Pas13b]. Request [KK12, KK13]. Request-Based-Revealing [KK12, KK13]. Requirements [OS16].

Requires [Raz19]. requiring [KHHH14]. ReSc [YFT18]. Rescue [TSH17].

Research [BNMH17, BA18, CDFZ16, FREP17, Roh19, SDC+17, SPG+19, WP15, BEB+18, GLIC10, Hof16, Pal15, Ven14]. Researchers [Con12, Con17, Edw14, Wall18, Win17].

Reservation [LSY+16]. reset [RY10].

Resettably [CPS16]. Resettably-Sound [COP+14].

Residue [CSt10]. Resilience [CATB19, NTY12, CJW+19, GLL+18, HYL+19].

Resiliency [YM16]. Resilient [AV12, BKKV10, FPS12, HD19, HHS18, JP19, LTZY16, LD13, Nyr+14, Pan14, PSD15, ZXY+12, YZ12, YNR12b, YCZY12, ZYT13, ZWTM15, ZZM17, ZY+19, ZYY19, ZY17a, ZYM18, ZH+19, ABC+18, CAM19, CQX18, DLZ16a, GV14a, KPS10, Kom18, LLG19, MMSD13, SCBL16, SGP+17, Wan18a, YSLL14, YKC+12, YLZ+16, ZY17b, ZYM19]. Resistance [CGCS12, GZSW19, PRC12, WLZL12, ZJ11, DLN13, FIO15, YXMY19].


result [ACK+10, ED17]. Results [DGlS12, LJF16, Hof16, Pan19, URK+19].

Respect [CATB19]. Respiratory [RSCX18]. Response [GHS14, HLKL15, ZHW+16, MRRT17].


Rethinking [Che13, HU15, LSG16, MV16a, WYZ+17].

Retrieval [BBB+16a, BTHJ12, CJP12, DS19, HK14b, JMG+16, JKHeY12, YK10, ZZ+11, CJP15, SWW+17]. Retrieving [Uto13]. returned [War11]. reusable [RS17c]. Reuse [ABF12]. Reveal [Sta13].

Revealed [Ano15d]. Revealing [BT12, KK12, KBR19, KK13]. reverse [TQL+14]. reversed [KYH18].

Reversibility [FSX12b, HWYW14].
Reversible [CLF11, CSS+13, HHS+15, MM17a, MR16, NC12, AMK12, CT11a, HLC16, JK13, KKK+18b, MM14a, NC13, PWLLL13, PC14, SM19a, TK14, WOLS12].

Reversibly [MKH+12]. Review [Ano15b, Ano16a, Ano17b, AY12a, AY12b, Ayu12, Bai12, Bar12, Con12b, Dew11, Ful10, Gas13, Gre19a, Gre19b, Hom17, Jol10, Kat13, Keb15, Koh10, Led16, Lop15b, Low12, Mei10, Mou15, Mur10, Nag19, PMG+19b, Sch15a, Sha10, Ter11, Xie12a, Xie12b, IAA+19, JAS+11, MM12, TPK12].

Reviewed [Sch15a]. Reviews [SR14].

Revised [DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11]. Revising [BT12]. revision [LT14b]. Revisited [CLY14, DKPW12, DKS12, GWWC15, KFOS12, LL11, Lop15a, PKTK12, Sar12, Tan12a, BCLI4, DGMT19, DDL15, HKT11, HYWS11, MZ15, TS16a, ZCL+12].

Revising [GLMS18, RSD19, TLW12, WSA15].

Reviving [TLZ+17]. Revocability [WHLH16]. Revocable [AEHS15, CD16b, LNWZ19, MML16, QZZ18, SE14, SE16, SZS14, SZDL14, TCT15, TT12, Umr15, FLL+14, JCL+18, LDZW19, WLFX17, WTT12].

Revocation [AEHS15, LLC+15, LW16, Lop15b, RDZ+16, XMCL13, YWZ+12, ATKI1, LJY18, WIWG11, ZYW+19]. Revoking [TAKS10].

Revolutionized [Orm16]. RF [VJH+18].

RF-Data [VJH+18]. RFID [CJP15, AATM18, AMKC19, BL12, BSSV12, BM11, CCGPDMG12, CCF17, CJP12, Cho14, DZS+12, FLL+14, Far14, FMTR12, GMSW14, GI12, GSN+16, GH15, GAI+18, HSH11, HDPC13, HQY+16, HQY+18, HCPPLB12, HCTEPL+12, HWWZ19, JLZ18, KNTU13, LNZ+13, LEW19, MO12, Mic16, MK12a, PPH12, PLSwdLE10, QZL+16a, QZL+16b, SBS+12, SPLHCB14, SBS18, SSKL16, TG17, WH17, WCFW18, YFT18].


ride-sharing [GBC19]. Right [Bro17, RCK17, SR12a, BBG+17, LHA+12b, Sch11].

Rightful [RR11]. Rights [LVRY10, SC19a, GLL16]. Rigorous [DK17]. Ring [CZCD18, GHPS12, HKL+12, LYY+16, XY18, YKRS10, YLA+13, ZJ14, ZGCZ18, DZ14, GCH+19, Hwa11, LHY+10].

Ring-LPN [HKL+12]. Ring-LWE [XY18].


RLWE-Based [GDDL18]. RNG [CGH17].


Robot [NSP+18, AASSAA18]. Robotic [SPW+16, VOGB18]. Robust [BGCAFM12, BC12a, CFOR12, DKL+19, GKB17, HURU11, HZC+12, JSZS12, LSL12b, LSR13, MR16, MU12, MS16, MC11, pNyWyY+14, OCDG11, RR11, RMG18, SJ12, SS17b, SC12, SST18, TLM16, TR14, TTL10, WLB11, WgMdZI12, gWpNyY+14, XNG+14, YHNSW15, YHS19, YY015, YY13, ZZW17b, AP10, AIA+18a, BWR12b, CLM+12, CNF+18, EAA+16, GZHD12, HZC+14, HZL18, IOV+18, KMG17, KIH19, LNK+18a, LW10, LZZ19b, PKS18, RS17c, yWpNyL11, yWpWyYp13, WYZ+17, WHZ+19, YSL+10, ZHH+17].

Robustness [HGT15, YKBS10, AEH17]. ROCA [Ano17f]. Rochefort [Car11]. Rock [Cri16].
[GB19, PH12b, ZVG16, HPJ19, ZVH14]. Role-Based [ZVG16, ZVH14]. Ron
[LHA12b]. Room [Smi11b, Pea11]. Root
[ARH14]. ROP [ZHS19]. Rosen [HR13].

Rosenhain [CDSL14]. Rotation
[MM17b, SBS18, LWW11]. Rotational
[KN10, KNR10]. Roulette [Ber17]. Round
[Ber17, jCPB12, COP14, CJZ13, DWWZ12, GCHR14, KOTY17, KMO14, LWZ12, LJ17, LJ18, LYG18, LSG19, Pan14, TYM17, XZLW15, Yon12, AY14b, ABB12, Blo15, DMSD18, JK19, LP11, LFW16, Sun11, TSSL11, TQL14, TCS14, XW12]. Round-Reduced
[DWWZ12, DMSD18]. Rounds
[GST12, Sas12, LYHH14, MNP12]. Router
[Bis17, JLZ18, SA15]. Routing [ARWK19, Ham12, KZG10, WLY15, LSG16, LC17]. Routing-Aware [ARWK19]. RSA
[Dun12b, Kia11, Pie10, APPVP15, BBBBB13, Bro17, BNST17, CCL19, CLSW12, Chm10, GM13a, GST13, Her14, Hin10, HLYS14, IK15, KV19a, KHHH14, KFL10, Lim11, LFK19, MV19, MZ15, Moo12, PT19, PY19, SM10a, SM10b, SLMI0, TK19, Win17, XWK17, YHK10, YXA16, sCR19a].

RSA-1024 [Bro17, Win17]. RSEL
[FLL14]. RST [LD13]. rubber [BSR14].

Rule [KWP13, NC12, TW2, McG11, Nor17, WYZZ12]. Rule-Based [TW12].

rules [PT18]. Rumor [FKOV15]. Run
[CEL19, IF16]. Run-Time [IF16]. runs
[Anol13b]. RunStream [KPC16].

Runtime [BJ10a, CLP13]. Rupture
[KA18]. Russian [McG11]. Ryoan
[HIZ18].

s [SCH15a, MM17b, NN12, RMP10, RMTA18, SS11, WJ19]. S-Box [RMTA18, RMP10].

S-Box/Inverse [RMTA18]. S-Boxes
[MM17b, NN12, WJ19, SS11]. S3BD
[WS19]. SA [LHM14]. SAC [JY14, MV12].

SADT [SM12]. SAE [DLK16]. SAE/LTE
[DLK16]. SAFE
[DSL18, RQD15, BL17, Gel13]. SafeCurves [BL17]. Safeguarding
[FGR17, NML19]. Safely [HM12].

SAFER [YCL17]. Safety
[OS16, BMM12, KO16, SAM19]. said
[Pro15]. Salsa20 [MAS16]. same [Con17].

Samia [Anol15b]. SAML [IMB17]. sample
[YWL17]. Samplers [HKK18]. sampling
[Ana14]. San [ACM11, Anol10a, Dun12b, IEE15, Kia11, Lin14b, Pie10]. Sancus
[NVM17]. Sandbox [HZX18].

Sanitize [PH12b]. Sanitizer [YM19].
Sanjit [Kat13]. Santa [MSh16, Rab10].

Sanya [LT11]. SARFUM [BCE10].

Sarkar [Kat13]. SAT [Che18]. satphone
[DH13]. SAV5 [CDMW19]. SAW
[CFL13]. sawtooth [Ye14]. SC11
[LCK11]. SCA [HF14b, PDJ19].

SCA-Resistant [HF14b]. SCADFA
[PDJ19]. scalability [YC11]. Scalable
[BSC17, CCT14, DT13, FMTR12, FS18, HDIFG15, KGV16, KAK18, LYZ13, LLA19, MBR15, PY19, QZL16a, WHL17, ATK17, BBTC20, DYZ15, GM13b, GSN16, JVD16, MNN16, WLY11, WLD13, WLFX17, YC11, KCR11, KS11].

Scalar
[ARM15a, NR15, YTS12, SKH15]. Scale
[DM15, GU13, JKH12, LSL19, LQD16, An19, CG12b, dCCSB16, DEL19, DLGT19, FX12, GSN16, SR10, VSB19, ZZK17, ZVH14]. Scaling [PPG19, YM18].

Scan [LWK11, DDFR13, KPS10].
Scan-based [LWK11]. scanning [Ara13].

Scattering [KA18]. Scenarios
[DSB15, HUR11, LW19]. Schedules
[Pud12]. Scheduling
[DK16a, LJP17, MV16b]. Schema [AN12].

Scheme
[ARM15a, ADM19, AMSPL19, SS15, Bai10, BHG12, BS14, BKJP12, BDH11, CMLS15, CLE16, CCW10, CLHC12, CHHW12,
CCZC13, CCC19, CGY+13, CLH13, CSW12, DA10, DS11, DKS12, EAAAI9, FR16, FGM10, GZZ+13, GH11b, GJ17, GLW12, GZH17, HYS11, HIFGFC15, HMR12, HWS+19, HLC+18, HPH17, Hül13, HLH19, HP12, HP17, IL15, JSZS12, JX+19, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KLM+12, LSL12b, LHFI2, LH+15, LTZY16, LH11c, LSQZ17, LSQ18a, LGWY12, LCDP15, L+15b, LYY+18b, LPRH14, MWZ12, MVVR12, MRL+18, MSas12, NXB13, NLLJ12, NLY15, Pet12, PDT12, RVH+16, RSD19, RMG19, SK12a, SSKL16, SJ12, SGP+12, SD12, Shen14, ST16, SWF+19, SP15b, SJWH+17, SSA13, Tan11, TTD11, TWZ11, WY10, WgMdz12, WgMW12, gWpNyY+14, WHL15, XWSW16, XHC+12, XJW13, YM16, Yam12, YZ+12, Ye10, Ye+14, YTH17, YL17, Y+17, YHK+10, YMWS11].

Scheme [YY17b, ZPM+15, ZZQ+19, ZC13, ZQQ15, ZW13b, ZM18, ZLDD12, ZY17a, ZGZ18, AM18, ARL13, AHS14, APK+18, AK+17, AM19, BC16, BDL+19, BD18, BDM+19, BOB13, BBA19, BAL10, BWR12b, BMM12, BZL12, BB16, CCL11, CLSW12, CNF+18, CH10, CT11a, CLHB13, CW14a, CTHP16, CBJ16, Cho14, DDF+19, DSCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, FHZ18, FZZ+12, GHZ12, GJ13, GMRT+15, GJ18, GPLZ13, GLM+16, GH16, GAI+18, GBC19, GTSS19, HKA+18, HZW18, HBBRM+16, HL12, HL11, HCCCI11, HLC16, HCC10, Hwa11, IB11, JNUH17, JKA19, JLT+12, JZS+10, JMW+16, KEF19, KI11, KPP16, KD15, KK13, KHB13, KKM+13, KKM+14, KK14, KCS+18, Kim16, KKK+18b, KKH19, KP18, KLW+16, KVL+17, KD17, KKD+18, KWH16, KL11, LXLY12, LZL+16, LSR13, LVC+10, LH0c, LYW+10, LZJX10, LNM+11, LMJC11, LK12, LLHS12, LKNL13, LDZ+14, LWYM16, LK+17, LNK+18a].

Scheme [LWK+18, LNK+18b, LWK+19, LFWS15, LHH11, LWL10a, LWL11, LW13b, LZC14, LZZ19, LDZW19, LLI6a, LL16b, LWY12, MCN+18, MMS+17c, MK12a, MGB19, MSas13, NR17, Nos14, NMX15, OK+17, OSNZ19, OPS14, OSANAM19, PY19, PFZBF18, QMC17, QMW17, RPS10, SGCCR+16, SM11, SYWX19, SCR19b, SMS+16, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWZY11, WYYY11, yWpNyL11, WLH13, WDBL13, WLZ+16, WZ16, WLFX17, Wan18a, WXMX19, WXSH19, WHZ+19, WDK19, WZ11, WKH11, WOLS12, WXX+17, XHH12, XWZ16, XWXC14, XXX15, XW+17, XTZ+19, XXCY19, XMHD13, YYJ+19, YC11, YCC16, YHMH18, YSMQ19, YWK+10a, YCT15, YXD18, YQOL17, YY13, YMSH10, ZYL+10, ZLY10, ZJX+14, ZYC+17, ZZY+19, ZYW+19, ZPWY12, ZHH+17, ZY17b, ZFZ+18, ZLY+19, ZCR12, ZB11, DT13, LLZ+12].

Schemes [AAUC18, ACA+16, ABF12, BV+13, BM12, BBEPT14, BS19, CMLRHS13, CQD18, CND19, CGL+12, Chl16, Des10b, EFGT18, FHKP17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZK14, MLCH10, MR14b, MMS17b, MBF18, MKRM10, MKASJ18, Ob11, PB12, PDH15, PH12b, Sch10, Shi11, SK17, SSU12, VSR12, WGF16, YNR12a, YNR12b, Yek10, YYW+12, AGHP14, AN15, AHW+12, BKR19, CDG12, CXX19, CHS11, CCG10, CTL13, DDD14, D13, DZ14, FPPG14, FGMP12, FMA+18, HKA19, HWDL16, HMO10, KTTU16, LWW+19, LHYZ12, MM12, MBP19, MA17b, N/Z+15, QXYW16, SES+16, Sar10a, Sar11, sHZ15, SAR18b, WW14, YT11b, ZCL+12, ZCLL14, ZT14].

Schneier [Sev16]. Scholarship [SPG+19]. Scholarship-for-Service [SPG+19].

Secure [NBZF17, NDG17, NR12, NMS14, NSMS14, PB12, PSM17, Per13, PBC17, PRN19, QZL16b, QZDJ16, QZZ18, RC18, RPM10, RR17, Rea16, RMZW19, RSAG15, RS9, SAM19a, SNJ11, SSSL16, ST19, SZS14, SVCV15, SP15b, SKH17, SS15, SRAA17, SAR18b, SSAF11, SVG16, SYW17, SYC17, SSM14, SZDL14, SGH15, SYL16, SR12b, SM18, TB18, TCI15, TWZ11, TG12, TCG16, VTY18, VM15, WgMW12, WKB16, WXLY16, WLY17, WDC18, WD91, WLS15, WBA17, WWH12, WS19, WMS12, tWmC12, WXSW16, XLQ09, XJJW13, XLP18, XHZ19, YNR12a, YNR12b, YTH17, YQZ19, YHK10, YKC11, YAM15, YY17b, YGD17, ZZ12, ZDL12, ZDHZ18, ZVH14, ZVG16, ZHT16, ZLW17, ZH19, ZBR11, AHS14, APK18, ABBBD13, AC16, AKK17, ACD15, AYSL14, BMDT19, BOB13, BHH19, BZD16, BKR19, BSR14, CCL11, CSD18, CLHJ13, CW14a, CS11, CDL18, DA18, DEL19, DMM10]. secure [DGL19, DMD18, FHH10a, FLL14, FGW12, FA14b, FIO15, FLYL16b, FS18, GA13, GAI18, GLL18, GCH15, HGWI11, HK15, HLYS14, HTC17, HPY10, IB11, JZS10, KPP16, KKA14, KRM10, KCS18, KUT16, KGW17, KDW17, KKD18, LLLS13, LDDM12, LH11b, LW16, LSR13, LHM10, LDUZ14, LWK18, LZD19, LWZ19, LWK19, LCT14, LAL15, LJY16, LHI18, LL16a, LL16b, LBOX12, MR14c, MHY18, NR17, NAACL12, NAL17, ODK17, OSNZ19, OSANAM19, PABC19, PSSD13, PLSeDE10, PWS19a, PY19, PBP19, Rao17, RG10, RYF13, RITF11, RS15, SGGCR16, SYL13, SWW16, SSS11, SM10c, SSPL13, SLX16, SLXX16, SC19b, Tar10, TLLM13, THA13, TLL12, VS11, WLZ16, WMY17, WXMM19, WHZ19, WDKV19, WCCH18, WL19, WXWC14, XX15, XZP19, XMY17, XWK17, YMYL19, YC12, yYqWqZC13, YZZ14, YZCT17, YQOL17, YY11, YLS12, YJC18, YMSH10, ZLY10, ZCLL14, ZZ15, ZQD16, ZYC17, ZG10]. secure [ZZ12, ZX11, ZY17b, ZC12, Znu13, ZLW19, ZSW18b, Ano12, DSDL18, HKR18, OKG12, YSS14, YFK12]. Secure-TWS [OKG12]. Secured [LC17, SGG18].

SecureLR [JHW19]. Securely [CC10, KP17, LHL14, MS16, WXY17, BC18, der10]. SecureMR [DMD18].

Securing [AASSAA18, BK12b, CMS15, CST17, Cla18, NPH14, PMZ13, SF10, SMS18, SWF19, SLI11, Ste15b, TRK14, YMA17, YT12, YWW19, CR10, DIn10, GH15, SK518, SA15, Tox14, YWW18].

