
Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/
29 April 2019
Version 1.464

Title word cross-reference

(2, 2) [KSSY12, LTC+15b], (K, N)
[Bai10, YC11], (n, t, n) [LHYZ12], (t, n)
[QD16, ZPWY12]. 0 [XHX+17], 1
[XHX+17]. 1, 2, 3 [SMDS11]. 11 [LJ17]. 13
[Bl05]. 2 [DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGL10, WY12]. 22 [MNP12]. 2k
[Sun16]. 3 [AP10, CG12b, DWZZ12,
FWS13, GZHD12, GH11a, KWS+12, LJ17,
LJ15, MKH+12, RS16, SS10b, SS12a, SGS14,
WSSO12, tWmC12, YT11a, YI14, YPRI17].
32 × 32 [SA14]. 3 × 3 [ÁMVZ12]. 4
[COP+14, DWZ12, HLYS14]. $49.00
[Sch15a]. 8 [LPO+17]. $99 [APPVP15]. =
[JUW10]. + [PYH+18]. 2 [YNX+16]. 3
[LHM14]. \( MT \) [HRB13]. \( \alpha \) [TTL10]. c

[KRDH13]. \( d \) [QD16]. \( d \times d \) [KA17]. \( \ell \)
[ZTL15]. \( \mathbf{F}_p + \nu \mathbf{F}_p \) [WGF16]. \( \gamma \) [DWZ12].
GF(2)[x] [SF12]. GF(2\(^m\)) [SKH15]. GF(2\(^n\))
[LBOX12]. \( K \)
[FXP12, FR16, CHX13, ZHT16].
\( L(1/4 + o(1)) \) [Jou13]. \( M \) [MMSD13, ÖS11].
\( \mathbf{F}_{p^{e p s o}} \) [AMORH13]. \( \mathbf{F}_q \) [SS13]. \( \mathcal{N}/\mathcal{P} \) [HN10].
GF(q) [LPdS10]. LWE [BV14]. \( \mu \) [Jia14a]. \( \mathcal{N} \)
[FR16]. \( n \times k(k \geq n/2) \) [MC11]. \( O(d^{13}) \)
[KA17]. \( O(n^2) \) [KS11]. \( P \) [DG17]. ±1
[HZW+14]. \( q \) [GMS11]. \( S \) [LJ15]. \( t \)
[HHM+11, Oba11]. \( w \) [Kre13].

-band [MMSD13]. -Bit [LPO+17]. -boxes
-dimensional [DWZ12, QD16]. -Diversity
[ZTL15]. -Encoded [DG17]. -Encoding
[XHX+17]. -Means [KRDH13]. -Multiple
[LTC+15b]. -NN [ZHT16]. -Party [JR13].
-trimmed [TTL10].

.onion [Boy16].

0.13um [KLM+12].


5G [CML+18, FMA+18]. 5th [BYL10, vDKS11].

6 [Ano17b, Bai12, Mur10]. 65th [Nac12].

72 [HYS18]. 768-bit [KFL+10].

8.8/11.2 [GLIC10]. 802.11 [FLH13, ZBR11]. 802.11s [BOB13]. 802.15.4 [NBZP17]. 802.16e [CL11]. 85 [WZM12a].


accumulator-based [LZY16]. Accumulators [PTT16].

Accuracy [CC14, Sar10a], accurate [HQY16], Achieve [BBC+13, Tan15a], Achieved [YM16, Goo12], Achieving [BN14, KTIU16, LW12, Pan14, PH12b, SL12, TK19]. ACIS [ANO11a]. ACM [ACM10, ACM11, ORM+10]. Acoustic [DLMM+18, GST13]. ACPN [LLG15].


Adam [Bar12]. adapted [IMB17].

Adaptive [CT11a, zGXW12, GLG12, HZW+14, HLAZ15, IAD10, Jin10, KD12a, Lin15, PWLL13, SOL13, CLP+13b, dCCSM+12, dCCSB+16, EEAZ13, FXP12, GKKG11, GLM+16, KS11, LHM14, LW+10, PC14, Sh11, Wan13, WKL11].

Adaptively [HPL14, OT12]. adder [MS13a].

Adding [CFVP16, CSL+14]. Additive [TM18, ZDL12]. Additively [PTK12].

Address [WLY17, PSJ+13]. addresses [AZH11].

Addressing [SVG16, SRB+12].

Adelson [BBB16b].


administration [ZHV14]. Adoption [LKKL13, YWK10b]. Advanced

[Böhl10, CSYY18, DR10, TC10, YWF18, ALL+18, DRF13, GLC10, Kra12, MKR10, NMWM16, SKK10]. Advances

[LLK18, PHWM10, WP15, Abe10, GIL10, LW11a, PJ12, Rab10]. Advantage

[WSSO12].

Adversarial [BAG12, BJ+14].

Adversaries [BC14, XTK10].

Adversary

[Yon12, KS11, LXJ12, ZPY12].

Advertisement [ANO16h, AMHJJ10].

Advertises [AHS13]. AES

[BW16, BBBP13, BKR11, BB10, DGP10, FAA+18, HF14b, LB13, Mar10c, MM14b, PBCC14, SY15a, YWF18]. AES-Like

[BW16]. AET [HTC+15]. Affiliation

[XLM+12, XGLM14, XZW15]. Affiliation-Hiding

[XLM+12, XGLM14, XZW15]. Ane

[AN16h, AMHJJ10]. Ane-transformation-invariant

[GZH12].

Ane-transformation-invariant

[AN17e, BVS+13, BL15, CW12b, CMA14, DZS+18, GDC16, HCTD+12, Sch13, SGL15, SLY+16, WSA15, AAT18, ASBdS16, BBP13, BVIB12, BPR14a, BPR14b, BFK16, BSR+14, BK12b, Bud16, Che15, CG14a, CGCS12, CGH17, DHLAW10, DK17, EWS14, FTV+10, zGXW12, GSC17, HLLG18, JSM18, JHHN12, LGL+12, LLY+12a, LWCJ14, Ma16, MD12b, MNR13, OF11, QRW+18, SEY14, SY15b, SD12, TLL13, WHN+12, Yon12, ZLQ15, ZHS+19]. Age

[Bla12, SR14, Lan17, Sto12]. Aged

[Ree15].

agency [Ald11, ABJ13]. agent

[GPVdBC12]. Aggregate

[CCT+14, PSM17, GLB+18, LLY15, LLY+18, ZQZW10, CLW16]. Aggregated

[LNY15]. Aggregated-Proof [LNY15].

Aggregating [DP12]. Aggregation [BJL16, LHK10, SP15b, ZHW+16, WMY16].

Aging [SKV12]. Agnes [Bur11, Joh15].

Agreement [Chi16, HCL+14, HEC+12, MNS11, TM12, WSS12, XLM+12, XGLM14, XZW15, APK+18, AN15, BGAD12, CSD18, CTL13, DLF+16, GH16, HPC12, HWB12, IS+16, IIV+18, KS11, KIH19, KIP18, KLW+16, KDW+17, LLLS13, LIK+17, NCL13, N11, N14, L5Z15, TLL12, XWK+17, XCL13, XMHD13, XHM14, YZZ+14, ZWQ+11, ZTJ16, ZZC15, OHJ10].

agriculture [APK+18]. Aided

[BGK12, BCGK12, BGB12, GMSV14, Vua10, ABBD13, LLY15, SFG+18, SSA11, WLF17]. AIPISte [AGLW16]. Air

[AUMT16, ZWX+18]. aircraft [XZ18W16].

Airflow [RSCX18]. Airway [RSCX18]. AK
CGH11, FSGW12, GTSS19, HL14, ISC+16, LNK+18b, LHM14, LYL15, LY14, MYYR13, QMC17, VS11, WLS14, YZL+18. ANSI [Ano11b]. answers [Wu16]. anti [QZ14]. anti-forensics [QZ14]. AntiNoise [WXL+17]. Antispoofing [MR14b]. Antoine [AY12]. any [Goo12, LP11]. Apache [Lit14]. API [FLW12]. Append [YNR12b]. Append-Only [YNR12b]. Application [AKP12, AK14, BD15, BRT12, BS12, CCLM13, CCKM16, CCW+10, CSTR16, CLCZ10, CHS15, Kup15, LW11a, LWKP12, MNS11, OO12, SEHK12, SS13, XJW+16, YWK10b, YTS12, ZH15, ZM16, Abe10, BBBP13, BT18, CZ15b, GLIC10, HH15, Jia14b, LGKY10, LWKP14, MSM+18b, NAL17, OTO18, SE18, SGCRM+18, XHH12, YY11, ZWQ+11, ZAC17]. Application-Level [CCW+10]. Application-Specific [BD15]. Applications [AMVZ12, Ana14, BKPV12, Ber18, BKS18, BCG+12b, BJCHA17, BSV12, CLCZ12a, CCLC12b, CPS16, CK18, DK15, FSK10, GKM16, GRL12, HH15, Jia14b, LGKY10, LWKP14, MSM+18b, NAL17, OTO18, SE18, SGCRM+18, XHH12, YY11, ZWQ+11, ZAC17].


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

**Assured** [Tan15a, WMYR16]. **Asymmetric** [HG12, XLM+12, XGLM14, XZLW15, ZZQ+19, ZWQ+11, CSS+13].

**asymmetric-histogram** [CSS+13].

**asymptotic** [DTZZ12, TD14].

**Asymptotically** [LPS12].

**Attack** [Ano15d, BRS17, BMB12, Bro17, Che18, CJP12, DSB15, FXP+17, zGXW12, GV14b, GDC16, HCETPL+12, HLAI15, JH12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LWP12, LWPF12, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNST17, CJP15, DFDR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYH14, LWP14, MBB11, MN12, NZL+15, SB17, SXL16, WYL13].

**attacker** [PLGMCdF18].

**Attackers** [BL15].

**Attacks** [ARP12, Ano17e, BGK12, BFK16, FXP+17, zGXW12, GV14b, GDC16, HCETPL+12, HLAI15, JH12, JKP12, LLSW16, LGL+12, LJ17, LCLW17, LWP12, LWPF12, MS12b, Pud12, SP13, SDM+12, WLC12, XJWW13, Ano17a, Blo15, BNST17, CJP15, DFDR13, FLZ+12, Goo12, KA17, LLY+12a, LC13, LYH14, LWP14, MBB11, MN12, NZL+15, SB17, SXL16, WYL13].

**attribute** [Fel13].

**attestation** [FQZF18].

**Attribute** [EGG+12].

**Authentication** [HM12].

**Authenticated** [Alo12, BCO13, BDMLN16, CCL16, CLY14, CCS14, CRE+12, DS11, EAA12, FVS17, FFL12, GTT11, GZ12, HCL12, HCL12, HCL14, HEC+12, KMY18, LHR10, LY16, LH11b, LCCJ13, LTT10, MR14a, MMY12, MMS17b, MHKS14, MSU13, PTT16, Sar10b, SM11b, Tan11, TW14, XLM+12, XCH+12, XGLM14, XZLW15, YS12, YL16, YTA+16, Yon12, ZPZ+16, ZXH16, AIB+16, CTL13, FA14b, FIO15, GPN+12, GLM+11, HPC12, HWW12, H11, HPY10, ISC+16, KMTG12, LWS10, LHH11, LML+13, NCL13, Nos11, Nos14.
PPTT15, PJ18, SMBA10, TCS14, Tso13, TKHK14, WZM12a, WZM12b, WTT12, XWXC14, XCL13, XWZ+18, YC12, YZZ+14, YZL+18, ZTZ16, ZXWA18, ZG10, ZZC15.

**Authenticating** [BS12, CHX13, GRL12, OKG+12, RGP12, WY12, ZCWS15, Cer18, LGCCGCRP14, PGLL10, ZLDD14].

**Authentication** [ASO14, AAZ+16, ACAT+15, AUMT16, ABB19, BL12, BCE+12, BCM12, BSSV12, Bel18, BKST18, BCD+12, Bis17, BF11, Boy16, BKJP12, BSV12, CGCGPDMG12, CTC+15, CC14, CSH+18, CCW+10, CCF17, CJ13, CD12, CJIP12, CLH13, DL15, DBPS12, DKPW12, DP12, FLH13, FR16, FMTR12, FD11, GHS14, Gl12, GI12, GM14, GU13, GMV17, GCK12, HZC+12, Hs12, HLLC11, Har13, Hay13, HBC13, HM10, HCPBL12, HCTE+12, HKL+12, HXC+11, HLC11, HRK18, IGR+16, JN12, JCM12, Jia17, JAEP10, KP12, KS18, KR+10, KSD+17, KPC+11, KLY+15, KTA12, KGP12, Kims15, KPKS12, KLM+12, K016, KH10, LLC11, LH12, LLG15, LCLL15, LNZ+13, LZCK14, LXNY15, LL+12, MWZ12, MEFO12, MKH+12, MBC15, MRRT17, MRS+17, May15, MLL12, Mor12, MSKRJ17, MPM+17, NR11, NR12, NJL12, NL15, OdH12, OO12, OS+12, PCDG14, PPRT12].

**Authentication** [PDT12, PWVT12, RS11, RWWL14, RSN14, SGG18, Saa12a, SBS+12, Sar12, SGC16, Sch+15b, SKV12, ST14, SM12, SD12, Sh11, SGC14, SSA13, SC12, SZDL14, SHS12, SAA12b, SRK+17, TGC16, TYK+12, TM12, Vet10, WGMdZ12, WHZ12, WZXL12, WgMW12, WZCC18, WSS12, WT10b, Xio12, YTP11, YFT17, ZBR11, ZHW+16, ZLD12, ZLDC15, AMN18, AabT16, ABK13, AAM18, Aia15, AL15, AHM+18, APK+18, Alp18, AIK18, ACF16, AZF+12, ATT+10, AN15, ACM12, BS13a, BDM18, BCM13, BGAD12, BLAN+16, BAL10, BMM12, BVOS15, BT18, BTW15, BM11, CLM+12, CML+18, CLP+13b, CTR12, CJXX19, CSD18, CH10, CCSW11, CHS11, CLH13, Ci15a, Ch13a, CJIP15, Cho14, CL11, DCA12, DSCS12, DLK+16, DMV15, DLN12, DZS+12, DMT12, uHAN+18, EA12, ED19, EA11, FPBG14, FHII10a, FLL+14, FPX12, Far14, FA14a, FHZW12, FQZF18].

**authentication** [FMA+18, GJ13, GMSW14, GDH19, GLPL13, GH16, GAI+18, GCS+12, GLB+18, GTSS19, HU15, HSH11, Ham12, Ham19, HDPC13, HZC+14, HZWW17, HL14, HCM11, HLC16, HCC10, HS11, IMB17, IC17, IG11, IB11, IOV+18, Jac16, JNUH17, JKAU19, Jia16, JKL+16, JMW+16, JAS+11, JXLZ15, KPP16, Kem11, KKG14, KSB+17, KVvE18, Kims11, Kims16, KIH19, KP18, KP17, KLW+16, KDW+17, LLLS13, LLZ+16, LC17, LH11, LT13, LH10c, LMN+18, LMJ11, LXMW12, LNKL13, LXX14, LIK+17, LCM+17, LNK+18a, LWK+18, LNK+18b, LHM14, LH13, Lit14, LLIW11, LTC+15a, LY15, LBR12, LTT10, MM12, MCN+18, MvO11, MMP19, MA17, MMS17c, MK12a, NR17, NACLR12, NCG13, NLYZ12, NB13, OF11, OCG11, OYHS14, PYH+18, PYP10, Par12b, PLGMCdF18, PZBF18, PA10, PAK15, PRN+19, QMC17, QMW17, SPLHCB14, SB17, SGGCR+16, Sar10a, SGJ+18, hSZZ15, SCKH10, SA15, SYW17].

**authentication** [SSS11, SKEG14, SHBC19, Tan12b, Tan15b, TODQ18, TG17, TTL12, Wan13, WW14, WLZ+16, WCFW18, Wat14a, Wat15, WDKV19, WT10a, WKK11, WWX+17, XH12, XWDN12, XCHH14, XMHD13, XH14, YHL16, YHHS16, YWK+10a, YSL+10, YMM13, YD17, ZYL+10, ZQW10, ZLDD14, ZH+17, ZX11, ZLY+19, ZZL+18, OHJ10].

**authentication-chaining** [EA11].

**authenticators** [SY+17].

**authenticity** [SYY17].

**Authority** [LSXY15, ZXLW15, ZQQ15, JB11, ZZ12].
Authorization [CS14, LMGC17, MPM+17, YKK18, AL15, DFJ+17, JAE10, JAS+11].

Authorized [HTC+15, LSLW16].

Authorship [BTW15, BAG12, LCM+17].

Autoblocking [YH16].

Automata [CCD15, Gas13, dRsd1VC12, HBBRNM+16, SS11, WOLSI2]. automata-based [SS11].

Automated [CCD15, Gas13, dRsd1VC12, HBBRNM+16, SS11, WOLSI2]. automated [SS11].

Automaton [YH16].

Automata [CCD15, Gas13, dRsd1VC12, HBBRNM+16, SS11, WOLSI2].

Automated [CCD15, Gas13, dRsd1VC12, HBBRNM+16, SS11, WOLSI2].

Autonomous [BT18].

Auxiliary [DL12, GGHW17, XXZ12, YCZY12].

Auxiliary-Input [XXZ12]. Availability [CK11, ADF12, CFVP16]. Available [Ano16d].

Average [Lim11, YL11].

Avoidance [CFZ+10].

Aware [BCF16, LMHH14, LMS16, QLL17, TODQ18, Wan13, ZFH+18].

Awareness [MSas12, Li10, MSas13].

Axiomatic [AT10].

Azure [Sti19].
Based
[WSSO12, WgMW12, WYW+13, Wan14, WZCC18, yWXY+18, WDC18, WLH15, WCL+18, WT10b, WMS+12, XNG+14, XNRG15, XXZ12, XMLC13, XQL11, Xio12, XGLM14, XWLJ16, XJW+16, XJR+17, XHX+17, YE12, YZLC12, YZX+12, YGL15, YT12, Ye10, Ye14, YH16, YTH17, YYO15, Y+17, YKNS12, YHK+10, YW+10, YKC+11, YFK+12, YCZY12, ZP+15, ZJ11, ZX+11, ZDL12, ZHL+12, ZQQ15, ZMW16, ZXYL16, ZMM17, ZPW16, ZVG16, ZPX+17, ZYM18, ZHL15, AM18, AGLW16, AaBT16, AY14a, AHS14, AAT16, ASO14, AKG13, ASVE13, Ar13, AT1+10, AHL+12, BS15, BDM18, BBP13, BGAD12, BAAS13, BOB13, BWR12, BW13, BWA13, BMM12, BC18, BBB16b, BK12b, CPPT18, CML+18, CFI13, CNY10, CCLL11, CTHP13, CJP12, CJP15, CCG10, CTL13, Cho14, Con12, dCCSM+12, Cra11, CDL18, DSCS12, DZ14].

based [DLN13, Dra16, uHAN+18, EZ15, FH13, Far14, FA14a, FA14b, FIO15, Fay16, FHZW18, FNWL18, Gai13, GJ13, GMOGCC15, GMRT+15, GKCK11, GMMP15, GCAddP11, GMS11, GLL+18, HSH11, HT11, Ham19, HGWY11, HMS13, HZC+14, HZL18, HFI14a, HWDL16, HZW11, HZW18, HBBN+16, HL11, Her14, H015, B113, HL14, HL11, HLC12, HLC16, HYWS11, HYS18, HYF18, HPY10, HKKH13, HCC10, Hwa11, IM18, IM14, ISC+16, IB11, IA15, IOV+18, Jac16, JNUI17, JKAU19, JK13, JLT+12, JZS+10, JMW+16, JSMG18, KPP16, K13, KM10a, KHM13, KKG14, Kim11, KGO10, K11, KSH18, LLY12, LZL+16, Lau12, LCL10, LK14, LH10c, LZJX10, LNM+11, LMJ11, LK12, LXLW12, LKAT12, LHS12, LNK13, LJJ14, LCL+15, LZY+16, LFZ+17, LNK+18a, LWK+18, LCT+14, LFWS15, LLM+19, LPdS10, Lin14a, LLY+12a, LW10, LSQ+11a, LSK+11b, LWK11, LW13b, LZZ+14, LPZJ15, LTC+15a, LYL15, LY15, LJJW+17].
based [LJWY18, LDZW19, LW+10, LL16a, LW13c, LWY12, LY14, MCM+18, MCP15, MJJS12, MJS13, ML16, MM12, MM13, Mes15, MBB11, MO14, MHT+13, MG15, M19, M11, NCL13, NZL+15, PPA18, PYY+18, PLPW13, PTK14, PWW10, PGLL10, PPB16, PLGMD18, PS14, PL16, PKA15, PC14, PPR+12, QZD16, QRW+18, QXY16, QMW17, RD17, RG10, RS15, SPLHC14, SGGR+16, SI12, SYL13, SE14, SE16, SH11, SM14, SR10, hSSZ15, SCKH10, SA16b, SSAF11, SWW+16, SSS11, SKE14, Sun16, SM16, SHBC19, SS11, TPL16, TQL+14, T15, TH16, TTT10, TPK12, TKKH14, VS11, VN17, WWY11, WYY11, WLL11, WLFX17, WXX+17, Wan18, WZG+12, WYLH16, WS14, WS12, WTT12, WOLS12, WCCC18, XHH12, XWW16, XW12, XCL13, XWS17, XCH14, XWW+18, XMHD13, XHM14, YYL+17, yYqWq13, Yan14, YTM+14, YCC16, YXA+18, YCT15, YLS12, YSSH10].
based [YKC+12, YLZ+16, YX+16, YL11, ZKA17, ZLW+12, ZC14, ZT14, ZTS16, ZML17, Z12, ZHI+17, ZL12, ZVH14, ZDW+16, ZLY+19, LZJX10, HZC+14, MM12, PP11, ZBR11, Kat13].

Based-Encryption [ZH15]. Bases
[EVP10, TSH14, FES10]. Basing
[Mate14, MN10]. Basis
[BNA15, ERRMG15, CG12b, Har15, LPP+18, Tam15]. Batch
[ZPX+17, AGHP14, CG10]. batch-based
[CG10]. Batters
[Chi13b]. battles
[Ano15e, Ano16f, Sch15c]. Bay
[Ano10, DDS12]. Bayes
[McG11]. Bayesian
[WY+13, ZL+17]. Be
[DSMM14, Par12a, YM16, AZH11, Ana14, Eve15, Ree15, RK11]. Beat
[LTKP16]. BECAN
[LZ+12]. Becomes
[Bra13]. been
[Ana14]. before
[GST12, Goo12]. Beginning
[Ch16].
Behavior [GSC17]. behavioral [HT11].
Behaviors [GAF+15], Behind [Fre10, Sti19]. Beijing [BYL10, Yan10].
Beissinger [Ayu12], Belief [BT12], Bell [JEA+15, QD16]. Benchmarked [MKAA17]. benchmarking [ZZKA17].
Benefit [HB14]. benefits [Wat14a].
Benford-Style [GHS12, GHS13]. biased [LLP+18]. Biclique [BKR11, KDH13].
Bilinear [ADB11, AK14, MBR15, MBF18, SA14]. Bilinear-Ternary [ADB11].
[MCDB12]. **Block-Wise** [SSA13].
Blockchain [Hur16]. blockcipher [CMMS17]. **Blockciphers** [LST12]. Blocks [JSDK+17, Bra15]. Bloom [ATKH+17].
**Blowfish** [KB10]. BLS [BP18]. BlueKrypt [Gir15]. Boardroom [LHF12]. Bodacious [KM10c].
**Body** [LZCK14, ASO14, CP18, LIK+17, SGJ+18]. body-sensor [ASO14]. bogus [XWDN12].
**Bombe** [Bur11, Car10]. Boneclike [SSA13]. Bonebrake [SS10c]. Bonebrake [TK19]. Book [Ano15b, Ano17b, Ayu12, Bar12, Dew11, Fu10, JDB10, Kob15, Kob10, Low12, Mei10, Mur12, Sch15a, Sha10, SR14, Ter11, To12].
**Boolean** [ACZ16, AS17, CW14b, DQFL12, Mur10, Sch15a, Sha10, SR14, Ter11, To12].
**Boolean-based** [CW14a, YCC16].
**Bootstrapping** [BGV14, GM14]. **Border** [LGM+16, ZTSR12]. **BotMosaic** [HB13].
**Botnet** [NS15]. botnets [HB13]. **Bottom** [Sm11b]. Bound [LST12, TK19]. **Bounded** [GW12, GJO+13, PSM17, QZ18, S12a, ZYT13, IM14]. bounding [PYH+18].
**Bounds** [Jia17, LJ15, SNN11, S110b, Sha10].
**Bouzefrane** [Ano15b]. Box [BW16, BCGN16, BR14, CPS16, HHPI17, KMO14, Mic10b, Rja12, SS10b, Kos16, LR13, MS13, RMP10, SFGFRM+18, ZZ12, ZSW+18a]. Boxes [NN12, LJ15, S111].
**BRAMs** [DG10, Branch [MPG16]. Branchless [RBS+17]. Brave **[KM10c].**
**Break** [SD12, JB11]. Break [Ayu12, Win17]. **Breakers** [St15, Mun17].
**Breaking** [AP13, CN12, Che18, Cop10a, KS11, TPL16, WGMdZ12, Ant14, Bri11].
**Breaks** [Ano17e]. breakthrough [Goo12]. breath [LSR13]. Breathing [CSH+18].
**Breathing-Based** [CSH+18]. **Bregman** [CCZC13]. **Bribeny** [CW12b]. Bridging [LRVW14, TMGP13]. **Briggs** [Bat12].
**Bring** [Zha15a]. Bringing [Ano15c, OYHSB14]. Britain [Ald11].
**British** [And13]. Broadcast [BS14, GMV17, HMR14, KH10, LGM17, LMG+18, PSM17, PPS12a, WQZ+16, XJW+16, Yan14, ZHW15, CPPT18, DNL13, WWYY11, XWDN12, YMM13, ZWQ+11, ZZ12, Zhu13]. Broadcasting [OO12, MK11, OCGD11, YY11]. broke [Bat10, Hea15]. Broken [MDAB10]. **Broker** [TK14]. **Broker-Less** [TK14]. **browser** [GJ+12]. browsers [R15]. **Bruce** [Sev16].
Brute [CJP12, JR14, CJP15]. Brute-Force [JR14, CJP12, CJP15]. **BRW** [CMLRHS13].
**BTC** [CLF11]. **BTC-compressed** [CLF11].
Buchwald [AB13]. **Bucket** [KKK10].
**Buyer-Friendly** [Fra16]. **BYOE** [Tan17a]. byte [Hof15, Hof16]. bytes [PDNH15, QZZ18, SS12a, ZYT13, IM14].
Byzantine [KS11, LKA19, YKGK13]. Byzantine-resistant [YKGK13].
**C** [AD12, ACZ16, Cra14, DGINJ14, C1G2 [LK12a]. CA [ACM11, DUN12b, K11, Lin14b, Pie10, Rab10]. **CABA** [MSK17].
**CABE** [XHH+17]. **Cache** [AB15, ADR18, DKMR15, HLAZ15, SY15a, DFL12, DK17].
**CacheAudit** [DKMR15]. **Caches** [LLG16, CDPAL16, DL1+12]. Caching [A18R, HLAZ15]. **cackled** [Bat12]. **CAD** [PGL10]. **Caernarvon** [KMP+11].
**Calculus** [MR10, Jou13]. **Calibrated** [LC15]. **California** [Ano10, IEE11b]. Call [Ano16a, Ano16b, Ano16d, CS14, KRM+10].
**Call-Back** [KRM+10]. **Calls** [Mur16]. cam [PKS18]. Cambridge [ACM10, PJ12].
Camellia [Bla15, LWKP12, LWKF12, LWKP14, SEHK12]. Camellia-192 [Bla15].
cameras [MKH+12]. Can [Ako12, AZH11, Bar15, DSN14, Y16, R11, R15, S10, GMMV17, LMS16].
Canada [JY14, MV12]. Cancellation [DLMM+18]. **Candidate** [GGH+16a].
candidates [ABM+12]. canonical [Bul10a].
Chaotic [BGGH11, IAD10, Ye10, GCH15, ISC16, KLW16, LWK18, LW10, NES14, WGZ12, ZT14]. Chapman [Fu10]. Character [SI12b]. Characteristic [BGJT14, SR10, BGJT13, Jou13].

Characterization [ALR13, BS13b, DPCM16, YZLC12, PLGMCdF18]. Characterizing [Ash14, JR13, MPJ16].


Choquet [SH11, SM11, SNM14]. Chosen [FSGW12, zGXW12, HLW12, HPY10, LCT14, LJC12a, LLML12, MH14, RS10, WWHL12, GLM16, GH12, LJC14].

Chosen-Ciphertext [RS10, FSGW12, LCT14, GH12, LJC14].

Church [ABJ13]. CHURNs [RBNB15]. Cipher [BW16, BFMT16, BCG12b, CMLS15, CGCS12, DM18, DG12, DWW12, Fis15, FXP17, GLLSN12, GCS13, HZ11, Hey17, IOM12, JKP12, KR11, KWS12, LPS12, LW12, LJC17, LWKP12, LWPF12, MRT12, MHC12, MS12b, OGG15, PH12a, PRC12, WSSO12, WHN12, YLC17, ZAG19, AMS10, BNY14, CR12, FVK17, HKT11, Hol12, Jeo13, KDH15, Lew10, LC13, LYHH14, LWKP14, MNP12, PL16, Rec15, RS14, Sar11, WYL14, WWBC14, ZSS18a, LGL12].

Ciphers [ABS12, BMS12, BSS13, BKLS12, Bru12, CWP12, DGI12, DJG15, EGG12, EKP13, GT12, GST12, GNL12, Has16, Hey17, IS12, KE19, KPC16, Kla10, LCL17, LLML12, LJ16, MD1b2, NN12, Pud12, Sasi12, SEHK12, Vua10, WH18, WW12, Xie12, ZH15, ZSW12, Zha12, Bay10, Bia12, Bior10, Die12, KM10a, LWK11, MRT10, MH15, MH18, QQGL13, SKK10, TQL14, WB12].

Ciphertext [BDPS12, CWWL12, zGXW12, HLW12, JMG16, JSMG18, KA17, LJC12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RW12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWJ16, ZHW15, CPPT18, FSGW12, GLM16, GH12, HPY10, HJK13, KTT12, LCT14, LFWS15, LJC14, LDZW19, QRW18, RD17, SGM16, WLFX17, XWS17, LAL15, LHL15].

Ciphertext-only [KA17]. Ciphertext-Policy [Rao17, XMLC13, XWJ16, ZHW15, JSMG18, LFWS15, LJC14, LDZW19, QRW18, RD17, SGM16, WLFX17, XWS17, LAL15, LHL15].

Ciphertexts [LLPY19, Sta12, WQZ16, AHL12, LCT14, NMP13, WXLY16]. Circle [SC10]. Circuit [Kar12, MTY11, XWS17, XWJ16, Lau12, MS13a]. Circuit-Size [MY11]. Circuits [AIK14, AS17, BR14, GGH16a, GH11a, GVW15, MFB18, SS10b, SS12a].


Classification [HPC10, HS18, KA1K17, SGP12, LZ17, LHL18]. Classifiers [KGV16, LCM17]. classroom [Pow14].

Claudius [Hol12]. CLEFIA [LWZ12, TSSL11, TS16a, WB12]. CLEFIA-128 [TSSL11]. CLEFIA-type [WB12]. Client
[ASM12, CTC+15, FD11, RAZS15, Vle12, FA14a, FA14b, hSZZ15, WT10a].

