An Improved Privacy Protection Security Protocol Based on NFC

Jie Ling[1], Ying Wang[1], Weifeng Chen[2]
(Corresponding author: Ying Wang)

Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China[1]
Computer Science & Information Systems, California University of Pennsylvania California, PA 15419, USA[2]
(Email: 526047587@qq.com)

(Received Sep. 15, 2015; revised and accepted Dec. 7 & Dec. 30, 2015)

Abstract

An improved NFC-based privacy protection protocol is proposed to protect user's privacy in NFC application. In this paper, user's privacy is protected by Chebyshev-map and certificateless public key cryptography in the protocol. As a trusted third party, Trusted Service Manager (TSM) participates in the process of user registration and verifies the identity of the parties if necessary. With high calculation speed, the proposed method can eliminate vulnerabilities of impersonations attacks and save the storage space of NFC devices.

Keywords: Identity authentication, NFC, privacy preserve, pseudonym

1 Introduction

NFC (Near Field Communication) is a short-range wireless communication technology that evolved from RFID which has been studied by scholars [15, 16, 18, 19], it's technology distance is around 4 inches, and it operates in the 13.56 MHz frequency band at a speed of 106 Kbps, 212 Kbps or 424 Kbps. NFC technology has been widely used in smart phones and other consumer electronics devices. The mobile phone with NFC-enabled can be used for mobile payment, e-ticketing, intelligent media browsing and data transmission and exchange, etc [5, 11]. It is vulnerable to eavesdropping, data tampering, data corruption, cloning and phishing attacks, resulting in the leak of user privacy data which is a serious threat to financial information and the user's property security.

How to strengthen and improve the security of NFC has become a hot issue of academic and industrial circles in recent years. A series of NFC security standards have been formulated. They expressly stipulated that key agreement is required for secret communications between users [9, 10]. In the key agreement, both users should exchange their certificates to get the public key of another party. Specifically, the certificate includes the user's personal information. Thus, the attacker can get the user's action and privacy by tracing the public key.

As an important privacy protection method, the pseudonym-based privacy protection methods have been widely used in many applications [6, 8, 12, 17]. In such applications, the user's identity is represented by a pseudonym, which is generated by the third trusted services manager randomly. It means that the user's identity has no relation to the user's real identity. Therefore, the attacker cannot get the user's real identity even if he could get the user's pseudonym. A lot of research have been done to strengthen the security of NFC. In [2], Chi et al. proposed the secure transaction protocol in NFC card emulation mode, but this protocol is no privacy protection. The Reference [20] proposed an NFC mobile trusted anonymous authentication enhanced privacy protection model which realized the anonymous authentication of users. However, this model requires an embedded mobile trusted computing module, which is difficult to implement in practical application. Eun et al. proposed an conditional privacy preserving security protocol for NFC-based applications [4].Eun et al. proposed an improved conditional privacy preserving security protocol for NFC-based applications [3]. However it updates pseudonym without the communication with the TSM which can be used only to keep track of the message constructor. So it has high computational efficiency. According to reveal that Eun et al.'s protocol could not withstand impersonation attack, the Reference [7] proposed an improved method, in which the TSM is responsible for generating pseudonym set and verifying the identity of users. The improved method can resist impersonation but results in additional space to store pseudonym set and low calculation efficiency.

This paper proposed an improved privacy protection security protocol based on NFC. Users need to register at the TSM and get the security information which will be involved in the process of key agreement to ensure the security and privacy of the protocol and mobile devices do not need more storage space. This protocol can withstand impersonation attack, improved the computing efficiency,

Table 1: Notation

Notation	Description
N_A	Nonce of A
ID_A	Random ID of user A
G	Elliptic curve base point
d_A	Private key of user A
Q_A	Public key of user$A$,Q_A=d_AG
Q_s	Public key of TSM
Z	shared secret value taking x-coordinate from P
r_A	Random integer generated by user A
SSK	Shared secret key
KDF	Key derivation function
$MacTag_A$	Key verification tag received from A
$Enc(k,m)$	Encrypt m with k
$Sig(k,m)$	Signature on m with k

and reduce the storage of NFC devices.

