A Complete Bibliography of Publications in *International Journal of Information Security*

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/  
23 January 2018  
Version 1.00

**Title word cross-reference**

- $(t,n)$ [QDW09]. 2" [Bae10]. $k$ [BDD01]. $n$ [CC12]. $O(n)$ [DYDW10]. $t$ [BDD01].
- -ary [Bae10]. -database [BDD01]. -Diffie [CC12]. -private [BDD01].
- .NET [KKKV07].
- /SSL [BJ16].
- 1 [KJS17]. 11770 [CH16].
- 88 [vOLW05].
adaptation [BM11]. actually
ad [Gol12, MS11, SF17]. ad-hoc
[MS11]. Adapting [GLP03, Sen14].
Adaptive [PPS13, MdSC+15]. Adding
[CON09]. ADroid [RHGTSC17]. advanced
[PGMLK+13, TMP13]. adversary
[QDW09]. advertising [KOSU16]. affects
[CFBvO09]. against
[DdP13, EMRN17, GYL+07, KK17, MS11,
MYLZ14, Nui12, SK06, VSR15, ZRJ14].
agent [LV10]. Aggregate [CL13].
agreement [CCS07, CL09, FGS12, GNS14, ZZQ+17].
Alambic [ABFO08]. algebraic
[DS07, KM10, SSVC16]. Algorithm
[JMV01, Bae10, GS15, SKK+17, TLX09].
algorithms [BEPL+17, CFK16, ML14].
alignment [KSM10]. all-encompassing
[EHM15]. All-or-Nothing [MTW+14].
AMACs [CL13]. ambients [TZH04].
Analysing [HL04]. Analysis
[AMMR17, CG14, DBMS10, GLP03,
SSFB15, ZZQ+17, ABC08, ASN+16,
AC08, BGKZ12, BEPL+17, Bel10, BFT08,
BNN04, CPPK15, CF07, DFF+16,
DRPW12, GLMS+04, GBS12, HLLK15,
IDHRCPMP15, KW15, KAC17, LRB+10,
MWZ06, MTW+14, CRC15, OT06, PDB11,
QLOW09, SK16, SS05a, SB09, SSE+15,
SPDR17, Vaj16, VdZW14, WYL+12, XSA13].
Analysing [BJ16, vOLW05]. anchor
[BB04b]. Android [GPS17, IDHRCPMP15,
LMMS17, MS15, RHGTSC17]. anomaly
[DGFL+17, KCM+15, RHGTSC17].
anomaly-based [RHGTSC17]. Anonymity
[LSWW14, SS05a]. anonymization [HN14].
anonymizing [ZO13]. Anonymous
[BFG+13, SK14, ACH013, AEFL12, BCL09,
CPPK15, KCB17, SF17]. answer [WZ07].
anti [GKBS12]. anti-SPIT [GKBS12].
antivirus [ASAAS15]. any [DaP13]. API
[You06]. applicable [QDW+15].
application [DGFL+17, Pen12, Roe11a,
Roe11b, SPM13, VdZW14, ZZQ+17].
application-layer [DGFL+17].
Applications [Gri06, BCA+10, BNTW12,
DJN10, DTK+18, GSS10, HSMY12,
HZL+17, KGG09, WYL+12, vORM06].
Applied [BJ15]. approach
[AV17, CFG17, CMS10, CACB16, DSO7,
HBH12, KAC16, KAC17, KKK+17, MG17,
MMS16, MYLZ14, NA14, TWPO8, VSR15].
approaches [ZO13]. apps [GPS17].
arithmetic [ABB+14]. ASICS
[BCF+17]. aspects
[AIC18]. assisted [DYDW10, VPI15].
assumption [HIST09]. assurance [ABN14].
asymmetric [ZZQ+17]. Ate [ZZH08].
ATNA [ACBC+15]. attack
[DRPW12, GMS03, Lu09, ML14, SS05a,
SSD14, XZQ+11]. attacker [RMADF13].
Attacking [SGE02]. attacks
[ASAAS15, BRS06, CACB16, DGFL+17,
EMRN17, HS15, Hub12, KM10, LLYV09,
MS11, Pen11, PPL15, SSVC16, TTS+06,
VSR15, XCD+12]. attestation
[BFG+13, BCL09, CGL+11]. attribute
[QZLH15, QDW+15, RD16].
attribute-based
[QLZH15, QDW+15, RD16]. auctions
[Bra06]. Audit [CCD+07, BS05].
Audit-based [CCD+07]. AUTH [RG13].
authenticated [BCF+17, Lin15, MPS10,
UST11, YRW14, ZZQ+17]. Authenticating
[CF07]. Authentication [GCSABdSS12,
BPW05b, BJ16, CL13, DFF+16, EWR+09,
Gol12, GTM11, HC10, HCN15, HL04, IT05,
KML03, K1B13, LSWW14, LCPD14, MB16,
ML17, MSK16, MS09, PS17, RG13, SK14,
SMM14, WP08, VH109, WLL14].
authentications [HZL+17]. authorities
[LMMO04]. authority [CON09, QLZH15].
authorization [BZV05, KLMM09, RV03,
SSFB15, SK14, WZ07]. automata
Automated [GLMS+04, JG15, GH05, dAKdG10].

