A Complete Bibliography of Publications in the
International Journal of Applied Cryptography

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/

02 January 2019
Version 1.02

Title word cross-reference

112 [BKK+12]. π [FFGL10].
-bit [BKK+12].
access [NNO+17, SS09]. Achieving
[CLL+10]. active [BdMM08]. advanced
[SS09, PB14]. adversaries [BdMM08].
adversary [PCR+09]. AES
[GSSC17, HSS09]. against
[BM08, BdMM08, JLP10, Leu08].
agreement [MU09, MU10]. algebraic
[HSS09]. ALPHA [HSS09]. among
[HW08]. analysis
[Cre10, HY08, LBM14, PR10, SS09, ACJT09].
Anonymous [BdMM08]. APOP [Leu08].
application [HSS09, JP13], applications
[SLdW12]. approach [LBM14]. arbitrary
[BCS17]. Asiacrypt [ACJT09]. aspects
[PR10]. assumption [CS13]. assumptions
[KP17]. asymmetric [BCS17]. attack
[Cre10, HN09, JLP10, LBM14, Leu08, PB14].
attacks [BM08, GSSC17, HS10]. Attribute
[CG17, HJSNS12, AA14, EMO+10, EMR12].
Attribute-based
[CG17, HJSNS12, AA14, EMO+10, EMR12]. auctions’ [DGK09]. authenticated
[ACS17]. authentication
[BdMM08, GMS09, Leu08, SS09].
authorisation [Tan12]. automatic [Cre10].
aware [GMS09].
backup [CML12]. backward [AA14].
based [AA14, BCS17, Boy08, CS13, CG17],
EMO+10, EMR12, GMS09, HJSNS12, ISW17, JP13, LBM14, Leu08, PSWH08, PR10, SOO10, between [SEV17]. bilinear
browser [GMS09]. browser-based [GMS09].
call [HS10]. Camellia [YKP13]. case
[GSSC17]. CCA [ISW17]. CCA-secure
[ISW17]. CCA2 [BCS17]. certificateless
[HW08]. chains [CLL+10]. challenge
[Leu08]. challenge-response [Leu08].
channel [PR10]. checking [FFGL17]. Chosen
[SLdW12]. Chosen-prefix
[SLdW12]. cipher
[HN09, YKP13, ZSWF10]. ciphertext
[CML12, EMO+10]. ciphertext-policy
[EMO+10]. ciphertexts [ACS17, KP17].
cloning [HJSNS12]. collisions [SLdW12].
commit [Lip17]. commit-and-prove
[Lip17]. committing [AO12]. compared
[Boy08]. Comparing [MU09]. comparison
[DGK08, DGK09, Veu14]. composability
[OMO08]. composable [AO12].
computation [JP13]. computing [JP13].
confirmation [GMS10]. consoles
[BKK+12]. constant [BdMM08, EMO+10].
constant-cost [BdMM08]. constrained
[ACS17]. content [SS09]. correction
[DGK09]. corruptions [BM08]. cost
[BdMM08]. critical [SS09]. cryptanalysis
[ZSWF10]. cryptography [HW08]. curve
[BKK+12]. curves [CS12, Fur14].

data [FFGL17]. databases [YBDD09].
datasets [YWPZ09]. decisional [CS13].
decryption [HKK+10, ISW17]. Defending
[JP10]. Delayed [JM08]. derivation
[CS12]. Designing [HS10]. devices
[ACS17]. different [Tan12]. Diffie
[CS13, CS12, MU10]. disclosure [JM08].
discrete [BKK+12]. disjointness
[YWPZ09]. distance [JP13].
distinguishing [HN09]. division [Veu14].
document [JP13]. Double [CML12]. drive
[SS09]. drive-host [SS09]. Dynamic
[AA14, EMR12].
eCKs [Cre10]. efficiency [CLL+10].
Efficient [DSMRY12, PSWH08, HLW08, Lip17, DGK09]. elliptic [BKK+12, CS12].
Encrypted [Veu14, YBDD09]. Encryption
[PB14, ACS17, BCS17, Boy08, CS13, CG17, DGK08, EMO+10, HJSNS12, ISW17, Tan12].
end [CS12]. enhanced [NNO+17].
ephemeral [MU10].
EphemeralKeyReveal [Cre10]. equality
[Tan12]. evolution [JLP10]. exchange
[BCNP09, BM08, OMO08]. explicit
[GMS10]. exposure [ISW17]. extended
[BCS17]. extensions [KP17]. extraction
[CS12].
Fair [HKK+10, OMO08]. fast [FFGL10].
fault [GSSC17]. feasibility [PCRS10].
FHMQV [SEV17]. five [HSS09].
five-round [HSS09]. forest [PB14].
framework
[AO12, FFGL10, HY08, OMO08].
frameworks [Boy08]. fully [CG17].
function [KP17]. function-private [KP17].
 functionalities [JP13]. functions
[FFGL10].

game [BKK+12]. games [HY08].
granularity [Tan12]. group
[AA14, ACJT09, BM08].
Hamming [JP13]. handling [ACS17]. hash
[FFGL10]. Hashing [Far14]. Hellman
[CS13, CS12, MU10]. Hessian [Far14].
hierarchical [CS13]. high [CLL+10].
HMQV [SEV17]. Homomorphic
[DGK08, CG17]. host [SS09]. hybrid
[CS13].
IBE [KP17]. ID [SOO10]. ID-based


MR2444651 [ACJT09]. multidimensional [HN09]. Multiuser [YBDD09]. mutual [GMS09, PR10].

NAXOS [Cre10]. networks [PCRS10]. nominative [HLW08, NNO+17]. non [AO12]. non-committing [AO12]. Notions [LN14]. number [CG17].


queries [YBDD09].

REFERENCES


Winternitz [BDE+13]. without [EMR12, HJSNS12, SOO10].

zero [Lip17]. zero-knowledge [Lip17].

References


REFERENCES


2010. CODEN ????: ISSN 1753-0563 (print), 1753-0571 (electronic).

Ciss:2012:REE

Chatterjee:2013:PHH

Damgaard:2008:HES

Damgaard:2009:CES

Dachman-Soled:2012:ERP

Emura:2010:CPA

Emura:2012:DAB

Farashahi:2014:HHC
REFERENCES

Fleischmann:2010:TFS


Feng:2017:NPR


Gajek:2009:UAP


Goldberg:2010:MRP


Ghosh:2017:PFA


Hinek:2012:ABE


Hong:2010:FTD

REFERENCES

**Huang:2008:EOM**


**Hakala:2009:MLD**


**Hagalisletto:2010:DAS**


**Huang:2009:FRA**


**Huang:2008:RAV**


**Herzberg:2008:LGF**


**Ishida:2017:CSR**


**Jin:2010:DAP**

REFERENCES


REFERENCES

ISSN 1753-0563 (print), 1753-0571 (electronic).


REFERENCES


Veugen:2014:EID

Wolf:2009:SOS

Yang:2009:MPQ

Yap:2013:PVC

Ye:2009:USD

Zhang:2010:SRC