International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 10 (November 2014) www.ijirae.com

A Survey of Technologies to Enable Security in Near-Field Communication Tag Design

C.Sathya M.Usharani
PG Scholar/ECE&Velammal Engineering College *Assistant Professor/ECE&Velammal Engineering College*

Abstract— Near-Field Communication (NFC) is a short range wireless communication technology, which operates in the principle of magnetic induction. A small electric current is created by a reader that in turn creates a magnetic field in the physical between the devices. A tag gets energized from the field. NFC tags are capable of store data in it and are either read-only or rewriteable. Because of its secure nature used to store personal data such as debit card and credit card information, PINs and networking contacts. The communication range in NFC is limited to within 10 centimeters; this gives a large degree of inherent security. Even though to prevent the lost or stolen devices from unauthorized NFC transactions, authentication should be performed before each transaction. To enable this feature the tag design support different technologies. This paper discusses various technologies to support secure transactions in NFC tags. And also introduces some methods that overcome enhanced implementation attacks such as side-channel attacks and fault analysis.

Keywords— near-field communications (NFC), radio frequency identification (RFID), advanced encryption standard (AES), elliptic curve cryptography, magnetic induction.

I. INTRODUCTION

Radio-Frequency Identification (RFID) is a wireless communication technique first patented in 1983 and is also governed by the standard ISO/IEC 18000-3. In RFID system, a reader and a tag communicate remotely in the RF field. Most of the tags used are passive tags i.e., they receive power supply from the RF field between the devices. A passive tag is a simple microchip that is attached to an antenna. The antenna is responsible for extracting power supply from the field for tag. But the active tags have their own power supply. Tags used in future RFID applications will have to provide additional functionality, such as security and data-storage features. The design of the tags must become more flexible to allow easier adaptation for new applications. But achieving these goals for passive tags is a highly challenging task [1].

Similar to RFID, NFC works in the 13.56MHz radiofrequency spectrum with less than 15mA power to communicate between the devices based on the principle of magnetic induction. A pair of ISO and ECMA standards defines NFC interfaces. Communication modes for NFC Interface and Protocol (NFCIP), setting active and passive communication modes, modulation scheme coding, collision control parameters and frame format are defined in ISO/IEC 18092 / ECMA-340. Communication modes used to minimize interference with card (tag) and contactless devices are specified by ISO/IEC 21481 / ECMA-352. RFID tag, which does not have anti-collision mechanisms cannot act as NFC tag, but the NFC tag can act as RFID tag.

Usage of NFC devices is growing continuously. Even though there are three main categories. They are,

1. Card Emulation mode
2. Peer to Peer mode
3. Reader/Writer mode

Card Emulation mode: In this mode NFC enabled mobile phone acts as a passive target. Some confidential data such as credit card or debit card information, ATM PINs are stored in the secure part of the NFC featured devices, which is read by the external reader and sand this information when it is desired for further processing.

Peer to Peer mode: This mode of communication takes place when two NFC featured devices needs to exchange data with each other. For example exchange business card.

Read or Write mode: NFC tags are designed to either read only or rewritable. This mode allows the NFC device to read or write data to NFC tag.

The NFC tags are numbered 1-4 based on operational specification defined by the NFC forum; technical information required to implement the reader/writer and associated control functionality of the NFC device. The four tag type specifications are,

Type 1 tag: It is based on ISO 14443A standard. These tags are capable of read and re-write. Memory availability is 96 bytes and can be expanded up to 2 kilobytes. Data are communicated at a speed of 106 Kbit/s.

Type 2 tag: It is also based on ISO14443A standard. Its specifications are as same as Type 1 tag except the memory availability which is 48 bytes and can be expandable to 2 kilobytes.

Type 3 tag: This type of tag is known as FeliCa and is based on the Japanese Industrial Standard (JIS) X6319-4. It has a variable memory availability feature. Memory limit is 1 megabyte per service and communication speed is 212kbit/s or 424kbit/s.

Type 4 tag: This type of tag is fully compatible with ISO14443A and ISO14443B standards. It has the maximum memory availability out of all type of tags, i.e., up to 32kilobytes per service and the communication speed are as same as the FeliCa tag.

The remainder of this paper is organized as follows. Section II explains the existing technologies used to provide security in NFC tags. Section III covers the proposed work of my project. Conclusions and future work are drawn in Section VI.

II. EXISTING TECHNOLOGIES

This section gives the survey of technologies used to design secure NFC tags.