d[automatically [ACMV15], automatically [KM07, XCW+12]. availability [Bel10].

AVL [RBD02]. aware [DGF+17, KJG+11, RSPMB16, Vaj16]. awareness [MPS14].

back [KNL16]. balance [MYLZ14]. BAR [KCB17].

Based [LLW+16, ACB14, AC08, BFP03, BFPP07, BLMI1, CCD+07, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10, CCS07, CHZ16, CFBvO09, CACB16, CK08, Dan07, Des09, EMRN17, FG12, GPS17, GBDJ14, CMS10].

Basic [BCJ+11]. batch [Pen13]. Bayes [Sen14].

Bayesian [ETAHCR08]. be [ASN+16]. bee [SS17]. beehives [SS17]. behaves [ASN+16].

Behavior [CACB16, MLCS16, XCW+12].


benefits [Rus04]. better [RAC16].

between [FGS12, LKH09]. bidimensional [KCM+15].

bilayer [MLCS16]. bindings [MSKD16]. Bio [ZZW+10].

Bio-Inspired [ZZW+10]. Biometric [Pla09, BCA+10, HCN15, IT05].

biometrics [BCA+10]. Bipartite [YOV09]. birthmark [XCW+12].

bit [GSS10, YOV09]. bit-length [YOV09]. Bitcoin [ML17]. bits


Bloom [MB16]. bootstrapping [EWR+09].


BRSIM [BP08]. BRSIM/UC [BP08].

Building [LD07]. business [KAC16, KHH07].
cloud-based [KNL16]. clustering [BT07, SKK+17]. co [BMP+14, PPL15].
co-residence [PPL15]. co-resident [BMP+14].
co-residence [PPL15].
co-residence [PPL15]. co-resident [BMP+14].
co-scaling [PPL15].
co-scaling [PPL15].
co-scaling [PPL15].
co-scaling [PPL15].
co-scaling [PPL15].
co-scalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-scalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-scalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-escalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-escalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-escalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-escalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].
co-escalability [Abb13, ABN14, Ano14, BMP+14, CMPPS15, FSG+14, GMH14, KNL16, PPL15, YAM+15].

Curve [JMV01], curves [HMCD04, KSZ07].

damage [WGMB13]. Data [LMMS17, SV11, SAL17, VdWZ14, ACF17, ABN14, BS05, BNTW12, BDH+10, CTM+16, EMRN17, EAH+07, HJDC15, HH16, Kūs05, LD17, OSSK16, SMMN12, YAM+15, ZO13].

Database [KSM10, BDD01]. databases [BW08, CMS10, EAH+07, HN14]. dataset [NRC15]. day [DFG+17].

decidability [Kūs05]. defending [SK06].

defense [MYLZ14, VSR15, WR08, ZRJ14]. defenses [LLWY09]. Definition [TMP13].

decision-making [LWYY09]. Delay [ZO13].

Delay-sensitive [ZO13]. delegatability [HYW11]. Delegation [CK08, BGTCU010, CON09, GOBdlC11, WZ07].

delegations [RV03]. Denial [LLWY09, WR08, TGS17].

denial-of-service [WR08]. dependence [HS09]. dependencies [ACF17].


design [BSCZ11, CMR06, CFBv009, LMM104]. designated [HSMW08, HYW11]. designed [KCM+15]. Designing [AV17].

detect [CACB16]. Detecting [DFG+17, AGIK07, BMP+14, PPL15, vORM06].

Detection [ABR16, CPP15, sLC05, SAL17, ASAAS15, ASN+16, BEPL+17, BT07, CL08, DTK+18, DFG+17, GPS17, KKK17, KJG+11, KSM10, McH01, MLCS16, REH15, RHGTSC17, Sen14, SF17, TLX09, VL13, WAB+09, ZXR+11, ZGK07].

detectors [AvO13]. deterministic [GS15]. developing [SK16]. Development [KK17].

Device [ACMV15]. Devices [LMMS17, GCSĀbSS12, IDHRP15, LKH09, LCPD14, MR03]. differential [MT+14]. Diffie [CC12, DS07].

