A Bibliography of Publications on Cryptography:
2010–2019

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 July 2022
Version 1.522

Title word cross-reference

(2, 2) [KSSY12, LTC+15b]. (K, N)
Bai10, YC11], (a, t, n) [LHYZ12], (t, n)
[QD16, ZPYW12]. 0 [XH1+17], 1
[XH1+17]. 1, 2, 3 [SMDS11]. $100 [Sch16a],
11 [LJ17]. 13 [Blo15]. 2
[AM19, DBPS12, EAA+16, ESS12, JR13,
MCDB12, PGL110, WK18, Wy12]. 22
[MNP12]. 2k [Sun16]. 3
[AP10, Bro19, CG12b, DWZ12, FSW13,
GZHD12, GH11a, KWS+12, LJ17, LJ15,
MKH+12, RS16, SS10b, SS12a, SGS14,
WSSO12, tWmC12, Y11a, Y11e, YPR17].
32 x 32 [SA14]. 3 x 3 [AMVZ12]. 4
[COP+14, DWZ12, HLYS14]. $49.00
[Sch15a]. 5 [YN19]. 8 [LPO+17, ZSH+19].

$9 [APPVP15]. = [JJW10]. + [PYH+18]. 2
[YX1+16]. 3 [LHM14]. MT [HRB13]. α
[TTL10]. c [KRDH13]. d [QD16]. d x d
[KA17]. $ [ZTL15]. F_p + νF_p [WGF16]. γ
[DFZ12]. GF(2)[x] [SF12]. GF(2m)
[HJ19, SKH15]. GF(2n) [LBOX12]. K
[FXP12, FR16, CHX13, SG19a, XMY+17,
XLP+18, ZWC17, ZHT16]. L(1/4 + o(1))
[Jon13]. M [MMSD13, OS11]. F(2^e)
[AMORH13]. Fq [SS13]. N/P [HN10].
GF(2^4) [GM16b]. GF(2^8) [GM16b]. GF(q)
[LPS10]. LWE [BV14]. μ [Jia14a]. N
[FR16]. n x k (k ≥ n/2) [MC11]. O(d13d)
[KA17]. O(n^2) [KS11]. P [DG17, GT19]. π
[EHKSS19]. ± 1 [HZW+14]. q
[CZCD18, GMS11]. S [LJ15]. t
[HM+11, Ob11]. w [Kre13].


-Encoded [DG17]. -Encoding [XHX+17].


-SDH [GMS11]. -Security [Jia14a].

-spotty [ÖS11]. -trimmed [TTL10].

.onion [Boy16].

0.13um [KLM+12].

1 [AAE+14, Ano15b, BH15, Bar16a, CGS12, Con17, Ful10, MSas12, SKP15].

1-58488-551-3 [Fu10]. '10 [Ano10a]. 1024 [Bro17, Win17]. 10Gbps [PRGBSAC19].


18th [MV12]. 192 [Blo15]. 1st [CGB+10].


23nd [MSH+16]. 256 [AKY13, App15, MAK+12]. 25th [TT18].

26th [TBL19]. 29th [Gil10]. 2D [HDGFPC15].

3 [ABM+12, BD15, jCPB+12, Ful10, LC17, Mor19a, NIS15]. 30th [Rab10]. 31st [PJ12].


5G [BBTC20, CML+18, FMA+18, GLL16, PSM+18, SAM+18, YHSW19]. 5G-based [BBTC20]. 5th [BYL10, vDKS11].

6 [Ano17b, Bai12, Mur10]. 64/128 [LJ18]. 65th [Nac12]. 6LoWPAN [BNNH19].

72 [HYS18]. 768-bit [KFL+10]. 795-bit [BBG+19].

8.8/11.2 [GLIC10]. 800 [MMKP16]. 800-160 [MMKP16]. 802.11 [FLH13, ZBR11]. 802.11s [BOB13].

802.15.4 [NBZP17]. 802.16e [CL11]. 802.16m [FZZ+12]. 85 [WZM12a]. 85th [RNQ16].

959 [ÁCZ16]. 978 [Ano15b, Ano17b, Bai12, Mur10].

978-0-691-14175-6 [Ano17b].

978-0-8218-8321-1 [Scl15a].

978-1-4200-4757-8 [Jeh10].

978-1-78548-004-1 [Ano15b].

978-1-84832-615-6 [Bai12].

978-3-540-49243-6 [Mur10]. 9798 [BM12, BMC13]. 9th [Cra12, GLIC10, HWG10].

AAA [BT18, MLM16]. AAA-based [MLM16]. AAoT [FQZF18]. Abandon [Loe15]. ABE [FJH12, HQZH14, HLC+19, OSNZ19, QZZ18, TY16a, YMC+17, ZSW+18b].

Advert [MT17]. Advertisement [Ano16, AMBJ10]. Advertises [AHS13].
AEP [LZD+19]. AEP-PPA [LZD+19].
AES [ARG19, ABO+17, BW16, BBPP13, BKR11, BB10, DGP10, FAA+18, FLYL16a, FLYL16b, GLMS18, GM16b, HMKG19, HF14b, LB13, Mar10c, MM14b, PBCC14, RMA18, SY15a, VGA19, WJ19, YWF18].
AES-Like [BW16, WJ19]. AET [HTC+15].
Affiliation [XLM+12, XGLM14, XZLW15]. Affiliations [VKK+19].
Affirmation [SRS+11, SSS+11, YSS+11]. Affirmative [HJ20].
Affirming [HJ20]. Affirmation [SRS+11, SSS+11, YSS+11].
Affirmative [HJ20]. Affirming [HJ20].
Africacrypt [BL10]. after [Sch18].
Against [Ano17e, BVS+13, BCHC19, BL15, BL16, CW12b, CMA14, DZS+18, DL17, FDY+19, GDDL18, GDCC16, HCETPL+12, HLC+19, KMZS19, MSS+18, MWES19, Sch13, SGH15, SLY+16, WAS15, AATM18, ASBdS16, AYSZ14, BBPP13, BD18, BVID12, BPR14a, BPR14b, BFK16, BSR+14, BK12b, BH19, Bud16, BCFK15, CKHP19, Che15, CG14a, CGCS12, CBYJ16, CGH17, DHLAW10, DK17, Dya19, EWS14, FTV+10, zGXW12, GSC17, HLLG18, HYL+19, JSMG18a, JH17, LDC13, LHM+10, LGL+12, LLY+12a, LWCJ16, LLC+18, Maif16, MBP19, MD12b, MN12, NDNR13, OF11, OSNZ19, QRW+18, SBM15, SEY14, SY15b, SD12, TLL13, WHN+12, You12, ZLQ15, ZHS+19, vV16].
Age [Bla12, SR14, Lan17, Sto12]. Aged [Ree15].
Aging [SKV12]. Agen [Bul11, Joh15]. Aghnostic [HFW+19]. Agreement [ADSH18, BSBB19, Ch16, HCL+14, HEC+12, KMS19, M12, WSS12, XLM+12, XZLW15, YLSZ19, AAL19, AQRH+18, APK+18, AN15, BGAD12, CSD18, CTL13, DLK+16, EBA+17, GH16, HPC12, HW10, HWB12, IS+C+16, IB11, IOV+18, KSI1, KIH19, KP18, KI1W+16, KDL+17, LLLS13, LLY06, LIK+17, MHL18, NCL13, Nos11, Nos14, ODK+17, OSNAM19, PY19, shZZ15, TLL12, WKK+17, XCL13, XXY+19, XMHD13, XH14, YZZ+14, YY13, ZWQ11, ZT16, ZGL+18a, ZZZC15, OHJ10].
agriculture [APK+18]. Aided [BGK12, BCGK12, BGB12, Gop19, GMSV14, LNWZ19, MV19, Vua10, ABBD13, LLY15, SGJ+18, SFAF11, WLFX17].
AIPISteg [AGLW16]. Air [AUM16, KTM+18, VOG18, ZZW+18].
aircraft [XZW16]. Airflow [RSCX18].
Airway [RSCX18]. AK [XHC+12].
AK-PPM [XHC+12]. AKA [LLLS13].
AKF [KDH15]. al [LLW16, LLSW16, MWZ12, PLPW13, SBS+12, Mac14, Keb15].
al-Qaed [Mac14, Keb15]. al. [ABJ13, SPLHC14]. Alan [CS12, Don14, Hel17, LCKB12]. Algebra [PWB17, Xie12a, Xie12b, BS15, Bull10b, CFR11, DW12, FGP14, Nag19].
Algebraic [ACA+16, HIJ+19, HL+19, LKY19, SK11, Tam15, Wat10, WCC17, Bull10a, CFR11, FMB+18, SA14, YTM+14].
Algorithm [AA19, ABC17, Ano11b, AK14b, BGT14, BKL18, CN14, CS10, jCPB+12, DCM18, ESI12, GKB17, HZS15, JHL12, JSZ12, JH17, JK16, KB10, LL11, LT14a, LLL17a, LLLH18, LLY+18, MSR+17, MRL+18, NdMM16, NV10, RR11, RRVC12, WH12, WZCC18, YPR17, YH16, ZSW+12, ZWW17, AIA+18b, Ang16,
Algorithmic [GO17, KRH18, RZ19, AY12a, AY12b].
Algorithmics [Gas13].
Algorithms [AMKA17, ABSSS19, AB10b, BCG12a, BR19, BJ10b, CN12, GP17, KRDH13, KHRG19, MR14a, MM17a, RPHJ11, TKM12, WH18, WRP70, YS15, ZW15, AGHP14, FLYL16a, Fri10a, LK10, Mac12, NACLR12, NC13, OO10, OO18, SD17, Xie12a, Xie12b].
Ali [ABJ13].
Aliens [Sch18].
ALIGNet [HFW19].
Alignment [Don14, HFW19, IA15, AJYG18, LYC10].
alignment-free [AJYG18, LYC10].
All-But-Many [CCL19].
all-seeing [Tox14].
Allies [Pau19].
Allocation [JWNS19].
Allowing [PRC12].
Allows [Bro17].
Almost [BKST18, FFL12, GDCC16, IM16, Oba11].
Almost-Tight [GDCC16].
Almost-Universal [BKST18].
Alpha [MV18].
Altera [SMOP15].
alternate [ZLW12].
Alternating [BKLS12, KDH15].
AMBTC [KSSY12].
AMD [Arm19, BWS19, MZLS18].
America [AB10a, Bha16, Fag17].
American [Sch15a, Mun17].
Americans [ABJ13].
Amherst [TT18].
Amoeba [MPA18].
among [BP11, MPJ16, SS17a].
amount [EEAZ13].
Amplification [ABF12, HM14].
Anal [KOP12, SOS15, Pau19].
analog-to-digital [Pau19].
Analyses [ZPXX17].
Analysing [GRL12].
Analysis [ABS12, ARP12, BRS17, BBB16a, BC14, BS14, BKLS18, Bui18, CFE16, CCG16, CGL12, DMR15, FSWF11, GZZ13, GWM16, GLG12, GA19, HC12, HHH13, HZW17, HB17, IBM13a, IS12, JT12a, KE19, KOP12, Kre13, LPS12, LTKP16, LCK11, LKY19, LLW16, LGLL12, MD12b, MAS16, MRTV12, MR10, NDC13, NSA15, NAL17, OMNER19, PH12a, PFS12, PS14, RZZ15, Rao10, RBS17, SK11, SY15a, SR12a, Shi11, SRRM18, SZDL14, SCGW14, VKC15, WRP70, WDDW12, YZLC12, ZH15, ZAG19, ZBPF18, Aia15, ACF16, AN15, BNY14, CFH13, CFL13, CDWM19, DMV15, DK17, DHW13, DMI12, FTV10, FAA18, FHM12, HM10, Lan11, LFH18, MFH13, NLYZ12, OMPSP19, PPA18, PL16, QGGL13, RITF11, SKEG14, TQL14, TLM13, Tso13, VS11, Ven14, WZ16, ZMYB17, ZZKA17, ZCZ19].
Analysis-Based [RZZ15].
Analytic [Kuz11, Sha10, Shp03, ZW15].
analytical [CDPLCA16, TKMZ13].
analytics [BLV17, GQH17, KPB18].
Analysing [BWS19, HREJ14, KL15, YGD17].
anchors [BCC19].
Ancient [Fox13, Rao10].
AND-gate [JSMG18].
and/or [YL13].
Andrew [Ano16a].
Android [Ano13a, Chi13b, EBK13, FHM12, KGP19, MF15, SFE10, YTF18].
Android-Powered [SFE10].
ANEL [BBB19].
Angle [ZPW16, PKS18].
Angle-Based [ZPW16].
Angular [pNyWyY14].
amination [WSS19].
Anisotropic [ZZCJ14].
Annotated [ATS15].
Annotating [SBK17].
Annual [Ano10a, IEE10, IEE11b, PJ12, Gil10, Rab10].
amonaly [AKK17, JVD16].
amonalous-based [JVD16].
amonisation [VY18].
amonosity [CDFS10, FVB18, HEC12, MV16b, MR10, SCGW14, TFS19, VFV17a, VFV17b, WLY17, ZYZ19, AIB16, BAG12, GH15, GH16, HSL18, HLR11, Par12b, PSJ13, SGJ18, WW14, YHL16, ZX11].
amonosity-Based [HEC12].
amonosity-preserving [AIB16].
amonization [XTK10].
amonized
SM18, VDB+16, YHSW19, AL15, Ano13f, ABO+17, BVIB12, LXMW12, MJS13, SSSA18, SSS11, SSP+13, XHM14, SAAB10.

Architecture-independent [BVIB12].

Architectures [AMKA17, BGG+13, BJCHA17, CMO+16, CHS15, DFKC17, FP19, MTM18, MKAA17, MKASJ18, RMERM19, SRT12, ST19, FPBG14, HL14, LGP19, MK11, Nov10, SHC+16]. archiving [VBC+15]. Area [GMVV17, GM16b, HC17, LZCK14, RMTA18, WH17, ABO+17, KP18, LMJC11, LIX+17, LZZ19b, Nov10, SGJ+18, WDV18]. Area-Optimal [GM16b]. Area-Time [HC17]. Areas [MV12, JY14]. Argument [BCI+13, ABM+12, LLM+19]. Arguments [BCI+13, ABM+12, LLM+19].

Argon2 [BDK16]. Argon2i [AB17]. argues [Dya19].

ARIA [PH12a]. ARITH [MSH+16, TBL19]. ARITH-26 [TBL19]. Arithmetic [AIK14, AAB17, BF19, BD19, CATB19, DDE+19, EZW18, Fre10, GH11a, HSA14, IEE13, KHF10, MSH+16, PG12, Roh19, TBL19, TT18, ZAG19, DTZZ12, MO14].

ARM [BYDC19]. ARM-FPGA [BYDC19].

ARMv8 [SD18]. ARMv8-A [SD18].

Array [BL12, MCD12, NKWF14]. Arrays [BL13, TRD11, EAB+19, KM10a].


ASBUS [YWF18]. ASIACRYPT [LW11a, Abl10]. ASIC [CFZ+10, KY18, MAA17]. Asking [DL15]. ASM [Vle12]. ASM-Based [Vle12].

ASP.NET [DR11]. Assessing [CBL13].

assets [WHJ17]. Assignment [LMS16]. Assisted [KCC17, LLKA19, GM13b, GPR+19, HZW18, WDV18].

Associated [Sar10a]. Associative [BS15]. Associativity [ABR12].

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

Assumptions [BDH11, CZF12, DN12, EKOS19, GKS17, KZ17, KM10c, PDNH15, SBM15, ABW10].

Assurance [BMBS10, Bar15, KMP+11, RBNB15, WL11, Ser12]. Assured [Tan15a, WMY16]. Asymmetric [DBT19, HG12, XLM+12, XZL14, XZL15, ZZQ+19, ZWQ+11, CSS+13, ZGL+18a].

asymmetric-histogram [CSS+13].

asymptotic [DTZZ12, TD14].

Asymptotically [LPS12]. Attack [ABSS19, Anol15d, BRS17, BIM16, BMS12, Bro17, Che18, CWZ19, CJP12, DHT+19, DSB15, FXP+17, zGXW12, GDLL18, GV14b, GDCC16, HSC19, HCTPL+12, HL25, JL15, JK12, Kam19, LSW16, LGL+12, LJJ17, LCL17, LJJ19, LBC18, LWKP12, LWKP12, LFK19, MSS17, MSS+18, MPA+18, MWES19, MS12b, Pud12, SKE+18, SBM15, SP13, SS15, SDM+12, WLC12, XJ13, YTF+18, YWM19, Anol17a, AYSZ14, BD18, Blo15, BNST17, CAM19, CJP15, DDFR13, FLZ+12, Goo12, GSAV18, KA17, LLY+12a, LC13, LYH14, LWKP14, MB11, MN12, NZL+15, OPS14, SB17, SXL16, SCBL16, WYL13, vV16].

Attacker [BCEO19, BCEO20, PLGM18].

Attackers [BL15, BL16]. Attacking [Bon19, GJ19].

[AMMV18, AB17, ARP12, Anol17e, BGK12, BCHL19, BCHC19, BFK14, CZ19, CHP19, CBRZ19, Che15, CMA14, DZS+18, DGS12, DL17, DHLAW10, DH18, EWS14, GPT+14, HLLG18, HI+19, Hay13, HLC+19, HR16, JSK+16, JW+17, KRN10, LLC11, LWZ1, LH14, LJ18, LW1, LWC14, LWML16, LCL17b, HY+18, LSG+19, MD12b, PJD+19, PYM+13, PS12, Sas12, SEY14, SY15a, SP15a, SH15, SVG16, SGH15, VWC19, W14, WHN+12, XNG+14, YKA16, YL17, YCM+13, ZLQ15, ZHS+19, AAT18, ACD18, BBP13, BVIB12, BVIB12, ...]
BCDN17, BZD$^{+16}$b, BSR$^{+14}$, BH19,
BCFK15, CBGY16, CGH17, dCSM$^{+12}$,
DCAT12, DJL$^{+12}$, DK17, Dra16, Eng15,
EA12, FTV$^{+10}$, FIO15, GPN$^{+16}$, GLMS18,
GBNM11, HAK19, HAGTFR13, KMP10a,
KPS10, LCD13, LHR$^{+10}$, LWK11, MBP19,
NDNR13, OF11, PX13, SGP$^{+17}$, TK19,
TS16a, TY16b, TTL13, VS11, WWBC14].
attacks [XWDN12]. attempt [Fed13].
Attestation [BWS19, FQZ18]. Attribution
[EGG$^{+12}$]. Attribute [AAC$^{+16}$, AHH$^{+12}$,
BFK$^{+10}$, Boy13, CD16b, CDL18, CDLW19,
CII$^{+19}$, FHR14, GZZ$^{+13}$, GSW$^{+16}$, Gli12,
GVW15, HSMY12, HBC$^{+19}$, Her14, KGP12,
LW11b, LW11c, LW12, LJLC12, LYZ$^{+13}$,
LHL$^{+14}$, LAL$^{+15}$, LHL15, LW16, OT12,
PRA18, PB12, RHH$^{+16}$, Rao17, SSW12,
TYM$^{+17}$, WDCL18, WHL15, WHL16,
WHL17, XMLC13, XWL16, XHX$^{+17}$,
ZPM$^{+15}$, ZQQ15, ZMM17, ZHW15, BTIK15,
CPPT18, FNWL18, HZL18, HZW18,
HYS18, HKHK13, JSMG18a, JSMG18b,
LCL$^{+15}$, LFZ$^{+17}$, LFWS15, LYL15,
LJW$^{+17}$, LJYW18, LDZW19, Nam19,
QRW$^{+18}$, RD17, SSL$^{+19}$, WLWG11,
WZC16, XWS17, XZP$^{+19}$, XZT$^{+19}$,
YSQ19, YCT15, ZWM14, ZML17,
ZGL$^{+18}$a, ZWY$^{+19}$, Ver17].
Attribute-Based
[AAC$^{+16}$, BFK$^{+10}$, Boy13, CD16b, CDLW19,
CII$^{+19}$, FHR14, GZZ$^{+13}$, GSW$^{+16}$,
GVW15, HSMY12, HBC$^{+19}$, LW11b, LW11c,
LW12, LJLC12, LYZ$^{+13}$, LHL$^{+14}$, LAL$^{+15}$,
LHL15, LW16, PB12, RHH$^{+16}$, Rao17,
SSW12, TYM$^{+17}$, WDCL18, WHL15,
WHL17, XMLC13, XWL16, XHX$^{+17}$,
ZPM$^{+15}$, ZQQ15, ZMM17, AHH$^{+12}$, CDL18,
Her14, WHL16, CPPT18, HZL18, HYS18,
HKHK13, JSMG18a, JSMG18b, LCL$^{+15}$,
LFZ$^{+17}$, LFWS15, LYL15, LJW$^{+17}$,
LJYW18, LDZW19, Nam19, QRW$^{+18}$,
RD17, WLWG11, WZC16, XWS17, XZP$^{+19}$,
XZT$^{+19}$, YSQ19, YCT15, ZML17,
ZWY$^{+19}$, Ver17]. Attribute-Hiding
[OT12, ZWM14]. Attributes
[CGI2a, VKK$^{+19}$, Yon11, LCL$^{+17}$a].
Attribution [AIF$^{+19}$, XHC$^{+12}$, FNP$^{+15}$].
Au-Id [HWZZ19]. Auction
[Con10, JWNS19, DLL15, HJM$^{+11}$].
auctions [MR14c, QSI18]. Audience
[DTE17]. Audio
[Ber18, DA12, FM15, GCK12, HGT15,
KD12a, KD12b, LA14, LSL12b, NXY$^{+17}$,
QF19, TC10, gWpNyY$^{+14}$, XNG$^{+14}$,
XNRG15, XNP$^{+18}$, ZS12, LSQ11a, SKEG14,
yWpNyL11, WYHY12, YQH12].
Audio-Visual [LaL14]. Audit [YRN12b].
Auditing [LMD16, LCDP15, TCN$^{+17}$,
XWK$^{+17}$, YYS$^{+16}$, YXA$^{+16}$].
Augmenting [AV18]. August
[AB10a, JY14, MV12, Rab10]. Aura
[HFCR13]. Austin [IEE13]. AuthCropper
[KLK$^{+19}$]. Authentic
[ASV$^{+18}$, HLT$^{+15}$, SZMK13].
Authenticate [HM12]. Authenticated
[Alo12, ADHS18, BSBB19, BCO13,
BDMLN16, CLL16, CLY14, CCS14, CRE$^{+12}$,
DS11, EAA12, ESS12, FVS17, FLFI12,
GTT11, GL12, GZ12, HC12, HL10a, HCL$^{+14}$,
HEC$^{+12}$, KMY18, KLK$^{+19}$, LHRK10, LY16,
LH11c, LCCJ13, LTT10, MR14a, MMY12,
MMS17b, MHKS14, MSU13, PTT16, Sar10b,
Smi11b, Tan11, TW14, WDV18, XLM$^{+12}$,
XHC$^{+12}$, XGLM14, XZLW15, YS12,
YLS12, YLY13, YRT$^{+16}$, Yon12, ZPZ$^{16}$,
ZXH16, ABC$^{+18}$, AIB$^{+16}$, ABR15, CTL13,
FA14b, FIO15, GPN$^{+12}$, GLM$^{+11}$, HPC12,
HWB10, HWB12, HL11, HPY10, ISC$^{+16}$,
JKA$^{+18}$, KMTG12, LWS10, LHH11,
LML$^{+13}$, NCL13, Nos11, Nos14, ODK$^{+17}$,
OSAN19, PPT15, P18, PPG19,
SMB10, TCS14, Tso13, TKHK14, WZM12a,
WZM12b, WTT12, WXGC14, XCL13,
XWZ$^{+18}$, YC12, YZZ$^{+14}$, YZL$^{+18}$, YLL$^{+18}$,
ZT16, ZGL$^{+18}$a, ZXWA18, ZG10, ZSC15].
Authenticating
[BS12, CHX13, GRL12, OKG$^{+12}$, RGP12,
WY12, ZCWS15, Bel18b, Cer18,
LFGCCGCRP14, PGLL10, RR16, ZLDD14].

**Authentication**

[AV18, AA19, ADM19, AAA+19, AMSPL19, ASO14, AAZ+16, ACAT+15, ACKB19, AUMT16, ABB19a, ATC17, BL12, BCE+12, BCM12, BNNH19, BSSV12, Bel18a, BKST18, BCD+12, Bis17, BF11, Boy16, BKP12, BNSV12, CC14, CSH+18, CRS+18, CCW+10, CCF17, CCC19, CJ13, CD12, CJP12, CLH13, DL15, DCM18, DBPS12, DP12, FLH13, FR16, FMTR12, FD11, GWP+19, GHS14, Gli12, GI12, GMDR19, GM14, GU13, GVV+17, GCK12, HZC+12, HvS12, HQY+18, HKK19, HLLC11, Har13, Hay13, HBC13, HM10, HCPBS12, HCETP+12, HKL+12, HFS+19, HFCR13, HXC+11, HLCL11, HCYZ18, HWZZ19, HRK18, IGR+16, JN12, JCM12, Jia17, JNX+19, JAE10, KP12, KS18b, KLN15, KTM+18, KRM+10, KSD+17, KPC+11, KLY+12, KTA12, KGP12, Kim15, KPS12, KLM+12, KO16, KH10, LLC11, LKBK19, LH12, LFH18, LLG15]. **Authentication**

[LS13a, BGE+18, BDM18, BDL+19, BD18, BCM13, BGAD12, BBTC20, BDM+19, BBB19, BLAN+16, BAL10, BMM12, B+OS15, BT18, BTW15, BM11, CLM+12, CML+18, CLP+13b, CAM19, CTL12, CUX19, CSD18, CNF+18, CH10, CCSW11, CHS11, CLWH13, C15a, Chil13a, CCMB19, CJP15, Cho14, CL11, CHL19, CRS13, CDWM19, DCAT12, DSCS12, DRN16, DEL19, DLK+16, DMV15, DLM13, DZS+12, DMT12, uHAN+18, EA12, ED19, EA11, FPP19, FH10a, FLL+14, FXP12, Far14, FA14a, FHZW18, FQZ18, FMA+18, FHM+10, FZZ+12, GJ13, GMSW14, GHD19, GEAHR11, GPLZ13, GH15, GH16, GAI+18, Gop19, GCSA+11, GMJ11, GLB+18, GBC19, GST+S9, HU15, HSH11, Ham12, Ham19, HWW19, HSHB18, HCDP13, HZC+14, HK17, HZWW17, HL12, HL14, HCM11, HLC16, HPL+19, HCC10, HS11, IMB17, IAA+19, IC17, IG11, IB11, IOV+18, Jac16]. **Authentication**

[JNUH17, JKAU19, Jia16, JKL+16, JM16, JAS+11, JXZ15, KPP16, Kem11, KGG14, KSB+17, KCS+18, KV+18, Kim11, Kim16, KHB19, KS19, KP14, KB17, KSW16, KDW+17, KKD+18, LLS13, LLZ+16, LC17, LL06, LHI1b, LT13, LH10c, LNM+11, LMC11, LCMW12, LNN13, LNK13, LXJ14, LK+17, LCM+17, LNK+18, LWK+18, LNK+18b, LZD+19, LWK+19, LW19, LHM14, LH13, LSQ15, LHH+18, Lit14, LWW11, LTC+15a, LL15, LZZ09b, LBR12, LTE10, MM12, MMLN15, MC+18, MDHM18, MVO11, MMP19, MA17b, MMS17c, MWW+18, MZL+19, MCB19, MHL18, MKL2a, MGB19, NSD17, NR17, NACL12, NCC13, NM18, NLYZ12, NML19, NB13, NXS10, NMX15, OSP+19, OF11, OCG11, OYHS14, PYH+18, PYP10, Par12b, PLGMCdF18, PCK19, PZFB18, PA10, ...
PKA15, PRN+19, QMC17, QMW17, QLZ19, RR17, SSA18, SCFB15, SPLHCB14, SB17, SGGCR+16, Sar10a, SK18, SSNS15].

authentication
[SVY19, SGJ+18, hSZZ15, SCKH10, SYWX19, SNG+17, SCR19b, SA15, SYW17, SSI11, SKEG14, SA19, SMS+16, SHBC19, Tan12b, Tan15b, Tan18, TODQ18, TZTC16, TG17, TLL12, VSB+19, Wan13, WW14, WLZ+16, Wan18b, WCFW18, WXSH19, Wat14a, Wat15, WDKV19, WT10a, WKH11, WXK+17, XHH12, XWDN12, XHCH14, XXY19, XMHD13, XHM14, Yi17, YHL16, YHS16, YYK+19, YWK+10a, YSL+10, YMM13, YN19, YY13, YD17, ZYL+10, ZQWZ10, ZCLL14, ZQD16, ZGL+18b, ZDHZ18, ZZY+19, ZXX11, ZLY+19, ZZZL18, OHJ10]. authentication-chaining [EA11]. authenticators [SYY+17].

authenticity [ADF12, VBC+15]. Authority [LNXY15, XZLW15, ZQQ15, JB11, SLL+19, ZWY+19, ZZ12]. Authorization [CS14, LMGC17, MPM+17, YKK18, AL15, DFJ+17, FHM+10, JAE10, JAS+11]. Authorized [GHY18, HTC+15, LLSW16, Ma17a, WZCH19]. authorizing [Bel18b].

Authorship [AIF+19, BTW15, BAG12, LCM+17]. Autoblocking [LLLH18, YH16].

Automata
[CCD15, Gas13, dRSdlVC12, Ang16, DGL19, HBBRM+16, KFEF19, SS11, WOLS12]. automata-based [SS11]. Automated [BHC19, CCK12, CCK16, DRS16, GLLSN12, JGP+18, LGM+16, Ste15a, Tom16, YSS14, BJR+14, GMMJ11, KKK+16]. Automatic [HWZZ19, MMP19, WW12, HL19].

Automation
[BGK12, DZS+18, IEE11a, KPP16]. Automotive [HK18, LMS16, MPM+17]. Autonomic [SEK+19]. Autonomous [MPA+18, BT18, SMS+16]. Auxiliary [DMS+16, DL12, GGHW17, XXZ12, YCY12, Kom18]. Auxiliary-Input [XXZ12, Kom18]. Availability [CK11, ADF12, CFVP16]. Available [Ano16e, HGOZ19].


BCEO19, BCEO20, BBB+16a, BSSV12, BHG12, BKPW12, BRT12, BHH+15,
BBKL19, BS13b, BFK+10, Bon12, BSJ15, BF19, Boy13, BKJP12, BDH11, BCF+14,
But17, CML15, CGL16, CGM014, CKHP19, CMRH17, CCM17, CSH+18,
CZLC12a, CZLC12b, CLHCl2, CCZC13, CLY14, CZLC14, CST+17, CZCD18,
CLND19, CGL+12, CDD13, CGY+13, CDD12, Ch12, CK18, CD16b, CDLW19, CHH+19,
DSM14, DHT+19, DL17, DS19, DA12, DLZ+16b, EM12, EKF+16, EFGT18, FM15,
FYD+19, FR15, FVS17, FP19, FSX12b, FSX12c, GT19, HCPLSB12, HKL+12]. Based
[HG12, HMR12, HSA14, HWS+19, HPO+15, HKR+18, HGT15, HLC+14, HLN+10, Hül13,
HRS16, HBG+17, HEC+12, HM19, HP12, HP17, JTZ+16, JP19, JHHN12, JEA+15,
JKHeY12, KMW19, KS18b, KZG10, KK12, KKA15, Kha10, KLY+12, KSSY12, KPKS12,
KHFR19, KRB12, KAK18, KS15, LGMCI7, LGM+18, LY+18a, LTKP16,
LSD12a, LKBK19, LSL12b, LW11b, LW11c, LW12a, LHF12, LJL12c, LY+13, LH+14,
LTH+15, LLG+15, LDLZ16, LTZY16, LLZ+17, LLLH18, LPL15, LSL15, LH+15, LH11c,
Lin15, LYL+18, LP12, LNW19, LZ+13, LCCJ13, LWCJ14, LNX15, LHL15, LW16,
LPO+17, LHW18, LL919, LHY+19a, LGPR14, LDB+15, LD13, LSC12, LBR12, LLH18,
MWZ12, Ma17a, MLO17, MEF012, MCD12, MVV12, MZ12b, MBC15,
MKN13, MZ17b, MCS+15, MSIS17b, MKF+16, MCF17, Men13a, MST18, Mor12,
MSKR17, MKAA17, Mu16, NIS15, NC12, NXH+17, NDR+19, NXB13, NLLJ12,
NLY15, pNyWyY+14]. Based
[OTD10, PB12, PSSK19, PTT16, PYM+15, PDNH15, PPS12b, PYS18, PG12, PAS13b,
PNRC17, QJC+18, QF19, RVH+16, RSR+19, RZZ+15, RS16, Rao17, RR11, RDZ+16,
RVRCM12, RW12, RJV+18, SBS18, SSW12, Sar18a, SS13, Sen17, SJL18, SXH+19, SJ12,
SGP+12, SPG+19, SP15b, SQA13, SRA17, SNK18, SH15, SBG12, TCR14,
TWZ11, TW12, TYM+17, TSH17, TT12, TTH15, TFS19, TC10, VDB+16,
VGA15, VAG19, Vil12, WY10, Wan10, WSSO12, WgMW12, WYW+13, Wan14,
WZCC18, yWXyZ+18, WDC18, WHL15, WHLH17, WLC+18, WT10b, WMS+12,
WZCH19, XNG+14, XNRG15, XZX12, XMLE13, XLQ09, XQL11, Xia12, XLG14,
XWLL16, XJW+16, XJR+17, XHX+17, XHZ+19, YE12, YLZ12, YXZ+12, YGFL15,
YH16, YTH17, YYO15, Y+17, YKNS12, YHK+10, YMS11, YK+11, YFK+12, YCZY12, ZSP+19,
ZPM+15, ZJ11, ZZX+11, ZDL12, ZLH+12]. Based
[ZQQ15, ZMW16, ZXYL16, ZWW17, ZM17, ZW17b, HY+19, ZPW16, ZWH15, ZV16, ZPXX17, ZGZC18,
ZYM18, ZHY+19, ZHL15, AM18, AGL16, AaBT16, ARL13, AY14a, AIS14,
AAT16, AA14, ASO14, AIA+18a, AIM+19, AKG13, ASVE13, ACA+16,
ARG19, AM19, Ara13, AT1+10, ACC+13, AHH+12, BK19, AVAH18, BS15, BDM18,
BDL+19, BBBP13, BD18, BGAD12, BAAS13, BBTC20, BDM+19, BOX13,
BWR12a, BW13, BWA13, BM12, BZD16a, BC18, BTK15, BBB16b, BK12b, CPPT18,
CML+18, CXX+19, CFL13, CFY+10, CCLL11, CTL12, CWSL12, CNF+18,
CRS+18, CG12b, CSZ+11, CHX13, CSS+13, CW14a, CLC+19, CWZ19, CXW19,
CCMB19, CTHP13, CJP12, CJP15, CCX10, CTL13, Ch14, Con12, CHL19, dCCSM+12,
Cra11, CDL18, DSSC12, DGMT19, DZ14, DNN13, Dra16, uHAN+18, EZ15, FH13,
FG19, Far14, FA14a, FA14b, FIO15]. Based
[Fay16, FLYL16b, FHZW18, FMC19,
Behaviors [GAF+15, HL19, ZMYB17].

Behavioural [MT17, Behind [Fre10, Sti19].

Being [NSP+18].

Belief [BT12, Bell [JEA+15, QD16].

Benchmarked [MKAA17].

Benchmarking [MTM18, ZZKA17].

Benefit [HB14].

benefits [Wat14a].

Benford [AOT13].

Bessel [GJ13].

best [Cha13c, Tay19].

Bet [Rom12].

Beta [MV18].

Beth [CTHP13].

better [LCL+17a].

Between [HSUS11, KA18, LRVW14, SAKM16, CLM+12, HLRI11, KPP16, Kim16, PBCCh14, WDDW12].

Beyond [JL18, LST12, MJS13, RS18, TS16b, FNP+15, JR14].

Big [FYD+19, GRRZ18, HLC+18, KPB18, LLSL19, MAI13, MMS17b, PH16, PNRC17, PWS+19b, YDY+16, ZLW+17, FS18, HL19, JLC18, LSBN14, QCX18, Rom12, Tan17b, WS14, WS19].

biggest [Rom11].

Bill [Bel15].

Billions [Hof16, SMBA10].

Binary [ADI11, ABSSS19, ADH18, AK14b, MBR15, MBF18, DGK18, SA14].

Binary-Ternary [ADI11].

Binding [HET+12, LBC18, ZLQ15, LZ11].

Bio [OK18, VGA19, AJYG18, GPVcDRO12, ZHL+11].

bio-cryptographic [ZHL+11].

bio-cryptosystems [AJYG18].

Bio-inspired [OK18, GPVcDRO12].

Bio-Key [VGA19].

BioAura [MSKRJ17].

biographical [Maf16].

biomedical [AIA+18b].

Biometric [Alp18, ATI+10, BDM+19, BCTP16, DWI12, HFS+19, JN12, YKM13, LGM+16, May15, NGAuHQ16, PMG+19b, SAR12, SKV12, SRRM18, SP19, Vet10, YLK+17, AAL19, AHM+18, BK19, DEL19, DMT12, GCSAdp11, GBC19, HT11, Ham19, KCS+18, LK12, LTC+15a, MLBL12, Sar10a, Sar18a, SR10, SC19b, YWZ+18, QZD16].

Biometric-based

[BDM+19, GBC19, KCS+18, SR10].

Biometrics [AHN+18, BW13, ERLM16, SP13, ZPW16, AGBR19, BOP14, CNF+18, FHZW18, GM16a, KLW+17, LXYL12, LH10c, LNM+11, LH14, LNK+18a, MRRT17, Rom11, SS17a, SCBF15, YY13].

biometrics-based [CNF+18, FHZW18, KLW+17, LXYL12, LH10c, LNM+11, YY13].

biosensor [Kim16].

Birkhäuser [Sha10].

birth [YY17a].

Birthday [ACD18, LST12, GJ19, RNQ16, SXL16, Nac12].

Birthday-Bound [LST12].

birthday-type [GJ19].

Birthing [TLZ+17].

Bit [CK17, CG14a, GV14b, HG12, HS18, KTM19, LJK17, LPO+17, NIS12, Ros11, YLL+12, APPVP15, BGG+19, KS11, KFL+10, MMN12, PLsvDE10, RH10, SLXX16, TWZ+12, TBK+18, VN17, ZSH+19].

bit-pair [SLXX16].

Bit-Wise [CG14a].

BitCoding [HS18].

Bitcoin [ADM16, BSR17, BH15, Bra15, Chl13b, HB14, Hur16, IM16, JK+17, Mic16, Sir16, Tay17, TS16b, VFV17a, VFV17b, WLY17, WHJ17, Ano16a].

Bitcoins [MPJ+16].

BitErrant [Ano17a].

Bits [BF12, LLL17a, YCL17].

Bitsliced [HMKG19].

Bitstream [SMOP15].

Bivariate [TWZ11].

Bivium [EV10].

BIX [Muf16].

BLAC [TAKS10].

Black [BR14, CPS16, HHP17, KOS16, KMO14, MSA13, JB11, Rja12, SS10b, YKA16, DDI3, SK14, YSC16, ZZ12, Crl16].

BlackBox [BR14, HHP17, KM14, Rja12, SS10b, KOS16, MSA13, ZZ12].

Blackbox [MSA13, SS12a].

Blackhole [SS15].

BlackWatch [HSC19].

BLAKE [AMP14, GV14b].

BLAKE-512-Based
Blanchette [SR14]. Blended [ACAT+15]. Bletchley [Bai12, Ano11c, Bri11, Cop06, Cop10a, Cop10b, GMT+12, GW14, McK10, McK11, McK12, Pea11, Sim10, Smi11a, Smi15b, Smi15a]. Blind [AP10, Ano15a, BCPV11, LCL17, LGFRH14, MR16, MNN12, RS16, YMWS11, HKB14, MO14, RSM15, RMG18, WLB11, yWpWyYpN13]. Blindfold [Nac16]. Blinded [SAT08, Ano15a, BCPV11, LCL17, LGFRH14, MR16, MNN12, RS16, YMWS11, HKB14, MO14, RSM15, RMG18, WLB11, yWpWyYpN13]. Blindfold [DSS17]. Blinding [CLHC12, KHHH14]. Block [´AMVZ12, BRS17, BSS+13, BFMT16, BDGH15, BCG+12b, CWP12, DWWZ12, EGG+12, FXP+17, GLLSN12, GT12, GST12, GNLS12, IS12, KR11, KWS+12, LKY19, LWZ12, LJ17, LCLW17, LGLL12, LWKP12, LWPF12, MCDB12, MRTV12, OGK+15, PH12a, PDJ+19, PRC12, Pud12, SJLX8, SGP+12, SSA13, WW12, YCL17, ZSW+12, BNY14, Jeo13, KM11, LGP19, LPZJ15, LC13, LYHH14, LWKP14, MCL+19, MNP12, MHV15, MHY+18, PL16, Sar11, SKK10, TQL+14, Tan17a, WB12, WWBC14, ZSW+18a, JKP12].

Block-Parallel [MCDB12]. Block-Wise [SSA13]. BlockA [CHL19]. Blockchain [Alz19, Ano19c, ATD17, AHWB20, CLC+19, Eya17, Hur16, HM19, JNWS19, KV18, NML19, Poc17, Scr18, SG19b, SJZG19, TBY17, VFS+19, ZXL19, HHBS18, JLX+19, LHH+18, Nor17, CHL19].


Boolean-based [CW14a, YCC16]. Blockchain-Based [HM19, HHBS18, JLX+19, LHH+18].


botnets [HB13]. Bottom [SS12a, ZYT13, IM14]. Bounding [ABB+19b, PYH+18]. Bounds [BCG19, CK17, Jia17, LJ15, SNJ11, SS10b, Sha10, Shp03]. Bouzefrane [Ano15b]. Box [BW16, BCG16, BCKP17, BR14, CPS16, HHP17, KMO14, LYL+18, Mic10b, RMTA18, Rja12, SS10b, SWF+19, KOS16, KCS+18, LRW13, MSA13, RMP10, SGFCRM+18, ZZ12, ZSW+18a].


breakthrough [Goo12]. breath [LS13].

Breathing [CSH+18, CRS+18, HCYZ18]. Breathing-Based [CSH+18, CRS+18].


British [And13]. Broadcast [BS14, GMVV17, HMR14, KH10, LMGC17, LST12].
LMG+18, PSM17, PPS12a, RMZW19,
SXH+19, WQZ+16, XJW+16, Yan14,
ZHW15, CPPT18, DLN13, SM19b,
WWYY11, WDZ19, XWDN12, XZP+19,
YMM13, ZWQ+11, ZZ12, Zhu13.

Broadcasting
[OO12, MK11, OCGD11, SM19b, YY11].
broken [Bat10, Hea15]. Broken
[MDAB10, Tur18]. Broker [TKR14].
Broker-Less [TKR14]. Browse [NA14].

Browser
[QF19, ABR13, ACC+13, BCZF15, GIH+12].
browser-based [ACC+13]. Browsers
[FVJ19, Rec15], browsing
[MWW+18, YYK+19]. Bruce [Sev16].
Brute [CJP12, JR14, CJP15]. Brute-Force
[JR14, CJP12, CJP15]. BW [CMLRHS13].
BSeIn [LHH+18]. BTC [CLF11, QJC+18].
BTC-compressed [CLF11]. Bubbles
[HHBS18]. Buchwald [ABJ13]. Bucket
[BKKV10]. Bug [Chi13b]. Build [IM16].

Building [BPS16, GB19, KMP+11, MJS13,
Sev16, WL11, CHH+13, LCKB12]. built
[GSV18], built-in [GSV18]. Bullet
[McG16]. Burdens [Bla12, SR14]. Bus
[AN17]. Business [LB+15]. Butterfly
[HQY+18]. Buyer [Fra16, KJN+16].
Buyer-Friendly [Fra16]. BYOE [Tan17a].
byte [Ho15, Ho16]. Bytecode [SEK+19].
bytes [PBC14]. Byzantine
[KS11, LLKA19, YKGK13].
Byzantine-resistant [YKGK13].

