

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** [CS13]. **bit** [BKK⁺12]. **blind** [AO12]. **block** [YKP13, ZSWF10]. **bounded** [CG17]. **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** [FYL17]. **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, Far14].

data [FYL17]. **databases** [YBDD09]. **datasets** [YWPZ09]. **decisional** [CS13]. **decryption** [HKK⁺10, ISW17]. **Defending** [JLP10]. **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]. **HMQR** [SEV17]. **Homomorphic** [DGK08, CG17]. **host** [SS09]. **hybrid** [CS13].

IBE [KP17]. **ID** [SOO10]. **ID-based**

[SOO10]. **ideal** [BNV17]. **identification** [KH08]. **identity** [Boy08, CS13, ISW17]. **identity-based** [Boy08, CS13, ISW17]. **improvement** [SS09]. **information** [PR10]. **information-based** [PR10]. **inputs** [CG17]. **integer** [Veu14]. **integers** [LN14]. **integrity** [FYL17]. **intersection** [DSMRY12].

key

[BCNP09, BM08, BdMM08, CS12, HJSNS12, ISW17, Leu08, MU09, MU10, Tan12]. **key-lookup** [BdMM08]. **key-recovery** [Leu08]. **keys** [KP17, MU10]. **knowledge** [Lip17].

lattice [PSWH08]. **lattice-based** [PSWH08]. **lattices** [BNV17]. **layered** [HY08]. **learning** [LBM14]. **length** [BCS17, EMO⁺10]. **line** [DGK09]. **linear** [HN09, KP17]. **local** [AA14]. **log** [NNO⁺17]. **logarithm** [BKK⁺12]. **long** [ACS17]. **lookup** [BdMM08].

MAC [HSS09]. **machine** [LBM14]. **management** [NNO⁺17]. **MD5** [Leu08, SLdW12]. **MD5-based** [Leu08]. **mechanism** [NNO⁺17]. **memory** [ACS17]. **message**

[BCS17, GMS10, PCR⁺09, PCRS10]. **mobile** [PCR⁺09, WOS09]. **mode** [CML12]. **model** [AA14, BCNP09]. **models** [HW08, MU09]. **move** [HLW08]. **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].

offline [WOS09]. **on-line** [DGK09]. **One** [BCNP09, ACJT09, BDE⁺13, HLW08]. **one-move** [HLW08]. **One-round** [BCNP09].

one-time [BDE⁺13]. **optimality** [PCRS10]. **optimistic** [OMO08]. **oracles** [EMR12, SOO10].

p [YKP13]. **p-Camellia** [YKP13]. **p-SMS4** [YKP13]. **Parallelisable** [YKP13]. **parties** [HKK⁺10]. **password** [JM08]. **peer** [MU09]. **Perfectly** [PCR⁺09]. **perspective** [BNV17]. **pirate** [JLP10]. **platforms** [WOS09]. **policy** [EMO⁺10]. **popular** [ACJT09]. **possibility** [PCRS10]. **post** [MU09]. **post-specified** [MU09]. **Power** [LBM14, KH08]. **Practical** [CS13, Leu08, BNV17, Boy08, PR10]. **pre** [MU09]. **pre-** [MU09]. **Preface** [BW10]. **prefix** [SLdW12]. **Preventing** [GSSC17]. **prime** [BKK⁺12]. **privacy** [FYL17, NNO⁺17]. **privacy-enhanced** [NNO⁺17]. **private** [DSMRY12, KP17, YBDD09, YWPZ09]. **problem** [BKK⁺12]. **profiling** [PB14]. **property** [HSS09]. **proposal** [CML12]. **protocol** [CS12, Cre10, OMO08]. **protocols** [GMS09, GMS10, HY08, MU10, SEV17]. **provably** [GMS09]. **prove** [Lip17]. **Prover** [Lip17]. **Prover-efficient** [Lip17]. **Public** [Tan12, FYL17, LW17].

queries [YBDD09].

