Title word cross-reference

(2, 2) [KSSY12, LTC+15b]. (k, n) [YC11]. (n, t, n) [LHYZ12]. (t, n) [QD16, ZPWY12]. 0 [XHX+17]. 1 [XHX+17], 1, 2, 3 [SMDS11]. 11 [LJ17], 13 [Blo15]. 2 [DBPS12, EAA+16, ESS12, JR13, MCDB12, PGLL10, WY12]. 22 [MNP12], 2k [Sun16]. 3 [AP10, CG12b, DWZ12, FWS13, GZH12, GH11a, KWS+12, LJ17, LJ15, MKH+12, RS16, SS10b, SS12a, SGS14, WSSO12, tWmC12, YT11a, YI14, YPRI17]. 32, 32 [SA14], 3 × 3 [AMVZ12]. 4 [COP14, DWZ12, HLYS14]. 49.00 [Sch15a]. 8 [LPO+17]. 89 [APPVP15] = [JJUW10]. + [PYH+18]. 2 [YXN+16], 3 [LHM14], MT [HRB13], α [TTL10], c [KRDH13], d [QD16], d × d [KA17], t [ZTL15], Fp + νFp [WGF16], γ [DWZ12], GF(2)[x] [SF12], GF(2^n) [SKH15], GF(2^n) [LBOX12], K [FXP12, FR16, CHX13, ZHT16]. L(1/4 + o(1)) [Jou13]. M [MMSD13, ÖS11]. F_{3,8,30} [AMORH13]. F_q [SS13], A^P [HN10], GF(q) [LPPS10], LWE [BV14], μ [Jia14a], N [FR16], n × k(k ≥ n/2) [MC11], O(d13d) [KA17], O(n^2) [KS11], P [DG17], ±1 [HZZ14], q [GMS11], S [LJ15], t [HJM+11, Oba11], w [Kre13].

LW12, Pan14, PH12b, SLZ12]. **ACIS**
[Ano11a]. **ACM** [ACM10, ACM11, Orm16].
**Acoustic** [DLM'M'+18, GST13]. **ACP**
[LLG15]. **Across** [LQD'+16, TYK'+12].
**Active** [LJ15, AGWL16, BAB'+13].
**activities** [DLM'T12]. **Activity** [NTKG17].
**Ad** [PD14, Shc14, XHC'+12, KM10b, LXJ14, SGGCR'+16]. **Ad-Hoc** [PD14].
**Adam** [Bar12]. **adapted** [IMB17].
**Adaptive** [CT11a, zGXW12, GLG12, HZW'+14, HLbZ15, KD12a, Li15, PWLL13, SOS15, CLP'+13b, dCCSM'+12, dCCSB'+16, EEAZ13, FXP12, GCK11, GLM'+16, KS11, LHM14, LW'+10, PCL14, SH11, Wan13, WKH11].
**Adaptively** [HP14, OT12].
**adder** [MS13a].
**Adding** [CFVP16, CSL'+14].
**Additive** [TM18, ZDL12].
**Address** [WLY17, PSJ'+13].
**addresses** [AZH11].
**Addressing** [SVG16, SRB'+12].
**Adelson** [BB16b].
**Adelson-Velskii** [BB16b].
**adjacency** [SA15].
**adjacent** [Kre13].
**Administering** [Pal16].
**Adoption** [LKKL13, YWK10b].
**Advanced** [Böhl0, CSYY18, DR10, TC10, ALL'+18, DDFR13, GLIC10, Kra12, MKRM10, NdMMW16, SKK10].
**Advances** [PHWM10, WP15, Abe10, Gll10, LW11a, PJJ12, Rab10].
**Agreement** [WSSO12].
**Aggregating** [DP12].
**Aggregation** [BJL16, LHK10, SP15b, ZHW'+16, WMYR16].
**Aging** [SKV12].
**Ages** [Bur11, Joh15].
**Agreement** [Chi16, HCL'+14, HEC'+12, MNS11, TM12, WSS12, XL'M'+12, XLM14, XZLW15, AN15, BGAD12, CSD18, CTL13, DLK'+16, GH16, HPC12, IS'C'+16, IB11, KS11, KLW'+16, KDW'+17, LLLS13, LlK'+17, NCL13, Nos11, Nos14, hSZ15, TLL12, WXK'+17, XCL13, XMHD13, YZ'Z'+14, ZWQ'+11, ZTZ16, ZC15, OHJ10].
**Aided** [BGK12, BCGK12, BGB12, GMS14, Vun10, ABB13, LLY15, SSA11, WLFX17].
**AI** [AGLW16].
**Air** [AUMT16, ZWX'+18].
**aircraft** [XWZW16].
**AK** [XHC'+12].
**AK-PPM** [XHC'+12].
**AKA** [LSS13].
**AKF** [KD15].
**al** [LLW16, LLSW16, MWZ12, PLPW13, SBS'+12, Mac14, Keb15].
**al-Qaeda** [Mac14, Keb15].
**al.** [ABJ13, SPLHCB14].
**Alan** [CS12, Don14, He17, LCKBJ12].
**Algebra** [Xie12, BS15, Bul10b, CFF11, DWZ12, FGPGP14].
**Algorithm** [SK11, Tan15, Wat10, Bul10a, CFF11, SA14, YTM'+14].
**Algorithm** [ABCL17, Ano11b, AK14, BGJT14, CNR14, jCPB'+12, ESS12, GKS17, JHL12, JSZ12, JH11, JL16, KB10, LL11, LT4a, LLL17, NdMMW16, NV10, RR11, RVRC12].

Android [Ch13b, EBFK13, FHM+12, SEF10].


Applications [AMVZ12, Ana14, BKPW12, BCG+12b, BJCHA17, BS12, CZL12a, CZL12b, CPS16, DK15, FSK10, GKM16,
TY16b, TLL13, WWBC14, XDWN12.

attempt [Fel13]. ATtiny [EGG+12].

Attribute
[AAC+16, AHL+12, BFK+10, Boy13, CD16, CDL18, FHR14, GZZ+13, GSW+16, Gli12, GVW15, HSMY12, Her14, KGP12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, OT12, PB12, RVH+16, Rao17, SSW12, TYM+17, WHL15, WHLH16, XMLC13, XWLJ16, ZPM+15, ZPQ15, ZMZ17, ZHW15, FNWL18, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, RD17, XWS17, YCT15, ZWM14, ZML17].

Attribute-Based
[AAC+16, BFK+10, Boy13, CD16, FHR14, GZZ+13, GSW+16, GVW15, HSMY12, LW11b, LW11c, LW12, LJLC12, LYZ+13, LHL+14, LAL+15, LHL15, LW16, PB12, RVH+16, Rao17, SSW12, TYM+17, WHL15, XMLC13, XWLJ16, ZPM+15, ZQ15, ZMZ17, CD18, Her14, WHL16, HKHK13, JSMG18, LCL+15, LFZ+17, LFWS15, LYL15, LJW+17, RD17, XWS17, YCT15, ZWM14, ZML17].

Attribute-Hiding
[OT12, ZWM14].

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

Attribution
[XHC+12, FNP+15]. Auction
[Con10, HJM+11]. auctions [MR14c].

Audience
[DT12, CHX13].

Audio
[DA12, FM15, GCK12, HGT15, KD12a, KD12b, LSL12b, NXH+17, TC10, gWpNyY+14, XNG+14, XNRIG15, ZS12, LSQ11a, SKEG14, yWpNyL11, YQH12].

Audit
[YNNR12b].

Audiating
[LMD16, TCN+17, YYS+16, YXA+16].

August
[AB10a, JY14, MV12, Rab10].

Austin
[IEE13].

Authentic
[HLT+15, SZMK13]. Authenticate
[HM12].

Authenticated
[Alo12, BCO13, BDMLN16, CLY14, CCS14, CRE+12, DS11, EAA12, ESS12, FVS17, FFL12, GTT11, GL12, GZ12, HC12, HL10a, HCL+14, HEC+12, KMY18, LHRK10, LY16, LH11b, LCCJ13, LTT10, MR14a, MMY12, MWS17b, MHKS14, MSU13, PT16, Sar10b, Smi11b, TW14, XLM+12, XHC+12, XGLM14, XZLW15, YS12, YLW13, YRT+16, Yon12, ZPZ+16, ZHX16, AIB+16, CTL13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HL11, HMP10, ISC+16, LWS10, LHH11, LML+13, NCL13, Nos11, Nos14, PPT15, SMBA10, Tso13, TKH14, WZM12a, WZM12b, WTT12, XWXC14, XCL13, YC12, YZZ+14, ZTZ16, ZXWA18, ZG10, ZZC15].

Authentication
[BS12, CHX13, GRL12, OKG+12, RGP12, WY12, ZCS15, LFGCGCRP14, PGL10].

Authentication
[ASO14, AAZ+16, ACAT+15, AUMT16, BL12, BCE+12, BCM12, BSSV12, BCD+12, Bis17, BF11, Boy16, BKJP12, BS12, CGCGPDM12, CTC+15, CC14, CCW+10, CCF17, CJ13, CD12, CJP12, CLH13, DL15, DBPS12, DKPW12, DP12, FLH13, FR16, FMTR12, FD11, GHS14, Gli12, GI12, GM14, GU13, GMMV17, GCK12, HZC+12, Hs12, HLLC11, Har13, Hay13, HBC13, HM10, HCPLS12, HCETPL+12, HKL+12, HXG+11, HCL11, IGR+16, JN12, JCM12, Jia17, JE10, KP12, KR+10, KSD+17, KPC+11, KLY+12, KTA12, KGP12, Kim15, KPKS12, KLM+12, KO16, KHH10, LLC11, LLG15, LCLL15, LNZ+13, LZCK14, LNX15, LLZ+12, MWZ12, MEF012, MKH+12, MBC15, MRRT17, MRS+17, May15, MLBL12, Mor12, MSKR17, MPM+17, NR11, NR12, NLLJ12, NLY15, Od12, OO12, OS12, PCG14, PR12, PDT12, PWVT12, RSI1, RWLL14, RSN14, Saa12a, SBS+12, Sar12].

Authentication
[SGC16, Sch15b, SKV12, ST14, SD12, Sh11, SGC14, SSA13, SC12, SZDL14, SHS12, SAA12b, SRK+17, TGC16, TYK+12, TM12, Vet10, WgMdZ12, WHZ12, WZXL12, WgMWW12, WSS12, WT10b, Xio12, YTP11, YFT17, ZB11, ZHW+16, ZLDD12, ZLDC15, AaBT16, ABK13, AATM18, Aia15, AL15,
ACF16, AZF+12, ATI+10, AN15, ACM12, BS13a, BCM13, BGAD12, BLAN+16, BAL10, BMM12, BHvOS15, BM11, CLM+12, CML+18, CLP+13b, CTL12, CS18, CH10, CCSW11, CHS11, CHLJ13, CZ15a, Chi13a, CJP15, Cho14, CL11, DCAT12, DSCS12, DLK+16, DMV15, DLN13, DZS+12, DMT12, EA12, EA11, FPBG14, FHH10a, FLL+14, FXP12, Far14, FA14a, FMA+18, GJ13, GMSW14, GH16, GCSAdP11, HU15, HS11, Ham12, HDPC13, HZC+14, HZWW17, HL14, HCM11, HLC16, HCC10, HS1, IM17, IC17, IG11, IB11, Jac16, JNUH17, Jia16, JKL+16, JMW+16, JAS+11. authentication
Based
[LYZ+13, LHL+14, LTH+15, LLC+15, LTYZ+16, LL+17, LPL+15, LSLW+15, LAL+15, LH+11, L+15, LPC+15, LNZ+15, LCCJ+15, LWCJ+14, LNYX+15, LHL+15, LW+16, LPO+17, LPGRH+14, LDB+15, LSC+12, LBR+12, MWZ+12, MLO+17, MEFO+12, MCDB+12, MV+12, MD+12, MBC+15, MKN+13, MZ+17, MCS+15, MCM+16, MCF+17, Mor+12, MSKRJ+17, MKAA+17, Muf+16, NC+12, NH+17, NXS+13, NML+12, NLY+15, pNWy+Y+14, OTD+10, PB+12, PTT+16, PYY+15, PDN+15, PPS+12, PG+12, PAS+13, PNR+17, RVH+16, RZZ+15, RS+16, Rao+17, RR+11, RDZ+16, RV+12, RS+12, Sar+18, SS+13, Sen+17, SJ+12, SP+12, SP+15b, SSA+13, SRAA+17, SH+15, SGH+15, TKR+14, TWZ+1, TW+12, TZY+12, TYM+17, TSH+17, TT+12, TTH+15, TC+10, VDB+16, VGA+15, V+12, WY+10, Wan+10, WSSO+12, WgMW+12, WYW+13, Wan+14, WLH+15, WCL+18, WT+10b, WMS+12, XNG+14, XNRG+15, XXZ+12, XMCL+13, XQ+11, Xio+12, XGLM+14, XWLJ+16, XJW+16]. Based
[XJR+17, XHZ+17, YE+12, YZLC+12, YZ+12, YGFL+15, YTS+12, Ye+10, Ye+14, YH+16, YTH+17, YYO+15, Y+17, YKNS+12, YMW+11, YK+11, YFK+12, YCY+12, ZPM+15, ZJ+11, ZXZ+11, ZDL+12, ZLH+12, ZQO+15, ZMW+16, ZXY+16, ZMM+17, ZPW+16, ZHW+15, ZVG+16, ZPXX+17, ZHL+15, AGL+16, AaBT+16, AY+14a, AHS+14, AAT+16, AA+14, ASO+14, AKG+13, ASVE+13, ATI+10, AHL+12, BS+15, BBPP+12, BGA+12, BAA+13, BOB+13, BWR+12, BW+13, BWA+13, BM+12, BC+18, BBB+16, BK+12b, CML+18, CFI+13, CFY+10, CCL+11, CT+12, CLS+12, CG+12b, CSZ+11, CHX+13, CSS+13, CW+14a, CTHP+13, CJP+12, CJP+15, CCG+10, CT+13, Cho+14, Con+12, dCCS+12, Cra+11, CDL+18, DCS+12, DZ+14, DNL+13, Dra+16, EZ+15, FH+13, Far+14, FA+14a, FA+14b, FIO+15, Fay+16, FNW+18, Gal+13, GJ+13, GMOG+15, GM+15, GKCK+11, GM+15, GCSA+11, GMS+11, G+18, HSH+11, HT+11, HGWY+11, HSM+13, HZC+14, HF+14a]. based
[HWD+16, HZWF+17, HBBR+16, HLR+11, Her+14, BH+13, HL+14, HL+11, HLC+12, HLC+16, HYWS+11, HPY+10, HKH+13, HCC+10, Hwa+11, IMB+17, IM+14, ISC+16, IB+11, IA+15, Jac+16, JNU+17, JK+13, JLT+12, JZ+10, JMW+16, JSMG+18, KPP+16, KK+13, KM+10a, KHK+13, KEG+C+11, Kim+11, KGO+10, K+11, LXLY+12, LL+16, L+12, LCL+10, LK+14, LH+10, LZJ+10, LNM+11, LMC+11, LK+12, LXM+12, LKT+12, LLHS+12, LNK+13, LXJ+14, LCL+15, LZY+16, LFZ+17, LCT+14, LFW+15, LP+14, Lin+14a, LLY+12a, LW+10, LSQ+12, LW+11b, LW+13, LZ+14, LYM+16, LL+16a, LW+13, LW+13c, LW+14, LC+14, MCN+18, MCD+15, MJGS+12, MJS+13, MLM+16, MMZ+12, Mes+15, MBB+11, MO+14, MHT+13, MG+15, NR+11, NC+13, NZL+15, PYH+18, PLPW+12, PT+14, P+10, PGL+10, PP+16, PLGMC+18, PS+14, PL+16, PK+15, PC+14, PPR+12, QZD+16, QYX+16, QMW+17, RD+17, R+10, RS+15]. based
[SPLHC+14, SGGC+16, SI+12, SY+13, SE+14, SE+16, SH+11, SM+11, SMN+14, SR+10, hSZ+15, SCK+10, SA+16b, SSA+11, SWW+16, SS+11, SKEG+14, Sun+16, SGM+16, SS+11, TPL+16, TQL+14, Tia+15, TH+16, TTL+10, TP+12, TK+14, VN+17, WYYZ+11, WW+11, WDLB+11, WLFX+17, WM+17,
Smi11a, Smi15b, Smi15a. **Blind** [AP10, Ano15a, BCPV11, LCL17, LGPR14, MR16, MN12, RS16, YMWS11, HKB14, MO14, RSM15, WLDB11, yWpWyYpN13]. **Blindfold** [Nac16]. **Blindfolded** [Vai1]. **Blinding** [CLHC12, KHHH14]. **Block** [AMV12, BRS17, BDGH15, BCG12b, CWP12, DWWZ12, EGG12, FXP17, GLLSN12, GT12, GST12, GNL12, IS12, KR11, KWS12, LWZ12, LJ17, LCIW17, LGLL12, LWPK12, LWPF12, MCD12, MRTV12, OGK15, PH12a, PRC12, Pud12, SGP12, SSA13, WW12, YCL17, ZSW12, BNY14, Jeo13, KMI11, LPZJ15, LC13, LYHH14, LWPK14, MN12, MHV15, PL16, Sar11, SKK10, TQL14, Tan17a, WB12, WWBC14, JK12]. **Block-Parallel** [MCD12]. **Block-Wise** [SS13]. **Blockchain** [Hur16]. **blockcipher** [CMMS17]. **Blockciphers** [LST12]. **Blocks** [JSK17, Bra15]. **Bloom** [ATKH17]. **Blowfish** [KB10]. **BlueKrypt** [Gir15]. **Boardroom** [LHF12]. **Bodacious** [KMO1c]. **Body** [LZCK14, ASO14, LIF17]. **body-sensor** [ASO14]. **bogus** [XWD12]. **Bombe** [Bur11, Car10]. **Bonebrake** [SS10]. **Book** [Ano15b, Ano17b, Ayu12, Bar12, Dew11, Ful10, Joh10, Keb15, Kobi10, Low12, Mei10, Mur10, Sch15a, Sha10, SR14, Ter11, Sto12]. **Boolean** [ACZ16, AS17, CW14a, DQFL12, FY11, LVV11, WT13, YCC16]. **Boolean-based** [CW14a, YCC16]. **Bootstrapping** [BGF14, GM14]. **Border** [LGM16, ZTSR12]. **BotMosaic** [HB13]. **Botnet** [NSA15]. **botnets** [HB13]. **Bottom** [Smi11b]. **Bound** [LST12]. **Bounded** [GVW12, GJO13, PDHN15, SS12a, ZYT13, IM14]. **bounding** [PYH18]. **Bounds** [Jia17, LJ15, SNJ11, SS10b, Sha10]. **Bouzefrane** [Ano15b]. **Box** [BW16, BCGN16, BR14, CPS16, HHP17, KMO14, Mic10b, Rja12, SS10b, KOS16, LRV13, MSas13, RMP10, ZZ12]. **Boxes** [NN12, LJ15, SS11]. **BRAMs** [DGP10]. **Branch** [EPAG16]. **Branchless** [RBS17]. **Brave** [KM10c]. **Breach** [SD12, JB11]. **Break** [Ayu12, Win17]. **Breakers** [Sti15, Mun17]. **Breaking** [AP13, CN12, Cop10a, KS11, TPL16, WgMDZ12, Ant14, Bri11]. **Breaks** [Ano17e]. **breakthrough** [Goo12]. **breath** [LSR13]. **Bribery** [CW12b]. **Bridging** [LRW14, TMGP13]. **Briggs** [Bai12]. **Bring** [Zha15a]. **Bringing** [Ano15c]. **British** [And13]. **Broadcast** [BS14, GMVV17, HMR14, KHI10, LMGC17, PSM17, PPS12a, WQZ16, XJW16, ZHW15, DLN13, WYYY11, XWDN12, YMM13, ZWQ11, ZZZ12, Zhu13]. **Broadcasting** [OO12, MK11, OCGD11, YY11]. **broke** [Bat10, Hea15]. **Broken** [MDAB10]. **Broker** [TKR14]. **Broker-Less** [TKR14]. **browser** [GIJ12]. **browsers** [Rec15b]. **Bruce** [Sev16]. **Brute** [CJP12, JR14, CJP15]. **Brute-Force** [JR14, CJP12, CJP15]. **BRW** [CMLRHS13]. **BTC** [CLF11]. **BTC-compressed** [CLF11]. **Buchwald** [ABJ13]. **Bucket** [BKK10]. **Bug** [Chi13b]. **Building** [BPS16, KMP11, MJS13, Sev16, WL11, LCKB12]. **Burdens** [Bla12, SR14]. **Bus** [AN17]. **Business** [LDB15]. **Buyer** [Fra16, KJ11]. **Buyer-Friendly** [Fra16]. **BYOE** [Tan17a]. **byte** [Hof15, Hof16]. **bytes** [PBCC14]. **Byzantine** [KS11, YKGK13]. **Byzantine-resistant** [YKGK13]. 

C [AD12, ACZ16, Cra14, DJS14]. **C1G2** [MK12a]. **CA** [ACM11, Don12b, Kia11, Lin14b, Pie10, Rab10]. **CABA** [MSKR17]. **CABE** [XH17]. **Cache** [AB15, DKMR15, HLAZ15, SY15a, DJL12, DK17]. **CacheAudit** [DKMR15]. **Caches** [LLGG16, CDPLCA16, DJL12]. **Caching** [HLAZ15]. **cackled** [Bai12]. **CAD** [PGL10]. **Caernarvon** [KMP11]. **Calculus** [MR10, Jou13]. **Calibrated**
[LW13c, RR11, RVRSCM12, CLL11, LW13b, JT12b, ZLW+12].

chaos-and-Hamming [CLL11].

Chaos-Based
[RR11, RVRSCM12, LW13c, ZLW+12].

Chaotic
[BCGH11, Ye10, GCH15, ISC+16, KLI+16, LW10, NES+14, WGZ+12, ZT14].

Chapman [Ful10].

Character
[SS12b].

Characteristic
[BGJT14, SR10, BGJT13, Jou13].

Characterizing
[Ash14, JR13, MPJ+16].

Chattarjee [Kat13].

cheat [WS12].

cheat-preventing [WS12].

Cheater
[KI11, Oba11].

Chebyshev [LPdS10].

Check
[GST12].

Check-before-Output
[GST12].

Checkability
[LHL+14].

Checkable
[IW14].

Checking
[GST12].

Chen
[LLLK10].

Chennai
[BC11].

China
[BYL10, IEE11a, LTW11, Yan10].

Chinese
[HF14a].

Cipher
[ABS+12, BMS12, BKLS12, Bru12, CWP12, DGI12, DJG+15, EGG+12, EKP+13, GT12, GST12, GNFL12, Hey17, IS12, KPC+16, Kla10, LCLW17, LG1L12, L1J16, MD12b, NN12, Pud12, Sas12, SEHK12, Vua10, WW12, Xie12, ZH15, ZSW+12, Zha12, Bay10, Bai12, Bor10, Die12, KM10a, LW11, MRT10, MHV15, QGG1L3, SKK10, TQL+14, WB12].

Ciphers
[BDPS12, CWWL12, zGXW12, HLW12, JMG+16, JSM18, KA17, L1ZC12a, L1ML12, MH14, P1DNH15, PPS12b, Raol17, RWZ12, RS10, SSW12, VSR12, WW1L12, XML13, XL1J16, ZHW15, FSG1W2, GLM+16, GH12, HPY10, HKK13, K1TT12, LCT+14, LFWS15, L1ZC14, RD17, SGM16, WLFX17, XWS17, LAL+15, LH115].

Ciphertext-only
[KA17].

Ciphertext-Policy
[Rao17, XML1C13, XWLJ16, ZWH15, JSM18, LFWS15, XWS17, L1AL+15, LH115].

Ciphertexts
[Sta12, WQZ+16, A1HL+12, LCT+14, NMP+13, WX1LY16].

Circle
[SC10].

Circuit
[Kar12, M1TY11, XWS17, XWLJ16, Lau12, M1S13a].

Circuit-Size
[M1TY11].

Circuits
[AIK14, AS17, BR14, GGH+16a, GH11a, GVV15, S10b, SS12a].

Circumventing
[BAG12].

CISSP
[STC11].

Citizen
[Ano16d].

City
[Ano17d].

Claims
[SK1Y14].

Class
[BCG12a, SY15a, XYXYX11, BJ16, Goo12, K1K10].

Classes
[AC1Z16].

Classical
[JE1A+15, MSU13, SSU12, CR12, RK11].

Classification
[HPC10, KAHKB17, SGP+12, ZLW+17].

Classifiers
[KGV16, LCM+17].

Classroom
[Pow14].

Claudius
[Hol12].

CLEFIA
[LWZ12, T1SLL11, T1S16a, WB12].

CLEFIA-128
[T1SLL11].

CLEFIA-type
[WB12].

Client
[AS1M12, CTC+15, FD11, RAZS15, Vle12, FA14a, FA14b, h1SSZ15, WT10a].

Client-Based
[AS1M12].

Client-Centric
[Vle12].

client-server
[FA14b, h1SSZ15].
Clients [Chi16, LH13]. cloaking [NZL\textsuperscript{15}].

Cloud [AJA16, BCQ\textsuperscript{+13}, BCK17, CWL\textsuperscript{+14}, CWL16, CDFZ16, CCT\textsuperscript{+14}, CLW16, DXA14, FCM14, FPY15, JLS12, KMSM15, KKA15, Kip15, LA15, LYZ\textsuperscript{+13}, LGR14, LLC\textsuperscript{+15}, LNXY15, MLO17, PSM17, Pet12, RSGG15, SKH17, SRAA17, TV15, Ve12, WLFX17, WWW17, XNKG15, XWSW17, XMLC13, XWLJ16, X JW\textsuperscript{+16}, YDY\textsuperscript{+16}, YHL16, YXA\textsuperscript{+16}, YMC\textsuperscript{+17}, ZDL12, ZLDC15, ZVG16, ZLW\textsuperscript{+17}, AaBT16, AZPC14, ASO14, AAZ\textsuperscript{+16}, AKK\textsuperscript{+17}, ADH17, ALL\textsuperscript{+18}, BG14, BK12b, CFVP16, CSD18, CLH\textsuperscript{+16}, CZ15b, CDL18, FH13, FNWL18, GZS\textsuperscript{+18}, HFT16, IC17, JKL\textsuperscript{+16}, LFWS15, LL16a, Wu17, YNX\textsuperscript{+16}].

Cloud-aided [WLFX17].

Cloud-Based [SRAA17, ASO14, BK12b, WCCH18].

Cloud-Manager-Based [KKA15].

Cloud-Guardians [BCQ\textsuperscript{+13}]. Cloudier [CFE16].

Clustered [DS11].

Clouds [BCQ\textsuperscript{+13}, RSN14, HFT16, IC17, JKL\textsuperscript{+16}, LFWS15, LL16a, Wu17, YNX\textsuperscript{+16}].

CoDied [WLFX17].

Cloud-Based [SRAA17, ASO14, BK12b, WCCH18].

Cloud-Manager-Based [KKA15].

Cloud-of-Clouds [BCQ\textsuperscript{+13}]. Cloudier [CFE16].

Cloud-Based [SRAA17, ASO14, BK12b, WCCH18].

Cloud-Guardians [BCQ\textsuperscript{+13}]. Cloudier [CFE16].

Clustered [DS11].

Clouding [CFF16].

Clouds [BCQ\textsuperscript{+13}, RSN14, HFT16, IC17, JKL\textsuperscript{+16}, LFWS15, LL16a, Wu17, YNX\textsuperscript{+16}].

Clustered [DS11].

Clustering [KRDH13, VSV15].

CMAC [SKK10].

Co [MBR15].

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

cocktail [OHJ10].

Code [AD12, Bud16, CCL\textsuperscript{+13}, Cop10a, Fox13, HG12, KSSY12, Mun17, PYM\textsuperscript{+13}, SS13, Sen17, St15, War11, ABBD13, Ant14, Bha16, Bri11, CCLL11, GI\textsuperscript{+12}, MCP15, McG11, McK12, Momo14, OF11, PA10, Wes15].

Code-Based [HG12, SS13, Sen17, MCP15].

code-breaking [Ant14, Bri11].

Code-cracking [War11].

Code-breaking [Car11].

Codebreakers [Ano11c, Bud16, Maf16, McK12, Smi11a].

Codebreaking [Bai12, Cop10b, McK10, McK11].

Coded [She14].

Codes [BBC\textsuperscript{+13}, Bay10, DBPS12, FMMV14, GMNS15, Gru15, HC17, KW14, MBR15, OTD10, SEY14, ST14, TLW12, WGF16, WSS12, Xie12, YTP11, Yek10, AT1\textsuperscript{+10}, Bul10a, CIZ15a, Chi13a, Fag17, Hea15, LTT10, MG15, ÖS11, Tan15b, YSL14, Ayu12, Low12].

