Indian Journal of Science and Technology, Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102543, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Study on the Cryptographic Algorithm for NFC

Heon-june Kim*

Department of Motion Art Design, Namseoul University, 91 Daehak-ro Seonghwan-eup Sebuk-gu Cheonan-si Chungcheongnam-do, 31020, South Korea; heonjunekim@gmail.com

Abstract

Objectives: Currently, NFC leads the mobile payment market. In such a situation, leakage and change of payment information and leakage of personal information by cracking can cause serious social problem. Accordingly, the coding technique used for security of NFC should be safer than now. **Methods/Statistical Analysis:**Though AES currently used in security of NSF is a safe coding technique, it is not equipped with certifying function. Thus, this paper, by combining AES with Modification Detection Code and Message Authentication Code, suggests an encryption algorithm with authentication function. **Findings:**To strengthen authentication function and integrity function, the new symmetric encryption algorithm was designed not to predictable relation and input-output relations of hash function. By simultaneously using Message Authentication Code and Modification Detection Code where blocked hand-shake method is applied, it is encryption algorithm suitable to the NFC environment.The encryption algorithm suggested in the paper generates hash values corresponding to Modification Detection Code and Message Authentication Code, along with the RD-I and RD-II part and the encryption part. Such hash values perform authentication functions using only output of the suggested algorithm without securing a separate authentication channel. **Improvements/Applications:**The suggested encryption algorithm combines existing Message Authentication Code and Modification Detection Code to use them for authentication. Consequently, it will guarantee authentication and encryption functions by securing a safer NFC communication channel.

Keywords: AES, Cryptographic, NFC, Security

1. Introduction

Recently, with distribution of various smart devices, users can enjoy various services. In particular, NFC chip mounted on Smartphone allows users to use various types of NFC service such as personal information service and financial information service. NFC technology is non-touch near-distance wireless communication technology. The user can use it intuitively and simply, and service providers can easily apply it on existing service, and provide service of more diverse and advanced technology. Smartphone makers and service providers pay attention to NFC service to provide various kinds of information with smart card, and financial service.When NFC technology was first introduced, it could not be widely applied and distributed because of lack of understanding about the construction of NFC infrastructure among communications companies, manufacturers, and VAN companies. But, afterwards, with the installment of NFC functions on smartphone by its makers, researches on NFC technology and distribution of it have been active. With the installment of NFC functions on smartphone, applications have been developed in various service areas, and the government and corporations have made active efforts to expand the area where they can be used[1]. Some foreign countries have been active in doing researches on NFC and applying it on various businesses. For example, the Japanese government, together with private partners like SONY and NTT Docomo and others popularized mobile payment market using Felica, non-touch card technology. Google, platform developer, is providing various services using NFC technology. Increasing number of companies are adopting it[1].

*Author for correspondence

2. Security Problem of NFC

Payment service using mobile NFC is made online/offline by using applications for payment and storing personal information and payment information. In such an environment, the threat in communications is caused from using RF communications between terminals when mobile NFC payment service is used offline.Typical risks which can arise in RF communication area are tapping the communication and alteration of it. Besides, there are other risks are DoS (Denial of Sevice) attack and Man-In-The-Middle (MITM) attack using frequency disturbance between mobile communication users. In addition, when communications are done using wireless Internet, there can be attack using private wireless AP (Access Point). And, as risk to mobile terminals using NFC service, there are information leakage and alteration using malicious code, phishing attack, and application and platform alteration, etc. If terminal is lost, private information and payment information can be exposed. Figure 1 classifies risks in NFC communications and in terminal.To deal with such security risks, NFC service providers and terminal makers should provide separate security services, SE (Secure Element) and TSM (Trust Service Manager). SE is the storage medium where personal information, credit card information, coupons used for mobile payment service can be stored. TSM is to provide trusted safe service between user and the company, and plays the role of mediator which manages SE information, installment, deletion, and updating of applications, and solve problems. As described, with the distribution of smartphone, the areas where NFC are applied are expanding rapidly. Table 1is comparative specifications of near distance wireless communications network. As shown in the Table 1, NFC applies encryption to be equipped with capability to perform important electronic payment.But, as the applied encryption method is AES-128, we should be cautious of rapid development of wireless communications network, and security leakage by various hacking and cracking.In addition, as AES is an open encryption, it cannot be considered as very safe[2]. As AES is symmetric algorithm, it can be suitable to NFC. So, it is currently used. But, with the increasing use of AES, unwanted access can increase. Thus, it is necessary to add asymmetric characteristics to NFC.Therefore, this paper, by adding authentication function used in asymmetric type to symmetric type, and applying it on NFC, wants to examine Authentication-NFC encryption algorithm, and form a safer NFC security channel.

