Verifiable and Untraceable Message Extraction System

Ya-Fen Chang*, Jian-Hong Ciou, and Jheng-Jhe Lin

Department of Computer Science and Information Engineering

National Taichung Institute of Technology

Taichung 404, Taiwan, R.O.C

cyf@cs.ccu.edu.tw

Received 18 May 2008; Revised 19 June 2009; Accepted 5 July 2009

Abstract. With the rapid growth of network technologies, privacy becomes an important issue. In this manuscript, we design a verifiable and untraceable message extraction system having users be able to get desired messages without leaking what they are. This system applies OT (oblivious transfer) to satisfy the special privacy requirement.

Keywords: OT scheme, NIOT scheme, e-magazine

References

[1] M. O. Rabin, "How to Exchange Secrets by Oblivious Transfer," *Technical Report TR-81,* Harvard Aiken Computation Laboratory, 1981.

[2] M. Bellare and S. Micali, "Non-interactive Obvious Transfer and Application," *Advances in Cryptology: CRYPTO'89,* Springer-Verlag, Germany, Vol. 435, pp. 119-135, 1989.

[3] S. Kim, S. Kim, G. Lee, "Secure Verifiable Non-interactive Oblivious Transfer Protocol Using RSA and Bit Commitment on Distributed Environment," *Future Generation Compute*r, Vol. 25, No. 3, pp. 352-357, March 2009.

[4] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *Information Theory*, Vol. 31, No. 4, pp. 469-472, 1985.

[5] T. Cormen, C. Leiserson, R. Rivest, C. Stein, *Introduction to Algorithms*, Cambridge, MA:MIT Press, 2001.

[6] D. Stinson, *Cryptography-Theory and Practice*, CRC Press, Boca Raton, 1995.

[7] X.Y. Wang, F.D. Guo, X.J. Lai, H.B. Yu, Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, *Rump Session of CRYPTO'04*, E-print, 2004.

[8] B. den Boer, "Oblivious Transfer Protecting Secrecy," *Advances in Cryptology: EUROCRYPT'9*0, Vol. 473, pp. 31-46, 1990.

[9] C. Crepeau, "Equivalence between Two Flavors of Oblivious Transfer," *Advances in Cryptology: CRYPTO'87*, Springer-Verlag, Germany, Vol. 293, pp. 350-354, 1987.

[10] C. Crepeau and J. Kilian, "Weakening Security Assumptions and Oblivious Transfer," *Advances in Cryptology: CRYPTO'88*, Springer-Verlag, Germany, Vol. 403, pp. 2-7, 1988.

[11] O. Wakaha and S. Ryota, "k out of n Oblivious Transfer without Random Oracle," *IEICE Transactions on Fundamentals of Electronics, Communication and Computer Sciences*, Vol. E87-A, No. 1, pp. 147-151, January 2004.

[12] S. Even, O. Goldreich, A. Lempel, "A Randomized Protocol for Signing Contracts," *Advanced in Cryptology: CRYPTO'82*, Plenum Press, New York, pp. 205-210, 1982.

* Correspondence author

[13] M. O. Rabin, "How to Exchange Secrets by Oblivious Transfer," *Technical Report TR-81*, Harvard Aiken Computation Laboratory, 1981.

[14] B. Aiello, Y. Ishai, O. Reingold, "Priced Oblivious Transfer: How to Sell Digital Goods," *Advances in Cryptology: EUROCRYPT 2001*, Springer-Verlag, Germany, Vol. 2045, pp. 119-135, 2001.

[15] M. Naor and B. Pinkas, "Efficient Oblivious Transfer Protocols," in *Proceedings of SIAM Symposium on Discrete Algorithms 2001*, pp. 448-457, January 2001.

[16] A. D. Saint and G. Persiano, "Public-randomness in Public-key Cryptography," *Advances in Cryptology: EUROCRYPT'90*, Springer-Verlag, Germany, Vol. 473, pp. 46-61, 1990.

[17] Y.F. Chang and W.C. Shiao, "The Essential Design Principles of Verifiable Non-interactive OT Protocols," in *Proceedings of ISDA 2008*, Vol. 3, pp. 241-245, November 2008.

[18] http://www.microsoft.com