The rest of the paper is organized as follows. Section 2 describes background knowledge related to proposed protocol. In Section 3, Eun et al.'s and Debiao et al.'s security protocol are provided. In Section 4, the proposed secure protocol based NFC is introduced. Security and performance analysis results are given in Section 5. Section 6 draws conclusions.

2 Background Knowledge

2.1 Chebyshev-map

Chebyshev-map [13] $T_n(x) : [-1,1] \rightarrow [-1,1]$ is mapping defined by n-degree Chebyshev polynomials $T_n(x) = \cos(n \times \arccos(x)), x \in [-1,1]$. The definition of recursive: $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), n \geq 2, x \in [-\infty, +\infty]$ and $T_0(x)$=1,$T_1(x)$=x.

Chebyshev polynomials satisfy the semigroup properties:$T_r(T_s(x)) = T_{r\times s}(x)$, and also meet the commutative:$T_r(T_s(x)) = T_s(T_r(x))$.

2.2 Pseudonym Composition

Pseudonym represents ID that changes randomly. The pseudonym are composed of the user's public key Q_A^i, the user's private key d_A^i,the TSM's identity and the TSM's signatureS_{TSM}^i.Pseudonym composition [8].

$$\begin{aligned} S_{TSM}^i &= Sig(d_{TSM}, Q_A^i \parallel Enc(Q_A^i, d_A^i) \parallel ID_{TSM}) \\ PN_A^i &= \{Q_A^i \parallel Enc(Q_A^i, d_A^i) \parallel S_{TSM}^i\}. \end{aligned}$$

Pseudonym can guarantee user anonymity, protect personal privacy. Usually pseudonym-based privacy protection method uses pseudonym set generated by TSM. TSM need to stores pseudonyms and the actual ID of users to reveal the anonymity in case of a problem. However, the method using the pseudonym requires additional costs for storage and communication. In order to improve the insufficiency of the user need additional storage space to save pseudonym set in NFC devices, some researchers are studying the methods of generating pseudonym without the help of TSM.

2.3 Notations

The notations used in the paper as shown in Table 1.

3 Related Work

3.1 Eun et al.'s Privacy Preserving Protocol

In order to protect the user's privacy, Eun et al [3] proposed a self-updateable pseudonym based method which can update pseudonym without the need to communicate with TSM. TSM only reveals the true identity of users in needed, and the communication and computation efficiency is high. The protocol process shown in Figure 1 and as follows:

1) A generates a nonce N_A and a random number r_A, Then, A computes $Q_A^{'} = r_AQ_A$, $Q_A^{''} = r_Ad_AQ_s + Q_A^{'}$ and sends the message $m_1 = \{Q_A^{'} \parallel N_A \parallel Q_A^{''}\}$ to B.

2) Upon receiving the message m_1, B generates a nonce N_B and a random number r_B. B computes $Q_B^{'} = r_BQ_B$, $Q_B^{''} = r_Bd_BQ_s + Q_B$ and sends the message $m_2 = \{Q_B^{'} \parallel N_B \parallel Q_B^{''}\}$ to A.

3) Upon receiving the message m_2, A computes $P = r_Ad_AQ_B^{'}$, $SSK = KDF(N_A, N_B, ID_A, Z)$, $MacTag_A = f(SSK, ID_A, Q_A, Q_B)$ and sends message $m_3 = \{MacTag_A\}$.

4) Upon receiving the message m_3, B computes $P = r_Bd_BQ_A^{'}$, $SSK = KDF(N_A, N_B, ID_A, Z)$,