A. AES Cryptography

Conventional AES cryptography engine has high complexity in order to maintain high throughput, but in NFC the throughput requirement is much lower. Overall response time required by the NFC specification is also much lower than other applications. So that [5] uses much slower AES engine. The design uses 8-bit AES encryption and decryption standard. It has 6 modules including an 8-bit Sbox, an addaakey unit, a subbytes unit, a keysch unit, a mixcol unit and a controller. But the design suffers from a known plain text attack.

B. Combining Asymmetric Cryptographic Standards

Known plain text attack can be avoided by using Advanced Encryption Standard and Elliptic Curve Cryptography together. Digital signing of messages and data encryption are processed within the Crypto unit and accessed by the microcontroller unit via micro-code patterns [1]. Tag authentication can be done either symmetrically by using AES or asymmetrically by using ECC. Reader authentication was done only in a symmetric manner.

III. PROPOSED WORK

We here introduce NFC technology in banking application for the purpose of using TAN id in ATM services. We can generate TAN id using NFC tags in ATM transactions and also in shopping purpose too. The TRF7970A is a Transceiver IC having integrated analog front end and data-framing device for a 13.56-MHz RFID and Near-Field Communication system. NFC feature TRF7970A Transceiver IC and low-power microcontroller MSP430G2553 acts as a reader for NFC tag. Built-in programming options make the device suitable for a wide range of applications for proximity and vicinity identification systems. NFC technology replaces RFID tags which provide more security and comfort comparing to RFID tags. Here NFC provides TAN ID which acts as one time password for the tag which provides more security by overcoming the enhanced implementation attacks, such as side-channel attacks and fault attacks. This overcomes the software encryption method to hardware encryption type which is placed along with the NFC reader.

A. Block Diagram

Block diagram for the proposed TAN id generation unit is shown in Fig.1. The TAN id will replace PIN no in ATM applications. It is generated by a list of random numbers stored in the NFC reader. To enable secure transaction, NFC reader checks for the availability of current TAN id. If it matches the device allows transaction, otherwise it blocks the tag. Finally reader replaces the NFC tag's TAN id with a random number stored in it. Advanced Encryption Standard and masking techniques are used to enable secure transmission of TAN id between reader and NFC tag. The crypto unit is placed in the reader such that it avoids Man-in-Middle attack and enhanced implementation attacks.

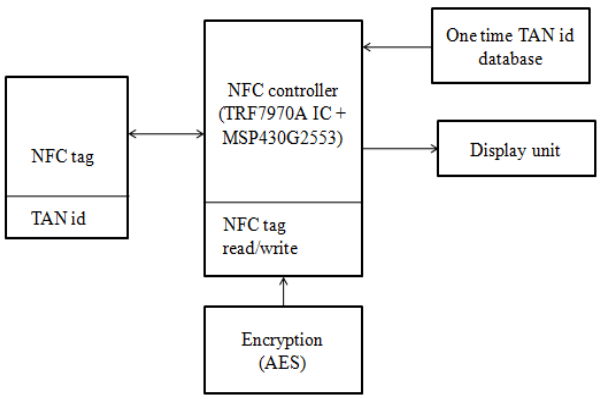

Fig.1. A simplified block diagram for TAN id generation unit with AES algorithm and masking technique implemented in the reader.

B. Flow Chart

The sequence of actions to generate TAN id that acts as a PIN for current transaction is shown in Fig.2. At first we have to initialize the system by pressing the power up button. The LED glows when the device is ready to use. TRF7970A Transceiver IC and MSP4302553 acts as a reader device. The reader device search for tags that is indicated by the blinking of LED. LED glows when it finds the tag in the physical space between reader and tag. It read the number in the current position of its storage and checks for the availability of that number in its memory. If it get matches displays the number and delete it from the list.

