RFID Data Security and Privacy Based on XOR Algorism

Chih-Yung Chen*

Department of Information Management,
St. John's University,
New Taipei 251, Taiwan, ROC
yung@mail.sju.edu.tw

Received 12 March 2011; Revised 25 May 2011; Accepted 20 August 2011

Abstract. The application of RFID after years of development, there are already many cases of the industries applied, and it is considered to be Tag as the next generation of Barcode. Therefore, if Tag use as a commodity recognition in the future, but as consumers purchase goods in shopping malls, if suffered from hackers by the analysis frequency signal to access information, the purchase of commodities are exposed completely. Therefore, RFID in the Data Security and Privacy is hidden in a crisis. RFID Data Security and Privacy protection using hardware ways to achieve the target is the best way; however, it is subject to the problem of Tag costs and capacity and is currently still unresolved issues. This study focus on the Data Security and Privacy protection and put forth a EPC specifications to use the model of XOR logic operation with the method of CRC examining the computing, and simulating the shopping mall system which provides a Data Security and Privacy protection system. We got the data after simulations to show that XOR computing to 8 bytes actual test, the required time is 17.29 Ticks in average, the spend time is rather short. Follow-up our simulations to the test data of DES encryption methods, an average time of 8,039.41 Ticks is required, the two time required considerable differences. It was informed that this study through practical shows that we could provide a match hardware encryption methods of the specific solutions to achieve their personal privacy protection, confidentiality, confirmed, and the fulfillment of the Data Security and Privacy protection.

Keywords: RFID, data security, privacy, EPC, tag, XOR

References

[1] Ministry of Finance RFID Office for Promoting Public Applied in the Area of Electronic Fortnightly RFID Developments, No. 5, http://RFID.More.Org.tw/epaper5/ver05.c.HTML

[2] Radio Frequency Identification Technology in the Federal Government, http://www.gao.gov/new.items/d05551.pdf

[3] Developing NationalPolicies on the Deployment of Radio Frequency Identification (RFID) Technology, http://www.ieeeusa.org/policy/positions/rfid.html

[4] L.Y. Li, "Identity in a Dynamic Base to Protect Low-cost Passive Radio Frequency Identification Tag Subject to the User Privacy," *Master's Thesis, Department of Information Engineer , National Chiao Tung University*, 2005.

[5] S. L. Garfinkel, A. Juels, R. Pappu, "RFID Privacy: an Overview of Problems and Proposed Solutions," *IEEE Security and Privacy*, Vol. 3, No. 3, pp. 34-43, 2005.

[6] Ministry of Economic Affairs office, "Promoting innovation Australia again Auto-ID Lab Lightweight Permitive," published, http://www.RFID.Org. tw/content.PHP? sn=195

[7] A. Juels, R. L. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

[8] T. Phillips, T. Karygiannis, R. Kuhn, "Security Standards for the RFID Market," *IEEE Security and Privacy*, Vol. 3, No. 6, pp. 85-89, 2005.

*Correspondence author