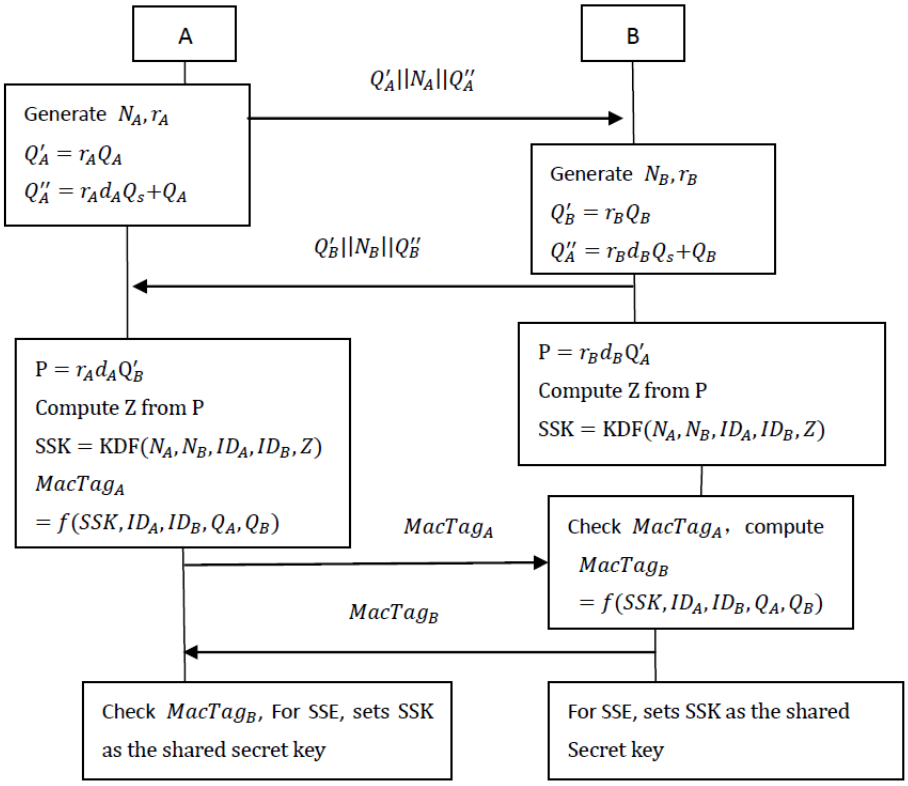

Figure 1: Eun et al.'s privacy protection protocol

If verify the message m_3 successfully, B sets SSK as the shared secret key and computes $MacTag_B = f(SSK, ID_A, Q_A, Q_B)$ sends message $m_4 = \{MacTag_B\}$ to A. Otherwise, B stops the session.

5) Upon receiving the message m_4 and verify it successfully, A sets SSK as the shared secret key, if validation fails, A stops the session.

3.2 Debiao et al.'s Privacy Protection Protocol

In paper [7] Debiao et al.pointed out that Eun et al. protocol has the impersonation attack vulnerabilities. An attacker can impersonate even without knowing the private key of user A, so $Q'_A = r_A G$, then $P_A = r_A Q'_B = r_A r_B Q_B = r_A r_B d_B G$, $P_B = r_B d_B Q'_A = r_B d_B r_A G$, $P_A = P_B$. Attacker and B could generate the same session key and $MacTag_A$ generated by attacker could pass B's verification. Besides, the TSM does not involve the above process. Then, the TSM cannot find the impersonation attack. Similarly, attacker can impersonate B. In order to overcome security weaknesses in Eun et al.'s protocol, Debiao et al. proposed the improvement privacy protocol, shown in Figure 2.

After receiving the user A's request for pseudonyms, the TSM generates n pseudonyms and sends them to A through a secure channel. The TSM also stores the user A's identity and pseudonyms into its database. Through the same method, the user A could get its pseudonyms and corresponding public/private keys.

User A and B require the pseudonymous set from the TSM and store them in the NFC device, randomly selected a pseudonym and the corresponding private key to start key agreement in the process of communication. The protocol can protect user's privacy and against impersonation attack, but NFC device requires additional costs for storage and computational efficiency decreased.

4 The Proposed Security Protocol

In view of the existing problems or shortcomings of above protocols, this paper proposes an improved privacy protection security protocol based on NFC, which uses Chebyshev-map and certificateless public key cryptography, TSM as a trusted third party to participate in the registration process and verify the true identity of the user when necessary. The protocol improves the computation efficiency, reduces the storage cost of NFC devices and can withstand impersonation attacks. This protocol includes the initialization phase and key agreement phase, and the process description is as follows.

