Hindawi
Security and Communication Networks
Volume 2017, Article ID 4796373, 9 pages
https://doi.org/10.1155/2017/4796373

Research Article

NFC Secure Payment and Verification Scheme with CS E-Ticket

Kai Fan,[1] Panfei Song,[1] Zhao Du,[1] Haojin Zhu,[2] Hui Li,[1] Yintang Yang,[3] Xinghua Li,[1] and Chao Yang[1]

[1]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China*
[2]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*
[3]*Key Laboratory of Ministry of Education for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi'an, China*

Correspondence should be addressed to Kai Fan; kfan@mail.xidian.edu.cn

Received 29 March 2017; Accepted 5 June 2017; Published 10 July 2017

Academic Editor: Qing Yang

As one of the most important techniques in IoT, NFC (Near Field Communication) is more interesting than ever. NFC is a short-range, high-frequency communication technology well suited for electronic tickets, micropayment, and access control function, which is widely used in the financial industry, traffic transport, road ban control, and other fields. However, NFC is becoming increasingly popular in the relevant field, but its secure problems, such as man-in-the-middle-attack and brute force attack, have hindered its further development. To address the security problems and specific application scenarios, we propose a NFC mobile electronic ticket secure payment and verification scheme in the paper. The proposed scheme uses a CS E-Ticket and offline session key generation and distribution technology to prevent major attacks and increase the security of NFC. As a result, the proposed scheme can not only be a good alternative to mobile e-ticket system but also be used in many NFC fields. Furthermore, compared with other existing schemes, the proposed scheme provides a higher security.

1. Introduction

IoT [1] is a large network that consists of various information sensing devices and the Internet. As a short-range, high-frequency communication technology, NFC (Near Field Communication) [2, 3] is one of the core technologies of IoT and is listed as one of the most promising technologies.

NFC is a development and breakthrough of the RFID (Radio Frequency Identification) [4–6] technology. It is a short-range, high-frequency, noncontact automatic identification wireless communication technology using the 13.56 MHz frequency band at a distance of less than 10 cm. Compared with traditional identification technology, it can not only provide simple and fast secure wireless connection but also has a good compatibility and low power consumption characteristic. Because its communication distance is less than 10 cm and it has SE (Secure Element) for storing data, NFC has a higher security performance and can be applicable to the payment and verification field which needs a higher security demand such as electronic train ticket, electronic movie ticket, and other fields [7]. Though it has lots of advantages, NFC faces many security problems. Especially in the open wireless communication environment [8, 9], the information exchange between the device and the device will make it easier to suffer any kinds of security attacks, such as man-in-the-middle attack and brute force attack, which will lead to disclosure of user privacy. These security problems have become one of the bottlenecks of NFC to promote its development.

On the current research status, researchers at home and abroad do not put forward a universal applicability scheme. In NFC mutual authentication phase, Yun-Seok et al. [10] propose a scheme that uses the asymmetric encryption and hash function to try to eliminate the security and privacy thread. Although the solution can solve the problem of mutual authentication and prevent replay attack and the man-in-the-middle attack, it lacks some necessary security attributes, such as the message authentication. Ceipidor et al. [11] propose a scheme which uses the symmetric encryption. This scheme implements the mutual authentication between the NFC mobile device and mobile POS device, but it cannot guarantee the integrity of the message.

In recent years, because the application of electronic ticket became wider and wider, more and more people are paying attention to security and privacy problems in ticket purchase and verification process. In the purchase process, Ceipidor et al. [12] put forward a scheme using symmetric encryption, asymmetric encryption, calibration values, and other technologies. For the possible security problems in the purchase ticket process, this solution is able to achieve mutual authentication and message integrity function and resist the man-in-the-middle attack to some extent. However, because of using the fixed symmetric key encryption, this scheme not only increases the complexity of mobile devices purchasing tickets on the Internet but also leads to the security performance being reduced greatly. Furthermore, the solution cannot cope with "spike refund" malicious ticket transactions behavior.

Meanwhile, in the verification process, some scholars believe that we can use infrastructure treatment scheme that is based on PKI (Public Key Infrastructure) system; the solution adopts asymmetric public key way to generate a digital signature. E-ticket holders and mobile verification devices can ensure its security through the random number verification mode under the PKI system. But this solution needs very complex calculation and cannot achieve necessary security attributes. At the same time, there are many other shortcomings, for example, the poor user experience and ticket clone issue, so the solution cannot solve security and privacy thread in the verification process. In order to better promote the NFC technology, a scheme is needed to be proposed to solve the security and privacy thread.

Therefore, in this paper, we propose a new NFC mobile electronic ticket payment and verification system. Compared with the old NFC system, this system not only solves problems that exist in purchase and verification process of e-ticket but also designs a CS E-Ticket, making entire system resist stronger attack with greater security.

The rest of this paper is organized as follows. In Section 2, the related works are provided. In Section 3, the NFC mobile electronic ticket system is provided, including scheme structure, CS E-Ticket, CS E-Ticket secure payment, and verification schemes. In Section 4, the performance analysis of the system is evaluated in terms of security and practicality. Section 5, the security proof with BAN logic of proposed protocol will be provided. Finally, concluding remarks are provided.

2. Related Works

2.1. The Session Key Generation Technology. In this part, we mainly discuss the offline session key generation technology [13] used in payment and verification system we proposed below. It can generate a set of new session keys in the offline environment. Key generation will be divided into two parts: the first part is initialization and the second part is the key generation process.

Initialization Settings. Alice and Bob share (K_{AB}, DK, m), K_{AB} is a long-term key assumed to be never expired, DK is called "distributed key," and m is a random number used to specify the number of keys that will be generated. m also varies randomly among different pairs of parties.