Client-Based [ASM12], Client-Centric [Vle12], client-server [FA14b, hSZZ15].

Clients [Chi16, LLPY19, LH13].

cooking [NZL+15]. Close [Wal18]. Cloud [AJA16, BÇQ+13, BCK17, CCL+14, CWL16, CDFZ16, CCT+14, CLW16, DXA14, FCM14, FPY15, JLS12, KMSMY15, KS18, KKA15, Küp15, LA15, LLPY19, LYZ+13, LGR14, LLC+15, LNYX15, MLO17, PSH17, Pet12, RSGG15, SGG18, SGJ+18, SHH17, SRAA17, TV15, Vle12, WLFX17, WWW17, XKG15, XWSW16, XMLC13, XWLJ16, XJW+16, YDH+16, YHL16, YXA+16, YMC+17, ZZQ+19, ZDL12, ZLDC15, ZVG16, ZLW+17, ZZZ+18, AAT16, AKKY17, AZP14, ASO14, AAZ+16, AAK+17, ADH17, ALL+18, BG14, BK12b, CFVP16, CSH16, CZ15b, CDL18, FH13, FNWL18, GLB+18, GZS+18, HSM13, HZW18, HY18, IMB17, JEO13, KKA14, KKM+13, KKM+14, KBB+17, LXX+14, LZY+16, LAL+15, LW13a, LYL15, LHL15, LCY+16, LCZ71, MLM16, NR17, Nam19, NB13, PPA18, PP11, RAO17, SY+17, SAR19b, SLM10, SKB+17, SWW+16, SWW+17, TLMM13, WL12, WSC14, WMX+17, WLS14, WCCH18, WL19, XXX15, WXY+18, YYS+16, YZC17].

cloud [YHHM18, YQOL17, YWT+12, ZYV+17, ZVH14, ZD+16, ZWS+18, ZFH+18, ZLY+19, ZHT16].

Cloud-aided [SGJ+18, WLFX17].

Cloud-Based [KKA15].

Cloud-Manager-Based [KKA15].

Cloud-of-Clouds [BCQ+13].

Cloudier [CFE16].

Clouds [BCQ+13, RSN14, HFT16, IC17, JKL+16, LFWS15, LL16a, WU17, YNX+16].

Clustered [DS11, KS18].

Clustering [KRDH13, VSV15].

CMAC [SKK10].

Co [MBR15, MRL+18].

Co-Design [MRL+18].

Co-Processor [MBR15].

cocktail [OHJ10].

Code [AD12, Bud16, CCL+13, Cop10a, Fox13, HG12, KSSY12, Mun17, PYM+13, SS13, Sen17, Sti15, War11, ABBD13, Ant14, Bha16, Bri11, CCLL11, GIJ+12, MCP15, McG11, McK12, Moo14, OF11, PA10, Wes15].

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

Code-breaking [Ant14, Bri11].

Code-cracking [War11].

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

Codebreaking [Bai12, Cop10b, McK10, McK11].

Codes [Ano19, BBC+13, Bay10, PKST18, DBPS12, DPW18, FMV14, GMS15, Gri15, HC17, KW14, MBR15, OTD10, SEY14, ST14, TLW12, WGF16, WSS12, Xie12, YTP15, Yek10, ATI+10, Bul10a, C475a, Chi13a, Fag17, Hea15, LTT10, MG15, OŠ11, Tan15b, YSIL14, Ayu12, Low12].

Codevelopment [DF16].

Coding [Che11, CWL16, CJ13, CG14a, DG17, He12, LCLL15, Per13, AZF+12, Bul10b, CJX19, DTZZ12, JYS+10, KM11, LLP+18, NDNR13, OF11, Tan15b, YTM+14, Kim15].

CoDiP2P [NCCG13].

Codon [HEK18].

Coefficients [BDB14].

Coercion [CW12b].

Cognitive [PP11, Kim11, OK18, RPG12].

Cog [Ara13].

Coin [ALR13, CLP13a, DSSM14, Mat14, BB14, Wag16].

Coins [Fok12].

CoinTerra [BH15].

COIP [BCF16].

COIP-Continuous [BCF16].

Colbert [Dew11].

Collaboration [CRE+12, PPCP14, HYS18].

Collaboration-Preserving [CRE+12].

Collaborative [LT14b, HB13].

Collect [Sch15c].

Collision [BK12a, ZL12, AKY13, SKP15, SBK+17].

Collision-based [ZL12].

Collision-Resistant [BK12a].

Collusion [MMSD13, RVH+16, FLZ+12, GMRT+15].

Collusion-resistant [GMRT+15].

Collusions [GVW12].

Color
BK12b, LR15, SSAF11, TLMM13].

Compute [Vai12]. Computer [BGK12, BCGK12, BGB12, Bul10b, DF16, Gas13, IEE10, IEE11b, IEE13, LL15, Orm16, Ter11, Vua10, ABBD13, DK12, FGPGP14, PHWM10, Sta11b]. Computer-Aided [BGK12, BCGK12, BGB12, ABBD13].

computers [Cop10b, LCKB12, Mac12, MvO11, PHWM10]. Computing [Aeon10, ACM11, Aja16, Aoo17c, BGC12b, Cer14, CGB10, DXA14, EAA12, FES10, Gao10, KMS15, KPI17, LCK11, LTI14a, LYZ+13, LLC+15, LLGJ16, LNYX15, MLO17, OS16, PAF18, Pet12, SJWH+17, SLIM10, Vai11, Vle12, XMCL13, XWJ16, YE12, YHL16, ZLDC15, AnBT16, Aa+16, An13, Cz15b, CSTR16, DKL+16, DWZ12, HSM13, HY18, Jeo13, JSMG18, KKA14, KKM+13, KKM+14, KSB+17, KH18, LXX+14, LYL15, LHL15, MS12a, NAM17, NCCG13, PPA18, PP11, PAK15, QZJD16, QW+18, Rao17, Tan12b, WSC14, Wan18, WDKV19, WLS14, WL19, XXX15, XWY+18, YHIM18, YWK+10a, YQOL17, YY11, ZWS+18, ZLY+19, ZSW+18b, YX+18].

Conceal [EEAZ13]. Concept [TM15]. Conceptual [PMZ12, SPM+13, TSH14]. Concrete [BS14]. Concurrent [CLP13a, FCM14, GJO+13, MRR13, OOR+14, AKG13, SRB+12, XLWZ16].

Condition [TD14]. Conditional [HBCC13, KPW13, LLG15, LSLW15, MLO17, JXW+16, FSFW11, FSFW12, HWD16, HY18, IOV+18, LCT+14, PZBF18, SKB+17, Tan12b]. Conditionally [ZJ14]. Conditions [Aeon17d]. Conference [BC11, CGB+10, CHe11, Cra12, Dan12, Dun12b, FMB12, GLIC10, IEE11a, JY14, LCK11, LW11a, LTW11, Lin14b, PJ12, SNJ11, Sah13, Yan10, AB10a, Abe10, BY10, BL10, GII10, GII10, HWG10, Kia11, LHI10a, Pie10, Rab10, vDKS11]. Confidential [HS11, AZPC14]. Confidentiality [BFK+10, HLLC11, OFMR16, SZQ+17, WDDW12, Bia12, CHX13, ZHT16].

Confidentiality-Preserving [OFMR16, SZQ+17]. Configurable [CVG+13]. Configuration [Bi17, SHB19].


Consecutive [Tan12a]. Consensus [ABCL17, JSK+17, LLKA19].

Consequences [Ess17]. Consideration [CJP12, CJP15, KM10b]. Considerations [KD12b]. considering [MLMSM12]. Consistency [BCK17, SES+16].

Consolidated [KKA14]. Constant [App14, AEHS15, CWL12, KOTY17, KHP16, KMO14, LP11, Pan14, ZM16, AHI+12, DWZ12, LCT+14, SGM16].

Constant-Round [KOTY17, KMO14, LP11]. Constant-Size [AEHS15, AHI+12, LCT+14, SGM16].

constants [DWZ12]. Constrained [BS15, CSH+18, EAA12, JMG+16, YN12a, Yon12, DMV15, KAS15, LZZ+16, LCL+17a].

Constraints [CCM16]. Construct [SGY11, WT13]. Constructed [Ye10, ZH15]. Constructing [CDS14, ZSW+12, HRV10].

Construction [BWLA16, DF11, EM12, FZT14, GWWC15, HHP17, KMO14, MSas12, Rog16, Sari10b, ST14, WZ15, WCL+18, WMS+12, XHZ+17, LFZ+17, MS13, SA14, YWL+17, YT11b, YKC+12, ZCLL14].

Constructions [BCF+14, DQFL12, HLI10b, KOTY17, SNJ11, SES+16, CZZ15a, CGKO11, NAL17, Zim10].

Constructive [Mau12, WB12]. constructs [BP10]. Containing [XWDN12].

contemporaries [LCKB12]. Contemporary [Opp11]. Content
[ADR18, BCP14a, MHT+13, PMZ13, PZPS15, WHZ12, WZXL12, YT12, ZXZ+11, GPN+12]. Content-based [MHT+13]. 


Continual [BKKV+10, XZY+12, YZ12, YCYZ12]. Continual-Leakage [YZ12]. Continually [DLW11]. Continuous [ACAT+15, BCF16, DHLAW10, uHAN+18, FMNV14, MSKRJ17, PYP10, Sch15b, Yam12, ZY17a, ZYM18, BTW15, PLGMD18].

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

Contributory [WQZ+16]. Control [ATS15, BFK+10, DLZ+16b, HHS+15, LGM+16, MM17, MK12b, NA10b, QZL+16a, RSN14, SGC14, TBCB15, XMLC13, YTH17, ACK+10, AMHJ10, CLH+16, CO11, Cra11, FNWL18, FS18, GHD19, IAS+11, LCL+17a, LCL+15, N/Z10, QCX18, Sch15c, SA15, Tan12b, Wan18, XHH12, ZML17, ZVH14, ZWS+18, ZH+18, ZZL+18].

Controllable [FH13, ZLDC15, ZHT16]. Controlled [FMTR12, WP17, Har16]. Controller [GMV17]. Controllers [AMH+16].

controls [CGHI1]. controversy [McG11].

conundrum [Eve12]. Conversations [WBC+10]. Converse [KPK12].

Conversion [BJ10]. Convertible [CLL16, LH11b, HL1, LHH11, XWXC14].

Convolution [DWZ18]. convolution [MG15]. cookies [DCAT12]. Cooperative [LLZ+12, SJW+17, ZLDC15, WQZ+13].

Coordinate [YYK18]. Coppersmith [Dra16]. coprocessor [ABC+12, BGG+13, IBM13b].

coprocessors [GCVR17]. Copy [YT12, MHT+13]. Copyright [SJ12, GJ13]. Core [LB13, YWF18, YS15, RSI7, HLYS14].


Correction [LSC+15, yWXY+18, Chl13a, Sun16]. Correctness [YGS+17, WS13]. Correlated [RS10, Jia16, ZPZ+16]. Correlation [BW12, FAA+18, LD13, SMD+12, WWB14, XHH12, YCL17]. correlations [Sar14]. Correspondence [SY14].


Cost [ABC+17, AMH+16, CML15, CJP12, GJ12, HLT+15, Man13, NVM+17, WMX+17, CZ14, CJP15, LEW19, Sar10a, YL11].

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


Counter [ARP12, Fay16].

Counterexample [KPK12]. Counterfeit [YFT17]. Counterfeiting [Ano16e].

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

counting [LLY+12a]. Coupling [SMS14]. cover [UUN13]. Covert [EPAG16, JRT+16, NSA15, LT13, LyWS10, SRB+12].

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

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

CPS [FQZF18]. CPU [ZBP18]. Crack [Fox13]. cracked [Ano13b, Mcg11, McK12, Mool14].

Cracking [Gri15, GAS+16, War11].


Crisis [Odh12]. Criteria [PYS18, ZZKA17].

Criteria-Based [PYS18]. crittografia [Sac14]. CRM [LHM+15]. Cropping [SR12b].

Cross [AKK+17, CLY14, DSB15, LHM+15, MV16a, YGFL15, ZY18].

Correcting [ATT+10, LTT10, MCP15]. Correction [LSC+15, yWXY+18, Chl13a, Sun16].

Correctness [YGS+17, WS13]. Correlated [RS10, Jia16, ZPZ+16]. Correlation [BW12, FAA+18, LD13, SMD+12, WWB14, XHH12, YCL17]. correlations [Sar14]. Correspondence [SY14].

counting [LLY+12a]. Coupling [SMS14]. cover [UUN13]. Covert [EPAG16, JRT+16, NSA15, LT13, LyWS10, SRB+12].

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

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

CPS [FQZF18]. CPU [ZBP18]. Crack [Fox13]. cracked [Ano13b, Mcg11, McK12, Mool14].

Cracking [Gri15, GAS+16, War11].


Crisis [Odh12]. Criteria [PYS18, ZZKA17].

Criteria-Based [PYS18]. crittografia [Sac14]. CRM [LHM+15]. Cropping [SR12b].

Cross [AKK+17, CLY14, DSB15, LHM+15, MV16a, YGFL15, ZY18],
ZXH16, ZTSR12, SS17, der10].

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

Cross-Layer [LHM+15, ZXH16].
cross-matching [SS17]. Cross-Site [DSB15]. Crossword [Mar10a]. Cryptis [GSC17]. Cryptanalysis [BW12, Bor10, CWPI12, CGCS12, DGL12, DJG+15, Far14, GST13, Gor10, Him10, IOM12, Jeo13, Kha10, KN10, KWS+12, LHIb, LNM+11, LJF16, LJ16, MWZ12, NXB13, OTD10, PSOMPL13, SPLHCB14, SM10a, SM10b, TY16a, TG17, Vua10, Wag10, WWYZ11, WWY11, WSSO12, WY14, XQL11, YCL17, YMWS11, AP11, BMB16, BKR11, Bul10a, Bul10b, Con12, Eis10, FVK17, Her10, KDH13, LLLK10, LFW+16, Nov10, RITF+11, SDM10, SDM14, Sun11, SvT10, Tam15, TSS11, WYL14, WWBC14, Ay12].

Cryptanalyzing [LLL17a, ZLW+12].

CryptDB [PRZB12]. Cryptic [Mar10a].

Crypto [Goo12, Pfl10, Rab10, SCPSN10a, SCPSN10b, SMK18, WL11, BSR+14, BGG+13].

Cryptocurrencies [JSK+17]. Cryptography

Cryptography [ACZ16, Ano15d, Ano16a, Ano16b, Ano19, App14, AAB17, ACM+17, ARM15, Bar12, BGRK12, Bar15, BRT12, BC110, BKKV10, BJ10, Buc10, BL17, BCF+14, CR11, CT18, CFJH14, Cas10, CGMO14, Che17, CST+17, CDFZ16, CS12, Cri12, DDI12, Dui12, DUK15, DX14, DP17, DHLH10, DF16, DK15, DR11, Eis10, FPH10, FSK10, Fd18, FBM12, Fre10, GO17, G17, GBT12, GLW12, Ham17, Hes12, HGI2, HKR+18, J12T12a, KM10c, KP10, KAK18, LSL12a, Lin17, LW110b, LGWY12, LMH14, LGH+17, LWHS17, LPO+17, MO12, MSI10, Maur12, Men13a, MR14c, Mic10b, M18ST, MV12, MMB17, NNA10, NS12, Orm16, P10Pa, PH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16, Sen10, SS13, Sen17, SK12b, SA16a, Sim15a, SGS14].

Cryptography [Sma16, Sta11a, Ste15a, VS16, WWL+14, WY12, Wes16, Yan12, Yan11, YTS12, YL17, ZZCJ14, ZÁC17, vTJ11, AMN18, AMORH13, AEH17, AAT16, AA14, ABBD13, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Bl612, BSR+14, BSW12, BBB16b, CFR11, Cha13b, CQX18,
Cho14, CSTR16, Con12, CDSLY14, DDD14, Dav11, DD13, Dur15, Far14, GCVR17, Har15, HH15, HZWW17, Ho16, IM14, JLT+12, JY14, JW14, KK10, KGO10, Kre13, KSH18, Lan11, LLLK10, Lin14b, LWL10a, Lüd12, LY14, MCN+18, MS13b, MD12a, MCP15, Mic10a, NLYZ12, Nov10, OK18, OTO18, PHW10, PP11, RY10, Sac14, Sah13, SK14, SSAF11, Sta1b, Sti11, Svo14, UK18, VDO14, VN17, WHJ17, WYK12, YT11a, YSC16, YXA+18, YDH+15, YR11, ZXW+18, vDKS11, Che11, LZJX10.

Cryptography [Nac12, Cou12, Ful10, Gas13, Low12, Mei10, Mur10, Ter11].

cryptography-based [BOB13].

Cryptography-Related [Cil11].

Cryptol [Lau12].

Cryptology [BC11, Bro11, Dun12b, LW11a, PSM17, Pie10, Rab10, HWG10, LTW11, Kob10].

Cryptomania [Gen13]. Cryptoprocessor [GV14b, SWM+10].

Cryptosystem [CCT+14, LH10b, SWM+10, BS15, Chi13a, Gal13, GV14a, GLB+18, IB11, MM13, MG15, NZM10, Sv1T0, yYqWqZC13, YY11].

Cryptosystems [AD11, OTD10, PSM17, BNST17, FWS13, SA16b].

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

Cryptology [BC11, Bro11, Dun12b, LW11a, PSM17, BNST17, FWS13, SA16b].

CT [Dun12b, Ki11, Pie10].

CT-RSA [Dun12b, Ki11, Pie10].

cube [MS12b].

Cubic [RW12, VM14].

Cuckoo [BHKN13].

Cuda [DLV16]. cultural [Mid10].

Culture [Bla12, SR14].

Currencies [TS16b].

Current [DP17, GCK12, FPBG14].

Curse [GG11, HB14].

curvature-feature [GG13].

Curved [SG15]. Curved [BC18].

Customization [OdH12].

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

Cyber-Espionage [LJS+14].

cyber-physical [GHD19, HZWW18, QMC17].

Cybernetica [Ano17c].

Cybersecurity [DF16, Hel17, Lan17, LRVW14].

Cycle [HG12, KU12, MKN13].

Cycle-Based [MKN13].

Cycles [WBA17, CLCZ10].

Cyber [Che18, OTD10].

D [AP10, CG12b, DBPS12, DWWZ12, EAA+16, GZHD12, KSV+12, LJ17, LJ15, MCDB12, MKH+12, PLL10, RS16, SG14, SRK+17, WSSO12, WY12, tWmC12, YI14, YPR11].

D-Based [WSSO12].

D-like [LJ15].

D-PUF [SRK+17].

Dana [Ano10].

Dandelion [VF17].

Dane [Ano10].

Dankel [VF17].

Dangers [VF17].

Dare [FMS12a].

Dao [FMS12a].

Daoism [FMS12a].

Darmstadt [FMB12, Sen10].

DASH [KCC17].

Data [Ano13c, ADF12, Bar12, BJL16, BCD+12, BJL12, BW12, BKLS18, CWL+14, CMLS15, CCW+10, CSV15, CCT+14, CLW16, DDS12, Dan12, DR12, DMS+16, DA12, DCA18, DLZ+16b, EKB+16, FMY15, FPy15, FRS+16, G1TT11, HSM14, HLT+15, HK14, IB13, KRD13, KG16, LLPY19, LLZ+17, LWJ+C14, LLZ+12, LZC+12b, MLO17, Mal13, MMS17b, MM14b, NNAM10, NR12, PD14, PSM17, PH12b, PNRC17, QZL+16a, QZZ18, RCP+18, Real16, RSN14, SGG18, SAKM16, Sar10b, SMSK18, SP15b, SKH17, Sia12, SL10, TCN+17, Tan15a, Vai12, VSY15, WZCC18, XNK15, XWSW16, YDY+16, YMC+17, ZXYL16, ZPXX17, ZTL15, ZLW+17, AP10, ASO14, Ana14, Ana11a, Ara13, ADH17, ALL+18, BLL+19, BTP1215T, BC18, BKL13, CDG12, CLH+16, CDF+10, CDL18, DFJ+10, DTZZ12, DRD11, ED17, FS18, GHD19, Gen10, GLB+18, GZS+18, HSM13, HKW+15, HMCK12, HH16, HYS18,
21

Directly [BKBK14, CDFZ16, Hof16, PPA18]. Directions [BKBK14, CDFZ16, Hof16, PPA18].

Directions [BKBK14, CDFZ16, Hof16, PPA18].

Directions [BKBK14, CDFZ16, Hof16, PPA18].

Directions [BKBK14, CDFZ16, Hof16, PPA18]. Directions [BKBK14, CDFZ16, Hof16, PPA18].

Directions [BKBK14, CDFZ16, Hof16, PPA18]. Directions [BKBK14, CDFZ16, Hof16, PPA18].
[LD13, SJ12]. **dyadic** [MO14]. **Dynamic** [ABB19, EKB+16, FHR14, HH15, KYH18, LHM+15, MWZ12, MM12, NKWF14, PPS12a, PNRC17, SSW12, SY14, SKV12, SGC14, VM15, XNKG15, XWSW16, XZY+12, XWZ+18, ZXYL16, CTL12, CSTR12, DSCS12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KH18, KPB17, LXMW12, LHM14, LZC17, NPH+14, PSJ+13, SES+16, SSS11, SGM16, XHM14, YZL+18, YD17, ZSMS18, ZZL+18].

**dynamic-identity** [JZS+10]. **dynamical** [JTI12b]. **Dynamics** [RSCX18, AaBT16, LTC+15a, Lud12].

**dynamics-based** [AaBT16].

**dyslexic** [Bha16].

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

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

**E-Learning** [Yon11].

**e-mail** [BTW15].

**E-passport** [LZJX10].

**E-rental** [LY14].

**E-Voting** [LGPRH14].

**E2** [WYL14]. **EAC** [LZJX10].

**Each** [YLL+12]. **EAP** [FLH13, HCZ+14, ZCLL14].

**EAP-based** [HCZ+14, ZCLL14].

**Easy** [Bel16, Bro11, And13].

**Earth** [Har14].

**easier** [MBF+13].

**Eat** [DSSDW14].

**Eavesdropping** [CWL16, Han12, PX13, YSJL14].

**EC** [Dra16, CFN+14, CCG+16, CMG+18].

**ECC** [BSSV12, JMW+16, KRH18].

**ECC-Based** [BSSV12].

**ECDSA** [BBB+16a, DHB16].

**ECG** [PLGMCdF18].

**ECG-based** [PLGMCdF18].

**Echo** [DLMM+18, HGT15].

**Eco-** **Based** [HGT15].

**Ecosystems** [LB+15, MTP19].

**EDAK** [ABB19].

**EdDSA** [JL16].

**Edwards** [JL16, LT14a, YTS12].

**Edwards-curve** [JL16].

**EFADS** [WLS14].

**Effect** [PLGMCdF18, WB12].

**Effective** [HTL+15, KRDH13, WMX+17].

**Effectively** [YMC+17].

**Efforts** [MAL10, SKV12, SHBC19].

**Efficiency** [ABF12, Chi16, DG17, FR+16, HRV10, LML12, LCL+17a, MS13b, WXLY16].

**Efficient** [ABB13, ASBdS16, ABF19, BWLA16, BCGH11, BHI12, BV11, BV14, CG12a, CML+18, CMLRHS13, CWVL12, CJ13, DWB12, Dun12a, DG17, EM12, FLH13, FHS13, GT12, GH13, GTR+11, GPN+12, GPT12, GJ15, GH12, GZH17, GCH15, HZC+12, HZL+18, HL10b, HBC13, HZL+15, HKL+12, HIFDGPC15, HCMD12, HH16, HC17, IAD10, KPC+11, Kim15, KHPP16, KH10, LLP+18, LDDAM12, LNT12, LXX+14, LCLL15, LSW15, LHYZ12, LWH17, LCL+17, LBOX12, MX13, MTY11, MVVR12, MU12, MP12, MC11, MN14, NES+14, NdMMW16, NZM10, P12, PAF18, PRC12, PG12, PCPK14, PNRC17, RBHP15, SGG11, SZ14, SGM16, TLCF16, TWZ11, TT12, TM18, WDC18, WLS14, WQZ+16, WCC18, XWZ16, XMLC13, YHL16, YNR12a, YNR12b, YLW13, YNQ15, YLA+13, YS15, ZQW10, ZLH+12, ZSW+12, ZJX+14, ZXYL16, ZCL+19, ZHS+19, ZPW16, ZHW15, AZPC14, AZF+12, CH11, CWS11].

**efficient** [CLHJ13, CZ14, Cho14, Cra11, CGKO11, EA12, FLL+14, Far14, FA14a, FA14b, FIO15, FNWL18, GH16, GLM+11, HPC12, HYS18, ISC+16, IB11, IOV+18, JCHS16, JZS+10, KKG14, KKH19, KL11, KSH18, LLS13, LH11a, LHI0c, LXM12, LAL+15, MLM16, Mes15, Nov10, OCDG11, PZBF18, PC14, Rao17, SZMK13, TLL2, Tso13, TKHK14, VN17, WYL13, WLZ+16, WT10a, WXK+17, XWZW16, yWqWqZC13, ZLY10, ZZ11, ZCLL14, ZTZ16, ZSC15, Zhu13, LLZ+12, TCL15].

**Efficiently** [FWS13, LGH+17, SLY+16].

**Effort**
[RSBGN12]. **Effort-Release** [RSBGN12].

**EGHR** [CML18]. **eHealth** [TMGP13].

**eID** [SGCR16]. eight [Sun11].

eight-round [Sun11]. **Einführung** [Buc10].

Einstein [HR13, Wes15]. Elbirt [Bar12].

**Election** [Ess17, TKM12]. elections [QS18].

**electrocardiogram** [ BLL19].

**Electrocardiography** [YH16].

**Electromagnetic** [HHH13]. **Electronic** [Bla12, PWVT12, SR14, YMW11].

**Elementary** [Led16, Sch15a, CM13].

**Elements** [Kra12].

**Elevation** [LZC12].

ElGamal [HLH19]. ElGamal-like [HLH19].

**Elliptic** [ADI11, AK14, ARM15, DW12, GPT12, LGH17, LWHS17, MST18, PPH12, SG15, AMN18, BAAS13, BL14, BL17, BBB16b, Cho14, Far14, IB11, KK10, MCN18, MS13b, NM10, SKH15, WHJ17].

**elliptic-curve** [BL17].

**ELmD** [BDMLN16].

Elsevier [Ano15b]. Email [Bel16, CCS14, XJW16, WR15]. embed [KPS10]. **Embedded** [AB15, BS12, BJCHA17, CFXY17, HC17, JWJ17, LWHS17, SOG15, SK12b, SDM12, WXY17, YGD17, YS15, Ano11a, CVG13, Ets10, MFH13, XWZW16].

**Embedding** [KD12a, MCDB12, XNRG15, XZZ18, YE12, ZS12, EA11, MKH12, PWLL13].

**Embeddings** [FHS13]. **Emergable** [YT12]. emerged [McG11]. **Emergence** [LMB12].

**Emergency** [HLKL15, YTH17, KLC10].

**Emerging** [BSV12, KSA16, OS16, FPG14, ZHH17].

**Empirical** [gWpNyY14, EBFK13, Sar14].

**Employees** [Mor12]. **EMV** [Cho10].

Enable [SMS14]. **Enabled** [GPT12, HFT16, QZL16a, QZL16b, SG16, SPC12, YSF18, BMI12, TODQ18, YFT18].

**Enabled/disabled** [HFT16]. Enables [IBM13a]. **Enabling** [FRS16, JSM18, SSY12, WPZM16, YYS16, MPP19, Sch12b]. eNB [CLM12].

**Enciphering** [CMLRHS13, HMR12, MLCH10, Sar11].

**Enclaves** [WBA17]. **Encoded** [DG17, HS18]. **Encoding** [BR14, CK18, SK12a, TJJF12, XHX17, PC14, Sun16].

**Encounter** [NA10a]. **Encrypt** [RAZ15, Ran14]. **Encrypted** [ADR18, BTHJ12, CWL14, CWL16, Cor14a, DWB12, DCA18, FCM14, FRS16, Gen13, GLG12, GZH17, HTZ12, HB17, HCDM17, IMB17, IBM13a, JSCM17, Kaw15, KGV16, LA15, LQD16, Lop12, Mur16, NBZP17, NNAM10, QLL17, SAKM16, Sia12, TM18, Vai12, WBC10, XWSW16, YDY16, ZDL12, XZYL16, ZVG16, ZLW17, AHM18, AZH11, BTPLST15, BGP17, BKV13, BL11, CH11, Cri16, CDL18, DL16, DRD11, ED17, FTV10, Gen10, GZS18, HH16, KHL18, LKX14, LZY16, LHL18, LW13a, OSS16, PRZB12, SXY18, SW17, Suc12, TKMZ13, WR15, WL19, XYX18, YX18, YQOL17, ZLY10, ZFH18, ZHT16].

**Encrypting** [CC10, Mar10c, dRSdlVC12, LGGCGRP14, Pow14]. **Encryption** [ADM12, AV12, AEH17, Alo12, AAC16, Ano13c, Ano14, Ano15c, Ano17d, AKP12, ABF12, AS16, BVS13, BWLA16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12, BS14, BV18, Bla16, BKLS12, BDPS12, BHPF14, BDMN16, Boy13, BV11, BV14, BGV14, CVM14, CMO16, CL16, CW112, CN12, CZF12, CLHC12, Che15, Che18, CGL12, Ch12, Ch16, CRE12, Con18, CNT12, CL16, CD16, DR10, DN12, DFJ10, DSB18, Des10b, DOS15, Dun12a, DF11, EAA12, ES11, FHH10b, FHR14, FJHJ12, Fei19, FFL12, Fuc11, GWCC15, GGH16a, GGHW17, GM13, GZZ13, GS16. GH11a, GH11b, GH12, GHPS12, GDCC16, GV12, GVW12, GM14, GL12, GKS17, Gue16, HSMY12, HLLG18, HZ11, HG12, HC17, HT17, HLC17, HPL12, IAD10, JLS12, JHL12, Jia14a, JR14, Kam13, KB10, KME12, KMY18, KTT12, KOS16].
Encryption

[KKA15, KFOS12, KHPP16, KS12, LMGC17, LMG+18, Lai17, Led16, LLSW16, LLPY19, LW11b, LW11c, LW12, LLJC12, LYZ+13, LHL+14, LLC+15, LTZY16, LLL17a, LSLW15, LH11b, LSQL18, LB13, LY15, LW16, LYY+18, LLML12, LLH18, MZHY15, MLO17, MMF14, MR14a, MTY11, MSMA18a, MVVR12, MSSM17b, MRL+18, MBF18, MPSR12, MT12, MKRM10, MSa12, Nac16, NdMMW16, NTY12, MCF14, NAL17, OT12, OGR+15, PMZ13, PR12, PB12, PDZH15, Per13, PTK12, PPS12a, PYS18, PMZ12, PCY+17, PRSV17, RVH+16, RCP+18, RZZ+15, RSBGN12, RDZ+16, RVRSM12, SGG18, Saa12a, SSLW12, Sar10b, Sch15a, SLGZ12, SZS14, She14, Sm11b, Sta12, SGG15, SMOP15, Tan11, TCN+17, TCLI15, TMC15, Tan17b, TDTH13, TKR14, TTT12, Unr15, Vai11, VSR12, VOG15, Wall18, WHC+15, WP17, WDCL18, WSS12, Wat12, WLC12, WDDW12, WZ15, WWH12, WMS+12, WQZ+16, XNK15, XY18].