Securities [WWL14]. Security [ABJ13, AHN18, ASBdS16, Ano13f, Ano15a, Ano15d, Ano19a, ABF12, AN15, ABHC16, ABB19b, AYS15, BCE10, BSBB19, BA18, BCM15, BCH19, BRT12, BPR14a, BPR14b, BLS12, BCN16, BPDS12, Bra15, BDH11, BP10, CF17, CFE16, CBX19, CHS11, CFXY17, CCD15, CCCC19, CCCC20, CPS16, CM11, DDS12, Dan12, DR12, DK16a, DF17, Eilb09, FREP17, FMA18, Fid18, FMA19, FP19, FS12b, FSX12c, GN16, GZ13, GR19a, GPR19, GSC17, HCC12, Hel17, Her19, HB17, HSUS11, HLW12, HXC11, HLC11, HL15, HLN10, IEE15, IS12, IGR16, JN12, JSA17, Jia14a, KBL11, KS18b, KFO12, KSD17, KD12b, LPS12, LST12, LW11a, LG14, LLY19, LHP17, LW12, LL17, LT11, LSQZ17, LYL18, LSQ18b, LP12, LW17, LZC12a, LW17, LZZ19b, LNG19, LDB15, LMS16, LLH18, MMK16, MCT11, MKN13]. Security
[MCS+15, MH14, Mau12, MV16a, MGG+19, MLBL12, MPM+17, MHMSGH16, Nac12, NNAM10, NDG+17, NVM+17, Nos11, Nos14, OSH16, Orm16, OS16, Pasi13a, PZPS15, PGLC17, PDNH15, PS14, PL16, PDT12, PNRC17, RB17, RCP+18, RVS+18, RQD+15, RWZ12, Rog16, RS10, SGI18, SN10, SNJ11, SBS+12, SBS18, SPD+10, Sar12, Sch13, SD12, Shi11, SC19a, SLM10, STC11, Sti19, SSP19, SAM+18, SMOP15, SCGW+14, Tso13, TV15, VFFHP19, Wal18, WYCF14, WSA15, WZC16, WRP70, WSS12, WHHL17, WCL+18, WS14, Yan10, YZLC12, YSF+18, YHSW19, YGS+17, YKK+17, YSS14, Yon11, YYW19, Zha15b, ZMI18, ZXL19, ZYY19, ZY17a, ZYH+19, ZCZ+19, vTJ11, AMN18, AB10a, Abe10, ABGR13, And19, ABM+12, Ano11a, AM19, AGBR19, AD17, BYL10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTHP13, CLCZ10, CVG+13],

security [DLK+16, DGMT19, DXWD16, DHW+13, Edw14, FHM+12, FA14a, Fei19, Fis15, GH19, GM16a, GLM+16, GMMJ11, GMS11, GHI12, HPJ+19, HDWL16, HWG10, HLR11, HRS13, Hsd19, HLV10, IAA+19, JK19, KNTU13, KSA16, KKK+16, Lan10, Lan13, LDC13, LH10a, LZ11, LXWM12, LH111, LZC14, LSG16, LLG19, MZA+13, MZZ+19, Men13b, MM14b, MSGCDPSS18, MMS+18b, NS10, Nam19, NCL13, NLYZ12, NML19, OK18, OYHSB14, PHWM10, PMG19a, QYW16, QLZ19, Ree15, RPSL10, RH10, SA12, Ser12, SYV19, SLZ12, SY15b, SYWXY19, Sir16, Sta11b, Tan17b, TODQ18, Tay19, TAH+13, TKG+17, UUN11, VCK+12, WCFW18, XLC13, YLL+18, YY17a, ZAAB17, Zha15a, vWEG18, XW12, YKC+12, Bar12],

Security-Aware [LJP17, LMS16, GHD19], security-enhanced [AMN18],

security-modified [MM14b], SEDURA [LY15], see [PZ15], Seed [AS17, LYHH14, Sun11], seeing [Tox14], seen [Goo12, PWS+19b], Segment [WOLP15], Segmentation [WYW+13, ZZCJ14], selectable [GLM+11],

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

Selection [KÖ14, KD12a, KD19, RP12, SEY14, YKA16, DRN16, FXP12], Selective [BTHJ12, GDCC16, JSA17, LW12, LSC+15, LZC12a, LLH18, PWS+19b, LZC14, LW13c],

Selective-Opening [LLH18], Self [Cer18, CLL16, CHHW12, CSV15, DM18, HZ11, LCL+17a, LLPY19, LH12, LHM14, PRGBSAC19, RCK17, SAA15, SM12, TAP19, WHZ12, WXWC14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11, YN19],

Self-adaptive [LHM14, FXP12, SH11],

Self-authenticating [Cer18],

Self-Authentication [HL12, LT13],

Self-Certified [CLL16, WXWC14, HL14, LH13, YN19],

self-composition [AGH+17],

Self-Controllable [ZLDC15], Self-Defense [RCK17], Self-Identifying [CSV15],

Self-Recovery [SAA15, CHHW12],

Self-restoration [WHZ12], Self-Sovereign [TAP19], Self-Synchronized [DM18, PRGBSAC19], Self-Synchronizing [HZ11],

Self-Updatable [LLPY19, LCL+17a], SELinux [SFE10],

seller [KJN+16], Semantic [DDY+19, MHW+19, YZCT17, HLR11, HT1C7, JS18a, WS19],

Semantic-aware [DDY+19], semantically [PPB19, SLXX16],

Semantics [CM11, GL12, KGP12], Semi [AAA+19, BDOZ11, KKK+16, SEK+19, WHZ12, ZXWL15, ZHS10, PGLL10],

Semi-automated [KKK+16],

Semi-Autonomic [SEK+19], Semi-Fragile [AAA+19, ZHS10, WHZ12, PGLL10],

Semi-homomorphic [BDOZ11],

Semi-trusted [ZXWL15], Seminary [SS10c], semirings [Dur15], Sender [WZ15], Sensational [YGFL15], sense [BH19, Kem11], Sensemaking [HGOZ19], Sensing
Shares [BLU+15, CFOR12, KU14, SA16a, WY12, AIM+19, LJY16]. Sharing [Bai10, BFM12, BBF14, CMM+15, CFOR12, CCL+13, CCT+14, CLW16, DR12, EM12, FHKP17, FR16, HYS11, HL10a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KU15, LYZ+13, LPL15, Lin15, LCCJ13, LTC+15b, LLKA19, NS12, Oba11, PSM17, QZZ18, QJC+18, SC10, SSU12, SZZT18, TLW12, TWZ11, WYCF14, WKB16, WGF16, WHLH17, XNK15, XZY+12, YFF12, YWZ+12, ZC13, AKK+17, ADH17, CD16a, CT11b, CW14a, CLC19, EZ15, EA11, FGMEM12, GPLZ13, GMP15, GLW13, GLB+18, GBC19, HF14a, HBBRNM+16, HCC11, HLC12, HYF18, KFE19, KI11, KTI16, KPB17, LXYL12, LH11a, LT13, LFWS15, LAL+15, LyWSZ10, LHYZ12, LH15, LLL+18, LEW19, LL16a, Mas17, OX10, OO18, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WLMG11, WMC17, WXZ19, WHZ+19, WDZ19, WLS14, WKH11, WW12, WOLS12, YC11, YCC16, ZCL+12, ZZ15, ZPWW12, SLL10]. Shell [WZCC18, YSS14, Tay14]. Shemanske [Gre19a]. Shenzhen [IEE11a]. Shield [NDG+17, KGV16]. Shift [AKP12, TAP19, ZH15, KKM11, LW19]. Shift-Type [AKP12]. Shifting [YWW10, CSS+13]. Shih [Joh10]. Shilling [CZ19]. Shopping [AHS13]. Shor [JL18, MNM+16]. Short [BGH12, CWW12, FR15, NR12, SK12, WQZ+16, XGLM14, JSMG18b, LL15, LJY16, RD17, ZPWW12]. Short-Output [NR12]. Shorter [Hu13, PPB16, TH16]. Should [Bel15, Eve16]. shows [Goo12]. Shparlinski [Sha10]. Shredder [AMH+16]. Shredding [AMH+16]. SIS [Ano12]. Shuffle [HMR12]. shuffler [BVIB12]. Shuffles [CKLM13]. shunned [Ree15]. Sicily [Cra12]. Side [AMMV18, AN17, Bar16b, BHC19, BCO13, Bul18, CFE16, CDK+10, CBL13, CATB19, DZS+18, DMWS12, DKMR15, EWS14, GZSW19, GWM16, GPT14, KOP12, LWML16, LFK19, NCD+13, PRC12, SG15, SR12a, Vua10, YL17, ZBP18, BVIB12, CAM19, DJL+12, GSAV18, MCL+19, MFH13, SG19a]. Side-Channel [AMMV18, Bar16b, BHC19, Bul18, CBL13, CATB19, DZS+18, EWS14, GWM16, GPT14, KOP12, LWML16, NCD+13, PRC12, SG15, YL17, ZBP18, DMWS12, GZSW19, LF19, BVIB12, GSAV18, MFH13]. Sided [HP14]. Sieve [VM14]. sieving [SD17]. SIFT [KLY+12]. Sign [ACC+13, LL15, MEFO12, SPM+13]. Sign-On [ACC+13, LL15, MEFO12, SPM+13]. Signal [GDLL18, Kar12, BLM+19, MS13b, RITF+11]. Signals [Fyo19, LJK17, XNRG15, AIA+18a, AIA+18b]. Signature [Ano13c, ABF12, ASS15, AEHS15, BGH12, BDH11, CZZ12, CLND12, CYY+13, CFGT18, FGM10, FR15, GJJ15, GJZ17, GMSV14, GHH18, HXZ15, HPO+15, HHP17, HUL13, HP17, JLI16, LTH+15, LDZ16, LYY+16, LGPRH14, MM12, NXB13, PH12b, ST16, TTH15, WZXL12, WH15, WYML16, WHLH16, XLQ09, XGLM14, Y+17, YHK+10, YMWS11, YLA+13, ZJ14, ZHL+12, ZSY19, AGHP14, CLSW12, CCG10, Con17, DZ14, DXWD16, DLN13, HYWS11, Hwa11, JZS+10, LHM+10, LDZ+14, LWZG10, LL16b, Nos14, QYWX16, QMJ17, QCX18, RMS15, SLM10, VS11, WSC14, XZZ16, YWL+17, YLS12, YKC+12, ZLY10]. signature-based [DLN13, QMJ17]. Signatures [Ano15a, ABC+17, AYS15, BBC+13, BDFK12, BHH+15, But17, DMO+19, Fuc11, CY13, GdM16, HHS18, HS18, HUL13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, Orn16, PST13, TH16, Ver17, WCD19, YT16, ASVE13, AYSZ14, BDL+11, BH19, BPP10, GCH+19, GMS11, HAGTFR13, Her14, LLY15, LJY16].
[Her19, Jin10, TLCF16, SS17a]. Soft-Error [TLCF16]. Softw [WZM12a]. Software [Bar15, Bee17, BCHC19, EWS14, FHLOJRH18, GZSW19, KYEV+18, LRVW14, MRL+18, MV16a, Sco18, SAM+18, TLZ+17, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GIJ+12, HL10, KHF10, LBOX12, SF12, YWT+12].


Sparse [AGW15, AAT16, BBC+13, PMG19a]. SPARTA [MMS+17a]. SpartanRPC [CS14]. Spatial [AV12, CZF12, PDMR12, ZWZ17b, CW14b, NZL+15].

[LGLK17, MPA+18]. **SSH**
[YSS14, Cri16, Lit14, Ran10, der10]. **SSL**
[BJR+14, Dav11, FHM+12, GJJ+12, HREJ+14, NP+11, Tay19]. **SSL/TLS**
[BJR+14, Dav11, PP11]. **SSL/TLS-based** [PP11]. **SSO** [MLM16]. **St**
[DDS12, Dan12, MNS11]. **ST-Numbering** [MNS11]. **stack** [JSM+18], **stage** [Mas17]. **stakeholders** [RR16]. **STAMP** [WPZM16]. **Standard** [Ano12, Ano13c, App13, ABC+17, BCM12, BV11, BV14, CT18, GJJ15, GJZ17, HZX15, LYX+19, LK18, LDZ16, Loc15, MVVR12, NIS15, OGK+15, RSD19, SZS14, TCI15, WWHL12, You12, ZC13, BCM13, HTC17, Kim11, LJTZ12, LL16b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, ZCL+19, AEH17, MKRM10, NdMMW16, SJ19]. **Standardization** [TRD11]. **Standardized** [BLN16]. **Standards** [BCM+15, Che17, DHW+13, NIS13]. **start** [Rom11]. **starts** [Sch16a]. **State** [BVS+13, BLM17a, BLM17b, But17, CG14a, CCL+13, CHS15, Dew11, DP17, FHR14, LK18, MKF+16, OMNER19, Sen17, WGD18, XZY+12, YM18, BBDL17, CK11, CGH17, Ham12, Mid10, QD16, Sir16]. **Stateful** [BVS+13, NTY12, VKP17, VSR12, YLL+18]. ** Stateless** [BHH+15, GM11, MKKA17, NTY12, VDO14, BBPD16, DCAT12]. **Stateless/Stateful** [NTY12]. **statement** [NIS13]. **Static** [DKMR15, IF16, Lan11, TLM13]. **Station** [LSY+16, Smi11a]. **stationary** [ZLDD12]. **Statistical** [Böh10, Bro11, DBPS12, HZ11, Hey17, LTKP16, OOR+14, SP13, Sim15a, GMT+12, SA19]. **Statistical-Attack** [SP13]. **Statistics** [gWpNyY+14]. **Statutory** [PH12b]. **Stealing** [RZW12, VWC19]. **Stealthy** [BRPB13]. **Steering** [HR13]. **Steganalysis** [Böh10, DA12, Fri12, JHHN12, KD12b, LJK17, LC15, SGP+12, Tan12a, YLL+12, Y14, YPRI17, BS11, LHM13, LSO11a, LSO11b, Sch12a]. **Steganalysis-Resistant** [YPRI17]. **Steganalytic** [Ber18, YPRI17]. **Steganographic** [DA10, HHS+15, LyWZZ12, WP15, AGLW16, LLC10, CAC14]. **Steganography** [AAA+19, AGW15, BCM12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZW+14, Joh10, KTM19, LJK17, LLY+12b, MAL10, PDMR12, Pau10, SK12a, SR12b, TJJF12, WWL+14, WYL18, WYZ12, YWW10, ZSA12, AOT13, BS11, BDK11, BHCDMR12, EEAZ13, GCK11, KKK18b, LyWSZ10, LRW13, LRW17, LWW+10, Maz13, MSM+18b, MS17, PHN+12, PMG19a, SAM+19b, SI12, ST15, Sun16, WKH11, WOLS12, ZMS14]. **StegNet** [WYL18]. **Stego** [YLL+12, SMSK18]. **Stego-Image** [YLL+12]. **Stenellenbosch** [BL10]. **step** [AKY13, YXA+18]. **Steps** [Ano13c]. **Stereotypes** [Söd13]. **Stern** [ACD18]. **STES** [CMLS15]. **Steven** [Ano16a, Led16, Sch15a]. **Still** [RAZS15, UK18]. **Stochastic** [ADR18]. **stolen** [Bha16]. **Stopping** [Sav13a]. **StopWatch** [LGR14]. **Storage** [BCQ+13, CWL16, CCT+14, CLW16, CDLW19, DLK+19, GLG12, HSM14, HLC+18, JSCM17, Küp15, LCK11, LMD16, LWCJ14, LCDP15, PBC+17, QLL17, SKH17, WHL17, XNKG15, YZDZ19, YJSL18, ZDL12, ZVG16, AY14a, AKK+17, BP10, CFVP16, CFZ+10, CLH+16, CDF+10, CDL18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, PLL+19, Sar10a, SYY+17, SWW+16, SWW+17, WS13, XWK+17, YXMYL19, YYS+16, YZCT17, YJC18, ZYC+17, ZVH14]. **store** [KV19b]. **Stored** [CMLS15, RSN14]. **Stores** [BCK17, GYW+19]. **stories** [Smi15b, ZMYB17]. **Storing** [DLWW11, HK19, LSC17]. **storm** [ACM12]. **Story** [Cer14, Keb15, Tur18, Ald11, Fag17, Gre17,
Hea15, Kus13, Mac14, Mun17, Pea11, Pet11]. **Strand** [SH15]. **Strange** [Acz11, Gre17]. **Strangeness** [Ber12]. **Strategic** [Sch12c]. **Strategies** [DSSDW14, DSSDW17, TJZF12, YCM+13, AZF+12, DRN16, WWW17]. **Strategy** [LH12, NRZQ15, FLZ+13]. **Stratix** [SMOP15, SMOP15]. **Stream** [ABS+12, BMS12, CMLSI5, DM18, DGFH18, DG12, DGF12, DJG+15, GKB17, GCS+13, HZ11, Hey17, IOM12, KE19, KPC+16, Kla10, MD12b, MHC12, MS12b, NN12, PNRC17, WH18, WHN+12, ZH15, Die12, KM10a, LWK11, LW13b, MRT10, OCGD11, QGGL13, RS14, SM19b]. **StreamCiphers** [ERRMG15]. **Streaming** [BSA+19, ZSA12, Cri16, XWZ+18, ZC12]. **Streams** [PCDG14, PWS+19b, HM10, PYP10]. **Street** [Gli12, KGP12]. **Street-Level** [Gli12, KGP12]. **Strength** [DM15, FHV16, Spa16]. **Strengthen** [BL12]. **Strengths** [XNP+18]. **Stribog** [AY14b]. **strikes** [Ran10]. **string** [FHV16]. **Strings** [SKE+18]. **Strong** [ADD10, KFOS12, PYM+15, SA19, SAA12b, Yon12, GH15, GH16, HYWS11, NCL13, OYHSB14, SVY19, WLZ+16, YLL+18, AYSZ14]. **StrongBox** [DGFI18]. **Stronger** [Boy16, ZYY19, MvO11, RK11]. **Strongly** [DDM17, HHP17, KW14, YS12]. **Structural** [LYY+18b, BKD11]. **Structure** [CJZ13, HP12, KD19, LMHH14, LJ15, LLG19, MKRM10, WYCF14, WJ19, CD16a, JKA+18, LLY12, SM19b, ZLW+12, ZPWY12]. **Structure-Independent** [MKRM10]. **Structure-preserving** [LLG19]. **Structured** [PMZ12]. **Structures** [GT11, HHH+13, LHKR10, LPL15, PB12, TS18, 3DFDR13, MKSI14, PPG19, Shy15, WS12, XWZ+18, ZZ15]. **STT** [VDB+16]. **Students** [PP10a, SDC+17, SPG+19]. **Studies** [Uto13]. **Study** [AIF+19, Ano17c, DDR+16, MZLS18, SY15a, SPG+19, STC11, CCG10, EBFK13, KD18, MHV15, SS17a, VGN14, VSB+19]. **Stuxnet** [BPBF12, Kus13, Zet14]. **Style** [GHS12, GHS13]. **Stylistic** [GA19]. **stylometry** [BAG12]. **sub** [GPLZ13]. **sub-passwords** [GPLZ13]. **Subcommittee** [Bla16]. **Subgroup** [CCL+19]. **Subject** [SC19a]. **subsimal** [LWZG10]. **submarines** [McGl11]. **subnormal** [AKM+15]. **Subreductive** [BB19]. **Subscribe** [BGP+17, DLZ+16b, OFMR16, PRSV17, SL11, TK14, YSM14]. **Subset** [BS14, RP12, AVAH18, ZZ11]. **subspaces** [ZWM14]. **Substituted** [HD19]. **Substitution** [DA10, KTM19, SGCRM+18, FVK17]. **substitution-transposition** [FVK17]. **Substring** [MRR+18, SOR16]. **substructure** [MRT10]. **success** [Ano14a]. **Succinct** [BC1+13, CKLM13]. **Such** [Roh19]. **sufficient** [TD14]. **suitable** [Jeo13, SKB+17]. **Suite** [MTM18, NA1R12]. **sum** [AVAH18]. **Sumo** [BS12]. **Sums** [SS12b]. **sun** [Cer15]. **Super** [Sch19b, BCND19, MZ17a]. **super-activation** [BCND19]. **Super-Isolated** [Sch19b]. **Superpoly** [HJ+19]. **Supersingular** [HIJ+19]. **Supervised** [CTC+15, GSAMCA18, HXHP17]. **Supply** [QZL+16a, QZL+16b, YFT17, YSF+18, YFT18]. **Support** [MSI18, ZZQ+19, CZ14, HHA19, JAS+11, MFF15, PWW10, PKK15, TLL10, VCK+12, ZMM+10, ZBR11]. **Supporting** [BBH19, CDLW19, FM12, HGOZ19, HCDM12, PH16, SG12, SOR16, Ver17, ABR13, HZ18, JSMG18b, YYS+16, CWZL13]. **supports** [WR15]. **Surfaces** [Sch19b, CDSL14]. **Surprises** [Bow11]. **Surreptitiously** [SFKR15]. **Surveillance** [BPR14a, BPR14b, GZH17, KLK+19, Lan10, Ano16h, Fei19]. **Survey** [AAUC18, AKB19, ABH+16, ABB+19, BGN17, BCTPL16, BHJP14,
BJCHA17, CLB19, DM19, GN16, GMDR19, HPC10, KMY18, KSD17, LGM16, MR14b, MSA18a, MSH10, MKK17, NDR19, NV10, OMFR16, OMNR19, PLLCX17, PWS19a, SKH17, SSP19, TRD11, TS16b, VV18, AA516, ABB14, ADH17, BM13, BGG13, BEB18, FMA18, HKA19, HT13, HGATďFR13, KJN16, KAS15, LK10, MJP19, MA17b, Maz13, MVH15, NR11, PPA18, THTC16, TKG17, VBC15, WWW17. Survival [YCM13, MMS17a].