Digital [JMV01, ASF04, JG15]. direct [BCL09, KME+16]. disclosure [KPM12, RAC16]. discovery [DMP13, JM17]. discrete [HMCD04].

Discretionary [F08]. distinguish [HT07]. distributed [ASF04, Das12, DHS04, HN14, KKK17, Pen12, TLX09, WZ07].

Distributing [VSM06]. distribution [ASF04, BFPP07, CRM06, GP17]. DNA [HT02]. DNS [SPDR17]. Do [BM11].

document [CF03]. documents [BFP03, BFPP07]. does [GSM+11]. Dolev [BPW05b, BP08]. domain [CON09, PGMLK+13]. domains [GMH14].

Double [ACHO13].

Double-authentication-preventing [PS17]. Double-trapdoor [ACHO13].

download [NRC15]. DPA [Bae10]. drift [Sen14]. drive [NRC15]. drive-by [NRC15].

DRM [LKH09]. DSA [MR04]. DTE [LH15]. DTLS [TGS17]. during [CBC08].

Dynamic [Roe11a, ZM07, CON09, CMS10, CZ06, KKK17, SSE+15, Roe11b].

dynamics [AICC18].

dynamicity [MRW02].
Flow [HS09, SdHZ16, BMP †14, BNN04, ZM07].
form [DdP13]. Formal
[ACMV15, GKB12, Yon18, dAKdG10, 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,
XSA13, ZRJ14]. free
[ARML06, BGKZ12, CLPP11, YRW14]. freeness [HIST09]. friendly [CLPP11].
Fujisaki [GMMV05]. full [Bra06]. Fully [CDF †13]. function [BGKZ12, SB14].
functionality [SP13]. functionality-based [SP13]. functions
[AMP12, GKK10, MS09, SM10]. future [LMMP06]. fuzzy [HCN15].

Gait [HCN15]. Game [wLW05, WYL †12].
genereal [BCD †13, Pen11]. generalised [BKMR08]. generalization [DJN10].
Generalized [BR18, KMR09].
Generalizing [KG11, AMP12]. generated [HINT02]. Generating [LC04]. generation
[KIJ †11, KZS07, MR04]. Generic
[Ala17, ZHV15, EWR †09, KME †16]. geographic [ABN14]. GeoProof [ABN14].
gesture [GCSDbSS12]. Global [Pri04].
goals [RL16]. gossip [ML14].
government [GObdlC11]. GPU [VP15].
GPU-assisted [VP15]. GQ [HRL09].
grained [KLMM09]. graph
[BCEM04, RV03]. graph-theoretical
[BCEM04]. graphical
[CG14, CFBvO09, GGM11, WLL14].
graphs [HS09, HLK15, KB13]. grid
[CLPP11, KLM09, LP11]. ground
[AvO13]. Group [EHSS14, BVST07, GNS14, IDHRPCMP15, RBD02, ZWQ †17]. groups
[PJ10]. guarantee [ABC08, Bel10].
guarantees [LSW14]. guest [AN †12, CM16, DMRS07, JZ11, YSM16, ZLL12].

Haar [KCM †15]. hand [GCSABdSS12].
Handling [WZ07]. handshake [TGS17].
hard [EAH †07]. hard-to-reverse
[EAH †07]. hardening
[DMDD16, DRR12, MRW02]. hardware
[BSCZ11, DLYW10]. hardware-assisted
[DLYW10]. harvesting [BR18]. hash
[AMP12, BGKZ12, GKK10, MS09,
MFES04, SB14]. hashing
[BDPV14, CHKO12, MP16]. health
[BDHZ15, QLZH15]. healthcare [QDW †15].
Hellman [CC12, DS07]. heterogeneous
[SAT09]. hidden [ABB17, GSS10, SSVC16].
Hierarchical [NAM06, LLY †16]. High
[BNTW12, BB04b, Pen13]. high-end
[BB04b]. High-performance [BNTW12].
higher [PDB11]. HiveSec [SS17]. hoc
[Gal12, MS11, SF17]. homomorphic
[EMRN17, MMS16]. hop [BT07]. host
[CL †11]. hotels [ZD †18]. hull
[ALPW13]. human [ALPW13, MBHT17].
Hybrid [KML03, CC10, GMMV05, MMS16].

