A Lightweight Authentication Protocol for Internet of Things

Jun-Ya Lee, Wei-Cheng Lin
Electrical Engineering
I-Shou University
Kaohsiung, Taiwan
leon01134@hotmail.com, byron@isu.edu.tw

Yu-Hung Huang
Electronic Engineering
I-Shou University
Kaohsiung, Taiwan
yjhuang@isu.edu.tw

Abstract—**The Internet of Things (IoT) refers to uniquely identifiable objects (things) which can interact with other objects through the global infrastructure of wireless/wired Internet. The communication technique among a large number of resource-constrained devices that generate large volumes of data has an impact on the security and privacy of the involved objects. In this paper, we propose an encryption method based on XOR manipulation, instead of complex encryption such as using the hash function, for anti-counterfeiting and privacy protection. The enhancement of the security is described and hardware design methodology is also demonstrated.**

Keywords-Internet of Things (IoT); Encryption; Security Protocol

I. INTRODUCTION

The term of IoT was first introduced used by Kevin Ashton who was laying the groundwork for what would become the Internet of Things (IoT) at MIT's AutoID lab in 1999 [1]. Advances in wireless networking technology and the greater standardization of communications protocols make internet of things become rapidly emerging and widespread [2, 3]. If all objects in daily life were equipped with identifiers and wireless connectivity, these objects could be communicated with each other and be managed by computers. In addition to the tremendous number of devices and objects that are going to be connected through communications networks. One of the looming problems for the IoT is the new degree of security required to keep all these devices secured. With the commercialization of the Internet, security concerns expanded to cover personal privacy, financial transactions, and the threat of cyber theft. In IoT, security is inseparable from safety. Security and privacy are key challenges to make the IoT a reality.

The IoT can be implemented based on serviced-oriented architecture which targets the association of unique identifiers with specific services [4]. In such architecture, the appropriate response is activated upon authenticating the unique identifier from a specific ID node in which the information was collected. Unique identification technologies (dominated by RFID) and low power sensors are the main enablers of IoT realization through the uniqueness of ID, small size, sensing, storage and processing capabilities. Due to the inherent vulnerabilities of the internet, security and privacy issues should be considered and addressed before the IoT is widely deployed. IoT-devices may communicate with each other without any human interaction or even (real time) human control. For the integrity and safety of the overall system it is essential that only authorized devices take part in this process. The Electronic Product Code (EPC) is one of the well known object identification schemes which could uniquely identify objects associated with an RFID tag. The Internet of Things (IoT) will present new security challenges in cryptographic security. In this paper, we focus on simple and efficient secure key establishment to be used in the associated IoT network.

II. LIGHTWEIGHT ENCRYPTION METHOD

A communication scenario used to creating the IOT using Radio Frequency Identification (RFID) tags via the Internet is shown on Figure 1.

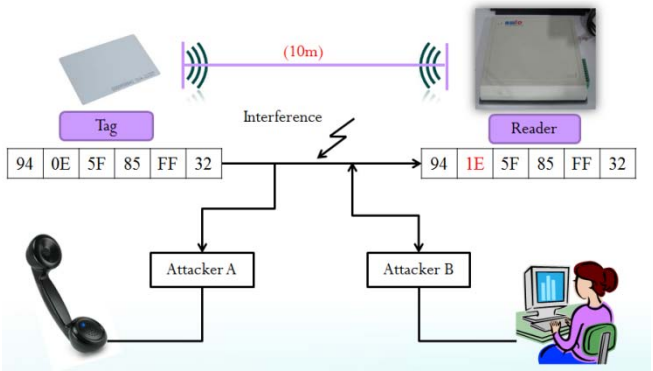

Figure 1. A communication scenario used to creating the IOT using RFID tag

The RFID readers are connected to the Internet. The tagged items are mobile and are expected to move through different reader fields and "connect" to the readers via their standard RFID communication protocol. The RFID reader identifies the tag using an appropriate authentication protocol. The lack of cryptography in basic RFID is a big impediment to security design. EPC tags of the Class-1 Gen-2 type have no explicit anti-counterfeiting features whatsoever. In principle, an attacker can simply skim the EPC from a target tag and program it into another, counterfeit tag or simulate the target tag on another type of wireless device[5].