Symposium [ACM10, ACM11, Ano10a, IEE10, IEE11b, IEE15, MSH16, TBL19, TT18, Wat10, Ano11a]. symptom [YZL18]. symptom-matching [YZL18]. SYN [DHT19]. Synchronization [BL12, VTY18, WXY17, yWXyZ18, AAM18, WDG19, XNG14]. Syntons [RCBK19]. Synthesis [SKE18, TCMLN19, RS17c]. Syst [HYS18, WZM119]. System [ADI11, Alz19, Ano10a, BBCL19, BD18, CZLC12a, CZLC14, Cor14b, CRST15, DDE19, DG15, GOPB12, Har16, HHS15, HZS19, IAD10, JN12, JLZ18, JWJ17, Jia10, KMP11, KZ17, LXY19, LFX18, LSY16, LIP12, MMB19, MLBL12, SNS14, LSS1K9, QLL17, RSCX18, SMG18, SRAA17, SSL11, XYL19, YE12, YXZ12, YKKK18, ZSM17, ZPW16, ZLDC15, ZVG16, AMH18, ARG19, BC18, BGG13, Bul10a, CH11, CT12, CZ14, CS11, FLYL16b, FNWL18, GKCK11, GH15, HHBS18, HKW15, HJM11, HLYS14, JCL13, KG19, LLL10, LLL17, LHL18, Lit14, LTC15a, LLL18, LZX19, MS12a, MNNW15, PSOMPL13, SSPL13, VSB19, WMX17, WZH19, WZ18, XWZW16, YXML19, YZL18, YWZ18, ZCZ19, ZYCT17, ZMM10, ZML17, ZZZ18, KKA14, Dew11]. System-Level [BBCL19, JWJ17]. System-on-Chip [HZS19]. Systematic [CCG16, CBL13, PC16, IAA19]. Systems [AMSP19, AN12, AEP18, AB15, Ano19a, BL15, BL16, BS13b, BCTPL16, BB10, CZ19, CWL16, CCF17, CRE12, DLZ16b, GI12, HXC11, HCL14, HLN10, HK18, KS18a, KKL19, LYY18, LMD16, LQY10, LYY16, LNZ13, MT17, MR14b, MJS19, OS12, PGLC17, PMG19b, PRR17, PH16, QZL16b, RST15a, RST15b, SBS12, SBS18, SML16, SKFR15, S616, SCH17, SGC14, SDM12, STC11, SSP19, TRK14, YNR12a, AT10, AT10, BK19, BGE18, BDL19, CFVP16, CFZ10, CLZ17, Cle8, dCCSM12, dCCSB16, CGH11, CVG13, CDA14, DEL19, DZS12, EIS10, FPX12, GNOG1C15, GHD19, GSN16, GPVCBRO12, HZW18, JSK16, JHCC14, KS16A, LCL15, LOK18, MDHM18, MLMS12, MGP10, MFH13, NLYZ12, QMC17, SS10a, SR10, SRB12, SMS16, SYND [MHC12]. Syndromes [BBC13]. Synergy [KRB12]. Synergy-Based
Systems-on-Chip [KS18a]. Systolic [MCDB12]. Systolic-Array [MCDB12].


Technique [HEK18, KBL11, ZLDQ14, BBBBBP13, CPPT18, GCSÅddP11, LH11a, Nam19, SM12, ST15, SKS +18, TS16a, ZWS +18]. Techniques [Bis17, DA12, GOS12, HPC10, HL10b, KDI9, LW12, Mor12, PJ12, VV18, AB10b, BM13, FGPG14, Gil10, HT13, KHF10, LH11b, O118, SM19a, VN17, WMX +17, Joh10].

Technologies
[ATD17, GB19, Int19, RC18, SJZG19, JAE10, JAS +11, Lan10, MMP19, Ano16a].

Technology [Ano19c, AHWB20, CGB +10, Eya17, Foli16, IEE11a, MZLS18, TBY17, VFS +19, Wu16, Ham19, IMB17, Pec17].

telecare [LWK +18, MA17b]. telephone [GMMJ11]. telephony [Clai18, SKEG14].

Telepresence [NSP+18]. teleprinter [GTM +12]. Television [DTE17]. Tell [Cer14, Pec17].

Template [NGAuHQ16, SKV12, YYK +17, AJYG18, ATI +10, GCSÅddP11, SC19b]. Templates [DBB12, AHN +18, AGBR19, LH14, QLZ19].

temporal [DZC16, JM +16, MTH +13, XMHD13].

temporal-credential-based [JM +16, XMHD13].

Tenant [TV15].

Tensor [FYD +19].

terahertz [WW13].

term [SKV12, vdG17, CFVP16, VBC +15].

termination [SRB +12].

TERMinator [MTM18].

ternary [ADI11].

Test [CHH +19, HTC +15, JEA +15, LLSW16, MZH15, SS10b, WH18, WZCH19, HTC17, ZCQ19, ZCL +19, Ano16i].

Testable [RMP10].

Testbed [BNHH19].

tester [RPSL10, SY15b].

Testing [BCG19, Coup12b, DB16, SS12a, YA14a, BJ +14, GR19b].

Tests [GLG12, MS12b, Sim15a, YM18].

Texas [IEE13].

text [GA19, GdM16, SMSK18, XZZ18, CR12, HAK19, SI12, SWW +17, ZMYB17].

Text-dependent [GdM16].

Textbook [PP10a].

Texture [TS17].

textures [NSX +18].

thanks [CBL10].

Theft [Ber12, Bot17, BTPLST15, ZMYB17].

Their [CZLC12b, CK18, FVJ19, HR19, JS18b, JSK +17, NR12, ZYY19, CQX18, FLY16a, Hof16, IK15, KK10, Mat19, Sti11]. them

[HLV10, JSK +16, Nor17, Rus15].
TNFS [FK19]. Today
[Ber16b, Cla18, Mac12]. Toeplitz [Ye10].
Token [TYK+12, ZM16, IMB17, Jac16, 
OMPSPL+19]. token-based [Jac16].
Token-Leakage [ZM16]. tokenisation
[Mar10b]. tokenless [Wat14a]. Tokens
[Muf16, DCAT12, HU15]. Tokyo [Sah13].
Tolerant [HK14b, M KK17, WCD19, ZM16, 
BZD16a, JLT’12, WMY16, XW13].
tolerating [ZWM14]. Tone [Yam12]. Tool
[DL15, DSSDW14, DSSDW17, Ros11]. Tool
[ASM12, DKMR15]. Toolbox
[AHS13, TRD11]. Toolkit [BJL12]. Tools
[Abe12, BBKK14, GO17, Ste15a, Lan11].
Top [SS12a, SS10c, Sta13, CHX13]. top-
[CHX13]. Top-Fanin [SS12a]. Top-Secret
[SS10c]. Topics [SCPSN10a, SCPSN10b, 
AB10b, Dun12b, Kia11, Pie10]. Topology
[HMKM14]. Topology-Preserving
[HMKM14]. Tor [LLY+12a]. Toronto
[MV12]. torsion [HR19]. Tossing
[ALR13, DSM14, Fok12, BB14]. Touch
[KTM+18, MWW+18, SPW+16, SHBC19, 
Alp18, CTL12, IAA+19, NSBM17, TZTC16].
touchstroke [Alp18]. TouchWB
[MWW+18]. Tower [ZAG19]. TPM
[GY13, KHN+11]. TQC [vDKS11]. Trace
[AB12, GA19, PS14, AA14, WGJT10].
Traceability [HCETPL+12, WYML6, 
WHHL6, YFT17, Chi13a, YYS+16].
Traceable [LZDW19, QRW+18].
Traceable-then-revocable [LZDW19].
traceback [LWY12, PJ18, WYL13]. traces
[MYYR13]. Tracing
[LW16, PPS12b, WXL+17, MFH13, PPR+12].
Track [Dun12b, Kia11, Pie10]. Tracking
[GHZ17, MDMJ17, SNC18]. Trade
[ASBdS16, BS14, GPR+19, SR10].
Trade-Offs
[ASBdS16, BS14, GPR+19, SR10]. Tradeoff
[WDDW12, MV16b]. Trading [TW12].
Traditional [SSP19]. Traffic
[BSA+19, DRS16, FGRQ18, HS18, 
KAHK17, VV18, ACMP19, AZH11, 
FTV+10, PPR+12, Tay19, VS11].
traffic-feature [FTV+10]. Training
[HHI2, GSAMCA18]. Traitor
[LW16, PPS12b, Bha16]. trajectory
[LVRY10]. Transaction
[BA12, MLN15, KVvE18, OYHSB14].
Transaction-based [BA12].
transactional [SPK17]. Transactions
[DG15, Mic16, Mu16, PAS13b, TV15, DK12, 
FG19, MLMSG12]. Transceiver
[NBZ17]. Transcript [Gl12]. Transfer
[AMSPL19, DN12, FMT12, HL10a, 
LCC13, WCL+18]. transferable
[GZXA19]. Transform [AN12, BCPV11, 
KTM19, LSL12b, pNyWyY+14, OWHS12, 
SM12, YWW15, BW13, MO14, NES+14, 
PC14, ST15, TK14, yWpWypN13].
Transformation
[CRE+12, FJHJ12, NXB13, TFS19, 
WmC12, GHzD12, HQZ14, PG1].
transformations [CJXX19, SA14].
Transforming [Eva17]. transition [CK11].
Transitioning [BR19]. translation
[AB13, CLY18, WSS+19]. transmission
[AK14a, BCDN17, BCND19, OSANAM19, 
PsDo+13, WQZ+13]. Transmissions
[BCO+18]. Transmitter [KPB17].
Transparency [TJZF12].
Transparency-Orientated [TJZF12].
Transparent
[CCW+10, XTK10, ZHS+19, CSR13, JYD16].
Transport [RBHP15, TW14].
transportation [SMS+16]. transposition
[FVK17]. Trapdoor
[BKPKW12, CLL+19, CBXJ19, CWW12, 
Mat14, RPSL10, CSZ+11, CW12a].
treatment [YSH14]. Tree
[BS14, CCC19, HSH11, XWX+18, BW13, 
BBB16b, CD16a, CFG+17, SCBL16].
Tree-based [ZSH11]. Trees
[SB18, BTPLST15, Kam19]. Trends
[FI12, GCK12, ZMS14, JAE10]. Triangular
[AMVZ12, RR16]. Tricks [GY13]. Trigger
[SS19]. trimmed [TTL10]. TRIMS

LCR$^{+18}$, LBC$^{18}$, MM$^{17a}$, MBC$^{15}$, MRL$^{+18}$, MS$^{16}$, NIS$^{12}$, NGAuHQ$^{16}$, NNAM$^{10}$, NN$^{12}$, NSMS$^{14}$, PMZ$^{13}$, PSS$^{+13}$, PAF$^{18}$, PDMR$^{12}$, PDT$^{12}$, PCPK$^{14}$, RSX$^{18}$, RMRM$^{19}$, RVSCM$^{12}$, RHLK$^{18}$, SR$^{12a}$, SFE$^{10}$, SS$^{17b}$, SS$^{19}$, SRAA$^{17}$, SC$^{12}$, SR$^{12b}$, Tan$^{12a}$, TKR$^{14}$, VJH$^{+18}$, WWL$^{+14}$, WgMdZ$^{12}$, YWW$^{10}$, YWW$^{15}$, YYS$^{19}$, YCL$^{17}$, YYS$^{14}$, ZHZ$^{17}$, ZWW$^{17}$, ZW$^{17a}$, ZHS$^{10}$].

Using [ZPW$^{16}$, ZS$^{12}$, dRSdlVC$^{12}$, ACMP$^{19}$, AASSAA$^{18}$, ATKH$^{+17}$, AHM$^{+18}$, APK$^{+18}$, ASVE$^{13}$, BK$^{19}$, BOP$^{14}$, BM$^{13}$, CSH$^{+18}$, CHS$^{11}$, CR$^{12}$, CLHJ$^{13}$, CB$^{16}$, CP$^{13}$, Cri$^{16}$, DA$^{18}$, Dav$^{11}$, DTZ$^{12}$, DGFH$^{18}$, DMD$^{18}$, uHAN$^{+18}$, EEAZ$^{13}$, FES$^{10}$, GQH$^{17}$, GR$^{19b}$, GSAMCA$^{18}$, GSV$^{18}$, GSGM$^{16}$, HAK$^{19}$, Ham$^{19}$, Har$^{14}$, HK$^{14a}$, HK$^{17}$, HZWW$^{17}$, HFCR$^{13}$, HWW$^{12}$, HL$^{14}$, HP$^{10}$, HCC$^{10}$, HS$^{11}$, JKA$^{+18}$, JCHS$^{16}$, JCL$^{+18}$, JM$^{+16}$, KG$^{+19}$, KI$^{11}$, KY$^{10}$, KKG$^{14}$, KCS$^{+18}$, KM$^{11}$, KKK$^{+18b}$, KSU$^{13}$, KTU$^{16}$, KPB$^{17}$, KD$^{19}$, KIL$^{+16}$, LLP$^{+18}$, LC$^{17}$, LH$^{11a}$, LIH$^{10c}$, LNM$^{+11}$, LXMW$^{12}$, LIH$^{13}$, LZX$^{19}$, LM$^{14}$, LML$^{+13}$, MM$^{12}$, MMLN$^{15}$, MS$^{13a}$, MM$^{13d}$, MM$^{14a}$, MKJ$^{12}$, MRR$^{+17}$, MSR$^{+17}$, MSM$^{+18b}$, MGB$^{19}$, NX$^{+18}$, NTKG$^{17}$, NSBM$^{17}$, PBCC$^{14}$, PPB$^{19}$, PC$^{14}$, QD$^{16}$, RR$^{17}$, RS$^{15}$, RS$^{17c}$, SCFB$^{15}$, SKE$^{+18}$, Sar$^{11}$, SM$^{19a}$, ST$^{15}$, SGFCRM$^{+18}$, SK$^{+18}$, SAR$^{18b}$, SPK$^{17}$, SLXX$^{16}$]. using [SA$^{19}$, SC$^{19b}$, SCBL$^{16}$, TLCF$^{16}$, TG$^{17}$, TK$^{14}$, TLL$^{13}$, UUN$^{11}$, VSB$^{+19}$, yWpNyL$^{11}$, gWpNyY$^{+14}$, WMX$^{+17}$, WH$^{17}$, XWK$^{+17}$, YWJ$^{+19}$, YQH$^{12}$, YZZ$^{+14}$, YSL$^{+10}$, YN$^{19}$, ZK$^{17}$, ZL$^{12}$, ZYC$^{+17}$, ZXW$^{+18}$, ZZZ$^{+18}$]. uth [CHL$^{19}$].

**V2G** [BT$^{18}$, TODQ$^{18}$]. Validating [GIJ$^{+12}$]. Validations [PDJ$^{+19}$]. Validity [BCF$^{16}$]. valuable [Ana$^{14}$]. Value [GYW$^{+19}$, LSL$^{12b}$, SZHY$^{19}$, YWW$^{10}$, BWA$^{13}$, KV$^{19b}$, So$^{14}$]. valued [BNA$^{15}$, TMK$^{11}$]. **VANET** [PZBF$^{18}$, WLZ$^{+16}$, Wu$^{17}$]. **VANETs** [BMM$^{12}$, CGCGPDMG$^{12}$, CST$^{+17}$, IOV$^{+18}$, LLG$^{15}$, MGB$^{19}$, YMI$^{13}$].

**Variability** [VDB$^{+16}$, SHBC$^{19}$]. Variable [CHHW$^{12}$, CMMS$^{17}$, XNP$^{+18}$, DTZ$^{12}$].

variable-interval [DTZ$^{12}$]. Variables [BB$^{10}$]. Variant [AAE$^{+14}$, MVVR$^{12}$, ZXA$^{18}$]. Variants [ASS$^{15}$, BB$^{10}$, HLC$^{+19}$, Hin$^{10}$]. Variation [DWZ$^{12}$]. Variations [DSB$^{16}$, SJZG$^{19}$]. Varied [GZ$^{12}$]. varieties [LR$^{15}$]. Varying [GKCK$^{11}$, BCDN$^{17}$].

Vehicles [LSY$^{+16}$]. Vehicular [HLKL$^{15}$, ZHW$^{+16}$, BBB$^{19}$, KM$^{10b}$, SGGCR$^{+16}$, WXSH$^{19}$]. Vein [KLY$^{+12}$].

Velskii [BBB$^{16b}$]. Ventilated [RSCX$^{18}$].

**Vera** [Ay$^{12}$]. Verifiability [EKOS$^{19}$, RST$^{15a}$, RST$^{15b}$, VSR$^{12}$, WWHL$^{12}$, YMC$^{+17}$, BRR$^{+15}$, Hwa$^{11}$].

Verifiable [CFE$^{16}$, CRST$^{15}$, Fuc$^{11}$, HYS$^{11}$, HLC$^{12}$, HLC$^{+18}$, KZZ$^{17}$, LWW$^{+19}$, LLL$^{+18}$, NBJ$^{19}$, QD$^{16}$, RDZ$^{+16}$, RS$^{17b}$, SZQ$^{+17}$, XWLJ$^{16}$, YNR$^{12a}$, YCR$^{16}$, GLM$^{+19}$, LZY$^{+16}$, LJW$^{+17}$, MGB$^{19}$, NMP$^{+13}$, PHGR$^{16}$, QS$^{18}$, XWS$^{17}$, ZZ$^{15}$]. verifiably [SEXY$^{18}$, ZLY$^{10}$]. Verification [AV$^{18}$, App$^{15}$, ABR$^{12}$, BCEO$^{19}$, BCEO$^{20}$, BL$^{15}$, BL$^{16}$, CCK$^{12}$, CCK$^{16}$, CM$^{11}$, EWS$^{14}$, Ess$^{17}$, GLLSN$^{12}$, GdM$^{16}$, GMSV$^{14}$,
93

HZS+19, Lin15, MT17, MV16a, OŠ12, PNRC17, RSR+19, SOF12, TSB18, Tom16, Vet10, ZPW16, AGHP14, ABF+14, ASVE13, BK19, BFG+14, BJ10a, BTW15, GPN+12, HFCR13, KKK+16, LEW19, MR14c, NPH+14, SD10, XHM14, YNX+16]. Verified [BFCZ12, YGS+17, HKA+18].