ID [FGS12]. ID-based [FGS12].
identification
[ALPW13, CL08, MGV17, NRC15].
identifiers [HINT02]. identifying
[KGG09, SPD †17]. Identity
[CCS07, LP11, LL †16, CHZ16, GOBdlC11,
HRL09, LMG17, LBZ †0, MPS14, NA14,
TMP13, Ust11, VdWZ14, YSM10, ZWQ †17].
Identity-Based [LL †16, CCS07, LP11,
CHZ16, HRL09, LMG17, LBZ †0, MPS14,
Ust11, YSM10, ZWQ †17]. IDSEC [CL08]. If
[AN †16, MBHT17]. IHE [ACBC †15]. II
[BB04b]. III [SKK †17]. image [HC10].
images [HLK15, MBHT17]. immune
[Hub12]. impact [SSD14]. implement
[ABFL12]. implementation
[BSCZ11, IDHRPCMP15, MFES04].
KPM12. **looks** [ASN+16]. **lottery** [GSS10].
Low [BGP07b, GS15, SSVC16].
**low-deterministic** [GS15].
**low-randomness** [BGP07]. LPN [RG13].

MAC [EMRN17]. **MAC-based** [EMRN17].
**machine** [MS14, SSE+15].
**machine-learning** [SSE+15]. **machines** [MLCS16, vOLW05].
Making [BR17].
MALICIA [NRC15]. **malicious** [ABB17, BRS06, CMS10, GPS17, RHGTSC17, WGMB13].
**Malware** [HLKI15, MLCS16, BEPL+17, SKK+17, VPI15, VRJ14].
**manageability** [TG05].
Management [CF03, ASF04, BF13, CH16, GMMZ06, GH05, LLWY09, NA14, RHL7, RBD02, SSN15, TMP13, VdWZ14, WW07, dAKdG10, vOLW05].
**mandatory** [DLR15].
Markov [ABB17, RHL7]. masquerade [Sen14]. MaX [BFP03]. maximum [AD08].
McEliece [NMBB12]. **McEliece-based** [NMBB12]. **mean** [BM11].
**measure** [BF13]. measurement [RMPADF13]. Measuring [RGL16].
**mechanism** [ACF17, LI07].
mechanisms [LBW05]. media [RAC16].
**mediated** [VSM06]. memory [SV11, vOLW05].
**memory-based** [SV11]. merging [CMR06]. Merkule [MFES04].
**mesh** [EHM15, SSN15]. Message [ANS+12, CM16, JZ11, YSM16, ZLL12, CL13, GP17, MS09].
**metering** [MSP+13, RDK18]. Method [SAL17, CYK09, IT05, KGG09, MP15, PJ10, SPDR17]. methodology [AvO13, Des09, GMMZ06].
microaggregation [SMMN12].
**microblogging** [ASN+16]. Microsoft [You06]. minimisation [VdWZ14].
Minimizing [KPM12, ZBD06]. mining [BNTW12, HBH12]. misbehavior [SF17].
MITF [SKK+17]. mitigation [YP12]. mix [Dan07, MS11, Pen11]. mix-based [MS11, Pen11]. mix-related [Dan07].
Mobile [EWR+09, LMMS17, ACB14, AGK16, AMRR17, CF07, GSM+11, GCSÁbdSS12, HCN15, HZL+17, IDHRPCMP15, LCPD14, LH15, LL14, LV10, WGMB13, BT07, SSE+15], mobile-phone [WGMB13]. Mobile-Sandbox [SSE+15].
MobileTrust [LV10]. model [ASF04, A17, ABB17, AC08, BM05, BGTCCBB10, ECEM04, EEB+15, GMMZ06, Gol12, GYJ+07, GKBS12, HL04, JGK+14, Kud02, LH15, MdSC+15, NSNK06, QLOW09, SK16, SPM13, SSP14, TND+15, ZGC07, ZZW+10]. model-checking [AC08].
**model-oriented** [SK16]. Modeling [CCB08, DLR15, ACMV15, KAC17, Yon18]. models [ABB17, Den08, DRPW12, FGS12, KAC16].
**modes** [BDPV14]. **Modification** [PDB11].
modified [KJS17]. modular [MSKD16, YOV09].
monitoring [HHB12, vORM06]. Multi [BT07, EHM15, OSSK16, ZZW+10, BNTW12, BFT08, CON09, Das12, GMH14, KM03, PGMLK+13, QLZH15, QLOW09, WR08].
**multi-authority** [QLZH15]. 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, TWF08]. multicast-based [MP15].
multifactor [IT05]. multiple [CC12, HMCDO4]. multiple-key [CC12].
multiplication [YOV09]. multiplications [HTM11].
multipliers [YOV09]. multiresolution [VSR15]. multiset [BA16].
multisignatures [HRL09]. must [ASN+16]. Mutual [HZL+17].
naive [Sen14]. Negative [EFH09, EAH+07]. negotiation [KLMM09].
**negotiation-based** [KLMM09]. Net
Nets [SSFB15]. Network [GPS17, ABCC08, BMP+14, CL09, EMRN17, GH05, LBZ+10, wLW05, MYLZ14, PMPGMLLM12, SAT09, TLX09, WYL+12, dAKdG10]. Network-based [GPS17]. Networked [MR03]. networks [ACB14, CMR06, CPPK15, Das12, DRPW12, EHM15, EMRN17, Go12, RBEH15, SS17, SSN15, SF17, YRW14, ZXZ+11, BT07].

