Anonymous Electronic Lottery Protocol

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


* Correspondence author

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