Code-development [DF16].

Coding [Che11, CWL16, CJ13, CG14a, DG17, He12, LCLL15, Per13, AZF\textsuperscript{+12}, Bul10b, DTZZ12, JZS\textsuperscript{+10}, KM11, NDR13, OF11, Tan15b, YTM\textsuperscript{+14}, Kim15].

CoDiP2P [NCCG13].

Coercion [CW12b].

Cognitive [PP11, Kim11, OK18, RGF12].

Coin [ALR13, CLP13a, DD12a, Mat14, BB14, Wag16].

Coins [Fok12].

CoinTerra [BH15].

COIP [BCF16].

COIP-Continuous [BCF16].

Colbert [Dew11].

Collaboration [CRE\textsuperscript{+12}, PCPK14].

Collaboration-Preserving [CRE\textsuperscript{+12}, PCPK14].

Collection [Sch15c].

Collusion [BK12a, ZL12, AKY13, SKP15, SBK\textsuperscript{+17}].

Collusion-based [ZL12].

Collision-Resistant [BK12a].

Collusion [MMSD13, RVH\textsuperscript{+16}, FLZ\textsuperscript{+12}, GMRT\textsuperscript{+15}].

collusion-resistant [GMRT\textsuperscript{+15}].

Collusions [GVW12].

Color [BCPV11, DD13, FR16, LW10, MR16, YWNW15, SNM14, yWpWyYpN13, WGZ\textsuperscript{+12}, YSC16].

Colossal [Hai17].

Colossus [Cop10a, Cop10b].

Coloured [PS14].

Column [FS15].

combating [FTV\textsuperscript{+10}].

combination [Wat14a].

Combinational [MS13a].

Combinatorial [ZAC17].

Combined [PP10b].

Combining [Chi13a, CDF\textsuperscript{+10}].

Coming [SOG15].

Comment [LCLL15].

Comments [IC17, Kim15, hZSZ15, TCL15, XWS17].

Commerce [Bl16, HvSi12, Orm16, Ano11a].

Commitments [Pas13a, CSZ\textsuperscript{+11}, LP11].

Committee [Bl16].

Common [CN12, DHB16, ESRI14].

Communication
ZWS\textsuperscript{+18}, ZSW\textsuperscript{+18}, YXA\textsuperscript{+18}. conceal

[EEAZ13]. Concept [TMC15]. Conceptual

[PMZ12, SPM\textsuperscript{+13}, TSH14]. Concrete

[BS14]. Concurrent

[CLP13a, FCM14, GJO\textsuperscript{+13}, MKRM10, OOR\textsuperscript{+14}, AKG13, SRB\textsuperscript{+12}, XLWZ16]. condition [TD14]. Conditional

[HBC13, KPW13, LGL15, LSL15, MLO17, XJW\textsuperscript{+16}, FSGW11, FSGW12, HWD16, LCT\textsuperscript{+14}, SKB\textsuperscript{+17}, Tan12b]. Conditionally [ZJ14]. Conditions

[Ano17d]. Conference

[BC11, CGB\textsuperscript{+10}, Che11, Cra12, Dan12, Dun12b, FBW12, GLJC10, IEE11a, JY14, LCK11, LW11a, LTW11, Lin14b, PJJ12, SNJ11, Sah13, Yan10, AB10a, Abe10, BYL10, BL10, Gil10, GG10, HWG10, K1a11, LH10a, Pie10, Rab10, vDKS11]. Confidential [HS11, AZPC14]. Confidentiality

[BFK\textsuperscript{+10}, HLLC11, OFMR16, SZQ\textsuperscript{+17}, WDD12, Bia12, CHX13, ZHT16]. Confidentiality-Preserving

[OFMR16, SZQ\textsuperscript{+17}]. Configurable

[CVG\textsuperscript{+13}]. Configuration [Bis17]. Configurations [SS10b]. Congruence

[VM14]. conjecture [GV14a]. conjunction [Kre13]. Conjunctive

[CWWL12, BL11, ZZ11]. conjunctive-subset [ZZ11]. Connection

[CW12b, HLYS14, MZ17a]. Connectivity

[GT11]. conscious [Ree15]. Consecutive

[Tan12a]. Consensus [ABCL17, JSDK\textsuperscript{+17}]. Consequences [Ess17]. Consideration

[CJP12, CJP15, KM10b]. Considerations

[KD12b]. considering [MLMSMG12]. Consistency [BCK17, SES\textsuperscript{+16}]. Consolidated [KK14]. Constant

[App14, AEHS15, CWWL12, KOTY17, KHPP16, KMO14, LP11, Pan14, ZMW16, AHL\textsuperscript{+12}, DWZ12, LCT\textsuperscript{+14}, SGM16]. Constant-Round

[KOTY17, KMO14, LP11]. Constant-Size

[AEHS15, AHL\textsuperscript{+12}, LCT\textsuperscript{+14}, SGM16]. constants [DWZ12]. Constrained

[BSJ15, EAA12, JMG\textsuperscript{+16}, YNR12a, Yon12, DMV15, KAS15, LLZ\textsuperscript{+16}, LCL\textsuperscript{+17a}]. Constraints [CCK16]. Construct

[SGY11, WT13]. Constructed

[Ye10, ZH15]. Constructing

[CDSLY14, ZSW\textsuperscript{+12}, HRV10]. Construction

[BWLA16, DF11, EM12, FZT14, GWGC15, HHP17, KMO14, MSas12, Rog16, Sar10b, ST14, WZ15, WCL\textsuperscript{+18}, WMS\textsuperscript{+12}, XHZ\textsuperscript{+17}, LFZ\textsuperscript{+17}, MSas13, SA14, YWL\textsuperscript{+17}, YT11b, YKC\textsuperscript{+12}, ZCLL14]. Constructions

[BCF\textsuperscript{+14}, DQFL12, HL10b, KOTY17, SNJ11, SES\textsuperscript{+16}, CZ15a, CGKO11, NAL17, ZIM10]. Constructive

[Mau12, WB12]. constructs [BP10]. Containing [XWDN12]. contemporaries [LCKB12]. Contemporary

[Opp11]. Content

[BCP14a, MHT\textsuperscript{+13}, PMZ13, PZPS15, WHZ12, WZWL12, YT12, ZZZ\textsuperscript{+11}, GPN\textsuperscript{+12}]. Content-based [MHT\textsuperscript{+13}]. contest

[Cra14]. Contests [WXY\textsuperscript{+17}]. Context

[Fra16, ZCS15]. contextual [Svo14]. Continual

[BKKV10, XZ\textsuperscript{+12}, YZ12, YCYZ12]. Continual-Leakage [YZ12]. Continually

[DLWW11]. Continuous

[ACAT\textsuperscript{+15}, BCF16, DHLAW10, FMV14, MSKRJ17, PYP10, Sch15b, Yam12, ZY17a, PLGMCdF18]. Continuous-Tone [Yam12]. contract

[Men13]. contrast

[DDD14, GQ13, LWL10a, MM14a]. Contributory [WQQ\textsuperscript{+16}]. Control

[ATS15, BFK\textsuperscript{+10}, DLZ\textsuperscript{+16b}, HHS\textsuperscript{+15}, LGM\textsuperscript{+16}, MM17, MK12b, NA10b, QZL\textsuperscript{+16a}, RSN14, SG14, TBCB15, XZCL13, YTH17, ACK\textsuperscript{+10}, AMHJ10, CLH\textsuperscript{+16}, CO11, Cra11, FNWL18, FS18, JAS\textsuperscript{+11}, LCL\textsuperscript{+17a}, LCL\textsuperscript{+15}, NZ10, Sch15c, SA15, Tan12b, XHH12, ZML17, ZWS\textsuperscript{+18}]. Controllable

[FI13, ZLDC15, ZHT16]. Controlled

[FMTR12, WP17, Har16]. Controller

[GMVV17]. Controllers [AMH\textsuperscript{+16}].
comundrum [Eve12]. Conversations [WBC+10]. Converse [KPKS12].
Conversion [Bj10]. Convertible [LH11b, HL11, LHH11, WXXC14].
convolutional [MG15]. cookies [DCAT12].
Cooperative [LLZ+12, SJWH+17, ZLDC15, WQZ+13].
Coppersmith [Dra16]. coprocessor [ABC+12, BGG+13, IBM13b].
coprocessors [GCVR17]. Copy [YT12, MHT+13]. Copyright [SJ12, GJ13].
Core [LB13, YS15, RS17, HLYS14]. cornerstone [Tan17b].
Correct [PST13]. CorrectDB [BS13a]. correcting [ATI+10, LTI10, MCP15].
Correction [LSC+15, Chi13a, Sun16]. Correctness [YGS+17, WS13].
Correlated [RS10, Jia16, ZPZ+16]. Correlation [BW12, SDM+12, WWBC14, XHH12, YCL17].
correlations [Sar14]. Correspondence [SY14]. corresponding [DWZ12].
Corrigendum [WZM12a]. cosmography [Pet11].
Cost [ABC+17, AMH+16, CMLS15, CJJP12, Gi12, HLT+15, Man13, NVM+17, WMX+17, CZ14, CJP15, Sar10a, YL11].
couldn’t [Bha16]. Countdown [Zet14].
Counter [ARP12, Fay16].
Counterexample [KPW13]. Counterfeit [YFT17]. Counterfeiting [Ano16e].
counterfeits [GSN+16]. Countermeasure [BBB+16a, MD12b].
Countermeasures [BGN17, EWS14, PZPS15, DK17]. counting [LLY+12a]. Coupling [SMS14]. cover [UUN13].
Covert [EPAG16, JTZ+16, NSA15, LT13, LyWSZ10, SRB+12].
CovertBand [NTKG17]. Cozzens [Led16, Sch15a]. CP [TY16a, YMC+17].
CP-ABE [YMC+17]. CPM [FYM+13].
Crack [Fox13]. cracked [Ano13b, McG11, McK12, Moo14].
Cracking [Gri15, GAS+16, War11].
Creativity [WP15]. credential [JMW+16, KKM+13, XMHD13].
Crisis [Odh12]. criteria [ZZKA17].
cryptogra [Sac14]. CRM [LHM+15].
Cropping [SR12b]. Cross [AKK+17, CLY14, DSB15, LHM+15, MV16a, YGFL15, ZXH16, ZTSR12, SS17, der10].
Cross-Border [ZTSR12]. Cross-Domain [CLY14]. Cross-group [AKK+17].
Cryptanalysis [BW12, Bor10, CWP12, CGCS12, DG12, DJJ+15, Fari14, GST13, Gor10, Hin10, IOM12, Jeo13, Kha10, KN10, KWS+12, LHIb, LNI+11, LJT+16, LJ16, MWZ12, NXB13, OTD10, PSOMPL13, SPLHCB14, SM10a, SM10b, TY16a, TG17, Vu16, Wag10, WYYZ11, WWYY11, WSSO12, WWY14, XQL11, YCL17, YMWS11, AP11, BMB16, BKR11, Bul10a, Bul10b, Con12, Eisi10, Her10, KDH13, LLLK10, LFW+16, Nov10, RITF+11, SDM10, SDM14, Sun11, SvT10, Tam15, TSL11, WYL14, WWBC14, AY12].
Cryptanalyzing [LLL17, ZLW+12].
CryptDB [PRZB12]. Cryptic [Mar10a]. Crypto [Goo12, Pi10, Rab10, SCPSN10a, SCPSN10b, WL11, BR14, BGG+13].
Cryptoclub [Ayu12]. Cryptocurrencies [JSK+17]. Cryptocurrency [BH15].
cryptograms [Shy15]. Cryptographer [Dun12b, Kia11, Pie10]. Cryptographers [Ano16d, BPS16, Goo12].
Cryptographic [Abe12, AMKA17, AD12, AMVZ12, App15, BLP12, BCGK12, BGB12, Bar15, BCM+15, BIKK14, BLS12, BDP11, BFCZ12, BDGH15, Bla12, BKL+13, BSJ15, BNA15, CCK12, CCCK16, CFE16, jCPB+12, CBL13, Cor14b, CRM [LHM+15]. credibility [JMW+16, KKM+13, XMHD13].
Des10a, DQFL12, DR11, Ess17, FKS+13, FY11, FLW12, Gir15, GM11, GLR10, GG11, Har16, HN10, HHH+13, HST14, HSA14, IBM13b, JR13, KOP12, LVV11, Loe15, MVV12, MP12, MKAA17, Muf16, MK12b, NIS13, NA10b, PTT16, PFS12, PS14, PJ12, RPM10, RSBGN12, Rja12, RBHP15, SK11, SEY14, SKFR15, Sch12c, Sev16, SGY11, SP15b, SDM+12, SR14, SOF12, TW12, Tom16, YZLC12, YNR12a, YNR12b, YS15, ABDP15, AY14a, ABB+14, ABF+14, ABC+12, BFS+14, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGN14, EBFK13, ESPR14, GGH16b, Gil10, GLR13, KSU13, KAS15.

Cryptography: KKK+16, LGKY10, MS13c, MMZ12, MM13, Mes15, MN10, NDNR13, Pal15, PLPW13, PSdO13, QZDJ16, SD10, WT13, WMX+17, YSM14, Zim10, Sha10.

Cryptographic-Key: SK11.

Cryptographical: KU12.


Cryptography: ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, App14, AAB17, ACM+17, ARM15, Bar12, BKG12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BL14, BSR+14, BFS+14, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGN14, EBFK13, ESPR14, GGH16b, Gil10, GLR13, KSU13, KAS15.

Cryptographic-Key: SK11.

Cryptographical: KU12.

Cryptography: [KKK+16, LGKY10, MS13c, MMZ12, MM13, Mes15, MN10, NDNR13, Pal15, PLPW13, PSdO+13, QZDJ16, SD10, WT13, WMX+17, YSM14, Zim10, Sha10]. Cryptographic-Key [SK11]. Cryptographical [KU12]. Cryptography [ADD10, BCGH11, BJL12, MC11, NDG+17, PLSvdLE10, SVCV15, GCH15, HJM+11, SA14]. Cryptography [ACZ16, Ano15c, Ano15d, Ano16a, Ano16b, Ano16h, App14, AAB17, ACM+17, ARM15, Bar12, BKG12, Bar15, BRT12, BCGN16, Bon12, BKKV10, BJ10, Buc10, BL14, BSR+14, BFS+14, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGN14, EBFK13, ESPR14, GGH16b, Gil10, GLR13, KSU13, KAS15].
Different

[LyWlZZ12, YWW10]. Different

[Dierent [GZ12, HHH+13, KU12, AKK+17, ABW10].

Differential [BMS12, BNY14, CWP12, CGCS12, ESS15, FXP+17, KWS+12, LGL+12, LJF13, LJ15, LYHH14, MRTV12, PH12a, QGGL13, Sun11, WHN+12, Blo15, DDER13, LLLK10, MNP12, PBC14, SDM10, SDM14, TSL11, TS16a, WYL14].

Dieential [BMS12, BNY14, CWP12, CGCS12, ESS15, FXP+17, KWS+12, LGL+12, LJF13, LJ15, LYHH14, MRTV12, PH12a, QGGL13, Sun11, WHN+12, Blo15, DDER13, LLLK10, MNP12, PBC14, SDM10, SDM14, TSL11, TS16a, WYL14].

Dierentials [WW12].

Diering [GGHW17].

Diering-Inputs [GGHW17].

Die [LZC14, ABD+15, Chi16, Hof16, HLCL11, HLYS14, Orm16, RH10].

Diusion [ZHL15, WB12, jT12b].

DIG [NKWF14].

DigiNotar [JB11].

digit [KWH16].

Digital [AYS15, BBC+13, BM13, BCP14a, FMS12a, GP17, HPO+15, Joh10, JL16, LZH+12b, MBF+13, MSH10, MMN12, NC12, pNyWyY+14, Orm16, PH12b, PAS13b, SAA15, SM13, SC12, SOS15, TC11, TS16b, Yon11, Y+17, YLS12, dRsdLC12, AGHP14, BPP10, CCG10, FLZ+12, Fri10a, GMS11, Har14, KM11, Lan13, LWZG10, MS13b, MM14a, MO14, Sim15b, SL10, yWyNyL11, ZZKA17, Zet14, Ano13a, Ano15b, Mou15].

Dilly [Bat10].

Dimensional [Ano17d, LZH+12b, XYXYX11, DWZ12, QD16].

dimensions [Pal15].

Directed [NLLJ12, KPS10].

Direction [NS12].

Directions [BKBK14, CDFZ16, Hof16].

Directly [LZH+12b].

directory [SMBA10].

disassociation [MLS12].

Disaster [NRZQ15, BBG+17].

disclosure [DZS+12, PKA15, SB17, WGJT10].

discovery [Ano11a].

Discrete [BGJT14, KLM+12, Xie12, AMORH13, BGJT13, MM13, Mes15, TPL16, VM14].

discrimination [GPVCdR012].

Discriminative [YI14].

Discussion [Gli12, Bull10a].

Discussions [KDJ12b].

Disk [GM14, Ran16].

Disks [Mar10c].

dispatching [YTH17].

Disreputable [ABJ13].

Disruption [HK14].

Disruption-Tolerant [HK14].

Dissection [Dun12a].

Dissent [SCGW+14].

Distance [PYH+18].

Distillation [BJ16].

Distinguisher [DWWZ12, AMS+10].

Distinguishers [SEHK12, ZSW+12, AY14b, AP11].

Distinguishing [KM10a].

Distortion [FHS13, Jia17, LGWY12, MM17].

Distortions [WLZL12].

Distributed-Healthcare [ZLDC15].

Distributing [Kup13, MS16].

Distribution [EAA+16, JEA+15, Lop15b, MSU13, NNA10, SK11, SNJ11, TC10, ABB+14, BB14, BGP+17, CML16, JSK+16, JLT+12, NACL12, YWL+17, YHHS16, YL11, ZWS+18].

dithered [UUN13].

Diversity [ZTL15].

Division [SS12b, MN14].

Divisors [CN12].

Deludes [ABJ13].

DLSFe [PNRC17].

Dmail [CCS14].

DNA [WGZ+12].

DNPs [ACF16].

DNS [HLAZ15].

Do [Bow11].

doc [NN15].

Document [BTHJ12, BPP10, DBPS12].

Document-centric [BPP10].

Documents [Bla12, HCDM12, Sta13, ZDL12, CH11, GA11, SR14].

does [LRW17].

Doesn’t [RS11, SS12a].

dog [Ran14].

Doing [JCM12].

Domain [AGW15, BDFK12, CLY14, DG17, LA15, MR16, PDMR12, SGY11, WLZL12, gWyNyY+14, AMK12, BGAD12, GJ13, IG11, LXC11, LPZJ15, LBR12, PWW10, QMC17, SCKH10, yWyWyYpN13, YWK+10a, YCM+13].

Domain-Specific [BDFK12].

Domains [LQD+16, LRVW14, KGO10, NES+14].

domination [GJMP15].

Don’t [BCK17, FHV16].

Dopant [BRPB13].

Dopant-Level [BRPB13].

DoS-resistant [HCC10].

dots [Lud12].

Double [AK14, ARM15, Lin15, PKTK12, Sas12].
Double-SP [Sas12], Doubling [Zha12].

Doubly [CFZ12, CW14b], Doubly-Spatial [CZF12].

Douglas [Ber16a], Down

[Ano17e, McG11], Download [ZGC16].

DPA [ZJ11], Draft [MCF17], DRAM

[SRK17], DRAMs [LSC15], DRBG

[YGS17]. Drift [GKS17, JSZS12].

Drift-Compensated [GKS17], Driscoll

[Bur11, Joh15]. Drive

[SYC17, Mac12, SYW17]. Drive-Thru

[SYC17, SYW17]. Driven

[BMP12, DLMM18], DriverGuard

[CDD13]. DRM [Pet12], DSA [Dra16],

DSP [MS13c], DSPs [DGP10], DSS

[Ano13a], DSSH [YLS12], DTKI [YCR16].

DTLS [AP13], DTRAB [FTV10]. Dual

[BWR12, CCG16, HF14b, NLYZ12, BW13, CFN14].

Dual-Rail [HF14b], Dummy

[GST12], duplication [LWLW11]. Durable

[LY15]. During [FGR17, ABJ13, RS17].

DWT [SJ12], dyadic [MO14], Dynamic

[EKB16, FHR14, HH15, LHM15, MWZ12, MM12, NKWF14, PPS12a, PNRC17, SSW12, SY14, SKV12, SGC14, VMV15, XNKG15, XWSW16, ZXY12, ZXYL16, CTL12, CSTR16, DSCS12, EA11, GLM11, JZS10, KKM13, KH18, KBP17, LXMW12, LHM14, LZX17, NPH14, PSJ13, SES16, SSS11, SGM16, YD17].

dynamic-identity [JZS10], dynamical

[jT12b]. dynamics

[AaBT16, LTM15a, Lüd12].

dynamics-based [AaBT16], dyslexic

[Bha16].

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

E-health [WMX17, IC17, JKL16].

E-Learning [Yon11], E-passport [LZI10].

e-rental [LY14], E-Voting [LGPRH14].

E2 [WYL14]. EAC [LZI10], Each [YLL12].

EAP [FLH13, HZC14, ZCLL14].

EAP-based [HZC14, ZCLL14]. Early

[Bro11, And13]. Earth [Har14], easier

[MFB13]. Easy

[Bel16, SMDS11, Tay14, Wu16, ZDW16].

Eat [DSSD14], Eavesdropping

[CW16, Han12, PX13, YSJ14]. EC

[Dra16, CFN14, CCG16], ECC

[BSSV12, JMW16], ECC-Based

[BSSV12]. ECDSA [BBB16a, DHB16].

ECG [PLGMC18], ECG-based

[PLGMC18]. Echo [DLMM18], HGT15.

Echo-Based [HGT15], economy [Sir16].

Ecosystems [LDB15], EdDSA [YL16].

Edge [DF16, MD15, Sun16]. Edition

[Cor14a, Kob10]. Editorial [OK18].

Education [LRV14], Edwards

[JL16, LT14a, YTS12], Edwards-curve

[JL16]. Effect [PLGMC18, WB12].

Effective [HLT15, KRD13, WMX17].

Effectively [YMC17], Effects [SKV12].

Efficiency

[ABF12, Chi16, DG17, FRS16, HR10, LLML12, LCL17a, MS13b, WXL16].

Efficient [ABB13, ASBel16, BWLA16, BCCH11, BHG12, BV11, BV14, CG12a, CML18, CMLR15, CWW12, CJ13, DWB12, Dml12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTP11, GPN12, GPT12, GJJ15, GH13, GZH17, GCH15, HZC12, HZC14, HL10b, HBC13, HZX15, HKL12, HIDFGC15, HCD12, HH16, HC17, KPC11, K15, KHP16, KH10, LDDAM12, LZX12, LXX14, LCL15, LSLW15, LHY12, LWIS17, LZC17, LBOX12, MX13, MTY11, MVVR12, MU12, MP12, MC11, MN14, NES14, NDMM16, NZM10, PB12, PRC12, PG12, PCK14, PR16, RB16, RS15, SGB16, SGM16, TLCD16, TWZ11, TT12, TM18, WQZ16, WCH18, XWLW16, XMLC13, YHL16, YNR12a, YNR12b, YLY13, YNZ15, YLA13, YS15, ZQWZ10, ZLH12, ZSW12, ZX14, XYL15, ZPW16, ZWH15, AZPC14, AZF12, CH11, CCSW12, CHJ13, CZ14, Cho14, Cra11, CGKO11, EA12, PLL14, Far14, FA14a].

efficient [FA14b, F1015, FNWL18, GH16,
LLSW16, LW11b, LW11c, LW12.

**Encryption**

[LJLC12, LY+13, LHL+14, LLC+15, LTZY16, LLL17, LSW15, LH11b, LB13, LY15, LW16, LLLM12, MZHY15, MLO17, MMP14, MR14a, MTY11, MS18, MVVR12, MMS17b, MPRI12, MT12, MKRM10, MSaq12, Nac16, NdMMW16, NTY12, NMS14, NAL17, OT12, OGK+15, PMZ13, PR12, PB12, PDMH15, Per13, PTKT12, PPS12a, PMZ12, PBC18, PRSV17, RVH+16, RZZ+15, RSBGN12, RDZ+16, RVRCSC12, Saa12a, SSW12, Sar10b, Sch15a, SLGZ12, SSZ14, She14, Sm11b, Sta12, SGH15, SMOP15, TCN+17, TCL15, TMC15, Tan17b, TDTD13, TKR14, TT12, Unr15, Vai11, VSR12, VOQ15, WHC+15, WP17, WSS12, Wat12, WLC12, WDDW12, WZ15, HHHL12, WMS+12, WQZ+16, XNK15, XXZ12, XJWW13, XWL16, XJW+16, XHX+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC+11, YFK+12, YCZZY12, YKLL12, ZOC10, ZPM+15, ZDL12, ZYT13, ZWTM15, ZQG15, ZMW16, ZZZ17, ZHW15, ZY17a.

**Encryption**

[ZWS+18, AHS14, ATKH+17, Ana14, Ano13b, Ano15e, Ano16f, ABR12, AMHJ10, ACD+15, ABL12, BAAS13, BC18, BGI14, BSW12, BGP+17, CFVP16, CFZ+10, CW14b, CLH+16, CMMS17, CZ15b, CS11, Chm10, CW12a, CD10, CM13, CGKO11, DLI16a, DMM17, DTZZ12, Eve12, Eve16, FH13, FSGW11, FSGW12, Fay16, GMOGCC15, GH13, GHPG13, GLM+16, GH12, GLL+18, HGWW11, HQZH15, HWDL16, HT13, HLR11, HLL11, HFT16, HKHHK13, JCHS16, Jia14b, JSM18, JHC14, Kam16, KHB13, KKM+14, LLW16, LCL+17a, LCL+15, LFZ+17, LCT+14, LFWS15, LPdS10, LHH11, LW10, LW13b, LZZ14, LPZ15, LCY+16, LZZ17, LJW+17, LLL+18, LL16a, LW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSas13, NES+14, Pet12, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SLM10, SKB+17, Spa16, SGM16].

**encryption**

[ZWS+18, AHS14, ATKH+17, Ana14, Ano13b, Ano15e, Ano16f, ABR12, AMHJ10, ACD+15, ABL12, BAAS13, BC18, BGI14, BSW12, BGP+17, CFVP16, CFZ+10, CW14b, CLH+16, CMMS17, CZ15b, CS11, Chm10, CW12a, CD10, CM13, CGKO11, DLI16a, DMM17, DTZZ12, Eve12, Eve16, FH13, FSGW11, FSGW12, Fay16, GMOGCC15, GH13, GHPG13, GLM+16, GH12, GLL+18, HGWW11, HQZH15, HWDL16, HT13, HLR11, HLL11, HFT16, HKHHK13, JCHS16, Jia14b, JSM18, JHC14, Kam16, KHB13, KKM+14, LLW16, LCL+17a, LCL+15, LFZ+17, LCT+14, LFWS15, LPdS10, LHH11, LW10, LW13b, LZZ14, LPZ15, LCY+16, LZZ17, LJW+17, LLL+18, LL16a, LW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSas13, NES+14, Pet12, Ran16, RG10, RWZ13, RPSL10, SES+16, SE18, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SLM10, SKB+17, Spa16, SGM16].

**encryption**

[Tam15, TPL16, jT12b, WGJT10, WY10, WWYZ11, WWYY11, WHY+12, WDZL13, WLFX17, WZG+12, WCCH18, WXZ16, XWW14, XSWC10, XXX15, XSW17, YT11b, yYqWqZC13, YZCT17, YCT15, YLZ+16, YL11, ZWQ+11, ZZ11, ZLW+12, ZXJ+14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZYC+17, ZZ12, ZL12, ZDW+16, ZY17b, Zhu13, Wan14, LAL+15, Sar18, Kat13].

**encryption-based**

[BC18].

**Encryption/Decryption**

[KB10].

**Encryptions**

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

**Encyclopedia**

[vTJ11].

**End**

[Ano15c, BRR+15, BGP+17, CFE16, Chn16, RST15a, RST15b, Ch13a].

**End-to-End**

[CFE16, RST15a, RST15b, Ano15c, BRR+15, BGP+17].

**endomorphism**

[FWS13].

**Endomorphisms**

[AK14, LGH+17].

**enemies**

[Fag17].

**Enemy**

[BC14, CAC14].

**Energetic**

[PD21].

**Energy**

[Ano15d, AZF+12, ABC+17, Bla16, JEA+15, LSC+15, MP12, TLCF16, TCN+17, VN17, CZ14, ZT16].

**Energy-Efficient**

[MP12, TLCF16].

**Energy-Harvesting**

[ABC+17].

**Energy-time**

[Ano15d].