C [AD12, ACZ16, Cra14, DGJN14]. C&C
[GN16]. C1G2 [MK12a]. CA [ACM11,
Dun12b, Kia11, Lin14b, Pie10, Rab10].
CABA [MSKRJ17]. CABLE [XHH+17].

Cache [AB15, ADR18, CBRZ19, DKMR15,
FDY+19, HLAZ15, LWML16, SY15a,
YVD19, DJL+12, DK17, MCL+19].
CacheAudit [DKMR15]. Caches
[LLGJ16, CDPLCA16, DJL+12]. Caching
[ADR18, HLAZ15], cackled [Bai12]. CAD
[PGLL10]. Caernarvon [KMP+11].

Calculus [MR10, Jou13]. Calibrated
[LC15]. California
[An10a, IEE15b, IEE15, MSH+16]. Call
[An10b, An10c, An10d, CS14, Hor19,
KRM+10]. Call-Back [KRM+10]. Calls
[Mur15, KGP+19]. cam [PKS18].
Cambridge [ACM10, PJ12]. Camellia
[Blo15, LKP12, LKP15, LKP14,
SEK12]. Camellia-12 [Blo15]. Camera
[ATC17]. Cameras [ASV+18, MKH+12].
Can [Alo12, AZH11, Bar15, DSM14,
KNTU13, YM16, Pec17, RK11, Rus15, Sto12,
GMV17, LMS16]. Canada [JY14, MV12].
Canal [GWP+19]. Cancelable
[QL19, AJY18, LZ11, LH14, YWZ+18].
Cancellation [DLMM+18]. cancelled
[An10c]. Candidate [GGH+16a].
candidates [ABM+12]. canonical [Bul10a].
CANS [HVG10, LTW11]. Can’t
[ASV+18, Kn17, RAZS15, PZ15].
CAOverif [ABF+14]. Capabilities
[CHN+18, GFBF12, Lop15a, KMG17].
Capability [IA15, LLL+17, LT13].

Capability-Based [LLZ+17]. Capacity
[LLY+18, TODQ18, WY18, XNRG15,
YW10, BCND19, CLZ+17, GZHD12,
PWLL13, WHL13]. Capacity-aware
[TODQ18]. Capacity-Raising [YW10].
Capitalism [Fid18]. CAPTCHA
[OTO18, SKG14]. CAPTCHA-based
[SKE14]. Capture
[ASV+18, MBA+18, NYR+14].
Capture-the-Flag [MB+18]. Captured
[HWZZ19, SPK17], capturing [PKS18].
Card [BDFK12, HMR12, HCL+14, PDT12,
An17c, CLHJ13, GLIC10, LKL13,
Mar10b, Cho10, SD12]. CARDIS [GLC10].
Cards
[BS15, LA10, PWV+12, WGMdZ12,
WGMW12, CHS11, CHH+13, HCC10, KY10,
LH10c, LNM+11, LXMW12, MM12,
SSGCR+16, YZZ+14, YSL+10, YY13]. care
[FHV+16]. caricature [CLY18]. CarGANs
[CLY18]. Carlo [CR12, FVK17, GKH+17].
Carol [Xie12a, Xie12b]. Carry [GWM16].
Carring [PV17]. Carved [LC15].
CASC [DZS+18]. Cascade [WGD18].
cascaded [DGL19]. Cascading [GT12].
Case [Ano17c, DR11, Kn17, SBS+12,
SY15a, SRT12, Uto13, YL17, Dya19, KD18,
LKKL13, MD12a, SS17a]. Cases [SG19b].
Cash [YMWS11, Bro12, Pec12, Zor12].
Casting [CW12b]. cat [Pow14]. Catalan
[SAM+19b]. Catalog [AHS13]. Catching
[STX+19]. CBA [KRM+10]. CCA
[AHS14, BWLA16, CBXJ19, CZLC14,
HWS+19, LLPY19, LTZY16, LSLW15,
LLG19, M Sas12, PDNH15, SYL13, SLZ12,
yYqWqZC13, ZYY19, ZY17a, ZSW+18b].
CCA-secure [BWLA16, CZLC14, LTZY16,
SYL13, yYqWqZC13, ZSW+18b].
CCA1 [M Sas13]. CCA2 [Gal13, GV14b, LLW16,
LLSW16, MVVR12, RG10, ZZ12, ZY17b].
CCA2-secure [LLW16, ZY17b]. CCM
[SKK10]. CDF [Ara13]. CDH
[PDNH15, ZG10]. CDPS [LLL+17b].
CDTA [YFT17]. cell [LLY+12a].
cell-counting-based [LLY+12a]. Cells
[DSB16]. Cellular [d RsdlVC12, Ang16,
FMA+18, HBBRMN+16, HCM11, KFE19,
KRM+10, SS11, WOLS12]. Censorship
[DRS16]. Centers [SDC+17]. centralized
[NACLR12]. centre
[Mck10, McK11, Pal16, IS+16]. Centric
[DLZ+16b, FP19, Vle12, XHZ+19, ZVG16,
AHM+18, BLV17, BPP10, PN10, YYW+19].
centroid [LLY12]. Centuries
[Cer15, Cer18]. Certificate
[GWWC15, HP12, LTH+15, LDZ16,
WMS+12, YLZ+16, ZGCZ18, BJR+14,
GLL+18, Lan13, LHM+10, LDZ+14, LL16a,
MBF+13, NPH+14, JB11].
Certificate-Based
[GWWC15, HP12, LTH+15, LDZ16,
WMS+12, ZGCZ18, YLZ+16, GLL+18,
LHM+10, LDZ+14, LL16a]. Certificateless
[CT18, GWWC15, IL15, LSQZ17, LSQ18a,
LZCK14, RSD19, SZS14, TCL15, WMS+12,
YT11a, YT11b, YJSL18, YY17b, ZM18,
ZSY19, DXWD16, HPC12, JXLZ15, LL16b,
SGJ+18, ZQWZ10, ZY17b]. Certificates
[HP17, Mu16, SC12, GJ12, HRE14].
Certification [LDB+15, Ver17]. Certified
[ABBD13, CLL16, STC11, HL14, LH13,
WXWC14, YN19]. CertShim [NPH+14].
chaff [KHM13]. Chain
[EA+16, FV17, KPW13, QZL+16a,
QZL+16b, YFT17, YSF+18, YFT18, CR12,
Par18, CL16, SJWH+17]. Chaining
[GGK18, YM18, EA11]. Chains
[GKG19, JSK+17, HLYS14, JCH16].
Challenge
[AD12, GHS14, SPK17, YDH+15, ZCC15].
Challenges
[CN12, FREP17, FS15, Fra15, Lal14, LLG16,
MRs+17, PCY+17, SBV14, TCMLN19,
ALL+18, Hod19, KJN+16, WS14]. Changes
[ALL+18]. Change [KJM18, ZWT13].
Changeable [FGM10, ZCL+12], changed
[Mac12]. changes [PTRV18]. Changing
[Abb12]. Channel
[AMMV18, AN17, ASN11, ACA+16, Bar16b,
BCHC19, Bul18, CDK+10, CBL13, CATB19,
DZS+18, EWS14, GMW16, GPT14, HLH19,
KOP12, LGR14, LML16, NDC+13, PCR12,
SG15, TTD12, YL17, ZBF18, ADG16,
BVI12, BCN17, CPPT18, CAM19,
DMWS12, DJL12, GZW19, GS18V,
JLT+12, LM14, LFK19, MFH13, ZYG18].
Channels
[ASN12, BGN17, DMR15, EPAG16,
FDY+19, KW14, SS19, VCD16, Vua10,
YDV19, AGH+17, BCN19, BEB+18, CL16,
DMV15, DKL+16, LWZG10, MCL+19,
NR11, SM19b, SRB+12, WMU14, ZPZ+16].
Chaos [AIA+18a, LW13c, RRI11,
RVRS12, ARG19, CCLL11, LW13b,
j1T12b, ZLW+12, SGFCRM+18].
chaos-and-Hamming [CCL11].
Chaos-Based [RR11, RVRS12, AIA+18a, LW13c, ZLW+12]. Chaotic
Chapman [Ful10]. Character [SS12b].

Characteristic [BGJT14, NR15, SR10, ZWZ17a, BGJT13, Jou13].

Characterization [ALR13, BS13b, CRS18, DPCM16, RZ19, ZWZ17a, BGJT13, Jou13].

Characterizing [Ash14, JR13, RVS18, MPJ16, MHC12].

Charging [CKHP19, LSY16].

Cheater [KI11, Oba11].

Chebyshev [HD19, LWW19, LPdS10].

Check [GST12].

Check-before-Output [GST12].

Checkability [LHL14].

Checkable [IW14].

Checking [FYMY15, YL17, SYY17, YXA16, PZL19].

Chen [LLLK10].

Chennai [BC11].

China [BYL10, IEE11a, LTW11, Yan10].

Chinese [HF14a].

Chip [Bis17, HZS19, KS18a, LGLK17, MDAB10, BAB13, BGG13].

Chips [Man13, SOS15].

Chirp [OWHS12].

Cho [SPLHCB14].

choice [LLP18].

Choquet [SH11, SM11, SNM14].

Chosen [FSGW12, zGXW12, HLW12, JMG16, JSMG18a, KA17, LCLZ12a, LLML12, MH14, PDNH15, PPS12b, Rao17, RWZ12, RS10, SSW12, VSR12, WWHL12, XMLC13, XWLJ16, YM19, ZHW15, CPPT18, FSGW12, GLM16, GH12, HPY10, HKHK13, JSMG18b, KTT12, LCT14, LFWS15, LZC14, LDZW19, QRW18, RD17, SGM16, WZC16, WLFX17, XWS17, LAL15, LHL15].

Ciphertext-only [KA17].

Ciphertext-Policy [CHH19, Rao17, RL15].

Ciphertexts [LLPY19, Sta12, WQZ16, AHL12, JSMG18b, LCT14, NMP13, WXLY16, ZHY19, ZWY19].

Circuit [AH19, EAAAA19, Kar12, MTL11, XWS17, XWLJ16, LDM12, MS13a].

Circuit-Size [MTY11].

circumstance [ZLY19].

Circumventing [BAG12].

CISSP [STC11].

cities [LSZ19, SSH18].

Citizen [Ano16e].

City [Ano17d, GAI18, JZU19, LNK18a].

claimant [YI17].

Claims [SKGY14].

Clara
Content-centric [YWW+19], Contents [BCG10, MSM+18b, SKS+18], contest [Cra14].
Context [WXY+17], Contextual [Ma17a].
Context-aware [AKS19, Fra16, SY+19, ZCWS15, BGE+18, SSSA18].
Context-Driven [SY+19].
Controlled [FMTR12, HKK19, WP17, WXM19, Har16, SM10c, XLC+19].
Controller [GMVV17].
Controllers [AMH+16].
controls [CGH11].
controversy [McG11].
conundrum [Eve12].
Conversations [WBC+10].
Converse [KPKS12].
Conversion [BJ10b].
Comparer [Pau19].
Convertible [CLL16, LH11c, HLH11, XWC14].
Convex [LLSL19].
Convolution [DWZ18, HZW19, HW19].
Convolutional [WYL18, KMG17, MG15].
Cookie [FVJ19].
kickers [DCAT12].
CookiExt [BCFK15].
Cooperative [LL+12, SJWH+17, ZLDC15, WQZ+13].
Coordinate [YKK18].
Coppersmith [Dra16].
Coprime [GL19].
coprocessor [ABC+12, BGG+13, IBM13b].
coprocessors [GCVR17].
Copy [YT12, MHT+13].
Copyright [SJ12, ZWWW17, GJ13].
Core [LB13, YWF18, YS15, AVAH18, RS17c, HLYS14].
Cores [MGG+19].
CORMORANT [HFS12].
cornerstone [Tan17b].
Correct [PST13, Lan11].
CorrectDB [BS13a].
correcting [ATI+10, LTT10, MCP15].
Correction [KSH18a, LSC+15, yWXyZ+18, Chl13a, Sun16].
Correctness [YGS+17, WS13].
Correlated [RS10, Jia16, ZPZ+16].
Correlation [BW12, FAA+18, LD13, SDM+12, WWBC14, XHH12, YCL17].
correlations [Sar14].
Correspondence [SY+14].
corresponding [DWZ12].
Corrigendum [HYS18, WZM12a].
Corrupted [Fyo19].
cosmography [Pet11].
Cost [ABC+17, AMH+16, CMLS15, CJP12, GL12, HLT+15, LZZ+19a, Man13, NVM+17, WMX+17, WHL17, CZ14, CJP15, LEW19, Sar10a, YL11].
Cost-Effective [HLT+15, WHL17, WMX+17].
Costas [TRD11].
Costs [KHPP16, RPHJ11].
could [And19].
couldn’t [Bha16].
Countdown [Zet14].
Counter [ARP12, KM18, MKAS18, Fay16].
Counterexample [KPS13].
Counterfeit [YFT17].
Counterfeiting
counterfeits [Alz19, Ano16f, Bro12].

Countermeasure [BBB16a, MD12b, GJ19, HYL19].

Countermeasures [BGN17, DZS18, EWS14, PZPS15, DK17, FAA18].

Counters [BM18].

Counting [Bul18, LLY12a].

Coupling [SMS14].

Course [KKM11].

Cousins [BPBF12].

Cover [UUN13].

Covert [EPAG16, JTZ16, NSA15, VCD16, YDV19, LT13, LyWSZ10, SRB12].

CovertBand [NTKG17].

Cozzens [Led16, Sch15a].

CP [TY16, YMC17].

CP-ABE [YMC17].

CPM [PYM13].

CPS [FQZF18].

CPUs [AVAH18].

Crack [Fox13].

Cracked [Ano13d, McG11, McK12, Moo14].

Cracking [Gri15, GAS16, War11].

crawlers [GPN12].

CRC [Ful10, Joh10, GMSW14].

CRC/Taylor [Joh10].

Create [DFKC17, HGOZ19].

Creating [Bre18, OO10, Pau19].

Creation [GJJ18].

Creativity [WP15].

Credential [YLSZ19, JMWW16, KKM13, XMHD13].

Credentials [CG12a, SSW12].

Credible [ZW15].

credit [Mar10b].

crims [Pea11].

Critics [Odd12].

Criteria [PYS18, ZZKA17].

Criteria-Based [PYS18].

Critical [YWZ18].

crittografia [Sac14].

CRM [LHM15].

Cropper [KLK19].

Cropping [SR12].

Cross [AKK17, CLY14, DS15, LHM15, MV16a, YGFL15, YZL18, ZKH16, ZTSR12, SS17a, der10].

Cross-Border [ZTSR12].

Cross-Domain [CLY14, YZL18].

Cross-group [AKK17].

Cross-Layer [LHM15, ZKH16].

cross-matching [SS17a].

Cross-Site [DS15].

Crossword [Mar10a].

Crowd [Lal14, MJS19].

CRT [PT19].

CRT-exponent [PT19].

Crypt [HHAW19].

Cryptanalysis [Bar16b, BW12, Bor10, CWP12, CGCS12, DG12, DJG15, Far14, GST13, Gor10, HK14a, Hin10, IOM12, Jec10, JL18, Kha10, KN10, KWS12, LH10b, LNM11, LJJ16, LFX18, LSQ15, LSQ12, LJS16, MW12, MV19, MZ15, NB13, OTD10, PSOMPL13, SPLHCB14, SM10a, SM10b, TY16a, TG17, Vua10, Wag10, WYYY11, WYYY11, WSSO12, WYWY11, XQL11, YCL17, YMW11, AP11, BMB16, BKR11, Bul10a, Bu10b, CJ16, Con12, DMSD18, Eis10, FKV17, Her10, KDH13, LLLK10, LFW16, Nov10, PT19, RITF11, SD10, SD14, Sun11, StV10, Tam15, TSLL11, WYL14, WWBC14, AY12a, AY12b].

Cryptanalyzing [LLL17a, LLLL11, ZLW12].

CryptDB [PRZB12].

Cryptic [Mar10a].

Crypto [Ano13a, BCC19, DMO19, Goo12, MWES19, Pfl10, Rab10, SCPN10a, SCPN10b, SMSK18, WL11, BSR14, BGG13, PTRV18, Hom17].

Crypto-Currency [DMO19].

Crypto-stego [SMSK18].

cryptoanarchist [Pec12].

Cryptoclub [Ayu12, BP06].

Cryptocurrencies [BNMH17, JSK17, BH19].

Cryptocurrency [Ano16a, BH15, Eya17, FVB18, RM19].

cryptograms [Shy15].

Cryptographer [Dun12b, Kia11, Pie10].

Cryptographers [Ano16e, BPS16, Goo12].

Cryptographic [Abe12, AMKA17, AD12, ARH18b, ARH18a, ÁMVZ12, App15, AHWB20, BMP12, BBD19, BEM16, BR19, BCG12, BGB12, Bar15, BCM15, BCHL19, BIKK14, BLS12, BDP11, BFCZ12, BDGH15, Bia12, BKL13, BS15, BNA15, CCK12, CCK16, CK17, CFE16, jCPB12, CBL13, CHN18, Cor14b, CATB19, CFG17, DB16, Des10a, DQFL12, DR11, Ess17, FKS13, FY11, FLW12, Gir15, GM11, GLR10, GG11, Har16, HN10, HH1H13, HST14, HSA14, IBM13b, JR13, JHW19, KOP12, LYY11, LLK18, Loe15, MVM12, MKK17, MP12, MKAA17, Muf16, MK12b, NIS13, NA10b, PTT16, PFS12, PS14, PJ12, RMP10, RBG112,
cryptographic

[AY14a, ABB+14, ABF+14, ABC+14, ABO+17, BYDC19, Bar19, BFG+14, BJ10a, Bon19, CFL13, Cha13a, CFZ+10, CR10, CP13, CLCZ10, Cra11, DGYN14, DFK13, ESR14, GGH+16b, GJJ18, GJ10, GLR13, HYL+19, JCL+18, KKK+16, KAS15, KKK+16, LGKY10, LLL+17b, MS13c, Mat19, MMZ12, MM13, Mes15, MSGCDPS18, MN10, NDNR13, OO18, OMPSPL+19, Pal15, PLPW13, PSDo+13, QZDJ16, SD10, WT13, WMX+17, YSM14, ZHL+11, ZVH14, Sha10].

Cryptographic-Key

[SK11].

Cryptographical

[KU12].

Cryptographically

[ADD10, BCGH11, BJL2, BKLS18, MC11, NDG+17, PLvdLE10, SVCV15, CBL10, GCH15, HJM+11, SA14].

Cryptography

[ACZ16, Alz19, Ano15c, Ano15d, Ano16b, Ano16c, Ano16j, Ano19a, App14, AAB17, AG18, ACM+17, ARM15b, Bar12, BGK12, Bar15, BBCL19, BRT12, BCGN16, Big08, Bon12, BF19, BKVKV10, BJ10b, Buc10, BL17a, BL17b, BL18, BCF+14, CNR14, CT18, CJIHF14, Cas10, CMOG14, Che17, CST+17, DFZ16, CSW12, Cil11, Cra12, DDS12, Dan12, DK02, DK07, DK15, DXA14, DP17, DHT19, DHLWA10, DF16, DKS12, DR11, Eis10, Elb09, FPS12, FHL19, Feh10, FSK10, Fid18, FBM12, Fre10, GT19, GO17, GFBF12, Gol19, G13, Gre19a, GPT12, GLW12, Ham17, HEP+11, Hes12, H12, HR19, HPS08, HKR+18, JS18b, JT12a, KM10c, KP10, KAK8, LSL12a, Lin17, LWL10b, LGWY12, LMHH14, LGH+17, LWHS17, LPO+17, MO12, MS10, Maur12, Men13a, MR14c, Mic10b, MST18, MV12].

Cryptography Based

[MMB17, NNA10, NDR+19, Nic02, NS12, Orn16, PP10a, PÁBC+19, PPH12, PG12, RW12, Rog16, SY14, SG15, SOG15, Sch16c, Sch18, Sch19b, Sen10, SS13, Sen17, SK12b, Seo18, She17, SA16a, Sim15a, SGS14, Sma16, Sta11b, Ste15a, VS16, VD19, WWL+14, WY12, Wes16, Yan12, Yan11, YTS12, YL17, YY19, ZCCJ14, ZAC17, vRDHSP17, vTJ11, AMN18, AMORH13, AHE17, AAT16, AAA14, ABBD13, And19, Ano11a, ABW10, ACK+10, BOB13, BB14, Ber14, BL14, BL17, BAB+13, Blö12, BS+14, BS12, BBBBB16b, CFB11, Cha13b, CQX18, Cho14, CSTR16, Con12, CDSLY14, DAD14, DA18, DAV11, DD13, DMT19, Dur15, Far14, GCY17, GAB19, Har15, HH15, HZWW17, Hod19, Hof16, IM14, JLT+12, JY14, JW14, Kam19, KL08, KL15, KD18, KKM11, K10].

Cryptography-Related

[BOB13].

Cryptological

[Cil11].

Cryptology

[BC11, Bro11, Dun12b, LW11a, Lag19, PWBJ17, PJ12, AB10a, Abe10, BYL10, BL10, FES10, FGP14, Gil10, GO10, Kia11, LH10a, MZ17a, Pal16, Pie10, Rab10, HW10, LT11, Kobl10].

Cryptomaniacs

[Gen13].

Cryptographic Systems

[SLXX16].

Cryptosystem

[CCT+14, KD19, LH10b, SZHY19, SWM+10, WSQ+16, Zaj19, ACD18, AK14a, BS15, Chi13a, Gal13, GV14a, GLB+18, IB11].

Cryptography-Based

[BOB13].

Cryptographer

[Cil11].

Cryptography-Related

[Cil11].

Cryptological

[BOB13].

Cryptological Systems

[SLXX16].

Cryptosystem

[CCT+14, KD19, LH10b, SZHY19, SWM+10, WSQ+16, Zaj19, ACD18, AK14a, BS15, Chi13a, Gal13, GV14a, GLB+18, IB11].

Cryptography
LZ11, LYC+10, MM13, MG15, NZM10, SvT10, yYqWqZC13, YY11, YY13, sCR19a.

Cryptosystems [ADI11, CLND19, OTD10, PSM17, ZSP19, AHG18, AJYJ18, AVAH18, BNST17, FWS13, SA16b, ZYM19].

Cryptovirology [YY17a].

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

CTRL-PACE [HKK19]. Cube [HIJ19, MS12b, YWM19]. Cubic [RW12, VM14]. Cuckoo [BHKN13, sCR19a].

CUDA [DLV16]. Cue [KT4+18].


Current [DP17, GCK12, FPBG14]. Curse [GG11, HB14]. curvature [GJ15]. curve [GJ13]. Curve [ARM15a, ADI11, ADSH18, ARM15b, BJ10b, FHL19, GT19, GPT12, LGH17, LWHS17, MSTA17, NR15, PÁBC19, PPH12, SG15, vRDHSP17, AMN18, BL14, BL17, BBB16b, Cho14, Far14, FWS13, IB11, Kh18, KKM11, KK10, Kre13, KKD18, MCN18, MS13b, MHL18, NZM10, SKH15, WH17, YY13, JL16]. Curve25519 [SG15].

Curves [AMMV18, ACA+16, AK14b, BSCTV17, BWR12a, CMRH17, DW12, Gres19a, LL11, LT14a, MST18, Nag19, PWBJ17, Sch19b, She17, TX16, YTS12, BL17, BP18, FK19].


Cyber-Epionage [LJS14+16]. cyber-physical [HD19, HZWZ18, QMC17].

Cyber-security [vdWEG18]. Cybernetica [Ano17c]. Cybersecurity [Bel15, DF16, Hel17, Lan17, LRWV14, Mos18, Sch19a, SDC17, SPG19, YK16, AP18, GGH17].

CybSI [YK16]. Cycle [HG12, KU12, MKN13]. Cycle-Based [MKN13]. Cycles [BSCTV17, WBA17, CLCZ10].

D [AM19, AP10, Bro19, CG12b, DBPS12, DWWZ12, EAA16, GZHD12, KWS12, LJ17, LJ15, MCD18, MKH12, PGL110, RS16, SGS14, SRK17, SRK18, WSSO12, WK18, WY12, tWnCl12, Y14, YPR117].

D-Based [WSSO12]. D-like [LJ15].

D-PUF [SRK17, SRK18]. D2D [Gop19, PSM18]. D2D-Aided [Gop19].


Darel [Xie12a, Xie12b]. Darmstadt [FBM12, Sen10]. DASH [KCC17]. Data [AAA19, ARWK19, Ano13e, ADF12, Bar12, BJL16, BCD12, BJL12, BW12, BKLS18, CWL14, CMLS15, CW10, CSV15, CCT14, CIW16, CDLW19, CH19, DDS12, Dan12, DR12, DK16a, DMS16, DA12, DCA18, DLZ16b, Ebo99, EKOS19, EKB16, FMY15, FYD19, FPY15, FRS16, GTT11, GRRZ18, HSM14, HWZ18, HLC18, HLT15, HVP18, HXZ18, HK14b, IBM13a, KRDH13, KGV16, KPB18, KD19, LLPY19, LLZ17, LSL19, LWC14, LCP15, LLZ12, LZC12b, Ma17a, MLO17, Mal13, MMS17b, MJW18, MGJ19, MMI14b, NNAM10, NR12, PV17, PD14, PSM17, PZL19, PBC17, PH12b, PH16, PNRC17, PWS19, QZL16a, QZZ18, RCP18, Rea16, RDK19, RSN14, SG18, SAKM16, Sar10b, SMSK18, SP15b, SKH17, Sia12, SC19a, SLM10, SOR16, TCN17, Tan15a, Vai12, VSV15, WZCC18, WHLH17, XNB15, XWSW16, YDY16, YZDZ19, YJSL18, YMC17, XYL16, ZPXX17, ZTL15, ZLW17, AP10, AAH19].

DARE [AN10a]. Darmstadt [FBM12, Sen10]. DASH [KCC17]. Data [AAA19, ARWK19, Ano13e, ADF12, Bar12, BJL16, BCD12, BJL12, BW12, BKLS18, CWL14, CMLS15, CW10, CSV15, CCT14, CIW16, CDLW19, CH19, DDS12, Dan12, DR12, DK16a, DMS16, DA12, DCA18, DLZ16b, Ebo99, EKOS19, EKB16, FMY15, FYD19, FPY15, FRS16, GTT11, GRRZ18, HSM14, HWZ18, HLC18, HLT15, HVP18, HXZ18, HK14b, IBM13a, KRDH13, KGV16, KPB18, KD19, LLPY19, LLZ17, LSL19, LWC14, LCP15, LLZ12, LZC12b, Ma17a, MLO17, Mal13, MMS17b, MJW18, MGJ19, MMI14b, NNAM10, NR12, PV17, PD14, PSM17, PZL19, PBC17, PH12b, PH16, PNRC17, PWS19, QZL16a, QZZ18, RCP18, Rea16, RDK19, RSN14, SG18, SAKM16, Sar10b, SMSK18, SP15b, SKH17, Sia12, SC19a, SLM10, SOR16, TCN17, Tan15a, Vai12, VSV15, WZCC18, WHLH17, XNB15, XWSW16, YDY16, YZDZ19, YJSL18, YMC17, XYL16, ZPXX17, ZTL15, ZLW17, AP10, AAH19].
data
[ASO14, AIM+19, Ana14, Ano11a, Ara13, ADH17, ALL+18, BLL+19, BC16, BHH19, BTPLST15, BC18, BCGS16, BKV13, BTK15, CD16a, CDGC12, CLH+16, CDF+10, CDL18, DDY+19, DFJ+10, DTZZ12, DRD11, DYZ+15, DZC16, ED17, FS18, GHD19, Gen10, GSAAMCA18, GLB+18, GZS+18, HKA+18, HSM13, HKA19, HKW+15, HL19, HK19, HMC12, HH16, HYS18, HYF18, JKA+18, JLC18, JHCC14, KCS+18, Kim16, KV19b, KH18, KWH16, LSBN14, LT14b, LXX+14, LZY+16, LLL+17b, LLH17, LHL+18, LZW19, LFWS15, LAL+15, LCW+16, LZZ17, LLL+18, LLU16a, LHA+16, MHS14, MRR+18, MSGCDPSS18, NJB19, Nami19, OO18, OSS16, OSANAM19, PPG19, PMG19a, PWS19a, PZ15, QCX18, QLZ19, RR16, RR17, SLL+19, Sch15c, SD17, SYY+17, SM19a, SM19b, SAR18b, SPK17, SW+17, Tan17b, TMK11, TKMZ13, WLWG11, WLH13, WM17, WX17, WDZ19, WLS14, WZW13, WS14, WS19, WL19, XXX15].

Data-Centric [DLZ+16b].

Data-Classifiers [KGV16].

Data-Compression [DA12].

data-independent [BCGS16].

Data-Minimizing [BCD+15].

Data-Oriented [NNAM10].

Database [BTHJ12, SBV14, WCL+18, AAH+19, BL11, JHCC14, LW13a, PBP19, PRZB12, SVGE14, Suc12, XMY+17, YXD18].

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

Databases [ABL+18, FCM14, HPC10, JKHeY12, Kaw15, RP12, WP17, GA11, JK13, LCY+16, SS17a, TG12].

datacenters [PRN+19].

Dataset [SP13].

datasets [LVRY10].

DATS [HVP+18].

Daubechies [Ara13, SM12, ST15].

Daunting [IBM13a].

David [RNQ16].

Day [MBM17, Zet14, Hof16].

Days [Bai12, Bri11].

DB [PYH+18].

DBDH [CW14b].

DBMS [SERF12].

DC [LHF12].

DC-Net [LHF12].

DCT [LDB14, LP12, SS17b].

DDH [LZZ12a].

DDos [PSJ+13, SP15a].

De-synchronization [XNG+14, AATM18].

deadly [HLV10].

Dealing [Sha13, VN16].

Death [Moo14].

Debate [Bla16].

Debiasing [USH19].

Debs [Sm15b].

debugging [MFH13].

Decade [SOG15].

December [Abe10, BYL10, BC11, Che11, GG10, HWG10, LH10a, LWW11, Yan10, Yan11].

Decentralization [JP19].

Decentralized [ABCLI7, CD16b, GZZ+13, HSMY12, HK14b, MT17, PPS12a, PAS13b, RVH+16, RSN14, TS16b, XTZ+19, YM19, HHBS18, SLL+19, WZC16].

Decentralizing [LW+11b].

Deception [GA19, vdWEG18].

Deciding [CLCZ10, Sch12c].

Decipher [Cor14b].

Deciphering [Bla16, GMS15, GSAV18].

decision [PKA15, RPG12].

Decisional [CCL+19, LZZ14].

Decisions [Bel18a, YW10b].

declarations [HWYW14].

Declassified [ABJ13].

Decodable [Yek10].

decoder [PMG19a].

Decoding [DBPS12, GMS15, Bax14, Bu10a].

Decomposition [AGH+17, LSL+12b, gWP+14, BWA13].

Decompression [PP10b, SHC+16].

Deconstructing [Tar10].

Decoupling [DMO+19, IM16].

decos [VSB+19].

decryptable [MBP19].

Decrypted [Kob10].

Decryption [CR12, Tay19].

Decryption [AN12, KB10, PTK12, FNWL18, LJYW+17, LJYW18, SES+16, SM10a, SM10b, Wu16, XTZ+19, XYL19, ZSW+18b].

Dedicated [Lin17, Nac12, NSP+18, A1K19, RNQ16].

deductive [ABF+14].

Deduplication [CDLW19, MGJ19, QLL17, SKH17, YDY+16, YZD19, ZHZ+19, KH18, SAR18b, ZFH+18].

Deep [BNMH17, CRS+18, DLGT19].
develop [Ham19]. Developed [Har16]. developers [Ano14c]. Developing [CH11]. Development [Pau10]. Developments [GCK12, Vai11]. Device [ADMB, ABC17, CFX17, DFHC17, HSUS11, KLM12, SRK+17, SRK+18, TYK+12, ZSH+19, CRS13, GM16a, KKG14, Kim16, OSP+19, Par12b, SHBC19, VV19, XHH12].

Device-to-Device [ADMB]. Devices [AAC+16, ATC17, BDM+19, CSH+18, CRS+18, DLWW11, EGG+12, FMC19, GPT12, GMSV14, HHH+13, HDWH12, HFS+19, JMG+16, LFH18, LWS17, LL19, MAF16, May15, MS16, NVM+17, RC18, RSX18, RPHJ11, Sch15b, SFE10, SWF+19, VWC19, WKB16, WT10b, XJR+17, Aa15, BMDT19, CLP+13b, CFL13, CTL12, Chi13a, FRT13, GTSS19, HFF16, IB11, KPP16, LKAT12, MvO11, MV15, NSBM17, OYHS14, PCK19, SSNS15, SCR19b, SHBC19, TZTC16, TG17, W81b, Yon11, Y+17, YLS12, dR5dVC12, AGHP14, BPP10, Bro19, CCG10, Cla18, FLZ+12, Fri0a, GMS11, Har14, HAGT14, KM11, Lan13, LWZG10, MS13b, MM14a, MO14, QCH18, Sim15b, SLM10, yWpNyL11, ZZKA17, Zet14, ZSMS18, Ano13c, Ano15b, Mou15].


discount [WGD18]. Discount [GH12]. Directly [LZ12b]. directory [SSY12].


Digital [AAA+19, YTS15, BB13, BCP14a, FMS12a, FR15, GP17, HPO+15, Jin10, Joh10, JL16, LZC+12b, MBF+13, MS10, MNN12, MMHS16, NC12, pNyWyY+14, Orm16, PH12b, PAS13b, RCK17, SAA15, SM13, Söd13, SC12, SOS15, TC11, TAP19, TS16b, Yon11, Y+17, YLS12, dR5dVC12, AGHP14, BPP10, Bro19, CCG10, Cla18, FLZ+12, Fri0a, GMS11, Har14, HAGT14, KM11, Lan13, LWZG10, MS13b, MM14a, MO14, QCH18, Sim15b, SLM10, yWpNyL11, ZZKA17, Zet14, ZSMS18, Ano13c, Ano15b, Mou15].
PAF18, BW13, CFN+14. **Dual-Form** [HHS18]. **Dual-key-binding** [LZ11].

**Dual-Mode** [PAF18]. **Dual-Rail** [HF14b].

**Dubai** [Nor17]. **Duet** [VJH+18]. **Dummy** [GST12]. **Duplication** [LWLW11].

**Duo** [BPBF12]. **Durable** [LY15]. **Durfee** [TK19].

**During** [FGR+17, ABJ13, BD+19, RS17c]. **DWT** [AM19, LD13, SJ12]. **Dynadic** [MO14].

**Dyad** [VJH+18]. **Dummy** [GST12]. **Dyslexic** [Bha16].

**D-Cycle** [SAM+19b]. **Dynamic** [ABB19a, BK19, BCG10, EKB+16, FHR14, HH15, HK19, KYH18, LHM+15, MWZ12, MZ12, NKWF14, OMNER19, PPS12a, PNRC17, RC18, SSW12, SY14, SKV12, SGC14, SHC+16, VMV15, XNKG15, XWSW16, XZY+12, YLSZ19, ZXYL16, BSBG19, CTL12, CBY16, CSTR16, DCS12, EA11, GLM+11, GLB+18, JZS+10, KKM+13, KKK+18b, KH18, KPB17, LDC13, LLY06, LXMW12, LHM14, LZC17, LZZH19b, NSX+18, NPH+14, PZL+19, PSJ+13, SES+16, SSS11, SM10c, SGM16, WZ19, XHM14, YLS+18, YD17, ZSMS18, ZLL+18]. **dynamic-identity** [JZS+10]. **dynamical** [JTH+12b]. **Dynamics** [RSCX18, AaBT16, GEARH11, LTC+15a, Lüd12, MCRH19, THTC16].

**Dynamics-based** [AaBT16]. ** Dyslexic** [Bha16].

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

**E-Health** [AMSPL19, WMX+17, AKS19, IC17, OSP+19, YZL+18, JKL+16].

**E-Learning** [Yon11]. **e-mail** [BTW15, Sch16b]. **e-Passport** [HKK19, LZX10]. **e-Passports** [LG10].

**e-rental** [YLL14]. **E-Voting** [KV18, LGPRH14, KZZ17]. **E.T.** [Sch16a].

**E2** [WYL14]. **E2E** [KZZ+17]. **EAC** [LZX10]. **Each** [YLL+12]. **EAP** [FLH13, HZC+14, ZLL14]. **EAP-based** [HZC+14, ZLL14]. **EAP** [WYL14].

**Ears** [GWP+19]. **Early** [Bel18a, Bro11, And13]. **Earth** [Har14].

**Easier** [MBF+13]. **Easy** [Bel16, SMD11, Tay14, Wu16, ZDW+16].

**Eats** [DSSDW14, DSSDW17].

**Eavesdropping** [CWL16, Han12, PX13, YSJL14]. **EbH** [GDMLFLC17]. **EC** [Dra16, BLN16, CFN+14, CCG+16, CMG+18]. **ECB4CI** [YZW+18]. **ECC** [BSSV12, CBL10, HJ19, JMW+16, KRH18, MMS19, ZSH+19].

**ECC-Based** [BSSV12]. **ECDSA** [BBB+16a, BH19, DHB16]. **ECG** [GDMLFLC17, HZW19, HW19, PLGMCdF18, ZAA17]. **ECG-based** [PLGMCdF18].

**Echo** [DLMM+18, GWP+19, HGT15].

**Echo-Based** [HGT15]. **economic** [WZ19].

**Ecosystem** [FRI13, RVS+18]. **Ecosystems** [LBD+15, MMP19].

**E-dKrypts** [XZL+19].

**Ed25519** [TV19]. **EDA** [ABB19a].

**EdDS** [JL16]. **Edge** [AHM+18, DF16, KAI18, XH+19, CXW19, JZU+19, MD15, PRN+19, SUN16, XZP+19].

**Edge-Based** [XH+19]. **Edge-centric** [AHM+18]. **edge-enabled** [JZU+19].** Edges** [BDL+19].

**Edition** [Cor14a, Kob10, Gre19b].

**Editors** [LSQZ17, OK18, Ano19a].

**Education** [LRVW14].

**Edward** [Ano16a, Sim10]. **Edwards** [ADSH18, JL16, LT14a, YTS12].

**Edwards-curve** [JL16]. **EFADS** [WLS14].

**Effect** [PLGMCdF18, WB12].

**Effective** [HLT+15, KRDH13, WHLH17, WMX+17].

**Effectively** [YMC+17]. **effectiveness** [Eng15].

**Effects** [ASV+18, MAL10, SKV12, SHBC19].

**Efficiency** [ABF12, Chi16, DG17, FRS+16, HRV10, LLML12, LCL+17a, MS13b, WXY16].

**Efficient** [ABB13, ASBD16, ABB19a, BWLA16, BCGH11, BHG12, BBKL19, BV11, BV14, CG12a, CML+18, CS10, CMLRHS13, CWWL12, CZZ18, CJ13, DA18, DZC16, DWH12, Dun12a, DG17,
EM12, FLH13, FHS13, GT12, GH13, GTH11, GPN+12, GPT12, GJJ15, GH12, GZH17, GCH15, HZC+12, HZC+14, HZL18, HL10b, HBC13, HZX15, HKL+12, HDRFP15, HCD12, HH16, HC17, HZSL05, IAD10, JCL+18, KZ17, KPC+11, Kim15, KHPP16, KKK+18a, KH10, LLP+18, LDDAM12, LZT12, LNNH13, LXK+14, LC15, LZWZ19, LZC17, LLD19, LCLL15, LZWZ19, LSLW15, LSH19, LLYZ12, LCP15, LSY+16, LWHS17, LZC17, LLD19, LBOX12, MCI18, MCI11, MNI4, NES+14, NdMWW16, NZM10, NZW15, PB12, PA18, PZL+19, PR12, PG12, PCPK14, PNRC17, RSD19, RS17a, RM19, RBHP15, SLL+19, SGY11, SNS14, SOR16, SG16, TSB18, TLCF16, TWZ11, TT12, TM18.

**Efficient** [USH19, WDCL18, WLS14, WQZ+16, WCC18, XLWZ16, XMLC13, XMY+17, XH16, YHL16, YNR12a, YNR12b, YLW13, YNQ15, YLA+13, YS15, ZGY18, ZQWZ10, ZLH+12, ZSW+12, ZXJ+14, ZXYL16, ZCL+19, ZHS+19, ZPW16, ZHW15, ZZZ17, AHC18, AQRH+18, AZPC14, AZF+12, ABR15, BBB19, CH11, CCSW11, CLHJ13, CZ14, Cho14, Cra11, CGKO11, EA12, FLL+14, Fur14, FA14a, FA14b, FIO15, FLY16b, FZZ+12, FNWL18, GH16, GLM+11, HPC12, HYS18, ISC+16, IB11, IOV+18, JCHS16, JZS+10, KKK14, KV19b, KIH19, KL11, KSH18a, KSH18b, LLSL13, LH11b, LH10c, LWY+10, LXMW12, LLH17, LZD+19, LAL+15, MDM18, MLM16, Mes15, MGB19, Nov10, NSX10, OCDG11, PZBF18, PC14, Rao17, SMMK13, SM19b, TAA13, TLL12, Tso13, TKHK14, VN17, WYL13, WLZ+16, WT10a, WXK+17, XZW16, XW+12, yYqWqZC13, ZLY10, ZZ11, ZCLL14, ZT16, ZZC15, Zhu13, sCR19a, LLZ+12, TCL15].

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

**Effort** [RSBGN12].

**Effort-Release** [RSBGN12].

**eHealth** [TMGP13].

**eID** [SGGR16].

**eight** [Sun11].

**eight-round** [Sun11].

**Einführung** [Buc10].

**Einstein** [HR13, Wes15].

**Elbirt** [Bar12].

**Election** [AD19, Ess17, RS17b, TKM12].

**Elections** [CEL+19, QS18].

**Electoral** [CEL+19].

**Electric** [LSY+16].

**Electrical** [VTY18].

**electrocardiogram** [ZGL+18b].

**electrocardiogram-based** [ZGL+18b].

**Electrocardiography** [LLLH18, YH16].

**Electromagnetic** [HHH+13].

**Electronic** [Bla12, PWVT12, SR14, YMS11, CLC+19].

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

**Elements** [Kra12].

**Elevation** [LZC+12b].

**ElGamal** [HLH19, ADM19].

**ElGamal-like** [HLH19].

**Eliminating** [Söd13].

**Elimination** [FGQ16].

**Elliptic** [AMMV18, ARM15a, ADM19, ADI11, AK14b, ARM15b, BSCTV17, CMRH17, DW12, FHL19, Gre19a, GPT12, KKM11, LGH+17, LWHS17, MST17, MST18, NR15, PÁBC+19, PPH12, SG15, Sch19b, Sch17, vRDEHSP17, AMN18, BAA13, BL14, BL17, BBB16b, Cho14, Fur14, FK19, IB11, Kh18, K10, KKD+18, MCN+18, MS13b, MHL18, NZM10, SKH15, WHJ17, YY13].

**elliptic-curve** [BL17].

**Elliptic-Elgamal-Based** [ADM19].

**ELmD** [BDMLN16].

**Elsevier** [Ano15b].

**Email** [Bel16, CCS14, RS19, XJW+16, WR15].

**embed** [KPS10].

**Embedded** [AEP18, AB15, BS12, BJJ17, CFXY17, HJ19, HC17, JW+17, LJP17, LWHS17, MGG+19, SOG15, SK12b, SWF+19, SS17b, SDM+12, WXY+17, YGD+17, YS15, ZSL+19, Ano11a, CVG+13, Eis10, MFH13, WHZ+19, XZW16].

**Embedding** [CMRH17, FR15, KD12a, MCD12, XNRG15, XNP+18, XZZ18, YEL12, ZS12, EA11, LHM13, MKH+12, PWL13].

**Embeddings** [FHS13].

**Emergable** [YT12].

**emerged** [McG11].

**Emergence** [LMB12].

**Emergency**
[HLKL15, YTH17, BDM+19, KLC+10]. **Emerging** [BSV12, KSA16, OS16, FPBG14, GLL16, ZHH+17]. *emphasis* [GMT+12].