Via [ADR18, BSCTV17, ABC+18, AHG18, BHKN13, BCI+13, BCG19, BR14, Bu18, CBZ19, CDSLY14, CFG+17, CLW16, DM19, GT12, GST13, GVW12, Gre19b, HFV+19, JHW+19, KKK+18a, LT13, LT14b, LFIH18, LH14, LEW19, LLKA19, MH14, Mor19b, PV17, PTK14, QZDJ16, RS10, SE16, SSAF11, SKEG14, TBCB15, WSS+19, tWinC12, YFW18, Yon11, ZOC10, ZCZQ19, Zim10]. Vice [LMS10]. Vichy [Kap11]. Vicious [NN15], victory [Pea11].


vision [BSW12, LWW+10]. Vista [FG19]. Visual [BNA15, CSW12, GLW12, HHS+15, KU14, KS15, Lal14, LPL15, LWL10b, LGWY12, LMHH14, LTC+15b, OTO18, SA16a, SC10, Shy15, TWNC18, WY12, Yam12, ZZX+11, CT11b, CST16, DDD14, DD13, GJJ18, GLW13, HT11, LW10a, MSM+18b, WYK12, WS12, YSC16, YR11]. Visualizing [Sav15]. VLSI [KB10]. VMOR [MSI18].

Vocal [WOLP15]. visibility [FG19]. Visible [Cas10, HWYW14, LZX+12b, PCK19, WZLW13, Lin14a]. Voting [Ber16b, CFE16, CRST15, CEL+19, KV18, LHF12, LGPRH14, RST15a, RST15b, Sch10, KZZ17]. Voumich [Ano16e, Bax14].


Vulnerabilities [BKJP12, HSUS11, MAS16, PDT12, RY10]. Vulnerability [MKN13, TM12, VKC15, Wal18, Ano17f, DMWS12, MYyr13]. Vulnerable [Ano15d]. vVote [CRST15].


Waknaghat [CGB+10]. Walker [Xie12a, Xie12b]. Wallets [Chi13b]. Wallis [Wes16]. Wan [RSD19]. wants [Nor17].

War [Has16, Mun17, Bud16, Car11, Sni11a]. Warbler [MFG16]. Warm [MCL+19]. warriors [Bud16]. wartime [McK10, McK11].

Was [Tur18, Goo12, LHA+12b]. Watching [NSP+18]. Watermark [CHHW12, DLMM+18, EMW14, FR15, GRRZ18, Jia10, KBL11, LZX+12b, MCDB12, QJC+18, SJ12, YE12, ZS12, HB13, TLL13, WYL13].
Watermark-Based [GRRZ18].
Watermark-Driven [DLM+18].
Watermarking [AAA+19, BCPVM10, BFFW, BGBP10, BBM15, CGB18, CHHCD12, CUC13, CHN+18, DG17, FM15, Fra15, Fra16, GKS17, GPl7, HPCI0, HEK18, HD19, HGT15, HHHK14, JSZS12, Jol10, JKHeY12, KD12a, LSL12b, LLY+18, LP12, LD13, MM17a, MR16, MZ12, NGAuHQ16, NC12, NXH+18, pNyWyY+14, OWHS12, RS16, RP12, RR11, RGM18, SAA15, SLGZ12, SS17b, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, yWpNyY+14, WXL+17, yWXYZ+18, WK18, tWmC12, XNG+14, XNRG15, XNP+18, YWNW15, YPR17, YKK+18, YYO15, ZXZ+11, ZWW17, ZWZH17a, ZWZHb, ZHS10, AP10, AIA+18a, AIA+18b, AIM+19, AM19, AMK12, BWR12b, BW13, BWA13, CCLL11, CT11a, CSS+13, GZHD12, GA11, HAK19, HKA+18, HURU11, HKB14, HWYW14, HLP+19, JK13, KMG17, KPS10, KJN+16, KM11, LSR13, LXM11, LLHS12, Lin14a, LWY12, MMD13, MM14a, MO14, MK11].

watermarking [NC13, PTK14, PWLL13, PWW10, PGLL10, PKS18, PC14, PPR+12, RS17c, SKS+18, Tay14, TK14, TLP10, TPK12, WLDB11, yWpNyL11, Wan13, yWpWpYpN13, WZLW13, YWT+12, ZKKA17, ZSMS18].

Watermark-Encryption [SLGZ12].

Watermarks [GL10, YT12]. WAVE [BMM12]. WAVE-enabled [BMM12].


Wearout [DFKC17]. web [GP+12, IMB17, KRM+10, KGO10, MWW+18, YYY+19, ATKH+17, BS12, BKJP12, CLB19, CTC+15, CFST17, CD12, DR11, Fra16, HSC19, HGOZ19, HCM11, HVP+18, NDS17, QF19, SP15a, SPM+13, ZGC16].


Wilderness [Acz11]. Will [Mos18, Dya19, Fat19, Nor17, Pec17]. win [Smi11a]. Window [TX16, Khl18, Win17, YWYZ12]. windows
Wireless-Charging-Based [CKHP19].
wiretap [BCDN17].
Wiring [HTZR12].
Wise [CG14a, SSA13].
WISP [PPH12].
Withholding [BRS17].
within [HSC19, KLN15].
Without [ASS15, CCL+13, FTC14, GS+W16, GSK17, LTC+15b, NA10a, YLQ09, YL13, ARM15a, AZH11, BT12, BF11, BV14, CCW+10, CJL16, CFG+17, DCA18, FSX12a, GH11a, GST12, GLM+16, HDPC13, ISC+16, KZZ17, LLY15, LGWY12, Par18, RG10, SYL13, SLZ12, TAKS10, WWYY11, XQL11, XHM14, YS12, YKC+11, YFK+12, ZY17b, ZYM18].
Witness [CXWT19, GGHW17].
Witness-based [CXWT19].
WLAN [KAHKB17].
woman [Fag17].
Women [Abb12, Hea15, McK10, Mck11, Mck12, Mun17].
Word [WW12, SCR19b].
word-independent [SCR19b].
Word-Oriented [WW12].
Words [GDM16, KM10a, SAM+19b].
Work [Gol19, RS11, Shp10, Tay14, BG14, HPJ+19, Sch15a].
workbench [CFH+13].
workflows [BPP10].
working [Wat14b].
Workload [BCO13].
Workshop [MV12, Sen10, Yan11].
Workshops [DDS12].
World [Ano16j, Ano17d, ABL+18, BFK16, BPS16, BLU+15, FKS+13, KM10c, LLM18, MDMJ17, Tom16, Con12, GJ+12, Goo12, LCKBJ12, Pec17, Pet11, Rom11, Sch15c, Zet14, Mun17].
world-class [Goo12].
Worm [CWXY16, WWC+11].
Worst [BIKK14].
would [McG11].
Wrapped [KM15, KM16].
Write [LLPY19, YNQ15, ZHZ+19].
Write-Efficient [YNQ15].
Writing [DKL+19, LT14b].
wrong [LHA+12b, UK18].
WSN [DL12, JLZ18].
WSNs [ARWK19, ABB19a, YLSZ19, ZYL+10].
Wu [LLK10].
WW2 [Don14].
Wyner [ADG16].

X [Smi11a, Tur18].
X25519 [TV19].
X.998 [Ano11b].
X.998-2010 [Ano11b].
XML [BPP10, CH11, GA11, SM19b].
XMSS [BDH11, HRB13, HBG+17].
XOR [App13, LZZ+19a].
XOR-Based [LZZ+19a].
XTEA [CWP12, IS12].
XTS [Mar10c].
XVIII [Sch15a].

Yamamoto [Car11].
Yan [Cot12b].
Yao [GKS17].
YCbCr [RMG18].
Years [DR10, BCV12].
Yehuda [Ful10].
Yen [LLK10].
yoking [HLS18].
Young [Söd13].
Yuan [FSM12a].
YubiKey [Jac16].
Yves [Ter11].

Z [JSM+18, Tur18].
z13 [ACD+15].
Zero [AMH+16, BSCTV17, BW12, CLP13a, COP+14, FMA+19, GO+13, GOS12, IW14, LKBK19, LLM+19, MX13, MBC+18, MT12, OOR+14, Pan14, SJ12, WCL+18, YCL17, Zet14, AIA+18a, AIA+18b, CJL16, HKA+18, KPP16, MDHM18, TLL13, WWBC14].
Zero-
Correlation [BW12, YCL17, WWBC14].
Zero-Knowledge [CLP13a, GOS12, IW14, MX13, MBC+18, MT12, Pan14, LLM+19, KPP16, MDHM18].
Zero-Watermark [SJ12, TLL13].
zero-watermarking [AIA+18a, AIA+18b].
Zynq [ZAAB17].

References

Akyildiz:2014:OTB


Applebaum:2017:AC


Abouaroek:2019:NAU


Aditya:2019:ISF


Abo-alian:2016:KDB

Ambrosin:2016:FAB


Albertini:2014:MHE


Ahmad:2019:PQE


Akdogan:2019:SKA


Arora:2012:ILM


REFERENCES

CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Ateniese:2017:LCS


Agrawal:2018:RLR


Ambrosin:2017:OBB


Adrian:2015:IFS


Adrian:2019:IFS


[ABF14] José Bacelar Almeida, Manuel Barbosa, Jean-Christophe Filliâtre, Jorge Sousa Pinto, and Bárbara Vieira. CAOVerif: an open-source deductive verifica-

**Ananth:2013:SFP**


**Avoine:2016:SSP**


**Aid:2013:DIO**


**Acar:2013:SPA**


**Archer:2018:KDR**

David W. Archer, Dan Bogdanov, Yehuda Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart, and Rebecca N. Wright. From

Andreeva:2012:SAS


At:2017:LAU


Archer:2016:MPP


Arapinis:2012:RET


Arapinis:2013:PSC

Myrto Arapinis, Sergiu Bursuc, and Mark Ryan. Privacy-supporting cloud computing by in-browser key translation. Journal


REFERENCES


**Armando:2013:AFB**


**Arnold:2015:NGH**


**Anastasiadis:2018:BTA**


**Amoah:2016:FMA**


**Ardagna:2010:ECP**

Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer,

Arias-Cabarcos:2019:SAA


ACM:2010:PAI


Avoine:2012:PFS


Austrin:2017:ICT


Aceto:2019:MME

Giuseppe Aceto, Domenico Ciuonzo, Antonio Montieri, and Antonio Pescapè. MIMETIC: Mobile encrypted traffic classifi-

Aczel:2011:SWL


Alvarez-Cubero:2016:AVL


Aizatulin:2012:VCC


Ayday:2012:DAA


Aliberti:2016:RPS


[ADMM16] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek. Secure multiparty computations on Bitcoin. Communications of

Araldo:2018:CEC

Anandakumar:2018:RHA

Ahmed:2017:IRD

Attrapadung:2015:RGS

Aminifar:2018:OME
REFERENCES


REFERENCES


REFERENCES

Amin:2016:DAP


Amin:2018:UAP


Altakrori:2019:AAA


Ali:2019:PRD

REFERENCES

Alhanahnah:2016:MTI


Almulla:2013:CKE


Anada:2017:CGS


Alam:2018:AFC


Ashraf:2014:MTG


Azarderakhsh:2014:NDP


Anada:2017:CGS


Alam:2018:AFC


Ashraf:2014:MTG


Azarderakhsh:2014:NDP


Almulla:2013:CKE

REFERENCES

4275–4301, October 2017. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).


REFERENCES


Asharov:2013:FCF


Alzahrani:2019:SAC


Araghi:2019:EHI


Awad:2016:SSZ


Arnedo-Moreno:2010:JRA


Arsalan:2012:IRW

Muhammad Arsalan, Sana Amien Malik, and Asifulullah Khan. Intelligent reversible watermarking in


REFERENCES

http://eprint.iacr.org/2013/446.

**Aumasson:2014:HFB**


**Ahmadian:2010:PDS**


**Alvarez:2012:CAB**


**Albrecht:2012:SDL**


**Arshad:2015:SAI**

Hamed Arshad and Morteza Nikooghadam. Security analysis and improvement of two authentication and...


Anonymous:2010:NDS

[Ano10a]

Anonymous:2010:MML

[Ano10b]

Anonymous:2011:AIS

[Ano11a]

Anonymous:2011:AXL

[Ano11b]

Anonymous:2011:MCB

[Ano11c]

Anonymous:2012:SHS

[Ano12]

Anonymous:2013:CFF

[Ano13a]
Anonymous: 2013: CRR


Anonymous: 2013: DSS


Anonymous: 2013: NCI


Anonymous: 2013: SSD


Anonymous: 2013: ERE

Anonymous:2014:TPC


Anonymous:2015:BSU


Anonymous:2015:BRDa


Anonymous:2015:CEB


Anonymous:2015:QCS


Anonymous:2015:UGB

REFERENCES

Anonymous:2016:BRBa

Anonymous:2016:EMT

Anonymous:2016:FVM

Anonymous:2016:GUP
Anonymous:2016:IICd


Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

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

Anonymous:2017:BRM


Anonymous:2017:CCS

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:2019:GES**


**Anonymous:2019:HCC**

Anonymous:2019:PBT


[Ano19c]

Anthes:2014:FTI


[Ant14]

Andriotis:2013:JSD


[AOT13]

Agarwal:2010:BRW


[AP10]

Aumasson:2011:CHF


[AP11]

AlFardan:2013:LTB


[AP13]

Abellan:2018:FCQ


[AP18]
129

REFERENCES

Ali:2018:SUA


Alcaide:2013:AAP


Applebaum:2013:GXG


Applebaum:2014:CCP


Appel:2015:VCP


Albrecht:2015:FBR

REFERENCES


Al-Qarni:2012:EII


Al-Qurishi:2018:EKA


Adj:2014:SRC

Altawy:2018:SLT


Altawy:2018:TCM


Agudo:2013:PAC


Abdulrahman:2015:NRR


Azarderakhsh:2015:PHS


Armasu:2019:IFA

Ambrose:2012:RII

Alghamdi:2019:RAM

Artemenko:2017:PGO

Asharov:2016:LPI

Asharov:2014:TCC
REFERENCES

Al-Sinani:2012:UCB


Ahmadi:2011:SKC


Ahmadi:2012:SKE


Asaar:2015:IBM


Alharbi:2018:CME

Rawan Alharbi, Tammy Stump, Nilofar Vafaie, Angela Pfammatter, Bonnie Spring, and Nabil Alshurafa. I can’t be myself: Effects of wearable cameras on the capture of authentic behavior in the wild. *Proceedings of the ACM on Interactive, Mobile, Wearable
REFERENCES


Al-Tariq:2017:SFP


Alam:2015:ACF


Aslan:2016:DEM


Abdalla:2012:LRS


Abdou:2018:SLV

REFERENCES


[AY14a] Tahir Ahmad and Usman Younis. Randomness testing of non-cryptographic hash functions for real-time


Alavi:2014:RQE


Barcellos:2018:RSP


Behnia:2013:IEB


Blaner:2013:IPP


Brennan:2012:ASC


Bai:2010:RKI

L. Bai. A reliable $(K, N)$ image secret sharing scheme with low infor-
REFERENCES

Bailin:2012:ERG


Berbecaru:2010:FSM


Barbay:2012:BRB


Barthe:2015:HAC


Barker:2016:RKM


Bartkewitz:2016:LPL


REFERENCES


REFERENCES


Bernstein:2017:SRD


Boldi:2012:IUG


Bingol:2019:EPP


Bollman:2015:PWI


Behrad:2020:NSA


Bernstein:2011:PCI

Daniel J. Bernstein and Sanjit Chatterjee, editors. Progress in Cryptology — INDOCRYPT 2011: 12th International
REFERENCES

144


REFERENCES


Boche:2017:CQA


Badrignans:2010:SSA


Balfanz:2012:FA


Bugliesi:2015:ART


Bana:2019:VMC


Bana:2020:VMC


**Buhrman:2014:PBQ**


**Bahri:2016:CCO**


**Bugliesi:2015:CPB**


**Benedetto:2010:DQE**


**Bahri:2012:SCS**


**Borghoff:2012:PLL**

Julia Borghoff, Anne Can-


REFERENCES


[Bitansky:2017:VGB] Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and
REFERENCES


**Bernstein:2014:CKR**


**Basin:2012:PRI**


**Basin:2015:ISC**


**Boche:2019:SMT**

Bicakci:2013:LSS


Botta:2014:PCI


Boyle:2014:EO


Basso:2011:BWC


Bessani:2013:DDS


Blasco:2016:SWB

REFERENCES

[Biddle:2012:GPL]

[Barker:2015:RKM]

[Belkacem:2014:DCM]

[Bruguera:2019:GEI]

[Bender:2012:DSP]
Bhasin:2015:EFB

Buchmann:2011:XPF

Biryukov:2016:ANG

Bernstein:2011:HSH

Barbareschi:2019:PBM
[BDL+19] Mario Barbareschi, Alessandra De Benedictis, Erasmo La Montagna, Antonino
Barbareschi:2018:PBH


Belkhouja:2019:BBA


Bossuet:2016:EPA


Bendlin:2011:SHE


Bertoni:2011:CSF

REFERENCES

[Bertoni:2012:KIO]

[Boldyreva:2012:SSE]

[Bottarelli:2018:PCW]

[Beebe:2017:MFC]
Nelson H. F. Beebe. The Mathematical-Function Computation Handbook: Pro-
gramming Using the MathCW Portable Software Library.
Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2017. ISBN 3-319-
64109-3 (hardcover), 3-319-
64110-7 (e-book). xxxvi +
1114 pp. LCCN QA75.5-
76.95. URL http://www.
springer.com/us/book/
9783319641096.

Bellovin:2015:WRC
Steven M. Bellovin. What
a real cybersecurity bill
should address. IEEE Se-
curity & Privacy, 13(3):
92, May/June 2015. CO-
DEN ????. ISSN 1540-7993
(print), 1558-4046 (elec-
tronic). URL http://ww
www.computer.org/csdl/
mags/sp/2015/03/msp2015030092.

Bellovin:2016:EEE
Steven M. Bellovin. Easy
email encryption. IEEE Se-
curity & Privacy, 14(6):
96. November/December
2016. CODEN ????. ISSN
1540-7993 (print), 1558-
4046 (electronic). URL
https://www.computer.
org/csdl/mags/sp/2016/
06/msp2016060096.html.

Bellovin:2018:UAE
Steven M. Bellovin. Usenet
authentication, and engi-
neering (or: Early design
decisions for Usenet).
Web article., February 23,
columbia.edu/~
smb/blog/2018-02/2018-
02-23.html.

Beltran:2018:IAA
Marta Beltrán. Identifying,
authenticating and authoriz-
ing smart objects and end
users to cloud services in
Internet of Things. Computers &
Security, 77(?):595–611,
August 2018. CODEN
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://ww
www.sciencedirect.com/
science/article/pii/S0167404818301366.

Bellovin:2019:LI
S. M. Bellovin. Layered
insecurity. IEEE Secu-
curity & Privacy, 17(3):96–
95, May/June 2019. ISSN
1540-7993 (print), 1558-
4046 (electronic).

Bajard:2016:MFA
Jean-Claude Bajard, Julien
Eynard, and Nabil Mer-
kiche. Multi-fault at-
tack detection for RNS
cryptographic architec-
ture. In Montuschi
et al. [MSH†16], pages 16–
ISSN 1063-6889. LCCN
URL http://ieeexplore.
ieee.org/servlet/opac?
puumber=7562813.
REFERENCES


[BF11] Nick J. Bouman and Serge Fehr. Secure authentication from a weak key, without leaking information. *Lecture Notes in
REFERENCES

157

Bas:2012:BLK

Bos:2019:ACI

Bhargavan:2012:VCI

Barthe:2014:PRV

Bobba:2010:ABM

Bhargavan:2016:MVP
Karthikeyan Bhargavan, Cedric Fournet, and Markulf

Beimel:2012:SSS


Berger:2016:EGF


Boldyrevare:2014:MEW


Battistello:2012:TBA


Barthe:2012:CACb

REFERENCES

10.1007/978-3-642-33125-1_1.


port, Inria, CNRS, University of Lorraine; Foundation UPMC — LIP 6, CNRS UMR 7606; Crypto-Experts, Lorraine, France; Paris, France; Paris, France, November 25, 2013. 16 pp. URL http://eprint.iacr.org/2013/400.pdf.