**Enforced**

[Set16].

**Enforcement**

[LSBN14].

**engagement**

[ISC+16].

**engine**

[BS13a].

**Engineering**

[FSS10, MSM18, MP12, PGL10, TQL+14].

**Engines**

[LB13, BGP+13].

**enhance**

[CZ14, SLM10].

**Enhanced**

[DLK16, DLK16, GM16, LNKL13].

**Enhancements**

[FSX12b, IA15, NNA10, CHS11].

**Enhancements**

[FSX12c].

**Enchancing**

[CSW12, IA15, Lan13, IS15].

**Enigma**

[KM15, KM16, LHA+16, Ore14, Ano16c, Bz11, Kap11, Kap13, McQ11, McK12].
Extend [TMC15]. Extended [BFMT16, DGP10, Gre17, HZW+14, HBG+17, SH15, Yam12, YSC16].

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

Extension [ARH14, EKP+13, GFBF12, GT12, RW12, SGY11, ZXJ+14]. Extensions [LWL10b]. external [ZZKA17]. Extract [AN12]. Extract-Transform-Load [AN12].

Extractability [BCP14b]. Extractable [CZLC12b, CZLC14, GGHW17].

Extraction [BWLA16, GST13, GPT14, PCPK14, GPP+16]. extractors [Zim10].

extraordinary [Hol12]. extreme [GJ13].

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

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

Fabrication-Induced [VDB+16]. Face [AQD12, XHH12]. Facial [KRBI12].

facilitate [Chi13a]. Facsimile [Ano16d].

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


Fair-Exchange [DG15]. Fairness [ALR13, Ash14, GHKL11, Wag16, MV16b].

Fake [KU14]. Fallen [HCPLSB12]. False [LLZ+12, CDGC12]. Families [KU12].

Family [BMS12, DGS12, DJG+15, FLB+10, FFL12, GN12, MGF16, YCL17]. Fanin [SS12a]. Fast [BLAN+16, Br12, CHS15, GSN+16, NR12, PRSV17, WHZ12, WBA17, WQZ+13, ZHW+16, FFH10a, KHMB13, MBB11].

FastAD [SMB10]. Faster [CN12, HVL17, TH16, Ant14]. Fault [AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JT12a, LGL+12, LCL17, LGLL12, MKRM10, MKAA17, PHI12a, RZZ+15, SEY14, YGD+17, BBBP13, PBCC14, WMYR16]. Fault-Based [BBB+16a]. fault-resistant [PBCC14].

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

FC [DDS12, Dan12]. FEAD [ZWM14].

Feasibility [AAC+16, FKS+13, WHC+15]. Feature [SGP+12, FT+10, GJ13, MHT+13].

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


Feedback-Based [PYM+15]. FEIPS [DG15]. Feistel [BFMT16, KDH15, Sasi12, SEHK12]. FHSD [SP15a]. FI [YNR12a]. FI-BAF [YNR12a].

Fiat [BDSG+13]. Fibonacci [FM15].

Fidelity [BCP14a]. Field [CLF+17, GHPS13, HSA14, SS12a, TGC16].

Fields [ARH14, BGJT14, HVL17, AA14, BGJT13, CZ15a, LBOX12, OŠ11]. Fight [Ano16e, Wu16].


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

Finger [KLY+12]. Fingerprint [MR14b, KKG14, ZHH+17]. Fingerprinting [TSH17, ZS12, FLZ+12, RS17]. Finite [BGJT14, CHS15, GMS15, HVL17, AA14, BGJT13, CZ15a, LBOX12, OŠ11].

Finite-State-Machine [CHS15]. firms [Ano15e]. First
Fully-Homomorphic-Encryption \cite{CN12}.

Fun \cite{APPVP15}.

Function
\cite{AMPH14, Bee17, FLS10, LyW1Z12, MMS17b, SGY11, WSSO12, AKY13, AP11, CMMS17, LK14, LP11, RS14, Sar11, SXL16, TQL14, WYW14}.

Functional
\cite{AS16, BSW12, Boy13, GGH16a, GVW12, LQD16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14}.

Functionalities
\cite{JR13}.

Functions
\cite{ACZ16, ALR13, BBC14, BIKK14, BKPW12, BK12a, CPS16, DMM14, DQFL12, FY11, IVV11, NR12, Rja12, RW12, SMS14, SLY16, Tan12a, YTP11, AY14a, BDP12a, CW12a, ESRI14, Gen10, HRV10, Li10, QZD16, WT13}.

Fundamentals
\cite{Joh10}.

Further
\cite{HCL14, WHY12}.

Fusion
\cite{FMS12a}.

Fusion
\cite{ABCL17}.

Future
\cite{AYS15, BCE12, BKBK14, Bon12, CDFZ16, GCK12, Mon13, Ano13d, FPBG14, Mac12, PHWM10, MJS13}.

Future-proof
\cite{Mon13}.

Fuzzy
\cite{KRDH13, NC12, SH11, XJWW13, KHM13, MMS13, SM11, SNM14}.

G
\cite{HLYS14}.

G2C
\cite{BMP12}.

GA
\cite{MMSD13}.

GA-fuzzy
\cite{MMSD13}.

gadgets
\cite{Gel13}.

Gait
\cite{XJR17, XJR17}.

Gait-Based
\cite{XJR17}.

Gait-Key
\cite{XJR17}.

Gallai
\cite{SS10b}.

Galois
\cite{CFR11, CLF17, HSA14}.

gambling
\cite{Ana14}.

Game
\cite{MZA13, LPZJ15, SD10, SKEG14}.

game-theoretic
\cite{SD10, SKEG14}.

Gap
\cite{LRW14, TMPG13}.

Gaps
\cite{SPM13, DKL16}.

Garble
\cite{AIK14}.

Garbling
\cite{App13}.

Gard
\cite{Kap11}.

Gate
\cite{Kar12}.

Gates
\cite{App13}.

Gateway
\cite{WZM12a, WZM12b, WL11, WXK17}.

Gateway-oriented
\cite{WZM12a, WZM12b}.

Gaussian
\cite{YW17}.

GCD
\cite{K11}.

GCM
\cite{SKK10}.

GCM/GMAC
\cite{SKK10}.

GDLP
\cite{MMZ12}.

Gear
\cite{AHS13}.

Gecos
\cite{GSC17}.

geese
\cite{Bai12}.

GenePrint
\cite{HQY16}.

General
\cite{FJI12, GBF12, Gue16, HP12, KOT17, LPL15, PBI2, SJW17, YFF12, ABDP15, Bai12, DGJ14, HQZH14, LWS10, WS12, YC11, ZYC17}.

General-Purpose
\cite{Gue16, ABDP15, DGJ14}.

generalisation
\cite{LR15}.

Generalised
\cite{Hes12}.

Generalization
\cite{GMNS15}.

Generalized
\cite{BFMT16, LPL15, PC14, TY16b, Ye14, ZAC17, ADG16, BNT17, KL11, NC13, YMSH10}.

Generating
\cite{ADD10, LCL17b, NN12, XYXY11, AGHP14, LW13b}.

Generator
\cite{ABS12, BCGH11, BH15, LTC15b, MR14a, MJGS12, NIS12, PS14, SOS15, SRK17, XJR17, Aia15, ACD15, GMRT15, GCH15, HKMB13, KKM13, XM13, YDH15}.

Generators
\cite{AS17, BCGH11, BH15, LTC15b, MR14a, MJGS12, NIS12, PS14, SOS15, SRK17, XJR17, Aia15, ACD15, GMRT15, GCH15, HKMB13, KKM13, XM13, YDH15}.

Generator
\cite{ADD10, BCK12a, CDK10, MVV12, NNAM10, HK14, CFY10, LGKY10, MRT10, PLSD10, SH11, SM11, XSWC10}.

Generators
\cite{AS17, LTKP16, MFG16, NIS12, PFS12, CP13, HRV10, MG15, Sti11, Zim10}.

Generic
\cite{BWLA16, BR14, Chi16, GWWC15, HXC11, Sar10b, SY15a, WCL18, ZCL14, HQY16, YT11b}.

generically
\cite{MHKS14}.

Genetic
\cite{JK13, MM17, ASVE13, EEA13, PTK14}.

genius
\cite{Hai17}.

Gentry
\cite{GH11b}.

Genuine
\cite{HR13}.

genus
\cite{FWS13}.

geo
\cite{Har14}.

geo-location
\cite{Har14}.

geodesics
\cite{ZZC14}.

Geographic
\cite{LC17}.

Geolocation
\cite{FPY15}.

Geometric
\cite{DSB16, GTT11, WLZL12, YWW15, CLZ17, GZHD12}.

geometrical
\cite{TC12}.

Geometrically
\cite{TC12}.

Geometry
\cite{tWmC12, CFR11, CZ15a}.

German
\cite{BDFK12, Blö12, Buc10, Cop10a}.

Germany
\cite{FBM12, GLIC10, Sen10, Wat10}.

Gesture
\cite{LCL17b}.

Gestures
\cite{AUMT16, GCA11}.

Get
\cite{GPT14, Sch11}.

Getting
\cite{ESS15}.

GGH
\cite{LH10b}.

Ghost
\cite{CDA14}.

GHZ
\cite{CCL13}. 
Nov10]. **Hardware-Based** [HLN+10].

**Hardware-Enforced** [Set16].

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

**hardwares** [SKH15]. **Hardy** [Xie12].

**Harmonic** [YWNW15]. **Harnessing** [DFKC17].

**Harvesting** [ABC+17, ZGC16]. **HAS-160** [WLC12].**Hash** [Ano12, AMPH14, BHH+15, BK12a, CLP13a, jCPB+12, CZLC12a, CZLC12b, CZLC14, CJP12, EAA+16, FLS+10, GI12, HCPLSB12, Hül13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, NTV12, NR12, NXB13, PTT16, Rja12, SGY11, WSS012, ZMZ17, AY14a, AKY13, AP11, CJP15, ESR14, KKG14, PPB16, RS14, SPLLHC14, SXL16, WYW14].

**Hash-Based** [BHH+15, GI12, HCPLSB12, Hül13, HRS16, HBG+17, MKF+16, MCF17, MKAA17, NXB13, CJP12, CJP15, PPB16, SPLLHC14].

**Hashing** [AAE14, ASBdS16, BHKN13, BKL+13, Kaw15, CP13].

**Haskell** [Rus15].

**hatching** [WYK12].

**HB** [HSH11, PY11+18].

**HDH** [PDNH15]. **Headline** [YGFL15].

**Health** [LYZ13, LHL15, Raol7, ZVG16, BC18, IC17, WMX+17, JKL+16].

**Healthcare**

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

**Hearing** [Bla16]. **Heartbeat** [IA15].

**Heartbleed** [DKA+14, Ven14].

**hedging** [RY10]. **Heights** [Gen13].

**Helios** [CFE16]. **Hell** [Han12].

**Hellman** [ABD+15, Ch16, Hof16, HLCL11, HLYS14, LZC14, Ornn16, RH10].

**Helmut** [Mur10].

**helped** [Smi11a].

**HeNB** [CLM+12].

**Herodotus** [Keb15, Mac14].

**heroine** [Fag17].

**Heterogeneous** [SP15b, SZMK13, SCKH10].

**Heuristic**

[BGJT14].

**HEVC** [DG17].

**HIBEB** [LW11c].

**Hickory** [NN15].

**Hidden**

[FMS12b, PSS+13, YLL+12, ZYT13, BDK11, LCT+17a, Sch15c, Sm15a].

**Hiding**

[GGH+16b, GL10, JHHN12, MK12b, OT12, XLM+12, XGLM14, ZXIW15, DDM17, KWH16, LXLY12, LT14b, UUN11, WLY13, WZLW13, ZWM14].

**Hierarchical**

[ADM12, BSSV12, FSX12a, LSLW15, NMS14, NLY15, OT12, WYLM16, ZMW16, ZHW+16, DSCS12, KPB17, LFZ+17, NZM10, RG10, SE14, SE16, WWYZ11].

**Hierarchy** [NAlb10b, VN16].

**High**

[AW17, ASBdS16, Ano17d, ARM15, Bar15, BDL+11, DM15, DG17, GL12, GCS+13, HZ11, KMP+11, KPC+16, LTKP16, LCK11, LPO+17, MS13b, MS13c, PCPK14, WYCF14, WL11, XNRG15, ABB13, GZHD12, GCVR17, KL13, MAK+12, RS17, WLH13, WLY16, WZLW13, WKLH11].

**High-Assurance** [Bar15, KMP+11, WL11].

**high-capacity** [GZHD12].

**High-Dimensional** [Ano17d].

**High-Efficiency** [DG17]. **High-Impact** [DM15]. **High-Level** [AW17, KPC+16, ABB13].

**High-Performance**

[GCS+13, LPO+17, GCVR17].

**High-Rate** [PCPK14].

**High-Security**

[WWCF14, BDL+11].

**high-speed** [ARM15, HZ11, LTKP16, BDL+11, KL13].

**high-throughput** [PCPK14].

**Higher**

[LWK12, PRC12, gWnpY+14, ZSW+12, LWKP14].

**Higher-Order** [LWK12, PRC12, ZSW+12, gWnpY+14, LWKP14].

**Highly**

[SZDL14, ACD+15, DT13].

**HIGHT** [CWP12, WWBC14].

**hijacking** [DCAT12].

**HILL** [KPW13, KA17].

**HIMMO** [GMRT+15].

**Hindering** [BTPLST15].

**HISS** [DT13].

**histogram** [CSS+13, Lin14a].

**Historians** [Cer14].

**History**

[Hai17, Han12].

**Hitler** [Hea15, Moo14].

**HMAC**

[GWM16, MAK+12, YGS+17].

**HMAC-DRBG** [YGS+17].

**HMAC-SHA256** [GWM16].

**Hoc**

[PD14, She14, XHC+12, KM10b, LXJ14, SGCR+16].

**Hoffstein** [Mei10].

**Holden**
Identity-Based

ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CGL+12, Chi12, FHH10b, FZT14, FSX12b, FSX12c, FSX12a, FY13, GJJ15, GJZ17, HZC+12, HSM14, HZX15, LSL12a, LLC+15, LTZY16, LSLW15, LH11b, LSC12, LBR12, MLO17, RDZ+16, SGH15, TKR14, Wan14, XZX12, XJW+16, YZK+12, YKC+11, YFK+12, YCZY12, ZLH+12, ZMW16, ZPXX17, CSZ+11, HSM13, HYWS11, LKAT12, LXJ14, MJGS12, RS15, SWW+16, Tia15, TH16, ZDW+16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HDWL16, HZW17, HLR11, HL11, HPY10, Hwa11, LK12, LCT+14, MJS13, MM13, NCL13, QYWX16, RG10, SE14, SE16, hSZZ15, SA16b, SFAF11, SG16, WLFX17, XW12, XCL13, YWL+17, yYqWqZC13, YMSH10, YKC+12, YXA+16, YNX+16, ZZ12, LZJX10, PN10, Sar18, Kat13.

Identity-Hidden

PSS+13, IImD

ACAT+15, 1Ds [IEEE]

IEEE


IEEE802.16e [HLLC11]. if [ABJ13, Rus15].

IFIP [GLIC10]. IFF [MMZ12]. Igor

[Sa10]. II

[Mu17, SCPSN10b, SMOP15, ZWS+18].

III [SMOP15]. Illegal [ABJ13]. Illogical

[Hel17]. Illumination [KLY+12]. Illusion

[GH514]. Illustrated [Cop10a]. Im

[BG1+10, BG1+12]. IM [Che11]. IMACC

[Che11]. Image [BAAS13, BWR12, CFH14, DA10, JKE12, KPS10, LA15, LLI17, MBC15, PW10, R16, RVRSCM12, SH11, SM11, SJ12, SGP+12, SSA13, SRAA17, SZZT18, WH12, WZCL12, WYV+13, WYCF14, WK12, YLL+12, YWNW15, Ye10, Ye14, YH16, ZZ+11, BWA13, BM13, CT11a, CW14a, EA11, GKCK11, HLC16, KM11, LXC11, LW10, LW11, LW13b, LPZJ15, MO14, NES+14, PTK14, SE18, Sch12a, SM13, SNM14, Sun16, JT12b, TSL10, TLL13, UUN11, UUN13, yWpWyYPN13, WZG+12, WKHI11, WOLS12, XSW10, YWL+17, YC11, YCC16, YSC16, ZLW+12, ZT14, ZL12].

Image-Guided [CFH14].

Image-Scrambling [LLL17].

ImageMagick [Tay14]. Imagery [BCP14a].

Images

[BCPV11, CLF11, FR16, GL10, LC15, LLY+12b, MR16, NC12, Yan12, dRSdVC12, AMK12, DD13, HWYW14, LW13b, MM14a, MKH+12, UUN13, WLH13, ZWLW13].

imaging [WW13]. IMI [PN10]. imitation [Hai17].

Impact

[Al12, BLS12, DM15, SF12]. Impartial

BCF16]. Imperceptibility [HTG15].

Imperceptible [Lin14a]. Imperfect

[ABD+15, BHvS15]. impersonation

[AAT18, GBM11].

Implants

[Mic16, SSP+13]. Implausibility

[GGH17]. Implementation

[BB16, BSJ15, BDM16, EGG+12, GP17, GL12, GPT12, GCS+13, HF14b, KB10, KGV16, MFG16, MAS16, NdMMW16, QL17, RPM10, VKP17, ZPM+15, BD+12, GH13, HBBRN+16, KY10, MM4a, MNW15, NES+14, PBC14, SK14, SAAB10, SF12].

Implementations

[BFCZ12, BFK16, BDGH15, BJ10, Bru12, CML13, CBL13, ERRGM15, LGH+17, ML10, Tom16, YZCL12, ABB13, ABF+14, BFG+14, BJR+14, CFN+14, CGH17, LBOX12, STA11b]. Implementing
[Dav11, GH11b, HTZR12, LTC+15a, SG15, SLM10, VOG15, SA16b]. Implicit [DWZ12].
Imply [ALR13, LRW17]. Importance [YL17, MLMG12]. Important [TC10].
Impossibility [ACM+17, BCF+14, Mat14]. Improbable [TS16a].
Improve [AQD12]. Improved [BCP14a, Chi12, CGKO11, GLLSN12, IK15, JLH12, KZG10, LT14a, LWZ12, LJF16, LHH11, LCCJ13, LC15, LLML12, PH12a, QZ14, SK12a, SEHK12, SP15a, SLM10, VOG15, SA16b, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GLW13, PWLL13, SDM10, XHH12, Wan14].
Improvement [FRS+16, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNM+11].
Improvements [EA12, HRV10, Tso13]. Improving [AB15, BCM+15, Chi12, FMS12b, GMS11, HCLL11, MHC12, Sar10a, SS11, YKBS10].

[CN12, CNT12]. **Integral** [AY14b, LWZ12, ZSW12, SM11, SM14, SH11]. **Integrated** [LY15, MU12, AL15, SY12]. **Integrating** [CFZ10, OdH12, HLYS14]. **Integration** [AOD12, Kar12, ZWY13]. **Integrity** [BCP14a, BCK17, FYMY15, MV16, PH12b, ED17, SW+16, YXA16, YNX16]. **Intel** [SF12]. **Intelligence** [Dew11, Bud16, GW14, Han12, Maf16]. **Intelligent** [AMK12, IEE11a, SAJL16, Wat14a, HLYS14, MKH12]. **Inter** [LBR12, BGAD12, SCKH10, SA15, YWK10a]. **Inter-domain** [LBR12, BGAD12, SCKH10, YWK10a]. **inter-router** [SA15]. **Interactive** [CFZ10, DFGW11, BCI13, Pas13a, PPR12]. **interceptor** [Cho10]. **Intercepts** [Don14]. **Interface** [WBA17]. **intermittent** [CL16]. **International** [ACM10, ACM11, BC11, CGB10, Che11, Dan12, FBM12, GLIC10, JY14, LCK11, LW11a, LTW11, MV12, PJ12, Sen10, WLR10, Yan10, AB10a, Abe10, Ano11a, BYL10, BL10, Gil10, GG10, HWG10, LHI10, IEE11a]. **Internet** [Ano13d, LFGCGRP14, TW14, AAC16, Ano13b, CLF17, CW12b, DR16, DG15, Gel13, JTZ16, LNK18, LGH17, LSG16, MJJS12, MJS13, MCF17, NLLJ12, NY15, Orm16, PLGMCdF18, SB17, SYW17, SYC17, SKEG14, WCC18, YCT15]. **Internet-Draft** [MCF17]. **InterNetworking** [SAAB10]. **interoperability** [HWW15]. **Interplay** [YD17]. **Interpolation** [JTZ16, KU14]. **Interpretation** [MZ17b]. **Interpretation-Based** [MZ17b]. **Intersection** [LY16]. **Interval** [PPR12, Cra11, DTZZ12, LWY12, MO14]. **Interval-based** [PPR12, Cra11]. **Intra** [HF14b]. **Intra-Masking** [HF14b]. **Intrinsic** [SN10, NS10, RCW15]. **Intrinsically** [SRK17]. **Introducing** [Fay16]. **Introduction** [DK15, Gas13, G13, JSK17, Low12, Mei10, Sch15a, SOG15, Sta11b, CM13, Buc10, Led16, Sch15a, Ful10, Mur10]. **Intrusion** [NSMS14, SAJL16, SBV14, YKC12]. **Intrusion-Resilient** [YKC12]. **Intrusive** [ARJ12, MFH13]. **invariance** [yWpNyL10]. **Invariant** [CSW12, NKWF14, RS16, WYW13, YWW15, GZHD12, LCM11]. **Invariants** [RK14, CDSLY14, KK10, MZ17a, TLL13]. **Invention** [ORM16]. **Invents** [Ant14]. **Inversion** [KHH14]. **Invert** [ZWT15]. **Inverted** [ZXY16]. **Invertible** [SLY16, UUN13]. **Investigating** [SPM13]. **Investigations** [Bla16, Har14]. **Invisibility** [BN14]. **Invisible** [Keb15, Mac14, SY13]. **InvisiMem** [AN17]. **INVISIOS** [ARJ12]. **Involving** [HLCL11]. **IoT** [ATM18, CCM17, NVM17, SGC16, TG17, WCFW18, WXY17, YFT17, YTH17, ZCWS15]. **IoT-Based** [YTH17]. **IoT-Enabled** [SGC16]. **IoTs** [SAJL16]. **IP** [AGL16, AZH11, PA10, RS17, SP15a, TJSF12, WBC10]. **IP-SEC** [PA10]. **IPE** [ZM16]. **iPhone** [Wu16]. **IPs** [GSFT16, NDG17]. **IPv6** [KL12]. **IRC** [HB13]. **IRC-based** [HB13]. **IRIW** [JKHeY12]. **irregular** [YWL17]. **ISBN** [Ano15b, Ano17b, Bai12, Joh10, Mur10, Sch15a]. **ISBN-13** [Joh10]. **Islet** [Dam12]. **ISO** [BCM12, BCM13, TS16a, WW11C]. **ISO/IEC** [BCM12, BCM13]. **Isogenies** [Y17]. **Isogeny** [Lau17]. **Isolated** [YS15]. **Isolating** [LG12]. **ISSAC** [Wat10]. **Issue** [Ano13, Ano16a, Ano16b, Ano16h, CSY18, GO17, LW13a, XW13, PHW10, Sim15b]. **Issues** [ABHC16, PZPS15, JAE10, KIN16, MV15]. **ISTE** [Ano15b]. **Italian** [Sac14]. **Italy** [Cra12]. **items** [YD17]. **Iterate** [HHR11]. **Iterated** [LPS12]. **iterative** [SXL16]. **ITUbee** [FXP17]. **J** [Bar12, Led16, Sch15a, WZM12a]. **J2ME** [GPT12]. **J2ME-Enabled** [GPT12].
[AS17, GT12, Gir15, PDHN15, PNRC17, Zha12]. **Length-Doubling** [Zha12]. lens [PHN+12]. **Less** [TKR14, GM13, Kam16].

**Lessons** [KMP+11, TGC16, WL11]. **Level** [AW17, Ano15a, BRPB13, BKJP12, CCW+10, DA10, Gli12, JWJ+17, KPC+16, KGP12, MV16a, ZLDC15, ABDDB13, MEF012, RS17, UUN13, YT11a, Bai12].

**Leveled** [BGV14]. leveling [LY15]. Levels [HLCL11, LRW17]. Leveraging [DMS+16, HCM11, MvO11, SKGY14].

Lewis [Mar10a]. Lexicographic [ZAC17]. LFSR [HLC12, MRT10]. LFSRs [QGGL13].


Lost [WBA17]. love [Fag17, FHM+12]. Lovers [Keb15, Mac14]. Low [ABC+17, AWSS17, BCO13, BCG+12b, CMLS15, DJL+12, FHS13, GST13, G12, LJK17, LBR12, Man13, NVM+17, RS17, SA116, WT10b, ZJJ11, C14, Chi13a, LGKY10, LKAT12, MV15, NR11, ZP+16].

Low-Distortion [FHS13]. low-end [Chi13a]. Low-Latency [BCG12b].
Low-Overhead [AWS17]. Low-Power [SAJL16, WT10b]. low-resource
[MHV15, ZP1+16]. Lower [LJ15, Sha10]. ip231 [LK14]. LPN [HKL+12]. LPSNR
[LP12]. LR [YZ12, ZWM14]. LR-FEAD [ZWM14]. LR-UESDE [YZ12]. LSB
[DA10, Tan12a]. LTE [CLM+12, LLLS13, QMW17, SGC16, TM12].
Lucas [RW12]. Lucia [DDS12, Dan12]. Lucky [AP13]. Lumpur [HWG10]. LUT
[ABCdS16]. Lyra2 [ASBdS16]. LZSS [CFY+10].

M [Orm16, Hs12]. M-Identity [Hs12]. MA [ACM10]. MAC
[Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN16]. MacGuffin
[LGL+12]. Machine
[AGHP14, Ano16c, CHS15, Sch12a, ABBD13, GJ13, Gup15, LLZ+16, LHA+16, QMC17, RY10, TTL10, War11, WS14].
Machine-generated [AGHP14].
machine-to-machine [QMC17]. Machines
[Ber16a, HB17, BBDL+17, KSU13, PWW10].
Macrakis [Keb15]. MacWilliams [OS11].
Made [Orn16, Sma16]. magic [PHN+12].
Magnetic [VGB+16]. Magnifying
[DKL+16]. Main [AMH+16, LY15, CS11].
Maintaining [WP15]. Make [Ayu12].
makes [Ken11]. Making
[BG14, dCCSB+16, Gel13, LA10, ZDW+16].
Malaysia [HWG10]. Malicious [AAE+14, BL15, TM18, VGA15, BK12b, WTT12].
malleable [KTT12]. Malleable
[CKLM13, MSas12, CG14a, FMV14, LP11, MSas13, OOR+14, Pas13a]. Mallory
[FHM+12]. Malware
[ATS15, GAF+15, Goo12]. man
[And13, Bat10, Kap13, Moo14].
Management
[ASM12, BS13b, CCFM12, CSL+14, GOPB12, KP12, KKA14, Lop15b, MKF+16, PN10, TMGP13, Vle12, YXZ+12, YSS14, ZJ11, ZTMR12, BMB10, BB16b, CFI13, Cha13c, dCCSM+12, dCCSB+16, Din10, KH18, MLNSMG12, MGP10, PLCS11, Sch11, SR10, SA15, SW+16, WW17, WQZ+13, YLS12, ZMM+10, Ano15b].
Manager [KKA15, Kim16]. Managing
[MD15, BC18]. MANET [KTU16].
Manhattan [SS10c]. manipulation [OF12].
Mansour [DKS12, LP12]. Manual [Sac14].
Manuale [Sac14]. Manuscript [Ano16d].
Many [LB13, HRS13, ZQW10].
Many-Core [LB13]. many-to-one
[ZQW10]. Map [XYX11, ISC+16, LZY+16, PC14, SE18, ZT14]. Maple [G13].
Mapping [CBL13, MI14]. Mappings
[MC11, CDPLCA16]. MapReduce
[LJLC12]. Maps
[Ye14, BAAS13, KLW+16, LW10]. March
[Ano10, Cra12, DDS12, Dan12b, IEE11a, Pie10, Sah13, WZM12a]. Marche
[CCFM12]. Margaret [Led16, Sch15a].
Marion [Kap13]. market [YW10b].
Markov [CR12]. Marotto [SE18].
Marshall [Don14]. Martin [AB13, Hof16].
Maryline [Ano15b]. Mashup [HTZ12].
Mashup-Providing [HTZ12]. Masked
[WH17]. Masking [HF14b, PYM+13]. Mass
[BPR14a, BPR14b]. Masses [Ano15c].
Master [Dew11, Mar10a]. Matching
[Lin15, Tan12a, MR14c, MHT+13, PPTT15, SS17]. MathCW [Bee17].
Mathematical
[Bee17, FGPGP14, Ham17, IBM13a, Mei10, Sch15a, Wes16, KM14, OO10, Sta11b].
Mathematical-Function
[Bee17]. Mathematician
[Ano17c]. mathematicians [Acz11]. Mathematics
[Ano17b, Ayu12, Led16, Sch15a, Ter11, CM13, Kra12, PHWM10, Wes16]. MATLAB
[TRD11]. Matrices
[AMVZ12, BNA15, AGK13, FES10]. Matrix
[BFCM16, SK12a, TD13, Ye10, Cha13b, TK14]. Matter
[Rau15, SS12a, DKA+14].
Max [And13], Maximizing [DBPS12].
MitM [TY16b]. mix [WGJT10]. mix-networks [WGJT10]. Mixed [ST16]. mMTC [CML+18]. Mo [RBS+17]. Mobile [BCD+12, FD11, GPT12, GdM16, HvS12, HLKL15, KP12, KKA15, May15, NRZQ15, Sch15b, SFE10, She14, SAA12b, WPZM16, WT10b, XHH12, XNKG15, XHC+12, YHL16, Yon11, ZLDD12, Aia15, AAZ+16, ALL+18, CLP+13b, CTL12, CCSW11, CTL13, FHH10a, FA14b, GM16, GH16, HZWW17, HL14, IB11, Kem11, KKA14, KKM+13, KKM+14, KKG14, KSB+17, LH13, OYHSB14, Par12b, hSZZ15, SSAF11, SKB+17, TKHK14, WT10a, YNX+16, ZDW+16, ZC12, MBF+13, SLL10].