**Empirical** [gWpNyY+14, EBFK13, Sar14].

**Employees** [Mor12], **Employing** [LGLK17].

**EMV** [Cho10].

**Enable** [SMS14].

**Enabled** [GPT12, HFT16, KV18, QZL+16a, QZL+16b, SG12, SGC16, SPCR12, YSF+18, BMW12, JZU+19, NML19, TODQ18, YFT18].

**Enabled/disabled** [HFT16].

**Enables** [IBM13a].

**Enabling** [FRS+16, GYW+19, JSM+18, PSM+18, SSY12, WPZM16, YYS+16, MMP19, Sch12b].

**eNB** [CLM+12].

**Encapsulation** [KG19].

**Enciphering** [CMLRHS13, HMR12, MLCH10, MKASJ18, Sar11].

**Encodes** [DG17, HS18].

**Encoder** [PMG19a].

**Encoding** [BR14, CK18, SK12a, TJJZF12, XHX+17, CJL16, PC14, SM19a, Sun16].

**Encounter** [NA10a].

**Encrypt** [RAZS15, Ran14].

**Encrypted** [ADR18, BTHJ12, BSA+19, CWL+14, CWL16, Cor14a, CDLW19, CHH+19, DWB12, DCA18, FGRQ18, FCM14, FR5+16, Fyo19, Gen13, GLG12, GKG19, GZH17, GYW+19, HWZP18, HZTR12, HB17, HCDM12, IMB17, IBM13a, JSCM17, Kaw15, KGV16, LA15, LGLK17, LQD+16, Lop16, Mur16, NBZP17, NNAM10, PBC+17, QLL17, Roh19, SAK16, SZHY19, Sia12, SOR16, TM18, Uto13, Vαι12, WBC+10, XWSW16, YDY+16, ZDL12, ZXYL16, ZVG16, ZLW+17, ACMP19, AAH+19, AHM+18, AZH11, BBPD16, BTPLST15, BGP+17, BVK13, BTIK15, BL11, CH11, Cri16, CDL18, DDY+19, DKL+16, DRD11, DJ19, ED17, FTV+10, Gen10, GSAMCA18, GZS+18, GSGM16, HKA19, HH16, JCL18, KHZ18, LKX+14, LHY+16, LHL+18, LZWZ19, LW13a, MRR+18, NJB19, OSSK16, PW919a, PB19, PRZB12, SG19a, Schl0b, SEXY18, SM19b, SWW+17, Suc12, TKMZ13, WR15, WS19, WL19, XMY+17, XWA+18, Yaa19, YXD18, YQOL17].

**encrypted** [YQZ+19, YJC18, ZLY10, ZZC17, ZF+18, ZHT16, ZZL+19].

**Encryption** [CC10, Mar10c, dRSdVLC12, Cia18, LFSGCCRP14, Pow14].

**Encryption** [ADM12, AV12, AUA18, AEH17, Alo12, AAC+16, AEP18, Ano13e, Ano14b, Ano15c, Ano17d, Arm19, AKP12, ABF12, AS16, Ag18, BVS+13, BWL16, BPR14a, BPR14b, Bel16, BDOZ11, BWR12a, BS14, BV18, Bla16, BKLS12, BPDS12, BHJP14, BDMN16, Boy13, BV11, BV14, BGV14, CVM14, CMO+16, CLL16, CWWL12, CN12, CZF12, CLHC12, Che15, Che18, CGL+12, Chii12, Chu16, CRE+12, Con18, CNT12, CLW16, CD16b, DR10, DN12, DFJ+10, DSLB18, Des10b, DGFH18, DOS15, Dun12a, DF11, EAA12, ESS12, FHH10b, FHR14, FJJH12, Fei19, FFL12, Fuc11, GWCC15, GGH+16a, GHGW17, GM13a, GZZ+13, GSW+16, GH11a, GH11b, GHS12, GHP512, GDCC16, GVW12, GVW15, GM14, GL12, GKS17, Gue16, HSMY12, HLLG18, HZ11, HG12, HWS+19, Hor19, HC17, HTC+15, HLH19, HP12, Int19, IAD10, JLS12, JSA17, JLB12].

**Encryption** [Jia14a, JR14, Kam13, KB10, KME+12, KMY18, KTT12, KOS16, KKA15, KFS12, KHPP16, KKK+18a, KJ18, KS12, KHRG19, LGMC17, LMG+18, Lau17, Led16, LSLW16, LLPY19, LW11b, LW11c, LW12, LJJL12, LZY+13, LHL+14, LLL+15, LTTZ16, LLL17a, LFX+18, LLLH18, LSLW15, LH11c, LSOL18b, LNWZ19, LB13, LY15, LW16, LYY+18b, LATV17, LLM12, LH18, MZNY15, MLO17, MPM14, MR14a, MT11, MM18a, MVV12, MMS17b, MSR+17, MRL+18, MBF18, MPS12, MZZS18, Mor19b, MT12, MKR10, MSas12, Nac16, NDMM1W16, NT12, NMS14, NAL17, OT12, OGK+15, ODIS17, PMZ13, PR12, PB12, PDHN15, PRBAS19, Per13, PKTK12, PPS12a, PYS18, PMZ12, PCY+17, PRSV17, PWS+19b, RVH+16, RCP+18, ...
Encryption
[Sta12, SGH15, SMOP15, Tan11, TCN17, TCL15, TMC15, Tan17b, TDT13, TKR14, TT12, TFS19, Unr11, Vai11, VSR12, VOG15, Wal18, WHC15, WP17, WDCL18, WSS12, Wat12, WLC12, WDDW12, WZ15, WHLH17, WWHL12, WMS12, WZC19, XNK15, XY18, XXZ12, XJJW13, XJWJ16, XJW16, XHX17, YZ12, YZX12, Ye10, Ye14, YH16, YKNS12, YNQ15, YKC11, Ano15c, BRR15, BGP17, JZU19, JSA17, FWS13, AK14b, LGH17].

Encryption-based
[SERF12, BC18, XWZ18].

Encryption/Decryption
[KB10].

Encryptions
[zGXW12, LG12, SLY16, RD17].

Encyclopedia
[vTJ11].

End
[Ano15c, BRR15, BGP17, CFE16, Chn16, MHMSGH16, RST15a, RST15b, BCT15, Bro19, CPT18, CFVP16, CFZ10, CW14b, CLH16, CMMS17, CLC19, CXWT19, CZ15b, CS11, Chm10, CW12a, CJW19, CDF10].

end-devices
[Ano15c, BRR15, BGP17, JZU19, JSA17].

endomorphism
[FWS13].

Endomorphisms
[AK14b, LGH17].

Endurance
[JS17].

Endurance-Aware
[JS17]. enemies
[Fag17].

Enemy
[BC14, CAC14].

Energetic
[PD12].

Energy
[Ano15c, AZF12, ABC17, Bla16, CKHP19, GPR19, JEA15, LSC15, LA12, LZ12, LFZ17, LW18, LCT14, LFWS15, LLM19, LPdS10, LHH11, LW10, LK10, LW13b, LZC14, LPZ15, LCY16, LZC17, LJW17, LJYW18, LLL18, LZKX19, LDZW19, LL16a, LW13c, LSC12, LLG19, MBP19, Mar12, Mar10b, MMS17c, Mes15, MML16, Mid10, Mon13, MSA13, NES14, Nam19, OP16C16, OSN19, PPA18, PEP12, PBP19, QW18, Ran16, RGI10, RWZ13, RPSL10, SES16, SE18, SLL19, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14].

encryption
[CM13, CGKO11, DLZ16a, DDM17, DTZ12, DMD18, Eve12, Eve16, FAA18, FHI13, FSGW11, FSGW12, FMB18, Fay16, GMOGCC15, GH13, GHPS13, GLM16, GH12, GL18, GZX19, HGWW11, HQZH14, HZL18, HKA19, HDWL16, HZWX18, H19, HT13, HL11, HK19, HL11, HY17, H16, HT17, HY18, HY19, HHHW19, HKHK13, JZU19, JCHS16, JCL18, Jia14b, JSMG18a, JSMG18b, JHCC14, JSM18, Kam16, KHMB13, KKM14, K12, KL12, LZ12, LFZ17, LW18, LCT14, LFWS15, LLM19, LPdS10, LHH11, LW10, LK10, LW13b, LZC14, LPZ15, LCY16, LZC17, LJW17, LJYW18, LLL18, LZKX19, LDZW19, LL16a, LW13c, LSC12, LLG19, MBP19, Mar12, Mar10b, MMS17c, Mes15, MML16, Mid10, Mon13, MSA13, NES14, Nam19, OP16C16, OSN19, PPA18, PEP12, PBP19, QW18, Ran16, RGI10, RWZ13, RPSL10, SES16, SE18, SLL19, Sar11, SYL13, SE14, SE16, SH11, SM11, SNM14].
LLD19, MP12, PAF18, RPHJ11, TLCF16, TCN+17, VN17, AHG18, CZ14, Fai19, HRK+19, MMF15, ZT16]. energy-based [MMF15]. Energy-Efficient [LLD19, MP12, TLCF16, AHG18].

Energy-Harvesting [ABC+17].

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

Enforcement [LLZ+17, Tan15a, Cra11, CFG+17]. Engage [SDE+17]. engagement [LSBN14].

engaging [ISC+16]. engine [BS13a].

Engineering [BCHL19, Be18a, FSK10, GHD19, LLK18, MMK16, SM18a, MP12, PGL11, SNG+17, TQL+14]. Engines [LB13, BGG+13]. Enhance [DHT+19, CZ14, SLM10]. Enhanced

[DTE17, KY10, KKM+13, MS17, SGG18, SS15, TV15, Y11, YCC16, AMN18, AM19, ACK+10, DLK+16, DXW16, GM16a, LNK13, YWZ+17, YQO17].

Enhancement [FSX12b, JSA17, LA15, NNA10, CHS11, SYV19]. Enhancements [Che18, FSX12c]. Enhancing [CSW12, IA15, Lan13, MZL+19, YS15, AGBR19].

Enigma [KM15, KM16, LHA+16, Ore14, Ano16d, Bur11, Cas15, Kap11, Kap13, McG11, McK12, Tur18]. Enigmas [Bat10].

Enough [JCM12, Ano14b]. Enrollment [YWZ+12, DEL19]. ensuing [SS17a].

Ensure [PWS+19a]., entangled [EAB+19].

Entanglement [Ano15d]. JEA+15. Entanglement-Based [JEA+15].


Entrepreneur [IM16]. Entropy [DSS14, DSS17, DK16, KP13, VS16, YGFL15, BNY14, TBK+18].

Entropy-Based [YGL15]. entTTS [YL17]. enumerators [ÖS11]. Environment [AARJ12, BCGN16, FYD+19, HQY+18, KKA15, MLO17, MRS+17, RQD+15, SSG18, SAM+19a, TV15, VFFHF19, YMA17, FHZW18, GAI+18, HL19, HLS14, KKM+14, Kim16, KS19, NR17, Par12b, RR16, SYW19, SKB+17, WL12, WCFW18, WT10a, XXX15, YWK+10a].

Environment-Independent [HQY+18].

Environments [HXHP17, HLKL15, LQY10, PAS13b, TMGP13, VFS+19, XLP+18, CNF+18, CLHJ13, CTL13, KPP16, KAS15, LNK+18b, LW13a, LCY+17, MHL18, NACLR12, SCY15, SA19, Tan12b, VDO14, VGL14].

Eof [Gup15]. ePassport [ABHC+16].


Equational [ABR12]. Equations [BB10, SR12a, DGL19, ZYGT17].

Equi [Ma17a, PD14]. Equi-Join [PD14, Ma17a].

Equifax [Ber17]. Equijoin [WP17]. equipped [KNT13]. Equivalence [ABR12, CCK12, CCCK16, GLW12, LYL+18, SS13, WGD18, HKT11]. Era [Mos18, OMNER19, KV19a, QCX18, ABJ13].

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

Error [GSGM16, KW14, LSC+15, MCP15, MKASJ18, TLCF16, Za19, ATT+10, BZD16a, Chi13a, CJW+19, LTT10].


Establishment [ASN12, Ano11b, BCO13, DL12, NYR+14, BEB+18, GTSS19, SZMK13, ZPZ+16, ZXW+18]. Estimating [VJH+18, MMF15]. Estimation [BCF16, GSN+16]. Estonian [Ano17c].
Fabrication-Induced [VDB+16]. Face [AQD12, MHW+19, RSX18, XHH12]. Facet [KRB12, TCMLN19, WSS+19]. facilitate [Chi13a]. Facsimile [Ano16e]. Factor [AMSPL19, ATC17, HXC+12, LLC11, PSSK19, AIB+16, BD18, CLP+13b, CNF+18, DR16, DMWS12, ED19, GMN+11, HC12, IC17, JKL+16, JM+16, Kem11, LNK+18a, LNK+18b, LW19, Lit14, MDHM18, NMX15, SNG+17, WW14, Wat14a]. Factoring [APPV15, KV19a, LMLL12, BGG+19, MM13, SD17]. Factorization [Coulb, FS15, HWS+19, KKK+18a, KFL+10, Kuz11, YAM+15, Mes15, TPL16].


False [KU14]. Fallen [HCPLS12]. False [LLZ+12, MWES19, CDGC12]. Families [BSS+13, KU12, FK19]. Family [ARH+18b, BMS12, BKST18, CB19, DG12, DJ+15, FLS+10, FFL12, GNL12, LYY+18b, MFG16, SB15, YCL17, BDVP12]. Fanin [S12a]. Fast [BLAN+16, Bru12, CHS15, DSLB18, DGK18, GSN+16, HMKG19, JGP+18, KL+18, LGLK17, NR12, PRSV17, Razi19, Rom11, SRR18, WHZ12, WBA17, WQZ+13, ZHW+16, FH10a, KHMB13, LNNH13, MBB11, YM18].

FastAD [SMBA10]. Faster [CN12, EZW18, FHLORH18, HVL17, TH16, ZSP+19, Ant14]. Fault [AMKA17, BMS12, BBB+16a, FXP+17, GST12, JWJ+17, JKP12, JT12a, LY19, LGL+12, LCLW17, LGLL12, MSS17, MKRM10, MKAA17, PH12a, RZZ+15, SMB15, SEY14, WCD19, YGD+17, BEM16, BBBP13, PBCC14, WMYR16].
Finding [Ano11b, Ber12, GQH17, DDS12, Dan12].

Financial [Hof16, Ste15a]. Fine [CDD13, PV17, YTH17, ZML17, CLH+16, FSGW11, LHH+18, XYLML19].

Fine-Grained [CDD13, PV17, YTH17, ZML17, CLH+16, LHH+18, XYLML19].

Finely [KLY+11]. Fingerprinting [FSGW11, LHH13].

First-Generation [BH15]. First-Order [FVJ19, HLV10].

First-Order-Based [LHW18].

First-time [WDG19]. FinTech [MZL+19].

firms [Ano15c]. First [Ano17d, BH15, DR10, LFX+18, LSQ17, MS17, PC16, W1118, AB10a, BCV12, Bre18, Con17, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14].

First-Generation [BH15]. First-Order [FVJ19]. Finite [BGJ14, CHS15, GMNS15, HVL17, HWS+19, WDG19, ZL19, AA14, BGJT13, CZ15a, GPLZ13, LBOX12, QF19].

Finite-State-Machine [CHS15].

Finite-time [WDG19]. FinTech [MZL+19].

firms [Ano15c]. First [Ano17d, BH15, DR10, LFX+18, LSQ17, MS17, PC16, W1118, AB10a, BCV12, Bre18, Con17, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14].

First-Generation [BH15]. First-Order [FVJ19]. Finite [BGJ14, CHS15, GMNS15, HVL17, HWS+19, WDG19, ZL19, AA14, BGJT13, CZ15a, GPLZ13, LBOX12, QF19].

Finite-State-Machine [CHS15].

Finite-time [WDG19]. FinTech [MZL+19].

firms [Ano15c]. First [Ano17d, BH15, DR10, LFX+18, LSQ17, MS17, PC16, W1118, AB10a, BCV12, Bre18, Con17, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14].

First-Generation [BH15]. First-Order [FVJ19]. Finite [BGJ14, CHS15, GMNS15, HVL17, HWS+19, WDG19, ZL19, AA14, BGJT13, CZ15a, GPLZ13, LBOX12, QF19].

Finite-State-Machine [CHS15].

Finite-time [WDG19]. FinTech [MZL+19].

firms [Ano15c]. First [Ano17d, BH15, DR10, LFX+18, LSQ17, MS17, PC16, W1118, AB10a, BCV12, Bre18, Con17, Kim11, LCKBJ12, Mic10a, SBK+17, Zet14].

First-Generation [BH15]. First-Order [FVJ19]. Finite [BGJ14, CHS15, GMNS15, HVL17, HWS+19, WDG19, ZL19, AA14, BGJT13, CZ15a, GPLZ13, LBOX12, QF19].

Finite-State-Machine [CHS15].

Finite-time [WDG19]. FinTech [MZL+19].
**FPGA-Based** [RJV+18]. **FPGA/ASIC** [CFZ+10]. **FPGAs** [DGP10, GT19, RHLK18, SMOP15, VMV15]. **Fractal** [JTZ+16, KM11]. **fraction** [IK15]. **fractal** [BW13, VM14]. **Fragile** [AAA+19, CHHW12, MCD12, SSA13, WK18, ZWZ17a, CCLL11, PGLL10, WHZ12]. **fragment** [BPP10]. **Fragmentation** [BDPS12, CDFZ+10]. **frame** [FMB+18, YQH12]. **Frames** [DG17, IM14]. **Framework** [BJL16, CD12, DG17, HXC+11, KPC+16, KYEV+18, LLG15, LSC+15, LY15, LQD+16, LNG19, MSU13, SK11, Scr18, SYC+17, SEK+19, TSH14, VPK17, XHZ+19, ZJ14, ATKH+17, BHCdFR12, CRS13, GQH17, GM13b, HPL+19, JZU+19, KKGK10, KM14, KS19, MMS+17a, MBF+13, PSQ+13, PLCGS11, PKA15, SD10, SA16b, SYW17, SA19, ZYC+17]. **frameworks** [LSBN14]. **France** [Kap11]. **Francis** [Joh10]. **Francisco** [Dun12b, Kia11, Pie10]. **Francois** [SR14]. **Frank** [ABJ13, Joh10, Mar10a]. **frankencerts** [BJR+14]. **Fraud** [Ber12, CEL+19, MT17]. **Fred** [Xie12a, Xie12b]. **Free** [App13, Boy16, CDD19, CDD20, HLH19, IL15, LSQZ17, LSQL18a, TWZ+12, TTH15, WZCH19, YY17b, ZHL+12, ZM18, AYJG18, ATK11, ED19, LYC+10, LL16a, SA12, SE16, YT11b]. **Free-View** [TWZ+12]. **FreeBSD** [MNNW15]. **Freedom** [Con18]. **Freestart** [SKP15]. **Freeze** [HHAW19]. **French** [Ant14]. **Frequency** [BBM15, KAHKB17, LTKP16, LWCJ14, TC10, CJP12, CJP15, EA12, NLYZ12]. **Frequency-Based** [LWCJ14]. **fresh** [GJ19]. **Freshness** [RBNB15]. **Fresnelet** [FMB+18]. **Friendly** [Fra16, KCC17, SZDL14, ACM12, BP18, FK19, KLW+16, RD17, WOLS12]. **Frontside** [DDR+16]. **FSR** [MD12b]. **FSR-Based** [MD12b]. **Fugue** [AP11]. **Fujisaki** [TFS19]. **Full** [Arm19, ALR13, DGFH18, HR19, HEC+12, LW12, VS16, WLC12, BKR11, DDM17, LC13, Ran16, SWW+17, SKP15, Tam15, TY16b]. **full-hiding** [DDM17]. **full-text** [SWW+17]. **Fully** [AKP12, BV11, BV14, BGV14, CMO+16, CN12, CZF12, CXT12, DOS15, GH11a, GH11b, GHS12, HLLC11, KKK+18a, LMGC17, LSLW15, LJM16, LATV17, LSC12, MVV12, MSMS18a, Nac16, NCC13, PB12, SGH15, Val11, VV19, WHC+15, XWW+18, ZZ12, DDL15, GH13, MBP19, ZXJ+14, ZML17]. **Fully-Homomorphic** [GH11b]. **Fully-Homomorphic-Encryption** [CN12]. **Fun** [APPVP15]. **Function** [AMPH14, Bec17, BKST18, BBKL19, CJJ13, FLS+10, GKK18, GKG19, GHPY18, LJJF19, LyWIZZ12, MMS17b, RJV+18, SGY11, WSO12, YWW+19, AKY13, ABO+17, AP11, Bar19, BDPV12, CMM17, Con17, LK14, LP11, RS14, Sar11, SXL16, SCBL16, TQL+14, WYY14]. **Function-based** [YWJ+19]. **Functional** [AS16, BV18, BSY12, Boy13, GGH+16a, GHW12, LQD+16, MVV12, RS15, Wat12, ZYT13, ZWTM15, ZWM14]. **Functionalities** [JR13]. **Functions** [ACZ16, ALR13, BBC+14, BKK14, BKPW12, BHT18, BKK12a, CCL+19, CPS16, DSSM14, DQFI12, FY11, LVV11, NIS15, NR12, Rja12, RD12, SMD14, SLY+16, Tan12a, WCXZ17, YTP11, AY14a, BDP11, BDK16, BCS16, CG12b, CQX18, CW12a, ESRJ14, Gen10, HRP10, HLU12, Kom18, Li10, QZDJ13, WT13]. **fundamental** [Breb18]. **Fundamentals** [Joh10]. **Further** [HCL+14, WHY+12]. **Fus** [FMS12a]. **Fusion** [ABCL17, YYK+17, HW19]. **Future** [AYS15, BCE+12, BKK14, Bon12, BLU+15, CDF16, Fri13, GCK12, HYS18, KHH+11, Mon13, SG19b, AP18, Ano13f, Dva19, FPBG14, Mac12, PPA18, PHWM10, MJS13]. **Future-proof** [Mon13]. **Fuzzy** [HWZP18, KRD13, NC12, SH11, USH19, XJWW13, Alp18, BSBG19, HK17, KHM13, LYC+10, MMS13, SM11, SMN14, SC19b].
FV [MRL+18, RJV+18].


Generating [Ano16f, Con17]. Generation [ABS+12, BCGH11, BH15, GT19, HEP+11, LKBK19, LTC+15b, MR14a, MJGS12, NIS12, PS14, SOS15, SRK+17, SRK+18, XJR+17, Aia15, ACD+15, BDK16, CJXX19, GMRT+15, GMdFPLC17, GCH15, KHM13, KKM+13, OMPSP+19, SGFCRM+18, SPK17, TBK+18, XW13, YDH+15, ZYGT17, ZYGY18, ZHL+11].

Generator [ADD10, BK12a, CDK+10, MVV12, NNA+10, NWF14, CFY+10, LGY10, MRT10, PLsvdLE10, SH11, SM11, XSWC10].

Generators [AS17, DLSB18, LTKP16, MFG16, NIS12, PFS12, CP13, GR19b, HRV10, MG15, Sti11, Zim10].

Generic [BWLA16, BR14, Ch16, DL17, GWWC15, HXC+11, Sar10b, SY15a, WCL+18, ZCLL14, GM13b, HQY+16, NXS10, Y11b, ZYM19].

generically [MIKS14]. Genetic [JK13, MM17a, ASVE13, EEAZ13, PTK14].

genius [Hai17]. Genomic [BKLS18, RCP+18]. Gentry [GH11b].


geo-location [Har14]. geodesics [ZZCJ14].

Geographic [LC17]. Geolocation [FPY15].

Geometric [ACA+16, DSB16, GT11, WLZL12, YWNW15, CLZ+17, GZH12, LWZ19].

generically [WLW+13]. Geometry [tWmC12, CFR11, CZ15a]. geospatial [HK19].

German [BDFK12, B1d12, Buc10, Cop10a]. Germany [FBM12, GLIC10, Sen10, Wat10].

Gesture [LCL17b, RSX18, SCR19b, SHBC19].

get-base [SHBC19]. gesture-typing [SCR19b].

Gestures [AUMT16, KTM+18, GCSAdP11]. Get [GPT14, Sch11]. gets [Cou12a, Kum10].

Getting [ESS15]. GF [GT19].

GHD [CJL16, LH10b]. GH [AK14a]. GH-public [AK14a].

Ghost [CDA14]. GHZ [CCL+13].
GHZ-State [CCL+13]. giant [Joh15].
GIFT [CWZ19]. girls [Mun17]. Girod
[GMNS15]. given [Bar19]. GLARM
[LLZ+16]. Glass [Fyo19]. glimpse [Mic10a].
Global [CLP13a, CLH13, MR5+17, GH16,
LH11b, TMK11, ZK11, LNK+18a]. Globally
[CCS14, LG10]. Glyph [XZZ18]. GMAC
[SKK10]. Goal [BMP12]. Goal-Driven
[BMP12]. Goes [BCD+12, RY10].
Goldfeder [Ano16a]. Goldreich [Lin17].
Goldfeder [Ano16a]. Goldreich [Lin17].
Goldstrike [BH15]. Goldwasser [Gol19].
Goliath [Sch15c]. Gong [LLW16]. Good
[DQFL12, FY11, Raz19, LBN14, RY10,
SA14, WT13]. goodbye [HU15].
Google [Har14, Loe15, VGN14]. Goppa
[Ran14]. GPGPU [CBL10, RVRSCM12].
GPGPUs [TLCF16]. GPUs [AVAH18, VKP17].
Graduated [BR14].
grail [Wat15, Mic10a]. Grain
[BMS12, SBM15, FSGW11]. Grained
[CDD13, PV17, YTH17, CLH5+16, LHH5+18,
XYML19, ZML17]. Granular [SY5+19].
Graph [ATS15, GTM11, WH18, GJMP15].
graph-based [GJMP15]. graphical [SKH15].
Graphical [BCV12, MC19, CTL12, Eng15,
LTC5+15a, MZL5+19]. graphical-based
[CTL12]. Graphics
[HMMK14, ABDP15, KY10, PGLL10].
Graphs [BFM12, KU12, KA18, Lau17,
PMZ12, BBGT12, KLN15]. Grassroots
[GB19]. Gray [DA10, UUN13]. Gray-Level
[DA10]. Great [Az11]. green
dCCSB5+16, ZT16]. Grey
[BCKP17, LRW13]. Grey-box [LRW13].
GREYC [AGBR19]. GREYC-Hashing
[AGBR19]. Grid
[CGB5+10, DLZ5+16b, KS15, LPL15, VTY18,
AMN18, BC16, CDWM19, DZC16, JAS5+11,
MCN5+18, WS12, YY11, ZZY5+19].
Grid-Based [LPL15, WS12]. Grids [SC10,
CT11b, GLW13, LKW5+19, Shy15, JAE10].
Gröbner [EVP10, FES10, Tam15]. Gros
[Dan12]. Gröstl [ABO5+17]. Ground
[KP17]. Group [AEHS15, BSBB19, BV12,
CZCD18, CGY5+13, CLW16, DT13, FVS17,
HL10a, Har13, L5+16, LCCJ13, LWL5+17,
TW14, XLM5+12, XGLM14, XZLW15,
YJSL18, ZK16, AKK5+17, CML5+18,
GBN11, HCCC11, HPY10, IOV5+18,
LLLS13, LWS10, LLM5+19, PY19, RS15,
SCBL16, WDZL13, WTT12, YZL5+18,
YLL5+18, ZZKA17, ZWQ5+11, ZGL5+18a].
Group-based [LL5+16, CML5+18].
group-key [IOV5+18]. Grouping [LNZ5+13].
Grouping-Proofs-Based [LNZ5+13].
Groups
[Abe12, GZ12, HWS5+19, NKG15, YS12,
YKNS12, LLY06, MZ17a, WQZ5+13, ZZ15].
Grover [JL18]. GRS [TD14]. GSR [LC17].
Guangdong [IEE11a]. Guaranteed
[TBCB15]. Guarantees [FVB5+18].
Guerrillas [Has16]. Guess
[FSCF11, Fok12]. Guessing
[Che15, LCL17b, XJW13, FIO15]. Guest
[Ano19a, Gup15, BdD19, LKL18].
Guidance [BD15]. Guide
[She17, STC11, Han12, Gre19a]. Guided
[CJFH14, ZS5+18]. Guiding [DG5+14].
GVW [HLC5+19]. gwAs [SAM5+19a].
Gyroscopes [SNK18]. GyroFinger
[SNK18].


Human [HHS+15, HZW19, IA15, DMT12, HZW19, H19, LWW+10, PYH+18]. Humans [RBNB15, RB17]. Hummingbird [ESS12].


Hybrid-Double [ARM15b]. hybrid-indexed [WXLY16]. hybridization [MMSD13]. Hyderabad [GG10]. Hyper [BL14, KO14, LZXR19, WGX+12].


ICISSP [Ano19a]. ICN [CHL19]. ICs [GSFT16]. ID [Ano17c, CTL13, CDP16a, EZ15, HCC10, IB11, KGO10, LGMC17, LY14, MWZ12, MM12, MMZ12, Mes15, PLPW13, Rom11, TPL16, TT12, TTH15, Wan18a, WDZ19, WT10b, WTT12, HWWZ19]. ID-based [MM12, LGMC17, MWZ12, TT12, TTH15, WT10b, CTL13, EZ15, HCC10, IB11, KGO10, LY14, MMZ12, Mes15, PLPW13, TPL16, Wan18a, WDZ19, WTT12].

ID-card [Ano17c]. ID2S [YRT+16]. IDEA [BNY14]. Ideal [LPO+17, WCL+18, HKT11, yQyWqZC13]. idealness [TD14]. Ideas [FREP17, Mac12].

idempotent [Dur15]. Identical [Bow11]. Identifiable [Oba11]. Identification [CZCD18, FSX12b, FSX12c, FSX12a, HWWZ19, KGP+19, VCA15, YGFL15, YK18, AGLW16, BOP14, CTHP13, CJP12, CIP15, DJ19, EA12, HQY+16, HL19, KI11, KI13, NLYZ12, WYZ+17, YTM+14, ZAAB17]. identified [AZH11]. Identifier [LHW18, GSGM16, MJS13]. identifiers [Cer18]. Identifying [Bel18b, CZ19, CSV15, SG16, ZCWS15, CAM19]. Identities [KH11, LBC18, GLM+11]. Identity [AHN+18, AQD12, ASM12, ASVE13, Ano15b, ACAT+15, ASS15, BWLA16, BCF16, BHG12, BPKW12, BDFK12, Ber12, Ber17, BS13b, Bow11, CA13, CCFM12, CSL+14, CSZ+11, CZLC12a, CZLC12b, CLHC12, CZLC14, CLND19, CGL+12, CGY+13, Ch12, dCCSM+12, Faa19, FHH10b, FZT14, FR15, FSX12b, FSX12c, FSX12a, GPP12, GR19a, Gla11, GY13, GDC16, GJJ15, GJZ17, HZC+12, Hs12, HSM13, HSM14, HXZ15, HYWS11, HYFH18, JGP+18, KKA14, KRB12, Kuz11, LMG+18, LYX+19, LMB12, LSL12a, LKT12, LNJ14, LLC+15, LTZY16, LSLW15, LH11c, LSC12, LBR12, MLO17, HW+19, MFB+13, MJGS12, MJW+18, MR10, ODH12, Par12a, PSS+13, PSJ+13, PWVT12, RDZ+16, RS15, SS10a, SG12, SS10b, SS12a, SAAB10, Sch11, Ser12, SXH+19, SSPC12, SKGY14, SWW+16, SGH15, TKR14, Tia15, TH16, THA+13, TMGP13, TAP19, TFS19, VJH+18, Vle12, VFFHF19, WY10, Wan14].

Identity [WZC19, XXZ12, XLQ09, XQL11, WI11].
XJW+16, YZX+12, YTM+14, Yon11, YHK+10, YKC+11, YFK+12, YCZY12, ZLH+12, ZMW16, ZYZ+19, ZDW+16, ZPXX17, ZYM18, ZY19, ZTSR12, vdWEG18, ATKH+17, Ano13f, BMB510, BOB13, BSBG19, BM12, BBGT12, CTHP13, dCCSB16, DZ14, Dm10, DWZ12, FA14b, GMRT+15, GR19b, GPVcDB102, HPJ+19, HZC+14, HWDL16, HZWW17, HLR11, HFCR13, HBO10, HBO12, HL11, HPY10, Hwa11, JCL+18, JZS+10, KKKG10, KKM+13, KL11, LKKL13, LI12, LXMW12, LCT+14, MMS+17a, MD15, MGP10, MJS13, MML16, MM13, NCL13, NML19, OSH11, PZL+19, PLCS11, QYWX16, RG10, Rom12, SSY12, SE14, SE16, SR10, hSZZ15, SA16b, Sim15b, SSAF11, SSS11, SG16, VGL14, WVVZ11, WYXY11, WSC14, WLFX17, WMX+17, Wan18b, WUX19, WHZ+19, Wat14b, WWW17, XW12, XCL13, XHM14, YWL+17, YWJ+19, yYQzWC13, YYS+16, YMSH10, YKC+12, YXA+16, YNX+16, ZMYB17, ZSM13, KAT13.

Identity [LZJX10, PN10, Sar18a, Kat13].

Identity-as-a-Service [VFFHF19].

identity-authentication [NML19].

Identity-Based [ASS15, BWLA16, BHG12, BKPW12, CZLC12a, CZLC12b, CZLC14, CLND19, CGL+12, CGY+13, Chi12, FHH10b, FZT14, FR15, FSX12b, FSX12c, FSX12a, GY13, GJJ15, GJZ17, HZC+12, HSM14, HZX15, LMG+18, LYY+19, LSL12a, LLC+15, LTZY16, LSLW15, LH11c, LSC12, LBR12, MLO17, RDZ+16, SGH15, TKR14, TFS19, Wan14, WZC91, XZC2, XJW+16, YZX+12, YHK+10, YKC+11, YFK+12, YCZY12, ZLH+12, ZMW16, ZYZ+19, ZPXX17, ZYM18, ZY19, CSZ+11, HSM13, HYWS11, HYF18, LKAT12, LJJ14, MJG12, RS15, SXH+19, SWW+16, Tia15, TH16, ZDW+16, BOB13, BMM12, CTHP13, DZ14, FA14b, GMRT+15, HZC+14, HWDL16, HZW17, HLR11, HBO10, HBO12, HL11, HPY10, Hwa11, JCL+18, LI12, LCT+14, MJS13, MM13, NCL13, PZL+19, QYWX16, RG10, SE14, SE16, hSZZ15, SA16b, SSAF11, SGM16, WLFX17, XW12, XCL13, YWL+17, YWJ+19, yYQzWC13, YKC+12, YXA+16, ZZ12, ZYM19, LZJX10, KAT13].

Identity-Enabled [SG12].

Identity-Hidden [PSS+13].

Identity-Preserving [MHW+19].

IdM [ACAT+15].

IDs [SOS15].

IEC [BCM12, BCM13].

IEEE [IEE10, IEE11b, IEE13, IEE15, MSH+16, TBL19, Yan10, Anop16g, BOB13, CL11, FLH13, FZZ+12, NBZP17, ZBR11].

IEEE802.16e [HLCL11].

if [ABJ13, Pec17, Rus15].

IFIP [GLIC10].

IFP [MMZ12].

IIFPTTT [BD18].

IG [Mun17, SCPSN10b, SMOP15, ZWS+18].

IEEE802.15.4a [CMC12].

III [SMOP15].

ILA [HZS+19].

Illegal [ABJ13].

Illinois [Nor17].

Illogical [Hel17].

Illustration [KLY+12].

Illumination [GHS14].

Illustrated [Cop10a].

Im [BGI+10, BGI+12].

IMA [Che11].

IMACC [Che11].

Image [BS11, Bai10, BAAS13, BDB14, BWR12a, CJFH14, CCC19, DA10, DCM18, DS19, GRRZ18, HD19, IAD10, JKHeY12, KPS10, KLK+19, LA15, LLL17a, LFX+18, LLLH18, LZX19, MBC15, MAL10, MSH+18, PW10, QIC+18, RS16, VRSC12, SH11, SM11, ZSY19, SJ12, SG+12, SMS18, SS17b, SSA13, SRA17, SZT18, TB18, VAG19, WHZ12, WXXL12, WXY+13, WYCF14, yWXyZ+18, WYK12, WYL18, YLL+12, YWWN15, Ye10, Ye14, YHX18, ZWX+11, ZWW17, ZWX17a, ZWX17b, ARG19, AM19, BWA13, BM13, Bro19, CT11a, CW14a, EA11, FMB+18, GKK11, HAK19, HLC16, KMG17, KM11, KKK+18b, LXXM11, LW10, LWL11, LW13b, LPZJ15, MO14, MS17, NES+14, PTK14, SE18, Sch12a, SM13, SM12, SNM14, ST15, SGFCRM+18, Sun16, jT12b, TTO10, TLL13, UUN11, UUN13, yWpWyYpN13, WD19, WHZ+19, WZ+12, WSS+19, WK111, WOLS12.
LLHS12, LW13a. Index-Based
[ZZYL16, LLHS12]. indexed [WXLY16].

Indexing [HCDM12]. India
[BC11, CGB+10, GG10, Rom12]. Indicator
[KU12]. Indicators [YT12, Pal16]. Indirect
[ABS+12]. Indistinguishability
[AS16, BCEO19, BCEO20, BV18, FMY15,
GGHR14, GGH+16a]. Indistinguishable
[LG12]. Individual [LMB12].

INDOCRYPT [BC11, GG10]. Induced
[VDB+16]. induction [BBBP13].

Industry [Ano11b, ATD17, QZL+16a, SXH+19,
Cha13c, LHH+18, Men13b, ZSMS18].

Infected [GST12]. Inferring
[Bro11, DBPS12, NC12, RHLK18].

Inferring [LS17, BSA+19, PTRV18].

Influence [RSCX18]. Information
[AQD12, ABCL17, Bai10, Big08, BF11,
CVM14, CDGC12, CGB+10, Rom12,
CST+17, CBL13, Dew11, DP12, FHPK17,
FHS13, FP19, HBC+19, HHH+13, IF16,
JJHHN12, KD19, LG12, LW11a, Low12,
MA17b, MAL10, NTKG17, RZ19, SGC14,
STC11, TWZ11, Uto13, WSS12, XHH+18,
XHZ+19, Yan10, Yek10, ZH15, ZBL19,
ZBF18, AB10a, AB10b, AL15, ASEV13,
BS11, BGP+17, CFG+17, DMWS12,
DGL19, GLM+19, HPJ+19, KL13, KPB18,
LZ11, LWK+18, MKH+12, Mar10b, SRB+12,
TKG+17, WHZ+19, WW13, Ano19a,
BLY10, LH10a]. Information-Centric
[FP19]. Information-Theoretic
[CVM14, WSS12, CDGC12, GLM+19].

Information-theoretical [ZZ15, KL13].

InfraStructs [WW13]. Infrastructure
[GM13a, HEP+11, PN10, VFFFH19,
GAI+18, JAE10, SA12, LG10].

Infrastructures
[JM14, FH16, YWZ+18]. ingenious
[Mac12]. Inhibiting [GS+16]. Initial
[PAS13b]. initialization [PCK19].

initiation [AN15]. Initiative [Sch16a].

Injected [LLZ+12]. Injecting
[BBGT12, LKZ+19]. Injection
[ABS+12, ARP12, DDR+16, JWJ+17,
PYM+13, YGD+17, CBY16]. Injections
[LCLW17]. Ink [Keb15, Mac14]. Inner
[ADM12, LG13, OT12, YKNS12,
DDM17]. Inner-Product [YKNS12].

Innovations [JSM+16]. Input
[GGHW17, XXZ12, Kom18, PBCC14].

Inputs [GGHW17]. InSCRYPT [BYL10].

Insecure [BCGN16, BWS19, Mur16, Lan17].

Insecurity [Bel19, HZ15, LSQ15, LRW17,
LCP15, SWY12, KY10, Wan14].

Insertion [XWDN12]. inside-out [AP11].

Nider [AJA16, ERLM16, LJS+14].

Insights [AH19]. Inspection
[FR+17, VCK+12, AZH11]. Inspired
[RMG18, BW13, GPVcBO12, OK18].

Inspires [SPG+19]. Instability [LMB12].

Installement [SYC+17], instance [BRT12].

Instances [H10]. Instantiating
[CMR17]. Instantiation [LNZW19].

Instantiations [L16]. instead
[AGH+17]. Institute [Wes16]. Instruction
[ARP12, AB15, EKP+13, HZ15, RS17a,
YM18, BVB12, DG18, SF12].

Instruction-Cache [AB15].

Instruction-Level [HZ15]. Instructions
[FHL19, KG19]. Insulated
[FZ13, LDZ16, LH11, HLZ+14,
RG10, RWZ13, WWZ11]. insurance
[GQH17]. INSuRE [SDC+17]. Integer
[Con12b, KTM19, LLY+18, AMK12, MM13,
Mes15, MN14, PC14, SD17].

Integer-factoring [SD17]. Integers
[CN12, CNT12, MH16]. Integral
[AY14b, LWZ12, LJF19, ZSW+12, SM11,
SM14, SH11]. Integrated
[LY15, MU12, AL15, SY12]. Integrating
[CFZ+10, LH12, OdH12, AEH17, HLYS14,
MCL+19]. Integration
[AQE12, Kar12, ZHY+13]. Integrity
[BCP14a, BCK17, DGFH18, FMY15,
MV16a, PZL+19, PH12b, SB18, TSB18,
Intel [Arm19, MZLS18, SF12]. Intellectual [FREP17, Bar19]. Intelligence [Dew11, SG19b, Ald11, Bud16, GW14, Han12, Maf16]. Intellectual [AMK12, IEE11a, SAJL16, VFS+19, Wat14a, HLYS14, MKH+12, SMS+16, ZCZ+19].

Intensify [HL12]. Inter [LBR12, OMPSPL+19, BGAD12, SCKH10, SA15, SHBC19, YWK+10a]. Inter-domain [LBR12, BGAD12, SCKH10, YWK+10a]. Inter-Pulse [OMPSPL+19]. inter-router [SA15]. inter-session [SHBC19].

Interaction [FMA+19, HSUS11, BBDP16, HK17]. Interactive [CJFH14, DF11, FSGW11, BCT+13, LH11a, LK18, LLY16, Pas13a, PPR+12, Yan14].

Interceptor [Cho10]. Intercepts [Don14]. Intercloud [DCA17]. interference [WBA17]. intermittent [VJH+18, CL16].

Internal [LCR+18]. International [ACM10, ACM11, BC11, CGB+10, Che11, Dan12, FBM12, GLIC10, JY14, LCK11, LW11a, LTW11, MV12, PJ12, Sen10, TT18, Wat10, Yan10, Yan11, AB10a, Abe10, Ano11a, BYL10, BL10, Gil10, GG10, HG10, LH10a, IEE11a].

Internet [Ano13f, LFGCGCRP14, TW14, AAC+16, Ano13d, Aks19, Bchl19, Bol18b, BLU+15, CLF+17, CCMB19, CW12b, CEL+19, DRS16, DG15, FREP17, FMA+19, Fri13, Gel13, GMDR19, HKA+18, Ham19, HZL18, HEP+11, JKAU19, JTZ+16, KHRG19, LNK+18b, LW19, LGH+17, LSG16, MJGS12, MJS13, MSL13, MCF17, NLLJ12, NLY15, Orm16, PGLMCD18, SB17, SXH+19, SS19, Söd13, SYv+19, SYW17, SYC+17, SKEG14, WVC19, WCCH18, XLC+19, YCT15, ZDH18, ZSY19].

Internet-Draft [MCF17].

Internet-of-Things [LBW19].

Internetworking [SAAB10].

Interoperability [HWK+15].

Interoperable [LG10]. interplay [JW14].

Interpolation [JTT+16, KU14].

Interpretation [MI17b].

Interpretation-Based [MI17b].

Interpreter [MS18]. intersection [Eng15, LZY+16]. Interval [PPR+12, Cra11, DTZZ12, LWY12, MO14].

Interval-based [PPR+12, Cra11].


Intrinsically [SRK+17, SRK+18].

Introducing [Ano16g, Fay16].