Encryption

[XXZ12, XJWW13, XWLJ16, XJW+16, XH+17, YZ12, YZX+12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC+11, YFK+12, YCZ12, YK DL12, ZY13, ZWMT15, ZQQ15, ZM16, ZMM17, ZHW15, ZY17a, ZYM18, ZWS+18, ZHZ+19, AHS14, ATK17+17, AKKY17, Ana14, Ano13b, Ano15e, Ano16f, ABR12, AMHJ10, ACD+15, AHL+12, BLL+19, BAAS13, BC18, BG14, BSW12, BGP+17, CPPT18, CFVP16, CFZ+10, CW14b, CLH+16, CMMS17, CZ15b, CS11, Chm10, CW12a, CDF+10, CM13, CGKO11, DLZ16a, DDM17, DTZZ12, Eve12, Eve16, FAA+18, FH13, FSGW11, FSGW12, FMF+18, Fay16, GMOGCC15, GH13, GHPS13, GLM+16, GH12, GLL+18, GZXA19, HGWW11, HQZH14, HZL18, HDW16, HZWS18, HT13, HLRI1, HL11, HFT16, HTC17, HYS18, HYF18, HKHK13, JCHS16, Jia14b, JSMG18, JHCC14, JSM+18, Kam16, KHM13, KKM+14, LLW16, LCL+17a, LCL+15, LFZ+17, LCT+14, LFWS15, LLM+19]. encryption

[LPJ10, LH11, LW10, LW13b, LZC14, LPZJ15, LCY+16, LZC17, LJW+17, LJYW18, LLL+18, LDZW19, LL16a, LW13c, LSC12, Mar10b, MMS17c, Mes15, Mid10, Mon13, MSA13, NES+14, Nam19, PPA18, Pet12, QRW+18, Ran16, RG10, RWZ13, RPSL10, SES+16, Se18, Sar11, SY13, SE14, SE16, SH11, SM11, SNM14, SLZ12, SY15b, Sha13, SGFCRM+18, SLM10, SKB+17, Spa16, SGP+17, SGM16, Tam15, TPL16, jT12b, WGJT10, WY10, WWY11, WWY+11, WHY+12, WDL19, WLFX17, Wan18, WGWZ12, WLS14, WCCH18, XWWX16, WXCC14, XWSC10, XXX15, XWS17, XWZ+18,YT11b, yYqWqC13, Yan14, YZC17, YHH18, YCT15, YLZ+16, YL11, ZWQ+11, ZZ11, ZLZ+12, XZJ+14, ZWM14, ZT14, Zha15a, ZCC15, ZML17, ZYC+17, ZCL+19, ZZ12, ZL12, ZDW+16, ZY17b, Zhu13, Wan14, LAL+15, Sar18a, Kat13]. encryption-based

[BC18, XZW+18].

Encryption/Decryption [KB10].

Encryptions

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

Encyclopedia [tJ11]. End

[Ano15c, BRR+15, BGP+17, CFE16, Chu16, 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 [PDMR12].

Energy [Ano15d, AZF+12, ABC+17, Bla16, JEA+15, LSC+15, MP12, PAF18, TLF16, TCN+17, VN17, CZ14, ZTZ16].

Energy-Efficient [MP12, TLF16].

Energy-Harvesting [ABC+17].

engagement [LSBN14], engaging [ISC+16], engine [BS13a], Engineering [Bel18, FSK10, GHD19, LLK18, MSM18a, MP12, PGLL10, TQL+14]. Engines [LB13, BGG+13]. enhance [CZ14, SL10]. Enhanced [DTE17, KY10, KKM+13, MS17, SGG18, TV15, YCC16, AMN18, ACK+10, DLK+16, GM16, LNKL13, YQOL17].


Ergodic [IAD10]. Erratum [YFK+12]. Error [KW14, LSC+15, MCP15, TLCF16, ATI+10, Chi13a, LTT10]. Error-correcting [MCP15, LTT10]. Errors [TM18, CSS+13].


Establishing [DKL+16, GSFT16]. Establishment [ASN12, Ano11b, BCO13, DL12, NRY+14, GTSS19, SZMK13, ZPZ+16, ZWX+18].

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

EUROCRYPT [PF12, Gil10]. Europe [GOPB12, Mid10]. European [GOPB12].

Evaluating [RAZS15, WP15]. Evaluation [BLKS18, CGCS12, DM15, EGG+12, KVvE18, KLM+12, MKN13, MLB12, SMOP15, ZLDD12, FPBG14, TPKT12, ZZKA17, ZLDD14]. Evaluations [ZM16].

evaluators [ZZKA17]. Evasive [BBC+14]. Eve [AAE+14, ERL16, FHM+12].

Even [ARH14, LPS12, Ana14, DK12].

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

Everyone [Ano15c]. Evidence [Bla12, SR14]. evident [MN10]. Evolution [LQY10, Tay17, BHvOS15].

Exact [TKM12]. exam [Mor12]. examination [VCK+12]. Examining [SP13]. Example [KD12b].

Exchange [CLY14, CST+17, DG15, FVS17, GZ12, HC12, LY16, MSU13, TYM+17, WSA15, WT10b, YS12, YLW13, YRT+16, Yon12, XZH16, AKB13, A1B+16, FHH10a, FA14b, FIO15, GBNM11, GLM+11, Jia14b, KMTG12, LWS10, LML+13, SEXY18, TCS14, Tso13, TKHK14, WHJ17, WZM12a, WZM12b, WT10a, WT12, WX12, YC12, ZWXA18, ZG10].

Excitation [SOS15]. Exclusive [Men13b].

Execution [AARJ12, RQD+15, YS15]. existing [FMA+18, HT13]. Expanding


F5 [LLY+12b]. Fa [FMS12a]. fabricating [WW13]. Fabrication [VDB+16]. Fabrication-Induced [VDB+16]. Face [AQD12, XHH12]. Facial [KRB12]. facilitate [Chi13a]. Facsimile [Ano16d]. Factor [HXC+11, LLC11, AIB+16, CLP+13b, DMWS12, ED19, HCl2, IC17, JKL+16, JM+16, Kem11, LNK+18a, LNK+18b, Lit14, WW14, Wat14a].


Fairness [ALR13, Ash14, GHKL11, Wag16, MV16b]. Fake [KU14]. Fallen [HCP15]. False [LL+12, CDGC12]. Families [BSS+13, KU12]. Family [ARH+18, BMS12, BKST18, DGIS12, DJG+15, FLS+10, FFL12, GNL12, LYY+18, MFG16, YCL17].

Fast [BLAN+16, Bru12, CHS15, DSLB18, GS+16, NR12, PRSV17, WHZ12, WBA17, WQZ+13, WHV+16, FHH10a, KHMB13, MB11]. FastAD [SMA10].

Faster [CN12, HVL16, TH16, Ant14]. Fault [AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JT12a, LGL+12, LCLW17, LGLL12, MKRM10, MKA17, PH12a, RZZ+15, SEY14, YGD+17, BBBP13, PBCC14, WMYR16]. Fault-Based [BBB+16a]. fault-resistant [PBCC14].

fault-tolerant [WMYR16]. FFI [Bha16]. FC [DDS12, Dan12]. FEAD [ZWM14].

Feasibility [AAC+16, FKS+13, WHC+15]. Feature [Ber18, SGP+12, FTV+10, GJ13, MHT+13]. Features [YI14, ZTL15, FNP+15, LCM+17, LTC+15a].

Feauveau [Ara13]. February [Ano10]. DSD12, Dan12, Dun12b, Kla11, Lir14b].

FedCohesion [CCFM12]. Federated [BS13b, CCFM12, CSL+14, SAM+19, BMBS10, JAS+11, TOD18]. federated-IoT-enabled [TODQ18].

Federation [SS+10a, NB13]. federations [MMS+17a, MLM16]. Feedback [HZ11, Hey17, PYM+15, SKGY14, ZH15, LWK11]. Feedback-Based [PYM+15].

FEIPS [DG15]. Feistel [BMT16, KDH15, Sas12, SEHK12]. FHE
Francis [Joh10]. Francisco
[ABJ13, Joh10, Mar10a].
frankencerts [BJR +14]. Fraud [Ber12].
Fred [Xie12]. Free [App13, Boy16, HLH19, IL15, TWZ +12, TTH15, ZHL +12, ATK11, ED19, LL16a, SA12, SE16, YT11b].
Free-View [TWZ +12]. FreeBSD [MNNW15].
FreeBSD [MNNW15].
Freedom [Con18]. Freestart [SKP15].
French [Ant14]. Frequency [BBM15, KAHKB17, LTKP16, LWCJ14, TC10, CJP12, CJP15, EA12, NLYZ12].
Frequency-Based [LWCJ14]. Freshness [RBNB15]. Fresnelet [FMB +18]. Friendly [Fra16, KCC17, SZDL14, ACM12, BP18, KLL +16, RD17, WOLS12]. Frontside [DDR +16].
FSR [MD12b]. FSR-Based [MD12b].
Fugue [AP11]. Full 
[ALR13, HEC +12, LW12, VS16, WLC12, BKR11, DDM17, LC13, Ran16, SWW +17, SKP15, Tam15, TY16b]. Full-hiding [DDM17] full-text [SWW +17]. Fully 
[AKP12, BV11, BV14, BGV14, CMO +16, CN12, CZF12, CNT12, DOS15, GH11a, GH11b, GHS12, HLLC11, LMGC17, LSLW15, LSC12, MVV12, MSM18a, Nac16, NCCG13, PB12, SGH15, Vai11, VV19, WHC +15, XWZ +18, ZZ12, GH13, ZXJ +14, ZML17].
Fully-Homomorphic 
[FH11b]. Fully-Homomorphic-Encryption [CN12].
Fun [APPVP15]. Function 
[AMPH14, Bee17, BKST18, FLS +10, LyW112, MMS17b, SCY11, WSSO12, AKY13, AP11, CMMS17, LK14, LP11, RS14, Sar11, SXL16, TQL +14, WYW14].
Functional 
[AS16, BV18, BSW12, Boy13, GGH +16a, GVW12, LQD +16, MVV12, Rus15, Wat12, ZYT13, ZWTM15, ZWM14].
Functionalities [JR13]. Functions 
[ACZ16, ALR13, BBC +14, BIKK14, BKPW12, BK12a, CPS16, D5MM14, DQFL12, FY11, LVV11, NR12, Rja12, RW12, SMS14, SLY +16, Tan12a, YTP11, AY14a, BDP11, CG12b, CQX18, CW12a, ESR114, Gen10, HRV10, Li10, QZDJ16, WT13].
Fundamentals [Joh10]. Further 
[HCL +14, WHY +12]. Fus [FMS12a].
Fusion [ABCL17]. Future 
[AYS15, BCE +12, BKBK14, Bon12, CDFZ16, GCK12, HYS18, Mon13, Ano13d, FPBG14, Mac12, PPA18, PHWM10, MJS13].
Future-proof [Mon13]. Fuzzy 
[KRDH13, NC12, SH11, XJWW13, Alp18, KHMB13, MMSD13, SM11, SNM14].
G [HLYS14]. G2 [BP18]. G2C [BMP12].
GA [MMSD13]. GA-fuzzy [MMSD13].
gadgets [Gel13]. Gait [XJR +17, XJR +17].
Gait-Based [XJR +17]. Gait-Key 
[XJR +17]. Gallai [SS106]. Galois 
[CFR11, CLF +17, HSA14]. gambling 
[Ana14]. Game 
[MZA +13, LPZJ15, SD10, SKEG14].
game-theoretic [SD10, SKEG14]. Gap 
[LRVW14, TMGP13, PPA18]. Gaps 
[SMP +13, DLK +16]. Garble [AIK14].
Garbling [App13]. Gard [Kap11]. Gate 
[Kar12]. Gates [App13]. Gateway 
[WZM12a, WZM12b, WL11, WXK +17].
Gateway-oriented [WZM12a, WZM12b].
Gaussian 
[HKR +18, YWL +17]. GCD 
GCM/GMAC [SKK10]. GDLP [MMZ12].
Gear [AHS13]. Geckos [GSC17]. geese 
[Bai12]. GenePrint [HQY +16]. Gener 
[HYS18]. General 
[Bar16, CJXX19, FJJH12, GFBF12, Gu16, HP12, KOTY17, LPL15, PB12, SJWH +17, YFF12, ABDP15, Bai12, DGNJ14, HZQH14, LWS10, WS12, YC11, ZYC +17].
General-Purpose 
[Gue16, ABDP15, DGNJ14]. generalisation 
[LR15]. Generalised [Hes12].
Generalization [GMNS15]. Generalized 
[BFMT16, LPL15, PC14, TY16b, Ye14, ZAC17, ADG16, BNST17, KL11, NC13, YMSH10]. Generated [ADD10, LCL17b]
Generating [Ano16e].  

Generating [ABS+12, BCGH11, BH15, LTC+15b,  
MR14a, MJGP12, NIS12, PS14, SOS15,  
SRK+17, XJR+17, Aia15, ACD+15,  
CJXX19, GMRT+15, GCH15, KHMB13,  
KKM+13, SGFCRM+18, XW13, YDH+15].

Generation [Ano16e].  

Generators [ADD10, BK12a, CDK+10, MVV12,  
NNAM10, NKWF14, CFY+10, LGKY10,  
MRT10, PLSvdLE10, SH11, SM11, XSWC10].

Generators [AS17, DSLB18, LTKP16, MFG16, NIS12,  
PFS12, CP13, HRV10, MG15, Sti11, Zim10].

Generic [BWLA16, BR14, Chi16,  
GWWC15, HXC+11, Sar10b, SY15a,  
WCL+18, ZCLL14, HQY+16, YTY11b].

generically [MHKS14].

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

Genius [Hai17].

Genomic [BKLS18, RCP+18].

Gentry [GH11b].

Genuine [HR13].

Genus [FWS13].

Geo [Har14].

Geo-location [Har14].

Geodesics [ZZCJ14].

Geographic [LC17].

Geolocation [FPY15].

Geometric [DSB16, GTT11, WLZL12, YWWN15,  
CLZ+17, GZHD12].

g eo-metrically [TLL13].

Geometrically [WYW+13].

Geometry [tWmC12, CFR11, CZ15a].

German [BDKF12, Biö12, Buc10, Cop10a].

Germany [FBM12, GLIC10, Sen10, Wat10].

Gesture [LCL17b, SHBC19].

g esture-based [SHBC19].

Gestures [AUMT16, GCSAddP11].

Get [GPT14, Sch11].

Getting [ESS15].

GH [GH10b].

Ghost [CD14].

GHZ [CCL+13].

GHZ-State [CCL+13].

g iant [Joh15].

girls [Mun17].

Girod [GMNS15].

GLARM [LLZ+16].

glimpse [Mic10a].

Global [CLP13a, CLH13, MRS+17, GH16, HL11a,  
TMK11, ZX11, LNK+18a].

Globally [CSS14].

Glyph [XZZ18].

GMAC [SKK10].

Goal [BM12].

Goal-Driven [BM12].

Goes [BCD+12, RY10].

Goldreich [Lin17].

Goldstrike [BH15].

Goliath [Sch15c].

Gong [LLW16].

Good [DQFL12, FY11,  
LSBN14, RY10, SA14, WT13].

g oodbye [HU15].

Google [Har14, Lo15, VGN14].

Goppa [MBR15].

Gordon [GW14].

GOST [LC13, WYW14].

Government [Ano15e].

GPG [Ran14].

GPGPU [RVRSCM12].

GPGPUs [TLCF16].

GPU [BCGH11, GCH15, HBBRM+16, HHJC14,  
MMB11, ZOC10].

GPUs [VKP17].

Graded [BR14].

Grain [BMS12, FSGW11].

Gray [DA10, UUN13].

Gray-Level [DA10].

Great [Acz11].

green [dCCSB+16, ZTZ16].

Grey [LRW13].

Grey-box [LRW13].

Grid [CGB+10, DLZ+16b, KS15, LPL15, AMN18,  
JAS+11, MCN+18, WS12, YYY11].

Grid-Based [LPL15, WS12].

Grids [SC10, CT11b, GLW13, SLY15, JAE10].

Gröbner [EVP10, FES10, Tam15].

Gros [Dan12].

Group [AEHS15, BSV12, CGY+13, CLW16, DT13,  
FVS17, HL10a, Har13, LLZ+16, LCCJ13,  
TW14, XLM+12, XGLM14, XZLW15,  
ZXH16, AKK+17, CML+18, GBNM11,  
HCCC11, HPY10, I0V+18, LLLS13, LWS10,  
LMM+19, RS15, WDZL13, WTT12, YZL+18,  
ZZKA17, ZWQ+11].

Group-based [LLZ+16, CML+18].

group-key [I0V+18].

Grouping [LNZ+13].

Grouping-Proofs-Based [LNZ+13].

Groups [Abe12, GZ12, XNK15, YS12,  
YKNS12, MZ17a, WQZ+13, ZZ15].

GRS [TD14].

Guangdong [IEE11a].

Guaranteed [TBCB15].

Guerrillas [Has16].

Guess

H.264 [JSZS12, JHHN12, LLHS12, LW13c, MU12, WDDW12, ZLDD12, ZLDD14]. H.264/AVC [JSZS12, JHHN12, LW13c]. H.264/SVC [MU12, WDDW12, ZLDD12, ZLDD14]. H.265 [GKSB17]. H.265/HEVC [GKSB17].


Handoff [HNC12, HZC14, XHCH14, ZBR11, ZCLL14]. Handover [HBCC13, LBR12, CLM12, CML18, HZWW17, QMW17, YHL16, YHHS16, YLS12]. Hands [GPT14, BSS11]. hands-on [BSS11]. Handshake [KK12, KK13, WZ11].


Hard-to-Invert [ZWTM15]. Hardcover [Joh10]. Harder [KTA12, Sch16]. Hardness [BHKN13, SS13]. Hardware [AW17, BRPB13, BDMMIN6, BJCHA17, CMLRHS13, DZS18, DOS15, ERRMG15, GP17, GCCV17, GCS13, HAK14, HG12, HSA14, HC17, HLN10, KAK18, LGH17, LLKA19, LRWW14, MLCH10, MCS15, MRL18, MZY18, NDC13, NdMMW16, PC16, PG12, RMP10, SN10, Set16, Sti19, Tay17, WOLP15, YSF18, ZHS19, ZAG19, AMN18, BDM18, BGG13, KHF10, MD12a, NS10, Nov10]. Hardware-Assisted [LLKA19]. Hardware-Based [HLN10]. Hardware-Enabled [YSF18]. Hardware-Enforced [Set16]. Hardware-Intrinsic [SN10, NS10]. Hardware/Software [MRL18]. hardwares [SKH15]. Hardy [Xie12].

Harmonic [YWNW15]. Harnessing [DFKC17]. Harvesting [ABC17, ZGC16]. HAS-160 [WLC12]. Hash [ANO12, AMPH14, BHH15, BKST18, BK12a, CLP13a, JCPB12, CZLC12a, CZLC12b, CZLC14, CJP15, EAA16, FLS10, GI12, HCPPSB12, Hui13, HRS16, HBG17, MKF16, MCF17, MKAA17, NTY12, NR12, XB13, PT16, Rja12, SGY11, WSS012, ZZM17, ZHZ19, AY14a, AKY13, AP11, CJP15, ESR014, KKG14, PPB16, RS14, SPLHC14, SXL16, WY14].

Hash-Based [BHH15, GI12, HCPPSB12, Hui13, HRS16, HBG17, MKF16, MCF17, MKAA17, NXB13, CJP12, CJP15, PPB16, SPLHC14].


Headline [YGFL15]. Health [LYZ13, LHL15, Rao17, ZVG16, BC18, Ham19, IC17, WMX17, YZL18, JKL16].

Healthcare [BN14, HLLK15, ZLDC15, ASO14, Kim16]. Hearing [Bla16]. Heartbeat [IA15].

Heartbleed [DKA14, Ven14]. hedging [RY10]. Heights [Gen13]. held [Cho10].


Heuristic [BGJT14]. HEVC
HIBE [LN11c].  Hickory [NN15]. Hidden
FMS12b, PSS+13, YLL+12, ZYT13, BDK11, LCL+17a, Sch15c, Smi15a.
Hiding
DCA18, GGH+16b, GL10, JHNN12, MK12b, OT12, XLM+12, XGML14, XZLW15, Ara13, DDM17, HZL18, KWH16, LXLY12, LT14b, UUN11, WLH13, WZLW13, ZWM14.
hiera
Lac15]. Hierarchical
ADM12, BSSV12, FSX12a, LSLW15, NMS14, NLY15, OT12, WYML16, ZMW16, ZHW+16, DSCS12, HYS18, KPB17, LFZ+17, NZM10, RG10, SE14, SE16, WWYZ11.
Hierarchy
NA10b, VN16]. High
AW17, ASBdS16, Ano17d, ARM15, Bar15, BDL+11, DM15, DG17, GL12, GCS+13, HZ11, KMP+11, KPC+16, KAK18, LTKP16, LCK11, LPO+17, MS13b, MS13c, PCPK14, WYCF14, WL11, XNRG15, ABBD13, GHZ12, GCVR17, KL13, MAK+12, RS17, WLH13, WXLW13, WZLW13, WKH11.
High-Assurance
[Bar15, MK+11, WL11]. high-capacity [GZH12].
High-Dimensional
[Ano17d]. High-Efficiency
[DG17]. High-Impact
[DM15]. High-Level
[AW17, KPC+16, ABBD13]. High-Performance
[GCS+13, KAK18, LPO+17, GCVR17]. High-Rate
[PCPK14]. High-Security
[WYCF14, BDL+11]. High-Speed
[ARM15, HZ11, LTKP16, BDL+11, KL13]. high-throughput
[MAK+12]. Higher
[LWK12, PRC12, gWpNyY+14, ZSW+12, LWKP14]. Higher-Order
[LWK12, PRC12, ZSW+12, gWpNyY+14, LWKP14]. Highly
[SZDL14, ACD+15, DT13]. HIGHT
[CWP12, WWBC14]. hijacking
[DCAT12]. HILL
[KPW13, KA17]. HIMO
[GMRT+15]. Hindering
[BTPLST15]. HISS
[DT13]. histogram
[CSS+13, Lin14a]. Historians
[Cer14]. Historical
[Hai17, Han12]. History
[ABJ13, Ano19, Cer14, Cop10a, LT14b, McK10, McK11, SE16, Smi15a].
history-free
[SE16]. Hitler
[Hea15, Moo14]. HMAC
[GWM16, MAK+12, YGS+17]. HMAC-DRBG
[YGS+17]. HMAC-SHA256
[GWM16]. Hoc
[LH12, PD14, She14, XHC+12, KM10b, LXX14, SGGR+16]. Hoffstein
[Mei10]. Holden
[Ano17b]. Hole
[Ano15d, BKKV10, PC16]. Holocaust
[Han12]. holy
[Wat15, Mic10a]. home
[KPP16, Cor14a]. Homogeneous
[HT11]. Homomorphic
[AKP12, BV11, BV14, BGV14, CMO+16, CN12, CJ13, CK18, CNT12, DOS15, GH11a, GH11b, GHS12, GHPS12, KOS16, KG16, Kim15, Lau17, LCLL15, MLO17, LSM18a, MRL+18, MBF18, Nac16, PKTK12, RCP+18, Tan15b, Vai11, WHC+15, XWZ+18, AKKY17, BDOZ11, BC18, CXXJ19, CW12a, GH13, GHPS13, GLM+16, LWL16, SEXY18, Tan15, WSC14, ZJX+14, ZYC+17]. Homomorphism
[Bra13]. Honey
[J14]. Hop
[RWLL14, LCT+14]. Hop-by-Hop
[RWLL14]. Hopf
[Kuz11]. hose
[BSR+14]. host
[LKKL13, der10]. hostile
[CDA14]. HotCalls
[WBA17]. House
[Ano16h, Bla16]. HP
[CGB+10]. Hromkovic
[Gas13]. HTTP
[BHCdFR12]. Huang
[LSW16]. Huffman
[Sun16]. Hui
[FMS12a]. Hui-Yuan
[FMS12a]. Human
[HHS+15, IA15, DMT12, LW+10, PYH+18]. Humans
[RBNB15]. Hummingbird
[ESS12]. Hummingbird-
[ESS12]. hunt
[Bha16]. hunted
[McG11]. HVS
[RMG18]. HWMP
[BOB13]. Hybrid
[ADI11, ARM15, JHW+19, KBL11, KKA15, LP12, NGAuHQ16, OA012, Per13, SGG18, XWLJ16, SAM+19, EEAZ13, KP18, XWLY16, WS14, XWS17, BOB13]. Hybrid-Double
[ARM15]. hybrid-indexed
[WXLW16]. hybridization
[MMSD13]. Hyderabad
[GG10]. Hyper
[BL14, WZG+12]. Hyper-and-elliptic-curve
[BL14].
hyper-chaotic [WGZ+12]. Hyperchaotic
[GMOGCCC15]. hyperelliptic
[FWS13, Kre13]. hypergeometric [YL11].

i-NVMM [CS11]. I/O [CDD13]. i2b2
[RCP+18]. IB [CZLC14]. IBC [BOB13].
IBC-HWMP [BOB13]. IBM [ABC+12, ACD+15, BAB+13, HKS+14, JSM+18].
i-NVMM [CS11]. I/O [CDD13]. i2b2
[RCP+18]. IB [CZLC14]. IBC [BOB13].
IBC-HWMP [BOB13]. IBM [ABC+12, ACD+15, BAB+13, HKS+14, JSM+18].

ICA [tWmC12]. ICICTA [IEE11a]. ICISC
[LH10a]. ICs [GSFT16]. IF
[Ano17c, CTL13, CDPICA16, EZ15, HCC10, IB11, KGO10, LMGCI7, LY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, TPL16, TT12, TTH15, Wan18, WT10b, WTT12].

ID-based [MM12, LMGCI7, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18, WTT12].

ID-card [Ano17c]. IDEA [BNY14]. Ideal
[LPO+17, WCL+18, HKT11, yYqWqZC13]. idealness [TD14]. ideas [Mac12].

idempotent [Dur15]. Identical [Bow11].
Identifiable [Oba11]. Identification
[FSX12b, FSX12c, FSX12c, VAG15, YGFL15, YKK18, AGLIW16, CTHP13, CJP12, CJP15, EA12, HQY+16, KI11, KL13, NLYZ12, YTM+14]. identified [AZH11].

identifier [MJ13]. identifiers [Cer18].

Identifying [CSV15, SVG16, ZCS15].

identities [GLM+11]. Identity [AQD12, ASM12, ASVE13, Ano15b, ACAT15, ASS15, BWLA16, BCF16, BGG12, BKWP12, BDFK12, Ber12, Ber17, BS13b, Bow11, Cal13, CCFM12, CSL+14, CSZ+11, CPL12a, CPL12b, CLHC12, CLYC14, CGL+12, CGY+13, Chi12, dCCSM+12, FHH10b, FZT14, FSX12b, FSX12c, FSX12c, GOBP12, Gy13, GDC16, GJG15, GJZ17, HZC+12, HwS12, HSM13, HSM14, HZ15, HYWS11, HYF18, KKA14, KRB12, Kuz11, LMG+18, LMB12, LSL12a, LKAT12, LJX14, LLC+15, LTZY16, LSLW15, LH11b, LSL12, LBR12, MLO17, MFB+13, MJGS12, MR10, OdH12, Par12a, PSS+13, PSJ+13, PWVT12, RZD+16, RS15, SS10a, SS10b, SS12a, SAAB10, Sch11, Ser12, SSCP12, SKGY14, SWW+16, SGH15, TKN14, Tina15, TH16, TMGP13, Vl16, WY10, Wan14, XZX12, XQL11, XJW+16, YXY+12, YTM+14, Yon11, YHK+10, YKK+11, YFK+12, YCZY12, ZHL+12, ZMW16, ZD+16, ZPXX17, ZYM18, ZTSM12, ATKH+17].

Identity [Ano13d, BMBS10, BOB13, BMM12, BBGT12, CTHP13, dCCSM+16, DJ14, D10, DWZ12, FA14b, GMRT+15, GVCdBR012, HZC+14, HWD16, HZWW17, HLR11, HWD16, HZWW17, HL11, HPY10, Hwa11, JZS+10, KKGK10, KKM+13, KL11, LKKL13, LK12, LMX12, LCT+14, MMM+17a, MD15, MGP10, MJS13, MLM16, MM13, NCL13, OJSI, PLCs11, QYWX16, RG10, SSS12, SE14, SR10, hSZZ15, SA16b, Sim15b, SASS11, SSS11, SG16, WWY11, WLY11, WSC14, WLFX17, WMX+17, Wat14b, WWWW17, XW12, XCL13, XHM14, YWL+17, yYqWqZC13, YYS+16, YMS10, YKK+12, YXA+16, YNX+16, ZZ12, LZJX10, PN10, Sar18a, Kat13].