Javed Barkatullah and Timo Hanke. Goldstrike 1: CoinTerra’s first-generation cryptoco
Breitner:2019:BNS


Bhattacharjee:2016:SWC


Behnia:2012:SEI


Bernstein:2015:SPS

Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing,
REFERENCES


Benhamouda:2019:SPD


Bosch:2014:SPS


Berman:2013:HPR


Berman:2018:CFC


Bonneau:2015:PEI


Biagioli:2012:CCS

Mario Biagioli. From ciphers to confidentiality: se-


REFERENCES

(8):082201, August 2016. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.


[BK12b] Adil Bouti and Jörg Keller. Securing cloud-based computations against malicious


REFERENCES


**Bidgoly:2016:MQV**


**Bernstein:2017:SCS**


**Blanchette:2012:BPC**


**Bai:2019:LMD**

Tong Bai, Jinzhao Lin, Guoquan Li, Huiqian Wang, Peng Ran, Zhangyong Li, Dan Li, Yu Pang, Wei Wu, and Gwanggil Jeon. A lightweight method of data encryp-


References


Bhattacharya:2018:UPC


Benamara:2016:ICA


Baldwin:2010:AFI


Bartoli:2019:VEW


Biswas:2012:IBA


Backes:2012:GCP

REFERENCES

[172]

Banik:2012:DFA


[BN14]

Babamir:2014:AKP


[BNNH19]

Baskaran:2019:TEL


[BNST17]

Bunder:2017:GAR

Martin Bunder, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien. A generalized attack on RSA


REFERENCES

174

DEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL
https://cacm.acm.org/
magazines/2019/1/233522/
fulltext.

[BOP14] Kyle O. Bailey, James S. Okolica, and Gilbert L. Peterson. User identifi-
cation and authentication using multi-modal behav-
ioral biometrics. Computers & Security, 43(??):77–
89, June 2014. CODEN CPSEDU. ISSN 0167-4048
www.sciencedirect.com/
science/article/pii/S0167404814000340.

[Bor10] Julia Borghoff. Cryptanal-
ysis of lightweight ciphers.
Ph.D. thesis, Department of Mathemat-
ic University of Denmark,
Lyngby, Denmark, 2010. x
+ 198 pp.

surprises do identical twins
have for identity science?
Computer, 44(7):100–102,
ISSN 0018-9162
(print), 1558-0814
(electronic).

[Boy13] Xavier Boyen. Attribute-
based functional encryp-
tion on lattices. Lecture
Notes in Computer Science,
CODEN LNCS09. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-36594-2_8/.

[Boy16] Griffin Boyce. Bake in
.onion for tear-free and
stronger Website authen-
tication. IEEE Security
& Privacy, 14(2):15–21,
March/April 2016. CO-
DEN ????? ISSN 1540-7993
(print), 1558-4046
(electronic).

[BP06] Janet Beissinger and Vera
Pless. The Cryptoclub: Us-
ing Mathematics to Make
and Break Secret Codes. A.
K. Peters, Ltd., Wellesley,
MA, USA, 2006. ISBN
1-56881-223-X. xvi +
199 pp. LCCN QA40.5
.B45 2006. URL http:
//www.loc.gov/catdir/
toc/ecip067/2006002743.
hmtl.

[BP10] Randal Burns and Zachary
Peterson. Security con-
structs for regulatory-
compliant storage. Com-
munications of the As-
sociation for Computing
Machinery, 53(1):126–130,
January 2010. CODEN
REFERENCES

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

Bohli:2011:RAP


Budroni:2018:HGB


Bencsath:2012:CSD


Brooke:2010:DCX


Bellare:2014:SSEa


Bellare:2014:SSEb

REFERENCES


[Bre18] R. Brewster. Re-creating the first flip-flop — a fundamental component of computers turns 100 [resources hands on]. *IEEE*
REFERENCES


REFERENCES


REFERENCES

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


REFERENCES

December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Boorghany:2015:CIL

Bojinov:2014:NMC

Basin:2011:AIS

Beaulieu:2013:SSF

Batina:2012:HEB
REFERENCES


REFERENCES

Blasco:2015:HDT


Brocardo:2015:AVM


Buchmann:2010:EKG


Budiansky:2016:CWN


Bulygin:2010:AOP


Bulygin:2010:CAC

Bultan:2018:SCA


Burke:2011:AMD


Butin:2017:HBS


Brakerski:2011:EFH


Bitansky:2018:IOF


Bayrak:2012:AII

References


REFERENCES


REFERENCES


Bock:2016:NDA


Staff:2014:KYS


Caldwell:2013:INP


Chakraborty:2019:TIP


Carter:2010:TB


Carlson:2011:JRW


Casselman:2010:VC


[Chen: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 imple-
REFERENCES


REFERENCES

Checkoway:2016:SAJ

Chadha:2012:AVE

Chatterjee:2016:TAD

Chou:2013:UGS

Cao:2019:AML
REFERENCES


REFERENCES


REFERENCES


REFERENCES

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

Chari:2010:DSC


Cui:2018:ABC


Cui:2019:ABS


Coras:2016:AML


Costello:2014:CAS


Cremers:2019:SAG

REFERENCES


[Carter:2013:SSA] Kyle Carter, Adam Foltzer,

**Centenaro:2013:TBA**


**Checkoway:2014:PDE**


**Cevallos:2012:USR**


**Carstensen:2011:AAA**


**Calzavara:2017:SWJ**


REFERENCES

Cheraghchi:2014:NMC

Corrigan-Gibbs:2014:KS

Chaudhuri:2010:PIC

Caballero-Gil:2012:LAR

Chmiel:2012:EPC

Coull:2011:ACO
REFERENCES

10:1–10:??, May 2011. CO-
DEN ATISBQ. ISSN 1094-
9224 (print), 1557-7406
(electronic).

[Cohney:2017:PSR] Shaanan Cohney, Matthew D.
Green, and Nadia Heninger. 
Practical state recovery at-
tacks against legacy RNG
implementations. Report, 
University of Pennsylva-
nia and The Johns Hop-
kins University, College
Park, PA and Baltimore,
MD, October 23, 2017. 
15 pp. URL https:/
duhkattack.com/paper.
pdf.

[Curtmola:2011:SSE] Reza Curtmola, Juan 
Garay, Seny Kamara, and 
Rafail Ostrovsky. Search-
able symmetric encryp-
tion: Improved definitions
and efficient constructions.
Journal of Computer Se-
curity, 19(5):895–934, ???
2011. CODEN JCSIET. 
ISSN 0926-227X (print), 
1875-8924 (electronic).

[Cheng:2012:PAI] Pengqi Cheng, Yan Gu, 
Zihong Ly, Jianfei Wang,
Wenlei Zhu, Zhen Chen,
and Jiwei Huang. A per-
fomance analysis of iden-
tity-based encryption
schemes. Lecture Notes in 
Computer Science, 7222: 
289–303, 2012. CO-
DEN LNCSD9. ISSN 
0302-9743 (print), 1611-
3349 (electronic). URL 
http://link.springer.
com/chapter/10.1007/978-
3-642-32298-3_19/.

Goyal, Ryan Moriarty, and 
Rafail Ostrovsky. Position-
based cryptography. SIAM 
Journal on Computing, 43 
CODEN SMJCAT. ISSN 
0097-5397 (print), 1095-
7111 (electronic).

[Cheng:2013:NIB] Xiangguo Cheng, Lifeng 
Guo, Jia Yu, Huiran Ma, 
and Yuexiu Wu. A new 
identity-based group sign-
nature scheme. International Journal of Compu-
ter Applications, 35(1): 
1–5, 2013. CODEN IJ-
CAFW. ISSN 1206-212X 
(print), 1925-7074 (elec-
tronic). URL https://
www.tandfonline.com/

[Chen:2010:NUP] Tzung-Her Chen and Jyun-
Ci Huang. A novel user-
participating authentica-
tion scheme. The Journal 
of Systems and Software, 
CODEN JSSODM. ISSN 
0164-1212.


[Che15] Yu-Chi Chen. SPEKS: Secure server-designation public key encryption with keyword search against...

[Chen:2017:CSQ]

Chen:2017:CSQ


[Chen:2018:ESA]

Chen:2018:ESA


[CHHW12]

CHHW12


[CHH+13]

CHH+13


[Cui:2019:CPA]

Cui:2019:CPA


[Chi12]

Chi12

Hung-Yu Chien. Improved anonymous multi-

**Chien:2013:CRC**


**Chirgwin:2013:ABB**


**Chien:2016:GAI**


**Conti:2019:BUB**


**Chmielowiec:2010:FPR**


**Cohen:2018:WCC**

Choudary:2010:SCD


Chou:2014:EMA


Chen:2011:SEI


Chu:2016:BEE


Chen:2013:ATK

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


[Cilardo:2011:EPT]

[Cil11]

[CJ13]

[CJF14]

[CJFH14]

[Cheon:2016:ANP]

[Cho:2012:CBF]

[Cho:2015:CBF]
Jung-Sik Cho, Young-Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mu-

Cui:2013:OSL


Chandra:2011:AST


Chailloux:2017:PLQ


REFERENCES

Calegari:2019:WPH

Chen:2019:BBS

Comon-Lundh:2010:DSP

Chang:2011:RSB

Chen:2017:PGF

Chong:2013:ASG
REFERENCES


Chen:2012:NCB


Chen:2013:TSE


Chande:2016:NSC


Cao:2012:SRH


Chen:2019:IBS

Jiahui Chen, Jie Ling, Jianting Ning, and Jintai


[Kaidi Cao, Jing Liao, and Lu Yuan. CariGANs: unpaired photo-to-caricature translation. *ACM Trans-
REFERENCES


Cheng:2017:ISK
[CLZ+17]

Cremers:2011:OSV
[CM11]

Cozzens:2013:MEE

Cui:2014:SSA

Checkoway:2018:WDL
Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. Where did I leave my keys?: lessons from the Juniper Dual EC incident. Communications of the Association for Computing Machinery, 61(11):148–155,


Cao:2016:OMA


Chatterjee:2017:IPB


Chen:2012:FAA


Chaudhry:2018:IRB


CNRS:2014:NAS


Coron:2012:PKC

Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi. Public key compression and modulus switching for fully homomorphic encryption over the integers. *Lecture Notes in Computer Sci-
REFERENCES


Lucian Constantin. The SHA1 hash function is now completely unsafe: Researchers have achieved the first practical SHA-1 collision, generating two PDF files with the same signature. ComputerWorld, ?? (?):??, February 23, 2017. CODEN CMPWAB. ISSN 0010-4841. URL https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html.


REFERENCES


[Rachel Courtland. Vir-


Chen:2012:DCC


Crampton:2011:PEC


Cramer:2012:TCT


Craver:2014:UCC


Clear:2012:CPA


Crichlow:2016:RSE

Crawford:2013:FCT

Chauhan:2018:PCD

Culnane:2015:VVV

Caranay:2010:ESP

Chhabra:2011:NSN

Clark:2012:RLA
REFERENCES


Chen:2017:SIE

[CSST+C17]  

Ciegis:2016:ADP

[CSTR16]  

Chong:2015:SID

[CSV15]  

Chow:2012:EPV

[CSW12]  

Chen:2018:SIA

[CSYY18]  

Chen:2011:IBT

[CSZ+11]  
REFERENCES

Chen:2011:ARI


Chen:2011:TVS


Canard:2018:CPK


Calzavara:2015:SLA


Chin:2013:SMB


Chang:2012:GBP


Chou:2013:TIB


Cao:2014:PPM


Chen:2012:IDC


Chen:2012:CKS


Chen:2016:EPN


Chen:2016:WPM

REFERENCES

ISSN 1532-0626 (print), 1532-0634 (electronic).


Chen:2014:CSI


Dharwadkar:2010:SSG


Djebbar:2012:ASB


Darivandpour:2018:ESP


Danezis:2012:FCDb

REFERENCES


[DCAT12] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad.

**Cordeiro:2016:MPG**


**Cordeiro:2012:IMB**


**Ding:2018:NPH**


**DePrisco:2013:CVC**


**DARco:2014:MIC**

P. D’Arco, R. De Prisco, and A. De Santis. Measure-independent characterization of contrast opti-


[DDFR13] DaRolt:2013:NDS


[DSS12] Danezis:2012:FCDa

George Danezis, Sven Dietrich, and Kazue Sako, editors. Financial Cryptography and Data Security: FC 2011 Workshops, RL-CPS and WECSR 2011, Rodney Bay, St. Lucia,

Dai:2019:SAM


DeOliveiraNunes:2019:SSC


derhans:2010:USC


Desmedt:2010:CF


Desmedt:2010:ES


Dew:2011:BRB

Nicholas Dew. Book review: The Information
REFERENCES


Durmuth:2011:DEN

DuPont:2016:ECC

DeCapitaniDiVimercati:2017:AMM

Deng:2017:LLH

Ding:2012:CLS
Lin Ding and Jie Guan. Cryptanalysis of Loiss stream cipher. The

DeCapitaniDiVimercati:2010:EPR
Djuric:2015:FSF


Dutta:2017:EFC


Dickens:2018:SCI


Dupressoir:2014:GGP


Drucker:2018:FMB


Dolev:2019:AAC

Shlomi Dolev, Niv Gilboa, and Ximing Li. Accumu-


[Dang:2019:SBS] Van Tuyen Dang, Tuong Thu Huong, Nguyen Huu Thanh, Pham Ngoc Nam, Nguyen Ngoc Thanh, and Alan Marshall. SDN-based SYN


[DJG+15] Lin Ding, Chenhui Jin, Jie Guan, Shaowu Zhang, Ting Cui, Dong Han, and Wei Zhao. Cryptanalysis of WG family of stream ciphers. *The Computer Journal*,
Domnitser:2012:NMC


Delfs:2002:ICP


Dolev:2012:ATC


Delfs:2015:ICP


[Doychev:2015:CTS]

[Dodis:2012:MAR]

[Dong:2012:UAS]

[DeLuca:2015:SUS]


[DKS12]
Orr Dunkelman, Nathan
Dinur:2017:IGA


Deng:2019:DMS


Degefa:2016:PSE


Djaziri-Larbi:2018:WDA


Dong:2013:PRS


DiPietro:2016:CLD

Diodis:2011:SSC


Dai:2016:MLR


Duan:2016:SDC


DeCarneDeCarnavalet:2015:LSE


Daneshgar:2018:SSS


DeMarsico:2019:SGR


Dong:2018:SSM

[Y. Dong, Ana Milanova, and Julian Dolby. Se-

DiPietro:2010:HKS


Drozdz:2019:SCC


Diesburg:2016:TLA


Dwivedi:2018:DLR


Dimitrakakis:2015:ELA


Demme:2012:SCV

John Demme, Robert Martin, Adam Waksman, and Simha Sethumadhavan. Side-channel vulnerability factor: a metric for mea-
REFERENCES


**David:2012:UCO**


**Donovan:2014:ATM**


**Doroz:2015:AFH**


**Duncan:2012:CAI**


**Ding:2017:CSM**


**Das:2016:CWM**

Dziembowski:2018:NMC


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE

REFERENCES

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

Dasgupta:2016:TDA


Dixon:2016:NTO


delRey:2012:EDI


Dini:2011:LLA


Dixit:2019:FBD


Das:2015:DCS

REFERENCES

Das:2016:MPU  

Das:2012:DPB  

Deng:2018:SFE  

Dachman-Soled:2014:COF  

Dodis:2014:HEY  
Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too — optimal recovery strategies for compromised RNGs. Report, Dept. of Computer Science, New York University; Dept. of Computer Science and Applied Mathematics, Weizmann Institute; Dept. of Computer Science, Northeastern University, New York, NY, USA; Tel Aviv, Israel; Boston, MA, USA, March 3, 2014. 27 pp. URL http://eprint.iacr.org/2014/
REFERENCES

Deng:2012:VIA

Dunkelman:2012:MEK

Dunkelman:2012:TCC

Dodis:2017:HEY

Dini:2013:HHS

Drosatos:2017:PET


Durcheva:2015:SAI


David:2012:PRE


Dorn:2012:ECE


Dong:2012:KKD


Dong:2012:NDI


Dai:2018:OPC

Wei Dai, William Whyte, and Zhenfei Zhang. Opti-


Lunzhi Deng and Jiwen.

**Dong:2016:EPP**


**Doss:2012:MDA**


**Delledonne:2018:CDA**


**Dent:2010:PS**


**Eslami:2011:SIS**

Z. Eslami and J. Zar epour Ahmadabadi. Secret image sharing with authentication-chaining and

**Erguler:2012:PAI**


**Ekberg:2012:AEP**


**Ehdaie:2016:HCR**


**Elrabaa:2019:PPP**


**Erbagci:2019:SHE**

Ermis:2017:KAP


Egele:2013:ESC


Esiner:2017:QRI


Esiner:2019:TFA


Edwards:2014:NRP


Edwards:2017:NSQ

El-Emam:2013:NSA

Espitau:2018:LAF

Eisenbarth:2012:CIP

El-Hadedy:2019:RPR

Eisenbarth:2010:CCE

Esiner:2016:FFB
[EKB+16] Ertem Esiner, Adilet Kachkeev, Samuel Braunfeld, Aliptekin Küpçü, and Öznur Özkasap. FlexD-PDP: Flexlist-based opti-

[Emura:2019:PPA]


[Elb09]


Evtyushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC


Engels:2012:HLA


Ebadi:2015:DPN

Essex:2017-DDU


Eibach:2010:OGB


Eldib:2014:FVS


Eyal:2017:BTT

Enos:2015:IBS

Emmart:2018:FME

Farash:2014:ECC

[FAA+18]

Faal:2019:MVE
Hossein Teimoori Faal. A multiset version of even-odd permutations iden-
REFERENCES


[FCM14] Luca Ferretti, Michele Colajanni, and Mirco

**Fuglerud:2011:SIA**


**Fang:2019:PPO**


**Fehr:2010:QC**


**Feigenbaum:2019:PSE**


**Felten:2013:LBA**


**Faugère:2010:CLR**

REFERENCES


REFERENCES

Fan:2018:MBP


Fan:2013:CPP

Fan:2010:PSN


Fan:2010:AMI


Farras:2017:IRN


Faz-Hernandez:2019:HPI

Faz-Hernández:2018:FSI


Fahl:2012:WEM


Fan:2014:ASA


Fawzi:2013:LDN

Florencio:2016:PSD


Feng:2018:ABB


Fidler:2018:CCN


Farash:2015:PSE


Fisher:2015:CS


Fei:2012:GTK

REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-35362-8_14/.

Fotiadis:2019:TRF


Fan:2013:CEM


Fan:2014:RRS


Ferguson:2010:SHF

Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Todayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family. Report, (various), October 1, 2010. ii + vi
REFERENCES

Forler:2012:DAC


Fei:2016:PPA


Fei:2016:SEF


Feng:2012:CAO


Fallahpour:2015:AWB


Ferrag:2018:SCN

Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-

Fomichev:2019:PZI


Farwa:2018:FAI


Ferretti:2019:FBS


Faust:2014:CNM


Feng:2012:USD

REFERENCES


[FMTR12] Ferreira:2015:LPA


[Feng:2018:ALA] Wei Feng, Yu Qin, Shi-

Fiore:2015:EIB


Frattolillo:2016:BFM


Frey:2010:ABC


Fernandes:2017:ITS

Fridrich:2010:SDM


Frikken:2010:SMC


Fridrich:2012:MTS


Fritsch:2013:CPE


Fu:2016:EPS


Frauchiger:2013:TRR

REFERENCES


REFERENCES


REFERENCES

SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). See [KL08].

[FVBA18]

[Franken:2019:ECP]

[FVT+17]
Behrouz Fathi-Vajargah and Mohadeseh Kanafchian. Improved Markov chain Monte Carlo method for cryptanalysis substitution-transposition cipher. Monte Carlo Methods and Applications, 23(2):147–??, June 2017. CODEN MC-

[Fanyang2012:SAK]
Fanyang, Naixue Xiong, and Jong Hyuk Park. A self-adaptive K selection mechanism for re-

**Fu:2017:DFA**


**Feng:2011:VBF**


**Feng:2019:SHO**


**Fan:2015:IRD**

Fan:2013:KIS


**Fyodorov:2019:SGM**


**Fan:2013:KIS**

Fan:2013:KIS

Fan:2014:NCI


Fu:2012:EHA


Gross-Amblard:2011:QPW


GomezPardo:2013:ICM


Guimaraes:2019:OIQ

REFERENCES

ISSN 1532-0626 (print), 1532-0634 (electronic).