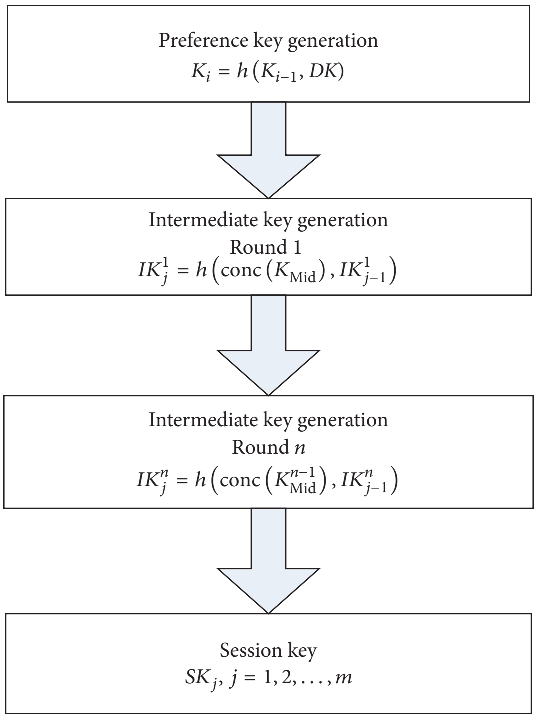

Preference key generation
$K_i = h(K_{i-1}, DK)$
Intermediate key generation
Round 1
$IK_j^1 = h(\text{conc}(K_{\text{Mid}}), IK_{j-1}^1)$
Intermediate key generation
Round n
$IK_j^n = h(\text{conc}(K_{\text{Mid}}^{n-1}), IK_{j-1}^n)$
Session key
SK_j, $j = 1, 2, \ldots, m$

Figure 1: Session key generation.

$\text{conc}(M1, M2, M3)$ operation represents the concatenation of the messages $M1$, $M2$, and $M3$, respectively.

$H(M, K)$ stands for the keyed-hash function of the message M and the key K.

$\text{Mid}(K_1, K_w)$ stands for the middle key among $\{K_1, K2, \ldots, K_W\}$.

The key generation process is shown in Figure 1.

The following steps show the details of the session key generation.

After sharing (K_{AB}, DK, m), Alice and Bob generate a set of "preference keys" K_i, where $i = i, \ldots, m$, based on K_{AB} as follows:

$$K_i = h(K_{i-1}, DK), \tag{1}$$

where $K_{\text{AB}} = K_0$. After generating the set of K_i, K_{AB} and DK can be removed from the system, to prevent the potential security problem.

The next step is to generate sets of intermediate keys. The purpose of intermediate key generation is to increase the difficulty for cryptanalysis. In other words, it increases difficulty to trace back to the preference key and crack the session key. Our proposed framework is general in that it does not specify the number of rounds the engaging parties need to perform. The higher the number of rounds performed, the greater the security of system. However, increasing the number of rounds will take more time to complete. The proposed intermediate key generation is performed as follows:

$$IK_j^x = h(\text{conc}(IK_{\text{Mid}}^{x-1}), IK_{j-1}^X), \tag{2}$$

where x specifies the round number. j specifies the number of intermediate keys that is generated, $j = 1, \ldots, m$. IK^{x-1}_{Mid1} stands for the set of $\{IK^{x-1}_{\text{Mid1}}, IK^{x-1}_{\text{Mid2}}, IK^{x-1}_{\text{Mid3}}\}$. $IK^{x}_{\text{Mid1}} = \text{mid}(IK^x_1, IK^x_{rm})$ and rm is the remaining number of intermediate keys in the set of IK^x_j. $IK^x_{\text{Mid2}} = \text{mid}(IK^x_{\text{mid1}}, IK^x_{rm})$. $IK^x_{\text{Mid3}} = \text{mid}(IK^x_1, IK^x_{\text{mid2}})$. $IK^1_{\text{Mid1}} = K_{\text{Mid1}}$, $IK^1_{\text{Mid2}} = K_{\text{Mid2}}$, and $IK^1_{\text{Mid3}} = K_{\text{Mid3}}$. The generation of $K_{\text{Mid1}}, K_{\text{Mid2}}$, and K_{Mid3} is the same as that of IK^x_{Mid1}, IK^x_{Mid2}, IK^x_{Mid3}. $IK^x_0 = \phi$.

The previously used intermediate keys in any round can be removed from the system. Thus, the remaining intermediate keys in each round can be written as follows:

$$\begin{gathered}\{K_1, K_2, \ldots, K_{rm}\} \\ \left\{IK^1_1, IK^1_2, \ldots, IK^1_{rm}\right\} \\ \left\{IK^2_2, IK^2_2, \ldots, IK^2_{rm}\right\} \\ \vdots \\ \{IK^n_1, IK^n_2, \ldots, IK^n_{rm}\}.\end{gathered} \tag{3}$$

The output of the last round of intermediate key generation is considered as session keys SK_j, where $j = 1, \ldots, m$, which is shown below:

$$IK^n_1 = SK_1, IK^n_2 = SK_2, \ldots, IK^n_{rm} = SK_m. \tag{4}$$

Then Alice and Bob can use SK_j as a credential to secure transactions. Because the session key was generated purely offline and is based on dynamically chosen input, it increases greatly the difficulty of crack.

2.2. Description of the NTRU Algorithm. The NTRU algorithm [14–16] is an open secret system invented by three professors of mathematics at Brown University in 1996. It is a cryptosystem based on polynomial rings, and its security depends on the shortest vector problem (SVP). Compared with RSA and ECC algorithm, the NTRU is simple and fast, has small storage space, and has the ability to resist quantum attacks. Therefore, next we will introduce the key generation, encryption, and decryption process as follows.

The NTRU cryptosystem depends on three integer parameters (N, p, q) and four sets L_f, L_g, L_m, L_ϕ of polynomials of degree $N-1$ with integer coefficients. Note that p and q need not be prime, but we will assume that $\gcd(p, q) = 1$, and q will always be considerably larger than p.

2.2.1. Key Generation. To create an NTRU key, we need to randomly choose two polynomials $f, g \in L_g$. The polynomial f must satisfy the additional requirement of having inverse modulo q and modulo p. We will denote these inverses by F_q and F_p; that is, $F_q \otimes f \equiv 1 \pmod{q}$ and $F_p \otimes f \equiv 1 \pmod{p}$.

Next compute the quantity $h \equiv F_q \otimes g \pmod{q}$.

Finally, the polynomial h is the public key. The polynomial f is the private key. In practice, the F_q and F_p also need to be kept confidential.

2.2.2. Encryption. If Alice wants to send a message to Bob, she begins by selecting a message m from the set of plaintexts L_m. Next she randomly chooses a polynomial $\phi \in L_\phi$ and uses Bob's public key h to compute $e \equiv p\phi \otimes h + m \pmod{q}$.

This is the encrypted message which Alice sends to Bob.

2.2.3. Decryption. Suppose that Bob has received the message e from Alice and wants to decrypt it using his private key f. To do this efficiently, Bob should have precomputed the polynomial F_p described before.

In order to decrypt e, Bob first computes $a \equiv f \otimes e \pmod{q}$, where he chooses the coefficients of a in the interval from $-q/2$ to $q/2$. Now treating a as a polynomial with integer coefficients, Bob recovers the message by computing $m = F_p \otimes a \pmod{p}$.

Finally, Bob gets the plaintext m that Alice sends to him.