Modelling [CJFH14, GBNM11, LTKP16, MKN13, PAS13b, Ana14, CDGC12].


modified [CTHP13, EEAZ13, MM14b].


Moments [WLDB11]. Monte Carlo [Gil10].

Money [RBS+17]. Monitoring [BCE+10, ASO14, KO16]. Monitors [IF16].

monopolizable [DJL+12]. Monte Carlo [CR12].

Montréal [JY14]. Morphing [MBC15].

Morphology [IA15]. MorphoSys [MD12a].

Morris [Gre11]. most [ESR14, GIJ+12].

Motion [GZH17, JHN12, AP10, SYW17].


Movement [ERLM16, ZP16].


MSP430X [GL12]. MST_1tn3 [SvT10].

Much [DL15]. Muhammad [ABJ13].

Multi [ASS15, BBEPT14, BRT12, CWL+14, Ch12, GVW12, GJ17, HC12, HRS16, IG11, KTT12, KMO14, LyWSZ10, MZH15, MEFO12, MLBL12, NGAuHQ16, OKG+12, OSS16, SK12b, TWZ+12, TMY+17, Wan14, WOLF15, XWSW16, YWW10, Ye14, ZC13, ZQQ15, ZLDC15, BGG+13, CLP+13b, CFVP16, CG12b, CLHJ13, CW14a, CZ15b, DFJ+17, GMGCCC15, GPVCbdRO12, GZS+18, HL14, HL11, HCCC11, HLC12, ISC+16, JHS16, KM11, LXMW12, LXX+14, LCT+14, LH13, LWY12, Mas17, QMC17, SCY15, SWW+16, SSS11, TLL12, WDZL13, WXK+17, XW16, YCC16, ZKK17].

multi-agent [GPVCbdRO12].

multi-architectural [DL15].

multi-authenticated [HL11].

Multi-Authority [ZQQ15].

Multi-Biometric [NGAuHQ16, MLBL12].

Multi-bit [TWZ+12]. Multi-ciphertext [KTT12].

Multi-cloud [CFVP16, SWW+16].

Multi-criteria [ZZKA17].

Multi-domain [IG11, QMC17].

Multi-factor [HC12, CLP+13b].

multi-flow [LWY12]. multi-gateway [WXK+17].

Multi-hop [LCT+14].

Multi-instance [BRT12].

Multi-Keyword...
[CWL+14, XWSW16, OSSK16, GZS+18, LK+14]. multi-lateral [SCY15].
multi-layered [JCHS16]. Multi-Level [ZLDC15, MEF012]. Multi-linear [BBEPT14]. Multi-Party [KMO14,
multi-server [CLHJ13, HL14, ISC+16, LXMW12, LH13, SSS11, TLL12]. Multi-Signature [ASS15]. multi-stage [Mas17].
Multicast [CC14, BAL10, HGWY11, LTT10, NACLR12]. Multicoupon [HIDFGPC15]. Multidevice [DPCM16].
Multidimensional [Her10, WWBC14, HMCK12]. Multifactor [MMY12]. Multigigabit [PP10b].
multi-hop [ADF12]. Multilayer [NXH+17]. Multilevel [FMS12b, HF14a, NSA15].
Multimedia [NSA15, PMZ13, PZPS15, PYM+15, WLY+15, ZW15, Zha15b, ZSA12, HM10, HWYW14, LLLK10, Wan13,
XWZW16, TW14]. Multimodal [GM16, Sar18, AT1+10, MHT+13].
MultiObjective [ZAC17]. Multipartite [HR13]. Multiparty [BDOZ11, CCL+13, Fri10b, ADMM16, LDDAM12]. Multiple
[DSB15, Dun12a, FR16, KBL11, LTX+15b, LQD+16, NDC+13, SY14, SC10, Sta12, GZS+18, LWZG10, LTC+15a, LZC17, MN14,
RWZ13, TKHK14]. Multiple-Parameter [NDC+13]. multiple-precision [MN14].
Multiple-Secret [SC10]. Multiplication [AK14, CMO+16, HVL17, SK12b, YTS12, AAT16, SKH15, SF12]. multiplicative
Multitone [GL10]. Multivariate [DP17, ST16, YL17, YDH+15].
multiwatermarking [WL12]. multiwavelet [PPW10]. Munich [Wat10].
Music [NTKG17, Wes16]. musical [Ana14].
Mutt [Ran14]. Mutual [CJP12, GI12, GM14, Kim16, SBS+12, WT10b, AATM18, CJP15, Cho14, CL11, FHH10a, Far14, GH16,
HDPC13, IB11, JNUH17, KLW+16, LIK+17, SPLHC14, TG17, XMHD13]. MVP [CD12]. mvSERS [HLKL15]. My [GPT14].
NDSS [Ano10]. nearest [LVRY10].
neighborhood [LVRY10]. nearly [PHGR16]. necessary [TD14]. needs [Sch12b]. neglected [Joh15]. Negligible
[ZMM+10]. nested [FHH10a]. Net [LHF12].
Nets [PS14]. Nets-based [PS14]. Network [Ano10, Bis17, CWL16, CJ13, CLH13, DRS16, Hay13, HDHW12, Kim15, KCC17,
LCL15, LY16, LTW11, MJGS12, NNA10, NRZQ15, SGC16, She14, TLW12, VKP17, VFV17, VQA15, VKE15, WP15, YZLC12,
YSJL14, AKM+11, AL15, Ano11a, AZF+12, CL11, DLK+16, FPBG14, HWG10, HB13, HKB14, JZS+10, LH11a, LK13, MZA+13,
MJS13, NDN13, OF11, PL16, RCW15, Ser12, SCKH10, Sta11a, Tan15b, WYL13, WS14, YLS12, ZOSZ17, Ste15b].
Network-Assisted [KCC17]. network-based [YLS12]. Network-Coded
[She14]. Network-on-Chip [Bis17].
Networking
[LCK11, LLZ+17, ZHL15, Kim11, LCM+17].
Networks
[ABCL17, ABC+17, BN14, BPSD17, BFM16, CS14, D516, DF16, FMS12b, GMVV17, HZC+12, HBCC13, HK14, KH10, LL21, LL15, LHM+15, LZC14, LCJ14, LL+12, MPM+17, NSA15, NYR+14, OO12, OKG+12, PYM+15, PCPK14, RWL14, SWPD12, She14, SP15b, Smi11b, SL11, SZT18, TCN+17, WXL+17, WLY+15, XHC+12, YM16, ZC13, ZW15, Zha15b, ZLDD12, ZSA12, Aia15, AS14, AIB+16, ADF12, BDK11, BLAN+16, BBB16b, CDGC12, CML+12, CLS12, CL11, DSCS12, DK12, DNL13, EEAZ13, FA14b, FMA+18, GH16, HGWW11, HZC+14, HZWW17, HCCC11, HCM11, HTC+10, JNU17, JLT+12, JMW+16, KM10b, KLC+10, KO16, KLW+16, KD+17, LLLS13, LC17, LMJC11, LX14, LIK+17, LNK+18, QMW17, RGP12, SGGCR+16, SA12, SZMK13, hSZZ15, SKK10, TKHK14, WGGJ10, Wan13, WW14, WXK+17, WX13, XWDN12, XHCH14, XMHD13, YHHS16, ZWQ+11, ZBR11, ZCL14, ZTZ16, ZHH+17, ZX11].
Neural
[YZLC12, EEAZ13].
Neuroscience
[BSR+14, JW14].
Neutrality
[Kha10].
Neutrality-Based
[Kha10].
Nevada
[IEE10].
ever
[Bai12].
Newly
[ABJ13].
Newman
[And13].
News
[Edw14, Edw17, Sav13a, Sav15, Sav16].
Next
[MR14a, MJS12, Aia15, ACD+15].
Next-Generation
[MR14a].
NFC
[LY14].
Niederreiter
[Ter11].
Nine
[Mac12, LHH14].
NIZK
[Pas13a].
NIZKs
[CLLM13].
NN
[ZHT16].
No
[WDDW12, Wu16, KKH14, MPJ+16].
nobody
[Sto12].
Node
[NYR+14, OKG+12, LC17, PX13, SAAB10].
Node-Capture
[NYR+14].
Nodes
[VGA15, ZYL+10].
Noise
[ASN11, YMA17, ZHH+17].
Noised
[JLS12].
Noisy
[JLS12, HZW+14].
Non
[AS17, AMH+16, BCI+13, CG14a, CPS16, DJL+12, EK+13, FHKP17, FMMV14, HK14, KTT12, LLG15, MFH13, MSas12, OOR+14, Pas13a, Svo14, WgMW12, YNQ15, YKLL12, ZLDD12, AI14a, BS15, CS11, ESR14, GIJ+12, Kre13, LP11, MSas13, SES+16, SXL16, XSWC10].
non-adjacent
[Kre13].
non-associative
[BS15].
Non-Black-Box
[CPS16].
Non-blind
[HK14].
Non-Boolean
[AS17].
non-browser
[GIJ+12].
Non-contextual
[Svo14].
non-cryptographic
[AY14a, ESR14].
non-dynamic
[SES+16].
Non-interactive
[BCI+13, Pas13a].
Non-intrusive
[MFH13].
non-iterative
[SXL16].
Non-Linear
[EK+13].
Non-malleability
[KTT12].
Non-Malleable
[MSas12, CG14a, FMMV14, OOR+14, Pas13a, LP11, MSas13].
Non-monopolizable
[DJL+12].
Non-perfect
[FHKP17].
Non-Repudiation
[LLG15].
Non-stationary
[ZLDD12].
Non-tamper
[WgMW12].
Non-uniformly
[YKLL12].
Non-Verifiable
[AMH+16, YNQ15, CS11].
Non-Interactive
[KOS16, GOS12].
Nonlinear
[CCM+15, KW14, LW13a, Lidi12].
Norm
[FHS13].
normal
[TY16a].
Normalization
[KLY+12, SJ12].
Normalized
[YGFL15].
Norman
[Low12].
note
[Gai13, Hwa11, Lim11].
nothing
[Cer15].
Notions
[KFOS12, SNJ11, Sar12, BP11].
Novel
[CLHC12, KRDH13, LLG15, LyWIZW12, LH11b, MJS12, MCS+15, SWM+10, SC12, VN16, WHZ12, WXW12, YZX+12, Ye14, ZMM17, BOB13, CH10, DDF13, HCC11, LXC11, LMJC11, LH13, LWW+10, LML+13, MRT10, NZL+15, SYW17, Sun16, TG17, jT12b, WYL13, WGG+12, YWT+12, ZBR11].
Optimization [WH17, ZÁC17, FLZ+12, GCSÁdP11, KHF10, PTK14, RYF+13].


Order [KS12, LWKP12, YKKL12, ZDL12, ZSW+12, AKY13, LW13a, LCY+16, LWKP14, gWpNyY+14, YL11]. Order-Preserving [KS12, YKKL12, YL11].

Organisational [Smi15a]. Organization [RSGG15]. Orientated [TJZF12]. Oriented [NNAM10, Rog16, RSGG15, WW12, WZM12a, WZM12b]. Orthogonal [tWmC12]. Oscillator [YKBS10]. OSN [BCF16]. OSNs [SZZT18, PZPS15]. Other [Smi15b]. OTS [Hul13]. outliers [Sch12b].

Outlive [Hur16]. Output [DK16, GST12, NR12, PBCC14]. Outright [ABJ13]. Outsourced [FRS+16, LLC+15, LQD+16, PD14, RDZ+16, YMA17, YMC+17, DFJ+10, FS18, HMCK12, LCL+15, LCY+16, LJJ+17, QZDJ16, ZML17, ZSW+18]. Outsourcing [DR12, LJLC12, LHL+14, SKB+16, SWW+16], outwitted [Car11, Fag17].

over-the-air [ZWX+18]. Overcoming [BKKV10, DY13]. Overhead [AWSS17, CCW+10, GHS12, ZJ11, RS17].

Overlay [CHS15, MJS13]. Oversight [Bla16]. overview [AA14, BDP+12]. own [Zha15a]. owners [GZS+18]. Ownership [FMTR12, RR11, HWYW14, KH18].

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


Pairing [Bon12, CWWL12, CST+17, KZG10, KHP16, LGPRH14, YTS12, Con12, LL16a, LR15, YT11b, ZY17b].


Parallel [App14, ARM15, CGB+10, GP17, LY16, LB13, MCDB12, MCI11, NdMMW16, SMD11, YE12, CSTR16, MRT10, RG10, RWZ13, WWYY11]. Parameters [NDC+13]. Parameters [HRB13], parametric [Bull10a]. Paranoia [Cor14a]. Paper [Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, McK11, McK12, Pea11, Smi11a, Smi15b, Smi15a, Bai12]. part [VM14].


Passau [GLIC10]. PASSERINE [Saa12a]. Password [ASBdS16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZHX16, ABK13, CTL12, DCS12, FA14a, FIO15, FHV16, HCC10, LWS10].

Passport [LZJX10]. Password [ASBdS16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZHX16, ABK13, CTL12, DCS12, FA14a, FIO15, FHV16, HCC10, LWS10].

Passion [Hof15]. Passive [DHB16, GSC17, SB17, BM13, LWW11, MK12a]. passport [LZJX10]. Password [ASBdS16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZHX16, ABK13, CTL12, DCS12, FA14a, FIO15, FHV16, HCC10, LWS10].
LNKL13, MM12, MvO11, Tso13, TKHK14, WZM12a, WZM12b, YC12, ZXWA18.

**Password-Authenticated**
- HCL+14, YRT+16, ZXH16, LWS10, WZM12a, WZM12b. **Password-Based**
  - BRT12, CLY14, FVS17, WgMW12, DSCS12, FA14a, FIO15, TKHK14.

**Password-Only** [YLW13]. **Passwords**
- BHvOS15, LCL17b, BCV12, Che13. **Past** [Bon12]. **Patchwork** [NXH13, Kuz11]. **peer** [TC10]. **Peaks** [Kuz11]. **Decompression** [PP10b]. **PC-Based** [Ye12]. **PCle** [IBM13b]. **PCM** [LY15]. **PCM-based** [LY15]. **PCPs** [MX13]. **PCs** [GPT14, GPP+16]. **PDGC** [CGB13]. **Peaks** [TC10]. **pearl** [Rus15]. **Pecherskii** [Kuz11]. **peer** [NCCG13, ZYW+13]. **peer-to-peer** [NCCG13, ZYW+13]. **payload-based** [JNUH17]. **Payment** [DG15, SYC+17, SYW17]. **Payments** [RBHP15, MPJ+16]. **PC** [Ye12].

**Per-File** [CCSW11]. **Per-File** [CCSW11]. **Photo** [YE12]. **Perceived** [CSW12]. **perceptual** [MK11]. **PEREA** [ATK11]. **Perfect** [Pas13a, Sch13, CZ15a, FHKP17, LLC10, Lew10, XW12]. **perfectly** [ADG16]. **Performance**
- Ako12, AW17, AB15, CGL+12, CCG10, DLK+16, DBPS12, EGG+12, ESRI14, FFPB14, GLG12, GCS+13, HKL+14, LCK11, LPO+17, MHC12, SKV12, TPKT12, WDDW12, Xio12, ZLDD12, ABDP15, GCVR17, MMS+17a, MS13c. **Performed** [Ano17d]. **perimeter** [Kal13]. **periodic** [KPS10]. **periodical** [CLSW12].

**Permission** [VN16]. **Permutation** [LJ16, GMSW14, LK14]. **permutation-based** [LK14]. **Permutations** [BKLS12, Mat14].

**Persistent** [CSYY18, TYK+12, ALL+18, PKA15]. **person** [PN10]. **person-centric** [PN10]. **Personal** [ESS15, LM18, YTH17]. **Perspective** [KMY18, SM18, RSGG15, Sir16, Wag16, Suc12, ZWT13]. **Perspectives** [Sen17, SPM+13]. **Pervasive** [ACAT+15, BCG+12b, YD17, PKA15, SCY15, Tan12b, YWK+10a]. **Petri** [PS14].

**PGP** [RAZS15]. **Phase** [NBZP17, ZWT13, ZHH+17]. **Phase-change** [ZWT13]. **Phase-Encrypted** [NBZP17]. **Phone** [Mur16, SAA12b, KR+10, LTC+15a]. **photo** [OF12]. **Photographic** [YSC+15]. **photos** [Pow14]. **Phrases** [BWC+10].

**Physical** [GPT14, GPP+16, HHH+13, SMOP15, HQY+16, KSA16, QMC17, VCK+12, WW13, YD17, ZHH+17]. **physical-layer** [HQY+16, ZHH+17]. **physio** [HT11]. **physio-behavioral** [HT11]. **Pi** [MR10]. **Pi-Calculus** [MR10]. **PICADOR** [BGP+17]. **PICARO** [PRC12]. **Piccolo** [IS12, Jo13]. **picture** [SM13]. **piecewise** [GMOC15]. **PIN** [MDAB10]. **Pinch** [DGP10]. **PinMe** [MDMJ17]. **Pinocchio**
Preseeding [Ran16]. Presence [BDPS12].
Present [Bon12, LJ16, WH17].
PRESENT-like [LJ16]. Preservation
[BCP14a, LLG15, VSV15, Yon11, LVRY10, TMLS12]. preserve [BAG12]. preserved
[SWW+17]. Preserving [ABCL17, BJL16, BHKN13, BJL12, CWL+14, CRE+12, GZZ+13, HSMY12, HLLC11, HXC+11, HHMK14, KS12, LMGC17, LNXY15, LQD+16, NSMS14, OFMR16, PR12, PD14, PSS+13, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, SQZ+17, SZZT18, WPZM16, YKKL12, ZDL12, ZHW+16, ZM16, ZHW15, ZLDC15, ZTLM15, AKM+11, AIB+16, ALL+18, BLV17, FH13, FMA+18, GH16, GA11, HSH11, IC17, JKL+16, KH18, LW13a, LCY+16, SYY+17, Tan12b, TSH14, YMM13, YNX+16, YLY11, ZYW+13, ZOSZ17]. Press
[Ano15b, Ano17b]. Press/Elsevier
[Ano15b]. Prevent
[HLAZ15, PYN+13, JSK+16]. Preventing
[DCAT12, SKEG14, WS12]. Prevention
[CWL16]. Primality [Cou12]. PRIME
[ACK+10, GM13]. Primitive
[App15, MCS+15]. Primitives
[BSJ15, EAA12, HLN+10, SP15b, ABDP15, BSR+14, Gor10]. PRINCE [BCG+12b].
Princeton [Ano17b]. principle [WW14].
Principles [DK15, FSK10, Fri10a, Sta11a]. print
[KPS10, PKS18]. print-cam
[PKS18]. print-scan
[KPS10]. Printer
[EMW14, FN+15]. Prior [NA10a].
Priority [LMS16, Bia12]. Prisoners
[Mac14, Keb15]. Privacy
[AKM+11, ABCL17, ALL+18, ACM12, ABHIC+16, BN14, BCF16, BJL16, BLV17, BS13a, BJL12, CVM14, CWL+14, CDFS10, DTE17, ESS15, FGR+17, GZZ+13, HSMY12, HBCIC13, HXC+11, JN12, KM10b, KCC17, KS12, KH18, LMGC17, LSBN14, LLG15, LNXY15, LQD+16, MYYR13, NSMS14, PD14, PSS+13, PPRT12, PZPS15, PSD15, Pet12, RVH+16, RWLL14, RBHP15, SS17, Set16, SZDL14, SZZT18, SOF12, TMLS12, TMGP13, WPZM16, WMYR16, YMM13, Yon11, ZHW+16, ZM16, ZOSZ17, ZHW15, ZLDC15, ZTLM15, AKM+11, AIB+16, ALL+18, BLV17, FH13, FMA+18, GH16, GA11, HSH11, IC17, JKL+16, KH18, LW13a, LCY+16, SYY+17, Tan12b, TSH14, YMM13, YNX+16, YLY11, ZYW+13, ZOSZ17]. Privacy-assured
[WMYR16]. Privacy-Aware
[BCF16, MGP10]. Privacy-Based
[BS13b]. Privacy-Enhanced
[DTE17, ACK+10]. Privacy-Friendly
[KCC17, ACM12]. Privacy-Preservation
[LLG15]. privacy-preserved
[SWW+17]. Privacy-Preserving
[ABCL17, BJL16, BJL12, CWL+14, GZZ+13, HSMY12, LMGC17, LNXY15, LQD+16, NSMS14, PD14, PPRT12, Pet12, RVH+16, RBHP15, SZDL14, SZZT18, WPZM16, ZHW+16, ZM16, ZHW15, ZLDC15, ZTLM15, AKM+11, ALL+18, KH18, ZOSZ17, BLV17, FMA+18, HSH11, SYY+17, Tan12b, ZYW+13]. Private
[GM13, Jia14a, QZL+16b, Sia12, WCL+18, Yek10, ZMW16, ZXYL16, HJM+11, IK15, WR15]. private-keys
[IK15]. Privilege
[Cha13c]. Privileged
[Dim10, WDSL13]. PRNG
[DK16]. Proactive
[SL10, WMYR16]. Probabilistic
[BFG+14, Rao10, WP17, KSU13]. Probabilistically
[WW14]. Probability
[DF11, HLC16]. Probability-based
[HLC16]. probable
[Sav13b]. Probably
[MMS17b]. probe
[Edw14]. Problem
[GKS17, LLGJ16, NA10b, TKM12, Mes15, MR14c, RH10, VM14]. Problems
[Dun12a, Fra15, GTR11, KRDH13, KPC+11, RBS+17, SK14, TPL16, WS14]. Procedure
[CS14, OS12]. Proceedings
[LCK11, Wat10, ACM10, ACM11, Abe10, BC11, CGB+10, Che11, Cra12, Dun12b, FB12, Gil10, GG10, HWG10, IEE10.
IEE11b, IEE13, LW11a, LTW11, Pie10, PJ12, Rab10, Sen10, Yan10, Yan11, AB10a, BL10, GLIC10, IEE11a, Kaa11, Lin14b, Sah13.

**Processing** [SAKM16, TKMZ13, VKPI17, BKV13, HWK+15, MS13b, PRZB12, WS14].

**Processor** [BH15, CLF+17, HKL+14, LB13, MBR15, YS15, ABD15, BAB+13, BGG+13, SSPL+13, Tar10]. **Processors** [GFBF12, Gue16, RYF+13].

**Product** [ADM12, CCM+15, OT12, YKNS12, Cha13b, DDM17]. **Products** [RS10].

**Professional** [STC11]. **Profiles** [BCF16]. **Profiling** [DP12]. **Program** [MZ17b, CLZ+17, GGH+16b, MFH13]. **Programmable** [CLF+17]. **Programming** [CLF+17].

**Progress** [AB10a, BL10, BC11, GG10]. **Progressive** [SA16a]. **Project** [ACK+10, SS10c]. **Projective** [CZ15a]. **Prominent** [ABJ13]. **Promise** [Pau10, PWVT12]. **promised** [HS11].

**Proof** [BDSG+13, Bla12, CZLC12a, CZLC14, FSX12c, Kuz11, LW12, NLY15, SR14, Ste15a, ZZZ+17, Mon13, PPTT15, WHJ17].

**Proofs** [BGK12, BCGK12, BGB12, BCI+13, BDSG+13, CZLC12b, IW14, LNZ+13, Maui2, NTY12, Sav13b, WPZM16, AGHP14, KPP16, KKK+16, Li10].

**Propagate** [GWM16]. **Propagation** [WWC+11, YZLC12]. **Properties** [CC12, CC16, DQFL12, FY11, JR13, KU12, Sch12c, CLCZ10, WT13]. **Property** [HEC+12, PR12, Rja12]. **Proportions** [Ber12]. **Propose** [BFMT16]. **proposed** [Bax14]. **Protect** [CTC+15, YMC+17, BV12, CDF+10, dCCSM+12]. **Protected** [BDG15, SG15].

**Propagating** [BGP14a, GSFT16, Mar10b, SCY15, Wat14b, ATKH+17, CDA14]. **Protection** [CDD13, GST12, Lop12, NGAuHQ16, NDG+17, RR11, SEY14, SJ12, ATI+10, HLSY14, KKM+13, LVRY10, RS17, TLL13, YW+12]. **protection-key** [HLYS14].

**Protocol** [BL12, BC14, BCM+15, BSSV12, BFK16, CC14, CCM17, FLH13, FMTR12, Fra16, GI12, HvS12, HC12, HL10a, HCPLSB12, HCETPL+12, HKL+12, JTZ+16, KMO14, LNZ+13, LCCJ13, LNX15, MBC15, MR10, PSS+13, SBS+12, SGC16, TYK+12, WT10b, XJR+17, YS12, YW+12, ZXM+11, AATT18, AGK13, AIB+16, AN15, BGAD12, CSD18, CCS11, CJP15, DLK+16, EA12, FA14b, FIO15, GMS14, GLM+11, HPC12, HL14, IC17, JKL+16, Kim11, KO16, LLLS13, LDDAM12, LKCL13, LSW10, LXMW12, LY14, LML+13, NCL13, NYLZ12, OHJ10, Par12b, SPLHC14, SB17, SWW+16, SSS11, SSPL+13, TG17, Tso13, TKH14, WCFW18, WZM12a, WZM12b, WMY16, WT10a, WTT12, WCCH18, XCL13, YC12, ZYX+14, YMM13, ZWQ+11, ZT16, ZYC+17, XZ+18, XZWA18, ZG10, ZZZ15, ZL11, BOB13, CJP12, LFGCGCR14, Ste15b].

**Protocols** [AP13, ABHC+16, BPM12, CCK12, CC16, CCF17, CDD15, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLC11, HL10b, KOS16, LY16, MS16, M12, Mur16, N14, NSMS14, PS14, SBS+12, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13b, ACM12, CML+18, CR10, CLCZ10, DGJN14, FT10+10, GB11, GLR13, HSH11, Ham12, HPC13, HZW17, HST14, KJN+16, KU13, KKK+16, LKCL13, MN10, NR11, Nos11, Nos14, SD10, YSL+10].

**Prototyping** [KPC+16]. **Provable** [BKLS12, CC14, EKB+16, Rog16, YMSH10, ZX11, ZPXX17, FA14a, IRS13, LHH11, WB12, XCL13]. **Provably** [BCGAM12, BCM12, BCM13, BHJP14, FH10a, GLL+18, IL15, LH11a, LL16b, PS17, WMS+12, XJWW13, YC12, ZYX+14, ZG10, ABB13, FIO15, SXL16, WX14]. **prove** [DGJN14]. **provenance** [CDL18, ZOS17].