[GB19]

Gupta:2019:DRB

Gorantla:2011:MKC

Guyeux:2015:ECS

Gao:2019:LBD

Gupta:2012:CDF
Gupta:2013:HPH


Gupta:2013:HPH

Gong:2016:ATI


Gong:2016:ATI

Guerin:2016:TDU


Guerin:2016:TDU

[Giot:2011:UKD]


[GG10] Guang Gong and Kis-

**Grigg:2011:CCN**


**GGH+16a**


**Garg:2016:HSS**


**Garg:2014:TRS**


**Garg:2017:ID1**

REFERENCES


[GH12] Lifeng Guo and Lei Hu. Efficient bidirectional proxy re-encryption with direct chosen-ciphertext security. *Computers and
Genge:2019:ESA


Gordon:2011:CFS


Gentry:2012:RSB


Gentry:2013:FSB


Gentry:2012:FHE


Gilad:2014:PHI

Yossi Gilad, Amir Herzberg, and Haya Shulman. Off-path hacking: The illusion of challenge–response


References

Guo:2019:NBT

Gravier:2015:WOD

Goyal:2013:CZK


Gu:2015:EIB

Geetha:2018:OVC


Guo:2010:HMW


Gouvea:2012:HSI


Gu:2019:GRM


Glassey:2011:MIM


Gu:2018:KAA


Gorawski:2012:EAS


Gligor:2012:SLT

attribute authentication (transcript of discussion).


Gollmann:2010:SCR


Ge:2016:DSR


Guo:2018:PSC


Gagne:2012:AVB


Guo:2011:EDA

Gong:2016:HES
Linming Gong, Shundong Li, Qing Mao, Daoshun Wang, and Jiawei Dou.
A homomorphic encryption scheme with adaptive chosen ciphertext security but without random oracle.

Gupta:2019:OIT
Peeyush Gupta, Yin Li, Sharad Mehrotra, Nisha Panwar, Shantanu Sharma, and Sumaya Almanee.
Obscure: information-theoretic oblivious and verifiable aggregation queries.

Gerault:2018:RAR
David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon.
Revisiting AES related-key differential attacks with constraint program-
REFERENCES


REFERENCES

Gueron:2016:HIA


Gonzalez-Manzano:2017:EHE


Gonzalez-Manzano:2019:LUR


Gunson:2011:UPS


Giambruno:2015:GGB


Garcia-Martinez:2015:HEB

REFERENCES


REFERENCES


Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Guo:2018:WBS


Gonzalez-Serrano:2018:SML


Gupta:2018:SCA


Guha:2017:RTS

References

Guin:2016:FCS


Gutman:2016:EAF


Gong:2016:FSC


Gierlichs:2012:ICD


Genkin:2013:RKE


REFERENCES


REFERENCES

Greenberg:2014:GWB


Gebotys:2016:PCP


Gao:2019:EUE


Goh:2013:TOT


Wang:2014:RAW


Gao:2015:GCC

Guo:2019:EER


Guo:2012:AKE


Guo:2017:EMD


Gao:2019:VQS


REFERENCES

Hamamreh:2012:RPA


Hamlin:2017:NMC


Hamidi:2019:ADS


Hanyok:2012:EH


Harn:2013:GA


Harrington:2014:GEF


Hardesty:2015:BAC

REFERENCES

Hardesty:2016:SUC

Hastings:2016:SWS

Hayes:2013:NSA

Houmansadr:2013:BCN

Hurlburt:2014:BBC

Hetzelt:2017:SAE

Hernandez-Becerril:2016:GIS
REFERENCES

Han:2019:ABI


He:2013:HEH


Holsing:2017:XEH


Hao:2012:SAM


Hu:2017:ATE


Hwang:2010:RIB


REFERENCES


[Huang:2018:BLD]


[HCYZ18]

[Hosny:2019:RCI]


[HD19]

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

[HDWH12]


[Hea15]

Nick Heath. Hacking the Nazis: The secret story of the women who broke Hitler’s codes. TechRepublic, ??(?):??, March
Hwang:2012:ABA


Hamad:2018:DWU


Hanka:2011:DPK


Hermelin:2010:MLC


Hellman:2017:TLC

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


REFERENCES

307


[HGZO19] Joshua Hibschman, Darren Gergle, Eleanor O’Rourke, and Haoqi Zhang. Isopleth: Supporting sense-making of professional Web applications to create readily available learning experiences. *ACM Transactions on Computer-Human Inter-

Hanocka:2019:APS


**Hayashi:2013:AEI**


**Huber:2014:TPW**


**Huang:2017:BBC**


**Haitner:2011:PRI**


**Hong:2015:RSM**


**Huang:2018:LRD**

Jianye Huang, Qiong Huang, and Willy Susilo.


[HJ14a] O. Hasan and S. A. Khayam. Towards for-


REFERENCES

**Handa:2019:SES**


**Hanzlik:2019:CPC**


**Heyse:2012:LEA**


**Heil:2014:APH**


**Houmansadr:2014:NBW**


**Hur:2013:REC**

Howe:2018:PDG


Holenstein:2011:ERO


Harn:2010:AGK


Hazay:2010:EST


Hsieh:2012:EHF


Hsich:2012:EHF


[Ham:2018:IYP] HyoungMin Ham, JongHyup Lee, and JooSeok Song.


[Hohenberger:2012:DDQ] Susan Hohenberger, Allison Lewko, and Brent Wa-


**Hoang:2012:ESB**


**Hirt:2014:BA**


**Harnik:2010:CIC**


**Hodgson:2019:SSC**


**Hoffmann:2015:LBQb**


**Hoffmann:2016:LBQb**

Leah Hoffmann. Last byte: Q&A: Finding new directions in cryptography: Whitfield Diffie and Martin Hellman on their meeting, their research, and the results that billions use every day. *Communications of the Association for Com-


Halder:2010:WTR


He:2012:ECT


Hurrah:2019:DWF


Howe:2015:PLB

REFERENCES

Hoffstein:2008:IMC


Hur:2010:CCS


Han:2016:GGA

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

Han:2018:BEI


Han:2014:GTK


He:2013:GME

REFERENCES


Hisil:2019:KLF


Hulsing:2013:OPX


Herranz:2013:SMS

Hulsing:2016:MMT


Haitner:2010:EIC


Hwang:2011:CDA


Hubballi:2018:NTC


Homma:2014:TFD


Hall:2019:BIA

REFERENCES


[hSZZ15] Runhua Shi, Hong Zhong, and Shun Zhang. Comments on two schemes of identity-based user authentication and key agreement for mobile client-


Matthias Herbert, Tobias Thiene, Jan Zibuschka, and Heiko Roßnagel. Secure mashup-providing platforms — implementing encrypted wiring. *Lecture
REFERENCES


REFERENCES

Han:2012:MIA


Hammad:2019:PSF


Hwang:2011:NIB


Holbl:2010:TPI


Holbl:2012:ITP


He:2016:STI

REFERENCES


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


REFERENCES

Huang:2019:AIA


Huang:2011:GFT


Huang:2018:PIB


Hu:2019:CAC


Hao:2011:NTV

[HYS11] Rong Hao, Jia Yu, and Zhiling Song. A note on a threshold verifiable multi-secret sharing...
REFERENCES

Huang:2011:IBS

Heys:2011:PSC

Han:2012:ERI

Han:2014:ERI
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):1561–1573, June 10, 2014. CODEN CCPEBO. ISSN

Huang:2011:IBS

Huang:2018:CT

Huang:2011:IBS


Md Saiful Islam and Naif Alajlan. Model-based alignment of heartbeat


REFERENCES

Irshad:2017:CPP


IEEE:2010:PIA


IEEE:2011:ICI


IEEE:2015:ISS

Imanimehr:2016:HPR


Islam:2011:MDA


Iyengar:2016:SPS


Imai:2015:IRR


Islam:2015:LFP


Ioannou:2014:PKC

Lawrence M. Ioannou and Michele Mosca. Public-


SK Hafizul Islam, Mohammad S. Obaidat, Pandi Vijayakumar, Enas Abdulhay, Fagen Li, and M. Krishna Chaitanya Reddy. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Future Generation Computer*


Ognjen Joldzic, Zoran Djuric, and Pavle Vuletic.


Jiang:2019:SSL

Jiang:2016:MAC

Jiang:2017:BMA

Jin:2010:ADW
C. Jin. Adaptive digital watermark system using soft computation. *International Journal of Com-
REFERENCES


[Jun:2012:IIR] Jong Yun Jun, Kunho Kim, Jae-Pil Heo, and Sung eui Yoon. IRIW: Image re-
REFERENCES

Jiang:2016:PPT

Jovanovic:2012:FAL

Joseffson:2016:ECD

Jiang:2018:AHP

Jordan:2018:QCS
Jajodia:2012:RET

Jia:2012:PKD

Jiang:2016:OOC
Jiang:2016:UTC

Jain:2012:BAS

Jan:2017:PPB

Joux:2013:NIC
Antoine Joux. A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic. Report 2013/095, CryptoExperts and Université de Versailles Saint-Quentin-en-Yvelines, Laboratoire PRISM, 45 avenue des Etats-Unis, F-78035 Versailles Cedex, France,
REFERENCES


**Jin:2019:RPP**


**Jeffs:2013:CCP**


**Juels:2014:HEE**


**Jain:2018:MDN**


**Jaiyeola:2018:IPN**


**Jalili:2017:EAS**

Jevdjic:2017:ASC


Jain:2016:APQ


Jedmayr:2017:BCI


Jordan:2018:EPE


Jiang:2018:CPA

REFERENCES


Juels:2014:INC


Jiang:2017:SLD


Jiao:2019:AMC


Jin:2015:NCD


Joux:2014:SAC

Jiang:2010:EDI


Jan:2019:SEE


Kurkcu:2018:CBE


Kornycky:2017:RFT


Koziel:2018:HPS

REFERENCES

Kamp:2013:MES


Kamp:2016:MEM


Kammüller:2019:ATI


Kapera:2011:SPD


Kapera:2013:MRM


Karafyllidis:2012:QGC


Kong:2015:CSM

Katz:2013:RIB


Kawamoto:2015:LSH


Karthigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP


Kim:2011:SSE


Khan:2018:APS

Imran Khan, Shehzad Ashraf Chaudhry, Muhammad Sher, Javed I. Khan, and Muhammad Khurram Khan. An anonymous and provably secure biometric-based au-


REFERENCES


Kleinjung:2010:FBR


Kikuchi:2012:SSN


Kostic:2019:UNV


Kramer:2010:FDC


Kim:2012:SLT


K:2019:IAM

REFERENCES


Khedr:2016:SSH


Kwon:2010:SEB


Koo:2018:PPD


Khazaei:2010:NBS


Kastner:2010:AOT


Kim:2014:MBM

[KHHH14] Heeseok Kim, Dong-Guk Han, Seokhie Hong, and Jaecheol Ha. Message blinding method requiring no multiplicative inversion for RSA. ACM Transactions on Embedded Computing Systems,
References

Khleborodov:2018:FEC


Khalil-Hani:2013:BEB


Kinkelin:2011:UTS


Kim:2016:EPE


Kolsch:2019:SBP


Kai:2011:CIS

REFERENCES

???? ISSN 1932-2232 (print), 1932-2240 (electronic).

Kiayias:2011:TCC


Kompara:2019:REM


Kim:2011:LBA


Kim:2015:CEH


Kim:2016:MAS


Khan:2016:BSW

REFERENCES

Konstantinou:2010:RCI


Kawai:2012:SHS


Kawai:2013:SHS


Khalil:2014:CIM


Khan:2015:CMB

REFERENCES

[KKD+18]

[KKJ+16]

[KKG14]

[KKGGK10]

[KK+16a]
Jinsu Kim, Dongyoung Koo, Yuna Kim, Hyun-

Kim:2018:ARD


Koblitz:2011:ECC


Khan:2013:EDC


Khan:2014:IPR


Katz:2008:IMC

[Jonathan Katz and Yehuda Lindell. *Introduction*]
to modern cryptography: Principles and Protocols.
Chapman and Hall/CRC [KL15]
cryptography and network security. Chapman and

Kushwah:2011:EIB [Kla10]

Prashant Kushwah and Sunder Lal. An efficient
identity based generalized signcryption scheme. Theoretical Computer Science,

Khakpour:2013:ITA [KLC+10]

Amir R. Khakpour and Alex X. Liu. An information-
theoretical approach to high-speed flow nature

Katz:2015:IMC

Jonathan Katz and Yehuda Lindell. Introduction
to modern cryptography. Chapman and hall/CRC
cryptography and network security series. Taylor and

Klapper:2010:PSS

Andrew Klapper. Pseudorandom Sequences and
Stream Ciphers, chapter 17, pages 1–23. Volume 2 of Atallah and Blan-

Ko:2010:MME

Jeonggil Ko, Jong Hyun Lim, Yin Chen, Rvázvan
Musvaloiu-E, Andreas Terzis, Gerald M. Masson, Tia
Gao, Walt Destler, Leo Selavo, and Richard P.
Dutton. MEDI$\text{S}$N: Medical emergency detection
11:1–11:??, August 2010. CODEN ????? ISSN 1539-9087.


REFERENCES


Koblitz:2015:RWE


Koblitz:2016:RWE


Kasamatsu:2012:TSE


Kandi:2017:ELC


Kline:2018:CAR


Kiyoshima:2014:CRB


REFERENCES

Knijnenburg:2017:PCE


Khovratovich:2010:RRA


Kobsa:2013:CJV


Kheiri:2014:CCV


Kumari:2016:APW


Koblitz:2010:BRB


Komargodski:2018:LRO

[Kom18] Ilan Komargodski. Leakage resilient one-way functions:

**Kasper:2012:SCA**


**Khamsemanan:2016:BBU**


**Kawachi:2017:GCR**


**Kollmitzer:2010:AQC**


**Kang:2012:AKM**

[Kolman:2017:SCG]

[Koya:2018:AHM]

[Kumar:2017:TAU]

[Kobusinska:2018:BDF]

[Kiltz:2011:EAH]

[Khalid:2016:RHL]
Ayesha Khalid, Goutam Paul, Anupam Chattopadhyay, Faezeh Abediostad, Syed Imad Ud Din, Muhammad Hassan, Baishik Biswas, and Prasanna Ravi. RunStream: a high-level rapid

**Kocabas:2012:CPB**


**Krenn:2013:CCR**


**Knudsen:2011:BCC**


**Krantz:2012:EAM**

[ Kra12 ] Steven G. (Steven George)

Kostinger:2012:SBL


Kostinger:2012:SBL

Kannan:2013:NQF


Krenn:2013:AWI


Kranz:2018:AAF


Khan:2010:RCB


Khan:2017:TPK

Kiljan:2017:SAC

Kwon:2018:CEI

Ksiezopolski:2012:QMQ

Klingler:2013:UPT


Kim:2012:SAH


Kawachi:2012:SKE

Akinori Kawachi, Hirotoshi Takebe, and Keisuke Tanaka. Symmetric-key encryption scheme with multi-ciphertext non-

**Kobayashi:2016:ASC**


**Klisowski:2012:CCP**


**Kai:2014:FSD**


**Kumagai:2010:UGS**


**Kupcu:2013:DTT**


**Kupcu:2015:OAS**

REFERENCES

[102x681] Kushner:2013:RSS


**Kuo:2016:SDD**


**Koyama:2012:NTD**


**Kamal:2010:EIN**


**Kreutz:2018:KPS**


**Kuo:2018:DRA**


**Kate:2010:PBO**

Kiayias:2017:EEV


Lu:2010:MSC


Lathey:2015:IEE


Lackey:2015:UHP


Lallie:2014:PCM


Liang:2015:SEC


REFERENCES


Laxmi:2017:GGS


Liu:2015:IEP


Lathrop:2011:SPI


Lavington:2012:ATH

S. H. (Simon Hugh) Lavington, Martin Campbell-Kelly, Christopher P. Burton, and Roger Johnson, editors. Alan Turing and his contemporaries: building the world’s first computers. British Computer
REFERENCES


Li:2015:NAC


Lee:2017:SUE


Liu:2017:GAU


Li:2017:CEH


Li:2017:RNF


Li:2017:CCF

Liu:2015:CEH

[JCL17b] Can Liu, Gradeigh D.

Liu:2018:VRU


Liang:2014:CCS


Liu:2016:EQU


Liu:2016:NOP


Luo:2019:SCT


Liu:2016:LCR


Liang:2015:CPA


Li:2018:CIC


Li:2017:PCL


Lekkas:2010:PMT


REFERENCES


Lertvorratham:2012:ISM


Liao:2013:NMS


Li:2014:ARM


Lenstra:2012:PK


Lum:2016:QEM

[LHA+16] Daniel J. Lum, John C. Howell, M. S. Allman, Thomas Gerrits, Varun B. Verma, Sae Woo Nam, Cosmo Lupo, and Seth Lloyd. Quantum enigma machine: Experimentally demonstrating quantum...

**Li:2012:BVS**

**Lin:2011:ICA**

**Lin:2018:BBB**

**Li:2010:AIS**

**Li:2014:SOA**
REFERENCES

ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Liu:2015:SSP

Li:2018:OPP

Lian:2014:SSA

Lin:2015:CND
Hui Lin, Jia Hu, Jianfeng Ma, Li Xu, and Li Yang. CRM: a new dynamic cross-layer reputation computation model in wire-

**Liu:2018:HMS**


**Liu:2012:ESS**


**Li:2010:PAP**


**Liu:2017:AMA**


**Lim:2011:NAN**


**Lim:2014:IVW**

REFERENCES

Lindell:2014:TCT

Lin:2015:LBD


Li:2012:OEA


Lesi:2017:SAS


Laszka:2014:STC


Liu:2017:OOA


Liu:2018:PAB


Libert:2016:BRD

Benoit Libert, Marc Joye, and Moti Yung. Born and


Kyuin Lee, Neil Klin-

Leva:2013:ABN


Le:2011:RMA


Lee:2015:TSS


Lu:2016:PFC


Lu:2016:PSC

REFERENCES


[Lee:2010:PMB]

[Lee:2011:TAT]

[Li:2015:IBE]

[Lyu:2019:SPP]
REFERENCES

www.sciencedirect.com/s.../pii/S030439751930386X

Lin:2016:SCU


Li:2017:ESD


Lyu:2018:PKE


academic.oup.com/comjnl/article/61/2/288/4259796

Li:2012:RIB


Liu:2018:GEI


Liu:2019:SBC


Li:2017:CIS


Li:2017:CCD


Li:2018:VSE


Li:2018:CIE

Li:2010:DCY


Lai:2013:SAS

Chengzhe Lai, Hui Li, Rongxing Lu, and Xuemin (Sherman) Shen. SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks. *Computer Networks*.