Figure 1. The risks of cracking.

Table 1. Comparison of short-range wireless technology

Technology	Frequency	Security	Standard Scope	Main Service
NFC	13.56MHz	Safe	Global	electronic payment
Bluetooth	2.4GHz	Unsafe	Global	File transfer
Zigbee	2.4GHz	Unsafe	Global	Device control
RFID	900MHz	Unsafe	Domestic	RFID

3. Proposed Algorithm for MFC

To strengthen authentication function and integrity function, the new symmetric encryption algorithm was designed not to predictable relation and input-output relations of hash function. By simultaneously using Message Authentication Code and Modification Detection Code where blocked hand-shake method is applied, it is encryption algorithm suitable to the NFC environment[3,4]. As shown in Figure 2, authorization function of the suggested encryption algorithm produces authentication information using secret key and normal message or encrypted message.Message x_1 is normal words if x is encrypted words, and encrypted words if x is normal words. It has the structure sharing the Message Authentication Code part which provides integrity and manages key, and the Modification Detection Code part which generates and possesses hash values.Modification Detection Code is calculated as follows. What is input is message x with $k >>$

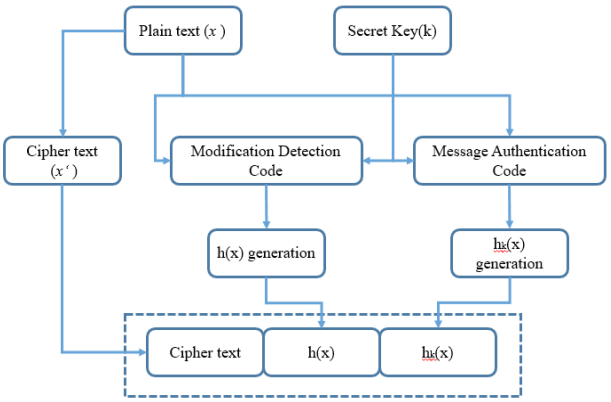

Figure 2. Proposed hybrid authentication structure.

4, and bit length $l = 64k$, and what is output is hash value for 256 bits against x. x is arranged as $x = x_1, x_2, x_3, \ldots, x_t$, as multiplication of 64 bits.Initial values of 64 bits, $I, \bar{I}$ are selected as follows[5,6]. I = 0x5252525252525252, $\bar{I}$ = 0x2525252525252525. If C_i^L and C_i^R are 32 bit values ofC_i in the left and right sides, we can $h(x) = H_t \| \widetilde{H_t}$ get as output by doing calculation following Equation (1) in the structure of Figure 3.

$$\begin{aligned} H_0 &= I & \widetilde{H_0} &= \bar{I} \\ k_i &= g(H_{i-1}) & \widetilde{K_i} &= \tilde{g}(\widetilde{H_{i-1}}) \\ C_i &= E_k(x_i) \oplus x_i & \widetilde{C_i} &= E_{\tilde{k}}(x_i) \oplus x_i \\ H_i &= C_i^R \| C_i^L & \widetilde{H_i} &= \widetilde{C_i^R} \| \widetilde{C_i^L} \end{aligned} \quad (1)$$

Message Authentication Code is calculated as follows. The input value x is data with bit length $32j$. And the secret key for Message Authentication Code 64 bits is $Z = Z[1], Z[2], \cdots Z[8]$[7,8]. The output value is 32 bit Message Authentication Code for x. Expand the keyunrelated with message. That is, expand key Z as X, Y, V, W, S, T composed of six 32 bits. Here, X and Y are initial values, V and W are cyclic values, and S and T are padding values added to the message. Perform initialization and padding. Treat the blocs. Treat 32 bit message bloc x_i as follows.