Random [PB14, EMR12, SOO10]. **randomisation** [GSSC17]. **Randomness** [CS12, LW17]. **recognition** [GMS10]. **recoverability** [GMS10]. **recovery** [Leu08]. **reduction** [BKK⁺12]. **registration** [BM08]. **relation** [HW08]. **reliable** [PCR⁺09, PCRS10]. **Remarks** [ACJT09]. **remote** [FYL17]. **resistance** [ISW17]. **response** [Leu08]. **results** [ZSWF10]. **reusing** [MU10]. **revocable** [ISW17]. **revocation** [AA14]. **RFID** [BdMM08, CLL⁺10]. **RFID-tagged** [CLL⁺10]. **robust** [DSMRY12]. **round** [BCNP09, HSS09]. **RSA** [LN14].

scheme [ACJT09, BDE⁺13, EMO⁺10, FYL17, HLW08, PSWH08]. **schemes** [CS13, ISW17, KH08, Tan12]. **secret** [CS12]. **Secure** [JP13, WOS09, BCS17, CML12, DGK08, DGK09, FFGL10, GMS09, ISW17, PCR⁺09, PCRS10, Veu14, YWPZ09]. **Securing** [BM08]. **security** [BDE⁺13, CLL⁺10, HY08, HW08, OMO08]. **semi** [HKK⁺10]. **semi-trusted** [HKK⁺10]. **separation** [SEV17]. **Session** [Cre10]. **Session-StateReveal** [Cre10]. **set** [DSMRY12, HS10]. **set-up** [HS10]. **Shannon** [HN09]. **shorter** [KP17]. **shortest** [BNV17]. **side** [PR10]. **Sieving** [BNV17]. **signature** [AA14, ACJT09, BDE⁺13, HLW08, PSWH08]. **signatures** [AO12, NNO⁺17, SOO10]. **signcryption** [EMR12]. **similarity** [JP13]. **SIP** [HS10]. **sloppy** [BKK⁺12]. **sloth** [LW17]. **SMS4** [YKP13, ZSWF10]. **SNARKs** [Lip17]. **Solving** [BKK⁺12]. **Some** [ZSWF10]. **specifications** [HY08]. **specified** [MU09]. **Sponge** [BCS17]. **Sponge-based** [BCS17]. **SSO** [NNO⁺17]. **standard** [AA14, BCNP09, PB14]. **StateReveal** [Cre10]. **strong** [BM08]. **stronger** [Cre10]. **Strongly** [SOO10]. **study** [GSSC17]. **superdistribution** [WOS09]. **supply** [CLL⁺10]. **supporting** [BdMM08, Tan12]. **synchronous** [PCRS10]. **system** [SS09]. **systems** [NNO⁺17].

tagged [CLL⁺10]. **tapestry** [Boy08]. **technique** [ACS17]. **test** [Tan12]. **tests** [YWPZ09]. **Theoretical** [PR10]. **third** [HKK⁺10]. **threshold** [HKK⁺10]. **time** [BDE⁺13]. **tolerating** [PCR⁺09]. **transmission** [PCR⁺09, PCRS10]. **trusted** [HKK⁺10]. **Trustworthy** [LW17]. **trx** [LW17]. **TWISTER** [FFGL10].

Unconditionally [PCRS10, YWPZ09]. **undirected** [PCRS10]. **unforgeable** [SOO10]. **unicorn** [LW17]. **universal**

[OMO08]. **universally** [AO12]. **unlinkability** [AA14]. **User** [GMS09, FYL17]. **User-aware** [GMS09]. **using** [BKK⁺12, Cre10, GSSC17].

variants [YKP13]. **various** [HW08]. **vectors** [BNV17]. **verifier** [AA14]. **verifier-local** [AA14]. **version** [BCS17].

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

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

References

Ali:2014:DAB

[AA14] Syed Taqi Ali and B. B. Amberker. Dynamic attribute-based group signature with verifier-local revocation and backward unlinkability in the standard model. *International Journal of Applied Cryptography. IJACT*, 3(2):148–165, 2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Ateniese:2009:RAO

[ACJT09] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. Remarks on “Analysis of one popular group signature scheme” in Asiacrypt 2006 [MR2444651]. *International Journal of Applied Cryptography. IJACT*, 1(4):320–322, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Agrawal:2017:NAE