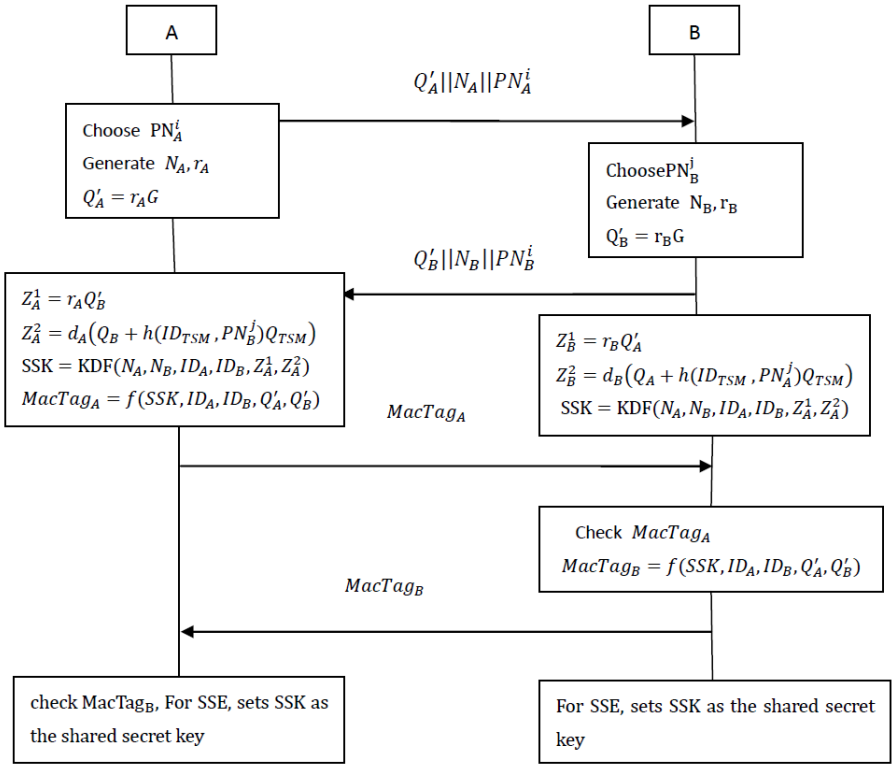

Figure 2: Debiao et al.'s privacy protection protocol

4.1 Initialization Phase

The premise of initialization phase is that the user A and B has been registered in the TSM. We assume that the user and the TSM mutual authentication has been conducted and the communication tunnel is secure. The process of register as follows:

1) A sends message $m_1 = \{q_A, ID_A\}$ to TSM ,q_A is the password generated by A and ID_A is A's identity.

2) Upon receiving the message m_1, TSM computes $R_A = T_{s_A}(x)$,s_A is the partial private key generated by certificateless public key cryptography [14].

In the key agreement and confirmation phase, when A sends a request to the TSM, TSM sends B's R_B to the A, the specific process is as follows:

1) A computes h$(ID_A \| ID_B \| s_A)$and sends $m_1 = \{h(ID_A \| ID_B \| s_A) \| ID_A \| ID_B\}$ to TSM.

2) Upon receiving the request message m_1, TSM computes $h'(ID_A \| ID_B \| s_A)$ and if $h'(ID_A \| ID_B \| s_A)$ equal m_1, TSM computes $Enc(Q_A, R_B)$ and sends $m_2 = \{Enc(Q_A, Q_B) \| ID_A \| ID_B \| ID_{TSM} \| S_{TSM}\}$ to A. S_{TSM} is TSM signature on the message, $S_{TSM} = Sig(Enc(Q_A, Q_B) \| ID_A \| ID_B \| ID_{TSM})$.

3) A receives the message m_2 and verify the TSM signature S_{TSM} and decrypt $Enc(Q_A, R_B)$ by own private key d_A to get R_B.

Similarly, B gets R_A through these steps.

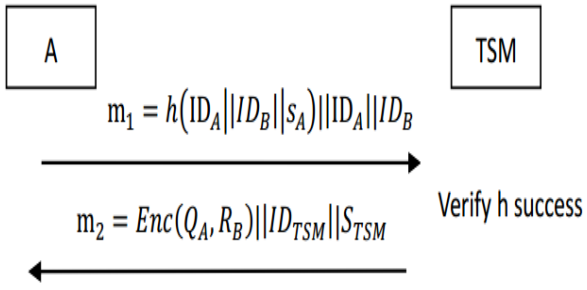

Figure 3: Initialization of the proposed protocol

4.2 Key Agreement and Confirmation Phase

Key agreement and confirmation process as shown in Figure 4, Specific steps are as follows:

1) A sends a request to TSM for getting R_B, generates a nonce N_A and a random number r_A, Then, A computes $Q'_A = r_A Q_A$, $Q''_A = r_A d_A Q_s + Q_A$ and sends the message $m_1 = \{Q'_A \| N_A \| Q''_A\}$ to B.