**Provide** [Ano15a]. **Provided** [K12].

**Providence** [Sch15a]. **provider** [DFJ+17].
providers [AKK+17, BK12b, YWK10b].
Providing [DLN13, HTZR12, MLM16].
Proving [Sar14, AGH+17]. Proximity [IW14].
Proxy [ASS15, GSW+16, GJJ15, GJZ17, HGWW11, 
HZX15, KP12, LSLW15, LAL+15, LSC12, 
ML017, MBC15, NAL17, Pet12, PRSV17, 
SYL13, WY10, WYML16, XJW+16, 
YMWS11, YCM+13, BGP+17, CLH+16, 
FSGW11, FSGW12, GH12, HWDL16, 
KKM+14, LCT+14, LFWS15, LL16a, LL16b, 
QM17, SLZ12, SKB+17, Tia15, WHY+12, 
XWXC14, YZCT17, ZLY10, ZDW+16].
Proxy-invisible [SYL13]. Ps [HDHW12].
Pseudo [NN12, XYXYX11, CFY+10, KMI0a, MG15, 
PLSvdLE10, SH11, SN11, SXXW10, Zim10].
Pseudo-Random [XYXYX11, CFY+10, KMI0a, MG15, 
PLSvdLE10, SH11, SN11, SXXW10, Zim10].
Pseudonymous [BDK12]. Pseudoprime [DW12].
Pseudorandom [AS17, BCGH11, BK12a, Kla10, MFG16, 
CP13, GCH15, HRV10].
Pseudorandomness [Sha10]. PSMPA [ZLDC15].
PSO [TLL13]. PSSPACE [JJUW10]. Public
[Ano11b, ABW10, BVS+13, BB14, BKLS12, 
BKKV10, CLP13a, Chet15, Cour12, 
FBM12, GKS17, HTCS+15, IM14, JLT+12, 
KFOS12, LLSW16, LPdS10, LZC14, 
MZHY15, MMP14, MTY11, Mat14, MPRS12, 
Muf16, NTY12, Om16, PDNH15, RSBGN12, 
RW12, RBHP15, Saa12a, SK12b, SMW+10, 
Sia12, SC12, SLY+16, SvT10, TMC15, TT12, 
WP17, WZ15, WWHL12, XNKG15, XXZ12, 
Xio12, XJWW13, YL17, YKC+11, YFK+12, 
YM+17, ZY17a, AA14, ATKH+17, BS15, 
BWS12, Dur15, HZWW17, HL14, LSN14, 
LLY15, LFWS15, LH13, LL16a, RPSL10, 
SES+16, SY15b, VN17, YT11b, YYS+16, 
ZZ11, ZCC15, ZY17b, FBM12].
Public-Coin [CLP13a, Mat14].
Public-Key [BVS+13, BKKV10, GKS17, 
KFOS12, MMP14, MPRS12, NTY12, 
Omm16, PNDH15, RSBGN12, RW12, SK12b, 
SWM+10, Sia12, XNKG15, XJWW13, 
YKC+11, YFK+12, ZY17a, ABW10, IM14, 
LPdS10, LZC14, BWS12, RPSL10, SES+16, 
VN17, ZCC15, ZY17b].
Publication [ZTL15]. Publicly
[NMP+13, SZQ+17, YNR12a]. Publish
[BGP+17, DLZ+16b, OFMR16, PRSV17, 
SLI11, TKR14, YSM14].
Publish/Subscribe [DLZ+16b, OFMR16, PRSV17, 
TKR14, YSM14]. published [MYY13].
Publisher [Ful10, Mur10]. Publishing
[VSV15]. Puebla [AB10a]. PUF
[CCKM16, CCM17, DSB16, KPKS12, 
KLM+12, MV12, SRK+17, VDB+16].
PUF-Based [CCM17, KPKS12, MV12].
Pufferfish [KM14]. PUFKY [MV12].
PUFs [IGR+16]. pulse [MRRT17].
pulse-response [MRRT17]. punctured
[MG15]. puppet [Lac15]. Purpose
[GFBF12, Gue16, ABPD15, DGNJ14, KM11].
purposes [ABB+14]. push [Wu17].
Pushdown [CCD15]. Pushing
[FHV16]. Puzzle [IBM13a]. Puzzles
[RSBGN12, dCCSM+12, dCCSB+16]. Py
[DG12]. Py-Family [DG12]. pyramid
[MHT+13].

Q&A [Hof15, Hof16]. Q3 [Ven14]. Qeda
[Mac14, Keb15]. QC [JY14, HC17, VOG15].
QC-MDPC [HC17]. QIM [JK17]. QIP
[JJSW10]. QS [AZPC14, HDHW12].
Quadratic [KRD13, SEY14, YDH+15].
Quadraticity [MS12b]. Quality
[CSCW12, NN12, YCM+13, SS11, WZLW13, WKH11].
Quantitative
[BL15, MLBL12, MV16b, HM10].
Quantization [SSA13].
Quantization-Based [SSA13]. Quantum
[Ano15d, Ano16c, Ano17d, Ano17e, BB14, 
Ber14, BCF+14, Che17, CCL+13, Feb10, 
FKS+13, Fol16, JEA+15, Kar12, KP10, 
LHA+16, MS16, MSU31, MKAA17, NNA10,
NA10b, RK11, RSM15, Sti11, TKM12, Unr15, WCL+18, Y+17, ZWS+18, ABB+14, BJ16, CML+16, Edw17, FRT13, GJMP15, IM14, JSK+16, KKK+16, LyWSZ10, LCW+16, Lii12, QD16, SK14, Svo14, YDH+15, vDKS11, Sen10, Yan11. 
R [BS12, LVV11, PP10b, WYW14]. 
RAKAPOSHI [IOM12]. RAM [RYF+13]. 
Resettable [CPS16]. Resettable [COP14].
Resettable-Sound [COP14]. Resilience
[NTY12, GLL+18]. Resiliency [YM16].
Resilient
[AV12, BKKV10, FPS12, LTZY16, NYR+14,
Pan14, PSD15, XZY+12, YZ12, YNR12b,
YCZY12, ZYT12, ZWTM15, ZMZ17, ZY17a,
DLZ16a, GV14a, KPS10, MMSD13, YSJL14,
YKC+12, YLZ+16, ZY17b]. Resistance
[CGS12, PRC12, WLZL12, ZJ11, DLM13,
FIO15]. Resistant [BK12a, CDK+10,
GV14b, HF14b, WHZ12, WgMW12, WH17,
YPRI17, GMRT+15, HCC10, PBCC14,
VCK+12, WTT12, YKTK13]. resisting
[SXL16, Tam15]. Resistive
[DSB16, TCLF16]. Resource
[JMG+16, SZMK13, YNR12a, AMH10,
KAS15, LLZ+16, MVH15, Wn13,
XWZW16, ZPZ+16]. Resource-Constrained
[YNR12a, LLZ+16]. Resource-efficient
[SZMK13, XWZW16]. Response
[GHS14, HJKL15, ZHW+16, MRRT17].
Resprinting [TBCB15]. restoration
[WHZ12]. restricted [CLH+16]. result
[ACK+10, ED17]. Results
[DGS12, LFJ16, Hof16, KG10].
Rethinking [Che13, HU15, LSG16, MV16a].
Retrieval [BBB+16a, BTHJ12, CJP12,
HK14, JMG+16, JKHe12, Ye10, ZXX+11,
CJP15, SWW+17]. returned [War11].
reusable [RS17]. Reuse [ABF12]. Reveal
[Sta13]. Revealed [Ano15d]. Revealing
[BT12, KK12, KK13]. reverse [TQL+14].
Reversibility [FSX12b, HWY14].
Reversible [CLF11, CSS+13, HHS+15,
MM17, MR16, NC12, AMK12, CT11a,
HLC16, JK13, MM14a, NC13, PWL13,
PC14, TK14, WOLS12]. Reversibly
[MKH+12]. Review
[Ano15b, Ano17b, YL12, Ayu12, Bai12,
Bar12, Cou12, Dew11, Fu10, Gas13, Joh10,
Kat13, Keb15, Koh10, Led16, Lop15b,
Low12, Mei10, Mou15, Mur10, Sch15a, Sha10,
Ter11, Xie12, JAS+11, MM12, TPKT12].
Reviewed [Sch15a]. Reviews [SR14].
Revised [DDS12, Dan12, MV12, BYL10,
JY14, LH10a, vDKS11]. Revising [BT12],
revision [LT14h]. Revisited [CLY14,
DKPW12, DKS12, GWVC15, KFOS12,
LL11, Lop15a, PTK12, Sar12, Tan12a,
BCL14, HKT11, HYWS11, TS16a, ZCL+12].
Revisiting [TLW12, WSA15].
Revocability [WHLH16]. Revocable
[AEHS15, CD16, SE14, SE16, SZS14,
SZDL14, TCE15, TT12, Unr15, FLL+14,
WLFX17, WTT12]. Revocation
[AEHS15, LLC+15, LW16, Lop15b, RZ+16,
XMLC13, YWZ+12, ATK11]. Revoking
[TAKS10]. Revolutionized [Orn16]. RFID
[CJP15, AATM18, BL12, BSSV12, BM11,
CGCGPDMG12, CCF17, CJP12, Cho14,
DZS+12, FLL+14, For14, FMT12,
GMSW14, GI12, GSN+16, HSH11, HDPC13,
HQC+16, HCPLSB12, HCETPL+12,
LNZ+13, MO12, Mic16, MK12a, PPH12,
PLSvdLE10, QQL+16a, QQL+16b, SBS+12,
SPL1CB14, TG17, WH17, WCF18].
RFID-Enabled [QQL+16a, QQL+16b].
RFID/NFC [Mic16]. RFID. [KOP12].
RGB [SNM14, ST16]. RI [Sch15a]. Rich
[CS12]. Richman [Xie12]. Riddle
[Fox13, KM15, KM16]. Right
[Bro17, SR12a, BBG+17, LHA+12, Sch11].
Rightful [RR11]. Rights [LYRY10].
Rigorous [DK17]. Ring
[GHPS12, HKL+12, YKS10, YLA+13,
ZJ14, DZ14, Hwa11]. Ring-LPN [HKL+12].
Rings [YM16]. rise [Ano14]. Risk
[Zha15b, PAK15]. risks [Lan10, SS17].
RKA [SLY+16]. RKA-Secure [SLY+16].
RLCPs [DDS12]. RLWE [XZ+14]. RNG
[CGH17]. RNGs [DSDDW14]. RNTS
[PSOMPL13]. roaming [SCKH10, ZX11].
Robotic [SPW+16]. Robust
[BGAPM12, BCG12a, CFFR12, GKB17,
HZC+12, JSZ12, LSL12b, LSR13, MR16,
MU12, MS16, MC11, pNyWyY+14, OCG11, RR11, SJ12, SC12, SZTZ18, TLCF16, TK14, TTL10, WLLDB11, WgMdZIZ12, gWpNyY+14, XNG+14, YWNW15, YYO15, AP10, CLM+12, EAA+16, GZHD12, HZC+14, LW10, PKS18, RS17, yWpNyL11, yWpWyYp13, YSL+10, ZHH+17.


Round-Reduced [DWZW12]. Rounds [GST12, Sas12, LYHH14, MNP12]. Router [Bis17, SA15]. Routlette [Ham12, KZG10, WLY+15, LSG16, LC17]. RSA [Du12b, Kin11, Pie10, APPVP15, BBBBB13, Bro17, BNS17, CLSW12, Chm10, GM13, GST13, Her14, Hin10, HLYS14, IK15, KHHH14, KFL+10, Lim11, Moo12, SM10a, SM10b, SM110, SM110, Win17, YXA+16].


scheme \cite{GZHD12, GJ13, GMRT+15, GLM+16, GH16, HBBRMN+16, HL11, HCCC11, HLC16, HCC10, Hwa11, IB11, JNUH17, JLT+12, JZS+10, JMWM+16, KI11, KPC16, KDHI15, KK13, KHM13, KK+14, KKG14, Kim16, KLW+16, KWD+17, KWH16, KL11, LXLY12, LLLZ+16, LSR13, LH10c, LZX10, LNM+11, LMJ11, LK12, LLHS12, LNKL13, LK+17, LNK+18, LFWS15, LH13, LHH11, LWW10a, LWLW11, LW13b, LZX14, LL16a, LL16b, LWY12, MCM+18, MMS17c, MK12a, MSas13, NR17, Nos14, QMC17, QMW17, RSPL10, SGGCR+16, SM11, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWYZ11, WYYY11, yWpNyL11, WHL13, WDZL13, WLFX17, WZ11, WKKH1, WOLS12, WXK+17, XHH12, XWW16, XXXC14, XXX15, XMHD13, YC11, YCC16, YWK+10a, YCT15, YMSH10, ZYL+10, ZLY10, ZX1+14, ZYC+17, ZPWY12, ZHH+17, ZY17b, ZC12, ZBR11, DT13, LLLZ+12]. Schemes \cite{ABF12, BVS+13, BMF12, BBEPT14, BSJ15, CMLRHS13, CGL+12, Chu16, Des10b, FHKP17, FFL12, HSM14, HPO+15, LWW10b, LZCK14, MLCH10, MR14b, MMS17b, MKRM10, Oba11, PB12, PDNH15, PH12b, Sch10, Shi11, SKH17, SSU12, VSCR12, WGF16, YNR12a, YNR12b, Yek10, YWYZ+12, AGHP14, AN15, AHI+12, CDGC12, CHS11, CCG10, CLT13, DDD14, DD13, DZ14, FPBG14, FGMP12, FMA+18, HWDL16, HM10, KTU16, LHYZ12, MM12, MA17, NZL+15, QYWX16, SES+16, Sar10a, Sar11, hSSZ15, WW14, YT11b, ZCL+12, ZCLL14, ZT14]. Schneier \cite{Sev16}. Science [Bow11, Gas13, IEE10, IEE11b, Ter11, Bia12, PHW10m, Pet11]. scientists \cite{Goo12}. Scientometric \cite{Pal15, Pal16}. Scope \cite{Bai12}. Score \cite{GCSAddP11}. scoring \cite{OSSK16}. Scrambling \cite{LLL17}. Screen \cite{SPW+16, CTL12}. Script \cite{Rao10, Bax14}. Scripting \cite{DSB15}. scroll \cite{GMOGCC15}. SDB \cite{HWK+15}. SDOO \cite{PL16}. SDOO-based \cite{PL16}. SDH \cite{GMS11}. SDIVIP \cite{YNX+16}. SDN \cite{KCC17}. SDVS \cite{Wan10}. SE \cite{LLLS13}. SE-AKA \cite{LLLS13}. seals \cite{MN10}. Seattle \cite{LCK11, KCR11}. Seberry \cite{AHS14}. SEC \cite{PA10}. Second \cite{AKY13, ABM+12}. Secondary \cite{RS11}. Secrecy \cite{ABD+15, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCW15, TCS14}. Secrecy-preserving \cite{TSH14}. Secret \cite{ASN11, ASN12, ADH17, Ayu12, BABB+16a, BMF12, BBEPT14, Bri11, CCM+15, CFOR12, CCL+13, DR12, Dew11, EM12, EA11, FHKP17, FR16, Fk12, HL10a, JLS12, KU14, KOTY17, KK12, KK13, KSSY12, KS15, LHF12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, Men13, MNS1, NS12, Oba11, PCPK14, SLL10, SC10, SS10c, SSU12, Sti15, TLW12, TWZ11, WBK16, WGF16, XZY+12, XJR+17, YFF12, YWYZ+12, ZC13, ADG16, AKK+17, BJ16, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEA13, EZ15, FH110a, GMMP15, GLW13, HF14a, HHI15, Ht15, HBBRMN+16, HCCC11, HLC12, KI11, KU16, L行为12, LT13, LyWSZ10, LHYZ12, Mas17, McK10, McK11, McK12, MB11, O010, Pea11, Pet11, QD16, Rus15, SB17, SA12, TQ+14, TD14, UUN11, UUN13, WL13, WZ11, WS12, WOLS12, Wu17, XW13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPWY12]. SECRET \cite{LLL17, Bia12}. secret-key
[BJ16]. Secret-Sharing [BBEPT14].
Secretocracy [Ber16b].

Secrets
[BT12, CG14b, DLWW11, FMS12a, Kob10, Man13, Bha16, Cop10b, GGH+16b, Gup15, HRS13, Smi11a, Ano17b]. Secure
[ADMM16, AARJ12, Ash14, AMH+16, BVS+13, BWLA16, BCGH11, BCG12a, BCO+13, BWA13, BJL12, BHJP14, BF11, Bru12, BDH11, BCEM15, CFOR12, CCM17, CZF12, CZLC14, Che15, CMA14, DL15, DMS+16, DG15, DLZ+16b, Edw17, FLH13, Fri10b, FD11, FSX12a, zGXW12, GKM16, GGH14, GFBF12, GT12, GV14b, GHKL11, GM14, GZS+18, HvS12, HSM14, Har16, HL10b, HP14, HTZR12, HMCK12, HLKL15, HK14, IL15, Jac16, KW14, KME+12, Kip15, KHI0, LJS+14, LL15, LYZ+13, LTH+15, LTZY16, LSLW15, LLGJ16, LY15, LHL15, LLM12, LSC12, MLO17, MNP14, Mal13, MVVR12, MMS17b, MK12a, MKAAA17, NBZP17, NDC+17, NR12, NMS14, NSMS14, PR12, PSM17, Per13, QZL+16b, QZDJ16, RMP10, Rea16, RSGG15, SNJ11, SZS14, SVCV15, SP15b, SKH17, SRAA17, SSA11, SVG16, SYW17, SYC+17, SMS14, SZDL14, SGH15, SLY+16, SR12b, TLC15, TWZ11].

Secure
[TG12, TGC16, VMV15, WgMW12, WKB16, WXLY16, WLY17, WLH15, WBA17, WWHL12, WMS+12, tWmC12, XWSW16, XJWW13, YNR12a, YNR12b, YTH17, YKC+11, YAM+15, YGD+17, ZXZ+11, ZDL12, ZVG16, ZHT16, ZLW+17, ZBR11, AHS14, ABBD13, ACF16, AKA+17, ACD+15, BOB13, BSR+14, CC11L, CSS18, CLH13, CW14a, CS11, CDL18, FHH10a, FLC+14, FSGW12, FA14b, FIO15, FS18, Gal13, GLL+18, GCH15, HGYY11, HWK+15, HLYS14, HPY10, IB11, JLS+10, KPP16, KKA14, KRM+10, KTOU16, KDW+17, LLLS13, LDDAM12, LH11a, LLW16, LSR13, LCT+14, LAL+15, LL16a, LL16b, LBOX12, MR14c, NR17, NACLR12, NAL17, PSdO+13, PLSSvLE10, Rao17, RG10, RYF+13, RITF+11, RS15, SGGCR+16, SYL13, SWW+16, SSS11, SSPL+13, SXL16, Tar10, TLM13, TLL12, WMX+17, WCHC18, WXXC14, XXX15, YC12, yYqWqZC13, YZZ+14, YZCT17, YY11, YLS12, YMSH10, ZLY10, ZC1L14, ZZ15, ZYC+17, ZG10, ZZ12, ZX11].

secure
[ZY17b, ZC12, Zhu13, ZSW+18, Ano12, OKG+12, YSS14, YFK+12]. Secure-TWS
[OKG12]. Secured [LC17].
Securely
[CC10, KP17, LHL+14, MS16, WXY+17, BC18, der10].

Securing
[BK12b, CMLS15, CST+17, NPH+14, PMZ13, SFE10, SLJ11, Ste15b, TKR14, YMA17, YT12, CR10, Din10, SA15, Tox14].

Security
[ABJ13, ASBD16, Ano13d, Ano15a, Ano15d, ABF12, AN15, ABHC+16, AYS15, BCE+10, BCM+15, BRT12, BPR14a, BPR14b, BLS12, BCGN16, BDPS12, Bra15, BDH11, BP10, CFST17, CFE16, CHS11, CFXY17, CCD15, CPS16, CM11, DDS12, Dan12, DR12, DFKC17, FMA+18, FSX12b, FSX12c, GZZ+13, GSC17, HC12, Hel17, HB17, HLW12, HXC+11, HLCL11, HLT+15, HLN+10, IS12, IGR+16, JN12, Jia14a, KBL11, KFOS12, KSD+17, KD12b, LPS12, LST12, LW11a, LK14, LW12, LZ+17, LTW11, LP12, LRW17, LZC12a, LDB+15, LMS16, MTY11, MKN13, MCS+15, MH14, Mau12, MV16a, MLBL12, MPM+17, Nac12, NNM10, NDG+17, NVM+17, Nos11, Nos14, Orm16, OS16, Pas13a, PZPS15, PDNH15, PS14, PL16, PDT12, PNR17, RQD+15, RWZ12, Rog16, RS10, SN10, SNJ11, SBS+12, Sbr12, Sch13, SD12, Shi11, SLM10].

Security
[ST11, STC11, SMOP15, SCGW+14, Tso13, TV15, WYCF14, WSA15, WSS12, WCL+18, WS14, Yan10, YZGC12, YGS+17, YSS14, Von11, Zha15b, ZY17a, vTJ11, AB10a, Abo10, ABGR13, ABM+12, Ano11a, AD17, BYL10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTHP13, CLC10, CVG+13, DLK+16, DHW+13, Edw14, FHM+12, FA14a, Fis15, GM16, GLM+16,
GMS11, GH12, HWDL16, HWG10, HLR11, HRS13, HLV10, KSA16, KKK+16, Lan10, Lan13, LH10a, LXMW12, LHH11, LZC14, LSG16, MZA+13, Men13, MII4b, NS10, NCL13, NLY12, OK18, OYHS12, PHWM10, QYWX16, Rec15, RPSL10, RH10, SA12, Ser12, SLZ12, SY15b, Sir16, Sta11a, Tan17b, UUN11, VCK+12, WCFW18, XCL13, Zha15a, WX12, YKC+12, Bar12].

Security-Aware [LMS16].

security-modified [MM14b]. SEDURA [LY15]. Seed [AS17, LYHH14, Sun11].


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

Selection [KD12a, RP12, SEY14, FXP12].

Selective [BTHJ12, GDCC16, LW12, LSC+15, LZC12a, LZC14, LW13c]. Self [CHHW12, CSV15, HZ11, LCL+17a, LHM14, SA15, WHZ12, XWXC14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11].


Seminary [SS10c]. semirings [Dur15].

Sender [WZ15]. Sensational [YGFL15].

sense [Kem11]. Sensing [Kar12, RPG12, XWZW16, Fay16].

Sensitive [Kaw15, RQD+15, Tan15a].

Sensitivity [YGD+17, LWW+10]. Sensor [ABC+17, BN14, CS14, DS11, KH10, LLC11, LLZ+12, NNM10, NYR+14, OKG+12, PX13, PCPK14, RWWL14, SP15b, YM16, AS14, AIB+16, ADF12, BLAN+16, BBB16b, CDGC12, CLSW12, DSCS12, DLN13, HTC+10, JNUH17, JMW+16, KLC+10, KO16, KLW+16, KDW+17, LC17, LNK+18, PL16, SMK13, SKK10, Wan13, WW14, WXK+17, XWDN12, XMHD13, ZYL+10]. Sensors [DL12, LIK+17].

Sensory [SGC14]. Seoul [HL10a, LW11a]. separation [MJS13]. Sequence [PFS12, WGD+12]. Sequences [ADD10, Kla10, NN12, XYYY11, HLC12, VM14].

Sequential [GLR10, GLR13, LLY15, WYL13]. Series [BJL16, Die12]. Serpent [PC16]. Server [BCO13, Che15, GMSV14, LYL15, YLW13, ATKH+17, CSD18, CLHJ13, FA14b, HDPC13, HL14, ISC+16, LXMW12, LH13, SY15b, hSZZ15, SSAF11, SSS11, TLL12, WT10a].

Server-Aided [GMSV14, LY15, SSAF11].


Service-Based [LDB+15].

Service-Oriented [RSGG15]. Services [Aono11b, DLZ+16b, MEFO12, OO12, ZHL15, AZPC14, CSD18, CHX13, IMB17, IG11, NZL+15, PP11, XXX15]. Session [BS12, BKP12, CFST17, SHS12, AN15, DCAT12]. Session-Based [BKP12]. Set [Cor14b, EKP+13, YZ12, Con12, TMK11]. set-valued [TMK11]. sets [SF12]. Setting [BKLS12, HPH17, MZHY15, TYM+17, XXZ12, ZHL15]. Settings [GZ12]. setup [Jia16]. Several [Sas12, ZT14]. SGX [WBA17]. SHA [AAE+14, ABM+12, App15, jCPB+12, LC17, MAK+12, SKP15]. SHA-1 [AAE+14, SKP15]. SHA-256
SHA-3
[App15, MAK+12]. SHA-1
[ABM*12, jCPB+12, LC17]. SHA
[SBK+17]. SHA256
[GWM16]. Shadow
[Kap11]. Shadows
[YSC+15]. SHAkes
[CNR14]. Shamir
[BDG+13, UUN11, WKB16]. Shannon
[AMS+10]. Shape
[RTF*11, SY14, Pet11]. Shapes
[CJFH14, LMHH14, SY14, SGS14, ZZZC14]. Share
[DRD11, LNXY15, OKG+12, TYK+12, XJR+17, PZPS15, SA12, TG12, YYS+16, YNX+16]. shared-secret
[SA12]. Shares
[CFOR12, KU14, SA16a, WY12]. Sharing
[BFM12, BBEPT14, CCM+15, CFOR12, CCL+13, CCT+14, CLW16, DR12, EM12, FHKP17, FR16, HL10a, HRS13, HLT+15, KU14, KOTY+17, KSSY12, KS15, LYX+13, LPL15, Lin15, LCCJ13, LTC+15b, NS12, Oba11, PSM17, SC10, SSU12, TG12, YP12, YYZ+12, ZC13, AKK+17, ADH17, CT11b, CW14a, EZ15, EA11, FGMP12, GJMP15, GLW13, HP14a, HBBRNM+16, HCCC11, HLC12, KI11, KU116, KBP17, LXLY12, LT13, LFWS15, LAL+15, LyWSZ10, LHY12, LHL15, LLL+18, LL16a, Mal17, Oo10, QD16, Rao17, TD12, UUN11, UUN13, WKB16, WD12, WOLS12, YC11, YCC16, ZC12, ZZ15, ZPWY12, ZLL10]. Shell
[YSS14, Tay14]. Shenzhen
[IEE11a]. Shield
[NDG+17, KGV16]. Shift
[AKP12, ZH15, LKW11]. Shift-Type
[AKP12]. Shifting
[YWW10, CSS+13]. Shih
[Joh10]. Shopping
[AHS13]. Shor
[MNM+16]. Short
[BHG12, CWWL12, NR12, SKV12, WQZ+16, XGLM14, LL15, RD17, ZPWY12]. Short-Output
[NR12]. Shorter
[Hül13, PPB16, TH16]. Should
[Eve16]. shown
[Ana14]. shows
[Goo12]. Shparlinski
[Sha10]. Shredder
[AMH+16]. Shredding
[AMH+16]. SHS
[Ano12]. Shuffle
[HMR12]. shuffler
[BVIB12]. Shuffles
[CLKM13]. shunned
[Ree15]. Sicily
[Cra12]. Side
[AN17, BCO13, CFE16, CDK+10, CBL13, DMWS12, DKMR15, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, SR12a, Via10, YL17, BVIB12, DJL+12, MFH13]. Side-Channel
[CBL13, EWS14, GWM16, GPT14, KOP12, NDC+13, PRC12, SG15, YL17, DMWS12, BVIB12, MFH13]. Sided
[HP14]. Sieve
[VM14]. SIFT
[KLY+12]. Sign
[LL15, MEO12, SPM+13]. Sign-On
[LL15, MEO12, SPM+13]. Signal
[Kar12, MS13b, RTF+11]. Signals
[LJK17, XNRG15]. Signature
[Ano13a, ABF12, ASS15, AEHS15, BHG12, BDH11, FGM10, GJJ15, GJZ17, GMSV14, HZX15, HP0+15, HHP17, Hül13, JL16, LIT+15, LGPRH14, MMN12, NBX13, PH12b, ST16, TTH15, WXL12, WLY15, WYML16, WHL16, XGLM14, Y+17, YMWS11, YLA+13, ZJ14, ZHL+12, AGHP14, CLSW12, CCG10, DZ14, DLN13, HYWS11, Hwa11, JZS+10, LWZG10, LL16b, Nos14, QYW16, QMW17, RSM15, SL10, XLL16, YWL+17, YLS12, YKC+12, ZLY10]. signature-based
[DLN13, QMW17]. Signatures
[Ano15a, ABC+17, AYS15, BBC+13, BDFK12, BH2+15, Fuc11, GY13, GdM16, HL13, HRS16, HBG+17, MFM+16, MCF17, MKAA17, Orm16, PST13, TH16, ASVE13, BDL+11, BP10, GMS11, Her14, LL15, PPB16, Tia15, ZQWZ10, Mou15]. Signcryption
[CMA14, DZY10, FZT13, FZT14, LI15, LSL12a, Rao17, XQL11, ZYD10, EZ15, HPO10, HS11, KL11, TK12, LK12, LI15, YMWS11, LH15]. Signed
[KWH16]. signer
[Hwa11]. Signing
[YAM+15]. Silent
[AMH+16]. Silverman
[Mei10]. Simon
[AMKA17]. Simple
[Ano13c, CZF12, Ros11, Sar10b, Sma16, TTD13, ZH15, Zin10, CLM+12, MMS17c]. Simpler
[TH16]. Simplified
[PS12]. Simulation
[CPS16, MS13a]. simulations
Simultaneous [YWZ+12].
Singapore [Abe10]. Single
[ABK13, LL15, MEFO12, Sas12, SPM+13]. Single-SP [Sas12]. Singular
[ABK13, LL15, MEFO12, Sas12, SPM+13]. Single-SP [Sas12]. Singular
[LSD12b, BWA13]. Sins [HLV10]. SIP
[KKGK10, ZZT16]. SIP-based [ZZT16]. SIPF [SYC+17]. Site [DSB15, SS10c].
siteDriverID [SSG+16]. Size
[AS17, AEHS15, CJ13, CSW12, EAA12, Kim15, LCLL15, MTY11, ZMW16, AHL+12, LCT+14, PPTT15, SGM16]. Size-Constrained [EAA12]. Skin
[FLS+10, KNR10]. Skin [AQD12]. skyline [BKVI13]. Slantlet [TK14]. Slicing
[MZ17b]. Sliding [BBG+17, Bro17, Win17]. SLMAP
[HCETP+12]. Slow [SMI11b]. Small
[BMJ14, BKLS12, BB10, CJ13, Kim15, LCLL15, YM16, AAT16, GJB13, Jous13]. Smart
[AN17, ABCI17, BSJ15, DLZ+16b, HCL+14, LA10, MFG16, PDDT12, WgMLZ12, WgMW12, CHS11, CLHJ13, HCC10, LH10c, LNM+11, LXMW12, LNKI13, LTC+15a, MM12, MCN+18, WMYR16, YZZ+14, YSL+10, Cho10, GLIC10, SD12].
Smart-Card-Based [HCL+14]. Smartphone [MDM17, DL15].
Smartphones [Cor14b]. smashed [Fag17].
Smith [ANO16a]. Smooth [XYX+11, YC11, ZBR11]. SMS
[APK+12, SdOD+13]. SMSCrypto
[PSO+15]. Snakes [PC16]. SNOW [PC16].
Snowden [Tox14]. SnC [GC17]. Social
[BSPDI7, KTA12, NSA15, NRZQ15, PYM+15, Rog16, SKGY14, SZT18, WLY+15, ZW15, Zha15b, ZHL15, BDK11, LCM+17, LZC17, SM11a]. Society
[SC15a, Sch12b]. Socio [NS12].
Socio-Rational [NS12]. SoD [VN16]. Soft
[TLCF16, SS17]. Soft-Error [TLCF16].
Softw [WZM12a]. Software
[Bar15, Bee17, EWS14, LRWW14, MV16a, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGH+16b, GIJ+12, HLV10, KHF10, LBOX12, SF12, YWT+12].
Solan [CGB+10]. solid [Cri16]. Solution
[Fll15, GSFT16, HLL15, Kam13, NA10b, YFT17, Cor14a]. Solutions
[LLGJ16, BLV17, KAS15, WW14]. Solved
[IBM13a]. Solving [ANO17c, BB10, Bull10a]. Some
[AD12, Ber12, Dur12, LWW10b, Mid10]. Somewhat
[KOS16]. Song [Cot12]. Sood
[MWZ12]. SOSEMANUK [PC16]. Sound
[COP14, LSR13, Sav15]. Source
[Bis17, FKOV15, MBC15, RWLL14, ABF+14, LZC17, PX13, Pow14].
Source-Based [MBC15]. Sources
[DBH16, BJ16, SSY12]. South
[BL10, LWY11a]. Soviet [Bud16]. SP
[Sas12, SEH12]. SPABox [FGR+17].
Space
[BWR12, BKL+13, NYR+14, RYF+13, ZZ15]. Space-Filling
[BWR12]. Spaces [SH15]. spam
[SKE14]. Spanish
[Pet11, SGG+16]. Sparse
[AGW15, AAT16, BCP+13]. SPARTA
[MMS+17a]. SpartanRPC [CS14]. Spatial
[AV12, CZF12, PDM12, CW14b, NZL+15]. Spatiotemporal [DMLT12]. Speaker
[BJCHA17, PPRP12]. Special
[AN13d, AN16a, AN16b, AN16b, AB10b, CSYY18, GO17, LW13a, PHWM10, XW13].
Specific
[BDK12, KME+12]. Specification
[SK11, SD10]. Specifications
[BMP12]. SPECK [LFW+16, AMK17]. Spectrum
[KD12a, TWZ+12, XNRG15, KBP17, LYY12, MMD13].
Spectrum-Based [TWZ+12, XNRG15]. Speech
[AGW15, LJK17, SAA15, YAMA17]. Speed
[ARM15, GL12, HZ11, KP17, LTKP16, BDL+11, KL13]. Speeding
[RVRRCM12]. SPECS [Che15]. spell
[Bha16]. SPHINCS [BHH+15]. Spies
[Keb15, Fag17, Mac14]. Spintronic
[IG+16]. Splicing [YSC+15]. Spline
[Tan12a]. Split [CG14a, XYZ+12].