Introduction [AG18, BCL19, BD19, DK02, DK07, DK15, Gas13, G13, Gre19b, HPS08, JSK+17, KL08, KL15, LLK18, Low12, Mei10, Men13a, Sch15a, SOG15, Sta11c, Big08, CM13, Buc10, Led16, Sch15a, Ful10, Mfr10].

Intrusion [NSMS14, SAJL16, SBV14, YKC+12, MMF15]. Intrusion-resilient [YKC+12]. Intrusive [AARJ12, MFB+13].

invariance [yWpNyL11]. Invariant [CSW12, NKWF14, RS16, WYW+13, YWNW15, ZGHD12, GMdFPLC17, LXC11].

Invariants [NKWF14, CDSLY14, KK10, MZ17a, TLL13].

Invention [Orm16]. invents [Ant14].

Inverse [JS18b, RMTA18, RMERM19].

Inversion [ABSSS19, KHH14]. Invert [ZWTM15]. Inverted [ZXYL16]. Invertible [SLY+16, UUN13].

Investigating [SPM13]. Investigations [Bla16, Har14].

Invisibility [BN14]. Invisible [AAA+19, Keb15, Mac14, SYL13].

InvisiMem [AN17]. INVISIOS [AARJ12].

Invited [SS19]. Involution [Brl2].

Involvement [LKBK19]. Invoking [HLCL11, RB17].

IoT [AATM18, AMSPL19, AMKC19, APDCR13, BD1+19, BBTC20, CCM17, CSH+18].
FQZF18, FMC19, GAI+18, HHBS18, Hod19, KV19a, KKK+18b, KKD+18, LSQ15, LZZ+19a, MMP19, NVM+17, OSANAM19, PCK19, RC18, SSA18A, SGC16, SJL18, TODQ18, TG17, Wan18h, WCFW18, WXK+17, XYL19, WYJ+19, YFT18, YTH17, ZCWS15, ZLY+19.

IoT-Based [YTH17, ZLY+19].


Jean-Jacques [Nac12]. Jeffrey [Mei10].


Joshua [Ano17b]. Journey [CFST17, RS19]. Joux [AY12a, Ay12b].


Katz [Ful10, Mon15]. KDM [CBXJ19, MTY11].

Kecck [BDPV12, RS17a, BD+12]. keep [Rus15]. Keeping [CG14b, Man13, Gup15].

KEM [CGZ15]. Kepler [LP19]. kept [Cha13c]. Kerberos [SKH10, TW14].

kernel [GM31b, HHAW19]. kernel-assisted [GM31b]. Key [ASN12, Alz19, ADHS18, Ano11b, ABB19a, BN14, BVS+13, BL12, BSBB19, BBP+16a, BD15, Bar16a, BR19, Ber16a, BM18, BCO13, BKLS12, BF11, BKK10, BB10, BKK10].

CVM14, CT18, CLY14, Che15, CLND19, CWZ19, CJ13, Chi16, CCT+14, CNT12, Cou12b, CMA14, DWWZ12, DL12, EAA+16, EFGT18, FZT13, FHLOJR18, FVS17, FM12, GDLL18, GFDB12, GT12, GZZ+13, GSW+16, GSTD13, GPT14, Giri15, GKS17, GZ12, GLB+18, GYW+19, HSMY12, HLLG18, HEP+11, HC12, HL10a, HWS+19, HCL+14, HTC+15, HEC+12, HLH19, Jia14a, JEA+15, KP12, KNZS19, KTT12, KFOS12, Kim15, KG19, LYX+19, LLSW16, LKBK19, LG10, LCLL15, LDZ16, LQY10, LY16, LH11c, LSQL18b, LCCJ13, LWL17, LYY+18b, LBR12, LH18, MZH15, MVV12, MMP14, MTY11, MMY12, MV19, MKK17, MPRS12, MSN11, MSU13, NNA10, NYR+14, NTY12, Orn16, PS17, PDNH15, PCPK14, Pud12, PNRC17]. Key [RVH+16, RSBGN12, RW12, Saa12a, SNJ11, SEHK12, Sas18, SK12b, Soc18, SWM+10, Sia12, SD18, SGL15, SLY+16, TMC15, TMY+17, TM12, VAG19, WP17, WSS12, WLC12, WZ15, WCL+18, WWHL12, WT10b, WSQ+16, WCXZ17, XNGK15, XXZ12, Xio12, XLM+12, XJWW13, XGLM14, XZLW15, XR+17, YM16, YZX+12, YS12, YLSZ19, YLW13, YRT+16, YL17, Yon12, YKC+11, YFK+12, ZSP+19, ZKH16, ZY17a, AHG18, AAL19, AA14, AQRH+18, ATKH+17, AK+18, ABB+14, AKG13, AIB+16, ABW10, ABR13, AN15, AK14a, AYSZ14, AVAH18, BS15, BGAD12, BB14, BZ16a, BJ16, BSW12, Bon19, BGG+13, BBE+18, BB16b, CFL13, Cha13a, CSD18, CLZ+17, CTL13, CML16, CLCZ10, DLK+16, DGS12, Dur15, DMSD18, EBAQ17, FHIOh10a, FA14b, FIO15, FHZW18, GMRT+15, GPP+16, GLMS18, GMdFPLC17, GH16, GBMN11, GLM+11, GSAV18, GTSS19, HPC12, HZW17, Hod19, HWB10]. Key [HWB12, HL11, HYL+19, HLYS14, HT1C7, IM14, ISC+16, IB11, IOV+18, JSK+16, JLT+12, Jia14b, JSMG18a, KDH15, KMTG12, KKG14, KV19b, KIH19, KP18, KLV+16, KDW+17, LLLS13, LLP+18, LLY06, LZ11, LHM+10, LYW+10, LWS10, LDZ+14, LIK+17, LPd10, LW13b, LZC14, LM14, LML+13, LLG19, MN12, MHL18, MRT10, NAACL12, NCL13, Nos11, Nos14, ODK+17, OSANAM19, PY19, RR16, RG10, RWZ13, RPS10, SES+16, SPD+10, Sar14, Sav16, SLZ12, SY15b, SZMK13, hSZZ15, SA15, SLXX16, SCBL16, SGP+17, StV10, TK19, TCS14, TLL12, Tso13, TKHK14, VV19, VN17, WWYZ11, WR10, WMU14, WDV18, WDK19, WZM12a, WZM12b, WT10a, WTT12, WQZ+13, WXK+17, XW12, XW13, XCL13, XXCY19, XY1L19, XLZ+19, XMHD13, XHM14, YTT11b, YC12, Yan14, YZZ+14, YHHS16, YLZ+18, YLYL+18, YN19, YY13, YLZ+16, ZCZQ19, ZPZ+16, ZYGT17, ZYGY18, ZWQ+11, ZZ1, ZHL+11, ZCC15, ZT16, ZGL+18a, ZXW+18]. Key [ZXWA18, ZCL+19, ZG10, ZZZC15, ZZC17, ZY17b, ZWS+18, ZCZ+19, ZHT16, vV16, CLW16, OHJ10, XR+17]. Key-Aggregate [CCT+14, PSM17, GLB+18, CLW16]. Key-Agreement [WSS12, APK+18]. Key-Alternating [BKLS12]. Key-Based [Xio12]. key-correlations [Sar14]. key-delegation [JSMG18a]. key-disclosure [ZZC17]. Key-Extraction [GPT14]. key-hash [KKG14]. Key-Insulated [FZT13, LDZ16, LH11c, HL11, LDZ+14, RG10, RWZ13, WWYZ11]. Key-Length [GT12]. Key-Length-Based [PNRC17]. Key-Policy [GZZ+13, GSW+16, HSMY12, RVH+16]. Keyed [KE19, MMS17b, YHHM18]. Keyed-Function [MMS17b]. KEYing [TW14, BCPV11, ABC+18, GJ19]. Keyless [PDM12, ZXW+18]. keyrings [MBB11]. Keys [ASN11, ABL+18, BF12, Bro17, CC10, HDWH12, LSQX19, MS16, PSM17, TW14, ZMW16, CGM+18, DMM10, HFH16, HL14,
IK15, KV19a, LLY15, LHA+12a, LH13, LW10, LLL+18, RWZ13. keystream [SM11]. Keystroke
[AaBT16, SP13, BGE+18, CTL12, GEAEH11, LTC+15a, MCRB19]. Keyword
[CWL+14, CHe15, HWZP18, HCDM12, HLH19, LSQ18b, WDC18, XSW16, XJWW13, ZXY16, BZ16a, BL11, CLH+16, DYY+19, FSEW12, GZS+18, LXK+14, OSS16, SY15b, WHY+12, WXY16, XWX+18, XTZ+19, XLC+19, YZCT17, YQZ+19]. Keywords
[CWWL12, ZZ11], KGC [YT11a]. Khudra
[CWZ19], Kiasu [LSG+19], Kiasu-BC [LSG+19]. kid [Tan17a]. Kind [WJ19].
King [ABJ13]. kiss
[HU15, KYEV+18, Ros11]. KLEIN
[GNL12]. Klepto [XY18]. knapsack
[ACD18]. Knapsacks [Dun12a]. Knaves
[CEL+19]. Knebl [Mun10]. KNEM
[GM13b]. Knights [CEL+19]. knocking
[KSB+17]. Know [BC14, CAC14, XTK10].
Knowledge [BSCTV17, CLP13a, COP+14, GJO+13, GOS12, IW14, LYY+16, MX13, MBC+18, M1210, OOR+14, Pan14, TSH14, Ano11a, KPP16, LLM+19, MDHM18].
Known [DWWZ12, JHL12, SEHK12].
Known-Key [DWWZ12, SEHK12]. Knuth
[Ten18]. Kobitz [BJ10b, TX16]. Kode
[NN15]. Korea [LH10a, LW11a]. KP
[FJHJ12, HXZH14]. KP-ABE
[FJHJ12, HXZH14]. Kristie [Keb15].
Kryptographie [Bl12]. Kryptographie
[Buc10]. Kuala [HWG10]. Kummer
[HR19]. Kurtois [YYO15]. Kyoto
[TBL19].

L [Low12, Xie12a, Xie12b]. LAAP [Gop19].
Labs [Ven14]. Labyrinth [Fox13]. Lacks
[BDSG+13]. LACO [AMSPL19]. LAKE
[BOC13]. Lanczos [FYD+19].
Lanczos-Based [FYD+19]. Land [Sch18].
Landis [BB16b]. language [Ksi12].
Languages [MX13, Wat12]. LANs [FLH13].

Lapin [HKL+12]. Laptop [GPT14]. Large
[AN12, DM15, FNWL18, JLS12, KHeY12, KCR11, KU12, LLS19, LW16, LQD+16, MC11, SP13, And19, dCCSB+16, DEL19, EEAZ13, FXP12, GSN+16, LFZ+17, LBOX12, SR10, VSB+19, ZZKA17, ZVH14].

Large-Scale [DM15, KHeY12, LLS19, LQD+16, And19, dCCSB+16, DEL19, FXP12, GSN+16, SR10, ZZKA17, ZVH14].

LARK [DS11]. Laser
[DDR+16, FNP+15, Liid12]. Last
[Hof15, Hof16]. Latency
[AYS15, BCG+12b]. Latency-Optimized
[AYS15]. lateral [SCY15]. Latest [Ber17].
Latin [AB10a]. Latincrypt [AB10a].

Lattice [ADM12, Ano11b, AYS15, BSJ15, EM12, EFG18, FGM10, GCH+19, HPO+15, HKR+18, LNW19, LPO+17, MLO17, NDR+19, PG12, AAT16, AVAH18, BH19, Dra16, LLM+19, MGB19].

Lattice-Based [ADM12, Ano11b, AYS15, BSJ15, EM12, EFG18, HPO+15, HKR+18, LNW19, LPO+17, MLO17, NDR+19, PG12, GCH+19, AAT16, LLM+19].

Lattices [Boy13, LYY+18a, LYX+19, Lau17, TH16, XXZ12, ZQ15, Kre13, Tia15, XLW16, yYqWqZC13]. launch [Zet14].

LAUP [BNHH19]. Laurent
[Ano15b, Ver17]. Law
[Bla12, SR14, Wu16, AOT13]. Layer
[HQY+18, LHM+15, PRGBSAC19, ZKH16, HQY+16, LKLD13, ZHH+17]. Layered
[Bel19, BS14, GRL12, WWL+14, JCHS16, Tan18, ZC12]. Layering [YYK+17]. LBlock
[KDH13, MNP12]. LDGM [BBC+13]. Lead
[Arm19]. Leader [ADH19, TKM12]. leads
[Ano14a]. leak [BBG+17]. Leakage
[AV12, Bar16b, BKKV10, CBRS19, CBL13, DCA18, DHB16, FPS12, GDL18, HHH+13, HHP17, HHS18, IL15, Kom18, LTZ16, LSQL19, NTGD17, NTY12, Pan14, SGH15, TTH15, Wan18a, XZY+12, YZLC12, YZ12, YCY12, ZYT13, ZWTM15, ZM16, ZSM17, ZY+19, ZYY19, ZY17a, ZY17b, ZYM18,
ZYH⁺19, ZBPFF18, ABC⁺18, CQX18, DLZ16a, DMWS12, GV14a, GLL⁺18, HYL⁺19, LGL19, SGP⁺17, YLZ⁺16, ZWM14, ZCC15, ZYM19. **Leakage-Free** [IL15, LSQZ17, TTH15]. **Leakage-Resilience** [NTY12]. **Leakage-Resilient** [AV12, FPS12, HHS18, LTZY16, Pan14, XZY⁺12, ZYT13, ZZM17, ZẎZ⁺19, ZY17a, ZYM18, ZYH⁺19, ZY17b, ABC⁺18, CQX18, DLZ16a, GV14a, LGL19, ZYM19]. **leakage-tolerating** [ZWM14]. **Leaking** [BF11]. **Leaks** [CATB19, DLV16, JGP⁺18, Sav13a]. **Leaky** [DLWW11]. **Learned** [KMP⁺11, WL11]. **Learning** [BNMH17, Bar16b, CTC⁺15, CRS⁺18, GN16, HFW⁺19, HXHP17, HGOZ19, KPC⁺11, KRB12, Mor19b, Raz19, RDK19, RHLK18, SPG⁺19, Yon11, ACM1P9, GJ13, GSAMCA18, KMG17, KD19, Sch12a, WS14, BCV12]. **learning-based** [WS14]. **Least** [KTM19]. **Leave** [GA19, CMG⁺18]. **Lecture** [Hel17]. **LED** [IS12, JKP12, MRTV12]. **Ledger** [Mu16]. **Leeds** [vDKS11]. **Left** [BBG⁺17]. **Left-to-right** [BBG⁺17]. **Legacy** [CS12, Smi1b, CGH17]. **Legal** [ZTSR12]. **LeGall** [Ara13]. **Legislation** [PH12b]. **Legitimacy** [IM16]. **Lemonade** [DFKC17]. **Lemons** [DFKC17]. **Length** [AS17, GT12, Gir15, PND15, PRC17, Zha12]. **Length-Doubling** [Zha12]. **Lengths** [BR19]. **lens** [PHN⁺12]. **LEO** [RM18]. **LESPP** [WLZ⁺16]. **Less** [TKR14, GM13a, Kan16]. **Lessons** [KMP⁺11, TGC16, WL11, CMG⁺18]. **Level** [AW17, A015a, BBC19, BNPB13, BKJP12, CCW⁺10, DA10, FGRQ18, Gli12, HZS⁺19, HS18, JWJ⁺17, KPC⁺16, KGP12, MV16a, XZL⁺19, ZLDC15, ABBBD13, CJO16, MEPO12, RS17c, UUN13, VSI1, YT11a, BAI12]. **Leveled** [BGV14]. **leveling** [LY15]. **Levels** [HLCL11, LRW17]. **Leveraging** [DMS⁺16, GMDF19, HCM11, MvO11, SKGY14, ZYGY18]. **Lewis** [Mar10a]. **Lexicographic** [ZÁC17]. **LSF** [HLCC12, MRT10, WGD18]. **LFSRs** [QGGL13]. **Liability** [Bra13]. **Liars** [Sch12b]. **Libertarian** [Eya17]. **Libgcrypt** [DK16b, Bro17, Win17]. **LibRA** [GMVV17]. **Library** [ович16, Bee17, BLS12, FLW12, KRH18]. **Licensing** [EAAAA19]. **Lie** [HWS⁺19]. **Life** [MK13, SCMS18, McK10, McK11, War11]. **Lifecycle** [Tan15a]. **Lifetime** [HSUS11]. **Lifting** [LSL12b]. **Light** [JE1⁺15, SWF⁺19, PCK19, SJ19, ARH⁺18a]. **Light-Weight** [SWF⁺19]. **lightning** [Ran10]. **Lightweight** [ADM19, AMPSL19, AMKA17, AARJ12, BNN19H, Bchl19, BSS⁺13, BFM17, BKL⁺13, BM11, CGCPDMG12, CWP12, CCF17, DS11, ESS12, EKP⁺13, FVB⁺18, FQZF18, GNL12, GA⁺18, Gop19, GMVV17, GMSV14, HZW18, HCT17⁺12, IS12, IOM12, KE19, MO12, MFG16, MPM⁺17, PCDG14, SBS18, She14, YN19, ZWY⁺13, ZSY19, ZLY⁺19, ZSH⁺19, AMN18, AATM18, AMKC19, AKKY17, BLL⁺19, BC16, BB19, Bor10, BBB16b, C11, DA18, FLL⁺14, GH15, GTSS19, KDH15, LLZ⁺16, MCN⁺18, MNP12, MH15, MHY⁺18, OSANAM19, PJ18, PSO⁺13, SGJ⁺18, Tan12b, TG17, WLZ⁺16, WCFW18, WWBC14, WXZ⁺18, XXY19, XHM14, YCT15, ZYY⁺19, ZSW⁺18a]. **Like** [BW16, ERLM16, HP17, WJ19, AHG18, CGCS12, CJZ13, HLH19, KO16, L15, L16, RS14]. **Lilliput** [BFMT16]. **Limitations** [CK17, DR12]. **Limited** [DFKC17, ZZC17]. **Limited-Use** [DFKC17]. **Limits** [AS16, GV14a, KS12]. **Lindell** [Ful10]. **Line** [FFL12, LKBB19, YMW11]. **Linear** [BCT⁺13, BW12, CGCS12, CMS14, EKP⁺13, FGM12, HK14a, LGLL12, L15, L16, LFW⁺16, WGF16, YCL17, BBEPT14, Bull10a, DMS18, FES10, GMGC15, Her10, HCCC11, LWK11, ÖS11, SA14.
XSWC10. Linear/Linear [EKP+13].
Linearly [ADD10, MBP19]. Lines [HR19].
Linguistic [OO18, OO10, OTO18].
linguists [Maf16]. link [Ham12, VS11].
link-state [Ham12]. Linkable [YLA+13].
Linkage [RCBK19]. linked [JCHS16].
linking [GSGM16, NPH+14]. Links [PRGBSAC19]. Linux [Feli13, HHAW19].
Lipreading [O'S12]. LISA [PCK19].
LISISAP [VS11]. List [AEHS15].
Listening [Lan17, MJS13]. Listless [SCY15].
literature [IAA+19]. live [ZZCJ14].
Lizard [MSS+18]. LLL [NV10]. Load [AN12, FXP12, PRN'+19, SG19a]. Loc [CDPLCA16]. Loc/ID [CDPLCA16].
RSX18, SNCK18, VV+19, WPZM16, WK18, CXX+19, CHX13, Har14, JK19, LWYM16, NZL+15, FC14, YXA+18].
Location-Based [JP19, Kim11, CXX+19, CHX13, LWYM16, NZL+15].
Location-dependent [PKA15].
BGJT13, MM13, Mes15, TPL16]. logarithms [BGG+19]. LogCA [AW15, AW17]. Logging [YNR12a, YNR12b]. Logic [Che18, Cil11, DGP10, Hei17, Nie02, RZZ+15, Ter11].
Loop [EFGT18, JS18b, DWZ12]. Loop-Abort [EFGT18]. losing [SLZ12].
Loss [DK16b, JTZ+16, DMV15]. Lossless [DA12, LZC+12b, GJ13, TTT10, WLH13].
Lossy [BKPW12, CCL+19, CW12a, DN12, ASO14, CQX18]. Lost [WBA17]. love [Fag17, FHM+12]. Lovers [Keb15, Mac14].
Low [ABC+17, AWSS17, Bai10, BCO13, BCG+12b, CMLS15, DJL+12, FHS13, FMC19, GST13, GI12, LJK17, LZZ+19a, LBR12, Man13, NVM+17, RM18, RS17c, SAJL16, WT10b, ZJ11, ABO+17, CZ14, CJL16, Chi13a, FQZF18, LGKY10, LKAT12, LEW19, MZH15, NN11, SG19a, ZPZ+16].
low-area [ABO+17]. Low-Bandwidth [GST13, NR11]. Low-Bit-Rate [LJK17].
Low-complexity [DJL+12]. Low-Cost [ABC+17, GI12, LZZ+19a, Man13, NVM+17, LEW19]. Low-Distortion [FHS13].
low-end [Chi13a].
Low-Latency [BCG+12b]. low-level [CJL16].
LR-UESDE [Y12]. LSB [DA10, LHM13, T12a]. LTE [CLM+12, DLK+16, LLS13, QMW17, SG16, TM12].
Luther [ABJ13]. IWE [BV11, XY18]. LWT [TB18]. Lyra2 [ASBdS16]. LZSS [CFY+10].

MATLAB [TRD11]. Matrices [AMVZ12, BNA15, AKG13, FES10]. Matrix [BFMT16, IAD10, KKK+18a, LYY+18b, SK12a, TTD13, Ye10, Cha13b, LLM+19, TK14]. matrix-vector [LLM+19].

Matlab [BK16, BNA15, AKG13, FES10]. Matrix [BFMT16, IAD10, KKK+18a, LYY+18b, SK12a, TTD13, Ye10, Cha13b, LLM+19, TK14]. Matrix [BFMT16, IAD10, KKK+18a, LYY+18b, SK12a, TTD13, Ye10, Cha13b, LLM+19, TK14]. Matrix [BFMT16, IAD10, KKK+18a, LYY+18b, SK12a, TTD13, Ye10, Cha13b, LLM+19, TK14].


Mechanisms [CBO+18, CCC19, GPR+19, JWNS19, JSK+17, SGG18, FHH10a, KSA16, MMZ12, PLGMCdf18]. Media [KBL11, Fri10a, vdWEG18]. Mediated [Fra16, YHK+10]. Medical [BDM+19, KBL11, UUN11, AIA+18a, AM19, AMK12, KCS+18, KSA16, AMK19, KLC+19]. Medicine [MA17b, LWK+18].


Memory [AN17, ABSSS19, ASBdS16, Arm19, AMH+16, BKKV10, DLZ16a, DHLAW10, GKM16, GM13a, GPR+19, Gue16, HT13, HF14b, Int19, KMJ18, LGLK17, LY15, MZLS18, PAF18, RC18, Raz19, SB18, TLCF16, WAK+19, XZL+19, ZHW+19, BBK16, BAB+13, CZ14, CS11, CVG+13, HMAW19, VCK+12, ZWT13, vV16].


Meshes [SGS14]. Meshram [PLPW13]. Message [ABS+12, AEP18, AK14a, DKPW12, HLLC11, Jia17, KHHH14, PSS+13, PPS12b, PA10, RWLL14, BCDN17, BCND19, CJXX19, CMMS17, EAA13, Jia16, LC17, LWK+19, YMM13, YJC18].


Method
[AGW15, Ara13, BBB+16a, CZ19, FLH13, GLLSN12, GMNS15, HXHP17, HHS+15, KTV19, LyWIZ12, LP12, LD13, LBR12, MU12, OWHS12, PS14, PWS+19b, QF19, SAA15, SY15a, SXH+19, SP15a, SZDL14, USH19, WZXL12, WZCC18, WJ19, XNG+14, XNRG15, YYO15, AGLW16, AIA+18a, ARG19, BLL+19, CSS+13, DJ19, Dra16, FVK17, JS18a, JDV16, Khi18, KHHH14, LLC10, LH11a, LT13, LT14b, LPZJ15, Mar12, MO14, PWW10, SI12, WT13, YWT+12, ZYGT17].

Methodology
[CBL13, Uto13, ZZKA17].

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

Metric
[YGFL15, DMWS12].

Metrics
[CVM14, PGLCX17, SSP19, BC18].

Mexico
[AB10a].

Meyer
[Bur11, Joh15].

MIBS
[CWZ19].

Microarchitectural
[MS18].

Microarchitecture
[ZBPF18].

Microcontroller
[GL12].

Microcontrollers
[LPO+17].

Microcosmic
[WWC+11].

Micropayment
[RM19].

microphones
[GSAV18].

Microprocessors
[SK12b].

Microsoft
[Loe15].

Mid-Air
[AUMT16, KTM+18].

Middle
[LJ17, LJ18, LYO+18, LSG+19, LWPK12, LWPF12, LWPK14, vV16].

Middleware
[FGQR18, FGR+17].

Middleware-Based
[FGQR18].

Midway
[Car11].

Might
[Hur16].

Migration
[SHS12].

MIKEY
[TW14].

Military
[KH14b].

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

million
[Sch16a].

Millionaire
[GSADD11].

miTLS
[BFK16].

MitM
[TY16b].

mix
[WGJT10].

mix-networks
[WGJT10].

Mixed
[ST16].

ML
[Ksi12].

mMTC
[CML+18].

MNC
[IM16].

Mo
[RSB+17].

Mobile
[ATC17, BCD+12, CBYJ16, FD11, GPT12, GdM16, HvS12, HFS+19, HLKL15, KP12, KKA15, LH12, LBC18, May15, NRZQ15, PH16, RXS18, Sch15b, SF10, She14, SS15, SAA12b, WPZM16, WT10b, XHH12, XNKG15, XHC+12, YHL16, Yon11, ZLDD12, Aia15, AZ+16, ALL+18, CLP+13b, CTL12, CCW16, CTL13, CRS13, uHAN+18, FHH10a, FA14b, FHZW18, FH+10, GM16a, GH16, HZWW17, HZW18, HL14, IAA+19, IB11, KMN11, KKA14, KKM+13, KKM+14, KKK14, KSB+17, KS19, LH11a, LZD+19, LH13, MHL18, ODK+17, OHYHSB14, Par12b, SSA18, SLL+19, SNS15, hSZ15, SM19b, SCR19b, SAEF11, SKB+17, SHBC19, TOTC16, TKH14, WSC14, WT10a, YHHM18, YNX+16, ZLDD14, ZDW+16, ZC12, ACMP19, MBF+13, SLL10].

mobile-cloud
[KKM+13].

mobiles
[GCSADD11].

Mobility
[CLH13, LNK+18a, CL11, GH16, LH11b, MYYR13, THA+13, YLS12, ZX11].

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

Modality
[SP19].

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

Minimalism
[DKS12].

Minimally
[AARJ12].

Minimization
[AH19].

Minimizing
[BCD+12].

Minimum
[KHPP16, DZ+12].

Mining
[BH15, BJL12, CZ19, DKS+16a, HDWH12, WZCC18, ZW15, Ano11a, ZMYB17].

Minus
[NXB13].

miracles
[MR14c].

Mirror
[Ano10b].

Misbehaving
[TAKS10, ATK11].

Misson
[Ano10a].

Mistakes
[DHB16].

misuse
[EBFK13].

Mitigate
[BKJP12, SS15].

Mitigating
[EPAG16, HRS16, S17].

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

miTLS
[BFK16].

MitM
[TY16b].

mix-networks
[WGJT10].

Mixed
[ST16].

ML
[Ksi12].

mMTC
[CML+18].

MNC
[IM16].

Mo
[RSB+17].

Mobile
[ATC17, BCD+12, CBJY16, FD11, GPT12, GdM16, HvS12, HFS+19, HLKL15, KP12, KKA15, LH12, LBC18, May15, NRZQ15, PH16, RXS18, Sch15b, SF10, She14, SS15, SAA12b, WPZM16, WT10b, XHH12, XNKG15, XHC+12, YHL16, Yon11, ZLDD12, Aia15, AZ+16, ALL+18, CLP+13b, CTL12, CCW16, CTL13, CRS13, uHAN+18, FHH10a, FA14b, FHZW18, FH+10, GM16a, GH16, HZWW17, HZW18, HL14, IAA+19, IB11, KMN11, KKA14, KKM+13, KKM+14, KKK14, KSB+17, KS19, LH11a, LZD+19, LH13, MHL18, ODK+17, OHYHSB14, Par12b, SSA18, SLL+19, SNS15, hSZ15, SM19b, SCR19b, SAEF11, SKB+17, SHBC19, TOTC16, TKH14, WSC14, WT10a, YHHM18, YNX+16, ZLDD14, ZDW+16, ZC12, ACMP19, MBF+13, SLL10].

mobile-cloud
[KKM+13].

mobiles
[GCSADD11].

Mobility
[CLH13, LNK+18a, CL11, GH16, LH11b, MYYR13, THA+13, YLS12, ZX11].

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

Modality
[SP19].

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

Model
ZWQ^+11, ZBR11, ZCLL14, ZTZ16, ZLDD14, ZHH^+17, ZX11, LNK^+18a.
Neural [Csh^+18, RSX18, SKS^+18, YZLC12, EEAZ13, HZW19, HW19, KM17G].
Neuroscience [BSR^+14, JW14].
Neutrality [Kha10]. Neutrality-Based
[And13]. News [And19, Edw14, Edw17, Lam13, Sav13a, Sav15, Sav16]. Next
[HEP^+11, MR14a, MJGS12, Aia15, ACD^+15]. Next-Generation [MR14a]. NFC
[LY14, Mic16]. NFSR [WGD18].
Niederreiter [HC17, MVVR12].
Nievergelt [Ter11]. Nine [Mac12, LYHH14].
NIST [MMKP16, ZSH^+19]. NIZK [Pas13a].
NIZKCTF [MBC^+18]. NIZKS [CKLM13].
NLM [OPS14]. NN [ZZC17, ZHT16]. No
[WDDW12, Wu16, KHHH14, MPJ^+16].
nobody [Sto12]. Node
[AA19, ARWK19, NYR^+14, OKG^+12, GM13b, LC17, PX13, SAAB10].
Node-Capture [NYR^+14]. Nodes
[VGA15, ZYL^+10]. Noise
[ASN11, Fyo19, LKB19, YMA17, BCND19, QLZ19, ZHH^+17]. Noised [JLS12]. Noisy
[ASN12, HZW^+14].
Non [AH19, AS17, AMH^+16, BBC19, BCI^+13, CG14a, CPS16, DJL^+12, DPW18, EKP^+13, FHKP17, FMNV14, GL19, GZX19, HWS^+19, HKB14, JSA17, KTT12, LC18, LLG15, MFH13, MSas12, OOR^+14, Pas13a, QJC^+18, RM18, RMG18, Svo14, SM18, WgMW12, XZL^+19, YNQ15, YKGL12, ZLDD12, AY14a, AM19, BS15, CS11, ESR14, GIJ^+12, Krf13, Lan11, LJY16, LP11, MSas13, SES^+16, SXL16, VBC^+15, XSWC10, Yan14, Kh18]. Non- [AH19].
Non-abelian [HWS^+19]. non-adjacent
[Kre13, Kh18]. non-associative [BS15].
Non-Black-Box [CPS16]. Non-blind
[HKB14, RMG18]. Non-Boolean [AS17].
non-browser [GIJ^+12]. non-compliant
[ Lan11]. Non-contextual [Svo14].
Non-Coprime [GL19].
non-cryptographic [AY14a, ESR14].
non-dynamic [SES^+16]. Non-interactive
[BCI^+13, LC18, Pas13a, LJY16, Yan14].
Non-interference [BBCL19].
Non-intrusive [MFH13]. non-iterative
[SXL16]. Non-Linear [EKP^+13, XSWC10].
Non-Linear/Linear [EKP^+13].
Non-malleability [KTT12].
Non-Malleable [DPW18, MSas12, CG14a, FMNV14, OOR^+14, Pas13a, LP11, MSas13].
non-medical [AM19]. Non-monopolizable
[DJL^+12]. Non-perfect [FHKP17].
Non-Repudiation [LLG15, VBC^+15].
Non-stationary [ZLDD12]. Non-tamper
[WgMW12]. Non-transferable [GZX19].
Non-uniform [QJC^+18]. Non-uniformly
[YKGL12]. Non-Volatile [AMH^+16, JSA17, RM18, SM18, XZL^+19, YNQ15, CS11].
Nonce [BZD^+16b, KMS19, BH19].
Nonce-Based [KMS19].
Nonce-disrespecting [BZD^+16b].
NonInteractive
[KOS16, GOS12, MBG^+18]. Nonlinear
[CCM^+15, KW14, LW13a, Li12].
Nonlinearity [MM17b]. Nonlinearly
[Fyo19]. Nonvolatile [ZH19]. Norm
[FHS13]. Normal [RERM19, TY16].
Normalization [KLY^+12, SJ12].
Normalized [YGFL15]. Normal
[Low12]. Note
[HYS11, Gal13, GR19b, Hwa11, Lim11].
nothing [Cer15]. Notifications [LBC18].
Notions [KFOS12, SNJ11, Sar12, BP11].
Novel
[CLHC12, DC18, KRDK13, LYY^+18a, LXY^+19, LLG15, LyWIZZ12, LH11c, MJGS12, MCS^+15, SSKL16, SWM^+10, SC12, VN16, WHZ12, WZXL12, YZX^+12, YLSZ19, Ye14, ZMZ17, BOB13, BSBG19, BB19, CH19, DDFR13, GPLZ13, HZW19, HCC111, JXLZ15, LXC11, LMJC11, LH13, LWW^+10, LML^+13, MRT10, NZL^+15, 


PZBF18, SAM+19b, SCR19b, SYW17, Sun16, TG17, jT12b, WYL13, WMXZ19, WGZ+12, YWT+12, ZYG17, ZBR11.


NTRUSign [Wan10]. NTT [MCDB12]. NTT-Based [MCDB12]. Nuclear [Hel17].

Number [ADI11, BKLS12, CDK+10, DSLB18, DFE+19, Fok12, Ham17, KA18, LTKP16, LCLW17, MFG16, NIS12, NNAM10, Sha10, Shp03, SMA10, Shp10, YWT+12, ZYGT17, ZBR11].

Numbering [MNS11]. Numbers [BCGH11, CK18, FM15, MC19, Shp10, AZH11, Ana14, GCH15, SMD11, SAM+19b, ZOC10].


O [CDD13]. Obfuscated [LMS16, OWHS12, ZM16]. Obfuscating [BGI+10, BGI+12]. Obfuscation [ABCL17, AS16, AWS17, BBC+14, BCKP17, BV18, BCP14b, BR14, C15b, DR16, EMW14, FKOV15, GGHR14, GGH+16a, GGH15, MI14, ZL19, BBGT12, CFVP16, GGH+16b, OSSK16]. Obfuscation-Based [ABCL17].

Obfuscator [FDY+19]. Obfuscators [PSD15]. Obfuscated [AWSS17]. Object [BCK17, SSSA18]. Objects [LLY+18, ZCWS15, Bel18b, HST14, SMBA10, WW13].

Oblivious [DN12, WCL+18, GGH14, GLM+19, RYF+13]. Obscure [GLM+19].


Occasion [Nac12, RNQ16]. Ocean [FG19]. October [CGB+10, IEE10, IEE11b].


officers [Maf16]. Official [Kip15]. Offline [Ano15a, GAS+16, JMG+16, LJW+17, LKat12, RSM15, XTZ+19, ZZC17].

Offline/online [LJW+17]. Offloading [JHCC14]. Offs [ASdS16, BS14, GPR+19, SR10]. offsets [YQH12]. Okamoto [TFS19]. Old [Che17, FREP17, GY13].

On-Chip [LGLK17, BAB+13]. On-cloud [EAAAA19].

On-demand [KKJ+16]. On-Line [FFL12]. On-siteDriverID [SGGCR+16].

On-the-fly [PS14]. One [BHT18, CBX19, CMR17, CPS16, DMMM14, DCM12, FD11, HP14, HG12, Mat14, NAI0a, Par18, PC16, TYM+17, WCXZ17, WX12, XYXY11, XZW15, Yon12, BM15, FHH10a, GPLZ13, HRV10, JK19, Kom18, LP11, LW10, LW13b, LML+13, Nor17, RK11, Rs15, SM10a, SPK17, SCBL16, TCS14, ZQW10].

One-Dimensional [XYXX11].

One-Round [TYM+17, XZW15, Yon12, WX12, JK19, TCS14]. One-Sided [HP14].

One-Time [N10a, DCM12, Par18, BM15, FHH10a, GPLZ13, LW10, LW13b, LML+13, SPK17].

One-Time-Password [FD11]. One-Way [BHT18, CBX19, CPS16, DMMM14, Mat14, WCXZ17, HRV10, Kom18, LP11, RK11, SCBL16]. Onion [KZG10]. Online [KZG10].

Online [KZG10]. One-Way [BPS17, HL19, JMG+16, KSD+17, PSM17, SKY14, SZT18, WXY+17, WCH19, ZHL15, AQRH+18, CCG10, DJ19, HYF18, KVvE18, LKat12, LJW+17, Mar12, MS+18b, SSK+18, SYW17, XTZ+19].

Online/Offline [JMG+16, LKat12, XTZ+19]. Only [BB10, YNR12b, YLW13, Bul10a, KMTG12].
KA17, Sar11]. Open [SS19, ABF+14, MHV15, Pow14, Win17, ZWQ+11].
open-source [ABF+14, Pow14]. OpenCL [ABDP15]. Opening
[GDCC16, LZC12a, LLH18, LZC14].
Openings [SP13]. openness [Bia12].
OpenPGP [MBB11]. OpenStack
[CSL+14]. Operable [BCF16]. Operand [MSI18].
Operating [KMP+11, CDA14, MNNW15]. Operation
[GLLSN12, JB11, SBS18, ALL+18, Fay16, Lin14a, SKK10, WGW+12]. Operational
[CRE+12, CM11, RZ19]. Operations
[Cih11, SEY14, SZHY19, YWW10, KJJ+16, LZY+16]. operative [HFCR13].
Opportunist [AA19]. Opportunities
[Lau17, Mc10b]. opportunity [Sch11].
Optical [PRGBSAC19]. Optimal
[AS17, CK17, DSSDW14, DSSDW17, GJJ18, GM16b, HRB13, PDN15, PPS12b, QJC+18, TX16, WMU14, Cha13a, CXWT19, DDD14, MCL+19, PPTT15, SYV19].
Optimality [MM17a, SDM+12]. Optimally
[DSMM14, CT12]. Optimally-Fair
[DSMM14]. Optimised [CMO+16].
Optimising [EVP10]. Optimistic
[WSA15, SEXY18]. Optimization
[AEP18, KD19, WH17, ZAC17, FLZ+12, GCSAbdd11, KHF10, PTK14, RFV+13, ZSMS18, scCR19b]. Optimizations [ZAG19].
Optimized
[ARH+18a, AYS15, EKB+16, GAB19, HGT15, LNL+19, MBF+13, MBR15, JS18a].
Optimizing [DWZ18, ZSMS18]. Optimum
[Oba11, YFF12]. Optional [PC16].
OR-Proof [FSX12c]. Oracle
[CBJX19, GLM+16, HKT11]. Oracles
[FZT14, FSX12a, GSW+16, XLQ09, XQL11, YS12, YKC+11, YLA+13, ZYM18, LLY15, RG10, SLY13, WWY11, YFK+12].
ORAM [RM18]. Order
[DC18, FYD+19, KSI12, LFX+18, LWKP12, PRC12, YKHL12, ZDL12, ZSW+12, ZBPFC18, AKY13, BKR19, LW13a, LCY+16, LWK14, gwpNyY+14, YL11].
Order-Hiding [DCA18].
Order-Preserving [KS12, YKHL12, YL11].
order-revealing [BKR19]. ordered
[AAL19]. organisational [Smi15a].
Organization [RSGG15]. Orientated
[TJZF12]. Oriented
[NNAM10, Rog16, RSGG15, WW12, NML19, SK18, WZM12a, WZM12b].
Origins [SJZG19]. Orthogonal
[FYD+19, tWmC12, XNP+18]. Oscillator
[YKBS10]. OSN [BCF16, BBDP16]. OSNs
[SZZT18, PZPS15]. other [BDK16, Smi15b].
OTS [Hül13]. outliers [Sch12b]. Outline
[Hur16]. Output [DK16b, GST12, NIS15, NR12, Uto13, PBC14]. Outputs
[SNCK18]. Outright [ABJ13]. outreach
[XTZ+19]. Outsourceable [QZZ18].
Outsourced [FRS+16, LLC+15, LHL+18, LQD+16, PD14, RDZ+16, XLP+18, YMA17, YMC+17, DFJ+10, FS18, HKA19, HMCK12, LCL+15, LC16, LWJ+17, QZD16, YSOM19, ZML17, ZSW+18b]. Outsourcing
[DR12, LJLC12, LHL+18, LSL19, LJWY18, OSNZ19, LW+19, SKB+17, SWW+16, XMY+17]. outwitted [Car11, Fag17].
Over-the-Air [VOGB18, ZXW+18].
Overcoming [BKKV10, DY13]. Overhead
[AWSS17, Bai10, CCW+10, GHS12, RM18, ZJ11, CXWT19, RS17c].
Overheads
[TSB18]. Overlay [CHS15, MJS13].
Oversight [Bla16]. overview
[AA14, BDP+12]. own
[Kum10, NA14, Zha15a]. owner [ZZC17].
owners [GZS+18, YQZ+19]. Ownership
[AMSPL19, FMTR12, RR11, HWYW14, KH18]. Oxford [Che11, Wes16]. Ozarow
[ADG16].
P [GT19, ZSH+19]. P-256 [ZSH+19]. P2P
dCCSM+12]. P3 [HK18]. PACE [HKK19].
Package [DB16]. Packet
[FGR+17, FGRQ18, JTZ+16, VPK17, XHC+12, AASSAA18, MV16b, PJ18, PX13,
Packet-Level [FGRQ18].

Packet [Bis17]. Pads [NA10a, BM15].

paGAN [NSX+18]. Paging [TSB18].

Paillier [Gal13, SZHY19]. Paillier-based [Gal13]. Pair [Lin15, SLXX16]. Pairing [Bon12, CMRH17, CWWL12, CST+17, KZG10, KHPP16, LKBK19, LSQ18a, LGPRH14, Men13a, MST18, WZCH19, YTS12, YY17b, ZM18, BP18, Con12, FK19, KSH18a, KSH18b, LL16a, LR15, MSGCDPS18, YT11b, ZY17b].

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

Pairing-Free [LSQ18a, WZCH19, YY17b, ZM18, LL16a, YT11b].

Pairings [ASS15, Hof15, IL15, LT14a, HWB10, HWB12, QYWX16, RS15, UK18].

Pairwise [DL12, YM16].

Palm [Kat13].

Palmprint [IEE11b].

Palmprint [LZ11, QLZ19, SC19b].

Pan-European [GOPB12]. Panacea [Hor19].

Paper [TSH17, Ano16i, SK14, YFK+12]. Papers [Ano16b, Ano16c, Ano16j, CWZL13, LW13a, XW13, DDS12, Dan12, MV12, BYL10, JY14, LH10a, vDSK11].

Paradigm [ABGR13, BSV12, Mau12, MP12, TAP19, Gop19, KKKM11, WQZ+13].

Parallel [AAH+19, App14, ARM15b, BBM15, BTK15, CGB+10, GP17, HW19, LY16, LB13, MCD12, MC11, NdMMW16, NR15, SMD11, YE12, ZGL+18b, CSTR16, FLYL16a, FLYL16b, MRT10, RG10, RWZ13, WWYZ11].

Parsing [MHW+19].

Part [BLM18, VM14, BD15, Bar16a, BCBL19].

Partial [CBJX19, DLV16, GFBF12, HFW+19, LG12, SG14, TK19, WDDW12, Xax14, EBAÇ+17].

Partial-Shape [HFW+19].

Partially [KB10, XZP+19].

Partition [Abb12].

Partitioned [YCR16, Kup13].

Partitioning [FVS17].

Partitioning-based [SHC+16]. partitions [CFG+17].