Identity-Based [ASS15, BWLA16, BGG12, BKWP12, CTCG12a, CTCG12b, CTCG14, CGL+12, CGY+13, Chi12, FHH10b, FZT14, FSX12b, FSX12c, FSX12c, Gy13, GJG15, GJZ17, HZC+12, HSM14, HZ15, LMG+18, LSL12a, LLC+15, LTZY16, LSLW15, LH11b, LSL12, LBR12, MLO17, RDZ+16, SGH15, TKN14, Wan14, XZX12, XJW+16, YXY+12, YHK+10, YKK+11, YFK+12, YCZY12, ZHL+12, ZMW16, ZPXX17, ZYM18, CSZ+11, HSM13, HYWS11, HYF18, LKAT12, LJX14, MJGS12, RS15, SWW+16, Tia15, TH16, ZD+16, BOB13, BMM12, CTHP13, D14, FA14b, GMRT+15, HZC+14, HWD16, HZWW17, HLR11, HWD16, HZWW17, HL11, HPY10, Hwa11, LK12, LCT+14, MJS13, MM13, NCL13, QYWX16, RG10, SE14, SE16, hSZZ15, SA16b, SASS11, SG16, WWY11, WSC14, WLFX17, WLY+17, yYqWqZC13, YMS10, YKK+12, YXA+16, YNX+16, ZZ12, LZJX10, PN10, Sar18a, Kat13].
YKC$^{+}$12, YXA$^{+}$16, ZZ12, LZJX10, Kat13. Identity-Hidden [PSS$^{+}$13]. IdM [ACAT$^{+}$15]. IDs [SOS15]. IEC [BCM12, BCM13]. IEEE [IEE10, IEE11b, IEE13, Yan10, BOB13, CL11, FLH13, NBZP17, ZBR11]. IEEE802.16e [HLCL11]. if [ABJ13, Rus15]. IFIP [GLIC10]. IFP [MMZ12]. Igor [Sha10]. II [Muni17, SCPSN10b, SMOP15, ZWS$^{+}$18]. III [SMOP15]. ILA [HZS$^{+}$19]. Illegal [ABJ13]. Illogical [Hel17]. Illumination [KLY$^{+}$12]. Illusion [GHS14]. Illustrated [Cop10a]. Im [BGI$^{+}$10, BGI$^{+}$12]. IMA [Che11]. IMACC [Che11]. Image [Bai10, BAAS13, BDB14, BWR12, CJFH14, DA10, IAD10, JKeY12, KPS10, LA15, LLL17a, MBC15, MAL10, MSM$^{+}$18b, PWW10, RS16, RVRSCM12, SH11, SM11, SJ12, SG$^{+}$12, SMSK18, SSA13, SRAA17, SZST18, TB18, WHZ12, WZXL12, WYWF13, WYCF14, yWXY$^{+}$18, WKY12, YLL$^{+}$12, YWNN15, Ye10, Ye14, YH16, YXW18, XZ$^{+}$11, BWA13, BM13, CT11a, CW14a, EA11, FMB$^{+}$18, GKK11, HLC16, KM11, LXCM11, IW10, LWLW11, LW13b, LPZJ15, MO14, MS17, NES$^{+}$14, PTK14, SE18, Sch12a, SM13, SM12, SNM14, SGFCRM$^{+}$18, Sun16, jT12b, TTL10, TLL13, UUN11, UUN13, yWpWY$^{+}$13, WGZ$^{+}$12, WKH11, WOLS12, XSWC10, YWL$^{+}$17, YC11, YCC16, YSC16, ZLW$^{+}$12, ZTU14, ZSMS18, ZL12]. Image-Guided [CJFH14]. Image-Scrambling [LL17a]. ImageMagick [Tay14]. Imagery [BCP14a, Ara13]. Images [BCPV11, BBMV15, CLF11, FR16, GL10, LC15, LLY$^{+}$12b, MR16, NC12, Yan12, dRSdVC12, AMK12, DD13, HWY14, LW13b, MM14a, MKH$^{+}$12, UUN13, WLH13, WZWL13]. imaging [WW13]. IMFlexCom [PAF18]. IM [FN10]. imitation [Hai17]. Impact [Alo12, BLS12, DM15, SF12]. Impartial [BCF16]. Imperceptibility [HGT15]. Imperceptible [Lin14a]. Imperfect [ABD$^{+}$15, BHvOS15]. Impersonation [AATM18, GBNM11]. Implants [Mic16, SSPL$^{+}$13]. Implausibility [GGHW17]. Implementation [BW16, BKLS18, BSJ15, BDMVN16, EGG$^{+}$12, GP17, GL12, GPT12, GCS$^{+}$13, HF14b, KB10, KGV16, MGF16, MAS16, NdMMW16, QLL17, RMP10, VKPI17, ZPM$^{+}$15, AMN18, BDP$^{+}$12, GH13, HBBRMN$^{+}$16, KY10, KSH18, MM14a, MNNW15, NES$^{+}$14, PBCC14, SK14, SAAB10, SF12]. Implementations [BFCZ12, BFK16, BDGH15, BJ10, Bru12, CMLRHS13, CBL13, ERRMG15, LGH$^{+}$17, MLCH10, Tom16, YZLC12, ABBD13, ABF$^{+}$14, BFG$^{+}$14, BJR$^{+}$14, CFN$^{+}$14, CG1H7, LBOX12, Sta11b, ZSW$^{+}$18a]. Implementing [Dav11, GH11b, HTZ12, LTC$^{+}$15a, SG15, SL010, VOG15, SA16b]. implicit [DWW12]. Imply [ALR13, LRW17]. Importance [YL17, MLMSMG12]. Important [TC10]. Impossibility [ACM$^{+}$17, BCF$^{+}$14, Mat14]. Impossible [Bio15, CWP12, LFJ16, TSL11, WYLY, WW12, MNP12, SDM10, SDM14]. improbable [TS16a]. Improve [AQD12]. Improved [Ber18, BCP14a, Chi12, CGKO11, FVK17, GLLSN12, IK15, JLH12, KZG10, LT14a, LWZ12, LJF16, LHH11, LCCJ13, LC15, LLLM12, PH12a, QZ14, SK12a, SEHK12, SS10b, SP15a, TS16a, WLC12, WWBC14, YHHS16, ZJ11, ZLDD12, GLW13, HB12, Nam19, PWLL13, SDM10, XHH12, Wan14]. Improving [FRS$^{+}$16, MWZ12, PLPW13, AN15, BMB16, CHS11, Far14, LNM$^{+}$11]. improvements [EA12, HRV10, Tso13]. Improving [AB15, BCM$^{+}$15, Chi16, FMS12b, GMS11, HLC11, MHC12, Sar10a, SS11, YWFW18, YKBS10]. IMS [IG11, MEF012]. In-Memory [PAF18]. In-Order [ZBP18]. Incentive [SJWH$^{+}$17, YTH17]. Incentive-Aware [YTH17]. Incident [CCG$^{+}$16, CMG$^{+}$18].
Interface [WBA17].
International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FBM12, GLIC10, JY14, LCK11, LW11a, LTW11, MV12, PJ12, Sen10, Wat10, Yan10, Yan11, AB10a, Abe10, Ano11a, BYL10, BL10, Gil10, GG10, HWG10, LII10a, IEE11a].
Internet [Ano13d, LFGCGCRP14, TW14, AAC+16, Ano13b, ClF+17, CW12b, DRS16, DG15, Gel13, Ham19, HZL18, JKAU19, JTZ+16, LNK+18b, LGH+17, LSG16, MJS13, MCF17, NLLJ12, NLY15, Orn16, PLGMCdF18, SB17, SYW17, SYC+17, SKEG14, WCCH18, YCT15].
Internet-Draft [MCF17].
Internetworking [SAAB10].
Interoperability [HWK+15].
Interplay [HWK+15].
Interpolation [JTZ+16, KU14].
Interpretation [MZ17b].
Interpretation-Based [MZ17b].
Intersection [LZY+16].
Interval [PPR+12, Cra11, DTZZ12, LWY12, MO14].
Interval-based [PPR+12, Cra11].
Intra [HF14b].
Intra-Masking [HF14b].
Intrinsic [HRK18, SN10, NS10, RCW15].
Intrinsically [SRK+17].
Introducing [Fay16].
Introduction [DK15, Gas13, G+13, JSK+17, LKL18, Low12, Mei10, Men13a, Sch15a, SOG15, Stal1b, CM13, Buc10, Led16, Sch15a, Full10, Mur10].
Intrusion [NSMS14, SAJL16, SBV14, YKC+12].
Intrusion-resilient [YKC+12].
Intrusive [AARJ12, MFH13].
Invariant [yWpNyl11].
Invariant [CSW12, NKWF14, RS16, WYW+13, YWN15, GZH12, LCM11].
Invariants [NKWF14, CDSLY14, KK10, MZ17a, TLL13].
Invention [Orn16].
Inverts [Ant14].
inversion [KHHH14].
Invert [ZWTM15].
Inverted [XYL16].
Invertible [SLY+16, UUN13].
Investigating [SPM+13].
Investigations [Bla16, Har14].
Invisibility [BN14].
Invisible [Keb15, Mac14, SYL13].
InvisiMem [AN17].
INVISIOS [AARJ12].
Involution [Bru12].
Involving [HLCL11].
IoT [AATM18, CCM17, CSH+18, FQZF18, GAI+18, MMP19, NVM+17, SGC16, TODQ18, TG17, WCFW18, WXK+17, YFT17, YFT18, YTH17, ZCW15, ZLY+19].
IoT-Based [YTH17, ZLY+19].
IoT-Enabled [SGC16].
IoT-Enabled [YTH17, ZLY+19].
IoT-Based [SAJL16, ZSW+18a].
IP [AGLW16, AZH11, PJ18, PA10, RS17, SP15a, TJZF12, WBC+10].
IP-SEC [PA10].
IPs [GSFT16, NDG+17].
IPs [AGLW16, AZH11, PJ18, PA10, RS17, SP15a, TJZF12, WBC+10].
IP-SEC [PA10].
IPs [GSFT16, NDG+17].
IPv6 [KP12].
IPA [ZM16].
iphone [Wu16].
IPs [GSFT16, NDG+17].
IPs [GSFT16, NDG+17].
IP-SEC [PA10].
IPs [GSFT16, NDG+17].
IR [BAAS13].
I, [HJJ+12].
IRC [HB13].
IRC-based [HB13].
IRIW [JKHeY12].
irregular [YWL+17].
ISBN [Ano15b, Ano17b, Bai12, Joh10, Mur10, Sch15a].
Islet [Dan12].
ISO [BCM12, BCM13, TS16a, WWBC14].
ISO/IEC [BCM12, BCM13].
Isogenies [Y+17].
Isogenous [YAK18].
Isogeny-Based [YAK18].
Isolated [YS15].
Isolating [LG12].
ISSAC [Wat10].
Issue [Ano13d, Ano16a, Ano16b, Ano16h, CSYY18, GO17, LW13a, LKK18, XW13, PHWM10, Sim15b].
Issues [ABHC+16, PZPS15, JAE10, KJN+16, MHV15].
ISTE [Ano15b].
Italian [Sac14].
Italy [Cra12].
items [YD17].
Iterate [HRH11].
Iterated [LPS12].
Iteration [CCZC13].
iterative [SXL16].
ITUbee [FZP+17].
J [Bar12, Led16, Sch15a, WZM12a].
J2ME [GTP12].
J2ME-Enabled [GTP12].
Jacobian [BAAS13].
Jacobians [Res12].
Jacques [Nac12].
jamming [YSJL14].
Janet [Ayu12].
Japan [Sah13, Maf16].
Japanese [Don14].
Java [GTP12, XHH12].
Jaypee [CGB+10].
Jean [Dew11, Nac12, SR14].
Jean-Baptiste [Dew11].
Jean-Francois [SR14].
Jean-Jacques [Nac12].
Jeffrey [Mei10].
Jill [Mei10].
Joe [Car11].
John [Wes16].
Johnny [HMI2, RAZS15].
Join [PD14].
Joint [ABF12, LC15, PMZ13, TCN+17, LSQ11b, ZC12]. Jonathan [Ful10, Mou15].
[CFST17]. Joux [AY12].
JPEG [AOT13, LSQ11b, LC15, MAL10, QZ14, SK12a, WHZ12, WLH13, ZC12].
Junction [VDB+16]. June
[ACM10, ACM11, Gil10, Kap11, Wes16].
Juniper [CCG+16, CMG+18]. Juraj [Gas13].
Just [Pf10]. JXTA [AMHJ10].
K2 [PS12]. Kalya [OGK+15]. Karatsuba
[BCL14, MRL+18]. Karhumen [BCPV11].
KASE [CLW16]. Katz [Ful10, Mou15].
KDM [MTY11]. Kecceak [BDP+12]. keep
[Rus15]. Keeping [CG14b, Man13, Gup15].
KEM [CZLC14]. kept [Cha13c]. Kerberos
[SCH10, TW14]. Key
[ASN12, Ano11b, ABB19, BN14, BVS+13, BL12, BBB+16a, BD15, Bar16, BCO13, BKLS12, BF11, BKKV10, BB10, CVM14, CT18, CLY14, Che15, CJ13, Chl16, CCT+14, CNT12, Cou12, CMA14, DWWZ12, DL12, EAA+16, FZT13, FVS17, FBMI2, GFBD12, GT12, GZZ+13, GSW+16, GST13, GPT14, Gir15, GKS17, GZ12, GLB+18, HSY12, HLLG18, HC12, HL10a, HCL+14, HCT+15, HEC+12, HLIH9, Jia14a, JEA+15, KPI12, KTT12, KFOS12, Kin15, LLSW16, LCLL15, LQY10, LY16, LH11b, LSQ18, LCCJ13, LYY+18, LBR12, LLH18, MZHY15, MVV12, MNP14, MTY11, MMY12, MPRS12, MNS11, MSU13, NNA10, NRY+14, NTY12, Orm16, PSM17, PDNH15, PCPK14, Pud12, PNRC17, RVIH16, RSBGN12, RW12, Saa12a, SK11, SNJ11, SEHK12, SK12b, SWM+10, Sia12, SGL15, SLY+16, TMC15, TYM+17, TM12, WP17, WSS12, WLC12, WZ15, WCL+18, WWHL12, WT10b, XNKG15]. Key
[XXZ12, Xio12, XLM+12, XJWW13, XGLM14, XZLW15, XJR+17, YM16, YZX+12, YS12, YLW13, YRT+16, YL17, Yon12, YKC+11, YFK+12, ZXH16, ZY17a, AA14, ATKH+17, APK+18, ABB+14, AKG13, AIB+16, ABW10, AN15, BS15, BAGD12, BB14, BJ16, BS12, BGG+13, BBB16b, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLCZ10, DLK+16, DGIS12, Dur15, FHH10a, FA14b, FIO15, FHZW18, GMT+15, GPP+16, GH16, GBMN11, GLM+11, GTSS19, HPC21, HZWW17, HBW12, HL11, HLYS14, HCT17, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSM18, KD15, KMT12, KKG14, KIH19, KP18, KLV+16, KDW+17, LLS13, LLP+18, LWS10, LIK+17, LPs10, LW13b, LZ14, LML+13, MNP12, MRT10, NACL12, NCL13, Nos11, Nos14, RG10, RWZ13, RPSL10, SES+16, Sar14, Sav16, SLZ12, SY15b, SMK13, SZZ15, SA15, SGP+17, St10, TK19, TCS14, TLL12, Tso13, TKh14]. key
[VV19, VN17, WWYZ11, WDK19, WZM12b, WT10a, WTT12, WQZ+13, WXX+17, WX12, XW13, XCL13, XMHD13, XHM14, YT11b, YC12, Yan14, YZZ+14, YHHS16, YZL+18, YLZ+16, ZPZ+16, ZWQ+11, ZZ11, ZCC15, ZZ16, ZXS+18, ZXL+19, ZG10, ZZZ15, ZY17b, ZWS+18, ZHT16, CLW16, OHJ10, XJR+17].
Key-Aggregate
[CCT+14, PSM17, GLB+18, CLW16]. Key-Agreement
[WSS12, APK+18]. Key-Alternating
[BBKS12]. Key-Based
[Xio12]. key-correlations
[Sar14].
key-delegation
[JSMG18]. Key-Establishment
[BCO13].
Key-Extraction
[GPT14]. key-hash
[KKG14]. Key-Insulated
[FZT13, LH11b, HL11, RG10, RWZ13, WWYZ11].
Key-Length
[GT12]. Key-Length-Based
[PNRC17]. Key-Policy
[GZZ+13, GSW+16, HSY12, RV16].
Keyed
[KE19, MMS17b, YHHM18].
Keyed-Function
[MMS17b]. KEYing
[TW14, BCPV11]. Keyless
[PDMR12, ZXW+18]. keyrings [MBB11].

**Keys** [ASN11, BF12, Bro17, CC10, HDWH12, MS16, PSM17, TW14, ZMW16, CMG+18, HL14, IK15, LLY15, LH13, LW10, LLL+18, RWZ13]. keystream [SM11].

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

**Keyword** [CWL+14, Che15, HCDM12, HLH19, LSQ18, WDC18, XWSW16, XJWW13, ZXY16, BL11, CLH+16, FSGW12, GJS+18, LKK+14, OSSK16, SY15b, WHY+12, WXLY16, XWY+18, YZCT17].

**Keywords** [CWWL12, ZZ11].

**KGC** [YT11a].

**Kid** [Tan17a].

**King** [ABJ13].

**Kiss** [HU15, Ros11].

**KLEIN** [GNL12].

**Klepto** [XY18].

**Knapsacks** [Dun12a].

**Knocking** [DB17].

**Know** [BC14, CAC14, XTK10].

**Knowledge** [CLP13a, COP+14, GJO+13, GOS12, LW14, MX13, MT12, OOR+14, Pan14, TSH14, Ano11a, KPP16, LLM+19]. Known [DWWZ12, JLH12, SEHK12]. Known-Key [DWWZ12, SEHK12]. Kobliitz [BJ10].

**Kode** [NN15].

**Korea** [LH10a, LW11a].

**KP** [FJH12, HQZH14].

**KP-ABE** [FJH12, HQZH14].

**Kristie** [Keb15].

**Kryptografie** [VlBö12].

**Kryptographie** [Buc10].

**Kuala** [HWG10].

**Kurtosis** [YYO15].

**L** [Low12, Xie12].

**Labs** [Ven14].

**Labyrinth** [Fox13].

**Lacks** [BDSG+13].

**LAKE** [BCO13].

**Landis** [BBB16b].

**Languages** [MX13, Wat12].

**LANs** [FLH13].

**Lapin** [HKL+15].

**Laptop** [GPT14].

**Large** [AN12, DM15, FNW18, JLS12, JKHeY12, KCR11, KU12, LW16, LQD+16, MC11, SP13, dCCSB+16, EEAZ13, FXP12, GSN+16, LFZ+17, LBOX12, SR10, ZZKA17, ZVH14].

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

**LARK** [DS11].

**LED** [IS12, JKP12, MRTV12].

**Learning** [CTC+15, KPC+11, KRBI2, Yon11, GJ13, Sch12a, WS14, BCV12].

**Learning-based** [WS14].

**Leave** [KPP16, LLM+19].

**Learning** [CTC+15, KPC+11, KRBI2, Yon11, GJ13, Sch12a, WS14, BCV12].

**Learning-based** [WS14].

**Leakage** [AV12, BKKV10, CBL13, DCA18, DHB16, FPS12, HHH+13, HHP17, IL15, LTZY16, NTKG17, NTY12, Pan14, SCH15, TTH15, Wan18, XZ12, YZLC12, YZ12, YCY12, ZYT13, ZWTS15, ZM16, ZMM17, ZY17a, ZY17b, ZYM18, ZBPF18, CQX18, DLZ16a, DMWS12, GV14a, GL+18, SP+17, YLZ+16, ZWM14, ZCC15].

**Leakage-Free** [IL15, TTH15].

**Leakage-Resilience** [NTY12].

**Leakage-Resilient** [AV12, BKKV10, CBL13, DCA18, DHB16, FPS12, HHH+13, HHP17, IL15, LTZY16, NTKG17, NTY12, Pan14, SCH15, TTH15, Wan18, XZ12, YZLC12, YZ12, YCY12, ZYT13, ZWTS15, ZM16, ZMM17, ZY17a, ZY17b, ZYM18, ZBPF18, CQX18, DLZ16a, DMWS12, GV14a, GL+18, SP+17, YLZ+16, ZWM14, ZCC15].

**Leaky** [DLWW11].

**Leak** [BBG+17].

**Leakage** [AV12, BKKV10, CBL13, DCA18, DHB16, FPS12, HHH+13, HHP17, IL15, LTZY16, NTKG17, NTY12, Pan14, SCH15, TTH15, Wan18, XZ12, YZLC12, YZ12, YCY12, ZYT13, ZWTS15, ZM16, ZMM17, ZY17a, ZY17b, ZYM18, ZBPF18, CQX18, DLZ16a, DMWS12, GV14a, GL+18, SP+17, YLZ+16, ZWM14, ZCC15].

**Learned** [KMP+11, WL11].

**Learning** [CTC+15, KPC+11, KRBI2, Yon11, GJ13, Sch12a, WS14, BCV12].

**Learning-based** [WS14].

**leave** [CMG+18].

**Lecture** [Hel17].

**LED** [IS12, JKP12, MRTV12].

**Ledger** [Muf16].

**Leeds** [vDKS11].

**Left** [BBG+17].
Less [TKR14, GM13, Kam16], [ADD10].
Lessons [KMP11, TGC16, WL11, CMG18], [AW17, Ano15a, BRPB13, BKJP12, CCW+10, DA10, Glii2, HZS+19, HS18, JWJ+17, KPC+16, KGP12, MV16a, ZLDC15, ABBD13, MEF012, RS17, UUN13, VS11, YT11a, Bai12].
Level-Doubling [Zha12].
Levels [HLCL11, LRW17].
Leveraging [DMS+16, HCM11, MvO11, SKGY14].
Lewis [Mar10a].
Lexicographic [ZAC17].
LFSR [HLC12, MRT10, WGD18].
LFSRs [QGGL13].
Liability [Bra13].
Libgcrypt [Sch12b].
Library [ACZ16, Bee17, BLS12, FLW12, KRH18].
Life [MK13, MK10, McK11, War11].
Lifecycle [Tan15a].
Lifting [LSL12b].
Light [JE15].
Lightweight [AMKA17, AARJ12, BSS+13, BFM16, BKL+13, BM11, CGCGPD12, CPWP12, CCF17, DS11, ESS12, EKP+13, FQZF18, GNL12, GAI+18, GMV17, GMSV14, HZWZ18, HCETPL+12, IS12, IOM12, KE19, MO12, MFG16, MPM+17, PCDG14, She14, ZWY+13, ZLY+19, AMN18, AATM18, AKKY17, BLL+19, Bor10, BB16b, CL11, FLL+14, GTSS19, KDH15, LLZ+16, MCN+18, MN12, MHI15, MHI+18, PJJ18, PSO+13, SGJ+18, Tan12b, TG17, WLZ+16, WCFW18, WWBC14, XWZ+18, XHM14, YCT15, ZSW+18a].
Like [BW16, ERLM16, CGCS12, HLH19, KO16, LJ15, LJ16, RS14].
Lilliput [BFMT16].
Limitations [DR12].
Limited [DFKC17].
Limited-Use [DFKC17].
Limits [AS16, GV14a, KS12].
Linear [Ful10].
Line [FFL12, YMWS11].
Linear [BCI+13, BW12, CGCS12, CMA14, EKP+13, FGMP12, LGLL12, LJ15, LJ16, LFW+16, WGF16, YCL17, BBEPT14, Bul10a, FES10, GOGGCC15, Her10, HCC11, LWK11, ÖS11, SA14, XSWC10].
Linear/Linear [EKP+13].
Linearly [ADD10].
Linguistic [OO10, OTO18].
liinguists [Maf16].
link [Ham12, VS11].
link-state [Ham12].
Linkable [YLA+13].
linked [JCHS16].
linking [NPH+14].
Linux [Fel13].
Lipreading [OIS12].
LISISAP [VS11].
List [AEHS15].
Listening [Lan17].
live [ZZCJ14].
live-wire [ZZCJ14].
Liveness [OS12].
Lives [Acz11, McK12].
LLL [NV10].
Load [AN12, FXP12, PRN19].
Loc [CDPLCA16].
Loc/ID [CDPLCA16].
Local [pNyWY14, TMK11, VCA15, WYW+13, LMJC11, LWW+10, PTK14].
Locality [Kaw15, NCCG13].
Localization [SRA17, GAI+18, NC13, SCY15].
Locally [Yek10].
locating [ZYL+10].
Location [Kim11, PSD15, PKA15, WPZM16, CHX13, Har14, NZL+15, PC14, YXA+18].
Location-based [Kim11, CHX13, NZL+15].
Location-dependent [PKA15].
Location-Privacy [PSD15].
Locations [KD12a, Alp18].
locator [MJS13].
loci [FES10].
Locking [AB15, FHS13, LCW+16, LHA+16].
Loève [BC11].
Log [YK18, PGLL10].
Logarithm [BGJT14, CLL16, VM14, AMORH13, BGJT13, MM13, Mes15, TPL16].
LogCA [AW17].
Logging [YR12a, YR12b].
Logic [Che18, Cil11, DGP10, Hel17, RZZ+15, Ter11].
logical [CO11].
Logistic [JHW+19].
Lois [DG12].
long [CFVP16, BF12].
long-term [CFVP16].
look [AY14a].
look-up [AY14a].
Looks [ERLM16, KTA12, Sch16].
lookup [LDDAM12].
lookup-table [LDDAM12].
loop [DWZ12].
losing [SLZ12].
Loss
[DK16, JTZ+16, DMV15]. **Lossless**
[DA12, LZC+12b, GJ13, TTL10, WLH13].
**Lossy**
[BKPW12, CW12a, DN12, ASO14, CQX18].

**Lovers** [Keb15, Mac14].
**Low**
[ABC+17, AWSS17, Bai10, BCO13, BCG+12b, CML15, DJL+12, FHS13, GST13, GI12, LJK17, LBR12, Man13, NVM+17, RS17, SAJL16, WT10b, ZJ11, CZ14, Chi13a, FQZF18, LGKY10, LKAT12, LEW19, MHV15, NR11, ZPZ+16].

**Low-Bandwidth** [GST13, NR11].

**Low-Bit-Rate** [LJK17].

**Low-complexity** [DJL+12].

**Low-Cost** [ABC+17, GI12, Man13, NVM+17, LEW19].

**Low-Distortion** [FHS13].

**Low-end** [Chi13a].

**Low-Latency** [BCG+12b].

**Low-Overhead** [AWSS17].

**Low-Power** [SAJL16, WT10b].

**Low-resource** [FQZF18, MHV15, ZPZ+16].

**Lower** [LJ15, Sha10].

**LPM** [LD13, PJ18].

**LPN** [HKL+12].

**LPSNR** [LP12].

**LR** [YZ12, ZWM14].

**LR-Fead** [ZWM14].

**LR-Uesde** [YZ12].

**LSB** [DA10, Tan12a].

**LTE** [CLM12, DLK+16, LLS13, QMW17, SGC16, TM12].

**Lucas** [RW12].

**Lucky** [AP13].

**Lumpur** [HWG10].

**LUT** [ABJ13].

**Lyu2** [ASBdS16].

**LZSS** [CFY+10].

**M** [Orm16, HvS12].

**M-Identity** [HvS12].

**MA** [ACM10].

**MAC** [Kim15, LCLL15, ABS+12, CJ13, GKM16, MS13a, MS13b, MS13c, VN16].

**MacGuffin** [LGL+12].

**Machine** [AGHP14, Ano16c, CHS15, Sch12a, ABBD13, GJ13, Gup15, LLZ+16, LHA+16, QMC17, RY10, TTL10, War11, WS14].

**Machine-generated** [AGHP14].

**machine-to-machine** [QMC17].

**Machines** [Ber16a, HB17, BBDL+17, KSU13, PWW10].

**Macrakis** [Keb15].

**MacWilliams** [ÖS11].

**Made** [Orm16, Sma16].

**magic** [PHN+12].

**Magnetic** [VDB+16].

**Magnifying** [DKL+16].

**Main** [AMH+16, LY15, ZHZ+19, CS11].

**Maintaining** [WP15].

**Make** [Ayu12].

**makes** [Kem11].

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

**Malaysia** [HWG10].

**Malicious** [AAE+14, BL15, TM18, VQA15, BK12b, WTT12].

**Malleable** [LGL+12].

**Malleability** [KTT12].

**Machines** [Ber16a, HB17, BBDL+17, KSU13, PWW10].

**Machines** [Ber16a, HB17, BBDL+17, KSU13, PWW10].

**Manhattan** [SS10].

**manipulation** [OF12].

**Mansour** [DKS12, LPS12].

**Manual** [Sac14].

**Manuale** [Sac14].

**Manuscript** [Ano16d].

**Many** [LB13, HRS13, ZQWZ10].

**Many-Core** [LB13].

**many-to-one** [ZQWZ10].

**Map** [XYXYX11, ISC+16, LZY+16, LK+18, PC14, SE18, ZT14].

**map-based** [LWK+18].

**Maple** [G’13].

**Mapping** [CBDL+13, MS17, MM14a].

**Mappings** [MC11, CDPLCA16].

**MapReduce** [LJLC12].

**Maps** [Ye14, BAAS13, KLW+16, LW10].

**March** [Ano10, Cra12, DSS12, Dan12, Dun12b, IEE11a, Pie10, Sah13, WZM12a].

**Marche** [CCFM12].

**Margaret** [Led16, Sch15a].

**Marian** [Kap13].
marking [PJ18]. Markov [CR12, FVK17].
Marotto [SE18]. Marshall [Don14].
Martin [ABJ13, Hof16]. Maryline
[Ano15b]. Mashup [HTZR12].
Mashup-Providing [HTZR12]. Masked
[WH17]. Masking [HF14b, PYM+13]. Mass
[BPR14a, BPR14b]. Masses [Ano15c].
Master [Dew11, Mar10a]. Matching
[Lin15, Tan12a, MR14c, MHT+13, PPTT15,
SS17, YZL+18]. MathCW [Bee17].
Mathematical [Bee17, FGPGP14, Ham17, IBM13a, Mei10,
Sch15a, Wes16, KMI14, OO10, Sta11b].
Mathematical-Function [Bee17].
Mathematician [Ano17e].
Mathematicians [Acz11]. Mathematics
[Ano17b, Ayu12, Led16, Sch15a, Ter11,
CM13, Kra12, PHWM10, Wes16].
MATLAB [TRD11]. Matrices
[AMVZ12, BNA15, AKG13, FES10]. Matrix
[BFM16, IAD10, LYY+18, SK12a,
TDTD13, Ye10, Cha13b, LLM+19, TK14].
matrix-vector [LLM+19]. Matter
[Rau15, SS12a, DKA+14]. Max [And13].
Maximizing [DBPS12]. Maxims [Kob10].
May [BL10, FBM12, Gil10, Sen10]. maze
[LLC10]. mbedTLS [YGS+17]. MC
[HIDFGPC15]. MC-2D [HIDFGPC15].
McEliece [DN12, GV14b, MBR15, MT12,
MG15, OTD10, SWM+10, VG15]. McOE
[FLL12]. MDPC [HC17, VOG15]. ME
[XHH12]. mean [TTL10]. Meaningful
[LTC+15b, SA16a]. Means
[KRD13, AMHJ10, Kam16, Pa16].
Measure [DDD14]. Measure-independent
[DDD14]. measurement [VGN14].
Measurements [DTE17]. measuring
[DMWS12]. Mechanical [RSCX18, Mat19].
Mechanism [ABB19, KD12b, LL15, Lin15,
PKTK12, Saa12a, SMOP15, ZHS+19, CL11,
FXP12, PLPW13, PSJ+13, WB12, YXA+16,
ZWM14]. Mechanisms
[CBO+18, JSK+17, SGG18, FHH10a,
KSA16, MMZ12, PLGMCdF18]. Media
[KBL11, Fri10a]. Mediated
[Fra16, YHK+10]. Medical
[KBL11, UUN11, AIA+18, AMK12, KSA16,
KLC+10]. Medicine [MA17, LWK+18].
MEDiSN [KLC+10]. Meet
[LJ17, LWKP12, LWPF12, LWKP14].
Meet-in-the-Middle
[LJ17, LWKP12, LWPF12, LWKP14].
meeting [Hof16]. Meets [RBHP15,
BSR+14, MZA+13, PYH+18, SM13].
Members [YWZ+12]. Membership
[FHR14]. MemGuard [CZ14]. Memorial
[Ano11c]. Memoriam [Gre11]. Memories
[AWSS17, BDGH11, YNQ15]. Memory
[AN17, ASBdS16, AMH+16, BKKV10,
DLZ16a, DHLAW10, GKM16, GM13, Gue16,
HT13, HF14b, LY15, PA18, TLCF16,
ZH+19, BAB+13, CZ14, CS11, CVG+13,
VCK+12, ZWT13]. Memory-less [GM13].
memoryless [BJ16]. Memristor [MCS+15].
Memristor-Based [MCS+15]. men
[McK10, McK11, McK12, MPJ+16].
mercurial [CSZ+11]. Merkle [XWZ+18].
Mesh
[BOB13, Y14, CG12b, HGWW11, HCC11,
WLD11, XHCH11, YHHS16, ZZCJ14].
Mesher [PLPW13]. Message
[DGJ+12, KPFW12, HLLC11, Jia17, KHHH14, PSS+13, PPS12b, PA10,
RWWL14, CJXX19, CMMS17, EEAZ13,
Jia16, LC17, YMM13]. Message-Based
[PPS12b]. Messages [Gen13, YLL+12,
BBM12, BTW15, KPS10, LCM+17, SA15].
Messaging [BFK+10, Wu17]. messy
[BBDL+17]. Metaheuristic [HCETPL+12].
Metamorphic [ATS15]. metaphors
[Mat19]. metering [WMYR16]. Meters
[DM15]. Method [AGW15, Ara13,
BBB+16a, FLH13, GLLSN12, GMNS15,
HHS+15, LyWZZ12, LP12, LD13, LBR12,
MU12, OWHS12, PS14, SAA15, SY15a,
SP15a, SZDL14, WZXL12, WZCC18,
XNG+14, XNRG15, YY015, AGLW16,
AIA+18, BLL+19, CSS+13, Dra16, FVK17,
[AK14, CMO+16, HVL17, SK12b, YTS12, AAT16, SKH15, SF12]. multiplicative [KHHH14]. Multipliers [ARM15].
Multiclient [FH10b], multisecret [FGMP12]. Multistream [WXL17].
Multitone [GL10], Multivariate [DP17, ST16, YL17, YDH15].
Mutt [Ran14]. Mutual [CJP12, GM14, Kim16, SBS12, WT10b, AT18, BDM18, CJP15, Cho14, CL11, FHH10a, Far14, GPL13, GH16, HDPC13, IB11, JNUH17, JKAU19, KIH19, KP18, KLW16, LIK17, MMP19, SPLHC14, TG17, XMHD13]. MVP [CD12]. mvSERS [HLKL15]. My [GPT14, CMG18].
Naïve [ZLW17]. Name [YCM+13]. Named [ABJ13, MPJ16]. National [Fid18, ABJ13]. Natural [ZCWS15].
Nets-based [PS14]. Network [Ano10, Bis17, CWL16, CJ13, CL13, DRS16, Hay13, HDWH12, HS18, Kim15, KCC17, LH12, LCLL15, LY16, LTW11, MJGS12, NNAM10, NRZQ15, SGC16, She14, TLW12, VKPI17, VFV17, VGA15, VKC15, WP15, YZLC12, YS1L14, AKM11, AL15, Ano11a, AZF12, CJXX19, CL11, DLK16, FFBG14, HWG10, HB13, HKB14, JZS10, KP18, LH11a, LKKL13, MZA13, MJS13, NDN13, OP11, PL16, RCW15, Ser12, SCKH10, SKS18, Sta11a, Tan15b, WYL13, WS14, YLS12, ZOS17, Ste15b]. Network-Assisted [KCC17].
network-based [YLS12]. Network-Coded [She14]. Network-on-Chip [Bis17]. Networking [LCK11, LLZ17, ZHL15, Kim11, LCM17].
Networks [ABCL17, ABC17, BN14, BPSD17, BFMT16, CS14, CSH18, DS11, DF16, FMS12b, GMVV17, HZC12, HBCC13, HK14, KH10, LCLL11, LI15, LHM15, LZCK14, LWCJ14, LLZ12, MPM17, NSA15, NYR14, OO12, OKG12, PYM15, PCPK14, RWLL14, SWYP12, She14, SP15b, Smi11b, SL11, SZT17, TCN17, WXL17, WLY15, XHC12, YM16, ZC13, ZW15, Zha15b, ZLDD12, ZSA12, Aia15, ASO14, APK18, AIB16, AIK18, ADF12, BDK11, BLAN16, BB16b, CDGC12, CLM12, CML18, CLSW12, CL11, DSCS12, DK12, DLN13, EEA13, FA14b, FMA18, GH16, HG16, HZC14, HZWW17, HCC11, HCM11, HTC10, HYF18, JNUH17, JLT12, JMW16, KM10b, KLC10, KO16, KLW16, KDW17, LLLS13, LC17, LJMC11, LJX14, LIK17, LN18b, MSM18b, QMW17, RPHG12, SGCC16, SA12, SG18, SZMK13, hSZ15, SK10, TODQ18, TKHK14, WGT10, Wan13, WW14, WXK17, WX13, XWDN12, XHCH14, XMHD13, YHHS16, ZWQ11]. networks [ZBR11, ZCLL14, ZTZ16, ZLDD14, ZHH17, ZX11, LNK18a].
Neural [CSH18, SKS18, YZLC12, EEA13]. Neuroscience [BSR14, JW14].
Neutrality [Kha10]. Neutrality-Based [Kha10]. Nevada [IEE10]. never [Bai12].
Oblivious
[DN12, WCL+18, CGH11, RYF+13].