NICs [CBC08]. NIZK [WT16]. no [BB04b]. noisy [BDH+10, KML03]. non [CDF+13, CHZ16, CL09, EHSS14, GRV05, HYWS11, KM03, MP16]. non-compressing [MP16]. non-delegatability [HYWS11].

non-interactive [CDF+13, CHZ16, CL09, EHSS14]. non-repudiation [GRV05, KM03]. noninterference [CDF+13, CHZ16, CL09, EHSS14]. non-repudiation [GRV05, KM03].

noninteractive [ACB14, CMR06, CPPK15, Das12, DRPW12, EHM15, EMRN17, Go12, RBEH15, SS17, SSN15, SF17, YRW14, ZXZ+11, BT07].

non-interactive [CDF+13, CHZ16, CL09, EHSS14]. non-repudiation [GRV05, KM03]. noninterference [BP04]. note [ZZH08].


Outbound [Sm04]. outsourced [CTM+16, LD17]. outsourcing [AL05, GYL+07, HJDC15, KU16]. overview [BMP05]. Own [ACMV15].

packets [vORM06]. packing [BEPL+17]. Paillier [NSNK06, DJN10]. Paillier-based [NSNK06]. pairing [YRW14, ZZH08]. pairing-free [YRW14]. pairings [BCL09, CCS07]. papers [ACM05].


Password-authenticated [MPS10]. passwords [CFBvO09]. past [JG15, LMP06]. patching [JMJ17].

pattern [OSSK16]. patterns [CFBvO09]. pay [Roe11a, Roe11b, DZW+18]. pay-TV [Roe11b, Roe11a, DZW+18]. PBAC [Kud02].

DAMe [PMPGMLLM12]. IEC [CH16]. LTE [LSW14]. offline [LMG17, LBZ+10]. on-line [BCD+13].


phone [CF07, GSM+11, HCN15, WGMB13]. physical [SM10]. physically [BR17].

PIOA [Yon18]. PIR [DYDW10]. pirates [Nu12]. PISHI [MBHT17]. PKI [BB04b, Daw04, LC04, LMM06, LMM004, VSM06].

PLAID [DFF+16]. Plaintext [MPS10].
platform [IDHRPCMP15], platforms [KPM12, RHGTSC17], point [ABB17, KW15], policies [ABCC08, ACMV15, AICC18, BCL13, CF03, CCB08, KAC17, LBW05, LRB+10, SB09].
Policy [SAL17, BZV05, GMH14, KNL16, MS15, TG05, XSA13, dARdG10].
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 [LLW+16, ALOW15, KOSU16, LCL14, Pen12, VHT09, WR15], practices [LD07].
pre [CMR06, Pen13], pre-computation [Pen13], pre-distribution [CMR06].
Preface [Ano11a, ACM05, BGP07a, BM05, Daw04, DV08, DMR07, Pri04, Sce05, Wai04, ZL06], prefix [BGKZ12], present [LMMP06], preservation [RAC16], preserve [EEB+15], preserved [LD17], preserving [ABF008, BGK08, CTA+16, KOSU16, KB13, KNL16, MB16, MCD11, NSTD09, NA14, QLZH15, RDK18].
Preventing [RAC16, PS17, YP12], prevention [VL13], primitives [MP16, SM10], principle [Bel10], Principles [CGL+11], Privacy [KB13, MB16, MSP+13, NSTD09, QLZH15, RDK18, ABFO08, AIC+09, AMRR17, BG08, BCA+10, BDHZ15, Bra06, CTA+16, EAH+07, GLMS+04, GYL+07, KOSU16, KBH07, KNL16, LD07, LD17, MCD11, NA14, PGMLK+13, RSPMB16, RMPAD13, YAM+15], privacy-aware [RSPMB16], Privacy-enhanced [MP+13], privacy-preserved [LD17], Privacy-preserving [KB13, MB16, NSTD09, QLZH15, RDK18, ABFO08, BGK08, CTA+16, KOSU16, MCD11, NA14], Private [BA16, DMP13, BDD01, BGP07b, KW15, LMD17, WR15].
Probabilistic [DHW11, BP04, GYL+07, MCD11, PJ10], problem [CC12, GBdCI11, GMS03, GP17, KG11, RG13, TWP08, YSM10], problems [HMCD04], process [HHB12], processes [RHL17], profiling [LCPD14], program [BDF04, HS09], programmability [Yon18], programmable [Sm04], programming [WZ07], programs [KM07, WGMB13], project [BF03], proof [WLLW14], proofs [BCJ+11], Proposal [IHNT02, IT05], proposals [BJ16], protected [BJ16].
Protecting [EAH+07], protection [AIC+09, GKB12, KK17], protocol [Ala17, ALPW13, Bel10, BFT08, CL09, DFF+16, DGZFGH13, HL04, HYWS12, LSWW14, ML17, RG13, RGL16, YR14, YAM+15], Protocols [DHS04, AC08, ABFL12, BGK08, BMV05, BNN04, CCS07, DVB02, DS07, GLP03, GRV05, KM03, Ki05, LCL16, MP15, MSN02, MS14, SFB15, Ust11, Vaj16, VdW14], Provably [YRW14, NSNK06], Provably [LCL14, RG13, VHT09], provenance [Abb13], providing [PGMLK+13], Provision [Kud02], Provision-based [Kud02], provisioning [TGS17], proxy [Lin15], pseudo [HIST09], pseudo-freeness [HIST09], public [ALOWL15, BJC+11, BZ03, DJN10, EHS14, GW09, LC04, Pen12, SSP14, Grit06], public-key [ALOWL15, BJC+11, DJN10, EHS14, SSP14], push [BFPP07], push-based [BFPP07], pushdown [BCL13], puzzle [WR08], puzzle-based [WR08], PVSS [Pen12].
QR [HZL+17], QR-code [HZL+17], 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], rational [ETAHCR08], RBAC [BGTCBB10], Re