Libert:2019:ZKA


Lu:2012:IEC


Lai:2018:EQK


Lee:2019:CSS


Liao:2019:ESO


Lee:2016:AGA


Lee:2006:DCK


Ling:2012:NCC


Luo:2012:FSI


Lee:2015:SAS


Li:2018:WMH

L. Li, H. Li, W. Yuan,

Lu:2012:BBE


LLZ+12

Lai:2016:GGB


LLZ+16

Li:2017:CBS


Lucamarini:2014:QKD


Lambert-Mogiliansky:2012:EII

REFERENCES

[Le:2016:ADS]

[Lai:2018:IBB]

[Lai:2017:FPP]

[Liu:2014:SCS]

[Li:2011:NRA]

[Lv:2013:NTP]
Lubacz:2010:VI


Lukasiewycz:2016:SAO


LoIacono:2019:NGR


Li:2018:RBB


Li:2018:TFA


Li:2013:ESC

Xiong Li, Jianwei Niu, Muhammad Khurram Khan, and Junguo Liao. An enhanced smart card based


Lin:2011:CRN


Ling:2012:SHS


Lima:2010:PKE


Lian:2015:GRG


Liu:2017:HPI


Lampe:2012:ATS


Lin:2018:CPF


Lin:2018:SSS


Lei:2013:RSW


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


Lee:2011:ACA


Lewko:2011:DAB


Liu:2013:SIP


REFERENCES

Liu:2013:TIE


Liu:2013:CBS


Liu:2016:PAB


Li:2019:TFA


Liu:2014:DAF


Liu:2017:EEC

Liu:2011:SBA


Li:2018:SCM


Lu:2012:HOM


Li:2019:PSA


Liu:2010:NDC

Feng Liu, ChuanKun Wu, and XiJun Lin. A new definition of the contrast

Liu:2010:SET


Liu:2017:SRG


Liu:2011:PIA


Liu:2016:NSC


Lu:2012:MMA


Li:2010:GCP


Luo:2012:ICB


Li:2016:DDA


Li:2012:IIA

Yanjun Li, Wenling Wu, and Lei Zhang. Improved integral attacks


Li:2010:NAS


Li:2019:VCM

Jing Li, Licheng Wang, Lihua Wang, Xianmin Wang, Zhengan Huang, and Jin Li. Verifiable Chebyshev maps-based chaotic encryption schemes with outsourcing computations in the cloud/fog scenarios.

Lin:2010:DSM


Li:2010:DSM


Li:2011:NW


Lai:2012:RHB

[LXJ14] Fagen Li, Pan Xiong, and Chunhua Jin. Identity-based deniable authentication for ad hoc net-


Li:2014:IBD

[LXWM12] Xiong Li, Yongping Xiong,

Luo:2014:ARP


Liu:2015:SDS


Lim:2016:AKE


Li:2010:AFF


Liu:2018:IMM


REFERENCES

Liao:2010:MPC

Lai:2018:NIB

Liu:2016:FIT

Lai:2018:NSH

Liu:2018:SKR

Li:2013:SSS
Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and se-


Liu:2014:CRA


Li:2019:APA


Li:2010:PES


Li:2012:ESS


Li:2019:IEU


Li:2019:ESM

Xingxin Li, Youwen Zhu, Jian Wang, and Ji Zhang. Efficient and secure multidimensional geometric range query over encrypted data

**[Liu:2019:RAS]**


**[Ma:2017:AEJ]**


**[Masdari:2017:STA]**


With a foreword by Christopher M. Bishop.


Mangard:2013:KSL


Martin:2010:FWL


Martin:2010:PCC


Martin:2010:XMA


Markoff:2012:FFO


Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP

[Mat14] Takahiro Matsuda. On the impossibility of basing public-coin one-way permutations on trapdoor permutations. Lecture...

**Matthiessen:2019:RCM**


**Maurer:2012:CCN**


**Mayron:2015:BAM**


**Mazurczyk:2013:VSD**


**Milo:2011:FGB**


**Mao:2015:PUA**
(print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/7/1573.

Matias:2018:NNZ


Malone:2013:MOD


Migliore:2018:PPF


Mainardi:2019:PRA


Massolino:2015:OSC


Mukhopadhyay:2011:PEA

Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. A parallel efficient architecture for large cryptographically robust

**Matula:2019:PCG**


**Madanayake:2012:BPS**


**McGraw:2017:IDH**


**McGrayne:2011:TWH**


**McGraw:2016:SBTd**


**McKay:2010:SLB**

REFERENCES


REFERENCES


Majzoub:2012:MRH


[MD12a]

Mansouri:2012:ACA


[MD12b]

Mansfield-Devine:2015:MIC


[MD15]

Murdoch:2010:CPB


[MDAB10]

Malina:2018:SET

REFERENCES


[MFG16] Kalikinkar Mandal, Xinxin Fan, and Guang Gong.


Matsuda:2014:CCS

Meloni:2016:RDR

Meziani:2012:IPS

Miller:2014:ADS

Mo:2018:RUA

Munoz-Hernandez:2016:EES
REFERENCES


REFERENCES

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

Michiels:2010:OWB

Michael:2016:RNI

Midgley:2010:SEE

Martinez-Julia:2012:NIB

Martinez-Julia:2013:BSI

Miao:2019:PPT

Memon:2018:TFS
Shiraz Memon, Jensen Jens, Elbers Willem, Helmut Neukirchen, Matthias

Mohanty:2011:RTP


Moessner:2012:SAS


Muller:2012:HPC


Mozaffari-Kermani:2017:FDA


Mozaffari-Kermani:2018:ERE

REFERENCES


[MLBL12] Leonardo Montecchi, Paolo Lollini, Andrea Bondavalli, and Ernesto La Mattina. Quantitative se-


References


REFERENCES


**Matsuo:2012:MAK**


**Meshram:2012:IBC**


**Mukhopadhyay:2014:EMP**


This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.

**Monz:2016:RSS**

McKusick:2015:DIF


Minier:2012:RKI


Mizuki:2011:ASN


Maimut:2012:LCR


Minamoto:2014:BDI


Mone:2013:FPE

Moore:2012:RFF

Moody:2014:DMW

Morad:2012:OEA

Morawiecki:2019:MS

Moriai:2019:PPD

Mosca:2018:CEQ

Moulick:2015:RDS

Minier:2012:EEC
Min:2018:AAB


Meiklejohn:2016:FBC


Mudhenk:2017:SAN


Mironov:2012:IDP


Mukhamedov:2010:IEP

Maimut:2014:AET  

Marasco:2014:SAS  

Micali:2014:CMS  

Manimehalai:2016:NRR  

Migliore:2018:HSC  

Moataz:2018:SSE  

Martinovic:2017:AUP  
Matsumoto:2017:ACG


Moghadam:2010:DRN


Maitra:2012:DSM

Subhashis Maitra and Amitabha Sinha. Design

Mendel:2012:DAL


Maitra:2012:NAC


Mroczkowski:2012:CAS


Maitra:2013:DSM

Subhashis Maitra and Amitabha Sinha. Design

**Maitra:2013:HEM**


**Maitra:2013:HPM**


**Miller:2016:RPS**


**Mukherjee:2017:EPP**


**Myers:2012:BCM**


**Myers:2013:BBC**

Steven Myers, Mona Sergi, and abhi shelat. Blackbox construction of a more

**Morales-Sandoval:2018:PBC**


**Montuschi:2016:ISC**


**Marton:2010:RDC**


**Mashimo:2018:VMS**


**Mosenia:2017:CCA**


REFERENCES


Malkin:2011:ECS

Meerwald:2012:ERW

Muftic:2016:BCC

Mundy:2017:CGU

Murphy:2010:BRB

Murdoch:2016:IDP
REFERENCES


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


REFERENCES

Mahmoody:2013:LEZ


Ma:2013:PVP


Meng:2015:CRS


Marko:2017:MDI


Mastroeni:2017:APS


Manshaei:2013:GTM


Ma:2015:PKE

[MZHY15] Sha Ma, Mingwu Zhang, Qiong Huang, and Bo Yang. Public key encryption
Meng:2019:ESF


Nagy:2010:OTP


Nagy:2010:QCS


Nikiforakis:2014:BYO


Naccache:2012:CST

Naccache:2016:FHE


Naranjo:2012:SAK


Nagaraj:2019:RCC


Nunez:2017:PRE


Namasudra:2019:IAB


Noureddine:2013:AMT

Nain:2017:SPE


Naskar:2012:FIR


Naskar:2013:GTL


Naranjo:2013:FDA


Ni:2013:EIB


Narasimhan:2013:HTD


Ngo:2017:CSS


NdMMW16


Newell:2013:PCD


Nejatollahi:2019:PQL


Nacer:2017:DAM

Naeem:2014:EIC


Nafea:2016:HMB


Nievergelt:2002:FLM


NIST:2012:RRN


NIST:2013:CSS


NIST:2015:SSP

NIST. SHA-3 standard: Permutation-based hash and extendable-output functions. FIPS PUB 202, National Institute for Standards and


Toan Nguyen and Nasir Memon. Tap-based user authentication for smartwatches. *Computers &
Norta:2019:SFB


Nieto:2013:PVC


Nieto:2014:FSH


Ntantogian:2015:GTF


Nguyen:2012:DQB


Neville-Neil:2015:KVH

George V. Neville-Neil.


[NRZQ15] Danmei Niu, Lanlan Rui, Cheng Zhong, and Xuesong Qiu. A composition and recovery strategy for mobile social network service...

**Naccache:2010:THI**


**Nojoumian:2012:SRS**


**Natarajan:2015:MAD**


**Nguyen:2017:DPA**


**Niksefat:2014:ZPP**


**Neuastedter:2018:BTW**

Carman Neuastedter, Samarth


[NYL+15] Ben Niu, Xiaoyan Zhu, Qinghua Li, Jie Chen, and Hui Li. A novel attack to spatial cloaking schemes in location-based services.

REFERENCES


REFERENCES

January 2017. CODEN IT-COB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Oggier:2011:ACA

Obrien:2012:EPM

Onica:2016:CPP

Oliynykov:2015:NES

Ou:2010:CPA

Ogiela:2018:EBI
Oliveira:2012:STA


Or-Meir:2019:DMA


Ortiz-Martin:2019:FAI


Ogiela:2010:UML


Ohtake:2012:AAH

REFERENCES

Ogiela:2018:LTC


[OO18]

Orlandi:2014:SCN


[OOR+14]

Oppliger:2011:CC


[Opp11]

Orumiehchiha:2014:PAN


[OPS14]

Orejel:2014:E


[Ore14]

Ormond:2016:CPR

Jim Ormond. Cryptography pioneers receive ACM A. M. Turing Award: Diffie

[Orm16]

Ozen:2011:MIS


Owczarek:2012:LPL


Osborn:2016:SSR


Ostad-Sharif:2019:TPS


Olson:2016:SIT

REFERENCES


[OTO18] Urszula Ogiela, Makato Okamoto:2012:AAH


[OTO18] Urszula Ogiela, Makato

**Praba:2010:MAC**


**Ohzeki:2012:NWM**


**Ortiz-Yepes:2014:BSA**


**Parrilla:2019:ECC**


**Parveen:2018:IEE**

REFERENCES


[Pas13a] Rafael Pass. Unprovable security of perfect NIZK and non-interactive

Pranata:2013:MDR


Paulson:2010:SDO


Paul:2019:RCS


Poh:2017:SDV


Park:2014:FRI

Jeong Soo Park, Ki Seok Bae, Yong Je Choi, and Doo Ho Choi. A fault-resistant implementation of AES using differential

**Poddar:2019:AED**


**Pun:2014:GIT**


**Paul:2016:TSO**


**Papadopoulos:2014:LQA**


**Perkovic:2019:LVL**


**Premnath:2014:EHR**

Sriram Nandha Premnath, Jessica Croft, Neal Pat-

**Poh:2017:SSE**


**Pang:2014:PPA**


**Patranabis:2019:SCS**


**Paul:2012:KSS**


**Pereira:2015:PKE**

Pippal:2012:SVU


Pearson:2011:NWC


Peck:2012:CAC


Peck:2017:BWD

Morgan E. Peck. Blockchain world — do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectrum, 54(10):38–60, October 2017. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Persichetti:2013:SAH


Peterson:2011:SWS


Petrlic:2012:PRE

REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-35416-8_7/


REFERENCES


Pointcheval:2012:ACE


[PKA15]

Patel:2018:LLA


Premarathne:2015:LDD


Pramila:2018:ICA


PJ12

PJ18

PK15

PKS18
REFERENCES


REFERENCES


Puthal:2017:DDK


Niu:2014:RDW


Powers:2014:OSCa


Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC

P:2018:ABE

Pereira:2016:SHB

Pennino:2019:PIS

Pendl:2012:ECC

Pyun:2012:IBF

Pathak:2012:PPS
Manas Pathak, Jose Portelo, Bhiksha Raj, and Isabel Trancoso. Privacy-preserving speaker authentication. *Lecture

**Phan:2012:DDB**


**Phan:2012:MBT**


**Piret:2012:PBC**


**Perez-Resa:2019:SSE**

A. Pérez-Resa, M. García-

Puthal:2019:SAL


Proudfoot:2015:WTH


Polyakov:2017:FPR

Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntanathan.


Proudfoot:2015:WTH


Priemuth-Schmid:2012:ASV


Permpoontanalarp:2014:FTG

Yongyuth Permpoontanalarp and Panupong Sornkhrom. On-the-fly trace generation approach to the security

**Perazzo:2015:DRL**


**Pereira:2013:SLC**


**Phatak:2013:SIN**


**Patranabis:2017:PSK**


**Pizzi:2018:ETM**

Picazo-Sanchez:2013:CRS


Park:2013:PPM


Pankhuri:2019:PBM


Papamanthou:2013:SCC


Peng:2019:GCS


Papakostas:2014:MBL


www.sciencedirect.com/science/article/pii/S0164121213001623

Pham:2019:SSS


Puthal:2019:SSE


Poller:2012:EIC


Peng:2010:IWM


Pongaliur:2013:SNS


Pja:2019:SSG


Pagnin:2018:HDB

Elena Pagnin, Anjia Yang, Qiao Hu, Gerhard Hancke, and Alkaterini Mitrokotsa. HB+DB: Distance bounding meets human based au-
REFERENCES

Philippaerts:2013:CMC


Pei:2015:SWT


Papadopoulos:2010:CAR


Phuong:2018:CBE


Popa:2015:HCD


Pournaghi:2018:NNE


Qu:2013:DPA


Qin:2018:NUW


Qiu:2017:PSB


Qiu:2017:AAS


Qiu:2017:DIR


Qiu:2019:CPT


Qiu:2019:CPT


Qi:2016:SPR


Qin:2018:BRO


Rabin:2010:ACC


Rankin:2010:HLH


Rankin:2014:HEY


Rankin:2016:HSP


Rao:2010:PAA

Rajesh P. N. Rao. Probabilistic analysis of an an-

[Rao:2017:SEC]

[Rauscher:2015:FMT]

[Raz:2019:FLR]

[Ruoti:2015:WJS]

[Radke:2017:SPP]

[Rupp:2015:CTM]
REFERENCES


Radke:2015:CFA


Reaves:2017:MBM


R:2018:SDM


Rao:2019:HPR


Reinicke:2017:RDS


Raisaro:2018:PPS

Jean Louis Raisaro, Gwangbae Choi, Sylvain Pradervand, Raphael Colsenet, Nathalie Jacquemont, Nicolas Rosat, Vincent Mooser,

Rabbachin:2015:WNI


Rao:2017:CFA


Riazi:2019:DLP


Reardon:2016:SDD


Reeve:2015:ARC


Ren:2010:CSH

Roh:2010:BSW

Rouhani:2018:RRT

ISSN 1936-7406 (print), 1936-7414 (electronic).

Robert-Inacio:2011:SAP

Rjasko:2012:BBP

Roy:2018:HFB


Reyhani-Masoleh:2018:NAR


Rezaeibagha:2019:PSB


Ryan:2016:NCE


Rogaway:2016:POP


Rohloff:2019:CAR


Romero:2011:FSW


Romero:2012:IBB

[Rom12] J. J. Romero. India’s big bet on identity. IEEE Spec-
REFERENCES

Rose:2011:KBT

Rao:2012:SSA

Rifa-Pous:2011:CEC

Rhee:2010:TSS

Ren:2015:ASE

Rawat:2011:CBR
Sanjay Rawat and Balasubramanian Raman. A

**Razaque:2016:TDP**


**Razaque:2017:SDA**


**Rosen:2010:CCS**


**Reeder:2011:WPD**


**Rivest:2014:SSR**


**Rossi:2015:IBS**


Jothi Rangasamy, Douglas Stebila, Colin Boyd, and Juan Manuel González-Nieto. Effort-release


[RSCX18]

Roy:2015:SCP


[RSGG15]

Rastegari:2019:ECS


[RSM15]

Ribeiro:2015:QBS


See also news story [Ano15a].

[Ano15a]

Resende:2019:BMI

REFERENCES


[Yogachandran Rahulamathavan:2016:UCA] Yogachandran Rahulamathavan, Suresh Veluru,

Rodriguez-Vazquez:2012:SCB

Reaves:2018:CSS

Roettger:2012:PKC

Ren:2014:HHM

Rogaway:2012:SCS
REFERENCES

Ren:2013:PPK


Ristenpart:2010:WGR


Ren:2013:DSE


Romashchenko:2019:OCM


Rajendran:2015:FAB


Sang:2012:SSF

REFERENCES


REFERENCES

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-27937-9_20/

Suoranta:2012:SAM


Sarreshtedari:2015:WMD


Schutz:2010:DIN


Sacco:2014:MC


Sahai:2013:TCT


Saeed:2016:IID

Ahmed Saeed, Ali Ahmadiania, Abbas Javed, and Hadi Larijani. Intelligent intrusion detection in low-power IoTs. ACM Transactions on Internet Technology (TOIT), 16(4):27:1–
REFERENCES

27:??, December 2016. CODEN ????. ISSN 1533-5399 (print), 1557-6051 (electronic).


[Sara10b] Palash Sarkar. A simple and generic construction of authenticated en-


Savage:2016:NKP


Safkhani:2017:PSD


Shwartz:2018:DMI

Stevens:2017:AFS

Sarkar:2015:DFA

Safkhani:2012:SMA

Safkhani:2018:SRO

Santos:2014:ACD

Shyu:2010:VMS


REFERENCES


Scholl:2019:SIE


Shrestha:2010:KBA


Stobert:2018:TAL


Seberry:2010:CTAa


Seberry:2010:CTAb


Scriber:2018:FDB


Streit:2018:PQK


Sherman:2017:ICC


Shakiba:2010:IID


Souissi:2012:OCP


Shakiba:2014:CCI

Seo:2014:RHI


Seo:2016:RHI


Salman:2018:BMM


Sasaki:2012:IKK


Staples:2019:SAB


Sendrier:2010:PQC

REFERENCES


**Sendrier:2017:CBC**


**Seo:2018:CSI**


**Serrato:2012:IAN**


**Sallam:2012:EBM**


**Sakai:2016:CDN**


**Sethumadhavan:2016:HEP**


**Severance:2016:BSB**

Charles Severance. Bruce...


[SGFCRM+18] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Marquez, B. Luna-Benso, and M. Aldape-Pérez. Substitution box generation using Chaos: An im-


Sanchez-Garcia:2016:SSA


Sun:2015:FSW


Shen:2018:CAL


Susilo:2016:EDT


REFERENCES


REFERENCES


REFERENCES

Satir:2012:CBT


Siad:2012:NAP


Simpson:2010:ESB


Simion:2015:RST


Simmonds:2015:DII


Sirer:2016:TPS


Shakeri:2012:RZW

Mahsa Shakeri and Mansour Jamzad. A robust zero-watermark copy-


References


**Sirivianos:2014:LSF** [SKGY14]


**Seo:2015:AEC** [SKH15]


**Shin:2017:SSD** [SKH17]


**Szalachowski:2010:CCG** [SKK10]


**Stevens:2015:FCF** [SKP15]


**Singh:2018:MWT** [SKS+18]

Amit Kumar Singh, Basant Kumar, Sanjay Kumar Singh, S. P. Ghdera, and Anand Mohan. Multiple watermarking technique for securing online social network contents using back propagation neu-

[Scheidat:2012:STT]


[Scheidat:2012:STT]


[Schultz:2010:MMP]


[Schultz:2010:MMP]

Somani:2010:IDS

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

Su:2016:SSP


Sun:2016:RSP


Shao:2012:AKP


Sarkar:2010:CRM


Sarkar:2010:CRT


Sorniotti:2010:PSS

Alessandro Sorniotti and Refik Molva. A prov-

**Seyedzadeh:2011:IES**


**Sengupta:2012:SAI**


**Sencar:2013:DIF**


**Swami:2018:AAS**


**Shibu:2019:ARR**


**Shokri:2019:ESS**

Madeh Shokri and Meghdad Mirabi. An efficient stream structure for broadcasting the encrypted XML
REFERENCES


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 ????.