3. The Design of NFC Mobile Electronic Ticket System

In this section, in order to better describe the system which we proposed, we will introduce it from the scheme structure, CS E-Ticket, CS E-Ticket secure payment, and verification schemes.

3.1. Scheme Structure. The system consists of server, mobile device, mobile POS terminals, and mobile verification terminals. There are four stages: registration, booking, purchase, and verification. The communication in e-ticket registration and booking process is done in a wireless way. In order to make the whole system more convenient and secure, the communication between mobile devices will be done via the NFC. Structure of the proposed scheme is shown in Figure 2.

(1) *Registration:* the user signs up to an online service. Server will store user's personal information, user's bank information, and sensitive information into its own database. Sensitive information includes the serial number of mobile device security element (IC) and shared key (K_0, DK, m) where K_0 is initial key, DK is distribution key, and m is random number. Later both user mobile device and server can create a set of session keys, $SK_{\text{MD-}Sj}$, $j = 1, 2, \ldots, m$, by using the key generation technology.

(2) *Booking:* user will use mobile device to book tickets on the ticket platform which service providers provide.

(3) *Purchase:* after booking process is finished, the user will use mobile device to complete payment operation via the mobile POS device. Later the mobile device will get e-ticket information. The communication between server and mobile POS terminal is realized by wireless way.

(4) *Verification:* the mobile verification terminal can communication with the user mobile device by NFC and easily verify the validity of the e-ticket stored in mobile device.

3.2. CS E-Ticket. This CS E-Ticket consists of the security and context, two parts [17]. The context part mainly consists

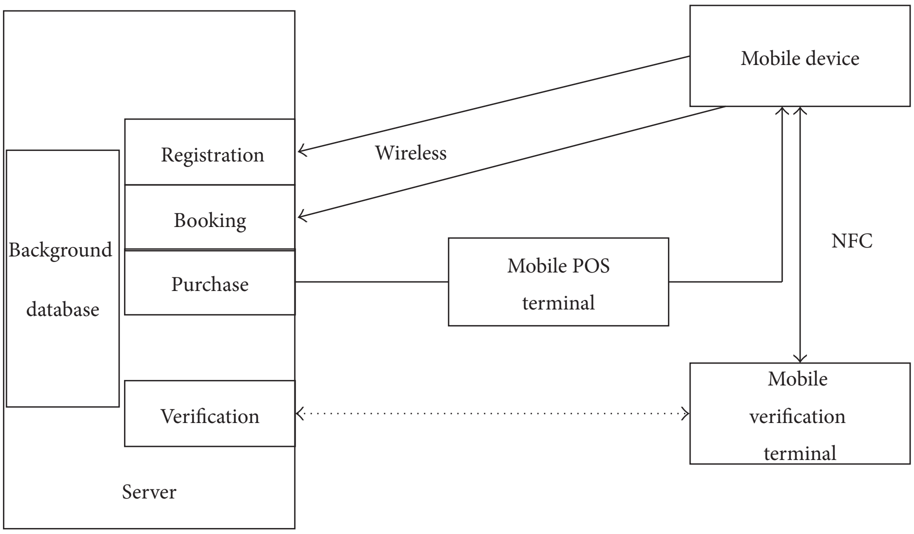


Figure 2: Scheme structure.

Table 1: CS E-Ticket.

Content part	Security part
Title	$\mathrm{ID}_{\text{ticket}}$
Location	$\mathrm{ID}_{\text{company}}$
Seat	IC
Time	R
Mark	
SK	$h(m)$
Package	

of some ticket certification information that ticket providers provide. The security part mainly includes some confidential information.

As shown in Table 1, the content part of ticket has title, location, seat number, time, and Mark. Among them, the Mark is used to indicate whether or not the ticket has been locked. The security part contains the following field: $\mathrm{ID}_{\text{ticket}}$, one time certification for ticket, and IC serial number. IC serial number is unique number built in the SE IC that cannot be modified or erased and $\mathrm{ID}_{\text{company}}$ represents service provider. R denotes a random number of tickets for each transaction.

The content part is encrypted by symmetric key. The security party is stored by using the calculated hash values. The CS E-Tickets style could be various depending on the service providers; take bus ticket as an example; it might not have the seat information. Finally, the CS E-Ticket providers will package the context and security part of ticket which has been encrypted.

This scheme clearly classifies the ticket information. On the one hand, it uses symmetric encryption encrypt content part to prevent information leakage; on the other hand, it adopts hash values to keep ticket information confidential, making the CS E-Ticket have stronger security.

3.3. CS E-Tickets NFC Payment Scheme. In this section, there are three entities involved in our payment scheme: the mobile device (MD from now on), the mobile POS terminal ($\mathrm{MD}_{\mathrm{POS}}$ from now on), and the server (S from now on). Description of symbols used in the program is shown in Symbols.

The user holds mobile device (MD) containing the necessary data information to achieve the certification of $\mathrm{MD}_{\mathrm{POS}}$. $\mathrm{MD}_{\mathrm{POS}}$ is responsible for the transaction process. The server as a trusted third party shares symmetric key and each entry ID with MD. All communication between MD and $\mathrm{MD}_{\mathrm{POS}}$ is done via NFC. The communication between the server and $\mathrm{MD}_{\mathrm{POS}}$ is done via the wireless communication which is based on the wireless security transport layer protocol (WTLS). Both sides of communication transfer payment information, key information, and entry id information in a safe way.

When session key needs to be updated, we can take the offline session key generation technology [11] to update the session key.