A lightweight cryptography protocol base on XOR operations are listed as follows.

This research work was supported by National Science Council, R.O.C., under Grant NSC101-2221-E-214-077.

978-1-4799-4780-5/14/$31.00 ©

$$Apwd = Apwd_M \,||\, Apwd_L = a_0\, a_1\, a_2 \ldots a_{30}\, a_{31} \quad (1)$$

$$R_{Tx} = h_{t1}\, h_{t2}\, h_{t3}\, h_{t4}\,(\text{base16}) = d_{t1}\, d_{t2}\, d_{t3}\, d_{t4}\,(\text{base10}) \quad (2)$$

$$R_{Mx} = h_{m1}\, h_{m2}\, h_{m3}\, h_{m4}\,(\text{base16}) = d_{m1}\, d_{m2}\, d_{m3}\, d_{m4}\,(\text{base10}) \quad (3)$$

$$\begin{aligned} PAD &= Apwd - PadGen(R_{Tx}, R_{Mx}) = PAD_1 \,||\, PAD_2 \\ &= a_{dt1}\, a_{dt2}\, a_{dt3}\, a_{dt4} \,||\, a_{(dt1+16)}\, a_{(dt2+16)}\, a_{(dt3+16)}\, a_{(dt4+16)} \\ &\quad ||\, a_{dm1}\, a_{dm2}\, a_{dm3}\, a_{dm4} \,||\, a_{(dm1+16)}\, a_{(dm2+16)}\, a_{(dm3+16)}\, a_{(dm4+16)} \\ &= d_{v1}\, d_{v2}\, d_{v3}\, d_{v4}\,(\text{base10}) \end{aligned} \quad (4)$$

$$CCpwd_M = Apwd_M \oplus PAD_1,\ CCpwd_L = Apwd_L \oplus PAD_2 \quad (5)$$

Finally, the generation of the cover-coded passwords or the access password can then be used for mutual authentication.

III. Hardware Implementation

A finite state machine is built to perform the operation procedure listed on Eqs (1) ~ (5). The state transition diagram is depicted in Fig. 2. The QuartusII Synthesis tool is used to generate a synthesized net-list of the proposed lightweight cryptography protocol. The logic diagram of the synthesized cryptography protocol is shown in Fig. 3. The simulation results of the lightweight cryptography protocol are shown in Fig. 4.

