

Analysis of Security Issues in SMC based RFID in Supply Chain Management with Energy Modeling

Rohit Pathak[‡], Satyadhar Joshi[†]

[‡] Acropolis Institute of Technology & Research, Indore, M.P., India
[†] Shri Vaishnav Institute of Technology & Science, Indore, M.P., India
xrohit@hotmail.com, satyadhar_joshi@yahoo.com

Abstract- RFID (Radio Frequency Identification) has been used in Supply Chain management but with the advent of Nanotechnology enabled RFID energy consumption is being constantly decreased. The major issues between implementation of such devices are their reliability and security. In this work we have implemented a novel and effective VPP (Virtual Party Protocol) for RFID systems. Use of VPP and insertion of anonymous has been implemented for RFID systems and the advantages over other methods are shown. The mathematical analysis is done for the proposal and its implications are discussed. In this protocol the creation of virtual party to hide the data of the Tags are shown, this method though can be used for joint computation and for other information the hardware needs to be tuned to the requirements. Energy requirements are also shown in this work for a VPP based RFID systems.

I. INTRODUCTION

Business is being enhanced by the advent of RFID technologies. RFID technologies benefit from development of many technologies. But the development of SMC where secure joint computation needs to be done is any area which is highly sophisticated because of fewer theories in the area. Business application of RFID can be felt in all domains and therefore building a secure model for RFID is a necessity. As we know that in supply chain management the Tags are passed from various Parties which want to get information about the Tags to detect the possibility of any errors or damage of the systems. In our previous work we have proposed the application of SMC protocols in RFIDs [20]. Five major Critical issues in an RFID security are defined as Confidentiality, Integrity, Authentication, Anonymity, and Availability are defined in [16]. Author has also done an elementary comparison of the security proposals. Cryptographic module based on an 8 bit microprocessor has been shown by Kaiser [1], where he has described the implementation of the protocol on the microprocessor. These methods are good for general RFID but not for passive RFIDs. Tracking resistance and identification performance has been discussed in [2], where author talks methods such as hiding of tag information using less complex and less costly password

management. RFID's application is supply chain management is well known, Piramuthu in [3] shows about the recent protocols for passive RFID system which are the most common used, in that work some issues to make lightweight cryptography is addressed but it does not give a totally hack proof system. Anti-counterfeit ownership transfer in a RFID system is an area in which the ownership transfer issue needs to be resolved, an attempt has been made in [4] for the proposing a solution. Noisy Cryptographic Protocols for Low-Cost RFID Tags has been proposed in [5], where the noise is used for improving the security. This method talks about the using the noisy environment and it shows the methodology to implement the same. The developments of Nanotechnology, MEMS have an effect on the RFID systems [6]. Thus in most of the cases author talks about cryptography but the problem of secure multi party computation has been not been addressed which we have tried to work in this project. The idea for coming with a SMC protocol is obvious and its applications are also vast in this area especially in Supply Chain Management. Tracking becomes an issue when RFID and reader interacts, thus a secret sharing needs to be build up between them, some elementary idea is being given earlier for the issue in [12]. Security of RFID basically depends on reader, responder and the database. Thus security measures taken and analysis has been previously done using for CASPER, CSP and FDR [9]. A hash lock was proposed by the author in the work for improving the security. Design of a lightweight RFID security protocol based on the ID Blind Scheme and ECC (Elliptic Curve Cryptography) has been shown in [6x]. It is expected to offers enhanced security feature in RFID security with respect to user privacy against tag cloning allowing an additional ECC modular operation [14]. Tag is tough the main focus sometimes reader also needs to hide information which is a rare case but eminent, idea is expanded in [13] where author has discussed about the reader side security issues and constrains.