Obscurity [Edw14]. observation
[WHY+12]. Observations [HCL+14].

Obtaining [BB10]. Occasion [Nac12].

October [CGB+10, IEE10, IEE11b].

Ocotonin [BS15]. odd [GJM+15]. Oded
[Lin17]. ODIN [ABCL17], odyssey [Car11].

OFDM [CLZ+17]. Off
[GPT14, GHS14, YMWS11]. Off-Line
[YMWS11]. Off-Path [GHS14]. offering
[Par12b]. Offers [Par10]. Office [Mor10].

officers [Mal16]. Official [Küp15]. Offline
[Ano16a, GAS+16, JMG+16, LJW+17,
LKT12, RSM15]. Offline/online
[LJW+17]. Offloading [JHC14]. Offs
[AsBd16, BS14, SR10]. offsets [YQH12].

Old [Che17, GY13]. on-chip [BAB+13].

On-Line [FFL12]. on-siteDriverID
[SGGCR+16]. On-the-fly [PS14]. One
[CP16, DSM14, DCAT12, FD11, HP14,
HG12, Mat14, NA10a, PC16, TYM+17,
XW12, XYXYX11, XZLW15, Yon12, BM15,
FH10a, GPLZ13, HRV10, LP11, LW10,
LW13b, LML+13, RK11, Rus15, SM10a,
TCS14, ZQZW10]. One-Dimensional
[XYXYX11]. One-Round
[TYM+17, XZLW15, Yon12, XW12, TCS14].

One-Sided [HP14]. One-Time
[NA10a, DCAT12, BM15, FH10a, GPLZ13,
LW10, LW13b, LML+13].

One-Time-Password [FD11]. One-Way
[CP16, DSM14, Mat14, HRV10, LP11,
RK11]. Onion [KZG10]. Online
[BPsd17, JMG+16, KSd+17, PSM17,
SKGY14, SZZT18, WXY+17, ZHL15,
Ccc10, HfYf18, KvVe18, LKT12,
LJW+17, SM+18b, SKS+18, SYW17].

Online/Offline [JMG+16, LKT12]. Only
[BB10, YNR12b, YLW13, Buì10a, KMTG12,
KA17, Sar11]. open
[ABF+14, MHV15, Pow14, Win17, ZWQ+11].

open-source [ABF+14, Pow14]. OpenCL
[ABDP15]. Opening
[GDC16, LZZC12a, LLH18, LZZC14].

Openings [SP13]. openness [Bia12].

OpenPGP [MBB11]. OpenStack
[CSL+14]. Operable [BCF16]. Operating
[KMP+11, CDA14, MNNW15]. Operation
[KLLSN12, JB11, AL+18, Fay16, Lin14a,
Skk10, WGZ+12]. Operational
[CRe+12, CM11]. Operations
[Cil11, SEY14, WYW10, LZY+16].

Opportunities [Lau17, Mic10b].

opportunity [Sch11]. Optimal
[AS17, DSSDW14, HBB13, PDN15,
PPS12b, Cha13a, DDD14, PPT15].

Optimality [MM17, SDM+12]. Optimally
[DSM14, GT12]. Optimally-Fair
[DSM14]. Optimised [CMO+16].

Optimising [EVP10]. Optimistic
[WSA15, SXXY18]. Optimization
[WH17, ZAC17, FLZ+12, GCSAdP11,
Khf10, PTK14, RYF+13, ZSM18].

Optimizations [ZAG19]. Optimized
[Ays15, EKB+16, HGT15, MFB+13,
MBR15]. Optimizing [DZW18, ZSM18].

Optimum [oba11, YFF12]. Optional
[PC16]. OR-Proof [FSX12c]. oracle
[GLM+16, HKT11]. Oracles
[FZT14, FSX12a, GSW+16, XQL11, YS12,
YKc+11, YLA+13, ZY18, LLY15, RG10,
SYL13, WWYY11, YFK+12]. Order
[DCN18, K12, LWP12, PRC12, YKKL12,
ZDL12, ZSW+12, ZBPF18, AKY13, LW13a,
LCY+16, LWP14, gWpWvY+14, YL11].

Order-Hiding [DCA18].

Order-Preserving [KS12, YK12, YL11].

organisational [Sm15a]. Organization
[RSGG15]. Oriented [TJZ12].

Oriented [NNM10, Rg16, RSGG15,
WW12, WZM12a, WZM12b]. Orthogonal
[tWmC12]. Oscillator [YKBS10]. OSN
[BCF16]. OSNs [SZZT18, PZPS15]. other
[Sm15b]. OTS [Hü13]. outliers [Sch12].

Outlive [Hur16]. Output
[DK16, GST12, NR12, PBCC14]. Outright
ABJ13. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18, LQD+16, PD14, RDZ+16, YMA17, YMC+17, DFK+10, FS18, HMK12, LCL+15, LCY+16, LJW+17, QZDJ16, ZML17, ZSW+18b].
Outsourcing [DR12, LJLC12, LHL+14, LJWY18, SKB+17, SWW+16].
Over-the-air [ZXW+18].
Overcoming [BKKV10, DY13].
Overhead [AWSS17, Bai10, 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].
P2P [dCCSM+12].
P3 [HK18].
Packet [FGR+17, JTZ+16, VKPI17, XHC+12, MV16b, PJ18, PX13, XWDN12].
Packets [Bis17].
Pads [NA10a, BM15].
Paillier [Gal13].
Paillier-based [Gal13].
Pair [Lin15].
Pairing [Bon12, CWWL12, CST+17, KZG10, KHPP16, LGPRH14, Meni3a, MST18, YTS12, BP18, Con12, KSH18, LL16a, LR15, YT11b, ZY17b].
Pairing-Based [Bon12, CST+17, KZG10, LGPRH14, Meni3a, MST18, YTS12, Con12, KSH18].
pairing-free [LL16a, YT11b].
pairing-friendly [BP18].
Pairings [ASS15, Hof15, IL15, LTI14a, HBW12, QYWX16, RS15, UK18].
pairs [MCP15].
Pairwise [DL12, YM16].
Palash [Kat13].
Palm [EE11b].
Pan [GOPB12].
Pan-European [GOPB12].
Paper [TSH17, Ano16g, SK14, YFK+12].
Papers [Ano16a, Ano16b, Ano16d, LW13a, LW13b, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11].
Paradigm [ABGR13, BSV12, Mau12, MP12, WQZ+13].
Parallel [App14, ARM15, BBM15, CGB+10, GP17, LY16, LB13, MCDB12, MC11, NdMMW16, SMDS11, YE12, CSTR16, MRT10, RG10, RWZ13, WWYZ11].
Parameter [NDC+13].
Parameters [HRB13, MBF18].
parametric [Bul10a].
Paranoia [Cor14a].
Park [Ano11c, Bri11, Cop10a, Cop10b, GW14, McK10, McK11, McK12, Pea11, Smi11a, Smi15b, Smi15a, Bai12].
part [Vol14, BD15, Bar16].
Partial [DL16, GFBF12, LG12, SGS14, TK19, WDDW12, Bax14].
Partially [KB10].
participants [KSU13, WTT12].
participating [CH10].
particle [ZSMS18].
Parts [YCR16, Küp13].
Partitioned [FVS17].
Partitioning [ADR18, AP11].
Party [Ash14, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, QZL+16b, TYM+17, ZM16, ED19, FIO15, GVW12, HPC12, HWB12, LyWSZ10, LML+13, Tso13, TKHK14, XLZW16, XCL13, YC12, YZZ+14, ZZZ15, GHKL11].
Passau [GLIC10].
PASSERINE [Saa12a].
Passion [Hof15].
Passive [DHB16, GSC17, SB17, BM13, uHAN+18, LWL11, MK12a].
passport [LZJX10].
Password [ASBdS16, BRT12, CLY14, DM15, FVS17, FD11, GAS+16, HCL+14, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZXH16, ABK13, AIC18, CTL12, DSCS12, FA14a, FIO15, FHV16, GPLZ13, HCC10, IOV+18, KMTG12, LWS10, LNKL13, MM12, Mvo11, Tso13, TKHK14, WZM12a, WZM12b, YC12, ZW18a].
Password-Authenticated [HCL+14, YRT+16, ZXH16, LWS10, WZM12a, WZM12b].
Password-Based [BRT12, CLY14, FVS17, WgMW12, DSCS12, FA14a, FIO15, IOV+18, TKHK14].
Password-Only [YLW13, KMTG12].
Passwords [BHvOS15, LCL17b, BCV12, Che13, GPLZ13].
Past [Bon12].
Patchwork [NXH+17, XNG+14].
Patchwork-Based [NXH+17, XNG+14].
Path [DMS+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13].
Patient [ZLDC15, ZVG16]. Patient-Centric [ZVG16]. Pattern [DCA18, ATKH+17, uHAN+18, KPS10, OSSK16, PPTT15]. Patterns [Ano16e, BPSD17, TSH17, WOLP15, BDK11].

PAWN [JNUH17], pay [CCSW11]. pay-TV [CCSW11]. Payload [CHH12, AZH11, JNUH17, JKAU19]. payload-based [JNUH17, JKAU19].

Payment [DG15, SYC15, JNUH17, JKAU19]. Payments [RBHP15, MPJ+16]. PC [YE12].

PC-Based [YE12]. PCIe [IBM13b]. PCM [LY15]. PCM-based [LY15]. PCPs [MX13].

PCs [GPT14, GPP+16], PDGC [CGB14]. Peaks [TC10]. pearl [Russ15].


Perceived [CSW12]. perceptual [MK11].

PEREA [ATK11]. Perfect [Pas13a, Sch13, CZS16, FHKP17, LLC10, Lew10, XW12].

perfectly [ADG16]. Performance [Alo12, AW17, AB15, CGL+12, CCG10, DLK+16, DBPS12, EGG+12, ER814, FBPB14, GLG12, GCS+13, HKL+14, KAK8, LCK11, LPO+17, MCH12, SKV12, TPK12, WDDW12, Xio12, YWF18, ZLDD12, ABDP15, GCVR17, MMS+17, MS13c, ZLDD14].

Performed [Ano17d].

perimeter [Cal13]. periodic [KPS10]. periodical [CLSW12]. Permission [VN16].

Permutation [LJ16, GMSW14, LK14].

permutation-based [LK14].

Permutations [ARH+18, BKL12, Mat14]. Persistent [CSY18, TYK+12, ALL+18, PAK15].

person [PN10]. person-centric [PN10].


Perspective [KMY18, MSt18a, RSGG15, Sir16, Wag16, JW14, Suc12, ZWT13].

Perspectives [Sen17, SP+13]. Perturbation [XZZ18]. Pervasive [ACAT15, BCG+12, YD17, JSM+18, PAK15, SCY15, Tan12b, YWK+10a].

Petri [PS14]. PGP [RAZ15]. Pharmaceutical [YSF+18]. Phase [LD13, NBZP17, ZWT13, ZHH+17].

Phase-change [ZWT13]. Phase-Encrypted [NBZP17]. philosophy [Mat19]. Phone [Mur16, SAA12b, KRM+10, LTC+15a].


Physical [GPT14, GPP+16, HHH+13, SMOP15, GHD19, HQY+16, HZW18, KSA16, QMC17, VCK+12, WW13, YD17, ZHH+17].


Pipelineable [BDML16].

Pipelined [HZ11, KB10, NdMM16].


Pixel-Wise [SSA13]. Pixels [PDM12, Tan12a]. PKC [BMY12].

PKCS#11 [CFL13]. PKDS [HLC11, HLYS14]. PKE [HTC+15].

PKE-AET [HTC+15]. PKI [Dav11, YCR16]. PKIs [KGO10]. PKZIP [HL12]. plain [LW13b]. Plaintext [BM15, JLH12, MSas12, MSas13].

Plaintexts [YKL12]. Plane [YLL+12]. Platform [YE12, ABF+14, NCCG13].

Platforms [HTZ12, LMS16, SOG15, LT14b].


Podolsky [HR13]. Point
[AK14, MH14, ZC13, ZM16].
Point-To-Point [ZC13].
MBR15, YS15, ABDP15, BAB+13, BGG+13, KSH18, SSPL+13, Tar10. **Processors**

[GBF12, Gue16, RYF+13]. **Product**

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

[LMG+18, RS10]. **Professional** [STC11].

**Profiles** [BCP16]. **Profiling** [DP12]. **Profit**

[APPVP15]. **Program** [MZ17b, Wai18, CLZ+17, GGH+16b, MFT13].

**Programmable** [CLF+17]. **Programming**

[Bee17, BCEM15, SY14, ASV13, HL10].

**Programs** [BG1+10, BGI+12, CL16]. **Progress**

[AB10a, BL10, BC11, GG10].

**Progressive** [SA16a]. **Project**

[ACK+10, SS10c, Wil18]. **projective** [CZ15a].

**Prominent** [AB13]. **Promise**

[Pau10, PWVT12]. **promised** [HS11].

**Proof** [BDSG+13, Bla12, CZLC12a, CZLC14, FSX12c, Kuz11, LW12, NLY15, SR14, Ste15a, ZZM17, Mon13, PPT15, WHJ17].

**Proofs** [BGK12, BCGK12, BGB12, BCI+13, BDSG+13, CZLC12b, IW14, LNZ+13, Mau12, NTY12, Sav13b, WPZM16, AGHP14, KPP16, KKK+16, Li10].

**Propagate** [GWM16]. **Propagation**

[SKS+18, WWC+11, YZLC12]. **Properties**

[CK12, CCK16, DQFL12, FY11, JR13, KU12, Sch12c, CLC10, WT13].

**Property** [HEC+12, PR12, Rja12]. **Proportions**

[Ber12]. **Propose** [BFMT16]. **proposed**

[Bax14]. **Protect** [CTC+15, YMC+17, BVIB12, CDF+10, dCCSM+12].

**Protected**

[BDGH15, SG15]. **Protecting**

[BCP14a, GSFT16, LLPY19, Mar10b, RCP+18, SCY15, Wat14b, ATK17, CDA14].

**Protection** [CDDD13, GST12, Lop12, NGAuH16, NGD+17, RR11, SEY14, SJ12, ATI+10, HLYS14, KKM+13, LVRY10, RS17, TLL13, YWT+12]. **protection-key**

[HLYS14]. **Protocol**

[BL12, BC14, BCM+15, BSSV12, BFK16, CC14, CCM17, FLH13, FMTR12, Fra16, GI12, HvS12, HCl12, HLI10a, HCP12, HCET1+12, HKL+12, JTZ+16, JHW+19, KMO14, LNZ+13, LCCJ13, LNX15, MBC15, MR10, PSS+13, SBS+12, SGC16, TYK+12, WT10b, XJR+17, YS12, YWF18, YWZ+12, ZZX+11, AATOM18, AKG13, AIB+16, AIKC18, AN15, BDM18, BGAD12, CSD18, CCW11, CJ15, DLK+16, EA12, FA14b, FIO15, GM15, GMS14, GLM+11, HPC12, HWS12, HL14, IC17, IOV+18, JKL+16, JLZ15, Kim11, KO16, LLL13, LDDAM12, LKKL13, LWS10, LXW12, LEW19, LY14, LML+13, NCL13, NLYZ12, OH10, Par12b, SPL114, SB17, SGJ+18, SSW+16, SSS11, SSPL+13, TG17, Tso13, TKH14, VS11, WCFW18, WZM12a, WZM12b, WLS14, WM1R6, WT10a, WTT12, WC18H, XCL13, XHM14, YC12, YZZ+14, YMM13, ZWQ+11, ZTM16, ZYC+17, ZW+18, ZXW18, ZG10, ZZC15, ZX11, BOB13, CJP12, LFGCGCP14].

**Protocol** [Ste15b]. **Protocols**

[AP13, ABHC+16, BMP12, CCK12, CCK16, CCF17, CCD15, Con10, CM11, Fra15, GRL12, GM11, GLR10, HLC11, HL10b, KOS16, LY16, MS16, MT12, Mur16, NYR+14, NMS14, PS15, SBS+12, Sch12c, SOF12, TM12, Xio12, YRT+16, Ala15, Ano13b, ACM12, CML+18, CR10, CLC10, DJG14, FTV+10, GBMD11, GLR13, HSH11, Ham12, HDP13, HZWW17, HST14, KIN+16, KUS15, KKK+16, LKK13, MN10, NR11, Nos11, Nos14, SD10, YSL+10].

**Prototyping** [KPC+16]. **Provable**

[BLKLS12, CC14, EKB+16, Rog16, YMSH10, ZK11, ZPXX14, FA14a, HRS13, LHL11, WB12, XCL13]. **Provably** [BCPM12, BCM12, BCM13, BHP14, FHH10a, GLL+18, IL15, LH11a, LL16b, PSM17, WMS+12, XJWW13, YC12, YZZ+14, ZG10, ABBD13, FIO15, SLX16, WXWC14]. **prove**

[DGJN14]. **provenance** [CDL18, ZOS17].

**Provide** [Ano15a]. **Provided** [KS12].

**Providence** [Sch15a]. **provider** [DFJ+17].

**providers** [AKK+17, BK12b, YWK10b].

**Providing**

[DLN13, HTZR12, KS18, MLM16]. **Proving**
Proximity [IW14, Alp18]. Proxy

Proxy [ASS15, GSW16, GJJ15, GJZ17, GZX19, HGWK11, HZX15, KP12, LSLW15, LAL15, LSC12, MLO17, MBC15, NAL17, Pet12, PRSV17, SYL13, WY10, WYML16, XJW16, YMWS11, YCM13, BGP17, CLH16, FSGW11, FSGW12, GH12, HWDL16, HYF18, KKM14, LCT14, LFWS15, LL16a, LL16b, QMW17, SLZ12, SKB17, Tia15, WHY12, Wan18, WLS14, XJWW13, YKC11, YFK12, ZY17a, ABW10, IM14, LPS10, LZC14, BSAW12, RPSL10, SES16, VN17, ZCC15, ZY17b].

Proxy-invisible [SYL13].

Ps [HDWH12].

Pseudo

Pseudo [NN12, XYXYX11, CFY10, KM10a, MG15, PLsvLE10, SH11, SM11, XSWC10, Zim10].

Pseudo-Random

Pseudo-Random [XYXYX11, CFY10, KM10a, MG15, PLsvLE10, SH11, SM11, XSWC10, Zim10].

Pseudonym [XHM14].

Pseudonymous [BDFK12].

Pseudoprime [DW12].

Pseudorandom

Pseudorandom [AS17, BCGH11, BK12a, Kla10, MFG16, CP13, GCH15, HRV10].

Pseudorandomness [Shi10].

PSMPA [ZLD15].

PSO [TLL13].

PSPACE [JUW10].

Public

Public [Ano11b, ABW10, BVS13, BB14, BKL12, BKKV10, CT18, CLP13a, Che15, CNT12, Cou12, FB12, GKS17, HT15, HLH19, IM14, JLT12, KFOS12, LLSW16, LP10, LSQ18, LZC14, LH18, MZH15, MPP14, MTK11, Mat14, MP12, Muf16, NDT12, Orn16, PDNH15, RSBGN12, RW12, RBHP15, SG18, Sa12a, SK12b, SM10, Sia12, SC12, SLY16, SGP17, SVT10, TMC15, TT12, WP17, WZ15, WWHL12, Wil18, XNK15, XXZ12, Xio12, XJWW13, YL17, YKC11, YFK12, YM17, ZYY17a, AA14, AT17, BS15, BSW12, Dur15, HZWW17, HL14, HTC17, LSNB14, LLY15, LFWS15, LH13, LL16a, RPSL10, SES16, SY15b, VN17, YTT11b, YYS16, ZZ11, ZCC15, ZCL19, ZY17b, FB12].

Public-Coin [CLP13a, Mat14].

Public-Key [BVS13, BKKV10, GKS17, KFOS12, LL18, MPP14, MP12, NDT12, Orn16, PDNH15, RSBGN12, RW12, SK12b, SW10, Sia12, XNK15, XJWW13, YKC11, YFK12, ZY17a, ABW10, IM14, LPS10, LZC14, BSW12, RPSL10, SES16, VN17, ZCC15, ZY17b].

Publication [ZTL15].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publish/Subscribe [DLZ16b, OFMR16, PRSV17, TKR14, YSM14].

Published

Published [MYYR13].

Publisher

Publisher [Ful10, Mur10].

Publishing

Publishing [ZTL15].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publish

Publish [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publish/Subscribe [DLZ16b, OFMR16, PRSV17, TKR14, YSM14].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publish

Publish [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publish/Subscribe [DLZ16b, OFMR16, PRSV17, TKR14, YSM14].

Published

Published [MYYR13].

Publisher

Publisher [Ful10, Mur10].

Publishing

Publishing [ZTL15].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publish

Publish [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publish/Subscribe [DLZ16b, OFMR16, PRSV17, TKR14, YSM14].

Published

Published [MYYR13].

Publisher

Publisher [Ful10, Mur10].

Publishing

Publishing [ZTL15].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publish

Publish [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publish/Subscribe [DLZ16b, OFMR16, PRSV17, TKR14, YSM14].

Published

Published [MYYR13].

Publisher

Publisher [Ful10, Mur10].

Publishing

Publishing [ZTL15].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publish

Publish [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publish/Subscribe [DLZ16b, OFMR16, PRSV17, TKR14, YSM14].

Published

Published [MYYR13].

Publisher

Publisher [Ful10, Mur10].

Publishing

Publishing [ZTL15].

Publicly

Publicly [NMP12, SZQ17, YNR12a].

Publish

Publish [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].

Publicly

Publicly [BGP17, DLZ16b, OFMR16, PRSV17, SL11, TKR14, YSM14].
Quantum-Oblivious-Key-Transfer-Based [WCL +18]. Quasi [BGJT14, OWHS12, OTD10, BGJT13].
Quasi-Chirp [OWHS12]. Quasi-Cyclic [OTD10]. Quasi-Polynomial [BGJT14, BGJT13].
R [BS12, LVV11, PP10b, WYW14].
R3579X [BDK11]. Rabbit [FSWF11].
Rabin [Chi13a]. Radial [pNyWyYp +14, CG12b]. Radio [KAKHB17, CJP12, CJP15, EA12, Kim11, NLYZ12, RPC12]. radio-frequency [CJP12, CJP15].
radio [GKCK11].
RAGuard [ZH +19]. Rail [HF14b].
Raising [YWW10]. RAKAPOSHI [IOM12].
RAM [RYF +13]. Ramanujan [KK10].
Randomized [ARP12, GT12, HHR11, SR12b, BWA13].
Randomness [AY14a, Ana14, ABF12, ACM +17, BWLA16, MS10, MS16, DTZZ12, FRT13, RY10, TC11].
Range [DCA18, HMCK12, JCHS16].
Rank [SS10b, FES10].
Ranked [CWL +14, XWSW16, GZS +18, LXK +14].
Ranking [ZDL12, AT10]. Rapid [KPC +16].
Rare [Sch11]. RASP [AZPC14]. RASP-QS [AZPC14]. Rate [LJK17, PPS12b, PCPK14].
Ratio [FHKP17]. Rational [CK18, KU14, KOTY17, NS12, TWZ11, ZC13].
Rationality [GLR10, GLR13].
RBAC [VN16]. RC4 [GC +13, Loc15, Rec15, RS14, Sar14].
RC4-like [RS14].
Re [ABR12, GSW +16, GZXA19, KKA15, LSLW15, LSC12, LBR12, MLO17, NAL17, Pet12, PRSV17, WY10, XJW +16, BGP +17, CFZ +10, CLH +16, CZ15b, FSGW11, FSGW12, FXP12, GH12, HWDL16, HYF18, KKM +14, LMJC11, LCT +14, LFS15, LL16a, SYL13, SLZ12, SKB +17, Tia15, WGJT10, WHY +12, Wan18, WLS14, XXX15, YZCT17, ZDW +16, LAL +15].
Re-authentication [LBR12, FXP12, LMJC11]. Re-Encryption [GS +16, KKA15, LSLW15, MLO17, NAL17, PRSV17, XJW +16, ABR12, GZXA19, LSC12, Pet12, WY10, BGP +17, CFZ +10, CLH +16, CZ15b, FSGW11, FSGW12, GH12, HWDL16, HYF18, KKM +14, LCT +14, LFS15, LL16a, SYL13, SLZ12, SKB +17, Tia15, WGJT10, WHY +12, Wan18, WLS14, XXX15, YZCT17, ZDW +16, LAL +15].
re-signatures [Tia15].
Reachability [SVG16]. Reactive [JR13].
Read [LLPY19, Sto12]. Read/Write [LLPY19]. readers [HDPC13]. readership
Robustness [HTG15, YKBS10, AEH17].

Rotational [KN10, KR10]. Roulette [Ber17]. Round [Ber17, jCPB+12, COP+14, DWZW12, GGH14, KOTY17, KMO14, LWZ12, LJ17, Pan14, TYM+17, XZLW15, Yun12, AY14b, ABM+12, Blo15, LP11, LFW+16, Sun11, TSSL11, TQL+14, TCS14, XW12]. Round-Reduced [DWZW12]. Rounds [GST12, Sas12, LYHH14, MNP12]. Router [Bis17, SA15]. Routing [Ham12, KZG10, WLY+15, LSG16, LC17].

RSA [Dun12b, Kia11, Pie10, APPVP15, BBBP13, Bro17, BNST+17, CLSW12, Chm10, GM13, GST13, Her14, Hin10, HLYS14, IK15, KHHH14, KFL+10, Lim11, Moot12, SM10a, S10b, SLM10, TK19, Win17, YHK+10, YXA+16]. RSA-1024 [Bro17, Win17].


Rule-Based [TW12]. Rumor [FKOV15]. Run [IF16]. Run-Time [IF16].

