Anonymous Reader Authentication for RFID-enabled Mobile Devices

Hung-Yu Chien* and Chieh-Shian Tu

Department of Information Management

National Chi-Nan University

Puli 545, Taiwan, R.O.C

{hychien, s96213533}@ncnu.edu.tw

Received 1 June 2009; Revised 30 June 2009; Accepted 15 July 2009

Abstract. Recently, Lo et al.'s have addressed that building a light-weight secure communication is necessary for reader-to-server channel in RFID systems, because resource-limited mobile readers are becoming more and more popular. Therefore, Lo et al. proposed an elliptic curve cryptography (ECC) - based lightweight authentication protocol for reader-server channel. However, we find that their scheme has the security weaknesses: (1) the trusted third party's private key would be disclosed such that the whole system would be broken and (2) there is no authentication of the keying materials. To conquer while preserving the light-weight property, we propose a new authentication protocol for reader-server channel using ID-based cryptography from elliptic curves.

Keywords: RFID, mutual authentication, Elliptic curve cryptography

References

[1] A.Yamamoto, S. Suzuki, H. Hada, J. Mitsugi, F. Teraoka, O. Nakamura, "A Temper Detection Method for RFID Data," *IEEE International Conference on RFID*, pp. 51-57, April 16-17, 2008.

[2] B. Song and C. J. Mitchell, "RFID Authentication Protocol for Low-cost Tags," In *WISEC*, pp. 140-147, 2008.

[3] D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," in *Conference on Computer and Communications Security – CCS'04*, ACM press, pp. 210-219, 2004.

[4] D. N. Duc, J. Park, H. Lee, K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," in *Proceedings of the 2006 Symposium on Cryptography and Information Security – SCIS'06*, 2006.

[5] H.Y. Chien and C.H. Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 standards," *Computer Standards and Interfaces*, Vol. 29, No. 2, pp. 254-259, February 2007.

[6] H. Y. Chien and C. W. Huang, "A Lightweight RFID Protocol Using Substring," In *EUC*, pp. 422-431, 2007.

[7] N.W. Lo, K.H. Yeh, C.Y. Yeun, "New Mutual Agreement Protocol to Secure Mobile RFID-enabled Devices," *Information Security Technical Report*, pp. 151-157, 2008.

* Correspondence author