2) Upon receiving the message m_1, B sends a request to TSM for getting R_A, generates a nonce N_B and a

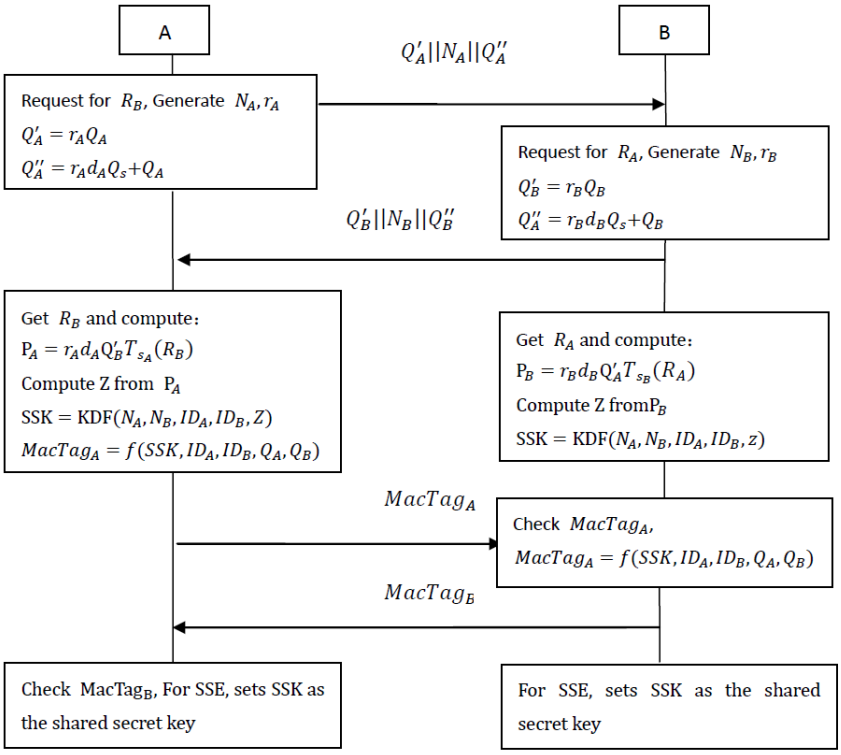

Figure 4: The proposed key agreement and confirm protocol

random number r_B. Then, B computes $Q'_B = r_B Q_B$, $Q''_B = r_B d_B Q_s + Q_B$ and sends the message $m_2 = \{Q'_B \parallel N_B \parallel Q''_B\}$ to A.

3) Upon receiving the message m_2, A computes $P_A = r_A d_A Q'_B T_{s_A}(R_B)$, computes Z from P and $SSK = KDF(N_A, N_B, ID_A, ID_B, Z)$, $MacTag_A = f(SSK, ID_A, ID_B, Q_A, Q_B)$ and sends message $m_3 = \{MacTag_A\}$ to B.

4) Upon receiving the message m_3, B computes $P_B = r_A d_A Q'_B T_{s_B}(R_A)$, computes Z from P and $SSK = KDF(N_A, N_B, ID_A, ID_B, Z)$, If verify the message m_3 successfully, B sets SSK as the session key, computes $MacTag_B = f(SSK, ID_A, ID_B, Q_A, Q_B)$ and sends the message $m_4 = \{MacTag_B\}$ to A. Otherwise, B stops the session.

5) A receives the message m_4 and the validation is successful, sets SSK as the session, if validation fails, A stops the session.

5 Protocol Analysis

5.1 Security Analysis

Security analysis shows that the proposed protocol can provide anonymity and mutual authentication, be against to impersonation attacks etc. The specific analysis is as follows:

Security 1: The proposed security protocol could provide user anonymity.