Scan [LWK11, DDFR13, KPS10].
Scan-based [LWK11]. scanning [Ara13].
Scattering [KA18]. Scenarios [DSB15].
Schedules [Pud12]. scheduling [MV16b].
Schema [AN12]. Scheme [ASS15, Bai10, BHG12, BS14, BKJP12, BDHI1, CMLS15, CLEL16, CCM+10, CLHC12, CHHW12, CCZC13, CGY+13, CLHI3, CSW12, DA10, DS11, DKS12, FGM10, GZZ+13, GH11b, GJ1Z17, GLW12, GZH17, HYS11, HIDFGPC15, HMR12, HH17, Hli13, HLH19, HP12, IL15, JSZS12, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KLM+12, LSL12b, LHF12, LTH+15, LTY16, LH11b, LGWY12, LTC+15b, LYY+18, LGPRH14, MWZ12, MVRI12, MRL+18, MN12, MSas12, NX13, NLLJ12, NLY15, Pet12, PDI12, RVH+16, RMG18, SK12a, SJ12, SGP+12, SD12, SHe14, ST16, SP15b, SJWH+17, SSA13, Tan11, TTD13, TWZ11, WYO10, WgMdz12, WgMW12, wWpNyY+14, WLH15, XWSH16, XHC+12, CXWJ13, YMI16, Yami12, YZ1X+12, Ye10, Ye14, YTH17, YL17, Y+17, YHK+10, YMWS11, ZPM+15, ZZQ+19, ZC13, ZQK15, ZLDD12, ZY17a, AMN18, AHS14, APK+18, ACK+17, BOB13, BAL10, BMM12, BB16b]. scheme [CCLL11, CLSW12, CH10, CT11a, CLJH13, CW14a, CTH13, Chol14, DSCS12, EAA+16, EZ15, FLL+14, Far14, FA14a, FH1Z18, GZH12, GJ13, GMRT+15, GPLZ13, GLM+16, GH16, GAI+18, GTSS19, HZ1W18, HBBRN16, HL11, HCC11, HL16, HCC10, Hwa11, IB11, JNU17, JKAU19, JLT+12, JZS+10, JM1W+16, KI11, KPP16, KDIH15, KK13, KHMB13, KKM+13, KMM+14, KKG14, Kim16, KIH19, KP18, KLM+16, KDW+17, KWH16, KL11, LXLY12, LZ1+16, LSR13, LH10c, LZ1X10, LNMI+11, LM1C11, LK12, LHLS12, LNK13, LK+17, LNK+18a, LWK+18, LNK+18b, LFW15, LH13, LHH11, LW110a, LWL11, LW13b, LZ14, LDZW19, LL16a, LL16b, LW12, MCF+18, MMS17c, MK12a, MSas13, NR17, Nos14, PZBF18, QM17, QMW17, RPSL10, SGGR+16, SM11, Tan12b, TY16a, TK14, TD14, TLL13, TLL12, UUN11, WWY11, WWYY11, yWpNyL11, WLH13, WDZL13, WLY+16, WLF17, Wan18, WDKV19, WZ11, WKL11, WOLS12, WXX+17, XHH12, XWZW16]. scheme [XMX14, XXX15, XM13, YC11, YC16, YJH18, YW+10a, YCT15, YXD18, YQOL17, YM10, ZYL+10, ZLY10, ZX+14, ZYC+17, ZP.CV12, ZZ+17, Zy17b, ZF+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12]. Schemes [ABF12, BV5+13, BF12, BBEPT14, BS15, CMLRHS13, CGL+12, Chu11, Des10b, FHKP17, FL12, HSM14, HLLG18, HPO+15, LWL10b, LZ1K4, MLCH10, MR14b, MMS17b, MFB18, MKRM10, Ob11, PB12, PDNH15, PH12b, Sc10, Shi11, SHK17, SSU12, VSR12, WGP16, YNR12a, YNR12b, Yek10, YWZ+12, AGH14, AN15, AHL+12, CDGC12, CJXX19, CHS11, CCG10, CTL13, DDD14, DD13, DZ14, FPBG14, FMP12, FMA+18, HD16, HM10, KT1U16, LHZ12, MM12, MA17, Nzl1+15, QYWX16, SES+16, Sar10a, Sar11, sSZZ15, SAR18b, WW14, Y11b, ZCL+12, ZCL14, ZT14]. Schneier [Sev16]. Science [Bow11, G12, Gas13, IEE10, IEE11b, Ter11, Bai12, PWH1M0, Pet11]. scientists [Goo12]. Scientometric [Pal15, Pal16]. Scope [Bai12]. Score [GCSAddP11]. scoring [OSSK16]. Scrambling [LL17a]. Screen [SPW+16, CTL12]. Script [Rao10, Bax14]. Scripting [DSB15]. scroll [GMOGCCC15]. SDB [HMK+15]. SDDO [PL16]. SDDO-based [PL16]. SDH [GMS11]. SDIVIP [YNX+16]. SDN [KCC17]. SDVS [Wan10]. SE [LL13]. SE-AKA [LL13]. seals [MN10]. Seam [LC15]. Seam-Carved [LC15]. Search
[CWL+14, Che15, DCA18, FRS+16, GTT11, HCDM12, HLH19, LSQM18, TMC15, WDC18, WW12, XWSW16, XJWW13, ZXYL16, BL11, CLH+16, FH13, FSGW12, GZS+18, HH16, OSSK16, SY15b, WHY+12, WXLY16, XWY+18, YD18, YQOL17, ZJ11]. Searchable [BHJP14, CWWL12, CLW16, CGKO11, FJHJ12, PCY+17, XNKG15, ZZQ+19, DLZ16a, DRD11, HQZH14, HCTS16, LZC17, LL+18, RPSL10, WXLY16, WCCH18, YZCT17]. Searches [Sia12, WR15]. searching [GPN+12]. Seattle [LCK11, KCR11]. Seberry [AHS14]. SEC [PA10]. Second [AKY13, ABM+12]. Secondary [RS11]. Secrecy [ABD+15, BKST18, KZG10, TSH14, Yon12, ATKH+17, Bia12, RCW15, TCS14]. Secrecy-preserving [TSH14]. Secret [ASN11, ASN12, ADH17, Ayu12, Bai10, BBB+16a, BFM12, BBEPT14, Bri11, CCM+15, CFOR12, CCL+13, DR12, Dew11, EM12, EA11, FFHP17, FR16, Foki12, HYS11, HLI0a, Has16, JLS12, KU14, KS18, KOTY17, KK12, KK13, KSSY12, KS15, LH12, LPL15, Lin15, LCCJ13, LTC+15b, LJ16, LLKA19, Men13b, MNS11, NS12, Ob11, PCPK14, QSH18, SLL10, SC10, SS10c, SSU12, Sti15, TLLW12, TWZ11, WKB16, WGF16, Wu18, XZY+12, XJR+17, YFF12, YWZ+12, ZCL13, Ald11, ADG16, AKK+17, Ara13, BJ16, Bud16, Cha13c, CT11b, CW14a, CLZ+17, DD13, EEAZ13, EZ15, FH10a, GJYM15, GLW13, HF14a, HH15, Hea15, HBBRNM+16, HCC11, HLC12, KI11, KTU16, LLY12, LT13, LYSZ10, LHYZ12, LEW19, Mas17, Mck10, Mck11, Mck12, MB11, OO10, Pea11, Pet11, QD16, Rus15, SB17, SA12, SAR18b, TQL+14, TD14, UUN11]. secret [UUN13, WYL13, WZ11, WS12, WOLS12, Wu17, XW13, YC11, YCC16, YSC16, ZCL+12, ZZ15, ZPYW12, LSC+15, Bai12]. secret-key [BJ16]. Secret-Sharing [BBEPT14]. Secretion [RSCX18]. Secretocracy [Ber16b]. Secrets [BT12, CG14b, DLWW11, FMS12a, Kob10, Man13, Bha16, Cop10b, GGH+16b, Gup15, HRS13, Smi11a, AnQ17b]. Secure [ADMM16, AARJ12, Ash14, AMH+16, BVS+13, BWLA16, BCGH11, BCG12a, BQ+13, BWA13, BHLJ12, BHJP14, BF11, Bru12, BDH11, BCGM15, CFOR12, CCM17, CZF12, CZL14, Che15, CMA14, DM18, DL15, DMS+16, DG15, DLZ+16b, Edw17, FLH13, Fri10b, FD11, FSX12a, zGXW12, GKM16, GGH14, GFBF12, GT12, GV14b, GHKL11, GMI4, GZS+18, Hv112, HSM14, HLLG18, Har16, HL10b, HP14, HTZ12, HMCK12, HLM115, HYS18, HK14, HLH19, IL15, Jac16, JH19+19, KW14, KME+12, Kup15, KH10, LJS+14, LL15, LH12, LYZ+13, LTH+15, LIT16, LSLW15, LLC16, LSLQ18, LY15, LHL15, LLML12, LSC12, LMO17, MMP14, Mal13, MVVR12, MMS17b, MK12a, MKA17, NZP17, NG+17, NR12, NMS14, NSMS14, PB12, PSM17, Per13, PRN+19, QZL+16b, QZDJ16, QZ18, RMP10, Rea16, RSGG15, SAM+19, SN11, SZ14, SVC15, SP15b, SKH17, SRA17, SAR18b]. Secure [SSAF11, SVG16, SYW17, SYC+17, SMS14, SZDL14, SGH15, SY+16, SR12b, TB18, TCL15, TWZ11, TG12, TGC16, VM15, WgMW12, WKB16, WXLY16, WLY17, WDC18, WHL15, WBA17, WWHL12, WMS+12, tWmC12, XW16, XJWW13, YNR12a, YNR12b, YTH17, YHK+10, YKC+11, YAM+15, YGD+17, ZXX+11, ZDL12, ZV14, ZVG16, ZHT16, ZLW+17, ZH+19, ZBR11, AHS14, APK+18, ABBD13, ACF16, AKK+17, ACD+15, BOB13, BSR+14, CCLL11, CSD18, CLHJ13, CW14a, CS11, CDL18, FHH10a, FLL+14, FSGW12, FA14b, FIO15, FS18, Gal13, GAI+18, GLL+18, GCH15, HGWY11, HWK+15, HLYS14, HTC17, HPY10, IB11, JZS+10, KPP16, KKA14, KRM+10, KTI16, KDW+17, LLLS13, LDDA12,
secure [Tar10, TLMM13, TLL12, VS11, WLZ+16, WMX+17, WDKV19, WCCH18, WL19, WXXC14, XXX15, YC12, yYqWqZC13, YZZ+14, YZCT17, YQOL17, YY11, YLS12, YMSH10, ZLY10, ZC15, ZZ15, ZYC+17, ZG10, ZZ12, ZX11, ZY17b, ZC12, Zhu13, ZSW+18, Ano12, DSB18, HRK18, OKG+12, YSS14, YFK+12].

Secure-TWS [OKG+12]. Secure [LC17, SGG18].

Security [SNJ11, SBS+12, Sar12, Sch13, SD12, Shi11, SLM10, STC11, Sti19, SMOP15, SGW+14, Tso13, TV15, Wal18, WYCF14, WSA15, WSS12, WCL+18, WS14, Yan10, YZLC12, YSF+18, YGS+17, YSS14, You11, Zha15b, ZY17a, vTJ11, AMN18, AB10a, Abe10, ABGR13, ABM+12, Ano11a, ADH17, BYL10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTHP13, CLCZ10, CVG+13, DLK+16, DWH+13, Edw14, FHM+12, FA14a, Fei19, Fis15, GHD19, GM16, GLM+16, GMS11, GH12, HWD16, HWG10, HLR11, HRS13, HLV10, KSA16, KKK+16, Lan10, Lan13, LH10a, LMXW12, LHH11, LZC14, LSG16, MZA+13, Men13b, MM14b, MSM+18, NS10, Nam19, NCL13, NLYZ12, OK18, OYHSB14, PHWM10, QYWX16, Rec15, RPSL10, RH10, SA12, Ser12, SLZ12, SY15b, Sir16, Sta11a, Tan17b, TOD18, UUN11, VCK+12, WCFW18, XCL13, Zha15a, XW12, YKC+12, Bar12].

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

Self-Controllable [ZLDC15].
XNKG15, XZY+12, YFF12, YWZ+12, ZC13, AKK+17, ADH17, CT11b, CW14a, EZ15, EA11, FGMP12, GPLZ13, GJMP15, GLW13, GLB+18, HF14a, HBBRM+16, HCC11, HYL12, HYF18, KI11, KTI16, KPBI7, LXLY12, LT13, LFSW15, LAL+15, LyWSZ10, LHY12, LHL15, LLL+18, LEW19, LL16a, Mas17, OO10, OO18, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WLS14, WKL11, WOL12, WOL12, WOL12, YC16, ZCL+12, ZZ15, ZPWY12, SLL10.

Solved [Smi11b]. Small
[BGJT14, BKLS12, BB10, CJ13, Kim15, LCLL15, YM16, AAT16, BGJT13, Jou13].

Some
[Ano17c, BB10, Bul10a]. Some
[AD12, Ber12, Dur15, LWL10b, Mid10]. Somewhat [HTC17, KOS16, MBF18]. Song
[Con12]. Sood [MWZ12]. SOSEMANUK
[PC16]. SOT [PAF18]. SOT-MRAM
[PAF18]. Sound [COP+14, LSR13, Sav15].
Source [Bis17, FKOV15, MBC15, RWLL14, ABF+14, LZC17, PX13, Pow14].

Source-Based [MBC15]. Sources
[DHB16, BJ16, SSY12]. South
[BL10, LW11a]. Soviet [Bud16]. SP
[Sas12, SEHK12]. SPABox [FGR+17].
Space [BWR12, BKL+13, NRY+14, RMG18, MSM+18b, RYF+13, ZZ15].

Space-Filling [BWR12]. Spaces [SH15]. spam [SKEG14]. Spanish
[Pet11, SGGCR+16]. Sparse
[AGW15, AAT16, BBC+13]. SPARTA
[MMS+17a]. SpartanRPC [CS14]. Spatial
[AV12, CZF12, PDMA12, CW14b, NZL+15].

Spatial-Temporal [DMT12]. Speaker
[BJCHA17, PPR12]. Special [Ano13d, Ano16a, Ano16b, Ano16h, AB10b, CSYY18, GO17, LW13a, LLK18, PHWM10, XW13].
Specific [BD15, BDFK12, KME+12].

Specification [HZS+19, SK11, SD10]. Specifications [BMP12]. SPECK
[DFW+16, AMKA17, BSS+13]. Spectrum
[KD12a, TZW+12, XNRG15, KP17, LWY12, MMS13]. Spectrum-Based
[TZW+12, XNRG15]. Speech
[AGW15, LJK17, SAA15, YMA17]. Speed
[ARM15, GL12, HZ11, KP17, LTK16, BDL+11, KL13]. Speeding [RVRSCM12].
Speedup [Che18]. SPEKS [Che15]. spell
[Bha16]. Sphere [Sti19]. SPHINCS
[BBH+15]. Spies
[Has16, Keb15, Fag17, Mac14]. Spintronic
[IGR+16]. Splicing [YSC+15]. Spline
[Tan12a]. Split [CG14a, XYZ+12]. Split-State
[CG14a, XYZ+12]. Splttable
[CP13]. SPN [LCLW17]. Spoken
[WBC+10]. sponge [BDP11].
SPONGENT [BK+13]. spongy [RS14].

SpooF [SP15a]. spotty [OS11]. Spread
[HGT15, KD12a, PSJ+13, TZW+12,
T [SJWH+17]. T-Chain [SJWH+17]. Table
[CCL+13, AY14a, LDDM12]. Tables
[PTT16, XHI14]. Tag [NNAM10, PPH12, CJP15, SLPHC14, CJP12]. Tags
[MO12, HSH11, HDPC13, HQY+16, LEW19, MK12a, PLSwLe10, 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 [SAS13]. Tampering
[CG14a, SRAA17, SGP+17]. TAO [Sta13].
Taormina [Cra12]. tap [ADG16]. target
[HRS16]. Targeted [ABJ13]. Tasks
[Abe12, FKS+13, CL16]. Taxonomy
[AJA16, GAF+15, KSM15, MA17]. Taylor
[Joh10]. TCC [Cra12, Lin14b, Sah13]. TEA
[CWP12]. Teaching [GY13]. Team
[LJS+14, Fpl10, Ant14]. Tear [Boy16].
Tear-Free [Boy16]. TEASE [ZBR11]. tech
[Ano15e]. Technical
[Sir16, TS16b, Wag16, JW14, Suc12].
Technique [HEK18, KBL11, ZLD14, BBBP13, CPPT18, GCSÅddP11, Nam19, SM12, SKS+18, TS16a, ZWS+18].
Techniques [Bis17, DA12, GOS12, HPC10, HL10b, LW12, Mor12, PJ12, AB10b, BM13, FGPGP14, Gil10, HT13, KHF10, LH11a, OO18, VN17, WMX+17, Joh10].
technologies
[JAE10, JAS+11, Lan10, MMP19].
Technology [CGB+10, Fol16, IEE11a, Wu16, Ham19, IMB17]. telecare
[LWK+18, MA17]. Telephony [SKEG14].
Television [DTE17]. Tell [Cer14].
Template
[NGAuHQ16, SKV12, ATT+10, GCSÅddP11].
Templates [DWB12, AHM+18]. temporal
[JMWh+16, MHT+13, XMHD13].
temporal-credential-based
[JMWh+16, XMHD13]. Tenant [TV15].
terahertz [WW13]. Term
[SKV12, CFVP16]. termination [SRB+12].
Ternary [ADI11]. Test
[HTC+15, JEA+15, LLSw16, MZHY15, SS10b, WH18, HTC17, ZCL+19, Ano16g].
Testable [RMP10]. tester
[RPSL10, SY15b]. Testing
[Con12, SS12a, AY14a, BJ+14]. Tests
[GLG12, MS12b, Sim15a]. Texas [IEE13].
Text [GdM16, SMS18, XZZ18, CR12, SI12, SWW+17]. Text-dependent [GdM16].
Textbook [PP10a]. Texture [TSH17].
Theft [Ber12, Ber17, BTP15]. Their
[CZLC12b, CK18, JSK+17, NR12, CQX18, Hof16, IK15, KG10, Mat19, Sti11]. them
[HLV10, JSK+16, Rus15]. Theological
HL10b, HP14, KOS16, NSMS14, ZM16, FIO15, HPC12, HWB12, ZZC15, GHKL11.

Two-Round [GGHR14], Two-Server [YLW13, KMTG12, CSD18], Twofish [MD12a], TWS [OKG+12]. Type [AKP12, CFI13, PFS12, SH15, BNST17, SYL13, WB12]. Type-based [CFI13, 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 [AAM18, GW14, TG17, WCFW18]. ultra-lightweight [AAM18, TG17, WCFW18].

ultralightweight [ACM12, GMSW14, SB17]. UMTS [OHJ10, TM12], un-traceability [Chi13a]. Unattended [BN14], unauthorizing [MLMSMG12]. Unauthorized [CBO+18]. Unbounded [LV1c, YZ12], unbreakable [Bha16]. Uncalibrated [SGP+12].


Unconditionally-Secure [CFOR12], uncorrelated [MSM+18b]. Uncovering [FMS12a, WBC+10]. Undeciphered [Rao10]. Undeniable [BH12].


union [BBDL+17, Bus16]. Unique [SSPC12, SOS15]. Unit [PP10b, Sta13, MS13a, MS13b, MS13c].

units [ABDP15]. Universal [ASM12, BKS18, BJL12, NR12].

Universally [DN12]. Universe [LW16, FNWL18, LFZ+17]. University [Ano17b, CGB+10, Wes16]. unlike [Goo12].

unlikely [Fag17], Unlimited [IBM13a]. Unlocking [VS16]. unmanned [XZW16].


Updatable [LLPY19, LCL+17]. Update [BCE+10, KE19, LQY10, FS18, WLF17].

update [GCSAddP11, LHY18]. Upper [AMVZ12]. URLs [AY14a]. USA [Dun12b, EIE13, K11, Lin14b, Pie10, Rab10, ACM10, ACM11, EIE10, EIE11b].

Usability [RAZ15]. Usable [DL15, TGC16], usage [AKK+17, BHCdFR12]. Use [CSV15, DFKC17, KOS16, NR12, YT12, der10, CZ15b, Die12, Hof16, KK10, MBB+13, Mat19, O010, Sti11, UK18].

Used [CGCPDMG12, BM15, MS13b]. useful [dCCSB+16]. Use-net [Bel18]. User [BLV17, BKJP12, FLH13, GdM16, Har16, JN12, LLC11, LCL17, MZH15, MBC15, MDM17, Odl12, PDT12, PWV12, RV+16, SDZ14, SP+13, WgMDZ12, WgMW12, ZHS+19, ZPW16, AaBT16, ATK+17, AP+18, BT18, CH10, CHS11, CLHJ13, DSC12, GH16, GTSS19, HL14, KKM+13, KLW+16, K+17, LH10c, LNM+11, LNL13, LH13, MM12, OKG+12, hSZZ15, SHBC19, WDKV19, WT10a, WOLS12, YHL16, YSL+10]. User-centric [BLV17]. User-controlled [Har16].

User-Friendly [SZDL14, WOLS12], User-Generated [LCL17b]. User-Level [BKJP12]. user-participating [CH01].

User-Transparent [ZHS+19]. Users
[DPCM16, KKA15, TAKS10, WPZM16, ATK11, uHAN+18]. uses [Rus15]. Using [ABS+12, AB3+14, Anol5a, Ayu12, ARM15, BBC+13, BCPV11, Bee7, BFT16, BKL12, BJ+14, CST+17, CCL+13, DSB16, DR12, DA10, DBPS12, DL12, ERLM16, ERRMG15, FMS12a, GH11a, GSC17, GAS+16, HEK18, HHS+15, IL15, Jm10, JEA+15, KBL11, Lac15, Lan11, LZ+13, LLL16, MM17, MBC15, MRL+18, MS16, NIS12, NGAuH16, NNAM10, NN12, NSMS14, PMZ13, PSS+13, PAF18, PDMR12, PDT12, PCKP14, RVRSCM12, SR12a, SFE10, SSA13, SRA17, SC12, SR12b, Tan12a, TKR14, WWL+14, WgMdZ12, WY12, ZZ12, YWW10, YWW15, YCL17, YSS14, ZH15, ZPW16, ZS12, dRsR12, ATRK+17, AHM+18, APK+18, ASVE13, BL+19, BM13, CSH+18, CHS11, CR12, CLHJ13, CPI3, Cri16, Dav11, DTZZ12, uHAN+18, EEAZ13, FES10, Ham19, Har14, HZWW17, HWB12, HL14, HPY10, HCC10, HS11, JCHS16, JMW+16, KI11, KY10, KKG14, KM11].

using [KU13, KTO16, KP17, KLS+16, LXXY12, LLP+18, LC17, LH10c, LNM+11, LXMW12, LH13, LML+13, MM12, MS13a, MMSD13, MM14a, MKH+12, MRRT17, MM+18b, NTKG17, PBCC14, PC14, QD16, RS15, RS17, Sar11, SGFCRM+18, SKS+18, SAR18b, TLF16, TG17, TK14, TLL13, UUN11, yWpNyL11, gWpNyY+14, WMX+17, WH12, YQH12, YZZ+14, YSL+10, ZZKA17, ZLW+12, ZYC+17, ZZW+18, ZZL+18]. utilization [NZM10].


Vicious [NN15].

Virtual [BR14, HB17, RY10, VDO14, CDA14].

Virtualization-Based [CDD13, QZDJ16].

Virus [WOLP15].

Visible [Cas10, HWYW14, LZC+12b, WZLW13, Lin14a].

VCTest [DP12], DGT12, GKR12, GKR13, HS12, OL12, YYG12].

Visitors [XGGG+14].

Vista [Bac10].

Vista-Driven [SP12].

Vitamins [ARR13].

Vivital [JG13].

Vixen [Cas10].

Vlad [KPS10].

Vladimir [KPS10].

Vladivostok [KPS10].

VLAN [MD11].

VLAN-Tagging [MD11].

Volume [XL12].

Volcanic [CPS15].

Volcanic Ash [CPS15].

Volcano [CPS15].

Voltage [BBBP13].

Voluntary [WGJT16].

Voting [Ber16a, CFE16, CRST15, LHF12, LGPRH14, RST15a, RST15b, Sch10].

Voytci [L01].

W [Mar10a, Xie12, Hüll13].

W-OTS [Hüll13].

WA [LCK11].

Waknaghat [CGB+10].

Walker [Xie12].

Wallet [Chi13b].

Wallets [Chi13b].

War [Has16, Mun17, Bud16, Car11, Sm11a].

Warbler [MFG16].

Wars [Bud16].

wartime [McK10, McK11].

was [Goo12, LHA+12].

Watermark [CHHW12, DLM+18, EMW14, Jin10, KBL11, LZC+12b, MCD12, SJ12, YE12, ZS12, HB12, TLL13, WYL13].

Watermark-Driven [DLM+18].

Watermarking [BCGAM12, BF12, BCV11, BDB14, BMM15, CG12b, CHHW12, CCZC13, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HEK18, HGT15, HMK14, JSS12, Joh10, JKH12, KD12a, LSL12b, LP12, LD13, MM17, MR16, MU12, NGA15, NC12, NY+17, pNyW14, OWHS12, RS16, RP12, RR11, RMI18, SA15, SLG12, SSA13, TB18, TW+12, TC10, WHZ12, WLZ12, WYW+13, gWpN14, WXL+17, wWX18, rWmC12, XNG+14, XNR15, YWN15, YPR17, YK18, YY15, ZZX+11, AP10, AIA+18, AMK12, BW13, BWA13, CCLL11, CT11a, CSS+13, GZHD12, GA11, HKB14, HWYW14, JK13, KPS10, KJN+16, KM11, LRS13, LXC11, LLS12, Lin14a, LWY12, MMS13, MM14a, MO14, MK11, NC13, PTK14, PWL13, PWW10, PGL10, PWS18, PC14, PPR+12, RS17, SSK+18, Tay14, TK14, TTT10, TP12, WLDB11, wWpN11, Wan13, yWpWyY13, WZLW13, WYT+12, ZZZ17, ZMS18].

Watermarking-Encryption [SLG12].

Watermarks [GL10, YT12].

WAVE [BMM12].

WAVE-enabled [BMM12].

Wavelet [AGW15, LSL12b, MR16, Ara13, AMK12, BW13, LXC11, MO14, wWpN11].

Wavelet-Domain [MR16].

Weak [BF11, DY13, HDW12, PYM+15, Pud12, GJMP15, RH10].

Weakening [SFKR15].

Weaker [Sas12].

Weakness [AMOR13].
REFERENCES


References


[AACB17] Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel,

[Arora:2012:ILM]

[Akleylek:2016:SPM]

[Aghili:2018:ISA]

[Alizadeh:2016:AMC]

[Abdalla:2010:PCL]
Michel Abdalla and Paulo S. L. M. Barreto, editors. Progress in cryptography — LatinCrypt 2010: first international conference on cryptography and information security in Latin


[ABBD13] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François

Arnold:2012:ICC


Atenieise:2017:LCS


Ambrosin:2017:OBB


Adrian:2015:IFS


Agosta:2015:OPP

Giovanni Agosta, Alessandro Barenghi, Alessandro Di Federico, and Ger-


10.1007/978-3-642-33272-2_1.


Avoine:2016:SSP


Aid:2013:DIO


Acar:2013:SPA


Andreeva:2012:SAS

REFERENCES


**ALMashrafi:2012:AIM**


**Applebaum:2010:PKC**


**Arias-Cabarcos:2015:BIP**


**Arnold:2015:NGH**


**Amoah:2016:FMA**


REFERENCES

80


Adikari:2011:HBT


Abdalla:2012:LBH


Andrychowicz:2016:SMC


Araldo:2018:CEC


Ahmed:2017:IRD


Attrapadung:2015:RGS

(print), 1460-2067 (electronic). URL http://comjnl.oxfordjournals.org/content/58/10/2698.

Antonopoulos:2017:DIS


Akinyele:2014:MGA


Abdullaziz:2016:AAI


Ahani:2015:SRB


Attrapadung:2012:ABE


Ali:2018:ECM


**Appelbaum:2013:SSG** [AHS13]


**Ak:2014:ICS** [AHS14]

Murat Ak, Turgut Hanoymak, and Ali Aydin Söçük. IND-CCA secure encryption based on a Zheng-Seberry scheme. [AIB+16]

**Amin:2016:DAP**

REFERENCES


REFERENCES


REFERENCES

Armedo-Moreno:2010:JRA

Arsalan:2012:IRW

Ahir:2017:LAR

Abbasinezhad-Mood:2018:DHI

Adj:2013:WDC

Aumasson:2014:HFB
Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan, and Luca Henzen. The Hash Function BLAKE. Informa-
REFERENCES

Ahmadian:2010:PDS

Alvarez:2012:CAB

Albrecht:2012:SDL

Arshad:2015:SAI

Aga:2017:ISM

Anawis:2014:ARR
Mark Anawis. Applications for randomness: Random


Anonymous:2012:SHS


Anonymous:2013:DSS


Anonymous:2013:NCI


Anonymous:2013:SSD


Anonymous:2013:SIS


Anonymous:2014:ERE


Anonymous:2015:BSU

REFERENCES


Anonymous:2015:BRDa


Anonymous:2015:CEB


Anonymous:2015:QCS


Anonymous:2015:UGB


Anonymous:2016:CPSd


Anonymous:2016:CPSe

Anonymous. Call for papers special issue on postquantum cryptography. IEEE Security & Privacy, ??(??):??, ???.

[Ano15b] Anonymous:2015:BRDa


[Ano15c] Anonymous:2015:BRDa


Anon Anonymous:2016:EMT


Anon Anonymous:2016:FVM


Anon Anonymous:2016:GUP


Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

describes how SHA-1 collision attacks could lead to 
rogous, and malware, file 
downloads via BitTorrent. 
the obvious solution, which 
and multiple checksum algorithms, 
and require all to match 
before concluding that two 
files are in fact identical.

Anonymous:2017:BRM

Anonymous. Book review: 
*The Mathematics of Sec- 
tests*, by Joshua Holden. 
Princeton University Press. 
CODEN NTSCF5. ISSN 1353-4858 (print), 1872-9371 (electron- 
science/article/pii/S1353485817300247.

Anonymous:2017:CCS

Anonymous. Cybernet- 
ica case study: Solv- 
ing the Estonian ID- 
card case. Web news 
URL https://cyber.ee/ 
en/news/cybernetica-case-
study-solving-the-estonian-
id-card-case/. The story 
[Ano17] describes a poor choice 
of generating large (about 
1024 bits) primes \( p \) and \( q \) 
that led to crackable RSA cryptography. The solution 
for Estonia was to switch to 
elliptic-curve cryptography 
that was also supported by 
the cards.

Anonymous:2017:HDQ

Anonymous. High-dimensional 
quantum encryption per- 
fomed in real-world city 
conditions for first time. 
CODEN SCHRCU. ISSN 
1930-5753 (print), 1930- 
6156 (electronic). URL 
https://www.scientificcomputing.com/news/2017/08/high-
dimensional-quantum-encryption-performed-real-world-
city-conditions-first-time.

Anonymous:2017:MBH

Anonymous. Mathematician 
breaks down how to 
defend against quantum 
computing attacks. *Re- 
CODEN REDEEA. ISSN 
2017/02/mathematician-
breaks-down-how-defend-
against-quantum-computing-
attacks.

Anonymous:2017:RV

Anonymous. ROCA vulner- 
ability. Wikipedia arti- 
cle., October 2017. URL 
org/wiki/ROCA_vulnerability. 
The ROCA vulnerability 
affects millions of smart- 
cards, and devices using
TPM (Trusted Platform Modules). It allows recovery of the private key from knowledge of the RSA public key, and thus, facilitates malicious cloning of the cards, and decrypting of some encrypted filesystems.

Anonymous:2019:HCC


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF


AlFardan:2013:LTB

REFERENCES


[AQD12] Garsah Farhan Al-Qarni and Farzin Deravi. Explicit integration of identity information from skin regions to improve


[AS16] Gilad Asharov and Gil

**Artemenko:2017:PGO**


**Andrade:2016:LEP**


**Asharov:2014:TCC**


**Al-Sinani:2012:UCB**


**Ahmadi:2011:SKC**


**Ahmadi:2012:SKE**

REFERENCES


**Al-Tariq:2017:SFP**


**Alam:2015:ACF**


**Aslan:2016:DEM**


**Abdalla:2012:LRS**


**Altaf:2017:LHL**


[AZF+12] Anya Apavatjrut, Wassim Znaidi, Antoine Fraboulet, Claire Goursaud, Katrina Jaffrès-Runser, Cédric

**Alshammari:2011:CET**


**Alavi:2014:RQE**


**Behnia:2013:IEB**


**Blaner:2013:IPP**


**Brennan:2012:ASC**


REFERENCES


**Bax:2014:PPD**


**Baylis:2010:CC**


**Bulygin:2010:OSS**


**Bennett:2014:QCP**


**Barenghi:2016:FBS**


**Boumerzoug:2016:LKM**

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


REFERENCES


Bernstein:2017:SRD

Boldi:2012:IUG

Bollman:2015:PWI

Bernstein:2011:PCI

Basin:2014:KYE

Bocu:2018:HEB
R. Bocu and C. Costache. A homomorphic encryption-based system for securely managing personal health

**Bichsel:2012:DMA**


**Badrignans:2010:SSA**


**Balfanz:2012:FA**


**Bugliesi:2015:ART**


**Buhrman:2014:PBQ**


**Bahri:2016:CCO**

Leila Bahri, Barbara Carminati, and Elena Ferrari.