Party [ABL+18, Ash14, BBKL19, HL10b, HP14, JR13, KOS16, KMO14, NSMS14, OSH16, QZL+16b, TMY+17, ZM16, DGL19, ED19, FIO15, GVW12, HPC12, HWB10, HWB12, LyWS10, LML+13, OSANAM19, Tso13, TTKH14, XLWZ16, XCL13, YC12, YZZ+14, ZZC15, GHKL11].

Pascal [LGP19].

Passau [GLC10].

PASSERINE [Saa12a].

Passion [Hof15].

Passive [DHB16, GSC17, HQLY18, SB17, BM13, uHAN18, LKLW11, MK12a].

Passport [HKK19, LZJX10].

Passports [LG10].

Password [ASBD16, BRT12, CLY14, CJW+19, DM15, DGMT19, FVS17, FD11, GAS+16, HMK19, HCL+14, LDD19, Lop15a, Lop15b, RS11, SD12, Shi11, WgMW12, YLW13, YRT+16, ZXH16, ABK13, AIK18, BKD16, CTL12, DSCS12, Eng15, FA14a, FIO15, FHV16, GPLZ13, HCC10, IOV+18, KMTG12, LWS10, LNLK13, LZ19b, MM12, MVL11, MZL+19, MCRB19, Par18, SVY19, Tso13, TTKK14, WZM12a, WZM12b, YC12, ZXWA18].

Password-Authenticated [HCL+14, YRT+16, ZXH16, LWS10, WZM12a, WZM12b].

Password-Based [BRT12, CLY14, FVS17, WgMW12, DGMT19, DSCS12, FA14a, FIO15, IOV+18, TTKK14].

Password-Only [YLW13, KMTG12].

Passwords [BHvOS15, LCL17b, BCV12, Che13, GPLZ13].

Past
[Bon12]. **Patching** [BCFK15]. **Patchwork** [NXH+17, XNG+14]. **Patchwork-Based** [NXH+17, XNG+14]. **Path** [DSM+16, GHS14, NLLJ12, ZW15, Ham12, RYF+13]. **Patient** [ZLDC15, ZVG16]. **Patient-Centric** [ZVG16]. **Patient-Centric** [ZLDC15, ZVG16]. **Patient-Centric** [ZVG16]. **Patient-Centric** [ZLDC15, ZVG16]. **Patient-Centric** [ZVG16]. **Patient-Centric** [ZLDC15, ZVG16]. **Patient-Centric** [ZVG16]. **Patient-Centric** [ZLDC15, ZVG16]. **Payload** [CHHW12, AZH11, JNUH17, JKAU19]. **payload-based** [JNUH17, JKAU19]. **Payment** [DG15, SYC+17, CHH+13, SYW17]. **Payments** [RBHP15, MPJ+16]. **PC** [YE12]. **PC-Based** [YE12]. **PCIE** [IBM13b]. **PCM** [LY15]. **PCM-based** [LY15]. **PCPs** [MX13]. **PCs** [GPT14, GPP+16]. **PDF** [Con17]. **PDGC** [CGB+10]. **PEA** [ZGL+18b]. **Peaks** [TC10]. **pearl** [Rus15]. **Pecherskii** [Kuz11]. **PEDCKS** [XLC+19]. **peer** [LLY06, NCCG13, ZWY+13]. **peer-to-peer** [NCCG13, ZWY+13]. **PEKS** [ZQD16]. **People** [Sod13]. **Per-File** [EMS+16]. **Per-session** [DMG19]. **Perceived** [CSW12]. **perception** [GMMJ11]. **Perceptual** [DCM18, MK11]. **PEREA** [AK11]. **Perfect** [PAS13a, Sch13, CZ15a, FHKP17, LLC10, Lew10, WX12]. **perfectly** [ADG16]. **Performance** [Alo12, AW15, AW17, AB15, ABPP16, BM18, CRS+18, CGL+12, CCG10, DHT+19, DLK+16, DGFH18, DBPS12, EGG+12, ESR14, FPBG14, GLG12, GPR+19, GCS+13, HKL+14, KHRG19, KAK18, LCK11, LGP19, LPO+17, MH12, SKV12, SSP19, TPKT12, WRP70, WDDW12, Xio12, YWF18, ZLDD12, vRSHP17, ABDP15, AHG18, BGE+18, CLB19, FHLD19, FLYL16a, GCVR17, HURU11, JLC18, MCL+19, MMS+17a, MS13c, PABC+19, ZLDD14]. **performances** [CBL10]. **Performed** [ANO17d]. **Perils** [FMA+19]. **perimeter** [Cal13]. **periodic** [KPS10]. **periodical** [CWSL12]. **Permission** [V16]. **Permutation** [LJ16, NIS15, Bar19, GMSW14, LK14]. **Permutation-Based** [NIS15, LK14]. **Permutations** [ARH+18b, ARH+18a, BKLS12, Faa19, Mat14]. **Persistent** [CSYY18, SXH+19, TYK+12, ALL+18, KV19b, PAK15]. **person** [PN10]. **person-centric** [PN10]. **Person** [ESS15, LYZ+13, Rao17, RSD19, ALL+18, BC18, MvO11, SYV19, WHZ+19, LHL15]. **Personalized** [FRS+16, VGA19, AT10]. **Personnel** [YTH17]. **Perspective** [ADH19, KMY18, MSM18a, RSGG15, Sir16, Wag16, Bon19, JWR14, Suc12, ZWT13]. **Perspectives** [PMG+19b, Sen17, SP+13]. **Perturbation** [XZZ18]. **Pervasive** [ACAT+15, BCG+12h, FHM+10, YD17, JSM+18, PAK15, SCY15, Tan12b, YWK+10a]. **Petri** [PS14]. **PGP** [RAZS15]. **Pharmaceutical** [YSF+18]. **Phase** [KMIJ18, LD13, NBP17, ZWT13, ZHH+17]. **Phase-change** [ZWT13]. **Phase-Encrypted** [NBZP17]. **philosophy** [Mat19]. **phishing** [HAK19]. **Phone** [MUR16, SAA12b, KRM+11, LTC+15a]. **photo** [CLY18, OF12]. **photo-to-caricature** [CLY18]. **Photographic** [YSC+15]. **Photographs** [TCMLN19]. **Photorealistic** [MHW+19]. **photos** [Pow14]. **Phrases** [WBC+10]. **Physical** [BEB+18, CK17, GPT14, GPP+16, HQY+18, HHH+13, PRGSA19, SMOP15, GH19, HQY+16, HZW18, KSB16, QMC17, VCK+12, WW13, YD17, ZHH+17]. **Physical-Layer** [HQY+18, HQY+16, ZHH+17]. **physicist** [Dya19]. **physio** [HT11]. **physio-behavioral** [HT11]. **Pi** [MR10, EHKSS19]. **Pi-Calculus** [MR10].
BLV17, BS13b, BJL12, CVM14, CWL+14, CDF10, DCA19, DTE17, ESS15, EKOS19, FGR+17, Fei19, Fri13, GZZ+13, HSMY12, HBC13, HXHP17, HXC+11, HK18, IE15, JN12, JLX+19, JP19, KM10b, KKK+18a, KLK+19, KCC17, Kni17, KS12, KH18, LGMC17, LSBN14, LLG15, LCDP15, LNXYY15, LSY+16, LQD+16, MYYR13, MJS+19, MV18, Mor19b, MTM18, NSMS14, PD14, PSS+13, PPR12, PZP15, PSD15, Pet12, PH16, RVH+16, RSR+19, RCP+18, RWWL14, Roh19, RHKL18, RBHP15, SS17a, SG12, SET16, SZDL14, SZTZ18, SOF12, TMLS12, TMGP13, VKK+19, VFFHF19, WPZM16, WMC17, WZCC18, WMYR16, YJSL18, YYY+17, YMM13, You11, YY17a, ZHW+16, ZM16, ZOSZ17, ZXL19, ZHW15, ZLDC15, ZHL15, ZTL15, vdG17, ARL13, AMPC13, AIA+18b, ACK+10, BGE+18.

privacy [BC16, BBDP16, BP11, BAG12, CD16a, CXX+19, CCMB19, CDF+10, DZC16, DZT+12, FH13, FMA+18, FZZ+12, GAI+18, HSH11, HKA19, HRK+19, HPL+19, IC17, IOV+18, JKL+16, JLC18, Kam16, KGK10, KM14, LYY+10, LWYM16, LHL+18, LZD+19, LSQ15, MZA+13, MGP10, MGB19, NJB19, OSP+19, PX13, PZBF18, QLZ19, RRR16, Sav16, Sch11, SSNS15, SLZ21, SYY+17, SCY15, SWW+17, SMS+16, Tan12b, WLZ+16, WZC16, Wan18b, WWW17, WS13, YYS+16, YXA+18, YYY+19, YQL17, YNX+16, ZWY+13, ZDHZ18, ZZY+19].

Privacy-protecting [Roh19, CD16a].

Privacy-supporting [ABR13].

Privacy-Aware [BCF16, ARL13, MGP10, ZDHZ18].

Privacy-Based [BS13b].

Privacy-Enhanced [DTE17, ACK+10, YQL17].

Privacy-Friendly [KCC17, ACM12].

Privacy-Preservation [LLG15].

privacy-preserved [SWW+17].

Privacy-Preserving [ABCL17, BJL16, BJL12, CWL+14, EKOS19, GZZ+13, HSMY12, KKK+18a, LMGC17, LNXYY15, LSY+16, LQD+16, MJS+19, Mor19b, MTM18, NSMS14, PD14, PPR12, Pet12, RVH+16, RSR+19, RHKL18, RBHP15, SZDL14, SZTZ18, VFFHF19, WPZM16, WZCC18, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, ALL+18, JX+19, KH18, LCDP15, WMC17, ZOSZ17, AMPC13, BC16, BBDP16, BLV17, CCMC19, DZC16, FMA+18, GAI+18, HSH11, HKA19, JLC18, LHL+18, LZD+19, LSQ15, MGB19, PZBF18, QLZ19, RR16, SYY+17, SMS+16, Tan12b, WZC16, Wan18b, YYY+19, ZWY+13].

Privacy-Preserving [ABCL17, BJL16, BJL12, CWL+14, EKOS19, GZZ+13, HSMY12, KKK+18a, LMGC17, LNXYY15, LSY+16, LQD+16, MJS+19, Mor19b, MTM18, NSMS14, PD14, PPR12, Pet12, RVH+16, RSR+19, RHKL18, RBHP15, SZDL14, SZTZ18, VFFHF19, WPZM16, WZCC18, ZHW+16, ZM16, ZHW15, ZLDC15, ZTL15, AKM+11, AKKY17, ALL+18, JX+19, KH18, LCDP15, WMC17, ZOSZ17, AMPC13, BC16, BBDP16, BLV17, CCMC19, DZC16, FMA+18, GAI+18, HSH11, HKA19, JLC18, LHL+18, LZD+19, LSQ15, MGB19, PZBF18, QLZ19, RR16, SYY+17, SMS+16, Tan12b, WZC16, Wan18b, YYY+19, ZWY+13].
process [CWZL13]. Processing [JG+18, SAKM16, SZHY19, TKMZ13, VKPI17, BKV13, HWK+15, MS13b, PRZB12, WS14].

Processor [BH15, CLF+17, HKL+14, LB13, MBR+15, RJV+18, Y16, YS15, ABDP15, BAB+13, BGG+13, KSH18b, SSPL+13, Tar10, KSH18a]. Processors [GFBF12, Gue16, SJL18, RYF+13, BV13, HWK+13, SAKM16, SZHY19, TKMZ13, VKPI17, LNZ12, BBD19, BGK12, BCGK12, BGB12, BCI+13, BDSG+13, CLZC12b, DKL+19, IW14, LN+12, Mau12, NTY12, RB17, Sav13b, WPZM16, AGHP14, KPP16, KKK+16, Li10].


Protect [CTC+15, CKHP19, YMC+17, BVIB12, CDF+10, dCCSM+12]. Protected [BGH15, SG15, ABG19]. Protecting [BCP14a, GSFT12, LLY19, Mar10b, RCP+18, Roh19, SCY15, Wat14b, ATK+17, CD16a, CXX+19, CDA14, FLYL16b].

Protection [AIM+19, BHC19, CDD13, DCA19, EAAA19, GST12, GPR+19, HXHP17, JP19, Lop12, NGAuH16, NDG+17, RR11, SEY14, SJ12, ZWW17, AIA+18b, ATI+10, HLYS14, HPL+19, KKM+13, Ksh12, LZ11, LWYM16, LVRY10, RS17c, TTL13, YWT+12, ZZY+19].

Protect-key [HLS14]. Protocol [ADSH18, BL12, BC14, BCM+15, BNN19, BSSV12, BFK16, BBKL19, CC14, CCM17, DCA19, FLH13, FHLOJR18, FMRTR12, Fra16, GI12, Hs12, HC12, HL10a, HCP12B12, HCET12, HKL+12, JIA+16, JHY19, KMS19, KMO14, LN13, LDDC13, LNX15, LYY+16, MBC15, MR10, PSS+13, SBS+12, SGC16, SS15, TCW+18, TYK+12, WT10b, XJ+17, YS12, YWF18, YLS19, YY+12, ZZ+11, ZYY19, AAT18, AMK19, AQ18, AKG13, AIB+16, AIK18, AN15, BDM18, BGAD12, CSD18, CWS11, CCMB19, CJ15, DLK+16, DDL15, EA12, EBA17, FA14b, FIO15, GMSW14, GH15, Gop19, GLM+11, HPC12, HWB12, HL14, IC17, IOV+18, JK19, JKL+16, JXL15, Kim11, KO16, LALL13, LDDM12, LKKL13, IWS10, LXMW12, LZ1+19, LW19, LY14, LML+13, NCL13, NLY12, NML19, OHJ10, Par12b, SSA18, SPLHCB14, SB17, SGJ+18, SWW+16, SSS11, SSPL+13, TG17, TIA+13, Tso13].

protocol [TKHK14, VS11, WM17, WYZ+17, Wan18b, WCFW18, WDZ19, WDV18, WZM12a, WZM12b, WLS14, WMYR16, WT10a, WTT12, WCCH18,
XCL13, XHM14, YC12, YZZ+14, YYYK+19, YMM13, YN19, ZWQ+11, ZT26, ZYC+17, ZWX+18, ZXWA18, ZG10, ZZZC15, ZXX11, BOB13, CJP12, LFGCGCRP14, Ste15b).

Protocols [ADH19, AP13, ABHC+16, BMP12, BSBB19, CCK12, CCCK16, CMRH17, CCF7, CZCD18, CCD15, CCD19, CCD20, Con10, CM11, EFTGT18, Fra15, GRL12, GM11, GLR10, HLLC11, HL10b, KL08, KOS16, LY16, LWL+17, MV19, MS16, MT12, Mur16, NYR+14, NSMS14, PS14, RB17, SBS+12, SBS18, Sch12c, SOF12, TM12, Xio12, YRT+16, Aia15, Ano13d, AKS19, ACC+13, ACM12, BJ10a, BK19, CML+18, CR10, CLCZ10, DGNJ14, FTV+10, GBNN11, GLR13, HSH11, HLS18, Ham12, HDP13, HZW17, HST14, HW10, KJN+16, KSU13, Ks12, KKK+16, LDC13, LLY06, LKKL13, MN10, NR11, Nos11, Nos14, SD10, WMU14, YSL+10].

Prototype [Bar16b]. Prototyping [KPC+16]. Provably [BKLS12, CC14, EKB+16, Rog16, YJSL18, YMSH10, YYW19, Z11, ZPPX17, FA14a, HRS13, LHH11, SYWX19, WB12, XCL13].


PSPACE [JJUW10]. PTAS [JLX+19]. Public [Alz19, Ano11b, ABW10, BVS+13, BB14, BM18, BKL12, BKV10, CT18, CLP13a, Che15, CLND19, CNT12, Cou12b, EKOS19, FBM12, GKS17, HEP+11, HWS+19, HCT+15, HLI19, IM14, JLT+12, JNVS19, KFOS12, LXY+19, LLSW16, LG10, LHA+12a, LPS10, LSQ18b, LZC14, LCPD15, LLH18, MZHY15, MPM14, MTY11, Mat14, MPRS12, Muf16, NTV12, Oerm16, PDNH15, RSBGN12, RVS+18, RW12, RBHP15, SGG18, Saa12a, Sch19a, SK12b, Seo18, SWM+10, Sia12, SC12, SL+16, SGP18, Svm+17, ST0, TMC15, TT12, WP17, WZ15, WWHL12, Wl18, WSQ+16, XNK15, XXZ12, Xio12, XJW13, YL17, YKC+11, YFK+12, YMC+17, ZCQ19, ZY17a, AA14, ATK+17, AK14a, ABAH18, BS15, BZD16a, BSW12, CFG+17, Dur15, HZWW17, Hbl19, HL14, HYL+19, HTC17, LSNB14, LLY15, LFSW15, LH13, LL16a, LLG19, RPSL10, SES+16, SY15b, SLXX16,
VN17, XWK17, XLC19, YT11b, YYS16, YN19, ZZ11). public
[ZCC15, ZCL19, ZY17b, FBM12].
Public-Coin [CLP13a, Mat14].
Public-Key [BV5+13, BKKV10, GKS17, KFOS12, LLLH18, MMP14, MPRS12, NTY12, Orr16, PDN15, RSBGN12, RW12, SK12b, Sco18, SWM10, Sia12, XNK15, XJWW13, YKC11, YFK12, ZY17a, ABW10, IM14, LPdS10, LZC14, AVAH18, BZD16a, BSW12, HYL19, LLG19, RPSL10, SES16, VN17, ZCC15, ZY17b]. Publication
[MMKP16, ZTL15].
Publicly [NMP13, SZQ17, YNR12a]. Publish
[BGP17, DLZ16b, OFMR16, PRSV17, SL11, Tkr14, YSM14].
Publish/Subscribe [DLZ16b, OFMR16, PRSV17, Tkr14, YSM14]. published
[MMKP16, ZTL15]. Publicly
[BL15, BL16, MLBL12, MV16b, HM10].
Quantization [SSA13], Quantization-Based [SSA13]. quantizer
[Pan19]. Quantum
[And19, Ano15d, Ano17d, Ano17e, BB14, Ber14, Bro12, BCF14, CK17, Che17, CCL13, FeH10, FKS13, Fol16, JEA15, JL18, Kar12, KP10, KG19, LL18, LM14, LHA16, MS16, MSU13, Mos18, MKAA17, NNA10, NA10b, NDR19, QC18, RK11, RSM15, RS18, Sas18, Sti11, SD18, TKM12, Unr15, WCL18, Y17, ZWS18, AP18, ABB14, BJ16, BCDN17, BCND19, CML16, Dya19, Edw17, FRT13, GJMP15, IM14, Jsk16, Kam19, KKK16, Lp11, Lam13, LyWS10, LCW16, Liid12, QD16, SPD10, SK14, Svo14, VV19, Wmu14, YDH15, vDKS11, Sen10, Yn11]. Quantum-Oblivious-Key-Transfer-Based
[WCL18]. Quasi
[BGJT14, OWHS12, OTD10, BGJT13]. Quasi-Chirp [OWHS12]. Quasi-Cyclic [OTD10]. Quasi-Polynomial
[BGJT14, BGJT13]. Quaternion
[HD19, YWNW15, yWpWyYpN13]. Queries
[GYW19, HLW12, LH1R10, PBC17, ZQ19, BKV13, CHX13, DFJ17, GLM19, HM12, PRZB12, TKM13, WL19]. Query
[DCA18, GA11, PCGG14, WCL18, XLP18, AAI19, AZPC14, BS13a, BKR19, CH11, ED17, Hwk15, JCHS16, JLC18, LAX14, LZW19, LW13a, XMY17, YQOL17, ZZC17, ZHT16, ZZL19]. Query-preserving [GA11]. Quest [Fox13]. Question [TWNC18, Cha13b]. Quisquater
[Nac12]. Quorum [Kar12].
R [Gret19a, BS12, DB16, LVV11, LJF19, PP10b, WYYW14]. R3579X [BDK11].
Rabbit [FSWF11]. Rabin [Chi13a]. Radar [Laz15].
Radial [HD19, pNyWyY+14, CG12b]. Radio [KAHKB17, CJP12, CJP15, EA12, Kim11, NLYZ12, RPG12]. radio-frequency [CJP12, CJP15].
Radix [ARM15a, GKC11]. Radix-8 [ARM15a].
RAGuard [ZHS19]. Rail [HF14b]. raised [LJY16].
Raising [YWW10]. RAKAPOSHI [IOM12]. RAM [RZF13].
Random-Grid [KS15]. Randomization [DDE+19, Gas13].
Randomized [ARP12, CATB19, GDLL18, GT12, HHR11, SR12b, BWA13].
Randomness [AY14a, Ana14, AFB12, ACM+17, BWLA16, DB16, HKK19, KMZS19, MS10, MS16, CHH+13, DTZZ12, FRT13, RY10, TC11].
Range [DCA18, BKR19, HMK12, JC1S16, LZW19]. range-query [BKR19]. Rank [SS10b, FES10].
Ranked [CWL+14, XWSW16, DDY+19, GZS+18, LXK+14, NJB19, YQZ+19]. Ranking [ZDL12, AT10]. ransom [Ano13b].
Ransomware [MPA+18, YY17a]. Rapid [KPC+16]. rare [Sch11]. RASP [AZPC14].
RASP-QS [AZPC14]. Rate [LJK17, PPS12b, PCPK14]. Ratio [FHKP17]. Rational [CK18, HR19, KU14, KOTY17, NS12, TWZ11, ZC13].
RC4-like [RS14]. RCB [ABC+18]. Re [ABR12, Bre18, GSW+16, GX19A19, KKA15, LK18, LSLW15, LSC12, LBR12, MLO17, NAL17, Pau19, Pet12, PRSV17, WY10, XJW+16, ABC+18, BGP+17, CFZ+10, CLH+16, CZ15b, DEL19, FSGW11, FSGW12, FPX12, GH12, GI9, HD16, HYF18, KKM+14, LMJC11, LCT+14, LFWS15, LL16a, Par18, SYL13, SLZ12, SKB+17, Tia15, WGT10, WHY+12, Wan18a, WX121, WLS14, XXX15, YZCT17, ZDW+16, LAL+15].
Re-authentication [LBR12, FXP12, LMC11]. Re-creating [Bre18, Pau19]. Re-Encryption [GSW+16, KKA15, LSLW15, MLO17, NAL17, PRSV17, XJW+16, ABR12, GX19A19, LSC12, Pet12, WY10, BGP+17, CFZ+10, CLH+16, CZ15b, FSGW11, FSGW12, GH12, HD16, HYF18, KKM+14, LCT+14, LFWS15, LL16a, SYL13, SLZ12, SKB+17, Tia15, WGT10, WHY+12, Wan18a, WX121, WLS14, XXX15, YZCT17, ZDW+16, LAL+15].
re-enrollment [DEL19]. re-keying [ABC+18, GJ19]. re-registration [Par18]. Re-Signature [LK18].
Read [LLPY19, Sto12]. Read/Write [LLPY19]. Reader [JLZ18].
Reader/Router [JLZ18]. readers [HDPC13]. readership [Bai12]. Readily [HGOZ19]. Ready [GOPB12, Mos18]. Real [AE18, Ano16j, Ano17d, ABL+18, AY15, Bel15, BFK16, BPS16, BNA15, Cer14, CC14, GSC17, JW1+17, LBC18, MK11, PNRC17, RHLK18, SK14, Tom16, Turl18, WLZ12, YE12, AY14a, Cou12a, Kus13, NSX+18].
Real-Time [AE18, AY15, GSC17, JW1+17, PNRC17, RHLK18, WLZ12, YE12, CC14, MK11, AY14a, NSX+18].

Reasoning [TSI14]. reboot [And19].

Receive [Orm16]. Receiver.

Receive [LTC+15a]. recall-based [LTC+15a].

Recoding [Abbi12, TMK11]. Recognition [AQD12, BCTPL16, BJCHA17, DM19, IA15, LGM+16, MI14b, Bag12, uHAN+18, HURU11]. Recommendation [BD15, Bar16a, Gir15, KKK+18a, NIS12, TBK+18].


Recovery [Bro17, DSSDW14, DSSDW17, LYY+18b, LL19, MPA+18, NRZQ15, QIC+18, SA15, SAA15, WZ15, BM15, CHHW12, CGH17, MBP19, PX13].

Rectangular [CWZ19, WLC12]. Recurrent [CSH+18, Pud12]. Recursive [LXLY12, WH18]. ReDCrypt [RHLK18]. Redesigning [VFV17a, VFV17b].


refined [KGP+19]. Refinement [BCEM15].

Refinements [LL11]. reflections [Hai17, OF12]. Reflexive [SRRM18].

refractive [PHN+12]. Refresh [LSC+15].


Rejewski [Kap13]. Rekeying [DT13, QLL17, CLSW12, DS11].

Rekeying-Aware [QLL17]. Related [AH19, CWZ19, Cil11, CMA14, DGIS12, HLLG18, Pud12, WLC12, DMSD18, GLMS18, GMDR19, MNP12]. Related-Key [CWZ19, CMA14, HLLG18, Pud12, WLC12, DGIS12, GLMS18].

Relational [HPC10, RP12, WP17, BFG+14, BL11, GA11, JK13, PYP10]. Relations [BP11, FHS13, HLR11, WGD18, KGO10, LLM+19].

Relationship [CZ19]. Release [KFOS12, RSBGN12, Unr15, WSS12]. released [GSGM16]. Relevance [Sim15a].


remapping [PSJ+13]. Remarks [SSU12].

remediations [ACC+13]. Remote [BCE+10, BWS19, CS14, FYMY15, LZCK14, MHL18, Sar12, SYY+17, VMV15].
WgMdZlZ12, WgMW12, CHS11, HU15, HL12, IB11, KKG14, LH10c, LNM+11, LNKLI3, LWK+18, LH13, MCL+19, MM12, Sar10a, WQZ+13, YSL+10, YN19, PZL+19.
remotely [Wat14b, YHHM18]. Removing [HKHK13]. renewable [HRK+19].
Renewal [MMY12]. renewed [GPLZ13]. rental [LY14]. Reordering [Alo12].
Requires [Raz19]. requiring [KHHH14]. ReSc [YFT18]. Rescue [TSH17].
Research [BNMH17, BA18, CDFZ16, FREP17, Roh19, SDC+17, SPG+19, WP15, BEB+18, GLIC10, Hof16, Pal15, Ven14].
Researchers [Con12, Con17, Edw14, Wal18, Win17]. Reservation [LSY+16]. reset [RY10].
Resiliency [YM16]. Resilient [AV12, BKKV10, FPS12, HD19, HHS18, JP19, LTZ16, LD13, NYR+14, Pan14, PSD15, XZY+12, YZ12, YNR12b, YCZY12, ZYT13, ZWTM15, ZM17, ZYZ+19, ZYY19, ZY17a, ZYM18, ZYH+19, ABC+18, CAM19, CQX18, DLZ16a, GV14a, KPS10, Kom18, LLG19, MMSD13, SCBL16, SGP+17, Wan18a, YSJL14, YKC+12, YLZ+16, ZY17b, ZYM19]. Resistance [CGCS12, GZSW19, PRC12, WLZL12, ZJ11, DLN13, FIO15, XYML19]. Resistive [DSB16, TLCF16]. Resistant [MM17b].
Resolution [LHW18]. Resistant [DR18]. Resource [CSH+18, CR5+18, HM19, JMG+16, JWN19, SIZM13, YNR12a, ZSH+19, AMH10, FZQF18, KAS15, LLZ+16, MHV15, Wan13, XWZW16, ZPY+16].
Resilience [FSX12b, HWYW14].
Rock-solid [Cri16], Rodney [DDS12], Rogozin [Kuz11], rogue [AYSZ14], Role [GB19, PH12b, ZVG16, HPJ+19, ZHV14].
Role-Based [ZVG16, ZVH14]. Ron [LHA+12b], Room [Sm11b, Pea11], Root [ARH14]. ROP [ZHS+19]. Rosen [HR13].
Rosenhain [CDSL14], Rotation [MM17b, SBS18, LWW11]. Rotational [KN10, KNR10]. Roulette [Ber17]. Round [Ber17, jCPB+12, COP+14, CIJZ13, DWWZ12, GCHR14, KOTY17, KMO14, LWZ12, LJ17, LJ18, LYD+18, LSG+19, Pan14, TYM+17, XZLW15, Yon12, AY14b, ABM+12, Blo15, DMSD18, JK19, LP11, LFW+16, Sun11, TSSL11, TQL+14, TCS14, XW12].
Round-Reduced [DWWZ12, DMSD18]. Rounds [GST12, Sas12, LYHH14, MNP12]. Router [Bis17, JLCZ18, SA15]. Routing [ARKW19, Ham12, KZG10, WLY+15, LSG16, LC17].
Routing-Aware [ARKW19]. RSA [Dun12b, Kia11, Pie10, APPVP15, BBBP13, Bro17, BNST17, CCL+19, CLSW12, Chm10, GM13a, GST13, Her14, Hin10, HLYS14, IK15, KV19a, KHHH14, KFL+10, Lim11, LFK19, MV19, MZ15, Moo12, PT19, PY19, SM10a, SM10b, SLM10, TK19, Win17, XWK+17, YHK+10, YXA+16, sCR19a].
s [Sch15a, MM17b, NN12, RMP10, RMTA18, SS11, WJ19]. S-Box [RMTA18, RMP10]. S-Box/Inverse [RMTA18]. S-Boxes [MM17b, NN12, WJ19, SS11]. S3BD [WS19]. SA [LHM14]. SAC [YJ14, MV12].
Scalar [ARM15a, NR15, YTS12, SKH15]. Scale [DM15, GU13, JKHeY12, LLSL19, LQD19, And19, CG12b, dCCSB11, LLKA19, MBR15, PY19, QZL+16a, WHL17, ATKH+17, BBTC20, DYZ+15, GM13b, GSN+16, JVD16, MNN+16, WLWG11, WDLZ13, WLFX17, YC11, KCR11, KS11].
Scalability [ACM11, Ano10a, Dun12b, LWW12, ZG16, LHY14, LLSL19, LQD19, And19, CG12b, dCCSB11, LLKA19, MBR15, PY19, QZL+16a, WHL17, ATKH+17, BBTC20, DYZ+15, GM13b, GSN+16, JVD16, MNN+16, WLWG11, WDLZ13, WLFX17, YC11, KCR11, KS11].
Scheduling [Pud12]. Scanning [DA16, LJ17, MV16b]. Schema [AN12].
Scheme [ARM15a, ADM19, AMSPL19, ASS15, Bai10, BG12, BS14, BKJP12, BDH11, CMLS15, CLL16, CCW+10, CLHC12, CHHW12,
CCZC13, CCC19, CGY+13, CLH13, CSW12, DA10, DS11, DKS12, EAAAA19, FR16, FGH10, GZZ+13, GH11b, GJZ17, GLW12, GZH17, HYS11, HIDFGPC15, HMR12, HWS+19, HLC+18, HHP17, Hul13, HLH19, HP12, HP17, IL15, JSZS12, JLX+19, KU14, KP12, KTT12, KK12, KKA15, KSSY12, KL+12, LSL12b, LBH12, LTH+15, LTFZY16, LH11c, LSQZ17, LSQL18a, LGWY12, LCPD15, LTC+15b, LYY+18b, LPRPH14, MWZ12, MVVR12, MRL+18, MMN12, MSas12, NXB13, NLLJ12, NLY15, Pet12, PDT12, RVH+16, RSD19, RMG18, SK12a, SSKL16, SJ12, SGP+12, SD12, She14, ST16, SWF+19, SP15b, SJWH+17, SSA13, Tan11, TTD10, TWZ11, WY10, WgMdz12, gwpNyY+14, WHL15, XWSW16, XHC+12, XJW13, YM16, Yam12, YZX+12, Ye10, Ye15, YTH17, YL17, Y+17, YHK+10, YMWS11].

Scheme [YY17b, ZPM+15, ZZQ+19, ZC13, ZQ15, ZW17b, ZM18, ZLD12, ZY17a, ZGZ18, AMN18, ARL13, AHS14, APK+18, AK+17, AM19, BC16, BDL+19, BD18, BDM+19, BOB13, BBN19, BAL10, BWR12b, BMM12, BZ12, BB16b, CCL11, CLSW12, CNE+18, CH10, CT11a, CLHJ13, CW14a, CTHP16, Cho14, DLY+19, DSCS12, EAA+16, EY15, FLL+14, Far14, FA14a, FHZW18, FZ+12, GZH12, GJ13, GMRT+15, GJJ18, GPLZ13, GLM+16, GH16, GAI+18, GBC19, GTSS19, HKA+18, HZW18, HBBRNM+16, HL12, HL11, HCCC11, HLC16, HCC10, Hwa11, IB11, JNUH17, JKAU19, JLT+12, JZS+10, JM+16, KFE19, KI11, KPP16, KD15, KK13, KHM13, KKM+13, KKM+14, KKG14, KCS+18, Kim16, KKK+18b, KHH19, KP18, KWL+16, KWL+17, KDW+17, KKD+18, KWH16, KL11, LXY12, LL+16, LSR13, LYC+10, LH10c, LYW+10, LZJX10, LNM+11, LMJC11, LIK12, LLH12, LNKL13, LDZ+14, LWYM16, LIK+17, LNK+18a].

Scheme [LWK+18, LNK+18b, LWK+19, LFWS15, LHH11, LWL10a, LWL11, LW13b, LZC14, LZZ19b, LDZ19, LL16a, LL16b, LWY12, MCN+18, MMS17c, MK12a, MGB19, MSas13, NR17, Nos14, NX15, ODK+17, OSNZ19, OPS14, OSANAM19, PY19, PZBF18, QC17, QMW17, RPS10, SGGCR+16, SM11, SYWX19, SCR19b, SMS+16, Tan12b, TY16, TK14, TD14, TLL13, UUN11, WWZY11, WWYY11, ywpNyL11, W1312, W1316, W1317, Wan18a, WXMZ19, WXSH19, WHZ+19, WDKV19, WZ11, WKK11, WOLS12, WXK+17, XHH12, XWZW16, XW114, XXX15, XWZ+17, XTZ+19, XXY19, XMHD13, YWJ+19, YC11, YCC16, YHMM18, YSQ19, YWK+10a, YCT15, YXD18, YQOL17, YYY13, YMSH10, ZYL+10, ZLY10, ZJX+14, ZYC+17, ZZY+19, ZYW+19, ZPYY12, ZHH+17, ZY17b, ZFH+18, ZLY+19, ZC12, ZBR11, DT13, LLZ+12].

Schemes [AAUC18, ACA+16, ABF12, BVS+13, BFM12, BB14, BS15, CMLR13, CZCD18, CLND19, CGL+12, Chn16, Des10b, EFGT18, FHK17, FFL12, HSM14, HLLG18, HPO+15, LWL10b, LZC14, MLCH10, MR14b, MMS17b, MBF18, MKRM10, MKASJ18, Ob11, PB12, PDN15, PH12b, Sch10, Shi11, STH17, SU12, VS12, WGF16, YNR12a, YNR12b, Yek10, YYW+12, AGP14, AN15, AHI+12, BKR19, CDG12, CXX19, CHS11, CCG10, CTL13, DDD14, DDI13, DZ14, FPG14, FGMP12, FMA+18, HKA19, HWD16, HM10, KTDU16, LWL+19, LHYZ12, MM12, MBP19, MA17b, NZL+15, QYWX16, SES+16, Sar10a, Sar11, hSZZ15, SAR18b, WW14, YT11b, ZC12, ZCL14, ZT14].

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

Scope [Bai12]. Score [GCSÁdP11, HW19].
scoring [OSSK16]. scrambler [Pau19].
Scrambling [LLL17a]. scream [DMSD18].
Screen [SPW+16, CTL2, IAA+19]. Script
[Rao10, Bax14]. Scripting [DSB15]. scroll
[GMOGCC15]. SDB [HWK+15]. SDDO
[PL16]. SDDO-based [PL16]. SDH
[GM11]. SDIVIP [YNX+16]. SDN
[DHT+19, KCC17, YHSW19]. SDN-Based
[DHT+19, YHSW19]. SDVS [Wan10]. SE
[LLLS13]. SE-eka [LLL13]. seals
[MN10]. Seam [LC15]. Seam-Carved
[LC15]. Search [AHN+18, CWL+14, Che15,
DCA18, FRSt+16, GTT11, HWP18,
HCDM12, HLH19, LSQL18b, SOR16,
TMC15, WCDL18, WW12, XWSW16,
XJW13, ZXY16, AGH18, BZD16a,
BT15, BL11, CLI+16, DDy+19, FH13,
FSG12, GZS+18, HKA19, HH16,
MRR+18, NJB19, OSSK16, PWS19a, SY15b,
WH1+12, WXLY16, WMC17, WS19,
WX+18, XTZ+19, XLC+19, YXD18,
YQOL17, YQZ+19, ZZ11, sCR19a].
Searchable [BHJP14, CWWL12, CLW16,
CGK011, FII11, HKA19, PBC+17,
PCY+17, XNKG15, ZZQ+19, CLC+19,
CXWT19, DLZ16a, DRD11, HZXH14, HK19,
HTC17, JCH16, LZC17, LLL+18, MML16,
RPSL10, WXLY16, WCCH18, YZCT17].
Searches [Sia12, WR15]. searching
[GNP+12]. Seattle [LCK11, KCR11].
Seberry [AHS14]. SEC [PA10]. SecLAP
[AMK19]. SECO [DYZ+15]. Second
[AKY13, ABM+12, Gre19, LGP19,
SNG+17]. Secondary [RS11]. Secrecy
[ABD+15, BKST18, BCND19, KZG10,
TSH14, Yon12, ABD+19, ATKH+17, Bia12,
RCW15, TCS14]. Secrecy-preserving
[TSH14]. Secret [ASN1, ASN2, ADH17,
Ay12, Bai10, BBP+16a, BFM12, BBEP14,
BP06, BCDN17, BCND19, Bri11, BLU+15,
CCM+15, CFOR12, CCL+13, DR12, Dew11,
EM12, EA11, FHKP17, FR16, Fok12, HYSS11,
HL10a, Has16, HZX+18, JLS12, KU14,
KS18b, KOTY17, K12, KK13, KSSY12,
KS15, LKBK19, LHF12, LPL15, Lini15,
LCCJ13, LTC+15b, L1J6, LLKA19, Men13b,
MNS1, NS12, Ob11, PCPK14, QS18,
SLL10, SC10, SS10c, SSU12, Shi15, TLW12,
TWF11, WKB16, WGF16, Wil18, XZY+12,
XJR+17, YFF12, YWZ+12, ZC13, Ald11,
AIM+19, ADG16, AKK+17, Ara13, AGBR19,
BJ16, BEB+18, Bud16, Cha13c, CT11b,
CW14a, CLz+17, DD13, EAAZ13, EZ15,
FHH10a, GEAH11, GJMP15, GLW13,
HF14a, H15, Hea15, HBBRNM+16,
HCC11, HLC12, KFE19, K111, KU116,
LXY12, LH11a, LT13, LyWS10, LHYZ12,
LEW19, Mas17, Mc10, Mc11, Mc12].
secret [MBB11, OO10, Par18, Pea11, Pet11,
QD16, Rus15, SB17, SA12, SAR18b, SM10c,
TQL+14, TD14, UUN11, UUN13, WYL13,
WZ11, WS12, WOLS12, Wu17, WX13,
YC11, YCC16, YSC16, ZCL+12, ZZ15,
ZPWY12, LSC+15, Bai12]. secret-key
[BJ16]. Secret-Sharing [BBEP14].
Secretion [RSC18]. Secretocacy
[Ber16c]. Secrets
[BT12, CG14b, DLWW11, FMS12a, Kob10,
Man13, Bha16, Cop06, Cop10b, GGH+16b,
Gup15, HRS13, LDC13, Smi11a, Ano17b].
SECURITY [Ano19a]. Section [BdD19].
Secure [ADM19, AMK19, AAL19, Alz19,
ACA+16, ADMM16, ABPP16, ABL+18,
AAR12, Ash14, AMH+16, BVS+13,
BWAL16, BCGH11, BCG12a, BCQ+13,
BWA13, BJ12, BHP14, BF11, Bru12,
BD11, BCEM15, CFOR12, CC17,
CFZ12, CZLC14, Che15, CDWM19, CMA14,
CDLW19, DM18, DL15, DMS+16, DG15,
DYZ+15, DLZ+16b, Edw17, EAB+19,
FLH13, FYD+19, FMC19, Fri10b, FDI1,
FSX12a, GQH17, zGXW12, GKM16,
GGHR14, GFBB12, GT12, GV14b,
GHKL11, GM14, GZS+18, HvS12, HSM14,
HLLG18, Har16, HL10b, HP14, HTZR12,
HMCK12, HLC+18, HLK15, HYSS18,
HK14b, HLH19, IL15, Jac16, JKA+18,
Secure [NBZF17, NDG17, NR12, NMS14, NSMS14, PB12, PSM17, Per13, PBC17, PRN19, QZL16b, QZDJ16, QQZ18, RC18, RMP10, RR17, Rea16, RMZW19, RSGG15, RS19, SAM19a, SNJ11, SSKL16, ST19, SZZ14, SVCV15, SP15b, SKH17, SS15, SRAA17, SAR18b, SSAL11, SVG16, SVY17, SYC17, SMS14, SZDL14, SGH15, SLY16, SR12b, SM18, TB18, TCL15, TWZ11, TG12, TGC16, VTY18, VMV15, WgMW12, WBK16, WXY16, WLY17, WDCL18, WDJ19, WHL15, WBA17, WWHL12, WS19, WMS12, tWmC12, WXSW16, XLQ09, XJWW13, XLP18, XHZ19, YN12a, YN12b, YTH17, YQZ19, YHK10, YKC11, YAM15, YY17b, YGD17, XXZ11, ZDL12, ZDHZ18, ZHV14, ZVG16, ZHT16, ZLV17, ZHZ19, ZBR11, AHS14, APK18, ABBD13, ACF16, AKK17, ACD15, AYSZ14, BMDT19, BOB13, BH19, BDZ16, BKR19, BSR14, CCLL11, CSD18, CLHJ13, CW14a, CS11, CDL18, DA18, DEL19, DMM10]. secure [DGL19, DMD18, FHI10a, FLL14, FSXW12, FA14b, FIO15, FLHY16b, FS18, Gal13, GAI18, GLL18, GCH15, HGWW11, HWW15, HLYS14, HTC17, HPY10, IB11, JZS10, KPP16, KKA14, KRM10, KCS18, KUT16, KLV17, KDW17, KDD18, LLLS13, LDDAM12, LH11b, LW16, LSR13, LHM10, LDZ14, LWK18, LZD19, LZW19, LWK19, LCT14, LAT15, LJY16, LH18, LL16a, LL16b, LBOX12, MR14c, MHY18, NR17, NAICR12, NA17, ODE17, OSNZ19, OSANAM19, PABC19, PSdO13, PLSvdLE10, PWS19a, PY19, PBP19, Rao17, RG10, RYF13, RITF11, RS15, SGGCR16, SYL13, SWW16, SSS11, SM10c, SSPL13, SXL16, SLXX16, SC19b, Tar10, TLM13, TAA13, TLL12, VS11, WLZ16, WMY17, WXZM19, WHZ19, WDKV19, WCCH18, WL19, WXWC14, XXY15, XZP19, XMY17, XWK17, YXMY19, YC12, yYqWqZC13, YZZ14, YZCT17, YQOL17, YY11, YLS12, YJC18, YMSH10, ZLY10, ZCLL14, ZZ15, ZQD16, ZYC17, ZG10]. Secure LR [JHW19]. Securely [CC10, KP17, LHL14, MS16, WXY17, BC18, der10]. Secure MR [DMD18]. Securing [AASSAA18, BK12b, CMLS15, CST17, Cla18, NPH14, PMZ13, SFE10, SMSK18, SWF19, SLI11, Ste15b, TKR14, YMA17, YTM12, YHY19, CR10, Din10, GH15, SKS18, SA15, Tox14, YWZ18]. Securities [WWL14]. Security [ABJ13, AHN18, ASBD16, Ano13f, Ano15a, Ano15d, Ano19a, ABF12, AN15, ABHC16, ABB19b, AYS15, BCA10, BSBB19, BA18, BCM15, BCHL19, BRT12, BPR14a, BPR14b, BLS12, BCNN16, BDP12, Bra15, BDH11, BP10, CFST17, CF16, CBX19, CHS11, CFXY17, CCD15, CCDD19, CSQL20, CPS16, CM11, DDS12, Dan12, DR12, DK16a, DFCK17, Elb09, FRRP17, FMA18, Fid18, FMA19, FP19, FSX12b, FSX12c, GN16, GZZ13, GR19a, GPR19, GSC17, HC12, Hel17, Her19, HB17, HSUS11, HWW12, HXC17, HLC11, HLT15, HYN10, IEE15, ISU12, IGR16, JN12, JSA17, Jia14a, KBL11i, KS13b, KFOS12, KSD17, KD12b, LPS12, LST12, LW11a, LK14, LLPY19, LJP17, LW12, LLZ17, LTW11, LSQZ17, LYL18, LSQ18b, LP12, LW17, LZC12a, LWL17, LZZ19a, LNZ19, LDB15, LMS16, LLC18, MMKP16, MNTY11, MKN13]. Security
[MCS+15, MH14, Mau12, MV16a, MGG+19, MLBL12, MPM+17, MHMSGH16, Nac12, NNAM10, NGD+17, NVM+17, Nos11, Nos14, OSH16, Orn16, OS16, Past13a, PZPS15, PGLCX17, PDHN15, PS14, PL16, PDT12, PNR17, RB17, RCP+18, RVS+18, RQD+15, RWZ12, Rog16, RS10, SGG18, SN10, SNJ11, SBS+12, SBS18, SPD+10, Sar12, Sch13, SD12, Shi11, SC19a, SLM10, STC11, Sti19, SSP19, SAM+18, SMOP15, SCGW+14, Tso13, TV15, VFFHF19, Wal18, WYCF14, WSA15, WZ16, WRP70, WSS12, WHLH17, WCL+18, WS14, Yan10, YZLC12, YSF+18, YHSW19, YGS+17, YYY17, YSS14, Yon11, YYW19, Zha15b, ZM18, ZXL19, ZYY19, ZY17a, ZYH+19, ZCZ+19, vTJ11, AMN18, AB10a, Abe10, ABGR13, And19, ABM+12, Ano11a, AM19, ABGR13, And19, ABM+12, Ano11a, AM19, AGBR19, ADH17, BLY10, BSS11, BDL+11, BLV17, BM11, BL11, CO11, CTHP13, CLCZ10, CVG+13],

security [DLK+16, DGMT19, DXWD16, DHW+13, Edw14, FHM+12, FA14a, Fei19, Fis15, GHD19, GM16a, GLM+16, GMMJ11, GMS11, GH12, HPJ+19, HWDL16, HWG10, HLR11, HRS13, Hod19, HLV10, IAA+19, JK19, KNTU13, KSA16, KKK+16, Lan10, Lan13, LDC13, LH10a, LZ11, LXMW12, LHH11, LZC14, LSG16, LLG19, MZA+13, MZL+19, Men13b, MM14b, MSGCDPSS18, MSK+18b, NS10, Nam19, NCL13, NLYZ12, NML19, OK18, OYHSB14, PHWM10, PMG19a, QYWX16, QLZ19, Rec15, RFS10, RH10, SA12, Ser12, SYV19, SLZ12, SY15b, SYWX19, Sar16, Stai11b, Tan17b, TODQ18, Tay19, THA+13, TKG+17, UUN11, VCK+12, WCFW18, XLC13, YLL+18, YY17a, ZAAB17, Zha15a, vdWEG18, WX12, YKC+12, Bar12],

Security-Aware [LJ17, LMS16, GHD19],

security-enhanced [AMN18],

security-modified [MM14b],

SEDURA [LY15], see [PZ15],

Seed [AS17, LYHH14, Sun11], seeing [Tox14],

seen [Goo12, PWS+19b],

Segment [WOLP15],

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

Selected [DD12, Dan12, MV12, BYL10, JY14, LH10a, vDKS11, JY14, MV12],

Selection [KÖ14, KD12a, KD19, RP12, SEY14, YKA16, DRN16, FXP12],

Selective [BTHJ12, GDCC16, JSA17, LW12, LSC+15, LZC12a, LLH18, PWS+19b, LZC14, LW13c],

Selective-Opening [LLH18],

Self [Cer18, CLL16, CHHW12, CV15, DM18, HZ11, LCL+17a, LLPY19, LH12, LHM14, PRGBSA19, RCK17, SAA15, SM12, TAP19, WHZ12, WXW14, ZLDC15, AGH+17, FXP12, HL14, LT13, LH13, SH11, YN19],

Self-adaptive [LHM14, FXP12, SH11],

Self-authenticating [Cer18],

Self-Certified [CLL16, WXW14, HL14, LH13, YN19],

self-composition [AGH+17],

Self-Controllable [ZLDC15],

Self-Defense [RCK17],

Self-Identifying [CSV15],

Self-Recovery [SAA15, CHHW12],

Self-restoration [WHZ12],

Self-Sovereign [TAP19],

Self-Synchronized [DM18, PRGBSA19],

Self-Synchronizing [HZ11],

Self-Updateable [LLPY19, LCL+17a],

SELinux [SFE10],

seller [KJN+16],

Semantic [DDY+19, MHW+19, YZCT17, HLR11, HTC17, JS18a, WS19],

Semantic-aware [DDY+19], semantically [YZCT17, HLR11, HTC17, JS18a, WS19],

Semantics [CM11, Glii12, KGP12],

Semi [AAA+19, BDOZ11, KKK+16, SEK+19, WHZ12, ZXW15, PGLL10],

Semi-automated [KKK+16],

Semi-Autonomic [SEK+19],

Semi-Fragile [AAA+19, WHZ12, PGLL10],

Semi-homomorphic [BDOZ11],

Semi-trusted [ZXW15],

Seminarty [SS10c].