**scoring** [OSSK16]. search [HH16, KJS17, OSSK16]. searchability [HJDC15]. searches [WR15]. Seberry [BH03]. second [ABM+12]. secrecy [CDF+13, Hub12]. secret [DdP13, GMS03, HJDC15, LMD17, PPSS13, QDW09]. secrets [BW08]. Secure [ABB17, AL05, BVS07, DZW+18, HN14, HSMW08, KW15, LCL16, MSKD16, SJ09, ZZX+11, ASF04, Ala17, BPW05a, BDF04, BNTW12, BT07, DdP13, KME+16, KU16, KZS07, LCL14, LLW+16, MB16, MLO+04, MMP14, NMBB12, Nu12, PJ10, QDW+15, RG13, SJ10, SK16, Smi04, TND+15, YAM+15]. secured [EHH15]. Securing


References

Abbadi:2013:FET
REFERENCES

**Aliasgari:2017:SCH**

**Alfaro:2008:CA**

**Aimeur:2008:LPP**

**Andreeva:2012:SAS**
REFERENCES


[ACF17] Davide Alberto Albertini, Barbara Carminati, and


Kostas G. Anagnostakis, Michael B. Greenwald, Sotiris Ioannidis, and Angelos D. Keromytis. COVERAGE: detecting and reacting to worm epidemics.

### Ayed:2018:ADS


### Anagnostopoulos:2016:NFM


### Atallah:2005:SOS


### Alawatugoda:2017:GCM

REFERENCES


REFERENCES


Almaatouq:2016:ILL


Blanton:2016:POS


Baek:2010:RAR


REFERENCES

Boyd:2017:AAK


Backes:2011:CSS


Brickell:2009:SSN


Beauquier:2013:SPE


Blundo:2001:PDI

REFERENCES

[Bartoletti:2004:SIS]

[Buhan:2010:ERC]

[Bertoni:2015:SPE]

[Bertoni:2014:SCS]

[Bella:2010:PGA]
Giampaolo Bella. The principle of guarantee avail-

**Bat-Erdene:2017:EAC**


**Bernhard:2013:AAU**


**Bertino:2003:CBF**


**Bertino:2007:SSP**

REFERENCES


REFERENCES


**Boyd:2005:PSI**


**Bielova:2011:DYR**


**Bella:2005:OVS**


**Bates:2014:DCR**


**Basin:2005:OSM**

REFERENCES


Bernardini:2017:MRP

Bernardini:2018:GES

Brandt:2006:HOF

Bohli:2006:KSA

Baldwin:2005:ESA

Baumgarten:2011:CSH
Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno. A case study in hardware Trojan design and implementation.
REFERENCES