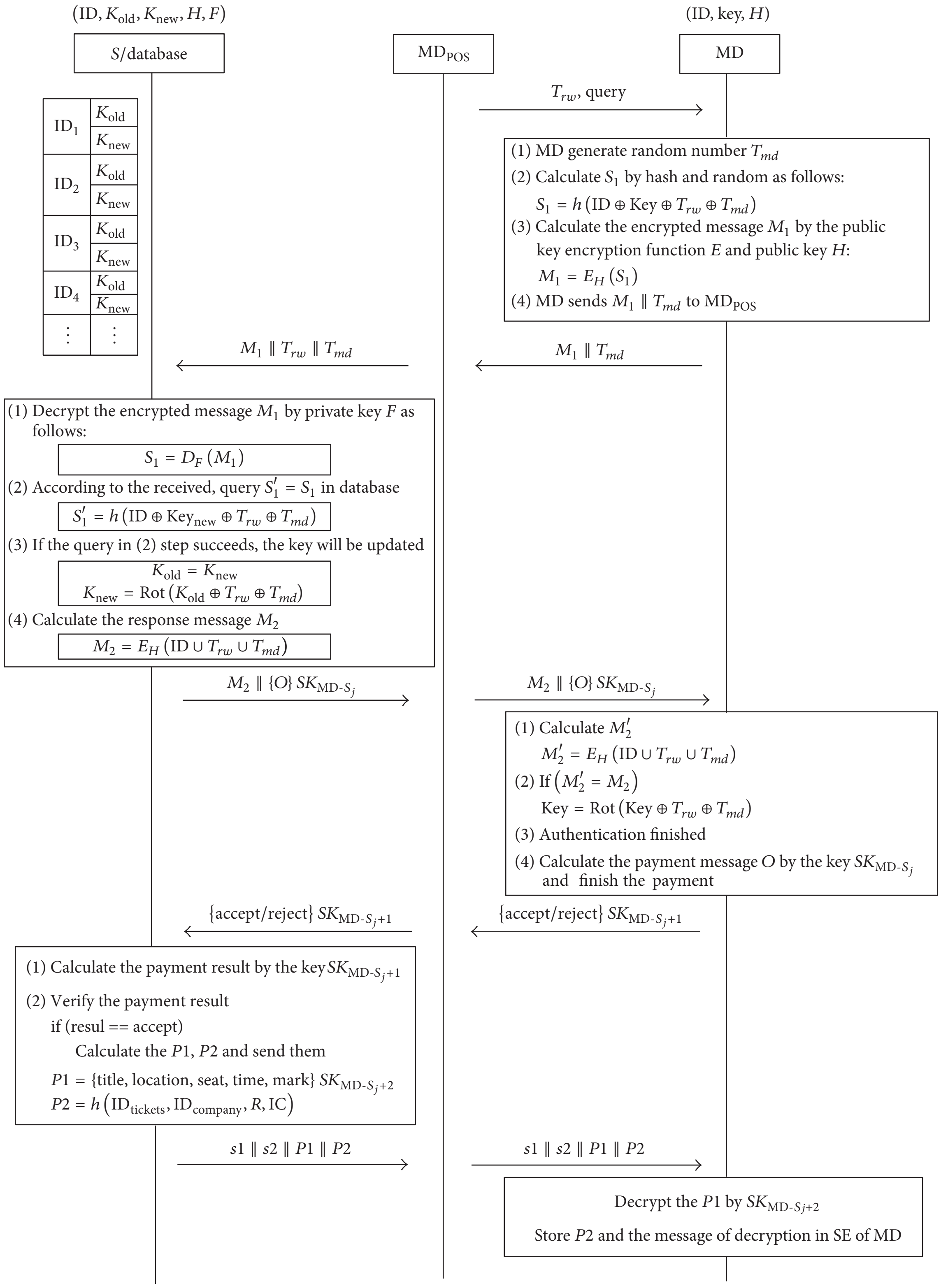
In order to start the payment process, user has to move MD closer to the RF field of the $\mathrm{MD}_{\mathrm{POS}}$ by using NFC multimodal features. Considering the e-ticket information security, we can store e-ticket information in NFC SE. Specific steps are in Figure 3.

3.3.1. Initialization. Firstly, the database generates the private key F and public key H and shares the public key H with the MD. Then the secret key K is generated by database and initialized to $K_i = \mathrm{Rot}(\mathrm{ID} \oplus r_{i,j})$. The $r_{i,j}$ is the random number that the system randomly assigns to the ith tag at the initialization phase. Meanwhile, it is shared with MD. In addition to the secret key K, the ID is stored in both the database and the MD.

3.3.2. The Authentication Process. There are two stages in the scheme that we proposed. One is authentication stage, and the other is payment stage. Then we will introduce the two stages in detail as follows.

Authentication Stage

(1) The $\mathrm{MD}_{\mathrm{POS}}$ first generates the random number T_{rw} by a pseudo-random generator and sends the authentication query *Query* and T_{rw} to the MD.


$(\text{ID}, K_{\text{old}}, K_{\text{new}}, H, F)$
S/database
MD_{POS}
$(\text{ID}, \text{key}, H)$
MD
ID_1
K_{old}
K_{new}
ID_2
K_{old}
K_{new}
ID_3
K_{old}
K_{new}
ID_4
K_{old}
K_{new}
⋮
⋮
T_{rw}, query
$M_1 \parallel T_{rw} \parallel T_{md}$
$M_1 \parallel T_{md}$
$M_2 \parallel \{O\}\, SK_{\text{MD-}S_j}$
$M_2 \parallel \{O\}\, SK_{\text{MD-}S_j}$
$\{\text{accept/reject}\}\, SK_{\text{MD-}S_j+1}$
$\{\text{accept/reject}\}\, SK_{\text{MD-}S_j+1}$
$s1 \parallel s2 \parallel P1 \parallel P2$
$s1 \parallel s2 \parallel P1 \parallel P2$

(1) MD generate random number T_{md}

(2) Calculate S_1 by hash and random as follows:

$S_1 = h\left(\text{ID} \oplus \text{Key} \oplus T_{rw} \oplus T_{md}\right)$

(3) Calculate the encrypted message M_1 by the public key encryption function E and public key H:

$M_1 = E_H\left(S_1\right)$

(4) MD sends $M_1 \parallel T_{md}$ to MD_{POS}

(1) Decrypt the encrypted message M_1 by private key F as follows:

$S_1 = D_F\left(M_1\right)$

(2) According to the received, query $S_1' = S_1$ in database

$S_1' = h\left(\text{ID} \oplus \text{Key}_{\text{new}} \oplus T_{rw} \oplus T_{md}\right)$

(3) If the query in (2) step succeeds, the key will be updated

$K_{\text{old}} = K_{\text{new}}$
$K_{\text{new}} = \text{Rot}\left(K_{\text{old}} \oplus T_{rw} \oplus T_{md}\right)$

(4) Calculate the response message M_2

$M_2 = E_H\left(\text{ID} \cup T_{rw} \cup T_{md}\right)$

(1) Calculate M_2'

$M_2' = E_H\left(\text{ID} \cup T_{rw} \cup T_{md}\right)$

(2) If $\left(M_2' = M_2\right)$

$\text{Key} = \text{Rot}\left(\text{Key} \oplus T_{rw} \oplus T_{md}\right)$

(3) Authentication finished

(4) Calculate the payment message O by the key $SK_{\text{MD-}S_j}$ and finish the payment

(1) Calculate the payment result by the key$SK_{\text{MD-}S_j+1}$

(2) Verify the payment result
    if (resul == accept)
        Calculate the $P1$, $P2$ and send them

$P1 = \{\text{title, location, seat, time, mark}\}\, SK_{\text{MD-}S_j+2}$
$P2 = h\left(\text{ID}_{\text{tickets}}, \text{ID}_{\text{company}}, R, \text{IC}\right)$

Decrypt the $P1$ by $SK_{\text{MD-}Sj+2}$

Store $P2$ and the message of decryption in SE of MD

Figure 3: CS E-Ticket NFC payment scheme.