[ACS17] Megha Agrawal, Donghoon Chang, and Somitra Kumar

- Sanadhya. A new authenticated encryption technique for handling long ciphertexts in memory constrained devices. *International Journal of Applied Cryptography. IJACT*, 3(3):236–261, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.086223>.
- [AO12] Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. *International Journal of Applied Cryptography. IJACT*, 2(3):229–249, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [BCNP09] Colin Boyd, Yvonne Cliff, Juan M. González Nieto, and Kenneth G. Paterson. One-round key exchange in the standard model. *International Journal of Applied Cryptography. IJACT*, 1(3):181–199, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [BCS17] Tarun Kumar Bansal, Donghoon Chang, and Somitra Kumar Sanadhya. Sponge-based CCA2 secure asymmetric encryption for arbitrary length message (extended version). *International Journal of Applied Cryptography. IJACT*, 3(3):262–287, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.086222>.
- [BDE⁺13] Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Hülsing, and Markus Rückert. On the security of the Winternitz one-time signature scheme. *International Journal of Applied Cryptography. IJACT*, 3(1):84–96, 2013. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [BdMM08] M. Burmester, B. de Medeiros, and R. Motta. Anonymous RFID authentication supporting constant-cost key-lookup against active adversaries. *International Journal of Applied Cryptography. IJACT*, 1(2):79–90, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [BKK⁺12] Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery. Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction. *International Journal of Applied Cryptography. IJACT*, 2(3):212–228, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Buchmann:2013:SWO

Burmester:2008:ARA

Bos:2012:SBP

Abe:2012:FUC

Boyd:2009:ORK

Bansal:2017:SBC

- [BM08] Emmanuel Bresson and Mark Manulis. Securing group key exchange against strong corruptions and key registration attacks. *International Journal of Applied Cryptography. IJACT*, 1(2):91–107, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [CG17] Michael Clear and Ciarán Mc Goldrick. Attribute-based fully homomorphic encryption with a bounded number of inputs. *International Journal of Applied Cryptography. IJACT*, 3(4):363–376, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089356>.
- [BNV17] Joppe W. Bos, Michael Naehrig, and Joop Van De Pol. Sieving for shortest vectors in ideal lattices: a practical perspective. *International Journal of Applied Cryptography. IJACT*, 3(4):313–329, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089353>.
- [Boy08] Xavier Boyen. A tapestry of identity-based encryption: practical frameworks compared. *International Journal of Applied Cryptography. IJACT*, 1(1):3–21, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Cai:2010:AHS] Shaoying Cai, Yingjiu Li, Tiejian Li, Robert H. Deng, and Haixia Yao. Achieving high security and efficiency in RFID-tagged supply chains. *International Journal of Applied Cryptography. IJACT*, 2(1):3–12, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Chakraborty:2012:DCM] Debrup Chakraborty and Cuauhtemoc Mancillas-López. Double ciphertext mode: a proposal for secure backup. *International Journal of Applied Cryptography. IJACT*, 2(3):271–287, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Bos:2017:SSV] Joppe W. Bos, Michael Naehrig, and Joop Van De Pol. Sieving for shortest vectors in ideal lattices: a practical perspective. *International Journal of Applied Cryptography. IJACT*, 3(4):313–329, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089353>.
- [Bresson:2008:SGK] Emmanuel Bresson and Mark Manulis. Securing group key exchange against strong corruptions and key registration attacks. *International Journal of Applied Cryptography. IJACT*, 1(2):91–107, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Bao:2010:P] Feng Bao and Guilin Wang. Preface. *International Journal of Applied Cryptography. IJACT*, 2(1):1–2, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Cremers:2010:SSS] Cas J. F. Cremers. Session-StateReveal is stronger than eCKs EphemeralKeyReveal: using automatic analysis to attack the NAXOS protocol. *International Journal of Applied Cryptography. IJACT*, 2(2):83–99, 2010.
- [CLL+10] Shaoying Cai, Yingjiu Li, Tiejian Li, Robert H. Deng, and Haixia Yao. Achieving high security and efficiency in RFID-tagged supply chains. *International Journal of Applied Cryptography. IJACT*, 2(1):3–12, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [CML12] Debrup Chakraborty and Cuauhtemoc Mancillas-López. Double ciphertext mode: a proposal for secure backup. *International Journal of Applied Cryptography. IJACT*, 2(3):271–287, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

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

Ciss:2012:REE

- [CS12] Abdoul Aziz Ciss and Djiby Sow. Randomness extraction in elliptic curves and secret key derivation at the end of Diffie–Hellman protocol. *International Journal of Applied Cryptography. IJACT*, 2(4):360–365, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Chatterjee:2013:PHH