Semirings [Dur15].

Sender [WZ15],

Sensational [YGFL15], sense [BH19, Kem11],

Sensemaking [HGOZ19],

Sensing
[CCZC13, Kar12, MJS+19, PWS+19b, uHAN+18, RPG12, XWZW16, Fay16].

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

**Sensitivity** [YGD+17, LW2+10]. Sensor
[ABC+17, BN14, CS14, DS11, KH10, LL11, LL2+12, NN11, NYR+14, OKG+12, PX13, PCPK14, RWL14, SP15b, Y16, ASO14, APK+18, AIB+16, AIK18, ADF12, BNN19, BLAN+16, BB16b, CDGC12, CWS12, DSC12, DL13, HKA+18, HCT+10, JN17, JW1+16, KL+10, KO16, KLW+16, KD17, LNK+18b, PL16, RR17, SMZ13, SSK10, Wn13, WW14, WD18, WX1+17, XWN12, XMD13, ZY17, ZY2+10]. Sensors
[DM19, DL12, LI+17, OMP18].

**Sensory** [SGC14]. Seoul [HL10a, LW11a].

**Separable** [LSSL19]. Separating
[RCB19]. Separation [MJS13]. Sequence
[PFS12, WGC+12]. Sequences
[ADD10, Kla10, NN12, XNP+18, XYXYX11, HL12, VM14].

**Sequential**
[GLR10, GLR13, HWZ19, LLY15, TLZ+17, SM19a, WYL13]. serial [MC19]. Series
[BJL16, EKOS19, Die12]. Serious [AG18].

**Serpent** [PC16]. serpentine [KMK11].

**Server**
[AV18, BCO13, Che15, GMS14, LSQL18, LN19, LYL15, MV19, YL13, ATK+17, BK19, BBD16, CSD18, CLHJ13, F14b, FHZ18, HDP13, HL14, ISC+16, KMTG12, KLW+17, LXM12, LH13, MHL18, SY15b, hSZZ15, SSS11, SSL11, TLL12, WT10a, XHM14, Y19, YY13].

**Server-Aided**
[GMS14, LN19, MV19, LYL15, SS11].

**Server-Designation** [Che15, LSQL18b].

**Server-Side** [BCO13].

**Service** [BKBK14, CCS14, GGG18, GKG19, Hay13, LDB+15, LBR12, MJW+18, NRZQ15, RSGG15, SP+19, SPPC12, Sti15, VS16, VFFH19, AaBT16, AAH+19, HK17, KPP16, LHL+18, LW13a, MMP19, MLM16, Par12b, SVY19, Wu17, YWK10b, ZX11, CWZL13, YCM+13].

**Service-Based** [LDB+15].

**Service-Oriented** [RSGG15]. **Services**
[ANO11, DLZ+16b, JP19, MEFO12, O012, PSM+18, ZHL15, AZPC14, Bel18b, CXX+19, CAM19, CSD18, CHX13, DYZ+15, GAI+18, IMB17, IGI1, LWYM16, LZD+19, MSL13, NSDA17, NZL+15, OK+17, PP11, WD19, XXX15, YJC18]. Session
[BS12, BKJP12, CFST17, SHS12, AN15, BCFK15, DCAT12, DGMT19, SHBC19].

**Session-Based** [BKJP12]. Set
[Cor14b, EKP+13, RSI17a, YZ12, Con12, GR19b, T112]. set-valued [T112].

**SET** [Sch16a]. Sets [GL19, SPK17, SF12]. Setting
[BKLS12, HH17, MZH15, Mal17a, TYM+17, XXX12, ZHL15, Kom18, MML16].

**Settings** [GA19, GZ12]. Setup
[KZZ17, SOR16, Jia16]. SEV [BWS19].

**Seventh** [CS10]. Several
[HLC+19, Saa12, ZT14]. SGX
[MZ18, TSB18, WBA17]. SHA [AAE+14, ABM+12, App15, jCPB+12, Con17, LC17, MAK+12, Mor19a, NIS15, SKP15]. SHA-1
[AAE+14, Con17, SKP15]. SHA-256
[App15, MAK+12]. SHA-3
[ABM+12, jCPB+12, LC17, Mor19a, NIS15]. SHA1
[Con17, SBK+17]. SHA-256
[GGMW16]. SHA3 [FLYL16b]. Shadow
[Kap11]. Shadows [YSC+15, SLX16].

**Shaft** [Gol19]. SHA1P [HR18]. Shakes
[CNR14]. Shamir
[BDSG+13, UUU11, WKB16]. Shannon
[AMS+10]. Shape
[HF19, RITF+11, SY14, Pet11]. Shapes
[CJFH14, LMM14, SY14, SGS14, ZZCJ14].

**Share** [LTC+15b, GJJ18, ZPYW12]. shareable [XY+18]. Shared
[DRD11, LNXY15, NSP+18, OKG+12, TYK+12, XJR+17, YSL18, GEA11, LDC13, Par18, PZP15, SA12, TG12, YXS+16, YNX+16]. shared-secret [SA12].
Shares [BLU+15, CFOR12, KU14, SA16a, WY12, AIM+19, LJY16]. Sharing
[Bai10, BFM12, BBEP14, CCM+15, CFOR12, CCL+13, CCT+14, CLW16, DR12, EM12, FHKP17, FR16, HYS11, HLI10a, HRS13, HLT+15, KU14, KOTY17, KSSY12, KS15, LYZ+13, LPL15, Lin15, LCCJ13, LTC+15b, LLKA19, NS12, Oba11, PSM17, QZZ18, QJC+18, SC10, SSU12, SZZT18, TLW12, TWZ11, WYCF14, WK16, WGF16, WHL17, XNK15, XZY+12, YFF12, YWZ+12, ZC13, AKK+17, ADH17, CD16a, CT11b, CW14a, CLC19, EZ15, EA11, FGP12, GPLZ13, GMP15, GL13, GLB+18, GBC19, HF14a, HBBRNM+16, HCCC11, HLC12, HYF18, KFE19, KI11, KTB16, KPB17, LLY12, LH11a, LT13, LWF15, LAL+15, LyWSZ10, LHY12, LHL15, LLI+18, LEW19, LLI6a, Mas17, OO10, OO18, QD16, Rao17, SAR18b, TD14, UUN11, UUN13, WLW11, WMC17, WMZ19, WHZ+19, WZ19, WLS14, WKH11, WS12, WOLS12, YC11, YCC16, ZC17+12, ZZ15, ZPWy12, SLL10].

Shell [WZCC18, YSS14, Tay14]. Shemanske [Gre19a]. Shenzhen [IEE11a].


Shredder [AMH+16]. Shredding [AMH+16]. SHS [Ano12]. Shuffle [HMR12]. shuffler [BVIB12]. Shuffles [CKLM13]. shunned [Rec15]. Sicily [Cra12]. Side [AMMV18, AN17, Bar16b, BCHC19, BCO13, Bul18, CFE16, CDK+10, CBL13, CATB19, DZS+18, DMWS12, DKMR15, EWS14, GZSW19, GWM16, GPT14, KOP12, LWML16, LFK19, NDC+13, PR12, SG15, SR12a, Vua10, YL17, ZBF18, BVI12, CAM19, DJL+12, GSAV18, MCL+19, MFH13, SG19a]. Side-Channel [AMMV18, Bar16b, BCHC19, Bul18, CBL13, CATB19, DZS+18, EWS14, GWM16, GPT14, KOP12, LWML16, NDC+13, PR12, SG15, YL17, ZBF18, DMWS12, GZSW19, LFK19, BVI12, GSAV18, MFH13]. Sided [HP14]. Sieve [VM14]. sieving [SD17]. SIFT [KLY+12]. Sign [ACC+13, LL15, MEFO12, SPM+13].

Sign-On [ACC+13, LL15, MEFO12, SPM+13]. Signal [GDLL18, Kar12, BLL+19, MS13b, RITF+11]. Signals [Fyo19, LJK17, XNRG15, AIA+18a, AIA+18b]. Signature [Ano13c, ABF12, ASS15, AEHS15, BHG12, BDH11, CZZ17, CLND19, CYY+13, EFGT18, FGM10, FR15, GJJ15, GJZ17, GMSV14, GY18, HZ15, HPO+15, HHP17, Hüi13, HP17, JL16, LTH+15, LDZ16, LYY+16, LGPRH14, MMN12, NXB13, PH12b, ST16, TTH15, WZXL12, WH15, WYML16, WHL16, XLQ09, XGLM14, Y+17, YHK+10, YMWS11, YLA+13, ZJ14, ZLH+12, ZSY19, AGHP14, CLSW12, CCG10, Con17, DZ14, DXWD16, DLN13, HYWS11, Hwa11, JZS+10, LHM+10, LDZ+14, LWZG10, LL16b, Nos14, QYWX16, QMW17, QCX18, RMS15, SLM10, VS11, WSC14, XLWZ16, YVL+17, YLS12, YKC+12, ZLY10]. signature-based [DLN13, QMW17]. Signatures [Ano15a, ABC+17, AYS15, BB+13, BDFK12, BHH+15, Bu17, DMO+19, Fuc11, GY13, GdM16, HHS18, HS18, Hüi13, HRS16, HB+17, MFK+16, MCF17, MKA17, Orm16, PST13, TH16, Ver17, WCD19, YT16, ASVE13, AYSZ14, BD+11, BH19, BPP10, GCH+19, GMS11, HAGTdFR13, Her14, LL15, LJY16,
[Her19, Jin10, TLCF16, SS17a]. Soft-Error [TLCF16]. Softw [WZM12a]. Software [Bar15, Bee17, BCH19, EWS14, FHLOJR18, GZSW19, KYEV18, LRWV14, MRL+18, MV16a, Sco18, SAM+18, TLZ+17, YGD+17, ZPM+15, AGHP14, ABF+14, CFH+13, DK17, Eve16, GGHP+16b, GJ+12, HLV10, KHF10, LBOX12, SF12, YWT+12]. Software-Defined [KYEV+18, SAM+18]. Solan [CGB+10]. solid [Cri16]. Solution [DHT19, Fra15, GSFT16, HLKL15, Kam13, NA10b, YFT17, YFT18, Cor14a, MDHM18, SVG14, ZAA17, SAM+19a]. Solutions [Ano19c, BCH19, LLGJ16, BLV17, KAS15, MMP19, OMPSPL+19, TKG+17, WW14]. solve [Pec17]. Solved [IBM13a]. Solving [Ano17c, BB10, Hod19, Bul10a]. Some [AD12, Ber12, Dur15, LWL10b, Mid10].


[AGW15, AAT16, BBC+13, PMG19a]. SPARTA [MMS+17a]. SpartanRPC [CS14]. Spatial [AV12, CZF12, PDM12, ZWZ17b, CW14b, NZL+15]. Spatiotemporal [DIMT12, CXX+19]. Speaker [BJCHA17, PPRT12, RSR+19]. Special [Ano13f, Ano16b, Ano16c, Ano16j, Ano19a, AB10b, AHWB20, BCH19, Bd19, CWZL13, CSYY18, GQ17, LW13a, LKL18, MMKP16, PHWM10, XW13, YYW19, Zor12]. Specific [BD15, BDF12, KME+12, ARH+18].

Specification [HZ5+19, Int19, SK11, CWZL13, SD10]. Specifications [BMP12]. SPECK [LFW+16, AMKA17, BSS+13]. Spectrum [KD12a, TWZ+12, XNRG15, XNP+18, KPB17, LWY12, MMSD13].


[LGLK17, MPA+18]. **SSH**  
[YSS14, Cri16, Lit14, Ran10, der10]. **SSL**  
[BJR+14, Dav11, FHM+12, GJ+12, HREJ+14, NPH+14, PP11, Tay19]. **SSL/TLS**  
[BJR+14, Dav11, PP11].  
**SSL/TLS-based** [PP11]. **SSO** [MLM16].  
**ST** [DDS12, Dan12, MNS11]. **ST-Numbering** [MNS11].  
**Stage** [Mas17]. **Stakeholders** [RR16].  
**STAMP** [WPZM16]. **Standard** [Ano12, Ano13c, App13, ABC+17, BCM12, BV11, BV14, CT18, GJJ15, GJZ17, HZX15, LYX+19, LK18, LDZ16, Loc15, MVVR12, NIS15, OGK+15, RSD19, SZS14, TCL15, WWHL12, ZC13, BCM13, HTC17, Kim11, LJTZ12, LL16b, Mas17, TS16a, WZM12a, WZM12b, WWBC14, YC12, ZCL+19, AEH17, MKRM10, NMMW16, SJ19].  
**Standardization** [TRD11]. **Standardized** [BLN16].  
**Standard** [BCM+15, Che17, DW+13, NIS13]. start [Rom11]. **starts** [Sch16a]. **State** [BVS+13, BLM17a, BLM17b, But17, CG14a, CCL+13, CHS15, Dew11, DP17, FHR14, LK18, MKF+16, OMNER19, Sen17, WGD18, XZY+12, YM18, BBDDL+17, CK11, CGH17, Ham12, Mid10, QD16, Sir16].  
**Stateful** [BVS+13, NTY12, VP17, VSR12, YLL+18]. **Stateless** [BBH+15, GM11, MKAA17, NTY12, VDO14, BBPD16, DCAT12].  
**Stateless**/**Stateful** [NTY12]. statement [NIS13]. **Static** [DKMR15, IF16, Lan11, TLM13].  
**Stationary** [ZLDD12]. **Statistical** [B¨oh10, Bro11, DBPS12, HZ11, Hey17, LTKP16, OOR+14, SP13, Sim15a, GMT+12, SA19]. **Statistical-Attack** [SP13]. Statistics [gWpNyY+14].  
**Statutory** [PH12b].  
**Stealing** [RZW12, VWC19].  
**Stealthy** [BRPB13].  
**Steering** [HR13]. **Steganalysis** [B¨oh10, DA12, Fri12, JHHN12, KD12b, LJK17, LC15, SGP+12, Tan12a, YLL+12, Y14, YPRI17, BS11, LHM13, LSQ11a, LSQ11b, Sch12a]. **Steganalysis-Resistant** [YPRI17]. **Steganalytic** [Ber18, YPRI17]. **Steganographic** [DA10, HHS+15, LyWIZZ12, WP15, AGLW16, LLC10, CAC14]. **Steganography** [AAA+19, AGW15, BCG12a, CLF11, FR16, FMS12b, Fri10a, Fri12, HZW+14, Joh10, KTM19, LJK17, LLY+12b, MAL10, PDMR12, Pau10, SK12a, SJ19, TJZF12, WWL+14, WYL18, WYWZ12, YWW10, ZSA12, AOT13, BS11, BHKdFR12, EEAZ13, GKCK11, KKK+18b, LyWSZ10, LRW13, LRW17, LWW+10, Maz13, MSM+18b, MS17, PHN+12, PMG19a, SAM+19b, SI12, ST15, Sun16, WKK11, WOLS12, ZMS14]. **StegNet** [WYL18]. **Stego** [YLL+12, SMSK18]. **Stego-Image** [YLL+12]. **Stemmen** [BL10]. **Step** [AKY13, YXA+18]. **Steps** [Ano13c].  
**Stereotypes** [S¨od13]. **Stern** [ACD18].  
**STES** [CMLS15]. **Steven** [Ano16a, Led16, Sch15a]. **Still** [RAZS15, UK18]. **Stochastic** [ADR18]. stolen [Bha16]. **Stopping** [Sav13a].  
**StopWatch** [LGR14]. **Storage** [BCQ+13, CWL16, CCT+14, CLW16, CDLW19, DK+19, GLG12, HSM14, HLC+18, JSCM17, K¨up15, LCK11, LMD16, LWCJ14, LCDP15, PBC+17, QLL17, SKH17, WHL17, XNK15, YZDZ19, YJSL18, ZDL12, ZVG16, AY14a, AKK+17, BP10, CFVP16, CFZ+10, CLH+16, CD+10, CDL18, ED19, FH13, FNWL18, GLB+18, HSM13, LBOX12, SLL+19, Sar10a, SY+17, SWW+16, SWW+17, WS13, XWK+17, YXLYML19, YYS+16, YZCT17, YJC18, ZYC+17, ZVH14]. store [KV19b]. **Stored** [CMLS15, RSN14]. Stores [BCK17, GYW+19]. stories [SM15b, ZMYB17]. **Storing** [DLWW11, HK19, LCZ17]. storm [ACM12]. **Story** [Cer14, Keb15, Tur18, Ald11, Fag17, Gre17,
HPC10, KMY18, KSD+17, LGM+16,
MR14b, MSM18a, MSI10, MKK17, NDR+19,
NV10, OFMR16, OMNER19, PGLCX17,
PWS19a, SKH17, SSP19, TRD11, TS16b,
VV18, AAZ+16, ABB+14, ADH17, BM13,
BGG+13, BEB+18, FMA+18, HKA19,
HHT3, HAGTaFR13, KJN+16, KAS15,
LK10, MMR19, MA17b, Maz13, MHV15,
NR11, PPA18, THT16, TKG+17, VBC+15,
WWW17]. Survival [YCM+13, MMS+17a].
Surviving [CFST17], suspect [der10].
sustainability [KP18]. SVC
[MU12, WDDW12, ZLDD12, ZLDD14].
SVD [AM19, FYD+19, LP12, TB18,
ZWW17, ZW17a, ZW17b]. SVM
[TLL13]. swarm [ZSMS18]. Swarms
[VGOB18]. SWIFT [PLCGS11]. Switching
[CNT12, GHPS12, GHPS13, WB12,
YW12]. Sybil [AQRH+18, dCCSM+12].
Symbil-precaution [AQRH+18]. Sylvester
[SS10b]. Symbol [CS10]. Symbolic
[BCEO19, BCEO20, Bu18, CBRZ19, Wat10].
Symmetric
[BPR14a, BPR14b, BDPS12, CVM14, FPS12,
GF8B12, JCHS16, KTT12, Kha10, MM17b,
PR12, PCY+17, TWZ11, WRP70, YKNS12,
BGG+13, CGKO11, DLZ16a, FH13,
GMRT+15, GMdFPLC17, Gor10, GCVR17,
HK19, KAS15, LCZ17, SSK10, ZCZ+19].
Symmetric-Key [CVM14, KTT12],
symmetrical [RS17c]. Symmetry [SG14].
Symposium [ACMI10, ACM11, Anol10a,
IEE10, IE11b, IEE13, IEE15, MSH+16,
TB19, TT18, Wat10, Anol11a]. symptom
[YWL+18]. symptom-matching [YWL+18].
SYN [DHT+19]. Synchronization
[BL12, VTY18, WXY+17, yWXYZ+18,
AATM18, WDG19, XNG+14].
Synchronized
[DM18, PRGBSAC19, ACM12].
Synchronizing [HZ11]. SYND [MHC12].
Syndicate [HM19]. Syndromes [BBC+13].
Synergy [KFB12]. Synergy-Based
[KFB12]. Synopses [RCBK19]. Synthesis
[SKE+18, TCMLN19, RS17c]. Syst
[HYS18, WZM12a]. System [AD11, Alz19,
Anol10a, BCA19, BD18, CZLC12a, CZLC14,
Cor14b, CRST15, DDE+19, DG15, GOPB12,
Har16, HHS+15, HZS+19, IAD10, JN12,
JLZ18, JWJ+17, Jia10, KMP+11, KZZ17,
LYX+19, LFX+18, LSY+16, LHW18, Lop12,
MMSB19, MLBL12, NNS14, PSSK19,
QLL17, RSCX18, SMSK18, SRAA17, SL11,
ZV19+16, YE12, YXZ+12, YKK18, ZMM17,
ZPW16, ZLDC15, ZV16, AHN+18,
ARG19, BC18, BGG+13, Bu10a, CH11,
CCT1, CZ14, CS11, FLX+16b, FNWL18,
GKCK11, GH15, HHBS18, HKW+15,
HJM+11, HLYS14, JCI3, KGP+19, LLLK10,
LLL+17b, LHH+18, Lit14, LTC+15a,
LLL+18, LZX19, MS12a, MNW15,
PSOMPL13, SSSL+13, VSB+19, WMX+17,
WJD19, WGZ+12, XWW16, XYL19,
Y18+18, YW18+18, ZCZ19, ZYCT17,
ZMM+10, ZML17, ZZ18+18, KKA14, Dew11].
System-Level [BBCL19, JWJ+17].
System-on-Chip [HZS+19]. Systematic
[CCT+16, CBL13, PC16, IAA+19]. Systems
[AMSP19, AN12, AE18, AB15, Anol19a,
BL15, BL16, BS13b, BCTPL16, BB10, CZ19,
CWL16, CCF17, CRE+12, DL2+16b, GH12,
HXC+11, HCL+14, HLN+10, HK18, KS18a,
KLL+19, LYY18a, LMD16, LM10, LY16,
LNZ+13, MT17, MR14b, MJS+19, OS12,
PGLCX17, PMG19b, PRSV17, PH16,
Q1L+16b, RST15a, RST15b, SBS+12,
SBS18, SSKL16, SKFR15, Se16, SHK17,
SG14, SDM+12, STC11, SPP19, TKR14,
YN12a, AT10, AT110, BK19, BG18,
BL19+16, CF16V, CFZ+10, CLZ+17, Cla18,
dCCSM+12, dCCSB+16, CHG11, CVG+13,
CDA14, DEL19, DZS+12, Eis10, FXP12,
GMOGCCC15, GH19, GSN+16,
GPVCdBR12, HZW18, JSK+16, JHH14,
K14, LCL+15, LWK+18, MDHM18,
MLMSMG12, MGP10, MFH13, NLYZ12,
QMC17, SS10a, SR10, SRB+12, SMS+16,
Systems-on-Chip [KS18a]. Systolic [MCDB12]. Systolic-Array [MCDB12].

SZK [MX13].


Thanks [CBL10]. Theft [Ber12, Ber17, BTPLST15, ZMYB17]. Their [CZLC12b, CK18, FVJ19, HR19, JS18b, JSK+17, NR12, ZYY19, CQX18, FLYL16a, Hof16, IK15, KK10, Mat19, Sti11]. them [HLV10, JSK+16, Nor17, Rus15].
Theological [SS10c]. Theory [Lau12, HF14a]. Theorem-based [Lau12].
Theorem [Lau12, HF14a]. Theoretically [ADH19, CVM14, MAL10, WSS12, CDGC12, GLM+19, SD10, SKEG14].
theoretical [KL13, ZZ15, Gas13]. Theoretically [TWZ11, DGL19].
Theory [ACM10, ACM11, AAUC18, CCKM16, CDFZ16, CDFS10, Cra12, FGM10, FBMI2, FS15, Gre19b, Res12, LW1a, Lin14b, Nac12, Per13, PJ12, RZ19, RBHP15, RST15a, RST15b, Sah13, SAKM16, Sha10, Shp03, Wes16, Yan10, Abe10, AB10b, Bull0b, CFR11, Gill10, LPZJ15, MZA+13, McG11, YTM+14, Cra12, Lin14b, Sah13, vDKS11].
theory-based [LPZJ15].

There [Cer15, NSP+18, McK10, McK11, SM13]. Thin [Chi16, JLX+19]. things [FQZF18, AAC+16, AKS19, BCHL19, Bel18b, CLF+17, CCMB19, FREP17, FMA+19, GMDR19, HKA+18, Ham19, HZL18, JKAU19, KHMRG19, LNK+18b, LW19, LGO+17, NLLJ12, NLY15, PLGMCD18, SB17, SXX+19, SSS9, SYV+19, WVC19, WCC18, XLC+19, YCT15, ZDZH18, ZSY19]. Third [jCPB+12, OSH16, QZL+16b, Sen10, BL10, ED19, Kip13]. Third-Party [OSH16, QZL+16b]. Third-Round [jCPB+12].

Three [AP13, Thomas [Gre19a]. thou [BDK11]. Threat [CSY18, ALL+18, Ven14, ZMYB17]. Threats [AJA16, ERLM16, GSC17, LJS+14, vdG17, TKG+17]. Three [AMSL19, Cz15a, HXC+11, LLY+18, LZX+12b, OSANAM19, PC16, Shi11, YKNS12, AIB+16, CNF+18, HWB10, IC17, JKL+16, LNK+18a, LNK+18b, LML+13, Tso13, TKH14, XCL13, YC12, YZZ+14].

Three-Dimensional [LLY+18, LZX+12b]. Three-Factor [AMSL19, HXC+11, AIB+16, IC17, JKL+16, LNK+18a, LNK+18b].
three-party [HW10, LML+13, Tso13, TKH14, XCL13, YC12, YZZ+14]. Threshold [CT11b, C111, FGM10, GLW13, HEP+11, HYS11, LWL10b, LYY+16, SSU12, Sta12, Tan11, WYC14, WLH15, XLQ09, YFF12, YHK+10, YLA+13, ZCL+12, DZ14, FGMP12, HF14a, HH15, JS16, LJJ16, O010, QD16, SES+16, Sh15, SG16, TD14, ZJ+14, ZPY12].

 tickets [LMJC11]. tied [Men13b]. Tiered [GGK18]. Ties [PYM+15]. Tight [GDCC16, LPS12, LH18, ZH+19]. Tightly [HL18]. Time [AEP18, ASB17, ANO17d, APP14, AYS15, BBC19, BJ16, Che17, EKOS19, FD11, GSC17, HC17, HGT15, IF16, J1W+17, JEA+15, KME+12, LCL+17a, LF+18, MWES19, NA10a, Nov10, PNRC17, Raz19, RHLK18, Ste15b, WLZ12, YE12, AY14a, An15d, BM15, CC14, CAT12, FHH10a, GPLZ13, GMDFPLC17, HU15, LW10, LW13b, LML+13, MK11, NSX+18, Par18, SP17, WD19, XLC+19, An16].


Timed [Jia14b, KFOS12, Tan15a, Unr15, WSS12]. Timed-Ephemerizer [Tan15a].

Timed-Release [KFD12, Unr15, WSS12]. Timing [BGN17, FY+19, GV14b, Hay13, LGR14, LFK19, VCD16, YDV19, AKM+15, AGH+17, MCL+19, SRB+12]. Tiny [ZOC10]. Titan [PP10b]. Titan-R [PP10b].

TLS [AV18, AP13, BD+17, BFCZ12, BZD+16b, BJ+14, CFN+14, Dav11].

TLS-based [PP11]. TMDTO [SS+18].
Validations [PDJ+19]. Validity [BCF16].

valueable [Ana14]. Value

[GYW+19, LSL12b, SZHY19, YWW10, BWA13, KV19b, Svo14]. valued

[BNA15, TMMK11]. VANET

[PZBF18, WLZ+16, Wu17]. VANETs

[BMM12, CGCGPDMG12, CST+17, IOV+18, LLLG15, MGB19, YMM13].

Variability [VDB+16, SHBC19]. Variable

[CHHW12, CMMS17, XNP+18, DTZZ12]. variable-interval [DTZZ12]. Variables

[BB10]. Variant

[AAC1+14, MVVR12, ZKX18]. Variants

[ASS15, BB10, HLC+19, Hin10]. Variation

[DWZ12]. Variations [DSB16, SJZG19].

Varied [GZ12]. varieties [LR15]. Varying

[GCX11, BCDN17].

Validating

[zvR15, BB10, HLC+19, Hin10]. Validation

[SC19b, RST15a, RST15b, VSR12, GKC11, BCDN17].

[ACZ16]. VBT

[WL19]. VDTNs

[PSS+13].

Vector

[ACZ16, FHD19, HMK14, JHHN12, Kav15, RS17a, WK18, Zaj19, ZYT13, ZM16, DWZ12, LLM+19, PWW10, TTL10, ZZ15].

vector-form [DWZ12]. Vectorial

[DFQL12, FY11]. vectorized [DGK18].

Vectors [XLP+18]. Vegas [IEE10]. vehicle [WXSH19]. vehicle-to-vehicle [WXSH19].

Vehicles [LSY+16]. Vehicular

[HLKL15, ZHW+16, BBB19, KM10b, SGGCR+16, WXSH19].

[Vein [KLY+12].

Velskii [BB16b].

Ventilated [RSCX18].

Vera [Ayu12]. Verifiability

[FKOS19, RST15a, RST15b, VSR12, WWHL12, YMC+17, BRR+15, Hwa11].

Verifiable [CFE16, CRST15, Fuc11, HYS11, HLC12, HLC+18, KZZ17, LWW+19, LLL+18, NJB19, QD16, RDZ+16, RS17b, SQX+17, XWL16, YNR12a, YCR16, GLM+19, LZY+16, LJW+17, MGB19, NNP+13, PHGR16, QSI8, XWS17, ZZ15].

verifiably [SEXY18, ZLY10]. Verification

[AV18, App15, ABR12, BCEO19, BCEO20, BL15, BL16, CCK12, CCK16, CM11, EWS14, ESS17, GLLSN12, DGM16, GMSV14,
HZS$^{+19}$, Lin15, MT17, MV16a, OŠ12, PNRC17, RSR$^{+19}$, SOF12, TSB18, Tom16, Vet10, ZPW16, AGHP14, ABF$^{+14}$, ASVE13, BK19, BFG$^{+14}$, BJ10a, BT15, GPN$^{+12}$, HFCR13, KKK$^{+16}$, LEW19, MR14c, NPH$^{+14}$, SD10, XHM14, YNX$^{+16}$.

Verified [BFCZ12, YGS$^{+17}$, HKA$^{+18}$].

verifier [DGJN14, HYWS11, WHJ17].

verifiers [AYSZ14]. Verify [BCK17, KRH18, SKGY14, KNTU13, SWW$^{+16}$].

Verifying [AD12, BFK16, GZSW19].

Verlag [Mei10].

Version [BCP14a, Faa19, K¨O14, DXWD16, ZDW$^{+16}$].

Versions [LWPF12, PS12].

Versus DDR$^{+16}$, NNA10, ABJ13, Svo14].

Very [BFM12, SBM15, YT16, Jou13, Kum10].

Via [ADR18, BSCTV17, ABC$^{+18}$, AHG18, BHKN13, BCI$^{+13}$, BCG19, BR14, Bu18, CBZ19, CDSLY14, CFG$^{+17}$, CLW16, DM19, GT12, GST13, GVW12, Gre19b, HFW$^{+19}$, JHW$^{+19}$, KKK$^{+18a}$, LT13, LT14b, LFI18, LH14, LEW19, LLKA19, MH14, Mor19b, PV17, PTK14, QZDJ16, RS10, SE16, SSAF11, SKEG14, TBCB15, WSS$^{+19}$, tWinC12, YWF18, Yon11, ZOC10, ZCZQ19, Zim10].

Vice [LMS10].

Vichy [Kap11].

Vicious [NN15]. victory [Pea11].

Video [BWR12a, BSA$^{+19}$, DG17, GKB17, JSSZ12, OŠ12, TWZ$^{+12}$, WLZL12, YE12, YT12, YTF$^{+18}$, Cri16, LLHS13, MK11, OCDG11, PMG19a, XWZW16].

Video-based [YTF$^{+18}$]. Videos [AAA$^{+19}$, GZH17, JSCM17].

Vietnam [ABJ13]. View [RS16, TWZ$^{+12}$, YCM$^{+13}$, ZGC16, CWZL13]. View-Invariant [RS16].

Viewpoint [BMDT19]. Views [VGA15, TG12].

Virtual [BCKP17, BR14, Cou12a, HB17, LBC18, RY10, VDO14, CDA14]. Virtualization [CDD13, RC18, QZDJ16].

Virtualization-Based [CDD13, QZDJ16].

Virus [WOLP15]. visibility [FG19].

Visible [Cas10, HWYW14, LZX$^{+12b}$, PK19, WZWL13, Lin14a].

Vision [BSW12, LWW$^{+10}$]. Vista [FG19]. Visual [BNA15, CSW12, GLW12, HHS$^{+15}$, KU14, KS15, Lal14, LPL15, LWL10b, LGWY12, LMHH14, LTC$^{+15b}$, OTO18, SA16a, SC10, Shy15, TWNC18, WY12, Yan12, ZXX$^{+11}$, CT11b, CSTR16, DDD14, DD13, GJJ18, GLW13, HT11, LWL10a, MSM$^{+18b}$, WYK12, WS12, YSC16, YR11].

Visualizing [Sav15]. VLSI [KB10]. VMOR [MSI18].

Vocal [LCR$^{+18}$].

Voice [JTZ$^{+16}$, LCR$^{+18}$, WBC$^{+10}$, LFCCGCRP14, TJZF12]. Voice-over-IP [TJZF12]. VoIP [BGAD12, Cla18, Maz13, SS10a, VGL14, ZTZ16].

VoIP/IMS [VGL14].

Volatile [AMH$^{+16}$, JSA17, RM18, SM18, XZL$^{+19}$, YNQ15, CS11].

Voltage [BBBP13].

VoltKey [LKBK19]. volume [WLDB11].

voluntary [WGJ10]. Voting [Ber16b, CF16, CRST15, CEL$^{+19}$, KV18, LHF12, LGPRH14, RST15a, RST15b, Sch10, KZZ17].

Voybach [Ano16c, Bax14].

VPCLMULQDQ [DGK18]. VPMADD [KG19].

VQAP [TWNC18]. VR [WSS$^{+19}$].

vs [Bur11, FOKV15, Mar10b].

Vulnerabilities [BKJP12, HSUS11, MAS16, PDT12, RY10].

Vulnerability [MKN13, TM12, VKC15, Wal18, Ano17f, DMWS12, MYYR13].

Vulnerable [Ano15d].

Vote [CRST15].

W [Mar10a, Xie12a, Xie12b, Hiil13].

W-OTS [Hiil13]. WA [LCK11].

Waknaghat [CGB$^{+10}$]. Walker [Xie12a, Xie12b].

Wallets [Chi13b].

Wallis [Wes16].

Wan [RSD19]. wants [Nor17].

War [Has16, Mun17, Bud16, Car11, Sni11a].

Warbler [MFG16].

Warm [MCL$^{+19}$].

warriors [Bud16].

wartime [McK10, McK11].

Was [Tur18, Goo12, LHA$^{+12b}$].

Watching [NSP$^{+18}$].

Watermark [CHHW12, DLMM$^{+18}$, EMW14, FR15, GRRZ18, Jia10, KBL11, LZX$^{+12b}$, MCD12, QJC$^{+18}$, SJ12, YE12, ZS12, HB13, TLL13, WYL13].
Watermark-Based [GRRZ18].
Watermark-Driven [DLM+18].
Watermarking [AAA+19, BCGAPM12, BF12, BCPZV11, BDB14, BCG10, BMBM15, CG12b, CHHW12, CCZC13, CHN+18, DG17, FM15, Fra15, Fra16, GKS17, GP17, HPC10, HEK18, HD19, HGT15, HHMK14, JSZS12, Jh10, JKH12, KD12a, LSL12b, LLY+18, LP12, LD13, MM17a, MR16, MU12, NGAnH16, NC12, NXH+17, pNyWyY+14, OWHS12, RS16, RP12, RR11, RMI18, SAA15, SGLZ12, SS17b, SSA13, TB18, TWZ+12, TC10, WHZ12, WLZL12, WYW+13, ywpNyY+14, XL+17, yWXY+18, WK18, tWmC12, XNG+14, XNRG15, XNP+18, YWNW15, YPR17, YKK18, YYO15, ZX+11, ZWW17, ZWZ17a, ZWZ17b, AP10, AIA+18a, AIA+18b, AIM+19, AM19, AMK12, BWR12b, BW13, BWA13, CCLL11, CT11a, CSS+13, GZHD12, GA11, HAK19, HKA+18, HURU11, HKB14, HWYW14, HPL+19, JK13, KMG17, KPS10, KJN+16, KM11, LSR13, LXC11, LLHS12, Lin14a, EYW12, MMS13, MM14a, MO14, MK11, NC13], Watermarking [PTK14, PWW13, PWW10, PGL10, P KS18, PC14, PPR+12, RS17c, SKS+18, Tay14, Tk14, TTL10, TPKT12, WLD11, ywpNyL11, Wan13, ywpWyNy13, WZ18, WYT+12, ZK17, ZMS+18].
Watermarking-Encryption [SLGZ12].
Watermarks [GL10, YT12].
Wave [BMM12].
Wave-Enabled [BMM12].
Wavelet [AGW15, KTM19, LSL12b, MR16, Ara13, AMK12, BW13, LXM11, MO14, ST15, ywpNyL11].
Wavelet-Domain [MR16].
Waves [MMS13].
Way [BHT18, CBXJ19, CPS16, DSS14, Mat14, WAXZ17, HRV10, Kom18, LP11, LM14, RK11, SCBL16].
Ways [MSL13].
WBAN [KS18b, XX19].
WBANs [KIH19, OSP+19].
Weak [BF11, DY13, HGH16, HDWH12, HLC+19, PYM+15, Pud12, BH19, GJMP15, RH10].
Weakening [SFRK15].
Weaker [Sas12, Wang18b].
Weakness [AMORH13].
Weaknesses [BFS11, BSS14].
Weapon [Zet14].
Wear [LY15].
Wear-Leveling [LY15].
Wearable [ASV+18, ATC17, BCTPL16, DM19, GWP+19, LCR+18, SS19, XJR+17, GTSS19, LK+17].
Wearout [DFKC17].
WEB [GP+12, IMB17, KRM+10, KGO10, MWW+18, YYY+19, ATKH+17, BS12, BKJP12, CLB19, CTC+15, CFST17, CD12, DR11, Fra16, HSC19, HGOZ19, HCM11, HVP+18, NDS17, QF19, SP15a, SP+13, ZGC16].
Web-Based [CD12].
web-content [GP+12].
WebCallerID [HCM11].
Website [Boy16].
Websites [RS11].
Webster [Pea11].
WEBSCR [DDS12].
Web [SB+12].
Weierstrass [LL11].
Weight [SWF+19, QSi11].
Weighted [YLL+12, YTH17].
Welshman [GW14].
Well [JCM12], were [McK10, McK11].
Western [Han12].
WG [GLIC10, DJG+15, ERRM15, ZAG19].
WG- [ERRM15].
WG-16 [ZAG19].
Where [CMG+18].
Wherefore [BDK11].
whether [Bar19].
while [Nor17].
Whit [LHA+12b].
White [BW16, BCGN16, LYL+18, Mic10b, SWF+19, DD13, YSC16, ZSW+18a].
White-Box [BW16, BCGN16, LYL+18, Mic10b, SWF+19, ZSW+18a].
Whitfield [Hof16].
who [Bat10, Bha16, Car11, Fag17, GSGM16, Hea15, Kap13, McK10, McK11, McK12, Moo14, XTK10].
wi [BMDT19].
wi-fi [BMDT19].
Wicked [SGH15].
Widespread [HDDH14, HFD16].
width [Kre13].
width- [Kre13].
Wiener [Kuz11].
Wigner [TC10].
Wild [ASV+18, HREJ14].
Wildcard [HI16].
Wildcards [DA18].
Wilderness [Acz11].
Will [Mos18, Dya19, Fal19, Nor17, Pec17].
win [Sm11a].
Window [TX16, Kh18, Win17, YWYZ12].
windows
Wine [Che17]. Wineskin
[Che17]. Wins [Ano16]. Wire
[ADG16, ZZC14]. Wire-tap [ADG16]. Wireless
[ABC+17, BN14, BOB13, BCG10, CB0+18, CKHP19, CS14, DPCM16, DS11, FLH13, HZC+12, HBCC13, KH10, LLC11, LHM+15, LZCK14, LWCJ14, LLZ+12, NNAM10, PSM+18, PCPK14, RCW15, RSD19, RWLL14, SWYP12, SP15b, TCN+17, YM16, ZLDD12, APK+18, AIB+16, AIKC18, ADF12, BNNH19, BLAN+16, BEB+18, BBB16b, CDGC12, CML+18, CLSW12, CL11, DSCS12, HKA+18, HGWW11, HZC+14, HZWW17, HCC11, HTC+10, HLYS14, JNUH17, JMW+16, KP18, KO16, KIW+16, KDW+17, LCAJ11, LNNH13, LIK+17, LMK+18b, LZZ+19b, NDRN13, PL16, PY19, QMW17, RR17, SA12, SGJ+14, SSMK13, SM19b, SCKH10, SKK10, TKHK14, Wan13, WW14, WMC17, WXK+17, XHCH14, XMHD13, YHHS16, ZYG17, ZYG18, ZBR11, ZC11, ZC11, ZH14+17. Wireless-Charging-Based
[CKHP19]. wiretap [BCDN17]. Wiretapping
[Lan10]. Wiring [HTZR12]. Wise
[CG14a, SSA13]. WISP
[PPH12]. Withholding
[BRS17]. within
[HSC19, KLN15]. Without
[ASS15, CCL+13, FZT14, GSW+16, GKS17, LTC+15b, NA10a, XLQ09, YLA+13, ARM15a, AZH11, BT12, BF11, BGV14, CCW+10, CJL16, CCG+17, DCA18, FSX12a, GH11a, GST12, GLM+16, HDPC13, ISC+16, KZS17, LYY15, LGWW12, Par18, RG10, SYL13, SLZ12, TAKS10, WWWW11, XQL11, XHM14, YS12, XKC+11, YFK+12, ZY17b, ZYM18]. Witness
[CXWT19, GGH17]. Witness-based
[CXWT19]. WLAN
[KAHK17]. woman
[Fag17]. Women
[Abb12, Hea15, Mck10, Mck11, McK12, Mun17]. Word
[WW12, SCR19b]. Word-independent
[SCR19b]. Word-Oriented
[WW12]. Word
[WW12, SCR19b]. Word-independent
[SCR19b]. Word-Oriented
[WW12]. Work
[WW12, SCR19b]. Word-independent
[SCR19b]. Word-Oriented
[WW12]. Work
Correlation [BW12, YCL17, WWBC14].
Zero-Knowledge [CLP13a, GOS12, IW14, MX13, MBC+18, MT12, Pan14, LLM+19, KPP16, MDHM18].
Zero-Watermark [SJ12, TLL13]. zero-watermarking [AIA+18a, AIA+18b].
Zynq [ZAAB17].