Bononi:2007:IDS

Bohli:2007:SGK

Biskup:2008:KSI

Bai:2005:SAP

Chikha:2016:BBA


REFERENCES


REFERENCES


\[\text{Crampton:2008:DRB}\]


\[\text{Chen:2008:IID}\]


\[\text{Cheng:2009:CKA}\]


\[\text{Chen:2013:AMA}\]


\[\text{Crampton:2011:UFC}\]

Chang:2011:EHS


Chen:2016:MGE


Casassa-Mont:2015:TSI


Chakrabarti:2006:KPD


Chakraborty:2010:CDB


Chadwick:2009:ASX

[David W. Chadwick, Sassa Otenko, and Tuan Anh Nguyen. Adding support to XACML for multdomain user to user dy-

**Chakravarty:2015:DAE**


**Celdran:2016:RPP**


**Cook:2009:EBC**


**Crescini:2006:PSD**


**deAlbuquerque:2010:FVA**


REFERENCES


REFERENCES

Damiani:2002:SSS

Dent:2008:SCE

Desoky:2009:LLB

Degabriele:2016:UPC

Duessel:2017:DZD

Draper-Gil:2013:OFE
G. Draper-Gil, J. Zhou,

[DJN10]


[Damgaard:2010:GPP]


[DHS04]


[DiPierro:2011:PTC]


[DLR15]


[DM07]

Daza:2004:PUI

Dolzhenko:2015:MRE

DeFrancesco:2007:ILS
DeKeulenaer:2016:LTS

DeCristofaro:2013:PDC

Dimitrakos:2007:GEP

Dewri:2012:OSH

Delicata:2007:AAV

Diaz-Santiago:2016:CST
Sandra Díaz-Santiago, Lil María

**Ding:2006:CNT**


**Ding:2010:NHA**


**Degano:2008:P**


**Dawson:2002:CCP**


**Ding:2010:NHA**

Deng:2018:SPT


Esponda:2007:PDP


ElHassani:2015:ION

Abdeljebbar Ameziane El Hassani, Anas Abou El Kalam, Adel Bouhoula, Ryma Abassi, and Abdellah Ait Ouahman. Integrity-OrBAC: a new model to preserve Critical Infras-

Emura:2014:GSI


Esfahani:2017:EHM


Estevez-Tapiador:2008:BRE


Elmufti:2009:MWS


Fiore:2012:RBS

REFERENCES


[GH05] Joshua D. Guttman and Amy L. Herzog. Rigorous automated network security management. *International Journal of In-


REFERENCES


Gollmann:2008:E [Gol08]


Golic:2012:NAM [Gol12]


Gunther:2017:LMT [GP17]


Garg:2017:NBD [GPS17]


Gritzalis:2006:PKI [Gri06]


Gurgens:2005:SFN [GRV05]

Sigrid Gürgens, Carsten Rudolph, and Holger Vogt. On the security of fair non-repudiation protocols. *In-
REFERENCES

Gihorn:2015:NAL


Glisson:2011:ERW


Gritti:2016:BED


Goldschlag:2010:THB


Gyory:2011:TBG

REFERENCES


REFERENCES


Han:2012:NCO


Hanley:2011:UTD


Huang:2011:ESD


Huang:2012:NEO


Huber:2012:PSS

Huang:2017:MAP


Isern-Deya:2015:PUG


Itakura:2002:PPI


Imamoto:2008:AEC

REFERENCES

James:2015:AIP


Jovanovikj:2014:CMS


Joh:2017:PSV


Johnson:2001:ECD


Jajodia:2011:MGE


Karimi:2016:UAA

Vahid R. Karimi, Paulo S. C. Alencar, and Donald D. Cowan. A uniform approach for access control and business models with explicit rule realization. *International Jour-
Karimi:2017:FMA


