Anonymous Electronic Lottery Protocol[1]

Chun-I Fan*, Chun-Liang Chang, Ming-Te Chen, and Pei-Hsiu Ho

Department of Computer Science and Engineering

National Sun Yat-sen University

Kaohsiung, Taiwan, ROC

cifan@cse.nsysu.edu.tw

Received 30 May 2009; Revised 1 July 2009; Accepted 10 July 2009

Abstract. Due to the mature of networks and communication technologies, electronic commerce is growing up rapidly and many advanced applications in electronic commerce have been developed recently, such as on-line shopping, on-line bidding, and on-line gambling. There are numerous types of gambling like typical lottery, sport lottery, and poker gambling. Our research will focus on the lottery games. Owing to some special characteristics of the lottery games, such as fairness and anonymity, it is hard to design a secure electronic lottery protocol. The transaction mechanism in an electronic lottery protocol is an important issue since it will affect the benefits of customers if it is not fair or secure. Generating random winning tickets in a lottery game has been discussed in many papers, but the fairness and anonymity for purchasing tickets and claiming the prizes are only discussed in few papers and these previous results cannot completely cope with the problems of fairness and anonymity. In the paper, we propose an electronic lottery protocol that can achieve fairness and robust anonymity simultaneously.

Keywords: electronic lottery, partially blind signatures, anonymous channels, secure rewarding, untraceable electronic cash

References

[1] D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques-EUROCRYPT* 03, LNCS 2656, pp. 416-432, 2003.

[2] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, Vol. 24, pp. 84-88, 1981.

[3] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, Vol. 1, No. 1, pp. 65-75, 1988.

[4] D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology Proceeding of CRYPTO 82*, pp. 199-203, 1983.

[5] S.S.M. Chow, L.C.K. Hui, S.M. Yiu, K.P. Chow, "Practical Electronic Lotteries with Offline TTP," *Computer Communications*, Vol. 29, pp. 2830-2840, 2006.

[6] C.I. Fan and C.L. Lei, "Secure Rewarding Schemes," in *Proceedings of the 30th Hawaii International Conference on System Sciences: Information System Track-Organizational Systems and Technology*, Vol. 3, pp. 571-580, 1997.

[7] C.I. Fan and C.L. Lei, "Low-Computation Partially Blind Signatures for Electronic Cash," *IEICE Transactions on Fundamentals of Electronics*, *Communications and Computer Sciences*, Vol. E81-A, pp. 818-824, 1998.

[8] C.I. Fan and C.L. Lei, "A User Efficient Fair Blind Signature Scheme for Untraceable Electronic Cash," *Journal of Information Science and Engineering*, Vol. 18, pp. 47-58, 2002.

[9] C.I. Fan, "Improved Low-Computation Partially Blind Signatures," *Applied Mathematics and Computation*, pp. 853-867, 2003.

[10] P.A. Fouque, G. Poupard, J. Stern, "Sharing Decryption in the Context of Voting or Lotteries," in *Proceedings of the 4th International Conference on Financial Cryptography*, LNCS 1962, pp. 90-104, 2001.

[11] D.M. Goldschlag and S.G. Stubblebine, "Publicly Verifiable Lotteries: Applications of Delaying Functions," in *Proceedings of the 2nd International Conference on Financial Cryptography*, LNCS 1465, pp. 214-226, 1998.

[12] W. Ham and K. Kim, "A Secure On-line Lottery Using Bank as a Notary," *CISC*, pp. 121-124, 2002.

[13] K. Kobayashi, H. Morita, M. Hakuta, T. Nakanowatari, "An Electronic Soccer Lottery System that Uses Bit Commitment," *IEICE Transaction on Information and Systems*, Vol. E83-D, No. 5, pp. 980-987, 2000.

[14] E. Konstantinou, V. Liagkou, P. Spirakis, Y.C. Stamatiou, M. Yung, "Electronic National Lotteries," in *Proceedings of the 8th International Conference on Financial Cryptography*, LNCS 3110, pp. 147-163, 2004.

[15] E. Kushilevitz and T. Rabin, "Fair E-Lotteries and E-Casinos," *The Cryptographers' Track at RSA Conference*, LNCS 2020, pp. 100-109, 2001.

[16] I. Ray and N. Natarajan, "An Anonymous and Failure Resilient Fair-Exchange E-Commerce Protocol," *Decision Support Systems*, Vol. 39, No. 3, pp. 267-292, 2005.

[17] K. Sako, "Implementation of a Digital Lottery Server on WWW," in *Proceedings of the International Exhibition and Congress on Secure Networking - CQRE (Secure) '99*, LNCS 1740, pp. 101-108, 1999.

[1] A partial result of this research has been presented at National Information Security Conference 2006, Taiwan.

* Correspondence author

[18] P. Syverson, "Weakly Secret Bit Commitment: Applications to Lotteries and Fair Exchange," in *Proceedings of the 11th IEEE Computer Security Foundations Workshop*, pp. 2-13, 1998.
[19] H. Xu, X. Fu, Y. Zhu, R. Bettati, J. Chen, W. Zhao, "SAS: A Scalar Anonymous Communication System," in *Proceedings of the 3rd International Conference on Networking and Mobile Computing*, LNCS 3619, pp. 452-461, 2005.
[20] J. Zhou and C. Tan, "Playing Lottery on the Internet," in *Proceedings of the 3rd International Conference on Information and Communications Security*, LNCS 2229, pp. 189-201, 2001.
[21] M. Abe and E. Fujisaki, "How to Date Blind Signatures," *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, pp. 244-251, 1996.