Due to the wireless communication in NFC applications, the adversary C could control the communication channel totally. Then, he could intercepts the message $m_1 = \{Q'_A \parallel N_A \parallel Q''_A\}$, $m_2 = \{Q'_B \parallel N_B \parallel Q''_B\}$, $m_3 = \{MacTag_A\}$ and $m_4 = \{MacTag_B\}$ transmitted between the user A and the user B. But the identities of A and B are included in Q''_A and Q''_B separately. Without the A and B private key d_A and d_B, the adversary cannot get the identity of A or B. Thus, the proposed security protocol could provide user anonymity.

Security 2: The proposed security protocol could provide session key security.

Suppose the adversary C could get a session key generated in a previous session. He has to compute $P_A = r_A d_A Q'_B T_{s_A}(R_B) = r_A d_A r_B d_B G T_{s_A}(T_{s_B}(x)) = r_B d_B (r_A d_A G) T_{s_B}(T_{S_A}(x)) = P_B$ from $Q'_A = r_A Q_A$ and $Q'_B = r_B Q_B$. if he wants to get the session key in the current session since A and B generate new random numbers r_A and r_B for each session. Then, the adversary has to solve the computational DiffieHellman problem. Due to the hardness of the computational Diffie-Hellman problem, the proposed security protocol could provide session key security.

Security 3: The proposed security protocol could withstand impersonation attacks.

Table 2: Performance comparison

	The initiator user	The target user	Total
Chi et al.'s protocol	$2T_m + T_a + 2T_{AES} + T_{kdf} \approx 2606T_{Mul}$	$2T_m + T_a + 2T_{AES} + T_{kdf} \approx 2606T_{Mul}$	$4T_m + 2T_a + 4T_{AES} + 2T_{kdf} \approx 5212T_{Mul}$
Eun et al.'s protocol.	$3T_m + T_a + 2T_h + 2T_{Mul} + T_{kdf} \approx 3608T_{Mul}$	$3T_m + T_a + 2T_h + 2T_{Mul} + T_{kdf} \approx 3608T_{Mul}$	$6T_m + 2T_a + 4T_h + 4T_{Mul} + 2T_{kdf} \approx 7216T_{Mul}$
Debiao et al.'s protocol	$4T_m + T_a + 3T_h + T_{kdf} \approx 4806T_{Mul}$	$4T_m + T_a + 3T_h + T_{kdf} \approx 4806T_{Mul}$	$8T_m + 2T_a + 6T_h + 2T_{kdf} \approx 9612T_{Mul}$
Proposed protocol	$3T_m + T_a + 2T_h + 2T_{Mul} + T_{kdf} + T_{sym} \approx 3613T_{Mul}$	$3T_m + T_a + 2T_h + 2T_{Mul} + T_{kdf} + T_{sym} \approx 3613T_{Mul}$	$6T_m + 2T_a + 4T_h + 4T_{Mul} + 2T_{kdf} + 2T_{sym} \approx 7226T_{Mul}$

Let A and B be initiator user and target user separately. Assuming an attacker C fake A generates the message $m_1 = \{Q_A^{'} \parallel N_A \parallel Q_A^{''}\}$, N_A is a random number generated by C. After receiving the message m_1, B generate a nonce N_B and a random number r_B, compute $Q_B^{'} = r_B Q_B$ and send the message $m_2 = \{Q_B^{'} \parallel N_B \parallel Q_B^{''}\}$ to C. However, C does not calculate $P_A = r_A d_A Q_B^{'} T_{s_A}(R_B)$, because C does not have the partial private key s_A of A and private key d_A, so C can't generate the message $m_3 = \{MacTag_A\}$. B is able to find an attack by examining the validity of $MacTag_A$. Also attacker C cannot fake B. Thus, the proposed protocol could against impersonation attack.

Security 4: The proposed security protocol could withstand modification attacks.

Suppose the adversary C intercepts the message $m_1 = \{Q_A^{'} \parallel N_A \parallel Q_A^{''}\}$ and send it to user B after modification. Due to the difficulty of the computational Diffie-Hellman problem, C cannot generate the valid message $MacTag_A = f(SSK, ID_A, ID_B, Q_A, Q_B)$ where $P_A = r_A d_A Q_B^{'} T_{s_A}(R_B)$, Z computed from P_A, and $SSK = KDF(N_A, N_B, ID_A, ID_B, Z)$. Then, B could find the attack by checking the validity of $MacTag_A$. Similarly, it is clear that A could also find the modification attack. Thus, the proposed security protocol could withstand the modification attack.