Kundu:2013:PPA


Kotzanikolaou:2017:BAR


Kozakevicius:2015:UQS

REFERENCES


Kate:2011:GCB

Kozina:2009:MIW

Kim:2014:EVE

Kong:2011:SSA

Kim:2017:MES
Kananizadeh:2017:DDP


Kolias:2017:TDS


Koshutanski:2009:EGS


Kremer:2003:FMP


Kopf:2007:TTU

REFERENCES


Knudsen:2010:CEA


Kasamatsu:2016:TSE


Korzhik:2003:HAB


Kuper:2009:GXS


Krukowski:2007:TS

Kurek:2016:TBC


Kim:2002:NEC


Khayati:2016:PPP


Kontaxis:2012:MID


Kundu:2010:DID


Konstantinou:2007:EGS

Elisavet Konstantinou, Yannis C. Stamatiou, and Christos Zaroliagis. Effi-

Kiraz:2016:EVA


Kudo:2002:PPB


Kusters:2005:DCP


Kamm:2015:SFP


Landwehr:2001:CS


REFERENCES


Lauer:2007:BOT

Li:2017:WOO

Levin:2007:WSL

Li:2015:TMM

Lin:2015:RNR
[Lin15] Han-Yu Lin. RPCAE: a novel revocable proxy con-

**Lee:2009:RTB**


**Liao:2014:POC**


**Liu:2016:PCC**


**Li:2009:DSA**


**Li:2006:USS**


Hoon Wei Lim and Kenneth G. Paterson. Identity-based cryptography for


REFERENCES


Malatras:2017:EUI


Mousazadeh:2014:RGA


Mann:2017:TFA


Miao:2016:MDU


Mana:2004:FSE


Mateu:2016:HAV

Víctor Mateu, Josep M.

Martina:2015:VMB


Mennink:2016:EPH


Mavrogiannopoulos:2014:TSK


MacKenzie:2010:PAK


Manulis:2014:PAI


[MS14] Takaaki Mizuki and Hiroki Shizuya. A formalization of card-based cryptographic protocols via abstract machine. *International Jour-
REFERENCES


R. P. McEvoy, M. Tunstall, C. Whelan, C. Murphy, and W. P. Marnane. All-or-Nothing Transforms as a countermeasure to dif-

**Mayer:2006:OFA**


**Mu:2014:RBD**


**Nunez:2014:BPP**


**Nali:2006:HTB**


**Niebuhr:2012:SPS**

REFERENCES

Naor:2010:ETR


Nappa:2015:MDI


Nguyen:2006:VSF


Nuida:2012:SCS


Nieto:2002:KRC


REFERENCES


Quinn:2009:AAE


Qian:2015:PPP


Raad:2016:PSR


Rodeh:2002:UAT


Riecker:2015:LEC


Hani Ragab-Hassen and Esma Lounes. A key management scheme evaluation using Markov pro-

**Reaves:2012:OVT**


**Rebollo-Monedero:2013:MPA**


**Roelse:2011:DST**


**Roelse:2011:EDS**


**Rashwan:2016:UTP**


Navajit Saikia and Prabin K. Bora. Perceptual

**Skoric:2016:FBR**


**Sen:2014:UIW**


**Singh:2017:RUA**


**Steinwandt:2002:APB**


**Sajedi:2009:SSB**


REFERENCES


REFERENCES


[SPM13]


[SS05a]


[SS05b]


[SS17]


[SSD14]

Michael Spreitzenbarth, Thomas Schreck, Flo-

Seifi:2015:ATA


Susil:2015:RMP


Sepahi:2014:LBC


Susil:2016:SSA


Saxena:2011:DRE

Nitesh Saxena and Jonathan Voris. Data remanence effects on memory-based entropy collection for RFID

**Trostle:2005:TIS**


**Tiloca:2017:IRD**


**Tian:2009:LSN**


**Tormo:2013:DAI**


**Tonicelli:2015:ITS**

Rafael Tonicelli, Anderson C. A. Nascimento, Rafael Dowsley, Jörn Müller-Quade, Hideki Imai, Goichiro Hanaoka, and Akira Otsuka. Information-theoretically secure oblivious polynomial evaluation in the commodity-based model. *International Journal of*
Tsuno:2006:ICA


Tartary:2008:CAM


Ustaoglu:2011:IB


Vajda:2016:ATA

REFERENCES

Veeingen:2014:DMC

Vasserman:2009:IKN

Vrakas:2013:IDP

vonOheimb:2005:ASM

vanOorschot:2006:MSD

Vasiliadis:2015:GAM
Giorgos Vasiliadis, Michalis...

**Vanrenen:2006:DSM**


**Valenzuela:2015:MAO**


**Waidner:2004:P**


**Wang:2013:USM**

 REFERENCES

[184]


Wu:2014:SSP


Ly:2005:GSN


Wang:2008:MLF


Wei:2015:TPE


Wang:2016:SSE


Wu:2007:RFT

Zhengping Wu and Alfred C. Weaver. Requirements of federated trust

**Wang:2012:SGN**


**Wang:2007:HDA**


**Yu:2015:EPR**

Yong Yu, Man Ho Au, Yi Mu, Shaohua Tang, Jian Ren, Willy Susilo, and Liju Dong. Enhanced privacy of a remote data integrity-checking proto-

**Yoneyama:2018:FMR**


**Young:2006:CEU**


**Yoshino:2009:BMM**


**Yeo:2006:SWE**


**Yaseen:2012:ITM**


REFERENCES


Zhou:2015:GCR


Zhao:2008:NAP


Zheng:2010:AAB


Zhu:2011:SLA