References

Akyildiz:2014:OTB


Applebaum:2017:AC


Abouaroek:2019:NAU


Abo-alian:2016:KDB

Ambrosin:2016:FAB


Albertini:2014:MHE


Ahmad:2019:PQE


Akdogan:2019:SKA


Arora:2012:ILM

REFERENCES

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

**Al-Azzam:2018:SRC**

**Akleylek:2016:SPM**

**Aghili:2018:ISA**

**Acar:2018:SHE**

**Alizadeh:2016:AMC**

**Abdalla:2010:PCL**
Michel Abdalla and Paulo S. L. M. Barreto, editors. *Progress in cryptology — Latincrypt 2010: first international conference on cryptology and in—

Atallah:2010:ATC


Anand:2015:ICL


Alwen:2017:TPA


Abbate:2012:RGWa


Alleaume:2014:UQK


Athmani:2019:EED


[ABB19a]

Avoine:2019:SDB


Almeida:2013:CCA


Arnold:2012:ICC

REFERENCES

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

**Ateniese:2017:LCS**


**Adrian:2015:IFS**


**Adrian:2019:IFS**


**Ambrosin:2017:OBB**


**Agrawal:2018:RLR**


[ABF+14] José Bacelar Almeida, Manuel Barbosa, Jean-Christophe Filliâtre, Jorge Sousa Pinto, and Bárbara Vieira. CAOVerif: an open-source deductive verifica-


[ABL+18] David W. Archer, Dan Bogdanov, Yehuda Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart, and Rebecca N. Wright. From


REFERENCES


Atighehchi:2015:NME


AlMashrafi:2012:AIM


Aldaya:2019:MTA


Applebaum:2010:PKC


Alzubi:2016:SCC


Arias-Cabarcos:2015:BIP

Patricia Arias-Cabarcos, Florina Almenarez, Ruben

**Armando:2013:AFB**


**Arnold:2015:NGH**


**Anastasiadis:2018:BTA**


**Amoah:2016:FMA**


**Ardagna:2010:ECP**

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

**Arias-Cabarcos:2019:SAA**


**ACM:2010:PAI**


**Avoine:2012:PFS**


**Austrin:2017:ICT**


**Aceto:2019:MME**

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

**Aczel:2011:SWL**


**Alvarez-Cubero:2016:AVL**


**Aizatulin:2012:VCC**


**Anyanwu:2010:DCS**


**Ayday:2012:DAA**


**Aliberti:2016:RPS**

Giulio Aliberti, Roberto Di Pietro, and Stefano Guarino. Reliable and perfectly secret communication over the generalized Ozarow–

**Attasena:2017:SSC**

**Abraham:2019:DPL**

**Adikari:2011:HBT**

**Abdalla:2012:LBH**

**Abro:2019:LEE**

**Andrychowicz:2016:SMC**
Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek. Secure multiparty computations on Bitcoin. *Communications of

Araldo:2018:CEC


Anandakumar:2018:RHA


Ahmed:2017:IRD


Attrapadung:2015:RGS


Aminifar:2018:OME

REFERENCES

Aumasson:2017:SCP


Atighehchi:2019:GHC


Antonopoulos:2017:DIS


Akinneye:2014:MGA


Abdullaziz:2016:AAI


Ahani:2015:SRB

Allender:2019:NIN

Ahmadzadeh:2018:HPE

Attrapadung:2012:ABE

Ali:2018:ECM

Akhtar:2018:BSI

Appelbaum:2013:SSG
J. Appelbaum, J. Horchert,

**Ak:2014:ICS**


**Au:2020:SIC**


**Ali:2018:CBR**


**Ali:2018:ZWA**

REFERENCES


Alhanahnah:2016:MTI


Alam:2018:AFC


Ashraf:2014:MTG


Azarderakhsh:2014:NDP


Almulla:2013:CKE


Anada:2017:CGS

REFERENCES

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

**Alabdulatif:2017:PPA**


**Afanasyev:2011:PPN**


**Andrysco:2015:SFP**


**Armknecht:2012:STH**


**Arfaoui:2019:CAA**

REFERENCES

www.sciencedirect.com/science/article/pii/S1389128619300465


REFERENCES

Asharov:2013:FCF

Alzahrani:2019:SAC

Araghi:2019:EHI

Awad:2016:SSZ

Arnedo-Moreno:2010:JRA


REFERENCES

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


[AN15] Hamed Arshad and Morteza Nikooghadam. Security analysis and improvement of two authentication and

Aga:2017:ISM


Aga:2017:ISM


Anderson:2013:MNF


Anderson:2019:QCN


Anghelescu:2016:FIP

REFERENCES


[Ano11c]

Anonymous:2011:MCB


[Ano12]

Anonymous:2012:SHS


[Ano13a]

Anonymous:2013:CFF


Anonymous:2014:TPC


Anonymous:2015:BSU


Anonymous:2015:BRDa


Anonymous:2015:CEB


Anonymous:2015:QCS


Anonymous:2015:UGB

Anonymous:2016:BRBa


Anonymous:2016:CPSd


Anonymous:2016:CPSe


Anonymous:2016:EMT


Anonymous:2016:FVM


Anonymous:2016:GUP

Anonymous:2016:IICd


Anonymous:2016:MBE


Anonymous:2016:SWT


Anonymous:2016:SIR


Anonymous:2017:BA

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

Anonymous:2017:BRM


Anonymous:2017:CCS

1024 bits) primes \( p \) and \( q \) that led to crackable RSA cryptography. The solution for Estonia was to switch to elliptic-curve cryptography that was also supported by the cards.

Anonymous:2017:HDQ


Anonymous:2017:MBH


Anonymous:2017:RV


Anonymous:2019:GES


Anonymous:2019:HCC

REFERENCES

Anonymous:2019:PBT


Anthes:2014:FTI


Andriotis:2013:JSD


Agarwal:2010:BRW


Aumasson:2011:CHF


AlFardan:2013:LTB


Abellan:2018:FCQ

REFERENCES

Ali:2018:SUA


Alcaide:2013:AAP


Applebaum:2013:GXG


Applebaum:2014:CCP


Appel:2015:VCP


Albrecht:2015:FBR

Al-Qarni:2012:EII


Al-Qurishi:2018:EKA


Arai:2013:MDH


Arab:2019:IEM


Adj:2014:SRC


Ambrose:2012:RII

Alghamdi:2019:RAM

Artemenko:2017:PGO

Andrade:2016:LEP

Asharov:2016:LPI
REFERENCES


REFERENCES


Alsulaiman:2013:IVB


Altman:2010:AAP


Azimpourkivi:2017:CBT


Aste:2017:BTF


Argyropoulos:2010:BTP


Au:2011:PPT


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


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


REFERENCES

Bard:2019:DWG

Baylis:2010:CC

Bulygin:2010:OSS

Bennett:2014:QCP
Barenghi:2016:FBS

Boumerzoug:2016:LKM

Benyamina:2019:ANE

Barenghi:2013:FIT

Baldi:2013:ULC

Barak:2014:OEF
Boaz Barak, Nir Bitansky,
REFERENCES


Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. [BBEP14]
REFERENCES


Bernstein:2017:SRD


Boldi:2012:IUG


Bingol:2019:EPP


Bollman:2015:PWI


Behrad:2020:NSA


Bernstein:2011:PCI

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

Konstantinosonti:2017:KYE


Basin:2014:KYE

[BCC+19]


Bocu:2018:HEB


Balagurusamy:2019:CA

[BC14]


Bao:2016:LPP


Bichsel:2012:DMA

Patrik Bichsel, Jan Camenisch, Bart De Decker, Jorn Lapon, and Vincent Naessens. Data-minimizing authentication goes mobile.
REFERENCES


Boche:2017:CQA


Badrignans:2010:SSA


Balfanz:2012:FA


Bugliesi:2015:ART


Bana:2019:VMC


Bana:2020:VMC

Gergei Bana, Rohit Chadha, Ajay Kumar Eeralla, and Mitsuhiro Okada. Verifica-


[BCG12b] Julia Borghoff, Anne Can-

Blais:2019:DTL


Baelde:2012:TPR


Bahi:2011:ECS


Barthe:2012:CACa


Beunardeau:2016:WBC

REFERENCES

Boneh:2016:BHP


Belleville:2019:ASP


Batina:2019:ISI


Bitansky:2013:SNI


Brandenburger:2017:DTC


Bitansky:2017:VGB

[Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and...


Bicakci:2013:LSS


Botta:2014:PCI


Boyle:2014:EO


Basso:2011:BWC


Bessani:2013:DDS


Blasco:2016:SWB

REFERENCES


REFERENCES


REFERENCES


[BDM18]


[BDM+19]


[BDMN16]


[BDOZ11]


[Bertoni:2011:CSF]

Bertoni:2012:KIO


Boldyreva:2012:SSE


Bottarelli:2018:PCW


Beebe:2017:MFC

Nelson H. F. Beebe. The Mathematical-Function Computation Handbook: Pro-
gramming Using the MathCW Portable Software Library.

Bellovin:2015:WRC


Bellovin:2016:EEE


Bellovin:2018:UAE


Beltran:2018:IAA


Bellovin:2019:L1


Bajard:2016:MFA

REFERENCES

Berghel:2012:ITF


Bera:2014:QC


Berghel:2016:CKF


Berghel:2016:DJT


Berghel:2016:S


Berghel:2017:ELR


Berretti:2018:IAS


Bouman:2011:SAW

[NBF11] Nick J. Bouman and Serge Fehr. Secure authentication from a weak key, without leaking information. *Lecture Notes in
REFERENCES


References


Beimel:2012:SSS


Berger:2016:EGF


Boldyreva:2014:MEW


Battistello:2012:TBA


Barthe:2012:CACb


[BGJT13] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. Re-
port, Inria, CNRS, University of Lorraine; Foundation UPMC — LIP 6, CNRS UMR 7606; Crypto-Experts, Lorraine, France; Paris, France; Paris, France, November 25, 2013. 16 pp. URL http://eprint.iacr.org/2013/400.pdf.

Barbulescu:2014:HQP


Barthe:2012:ACA


Biswas:2017:STC


Borcea:2017:PEE


Brakerski:2014:LFH


Barkatullah:2015:GCF

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


Bhattacharjee:2016:SWC


Behnia:2012:SEI


Bernstein:2015:SPS

REFERENCES


Benhamouda:2019:SPD


Bosch:2014:SPS


Berman:2013:HPR


Berman:2018:CFC


Bonneau:2015:PEI


Biagioli:2012:CCS

Mario Biagioli. From ciphers to confidentiality: se-


REFERENCES

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

Bouraoui:2017:HAE


Bogdanov:2012:UTC


Benhamouda:2016:NFP


Brubaker:2014:UFA


Boldyreva:2012:NPG


Bouti:2012:SCB

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


REFERENCES


[BL15] Amir Jalaly Bidgoly and Behrouz Tork Ladani. Modelling and quantitative verification of reputation systems against malicious


[BLa16]

[Bernstein:2017:SCS]


[BLL19] Tong Bai, Jinzhao Lin, Guoquan Li, Huiqian Wang, Peng Ran, Zhangyong Li, Dan Li, Yu Pang, Wei Wu, and Gwanggil Jeon. A lightweight method of data encryp-


Special Issue: Alan Turing.
REFERENCES


REFERENCES

Bhattacharya:2018:UPC


Benamara:2016:ICA


Baldwin:2010:AFI


Bartoli:2019:VEW


Biswas:2012:IBA


Backes:2012:GCP


REFERENCES


REFERENCES


**Biryukov:2014:DEA**


**Ben-Othman:2013:IHN**


**Bohme:2010:ASS**


**Boneh:2012:PBC**


**Boneh:2019:ACK**

REFERENCES


REFERENCES

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

Bohli:2011:RAP


Budroni:2018:HGB


Bencsath:2012:CSD


Brooke:2010:DCX


Bellare:2014:SSEa


Bellare:2014:SSEb

REFERENCES


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


Briggs:2011:SDC


Broemeling:2011:AES


Brooks:2012:QCE


Brook:2017:LSR


Broumandnia:2019:MCM


Becker:2013:SDL

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

Benaloh:2015:EEV

REFERENCES


Bag:2017:BBW


Bellare:2012:MIS


Birrell:2013:FIM

Bhattacherjee:2014:CAT

Bagheri:2015:NNA

Bendiab:2019:FNF

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

**Boorghany:2015:CIL**

Ahmad Boorghany, Siavash B. Sarmadi, and Rasool Jalili.
ISSN 1539-9087 (print), 1558-3465 (electronic).

**Bojinov:2014:NMC**

Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln.

**Beaulieu:2013:SSF**

Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers.

**Batina:2012:HEB**

Lejla Batina, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede.
REFERENCES


References


Bhatnagar:2012:IVE


Bhatnagar:2012:NRA


Buhren:2019:IUP


Bai:2019:HAF


Bao:2010:ISC


Bo:2016:ETK

REFERENCES

(4):1083–1093, March 25, 2016. CODEN CCPEBO. ISSN 1532-0626 (print), [CAM19]
1532-0634 (electronic).

adversaries: practical forgery
attacks on GCM in TLS.
In 10th Usenix Workshop on Offensive Technolo-
gies, pages 1–11. USENIX, Berkeley, CA, USA, Au-
gust 2016. URL https://
www.usenix.org/conference/
woot16/workshop-program/
presentation/bock.

[CAC14] CACM Staff. Know
your steganographic en-
demy. Communications of
the Association for Com-
puting Machinery, 57(5):
8, May 2014. CODEN
CACMA2. ISSN 0001-0782
(print), 1557-7317 (elec-
tronic).

[Cal13] Tracey Caldwell. Identity
— the new perimeter. Net-
18, April 2013. CODEN
NTSCF5. ISSN 1353-4858
(print), 1872-9371 (elec-
tronic). URL http://
www.sciencedirect.com/
science/article/pii/S1353485813700515.

[CAS19] Nilesh Chakraborty, Vi-
jay S. Anand, and Sam-
rat Mondal. Towards iden-
tifying and preventing behav-
orial side channel at-
tack on recording attack
resilient unaided authenti-
cation services. Computers &
Security, 84(??):193–
205, July 2019. CODEN
CPSEDU. ISSN 0167-4048
(print), 1872-6208 (elec-
tronic). URL https://
www.sciencedirect.com/
science/article/pii/S0167404818302062.

[Car10] Frank Carter. The Turing
Bomb. Rutherford Jour-
nal, 3(??):??, ???? 2010.
CODEN ???? ISSN
1177-1380. URL http://
rutherfordjournal.org/
article030108.html.

[Car11] Elliot Carlson. Joe
Rochefort’s war: the
odyssey of the codebreaker
who outwitted Yamamoto
at Midway. Naval Institute
Press, Annapolis, MD, US,
2011. ISBN 1-61251-060-

[Cas10] Bill Casselman. Visible
cryptography. Notices of
the American Mathematical
Society, 57(3):378–379,
March 2010. CODEN
REFERENCES


[CBL13] William E. Cobb, Rusty O. Baldwin, and Eric D. Laspe. Leakage mapping: a systematic methodology for assessing the side-channel information leakage of cryptographic imple-

**Chang:2018:DMU**


**Chattopadhyay:2019:QIL**


**Chadin:2010:EKS**


**Chang:2014:RRT**


**Chen:2019:IAS**


**Chadha:2016:AVE**

Chretien:2015:SPP


Chretien:2019:TMF


Chretien:2020:TMF


Chen:2017:LAA


Carota:2012:FFI


Chou:2010:PSO

Checkoway:2016:SAJ


Chadha:2012:AVE


Chatterjee:2016:TAD


Chou:2013:UGS


Cao:2019:AML


Chang:2011:SFW

Chin-Chen Chang, Kuo-
REFERENCES


Cheng-Kang Chu, Sherman S. M. Chow, Wen-

Chen:2010:ALD


Chen:2013:WSB


Chiasson:2012:MWB


Canard:2016:HPP


Cui:2016:RDA

Criswell:2014:VGP


Cheng:2013:DVB


Ciriani:2010:CFE


Choo:2016:CCT


Cao:2012:ITM

REFERENCES


REFERENCES

[Culnane:2019:KKR]

[Ceruzzi:2014:HFT]

[Cerf:2015:CTN]

[Cerf:2018:CSA]

[Chang-Fong:2016:CSC]

[Crampton:2017:CEI]

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

Centenaro:2013:TBA


Checkoway:2014:PED


Cevallos:2012:USR


Carstensen:2011:AAA


Calzavara:2017:SWJ

Celesti:2016:ALT


Choo:2017:EDF


Chang:2010:PRN

Weiling Chang, Binxing Fang, Xiaochun Yun, Shupeng Wang, and Xiangzhan Yu. A pseudorandom number generator based on LZSS. In *2010 Data Compression Conference (DCC)*, page 524. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010.

Chen:2010:IFA


Camenisch:2012:EAA


Che:2012:WAM

REFERENCES

198

(print), 1744-5779 (electronic).

Cheraghchi:2014:NMC


Corrigan-Gibbs:2014:KS


Chaudhuri:2010:PIC


Caballero-Gil:2012:LAR


Chmiel:2012:EPC


Coull:2011:ACO

REFERENCES


中枢:2017:PSR


中枢:2011:SSE


中枢:2012:PAI


中枢:2014:PBC


中枢:2013:NIB


中枢:2010:NUP

Chang:2011:DEQ


Chang:2013:MPQ


Chappell:2013:PMI


Chen:2013:CCCC


Chen:2011:CCI


Cheswick:2013:RP


Chen:2015:SSS

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

Chen:2017:CSQ


Chen:2018:ESA


Courtois:2013:BRC


Cui:2019:CPA


Chen:2012:SRF


Chien:2012:IAM

Hung-Yu Chien. Improved anonymous multi-


\[\text{Cilardo:2011:EPT}\]


\[\text{Cheng:2013:EHM}\]


\[\text{Cao:2014:SCI}\]


\[\text{Cheon:2016:ANP}\]


\[\text{Cho:2012:CBF}\]


\[\text{Cho:2015:CBF}\]

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

**Choi:2019:PTE**


**Chang:2019:GTS**


**Cui:2013:OSL**


**Chandra:2011:AST**


**Chailloux:2017:PLQ**

REFERENCES


REFERENCES


Calegari:2019:WPH


Chen:2019:BBS


Comon-Lundh:2010:DSP


Chang:2011:RSB


Chen:2017:PGF


Chong:2013:ASG

REFERENCES


Jiahui Chen, Jie Ling, Jianting Ning, and Jintai


[Cui:2016:KAS]


[Chen:2014:CDP]

[CLY18] Kaidi Cao, Jing Liao, and Lu Yuan. CariGANs: unpaired photo-to-caricature translation. *ACM Trans-
Cozzens:2013:MEE

Cui:2014:SSA

Checkoway:2018:WDL
Stephen Checkoway, Jacob Maskievicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. Where did I leave my keys?: lessons from the Juniper Dual EC incident. *Communications of the Association for Computing Machinery*, 61(11):148–155,
Coles:2016:NAU


Chakraborty:2013:EHI


Chakraborty:2015:SSC


Chen:2017:VME

REFERENCES


REFERENCES

Chin:2011:ACS

Conitzer:2010:AP

Constantin:2012:RSN

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

Connolly:2018:FE

Copeland:2006:CSB
B. Jack Copeland, editor. Colossus: the secrets of Bletchley Park’s code-breaking computers. Oxford University Press, Walton Street, Oxford OX2...
REFERENCES

0-19-957814-1 (paperback).
xvi + 462 + 16 pp.
.colossus-computer.com/. [Copeland:2010:CBG]

B. Jack Copeland. Colossus: Breaking the German
‘Tunny’ code at Bletchley Park. An illustrated
CODEN ???: ISSN 1177-1380. URL http://
rutherfordjournal.org/article030109.html.

[Cor14a] Tim Cordova. Encrypted backup solution: Home
3:??, January 2014. CODEN LIJOFX. ISSN 1075-
3583 (print), 1938-3827 (electronic).

to decipher cryptographic system. Scientific Computing, August
www.scientificcomputing.com/news/2014/08/smartphones-
set-out-decipher-cryptographic-system. The article
describes use of thousands of mobile phones to attempt
a parallel brute-force attack on elliptic-curve and RSA algorithms,
in a research project by Ramasany Gowthami and Arjen Lenstra at the LACAL
laboratory at EPFL, Lausanne, Switzerland.

[Cour12a] Rachel Courtland. Vir-

[Cor14b] [COP+14] Kai-Min Chung, Rafail
Ostrovsky, Rafael Pass,
Muthuramakrishnan Venkitasubramaniam, and Ivan
Visconti. 4-round resettably-
sound zero knowledge.

**Coutinho:2012:**


**Claessen:2013:**


**Canard:2018:**


**Chung:2016:**


**Chen:2018:**


**Chevalier:2010:**

Chen:2012:DCC


Crampton:2011:PEC


Cramer:2012:TCT


Craver:2014:UCC


Clear:2012:CPA


Crichlow:2016:RSE


Chapin:2014:SRP


Chattaraj:2018:NTS


Chauhan:2018:BBA


Chadwick:2014:AFI


Chen:2013:RWM

Chen:2017:SIE


Ciegis:2016:ADP


Chong:2015:SID


Chow:2012:EPV


Chen:2018:SIA


Chen:2011:IBT

REFERENCES

Chen:2011:ARI


Chen:2011:TVS


Canard:2018:CPK


Calzavara:2015:SLA


Chang:2012:GBP


Chou:2013:TIB

REFERENCES


REFERENCES

Cao:2014:PPM

Chen:2012:IDC

Chen:2012:CKS

Chen:2016:WPM
REFERENCES

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

Chen:2019:MBR


Cao:2019:PPS


Chen:2014:MLC


Chen:2015:TCP


Chen:2019:WBS


Cao:2013:SIPa


Chen:2014:MLC


**Chen:2014:CSI**


**Dharwadkar:2010:SSG**


**Djebbar:2012:ASB**


**Darivandpour:2018:ESP**


**Danezis:2012:FCDb**

REFERENCES


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

**Cordeiro:2016:MPG**


**Cordeiro:2012:IMB**


**Ding:2018:NPH**


**DePrisco:2013:CVC**


**DArco:2014:MIC**

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


Dai:2019:SAM


DeOliveiraNunes:2019:SSC


derhans:2010:USC


Desmedt:2010:CF


Desmedt:2010:ES


Dew:2011:BRB

Nicholas Dew. Book review: *The Information*
REFERENCES


Durmuth:2011:DEN


DuPont:2016:ECC


DeCapitaniDiVimercati:2010:EPR


DeCapitaniDiVimercati:2017:AMM


Deng:2017:LLH


Ding:2012:CLS

Lin Ding and Jie Guan. Cryptanalysis of Loiss stream cipher. The
Djuric:2015:FSF

Dutta:2017:EFC

Dickens:2018:SCI

Dupressoir:2014:GGP

Drucker:2018:FMB

Dolev:2019:AAC
Shlomi Dolev, Niv Gilboa, and Ximing Li. Accumu-
References


[DHT+19] Van Tuyen Dang, Truong Thanh, Nguyen Huu Thanh, Pham Ngoc Nam, Nguyen Ngoc Thanh, and Alan Marshall. SDN-based SYN...


[DJG+15] Lin Ding, Chenhui Jin, Jie Guan, Shaowu Zhang, Ting Cui, Dong Han, and Wei Zhao. Cryptanalysis of WG family of stream ciphers. *The Computer Jour-
REFERENCES


Domnitser:2012:NMC


Delfs:2002:ICP


Delfs:2007:ICP


Dolev:2012:ATC


Delfs:2015:ICP

REFERENCES


[DKA+14] Delimitrou:2016:SID

[DKL+16] Dorre:2016:ELO


[DKL+19] Dobre:2016:MCG


REFERENCES


[Dong:2018:SSM] Yao Dong, Ana Milanova, and Julian Dolby. Se-

**DiPietro:2010:HKS**


**Drozdz:2019:SCC**


**Diesburg:2016:TLA**


**Dwivedi:2018:DLR**


**Dimitrakakis:2015:ELA**


**Demme:2012:SCV**

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

**David:2012:UCO**


**Donovan:2014:ATM**


**Doroz:2015:AFH**


**Duncan:2012:CAI**


**Ding:2017:CSM**


**Das:2016:CWM**

Dziembowski:2018:NMC


Dong:2012:NCV


Daemen:2010:FYA


Duong:2011:CWC


Dautrich:2012:SLU


Draziotis:2016:EDL


Dong:2011:SSE

Dasgupta:2016:TDA


Dixon:2016:NTO


delRey:2012:EDI


Dini:2011:LLA


Dixit:2019:FBD


Das:2015:DCS

REFERENCES

Das:2016:MPU

Das:2012:DPB

Deng:2018:SFE

Dachman-Soled:2014:COF

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


Dong:2012:KKD

Dong:2012:NDI


[DY13] Yevgeniy Dodis and Yu Yu. Overcoming weak expectations. Lecture Notes in

[DZ14] Lonzhi Deng and Jiwen
REFERENCES


Dong:2016:EPP

Ding:2016:EPP


Delledonne:2018:CDA


Dent:2010:PS


Eslami:2011:SIS

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

Erguler:2012:PAI

Ekberg:2012:AEP

Ehdaie:2016:HCR

Elrabaa:2019:PPP

Erbagci:2019:SHE


El-Emam:2013:NASA


Espitau:2018:LAF


El-Hadedy:2019:RPR


Eisenbarth:2010:CCE


Esiner:2016:FFB

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

Emura:2019:PPA


Engels:2013:NLL


Elbirt:2009:UAC


ElBansarkhani:2012:ELB


Embar:2014:PWO


English:2015:SME

Rosanne English. Simulating and modelling the effectiveness of graphical password intersection attacks.

Evtyushkin:2016:UMC


Eberz:2016:LLE


El-Razouk:2015:NHI


Estebanez:2014:PMC


Engels:2012:HLA


Ebadi:2015:DPN

Hamid Ebadi, David Sands, and Gerardo Schneider. Differential privacy: Now it’s getting personal. ACM SIGPLAN Notices, 50(1):69–81, January 2015. CODEN SINODQ. ISSN 0362-
REFERENCES


REFERENCES


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


[FCM14] Luca Ferretti, Michele Colajanni, and Mirco

Fuglerud:2011:SIA


Fang:2019:PPO


Fehr:2010:QC


Feigenbaum:2019:PSE


Felten:2013:LBA


Faugere:2010:CLR

Fleischmann:2012:MFA


Fan:2018:OVG


Feng:2010:CTS


Farras:2012:LTM


Faugere:2014:MCA


Fan:2017:SSP

Jingyuan Fan, Chaowen Guan, Kui Ren, Yong Cui, and Chunming Qiao. SPABox: Safeguarding privacy during deep packet inspection at a MiddleBox. *IEEE/ACM Transactions on Networking*, 25
Fan:2018:MBP


Fan:2013:CPP


Fan:2010:PSN

Chun-I Fan, Pei-Hsiu Ho, and Ruei-Hau Hsu. Provably secure nested one-time secret mechanisms for fast mutual authentication and key exchange in mobile communications.


Fan:2010:AMI


Farras:2017:IRN


Faz-Hernandez:2019:HPI


Florencio:2016:PSD

Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. Pushing on string: the ‘don’t care’ region of password strength. 


Feng:2018:ABB


Fidler:2018:CCN


Farash:2015:PSE


Fisher:2015:CS


Fei:2012:GTK

Han Fei, Qin Jing, Zhao Huawei, and Hu Jiankun. A general transformation from KP-ABE to searchable encryption. Lecture Notes in Computer Science, 7672:165–178, 2012. CODEN LNCSD0. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
REFERENCES

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


REFERENCES

Forler:2012:DAC

Fei:2016:PPA

Fei:2016:SEF

Feng:2016:CAO

Fallahpour:2015:AWB

Ferrag:2018:SCN
Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-


See retraction notice [?].


REFERENCES


Fraczek:2012:MSI


Fernandez-Mir:2012:SRA


Ferreira:2015:LPA


Fu:2018:LUA


Fokkink:2012:TCG


Folger:2016:TQH


[FQZF18] Wei Feng, Yu Qin, Shi...

[Fra16]


[Frep17]

REFERENCES


REFERENCES


REFERENCES


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

Fanti:2018:DLC


Franken:2019:ECP


Fathi-Vajargah:2017:IMC


Fiore:2017:PGP


Feng:2013:ECE


Fanyang:2012:SAK

Fanyang, Naixue Xiong, and Jong Hyuk Park. A self-adaptive $K$ selection mechanism for re-
REFERENCES


Fan:2014:NCI

Fu:2012:EHA

Gross-Amblard:2011:QPW

Grondahl:2019:TAA

Guimaraes:2019:OIQ
REFERENCES

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

Gregio:2015:TTM


Gope:2018:LPP


Galindo:2013:NIC

David Galindo. A note on an IND-CCA2 secure [Gas13]


Gasarch:2013:RBC


Gutierrez:2016:IDO


Ghoshal:2019:RSC

Sucheta Ghoshal and Amy Pailey.

Gupta:2019:DRB

Gupta:2019:DRB


Goru:2011:MKC


Guyeux:2015:ECS


Gao:2019:LBD


Gupta:2012:CDF

REFERENCES

Gupta:2013:HPH

Gupta:2013:HPH

Guerra-Casanova:2011:SOT

Granado-Criado:2017:HCH

Gao:2018:PRR

Guerin:2016:TDU
Nilson Donizete Guerin, Jr., Flavio de Barros Vidal, and Bruno Macchiavello. Text-dependent

**Giot:2011:UKD**


**Geller:2013:MIS**


**Gentry:2010:CAF**


**Gentry:2013:EMH**


**Gaspar:2012:SEF**


**Gong:2010:PCI**

Guang Gong and Kis-


REFERENCES


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


**Guo:2019:NBT**


**Gravier:2015:WOD**


**Goyal:2013:CZK**


References


REFERENCES


REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29101-2_15/


Gueron:2016:HIA


Gonzalez-Manzano:2017:EHE


Gonzalez-Manzano:2019:LUR


Gunson:2011:UPS


Giambruno:2015:GGB


Garcia-Martinez:2015:HEB

REFERENCES


García-Morchon:2015:HCR


Guo:2011:ISS


Guo:2014:SAS


Gao:2014:URA


Good:2012:BTC

REFERENCES


Keke Gai, Meikang Qiu, and Houcine Hassan. Secure cyber incident analytics framework using Monte

**Ghatak:2019:IBS**


**Ghosal:2019:NPP**


**Greengard:2011:MRM**


**Green:2017:SSE**


**Green:2019:RMC**


**Green:2019:RNT**

Frederic Green. Review

Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Guo:2018:WBS


Gonzalez-Serrano:2018:SML


Gupta:2018:SCA


Guha:2017:RTS

REFERENCES

41:??, May 2017. CODEN ??? ISSN 1550-4832 (print), 1550-4840 (electronic).

Guin:2016:FCS


Gutman:2016:EAF


Gong:2016:FSC


Gierlichs:2012:ICD


Genkin:2013:RKE

Ge:2016:KPA


Gazi:2012:EOS


Gallin:2019:GFP


Gupta:2019:LAU


Goodrich:2011:EAD


Grosse:2013:AS


Greenberg:2014:GWB


Gebotys:2016:PCP


Gao:2019:EUE


Wang:2014:RAW


Gao:2015:GCC


Goh:2013:TOT

Guo:2019:EER


Guo:2012:AKE


Guo:2017:EMD


Gao:2012:RHC


Guo:2018:SMK


Gao:2019:VQS

GZSW19 Pengfei Gao, Jun Zhang, Fu Song, and Chao Wang. Verifying and quantifying side-channel resistance of...


Hamamreh:2012:RPA


Hamlin:2017:NMC


Hamidi:2019:ADS


Hanyok:2012:EHH


Harn:2013:GA


Harrington:2014:GEF


Hardesty:2015:BAC

Hardesty:2016:SUC

Hastings:2016:SWS

Hayes:2013:NSA

Houmansadr:2013:BCN

Hurlburt:2014:BBC

Hetzelt:2017:SAE

Hernandez-Becerril:2016:GIS
Hao:2012:SAM

Hu:2017:ATE

Hwang:2010:RIB
Hsu:2011:NLM


Hore:2012:IED


Hernandez-Castro:2012:MTA


Huang:2014:FOS


Hsu:2011:WLC


Hernandez-Castro:2012:AFH

Huang:2018:BLD


Hosny:2019:RCI


Han:2013:RMA

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

Heninger:2012:MYP


Heath:2015:HNS

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


Hwang:2012:ABA


Hamad:2018:DWU


Hermelin:2010:MLC


Herranz:2014:ABS

[Her14] Javier Herranz. Attribute-based signatures from RSA. *Theoretical Computer Science*, 527(?):73–82, March 27, 2014. CODEN TCSCDI. ISSN 0304-


[HGOZ19] Joshua Hibschman, Darren Gergle, Eleanor O’Rourke, and Haoqi Zhang. Isopleth: Supporting sense-making of professional Web applications to create readily available learning experiences. ACM Transactions on Computer-Human In-
REFERENCES


[HHBS18] Mohamed Tahar Hammi, Badis Hammi, Patrick Bel-lot, and Ahmed Serhrouchni. Bubbles of trust: a decentralized blockchain-


Hinarejos:2015:MES


Hao:2019:IDP


Hinkelmann:2011:CPA


Hasan:2014:TFL

[HK14a] O. Hasan and S. A. Khayam. Towards for-


Handa:2019:SES

Houmansadr:2014:NBW

Hur:2013:REC

Hanzlik:2019:CPC

Heyse:2012:LEA

Heil:2014:APH
REFERENCES


REFERENCES


**Huang:2014:SWC**


**Hefeeda:2010:ASM**


**Herzberg:2012:TJA**


**Hwang:2019:BBR**


**Hore:2012:SMR**


**Hajihassani:2019:FAI**


[Hof16] Leah Hoffmann. Last byte: Q&A: Finding new directions in cryptography: Whitfield Diffie and Martin Hellman on their meeting, their research, and the results that billions use every day. *Communications of the Association for Com-


REFERENCES


Halder:2010:WTR


He:2012:ECT


Howe:2015:PLB


Hurrah:2019:DWF


Hadlington:2019:ERW
Hoffstein:2008:IMC


Hur:2010:CCS


Han:2010:BEI


Han:2014:GTK


He:2013:GME

REFERENCES


Muneeb Ul Hassan, Mubashir Hussain Rehman, Ramamo hanarao Kotagiri, Jiekui Zhang, and Jinjun Chen. Differential privacy for renewable energy resources based smart metering. Journal of Parallel and Distributed Computing, 131(??):69–80, September


[HSA14] N. Homma, K. Saito, and T. Aoki. Toward formal design of practical cryptographic hardware based on Galois field arithmetic. IEEE Transac-
REFERENCES

Hall:2019:BIA

Han:2014:IBS

Halevi:2011:TBH

Han:2012:PPD

Heather:2014:CPE

Han:2013:IBD

Ho:2011:EIB
Chen-Han Ho, Garret Staus, Aaron Ulmer, and Karthikeyan Sankaralingam.


Kaibin Huang, Raylin Tso, and Yu-Chi Chen. Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its ex-
REFERENCES


Herbert:2012:SMP


[HU15]


Hulsing:2013:WOS


Hurlburt:2016:MBO


Hammerle-Uhl:2011:RWI


Harvey:2017:FPM

David Harvey, Joris Van Der Hoeven, and Grégoire Lecerf. Faster polynomial multiplication over finite fields. Journal of
REFERENCES

the ACM, 63(6):52:1–52:??, February 2017. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

**Hunger:2018:DDC**


**Han:2012:MIA**


**Hammad:2019:PSF**


**Hwang:2011:NIB**


**Holbl:2010:TPI**


**Holbl:2012:ITP**

Marko Hölbl, Tatjana Welzer, and Bostjan Brunen. An improved two-party identity-based authenticated key agreement protocol using pair-
He:2012:ICS

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.

Heng:2010:CNS

Hsu:2014:VWR
He:2018:MBF

Huang:2019:AIA

Huang:2018:PIB

Hu:2019:CAC
Chengyu Hu, Rupeng

Hao:2011:NTV


Huang:2011:IBS


Heys:2011:PSC


Han:2012:ERI

REFERENCES


Han:2014:ERI

Han:2018:ERA

Huang:2018:ILA

Huang:2005:EMP


IBM:2013:DMP


IBM:2013:IPC


Irshad:2017:CPP


IEEE:2011:ICl


IEEE:2011:PIA

IEEE:2013:PIS


IEEE:2015:ISS


Imanimehr:2016:HPR


Islam:2011:MDA


Iyengar:2016:SPS


Imai:2015:IRR


Ioannou:2014:PKC


Ingram:2016:AMB


Ioannou:2014:PKC


Intel:2019:IAM


Isobe:2012:SCL

Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii. Slide cryptanalysis of lightweight

Islam:2018:REP


Isobe:2012:SAL


Irshad:2016:EAM


Ishai:2014:PCP


Jacobs:2016:STB

Jie:2010:AAI

Jie:2011:RGA

Jho:2016:SSE

Jia:2018:ERH
REFERENCES


REFERENCES


October 2018. ISSN 1540-7993 (print), 1558-4046 (electronic).

Jiang:2018:AHP


Jeong:2012:IKP


Jajodia:2012:RET


Jia:2012:PKD


Jiang:2019:PPP


REFERENCES


[Jain2018:MDN] Ajay Jain and Sachin Soni. Multi-directional navigation method for optimized consumption of user generated content through semantic mapping of features derived from the user generated content. ACM SIGSOFT Software Engineering Notes, 43(4):52,
Jaiyeola:2018:IPN


Jalili:2017:EAS


Jevdjic:2017:ASC


Judymer:2017:BCI


Jordan:2018:EPE

M. Jordan, N. Sardino, M. McGrath, C. Zoellin,
REFERENCES


**Jiang:2018:CPA**


**Jiang:2018:FCP**


**Jiang:2012:DCA**


**Joye:2012:FAC**

Tong:2012:NBD


Jiang:2016:CVI


Juels:2014:INC


Jin:2015:NCD

REFERENCES

Joux:2014:SAC


Jiang:2010:EDI


Jan:2019:SEE


Khazaei:2017:COA


Kurkcu:2018:CBE


Kornycky:2017:RFT

Joe Kornycky, Omar Abdul-

Koziel:2018:HPS


Kamp:2013:MES


Kamp:2016:MEM


Kammuller:2019:ATI


Kapera:2013:SPD


Kapera:2013:MRM

Karafyllidis:2012:QGC


Kawamoto:2015:LSH


Kong:2015:CSM


Kartigaikumar:2010:PPV


Kallel:2011:SMM


Kleinrouweler:2017:SAP


Kim:2011:SSE


Khan:2018:APS


Kraetzer:2012:PCS


Kieffer:2018:IBC


Kumar:2019:SSH

[KD19] Chanchal Kumar and Mohammad Najmud Doja. A secure structure for hiding information in a cryptosys-


Kim:2012:SLT


Kwon:2010:SEB


Koo:2018:PPD


Khazaei:2010:NBS


REFERENCES

Kolsch:2019:SBP


Kai:2011:CIS


Kiayias:2011:TCC


Kim:2011:LBA


Kim:2015:CEH

Kim:2016:MAS


Khan:2016:BSW


Konstantinou:2010:RCI


Kawai:2012:SHS


Kawai:2013:SHS


Khalil:2014:CIM

Issa Khalil, Abdallah Khreishah, and Muhammad Azeem. Consolidated Identity Management System for secure mobile cloud


Khan:2014:IPR


Katz:2008:IMC


Kushwah:2011:EIB


Khakpour:2013:ITA


Katz:2015:IMC


Klapper:2010:PSS

Andrew Klapper. *Pseudorandom Sequences and Stream Ciphers*, chapter 17, pages 1–23. Volume 2 of Atallah and Blanton [AB10b], second edi-
REFERENCES

Ko:2010:MME


Kim:2019:AAI


Koeberl:2012:EPD


Kent:2015:AGA

[102x681] Kent:2015:AGA


Kumari:2016:UFM

[102x681] Kumari:2016:UFM

Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Hamed Arshad, and Muhammad Khurram Khan. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. *Future Generation Computer Systems*, 63(??):56–75, Octo-
Kumari:2017:DPS


Kim:2012:INS


Keller:2010:DAS


Khomejani:2010:PCT


Koblitz:2010:BNW

Kiani:2011:MPD


Kifer:2014:PFM


Koblitz:2015:RWE


Kasamatsu:2012:TSE


Kandi:2017:ELC

Kline:2018:CAR


Kiyoshima:2014:CRB


Karger:2011:LLB


Katz:2012:TSP


Kavun:2018:SAE


KMSM15

REFERENCES

Kang:2019:NBK


Khovratovich:2010:RCA


Knijnenburg:2017:PCE


Khovratovich:2010:RRA


Kobsa:2013:CJV


Kheiri:2014:CCV


Kumari:2016:APW

Shipra Kumari and Hari Om. Authentication protocol for wireless sensor networks applications like

**Koblitz:2010:BRB**


**Komargodski:2018:LRO**


**Kasper:2012:SCA**


**Kollmitzer:2010:AQC**

Kang:2012:AKM


Kolman:2017:SCG


Koya:2018:AHM


Kumar:2017:TAU


Kobusinska:2018:BDF

Kiltz:2011:EAH


Khalid:2016:RHL


Kocabaş:2012:CPB


Kang:2016:DSA


Keskinarkaus:2010:IWD


Krenn:2013:CCR

REFERENCES

Knudsen:2011:BCC

Krantz:2012:EAM

Kostinger:2012:SBL

Kannan:2013:NQF

Krenn:2013:AWI

K:2018:AAF
Keerthi K., Chester Rebeiro, and Aritra Hazra. An algorithmic approach to formally verify an ECC li-
Khan:2010:RCB

[102x681]


King:2011:BBB

[102x681]


Kolesnikov:2012:LPP

[102x681]


Kumar:2015:RGB

[102x681]


Kalayappan:2018:PAH

[102x681]


Karthiga:2018:PSA

[102x681]

REFERENCES


(Kwon:2018:EIP) Jihoon Kwon, Seog Chung

**Ksiepopolski:2012:QMQ**


**Kim:2012:SSS**


**Klingler:2013:UPT**


**Khamis:2018:CCT**

Kalisowski:2012:CCP

Kai:2014:FSD

Kumagai:2010:UGS
J. Kumagai. UK gets a

**Kupcu:2013:DTT**


**Kupcu:2015:OAS**


**Kushner:2013:RSS**


**Kuznetsov:2011:APP**


**Kshetri:2018:BEV**


**Kilgallin:2019:FRK**


**Kim:2019:IED**

[KV19b] Jungwon Kim and Jeffrey S. Vetter. Implementing efficient data compression and encryption in a...