REFERENCES

Beunardeau:2016:WBC


Bitansky:2013:SNI


Brandenburger:2017:DTC


Bernstein:2014:CKR


Basin:2012:PRI


Basin:2013:PRI

David Basin, Cas Cremers, and Simon Meier. Prov-

**Basin:2015:ISC**


**Bicakci:2013:LSS**


**Botta:2014:PCI**


**Boyle:2014:EO**


**Basso:2011:BWC**

REFERENCES


REFERENCES

[Baschos:2015:EFB]

[Baschos:2011:XP]

[Backstrom:2011:WAT]

[Baschos:2011:XPF]

[Barbareschi:2018:PBH]

[Bosquet:2016:EPA]
Bendlin:2011:SHE


Bertoni:2011:CSF


Bertoni:2012:KIO


Boldyreva:2012:SSE


Bitansky:2013:WFS


Bertoni:2011:CSF


Bertoni:2012:KIO


Boldyreva:2012:SSE


Beebe:2017:MFC


[Ber18] Stefano Berretti. Improved audio steganalytic

**Bouman:2011:SAW**


**Bas:2012:BLK**


**Bhargavan:2012:VCI**


**Barthe:2014:PRV**


**Bobba:2010:ABM**

REFERENCES

Bhargavan:2016:MVP

Beimel:2012:SSS

Berger:2016:EGF

Boldyreva:2014:MEW

Battistello:2012:TBA

Barthe:2012:CACb
REFERENCES


[B&DG+17]


[B&G15]


[B&G+16]


[B&G16]


[B&G+17]

REFERENCES


REFERENCES

119


Biagioli:2012:CCS


Beimel:2014:CCW


Biswas:2017:SA


Brumley:2010:CAI


Boche:2016:DSK


Bouraoui:2017:HAE

REFERENCES

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


REFERENCES


[BKLS18] Dan Bogdanov, Liina Kumm, Sven Laur, and Ville Sokk. Implementation and evaluation of an algorithm for cryptographically private principal component analysis on genomic data. IEEE/ACM Transactions on Computational Biol-


Bellare:2012:IBL


Bogdanov:2011:BCF [BL10]


Bothe:2013:EFS


Bibak:2018:AUH


Byun:2011:SMC

Jin Wook Byun and Dong Hoon Lee. On


Benzaid:2016:FAW


Bai:2019:LMD


Blomer:2012:TKG


Blondeau:2015:IDA


Buchmann:2017:PCU


Bernstein:2012:SIN


Biswas:2012:IBA


Backes:2012:GCP


Banik:2012:DFA


Babamir:2014:AKP


Buckley:2015:RVV


Bunder:2017:GAR

REFERENCES


REFERENCES


REFERENCES


Bojinov:2014:NMC

Basin:2011:AIS

Beaulieu:2013:SSF

Batina:2012:HEB

Broustis:2012:GAN
REFERENCES


Buchmann:2010:EKG


Bulygin:2010:CA


Burke:2011:AMD


Brakerski:2011:EFH


Brakerski:2014:EFH

Zvika Brakerski and Vinod Vaikuntanathan. Efficient

**Bitansky:2018:IOF**


**Bayrak:2012:AII**


**Bogdanov:2012:ZCL**


**Bhatnagar:2013:BIW**


**Bai:2016:ALC**

REFERENCES


REFERENCES

137


Carter:2010:TB


Carlson:2011:JRW


Casselman:2010:VC


Cobb:2013:LMS


Chang:2018:DMU


Cachingin:2010:EKS


Chang:2014:RRT

Chin-Chen Chang and Ting-Fang Cheng. A reliable real-time multicast authentication protocol with provable accuracy. *Fundamenta Informaticae*, 131
Chadha:2016:AVE


Chretien:2015:SPP


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO


Checkoway:2016:SAJ

Stephen Checkoway, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Ho-vav Shacham, and Ralf-Philipp Weinmann. A systematic analysis of the Juniper Dual EC incident.
REFERENCES


Chadha:2012:AVE


Chatterjee:2016:TAD


Chou:2013:UGS


Chatterjee:2017:PBS


Cascudo:2015:SSN


Chatterjee:2017:PBS


**Cho:2014:DGA**


**Chen:2011:EAA**


**Chu:2014:KAC**


**Chen:2010:ALD**


**Chen:2013:WSB**

REFERENCES

Chiasson:2012:MWB


Cui:2016:RD


Criswell:2014:VGP


Cheng:2013:DVB


Ciriani:2010:TPA


Ciriani:2010:CFE


Ciriani:2010:CDFS

REFERENCES

Choo:2016:CCT


Cao:2012:ITM


Chari:2010:DSC


Cui:2018:ABC


Coras:2016:AML


Costello:2014:CAS

Ceruzzi:2014:HFT


Cerf:2015:CTN


Cerf:2018:CSA


Chang-Fong:2016:CSC


Carter:2013:SSA


Centenaro:2013:TBA

REFERENCES

Checkoway:2014:PED


Cevallos:2012:USR


Carstensen:2011:AAA


Calzavara:2017:SWJ


Celesti:2016:ALT


Choo:2017:EDF

Kim-Kwang Raymond Choo, Yunsi Fei, Yang Xiang, and Yu Yu. Embedded device forensics and security. ACM Transactions

**Chang:2010:PRN**


**Chen:2010:IFA**


**Camenisch:2012:EAA**


**Che:2012:WAM**


**Cheraghchi:2014:NMC**


**Corrigan-Gibbs:2014:KS**

146


[Curtmola:2011:SSE] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions

**Cheng:2012:PAI**


**Chandran:2014:PBC**


**Chen:2010:NUP**


**Chang:2011:DEQ**


**Chan:2013:OCK**

REFERENCES


Chen:2018:ESA


Chen:2012:SRF


Chien:2013:CR


Chirgwin:2013:ABB

R. Chirgwin. Android bug batters Bitcoin wallets. The Register, ??(??): ??, 2013. URL ????.

Chien:2016:GAI


Chmielowiec:2010:FPR

Andrzej Chmielowiec. Fixed points of the RSA encryp-
REFERENCES


REFERENCES


Chang:2019:GTS


Chandra:2011:AST


Chung:2018:ERN


Chase:2013:SMN


Chuang:2011:LMA


Colin:2016:CTC

Alexei Colin and Brandon Lucia. Chain: tasks and channels for reliable intermittent programs. ACM
REFERENCES


**Comon-Lundh:2010:DSP**


**Chang:2011:RSB**


**Chen:2017:PGF**


**Chong:2013:ASG**


**Chen:2016:RPR**


**Chen:2012:NCB**

REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-27901-0_7/.  


[CLSW12] Shih-Ying Chang, Yue-Hsun Lin, Hung-Min Sun, and Mu-En Wu. Practical RSA signature scheme based on periodical rekey-


REFERENCES


Chakraborty:2015:SSC


Chen:2017:VME


Cao:2016:OMA


Chen:2012:FAA


CNRS:2014:NAS


See [BGJT14].

Coron:2012:PKC

REFERENCES

4_26; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_27. [Con18]

Chin:2011:ACS


Conitzer:2010:AP


Constantin:2012:RSN


Connolly:2018:FE


Copeland:2010:CBG


Copeland:2010:CSB


Chung:2014:RRS

Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, and Ivan

**Cordova:2014:EBS**


**Corthesy:2014:SSD**


**Coutinho:2012:RPT**


**Claessen:2013:SPN**


**Canard:2018:NTC**


Chin-Ling Chen, Jung-pil Shin, Yu-Ting Tsai, Aniello Castiglione, and Francesco Palmieri. Securing information exchange in VANETs by using pairing-based cryptography. *International Jour-


Chen:2011:TVS


Canard:2018:CPK


Calzavara:2015:SLA


Chin:2013:SMB


Chang:2012:GBP


Chou:2013:TIB


Crenne:2013:CMS

[CVГ+13] Jérémie Crenne, Romain...

Calmon:2014:ITM

Chung:2012:CBI

Chen:2014:SBB

Chen:2014:DSE


[Chen:2015:TCP] Shangdi Chen and Xiaolian Zhang. Three constructions of perfect authentication codes from projective geometry over fi-


**Djejbar:2012:ASB**


**Djejbar:2012:ASB**


**Davies:2011:IST**


**Djong:2012:DAU**


**Dou:2018:OHR**

<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>YEAR</th>
<th>AUTHORS</th>
<th>TITLE</th>
<th>VOLUME</th>
<th>NUMBER</th>
<th>PAGES</th>
<th>JOURNAL</th>
<th>CODEN</th>
<th>ISSN</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dacosta:2012:OTC</td>
<td>2012</td>
<td>Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor</td>
<td>One-time cookies: Preventing session hijacking attacks with stateless authentication tokens.</td>
<td>12</td>
<td>1</td>
<td>1-??</td>
<td>ACM Transactions on Internet Technology (TOIT)</td>
<td>TCIT</td>
<td>1533-5399</td>
<td><a href="http://www.acm.org/pubs/cnc/otit/12-1-1-1-">http://www.acm.org/pubs/cnc/otit/12-1-1-1-</a>??</td>
</tr>
</tbody>
</table>
DaRolt:2013:NDS


Datta:2017:SFH


Castro:2016:FVB


Danezis:2012:FCDa


derhans:2010:USC


Desmedt:2010:CF

REFERENCES


Deng:2017:LLH

Ding:2012:CLS

Djuric:2015:FSF

Dutta:2017:EFC

Dupressoir:2014:GGP

Ding:2012:NRR
REFERENCES

Drimer:2010:DBP


Dubeuf:2016:EPA


Dodis:2010:CA


Driessen:2013:ESA


Diem:2012:UES


Drosou:2012:SAH

REFERENCES


[DK16] Felix Dörre and Vladimir Klebanov. Entropy loss and output predictability in the Libgcrypt PRNG. Report CVE-2016-6313, Karlsruhe Institute of Technology, Karlsruhe, Germany, August 18, 2016. 2 pp. URL http:
REFERENCES

//formal.iti.kit.edu/~
klebanov/pubs/libgcrypt-
cve-2016-6313.pdf.

Doychev:2017:RAS


Doychev:2015:CTS


Durumeric:2014:MH


Dolev:2016:MCG


Doychev:2015:CTS


Do dishes:2012:MAR


Dunkelman:2012:MCE

Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The Even–Mansour scheme revisited. Lecture
REFERENCES


REFERENCES


**Dimitrakakis:2015:ELA**


**Demme:2012:SCV**


**Doroz:2015:AFH**


**Duncan:2012:CAI**

REFERENCES

Ding:2017:CSM

Das:2016:CWM

Dziembowski:2018:NMC

Dong:2012:NCV

Daemen:2010:FY

Duong:2011:CWC

Dautrich:2012:SLU
REFERENCES

Draziotis:2016:EDL

Dong:2011:SSE

Dixon:2016:NTO

Dini:2011:LLA

Das:2015:DCS
REFERENCES

comjnl.oxfordjournals.org/content/58/4/808.

Das:2016:MPU

Das:2012:DPB

Deng:2018:SFE

Dachman-Soled:2014:COF

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


David:2012:PRE [DW12]

Dorn:2012:ECE [DWB12]

Dong:2012:KKD [DWWZ12]

Dong:2012:NDI [DWZ12]

Dai:2018:OPC [DWZ18]

Deng:2014:CCC [DXA14]
Robert H. Deng, Yang Xiang, and Man Ho Au.

**Dodis:2013:OWE**


**Deng:2014:TNI**


**Dossedonne:2018:CDA**


**Dent:2010:PS**

REFERENCES


[QRI] Ertem Esiner and Anwita-man Datta. On query result integrity over encrypted data. Information Processing Letters, 122
Esiner:2019:TFA


Edwards:2014:NRP


Edwards:2017:NSQ


El-Emam:2013:NSA


Eisenbarth:2010:CCE

Thomas Eisenbarth. Crypt-

[187]

[Esiner:2016:FFB]

[EM14]

[Engels:2013:NLL]

[EPAG16]

[ElBansarkhani:2012:ELB]

[ERL16]

[Embar:2014:PW]

[EPAG16]

[Evtushkin:2016:UMC]

[ERLM16]

[Eberz:2016:LLE]
REFERENCES


Evett:2016:SES


Eibach:2010:OGB


Eldib:2014:FVS


Enos:2015:IBS


Farash:2014:ECC


Farash:2014:SEI

REFERENCES


**Fahd:2018:CPA**


**Fagone:2017:WWS**


**Farash:2014:CIE**


**Fay:2016:ICM**


**Fischlin:2012:PKC**

REFERENCES


REFERENCES

0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-34047-5_12/


Fan:2010:PSN


Fan:2010:AMI


Farras:2017:IRN


Fahl:2012:WEM


Fan:2014:ASA


Fawzi:2013:LDN


REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-30598-6_6/.

[Feng:2012:CAO] Hui Feng, Hefei Ling, Fuhao Zou, Weiqi Yan, and
Zhengding Lu. A collusion attack optimization strategy for
digital fingerprinting. ACM Transactions on Multimedia
Computing, Communications, and Applications, 8(2S):36:1–
36:??, September 2012. CODEN ???? ISSN 1551-6857 (print),
1551-6865 (electronic).

watermarking based on Fibonacci numbers. IEEE/ACM
Transactions on Audio, Speech, and Language Processing,
23(8):1273–1282, August 2015. CODEN ???? ISSN 2329-
9290.

[Ferrag:2018:SCN] Mohamed Amine Ferrag,
Leandros Maglaras, Antonios Argyriou, Dimitrios
Kosmanos, and Helge Janicke. Security for 4G and
5G cellular networks: a survey of existing authentication
and privacy-preserving schemes. Journal of Network and
Computer Applications, 101 (??):55–82, January 1,
2018. CODEN JNCAF3. ISSN 1084-8045 (print),
science/article/pii/S1084804517303521.

[Farwa:2018:FAI] Shabieh Farwa, Nazeer Muhammad, Nargis Bibi,
Saijad A. Haider, Syed R. Naqvi, and Sheraz Anjum.
Fresnelet approach for image encryption in the algebraic
frame. Applied Mathematics and Computation, 334(??):343–355,
October 1, 2018. CODEN AMHCBQ. ISSN 0096-
3003 (print), 1873-5649 (electronic). URL http://

Nielsen, and Daniele Venturi. Continuous non-
malleable codes. Lecture Notes in Computer Science,
8349:465–488, 2014. CODEN LNCSD9. ISSN
0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-54242-8_20/.


See also [?].


REFERENCES


[FQZF18] Wei Feng, Yu Qin, Shijun Zhao, and Dengguo architectures.
REFERENCES


Fathimal:2016:SSS


Frattolillo:2015:WPP


Frattolillo:2016:BFM


Frey:2010:ABC


Fridrich:2010:SDM


Frikken:2010:SMC

REFERENCES


Fang:2012:CCS


Ferguson:2010:CED


Feng:2011:GDA


Fujioka:2012:SHI


Fujioka:2012:SEI


Fujioka:2012:SEP

REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-31284-7_9/. [FTV+10]


[Feng:2013:ECE] Jun Feng, Xueming Wang, and Hong Sun. Efficiently computable endomorphism for genus 3 hyperelliptic curve cryptosys-

**Fanyang:2012:SAK**


**Fan:2015:IRD**


**Fan:2013:KIS**


**Fan:2014:NCI**

REFERENCES

204


William Gasarch. Review of Theoretical Computer
References


Gutierrez:2016:IDO


Gorantla:2011:MKC


Gupta:2012:CDF


Gupta:2013:HPH


Guyeux:2015:ECS

Guerra-Casanova:2011:SOT


Granado-Criado:2017:HCH


Gong:2016:ATI


Guerin:2016:TDU


Geller:2013:MIS


Gentry:2010:CAF


[GGH+16b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Hiding secrets in software: a cryptographic approach to program obfuscation. Communications of the Association for Comput-
REFERENCES

Garg:2014:TRS

[Garg:2017:IDI]

[Gh11b]

[L14a]

[Gh12]
Craig Gentry and Shai Halevi. Efficient implementation of fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In *IEEE [IEE11b]*.

[Gh13]

[Gh16]
Prosanta Gope and Tzonelih Hwang. An efficient mu-


REFERENCES


DEN ????. ISSN 2471-2566 (print), 2471-2574 (electronic).

Grigoriev:2017:YMP


Gaj:2017:DCR


Guo:2010:HMW


Gouvea:2012:HSI


Guo:2018:KAA


Gorawski:2012:EAS


[GL12]


REFERENCES

214


[GLM+16] Linming Gong, Shundong Li, Qing Mao, Daoshun Wang, and Jiawei Dou.


[GM13] Behrad Garmany and Tilo Müller. PRIME: Pri-

**Gotzfried:2014:MAT**


**Gofman:2016:MBE**


**Giambruno:2015:GGB**


**Garcia-Martinez:2015:HEB**


**Garcia-Morchon:2015:HCR**


**Guo:2011:ISS**

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

**Guo:2014:SAS**


**Gao:2014:URA**


**Groza:2017:LCL**


**Gong:2012:KNF**


**Garay:2017:SIA**

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


Michael T. Goodrich, Charalampos Papamanthou, Duy Nguyen, Roberto Tamassia, Cristina Videira Lopes, Olga Ohrimenko, and Nikos Triandopoulos. Efficient verification of web-content searching through authenticated web...

**[Genkin:2016:PKE]**


**[Gonzalez-Pardo:2012:CID]**


**[Greengard:2011:MRM]**


**[Green:2017:SSE]**

story-of-extended-random/[1]

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

Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Guha:2017:RTS


Guin:2016:FCS


Gong:2016:FSC


Gierlichs:2012:ICD

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

**Genkin:2013:RKE**


**Ge:2016:KPA**


**Gazi:2012:EOS**


**Gupta:2019:LAU**


**Goodrich:2011:EAD**

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


REFERENCES

Gorbunov:2015:ABE

Greenberg:2014:GWB

Gebotys:2016:PCP

Wang:2014:RAW

Gao:2015:GCC

Goh:2013:TOT
Guo:2012:AKE


Guo:2017:EMD


Gao:2012:RHC


Guo:2018:SMK


Guo:2019:NTP


Ge:2013:SAP

Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang. Secu-


Harn:2013:GA

Harrington:2014:GEF

Hardesty:2015:BA

Hardesty:2016:SUC

Hastings:2016:SWS

Hayes:2013:NSA

Houmansadr:2013:BCN

Hurlburt:2014:BBC

Hetzelt:2017:SAE
Felicitas Hetzelt and Robert Buhren. Security anal-

**Hernandez-Becerril:2016:GIS**


**He:2013:HEH**


**Hu:2017:ATE**


**Hulsing:2017:XEH**


**Hao:2012:SAM**

Hwang:2010:RIB


Hsu:2011:NLM


Hore:2012:IED


Hernandez-Castro:2012:MTA


Huang:2014:FOS


Hsu:2011:WLC

REFERENCES


Hernandez-Castro:2012:AFH


Han:2013:RMA


Heninger:2012:MYP


Heath:2015:HNS


Hwang:2012:ABA


Hamad:2018:DWU

[HEK18] Safwat Hamad, Ahmed Elhadad, and Amal Khalifa. DNA watermarking using

Hellman:2017:TLC


Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Heys:2017:SCF


Harn:2014:MTS

Hoang:2014:IMD


Hua:2015:TSE


Huang:2016:EDP


Heyse:2012:TOC


Han:2011:PEB


Harn:2015:DTS


comjnl.oxfordjournals.org/content/58/10/2583.


REFERENCES


[HK+14] Timothy Heil, Anil Kr


tronic). URL http://
/ieeexplore.ieee.org/
stamp/stamp.jsp?tp=&arnumber=
5416683.

Carmit Hazay and Yehuda
Lindell. Efficient Secure
Two-Party Protocols: Tech-
niques and Constructions.
Information Security and
Cryptography. Springer-
Verlag, Berlin, Germany / Hei-
delberg, Germany / London, UK / etc., 2010. ISBN 3-642-
14302-4 (hardcover), 3-642-
14303-2 (e-book). ISSN
1619-7100 (print), 2197-
http://www.springerlink.com/
content/978-3-642-14303-
8.

Chien-Lung Hsu and Han-
Yu Lin. New identity-based
key-insulated convertible
multi-authenticated en-
cryption scheme. Journal
of Network and Computer
Applications, 34(5):1724–
1731, September 2011. CO-
DEN JNCAF3. ISSN 1084-
8045 (print), 1095-8592
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S1084804511001172.

Wen-Bin Hsieh and Jenq-
Shiou Leu. An anony-
mous mobile user authenti-
cation protocol using self-
certified public keys based
on multi-server architec-
tures. The Journal of Su-
percomputing, 70(1):133–
148, October 2014. CO-
DEN JOSUED. ISSN
0920-8542 (print), 1573-
0484 (electronic). URL
http://link.springer.
com/article/10.1007/s11227-
014-1135-8.

Haider Salim Hmood, Zhi-
tang Li, Hasan Khalaf Ab-
dulwahid, and Yang Zhang.
Adaptive caching approach
to prevent DNS cache poi-
soning attack. The Com-
puter Journal, 58(4):973–
985, April 2015. CODEN
CMPJA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
comjnl.oxfordjournals.
org/content/58/4/973.

Chunqiang Hu, Xiaofeng
Liao, and Xiuzeheh Cheng.
Verifiable multi-secret shar-
ing based on LFSR se-
quencies. Theoretical Com-
puter Science, 445(1):52–
62, August 3, 2012. CO-
DEN TCSCDI. ISSN 0304-
3975 (print), 1879-2294
(electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0304397512004276.
REFERENCES

235


REFERENCES


Hefeeda:2010:ASM


Herzberg:2012:TJA


Hore:2012:SMR


Hoang:2012:ESB


Hirt:2014:BA


Harnik:2010:CIC

SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hoffmann:2015:LBQb

Hoffmann:2016:LBQb

Hyla:2012:CBE

Hazay:2014:OSA

Halder:2010:WTR
He:2012:ECT


Howe:2015:PLB


Hur:2010:CCS


Han:2016:GGA


Han:2014:GTK


He:2013:GME

REFERENCES


Hulsing:2013:OPX


Hussain:2018:SSH


Herranz:2013:SMS


Hulsing:2016:MMT


Huang:2014:AFS


[HSM14] Jinguang Han, Willy Susilo, and Yu Mu. Identity-based secure distributed data...


Huang:2015:PAP


Huang:2017:SSS


Hald:2015:RRA


Hulse:2013:WOS


Herbert:2012:SMP


Hurlburt:2016:MBO


ber, Germany / London, UK / etc., 2010. ISBN 3-642-17618-6 (softcover). LCCN ???.

**He:2015:SSQ**

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

**Hsu:2014:VWR**


**Huang:2011:GFT**


**Huang:2018:PIB**


**Hao:2011:NTV**


**Huang:2018:CT**

Qinlong Huang, Yixian Yang, and Mansuo Shen. Corrigendum to “Secure

See [?].


Qi Han, Yinghui Zhang, and Hui Li. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. Future Generation Computer Systems, 83(??):269–277, June 2018. CODEN FGSEVI. ISSN 0167-739X.
Huang:2019:ILA


Han:2014:ATS


He:2017:AHA


He:2018:LAB


He:2015:IEI


IEEE:2010:PIA


IEEE:2011:ICI


IEEE:2011:PIA


IEEE:2013:PIS


Imanimehr:2016:HPR


Islam:2011:MD

REFERENCES


[Iyengar:2016:SPS]

[Imai:2015:IRR]

[Islam:2015:LFP]

[Ioannou:2014:PKC]

[I:2017:ETB]

[Isobe:2012:SCL]
Takanori Isobe, Toshihiro Ohigashi, and Masakatu

Islam:2018:REP


Isobe:2012:SAL


Irshad:2016:EAM


Ishai:2014:PCP


Jacobs:2016:STB


**REFERENCES**


**Jie:2010:AAI**


**Jie:2011:RGA**


**Prins:2011:DCA**


**Jain:2013:MSD**


**Jho:2016:SSE**


**Jakobsson:2012:AWD**


**Prins:2011:DCA**

Chang:2012:TRR

Jogenfors:2015:HBT

Jeong:2013:CBC

Jo:2014:ODE

Jing:2012:MVB

Jiang:2019:SSL

Jiang:2014:UIS

Jiang:2014:TEA

Jiang:2016:MAC

Jiang:2017:BMA

Jin:2010:ADW

Jain:2010:QP
REFERENCES


REFERENCES


Jeong:2012:IKP


Jajo:2012:RET


Jia:2012:PKD


Jiang:2016:OOC


Jiang:2016:UTC

REFERENCES

Jain:2012:BAS


Jan:2017:PPB


Johnson:2010:BRF


Johnson:2015:NGA


Joux:2013:NIC


Jes:2013:CCP


Jeoffs:2013:CCP
REFERENCES


Yinhao Jiang, Willy Susilo,

**Jiang:2012:DCA**


**Joye:2012:FAC**


**Tong:2012:NBD**


**Jiang:2016:CVI**


**Juels:2014:INC**

Ari Juels and Bonnie Wong. The interplay of neuroscience and cryptography: technical perspective. *Communications of
the Association for Computing Machinery, 57(5):109, May 2014. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

**Jiang:2017:SLD**


**Jin:2015:NCD**


**Joux:2014:SAC**


**Jiang:2010:EDI**


**Khazaei:2017:COA**


REFERENCES

Karaflidis:2012:QGC

Kong:2015:CSM

Katz:2013:RIB

Kawamoto:2015:LSH

Karthigaikumar:2010:PPV

Kallel:2011:SMM

Kleinrouweler:2017:SAP
Jan Willem Kleinrouweler, Sergio Cabrero, and Pablo Cesar. An SDN architecture for privacy-friendly network-assisted DASH. *ACM Transactions...

Kara:2019:ALS


Keblusek:2015:BRK


Kemshall:2011:WMT


Kleinjung:2010:FBR


Kikuchi:2012:SSN

REFERENCES


Kramer:2010:FDC


Kim:2012:SLT


Khedr:2016:SSH


Kwon:2010:SEB


Koo:2018:PPD


Khazaei:2010:NBS

REFERENCES


REFERENCES

UK / etc., 2011. ISBN 3-642-19073-1. LCCN ????

Kompara:2019:REM


Kim:2011:LBA


Kim:2015:CEH


Kim:2016:MAS


Kim:2016:BSW


Konstantinou:2010:RC1

[KK10] 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

Karopoulos:2010:FIP


Kubota:2016:SAV


Khan:2013:EDC


Khan:2014:IPR


Kushwah:2011:EIB


Khakpour:2013:ITA

[KL13] Amir R. Khakpour and Alex X. Liu. An information-

**Klapper:2010:PSS**


**Ko:2010:MME**


**Koeberl:2012:EPD**


**Kumari:2016:UFM**


**Kim:2012:INS**


Koblitz:2016:RWE


Kasamatsu:2012:TSE


Kiyoshima:2014:CRB


Karger:2011:LLB


Kanwal:2015:TTM


Katz:2012:TSP


Khamsemanan:2016:BBU


Kawachi:2017:GCR


Kollmitzer:2010:AQC


Kang:2012:AKM


Kolman:2017:SCG


Koya:2018:AHM

Kumar:2017:TAU


Kiltz:2011:EAH


Khalid:2016:RHL


Kocabaş:2012:CPB


Kang:2016:DSA


Keskinarkaus:2010:IWD

A. Keskinarkaus, A. Pramila.

**[Kra12]**


**[KRB12]**


**[KR11]**


**[Krantz:2012:EAM]**


**[Kostinger:2012:SBL]**


**[Kannan:2013:NQF]**
REFERENCES


[References]


REFERENCES


[KU14] Hiroshi Kai and Keita Ueda. Fake shares detection on a visual secret sharing scheme by rational interpolation. *ACM Communications in Computer
Kupcu:2013:DTT


Kupcu:2015:OAS


Kuznetsov:2011:APP


Kiljan:2018:ETA


Karpovsky:2014:DSS


Kuo:2016:SDD


Liang:2015:SEC


Landau:2010:SSR


Launchbury:2012:TBC


Lauter:2017:POL

REFERENCES

Liu:2013:PAE


Luo:2012:ESI


Lupu:2012:IBK


Lu:2013:CSA


Liu:2015:IAC


Laxmi:2017:GGS

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

Lathrop:2011:SPI

Li:2015:NAC

Lee:2017:SUE
Liu:2017:GAU


Li:2015:CEH


Liang:2014:CCS


Liu:2016:EQD

Yang Liu, Zhu Cao, Cheng Wu, Daiji Fukuda, Lixing You, Jiaqiang Zhong, Takayuki Numata, Si-


[Liu:2016:NOP] Zhenhua Liu, Shuhong Duan, Peilin Zhou, and Baocang Wang. Traceable-then-revocable ciphertext-policy attribute-based en-

[Liu:2019:TTR] Zhenhua Liu, Shuhong Duan, Peilin Zhou, and Baocang Wang. Traceable-then-revocable ciphertext-policy attribute-based en-


REFERENCES

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


Lop ez-Garcia:2014:PBB


Liu:2012:FVC


Lee:2010:ISC

REFERENCES


REFERENCES


**Liu:2015:SSP**

**Lian:2014:SSA**

**Li:2018:OPP**

**Liu:2012:ESS**
REFERENCES

www.sciencedirect.com/science/article/pii/S0164121212000234


[Lin15] Pei-Yu Lin. Double verification secret sharing mechanism based on adaptive

**Lindell:2017:TFC**


**Litton:2014:TFA**


**Liu:2015:LBD**


**Liu:2016:LCP**


**Li:2017:MMA**


**Li:2016:IRI**

REFERENCES

Li:2017:SQS

Liu:2017:OOA

Li:2012:OEA

Laszka:2014:STC

Liu:2012:BIB
Fagen Li and Muhammad Khurram Khan. A biometric identity-base

Lee:2014:SPB


Li:2012:IBO


Leva:2013:ABN


Le:2011:RMA


Lee:2015:TSS


Jingqiang Lin, Bo Luo, Le Guan, and Jiwu Jing. Secure computing using registers and caches: The

**Lyu:2018:PKE**


**Li:2012:RIB**


**Liu:2018:GEI**


**Liu:2019:SBC**


**Li:2017:CIS**

Li:2017:CCD


Liu:2018:VSE


Li:2010:DCY


Lai:2013:SAS


Libert:2019:ZKA


Lu:2012:IEC

Xianhui Lu, Bao Li, Qixiang Mei, and Yamin Liu. Improved efficiency of chosen ciphertext secure encryption from factoring. *Lecture Notes in Computer Science*, 7232:34–45, 2012. CODEN LNCS'D9. ISSN
Lai:2018:EQK

Lee:2019:CSS

Lee:2016:CAM

Lee:2016:AGA

Luo:2012:FSI
Xiangyang Luo, Fenlin Liu, Chunfang Yang, Shiguo Lian, and Daoshun Wang. On F5 steganography in


[LMB12] Ariane Lambert-Mogiliansky and Jerome R. Busemeyer. Emergence and instability of individual identity. Lecture Notes in Computer Science, 7620:

Le:2016:ADS


Lai:2018:IBB


Lai:2017:FPP


Liu:2014:SCS


Li:2011:NRA


Lv:2013:NTP

[LML+13] Chao Lv, Maode Ma, Hui Li, Jianfeng Ma, and Yaoyu Zhang. An novel three-party authenticated key exchange protocol using one-time key. Journal

Lukasiewycz:2016:SAO


Li:2018:RBB


Li:2018:TFA


Li:2013:ESC


Li:2011:CIB

[LMN+11] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, and Cheng-Lian Liu. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart

**Liu:2015:SAB**


**Liu:2013:GPB**


**Loeb:2015:MGM**


**Lopriore:2012:EPP**


**Lopriore:2015:PCR**


**Lopriore:2015:PMD**

[Lop15b] Lanfranco Lopriore. Password management: Distribution, review and revoca-
REFERENCES


Lampe:2012:ATS


Liu:2015:GTB


Liu:2016:PPO


Libert:2010:KES


Lubicz:2015:GMA


Lukowiak:2014:CEB

Marcin Lukowiak, Stanislaw Radziszowski, James
REFERENCES


Liskiewicz:2013:GBS


Liskiewicz:2017:SLS


Lane:2014:PBD


Luo:2012:FSU


Lin:2015:SSE


Lychev:2016:RSI

Robert Lychev, Michael Schapira, and Sharon

Lee:2012:IBS


Liang:2015:EFC


Liu:2011:DBA


Liu:2011:NJD


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

Liu:2015:IMB

Liu:2015:MSG

Lao:2016:BFD

Lysyanskaya:2010:AEC

Lin:2011:CNS
Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, ed-

Li:2016:LRC


Ludge:2012:NLD


Lucchese:2010:RPT


Lafitte:2011:CBF


Liu:2010:CIE

Hongjun Liu and Xingyuan Wang. Color image en-
REFERENCES


[LW11c] Dong Hoon Lee and Xiaoyun Wang. Special issue papers: Nonlinear order preserving index for encrypted database query in service...