- [CS13] Sanjit Chatterjee and Palash Sarkar. Practical hybrid (hierarchical) identity-based encryption schemes based on the decisional bilinear Diffie–Hellman assumption. *International Journal of Applied Cryptography. IJACT*, 3(1):47–83, 2013. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Damgaard:2008:HES

- [DGK08] Ivan Damgård, Martin Geisler, and Mikkel Krøigård. Homomorphic encryption and secure comparison. *International Journal of Applied Cryptography. IJACT*, 1(1):22–31, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Damgaard:2009:CES

- [DGK09] Ivan Damgård, Martin Geisler, and Mikkel Krøigård. A correction to ‘Efficient and secure comparison for on-line auctions’. *International Journal of*

Applied Cryptography. IJACT, 1(4):323–324, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Dachman-Soled:2012:ERP

- [DSMRY12] Dana Dachman-Soled, Tal Malkin, Mariana Raykova, and Moti Yung. Efficient robust private set intersection. *International Journal of Applied Cryptography. IJACT*, 2(4):289–303, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Emura:2010:CPA

- [EMO⁺10] Keita Emura, Atsuko Miyaji, Kazumasa Omote, Akito Nomura, and Masakazu Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. *International Journal of Applied Cryptography. IJACT*, 2(1):46–59, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Emura:2012:DAB

- [EMR12] Keita Emura, Atsuko Miyaji, and Mohammad Shahriar Rahman. Dynamic attribute-based signcryption without random oracles. *International Journal of Applied Cryptography. IJACT*, 2(3):199–211, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Farashahi:2014:HHC

- [Far14] Reza Rezaeian Farashahi. Hashing into Hessian curves. *International Journal of Applied Cryptography. IJACT*, 3(2):139–147,

2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Fleischmann:2010:TFS

- [FFGL10] Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks. TWISTER π — a framework for secure and fast hash functions. *International Journal of Applied Cryptography. IJACT*, 2(1):68–81, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Feng:2017:NPR

- [FYL17] Yiteng Feng, Guomin Yang, and Joseph K. Liu. A new public remote integrity checking scheme with user and data privacy. *International Journal of Applied Cryptography. IJACT*, 3(3):196–209, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.086232>.

Gajek:2009:UAP

- [GMS09] Sebastian Gajek, Mark Manulis, and Jörg Schwenk. User-aware provably secure protocols for browser-based mutual authentication. *International Journal of Applied Cryptography. IJACT*, 1(4):290–308, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Goldberg:2010:MRP

- [GMS10] Ian Goldberg, Atefeh Mashatan, and Douglas R. Stinson. On mes-

sage recognition protocols: recoverability and explicit confirmation. *International Journal of Applied Cryptography. IJACT*, 2(2):100–120, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Ghosh:2017:PFA

- [GSSC17] Shamit Ghosh, Dhiman Saha, Abhrajit Sengupta, and Dipanwita Roy Chowdhury. Preventing fault attacks using fault randomisation with a case study on AES. *International Journal of Applied Cryptography. IJACT*, 3(3):225–235, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.086231>.

Hinek:2012:ABE

- [HJSNS12] M. Jason Hinek, Shaoquan Jiang, Reihaneh Safavi-Naini, and Siamak F. Shahandashti. Attribute-based encryption without key cloning. *International Journal of Applied Cryptography. IJACT*, 2(3):250–270, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Hong:2010:FTD

- [HKK⁺10] Jeongdae Hong, Jinil Kim, Jihye Kim, Matthew K. Franklin, and Kunsoo Park. Fair threshold decryption with semi-trusted third parties. *International Journal of Applied Cryptography. IJACT*, 2(2):139–153, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