Security 5: The proposed security protocol could withstand replay attacks.

Suppose the adversary C intercepts the message $m_1 = \{Q_A^{'} \parallel N_A \parallel Q_A^{''}\}$ and replay it to B, where $Q_A^{'} = r_A Q_A$. N_A and r_A are a nonce and a random number generated by A.We also suppose C replay the message $m_3 = \{MacTag_A\}$ to B upon receiving the message $m_2 = \{Q_B^{'} \parallel N_B \parallel Q_B^{''}\}$. However, B could find the attack by checking the validity of $MacTag_A$ since B generates a new nonce N_B for each session. From the similar steps, we could demonstrate that the user A could find the replay attack. Thus, the proposed security protocol could withstand the replay attack.

5.2 Performance Analysis

In this section, the computational cost and storage space of the proposed protocol is analyzed and also compared with Eun et al.'s protocol and Debiao et al.'s protocol in Table 2. Notations are defined as follows:

T_m: The running time of an elliptic curve point multiplication operation;

T_a: The running time of an elliptic curve point addition operation;

T_{Mul}: The running time of a modular multiplication operation;

T_h: The running time of a hash function operation;

T_{kdf}: The running time of a key derivation function operation;

T_{sym}: The running time of elliptic curve encryption or decryption.

According to the paper [1], the elliptic curve point multiplication operation is computational expensive and hash function operation is more efficient than other operations. To be specific, the following values are used:$T_m \approx 1200T_{Mul}$, $T_a \approx 5T_{Mul}$, $T_h \approx 0.36T_{Mul}$. Generally speaking, the key derivation function is constructed through hash function, so $T_{kdf} \approx T_h \approx 0.36T_{Mul}$. Elliptic curve decryption mainly involves addition operation, so $T_{sym} \approx T_a \approx 5T_{Mul}$. In [2], the protocol using AES encryption in the key agreement process. As we all know symmetric encryption algorithm is faster than asymmetric cryptography algorithm. So the running time of AES encryption algorithm is negligible compared to other computing time.

In the Debiao et al.'s protocol, NFC device need additional space to store pseudonym set. A pseudonym is composed of public key, private key(encrypted with long-term key of user), ID of TSM, and signature on the message. The size of the fields generally used in NFC protocol is shown in Table 3. The size of a signal pseudonym is computes as follows:

Size of PN=Public key + Encrypted Private Key + ID of TSM +Signature=1200its

Suppose the number of pseudonyms is 1000, the memory needed to store these much pseudonyms is 146.48Kbytes. However it is not a big deal, when considering the recent trends of combining mobile device and NFC. But updated environment is limited because of the billing charges of mobile devices.

Table 3: Size of the fields

Field	Size
N_A, N_B,r_A,r_B	96bits
Q_A,Q_B	200bits
$MacTag_A$,$MacTag_B$	96bits
SSK	128bits
d_A,Z	192bits
$Enc(Q_A, d_A)$	352bits
S_{STM}	448bits

According to the protocol analysis, Chi et al.'s protocol and Eun et al.'s protocol computation efficiency are the highest, but cannot against the impersonation attack. Debiao et al.'s protocol can against the impersonation attack vulnerabilities, but the computational efficiency is low and NFC devices need additional space to store pseudonym set. The proposed protocol can against the impersonation attack, improve the computational efficiency, reduce the storage space of the NFC device and computational efficiency is improved by 24.8% compared with Debiao et al.'s.

6 Conclusion

In this paper, we proposed an improved privacy protection security protocol, according to find out the deficiencies of the protocols from Eun et al. and Debiao et al. The analysis results of security and performance show that the improved protocol can provide user anonymity, session key security, resist against the modification attacks, withstand replay attacks and withstand impersonation attack. Furthermore, the improved protocol improves the computing efficiency and reduces the storage for NFC.