DDS12, Dan12, MNS11. ST-Numbering [MNS11]. stage [Mas17]. STAMP [WPZM16]. Standard [Ano12, Ano13a, App13, ABC+17, BCM12, BV11, BV14, GJJ15, GJZ17, HZX15, Loe15, MVVR12, OGK+15, SZN14, TCL15, WWHL12, Yon12, ZC13, BCM13, Kim11, Lzt12, LL16b, Mas17, TSt16a, Wzm12a, Wzm12b, WWB14, YC12, MRRM10, NdMMW16].


Steering [HR13]. Steganalysis [Böh10, DA12, Fri12, JHHN12, KDI12, LJK17, LC15, SGP+12, Tan12a, YLL+12, Y114, YPRI17, LSQ11a, LSQ11b, Sch12a].

Steganalysis-Resistant [YPRI17].

Steganalytic [YPRI17]. Steganographic [DA10, HHS+15, Lw11212, WP15, AGL16, LCC10, CAC14]. Steganography [AGW15, BCG12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZW+14, Joh10, LJK17, LLY+12b, PD12a, Pn10, SK12a, SR12b, TZZ12, YWW10, ZSA12, AUT13, BDK11, BHCdFR12, EEA13, GCK11, Lw11210, LW13, LW17, LWW+10, Maz13, PHN+12, SI12, Sun16, WKH11, WOLS12, ZMS14].

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


storm [AC12]. Story [Cer14, Keb15, Fag17, Gre17, Hea15, Mac14, Mun17, Pea11, Pet11]. Strand [SH15].

strange [Acz11, Gre17]. Strangeness [Ber12]. Strategic [Sch12c]. Strategies [DSSD14, TZZ12, YCM+13, AZF+12, WW17]. Strategy [RZQ15, FLZ+12].

Stratix [SMOP15, SMOP15]. Stream [ABS+12, BMS12, CMLS15, DG12, DGS12, DJG+15, GKS17, GCS+13, HZ11, Hey17, IOM12, KPC+16, Kla10, MD12b, MHC12, MS12b, NN12, PNRC17, WHN+12, ZH15, Dic12, KM10a, LW11, LW13b, MRT10.
BB10, CWL16, CCF17, CRE+12, DLZ+16b, GI12, HXC+11, HCL+14, HLN+10, LMD+16, LQY10, LY16, LNZ+13, MR14b, OŚ12, PRSV17, QZL+16b, RST15a, RST15b, SBS+12, SFKR15, Sev16, SKH17, SGC14, SDM+12, STC11, TKR14, YR12a, AT10, ATI+10, CFVP16, CFZ+10, CLZ+17, dCCSM+12, dCCSB+16, CGH11, CVG+13, CDA14, DZS+12, Eis10, FXP12, GMOGCC15, GSN+16, GPVCD12, JSK+16, JHCC14, KSA16, LCL+15, MLMSMG12, MGP10, MFI13, NLYZ12, QMC17, SS10a, SR10, SRB+12, WS14, YSM14, Zhu13, MA17, Ano11a.

Systolic [MCDB12].

Systolic-Array [MCDB12].

SZK [MX13].

T [SJWH+17].

T-Chain [SJWH+17].

Table [CCL+13, AY14a, LDDAM12].

Tables [PTT16].

Tag [NNAM10, PPH12, CJP15, SPLHCB14, CJP12].

Tags [MO12, HSH11, HDPC13, HQY+16, MK12a, PLsVdLE10, TG17, WCFW18].

Taipei [Yan11].

Taiwan [Yan11].

Takes [Ano16c].

Talking [FD11].

Tamed [NXB13].

Taming [BBDL+17].

tamper [MN10, NC13, WgMW12].

tamper-evident [MN10].

Tamperable [ACM+17].

Tampered [SSA13].

Tampering [CG14a, SRAA17].

TAO [Sta13].

Taormina [Cra12].

tap [ADG16].

target [HRS16].

Targeted [ABJ13].

Tasks [Abe12, FKS+13, CL16].

Taxonomy [AJA16, GAF*15, KMSM15, MA17].

TCC [Cra12, Lin14b, Sah13].

TEA [CWP12].

Teaching [GY13].

Team [LJS+14, Ph10, Ant14].

Tear [Boy16].

Tear-Free [Boy16].

TEASE [ZBR11].

tech [Ano15e].

Technical [Sir16, TS16b, Wag16, JW14, Suc12].

Technique [KBL11, BBBP13, GCSAddP11, TS16a, ZWS+18].

Techniques [Bis17, DA12, GOS12, HPC10, HL10b, LW12, Mor12, PJ12, AB10b, BM13, FGPGP14, Gil10, HT13, KHF10, LH11a, VN17, WMX+17, Joh10].

technologies [JAE10, JAS+11, Lue10].

Technology [GCB+10, Fol16, IEE11a, Wu16, IMB17].

Telecare [MA17],

Telephony [SKEG14].

Television [DTE17],

Tell [Cer14].

Template [NGAuHQ16, SKV12, ATI+10, GCSAddP11].

Templates [DWB12].

temporal [JMW+16, MHT+13, XMD13].

temporal-credential-based [JMW+16, XMD13].

Tenant [TV15].

terahertz [WW13].

Term [SKV12, CFVP16].

termination [SRB+12].

Ternary [ADI11].

Test [HTC+15, JEA+15, LLSW16, MZH15, SS10b, Ano16g].

Testable [RMP10].

tester [RPSL10, SY15b].

Testing [Cou12, SS12a, AY14a, BJR+14].

Tests [GLG12, MS12b, Sim15a].

Texas [IEE13].

Text [GdM16, CR12, SI12, SWW+17].

Text-dependent [GdM16].

Textbook [PP10a].

Texture [TSH17].

Theft [Ber12, Ber17, BTPLST15].

Their [CZL12b, JKS+17, NR12, Hof16, IK15, KK10, Sti11].

them [HLV10, JKS+16, Rus15].

Theological [SS10c].

Theorem [Lau12, HF14a].

Theorem-based [Lau12].

Theoretic [CVM14, WSS12, CDGC12, SD10, SKEG14].

theoretical [KL13, ZZ15, Gas13].

Theoretically [TWZ11].

Theories [ABR12].


theory-based [LPZ15].

There [Cer15, McK10, McK11, SM13].

Thin [Chi16].

Things [AAC+16, CLF+17, LNK+18, LGH+17, NLLJ12, NLY15,
Transfer
[DN12, FMTR12, HL10a, LCCJ13, WCL+18].

Transform
[AN12, BCPV11, LSL12b, pNyWyY+14, OWHS12, YWNW15, BW13, MO14, NES+14, PC14, TK14, yWpWyypN13].

Transformation
[CRE+12, FJHJ12, NXB13, tWmC12, GZHD12, HQZH14, PGLL10].

Transformations
[SA14].

transmission
[PSdO+13, WQZ+13].

Transmitter
[KPB17].

Transparency
[TJZF12].

Transparency-Orientated
[TJZF12].

Transparent
[CCW+10, XTK10].

Transport
[RBHP15, TW14].

Trapdoor
[BKPW12, CWWL12, Mat14, RPSL10, CSZ+11, CW12a].

treatment
[YSM14].

Tree
[BS14, HSH11, BW13, BBB16b].

Tree-based
[BS14, HSH11, CW12a].

Trees
[BTPLST15].

Trends
[Fri12, GCK12, ZMS14, JAE10].

Trends
[Fri12, GCK12, ZMS14, JAE10].

Triangular
[AMVZ12].

Tricks
[GY13].

trimmed
[TTL10].

TRIMS
[MGP10].

Triple
[LW13b, MS12a].

Triplet Image
[LW13b].

Triumphant
[McG11].

Trivium
[MS12b, SR12a].

TRNGs
[YKB10].

Trojan
[NDC+13].

Trojans
[BRPB13].

True
[FRT13, LTKP16, Fag17].

True Erase
[DMS+16].

Truly
[LA10].

Truncated
[KWS+12, WW12].

Trust
[Bar15, BCK17, Gli12, GM14, GSFT16, IGR+16, KMSM15, KGP12, PYM+15, PH12b, PAS13b, Rau15, TMGP13, TV15, WLY+15, Zha15b, CO11, KGO10, MLMSMG12, MGP10, Sch12b, YTL11a].

Trusted
[AWSS17, EAA12, FPY15, YCR16, HTC+10, KÜP13, XZLW15].

trustworthy
[KM10b].

TTP
[ATK11].

TTP-free
[ATK11].

TTPs
[KGO10, TAKS10].

Tulip
[JB11].

Tunnel
[VDB+16, ZBR11].

Tunnel-based
[ZBR11].

tunnels
[Cri16].

Tunny
[Cop10a].

Turing
[Orm16, Blö12, Car10, CS12, Don14, Hai17, Hel17, KSU13, LCKBJ12].

Tutorials
[Lin17].

Tutte
[Ha17].

TV
[CCSW11].

Tweakable
[CMLRHS13, LST12, MLCH10, Sar11, Zha12].

twelve
[BCV12].

twice
[BM15].

TWINE
[KDH13, TY16b].

Twins
[Bow11].

Two
[Ash14, Bru12, CTL13, DZ14, GGHR14, GLW12, HL10b, HP14, KOS16, KU12, LLC11, Lit14, NSMS14, OTD10, YSL+10, YLW13, ZM16, AN15, CSD18, CHS11, DHW+13, FIO15, HPC12, HDW16, JLT+12, JM10+16, Kem11, Li10, McG11, QYWX16, Rus15, SM10b, hSZZ15, WW14, Wat14a, YT11b, ZZC15, GHKL11].

Two-channel
[JLT+12].

Two-Factor
[LLC11, Lit14, JM10+16, Kem11, WW14, Wat14a].

Two-Party
[Ash14, HL10b, HP14, KOS16, NSMS14, ZM16, FIO15, HPC12, ZZC15, GHKL11].

Two-Round
[GGHR14].

Two-Server
[YLW13, CS18].

TwoFish
[MD12a].

Type
[AKP12, CFL13, PFS12, SH15, BNST17, SYL13, WB12].

Type-based
[CFL13, SYL13].

Type-Flaw
[SH15].

Types
[BCEM15].

U.S.
[Maf16].

Ubiquitous
[OS16, Par12b].

UESDE
[YZ12].

UHF
[HQY+16, PPH12].

UK
[Che11, PJ12, vDKS11, Ano15e].

Ukraine
[OGK+15].

ultra
[ATM18, GW14, TG17, WCFW18].

Ultra-lightweight
[ATM18, TG17, WCFW18].

ultralightweight
[ACM12, GMSW14, SB17].

UMTS
[OHJ10, TM12].

un-traceability
[Chi13a].

Unattended
[BN14].

unauthentic
[LLMSMG12].

Unbounded
[WW11c, YZ12].

unbreakable
[Bha16].

Uncalibrated
[SGP+12].

Uncertainty
[FHS13, BBGT12].

Unclonable
[Ano16e].

Unconditional
[Jia14a].

Unconditionally
[CFOR12, LHF12, SNJ11].

Unconditionally-Secure
[CFOR12].

Uncovering
[FMS12a, WBC+10].

Undeciphered
[Rao10].

Undeniable
underfeeding [BBBP13].
underhanded [Cra14]. Understanding [EPAG16, PP10a, Bar12]. Undisturbed [YCL17]. Unexpanded [SA16a].
Unforgeable [HHP17]. Unidirectional [LSC12, DKL+16]. Unified [ZSW+12].
uniformly [YKKL12]. Unilaterally [GRL12].
unintended [Ess17]. union [BBDL+17, Bud16]. Unique [SSPC12, SOS15].
units [ABDP15]. Universal [ASM12, BJL12, NR12].
university [YKKL12]. Universe [LW16, FNWL18, LFZ+17]. University [Ano17b, CGB+10, Wes16].
 Unlike [Goo12]. unlikely Fag17].
Unlocking [VS16]. unmanned [XWZW16].
Unprovable [Pas13a]. unsigncryption [EZ15]. unspoofable [NR11].
unstructured [CML16]. untrusted [Mun17, Pea11]. untraceability [YHL16].
untraceable [JMW+16]. Untrusted [LQY10, MS16, ATKH+17, DRD11, MoO11, WS13].
updateable [LCL+17a]. Update [BCE+10, LQY10, FS18, WLFX17]. updating [GCS+AddP11].
Upper [AMVZ12]. URLs [AY14a]. USA [Dun12b, IEE13, Kia11, Lin14b, Pie10, Rab10, ACM10, ACM11, IEE10, IEE11b].
Usability [RAZS15]. Usable [DL15, TGC16].
usage [AKK+17, BHC+12]. Use [CSV15, DFKC17, KOS16, NR12, YT12, der10, CZ15b, Die12, Hof16, KK10, 
MBF+13, OO10, Sti11]. Used [CGCGPDMG12, BM15, MS13b]. useful [dCCSB+16].
Use [BLV17, BKJP12, FLH13, GdM16, Har16, JN12, LLCL17, MZHY15, MBC15, 
MMJ17, OdH12, PDT12, PWVT12, RVH+16, SZDL14, SPM+13, WgMdZI12, WgMW12, ZPW16, AaBT16, ATKH+17, 
CH10, CHS11, CLHJ13, DSCS12, GH16, HL14, KKM+13, KLW+16, KDW+17, LH10c, 
LMN+11, LNKL13, LH13, MM12, OKG+12, hSZZ15, WT10a, WOLS12, YHL16, YSL+10].
User-centric [BLV17]. User-controlled [Har16]. User-Friendly [SZDL14, WOLS12].
User-Generated [LCL17b]. User-Level [BKJP12]. user-participating [CH10].
Users [DPCE16, KAK15, TAKS10, WPZM16, ATK11]. uses [Rus15]. Using [ABS+12, ABB+14, Ano15a, Ayu12, ARM15, 
BBC+13, BCPV11, Bee17, BFMT16, BKLS12, BJR+14, CST+17, CCL+13, DSB16, 
DR12, DA10, DBPS12, DL12, ERLM16, ERRMG15, FMS12a, GH11a, GSC17, 
GAS+16, HHS+15, IL15, JEA+15, KBL11, Lac15, LYZ+13, LLG16, MM17, MBC15, 
MS16, NIS12, NGAuH16, NNAM10, NN12, NMS14, PMZ13, PSS+13, PDMR12, PDT12, 
PCPK14, RVRS812, SR12a, SFE10, SSA13, SRA17, SC12, SR12b, Tan12a, TKR14, 
WgMdZI12, WY12, YWW10, YWNN15, YCL17, YSS14, ZH15, ZP16, ZS12, 
dsRdzV12, ATKH+17, ASVE13, BM13, CHS11, CR12, CLHJ13, CP13, Crl16, Dav11, 
DTZZ12, EEAZ13, FES10, Har14, HZW17, HL14, HPY10, HCC10, HS11, JCHS16, 
JMW+16, KII1, KY10, KKG14, KM11, KSV13, KU11, KBP17, KLW+16, LXLY12, 
LC17, LH10c, LNM+11, LXWM12, LH13, 
MLM+13, MM12, MS13a, MMS13, MM14a].
using [MKH+12, MRR17, NTKG17, 
PBC14, PC14, QD16, RS15, RS17, Sar11, 
TLCE16, TG17, TK14, TLL13, UUN11, 
yWPvNy11, gWPvNy+14, WMX+17, 
WHJ17, YWH12, ZZ+14, YSL+10, 
ZZKA17, ZLW+12, ZYC+17, ZXW+18].
utilization [NZM10].
Validating [GLJ+12]. Validation [FPY15, BJR+14]. Validity [BCF16].
valuable [Ana14]. Value [LSL12b, YWW10, BWA13, Svo14]. valued 
[BNA15, TMK11]. VANETs [Wu17].
VANETs [BMM12, CGCGPDMG12,
Watermark [CHHW12, DLMM+18, EMW14, KBL11, LZC+12b, MCD12, SJ12, YE12, ZS12, HB13, TLL13, WYL13].

Watermark-Driven [DLMM+18].

Watermarking [BCGAPM12, BF12, BCPV11, CG12b, CHHW12, DG17, FM15, Fra15, Fra16, GKS17, GP17, HFC10, HGT15, HHMK14, JSZ12, Joh10, JKHeY12, KD12a, LSL12b, LP12, MM17, MR16, MU12, NGAuHQ16, NC12, NXH+17, pNyWyY+14, OHWS12, RS16, RP12, RR11, SAA15, SLGZ12, SSA13, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, gWPnyY+14, WXL+17, tWmC12, XNG+14, XNRG15, YWNW15, YPR17, YYO15, ZZX+11, AP10, AMK12, BW13, BWA13, CCLL11, CT11a, CSS+13, GHZ12, GA11, HKB14, HWYW14, JK13, KPS10, KJN+16, KM11, LSR13, LXC11, LLH12, Lin14a, LWY12, MMSD13, MM14a, MO14, MK11, NC13, PTK14, PWLL13, PW10, PGLL10, P KS18, PC14, PR+12, RS17, Tay14, TK14, TTL10, TPKT12, WLDB11, yWPnyL11, Wnl3, yWPnWyCyN13, WZL13, YWT+12, ZZKA17].

Watermarking-Encryption [SLGZ12].

Watermarks [GL10, YT12].

WAVE [BMM12].

Wavelet [AGW15, LSL12b, MR16, AMK12, BW13, LXC11, MO14, WPnyL11].

Wavelet-Domain [MR16].

Way [CPS16, DSS14, Mat14, HR10, LP11, RK11].

Weak [BF11, DY13, HDWH12, PYM+15, Pud12, GJP15, RH10].

Weakening [SFKR15].

Weaker [SS12].

Weakness [AMOR13].

weaknesses [Nos11, Nos14].

weapon [Zet14].

Wear [LY15].

Wear-leveling [LY15].

Wearable [BCTPL16, XJR+17, LIK+17].

Wearout [DFKC17].

web [GPn+12, IMB17, KRM+10, KGO10, ATK17, BS12, BKJP12, CTC+15, CFST17, CD12, DR11, Fra16, HCM11, SP15a, SPm+13, ZGC16].

Web-Based [CD12].

web-content [GNP+12].

WebCAllerID [HCM11].

Website [Boy16].

 Websites [RS11].

Webster [Pea11].

WECNR [DDS12].

Wei [SBS+12].

Weierstrass [LL11].

weight [O’S11].

Weighted [YLL+12, YTH17].

Welchman [GW14].

Well [JCM12].

Wherefore [BDK11].

Wear [LY15].

Wear-leveling [LY15].

Wearable [BCTPL16, XJR+17, LK17].

Wearout [DFKC17].

Withholding [BR17].
REFERENCES

BF11, BGV14, CCW+10, FSX12a, GH11a, GST12, GLM+16, HDPC13, ISC+16, LLY15, LGWY12, RG10, SYL13, SLZ12, TAKS10, WWYY11, XQL11, YS12, YKC+11, YFK+12, ZY17b. Witness [GGHW17].

WLAN [KAHKB17], woman [Fag17], women [Hea15, McK10, McK11, McK12, Mun17].

Word [WW12], Word-Oriented [WW12], Words [GdM16, KM10a]. Work [RS11, Shp10, Tay14, BG14, Sch15a].

workbench [CFH+13], workflows [BPP10], working [Wat14b], Workload [BCO13].

Workshop [MV12, Sen10, Yan11], Workshops [DDS12]. World [Aano16h, Aano17d, BFK16, BPS16, FKS+13, KM10c, MDMJ17, Tom16, Con12, GIJ+12, Goo12, LCKBJ12, Pet11, Sch15c, Zet14, Mun17].

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

Worst [BIKK14], would [McG11].

Wrapped [KM15, KM16], Write [YNQ15], Write-Efficient [YNQ15], writing [LT14b], wrong [LHA+12]. WSN [DL12], WSNs [ZYL+10], Wu [LLLK10].

WW2 [Don14], Wyner [ADG16].

X [Smi11a], X9.98 [Ano11b], X9.98-2010 [Ano11b], XML [BPP10, CH11, GA11].

XMSS [BDH11, HRB13, HBG+17], XOR [App13], XTEA [CWP12, IS12], XTS [Mar10c], xviii [Sch15a].

Yamamoto [Car11], Yan [Cou12], Yao [GKS17], Years [DR10, BCV12], Yehuda [Full0]. Yen [LLLK10], Yuan [FMS12a].

YubiKey [Jac16], Yves [Ter11].

z13 [ACD+15], Zero [AMH+16, BW12, CLP13a, COP14, GJO+13, GOS12, IW14, MX13, MT12, OOR+14, Pan14, SJ12, WCL+18, YCL17, Zet14, KPP16, TLL13, WWBC14]. Zero-Correlation [BW12, YCL17, WWBC14]. Zero-Cost [AMH+16].

Zero-Knowledge [CLP13a, GOS12, IW14, MX13, MT12, Pan14, KPP16]. Zero-Watermark [SJ12, TLL13]. Zheng [AHS14].

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

References

Akyildiz:2014:OTB


Applebaum:2017:AC


Abo-alian:2016:KDB

Alshaimaa Abo-alian, Nagwa L. Badr, and M. F. Tolba. Keystroke dynamics-based user authentication service for cloud computing. Concurrency and Computation: Practice and Experience, 28(9):2567–2585,
REFERENCES

June 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Ambrosin:2016:FAB


Albertini:2014:MHE


Arora:2012:ILM


Akleylek:2016:SPM


Aghili:2018:ISA

REFERENCES

January 2018. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).


REFERENCES

Almeida:2013:CCA

Arnold:2012:ICC

Ateniese:2017:LCS

Ambrosin:2017:OBB

Adrian:2015:IFS


José Bacelar Almeida, Manuel Barbosa, Jean-Christophe Filliâtre, Jorge Sousa Pinto, and Bárbara Vieira. CAOVerif: an open-source deductive verification platform for cryptographic software imple-

**Ananth:2013:SFP**


**Avoine:2016:SSP**


**Aid:2013:DIO**


**Acar:2013:SPA**


**Andreeva:2012:SAS**

Elena Andreeva, Andrey Bogdanov, Bart Mennink, Bart Preneel, and Christian Rechberger. On security arguments of the second round SHA-3 candidates. *International Journal of Information Secu-
Arapinis:2012:RET


ALMashrafi:2012:AIM


Applebaum:2010:PKC


Arias-Cabarcos:2015:BIP


Arnold:2015:NGH

Amoah:2016:FMA


Ardagna:2010:ECP


Avoine:2012:PFS


Austrin:2017:ICT

[ACM17] Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth. On the impossibility of cryptography
REFERENCES


**Aczel:2011:SWL**


**Alvarez-Cubero:2016:AVL**


**Aizatulin:2012:VCC**


**Anyanwu:2010:DCS**


**Ayday:2012:DAA**


**Aliberti:2016:RPS**

REFERENCES


[AGH+17] Timos Antonopoulos, Paul Gazzillo, Michael Hicks, Eric Koskinen, Tachio Ter-auchi, and Shiyi Wei. Decomposition instead of self-composition for proving the absence of timing chan-


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


REFERENCES


Ahir:2017:LAR


Adj:2013:WDC


Aumasson:2014:HFB


Ahmadian:2010:PDS


Alvarez:2012:CAB


Albrecht:2012:SDL

Alexander Albrecht and Felix Naumann. Schema

Arshad:2015:SAI


Aga:2017:ISM


Anawis:2014:ARR


Anderson:2013:MNF


Anonymous:2010:NDS


REFERENCES


[Ano15d] Anonymous. Quantum cryptography security hole revealed, energy-time entanglement vulnerable to attack. *Scientific Computing, ??(??):??*, Decem-
REFERENCES

Anonymous:2015:UGB


Anonymous:2016:CPSd


Anonymous:2016:CPSe


Anonymous:2016:EMT


Anonymous:2016:FVM


Anonymous:2016:GUP

Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

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

Anonymous:2017:BRM


Anonymous:2017:CCS

that was also supported by the cards.