(2) The MD generates the random number T_{md} and calculates the message $S_1 = h(\mathrm{ID} \oplus \mathrm{Key} \oplus T_{rw} \oplus T_{md})$ by T_{md} and the received random number T_{rw}. After the calculation is complete, the MD will encrypt the message S_1 by the public key H of the NTRU to get the encrypted message $M_1 = E_H(S_1)$ and sends T_{md} and M_1 to M_{POS}.

(3) When M_{POS} receives message $M_1 = E_H(S_1)$, it will decrypt the message by the private key F in order to get the message S_1. Then M_{POS} tries to find an MD which can satisfy the requirement $S_1' = h(\mathrm{ID} \oplus \mathrm{Key}_{\mathrm{new}} \oplus T_{rw} \oplus T_{md}) = S_1$ in the database back. If this search succeeds, MD is authenticated. Otherwise, the protocol is abandoned. After MD is authenticated, M_{POS} will update the key as shown in Figure 3 and calculate the response message $M_2 = E_H(\mathrm{ID} \cup T_{rw} \cup T_{md})$ by the public key H. Finally, M_{POS} sends message $M_2 \parallel \{O\}SK_{\text{MD-}S_j}$ to the MD.

(4) As soon as receiving the response message M_2, this value will be compared with a computed local version M_2'. If comparison is successful, M_{POS} is authenticated and the key will be updated as shown in Figure 2; otherwise, the protocol is abandoned.

Payment Phase

(1) After the MD is authenticated, the $\mathrm{MD}_{\mathrm{POS}}$ sends message $M_2 \parallel \{O\}SK_{\text{MD-}S_j}$ to the MD. MD decrypts the payment submessage $\{O\}SK_{\text{MD-}S_j}$ by session key $SK_{\text{MD-}S_j}$ which is stored into itself. Once MD verifies the payment information O, MD will agree and finish the payment (see Figure 3). Meanwhile, it will send payment verification information $\{\text{accept/reject}\}SK_{\text{MD-}S_j+1}$ to $\mathrm{MD}_{\mathrm{POS}}$.

(2) When the $\mathrm{MD}_{\mathrm{POS}}$ receives the payment verification information, it will first view the random numbers $s1$ and $s2$, when $s1$ and $s2$ meet a certain threshold, the user will be blacklisted. Then $\mathrm{MD}_{\mathrm{POS}}$ will use $SK_{\text{MD-}S_j+1}$ to decrypt $\{\text{accept/reject}\}SK_{\text{MD-}S_j+1}$ and view the content. Once the verification information is accepted, the $\mathrm{MD}_{\mathrm{POS}}$ will send ticket information to the MD. MD will store the received ticket information into SE of itself (see Figure 3).

3.4. Offline CS E-Ticket Secure Verification. In the verification process, there are two entries: user mobile device (MD) and mobile verification device (MD_V). The verification process is similar to the payment process, which is shown in Figure 4.

Firstly, the MD and MD_V need to complete the mutual authentication by using M_1/M_2; then MD will send MD_V the e-ticket information $P1$, $P2$ where $\mathrm{MD}_{\mathrm{POS}}$ sends MD in the payment phase. Finally, the MD_V will verify whether the content and security parts of e-ticket information are right.

4. Security Analysis of NFC Mobile Electronic Ticket System

4.1. Security Analysis. In this section, we will analyze our proposed system scheme from the point of view of security and practicability.

4.1.1. Mutual Authentication. The scheme uses message $M_1 = E_H(S_1)$ to implement the authentication for mobile POS device and then use again $M_2 = E_H(\mathrm{ID} \cup T_{rw} \cup T_{md})$ to implement the authentication for mobile device. So the scheme can implement mutual authentication.

4.1.2. Confidentiality. In the proposed scheme, all exchange information will use symmetric key to ensure that the message is in the cipher state.

4.1.3. Nontracking. Because the response message generated by the same devices is different in each session, attacker could not assure the tracking attack successfully because there is no the fixed messages [5].

4.1.4. Brute Force Attack. According to the proposed system scheme, it is difficult to find the correct session key as session key change every time at the completion of transaction. In addition, applying an offline key generation technology can increase resistance to brute force attacks [18].

4.1.5. Forward Security. Because the session key is different in each session, the attacker cannot obtain the previous interactive information.

4.1.6. Replay Attack Prevention. By using nonce and limited-use session keys, the proposed system scheme can prevent replay attack [16] as the session keys used in this scheme are used only once.

4.1.7. Man-in-the-Middle-Attack. An attacker who pretends to be an authorized party is not able to analyze the transmitted message since the session keys used in our scheme are changed constantly by using strong encryption.

4.1.8. The "Spike Refund" Attack. Because the scheme will calculate the times of purchase and refund within a certain period of time, if the times reach the upper limit, the user will be pulled into the blacklist. By this way, the system scheme we proposed can prevent "spike refund" attack.

4.1.9. The e-Ticket Clone Attack. For the system scheme we proposed, on the one hand, the security part information is displayed to user in the form of hash value. On the other hand, we bind the IC serial number to user mobile device. By this way, the cloned e-ticket cannot finish the authentication and verification process, which prevent the e-ticket clone attack [19].

4.2. Practicability Analysis. For the train stations, airports and other places where the flow of people is large and the security needs are higher, the proposed scheme has a strong practicability comparing with other schemes in Table 2.

According to Table 2, the proposed scheme has fewer operations and hash computation and spends less time to complete the transaction. The scheme only adopts simple shift operation and symmetric key with a lightweight.

Table 2: The analysis of practicability.