Acknowledgments

This work is supported by the science and technology project of Guangdong Province(No.2015B010128014, 2015B010108002, 2015B090906016, 2014A010103029 and 2014B090908011), and the Project of Guangzhou Science and Technology(No.201508010026).

References

[1] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," *Ad Hoc & Sensor Wireless Networks*, vol. 21, no. 2, pp. 121–149, 2014.

[2] Y. L. Chi, C. H. Chen, and I. C. Lin, "The secure transaction protocol in NFC card emulation mode," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 431–438, 2015.

[3] H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 1, pp. 153–160, 2013.

[4] H. Eun, H. Lee, J. Son, and S. Kim, "Conditional privacy preserving security protocol for NFC applications," in *IEEE International Conference on Consumer Electronics (ICCE'12)*, pp. 380–381, Las Vegas, NV, Jan. 2012.

[5] Gartner, *Market Insight: The Outlook on Mobile Payment*, Technical Report, Market Analysis and Statistics, May 2010.

[6] P. Gope and T. L. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Systems Journal*, vol. 99, no. 1, pp. 1–10, 2015.

[7] D. He, N. Kumar, and J. H. Lee, "Secure pseudonym-based near field communication protocol for the consumer internet of things," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 1, pp. 56–62, 2015.

[8] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 7336–746, 2011.

[9] ISO/IEC, *Information Technology – Telecommunications and Information Exchange Between Systems – NFC Security – Part 1: NFC-SEC NFCIP-1 Security Services and Protocol*, ISO/IEC 13157-1:2010.

[10] ISO/IEC, *Information Technology – Telecommunications and Information Exchange Between Systems – NFC Security – Part 2: NFC-SEC Cryptography Standard Using ECDH and AES*, ISO/IEC 13157-2: 2010.

[11] Juniper Research, *NFC Mobile Payments and Retail Marketing: Business Models & Forecasts 2012-2017*, Tenical Report, May 2012.

[12] J. H. Lee, J. Chen, and T. Ernst, "Securing mobile network prefix provisioning for NEMO based vehicular networks," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 170–187, 2012.

[13] J. Li, S. Li, and Z. Chen, "Cryptanalysis and improvement of lai's authenticated group key transfer protocol," *Application Research of Computers*, vol. 32, no. 1, pp. 254–257, 2015.

[14] X. Niu, S. Guo, and Y. Wang, "Elliptic curve lightweight authentication and key agreement scheme," *Computer Science*, vol. 42, no. 1, pp. 137–141, 2015.

[15] Q. Qian, Y. L. Jia, and R. Zhang, "A lightweight RFID security protocol based on elliptic curve crytograph," *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361, 2016.

[16] S. Wang, S. Liu, and D. Chen, "Security analysis and improvement on two RFID authentication protocols," *Wireless Personal Communications*, vol. 82, no. 1, pp. 21–33, 2015.

[17] X. Wang, Z. Huang, Q. Wen, and H. Zhang, "An efficient anonymous batch authenticated and key agreement scheme using self-certified public keys in VANETs," in *IEEE Region 10 Conference on TENCON*, pp. 1–4, Xian, Oct. 2013.

[18] C. H. Wei, M. S. Hwang, and A. Y. H Chin, "A mutual authentication protocol for RFID," *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, 2011.

[19] C. H. Wei, M. S. Hwang, and Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Network Security*, vol. 10, no. 5, pp. 508–520, 2012.

[20] Z. Wu, "Research on privacy-preserving key technologies of the NFC mobile application system," *The PLA Information Engineering University*, 2012.

Jie Ling received his Ph.D degree in computation mathematics from Sun Yat-sen University (China) in June 1998. He is a professor in computer science in Guangdong University of Technology. His current research interest fields include computer applications and Intelligent video processing technology.

Ying Wang received her bachelor's degree from University of Jinan in China in June 2013. She is currently a master degree candidate in Guangdong University of Technology (China). Her current research interest includes network security protocols, cloud computing security and big data security.

Weifeng Chen received Ph.D. degree in Computer Science from University of Massachusetts at Amherst in September 2006. He is also a tenured associate professor in Department of Mathematics and Computer Science in California University of Pennsylvania. His current research interest includes cyber security, privacy protection, artificial intelligence and big data security.