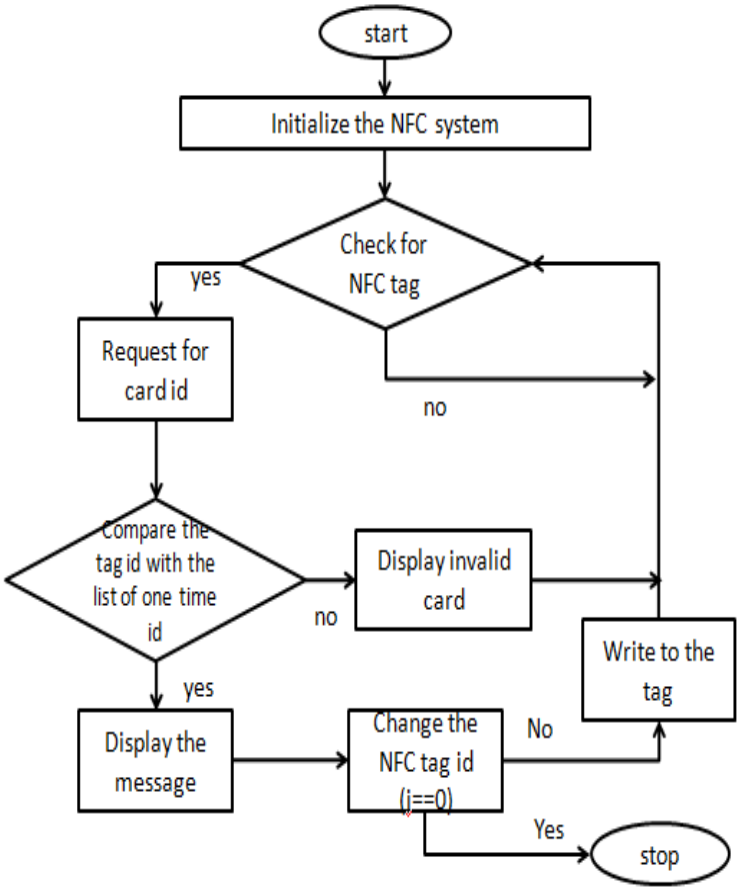

Fig.2. Flow chart for TAN id generation

IV. CONCLUSION AND FUTURE WORK

In this project we introduce a new communication method named NFC in banking applications. We used TRF7970A NFC booster pack along with MSP430G2553 launch pad to perform this NFC communication in the banking application. For secured communication AES cryptography method is used to encrypt and decrypt the values transmitted between the tag and TRF7970A. And additionally a concept of one time keying is introduced in NFC tag for the application of banking. This provides maximum security to all vulnerable attacks in the communication path. We designed the Tag id based security method in NFC application to ensure maximum security and reliability. It overcomes all the attacks represented in the existing system. In future we plan to provide TAN ID to the Multi bank ATM system for authentication purpose.

ACKNOWLEDGMENT

I thank the lord Almighty for showering blessings on me, which enabled to carry out this project successfully.

REFERENCES

[1] Thomas Plos, Michael Hutter, Martin Feldhofer, Maksimiljan Stiglic, and Francesco Cavaliere “Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography”, IEEE Trans. on VLSI Systems, vol.,21,no.11, Nov.2013

[2] ,J.W. Lee, D. H. T. Vo, S.H. Hong, and Q.-H. Huynh, “A fully integrated high security NFC target IC using 0.18 µm CMOS process”, in Proc. ESSCIRC, Sep. 2011, pp. 551–554

[3] T.Plos and M. Feldhofer "Hardware Implementation of a Flexible Tag Platform for Passive RFID Devices", in Proc. 14th Euromicro Conf. Digital System Design, Aug. 2011, pp. 293–300.
[4] A.Ricci, M. Grisanti, I. De Munari, and P. Ciampolini, "Design of a 2 µW RFID baseband processor featuring an AES cryptography primitive", in Proc. Int. Conf. Electron., Circuits Syst., Sep. 2008, pp. 376–379.
[5] A.S. Man, E. S. Zhang, V. K. Lau, C. Tsui, and H. C. Luong, "Low power VLSI design for a RFID passive tag baseband system enhanced with an AES cryptography engine," in Proc. Eurasia, Sep. 2007, pp. 1–6.
[6] Majid Baghaei-Nejad, Zhuo Zou, Hannu Tenhunen, Li-Rong Zheng, "A Novel Passive Tag with Asymmetric Wireless Link for RFID and WSN Applications", IEEE Transactions, 2007
[7] H.Yan, H. jianyun, L. Qiang, and M. Hao, "Design of low-power baseband-processor for RFID tag", in International Symposium on Applications and the Internet Workshops, (SAINT 2006), Phoenix, Arizona, USA ,23-27 January, 2006. Proceedings. IEEE Computer Society, January 2006, pp. 4–7.
[8] N.Yoshikawa, F. Matsuzaki, N. Nakajima, K. Fujiwara, K. Yoda, and K. Kawasaki, "Design and Component Test of a Tiny Processor Based on the SFQ Technology", IEEE Trans. on Applied Superconductivity, vol. 13, no. 2, June 2003
[9] André Abrial, Jacky Bouvier, Marc Renaudin , Patrice Senn,, and Pascal Vivet, "A New Contactless Smart Card IC Using an On-Chip Antenna and an Asynchronous Microcontroller", IEEE Journal of solid-state circuits, vol. 36, no. 7, July 2001
[10] Christian Piguet, Jean-Marc Masgonty, Claude Arm, Serge Durand, Thierry Schneider, "Low-Power Design of 8-b Embedded Cool Risc Microcontroller Cores", IEEE Journal of Solid-State Circuits, vol. 32, no. 7, July 1997