	Symmetric encryption	Symmetric decryption	Nonsymmetric encryption	Nonsymmetric decryption	Hash function	Message number
Yun-Seok et al.	4	4	1	1	3	6
Ceipidor et al.	—	—	2	2	3	6
León-Coca et al.	7	7	—	—	—	7
E-ticket NFC payment scheme	2	2	1	1	1	5
Offline e-ticket verification scheme	2	2	1	1	1	5

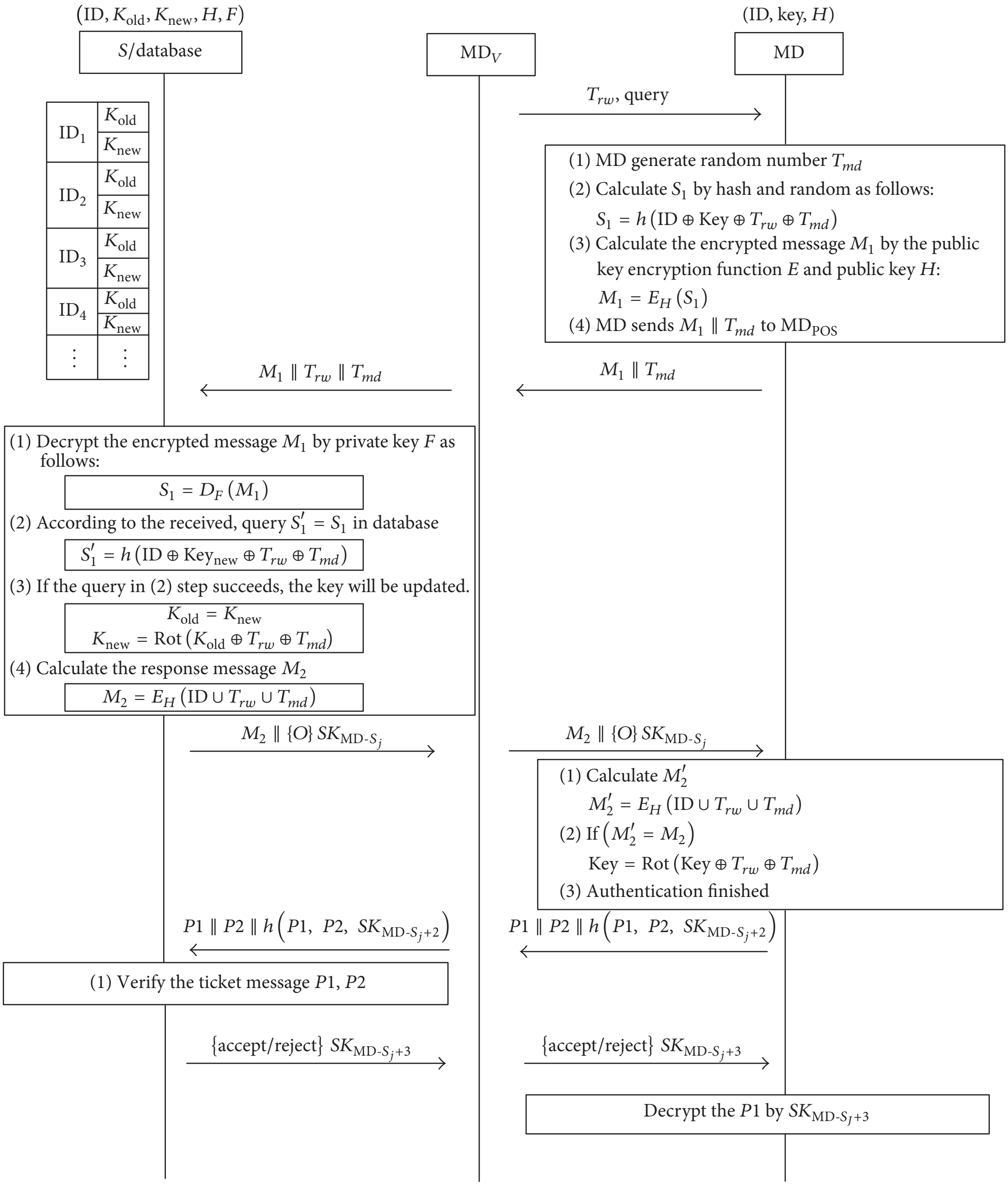

$(\mathrm{ID}, K_{\mathrm{old}}, K_{\mathrm{new}}, H, F)$
S/database
MD_V
$(\mathrm{ID}, \mathrm{key}, H)$
MD
T_{rw}, query
ID_1
K_{old}
K_{new}
ID_2
K_{old}
K_{new}
ID_3
K_{old}
K_{new}
ID_4
K_{old}
K_{new}
⋮ ⋮
(1) MD generate random number T_{md}
(2) Calculate S_1 by hash and random as follows:
$S_1 = h(\mathrm{ID} \oplus \mathrm{Key} \oplus T_{rw} \oplus T_{md})$
(3) Calculate the encrypted message M_1 by the public key encryption function E and public key H:
$M_1 = E_H(S_1)$
(4) MD sends $M_1 \parallel T_{md}$ to $\mathrm{MD}_{\mathrm{POS}}$
$M_1 \parallel T_{rw} \parallel T_{md}$
$M_1 \parallel T_{md}$
(1) Decrypt the encrypted message M_1 by private key F as follows:
$S_1 = D_F(M_1)$
(2) According to the received, query $S_1' = S_1$ in database
$S_1' = h(\mathrm{ID} \oplus \mathrm{Key}_{\mathrm{new}} \oplus T_{rw} \oplus T_{md})$
(3) If the query in (2) step succeeds, the key will be updated.
$K_{\mathrm{old}} = K_{\mathrm{new}}$
$K_{\mathrm{new}} = \mathrm{Rot}(K_{\mathrm{old}} \oplus T_{rw} \oplus T_{md})$
(4) Calculate the response message M_2
$M_2 = E_H(\mathrm{ID} \cup T_{rw} \cup T_{md})$
$M_2 \parallel \{O\}\, SK_{\mathrm{MD}\text{-}S_j}$
$M_2 \parallel \{O\}\, SK_{\mathrm{MD}\text{-}S_j}$
(1) Calculate M_2'
$M_2' = E_H(\mathrm{ID} \cup T_{rw} \cup T_{md})$
(2) If $(M_2' = M_2)$
$\mathrm{Key} = \mathrm{Rot}(\mathrm{Key} \oplus T_{rw} \oplus T_{md})$
(3) Authentication finished
$P1 \parallel P2 \parallel h(P1,\ P2,\ SK_{\mathrm{MD}\text{-}S_j+2})$
$P1 \parallel P2 \parallel h(P1,\ P2,\ SK_{\mathrm{MD}\text{-}S_j+2})$
(1) Verify the ticket message $P1$, $P2$
{accept/reject} $SK_{\mathrm{MD}\text{-}S_j+3}$
{accept/reject} $SK_{\mathrm{MD}\text{-}S_j+3}$
Decrypt the $P1$ by $SK_{\mathrm{MD}\text{-}S_J+3}$

Figure 4: CS E-Ticket NFC verification protocol.