II. PROBLEM STATEMENT

- Cybernetics, Part C: Applications and Reviews, Vol. 38, Issue 3, pp. 360–376, May 2008, DOI=10.1109/TSMCC.2007.913918.
- [4] Chin-Ling C., Yu-Yi C., Yu-Cheng H., Chen-Shen L., Chia-I L., Tzay-Farn S., "Anti-counterfeit ownership transfer protocol for low cost RFID system," *WSEAS Transactions on Computers*, Vol. 7, Issue 8, pp. 1149–1158, Aug. 2008.
- [5] Chabanne H., Fumaroli G., "Noisy Cryptographic Protocols for Low-Cost RFID Tags," *IEEE Transactions on Information Theory*, Vol. 52, Issue 8, pp. 3562–3566, Aug. 2006, DOI=10.1109/TIT.2006.878219.
- [6] Rohit P., Satyadhar J., "Multi Scale Modeling and Intricate Study of MEMS Based Elements in RFID systems" *Proc. Conference on Innovative Technologies in Intelligent Systems & Industrial Applications, (CITISIA2009)*, Jul. 2009, DOI=10.1109/CITISIA.2009.5224196.
- [7] Damgard I., Pedersen M.O., "RFID security: tradeoffs between security and efficiency," *Cryptology ePrint Archive*, Report 2006/234, 2006.
- [8] Rohit P., Satyadhar J., "Secure Multi-party Computation Using Virtual Parties for Computation on Encrypted Data," *Advances in Information Security and Assurance, Springer Lecture Notes on Computer Science, Springer Berlin / Heidelberg*, Vol. 5576/2009, Jun. 2009, DOI=10.1007/978-3-642-02617-1_42.
- [9] Hyun-Seok K., Jin-Young C., "Security and Privacy Analysis of RFID Authentication Protocol for Ubiquitous Computing," *Proc. 16th International Conference on Computer Communications and Networks, ICCCN 2007*, pp. 1359–1363, 13-16 Aug. 2007
- [10] Mache J., Allick C., "The Cost of Preserving Privacy: Performance Measurements of RFID Pseudonym Protocols," *Proc. The Second International Conference on Availability, Reliability and Security, ARES 2007*, pp. 606–609, 10-13 Apr. 2007.
- [11] Zongwei L., Chan T., Li J.S., "A lightweight mutual authentication protocol for RFID networks," *Proc. IEEE International Conference on e-Business Engineering, ICEBE 2005*, pp. 620–625, 18-21 Oct. 2005
- [12] Yoon-Su J., Ning S., Yoon-Cheol H., Ki-Su K., Sang-Ho L., "RFID Authentication Protocol Using Synchronized Secret Information," *Proc. The First International Symposium on Data, Privacy, and E-Commerce, ISDPE 2007*, pp. 459–461, 1-3 Nov. 2007
- [13] Inseop K., Byunggil L., Howon K., "Privacy-Friendly Mobile RFID Reader Protocol Design based on trusted Agent and PKI," *Proc. IEEE Tenth International Symposium on Consumer Electronics, ISCE apos;06*, pp. 1–6, 2006.
- [14] Kim S.J., Kim Y.S., Park S.C., "RFID Security Protocol by Lightweight ECC Algorithm" *Proc. 6th International Conference on Advanced Language Processing and Web Information Technology, ALPIT 2007*, pp. 323-328, 22-24 Aug. 2007.
- [15] Mooseop K., Jaecheol R., Yongje C., Sungik J., "Low-cost Cryptographic Circuits for Authentication in Radio Frequency Identification Systems," *Proc. IEEE Tenth International Symposium on Consumer Electronics, ISCE apos;06*, pp.1–5, 2006
- [16] Sharif A., Potdar V., "A Critical Analysis of RFID Security Protocols," *Proc. 22nd International Conference on Advanced Information Networking and Applications - Workshops, AINAW 2008*, pp.1357–1362, 25-28 Mar. 2008.
- [17] Sample A.P., Yeager D.J., Powledge P.S., Mamishev A.V., Smith J.R., "Design of an RFID-Based Battery-Free Programmable Sensing Platform," *IEEE Transactions on Instrumentation and Measurement*, Vol. 57, Issue 11, pp. 2608-2615, Nov. 2008.
- [18] Zongwei L., Terry C., Jenny S.L., Edward W., William C., Victor N., Wilton F., "Experimental Analysis of an RFID Security Protocol," *Proc. IEEE International Conference on e-Business Engineering, ICEBE '06*, pp. 62-70, Oct. 2006.
- [19] Rohit P., Satyadhar J., "Secure Multi-Party Computation Protocol for Statistical Computation on Encrypted," *Proc. of 2009 International Conference on Software Technology and Engineering (ICSTE 2009)*, 24-26 Jul. 2009.
- [20] Rohit P., Satyadhar J., "Secure Multi-party Computation Protocol for Defense Applications in Military Operations using Virtual Cryptography," *Contemporary Computing, Communications in Computer and Information Science, Springer Berlin Heidelberg*, Vol. 40, 17-19 Aug. 2009, DOI=10.1007/978-3-642-03547-0_37.
- [21] Rohit P., Satyadhar J., "Secured Communication for Business Process Outsourcing using Optimized Arithmetic Cryptography Protocol based on Virtual Parties," *Contemporary Computing, Communications in*
- Computer and Information Science, Springer Berlin Heidelberg*, Vol. 40, 17-19 Aug. 2009, DOI=10.1007/978-3-642-03547-0_20.