**Liu:2013:TIE**


**Liu:2013:CBS**


**Liu:2013:PAB**


**Lew:2014:DAF**


**Liu:2017:EEC**


**Liu:2011:SBA**

Yu Liu, Kaijie Wu, and Ramesh Karri. Scan-based attacks on linear feedback shift register based stream ciphers. *ACM Transactions on Design Automation of
Li:2018:SCM

Lu:2012:HOM

Lu:2014:HOM

Liu:2010:NDC

Liu:2010:SET
Liu:2011:PIA


Lu:2012:MMA


Li:2010:GCP


Lou:2010:NAS


Luo:2012:ICB


Li:2012:IIA

REFERENCES


[LWZG10]


[LXCM11] Li:2011:NIW


[LXCM11]


[LXJ14]


[LXK+14]


[LXLY12]

[Li:2012:ESD] Li:2012:ESD


[LXJ14]

**Luo:2014:ARP**


**Liu:2015:SDS**


**Liu:2015:SAA**


**Liao:2012:NSM**

Xin Liao, Qiao yan Wen,


**Liu:2017:ESS**


**Li:2010:PES**


**Liu:2012:ESS**


**Li:2016:BMA**


**Masdari:2017:STA**

Mohammad Masdari and Safiyyeh Ahmadzadeh. A

**MacCormick:2012:NAC**


**Macrakis:2014:PLS**


**Maffeo:2016:UNC**


**Michail:2012:EHT**


**Moskowitz:2010:ITE**

Malkin:2013:SCB


Mangard:2013:KSL


Martin:2010:FWL


Mazumdar:2016:CIS


Mashhadi:2017:NMS

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

Matsuda:2014:IBP

Mayron:2015:BAM

Matthiessen:2019:RCM

Maurer:2012:CCN

Mazurczyk:2013:VSD

Milo:2011:FGB

Mao:2015:PUA


[Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury. A parallel efficient architecture for large cryptographically robust $n \times k (k \geq n/2)$ mappings. *IEEE Transactions on Computers*, 60(3):375–385, March 2011. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).]

McGrew:2017:IDH


McGrayne:2011:TWH


McKay:2010:SLB


Mahmood:2018:ECC


Marquez-Corbella:2015:ECP

Irene Márquez-Corbella and Ruud Pellikaan. Error-correcting pairs: a new approach to code-based cryp-
Mathew:2015:NMB


Majzoub:2012:MRH


Mansouri:2012:ACA


Mansfield-Devine:2015:MIC


Muroch:2010:CPB


Mosenia:2017:PTS


Maachaoui:2012:MLA


Maiekejohn:2010:BRB


Meiklejohn:2010:BRB


Menn:2013:ESC


Meshram:2015:EIB

REFERENCES

Moreno:2013:NIP

Moufek:2015:MCB

Marmol:2010:TPA

Matsuda:2014:CCS

Meziani:2012:IPS

Miller:2014:ADS
Andrew Miller, Michael Hicks, Jonathan Katz, and Elaine Shi. Authenticated data structures, generically. ACM SIGPLAN Notices, 49(1):411–423, January 2014. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867


Midgley:2010:SEE

Martinez-Julia:2012:NIB

Martinez-Julia:2013:BSI

Mohanty:2011:RTP

Moessner:2012:SAS

Muller:2012:HPC

Mozaffari-Kermani:2017:FDA
MKAA17] Mehran Mozaffari-Kermani, Reza Azarderakhsh, and


Leonardo Montecchi, Paolo Lollini, Andrea Bondavalli, and Ernesto La Mattina. Quantitative security evaluation of a

Mancillas-Lopez:2010:RHI


Mendez:2016:PES


Manzanares-Lopez:2012:ICU


Ma:2017:LBI


Madhusudhan:2012:DIB

Meshram:2013:IBC

Maity:2014:FIR

Maity:2017:ODC

Mulholland:2017:DCD

Moldovyan:2012:BBD
Mahmoody:2014:PPK


Marino:2019:ACN


Matedy:2013:CRS


Mazumder:2017:PSK


Mazumder:2017:SAE


Macedo:2017:SSP


Maitany:2013:CRS


Matsuo:2012:MAK

Meshram:2012:IBC

Moran:2010:BCP

Mukhopadhay:2014:EMP

Monz:2016:RSS
REFERENCES

URL http://science.sciencemag.org/content/351/6277/1068.


Moore:2012:RFF


Moody:2014:DMW


Morad:2012:OEA


Moulick:2015:RDS


Minier:2012:EEC


Meiklejohn:2016:FBC


Mundhenk:2017:SAN


**Mironov:2012:IDP**


**Mukhamedov:2010:IEP**


**Maimut:2014:AET**

Diana Maimut and Reza Reyhanitabar. Authenti-

cated encryption: Toward next-generation algo-


**Marasco:2014:SAS**


**Micali:2014:CMS**


**Manimehalai:2016:NRR**

Migliore:2018:HSC


Martinovic:2017:AUP


Matsumoto:2017:ACG


Moghadam:2010:DRN


Mendel:2012:DAL

Maitra:2012:NA


Mroczkowski:2012:CAS


Maitra:2013:DSM


Maitra:2013:HEM


Maitra:2013:HPM


Miller:2016:RPS


Mukherjee:2017:EPP

REFERENCES


REFERENCES

Miret:2018:PBC [MST18]

Mosca:2013:QKD [MSU13]

Muftic:2016:BCC [Muf16]
Sead Muftic. BIX certificates: Cryptographic tokens for anonymous transactions based on certificates public ledger. *Ledger*, 1(??):19–37, ???? 2016. ISSN 2379-5980. URL

Malkin:2011:ECS [MTY11]

Meerwald:2012:ERW [MU12]
Mundy:2017:CGU


Murphy:2010:BRB


Murdoch:2016:IDP


Miri:2012:SAC


Min:2016:RSC


Mishra:2016:AFP

Abhishek Mishra and Parv Venkitasubramaniam. Anonymity and fairness in packet
REFERENCES


Mannan:2011:LPD


Maes:2012:PFF


Mathew:2012:EIC


Ma:2012:CIS


Mahmoody:2013:LEZ

Ma:2013:PVP


Marko:2017:MDI


Mastroeni:2017:APS


Manshiae:2013:GTM


Ma:2015:PKE


Nagy:2010:OTP


Nagy:2010:QCS


REFERENCES


Narasimhan:2013:HTD

Ngo:2017:CSS

Nedjah:2016:PYP

Newell:2013:PCD

Naeem:2014:EIC
REFERENCES

Nafea:2016:HMB


NIST:2012:RRN


NIST:2013:CSS


Nguyen:2014:DDI


Ning:2012:DPB


Ning:2015:APB


Ning:2012:DCA

[Huangsheng Ning, Hong Liu, Laurence T. Yang, and Yan Zhang. Dual...

**Nieto:2013:PVC**


**Nieto:2014:FSH**


**Nguyen:2012:DQB**


**Neville-Neil:2015:KVH**


**Nagy:2010:KDV**


**Navin:2010:ETU**

REFERENCES


[NR12] Long Hoang Nguyen and A. W. Roscoe. Short-

**Namasudra:2017:NSA**


**Niu:2015:CRS**


**Naccache:2010:THI**


**Nojoumian:2012:SRS**


**Natarajan:2015:MAD**


**Niksefat:2014:ZPP**

Salman Niksefat, Babak


Nguyen:2010:LAS


Noorman:2017:SLC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Orencik:2016:MKS


Otmani:2010:CTM


Ogiela:2018:VCA

Ohzeki:2012:NWM


Ortiz-Yepes:2014:BSA


Praba:2010:MAC


Parveen:2018:IEE


Pal:2015:SDC


Pal:2016:ACC


Pandey:2014:ACR

Parent:2012:WAI


Park:2012:APO


Pass:2013:USP


Pasanata:2013:MDR


Paulson:2010:SDO


Pandit:2012:EFS

REFERENCES


**Pang:2014:PPA**


**Paul:2012:KSS**


**Pereira:2015:PKE**


**Pippal:2012:SVU**


**Pearson:2011:NWC**


**Persichetti:2013:SAH**

Edoardo Persichetti. Secure and anonymous hy-


[PGLL10] Fei Peng, Re-Si Guo, Chang-Tsun Li, and Min Long. A semi-fragile watermarking algorithm...

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 computer science”. *Computers and Mathematics with Applications*, 60(2):175, July 2010. CODEN CMAPDK. ISSN 0898-
REFERENCES

Pieprzyk:2010:TCC


Pointcheval:2012:ACE


Patel:2018:LLA


Premarathne:2015:LDD


Pramila:2018:ICA

Anu Pramila, Anja Keskinarkaus, and Tapio Seppänen. Increasing the capturing angle in...


Peris-Lopez:2010:CSP


Poh:2012:SEC


Pande:2013:SMC


Poursakidis:2010:TPC


Puthal:2017:DDK


Niu:2014:RDW

Pan pan Niu, Xiang yang Wang, Hong ying Yang, Pei Wang, and Ai long Wang. A robust digital watermarking based on local complex angular radial

**Powers:2014:OSCa**


**Paar:2010:UCT**


**Papadopoulos:2010:TRM**


**Park:2011:ACC**


**Pereira:2016:SHB**

REFERENCES

Pendl:2012:ECC


Pyun:2012:IBF


Pathak:2012:PPS


Phan:2012:DDB


Phan:2012:MBT


Papadopoulos:2015:PAP

Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Practical authenticated pattern matching
REFERENCES

with optimal proof size. 
Proceedings of the VLDB Endowment, 8(7):750–761, 
February 2015. CODEN ??? ISSN 2150-8097.

Pandey:2012:PPS

Omkant Pandey and Yan- 
nis Rouselakis. Prop- 
erty preserving symmet-
ric encryption. Lecture 
Notes in Computer Sci-
CODEN LNCS11. ISSN 
0302-9743 (print), 1611-
3349 (electronic). URL 
http://link.springer.com/accesspage/chapter/
10.1007/978-3-642-29011-4_22; http://link.springer.com/chapter/10.1007/978-3-642-29011-4_23/.

Piret:2012:PBC

Gilles Piret, Thomas Roc- 
he, and Claude Carlet. PI-
CARO — a block cipher 
allowing efficient higher-
order side-channel resis-
tance. Lecture Notes in 
Computer Science, 7341: 
311–328, 2012. CO- 
DEN LNCS91. ISSN 
0302-9743 (print), 1611-
3349 (electronic). URL 
http://link.springer.com/chapter/10.1007/978-
3-642-31284-7_19/.

Puthal:2019:SAL

Deepak Puthal, Rajiv Ranjan, Ashish Nanda, Priyadars Nanda, Prem Prakash Jayaraman, and Albert Y.

Zomaya. Secure authentication and load balancing of distributed edge data-
centers. Journal of Parallel and Distributed Computing, 124(??):60–69, February 2019. CODEN JPD-
CER. ISSN 0743-7315 (print), 1096-0848 (elec-
science/article/pii/S074373151830741X.

Polyakov:2017:FPR

Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntanathan. Fast proxy re-encryption for publish/subscribe sys-
tems. ACM Transactions on Privacy and Security (TOPS), 20(4):14:1–14:??, October 2017. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (elec-
tronic).

Popa:2012:CPQ

Raluca Ada Popa, Catherine M. S. Redfield, Nicko-
lai Zeldovich, and Hari Bal-
akrishnan. CryptDB: pro-
cessing queries on an en-
crypted database. Com-
munications of the As-
sociation for Computing 
Machinery, 55(9):103–111, 
September 2012. CODEN 
CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-
tronic).
REFERENCES


[PSM17] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay. Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud. IEEE Transactions on Comput-
REFERENCES


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC


Papakostas:2014:MBL


Papamanthou:2016:AHT


Pudovkina:2012:RKA

Marina Pudovkina. A related-key attack on block


[PYM+13] Pieter Philippaerts, Yves Younan, Stijn Muylle, Frank Piessens, Sven Lachmund, and Thomas Walter. CPM: Masking code point-

Pei:2015:SWT


Papadopoulos:2010:CAR


Phuong:2018:CBE


Pournagh:2018:NNE


Patsakis:2015:PSM


Qiu:2018:QDS

Lirong Qiu, Feng Cai, and

Qin:2016:VTQ

Qiu:2017:AAS

Qiu:2017:PSB


Saifu Qi, Yuanqing Zheng, Mo Li, Yunhao Liu, and Jinli Qiu. Scalable industry data access control in RFID-enabled supply chain. *IEEE/ACM Transactions on Network-
Qi:2016:SPR  

Qi:2018:SPR  

Qin:2018:BRO  

Rankin:2010:HLH  

Rankin:2014:HEY  

Rankin:2016:HSP  

Rao:2010:PAA  
Rao:2017:SEC


Rauscher:2015:FMT


Ruoti:2015:WJS


Rupp:2015:CTM


Radke:2015:CFA


Reaves:2017:MBM


[Raisaro:2018:PPS]


[Rabbachin:2015:WNI]


[Reardon:2016:SDD]

REFERENCES

R4223 2016. URL http://www.springerlink.com/content/978-3-319-28778-2.


Rahaman:2010:STB


Rogaway:2016:POP


Rhee:2010:TSS


Rifa-Pous:2012:AHD


Rao:2012:SSA

REFERENCES


Roy:2017:LOS

Rangasamy:2012:ERP

Ren:2018:IAS

Roy:2015:SCP

Ribeiro:2015:QBS

Ruj:2014:DA
Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak. Decentralized access control with anonymous authentication of data stored in clouds. *IEEE Transactions on
REFERENCES


Ryan:2015:EEV

Ryan:2015:EEVb

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

Rahulamathavan:2016:UCA

Rodriguez-Vazquez:2012:SCB

Roettger:2012:PKC
Eric Roettger and Hugh C. Williams. Public-key cryptography based on a cubic extension of the Lucas
functions. *Fundamenta Informaticae*, 114(3-4):325-344, August 2012. CODEN FUMAAJ. ISSN 0169-2968 (print), 1875-8681 (electronic).

**Ren:2014:HHM**


**Rogaway:2012:SCS**


**Ren:2013:DSE**


**Rajendran:2015:FAB**

J. Rajendran, Huan Zhang, Chi Zhang, G. S. Rose, Youngok Pino, O. Sinanoglu, and R. Karri. Fault
REFERENCES

385


**Sang:2012:SSF**


**Sakalli:2014:ACC**


**Somanatha:2015:RAK**


**Shivani:2016:PVC**


**Siad:2016:NFI**


**Saarinen:2012:PPK**

Markku-Juhani O. Saari-

**Suorananta:2012:SAM**


**Sarreshtedari:2015:WMD**


**Schutz:2010:DIN**


**Sacco:2014:MC**


**Sahai:2013:TCT**

REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Notes in Computer Science, 7170:72–89, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-</td>
</tr>
<tr>
<td>[Sar14]</td>
<td>Santanu Sarkar. Proving empirical key-correlations in RC4. Information Processing Letters,</td>
</tr>
<tr>
<td>[Sar18a]</td>
<td>Neyire Deniz Sarier. Multimodal biometric Identity Based Encryption. Future Generation Computer</td>
</tr>
<tr>
<td></td>
<td>Systems, 80(??):112–125, March 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).</td>
</tr>
<tr>
<td></td>
<td>Systems, 80(??):112–125, March 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).</td>
</tr>
<tr>
<td>[Sav13a]</td>
<td>Neil Savage. News: Stopping the leaks. Communications of the Association for Computing Machinery,</td>
</tr>
<tr>
<td></td>
<td>22–24, June 2013. CODEN</td>
</tr>
</tbody>
</table>
REFERENCES

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


REFERENCES

CODEN SRECD8. ISSN 0163-5808 (print), 1943-5835 (electronic).

**Shyu:2010:VMS**


**Srinivasan:2012:RAP**


**Syta:2014:SAA**


**Schoenmakers:2010:VS**


**Schwartz:2011:IMP**


**Schaaathun:2012:MLI**


REFERENCES

3/13/data_and_goliath_bruc_scheiner_on; http://www.democracynow.org/blog/2015/3/13/part_2_bruc_scheiner_on_the

Schneier:2016:CHT


Shrestha:2010:KBA


Seberry:2010:CTAa


Seberry:2010:CTAb


Shu:2015:PML


Saleh:2010:GTF


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

Salman:2018:BMM

Sasaki:2012:IKK

Sendrier:2010:PQC

Sendrier:2017:CBC

Serrato:2012:IAN

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

**Set16**


**Sev16**


**SEXY18**


**Savas:2014:SMQ**


**Su:2012:IIN**


**Shabtai:2010:SAP**

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

Schneier:2015:SWC

Sasdric:2015:ICS

Shu:2014:DAS

Saxena:2016:API

Silva-Garcia:2018:SBG

S:2018:EDS
Prabu S, Gpinath Ganapathy, and Ranjan Goyal. Enhanced data security for public cloud environment with secured hy-

**Sanchez-Garcia:2016:SSA**


**Sun:2015:FSW**


**Shen:2018:CAL**


**Susilo:2016:EDT**


**Shankar:2012:BDF**

REFERENCES


Jeffrey Shallit. Book
REFERENCES


Shaw:2013:DE


Syed:2019:TGB


Shen:2014:LES


Shim:2011:SA


Shparlinski:2010:NWP


Suoranta:2012:ASM

[Sanna Suoranta, Jani Heikkinen, and Pekka Sil-
REFERENCES


Shyu:2015:VCR


Satir:2012:CBT


Siad:2012:NAP


Simion:2015:RST


Simmonds:2015:DI


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


Shin:2017:SSD


Szalachowski:2010:CCG

P. Szalachowski, B. Ksiezepe, and Z. Kotulski. CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block...
<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Start Page</th>
<th>End Page</th>
<th>Year</th>
<th>URL</th>
</tr>
</thead>
</table>


REFERENCES


REFERENCES

[16 pp. LCCN D810.C88 S659 2011.]

**Smith:2011:RBA**


**Smith:2015:HHB**


**Smith:2015:DBP**


**Swierczynski:2015:PSE**


**Stankovski:2014:CFE**


**Sharma:2018:CSS**


**Sadeghi:2010:THI**

Ahmad-Reza. Sadeghi and David Naccache, edi-

Safavi-Naini:2011:USC


Seyedzadeh:2014:RCI


Suresh:2015:AGU


Suriadi:2012:PCV


Schaumont:2015:IEP


[SP+13] San-Tsai Sun, Eric Pospisil.


REFERENCES

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


REFERENCES

Szaban:2011:IQB


Saxena:2012:BIT


Sendrier:2013:HCE


Sadhya:2017:PRE


Singh:2013:QBF

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

Smith:2011:SMC

Srivastava:2012:UIE

Strydis:2013:SAP

Sood:2011:SDI

Spiez:2012:RCT

Sahai:2012:DCC
Amit Sahai, Hakan Seyalioglu, and Brent Waters.


Staff:2013:ITD

Stewart:2011:CCI

Steel:2015:APF

Stenn:2015:SNT

Stipcevic:2011:QRN

Stickney:2015:CBS

Stiles:2019:HSB
D. Stiles. The hardware security behind Azure Sphere. IEEE Micro,
Stolte:2012:EDA


Suciu:2012:SED


Sung:2011:DCE


Sun:2016:NEB


Shen:2015:CSC


Song:2016:IAR


Svozil:2014:NCC

Karl Svozil. Non-contextual chocolate balls versus value indefinite quantum cryptography. Theoretical
REFERENCES


**Sahillioglu:2014:SCM** [SY14]


**Savas:2015:GMA** [SYL13]


**Shao:2015:SAS** [SYW17]


**Song:2017:SSI** [SYC17]


**Seo:2013:PIC** [SYL13]


**Song:2017:SAM** [SYW17]

Jun Song, Fan Yang, and Lizhe Wang. Secure au-
Shen:2017:RDP


Sui:2014:DAH


Shen:2014:ERC


Shi:2013:REA


Sun:2017:CPP


REFERENCES

www.sciencedirect.com/science/article/pii/S1084804512001609

Tang:2015:ETE


Tang:2015:HAC


Tankard:2017:BNK


Tankard:2017:ECB


Tarnovsky:2010:DSP


Taylor:2014:WSE


Taylor:2017:EBH


REFERENCES

Tian:2014:DFS


Tiplea:2014:NSC


Tao:2013:SMS


Terai:2011:BRB


Tassa:2012:SDC


Tewari:2017:CNU

REFERENCES

Theofanos:2016:SUE


Tian:2016:IBS


Tian:2015:IBP


Tian:2012:TOE


Thabit:2014:RRW


Takayasu:2019:PKE

REFERENCES

Tu:2014:EPB

Tani:2012:EQA

Tu:2013:PAQ

Tariq:2014:SBL

Tan:2016:ESE

Tsaur:2012:ESM
Tsai:2013:ZWS

Tetali:2013:MSA

Tang:2012:RSS

Tsay:2012:VUL

Tsoutsos:2018:EDM

Tang:2015:ECP
Qiang Tang, Hua Ma, and Xiaofeng Chen. Extend the concept of public key encryption with delegated search. The Com-
REFERENCES


[Tox14] Bob Toxen. The NSA and Snowden: securing the all-seeing eye. *Communications of the Association for Computing Machinery*, 57


F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical sur-
Tao:2014:CFS

Toreini:2017:TRP

Tang:2011:IDC

Tso:2013:SAI

Tseng:2012:ERI

Tseng:2015:LFI
Tsai:2010:RLI


Tupakula:2015:TES


Thorpe:2012:CRB


Tripunitara:2014:CKM


Wu:2012:SWG


Tartary:2011:EIT


Jonathan Valamehr, Melissa Chase, Seny Kamara, Andrew Putnam, Dan
REFERENCES


[VDO14]

Vatajelu:2016:SMB


[Ven14]

vDam:2011:TQC


[VFKS11]

Visegrady:2014:SCV


[VenafiLabs:2014:VLQ]


[Vetter:2010:ABV]


[Venkatkrishnan:2017:DRB]


[Vle12] Vleju:2012:CCA

Srinivas Vivek and C. E. Veni Madhavan. Cubic Sieve Congruence of the Discrete Logarithm Problem,

**Vliegen:2015:SRD**


**Veloudis:2016:NPH**


**Vollala:2017:EEM**


**VonMaurich:2015:IQM**


**Vembuselvi:2011:LLL**


**Vassilev:2016:ESU**


REFERENCES


REFERENCES


REFERENCES

Weisse:2017:RLC


Wright:2010:USP


Wu:2018:ESS


Wang:2018:SNU


Wei:2018:GCQ


Wang:2018:SEA

Haijiang Wang, Xiaolei Dong, Zhenfu Cao, and...

Wei:2012:NTB


Wazid:2019:DSK


Wang:2013:SES


West:2015:EC


Wess:2016:JWM


[Wu:2011:HQI]  Chia-Chun Wu, Shang-Juh Kao, and Min-Shiang Hwang. A high quality image sharing with steganography and adap-


 REFERENCES


Wendzel:2015:CME


Wang:2017:PPK


Wang:2016:SEP


Wu:2013:FTR


Wu:2016:CBE


Wei:2015:TPE

Lei Wei and Michael K. Reiter. Toward practical encrypted email that supports private, regular-

Wu:2012:RGB


Williams:2013:APC


Whitworth:2014:SPC


Wang:2015:RSA


Wang:2014:NDH


[WTT12] Tsu-Yang Wu, Yuh-Min Tseng, and Tung-Tso Tsai. A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. Computer Networks
REFERENCES

Wu:2016:LTN

Wu:2017:SPM

WW12

WW13

WW14

WWBC14
Long Wen, Meiqin Wang, Andrey Bogdanov, and HuaiFeng Chen. Multidimensional zero-correlation attacks on lightweight


REFERENCES

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


[Wang:2017:FWA] Ran Wang, Guangquan Xu, Bin Liu, Yan Cao, and Xiaohong Li. Flow watermarking for anti-noise and multistream trac-


[WY10] Xu An Wang and Xiaoyuan

**Wang:2013:NSW**

**Wei:2014:IDC**

**Wei:2016:APS**
REFERENCES


REFERENCES


Wei:2012:CSO


Wei:2012:GOP


Wang:2012:NIS


Xu:2014:AHA

REFERENCES


Kai Xi, Jiankun Hu, and Fengling Han. Mobile device access control: an improved correlation based face authentication scheme and its Java ME appli-


Xie:2012:RAA


Xiong:2012:PPK


Xu:2017:GKG


Xu:2012:AHA


Xu:2016:CIB


Xu:2013:PKE


Xu:2012:AHA
Xiang:2016:EMP

Xue:2013:TCB

Xie:2013:ECP

Xiang:2014:PBA

Xia:2015:SPK

Xiang:2015:SSB
[XNRG15] Yong Xiang, I. Natgunananthan, Yue Rong, and Song Guo. Spread spectrum-based high embedding capacity water-


[XW13] Kaiqi Xiong, Ronghua Wang, Wenliang Du, and Peng Ning. Containing bogus packet insertion at-

[XWSW16]


[XWLJ16]


[XWXC14]


[Xie:2014:SCP]


[XWY+18]

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


References


Ye:2014:NIE


Yekhanin:2010:LDC


Yoshida:2012:OGT


Yu:2012:EPF


Yang:2017:CCS


Yang:2018:RRE

REFERENCES

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

Yuce:2017:AFI


Yang:2015:SHI


Ye:2017:VCS


Ye:2016:IEA


Ye:2018:RKF


 REFERENCES

tronic). See erratum [YFK+12].

Yu:2012:IRI


Young:2013:TPC


Yang:2018:AIW


Yum:2012:OPE


Yoshino:2012:SIP


Yum:2011:ACO

REFERENCES


[YL†16] Qihong Yu, Jigu Li, Yichen Zhang, Wei Wu,

Yagan:2016:WSN


Yakubu:2017:SSN


Yu:2017:A


Ying:2013:PPB


Yu:2010:PSI


REFERENCES

/Yoneyama:2012:ORA


/Yang:2012:EMA


[Yang:2017:SAS]


/Yengisetty:2011:AVC


/Yi:2016:IPA

Xun Yi, Fang-Yu Rao, Zahir Tari, Feng Hao, Elisa Bertino, Ibrahim Khalil, and Albert Y. Zomaya. ID2S password-authenticated key ex-

**Yang:2012:SAK**


**Yumbul:2015:EEP**


**Yang:2015:EPS**


**Yang:2016:ECV**


**Yang:2018:HEP**


**Yao:2014:NCR**

Hongyi Yao, Danilo Silva, Sidharth Jaggi, and Michael

**[YT11a]**


**[YT11b]**


**[YT12]**


**[YT12]**


**[YT12]**


**[YT12]**


[Yu:2012:SME] Jia Yu, Shuguang Wang, Huawei Zhao, Minglei Shu, Jialiang Lv, and Qiang Guo. A simultaneous members enrollment and revo-


Ye:2018:ISS


Yoon:2011:SBC


Yesilyurt:2015:RWM


Yang:2013:ECS


Yang:2016:EP


Yang:2012:LUC

Bo Yang and Mingwu Zhang. LR-UESDE: a continual-leakage resilient encryption with unbounded extensible set delegation. *Lecture Notes in Computer Science*, 7496:
Yang:2017:SKS


Yang:2018:CDD


Yang:2012:BPN


Yang:2012:NIB


Yang:2014:PST

Haomin Yang, Yaoxue Zhang, Yuezhi Zhou, Xiaoming Fu, Hao Liu, and Athanasios V. Vasilakos. Provably secure three-party authenticated key agreement protocol us-

**Zufiria:2017:GLM**


**Zidaric:2019:HOA**


**Zoni:2018:CSC**


**Zhang:2011:TNT**


**Zhu:2012:JLS**


Zhang:2012:AOP


Zhou:2016:IBP


Zetter:2014:CZD


Zhou:2018:SAE


Zhao:2010:PSA


Zhou:2016:HFD

REFERENCES

Gao:2012:DES

Zadeh:2015:ASP

Zhang:2015:BYO

Zhang:2015:STR

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


Zh:2015:IDM


Zhu:2015:IDM

Zh:2016:SCI


Zhu:2015:IDM

Zhang:2019:REU


Zhu:2015:IDM

Zhu:2013:TSC


Zhu:2015:IDM

Zhu:2013:TSC

January 2015. CODEN IT-COB4. ISSN 0018-9340 (print), 1557-9956 (electronic).


REFERENCES


REFERENCES

www.sciencedirect.com/science/article/pii/S0164121216302606


Zheng:2016:EUV


Zhao:2012:SSS


Zhou:2017:IBB


Zenger:2016:AKE


Zhang:2015:MAA


Zhang:2010:EMO

Lei Zhang, Bo Qin, Qianhong Wu, and Futai Zhang.

Zmudzinski:2012:WEU


Zhao:2012:SSM


Zheng:2018:GDP


Zhang:2012:EHO


Zhou:2018:TPW

REFERENCES


Lan Zhou, Vijay Varadharajan, and K. Gopinath. A secure role-based cloud storage system for encrypted patient-centric health records. *The
REFERENCES

Zhou:2014:SAC


Zhang:2015:FAA


Zhang:2014:LFL


Zhou:2018:QT

Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki, and Arcangelo Castiglione. Quantum technique for access control in cloud computing II: Encryption and key distribution. *Journal of Network and Computer...


Zhang:2018:AKE


Zhang:2018:VPA


Zhang:2011:SIR


Zhou:2011:CLR


Zhou:2017:CLR


REFERENCES

Zhang:2011:EPK


Zhao:2012:FCS


Zheng:2015:EPT


Zhang:2015:ITS


Zheng:2015:EPT


Zheng:2015:EPT


Zaidan:2017:NDW

Zhu:2018:CA

Zhu, Biaokai; Zhao, Jumin; Li, Dengao; Wang, Hong; Bai, Ruiqin; Li, Yanxia; Wu, Hao. Cloud access control authentication system using dynamic accelerometers data. *Concurrency and Computation: Practice and Experience*, 30(20):e4474:e4474, October 25, 2018. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Zhang:2017:NLR


Zeng:2019:SAE