Computation Cost. Compared with other protocols, the protocols we have proposed only require less operation, including hash operation and encryption operation. Therefore, our protocol is more low-cost.

Communication Cost. When the protocol we proposed is compared with other protocols, we can observe that the authentication phase and transaction phase only require five messages; it is less than other protocols in communication. This means that our protocol is more fast and effective.

5. Security Proof with BAN Logic

Because the authentication of payment and verification protocol is the same, we will use the BAN logic [20, 21] to prove the mutual authentication part of the payment in this section.

The core security assurance of the proposed protocol is the secure mutual authentication, which means the following security aims should be achieved.

Security Aim 1. Database needs to make sure the received message $M_1 \parallel T_{rw} \parallel T_{md}$ is exactly the one sent by MD. This means that we need to achieve Database $\mid\equiv$ MD_i $\mid\sim$ (M_1, T_{rw}, T_{md}) and Database $\mid\equiv$ MD_i $\mid\equiv$ (M_1, T_{rw}, T_{md}).

Security Aim 2. The MD needs to make sure the received message M_2 is exactly the one sent by the Database, which means the following formulas need to be achieved: MD_i $\mid\equiv$ Database $\mid\sim$ M_2 and MD_i $\mid\equiv$ Database $\mid\equiv$ M_2.

5.1. Security Assumption. According to the given protocol, with the Database and $\mathrm{MD}_{\mathrm{POS}}$ connected securely, the following conditions can be achieved:

$$\text{AS1: Database} \mid\equiv \text{ Database} \overset{r_{i,j}}{\rightleftarrows} \mathrm{MD}_i$$

$$\text{AS2: } \mathrm{MD}_i \mid\equiv \text{ Database} \overset{r_{i,j}}{\rightleftarrows} \mathrm{MD}_i$$

$$\text{AS3: } \mathrm{MD}_{\mathrm{POS}} \Rightarrow (T_{rw})$$

$$\text{AS4: } \mathrm{MD}_{\mathrm{POS}} \mid\equiv \#(T_{rw})$$

$$\text{AS5: Database} \mid\equiv \#(T_{rw})$$

$$\text{AS6: } \mathrm{MD}_i \Rightarrow (T_{md})$$

$$\text{AS7: } \mathrm{MD}_i \mid\equiv \#(T_{md})$$

5.2. Security Analysis. According to the payment protocol $K_i = \mathrm{Rot}(\mathrm{ID} \oplus r_{i,j})$, together with the assumptions AS1 and AS2, we can deduce $\mathrm{Database}_i$ $\mid\equiv$ Database $\overset{K_i}{\rightleftharpoons}$ MD_i and MD_i $\mid\equiv$ Database $\overset{K_i}{\rightleftharpoons}$ MD_i. In this scheme, the database will receive the message $M_1 \parallel T_{rw} \parallel T_{md}$ forwarded from the $\mathrm{MD}_{\mathrm{POS}}$, where $M_1 = E_H(\mathrm{ID} \oplus K \oplus T_{md} \oplus T_{rw})$. As we have achieved K_i as secret between the database and MD, we can take K_i as the secret key to protect messages. So we can simply write the received message of database as $(M_1 \parallel T_{rw} \parallel T_{md})_{K_i}$, and we have Database $\triangleleft$ $(M_1 \parallel T_{rw} \parallel T_{md})_{K_i}$. For the reason of "message-meaning rule" of BAN, $(P \mid\equiv Q \overset{Y}{\rightleftharpoons} P, P \triangleleft \langle X \rangle_Y)/P \mid\equiv (Q \mid\sim X)$, we can deduce Database $\mid\equiv$ MD_i $\mid\sim$ (M_1, T_{rw}, T_{md}).

From the assumption AS5: Database $\mid\equiv$ $\#(T_{rw})$ and the BAN rule of $P \mid\equiv \#(\mathrm{X}), /P \mid\equiv \#(X, Y)$, we know Database $\mid\equiv$ $\#(M_1, T_{rw}, T_{md})$. Because we have achieved Database $\mid\equiv$ MD_i $\mid\sim$ $\#(M_1, T_{rw}, T_{md})$, together with the "nonce-verification" rule $(P \mid\equiv (\#(X)), P \mid\equiv (Q \mid\sim X))/P \mid\equiv (Q \mid\equiv X)$, we will achieve Database $\mid\equiv$ MD_i $\mid\equiv$ (M_1, T_{rw}, T_{md}), and the first security aim of the given protocol is achieved.

For the same reason, we can also deduce MD_i $\mid\equiv$ Database $\mid\sim$ M_2 and MD_i $\mid\equiv$ Database $\mid\equiv$ M_2, and the second of security aim is also achieved, and the security of mutual authentication of the proposed protocol has been proved.

6. Conclusions

Firstly, this paper designs and introduces an electronic ticket system from the point of view of the registration, booking, ticketing, and verification. This system is composed of servers, mobile device, mobile POS device, and mobile verification terminals. For the problems existing in ticketing process, this paper proposes an e-ticket NFC payment scheme. This scheme can not only give the user good experience but also protect the user e-ticket security information. For the problems in the verification process, an offline session key generation and distribution technology is introduced. On the one hand, this technology increases the security of the communication between each entity. On the other hand, it can cope with the "spike refund" issue so that the system we proposed can be applied to train tickets, air tickets, and other fields which need higher requirements.

Symbols

SE:	Security element of NFC devices
MD:	User mobile device
$\mathrm{MD}_{\mathrm{POS}}$:	Mobile POS device
ID:	User mobile device ID
T_{rw}, T_{md}:	Random number generated by MD, $\mathrm{MD}_{\mathrm{pos}}$
O:	Payment information
H:	The public key of database
$P1, P2$:	The content part and security of e-ticket
$\{m\}SK$:	The message m encrypted by the key SK
$h(m)$:	The hash of the message m
$S1, S2$:	The number of times of purchase and refund in a certain time
$SK_{\text{MD-}Sj}$:	Shared session key between MD and server
$\{h(m)\}SK$:	The hash of the message m encrypted by key SK
F:	The private key of database.

Disclosure

Part of the work entitled "NFC Secure Payment and Verification Scheme for Mobile Payment" was presented at the 11th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2016), Bozeman, Montana, USA, August 8–10, 2016.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work has been financially supported by the National Natural Science Foundation of China (nos. 61303216, 61272457, U1401251, and 61373172), the National High Technology Research and Development Program of China (863 Program) (no. 2012AA013102), the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (no. ICT170312), and National 111 Program of China B16037 and B08038.