$$v \leftarrow (v \lll 1), \quad \mathbf{U} \leftarrow \left(v \bigoplus \square \mathbf{W} \right)$$

$$t_1 \leftarrow \left(H_1 \bigoplus x_i \right) \times \left((H_2 \oplus x_i) + U \; OR \; A \right) AND \; C$$

$$t_2 \leftarrow \left(H_2 \bigoplus x_i \right) \times \left((H_1 \oplus x_i) + U \; OR \; B \right) AND \; D$$

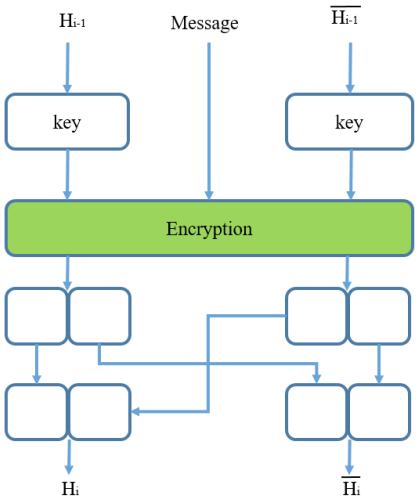

Figure 3. The modification detection code structure.

$$H_1 \leftarrow t_1, H_2 \leftarrow t_2$$

where, x_i means multiplication a $mod\ 2^{32} - i$ t, $\bigoplus \square$ means addition at $mod\ 2^{32}$, $\lll$ means one bit rotation to the left. Finally, the resulting value of Message Authentication Code is $= H_{1 \oplus H_2}$ [9,10]. As described, we can acquire Modification Detection Code and Message Authentication Code, calculate values on the two functions, and add them to a single frame like Equation (2).

$$C = E_k(x \| h(x)) \& E_k(x \| h_k(x)) \quad (2)$$

Equation (2) is encrypted message C value, a single data by adding Message Authentication Code value using Modification Detection Code value acquired by encrypting message x and $h_k(x)$. Here, values generated by Modification Detection Code and Message Authentication Code should maintain mutual independence, even if the same Iand the same message x are used as shown in Equation(3).

$$E_k(x \| h_k(x)) \neq (E_k(x), E_k(h(x))) \quad (3)$$

If one ignores the conditions of Equation (3), or Modification Detection Code and Message Authentication Code have the dependent relationship, decryption cannot be performed even if padding is performed, because the criteria to distinguish Modification Detection Code and Message Authentication Code values inside the data. As explained up to now, the purposed encryption algorithm structure is clearly different from the existing symmetric type-based bloc encryption algorithm. The overall bloc map of the purposed encryption algorithm is shown in