- [HLW08] **Huang:2008:EOM**
 Qiong Huang, Dennis Y. W. Liu, and Duncan S. Wong. An efficient one-move nominative signature scheme. *International Journal of Applied Cryptography. IJACT*, 1(2):133–143, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [HN09] **Hakala:2009:MLD**
 Risto M. Hakala and Kaisa Nyberg. A multidimensional linear distinguishing attack on the Shannon cipher. *International Journal of Applied Cryptography. IJACT*, 1(3):161–168, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [HS10] **Hagaliletto:2010:DAS**
 Anders Moen Hagaliletto and Lars Strand. Designing attacks on SIP call set-up. *International Journal of Applied Cryptography. IJACT*, 2(1):13–22, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [HSS09] **Huang:2009:FRA**
 Jianyong Huang, Jennifer Seberry, and Willy Susilo. A five-round algebraic property of AES and its application to the ALPHA-MAC. *International Journal of Applied Cryptography. IJACT*, 1(4):264–289, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [HW08] **Huang:2008:RAV**
 Qiong Huang and Duncan S. Wong. On the relation among various security models for certificateless cryptography. *International Journal of Applied Cryptography. IJACT*, 1(2):108–119, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [HY08] **Herzberg:2008:LGF**
 Amir Herzberg and Igal Yoffe. The layered games framework for specifications and analysis of security protocols. *International Journal of Applied Cryptography. IJACT*, 1(2):144–159, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [ISW17] **Ishida:2017:CSR**
 Yuu Ishida, Junji Shikata, and Yohei Watanabe. CCA-secure revocable identity-based encryption schemes with decryption key exposure resistance. *International Journal of Applied Cryptography. IJACT*, 3(3):288–311, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.086229>.
- [JLP10] **Jin:2010:DAP**
 Hongxia Jin, Jeffrey Lotspiech, and Serdar Pehlivanoglu. Defending against the pirate evolution attack. *International Journal of Applied Cryptography. IJACT*, 2(1):23–34, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

- [JM08] **Jakobsson:2008:DPD**
Markus Jakobsson and Steven Myers. Delayed password disclosure. *International Journal of Applied Cryptography. IJACT*, 1(1):47–59, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [JP13] **Jarrous:2013:SCF**
Ayman Jarrous and Benny Pinkas. Secure computation of functionalities based on Hamming distance and its application to computing document similarity. *International Journal of Applied Cryptography. IJACT*, 3(1):21–46, 2013. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [KH08] **Kurosawa:2008:PIS**
Kaoru Kurosawa and Swee-Huay Heng. The power of identification schemes. *International Journal of Applied Cryptography. IJACT*, 1(1):60–69, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [KP17] **Kurosawa:2017:IFP**
Kaoru Kurosawa and Le Trieu Phong. IBE and function-private IBE under linear assumptions with shorter ciphertexts and private keys, and extensions. *International Journal of Applied Cryptography. IJACT*, 3(3):210–224, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089355>.
- [LBM14] **Lerman:2014:PAA**
Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. Power analysis attack: an approach based on machine learning. *International Journal of Applied Cryptography. IJACT*, 3(2):97–115, 2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Leu08] **Leurent:2008:PKR**
Gaëtan Leurent. Practical key-recovery attack against APOP, an MD5-based challenge-response authentication. *International Journal of Applied Cryptography. IJACT*, 1(1):32–46, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Lip17] **Lipmaa:2017:PEC**
Helger Lipmaa. Prover-efficient commit-and-prove zero-knowledge SNARKs. *International Journal of Applied Cryptography. IJACT*, 3(4):344–362, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089355>.
- [LN14] **Loebenberger:2014:NRI**
Daniel Loebenberger and Michael Nüsken. Notions for RSA integers. *International Journal of Applied Cryptography. IJACT*, 3(2):116–138, 2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

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

Lenstra:2017:TPR

- [LW17] Arjen K. Lenstra and Benjamin Wesolowski. Trustworthy public randomness with sloth, unicorn, and trx. *International Journal of Applied Cryptography. IJACT*, 3(4):330–343, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089354>.

Menezes:2009:CPP

- [MU09] Alfred Menezes and Berkant Ustaoglu. Comparing the pre- and post-specified peer models for key agreement. *International Journal of Applied Cryptography. IJACT*, 1(3):236–250, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Menezes:2010:REK

- [MU10] Alfred Menezes and Berkant Ustaoglu. On reusing ephemeral keys in Diffie–Hellman key agreement protocols. *International Journal of Applied Cryptography. IJACT*, 2(2):154–158, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Nakagawa:2017:PEA

- [NNO⁺17] Sanami Nakagawa, Takashi Nishide, Eiji Okamoto, Keita Emura, Goichiro Hanaoka, Yusuke Sakai, and Akihisa Kodate. A privacy-enhanced access log management mechanism in SSO

systems from nominative signatures. *International Journal of Applied Cryptography. IJACT*, 3(4):394–406, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL <https://www.inderscienceonline.com/doi/pdf/10.1504/IJACT.2017.089373>.