REFERENCES


REFERENCES

3-642-14452-7 (e-book).

Son:2018:GFD


[SNCK18]

Siadati:2017:MYS


[SNG17]

Safavi-Naini:2011:USC


[Saf11]

Seyedzadeh:2014:RCI


[Sey13]

Soderstrom:2013:DDY

References


**Spafford:2016:SE**


**Salvail:2010:STR**


**Sherman:2019:PBL**


**Skracic:2017:AAU**


**Safkhani:2014:CCA**

al. protocol: a hash-based RFID tag mutual authentication protocol. [SR10]

Sun:2013:IUP

Serwadda:2016:TRR

Shaikh:2010:CTO

Schilling:2012:ATU

Sur:2012:SSU
Stanton:2014:BRB


Singh:2017:SCB


Stefan:2012:ACT


Sutar:2017:DPI


Sutar:2018:DPI


Sluganovic:2018:ARE

Ivo Sluganovic, Marc

Sethumadhavan:2012:CHD


**Shparlinski:2012:CSD**


**Sendrier:2013:HCE**


**Singh:2015:EST**


**Sadhya:2017:PRE**


**Shivani:2017:RIE**


**Siegel:2019:UOC**

REFERENCES

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

Singh:2013:QBF


Smith:2011:SMC


Sakai:2016:NCS


Shahandashti:2015:RUP


Sundararajan:2019:SMC


Shrivastava:2012:UIE

Swapnil Shrivastava, Zia Saqib, Gopinath P., and Peeyush Chomal.
REFERENCES


Schillewaert:2014:CCA

Shrestha:2015:CIS

Shen:2016:RMM

Sethumadhavan:2019:SA

Stallings:2011:C

Stallings:2011:CNS
Stanoyevitch:2011:ICM


Stanek:2012:TEM


Staff:2013:ITD


Stewart:2011:CCI


Steel:2015:APF


Stenn:2015:SNT


Stipcevic:2011:QRN

**REFERENCES**


REFERENCES


[SSL16] Shenghui Su, Tao Xie, and Shuwang Li. A provably secure non-iterative hash function resisting birth-


**Song:2017:SAM**


**Shuai:2019:AAS**


**Shen:2017:RDP**


**Shah:2019:PCB**


 REFERENCES

(Tan:2011:CTA)


(Tan:2012:SLM)


(Tan:2012:LCP)


(Tang:2015:ETE)


(Tang:2015:HAC)


(Tankard:2017:BNK)


REFERENCES


[TDTD13] Chengdong Tao, Adam

Teng:2018:KPA


Terai:2011:BRB


Tseng:2019:AMR


Tassa:2012:SDC


Tewari:2017:CNU


Theofanos:2016:SUE


Takayasu:2019:PKE [TK19] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks...

[TKM12]


[TKMZ13]


[TKR14]

REFERENCES


Tao:2018:AAC

Tomb:2016:AVR

Toxen:2014:NSS

Tsougenis:2012:PEM

Tan:2016:BIB

Tang:2014:PAB
Ming Tang, Zhenlong Qiu, Weijie Li, Weijin Sun, Xiaobo Hu, and Huanguo Zhang. Power analysis


**[TSB18]**


**[TSH17]**

**[TSH14]**


**[Toreini:2017:TRP]** Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. Texture to the rescue: Practical paper fingerprinting based on texture patterns. *ACM Transactions on Privacy and Se-
curity (TOPS), 20(3):9:1–9:??, August 2017. CO- 
DEN ???? ISSN 2471-2566 
(print), 2471-2574 (elec-
tronic).

[Tang:2011:IDC] Xuehai Tang, Bing Sun, 
Ruilin Li, and Chao 
Li. Impossible differen-
tial cryptanalysis of 13-
round CLEFIA-128. The 
Journal of Systems and 
Software, 84(7):1191–1196, 
July 2011. CODEN JS-
SODM. ISSN 0164-1212.

[Tso:2013:SAI] Raylin Tso. Security anal-
ysis and improvements of 
a communication-efficient 
three-party password au-
thenticated key exchange 
protocol. The Journal 
of Supercomputing, 66(2): 
CODEN JOSUED. ISSN 
0920-8542 (print), 1573-
0484 (electronic). URL 
http://link.springer.
comjnl.oxfordjournals.
org/content/55/4/475.
full.pdf+html.

[Tenca:2018:PIS] Alexandre Tenca and Nao-
fumi Takagi, editors. Pro-
cceedings of the 25th In-
ternational Symposium on 
Computer Arithmetic, 25-
27 June 2018 Amherst, 
MA, USA. IEEE Computer 
Society Press, 1109 Spring 
Street, Suite 300, Silver 
Spring, MD 20910, USA, 
June 2018. ISBN 1-5386-
2612-8 (USB). 1-5386-
265-9. ISSN 2576-2265. 
LCCN QA76.9.C62. IEEE 
catalog number CFP18121-
USB.

lossless image watermarking based on α-trimmed 
mean algorithm and support vector machine. The 
Journal of Systems and
Turing:2018:XYZ


Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG


Tupakula:2015:TES


Turan:2019:CFF


Tripunitara:2014:CKM


Wu:2012:SWG


Tupakula:2015:TES


Turan:2019:CFF


Turing:2018:XYZ


Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG

Toor:2018:VQA

Tartary:2011:EIT

Tian:2012:SSB

Trost:2016:OPC

Tan:2016:CCA

Tolba:2016:GMA
REFERENCES


UlHassan:2019:DPR


Ueno:2019:TBP


Uto:2013:MRI


Ulutas:2011:MIS


Ulutas:2013:ISI


Vaikuntanathan:2011:CBN


vanDam:2011:TQC

Visegrady:2014:SCV

vanderWalt:2018:CSI

VenafiLabs:2014:VLQ

Vergnaud:2017:CAB

Vetter:2010:ABV
Vo:2019:ISA


Voulgaris:2019:BTI


Venkatakrishnan:2017:DRB


Vernize:2015:MNI


Vijayarajan:2019:BKB

REFERENCES


Vrakas:2014:OUI

Viennot:2014:MSG

Vasisht:2018:DEU

Vu:2015:NAN

Vgena:2019:TAL

Vasiliadis:2017:DIS
Giorgos Vasiliadis, Lazaros


S. Sree Vivek, S. Sharmila Deva.

**Vlachos:2015:DPC**


**vanTilborg:2011:ECS**


**Viswanathan:2018:EEG**


**Vuagnoux:2010:CAC**


**vanVredendaal:2016:RMM**


**VanDijkhuizen:2018:SNT**

REFERENCES


REFERENCES

Wang:2013:CRA

Wang:2014:IIA

Wang:2018:LRI

Wang:2018:PPA

Ward:2011:CCM

Watt:2010:IP1
Waters:2012:FER


Watts:2014:ICB


Watts:2015:HGA


Wang:2012:PCE


Weisse:2017:RLC

REFERENCES


REFERENCES


Wang:2019:SFE


Wang:2013:SES


Wang:2018:ERS


West:2015:EC


Wess:2016:JWM


Wang:2016:SSS

Xianfang Wang, Jian Gao, and Fang-Wei Fu. Secret sharing schemes from linear codes over $F_p + \nu F_p$. *International Journal of Foundations of Computer Science (IJFCS)*, 27


Lin Wang and Zhi Hu. On graph algorithms for degeneracy test and recursive description of stream ciphers. Fundamenta Infor-
REFERENCES

Wang:2015:EFF

Wang:2017:DVP

Wei:2016:PAB

Wang:2017:DVP

Wei:2012:DAA

Wei:2012:FOP
Xu An Wang, Xinyi Huang, Xiaoyuan Yang, Longfei Liu, and Xuguang Wu. Further observation on proxy re-encryption
REFERENCES

Wang:2012:NFS | [WHZ12]
---

Wang:2019:RSI | [WHZ+19]


Williams:2018:FPD | [Wil18]

Winder:2017:ROS | [Win17]

Qian Wang and Chenhui Jin. A method to bound the number of active S-boxes for a kind of AES-like

See [BBG+17].


Wei:2012:IRK

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

Wang:2011:RBM


Wei:2015:FST


Wei:2014:EEF

Wang:2011:HAB


Wu:2015:TRM


Wang:2017:ABS

[WLY17] Qi Wang, Xiangxue Li, and Yu Yu. Anonymity for Bitcoin from secure escrow address. IEEE Access, ??(??):1, ???. 2017. ISSN 2169-3536.

Wang:2016:LLE


Wang:2012:RTC


Wang:2017:PPD


Wu:2012:PSC

[Wei Wu, Yi Mu, Willy Susilo, Xinyi Huang, and Li Xu. A provably secure construction of certificate-

Watanabe:2014:OAC


Wang:2017:CES


Won:2016:PAA


Wang:2015:HAD


Wu:2012:UFS

Wendzel:2015:CME

Wang:2017:PPK

Wang:2016:SEP

Wu:2013:FTR

Wu:2016:CBE

Wei:2015:TPE
Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-expression searches. International Journal of In-


REFERENCES


REFERENCES

Wei:2019:VFA


Wang:2012:PAC


Wu:2010:IBM


Wang:2013:NMC


Wu:2012:EUA


Wu:2012:RIB

Tsu-Yang Wu, Yuh-Min Tseng, and Tung-Tso Tsai. A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. *Computer Networks*
REFERENCES


[WWBC14] Long Wen, Meiqing Wang, Andrey Bogdanov, and Huafeng Chen. Multidimensional zero-correlation attacks on lightweight...


REFERENCES

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


[Wu:2017:EAK]

[Wang:2016:SHI]

[Wang:2019:CSS]
Wang:2019:NTB


Wang:2017:SRS


Wang:2010:IIB


Weir:2012:AVC


Wang:2014:NAI


Weir:2012:IHV


Wang:2013:NSW

Xiaogang Wang, Ming Yang, and Junzhou Luo. A novel sequential watermark detection model for efficient traceback of se-

**Wei:2014:IDC**


**Wu:2018:SMI**


**Wei:2016:APS**


**Wang:2013:BSB**


**Wang:2014:CGR**


**Wang:2017:RRA**

REFERENCES

[1999], 129 (part 1)(??): 64–78, December 24, 2017.


[WZLW13] Chi-Yao Weng, Yu Hong Zhang, Li Chun Lin, and Shiuh-Jeng Wang. Visible watermarking images in...

Wei:2012:CSO


See [FZM12b].

Wei:2012:GOP


Wang:2012:NIS


Xiong:2013:NIB


Xu:2014:AHA

Chang Xu, Hua Guo, Zhoujun Li, and Yi Mu. Affiliation-hiding authenticated asymmetric group key agreement based on short signature. *The Computer Journal, 57
REFERENCES


REFERENCES

Xu:2013:PKE


Xu:2019:TPT


Xue:2018:SNN


Xiong:2009:PSI


Xiang:2016:EMP

Xue:2013:TCB


Xie:2013:ECP


Xu:2017:EOS


Xiang:2014:PBA


Xia:2015:SPK

REFERENCES


REFERENCES


Kaiqi Xiong, Ronghua Wang, Wenliang Du, and Feng Ning. Containing bogus packet insertion attacks for broadcast authentication in sensor networks. [XWS17]


See [XWLJ16].

Xia:2016:SDM


Xie:2014:SCP


Xu:2018:SKS


Xu:2018:DFH


Xiao:2016:REM

Chen Xiao, Lifeng Wang, Mengjiao Zhu, and Wendong Wang. A resource-efficient multimedia encryption scheme for embedded video sensing sys-

**Xu:2019:LAM**


**Xiong:2015:SRE**


**Xie:2012:DPK**


**Xiao:2018:KRL**


**Xu:2019:SIC**


**Xing-Yuan:2011:PRS**

[WXYXYX11] Wang Xing-Yuan, Qin


REFERENCES

ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Yoo:2017:PQD

Yaacoubi:2019:REM

Yamaguchi:2012:EVC

Yu:2015:SDS

Yang:2010:PII

Yang:2011:PQC
Yang:2014:BEB


Yang:2011:GSS


Yang:2012:PST


Yi:2017:ZCL


Yuan:2013:PVQ

Lihua Yuan, Chao-Chih Chen, Prasant Mohapatra, Chen-Nee Chuah, and Krishna Kant. A proxy

**Yu:2016:DNF**


**Yao:2015:LAB**


**Yuen:2012:IBE**


**Yu:2017:PDA**


**Yasuda:2015:MQC**


**Yu:2012:EPF**


**Yang:2017:CCS**


**Yang:2018:RRE**


**Yuce:2017:AFI**


**Yang:2015:SHI**

Ye:2017:VCS

Ye:2016:IEA

Yang:2016:EHA

Yu:2010:IBF

**Yao:2019:RSA**


**Yang:2014:MDF**


**Yamada:2017:EPA**


**Youn:2018:DAH**


**Yang:2018:CPG**


**Yang:2016:TCP**

Baijian Justin Yang and Brian Kirk. Try-CybSI: A platform for trying out cybersecurity. *IEEE Se-
REFERENCES


Zhi-Fang Yang, Chih-Ting Kuo, and Te-Hsi Kuo. Authorization identification by watermarking in log-


Ilsun You, Jong-Hyouk Lee, and Kouichi Saku-rai. DSSH: Digital signature based secure handover for network-based mobil-


REFERENCES

Yu:2010:PSI

Yu:2011:CLE

Ying:2019:LRU

Young:2015:DWE

Yavuz:2012:BFB

Yavuz:2012:ECR
Attila A. Yavuz, Peng Ning, and Michael K. Reiter. Efficient, compromise

**Yu:2016:SSD**


**Yong:2011:SPP**


**Yang:2017:SAS**


**Yang:2012:EMA**

Rui Yang, Zhenhua Qu, and Jiwu Huang. Exposing MP3 audio forgeries using frame offsets. *ACM Transactions on Multimedia Computing, Communications, and Applications*,
Yin:2017:QPE


Yin:2019:SCM


Yengisetty:2011:AVC


Yi:2016:IPA


Yang:2012:SAK


Yumbul:2015:EEP

Kazim Yumbul and Erkay Savaş. Enhancing an embedded processor core for efficient and isolated execution of cryptographic al-

**Yang:2015:EPS**


**Yang:2018:HEP**


**Yuen:2014:TCT**

REFERENCES


Yang:2019:ISO


YSTQM19

Ylonen:2014:SAA


YT12

Yang:2011:CCK


YT11a

Yamada:2012:UEW


YT16

Yi:2016:VSF

Ye:2018:VBA


Yeh:2017:SIB


Yang:2014:IBI


Yang:2011:ACD

[YWF18] Xiaokun Yang, Wujie Wen, and Ming Fan. Improving AES core performance via an advanced ASBUS protocol. *ACM Journal on Emerging Technolo-
Yan:2019:IFF

[Hongyang Yan, Yu Wang, Chunfu Jia, Jin Li, Yang Xiang, and Witold Pedrycz.

Yao:2010:IDA


Ye:2019:NCA


Yang:2015:RCI

[Hong-Ying Yang, Xiang-Yang Wang, Pan-Pan Niu, and Ai-Long Wang. Robust color image watermarking using geometric

Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


Yang:2010:CRS


Wang:2018:CIW


Yang:2019:SCC

Haomiao Yang, Xiaofen Wang, Chun Yang, Xin Cong, and You Zhang. Se-


References

Ye:2018:ISS


Yoon:2011:SBC


Yoon:2013:RBB


Young:2017:PSC


Yu:2017:PFS


Yildiz:2017:BLF

Muhammet Yildiz, Berrin Yanikoğlu, Alisher Kholmatov, Alper Kanak, Umut Uludağ, and Hakan


Yang:2012:LUC


Yang:2017:SKS


Yang:2019:HDS


Yang:2018:CDD


Chee, San Ling, Mulan Liu, and Huaxiong Wang. 

Zhang:2019:EPK


Zhang:2015:IAI


Zeng:2019:PKE


Zhou:2019:SAN

REFERENCES


Zhang:2018:SSH


Zetter:2014:CZD


Zhou:2016:IBP


Zhou:2018:SAE


ZDHZ18

ZDL12
REFERENCES

Zhao:2010:PSA


Zhou:2016:HFD


Zhou:2018:CBG


Zhang:2018:AAG


Zhang:2018:PPE


Gao:2012:DES

REFERENCES


Zadeh:2015:ASP


Zhang:2012:LDC


Zhang:2015:BYO


Zhang:2015:STR


Zhang:2015:RAS

Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, and Vijayakumar Bhagavatula. A pitfall in fingerprint bio-

**Zhu:2015:IDM**


**ZHL15**

**Zhao:2010:IFU**


**ZHS10**

**Zhu:2016:SCI**


**ZHT16**

**Zhu:2013:TSC**

Zhou:2015:EPP


Zhang:2016:PPV


Zuo:2019:WDH


Zimand:2010:SEC


Zhang:2011:FBP


Zeng:2014:NFC

Zhou:2012:CBF

Zhang:2019:CCF

Zhou:2015:PPS

Zhao:2012:IAS

Zhao:2014:TAH

Zhang:2012:EEF
Yummei Zhang, Joseph K. Liu, Xinyi Huang, Man Ho


Zhang:2016:TLT


Zhang:2018:SPF


Zhang:2017:FGA


Zhang:2010:NSS


Zielinska:2014:TS


Zhang:2016:CAH

Leyou Zhang, Yi Mu, and Qing Wu. Compact anonymous hierarchical identity-based encryption with constant size private keys. The Computer Journal, 59(4):452–461, April 2016. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (elec-
REFERENCES

Zaeem:2017:MAI

Zafar:2010:GRN

Zorpette:2012:BEC

Zhang:2017:PPN

Zavattoni:2015:SIA

Zheng:2016:EUV
Zhao:2012:SSS


Zhou:2017:IBB


Zenger:2016:AKE


Zhang:2016:SBA


Zhang:2015:MAA

October 6, 2010. CODEN ???? ISSN 1389-1286.

Zmudzinski:2012:WEU

Zhao:2012:SSM

Zhou:2019:LIN

Zheng:2018:GDP

Zanon:2019:FKC

Zhang:2012:EHO
Wentao Zhang, Bozhan Su, Wenling Wu, Dengguo Feng, and Chunhun Wu. Extending higher-order integral: An efficient uni-

Zhou:2018:TPW


Zuo:2018:CSA


Zhu:2015:PPD

REFERENCES

Zwattendorfer:2012:CBL

Bernd Zwattendorfer, Arne Tauber, Klaus Stranacher, and Peter Reichstädt.

Zhang:2016:EEA

Liping Zhang, Shanyu Tang, and Shaohui Zhu.

Zhou:2016:SRB

Lan Zhou, Vijay Varadharajan, and K. Gopinath.

Zhang:2015:FAA


Zhang:2014:LFL

Mingwu Zhang, Chunzhi Wang, and Kirill Morozov.
LR-FEAD: leakage-

Zhang:2011:AGK


Zhou:2018:QTA


Zilberberg:2013:PCM


Zhang:2015:FER


Zhang:2017:FBI

Yunpeng Zhang, Chengyou Wang, Xiaoli Wang, and Min Wang. Feature-based image watermarking algorithm using SVD and APBT for copyright protection. Future Internet, 9 (2):13, April 19, 2017. CODEN ???? ISSN 1999-
REFERENCES


[ZXJ+14] Xiaojun Zhang, Chunxiang Xu, Chunhua Jin, Run Xie, and Jining Zhao. Efficient fully homomorphic encryption from RLWE with an


REFERENCES


[ZYGY18] Furui Zhan, Nianmin Yao, Zhenguo Gao, and Haitao Yu. Efficient key generation leveraging wireless channel reciprocity for MANETs. *Journal of Network and Computer Ap-
REFERENCES


REFERENCES

Zhou:2017:ENQ


Zaidan:2017:NDW

Zhu:2018:CAC

Zhu:2019:ICR

Zhang:2017:NLR
[Leyou Zhang, Jingxia Zhang, and Yi Mu. Novel leakage-resilient attribute-based encryption from...