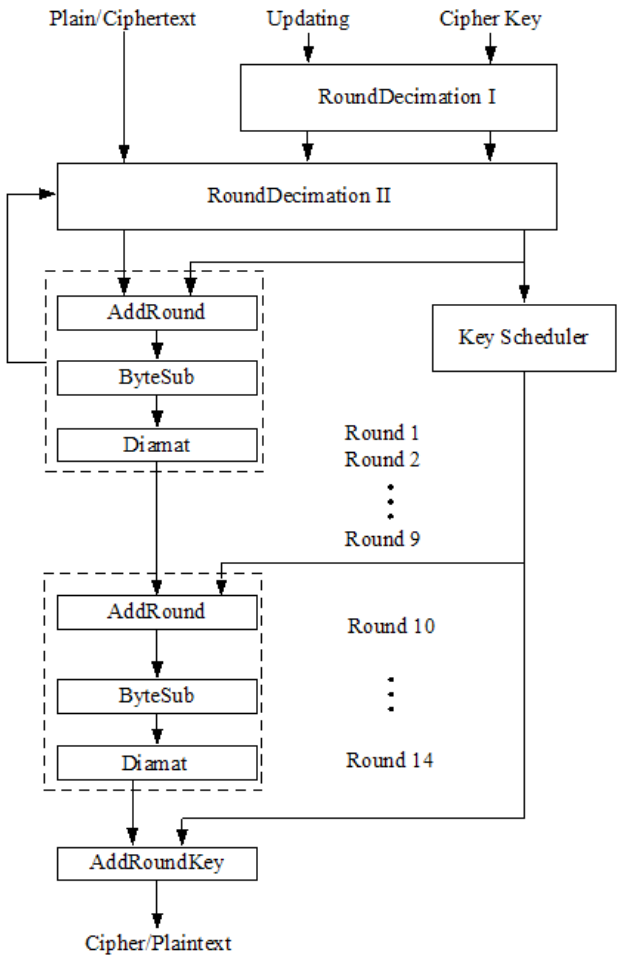

Figure 4. Proposed algorithm.

Figure 4.Previous processing generates round information which will perform algorithm, and the encryption calculation part performs basic rounding with round information up to 9 rounds, and various round calculations with the numbers of round from round 10 to 14.In addition, the encryption algorithm suggested in the paper generates hash values corresponding to Modification Detection Code and Message Authentication Code, along with the RD-I and RD-II part and the encryption part. Such hash values perform authentication functions using only output of the suggested algorithm without securing a separate authentication channel.

4. Conclusions

As the AES encryption algorithm used in the NFC environment does not have authentication functions, it needs to acquire authentication functions with a method to combine Message Authentication Code or Modification Detection Code with hash function, to be used in wireless network like NFC. Thus, it has the problem of its bandwidth being increased as encryption data and authentication data need to be sent separately on wireless channel. And, with the increase of transmitted data, transmission efficiency decreases. But, the bigger problem of it is lower safety of it because authentication data is not encrypted. Separation of encryption and authentication leads to overuse of bandwidth and exposure to the risk of cracking, causing the situation where safety cannot be secured.Thus, this research suggested an encryption algorithm combining Message Authentication Code and Modification Detection Code in the NFC environment to include authentication functions to encrypted data in limited bandwidth. The suggested encryption algorithm is the algorithm combining existing Message Authentication Code and Modification Detection Code to use them for authentication. Consequently, it will guarantee authentication and encryption functions by securing a safer NFC communication channel. Therefore, in the future NFC network environment, the suggested encryption algorithm based on symmetric type encryption algorithm will be used more efficiently than asymmetric type encryption algorithm inefficient in the perspectives of safety and network management.

5. Acknowledgement

Funding for this paper was provided by Namseoul University.

6. References

1. Near-field communication (NFC)[Internet]. [cited 2016 Sep 20]. Available from:https://en.wikipedia.org/wiki/Near_field_communication.
2. Advanced Encryption Standard (AES) [Internet]. [cited 2016 Sep 15]. Available from:https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
3. Serpent cryptography on static and dynamic reconfigurable hardware[Internet]. [cited 2006 Mar 08]. Available from: http://ieeexplore.ieee.org/document/1618428/.
4. Security in Near Field Communication(NFC) [Internet]. [cited 2006 Jan]. Available from: https://www.researchgate.net/publication/237424298_Security_in_Near_Field_Communication_NFC.
5. Roland M, Langer J, Scharinger J. Security vulnerabilities of the NDEF signature record type.2011 3rd International

Workshop on Near Field Communication; 2011 Feb. p. 65–70.
6. Damgard IB, Denmark AC. Collision free hash functions and public key signature schemes.EUROCRYPT'87 Proceedings of the 6th annual international conference on Theory and application of cryptographic techniques; 1987. p. 203–16.
7. Analysis and design of cryptographic hash functions[Internet]. [cited 2003 Feb]. Available from: https://securewww.esat.kuleuven.be/cosic/publications/thesis-2.pdf.
8. Kar J, Majhi B. An efficient password security of three-party key exchange protocol based on ECDLP. International Journal of Security and Security. 2009 Nov; 3(5):405–13.
9. Anderson R. The classification of hash functions. Proceedings of the 4th Institute of Management Accountants Conference on Cryptography and Coding; 1995. p. 83–94.
10. Dobbertin H. Cryptanalysis of MD-4. Journal of Cryptology. 1998 Sep; 11(4):253–71.