References

[1] H. Ning and B. Wang, *RFID major projects and the state internet of things*, Mechanical Industry Press, 2008.

[2] V. Odelu, A. K. Das, and A. Goswami, "SEAP: secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 30–38, 2016.

[3] M. Badra and R. B. Badra, "A lightweight security protocol for NFC-based mobile payments," in *Proceedings of the 7th International Conference on Ambient Systems, Networks and Technologies, ANT 2016 and the 6th International Conference on Sustainable Energy Information Technology, SEIT 2016*, pp. 705–711, May 2016.

[4] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Security & Communication Networks*, pp. 1–14, 2015.

[5] K. Fan, J. Li, H. Li, X. Liang, X. S. Shen, and Y. Yang, "RSEL: revocable secure efficient lightweight RFID authentication scheme," *Concurrency and Computation: Practice and Experience*, vol. 26, no. 5, pp. 1084–1096, 2014.

[6] E. Haselsteiner, "Security in Near Field Communication (NFC)," in *Proceedings of the Workshop on Rfid Security Malaga*, 2006.

[7] M. Pasquet, J. Reynaud, and C. Rosenberger, "Secure payment with NFC mobile phone in the smart touch project," in *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS '08)*, pp. 121–126, May 2008.

[8] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: a QoE-oriented framework," *IEEE Network*, vol. 30, no. 1, pp. 2–57, 2016.

[9] Q. Xu, Z. Su, B. Han, D. Fang, Z. Xu, and X. Gan, "Analytical model with a novel selfishness division of mobile nodes to participate cooperation," *Peer-to-Peer Networking and Applications*, 2015.

[10] Y. S. Lee, E. Kim, and M. S. Jung, "A NFC based authentication method for defense of the man in the middle attack," in *Proceedings of the 3rd International Conference on Computer Science and Information Technology*, pp. 10–14, 2013.

[11] U. B. Ceipidor, C. M. Medaglia, A. Marino, S. Sposato, and A. Moroni, "KerNeeS: a protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions," in *Proceedings of the 2012 9th International ISC Conference on Information Security and Cryptology, ISCISC 2012*, pp. 115–120, September 2012.

[12] U. B. Ceipidor, C. M. Medaglia, A. Marino et al., "Mobile ticketing with NFC management for transport companies problems and solutions," in *Proceedings of the 2013 5th International Workshop on Near Field Communication, NFC 2013*, pp. 1–6, February 2013.

[13] S. Kayser, B. Bewernick H, and R. Hurlemann, "A secure offline key generation with protection against key compromise. Physical review. B," *Condensed matter*, vol. 51, no. 4, pp. 2550–2555, 2009.

[14] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU. A Ring-Based Public Key Cryptosystem Algorithmic Number Theory*, Springer, Berlin, Germany, 1998.

[15] J. H. Cheon, J. Jeong, and C. Lee, "An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero," *LMS Journal of Computation and Mathematics*, vol. 19, no. A, pp. 255–266, 2016.

[16] C. van Vredendaal, "Reduced memory meet-in-the-middle attack against the NTRU private key," *LMS Journal of Computation and Mathematics*, vol. 19, no. A, pp. 43–57, 2016.

[17] W. J. Wu and W. H. Lee, "An NFC E-ticket system with offline authentication," in *Proceedings of the 9th International Conference on Information, Communications and Signal Processing, ICICS 2013*, December 2013.

[18] C. Thammarat, R. Chokngamwong, C. Techapanupreeda, and S. Kungpisdan, "A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys," in *Proceedings of the International Conference on Information Networking (ICOIN '15)*, pp. 133–138, Siem Reap, Cambodia, January 2015.

[19] K. Fan, P. Song, Z. Du et al., "NFC secure payment and verification scheme for mobile payment," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9798, pp. 116–125, 2016.

[20] M. Cohen and M. Dam, "Logical omniscience in the semantics of BAN Logic," in *Proceedings of the Foundations of Computer Security Workshop*, pp. 121–132, 2003.

[21] A. Qiao-Mei M, "The design of low-cost RFID protocols and BAN formal analysis," *Journal of Baoji University of Arts Sciences*, 2016.

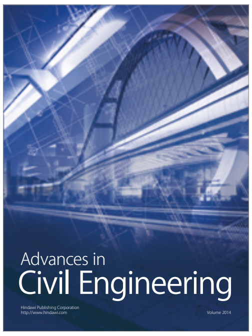
Journal of
Engineering

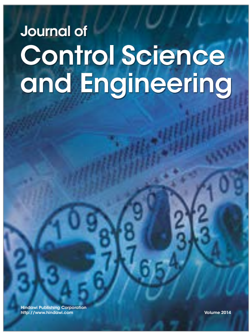
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

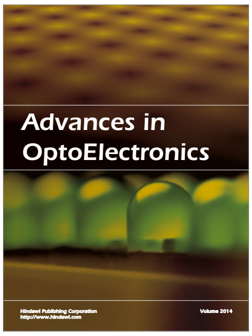
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

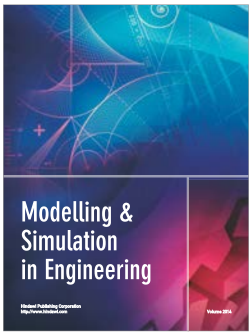
Journal of
Robotics

Journal of
Electrical and Computer Engineering

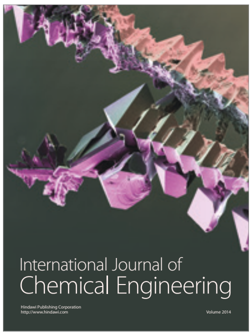

Advances in
OptoElectronics

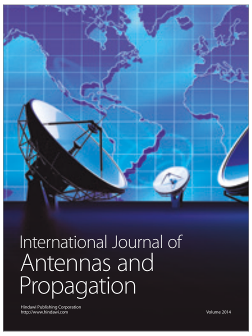
VLSI Design

International Journal of
Navigation and Observation

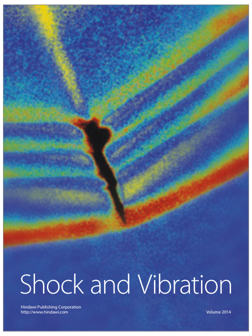

Modelling &
Simulation
in Engineering

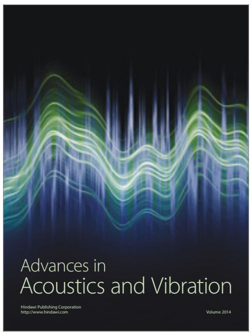
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration