Title word cross-reference

(t, n) [QDW09], 2w [Bae10], k [BDD01, MU18, RMSCR19], n [CC12], O(n) [DYDW10], t [BDD01].

-anonymization [MU18, RMSCR19], -ary [Bae10], -database [BDD01], -Diffie [CC12], -private [BDD01].

.NET [KKKV07].

/SSL [BJ16].

1 [KJS17], 11770 [CH16].


3 [ABM+12], 3GPP [EWR+09].

88 [vOLW05].

AAanA [SK14], absence [AvO13], absolute [AvO13], abstract [BLM11, DM07, MS14],
abstract-based [BLM11], abstraction [MLCS16], abused [CYA+18]. Acceptable [BB04b]. Access
[loP18, SAL17, ACF17, ACBC+15, BLM11, CF03, CK08, CZ06, HSMY12, JSMG18a, KAC16, KAC17, Kud02, LD17, LRB+10, MS15, Pen12, PMPGMLLM12, RD16].

account [BRS06], accounts [ASN+16], accreditation [DFBJR18], Accumulable
[CL08, Fon08]. **capacity** [SJ09]. **capture** [MR03]. **card** [ABFL12, DMDM16, GdKGV14, MS14, MLM19]. **card-based** [MS14]. **cards** [MPP14]. carried [QLOW09]. **cascade** [WPD18].

cascade-instantiable [WPD18]. **case** [BSCZ11, GLMS+04, SKK+17]. cases [Pla09]. **cash** [LCL14]. **CASSANDRA** [MCD11]. cast [YYK+18]. **CCA** [PPSS13].

CDH [HIST09]. **ceremonies** [MdSC+15]. **Certificate** [MFES04, CLPP11, Rus04, Ust11]. certificate-based [Ust11]. certificate-free [CLPP11]. **Certificateless** [ZWQ+17, CFG17, Den08, FGS12, SSP14]. **certification** [BCF+17, LMM004]. certified [IZS08]. chained [DZW+18].

challenges [HC10]. **channel** [DSFK19, HS15, KDYS19, MSK16, MS09, MTW+14]. channels [DHW11, KKL17, KML03].

characterization [MSN02]. **check** [KO02]. **checker** [BMV05]. checking [AC08, GKB12, HL04, MS15, NST09, YAM+15].

checksums [GKK+10]. **CHES** [DSY06]. chosen [LLW+16]. chosen-ciphertext [LLW+16]. **cipher** [Lu09, TTS+06]. ciphers [CYK09, IMI18, KM10]. **Ciphertext** [JMSG18a, JMSG18b, LMG17, LLW+16].

Ciphertext-policy [JMSG18a, JMSG18b]. **ciphertexts** [JMSG18b, PPSS13]. class [DS07, MLCS16]. **Classification** [SAL17, CBC08]. classify [BEPL+17]. click [ALPW13, CFBv09, MBHT17, SGLC19]. click-based [CFBv09]. **clients** [SPDR17]. close [DHW11]. Cloud

[Abb13, ABN14, A014, BMP+14, CMMPS15, FSG+14, GMH14, HK19, KNL16, LZQ+18, MSGCDPS18, PLL15, VHL19, WMS+19, YAM+15]. **cloud-based** [KNL16]. clustering [BT07, RMSCR19, SKK+17].

clustering-based [RMSCR19]. co [BMP+14, PLL15]. **co-residence** [PLL15]. co-resident [BMP+14]. code [DMDD16, HZL+17, KKKV07]. codes [CL13, Nui12]. **coding** [EHR17, TWP08].

coding-enabled [EMR17]. **collection** [SV11]. **Collision** [MS09, CHKO12, KW15]. **collision-resistant** [CHKO12]. collision [DdP13, Nui12]. collusion-secure [Nui12].

Colored [SSF15]. **coloring** [RS18]. column [CMS10]. **combinations** [KAC17]. combinatorial [CMR06]. combining [SSE+15]. command [SNX19]. **commerce** [ABF008, GLP03, ZGC07].

commercial [NVB+02]. commitment [GSS10, HCN15]. Commix [SNX19]. commodity [TND+15].

commodity-based [TND+15]. common [DMP13]. communication [CPPK15, GBG18, KCB17, LMD17, VdW14]. communication-efficient [LMD17].

communications [MB16]. Comparing [BBR18]. comparisons [AL05]. compatible [LI07]. Complete [ABCC08, BB04a, LCL14, MSN02].

completeness [WH58]. **compliance** [CCD+07]. **Compliant** [DVBO2]. components [AV17]. composability [Vaj16]. composable [BFS+13].

comprehensive [BF13, LRB+10, SE09]. compressing [MP16]. compression [RSMA19]. compromised [SPDR17].

computation [ABB17, BNTW12, Pen13]. Computational [BP04, LCL16].

computations [BGP07b, KU16]. compute [MCD11]. Computer [Lau01, BCEM04, LL14, vORM06].

Computing [BJ15, A014, LI07, PRI04]. concept [Sen14]. **conceptual** [JGK14]. Concrete [BLM11, BCL09]. Concrete-[BLM11], concurrent [ASAAS15].

Conditional [BDHK08]. **conditions** [BDPV14, sLC05]. Conference [CL09].

confidential [HN14]. **confidentiality** [BB04a, KNL16]. configuration [ABR16, ABC08]. confinement [Fon08, SPM13, SS05b]. confirmation [PSDNSAHJ19]. conflict [RV03].
conjunctive [LZQ+18]. connection
[LSWW14, SS05a]. connection-based
[SS05a]. considering [TTS+06]. constant
[BGP07b, PPSS13]. constant-round
[BGP07b]. constant-size [PPSS13].
constants [BR17]. constrained [SS17].
construct [YSM10]. construction
[Ala17, BGKZ12, NSNK06, YYY+18].
constructions
[HSMY12, KME+16, ZVH15]. consumer
[LKH09]. consumption [RBEH15].
consumption-based [RBEH15]. contacts
[DMP13]. containing [IT05]. Content
[BFP03, HC10, LKH09, Pla09].
Content-based [BFP03, HC10]. context
[DGF+17, HS09, JGK14]. context-aware
[DGF+17]. context-sensitive [HS09].
contextual [CCB08]. continuous [EG18].
contourlet [SJ10]. contract [IZS08].
contracts [GYL+07]. Control
[LMMS17, SAL17, ACF17, AJC+09, Ano11b,
ACBC+15, BLM11, BNN04, CF03, CCD+07,
CK08, CZ06, HS09, HSMY12, KAC16,
KAC17, KLMM09, Kud02, KNL16, LRB+10,
MS15, Pen12, RM12, TZH04, ZM07].
Controlled [BB04a, BFG+13, SM10].
conversations [DBMS10]. convertible
[Lin15]. convex [ALPW13]. cookie
[ACB14]. cookie-based [ACB14].
cooperation [AGIK07]. coprocessors
[Smi04]. correcting [KM07]. cost
[DRPW12, DYW10]. cost-benefit
[DRPW12]. counter [BF13].
counter-measure [BF13].
countermeasure
[GBDJ14, MTW+14, Pen11].
countermeasures [Bae10]. Counting
[KM10]. country [SKK+17]. cover [SJ10].
COVERAGE [AGIK07]. covert [DHW11].
Cracker [SGE02]. credential
[AYHK18, ABFL12]. credentials [SF17].
Critical [EEB+15]. cross [PMPGMLM12].
cross-layer [PMPGMLM12]. CRT
[OT06]. CRT-based [OT06]. CRUST
[GW09]. Cryptanalysis
[ALPW13, DSY06, MS11]. Cryptanalytic
[CJMS19]. Crypto [Yon06]. cryptographic
[ARML06, BPW05b, BGK08, BDS+10,
DFF+16, DSRHC16, GW09, JCL+18, KU16,
Küs05, MR03, MS14, MSGCDPSS18].
Cryptographically [BCJ+11].
cryptography [ALOW15, LP11].
cryptologic [DVB02]. cryptosystem
[HCN15, IT05, MS11, SGE02].
cryptosystems [KG11, NMBB12, OT06].
Cryptoviral [Yon06]. CSOC
[SGJC18, SGJ19]. cuckoo [VH19]. current
[HC10]. Curve [JMV01]. curves
[HMC04, KSZ07]. Cyber [SSD14].
Cyber-attack [SSD14]. cycle [AYHK18].
damage [WGMB13]. DAMe
[PMPGMLM12]. Data [LMMS17, SV11,
SAL17, VdWZ14, ACF17, ABN14, BS05,
BNTW12, BDH+10, CTM+16, EMRN17,
EAH+07, GSAMCA18, GKS19, HIDC15,
HK19, HH16, Küs05, LD17, MSGCDPSS18,
OSSK16, SMMN12, VH19, YAM+15, ZO13].
Database [KS10, BDD01]. databases
[BW08, CMS10, EAH+07, HN14]. dataset
[NRC15]. datasets [MU18]. day [DGF+17].
dealership [GSP+16]. decentralized
[LLWY09]. decidability [Küs05]. decision
[WP18]. dedicated [ZZG19]. Defeating
[DSB19]. defending [SK06]. defense
[MYLZ14, VSR15, WR08, ZJR14]. defenses
[LLWY09]. Definition [TMP13]. degree
[SSVC16]. Delay [Z013]. Delay-sensitive
[ZO13]. delegatability [HYWS11].
Delegation [CK08, BGTCCBB10, CON09,
GOBdi11, WZ07, ZZG19]. delegations
[RV03]. deniable [GCH+19]. Denial
[LLWY09, WR08, TGS17].
denial-of-service [WR08]. dependence
[HS09]. dependencies [ACF17].
dependency [CMS10]. dependency-based
[CMS10]. Deployment
[ACBC+15, HIDFGR19, Das12]. depth
dynamicity [AIC18]. dynamics [MRW02].

E-business [KBH07]. E-cash [LCL14].
e-commerce [GLP03, ZGC07].
eduroam [PMPGMLLM12].
eduroam/DAMe [PMPGMLLM12].
effective [MGR19, ZGC07]. Effectiveness [SK16, SGJC18]. effects [SV11]. efficiency [HMCDO4, MG17, PDB11, Pen13].
Efficient [HRL09, HH16, HYWS11, JCL+18, KJ14, KU16, KSZ07, LMG17, LBZ+10, MP16, NP01, RD16, SMMN12, Bae06, BR18, BCD+13, EMRN17, HN14, HYWS12, LMD17, LCL14, MCD11, Pen11]. effort [SGJ19]. eID [RLEM18]. Elastic [CYK09].
Electronic [GSM+11, ABFO08, BEDH15, DJN10, KO02]. E-Marcus [BR18]. elicit [SK16].
elliptic [HMCDO4, KSZ07, JMV01].
email [IZS08, WR15].
Embedding [BDH+10, SJ09]. enabled [EMRN17].
Enabling [BS05]. encapsulation [MPS14].
encapsulating [EHM15]. encrypted [CTM+16, DBMS10, GSAMCA18, HH16, KJ14, OSSK16, SEXY18, WPD18, WR15].
encryption [ARMLS06, BZ03, CC12, Den08, EHS14, FGS12, GMV05, GSP+16, HK19, IM18, JCL+18, JSMG18a, JSMG18b,
KME++16, LMG17, LZQ+18, Lin15, PPSS13, QLZ15, QDW+15, SSP14, YP06, ZZG19, ZVH15, LLW+16, Dan07]. end [BB04b].

ended [Küis05]. energy [RBEH15].

enforced [BM11]. enforcement [ACMV15, AICC18, BCL13, DLR15, LBW05].

enforcing [BB04a]. engineering [GMMZ06, MLM19, SK16].

Enhanced [ABN14, YAM+15, LV10, MSP+13, JTV19].

Enhancing [ACB14, CLW+11, KLMM09].

Ensuring [SAT09, SGJ19].

enterprise [WYL+12].

Entropy [BEPL+17, HLKI15, SV11].

environment [CLW+11, GOBdIC11, LRB+10, NVB+02].

environments [FSG+14, GYL+07, LI07, PPL15, WAB+09].

epidemics [AGIK07]. equations [KM10, SSVC16].

Erratum [Roe11b]. errors [ABR16].

Escrow [ARMLS06, YSM10].

Escrow-free [ARMLS06].

ESORICS [Sne05].

establishing [Abb13]. establishment [BVS07, Das12, YRW14].

Estimating [AD08, WHS18]. estimation [RMPADF13].

EUFORBIA [BFP03]. evading [XCW+12].

Evaluation [AvO13, AKG16, BBD04a, HIDDGHR19, RHL17, SK06, SNX19, TND+15].

evenhandedness [IZS08].

events [RHGTC17]. evidence [SdHZ16].

evidence-based [SdHZ16].

EXAM [LBW+10]. exchange [AvO13, AKG16, BBD04a, HIDDGHR19, RHL17, SK06, SNX19, TND+15].

Excursus [Fra18]. Execution [SK06, MLO+04]. exhaustive [KJS17].

experimental [BCD+13, DBS19].

experiments [QLOW09]. explicit [KAC16].

exploitation [JM17, MLM19, SNX19].

exploiting [ACF17]. exploits [ZRJ14].

exploring [HS15]. exponentiation [Bae10].

expression [WR15]. expressive [RD16].

extended [ACF17, BGTCBB10, Lop18, MS15].


FA [Bae10]. facets [BFT08, QLOW09].

facets [AKG16]. factor [CG14, ML17].

failures [SK06]. Fair [KM03, DGZFGH13, GRV05, HYWS12, SEXY18, SGJ19].

familiarity [ZGC07]. familiarity-based [ZGC07]. family [AMP12, MSN02]. fault [CL09, GKS19, RB02]. fault-tolerance [CL09]. fault-tolerant [GKS19, RB02].

FCS [ACM05]. FCS/VERIFY [ACM05].

feature [YP06]. federated [WW07].

federating [PMPGM11]. file [SLC05].

file-based [SLC05]. filter [MB16, VH19].

filtering [BFP03]. find [SSVC16]. fine [KLMM09]. fine-grained [KLMM09].

fingerprint [CC10, Nui12]. finite [BCL13].

firewall [ABR16, KNL16, MWZ06]. first [LM06]. first-order [LM06]. fixed [HMCD04].

Flexible [JSMG18b, QDW+15].

floating [ABB17, KW15]. floating-point [ABB17].

Flow [HS09, SdHZ16, BMP+14, BNN04, ZM07].


form [DP13]. Formal [ACMV15, GKS12, Yon18, dAKdG10, CMN+18, KAC17, NSN06, PDB11, RV03, VdWZ14].

formalism [GBDJ14]. formalization [MS14]. forward [CDF+13, KME+16].

forward-secure [KME+16]. four [Dan07].

Fractional [BCA+10]. framework [Abb13, ABFL12, BFT08, KNL16, MB16, MLO+04, RV03, Vaj16, VdWZ14, WR08, WHS18, XSA13, ZRJ14].

free [ARMLS06, BGKZ12, CLPP11, YRW14].

freeness [HIST09]. friendly [CLPP11].

Fujisaki [GMMV05]. full [Bra06]. Fully [CDF+13]. function [BGKZ12, SB14].

functionality [SPM13]. functionally-based [SPM13]. functions
Incompleteness [SAL17].
Inconsistency [SAL17].
inductive [MP15].
inference [AJC+09, JG15].
Information [KBH07, TND+15, ASF04, AD08, ABFL12, BDHZ15, BB04a, BDD01, CMMPS15, DdP13, DBMS10, EFH09, GI19, HS09, IHNT02, KPM12, LMD17, LeSCL+18, MU18, Nam06, Pia09, WHS18, ZM07].
infrastructure [CLPP11, TMP13, Gri06].
Infrastructures [EEB+15].
injection [DSB19, DTK+18, SNX19].
Insider [YP12].
inspection [BDF04].
inspiration [SS17, ZZW+10].
instance [Sen14].
instance-weighted [Sen14].
instances [BMP+14, JG15].
instantiable [WPD18].
instantiations [CYK09].
Instruction [DM07].
Instruction-level [DM07].
insurance [GYL+07].
Integrating [Ust11, ZGK07].
Integrity [MI18, LZQ+18, EEB+15, Lvk18, Yam+15, Eeb+15].
integrity-checking [Yam+15].
Integrity-OrBAC [EEB+15].
Integrity-verifiable [Lzq+18].
i intelligence [KKK17].
Intelligence-based [KKK17].
Interacting [vOlw05].
Interactive [MS09, CDF+13, CHZ16, CL09, EHSS14, MS09].
intermediaries [DGZFGH13].
International [KBH07].
interpretation [DM07].
intersection [MCD11].
intrusion [AYHK18].
Intrusion [BT07, MCh01, Wab+09, CL08, KKK17, KSM10, RBEH15, TLX09, Vl13, ZGK07].
intrusions [MYLZ14].
Investigating [ASAA15].
investigation [SGJ19].
investigations [JG15].
Intrusion [VH19].
labels [ZM07].
Large [TLX09, Das12, Rlem18, SMMN12].
Large-scale [TLX09, Das12, Rlem18].
Lattice [GCH+19, SPIP14, BBR18].
Lattice-based [GCH+19, SPIP14, BBR18].
lattices [KJ14].
layer [DGF+17, PMPGMLLM12, WR08].
leakage [AD08, DdP13, DBMS10, WT16].
leakage-resilient [WT16].
learning [GSAMCA18, GBg18, KA18, SSE+15, TLX09].
legal [LeV07].
length [Yov09].
Less [BFS+13].
level [DM07, SCL+18, SGJC18].
library [BPW05b].
Lightweight [RBEH15].
like [ASN+16].
Limits [BP08].
line [BCD+13, LMMO04].
link [DMDD16].
Link-time [DMDD16].
linkability [BFG+13]. Linkable [GP17].
Low [BGP07b, GS15, MU18, SSVC16]. low-deterministic [GS15]. Low-randomness [BGP07b]. LPN [RG13].
LTE [LSWW14]. MAC [EMRN17]. MAC-based [EMRN17]. machine
[GSAMCA18, KA18, MS14, SSe15]. machine-learning [SSe15]. machines [MLCS16, vOLW05]. Making [BR17].
MALICIA [NRC15]. malicious [ABB17, BRSO6, CMS10, GPS17, RHTGSC17, WGMB13]. Malware [HLK15, MLCS16, BEPL17, BDMM19, SSK17, VPI15, ZRJ14]. manageability [TG05]. Management [CF03, ASF04, BF13, CH16, GMMZ06, GH05, LIWW09, Lop18, LcSCL18, NA14, RHL17, RLEM18, RBD02, SSN15, Tmpr13, VdWZ14, WPD18, WW07, dAKdG10, vOLW05]. managing [AMLH18]. mandatory [DLR15]. Markov [ABB17, RHL17]. masquerade [Sen14]. matching [FHV18, SBB19]. MaX [BFP03].
[EWZ+09, FN19, LMMS17, ACB14, AKG16, AMRR17, CF07, GSM+11, GCSABdSS12, HIDFGHR19, HC15, HZL17, IDHRPC15, LC14, LH15, LL15, LV10, MTSH18, VGMB13, BT07, SSe15]. mobile-phone [WGMB13]. Mobile-Sandbox [SSe15]. MobileTrust [LV10]. model
[ASF04, Ala17, ABB17, AC08, BMV05, BGTCBB10, BCOER04, EEB+15, GMMZ06, Gol12, GYL07, GKB12, HL04, JGK14, Kud02, LH15, MDS+15, NSK06, QLOW09, SK16, SPM13, SSP14, TD15, YLL18, ZCG07, ZZW10]. model-checking [AC08]. model-oriented [SK16]. Modeling [CCB08, DLR15, ACVM15, KAC17, Yon18]. models
[BT07, EHM15, KWCK19, OSSK16, YYY18, ZZW10, BNTW12, BT08, CON09, Dac12, GMH14, KM03, PGMLK+13, QLZ15, QLOW09, WR08]. multi-authority [QLZH15]. Multi-cast [YY18]. Multi-device [KWCK19]. multi-domain [CON09, PGMLK+13].
multi-domains [GMH14], multi-faceted [BFT08, QLOW09]. Multi-hop [BT07].
Multi-keyword [OSK16], multi-layer [WR08], Multi-Net [ZZW+10],
Multi-operator [EHM15], multi-party [BNTW12, KM03], multi-phase [Das12],
multiagent [ZGC07], multicast [MP15, PJ10, TWP08], multicast-based [MP15],
multicoupon [HIDFGHR19], multifactor [IT05], multiple [CC12, HMCD04, WMS+19],
multiple-key [CC12], multiplication [YOV09], multiplications [HTM11], multipliers [YOV09],
multiresolution [VSR15], multiset [BA16], multisignatures [HRL09], must [ASN+16], Mutual [HZZ+17],
naive [Sen14], names [CYA+18], need [JTV19]. Negative [EFH09, EAH+17, DNF+19],
negotiation [KLMM09], negotiation-based [KLMM09],
Net [ZZW+10, WYL+12], Nets [SSF15],
Network [GPS17, ABCC08, BMP+14, CL09, EMRN17, GBG18, GH05, LBZ+10, wLW05, MYLZ14, PMPGMLLM12, RS18, SAT09, TLX09, WYL+12, dAKdG10],
Network-based [GPS17], Networked [MR03], networks [ACB14, CMR06, CPPK15, Das12, DRPW12, EHM15, EMRN17, FN19, Go12, GBG18, RBEH15, RMSCR19, SS17, SSN15, SF17, YRW14, ZXZ+11, BT07]. next [AMLH18], next-generation [AMLH18],
NICs [CBC08], NIZK [WT16], no [BB04b, CMN+18], noise [EG18], noisy [BDH+10, KML03], non [CDF+13, CHZ16, CL09, EHS14, GRV05, HYWS11, KM03, MP16, RMSCR19],
non-compressing [MP16], non-delegatability [HYWS11],
non-deterministic [RMSCR19], non-interactive [CDF+13, CHZ16, CL09, EHS14],
non-repudiation [GRV05, KM03],
noninterference [BP04], note [ZHH08],
Nothing [MTW+14], notions [BCL09, BFS+13], novel [KLN16, Lin15],
numerical [SMN12, ZO13], obfuscation [OSK16], object [HS09, SS05b],
object-sensitive [HS09], oblivious [BA16, HSMY12, LD17, TND+15], obtain [Bra06]. Off [BCD+13, CJS19], Off-line [BCD+13], Off-line/on-line [BCD+13],
Offline [MWZ06, LMG17, LBZ+10], OFMC [BMV05], Ohgishi [CHZ16],
Okamoto [GMMV05], on-line [BCD+13, LMM04], on-the-fly [CL13], one [GMS03, MLCS16, YRW14], one-class [MLCS16], one-pass [YRW14], onion [CDF+13, CFG17], OnionDNS [SCL+18],
online [LMG17, LD07, LBZ+10], online/offline [LMG17, LBZ+10], only [LD17], Opacity [BKMR08], open [Küs05, RM12], open-ended [Küs05],
opening [EHS14], operational [SGJC18],
operations [BA16, HMM11, NRC15],
operator [EHM15], Optimal [DRPW12, EGH18, GYL+07, VSR15],
optimisation [PDB11], optimistic [DGZFG13, HYWS12, SEXY18],
Optimization [MU18, LL14], oracle [HYWS11, You18], oracles [HSMW08, HYWS12],
OrbAC [EEB+15, GBDJ14], order [LM06],
oriented [SK16, WW07], OSBE [HSMY12],
Outbound [Sm104]. Outsourced [FHV18, CTM+16, LD17], outsourcing [AL05, GYL+07, HJDC15, KU16], overview [BMP05], Own [ACMV15],
packets [vORM06], packing [BEPL+17],
pads [dSFK19], pages [SGLC19], Paillier [NSNK06, DJ10],
Paillier-based [NSNK06], pairing [MSGCDPSS18, YRW14, ZHH08].
pairing-based [MSGCDPSS18].
pairing-free [YRW14]. pairings
[BCL09, CCS07]. papers [ACM05].
paradigm [BCD+13]. parallelism [SBB19].
parallelizable [MP16]. parameter
[DTK+18]. parameters [NMBB12].
parazoa [AMP12]. parties
[HZL+17, KPM12]. party
[BNTW12, KM03, LCL16, MR04]. pass
[YRW14]. Passive
[CBC08, SS05a, ALOW15].
passwords [MPS10, MRW02, CG14, CJMS19, GTM11,
KJS17, Lop18, MSKD16, SB09, WLLW14].
Password-authenticated [MPS10].
passwords [CFBvO09, JTV19]. past
[JG15, LMMP06]. patching
[JM17].
pattern [FHV18, OSSK16, SBB19]. patterns
[CFBvO09]. pay
[Roe11a, Roe11b, DZW+18]. pay-TV
[Roe11b, Roe11a, DZW+18]. PBAC
[Kud02]. perception
[MTSH18].
Perceptrual [SB14]. Perfect [Hub12].
performance [BRR18, BNTW12,
HIDFGHR19, IDHRPCMP15, SK16, SSN15].
Periodicity [JM17]. permutations [BR17].
personal [IHNT02, QLZH15]. personality
[PPL15]. Petri [SSF15]. phase [Das12].
phone [CF07, GMS+11, HCN15, WGBM13].
phylogeny [BDMM19]. physical [SM10].
physically [BR17]. PIN [dSFK19]. PINs
[MTSH18]. PLOAs [Yon18]. PIR
[DYDW10]. pirates [Nui12]. PiSHi
[MBHT17]. PKI [BB04b, Daw04, LC04,
LMMP06, LMM004, VSM06]. PLAID
[DFR+16]. Plaintext [MPS14]. platform
[IDHRPCMP15, MBRPS18]. platforms
[KPM12, RHGTSC17]. point
[ABB17, KW15]. policies [ABCC08,
ACMV15, AICC18, BCL13, CF03, CCB08,
KAC17, LBW05, LRB+10, RRI+19, SB09].
Policy [SAL17, BVZ05, GMH14, JSMG18a,
JSMG18b, KNL16, MS15, TG05, XSA13,
dAKdG10]. PolicyUpdater [CZ06].
pollution [EMRN17]. Polly [SGE02].
polymorphic [KJG+11]. polynomial
[SGE02, TND+15]. polynomial-based
[SGE02]. polynomials [GMS03]. Portfolio
[LL14]. posteriori [ACBC+15]. potential
[WGMB13]. practicability
[IDHRPCMP15]. Practical
[LLV+16, ALOW15, GKS19, KOSU16,
LCL14, Pen12, VHT09, WR15]. practices
[LD07]. pre [CMR06, Pen13].
pre-computation [Pen13].
pre-distribution [CMR06]. Preface
[Ano11a, ACM05, BGP07a, BM05, Daw04,
DV08, DMRS07, Pri04, Sne05, Wai04, ZL06].
prefix [BGKZ12]. present [LMMP06].
preservation [RAC16]. preserve
[EBB+15]. preserved [JSMG18a, LD17].
preserving [ABFO08, BGK08, CTM+16,
DFBJR18, GKS19, HLS18, KOSU16, KB13,
KNL16, MB16, MCD11, NST09, NA14,
QLZH15, RDK18, WMS+19]. Preventing
[RAC16, PS17, YP12]. prevention
[PSDSNAHJ19, VL13]. primitives
[MP16, SM10]. principle [Bel10].
Principles [CGL+11]. Privacy
[KB13, MB16, MSP+13, NST09, QLZH15,
RDK18, ABFO08, AJC+09, AMRR17,
BGK08, BCA+10, BDHZ15, Bra06,
CTM+16, EG18, EAH+07, GLMS+04,
GKS19, GYL+07, KOSU16, KBB07, KNL16,
LD07, LD17, LeSCL+18, MCD11,
MBRPS18, NA14, PGMLK+13, RSPMB16,
RMPADF13, WMS+19, YAM+15, ZZG19].
privacy-aware [MBRPS18, RSPMB16].
Privacy-enhanced [MP+13].
privacy-preserved [LD17].
Privacy-preserving
[KB13, MB16, NST09, QLZH15, RDK18,
ABFO08, BGK08, CTM+16, GKS19,
KOSU16, MCD11, NA14, WMS+19].
Private [BA16, DMP13, BDD01, BGP07b,
KW15, LMD17, VH19, WR15].
Probabilistic
[DHW11, BP04, GYL+07, MCD11, PJ10].


QR [HBL17]. QR-code [HBL17]. query [BB04a, KCM+15]. queue [BF13].

race [SLC05]. RAM [LD17]. RAM-based [LD17]. ramp [LMD17]. random

BR17, BR18, Das12, HSMW08, HYWS11, HYWS12, VSR15, Yon18]. Randomized

ML14]. randomness [BGP07b]. ransomware [CMN+18]. rational

[ETAHCR08]. RBAC [BGTCBB10]. re

[GI19, Dan07]. Re-encryption [Dan07]. re-identification [GI19]. reacting

[AGIK07]. reactive [BDHK08]. Reactively

[BPW05a]. reader [GdKV14]. real


[GCSADB12]. recommender [ABFO08]. record [QLZH15]. records [QDW+15]. recovery [CMS10, NVB+02]. rectangle

[Lut09]. recursive [Rus04]. Redistributing

[LKH09]. refinement [dAKG10]. reflects

[PPL15]. refunds [KO02]. regions [EG18]. Regular [Bae10, WR15].

regular-expression [WR15]. rekeying

[PI10]. Related [Lut09, Dan07]. Related-key [Lut09]. relation

[MS11, Pen11]. Relations [FGS12]. relationships [CTM+16, RAC16]. relaxed

[BFS+13]. release [NAM06]. reliable

[ABCC08, AvO13]. remanence [SV11]. remote

[CGL+11, GW09, MMS16, YAM+15]. renewable [BDH+10]. repeated [VORM06]. Replacement [XCW+12]. representations

[EFH09]. repudiation [GRV05, KM03]. reputation [LI07, SDHZ16]. Requirements

[GMMZ06, WW07, SK16]. Research

[Gri06, RM12]. residence [PPL15]. resident [BMP+14]. resilient

[MR03, WT16]. resistance [TGS17]. resistant

[CHK012, SCL+18, MS09]. resolutions [RV03]. Resolving [CTM+16]. resource

[LVK18, SS17]. resource-bounded [LVK18]. resource-constrained [SS17]. resources

[TZH04]. response [SSD14]. Restricted

[SF17]. results [BCD+13, DLR15]. retention [GSM+11]. retrieval


searchability [HJC15]. searchable [HK19, LZQ+18]. searches [WR15]. searching [YH19]. Seberry [BZ03]. second [ABM+12]. secrecy [CDF+13, Hub12]. secret [DdP13, GMS03, HJC15, LMD17, PPSS13, QDW09]. secrets [BW08, JTV19]. Secure [ABB17, AL05, BSV07, DZ+18, HN14, HSMW08, KW15, LCL16, MSK16, SJ09, SBB19, XZX+11, ASF04, AIA17, BPW05a, BDF04, BNTW12, BT07, DdP13, KME+16, KU16, KSZ07, LCL14, LLW+16, MB16, MLO+04, MBRPS18, MPP14, NMBBI2, Nui12, PJ10, QDW+15, RG13, SJ10, SK16, SMI04, TND+15, WPD18, YYY+18, YAM+15]. secured [EHM15]. Securing [DDPS02, BFPP07, CC10]. Security [Ano14, BCL13, BDHZ15, FSG+14, GMH14, HJC15, OT06, ZZW+10, ACB14, ABC08, ABM+12, Ano11b, AC08, AICC18, BCJ+11, BGKZ12, BMV05, BR10, BCF+17, BFT08, BCL09, BFS+13, BNN04, BEM04, CLW+11, CFbVo09, CYK09, CLPP11, CCB08, DSB19, DM17, Den08, DRP12, EHM15, FGS12, GS15, GLMS+04, GYL+07, GRV05, GH05, HS15, HMCDO4, JKK14, KKKV07, KHB07, KLMM09, KMR09, Lan01, LBW05, LP11, LV10, wLW05, MdSC13, MP15, MSGCPS18, SNNK06, PDB11, RM12, RG13, RGL16, SK16, SS17, SSN15, SM10, SAT09, TG05, VSM06, WLY+12, WHS18, YLL+18, YRW14, YP06, ZM07, dAKdG10, vOLW05, BJ15, Pri04, KBH07]. security-mediated [VSM06]. security-sensitive [HS15]. seizure [SCL+18]. seizure-resistant [SCL+18]. selected [ACM05]. Selecting [NMBI2]. selection [GBDJ14, SJ10, SSVC16, ZGC07]. selective [ZZG19]. selective-ID [ZZG19]. SELinux [XSA13]. sellers [ZGC07]. semantics [KJG+11]. sensitive [HS15, HS09, RAC16, ZO13]. sensor [CMR06, Das12, KCM+15, LBZ+10, RBH15, YRW14, XZZ+11]. sensors
support [CON09, MLCS16]. supporting
[ARMIL06, JSMG18a, JSMG18b, RV03]. supports [WR15]. surfing [WLLW14].
surveillance [Lev07, LcSCL+18, MBRPS18, RSPMB16].
survey [Den08, FSG+14]. suspect [GBG18]. swarm [KKK17]. swarms [SS17].
symbolic [BMV05, BFT08]. Symmetric [BPW05b, HK19]. Symposium [BJ15].
System [JTV19, ABFO08, Ano11b, BFP03, BFPP07, CL08, CZ06, DmJS10, IZS08, KO02, KJS17, LKH09, LCL14, MGV17, MFES04, MS15, RM12, RLEM18, RBEH15, SSD14, VL13, vORM06, DNF+19].
System-assigned [JTV19]. system-based [MGV17]. systematic [SK16]. systems [ASF04, AMRR17, BDHZ15, BB04a, BCF+17, BmKM08, DSRC16, GMH14, HZL+17, Hub12, LKV18, LV10, RSPMB16, Roe11a, SK16, SV11, SS05a, ZGC07, dAKdG10, Roe11b].
theoretically [TND+15]. Theory [Rus04]. third [KPM12]. threat [MdS+15, YP12].
ubiquitous [LI07]. UC [BP08]. UMTS [LSWW14]. UMTS/LTE [LSWW14]. unauthorized [YP12]. Uncertain
[AJC+09]. uncertainty [SdHZ16].
unclonable [BR17, SM10]. Understanding [LM06, MS15, RSPMB16, WGM13].
undetectable [VHT09]. unforgeability [You18]. unification [KM07]. uniform [KAC16].
unifying [BCD+13]. universal [HSMW08, Vaj16, Dau17]. unknown [BEPL+17]. unmanaged [KKKV07].
Usage [LMMS17, SF17]. use [LMM04, Pla09, SK06, SS05b]. use-based [SS05b]. useful [HS04].
user-controlled [BFG+13]. User-friendly [CLPP11]. users [CF07, KOSU16]. Using [GB18, HTM11, RBD02, SJ10, Sen14, TZH04, ACB14, AMLH18, AGIK07, AICC18, ACBC+15, BMP+14, BCL13, BDMM19, CLW+11, CF07, DGF+17, EWR+09, GKKT10, GSAMCA18, GBDJ14, GKB12, HLKI15, HCN15, HL04, IDHRPCMP15, JCL+18, KJS17, KA18, KSM10, LM06, MB16, MSKD16, MP15, MP16, MLS16, QLZH15, RHL17, RRI+19, SSB15, SSD14, VH19, Yon18, You06, vOLW05]. utilising [LCPD14].

Verifying [MP15]. versus [MTSH18]. very [Bae10]. via [MTSH18, MS14]. victims [CMN+18]. video [LeSCL+18, MBRPS18, RSPMB16, SB14]. views [KMR09]. violation [GYL+07].

virtual [RM12]. visible [LC04]. Visualization [XSA13].
vulnerabilities [DTK+18, SNX19]. vulnerability [AV17, JM17, ML19, ZRJ14].

warning [ABFL12]. Watermarking [Fra18, BMP+14]. wavelet [KCM+15]. web [AYHK18, AV17, DTK+18, GLMS+04, MSKD16, SGLC19, BFP03, BJ16, EWR+09, KGG09, SNX19]. web-based [AYHK18].
weighted [Sen14]. wildcard [HH16]. WinRAR [YP06]. Wireless [BT07, CMR06, CBC08, EHM15, EMRN17, KKK17, LBZ+10, RBEH15, SS17, SSN15, YRW14, ZXZ+11]. Wirelessly [GdKGV14].
without [GW09, HSMW08, HYWS11, HYWS12, YSM10]. workflow [ARMLS06]. workplace [Lev07]. worm [AGIK07, KJG+11]. worms [vORM06].
Write [LD17, JTV19]. Write-only [LD17].

XACML [CON09, RRI+19]. Xen [PPL15]. Xen-based [PPL15]. XML [BFPP07, CF03, KMR09]. XOR [BP08, BGP07b]. XQuery [DTK+18].
XTEA [Lu09].

Yao [BPW05b, BP08]. Yao-style [BPW05b, BP08]. yoking [HLS18].

zero [DGF+17, PSDSNAHJ19]. zero-confirmation [PSDSNAHJ19]. zero-day [DGF+17]. Zheng [BZ03]. ZombieCoin [AMLH18].
References

Abbadi:2013:FET


Aliasgari:2017:SCH


Alfaro:2008:CAC


Ates:2012:WHI


Aimeur:2008:LPP


Andreeva:2012:SAS

Elena Andreeva, Andrey Andreeva.


Albertini:2017:EAC


Abe:2013:DTA


Aldini:2008:EMI

Anagnostakis:2007:CDR


Ayed:2018:ADS


An:2009:UIC


Anagnostopoulos:2016:NFM


Atallah:2005:SOS


REFERENCES


Anonymous:2011:P
[ANS+12]


Anonymous:2011:SIS
[Ano11b]


Anonymous:2014:SCC
[Ano14]


Ahmed:2012:MGE
[Irf12]


Al-Riyami:2006:EFE
[ARMLS06]


Ileana Buhan, Jeroen Doumen, Pieter Hartel,

**Backes:2008:CRS**


**Bertino:2015:SPE**


**Bernardi:2019:DMD**


**Bertoni:2014:SCS**


**Bella:2010:PGA**

Giampaolo Bella. The principle of guarantee availability for security protocol analysis. *International
References


Bat-Erdene:2017:EAC

Boteanu:2013:CSQ

Bertino:2003:CBF

Bertino:2007:SSP
Brzuska:2013:LMR

Bracciali:2008:SFM

Balopoulos:2008:SIP

Bagheri:2012:SFP

Backes:2007:P

### Ben-Ghorbel-Talbi:2010:DME


### Bella:2015:SIS


### Brown:2016:API


### Bryans:2008:OGT


### Bouzida:2011:CAB

Boyd:2005:PSI


Bielova:2011:DYR


Bella:2005:OVS


Bates:2014:DCR


Basin:2005:OSM


Buchholtz:2004:CCF

Mikael Buchholtz, Hanne Riis Nielson, and Flemming Nielson. A calculus for
REFERENCES


REFERENCES

Bononi:2007:IDS

Bohli:2007:SGK

Biskup:2008:KSI

Baek:2003:ZSP

Bai:2005:SAP

Chikha:2016:BBA
Corbett:2008:PCW

Chen:2010:HSS

Chen:2012:DHP

Cederquist:2007:ABC


Catuogno:2014:ATF


Cokер:2011:PRA


Camacho:2012:SAC


Chen:2018:MGE


[CG14]

[CGL+11]

[CH16]

[CHKO12]


**Crampton:2011:UFC**


**Chang:2011:EHS**


**Chen:2016:MGE**


**Casassa-Mont:2015:TSI**


**Cimitile:2018:TNM**


**Desoky:2009:LLB**


**Domingo-Ferrer:2018:DGS**


**Degabriele:2016:UPC**


**Duessel:2017:DZD**


**Draper-Gil:2013:OFE**

G. Draper-Gil, J. Zhou, J. L. Ferrer-Gomila, and M. F. Hinarejos. An opti-

Daza:2004:PUI


DiPierro:2011:PTC


Damgaard:2010:GPP


Dolzhenko:2015:MRE


DeFrancesco:2007:ILS


REFERENCES


Abdeljebar Ameziane El

Esponda:2009:NRI


ElSalamouny:2018:ONF


Egners:2015:MOW


Emura:2014:GSI


Esfahani:2017:EHM

Alireza Esfahani, Georgios Mantas, Jonathan Rodriguez, and José Carlos Neves. An efficient
REFERENCES


Estevez-Tapiador:2008:BRE


Elmufti:2009:MWS


Mohammad R. Faghani and Uyen T. Nguyen. Mobile botnets meet social networks: design and anal-


Gao:2019:LBD


Guerra-Casanova:2012:AMD


Gulyas:2019:HIA


Gutman:2005:RAN


Gritzalis:2012:FAR

Dimitris Gritzalis, Panagiotis Katsaras, Stylianos Basagiannis, and Yannis Soupionis. Formal analysis

**Gauravaram:2010:HFU**


**Gorrieri:2004:AAT**


**Gravigi:2003:ACP**


**Gouglidis:2014:SPV**

REFERENCES


**Gollmann:2008:E**


**Golic:2012:NAM**


**Gunther:2017:LMT**


**Garg:2017:NBD**


**Gritzalis:2006:PKI**


**Gurgens:2005:SFN**

Sigrid Gürgens, Carsten

...

Gihorn:2015:NAL


Gonzalez-Serrano:2018:SML


Glisson:2011:ERW


Gritti:2016:BED


Goldschlag:2010:THB

REFERENCES


Hoang:2015:GAM


Hu:2016:EWS


Hinarejos:2019:DPE


Hasegawa:2009:PFC


Hadavi:2015:SSS


Hiemenz:2019:DSS


Hopcroft:2004:ASA


Han:2015:MAU


Hitchcock:2004:ESM


Herranz:2014:SEA

Javier Herranz and Jordi Nin. Secure and ef-


REFERENCES


Isern-Deya:2015:PUG


Itakura:2002:PPI


Itakura:2005:PMB


Imamoto:2008:AEC


REFERENCES


Jiang:2018:FCP


Joudaki:2019:ETS


Karimi:2016:UAA

REFERENCES


Karimi:2017:FMA

Kundu:2013:PPA

Knights:2007:IJI

Kotzanikolaou:2017:BAR

Kozakevicius:2015:UQS
REFERENCES

Kulah:2019:SAD

Kate:2011:GCB

Kozina:2009:MIW

Kim:2014:EVE

Kong:2011:SSA


Steve Kremer and Olivier Markowitch. Fair multiparty non-repudiation protocols. *International Jour...
REFERENCES

Köpf:2007:TTU


Knudsen:2010:CEA


Kasamatsu:2016:TSE


Korzhik:2003:HAB


Kuper:2009:GXS

Kruko:2007:TS


Kurek:2016:TBC


Khayati:2016:PPP


Kontaxis:2012:MID


Kim:2002:NEC


Kundu:2010:DID

REFERENCES

Konstantinou:2007:EGS

Kiraz:2016:EVA

Kudo:2002:PPB

Kusters:2005:DCP

Kamm:2015:SFP
REFERENCES


REFERENCES


[LD17] Lichun Li and Anwitaman Datta. Write-only obliv-


REFERENCES


REFERENCES


REFERENCES


Li:2018:IVC


[LZQ+18]

Malhi:2016:PPA


Mehrnezhad:2017:PCI


Martinez-Balleste:2018:DIS


Marconi:2011:CPE

Luciana Marconi, Mauro Conti, and Roberto Di Pietro. CASSANDRA: a probabilistic, efficient, and privacy-preserving solution
REFERENCES


REFERENCES

Mousazadeh:2014:RGA


Mann:2017:TFA


Miao:2016:MDU


Mesbah:2019:REJ


Mana:2004:FSE

REFERENCES


REFERENCES


**MacKenzie:2004:TPG**


**Monrose:2002:PHB**


REFERENCES

Mizuki:2014:FCB

[MS14]

Mustafa:2015:UIA

[MS15]

Manulis:2016:SMP

[MSKD16]

Mizuki:2002:CCF

[MSN02]

Marmol:2013:PEA
Félix Gómez Mármol,

Mehrnezhad:2018:SPM


McEvoy:2014:ANT


Murakami:2018:OAA


Mayer:2006:OFA


Mu:2014:RBD

Chengpo Mu, Meng Yu, Yingjiu Li, and Wanyu


REFERENCES


REFERENCES


REFERENCES


Priami:2004:PSI

Poettering:2017:DAP

Pérez-Sola:2019:DSP

Qin:2009:SSS

Qin:2015:FAB

Quinn:2009:AAE
[ QLOW09 ] Karl Quinn, David Lewis, Declan O’Sullivan, and


REFERENCES


Ribeiro:2018:SRH

Reaves:2012:OVT

Rebollo-Monedero:2013:MPA

Ros-Martín:2019:SND

Roelse:2011:DST

Roelse:2011:EDS
Peter Roelse. Erratum to: Dynamic subtree trac-


Mohammad Hasan Samadani, Mehdi Berenji, and Marina Blanton. Secure

[SCL+18]

[Skoric:2016:FBR]

[Sen:2014:UIW]

[Seo:2018:AOF]

[Singh:2017:RUA]
REFERENCES


Steinwandt:2002:APB


Shah:2019:MEF


Shah:2018:MMM


Saini:2019:YCS


Sajedi:2009:SSB

REFERENCES


Lhee:2005:DFB


Skoric:2010:FDS


Sole:2012:EMT


Snekkenes:2005:PSI


Stasinopoulos:2019:CAE

Stevanovic:2017:MIC

Schreuders:2013:FBA

Serjantov:2005:PAA

Skalka:2005:SUB

Sampangi:2017:HSR

Shameli-Sendi:2014:ACA
Alireza Shameli-Sendi and

Spreitzenbarth:2015:MSC


Seifi:2015:ATA


Silva:2015:RMP


Sepahi:2014:LBC


Susil:2016:SSA

Petr Susil, Pouyan Sepehrdad, Serge Vaudenay, and Nicolas Courtois. On selection of samples in algebraic attacks and a new...


REFERENCES


REFERENCES


[Vajda:2016:ATA]

[VdWZ14]

[VH19]

[Vasserman:2009:IKN]

[Vrakas:2013:IDP]

[vonOheimb:2005:ASM]
David von Oheimb, Volk-
REFERENCES


**Waidner:2004:**

**Wang:2013:**

**Wangen:2018:**

**Wu:2014:**

**Lye:2005:**
REFERENCES


[Wu:2007:RFT] Zhengping Wu and Alfred C. Weaver. Requirements of federated trust management for service-oriented architectures. In-


REFERENCES

[107]

1. Yang:2018:NSS

2. Yoshino:2009:BMM

3. Yeo:2006:SWE
Yaseen:2012:ITM


Yasmin:2014:PSP


Yuen:2010:HCl


Yang:2016:MGE


Yoneyama:2018:MCK

Zhou:2006:MTI


Zhou:2006:P


Zhang:2007:FBT


Zulkernine:2007:ISS


Zhang:2007:FBT


Zulkernine:2007:ISS


Zheng:2007:DSL

Zakerzadeh:2013:DSA


Zhang:2014:DFA


Zhu:2011:SLA

REFERENCES

Zheng:2019:IDR


Zhao:2008:NAP


Zheng:2010:AAB