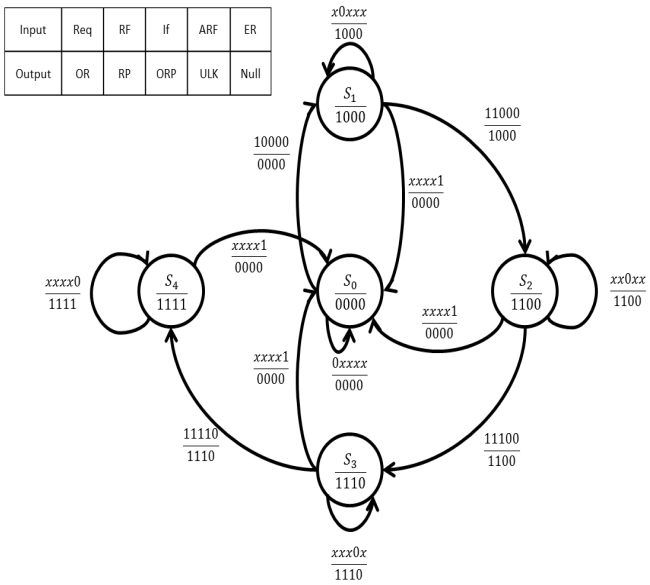

Figure 2. State transition diagram for lightweight cryptography protocol

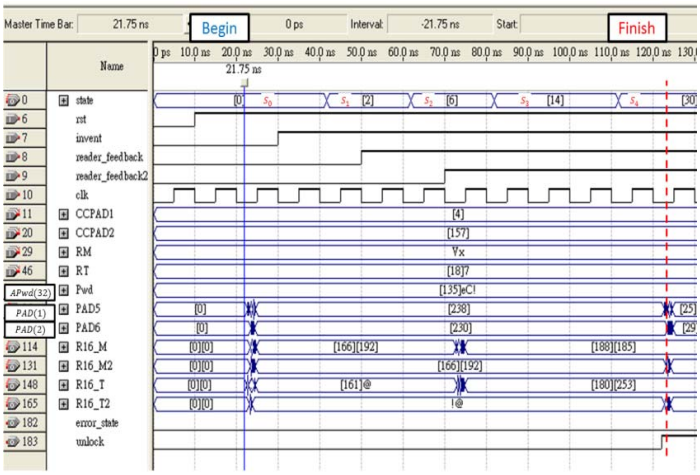

Figure4. Simulation results of the proposed lightweight cryptography protocol

IV. Conclusion

Based on IoT, the existing RFID system security mechanisms can be enhanced with a focus on cryptographic protocols. The weaknesses or flaws in the original RFID protocols can be improved using the present lightweight cryptography protocol. The hardware implementation of the lightweight cryptography protocol is demonstrated in this paper. In addition, the proposed protocol can be used to establish the mutual authentication procedure in a typical RFID system for IOT applications.

References

[1] Ashton K. That 'Internet of things' thing. RFID Journal, 2011, http://www.rfidjournal.com

[2] M.A. Feki, F. Kawsar, M. Boussard, and L. Trappeniers, The internet of things: The next technological revolution, Computer, vol. 46, no. 2, pp. 24-25, 2013.

[3] OpenIoT Consortium, "Open source solution for the internet of thingsinto the cloud," January 2012, http://www.openiot.eu [Accessed on: 2012-04-08].

[4] Internet of Things(IOT): http://en.wikibooks.org

[5] A. Juels. RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communication, 24(2), February 2006, pp 381 - 394.

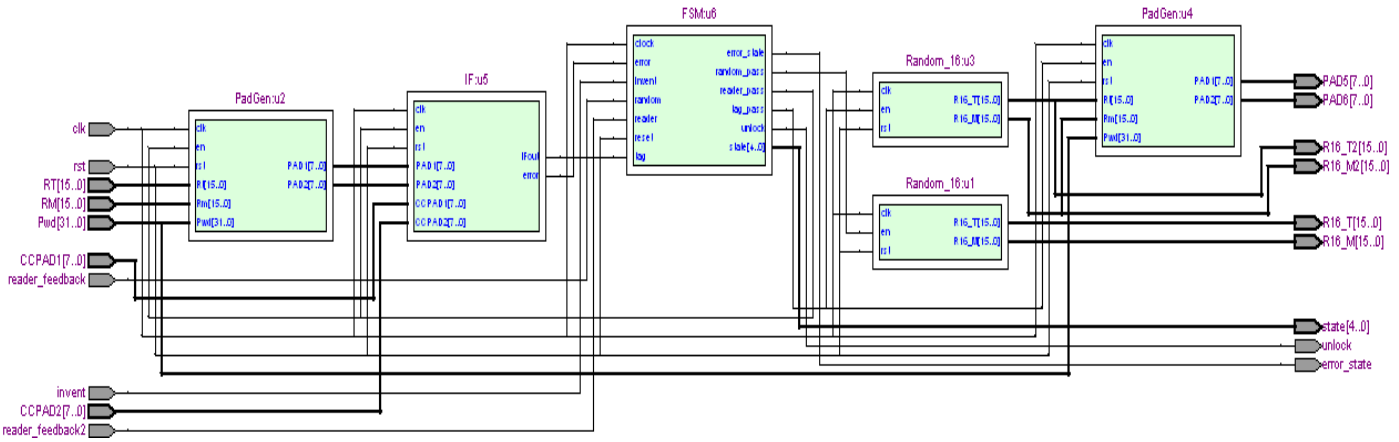

Figure3. Logic diagram of the synthesized cryptography protocol