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

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`.

Abe:2012:FUC

[AO12] Masayuki Abe and Miyako Ohkubo. A framework for universally composable noncommitting blind signatures. *International Journal of Applied Cryptography. IJACT*, 2(3):229–249, 2012. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic).

Boyd:2009:ORK

[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).

Bansal:2017:SBC

[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`.

Buchmann:2013:SWO

[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).

Burmester:2008:ARA

[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).

Bos:2012:SBP

[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).

Bresson:2008:SGK

[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).

Bos:2017:SSV

[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`.

Boyen:2008:TIB

[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).

Bao:2010:P

[BW10] 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).

Clear:2017:ABF

[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`.

Cai:2010:AHS

[CLL$^+$10] Shaoying Cai, Yingjiu Li, Tieyan 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

[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).

Cremers:2010:SSS

[Cre10] 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. 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. TWISTERπ — 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 message 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).

Huang:2008:EOM

[HLW08] 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).

Hakala:2009:MLD

[HN09] 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).

Hagalisletto:2010:DAS

[HS10] Anders Moen Hagalisletto 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).

Huang:2009:FRA

[HSS09] 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).

Huang:2008:RAV

[HW08] 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).

Herzberg:2008:LGF

[HY08] 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).

Ishida:2017:CSR

[ISW17] 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`.

Jin:2010:DAP

[JLP10] 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).

Jakobsson:2008:DPD

[JM08] 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).

Jarrous:2013:SCF

[JP13] 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).

Kurosawa:2008:PIS

[KH08] 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).

Kurosawa:2017:IFP

[KP17] 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.2017.086224`.

Lerman:2014:PAA

[LBM14] 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).

Leurent:2008:PKR

[Leu08] 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).

Lipmaa:2017:PEC

[Lip17] 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`.

Loebenberger:2014:NRI

[LN14] 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).

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, Kannan Srinathan, 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).

Patra:2010:URS

[PCRS10] 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).

Prouff:2010:TPA

[PR10] 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).

Plantard:2008:ELB

[PSWH08] 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).

Sarr:2017:SBF

[SEV17] Augustin P. Sarr and Philippe Elbaz-Vincent. On the separation between the FHMQV and HMQV protocols. *International Journal of Applied Cryptography. IJACT*, 3(4):377–393, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL `https://www.inderscienceonline.com//doi/pdf/10.1504/IJACT.2017.089357`.

Stevens:2012:CPC

[SLdW12] 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).

Sato:2010:SUI

[SOO10] 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).

Sui:2009:CAI

[SS09] 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).

Tang:2012:PKE

[Tan12] 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 Stüble. 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. CODEN ???? 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).