**Anonymous:2017:HDQ**


**Anonymous:2017:MBH**


**Anonymous:2017:RV**


**Anonymous:2017:MBH**


**Andriotis:2013:JSD**


**Agarwal:2010:BR**

REFERENCES

ISSN 1551-6857 (print), 1551-6865 (electronic).


Al-Qarni:2012:EII


Adj:2014:SRC


Azarderakhsh:2015:PHS


Ambrose:2012:RII


Asharov:2016:LPI


Artemenko:2017:PGO

Andrade:2016:LEP


Ahmadi:2011:SKC


Ahmadi:2012:SKE


Asharo:2014:TCC


Al-Sinani:2012:UCB


**Alam:2015:ACF**


**Aslan:2016:DEM**


**Abdalla:2012:LRS**


**Altaf:2017:LHL**


**Awad:2017:OLO**


**Anzala-Yamajako:2012:RAC**

Ahmad:2014:RTN


AlTawy:2014:IDR


Ayub:2012:BRB


Apavatjrut:2012:EEA


Alshammari:2011:CET

Riyad Alshammari and A. Nur Zincir-Heywood. Can encrypted traffic be identified without port numbers, IP addresses and payload inspection? *Computer Networks (Amsterdam, Netherlands: 1999)*,
REFERENCES


Alavi:2014:RQE


Behnia:2013:IEB


Bailin:2012:ERG


Berbecaru:2010:FSM

Diana Berbecaru, Luca Albertalli, and Antonio Lioy. The ForwardDiffsig scheme for multicast authen-
REFERENCES


REFERENCES


[Barak:2014:OEF] Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth,

Beurdouche:2017:MSU


Bernstein:2017:SRD


Boldi:2012:IUG


Bernstein:2011:PCI


[BCEM15] Michele Bugliesi, Stefano Calzarava, Fabienne Eigner, and Matteo Maffei. Affine refinement types for secure distributed programming. *ACM Transactions on Programming Lan-
REFERENCES

Buhrman:2014:PBQ


Bahri:2016:CCO


Bahi:2012:SCS


Borghini:2012:PLL


Baelde:2012:TPR


Bahi:2011:ECS

Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux.

Barthe:2012:CA


Beunardeau:2016:WBC


Bitansky:2013:SNI


Brandenburger:2017:DTC


Bernstein:2014:CKR

Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange. Curve41417: Karatsuba revisited. Report, Department of Computer Science, University of Illinois at Chicago, and Department of Mathematics and Computer Science, Technische Universität Eindhoven, Chicago, IL 60607-7045, USA and P.O. Box 513, 5600 MB Eindhoven, The Nether-
REFERENCES


REFERENCES

101

(184x646) REFERENCES

101


[Besso:2011:BWC]

[Basso:2011:BWC]

Basso:2011:BWC

Bassani:2013:DDS


Bessani:2013:DDS


Bhasin:2015:EFB

[BDGH15]

Biddle:2012:GPL


Biddle:2012:GPL

[BCV12]

Bender:2012:DSP


Bender:2012:DSP

[BDGH15]
Buchmann:2011:XPF


Backstrom:2011:WAT


Bernstein:2011:HSH


Bossuet:2016:EPA


Bendlin:2011:SHE


Bertoni:2011:CSF

REFERENCES

//sponge.noekeon.org/CSF-0.1.pdf.


REFERENCES

89, January 2012. CODEN CPTRB4. ISSN 0018-9162.


REFERENCES

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

Barthe:2014:PRV


Bobba:2010:ABM


Bhargavan:2016:MVP


Beimel:2012:SSS


Berger:2016:EGF


Boldyreva:2014:MEW

Alexandra Boldyreva and Paul Grubbs. Making


Barbulescu:2013:QP


Barbulescu:2014:HQP


Barthe:2012:ACA


Biswas:2017:STC


Borcea:2017:PEE


Brakerski:2014:LFH

Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on
REFERENCES

*Barkatullah:2015:GCF*


*Behnia:2012:SEI*


*Bernstein:2015:SPS*


diff.pdf.


B. B. Brumley and K. U. Jarvinen. Conversion al-

**Boche:2016:DSK**


**Bouraoui:2017:HAE**


**Bogdanov:2012:UTC**


**Benhamouda:2016:NFP**


**Brubaker:2014:UFA**

USA, 2014. ISBN ???. LCCN ???. URL ???.

**Boldyreva:2012:NPG**


**Bouti:2012:SCB**


**Bhuyan:2014:DDD**


**Braun:2012:ULA**


**Brakerski:2010:OHB**


**Bogdanov:2013:SDS**

Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. SPONGENT: The design space of lightweight cryptographic hashing. *IEEE
REFERENCES


Byun:2011:SMC


Bai:2012:SSR


Bernstein:2014:HEC


Bidgoly:2015:MQV


Blanchette:2012:BPC


Blaze:2016:UHR

Benzaid:2016:FAW


Buchmann:2017:PCU


Blomer:2012:TKG


Blondeau:2015:IDA


Bernstein:2012:SIN


Bestavros:2017:PSU

REFERENCES


CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-27375-9_4/.

Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar. A differential
fault attack on the grain family of stream ciphers. Lecture Notes in
Computer Science, 7428:122–139, 2012. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-33027-8_8/.

Faezeh Sadat Babamir and Ali Norouzi. Achieving key privacy and invisibility
full.pdf+html.

N. Buckley, A. K. Na-
REFERENCES


REFERENCES


REFERENCES

org/csdl/mags/sp/2016/06/msp2016060007.html.

Balsa:2017:TIC


Brakerski:2014:VBB


Brakerski:2013:WHB


Bradbury:2015:BSB


Briggs:2011:SDC


Broemeling:2011:AES


Brook:2017:LSR

REFERENCES


REFERENCES


REFERENCES


[Buchmann:2010:EKG]

[Bulygin:2010:CA]

[Burk:2011:AMD]

[Bruzek:2011:EFH]

[Buk10]
[Budiansky:2016:CWN]

[BV11]
Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE.

[BV14]
Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE.
Bayrak:2012:AII


Baek:2013:SPK


Bhatnagar:2013:BIW


Bai:2016:ALC


Bhatnagar:2013:SRI

REFERENCES


Carlson:2011:JRW


Casselman:2010:VC


Cobb:2013:LMS


Cacín:2010:EKS


Chang:2014:RRT


Chadha:2016:AVE


Chretien:2015:SPP


[Chatterjee:2016:TAD] Urbi Chatterjee, Rajat Subhra Chakraborty, Hitesh Kapoor, and Debdeep Mukhopadhyay. Theory and application of delay constraints in arbiter PUF. *ACM*
REFERENCES


REFERENCES


Chu:2014:KAC


Chen:2010:ALD


Cui:2016:RD


Criswell:2014:VGP


Cheng:2013:DVB

Yueqiang Cheng, Xuhua Ding, and Robert H. Deng. DriverGuard: Virtualization-based fine-grained protection on I/O

Ciriani:2010:CFE


Ciriani:2010:TPA


Choo:2016:CCT


Cao:2012:ITM


Chari:2010:DSC

REFERENCES


REFERENCES


Celesti:2016:ALT


Choo:2017:EDF


Chang:2010:PRN


Chen:2010:IFA


Camenisch:2012:EAA


Che:2012:WAM


REFERENCES


Cohney:2017:PSR


Curtmola:2011:SSE


Cheng:2012:PAI


Chandran:2014:PBC


Chen:2010:NUP


Chang:2011:DEQ


Cha13a

Aldar C.-F. Chan. On optimal cryptographic key derivation. Theoretical
REFERENCES

Chang:2013:MPQ

Chappell:2013:PMI

Chen:2011:CCI

Cheswick:2013:RP

Chen:2015:SSS

Chen:2017:CSQ
REFERENCES


REFERENCES


Cilardo:2011:EPT


Cheng:2013:EHM


Cao:2014:SCI


Cho:2012:CBF


Chase:2013:SMN

Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn. Succinct malleable NIZKs and an application to compact shuf-
Chuang:2011:LMA


Colin:2016:CTC


Comon-Lundh:2010:DSP


Chang:2011:RSB


Chen:2017:PGF


Chong:2013:ASG

Song-Kong Chong, Cheng-Chi Lee, and Min-Shiang Hwang. An authentication scheme for the global mobility network. Parallel
REFERENCES

Processing Letters, 23(3):1350009, September 2013. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Chen:2016:RPR


Chen:2012:NCB


Chen:2013:TSE


Cao:2012:SRH


Canetti:2013:PCC

Castro:2013:RAM


Chang:2012:PRS


Cui:2016:KAS


Chen:2014:CDP


Cheng:2017:ISK


Cremers:2011:OSV

REFERENCES

Cozzens:2013:MEE

Cui:2014:SSA

Coles:2016:NAU

Chakraborty:2013:EHI
REFERENCES

**Chakraborty:2015:SSC**


**Chen:2017:VME**


**Cao:2016:OMA**


**Chen:2012:FAA**


**CNRS:2014:NAS**


**Coron:2012:PKC**

REFERENCES

Chin:2011:ACS

Conitzer:2010:AP

Constantin:2012:RSN

Copeland:2010:CBG

Copeland:2010:CSB

Chung:2014:RRS

Cordova:2014:EBS
Tim Cordova. Encrypted


[CRST15] Chris Culnane, Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague. vVote:
REFERENCES

Chhabra:2011:NSN

Chapin:2014:SRP

Chattaraj:2018:NTS

Chadwick:2014:AFI

Chen:2013:RWM
Xianyi Chen, Xingming Sun, Huiyu Sun, Zhili Zhou, and Jianjun Zhang. Reversible watermarking method based on asymmetric histogram shifting of pre-
REFERENCES

- Chen:2017:SIE

- Ciegis:2016:ADP

- Chong:2015:SID

- Chow:2012:EPV

- Chen:2018:SIA

- Chen:2011:IBT
  Xiaofeng Chen, Willy Susilo, Fangguo Zhang, Haibo Tian, and Jin Li. Identity-based trapdoor

**Chen:2011:ARI**


**Calzavara:2015:SLA**


**Chin:2013:SMB**


**Chang:2012:GBP**


**Chou:2013:TIB**

Crenne:2013:CMS


Calmon:2014:ITM


Chung:2012:CBI


Chen:2014:SBB


Chen:2014:DSE

Jie Chen and Hoeteck Wee. Doubly spatial encryption from DBDH. *Theoretical Computer Science*, 543(??):79–89, July
REFERENCES


REFERENCES

Dharwadkar:2010:SSG


Djebbar:2012:ASB


Danezis:2012:FCDb


Davies:2011:IST


Diong:2012:DAU


Dacosta:2012:OTC

Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. *ACM Trans-
actions on Internet Technology (TOIT), 12(1):1-1:??, June 2012. CODEN
???? ISSN 1533-5399 (print), 1557-6051 (electronic).

**[Cordeiro:2016:MPG]**


**[Cordeiro:2012:IMB]**


**[DePrisco:2013:CVC]**


**[DArco:2014:MIC]**


**[DaRolt:2013:NDS]**

Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. A novel differential scan attack on advanced DFT structures. *ACM Transac-
REFERENCES


Dew:2011:BRB


Dew:2011:BRB

[Dew11]


DuPont:2016:ECC


DeCapitanidiVimercati:2017:AMM


Deng:2017:LLH

Zhaoxia Deng, Ariel Feldman, Stuart A. Kurtz, and Frederic T. Chong. Lemonade from lemons: Harnessing device wearout to create limited-use security architectures. ACM SIGARCH Computer Ar-
REFERENCES


Ding:2012:CLS


Djuric:2015:FSF


Dutta:2017:EFC


Dupressoir:2014:GGP


Ding:2012:NRR


Drimer:2010:DBP

Saar Drimer, Tim Güneysu, and Christof Paar. DSPs, BRAMs, and a pinch of logic: Extended recipes for AES on FPGAs. ACM Transactions on Reconfigurable Technology and Systems, 3(1):3:1–3:??, January 2010. CODEN ????
REFERENCES

Dubeuf:2016:EP

Dodis:2010:CA

Driessen:2013:ESA

Diem:2012:UES

Drosou:2012:SAH

Dinoor:2010:PIM
REFERENCES


REFERENCES

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

**Durumeric:2014:MH**


**Dolev:2016:MCG**


**Doychev:2015:CTS**


**Dodis:2012:MAR**


**Dunkelman:2012:MCE**


REFERENCES

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


[DMWS12] John Demme, Robert Martin, Adam Waksman, and...

**David:2012:UCO**


**Donovan:2014:ATM**


**Doroz:2015:AFH**


**Duncan:2012:CAI**


**Ding:2017:CSM**


**Das:2016:CWM**

Aveek K. Das, Parth H. Pathak, Chen-Nee Chuah,


**[Dixon:2016:NTO]** Lucas Dixon, Thomas Ristenpart, and Thomas


Dachman-Soled:2014:COF


Dodis:2014:HEY


Dini:2013:HHS


Drosatos:2017:PET


Deng:2012:VIA


Dunkelman:2012:MEK

Orr Dunkelman. From multiple encryption to knapsacks — efficient dis-
REFERENCES

section of composite problems. Lecture Notes in Computer Science, 7668: [DW12]

Dunkelman:2012:TCC


Dorn:2012:ECE


Dong:2012:KKD


Durcheva:2015:SAI


[Dur15]


REFERENCES


[EB17] Ertem Esiner and Anwita-


[Ekb16] Ertem Esiner, Adilet Kach...

**Engels:2013:NLL**

**ElBansarkhani:2012:ELB**

**Embar:2014:PWO**

**Evtyushkin:2016:UMC**

**Eberz:2016:LLE**

**El-Razouk:2015:NHI**
H. El-Razouk, A. Reyhani-Masoleh, and Guang Gong. New hardware implementations of WG and WG-StreamCiphers using poly-

**Estebanez:2014:PMC**


**Engels:2012:HLA**


**Ebadi:2015:DPN**


**Ess:2017:DDU**


**Everett:2012:EC**


**Everett:2016:SES**

REFERENCES


[Jason Fagone. *The woman who smashed codes: a true story of love, spies, and the unlikely heroine who outwitted America’s enemies*. Dey Street Books,]


[Feh10] Serge Fehr. Quantum


[FHM+12] Sascha Fahl, Marian Harbach, Thomas Muders,


REFERENCES

**Fei:2012:GTK**


**Fan:2013:CEM**


**Fan:2013:CEM**


**Fehr:2013:FCC**


**Ferguson:2010:SHF**

REFERENCES

hash.info/sites/default/files/skein1.3.pdf.

Forler:2012:DA


Feng:2012:CAO


Fallahpour:2015:AWB


Ferrag:2018:SCN


Faust:2014:CNM


Feng:2012:USD

Fraczek:2012:MSI


Fernandez-Mir:2012:SRA


Ferreira:2015:LPA


Fu:2018:LUA


Fokkink:2012:TCG


Folger:2016:TQH

REFERENCES


Fox:2013:RLQ


Faigl:2014:PEC


Faust:2012:PLR


Fu:2015:TVG


Fathimal:2016:SSS

REFERENCES

CODEN ????? ISSN 0219-4678.


[Fu:2016:EPS] Zhangjie Fu, Kui Ren, Jianguang Shu, Xingming Sun, and Fengxiao Huang. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Transactions on Parallel and

Frauchiger:2013:TRR


Forbes:2015:CTC


Fugkeaw:2018:SSA


Fang:2011:ICP


Fang:2012:CCS


Ferguson:2010:CED

Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. Cryptography Engineering: Design Principles and Practical Ap-
REFERENCES


Feng:2011:GDA


Fujioka:2012:SHI


Fujioka:2012:SEP


Fadlullah:2010:DCA


Fuchsbauer:2011:CSV

REFERENCES


Fulton:2010:BRB


Fiore:2017:PGP


Feng:2013:ECE


Fanyang:2012:SAK


Fu:2017:DF


Feng:2011:VBF

Keqin Feng and Jing Yang.

**Fan:2015:IRD**


**Fan:2013:KIS**


**GomezPardo:2013:ICM**


**Gross-Amblard:2011:QPW**


**Gregio:2015:TTM**

REFERENCES


**Galindo:2013:NIC**


**Gasarch:2013:RBC**


**Gore:2015:ECS**


**Gupta:2012:RBC**

Swati Gupta, Seongho Cho, and C.-C. Jay Kuo. Current developments and
future trends in audio authentication. *IEEE Multi-

**Gupta:2013:HPH**
Sourav Sen Gupta, A. Chatt-
High-performance hardware implementation for RC4 stream cipher. *IEEE Transactions on Compu-

**Guerra-Casanova:2011:SOT**
J. Guerra-Casanova, C. Sánchez-
Ávila, A. de Santos Sierra, and G. Bailador del Pozo.
Score optimization and template updat-
ing in a biometric technique for authen-
ember 2011. CODEN JS-
SODM. ISSN 0164-1212 (print), 1873-1228 (elec-
science/article/pii/S0164121211001427.

**Granado-Criado:2017:HCH**
José M. Granado-Criado and Miguel A. Vega-
Rodríguez.
Hardware coprocessors for high-
CODEN JOSUED. ISSN 0920-8542 (print), 1573-
0484 (electronic).

**Gong:2016:ATI**
Junqing Gong, Xiaolei Dong, Zhenfu Cao, and Jie Chen.
org/content/59/11/1669.

**Guerin:2016:TDU**
Nilson Donizete Guerin, 
Jr., Flavio de Barros Vi-
dal, and Bruno Macchi-
avello.
Text-dependent user verification of hand-
written words and signature
s on mobile devices. *The Computer Journal*, 59(9):1415–1425, Septem-
org/content/59/9/1415.
REFERENCES

Geller:2013:MIS


Gentry:2010:CAF


Gentry:2013:EMH


Gaspar:2012:SEF


Gong:2010:PCI


Grigg:2011:CCN


Garg:2016:CIO

Sanjam Garg, Craig Gentry, Shai Halevi, Mari-


Gentry:2013:EIF


Gope:2016:EMA


Gordon:2011:CFS


Gentry:2012:RSB


Gentry:2013:FSB


Gentry:2012:FHE


Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov.


Guangyong Gao and Guoping Jiang. A lossless copyright authentication scheme based on Bessel–Fourier moment and ex-

Gu:2015:EIB


Gravier:2015:WOD


Goyal:2013:CZK


Gu:2017:IBM


Geetha:2011:VRN


Garay:2016:MPA

Juan A. Garay, Vladimir

[194]
REFERENCES


Grigoriev:2017:YMP


Gaj:2017:DCR


Guo:2010:HMW


Gouvea:2012:HSI


Gorawski:2012:EAS


Gligor:2012:SLT

Virgil Gligor. Street-level trust semantics for attribute authentication (transcript of discussion).
REFERENCES


Gollmann:2010:SCR


Guo:2018:PSC


Gagne:2012:AVB


Guo:2011:ED


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.
Gradwohl:2010:SRC


Gradwohl:2013:SRC


Guo:2012:ETD


Guo:2013:TVS


Goyal:2011:SCP


Garmany:2013:PPR


REFERENCES

Guo:2014:SAS


Gao:2014:URA


Groza:2017:LCL


Gong:2012:KNF


Garay:2017:SIA


Goodin:2012:CBS

Dan Goodin. Crypto breakthrough shows Flame was designed by world-class scientists: The spy malware achieved an attack unlike any cryptographers have seen be-

Garcia:2012:ERP


Gorski:2010:CDS


Groth:2012:NTN


Glowacz:2017:IDW


Goodrich:2012:EVW


Genkin:2016:PKE


Grossschadl:2012:EJI

[Johann Großschädl, Dan Page, and Stefan Tillich.
Efficient Java implementation of elliptic curve cryptography for J2ME-enabled mobile devices. 

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


Thomas Gibson-Robinson and Gavin Lowe. Analysing applications layered on
REFERENCES


Guha:2017:RTS


Guin:2016:FCS


Gong:2016:FSC


Gierlichs:2012:ICD


Genkin:2013:RKE

Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. Technical and web report, Technion and Tel Aviv University and Weizmann Institute of Science, Haifa and Tel Aviv, Israel, December 18, 2013. URL http://www.cs.tau.ac.il/~tromer/acoustic/;
REFERENCES


Galindo:2014:LCL


Ghosh:2014:BBB


Gorbunov:2012:FEB


Gorbunov:2015:ABE


Greenberg:2014:GWB


Gebotys:2016:PCP

REFERENCES

Wang:2014:RAW

Gao:2015:GCC

Guo:2012:AKE

Guo:2017:EMD

Gao:2012:RHC
Xifeng Gao, Caiming Zhang, Yan Huang, and Zhigang Deng. A robust high-capacity affine-transformation-invariant scheme for watermarking 3D geometric mod-
Guo:2018:SMK


Ge:2013:SAP


Hamamreh:2012:RPA


Hamlin:2017:NMC


Hanyok:2012:EHH

Robert J. Hanyok. Eaves-

Hardesty:2016:SUC

Hayes:2013:NSA

Houmansadr:2013:BCN

Hurlburt:2014:BBC
REFERENCES

1520-9202 (print), 1941-045x (electronic).

Hetzelt:2017:SAE

Hernandez-Becerril:2016:GIS

He:2013:HEH

Hulsing:2017:XEH

Hao:2012:SAM

Hu:2017:ATE
Hwang:2010:RIB


Hsu:2011:NLM


Hore:2012:IED


Hernandez-Castro:2012:MTA


Huang:2014:FOS


Hsu:2011:WLC

Francis Hsu, Hao Chen, and Sridhar Machiraju. WebCallerID: Leveraging cellular networks for Web

Hernandez-Castro:2012:AFH

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

Hwang:2012:ABA

Hellman:2017:TLC
Martin E. Hellman. Turing Lecture: Cybersecu-

Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Heys:2017:SCF


Harn:2014:MTS


Hoang:2014:IMD

REFERENCES

Huang:2016:EDP

Heyse:2012:TOC

Hua:2015:TSE

Han:2011:PEB

Harn:2015:DTS

Hu:2016:EWS
REFERENCES

Hayashi:2013:AEI


Huber:2014:TPW


Huang:2017:BBC


Haitner:2011:PRI


Hong:2015:RSM


Hinarejos:2015:MES

REFERENCES


Heil:2014:APH


Holenstein:2011:ERO


Harn:2010:AGK


Hazay:2010:EST


Hsu:2011:NIB


Hsieh:2014:AMU

[Wen-Bin Hsieh and Jenq-Shiou Leu. An anonymous mobile user authenti-

Hmood:2015:ACA


Hu:2012:VMS


Hu:2016:PBR


Huang:2011:ISL


Huang:2015:MSE

Harn:2011:FDM


Humire:2010:SPR


Herranz:2011:RBS


Hohenberger:2012:DDQ

REFERENCES


Huang:2014:SWC

Hefeeda:2010:ASM

Herzberg:2012:TJA

Hore:2012:SMR

Hoang:2012:ESB

Hirt:2014:BA
Martin Hirt, Ueli Maurer, and Pavel Raykov. Broadcast amplification. Lecture
Harnik:2010:CIC


Hoffmann:2015:LBQb


Hoffmann:2016:LBQb


Hylla:2012:CBE


Hazay:2014:OSA

Carmit Hazay and Arpita Patra. One-sided adaptively secure two-party computation. Lecture Notes in Computer Science, 8349:368–393, 2014. CODEN LNCSDO. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
REFERENCES


Halder:2010:WTR


He:2012:ECT


Hur:2010:CCS


Han:2016:GGA


Howe:2015:PLB


Han:2014:GTK

Fei Han, Jing Qin, Huawei Zhao, and Jiankun Hu. A general transformation


Haitner:2010:EIC


Hwang:2011:CD


Homma:2014:TFD


Halevi:2011:TBH


Han:2013:IBD


Han:2014:IBS


Han:2012:PPD

Jinguang Han, Willy Susilo, Yi Mu, and Jun Yan.

Heather:2014:CPE


Shi:2015:CTS


Hamdy:2011:HPB


Henson:2013:MES


Hu:2010:TTW


Huang:2015:PAP

224

Herbert:2012:SMP

Hald:2015:RRA

Hulsing:2013:WOS

Hurlburt:2016:MBO

Harvey:2017:FPM

Han:2012:MIA
Hwang:2011:NIB


He:2016:STI


Heng:2010:CNS


Huang:2011:GFT


Hsu:2014:VWR

REFERENCES


He:2015:IEI


Islam:2011:MES


IBM:2013:DMP


IBM:2013:IPC


Irshad:2017:CPP

[IC17] Azeem Irshad and Shehzad Ashraf Chaudhry.


Islam:2011:MD


Islam:2015:LFP


Iyengar:2016:SPS


Imai:2015:IRR


Ioannou:2014:PKC


I:2017:ETB

REFERENCES


IOM12

IS12

Ishai:2014:PCP

Jacobs:2016:STB

Jie:2010:AAI
Wei Jie, Junaid Arshad, and Pascal Ekin. Authentication and authorization infrastructure for Grids —

Jie:2011:RGA


Jas:2011:RGA

Prins:2011:DCA


Jb11

Jho:2016:SSE


Jas:2011:RGA


Jas:2011:RGA

Chang:2012:TRR


Jas:2011:RGA

Jogenfors:2015:HBT


REFERENCES

www.sciencedirect.com/
science/article/pii/S0020019015001908

Jiang:2017:BMA
[JKHeY12]


Jain:2010:QP
[JJUW10]


Jawad:2013:GAD
[JK13]


Jun:2012:IIR


Jiang:2016:PPT
[JKL+16]


Jovanovic:2012:FAL

Josefsson:2016:ECD


Jeong:2012:IKP


Jajoedia:2012:RET


Jia:2012:PKD


Jiang:2016:OOC


R. Amzi Jeffs and Mike Rosulek. Characterizing

**Juels:2014:HEE**


**Jevdjic:2017:ASC**


**Jain:2016:APQ**


**Judit Mayer:2017:BCI**


**Jiang:2018:CPA**


Poul-Henning Kamp. More encryption means less privacy. *Communications of
REFERENCES


Karakoc:2015:AKA


Kumari:2017:DSU


Keblusek:2015:BRK


Kemshall:2011:WMT


Kleinjung:2010:FBR

Thorsten Kleinjung, Kazumaro Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA modulus. Report 1.4, EPFL IC LACAL [and others], Station 14, CH-1015 Lausanne, Switzerland [and others], February 18, 2010. URL https:/
Kikuchi:2012:SSN

Kramer:2010:FDC

Kim:2012:SLT

Khedr:2016:SSH

Kwon:2010:SEB

Koo:2018:PPD
References

Khazaei:2010:NBS

Kastner:2010:AOT

Kim:2014:MBM

Khalil-Hani:2013:BEB

Kim:2016:EPE

Kai:2011:CIS
REFERENCES

Kia:2011:TCC

Kim:2011:LBA

Kim:2015:CEH

Kim:2016:MAS

Khan:2016:BSW

Konstantinou:2010:RCI
Elisavet Konstantinou and Aristides Kontogeorgis. Ramanujan’s class invariants and their use in elliptic curve cryptography. Computers and

Kawai:2012:SHS


Kawai:2013:SHS


Khalil:2014:CIM


Khan:2015:CMB


Khan:2014:MEK

REFERENCES


Keller:2010:DAS

Khomejani:2010:PCT

Koblitz:2010:BNW

Kifer:2014:PFM

Koblitz:2015:RWE
REFERENCES


REFERENCES

Khovratovich:2010:RCA


Khovratovich:2010:RRA


Kumari:2016:APW


e/article/pii/S1389128616301384.

Koblitz:2010:BRB


Kasper:2012:SCA


Khamsemanan:2016:BBU


Kawachi:2017:GCR

[KOTY17] Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka,

**Kollmitzer:2010:AQC**


**Kang:2012:AKM**


**Kolman:2017:SCG**


**Kumar:2017:TAU**


**Kiltz:2011:EAH**


**Krantz:2012:EAM**


**Kostinger:2012:SBL**


**Krenn:2013:AWI**


**Khan:2010:RCB**

REFERENCES


[KSSY12] Cheonshik Kim, Dongkyoo Shin, Dongil Shin, and Ching-Nung Yang. A $(2,2)$ secret sharing scheme

Klingler:2013:UPT


Kobayashi:2016:ASC


Klisowski:2012:CCP


Kim:2012:SAH


Kawachi:2012:SKE

REFERENCES

Kai:2014:FSD


Kupcu:2013:DTT


Kupcu:2015:OAS


Kuznetsov:2011:APP


Kiljan:2018:ETA


Karpovsky:2014:DSS


Kuo:2016:SDD

Wen-Chung Kuo, Chun-Cheng Wang, and Hong-Ching Hou. Signed digit data hiding scheme. *Infor-
REFERENCES

Koyama:2012:NTD


Kamal:2010:EIN


Lathey:2015:IEE


Lu:2010:MSC


Lackey:2015:UHP


Liang:2015:SEC

Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy


Luo:2012:ESI


Lupu:2012:IBK


Lu:2013:CSA


Liu:2015:IAC


Laxmi:2017:GGS


Liu:2013:IAG

Yining Liu, Chi Cheng, Jianyu Cao, and Tao Jiang. An improved authenticated group key transfer protocol based on secret sharing. *IEEE Transactions on

[LCL+15]


[LCL+17a]


[LCL17b]


[Li:2015:NAC]


[Lee:2017:SUE]


[Liu:2017:GAU]


REFERENCES


Lin:2011:NIB


[LH13] Yi-Pin Liao and Chih-Ming

**Lenstra:2012:RWW**


**Lum:2016:QEM**


**Li:2012:BVS**


**Lin:2011:ICA**


**Li:2010:AIS**

cember 2010. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).