Kiljan:2018:ETA


Karpovsky:2014:DSS


Kuo:2016:SDD


Koyama:2012:NTD


Kamal:2010:EIN


Kreutz:2018:KPS

D. Kreutz, J. Yu, P. Esteves-Verissimo, C. Magalhães, and F. M. V. Ramos. The KISS principle in software-defined networking: A

**Kuo:2018:DRA**


**Kate:2010:PBO**


**Kiayias:2017:EEV**


**Lu:2010:MSC**


**Lathey:2015:IEE**


**Lackey:2015:UHP**


Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanath.

**Launchbury:2012:TBC**


**Lauter:2017:POL**


**Lazarus:2015:RE**


**Liu:2013:PAE**


**Loreti:2018:PAB**


**Luo:2012:ESI**


**Lupu:2012:IBK**

Radu Lupu, Eugen Borcoci, and Tinku Rasheed. Identity-based key deriva-


REFERENCES

Lathrop:2011:SPI

Lavington:2012:ATH

Li:2015:NAC

Lee:2017:SUE

Liu:2017:GAU
REFERENCES


**Li:2014:PSC**


**Li:2016:CBK**


**Liu:2019:TTR**


**Ledin:2016:RME**


**Lewand:2010:PC**


**Liu:2019:DVP**

Lago-Fernandez:2014:NAA


Leung:2018:TTA


Luo:2019:SCT


Liu:2016:LCR


Liang:2015:CPA


Li:2018:CIC

[M. Li, H. Fan, Y. Xiang, Y. Li, and Y. Zhang. Cryptanalysis and improvement of a chaotic im-

Li:2017:PCL


Lekkas:2010:PMT


Lancrenon:2012:IP1


Liu:2017:ECC


Lan:2010:RNG


Li:2012:FDM

Wei Li, Dawu Gu, Zhiqiang Liu, Ya Liu, and Xi-

Lee:2017:FFE


Lee:2019:TES


Lopez-Garcia:2014:PBB

REFERENCES

Li:2014:SCA


Liu:2012:FVC


Lee:2010:CGC


Lee:2010:EBB


Lee:2011:IMS

REFERENCES


Daniel Lerch-Hostalot and


Xiong Li, Maged Hamada Ibrahim, Saru Kumari, Arun Kumar Sangaiah,


Litton:2014:TFA


Liu:2015:LBD


Liu:2016:LCP


Li:2017:MMA


Li:2018:MMA


Liu:2019:ICA


REFERENCES


[LL15] Cheng-Chi Lee and Yan-


REFERENCES

Li:2015:ANA

Li:2017:ESD

Lyu:2018:PKE

Lyu:2019:SPP

Lin:2016:SCU

LLG15

LLH17

LLG19

LLH18

LLHS12
Jian Li, Hongmei Liu, Jiwu Huang, and Yun Q. Shi. Reference index-based H.264 video watermarking scheme. *ACM...


Lee:2019:CSS


Lee:2016:CAM


Lee:2016:AGA


Ling:2012:NCC

REFERENCES


[Li:2018:WMH] Li:2018:WMH


Qi Li, Patrick P. C. Lee, Peng Zhang, Purui Su,

**Lucamarini:2014:QKD**


**Lambert-Mogiliansky:2012:EII**


**Le:2016:ADS**


**Lai:2018:IBB**


**Lai:2017:FPP**

Liu:2014:SCS


Li:2011:NRA


Lv:2013:NTP


Lubacz:2010:VI


Lukasiewycz:2016:SAO


LoIacono:2019:NGR


Li:2018:RBB


[Lop15a] Lanfranco Lopriore. Password capabilities revis-
REFERENCES

Lopriore:2015:PMD


Lin:2011:CRN


Ling:2012:SHS


Lima:2010:PKE


Lian:2015:GRG

REFERENCES

comjnl.oxfordjournals.org/content/58/10/2426.


[Lukowiaiak:2014:CEB]


[Liskiewicz:2013:GBS]


[Liskiewicz:2017:SLS]


[Luo:2012:FSU]


[Lin:2015:SSE]

Chung-Hsiang Lin, De-Yu Shen, Yi-Jung Chen, Chia-Lin Yang, and Cheng-Yuan Michael Wang. SE-

Lychev:2016:RSI


Liu:2019:IMM


Liang:2015:EFC


Lin:2017:ESF


Liu:2016:EPP


Lee:2013:CCM

REFERENCES


Yingjie Lao, Qianying Tang, Chris H. Kim, and Keshab K. Parhi. Beat frequency detector-based high-speed true random number generators: Statistical modeling and analysis. *ACM Jour-


Claudio Lucchese, Michail Vlachos, Deepak Rajan, and Philip S. Yu. Rights
REFERENCES

Lafitte:2011:CBF

Liu:2010:CIE

Lee:2011:ACA

Lewko:2011:DAB

Lewko:2011:UHA


REFERENCES


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


Lu:2012:HOM Jiqiang Lu, Yongzhuang Wei, Jongseung Kim, and

Lu:2014:HOM


Liu:2010:NDC


Liu:2017:SRG


Liu:2011:PIA


Junzhou Luo, Xiaogang Lu:2010:NAS


Liu:2016:NSC

Liu:2016:NSC


Li:2014:EMK


Lai:2012:RHB


Luo:2014:ARP


Liu:2015:SDS


Lim:2016:AKE

Hoon Wei Lim and Guomin Yang. Authenticated key exchange protocols for parallel network file systems. *IEEE Transactions on Parallel and Dist-


Tingting Lin, Hailun Yan, Xuejia Lai, Yixin Zhong, and Yin Jia. Security eval-
evaluation and improvement of
a white-box SMS4 imple-
mentation based on affine
equivalence algorithm. The
Computer Journal, 61(12):
1783–1790, December 1,
2018. CODEN CM-
PJA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
academic.oup.com/comjnl/article/61/12/1783/5055352.

Li:2010:ESS

C Chung Ki Li, Guomin
Yang, Duncan S. Wong, Xi-
aotie Deng, and Sherman
S. M. Chow. An efficient
signcryption scheme with
key privacy and its exten-
sion to ring signcryption.
Journal of Computer Secu-
rity, 18(3):451–473, ????
2010. CODEN JCSIET.
ISSN 0926-227X (print),
1875-8924 (electronic).

Liao:2012:NSM

Xin Liao, Qiao yan Wen,
Ze li Zhao, and Jie Zhang.
A novel steganographic
method with four-pixel
differencing and modu-
lus function. Fundamenta
Informaticae, 118(3):281–
289, August 2012. CODEN
FUMAAJ. ISSN 0169-2968
(print), 1875-8681 (elec-
tronic).

Liao:2010:MPC

Xin Liao, Qiao yan Wen,
Ying Sun, and Jie Zhang.
Multi-party covert commu-
nication with steganogra-
phy and quantum secret
sharing. The Journal
of Systems and Software,
83(10):1801–1804, October
2010. CODEN JSSODM.
ISSN 0164-1212.

Lai:2019:NIB

Qi Qi Lai, Bo Yang, Zhe
Xia, Yannan Li, Yuan
Chen, and Zhenlong Li.
Novel identity-based hash
proof system with compa-
ct master public key from
lattices in the stan-
dard model. Interna-
tional Journal of Foun-
dations of Computer Sci-
ence (IJFCS), 30(4):589–
606, June 2019. ISSN
0129-0541. URL https:
//www.worldscientific.
com/doi/10.1142/S0129054119400148.

Liu:2016:FIT

Joseph K. Liu, Sze Ling
Yeo, Wun-She Yap, Sher-
man S. M. Chow, Dun-
can S. Wong, and Willy
Susilo. Faulty instanti-
ations of threshold ring
signature from threshold
proof-of-knowledge proto-
col. The Computer Jour-
nal, 59(7):945–954, July
2016. CODEN CM-
PJA6. ISSN 0010-4620
(print), 1460-2067 (elec-
tronic). URL http://
comjnl.oxfordjournals.
org/content/59/7/945.


[LZC⁺12b] Yong Luo, Yan Zhao, Lei Cheng, Jianxin Wang, and Xuchong Liu. Lossless visible three-dimensional watermark of digital elevation model data. Lecture Notes in Computer Science, 7220:138–147, 2012. CODEN LNCSDE. ISSN 0302-9743 (print), 1611-
Liu:2014:PKE


Liu:2017:ESS


Liu:2014:CRA


Liu:2019:IEU

Hongjun Liu, Yingqian Li:2019:APA


Li:2010:PES


Ma:2017:AEJ


Masdari:2017:STA


MacCormick:2012:NAC


With a foreword by Christopher M. Bishop.

Macrakis:2014:PLS


Maffeo:2016:UNC


Michail:2012:EHT

Harris E. Michail, George S. Athanasiou, Vasilis Keloukas, George Theodoridis, and Costas E. Goutis. On the exploitation of a high-throughput SHA-256 FPGA design for


Mazumdar:2016:CIS


Mashhadi:2017:NMS


Matsuda:2014:IBP


Matthiessen:2019:RCM


Maurer:2012:CCN


Mayron:2015:BAM


Mainardi:2019:PRA


Massolino:2015:OSC


Mukhopadhyay:2011:PEA

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).

Matula:2019:PCG

David W. Matula and Zizhen Chen. Precise and concise graphical representation of the natural numbers. In Takagi et al. [TBL19], pages 100–103. ISBN 1-72813-366-1. ISSN 1063-6889.

Madanayake:2012:BPS


McGrew:2017:IDH


McGrayne:2011:TWH


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


REFERENCES

435


REFERENCES


[MHKS14] Andrew Miller, Michael Hicks, Jonathan Katz,

Mo:2018:RUA


Munoz-Hernandez:2016:EES


Mou:2013:CBC


Mohd:2015:SLB


Ma:2019:PFC

Mohd:2018:HDM


Micciancio:2010:FGC


Michiels:2010:OWB


Michael:2016:RNI


Midgley:2010:SEE


Martinez-Julia:2012:NIB


Martinez-Julia:2013:BSI

Pedro Martinez-Julia and Antonio F. Skarmeta. Beyond the separation of identifier and locator:


Mozaffari-Kermani:2017:FDA


Mozaffari-Kermani:2018:ERE


McGrew:2016:SMH


Malik:2012:AIC


Menesidou:2017:CKM


Marconato:2013:VLC

[G. Vache Marconato, M. Kaâniche, and V. Nicomette. A

Mozaffari-Kermani:2010:CSI


Montecchi:2012:QSE


Mancillas-Lopez:2010:RHI


Mendez:2016:PES


Manzanares-Lopez:2012:ICI

Pilar Manzanares-Lopez, Josemaría Malgos-Sanahuja, and Juan Pedro Muñoz-Gea. The importance of considering unauthentic transactions in trust management systems. *Journal
REFERENCES

Ma:2017:LBI

Maity:2014:FIR

Meshram:2013:IBC
Chandrashekhar Meshram and Suchitra A. Meshram.


Mondal:2014:DSM
Maity:2017:ODC


Mazumdar:2017:CRS


Mulholland:2017:DCD


Martins:2019:HHR


Merlo:2015:MEP


Mailloux:2016:PSS


Miao:2016:RAS

Yinbin Miao, Jianfeng Ma, and Zhiquan Liu. Revocable and anonymous search-

Maeng:2015:TAU


Moldovyan:2012:BBD


Mahmoody:2014:PPK


Marino:2019:ACN


Macedo:2017:SPP

REFERENCES


Mukhopadhyay:2014:EMP


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

Monz:2016:RSS


McKusick:2015:DIF


Minier:2012:RKI


Mizuki:2011:ASN


Maimut:2012:LCR

Diana Maimut and Khaled Ouafi. Lightweight cryp-
Minamoto:2014:BDI


Mone:2013:FPE


Moore:2012:RFF


Moriai:2019:PPD

Mosca:2018:CEQ


Moulick:2015:RDS


Minier:2012:EEC


Min:2018:AAB


Meiklejohn:2016:FBC


Mundhenk:2017:SAN

Mironov:2012:IDP


Mukhamedov:2010:IEP


Maimut:2014:AET


Marasco:2014:SAS


Micali:2014:CMS


Manimehalai:2016:NRR


Migliore:2018:HSC

[VMR18] Vincent Migliore, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline

Moataz:2018:SSE


Martinovic:2017:AUP


Matsumoto:2017:ACG


Moghadam:2010:DRN


Mendel:2012:DAL

Maitra:2012:NAC

Mroczkowski:2012:CAS

Maitra:2013:DSM

Maitra:2013:HEM

Maitra:2013:HPM

Miller:2016:RPS

Mukherjee:2017:EPP
Srilekha Mukherjee and Goutam Sanyal. Enhanced


[MSI10] Kinga Marton, AlinSuciu, and IosifIg nat. Ran-
Mashimo:2018:VMS


Mosenia:2017:CCA


Mazurczyk:2013:FWS


Martins:2018:SFH


Muhammad:2018:ISU


Migliore:2017:HSA

Vincent Migliore, Cédric Seguin, Maria Méndez Real, Vianney Lapotre, Arnaud Tisserand, Caroline Fontaine, Guy Gogniat, and Russell Tessier. A high-speed accelera-


REFERENCES

180–193, 2012. CO- 
DEN LNCSD9. ISSN 0302-9743 (print), 1611- 
com/chapter/10.1007/978-3-642-31448-3_14.

Mamais:2017:BVP


Mouris:2018:TSB


Muftic:2016:BCC


Mundy:2017:CGU

REFERENCES


Murphy:2010:BRB

Murdoch:2016:IDP

Min:2016:RSC

Mishra:2016:AFP

Modersheim:2018:ABP
Sebastian Mödersheim and Luca Viganò. Alpha–beta privacy. ACM Transactions on Privacy
REFERENCES

458


Mefenza:2019:CSA


Mannan:2011:LPD


Maes:2012:PFF


Mathew:2012:EIC


Moghimi:2019:MFD


Meng:2018:TTB

Weizhi Meng, Yu Wang, Duncan S. Wong, Sheng

Ma:2012:CIS


Mahmoody:2013:LEZ


Ma:2013:PVP


Meng:2015:CRS


Marko:2017:MDI


Mastroeni:2017:APS

Isabella Mastroeni and Damiano Zanardini. Ab-

Manshaei:2013:GTM


Ma:2015:PKE


Meng:2019:ESF


Mofrad:2018:CSI


Nagy:2010:OTP


Nagy:2010:QCS


Namasudra:2019:IAB

Noureddine:2013:AMT

Nain:2017:SPE

Naskar:2012:FIR

Naskar:2013:GTL

Naranjo:2013:FDA


[NIST:2012:RRN] NIST. Recommendation for random number generation using determinis-
tic random bit generators. Special Publication 800-90, National Institute for Standards and Technology, Gaithersburg, MD 20899-8900, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.


REFERENCES

Nguyen:2012:DQB

Neville-Neil:2015:KVH

Nagy:2010:KDV

Navin:2010:ETU

Nordrum:2017:GBD

Nose:2011:SWA
REFERENCES


REFERENCES

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

Namasudra:2017:NSA

Niu:2015:CRS

Naccache:2010:THI

Nojoumian:2012:SRS

Natarajan:2015:MAD

Nguyen:2017:DPA
Niksefat:2014:ZPP


Neustaedter:2018:BTW


Nagano:2018:PRT


Nandakumar:2017:CAI


Nguyen:2012:LRS

REFERENCES


Nie:2013:CHB


Natgunanathan:2017:PBM


Ntantogian:2010:GME

REFERENCES

Newell:2014:NCR

Niu:2015:NAS

Nikooghadam:2010:EUE

Obana:2011:AOC

Oligeri:2011:REA

Obrenovic:2012:IUC
REFERENCES


REFERENCES

**Ou:2010:CPA**


**Ogiela:2018:EBI**


**Oliveira:2012:STA**


**Or-Meir:2019:DMA**


**Ortiz-Martin:2019:FAI**


**Ogiela:2010:UML**

Marek R. Ogiela and Urszula Ogiela. The use of mathematical linguistic methods in creating secret sharing thresh-


REFERENCES


[OSANAM19] Arezou Ostad-Sharif, Hamed


Olson:2016:SIT


Ohtake:2019:OSA


Orencik:2016:MKS


Okamoto:2012:AAH

Otmani:2010:CTM

Ogiela:2018:VCA

Ohzeki:2012:NWM

Ortiz-Yepes:2014:BSA

Praba:2010:MAC

Parrilla:2019:ECC
Luis Parrilla, José A. Álvarez-Bernejo, Encarnación Castillo, Juan A.


REFERENCES


REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-35130-3_10.

Pereira:2015:PKE


Pippal:2012:SVU


Pearson:2011:NWC


Peck:2012:CAC


Peck:2017:BWD

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

Persichetti:2013:SAH


REFERENCES


Park:2012:IDF


Pohls:2012:RDI


Premnath:2016:SPC


Parno:2016:PNP


Papas:2012:MLR


Park:2010:SIC

Jong Hyuk Park, Sajid

Pieprzyk:2010:TCC


Pieprzyk:2010:TCC

Pointcheval:2012:ACE


Patel:2018:LLA


Premarathne:2015:LDD

REFERENCES


Pramila:2018:ICA

Peter:2012:AHE

Phuc:2016:SAS

Perez:2011:FDS

Peris-Lopez:2018:EAC


REFERENCES

Park:2011:ACC


P:2018:ABE


Pereira:2016:SHB


Pennino:2019:PIS


Pendl:2012:ECC


Pyun:2012:IBF

Young June Pyun, Younghoe Park, Douglas S. Reeves, Xinyuan Wang, and Peng Ning. Interval-based flow watermarking for tracing...

**Pathak:2012:PPS**


**Papadopoulos:2015:PAP**


**Papadopoulos:2015:PAP**


**Papadopoulos:2015:PAP**


**Pandey:2012:PPS**


**Piret:2012:PBC**

Gilles Piret, Thomas Roche.
Perez-Resa:2019:SSE


Puthal:2019:SAL


Proudfoot:2015:WTH


Polyakov:2017:FPR


Popa:2012:CPQ

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-
Pizzi:2018:ETM


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Pankhuri:2019:PBM


Papamanthou:2013:SCC


Peng:2019:GCS

[Peng and Takayasu 2019] Liqiang Peng and Atsushi Takayasu. Generalized cryptanalysis of small CRT-exponent RSA. Theoretical Computer Science,
REFERENCES


REFERENCES


Pei:2013:ARW


Pham:2019:SSS


Puthal:2019:SSE


Poller:2012:EIC


Peng:2010:IWM


Pongaliur:2013:SNS


Pja:2019:SSG

Alphonse Pja and Venkatramana Reddy Y. Scal-

**Pagnin:2018:HDB**


**Philippaerts:2013:CMC**


**Pei:2015:SWT**


**Papadopoulos:2010:CAR**


**Phuong:2018:CBE**


**Popa:2015:HCD**

R. A. Popa and N. Zeldovich. How to compute
with data you can’t see. 

**Pournaghi:2018:NNE**


**Peng:2019:EDI**


**Patsakis:2015:PSM**


**Qiu:2018:QDS**


**Qin:2016:VTQ**


REFERENCES


[QZDJ16] Weizhong Qiang, Kang Zhang, Weiqi Dai, and Hai Jin. Secure cryp-


[QZDJ16] Weizhong Qiang, Kang Zhang, Weiqi Dai, and Hai Jin. Secure cryp-

Qi:2016:SID


Qi:2016:SPR


Qin:2018:BRO


Rabin:2010:ACC


Rankin:2010:HLH


Rankin:2014:HEY

REFERENCES

Rankin:2016:HSP


Rao:2010:PAA


Rao:2017:SEC


Rauscher:2015:FMT


Raz:2019:FLR


Ruoti:2015:WJS


Radke:2017:SPP

REFERENCES


Rupp:2015:CTM


Radke:2015:CFA


Reaves:2017:MBM


R:2018:SDM


Rao:2019:HPR


Reinicke:2017:RDS

[RCK17] Bryan Reinicke, Jeffrey Cummings, and Howard Kleinberg. The right to digital self-defense. *IEEE


REFERENCES


Reyhani-Masoleh:2018:NAR


Rezaeibagha:2019:PSB


Ryan:2016:NCE


Rogaway:2016:POP


Rohloff:2019:CAR

Kurt Rohloff. Computer arithmetic research to accelerate privacy-protecting encrypted computing such as homomorphic encryption. In Takagi et al. [TBL19], page 197. ISBN 1-72813-366-1. ISSN 1063-6889.


[RQD+15] Jianbao Ren, Yong Qi,

Rawat:2011:CBR


Razaque:2016:TDP


Rosen:2010:CCS


Reeder:2011:WPD


Rivest:2014:SSR

REFERENCES


Parvin Rastegari, Willy Susilo, and Mohammad Rastegari:2019:ECS


See also news story [Ano15a].

João S. Resende, Patrícia R.


[Rus15] 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**


**Reaves:2018:CSS**


**Roettger:2012:PKC**


**Ren:2014:HHM**

Rogaway:2012:SCS


Ren:2013:PPK


Ristenpart:2010:WGR


Ren:2013:DSE


Romashchenko:2019:OCM


Rajendran:2015:FAB

REFERENCES

Sang:2012:SSF

Sakalli:2014:ACC

Somanatha:2015:RAK

Shivani:2016:PVC

Siad:2016:NFI

Subramanian:2019:SAF
Nalini Subramanian and J. Andrews. Strong authentication framework using statistical approach for cloud environments. Concurrency and Computa-
REFERENCES

Saaninen:2012:PPK

Suoranta:2012:SAM

Sarreshtedari:2015:WMD

Schutz:2010:DIN

Sacco:2014:MC

Sahai:2013:TCT
Sadat:2019:SSG

Saracevic:2019:NAS

Sarier:2010:IAS
Neyire Deniz Sarier. Im-


[SAR18b] Priyanka Singh, Nishant Agarwal, and Balasubramanian Raman. Secure data deduplication using secret sharing schemes over cloud. *Future Genera-
REFERENCES


Masoumeh Safkhani and Nasour Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. The Journal
REFERENCES

Shwartz:2018:DMI

Stevens:2017:AFS

Sarkar:2015:DFA

Safkhani:2012:SMA

Safkhani:2018:SRO

Santos:2014:ACD
REFERENCES

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


REFERENCES


[Sch16c] Bruce Schneier. Cryptography is harder than it

**Schneier:**2018:CAA


**Schneier:**2019:CPI


**Scholl:**2019:SIE


**Shrestha:**2010:KBA


**Stobert:**2018:TAL


**Seberry:**2010:CTAa


**Seberry:**2010:CTAb

Jennifer Seberry, Chris Charnes, Josef Pieprzyk,
REFERENCES

525


**Scriber:2018:FDB**


**shree:2019:ERC**


**Smith-Creasey:2019:NWI**


**Shu:2015:PML**


**Saleh:2010:GTF**


**Shen:2012:PAS**

Jing Shen and Yusong Du. A password authentication scheme against Smart Card security breach. *Lecture...
REFERENCES


[SDM+12] Youssef Souissi, Nicolas Debande, Sami Mekki, Sylvain Guilley, and Ali Maalaoui. On the optimality of correlation power attack on embedded cryptographic systems. Lecture Notes in Computer Science, 7322:169–178, 2012. CODEN LNCS89. ISSN 0302-9743 (print), 1611-


REFERENCES


Sethumadhavan:2016:HEP

Severance:2016:BSB

Seo:2018:AOF

Savas:2014:SMQ

Su:2012:IIN

Shabtai:2010:SAP
REFERENCES

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

Schneier:2015:SWC

Sarma:2012:STP

Sasdrich:2015:ICS

Sakellariou:2019:HEK

Sgantzos:2019:AII

Shu:2014:DAS

Saxena:2016:API
[SGC16] Neetesh Saxena, Santiago Grijalva, and Narendra S.


**Susilo:2016:EDT**


**Shankar:2012:BDF**


**Sun:2017:PKE**


**Sipiran:2014:SCA**


**Shaolan:2011:EDE**

REFERENCES


REFERENCES


REFERENCES


Sabri:2011:AFS

Sachnev:2012:IME

Seo:2012:MPM

Scarani:2014:BPQ

Sepczuk:2018:NRB

Son:2017:NOC
Junggab Son, Donghyun Kim, Md Zakirul Alam Bhuiyan, Rasheed Hussain, and Heekuck Oh. A new outsourcing conditional proxy re-encryption suitable for mobile cloud environment. *Concurrency
REFERENCES


REFERENCES


Stevens:2015:FCF

Singh:2018:MWT

Scheidat:2012:STT

Schmitz:2012:NAC

Srivatsa:2011:ESA

Schultz:2010:MMP
David Schultz, Barbara Liskov, and Moses Liskov. MPSS: Mobile Proactive Secret Sharing. ACM
REFERENCES


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


Santanu Sarkar and Sub-


[Swami:2018:AAS] Shivam Swami and Kartik Mohanram. ARSE-NAL: Architecture for se-

**Shibu:2019:ARR**


**Shokri:2019:ESS**


**Smart:2016:CMS**


**Stanton:2010:FAD**


**Salmon:2011:PRN**


**Smith:2011:SSX**

Smith:2011:RBA


Smith:2015:HHB


Smith:2015:DBP


Swierczynski:2015:PSE


Stankovski:2014:CFE


Sucasas:2016:APP

REFERENCES


[SNM14] Seyed Mohammad Seyedzadeh, Benyamin Norouzi, and Sattar Mirzakuchaki. RGB

---

Soderstrom:2013:DDY


---

Suriadi:2012:PCV


---

Schaumont:2015:IEP


---


---

Strizhov:2016:SPS


---

Suresh:2015:AGU


---

Serwadda:2013:ELK

[SP13] Abdul Serwadda and Vir V. Phoha. Examining a large keystroke biometrics dataset for statistical-

**Shiaeles:2015:FII**


**Shim:2015:SDA**


**Spafford:2016:SE**


**Salvail:2010:STR**


**Sherman:2019:PBL**

Skracic:2017:AAU


Safkhani:2014:CCA


Sun:2013:IUP

San-Tsai Sun, Eric Pospisil, Ildar Mushukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. [SR12a]


Serwadda:2016:TRR


Shaikh:2010:CTO


Schilling:2012:ATU

Thorsten Ernst Schilling


REFERENCES


Szaban:2011:IQB


Saxena:2012:BIT


Shparlinski:2012:CSD


Sendrier:2013:HCE


Singh:2015:EST


Sadhya:2017:PRE

Shivani:2017:RIE


Siegel:2019:UOC


Singh:2013:QBF


Smith:2011:SMC


Sakai:2016:NCS


Shahandashti:2015:RUP

Sundararajan:2019:SMC


Shrivastava:2012:UIE


Strydis:2013:SAP


Sood:2011:SDI


Saadeh:2018:HAP

Spiez:2012:RCT


Sahai:2012:DCC


Schaffer:2012:EII


Schillewaert:2014:CCA


Shrestha:2015:CIS


Shen:2016:RMM


Sethumadhavan:2019:SA

S. Sethumadhavan and M. Tiwari. Secure archi-
REFERENCES

Stallings:2011:C

Stallings:2011:CNS

Stanoyevitch:2011:ICM

Stanek:2012:TEM

Staff:2013:ITD

Stewart:2011:CCI

Steel:2015:APF
Stenn:2015:SNT


Stipcevic:2011:QRN


Stickney:2015:CBS


Stiles:2019:HSB


Stolte:2012:EDA


Suciu:2012:SED


Sung:2011:DCE

Sun:2016:NEB


Shen:2015:CSC


Song:2016:IAR


Shmueli:2014:IDE


Svozil:2014:NCC


Svaba:2010:PKC

ShanmugaPriya:2019:PAS


Shi:2019:LWW


Shoufan:2010:NCA


Song:2016:IBS


Song:2017:PPF


Sheldon:2012:IWN

Sha:2019:CED

Savas:2015:GMA

Su:2016:PSN

Song:2017:SSI
Jun Song, Fun Yang, Kimberley Raymond Choo, Zhijian Zhuang, and Lizhe Wang. SIPF: a secure installment payment framework for drive-thru Inter-
Seo:2013:PIC

SoltaniPanah:2019:CDG

Song:2017:SAM

Shuai:2019:AAS

Shen:2017:RDP

Sui:2014:DAH
Yan Sui, Xukai Zou,


REFERENCES


REFERENCES


[Tau:2010:AWB]


[Tay:2011:DR]


[Tan:2015:CER]


[Tau:2019:SFE]

[Tan:2017:JDC]

[Tan:2014:DFS]

Haibo Tian, Xiaofeng Chen, and Willy Susilo. Deniability and forward secrecy of one-round au-


Sheng-Hua Teng. 2018


Tamir Tassa and Elad Gudes. Secure distributed computation of anonymized views of shared databases. *ACM Trans-


Tu:2013:PAQ


Tariq:2014:SBL


Tan:2016:ESE


Tetali:2013:MSA

1523-2867 (print), 1558-1160 (electronic). OOPSLA ’13 conference proceedings.

[Tang:2012:RSS]

[Tian:2017:RSP]

[Tsay:2012:VUL]

[Tsoutsos:2018:EDM]

[Tang:2015:ECP]

[Tormo:2013:IMP]
Gines Dolera Tormo, Felix Gomez Marmol, Joao Girao, and Gregorio Mar-

**Terrovitis:2011:LGR**


**Terrovitis:2012:PPD**


**Tao:2018:AAC**


**Tomb:2016:AVR**


**Toxen:2014:NSS**


**Tsougenis:2012:PEM**

REFERENCES

Tan:2016:BIB

Tang:2014:PAB

Taylor:2011:CAS

Tezcan:2016:IID

Tschorsch:2016:BBT

Taassori:2018:VRP
Meysam Taassori, Ali Shafiee, and Rajeev Balasubramonian. VAULT: Reducing paging overheads

**[Tao:2014:CFS]**


**[Toreini:2017:TRP]**


**[Tang:2011:IDC]**


**[Tso:2013:SAI]**


**[Tseng:2012:ERI]**


**[Tenca:2018:PIS]**

REFERENCES

Street, Suite 300, Silver Spring, MD 20910, USA, June 2018. ISBN 1-5386-2612-8 (USB), 1-5386-2665-9. ISSN 2576-2265. LCCN QA76.9.C62. IEEE catalog number CFP18121-USB.

Tseng:2015:LFI


Tsai:2010:RLI


Turan:2019:CFF


Thorpe:2012:CRB


Tupakula:2015:TES


[T]
REFERENCES


575

REFERENCES

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

Tan:2016:CCA


Tolba:2016:GMA


Trammel:2012:DTP


Tian:2017:ORA


Teh:2016:STD


Ehatisham-ul-Haq:2018:CAS

[uHAN+18] Muhammad Ehatisham ul Haq, Muhammad Awaís Azam, Usman Naem, Yasar Amin, and Jonathan Loo. Continuous authentication of smartphone users based on activity pattern

[Uzunkol:2018:SWU]

[Unruh:2015:RQT]

[Ueno:2019:TBP]

[Uto:2013:MRI]

[Ulutas:2011:MIS]

[Ulutas:2013:ISI]
REFERENCES

Vaikuntanathan:2011:CBN


Vaikuntanathan:2012:HCE


Vigil:2015:IAN


Valamehr:2012:IRM


Venkataramani:2016:DHC


Vatajelu:2016:SMB

[VDB+16] Elena Ioana Vatajelu, Giorgio Di Natale, Mario Barbareschi, Lionel Torres, Marco Indaco, and Paolo Prinetto. STT–MRAM-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability. ACM
vandeGraaf:2017:LTT


vanDam:2011:TQC


Visegrady:2014:SCV


Vergnaud:2017:CAB

REFERENCES


REFERENCES


[VKK+19] Katerina Vgena, Angeliki Kitsiou, Christos Kalloni-...

Vasiliadis:2017:DIS


Vleju:2012:CCA


Vivek:2014:CSC


Vleigen:2015:SRD


Veloudis:2016:NPH


Christine van Vredendaal. Reduced memory meet-in-the-middle attack against the NTRU private key. *LMS Journal of Computation and Mathematics*, 19
Van Dijkhuizen: 2018:SNT


Vazirani: 2019:FDI


Valente: 2019:SSA


Wagstaff: 2010:C


Wagner: 2016:TPF


Woo: 2019:UEM

Walter:2018:RCS


Wang:2010:NSB


Wang:2013:CRA


Wang:2014:IIA


Wang:2018:LRI


Wang:2018:PPA


Weisse:2017:RLC


Wright:2010:USP


Wu:2018:ESS


Wang:2019:IFT


Wang:2018:SNU


Wei:2018:GCQ

Chun-Yan Wei, Xiao-Qiu Cai, Bin Liu, Tian-Yin Wang, and Fei Gao. A generic construction of quantum-oblivious-key-transfer-based private query...

**Wu:2017:HMA**


**Wang:2018:SEA**


**Wei:2012:NTB**


**Wazid:2019:DSK**

REFERENCES

Wazid:2018:AKM

Wang:2019:SFE

Wang:2013:SES

West:2015:EC

Wess:2016:JWM
Wang:2018:ERS


Wang:2016:SSS


Wang:2010:DVT


Wang:2012:BRR


Wang:2012:SPB

Wang:2017:DRM


Wang:2017:DVP


Wei:2016:PAB


Wei:2017:CES


Wei:2018:GAD

REFERENCES

DEN IFCS EN. ISSN 0129-0541.


Winder:2017:ROS


Wang:2019:MBN


Wang:2018:VMF


Wang:2016:DRS


Wu:2011:HQI


Weissman:2011:LLB

Wang:2012:MCE


Wu:2019:VFS


Wei:2012:IRK


Wang:2011:RBM


Wang:2017:CAS


Wang:2013:HCL

Wei:2015:FST

Wei:2014:EEF

Wang:2011:HAB

Wu:2015:TRM

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

Wang:2016:LLE

Wang:2012:RTC
Liyun Wang, Hefei Ling, Fuhao Zou, and Zhengding

[Wang:2017:PPD]


[Wang:2017:CES]


[Wu:2012:PSC]


[Watanabe:2014:OAC]


[Won:2016:PAA]

REFERENCES


Peter Williams and Radu Sion. Access privacy and correctness on untrusted


[Wu:2016:BPK] Qianhong Wu, Yang Sun, Bo Qin, Jiankun Hu, Weiran Liu, Jianwei Liu, and Yong Ding. Batch pub-

Watanabe:2012:ITT


Wei:2019:VFA


Wang:2012:PAC


Wu:2010:EUA


Wu:2010:IBM

REFERENCES


REFERENCES

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


Wang:2019:CSS


Wang:2019:NTB

REFERENCES


**[WY+13]** Xiangyang Wang, Hongying Yang, Jing Wang, Lili Chen, and Panpan Niu. Bayesian segmentation based local geometrically invariant image watermarking. *Fundamenta
REFERENCES


Wang:2014:CGR


Wang:2017:RRA


Wen:2011:DSH


Wei:2015:CPK


Wang:2016:SAP


Wang:2018:AMB

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Xu:2016:CCP

Xiong:2017:CCC

Xia:2016:SDM

Xie:2014:SCP

Xu:2018:SKS
JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).


Yang:2010:PII


Yang:2011:PQC


Yang:2014:BEB


Yang:2011:GSS


Yang:2012:PST

Yang:2016:EBB


Yi:2017:ZCL


Yuan:2013:PVQ


Yuen:2012:IBE

Yu:2017:PDA


Yasuda:2015:MQC


Yao:2019:CTC


Yasuda:2015:MQC


Yao:2019:CTC


Yan:2016:DEB


Ye:2010:ACC


Yamada:2012:PBR

Takaaki Yamada and Isao Echizen. PC-based real-time video watermark embedding system independent of platform for parallel computing. Lecture Notes in Computer Science, 7110:15–33, 2012. CODEN LNCS0D. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
Ye:2014:NIE


Yekhanin:2010:LDC


Yoshida:2012:OGT


Yu:2012:EPF


Yang:2017:CCS


Yang:2018:RRE

References


Ye:2016:IEA


Ye:2017:VCS

Yang:2016:IHA


Yu:2010:IBF


Yang:2016:EHA


Yao:2019:RSA


Yang:2014:MDF


Yamada:2017:EPA


(print), 1875-8681 (electronic). See erratum [YFK+12].

Yum:2012:OPE


Young:2013:TPC


Yang:2018:AIW


Yang:2019:NAK


Yi:2013:ETS


Yu:2016:CBE


Yagan:2016:WSN


Yan:2018:FPS


Yao:2019:ACC


REFERENCES


[2012] Kazuki Yoneyama. One-round authenticated key exchange with strong forward secrecy in the stan-

**Yang:2017:SAS**


**Yang:2012:EMA**


**Yin:2017:QPE**


**Yin:2019:SCM**


**Yengisetty:2011:AVC**

Yi:2016:IPA


Yang:2012:SAK


Yumbul:2015:EEP


Yang:2015:EPS


Yang:2016:ECV


Yang:2018:HEP

Kun Yang, Haoting Shen, Domenic Forte, Swarup Bhunia, and Mark Tehranipoor. Hardware-enabled pharmaceutical supply chain security. ACM Transac-
Yang:2019:ISO


Yeh:2010:TRR


Yuen:2014:TCT


Yang:2011:CCK


Yao:2014:NCR


Yeh:2010:TRR


Yuen:2014:TCT

REFERENCES

Yang:2011:CPK


Yamada:2012:UEW


Yi:2016:VSF


Ye:2018:VBA


Yeh:2017:SIB


Yang:2014:IBI

Yang:2011:ACD


Yasuda:2012:ASM


Yang:2018:IAC


Yan:2019:IFF


Yao:2010:IDA


Yao:2010:ASP

Yan:2017:PIS  

Ye:2019:NCA  

Yang:2015:RCI  

Wang:2011:RDA  

Wang:2013:RBC  

Yu:2012:NWM  
Yang:2010:CRS


Wang:2018:CIW


Yang:2019:SCC


Yan:2012:SMA


Yu:2012:SME


Yang:2018:EEC

Wencheng Yang, Song Wang, Guanglou Zheng, Junaid Chaudhry, and Craig Valli. ECB4CI: an enhanced cancelable bio-

Yu:2016:CDI


Yang:2018:PBC


Ye:2018:ISS


Yoon:2011:SBC


Yoon:2013:RBB


Yang:2012:LUC

Yang:2016:EPA

Yu:2019:PSI

Yan:2019:HDS
REFERENCES

Yang:2018:CDD

Yang:2012:BPN

Yang:2012:NIB

Yang:2014:PST

Zhai:2017:EEI
[ZAAB17] Xiaojun Zhai, Amine Ait Si Ali, Abbes Amira, and Faycal Bensaali. ECG encryption and identification based security solution on the Zynq SoC for connected health systems. Journal of Parallel and Distributed Computing, 106(??):143–152, August 2017. CODEN JPD CER. ISSN 0743-7315 (print), 1096-0848 (elec-


Zhang:2013:RMS


Zhang:2015:PCL


Zhang:2012:TCS


Zhang:2014:GCS


Zhang:2019:EPK


Zhang:2014:IAI

Zhi-Kai Zhang, Michael Cheng Yi Cho, Zong-Yu Wu, and Shiu Lap Ying Winston Shieh. Identifying and authenticating IoT ob-


[ZDW+16] Yunya Zhou, Hua Deng, Qianhong Wu, Bo Qin, Jianwei Liu, and Yong Ding. Identity-based proxy re-encryption version 2: Making mobile access easy in cloud. *Future Generation Computer Systems*, 62(??):128–139, September 2016. CODEN FG-
Zetter:2014:CZD


Zhou:2018:SAE


Zhou:2018:HFD


Zhao:2010:PSA


Zhou:2016:HFD


Zhang:2018:AAG

Qikun Zhang, Yong Gan, Lu Liu, Xianmin Wang, Xiangyang Luo, and Yuanzhang Li. An authenticated asymmetric group key agreement based on attribute encryption. *Journal of Network and Computer Applications*, 123(??):1–10, December 1, 2018. CODEN JNCAF3. ISSN 1084-8045.
REFERENCES

Zhang:2018:PPE


Gao:2012:DES


Zadeh:2015:ASP


Zhang:2012:LDC


Zhang:2015:BYO


Zhang:2015:STR


Zhu:2015:IDM

Zhu:2013:TSC


Zhu13


Zhou:2015:EPP


Zimand:2010:SEC


Zuo:2019:WDH


Zhang:2011:FBP
Zeng:2014:NFC


Zhou:2012:CBF


Zhang:2019:CCF


Zhou:2015:PPS


Zhao:2012:IAS


Zhao:2014:TAH

Yifan Zhao, Swee-Won Lo, Robert H. Deng, and Xuhua Ding. Technique for authenticating H.264/


Zhou:2019:LIB


Zhang:2016:TLT


Zhang:2018:SPF


Zhang:2017:FGA


Zhang:2010:NSS


Zielinska:2014:TS

REFERENCES


REFERENCES

Zheng:2016:EUV


Zhao:2012:SSS


Zhou:2017:IBB


Zenger:2016:AKE


Zhang:2016:SBA


Zhang:2015:MAA

REFERENCES


REFERENCES


Zhu:2015:PPD


Zwattendorfer:2012:CBL


Zhang:2016:EEA


Zhou:2016:SRB


Zhang:2016:FAA

Zhiyong Zhang and Kanliang Wang. A formal analytic approach to credible potential path and mining...

[**Zhang:2014:LFL**]


[**Zilberberg:2013:PCM**]


[**Zhang:2011:AGK**]


[**Zhang:2015:FER**]


Zhou:2018:QTA


Zilberberg:2013:PCM

REFERENCES

Zhang:2017:FBI


Zhang:2013:LPP


Zhang:2019:MAA


Zhang:2017:FWI


Zhang:2017:RIW


Zhou:2011:PSA


Zhang:2016:PAG

Yuexin Zhang, Yang Xiang, and Xinyi Huang.


Zhan:2018:EKG


Zhou:2018:CLR


Zhou:2019:CLR


Zhou:2019:GCC


Zhang:2010:ASL


Zhou:2019:GCC

Zhang:2013:BLR


Zhao:2019:LRC


Zhang:2019:LRH


Zhang:2011:EPK


Zhao:2012:FCS


Zhang:2015:ITS

Jie Zhang and Futai Zhang. Information-theoretical secure verifiable secret sharing with vector space access structures over bilinear groups and its applications. Future Generation Computer Systems, 52(??):109–
REFERENCES

Zheng:2015:EPT

Zhou:2017:ENQ


Zaidan:2017:NDW

Zhu:2018:CAC

Zhu:2019:ICR
Youwen Zhu, Yue Zhang, Xingxin Li, Hongyang Yan, and Jing Li. Im-

**[ZZM17]**


**[ZZQ+19]**


**[ZSY+19]**