Okada:2008:OFE

- [OMO08] Yusuke Okada, Yoshifumi Manabe, and Tatsuaki Okamoto. An optimistic fair exchange protocol and its security in the universal composability framework. *International Journal of Applied Cryptography. IJACT*, 1(1):70–77, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Patel:2014:RFP

- [PB14] Hiren Patel and Rusty O. Baldwin. Random forest profiling attack on Advanced Encryption Standard. *International Journal of Applied Cryptography. IJACT*, 3(2):181–194, 2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Patra:2009:PRS

- [PCR⁺09] Arpita Patra, Ashish Choudhary, C. Pandu Rangan, Kamman Sriathan, and Prasad Raghavendra. Perfectly reliable and secure message transmission tolerating mobile adversary. *International Journal of Applied Cryptography. IJACT*, 1(3):200–224, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

- [PCRS10] **Patra:2010:URS** Arpita Patra, Ashish Choudhury, C. Pandu Rangan, and Kannan Srinathan. Unconditionally reliable and secure message transmission in undirected synchronous networks: possibility, feasibility and optimality. *International Journal of Applied Cryptography. IJACT*, 2(2):159–197, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [PR10] **Prouff:2010:TPA** E. Prouff and M. Rivain. Theoretical and practical aspects of mutual information-based side channel analysis. *International Journal of Applied Cryptography. IJACT*, 2(2):121–138, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [PSWH08] **Plantard:2008:ELB** Thomas Plantard, Willy Susilo, Khin Than Win, and Qiong Huang. Efficient lattice-based signature scheme. *International Journal of Applied Cryptography. IJACT*, 1(2):120–132, 2008. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [SEV17] **Sarr:2017:SBF** Augustin P. Sarr and Philippe Elbaz-Vincent. On the separation between the FHMV and HMQV protocols. *International Journal of Applied Cryptography. IJACT*, 3(4):377–393, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [SLdW12] **Stevens:2012:CPC** Marc Stevens, Arjen K. Lenstra, and Benne de Weger. Chosen-prefix collisions for MD5 and applications. *International Journal of Applied Cryptography. IJACT*, 2(4):322–359, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [SOO10] **Sato:2010:SUI** Chifumi Sato, Takeshi Okamoto, and Eiji Okamoto. Strongly unforgeable ID-based signatures without random oracles. *International Journal of Applied Cryptography. IJACT*, 2(1):35–45, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [SS09] **Sui:2009:CAI** Jiayuan Sui and Douglas R. Stinson. A critical analysis and improvement of advanced access content system drive-host authentication. *International Journal of Applied Cryptography. IJACT*, 1(3):169–180, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).
- [Tan12] **Tang:2012:PKE** Qiang Tang. Public key encryption schemes supporting equality test with authorisation of different granularity. *International*

Journal of Applied Cryptography. IJACT, 2(4):304–321, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Veugen:2014:EID

- [VeU14] Thijs Veugen. Encrypted integer division and secure comparison. *International Journal of Applied Cryptography. IJACT*, 3(2):166–180, 2014. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Wolf:2009:SOS

- [WOS09] Marko Wolf, André Osterhues, and Christian Stübke. Secure offline superdistribution for mobile platforms. *International Journal of Applied Cryptography. IJACT*, 1(4):251–263, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Yang:2009:MPQ

- [YBDD09] Yanjiang Yang, Feng Bao, Xuhua Ding, and Robert H. Deng. Multiuser private queries over encrypted databases. *International Journal of Applied Cryptography. IJACT*, 1(4):309–319, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Yap:2013:PVC

- [YKP13] Huihui Yap, Khoongming Khoo, and Axel Poschmann. Parallelisable variants of Camellia and SMS4 block cipher: p-Camellia and p-SMS4. *International Journal of Applied Cryptography. IJACT*, 3(1):1–20, 2013. CO-

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

Ye:2009:USD

- [YWPZ09] Qingsong Ye, Huaxiong Wang, Josef Pieprzyk, and Xian-Mo Zhang. Unconditionally secure disjointness tests for private datasets. *International Journal of Applied Cryptography. IJACT*, 1(3):225–235, 2009. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Zhang:2010:SRC

- [ZSWF10] Wentao Zhang, Bozhan Su, Wenling Wu, and Dengguo Feng. Some results on cryptanalysis of SMS4 block cipher. *International Journal of Applied Cryptography. IJACT*, 2(1):60–67, 2010. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).