**Li:2017:AMA**


**Lim:2011:NAN**


**Lin:2014:IVW**


**Lindell:2014:TCT**


**Lim:2015:DV**

Lindell:2017:TFC


Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP


Li:2017:MMMA


Li:2016:IRI


Li:2017:SQS


**Li:2012:OEA**


**Laszka:2014:STC**


**Lee:2014:SPB**


**Liu:2017:OOA**


**Li:2012:BIB**


Lee:2010:PMB


Lee:2011:TA


Li:2015:IBE


Li:2015:ANA


Lin:2016:SCU


Li:2012:RIB


Li:2017:CIS

Chengqing Li, Dongdong


REFERENCES

comjnl.oxfordjournals.org/content/59/11/1689.

Lee:2016:AGA


Ling:2012:NCC


Luo:2012:FSI


Lee:2015:SAS


Lu:2012:BBE


Lai:2016:GGB

Chengzhe Lai, Rongxing Lu, Dong Zheng, Hui Li, and Xuemin (Sherman) Shen. GLARM: Group-based lightweight authentication scheme for resource-constrained ma-
REFERENCES


Lambert-Mogiliansky:2012:EII


Li:2011:NRA

Guangsong Li, Jianfeng Ma, Qi Jiang, and Xi Chen.

Le:2016:ADS


Lai:2017:FPP


Liu:2014:SCS


Lv:2013:NTP


Lv:2013:NTP

Lukasiewycz:2016:SAO


Lv:2013:NTP

Li:2018:TF


Li:2018:TF

Li:2013:ESC


Li:2011:CIB

Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, and Cheng-Lian Liu. Cryptanalysis and improvement


**Low:2012:BRB**


**Lin:2011:CRN**


**Ling:2012:SHS**


**Lima:2010:PKE**


**Lian:2015:GRG**


**Liu:2017:HPI**


Lampe:2012:ATS


Liu:2015:GTB


Liu:2016:PPO


Libert:2010:KES


Lubicz:2015:GMA


REFERENCES


REFERENCES


(Liu:2015:IMB) Chao-Liang Liu, Cheng-Jung Tsai, Ting-Yi Chang, Wang-Jui Tsai, and Po-Kai Zhong. Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on

Liu:2015:MSG


Liu:2015:MSG

Lysyanskaya:2010:AEC


Lysyanskaya:2010:AEC

Lin:2011:CNS


Li:2015:FSC

Lao:2016:BFD


Lao:2016:BFD

Lin:2011:CNS

REFERENCES

Li:2016:LRC

Ludge:2012:NLD

Lucchese:2010:RPT

Lafitte:2011:CBF

Liu:2010:CIE
REFERENCES


[LW13b] Dongxi Liu and Shenlu Wang. Triple-image en-

Lui:2013:CBS


Lui:2016:PAB


Liu:2014:DAF


Liu:2017:EEC


Liu:2011:SBA


Liu:2012:HOM

Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic. The higher-order meet-in-the-middle attack and its application to the Camellia block ci-
Lu:2014:HOM


Liu:2010:NDC


Liu:2010:SET

Feng Liu, ChuanKun Wu, and XiJun Lin. Some extensions on threshold visual cryptography schemes.

Liu:2011:PIA


Liu:2012:MMA

Li:2010:GCP


Lou:2010:NAS


Luo:2012:ICB


Li:2012:IIA


Lin:2010:DSM


Li:2011:NW


[Lim:2016:AKE]

[Lu:2014:DAN]

[Liu:2015:SAA]

[Liao:2012:NSM]

[Liao:2010:MPC]

[Li:2013:SSS]
Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE


[LZJX10] C. H. Li, X. F. Zhang,

Li:2012:ESS


Li:2016:BMA


Maeo:2016:UNC


MacCormick:2012:NAC


Macrakis:2014:PLS


Maffeo:2016:UNC

[Maf16] Steven E. Maffeo. *U.S. Navy codebreakers,* lin-


**Mashhadi:2017:NMS**  

**Matsuda:2014:IBP**  

**Maurer:2012:CCN**  

**Mayron:2015:BAM**  

**Mazurczyk:2013:VSD**  

**Milo:2011:FGB**  
REFERENCES


Mao:2015:PUA

Malone:2013:MOD

Massolino:2015:OSC

Mukhopadhay:2011:PEA

Madanayake:2012:BPS

McGrew:2017:IDH
REFERENCES


[Mathew:2015:NMB] Jimson Mathew, Rajat Subhra Chakraborty, Durga Prasad Sahoo, Yuanfan Yang,


[Maachaoui:2012:MLA][MEFO12] M. Maachaoui, A. Abou El Kalam, C. Fraboul,

**Meiklejohn:2010:BRB**


**Menn:2013:ESC**


**Meshram:2015:EIB**


**Mandal:2016:DIW**


**Moreno:2013:NIP**


**Moufek:2015:MCB**

Hamza Moufek and Kenza Guenda. McEliece cryptosystem based on punctured convolutional codes and the pseudo-random...

**Marmol:2010:TPA**


**Matsuda:2014:CCS**


**Meziani:2012:IPS**


**Miller:2014:ADS**


**Mou:2013:CBC**


**Mohd:2015:SLB**

Bassam J. Mohd, Thaier Hayajneh, and Athanasios V. Vasilakos. A sur-

**Micciancio:2010:FGC**


**Michiels:2010:OWB**


**Michael:2016:RNI**


**Midgley:2010:SEE**


**Martinez-Julia:2012:NIB**


**Martinez-Julia:2013:BSI**

REFERENCES


Moessner:2012:SAS


Muller:2012:HPC


Mozaffari-Kermani:2017:FDA


McGrew:2016:SMH


Malik:2012:AIC

Marconato:2013:VLC


Mancillas-Lopez:2010:RHI


Mendez:2016:PES

REFERENCES

Manzanares-Lopez:2012:ICU


Ma:2017:LBI


Madhusudhan:2012:DIB


Meshram:2013:IBC


Maity:2014:FIR


Mondal:2014:DSM

Subijit Mondal and Subhashis Maitra. Data security-modified AES algorithm and its applica-

**Maity:2017:ODC**


**Mulholland:2017:DCD**


**Moldovyan:2012:BBD**


**Mahmoody:2014:PPK**


**Macedo:2017:SSP**


**Mazumder:2017:PSK**

Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. Probably secure keyed-function based authenticated encryption schemes

**Mazumder:2017:SAE**


**Maity:2013:CRS**


**Matsuo:2012:MAK**


**Meshram:2012:IBC**


**Mukhopadhyay:2014:EMP**

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

Monz:2016:RSS


McKusick:2015:DIF


Minier:2012:RKI


Mizuki:2011:ASN


Maimut:2012:LCR


Minamoto:2014:BDI

Teruya Minamoto and Ryuji Ohura. A blind digital image watermarking method based on

Mone:2013:FPE


Moore:2012:RFF


Moody:2014:DMW


Morad:2012:OEA


Moullick:2015:RDS


Minier:2012:EEC


Meiklejohn:2016:FBC

[MPJ+16] Sarah Meiklejohn, Marijor Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M.

Mundhenk:2017:SAN


Mironov:2012:IDP


Mukhamedev:2010:IEP


Mainut:2014:AET


Marasco:2014:SAS

REFERENCES


REFERENCES


Steven Myers, Mona Sergi, and abhi shelat. Black-
REFERENCES


REFERENCES

Manshaei:2013:GTM

Ma:2015:PKE

Nagy:2010:OTP

Nagy:2010:QCS

Naccache:2012:CST

Naccache:2016:FHE

Naranjo:2012:SAK

**Nunez:2017:PRE**


**Noureddine:2013:AMT**


**Nain:2017:SPE**


**Naskar:2012:FIR**


**Naskar:2013:GTL**

REFERENCES

Naranjo:2013:FDA


Ni:2013:EIB


Narasimhan:2013:HTD


Ngo:2017:CSS


Nedjah:2016:PYP

REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-33065-0_8/.


Nichols:2014:CSS


Nguyen:2011:APB


Nguyen:2012:SOU


Namasudra:2017:NSA


Niu:2015:CRS


Naccache:2010:THI

many / London, UK / etc., 2010. ISBN 3-642-14451-9, 3-642-14452-7. xvi + 407 pp. LCCN ????.


Nguyen:2010:LAS


Noorman:2017:SLC


Nie:2013:CHB

[NXB13] Xuyun Nie, Zhaohu Xu, and Johannes Buchmann.


Natgunanathan:2017:PBM


Newell:2014:NCR

REFERENCES


REFERENCES


Onica:2016:CPP [OFMR16]

Oliynykov:2015:NES [OGK+15]

Ou:2010:CPA [OHJ10]

Ogiela:2018:EBI [OK18]

Oliveira:2012:STA [OKG+12]

Ogiela:2010:UML [OO10]
Marek R. Ogiela and Urszula Ogiela. The use of mathematical linguistic methods in creat-

[Ohtake:2012:AAH]

[Orejel:2014:E]

[Ormand:2016:CPR]

[Ozen:2011:MIS]
Mehmet Özen and Vedat Şiap. The MacWilliams identity for m-spotty weight enumerators of linear codes

**Owczarek:2012:LPL**


**Osborn:2016:SSR**


**Orencik:2016:MKS**


**Okamoto:2012:AAH**


**Otmani:2010:CTM**

Ogiela:2018:VCA

Ohzeki:2012:NWM

Ortiz-Yepes:2014:BSA

Praba:2010:MAC

Pal:2015:SDC

Pal:2016:ACC
Pandey:2014:ACR


Parent:2012:WAI


Park:2012:APO


Pass:2013:USP


Pranata:2013:MDR


Paulson:2010:SDO


Pandit:2012:EFS

Tapas Pandit and Rana Barua. Efficient fully secure attribute-based en-

Park:2014:FRI


Pun:2014:GIT


Paul:2016:TSO


Papadopoulos:2014:LQA


Premnath:2014:EHR

REFERENCES

Poh:2017:SSE


Pang:2014:PPA


Paul:2012:KSS


Pereira:2015:PKE


Pippal:2012:SVU


Pearson:2011:NWC

REFERENCES

Persichetti:2013:SAH

Peterson:2011:SWS

Petrlic:2012:PRE

Pfleeger:2010:CJD

Peinado:2012:CAT

Poppelmann:2012:TEA
REFERENCES


[PHWM10] Jong Hyuk Park, Sajid Hussain, Guilin Wang, and Yi Mu. Special issue of computers and mathematics with applications on Advances in cryptography, security and applications for future com-


[Park:2010:SIC] Jong Hyuk Park, Sajid Hussain, Guilin Wang, and Yi Mu. Special issue of computers and mathematics with applications on Advances in cryptography, security and applications for future com-

Pieprzyk:2010:TCC


Pointcheval:2012:ACE


Premarathne:2015:LDD


Pramila:2018:ICA


Shawn Powers. The open-source classroom: encrypt-

Paar:2010:UCT


Papadopoulos:2010:TRM


Park:2011:ACC


Pereira:2016:SHB


Pendl:2012:ECC


Pyun:2012:IBF

Young June Pyun, Youngehee Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing interactive traffic. Computer Networks (Amster-
REFERENCES

Papadopoulos:2015:PAP

Pandey:2012:PPS

Piret:2012:PBC
Gilles Piret, Thomas Roche, and Claude Carlet. PI-
REFERENCES


**Polyakov:2017:FPR**


**Popa:2012:CPQ**


**Priemuth-Schmid:2012:ASV**


**Permpoonanalarp:2014:FTG**


**Perazzo:2015:DRL**


**Pereira:2013:SLC**

Geovandro C. C. F. Pereira.

Phatak:2013:SIN


Patranabis:2017:PSK


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC

Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia. Signatures of correct computation. *Lecture Notes in Computer Science*, 7785:

**Papakostas:2014:MBL**


**Papamanthou:2016:AHT**


**Pudo:2012:RKA**


**Pei:2013:AR**


**Poller:2012:EIC**


**Peng:2010:IWM**

Hong Peng, Jun Wang, and Weixing Wang. Image watermarking method in mult-

**Pongaliur:2013:SNS**


**Pagnin:2018:HDB**


**Philippaerts:2013:CMC**


**Pei:2015:SWT**


**Papadopoulos:2010:CAR**


**Patsakis:2015:PSM**

Constantinos Patsakis, Athanasios Zigomitros, Achilles Papageorgiou, and Agusti Solanas. Privacy and security for multimedia content shared on
REFERENCES


Qin:2016:VTQ


Qu:2013:DPA


Qiu:2017:PSB


Qin:2017:DIR

Qin:2016:STI


Qian:2014:IAF


Qiang:2016:SCF


Qi:2016:SID


Qi:2016:SPR


Rabin:2010:ACC

Rankin:2010:HLH


Rankin:2014:HEY


Rankin:2016:HSP


Rao:2010:PAA


Rao:2017:SEC


Rauscher:2015:FMT


Ruoti:2015:WJS

Rupp:2015:CTM


Rabbachin:2015:WNI


Radke:2015:CFA


Rao:2017:CFA


Ren:2016:IBE


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


Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague. End-to-end verifiability in voting systems, from theory to practice. IEEE Security & Priva-
Ryan:2015:EEVb


Russo:2015:FPT


Rahulamathavan:2016:UCA


Rodriguez-Vazquez:2012:SCB


Roettger:2012:PKC


Ren:2014:HHM

Rogaway:2012:SCS


Ren:2013:PPK


Ristenpart:2010:WGR

Thomas Ristenpart and Scott Yilek. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In Anony-
mous [Ano10], page ??

Ren:2013:DSE


Rajendran:2015:FAB


Sang:2012:SSF

Sakalli:2014:ACC  

Somanatha:2015:RAK  

Shivani:2016:PVC  

Siad:2016:NFI  

Saarinen:2012:PPK  

Suoran:2012:SAM  
Sanna Suoranta, André


Saleh:2016:PED [SAKM16] Eyad Saleh, Ahmad Alsadeh, Ahmad Kayed, and Christoph


REFERENCES


REFERENCES


**Seberry:2010:CTAb**


**Shen:2012:PAS**


**Saleh:2010:GTF**


Su:2012:II


Shabtai:2010:SAP


Shu:2014:DAS


Sasdrich:2015:ICS


Schneier:2015:SWC


Saxena:2016:AP1

REFERENCES

Sanchez-Garcia:2016:SSA


Sun:2015:FSW


Susilo:2016:EDT


Shankar:2012:BDF


Sipiran:2014:SCA


Shaolan:2011:EDE

REFERENCES

1-61284-289-5. LCCN ?????

Seyedzadeh:2011:IEA

Song:2015:ADT

Shallit:2010:BRB

Shaw:2013:DE

Shen:2014:LES

Shim:2011:SA
REFERENCES


Shparlinski:2010:NWP


Suorananta:2012:ASM


Shyu:2015:VCR


Satir:2012:CBT


Siad:2012:NAP


Simion:2015:RST

Simmonds:2015:DII

Sirer:2016:TPS

Shakeri:2012:RZW

Shin:2017:CGI

Sabri:2011:AFS

Sachnev:2012:IME
Seo:2012:MPM


Scarani:2014:BPQ


Son:2017:NOC


Soupionis:2014:GTA


Sirivianos:2014:LSF


Seo:2015:AEC

REFERENCES


REFERENCES


Sencar:2013:DIF


Smart:2016:CMS


Stanton:2010:FAD


Salmon:2011:PRN

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

Smith:2011:SSX


Smith:2011:RBA

REFERENCES


Reihaneh Safavi-Naini and Shaoquan Jiang. Unconditionally secure conference key distribution: Secu-


[Shiaeles:2015:FII] Stavros N. Shiaeles and Maria Papadaki. FHSD: an improved IP spoof de-


**Shparlinski:2012:CSD**


**Sendrier:2013:HCE**


**Sadhy:2017:PRE**


**Singh:2013:QBF**


**Smith:2011:SMC**

Shrivastava:2012:UIE


Strydis:2013:SAP


Sood:2011:SDI


Spiez:2012:RCT


Sahai:2012:DCC


Schaffer:2012:EI


REFERENCES


REFERENCES

Sun:2016:NEB

Shen:2015:CSC

Song:2016:IAR

Svozil:2014:NCC

Svaba:2010:PK

Shoufan:2010:NCA
REFERENCES

382

Song:2016:IBS


Song:2017:PPF


Sheldon:2012:IWN


Su:2016:PSN


Sahillioğlu:2014:SCM


Savas:2015:GMA


Shao:2015:SAS


Song:2017:SSI


Song:2017:SAM


Seo:2013:PIC


Song:2017:RDP


Shen:2017:RDP


Sui:2014:DAH

[Yan Sui, Xukai Zou, Eliza Y. Du, and Feng Li. Design and analysis


REFERENCES

www.sciencedirect.com/science/article/pii/S1353485817300259


Tewari:2017:CNU


Theofanos:2016:SUE


Tian:2016:IBP


Tian:2015:IBP


Tian:2012:TOE


Thabit:2014:RRW


[Tu:2014:EPB]


[Tani:2012:EQA]


[Tu:2013:PAQ]


[Tariq:2014:SBL]


[Tan:2016:ESE]

REFERENCES


Tang:2012:RSS


Tsai:2013:ZWS


Tetali:2013:MSA


Tsay:2012:VUL


Tsoutsos:2018:EDM


**Tan:2016:BIB**


**Tang:2014:PAB**


**Taylor:2011:CAS**


**Tezcan:2016:IID**


**Tschorsch:2016:BBT**


**Tao:2014:CFS**

Jia Tao, Giora Slutzki, and Vasant Honavar. A concep-

**Toreini:2017:TRP**


**Tang:2011:IDC**


**Tso:2013:SAI**


**Tseng:2012:ERI**


**Tseng:2015:LFI**


**Tsai:2010:RLI**

H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai. Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine. *The
REFERENCES


Tupakula:2015:TES


Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG


Tartary:2011:EIT


Tian:2012:SSB

Huawei Tian, Zheng Wang, Yao Zhao, Rongrong Ni, and Lunming Qin. Spread spectrum-based multi-bit watermarking for free-view video. Lecture Notes in
REFERENCES


REFERENCES


REFERENCES


Visegrady:2014:SCV


VenafiLabs:2014:VLQ


Vetter:2010:ABV


Venkatakrishnan:2017:DRB


Vernize:2015:MNI


Viennot:2014:MSG


REFERENCES


REFERENCES


[WDDW12] Zhuo Wei, Xuhua Ding, Robert Huijie Deng, and Yongdong Wu. No trade-off between confidentiality and performance: An analysis on H.264/SVC par-

www.sciencedirect.com/science/article/pii/S074373151730237X.
REFERENCES

Wang:2013:SES

Wang:2016:SSS

West:2015:EC

Wess:2016:JWM

Wang:2010:DVT

Wang:2010:BRR
Ding Wang, Chun guang Ma, Sen dong Zhao, and Chang li Zhou. Breaking a robust remote user authentication scheme using smart cards. Lecture

[WH17]

Wang:2017:DRM


[WHC+15]

Wei:2012:NCI


[WHJ17]
REFERENCES


Wu:2011:HQI  

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

Wang:2011:RBM  

Wang:2017:CAS  
Wang:2013:HCL


Wei:2015:FST


Wu:2015:TRM


Wang:2017:ABS


Wang:2012:RTC


Wu:2012:PSC


Wang:2017:CES

[WMX+17] Xu An Wang, Jianfeng Ma, Fatos Xhafa, Mingwu Zhang, and Xiaoshuang Luo. Cost-effective secure
REFERENCES


Wang:2016:SEP


Wei:2015:TPE


Wu:2013:FTR


Wu:2016:CBE


Wu:2012:RGB


Tsu-Yang Wu and Yuh-Min Tseng. An ID-based mutual authentication and key exchange protocol for low-power mobile devices. The Computer Journal,
REFERENCES


[Wang:2013:NMC]

[Wu:2016:LTN]

[Wu:2017:SPM]

[Wu:2012:AST]

[Willis:2013:IFI]
Karl D. D. Willis and An-
REFERENCES


Wang:2014:ATF


Wen:2014:MZC


Wang:2011:MMW


Weng:2012:NCC


Werner:2017:CIM

Wang:2011:CIB

[WWYY11]

Wang:2011:CHI

[WWYZ11]

Wang:2016:SHI

Wu:2017:EAK

[WXK+17]
Wang:2017:SRS

Wang:2010:IIB

Weir:2012:AVC

Wang:2014:NAI

Weir:2012:IHV

Wang:2013:NSW
REFERENCES


Xu:2012:APA


Xu:2014:TBH


Xue:2017:CNC


Xie:2012:RAA


Xiong:2012:PPK

Kaiqi Xiong. The per-

**Xu:2017:GKG**


**Xu:2016:CIB**


**Xu:2013:PKE**


**Xue:2013:TCB**


**Xiang:2016:EMP**


[H] Hu Xiong, Zhiguang Qin, and Fagen Li. Cryptanalysis of an identity based signcryption without random oracles. *Fundamenta Informaticae*, 107(1):105–109, January 2011. CODEN FUMAAJ. ISSN
REFERENCES

[0169-2968] Xin:2010:IEB


[XSWC10]

[XW13]

Xiao:2010:TAT


[XTK10]

[XWDN12]

Xiong:2012:CBP


[XW12]

Xie:2012:ORI


[XW13]

Xie:2013:SIP


[XW16]

Xu:2016:CCP

Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. IEEE Trans-


REFERENCES


REFERENCES


Yang:2010:PII


Yang:2011:GSS


Yang:2012:PST

REFERENCES

[424]


Yang:2016:EBB


[428]

Yi:2017:ZCL


[433]

Yao:2015:LAB


[438]

Yuen:2012:IBE

Tsz Hon Yuen, Sherman S. M. Chow, Ye Zhang, and Siu Ming Yiu. Identity-based encryption resilient to continual auxiliary leakage. Lecture Notes in

Yu:2017:PDA


Yasuda:2015:MQC


Ye:2010:ACC


Yamada:2012:PBR


Ye:2014:NIE

Ruisong Ye. A novel image encryption scheme


[YI14] Ying Yang and Ioannis Ivrissimtzis. Mesh discrim
inative features for 3D ste-

ganalysis. ACM Transac-
tions on Multimedia Com-
puting, Communications,
and Applications, 10(3):
CODEN ???. ISSN 1551-
6857 (print), 1551-6865
(electronic).

[YKBS10] Sang-Kyung Yoo, Deniz
Karakoyunlu, Berk Birand,
and Berk Sunar. Improv-
ing the robustness of ring
oscillator TRNGs. ACM
Transactions on Reconfig-
urable Technology and Sys-
tems, 3(2):9:1–9:??, May
2010. CODEN ???. ISSN
1936-7406 (print), 1936-
7414 (electronic).

[YKC+11] Jia Yu, Fanyu Kong,
Xiangguo Cheng, Rong
Hao, and Jianxi Fan.
Forward-secure identity-
based public-key encryp-
tion without random or-
acles. Fundamenta Infor-
maticae, 111(2):241–256,
April 2011. CODEN FU-
MAAJ. ISSN 0169-2968
(print), 1875-8681 (elec-
tronic). See erratum
[YFK+12].

[YKC+12] Jia Yu, Fanyu Kong, Xi-
angguo Cheng, Rong Hao,
and Jianxi Fan. Intrusion-
resilient identity-based sig-
nature: Security defini-
tion and construction. The
Journal of Systems and
Software, 85(2):382–391,
February 2012. CODEN
JSSODM. ISSN 0164-1212
(print), 1873-1228 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S0164121211002342.

[Young:2013:TPC] Maxwell Young, Aniket
Kate, Ian Goldberg, and
Martin Karsten. Towards
practical communication in
Byzantine-resistant DHTs.
IEEE/ACM Transactions
on Networking, 21(1):190–
203, February 2013. CO-
DEN IEANEP. ISSN 1063-
6692 (print), 1558-2566
(electronic).

[Yum:2012:OPE] Dae Hyun Yum, Duk Soo
Kim, Jin Seok Kim, and
Pil Joong Lee. Order-
preserving encryption for
non-uniformly distributed
plaintexts. Lecture Notes
in Computer Science, 7115:
84–97, 2012. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer.com/chapter/
10.1007/978-3-642-27890-
7_7/.

Kunihiro, Ken Naganuma,

**Yum:2011:ACO**


**Yi:2017:ICM**


**Yuen:2013:ELT**


**Yang:2012:WSI**


**You:2012:DDS**

REFERENCES

Engineering, 27(3):??, ???? 2012. CODEN CSSEEI. ISSN 0267-6192.


[Yu:2016:SSD] Yong Yu, Jianbing Ni, Qi Xia, Xiaofen Wang, Haomiao Yang, and Xiaosong Zhang. SDIVIP²: shared data integrity ver-

**Yong:2011:SPP**


**Yoneyama:2012:ORA**


**Yang:2012:EMA**


**Yengisetty:2011:AIV**


**Yi:2016:IPA**

Xun Yi, Fang-Yu Rao,

**Yang:2012:SAK**


**Yang:2015:EPS**


**Yang:2016:ECV**


**Yao:2014:NCR**

REFERENCES


[Yeh:2017:SIB] Lo-Yao Yeh, Woei-Jiunn Tsaur, and Hsin-Han Huang. Secure IoT-based, incentive-aware emergency personnel dispatching scheme with weighted fine-grained...

**Yang:2014:IBI**


**Yang:2011:ACD**


**Yasuda:2012:ASM**


**Yao:2010:IDA**


**Yao:2010:ASP**


**Yan:2017:PIS**

Jianhua Yan, Licheng Wang, Jing Li, Muzi Li,

Yang:2015:RCI


Wang:2011:RDA


Wang:2013:RBC


Yu:2012:NWM


Yang:2010:CRS

Yu:2012:SME


Yu:2016:CDI


YY11


YYO15


Yang:2013:ECS

Xiao yuan Yang, Li qiang Wu, Min qing Zhang, and Xiao-Feng Chen. An efficient CCA-secure cryptosystem over ideal lattices from identity-based


Yang:2014:PST


Zuñiga:2017:GLM


Zhang:2011:TNT


Zhu:2012:JLS


Zhang:2013:RMS


Zhang:2015:PCL

Zongyang Zhang, Sherman


REFERENCES

Zetter:2014:CZD


Zhao:2010:PSA


Zhou:2016:HFD


Gao:2012:DES


Zadeh:2015:ASP


Zhang:2012:LDC

REFERENCES


REFERENCES

Zhou:2015:EPP

Zhang:2016:PPV

Zimand:2010:SEC

Zhang:2011:FBP

Zeng:2014:NFC

Zhou:2012:CBF
Zhou:2015:PPS


Zhao:2012:IAS


Zhang:2012:CCB


Zhu:2017:PSN


Zhang:2015:RBA


**Zhang:2010:ESP**


**Zhang:2010:NSS**


**Zielinska:2014:TS**


**Zhang:2016:CAH**

Leyou Zhang, Yi Mu, and Qing Wu. Com-


Zhao:2012:SSS

Zhou:2017:IBB


Zenger:2016:AKE


Zhang:2015:MAA


Zmudzinski:2012:WEU


Zhao:2012:SSM

Zhang:2012:EHO


Zuo:2018:CSA


Zhang:2014:NCM


Zhu:2015:PPD


Zwattendorfer:2012:CBL


Zhang:2016:EEA

[LZT16] Liping Zhang, Shanyu Tang, and Shaohui Zhu. An energy efficient authenticated key agreement protocol for SIP-based green

Zhou:2016:SRB


Zhang:2015:FAA


Zhang:2014:LFL


Zhang:2011:AGK


Zhou:2018:QT A

References


[ZWTM15] Zhang:2015:FER

[ZXJ+14] Zhang:2013:LPP


Zhang:2018:AKE

Zhang:2018:VPA

Zhang:2016:DEP

Zhou:2017:CLR

Zhou:2017:LRC
Yanwei Zhou and Bo Yang. Leakage-resilient CCA2-secure certificateless public-key encryption scheme without bilinear pairing. *Information Processing...*
REFERENCES


REFERENCES

Zhao:2012:FCS


Zhang:2015:ITS


Zheng:2015:EPT


Zaidan:2017:NDW


Zhang:2017:NLR

2067 (electronic). URL